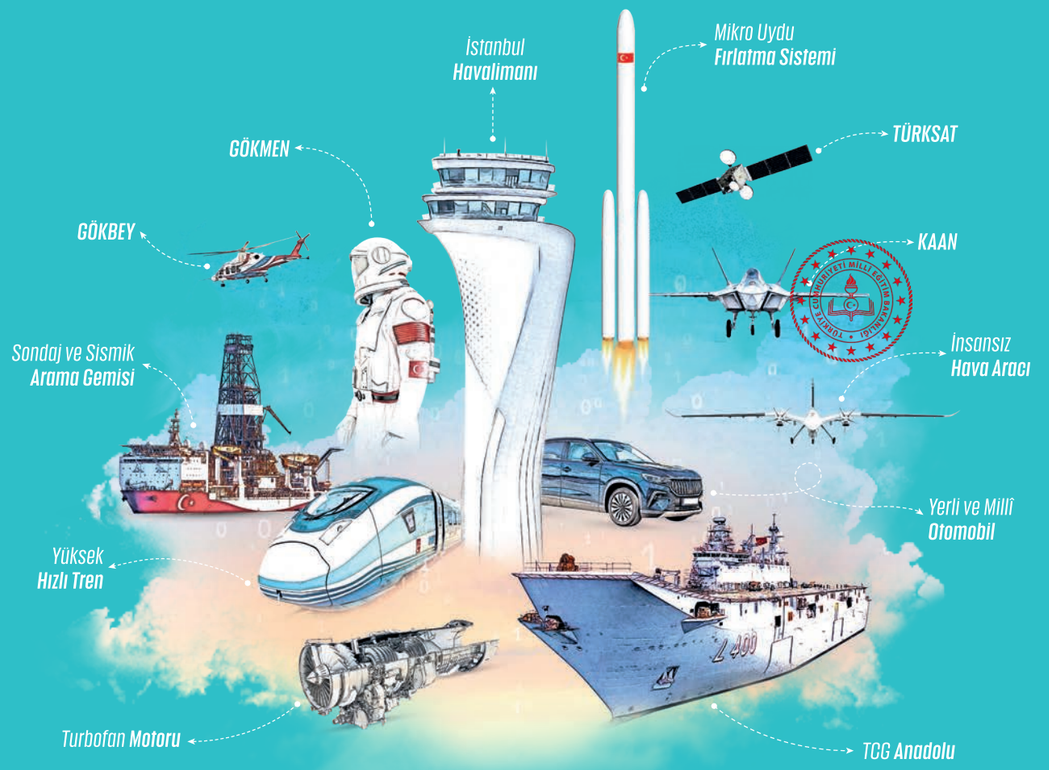
Bu kitaba sığmayan daha neler var!

eba
www.eba.gov.tr

Karekodu okut, bu kitapla ilgili EBA içeriklerine ulaş!

Teknoloji Yolculuğumuz



BU DERS KİTABI MİLLÎ EĞİTİM BAKANLIĞINCA ÜCRETSİZ OLARAK VERİLMİŞTİR.
PARA İLE SATILAMAZ.

ISBN: 978-625-5498-40-3

Bandrol Uygulamasına İlişkin Usul ve Esaslar Hakkında Yönetmeliğin Beşinci Maddesinin İkinci Fıkrası Çerçevesinde Bandrol Taşıması Zorunlu Değildir.

SİBER GÜVENLİK ALANI SİSTEM VE AĞ TEMELLERİ 9 DERS MATERYALİ

MESLEKİ VE TEKNİK ANADOLU LİSESİ

SİBER GÜVENLİK ALANI



SİSTEM VE AĞ TEMELLERİ

9

DERS MATERYALİ

MESLEKİ VE TEKNİK ANADOLU LİSESİ

SİBER GÜVENLİK ALANI

SİSTEM VE AĞ TEMELLERİ

9. SINIF

DERS MATERYALİ

YAZARLAR

Ayhan ÖZREK

İbrahim BİLGİN

Neslihan GENÇ

MİLLÎ EĞİTİM BAKANLIĞI YAYINLARI .....: 10954
YARDIMCI VE KAYNAK KİTAPLAR DİZİSİ.....: 03873

Her hakkı saklıdır ve Millî Eğitim Bakanlığına aittir.
Ders materyalinin metin, soru ve şekilleri kısmen de olsa hiçbir surette alınıp yayımlanamaz.

HAZIRLAYANLAR

Dil Uzmanı	**Erman Erşan YORGANCILAR**
Program Geliştirme Uzmanı	**Hakan KARADAĞLI**
Rehberlik Uzmanı	**Zeynep GÖÇ HİSARKAYA**
Ölçme ve Değerlendirme Uzmanı	**Günay DURUCAN**
Görsel Tasarım Uzmanı	**Mehmet YILMAZ**

ISBN: 978-625-5498-40-3

Millî Eğitim Bakanlığının 24.12.2020 gün ve 18433886 sayılı oluru ile
Meslekî ve Teknik Eğitim Genel Müdürlüğünce ders materyali olarak hazırlanmıştır.



İSTİKLÂL MARŞI

Korkma, sönmez bu şafaklarda yüzen al sancak;
Sönmeden yurdumun üstünde tüten en son ocak.
O benim milletimin yıldızıdır, parlayacak;
O benimdir, o benim milletimindir ancak.

Çatma, kurban olayım, çehreni ey nazlı hilâl!
Kahraman ırkıma bir gül! Ne bu şiddet, bu celâl?
Sana olmaz dökülen kanlarımız sonra helâl.
Hakkıdır Hakk'a tapan milletimin istiklâl.

Ben ezelden beridir hür yaşadım, hür yaşarım.
Hangi çılgın bana zincir vuracakmış? Şaşarım!
Kükremiş sel gibiyim, bendimi çiğner, aşarım.
Yırtarım dağları, enginlere sığmam, taşarım.

Garbın âfâkını sarmışsa çelik zırhlı duvar,
Benim iman dolu göğsüm gibi serhaddim var.
Ulusun, korkma! Nasıl böyle bir imanı boğar,
Medeniyyet dediğin tek dişi kalmış canavar?

Arkadaş, yurduma alçakları uğratma sakın;
Siper et gövdeni, dursun bu hayâsızca akın.
Doğacaktır sana va'dettiği günler Hakk'ın;
Kim bilir, belki yarın, belki yarından da yakın.

Bastığın yerleri toprak diyerek geçme, tanı:
Düşün altındaki binlerce kefensiz yatanı.
Sen şehit oğlusun, incitme, yazıktır, atanı:
Verme, dünyaları alsan da bu cennet vatanı.

Kim bu cennet vatanın uğruna olmaz ki feda?
Şüheda fışkıracak toprağı sıksan, şüheda!
Cânı, cânânı, bütün varımı alsın da Huda,
Etmesin tek vatanımdan beni dünyada cüda.

Ruhumun senden İlâhî, şudur ancak emeli:
Değmesin mabedimin göğsüne nâmahrem eli.
Bu ezanlar -ki şehadetleri dinin temeli-
Ebedî yurdumun üstünde benim inlemeli.

O zaman vecd ile bin secde eder -varsa- taşım,
Her cerîhamdan İlâhî, boşanıp kanlı yaşım,
Fışkırır ruh-ı mücerret gibi yerden na'şım;
O zaman yükselerek arşa değer belki başım.

Dalgalan sen de şafaklar gibi ey şanlı hilâl!
Olsun artık dökülen kanlarımın hepsi helâl.
Ebediyyen sana yok, ırkıma yok izmihlâl;
Hakkıdır hür yaşamış bayrağımın hürriyyet;
Hakkıdır Hakk'a tapan milletimin istiklâl!

Mehmet Âkif Ersoy

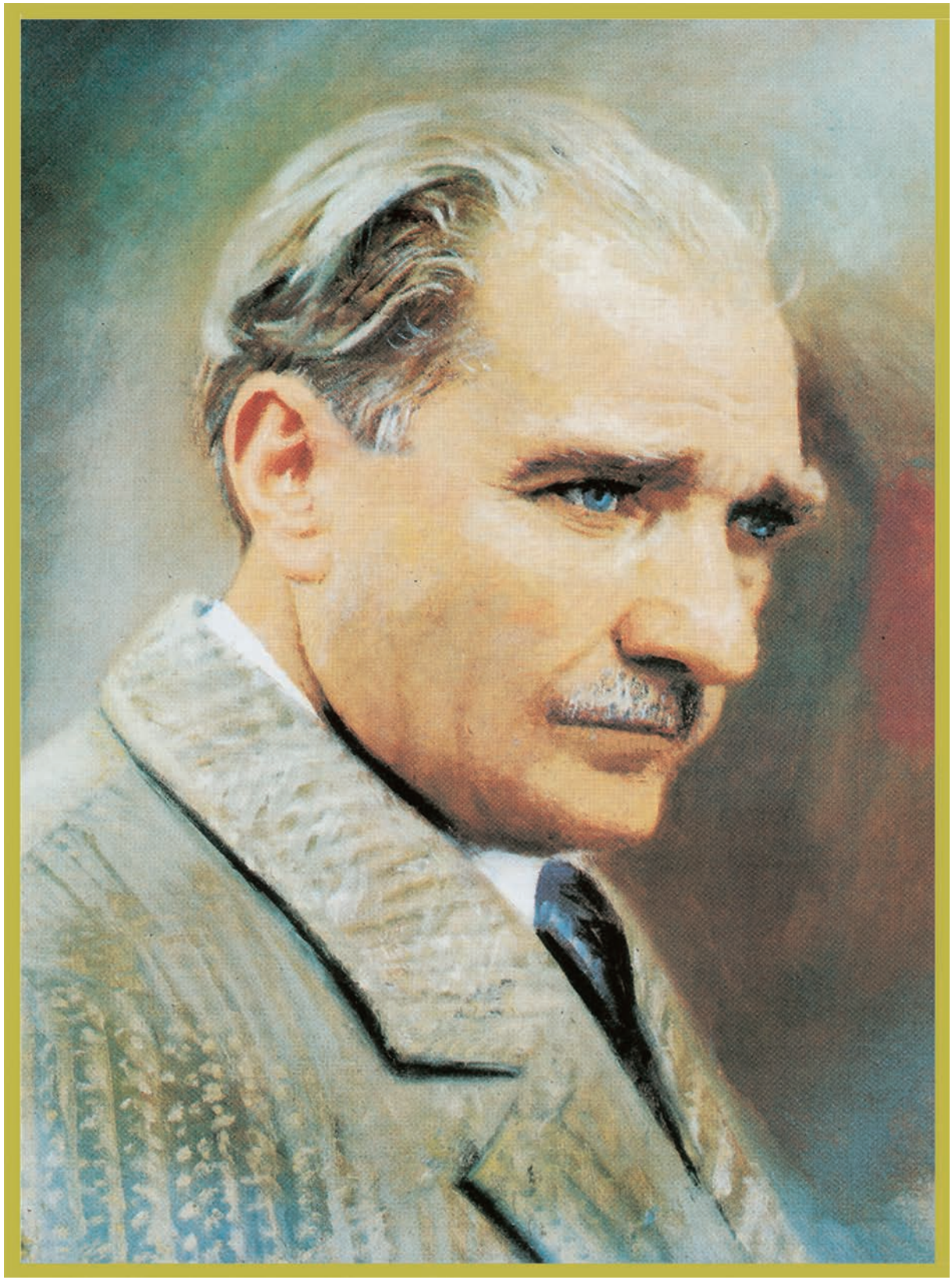
GENÇLİĞE HİTABE

Ey Türk gençliği! Birinci vazifen, Türk istiklâlini, Türk Cumhuriyetini, ilelebet muhafaza ve müdafaa etmektir.

Mevcudiyetinin ve istikbalinin yegâne temeli budur. Bu temel, senin en kıymetli hazinendir. İstikbalde dahi, seni bu hazineden mahrum etmek isteyecek dâhilî ve hâricî bedhahların olacaktır. Bir gün, istiklâl ve cumhuriyeti müdafaa mecburiyetine düşersen, vazifeye atılmak için, içinde bulunacağın vaziyetin imkân ve şeraitini düşünmeyeceksin! Bu imkân ve şerait, çok namüsait bir mahiyette tezahür edebilir. İstiklâl ve cumhuriyetine kastedecek düşmanlar, bütün dünyada emsali görülmemiş bir galibiyetin mümessili olabilirler. Cebren ve hile ile aziz vatanın bütün kaleleri zapt edilmiş, bütün tersanelerine girilmiş, bütün orduları dağıtılmış ve memleketin her köşesi bilfiil işgal edilmiş olabilir. Bütün bu şeraitten daha elîm ve daha vahim olmak üzere, memleketin dâhilinde iktidara sahip olanlar gaflet ve dalâlet ve hattâ hıyanet içinde bulunabilirler. Hattâ bu iktidar sahipleri şahsî menfaatlerini, müstevlîlerin siyasî emelleriyle tevhit edebilirler. Millet, fakr u zaruret içinde harap ve bîtap düşmüş olabilir.

Ey Türk istikbalinin evlâdı! İşte, bu ahval ve şerait içinde dahi vazifen, Türk istiklâl ve cumhuriyetini kurtarmaktır. Muhtaç olduğun kudret, damarlarındaki asil kanda mevcuttur.

Mustafa Kemal Atatürk



MUSTAFA KEMAL ATATÜRK

İÇİNDEKİLER

Ders Materyalinin Tanıtımı 15

1. ÖĞRENME BİRİMİ: DONANIM BİRİMLERİ 18

1.1. İÇ DONANIM BİRİMLERİ 21

1.1.1. Anakart 21

1.1.2. İşlemci 29

1.1.3. Bellekler 36

1.1.4. Disk Sürücüler 40

1.1.5. RAID Teknolojisi 44

1.1.6. Ekran Kartı 45

1.1.7. Ağ Arayüz Kartı 46

1.1.8. Ses Kartı 48

1.1.9. Bilgisayar Kasaları 49

1.1.10. Güç Kaynağı 50

1.1.11. Kuantum Bilgisayarlar 53

1.2. DIŞ DONANIM BİRİMLERİ 57

1.2.1. Giriş Aygıtları 57

1.2.2. Çıkış Aygıtları 59

1.2.3. Giriş-Çıkış Aygıtları 61

1.3. ENERJİ VERİMLİ DONANIM BİRİMLERİ 65

1.3.1. Enerji Verimliliği Sınıfları ve Etiketler 65

1.3.2. Enerji Verimliliği Yüksek Donanımların Belirlenmesi 70

1.3.3. Performans ve Enerji Dengesi (PPW) 70

ÖLÇME VE DEĞERLENDİRME 74

2. ÖĞRENME BİRİMİ: AĞ İLETİŞİMİ 80

2.1. OSI REFERANS MODELİ 83

2.1.1. Ağ ve Türleri 83

2.1.2. Ağ Topolojileri 84

2.1.3. Ağ Cihazları 88

2.1.4. OSI Modelinin Katmanlı Yapısı 90

2.1.5. Uygulama Katmanı 92

2.1.6. Sunum Katmanı 92
2.1.7. Oturum Katmanı 93
2.1.8. Taşıma Katmanı 93
2.1.9. Ağ Katmanı 96
2.1.10. IPv4 Protokolü 100
2.1.11. IPv4 Adres Yapısı 101
2.1.12. IPv4 Sınıflı Adresleme 102
2.1.13. IPv4 Adres Türleri 103
2.1.14. Özel IPv4 Adres Aralıkları (Private IP Addresses) 104
2.1.15. Genel IPv4 Adresleri (Public IP Addresses) 104
2.1.16. Alt Ağ Maskesi 105
2.1.17. Varsayılan Ağ Geçidi 106
2.1.18. APIPA Adresi 107
2.1.19. Loopback Adresi 107
2.1.20. IPv4 Alt Ağlara Bölme İşlemi 108
2.1.21. VLSM ile IP Adresi Planlama 111
2.1.22. IPv6 Protokolü 115
2.1.23. IPv6 Adres Yapısı 116
2.1.24. IPv6 Adres Türleri 117
2.1.25. IPv6 Adreslerini Sadeleştirme 118
2.1.26. ICMP Protokolü 120
2.1.27. ARP Protokolü 127
2.1.28. Veri Bağı Katmanı 133
2.1.29. Veri Bağı Katmanı Protokolleri 134
2.1.30. Ethernet 134
2.1.31. Wi-Fi 135
2.1.32. HDLC 136
2.1.33. PPP 136
2.1.34. Fiziksel Katman 138
2.1.35. Ethernet Fiziksel Katman Standartları 138
2.1.36. PoE (Power over Ethernet) 138
2.1.37. Ağ Medyaları 139
2.1.38. Bakır Kablo Türleri 139
2.1.39. Bükümlü Çift Yama Kablo Türleri 140

2.1.40. Bükümlü Çift Kablo Kategorileri 141
2.1.41. Bükümlü Çift Kablo Sonlandırma Standartları 142
2.1.42. Bakır Kablo Konnektör Türleri 142
2.1.43. Fiber Optik Kablo Türleri 147
2.1.44. Fiber Optik Kablo Konnektörleri 149
2.2. TCP/IP PROTOKOL KÜMESİ 150
2.2.1. TCP/IP Modeli ile OSI Referans Modelinin Karşılaştırılması 150
2.3. AĞ PROTOKOLLERİ 155
2.3.1. DHCP Protokolü 156
2.3.2. DHCPv4 Süreci DORA 156
2.3.3. DHCPv6 167
2.3.4. DNS Protokolü 175
2.3.5. HTTP ve HTTPS Protokolleri 175
2.3.6. FTP Protokolü 183
2.3.7. SMTP ve POP3 Protokolleri 192
2.3.8. Telnet ve SSH Protokolleri 199
2.3.9. TFTP Protokolü 206
ÖLÇME VE DEĞERLENDİRME 213

3. ÖĞRENME BİRİMİ: İŞLETİM SİSTEMLERİ 222
3.1. MASAÜSTÜ VE MOBİL İŞLETİM SİSTEMLERİ 225
3.1.1. İstemci-Sunucu 226
3.1.2. İşletim Sistemi Türleri 227
3.1.3. Mobil İşletim Sistemleri 228
3.1.4. Açık Kaynak Kodlu İşletim Sistemleri 230
3.1.5. Kapalı Kaynak Kodlu İşletim Sistemleri 266
3.2. SUNUCU İŞLETİM SİSTEMLERİ 295
3.2.1. Sunucu İşletim Sistemi Kurulumu 297
3.2.2. Sunucu İşletim Sistemi Yapılandırması 301
3.2.3. Sunucuda Veri Güvenliği 305
ÖLÇME VE DEĞERLENDİRME 310

4. ÖĞRENME BİRİMİ: SANALLAŞTIRMA VE BULUT BİLİŞİM 316

4.1. SANALLAŞTIRMA 319

4.1.1. Hipervizör Türleri 319

4.1.2. Konteyner Mimarisi 337

4.2. BULUT BİLİŞİM 354

4.2.1. Bulut Bilişim Sistemleri 356

4.2.2. Bulut Bilişim İşletim Sistemleri 358

ÖLÇME VE DEĞERLENDİRME 363

5. ÖĞRENME BİRİMİ: SİBER GÜVENLİĞE GİRİŞ 368

5.1. ETİK VE YASAL SORUMLULUKLAR 371

5.1.1. Etik İlkeleri 372

5.1.2. Mahremiyet (Gizlilik) İlkeleri 373

5.1.3. Bilgi Güvenliğiyle İlgili Yasal Zorunluluklar 373

5.1.4. Telif Hakkı 374

5.1.5. Dijital Vatandaşlık 374

5.1.6. Siber Güvenlik Uzmanı 378

5.2. GENEL GÜVENLİK KONSEPTİ 379

5.2.1. Güvenlik Kavramları 379

5.2.2. Güçlü Parola ve Bütünlük Kontrolü 380

5.2.3. Hacker Kavramı 382

5.2.4. Siber Saldırı Yaşam Döngüsü 384

5.2.5. Siber Saldırı Türleri 385

5.2.6. Zararlı Yazılım ve Kullanım Yerleri 387

5.2.7. Sosyal Mühendislik Saldırı Türleri 390

5.2.8. Tehdit Aktörleri 393

5.2.9. Siber Tehdit İstihbaratı ve Yöntemleri 394

5.2.10. Tehdit ve Risk 396

5.2.11. Zafiyet Testi ve Sızma Testi 399

5.2.12. Siber Saldırılara Karşı Güvenlik Takımları 402

5.2.13. Siber Güvenlik Kontrolleri 403

5.2.14. Bilgi Güvenliği Standartları 404

5.2.15. Uluslararası Siber Güvenlik Çerçeveleri 406

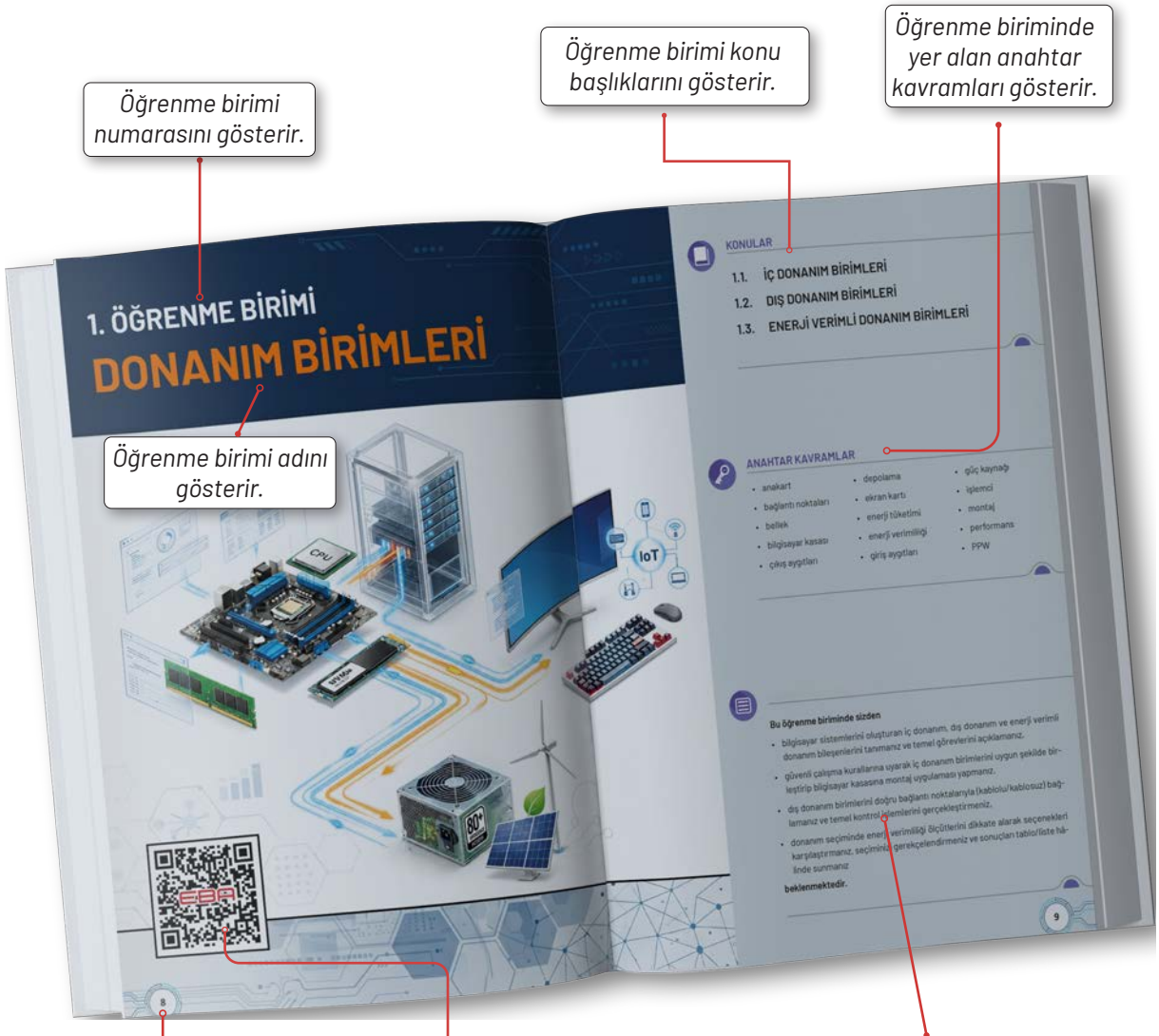
5.2.16. Siber Güvenlik Sertifikasyon Süreçleri 407
5.3. FİZİKSEL GÜVENLİK 411
5.3.1. Erişim Kontrol Sistemleri (Kayıt ve Yetkilendirme) 411
5.3.2. Çevre Güvenliği 411
5.3.3. Kamera ve İzleme Sistemleri (CCTV) 412
5.3.4. Yangın, Sel ve Çevresel Önlemler 412
5.3.5. Enerji Güvenliği 412
5.4. DİJİTAL ARŞİVLEME 413
ÖLÇME VE DEĞERLENDİRME 416

6. ÖĞRENME BİRİMİ: KRİPTOGRAFİ 420
6.1. KRİPTOLOJİ TEMELLERİ 422
6.1.1. Kriptografi, Kriptanaliz ve Kodlama 424
6.2. KLASİK KRİPTOGRAFİ 435
6.2.1. Sezar Şifreleme Algoritması 435
6.2.2. Vigenere Şifreleme Algoritması 437
6.2.3. Yerine Koyma Şifrelemesi 439
6.2.4. Vernam Şifrelemesi 439
6.2.5. Klasik Şifreleme Yöntemlerinin Güçlü ve Zayıf Yönleri 440
6.3. ÖZET FONKSİYONLARI 446
6.3.1. Hash Fonksiyonu 446
6.3.2. MD5, SHA-1, SHA-256 ve SHA-512 Algoritmaları 451
6.3.3. Parola Saklama, Hashleme ve Salting 454
6.3.4. Rainbow Table Mantığı 455
6.3.5. Bcrypt, Scrypt ve Argon2 Mantığı 455
6.4. SİMETRİK KRİPTOGRAFİ 459
6.4.1. Simetrik Şifrelemenin Çalışma Mantığı 459
6.4.2. DES, 3DES, AES ve RC4 Algoritmaları 464
6.4.3. AES ile Simetrik Şifreleme Mantığı 465
6.4.4. Simetrik Şifreleme Yöntemlerini Karşılaştırma 468
6.5. ASİMETRİK KRİPTOGRAFİ 469
6.6. DİJİTAL İMZA VE SERTİFİKALAR 479
6.6.1. Dijital İmza 479
6.6.2. Elektronik İmza ve 5070 Sayılı Elektronik İmza Kanunu 481

6.6.3. Dijital Sertifika 481
6.6.4. X.509 Sertifikaları, Sertifika Otoritesi ve Güven Zinciri 482
6.6.5. SSL/TLS Sertifikalarının Web Sitelerinde Kimlik Doğrulamadaki Rolü 482
6.6.6. Dijital İmza ve Sertifikaları Karşılaştırma 485
6.7. VERİ GİZLEME 487
6.7.1. Steganografi 487
6.7.2. Steganografi ile Kriptografi Arasındaki Fark 487
6.7.3. Dijital Watermarking ve Steganaliz 488
ÖLÇME VE DEĞERLENDİRME 500

KAYNAKÇA 504
GENEL AĞ, GÖRSEL, E-İÇERİK KAYNAKÇASI KAREKODU 507
CEVAP ANAHTARLARI KAREKODU 507
TÜRKİYE'NİN MÜLKİ İDARE BÖLÜMLERİ İLE KARA VE DENİZ KOMŞULARI HARİTASI 508
TÜRK DÜNYASI HARİTASI 509

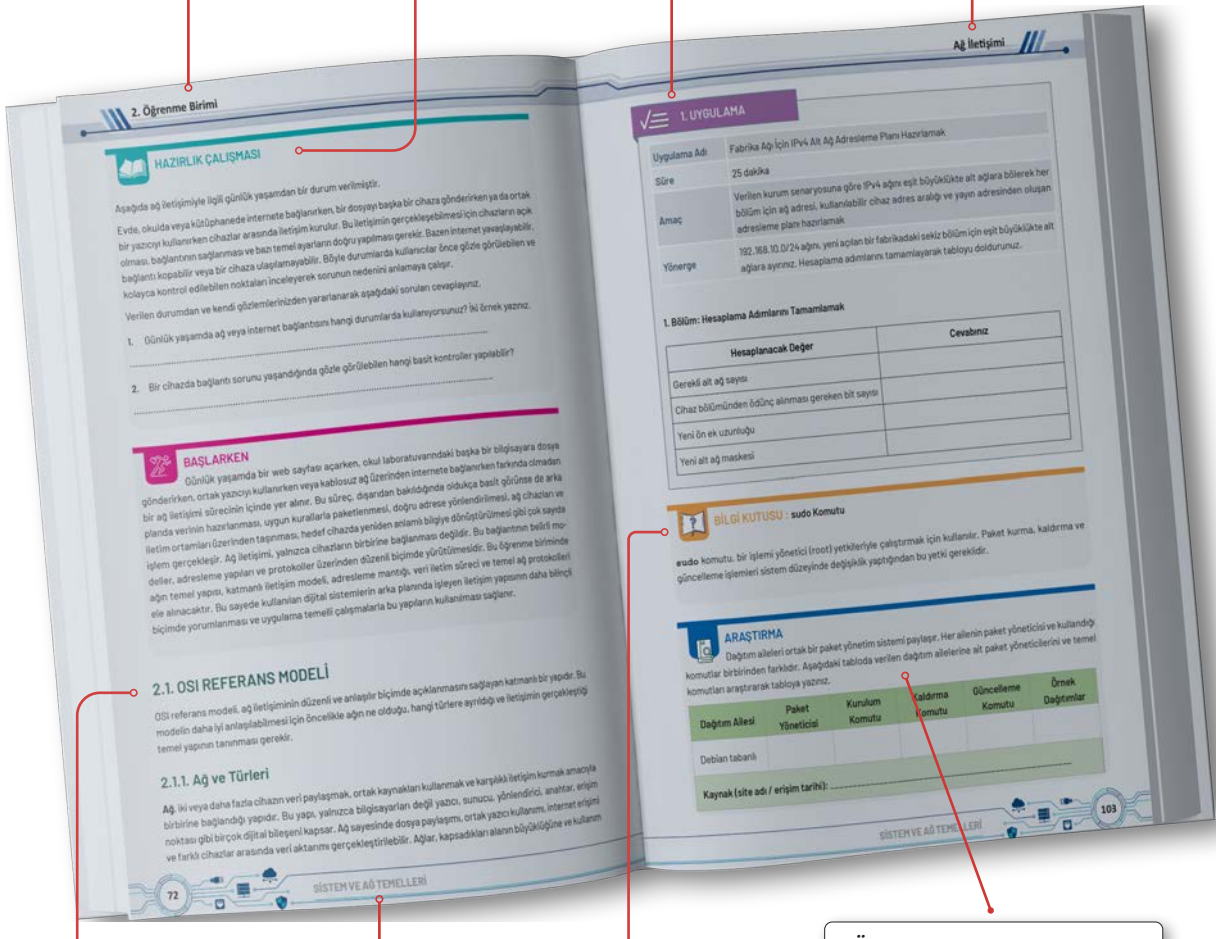
Ders Materyalinin Tanıtımı



MATERYAL GENELİNDE KULLANILAN İKONLAR

Konular	Uygulama	Sıra Sizde
Anahtar Kavramlar	Bilgi Kutusu	Kontrol Noktası
Beklentiler	Başlarken	Örnek Uygulama
Hazırlık Çalışmaları	Araştırma	Siber Güvenlik Penceresi

Ders Materyalinin Tanıtımı



Konulara başlanmadan önce yapılacak hazırlık çalışmalarını gösterir.

Öğrenme birimi adını gösterir.

Konuları destekleyici ve pekiştirici uygulama çalışmalarını gösterir.

Öğrenme birimi numarasını gösterir.

Öğrenme birimi çıktılarıyla bağlantılı araştırma çalışmalarını gösterir.

Konu başlığını gösterir.

Ders materyalinin adını gösterir.

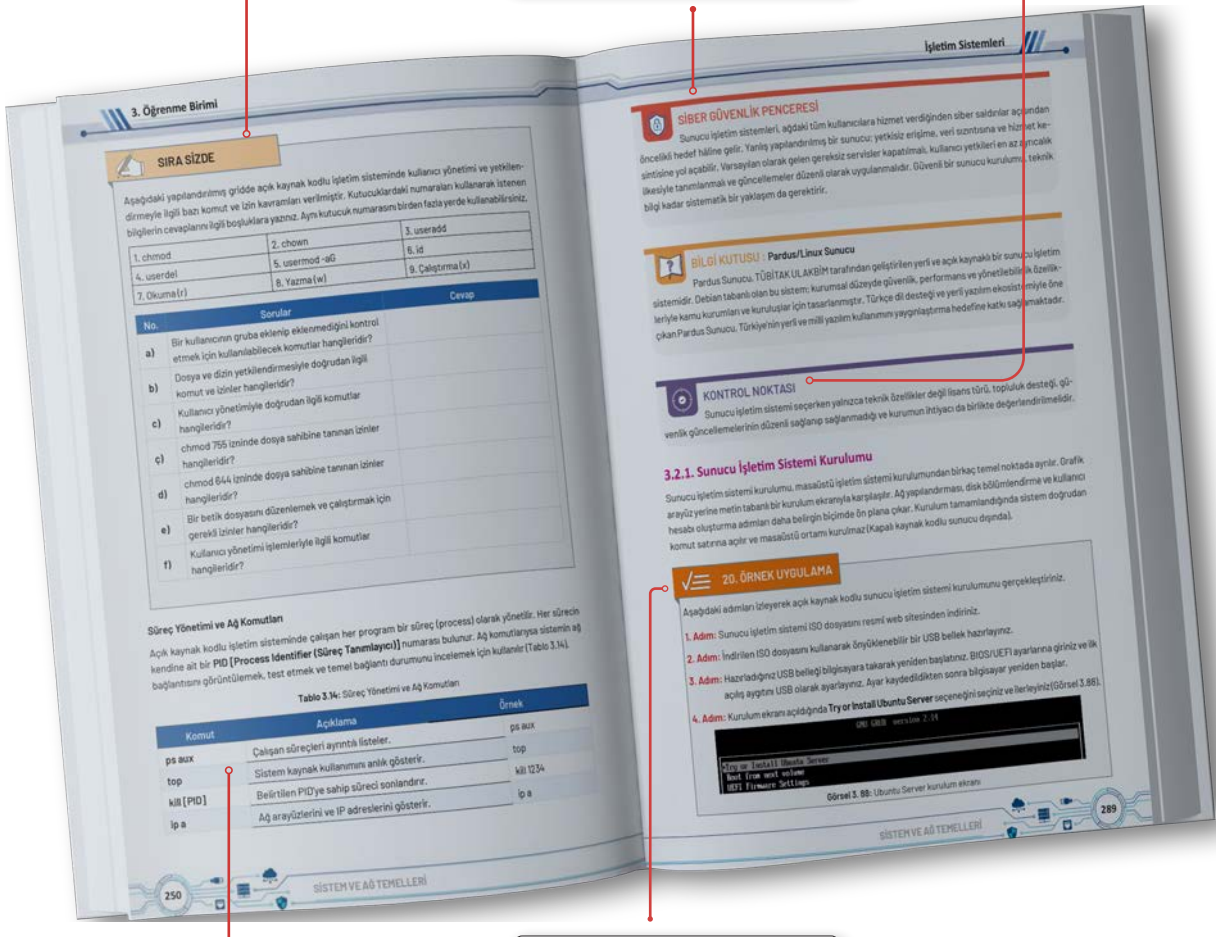
Konuları pekiştirici ve destekleyici ek bilgileri gösterir.

Ders Materyalinin Tanıtımı

İşlenen konuyla ilgili dikkat edilmesi gereken temel noktaları gösterir.

Konuları destekleyici ve pekiştirici sıra sizde çalışmalarını gösterir.

Konuyla ilgili siber güvenlik risklerini ve alınması gereken önlemleri hatırlatır.

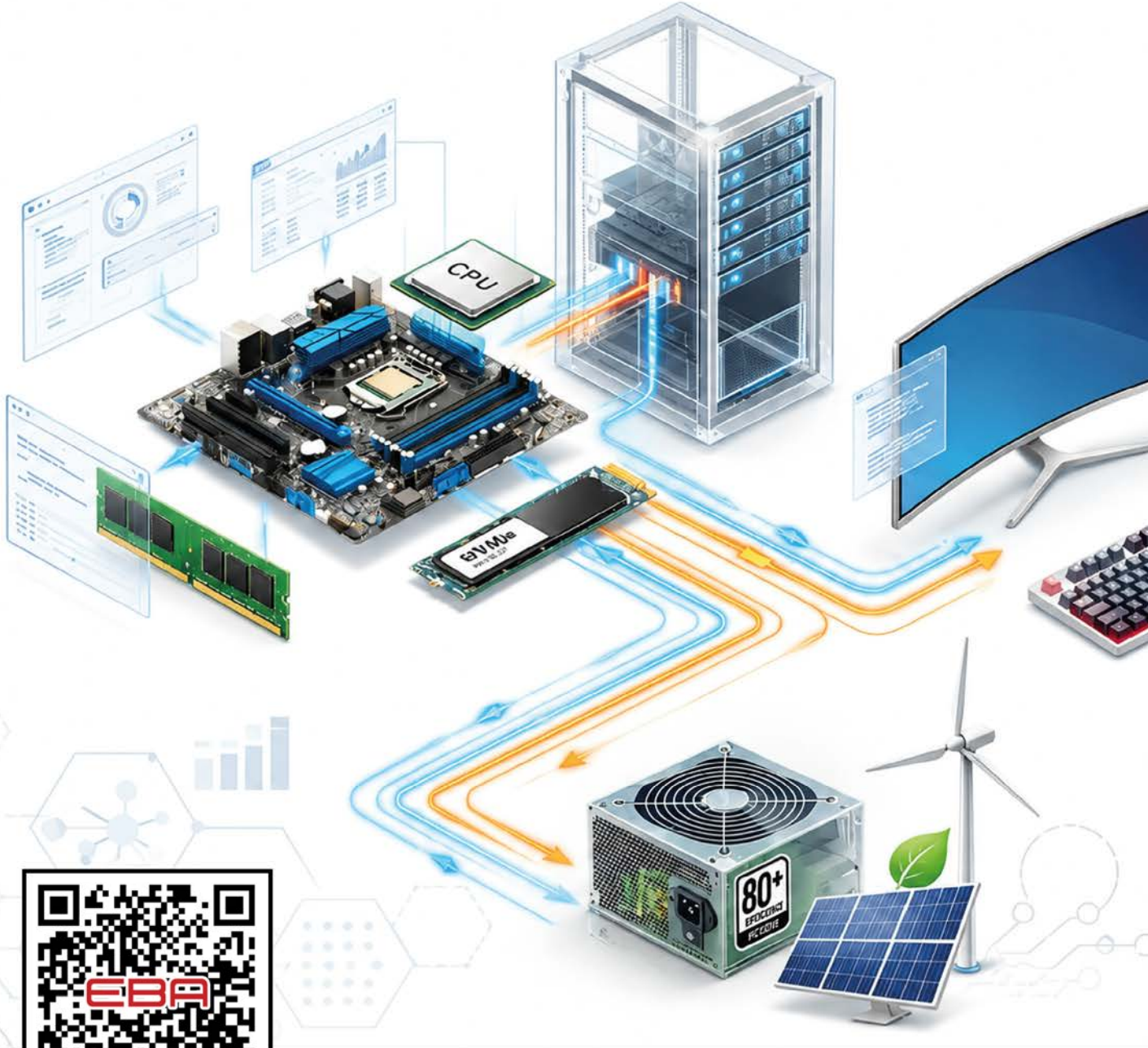


Konuları destekleyici ve pekiştirici örnek uygulama çalışmalarını gösterir.

Öğrenme birimi içinde kullanılan tabloları gösterir.

1. ÖĞRENME BİRİMİ

DONANIM BİRİMLERİ





KONULAR

1.1. İÇ DONANIM BİRİMLERİ

1.2. DIŞ DONANIM BİRİMLERİ

1.3. ENERJİ VERİMLİ DONANIM BİRİMLERİ

ANAHTAR KAVRAMLAR

- anakart
- bağlantı noktaları
- bellek
- bilgisayar kasası
- çıkış aygıtları
- depolama
- ekran kartı
- enerji tüketimi
- enerji verimliliği
- giriş aygıtları
- güç kaynağı
- işlemci
- montaj
- performans
- PPW

Bu öğrenme biriminde sizden

- bilgisayar sistemlerini oluşturan iç donanım, dış donanım ve enerji verimli donanım bileşenlerini tanımanız ve temel görevlerini açıklamanız,
- güvenli çalışma kurallarına uyarak iç donanım birimlerini uygun şekilde birleştirip bilgisayar kasasına montaj uygulaması yapmanız,
- dış donanım birimlerini doğru bağlantı noktalarıyla (kablolu / kablosuz) bağlamanız ve temel kontrol işlemlerini gerçekleştirmeniz,
- donanım seçiminde enerji verimliliği ölçütlerini dikkate alarak seçenekleri karşılaştırmanız, seçiminizi gerekçelendirmeniz ve sonuçları tablo / liste hâlinde sunmanız

beklenmektedir.

HAZIRLIK ÇALIŞMASI

1. Aşağıdaki görsel, dijital veri güvenliği ile ilgili verilmiştir. Görseli inceleyiniz.



Verilen görselden hareketle aşağıdaki soruları cevaplayınız.

a) Görseldeki öğrencinin, bilgisayarın sadece ekranını kırarak içindeki fotoğraf, belge ve şifrelerin tamamen yok olacağını düşünmesindeki mantık hatasını nasıl açıklarsınız?

_____

_____

b) Görseldeki diğer öğrenci, arkadaşının "Artık kimse verilerime ulaşamaz." düşüncesini neden bilgisayar kasasını göstererek sorgulamaktadır? Açıklayınız.

_____

_____

2. Eski bir telefon, tablet veya bilgisayar başkasına verilmeden önce içindeki verilerin korunmasının neden önemli olduğunu ve verilerin başkalarının eline geçmemesi için hangi önlemlerin alınması gerektiğini açıklayınız.

_____

_____

BAŞLARKEN

Günlük hayatta kullanılan bilgisayarların bazen aniden yavaşladığı, fan sesinin rahatsız edici şekilde arttığı, ekranın görüntü vermediği veya klavye, fare, yazıcı gibi parçaların aniden çalışmayı durdurduğu fark edilebilir. Bazen sorun tek bir parçadan kaynaklanır. Kimi zaman parçaların birbiriyle uyumsuzluğu veya yanlış bağlantılar sistemin kararlılığını bozar. Aynı işi yapan iki bilgisayardan birinin hızlı ve sessiz çalışırken diğerinin aşırı ısınması, donanım bileşenlerinin doğru seçilip seçilmediğiyle doğrudan ilgilidir. Cihazların çalışma mantığını anlamak hem zaman kazandırır hem de daha güvenli ve verimli tercihler yapılmasını sağlar.

1.1. İÇ DONANIM BİRİMLERİ

Bilgisayar kasasının veya dizüstü bilgisayarın gövdesinin içinde yer alan, veriyi işleyen, saklayan ve diğer bileşenlerle paylaşarak sistemin çalışmasını sağlayan fiziksel parçalara **iç donanım birimleri** denir. Bu bileşenler birbirleriyle sürekli iletişim hâlindedir ve bilgisayarın hızını, kararlılığını ve kullanım deneyimini doğrudan etkiler ancak performansı belirleyen yalnızca parçaların tek tek gücü değildir. Parçaların birbirleriyle uyumu ve doğru şekilde kurulması da en az parçaların gücü kadar önemlidir. Bu nedenle iç donanım birimleri incelenirken hem görevleri hem de bağlantı ve uyumluluk ilişkileri birlikte değerlendirilir.

Unutulmamalıdır ki siber güvenliğin ve veri bütünlüğünün ilk adımı, parçaları birbirleriyle uyumlu ve kararlı çalışan fiziksel bir sistem (donanım) kurmaktır.

1.1.1. Anakart

Anakart (mainboard), bilgisayar kasasının içinde yer alan ve sistemi oluşturan donanım parçalarını bir araya getiren temel devre kartıdır (Görsel 1.1). Merkezî işlem birimi [Central Processing Unit (CPU)], Rastgele Erişimli Bellek [Random Access Memory (RAM)], ekran kartı, depolama birimleri gibi iç donanımlar anakart üzerindeki yuva ve bağlantı noktalarına doğrudan bağlanır. Klavye, fare, monitör, yazıcı gibi dış donanımlar ise portlar üzerinden dolaylı olarak bağlanır.



Görsel 1.1: Anakart

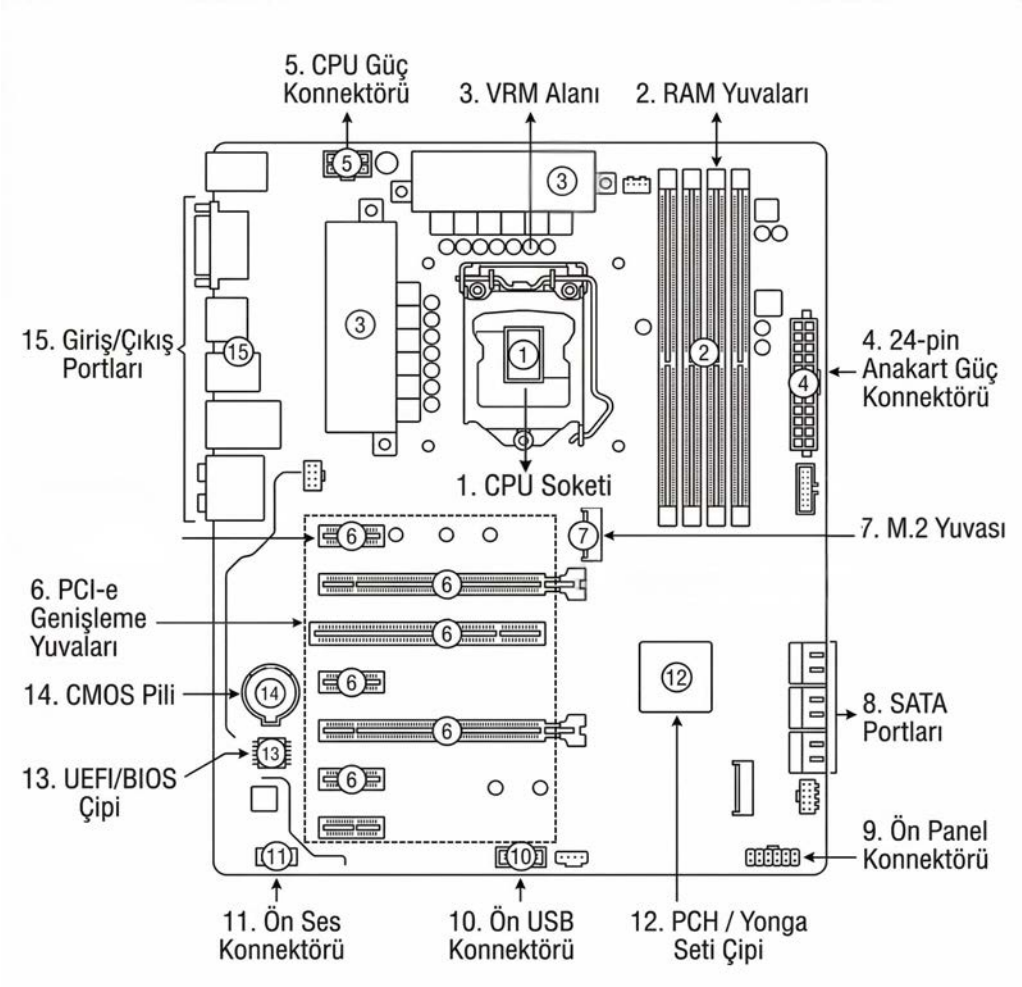
Anakartın temel görevlerinden biri iletişimi sağlamaktır. Üzerindeki iletken yollar (veri yolları) sayesinde donanım parçaları arasında veri alışverişi gerçekleşir. Bu nedenle sistemdeki veri trafiğinin merkezinde yer alır. Anakartın bir diğer görevi ise güç dağıtımıdır. Güç kaynağından aldığı elektriği bileşenlerin ihtiyaçlarına uygun şekilde güvenli biçimde iletir.

BİLGİ KUTUSU : Statik Elektrik ve Anakart Güvenliği

İnsan vücudunda biriken statik elektrik, anakart üzerindeki hassas elektronik bileşenlere zarar verebilir. Bu nedenle anakarta veya diğer donanım parçalarına dokunmadan önce statik elektriği boşaltmaya yönelik antistatik önlemler (antistatik bileklik kullanmak, topraklanmış bir yüzeye temas etmek, halı veya yünlü kumaş gibi statik elektrik biriktirebilen yüzeylerden uzak durmak vb.) alınmalıdır.

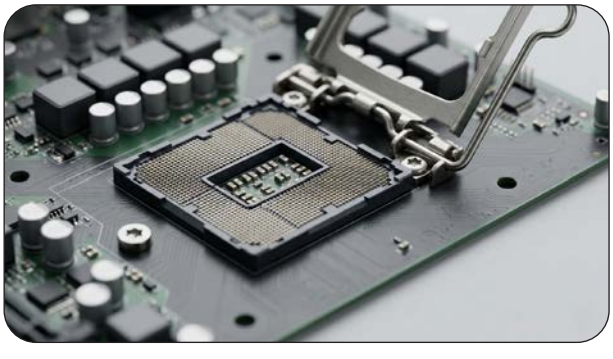
1.1.1.1. Anakart Bileşenleri

Anakartın **iletişim merkezi** olmasını sağlayan yapı, üzerinde bulunan bazı temel bileşenlerdir. Bu bileşenler; verinin hangi yollarla taşınacağını, hangi parçaların hangi yuvalara bağlanacağını ve dış donanımların hangi bağlantı noktalarından sisteme erişeceğini belirler. Anakart üzerindeki bileşenleri (Görsel 1.2) anlamak hem uyumluluk kontrolü yapmayı hem de montaj sırasında doğru bağlantıyı kurmayı kolaylaştırır.



Görsel 1.2: Anakart bileşenleri

1. **İşlemci Soketi (CPU Socket):** Bilgisayarın **beyni** olan işlemcinin takıldığı ve özel bir mandal mekanizmasıyla kilitlendiği fiziksel yuvadır (Görsel 1.3). İşlemci, anakartla ve diğer donanımlarla olan tüm iletişimini bu soket aracılığıyla kurar. Her işlemci her anakarta takılamaz. İşlemcinin markasına ve nesline göre soket yapısı değişiklik gösterir. Soket tipi, işlemcinin hangi anakartla kullanılabileceğini belirleyen temel uyumluluk bilgisidir.



Görsel 1.3: İşlemci soketi

BİLGİ KUTUSU : İşlemci Soket Tipleri (LGA-PGA)

İşlemciler anakarta takılırken bağlantı noktalarının (pinlerin) bulunduğu yere göre şu iki yaygın yapı görülür:

LGA (Land Grid Array): Pinler soketin içinde yer alır. İşlemcinin alt yüzeyinde düz temas noktaları bulunur.

PGA (Pin Grid Array): Pinler işlemcinin alt yüzeyindedir. Sokette bu pinlerin gireceği delikler bulunur.

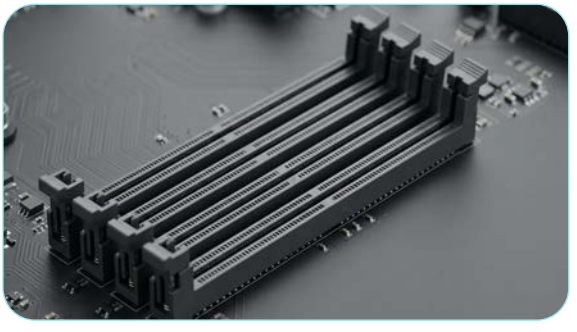
Montaj Uyarısı: İşlemci sokete yerleştirilirken hizalama işaretlerine dikkat edilmeli, parça zorlanmamalıdır. Pinlerin eğilmesi, sistemin açılmamasına veya işlemcinin bozulmasına neden olabilir.

ARAŞTIRMA

İki farklı işlemci soketi örneğini genel ağda araştırınız ve edindiğiniz bilgilere göre aşağıdaki tabloyu doldurunuz.

Soket Adı	Örnek İşlemci Marka-Modeli	Kaynak (Site adı)

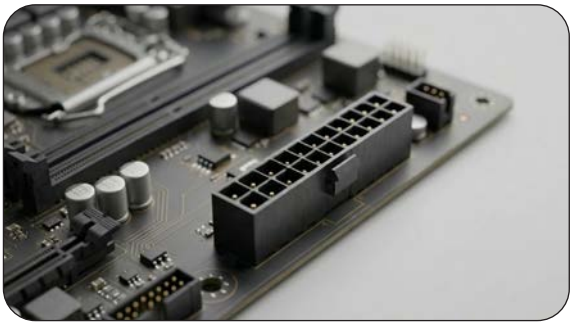
2. **RAM Yuvaları (RAM Slots):** RAM modüllerinin anakarta takıldığı bağlantı noktalarıdır (Görsel 1.4). RAM, bilgisayar çalışırken ihtiyaç duyulan bilgileri kısa süreli olarak tutar ve işlemcinin bu bilgilere hızlı erişmesine yardımcı olur. Bu nedenle RAM yuvaları genellikle işlemciye yakın bir yerde konumlanır. Anakartın modeline ve fiziksel boyutuna bağlı olarak yuva sayısı değişebilir.



Görsel 1.4: RAM yuvaları

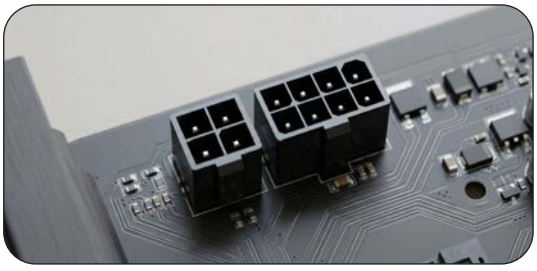
3. **VRM [Voltage Regulator Module (Voltaj Regülatör Modülü)]:** Güç kaynağından gelen enerjiyi, CPU'nun ihtiyaç duyduğu daha düşük ve kararlı voltaj seviyelerine dönüştüren ve düzenleyen devrelerdir. Örneğin 12 V seviyesini CPU'nun çalışacağı çok daha düşük değerlere indirir.

4. **24-Pin Anakart Güç Konnektörü:** Güç kaynağından gelen elektriği anakarta ileten ana bağlantıdır (Görsel 1.5). Anakart üzerindeki birçok bileşenin çalışması için gerekli enerji bu bağlantı üzerinden anakarta ulaşır ve sistem içinde dağıtılır.



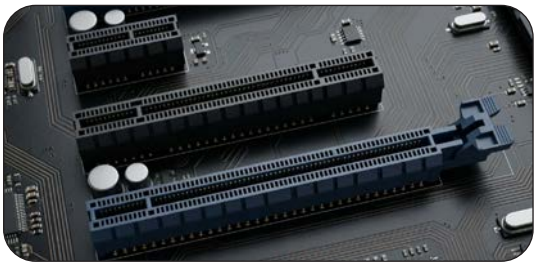
Görsel 1.5: 24-pin anakart güç konnektörü

5. **CPU Güç Konnektörü:** Anakart üzerindeki bu bağlantı noktası, güç kaynağından gelen elektrik enerjisini işlemciye ve işlemci çevresindeki güç düzenleme devrelerine (VRM) iletir (Görsel 1.6). Bu konnektör genellikle 4 pin veya 8 pin (4 + 4) olarak bulunur. 4 + 4 pin, iki ayrı 4 pinli konnektörün birleştirilebilir yapıda olduğu anlamına gelir.



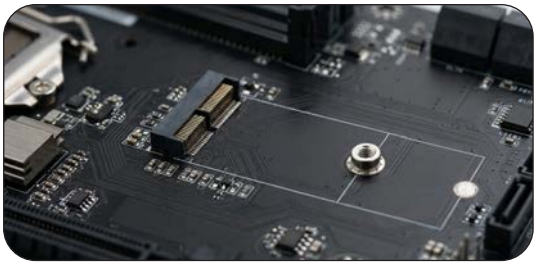
Görsel 1.6: CPU güç konnektörü

6. **PCIe (Peripheral Component Interconnect Express) Genişleme Yuvaları:** Ekran kartı, ağ kartı gibi ek donanımların anakarta takılarak bilgisayara bağlanmasını sağlayan yüksek hızlı genişleme yuvalarıdır (Görsel 1.7). PCIe'yi tanımlarken şerit sayısı ve nesil bilgileri önemlidir. **Şerit sayısı** (x1, x4, x8, x16), bağlantının kaç şerit kullandığını gösterir. Şerit sayısı arttıkça veri taşıma kapasitesi artar. **Nesil** (Gen3, Gen4, Gen5) ise sürümü ifade eder. Nesil yükseldikçe aktarım kapasitesi artar. PCIe nesilleri genellikle geriye dönük uyumludur yani yeni bir PCIe kartı daha eski bir yuvada çalışabilir ancak bağlantı daha düşük neslin hızında çalışır.



Görsel 1.7: PCIe genişleme yuvaları

7. **M.2 Yuvası:** Modern bilgisayarlarda SSD [Solid State Drive (Katı Hâl Sürücüsü)] gibi yüksek performanslı depolama aygıtları ve kablosuz iletişim kartları (Wi-Fi, Bluetooth) için tasarlanmış yeni nesil bir arabirimdir (Görsel 1.8). Geleneksel kutu şeklindeki 2,5 inç SSD'lerin aksine, doğrudan anakart üzerindeki özel yuvalara takılan oldukça küçük ve ince bir yapıya sahiptir.



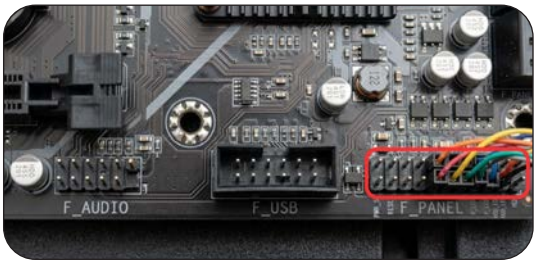
Görsel 1.8: M.2 yuvası

8. **SATA (Serial ATA) Portları:** HDD [Hard Disk Drive (Sabit Disk Sürücüsü)], SSD gibi depolama birimlerinin anakarta veri kablosu ile bağlandığı bağlantı noktalarıdır (Görsel 1.9). SATA III bağlantısı teorik olarak 6 Gb/sn (yaklaşık 600 MB/sn) veri aktarım hızına kadar destekler ancak pratikte hız, kullanılan diske ve sisteme göre değişebilir.



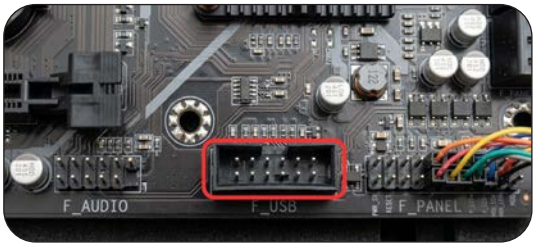
Görsel 1.9: SATA portları

9. **Ön Panel Konnektörü:** Kasanın güç (power) düğmesi, yeniden başlatma (reset) düğmesi, gösterge LED'leri gibi ön panel bağlantılarının anakarta bağlandığı pin grubudur (Görsel 1.10).



Görsel 1.10: Ön panel konnektörü

10. **Ön USB (Universal Serial Bus) Konnektörü:** Kasanın ön kısmındaki USB portlarının anakarta bağlandığı bağlantı noktasıdır (Görsel 1.11). Bu bağlantı sayesinde ön paneldeki USB girişleri çalışır ve cihazlar bilgisayara bağlanabilir.
11. **Ön Ses Konnektörü:** Kasanın ön kısmındaki kulaklık ve mikrofon girişlerinin anakarta bağlandığı bağlantı noktasıdır (Görsel 1.12). Bu bağlantı sayesinde ön panel ses giriş-çıkışları çalışır.
12. **Yonga Seti (Chipset):** Anakart üzerinde işlemci dışındaki birçok bağlantının nasıl çalışacağını düzenleyen ve sistemi düzenli hâle getiren temel bileşenlerden biridir. USB bağlantıları, depolama birimleri, ağ, ses gibi birimler çoğunlukla yonga seti üzerinden yönetilir. Bu nedenle yonga seti; anakartın kaç tane ve hangi tür bağlantıyı desteklediği, hangi hızlarda çalışabildiği, hangi genişleme seçeneklerini sunduğu gibi konularda belirleyici olabilir. Kısacası yonga seti, anakartın özellik haritasını okumada önemli bir anahtardır.



Görsel 1.11: Ön USB konnektörü



Görsel 1.12: Ön ses konnektörü

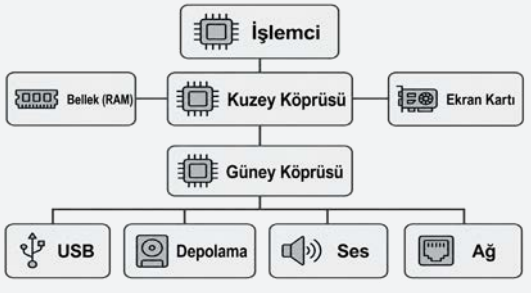
KONTROL NOKTASI

Anakart seçiminde bağlantı ve genişleme seçeneklerini anlamak için soket bilgisinin yanı sıra yonga seti bilgisi de belirleyici bir rol oynar.

BİLGİ KUTUSU : Geçmişten Günümüze Yonga Seti Yapısı

Eski Yapı

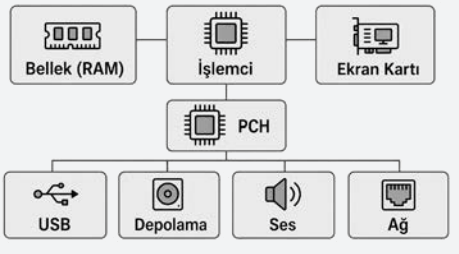
Geçmiş yıllardaki anakart tasarımlarında veri trafiği iki ayrı çip üzerinden yönetilirdi. İşlemciye yakın yüksek hızlı bileşenler (bellek ve ekran kartı) **Kuzey Köprüsü** tarafından yönetilirdi. USB portları, depolama birimleri, ses gibi çevre bağlantıları ise **Güney Köprüsü** tarafından yönetilirdi (Görsel 1.13).



Görsel 1.13: Kuzey-Güney Köprüsü

Güncel Yapı

Günümüz anakartlarında iki köprünün görevleri tek bir çipte birleştirilmiştir. Bellek ve ekran kartıyla yüksek hızlı iletişim doğrudan işlemciye (CPU) aktarılmıştır. USB, depolama, ses gibi çevre bağlantılarının yönetimi ise anakart üzerindeki tek bir çipte toplanır. Bu bütünleşik yapı, **PCH (Platform Controller Hub)** veya genel ifadeyle **yonga seti** olarak adlandırılır (Görsel 1.14).



Görsel 1.14: PCH

13. **UEFI/BIOS [Unified Extensible Firmware Interface (Birleşik Genişletilebilir Üretici Yazılımı Arayüzü)]/[Basic Input/Output System (Temel Giriş-Çıkış Sistemi)] Çipi:** Anakart üzerinde bulunan ve bilgisayarın açılış sürecini yöneten temel sistem yazılımını saklayan kalıcı bir bellek çipidir. Bilgisayar açıldığında donanımların ilk kontrollerini yapar, bileşenlerin tanınmasını sağlar ve işletim sisteminin başlatılmasına yardımcı olur. Güncel sistemlerde UEFI, klasik BIOS yapısının yerini almıştır. Daha hızlı açılış, grafik arayüz, güvenli önyükleme (Secure Boot) gibi özelliklerle güvenliği destekler. Modern UEFI sistemlerinde güvenliği daha da artırmak amacıyla **TPM [Trusted Platform Module (Güvenilir Platform Modülü)] 2.0** çipi de kullanılır. TPM 2.0, şifreleme anahtarlarını ve kimlik doğrulama verilerini güvenli biçimde saklar, disk şifreleme ve sistem bütünlüğü doğrulama gibi işlemleri donanım düzeyinde destekler.

14. **CMOS [Complementary Metal-Oxide-Semiconductor (Tamamlayıcı Metal-Oksit-Yarı İletken)] Pili:** Bilgisayarın fişi çekilse bile tarih-saat bilgisi ile bazı temel BIOS/UEFI ayarlarının korunmasını sağlayan küçük pildir (Görsel 1.15). Pil zayıfladığında saat / tarih sıfırlanabilir ve bazı ayarlar varsayılan değerlere dönebilir.



Görsel 1.15: CMOS pili

15. **Giriş-Çıkış Portları (Input/Output Ports):** Klavye, fare, monitör, yazıcı, ağ kablosu gibi dış donanımların bilgisayara bağlandığı bağlantı noktalarıdır. Bu portlar, bilgisayar ile çevre birimleri arasında veri alışverişini sağlar ve genellikle kasanın arka panelinde yer alır (Görsel 1.16). Anakartın marka, model ve form faktörüne göre bu portların türleri ve sayısı değişiklik gösterebilir.



Görsel 1.16: Giriş-çıkış portları

PS/2: Klavye ve fare için kullanılan eski bir bağlantıdır. Eski sistemlerle uyumluluk için günümüzde bazı anakartlarda bulunur. Klavye için mor, fare için yeşil renktedir veya yarı yarıya renklendirilmiştir.

VGA [Video Graphics Array (Video Grafik Dizisi)]: Monitöre analog görüntü aktarır. Yeni nesil anakartlarda genellikle yer almaz. Bugün yerini HDMI veya DisplayPort almıştır.

HDMI [High-Definition Multimedia Interface (Yüksek Çözünürlüklü Çoklu Ortam Arayüzü)]: Bilgisayardaki görüntü ve sesi tek bir kablo üzerinden monitör, televizyon veya projeksiyon cihazına ileten dijital bağlantı türüdür. Günümüzde ekran bağlantısı için en sık kullanılan seçeneklerden biridir.

DisplayPort (DP): Bilgisayardan monitöre dijital görüntü aktarımı yapan bir bağlantı türüdür ve çoğu sistemde ses aktarımını da destekler. Yüksek çözünürlük ve yüksek yenileme hızı gerektiren görüntüleme ihtiyaçlarında tercih edilebilir.

USB [Universal Serial Bus (Evrensel Seri Veri Yolu)]: Klavye, fare, bellek, yazıcı gibi birçok cihazın bilgisayara bağlanmasını sağlayan yaygın bağlantı noktasıdır. Anakartın marka ve modeline göre USB portlarının sayısı, desteklediği hız ve uç tipi (Type-A, Type-C gibi) değişebilir.

Thunderbolt: Uyumlu cihazlar arasında çok hızlı veri aktarımı yapılmasını sağlayan gelişmiş bir bağlantı türüdür. Bazı sistemlerde aynı bağlantı üzerinden görüntü aktarımı ve cihaz şarjı da gerçekleştirilebilir. Görünüş olarak USB Type-C'ye benzeyebilir ancak her Type-C girişinde Thunderbolt desteği bulunmayabilir.

LAN (RJ-45): Bilgisayarın kablolu ağ ve internete bağlanmasını sağlar. Bugün birçok anakart, yüksek hızlı kablolu ağ desteği sunar. Genellikle kablosuz bağlantıya göre daha hızlı ve kararlı ağ iletişimi sağlar.

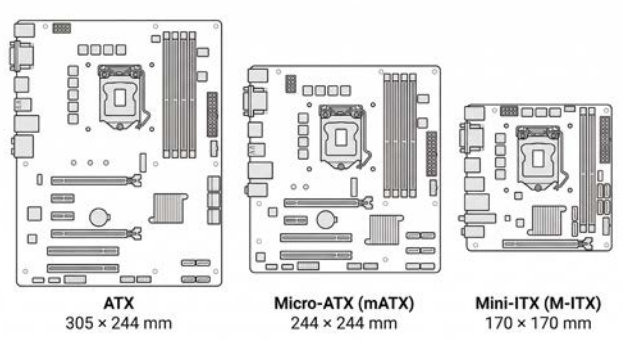
Wi-Fi: Bilgisayarın kablosuz ağa bağlanabilmesi için antenlerin takıldığı bağlantı noktasıdır.

Ses Giriş-Çıkış (Audio Jack) Portları: Kulaklık, hoparlör, mikrofon gibi ses aygıtlarının bilgisayara bağlandığı bağlantı noktalarıdır. Anakartın modeline göre ses portlarının sayısı ve işlevleri değişebilir.

Optik Ses (Optical Audio): Diğer adı **S/PDIF** olan bu bağlantı, dijital sesin cihazlar arasında optik kablo ile iletilmesini sağlar.

1.1.1.2. Anakart Biçim Standartları (Form Faktörleri)

Bir anakartın fiziksel boyutunu, kasaya montaj düzenini ve bağlantı noktalarının genel yerleşimini belirleyen standartlara **form faktörü** denir. Form faktörü, anakartın hangi kasaya sığacağını ve sistemin yerleşimini doğrudan etkiler. Genel olarak anakart boyutu büyüdükçe RAM slot, genişleme yuvası ve port sayısı artabilir. Daha küçük anakartlarda ise yer kısıtı nedeniyle bu sayılar sınırlı olabilir ancak kesin özellikler anakartın marka ve modeline göre değişir. Görsel 1.17'de farklı form faktörlerine sahip anakart örnekleri gösterilmektedir.



Görsel 1.17: Anakart form faktörleri

ATX (Advanced Technology eXtended): Masaüstü bilgisayarlarda en yaygın biçimdir. Daha geniş yerleşim alanı sayesinde çoğu modelde daha fazla bağlantı (yuva) seçeneği sunabilir. Standart ölçüsü yaklaşık 305 × 244 mm'dir.

Micro-ATX (mATX): ATX'e göre daha kompakt bir seçenektir. Birçok durumda ATX kasalarla uyumlu olabildiği için tercih edilir. Standart ölçüsü yaklaşık 244 × 244 mm'dir.

Mini-ITX (Mini-Information Technology eXtended): Küçük kasalar için tasarlanmış kompakt form faktörüdür. Yer tasarrufu sağlar. Bu nedenle bağlantı (yuva) sayısı daha sınırlı olabilir. Standart ölçüsü yaklaşık 170 × 170 mm'dir.

1.1.1.3. Uyumlulukta Anakartın Rolü

Bir bilgisayarın sorunsuz ve yüksek performanslı çalışması için yalnızca güçlü parçalar seçmek yeterli değildir. Sistemin kararlı olabilmesi için seçilen tüm bileşenlerin anakart ile donanımsal olarak uyumlu olması gerekir. Anakartın işlemci soketi (hangi marka-nesil işlemcinin takılabileceği), bellek yuvaları (hangi tür ve kapasitede RAM desteklediği) ve form faktörü (kartın fiziksel boyutu) bilgisayarın temel sınırlarını ve yükseltme seçeneklerini belirler. Bu yüzden parça seçerken **güç** kadar **uyum** da önemlidir.

KONTROL NOKTASI

Bir bilgisayar toplarken veya parça seçerken sistemin sorunsuz çalışması için önce en temel uyumluluk noktalarını kontrol etmek gerekir. Şu üç kontrol, kurulumun doğru ilerlemesi için ilk sırada yer alır:

1. **İşlemci Uyumu:** Anakartın işlemci soketi ve desteklediği işlemci ailesi uyumlu mu?
2. **Bellek Uyumu:** Desteklenen bellek türü ve kapasite sınırı uygun mu (DDR türü, slot sayısı)?
3. **Kasa Uyumu:** Anakartın form faktörü kasaya uyuyor mu (ATX, mATX ve Mini-ITX)?

1. ETKİNLİK

Etkinlik Adı	Anakart Avı
Süre	40 dakika
Amaç	Anakart seçiminde uyumluluk önceliklerini kullanarak doğru bilgiye ulaşmak ve gerekçeli seçim yapmak
Yönerge	Sınıf mevcuduna göre 3-4 kişilik gruplar oluşturunuz. E-ticaret veya üretici sitesinden bir anakart modeli seçiniz. Aşağıdaki formu seçtiğiniz anakarta göre doldurunuz. Grupça seçtiğiniz anakartı sınıfta tanıtınız.

Anakart Kimliği ve Özellik Formu	
Seçilen Anakart (Marka-Model):	
Kaynak (Site Adı):	
A) Temel Kimlik Bilgileri	
İşlemci Soketi:	
Yonga Seti:	
Anakart form faktörü:	
B) Bellek (RAM)	
RAM Tipi:	
RAM Slotu Sayısı:	
Diğer RAM Bilgileri:	
C) Depolama	
M.2 Slotu Sayısı:	
SATA Portu Sayısı:	
Ç) Genişleme Yuvaları	
PCIe x1 Slotu Sayısı:	
PCIe x4 Slotu Sayısı:	
PCIe x8 Slotu Sayısı:	
PCIe x16 Slotu Sayısı:	
PCIe Hızı ve Nesli (Varsa):	

D) Bağlantı ve Port Özeti	
USB (Type-A):	☐ Var ☐ Yok | Sayısı: _____
USB (Type-C):	☐ Var ☐ Yok | Sayısı: _____
Thunderbolt:	☐ Var ☐ Yok
HDMI:	☐ Var ☐ Yok
DisplayPort:	☐ Var ☐ Yok
LAN (RJ-45):	☐ Var ☐ Yok | Hız bilgisi (varsa): _____
Wi-Fi:	☐ Var ☐ Yok
Ses Giriş-Çıkış:	☐ Var ☐ Yok
PS/2:	☐ Var ☐ Yok

Seçim Gerekçesi	
1.	
2.	
3.	

Değerlendirme

Çalışmanız öğretmeniniz tarafından analitik dereceli puanlama anahtarına göre değerlendirilecektir. Çalışmanızı yaparken buradaki ölçütleri dikkate alınız. Analitik dereceli puanlama anahtarı formuna ulaşmak için karekodu okutunuz. Dijital yayınlarda karekodun üstüne tıklayarak içeriğe ulaşabilirsiniz.

Çalışmanızı tamamladıktan sonra grup değerlendirme formunu doldurarak grup üyelerinin çalışmaya katkı düzeylerini değerlendiriniz. Grup değerlendirme formuna ulaşmak için karekodu okutunuz. Dijital yayınlarda karekodun üstüne tıklayarak içeriğe ulaşabilirsiniz.

1.1.2. İşlemci

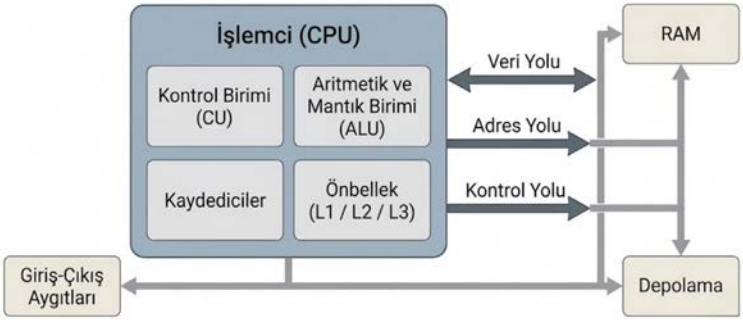
İşlemci veya **Merkezî İşlem Birimi [Central Processing Unit (CPU)]**, bilgisayarda verilen komutları işleyen ve sistemin çalışmasını yöneten temel bileşendir (Görsel 1.18). İşlemci; hesaplamaları yapar, işlemlerin sırasını düzenler ve ortaya çıkan sonuçların bellek, depolama ve giriş-çıkış birimleriyle paylaşılmasını sağlar. Bir bilgisayarın hızı, verimliliği ve performansı büyük ölçüde işlemcinin yapısına ve özelliklerine bağlıdır.



Görsel 1.18: İşlemci ve işlemci soketi

1.1.2.1. İşlemcinin Yapısı

Bir işlemci, silisyum adı verilen yarı iletken bir malzeme üzerine inşa edilir. Bu silikon tabanın üzerinde **transistör** adı verilen milyarlarca küçük elektronik anahtar bulunur. Her bir transistör, tıpkı bir elektrik düğmesi gibi açılıp kapanarak akımın geçip geçmediğini kontrol eder. Açık konum bir (**1**), kapalı konum sıfır (**0**) olarak kabul edilir. İşlemci, bu milyarlarca transistörün açılıp kapanma durumlarını düzenleyerek bilgisayardaki tüm hesaplamaları, karşılaştırmaları ve veri akışını gerçekleştirir. Bir işlemci, görevlerine göre dört bölümden oluşur (Görsel 1.19).



Görsel 1.19: İşlemci yapısı ve iletişim yolları

1. **Kontrol Birimi [Control Unit (CU)]:** İşlemcinin yönetim merkezidir. Bellekten gelen komutları alır, bu komutların ne anlama geldiğini çözer ve sistemdeki diğer donanım birimlerine gerekli işlem sinyallerini gönderir. Bilgisayar içindeki veri trafiğini ve işlemlerin zamanlamasını organize eder.
2. **Aritmetik ve Mantık Birimi [Arithmetic Logic Unit (ALU)]:** İşlemcinin hesaplama merkezidir. Toplama, çıkarma, çarpma, bölme gibi matematiksel işlemlerin yanı sıra veriler arasındaki büyüklük, küçüklük, eşitlik gibi mantıksal karşılaştırma işlemlerini de gerçekleştirir.
3. **Kaydediciler (Registers):** İşlemcinin çekirdeğinde yer alan, veri kapasitesi çok küçük ancak erişim hızı en yüksek olan geçici veri saklama alanlarıdır. İşlemci, o an üzerinde doğrudan işlem yaptığı verileri, adresleri ve komutları bu birimde tutar.
4. **Önbellek (Cache):** İşlemci ile RAM arasında köprü görevi gören yüksek hızlı bir bellek türüdür. İşlemcinin veri işleme hızı, RAM'in veri gönderme hızından çok daha yüksektir. Bu hız farkından kaynaklanan beklemeyi önlemek için işlemcinin en sık kullandığı veriler ve komutlar önbellekte hazır bekletilir. Böylece sistemin genel performansı artar.

KONTROL NOKTASI

İşlemci seçerken anakartın soket tipiyle uyumlu olup olmadığı mutlaka kontrol edilmelidir. Uyumsuz bir işlemci, fiziksel olarak sokete takılsa bile sistem çalışmaz. Soket uyumluluğu; işlemci nesli, üreticisi ve anakart modeline göre değişir.

1.1.2.2. İşlemci İletişim Yolları

İşlemci, tek başına çalışan bir parça değildir. İşlemcinin; RAM, depolama birimleri ve giriş-çıkış aygıtlarıyla sürekli veri alışverişi yapması gerekir. Bu iletişim, anakart üzerinde bulunan ve farklı görevler için özelleşmiş iletim hatları (bus) aracılığıyla gerçekleşir. Bu hatlar, işlemci ile diğer donanımlar arasında bilginin taşınmasını, hedefin adreslenmesini ve işlemin yönetilmesini sağlar. İletişim yolları taşıdıkları bilgi türüne göre üç ana grupta incelenir (Görsel 1.19).

1. **Veri Yolu (Data Bus):** İşlemci ile bellek veya diğer birimler arasında asıl verilerin (sayılar, harfler ve komutlar) taşındığı hattır. Çift yönlü çalışır. Başka bir ifadeyle veriler işlemciden dışarı gönderilebildiği gibi dışarıdan işlemciye de gelebilir. Veri yolunun genişliği (örneğin 32 bit veya 64 bit), işlemcinin tek seferde taşıyabileceği veri miktarını belirler.
2. **Adres Yolu (Address Bus):** İşlemcinin hangi bellek hücresine veya hangi donanım birimine erişmek istediğini adres bilgisi olarak ilettiği yoldur. Tek yönlüdür. Başka bir ifadeyle adres bilgisi, yalnızca işlemciden çıkarak belleğe veya diğer birimlere gider. Adres yolunun genişliği, işlemcinin doğrudan adresleyebileceği maksimum RAM kapasitesini belirler.
3. **Kontrol Yolu (Control Bus):** İşlemcinin diğer birimlere ne yapmaları gerektiğini bildiren sinyallerin taşındığı hattır. Örneğin okuma (read), yazma (write), saat (clock) gibi sinyaller bu yol üzerinden iletilir. Kontrol yolu sayesinde sistemdeki veri akışı düzenli ve senkronize bir şekilde yürütülür.

BİLGİ KUTUSU : Veri Yolu Genişliği ve İşlemci Performansı

İlk kişisel bilgisayarlarda veri yolu genişliği 8 bit ile sınırlıydı. Teknoloji geliştikçe bu genişlik 16 bit, 32 bit ve bugün yaygın olarak kullanılan 64 bite çıkmıştır. Veri yolu genişliği iki katına çıktığında işlemcinin tek seferde taşıyabileceği veri miktarı da iki katına çıkar. Bu durum, uygun donanım ve yazılım koşullarında işlemcinin verileri daha verimli işlemesini sağlar.

1.1.2.3. İşlemci Çalışma Mekanizması

İşlemci (CPU), komutları belli bir sırayla işleyerek programların çalışmasını sağlar. Bu işleyiş, komut döngüsü (instruction cycle) olarak adlandırılan ve bilgisayar açık olduğu sürece sürekli tekrarlanan dört temel adımdan oluşur. Bu adımlar sırasında işlemci, anakart üzerindeki veri yolu, adres yolu ve kontrol yolu aracılığıyla bellek ve diğer donanımlarla iletişim kurar.

1. **Getir (Fetch): İ**şlemci, sıradaki komutu bellekten alır. **Program sayacı [Program Counter (PC)]**, hangi komutun sırada olduğunu takip eder. Komut adresi, adres yolu üzerinden belleğe iletilir. Kontrol yoluyla **okuma** sinyali gönderilir ve komut, veri yolu aracılığıyla işlemciye taşınarak **komut kaydedicisine [Instruction Register (IR)]** aktarılır. Program sayacı bir sonraki komuta hazırlanır.
2. **Çözümle (Decode):** Getirilen komut makine diliyle yazılmıştır. Kontrol birimi bu komutu inceleyerek ne yapılacağını belirler (hesaplama, veri taşıma, karşılaştırma vb.). Hangi birimlerin devreye gireceği planlanır. Bu aşama büyük ölçüde işlemci içinde gerçekleşir.
3. **Çalıştır (Execute):** Komut uygulanır. Matematiksel veya mantıksal bir işlemse ALU devreye girer, iletişim yolları kullanılmaz. Bellekten veri okunacaksa adres yoluna adres, kontrol yoluna **okuma** sinyali gönderilir ve veri, veri yolu ile gelir. Belleğe veri yazılacaksa adres ve veri, ilgili yollara yerleştirilip **yazma** sinyali iletilir.
4. **Sakla / Geri-Yaz (Store/Write-Back):** İşlem sonucu kaydediciye veya belleğe yazılır. Kaydediciye yazılıyorsa iletişim yolları kullanılmaz. Belleğe yazılıyorsa adres ve veri, ilgili yollara yerleştirilip kontrol yoluyla **yazma** sinyali gönderilir.

SIRA SİZDE

Aşağıdaki yapılandırılmış gridde numaralandırılmış kutucuklarda işlemcinin veri iletim süreçleri ile ilgili kavramlar verilmiştir. 5 + 3 işleminin gerçekleşmesini hayal ederek, aşağıdaki soruların cevaplarını kutucuk numaralarını kullanarak ilgili boşluklara yazınız (Bir kutucuğu birden fazla cevap için kullanabilirsiniz).

1. Kontrol Birimi (CU)	**2.** Aritmetik ve Mantık Birimi (ALU)	**3.** Kaydediciler
4. Komut Kaydedicisi (IR)	**5.** Veri Yolu	**6.** Adres Yolu
7. Kontrol Yolu	**8.** Okuma Sinyali	**9.** Yazma Sinyali
10. RAM (Bellek)	**11.** Getir (Fetch)	**12.** Çözümle (Decode)
13. Çalıştır (Execute)	**14.** Sakla / Geri-Yaz (Store/Write-Back)	**15.** Program Sayacı (PC)

	Sorular	Cevap
a)	Bellekten veri okunurken kullanılan yol ve sinyal hangisidir?	
b)	5 sayısının bellekten işlemciye getirilmesinde görev alan iletişim yolları hangileridir?	
c)	Komutun bellekten alınması sırasında görev alan birimler hangileridir?	
ç)	Toplama işleminin yapılmasında görev alan birim ve aşama hangisidir?	
d)	Komutun çözümleme aşamasında görev alan birim ve aşama hangisidir?	
e)	Bellekten getirilen komutun tutulduğu birimler hangileridir?	
f)	5 + 3 işleminin işlemci içinde gerçekleştiği komut döngüsü aşamaları hangileridir?	
g)	İşlemci, 5 + 3 komutunu çözümleyip toplama yapılacağını anladığında komut döngüsünün hangi aşaması tamamlanmış olur?	
ğ)	İşlemci ile bellek arasındaki veri alışverişinde görev alan iletişim yolları hangileridir?	
h)	Toplama işlemi yapıldıktan sonra sonuç (8), belleğe aktarılırken işlemci hangi sinyali kullanır?	
ı)	Okuma veya yazma gibi işlemin türünü belirten yol hangisidir?	

1.1.2.4. İşlemci Performansını Etkileyen Faktörler

Komut döngüsünün daha hızlı ve verimli yürütülmesi, işlemcinin genel performansını etkiler. İşlemci performansını belirleyen bazı temel faktörler şunlardır:

Saat Hızı (Clock Speed): İşlemcinin çalışma ritmini ve çalışma frekansını belirleyen saat darbesi hızıdır. Günümüz modern işlemcilerinde GHz (Gigahertz) ile ifade edilir. Saat hızı yükseldikçe işlemci, kısa süre içinde daha fazla adım gerçekleştirebilir ancak saat hızı, performansı belirleyen tek ölçüt değildir.

Çekirdek (Core) Sayısı: Modern işlemcilerde birden fazla çekirdek bulunabilir. Birden fazla çekirdek, aynı anda farklı işleri paylaşarak yapmayı kolaylaştırır. Böylece çoklu görevlerde ve aynı anda çalışan uygulamalarda performans artabilir.

Önbellek (Cache) Boyutu: Önbellek, işlemcinin sık kullandığı veri ve komutlara daha hızlı erişmesini sağlar. Önbellek boyutu arttıkça RAM'e gitme ihtiyacı azalabilir ve sistem daha akıcı çalışabilir.

Boru Hattı (Pipelining): İşlemcinin getir, çözümle, çalıştır, sakla-geri yaz adımlarını sıraya dizmek yerine örtüşecek şekilde yürütmesine denir. Böylece işlemci, bir komut üzerinde çalışırken diğer komutun bir sonraki adımına da hazırlanabilir.

BİLGİ KUTUSU : **Hız Aşırtma (Overclocking)**

İşlemcinin frekansının (saat hızının), üretici tarafından belirlenen standart değerlerin üzerine çıkarılması işlemidir. Performansı artırsa da aşırı ısınma ve enerji tüketimine neden olduğu için soğutma ihtiyacını artırır.

1.1.2.5. İşlemci Mimarisi

İşlemciler, komutları işleme biçimlerine göre RISC [Reduced Instruction Set Computer (Azaltılmış Komut Setli Bilgisayar)] ve CISC [Complex Instruction Set Computer (Karmaşık Komut Setli Bilgisayar)] isminde iki temel mimaride tasarlanır. Bu mimariler, komut setlerinin karmaşıklığı, işlem hızı ve kullanım alanları açısından farklılık gösterir.

RISC Mimarisi: RISC mimarisinde komut sayısı azdır. Komutlar basit yapılı ve sabit uzunluktadır. Bu sayede çoğu komut, tek bir saat darbesinde yürütülebilir. İşlemci içinde çok sayıda genel amaçlı kaydedici bulunur. Bellek erişimi yalnızca **yükle (load)** ve **sakla (store)** komutlarıyla yapılır. Diğer komutlar, kaydediciler üzerinde çalışır. Donanım tasarımı daha basit ve az transistörlü olduğu için enerji tüketimi düşüktür. Bu özellikleri sayesinde RISC işlemciler; akıllı telefonlar, tabletler, giyilebilir cihazlar, gömülü sistemler, IoT cihazları, yeni nesil bilgisayarlar (M serisi) ve enerji verimli sunucularda yaygın olarak kullanılır. RISC mimarisine örnek olarak ARM, RISC-V, M serisi (M1, M2, M3) ve MIPS gösterilebilir.

CISC Mimarisi: CISC mimarisinde komut sayısı fazladır, komutlar karmaşık yapılı ve değişken uzunluktadır. Bir komut birden fazla saat darbesinde yürütülebilir ve tek bir komut, bellekten veri alıp işlem yapıp sonucu kaydedebilir. Kaydedici sayısı RISC'e göre daha azdır. Birçok komut doğrudan bellek üzerinde işlem yapabilir. Donanım tasarımı daha karmaşık ve transistör sayısı fazla olduğu için enerji tüketimi genellikle daha yüksektir. Bu özellikleriyle CISC işlemciler; masaüstü ve dizüstü bilgisayarlar, oyun konsolları, yüksek performans gerektiren sunucular ve bilimsel hesaplamalarda tercih edilir. CISC mimarisinin en bilinen örneği **x86** mimarisidir.

BİLGİ KUTUSU : Bugünün RISC ve CISC Mimarisi

Bugün RISC ve CISC arasındaki keskin ayrım azalmıştır. Modern CISC işlemciler, iç yapılarında RISC benzeri çekirdekler kullanır. Karmaşık komutlar, işlemci içinde daha basit işlemlere dönüştürülerek çalıştırılır. Açık kaynaklı RISC mimarisi RISC-V; sunucu, yapay zekâ donanımları gibi alanlarda hızla yaygınlaşmaktadır.

SIRA SİZDE

Ortadaki özellik sütununu inceleyiniz. Her özellik için RISC ve CISC mimarilerinin nasıl farklılaştığını ilgili sütunlara yazınız.

RISC	Özellik	CISC
	Komut Uzunluğu	
	Çalışma Süresi (Saat Darbesi)	
	Bellek Erişimi	
	Donanım Tasarımı	
	Transistör Sayısı	
	Enerji Tüketimi	
	Kaydedici Sayısı	
	Yaygın Örnekler	
	Temel Kullanım Alanları	

1.1.2.6. İşlemci Soğutma Çeşitleri

İşlemci çalışırken harcadığı enerjinin bir kısmı ısıya dönüşür. Sıcaklığın artması, işlemcinin performansını düşürebilir ve sistemin kararsız çalışmasına yol açabilir. Bu nedenle işlemcinin güvenli sıcaklık aralığında çalışmasını sağlamak için soğutma sistemleri kullanılır.

Hava Soğutma: En yaygın yöntemdir. İşlemci üzerine yerleştirilen metal soğutucu blok, ısıyı alır. Fan ise ısınan havayı uzaklaştırarak soğutmayı hızlandırır (Görsel 1.20). Kurulumu genellikle kolay, maliyeti düşüktür.



Görsel 1.20: İşlemcide hava soğutma sistemi

Sıvı Soğutma: Isının bir sıvı yardımıyla taşındığı sistemdir. İşlemci üzerindeki blok, ısıyı sıvıya aktarır. Sıvı, radyatöre taşınan ısıyı fanlar yardımıyla havaya verir (Görsel 1.21). Daha etkili soğutma sağlayabilir ancak kurulumu hava soğutmaya göre daha karmaşıktır ve maliyeti daha yüksektir.

Pasif Soğutma: Fan, pompa gibi hareketli parça kullanmaz. Isı, soğutucu üzerindeki kanatçıklar ve doğal hava akışıyla dağıtılır (Görsel 1.22). Sessizdir ancak soğutma kapasitesi sınırlıdır ve genellikle düşük güç tüketimli sistemlerde kullanılır.

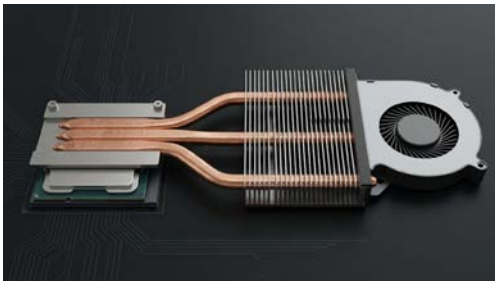
Isıl Borulu (Heat Pipe) Soğutma: İçinde özel bir akışkan bulunan ısıl borular, ısıyı işlemciden alıp soğutucunun farklı bölgelerine hızlı şekilde taşır (Görsel 1.23). Özellikle alanın sınırlı olduğu dizüstü bilgisayarlarda yaygındır.



Görsel 1.21: İşlemcide sıvı soğutma sistemi



Görsel 1.22: İşlemcide pasif soğutma sistemi



Görsel 1.23: İşlemcide ısıl borulu soğutma sistemi

BİLGİ KUTUSU : Termal Macun

İşlemci ile soğutucu blok arasında mikroskobik boşluklar bulunur. Bu boşluklardaki hava ısıyı iyi iletmez. Termal macun, boşlukları doldurarak ısının işlemciden soğutucuya daha verimli aktarılmasını sağlar. Zamanla performansı azalabileceği için gerektiğinde macun yenilenmelidir.

SİBER GÜVENLİK PENCERESİ

İşlemci yalnızca bir performans bileşeni değildir. Siber güvenlik açısından kritik bir saldırı yüzeyidir. İşlemcinin komut döngüsündeki ve önbellek mimarisindeki bazı tasarım özellikleri, kötü niyetli yazılımlar tarafından istismar edilebilir.

Önbellek Temelli Saldırılar: İşlemcinin önbelleği, sık kullanılan verileri geçici olarak saklar. Saldırganlar, önbelleğe erişim sürelerini ölçerek başka bir programın hangi verilerle çalıştığını tahmin edebilir. Bu yöntemle şifreler, kriptografik anahtarlar gibi hassas veriler dolaylı olarak elde edilebilir.

Spekülatif Yürütme Açıkları: Modern işlemciler, komut döngüsünü hızlandırmak için sonraki komutları tahmin ederek önceden çalıştırır. Bu mekanizma kötüye kullanıldığında işlemci, erişilmemesi gereken bellek bölgelerinden veri okuyabilir hâle gelebilir.

Hız Aşırtma ve Sistem Kararsızlığı: İşlemcinin sınırları dışında çalıştırılması, hesaplama hatalarına yol açabilir. Bu hatalar bazı durumlarda güvenlik denetimlerinin atlatılmasında kullanılabilir.

Güvenli bir sistem kurulumu, yalnızca yazılım güncellemeleriyle değil donanımın güvenli yapılandırılmasıyla da başlar. İşlemci tasarımındaki güvenlik açıkları, işletim sistemi veya uygulama yazılımından bağımsız olarak tüm sistemi etkileyebilir.

ARAŞTIRMA

İşlemci tasarımından kaynaklanan güvenlik açıkları, 2018 yılında tüm dünyada manşetlere taşınmış ve milyonlarca sistemi etkileyen iki kritik güvenlik açığının kamuoyuyla paylaşılmasına neden olmuştur.

Aşağıdaki soruları araştırınız ve bulduğunuz bilgileri tabloya yazınız.

- 2018 yılında açıklanan işlemci kaynaklı iki büyük güvenlik açığını araştırınız. Bu açıkların hangi işlemci mekanizmasını hedef aldığını belirleyiniz.
- Bu açıkları gidermek için hangi önlemler alınmıştır? Donanım güncellemesi mi yoksa yazılım yaması mı daha etkili olmuştur? Neden?
- Bu tür açıkların önüne geçmek için işlemci üreticileri, tasarım aşamasında hangi güvenlik önlemlerini alabilir?

Güvenlik Açığının Adı	Hedef Aldığı İşlemci Mekanizması
Kaynak (Site Adı ve Erişim Tarihi-Saati):	

1.1.3. Bellekler

Bellek; veri ve komutların saklandığı, gerektiğinde işleneceği birime iletildiği elektronik depolama birimidir. Bilgisayar, akıllı telefon, tablet, yazıcı, yönlendirici, gömülü sistemler gibi pek çok dijital cihaz; çalışabilmek için farklı türlerde bellek birimlerine ihtiyaç duyar. Bellekler, verinin kalıcı olarak saklanıp saklanmadığına göre **ROM [Read Only Memory (Salt Okunur Bellek)]** ve **RAM [Random Access Memory (Rastgele Erişimli Bellek)]** olarak iki ana gruba ayrılır.

1.1.3.1. ROM Bellekler

ROM, güç kesildiğinde içindeki verinin silinmediği kalıcı bellek türüdür. Dijital cihazların her açılışta ihtiyaç duyduğu temel başlangıç talimatları, ROM türündeki belleklerde saklanır. Klasik ROM, üretim aşamasında bir kez yazılır ve sonradan değiştirilemez. Teknoloji geliştikçe bu katı yapı, farklı ihtiyaçlara yanıt verecek biçimde evrilmiş ve ROM ailesinde birbirinden farklı türler ortaya çıkmıştır.

PROM [Programmable ROM (Programlanabilir Salt Okunur Bellek)]: Fabrikadan boş çıkan ve özel bir cihaz aracılığıyla yalnızca bir kez programlanabilen bellek türüdür. Yazma işlemi tamamlandıktan sonra içerik bir daha değiştirilemez.

EPROM [Erasable Programmable ROM (Silinebilir Programlanabilir Salt Okunur Bellek)]: Ultraviyole (UV) ışığına maruz bırakılarak içeriği silinen ve ardından yeniden programlanabilen bellek türüdür. Silme işlemi için çipin devreden çıkarılması ve özel bir UV kaynağına tutulması gerekir.

EEPROM [Electrically Erasable Programmable ROM (Elektrikle Silinebilir Programlanabilir Salt Okunur Bellek)]: Elektrik sinyaliyle silinip yeniden yazılabilen bellek türüdür. Silme işlemi devre üzerindeyken ve bayt bayt yapılabilir. Bu özelliği EPROM'a göre çok daha esnek bir kullanım sunar.

Flaş (Flash) Bellek: EEPROM teknolojisinin geliştirilmiş ve yüksek kapasitelere ulaşmış biçimidir. EEPROM'dan farklı olarak silme işlemi bayt bayt değil blok blok yapılır. Bu tasarım, yazma hızını artırır ve maliyeti düşürür. Flaş bellek teknolojisiyle USB bellekler, SD kartlar, SSD'ler ve modern sistemlerdeki BIOS/UEFI çipleri üretilir.

1.1.3.2. RAM Bellekler

RAM; bilgisayarlar, mobil cihazlar çalışırken verilerin ve komutların geçici olarak tutulduğu bellektir. Güç kesildiğinde içindeki tüm veriler silinir. İşlemci, çalıştıracağı komutları ve işleyeceği verileri doğrudan RAM'den alır ve sonuçları yine buraya yazar. Açık uygulamalar, işlenen dosyalar ve tarayıcı sekmeleri RAM üzerinde tutulur. Bu nedenle RAM kapasitesi, bir cihazın aynı anda kaç işi sorunsuz yürütebileceğini doğrudan etkiler. RAM bellekler üç farklı açıdan incelenir.

1. **Çalışma Mantığına Göre RAM Bellekler**

SRAM [Static RAM (Statik Rastgele Erişimli Bellek)], veriyi tutmak için sürekli yenileme gerektirmeyen, son derece hızlı ancak üretimi pahalı bellek türüdür. Yüksek maliyeti nedeniyle büyük kapasitelerde üretilmez. İşlemcinin içindeki önbelleklerinde SRAM kullanılır.

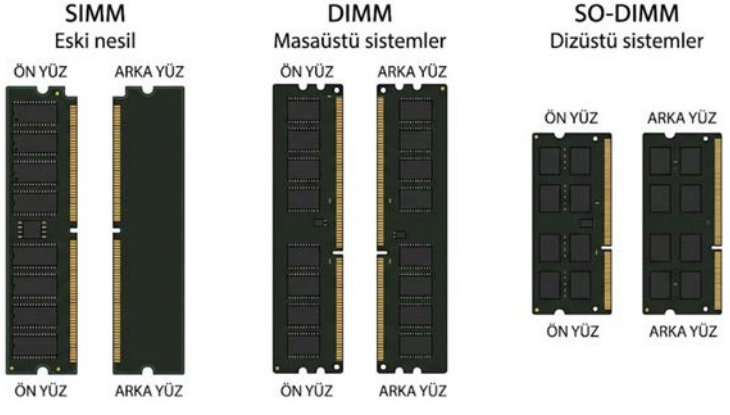
DRAM [Dynamic RAM (Dinamik Rastgele Erişimli Bellek)], veriyi tutabilmek için sürekli yenileme sinyaline ihtiyaç duyan bellek türüdür. SRAM'e göre daha yavaş ancak çok daha ucuz olduğu için yüksek kapasitelerde üretilebilir. Dijital cihazlardaki ana bellek modülleri DRAM teknolojisiyle üretilir.

2. **Fiziksel Yapısına Göre RAM Bellekler**

SIMM [Single In-line Memory Module (Tek Sıralı Bellek Modülü)], bellek kartının yalnızca bir yüzündeki bağlantı noktalarının aktif olduğu eski nesil fiziksel yapıdır (Görsel 1.24). Günümüz cihazlarında artık kullanılmamaktadır.

DIMM [Dual In-line Memory Module (Çift Sıralı Bellek Modülü)], bellek kartının her iki yüzündeki bağlantı noktalarının birbirinden bağımsız çalıştığı günümüz standardıdır (Görsel 1.24). Masaüstü bilgisayarlarda kullanılır.

SO-DIMM [Small Outline DIMM (Küçük Boyutlu DIMM)], DIMM'in boyutça kısaltılmış versiyonudur (Görsel 1.24). Dizüstü bilgisayarlar ve küçük form faktörlü sistemlerde tercih edilir. İçerdiği teknoloji DIMM ile aynıdır, yalnızca fiziksel boyutu daha küçüktür.



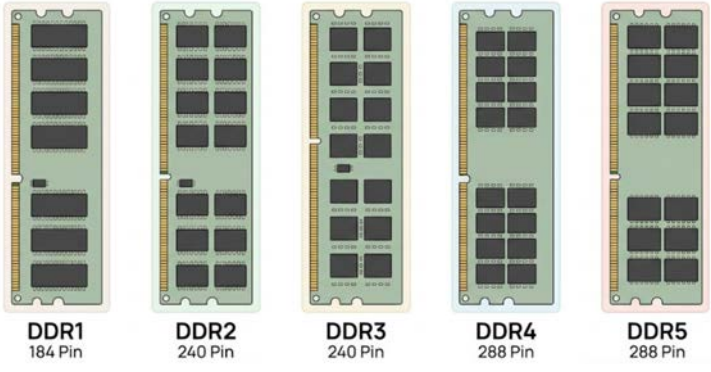
Görsel 1.24: Fiziksel yapısına göre RAM bellekler

3. DRAM Türlerine Göre RAM Bellekler

SDRAM [Synchronous (Eşzamanlı) DRAM], işlemcinin saat sinyaliyle eşzamanlı çalışan bellek türüdür. Günümüz modern bellek teknolojilerinin temelini oluşturur.

RDRAM (Rambus DRAM), yüksek performans hedefiyle geliştirilmiş özel bir bellek türüdür. Dönemine göre hızlıydı ancak yüksek maliyet ve ısı üretimi nedeniyle yaygınlaşamamış ve piyasadan çekilmiştir.

DDR [Double Data Rate (Çift Veri Hızı)], her saat darbesinde iki kez veri taşıyarak SDRAM'e göre iki kat daha fazla veri aktarabilen bellek teknolojisidir. Nesil yükseldikçe hız artar, voltaj düşer ve enerji verimliliği iyileşir. Her neslin ayrı bir yuvası olduğundan farklı nesiller birbirinin yuvalarıyla fiziksel olarak uyumlu değildir. DDR serisinde DDR1'den DDR5'e kadar her nesilde hız artarken voltaj düşmüş ve enerji verimliliği iyileşmiştir. Görsel 1.25'te nesillerine göre DDR RAM modülleri ve pin sayıları görülmektedir.



Görsel 1.25: Nesillerine göre DDR RAM modülleri

KONTROL NOKTASI

Bir bilgisayara bellek eklerken veya değiştirirken yalnızca kapasite yeterli değildir. Şu dört uyumluluk noktası kontrol edilmelidir:

- **Nesil Uyumu:** Anakartın desteklediği DDR nesliyle bellek modülünün neslinin örtüşmesi gerekir. Örneğin DDR4 yuvası olan bir anakarta DDR5 modülü fiziksel olarak takılamaz.
- **Frekans:** Bellek modülünün frekansı (MHz), anakartın desteklediği frekans aralığında olmalıdır. Desteklenmeyen bir frekansta çalışan modül, anakart tarafından daha düşük bir frekansta çalıştırılabilir.
- **Slot Sayısı ve Kapasite Sınırı:** Anakart üzerindeki slot sayısı ve desteklenen maksimum kapasite, takılabilecek bellek miktarını belirler.
- **Form Faktörü:** Masaüstü bilgisayarlar DIMM, dizüstü bilgisayarlar ise SO-DIMM modülü kullanır. Bu ikisi birbirinin yuvasına takılamaz.

LPDDR [Low Power (Düşük Güç) DDR], DDR teknolojisinin akıllı telefonlar, tabletler ve ince dizüstü bilgisayarlar için düşük güç tüketimi önceliğiyle yeniden tasarlanmış versiyonudur. LPDDR4, LPDDR5 gibi nesilleri mevcuttur.

GDDR [Graphics (Grafik) DDR], DDR teknolojisinin ekran kartları için özelleştirilmiş versiyonudur. Ekran kartının işlemcisi olan GPU, aynı anda çok büyük miktarda görüntü verisini işlemek zorundadır. GDDR, bu ihtiyaca yanıt verecek şekilde yüksek bant genişliği öncelikli olarak tasarlanmıştır. GDDR5, GDDR6 gibi nesilleri mevcuttur.

SIRA SİZDE

Aşağıda bir bilgisayar laboratuvarının yenilenmesi sürecinde bellek türleri ve uyumluluk kararlarını konu alan bir senaryo verilmiştir.

Senaryo

Bilişim teknolojileri öğretmeni Sercan Bey, okuldaki bilgisayar laboratuvarını yenilemek için teknik bir değerlendirme yapıyor. Elinde dört farklı bilgisayar bulunuyor ve her biri için farklı bir karar alması gerekiyor.

1. Bilgisayar (Masaüstü)
   - Anakart DDR4 destekliyor ve dört adet DIMM slotu var.
   - Şu an yalnızca bir adet slota 8 GB DDR4-3200 takılıdır.
   - Bilgisayar, video düzenleme yazılımı çalıştırırken belirgin şekilde yavaşlıyor.

2. Bilgisayar (Dizüstü)
   - Anakart DDR4 destekliyor ve bir adet SO-DIMM slotu var.
   - Sercan Bey, depoda yedek olarak bir adet 8 GB DDR4-3200 DIMM modülü buluyor ve bunu dizüstü bilgisayara takmak istiyor.

3. Bilgisayar (Eski Masaüstü)
   - Anakart DDR3 destekliyor ve iki adet DIMM slotu var.
   - Sercan Bey'in elinde yedek olarak bir adet 8 GB DDR4-3200 DIMM modülü bulunuyor.

4. Bilgisayar (Yeni Masaüstü)
   - Anakart DDR5 destekliyor ve dört adet DIMM slotu var.
   - Sercan Bey, biri 16 GB DDR5-4800, diğeri 16 GB DDR5-6000 olan iki farklı modül arasında karar veremiyor.

Aşağıdaki soruları senaryo metnine dayanarak cevaplayınız. Kararlarınızı teknik gerekçelerle destekleyiniz.

Sorular

1. Birinci bilgisayar için Sercan Bey hangi tür bellek modülü almalıdır? Kapasite ve uyumluluk açısından gerekçesini yazınız.

Bellek Türü: _____ **Kapasite Öneriniz:** _____	**Gerekçeniz:** _____ _____ _____

2. Sercan Bey bulduğu DIMM modülünü ikinci bilgisayara takabilir mi? Neden?

☐ Evet ☐ Hayır	**Gerekçeniz:** _____ _____ _____ **Uygun Form Faktörü:** _____

3. Sercan Bey elindeki DDR4-3200 modülünü üçüncü bilgisayara takabilir mi? Neden?

☐ Evet ☐ Hayır	**Gerekçeniz:** _____ _____ _____ **Bu Bilgisayar İçin Uygun Nesil:** _____

4. Sercan Bey, dördüncü bilgisayar için her iki modül de fiziksel olarak uyumlu olduğundan iki modülden hangisini tercih etmelidir? Bu modüllerin frekans farkı, sistemi nasıl etkiler?

☐ 16 GB DDR5-4800 ☐ 16 GB DDR5-6000	**Frekans Farkının Etkisi:** _____ _____ **Anakart DDR5-4800 destekliyorsa DDR5-6000 nasıl çalışır?** _____

Genel Değerlendirme

Bir bellek modülü seçerken kontrol edilmesi gereken dört uyumluluk ölçütünü aşağıya yazınız.

1	
2	
3	
4	

1.1.4. Disk Sürücüler

Bilgisayarda işlemci hesaplar, RAM geçici olarak tutar ancak verinin kalıcı olarak saklanması için ayrı bir birime ihtiyaç vardır. Bu birim, disk sürücüsüdür. Disk sürücüsü, bilgisayar kapatıldığında bile dosyaların, işletim sisteminin ve uygulamaların korunmasını sağlar. Disk sürücüleri; veriyi fiziksel olarak nasıl sakladıklarına, okuma-yazma hızlarına, bağlantı arabirimlerine ve kullanım alanlarına göre farklılık gösterir.

1.1.4.1. HDD

HDD [Hard Disk Drive (Sabit Disk Sürücüsü)], veriyi manyetik olarak kaplı dönen diskler (plaka) üzerinde saklayan mekanik depolama birimidir. Plakalar yüksek hızda dönerken okuma-yazma kafası veriye erişir. Bu mekanik yapı, HDD'nin temel çalışma ilkesini belirler. HDD'nin kapasitesi diğer depolama türlerine kıyasla düşük maliyetle yükseğe çıkabilir. Bu nedenle büyük veri arşivleri, yedekleme sistemleri ve maliyet odaklı depolama çözümlerinde tercih edilir ancak mekanik yapısı nedeniyle hareketli parça içerir. Bu durum hem erişim hızını sınırlar hem de fiziksel darbeye karşı duyarlılığı artırır. HDD'ler **bağlantı arabirimine** göre iki grupta incelenir.

SATA [Serial Advanced Technology Attachment (Seri Gelişmiş Teknoloji Bağlantısı)] HDD: Günümüz masaüstü ve dizüstü bilgisayarlarında en yaygın kullanılan HDD bağlantı türüdür (Görsel 1.26). Veri ve güç kabloları ayrıdır, anakart üzerindeki SATA portuna bağlanır.

SAS [Serial Attached SCSI (Seri Bağlı SCSI)] HDD: Sunucu ve kurumsal depolama sistemlerinde kullanılan yüksek performanslı bağlantı türüdür. SATA'ya göre daha hızlı ve güvenilirdir ancak maliyeti yüksektir.



Görsel 1.26: SATA HDD

BİLGİ KUTUSU : HDD'lerde Dönüş Hızı (RPM)

HDD'lerde plaka dönüş hızı, RPM [Revolutions Per Minute (Dakikadaki Devir Sayısı)] ile ifade edilir. Yaygın değerler 5.400 RPM ve 7.200 RPM'dir. Dönüş hızı arttıkça veriye erişim süresi kısalır ancak ısı üretimi ve güç tüketimi de artar.

1.1.4.2. SSD

SSD [Solid State Drive (Katı Hâl Sürücüsü)], veriyi dönen disk veya hareketli parça kullanmadan flaş bellek hücrelerinde saklayan depolama birimidir. Mekanik yapı içermediğinden erişim hızı HDD'ye kıyasla çok daha yüksektir, fiziksel darbeye karşı dayanıklıdır ve sessiz çalışır.



Görsel 1.27: SATA SSD

SATA SSD: HDD ile aynı SATA arabirimini kullanan SSD türüdür (Görsel 1.27). Fiziksel boyut olarak genellikle 2,5 inç formunda üretilir ve anakarta HDD ile aynı kablo bağlantısıyla bağlanır. Bu özelliği, eski sistemlerde HDD'nin yerini kolayca almasını sağlar.

SATA arabiriminin veri aktarım hızı teorik olarak 600 MB/sn ile sınırlıdır. SATA SSD bu sınır dâhilinde HDD'ye göre belirgin biçimde hızlı çalışır ancak NVMe SSD'nin sunduğu hızlara ulaşamaz.

NVMe SSD: NVMe [Non-Volatile Memory Express (Geçici Olmayan Bellek Hızlandırıcı)], flaş bellek depolamanın yüksek hız potansiyelinden tam anlamıyla yararlanmak için geliştirilmiş modern bir arabirim protokolüdür. SATA'nın sabit disk döneminden gelen kısıtlamalarını ortadan kaldırır ve doğrudan PCIe şeritleri üzerinden işlemciyle iletişim kurar.

NVMe SSD'ler çoğunlukla M.2 form faktöründe üretilir ve anakart üzerindeki M.2 yuvasına doğrudan takılır ve ayrıca kablo gerektirmez (Görsel 1.28). Veri aktarım hızı modele ve nesle göre değişmekle birlikte SATA SSD'nin birkaç katına ulaşabilir. Yüksek performans gerektiren sistemlerde, oyun bilgisayarlarında ve profesyonel iş istasyonlarında yaygın olarak kullanılır.



Görsel 1.28: NVMe SSD

KONTROL NOKTASI

M.2 bir yuva türüdür, NVMe ise bir arabirim protokolüdür. M.2 yuvaya hem SATA hem NVMe SSD takılabilir ancak iki modül, fiziksel olarak benzer görünse de çalışma hızları arasında büyük fark vardır. Üründe yalnızca **M.2 SSD** yazıyor olması, NVMe olduğu anlamına gelmez. Arabirim bilgisi, ayrıca kontrol edilmelidir.

1.1.4.3. Optik Sürücüler

Optik sürücü, veriyi lazer ışığıyla okuyup yazabilen depolama birimidir. CD, DVD ve Blu-ray diskler bu teknolojinin en yaygın örnekleridir (Görsel 1.29). Her nesil, daha kısa dalga boylu lazer kullanarak daha yüksek veri yoğunluğuna ulaşmıştır.

Bu dönemde optik sürücüler, bilgisayarlarda eskisi kadar yer bulmaz. İnce dizüstü bilgisayarlarda ve birçok masaüstü sistemde artık standart olarak bulunmaz. Bununla birlikte film arşivleme, yazılım dağıtımı, uzun süreli veri yedekleme gibi özel kullanım alanlarında varlığını korumaktadır.



Görsel 1.29: Optik sürücüler

1.1.4.4. Disk Sürücülerinin Karşılaştırması

Disk sürücüleri depolama yöntemi, hız, bağlantı arabirimi ve kullanım amacı açısından birbirinden belirgin biçimde ayrılır. Tablo 1.1, bu farklılıkları bir arada göstermektedir.

Tablo 1.1: Disk Sürücülerinin Özellikleri

Özellik	HDD	SATA SSD	NVMe SSD	Optik Sürücü
Depolama Yöntemi	Manyetik (mekanik)	Flaş bellek	Flaş bellek	Lazer / optik
Hız	Düşük	Orta	Yüksek	Düşük
Bağlantı Arabirimi	SATA/SAS	SATA	PCIe/M.2	SATA/USB
Fiziksel Dayanıklılık	Düşük (hareketli parça)	Yüksek	Yüksek	Orta (disk kırılganlığı)
Kapasite / Maliyet	En avantajlı	Orta	En yüksek maliyet	Düşük maliyet
Yaygın Kullanım	Arşiv, yedekleme	Genel kullanım	Yüksek performans	Arşivleme, medya

KONTROL NOKTASI

Depolama birimi seçerken tek ölçüt hız değildir. Bütçe, kapasite ihtiyacı, sistemin bağlantı desteği ve kullanım amacı birlikte değerlendirilmelidir. Örneğin büyük kapasiteli arşiv için HDD hâlâ mantıklı bir seçenekken işletim sistemi diski için SSD, belirgin bir performans farkı yaratır.

SIRA SİZDE

Senaryo başlığında belirtilen kullanım senaryolarını okuyunuz. O senaryo için en uygun disk sürücüsünü aşağıdan seçerek, önündeki harfi **Cevap** sütununa yazıp doğru senaryo ile eşleştiriniz.

A: SATA HDD	B: SAS HDD	C: SATA SSD	Ç: NVMe SSD	D: Optik Sürücü

Senaryo	Cevap
1. Bir okul; yüzlerce öğrencinin kayıt dosyalarını, fotoğraflarını ve belgelerini düşük maliyetle uzun süre saklamak istiyor.	
2. Bir oyun geliştiricisi, büyük boyutlu oyun dosyaları yüklenirken oluşan bekleme süresini en aza indirmek için depolama birimini yükseltmek istiyor.	
3. Bir müzik prodüksiyon şirketi, eski konserlerden derlenen arşiv materyallerini kalıcı olarak saklamak ve bunlara zaman zaman erişmek istiyor.	
4. Bir öğrenci, eski bir dizüstü bilgisayarını yavaşlık nedeniyle yenilemek istiyor ama bütçesi sınırlı ve mevcut dizüstü bilgisayarında belirgin bir hız artışı sağlamaya karar veriyor.	

ARAŞTIRMA

Kullandığınız veya evinizde bulunan bir bilgisayarın yahut akıllı telefonun depolama birimini araştırınız. Araştırma sonucunda depolama birimiyle ilgili edindiğiniz bilgileri aşağıdaki başlıkların karşısına yazınız.

Cihaz Türü	
Depolama Birimi Türü	
Kapasite	
Bağlantı Arabirimi (Varsa belirtiniz.)	
Bilgiye Ulaştığınız Yöntem	

Araştırma sonucunda aşağıdaki soruları cevaplayınız:

1. Araştırma sürecinde cihazın depolama bilgisine nasıl ulaştınız (Ayarlar menüsü, sistem bilgisi, üretici sitesi vb.)?
2. Bu cihaz için farklı bir depolama birimi seçseydiniz hangisini tercih ederdiniz? Neden?
3. Seçtiğiniz depolama biriminin avantajı ve dezavantajı nedir?

1.1.5. RAID Teknolojisi

RAID [Redundant Array of Independent Disks (Bağımsız Disklerin Yedekli Dizisi)], birden fazla disk sürücüsünü tek bir mantıksal birim olarak bir araya getiren depolama teknolojisidir. Tek bir disk yerine birden fazla diskin birlikte çalıştırılması; performansı artırma, veri güvenliğini sağlama veya her ikisini birden elde etme amacıyla kullanılır. RAID teknolojisi temelde iki ilkeye dayanır.

1. Şeritleme (Striping): Veri, diskler arasında bölünerek paralel yazılır. Bu yöntem, okuma ve yazma hızını artırır ancak disklerden biri arızalanırsa tüm veri kaybolur.

2. Yansıtma (Mirroring): Aynı veri, birden fazla diske eş zamanlı olarak yazılır. Disklerden biri arızalansa bile veri, diğerinden okunmaya devam eder.

RAID yapılandırmaları donanım veya yazılım tabanlı olarak kurulabilir. **Donanım RAID**; ayrı bir RAID denetleyici kartı üzerinden yönetilir, daha yüksek performans sunar ancak maliyeti fazladır. **Yazılım RAID** ise işletim sistemi üzerinden yapılandırılır, maliyet avantajı sağlar ancak işlemciyi daha fazla kullanır.

RAID teknolojisinde farklı ihtiyaçlara yönelik geliştirilmiş çok sayıda seviye bulunur. RAID 2, RAID 3, RAID 4, RAID 7 gibi seviyeler teknik açıdan var olsa da günümüz sistemlerinde artık tercih edilmemektedir.

BİLGİ KUTUSU : Yedekleme ve RAID İlişkisi

RAID, tek başına bir yedekleme çözümü değildir. Disklerin aynı fiziksel ortamda bulunması nedeniyle yangın, su baskını, güç dalgalanması gibi durumlarda tüm diskler birlikte zarar görebilir. Bu nedenle RAID, tek başına yeterli bir veri koruma yöntemi olarak değil düzenli yedekleme stratejilerinin tamamlayıcısı olarak değerlendirilmelidir.

RAID 0 (Şeritleme): Veriyi en az iki disk arasında bölerek okuma ve yazma hızını artırır ancak disklerden biri arızalanırsa tüm veri kaybolur. Bu nedenle hız öncelikli ve veri kaybının tolere edilebildiği sistemlerde tercih edilir.

RAID 1 (Yansıtma): Aynı veriyi en az iki diske eş zamanlı yazarak disklerden biri arızalansa bile veri erişimini sürdürür. İşletim sistemi diskleri ve kritik veri barındıran sistemlerde yaygın olarak kullanılır.

RAID 5 (Şeritleme ve Eşlik Biti): Veri ve eşlik bitini en az üç disk arasında dağıtık olarak yazar, bir disk arızalanırsa veri yeniden oluşturulabilir. Dosya sunucuları ve genel amaçlı sunucu depolamasında yaygın olarak tercih edilir.

RAID 6 (Çift Eşlik Biti): RAID 5'in geliştirilmiş versiyonudur. Çift eşlik biti sayesinde aynı anda iki disk arızalansa bile veri korunur ve en az dört disk gerektirir. Yüksek güvenilirlik gerektiren büyük veri merkezlerinde tercih edilir.

RAID 10 (Şeritleme ve Yansıtma): RAID 1 ve RAID 0'ı birleştirerek hem yüksek performans hem veri güvenliği sunar ancak en az dört disk gerektirir. Yüksek performans ve güvenilirliğin bir arada gerektiği kurumsal sistemlerde, e-posta ve veri tabanı sunucularında kullanılır.

KONTROL NOKTASI

RAID seçiminde tek ölçüt hız ya da güvenlik değildir. Bütçe, disk sayısı, kapasite ihtiyacı ve sistemin tolerans edebileceği arıza süresi birlikte değerlendirilmelidir. Yüksek hız için RAID 0, yüksek güvenlik için RAID 1 veya RAID 6, her ikisi için RAID 10 tercih edilebilir.

1.1.6. Ekran Kartı

Bilgisayarda üretilen görüntünün ekrana aktarılması, bu işin fiziksel hesaplamasını üstlenen bir donanım birimi olmadan mümkün değildir. **Ekran kartı (graphics card)**, grafik verilerini işleyerek monitör, televizyon, projektör gibi görüntüleme cihazlarına aktaran donanım birimidir (Görsel 1.30). Oyunlardan video düzenlemeye, üç boyutlu modelleme yazılımlarından yapay zekâ uygulamalarına kadar görsel hesaplama gerektiren her alanda ekran kartı belirleyici bir rol üstlenir. Bugün ekran kartları yalnızca görüntü çıkışıyla sınırlı kalmaz. Bilimsel hesaplama, veri işleme gibi alanlarda da kullanılır.



Görsel 1.30: Ekran kartı

1.1.6.1. Ekran Kartının Yapısı

Bir ekran kartı, birbirine bağlı dört temel bileşenden oluşur. Bu bileşenlerin her biri, görüntü verilerinin işlenmesinden ekrana aktarılmasına kadar geçen sürecin farklı bir aşamasını üstlenir.

GPU [Graphics Processing Unit (Grafik İşlem Birimi)]: Ekran kartının merkezî işlem çipidir. CPU'dan farklı olarak aynı anda çok sayıda küçük hesaplamayı paralel yürütecek şekilde tasarlanmıştır. Bu yapı özellikle piksel işleme, üç boyutlu hesaplama, yapay zekâ iş yükleri gibi paralel işlem gerektiren görevlerde GPU'yu son derece verimli kılar.

VRAM [Video Random Access Memory (Video Rastgele Erişimli Bellek)]: GPU'nun doğrudan eriştiği yüksek hızlı grafik belleğidir. İşlenecek görüntü verileri, dokular ve kare tamponları VRAM üzerinde tutulur. VRAM kapasitesi arttıkça GPU daha yüksek çözünürlüklü içeriklerle ve daha büyük veri kümeleriyle çalışabilir. GDDR serisi (GDDR5 ve GDDR6), VRAM teknolojisinin güncel standardıdır.

Soğutma Sistemi: GPU yoğun grafik işlemleri sırasında önemli miktarda ısı üretir. Bu ısının denetim altında tutulması hem performans hem de uzun ömür açısından kritiktir. Haricî ekran kartlarında çoğunlukla fan ve ısı borusu içeren hava soğutma sistemleri kullanılır. Yüksek performanslı modellerde ise sıvı soğutma çözümleri tercih edilebilir.

Çıkış Portları: Ekran kartı, ürettiği görüntü sinyalini çıkış portları aracılığıyla görüntüleme cihazına aktarır.

Günümüz ekran kartlarında yaygın olarak şu port türleri bulunur (Görsel 1.31):

1. **VGA:** Analog görüntü sinyali taşır. Yeni nesil ekran kartlarında artık yer almaz, eski sistemlerle uyumluluk için hâlâ karşılaşılabilir.
2. **DVI** [Digital Visual Interface (Dijital Görsel Arayüz)]: Dijital görüntü sinyali taşır. Analog VGA'dan sonra HDMI'dan önce yaygınlaşmış bir bağlantı türüdür.
3. **HDMI:** Görüntü ve sesi tek kablo üzerinden aktarır. Televizyon ve monitör bağlantısında yaygın olarak kullanılır.
4. **DisplayPort:** Yüksek çözünürlük ve yüksek yenileme hızı gerektiren ekranlar için tercih edilir. Birden fazla monitörü tek porttan zincirleme bağlamayı (daisy chain) destekler.



Görsel 1.31: Ekran kartı çıkış portları

BİLGİ KUTUSU : Çoklu Monitör Kurulumu

Bir ekran kartında birden fazla çıkış portu bulunabilir. Bu sayede tek bir bilgisayara aynı anda birden fazla monitör bağlanabilir. Çoklu monitör kurulumları özellikle finans, tasarım, yazılım geliştirme gibi alanlarda yaygındır.

1.1.6.2. Entegre (Tümleşik) Ekran Kartı

Entegre ekran kartı, ayrı bir PCIe kartı olmaksızın grafik işleme işlevini sisteme dâhil eden çözümdür. İki farklı biçimde karşılaşılır.

İşlemciye Entegre GPU: Grafik birimi, işlemci çipinin içine entegre edilmiştir. İşlemci ve GPU aynı silikon üzerinde birlikte çalışır. GPU için ayrı bir bellek yoktur, ana bellek (RAM) paylaşılır. Düşük güç tüketimi sayesinde dizüstü bilgisayarlarda ve ince tasarımlı sistemlerde yaygın olarak kullanılır.

Anakarta Tümleşik (Onboard) GPU: Anakart üzerinde işlemciden bağımsız ayrı bir GPU çipi bulunur ancak bu çip haricî bir PCIe kartı değildir. İşlemciye entegre GPU'ya kıyasla biraz daha bağımsız bir yapıya sahiptir. Bütçe odaklı masaüstü sistemlerde ve özel grafik gereksinimi olmayan iş istasyonlarında tercih edilir.

1.1.6.3. Haricî Ekran Kartı

Haricî ekran kartı, anakart üzerindeki PCIe x16 yuvasına takılan ve yalnızca grafik işlemeye adanmış bağımsız bir donanım birimidir. Kendi GPU çipi, VRAM'i ve soğutma sistemi bulunur. İşlemcinin kaynaklarına bağımlı değildir. Bu bağımsız yapı, haricî ekran kartlarına entegre çözümlere kıyasla çok daha yüksek grafik performansı sağlar. Yüksek çözünürlüklü oyunlar, üç boyutlu modelleme ve animasyon yazılımları, video düzenleme, yapay zekâ model eğitimi, bilimsel hesaplama gibi yoğun grafik veya paralel işlem gerektiren alanlarda haricî ekran kartı kullanımı zorunlu hâle gelir.

BİLGİ KUTUSU : Entegre ve Haricî Ekran Kartının Birlikte Çalışması

Bir bilgisayarda hem entegre hem haricî ekran kartı bulunabilir. İşletim sistemi, enerji tasarrufu için hafif görevlerde entegre GPU'yu, yoğun işlemlerde ise haricî ekran kartını devreye sokabilir.

1.1.7. Ağ Arayüz Kartı

Her bilgisayar, ağa bağlanabilmek için kablolu veya kablosuz bir bağlantı noktasına ihtiyaç duyar. Bu bağlantı için ağ arayüz kartı [Network Interface Card (NIC)] kullanılır ve bilgisayarın ağ üzerindeki diğer cihaz, sunucu ve internet altyapısıyla iletişim kurmasını sağlayan donanım birimidir. Kablolu veya kablosuz olarak veri paketlerini gönderir ve alır. Bu süreçte ağ protokollerinin gerektirdiği düşük düzeyli iletişim işlemlerini üstlenir. Bu dönemde ağ arayüz kartı çoğunlukla anakarta tümleşik (onboard) biçimde gelir ancak özel ihtiyaçlar doğrultusunda PCIe yuvasına takılan haricî NIC kartları da kullanılır.

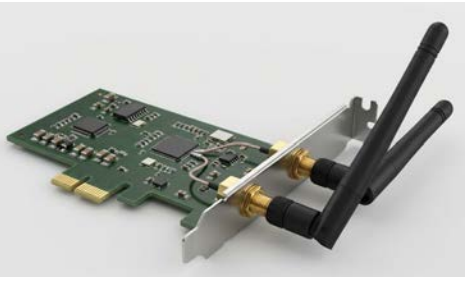
1.1.7.1. Ağ Arayüz Kartı Türleri

Ağ arayüz kartları, kullandığı iletişim ortamına göre üç ana türde incelenir.



Görsel 1.32: Kablolu ağ arayüz kartı

Kablolu NIC (Ethernet): Ağ kablosuyla fiziksel bağlantı kuran türdür. RJ-45 girişine takılan Ethernet kablosu aracılığıyla veri iletimi gerçekleştirir (Görsel 1.32). Kablolu bağlantı, kablosuz alternatiflerine göre daha kararlı, hızlı ve dış parazitlere karşı dayanıklıdır. Bu nedenle sunucu odaları, oyun bilgisayarları, kurumsal ağlar gibi güvenilirlik ve hızın ön planda olduğu ortamlarda tercih edilir. Şu anda 1 Gbps (Gigabit Ethernet) hız standardı yaygın kullanımdadır. Yüksek performanslı sistemlerde 10 Gbps ve üzeri çözümler de mevcuttur.



Görsel 1.33: Kablosuz ağ arayüz kartı

Kablosuz NIC (Wi-Fi): Radyo dalgaları aracılığıyla bir kablosuz erişim noktasına veya kablosuz yönlendiriciye bağlanarak ağa erişim sağlar. Fiziksel kablo gerektirmediğinden mobil cihazlarda, dizüstü bilgisayarlarda ve akıllı telefonlarda standart olarak kullanılır. Masaüstü sistemlerde ise anakarta tümleşik olarak gelebileceği gibi PCIe yuvasına takılan kart biçiminde (Görsel 1.33) veya USB arabirimi üzerinden de eklenebilir. **IEEE 802.11** standardı ailesinin farklı sürümleri (802.11n, 802.11ac, 802.11ax gibi) kablosuz NIC'lerin çalışma frekansını, hızını ve menzilini belirler.

BİLGİ KUTUSU : Wi-Fi Bir Kısaltma Değil

Wi-Fi adının bir kısaltma olduğu yaygın bir yanılgıdır. Gerçekte Wi-Fi, herhangi bir ifadenin kısaltması değildir. IEEE 802.11 kablosuz ağ standardını tanımlamak için oluşturulmuş özgün bir terimdir. Günlük kullanımda ise kablosuz ağ bağlantısının genel adı hâline gelmiştir.

Fiber Optik NIC: Veriyi elektrik sinyali yerine ışık darbeleri aracılığıyla ileten türdür (Görsel 1.34). **SFP [Small Form-factor Pluggable (Küçük Form Faktörlü Takılabilir)]** yuvasına fiber optik kablo bağlanır. Bakır kabloya kıyasla çok daha yüksek hız ve uzun mesafe iletimi sunar ve elektromanyetik parazitlerden etkilenmez. Veri merkezleri, kampüs ağları ve yüksek bant genişliği gerektiren kurumsal altyapılarda kullanılır.



Görsel 1.34: Fiber optik ağ arayüz kartı

1.1.7.2. MAC Adresi

Ağa bağlanan her cihazın, diğer cihazlardan ayırt edilebilmesi için benzersiz bir kimlik bilgisine ihtiyacı vardır. **MAC [Media Access Control (Ortam Erişim Denetimi)] adresi**, her ağ arayüz kartına üretim aşamasında üretici tarafından kalıcı olarak atanan ve o kartı dünya genelinde benzersiz biçimde tanımlayan fiziksel adrestir. Verinin yerel ağ içinde doğru cihaza ulaşmasında MAC adresi belirleyici rol oynar. MAC adresi, onaltılık (hexadecimal) sayı sistemiyle ifade edilen 48 bitlik (6 baytlık) bir değerdir. Genellikle iki nokta (:) veya tire (-) ile ayrılan altı çift, onaltılık rakamdan oluşur.

Örnek: A4:C3:F0:1B:7E:22

MAC adresi şu iki eşit bölüme ayrılır:

OUI [Organizationally Unique Identifier (Organizasyona Özgü Tanımlayıcı)]: İlk 24 bit (3 bayt), kartı üreten firmaya IEEE tarafından atanmış üretici kodudur. Bu kod sayesinde bir MAC adresinden kartın üreticisi belirlenebilir.

Cihaz Tanımlayıcısı: Son 24 bit (3 bayt), üretici tarafından her karta özgü olarak atanan seri numarasıdır. Aynı üreticinin farklı kartları bu bölümde birbirinden ayrılır.

KONTROL NOKTASI

MAC adresi fiziksel kimlik, IP adresi ise mantıksal konumdur. Posta sistemine benzetmek gerekirse MAC adresi alıcının kimliği, IP adresi ise alıcının bulunduğu adrestir. Yerel ağda paketin doğru karta ulaşması, MAC adresiyle sağlanırken internette doğru ağa ulaşması IP adresiyle gerçekleşir.

ARAŞTIRMA

Kişisel bilgisayar, tablet veya akıllı telefonunuzun MAC adresini nasıl tespit edeceğinizi araştırarak edindiğiniz bilgileri işlem adımları hâlinde yazınız. Bu adımları uygulayıp, cihazınızın MAC adresini tespit ederek işletim sistemiyle birlikte aşağıdaki çizelgeye yazınız.

Cihaz Türü	İşletim Sistemi	MAC Adresi
Kişisel Bilgisayar		
Akıllı Telefon		
Tablet		

1.1.8. Ses Kartı

Bilgisayarlarda ses üretimi ve işlenmesi için de ayrı bir donanım birimine ihtiyaç vardır. **Ses kartı**, dijital ses verilerini analog ses sinyallerine dönüştürerek hoparlör, kulaklık gibi çıkış aygıtlarına ileten aynı zamanda mikrofon gibi giriş aygıtlarından gelen analog sinyalleri dijitale çevirerek sisteme aktaran donanım birimidir.

Ses kartı, tıpkı ağ arayüz kartı gibi günümüz anakartlarının büyük çoğunluğuna tümleşik (onboard) biçimde gelir. Günlük kullanım, müzik dinleme, video izleme gibi standart ihtiyaçlar için tümleşik ses kartı yeterlidir. Profesyonel müzik üretimi, ses kayıt stüdyosu çalışmaları, yüksek kaliteli oyun deneyimi gibi özel ihtiyaçlar söz konusu olduğunda ise **PCIe yuvasına** takılan haricî ses kartları tercih edilir. Ses kartının temel bileşenleri şunlardır:

DSP [Digital Signal Processor (Dijital Sinyal İşlemci)]: Ses verilerini işleyen, efekt uygulayan ve sesi optimize eden özel çiptir. İşlemcinin bu yükü taşıması yerine ses işleme görevi DSP'ye devredilir.

DAC [Digital-to-Analog Converter (Dijital-Analog Dönüştürücü)]: Bilgisayardaki dijital ses verisini analog sinyale çevirerek hoparlör veya kulaklığa iletir.

ADC [Analog-to-Digital Converter (Analog-Dijital Dönüştürücü)]: Mikrofon veya enstrümandan gelen analog sesi dijital veriye dönüştürür.

Ses Giriş-Çıkış Portları: 3,5 mm ses jakı en yaygın bağlantı türüdür. Kulaklık çıkışı, mikrofon girişi, hat girişi ve çıkışı bu portlar üzerinden gerçekleşir. Yüksek kaliteli ses kartlarında optik ses (S/PDIF) ve XLR portları da bulunabilir.

1.1.9. Bilgisayar Kasaları

Bilgisayarın iç donanım birimlerini bir arada tutan, fiziksel darbelerden, tozdan ve elektromanyetik parazitlerden koruyan yapıya **bilgisayar kasası** denir. Kasa yalnızca bir kap değildir. İç bileşenlerin düzenli yerleşimini, kablo yönetimini, hava akışını ve ısı dağılımını da doğrudan etkiler. Doğru seçilmiş bir kasa, sistemin kararlı ve serin çalışmasına önemli katkı sağlar. Bilgisayar kasaları form faktörlerine ve kullanım amaçlarına göre çeşitli türlerde üretilir.



Görsel 1.35: Kule kasa çeşitleri

Kule (Tower) Kasa: Dikey konumda duran, masaüstü bilgisayar sistemlerinde en yaygın kullanılan kasa türüdür. Fiziksel boyutuna göre üç alt kategoride incelenir (Görsel 1.35).

1. **Full Tower (Tam Kule):** En büyük kule kasadır. Çok sayıda PCIe kartı, depolama birimi ve gelişmiş soğutma çözümleri için geniş iç alan sunar. Sunucu benzeri iş istasyonlarında ve yüksek performanslı oyun sistemlerinde tercih edilir.
2. **Mid Tower (Orta Kule):** Kule kasaların en yaygın boyutudur. ATX ve Micro-ATX anakartlarla uyumludur, iç alan ile fiziksel boyut arasında dengeli bir seçenek sunar.
3. **Mini Tower (Küçük Kule):** Küçük form faktörlü sistemler için tasarlanır. Micro-ATX ve Mini-ITX anakartlarla uyumludur, masa üzerinde daha az yer kaplar.

Masaüstü (Desktop) Kasa: Yatay konumda duran ve üzerine monitör yerleştirilebilen kasa türüdür (Görsel 1.36). Ofis ortamlarında alan tasarrufu için tercih edilir. Bu dönemde kule kasalar kadar yaygın değildir.

Küçük Form Faktörlü (SFF) Kasa: Mini-ITX anakartlara uygun, son derece kompakt boyutlarda üretilen kasa türüdür (Görsel 1.37). Medya merkezi uygulamaları, ince istemciler ve kısıtlı alanlarda kullanılan sistemler için uygundur. İç alanın sınırlı olması nedeniyle soğutma ve genişleme seçenekleri kısıtlıdır.

Raf (Rack) Kasa: Sunucu raflarına monte edilmek üzere tasarlanmış, yatay ve ince profilli kasa türüdür (Görsel 1.38). Birim yüksekliği **U (rack unit)** ile ölçülür. 1U yaklaşık 44 mm'ye karşılık gelir. Birden fazla sunucunun düzenli ve verimli biçimde bir araya getirildiği veri merkezleri ve kurumsal bilişim altyapılarında kullanılır.



Görsel 1.36: Masaüstü kasa



Görsel 1.37: SFF kasa



Görsel 1.38: Raf kasa

BİLGİ KUTUSU : Kasa Seçiminde Dikkat Edilecek Hususlar

Kasa seçimi yapılırken anakartın form faktörü, soğutma ihtiyacı, PCIe kart sayısı ve fiziksel alan göz önünde bulundurulmalıdır. Özellikle güçlü ekran kartı kullanılan sistemlerde kartın fiziksel uzunluğunun kasaya sığıp sığmadığı kontrol edilmelidir.

1.1.10. Güç Kaynağı

Bilgisayar bileşenlerinin çalışabilmesi için elektrik enerjisine ihtiyaçları vardır ancak bu enerji doğrudan prizden alınan formda kullanılamaz. **PSU [Power Supply Unit (Güç Kaynağı Birimi)]**, şehir şebekesinden gelen alternatif akımı (AC) bilgisayar bileşenlerinin ihtiyaç duyduğu doğru akıma (DC) dönüştüren ve belirli voltaj seviyelerinde sisteme dağıtan donanım birimidir (Görsel 1.39).



Görsel 1.39: Güç kaynağı

Güç kaynağının görevi yalnızca dönüşüm yapmakla sınırlı değildir. Voltaj dalgalanmalarına karşı bileşenleri korur, aşırı yük veya kısa devre durumlarında sistemi kapatarak hasarı önler. Güç kaynağı, bilgisayarın tüm bileşenlerine gerekli elektriği güvenli biçimde sağlayan birimdir. Seçim yapılırken toplam güç kapasitesinin (Watt) sistemin ihtiyacını karşılaması, farklı bileşenler için gerekli voltaj hatlarını (+3,3 V, +5 V, +12 V gibi) sunması ve enerji verimliliğini gösteren **80 PLUS** sertifikasına sahip olması önemlidir. Anakart, işlemci, ekran kartı ve depolama birimlerine uygun konnektörleri (24 pin, 4+4 pin CPU, PCIe, SATA vb.) desteklemesi, sistemin sorunsuz çalışmasına katkı sağlar.

BİLGİ KUTUSU : Güç Kaynağı Kalitesinin Önemi

Düşük kaliteli güç kaynakları, voltaj dalgalanmalarına karşı yeterli koruma sağlayamayabilir. Bu durum; işlemci, bellek, depolama birimi gibi hassas bileşenlerin zarar görmesine yol açabilir. Güç kaynağı, sistemin en az dikkat çeken ama en kritik bileşenlerinden biridir.

SİBER GÜVENLİK PENCERESİ

Donanım güvenliği yalnızca yazılım güncellemeleriyle sağlanamaz. Fiziksel bileşenlerin güvenli yapılandırılması da kritik öneme sahiptir.

Güç Kaynağı Kalitesi: Voltaj dalgalanmaları yalnızca donanım arızasına değil veri bozulmalarına da yol açabilir. Bozulan veri bazı durumlarda sistem güvenliğini tehdit eden hatalara zemin hazırlar.

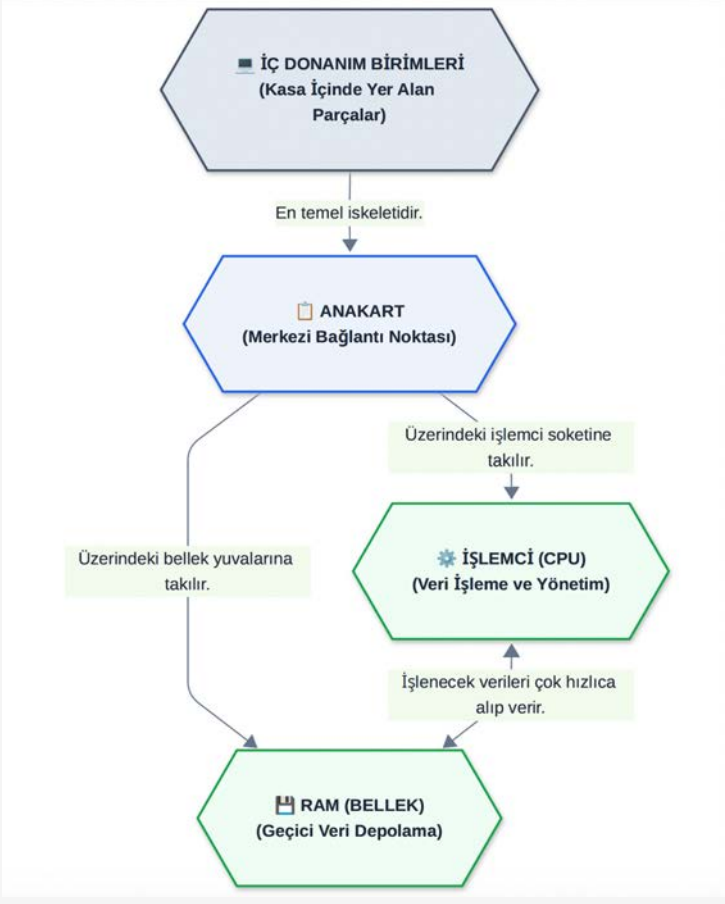
Yetkisiz Donanım Erişimi: Kasanın fiziksel olarak güvensiz bir ortamda bırakılması, kötü niyetli kişilerin bellek modülü, depolama birimi gibi bileşenlere doğrudan erişmesine olanak tanır. Bu durum veri çalınmasına veya zararlı donanım eklenmesine yol açabilir.

Eski ve Desteksiz Donanım: Güvenlik yamalarını desteklemeyen eski bileşenler sistemi savunmasız bırakabilir.

Fiziksel güvenlik, siber güvenliğin temelidir. Yazılım ne kadar güçlü olursa olsun, donanıma fiziksel erişim sağlanmışsa sistem güvende değildir.

2. ETKİNLİK

Etkinlik Adı	İç Donanım Birimleri Kavram Haritası
Süre	Araştırma (ders dışı) - Bir hafta
Amaç	Bir bilgisayarın iç donanım birimlerini (CPU, RAM, GPU, anakart, güç kaynağı, depolama birimi, soğutucu vb.) araştırarak her birimin görevini diğer birimlerle olan fiziksel, işlevsel bağlantılarını ve temel özelliklerini açıklamak
Yönerge	Aşağıda **iç donanım birimleri** kavram haritasının bir bölümü verilmiştir. Bu harita yalnızca üç adet bileşeni kapsamakta ve tüm alanları doldurulmuş olarak sunulmaktadır. Haritayı dikkatle inceleyiniz.



Bu haritada diğer iç donanım birimleri ve yapısındaki bileşenleri yer almıyor. Göreviniz, bunları ve bulduğunuz diğer bileşenleri ekleyerek haritayı tamamlamaktır.

Yönerge Adımları	
1	**Örnek Haritanın İncelenmesi ve Eksiklerin Listelenmesi** Önceki sayfadaki örnek haritayı dikkatlice okuyunuz. Hangi bileşenlerin eksik olduğunu tespit ederek aşağıya yazınız. . . . .
2	**Her Eksik Bileşenin Araştırılması** Güvenilir kaynaklardan (ders kitabı, MEB kaynakları, TDK Bilim ve Sanat Terimleri Sözlüğü vb.) şu soruların cevabını bulunuz: Bileşenin görevi nedir, hangi bileşenle nasıl bağlanır, yapısında neler vardır, en önemli teknik özelliği (hız, kapasite, voltaj vb.) nedir ve HDD ile SSD arasındaki farklar nelerdir?
3	**Kavram Haritasının Oluşturulması** Örnek haritayı temel alınız ve araştırdığınız bileşenleri bu haritaya ekleyiniz. Haritanızda en az yedi adet bileşen, her bileşenin görevi, bağlantı tipi ve bir teknik özelliği yer almalıdır. İster dijital ortamda ister karton üzerinde kavram haritasını hazırlayınız.
4	**Kaynakların Not Alınması** Kullandığınız en az iki adet kaynağı (kitap adı, web sitesi adresi vb.) aşağıya yazınız. . . . .
5	**Sunumun Hazırlanması** Kavram haritanızı sınıfa tanıtınız. **Bir bileşeni kaldırsaydık bilgisayara ne olurdu ve hangi bileşen veya bileşenler olmasaydı bilgisayar çalışmazdı** sorularına cevap veriniz.

⚠ **Dikkat:** Kavram haritası bir liste değil bileşenler arasındaki iletişim, güç ve uyumluluk ilişkilerini görsel olarak ortaya koyan bir düşünce haritasıdır. Bağlantı etiketleri (hangi yuva, hangi konnektör vb.) ne kadar teknik olursa haritanın değeri o kadar artar.

Değerlendirme

Çalışmanız öğretmeniniz tarafından analitik dereceli puanlama anahtarına göre değerlendirilecektir. Çalışmanızı yaparken buradaki ölçütleri dikkate alınız. Analitik dereceli puanlama anahtarı formuna ulaşmak için karekodu okutunuz. Dijital yayınlarda karekodun üstüne tıklayarak içeriğe ulaşabilirsiniz.

1.1.11. Kuantum Bilgisayarlar



Görsel 1.40: Kuantum bilgisayar

Kuantum bilgisayar, klasik bilgisayarların temel aldığı ikili (0 ve 1) mantık yerine kuantum fiziğinin ilkelerinden yararlanarak hesaplama yapan yeni nesil bir bilgisayar türüdür (Görsel 1.40). Klasik bilgisayarlarda bilginin en küçük birimi olan bit yalnızca 0 veya 1 değerini alabilirken kuantum bilgisayarlarda bu rolü üstlenen **qubit (kuantum biti)** ölçüm yapılmadan önce olasılıksal bir yapıda bulunur.

Qubitleri farklı kılan üç temel kuantum özelliği vardır.

1. **Süperpozisyon (Superposition):** Qubit, ölçüm yapılmadan önce 0 ve 1 durumlarını olasılıklar hâlinde birlikte temsil edebilir. Bu özellik, bazı problemler için çok sayıda olasılığın aynı anda değerlendirilebilmesine imkân tanır.
2. **Dolanıklık (Entanglement):** İki qubit dolanık hâle geldiğinde ölçüm sonuçları birbirine bağlıdır. Biri ölçüldüğünde diğerinin sonucu da bu ilişkiye göre belirlenir.
3. **Girişim (Interference)**: Kuantum algoritmalarında bazı olasılıkların etkisi azalırken bazıları güçlenir. Böylece ölçüm sonunda istenen sonucun elde edilme olasılığı artırılabilir.

Kuantum hesaplamada qubit sayısı arttıkça teorik olarak temsil edilebilen olası durum sayısı çok hızlı büyür. Bu nedenle kuantum bilgisayarlar; kriptografi, ilaç geliştirme, optimizasyon, simülasyon, yapay zekâ gibi alanlarda bazı özel problem türleri için yüksek potansiyel taşır.

BİLGİ KUTUSU : Qubit Sayısının Gücü

n adet qubit, ölçüm yapılmadan önce 2^n olası durumu temsil edebilir. Örneğin 10 qubit 1.024 olası durumu ifade edebilir. Qubit sayısı büyüdükçe bu sayı çok hızlı artar. Bu nedenle klasik bir bilgisayarın olası durumları sırayla denemesi gereken bazı problem türlerinde kuantum yaklaşımı önemli bir avantaj sağlar.

Kuantum bilgisayarlar henüz klasik bilgisayarların yerini alacak olgunluğa ulaşmamıştır. Qubitler çevresel etkilerden kolayca etkilenebildiği için hata oranı yüksektir ve birçok kuantum sisteminin çalışması için çok düşük sıcaklıkların sağlanması gerekir. Bu nedenle bugün kuantum bilgisayarlar çoğunlukla laboratuvar ortamlarında geliştirilmekte, bazıları ise bulut tabanlı sistemler üzerinden araştırmacıların kullanımına sunulmaktadır. Kuantum bilgisayarlar, klasik bilgisayarların **yerine geçen** değil belirli problem türlerinde onları **tamamlayan** sistemler olarak görülmektedir. Bu nedenle metin yazma, e-posta gönderme, video oynatma gibi günlük işler için klasik bilgisayarlar daha yeterli ve pratiktir. Kuantum bilgisayarlar ise özellikle bazı optimizasyon, simülasyon ve kriptografi problemlerinde avantaj sunar.

SİBER GÜVENLİK PENCERESİ

Mevcut internet altyapısının önemli bir bölümü, RSA, ECC gibi açık anahtarlı şifreleme sistemlerine dayanır. Yeterince güçlü ve hata oranı düşük bir kuantum bilgisayar, **Shor** algoritmasıyla bu tür şifreleme yöntemleri için geleceğe dönük bir risk oluşturabilir. Bu nedenle uluslararası kuruluşlar **kuantum sonrası (post-kuantum) kriptografi** yaklaşımları üzerinde çalışmaktadır. Ulusal Standartlar ve Teknoloji Enstitüsü [National Institute of Standards and Technology (NIST)], 2024 yılında post-kuantum kriptografi için ilk standartlarını yayımlamaya başlamıştır. Bu tehdidin farkında olan uluslararası kuruluşlar şimdiden harekete geçmiştir.

3. ETKİNLİK

Etkinlik Adı	Kuantum Bilgisayarlar
Süre	Araştırma (ders dışı) - Bir hafta
Amaç	Kuantum bilgisayarlarla ilgili güncel bir makaleden edinilen bilgileri kısa bir dijital video sunumu ile açıklamak
Yönerge	Kuantum bilgisayarlar konusunda güncel bir makale bularak okuyunuz. Makaleyle ilgili aşağıdaki formu doldurunuz. Edindiğiniz bilgileri kullanarak kısa bir dijital video sunum hazırlayınız ve sınıfta arkadaşlarınızla 15 dakikalık süre içinde paylaşınız.

Makale Başlığı	
Yayın Kaynağı	
Yayın Tarihi	
Makalenin Ana Konusu	
Kısa Özeti	
Kaynak (Site Adı ve Erişim Tarihi-Saati)	

Değerlendirme

Çalışmanız öğretmeniniz tarafından analitik dereceli puanlama anahtarına göre değerlendirilecektir. Çalışmanızı yaparken buradaki ölçütleri dikkate alınız. Analitik dereceli puanlama anahtarı formuna ulaşmak için karekodu okutunuz. Dijital yayınlarda karekodun üstüne tıklayarak içeriğe ulaşabilirsiniz.

1. UYGULAMA

Uygulama Adı	İç Donanım Birimlerinin Montajı
Süre	40 dakika
Amaç	İş sağlığı ve güvenliği kurallarına uyarak iç donanım birimlerini tanıyarak bilgisayar kasasına doğru sırayla montajını yapmak
Yönerge	Öğretmeninizin yönlendirmesiyle 3-4 kişilik gruplar oluşturunuz. Öğretmeniniz montaj sürecini adım adım gösterdikten sonra grubunuzla birlikte aşağıda verilen montaj adımlarını sırasıyla izleyerek bilgisayarın iç donanım birimlerini kasaya monte ediniz. Her adımda iş bölümü yapınız, tüm grup üyelerinin sürece aktif olarak katılması gerektiğini unutmayınız. Her adımı tamamladığınızda Kontrol sütununa tik (✓) atarak işaretleyiniz.

İş Sağlığı ve Güvenliği Kuralları

Kişisel Koruyucu Donanım

- Statik elektrik kaynaklı bileşen hasarını önlemek için antistatik bileklik takınız. Bileklik yoksa çalışmaya başlamadan önce metal bir yüzeye dokunarak vücudunuzdaki statik elektriği boşaltınız.

Elektrik Güvenliği

- Montaj öncesinde güç kablosunun prize takılı olmadığını kontrol ediniz. Enerjili sistem üzerinde kesinlikle çalışmayınız.

Donanım Güvenliği

- Bileşenleri yalnızca kenarlarından tutunuz. Devre yüzeylerine ve pin bölgelerine dokunmayınız.
- Bileşenleri yuvalarına takmak için zorlamayınız. Hizalama işaretlerini kontrol ediniz. Bileşenlere aşırı kuvvet uygulanması, pin kırılmasına veya yuva hasarına yol açabilir.
- Vidaları aşırı sıkmayınız. Sıkılması durumunda devre kartı veya yuva zarar görebilir.

Kimyasal Madde Güvenliği

- Termal macunun cilt ve gözle temasından kaçınınız. Uygulamadan sonra ellerinizi yıkayınız.

Çalışma Alanı Düzeni

- Çalışma yüzeyini temiz ve düzenli tutunuz. Küçük vidalar ve bileşenler için düzenli bir alan oluşturunuz.
- Keskin kenarlı bileşenleri dikkatli tutunuz. Yaralanmalara karşı dikkatli olunuz.

1	Kasayı çalışma alanına yerleştirip yan kapağı açınız ve kasanın iç yapısını inceleyiniz.	☐ Tamamlandı
2	Anakart koruyucularını (standoff) kasaya sabitleyiniz. Anakartı vida deliklerini hizalayarak kasaya yerleştiriniz ve vidayla sabitleyiniz.	☐ Tamamlandı
3	İşlemciyi anakart üzerindeki sokete yön işaretlerine dikkat ederek, yerleştirip sabitleme mandalını kapatınız.	☐ Tamamlandı
4	Termal macunu işlemcinin üzerine ince bir tabaka hâlinde uygulayıp, işlemci soğutucusunu takınız ve anakarta fanı bağlayınız.	☐ Tamamlandı
5	RAM modüllerini anakart üzerindeki uygun yuvalara yerleştiriniz. Kilitler kapanana kadar bastırınız.	☐ Tamamlandı
6	Depolama birimini türüne uygun (HDD veya SSD) yuvaya yerleştirip, sabitleyerek SATA veri kablosunu bağlayınız.	☐ Tamamlandı
7	Güç kaynağını kasaya yerleştiriniz ve vidayla sabitleyiniz.	☐ Tamamlandı
8	24-pin anakart, CPU ve depolama birimi güç konnektörlerini bağlayınız.	☐ Tamamlandı
9	Ön panel konnektörlerini (güç düğmesi, reset ve LED) anakart üzerindeki ilgili pinlere bağlayınız.	☐ Tamamlandı
10	Tüm kablo bağlantılarını kontrol edip gevşek veya bağlanmamış kablo olmadığını doğrulayınız.	☐ Tamamlandı
11	Kasanın yan kapağını kapatınız.	☐ Tamamlandı

Değerlendirme

Çalışmanız öğretmeniniz tarafından kontrol listesine göre değerlendirilecektir. Çalışmanızı yaparken buradaki ölçütleri dikkate alınız. Kontrol listesi formuna ulaşmak için karekodu okutunuz. Dijital yayınlarda karekodun üstüne tıklayarak içeriğe ulaşabilirsiniz.

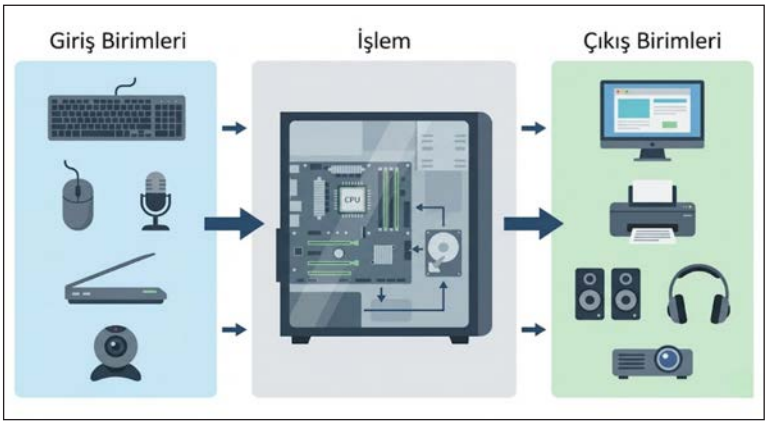
Çalışmanızı tamamladıktan sonra grup değerlendirme formunu doldurarak grup üyelerinin çalışmaya katkı düzeylerini değerlendiriniz. Grup değerlendirme formuna ulaşmak için karekodu okutunuz. Dijital yayınlarda karekodun üstüne tıklayarak içeriğe ulaşabilirsiniz.

Çalışmanızın öğrenme sürecinize katkısını değerlendirmek için öz değerlendirme formunu doldurunuz. Formu tamamladıktan sonra öğretmeninizle paylaşınız veya EBA Portfolyo'ya yükleyiniz. Öz değerlendirme formuna ulaşmak için karekodu okutunuz. Dijital yayınlarda karekodun üstüne tıklayarak içeriğe ulaşabilirsiniz.

1.2. DIŞ DONANIM BİRİMLERİ

Bilgisayar kasasının dışında bulunan veya bilgisayara dışarıdan bağlanan, kullanıcının bilgisayara veri girmesini ve bilgisayardan çıkan sonuçları almasını sağlayan aygıtlara **dış donanım birimleri** denir. Bu birimler, bilgisayar ile kullanıcı arasındaki etkileşimi kurar. Klavye, fare, mikrofon gibi giriş aygıtlarıyla sisteme veri ve komut gönderilir. Monitör, yazıcı, hoparlör gibi çıkış aygıtlarıyla da üretilen çıktılar kullanıcıya sunulur. Bilgisayarın çalışma mantığı, bu **giriş-işlem-çıkış** akışıyla açıklanabilir (Görsel 1.41). Bu akış şöyle gerçekleşir:

- Giriş aygıtlarıyla bilgisayara veri aktarılır.
- İç donanım birimleri bu veriyi işler (Örneğin işlemci, RAM'in desteğiyle veriyi işleyip gerektiğinde depolama birimlerine kaydeder.).
- Ortaya çıkan sonuç, çıkış aygıtlarıyla kullanıcıya iletilir.



Görsel 1.41: Bilgisayarda giriş-işlem-çıkış akışı

Dış donanım birimlerinin doğru çalışması için uygun bağlantı noktalarının seçilmesi, kablolu veya kablosuz bağlantıların doğru yapılması ve temel ayarların kontrol edilmesi önemlidir. Tanınmayan aygıtların bilgisayara bağlanması, kişisel veriler ve cihaz güvenliği açısından risk oluşturabileceğinden dikkatli olunmalıdır.

1.2.1. Giriş Aygıtları

Bilgisayarın işlemcisi ne kadar güçlü olursa olsun, dış dünyadan veri almadığı sürece hiçbir işlem yapamaz. Tıpkı insanların çevreyi algılamak için duyu organlarına ihtiyaç duyması gibi bilgisayarlar da kullanıcıdan veri ve komut almak için **giriş aygıtları**na gereksinim duyar. Bu aygıtlar; klavyeye basılan tuşları, fareyi hareket ettirirken verilen yön bilgisini, mikrofona konuşulan sesi veya tarayıcıya yerleştirilen belgedeki görüntüyü bilgisayarın işleyebileceği dijital sinyallere dönüştüren donanımlardır (Görsel 1.42) ve USB portları üzerinden kablolu veya Bluetooth ve Wi-Fi teknolojileriyle kablosuz olarak bilgisayara bağlanır.



Görsel 1.42: Kullanımı yaygın giriş aygıtları

Klavye: Bilgisayara metin, rakam ve komut girilmesini sağlayan temel giriş aygıtıdır. Bağlantı türüne göre kablolu (USB ya da PS/2) veya kablosuz çeşitleri bulunur.

Fare (Mouse): Ekrandaki imleci yönlendirerek seçme, tıklama, sürükleme ve kaydırma işlemlerini gerçekleştiren optik veya lazer sensörlü, kablolu ve kablosuz modelleri bulunan giriş aygıtıdır.

Dokunmatik Yüzey (Touchpad): Dizüstü bilgisayarlarda farenin işlevini üstlenen ve parmak hareketleriyle imleci yönlendirmeyi sağlayan giriş yüzeyidir.

Mikrofon: Ses dalgalarını dijital veriye dönüştüren, çevrimiçi iletişim, oyun ve sesli komut uygulamalarında kullanılan giriş aygıtıdır.

Web Kamerası (Webcam): Canlı görüntü ve fotoğraf aktarımı yapan, uzaktan eğitim, video konferans ve içerik yayıncılığında yaygın olarak kullanılan giriş aygıtıdır.

Tarayıcı (Scanner): Kâğıt üzerindeki yazı, fotoğraf veya belgeleri optik olarak okuyarak dijital dosyaya (PDF, JPEG vb.) dönüştüren giriş aygıtıdır.

Grafik Tablet ve Dijital Kalem: Dijital çizim yapmak, tasarım oluşturmak veya ekranda el yazısı kullanmak için tasarımcılar ve dijital sanatçılar tarafından kullanılan hassas giriş yüzeyidir.

Oyun Kumandası (Gamepad/Joystick): Video oyunlarında karakterleri, araçları ve kamerayı ergonomik biçimde kontrol etmek için tasarlanmış, kablolu veya kablosuz modelleri bulunan giriş aygıtıdır.

Barkod ve Karekod (QR) Okuyucu: Çizgisel barkod ve karekodları okuyarak içerdiği veriyi sisteme ileten; market, kargo ve depo yönetiminde kullanılan giriş aygıtıdır.

SİBER GÜVENLİK PENCERESİ

Parmak izi okuyucular, yüz tanıma kameraları, retina tarayıcılar gibi biyometrik okuyucular kişiye ait fiziksel özellikleri kullanarak kimlik doğrulama yapan özel giriş aygıtlarıdır. Günümüzde bu yöntemler yalnızca yüksek güvenlikli alanlarda değil bilgisayarlar, tabletler, akıllı telefonlar gibi günlük kullanılan cihazlarda da oturum açma ve erişim kontrolü amacıyla kullanılmaktadır.

Türkiye'de 6698 sayılı KVKK (Kişisel Verilerin Korunması Kanunu) kapsamında biyometrik veriler, özel nitelikli kişisel veri olarak kabul edilir ve işlenmesinde daha yüksek güvenlik önlemleri gerektirir. Şifre değiştirilebilir ancak parmak izi ya da yüz verisi değiştirilemez. Bu nedenle biyometrik verilerin amaç dışı kullanılmaması ve yetkisiz erişime karşı korunması, siber güvenlik açısından kritik bir konudur.

BİLGİ KUTUSU : Giriş Aygıtlarının Gelişimi

İlk dönem kişisel bilgisayarlarda kullanıcılar bilgisayara komutları çoğunlukla klavye aracılığıyla giriyordu. Grafik arayüzlerin yaygınlaşmasıyla fare kullanımı da önem kazandı ve kullanıcılar ekrandaki simgeleri, menüleri ve pencereleri daha kolay yönetmeye başladı. Zamanla mikrofon, web kamerası, tarayıcı, barkod / karekod okuyucu, grafik tablet gibi farklı giriş aygıtları yaygınlaştı. Böylece bilgisayara yalnızca metin ve komut değil ses, görüntü, belge, çizim, kodlanmış bilgi gibi farklı veri türleri de aktarılabilir hâle geldi.

SIRA SİZDE

Aşağıdaki senaryolarda kişilerin mesleklerini ve amaçlarını okuyunuz. Hangi giriş aygıtına ihtiyaç duyacaklarını yazınız. Ardından cevaplarınızı sınıfta paylaşınız.

Kullanıcı ve Senaryo	Gerekli Giriş Aygıtı
Zeynep (İllüstratör) Dijital ortamda çizgi roman karakterleri tasarlamaktadır. Çizgilerini bilgisayarda yapacak ve her fırça darbesindeki basıncı hassas biçimde ayarlamak istemektedir.	
Ahmet (Depo Görevlisi) Büyük bir marketin deposunda yüzlerce ürünün stok girişini hızla sisteme kaydetmekle görevlidir. Ürünlerin ambalajında numaralar yerine optik kodlar bulunmaktadır.	
Selin (Siber Güvenlik Uzmanı) Çok gizli verilerin bulunduğu bir siber güvenlik şirketinin sistem odasına giriş yapacaktır. Sistemin onu şifre sormaksızın ve hatasız biçimde tanıması gerekmektedir.	
Can (E-Spor Oyuncusu) Arkadaşlarıyla internet üzerinden çok oyunculu bir yarış turnuvasına katılacaktır. Klavyeyle araç kontrolünün yeterince ergonomik olmadığını düşünmektedir.	

1.2.2. Çıkış Aygıtları

Bilgisayar bir işlemi tamamladığında sonucun kullanıcıya ulaşması gerekir. Bu aktarımı sağlayan donanımlara **çıkış aygıtları** denir (Görsel 1.43). Monitörde beliren görüntü, hoparlörden yükselen ses veya yazıcıdan çıkan belge; hepsi bilgisayarın ürettiği sonucun farklı biçimlerdeki yansımasıdır.



Görsel 1.43: Kullanımı yaygın çıkış aygıtları

Monitör

Monitör, bilgisayarın ürettiği görüntüyü kullanıcıya sunan temel çıkış aygıtıdır. Masaüstü sistemlerde bağımsız bir ekran olarak kullanılırken dizüstü bilgisayarlarda gövdeye entegre edilmiştir. HDMI, DisplayPort veya USB-C bağlantılarıyla bilgisayara bağlanır. Monitörün görüntü kalitesini belirleyen başlıca özellikler; çözünürlük, yenileme hızı ve panel teknolojisidir.

Monitör türleri panel teknolojisine göre farklılık gösterir.

LCD [Liquid Crystal Display (Sıvı Kristal Ekran)] / LED [Light Emitting Diode (Işık Yayan Diyot)]: Sıvı kristal teknolojisine dayanan ve arka aydınlatma için LED kullanan monitörlerdir. Düşük enerji tüketimi ve uzun ömrüyle yaygın kullanım alanı bulur.

IPS [In-Plane Switching (Düzlem İçi Anahtarlama)]: Geniş görüş açısı ve doğru renk üretimiyle grafik tasarım, fotoğraf-video düzenleme gibi renk hassasiyeti gerektiren işlerde tercih edilen LCD panel türüdür.

OLED [Organic Light Emitting Diode (Organik Işık Yayan Diyot)]/AMOLED [Active Matrix OLED (Aktif Matrisli OLED)]: Her pikselin kendi ışığını ürettiği gerçek siyah, yüksek kontrast, canlı renkler sunan ve akıllı telefon, tablet veya üst segment ekranlarda yaygın olarak kullanılan teknolojidir.

Mini LED: LCD/LED teknolojisinin geliştirilmiş bir versiyonudur. Arka aydınlatmada çok sayıda küçük LED kullanarak daha hassas parlaklık kontrolü ve yüksek kontrast sağlar.

E-ink (Elektronik Mürekkep): Elektrik yüküyle yeniden düzenlenen parçacıklardan görüntü oluşturan ve ışık yaymayan, düşük enerji tüketen, e-kitap okuyucularda yaygın olarak kullanılan panel teknolojisidir.

Projeksiyon

Projeksiyon (projektör), bilgisayardan gelen görüntüyü büyüterek beyaz perde veya düz bir yüzeye yansıtan çıkış aygıtıdır. Sunum, eğitim ve sinema ortamlarında geniş kitlelere görüntü aktarımı için kullanılır. HDMI bağlantısıyla kablolu, Wi-Fi veya Miracast ile kablosuz bağlanabilir. Projeksiyon türleri yansıtma teknolojisine göre farklılık gösterir.

DLP: Küçük aynalardan oluşan bir çip aracılığıyla görüntü oluşturan taşınabilir projeksiyonlarda yaygın olarak kullanılan teknolojidir.

LCD: Işığı sıvı kristal panellerden geçirerek parlak ve renkli görüntüler üreten, sınıf ve toplantı ortamlarında tercih edilen teknolojidir.

Lazer: Işık kaynağı olarak lazeri kullanan, yüksek parlaklığı ve uzun ömrüyle büyük salon ve sinema ortamlarında tercih edilen teknolojidir.

Yazıcı

Yazıcı (Printer), bilgisayardaki dijital belge, görsel veya tasarımı fiziksel ortama aktaran çıkış aygıtıdır. Kullanım amacına ve baskı teknolojisine göre farklı türleri bulunur. Yazıcı türleri baskı teknolojisine göre ayrılır.

Mürekkep Püskürtmeli: Kâğıda küçük mürekkep damlacıkları püskürterek baskı yapar. Renkli baskılarda uygun maliyetiyle ev ve küçük ofis kullanımında yaygındır. Fotoğraf kalitesinde çıktı üretilebilir.

Lazer: Toner adı verilen toz boyayı ısıyla kâğıda yapıştırarak baskı yapar. Hızlı ve yüksek hacimli baskı gerektiren ofis ortamlarında tercih edilir. Siyah beyaz ve renkli modelleri bulunur.

Termal: Isıya duyarlı özel kâğıda baskı yapar. Mürekkep veya toner kullanmaz. Market fişleri, kargo etiketleri, bilet baskısı gibi alanlarda kullanılır.

3D Yazıcı: Dijital tasarım dosyasından katman katman malzeme ekleyerek üç boyutlu nesne üretir. Plastik, reçine, metal gibi farklı malzemeler kullanılabilir. Prototip geliştirme, tıbbi implant üretimi, mimari maket yapımı ve eğitim alanlarında giderek yaygınlaşmaktadır.

Hoparlör ve Kulaklık

Hoparlör ve kulaklık, bilgisayarın ürettiği dijital ses sinyalini analog sese dönüştürerek kullanıcıya ileten çıkış aygıtlarıdır. Ses kartından veya anakart üzerindeki ses çıkışından beslenir. İkisi arasındaki temel fark kullanım biçimidir.

Hoparlör: Bilgisayarın ürettiği dijital ses sinyalini analog sese dönüştürerek çevreye yayan ve stereo, subwoofer destekli veya çok kanallı modelleri bulunan çıkış aygıtıdır.

Kulaklık: Sesi yalnızca kullananın duymasını sağlayan, kablolu ve kablosuz (Bluetooth) modelleri bulunan çıkış aygıtıdır.

SIRA SİZDE

Aşağıdaki senaryolarda kişilerin mesleklerini ve amaçlarını okuyunuz. Hangi çıkış aygıtına ihtiyaç duyacaklarını yazınız. Ardından cevaplarınızı sınıfta paylaşınız.

Kullanıcı ve Senaryo	Gerekli Çıkış Aygıtı
Emre (Mühendislik Öğrencisi) Tasarladığı köprü modelinin üç boyutlu fiziksel bir kopyasını elde etmek istiyor. Bilgisayarda çizdiği tasarımı elle tutulur bir nesneye dönüştürmesi gerekiyor.	
Ayşe (Öğretmen) 50 kişilik bir sınıfa sunum yapacak. Herkesin ekranı net görebilmesi için görüntünün büyük bir yüzeye yansıtılması gerekiyor.	
Kerem (Grafik Tasarımcı) Müşterisine teslim edeceği logo tasarımını yüksek kalitede kâğıda bastırmak istiyor. Renk doğruluğu ve çözünürlük önceliği var.	
Miray (E-Spor Oyuncusu) Gece geç saatlerde oyun oynuyor, aynı odada uyuyan kardeşini rahatsız etmek istemiyor ancak oyunun seslerini duymak istiyor.	

1.2.3. Giriş-Çıkış Aygıtları

Bazı aygıtlar yalnızca veri almaz veya yalnızca veri vermez, her iki işlevi de aynı anda yerine getirir. Bu tür aygıtlar **giriş-çıkış aygıtları** olarak adlandırılır (Görsel 1.44). Bu aygıtlar, giderek yaygınlaşmaktadır. Bilgisayar, tablet ve akıllı telefon kullanımının yanı sıra eğitim, sağlık ve eğlence alanlarında da önemli bir yer edinmektedir.



Görsel 1.44: Giriş-çıkış aygıtları

Dokunmatik Ekran (Touchscreen): Parmak dokunuşlarını algılayarak sisteme ileten ve aynı anda işlenmiş görüntüyü kullanıcıya sunan ve tablet, akıllı telefon ve bazı dizüstü bilgisayarlarda kullanılan giriş-çıkış aygıtıdır.

Giriş İşlevi: Parmak dokunuşu ve hareketleri sisteme iletilir.

Çıkış İşlevi: İşlenmiş görüntü kullanıcıya sunulur.

Kulaklık-Mikrofon (Headset): Mikrofon aracılığıyla sesi sisteme iletirken kulaklık bölümüyle ses çıktısını kullanıcıya aktaran ve oyun, çevrimiçi toplantı ve uzaktan eğitimde tercih edilen giriş-çıkış aygıtıdır. Kablolu ve kablosuz modelleri mevcuttur.

Giriş İşlevi: Mikrofon sesi sisteme gönderir.

Çıkış İşlevi: Kulaklık ses çıktısını kullanıcıya iletir.

İnteraktif Tahta (Akıllı Tahta): Dokunmatik yüzeyi aracılığıyla komut alırken entegre ekran veya projeksiyon ile görüntü sunan ve tahtanın, projeksiyon cihazının ve bilgisayarın işlevlerini tek sistemde birleştiren giriş-çıkış aygıtıdır.

Giriş İşlevi: Dokunma ve kalem hareketleri sisteme aktarılır.

Çıkış İşlevi: Bilgisayar görüntüsü büyük yüzeyde gösterilir.

VR Gözlük (Sanal Gerçeklik Gözlüğü): Kafa hareketi, konum ve kontrolcü verilerini sisteme iletirken her iki göze ayrı görüntü göndererek kullanıcıyı üç boyutlu dijital ortama taşıyan giriş-çıkış aygıtıdır. Oyun ve eğlence alanlarının yanı sıra mimarlık, tıp eğitimi, askerî simülasyon, uzaktan eğitim gibi alanlarda da kullanılır.

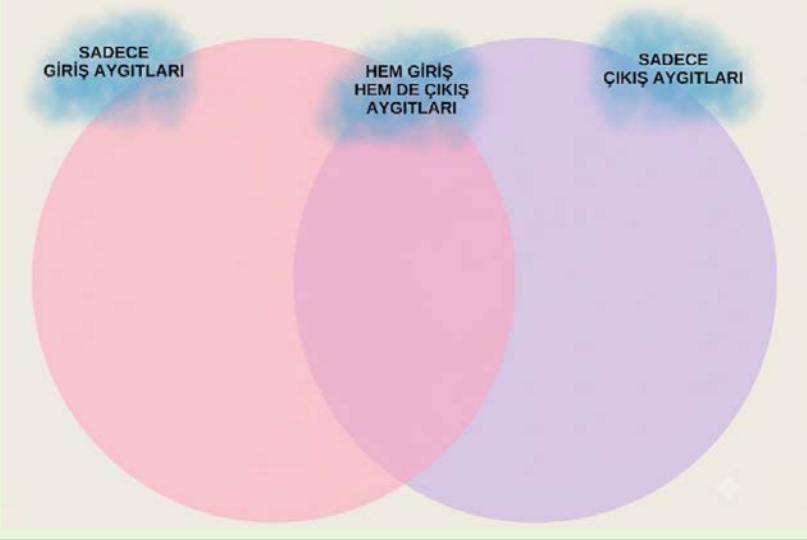
Giriş İşlevi: Kafa hareketi, konum ve kontrolcü verileri sisteme iletilir.

Çıkış İşlevi: Her göze ayrı görüntü gönderilerek sanal ortam oluşturulur.

SIRA SİZDE

Aşağıda verilen aygıt listesini inceleyiniz. Yalnızca giriş işlevi gören aygıtları sol daireye, yalnızca çıkış işlevi gören aygıtları sağ daireye, her ikisini birden yapanları ise ortadaki kesişim alanına yazınız.

Aygıt Listesi				
Monitör	Klavye	Akıllı Tahta	Hoparlör	Tarayıcı
Dokunmatik Ekran	Fare	Yazıcı	Mikrofon	Kulaklık-Mikrofon
Projeksiyon	Oyun Kumandası	Grafik Tablet	VR Gözlük	Web Kamerası



2. UYGULAMA

Uygulama Adı	Dış Donanım Birimlerinin Montajı
Süre	40 dakika
Amaç	İş sağlığı ve güvenliği kurallarına uyarak dış donanım birimlerini bilgisayara doğru bağlantı noktalarından bağlamak
Yönerge	Öğretmeninizin yönlendirmesiyle 3-4 kişilik gruplar oluşturunuz. Öğretmeniniz montaj sürecini adım adım gösterdikten sonra grubunuzla birlikte aşağıda verilen montaj adımlarını sırasıyla izleyerek bilgisayarın dış donanım birimlerini kasaya bağlayınız. Her adımda iş bölümü yapınız, tüm grup üyelerinin sürece aktif olarak katılması gerektiğini unutmayınız. Her adımı tamamladığınızda Kontrol sütununa tik (✓) atarak işaretleyiniz.

İş Sağlığı ve Güvenliği Kuralları

Elektrik Güvenliği

- Tüm bağlantıları tamamlamadan önce bilgisayarın güç kablosunun prizden çıkarılmış olduğundan emin olunuz.
- Güç kablosunu yalnızca tüm bağlantılar tamamlandıktan sonra takınız.

Donanım Güvenliği

- Konektörleri yuvalarına zorlamayınız, doğru yön ve eşleşmeyi kontrol ediniz. Yanlış yönde uygulanan kuvvet pin kırılmasına veya port hasarına yol açar.
- USB, HDMI, ses jakı gibi konektörleri yanlış yuvaya takmamaya dikkat ediniz. Renk ve şekil kodlarını kontrol ediniz.
- Kabloları çekerken konektörden tutunuz. Kablo gövdesinden çekmeyiniz.

Çalışma Alanı Düzeni

- Çalışma yüzeyini temiz ve düzenli tutunuz. Kablolar zemine dağıtılmamalıdır.
- Kablolar üzerinde yürümeyiniz. Takılma ve düşme riskine karşı dikkatli olunuz.

Montaj Adımları

Adım	Yapılacak İşlem	Kontrol
1	Monitörü bağlayınız. Monitörün sinyal kablosunu (HDMI veya DisplayPort) bilgisayarın ilgili görüntü çıkışına bağlayınız. Konnektörün yerine oturduğunu kontrol ediniz. Ardından monitörün güç kablosunu prize takınız.	☐ Tamamlandı
2	Klavyeyi bağlayınız. Klavyenin USB konnektörünü bilgisayarın USB portuna bağlayınız. Kablosuz klavye kullanıyorsanız alıcıyı USB portuna takınız.	☐ Tamamlandı

3	Fareyi bağlayınız. Farenin USB konnektörünü boş bir USB portuna bağlayınız. Kablosuz fare kullanıyorsanız alıcıyı farklı bir USB portuna takınız.	☐ Tamamlandı
4	Hoparlör veya kulaklığı bağlayınız. Hoparlör veya kulaklığın 3,5 mm jaklı kablosunu bilgisayarın ses çıkış portuna (genellikle yeşil renkli) bağlayınız. USB hoparlör kullanıyorsanız USB portunu tercih ediniz.	☐ Tamamlandı
5	Web kamerasını bağlayınız. Web kamerasının USB kablosunu bilgisayardaki boş bir USB portuna bağlayınız. Sistem sürücüyü otomatik olarak tanıyacaktır.	☐ Tamamlandı
6	Yazıcıyı bağlayınız. Yazıcının USB kablosunu bilgisayara bağlayınız. Yazıcının güç kablosunu prize takınız ve yazıcıyı açınız. Gerekirse sürücü kurulumunu tamamlayınız.	☐ Tamamlandı
7	Ağ kablosunu bağlayınız. RJ-45 konektörlü ağ kablosunu bilgisayarın Ethernet portuna bağlayınız. Kablosuz bağlantı kullanıyorsanız bu adımı atlayabilirsiniz.	☐ Tamamlandı
8	Güç kablosunu takınız ve sistemi açınız. Tüm bağlantılar tamamlandıktan sonra bilgisayarın güç kablosunu takınız. Sistemi açınız ve her aygıtın işletim sistemi tarafından tanınıp tanınmadığını kontrol ediniz.	☐ Tamamlandı

Değerlendirme

Çalışmanız öğretmeniniz tarafından kontrol listesine göre değerlendirilecektir. Çalışmanızı yaparken buradaki ölçütleri dikkate alınız. Kontrol listesi formuna ulaşmak için karekodu okutunuz. Dijital yayınlarda karekodun üstüne tıklayarak içeriğe ulaşabilirsiniz.

Çalışmanızı tamamladıktan sonra grup değerlendirme formunu doldurarak grup üyelerinin çalışmaya katkı düzeylerini değerlendiriniz. Grup değerlendirme formuna ulaşmak için karekodu okutunuz. Dijital yayınlarda karekodun üstüne tıklayarak içeriğe ulaşabilirsiniz.

Çalışmanızın öğrenme sürecinize katkısını değerlendirmek için öz değerlendirme formunu doldurunuz. Formu tamamladıktan sonra öğretmeninizle paylaşınız veya EBA Portfolyo'ya yükleyiniz. Öz değerlendirme formuna ulaşmak için karekodu okutunuz. Dijital yayınlarda karekodun üstüne tıklayarak içeriğe ulaşabilirsiniz.

1.3. ENERJİ VERİMLİ DONANIM BİRİMLERİ

Bir bilgisayarın ya da akıllı cihazın prizden veya bataryadan aldığı enerjinin tamamı doğrudan işleme (performansa) dönüşmez. Enerjinin bir kısmı sistem içinde ısı olarak açığa çıkar. Isının artması; fanların daha sık ve hızlı çalışmasına, cihazın daha gürültülü olmasına ve uzun vadede donanımın yıpranmasına yol açabilir. Bazı durumlarda sistem, aşırı ısınmayı önlemek için performansını geçici olarak düşürebilir. Bu nedenle sistem kurulurken yalnızca **en güçlü** parçaları seçmek her zaman en iyi sonucu vermez. Asıl önemli olan **kullanım amacını karşılayan ve enerjiyi daha verimli kullanan donanımları tercih edebilmektir.** Bir donanımın enerjiyi ne kadar verimli kullandığı, ürünler üzerinde yer alan verimlilik sınıfları ve etiketlerden anlaşılır.

1.3.1. Enerji Verimliliği Sınıfları ve Etiketler

Enerji verimliliği sınıfları ve etiketler, bir donanımın belirli koşullarda enerjiyi ne kadar etkili kullandığına dair kısa ve karşılaştırılabilir bilgiler sunar. Bu etiketler yalnızca **kaç Watt harcanmış** sorusunu değil harcanan enerjinin ne kadarının işe dönüştüğünü de yanıtlamaya yardımcı olur. Böylece benzer görevi yapan seçenekler arasında aynı işi daha az enerjiyle yapan ürünleri ayırt etmek kolaylaşır.

Donanım seçiminde enerji verimliliğini değerlendirirken karşılaşılan temel göstergeler ve bunların ne anlama geldiği Tablo 1.2'de özetlenmiştir.

Tablo 1.2: Donanımlarda Enerji Verimliliği Göstergeleri ve Sertifikalar

Gösterge / Sertifika	Nerede Görülür?	Ne Anlatır?
80 PLUS	Güç kaynağı (PSU)	Şebekeden alınan elektriğin ne kadarının bilgisayara aktarıldığını (verim oranını) gösterir.
TDP (Isıl Tasarım Gücü)	İşlemci (CPU), Ekran Kartı (GPU)	Donanımın tam yükte çalışırken harcadığı gücü ve dışarı atılması gereken maksimum ısı miktarını belirtir.
AB Enerji Etiketi	Monitörler, televizyonlar	Cihazların enerji verimliliğini A'dan (en yüksek verimlilik) G'ye (en düşük verimlilik) kadar harflerle sınıflandırır.
ENERGY STAR	Bilgisayarlar, monitörler, ofis cihazları	Cihazın boşta, uykuda veya çalışırken uluslararası enerji tasarrufu standartlarını karşıladığını belgeler.
EPEAT	Bilgisayarlar, monitörler, sunucular	Ürünün sadece az elektrik harcadığını değil aynı zamanda geri dönüştürülebilir, tamir edilebilir ve çevre dostu olduğunu (yaşam döngüsünü) belgeler.

KONTROL NOKTASI

Donanım seçimindeki en yaygın yanılgı, her zaman en güçlü olanın en iyisi olduğunu düşünmektir. Oysa bu yanılgının sonucu; ihtiyaç fazlası güç, israf edilen elektrik ve fazladan ısınan bir sistem demektir. Enerji etiketleri bu noktada bambaşka bir vizyon sunar. En güçlü olanı değil kullanım amacını eksiksiz karşılarken enerjiyi israf etmeyen **en verimli** donanımı seçmeye rehberlik eder.

1.3.1.1. Güç Kaynakları İçin Verimlilik

80 PLUS sertifikası, bir güç kaynağının şebekeden çektiği elektriğin ne kadarını bilgisayar bileşenlerine aktarabildiğini gösterir. Kalan kısım ısı olarak kaybolur. Sınıf ne kadar yüksekse kayıp o kadar azdır. Tablo 1.3'te 80 PLUS verimlilik sınıfları görülmektedir. 80 PLUS ölçümleri farklı yük seviyelerinde yapılır ve bu tabloda karşılaştırmayı kolaylaştırmak için %50 yük değerleri örneklenmiştir.

Tablo 1.3: 80 PLUS Verimlilik Sınıfları

Sınıf (80 PLUS)	%50 Yük Verimi	Kayıp Isı (500W'ta)	Tipik Kullanım
Standart (Beyaz)	%80	125W	Düşük bütçeli sistemler, temel bilgisayarlar
Bronze	%85	88W	Standart ev ve ofis bilgisayarları
Silver	%88	68W	Orta seviye sistemler
Gold	%90	56W	Üst düzey iş istasyonları, oyun bilgisayarları
Platinum	%92	43W	7/24 çalışan yerel sunucular
Titanium	%94	32W	Kritik sistemler, ana veri merkezleri
Ruby	%96,5	18W	Yapay zekâ (AI) ve bulut veri merkezleri
Not: Tablodaki değerler, sertifikasyonun temelini oluşturan standart 115V testlerine göredir. Türkiye'deki gibi 220V şebeke kullanan yerlerde cihazlar, şebeke geriliminin sağladığı avantajla bu tablodaki değerlerden yaklaşık %2 daha yüksek verimle çalışır.			

Örnek: Yapay zekâ (AI) modellerini eğiten büyük veri merkezlerinde yeni nesil **Ruby** veya **Titanium** güç kaynakları kullanılır. Orta ölçekli bir okul veya ofis bilgisayarı için ise **Bronze** veya **Silver** sertifikalı modeller genellikle en dengeli tercihtir.

1.3.1.2. İşlemciler İçin Verimlilik

İşlemcilerde enerji verimliliği **TDP [Thermal Design Power (Isıl Tasarım Gücü)]** değeriyle ifade edilir. TDP, işlemcinin tam yükte açığa çıkarabileceği maksimum ısı miktarını Watt cinsinden gösterir. Düşük TDP değeri, aynı işi yaparken daha az enerji harcandığı anlamına gelir (Tablo 1.4).

Tablo 1.4: İşlemci TDP Değerleri ve Kullanım Alanları

Seri	Tipik TDP	Kullanım Alanı
Düşük güç serisi	35W	Uzun süre açık kalan sistemler, enerji öncelikli ofisler
Standart seri	65W	Genel masaüstü, denge odaklı sistemler
Yüksek performans serisi	105W+	Video düzenleme, grafik tasarım, simülasyon
Dizüstü (U serisi-P serisi)	15-28W	Taşınabilir genel sistemler, pil ömrü öncelikli sistemler

Örnek: Yalnızca belge düzenleme ve e-posta için kullanılan bir okul bilgisayarı için 35W TDP'li düşük güç serisi işlemci yeterlidir. 105W'lık yüksek performans serisi, aynı amaç için gereksiz ısı ve enerji harcaması anlamına gelir.

1.3.1.3. Ekran Kartları İçin Verimlilik

Ekran kartlarında enerji verimliliği salt güç tüketimiyle değil harcanan her bir Watt elektrik başına üretilen performans (performans/Watt) ile ölçülür. Bir ekran kartının verimliliğini belirleyen en önemli faktör, üretim teknolojisidir (nanometre-nm). Üretim teknolojisi küçüldükçe (örneğin 3-4 nm seviyelerine indikçe), çip üzerindeki transistörler daha az enerjiyle daha fazla işlem yapabilir hâle gelir. Bu sayede güncel nesil bir ekran kartı, eski nesil bir karta göre daha az enerji harcayarak ve daha az ısınarak çok daha yüksek performans sunar (Tablo 1.5).

Tablo 1.5: Ekran Kartları Nesilleri ve Verimlilik Seviyeleri

Verimlilik Seviyesi	Mimari Nesli (Üretim Teknolojisi)	Ortalama Güç Tüketimi	Verimlilik Yorumu
Yüksek	Güncel Nesil (3-4 nm üretim)	100 - 150W	En yüksek performans/Watt oranını sunar. İşlem başına minimum ısı üretir.
Orta	Bir Önceki Nesil (7-8 nm üretim)	150 - 200W	Ortalama bir performans/Watt dengesine sahiptir.
Düşük	Eski Nesil (10 nm ve üzeri)	200W+	Aynı işlemi yapmak için çok daha fazla elektrik harcar ve yüksek ısı üretir.

BİLGİ KUTUSU : Ekran Kartları Artık Yalnızca Görüntü İçin Kullanılmıyor

İşlemci, genellikle az sayıda ancak güçlü çekirdeklerle birçok işi sırayla ve hızlı biçimde yürütür. Ekran kartı ise çok sayıda küçük işlem birimiyle aynı anda çok sayıda hesaplamayı yapmaya uygundur (paralel işlem). Bu özellik, ekran kartlarının bugün yalnızca oyun ve görüntü işlemede değil yapay zekâ uygulamaları, büyük veri analizleri, bilimsel hesaplamalar, bazı özel kriptografik işlemler gibi yoğun hesaplama gerektiren alanlarda da kullanılmasını sağlamıştır. Bu tür sistemlerde yüksek performans hedeflendiğinde, toplam enerji tüketiminde ekran kartlarının payı önemli ölçüde artabilir. Bu nedenle enerji verimliliği değerlendirilirken ekran kartının güç ihtiyacı da dikkate alınmalıdır.

Örnek: Yalnızca belge düzenleme için kullanılan bir okul bilgisayarına 200W tüketen eski nesil bir ekran kartı takmak gereksiz enerji harcaması ve aşırı ısınma demektir. Aynı iş için güncel nesil, 100W tüketen bir ekran kartı takılması hem daha az enerji harcaması hem de çok daha az ısı üretmesi anlamına gelir.

1.3.1.4. RAM'ler İçin Verimlilik

Belleklerde (RAM) enerji verimliliğini belirleyen en temel faktörler; donanımın nesli (DDR standardı) ve tercih edilen kapasitedir. RAM teknolojisi geliştikçe (örneğin DDR3'ten DDR5'e geçişte), veri aktarım hızı artarken çalışma voltajı (gerilim) düşer. Voltajın düşmesi, modül başına harcanan elektriğin azalması anlamına gelir (Tablo 1.6). RAM, sistem açık olduğu sürece içindeki veriyi korumak için sürekli enerji çekmek zorundadır. Bu nedenle bir sisteme ihtiyaç duyulandan daha fazla kapasitede bellek takmak, hiç kullanılmayan yongaların bile sürekli elektrik tüketmesine yol açar.

Tablo 1.6: Bellek Nesilleri ve Verimlilik

Bellek Nesli	Çalışma Voltajı	Verimlilik Yorumu
DDR3	1.5V	Eski nesildir. Hızına oranla enerji tüketimi ve ısı üretimi en yüksek olan türdür.
DDR4	1.2V	Standart kullanımdır. DDR3'e göre hem daha hızlı hem de daha verimlidir.
DDR5	1.1V	Güncel ve en yüksek verimli nesildir. Üzerinde kendi güç yönetim çipi (PMIC) bulunur.

BİLGİ KUTUSU : **Bellekler Üzerindeki Soğutucular Ne İşe Yarar?**

Eski nesil veya standart ofis belleklerinde genellikle soğutucu bulunmazdı ancak bugün yüksek hızlarda (frekanslarda) çalışan performans bellekleri ve güç yönetimini kendi üzerinde yapan yeni nesil DDR5 yongaları, işlem sırasında ciddi şekilde ısınmaktadır. Artan bu ısıyı hızla dağıtmak ve ısı kaynaklı performans kaybını (yavaşlamayı) önlemek için modern belleklerin üzerinde tıpkı işlemcilerdeki gibi alüminyum **soğutucu bloklar (heatsink)** kullanılır.

Örnek: Sadece ofis programlarının ve web tarayıcısının kullanılacağı bir kayıt bilgisayarına 64 GB kapasitesinde RAM takmak performansı artırmaz. Kapasitenin büyük bir kısmı boş kalacağı için gereksiz yere enerji tüketir. Böyle bir sistem için 8 GB veya 16 GB kapasiteli, düşük voltajla çalışan (örneğin DDR5) bir bellek seçmek en verimli yaklaşımdır.

1.3.1.5. Depolama Birimleri İçin Verimlilik

SSD'ler, HDD'lere göre çok daha az enerji tüketir. Hareketli parçası olmadığından hem daha az güç harcar hem de daha az ısınır. Bununla birlikte bir diskin verimliliği sadece anlık güç tüketimiyle değil harcadığı Watt başına ne kadar hızlı veri aktarabildiğiyle (performans/Watt) ölçülür. Depolama türü seçerken kullanım amacı ön planda tutulmalıdır (Tablo 1.7).

Tablo 1.7: Depolama Birimleri ve Verimlilik

Depolama Birimi	Aktif Güç	Verimlilik	Tipik Kullanım
NVMe PCIe SSD	~4–5W	En verimli	İşletim sistemi, yoğun kullanım
SATA SSD	~2–3W	Verimli	Genel depolama, ekonomik SSD
5400 RPM HDD	~4–6W	Orta	Büyük arşiv, seyrek erişim
7200 RPM HDD	~6–8W	Düşük	Yüksek performans gerektiren eski HDD kullanımı

Örnek: Siber güvenlik laboratuvarında işletim sistemi ve çalışma dosyaları için NVMe SSD, büyük log arşivleri için 5400 RPM HDD veya ek bir SATA SSD kullanılabilir.

1.3.1.6. Monitörler İçin Verimlilik

Monitörlerde iki yaygın sertifika sistemi kullanılır. ENERGY STAR gibi programlar, monitörlerin özellikle uykuda veya boşta düşük enerji tüketmesini ve güç yönetimi özelliklerini teşvik eder. Uykuda veya boşta tüketim değerleri, ürün türüne ve modeline göre değişebilir. AB Enerji Etiketi'nde ise A'dan G'ye harf sınıfları kullanılır (Tablo 1.8). A, en verimli sınıftır. LED panel teknolojisi, eski floresan panellere göre daha az enerji tüketir.

Tablo 1.8: Monitörlerde Enerji Sınıfları ve Yaklaşık Güç Tüketimi

Sınıf	Yaklaşık Güç Tüketimi	Tipik Kullanım
A Sınıfı	< 9 W	Güncel piyasada çok nadir bulunan ultra verimli modeller.
B Sınıfı	~9 W	En verimli yeni nesil ofis odaklı monitörler.
C Sınıfı	~12 W	Yaygın olarak tercih edilen, verimli standart ofis monitörleri.
D Sınıfı	~12 - 15 W	Denge odaklı standart ev ve genel kullanım modelleri.
E Sınıfı	~17 - 19 W	Yüksek yenileme hızına (Hz) sahip oyuncu (gaming) monitörleri.
F Sınıfı	~20 - 23 W	Daha eski nesil panellere sahip veya görece yüksek tüketimli modeller.
G Sınıfı	> 24 W	Verimliliği en düşük olan, yüksek tüketimli modeller.
Not: Bu tablo, güncel 24 inç (24") LED monitörlerin yaklaşık güç tüketim verilerini temsil etmektedir.		

Örnek: Günlük 8 saat kullanılan bir ofiste B sınıfı verimli bir monitör (yaklaşık 9W), G sınıfı bir monitöre (yaklaşık 25W) kıyasla saatte 16W daha az enerji harcar.

1 Monitörün Yıllık Tasarrufu: 16W x 8 saat x 260 iş günü = Yılda yaklaşık 33 kWh

Okul Çapında Tasarruf: İçinde 200 adet bilgisayar bulunan bir okulda G sınıfı monitörlerin B sınıfı monitörlerle değiştirilmesi, yılda toplam 6.600 kWh enerji tasarrufu sağlar.

BİLGİ KUTUSU : ENERGY STAR ve EPEAT

ENERGY STAR, ABD Çevre Koruma Ajansı [Environmental Protection Agency (EPA)] tarafından yönetilen bir enerji verimliliği sertifika programıdır. Bu sertifikayı alan ürünler, aynı kategorideki standart ürünlere kıyasla daha az enerji tüketir.

EPEAT [Electronic Product Environmental Assessment Tool (Elektronik Ürün Çevresel Değerlendirme Aracı)], bilgisayar ve çevre birimleri için çevresel sürdürülebilirlik ölçütlerini değerlendiren bir sistemdir. Bronze, silver ve gold olmak üzere üç sınıfı bulunur. Gold sınıfı en yüksek çevresel performansı temsil eder.

1.3.2. Enerji Verimliliği Yüksek Donanımların Belirlenmesi

Enerji verimliliği yüksek donanım, aynı kullanım amacını karşılarken daha az enerji tüketen ve daha az ısı üretendir. Bu donanımları belirlemek için seçim süreci ihtiyacın netleştirilmesiyle başlar. Önce bilgisayarın hangi amaçla kullanılacağı belirlenir (ev-ofis kullanımı, grafik tasarım, oyun, yazılım geliştirme, laboratuvar, atölye ortamı gibi). Daha sonra aynı işi yapabilecek seçenekler ortak ölçütlerle karşılaştırılır. Karşılaştırmada yalnızca hız, performans veya kapasite değil güç tüketimi, verimlilik bilgileri (etiketleri), çalışma sırasında oluşan ısı ve sistemin genel gereksinimleri (soğutma, güç kaynağı ihtiyacı gibi) birlikte değerlendirilir (Görsel 1.45).



Görsel 1.45: Enerji verimliliği yüksek donanım belirlenmesi aşamaları

Seçim yaparken şöyle bir kontrol listesi oluşturulabilir:

- Ürün üzerinde veya teknik bilgilerde verimlilik göstergesi (etiket veya sertifika) var mı?
- Boşta ve yük altında tüketim değerleri hakkında bilgi veriliyor mu?
- Kullanım amacına göre gereksiz güç tüketen bileşen var mı?
- Isı ve soğutma ihtiyacı (fan sayısı, gürültü vb.) yönetilebilir mi?
- Uzun süreli kullanım için kararlılık ve dayanıklılık uygun mu?

1.3.3. Performans ve Enerji Dengesi (PPW)

Bir donanımın enerji verimliliğini değerlendirirken ölçüt, harcanan her bir Watt enerji karşılığında ne kadar iş üretildiğidir. Bunun ölçümü PPW [Performance Per Watt (Watt Başına Performans)] olarak ifade edilir.

PPW = Performans Puanı / Ortalama Güç Tüketimi (W)

Yüksek PPW: Aynı enerji ile daha çok iş —> verimli donanım

Düşük PPW: Aynı iş için daha çok enerji —> verimi düşük donanım

PPW'nin günlük kullanımda neden önemli olduğunun gösterildiği Tablo 1.9'da PPW arttıkça enerji tüketimi, ısı, kullanım maliyeti gibi alanlarda nasıl avantaj sağlandığı özetlenmektedir.

Tablo 1.9: PPW'nin Kullanıma Etkileri

Etki Alanı	Açıklama
Elektrik faturası	Yüksek PPW'li donanımlar, aynı işi daha az enerjiyle yapar ve uzun vadede faturayı düşürür.
Isı ve gürültü	Verimli donanımlar daha az ısınır, fan gürültüsü ve soğutma ihtiyacı azalır.
Pil ömrü	Dizüstü bilgisayar ve tabletlerde yüksek PPW, aynı pille daha uzun kullanım anlamına gelir.
Sistem kararlılığı	Az ısınan donanımlar daha az arızalanır, 7/24 çalışan sistemlerde güvenilirlik artar.
Çevresel etki	Daha az enerji tüketimi, daha az karbon salınımı ve kaynak harcaması anlamına gelir.

PPW'ye göre sıralama yapabilmek için karşılaştırılan donanımların aynı koşullarda değerlendirilmesi gerekir çünkü farklı uygulamalar, ayarlar ve iş yükleri aynı donanımın hem performansını hem de güç tüketimini değiştirebilir. Bu nedenle önce ortak bir iş yükü seçilir. Ardından performans ve güç tüketimi bu iş yükünde ölçülerek PPW hesaplanır.

KONTROL NOKTASI

PPW karşılaştırması, aynı donanım türü içinde anlamlıdır. Örneğin bir işlemci ile bir monitörün PPW'si doğrudan karşılaştırılmaz.

Tablo 1.10'da üç farklı güç sınıfındaki işlemcinin PPW değeri hesaplanmış ve sonuçlar büyükten küçüğe doğru sıralanmıştır. En yüksek PPW'ye sahip işlemci, mutlak performansta birinci olmayabilir ancak harcanan her Watt için en fazla işi yapandır. Uzun vadede enerji ve maliyet açısından en verimli seçim olabilir.

Tablo 1.10: İşlemci PPW Karşılaştırması

Sıra	İşlemci Profili	Max TDP (W)	Performans Puanı (CPU Mark)	PPW (puan/W)
1	İşlemci C (105 W sınıfı, yüksek performans)	105	85.000	809.52
2	İşlemci B (65 W sınıfı, masaüstü)	65	44.877	690.42
3	İşlemci A (35 W sınıfı, enerji odaklı)	35	23.024	657.83
Not: PPW değeri Performans Puanı / TDP formülüyle hesaplanmıştır. Bu örnekte İşlemci C, en yüksek güç tüketen işlemci olmasına rağmen, sağladığı yüksek performans sayesinde en yüksek PPW değerine ulaşmıştır. Bu durum, PPW'nin yalnızca düşük güç tüketimiyle değil performans-enerji dengesiyle ilgili olduğunu gösterir.				

Tablo 1.11, farklı depolama teknolojilerinin tipik okuma hızı, etkin güç tüketimi ve hesaplanan PPW değerlerini göstermektedir. Yüksek PPW, depolama biriminin harcadığı her Watt enerji başına daha fazla veri aktarabildiği anlamına gelir. Tabloya göre NVMe SSD'lerin PPW değeri, HDD'lere göre yaklaşık 30-50 kat daha yüksektir.

Tablo 1.11: Depolama Birimlerinin PPW Karşılaştırması

Sıra	Depolama türü	Tipik okuma hızı (MB/sn)	Tipik etkin güç (W)	PPW (MB/sn/W)
1	NVMe SSD (PCIe 4.0 x4)	~7.000	~7	~1.000
2	NVMe SSD (PCIe 3.0 x4)	~3.500–3.900	~6	~580–650
3	SATA SSD (SATA III)	~550–600	~2,5–3	~180–240
4	HDD (7200 rpm)	~150–200	~6–9	~20–33
Not: PPW değerleri, depolama birimlerinin etkin okuma sırasındaki tipik hız ve güç tüketimine göre hesaplanmıştır. NVMe SSD'lerin yüksek PPW'si, aynı enerji ile çok daha fazla veri aktarabildiklerini gösterir ancak depolama seçiminde PPW'nin yanı sıra kapasite, maliyet, dayanıklılık ve boşta güç tüketimi de dikkate alınmalıdır.				

SİBER GÜVENLİK PENCERESİ

Siber güvenlik laboratuvarları ve sunucu sistemleri çoğu zaman günlerce, hatta aylarca kapatılamadan çalışır. Bu ortamlarda yüksek enerji tüketimi ciddi sorunlar getirir. Aşırı ısınan donanımlar daha sık arızalanır, soğutma sistemleri yoğun çalışır ve sistemin kararlılığı azalır. Kararlı çalışmayan bir sistem ise güvenlik açığı anlamına gelir. Bu nedenle güvenlik odaklı sistemlerde enerji verimli donanım seçimi yalnızca bir tasarruf kararı değil aynı zamanda bir güvenilirlik ve güvenlik kararıdır. 7/24 çalışan sistemler için 80 PLUS Platinum veya Titanium güç kaynakları, düşük TDP'li işlemciler ve pasif soğutmayı destekleyen donanımlar tercih edilmelidir.

SIRA SİZDE

Aşağıdaki işlemcilerin PPW değerlerini hesaplayınız, en yüksekten en düşüğe sıralayınız ve en dengeli işlemciyi belirleyiniz.

İşlemci	Performans Puanı	Ort. Güç (W)	PPW = Puan ÷ Güç	Sıralama
A	22.000	130 W	.....	.....
B	18.000	65 W	.....	.....
C	15.000	45 W	.....	.....
En yüksek PPW'ye sahip işlemci: ..... Bu işlemci neden en verimlidir?:				

BİLGİ KUTUSU : Ahilik Kültürü ve Bilinçli Donanım Kullanımı

Ahilik kültüründe meslek sahibi bireylerin işini özenle yapması, dürüst davranması, kaliteli ürün ortaya koyması ve kaynakları israf etmemesi önemlidir. Bu anlayış, günümüz bilişim teknolojileri alanında da geçerlidir.

Bilgisayar donanımı seçerken yalnızca en güçlü veya en pahalı parçayı tercih etmek her zaman doğru bir yaklaşım değildir. Kullanım amacına uygun, uzun ömürlü, enerji verimli ve bakım-onarımı mümkün donanımların seçilmesi daha bilinçli bir davranıştır. Bu yaklaşım; gereksiz tüketimi azaltır, ekonomik kaynakların verimli kullanılmasına katkı sağlar ve elektronik atık oluşumunu azaltmaya yardımcı olur. Bu nedenle bilinçli donanım seçimi, Ahilik kültüründeki israftan kaçınma ve topluma faydalı olma anlayışıyla ilişkilendirilebilir.

4. ETKİNLİK

Etkinlik Adı	Donanım Karşılaştırma Tablosu
Süre	30 dakika
Amaç	Enerji verimliliğini temel kriter olarak alarak donanım birimlerini fiyat ve performans açısından karşılaştırmak ve en uygun seçimi gerekçelendirmek
Yönerge	Aynı kullanım amacı için kullanılabilecek aynı tür üç farklı donanım seçeneği belirleyiniz. Her seçeneğin fiyat, performans, enerji tüketimi ve kullanım alanı bilgilerini toplayınız. Aşağıdaki tabloyu doldurunuz ve En Uygun Denge seçimini işaretleyiniz. Seçiminizi sınıfınıza sunarak gerekçenizi açıklayınız.

Donanım / Seçenek	Enerji / Verimlilik	Performans (kısa)	Fiyat (yaklaşık)	Kullanım Alanı	Seçim Notu (Neden?)
1. Seçenek					
2. Seçenek					
3. Seçenek					

En Uygun Denge: ☐ 1. Seçenek ☐ 2. Seçenek ☐ 3. Seçenek

Gerekçe: _____

Değerlendirme

Çalışmanız öğretmeniniz tarafından analitik dereceli puanlama anahtarına göre değerlendirilecektir. Çalışmanızı yaparken buradaki ölçütleri dikkate alınız. Analitik dereceli puanlama anahtarı formuna ulaşmak için karekodu okutunuz. Dijital yayınlarda karekodun üstüne tıklayarak içeriğe ulaşabilirsiniz.

ÖLÇME VE DEĞERLENDİRME

A) Aşağıdaki yapılandırılmış gridde numaralandırılmış kutucuklarda bazı bellek türleri ve bellek içeren bileşenler verilmiştir. Aşağıdaki soruların cevaplarını kutucuk numaralarını kullanarak ilgili boşluklara yazınız (Bir kutucuğu birden fazla cevap için kullanabilirsiniz.).

1 RAM 	2 ROM 	3 Flash Bellek 
4 SRAM 	5 DRAM 	6 EEPROM 
7 BIOS/UEFI Çipi 	8 SSD 	9 PROM 

1. Elektrik gücü aniden kesildiğinde üzerindeki tüm verileri kaybeden geçici bellek türleri hangileridir?

.....

2. Elektrik gücü kesilse bile verilerini koruyan kalıcı bellek türleri hangileridir?

.....

3. Elektrik sinyalleri kullanılarak üzerine birden fazla kez yazma işlemi yapılabilen bellek türleri hangileridir?

.....

4. Kullanıcı tarafından bir kez yazılıp daha sonra değiştirilemeyen (salt okunur) bellek türü hangisidir?

.....

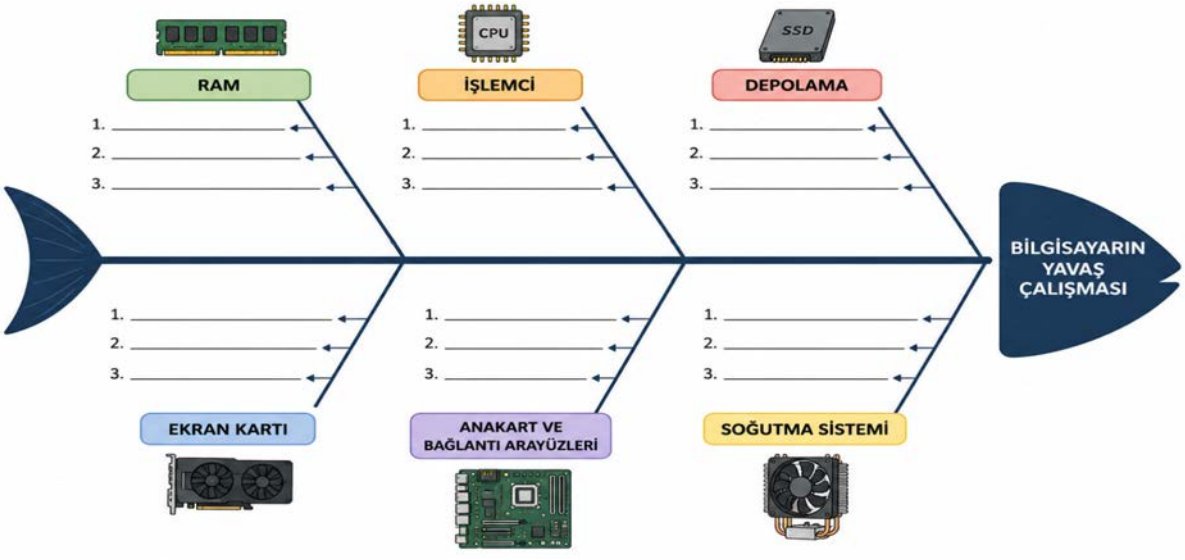
5. İşlemci önbelleğinde (cache) kullanılan, yüksek hızlı ve düşük gecikmeli bellek türü hangisidir?

.....

B) Aşağıdaki tanımları kavramlarla eşleştiriniz. Tanımların başındaki boşluğa ilgili kavramın harfini yazınız.

	Tanım	Kavram
	1. Monitör veya projektör bağlantısı için kullanılan görüntü çıkış portudur.	**A)** SATA portu
	2. İki kübit arasında özel bir ilişki oluşturarak birindeki durumun diğeriyle bağlantılı olmasını sağlayan kuantum özelliğidir.	**B)** PCIe x16 yuvası
	3. Klavye, fare, web kamera gibi çevre birimlerinin bağlandığı porttur.	**C)** CMOS pili
	4. Depolama birimlerinin anakarta veri kablosuyla bağlandığı bağlantı noktasıdır.	**Ç)** USB Type-A
	5. Kuantum bilgisayarlara dayanıklı şifreleme yöntemlerini kapsayan alandır.	**D)** 80 PLUS
	6. Bilgisayar kapalıyken tarih ve saat bilgisini koruyan küçük pildir.	**E)** HDMI/DisplayPort
	7. Güç kaynaklarının yüksek enerji verimliliğini belgeleyen sertifika sistemidir.	**F)** ATX
	8. Aynı anda 0 ve 1 durumlarını taşıyabilen kuantum bilgi birimidir.	**G)** Kübit
	9. Kübitlerin kuantum özelliklerini çevre etkisiyle kaybetmesidir.	**H)** Dekoherans
	10. Yüksek hızlı genişleme kartlarının bağlandığı yuvadır.	**I)** Post-kuantum kriptografi
		J) Dolanıklık

C) Aşağıdaki balık kılçığı diyagramında ana problem, bilgisayarın yavaş çalışması olarak verilmiştir. Diyagramdaki her dal, bilgisayarın farklı bir donanım bileşenini göstermektedir. Her dal için bilgisayarın yavaş çalışmasına neden olabilecek en az ikişer adet donanımsal sorun yazınız (Yalnızca donanım kaynaklı nedenleri yazınız.).



Ç) Aşağıdaki soruların doğru cevabını işaretleyiniz.

1. Anakart üzerinde işlemcinin takıldığı fiziksel yuvaya verilen ad aşağıdakilerden hangisidir?

A) Yonga seti (Chipset) B) CMOS pili C) CPU soketi

D) PCIe yuvası E) RAM yuvası

2. Aşağıdakilerden hangisi RAM'in <u>temel</u> özelliğidir?

A) Bilgisayar kapatıldığında verileri kalıcı olarak saklar.

B) Güç kesildiğinde içeriği silinir.

C) Sistemin görsel çıkışını yönetir.

D) Ağ üzerinden gelen verileri depolar.

E) Yalnızca depolama birimlerinden veri okur.

3. TDP değerinin işlemcilerde ifade ettiği durum aşağıdakilerden hangisidir?

A) Saniyede yapabileceği işlem sayısı

B) Çekirdek sayısı ve önbellek kapasitesi

C) Tam yükte açığa çıkarabileceği maksimum ısı miktarı

D) Desteklediği maksimum bellek kapasitesi

E) Çalışma voltajı ve güç hattı sayısı

4. NVMe SSD ile 7200 RPM HDD karşılaştırıldığında aşağıdakilerden hangisi doğrudur?

A) HDD, hareketli parçası olmadığı için daha uzun ömürlüdür.

B) NVMe SSD, yalnızca masaüstü bilgisayarlarda kullanılabilir.

C) HDD, NVMe SSD'ye göre daha hızlı okuma hızına sahiptir.

D) NVMe SSD yalnızca yazma hızında HDD'den üstündür.

E) NVMe SSD, HDD'ye göre daha az enerji tüketir.

5. RAID seviyeleri ile ilgili aşağıdaki ifadelerden hangisi doğrudur?

A) RAID 0 veri güvenliğini artırır.

B) RAID 1 okuma ve yazma hızını artırır.

C) RAID 5 en az iki disk gerektirir.

D) RAID 6 aynı anda iki disk arızasına karşı koruma sağlar.

E) RAID 10 yalnızca hız odaklı sistemler için tasarlanmıştır.

6. MAC adresi ile ilgili aşağıdaki bilgilerden hangisi yanlıştır?

A) MAC adresi, IP adresiyle aynı olup yalnızca farklı bir isimle anılır.

B) MAC adresi 48 bitten oluşan fiziksel bir adrestir.

C) Her ağ arayüz kartına üretici tarafından atanan eşsiz bir adrestir.

D) MAC adresinin ilk 24 biti üreticiyi, son 24 biti cihazı tanımlar.

E) MAC adresi yerel ağda cihazların birbirini tanımasını sağlar.

7. **Ekran kartı üzerindeki VRAM'in temel işlevi aşağıdakilerden hangisidir?**

A) Grafik verilerini geçici olarak tutmak

B) İşletim sisteminin çalışması için gerekli dosyaları saklamak

C) Bilgisayarın enerji tüketimini düzenlemek

D) Ağ üzerinden veri alışverişini yönetmek

E) İşlemcinin önbelleğini desteklemek

8. **Bir anakartın form faktörünün ifade ettiği bilgi aşağıdakilerden hangisidir?**

A) Desteklediği işlemci hızı

B) Fiziksel boyutu

C) Desteklediği RAM tipi

D) Güç tüketimi değeri

E) Yonga seti modeli

9. **Monitör teknolojileri arasında EU A sınıfı etiketinin anlamı aşağıdakilerden hangisidir?**

A) En yüksek çözünürlük değeri

B) En yüksek yenileme hızı

C) En verimli enerji kategorisi

D) OLED panel teknolojisi

E) En düşük parlaklık değeri

10. **PPW değerinin hesaplanması için kullanılan formül aşağıdakilerden hangisidir?**

A) Güç tüketimi ÷ Performans puanı

B) Performans puanı × Güç tüketimi

C) Sıcaklık ÷ Güç tüketimi

D) Performans puanı + Güç tüketimi

E) Performans puanı ÷ Güç tüketimi

D) Bağlam temelli soruların doğru cevaplarını ayrılan alanlara yazınız.

1-3. soruları aşağıdaki senaryoya göre cevaplayınız.

Yazılım geliştirici Günce, yeni bilgisayarını yapılandırmak üzere teknik bir servise danışıyor. Günce aynı anda birden fazla uygulamayla yoğun çoklu görev yapıyor, büyük veri setlerini derliyor ve bilgisayarını 7/24 açık tutmak istiyor. Teknisyen ona şu iki seçeneği sunuyor:

A: 35W TDP düşük güç serisi işlemci, DDR5 bellek, NVMe SSD, 80 PLUS Gold 350W güç kaynağı

B: 125W TDP yüksek performanslı işlemci, DDR4 bellek, 7200 RPM HDD, 80 PLUS Bronze 600W güç kaynağı

1. Günce'nin kullanım amacına göre A ve B seçeneklerinin enerji verimliliğini karşılaştırıp hangi seçeneğin daha uygun olduğunu gerekçeleriyle yazınız.

.....

.....

2. 7/24 kesintisiz çalışan bir bilgisayarda yüksek enerji tüketen işlemci kullanılması yalnızca fatura maliyetini değil sistem güvenilirliğini de etkiler. Bu ilişkiyi siber güvenlik bağlamında açıklayınız.

.....

.....

3. B'deki 7200 RPM HDD, NVMe SSD ile değiştirilirse hem performans hem enerji açısından hangi değişiklikler yaşanır?

.....

.....

4-5. soruları aşağıdaki senaryoya göre cevaplayınız.

Bir şirketin BT yöneticisi, güvenlik sunucusu için iki işlemci değerlendiriyor. Sunucu, yılın tamamında günün 24 saati çalışmakta ve zamanın %30'u tam yük, %70'i boşta geçmektedir.

	Performans Puanı	Tam Yük Gücü (W)	Boşta Gücü (W)
1. İşlemci	22.000	180W	35W
2. İşlemci	18.000	65W	12W

4. Her iki işlemci için tam yükteki PPW değerlerini hesaplayınız ve karşılaştırınız.

.....

.....

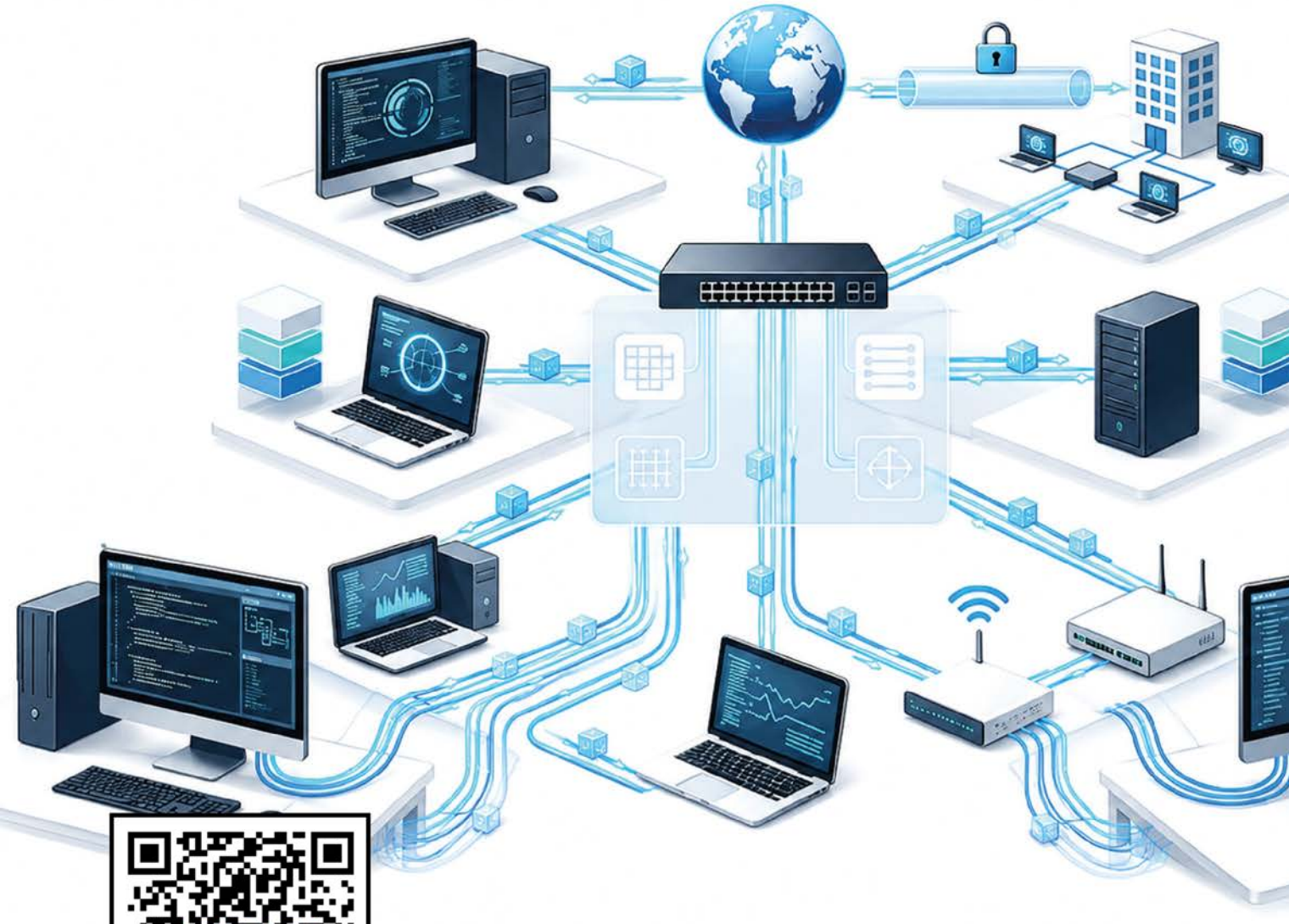
5. Bu sunucu için yalnızca tam yük PPW değerine bakmak yanıltıcı olabilir. Boşta güç tüketimini de hesaba katarak hangi işlemcinin daha verimli olacağını açıklayınız.

.....

.....

2. ÖĞRENME BİRİMİ

AĞ İLETİŞİMİ





KONULAR

2.1. OSI REFERANS MODELİ
2.2. TCP/IP PROTOKOL KÜMESİ
2.3. AĞ PROTOKOLLERİ

ANAHTAR KAVRAMLAR

- 10BASE-T
- ağ iletişimi
- ARP
- broadcast
- DHCP
- DNS
- Ethernet
- FTP
- HDLC
- HTTP
- HTTPS
- ICMP
- IPv4
- IPv6
- kapsülleme
- LAN
- loopback
- OSI
- referans modeli
- router
- SMTP
- SSH
- subnetting
- TCP
- TCP/IP modeli
- Telnet
- TFTP
- UDP
- VLSM
- VPN
- WAN
- Wi-Fi

Bu öğrenme biriminde sizden

- OSI referans modelini kullanarak ağ iletişiminin nasıl gerçekleştiğini açıklamanız
- ağ türlerini, ağ topolojilerini ve ağ cihazlarını ayırt etmeniz
- kapsülleme ve kapsül açma süreçlerini katmanlarla ilişkilendirmeniz
- TCP ve UDP protokollerinin temel özelliklerini karşılaştırmanız
- IPv4 ve IPv6 adresleme mantığını kavramanız
- Alt ağ maskesi, varsayılan ağ geçidi, APIPA ve loopback kavramlarını açıklamanız
- IPv4 alt ağlara bölme ve VLSM uygulamaları yapmanız
- yönlendirici ve istemcileri statik IPv4 ve IPv6 adresleri ile yapılandırarak bağlantı testleri yapmanız
- ARP ve ICMP protokollerinin ağ iletişimindeki görevlerini açıklamanız
- veri bağı ve fiziksel katmanla ilgili temel protokol, ortam ve kablo yapılarını tanımanız
- T568A, T568B ve çapraz kablo sonlandırma uygulamaları yapmanız
- TCP/IP modeli ile OSI referans modelini karşılaştırmanız
- DHCP, DNS, HTTP/HTTPS, FTP, SMTP/POP3, Telnet/SSH, TFTP gibi ağ protokollerini tanıyarak temel uygulamalar yapmanız

beklenmektedir.

HAZIRLIK ÇALIŞMASI

Aşağıda ağ iletişimiyle ilgili günlük yaşamdan bir durum verilmiştir.

Evde, okulda veya kütüphanede internete bağlanırken, bir dosyayı başka bir cihaza gönderirken ya da ortak bir yazıcıyı kullanırken cihazlar arasında iletişim kurulur. Bu iletişimin gerçekleşebilmesi için cihazların açık olması, bağlantının sağlanması ve bazı temel ayarların doğru yapılması gerekir. Bazen internet yavaşlayabilir, bağlantı kopabilir veya bir cihaza ulaşılamayabilir. Böyle durumlarda kullanıcılar önce gözle görülebilen ve kolayca kontrol edilebilen noktaları inceleyerek sorunun nedenini anlamaya çalışır.

Verilen durumdan ve kendi gözlemlerinizden yararlanarak aşağıdaki soruları cevaplayınız.

1. Günlük yaşamda ağ veya internet bağlantısını hangi durumlarda kullanıyorsunuz? İki örnek yazınız.

   .....

2. Bir cihazda bağlantı sorunu yaşandığında gözle görülebilen hangi basit kontroller yapılabilir?

   .....

3. Okul laboratuvarında, evde veya iş yerinde birden fazla cihazın aynı bağlantı ortamını kullanması hangi kolaylıkları sağlayabilir?

   .....

4. Cihazların birbirleriyle iletişim kurabilmesi için nelerin gerekli olduğunu düşünüyorsunuz?

   .....

BAŞLARKEN

Günlük yaşamda bir web sayfası açarken, okul laboratuvarındaki başka bir bilgisayara dosya gönderirken, ortak yazıcıyı kullanırken veya kablosuz ağ üzerinden internete bağlanırken farkında olmadan bir ağ iletişimi sürecinin içinde yer alınır. Bu süreç, dışarıdan bakıldığında oldukça basit görünse de arka planda verinin hazırlanması, uygun kurallarla paketlenmesi, doğru adrese yönlendirilmesi, ağ cihazları ve iletim ortamları üzerinden taşınması, hedef cihazda yeniden anlamlı bilgiye dönüştürülmesi gibi çok sayıda işlem gerçekleşir. Ağ iletişimi, yalnızca cihazların birbirine bağlanması değildir. Bu bağlantının belirli modeller, adresleme yapıları ve protokoller üzerinden düzenli biçimde yürütülmesidir. Bu öğrenme biriminde ağın temel yapısı, katmanlı iletişim modeli, adresleme mantığı, veri iletim süreci ve temel ağ protokolleri ele alınacaktır. Bu sayede kullanılan dijital sistemlerin arka planında işleyen iletişim yapısının daha bilinçli biçimde yorumlanması ve uygulama temelli çalışmalarla bu yapıların kullanılması sağlanır.

2.1. OSI REFERANS MODELİ

OSI referans modeli, ağ iletişiminin düzenli ve anlaşılır biçimde açıklanmasını sağlayan katmanlı bir yapıdır. Bu modelin daha iyi anlaşılabilmesi için öncelikle ağın ne olduğu, hangi türlere ayrıldığı ve iletişimin gerçekleştiği temel yapının tanınması gerekir.

2.1.1. Ağ ve Türleri

Ağ, iki veya daha fazla cihazın veri paylaşmak, ortak kaynakları kullanmak ve karşılıklı iletişim kurmak amacıyla birbirine bağlandığı yapıdır. Bu yapı, yalnızca bilgisayarları değil yazıcı, sunucu, yönlendirici, anahtar, erişim noktası gibi birçok dijital bileşeni kapsar. Ağ sayesinde dosya paylaşımı, ortak yazıcı kullanımı, internet erişimi ve farklı cihazlar arasında veri aktarımı gerçekleştirilebilir. Ağlar, kapsadıkları alanın büyüklüğüne ve kullanım amaçlarına göre farklı türlere ayrılır.

Yerel alan ağı [Local Area Network (LAN)], sınırlı bir fiziksel alan içinde kurulan ağ yapısıdır. Sınıf, laboratuvar, ofis, ev gibi ortamlarda kullanılır. LAN'larda veri iletimi genellikle hızlıdır ve iletişim çoğunlukla switch gibi cihazlar üzerinden gerçekleşir. Yönetimi diğer ağ türlerine göre daha kolaydır. Bir bilgisayar laboratuvarında bulunan yirmi adet öğrenci bilgisayarı, öğretmen bilgisayarı ve ortak yazıcının aynı anahtar üzerinden birbirlerine bağlı olduğu yapı buna örnek gösterilebilir. Bu yapıda cihazlar, aynı yerel ağ içinde bulunur ve iletişim kısa mesafede gerçekleşir.

Metropol alan ağı [Metropolitan Area Network (MAN)], bir şehir veya büyük yerleşkelerde kurulan ağ yapısıdır. Bu ağ türü, birden fazla yerel ağın şehir düzeyinde birbirine bağlanmasıyla oluşur. Üniversite kampüsleri, büyük belediye yerleşkeleri veya aynı şehirdeki farklı kurumsal binalar MAN yapısına göre örnek olabilir. MAN, LAN'dan daha geniş, WAN'dan daha dar kapsamlıdır. Bu ağ türünde merkezî bağlantılar, omurga hatlar ve daha planlı ağ yönetimi ön plana çıkar.

Geniş alan ağı [Wide Area Network (WAN)]; farklı şehirlerde, bölgelerde hatta ülkelerde bulunan ağların birbirine bağlanmasıyla oluşan yapıdır. Bu tür yapılarda mesafe arttığı için yönlendirme, servis sağlayıcı bağlantıları, gecikme, güvenlik, süreklilik gibi konular daha önemli hâle gelir. Farklı şehirlerde bulunan iki kurum binasının ortak veri tabanı sistemi üzerinde çalışması WAN yapısına örnek olabilir. İnternet de geniş ölçekte değerlendirildiğinde çok büyük bir WAN mantığıyla düşünülebilir.

Sanal özel ağ [Virtual Private Network (VPN)], kullanıcıların internet üzerinden başka bir ağa güvenli biçimde bağlanmasını sağlayan yapıdır. VPN sayesinde kullanıcı, fiziksel olarak kurum dışında olsa bile yetkiliyse kurum ağına sanki içerideymiş gibi erişebilir. Temel amaç, genel internet altyapısı üzerinden güvenli ve denetimli iletişim sağlamaktır. Evden çalışan bir öğretmenin okul ağına güvenli şekilde bağlanması veya bir kurum personelinin uzaktan sistemlere erişmesi VPN yapısına örneklerdir.

Ağ türlerini doğru ayırt etmek; adresleme, yönlendirme, topoloji ve protokol kavramlarının anlaşılması açısından önemlidir çünkü ağın büyüklüğü arttıkça kullanılacak cihazlar, iletişim yöntemleri ve yönetim yaklaşımı da değişir.

SIRA SİZDE

Aşağıdaki öğrenci ifadelerini okuyunuz. Her ifadenin doğru veya yanlış olduğuna karar veriniz. Yanlış olduğunu düşündüğünüz ifadelerin doğru hâlini ilgili alana yazınız.

Öğrenci	Öğrencinin İfadesi	Doğru	Yanlış
1. Öğrenci	Aynı binada bulunan bütün ağlar, kullanım amaçları dikkate alınmadan LAN olarak değerlendirilir.	☐	☐
2. Öğrenci	Bir şehir ölçeğinde farklı yerel ağları birbirine bağlayan yapı MAN olarak adlandırılabilir.	☐	☐
3. Öğrenci	VPN yalnızca fiziksel olarak aynı ortamda bulunan cihazların birbirine bağlanması için kullanılır.	☐	☐

Yanlış olduğunu düşündüğünüz ifadelerin doğru hâlini yazınız.

.....

.....

.....

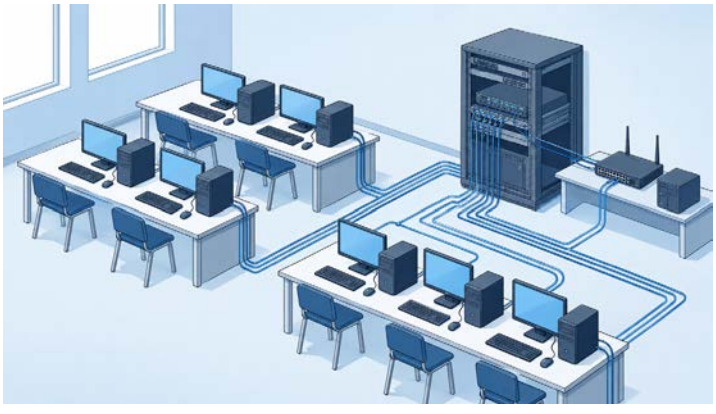
Seçimlerinizi kısaca açıklayınız.

.....

2.1.2. Ağ Topolojileri

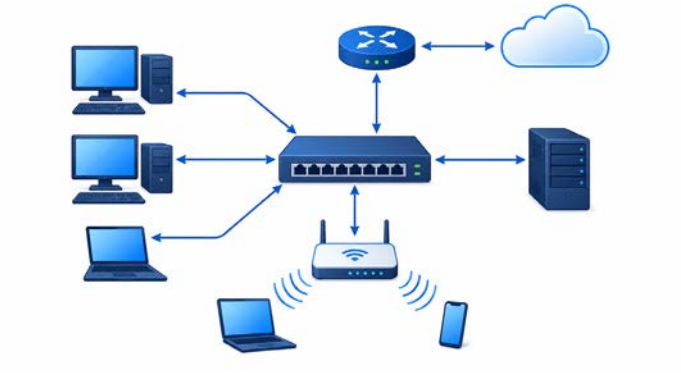
Ağ topolojisi, ağdaki cihazların hangi düzende bağlandığını ve veri akışının hangi yapıya göre gerçekleştiğini ifade eder. Topoloji, ağın yalnızca görünüşünü değil aynı zamanda çalışma mantığını, arıza davranışını, genişleme kapasitesini ve yönetim kolaylığını da etkiler. Bu nedenle topoloji, ağ tasarımının temel bileşenlerinden biridir.

Fiziksel topoloji, cihazların ve kabloların gerçek yerleşimini gösterir (Görsel 2.1). Bilgisayarların hangi noktada bulunduğu, hangi kablonun hangi cihaza bağlandığı ve ağın fiziksel olarak nasıl kurulduğu bu başlık altında değerlendirilir. Temel ağ topolojileri arasında yıldız, veri yolu, halka, ağaç ve örgü topolojileri yer alır.



Görsel 2.1: Fiziksel topoloji

Mantıksal topoloji, verinin ağ içinde nasıl hareket ettiğini açıklar (Görsel 2.2). Fiziksel bağlantı şekli ile verinin izlediği yol her zaman bire bir aynı olmayabilir. Bu nedenle ağ topolojisi değerlendirilirken yalnızca kablo düzenine bakmak yeterli değildir. Veri akış mantığı da dikkate alınmalıdır.



Görsel 2.2: Mantıksal topoloji

Yıldız topolojide tüm cihazlar merkezde bulunan bir anahtara veya benzeri bir cihaza bağlanır (Görsel 2.3). Yönetim kolaylığı ve yaygın kullanımı nedeniyle bugün en sık karşılaşılan topolojidir.



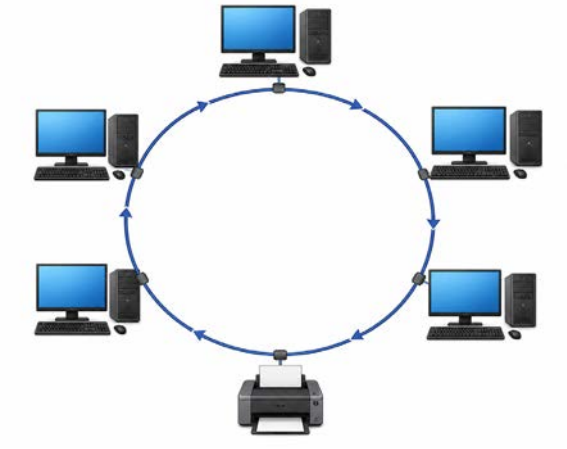
Görsel 2.3: Yıldız topoloji

Veri yolu topolojisinde tüm cihazlar ortak bir iletişim hattını paylaşır (Görsel 2.4). Yapı basit görünse de tek hat üzerindeki sorunlar tüm sistemi etkileyebilir.



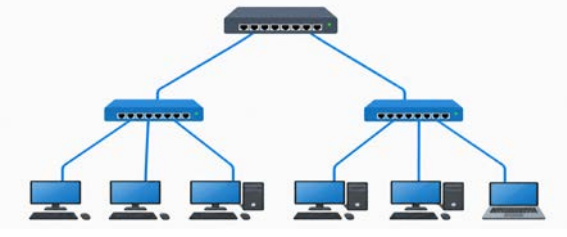
Görsel 2.4: Veri yolu topolojisi

Halka topolojide cihazlar dairesel bir düzen içinde birbirine bağlanır ve veri, belirli bir sıra ile dolaşır (Görsel 2.5).



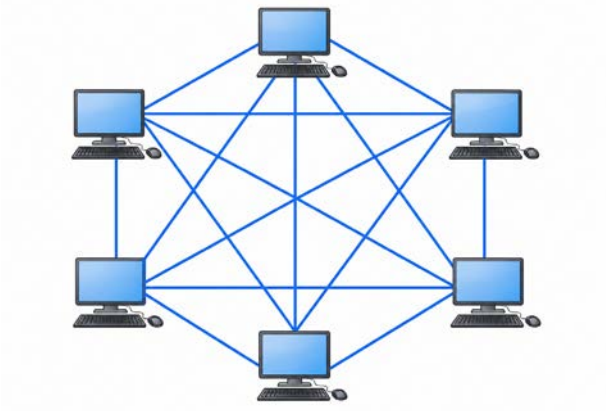
Görsel 2.5: Halka topolojisi

Ağaç topolojide hiyerarşik bir yapı vardır. Özellikle büyüyen ağlarda alt birimlerin düzenli biçimde bağlanmasında kullanılır (Görsel 2.6).



Görsel 2.6: Ağaç topolojisi

Örgü topolojide cihazlar arasında birden fazla bağlantı bulunur. Bu yapı, yedeklilik gerektiren ağlarda tercih edilir (Görsel 2.7).



Görsel 2.7: Örgü topolojisi

Topoloji seçimi yapılırken kurulum maliyeti, bakım kolaylığı, arıza toleransı, genişleme ihtiyacı, performans gibi ölçütler birlikte değerlendirilmelidir. Bu nedenle ağ topolojileri yalnızca isim olarak değil kullanım bağlamı içinde öğrenilmelidir.

1. ETKİNLİK

Etkinlik Adı	Uygun Ağ Topolojisini Belirlemek
Süre	20 dakika
Amaç	Ağ topolojilerini kullanım alanları, avantajları ve sınırlılıkları bakımından karşılaştırarak verilen durumlara uygun topolojiyi belirlemek
Yönerge	Aşağıdaki durumları arkadaşınızla birlikte inceleyiniz. Her durum için uygun olduğunu düşündüğünüz ağ topolojisini yazınız ve seçiminizi kısa biçimde gerekçelendiriniz. Okul ağıyla ilgili verilen durumu değerlendirerek çözüm önerinizi oluşturunuz.

1. Bölüm: Durumlara Uygun Topolojiyi Belirlemek

Durum	Seçtiğiniz Topoloji	Seçiminizin Gerekçesi
Bir bilgisayar laboratuvarındaki bütün bilgisayarların merkezde bulunan bir switche bağlanması istenmektedir. Bir bilgisayarda oluşan bağlantı sorununun diğer bilgisayarların çalışmasını etkilememesi beklenmektedir.		
Bazı cihazların ortak bir iletişim hattını kullanacağı düşük maliyetli bir ağ tasarlanmaktadır ancak ana hatta oluşabilecek bir sorunun bütün ağı etkileyebileceği bilinmektedir.		
Cihazların kapalı bir düzen içinde birbirine bağlanması ve verinin belirli bir sıra izleyerek ilerlemesi istenmektedir.		
Üç katlı bir okul binasında her kattaki sınıfların ayrı birimlere bağlanması, bu birimlerin de merkezî bir cihaz üzerinden yönetilmesi planlanmaktadır.		
Kesintisiz çalışması gereken bir sistemde cihazlar arasında birden fazla bağlantı yolunun bulunması istenmektedir. Bir bağlantı kullanılamaz hâle geldiğinde veri aktarımının farklı bir yol üzerinden sürdürülmesi beklenmektedir.		

2. Bölüm: Örnek Bir Okul Ağı İçin Çözüm Üretmek

Durum: Örnek bir okul binasında üç katlı yeni bir bölüm hizmete açılacaktır. Her katta beş sınıf bulunmaktadır. Kurulacak ağ altyapısının güvenilir, kolay yönetilebilir ve ileride yapılabilecek genişletmelere uygun olması beklenmektedir.

Aşağıdaki soruları cevaplayınız.

1. Bu yapı için hangi topolojinin veya topolojilerin kullanılması uygun olabilir?

   .....

   .....

2. Seçtiğiniz topolojinin sağlayacağı iki avantajı yazınız.

   .....

   .....

3. Ağın ileride genişletilmesi gerektiğinde hangi noktalar dikkate alınmalıdır?

   .....

   .....

Değerlendirme

Çalışmanız öğretmeniniz tarafından analitik dereceli puanlama anahtarına göre değerlendirilecektir. Çalışmanızı yaparken buradaki ölçütleri dikkate alınız. Analitik dereceli puanlama anahtarı formuna ulaşmak için karekodu okutunuz. Dijital yayınlarda karekodun üstüne tıklayarak içeriğe ulaşabilirsiniz.

2.1.3. Ağ Cihazları

Ağ iletişimi, farklı görevler üstlenen cihazların ve iletim ortamlarının birlikte çalışmasıyla gerçekleşir. Ağ üzerindeki her cihaz aynı işlevi yerine getirmez. Bazı cihazlar veriyi üretir veya kullanır, bazı cihazlar verinin doğru hedefe ulaşmasını sağlar, bazı yapılar ise verinin taşınacağı ortamı oluşturur. Ağ cihazlarının görevlerini doğru ayırt etmek hem ağ kurulumu hem de bağlantı sorunlarının giderilmesi açısından önemlidir.

Uç cihazlar, ağ iletişiminin başladığı veya sona erdiği cihazlardır. Bilgisayar, dizüstü bilgisayar, tablet, ağ yazıcısı, IP kamera, sunucu gibi cihazlar bu grupta yer alabilir. Uç cihazlar veriyi üretir, kullanır, işler veya görüntüler.

Ara cihazlar, ağ içindeki veri akışını düzenleyen ve cihazlar arasındaki iletişimin gerçekleşmesine yardımcı olan yapılardır. Anahtar, yönlendirici, modem ve erişim noktası bu grupta değerlendirilebilir. Ara cihazların görevleri, kullanım amaçlarına göre birbirinden farklıdır.

İletim ortamı, verinin fiziksel veya elektromanyetik olarak taşındığı yapıdır. Bakır kablolar, fiber optik kablolar ve kablosuz sinyaller iletim ortamlarına örnektir. Ağ cihazlarının iletişim kurabilmesi için uygun iletim ortamının seçilmesi gerekir. Ağ cihazları ve veri iletim ortamları Görsel 2.8'de gösterilmiştir.



Görsel 2.8: Ağ cihazları

Temel Ağ Cihazları ve Görevleri

Ağ yapısında kullanılan cihazlar, iletişim sürecinin farklı aşamalarında belirli görevler üstlenir. Aynı yerel ağda veri iletimini düzenleme, farklı ağlar arasında paketleri yönlendirme, kablosuz erişim sağlama ve ağ üzerindeki cihazlara çeşitli hizmetler sunma bu görevlerden bazılarıdır. Ağ cihazlarının görevlerinin bilinmesi, kurulacak yapıya uygun cihazların seçilmesi ve bağlantı sorunlarının daha kolay belirlenmesi açısından önemlidir.

Tablo 2.1'de ağ cihazlarının temel görevleri ve kullanım alanları gösterilmiştir.

Tablo 2.1: Temel Ağ Cihazları ve Görevleri

Ağ Cihazı	Temel Görevi	Kullanım Örneği
Anahtar (Switch)	Aynı yerel ağdaki cihazlar arasında veri iletimini düzenler. Ethernet çerçevelerini hedef MAC adreslerine göre ilgili bağlantı noktasına iletir.	Bilgisayar laboratuvarındaki bilgisayarların aynı yerel ağda birbirine bağlanması
Yönlendirici (Router)	Farklı ağlar arasındaki paket iletimini gerçekleştirir. Hedef IP adresine göre uygun yolu belirler.	Okul laboratuvarı ağı ile internet veya farklı alt ağlar arasında iletişim kurulması
Modem	Servis sağlayıcı bağlantısının yerel ağa ulaştırılmasına yardımcı olur. Kullanılan erişim teknolojisine göre gerekli sinyal dönüşümünü gerçekleştirebilir.	İnternet servis sağlayıcısından gelen bağlantının ev veya okul ağına aktarılması
Erişim Noktası (Access Point)	Kablosuz cihazların yerel ağa bağlanmasını sağlar.	Dizüstü bilgisayarların, tabletlerin ve telefonların kablosuz ağ üzerinden iletişim kurması
Sunucu	Ağdaki diğer cihazlara belirli hizmetler sunar.	Dosya paylaşımı, web hizmeti, DNS veya DHCP hizmeti sağlanması
Ağ Yazıcısı	Ağ üzerinden gönderilen yazdırma isteklerini alır ve işler.	Birden fazla bilgisayarın ortak yazıcıyı kullanması

2.1.4. OSI Modelinin Katmanlı Yapısı

Ağ iletişimi çok aşamalı bir süreçtir. Verinin hazırlanması, uygun biçime dönüştürülmesi, adrese bağlanması, iletilmesi ve hedefte yeniden anlamlandırılması tek bir adımda gerçekleşmez. Bu süreci düzenli ve anlaşılır biçimde açıklamak için katmanlı bir modele ihtiyaç duyulur. OSI referans modeli, bu ihtiyaca cevap veren temel yapılardan biridir. Katmanlı model, ağdaki görevleri daha anlaşılır hâle getirir. Ağ ile ilgili kavramları açıklamak için ortak bir anlatım sağlar. Farklı üreticilerin geliştirdiği ürünlerin birlikte çalışmasını kolaylaştırır. Bir katmanda yapılan değişikliklerin diğer katmanları etkilemesini azaltır.

OSI referans modeli, ağ iletişimini yedi katmanda ele alan kavramsal bir modeldir. Bu modelin amacı, iletişim görevlerini parçalara ayırarak her katmanın sorumluluğunu açık biçimde göstermektir. OSI modeli doğrudan çalışan fiziksel bir ürün değildir. Ağ iletişim süreçlerini incelemek, açıklamak ve sınıflandırmak için kullanılan bir çerçevedir (Görsel 2.9).

KATMAN	AÇIKLAMA	ÖRNEKLER
7 UYGULAMA (Application)	Ağ hizmetlerine erişim sağlayan uygulamalar için arayüz sağlar.	• HTTP/HTTPS • FTP • SMTP • DNS
6 SUNUM (Presentation)	Verilerin biçimini düzenler, şifreleme, sıkıştırma ve çeviri işlemlerini gerçekleştirir.	• TLS/SSL • JPEG • ASCII • MPEG
5 OTURUM (Session)	İki uygulama arasında oturum kurulmasını, yürütülmesini ve sonlandırılmasını sağlar.	• NetBIOS • RPC • SIP
4 TAŞIMA (Transport)	Uçtan uca güvenilir veri iletimi sağlar.	• TCP • UDP
3 AĞ (Network)	Verilerin ağlar arasında yönlendirilmesini sağlar.	• IP (IPv4/IPv6) • ICMP • OSPF
2 VERİ BAĞI (Data Link)	Aynı ağ üzerindeki cihazlar arasında güvenilir veri iletimi sağlar.	• Ethernet (802.3) • Wi-Fi (802.11) • PPP
1 FİZİKSEL (Physical)	Bitlerin fiziksel ortam üzerinden iletimini sağlar.	• UTP Kablo • Fiber Optik • Hub, Repeater

Görsel 2.9: OSI referans modeli

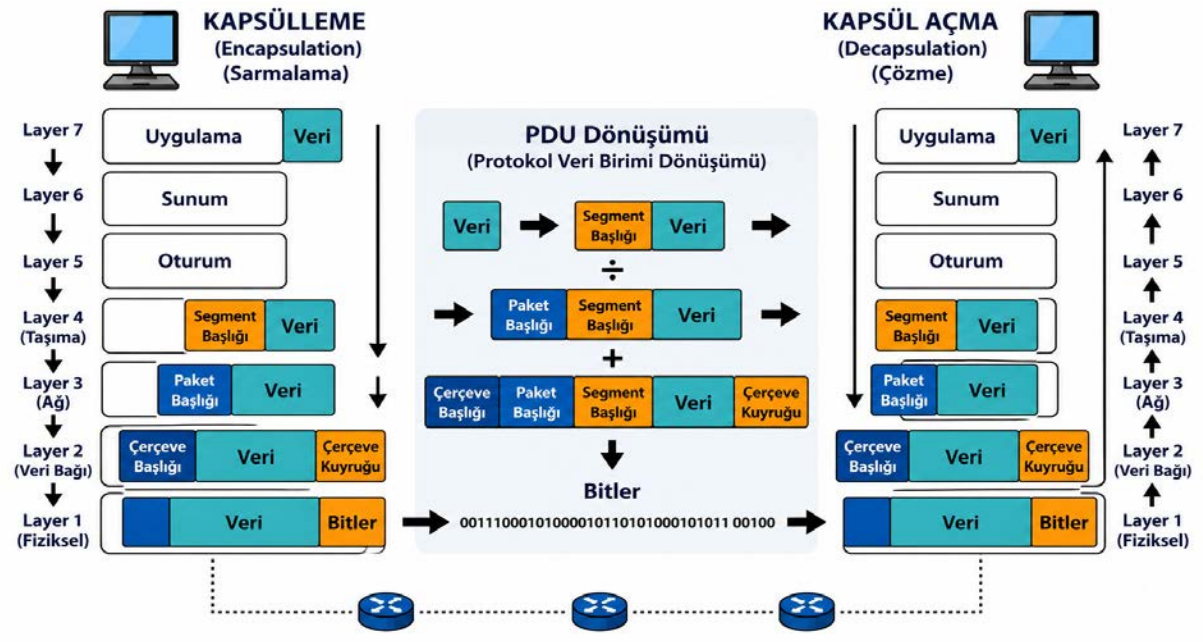
Katmanlar birlikte çalışarak verinin kaynaktan hedefe uygun biçimde ulaşmasını sağlar. En alt katman fiziksel iletimle ilgilenirken en üst katman kullanıcıya en yakın hizmetleri temsil eder. Katmanlı model kullanmanın en önemli yararı, karmaşık iletişim sürecini daha anlaşılır hâle getirmesidir. Böylece sorunlar daha kolay analiz edilir ve görevler daha net sınıflandırılır.

Kapsülleme (Encapsulation) ve Kapsül Açma (Decapsulation)

Bir veri, ağ üzerinden gönderilmeden önce doğrudan ham hâliyle iletilmez. Veri, üst katmanlardan alt katmanlara doğru ilerlerken her katmanda o katmanın görevine uygun bilgiler eklenerek iletime hazırlanır. Bu sürece kapsülleme denir. Kapsülleme sırasında uygulama katmanlarından gelen veri; taşıma katmanında kullanılan protokole göre segment veya datagram, ağ katmanında paket, veri bağı katmanında çerçeve ve fiziksel katmanda bit akışı biçiminde ele alınır. Böylece veri, ağ ortamında taşınabilecek uygun yapıya dönüştürülür.

Veri hedef cihaza ulaştığında ters yönde bir işlem gerçekleşir. Alt katmanlardan üst katmanlara doğru ilerleyen veri, her aşamada ilgili başlık ve kontrol bilgilerinden ayrılarak yeniden anlamlı hâle getirilir. Bu sürece **kapsül açma** denir. Kapsülleme ve kapsül açma kavramları anlaşılmadan veri birimlerinin neden farklı katmanlarda

farklı adlarla anıldığı ve iletişimin neden çok aşamalı olduğu tam olarak kavranamaz (Görsel 2.10).



Görsel 2.10: Kapsülleme ve kapsül açma süreçleri

2. ETKİNLİK

Etkinlik Adı	Verinin Ağdaki Yolculuğunu İncelemek
Süre	20 dakika
Amaç	Kapsülleme ve kapsül açma süreçlerini OSI katmanlarıyla ilişkilendirerek protokol veri birimlerinin dönüşüm sırasını açıklamak
Yönerge	Kaynak cihazdan gönderilen verinin hedef cihaza ulaşıncaya kadar geçirdiği aşamaları inceleyiniz. Aşağıdaki tablolardaki eksik alanları doldurunuz. Çalışmanızı tamamladıktan sonra cevaplarınızı arkadaşınızın cevaplarıyla karşılaştırınız.

1. Bölüm: Kapsülleme Sürecini Tamamlamak

İşlem Sırası	OSI Katmanı	Protokol Veri Birimi	Bu Aşamada Gerçekleşen Temel İşlem
1	Uygulama, sunum ve oturum katmanları	Veri	Kullanıcıya ait bilgi, ağ üzerinden aktarılmak üzere hazırlanır.
2	Taşıma katmanı		Veriye uçtan uca iletişim için gerekli bilgiler eklenir.
3	Ağ katmanı		
4	Veri bağı katmanı		Yerel ağda iletim için gerekli MAC adresi ve hata kontrolü bilgileri eklenir.
5	Fiziksel katman		

Not: Taşıma katmanındaki protokol veri birimi, kullanılan protokole göre farklı adlandırılabilir. TCP kullanıldığında **segment**, UDP kullanıldığında **datagram** ifadesi kullanılır.

2. Bölüm: Kapsül Açma Sürecini Tamamlamak

İşlem Sırası	OSI Katmanı	Protokol Veri Birimi	Bu Aşamada Gerçekleşen Temel İşlem
1	Fiziksel katman		Bitler alınır ve veri bağı katmanına aktarılır.
2	Veri bağı katmanı		
3	Ağ katmanı		IP adresi bilgileri incelenir.
4	Taşıma katmanı		
5	Uygulama, sunum ve oturum katmanları	Veri	Veri, uygulamanın kullanabileceği anlamlı bilgiye dönüştürülür.

3. Bölüm: Süreci Yorumlamak

1. Kaynak cihazda veriye neden farklı katmanlarda yeni bilgiler eklenir?

   .....

   .....

2. Veri bağı katmanındaki çerçeve ile ağ katmanındaki paket arasında nasıl bir ilişki vardır?

   .....

   .....

3. Hedef cihazda kapsül açma işlemi gerçekleşmeseydi kullanıcı veriye ulaşabilir miydi? Cevabınızı gerekçelendiriniz.

   .....

   .....

2.1.5. Uygulama Katmanı

Uygulama katmanı, kullanıcının ağ hizmetleriyle doğrudan karşılaştığı katmandır. Kullanıcı bir web sayfasına eriştiğinde, e-posta gönderdiğinde, dosya aktardığında veya uzaktan bağlantı kurduğunda uygulama katmanıyla ilişkili hizmetlerden yararlanır. Bu katman, kullanıcı programlarının ağ üzerinden veri alışverişi yapabilmesi için gerekli hizmetleri sunar. Web erişimi, ad çözümleme, dosya aktarımı, e-posta iletişimi gibi işlemler uygulama katmanıyla ilişkilidir. HTTP, HTTPS, DNS, FTP, SMTP, POP3 ve SSH bu katmanda ele alınan protokollere örnek verilebilir.

2.1.6. Sunum Katmanı

Sunum katmanı, verinin hedef sistem tarafından doğru biçimde yorumlanabilmesi için uygun gösterim yapısına dönüştürülmesiyle ilişkilidir. Farklı sistemlerde veriler farklı biçimlerde temsil edilebildiği için bilginin ortak ve anlamlı bir yapıyla iletilmesi gerekir. Veri biçimlendirme, kodlama uyumu ve veri gösterim biçimlerinin dönüştürülmesi bu katman kapsamında ele alınır. Sıkıştırma, sıkıştırılmış verinin açılması, şifreleme, şifre çözme gibi

işlemler de kavramsal olarak sunum katmanıyla ilişkilendirilebilir. Uygulama katmanı kullanıcı hizmetlerine odaklanırken sunum katmanı verinin nasıl temsil edildiğiyle ilgilenir.

2.1.7. Oturum Katmanı

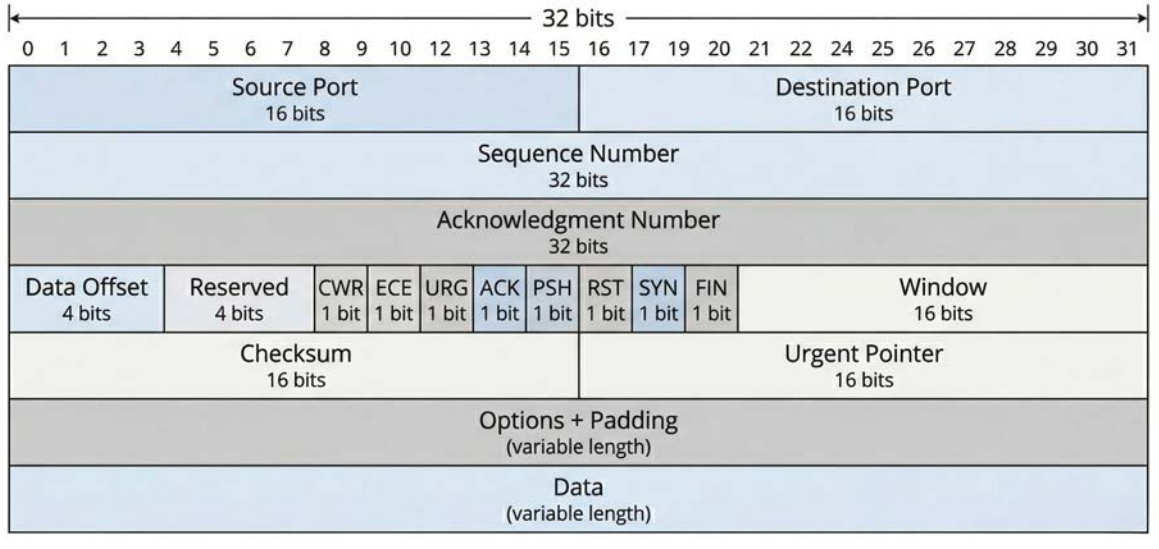
Oturum katmanı, iki sistem arasında kurulan iletişimin başlatılması, sürdürülmesi ve sonlandırılmasıyla ilgilenir. Bir ağ iletişimi yalnızca verinin gönderilmesinden ibaret değildir. İletişimin hangi aşamada başladığı, nasıl devam ettiği ve ne zaman tamamlandığı da önem taşır. Bu katman, uygulamalar arasındaki veri alışverişinin belirli bir düzen içinde yürütülmesiyle ilişkilidir. Gerektiğinde iletişimin eş zamanlı ilerlemesine, belirli kontrol noktalarından devam edebilmesine ve uygun biçimde sonlandırılmasına katkı sağlar. Oturum yönetimiyle ilişkili bazı kimlik doğrulama süreçleri de bu bağlamda değerlendirilebilir.

2.1.8. Taşıma Katmanı

Taşıma katmanı, verinin kaynak cihazdaki ilgili uygulamadan hedef cihazdaki ilgili uygulamaya uçtan uca iletilmesini düzenler. Bu katmanda port numaraları kullanılarak aynı cihaz üzerinde çalışan farklı uygulamaların veri trafiği birbirinden ayrılır. Veri gerektiğinde daha küçük parçalara bölünür, alıcı tarafta doğru sırayla birleştirilir ve kullanılan protokole göre iletimin güvenilirliği kontrol edilir. TCP ve UDP, taşıma katmanıyla ilişkilendirilen temel protokollerdir. TCP; bağlantı kurma, sıralama, hata kontrolü, yeniden gönderim gibi işlemlerle daha güvenilir bir iletim sağlar. UDP ise bağlantı kurma ve ayrıntılı kontrol işlemlerini azaltarak daha hızlı fakat daha az denetimli bir iletim sunar.

TCP ve Üç Yollu El Sıkışma Süreci

İletim Kontrol Protokolü [Transmission Control Protocol (TCP)], bağlantı odaklı çalışan ve güvenilir veri iletimini destekleyen bir taşıma katmanı protokolüdür. TCP iletişiminde veriler belirli bir düzen içinde sıralanır, alınan veriler onaylanır ve gerektiğinde kayıp veriler yeniden gönderilir. Bu özellikler, özellikle verinin eksiksiz ve doğru sırayla ulaştırılmasının önemli olduğu uygulamalarda TCP'yi işlevsel hâle getirir. TCP başlığı, iletişimin düzenli biçimde yürütülmesini sağlayan kontrol alanlarını içerir. Bu alanlar sayesinde kaynak ve hedef uygulamalar belirlenir, veri sırası takip edilir, alıcının kabul edebileceği veri miktarı bildirilir ve iletim sırasında oluşabilecek hatalar denetlenir. TCP'nin temel amacı, verinin eksiksiz ve doğru sırayla hedefe ulaşmasını desteklemektir (Görsel 2.11).



Görsel 2.11: TCP başlık yapısı

Source Port 16 Bits (Kaynak Portu): Veriyi gönderen uygulamanın port numarasını taşır. Böylece segmentin hangi istemci veya uygulama sürecinden geldiği anlaşılır. Örneğin bir tarayıcı geçici bir kaynak port kullanarak web sunucusuna bağlanabilir.

Destination Port 16 Bits (Hedef Portu): Verinin hedefte hangi uygulamaya teslim edileceğini gösterir. Örneğin 80 numaralı port web servisiyle, 22 numaralı port SSH ile ilişkilendirilebilir. TCP'nin uygulamaları birbirinden ayırmasında bu alan kritik önemdedir.

Sequence Number 32 Bits (Sıra Numarası): Gönderilen veri akışındaki konumu gösterir. Alıcı taraf bu alan sayesinde verileri doğru sırayla birleştirebilir ve eksik segmentleri fark edebilir. TCP'nin sıralı ve güvenilir iletim sağlamasında temel alanlardan biridir.

Acknowledgment Number 32 Bits (Onay Numarası): Alıcının beklediği bir sonraki baytı belirtir. Bu alan "Şu ana kadarki veriyi aldım, sıradaki şu olsun." anlamına gelir. Bu mekanizma TCP'nin onaylama mantığını oluşturur.

Data Offset 4 Bits (Başlık Uzunluğu): TCP başlığının nerede bittiğini ve gerçek verinin nerede başladığını gösterir. Başlık uzunluğu sabit olmayabilir çünkü opsiyonlar eklenebilir. Bu alan, alıcı sistemin veriyi doğru yerden okumaya başlamasını sağlar.

Reserved 4 Bits (Ayrılmış Alan): Gelecekte kullanılabilecek özellikler için ayrılmıştır. Güncel standartta, gönderilen segmentlerde bu bitlerin sıfır olması beklenir. Alıcı taraf da bilmediği ek anlamlar varsa bunları yok sayar.

Bayraklar / Kontrol Bitleri: Bu bitler TCP bağlantısının durumunu ve segmentin amacını belirtir. Güncel olarak atanmış kontrol bitleri; CWR, ECE, URG, ACK, PSH, RST, SYN ve FIN'dir.

Window 16 Bits (Pencere Boyutu): Alıcının o anda ne kadar veri kabul edebileceğini gösterir. Bu alan, akış kontrolü için kullanılır. Bir başka ifadeyle gönderen, alıcının kapasitesini aşmadan veri yollar.

Checksum 16 Bits (Sağlama Toplamı): Segmentte hata olup olmadığını denetlemek için kullanılır. TCP bunu zorunlu olarak hesaplar, alıcı da kontrol ederek başlık veya veride bozulma olup olmadığını anlayabilir.

Urgent Pointer 16 Bits (Acil İşaretçisi): Acil veri mekanizmasıyla ilgili konumu belirtir. Bugün çok sık kullanılan bir alan değildir ama TCP standardında yer almaya devam eder.

Options + Padding (Seçenekler ve Doldurma): Başlıkta isteğe bağlı ek bilgiler taşınır. Örneğin MSS, Window Scale, SACK, Timestamp gibi alanlar burada bulunabilir. **Padding** ise başlığı 32 bit hizasına tamamlamak için eklenen doldurma bitleridir.

Data (Veri): Uygulamadan gelen gerçek kullanıcı verisidir. TCP başlığındaki tüm alanlar, aslında bu verinin doğru uygulamaya, doğru sırayla ve güvenilir biçimde ulaşmasını sağlamak için vardır.

TCP'de bağlantı kurulmadan önce üç yollu el sıkışma adı verilen süreç gerçekleşir (Görsel 2.12). Bu yapı, TCP'nin neden güvenilir iletişimle ilişkilendirildiğini açıkça gösterir.



Görsel 2.12: TCP üçlü el sıkışma adımları

TCP üçlü el sıkışma adımları şunlardır:

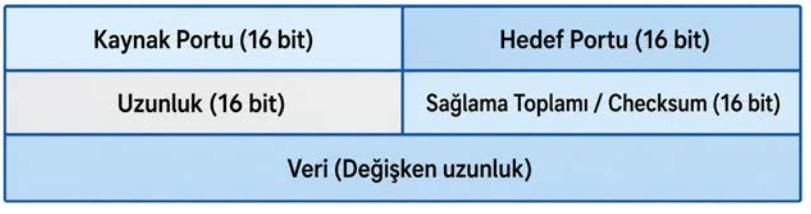
1. Adım: İstemci, sunucuya bir TCP bağlantısı kurmak istediğini bildirir. Bu amaçla sunucuya SYN bayrağı ayarlanmış bir segment gönderir. Bu segmentte yer alan **Seq = 100** değeri, istemcinin başlangıç sıra numarasını gösterir. Bu aşamada istemci, bağlantıyı başlatmış olur ve **SYN-SENT** durumuna geçer. Sunucu ise hâlâ bağlantı isteklerini dinleyen **LISTEN** durumundadır.

2. Adım: Sunucu, istemciden gelen SYN segmentini alır ve bağlantı isteğini kabul ettiğini bildirir. Bunun için istemciye **SYN + ACK** bayrakları ayarlanmış bir segment gönderir. Buradaki **Seq = 200** değeri, sunucunun kendi başlangıç sıra numarasını gösterir. **Ack = 101** değeri ise sunucunun, istemciden gelen **Seq = 100** değerini aldığını ve artık bir sonraki olarak **101** değerini beklediğini gösterir. Bu aşamada sunucu **SYN-RECEIVED** durumuna geçer.

3. Adım: İstemci, sunucudan gelen **SYN + ACK** segmentini aldığını bildirir. Bunun için sunucuya **ACK** bayrağı ayarlanmış bir segment gönderir. Bu segmentteki **Seq = 101** değeri, istemcinin bir sonraki sıra numarasını gösterir. **Ack = 201** değeri ise istemcinin sunucunun **Seq = 200** değerini aldığını ve artık **201** değerini beklediğini ifade eder. Bu son onaydan sonra TCP bağlantısı kurulmuş olur. İstemci ve sunucu **ESTABLISHED** durumuna geçer ve veri iletimi başlayabilir.

UDP Başlığı

Kullanıcı Veri Birimi Protokolü [User Datagram Protocol (UDP)], bağlantı kurulmasını gerektirmeden çalışan ve daha düşük protokol ek yüküyle veri iletimi sağlayan bir taşıma katmanı protokolüdür. TCP'ye göre daha sade bir başlık yapısına sahiptir. UDP, teslim sırasını veya verinin hedefe kesin olarak ulaştığını yerleşik olarak garanti etmez. Bununla birlikte daha az kontrol mekanizması kullanması, bazı uygulamalarda düşük gecikme avantajı sağlayabilir. UDP başlığı; kaynak portu, hedef portu, uzunluk ve sağlama toplamı alanlarından oluşur. Başlık alanlarının az olması, UDP'nin daha sade bir yapıda çalışmasını sağlar (Görsel 2.13).



Görsel 2.13: UDP datagram başlığı

Kaynak Portu (16 bit): Veriyi gönderen uygulamanın port numarasını gösterir. UDP datagramının hangi uygulamadan çıktığını belirtir. Örneğin bir istemci uygulama, veri gönderiyorsa onun port numarası burada yer alır.

Hedef Portu (16 bit): Verinin hedefte hangi uygulamaya teslim edileceğini gösterir. Alıcı cihazdaki ilgili servis veya uygulama bu port numarasına göre belirlenir.

Uzunluk (16 bit): UDP başlığı ile verinin toplam uzunluğunu gösterir. Sadece veri boyutunu değil başlık ve veri birlikte toplam kaç bayt tuttuğunu belirtir.

Sağlama Toplamı / Checksum (16 bit): Verinin iletim sırasında bozulup bozulmadığını kontrol etmek için kullanılır. Bir tür hata denetimi sağlar. Alıcı taraf bu alanı kontrol ederek datagramda bozulma olup olmadığını anlayabilir.

Veri (Değişken Uzunluk): Uygulamadan gelen gerçek kullanıcı verisini taşır. Başlık dışındaki asıl içerik burada bulunur. Bu veri, bazen çok kısa bazen daha uzun olabilir. Bu yüzden alanın uzunluğu sabit değildir.

UDP başlığı, TCP başlığına göre daha basit olduğundan veri iletimi daha hafif bir yapı üzerinden gerçekleştirilir ancak bu sadelik, teslim garantisinin ve sıra kontrolünün TCP kadar güçlü olmadığı anlamına gelir.

TCP ve UDP

TCP ve UDP arasındaki fark, ağ iletişiminde hangi önceliğin öne çıktığını gösterir. TCP daha kontrollü, güvenilir ve bağlantı odaklı bir yapı sunar. UDP ise daha sade, bağlantısız ve düşük ek yükle çalışan bir yapı sağlar. TCP'de veri sırası korunur, gerekli durumlarda onay mekanizması kullanılır ve kayıp veri yeniden gönderilebilir. Bu nedenle web erişimi, dosya aktarımı, e-posta gibi güvenilirliğin önemli olduğu uygulamalarda TCP daha uygun bir yapı sunar. UDP'de ise daha az kontrol bilgisi bulunur. Bu yaklaşımda teslim garantisi ve ayrıntılı sıra kontrolü TCP kadar güçlü değildir. Gerçek zamanlı tepkinin önemli olduğu bazı iletişim senaryolarında UDP daha uygun olabilir.

SIRA SİZDE

Aşağıdaki durumlarda TCP veya UDP protokollerinden hangisinin tercih edilmesi gerektiğini işaretleyiniz. Seçiminizin gerekçesini kısaca yazınız.

Durum	TCP	UDP	Gerekçeniz
Bir dosyanın eksiksiz ve doğru sırayla karşı tarafa ulaştırılması gerekmektedir.	☐	☐	
Gerçek zamanlı ses aktarımında düşük gecikme önceliklidir.	☐	☐	
İletimden önce bağlantı kurulması ve verilerin onaylanması istenmektedir.	☐	☐	
Daha düşük protokol ek yüküyle veri iletimi yapılması önceliklidir.	☐	☐	

Aşağıdaki TCP bağlantı kurma adımlarını gerçekleşme sırasına göre numaralandırınız.

Sıra	TCP İletisi
	ACK
	SYN
	SYN + ACK

2.1.9. Ağ Katmanı

Ağ katmanı, OSI referans modelinin üçüncü katmanıdır. Bu katman, verinin yalnızca aynı yerel ağ içinde değil farklı ağlar arasında da hedefe ulaştırılmasını sağlar. Ağ katmanının temel görevleri arasında mantıksal adresleme, yönlendirme, paket iletimi ve uygun yolun belirlenmesi bulunur. Ağ katmanında protokol veri birimi **paket** olarak adlandırılır. Paketlerin kaynak cihazdan hedef cihaza ulaşabilmesi için IP [Internet Protocol (İnternet Protokolü)] kullanılır. IP, cihazlara mantıksal adresler vererek paketlerin hangi kaynaktan geldiğini ve hangi hedefe ulaşması gerektiğini belirler. IPv4 ve IPv6, bu protokolün yaygın olarak kullanılan iki sürümüdür.

Ağ katmanı, yönlendiriciler aracılığıyla paketlerin farklı ağlar arasında uygun yollar üzerinden ilerlemesini sağlar. Böylece internet gibi geniş ölçekli ağ yapılarında iletişim gerçekleştirilebilir. Bu katmanda yalnızca veri iletimi değil hata bildirimleri ve ağ tanılama işlemleri de önemlidir. ICMP[Internet Control Message Protocol (İnternet Kontrol Mesaj Protokolü)], IP tabanlı iletişimde hata, durum ve erişilebilirlik bilgilerinin iletilmesine katkı sağlar. Bir hedefe ulaşılamadığında, paketin yaşam süresi dolduğunda veya bağlantı testi yapılmak istendiğinde ICMP mesajlarından yararlanılabilir.

Sayı Sistemleri

Bilgisayarlar verileri ikili sayı sistemiyle işler ancak insanların bilgileri daha kolay okuyabilmesi ve yazabilmesi için bazı değerler onluk veya on altılı sayı sistemiyle gösterilir. Ağ teknolojilerinde özellikle IP adreslerinin, alt ağ maskelerinin ve IPv6 adreslerinin anlaşılabilmesi için sayı sistemleri arasında dönüşüm yapılabilmesi önemlidir.

İkili Sayı Sistemi (Binary): İkili sayı sistemi, yalnızca 0 ve 1 rakamlarından oluşan ve bilgisayarların verileri işlemek için kullandığı temel sayı sistemidir (Görsel 2.14). Bu sistem 2 tabanına dayanır ve her basamağın değeri ikinin kuvvetlerine göre belirlenir. Bilgisayarlar elektronik yapıları gereği verileri açık-kapalı, var-yok veya yüksek-düşük gibi iki farklı durumla temsil edebildiği için ikili sayı sistemiyle çalışır. İkili sistemde yer alan her bir **0** veya **1**'e **bit** adı verilir ve 8 bit bir araya gelerek 1 baytı (byte) oluşturur. Ağ katmanında ikili sayı sistemi özellikle IP adreslerinin, alt ağ maskelerinin ve yönlendirme işlemlerinin anlaşılmasında büyük önem taşır.



Görsel 2.14: İkili sayı sisteminde veri gösterimi

Örnek: $(11110011)_2$ Sayısını Onluk Sayı Sistemine Dönüştürme

İkili sayı sistemindeki her basamak, sağdan sola doğru ikinin kuvvetleriyle çarpılır.

$(11110011)_2 =$

$1 \times 2^7 + 1 \times 2^6 + 1 \times 2^5 + 1 \times 2^4 + 0 \times 2^3 + 0 \times 2^2 + 1 \times 2^1 + 1 \times 2^0$

$= 128 + 64 + 32 + 16 + 0 + 0 + 2 + 1$

$= 243$

$(11110011)_2 = (243)_{10}$

Onluk sistemdeki bir sayının ikili sistemdeki karşılığını bulmak için sayı, sürekli ikiye bölünerek elde kalan bir (1) ve sıfır (0) değerleri sağdan sola doğru yazılır.

Örnek: $(68)_{10}$ Sayısını İkili Sayı Sistemine Dönüştürme

Onluk sayı sistemindeki sayı sürekli ikiye bölünür. Kalan değerler aşağıdan yukarıya doğru okunur.

İşlem	Kalan
68 ÷ 2 = 34	0
34 ÷ 2 = 17	0
17 ÷ 2 = 8	1
8 ÷ 2 = 4	0
4 ÷ 2 = 2	0
2 ÷ 2 = 1	0
1 ÷ 2 = 0	1

Kalanlar aşağıdan yukarıya doğru okunduğunda

$(68)_{10} = (1000100)_2$

Onluk (Decimal) Sayı Sistemi: Günlük yaşamda en sık kullanılan sistemdir. Bu sistemde 0'dan 9'a kadar rakamlar kullanılır ve her basamağın değeri 10'un kuvvetlerine göre belirlenir. Ağ adresleri kullanıcıya sunulurken de özellikle IPv4 adresleri onlu sistemle gösterilir. Böylece adresler daha okunabilir ve yazılabilir hâle gelir.

Örnek: $(150)_{10}$ Sayısının Basamak Değerlerini Gösterme

$(150)_{10} =$

$1 \times 10^2 + 5 \times 10^1 + 0 \times 10^0$

$= 100 + 50 + 0$

$= 150$

Onaltılık (Hexadecimal) Sayı Sistemi: 16 tabanına dayanan bir sayı sistemidir ve 0, 1, 2, 3, 4, 5, 6, 7, 8, 9 rakamları ile A, B, C, D, E ve F sembollerini kullanır. Bu sistemde A = 10, B = 11, C = 12, D = 13, E = 14 ve F = 15 değerini ifade eder. Bilgisayar sistemlerinde büyük ikili sayıların daha kısa ve düzenli biçimde gösterilmesi için onaltılık sayı sistemi kullanılır. Özellikle ağ katmanında IPv6 adreslerinin yazımında onaltılık gösterim önemli bir yere sahiptir. Onaltılık sayı sistemi, ikili sayı sistemiyle doğrudan ilişkilidir çünkü her 4 bitlik ikili grup, bir onaltılık değere karşılık gelir. Örneğin 1010 ikili sayısı onluk sistemde 10'a, onaltılık sistemde ise A'ya eşittir. Bu nedenle onaltılık sayı sistemi hem bilgisayarların çalışma mantığını anlamada hem de ağ teknolojilerinde adresleme ve veri gösterimini kolaylaştırmada önemli bir sayı sistemidir.

Örnek: $(4ACD8)_{16}$ Sayısını İkili Sayı Sistemine Dönüştürme

Her on altılı rakam dört bitlik ikili karşılığıyla yazılır.

On Altılı Rakam	4	A	C	D	8
İkili Karşılığı	0100	1010	1100	1101	1000

Gruplar yan yana yazıldığında

$(4ACD8)_{16} = (01001010110011011000)_2$

Örnek: $(11110000101010111110)_2$ Sayısını On Altılı Sayı Sistemine Dönüştürme

İkili sayı, sağdan sola doğru dörderli gruplara ayrılır. Ardından her grup bir on altılı sembolle eşleştirilir.

İkili Grup	1111	0000	1010	1011	1110
On Altılı Karşılığı	F	0	A	B	E

Sonuç

$(11110000101010111110)_2 = (F0ABE)_{16}$

1. UYGULAMA

Uygulama Adı	Sayı Sistemleri Arasında Dönüşüm Yapmak
Süre	25 dakika
Amaç	İkili, onluk ve on altılı sayı sistemleri arasında dönüşüm yapmak
Yönerge	Aşağıdaki dönüşüm işlemlerini gerçekleştiriniz. İşlem basamaklarını ilgili alanlara düzenli biçimde yazınız. Çalışmanızın sonunda IPv4 ve IPv6 adreslerinde kullanılan sayı gösterimlerinin ağ adresleme mantığı açısından neden önemli olduğunu açıklayınız. Cevaplarınızı tamamladıktan sonra sonuçlarınızı arkadaşınızın cevaplarıyla karşılaştırınız.

1.Bölüm: İkili Sayı Sisteminden Onluk Sayı Sistemine Dönüştürmek

İkili Sayı	İşlem Basamakları	Onluk Karşılığı
$(11110000)_2$		
$(10101010)_2$		

2.Bölüm: Onluk Sayı Sisteminden İkili Sayı Sistemine Dönüştürmek

Onluk Sayı	Bölme İşlemleri	İkili Karşılığı
$(101)_{10}$		
$(168)_{10}$		

3.Bölüm: Onluk Sayının Basamak Değerlerini Yazmak

Onluk Sayı	Basamak Değerlerine Ayrılmış Biçimi
$(16870)_{10}$	

4.Bölüm: On Altılı Sayı Sisteminden İkili Sayı Sistemine Dönüştürmek

On Altılı Sayı	Dörder Bitlik Gruplar	İkili Karşılığı
$(3A7F)_{16}$		
$(B2C8)_{16}$		

5.Bölüm: İkili Sayı Sisteminden On Altılı Sayı Sistemine Dönüştürmek

İkili Sayı	Dörder Bitlik Gruplar	On Altılı Karşılığı
$(110101101011)_2$		
$(001111101010)_2$		

6.Bölüm: Sonucu Yorumlamak

IPv4 adreslerinde çoğunlukla onluk, IPv6 adreslerinde ise on altılı gösterimin kullanılmasının temel nedeni nedir?

.....

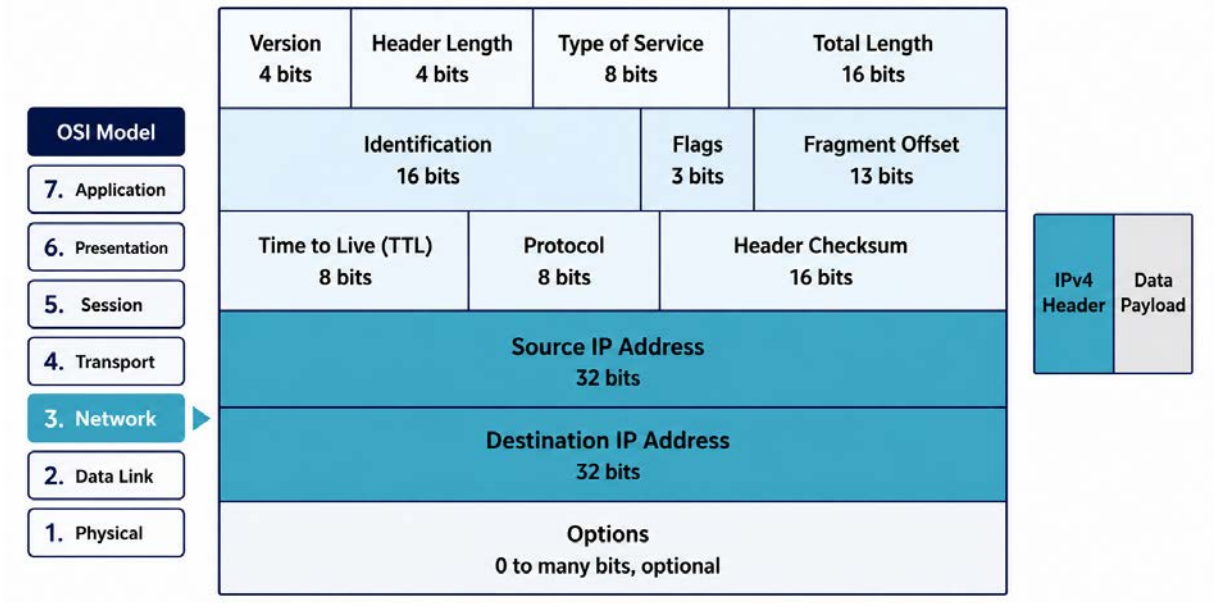
.....

Değerlendirme

Çalışmanız öğretmeniniz tarafından kontrol listesine göre değerlendirilecektir. Çalışmanızı yaparken buradaki ölçütleri dikkate alınız. Kontrol listesi formuna ulaşmak için karekodu okutunuz. Dijital yayınlarda karekodun üstüne tıklayarak içeriğe ulaşabilirsiniz.

2.1.10. IPv4 Protokolü

İnternet Protokolü sürüm 4 [Internet Protocol version 4 (IPv4)], ağ katmanında çalışan ve cihazların mantıksal olarak adreslenmesini sağlayan protokollerden biridir. Ağ üzerindeki cihazların tanımlanabilmesi ve verinin doğru hedefe ulaştırılabilmesi için her cihaza uygun bir IP adresi atanması gerekir. IPv4, bu adresleme yapısını kullanarak paketlerin kaynaktan hedefe yönlendirilmesine katkı sağlar. IPv4 bağlantısız çalışan bir protokoldür. Paket gönderilmeden önce kaynak ve hedef cihaz arasında doğrudan bir bağlantı kurulması gerekmez. IPv4, paketlerin hedefe kesin olarak ulaştırılacağını tek başına garanti etmez. Güvenilir iletimin gerekli olduğu durumlarda TCP gibi üst katman protokollerinin mekanizmalarından yararlanılır. IPv4 paketleri, başlık ve veri yükü olmak üzere iki temel bölümden oluşur. Başlıkta kaynak ve hedef IPv4 adresleri, yaşam süresi, üst katman protokolü, hata denetimi gibi iletim için gerekli bilgiler yer alır. Veri yükü bölümünde ise taşınan asıl içerik bulunur (Görsel 2.15).



Görsel 2.15: IPv4 başlık yapısı

Version: Paketin hangi IP sürümüne ait olduğunu gösterir ve IPv4 paketlerinde bu değer 4 bit olarak yer alır.

Header Length: IPv4 başlığının ne kadar uzun olduğunu belirtir ve alıcı cihazın başlığın nerede bitip veri bölümünün nerede başladığını anlamasını sağlar.

Type of Service: Paketin ağ üzerinde nasıl önceliklendirileceği veya hangi hizmet kalitesiyle ele alınacağına ilişkin bilgileri taşır.

Total Length: IP paketinin başlık ve veri bölümü dâhil olmak üzere toplam uzunluğunu gösterir.

Identification: Paket parçalandığında bu parçaların aynı pakete ait olduğunu belirlemek için kullanılan tanımlama bilgisini içerir.

Flags: Paketin parçalanıp parçalanmayacağını ve parçalanmış paketin devam parçalarının olup olmadığını gösteren kontrol bitlerini taşır.

Fragment Offset: Parçalanmış bir paketin her bölümünün orijinal paketin hangi kısmına ait olduğunu belirtir ve parçaların doğru sırayla birleştirilmesini sağlar.

Time To Live (TTL): Paketin ağda sonsuza kadar dolaşmasını önlemek için her yönlendiricide azaltılan bir sayaç görevi görür.

Protocol: IPv4 paketinin veri bölümünde hangi üst katman protokolünün bulunduğunu gösterir. Örneğin TCP, UDP veya ICMP bu alan üzerinden anlaşılır.

Header Checksum: Yalnızca IPv4 başlığında hata olup olmadığını kontrol etmek için kullanılan doğrulama bilgisini içerir.

Source IP Address: Paketi gönderen kaynağın IPv4 adresini taşır.

Destination IP Address: Paketin ulaşması gereken hedef cihazın IPv4 adresini gösterir.

Options: İsteğe bağlı ek denetim veya özel amaçlı bilgilerin başlığa eklenmesini sağlayan değişken uzunluklu alandır.

2.1.11. IPv4 Adres Yapısı

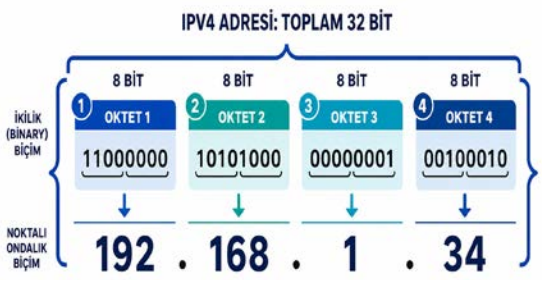
IPv4 adresi, toplam 32 bitten oluşur. Bu bitler, **oktet** adı verilen dört ayrı bölüm hâlinde gösterilir. Her oktet 8 bit uzunluğundadır ve onluk sayı sistemiyle yazıldığında 0 ile 255 arasında değer alabilir.

IPv4 adresleri, okunmasını kolaylaştırmak amacıyla noktalı onluk gösterimle yazılır. Örneğin aşağıdaki adres dört oktetten oluşur.

192.168.10.25

Oktet	Değer	İkili Karşılığı
1. oktet	192	11000000
2. oktet	168	10101000
3. oktet	10	00001010
4. oktet	25	00011001

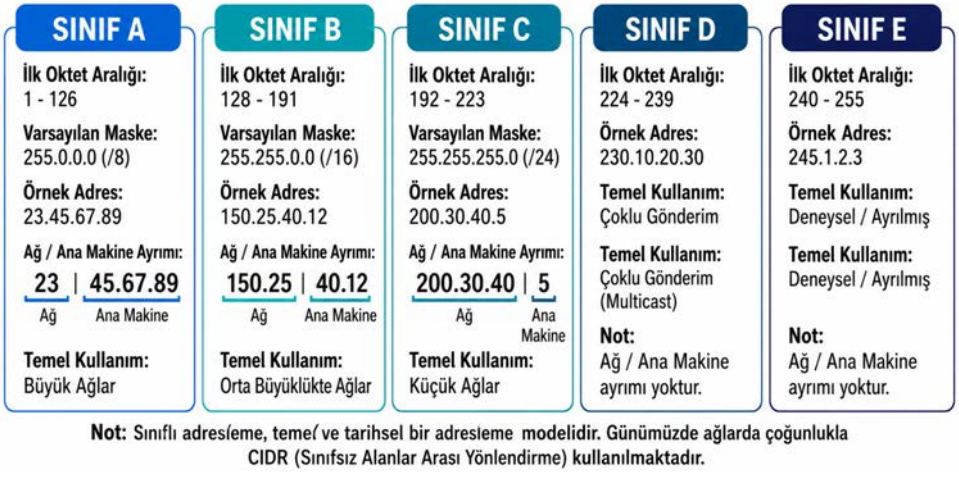
IPv4 adres yapısı Görsel 2.16'da gösterilmiştir.



Görsel 2.16: IPv4 adres yapısı

2.1.12. IPv4 Sınıflı Adresleme

IPv4 adresleri, tarihsel olarak adres alanının büyüklüğüne ve kullanım amacına göre sınıflara ayrılmıştır. Bu yaklaşım, ağ ve cihaz bölümlerinin belirli sınırlara göre ayrılmasını sağlar. Günümüzde adres alanının daha esnek kullanılabilmesi için CIDR ve alt ağlara bölme yöntemleri tercih edilmektedir. Bununla birlikte sınıflı adresleme yapısı, IPv4 adresleme mantığının anlaşılması açısından önemlidir. A, B ve C sınıflarında adresin belirli bir bölümü ağı, kalan bölümü ise ağ içindeki cihazı temsil eder (Görsel 2.17 ve 2.18). D sınıfı adresler tekil cihaz adreslemek için değil, multicast gruplarını tanımlamak için kullanılır. E sınıfı adresler ise normal cihaz adreslemesinde kullanılmaz.



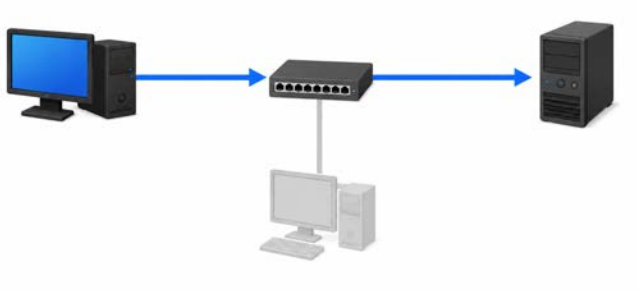
Görsel 2.17: IPv4 sınıflı adresleme yapısı

Adres Sınıfı	İlk Oktet Aralığı	İlk Oktetin İkilik Yapısı	Başlangıç Adresi	Bitiş Adresi	Varsayılan Alt Ağ Maskesi / Kullanım Türü
A	1-126	00000001 - 01111110	1.0.0.0	126.255.255.255	255.0.0.0
B	128-191	10000000 - 10111111	128.0.0.0	191.255.255.255	255.255.0.0
C	192-223	11000000 - 11011111	192.0.0.0	223.255.255.255	255.255.255.0
D	224-239	11100000 - 11101111	224.0.0.0	239.255.255.255	Çoklu Yayın
E	240-255	11110000 - 11111111	240.0.0.0	255.255.255.255	Rezerve

Görsel 2.18: IPv4 adres sınıflarının aralıkları

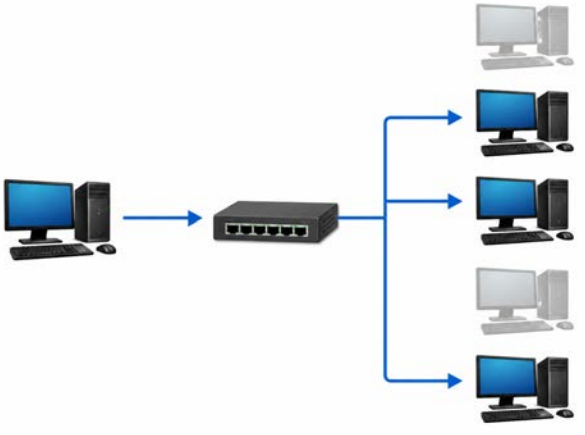
2.1.13. IPv4 Adres Türleri

IPv4 iletişiminde verinin hangi hedeflere gönderileceğine göre farklı adresleme türlerinden yararlanılır. Bu türler; tek bir cihaza, belirli bir cihaz grubuna veya yerel ağdaki bütün cihazlara yönelik iletişimi açıklar.



Görsel 2.19: Unicast yapısı

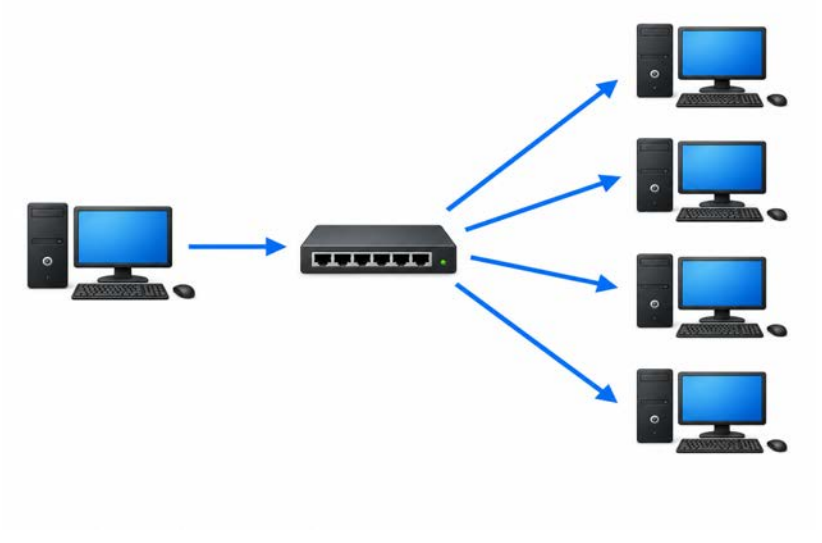
Unicast, verinin tek bir kaynaktan tek bir hedefe gönderilmesidir. Günlük ağ kullanımında en sık karşılaşılan iletişim biçimidir. Bir bilgisayarın belirli bir sunucuya bağlanması veya bir istemcinin belirli bir yazıcıya veri göndermesi unicast iletişime örnek verilebilir (Görsel 2.19).



Görsel 2.20: Multicast yapısı

Multicast, verinin belirli bir alıcı grubuna gönderilmesidir. Bu iletişim türünde veri bütün cihazlara değil, yalnızca ilgili gruba ulaştırılır. Aynı içeriğin seçilmiş birden fazla alıcıya gönderilmesi gereken durumlarda multicast kullanılabilir (Görsel 2.20).

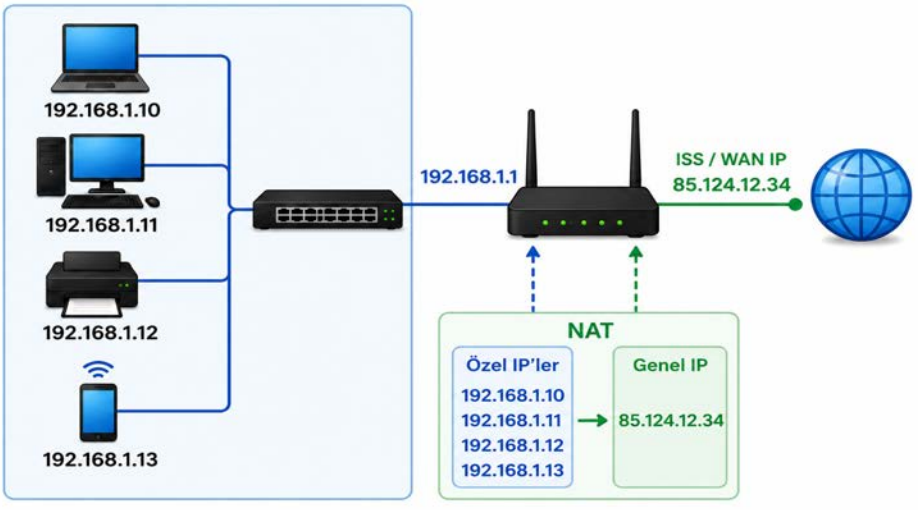
Broadcast, verinin aynı yayın alanında bulunan bütün cihazlara gönderilmesidir. Bazı ağ keşif ve duyuru işlemlerinde broadcast iletişimden yararlanılır. Broadcast trafiğinin gereksiz biçimde artması ağ performansını olumsuz etkileyebileceği için bu yapı kontrollü biçimde kullanılmalıdır (Görsel 2.21).



Görsel 2.21: Broadcast yapısı

2.1.14. Özel IPv4 Adres Aralıkları (Private IP Addresses)

Özel IPv4 adresleri, yerel ağlarda kullanılmak üzere ayrılmış adres bloklarıdır. Bu adresler ev, okul, laboratuvar ve kurum ağlarında yaygın biçimde kullanılır. Özel adresler internet üzerinde doğrudan genel yönlendirme amacıyla kullanılmaz (Görsel 2.22).



Görsel 2.22: Özel IPv4 adreslerinin çalışma yapısı

Özel adres aralıkları sayesinde farklı kurumlar kendi iç ağlarında aynı adres bloklarını kullanabilir. Örneğin iki farklı okulun laboratuvarında 192.168.1.0/24 ağı kullanılabilir. Bu adresler, yalnızca ilgili yerel ağ içinde anlamlıdır (Görsel 2.23).

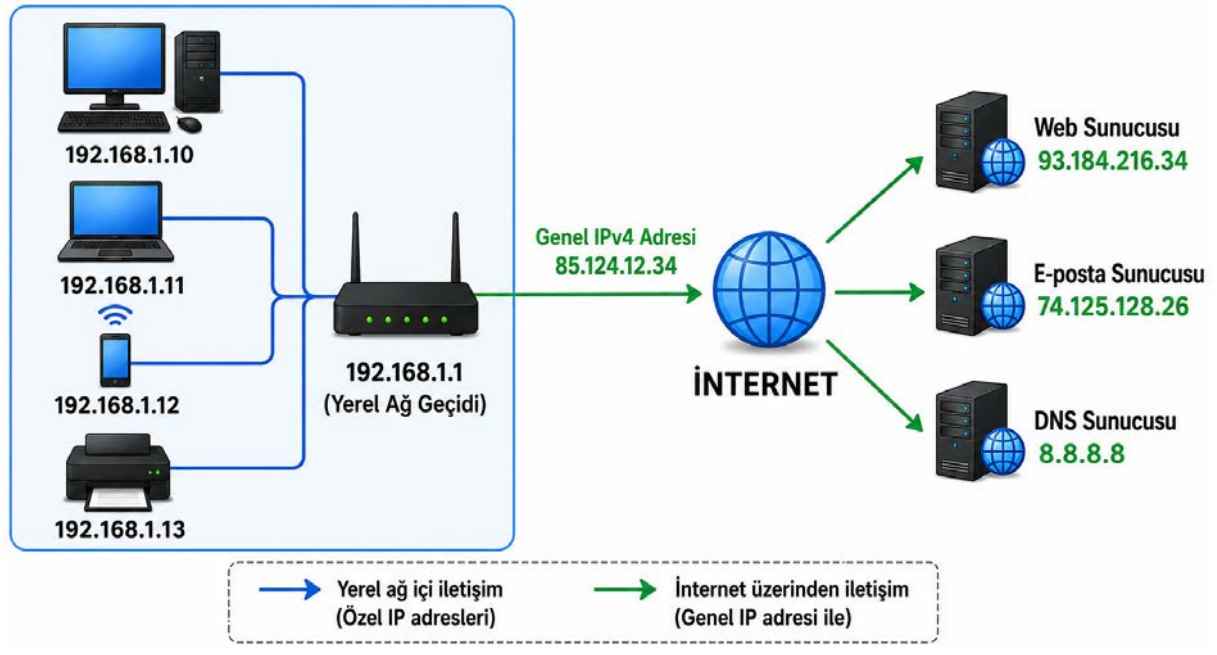
Adres Sınıfı	Özel IP Başlangıç Adresi	Özel IP Bitiş Adresi	Varsayılan Alt Ağ Maskesi
A	10.0.0.0	10.255.255.255	255.0.0.0
B	172.16.0.0	172.31.255.255	255.255.0.0
C	192.168.0.0	192.168.255.255	255.255.255.0

Görsel 2.23: Özel IPv4 adres aralıkları

2.1.15. Genel IPv4 Adresleri (Public IP Addresses)

Genel IPv4 adresleri, internet üzerinde yönlendirilebilen ve dış ağlarla iletişim kurulmasını sağlayan adreslerdir. Bu adresler, internet servis sağlayıcıları veya ilgili yetkili yapılar aracılığıyla kullanıma sunulur (Görsel 2.24).

Yerel ağdaki cihazlar çoğunlukla özel IPv4 adresleriyle çalışır. İnternet üzerindeki hizmetlere erişim sağlanırken dış ağlarla iletişim kurabilen genel adreslerden yararlanılır. Genel adresler ile özel adresler arasındaki temel fark, kullanım alanları ve internet üzerinde yönlendirilebilme durumlarıdır. Her özel adres aralığı dışında kalan IPv4 adresi doğrudan genel cihaz adresi olarak değerlendirilemez. Loopback, APIPA, multicast, ayrılmış adres blokları gibi özel amaçlı adresler de bulunmaktadır.



Görsel 2.24: Genel IPv4 adreslerinin çalışma şekli

2.1.16. Alt Ağ Maskesi

Alt ağ maskesi, bir IPv4 adresinin hangi bölümünün ağı, hangi bölümünün ise ağ içindeki cihazı temsil ettiğini belirleyen yapıdır. Bir IPv4 adresinin hangi ağa ait olduğunu anlayabilmek için IP adresi ile alt ağ maskesi birlikte değerlendirilir. Aynı ağ adresine sahip cihazlar çoğunlukla doğrudan iletişim kurabilir. Farklı ağlarda bulunan cihazların haberleşebilmesi için ise yönlendirici ve varsayılan ağ geçidi kullanılması gerekir. Bir IPv4 adresinin ağ adresini belirlemek için IP adresi ile alt ağ maskesine bit düzeyinde **AND işlemi** uygulanır. AND işleminde yalnızca karşılaştırılan iki bit de 1 olduğunda sonuç 1 olur. Diğer durumlarda sonuç 0 olarak belirlenir.

Birinci Bit	İkinci Bit	AND İşleminin Sonucu
0	0	0
0	1	0
1	0	0
1	1	1

Sınıflı IPv4 adresleme yaklaşımında kullanılan varsayılan alt ağ maskeleri ve ön ek uzunlukları şunlardır:

Adres Sınıfı	Varsayılan Alt Ağ Maskesi	Ön Ek Uzunluğu
Sınıf A	255.0.0.0	/8
Sınıf B	255.255.0.0	/16
Sınıf C	255.255.255.0	/24

Not: Varsayılan sınıflı maskeler, IPv4 adresleme mantığını anlamayı kolaylaştırır. Güncel ağ planlamasında ağlar yalnızca sınıf sınırlarına bağlı kalmadan farklı ön ek uzunluklarıyla bölünebilir.

1. Örnek: Bir IPv4 Adresinin Ağ Adresini Bulmak

192.168.1.10 IPv4 adresi ve 255.255.255.0 alt ağ maskesi birlikte değerlendirildiğinde ağ adresi aşağıdaki biçimde bulunur.

Değerlendirilen Unsur	Değer
IPv4 adresi	192.168.1.10
Alt ağ maskesi	255.255.255.0
Ön ek uzunluğu	/24
Ağ adresi	192.168.1.0

/24 gösterimi, ilk 24 bitin ağı temsil ettiğini belirtir. Bu nedenle son oktet cihazlara ayrılmıştır.

2. Örnek: İki IPv4 Adresi Aynı Ağda mı?

Varsayılan sınıflı adresleme yaklaşımına göre aşağıdaki iki adres şöyledir:

155.200.15.20

155.150.18.25

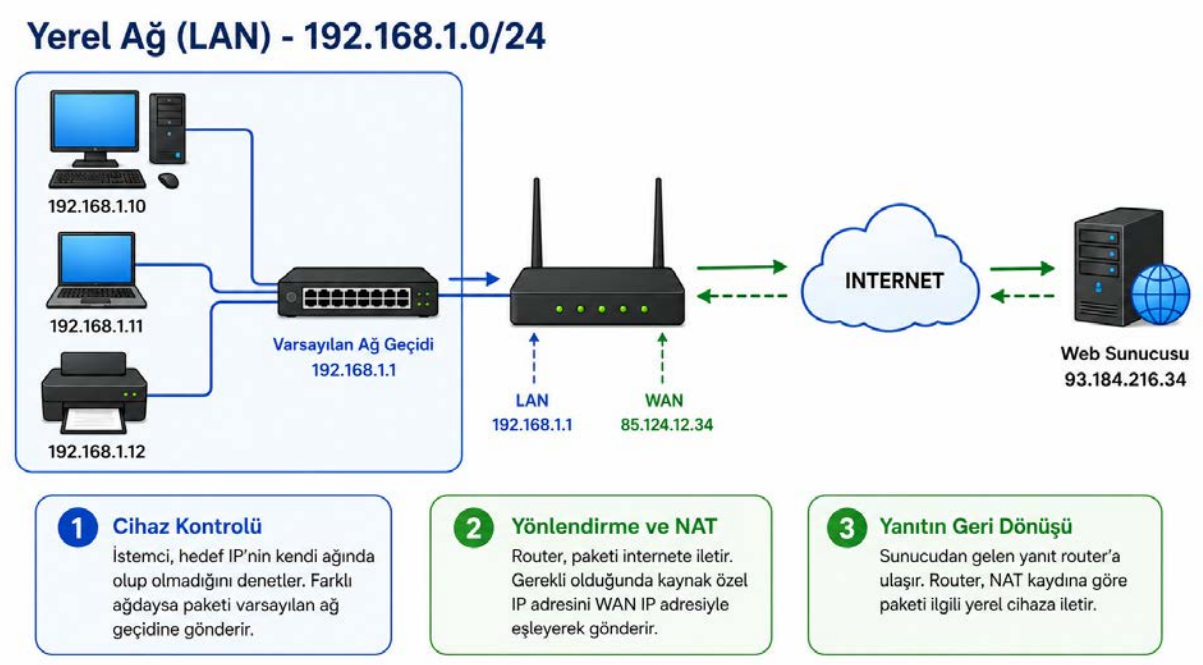
Bu adreslerin ilk okteti 155 olduğu için adresler Sınıf B aralığında yer alır. Varsayılan alt ağ maskesi 255.255.0.0, bir başka ifadeyle /16 olur.

IPv4 Adresi	Alt Ağ Maskesi	Ağ Adresi
155.200.15.20	255.255.0.0	155.200.0.0
155.150.18.25	255.255.0.0	155.150.0.0

Ağ adresleri farklı olduğu için bu iki cihaz aynı ağda değildir.

2.1.17. Varsayılan Ağ Geçidi

Varsayılan ağ geçidi (alt ağ geçidi), bir cihazın kendi yerel ağı dışındaki hedeflere ulaşmak için kullandığı çıkış noktasıdır. Bu görev genellikle yönlendiricinin ilgili yerel ağa bağlı arayüzü tarafından yerine getirilir. Aynı ağdaki cihazlar çoğunlukla doğrudan iletişim kurabilir ancak hedef cihaz farklı bir ağda bulunuyorsa veri önce varsayılan ağ geçidine gönderilir. Yönlendirici, paketin hedef adresini inceleyerek veriyi uygun ağa iletir. Bir istemciye tanımlanan varsayılan ağ geçidi adresinin, istemcinin bulunduğu yerel ağdan erişilebilir olması gerekir. Yanlış ağ geçidi adresi girildiğinde cihaz, aynı yerel ağdaki sistemlerle iletişim kurabilse bile farklı ağlara veya internete ulaşamayabilir (Görsel 2.25).



Görsel 2.25: Varsayılan ağ geçidinin çalışma yapısı

2.1.18. APIPA Adresi

Otomatik Özel IP Adresleme [Automatic Private IP Addressing (APIPA)], bir istemcinin DHCP sunucusundan otomatik IPv4 adresi alamadığı durumda kendisine geçici bir bağlantı-yerel adres atamasıyla ilgili yapıdır.

APIPA adresleri 169.254.0.0/16 adres bloğuyla ilişkilidir. Bir cihazda 169.254.x.x biçiminde bir adres görülmesi, çoğunlukla DHCP sunucusuna ulaşılamadığını veya otomatik adres alma sürecinin tamamlanamadığını düşündürür.

APIPA adresi kullanan cihaz, aynı yerel bağlantı üzerindeki uygun cihazlarla sınırlı iletişim kurabilir ancak bu adres yapısı, planlı ve kalıcı ağ kullanımı için tasarlanmamıştır. APIPA adresi alan bir istemci çoğunlukla yönlendirici üzerinden farklı ağlara veya internete erişemez.

Not: Bir istemcide APIPA adresi görülmesi, ağ kartının mutlaka arızalı olduğu anlamına gelmez. Öncelikle fiziksel bağlantı, DHCP hizmeti ve ağ yapılandırması kontrol edilmelidir.

2.1.19. Loopback Adresi

Loopback adresi, bir cihazın kendi TCP/IP iletişim yapısını sınamak amacıyla kullandığı özel adrestir. IPv4 için 127.0.0.0/8 adres bloğu loopback amacıyla ayrılmıştır. En yaygın kullanılan loopback adresi 127.0.0.1'dir. Bu adres, **localhost** adıyla da bilinir. Loopback adresine gönderilen veri fiziksel ağa çıkmaz. Veri, cihazın kendi içinde geri döner. Böylece ağ kartı, kablo, switch veya dış ağ bağlantısı kullanılmadan cihazın TCP/IP yapısı temel düzeyde sınanabilir. Ağ sorunları incelenirken loopback testi temel bir başlangıç noktasıdır. Loopback testi başarılı olduğunda cihazın kendi iç TCP/IP yapısının çalıştığı değerlendirilir. Ardından yerel ağ bağlantısı, varsayılan ağ geçidi ve dış ağ erişimi sırayla kontrol edilebilir.

Özellik	Açıklama
Ayrılmış IPv4 bloğu	127.0.0.0/8
Yaygın kullanılan adres	127.0.0.1
Yaygın adı	localhost
Temel kullanım amacı	Cihazın kendi TCP/IP yapısını sınamak
Veri fiziksel ağa çıkar mı?	Hayır

SIRA SİZDE

Aşağıdaki ağ durumlarını inceleyiniz ve cevaplarınızı tablodaki ilgili alanlara yazınız.

Durum	Cevabınız
192.168.10.25/24 ve 192.168.10.80/24 adreslerine sahip iki cihaz aynı ağda mıdır?	
192.168.10.25/24 adresine sahip bir cihazın 192.168.20.15/24 adresindeki sunucuya ulaşabilmesi için hangi ağ cihazı veya yapılandırma bilgisi gereklidir?	
Bir istemcide 169.254.18.42 adresi görülmektedir. Bu durum hangi kavramla ilişkilidir ve hangi sorun araştırılmalıdır?	
Bir cihazın kendi TCP/IP yapısını fiziksel ağa çıkmadan sınamak için hangi adres kullanılabilir?	

2.1.20. IPv4 Alt Ağlara Bölme İşlemi

Alt ağlara bölme (subnetting), bir IPv4 ağının daha küçük ve yönetilebilir ağlara ayrılması işlemidir. Bu yöntem sayesinde büyük bir adres alanı; laboratuvar, idari bölüm veya öğretmenler odası gibi farklı kullanım alanlarına göre düzenlenebilir. Her alt ağ için ayrı bir **ağ adresi**, **yayın adresi (broadcast)** ve **kullanılabilir cihaz adresi aralığı** oluşur. Böylece adresleme planı daha anlaşılır hâle gelir, yayın trafiği sınırlandırılabilir ve ağ yönetimi kolaylaşır. Alt ağlara bölme işleminde cihaz bölümündeki bazı bitler ağ bölümüne aktarılır. Ağ bölümüne aktarılan bit sayısı arttıkça oluşturulabilecek alt ağ sayısı artar; ancak her alt ağda kullanılabilecek cihaz adresi sayısı azalır. IPv4 işlemlerinde kullanılan formüller Tablo 2.2'de verilmiştir.

Tablo 2.2: IPv4 Hesaplama Formülleri

Hesaplanacak Değer	Formül	Açıklama
Alt ağ sayısı	2^s	s, alt ağ oluşturmak amacıyla cihaz bölümünden ödünç alınan bit sayısıdır.
Bir alt ağdaki toplam adres sayısı	2^h	h, cihazlar için kalan bit sayısıdır.
Bir alt ağdaki kullanılabilir cihaz adresi sayısı	$2^h - 2$	Ağ adresi ve yayın adresi cihazlara verilemez.

Bir alt ağın adres aralığını belirleyebilmek için blok büyüklüğü hesaplanır. Son oktette işlem yapılan örneklerde blok büyüklüğü şu yöntemle bulunabilir:

Blok büyüklüğü = 256 – Alt ağ maskesinin ilgili oktetteki değeri

Örnek Çözüm: 192.168.10.0/24 Ağını 4 Eşit Alt Ağa Bölmek

192.168.10.0/24 ağı dört eşit alt ağa bölünecektir.

1. Adım: Gerekli Alt Ağ Bitini Belirlemek

Dört alt ağ oluşturulması gerektiği için şu hesaplama yapılır:

$2^2 = 4$

Cihaz bölümünden iki bit ağ bölümüne aktarılmalıdır.

/24 + 2 bit = /26

Yeni alt ağ maskesi şöyledir:

255.255.255.192

2. Adım: Blok Büyüklüğünü Hesaplamak

256 – 192 = 64

Alt ağlar son oktette 64 artarak ilerler.

3. Adım: Kullanılabilir Cihaz Adresi Sayısını Hesaplamak

/26 ağında cihazlar için altı bit kalır.

$2^6 – 2 = 62$

Her alt ağda 62 kullanılabilir cihaz adresi bulunur.

4. Adım: Alt Ağları Tabloya Yazmak

Alt Ağ	Ağ Adresi	İlk Kullanılabilir Adres	Son Kullanılabilir Adres	Yayın Adresi
1	192.168.10.0/26	192.168.10.1	192.168.10.62	192.168.10.63
2	192.168.10.64/26	192.168.10.65	192.168.10.126	192.168.10.127
3	192.168.10.128/26	192.168.10.129	192.168.10.190	192.168.10.191
4	192.168.10.192/26	192.168.10.193	192.168.10.254	192.168.10.255

2. UYGULAMA

Uygulama Adı	Fabrika Ağı İçin IPv4 Alt Ağ Adresleme Planı Hazırlamak
Süre	25 dakika
Amaç	Verilen kurum senaryosuna göre IPv4 ağını eşit büyüklükte alt ağlara bölerek her bölüm için ağ adresi, kullanılabilir cihaz adres aralığı ve yayın adresinden oluşan adresleme planı hazırlamak
Yönerge	192.168.10.0/24 ağını, yeni açılan bir fabrikadaki sekiz bölüm için eşit büyüklükte alt ağlara ayırınız. Hesaplama adımlarını tamamlayarak tabloyu doldurunuz.

1. Bölüm: Hesaplama Adımlarını Tamamlamak

Hesaplanacak Değer	Cevabınız
Gerekli alt ağ sayısı	
Cihaz bölümünden ödünç alınması gereken bit sayısı	
Yeni ön ek uzunluğu	
Yeni alt ağ maskesi	
Blok büyüklüğü	
Her alt ağdaki toplam adres sayısı	
Her alt ağdaki kullanılabilir cihaz adresi sayısı	

2. Bölüm: Alt Ağları Belirlemek

Bölüm	Ağ Adresi	İlk Kullanılabilir Adres	Son Kullanılabilir Adres	Yayın Adresi
1. Bölüm				
2. Bölüm				
3. Bölüm				
4. Bölüm				
5. Bölüm				
6. Bölüm				
7. Bölüm				
8. Bölüm				

3. Bölüm: Sonucu Yorumlamak

Aşağıdaki soruları cevaplayınız.

1. Yeni alt ağ maskesi neden /27 olmuştur?

.....

.....

2. Her alt ağda kaç kullanılabilir cihaz adresi bulunmaktadır?

.....

.....

3. Bütün bölümlerin aynı sayıda cihaza sahip olmadığı bir kurumda, eşit büyüklükte alt ağlar kullanılması adres israfına yol açabilir mi? Açıklayınız.

.....

.....

Değerlendirme

Çalışmanız öğretmeniniz tarafından analitik dereceli puanlama anahtarına göre değerlendirilecektir. Çalışmanızı yaparken buradaki ölçütleri dikkate alınız. Analitik dereceli puanlama anahtarı formuna ulaşmak için karekodu okutunuz. Dijital yayınlarda karekodun üstüne tıklayarak içeriğe ulaşabilirsiniz.

2.1.21. VLSM ile IP Adresi Planlama

Değişken Uzunluklu Alt Ağ Maskesi [Variable Length Subnet Mask (VLSM)], bir ana ağın farklı büyüklükteki alt ağlara ayrılmasını sağlayan yöntemdir. Eşit alt ağlara bölme işleminde bütün alt ağlar aynı büyüklükte oluşturulur. VLSM yönteminde ise her bölüm için gerekli cihaz sayısı ayrı ayrı değerlendirilir ve ihtiyacı karşılayan en küçük uygun adres bloğu seçilir.

Bu yöntem, IPv4 adreslerinin daha verimli kullanılmasını sağlar. Örneğin altmış cihaz bulunan bir laboratuvar ile on cihaz bulunan bir müdürlük için aynı büyüklükte ağ ayrılması gereksiz adres kullanımına yol açabilir. VLSM kullanıldığında laboratuvara daha büyük, müdürlüğe ise daha küçük bir alt ağ verilebilir. VLSM planlamasında şu aşamalar izlenir:

1. Bölümlerin cihaz gereksinimleri belirlenir.
2. Bölümler, ihtiyaç duydukları cihaz sayısına göre büyükten küçüğe sıralanır.
3. Her bölüm için ihtiyacı karşılayan en küçük alt ağ seçilir.
4. En büyük alt ağdan başlanarak uygun adres blokları sırayla yerleştirilir.
5. Ağ adresi, kullanılabilir cihaz aralığı ve yayın adresi tabloya yazılır.
6. Ayrılmamış adres alanları ileride kullanılmak üzere belirlenir.

Örnek Çözüm: Okul Birimleri İçin VLSM Planlaması

Bir okulda aşağıdaki birimler için IP adresi planlaması yapılacaktır.

Birim	Cihaz Gereksinimi
Bilgisayar laboratuvarı	60
Öğretmenler odası	25
Müdürlük	10

Kullanılacak Ana Ağ: 192.168.1.0/24

1. Adım: Gereksinimleri Büyükten Küçüğe Sıralamak

Sıra	Birim	Gerekli Cihaz Sayısı
1	Bilgisayar laboratuvarı	60
2	Öğretmenler odası	25
3	Müdürlük	10

2. Adım: Bilgisayar Laboratuvarı İçin Uygun Ağı Belirlemek

$2^5 - 2 = 30$ —> Yetersiz

$2^6 - 2 = 62$ —> Yeterli

Altı cihaz biti kaldığında ön ek uzunluğu /26 olur.

Özellik	Değer
Verilen ağ	192.168.1.0/26
Alt ağ maskesi	255.255.255.192
İlk kullanılabilir adres	192.168.1.1
Son kullanılabilir adres	192.168.1.62
Yayın adresi	192.168.1.63

3. Adım: Öğretmenler Odası İçin Uygun Ağı Belirlemek

$2^4 - 2 = 14$ —> Yetersiz

$2^5 - 2 = 30$ —> Yeterli

Beş cihaz biti kaldığında ön ek uzunluğu /27 olur.

Özellik	Değer
Verilen ağ	192.168.1.64/27
Alt ağ maskesi	255.255.255.224
İlk kullanılabilir adres	192.168.1.65
Son kullanılabilir adres	192.168.1.94
Yayın adresi	192.168.1.95

4. Adım: Müdürlük İçin Uygun Ağı Belirlemek

$2^3 - 2 = 6$ —> Yetersiz

$2^4 - 2 = 14$ —> Yeterli

Dört cihaz biti kaldığında ön ek uzunluğu /28 olur.

Özellik	Değer
Verilen ağ	192.168.1.96/28
Alt ağ maskesi	255.255.255.240
İlk kullanılabilir adres	192.168.1.97
Son kullanılabilir adres	192.168.1.110
Yayın adresi	192.168.1.111

5. Adım: VLSM Planını Tabloya Aktarmak

Birim	Gereksinim	Verilen Ağ	İlk Kullanılabilir Adres	Son Kullanılabilir Adres	Yayın Adresi
Bilgisayar laboratuvarı	60	192.168.1.0/26	192.168.1.1	192.168.1.62	192.168.1.63
Öğretmenler odası	25	192.168.1.64/27	192.168.1.65	192.168.1.94	192.168.1.95
Müdürlük	10	192.168.1.96/28	192.168.1.97	192.168.1.110	192.168.1.111

Ayrılmayan adres alanı, ileride yapılabilecek genişletmeler için kullanılabilir.

3. UYGULAMA

Uygulama Adı	VLSM ile IP Adresi Planlamak
Süre	35 dakika
Amaç	Farklı cihaz gereksinimlerine sahip bölümler için en uygun alt ağ büyüklüklerini belirleyerek verimli bir IPv4 adresleme planı oluşturmak
Yönerge	Bir fabrikadaki bölümler için 172.16.0.0/24 ana ağı kullanılacaktır. Bölümlerin cihaz gereksinimlerini büyükten küçüğe sıralayınız. Her bölüm için ihtiyacı karşılayan en küçük uygun alt ağı belirleyiniz. Ardından VLSM planlama tablosunu doldurunuz.

1. Bölüm: Gereksinimleri Sıralamak

Bölüm	Cihaz Gereksinimi	Büyükten Küçüğe Sırası
Muhasebe	50	
Güvenlik sistemi	10	
Üretim	100	
Depo	20	

2. Bölüm: Uygun Alt Ağları Belirlemek

Bölüm	Gerekli Cihaz Sayısı	En Küçük Uygun Cihaz Biti Sayısı	Kullanılabilir Adres Sayısı	Ön Ek Uzunluğu	Alt Ağ Maskesi
Üretim	100				
Muhasebe	50				
Depo	20				
Güvenlik sistemi	10				

3. Bölüm: VLSM Planlama Tablosunu Tamamlamak

Bölüm	Gereksinim	Verilen Ağ	İlk Kullanılabilir Adres	Son Kullanılabilir Adres	Yayın Adresi
Üretim	100				
Muhasebe	50				
Depo	20				
Güvenlik sistemi	10				

4. Bölüm: Sonucu Yorumlamak

Aşağıdaki soruları cevaplayınız.

1. VLSM planlamasında bölümlerin neden büyükten küçüğe sıralanması gerekir?

   .....
   .....

2. Bütün bölümlere aynı büyüklükte ağ verilseydi hangi sorun ortaya çıkabilirdi?

   .....
   .....

3. Planlama tamamlandığında kullanılmadan kalan adres aralığını yazınız.

   .....

4. Eşit alt ağlara bölme yöntemi ile VLSM arasındaki temel fark nedir?

   .....
   .....

Değerlendirme

Çalışmanız öğretmeniniz tarafından analitik dereceli puanlama anahtarına göre değerlendirilecektir. Çalışmanızı yaparken buradaki ölçütleri dikkate alınız. Analitik dereceli puanlama anahtarı formuna ulaşmak için karekodu okutunuz. Dijital yayınlarda karekodun üstüne tıklayarak içeriğe ulaşabilirsiniz.

2.1.22. IPv6 Protokolü

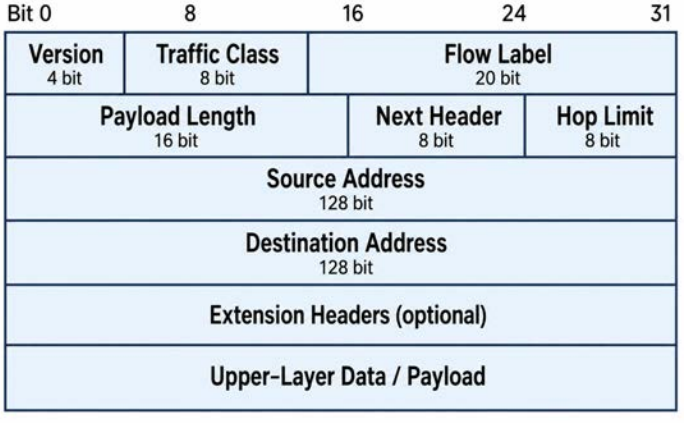
İnternet Protokolü sürüm 6 [Internet Protocol version 6 (IPv6)], ağ üzerindeki cihazların daha geniş bir adres alanı içinde tanımlanabilmesini sağlayan yeni nesil internet protokolüdür. İnternete bağlanan bilgisayarların, mobil cihazların, sunucuların ve diğer ağ bileşenlerinin sayısının artması, daha geniş bir adresleme yapısına ihtiyaç duyulmasına yol açmıştır. IPv4 adresleri 32 bit uzunluğundayken IPv6 adresleri 128 bit uzunluğundadır. Bu yapı, IPv6'nın çok daha geniş bir adres alanı sunmasını sağlar. IPv6 yalnızca adres sayısını artırmak amacıyla geliştirilmemiştir. Aynı zamanda yeni nesil ağ gereksinimlerine daha uygun, esnek ve düzenli bir adresleme yapısı oluşturmayı amaçlar.

IPv6 adresleri, okunabilirliği artırmak amacıyla on altılı sayı sistemiyle yazılır. Bir IPv6 adresi, iki nokta (:) işaretiyle ayrılan sekiz gruptan oluşur. Her grup 16 bit uzunluğundadır ve dört on altılı sembolle gösterilebilir.

Örnek bir IPv6 adresi şöyledir.

2001:0db8:abcd:0012:0000:0000:0000:0025

IPv6 adreslerinde gereksiz sıfırlar belirli kurallara göre kaldırılabilir. Böylece uzun adresler daha kısa ve okunabilir biçimde yazılabilir. IPv6 başlık yapısı Görsel 2.26'da gösterilmiştir.



Görsel 2.26: IPv6 Başlık yapısı

BİLGİ KUTUSU : IPv6'nın Sağladığı Ek Kolaylıklar

IPv6, yalnızca daha fazla adres üretmek için geliştirilmiş bir protokol değildir. Aynı zamanda ağların daha düzenli, esnek ve yönetilebilir biçimde çalışmasına katkı sağlar. IPv6 ile birlikte adresleme yapısı daha hiyerarşik bir hâl aldığı için büyük ağlarda yönlendirme işlemleri daha verimli gerçekleştirilebilir. Bu durum, internet omurgasında yönlendirme tablolarının daha düzenli tutulmasına yardımcı olur. IPv6'nın önemli özelliklerinden biri, cihazların ağa bağlandıklarında bazı yapılandırma bilgilerini otomatik olarak alabilmesidir. Böylece istemci cihazlar, uygun durumlarda kendi IPv6 adreslerini oluşturabilir ve ağa daha kolay katılabilir. Bu özellik özellikle çok sayıda cihazın bulunduğu ortamlarda yapılandırma sürecini kolaylaştırır. IPv6'da yayın (broadcast) yerine çoklu gönderim (multicast), isteğe bağlı grup iletişimi gibi daha verimli iletişim yaklaşımları tercih edilir. Bu sayede ağ üzerindeki gereksiz trafik azaltılabilir. Ayrıca IPv6, yeni nesil ağ gereksinimlerini karşılayacak şekilde güvenlik, hareketlilik ve genişleyebilirlik açısından da daha uygun bir temel sunar.

IPv6 Başlık Alanları

IPv6 başlık alanlarıyla ilgili bilgiler Tablo 2.3'te verilmiştir.

Tablo 2.3: IPv6 Başlık Alanları

Başlık Alanı	Uzunluğu	Açıklama
Version (Sürüm)	4 bit	Pakette kullanılan IP sürümünü belirtir. IPv6 paketlerinde bu değer 6'dır.
Traffic Class (Trafik Sınıfı)	8 bit	Paketlerin öncelik veya hizmet sınıfı gibi bilgilere göre değerlendirilmesine yardımcı olur.
Flow Label (Akış Etiketi)	20 bit	Aynı veri akışına ait paketlerin ağ içinde ilişkilendirilebilmesini sağlar.
Payload Length (Veri Yükü Uzunluğu)	16 bit	IPv6 temel başlığından sonra gelen bölümün uzunluğunu bayt cinsinden gösterir. Ek başlıklar varsa bunlar da bu uzunluğa dâhildir.
Next Header (Sonraki Başlık)	8 bit	IPv6 temel başlığından sonra hangi başlığın geldiğini belirtir. Sonraki bölüm bir ek başlık veya doğrudan TCP, UDP veya ICMPv6 gibi bir üst katman başlığı olabilir.
Hop Limit (Atlama Sınırı)	8 bit	Paketin ağ üzerinde sonsuza kadar dolaşmasını önler. Paket her yönlendiriciden geçtiğinde değer bir azaltılır. Değer sıfıra ulaştığında paket atılır.
Source Address (Kaynak Adresi)	128 bit	Paketi gönderen cihazın IPv6 adresini taşır.
Destination Address (Hedef Adresi)	128 bit	Paketin gönderildiği hedef cihazın IPv6 adresini taşır.

Not: IPv6 yapısında isteğe bağlı bilgiler, temel başlığın içine yerleştirilmez. Gerektiğinde **ek başlıklar (extension headers)** kullanılır. Bu ek başlıklar, IPv6 temel başlığı ile üst katman verisi arasına eklenir. Üst katman verisi çoğunlukla TCP, UDP veya ICMPv6 başlığıyla taşınan veriden oluşur.

2.1.23. IPv6 Adres Yapısı

IPv6 adresleri 128 bit uzunluğundadır. Bu adresler, iki nokta (:) işaretiyle ayrılan sekiz adet 16 bitlik grup hâlinde yazılır. Şu IPv6 adresini inceleyiniz.

Grup Sırası	1. Grup	2. Grup	3. Grup	4. Grup	5. Grup	6. Grup	7. Grup	8. Grup
IPv6 Grubu	2001	0db8	abcd	0012	0000	0000	0000	0025
Bit Uzunluğu	16	16	16	16	16	16	16	16

Sekiz grubun toplam uzunluğu şöyle hesaplanır.

8 × 16 bit = 128 bit

IPv6 adresleri, bir ön ek uzunluğuyla birlikte yazılabilir. Verilen örnekte /64 ifadesi, adresin ilk 64 bitinin ağ ön eki olarak değerlendirildiğini gösterir.

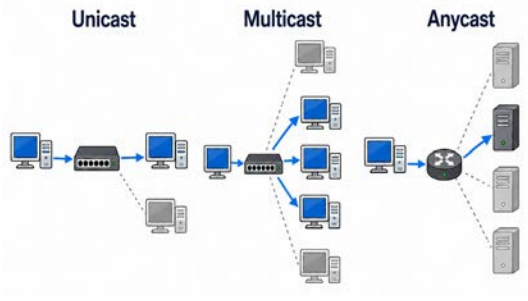
2001:0db8:abcd:0012:0000:0000:0000:0025/64

Adres Bölümü	Değer	Temel İşlev
Ağ ön eki	2001:0db8:abcd:0012	Arayüzün bağlı olduğu IPv6 ağını belirtir.
Arayüz kimliği	0000:0000:0000:0025	İlgili ağ içindeki arayüzün tanımlanmasına yardımcı olur.

Not: /64 ön ek uzunluğu yaygın kullanılan IPv6 ağlarında sıklıkla görülür ancak bütün IPv6 adreslerinin zorunlu olarak aynı biçimde bölündüğü düşünülmemelidir. Ön ek uzunluğu ağ planına göre belirlenir.

2.1.24. IPv6 Adres Türleri

IPv6 iletişiminde verinin hangi hedefe veya hedef grubuna gönderileceğine göre farklı adres türlerinden yararlanılır (Görsel 2.27). IPv6 adresleme yapısında unicast, multicast ve anycast adres türleri bulunur. Ayrıca cihazın kendi IPv6 iletişim yapısını sınamak amacıyla kullanılan loopback adresi vardır. IPv6'da IPv4'teki broadcast yaklaşımı aynı biçimde kullanılmaz. Birden fazla arayüze yönelik grup iletişiminde multicast adreslerden yararlanılır.



Görsel 2.27: IPv6 adres türleri

IPv6 adres türleri ve temel işlevleri Tablo 2.4'te verilmiştir.

Tablo 2.4: IPv6 Adres Türleri ve Temel İşlevleri

IPv6 Adres Türü	Temel İşlevi	Kullanım Örneği
Unicast	Verinin tek bir kaynak arayüzden tek bir hedef arayüze gönderilmesini sağlar.	Bir istemcinin belirli bir sunucuya erişmesi
Multicast	Verinin belirli bir alıcı grubuna gönderilmesini sağlar.	Aynı gruptaki arayüzlere yönelik keşif veya duyuru işlemleri
Anycast	Aynı adresin birden fazla arayüze atanabilmesini sağlar. Paket, yönlendirme ölçütlerine göre uygun arayüzlerden birine ulaştırılır.	Dağıtık hizmetlerde uygun sunucuya erişilmesi
Loopback	Cihazın kendi IPv6 iletişim yapısını fiziksel ağa çıkmadan sınamasını sağlar.	::1 adresiyle temel yerel test yapılması
Link-local	Aynı yerel bağlantı üzerindeki cihazların yönlendiriciye gerek duymadan iletişim kurmasını sağlar. Yönlendiriciler tarafından farklı ağlara aktarılmaz.	Aynı yerel ağdaki cihazların komşu keşfi ve otomatik yapılandırma işlemlerinde kullanılması

BİLGİ KUTUSU : Bir Arayüzde Birden Fazla IPv6 Adresi

Bir ağ arayüzüne aynı anda birden fazla IPv6 adresi atanabilir. Örneğin bir arayüz aynı yerel bağlantıdaki cihazlarla iletişim kurmak için bir link-local adresi, farklı ağlardaki cihazlara erişmek için ise yönlendirilebilir unicast adresi kullanabilir.

2.1.25. IPv6 Adreslerini Sadeleştirme

IPv6 adresleri uzun bir yapıya sahip olduğu için tam biçimleriyle yazıldıklarında okuma ve yazma güçlüğü oluşturabilir. Bu nedenle IPv6 adreslerinde belirli sadeleştirme kuralları uygulanır. Sadeleştirme işlemi adresin değerini değiştirmez yalnızca daha kısa ve okunabilir biçimde yazılmasını sağlar.

Birinci Kural: Grupların Başındaki Gereksiz Sıfırları Kaldırma

Her 16 bitlik grubun başında bulunan gereksiz sıfırlar kaldırılabilir.

Tam Gösterim	Sadeleştirilmiş Gösterim
004a	4a
0007	7
00b2	b2
0000	0

Bir grubun tamamı sıfırlardan oluşuyorsa grup, en az bir adet 0 ile gösterilir.

İkinci Kural: Ardışık Sıfır Gruplarını Kısaltma

Yalnızca sıfırlardan oluşan ardışık gruplar, iki adet iki nokta (::) işaretiyle kısaltılabilir.

Verilen adresi inceleyiniz.

2001:0db8:0000:0000:0000:0000:0000:0025

Öncelikle grupların başındaki gereksiz sıfırlar kaldırılır.

2001:db8:0:0:0:0:0:25

Ardından ardışık sıfır grupları :: ile kısaltılır.

2001:db8::25

:: işareti bir IPv6 adresinde yalnızca bir kez kullanılabilir çünkü adres yeniden tam biçimine dönüştürülmek istendiğinde kaç adet sıfır grubunun ekleneceğinin açıkça anlaşılması gerekir.

Bir IPv6 adresinde birden fazla sıfır dizisi varsa en uzun sıfır dizisi kısaltılır. Sıfır dizilerinin uzunlukları eşitse solda bulunan dizi tercih edilir.

Not: IPv6 adresleri yazılırken on altılı harflerin küçük yazılması tercih edilir. Örneğin 0DB8 yerine db8 yazılabilir.

Örnek Çözüm: IPv6 Adresini Sadeleştirmek

Aşağıdaki IPv6 adresini sadeleştiriniz.

2001:0db8:0000:0000:0000:ff00:0042:8329

1. Adım: Grupların Başındaki Gereksiz Sıfırları Kaldırmak

2001:db8:0:0:0:ff00:42:8329

2. Adım: Ardışık Sıfır Gruplarını Kısaltmak

2001:db8::ff00:42:8329

Sonuç

2001:db8::ff00:42:8329

4. UYGULAMA

Uygulama Adı	IPv6 Adreslerini Sadeleştirmek
Süre	25 dakika
Amaç	IPv6 adreslerindeki gereksiz sıfırları belirleyerek adresleri kurallara uygun ve okunabilir biçimde sadeleştirmek
Yönerge	Aşağıdaki IPv6 adreslerini sadeleştiriniz. Önce her grubun başındaki gereksiz sıfırları kaldırınız. Ardından uygun olan adreslerde ardışık sıfır gruplarını çift iki nokta (::) işaretiyle kısaltınız. Çift iki nokta (::) işaretinin bir IPv6 adresinde yalnızca bir kez kullanılabileceğini unutmayınız.

Sıra	Tam IPv6 Adresi	Baştaki Sıfırlar Kaldırıldıktan Sonraki Biçimi	Sadeleştirilmiş Biçimi
1	2001:0db8:0000:0000:0000:0000:0000:0042		
2	1234:0000:00ab:0000:0000:0000:0000:5678		
3	2001:0db8:000a:000b:000c:000d:000e:000f		
4	fd12:3456:0000:0000:00ab:0000:0000:5678		

Aşağıdaki soruları cevaplayınız.

1. Üçüncü adreste neden çift iki nokta (::) işareti kullanılmamıştır?

.....

.....

.....

2. Dördüncü adreste iki farklı sıfır dizisi bulunmaktadır. Bu dizilerin uzunlukları eşit olduğunda hangi dizi kısaltılmalıdır?

.....

.....

.....

3. Dördüncü adresin fd12:3456::ab::5678 biçiminde yazılması neden doğru değildir?

.....

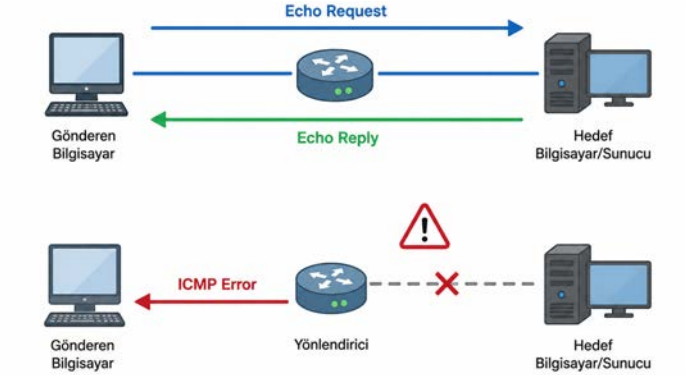
.....

.....

2.1.26. ICMP Protokolü

İnternet Kontrol Mesajı Protokolü [Internet Control Message Protocol (ICMP)], IP tabanlı ağ iletişiminde hata bildirimlerinin, kontrol mesajlarının ve temel tanılama bilgilerinin iletilmesini sağlayan protokoldür (Görsel 2.28). ICMP, kullanıcıya ait asıl uygulama verilerini taşımaktan çok iletişimin durumu hakkında bilgi vermek amacıyla kullanılır. Bir hedefe ulaşılamaması, paketin ağ üzerinde ilerlerken yaşam süresinin dolması veya temel erişim durumunun sınanması gibi işlemlerde ICMP mesajlarından yararlanılır. Bu nedenle ICMP, ağ sorunlarının belirlenmesinde ve bağlantı durumunun incelenmesinde önemli bir yere sahiptir. ICMP'nin yaygın kullanım alanlarından biri ping işlemidir. Bir hedefe ping komutuyla erişim isteği gönderildiğinde karşı taraftan yanıt alınması, temel IP iletişiminin sağlandığını gösterir. Ağ üzerinde izlenen yolun incelenmesinde ise tracert komutundan yararlanılır.

ICMP mesajlarında **Type** alanı mesajın temel türünü, **Code** alanı ise mesajla ilgili daha ayrıntılı durumu belirtir. Örneğin hedefe ulaşılamadığını bildiren mesajın farklı nedenleri Code alanı aracılığıyla açıklanabilir.



Görsel 2.28: ICMP protokolünün çalışma mantığı

ICMPv4 protokolünde kullanılan bazı temel mesaj türleri Tablo 2.5'te verilmiştir.

Tablo 2.5: ICMPv4 Temel Mesaj Türleri

Mesaj Türü	Type	Yaygın Code Değeri veya Aralığı	Temel İşlevi
Echo Request	8	0	Hedef cihaza temel erişim isteği gönderir. ping işleminin ilk adımıdır.
Echo Reply	0	0	Hedef cihazın Echo Request mesajına verdiği yanıttır.
Destination Unreachable	3	Duruma göre değişir.	Hedef ağa, hedef cihaza veya ilgili hizmete ulaşılamadığını bildirir.
Redirect	5	Duruma göre değişir.	Paket için daha uygun bir yönlendirici veya yol bulunduğuna ilişkin bilgi verir.
Time Exceeded	11	Duruma göre değişir.	Paketin yaşam süresinin dolduğunu bildirir. Yön izleme işlemlerinde önemlidir.
Parameter Problem	12	Duruma göre değişir.	IP başlığındaki bir sorun nedeniyle paketin işlenemediğini bildirir.

Not: IPv4 bağlantılarında ICMPv4, IPv6 bağlantılarında ise ICMPv6 kullanılır. İki protokol benzer amaçlara hizmet eder ancak mesaj türlerinin sayısal değerleri birbirinden farklıdır. IPv6 bağlantısında temel erişim testi yapılırken ICMPv6 Echo Request ve Echo Reply mesajlarından yararlanılır (Tablo 2.6).

Tablo 2.6: ICMPv4 ve ICMPv6 İşlemleri

İşlem	ICMPv4	ICMPv6
Temel erişim isteği	Echo Request	Echo Request
Temel erişim yanıtı	Echo Reply	Echo Reply
Hedefe ulaşılamaması	Destination Unreachable	Destination Unreachable
Paketin ağ üzerinde ilerleme sınırının dolması	Time Exceeded	Time Exceeded

ping komutu, bir cihazın başka bir cihaza IP düzeyinde erişip erişemediğini sınamak amacıyla kullanılır. Hedef cihaza Echo Request mesajı gönderilir. Hedeften Echo Reply mesajı alınırsa temel ağ erişiminin sağlandığı değerlendirilir. Başarılı bir ping sonucu, hedef cihaza temel IP erişiminin bulunduğunu gösterir ancak web, e-posta veya dosya aktarımı gibi uygulama hizmetlerinin kesin olarak çalıştığını tek başına kanıtlamaz. Bu hizmetler kendi uygulama adımlarıyla ayrıca sınanmalıdır.

tracert komutu, paketin hedefe ulaşırken geçtiği ara yönlendiricileri incelemeye yardımcı olur. Windows tabanlı sistemlerde tracert, yaşam süresi değeri giderek artırılan ICMP Echo Request veya ICMPv6 mesajları gönderir. Ara yönlendiricilerden dönen Time Exceeded mesajları ve hedef cihazın yanıtı incelenerek izlenen yol belirlenir.

Bazı ara yönlendiriciler Time Exceeded mesajı göndermeyebilir. Böyle bir durumda tracert çıktısında yıldız (*) işaretleri görülebilir. Bu durum her zaman hedefe ulaşılamadığı anlamına gelmez.

Komut	Temel Sorusu	Kullanım Amacı
ping <hedef_adres>	Hedefe temel düzeyde erişilebiliyor mu?	IP erişimini sınamak
tracert <hedef_adres>	Hedefe giderken hangi ara yönlendiricilerden geçiliyor?	İzlenen yolu incelemek

5. UYGULAMA

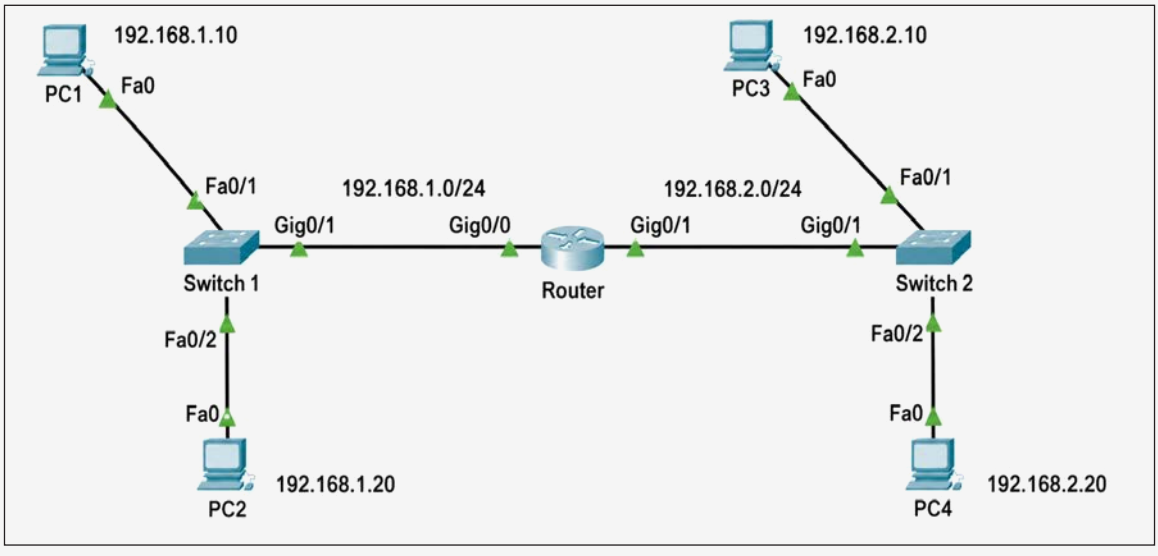
Uygulama Adı	IPv4 ve IPv6 ile Bağlantı Testleri Yapmak
Süre	60 dakika
Amaç	Yönlendirici ve istemci cihazları statik IPv4 ve IPv6 adresleriyle yapılandırarak ping ve tracert komutlarıyla temel ağ iletişimini sınamak
Araç Gereç	Ağ simülasyon programı, bir yönlendirici, iki switch, en az iki istemci bilgisayar, çalışma yaprağı.

Dikkat Edilecek Noktalar

- IP adreslerini, alt ağ maskelerini ve ön ek uzunluklarını doğru yazınız.
- İstemcilerin varsayılan ağ geçidi bilgilerini eksiksiz tanımlayınız.
- Yönlendirici arayüzlerini no shutdown komutuyla etkinleştiriniz.
- IPv4 ve IPv6 test sonuçlarını ayrı alanlara kaydediniz.
- ping komutuyla temel erişimi, tracert komutuyla izlenen yolu inceleyiniz.
- Grup içinde görev paylaşımı yapınız.

A) Statik IPv4 Adresleriyle Bağlantı Testi Yapmak

İki farklı IPv4 ağını yönlendirici aracılığıyla birbirine bağlamak ve bağlantı sonuçlarını `ping` ile `tracert` komutlarını kullanarak incelemek. (IPv4 ile ping ve tracert uygulama topolojisi Görsel 2.29'da verilmiştir.)



Görsel 2.29: IPv4 ile ping ve tracert uygulaması

Adres Planı

Aşağıdaki plan kullanılabilir.

Cihaz veya Arayüz	IPv4 Adresi	Alt Ağ Maskesi	Varsayılan Ağ Geçidi
Yönlendirici G0/1	192.168.1.1	255.255.255.0	–
Yönlendirici G0/2	192.168.2.1	255.255.255.0	–
PC1	192.168.1.10	255.255.255.0	192.168.1.1
PC3	192.168.2.10	255.255.255.0	192.168.2.1

1. Adım: Yönlendirici Arayüzlerini Yapılandırmak

Yönlendirici arayüzlerini yapılandırınız.

Router> enable

Router# configure terminal

Router(config)# interface g0/1

Router(config-if)# ip address 192.168.1.1 255.255.255.0

Router(config-if)# no shutdown

Router(config-if)# exit

Router(config)# interface g0/2

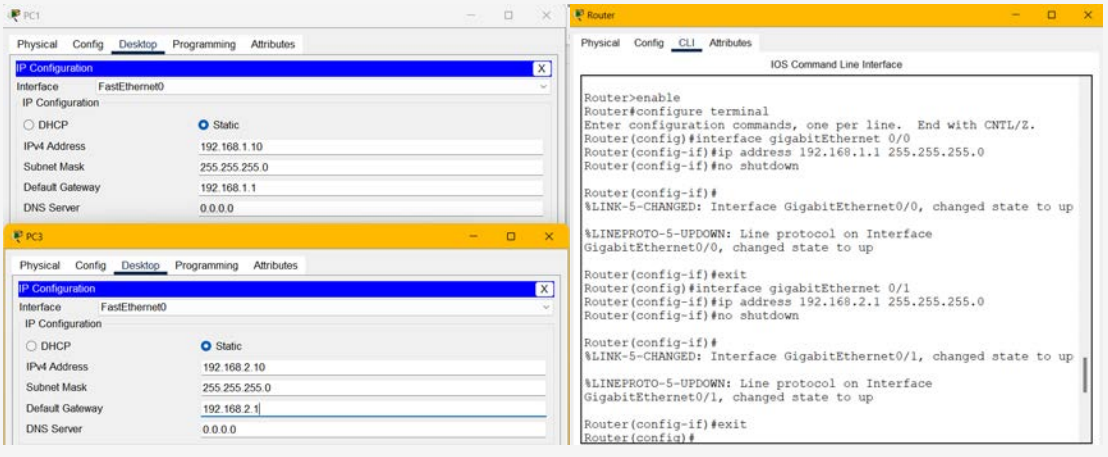
Router(config-if)# ip address 192.168.2.1 255.255.255.0

Router(config-if)# no shutdown

Router(config-if)# end

2. Adım: İstemci Bilgisayarları Yapılandırmak

İstemci bilgisayarlarda **Desktop > IP Configuration** bölümünü açınız. Adres planındaki IPv4 adresini, alt ağ maskesini ve varsayılan ağ geçidini ilgili alanlara yazınız (Görsel 2.30).



Görsel 2.30: Yönlendirici ve istemcilerin IPv4 yapılandırılması

3. Adım: Ağ Geçidine Erişimi Sınamak

PC1 cihazında **Desktop > Command Prompt** bölümünü açınız.
ping 192.168.1.1

4. Adım: Farklı Ağdaki İstemciye Erişimi Sınamak

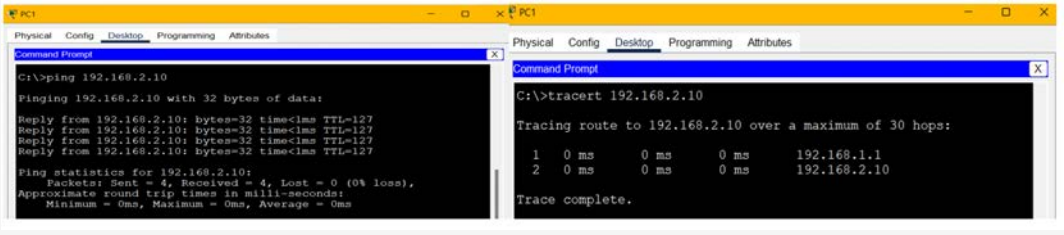
Farklı ağdaki istemciye erişimi sınayınız.

ping 192.168.2.10

5. Adım: İzlenen Yolu İncelemek

tracert 192.168.2.10

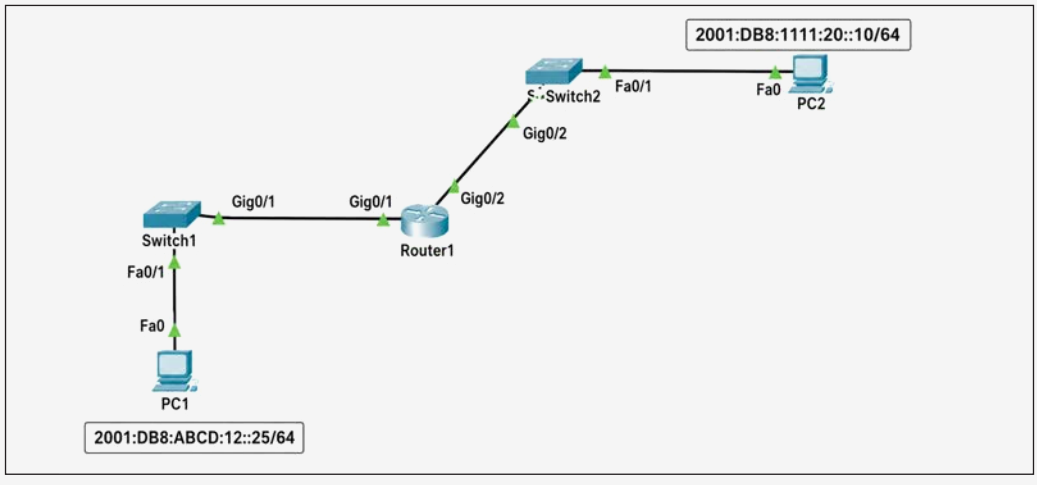
ping ve tracert sonuçları komut satırında gösterilmiştir (Görsel 2.31).



Görsel 2.31: IPv4 bağlantısında ping ve tracert sonuçları

B) Statik IPv6 Adresleriyle Bağlantı Testi Yapmak

Amaç: İki farklı IPv6 ağını yönlendirici aracılığıyla birbirine bağlamak ve bağlantı sonuçlarını ping ile tracert komutlarını kullanarak incelemek (IPv6 ile ping ve tracert uygulama topolojisi Görsel 2.32'de verilmiştir.)



Görsel 2.32: IPv6 ile ping ve tracert uygulaması

Adres Planı

Cihaz veya Arayüz	IPv6 Adresi	Ön Ek Uzunluğu	Varsayılan Ağ Geçidi
Yönlendirici G0/1	2001:db8:abcd:12::1	/64	—
Yönlendirici G0/2	2001:db8:1111:20::1	/64	—
PC1	2001:db8:abcd:12::10	/64	2001:db8:abcd:12::1
PC2	2001:db8:1111:20::10	/64	2001:db8:1111:20::1

1. Adım: IPv6 Yönlendirmeyi Etkinleştirmek

IPv6 yönlendirmeyi etkinleştiriniz.

Router> enable
Router# configure terminal
Router(config)# ipv6 unicast-routing

2. Adım: Sol Taraftaki Yönlendirici Arayüzünü Yapılandırmak

Sol taraftaki yönlendirici arayüzünü yapılandırınız.

```
Router(config)# interface g0/1
Router(config-if)# ipv6 address 2001:db8:abcd:12::1/64
Router(config-if)# no shutdown
Router(config-if)# exit
```

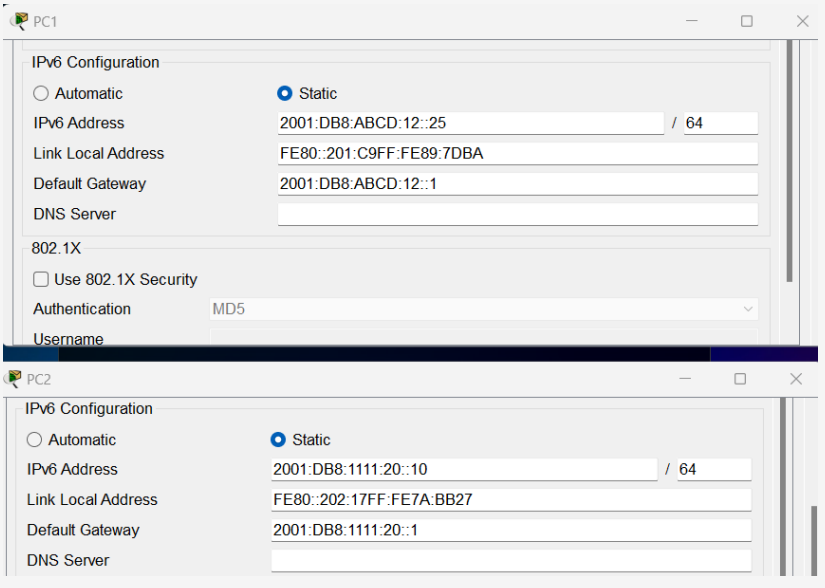
3. Adım: Sağ Taraftaki Yönlendirici Arayüzünü Yapılandırmak

Sağ taraftaki yönlendirici arayüzünü yapılandırınız.

```
Router(config)# interface g0/2
Router(config-if)# ipv6 address 2001:db8:1111:20::1/64
Router(config-if)# no shutdown
Router(config-if)# end
```

4. Adım: İstemci Bilgisayarları Yapılandırmak

İstemci bilgisayarlarda **Desktop > IP Configuration** bölümünü açınız. Adres planında verilen IPv6 adreslerini, ön ek uzunluklarını ve varsayılan ağ geçidi bilgilerini ilgili alanlara yazınız (Görsel 2.33).



Görsel 2.33: İstemcilerin statik IPv6 adresleriyle yapılandırılması

5. Adım: Ağ Geçidinize Erişimi Sağlamak

Ağ geçidinize erişimi şöyle sağlayınız:

```
ping 2001:db8:abcd:12::1
```

6. Adım: Farklı IPv6 Ağındaki İstemciye Erişimi Sağlamak

Farklı IPv6 ağındaki istemciye erişimi şöyle sınayınız:

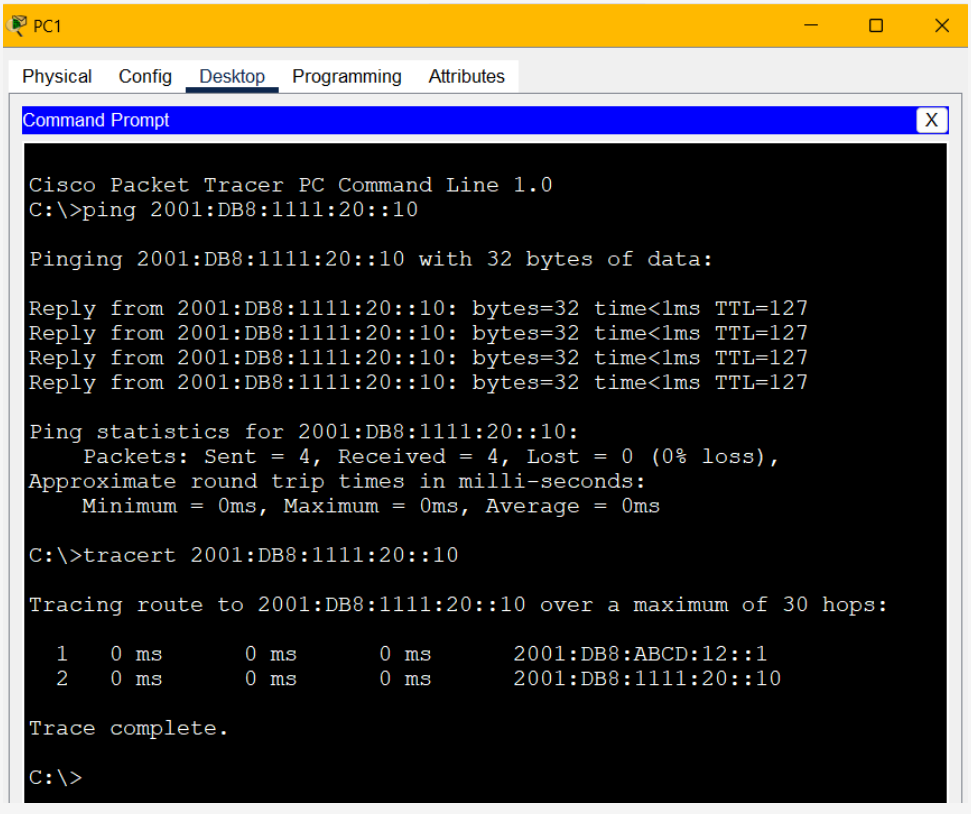
```
ping 2001:db8:1111:20::10
```

7. Adım: İzlenen Yolu İncelemek

İzlenen yolu şöyle inceleyiniz:

tracert 2001:db8:1111:20::10

IPv6 bağlantısında ping ve tracert sonuçları Görsel 2.34'te verilmiştir.



Görsel 2.34: IPv6 bağlantısında ping ve tracert sonuçları

IPv4 ve IPv6 bağlantı testleri gözlem tablosunu doldurunuz.

İncelenen Durum	IPv4 Test Sonucu	IPv6 Test Sonucu
Yönlendirici arayüzleri doğru adreslerle yapılandırıldı mı?	☐ Evet ☐ Hayır	☐ Evet ☐ Hayır
İstemci adresleri doğru yazıldı mı?	☐ Evet ☐ Hayır	☐ Evet ☐ Hayır
Varsayılan ağ geçidi bilgileri doğru tanımlandı mı?	☐ Evet ☐ Hayır	☐ Evet ☐ Hayır
İstemciden kendi ağ geçidine ping yanıtı alındı mı?	☐ Evet ☐ Hayır	☐ Evet ☐ Hayır
Farklı ağdaki istemciye ping yanıtı alındı mı?	☐ Evet ☐ Hayır	☐ Evet ☐ Hayır
tracert çıktısında yönlendirici gözlemlendi mi?	☐ Evet ☐ Hayır	☐ Evet ☐ Hayır
Kullanılan hedef adres		
Gözlemlenen ara nokta veya noktalar		
Karşılaşılan sorun varsa kısa açıklaması		

Sonuçları Yorumlamak

Aşağıdaki soruları cevaplayınız.

1. Aynı yerel ağ içindeki iletişim ile farklı ağlardaki iletişim arasında nasıl bir fark bulunmaktadır?

.....
.....

2. Farklı ağlar arasında iletişim kurulurken yönlendirici hangi görevi üstlenmektedir?

.....
.....

3. ping işlemi başarılı olduğu hâlde tracert çıktısında bazı ara noktalarda yıldız işareti görülebilir mi? Açıklayınız.

.....
.....

4. IPv4 ve IPv6 bağlantı testlerinin ortak yönleri nelerdir?

.....
.....

Değerlendirme

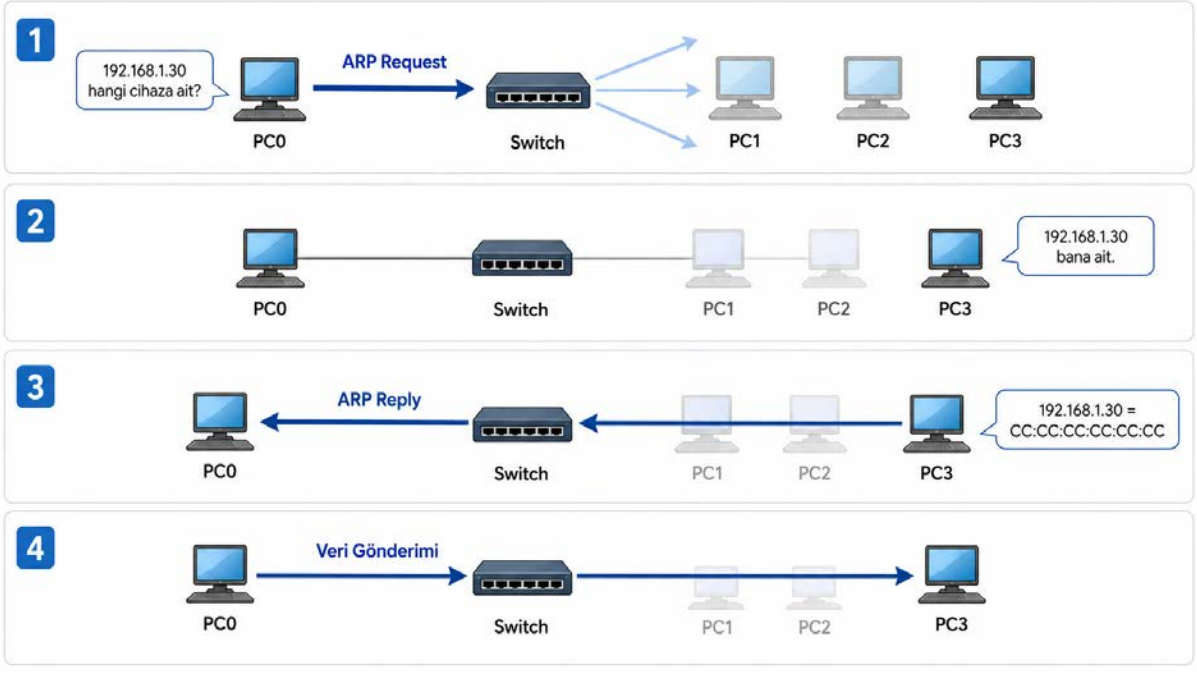
Çalışmanız öğretmeniniz tarafından kontrol listesine göre değerlendirilecektir. Çalışmanızı yaparken buradaki ölçütleri dikkate alınız. Kontrol listesi formuna ulaşmak için karekodu okutunuz. Dijital yayınlarda karekodun üstüne tıklayarak içeriğe ulaşabilirsiniz.

2.1.27. ARP Protokolü

Adres Çözümleme Protokolü [Address Resolution Protocol (ARP)], IPv4 kullanan yerel ağlarda IP adresi ile veri bağı katmanında kullanılan fiziksel adres arasında eşleştirme yapılmasını sağlayan protokoldür. Ethernet ağlarında bu fiziksel adres, MAC adresidir. ARP sayesinde bir cihaz, iletişim kurmak istediği sonraki hedefe ait IPv4 adresini kullanarak gerekli MAC adresini öğrenebilir. Bir cihaz aynı yerel ağdaki başka bir cihaza veri göndermek istediğinde yalnızca hedef IPv4 adresini bilmesi yeterli olmaz. Ethernet çerçevesinin yerel ağ içinde doğru hedefe iletilebilmesi için hedef cihazın MAC adresine de ihtiyaç vardır. Gönderici cihaz, gerekli eşleştirme kendi ARP tablosunda bulunmuyorsa ARP isteği gönderir. İlgili hedef cihaz, ARP yanıtı vererek kendi MAC adresini bildirir. Öğrenilen IP–MAC eşleştirmesi daha sonraki iletimlerde kullanılmak üzere ARP tablosunda geçici olarak saklanabilir. ARP, ağ katmanında kullanılan IPv4 adresleri ile veri bağı katmanında kullanılan MAC adresleri arasında işlevsel bir ilişki kurar. Bu nedenle ARP süreci, kapsülleme ve yerel ağ iletişiminin anlaşılması açısından önemlidir.

Not: ARP, IPv4 iletişimiyle ilişkilidir. IPv6 iletişiminde aynı amaç için ARP kullanılmaz. IPv6 cihazları, komşu cihazların veri bağı katmanı adreslerini belirlemek için ICMPv6 ile ilişkili Komşu Keşfi (Neighbor Discovery) mekanizmalarından yararlanır (Görsel 2.35).

Dikkat: Hedef cihaz aynı yerel ağda bulunuyorsa gönderici cihaz, hedef cihazın MAC adresini öğrenir ve çerçeveyi doğrudan hedef cihaza gönderir. Hedef cihaz farklı bir ağda bulunuyorsa gönderici cihaz, uzak cihazın MAC adresini doğrudan öğrenmeye çalışmaz. Bu durumda kendi yerel ağındaki varsayılan ağ geçidinin MAC adresini belirler ve çerçeveyi yönlendiricinin ilgili arayüzüne gönderir.



Görsel 2.35: ARP protokolünün çalışma süreci

6. UYGULAMA

Uygulama Adı	ARP Sürecini Simülasyon Ortamında Gözlemlemek
Süre	25 dakika
Amaç	Aynı yerel ağda bulunan cihazlar arasındaki ARP isteği ve ARP yanıtı sürecini izlemek, oluşan IPv4–MAC adresi eşleştirmesini ARP tablosunda doğrulamak
Araç Gereç	Ağ simülasyon programı, bir switch, dört istemci bilgisayar, çalışma yaprağı.

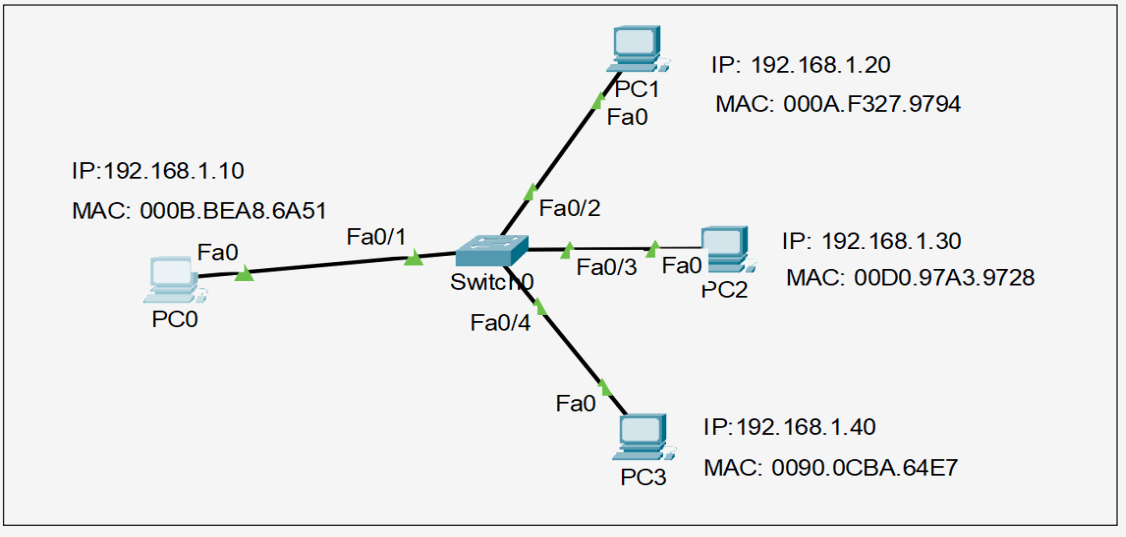
Dikkat Edilecek Noktalar

- Bütün istemcileri aynı IPv4 ağında yapılandırınız.
- IP adreslerini tabloya uygun biçimde yazınız.
- ARP Request ve ARP Reply mesajlarını birbirinden ayırt ediniz.
- ARP isteğinin yayın, ARP yanıtının ise normal durumda tekil gönderim biçiminde iletildiğini gözlemleyiniz.
- ARP tablosunu işlem öncesinde ve sonrasında karşılaştırınız.
- Simülasyon programının sürümüne göre menü adları küçük farklılıklar gösterebilir.
- Grup içinde görev paylaşımı yapınız.

Ağ simülasyon programında aşağıdaki cihazları çalışma alanına ekleyiniz.

- Bir switch
- Dört istemci bilgisayar

Cihazları switche uygun bağlantı kablolarıyla bağlayınız. ARP protokolü simülasyon topolojisi Görsel 2.36'da verilmiştir.



Görsel 2.36: ARP protokolü simülasyon topolojisi

Adres Planı

Cihaz	IPv4 Adresi	Alt Ağ Maskesi
PC0	192.168.1.10	255.255.255.0
PC1	192.168.1.20	255.255.255.0
PC2	192.168.1.30	255.255.255.0
PC3	192.168.1.40	255.255.255.0

1. Adım: İstemcileri Yapılandırmak

Her istemciyi açınız. **Desktop > IP Configuration** bölümüne geçiniz. Adres planındaki IPv4 adresini ve alt ağ maskesini ilgili alanlara yazınız.

2. Adım: PC0 Cihazının ARP Tablosunu Kontrol Etmek

PC0 cihazında **Desktop > Command Prompt** bölümünü açarak şu komutu çalıştırınız:
arp -a

3. Adım: Simülasyon Moduna Geçmek

Simülasyon programında **Simulation** modunu açınız. Olay filtresi kullanılabiliyorsa ARP ve ICMP mesajlarını görünür hâle getiriniz.

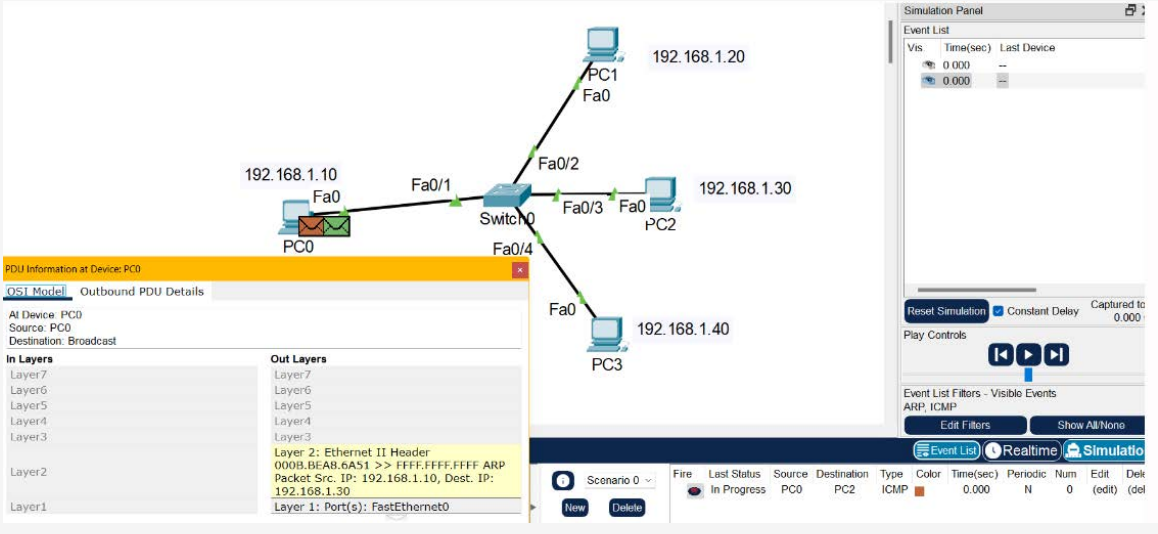
4. Adım: PC0 Cihazından PC2 Cihazına İleti Göndermek

Simülasyon programındaki basit PDU gönderme aracını kullanarak PC0 cihazından PC2 cihazına bir ileti gönderiniz.

Alternatif olarak PC0 komut satırında aşağıdaki komutu kullanabilirsiniz.

ping 192.168.1.30

Simülasyon ortamında PDU gönderimi Görsel 2.37'de gösterilmiştir.



Görsel 2.37: Simülasyon ortamında PDU gönderimi

5. Adım: ARP Request Mesajını İncelemek

Simülasyon akışını adım adım ilerletiniz. PC0 cihazının hedef MAC adresini henüz bilmediği için ARP Request mesajı gönderdiğini gözlemleyiniz.

Aşağıdaki noktaları inceleyiniz.

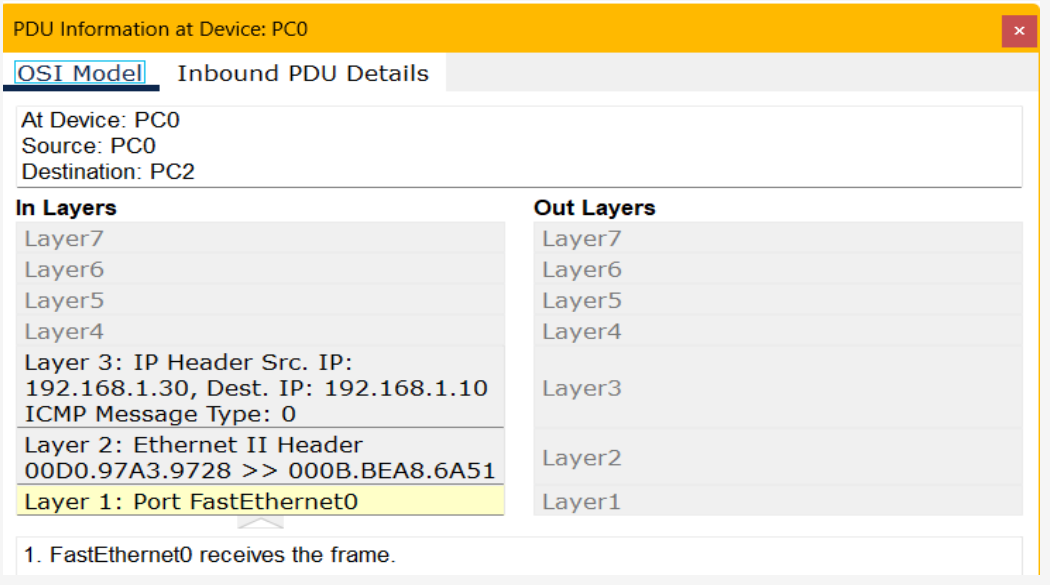
- ARP isteğini hangi cihaz göndermiştir?
- İstekte aranan IPv4 adresi nedir?
- Yayın MAC adresi hangi değerdir?
- Anahtar isteği hangi cihazlara iletmiştir?

6. Adım: ARP Reply Mesajını İncelemek

Simülasyon akışını ilerletmeye devam ediniz. PC2 cihazının kendi IPv4 adresiyle eşleşen isteği aldığını ve ARP Reply mesajı gönderdiğini gözlemleyiniz (Görsel 2.38).

Aşağıdaki noktaları inceleyiniz.

- ARP yanıtını hangi cihaz göndermiştir?
- Yanıtta bildirilen IPv4 adresi nedir?
- Yanıtta bildirilen MAC adresi nedir?
- ARP yanıtı yayın biçiminde mi, tekil gönderim biçiminde mi iletilmiştir?



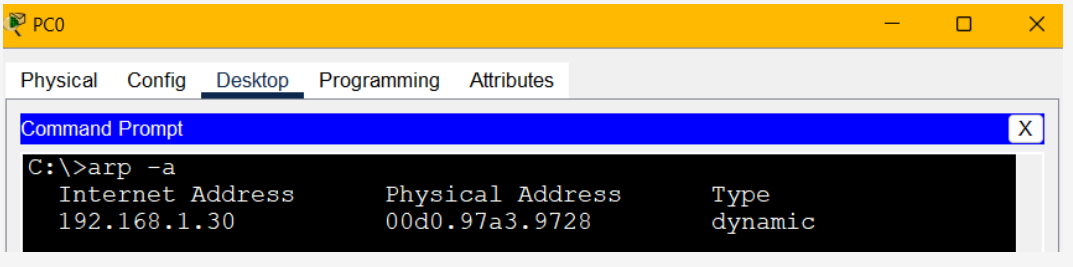
Görsel 2.38: ARP isteği ve ARP yanıtının gözlemlenmesi

7. Adım: ARP Tablosunu Yeniden Görüntülemek

PC0 cihazında aşağıdaki komutu yeniden çalıştırınız.

arp -a

192.168.1.30 adresiyle ilişkilendirilen MAC adresinin tabloya eklendiğini doğrulayınız (Görsel 2.39).



Görsel 2.39: arp -a komutuyla ARP tablosunun görüntülenmesi

8. Adım: İkinci Gönderimi Karşılaştırmak

PC0 cihazından PC2 cihazına ikinci kez ileti gönderiniz. ARP tablosunda geçerli eşleştirme bulunduğu sürece yeni bir ARP isteğinin gerekli olup olmadığını gözlemleyiniz.

ARP Süreci Gözlem Tablosu

İncelenen Unsur	Gözlemlediğiniz Sonuç
İletiyi başlatan cihaz	
Hedef cihaz	
Hedef cihazın IPv4 adresi	
İlk gönderimden önce hedef cihaz ARP tablosunda bulunuyor muydu?	☐ Evet ☐ Hayır
ARP Request mesajını gönderen cihaz	
ARP Request mesajındaki hedef IPv4 adresi	
ARP Request mesajında kullanılan hedef MAC adresi	
ARP isteği yerel ağda hangi cihazlara ulaştı?	
ARP Reply mesajını gönderen cihaz	
ARP Reply mesajında bildirilen MAC adresi	
ARP Reply mesajı yayın mı, tekil gönderim mi?	
İşlem sonrasında arp -a tablosuna eklenen eşleştirme	
İkinci gönderimde yeni bir ARP isteği gözlemlendi mi?	☐ Evet ☐ Hayır
Karşılaşılan sorun varsa kısa açıklaması	

Sonuçları Yorumlamak

Aşağıdaki soruları cevaplayınız.

1. Aynı yerel ağdaki bir cihazın yalnızca hedef IPv4 adresini bilmesi neden yeterli değildir?

.....
.....

2. ARP Request mesajı neden yayın biçiminde gönderilir?

.....
.....

3. Yerel ağdaki bütün cihazlar ARP isteğini aldığı hâlde neden yalnızca PC2 yanıt vermiştir?

.....
.....

4. İkinci gönderimde yeniden ARP isteği gönderilmemesinin nedeni ne olabilir?

.....
.....

5. Hedef cihaz farklı bir ağda bulunsaydı PC0 hangi cihazın MAC adresini öğrenmeye çalışırdı?

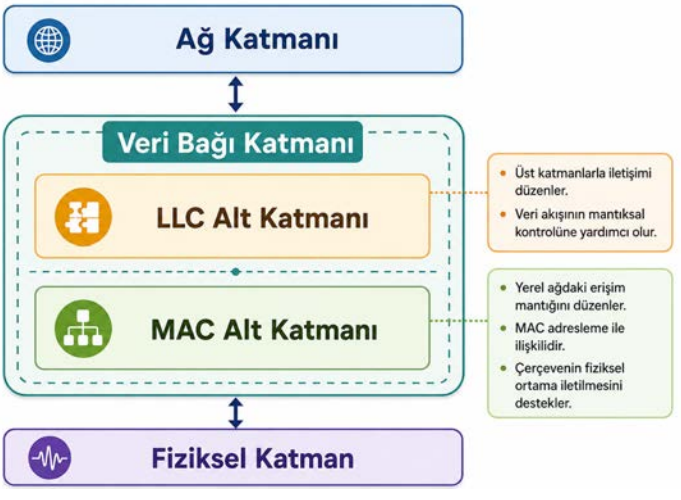
.....
.....

Değerlendirme

Çalışmanız öğretmeniniz tarafından kontrol listesine göre değerlendirilecektir. Çalışmanızı yaparken buradaki ölçütleri dikkate alınız. Kontrol listesi formuna ulaşmak için karekodu okutunuz. Dijital yayınlarda karekodun üstüne tıklayarak içeriğe ulaşabilirsiniz.

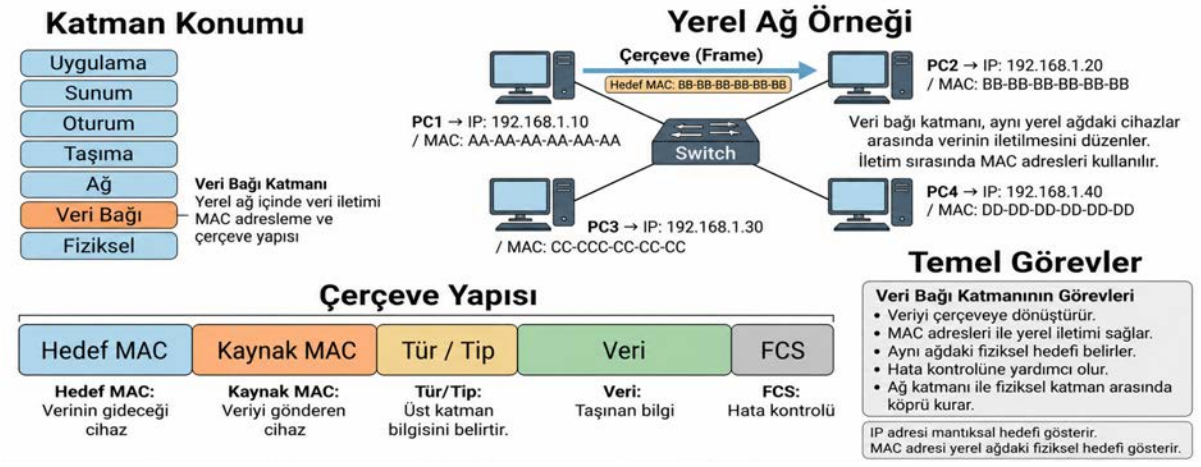
2.1.28. Veri Bağı Katmanı

Veri bağı katmanı, verinin fiziksel bağlantı üzerinden çerçeve düzeyinde düzenli biçimde iletilmesini sağlayan katmandır. Bu katmanda üst katmandan gelen veriye, kullanılan iletişim teknolojisine uygun kontrol bilgileri eklenir ve veri **çerçeve (frame)** biçiminde iletime hazırlanır. Ağ katmanı, paketin ulaşacağı mantıksal hedefi IP adresiyle belirler. Veri bağı katmanı ise paketin mevcut bağlantı veya yerel ağ bölümü üzerinde nasıl taşınacağını düzenler. Ethernet ağlarında bu işlem sırasında MAC adreslerinden yararlanılır. Veri bağı katmanı yalnızca kablolu yerel ağlarla sınırlı değildir. Kablolu Ethernet bağlantıları, kablosuz Wi-Fi iletişimi ve belirli noktadan noktaya bağlantılar farklı çerçeve yapılarından yararlanabilir. Kullanılan iletişim ortamı değişse de temel amaç; veriyi uygun çerçeve yapısıyla düzenlemek, yerel iletimi gerçekleştirmek ve fiziksel katman ile ağ katmanı arasında işlevsel bir bağlantı kurmaktır (Görsel 2.40).



Görsel 2.40: Veri bağı katmanının diğer katmanlar arasındaki yeri

Veri bağı katmanının temel yapısı Görsel 2.41'de gösterilmiştir.



Görsel 2.41: Veri bağı katmanının temel yapısı

2.1.29. Veri Bağı Katmanı Protokolleri

Veri bağı katmanında farklı iletişim ortamlarına ve bağlantı türlerine uygun çeşitli yapılar kullanılır. Bu yapılar verinin çerçevelenmesini, iletim kurallarının belirlenmesini ve bağlantının düzenli biçimde yürütülmesini sağlar (Tablo 2.7). Ethernet, kablolu yerel ağlarda yaygın olarak kullanılır. Wi-Fi, kablosuz yerel ağ iletişimini düzenler. HDLC ve PPP ise özellikle seri veya noktadan noktaya bağlantılarla ilişkilidir.

Tablo 2.7: Veri Bağı Katmanı Protokolleri

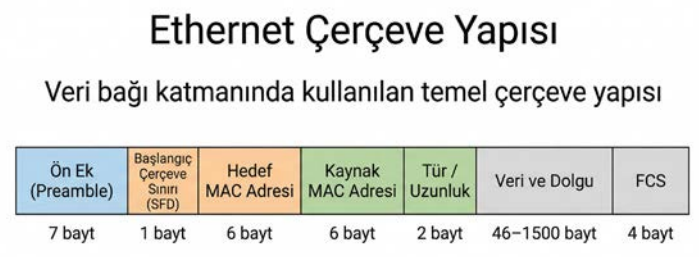
Yapı	Temel Kullanım Alanı	Öne Çıkan Özelliği
Ethernet	Kablolu yerel ağlar	MAC adresleri ve Ethernet çerçeveleriyle yerel ağ iletişimini düzenler.
Wi-Fi	Kablosuz yerel ağlar	Radyo dalgaları üzerinden kablosuz iletişim sağlar.
HDLC	Seri bağlantılar, noktadan noktaya veya belirli çok noktalı bağlantılar	Çerçeve temelli ve düzenli veri iletimi sağlar.
PPP	Noktadan noktaya bağlantılar	Bağlantı kurulumu, yapılandırma ve isteğe bağlı kimlik doğrulama işlevlerini destekler.

Bu yapılar aynı katmanla ilişkili olmakla birlikte aynı ortamda ve aynı amaçla kullanılmaz. Ağ tasarımında bağlantı türüne, iletim ortamına ve yönetim gereksinimlerine uygun yapı seçilmelidir.

2.1.30. Ethernet

Ethernet, kablolu yerel ağlarda yaygın olarak kullanılan iletişim teknolojilerinden biridir. Okullarda, ofislerde, laboratuvarlarda ve ev ağlarında bulunan birçok kablolu bağlantı Ethernet yapısından yararlanır. Ethernet iletişiminde veriler çerçeve adı verilen yapılar hâlinde taşınır. Ethernet çerçevesindeki hedef ve kaynak MAC adresleri, verinin yerel ağ içindeki uygun arayüze ulaştırılmasına yardımcı olur (Görsel 2.42). Örneğin bir bilgisayar aynı yerel ağdaki yazıcıya veri gönderecekse IP adresi mantıksal hedefi, Ethernet çerçevesindeki hedef MAC adresi ise yerel bağlantı üzerindeki hedef arayüzü gösterir.

Anahtarlar (switch), aldıkları Ethernet çerçevelerindeki MAC adreslerini kullanarak yerel ağ trafiğini uygun bağlantı noktalarına iletir. Böylece çerçevelerin bütün bağlantı noktalarına gereksiz yere gönderilmesi azaltılabilir.



Görsel 2.42: Ethernet çerçeve yapısı

Ön Ek (Preamble): Alıcı arayüzün gelen veri akışına senkronize olmasına yardımcı olur.

Başlangıç Çerçeve Sınırı (SFD): Çerçevenin başlayacağı noktayı belirtir.

Hedef MAC Adresi: Çerçevenin ulaştırılacağı hedef arayüzü gösterir.

Kaynak MAC Adresi: Çerçeveyi gönderen arayüzü gösterir.

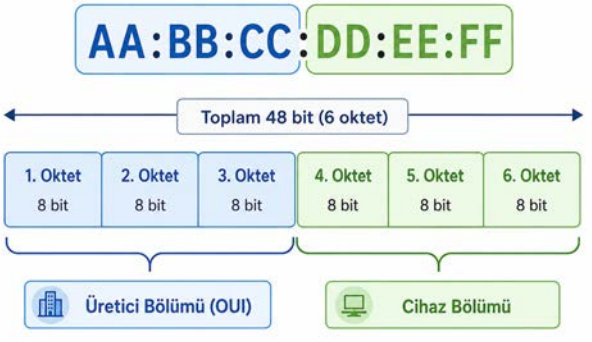
Tür / Uzunluk: Taşınan üst katman bilgisini veya veri alanının uzunluğunu belirtir.

Veri ve Dolgu: Taşınan asıl veriyi içerir. Gerektiğinde minimum uzunluğa ulaşmak için dolgu eklenebilir.

FCS: Çerçevede iletim sırasında hata oluşup oluşmadığının denetlenmesine yardımcı olur.

MAC Adresi

Ortam Erişim Kontrolü [Media Access Control (MAC)] adresi, veri bağı katmanında ağ arayüzlerinin yerel bağlantı üzerinde ayırt edilmesine yardımcı olan adrestir. Ethernet arayüzlerinde yaygın olarak 48 bit uzunluğunda MAC adresleri kullanılır. Bu adresler genellikle altı adet iki haneli on altılı grup biçiminde yazılır (Görsel 2.43).



Görsel 2.43: MAC adres yapısı

Örnek:

00:1a:2b:3c:4d:5e

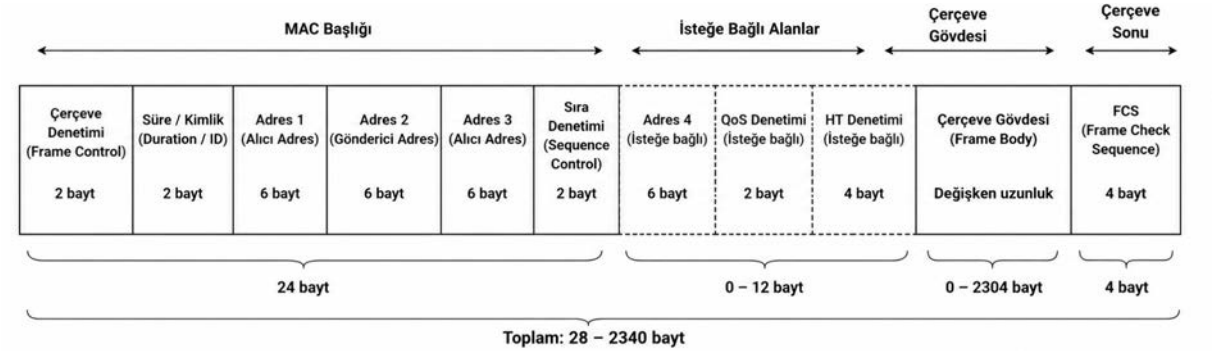
Genel üretici atamasıyla kullanılan birçok 48 bitlik MAC adresinde ilk 24 bit üreticiyle ilişkili bölümü, kalan 24 bit ise ilgili arayüz için ayrılan bölümü gösterir ancak yerel olarak atanmış veya yazılım aracılığıyla değiştirilmiş MAC adresleri de bulunabilir. Bu nedenle MAC adresi her durumda değiştirilemez ve yalnızca üretici tarafından belirlenir biçiminde yorumlanmamalıdır.

Ethernet çerçevelerindeki kaynak ve hedef alanlarında MAC adresleri kullanılır. ARP protokolü de IPv4 adresleriyle MAC adresleri arasındaki eşleştirmenin belirlenmesine yardımcı olur.

2.1.31. Wi-Fi

Wi-Fi, kablosuz yerel ağ iletişiminde kullanılan yapıdır. Veri bağı katmanı açısından Ethernet'e benzer biçimde çerçeve temelli iletişimden yararlanır ancak veri aktarımı fiziksel kablo yerine radyo dalgaları üzerinden gerçekleştirilir. Kablosuz ortamın paylaşılması nedeniyle Wi-Fi iletişiminde sinyal gücü, mesafe, kanal kullanımı, çevredeki diğer kablosuz ağlar, elektromanyetik parazit gibi etkenler önem taşır. Bu nedenle kablosuz ağların planlanmasında yalnızca bağlantının kurulması değil iletişim kalitesinin sürdürülebilmesi de dikkate alınmalıdır.

Wi-Fi çerçeveleri, Ethernet çerçevelerinden farklı alanlara sahip olabilir. Kullanılan çerçeve türüne ve verinin izlediği yöne göre birden fazla adres alanından yararlanılabilir (Görsel 2.44).



Görsel 2.44: Wi-Fi çerçeve yapısı

Wi-Fi çerçeve yapısındaki alanlar ve temel işlevleri Tablo 2.8'de verilmiştir.

Tablo 2.8: Wi-Fi Çerçeve Yapısındaki Alanlar ve Temel İşlevleri

Alan	Temel İşlevi
Çerçeve Denetimi (Frame Control)	Çerçevenin türünü ve temel kontrol bilgilerini belirtir.
Süre / Kimlik (Duration/ID)	Kablosuz ortamın kullanım süresi veya ilgili kimlik bilgisiyle ilişkilidir.
Adres Alanları	Çerçeve türüne ve iletim yönüne göre kaynak, hedef, erişim noktası veya ağ içi yönlendirme bilgilerini taşıyabilir.
Sıra Denetimi (Sequence Control)	Çerçevelerin sıralanmasına ve izlenmesine yardımcı olur.
QoS Denetimi — İsteğe Bağlı	Hizmet kalitesi ve trafik önceliğiyle ilişkili bilgileri taşıyabilir.
HT Denetimi — İsteğe Bağlı	Belirli yüksek hızlı kablosuz iletim özellikleriyle ilişkili ek kontrol bilgilerini taşıyabilir.
Çerçeve Gövdesi (Frame Body)	Taşınan asıl veriyi içerir.
FCS	Çerçevede hata oluşup oluşmadığının denetlenmesine yardımcı olur.

2.1.32. HDLC

Yüksek Düzey Veri Bağı Kontrolü [High-Level Data Link Control (HDLC)], çerçeve temelli veri iletimini düzenleyen veri bağı katmanı protokollerinden biridir. Özellikle seri bağlantılarla ilişkilidir. Noktadan noktaya bağlantılarda ve belirli çok noktalı yapılarda kullanılabilir. HDLC, verinin belirli kurallara göre çerçevelenmesini ve bağlantı üzerinden düzenli biçimde iletilmesini sağlar. Ethernet daha çok yerel ağ iletişimiyle ilişkilendirilirken HDLC, özellikle iki ağ cihazı arasındaki doğrudan seri bağlantıların açıklanmasında yararlı bir örnektir. HDLC, güncel ağlarda her senaryoda kullanılan tek çözüm değildir ancak veri bağı katmanında bağlantı türüne göre farklı çerçeveleme yöntemlerinin bulunabileceğini göstermesi açısından önemlidir.

2.1.33. PPP

Noktadan Noktaya Protokol [Point-to-Point Protocol (PPP)], iki uç arasındaki doğrudan bağlantılarda kullanılan veri bağı katmanı protokollerinden biridir. PPP, bağlantı üzerinden taşınacak verinin çerçevelenmesini sağlar. Ayrıca bağlantının kurulması, yapılandırılması, sürdürülmesi ve sonlandırılmasıyla ilişkili işlevleri destekler. PPP yapısında gerektiğinde kimlik doğrulama mekanizmalarından yararlanılabilir. Böylece bağlantı kurmaya

çalışan tarafın doğrulanması sağlanabilir. PPP ayrıca farklı ağ katmanı protokollerinin taşınmasına yönelik yapılandırma işlemlerini destekleyebilir.

PPP'nin kimlik doğrulama desteği bulunması, aktarılan verilerin mutlaka şifrelendiği anlamına gelmez. PPP tek başına veri gizliliğini garanti eden bir şifreleme protokolü değildir. Bu nedenle PPP, **güvenli iletişim protokolü** biçiminde tanımlanmamalıdır. HDLC ve PPP özelliklerinin karşılaştırılması Tablo 2.9'da verilmiştir.

Tablo 2.9: HDLC ve PPP Özelliklerinin karşılaştırılması

Özellik	HDLC	PPP
Temel kullanım yaklaşımı	Seri bağlantılarda çerçeve temelli iletişim	Noktadan noktaya bağlantılarda çerçeve temelli iletişim
Bağlantı yönetimi	Temel çerçeveleme ve bağlantı düzeni	Bağlantının kurulması ve yapılandırılması için ek işlevler
Kimlik doğrulama desteği	Temel yapının zorunlu bir özelliği değildir.	İsteğe bağlı olarak desteklenebilir.
Şifreleme garantisi	Yoktur.	Tek başına sağlamaz.
Ağ katmanı protokollerini yapılandırma	Kullanılan yapıya göre değişir.	Farklı ağ katmanı protokollerine yönelik yapılandırma işlevlerini destekleyebilir.

SIRA SİZDE

Aşağıdaki kullanım durumlarını inceleyiniz ve her durumla ilgili uygun yapı veya kavramı tabloya yazınız. Ardından soruyu gerekçesiyle cevaplayınız.

Kullanım Durumu	Uygun Yapı veya Kavram
Bir okul laboratuvarındaki masaüstü bilgisayarlar kablolu yerel ağ üzerinden iletişim kurmaktadır.	
Tabletler ve dizüstü bilgisayarlar kablosuz erişim noktası üzerinden ağa bağlanmaktadır.	
İki ağ cihazı arasındaki seri bağlantıda çerçeve temelli iletişim gerçekleştirilmektedir.	
Noktadan noktaya bağlantıda bağlantı yönetimi ve isteğe bağlı kimlik doğrulama işlevlerine ihtiyaç duyulmaktadır.	
Aynı yerel ağdaki hedef arayüzün fiziksel adresi Ethernet çerçevesinde kullanılmaktadır.	

Aşağıdaki soruyu cevaplayınız.

PPP'nin kimlik doğrulama mekanizmalarını desteklemesi, PPP üzerinden iletilen bütün verilerin otomatik olarak şifrelendiği anlamına gelir mi? Cevabınızı açıklayınız.

.....

.....

2.1.34. Fiziksel Katman

Fiziksel katman, verinin ağ ortamında bit düzeyinde taşınmasını sağlayan katmandır. Veri; kullanılan iletim ortamına göre elektriksel, optik veya elektromanyetik sinyaller biçiminde aktarılır. Kablolar, konnektörler, bağlantı noktaları, sinyal türleri, iletim hızları ve fiziksel bağlantı kuralları bu katmanla ilişkilidir. Fiziksel katman, ağın en somut bölümünü oluşturur. Çünkü kablo bağlantıları, portlar, konnektörler ve fiziksel sağlamlık testleri doğrudan gözlemlenebilir.

Fiziksel katmanda bir sorun bulunduğunda üst katmanlardaki yapılandırmalar doğru olsa bile iletişim sağlıklı biçimde gerçekleşmeyebilir. Bu nedenle ağ sorunları incelenirken kablo, konnektör, port, sinyal durumu gibi fiziksel unsurlar öncelikle kontrol edilmelidir.

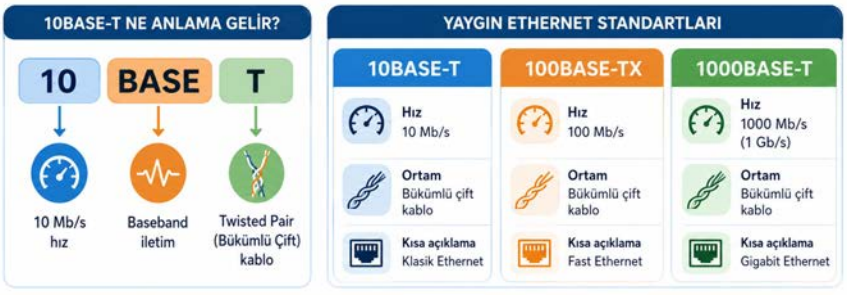
2.1.35. Ethernet Fiziksel Katman Standartları

Ethernet teknolojisi zaman içinde farklı hızları ve kablo yapılarını destekleyecek biçimde geliştirilmiştir. Fiziksel katman standartlarının adlarında kullanılan ifadeler, iletim hızını ve ortam türünü anlamaya yardımcı olur.

Örneğin 10BASE-T ifadesinde:

- **10**, saniyede 10 megabitlik veri iletim hızını;
- **BASE**, temel bant (baseband) iletimini;
- **T**, bükümlü çift (twisted pair) bakır kabloyu ifade eder.

Ethernet fiziksel katmanında kullanılan bazı temel standartlar Görsel 2.45'te verilmiştir.



Görsel 2.45: Ethernet fiziksel katman standartları

2.1.36. PoE (Power over Ethernet)

Ethernet Üzerinden Güç [Power over Ethernet (PoE)], uygun Ethernet kablosu üzerinden veriyle birlikte elektrik enerjisinin de iletilmesini sağlayan teknolojidir. Bu yapı sayesinde bazı ağ cihazlarında ayrı bir güç adaptörü veya ek elektrik kablosu kullanma ihtiyacı azalabilir.

PoE özellikle aşağıdaki cihazlarda kullanılabilir.

- IP kameralar
- Kablosuz erişim noktaları
- IP telefonlar
- PoE desteği bulunan bazı ağ cihazları

PoE'nin önemli avantajlarından biri, cihazların elektrik prizine yakın olmak zorunda kalmadan daha uygun noktalara yerleştirilebilmesidir. Örneğin tavana yerleştirilen bir kablosuz erişim noktası veya koridordaki bir IP kamera, desteklenen koşullarda tek Ethernet kablosu üzerinden hem ağ bağlantısı hem de elektrik enerjisi alabilir.

Not: PoE kullanımı için güç sağlayan portun veya enjektörün, bağlantı kablosunun ve uç cihazın uygun olması gerekir. Her Ethernet portu ve her ağ cihazı otomatik olarak PoE desteğine sahip değildir.

2.1.37. Ağ Medyaları

Ağ medyaları, verinin cihazlar arasında taşındığı fiziksel veya elektromanyetik iletim ortamlarıdır. Ağ iletişiminin gerçekleşebilmesi için cihazların yalnızca doğru biçimde yapılandırılması yeterli değildir. Verinin taşınacağı uygun ortamın da seçilmesi gerekir.

Ağ medyaları genel olarak üç grupta incelenebilir (Tablo 2.10).

Tablo 2.10: Ağ Medya Türleri ve Temel Özellikleri

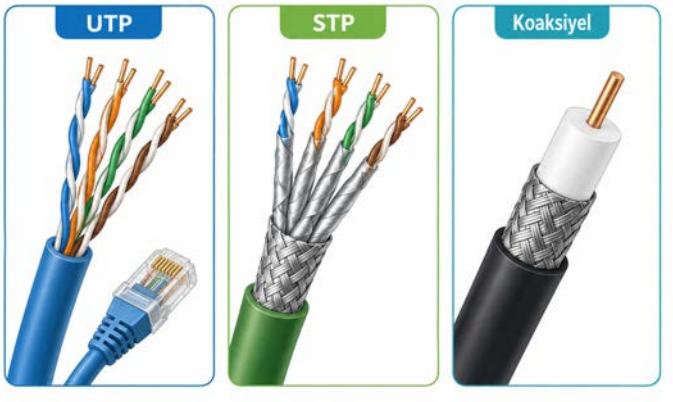
Ağ Medyası	Sinyal Türü	Temel Özelliği	Kullanım Örneği
Bakır kablo	Elektriksel sinyal	Yerel ağlarda yaygın, erişilebilir ve uygulaması görece kolaydır.	Bilgisayar ile switch arasındaki Ethernet bağlantısı
Fiber optik kablo	Işık sinyali	Yüksek hız, uzun mesafe ve elektromanyetik parazitlere karşı dayanıklılık avantajı sağlar.	Kampüs omurgası veya farklı binalar arasındaki bağlantı
Kablosuz ortam	Elektromanyetik dalga	Fiziksel kablo kullanmadan bağlantı kurulmasını sağlar.	Kablosuz erişim noktası üzerinden Wi-Fi bağlantısı

İletim ortamı seçilirken hız gereksinimi, bağlantı mesafesi, ortam koşulları, elektromanyetik parazit olasılığı, maliyet ve kurulum kolaylığı birlikte değerlendirilmelidir.

2.1.38. Bakır Kablo Türleri

Bakır kablolar, veriyi elektriksel sinyaller aracılığıyla taşıyan iletim ortamlarıdır. Özellikle yerel ağ bağlantılarında yaygın biçimde kullanılır. Kurulumlarının görece kolay olması, yaygın bulunmaları ve birçok kullanım senaryosunda uygun maliyet sunmaları önemli avantajlarıdır.

Bakır kabloların seçimi yapılırken iletim hızı, bağlantı mesafesi, elektromanyetik parazit, fiziksel ortam ve kullanılacak konnektör türü dikkate alınmalıdır (Görsel 2.46).



Görsel 2.46: Bakır kablo türleri

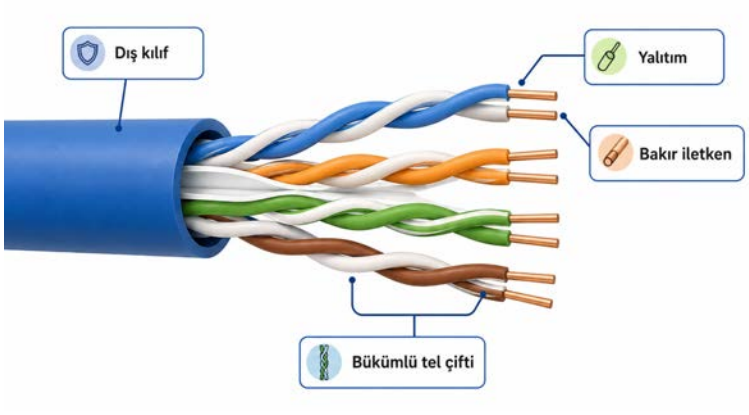
Bakır kablo türleri ve genel kullanım alanları Tablo 2.11'de verilmiştir.

Tablo 2.11: Bakır Kablo Türleri ve Genel Kullanım Alanları

Bakır Kablo Türü	Temel Yapısı	Genel Kullanım Alanı
Korumasız bükümlü çift kablo (UTP)	İletken çiftlerin birbirine sarılmasıyla oluşur. Ek metal koruma katmanı bulunmaz.	Yerel ağ bağlantıları
Korumalı bükümlü çift kablo (STP)	Parazit etkisini azaltmaya yardımcı olan ek koruma katmanları içerir.	Elektromanyetik parazit riskinin daha yüksek olduğu ortamlar
Koaksiyel kablo	Merkez iletken, yalıtım ve dış koruma katmanlarından oluşur.	Bazı eski ağ yapıları, yayın ve belirli iletişim altyapıları

2.1.39. Bükümlü Çift Yama Kablo Türleri

Bükümlü çift kablolar, yerel ağlarda yaygın olarak kullanılan iletim ortamları arasındadır. Bu kablolarda iletken damarlar belirli bir düzene göre konnektöre yerleştirilir. Kablonun iki ucunda kullanılan pin sırasına göre düz veya çapraz yama kablo oluşturulabilir (Görsel 2.47).



Görsel 2.47: Bükümlü Çift Kablonun Yapısı

Düz kabloda, kablonun iki ucu aynı sonlandırma standardına göre hazırlanır. Başka bir ifadeyle iki uçta da aynı pin dizilimi kullanılır.

Örnek

- Birinci uç: T568A
- İkinci uç: T568A

veya

- Birinci uç: T568B
- İkinci uç: T568B

Düz kablolar, geleneksel kullanım yaklaşımında farklı türdeki cihazların bağlanmasında kullanılır. Bilgisayar ile switch veya yönlendirici ile switch bağlantısı buna örnek verilebilir.

Çapraz kabloda kablonun bir ucu T568A, diğer ucu ise T568B standardına göre hazırlanır.

- Birinci uç: T568A
- İkinci uç: T568B

Çapraz kablolar, geleneksel kullanım yaklaşımında benzer türdeki cihazların doğrudan bağlanmasında kullanılabilir. Örneğin iki bilgisayarın veya iki switchin doğrudan birbirine bağlanması bu yapıyla ilişkilendirilebilir.

Auto MDI-X: bugün birçok ağ cihazı Auto MDI-X özelliğini destekler. Bu özellik, bağlantı için gerekli kablo düzeninin cihaz tarafından otomatik olarak algılanmasına yardımcı olur. Böylece birçok kullanım senaryosunda düz veya çapraz kablo seçimi kullanıcı açısından daha az kritik hâle gelir. Bununla birlikte T568A, T568B ve çapraz kablo mantığının öğrenilmesi önemlidir. Fiziksel bağlantı yapısının ve sonlandırma standartlarının bilinmesi, yanlış sonlandırmaların fark edilmesi ve laboratuvar uygulamalarının doğru gerçekleştirilmesi açısından önemlidir. Düz ve çapraz yama kablo türleri Görsel 2.48'de gösterilmiştir.



Görsel 2.48: Düz ve çapraz yama kablo türleri

2.1.40. Bükümlü Çift Kablo Kategorileri

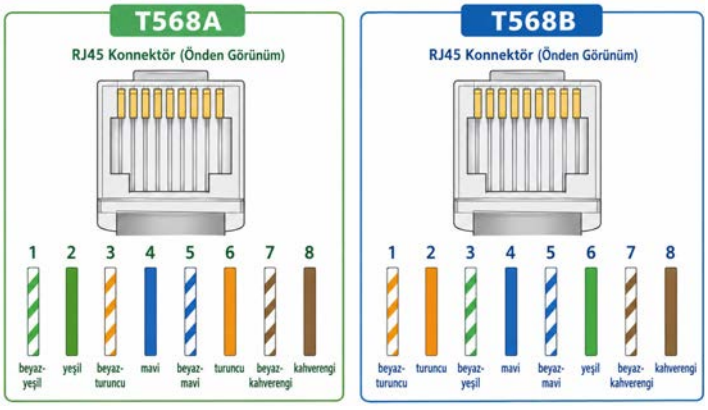
Bükümlü çift kablolar, destekledikleri iletim kapasitesi ve kullanım koşullarına göre farklı kategorilere ayrılır (Tablo 2.12). Kablo kategorisi seçilirken yalnızca hedef hız değil bağlantı uzunluğu, ortam koşulları, kurulum kalitesi ve kullanılacak ağ cihazları da dikkate alınmalıdır.

Tablo 2.12: Bükümlü Çift Kablo Kategorileri ve Genel Kullanım Özellikleri

Kablo Kategorisi	Genel Kullanım Yaklaşımı	Yaygın Mesafe Yaklaşımı	Örnek Kullanım
Cat5e	Gigabit Ethernet bağlantılarında kullanılabilir.	Uygun kurulum koşullarında 100 m kanal uzunluğuna kadar	Standart yerel ağ bağlantıları
Cat6	Gigabit Ethernet bağlantılarında yaygındır. Belirli koşullarda 10 Gb/s bağlantıları da destekleyebilir.	Gigabit bağlantılarda 100 m, 10 Gb/s için uygun kurulum koşullarında daha kısa mesafeler	Yerel ağ ve sınırlı yüksek hızlı bağlantılar
Cat6A	10 Gb/s bağlantılar için daha uygun yapı sunar.	Uygun kurulum koşullarında 100 m kanal uzunluğuna kadar	Kurumsal ağlar ve yüksek hızlı yerel bağlantılar
Cat8	Çok yüksek hızlı ve kısa mesafeli bakır bağlantılar için kullanılır.	25 Gb/s ve 40 Gb/s hızlarda en fazla 30 m kanal uzunluğu	Veri merkezi bağlantıları

2.1.41. Bükümlü Çift Kablo Sonlandırma Standartları

Bükümlü çift kablolarda bulunan sekiz iletken damar, konnektör içindeki pinlere belirli bir sıraya göre yerleştirilir. Bu sıra rastgele belirlenemez. İletim çiftlerinin doğru eşleşmesi, bağlantının kararlı biçimde kurulabilmesi ve veri aktarımının sağlıklı yürütülmesi kullanılan sonlandırma düzenine bağlıdır.



Görsel 2.49: Bükümlü çift kablo sonlandırma standartları

Ethernet tabanlı yerel ağ uygulamalarında yaygın olarak kullanılan iki temel sonlandırma standardı **T568A** ve **T568B**'dir. Her iki standartta da sekiz damar bulunur. Standartlar arasındaki temel fark, yeşil ve turuncu çiftlerin pinlere yerleştirilme sırasıdır (Görsel 2.49).

T568A ve T568B Renk Sıraları

Düz kablolarda kablonun her iki ucu aynı sonlandırma standardına göre hazırlanır. T568A düz kabloda kablonun her iki ucu T568A, T568B düz kabloda ise her iki ucu T568B standardına göre sonlandırılır. Çapraz kabloda kablonun bir ucu T568A, diğer ucu T568B standardına göre hazırlanır. Çapraz kabloda kablonun bir ucu T568A, diğer ucu ise T568B standardına göre hazırlanır.

Düz kabloda iki uç aynı standarda göre sonlandırılır. Çapraz kabloda ise kablonun bir ucunda T568A, diğer ucunda T568B standardı kullanılır.

2.1.42. Bakır Kablo Konnektör Türleri

Bakır kablolarda kullanılan konnektörler, kablonun yapısına ve kullanım alanına göre değişir. Bükümlü çift Ethernet kablolarında günlük kullanımda **RJ45** olarak adlandırılan sekiz konumlu modüler konnektör yaygın olarak kullanılır. Telefon ve bazı DSL bağlantılarında RJ11, koaksiyel kablolarda ise BNC gibi farklı konnektör türlerinden yararlanılabilir (Görsel 2.50). Bu nedenle bütün bakır kabloların aynı konnektörle sonlandırıldığı düşünülmemelidir. Ethernet tabanlı yerel ağ uygulamalarında RJ45 konnektörün doğru biçimde sonlandırılması önemlidir. Damarların uygun pinlere yerleştirilmemesi, iletkenlerin konnektör içine tam oturmaması veya sıkma işleminin hatalı yapılması bağlantı sorunlarına yol açabilir. Temel bakır kablo konnektörleri ve kullanım alanları şunlardır:



Görsel 2.50: Bakır kablo konnektör türleri

Konnektör Türü	Genel Kullanım Alanı
RJ45 olarak bilinen 8P8C modüler konnektör	Bükümlü çift Ethernet kabloları
RJ11	Telefon ve bazı DSL bağlantıları
BNC	Koaksiyel kablo kullanılan belirli iletişim yapıları

7. UYGULAMA

Uygulama Adı	Bükümlü Çift Ethernet Kablolarını Sonlandırmak
Süre	90 dakika
Amaç	Bükümlü çift Ethernet kablolarını T568A ve T568B standartlarına uygun biçimde sonlandırmak, düz ve çapraz kablo yapıları arasındaki farkı uygulamalı olarak gözlemlemek ve hazırlanan kabloların sağlamlığını test etmek
Araç Gereç	Bükümlü çift Ethernet kablosu, en az altı adet RJ45 olarak bilinen modüler konnektör, kablo soyma aparatı, RJ45 sıkma pensesi, kablo test cihazı, çalışma yaprağı, öğretmenin belirlediği iş sağlığı ve güvenliği ekipmanları.

İş Sağlığı ve Güvenliği Uyarıları

- Kablo soyma aparatı ve sıkma pensesini yalnızca öğretmeninizin yönergesine uygun biçimde kullanınız.
- Kesici yüzeyleri elinize ve arkadaşlarınıza doğru yöneltmeyiniz.
- Hasarlı aletleri kullanmayınız.
- Çalışma masasını düzenli tutunuz.
- Kesilen kablo parçalarını çalışma alanında bırakmayınız.
- Kabloyu enerji taşıyan bir cihaza bağlıyken sonlandırmaya çalışmayınız.
- Hazırlanan kabloyu kullanmadan önce test cihazıyla kontrol ediniz.
- Grup içinde görev paylaşımı yapınız.

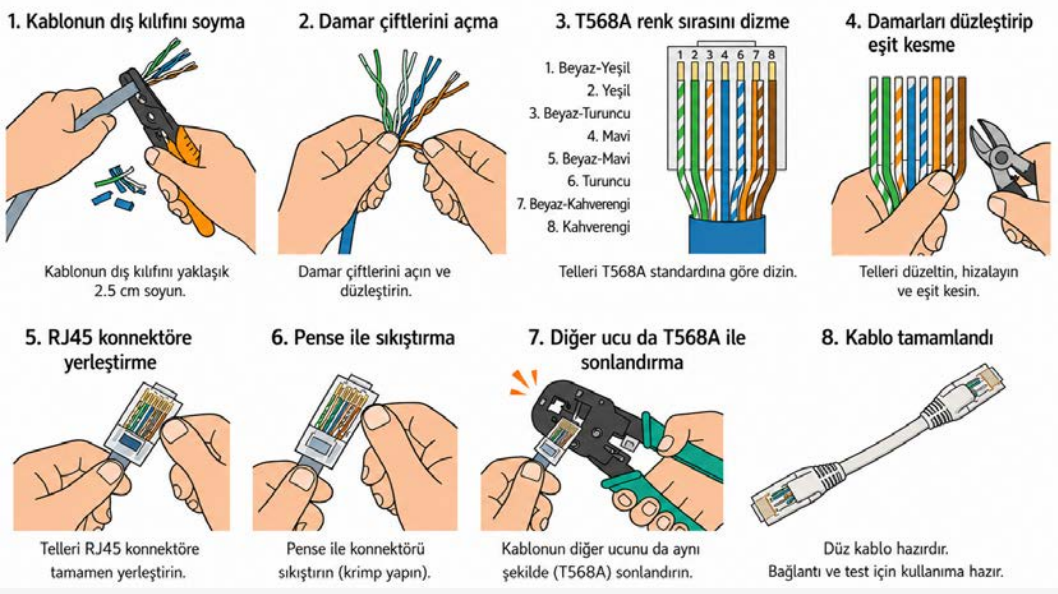
Kablo Sonlandırma İşlem Basamakları

1. Hazırlayacağınız kablonun türünü belirleyiniz: T568A düz, T568B düz veya çapraz kablo.
2. Kullanacağınız kabloyu uygun uzunlukta kesiniz.
3. Kablonun dış kılıfını, iç damarlara zarar vermeden dikkatlice soyunuz.
4. Bükümlü çiftleri ayırınız. Damarların gereğinden fazla açılmamasına dikkat ediniz.
5. İletken damarları kullanacağınız standardın renk sırasına göre diziniz.
6. Damarları yan yana getirerek düzleştiriniz.
7. Damar uçlarını birbirleriyle aynı uzunlukta olacak biçimde kesiniz.
8. Damarları pin sırasını bozmadan RJ45 konnektörün içine yerleştiriniz.
9. Bütün damarların konnektörün sonuna kadar ulaştığını kontrol ediniz.
10. Kablonun dış kılıfının konnektörün tutucu bölümünün içine girdiğini doğrulayınız.
11. Konnektörü sıkma pensesine yerleştiriniz ve uygun biçimde sıkınız.
12. Kablonun diğer ucunu temrinde belirtilen standarda göre hazırlayınız.
13. Her iki uçtaki pin sırasını görsel olarak yeniden kontrol ediniz.
14. Hazırladığınız kabloyu test cihazına bağlayınız.
15. Test sonucunu ortak gözlem formuna kaydediniz.

1. T568A Standardına Göre Düz Kablo Sonlandırmak

Amaç: Kablonun iki ucunu da T568A standardına göre hazırlayarak düz Ethernet kablosu oluşturmak (Görsel 2.51)

Birinci Uç: T568A
İkinci Uç: T568A

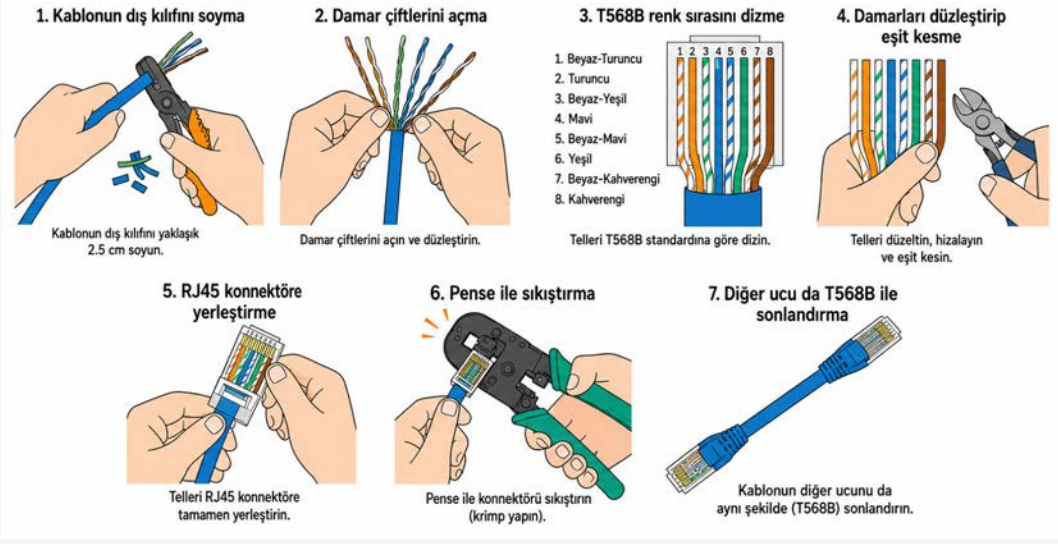


Görsel 2.51: T568A standardına göre RJ45 düz kablo sonlandırma uygulaması

2. T568B Standardına Göre Düz Kablo Sonlandırmak

Amaç: Kablonun iki ucunu da T568B standardına göre hazırlayarak düz Ethernet kablosu oluşturmak (Görsel 2.52)

Birinci Uç: T568B
İkinci Uç: T568B



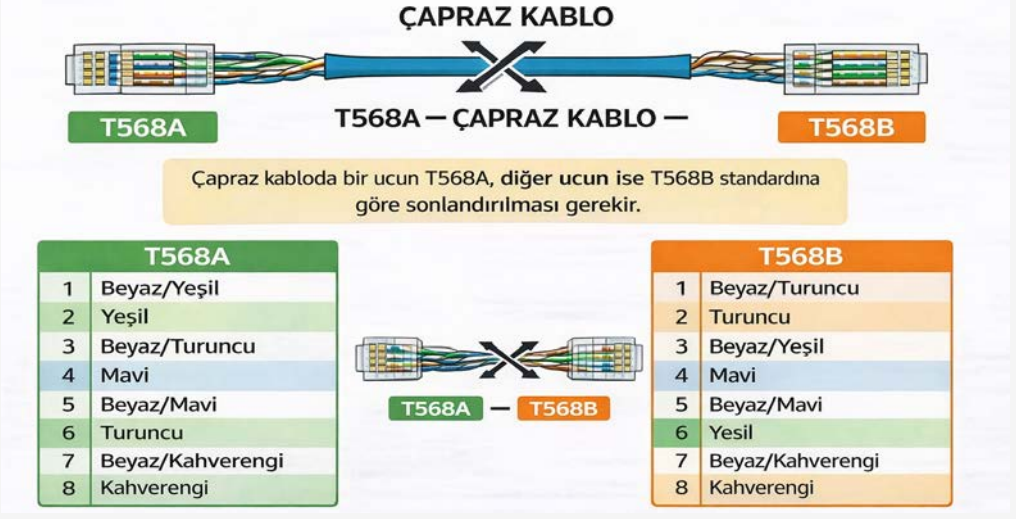
Görsel 2.52: T568B standardına göre RJ45 düz kablo sonlandırma uygulaması

3. Çapraz Kablo Sonlandırmak

Amaç: Kablonun bir ucunu T568A, diğer ucunu T568B standardına göre hazırlayarak çapraz Ethernet kablosu oluşturmak (Görsel 2.53)

Birinci Uç: T568A

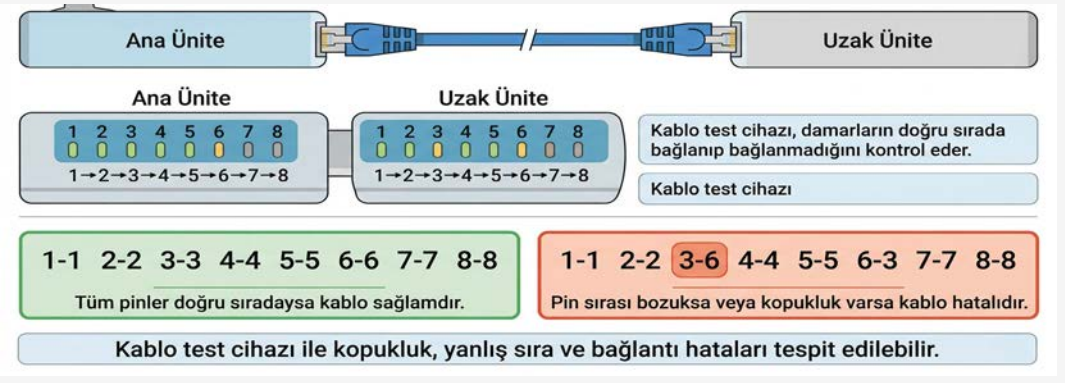
İkinci Uç: T568B



Görsel 2.53: Çapraz kablo sonlandırma uygulaması

Kablo Test Cihazıyla Sağlamlık Testi

Kablo test cihazı, sonlandırılan kablonun iletkenlerinin doğru pinlere bağlanıp bağlanmadığını kontrol etmek amacıyla kullanılır. Test cihazı sayesinde damar sırası, kopukluk, yanlış eşleşme ve belirli bağlantı hataları gözlemlenebilir (Görsel 2.54).



Görsel 2.54: Kablo test cihazıyla sağlamlık testi

Kablo sonlandırma işlemi yalnızca konnektörün sıkılmasıyla tamamlanmış sayılmaz. Hazırlanan kablo, kullanılmadan önce mutlaka test edilmelidir. Böylece fiziksel bağlantı sorunları ağ cihazlarına bağlanmadan önce belirlenebilir.

Test İşlemi

1. Hazırladığınız kablonun bir ucunu test cihazının ana bölümüne bağlayınız.
2. Diğer ucu test cihazının uzak birimine bağlayınız.
3. Test cihazını çalıştırınız.
4. Pin göstergelerini sırasıyla inceleyiniz.
5. Test sonucunu gözlem formuna yazınız.
6. Hata varsa kablonun iki ucundaki damar sırasını yeniden kontrol ediniz.
7. Gerekirse hatalı konnektörü çıkararak yeniden sonlandırma yapınız.
8. Yeniden test gerçekleştiriniz.

Beklenen Test Sonuçları

Kablo Türü	Beklenen Pin Eşleşmesi
T568A düz kablo	1→1, 2→2, 3→3, 4→4, 5→5, 6→6, 7→7, 8→8
T568B düz kablo	1→1, 2→2, 3→3, 4→4, 5→5, 6→6, 7→7, 8→8
Çapraz kablo	1→3, 2→6, 3→1, 4→4, 5→5, 6→2, 7→7, 8→8

Kablo Sonlandırma ve Test Sonuçları

Hazırlanan Kablo	Birinci Uç	İkinci Uç	Görsel Kontrol Sonucu	Test Cihazı Sonucu	Gerekliyse Yapılan Düzeltme
T568A düz kablo	T568A	T568A	☐ Uygun ☐ Hatalı	☐ Başarılı ☐ Hatalı	
T568B düz kablo	T568B	T568B	☐ Uygun ☐ Hatalı	☐ Başarılı ☐ Hatalı	
Çapraz kablo	T568A	T568B	☐ Uygun ☐ Hatalı	☐ Başarılı ☐ Hatalı	

Kablo Sonlandırma ve Sağlamlık Testi Dijital Rapor Şablonu

Grup Üyeleri:

.....

Uygulama Tarihi:

.....

Rapor Alanı	Açıklamanız
Hazırlanan kablo türleri	
T568A düz kablonun test sonucu	
T568B düz kablonun test sonucu	
Çapraz kablonun test sonucu	
Tespit edilen hata veya hatalar	
Uygulanan düzeltici işlem	
T568A ve T568B standartları arasındaki temel fark	
Çapraz kablonun düz kablodan farkı	
Uygulama sırasında dikkat edilmesi gereken güvenlik kuralı	

Değerlendirme

Çalışmanız öğretmeniniz tarafından kontrol listesine göre değerlendirilecektir. Çalışmanızı yaparken buradaki ölçütleri dikkate alınız. Kontrol listesi formuna ulaşmak için karekodu okutunuz. Dijital yayınlarda karekodun üstüne tıklayarak içeriğe ulaşabilirsiniz.

2.1.43. Fiber Optik Kablo Türleri

Fiber optik kablolar, veriyi elektriksel sinyaller yerine ışık sinyalleri aracılığıyla taşıyan iletim ortamlarıdır (Görsel 2.55). Bu özellikleri sayesinde yüksek hızlı ve uzun mesafeli ağ bağlantılarında önemli avantajlar sağlar. Fiber optik kablolar, elektromanyetik parazitlerden bakır kablolar gibi etkilenmez. Bu nedenle güçlü elektriksel cihazların bulunduğu ortamlarda, bina ve kampüs omurgalarında, veri merkezlerinde ve geniş ölçekli iletişim altyapılarında tercih edilebilir. Fiber optik kablo seçilirken yalnızca iletim hızı değil bağlantı mesafesi, kullanılacak ağ cihazları, konnektör türü, ortam koşulları ve kurulum maliyeti de dikkate alınmalıdır.



Görsel 2.55: Fiber optik kablonun yapısı

Fiber optik kablonun temel kısımları ve temel işlevleri Tablo 2.13'te verilmiştir.

Tablo 2.13: Fiber Optik Kablonun Temel Kısımları ve Temel İşlevleri

Bölüm	Temel İşlevi
Çekirdek (Core)	Işık sinyalinin ilerlediği merkez bölümdür.
Kaplama (Cladding)	Işığın çekirdek içinde ilerlemesine yardımcı olan çevre katmandır.
Koruyucu Kaplama (Coating/ Buffer)	Fiber yapının fiziksel etkilerden korunmasına yardımcı olur.
Dış Kılıf (Outer Jacket)	Kabloyu dış ortamdan, sürtünmeden ve belirli fiziksel etkilerden korur.

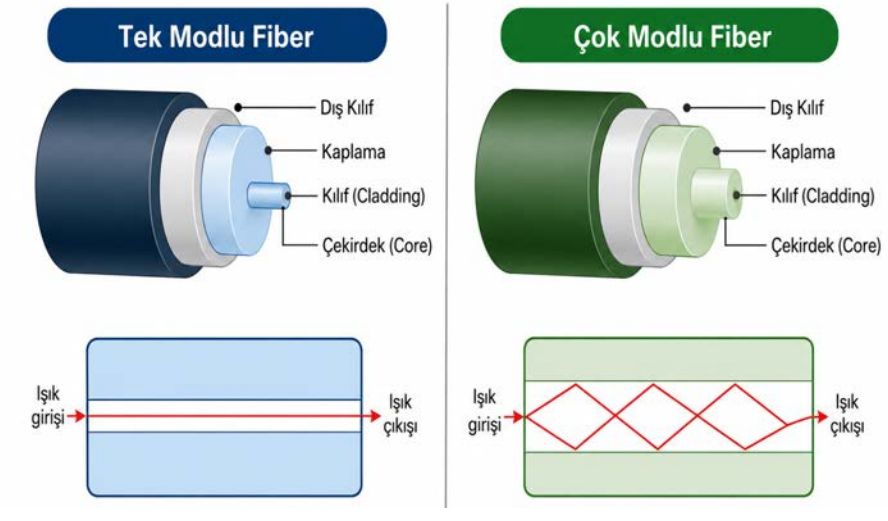
Tek Modlu Fiber

Tek modlu fiber, ışığın çekirdek içinde daha sınırlı bir yayılım yolu izlediği fiber optik kablo türüdür. Çekirdeğinin daha dar olması, ışığın farklı yollar üzerinden dağılmasını azaltır. Bu özellik, sinyalin daha uzun mesafelere daha kararlı biçimde iletilmesine yardımcı olur.

Tek modlu fiber kablolar; şehirler arası bağlantılarda, servis sağlayıcı omurgalarında, kampüsler arası iletişimde ve uzun mesafeli kurumsal ağ bağlantılarında kullanılabilir. Tek modlu fiber şu cümleyle özetlenebilir: "Daha uzun mesafe, daha dar çekirdek, daha sınırlı ışık yayılımı."

Çok Modlu Fiber

Çok modlu fiber, ışığın çekirdek içinde birden fazla yayılım yolu izleyebildiği fiber optik kablo türüdür. Çekirdeğinin tek modlu fibere göre daha geniş olması, ışığın farklı açılarla ilerleyebilmesini sağlar. Bu yapı kısa ve orta mesafeli bağlantılarda işlevseldir ancak mesafe arttıkça farklı ışık yollarının oluşturduğu yayılım farkları sinyal kalitesini etkileyebilir. Çok modlu fiber kablolar; bina içi ağ bağlantılarında, sunucu odalarında, veri merkezlerinde ve kampüs içindeki kısa mesafeli fiber bağlantılarda kullanılabilir. Çok modlu fiber şu cümleyle özetlenebilir: Daha kısa mesafe, daha geniş çekirdek ve birden fazla ışık yayılım yoludur. Tek modlu ve çok modlu fiber optik kablolar Görsel 2.56'da gösterilmiştir.



Görsel 2.56: Tek modlu ve çok modlu fiber optik kablolar

Tek ve çok modlu fiberin karşılaştırılması Tablo 2.14'te verilmiştir.

Tablo 2.14: Tek ve Çok Modlu Fiberin Karşılaştırılması

Özellik	Tek Modlu Fiber	Çok Modlu Fiber
Çekirdek yapısı	Daha dardır.	Daha geniştir.
Işığın ilerleme biçimi	Daha sınırlı bir yayılım yolu izler.	Birden fazla yayılım yolu izleyebilir.
Genel mesafe yaklaşımı	Uzun mesafeli bağlantılar için daha uygundur.	Kısa ve orta mesafeli bağlantılar için uygundur.
Yayılım farklarının etkisi	Daha düşüktür.	Mesafe arttıkça daha belirgin olabilir.
Örnek kullanım alanı	Servis sağlayıcı omurgası, şehirler arası bağlantı, kampüsler arası bağlantı	Bina içi ağ, sunucu odası, veri merkezi, kampüs içi kısa bağlantı
Donanım ve kurulum yaklaşımı	Kullanılan donanıma göre daha yüksek maliyet oluşturabilir.	Kısa mesafeli bazı kurulumlarda daha uygun maliyetli olabilir.

2.1.44. Fiber Optik Kablo Konnektörleri

Fiber optik kabloların ağ cihazlarına, optik modüllere ve bağlantı panellerine bağlanabilmesi için uygun **fiber optik konnektörler** kullanılır. Fiber optik bağlantılarda iletim elektriksel değil, optiktir. Bu nedenle bağlantı yüzeylerinin hizalanması, temizliği ve fiziksel bütünlüğü önem taşır. Fiber optik kablolarda farklı konnektör türleri bulunabilir. Kullanılacak konnektör; ağ cihazına, optik modüle, bağlantı paneline ve kurulum yapısına göre seçilir. LC, SC ve ST yaygın olarak tanınması gereken fiber optik konnektör türleri arasındadır (Görsel 2.57).



Görsel 2.57: Fiber optik kablo konnektörleri

Fiber optik konnektör türleri Tablo 2.15'te verilmiştir.

Tablo 2.15: Fiber Optik Konnektör Türleri

Konnektör Türü	Temel Yapısı	Genel Kullanım Yaklaşımı
LC	Küçük boyutlu ve mandallı yapıdadır.	Bağlantı yoğunluğunun yüksek olduğu modern ağ cihazlarında ve optik modüllerde yaygın olarak kullanılabilir.
SC	Kareye yakın gövdeli, takılıp çıkarılması kolay bir yapıdadır.	Fiber bağlantı panellerinde ve çeşitli ağ bağlantılarında yaygın olarak kullanılabilir.
ST	Yuvarlak gövdeli ve döndürülerek sabitlenen bir yapıdadır.	Daha eski veya belirli fiber optik kurulumlarda görülebilir.

İş Sağlığı ve Güvenliği Uyarısı: Fiber optik kablonun veya konnektörün ucuna doğrudan bakmayınız. Fiber bağlantıda görünür olmayan ışık sinyalleri bulunabilir. Fiber optik kablo kesme, soyma ve sonlandırma işlemlerini yalnızca uygun ekipmanla ve öğretmen gözetiminde gerçekleştiriniz. Fiber parçalarını çalışma alanında bırakmayınız.

Fiziksel katmanda kullanılacak iletim ortamı seçilirken tek bir ölçüte göre karar verilmemelidir. Hız, mesafe, ortam koşulları, maliyet, bağlantı yoğunluğu, güvenilirlik ve kurulum gereksinimleri birlikte değerlendirilmelidir. Yerel ağlarda bakır kablolar yaygın olarak kullanılabilirken uzun mesafeli veya yüksek kapasiteli omurga bağlantılarında fiber optik kablolar tercih edilebilir. Kablosuz ortamlar ise hareketlilik ve kullanım kolaylığı sağlar.

2.2. TCP/IP PROTOKOL KÜMESİ

TCP/IP protokol kümesi, ağ üzerindeki cihazların belirli kurallara göre iletişim kurmasını sağlayan protokollerin bütünüdür. İnternet erişimi, web sayfalarının görüntülenmesi, e-posta gönderimi, dosya aktarımı, ad çözümleme ve farklı ağlar arasındaki veri iletimi bu protokol kümesindeki yapıların birlikte çalışmasıyla gerçekleşir.

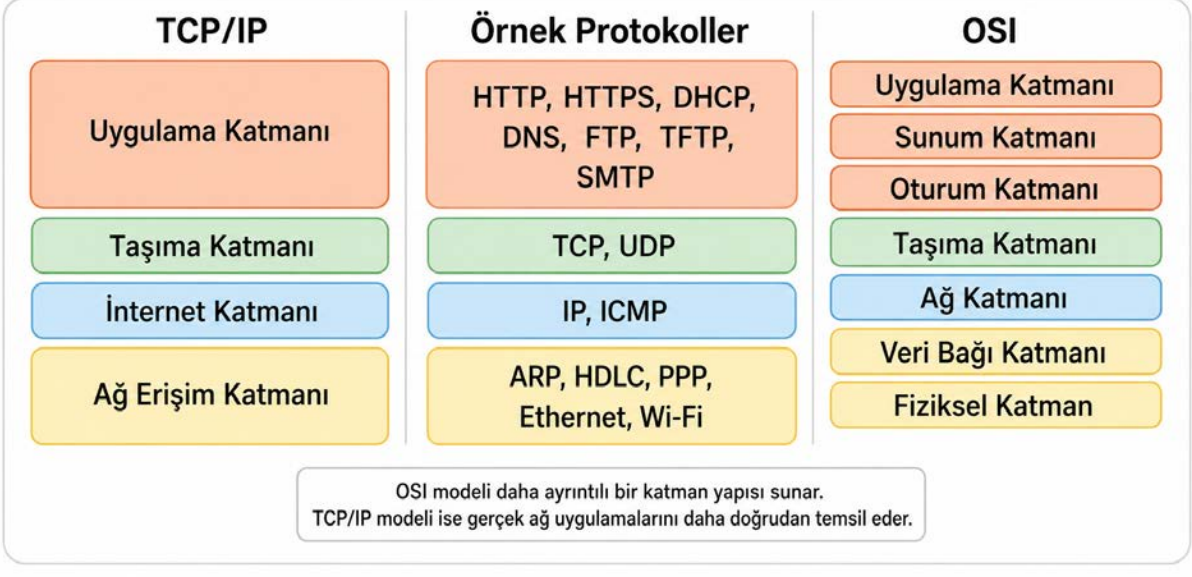
TCP/IP modeli ise bu iletişim sürecini daha anlaşılır hâle getirmek amacıyla protokolleri ve görevleri katmanlar altında ele alan yapıdır. TCP/IP modeli çoğunlukla **uygulama**, **taşıma**, **internet** ve **ağ erişim** olmak üzere dört katmanda incelenir.

Her katman belirli bir sorumluluk alanına sahiptir. Bir web sayfasına erişildiğinde yalnızca tek bir protokol çalışmaz. Uygulama katmanında web erişimiyle ilişkili protokoller kullanılır, taşıma katmanında uçtan uca iletişim düzenlenir, internet katmanında mantıksal adresleme ve yönlendirme gerçekleştirilir, ağ erişim katmanında ise veri fiziksel veya kablosuz ortam üzerinden taşınır.

Not: ARP, IPv4 adresi ile MAC adresi arasındaki eşleştirmeyi sağladığı için internet katmanı ile ağ erişim katmanı arasındaki ilişkiyi anlamada önemlidir. Bu nedenle ARP, katmanlar arası iletişimi açıklayan bir yapı olarak değerlendirilmelidir.

2.2.1. TCP/IP Modeli ile OSI Referans Modelinin Karşılaştırılması

OSI referans modeli ile TCP/IP modeli, ağ iletişimini katmanlı biçimde açıklayan iki önemli yapıdır. Her iki model de karmaşık iletişim sürecini daha anlaşılır görev alanlarına ayırır. Bununla birlikte katman sayıları ve kullanım yaklaşımları farklıdır (Görsel 2.58).



Görsel 2.58: TCP/IP modeli ile OSI referans modelinin karşılaştırılması

OSI referans modeli, ağ iletişim görevlerini yedi katmanda ele alan kavramsal bir başvuru çerçevesidir. TCP/IP modeli ise internet tabanlı ağlarda kullanılan protokolleri ve görevleri çoğunlukla dört katman altında açıklar. OSI referans modelindeki bazı katmanlar, TCP/IP modelinde daha geniş kapsamlı tek bir katman altında değerlendirilir (Tablo 2.16).

Tablo 2.16: OSI Referans Modeli ile TCP/IP Modelinin Katmanlarının Karşılaştırılması

OSI Referans Modeli	TCP/IP Modeli
7. Uygulama Katmanı	Uygulama Katmanı
6. Sunum Katmanı	Uygulama Katmanı
5. Oturum Katmanı	Uygulama Katmanı
4. Taşıma Katmanı	Taşıma Katmanı
3. Ağ Katmanı	İnternet Katmanı
2. Veri Bağı Katmanı	Ağ Erişim Katmanı
1. Fiziksel Katman	Ağ Erişim Katmanı

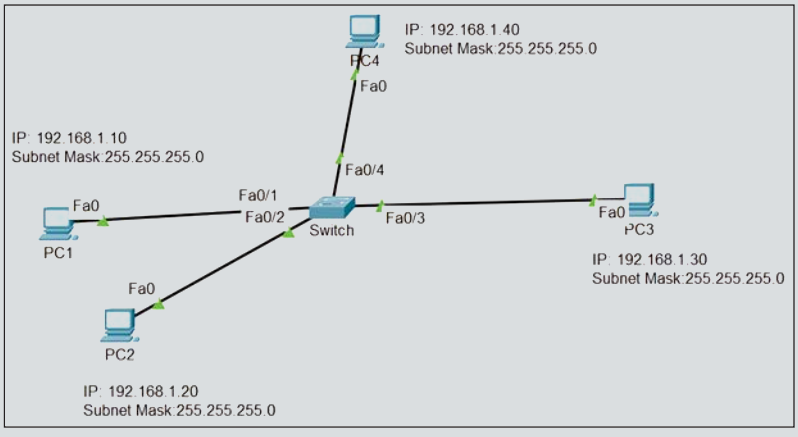
- OSI modelindeki uygulama, sunum ve oturum katmanlarının işlevleri TCP/IP modelindeki uygulama katmanı kapsamında ele alınır. Bu katman; kullanıcıya yönelik ağ hizmetlerini, veri biçimlendirme ve dönüştürme işlemlerini ve oturum yönetimini kapsar.
- Taşıma katmanı her iki modelde de ayrı bir katman olarak bulunur ve uçtan uca iletişim, hata denetimi ve port numaralarıyla ilişkilidir.
- OSI modelindeki ağ katmanı, TCP/IP modelindeki internet katmanına karşılık gelir. Bu katman mantıksal adresleme ve yönlendirme işlemlerini gerçekleştirir.
- OSI modelindeki veri bağı ve fiziksel katmanların işlevleri, TCP/IP modelindeki ağ erişim katmanı kapsamında ele alınır. Bu katman; çerçeveleme, ortam erişimi ve bitlerin fiziksel ya da kablosuz ortam üzerinden iletilmesiyle ilişkilidir.

BİLGİ KUTUSU : Katmanlı Ağ Modelleri Neden Kullanılır?

Katmanlı ağ modelleri, ağ iletişimini daha küçük ve yönetilebilir bölümlere ayırarak sistemlerin anlaşılmasını kolaylaştırır. Her katman belirli görevlerden sorumlu olduğu için bir ağ sorunu ortaya çıktığında problemin kaynağı daha sistemli biçimde araştırılabilir. Örneğin bağlantı kablosu, IP yapılandırması ve kullanılan uygulama ayrı aşamalarda kontrol edilebilir. Katmanlı yapı ayrıca farklı üreticilere ait cihazların ve ağ yazılımlarının ortak standartlara göre birlikte çalışmasına katkı sağlar.

8. UYGULAMA

Uygulama Adı	Aynı Ağdaki İki Bilgisayarı TCP/IP Yapılandırmasıyla Haberleştirmek
Süre	20 dakika
Amaç	Aynı yerel ağdaki iki bilgisayara uygun IPv4 adresleri ve alt ağ maskeleri tanımlayarak temel iletişimi gerçekleştirmek ve bağlantıyı ping komutuyla sınamak (Görsel 2.59)
Yönerge	Aşağıdaki adres planını kullanarak aynı yerel ağda bulunan iki istemci bilgisayarı TCP/IP ayarlarıyla yapılandırınız. Cihazları uygun kablolarla switche bağlayınız. Her iki bilgisayarda IPv4 adresi ve alt ağ maskesi bilgilerini tanımlayınız. Yapılandırmayı ipconfig komutuyla kontrol ediniz ve bilgisayarlar arasındaki bağlantıyı ping komutuyla sınayınız. Elde ettiğiniz sonuçları gözlem tablosuna yazınız ve uygulama sonunda soruları cevaplayınız.
Araç Gereç	Ağ simülasyon programı, bir switch, iki istemci bilgisayar, çalışma yaprağı.



Görsel 2.59: Aynı ağdaki iki bilgisayarın TCP/IP yapılandırması

Dikkat Edilecek Noktalar

- İki istemciyi aynı switche bağlayınız.
- İstemciler için aynı ağ bloğunda bulunan farklı IPv4 adresleri kullanınız.
- Her iki istemcide de aynı alt ağ maskesini tanımlayınız.
- Aynı yerel ağdaki iletişim için varsayılan ağ geçidi tanımlamanın zorunlu olmadığını gözlemleyiniz.
- Bağlantı sağlanamazsa fiziksel bağlantıları, IP adreslerini, alt ağ maskelerini ve switch portlarını sırayla kontrol ediniz.
- Grup içinde görev paylaşımı yapınız.

Adres Planı

Cihaz	IPv4 Adresi	Alt Ağ Maskesi	Varsayılan Ağ Geçidi
PC1	192.168.1.10	255.255.255.0	Bu uygulamada gerekli değildir.
PC3	192.168.1.30	255.255.255.0	Bu uygulamada gerekli değildir.

İki cihazın ağ adresi aşağıdaki biçimde değerlendirilir.

Cihaz	IPv4 Adresi	Ön Ek Uzunluğu	Ağ Adresi
PC1	192.168.1.10	/24	192.168.1.0
PC3	192.168.1.30	/24	192.168.1.0

Her iki cihazın ağ adresi aynı olduğu için cihazlar aynı yerel ağda bulunmaktadır.

Uygulama Adımları

1. Adım: Topolojiyi Oluşturmak

Ağ simülasyon programında aşağıdaki cihazları çalışma alanına ekleyiniz.

- bir switch
- PC1
- PC3

İstemcileri uygun bakır düz kablolarla switche bağlayınız.

2. Adım: PC1 Cihazını Yapılandırmak

PC1 cihazını açınız. **Desktop > IP Configuration** bölümüne geçiniz.

Aşağıdaki bilgileri giriniz:

IPv4 Address: 192.168.1.10

Subnet Mask: 255.255.255.0

Bu uygulamada varsayılan ağ geçidi alanını boş bırakabilirsiniz.

3. Adım: PC3 Cihazını Yapılandırmak

PC3 cihazını açınız. **Desktop > IP Configuration** bölümüne geçiniz.

Aşağıdaki bilgileri giriniz.

IPv4 Address: 192.168.1.30

Subnet Mask: 255.255.255.0

Bu uygulamada varsayılan ağ geçidi alanını boş bırakabilirsiniz.

4. Adım: Yapılandırmayı Kontrol Etmek

PC1 ve PC3 cihazlarının komut satırlarında aşağıdaki komutu kullanarak yapılandırma bilgilerini kontrol ediniz.

ipconfig

5. Adım: PC1 Cihazından PC3 Cihazına Erişimi Sınamak

PC1 cihazının komut satırında aşağıdaki komutu çalıştırınız.

ping 192.168.1.30

6. Adım: Ters Yönde Erişimi Sınamak

PC3 cihazının komut satırında aşağıdaki komutu çalıştırınız.

ping 192.168.1.10

7. Adım: Sonuçları Kaydetmek

Elde ettiğiniz sonuçları gözlem tablosuna yazınız.

Not: İlk ping denemesinde ARP eşleştirmesinin oluşturulması nedeniyle kısa bir gecikme veya ilk yanıtta başarısızlık görülebilir.

Aynı Ağdaki İki Bilgisayarın TCP/IP Yapılandırması Gözlem Tablosu

İncelenen Unsur	Gözlemlediğiniz Sonuç	
PC1 cihazının IPv4 adresi		
PC1 cihazının alt ağ maskesi		
PC3 cihazının IPv4 adresi		
PC3 cihazının alt ağ maskesi		
İki cihaz aynı switche bağlı mı?	☐ Evet	☐ Hayır
İki cihazın ağ adresleri aynı mı?	☐ Evet	☐ Hayır
PC1 üzerinden PC3 cihazına ping yanıtı alındı mı?	☐ Evet	☐ Hayır
PC3 üzerinden PC1 cihazına ping yanıtı alındı mı?	☐ Evet	☐ Hayır
Varsayılan ağ geçidi tanımlandı mı?	☐ Evet	☐ Hayır
Varsayılan ağ geçidi tanımlanmadan iletişim sağlandı mı?	☐ Evet	☐ Hayır
Karşılaşılan sorun varsa kısa açıklaması		
Sorunu gidermek için yapılan işlem		

Sonuçları Yorumlamak

Aşağıdaki soruları cevaplayınız.

1. İki bilgisayarın aynı yerel ağda haberleşebilmesi için hangi temel koşulların sağlanması gerekir?

.....
.....

2. Bu uygulamada neden yönlendirici kullanılmamıştır?

.....
.....

3. Bu uygulamada varsayılan ağ geçidi tanımlanmadan iletişim kurulabilmesinin nedeni nedir?

.....
.....

4. PC3 cihazının IPv4 adresi 192.168.2.30/24 olarak değiştirilseydi iletişim doğrudan sürdürülebilir miydi? Açıklayınız.

.....
.....

Değerlendirme

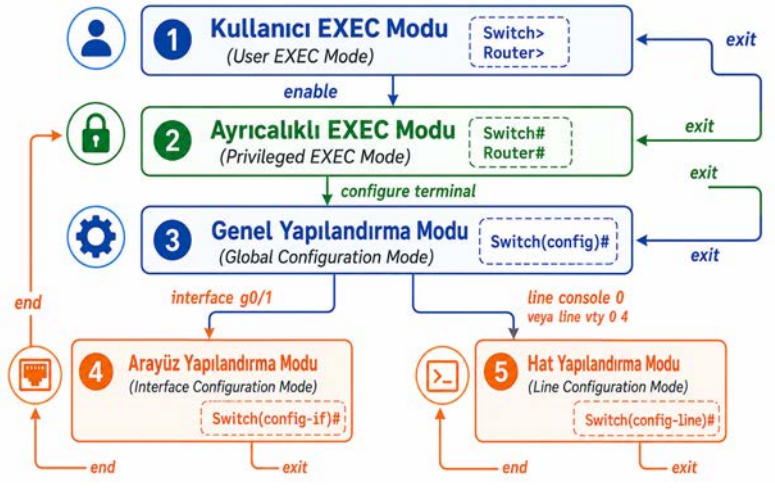
Çalışmanız öğretmeniniz tarafından kontrol listesine göre değerlendirilecektir. Çalışmanızı yaparken buradaki ölçütleri dikkate alınız. Kontrol listesi formuna ulaşmak için karekodu okutunuz. Dijital yayınlarda karekodun üstüne tıklayarak içeriğe ulaşabilirsiniz.

2.3. AĞ PROTOKOLLERİ

Ağ iletişimi yalnızca cihazların birbirine bağlanmasıyla tamamlanmaz. Cihazların belirli görevleri ortak kurallara göre yerine getirebilmesi için ağ protokollerinden yararlanılır. IP adreslerinin otomatik dağıtılması, alan adlarının IP adresleriyle eşleştirilmesi, web sayfalarının görüntülenmesi, dosya aktarımı, e-posta iletişimi ve ağ cihazlarının uzaktan yönetilmesi farklı protokoller aracılığıyla gerçekleştirilir.

Ağ Cihazlarında Temel Komut Modları

Bazı uygulamalarda yönlendirici ve switch cihazlarının komut satırı arayüzü kullanılacaktır. Cihaza IP adresi vermek, arayüzü etkinleştirmek, DHCP havuzu oluşturmak, bağlantıyı sınamak gibi işlemler belirli komut modlarında gerçekleştirilir (Görsel 2.60).



Görsel 2.60: Switch ve yönlendiricilerde temel komut modları

Komut veya Komut Modu	Temel İşlevi
enable	Ayrıcalıklı komut moduna geçer.
configure terminal	Genel yapılandırma moduna geçer.
interface g0/1	Belirtilen arayüzün yapılandırma moduna geçer.
no shutdown	Arayüzü etkinleştirir.
exit	Bir önceki komut moduna döner.
end	Yapılandırma modundan çıkar.
show running-config	Etkin yapılandırmayı görüntüler.
show ip interface brief	Arayüzlerin temel durumunu özetler.

2.3.1. DHCP Protokolü

Dinamik Ana Bilgisayar Yapılandırma Protokolü [Dynamic Host Configuration Protocol (DHCP)], istemci cihazlara ağ yapılandırma bilgilerini otomatik olarak dağıtan protokoldür. DHCP sayesinde bilgisayar, tablet, yazıcı vb. istemcilerin IP adreslerinin tek tek elle girilmesi gerekmez. DHCP sunucusu, önceden tanımlanmış bir adres havuzundan uygun IP adreslerini istemcilere belirli sürelerle tahsis eder. Ağ yapısına göre istemcilere aşağıdaki bilgiler de iletilebilir.

- IP adresi
- alt ağ maskesi
- varsayılan ağ geçidi
- DNS sunucusu adresi
- adresin kullanım süresi

DHCP kullanımı, özellikle çok sayıda cihazın bulunduğu ağlarda yapılandırma sürecini kolaylaştırır. Elle adres verme sırasında oluşabilecek IP çakışması, yanlış alt ağ maskesi veya hatalı ağ geçidi tanımlama gibi sorunların azaltılmasına yardımcı olur. DHCP hizmeti ayrı bir sunucu üzerinden sağlanabileceği gibi uygun özelliklere sahip yönlendiriciler tarafından da sunulabilir.

2.3.2. DHCPv4 Süreci DORA

Bir istemcinin DHCP sunucusundan otomatik IPv4 adresi alması sırasında temel olarak dört adımlı bir süreç gerçekleşir. Bu süreç, aşamaların İngilizce adlarının ilk harflerinden oluşan **DORA** kısaltmasıyla ifade edilir.

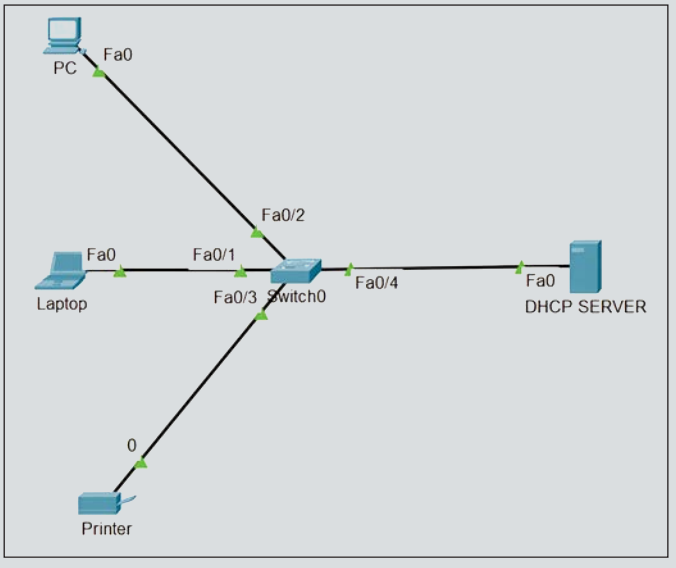
DHCPv4 DORA Aşamaları Tablo 2.17'de verilmiştir.

Tablo 2.17: DHCPv4 DORA Aşamaları

Sıra	Mesaj	Mesajı Gönderen	Temel İşlevi
1	Discover	İstemci	Ağda kullanılabilir bir DHCP sunucusu aradığını bildirir.
2	Offer	DHCP sunucusu	İstemciye uygun bir IPv4 adresi ve yapılandırma bilgileri önerir.
3	Request	İstemci	Önerilen IPv4 adresini kullanmak istediğini bildirir.
4	Acknowledgment – DHCPACK	DHCP sunucusu	İstemcinin isteğini onaylar ve yapılandırmanın kullanılabileceğini bildirir.

9. UYGULAMA

Uygulama Adı	DHCPv4 ile Otomatik IPv4 Adresi Dağıtmak
Süre	60 dakika
Amaç	DHCPv4 hizmetini kullanarak istemci cihazlara otomatik IPv4 yapılandırması sağlamak; bağımsız DHCP sunucusu ve yönlendirici tabanlı DHCP dağıtımını yapılandırmak, istemcilerin aldığı adresleri kontrol etmek ve bağlantı testleriyle sonucu doğrulamak (Görsel 2.61)
Araç Gereç	Ağ simülasyon programı, switch, yönlendirici, sunucu, istemci bilgisayarlar, dizüstü bilgisayar, ağ yazıcısı.



Görsel 2.61: DHCP Sunucusu üzerinden otomatik IPv4 dağıtımı topolojisi

Dikkat Edilecek Noktalar

- Sunucu veya yönlendirici üzerindeki DHCP havuzunu doğru ağ adresine göre tanımlayınız.
- Dağıtılmaması gereken sabit adresleri havuz dışında bırakınız.
- İstemcilerin DHCP seçeneğini etkinleştiriniz.
- İstemcilerin aldığı IP adreslerini, alt ağ maskelerini ve varsayılan ağ geçitlerini kaydediniz.
- Birbirinden farklı ağlarda bulunan istemciler için yönlendirici yapılandırmasını kontrol ediniz.
- Uygulama sonunda ping komutuyla temel erişimi sınayınız.
- Grup içinde görev paylaşımı yapınız.

A) DHCP Sunucusu Üzerinden Otomatik IPv4 Adresi Dağıtmak

Amaç: Aynı yerel ağda bulunan istemci cihazların ayrı bir DHCP sunucusundan otomatik IPv4 adresi almasını sağlamak

Adres Planı

Cihaz	IPv4 Adresi	Alt Ağ Maskesi	Yapılandırma Türü
DHCP sunucusu	192.168.10.2	255.255.255.0	Statik
Bilgisayar	DHCP üzerinden alınacak	DHCP üzerinden alınacak	Otomatik
Dizüstü bilgisayar	DHCP üzerinden alınacak	DHCP üzerinden alınacak	Otomatik
Ağ yazıcısı	DHCP üzerinden alınacak	DHCP üzerinden alınacak	Otomatik

DHCP Havuzu

Alan	Tanımlanacak Değer
Havuz adı	LAN_HAVUZU
Başlangıç IPv4 adresi	192.168.10.100
Alt ağ maskesi	255.255.255.0
Varsayılan ağ geçidi	Bu topolojide zorunlu değildir.
DNS sunucusu	DNS uygulaması yapılmayacaksa boş bırakılabilir.
Dağıtılacak en fazla istemci sayısı	Öğretmenin belirlediği uygun değer

Uygulama Adımları

1. Adım: Topolojiyi Oluşturmak

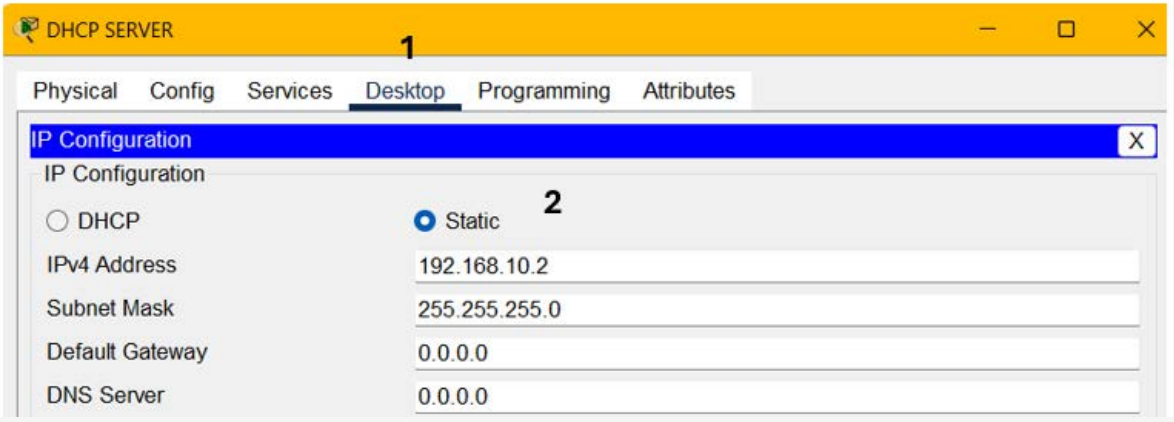
Simülasyon alanına şu cihazları ekleyiniz:

- bir switch
- bir sunucu
- bir bilgisayar
- bir dizüstü bilgisayar
- bir ağ yazıcısı

Cihazları switche uygun kablolarla bağlayınız.

2. Adım: DHCP Sunucusuna Sabit IPv4 Adresi Vermek

Sunucuyu açınız. **Desktop > IP Configuration** bölümüne geçiniz (Görsel 2.62).



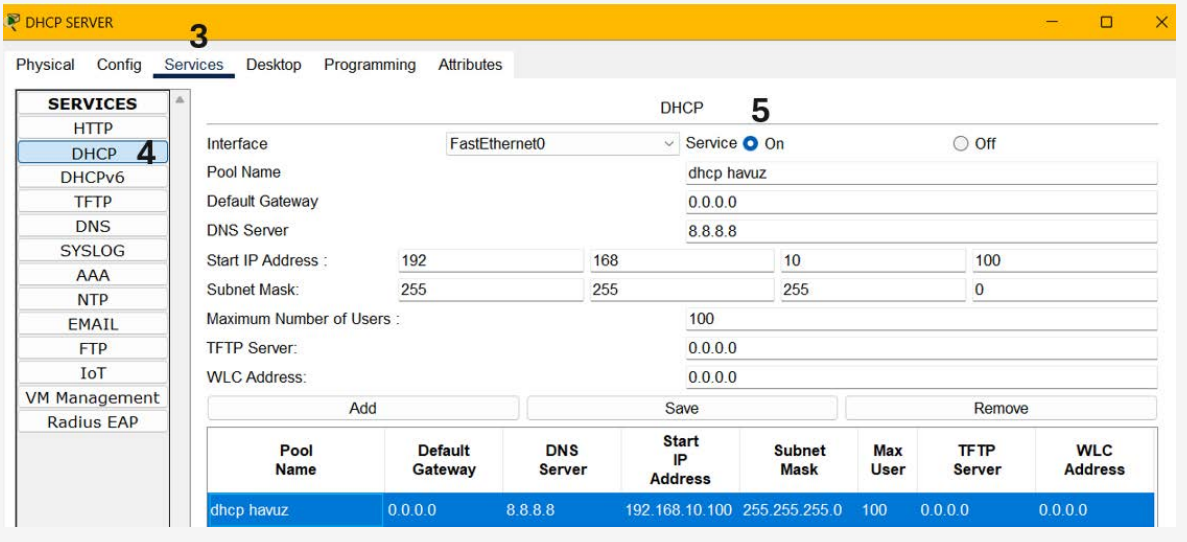
Görsel 2.62: DHCP sunucusuna sabit IPv4 adresi verilmesi

IPv4 Address: 192.168.10.2

Subnet Mask: 255.255.255.0

3. Adım: DHCP Hizmetini Etkinleştirmek

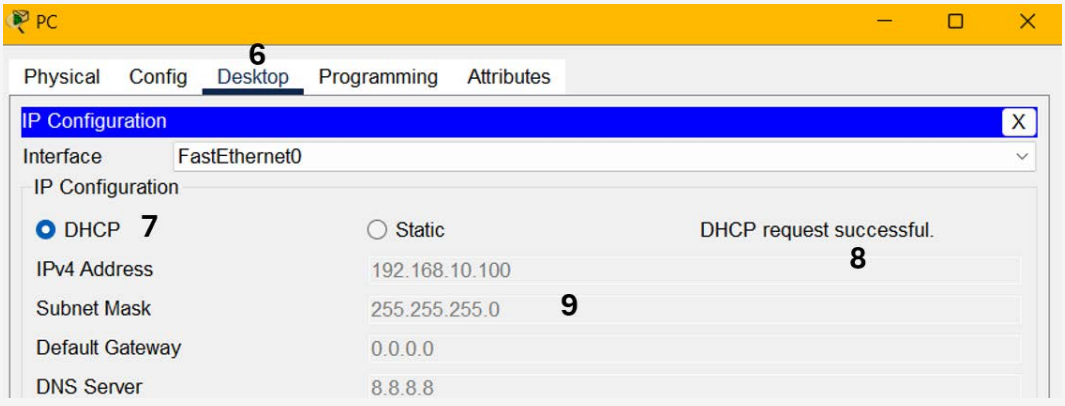
Sunucuda **Services > DHCP** bölümüne geçiniz. DHCP hizmetini etkinleştiriniz. LAN_HAVUZU adlı havuzu oluşturunuz ve tabloda verilen değerleri giriniz (Görsel 2.63).



Görsel 2.63: DHCP sunucusunda IPv4 adres havuzunun oluşturulması

4. Adım: Bilgisayarı DHCP İstemcisi Olarak Yapılandırmak

Bilgisayarı açınız. **Desktop > IP Configuration** bölümüne geçiniz. **DHCP** seçeneğini etkinleştiriniz (Görsel 2.64).



Görsel 2.64: İstemcinin DHCP üzerinden otomatik IPv4 adresi alması

5. Adım: Diğer İstemcileri Yapılandırmak

Aynı işlemi dizüstü bilgisayar ve ağ yazıcısı için de gerçekleştiriniz.

6. Adım: Otomatik Dağıtılan Adresleri Kontrol Etmek

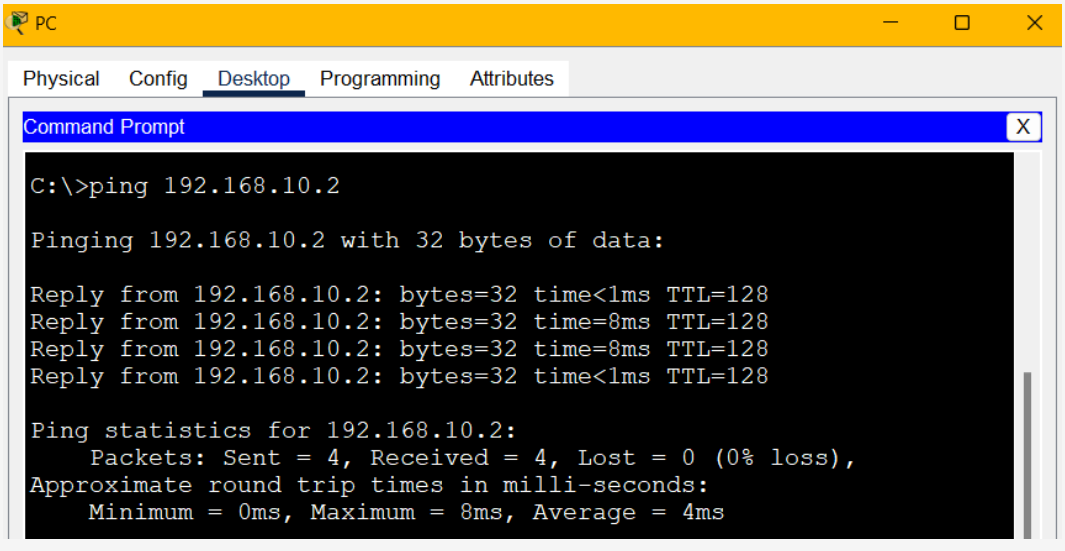
Her cihazın aldığı IPv4 adresini inceleyiniz. İstemcilerin 192.168.10.0/24 ağı içinde ve belirlenen havuz aralığından adres aldığını doğrulayınız.

7. Adım: Bağlantı Testini Gerçekleştirmek

Bilgisayardan DHCP sunucusuna erişimi sınayınız:

ping 192.168.10.2

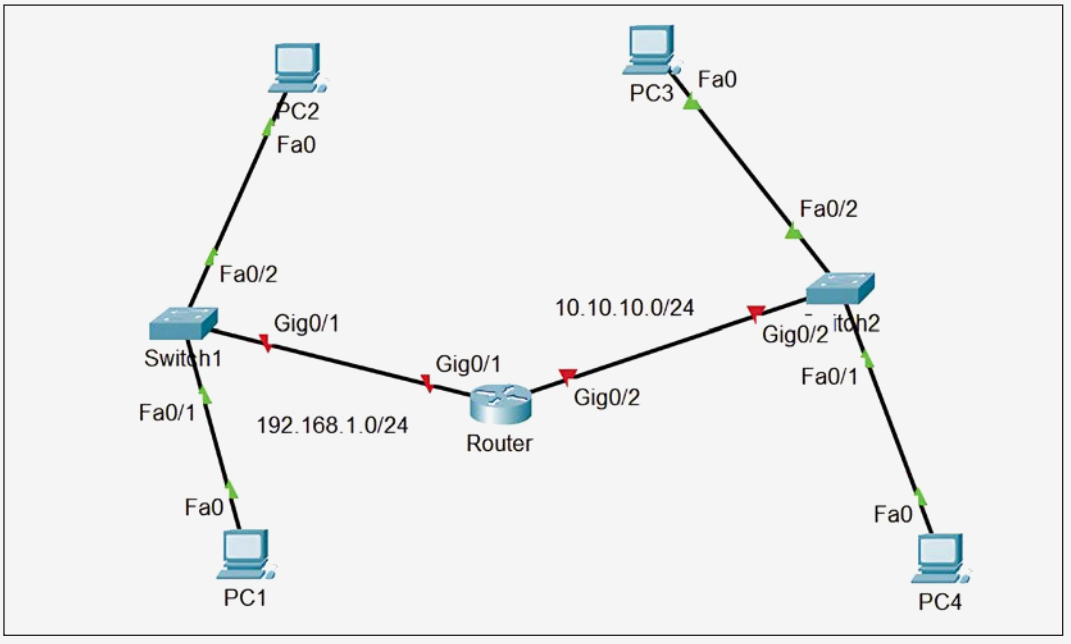
Dizüstü bilgisayarın aldığı IPv4 adresini belirledikten sonra bilgisayardan bu adrese de ping gönderiniz (Görsel 2.65).



Görsel 2.65: DHCP üzerinden adres alan istemciler arasında bağlantı testi

B) Yönlendirici Üzerinden Otomatik IPv4 Adresi Dağıtmak

Amaç: İki farklı yerel ağa bağlı istemcilere yönlendirici üzerindeki DHCP hizmetini kullanarak otomatik IPv4 adresleri dağıtmak (Görsel 2.66)



Görsel 2.66: Yönlendirici üzerinden DHCPv4 dağıtımı topolojisi

Adres Planı

Ağ Bölümü	Ağ Adresi	Yönlendirici Arayüzü	Varsayılan Ağ Geçidi
Sol istemci ağı	192.168.1.0/24	G0/1	192.168.1.1
Sağ istemci ağı	10.10.10.0/24	G0/2	10.10.10.1

Topolojide Kullanılacak Cihazlar

- bir yönlendirici
- iki switch
- dört istemci bilgisayar

PC1 ve PC2 cihazlarını sol switche, PC3 ve PC4 cihazlarını sağ switche bağlayınız. Sol switchi yönlendiricinin G0/1, sağ switchi ise G0/2 arayüzüne bağlayınız.

Uygulama Adımları

1. Adım: Yönlendiricinin Sol Arayüzünü Yapılandırmak

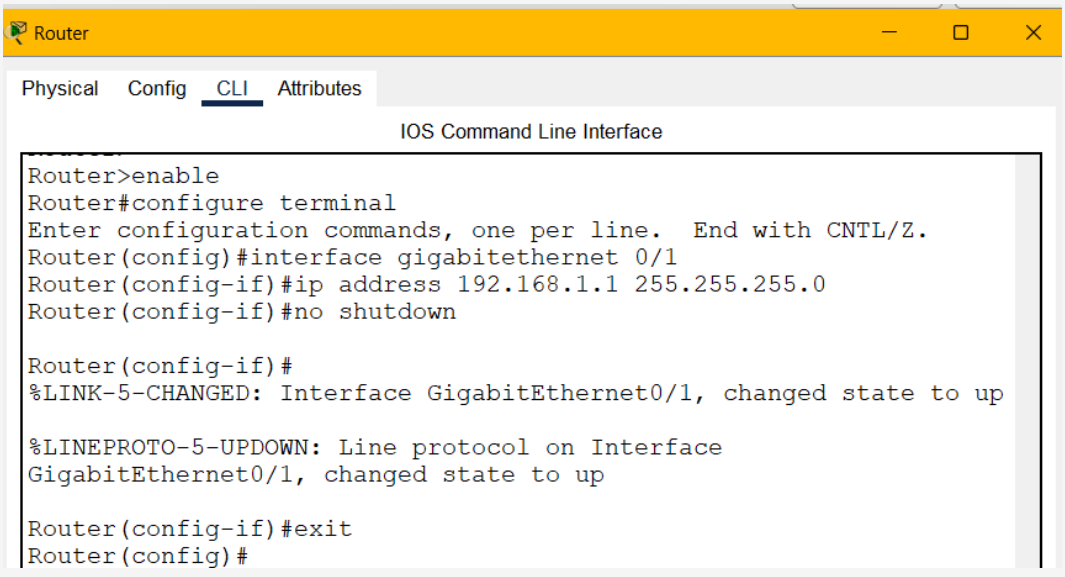
Yönlendiricinin sol arayüzünü şöyle yapılandırınız:

```
Router> enable
Router# configure terminal
Router(config)# interface g0/1
Router(config-if)# ip address 192.168.1.1 255.255.255.0
```

Router(config-if)# no shutdown

Router(config-if)# exit

Yönlendiricinin G0/1 Arayüzünün Yapılandırılması Görsel 2.67'de gösterilmiştir.



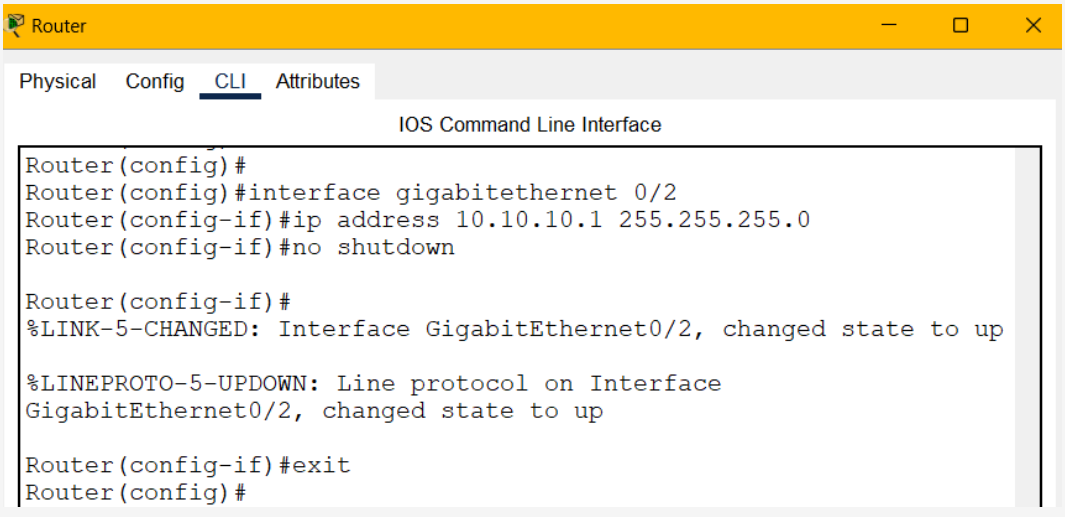
Görsel 2.67: Yönlendiricinin G0/1 arayüzünün yapılandırılması

2. Adım: Yönlendiricinin Sağ Arayüzünü Yapılandırmak

Yönlendiricinin sağ arayüzünü şöyle yapılandırınız:

Router(config)# interface g0/2
Router(config-if)# ip address 10.10.10.1 255.255.255.0
Router(config-if)# no shutdown
Router(config-if)# exit

Yönlendiricinin G0/2 Arayüzünün Yapılandırılması Görsel 2.68'de gösterilmiştir.



Görsel 2.68: Yönlendiricinin G0/2 arayüzünün yapılandırılması

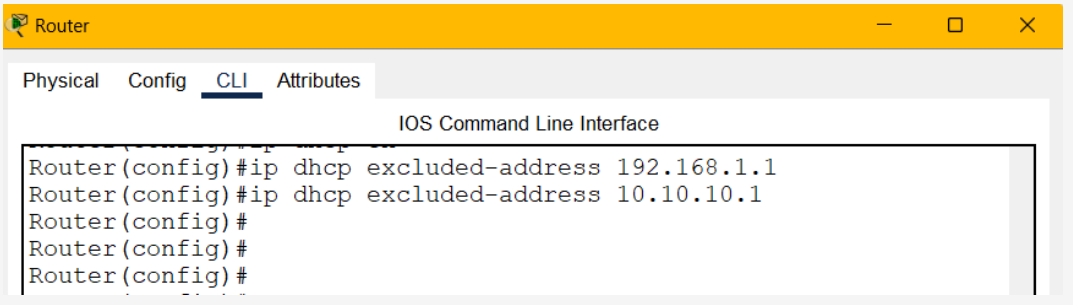
3. Adım: Dağıtılmayacak IPv4 Adreslerini Ayırmak

Yönlendirici arayüzlerinde kullanılan IPv4 adresleri istemcilere dağıtılmamalıdır.

Router(config)# ip dhcp excluded-address 192.168.1.1

Router(config)# ip dhcp excluded-address 10.10.10.1

DHCP dağıtımında kullanılmayacak IPv4 adreslerinin ayrılması Görsel 2.69'da gösterilmiştir.



Görsel 2.69: DHCP dağıtımında kullanılmayacak IPv4 adreslerinin ayrılması

4. Adım: Sol Ağ İçin DHCP Havuzunu Oluşturmak

Sol ağ için DHCP havuzunu şöyle oluşturunuz:

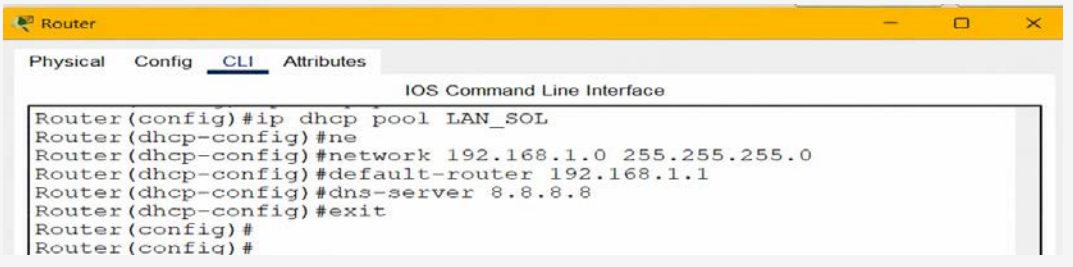
Router(config)# ip dhcp pool LAN_SOL

Router(dhcp-config)# network 192.168.1.0 255.255.255.0

Router(dhcp-config)# default-router 192.168.1.1

Router(dhcp-config)# exit

LAN_SOL DHCP havuzunun oluşturulması Görsel 2.70'te gösterilmiştir.



Görsel 2.70: LAN_SOL DHCP havuzunun oluşturulması

5. Adım: Sağ Ağ İçin DHCP Havuzunu Oluşturmak

Sağ ağ için DHCP havuzunu şöyle oluşturunuz:

Router(config)# ip dhcp pool LAN_SAG

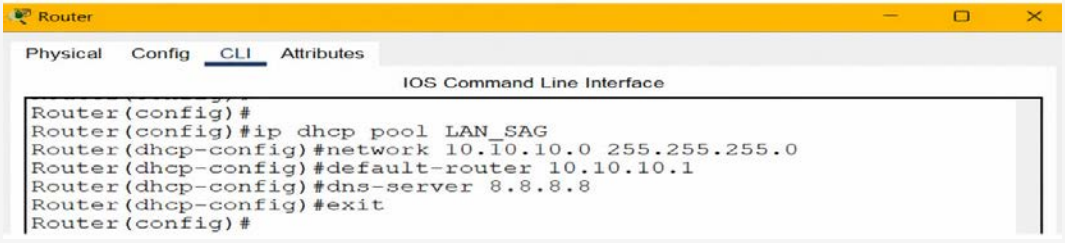
Router(dhcp-config)# network 10.10.10.0 255.255.255.0

Router(dhcp-config)# default-router 10.10.10.1

Router(dhcp-config)# exit

Router(config)# end

LAN_SAG DHCP havuzunun oluşturulması Görsel 2.71'de gösterilmiştir.

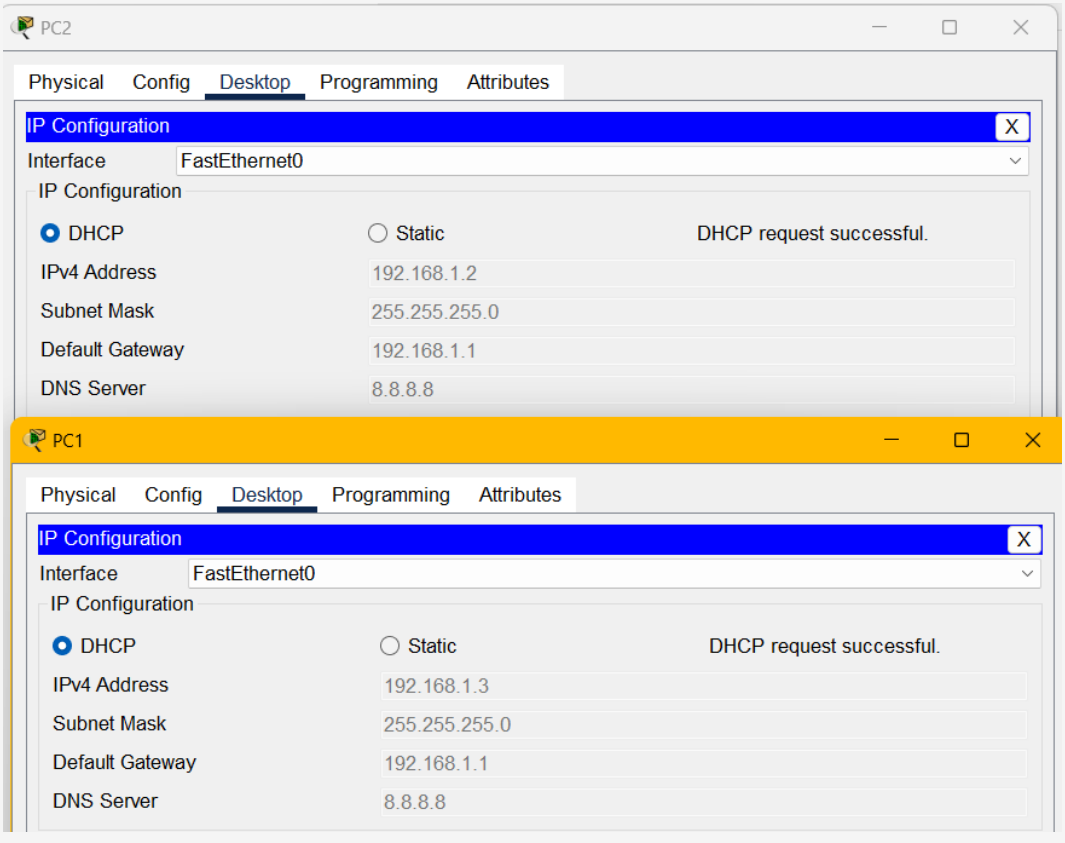


Görsel 2.71: LAN_SAG DHCP havuzunun oluşturulması

6. Adım: Sol Taraftaki İstemcileri Yapılandırmak

PC1 ve PC2 cihazlarında **Desktop > IP Configuration** bölümüne geçiniz. **DHCP** seçeneğini etkinleştiriniz.

Sol ağdaki istemcilerin DHCP üzerinden IPv4 adresi alması Görsel 2.72'de gösterilmiştir.

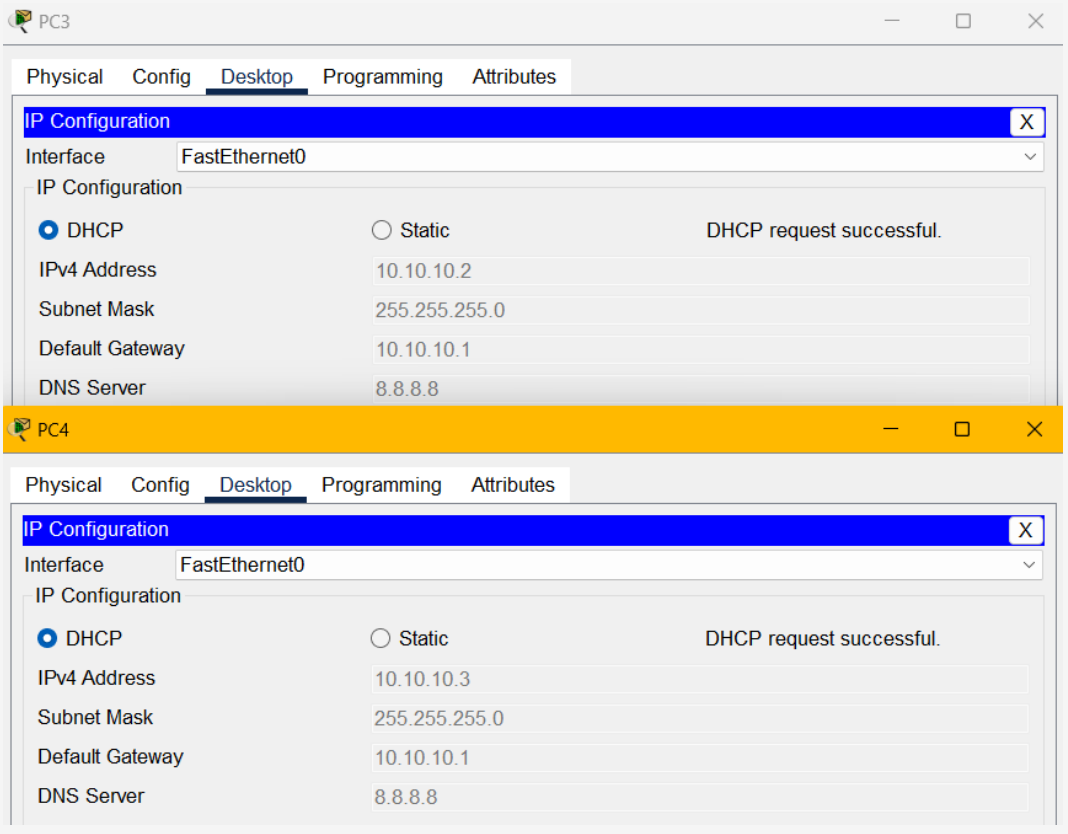


Görsel 2.72: Sol ağdaki istemcilerin DHCP üzerinden IPv4 adresi alması

7. Adım: Sağ Taraftaki İstemcileri Yapılandırmak

PC3 ve PC4 cihazlarında **DHCP** seçeneğini etkinleştiriniz.

Sağ ağdaki istemcilerin DHCP üzerinden IPv4 adresi alması Görsel 2.73'te gösterilmiştir.



Görsel 2.73: Sağ ağdaki istemcilerin DHCP üzerinden IPv4 adresi alması

8. Adım: İstemcilerin Aldığı Adresleri Kontrol Etmek

Her istemcide aşağıdaki komutu çalıştırınız.

ipconfig

Aşağıdaki sonuçları doğrulayınız.

İstemci Grubu	Beklenen IPv4 Ağı	Beklenen Varsayılan Ağ Geçidi
PC1, PC2	192.168.1.0/24	192.168.1.1
PC3, PC4	10.10.10.0/24	10.10.10.1

9. Adım: DHCP Dağıtım Kayıtlarını Görüntülemek

Yönlendiricide aşağıdaki komutu çalıştırınız.

Router# show ip dhcp binding

Bu komut, DHCP üzerinden istemcilere tahsis edilen IPv4 adreslerini incelemeye yardımcı olur.

Gerektiğinde havuzların durumunu görüntülemek için aşağıdaki komut da kullanılabilir.

Router# show ip dhcp pool

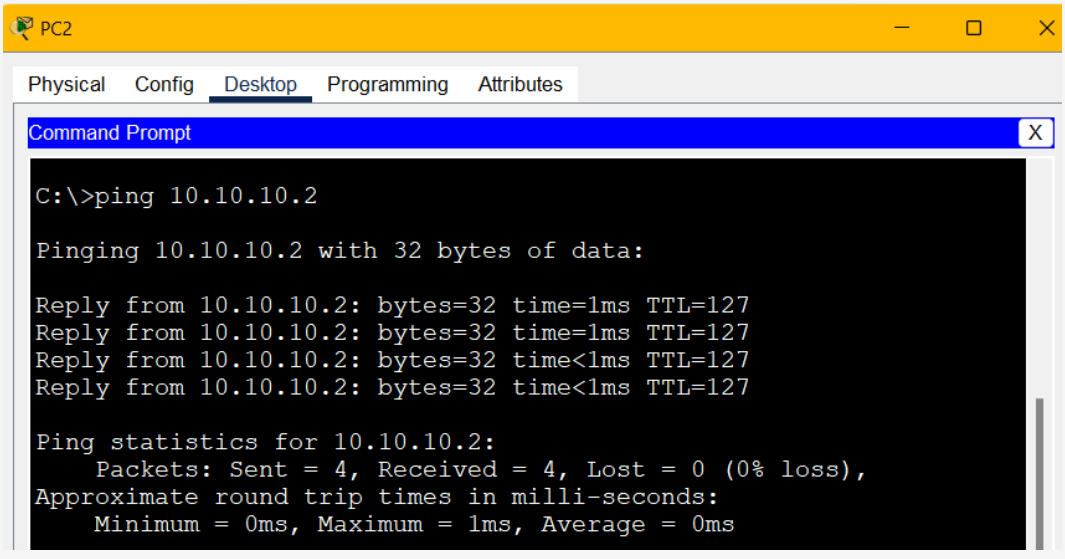
10. Adım: Bağlantı Testlerini Gerçekleştirmek

PC1 cihazından aynı ağdaki PC2 cihazına ve farklı ağdaki PC3 cihazına ping gönderiniz.

ping <PC2'nin aldığı IPv4 adresi>

ping <PC3'ün aldığı IPv4 adresi>

DHCP üzerinden adres alan farklı ağlardaki istemciler arasında bağlantı testi Görsel 2.74'te gösterilmiştir.



Görsel 2.74: DHCP üzerinden adres alan farklı ağlardaki istemciler arasında bağlantı testi

DHCPv4 Sonuçları Gözlem Tablosu

İncelenen Unsur	Temrin 1: DHCP Sunucusu		Temrin 2: Yönlendirici	
DHCP hizmeti etkinleştirildi mi?	☐ Evet	☐ Hayır	☐ Evet	☐ Hayır
İstemciler otomatik IPv4 adresi aldı mı?	☐ Evet	☐ Hayır	☐ Evet	☐ Hayır
İstemciler doğru ağ bloğundan adres aldı mı?	☐ Evet	☐ Hayır	☐ Evet	☐ Hayır
Varsayılan ağ geçidi gerekli miydi?	☐ Evet	☐ Hayır	☐ Evet	☐ Hayır
ping testi başarılı oldu mu?	☐ Evet	☐ Hayır	☐ Evet	☐ Hayır
Karşılaşılan sorun varsa kısa açıklaması				

Değerlendirme

Çalışmanız öğretmeniniz tarafından kontrol listesine göre değerlendirilecektir. Çalışmanızı yaparken buradaki ölçütleri dikkate alınız. Kontrol listesi formuna ulaşmak için karekodu okutunuz. Dijital yayınlarda karekodun üstüne tıklayarak içeriğe ulaşabilirsiniz.

2.3.3. DHCPv6

Dinamik Ana Bilgisayar Yapılandırma Protokolü sürüm 6 [Dynamic Host Configuration Protocol version 6 (DHCPv6)], IPv6 ağlarında istemcilerin adres ve yapılandırma bilgilerinin otomatik olarak belirlenmesine yardımcı olan yapıdır. IPv4 ağlarında yaygın olarak kullanılan DHCPv4 yaklaşımından farklı olarak IPv6 otomatik yapılandırmasında yalnızca tek bir yöntem bulunmaz. IPv6 ağlarında yönlendirici ilanları [Router Advertisement (RA)] önemli bir işleve sahiptir. İstemciler, yönlendiricinin gönderdiği RA mesajlarından yararlanarak ağ ön eki ve ağ geçidiyle ilişkili bilgileri öğrenebilir. Kullanılacak yapılandırma modeline göre istemcinin IPv6 adresi kendisi tarafından oluşturulabilir veya DHCPv6 sunucusu tarafından sağlanabilir.

IPv6 otomatik yapılandırma modları Tablo 2.18'de verilmiştir.

Tablo 2.18: IPv6 Otomatik Yapılandırma Modları

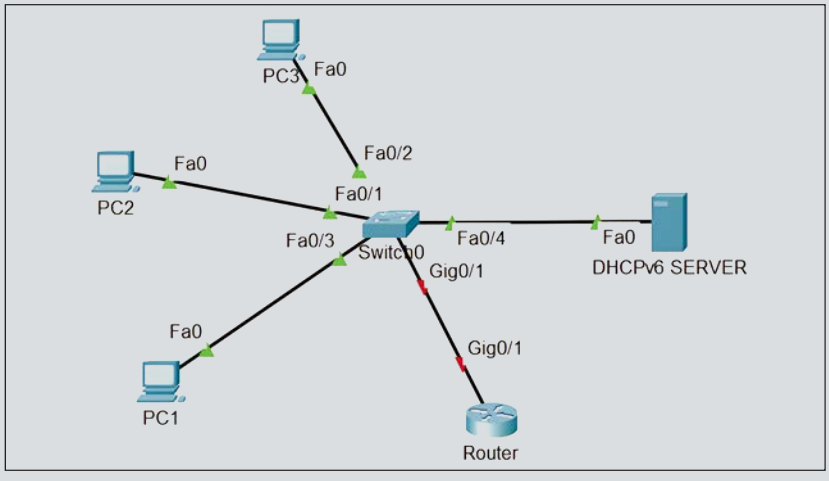
Yapılandırma Modeli	IPv6 Adresi Nasıl Belirlenir?	Tamamlayıcı Bilgiler Nasıl Alınır?	Varsayılan Ağ Geçidi Nasıl Öğrenilir?
Durumsuz Otomatik Yapılandırma — SLAAC	İstemci, RA mesajıyla aldığı ağ ön ekinden yararlanarak kendi IPv6 adresini oluşturur.	DHCPv6 sunucusu zorunlu değildir.	RA mesajları üzerinden öğrenilir.
Durumsuz Otomatik Yapılandırma + DHCPv6	İstemci, IPv6 adresini SLAAC yöntemiyle kendisi oluşturur.	DNS sunucusu gibi ek bilgiler DHCPv6 üzerinden alınabilir.	RA mesajları üzerinden öğrenilir.
Durumlu DHCPv6	İstemci, IPv6 adresini DHCPv6 sunucusundan alır.	Adres ve belirli ek yapılandırma bilgileri DHCPv6 sunucusu tarafından sağlanır.	RA mesajları üzerinden öğrenilir.

BİLGİ KUTUSU : IPv6 Adres Çakışması Nasıl Önlenir?

Bir IPv6 adresi bir ağ arayüzüne tanımlandığında cihaz bu adresi hemen kullanmaya başlamaz. Öncelikle adresin aynı yerel ağda başka bir cihaz tarafından kullanılıp kullanılmadığını denetler. Bu işlem Yinelenen Adres Algılama [Duplicate Address Detection (DAD)] olarak adlandırılır. Cihaz, kullanmak istediği IPv6 adresiyle ilgili bir Komşu İsteği (Neighbor Solicitation) mesajı gönderir. Ağda aynı adresi kullanan başka bir cihaz varsa bu cihaz Komşu İlanı (Neighbor Advertisement) mesajıyla karşılık verir ve adresin çakıştığı anlaşılır. Herhangi bir yanıt alınmazsa IPv6 adresi yerel bağlantıda benzersiz kabul edilerek kullanılmaya başlanır. DAD işlemi, adresin SLAAC, DHCPv6 veya elle yapılandırma yoluyla edinilmesinden bağımsız olarak adres çakışmalarının önlenmesine yardımcı olur.

10. UYGULAMA

Uygulama Adı	Durumlu DHCPv6 ile Otomatik IPv6 Adresi Almak
Süre	30 dakika
Amaç	İstemci cihazların durumlu DHCPv6 modeliyle otomatik IPv6 adresi almasını sağlamak, RA mesajlarının ve DHCPv6 sunucusunun yapılandırma sürecindeki rollerini ayırt etmek (Görsel 2.75)
Araç Gereç	Ağ simülasyon programı, bir yönlendirici, bir switch, bir DHCPv6 sunucusu, üç istemci bilgisayar, çalışma yaprağı .



Görsel 2.75: Durumlu DHCPv6 uygulaması topolojisi

Dikkat Edilecek Noktalar

- Yönlendiricinin IPv6 yönlendirme özelliğini etkinleştiriniz.
- Yönlendirici arayüzünü doğru IPv6 adresiyle yapılandırınız.
- DHCPv6 sunucusuna sabit IPv6 adresi veriniz.
- DHCPv6 havuzunda kullanılacak ön eki doğru tanımlayınız.
- Yönlendirici arayüzünde yönetilen yapılandırma bayrağını etkinleştiriniz.
- İstemcilerde otomatik IPv6 yapılandırma seçeneğini kullanınız.
- İstemcilerin aldığı IPv6 adreslerini kaydediniz.
- ping komutuyla temel IPv6 iletişimini sınayınız.
- Grup içinde görev paylaşımı yapınız.

Cihaz veya Arayüz	IPv6 Adresi	Ön Ek Uzunluğu	Yapılandırma Türü
Yönlendirici G0/1	2001:db8:1::1	/64	Statik
DHCPv6 sunucusu	2001:db8:1::10	/64	Statik
PC1	DHCPv6 üzerinden alınacak	/64	Otomatik
PC2	DHCPv6 üzerinden alınacak	/64	Otomatik
PC3	DHCPv6 üzerinden alınacak	/64	Otomatik

DHCPv6 Havuzu

Alan	Tanımlanacak Değer
Havuz adı	IPV6_HAVUZU
IPv6 ön eki	2001:db8:1::/64
DNS sunucusu	Simülasyon ekranında kullanılan örnek değer korunabilir.
Varsayılan ağ geçidi	DHCPv6 havuzundan dağıtılmaz, istemciler tarafından RA üzerinden öğrenilir.

Uygulama Adımları

1. Adım: Topolojiyi Oluşturmak

Ağ simülasyon programında aşağıdaki cihazları çalışma alanına ekleyiniz.

- bir yönlendirici
- bir switch
- bir DHCPv6 sunucusu
- PC1, PC2 ve PC3

2. Adım: Yönlendiricide IPv6 Yönlendirmeyi Etkinleştirmek

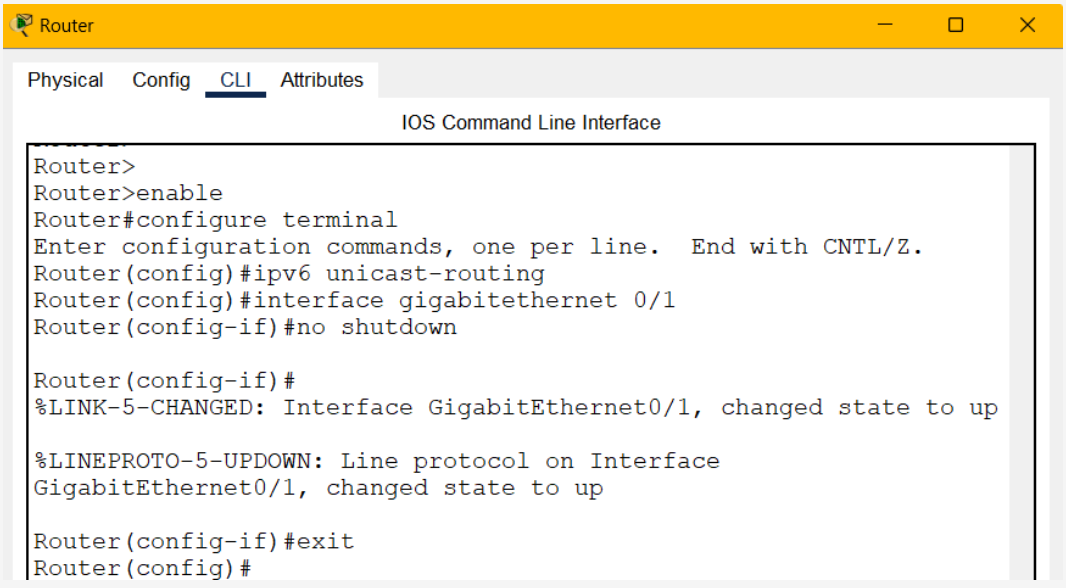
Yönlendiricinin komut satırı arayüzünü açınız. Aşağıdaki komutları uygulayınız.

```
Router> enable
Router# configure terminal
Router(config)# ipv6 unicast-routing
```

Ardından G0/1 arayüzüne geçiniz ve arayüzü etkinleştiriniz.

```
Router(config)# interface gigabitethernet 0/1
Router(config-if)# no shutdown
```

Yönlendiricinin G0/1 arayüzünün etkinleştirilmesi Görsel 2.76'da gösterilmiştir.

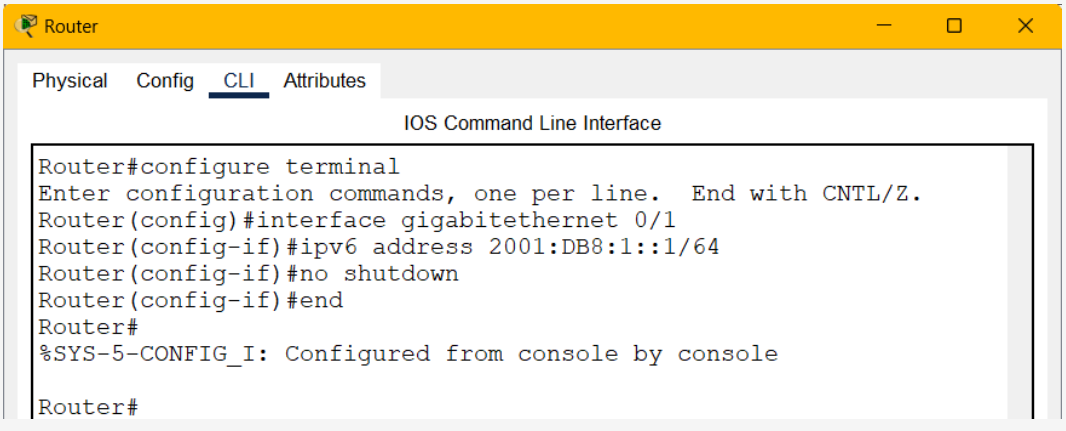


Görsel 2.76: Yönlendiricinin G0/1 arayüzünün etkinleştirilmesi

3. Adım: Yönlendirici Arayüzüne IPv6 Adresi Vermek

Router(config-if)# ipv6 address 2001:db8:1::1/64

Yönlendirici arayüzüne sabit IPv6 adresi verilmesi Görsel 2.77'de gösterilmiştir.



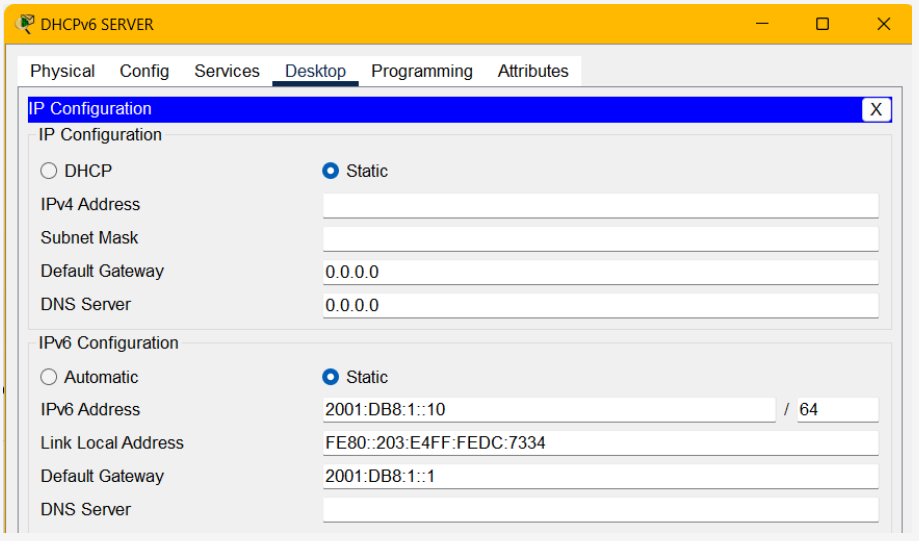
Görsel 2.77: Yönlendirici arayüzüne sabit IPv6 adresi verilmesi

BİLGİ KUTUSU

IPv6 ağlarında yönlendirici arayüzüne verilen adres, yalnızca yönlendiricinin tanımlanması için kullanılmaz. Bu adres aynı zamanda ilgili ağ bölümündeki cihazların başka ağlara erişirken kullanacağı çıkış noktasıdır. Bu nedenle yönlendirici arayüz adresi, sunucu ve istemcilerin bulunduğu IPv6 ön ekiyle uyumlu olmalıdır. Örneğin 2001:db8:1::/64 ağı içinde yapılandırılan 2001:db8:1::1/64 adresi, bu yerel IPv6 ağının yönlendirici arayüzünü temsil eder. Sonraki adımlarda DHCPv6 sunucusuna aynı ağ ön eki içinde sabit adres verilmesi ve istemcilerin otomatik IPv6 adresi alması bu yapı üzerine kuruludur.

4. Adım: DHCPv6 Sunucusuna Sabit IPv6 Adresi Vermek

DHCPv6 sunucusunu açınız. **Desktop > IP Configuration** bölümüne geçiniz. IPv6 yapılandırma alanında **Static** seçeneğini etkinleştiriniz (Görsel 2.78).



Görsel 2.78: DHCPv6 sunucusuna sabit IPv6 adresi verilmesi

Aşağıdaki bilgileri giriniz.

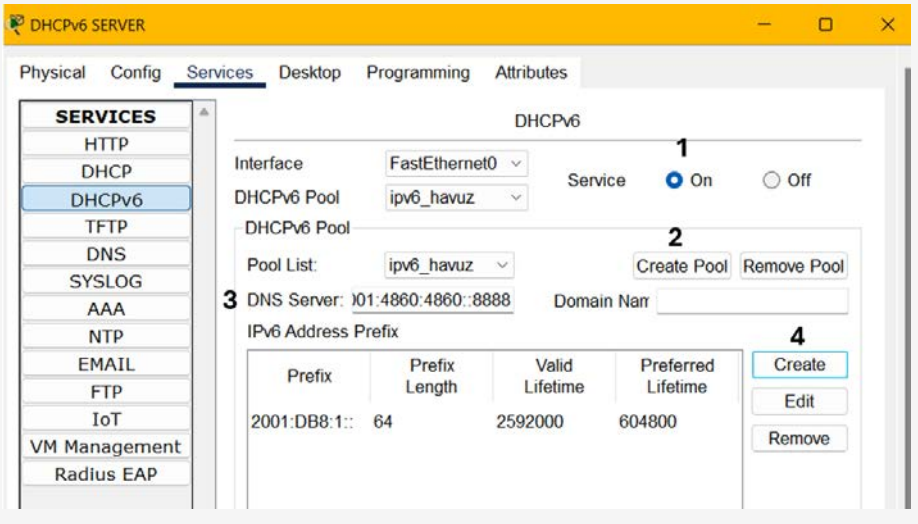
IPv6 Address: 2001:db8:1::10 **Prefix Length:** 64 **Default Gateway:** 2001:db8:1::1

5. Adım: DHCPv6 Havuzunu Oluşturmak

Sunucuda **Services > DHCPv6** bölümüne geçiniz. DHCPv6 hizmetini etkinleştiriniz (Görsel 2.79).

Aşağıdaki değerleri kullanarak yeni havuz oluşturunuz.

Pool Name: IPV6_HAVUZU **IPv6 Prefix:** 2001:db8:1:: **Prefix Length:** 64



Görsel 2.79: DHCPv6 sunucusunda IPv6 havuzunun oluşturulması

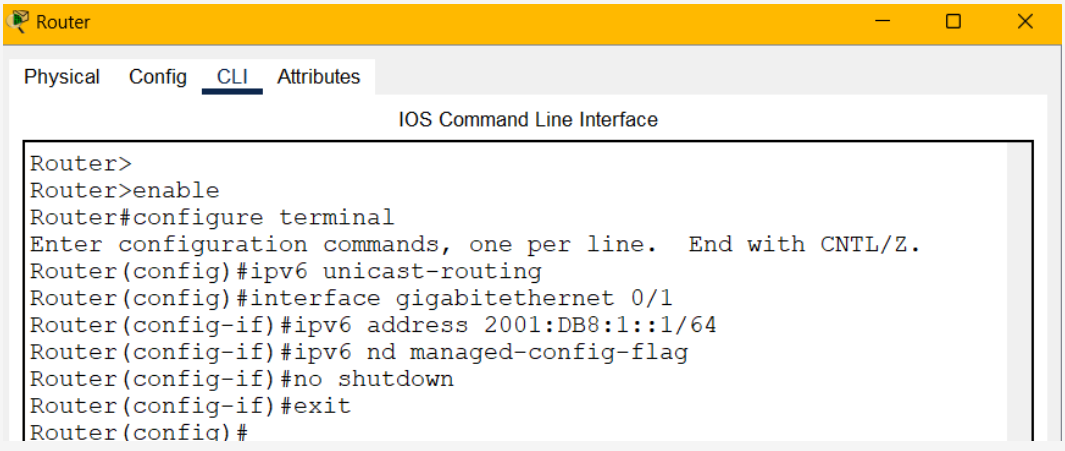
6. Adım: RA Üzerinde Yönetilen Yapılandırma Bayrağını Etkinleştirmek

Yönlendirici arayüzünde aşağıdaki komutu çalıştırınız (Görsel 2.80).

Router(config-if)# ipv6 nd managed-config-flag

Ardından yapılandırmadan çıkınız.

Router(config-if)# end

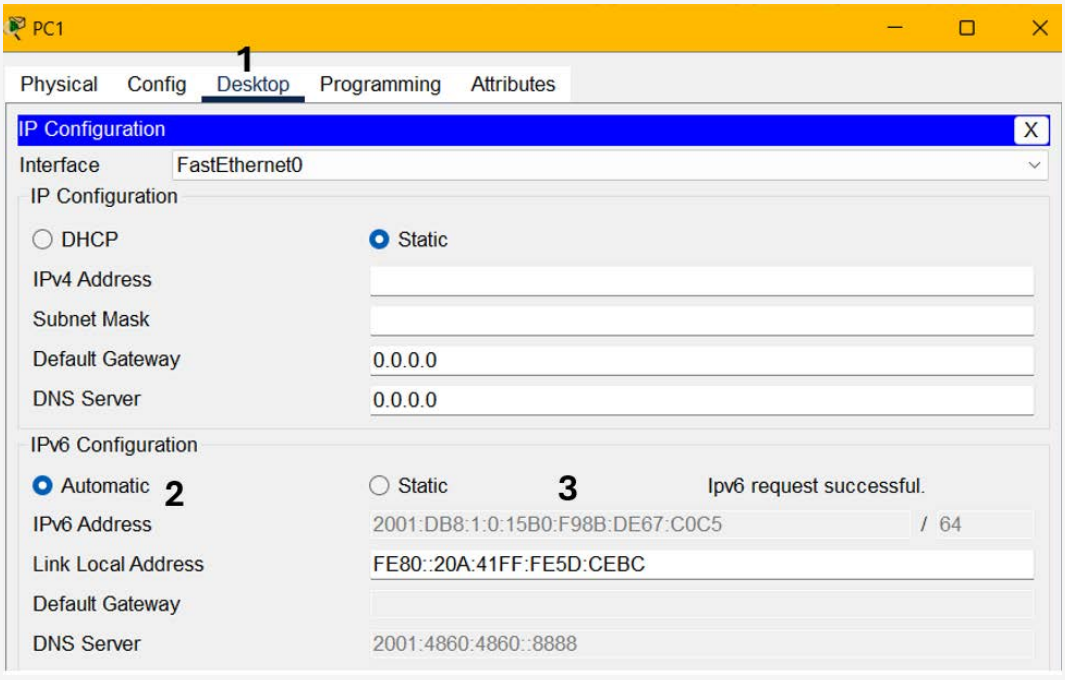


Görsel 2.80: Yönlendiricide RA yönetilen yapılandırma bayrağının etkinleştirilmesi

7. Adım: İstemcilerde Otomatik IPv6 Yapılandırmasını Etkinleştirmek

PC1, PC2 ve PC3 cihazlarını sırayla açınız. **Desktop > IP Configuration** bölümüne geçiniz. IPv6 yapılandırma alanında **Automatic** seçeneğini etkinleştiriniz (Görsel 2.81).

İstemcilerin 2001:db8:1::/64 ön ekine sahip IPv6 adresleri aldığını doğrulayınız.



Görsel 2.81: İstemcilerin DHCPv6 üzerinden otomatik IPv6 adresi alması

8. Adım: İstemcilerin Aldığı Adresleri Kaydetmek

İstemcilerin IPv6 yapılandırma ekranlarını inceleyiniz. Aşağıdaki tabloyu doldurunuz.

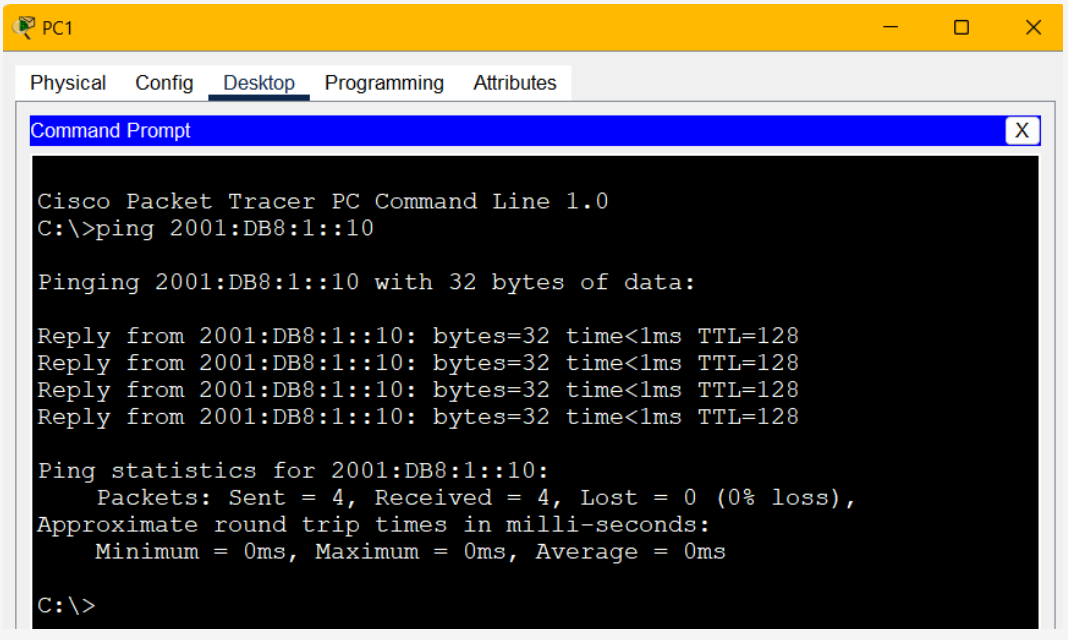
İstemci	Otomatik Alınan IPv6 Adresi	Ön Ek Uzunluğu	Link-Local Adresi	DNS Sunucusu
PC1				
PC2				
PC3				

9. Adım: IPv6 Bağlantısını Sınamak

PC1 cihazında **Desktop > Command Prompt** bölümünü açınız. DHCPv6 sunucusuna erişimi sınayınız.

ping 2001:db8:1::10

IPv6 bağlantısının ping komutuyla sınanması Görsel 2.82'de gösterilmiştir.



Görsel 2.82: IPv6 bağlantısının ping komutuyla sınanması

DHCPv4 ve DHCPv6 Otomatik Yapılandırma Gözlem Tablosu

İncelenen Unsur	1.DHCP Sunucusu Üzerinden IPv4	2.Yönlendirici Üzerinden IPv4	3.Durumlu DHCPv6
Otomatik yapılandırma hizmeti etkinleştirildi mi?	☐ Evet ☐ Hayır	☐ Evet ☐ Hayır	☐ Evet ☐ Hayır
İstemciler doğru ağ bloğundan adres aldı mı?	☐ Evet ☐ Hayır	☐ Evet ☐ Hayır	☐ Evet ☐ Hayır
Dağıtılan adres türü	IPv4	IPv4	IPv6

Kullanılan ağ veya ön ek			
Varsayılan ağ geçidi gerekli miydi?			
Varsayılan ağ geçidi hangi yöntemle öğrenildi?			
DNS sunucusu bilgisi tanımlandı mı?			
İstemciler arasında veya sunucuya ping testi başarılı oldu mu?	☐ Evet ☐ Hayır	☐ Evet ☐ Hayır	☐ Evet ☐ Hayır
Karşılaşılan sorun varsa kısa açıklaması			
Sorunu gidermek için yapılan işlem			

Sonuçları Yorumlamak

Aşağıdaki soruları cevaplayınız.

1. DHCPv4 ve durumlu DHCPv6 yaklaşımlarının ortak yönü nedir?

.....
.....

2. IPv6 istemcileri varsayılan ağ geçidi bilgisini hangi yöntemle öğrenir?

.....
.....

3. SLAAC ile durumlu DHCPv6 arasındaki temel fark nedir?

.....
.....

4. Temrin 1'de varsayılan ağ geçidi zorunlu değilken Temrin 2'de neden gereklidir?

.....
.....

5. Temrin 3'te yönlendiricinin RA mesajları hangi açıdan önemlidir?

.....
.....

Değerlendirme

Çalışmanız öğretmeniniz tarafından kontrol listesine göre değerlendirilecektir. Çalışmanızı yaparken buradaki ölçütleri dikkate alınız. Kontrol listesi formuna ulaşmak için karekodu okutunuz. Dijital yayınlarda karekodun üstüne tıklayarak içeriğe ulaşabilirsiniz.

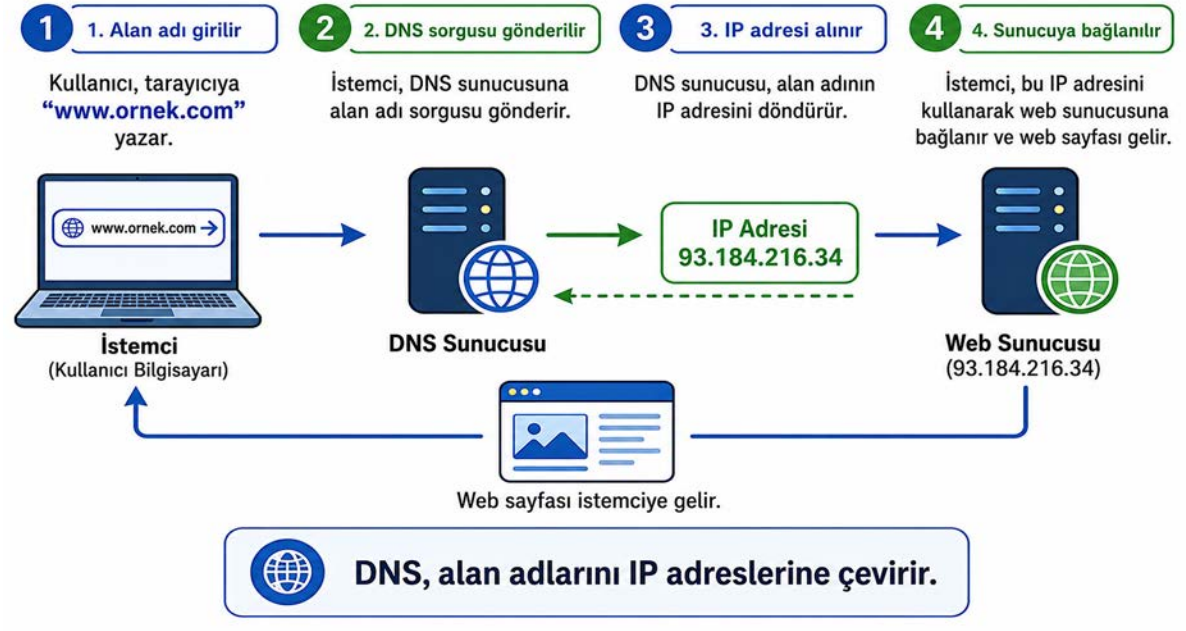
2.3.4. DNS Protokolü

Alan Adı Sistemi [Domain Name System (DNS)], alan adlarıyla ağ kaynaklarına ait bilgilerin eşleştirilmesini sağlayan isim çözümleme sistemidir. Kullanıcılar web sitelerini ve ağ hizmetlerini çoğunlukla sayısal IP adresleriyle değil anlamlı alan adlarıyla hatırlar. Ağ iletişiminin gerçekleştirilebilmesi için ise hedef cihazın IP adresinin bilinmesi gerekir. Bir kullanıcı tarayıcıya alan adı yazdığında sistem, bu adla ilişkili kayıtları sorgular. İlgili adres kaydı bulunduğunda alan adı, hedef sunucunun IP adresiyle eşleştirilir. Böylece kullanıcılar karmaşık sayısal adresleri ezberlemek zorunda kalmadan ağ hizmetlerine erişebilir.

DNS yalnızca web sayfalarına erişimde kullanılmaz. E-posta sunucuları, dosya aktarım sunucuları ve farklı ağ hizmetleri de alan adlarıyla ilişkilendirilebilir. Örneğin aşağıdaki alan adları farklı hizmetleri gösterebilir.

Alan Adı	İlişkili Hizmet
www.siber.test	Web sunucusu
ftp.okul.test	FTP sunucusu

DNS sistemi hiyerarşik bir yapıya sahiptir. İstemcinin ilk başvurduğu yapı çoğunlukla DNS çözümleyicisidir. Çözümleyici gerekli kaydı kendi verilerinde bulamazsa ilgili DNS yapılarına sorgu gönderir (Görsel 2.83).

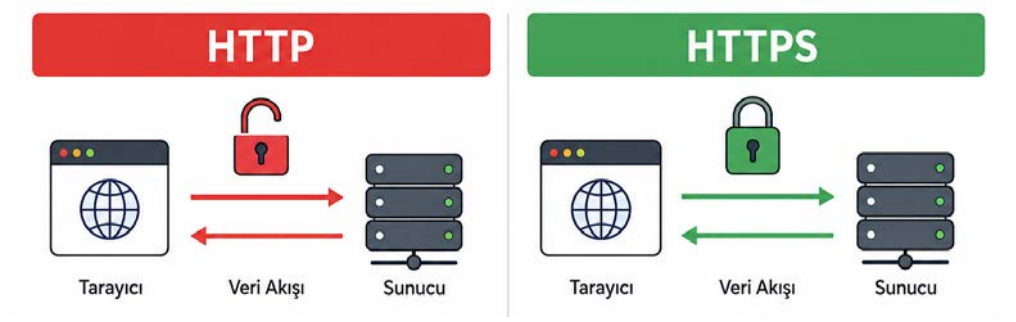


Görsel 2.83: DNS çözümleme sürecinin temel mantığı

2.3.5. HTTP ve HTTPS Protokolleri

Hiper Metin Aktarım Protokolü [Hypertext Transfer Protocol (HTTP)], web içeriklerinin istemci ile sunucu arasında iletilmesini sağlayan uygulama katmanı protokolüdür. Bir kullanıcı tarayıcı üzerinden bir web sayfasına erişmek istediğinde istemci, sunucuya istek gönderir. Sunucu ise isteği değerlendirerek uygun yanıtı iletir. HTML belgeleri, görseller ve diğer web içerikleri bu iletişim sürecinde taşınabilir. HTTPS, HTTP iletişiminin TLS ile korunduğu yapıdır. Bu kullanımda istemci ile sunucu arasındaki veri iletimi şifrelenir. Böylece üçüncü tarafların iletişimi kolayca okuyabilmesi veya değiştirebilmesi zorlaştırılır. Özellikle kullanıcı girişi, kişisel veri aktarımı ve hassas işlemlerin yürütüldüğü web hizmetlerinde HTTPS kullanımı önemlidir.

HTTP ile HTTPS aynı temel web erişimi mantığına dayanır. İki yapı arasındaki temel fark, bağlantının korunma biçimidir (Görsel 2.84).



Görsel 2.84: HTTP ve HTTPS bağlantılarının karşılaştırılması

HTTP ve HTTPS bağlantılarının karşılaştırılması Tablo 2.19'da verilmiştir.

Tablo 2.19: HTTP ve HTTPS Bağlantılarının Karşılaştırılması

Özellik	HTTP	HTTPS
Açılımı	Hypertext Transfer Protocol	Hypertext Transfer Protocol Secure
Temel işlevi	Web içeriğini istemci ile sunucu arasında taşır.	Web içeriğini istemci ile sunucu arasında TLS korumasıyla taşır.
Bağlantı güvenliği	İletişim varsayılan olarak şifrelenmez.	İletişim TLS ile korunur.
Yaygın varsayılan port	80	443
Adres çubuğundaki yaygın gösterim	http://	https://
Kullanım yaklaşımı	Güvenlik gereksiniminin sınırlı olduğu temel web erişimleri	Hassas veri içeren veya güvenli bağlantı gerektiren web erişimleri

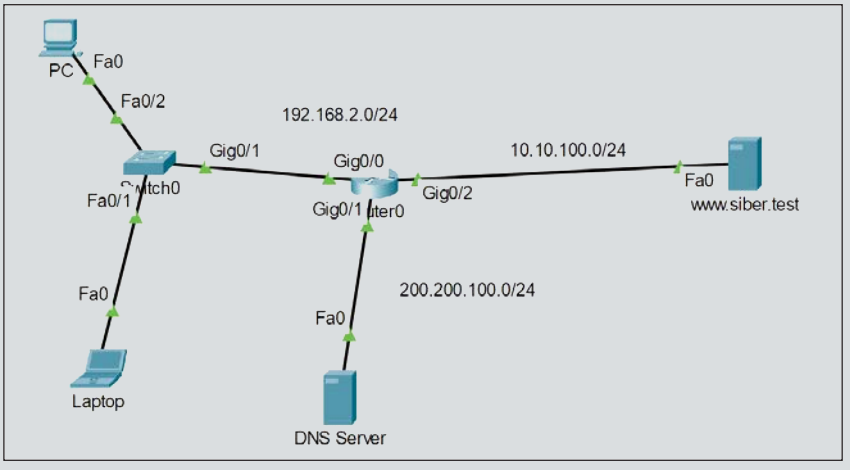
Dikkat: Adres çubuğunda https:// ifadesinin bulunması, istemci ile sunucu arasındaki bağlantının TLS ile korunduğunu gösterir. Bu durum, web sitesindeki bütün bilgilerin kesinlikle doğru veya güvenilir olduğunu tek başına kanıtlamaz.

BİLGİ KUTUSU

Bir web adresi incelenirken bağlantı yöntemi, alan adı ve sayfa yolu birlikte değerlendirilir. Örneğin https://www.meb.gov.tr/duyurular adresinde https:// bağlantı yöntemini, www.meb.gov.tr alan adını, /duyurular ise sunucu üzerindeki ilgili sayfa yolunu gösterir. HTTP veya HTTPS bilgisi, istemci ile sunucu arasındaki web bağlantısının nasıl kurulduğunu anlamaya yardımcı olur. Alan adı ise kullanıcının hangi sunucuya eriştiğini gösterir. Bu nedenle web adresleri okunurken yalnızca bağlantı başlangıcına değil, alan adının doğru yazılıp yazılmadığına da dikkat edilmelidir.

11. UYGULAMA

Uygulama Adı	DNS Çözümleme ve HTTP Web Erişimini Gerçekleştirmek
Süre	35 dakika
Amaç	DNS sunucusunda alan adı–IPv4 adresi eşleştirmesi oluşturarak istemcilerin web sunucusuna alan adı üzerinden erişmesini sağlamak ve HTTP web erişimini sınamak (Görsel 2.85)
Araç Gereç	Ağ simülasyon programı, bir yönlendirici, bir switch, bir DNS sunucusu, bir web sunucusu, bir bilgisayar, bir dizüstü bilgisayar, çalışma yaprağı.



Görsel 2.85: DNS çözümleme ve HTTP web erişimi topolojisi

Dikkat Edilecek Noktalar

- Yönlendirici arayüzlerine doğru IPv4 adreslerini veriniz.
- DNS ve web sunucularını ilgili ağlarda statik olarak yapılandırınız.
- İstemcilere doğru varsayılan ağ geçidi ve DNS sunucusu bilgilerini giriniz.
- DNS sunucusunda www.siber.test alan adını web sunucusunun IPv4 adresiyle eşleştiriniz.
- Önce IP adresleriyle temel bağlantıyı, ardından alan adıyla DNS çözümlemesini sınayınız.
- Son olarak web tarayıcısı üzerinden HTTP erişimini doğrulayınız.
- Grup içinde görev paylaşımı yapınız.

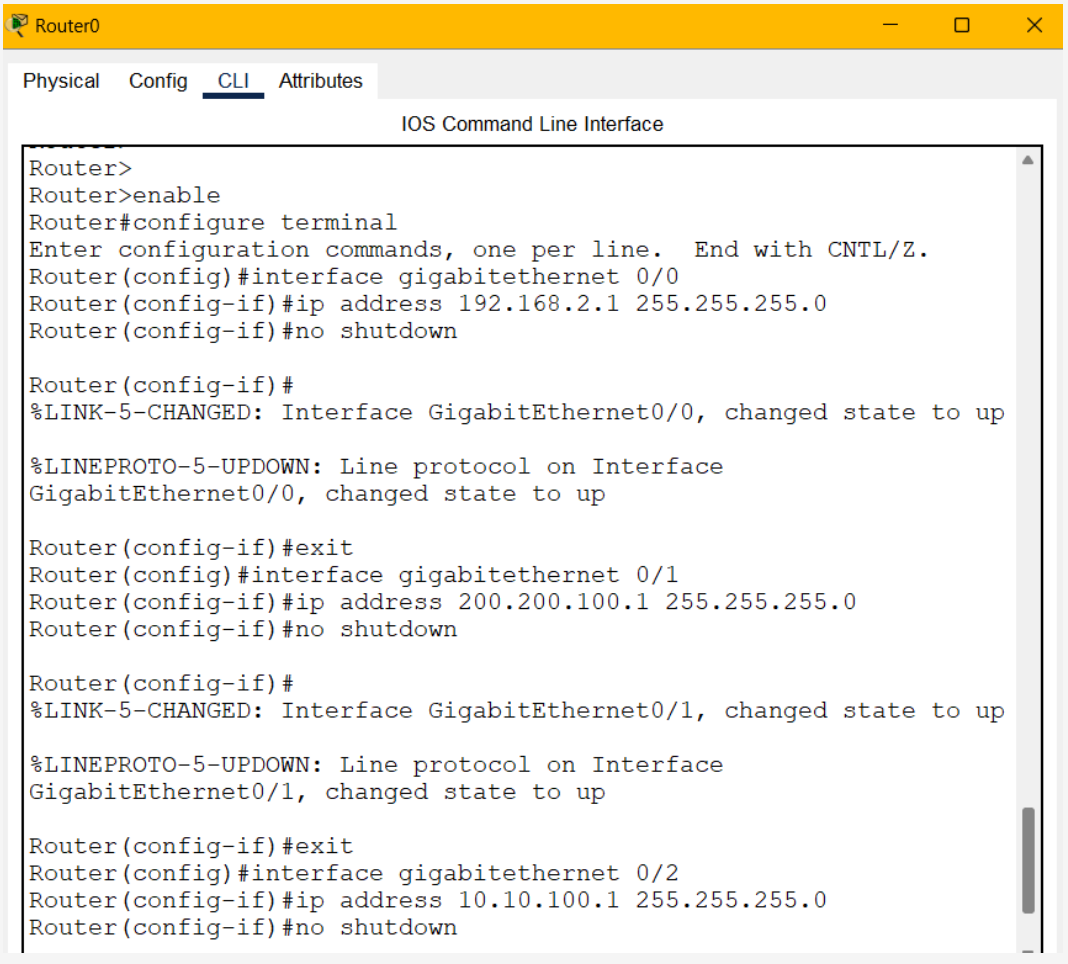
Cihaz veya Arayüz	IPv4 Adresi	Alt Ağ Maskesi	Varsayılan Ağ Geçidi	DNS Sunucusu
Yönlendirici G0/0	192.168.2.1	255.255.255.0	–	–
Yönlendirici G0/1	200.200.100.1	255.255.255.0	–	–
Yönlendirici G0/2	10.10.100.1	255.255.255.0	–	–
DNS sunucusu	200.200.100.2	255.255.255.0	200.200.100.1	–
Web sunucusu	10.10.100.2	255.255.255.0	10.10.100.1	–
Bilgisayar	192.168.2.10	255.255.255.0	192.168.2.1	200.200.100.2
Dizüstü bilgisayar	192.168.2.20	255.255.255.0	192.168.2.1	200.200.100.2

1. Adım: Yönlendirici Arayüzlerini Yapılandırmak

Yönlendirici arayüzlerini şöyle yapılandırınız:

```
Router> enable
Router# configure terminal
Router(config)# interface g0/0
Router(config-if)# ip address 192.168.2.1 255.255.255.0
Router(config-if)# no shutdown
Router(config-if)# exit
Router(config)# interface g0/1
Router(config-if)# ip address 200.200.100.1 255.255.255.0
Router(config-if)# no shutdown
Router(config-if)# exit
Router(config)# interface g0/2
Router(config-if)# ip address 10.10.100.1 255.255.255.0
Router(config-if)# no shutdown
Router(config-if)# end
```

Yönlendirici arayüzlerinin IPv4 yapılandırma işlemleri Görsel 2.86'da gösterilmiştir.



Görsel 2.86: Yönlendirici arayüzlerinin IPv4 yapılandırması

2. Adım: DNS Sunucusunu Yapılandırmak

DNS sunucusunda **Desktop > IP Configuration** bölümünü açınız. Aşağıdaki bilgileri giriniz.

IPv4 Address: 200.200.100.2

Subnet Mask: 255.255.255.0

Default Gateway: 200.200.100.1

3. Adım: Web Sunucusunu Yapılandırmak

Web sunucusunda **Desktop > IP Configuration** bölümünü açınız. Aşağıdaki bilgileri giriniz.

IPv4 Address: 10.10.100.2

Subnet Mask: 255.255.255.0

Default Gateway: 10.10.100.1

4. Adım: İstemcileri Yapılandırmak

Bilgisayar için aşağıdaki bilgileri giriniz.

IPv4 Address: 192.168.2.10

Subnet Mask: 255.255.255.0

Default Gateway: 192.168.2.1

DNS Server: 200.200.100.2

Dizüstü bilgisayar için aşağıdaki bilgileri giriniz.

IPv4 Address: 192.168.2.20

Subnet Mask: 255.255.255.0

Default Gateway: 192.168.2.1

DNS Server: 200.200.100.2

5. Adım: DNS Kaydını Oluşturmak

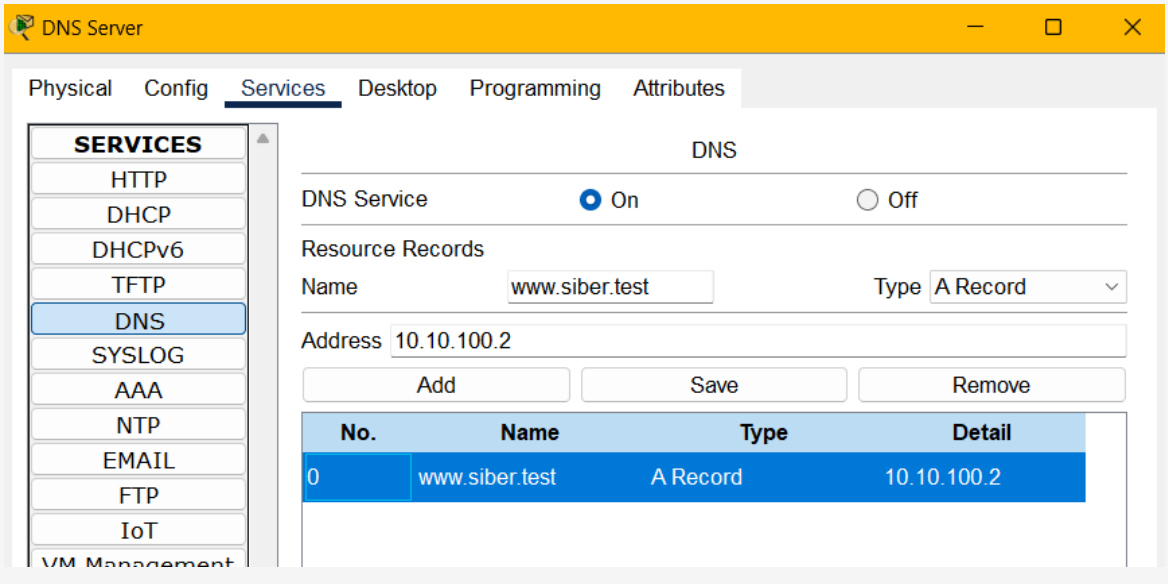
DNS sunucusunda **Services > DNS** bölümünü açınız. DNS hizmetini etkinleştiriniz (Görsel 2.87).

Aşağıdaki kaydı ekleyiniz.

Name: www.siber.test

Type: A

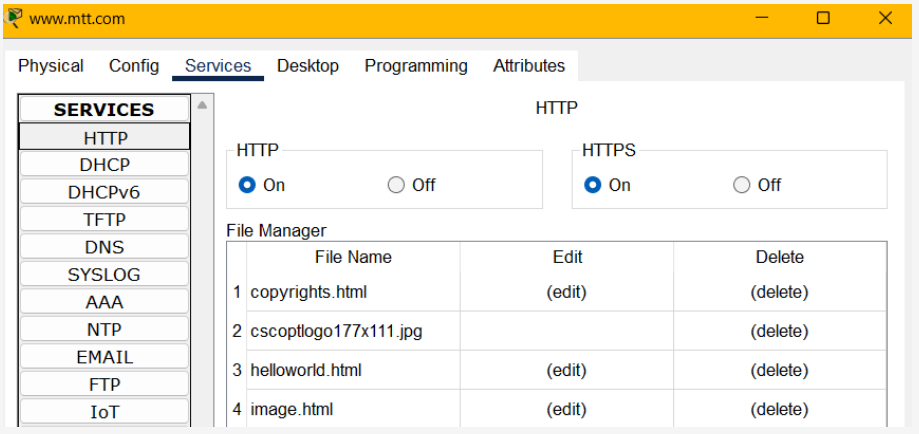
Address: 10.10.100.2



Görsel 2.87: DNS sunucusunda www.siber.test A kaydının oluşturulması

6. Adım: HTTP Hizmetini Etkinleştirmek

Web sunucusunda **Services > HTTP** bölümünü açınız. HTTP hizmetini etkinleştiriniz (Görsel 2.88).
Ana sayfa içeriğine aşağıdaki metni yazabilirsiniz.
www.siber.test web sunucusuna hoş geldiniz.



Görsel 2.88: Web sunucusunda HTTP hizmetinin etkinleştirilmesi

7. Adım: IP Düzeyindeki Bağlantıyı Sınamak

Bilgisayarın komut satırını açınız. Öncelikle DNS sunucusuna erişimi sınayınız.
ping 200.200.100.2
Ardından web sunucusuna erişimi sınayınız.
ping 10.10.100.2

8. Adım: DNS Çözümlemesini Sınamak

Aşağıdaki komutu çalıştırınız.
ping www.siber.test
Komut çıktısında www.siber.test alan adının 10.10.100.2 IPv4 adresiyle ilişkilendirildiğini gözlemleyiniz.

9. Adım: HTTP Web Erişimini Sınamak

Bilgisayarda **Desktop > Web Browser** bölümünü açınız. Adres çubuğuna aşağıdaki adresi yazınız.
www.siber.test
Web sayfasının açıldığını doğrulayınız (Görsel 2.89).



Görsel 2.89: www.siber.test alan adı kullanılarak HTTP web sayfasına erişilmesi

DNS Çözümleme ve Web Erişimi Gözlem Tablosu

İncelenen Unsur	Gözlemlediğiniz Sonuç	
DNS sunucusunun IPv4 adresi		
Web sunucusunun IPv4 adresi		
Oluşturulan alan adı		
DNS sunucusuna ping yanıtı alındı mı?	☐ Evet	☐ Hayır
Web sunucusuna IPv4 adresiyle ping yanıtı alındı mı?	☐ Evet	☐ Hayır
ping www.siber.test komutunda çözümlenen IPv4 adresi		
http://www.siber.test adresinden web sayfası açıldı mı?	☐ Evet	☐ Hayır
Karşılaşılan sorun varsa kısa açıklaması		
Sorunu gidermek için yapılan işlem		

Sonuçları Yorumlamak

Aşağıdaki soruları cevaplayınız.

1. ping 10.10.100.2 komutu başarılı olduğu hâlde ping www.siber.test komutu başarısız olursa hangi yapılandırma kontrol edilmelidir?

   .....
   .....

2. DNS sunucusundaki A kaydının temel görevi nedir?

   .....
   .....

3. HTTP ve HTTPS arasındaki temel fark nedir?

   .....
   .....

4. HTTPS bağlantısı kurulması, web sitesindeki bütün içeriklerin kesinlikle güvenilir olduğunu kanıtlar mı?

   .....
   .....

Değerlendirme

Çalışmanız öğretmeniniz tarafından kontrol listesine göre değerlendirilecektir. Çalışmanızı yaparken buradaki ölçütleri dikkate alınız. Kontrol listesi formuna ulaşmak için karekodu okutunuz. Dijital yayınlarda karekodun üstüne tıklayarak içeriğe ulaşabilirsiniz.

3. ETKİNLİK

Etkinlik Adı	HTTP ve HTTPS Bağlantılarını Karşılaştırmak
Süre	10 dakika
Amaç	HTTP ve HTTPS bağlantılarını veri güvenliği, adres gösterimi ve kullanım alanları bakımından karşılaştırmak
Yönerge	Aşağıdaki karşılaştırma ölçütlerini inceleyiniz. HTTP ile HTTPS bağlantılarının temel özelliklerini tabloya yazınız. Ardından verilen ifadeyi değerlendiriniz.

Karşılaştırma Ölçütü	HTTP	HTTPS
Web erişimindeki temel görevi		
Bağlantının TLS ile korunması		
Yaygın varsayılan port		
Adres çubuğundaki yaygın başlangıç ifadesi		
Hassas bilgilerin iletimi açısından uygunluğu		

Bir öğrenci aşağıdaki ifadeyi kullanmıştır.

"Adres çubuğunda https:// yazıyorsa web sitesindeki bütün bilgiler kesinlikle doğrudur."

Bu ifadeyi değerlendiriniz.

.....

.....

.....

.....

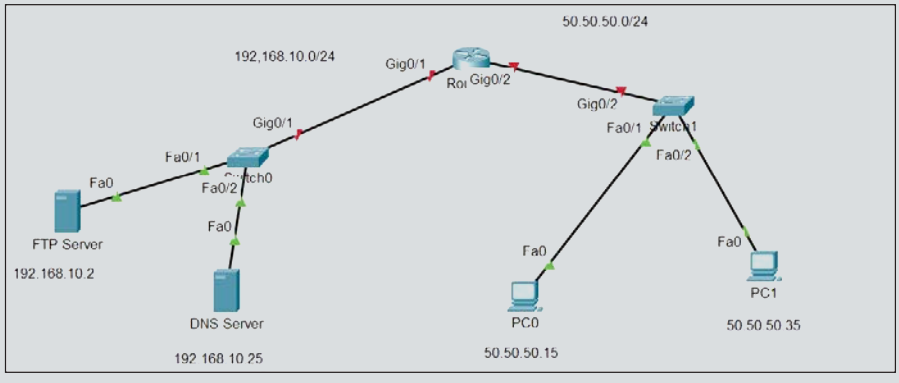
2.3.6. FTP Protokolü

Dosya Aktarım Protokolü [File Transfer Protocol (FTP)], ağ üzerindeki istemci ve sunucu cihazlar arasında dosya aktarımı yapılmasını sağlayan uygulama katmanı protokolüdür. Bir istemci, FTP sunucusuna bağlanarak yetkileri doğrultusunda dosyaları listeleyebilir, sunucudan dosya indirebilir veya sunucuya dosya yükleyebilir. FTP, ağ iletişiminin yalnızca web sayfalarının görüntülenmesi veya bağlantı testlerinin yapılmasıyla sınırlı olmadığını gösterir. Ağ üzerindeki farklı sistemler arasında dosya paylaşımı da belirli protokol kurallarına göre gerçekleştirilir.

FTP hizmetinde kullanıcı adı ve parolayla oturum açılması gerekebilir. Kullanıcı hesabına tanımlanan yetkiler, hangi işlemlerin gerçekleştirilebileceğini belirler. Örneğin bir kullanıcıya yalnızca dosyaları listeleme ve indirme yetkisi verilebilirken başka bir kullanıcıya dosya yükleme yetkisi de tanımlanabilir.

12. UYGULAMA

Uygulama Adı	FTP ile Dosya Aktarımı Gerçekleştirmek
Süre	35 dakika
Amaç	FTP protokolünü kullanarak alan adı üzerinden dosya aktarımı gerçekleştirmek (Görsel 2.90)
Yönerge	Aşağıdaki adres planını kullanarak FTP ve DNS sunucularını, yönlendirici arayüzlerini ve istemci cihazları yapılandırınız. DNS sunucusunda FTP sunucusuna ait alan adı kaydını oluşturunuz. İstemci bilgisayardan önce IP düzeyinde bağlantıyı, ardından alan adı çözümlemesini sınayınız. FTP sunucusuna kullanıcı hesabıyla bağlanarak dosya listesini görüntüleyiniz ve örnek dosyayı indiriniz. Elde ettiğiniz sonuçları gözlem tablosuna yazınız ve uygulama sonunda soruları cevaplayınız.
Araç Gereç	Ağ simülasyon programı, bir yönlendirici, iki switch, bir FTP sunucusu, bir DNS sunucusu, iki istemci bilgisayar, çalışma yaprağı.



Görsel 2.90: FTP dosya aktarımı uygulaması topolojisi

Dikkat Edilecek Noktalar

- Yönlendirici arayüzlerine doğru IPv4 adreslerini veriniz.
- FTP ve DNS sunucularını statik IPv4 adresleriyle yapılandırınız.
- İstemcilere doğru varsayılan ağ geçidi ve DNS sunucusu bilgilerini giriniz.
- DNS sunucusunda ftp.okul.test alan adını FTP sunucusunun IPv4 adresiyle eşleştiriniz.
- FTP sunucusunda kullanıcı hesabının yetkilerini kontrol ediniz.
- Önce IP düzeyindeki bağlantıyı, ardından DNS çözümlemesini sınayınız.
- FTP sunucusuna bağlanarak dosya listesini görüntüleyiniz ve örnek dosyayı indiriniz.
- Grup içinde görev paylaşımı yapınız.

Adres Planı

Cihaz veya Arayüz	IPv4 Adresi	Alt Ağ Maskesi	Varsayılan Ağ Geçidi	DNS Sunucusu
Yönlendirici G0/1	192.168.10.1	255.255.255.0	–	–
Yönlendirici G0/2	50.50.50.1	255.255.255.0	–	–
FTP sunucusu	192.168.10.2	255.255.255.0	192.168.10.1	–
DNS sunucusu	192.168.10.25	255.255.255.0	192.168.10.1	–
PC0	50.50.50.15	255.255.255.0	50.50.50.1	192.168.10.25
PC1	50.50.50.35	255.255.255.0	50.50.50.1	192.168.10.25

1. Adım: Topolojiyi Oluşturmak

Ağ simülasyon programında aşağıdaki cihazları çalışma alanına ekleyiniz.

- bir yönlendirici
- iki switch
- bir FTP sunucusu
- bir DNS sunucusu
- PC0
- PC1

Cihazları Görsel 2.90'da verilen topolojiye uygun biçimde bağlayınız.

2. Adım: Yönlendirici Arayüzlerini Yapılandırmak

Yönlendiricinin komut satırı arayüzünü açınız. Aşağıdaki komutları giriniz.

```
Router> enable
Router# configure terminal
Router(config)# interface gigabitethernet 0/1
Router(config-if)# ip address 192.168.10.1 255.255.255.0
Router(config-if)# no shutdown
Router(config-if)# exit
Router(config)# interface gigabitethernet 0/2
Router(config-if)# ip address 50.50.50.1 255.255.255.0
Router(config-if)# no shutdown
Router(config-if)# end
```

3. Adım: FTP ve DNS Sunucularını Yapılandırmak

FTP sunucusunda **Desktop > IP Configuration** bölümünü açınız. Aşağıdaki bilgileri giriniz.

IPv4 Address: 192.168.10.2

Subnet Mask: 255.255.255.0

Default Gateway: 192.168.10.1

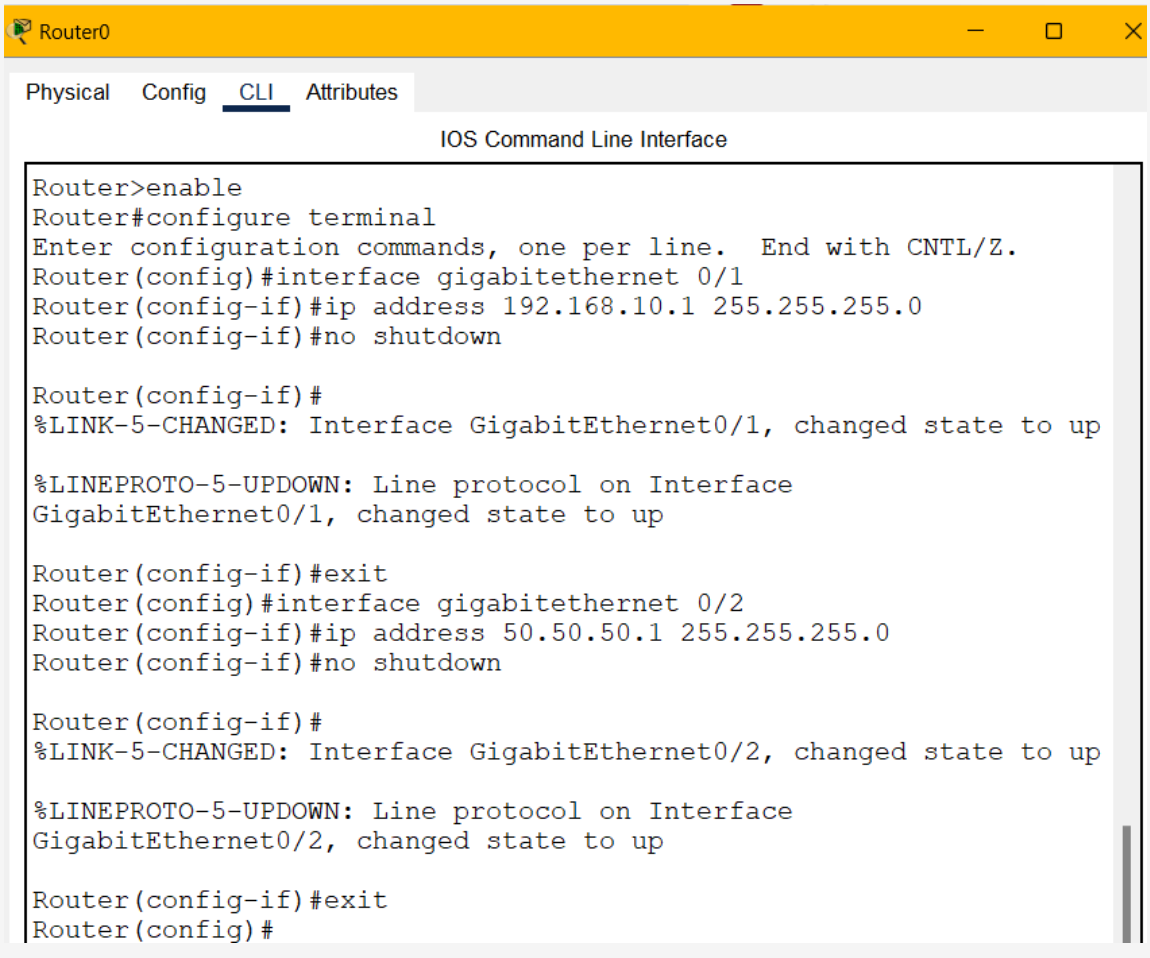
DNS sunucusunda **Desktop > IP Configuration** bölümünü açınız. Aşağıdaki bilgileri giriniz.

IPv4 Address: 192.168.10.25

Subnet Mask: 255.255.255.0

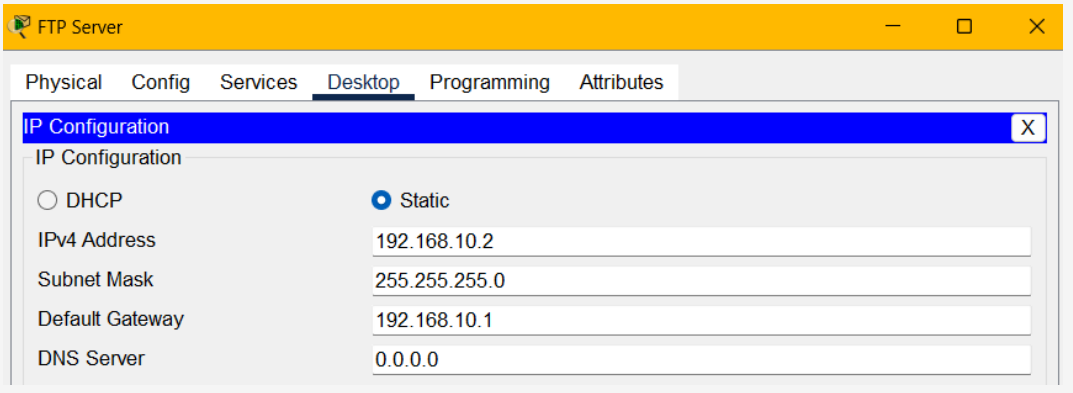
Default Gateway: 192.168.10.1

Yönlendirici arayüzlerinin IPv4 yapılandırma işlemi Görsel 2.91'de gösterilmiştir.

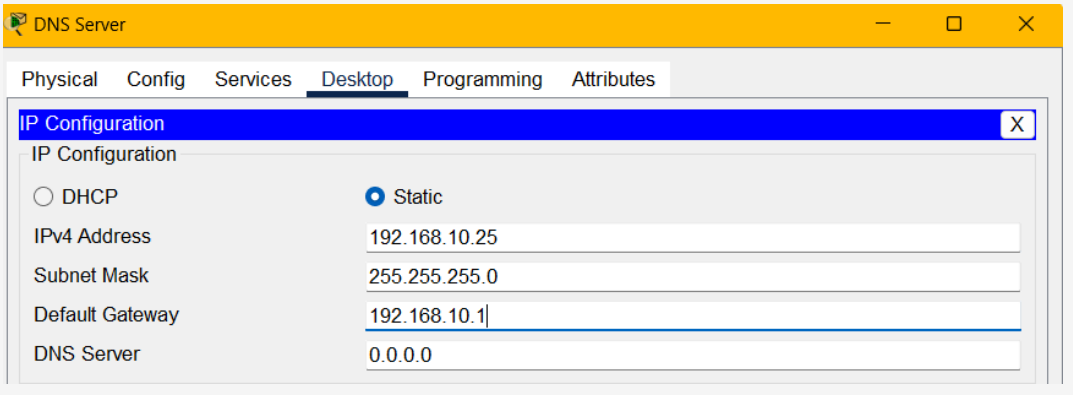


Görsel 2.91: Yönlendirici arayüzlerinin IPv4 yapılandırması

FTP sunucusunun IPv4 yapılandırması Görsel 2.92'de ve DNS sunucusunun IPv4 yapılandırması Görsel 2.93'te gösterilmiştir.



Görsel 2.92: FTP sunucusunun IPv4 yapılandırması



Görsel 2.93: DNS sunucusunun IPv4 yapılandırması

4. Adım: İstemci Cihazları Yapılandırmak

PC0 cihazında **Desktop > IP Configuration** bölümünü açınız. Aşağıdaki bilgileri giriniz.

IPv4 Address: 50.50.50.15

Subnet Mask: 255.255.255.0

Default Gateway: 50.50.50.1

DNS Server: 192.168.10.25

PC1 cihazında **Desktop > IP Configuration** bölümünü açınız. Aşağıdaki bilgileri giriniz.

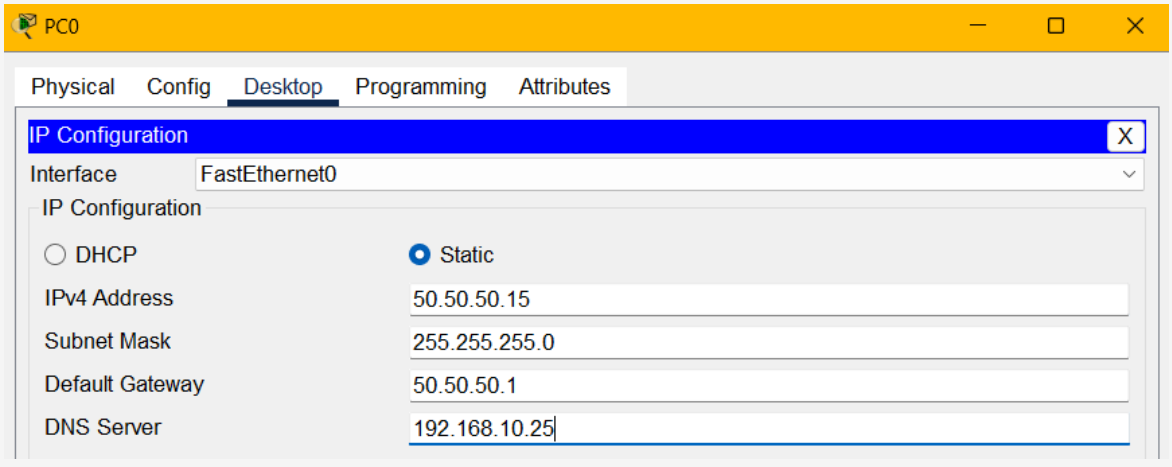
IPv4 Address: 50.50.50.35

Subnet Mask: 255.255.255.0

Default Gateway: 50.50.50.1

DNS Server: 192.168.10.25

İstemcinin IPv4 ve DNS yapılandırması Görsel 2.94'te gösterilmiştir.



Görsel 2.94: İstemcinin IPv4 ve DNS yapılandırması

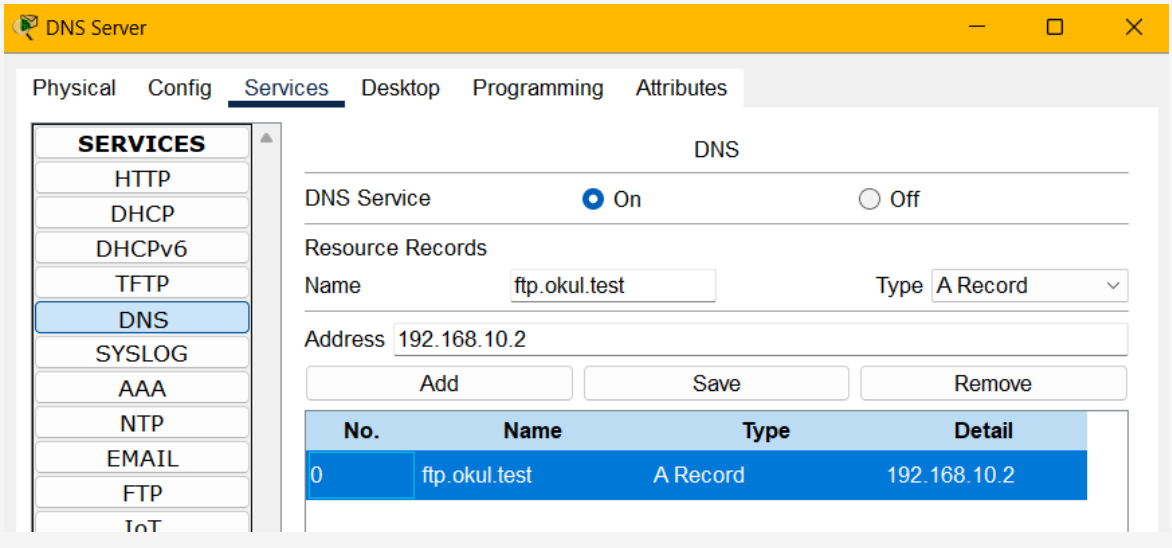
5. Adım: DNS Kaydını Oluşturmak

DNS sunucusunda **Services > DNS** bölümünü açınız. DNS hizmetini etkinleştiriniz (Görsel 2.95).

Aşağıdaki kaydı oluşturunuz.

Name: ftp.okul.test
Type: A
Address: 192.168.10.2

Kaydı girdikten sonra **Add** düğmesine tıklayınız.



Görsel 2.95: DNS sunucusunda ftp.okul.test A kaydının oluşturulması

6. Adım: FTP Hizmetini Etkinleştirmek

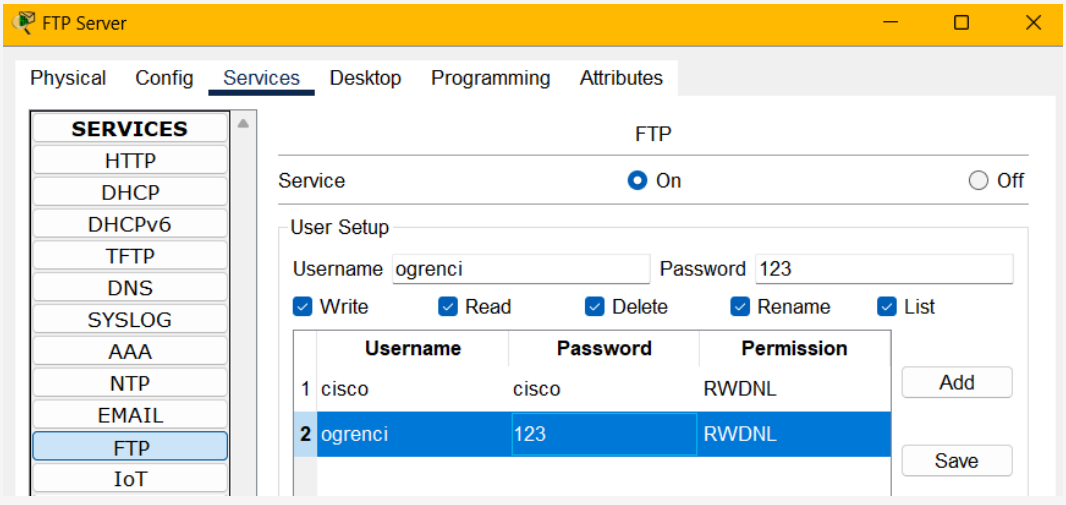
FTP sunucusunda **Services > FTP** bölümünü açınız. FTP hizmetini etkinleştiriniz.

Aşağıdaki kullanıcı hesabını oluşturunuz.

Username: ogrenci

Password: 123

Kullanıcıya uygulamada gerçekleştirilecek işlemlere uygun yetkileri veriniz. En azından dosyaları listeleme ve indirme yetkisinin etkin olduğundan emin olunuz (Görsel 2.96).



Görsel 2.96: FTP sunucusunda kullanıcı hesabının oluşturulması

7. Adım: IP Düzeyindeki Bağlantıyı Sınamak

PC0 cihazında **Desktop > Command Prompt** bölümünü açınız.

Öncelikle istemci tarafındaki yönlendirici arayüzüne erişimi sınayınız.

ping 50.50.50.1

Ardından FTP sunucusuna erişimi sınayınız.

ping 192.168.10.2

Son olarak DNS sunucusuna erişimi sınayınız.

ping 192.168.10.25

Bu testlerin başarılı olması, istemci cihazın yönlendirici aracılığıyla diğer ağdaki FTP ve DNS sunucularına erişebildiğini gösterir.

8. Adım: DNS Çözümlemesini Sınamak

PC0 cihazının komut satırında aşağıdaki komutu giriniz.

ping ftp.okul.test

Komut çıktısında ftp.okul.test alan adının 192.168.10.2 IPv4 adresiyle ilişkilendirildiğini gözlemleyiniz.

9. Adım: FTP Sunucusuna Bağlanmak

Aynı komut satırında aşağıdaki komutu giriniz.

ftp ftp.okul.test

Bağlantı kurulduğunda kullanıcı adı ve parola bilgilerini giriniz.

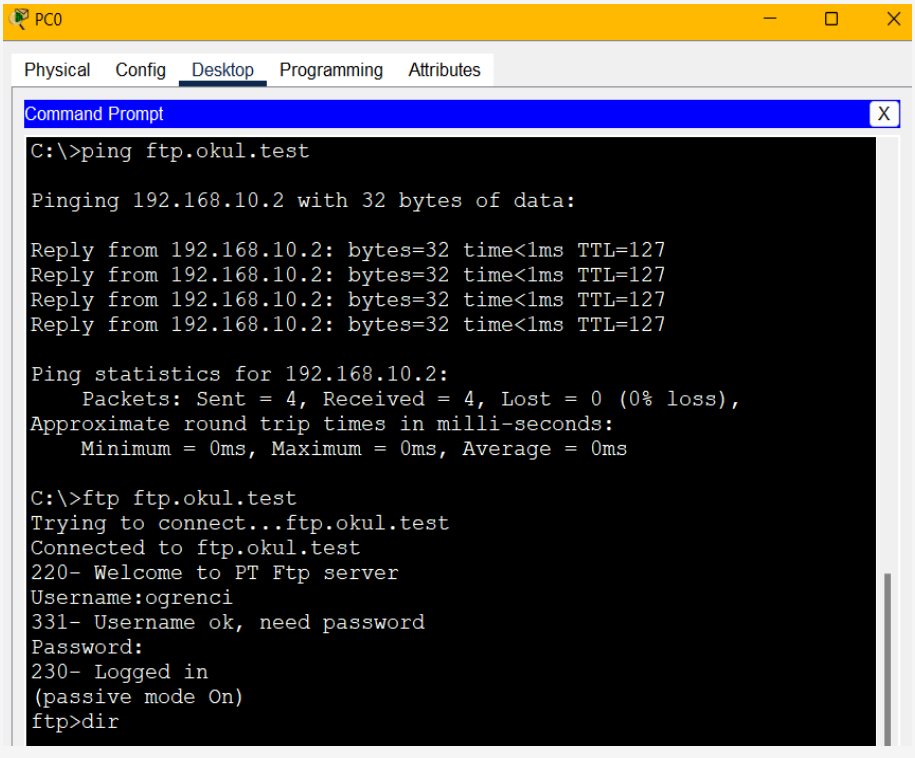
Username: ogrenci

Password: 123

Giriş başarılı olduğunda FTP sunucusundaki dosyaları listelemek için aşağıdaki komutu kullanınız.

dir

PC0 cihazından FTP sunucusuna alan adıyla bağlantı kurulması Görsel 2.97'de gösterilmiştir.



Görsel 2.97: PC0 cihazından FTP sunucusuna alan adıyla bağlanılması

10. Adım: Sunucudan Örnek Dosyayı İndirmek

Öğretmeninizin FTP sunucusunda önceden hazırladığı örnek dosyayı indiriniz.

Örnek dosya adı:

ornek.txt

Dosyayı indirmek için aşağıdaki komutu kullanınız.

get ornek.txt

İşlemi tamamladıktan sonra FTP oturumundan çıkınız.

quit

FTP Dosya Aktarımı Gözlem Tablosu

İncelenen Unsur	Gözlemlediğiniz Sonuç
FTP sunucusunun IPv4 adresi	
DNS sunucusunun IPv4 adresi	
FTP sunucusu için oluşturulan alan adı	
FTP sunucusuna IP adresiyle ping yanıtı alındı mı?	☐ Evet ☐ Hayır
DNS sunucusuna ping yanıtı alındı mı?	☐ Evet ☐ Hayır
ping ftp.okul.test komutunda çözümlenen IPv4 adresi	
FTP sunucusuna alan adıyla bağlantı kuruldu mu?	☐ Evet ☐ Hayır
Kullanıcı hesabıyla oturum açıldı mı?	☐ Evet ☐ Hayır
dir komutuyla dosyalar listelendi mi?	☐ Evet ☐ Hayır
ornek.txt dosyası indirildi mi?	☐ Evet ☐ Hayır ☐ Simülasyon sürümünde desteklenmedi
Karşılaşılan sorun varsa kısa açıklaması	
Sorunu gidermek için yapılan işlem	

Sonuçları Yorumlamak

Aşağıdaki soruları cevaplayınız.

1. FTP protokolünün temel görevi nedir?

   .....

2. ping 192.168.10.2 komutu başarılı olduğu hâlde ftp ftp.okul.test komutuyla bağlantı kurulamıyorsa hangi yapılandırmalar kontrol edilmelidir?

   .....

3. DNS sunucusundaki A kaydı bu uygulamada hangi görevi üstlenmektedir?

   .....

4. FTP kullanıcı hesabına verilen yetkiler neden önemlidir?

   .....

5. Temel FTP protokolü hassas dosyaların aktarımında neden tek başına yeterli görülmemelidir?

   .....

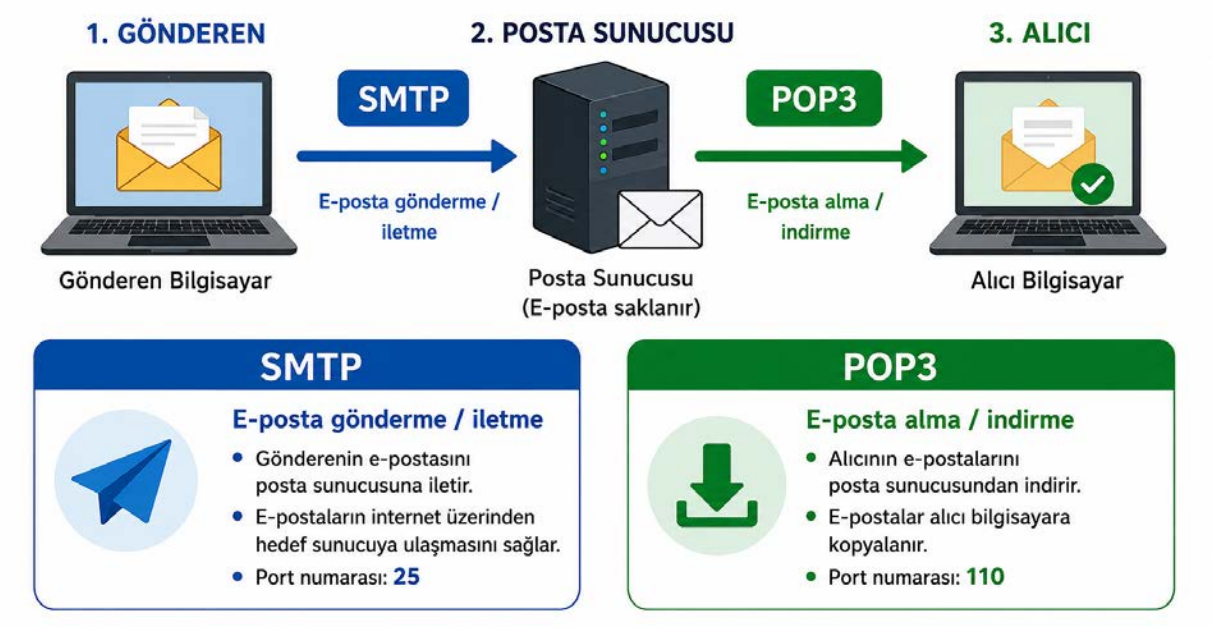
Değerlendirme

Çalışmanız öğretmeniniz tarafından kontrol listesine göre değerlendirilecektir. Çalışmanızı yaparken buradaki ölçütleri dikkate alınız. Kontrol listesi formuna ulaşmak için karekodu okutunuz. Dijital yayınlarda karekodun üstüne tıklayarak içeriğe ulaşabilirsiniz.

2.3.7. SMTP ve POP3 Protokolleri

E-posta iletişimi, ağ üzerinde farklı görevler üstlenen protokollerin birlikte çalışmasıyla gerçekleştirilir. Bir e-postanın gönderilmesi ile alıcının posta kutusundan alınarak görüntülenmesi aynı işlem değildir. Bu süreçlerde farklı protokoller kullanılır. **Basit Posta Aktarım Protokolü [Simple Mail Transfer Protocol (SMTP)]**, e-postaların gönderilmesi ve posta sunucuları arasında iletilmesiyle ilişkili uygulama katmanı protokolüdür. Bir kullanıcı e-posta istemcisinde mesaj oluşturup gönderdiğinde ileti, SMTP aracılığıyla posta sunucusuna aktarılır.

Postane Protokolü Sürüm 3 [Post Office Protocol Version 3 (POP3)], posta sunucusunda bulunan e-postaların istemci cihaza alınmasıyla ilişkili uygulama katmanı protokolüdür. Kullanıcı gelen kutusunu kontrol ettiğinde veya iletileri almak için ilgili düğmeye tıkladığında istemci, POP3 aracılığıyla posta sunucusundaki mesajlara erişir (Görsel 2.98).



Görsel 2.98: SMTP ve POP3 protokollerinin e-posta iletişimindeki görevleri

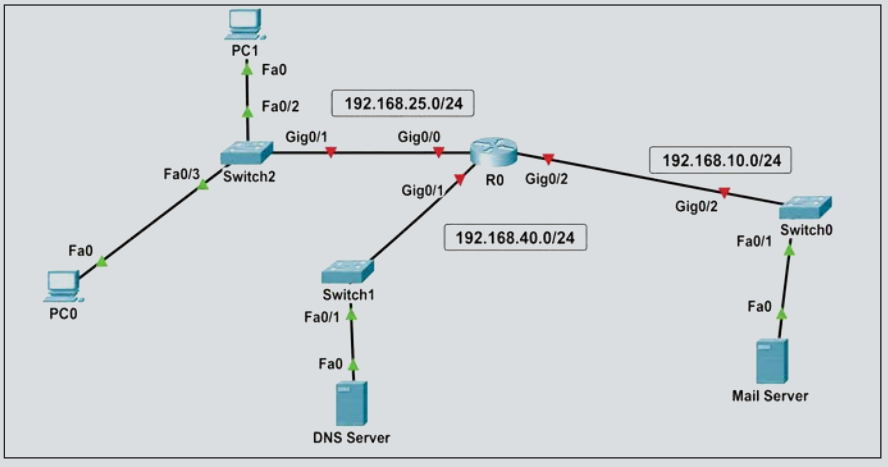
İstemcilerin posta hizmetine mesaj göndermesi amacıyla kullanılan yapılarda 587 numaralı port da yaygın olarak tercih edilir.

BİLGİ KUTUSU : E-Postalara Dosya Nasıl Eklenir?

E-posta sistemleri başlangıçta ağırlıklı olarak metin iletmek amacıyla geliştirilmiştir. Görsel, belge, ses, video gibi dosyaların e-postaya eklenebilmesi için MIME (Multipurpose Internet Mail Extensions) standardından yararlanılır. MIME, ileti içeriğinin türünü belirtir ve metin dışındaki verileri e-posta sistemi üzerinden taşınabilecek biçime dönüştürür. Bu dönüşüm nedeniyle eklenen bir dosyanın iletim sırasındaki veri boyutu özgün dosya boyutundan daha büyük olabilir. Alıcının e-posta uygulaması, MIME bilgilerini okuyarak ileti metnini ve ekli dosyaları uygun biçimde görüntüler.

13. UYGULAMA

Uygulama Adı	SMTP ve POP3 ile E-Posta Göndermek ve Almak
Süre	35 dakika
Amaç	SMTP ve POP3 protokollerini kullanarak e-posta gönderme ve alma işlemini gerçekleştirmek (Görsel 2.99)
Yönerge	Aşağıdaki adres planını kullanarak DNS sunucusunu, posta sunucusunu, yönlendirici arayüzlerini ve istemci cihazları yapılandırınız. DNS sunucusunda posta sunucusuna ait alan adı kaydını oluşturunuz. Posta sunucusunda alan adını ve kullanıcı hesaplarını tanımlayınız. İstemci bilgisayarlarda e-posta hesaplarını yapılandırarak SMTP ile mesaj gönderiniz, POP3 ile gelen mesajı alınız. Elde ettiğiniz sonuçları gözlem tablosuna yazınız ve uygulama sonunda soruları cevaplayınız.
Araç Gereç	Ağ simülasyon programı, bir yönlendirici, üç switch, bir DNS sunucusu, bir posta sunucusu, iki istemci bilgisayar, çalışma yaprağı.



Görsel 2.99: SMTP ve POP3 e-posta uygulaması topolojisi

Dikkat Edilecek Noktalar:

- Yönlendirici arayüzlerini doğru IPv4 adresleriyle yapılandırınız.
- DNS ve posta sunucularına uygun statik IPv4 adreslerini veriniz.
- İstemcilerin varsayılan ağ geçidi ve DNS sunucusu bilgilerini eksiksiz giriniz.
- DNS sunucusunda mail.example.com alan adını posta sunucusunun IPv4 adresiyle eşleştiriniz.
- Posta sunucusunda example.com alan adını ve kullanıcı hesaplarını oluşturunuz.
- İstemcilerde gelen posta ve giden posta sunucusu alanlarına mail.example.com yazınız.
- Önce IP düzeyindeki bağlantıyı ve DNS çözümlemesini sınayınız.
- SMTP ile mesaj gönderiniz ve POP3 ile mesajı alınız.
- Grup içinde görev paylaşımı yapınız.

Adres Planı

Cihaz veya Arayüz	IPv4 Adresi	Alt Ağ Maskesi	Varsayılan Ağ Geçidi	DNS Sunucusu
Yönlendirici G0/0	192.168.25.1	255.255.255.0	–	–
Yönlendirici G0/1	192.168.40.1	255.255.255.0	–	–
Yönlendirici G0/2	192.168.10.1	255.255.255.0	–	–
DNS sunucusu	192.168.40.2	255.255.255.0	192.168.40.1	–
Posta sunucusu	192.168.10.2	255.255.255.0	192.168.10.1	–
PC0	192.168.25.10	255.255.255.0	192.168.25.1	192.168.40.2
PC1	192.168.25.20	255.255.255.0	192.168.25.1	192.168.40.2

1. Adım: Yönlendirici Arayüzlerini Yapılandırmak

Yönlendiricinin komut satırı arayüzünü açınız. Aşağıdaki komutları giriniz.

Router> enable

Router# configure terminal

Router(config)# interface gigabitethernet 0/0

Router(config-if)# ip address 192.168.25.1 255.255.255.0

Router(config-if)# no shutdown

Router(config-if)# exit

Router(config)# interface gigabitethernet 0/1

Router(config-if)# ip address 192.168.40.1 255.255.255.0

Router(config-if)# no shutdown

Router(config-if)# exit

Router(config)# interface gigabitethernet 0/2

Router(config-if)# ip address 192.168.10.1 255.255.255.0

Router(config-if)# no shutdown

Router(config-if)# end

2. Adım: DNS ve Posta Sunucularını Yapılandırmak

DNS sunucusunda **Desktop > IP Configuration** bölümünü açınız. Aşağıdaki bilgileri giriniz.

IPv4 Address: 192.168.40.2

Subnet Mask: 255.255.255.0

Default Gateway: 192.168.40.1

Posta sunucusunda **Desktop > IP Configuration** bölümünü açınız. Aşağıdaki bilgileri giriniz.

IPv4 Address: 192.168.10.2

Subnet Mask: 255.255.255.0

Default Gateway: 192.168.10.1

3. Adım: İstemci Cihazları Yapılandırmak

PC0 cihazında **Desktop > IP Configuration** bölümünü açınız. Aşağıdaki bilgileri giriniz.

IPv4 Address: 192.168.25.10

Subnet Mask: 255.255.255.0

Default Gateway: 192.168.25.1

DNS Server: 192.168.40.2

PC1 cihazında **Desktop > IP Configuration** bölümünü açınız. Aşağıdaki bilgileri giriniz.

IPv4 Address: 192.168.25.20

Subnet Mask: 255.255.255.0

Default Gateway: 192.168.25.1

DNS Server: 192.168.40.2

4. Adım: DNS Kaydını Oluşturmak

DNS sunucusunda **Services > DNS** bölümünü açınız. DNS hizmetini etkinleştiriniz.

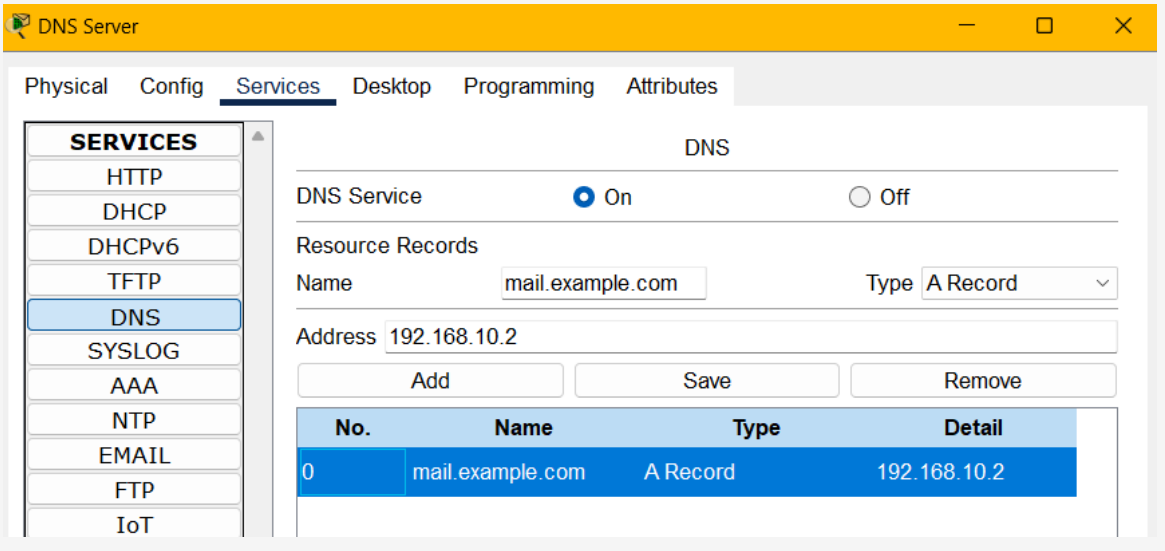
Aşağıdaki kaydı oluşturunuz.

Name: mail.example.com

Type: A

Address: 192.168.10.2

Kaydı girdikten sonra **Add** düğmesine tıklayınız (Görsel 2.100).



Görsel 2.100: DNS sunucusunda mail.example.com A kaydının oluşturulması

5. Adım: Posta Sunucusunda E-Posta Hizmetini Etkinleştirmek

Posta sunucusunda **Services > EMAIL** bölümünü açınız. E-posta hizmetinin etkin olduğundan emin olunuz.

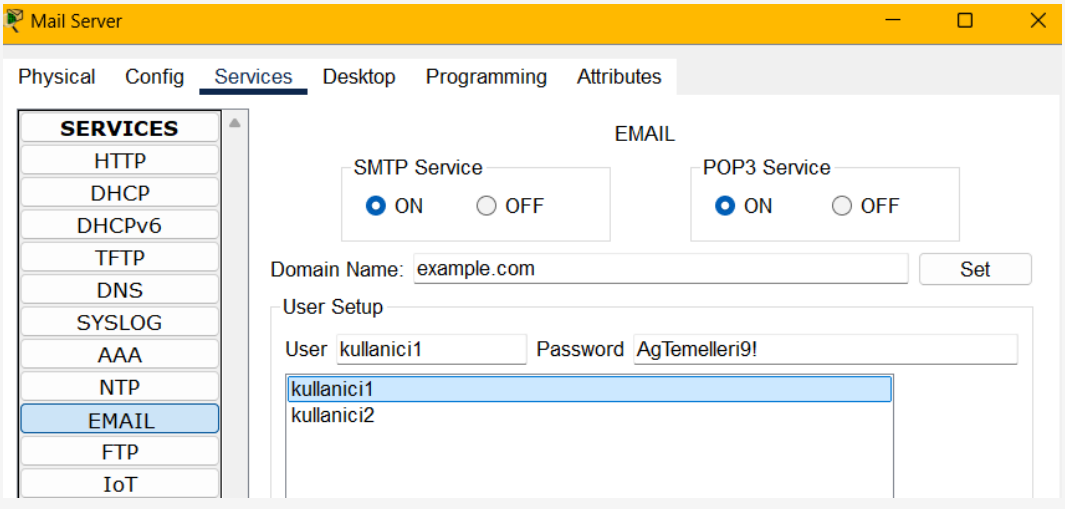
Alan adı bölümüne aşağıdaki değeri yazınız.

Domain Name: example.com

Ardından aşağıdaki kullanıcı hesaplarını oluşturunuz.

Kullanıcı Adı	Parola	Oluşturulan E-Posta Adresi
kullanici1	AgTemelleri9!	kullanici1@example.com
kullanici2	PostaUygulama9!	kullanici2@example.com

Kullanıcı bilgilerini girdikten sonra **Add (+)** düğmesine tıklayarak hesapları ekleyiniz (Görsel 2.101).



Görsel 2.101: Posta sunucusunda alan adının ve kullanıcı hesaplarının oluşturulması

6. Adım: İstemcilerde E-Posta Hesaplarını Yapılandırmak

PC0 cihazında **Desktop > Email** bölümünü açınız. Aşağıdaki bilgileri giriniz.

Your Name: Kullanıcı 1

Email Address: kullanici1@example.com

Incoming Mail Server: mail.example.com

Outgoing Mail Server: mail.example.com

Username: kullanici1

Password: AgTemelleri9!

Bilgileri girdikten sonra hesabı kaydediniz.

7. Adım: E-Posta Hesaplarını Yapılandırmak

PC1 cihazında Desktop > Email bölümünü açınız. Aşağıdaki bilgileri giriniz.

Your Name: Kullanıcı 2

Email Address: kullanici2@example.com

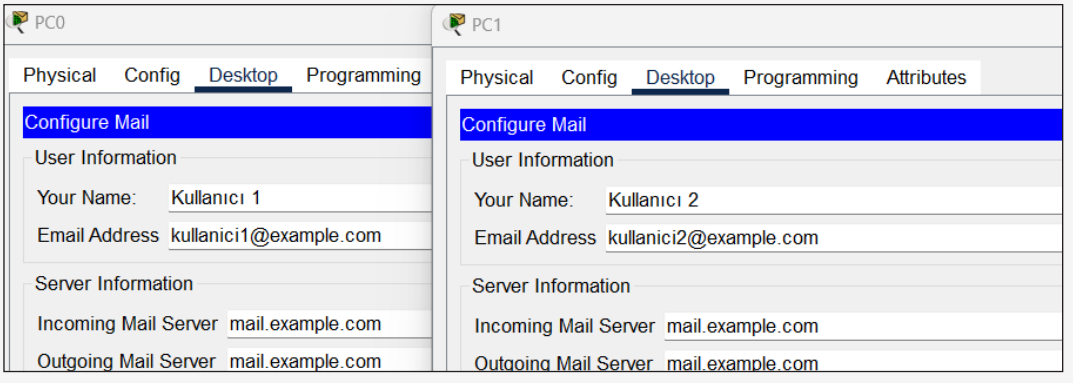
Incoming Mail Server: mail.example.com

Outgoing Mail Server: mail.example.com

Username: kullanici2

Password: PostaUygulama9!

Bilgileri girdikten sonra hesabı kaydediniz (Görsel 2.102).



Görsel 2.102: İstemcilerde e-posta hesaplarının yapılandırılması

8. Adım: PC0 Cihazından E-Posta Göndermek

PC0 cihazında e-posta istemcisini açınız. **Compose** veya yeni mesaj oluşturma bölümüne geçiniz.

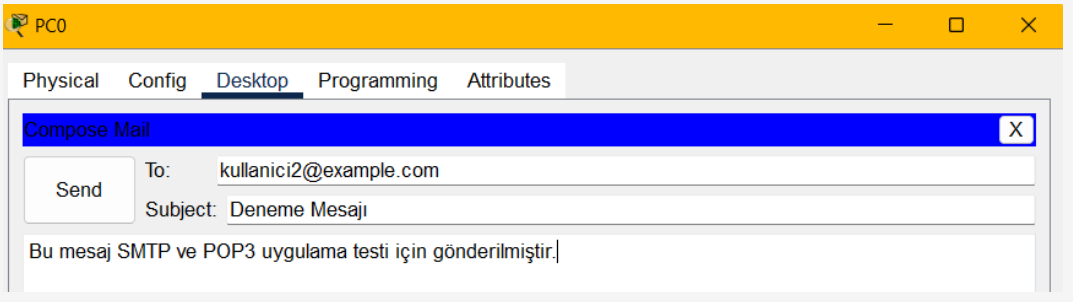
Aşağıdaki bilgileri giriniz.

To: kullanici2@example.com

Subject: Deneme Mesajı

Message: Bu mesaj SMTP ve POP3 uygulama testi için gönderilmiştir.

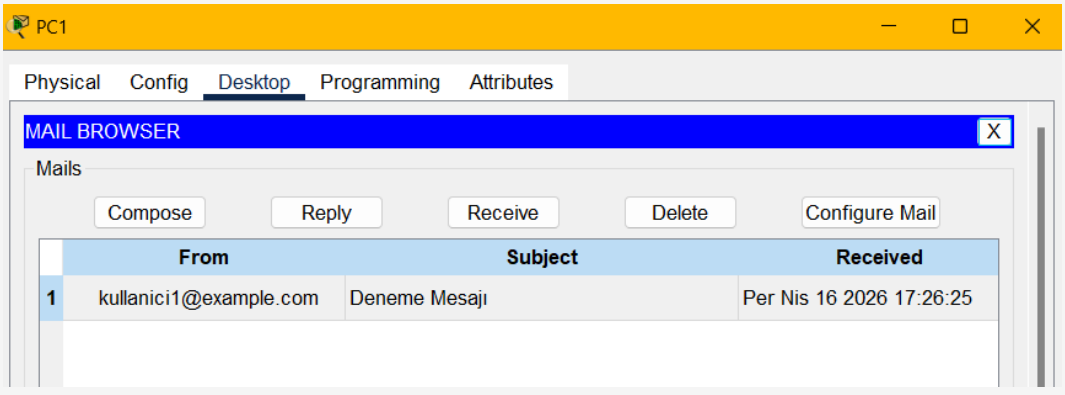
Mesajı gönderiniz (Görsel 2.103).



Görsel 2.103: PC0 cihazından SMTP ile e-posta gönderilmesi

9. Adım: PC1 Cihazında E-Postayı Almak

PC1 cihazında **Desktop > Email** bölümünü açınız. Gelen kutusunu kontrol ediniz. Gerekirse **Receive** düğmesine tıklayınız (Görsel 2.104).



Görsel 2.104: PC1 cihazında POP3 ile e-postanın alınması

10. Adım: Ters Yönde Mesaj Göndererek İşlemi Doğrulamak

PC1 cihazından PC0 cihazına aşağıdaki bilgileri kullanarak yeni bir mesaj gönderiniz.

To: kullanici1@example.com
Subject: Yanıt Mesajı
Message: SMTP ve POP3 uygulaması başarıyla tamamlanmıştır.

PC0 cihazının gelen kutusunu kontrol ederek mesajı alınız.

SMTP ve POP3 E-Posta Uygulaması Gözlem Tablosu

İncelenen Unsur	Gözlemlediğiniz Sonuç
DNS sunucusunun IPv4 adresi	
Posta sunucusunun IPv4 adresi	
DNS sunucusunda oluşturulan alan adı	
Posta sunucusunda tanımlanan alan adı	
Birinci e-posta hesabı	
İkinci e-posta hesabı	
ping 192.168.10.2 komutuyla posta sunucusuna erişildi mi?	☐ Evet ☐ Hayır
ping mail.example.com komutunda çözümlenen IPv4 adresi	
PC0 cihazından mesaj gönderildi mi?	☐ Evet ☐ Hayır
PC1 cihazında mesaj alındı mı?	☐ Evet ☐ Hayır
Ters yönde mesaj gönderildi mi?	☐ Evet ☐ Hayır
SMTP protokolünün gözlemlenen görevi	
POP3 protokolünün gözlemlenen görevi	
Karşılaşılan sorun varsa kısa açıklaması	
Sorunu gidermek için yapılan işlem	

Sonuçları Yorumlamak

Aşağıdaki soruları cevaplayınız.

1. SMTP protokolünün e-posta iletişimindeki temel görevi nedir?

.....
.....

2. POP3 protokolünün e-posta iletişimindeki temel görevi nedir?

.....
.....

3. IP adresine ping 192.168.10.2 komutuyla erişilebildiği hâlde ping mail.example.com komutuyla alan adına erişilemiyorsa hangi DNS yapılandırmaları kontrol edilmelidir?

.....
.....

4. Kullanıcı adı ve parola bilgilerinin doğru tanımlanması neden önemlidir?

.....
.....

5. Temel SMTP ve POP3 iletişimi gerçek sistemlerde neden tek başına yeterince güvenli görülmemelidir?

.....
.....

Değerlendirme

Çalışmanız öğretmeniniz tarafından kontrol listesine göre değerlendirilecektir. Çalışmanızı yaparken buradaki ölçütleri dikkate alınız. Kontrol listesi formuna ulaşmak için karekodu okutunuz. Dijital yayınlarda karekodun üstüne tıklayarak içeriğe ulaşabilirsiniz.

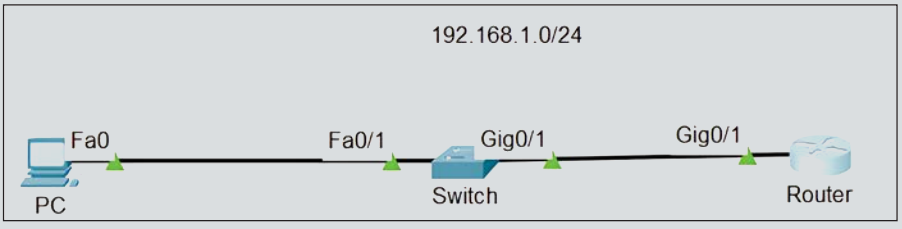
2.3.8. Telnet ve SSH Protokolleri

Telnet ve SSH, ağ üzerindeki cihazlara komut satırı aracılığıyla uzaktan erişilmesini sağlayan uygulama katmanı protokolleridir. Her iki protokol de yönlendirici, switch veya sunucu gibi sistemlerin başka bir cihaz üzerinden yönetilmesine yardımcı olur. Telnet ve SSH arasında veri güvenliği bakımından önemli bir fark bulunmaktadır. **Telnet**, uzak terminal erişimi için kullanılan temel protokollerden biridir. Telnet bağlantısında istemci, uzaktaki cihazın komut satırı arayüzüne erişebilir ve yönetim komutlarını çalıştırabilir. Telnet yaygın olarak 23 numaralı portu kullanır ancak temel Telnet iletişiminde parola ve komutlar şifrelenmeden iletilebilir. Bu nedenle Telnet gerçek ağ ortamlarında güvenli uzaktan yönetim yöntemi olarak tercih edilmemelidir.

Güvenli Kabuk [Secure Shell (SSH)], ağ cihazlarına daha güvenli biçimde uzaktan erişilmesini sağlayan protokoldür. SSH bağlantısında istemci ile uzaktaki cihaz arasındaki iletişim şifrelenir. Böylece oturum açma bilgileri ve yönetim komutları Telnet bağlantısına göre daha korunaklı biçimde iletilir. SSH yaygın olarak 22 numaralı portu kullanır.

14. UYGULAMA

Uygulama Adı	Telnet ve SSH ile Uzaktan Erişimi Karşılaştırmak
Süre	30 dakika
Amaç	Telnet ve SSH protokolleriyle yönlendiriciye uzaktan erişim sağlamak ve güvenlik açısından karşılaştırma yapmak (Görsel 2.105)
Yönerge	Aşağıdaki adres planını kullanarak yönlendirici ve istemci bilgisayarı aynı yerel ağda yapılandırınız. Önce temel bağlantıyı ping komutuyla sınayınız. Yönlendirici üzerinde Telnet erişimini etkinleştirerek istemci bilgisayardan bağlantı kurunuz. Ardından SSH erişimi için gerekli yapılandırmaları yapınız ve istemci bilgisayardan SSH bağlantısını gerçekleştiriniz. Son durumda Telnet erişiminin kapatıldığını doğrulayınız. Elde ettiğiniz sonuçları gözlem tablosuna yazınız ve uygulama sonunda soruları cevaplayınız.
Araç Gereç	Ağ simülasyon programı, bir yönlendirici, bir switch, bir istemci bilgisayar, çalışma yaprağı.



Görsel 2.105: Telnet ve SSH uzaktan erişim uygulaması topolojisi

Dikkat Edilecek Noktalar

- Yönlendirici ve istemci bilgisayarı aynı yerel ağda yapılandırınız.
- Uzaktan erişim denemelerinden önce ping komutuyla temel bağlantıyı sınayınız.
- Telnet bağlantısını yalnızca laboratuvar ortamında karşılaştırma amacıyla kullanınız.
- SSH yapılandırmasında cihaz adını, alan adını, kullanıcı hesabını ve RSA anahtarını eksiksiz tanımlayınız.
- Son yapılandırmada sanal terminal hatlarını yalnızca SSH bağlantısına izin verecek biçimde sınırlandırınız.
- Grup içinde görev paylaşımı yapınız.

Adres Planı

Cihaz veya Arayüz	IPv4 Adresi	Alt Ağ Maskesi	Varsayılan Ağ Geçidi
Yönlendirici G0/1	192.168.1.1	255.255.255.0	–
İstemci bilgisayar	192.168.1.10	255.255.255.0	192.168.1.1

1. Adım: Topolojiyi Oluşturmak

Ağ simülasyon programında aşağıdaki cihazları çalışma alanına ekleyiniz.

- bir yönlendirici
- bir switch
- bir istemci bilgisayar

İstemci bilgisayarı switche, switchi ise yönlendiricinin G0/1 arayüzüne uygun kablolarla bağlayınız.

2. Adım: Yönlendirici Arayüzünü Yapılandırmak

Yönlendiricinin komut satırı arayüzünü açınız. Aşağıdaki komutları giriniz.

Router> enable

Router# configure terminal

Router(config)# interface gigabitethernet 0/1

Router(config-if)# ip address 192.168.1.1 255.255.255.0

Router(config-if)# no shutdown

Router(config-if)# exit

Router(config)# end

3. Adım: İstemci Bilgisayarı Yapılandırmak

İstemci bilgisayarda **Desktop > IP Configuration** bölümünü açınız. Aşağıdaki bilgileri giriniz.

IPv4 Address: 192.168.1.10

Subnet Mask: 255.255.255.0

Default Gateway: 192.168.1.1

4. Adım: Temel IP Erişimini Sınamak

İstemci bilgisayarda **Desktop > Command Prompt** bölümünü açınız. Aşağıdaki komutu çalıştırınız.
ping 192.168.1.1
Yanıt alındığını doğrulayınız. Bağlantı kurulamazsa fiziksel bağlantıları, IP adreslerini, alt ağ maskesini ve yönlendirici arayüzünün etkin olup olmadığını kontrol ediniz.

Telnet Yapılandırması

5. Adım: Yönlendiricide Telnet Erişimini Etkinleştirmek

Yönlendiricinin komut satırı arayüzünde aşağıdaki komutları giriniz.
Router> enable

Router# configure terminal

Router(config)# line vty 0 4

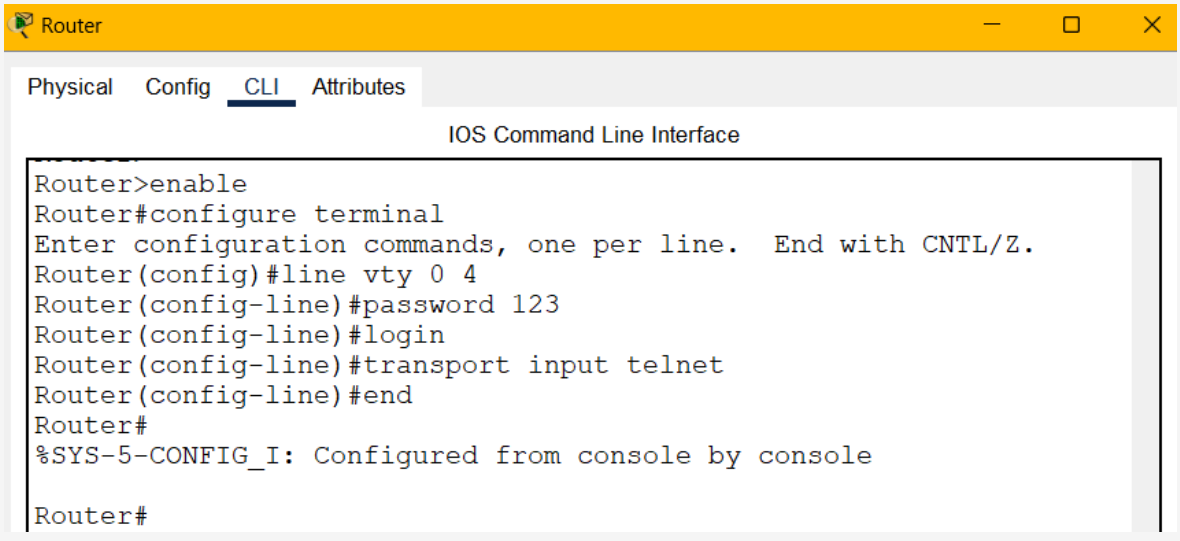
Router(config-line)# password 123

Router(config-line)# login

Router(config-line)# transport input telnet

Router(config-line)# end

Yönlendiricide Telnet erişiminin yapılandırılması Görsel 2.106'da gösterilmiştir.

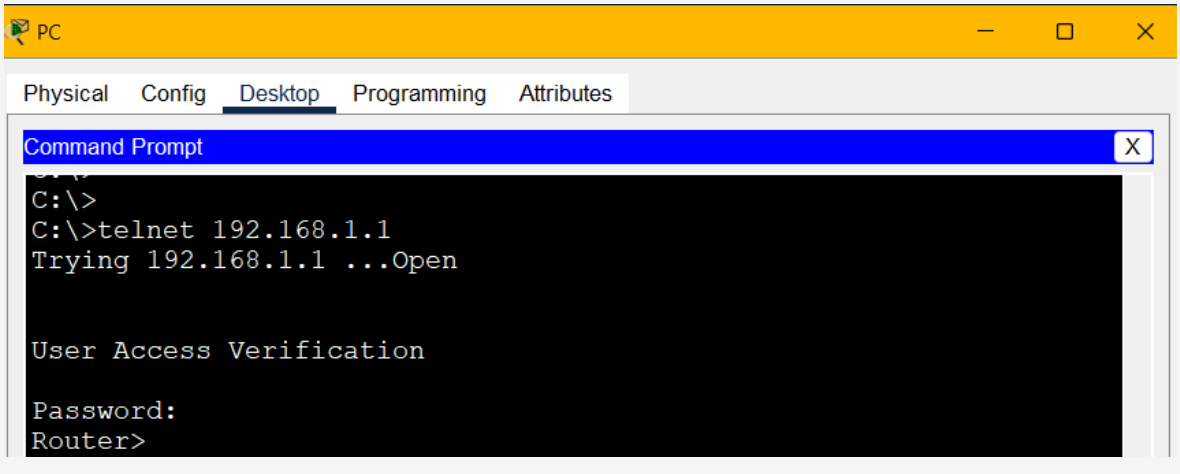


Görsel 2.106: Yönlendiricide Telnet erişiminin yapılandırılması

Bu komutlarla uzaktan erişimde kullanılacak sanal terminal hatları seçilmiş, sanal terminal hatları için parola tanımlanmış ve Telnet bağlantısı etkinleştirilmiş olur.

6. Adım: İstemci Bilgisayardan Telnet Bağlantısı Kurmak

İstemci bilgisayarın komut satırında aşağıdaki komutu çalıştırınız.
telnet 192.168.1.1
Bağlantı kurulduğunda aşağıdaki parolayı giriniz.
Password: 123
Giriş başarılı olursa istemci bilgisayarın yönlendiriciye Telnet üzerinden erişebildiğini doğrulayınız (Görsel 2.107).



Görsel 2.107: İstemci bilgisayardan yönlendiriciye Telnet ile bağlanılması

SSH Yapılandırması

7. Adım: Yönlendiricide SSH Erişimini Etkinleştirmek

Yönlendiricinin komut satırı arayüzünde aşağıdaki komutları giriniz.

Router> enable

Router# configure terminal

Router(config)# hostname Router1

Router1(config)# ip domain-name ozrek.local

Router1(config)# username admin secret 123

Router1(config)# crypto key generate rsa

RSA anahtar uzunluğu sorulduğunda aşağıdaki değeri giriniz.

How many bits in the modulus [512]: 1024

Ardından aşağıdaki komutları uygulayınız.

Router1(config)# ip ssh version 2

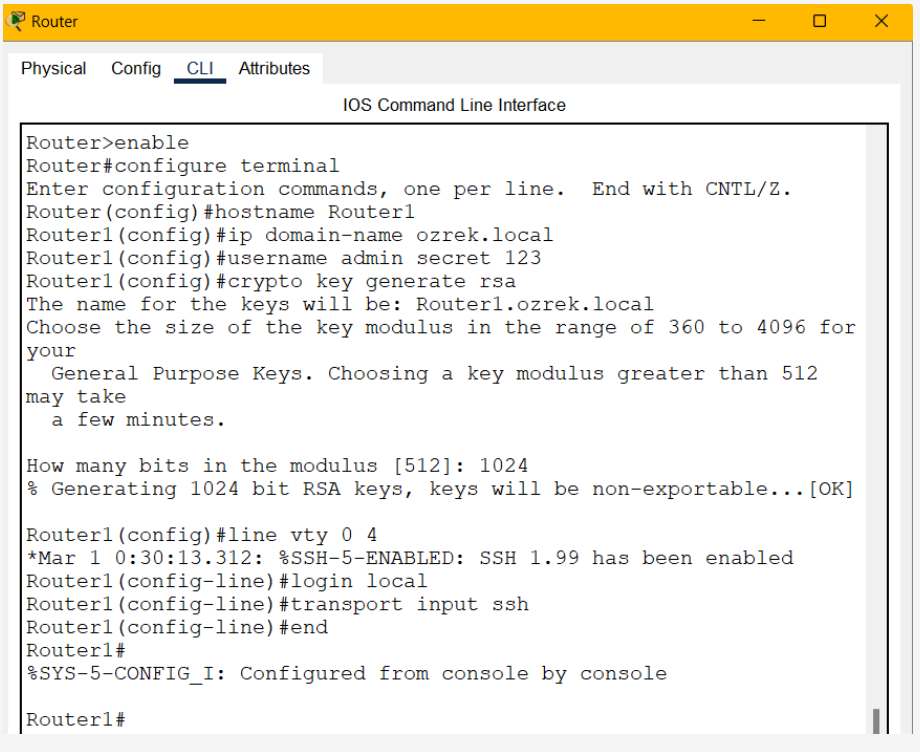
Router1(config)# line vty 0 4

Router1(config-line)# login local

Router1(config-line)# transport input ssh

Router1(config-line)# end

Yönlendiricide SSH erişiminin yapılandırılması Görsel 2.108'de gösterilmiştir.



Görsel 2.108: Yönlendiricide SSH erişiminin yapılandırılması

Bu komutlarla

- yönlendiriciye Router1 adı verilmiş
- RSA anahtarının üretilebilmesi için ozrek.local alan adı tanımlanmış
- admin adlı yerel kullanıcı hesabı oluşturulmuş
- RSA anahtarı üretilmiş
- desteklenen simülasyon ortamında SSH sürüm 2 etkinleştirilmiş
- sanal terminal hatlarında yerel kullanıcı hesabıyla oturum açılması sağlanmış
- gelen uzaktan erişim bağlantıları yalnızca SSH ile sınırlandırılmıştır.

8. Adım: İstemci Bilgisayardan SSH Bağlantısı Kurmak

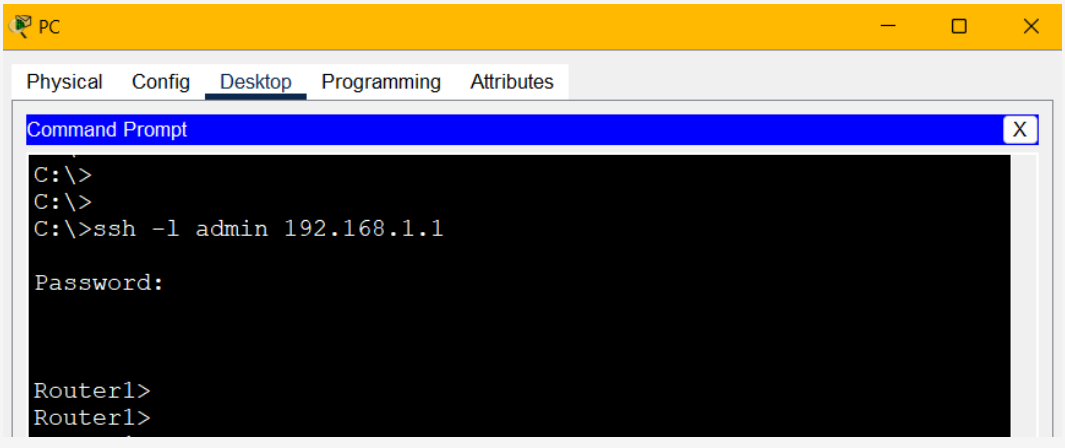
İstemci bilgisayarın komut satırında aşağıdaki komutu çalıştırınız.

```
ssh -l admin 192.168.1.1
```

Parola sorulduğunda aşağıdaki değeri giriniz.

```
Password: 123
```

Giriş başarılı olursa istemci bilgisayarın yönlendiriciye SSH üzerinden erişebildiğini doğrulayınız (Görsel 2.109).



Görsel 2.109: İstemci bilgisayardan yönlendiriciye SSH ile bağlanılması

Not: -l parametresi, SSH bağlantısında kullanılacak kullanıcı adını belirtir. Kullanıcı adı komut içinde tanımlandığı için bağlantı sırasında ayrıca kullanıcı adı sorulmayabilir.

Güvenli Son Durumu Doğrulama

9. Adım: Telnet Bağlantısının Artık Kabul Edilmediğini Kontrol Etmek

SSH yapılandırmasını tamamladıktan sonra istemci bilgisayarda yeniden Telnet bağlantısı kurmayı deneyiniz.

telnet 192.168.1.1

Son yapılandırmada sanal terminal hatlarında yalnızca SSH bağlantısına izin verildiği için Telnet bağlantısının kabul edilmemesi beklenir.

Bu sonucu oluşturan komut aşağıdadır.
transport input ssh

Telnet ve SSH bağlantılarının aynı anda açık bırakılması teknik olarak mümkün olsa da bu uygulamada güvenli son durum olarak yalnızca SSH erişimi tercih edilmektedir.

10. Adım: SSH Yapılandırmasını Kontrol Etmek

Yönlendiricide aşağıdaki komutu çalıştırınız.

Router1# show ip ssh

Kullanılan simülasyon sürümü destekliyorsa SSH sürümünü ve yapılandırma durumunu inceleyiniz.

Sanal terminal hatlarındaki yapılandırmayı görmek amacıyla aşağıdaki komutu da kullanabilirsiniz.

Router1# show running-config

Telnet ve SSH Uzaktan Erişim Uygulaması Gözlem Tablosu

İncelenen Unsur	Gözlemlediğiniz Sonuç
Yönlendiricinin IPv4 adresi	
İstemci bilgisayarın IPv4 adresi	
ping 192.168.1.1 testi başarılı oldu mu?	☐ Evet ☐ Hayır
Telnet bağlantısı ilk yapılandırmada kuruldu mu?	☐ Evet ☐ Hayır
SSH bağlantısı kuruldu mu?	☐ Evet ☐ Hayır
SSH bağlantısında kullanılan kullanıcı adı	
SSH yapılandırmasında kullanılan alan adı	
RSA anahtarı üretildi mi?	☐ Evet ☐ Hayır
Son yapılandırmada Telnet bağlantısı kabul edildi mi?	☐ Evet ☐ Hayır
Güvenli uzaktan yönetim için tercih edilmesi gereken protokol	
Karşılaşılan sorun varsa kısa açıklaması	
Sorunu gidermek için yapılan işlem	

Sonuçları Yorumlamak

Aşağıdaki soruları cevaplayınız.

1. Telnet ve SSH protokollerinin ortak görevi nedir?

.....

.....

.....

.....

2. Gerçek ağ ortamlarında neden Telnet yerine SSH kullanılması daha uygundur?

.....

.....

3. login local komutunun temel işlevi nedir?

.....

.....

4. transport input ssh komutu hangi amacı taşır?

.....

.....

5. RSA anahtarı SSH yapılandırmasında neden gereklidir?

.....

.....

Değerlendirme

Çalışmanız öğretmeniniz tarafından kontrol listesine göre değerlendirilecektir. Çalışmanızı yaparken buradaki ölçütleri dikkate alınız. Kontrol listesi formuna ulaşmak için karekodu okutunuz. Dijital yayınlarda karekodun üstüne tıklayarak içeriğe ulaşabilirsiniz.

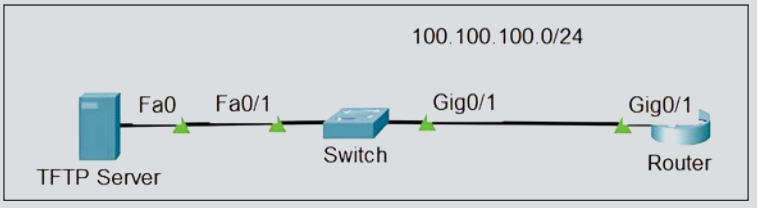
2.3.9. TFTP Protokolü

Basit Dosya Aktarım Protokolü [Trivial File Transfer Protocol (TFTP)], ağ üzerindeki cihazlar arasında temel dosya aktarımı yapılmasını sağlayan uygulama katmanı protokolüdür. TFTP, FTP protokolüne göre daha sınırlı bir yapıya sahiptir. Kullanıcı hesabıyla oturum açma, ayrıntılı yetkilendirme, gelişmiş dosya yönetimi gibi işlevlerden çok dosya gönderme ve alma işlemlerine odaklanır. TFTP genellikle UDP 69 numaralı portla ilişkilidir. Basit yapısı nedeniyle ağ cihazlarının yapılandırma dosyalarının, yedekleme dosyalarının ve desteklenen ortamlarda işletim sistemi dosyalarının aktarılmasında kullanılabilir.

TFTP protokolünün ağ cihazı yönetimi açısından önemli kullanım alanlarından biri yedeklemedir. Bir yönlendiricinin çalışan yapılandırması veya başlangıç yapılandırması TFTP sunucusuna kopyalanabilir. Gerektiğinde daha önce alınan yedek dosya yeniden cihaza aktarılabilir. Böylece yapılandırma hataları, cihaz değişiklikleri veya bakım işlemleri sırasında önceki yapılandırmaya dönülmesi kolaylaşır.

15. UYGULAMA

Uygulama Adı	TFTP ile Dosya Yedekleme ve Geri Yükleme İşlemleri Yapmak
Süre	30 dakika
Amaç	Yönlendiricinin çalışan ve başlangıç yapılandırma dosyalarını TFTP sunucusuna yedeklemek, yedek dosyalarını doğrulamak ve çalışan yapılandırmayı geri yüklemek (Görsel 2.110)
Yönerge	Aşağıdaki adres planını kullanarak yönlendirici ve TFTP sunucusunu aynı yerel ağda yapılandırınız. TFTP sunucusuna erişimi ping komutuyla sınayınız. Yönlendiricinin çalışan ve başlangıç yapılandırma dosyalarını TFTP sunucusuna yedekleyiniz. Yedeklenen dosyaları sunucuda doğrulayınız. Ardından çalışan yapılandırmayı yedekten geri yükleyerek sonucu gözlemleyiniz. Kullanılan cihaz ve simülasyon sürümü destekliyorsa işletim sistemi dosyasını da TFTP sunucusuna yedekleyiniz.
Araç Gereç	Ağ simülasyon programı, bir yönlendirici, bir switch, bir TFTP sunucusu, çalışma yaprağı.



Görsel 2.110: TFTP ile yapılandırma dosyalarını yedekleme topolojisi

Dikkat Edilecek Noktalar

- Yönlendirici ve TFTP sunucusunu aynı yerel ağda yapılandırınız.
- TFTP sunucusuna erişimi ping komutuyla sınayınız.
- Dosya adlarını yönergede verilen biçimde yazınız.
- Yedekleme işleminden sonra dosyaların TFTP sunucusunda göründüğünü doğrulayınız.
- Geri yükleme işleminden önce yönlendirici üzerinde kontrollü bir değişiklik yapınız.
- Yedek dosyayı geri yükledikten sonra değişikliğin geri alındığını doğrulayınız.
- Grup içinde görev paylaşımı yapınız.

Adres Planı

Cihaz veya Arayüz	IPv4 Adresi	Alt Ağ Maskesi	Varsayılan Ağ Geçidi
Yönlendirici G0/1	100.100.100.1	255.255.255.0	–
TFTP sunucusu	100.100.100.2	255.255.255.0	100.100.100.1

A) Yapılandırma Dosyalarını Yedeklemek ve Geri Yüklemek

1. Adım: Topolojiyi Oluşturmak

Ağ simülasyon programında aşağıdaki cihazları çalışma alanına ekleyiniz.

- bir yönlendirici
- bir switch
- bir TFTP sunucusu

Yönlendiricinin G0/1 arayüzünü ve TFTP sunucusunu switche uygun kablolarla bağlayınız.

2. Adım: Yönlendirici Arayüzünü Yapılandırmak

Yönlendiricinin komut satırı arayüzünü açınız. Aşağıdaki komutları giriniz.

Router> enable

Router# configure terminal

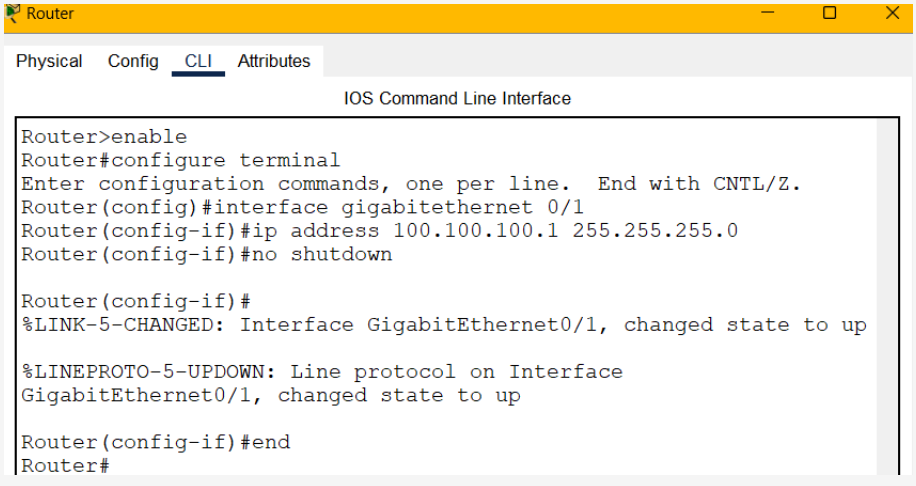
Router(config)# interface gigabitethernet 0/1

Router(config-if)# ip address 100.100.100.1 255.255.255.0

Router(config-if)# no shutdown

Router(config-if)# end

Yönlendiricinin G0/1 arayüzünün IPv4 yapılandırması Görsel 2.111'de gösterilmiştir.



Görsel 2.111: Yönlendiricinin G0/1 arayüzünün IPv4 yapılandırması

3. Adım: TFTP Sunucusunu Yapılandırmak

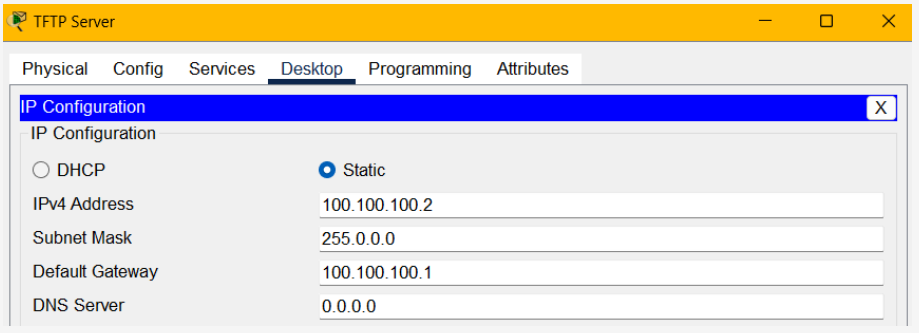
TFTP sunucusunda **Desktop > IP Configuration** bölümünü açınız. Aşağıdaki bilgileri giriniz.

IPv4 Address: 100.100.100.2

Subnet Mask: 255.255.255.0

Default Gateway: 100.100.100.1

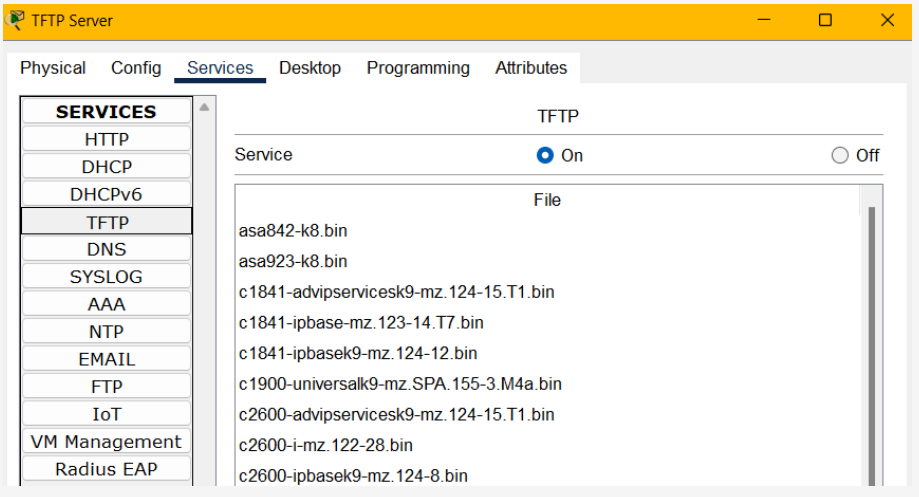
TFTP sunucusunun IPv4 yapılandırması Görsel 2.112'de gösterilmiştir.



Görsel 2.112: TFTP sunucusunun IPv4 yapılandırması

4. Adım: TFTP Hizmetini Etkinleştirmek

TFTP sunucusunda **Services > TFTP** bölümünü açınız. TFTP hizmetinin **On** durumunda olduğunu doğrulayınız (Görsel 2.113).



Görsel 2.113: TFTP sunucusunda dosya aktarım hizmetinin etkinleştirilmesi

5. Adım: TFTP Sunucusuna Erişimi Sınamak

Yönlendiricinin komut satırı arayüzünde aşağıdaki komutu çalıştırınız.

Router# ping 100.100.100.2

Yanıt alındığını doğrulayınız. ping testi başarısız olursa kablo bağlantısını, yönlendirici arayüzünün etkin olup olmadığını, IPv4 adreslerini ve alt ağ maskelerini kontrol ediniz.

6. Adım: Çalışan Yapılandırma Dosyasını Yedeklemek

Yönlendiricide aşağıdaki komutu çalıştırınız.

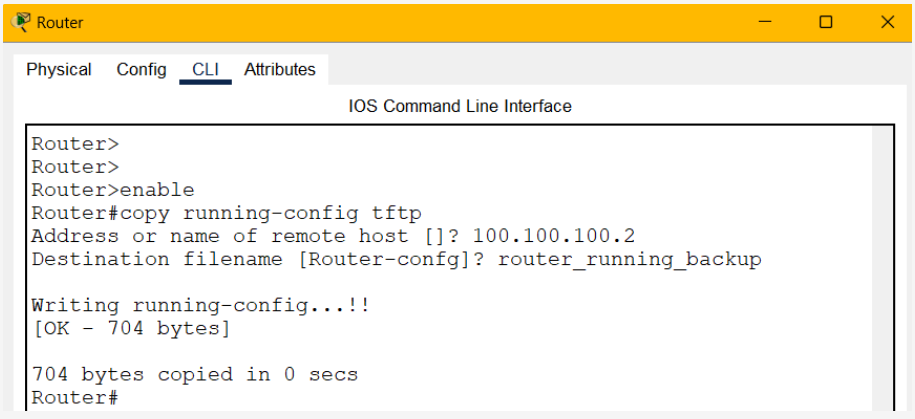
Router# copy running-config tftp

Sistem tarafından istenen alanları aşağıdaki biçimde doldurunuz.

Address or name of remote host? 100.100.100.2

Destination filename? router_running_backup

Bu işlem tamamlandığında yönlendiricinin etkin olarak kullandığı yapılandırma dosyası TFTP sunucusuna kopyalanmış olur (Görsel 2.114).



Görsel 2.114: Çalışan yapılandırma dosyasının TFTP sunucusuna yedeklenmesi

7. Adım: Başlangıç Yapılandırma Dosyasını Yedeklemek

Öncelikle çalışan yapılandırmayı başlangıç yapılandırmasına kaydediniz.

Router# copy running-config startup-config

Ardından başlangıç yapılandırmasını TFTP sunucusuna yedekleyiniz.

Router# copy startup-config tftp

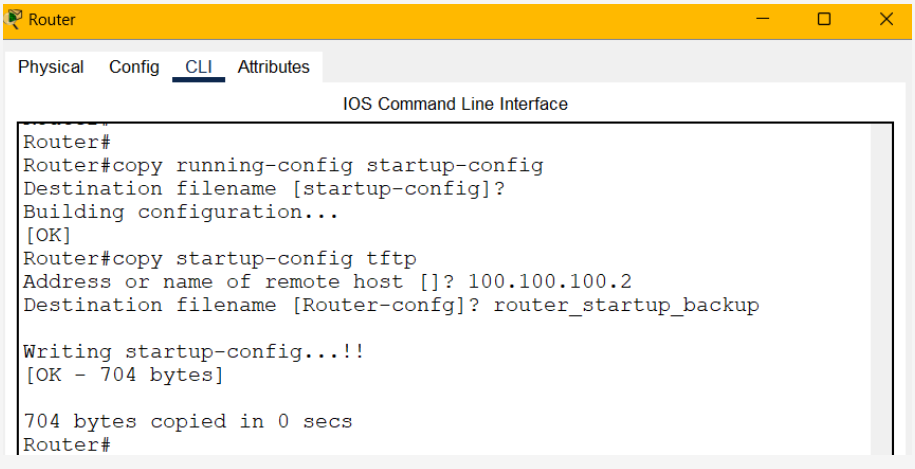
Sistem tarafından istenen alanları aşağıdaki biçimde doldurunuz.

Address or name of remote host? 100.100.100.2

Destination filename? router_startup_backup

Bu işlem tamamlandığında yönlendiricinin başlangıç yapılandırma dosyası TFTP sunucusuna kopyalanmış olur.

Başlangıç yapılandırma dosyasının TFTP sunucusuna yedeklenmesi Görsel 2.115'te gösterilmiştir.



Görsel 2.115: Başlangıç yapılandırma dosyasının TFTP sunucusuna yedeklenmesi

Not: running-config, yönlendiricinin o anda etkin olarak kullandığı yapılandırmadır. startup-config ise cihaz yeniden başlatıldığında kullanılacak başlangıç yapılandırmasıdır.

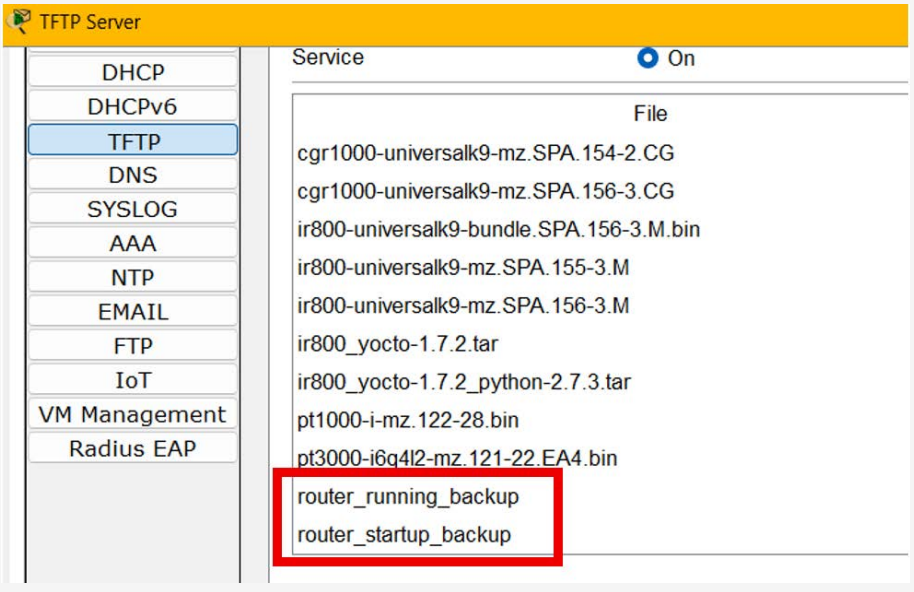
8. Adım: Yedeklenen Dosyaları TFTP Sunucusunda Görüntülemek

TFTP sunucusunda **Services > TFTP** bölümünü açınız. Aşağıdaki dosyaların listede bulunduğunu doğrulayınız.

router_running_backup

router_startup_backup

Yedeklenen yapılandırma dosyalarının tftp sunucusunda görüntülenmesi Görsel 2.116'da gösterilmiştir.



Görsel 2.116: Yedeklenen yapılandırma dosyalarının tftp sunucusunda görüntülenmesi

9. Adım: Yönlendiricinin Adını Geçici Olarak Değiştirmek

Yedekten geri yükleme işleminin sonucunu gözlemleyebilmek amacıyla yönlendiricinin adını geçici olarak değiştiriniz.

Router# configure terminal

Router(config)# hostname DenemeRouter

DenemeRouter(config)# end

Komut satırı isteminin aşağıdaki biçimde değiştiğini gözlemleyiniz.

DenemeRouter#

10. Adım: Çalışan Yapılandırmayı TFTP Sunucusundaki Yedekten Geri Yüklemek

Yönlendiricide aşağıdaki komutu çalıştırınız.

DenemeRouter# copy tftp running-config

Sistem tarafından istenen alanları aşağıdaki biçimde doldurunuz.

Address or name of remote host? 100.100.100.2

Source filename? router_running_backup

Destination filename [running-config]?

Son satırda **Enter** tuşuna basınız.

B) İşletim Sistemi Dosyasını Yedekleme

1. Adım: İşletim Sistemi Dosyasını Belirlemek

Yönlendiricide Flash belleğin içeriğini görüntülemek amacıyla desteklenen komutlardan birini kullanınız.
Router# show flash:
Listede işletim sistemi dosyasını belirleyiniz.

2. Adım: İşletim Sistemi Dosyasını TFTP Sunucusuna Yedeklemek

Kullanılan cihaz ve simülasyon sürümü destekliyorsa aşağıdaki komutu çalıştırınız.
Router# copy flash: tftp:
Sistem tarafından istenen alanlara

- kaynak dosya adını,
- TFTP sunucusunun 100.100.100.2 IPv4 adresini,
- hedef dosya adını giriniz.

3. Adım: Sunucudaki Dosyayı Doğrulamak

TFTP sunucusunda **Services > TFTP** bölümünü açınız. İşletim sistemi dosyasının listede görünüp görünmediğini kontrol ediniz.
TFTP Yedekleme ve Geri Yükleme Uygulaması Gözlem Tablosu

İncelenen Unsur	Gözlemlediğiniz Sonuç
Yönlendiricinin IPv4 adresi	
TFTP sunucusunun IPv4 adresi	
ping 100.100.100.2 testi başarılı oldu mu?	☐ Evet ☐ Hayır
router_running_backup dosyası sunucuda göründü mü?	☐ Evet ☐ Hayır
router_startup_backup dosyası sunucuda göründü mü?	☐ Evet ☐ Hayır
Yönlendiricinin adı geçici olarak DenemeRouter biçiminde değiştirildi mi?	☐ Evet ☐ Hayır
Çalışan yapılandırma TFTP sunucusundaki yedekten geri yüklendi mi?	☐ Evet ☐ Hayır
Geri yükleme sonrasında yönlendirici adı önceki hâline döndü mü?	☐ Evet ☐ Hayır
Kullanılan cihaz ve simülasyon sürümü işletim sistemi dosyasının yedeklenmesini destekliyor mu?	☐ Evet ☐ Hayır
İşletim sistemi dosyası belirlendi mi?	☐ Evet ☐ Hayır ☐ Desteklenmiyor
İşletim sistemi dosyası TFTP sunucusunda görüntülendi mi?	☐ Evet ☐ Hayır ☐ Desteklenmiyor
Karşılaşılan sorun varsa kısa açıklaması	
Sorunu gidermek için yapılan işlem	

Değerlendirme

Çalışmanız öğretmeniniz tarafından kontrol listesine göre değerlendirilecektir. Çalışmanızı yaparken buradaki ölçütleri dikkate alınız. Kontrol listesi formuna ulaşmak için karekodu okutunuz. Dijital yayınlarda karekodun üstüne tıklayarak içeriğe ulaşabilirsiniz.

ÖLÇME VE DEĞERLENDİRME

A) Aşağıdaki yapılandırılmış gridde numaralandırılmış kutucuklarda ağ iletişimiyle ilgili bazı protokoller verilmiştir. Kutucuk numaralarını kullanarak soruların cevaplarını ilgili boşluklara yazınız. Aynı kutucuk numarasını birden fazla cevap için kullanabilirsiniz.

❶ SSH	❷ DHCP	❸ FTP	❹ ICMP
❺ SMTP	❻ HDLC	❼ HTTPS	❽ ARP
❾ TFTP	❿ TCP	⓫ POP3	⓬ DNS
⓭ UDP	⓮ PPP	⓯ HTTP	⓰ Telnet

1. İstemcilere otomatik IP yapılandırması sağlanması ve alan adlarının IP adresleriyle ilişkilendirilmesi süreçlerinde kullanılan protokoller hangileridir?

   Cevap: .....

2. IPv4 adresi ile MAC adresi arasında eşleştirme yapılması ve ağdaki erişilebilirliğin sınanması süreçleriyle ilişkili protokoller hangileridir?

   Cevap: .....

3. Taşıma katmanında bağlantı odaklı ve güvenilir veri iletimini sağlayan protokol ile önceden bağlantı kurmadan çalışan protokol hangileridir?

   Cevap: .....

4. E-postaların gönderilmesi ve posta sunucusunda bulunan mesajların istemci cihaza alınması süreçleriyle ilişkili protokoller hangileridir?

   Cevap: .....

5. Ağ cihazlarına uzaktan erişimde kullanılan; temel kullanımda güvenli olmayan protokol ile güvenli erişim sağlayan protokol hangileridir?

   Cevap: .....

6. Dosya aktarımı ve ağ cihazlarının yapılandırma dosyalarının temel düzeyde yedeklenmesi süreçlerinde kullanılabilen protokoller hangileridir?

   Cevap: .....

7. Web sayfalarına erişim ve bağlantının TLS ile korunarak gerçekleştirilmesi süreçlerinde kullanılan protokoller hangileridir?

   Cevap: .....

8. Noktadan noktaya bağlantılarda kullanılabilen veri bağı katmanı protokolleri hangileridir?

Cevap: .....

9. Güvenli uzaktan yönetim veya TLS ile korunan web erişimi sağlamak amacıyla kullanılabilen protokoller hangileridir?

Cevap: .....

10. Gerçek zamanlı ses aktarımında düşük gecikme öncelikli olduğunda tercih edilebilecek taşıma katmanı protokolü hangisidir?

Cevap: .....

11. Dosyanın eksiksiz ve doğru sırada iletilmesinin öncelikli olduğu bir aktarım işleminde tercih edilebilecek taşıma katmanı protokolü hangisidir?

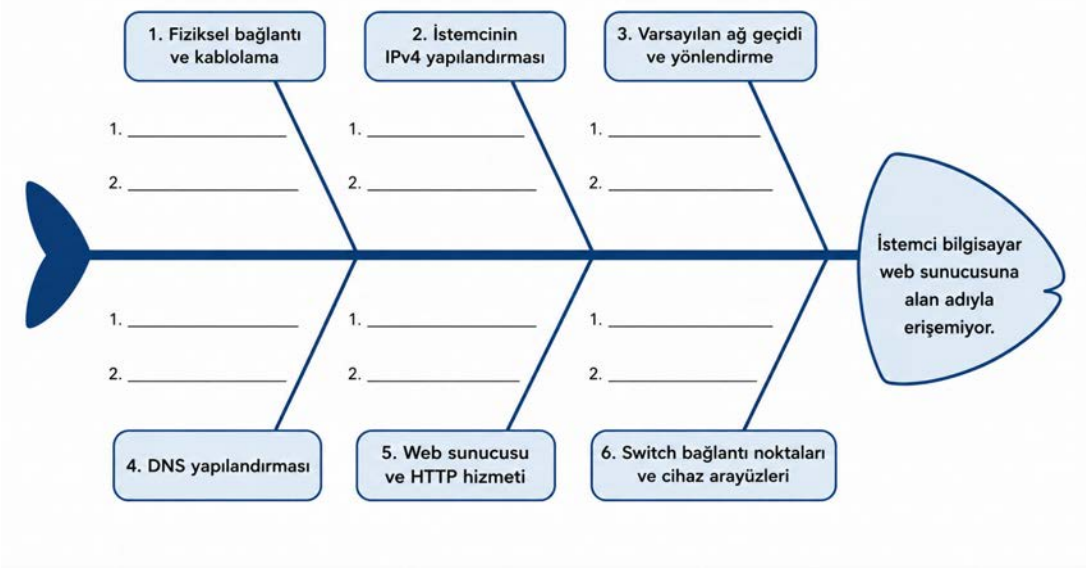
Cevap: .....

B) Aşağıdaki durumu inceleyiniz ve soruna yol açabilecek nedenleri ilgili alanlara yazınız.

Bir istemci bilgisayar, tarayıcı üzerinden aşağıdaki web sayfasına erişememektedir:

http://www.siber.test

Diyagramdaki ana kılçıklarda sorunun inceleneceği alanlar yer almaktadır. Her ana kılçık için soruna yol açabilecek en az iki alt neden yazınız.



C) Aşağıdaki soruların doğru cevabını işaretleyiniz.

1. **Aynı şehir içinde bulunan farklı okul binalarındaki yerel ağların birbirine bağlanmasıyla oluşan yapı aşağıdakilerden hangisidir?**

A) LAN B) MAN C) VPN

D) PAN E) VLAN

2. Bir bilgisayar laboratuvarında bütün istemciler merkezde bulunan bir switche bağlanmıştır. Bir istemcinin kablosunda oluşan arıza diğer istemcilerin çalışmasını doğrudan etkilememektedir.

Belirtilen yapı aşağıdaki topolojilerden hangisidir?

A) Halka B) Veri yolu C) Yıldız

D) Örgü E) Noktadan noktaya

3. **Kapsülleme sırasında yerel ağda iletim için MAC adreslerinin ve hata kontrolü bilgilerinin eklendiği OSI katmanı aşağıdakilerden hangisidir?**

A) Uygulama katmanı B) Taşıma katmanı

C) Ağ katmanı D) Veri bağı katmanı

E) Fiziksel katman

4. **Kapsülleme sürecinde protokol veri birimlerinin genel sıralaması aşağıdakilerden hangisidir?**

A) Veri → paket → bit → çerçeve → segment

B) Veri → segment veya datagram → paket → çerçeve → bit

C) Bit → veri → segment → çerçeve → paket

D) Paket → veri → çerçeve → bit → segment

E) Veri → çerçeve → segment → paket → bit

5. **TCP bağlantısının kurulmasında kullanılan üç yollu el sıkışma sürecinin doğru sıralaması aşağıdakilerden hangisidir?**

A) ACK → SYN → SYN + ACK
B) SYN + ACK → ACK → SYN
C) SYN → SYN + ACK → ACK
D) SYN → ACK → SYN + ACK
E) ACK → SYN + ACK → SYN

6. **Gerçek zamanlı ses aktarımında düşük gecikmenin, ayrıntılı teslim denetiminden daha öncelikli olduğu bir durumda hangi taşıma katmanı protokolü tercih edilebilir?**

A) ARP
B) TCP
C) ICMP
D) UDP
E) DNS

7. **192.168.10.25/24 ve 192.168.10.80/24 adreslerine sahip iki bilgisayarın iletişimiyle ilgili aşağıdaki ifadelerden hangisi doğrudur?**

A) Cihazlar farklı ağlardadır ve mutlaka yönlendirici kullanmalıdır.
B) Cihazlar aynı ağdadır ve yerel ağ içinde doğrudan iletişim kurabilir.
C) Cihazlardan biri APIPA adresi kullanmaktadır.
D) Cihazlar yalnızca DNS sunucusu üzerinden iletişim kurabilir.
E) Cihazların iletişim kurabilmesi için IPv6 adresi tanımlanmalıdır.

8. **Bir istemcide 169.254.18.42 IPv4 adresinin görülmesi aşağıdaki durumlardan hangisiyle ilişkilidir?**

A) İstemcinin DHCP üzerinden uygun IPv4 adresi alamaması
B) İstemcinin loopback testi gerçekleştirmesi
C) İstemcinin genel IPv4 adresi kullanması
D) DNS çözümlemesinin başarıyla tamamlanması
E) Yönlendiricinin IPv6 yönlendirmeyi etkinleştirmesi

9. Bir cihazın kendi TCP/IP iletişim yapısını fiziksel ağa çıkmadan sınamak amacıyla yaygın olarak kullanılan IPv4 adresi aşağıdakilerden hangisidir?

A) 0.0.0.0 B) 10.0.0.1 C) 127.0.0.1

D) 169.254.1.1 E) 255.255.255.255

10. /27 ön ek uzunluğuna sahip bir IPv4 alt ağında kullanılabilecek cihaz adresi sayısı kaçtır?

A) 14 B) 16 C) 28

D) 30 E) 32

11. Elli (50) istemciye IPv4 adresi verilmesi gereken bir ağ için kullanılabilecek <u>en küçük</u> uygun ön ek uzunluğu aşağıdakilerden hangisidir?

A) /28 B) /27 C) /26

D) /25 E) /24

12. Aşağıdaki IPv6 adreslerinden hangisi 2001:0db8:0000:0000:0000:0000:0000:0042 adresinin doğru sadeleştirilmiş biçimidir?

A) 2001:db8:0:42 B) 2001:db8::42

C) 2001::db8::42 D) 2001:db8:42::

E) 2001:0db8::0000:0042::

13. Aynı IPv6 adresinin birden fazla arayüze atanabildiği ve paketin yönlendirme ölçütlerine göre uygun arayüzlerden birine ulaştırıldığı adres türü aşağıdakilerden hangisidir?

A) Broadcast B) Loopback C) Multicast

D) Link-local E) Anycast

14. ping komutuyla gerçekleştirilen temel erişim testinde aşağıdaki protokollerden hangisi kullanılır?

A) DHCP B) ICMP C) FTP

D) SMTP E) TFTP

15. **Bir ARP Request mesajı Ethernet ağında yayımlanırken kullanılan hedef MAC adresi aşağıdakilerden hangisidir?**

A) 00:00:00:00:00:00
B) 11:11:11:11:11:11
C) ff:ff:ff:ff:ff:ff
D) aa:aa:aa:aa:aa:aa
E) 127:0:0:1

16. **Bükümlü çift Ethernet kablosunun bir ucunda T568A, diğer ucunda T568B standardının kullanılmasıyla oluşan kablo türü aşağıdakilerden hangisidir?**

A) Çapraz kablo
B) Koaksiyel kablo
C) Fiber optik kablo
D) Seri kablo
E) Konsol kablosu

17. **DHCPv4 adres edinme sürecinin doğru sıralaması aşağıdakilerden hangisidir?**

A) Offer → Discover → Acknowledgment → Request
B) Request → Offer → Discover → Acknowledgment
C) Acknowledgment → Request → Discover → Offer
D) Discover → Offer → Request → Acknowledgment
E) Discover → Request → Offer → Acknowledgment

18. **HTTP iletişiminin TLS ile korunmuş biçimi aşağıdakilerden hangisidir?**

A) FTP
B) DNS
C) HTTPS
D) SSH
E) POP3

19. **E-postaların gönderilmesi ve posta sunucusundaki mesajların istemciye alınmasıyla ilişkili protokoller sırasıyla aşağıdakilerden hangisidir?**

A) SMTP ve POP3
B) HTTP ve DNS
C) FTP ve TFTP
D) DNS ve DHCP
E) HTTP ve HTTPS

Ç) Senaryo temelli soruların cevaplarını ayrılan alanlara yazınız.

1-3. soruları aşağıdaki senaryoya göre cevaplayınız.

Bir okulun bilişim teknolojileri laboratuvarında istemciler 192.168.10.0/24 ağında bulunmaktadır. DNS sunucusu 192.168.20.2, web sunucusu ise 192.168.30.2 IPv4 adresiyle yapılandırılmıştır. Yönlendiricinin ilgili arayüzleri aşağıdaki adreslere sahiptir.

Yönlendirici Arayüzü	IPv4 Adresi
G0/0	192.168.10.1/24
G0/1	192.168.20.1/24
G0/2	192.168.30.1/24

DNS sunucusunda aşağıdaki A kaydı oluşturulmuştur.

www.siber.test → 192.168.30.2

Laboratuvarda üç farklı durum gözlemlenmiştir.

- Birinci bilgisayar otomatik IPv4 adresi alamamış ve 169.254.18.42 adresini kullanmaya başlamıştır.
- İkinci bilgisayar 192.168.30.2 adresindeki web sunucusuna ping komutuyla erişebilmekte ancak tarayıcı üzerinden http://www.siber.test adresini açamamaktadır.
- Ağ yöneticisi, yönlendiriciyi laboratuvar dışındaki yetkili bir bilgisayardan güvenli biçimde yönetmek istemektedir.

1. Birinci bilgisayarda görülen 169.254.18.42 adresi hangi kavramla ilişkilidir? Bu durumun giderilmesi için hangi kontroller yapılmalıdır?

.....
.....
.....

2. İkinci bilgisayar web sunucusuna IPv4 adresiyle erişebildiği hâlde www.siber.test alan adıyla erişememektedir. Sorunun olası nedenlerini ve kontrol edilmesi gereken yapılandırmaları yazınız.

.....
.....
.....

3. Ağ yöneticisinin yönlendiriciye uzaktan erişimi için Telnet mi yoksa SSH mı kullanması daha uygundur? Cevabınızı güvenlik açısından gerekçelendiriniz.

.....
.....
.....

4-6. soruları aşağıdaki senaryoya göre cevaplayınız.

Yeni açılan bir mesleki ve teknik Anadolu lisesinde aşağıdaki birimler için IPv4 adresleme planı hazırlanacaktır.

Birim	Cihaz Gereksinimi
Birinci bilgisayar laboratuvarı	90
İkinci bilgisayar laboratuvarı	45
İdari birimler	20
Güvenlik sistemi	10

Kullanılacak ana ağ aşağıda verilmiştir.

192.168.50.0/24

4. Her birim için ihtiyacı karşılayan en küçük uygun ön ek uzunluğunu ve alt ağ maskesini yazınız.

Birim	Cihaz Gereksinimi	Ön Ek Uzunluğu	Alt Ağ Maskesi
Birinci bilgisayar laboratuvarı	90		
İkinci bilgisayar laboratuvarı	45		
İdari birimler	20		
Güvenlik sistemi	10		

5. VLSM planlama tablosunu tamamlayınız.

Birim	Verilen Ağ	İlk Kullanılabilir Adres	Son Kullanılabilir Adres	Yayın Adresi
Birinci bilgisayar laboratuvarı				
İkinci bilgisayar laboratuvarı				
İdari birimler				
Güvenlik sistemi				

6. VLSM kullanılmasının eşit büyüklükte alt ağlar oluşturmaya göre sağlayacağı temel avantajı açıklayınız. Planlama sonunda kullanılmadan kalan adres bloğunu yazınız.

.....
.....
.....
.....

D) Aşağıdaki tanımların önündeki harfleri, ait olduğu kavramın yanındaki parantezin içine yazarak eşleştiriniz.

Kavram	Tanım
1. ( ) Switch	**A)** Aynı yerel ağdaki Ethernet çerçevelerini hedef MAC adresine göre uygun bağlantı noktasına ileten cihazdır.
2. ( ) Router	**B)** Farklı ağlar arasında paket iletimi gerçekleştiren ve hedef IP adresine göre uygun yolu belirleyen cihazdır.
3. ( ) PoE	**C)** Ethernet kablosu üzerinden veriyle birlikte elektrik enerjisinin taşınmasını sağlayan yapıdır.
4. ( ) RJ45	**Ç)** Bükümlü çift Ethernet kablolarında yaygın olarak kullanılan modüler konnektördür.
5. ( ) Ethernet	**D)** Kablolu yerel ağ iletişiminde yaygın olarak kullanılan veri bağı katmanı teknolojisidir.
6. ( ) HDLC	**E)** Seri bağlantılarda kullanılabilen veri bağı katmanı protokollerinden biridir.
7. ( ) PPP	**F)** Noktadan noktaya bağlantılarda kullanılan veri bağı katmanı protokollerinden biridir.
8. ( ) DHCPACK	**G)** DHCP sunucusunun istemciye önerilen yapılandırmayı kullanabileceğini bildirdiği onay mesajıdır.
9. ( ) DNS A kaydı	**Ğ)** Bir alan adını IPv4 adresiyle eşleştiren DNS kaydıdır.
10. ( ) FTP	**H)** Kullanıcı hesabı ve yetkiler doğrultusunda dosya listeleme, indirme veya yükleme işlemlerinin yapılmasını sağlayan protokoldür.
11. ( ) POP3	**I)** Posta sunucusunda bulunan e-postaların istemci tarafından alınmasıyla ilişkili protokoldür.
12. ( ) TFTP	**J)** Temel dosya aktarımı ve ağ cihazı yapılandırma yedekleri için kullanılabilen sade yapılı protokoldür.
13. ( ) startup-config	**K)** Ağ cihazının yeniden başlatıldığında kullanacağı başlangıç yapılandırma dosyasıdır.
14. ( ) SMTP	**L)** E-postaların gönderilmesi ve posta sunucuları arasında iletilmesiyle ilişkili protokoldür.

3. ÖĞRENME BİRİMİ

İŞLETİM SİSTEMLERİ











KONULAR

3.1. MASAÜSTÜ VE MOBİL İŞLETİM SİSTEMLERİ

3.2. SUNUCU İŞLETİM SİSTEMLERİ

ANAHTAR KAVRAMLAR

- açık kaynak kodlu işletim sistemi
- açılış süreci
- betik
- çekirdek
- dağıtım
- dizin yapısı
- dosya sistemi
- güvenlik testi
- işletim sistemi
- istemci
- kabuk
- kapalı kaynak kodlu işletim sistemi
- komut satırı
- kullanıcı yönetimi
- önyükleyici
- PowerShell
- servis
- sunucu
- süreç yönetimi
- terminal
- yetkilendirme

Bu öğrenme biriminde sizden

- istemci-sunucu mimarisini ve işletim sistemi türlerini tanıyarak aralarındaki farkları açıklamanız
- açık kaynak kodlu işletim sistemini kurmanız, dizin yapısını ve dosya sistemini kavramanız, terminal komutlarını ve metin editörlerini kullanarak temel sistem yönetimi işlemleri gerçekleştirmeniz ve betik dosyaları oluşturmanız
- kapalı kaynak kodlu işletim sistemini kurmanız, komut satırı (cmd) ve PowerShell ortamlarında komutlar çalıştırmanız, betik dosyaları oluşturmanız ve sistem yönetim araçlarını kullanarak sistemi izleyip raporlamanız
- sunucu işletim sistemi kurarak servis yapılandırması yapmanız, veri güvenliği adımlarını uygulamanız ve güvenlik testi gerçekleştirmeniz

beklenmektedir.

HAZIRLIK ÇALIŞMASI

1. **Aşağıda farklı dijital cihazların kullanımına ilişkin bir görsel verilmiştir. Görseli inceleyiniz.**



Verilen görselden hareketle aşağıdaki soruları cevaplayınız.

a) Soldaki öğrenci, evdeki bilgisayarda dosya klasörlerini kolayca düzenleyebildiğini ancak telefonunda aynı klasör yapısını bulamadığını söylüyor. Bu farklılığı nasıl açıklarsınız?

_____

_____

b) Görseldeki tableti olan öğrenci, bazı uygulamaların tabletinde çalıştığını ancak bilgisayarında çalışmadığını söylüyor. Bir uygulama, tabletinizde çalışırken neden bilgisayarınızda çalışmayabilir? Açıklayınız.

_____

_____

2. **Bir bilgisayar, tablet veya telefon açıldığında ekranın gelmesi, donanımların çalışması, uygulamaların açılması ve dosyaların saklanması için arka planda nelerin gerçekleştiğine dair düşüncelerinizi açıklayınız.**

_____

_____

BAŞLARKEN

Uzaktan çalışan bir yazılımcı, sabah bilgisayarını açarak kod editörünü ve çevrim içi toplantı uygulamasını kullanmakta, geliştirdiği uygulamanın çalıştığı sunucuyu takip etmektedir. Bir siber güvenlik uzmanı; ağ trafiğini izlemek, güvenlik uyarılarını incelemek ve sistemlerdeki olası açıkları değerlendirmek için farklı yazılımlardan yararlanmaktadır. Bir öğretmen derste bilgisayarını ya da akıllı tahtayı açarak sunumunu başlatmakta, gerektiğinde tabletinden ders notlarına erişmektedir. Bir üniversite öğrencisi öğleden sonra kütüphanedeki masaüstü bilgisayardan araştırma yapmakta ve tabletinde dijital kaynaklarını incelemektedir. Bir e-spor oyuncusu antrenman ya da turnuva sırasında bilgisayarını, kulaklığını, klavyesini ve internet bağlantısını uyumlu biçimde kullanmaktadır. Uygulamaların, dijital hizmetlerin ve çevrim içi platformların bağlı olduğu sunucular ise farklı yerlerde 7/24 çalışmaya devam etmektedir. Bu cihazların donanımları birbirinden farklıdır ancak hepsinin güç düğmesine bastığınızda arka planda sessizce devreye giren ve tüm parçaların birlikte çalışmasını sağlayan ortak bir yazılım katmanı vardır. Bu katman olmadan cihaz, dünyanın en iyi donanımına sahip olsa bile kullanılamaz. Kullanıcıyı karşılayan tek şey siyah bir ekran ve bir hata mesajı olur.

Tüm müzisyenlerin ve enstrümanların hazır olduğu yetenekli bir orkestra, onu yöneten bir şef olmadığı zaman işini doğru yapamaz. İşletim sistemi de orkestra şefi gibidir, donanımların doğru ve zamanında çalışmasını sağlar.

3.1. MASAÜSTÜ VE MOBİL İŞLETİM SİSTEMLERİ

Güç düğmesine basılan bir bilgisayar kısa süre içinde ekranını açar, bileşenlerini devreye alır ve kullanıcıya hazır bir çalışma ortamı sunar. Bu süreç olağan görünse de arka planda onlarca işlem art arda gerçekleşir. İlk olarak donanım bileşenleri kontrol edilir, ardından depolama birimindeki işletim sistemi bulunarak belleğe yüklenir, sürücüler başlatılır ve çalışma ortamı hazırlanır. Bir bilgisayarın açılışından kapanışına kadar tüm bu koordinasyonu üstlenen yazılıma **işletim sistemi** denir.

İşletim sistemi; donanım, kullanıcılar ve uygulamalar arasında köprü görevi gören temel sistem yazılımıdır. Bilgisayar açıldığı andan kapanana kadar arka planda çalışır; donanım kaynaklarını yönetir, uygulamaların bu kaynaklara erişimini düzenler ve kullanıcının sistemle etkileşim kurmasına zemin hazırlar. İşletim sistemi iki temel bileşenden oluşur:

- **Çekirdek (Kernel):** Donanımla doğrudan iletişim kuran en alt katmandır. Bellek yönetimi, süreç yönetimi, donanım sürücüleriyle iletişim gibi temel görevleri yerine getirir. Kullanıcı uygulamaları çekirdeğe doğrudan erişemez, bu katman her zaman korumalı biçimde çalışır.
- **Kabuk (Shell):** Kullanıcının işletim sistemiyle iletişim kurduğu katmandır. Grafiksel kullanıcı arayüzü (masaüstü ortamı) veya metin tabanlı komut satırı biçiminde olabilir.

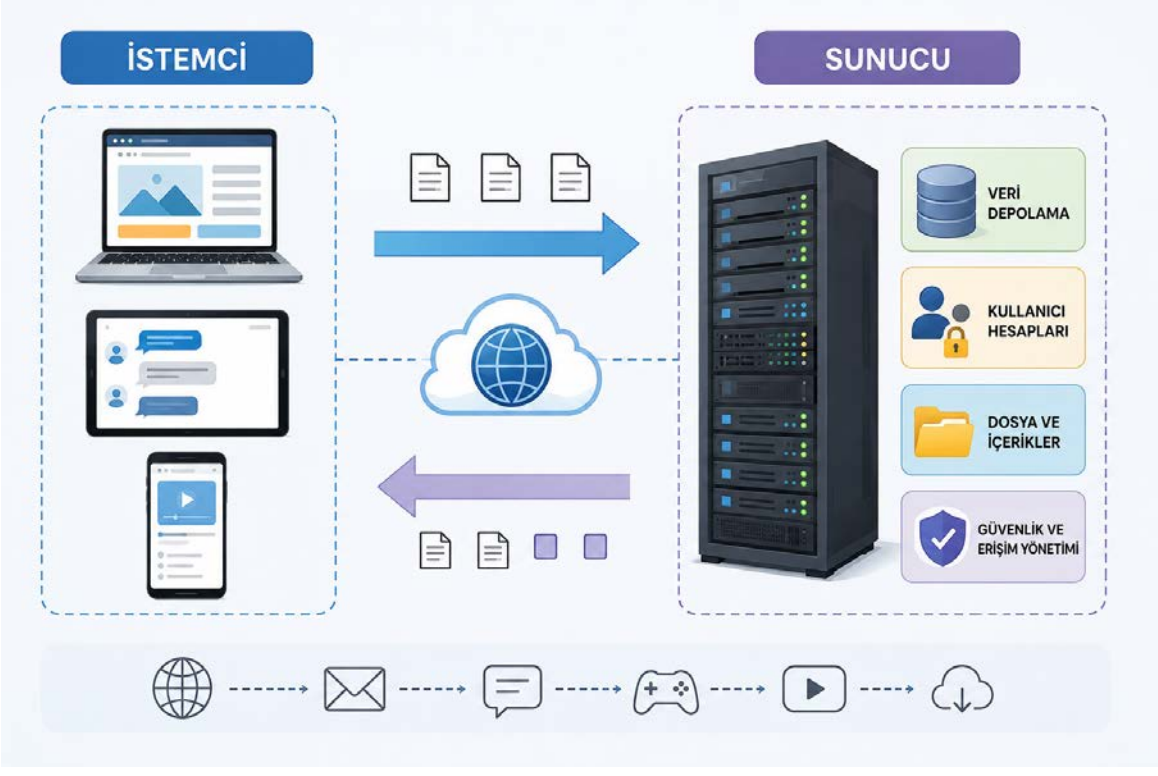
İşletim sisteminin yerine getirdiği bazı önemli görevler Tablo 3.1'de özetlenmiştir.

Tablo 3.1: İşletim Sisteminin Temel Görevleri

Görev	Açıklama
Süreç yönetimi	Çalışan uygulamaları izler, işlemci zamanını uygulamalar arasında paylaştırır.
Bellek yönetimi	Her uygulamaya RAM'de ayrı bir alan ayırır, uygulamaların birbirinin verilerine yetkisiz erişimini engeller.
Depolama yönetimi	Dosyaların oluşturulmasını, silinmesini ve düzenlenmesini yönetir.
Aygıt yönetimi	Klavye, ekran, ağ kartı gibi donanımlarla iletişimi sürücüler aracılığıyla kurar.
Güvenlik ve erişim denetimi	Kullanıcı kimlik doğrulamasını yapar, hangi kullanıcının neye erişebileceğini belirler.

3.1.1. İstemci-Sunucu

Günlük hayatta birçok dijital hizmeti tek bir cihaz **tek başına** yürütmez. Örneğin bir video izlerken, mesajlaşırken veya çevrim içi bir oyuna bağlanırken; telefonunuz veya bilgisayarınız ekranda gördüğünüz içeriği gösterir, komutlarınızı gönderir ve gelen sonuçları size sunar. Asıl içerik, veri ve hizmet ise çoğu zaman farklı bir bilgisayarda tutulur ve yönetilir. Bu iş bölümüne dayalı çalışma biçimi istemci-sunucu (client-server) yaklaşımı olarak adlandırılır (Görsel 3.1). Bu yaklaşım sayesinde veriler merkezde saklanır ve kullanıcılar farklı cihazlardan aynı hizmete erişebilir.



Görsel 3.1: İstemci-Sunucu çalışma mantığı

İstemci (Client): İstemci, bir hizmeti kullanan taraftır. Kullanıcıdan aldığı tıklama, arama, giriş yapma gibi komutları sunucuya iletir ve sunucudan gelen yanıtı kullanıcıya gösterir. Bilgisayar, tablet veya telefon istemci olabilir. Örneğin bir web tarayıcısı, bir e-posta uygulaması veya çevrim içi oyun uygulaması istemci olarak çalışır.

Sunucu (Server): Sunucu, bir hizmeti sunan taraftır. İstemcilerden gelen istekleri alır, gerekli işlemleri yapar ve sonucu geri gönderir. Sunucular genellikle çok sayıda kullanıcıya aynı anda hizmet verebilmek için sürekli çalışır. Web sitelerinin sayfaları, kullanıcı hesap bilgileri, dosyalar veya oyun verileri çoğunlukla sunucularda saklanır ve yönetilir. Bu nedenle sunucularda erişim izinleri ve güvenlik ayarları daha kritik hâle gelir.

Günlük hayattaki bazı istemci–sunucu örnekleri şunlardır:

Mesajlaşma: Telefon mesajı gönderir, sunucu mesajı ilgili kişiye iletir.

Okul / Kurum Sistemi: Öğrenci not görüntüler, sunucu not verisini tutar ve kullanıcının yetkisine göre yalnızca erişmesine izin verilen bilgileri gösterir.

Çevrim içi oyun: İstemci oyuncunun hareketlerini sunucuya gönderir, sunucu oyundaki herkesin durumunu hesaplayarak her oyuncunun ekranını günceller.

Bulut depolama: İstemci dosyayı yükler veya indirir, sunucu dosyayı saklar ve senkronize eder.

3.1.2. İşletim Sistemi Türleri

İşletim sistemleri, kullanıldıkları cihaza ve üstlendikleri role göre farklı biçimlerde tasarlanır. Bir akıllı telefonun işletim sistemiyle bir web sunucusunun işletim sistemi aynı temel görevleri yerine getirse de donanım özellikleri, kullanım biçimi ve güvenlik gereksinimleri açısından birbirinden belirgin biçimde ayrışır. İşletim sistemleri genel olarak masaüstü, mobil ve sunucu işletim sistemleri olmak üzere üç ana türde ele alınır (Tablo 3.2).

Tablo 3.2: İşletim Sistemi Türleri ve Özellikleri

Tür	Kullanıldığı Cihazlar	Temel Özellikler
Masaüstü	• Masaüstü bilgisayarlar • Dizüstü bilgisayarlar	• Grafiksel arayüz • Çok görevli çalışma • Geniş uygulama desteği
Mobil	• Akıllı telefon • Tablet	• Dokunmatik arayüz • Düşük güç tüketimi • Uygulama mağazası ekosistemi
Sunucu	• Sunucular • Veri merkezleri	• Yüksek kararlılık • Çok kullanıcılı erişim • Servis yönetimi • Güvenlik odaklı yapı

Bu üç tür (Görsel 3.2) arasındaki en belirgin fark, kullanım amacında gizlidir. Masaüstü işletim sistemleri bireysel kullanıcıya odaklanır; kullanıcı dostu bir arayüz ve geniş uygulama desteği sunar. Mobil işletim sistemleri pil ömrü ve dokunmatik kullanım için optimize edilmiştir. Sunucu işletim sistemleriyse grafiksel arayüz yerine komut satırını ön plana çıkarır. Kaynak verimliliği, kesintisiz çalışma ve çok sayıda kullanıcıya eş zamanlı hizmet verebilme bu sistemlerin önceliklerdir.



Görsel 3.2: İşletim sistemi türleri

3.1.3. Mobil İşletim Sistemleri

Bugün en yaygın kullanılan bilişim araçları büyük ölçüde akıllı telefonlar ve tabletlerdir. Bu cihazların temelinde, masaüstü sistemlerin aksine taşınabilirlik, dokunmatik kullanım ve düşük güç tüketimi gözetilerek tasarlanmış özel işletim sistemleri bulunur. Mobil işletim sistemi; dokunmatik ekranlarla kullanıma uygun arayüz, sınırlı pil kapasitesini verimli kullanan güç yönetimi, kablosuz ağlar üzerinden sürekli bağlantı gibi temel önceliklere göre geliştirilmiştir. Bugün bu alanda iki sistem öne çıkmaktadır: Açık kaynak kodlu mobil işletim sistemi ve kapalı kaynak kodlu mobil işletim sistemi (Tablo 3.3).

Tablo 3.3: Açık Kaynak Kodlu ve Kapalı Kaynak Kodlu Mobil İşletim Sistemi Karşılaştırması

Özellik	Açık Kaynak Kodlu Mobil İşletim Sistemi	Kapalı Kaynak Kodlu Mobil İşletim Sistemi
Çekirdek	Linux tabanlı çekirdek yapısı	Unix tabanlı çekirdek yapısından türeyen kapalı sistem mimarisi
Uygulama mağazası	Geliştiriciye ait resmî uygulama mağazası	Geliştiriciye ait resmî uygulama mağazası
Üçüncü taraf uygulama	Belirli ayarlar yapılırsa destekleyebilir.	Varsayılan olarak desteklemez veya sınırlandırır.
Özelleştirme	Yüksek	Sınırlı
Güncelleme dağıtımı	Cihaz üreticisi veya hizmet sağlayıcıya bağlı	Geliştirici tarafından doğrudan

- **Açık Kaynak Kodlu Mobil İşletim Sistemi:** Linux çekirdeği üzerine inşa edilmiş açık kaynaklı bir mobil işletim sistemidir. Akıllı telefon pazarında en geniş kullanıcı tabanına sahip olan sistem, açık kaynak yapısı sayesinde farklı üreticiler tarafından kendi cihazlarına uyarlanabilmektedir. Uygulamalar resmî uygulama mağazası üzerinden dağıtılır ancak güvenlik denetimi dışındaki kaynaklardan da uygulama yüklenebilir. Bu esneklik beraberinde güvenlik risklerini de getirir.
- **Kapalı Kaynak Kodlu Mobil İşletim Sistemi:** Yalnızca belirli bir üreticinin cihazlarında çalışmak üzere geliştirilmiş kapalı kaynaklı bir mobil işletim sistemidir. Donanım ve yazılım aynı üretici tarafından kontrol edildiğinden bütünleşik bir kullanıcı deneyimi sunar. Uygulamalar yalnızca kendi resmî uygulama mağazası üzerinden dağıtılır ve sıkı inceleme sürecinden geçer. Bu yapı güvenliği artırır ancak kullanıcıya daha az özelleştirme özgürlüğü tanır.

BİLGİ KUTUSU : Unix ve Linux Çekirdek Sistemleri

Unix, 1970'lerin başında geliştirilen ve kararlılığıyla öne çıkan bir işletim sistemi ailesidir. Bugün hâlâ pek çok modern sistemin tasarımına ilham kaynağı olmaya devam etmektedir. Linux ise Unix'ten esinlenerek sıfırdan yazılmış, açık kaynaklı bir çekirdektir. Sunuculardan süper bilgisayarlara, akıllı televizyonlardan açık kaynak kodlu mobil işletim sistemli telefonlara kadar pek çok farklı cihazda kullanılmaktadır.

Yaygın kullanılan açık kaynak kodlu mobil işletim sistemlerinde Linux tabanlı çekirdek yapısı öne çıkarken, kapalı kaynak kodlu bazı mobil işletim sistemlerinde Unix benzeri Darwin tabanlı çekirdek yapısı kullanılmaktadır. İkisi de güçlü ve güvenilir sistemler olmakla birlikte farklı mimariler üzerine kurulmuştur. Bu fark, günlük kullanımda doğrudan hissedilmez ancak sistemlerin güvenlik yapısı ve kararlılığı büyük ölçüde bu temele dayanır.

Mobil cihazlar sınırlı pil kapasitesiyle çalıştığı için işletim sistemi güç yönetimini kritik bir öncelik olarak ele alır. Arka planda çalışan uygulamaları denetler, ekran parlaklığını otomatik ayarlar ve kullanılmayan bağlantı birimlerini (Wi-Fi, Bluetooth ve GPS) gerektiğinde devre dışı bırakabilir. Böylece pil ömrü uzatılırken sistem performansı da korunur.

Her iki işletim sistemi de uygulamaların kamera, mikrofon, konum, rehber gibi hassas verilere erişimini izin sistemiyle denetler. Kullanıcı, hangi uygulamanın hangi veriye erişeceğini ayrı ayrı onaylar veya reddeder. Bu sistem, kullanıcı gizliliğini koruyan temel güvenlik katmanlarından biridir.

SİBER GÜVENLİK PENCERESİ

Mobil cihazlar, taşınabilir yapıları ve sürekli ağa bağlı kalmaları nedeniyle siber saldırılar için cazip hedeflerdir. Dikkat edilmesi gereken başlıca tehditler şunlardır:

- **Gereksiz izin isteyen uygulamalar:** Bir el feneri uygulamasının rehbere veya konuma erişim istemesi, kişisel verilerin toplanabileceğinin işaretidir.
- **Resmî olmayan kaynaklardan uygulama yükleme:** Özellikle açık kaynak kodlu mobil işletim sistemli cihazlarda resmi mağaza dışından yüklenen uygulamalar kötü amaçlı yazılım barındırabilir.
- **Sistem kilidi kırma (Jailbreak ve root işlemleri):** Sistemin güvenlik katmanlarını devre dışı bırakabilir. Bu durum cihazı kötü amaçlı yazılımlara karşı savunmasız hâle getirir.
- **Güncelleme ihmali:** İşletim sistemi güncellemeleri yalnızca yeni özellikler değil güvenlik açıklarına yönelik yamalar da içerir. Güncel tutulmayan cihazlar bilinen açıklara karşı korumasız kalır.

ARAŞTIRMA

Kullandığınız akıllı telefonu veya tableti inceleyiniz. Aşağıdaki bilgileri araştırarak tabloya yazınız.

Bilgi	Cihazınızdaki Bilgiler
Cihaz türü	
İşletim sistemi ve sürümü	
Son güncelleme tarihi	
Yüklü uygulama sayısı	
Konum iznine sahip uygulama sayısı	
Kamera iznine sahip uygulama sayısı	

Araştırma sonucunda aşağıdaki soruları yanıtlayınız.

1. Konum veya kamera iznine sahip uygulamalar arasında bu izne gerçekten ihtiyaç duymadığını düşündüğünüz bir uygulama var mı? İzni iptal etmeyi düşünür müsünüz?
2. İşletim sisteminizin güncel sürümü nedir? Cihazınızda bu sürüm yüklü mü?

KONTROL NOKTASI

Açık kaynak kodlu ve kapalı kaynak kodlu mobil işletim sistemi arasındaki fark yalnızca arayüz tercihi değildir. Güncelleme politikası, uygulama dağıtım modeli ve güvenlik mimarisi açısından da birbirinden önemli ölçüde ayrışır. Bir güvenlik uzmanı için bu farklılıkları bilmek, cihaz güvenliğini doğru değerlendirmenin ilk adımıdır.

3.1.4. Açık Kaynak Kodlu İşletim Sistemleri

Açık kaynak kodlu işletim sistemlerinde kaynak kod herkese açıktır. İsteyen herkes inceleyebilir, değiştirebilir ve kendi ihtiyacına göre uyarlayabilir. Bu yapı, geniş bir geliştirici topluluğunun sisteme katkı sağlamasına olanak tanır. Bu kategorinin en yaygın temsilcisi Linux'tur.

Linux, 1991 yılında Finlandiyalı yazılım geliştirici Linus Torvalds tarafından geliştirilen, açık kaynak kodlu ve özgürce dağıtılabilen bir işletim sistemi çekirdeğidir. Başlangıçta kişisel bir proje olarak tasarlanan Linux, zamanla dünya genelinden binlerce geliştiricinin katkısıyla büyümüş ve günümüzün en yaygın kullanılan işletim sistemi çekirdeklerinden biri hâline gelmiştir. Bugün Linux; web sunucularından akıllı telefonlara, gömülü sistemlerden süper bilgisayarlara (Olağan bilgisayarlardan çok daha yüksek işlem gücüne sahip, bilimsel araştırma ve karmaşık hesaplamalarda kullanılan özel sistemlerdir.) kadar pek çok farklı platformda kullanılmaktadır.

BİLGİ KUTUSU : Linux ve GNU

Teknik olarak **Linux** yalnızca çekirdektir. Kullanıcının günlük işlemler yapabilmesi için çekirdeğin yanında dosya yönetimi, metin işleme, kabuk gibi temel araçlara da ihtiyaç vardır. Bu araçların büyük çoğunluğunu sağlayan proje, 1983 yılında Richard Stallman tarafından başlatılan **GNU** [GNU's Not Unix (GNU Unix Değildir)] projesidir. Bu nedenle teknik çevrelerde kullanılan tam adı **GNU/Linux**'tur. Günlük kullanımda ise kısaca **Linux** olarak anılır.

Açık kaynak kodlu işletim sistemlerini diğer işletim sistemlerinden ayırt eden başlıca özellikler şunlardır:

Açık Kaynak: Kaynak kodu herkese açıktır; herkes inceleyebilir, değiştirebilir veya dağıtabilir.

Ücretsiz Kullanım: Çoğu dağıtım lisans ücreti gerektirmez.

Topluluk Desteği: Geniş bir geliştirici ve kullanıcı topluluğu tarafından desteklenir, hatalar hızla tespit edilip giderilir.

Özelleştirilebilirlik: Masaüstü ortamından çekirdek yapılandırmasına kadar her katman kullanıcı ihtiyacına göre düzenlenebilir.

Esneklik ve Taşınabilirlik: Masaüstü bilgisayarlardan gömülü sistemlere ve sunuculara kadar geniş bir donanım yelpazesinde çalışır.

Paket Yönetimi: Yazılım kurulum, güncelleme ve kaldırma işlemleri paket yöneticileri aracılığıyla merkezi olarak yönetilir.

Dağıtım Çeşitliliği: Farklı kuruluş ve topluluklar tarafından geliştirilen onlarca dağıtım, farklı kullanım amaçlarına ve donanım gereksinimlerine göre seçilebilir.

3.1.4.1. Açık Kaynak Kodlu İşletim Sistemi Dağıtımları

Linux çekirdeği tek başına kullanıma hazır bir sistem değildir. Farklı kuruluşlar ve topluluklar bu çekirdeği alarak üzerine araçlar, masaüstü ortamları ve uygulama paketleri ekleyerek kullanıma hazır sistemler oluşturur. Bu sistemlerin her birine **dağıtım (distribution veya distro)** adı verilir.

Dağıtımlar, hedef kitleye ve kullanım amacına göre farklı biçimlerde geliştirilir. Bazıları kişisel masaüstü kullanımına yönelik kolay kurulum ve kullanıcı dostu arayüzlere öncelik verirken bazıları sunucu ortamları için kararlılığı ve uzun dönem desteği ön planda tutar. Siber güvenlik alanına özel dağıtımlar ise güvenlik testi ve ağ analizi araçlarıyla donatılmış olarak gelir. Bu çeşitlilik, açık kaynak kodlu işletim sistemlerinin geniş bir kullanım alanına yayılmasını sağlayan temel etkenlerden biridir.

Açık kaynak kodlu işletim sistemi dağıtımları, temel aldıkları altyapıya göre aileler hâlinde gruplanır. Aynı aileye ait dağıtımlar ortak bir paket yönetim sistemi, benzer dizin yapısı ve ortak yapılandırma araçları paylaşır. Bu nedenle bir dağıtımda edinilen deneyim, aynı ailenin diğer dağıtımlarına kolayca aktarılabilir. Yaygın dağıtım aileleri şunlardır:

1. **Debian tabanlı dağıtımlar:** Kararlılığı ve geniş paket deposuyla öne çıkar. Topluluk desteği güçlüdür.
2. **RPM tabanlı dağıtımlar:** Kurumsal kullanıma yönelik güçlü yönetim araçları ve uzun dönem destek sunar.
3. **Arch tabanlı dağıtımlar:** Sade ve özelleştirilebilir yapısıyla ileri düzey kullanıcılara yöneliktir.

Tablo 3.4'te açık kaynak kodlu işletim sistemi dağıtım kategorileri ve örnek dağıtımlar verilmiştir.

Tablo 3.4: Açık Kaynak Kodlu İşletim Sistemi Dağıtım Kategorileri

Kategori	Temel Özellikler	Örnek Dağıtımlar
Masaüstü ve kişisel kullanım	Kullanıcı dostu arayüz, kolay kurulum, geniş uygulama desteği	Ubuntu, Linux Mint, Manjaro
Kurumsal ve sunucu kullanımı	Uzun dönem destek, yüksek kararlılık, kurumsal yazılım uyumluluğu	Debian, RHEL, Rocky Linux, Alma Linux
Siber güvenlik ve sızma testi	Güvenlik araçları, ağ analizi yazılımları, dijital adli analiz desteği	Kali Linux, Parrot OS
Millî ve yerelleştirilmiş kullanım	Yerli dil desteği, kamu altyapısına uyum, ulusal yazılım ekosistemi	Pardus

1. ETKİNLİK

Etkinlik Adı	Açık Kaynak Kodlu İşletim Sistemi Dağıtımları Zaman Çizelgesi
Süre	Araştırma (ders dışı)-1 hafta
Amaç	Farklı kategorilerdeki açık kaynak kodlu işletim sistemi dağıtımlarını araştırarak tarihsel gelişimlerini dijital bir zaman çizelgesi ile açıklamak
Değerlendirme	Analitik Dereceli Puanlama Anahtarı
Yönerge	Tablo 3.4'te verilen kategorilerden yola çıkarak her kategoriden en az bir dağıtım seçiniz. Seçtiğiniz dağıtımları araştırarak aşağıdaki tablodaki bilgileri doldurunuz. Tabloya en az altı dağıtım ekleyiniz. Eklediğiniz dağıtımlara göre soruları cevaplayınız. Tabloyu tamamladıktan sonra bu bilgileri kullanarak dağıtımların tarihsel gelişimini gösteren dijital bir zaman çizelgesi hazırlayınız. Zaman çizelgenizde dağıtımları kategorilerine göre gruplandırınız. Hazırladığınız zaman çizelgesini sınıfta arkadaşlarınızla 15 dakikalık süre içinde paylaşınız.

Dağıtım Adı	İlk Çıkış Yılı	Geliştirici / Kuruluş	Güncel Durum (Devam ediyor. / Sona erdi.)	Kategori

1. Araştırdığınız dağıtımlar arasında güncel durumu devam eden en eski dağıtım hangisidir?

_____

_____

_____

_____

2. Sona eren dağıtımların işlevini hangi dağıtımlar sürdürmektedir?

_____

_____

_____

_____

3. Siber güvenlik odaklı dağıtımlar hangi yıllarda ortaya çıkmıştır? Bu dağıtımların tam da o dönemde geliştirilmiş olmasını nasıl açıklarsınız?

_____

_____

_____

Kaynak (site adı / erişim tarihi): _____

_____

Değerlendirme

Çalışmanız öğretmeniniz tarafından analitik dereceli puanlama anahtarına göre değerlendirilecektir. Çalışmanızı yaparken buradaki ölçütleri dikkate alınız. Analitik dereceli puanlama anahtarı formuna ulaşmak için karekodu okutunuz. Dijital yayınlarda karekodun üstüne tıklayarak içeriğe ulaşabilirsiniz.

SİBER GÜVENLİK PENCERESİ

Siber güvenlik odaklı açık kaynak kodlu dağıtımlar, bilgisayar sistemlerine saldırmak için değil güvenlik uzmanlarının bu sistemlerdeki zayıf noktaları bulup gidermek için kullandığı özel işletim sistemleridir. İçerdikleri araçlar yanlış ellerde ciddi zarara yol açabilir. Başka kişi veya kurumların sistemlerine izinsiz erişmek, bu araçlar kullanılsa da kullanılmasa da yasalara göre suç oluşturur. Siber güvenlik eğitiminin temel ilkelerinden biri şudur: Bir aracı kullanmayı öğrenmek yetmez; bu aracın ne zaman, nerede ve hangi sınırlar içinde kullanılabileceği de bilinmelidir.

3.1.4.2. Açık Kaynak Kodlu İşletim Sisteminin Açılış Süreci

Bilgisayar başlatıldığında işletim sisteminin yüklenip çalıştırılmasını kapsayan açık kaynak kodlu işletim sisteminin açılış süreci, güç düğmesine basılmasından sistemin kullanıma hazır hâle geldiği ana kadar olan aşamaları içerir (Görsel 3.3).



Görsel 3.3: Açık kaynak kodlu işletim sistemlerinde açılış süreci

1. **BIOS/UEFI ve POST:** Güç düğmesine basıldığında anakart üzerindeki **BIOS [Basic Input/Output System (Temel Giriş-Çıkış Sistemi)]** veya **UEFI [Unified Extensible Firmware Interface (Birleşik Genişletilebilir Üretici Yazılım Arayüzü)]** yazılımı devreye girer. İlk olarak donanım bileşenlerinin çalışır durumda olup olmadığını denetler. Bu denetime **POST [Power-On Self-Test (Açılış Kendi Kendine Test)]** adı verilir. Sorun tespit edilmezse sistem önyükleyiciyi bulur, sorun varsa sesli veya görsel uyarı verilir.
2. **GRUB Önyükleyicisi:** Bu aşamada en yaygın kullanılan önyükleyici **GRUB**'dur **[GRand Unified Bootloader (Büyük Birleşik Önyükleyici)]**. GRUB, hangi işletim sisteminin açılacağını seçmeye izin verir ve Linux çekirdeğini başlatmak için gerekli dosyaları yükler. GRUB ayarları çoğunlukla /boot/grub/grub.cfg dosyasında bulunur.
3. **Linux Çekirdeği (vmlinuz) Yüklenmesi:** Linux'ta çekirdeğin sıkıştırılmış çalıştırılabilir hâli genellikle **vmlinuz** adıyla bulunur. GRUB, çekirdeği belleğe yükler. Böylece Linux çekirdeği çalışmaya başlar.
4. **Başlangıç Diskinin (initrd/initramfs) Kullanılması:** Linux çekirdeği, açılışın ilk aşamasında bazı sürücülere ve temel araçlara ihtiyaç duyar. Bu amaçla **initrd/initramfs** (başlangıç RAM diski) kullanılır. Bu yapı, çekirdeğin diskleri tanımasına ve asıl dosya sistemine geçiş yapmasına yardımcı olur.
5. **Kök Dosya Sistemine Geçiş (root):** Çekirdek, donanımı tanıdıktan sonra kalıcı **kök dosya sistemine (root)** geçer. Bu aşamadan sonra sistemdeki dosyalar ve klasör yapısı normal şekilde kullanılmaya başlanır.
6. **systemd'nin Başlatılması ve Oturum Açma:** Çekirdek, sistemdeki servisleri başlatmak ve süreçleri yönetmek için **systemd**'yi çalıştırır. systemd, sistem açılırken gerekli servisleri sırayla başlatır. Sistem grafik arayüzle açılacaksa bir giriş ekranı (login) görüntülenir, grafik arayüz yoksa kullanıcı komut satırından oturum açar. Oturum açıldıktan sonra masaüstü ortamı veya terminal kullanıma hazır hâle gelir.

SİBER GÜVENLİK PENCERESİ

Açılış süreci, sistemin en savunmasız olduğu anlardan birini oluşturur. Saldırganlar bu aşamada devreye girebilmek için önyükleyiciyi hedef alabilir veya zararlı yazılımları BIOS/UEFI düzeyine yerleştirmeye çalışabilir. UEFI'nin Secure Boot özelliği, yalnızca dijital olarak imzalanmış yazılımların yüklenmesine izin vererek bu tür saldırılara karşı bir koruma katmanı sağlar. Bu nedenle UEFI ayarlarına yetkisiz erişimin önlenmesi, sistem güvenliğinin temel adımlarından biri olarak değerlendirilir.

3.1.4.3. Açık Kaynak Kodlu İşletim Sistemlerinde Dosya Sistemi

Dosya sistemi, depolama birimindeki verilerin saklanmasını ve organizasyonunu hiyerarşi içinde düzenleyen bir yapıdır. Bu yapı; işletim sistemiyle donanım arasında köprü görevi görerek sistemde performansı, verimliliği ve güvenliği artırmak için loglama, şifreleme, sıkıştırma, erişim kontrolü, veri bütünlüğü, maksimum dosya boyutu, adresleme kapasitesi gibi özellikler sunar.

Açık kaynak kodlu işletim sistemlerinde birden fazla dosya sistemi türü bulunmaktadır. Her biri farklı kullanım ihtiyaçlarına göre geliştirilmiştir. Yaygın olarak kullanılan dosya sistemleri Tablo 3.5'te verilmiştir.

Tablo 3.5: Açık Kaynak Kodlu İşletim Sistemlerinde Kullanılan Dosya Sistemleri

Dosya Sistemi	Tam Adı	Temel Özellikler	Yaygın Kullanım Alanı
ext4	Fourth Extended Filesystem	Günlükleme (journaling) desteği, yüksek kararlılığı ve 1 exabayta kadar disk desteğiyle Linux'ta en yaygın kullanılan dosya sistemidir.	Masaüstü ve sunucu sistemleri, genel amaçlı kullanım
XFS	X Filesystem	Büyük dosya ve yüksek veri hacmiyle güçlü performans sunar, paralel G/Ç işlemlerinde öne çıkar.	Veri merkezleri, yüksek performanslı sunucular
Btrfs	B-tree Filesystem	Anlık görüntü (snapshot) alma, yerleşik RAID desteği, veri bütünlüğü denetimi gibi modern ve gelişmiş özellikler sunar.	Yedekleme sistemleri, sanallaştırma ortamları
ext3	Third Extended Filesystem	Journaling desteği sunan ext2'nin geliştirilmiş sürümüdür. ext4'ün yaygınlaşmasıyla kullanımı azalmıştır.	Eski sistemler, düşük kaynak gerektiren ortamlar
ext2	Second Extended Filesystem	Journaling desteği yoktur. Küçük ve düşük kaynaklı sistemlerde tercih edilebilir.	USB bellekler, gömülü sistemler
ReiserFS	Reiser Filesystem	Küçük dosyalarda yüksek performans sağlar. Aktif geliştirmesi durmuştur.	Eski Linux sistemleri
JFS	Journaled File System	Düşük CPU kullanımı ve journaling desteği sunar.	Sunucular, eski kurumsal sistemler

Açık kaynak kodlu işletim sistemlerinde yaygın olarak ext (extended) dosya sistemlerinin son sürümü olan **ext4** kullanılmaktadır. Yüksek kararlılığı, geniş dosya sistemi desteği ve günlükleme özelliğiyle masaüstünden sunucuya pek çok ortamda tercih edilen standart dosya sistemidir.

SİBER GÜVENLİK PENCERESİ

Dosya sistemi seçimi yalnızca performansı değil güvenliği de doğrudan etkiler. Dijital adli analizde (forensics) incelenen sistemlerde dosya sistemi türü, silinen dosyaların kurtarılabilirliğini ve iz bırakma kapasitesini belirler. Örneğin journaling özelliği sayesinde ext4, sistemde yapılan değişikliklerin kaydını tutar. Bu durum hem veri kurtarmayı hem de saldırı izlerinin takibini kolaylaştırır. Btrfs'in anlık görüntü özelliğiyse sistem ele geçirilmeden önceki durumun kopyasını almanın bir yolunu sunar.

SIRA SİZDE

Tablo 3.5'teki bilgilerden yararlanarak aşağıdaki karşılaştırma tablosunu doldurunuz. İlk beş özellik için ✓ **(var / evet)** veya ✗ **(yok / hayır)** işareti kullanınız. **Yaygın kullanım alanı** satırı için kısa bir açıklama yazınız.

Özellik	ext4	XFS	Btrfs	ext2 / ext3
Journaling desteği				
Snapshot (anlık görüntü)				
Yerleşik RAID desteği				
Performans (büyük dosyalar)				
Geliştirme durumu				
Yaygın kullanım alanı				

3.1.4.4. Açık Kaynak Kodlu İşletim Sistemi Kurulumu

Açık kaynak kodlu işletim sistemi kurulumu, seçilen dağıtımın hedef bilgisayara yüklenmesi ve kullanıma hazır hâle getirilmesi sürecini kapsar. Kurulum öncesinde dağıtıma ait ISO dosyasının indirilmesi ve önyüklenebilir bir USB bellek hazırlanması gerekir.

BİLGİ KUTUSU : Canlı (Live) Disk

Bazı Linux dağıtımları, kurulum gerektirmeksizin doğrudan USB bellekten çalıştırılabilir. Bu özelliğe canlı disk adı verilir. Canlı disk sayesinde sistemi bilgisayara kurmadan önce deneyebilir, sistemin arayüzünü ve temel işlevlerini inceleyebilirsiniz. Canlı disk modunda yapılan değişiklikler sisteme kaydedilmez, bilgisayar yeniden başlatıldığında her şey sıfırlanır.

1. ÖRNEK UYGULAMA

Siber güvenlik odaklı açık kaynak kodlu işletim sistemlerinden birinin kurulumunu aşağıdaki adımları izleyerek gerçekleştiriniz.

1. Adım: Açık kaynak kodlu işletim sistemini resmî web sitesinde Installer sayfasından sisteminize uygun ISO dosyasını seçerek indiriniz (Görsel 3.4).



Görsel 3.4: Açık kaynak kodlu işletim sistemi ISO dosyasının indirilmesi

2. Adım: İndirilen ISO dosyasını kullanarak önyüklenebilir bir USB bellek hazırlayınız.

3. Adım: Hazırladığınız USB belleği bilgisayara takarak yeniden başlatınız. BIOS/UEFI ayarlarına giriniz ve ilk açılış aygıtını USB olarak ayarlayınız. Ayar kaydedildikten sonra bilgisayar yeniden başlar ve kurulum ekranı açılır.

4. Adım: İşletim sistemi kurulum menüsünden Graphical install seçeneğini seçiniz (Görsel 3.5).



Görsel 3.5: Kurulum menüsü

5. Adım: Dil seçimi ekranında Turkish -Türkçe seçeneğini seçiniz.

6. Adım: Konum seçimi ekranında Türkiye'yi seçiniz.

7. Adım: Klavye yapılandırması ekranında kullandığınız klavye düzenine göre (Q düzeni veya F düzeni) seçim yapınız.

8. Adım: Ağ yapılandırması ekranında bilgisayarınıza ana bilgisayar adı (hostname) olarak **siber** yazınız (Varsayılan olarak **kali** yazılıdır.).

9. Adım: Alan adı (domain name) ekranı boş bırakılabilir.

10. Adım: Kullanıcıları ve parolaları oluştur bölümünde ilk olarak yeni kullanıcının tam adını giriniz ve sonraki adımda yeni kullanıcı hesabı için kullanıcı adını **siber** olarak giriniz. Kullanıcı adları küçük harfle başlamalıdır.

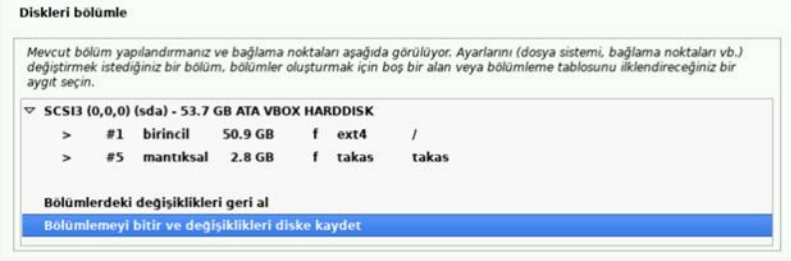
11. Adım: Oluşturmak istediğiniz yeni kullanıcı hesabı için güçlü bir parola belirleyiniz.

12. Adım: Diskleri bölümle ekranında bölümleme yöntemi olarak **Yardımcı ile-diskin tamamını kullan** seçeneğini seçiniz.

13. Adım: Ardından gelen disk bölüme ekranında **bölümlenecek disk seçimini** yapınız.

14. Adım: Bölümleme şeması olarak **Tüm dosyalar tek bölümde** seçeneğini seçiniz.

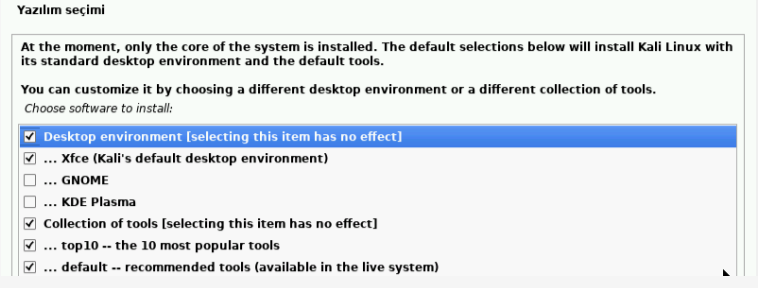
15. Adım: Bölüm yapılandırma özetini gösteren ekranda değişiklikleri diske kaydetmek için **Bölümlemeyi bitir ve değişiklikleri diske kaydet** seçeneğini onaylayınız (Görsel 3.6).



Görsel 3.6: Bölüm yapılandırma özeti

16. Adım: Son olarak **Değişiklikler diske kaydedilsin mi?** sorusuna **Evet** seçeneğini işaretleyerek devam ediniz.

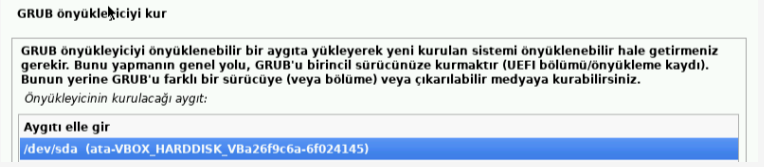
17. Adım: Yazılım seçimi ekranında varsayılan seçeneklerle devam ediniz ve kurulumun tamamlanmasını bekleyiniz (Görsel 3.7).



Görsel 3.7: Yazılım seçimi ekranı

18. Adım: GRUB önyükleyiciyi kur ekranında **GRUB önyükleyici birincil sürücünüze yüklensin mi?** sorusuna Evet seçeneğini işaretleyerek devam ediniz.

19. Adım: Önyükleyicinin kurulacağı aygıtı seçerek kuruluma devam ediniz (Görsel 3.8) ve kurulumun bitmesini bekleyiniz.



Görsel 3.8: GRUB önyükleyicinin kurulacağı aygıt seçim ekranı

20. Adım: **Kurulum tamamlandı** ekranı görüntülendiğinde USB belleği bilgisayardan çıkarınız ve Devam düğmesine tıklayarak sistemi yeniden başlatınız.

21. Adım: Sistem yeniden başladığında işletim sistemi giriş ekranı gelir. Kurulum sırasında oluşturduğunuz kullanıcı adı ve parolayı girerek Oturum aç düğmesine tıklayınız. İşletim sistemi masaüstü açılır ve sistem kullanıma hazır hâle gelir (Görsel 3.9).



Görsel 3.9: İşletim sistemi masaüstü ekranı

2. ETKİNLİK

Etkinlik Adı	Pardus Kurulumu
Süre	Kurulum uygulaması + sunum hazırlama (ders dışı) - 1 hafta
Amaç	Açık kaynak kodlu işletim sisteminin kurulum sürecini adım adım uygulayarak sistemi kullanıma hazır hâle getirmek
Yönerge	Pardus kurulum adımlarını sınıfta gösterilen uygulama doğrultusunda gerçekleştiriniz. Kurulum sürecinin her adımını ekran görüntüsü alarak belgeleyiniz. Aldığınız ekran görüntülerini ve açıklamalarını bir sunum dosyasına aktarınız. Hazırladığınız sunumu sınıf arkadaşlarınızla 15 dakikalık süre içinde paylaşınız.

Sunumda Yer Alacak Bölümler

Bölüm	İçerik
1. Hazırlık	ISO dosyasının indirilmesi ve önyüklenebilir USB hazırlama adımları
2. Kurulum Adımları	BIOS/UEFI ayarı, dil/konum/klavye seçimi, kullanıcı oluşturma, disk bölümlendirme
3. Kurulum Sonrası	Sistemin çalışır durumda olduğunu gösteren ekran görüntüsü
4. Sorunlar ve Çözümler	Kurulum sırasında karşılaşılan sorunlar ve nasıl çözüldüğü

Değerlendirme

Çalışmanız öğretmeniniz tarafından analitik dereceli puanlama anahtarına göre değerlendirilecektir. Çalışmanızı yaparken buradaki ölçütleri dikkate alınız. Analitik dereceli puanlama anahtarı formuna ulaşmak için karekodu okutunuz. Dijital yayınlarda karekodun üstüne tıklayarak içeriğe ulaşabilirsiniz.

3.1.4.5. Yardımcı Yazılımların Kurulumu

Açık kaynak kodlu işletim sistemlerinde yazılım kurulumu, **paket yöneticisi** aracılığıyla gerçekleştirilir. Paket yöneticisi, yazılımların kurulmasını, güncellenmesini ve kaldırılmasını tek bir araçtan yönetmeye olanak tanır. Debian tabanlı dağıtımlarda bu işlem için **APT [A**dvanced **P**ackage **T**ool **(Gelişmiş Paket Aracı)]** kullanılır.

APT, yazılımları **paket deposu** adı verilen sunuculardan indirir. Sistemdeki depoların listesi **/etc/apt/sources.list** dosyasında tutulur. Yeni bir yazılım kurmadan önce depo listesini güncellemek, en güncel sürüme erişimi sağlar. Debian tabanlı dağıtımlarda kullanılan temel APT komutları Tablo 3.6'da verilmiştir.

Tablo 3.6: Temel APT Komutları

Komut	Açıklama
sudo apt update	Paket listesini günceller. Yazılım kurmaz yalnızca depolardaki paket listelerini indirip yeniler.
sudo apt upgrade	Yüklü tüm paketleri en güncel sürümlerine yükseltir.
sudo apt full-upgrade	Bağımlılık değişikliklerini de kapsayan tam güncelleme yapar.
sudo apt install [paket adı]	Belirtilen paketi kurar. Tek seferde birden fazla paket için paket adları arasına boşluk bırakılır.
sudo apt remove [paket adı]	Belirtilen paketi sistemden kaldırır.
sudo apt autoremove	Artık kullanılmayan paketleri sistemden kaldırır.
apt search [anahtar kelime]	Depolarda anahtar kelimeyle paket arar (Genellikle sudo gerekmez.).

BİLGİ KUTUSU : sudo Komutu

sudo komutu, bir işlemi yönetici (root) yetkileriyle çalıştırmak için kullanılır. Paket kurma, kaldırma ve güncelleme işlemleri sistem düzeyinde değişiklik yaptığından bu yetki gereklidir.

2. ÖRNEK UYGULAMA

Aşağıdaki adımları izleyerek paket yönetimi ve yardımcı yazılım kurulum işlemlerini gerçekleştiriniz.

1. Adım: Uçbirim öykünücüsünü açınız.

2. Adım: Paket listesini güncellemek için **sudo apt update** komutunu çalıştırınız (Görsel 3.10).

```
┌──(siber㉿siber)-[~]
└─$ sudo apt update
İndir: 1 http://kali.download/kali kali-rolling InRelease [34,0 kB]
İndir: 2 http://kali.download/kali kali-rolling/main arm64 Packages [21,0 MB]
İndir: 3 http://kali.download/kali kali-rolling/main arm64 Contents (deb) [49,9 MB]
İndir: 4 http://kali.download/kali kali-rolling/contrib arm64 Packages [96,4 kB]
İndir: 5 http://kali.download/kali kali-rolling/contrib arm64 Contents (deb) [178 kB]
İndir: 6 http://kali.download/kali kali-rolling/non-free arm64 Packages [137 kB]
İndir: 7 http://kali.download/kali kali-rolling/non-free arm64 Contents (deb) [866 kB]
13 sn.'de 72,2 MB alındı (5.574 kB/s)
1528 paket yükseltilebilir. Bu paketleri görmek için 'apt list --upgradable' komutunu çalıştırın.
```

Görsel 3.10: Paket listesinin güncellenmesi

3. Adım: **tree** paketinin kurulumunu **sudo apt install tree** komutuyla gerçekleştiriniz (Görsel 3.11). Bu paket dizin yapısını ağaç görünümünde listeler.

```
┌──(siber㉿siber)-[~]
└─$ sudo apt install tree
Installing:
  tree

Summary:
  Upgrading: 0, Installing: 1, Removing: 0, Not Upgrading: 1528
  Download size: 61,5 kB
  Space needed: 175 kB / 3.313 MB available

İndir: 1 http://mirror.telepoint.bg/kali kali-rolling/main arm64 tree arm64 2.3.2-1 [61,5 kB]
3 sn.'de 61,5 kB alındı (24,5 kB/s)
Daha önce seçili olmayan tree paketi seçiliyor.
(Veritabanı okunuyor ... 421293 dosya veya dizin kurulu durumda.)
Paket açılacak: .../tree_2.3.2-1_arm64.deb ...
Paket açılıyor: tree (2.3.2-1) ...
Ayarlanıyor: tree (2.3.2-1) ...
Tetikleyiciler işleniyor: man-db (2.13.1-1+b1) ...
Tetikleyiciler işleniyor: kali-menu (2026.1.5) ...
```

Görsel 3.11: tree paketinin kurulması

4. Adım: Paketin kurulup kurulmadığını doğrulamak için terminalde **tree** komutunu çalıştırınız. Komut hatasız çalışıyorsa tree paketi başarıyla kurulmuş demektir (Görsel 3.12).

```
┌──(siber㉿siber)-[~]
└─$ tree
.
├── Belgeler
├── Genel
├── İndirilenler
├── Masaüstü
├── Müzik
├── Resimler
├── Şablonlar
└── Videolar

9 directories, 0 files
```

Görsel 3.12: tree komutuyla kurulumun doğrulanması

5. Adım: **tree** paketini **sudo apt remove tree** komutuyla sistemden kaldırınız (Görsel 3.13).

```
┌──(siber㉿siber)-[~]
└─$ sudo apt remove tree
REMOVING:
  tree

Summary:
  Upgrading: 0, Installing: 0, Removing: 1, Not Upgrading: 1528
  Freed space: 175 kB

Continue? [E/h] e
(Veritabanı okunuyor ... 421301 dosya veya dizin kurulu durumda.)
Kaldırılıyor: tree (2.3.2-1) ...
Tetikleyiciler işleniyor: man-db (2.13.1-1+b1) ...
Tetikleyiciler işleniyor: kali-menu (2026.1.5) ...
```

Görsel 3.13: tree paketinin kaldırılması

3. ETKİNLİK

Etkinlik Adı	Açık Kaynak Kodlu İşletim Sistemi Yardımcı Yazılım Kurulumu ve Yönetimi
Süre	20 dakika
Amaç	Açık kaynak kodlu işletim sisteminde paket yöneticisini kullanarak yardımcı yazılım kurmak ve kurulan yazılımı yönetmek
Yönerge	Uçbirim öykünücüsünü açarak aşağıdaki adımları sırasıyla gerçekleştiriniz. Her adımı tamamladıktan sonra ekran görüntüsü alınız. Adımları tamamladıktan sonra aldığınız ekran görüntülerini sınıfta paylaşınız. Her adımı tamamladığınızda Kontrol sütununa tik (✓) atarak işaretleyiniz.

Uygulama Adımları

Adım	Yapılacak İşlem	Kontrol
1	Paket listesini güncelleyiniz.	☐ Tamamlandı
2	**curl** paketini kurunuz.	☐ Tamamlandı
3	Kurulumun gerçekleşip gerçekleşmediğini doğrulamak için **curl –version** komutunu çalıştırınız.	☐ Tamamlandı
4	**curl** paketini sistemden kaldırınız.	☐ Tamamlandı
5	**curl –version** komutunu tekrar çalıştırarak paketin kaldırıldığını doğrulayınız.	☐ Tamamlandı
6	Aldığınız ekran görüntülerini sınıfta paylaşınız.	☐ Tamamlandı

Değerlendirme

Çalışmanız öğretmeniniz tarafından kontrol listesine göre değerlendirilecektir. Çalışmanızı yaparken buradaki ölçütleri dikkate alınız. Kontrol listesi formuna ulaşmak için karekodu okutunuz. Dijital yayınlarda karekodun üstüne tıklayarak içeriğe ulaşabilirsiniz.

3.1.4.6. Açık Kaynak Kodlu İşletim Sisteminin Dizin Yapısı

Açık kaynak kodlu işletim sisteminde **her şey bir dosyadır** felsefesi benimsenmiştir. Donanım aygıtları, sistem bilgileri ve yapılandırma ayarları dâhil her bileşen dosya olarak temsil edilir. Tüm bu dosyalar, en tepesinde **kök dizinin (/)** bulunduğu hiyerarşik bir ağaç yapısında düzenlenir. Diğer tüm dizinler kök dizinin altında yer alır. Dizin yapısı **FHS [Filesystem Hierarchy Standard (Dosya Sistemi Hiyerarşi Standardı)]** ile belirlenmiştir. Bu standart sayesinde farklı dağıtımlarda dizin yapısı tutarlı bir biçimde düzenlenir. Temel dizinler Tablo 3.7'de verilmiştir.

Tablo 3.7: Açık Kaynak Kodlu İşletim Sistemleri Temel Dizinleri

Dizin	Açıklama
/	Kök dizindir. Tüm dizinler bu dizinin altında yer alır.
/bin	ls, cp, mkdir gibi temel sistem komutlarının bulunduğu dizindir.
/boot	Açılış için gerekli çekirdek dosyaları ve önyükleyici yapılandırmasının bulunduğu dizindir.
/dev	USB, disk, CD-ROM gibi donanım aygıtlarını temsil eden dosyaların bulunduğu dizindir.
/etc	Sistem ve uygulama yapılandırma dosyalarının bulunduğu dizindir.
/home	Kullanıcıların kişisel dosyalarının bulunduğu dizindir. Her kullanıcı için ayrı bir alt dizin oluşturulur.
/lib	Sistem kütüphanelerinin bulunduğu dizindir.
/media	USB bellek gibi çıkarılabilir aygıtların otomatik bağlandığı dizindir.
/opt	Üçüncü taraf uygulamaların kurulduğu dizindir.
/root	Root kullanıcısının ev dizinidir.
/srv	Sistem üzerinde çalışan hizmetlere ait dosyaların bulunduğu dizindir.
/tmp	Geçici dosyaların bulunduğu dizindir. Sistem yeniden başlatıldığında içerik silinir.
/usr	Kullanıcılar arasında paylaşılan program, komut ve kütüphanelerin bulunduğu dizindir.
/var	Sistem ve uygulamalara ait log dosyalarıyla dinamik verilerin bulunduğu dizindir.

SİBER GÜVENLİK PENCERESİ

Açık kaynak kodlu işletim sistemlerinin dizin yapısında bazı dosyalar ve dizinler siber güvenlik açısından özellikle kritik öneme sahiptir.

- **/etc/passwd:** Sistemdeki tüm kullanıcı hesaplarının bilgilerini içerir. Kullanıcı adı, UID, GID, ev dizini gibi bilgiler burada tutulur.
- **/etc/shadow:** Kullanıcı parolalarının şifrelenmiş hallerinin saklandığı dosyadır. Yalnızca root kullanıcısı okuyabilir.
- **/var/log:** Sistem ve uygulama kayıtlarının (log) tutulduğu dizindir. Saldırı tespiti ve adli analiz çalışmalarında ilk incelenen yerdir.
- **~/.bash_history:** Her kullanıcının terminalde çalıştırdığı komutların geçmişini tutar. Yetkisiz erişim durumunda saldırgan bu dosyayı inceleyerek sistem hakkında bilgi toplayabilir.

3.1.4.7. Terminal Komutları

Uçbirim öykünücüsü (terminal), kullanıcının sistemi komutlar aracılığıyla yönettiği metin tabanlı arayüzdür. Grafik arayüzün erişemediği birçok sistem işlemi terminal üzerinden gerçekleştirilebilir. Bu nedenle terminal komutlarına hâkim olmak, sistem yönetimi ve siber güvenlik alanında temel bir beceridir.

Yardım ve Bilgi Alma Komutları

Açık kaynak kodlu işletim sisteminde bir komutu kullanmadan önce o komutun ne işe yaradığını, hangi seçeneklerle çalıştırılabileceğini ve ürettiği çıktının nasıl yorumlanacağını öğrenmek gerekebilir. Bu amaçla sisteme yerleşik yardım araçları kullanılır (Tablo 3.8).

Tablo 3.8: Yardım Komutları

Komut	Açıklama	Örnek
man [komut]	Komutun kılavuz sayfasını gösterir.	man ls
[komut] —help	Komutun kısa kullanım bilgisini gösterir.	ls —help
whatis [komut]	Komutun tek satırlık açıklamasını gösterir.	whatis ls
which [komut]	Komutun dosya sistemindeki konumunu gösterir.	which python3

Bilgi alma komutları ise bilgisayar adı, çekirdek sürümü, kullanıcı kimliği, tarih, saat, disk kullanımı, bellek miktarı gibi birçok sistem bilgisine erişimi sağlar (Tablo 3.9).

Tablo 3.9: Bilgi Alma Komutları

Komut	Açıklama	Örnek
uname -a	Sistem çekirdeği ve sürümü hakkında bilgi verir.	uname -a
hostname	Bilgisayarın ağ üzerindeki adını görüntüler.	hostname
lsb_release -a	Kullanılan Linux dağıtımıyla ilgili bilgileri verir.	lsb_release -a
whoami	Etkin kullanıcı adını gösterir.	whoami
who	Sisteme giriş yapan kullanıcılar hakkında bilgi verir.	who
uptime	Sistemin çalışma süresini ve ortalama yük durumunu gösterir.	uptime
date	Sistemin tarih ve saat bilgisini görüntüler.	date
df -h	Disk kullanımı hakkında bilgi verir.	df -h
du -sh [dizin]	Belirtilen dizinin kapladığı alanı gösterir.	du -sh /home/siber
free -h	Bellek kullanımını gösterir.	free -h
history	Terminalde çalıştırılan komutların geçmişini gösterir.	history

3. ÖRNEK UYGULAMA

Aşağıdaki adımları izleyerek yardım ve bilgi alma komutlarını uygulayınız.

1. Adım: Uçbirim öykünücüsünü açınız.

2. Adım: **whatis** komutuyla **ls** komutunun tek satırlık açıklamasını görüntüleyiniz (Görsel 3.14).

```
┌──(siber㉿siber)-[~]
└─$ whatis ls
ls (1)               - list directory contents
```

Görsel 3.14: whatis komutu kullanımı

3. Adım: **man** komutuyla **ls** komutunun kılavuz sayfasını açınız, kapatmak için **q** tuşuna basınız (Görsel 3.15).

```
LS(1)                                                          User Commands
                                        LS(1)

NAME
       ls - list directory contents

SYNOPSIS
       ls [OPTION]... [FILE]...

DESCRIPTION
       List information about the FILEs (the current directory by default).  Sort entries alphabetically if none of -cf
tuvSUX nor --sort is specified.

       Mandatory arguments to long options are mandatory for short options too.

       -a, --all
              do not ignore entries starting with .

       -A, --almost-all
              do not list implied . and ..
 Manual page ls(1) line 1 (press h for help or q to quit)
```

Görsel 3.15: man ls çıktısı

4. Adım: **cp** komutunun kısa kullanım bilgisini **- -help** parametresiyle görüntüleyiniz (Görsel 3.16).

```
┌──(siber㉿siber)-[~]
└─$ cp --help
Kullanım: cp [SEÇENEK]... [-T] KAYNAK HEDEF
   veya:  cp [SEÇENEK]... KAYNAK... DİZİN
   veya:  cp [SEÇENEK]... -t DİZİN KAYNAĞI
KAYNAK'ı HEDEF'e veya birden fazla KAYNAK'ları DİZİN'e kopyala.

Uzun seçeneklere olan gerekli argümanlar kısa seçenekler için de geçerlidir.
  -a, --archive                -dR --preserve=all ile aynı
      --attributes-only        dosya verisini kopyalama, yalnızca nitelikleri
      --backup[=DENETİM]       her mevcut hedef dosyanın yedeğini al
  -b                           --backup gibi; ancak argüman almaz
      --copy-contents          özyineli ise özel dosyaların içeriğini kopyala
  -d                           --no-dereference --preserve=links ile aynı
      --debug                  explain how a file is copied.  Implies -v
  -f, --force                  eğer açılamayan mevcut bir hedef dosyasıysa
                                 kaldır ve yeniden dene (eğer -n seçeneği de
                                 kullanılmışsa bu seçenek yok sayılır)
  -i, --interactive            üzerine yazmadan önce sor (önceki bir -n
```

Görsel 3.16: cp - -help çıktısı

5. Adım: **which** komutuyla **find** komutunun sistemdeki konumunu görüntüleyiniz.

6. Adım: **uname -a** komutunu çalıştırarak sistem çekirdeği ve işletim sistemi hakkında bilgi alınız.

7. Adım: **whoami** komutunu çalıştırarak etkin kullanıcı adını görüntüleyiniz.

8. Adım: **uptime** komutunu çalıştırarak sistemin çalışma süresini görüntüleyiniz.

9. Adım: **free -h** komutunu çalıştırarak bellek kullanım bilgisini görüntüleyiniz.

10. Adım: **history** komutunu çalıştırarak terminalde daha önce kullanılan komutları görüntüleyiniz.

11. Adım: Ekrana gelen bilgileri inceleyiniz (Görsel 3.17).

```
┌──(siber㉿siber)-[~]
└─$ which find
/usr/bin/find

┌──(siber㉿siber)-[~]
└─$ uname -a
Linux siber 6.18.12+kali-arm64 #1 SMP PREEMPT Kali 6.18.12-1kali1 (2026-02-25) aarch64 GNU/Linux

┌──(siber㉿siber)-[~]
└─$ who
siber    seat0        2026-06-08 20:35 (:0)

┌──(siber㉿siber)-[~]
└─$ uptime
 10:54:48 up 12:30,  1 user,  load average: 0,01, 0,02, 0,00

┌──(siber㉿siber)-[~]
└─$ free -h
               total        used        free      shared  buff/cache   available
Mem:           3,8Gi       856Mi       1,8Gi        16Mi       1,4Gi       3,0Gi
Swap:          1,0Gi          0B       1,0Gi

┌──(siber㉿siber)-[~]
└─$ history
    1  whatis ls
    2  man ls
    3  cp --help
    4  clear
```

Görsel 3.17: Bazı yardım ve bilgi alma komutlarının kullanımı

Dosya ve Dizin Yönetimi Komutları

Dosyalar ve dizinler, açık kaynak kodlu işletim sisteminin temel yapı taşlarıdır. Dosya ve dizinler üzerinde işlem yapmak için kullanılan temel komutlar, kullanıcının dosya sistemi üzerinde gezinmesini, dosya/dizin oluşturmasını, bunları kopyalamasını, taşımasını ve silmesini sağlar. Tablo 3.10'da en sık kullanılan komutlar ve örnekleri verilmiştir.

Tablo 3.10: Dosya ve Dizin Yönetimi Temel Komutları

Komut	Açıklama	Örnek
pwd	Bulunulan dizinin tam yolunu gösterir.	pwd
ls -la	Dizin içeriğini ayrıntılı ve gizli dosyalarla birlikte listeler.	ls -la
cd [dizin]	Dizin değiştirir. cd .. bir üst dizine çıkar, cd veya cd ~ ana dizine döner.	cd /etc
mkdir [ad]	Yeni dizin oluşturur. -p parametresiyle iç içe dizinler oluşturulabilir.	mkdir belgeler
rmdir [ad]	Boş bir dizini siler. Dolu dizinleri silmek için rm -r kullanılır.	rmdir belgeler

Komut	Açıklama	Örnek
touch [dosya]	Boş dosya oluşturur veya var olan dosyanın zaman damgasını günceller.	touch test.txt
cp [kaynak] [hedef]	Dosya veya dizini kopyalar. Dizin kopyalamak için -r parametresi gerekir.	cp test.txt /tmp
mv [kaynak] [hedef]	Dosya veya dizini taşır, hedef olarak yeni bir ad verilirse yeniden adlandırır.	mv test.txt yeni.txt
rm [dosya/dizin]	Dosya veya dizini siler. Dizini tüm içeriğiyle silmek için -r, zorlamak için -f parametresi kullanılır.	rm -r klasor
find [yol] -name [kriter]	Belirtilen yolda, adı verilen desene uyan dosya veya dizinleri arar.	find /home -name '*.txt'

KONTROL NOKTASI

rm komutuyla silinen dosyalar geri getirilemez. Dizin silmek için kullanılan **rm -r** komutu tüm içerikleri birlikte siler. Silme işlemi yapmadan önce doğru dizinde olduğunuzu **ls** komutuyla doğrulayınız.

Dosyaların içeriğini görüntülemek, içeriğinde aramak veya dosyalar üzerinde basit düzenlemeler yapmak için aşağıdaki komutlar kullanılır. Bu komutlar özellikle log dosyalarını inceleme, yapılandırma dosyalarını okuma ve metin tabanlı verileri işleme görevlerinde işinizi kolaylaştırır. Temel dosya içeriği işleme ve görüntüleme komutları Tablo 3.11'de gösterilmektedir.

Tablo 3.11: Temel Dosya İşleme ve Görüntüleme Komutları

Komut	Açıklama	Örnek
cat [dosya]	Dosyanın tüm içeriğini ekrana yazdırır.	cat /etc/hostname
less [dosya]	Uzun dosyaları sayfa sayfa görüntüler. Çıkmak için q tuşuna basılır.	less /var/log/syslog
head [dosya]	Dosyanın ilk 10 satırını gösterir.	head /var/log/syslog
tail [dosya]	Dosyanın son 10 satırını gösterir. Log takibi için -f kullanılır.	tail -f /var/log/syslog
grep "metin" [dosya]	Dosya içinde belirtilen metni arar.	grep "error" /var/log/syslog
wc [dosya]	Dosyadaki satır, kelime ve karakter sayısını verir.	wc /etc/passwd
echo "metin"	Metni terminal ekranına yazdırır.	echo "Merhaba"
echo "metin" > [dosya]	Dosya oluşturur veya mevcut dosyanın üzerine yazar.	echo "Ali" > isimler.txt
echo "metin" >> [dosya]	Var olan dosyanın sonuna ekleme yapar.	echo "Veli" >> isimler.txt

4. ÖRNEK UYGULAMA

Aşağıdaki adımları izleyerek yardım, bilgi alma ve dosya/dizin komutlarını uygulayınız.

1. Adım: Uçbirim öykünücüsünü açınız.

2. Adım: **pwd** komutuyla bulunduğunuz dizini görüntüleyiniz.

3. Adım: **mkdir** komutuyla **güvenlik_raporlari** adında bir dizin oluşturunuz.

4. Adım: **cd** komutuyla oluşturduğunuz dizine geçiniz.

5. Adım: **touch** komutuyla **olay.txt** adında boş bir dosya oluşturunuz.

6. Adım: **echo** komutuyla dosyanın içine "**Yetkisiz giriş denemesi tespit edildi**." metnini ekleyiniz.

7. Adım: **cat** komutuyla dosya içeriğini görüntüleyiniz.

8. Adım: **cp** komutuyla dosyanın **yedek_olay.txt** adında yedeğini oluşturunuz.

9. Adım: **mv** komutuyla yedek dosyanın adını **olay_yedek.txt** olarak değiştiriniz.

10. Adım: **ls -la** komutuyla dizin içeriğini görüntüleyiniz.

11. Adım: **find** komutuyla bulunduğunuz dizin içerisinde .txt uzantılı dosyaları arayınız.

12. Adım: Ekrana gelen bilgileri inceleyiniz (Görsel 3.18).

```
┌──(siber㉿siber)-[~]
└─$ pwd
/home/siber

┌──(siber㉿siber)-[~]
└─$ mkdir guvenlik_raporlari

┌──(siber㉿siber)-[~]
└─$ cd guvenlik_raporlari

┌──(siber㉿siber)-[~/guvenlik_raporlari]
└─$ touch olay.txt

┌──(siber㉿siber)-[~/guvenlik_raporlari]
└─$ echo "Yetkisiz giriş denemesi tespit edildi." > olay.txt

┌──(siber㉿siber)-[~/guvenlik_raporlari]
└─$ cat olay.txt
Yetkisiz giriş denemesi tespit edildi.

┌──(siber㉿siber)-[~/guvenlik_raporlari]
└─$ cp olay.txt yedek_olay.txt

┌──(siber㉿siber)-[~/guvenlik_raporlari]
└─$ mv yedek_olay.txt olay_yedek.txt

┌──(siber㉿siber)-[~/guvenlik_raporlari]
└─$ ls -la
toplam 16
drwxrwxr-x  2 siber siber 4096 Haz  9 11:15 .
drwx------ 17 siber siber 4096 Haz  9 11:13 ..
-rw-rw-r--  1 siber siber   40 Haz  9 11:14 olay.txt
-rw-rw-r--  1 siber siber   40 Haz  9 11:14 olay_yedek.txt

┌──(siber㉿siber)-[~/guvenlik_raporlari]
└─$ find . -name "*.txt"
./olay_yedek.txt
./olay.txt
```

Görsel 3.18: Dosya ve dizin yönetimi uygulamasının çıktısı

SIRA SİZDE

Aşağıdaki tabloda kullanım durumları ve komutlar verilmiştir. Her durumda hangi komutun kullanılacağını belirleyerek ilgili kutucuğa tik (✓) işareti koyunuz. Bazı durumlar için birden fazla komut işaretlenebilir.

Kullanım Durumu	man	whatis	whoami	Ls -la	cd	mkdir	touch	rm	cat	grep
Bir komutun ayrıntılı kılavuz sayfasına ulaşmak										
Bir komutun tek satırlık açıklamasını göstermek										
Etkin kullanıcı adını öğrenmek										
Dizin içeriğini ayrıntılı listelemek										
Dizinler arasında geçiş yapmak										
Yeni bir dizin oluşturmak										
Boş bir dosya oluşturmak										
Dosya veya dizin silmek										
Dosyanın tüm içeriğini görüntülemek										
Dosya içinde belirli bir metni aramak										

Arşivleme ve Dosya İndirme Komutları

Dosya ve dizinler arşivlenerek tek bir dosya hâline getirilebilir veya sıkıştırılarak daha az yer kaplaması sağlanabilir. Bu işlem özellikle yedekleme ve dosya paylaşımı süreçlerinde kullanılır. Terminal üzerinden internetten dosya indirmek için ise **wget**, **curl** gibi araçlardan yararlanılır. Açık kaynak kodlu işletim sistemlerinde kullanılan temel arşivleme ve dosya indirme komutları Tablo 3.12'de verilmiştir.

Tablo 3.12: Arşivleme ve Dosya İndirme Komutları

Komut	Açıklama	Örnek
tar -cvf [arşiv] [dizin]	Bir dizini sıkıştırmadan arşivler.	tar -cvf yedek.tar belgeler/
tar -xvf [arşiv]	Arşiv dosyasını açar.	tar -xvf yedek.tar
tar -czvf [arşiv] [dizin]	Dizini sıkıştırılmış arşiv olarak oluşturur.	tar -czvf yedek.tar.gz belgeler/
tar -xzvf [arşiv]	Sıkıştırılmış arşivi açar.	tar -xzvf yedek.tar.gz

Komut	Açıklama	Örnek
zip [arşiv] [dosya]	ZIP arşivi oluşturur.	zip yedek.zip dosya.txt
unzip [arşiv]	ZIP arşivini açar.	unzip yedek.zip
wget [URL]	Belirtilen adresten dosya indirir.	wget https://example.com/test.txt
curl -O [URL]	Belirtilen adresten dosya indirir.	curl -O https://example.com/test.txt

SİBER GÜVENLİK PENCERESİ

wget ve **curl** komutları internetten doğrudan dosya indirmeye olanak tanır. Bu komutlarla indirilen dosyalar tarayıcının güvenlik denetimlerinden geçmez. Bilinmeyen veya güvenilmeyen kaynaklardan indirilen dosyalar zararlı yazılım içerebilir; sistemi ele geçirmeye, veri çalmaya veya arka kapı açmaya yönelik kodlar barındırabilir. İndirme işlemi yapmadan önce kaynağın güvenilir olduğundan emin olunuz.

5. ÖRNEK UYGULAMA

Aşağıdaki adımları izleyerek arşivleme ve dosya indirme komutlarını uygulayınız.

1. Adım: Uçbirim öykünücüsünü açınız.

2. Adım: **/tmp** dizini altında **mkdir** komutuyla **yedek** adlı bir dizin oluşturunuz ve dizinin içine **touch** komutuyla üç boş dosya ekleyiniz (Görsel 3.19).

```
┌──(siber㉿siber)-[~]
└─$ cd /tmp

┌──(siber㉿siber)-[/tmp]
└─$ mkdir yedek

┌──(siber㉿siber)-[/tmp]
└─$ touch yedek/dosya1.txt yedek/dosya2.txt yedek/dosya3.txt
```

Görsel 3.19: Dizin ve dosyaların oluşturulması

3. Adım: **tar -czvf** komutuyla **yedek** dizinini **yedek.tar.gz** adıyla sıkıştırarak arşivleyiniz (Görsel 3.20).

```
┌──(siber㉿siber)-[/tmp]
└─$ tar -czvf yedek.tar.gz yedek
yedek/
yedek/dosya3.txt
yedek/dosya2.txt
yedek/dosya1.txt
```

Görsel 3.20: Sıkıştırılmış arşiv oluşturma

4. Adım: **mkdir** komutuyla **yedek_acik** adlı bir dizin oluşturunuz ve **tar -xzvf** komutuyla arşivi bu dizine açınız (Görsel 3.21).

```
┌──(siber㉿siber)-[/tmp]
└─$ mkdir yedek_acik

┌──(siber㉿siber)-[/tmp]
└─$ tar -xzvf yedek.tar.gz -C yedek_acik
yedek/
yedek/dosya3.txt
yedek/dosya2.txt
yedek/dosya1.txt
```

Görsel 3.21: Arşivin başka bir dizin içine açılması

5. Adım: **ls -la** komutuyla arşivin açıldığı dizini listeleyiniz (Görsel 3.22).

```
┌──(siber㉿siber)-[/tmp]
└─$ ls -la yedek_acik
toplam 0
drwxrwxr-x  3 siber siber  60 Haz  9 15:19 .
drwxrwxrwt 14 root  root  360 Haz  9 15:18 ..
drwxrwxr-x  2 siber siber 100 Haz  9 15:14 yedek

┌──(siber㉿siber)-[/tmp]
└─$ ls -la yedek_acik/yedek
toplam 0
drwxrwxr-x 2 siber siber 100 Haz  9 15:14 .
drwxrwxr-x 3 siber siber  60 Haz  9 15:19 ..
-rw-rw-r-- 1 siber siber   0 Haz  9 15:14 dosya1.txt
-rw-rw-r-- 1 siber siber   0 Haz  9 15:14 dosya2.txt
-rw-rw-r-- 1 siber siber   0 Haz  9 15:14 dosya3.txt
```

Görsel 3.22: Açılan arşiv içeriğinin listelenmesi

6. Adım: **curl** komutuyla **https://example.com/index.html** adresinden örnek bir dosya indiriniz (Görsel 3.23).

```
┌──(siber㉿siber)-[/tmp]
└─$ curl -O https://www.example.com/index.html
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100   528    0   528    0     0     34      0              00:15                97
```

Görsel 3.23: curl komutuyla dosya indirme

SIRA SİZDE

Siber güvenlik odaklı açık kaynak kodlu işletim sistemi dağıtımı kurulu sisteminizde proje dosyalarınızı düzenli biçimde yedeklemeniz ve terminal üzerinden güvenilir bir kaynaktan dosya indirme işlemini incelemeniz istenmektedir. Bu çalışmada bir proje dizini oluşturacak, dosyaları arşivleyecek, arşivi farklı bir dizine açacak ve indirme komutlarını uygulayacaksınız.

Verilen görevleri terminalde gerçekleştiriniz ve kullandığınız komutları tabloya yazınız.

No.	Görev	Kullandığım Komut
1	**/tmp** dizininde **proje** adlı bir dizin oluşturunuz ve içine iki boş dosya ekleyiniz.	

No.	Görev	Kullandığım Komut
2	**proje** dizinini **proje.tar.gz** adıyla sıkıştırılmış arşiv olarak kaydediniz.	
3	Oluşturduğunuz arşivin bulunduğu dizini listeleyiniz.	
4	Arşivi **/tmp** içerisinde oluşturduğunuz **proje_acilan** dizinine açınız.	
5	**wget** veya **curl** komutlarını kullanarak **https://www.example.com/index.html** adresinden dosya indiriniz.	
6	İndirilen dosyanın adını ve bulunduğu yeri listeleyerek doğrulayınız.	

Yetkilendirme, Kullanıcı ve Grup Yönetimi

Açık kaynak kodlu işletim sisteminde her dosya ve dizinin bir sahibi ve erişim izinleri vardır. Bu izinler; okuma (r), yazma (w) ve çalıştırma (x) olarak tanımlanır. Çok kullanıcılı yapısı nedeniyle sisteme kimlerin erişebileceğini ve hangi kaynaklara ulaşabileceğini belirlemek için yetkilendirme, kullanıcı ve grup yönetimi komutları kullanılır (Tablo 3.13).

Tablo 3.13: Yetkilendirme, Kullanıcı ve Grup Yönetimi Komutları

Komut	Açıklama	Örnek
ls -l	Dosya ve dizin izinlerini ayrıntılı listeler.	ls -l rapor.txt
chmod [izin] [dosya]	Dosya veya dizin izinlerini değiştirir.	chmod 600 rapor.txt
chown [kullanıcı] [dosya]	Dosyanın sahibini değiştirir.	sudo chown ogrenci rapor.txt
passwd [kullanıcı]	Kullanıcı parolasını değiştirir.	sudo passwd ogrenci
useradd [ad]	Yeni kullanıcı oluşturur.	sudo useradd ogrenci
userdel [ad]	Kullanıcıyı siler.	sudo userdel ogrenci
groupadd [ad]	Yeni grup oluşturur.	sudo groupadd ekip
usermod -aG [grup] [kullanıcı]	Kullanıcıyı belirtilen gruba ekler.	sudo usermod -aG ekip ogrenci
id [kullanıcı]	Kullanıcının UID, GID ve grup bilgilerini gösterir.	id ogrenci

BİLGİ KUTUSU : Yaygın Dosya İzinleri

Linux'ta dosya ve dizin izinleri sayısal ifadelerle gösterilebilir. Sık kullanılan bazı izin örnekleri şu şekildedir:

- 600 - Yalnızca dosya sahibi dosyayı okuyabilir ve dosyaya yazabilir.
- 644 - Dosya sahibi dosyayı okuyabilir ve dosyaya yazabilir, diğer kullanıcılar yalnızca okuyabilir.
- 700 - Yalnızca dosya sahibi dosyayı okuyabilir, çalıştırabilir ve dosyaya yazabilir.
- 755 - Dosya sahibi tüm izinlere sahiptir, diğer kullanıcılar dosyayı okuyabilir ve çalıştırabilir.

KONTROL NOKTASI

Dosya izinlerinin gereğinden fazla verilmesi güvenlik açığı oluşturur. Bir dosyaya 777 izni vermek herkesin o dosyayı okuma, yazma ve çalıştırma yetkisine sahip olması demektir. Bu durum özellikle çok kullanıcılı sistemlerde ve sunucu ortamlarında ciddi risk taşır. İzin verirken yalnızca gereken yetkiyi, yalnızca gereken kullanıcıya tanıyınız.

6. ÖRNEK UYGULAMA

Aşağıdaki adımları izleyerek yetkilendirme ve kullanıcı yönetimi komutlarını uygulayınız.

1. Adım: Uçbirim öykünücüsünü açınız.

2. Adım: **touch** komutuyla **/tmp** dizininde **rapor.txt** adlı bir dosya oluşturunuz ve ls -l komutuyla dosyanın mevcut izinlerini görüntüleyiniz (Görsel 3.24).

```
┌──(siber㉿siber)-[/tmp]
└─$ touch rapor.txt

┌──(siber㉿siber)-[/tmp]
└─$ ls -l rapor.txt
-rw-rw-r-- 1 siber siber 0 Haz  9 19:00 rapor.txt
```

Görsel 3.24: Oluşturulan dosyanın izinlerinin görüntülenmesi

3. Adım: **chmod** komutuyla dosyaya yalnızca dosya sahibinin okuma ve yazma iznine sahip olacağı izinleri veriniz ve izin değişikliğini **ls -l** komutuyla doğrulayınız (Görsel 3.25).

```
┌──(siber㉿siber)-[/tmp]
└─$ chmod 600 rapor.txt

┌──(siber㉿siber)-[/tmp]
└─$ ls -l rapor.txt
-rw------- 1 siber siber 0 Haz  9 19:00 rapor.txt
```

Görsel 3.25: Dosya izinlerinin değiştirilmesi

4. Adım: **useradd** komutuyla **siber_user** adlı test kullanıcısını yönetici yetkisiyle oluşturunuz ve oluşturduğunuz test kullanıcısının **id** komutuyla kimlik bilgilerini görüntüleyiniz (Görsel 3.26).

```
┌──(siber㉿siber)-[/tmp]
└─$ sudo useradd siber_user
[sudo] password for siber:

┌──(siber㉿siber)-[/tmp]
└─$ id siber_user
uid=1001(siber_user) gid=1001(siber_user) gruplar=1001(siber_user)
```

Görsel 3.26: Kullanıcının oluşturulması ve kimlik bilgilerinin görüntülenmesi

5. Adım: Uygulama sonunda oluşturduğunuz test kullanıcısını **userdel** komutuyla siliniz (Görsel 3.27).

```
┌──(siber㉿siber)-[/tmp]
└─$ sudo userdel siber_user
```

Görsel 3.27: Oluşturulan kullanıcının silinmesi

SIRA SİZDE

Aşağıdaki yapılandırılmış gridde açık kaynak kodlu işletim sisteminde kullanıcı yönetimi ve yetkilendirmeyle ilgili bazı komut ve izin kavramları verilmiştir. Kutucuklardaki numaraları kullanarak istenen bilgilerin cevaplarını ilgili boşluklara yazınız. Aynı kutucuk numarasını birden fazla yerde kullanabilirsiniz.

1. chmod	2. chown	3. useradd
4. userdel	5. usermod -aG	6. id
7. Okuma (r)	8. Yazma (w)	9. Çalıştırma (x)

	Sorular	Cevap
a)	Bir kullanıcının gruba eklenip eklenmediğini kontrol etmek için kullanılabilecek komutlar hangileridir?	
b)	Dosya ve dizin yetkilendirmesiyle doğrudan ilgili komut ve izinler hangileridir?	
c)	Kullanıcı yönetimiyle doğrudan ilgili komutlar hangileridir?	
ç)	chmod 755 izninde dosya sahibine tanınan izinler hangileridir?	
d)	chmod 644 izninde dosya sahibine tanınan izinler hangileridir?	
e)	Bir betik dosyasını düzenlemek ve çalıştırmak için gerekli izinler hangileridir?	
f)	Sistemde artık kullanılmayan bir kullanıcı hesabını silmek için hangi komut kullanılır?	

Süreç Yönetimi ve Ağ Komutları

Açık kaynak kodlu işletim sisteminde çalışan her program bir süreç (process) olarak yönetilir. Her sürecin kendine ait bir **PID [Process Identifier (Süreç Tanımlayıcı)]** numarası bulunur. Ağ komutlarıysa sistemin ağ bağlantısını görüntülemek, test etmek ve temel bağlantı durumunu incelemek için kullanılır (Tablo 3.14).

Tablo 3.14: Süreç Yönetimi ve Ağ Komutları

Komut	Açıklama	Örnek
ps aux	Çalışan süreçleri ayrıntılı listeler.	ps aux
top	Sistem kaynak kullanımını anlık gösterir.	top
kill [PID]	Belirtilen PID'ye sahip süreci sonlandırır.	kill 1234
ip a	Ağ arayüzlerini ve IP adreslerini gösterir.	ip a

Komut	Açıklama	Örnek
ping [hedef]	Hedef adrese bağlantı testi yapar.	ping 8.8.8.8
ss -tuln	Sistemde dinleme durumunda olan ağ bağlantılarını ve açık portları listeler.	ss -tuln
nmap localhost	Yerel sistemdeki açık portları tarar.	nmap localhost

SİBER GÜVENLİK PENCERESİ

ip a, ping, nmap gibi ağ komutları yalnızca kendi cihazınızda veya öğretmeninizin izin verdiği laboratuvar ortamında kullanılmalıdır. Bu komutlarla başkalarının sistemlerini izinsiz taramak veya test etmek yasal suç oluşturur. Siber güvenlik alanında bu araçları kullanabilmek teknik bilgi kadar etik sorumluluk da gerektirir.

7. ÖRNEK UYGULAMA

Aşağıdaki adımları izleyerek süreç yönetimi ve ağ komutlarını uygulayınız.

1. Adım: Uçbirim öykünücüsünü açınız.

2. Adım: **ps aux** çalışan süreçleri listeleyiniz (Görsel 3.28).

```
┌──(siber㉿siber)-[~]
└─$ ps aux
USER         PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root           1  0.1  0.3  24904 15224 ?        Ss   18:48   0:00 /sbin/init splash
root           2  0.0  0.0      0     0 ?        S    18:48   0:00 [kthreadd]
root           3  0.0  0.0      0     0 ?        S    18:48   0:00 [pool_workqueue_release]
root           4  0.0  0.0      0     0 ?        I<   18:48   0:00 [kworker/R-rcu_gp]
root           5  0.0  0.0      0     0 ?        I<   18:48   0:00 [kworker/R-sync_wq]
root           6  0.0  0.0      0     0 ?        I<   18:48   0:00 [kworker/R-kvfree_rcu_reclaim]
root           7  0.0  0.0      0     0 ?        I<   18:48   0:00 [kworker/R-slub_flushwq]
root           8  0.0  0.0      0     0 ?        I<   18:48   0:00 [kworker/R-netns]
root           9  0.0  0.0      0     0 ?        I    18:48   0:00 [kworker/0:0-events_power_efficient]
root          10  0.0  0.0      0     0 ?        I<   18:48   0:00 [kworker/0:0H-events_highpri]
root          11  0.0  0.0      0     0 ?        I    18:48   0:00 [kworker/0:1-events]
root          12  0.0  0.0      0     0 ?        I    18:48   0:00 [kworker/u8:0-events_unbound]
```

Görsel 3.28: Çalışan süreçlerin listelenmesi

3. Adım: **top** komutuyla sistem kaynak kullanımını anlık görüntüleyiniz. Çıkmak için **q** tuşuna basınız (Görsel 3.29).

```
┌──(siber㉿siber)-[~]
└─$ top

top - 16:38:38 up 1 min,  1 user,  load average: 0,24, 0,11, 0,04
Tasks: 159 total,   1 running, 158 sleeping,   0 stopped,   0 zombie
%Cpu(s):  0,3 us,  0,8 sy,  0,0 ni, 98,8 id,  0,0 wa,  0,0 hi,  0,0 si,  0,0 st
MiB Mem :   3906,8 total,   2381,2 free,    800,6 used,    879,2 buff/cache
MiB Swap:   1064,0 total,   1064,0 free,      0,0 used.   3106,3 avail Mem

    PID USER      PR  NI    VIRT    RES    SHR S  %CPU  %MEM     TIME+ COMMAND
     38 root      39  19       0      0      0 S   0,3   0,0   0:00.06 khugepaged
    676 root      20   0  588708 191320  88444 S   0,3   4,8   0:02.43 Xorg
   1172 siber     20   0  283516  31304  23944 S   0,3   0,8   0:00.20 wrapper-2.0
      1 root      20   0   24624  14872  11048 S   0,0   0,4   0:00.29 systemd
      2 root      20   0       0      0      0 S   0,0   0,0   0:00.00 kthreadd
      3 root      20   0       0      0      0 S   0,0   0,0   0:00.00 pool_workqueue_release
      4 root       0 -20       0      0      0 I   0,0   0,0   0:00.00 kworker/R-rcu_gp
      5 root       0 -20       0      0      0 I   0,0   0,0   0:00.00 kworker/R-sync_wq
      6 root       0 -20       0      0      0 I   0,0   0,0   0:00.00 kworker/R-kvfree_rcu_reclaim
      7 root       0 -20       0      0      0 I   0,0   0,0   0:00.00 kworker/R-slub_flushwq
      8 root       0 -20       0      0      0 I   0,0   0,0   0:00.00 kworker/R-netns
      9 root      20   0       0      0      0 I   0,0   0,0   0:00.00 kworker/0:0-cgroup_release
```

Görsel 3.29: top komutunun kullanımı

4. Adım: Ağ arayüzlerini ve IP adreslerini **ip a** komutuyla görüntüleyiniz (Görsel 3.30).

```
┌──(siber㉿siber)-[~]
└─$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:fe:3f:cf brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic noprefixroute eth0
       valid_lft 85994sec preferred_lft 85994sec
    inet6 fd17:625c:f037:2:ad05:3d74:e8df:b894/64 scope global temporary dynamic
       valid_lft 85995sec preferred_lft 13995sec
    inet6 fd17:625c:f037:2:a00:27ff:fefe:3fcf/64 scope global dynamic mngtmpaddr noprefixroute
       valid_lft 85995sec preferred_lft 13995sec
    inet6 fe80::a00:27ff:fefe:3fcf/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
```

Görsel 3.30: Ağ arayüzlerinin görüntülenmesi

5. Adım: **ping** komutuyla **b**elirlenen hedefe bağlantı testi yapınız. Durdurmak için **Ctrl+C** tuşlarına basınız (Görsel 3.31).

```
┌──(siber㉿siber)-[~]
└─$ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=64 time=30.0 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=64 time=38.3 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=64 time=35.3 ms
^C
— 8.8.8.8 ping statistics —
3 packets transmitted, 3 received, 0% packet loss, time 2004ms
rtt min/avg/max/mdev = 30.048/34.580/38.348/3.431 ms
```

Görsel 3.31: ping komutuyla bağlantı testi

6. Adım: Yerel sisteminizdeki açık portları **nmap localhost** komutuyla tarayınız (Görsel 3.32).

```
┌──(siber㉿siber)-[~]
└─$ nmap localhost
Starting Nmap 7.98 ( https://nmap.org ) at 2026-06-09 18:56 +0300
Nmap scan report for localhost (127.0.0.1)
Host is up (0.0000010s latency).
Other addresses for localhost (not scanned): ::1
All 1000 scanned ports on localhost (127.0.0.1) are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Nmap done: 1 IP address (1 host up) scanned in 0.06 seconds
```

Görsel 3.32: nmap localhost komutu çıktısı

SIRA SİZDE

Siber güvenlik odaklı açık kaynak kodlu işletim sistemi dağıtımı kurulu sisteminizde beklenmedik bir yavaşlama yaşandığını fark ettiniz. Hangi süreçlerin çalıştığını, sistem kaynaklarının nasıl kullanıldığını ve ağ bağlantı durumunu incelemeniz gerekmektedir.

Verilen görevleri terminalde gerçekleştiriniz ve kullandığınız komutları tabloya yazınız.

No.	Görev	Kullandığım Komut
1	Çalışan süreçleri listeleyiniz.	
2	Sistem kaynak kullanımını anlık görüntüleyiniz.	
3	Ağ arayüzlerini ve IP adreslerini listeleyiniz.	
4	Öğretmeninizin belirlediği hedef adrese bağlantı testi yapınız.	
5	Yerel sisteminizde dinlemede olan açık portları tarayınız.	

Zamanlanmış Görevler

Bazı komutların belirli zamanlarda otomatik olarak çalıştırılması gerekebilir. Bu işlem için cron aracı kullanılır (Tablo 3.15). Cron görevleri crontab dosyasında tanımlanır. Bu sayede yedekleme, günlük kayıt oluşturma veya belirli aralıklarla yapılması gereken kontroller otomatik olarak gerçekleştirilebilir.

Tablo 3.15: Cron Komutları

Komut	Açıklama
crontab -e	Cron görev dosyasını açar; yeni görev eklemek, düzenlemek veya silmek için kullanılır.
crontab -l	Tanımlanmış cron görevlerini listeler.
crontab -r	Tüm cron görevlerini siler. Geri alınamadığı için dikkatli kullanılmalıdır.

BİLGİ KUTUSU : Cron Söz Dizimi

Cron görevleri beş alandan oluşan bir zaman ifadesiyle başlar.

dakika saat ayın_günü ay haftanın_günü [komut]

(0-59)(0-23) (1-31) (1-12) (0-7)

***** işareti ilgili alanda **her zaman** anlamına gelir. Örneğin

*** * * * * date >> /tmp/test.log**: Her dakika çalışır.

0 8 * * * date >> /tmp/test.log: Her gün sabah 08.00'de çalışır.

0 8 * * 1 date >> /tmp/test.log: Yalnızca Pazartesi günleri sabah 08.00'de çalışır.

SİBER GÜVENLİK PENCERESİ

Saldırganlar sisteme sızdıktan sonra **crontab** dosyasına zararlı komutlar ekleyerek kalıcı erişim sağlayabilir. Bu yöntemle sistem her yeniden başlatıldığında veya belirlenen aralıklarla zararlı kod otomatik olarak çalıştırılabilir. Bu nedenle sistem yöneticileri düzenli aralıklarla **crontab -l** komutuyla zamanlanmış görevleri denetlemelidir.

SIRA SİZDE

Aşağıdaki cron ifadelerini inceleyiniz. Her ifadenin hangi zaman aralığında çalışacağını karşısındaki boşluğa yazınız.

No.	Cron İfadesi	Çalıştığı Zaman
1	**0 0 * * ***	
2	**30 8 * * 1-5**	
3	*** * * * ***	
4	**0 12 1 * ***	
5	**0 23 * * 6**	

8. ÖRNEK UYGULAMA

Aşağıdaki adımları izleyerek zamanlanmış bir görev oluşturunuz.

1. Adım: Uçbirim öykünücüsünü açınız.

2. Adım: Mevcut cron görevlerini **crontab -l** komutuyla listeleyiniz. Henüz tanımlanmış görev yoksa terminalde no crontab for [kullanıcı adı] mesajı görüntülenir, bu normal bir durumdur (Görsel 3.33).

```
┌──(siber㉿siber)-[~]
└─$ crontab -l
no crontab for siber
```

Görsel 3.33: Mevcut cron görevlerinin listelenmesi

3. Adım: **crontab -e** komutuyla cron görev dosyasını açınız. Nano editörü açılacaktır (Görsel 3.34).

```
 GNU nano 8.7.1                                  /tmp/crontab.bn9Tn0/crontab *
# Edit this file to introduce tasks to be run by cron.
#
# Each task to run has to be defined through a single line
# indicating with different fields when the task will be run
# and what command to run for the task
#
# To define the time you can provide concrete values for
# minute (m), hour (h), day of month (dom), month (mon),
# and day of week (dow) or use '*' in these fields (for 'any').
```

Görsel 3.34: Cron düzenleyicisinin açılması

4. Adım: Her dakika **/tmp/cron_test.log** dosyasına tarih ve saat bilgisini ekleyen güvenli bir görev tanımlayınız. ***** date >> /tmp/cron_test.log** satırını düzenleyiciye ekleyip Ctrl+O ve Enter ile kaydedip Ctrl+X ile çıkınız (Görsel 3.35).

```
 GNU nano 8.7.1                                  /tmp/crontab.BU6M2J/crontab *
* * * * * date >> /tmp/cron_test.log
```

Görsel 3.35: Cron görevi ekleme

5. Adım: Birkaç dakika bekledikten sonra log dosyasının oluşup oluşmadığını **cat** komutuyla kontrol ediniz (Görsel 3.36).

```
┌──(siber㉿siber)-[~]
└─$ cat /tmp/cron_test.log
Paz 14 Haz 2026 16:56:01 +03
Paz 14 Haz 2026 16:57:01 +03
Paz 14 Haz 2026 16:58:01 +03
```

Görsel 3.36: Cron görevinin sonucunun kontrol edilmesi

6. Adım: **crontab -e** komutuyla düzenleyiciyi tekrar açınız, eklediğiniz satırı siliniz ve Ctrl+O, Enter, Ctrl+X ile kaydederek çıkınız.

SIRA SİZDE

Siber güvenlik odaklı açık kaynak kodlu işletim sistemi dağıtımı kurulu sisteminizde her iki dakikada bir çalışarak /tmp dizinine günlük kaydı bırakan otomatik bir izleme görevi oluşturmanız istenmektedir. Bu görev sistem dosyalarına dokunmayacak; yalnızca tarih ve saat bilgisini kaydedecektir.

Verilen görevleri terminalde gerçekleştiriniz ve kullandığınız komutları tabloya yazınız.

No.	Görev	Kullandığım Komut
1	Mevcut cron görevlerini listeleyiniz.	
2	Cron düzenleyicisini açınız.	
3	Her iki dakikada bir /tmp/cron_test.log dosyasına tarih bilgisini ekleyen bir görev oluşturunuz.	
4	Oluşan log dosyasını görüntüleyiniz.	
5	Eklediğiniz cron görevini kaldırınız.	

4. ETKİNLİK

Etkinlik Adı	Sistem Durumu İnceleme ve Raporlama
Süre	20 dakika
Amaç	Temel açık kaynak kodlu işletim sistemi terminal komutlarını kullanarak sistem durumu, kullanıcı bilgileri, süreçler, ağ bağlantısı, açık portlar, servisler ve zamanlanmış görevler hakkında bilgi toplamak
Yönerge	Uçbirim öykünücüsünü açarak aşağıdaki adımları sırasıyla gerçekleştiriniz. Her adımı tamamladıktan sonra kullandığınız komutu ve elde ettiğiniz veriyi tabloya yazınız. Gerekli adımlarda ekran görüntüsü alınız. Tüm adımları tamamladıktan sonra bulgularınızı kısa bir rapor hâline getiriniz. Her adımı tamamladığınızda Kontrol sütununa tik (✓) atarak işaretleyiniz.

Güvenli Kullanım Uyarısı: Bu uygulamada yer alan komutlar yalnızca öğrencinin kendi yerel sistemi veya öğretmenin belirlediği güvenli laboratuvar ortamı üzerinde kullanılmalıdır. Başka cihazlara, okul ağına veya üçüncü kişilere ait sistemlere izinsiz bağlantı testi, tarama veya müdahale yapılmamalıdır.

Uygulama Adımları

Adım	Yapılacak İşlem	Kullanılan Komut	Elde Edilen Veri Kısa Açıklama	Kontrol
1	Oturum açan kullanıcı adını görüntüleyiniz.			☐ Tamamlandı
2	Kullanıcının kimlik ve grup bilgilerini görüntüleyiniz.			☐ Tamamlandı

Adım	Yapılacak İşlem	Kullanılan Komut	Elde Edilen Veri Kısa Açıklama	Kontrol
3	Sistem bilgilerini görüntüleyiniz.			☐ Tamamlandı
4	Disk kullanım durumunu inceleyiniz.			☐ Tamamlandı
5	Bellek kullanım durumunu inceleyiniz.			☐ Tamamlandı
6	Çalışan süreçleri listeleyiniz.			☐ Tamamlandı
7	Sistem kaynak kullanımını anlık görüntüleyiniz.			☐ Tamamlandı
8	Ağ arayüzlerini ve IP adreslerini listeleyiniz.			☐ Tamamlandı
9	Öğretmeninizin belirlediği hedef adrese bağlantı testi yapınız.			☐ Tamamlandı
10	Öğretmeninizin belirlediği alan adı için IP adresi sorgulaması yapınız.			☐ Tamamlandı
11	Yerel sisteminizde dinlemede olan açık portları listeleyiniz.			☐ Tamamlandı
12	Mevcut kullanıcıya ait zamanlanmış görevleri listeleyiniz.			☐ Tamamlandı
13	Çalışan servisleri görüntüleyiniz.			☐ Tamamlandı
14	Bulgularınızı içeren kısa bir rapor dosyası oluşturunuz.			☐ Tamamlandı
15	Oluşturduğunuz rapor dosyasının izinlerini görüntüleyiniz.			☐ Tamamlandı

Rapor Bölümü: Uygulama adımlarında elde ettiğiniz verileri kullanarak aşağıdaki soruları yanıtlayınız.

1. Sistemde en fazla kaynak kullanan süreç hangisidir?

   .....

2. .....

   ...Bellek veya disk kullanımında dikkat çeken bir durum var mı?

   .....

   .....

3. Ağ bağlantısının çalışıp çalışmadığını hangi veriye göre belirlediniz?

   .....

   .....

4. Yerel sistemde dinlemede olan portlardan biri hangisidir?

.....

.....

5. Zamanlanmış görev veya çalışan servislerde dikkat çeken bir bulgu var mı?

.....

.....

6. Sistemin genel durumunu tek cümleyle özetleyiniz.

.....

.....

Değerlendirme

Çalışmanız öğretmeniniz tarafından kontrol listesine göre değerlendirilecektir. Çalışmanızı yaparken buradaki ölçütleri dikkate alınız. Kontrol listesi formuna ulaşmak için karekodu okutunuz. Dijital yayınlarda karekodun üstüne tıklayarak içeriğe ulaşabilirsiniz.

3.1.4.8. Açık Kaynak Kodlu İşletim Sistemi Editörleri

Metin dosyaları oluşturmak ve düzenlemek için grafiksel arayüze ihtiyaç duymadan doğrudan terminal üzerinden çalışan editörler kullanılır. Bu editörler özellikle sunucu ortamlarında, uzak sistem yönetiminde ve betik dosyası hazırlamada vazgeçilmezdir. En yaygın kullanılan terminal tabanlı metin editörleri **nano** ve **vim**'dir.

Nano Metin Editörü

Nano, kullanımı kolay ve yeni başlayanlar için uygun bir terminal metin editörüdür. Editör açıkken ekranın alt kısmında kullanılabilecek kısayollar görüntülenir. Bir dosyayı nano ile açmak veya oluşturmak için terminale **nano [dosya_adı]** komutu yazılır.

Nano editöründe en sık kullanılan kısayollar Tablo 3.16'da verilmiştir.

Tablo 3.16: Nano Editörü Kısayolları

Kısayol	İşlev
Ctrl + O	Dosyayı kaydeder.
Ctrl + X	Editörden çıkar.
Ctrl + W	Dosya içinde metin arar.
Ctrl + K	İmlecin bulunduğu satırı keser.
Ctrl + U	Kesilen satırı yapıştırır.
Ctrl + G	Yardım ekranını açar.

9. ÖRNEK UYGULAMA

Nano editörünün kullanımını aşağıdaki adımları izleyerek gerçekleştiriniz.

1. Adım: Uçbirim öykünücüsünü açınız.

2. Adım: **nano** komutuyla **notlar.txt** adlı yeni bir dosya oluşturunuz (Görsel 3.37).

```
┌──(siber㉿siber)-[~]
└─$ nano notlar.txt
```

Görsel 3.37: Nano editörünün açılması

3. Adım: Editör açıldıktan sonra Görsel 3.38'deki metni giriniz.

```
 GNU nano 8.7.1                    notlar.txt *
Siber güvenlik notu: Yetkisiz erişim girişimiz tespit edildi.
Tarih: 2026-06-14
```

Görsel 3.38: Nano editöründe metin girişi

4. Adım: **Ctrl+O** ve **Enter** tuşlarıyla dosyayı kaydediniz. Ardından **Ctrl+X** ile editörden çıkınız.

5. Adım: **cat** komutuyla dosya içeriğini görüntüleyerek kaydetme işlemini doğrulayınız (Görsel 3.39).

```
┌──(siber㉿siber)-[~]
└─$ cat notlar.txt
Siber güvenlik notu: Yetkisiz erişim girişimiz tespit edildi.
Tarih: 2026-06-14
```

Görsel 3.39: Dosya içeriğinin doğrulanması

Vim Metin Editörü

Vim, güçlü özelliklere sahip ileri düzey bir terminal metin editörüdür. Sunucu ortamlarında ve sistem yönetiminde varsayılan editör olarak yaygın biçimde kullanılır. Bir dosyayı vim ile açmak veya oluşturmak için terminale **vim [dosya_adı]** komutu yazılır.

Vim üç farklı modda çalışır.

1. **Komut Modu:** Vim açıldığında bu modda başlar. Dosya içinde gezinme, silme, kopyalama ve yapıştırma işlemleri bu modda yapılır. Diğer modlardan komut moduna dönmek için **Esc** tuşuna basılır.
2. **Ekleme Modu:** Dosyaya metin eklemek için kullanılır. Komut modundan ekleme moduna geçmek için **i** tuşuna basılır.
3. **Satır Modu:** Komut modunda **:** (iki nokta) yazılarak girilir. Dosyayı kaydetme ve çıkış işlemleri bu modda yapılır.

Vim editöründe en sık kullanılan komutlar Tablo 3.17'de verilmiştir.

Tablo 3.17: Vim Editörü Komutları

Komut	İşlev
i	Ekleme moduna geçer.
Esc	Komut moduna döner.
:w	Dosyayı kaydeder.
:q	Editörden çıkar.
:wq	Kaydeder ve çıkar.
:q!	Kaydetmeden zorla çıkar.
dd	İmlecin bulunduğu satırı siler.
yy	İmlecin bulunduğu satırı kopyalar.
p	Kopyalanan satırı yapıştırır.

10. ÖRNEK UYGULAMA

Vim editörünün kullanımını aşağıdaki adımları izleyerek gerçekleştiriniz.

1. Adım: Uçbirim öykünücüsünü açınız.

2. Adım: **vim** komutuyla **rapor.txt** adlı yeni bir dosya oluşturunuz (Görsel 3.40).

```
┌──(siber㉿siber)-[~]
└─$ vim rapor.txt
```

Görsel 3.40: Vim editörünün açılması

3. Adım: **i** tuşuna basarak Vim ekleme moduna geçiniz ve editörde **Sistem taraması tamamlandı. Açık port: 22 (SSH)** metnini giriniz (Görsel 3.41).

```
Sistem taraması tamamlandı.
Açık port: 22 (SSH)
```

Görsel 3.41: Vim ekleme modunda metin girişi

4. Adım: Esc tuşuna basarak komut moduna dönünüz. **:wq** yazıp Enter tuşuna basarak dosyayı kaydedip çıkınız.

5. Adım: **cat** komutuyla dosya içeriğini görüntüleyerek kaydetme işlemini doğrulayınız (Görsel 3.42).

```
┌──(siber㉿siber)-[~]
└─$ cat rapor.txt
Sistem taraması tamamlandı.
Açık port: 22 (SSH)
```

Görsel 3.42: Dosya içeriğinin doğrulanması

SIRA SİZDE

Siber güvenlik odaklı açık kaynak kodlu işletim sistemi dağıtımı kurulu sisteminizde bir sistem inceleme raporu hazırlamanız istenmektedir. Raporu önce **nano** editörüyle oluşturacak, ardından **vim** editörüyle güncelleyeceksiniz.

Verilen görevleri terminalde gerçekleştiriniz ve kullandığınız komutları tabloya yazınız.

No.	Görev	Kullandığım Komut
1	**nano** komutuyla **tarama_raporu.txt** adlı yeni bir dosya oluşturunuz.	
2	Dosyaya sistem adı, tarih ve en az iki satır gözlem notu giriniz. Kaydedip çıkınız.	
3	**cat** komutuyla dosya içeriğini görüntüleyiniz.	
4	**vim** komutuyla aynı dosyayı açınız ve sonuna bir satır daha ekleyiniz. Kaydedip çıkınız.	
5	**cat** komutuyla dosyanın güncel içeriğini görüntüleyerek değişikliği doğrulayınız.	

3.1.4.9. Betik Dosyası

Betik (Script), terminalde tek tek çalıştırılan komutların bir dosyaya yazılarak otomatik biçimde sırayla çalıştırılmasını sağlayan metin dosyasıdır. Açık kaynak kodlu işletim sisteminde betik dosyaları genellikle **.sh** uzantısıyla kaydedilir. Betikler; sistem bilgilerini görüntüleme, rapor oluşturma, dosya işlemlerini otomatikleştirme ve tekrarlanan görevleri daha hızlı gerçekleştirme amacıyla kullanılabilir.

Basit bir betik dosyası oluşturmak için öncelikle nano veya vim gibi bir metin editörüyle dosya hazırlanır. Daha sonra dosya çalıştırılabilir hâle getirilir ve terminal üzerinden çalıştırılır.

Temel betik komutları Tablo 3.18'de verilmiştir.

Tablo 3.18: Basit Betik Dosyasında Kullanılan İfadeler ve Komutlar

Komut	Açıklama	Örnek
#!/bin/bash	Betiğin Bash kabuğuyla çalıştırılacağını belirtir. Genellikle betik dosyasının ilk satırına yazılır.	#!/bin/bash
echo	Ekrana metin yazdırır.	echo "Merhaba"
tee -a [dosya]	Çıktıyı hem ekrana yazdırır hem de belirtilen dosyaya yazdırır.	echo "Merhaba" | tee -a rapor.log
$(komut)	Bir komutun çıktısını başka bir komutun içinde kullanmayı sağlar.	echo "$(hostname)"
chmod +x	Betik dosyasını çalıştırılabilir hâle getirir.	chmod +x betik.sh
./[dosya]	Bulunulan dizindeki betik dosyasını çalıştırır.	./betik.sh

11. ÖRNEK UYGULAMA

Nano editörüyle betik dosyası oluşturma, düzenleme ve çalıştırma işlemlerini aşağıdaki adımları izleyerek gerçekleştiriniz.

1. Adım: Uçbirim öykünücüsünü açınız.

2. Adım: **nano** komutuyla **kontrol.sh** adlı bir betik dosyası oluşturunuz (Görsel 3.43).

```
┌──(siber㉿siber)-[~]
└─$ nano kontrol.sh
```

Görsel 3.43: Betik dosyasının oluşturulması

3. Adım: Dosyaya aşağıdaki Görsel 3.44'teki satırları giriniz ve Ctrl+O, Enter, Ctrl+X ile kaydedip çıkınız.

```
  GNU nano 8.7.1                    kontrol.sh
#!/bin/bash
echo "Sistem adı: $(hostname)"
echo "Tarih: $(date)"
echo "Kullanıcı: $(whoami)"
```

Görsel 3.44: Betik dosyasına içerik girişi

4. Adım: **chmod** komutuyla betik dosyasını çalıştırılabilir hâle getiriniz (Görsel 3.45).

```
┌──(siber㉿siber)-[~]
└─$ chmod +x kontrol.sh
```

Görsel 3.45: Betik dosyasının çalıştırılabilir hâle getirilmesi

5. Adım: Betiği **./kontrol.sh** komutuyla çalıştırınız ve çıktıyı inceleyiniz (Görsel 3.46).

```
┌──(siber㉿siber)-[~]
└─$ ./kontrol.sh
Sistem adı: siber
Tarih: Paz 14 Haz 2026 18:46:44 +03
Kullanıcı: siber
```

Görsel 3.46: Betik dosyasının çalıştırılması ve çıktısı

SIRA SİZDE

Siber güvenlik odaklı açık kaynak kodlu işletim sistemi dağıtımı kurulu sisteminizde her çalıştırıldığında sistem bilgilerini ekrana yazdıran ve **/tmp/sistem_rapor.log** dosyasına kaydeden bir betik dosyası oluşturmanız istenmektedir. Verilen görevleri terminalde gerçekleştiriniz ve kullandığınız komutları tabloya yazınız. Tüm adımların ekran görüntülerini alarak dijital bir içerik oluşturunuz ve sınıfta paylaşınız.

No.	Görev	Kullandığım Komut
1	**nano** komutuyla **sistem_bilgi.sh** adlı bir betik dosyası oluşturunuz.	
2	Betik dosyasına sistem adı, tarih, kullanıcı adı, çalışma süresi bilgisini ekrana yazdıran ve **sistem_rapor.log** dosyasına kaydeden komutları giriniz. Kaydedip çıkınız.	
3	Betik dosyasını çalıştırılabilir hâle getiriniz.	
4	Betiği çalıştırarak çıktıyı inceleyiniz.	
5	Log dosyasının içeriğini görüntüleyiniz.	
6	Gerçekleştirdiğiniz tüm adımların ekran görüntülerini alarak dijital bir içerik oluşturunuz ve sınıfta paylaşınız.	

3.1.5. Kapalı Kaynak Kodlu İşletim Sistemleri

Kişisel bilgisayarlarda yaygın olarak kullanılan kapalı kaynak kodlu işletim sistem; grafik arayüzü, geniş uygulama desteği ve kullanıcı dostu yapısıyla öne çıkar. Donanım ve yazılım üreticileriyle geniş bir ekosistem oluşturur. Hem bireysel kullanıcılara hem de kurumsal ortamlara yönelik sürümleri bulunmaktadır.

Kapalı kaynak kodlu işletim sisteminin temel özellikleri şunlardır:

Grafiksel Kullanıcı Arayüzü: Masaüstü, simgeler, pencereler ve menüler aracılığıyla kullanımı kolaylaştırır.

Çok Kullanıcılı Yapı: Aynı bilgisayarda birden fazla kullanıcı hesabı oluşturulabilir. Böylece kullanıcı kendi ayarlarını ve dosyalarını ayrı tutar.

Geniş Uygulama Desteği: Oyunlardan ofis yazılımlarına, mühendislik araçlarından güvenlik yazılımlarına kadar geniş bir uygulama yelpazesi desteklenir.

Güvenlik Araçları: Yerleşik güvenlik duvarı, virüs koruması, kullanıcı hesabı denetimi gibi araçlar sistemi korur.

Donanım Uyumluluğu: Geniş donanım desteği sayesinde farklı üreticilerin bileşenleriyle uyumlu çalışır.

Bu işletim sistemi, ilk sürümünden günümüze kadar önemli değişimler geçirmiştir. Her yeni sürüm, kullanıcı arayüzü, güvenlik, performans ve donanım desteği açısından önceki sürüme göre gelişimler sunmuştur. Yıllar içinde hem bireysel kullanıcılara hem de kurumsal ortamlara yönelik farklı sürümler geliştirilmiştir. Güncel sürümler; güvenlik, kararlılık, uygulama uyumluluğu ve donanım desteği açısından önceki sürümlere göre geliştirilmiş özellikler sunmaktadır.

ARAŞTIRMA

Yaygın olarak kullanılan kapalı kaynak kodlu işletim sisteminin tarihsel gelişimini araştırınız. İlk sürümden günümüze kadar çıkan sürümleri, çıkış yıllarını ve her sürümün öne çıkan özelliğini aşağıdaki tabloya yazınız.

Sürüm Adı	Çıkış Yılı	Öne Çıkan Özellik
Kaynak (site adı / erişim tarihi): _____		

Açık Kaynak Kodlu ve Kapalı Kaynak Kodlu İşletim Sistemleri Karşılaştırması

Açık kaynak kodlu ve kapalı kaynak kodlu işletim sistemleri, farklı felsefeler üzerine inşa edilmiştir. İkisi de geniş kullanıcı kitlesine hitap etmekle birlikte kaynak yapısı, lisanslama, güvenlik anlayışı ve kullanım senaryoları

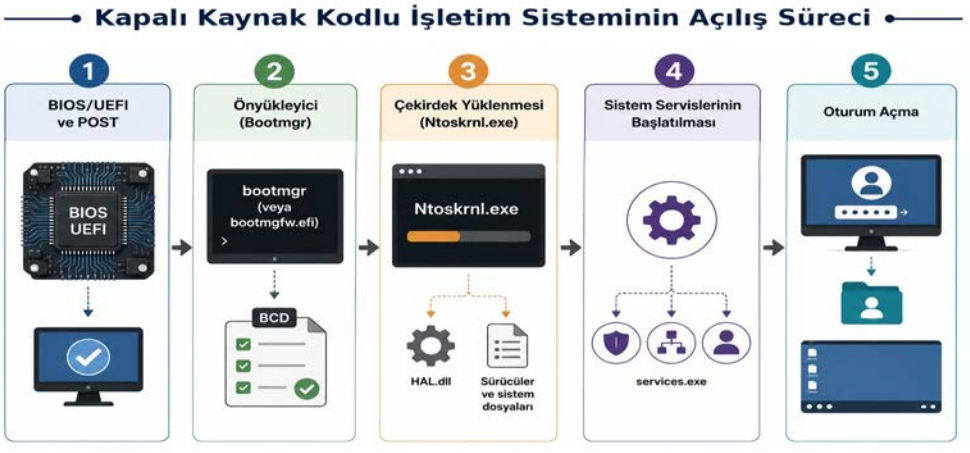
bakımından birbirinden belirgin biçimde ayrışır. Temel farklılıklar Tablo 3.19'da verilmiştir.

Tablo 3.19: Açık Kaynak Kodlu ve Kapalı Kaynak Kodlu İşletim Sistemi Karşılaştırması

Özellik	Açık Kaynak Kodlu	Kapalı Kaynak Kodlu
Lisans	Çoğu dağıtım ücretsiz ve özgürce dağıtılabilir.	Genellikle lisanslı olarak kullanılır.
Kullanıcı arayüzü	Komut satırı güçlüdür; farklı masaüstü ortamları kullanılabilir.	Grafik arayüz ağırlıklıdır; komut satırı ve betik dili desteği vardır.
Güncelleme yönetimi	Dağıtıma göre değişir; genellikle kullanıcı veya sistem yöneticisi tarafından yönetilir.	Otomatik güncelleme desteği vardır; kullanıcı veya sistem yöneticisi tarafından yapılandırılabilir.
Güvenlik yaklaşımı	Yetkilendirme, paket depoları ve açık kaynak denetimiyle güçlü güvenlik yapısı sunar.	Geniş kullanıcı kitlesi nedeniyle sık hedef alınır; yerleşik güvenlik araçlarıyla koruma sağlar.
Uygulama desteği	Sunucu, geliştirici, siber güvenlik ve teknik araçlarda güçlüdür.	Ofis, oyun, ticari yazılımlar ve son kullanıcı uygulamalarında geniş desteğe sahiptir.
Donanım sürücüsü	Yaygın donanımlar için destek sunar; bazı özel donanımlarda ek yapılandırma gerekebilir.	Çok geniş donanım ve üretici sürücü desteğine sahiptir.

3.1.5.1. Kapalı Kaynak Kodlu İşletim Sisteminin Açılış Süreci

Kapalı kaynak kodlu işletim sisteminin açılış süreci, bilgisayar başlatıldığında işletim sisteminin belleğe yüklenip kullanıma hazır hâle gelmesini ifade eder. Açık kaynak kodlu işletim sisteminin açılış süreciyle benzer aşamalar izlense de kullandığı bileşenler ve dosya adları farklıdır. Açılış süreci genel olarak şu aşamalardan oluşur (Görsel 3.47):



Görsel 3.47: Kapalı kaynak kodlu işletim sisteminin açılış süreci

1. **BIOS/UEFI ve POST:** Güç düğmesine basıldığında BIOS/UEFI devreye girer ve donanım bileşenlerini denetler (POST). Sorun yoksa önyükleyiciyi arar.

2. **Önyükleyici (Bootmgr):** BIOS sistemlerde **bootmgr,** UEFI sistemlerde **bootmgfw.efi** çalışır. Önyükleyici, **BCD [Boot Configuration Data (Önyükleme Yapılandırma Verisi)]** dosyasını okur ve hangi işletim sisteminin başlatılacağını belirler. Ardından çekirdek yükleyiciyi devreye alır.
3. **Çekirdek Yüklenmesi (Ntoskrnl.exe):** Çekirdek dosyası olan **Ntoskrnl.exe** belleğe yüklenir. Çekirdek; donanım sürücülerini, kayıt defterini ve sistem dosyalarını yükler. **HAL.dll [Hardware Abstraction Layer (Donanım Soyutlama Katmanı)]** işletim sisteminin donanımla iletişimini sağlar.
4. **Sistem Servislerinin Başlatılması:** Çekirdek, **services.exe** aracılığıyla sistem servislerini (güvenlik, ağ yönetimi, kullanıcı oturumu vb.) başlatır.
5. **Oturum Açma: winlogon.exe** süreci kullanıcıdan kimlik bilgilerini ister. Doğrulama tamamlandığında kullanıcı profili yüklenir ve masaüstü ortamı hazır hâle gelir.

BİLGİ KUTUSU : Açık Kaynak Kodlu ve Kapalı Kaynak Kodlu İşletim Sistemlerinin Açılış Süreçleri

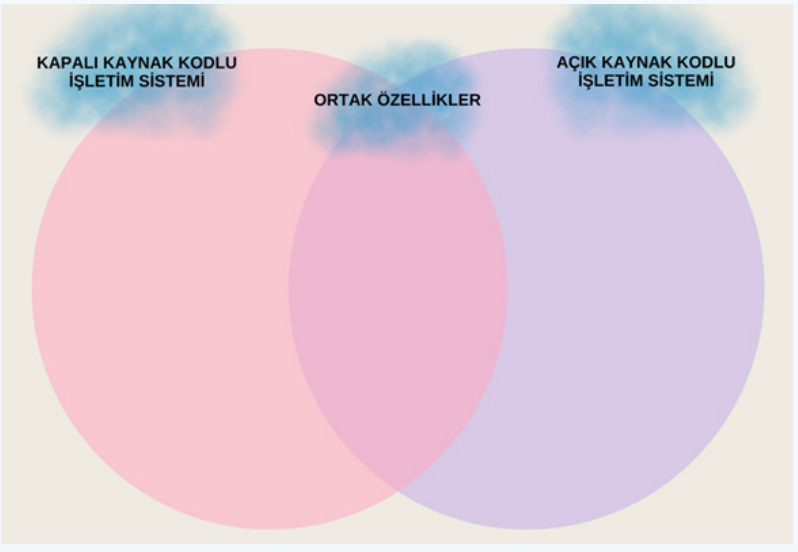
Açık kaynak kodlu işletim sisteminin açılış sürecinde **GRUB** önyükleyici, **vmlinuz** çekirdek ve **systemd** servis yöneticisi görevini üstlenirken kapalı kaynak kodlu işletim sisteminde bu görevleri sırasıyla **bootmgr, Ntoskrnl.exe** ve **services.exe** üstlenir. Her iki sistem de BIOS/UEFI ile başlar ve benzer aşamalardan geçer; ancak kullandıkları bileşenler ve dosya adları farklıdır.

SIRA SİZDE

Açık kaynak kodlu ve kapalı kaynak kodlu işletim sistemlerinin açılış süreçlerini karşılaştırınız. Aşağıda verilen ifadelerin numaralarını Venn şemasında uygun bölümlere yerleştiriniz.

No.	İfadeler
1	BIOS/UEFI ve POST aşaması bulunur.
2	Bootmgr veya bootmgfw.efi kullanılır.
3	GRUB önyükleyicisi kullanılabilir.
4	İşletim sistemi çekirdeği belleğe yüklenir.
5	BCD dosyası başlatılacak işletim sistemini belirlemede kullanılır.
6	vmlinuz çekirdek imajı kullanılır.
7	Ntoskrnl.exe çekirdek dosyası olarak görev yapar.
8	Sistem servisleri başlatılır.
9	systemd servis yönetimini üstlenir.

No.	İfadeler
10	services.exe sistem servislerinin başlatılmasında görev alır.
11	Kullanıcı oturum açma ekranına ulaşır.
12	winlogon.exe oturum açma sürecinde görev alır.



3.1.5.2. Kapalı Kaynak Kodlu İşletim Sistemi Dosya Sistemi

Dosya sistemi, depolama birimindeki verilerin saklanmasını ve düzenlenmesini yönetir. Her sürücünün kendi kök dizini bulunur (örneğin **C:\, D:** gibi). İşletim sisteminin kurulu olduğu sürücü genellikle **C:** sürücüsüdür. Tüm sistem dosyaları, program dosyaları ve kullanıcı verileri bu dizin altında organize edilir. Kapalı kaynak kodlu işletim sistemlerinde kullanılan başlıca dosya sistemleri şunlardır:

NTFS [New Technology File System (Yeni Teknoloji Dosya Sistemi)]: Modern sürümlerde kullanılan varsayılan dosya sistemidir. Şifreleme, erişim denetimi, günlükleme (journaling) ve büyük dosya desteği sunar.

FAT32 [File Allocation Table 32 (32-bit Dosya Ayırma Tablosu)]: Eski sistemlerle geniş uyumluluk sağlayan dosya sistemidir. Tek bir dosya için 4 GB boyut sınırı bulunur. USB bellekler ve taşınabilir depolama aygıtlarında hâlâ kullanılmaktadır.

exFAT [Extended File Allocation Table (Genişletilmiş Dosya Ayırma Tablosu)]: FAT32'nin dosya boyutu sınırlamalarını aşmak için geliştirilmiştir. Büyük dosya desteği vardır ve özellikle SD kart ve USB belleklerde yaygın olarak kullanılır.

BİLGİ KUTUSU : ReFS

Sunucu ve kurumsal ortamlar için geliştirilen **ReFS [Re**silient **F**ile **S**ystem **(Dayanıklı Dosya Sistemi)]**, veri bütünlüğü denetimi ve otomatik hata düzeltme özellikleriyle öne çıkar. Masaüstü sistemlerde yaygın kullanılmaz. Büyük ölçekli depolama ve sunucu altyapılarında tercih edilir.

Kapalı kaynak kodlu işletim sisteminde bulunan temel dizin yapısı Tablo 3.20'de gösterilmektedir.

Tablo 3.20: Kapalı Kaynak Kodlu İşletim Sisteminde Temel Dizinler

Dizin	Açıklama
C:	İşletim sisteminin genellikle kurulu olduğu sürücünün kök dizinidir.
C:\Windows	İşletim sisteminin çalışması için gerekli temel dosyaların bulunduğu dizindir.
C:\Windows\System32	Sistem dosyaları, sürücüler ve temel kütüphanelerin (.dll) bulunduğu dizindir.
C:\Windows\Logs	Sistem ve uygulama günlük (log) dosyalarının tutulduğu dizindir.
C:\Windows\Temp	Sistem ve uygulamalar tarafından kullanılan geçici dosyaların bulunduğu dizindir.
C:\Users	Kullanıcı hesaplarının kişisel dizinlerini içerir. Her kullanıcı için ayrı bir alt dizin oluşturulur.
C:\Program Files	64-bit programların varsayılan olarak kurulduğu dizindir.
C:\Program Files (x86)	32-bit programların varsayılan olarak kurulduğu dizindir.
C:\ProgramData	Tüm kullanıcılar tarafından kullanılan uygulama verilerinin tutulduğu ortak dizindir.
C:\Recovery	Sistem kurtarma işlemlerine ait dosyaların bulunabileceği dizindir.
C:\Windows\System32\winevt\Logs	Olay Görüntüleyicisi (Event Viewer) günlüklerinin (.evtx) tutulduğu dizindir.

SİBER GÜVENLİK PENCERESİ

Siber güvenlik analizlerinde bazı dizinler özellikle dikkat gerektirir.

- **C:\Windows\System32:** Kötü amaçlı yazılımlar meşru sistem dosyalarını taklit etmek için bu dizini hedef alır.
- **C:\Windows\Logs** ve **C:\Windows\System32\winevt\Logs**: Saldırı tespiti ve adli analizde incelenen günlük dosyaları burada tutulur.
- **C:\Users\[Kullanıcı]\AppData:** Tarayıcı geçmişi, uygulama verileri ve oturum bilgileri bu dizinde saklanır; kötü amaçlı yazılımlar sıklıkla bu dizini hedef alır.
- **C:\Windows\Temp:** Zararlı yazılımlar geçici dosyalarını bu dizine bırakabilir; düzenli temizlik önerilir.

3.1.5.3. Kapalı Kaynak Kodlu İşletim Sistemi Kurulumu

Kapalı kaynak kodlu işletim sistemi kurulumu, ISO dosyasının indirilmesi ve önyüklenebilir bir USB bellek hazırlanmasıyla başlar. Kurulum işlemine başlamadan önce bilgisayarın gerekli sistem gereksinimlerini karşıladığından emin olunmalıdır.

BİLGİ KUTUSU : Sistem Gereksinimleri

Güncel sürümün kurulabilmesi için sistemde 64-bit işlemci, en az 4 GB RAM, 64 GB depolama alanı, UEFI önyükleme desteği ve TPM [Trusted Platform Module (Güvenilir Platform Modülü)] 2.0 desteği bulunmalıdır. TPM, cihaz güvenliği için kullanılan özel bir donanım bileşenidir. Şifreleme anahtarlarının korunması, cihaz kimliğinin doğrulanması ve güvenli açılış süreçlerinde görev alır.

12. ÖRNEK UYGULAMA

Aşağıdaki adımları izleyerek kapalı kaynak kodlu işletim sistemi kurulumunu gerçekleştiriniz.

1. Adım: Geliştirici firmanın resmî web sitesinden işletim sistemine ait ISO dosyasını indiriniz.

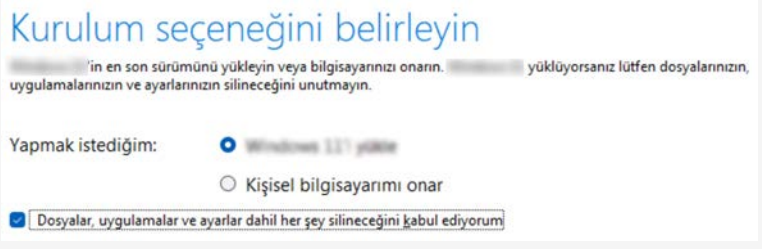
2. Adım: İndirilen ISO dosyasını kullanarak önyüklenebilir bir USB bellek hazırlayınız.

3. Adım: Hazırladığınız USB belleği bilgisayara takarak yeniden başlatınız. BIOS/UEFI ayarlarına giriniz ve ilk açılış aygıtını USB olarak ayarlayınız. Ayar kaydedildikten sonra bilgisayar yeniden başlar ve kurulum ekranı açılır.

4. Adım: Kurulum ekranında dil ve klavye ayarlarını seçerek ilerleyiniz.

5. Adım: Ürün anahtarı ekranında, eğer lisansınız yoksa Ürün anahtarım yok seçeneğini tıklayınız.

6. Adım: Kurulum türü olarak 11'i yükle seçeneğini seçiniz (Görsel 3.48).

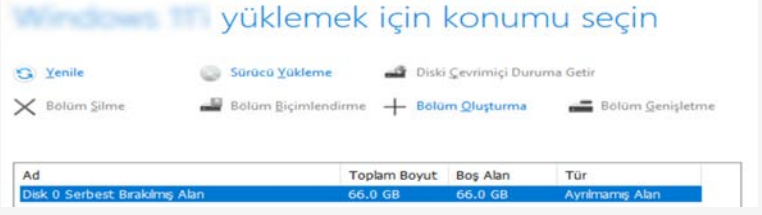


Görsel 3.48: Kurulum türü seçimi ekranı

7. Adım: Lisans koşullarını kabul ederek İleri düğmesine tıklayınız.

8. Adım: Kurulacak sürümü seçiniz. Lisansınıza uygun sürümü (Home, Pro vb.) seçerek İleri düğmesine tıklayınız.

9. Adım: Kurulumun yapılacağı diski seçiniz [Görsel 3.49 (Gerekirse Bölüm Oluşturma tıklanarak yeni bir bölüm oluşturulabilir.)].



Görsel 3.49: Disk seçim ekranı

10. Adım: Yüklemeye hazır ekranında kurulum özetini inceleyiniz ve Yükle düğmesine tıklayınız.

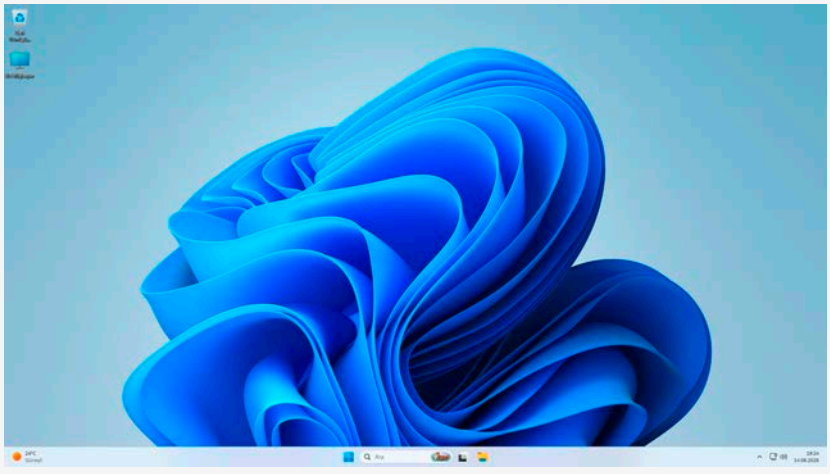
11. Adım: Kurulumun tamamlanmasını bekleyiniz. Bu sırada bilgisayar birkaç kez yeniden başlayacaktır.

12. Adım: Sistem yeniden başladıktan sonra ülke/bölge ve klavye düzeni seçimini yapınız.

13. Adım: Bilgisayara bir ad veriniz ve İleri düğmesine tıklayınız.

14. Adım: Hesap oluşturma ekranında çevrim içi hesap veya yerel hesap ile oturum açınız.

15. Adım: Gizlilik ayarlarını yapılandırınız, Kabul Et düğmesine tıklayınız ve masaüstünün yüklenmesini bekleyiniz (Görsel 3.50).



Görsel 3.50: Kapalı kaynak kodlu işletim sistemi masaüstü ekranı

5. ETKİNLİK

Etkinlik Adı	Kapalı Kaynak Kodlu İşletim Sistemi Kurulumu
Süre	40 dakika
Amaç	Kapalı kaynak kodlu işletim sisteminin kurulum sürecini adım adım uygulayarak sistemi kullanıma hazır hâle getirmek
Yönerge	Sınıfta gösterilen kurulum adımlarını izleyerek kapalı kaynak kodlu işletim sistemini kendiniz kurunuz. Her adımı tamamladığınızda Kontrol sütununa tik (✓) atarak işaretleyiniz.

Uygulama Adımları

No.	Görev	Kontrol
1	ISO dosyasını resmî web sitesinden indiriniz.	☐ Tamamlandı
2	Önyüklenebilir USB bellek hazırlayınız.	☐ Tamamlandı
3	BIOS/UEFI ayarlarından ilk açılış aygıtını USB olarak ayarlayınız.	☐ Tamamlandı

No.	Görev	Kontrol
4	Dil ve klavye ayarlarıyla kurulum sürümünü seçerek ilerleyiniz.	☐ Tamamlandı
5	Disk seçimi yaparak kurulumu başlatınız.	☐ Tamamlandı
6	Sürüme göre çevrim içi bir hesapla veya yerel hesap oluşturarak sisteme giriş yapınız.	☐ Tamamlandı
7	Gizlilik ayarlarını yapılandırınız.	☐ Tamamlandı
8	Kurulum tamamlandıktan sonra masaüstünü inceleyiniz. Görev çubuğunu, Başlat menüsünü ve sistem tepsisini gözlemleyiniz.	☐ Tamamlandı

Değerlendirme

Çalışmanız öğretmeniniz tarafından kontrol listesine göre değerlendirilecektir. Çalışmanızı yaparken buradaki ölçütleri dikkate alınız. Kontrol listesi formuna ulaşmak için karekodu okutunuz. Dijital yayınlarda karekodun üstüne tıklayarak içeriğe ulaşabilirsiniz.

Çalışmanızın öğrenme sürecinize katkısını değerlendirmek için öz değerlendirme formunu doldurunuz. Formu tamamladıktan sonra öğretmeninizle paylaşınız veya EBA Portfolyo'ya yükleyiniz. Öz değerlendirme formuna ulaşmak için karekodu okutunuz. Dijital yayınlarda karekodun üstüne tıklayarak içeriğe ulaşabilirsiniz.

3.1.5.4. Komut İstemi ve Temel Komutlar

Windows işletim sisteminde komut satırı arayüzüne **Komut İstemi [Command Prompt (CMD)]** adı verilir. Komut İstemi, **DOS**'un **[Disk Operating System (Disk İşletim Sistemi)]** mirasından gelen metin tabanlı bir arayüzdür. Grafik arayüz kullanılmadan sistem işlemlerinin gerçekleştirilebildiği bu ortam, Başlat menüsünde **cmd** yazılarak açılır.

Yardım ve Sistem Komutları

Açık kaynak kodlu işletim sisteminde olduğu gibi kapalı kaynak kodlu işletim sisteminde de bir komutun kullanımı hakkında bilgi almak için yerleşik yardım araçları kullanılır (Tablo 3.21).

Tablo 3.21: Yardım Komutları

Komut	Açıklama	Örnek
help	Kullanılabilecek komutların listesini görüntüler.	help
[komut] /?	Belirtilen komutun kullanım bilgisini gösterir.	dir /?

Bilgisayar adı, kullanıcı kimliği, işletim sistemi sürümü, donanım bilgileri gibi sistem bilgilerine ulaşmak için bilgi alma komutları kullanılır (Tablo 3.22).

Tablo 3.22: Sistem Bilgisi Komutları

Komut	Açıklama	Örnek
whoami	Etkin kullanıcı adını gösterir.	whoami
hostname	Bilgisayarın ağdaki adını gösterir.	hostname
ver	İşletim sistemi sürümünü gösterir.	ver
systeminfo	İşletim sistemi, donanım ve ağ bilgilerini gösterir.	systeminfo
date	Sistem tarihini gösterir ve değiştirmeye izin verir.	date
time	Sistem saatini gösterir ve değiştirmeye izin verir.	time
cls	Komut İstemi ekranını temizler.	cls

Dosya ve Klasör Yönetimi Komutları

Dosya ve klasörler üzerinde gezinme, oluşturma, kopyalama, taşıma, silme gibi işlemler için dosya ve klasör yönetimi komutları kullanılır (Tablo 3.23).

Tablo 3.23: Dosya ve Klasör Yönetimi Komutları

Komut	Açıklama	Örnek
dir	Bulunulan dizinin içeriğini listeler.	dir
cd [dizin]	Dizin değiştirir. cd .. bir üst dizine çıkar.	cd C:\Users
mkdir [ad]	Yeni klasör oluşturur.	mkdir proje
rmdir [ad]	Boş klasörü siler.	rmdir proje
copy [kaynak] [hedef]	Dosya kopyalar.	copy notlar.txt C:\Temp
move [kaynak] [hedef]	Dosya taşır veya yeniden adlandırır.	move notlar.txt C:\Temp
del [dosya]	Dosyayı siler.	del notlar.txt
ren [eski] [yeni]	Dosya veya klasörü yeniden adlandırır.	ren notlar.txt arsiv.txt
type [dosya]	Dosya içeriğini ekrana yazdırır.	type notlar.txt
echo [metin]	Ekrana metin yazdırır veya dosyaya yazar.	echo Merhaba > notlar.txt



KONTROL NOKTASI

del komutuyla silinen dosyalar Geri Dönüşüm Kutusu'na gönderilmez, kalıcı olarak silinir. Silme işlemi yapmadan önce doğru dizinde olduğunuzu **dir** komutuyla doğrulayınız.

Dosya İndirme Komutu

Komut İstemi üzerinden internetten dosya indirmek için **curl** komutu kullanılır. Açık kaynak kodlu işletim sisteminde olduğu gibi kapalı kaynak kodlu işletim sisteminde de **curl** kullanılabilir (Tablo 3.24).

Tablo 3.24: Dosya İndirme Komutu

Komut	Açıklama	Örnek
curl -O [URL]	Belirtilen adresten dosya indirir.	curl -O https://example.com/index.html

13. ÖRNEK UYGULAMA

Aşağıdaki adımları izleyerek Komut İstemi'nde yardım, sistem bilgisi ve dosya/klasör yönetimi komutlarını uygulayınız.

1. Adım: Başlat menüsüne cmd yazarak Komut İstemi'ni açınız.

2. Adım: **help** komutunu çalıştırarak kullanılabilecek komutların listesini görüntüleyiniz (Görsel 3.51).

```
C:\Windows\System32>help
For more information on a specific command, type HELP command-name
ASSOC          Displays or modifies file extension associations.
ATTRIB         Displays or changes file attributes.
BREAK          Sets or clears extended CTRL+C checking.
BCDEDIT        Sets properties in boot database to control boot loading.
CACLS          Displays or modifies access control lists (ACLs) of files.
CALL           Calls one batch program from another.
CD             Displays the name of or changes the current directory.
CHCP           Displays or sets the active code page number.
CHDIR          Displays the name of or changes the current directory.
CHKDSK         Checks a disk and displays a status report.
```

Görsel 3.51: help komutu kullanımı

3. Adım: **dir /?** komutuyla dir komutunun kısa kullanım bilgisini görüntüleyiniz (Görsel 3.52).

```
C:\Windows\System32>dir /?
Displays a list of files and subdirectories in a directory.

DIR [drive:][path][filename] [/A[[:]attributes]] [/B] [/C] [/D] [/L] [/N]
  [/O[[:]sortorder]] [/P] [/Q] [/R] [/S] [/T[[:]timefield]] [/W] [/X] [/4]

  [drive:][path][filename]
              Specifies drive, directory, and/or files to list.

  /A          Displays files with specified attributes.
  attributes   D  Directories                R  Read-only files
               H  Hidden files               A  Files ready for archiving
               S  System files               I  Not content indexed files
```

Görsel 3.52: dir komutunun yardım bilgisi

4. Adım: **whoami** ve **hostname** komutlarını çalıştırarak sistem bilgilerini görüntüleyiniz (Görsel 3.53).

```
C:\Windows\System32>whoami
siber\siber

C:\Windows\System32>hostname
siber
```

Görsel 3.53: Sistem bilgilerinin görüntülenmesi

5. Adım: **cd** komutuyla C:\ dizinine geçiniz ve **dir** komutuyla içeriğini listeleyiniz (Görsel 3.54).

```
C:\Windows\System32>cd C:\

C:\>dir
 Volume in drive C has no label.
 Volume Serial Number is B098-C71D

 Directory of C:\

07.03.2026  02:50    <DIR>          inetpub
01.04.2024  11:45    <DIR>          PerfLogs
06.06.2026  18:33    <DIR>          Program Files
18.05.2026  06:12    <DIR>          Program Files (x86)
04.06.2026  20:44    <DIR>          Temp
17.05.2026  21:38    <DIR>          Users
04.06.2026  18:48    <DIR>          Windows
               0 File(s)              0 bytes
               7 Dir(s)  52.982.738.944 bytes free
```

Görsel 3.54: Kök dizin içeriğinin görüntülenmesi

6. Adım: **mkdir** komutuyla **C:\Temp** klasörünü oluşturunuz, **C:\Temp** klasörünün içine **echo** komutuyla **notlar.txt** adlı dosya oluşturarak dosyaya **Sistem ve Ağ Temelleri Notları** metnini ekleyiniz (Görsel 3.55).

```
C:\>mkdir C:\Temp

C:\>cd C:\Temp

C:\Temp>echo Sistem ve Ağ Temelleri Notları > notlar.txt
```

Görsel 3.55: Klasör ve dosya oluşturma uygulaması

7. Adım: **type** komutuyla **notlar.txt** dosyasının içeriğini görüntüleyiniz (Görsel 3.56).

```
C:\Temp>type notlar.txt
Sistem ve Ağ Temelleri Notları
```

Görsel 3.56: Oluşturulan dosya içeriğinin görüntülenmesi

8. Adım: **copy** komutuyla **notlar.txt** dosyasını **arsiv.txt** isimli dosyaya kopyalayınız (Görsel 3.57).

```
C:\Temp>copy notlar.txt arsiv.txt
        1 file(s) copied.
```

Görsel 3.57: Dosya kopyalama uygulaması

9. Adım: **curl -O** komutuyla **C:\Temp** dizini içerisine **https://example.com/index.html** adresinden örnek bir dosya indiriniz (Görsel 3.58).

```
C:\Temp>curl -O https://example.com/index.html
  % Total    % Received % Xferd  Average Speed  Time    Time    Time   Current
                                  Dload  Upload  Total   Spent   Left   Speed
100    559   0    559   0      0    299      0           00:01           301
```

Görsel 3.58: curl -O komutunun kullanımı

10. Adım: C:\Temp dizin içeriğini listeleyiniz (Görsel 3.59).

```
C:\Temp>dir
 Volume in drive C has no label.
 Volume Serial Number is B098-C71D

 Directory of C:\Temp

14.06.2026  20:12    <DIR>          .
14.06.2026  20:10                33 arsiv.txt
14.06.2026  20:12               559 index.html
14.06.2026  20:10                33 notlar.txt
               3 File(s)            625 bytes
               1 Dir(s)  50.064.838.656 bytes free
```

Görsel 3.59: C:\Temp dizin içeriğinin görüntülenmesi

SIRA SİZDE

Açık kaynak kodlu işletim sistemindeki çalışmalarınıza benzer şekilde kapalı kaynak kodlu işletim sisteminde de bir proje klasörü oluşturmanız, dosyalar hazırlamanız ve sistem bilgilerini incelemeniz istenmektedir.

Verilen görevleri Komut İstemi'nde gerçekleştiriniz ve kullandığınız komutları tabloya yazınız.

No.	Görev	Kullandığım Komut
1	**copy** komutunun kısa kullanım bilgisini görüntüleyiniz.	
2	Etkin kullanıcı adını ve bilgisayar adını görüntüleyiniz.	
3	**C:\Okul** adlı yeni bir klasör oluşturunuz.	
4	**C:\Okul** dizinine geçiniz.	
5	**odev.txt** adlı bir dosya oluşturunuz ve içine **İşletim Sistemleri** metnini ekleyiniz.	
6	Dosya içeriğini görüntüleyiniz.	
7	**odev.txt** dosyasını **teslim.txt** olarak kopyalayınız.	
8	Aynı dizin içerisine **https://example.com/test.txt** adresinden dosya indiriniz.	
9	Dizin içeriğini listeleyiniz.	

Kullanıcı ve Grup Yönetimi Komutları

Kapalı kaynak kodlu işletim sisteminde kullanıcı ve grup yönetimi **net** komutu aracılığıyla Komut İstemi üzerinden gerçekleştirilebilir. Sisteme kimlerin erişebileceği ve hangi gruplara dâhil olacağı bu komutlarla yönetilir (Tablo 3.25).

Tablo 3.25: Kullanıcı ve Grup Yönetimi Komutları

Komut	Açıklama	Örnek
net user	Sistemdeki kullanıcıları listeler.	net user
net user [ad] [parola] /add	Yeni kullanıcı oluşturur.	net user ogrenci 1234 /add
net user [ad] /delete	Kullanıcıyı siler.	net user ogrenci /delete
net localgroup	Sistemdeki grupları listeler.	net localgroup
net localgroup [grup] [kullanıcı] /add	Kullanıcıyı gruba ekler.	net localgroup Administrators ogrenci /add

Süreç Yönetimi Komutları

Çalışan her program bir süreç olarak yönetilir. Açık kaynak kodlu işletim sistemindeki **ps** ve **kill** komutlarına benzer şekilde **tasklist** ve **taskkill** komutları kullanılır (Tablo 3.26).

Tablo 3.26: Süreç Yönetimi Komutları

Komut	Açıklama	Örnek
tasklist	Çalışan süreçleri listeler.	tasklist
taskkill /PID [numara]	Belirtilen PID'ye sahip süreci sonlandırır.	taskkill /PID 1234
taskkill /IM [ad]	Belirtilen addaki süreci sonlandırır.	taskkill /IM notepad.exe

BİLGİ KUTUSU : Yönetici Yetkisiyle Çalıştırma

Kullanıcı oluşturma, silme, zamanlanmış görev oluşturma gibi sistem düzeyindeki işlemler yönetici yetkisi gerektirir. Komut İstemi'ni yönetici yetkisiyle açmak için Başlat menüsüne **cmd** yazınız, sağ tıklayarak **Yönetici olarak çalıştır** seçeneğini tıklayınız. Kullanıcı Hesabı Denetimi ekranı açılırsa onaylayınız.

14. ÖRNEK UYGULAMA

Aşağıdaki adımları izleyerek Komut İstemi'nde kullanıcı ve grup yönetimiyle süreç yönetimi komutlarını uygulayınız.

1. Adım: Başlat menüsüne **cmd** yazarak Komut İstemi'ni yönetici olarak çalıştırınız.

2. Adım: **net user** komutuyla sistemdeki kullanıcıları listeleyiniz (Görsel 3.60).

```
C:\>net user

\\SIBER Kullanıcı Hesapları

-------------------------------------------------------------------------------
Administrator            Guest                    siber
VarsayılanHesap          WDAGUtilityAccount
Komut başarıyla tamamlandı.
```

Görsel 3.60: Sistem kullanıcılarının listelenmesi

3. Adım: **net user** komutuyla **testuser** adlı şifresi **Test123** olan yeni bir kullanıcı oluşturunuz ve kullanıcı bilgilerini görüntüleyiniz (Görsel 3.61).

```
C:\>net user testuser Test123 /add
Komut başarıyla tamamlandı.


C:\>net user

\\SIBER Kullanıcı Hesapları

-------------------------------------------------------------------------------
Administrator            Guest                    siber
testuser                 VarsayılanHesap          WDAGUtilityAccount
Komut başarıyla tamamlandı.
```

Görsel 3.61: Yeni kullanıcı oluşturma ve listeleme

4. Adım: **tasklist** komutuyla çalışan süreçleri listeleyiniz (Görsel 3.62).

```
C:\>tasklist

Image Name                     PID Session Name        Session#    Mem Usage
========================= ======== ================ =========== ============
System Idle Process              0 Services                   0          8 K
System                           4 Services                   0        344 K
Registry                       148 Services                   0     65.468 K
smss.exe                       548 Services                   0      1.856 K
csrss.exe                      700 Services                   0      8.584 K
wininit.exe                    808 Services                   0     11.088 K
csrss.exe                      816 Console                    1      8.320 K
```

Görsel 3.62: Çalışan süreçlerin listelenmesi

5. Adım: **start** komutuyla Not Defteri'ni başlatınız ve taskkill komutuyla sonlandırınız (Görsel 3.63).

```
C:\>start notepad.exe

C:\>taskkill /IM notepad.exe
SUCCESS: Sent termination signal to the process "Notepad.exe" with PID 6632.
```

Görsel 3.63: Süreç başlatma ve sonlandırma

6. Adım: **net user** komutuyla **testuser** kullanıcısını siliniz (Görsel 3.64).

```
C:\>net user testuser /delete
Komut başarıyla tamamlandı.
```

Görsel 3.64: Oluşturulan kullanıcının silinmesi

SIRA SİZDE

Yönetici yetkisiyle açtığınız Komut İstemi'nde bir test kullanıcısı oluşturmanız, sistemdeki süreçleri incelemeniz ve çalışmalar tamamlandıktan sonra test kullanıcısını silmeniz istenmektedir.

Verilen görevleri Komut İstemi'nde gerçekleştiriniz ve kullandığınız komutları tabloya yazınız.

No.	Görev	Kullandığım Komut
1	Sistemdeki kullanıcıları listeleyiniz.	
2	**sinav** adlı şifresi **sinav987** olan yeni bir kullanıcı oluşturunuz.	
3	**sinav** kullanıcısının bilgilerini görüntüleyiniz.	
4	**sinav** kullanıcısını **Users** grubuna ekleyiniz.	
5	Çalışan süreçleri listeleyiniz.	
6	**Hesap makinesi** sürecini başlatınız ve ardından adıyla sonlandırınız.	
7	**sinav** kullanıcısını siliniz.	

Ağ Komutları

Ağ komutları, sistemin ağ bağlantısını görüntülemek, test etmek ve temel bağlantı durumunu incelemek için kullanılır. Açık kaynak kodlu işletim sisteminde kullanılan **ip/ifconfig, ping, netstat/ss** ve **traceroute** komutlarına benzer şekilde kapalı kaynak kodlu işletim sisteminde **ipconfig, ping, netstat** ve **tracert** komutları kullanılır (Tablo 3.27).

Tablo 3.27: Ağ Komutları

Komut	Açıklama	Örnek
ipconfig	Ağ arayüzlerini ve IP adreslerini gösterir.	ipconfig
ipconfig /all	Tüm ağ arayüzlerinin ayrıntılı bilgisini gösterir.	ipconfig /all
ping [hedef]	Hedef adrese bağlantı testi yapar.	ping 8.8.8.8
netstat -an	Ağ bağlantılarını ve açık portları listeler.	netstat -an
tracert [hedef]	Hedefe giden ağ yolunu gösterir.	tracert 8.8.8.8

SİBER GÜVENLİK PENCERESİ

ping, **tracert**, **netstat** gibi ağ komutları yalnızca kendi cihazınızda veya öğretmeninizin izin verdiği laboratuvar ortamında kullanılmalıdır. Başkalarının sistemlerine izinsiz erişim girişimi yasal suçtur.

15. ÖRNEK UYGULAMA

Aşağıdaki adımları izleyerek Komut İstemi'nde ağ komutlarını uygulayınız.

1. Adım: Başlat menüsüne **cmd** yazarak Komut İstemi'ni açınız.

2. Adım: **ipconfig** komutuyla ağ arayüzlerini ve IP adreslerini görüntüleyiniz (Görsel 3.65).

```
C:\>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . : home
   IPv6 Address. . . . . . . . . . . : fd17:625c:f037:2:3a6f:49f4:e9f1:7af4
   Temporary IPv6 Address. . . . . . : fd17:625c:f037:2:88d:6226:bb9:3a55
   Link-local IPv6 Address . . . . . : fe80::bc82:edc1:145a:9e2b%13
   IPv4 Address. . . . . . . . . . . : 10.0.2.15
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : fe80::2%13
                                       10.0.2.2
```

Görsel 3.65: Ağ bilgilerini görüntüleme

3. Adım: **ping** komutuyla belirlenen hedefe bağlantı testi yapınız (Görsel 3.66).

```
C:\>ping 8.8.8.8

Pinging 8.8.8.8 with 32 bytes of data:
Reply from 8.8.8.8: bytes=32 time=45ms TTL=128
Reply from 8.8.8.8: bytes=32 time=49ms TTL=128
Reply from 8.8.8.8: bytes=32 time=90ms TTL=128
Reply from 8.8.8.8: bytes=32 time=110ms TTL=128

Ping statistics for 8.8.8.8:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss)
Approximate round trip times in milli-seconds:
    Minimum = 45ms, Maximum = 110ms, Average = 73ms
```

Görsel 3. 66: ping komutuyla bağlantı testi

4. Adım: **netstat -an** komutuyla ağ bağlantılarını ve açık portları listeleyiniz (Görsel 3.67).

```
C:\>netstat -an

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:5040           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:7680           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49664          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49665          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49666          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49667          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49669          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49672          0.0.0.0:0              LISTENING
  TCP    10.0.2.15:139          0.0.0.0:0              LISTENING
  TCP    10.0.2.15:49674        98.66.133.186:443      ESTABLISHED
```

Görsel 3.67: Ağ bağlantıları ve açık portların listelenmesi

SIRA SİZDE

Sisteminizde ağ bağlantısıyla ilgili bir sorun yaşandığını fark ettiniz. Ağ durumunu incelemeniz ve bağlantı testleri yapmanız gerekmektedir.

Verilen görevleri Komut İstemi'nde gerçekleştiriniz ve kullandığınız komutları tabloya yazınız.

No.	Görev	Kullandığım Komut
1	Ağ arayüzlerinin ayrıntılı bilgisini görüntüleyiniz.	
2	Öğretmeninizin belirlediği hedefe bağlantı testi yapınız.	
3	Ağ bağlantılarını ve açık portları listeleyiniz.	
4	Belirlenen hedefe giden ağ yolunu görüntüleyiniz.	

Zamanlanmış Görev Komutu

Belirli komutların veya programların belirli zamanlarda otomatik olarak çalıştırılması gerekebilir. Bu işlem için **schtasks** komutu kullanılır. Açık kaynak kodlu işletim sistemindeki **cron** aracına benzer şekilde çalışan **schtasks,** yedekleme, sistem denetimi veya belirli uygulamaların otomatik başlatılması gibi görevlerin zamanlanmasını sağlar (Tablo 3.28).

Tablo 3.28: Zamanlanmış Görev Komutu

Komut	Açıklama	Örnek
schtasks /query	Tanımlanmış görevleri listeler.	schtasks /query
schtasks /create /tn [ad] /tr [komut] /sc [sıklık] /st [saat]	Yeni zamanlanmış görev oluşturur.	schtasks /create /tn "Test" /tr "notepad.exe" /sc daily /st 08:00 /ru "testuser"
schtasks /delete /tn [ad]	Belirtilen görevi siler.	schtasks /delete /tn "Test"

BİLGİ KUTUSU : schtasks ve cron Karşılaştırması

Açık kaynak kodlu işletim sisteminde zamanlanmış görevler **crontab** dosyasına yazılırken kapalı kaynak kodlu işletim sisteminde **schtasks** komutu veya Görev Zamanlayıcı grafik arayüzü kullanılır. Her iki araç da belirli aralıklarla görev çalıştırmaya olanak tanır; ancak söz dizimi ve yapılandırma yöntemi farklıdır.

16. ÖRNEK UYGULAMA

Aşağıdaki adımları izleyerek Komut İstemi'nde **schtasks** komutuyla zamanlanmış görev oluşturunuz ve yönetiniz.

1. Adım: Başlat menüsüne **cmd** yazarak Komut İstemi'ni yönetici olarak çalıştırınız.

2. Adım: **schtasks /query** komutuyla mevcut zamanlanmış görevleri listeleyiniz (Görsel 3.68).

```
C:\>schtasks /query

Folder: \
TaskName                                 Next Run Time          Status
======================================== ====================== ===============
[redacted]EdgeUpdateTaskMachineCore{CB162 15.06.2026 20:01:52    Ready
[redacted]EdgeUpdateTaskMachineUA{CBB4E6A 14.06.2026 21:31:52    Ready
[redacted] Reporting Task-S-1-5-21-3824504 15.06.2026 20:26:36    Ready
[redacted] Standalone Update Task-S-1-5-21 15.06.2026 22:27:42    Ready
[redacted] Startup Task-S-1-5-21-382450452 N/A                    Ready
```

Görsel 3.68: Zamanlanmış görevlerin listelenmesi

3. Adım: **testuser** adlı kullanıcı oluşturunuz ve **schtasks /create** komutuyla her gün saat 08:00'de Not Defteri'ni açan bir görev oluşturunuz (Görsel 3.69).

```
C:\>net user testuser Test123 /add
Komut başarıyla tamamlandı.


C:\>schtasks /create /tn "GunlukTest" /tr "notepad.exe" /sc daily /st 08:00 /ru "testuser"
SUCCESS: The scheduled task "GunlukTest" has successfully been created.
```

Görsel 3.69: Zamanlanmış görev oluşturma

4. Adım: **schtasks /query** komutuyla oluşturduğunuz görevi listeleyerek doğrulayınız (Görsel 3.70).

```
C:\>schtasks /query

Folder: \
TaskName                                 Next Run Time          Status
======================================== ====================== ===============
GunlukTest                               15.06.2026 08:00:00    Ready
```

Görsel 3.70: Oluşturulan zamanlanmış görevin doğrulanması

5. Adım: **schtasks /delete** komutuyla oluşturduğunuz görevi siliniz (Görsel 3.71).

```
C:\>schtasks /delete /tn "GunlukTest"
WARNING: Are you sure you want to remove the task "GunlukTest" (Y/N)? y
SUCCESS: The scheduled task "GunlukTest" was successfully deleted.
```

Görsel 3.71: Oluşturulan zamanlanmış görevin silinmesi

SIRA SİZDE

Aşağıdaki kavrama ilişkin istenen ifadelere göre tabloyu doldurunuz.



6. ETKİNLİK

Etkinlik Adı	Komut Satırı Uygulaması
Süre	40 dakika
Amaç	Komut İstemi'nde yapılacak işlemlere uygun komutları belirleyerek sistemi yapılandırmak
Yönerge	Komut İstemi'ni yönetici olarak çalıştırınız. Aşağıdaki tabloda her adım için yapılacak işlem verilmiştir. Uygun komutu belirleyerek uygulayınız. Her adımı tamamladığınızda Kontrol sütununa tik (✓) atarak işaretleyiniz.

Senaryo: Okulunuzun bilişim laboratuvarına yeni teslim alınan bilgisayarı sisteme dahil etmekle görevlendirildiniz. Bilgisayarda bir laboratuvar kullanıcısı oluşturmanız, çalışma dizinlerini düzenlemeniz, sistem durumunu incelemeniz ve belirli görevleri otomatikleştirmeniz istenmektedir.

Güvenli Kullanım Uyarısı: Bu uygulamada yer alan komutlar yalnızca öğrencinin kendi yerel sistemi veya öğretmenin belirlediği güvenli laboratuvar ortamı üzerinde kullanılmalıdır. Başka cihazlara, okul ağına veya üçüncü kişilere ait sistemlere izinsiz bağlantı testi, tarama veya müdahale yapılmamalıdır.

Uygulama Adımları

Adım	Yapılacak İşlem	Kullanılan Komut	Kontrol
1	Kullanılabilecek komutları listeleyiniz.		☐ Tamamlandı
2	Etkin kullanıcı adını görüntüleyiniz.		☐ Tamamlandı
3	Bilgisayar adını görüntüleyiniz.		☐ Tamamlandı
4	C:\ dizininin içeriğini listeleyiniz.		☐ Tamamlandı
5	C:\Lab dizinine geçiniz.		☐ Tamamlandı
6	C:\Lab\Belgeler adlı yeni bir dizin oluşturunuz.		☐ Tamamlandı
7	C:\Lab\Belgeler dizininde sistem_raporu.txt adlı bir dosya oluşturunuz ve içine "Sistem kurulumu tamamlandı." metnini ekleyiniz.		☐ Tamamlandı
8	sistem_raporu.txt dosyasının içeriğini ekrana yazdırınız.		☐ Tamamlandı
9	sistem_raporu.txt dosyasını C:\Lab dizinine kopyalayınız.		☐ Tamamlandı

10	C:\Lab\Belgeler dizinindeki sistem_raporu.txt dosyasını siliniz.		☐ Tamamlandı
11	İnternetten bir dosya indiriniz ve C:\Lab dizinine kaydediniz.		☐ Tamamlandı
12	labkullanici adlı yeni bir kullanıcı oluşturunuz. ⚠		☐ Tamamlandı
13	labkullanici kullanıcısını Kullanıcılar grubuna ekleyiniz. ⚠		☐ Tamamlandı
14	labkullanici kullanıcısını siliniz. ⚠		☐ Tamamlandı
15	Çalışan süreçleri listeleyiniz.		☐ Tamamlandı
16	notepad.exe sürecini sonlandırınız.		☐ Tamamlandı
17	Ağ arayüzlerini ve IP adreslerini görüntüleyiniz.		☐ Tamamlandı
18	Öğretmeninizin belirlediği hedefe bağlantı testi yapınız.		☐ Tamamlandı
19	Açık portları listeleyiniz.		☐ Tamamlandı
20	Her gün 08:00'de çalışacak bir zamanlanmış görev oluşturunuz. ⚠		☐ Tamamlandı
21	Zamanlanmış görevleri listeleyiniz.		☐ Tamamlandı

⚠ **Dikkat:** 12, 13, 14 ve 20. adımlardaki komutlar yönetici yetkisi gerektirir. Komut İstemi yönetici olarak açılmadan bu komutlar çalıştırılamaz.

Değerlendirme

Çalışmanız kontrol listesine göre değerlendirilecektir. Çalışmanızı yaparken buradaki ölçütleri dikkate alınız. Kontrol listesi formuna ulaşmak için karekodu okutunuz. Dijital yayınlarda karekodun üstüne tıklayarak içeriğe ulaşabilirsiniz.

3.1.5.5. PowerShell

PowerShell, kapalı kaynak kodlu işletim sisteminde sistem yönetimi, otomasyon ve betik programlama işlemleri için kullanılan gelişmiş bir komut satırı ortamıdır. Nesne tabanlı yapısı ve geniş komut kütüphanesiyle sistem yöneticileri, yazılım geliştiriciler ve ileri düzey kullanıcılar tarafından yaygın biçimde kullanılır. PowerShell'i açmak için Başlat menüsüne **PowerShell** yazılır. Yönetici yetkisiyle açmak için sağ tıklayarak **Yönetici olarak çalıştır** seçeneği tıklanır.

BİLGİ KUTUSU : PowerShell ve cmd Karşılaştırması

cmd yalnızca metin tabanlı komutlar çalıştırırken PowerShell nesneler üzerinde işlem yapar. PowerShell komutları **Fiil-İsim** yapısıyla oluşturulur: **Get-Process, Set-Location, Remove-Item** gibi. Bu yapı komutların ne yaptığını anlamayı kolaylaştırır.

PowerShell'de kullanılan temel komutlar Tablo 3.29'da verilmiştir.

Tablo 3.29: Temel PowerShell Komutları

Komut	Açıklama	Örnek
Get-Help [komut]	Belirtilen komut hakkında yardım bilgisi gösterir.	Get-Help Get-Process
Get-Command	Kullanılabilecek komutları listeler.	Get-Command
Get-Process	Çalışan süreçleri listeler.	Get-Process
Stop-Process -Name [ad]	Belirtilen süreci sonlandırır.	Stop-Process -Name notepad
Get-Service	Sistem servislerini listeler.	Get-Service
Get-ChildItem	Bulunulan dizinin içeriğini listeler.	Get-ChildItem C:\
Set-Location [dizin]	Dizin değiştirir.	Set-Location C:\Users
Copy-Item [kaynak] [hedef]	Dosya veya dizin kopyalar.	Copy-Item notlar.txt C:\Temp
Remove-Item [dosya]	Dosya veya dizin siler.	Remove-Item notlar.txt
Write-Host [metin]	Ekrana metin yazdırır.	Write-Host "Merhaba"
Get-Content [dosya]	Dosya içeriğini gösterir.	Get-Content notlar.txt
Get-NetIPAddress	Ağ bilgilerini gösterir.	Get-NetIPAddress

17. ÖRNEK UYGULAMA

Aşağıdaki adımları izleyerek PowerShell'de temel komutları uygulayınız.

1. Adım: Başlat menüsüne **PowerShell** yazarak PowerShell'i açınız.

2. Adım: **Get-Help Get-Process** komutuyla **Get-Process** komutunun yardım bilgisini görüntüleyiniz (Görsel 3.72).

```
PS C:\Windows\System32> Get-Help Get-Process

NAME
    Get-Process

SYNTAX
    Get-Process [[-Name] <string[]>] [-ComputerName <string[]>] [-Module] [-FileVersionInfo]  [<CommonParameters>]

    Get-Process [[-Name] <string[]>] -IncludeUserName  [<CommonParameters>]

    Get-Process -Id <int[]> -IncludeUserName  [<CommonParameters>]

    Get-Process -Id <int[]> [-ComputerName <string[]>] [-Module] [-FileVersionInfo]  [<CommonParameters>]
```

Görsel 3.72: Get-Help komutu kullanımı

3. Adım: Get-Process komutuyla çalışan süreçleri listeleyiniz (Görsel 3.73).

```
PS C:\Windows\System32> Get-Process

Handles  NPM(K)    PM(K)      WS(K)     CPU(s)      Id  SI ProcessName
-------  ------    -----      -----     ------      --  -- -----------
    148       9     2436      12404               5268   0 AggregatorHost
    374      21    32520      60820       0,69  10732   1 ApplicationFrameHost
    312      16     5356      31236       0,17   2180   1 backgroundTaskHost
    499      22     8600       3380       0,48   2440   1 backgroundTaskHost
    245      12     4456      27728       0,27   2820   1 backgroundTaskHost
    246      14     9988       3428       0,31   4408   1 backgroundTaskHost
    370      16    16876      18008       0,31   9608   1 backgroundTaskHost
    454      25    35016      70308       1,77   5912   1 CrossDeviceResume
```

Görsel 3.73: Çalışan süreçlerin listelenmesi

4. Adım: Get-Service komutuyla sistem servislerini listeleyiniz (Görsel 3.74).

```
PS C:\Windows\System32> Get-Service

Status   Name               DisplayName
------   ----               -----------
Stopped  AarSvc_41869       Agent Activation Runtime_41869
Stopped  ADPSvc             Toplu Veri Platformu Hizmeti
Stopped  ALG                Uygulama Katmanı Ağ Geçidi Hizmeti
Running  AppIDSvc           Uygulama Kimliği
Running  Appinfo            Uygulama Bilgileri
Stopped  AppReadiness       Uygulama Hazır Olma Durumu
Stopped  AppXSvc            AppX Deployment Service (AppXSVC)
```

Görsel 3.74: Sistem servislerinin listelenmesi

5. Adım: Set-Location C: komutuyla kök dizine geçiniz ve **Get-ChildItem** komutuyla içeriği listeleyiniz (Görsel 3.75).

```
PS C:\Windows\System32> Set-Location C:\
PS C:\> Get-ChildItem


    Directory: C:\


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----         7.03.2026     02:50                inetpub
d-----         1.04.2024     11:45                PerfLogs
d-r---         6.06.2026     18:33                Program Files
d-r---        18.05.2026     06:12                Program Files (x86)
d-r---        17.05.2026     21:38                Users
d-----        14.06.2026     19:35                Windows
```

Görsel 3.75: Dizin içeriğinin listelenmesi

6. Adım: Write-Host komutuyla ekrana kendi adınızı yazdırınız (Görsel 3.76).

```
PS C:\> Write-Host "Adım: Sistem ve Ağ Temelleri"
Adım: Sistem ve Ağ Temelleri
```

Görsel 3.76: Write-Host komutu kullanımı

PowerShell Betik Dosyası Oluşturma

PowerShell betik dosyaları **.ps1** uzantısıyla kaydedilir. Betik dosyası oluşturmak için bir metin editörü veya PowerShell ISE kullanılabilir. Betik dosyasını çalıştırmadan önce yürütme ilkesinin ayarlanması gerekebilir.

BİLGİ KUTUSU : Yürütme İlkesi

Güvenlik amacıyla PowerShell varsayılan olarak betik çalıştırmayı kısıtlar. Betik çalıştırabilmek için yönetici yetkisiyle şu komutu çalıştırınız:

Set-ExecutionPolicy -Scope Process RemoteSigned

Bu ayar yerel olarak oluşturulan betiklerin çalıştırılmasına izin verir.

PowerShell'de kullanılan temel betik komutları Tablo 3.30'da verilmiştir.

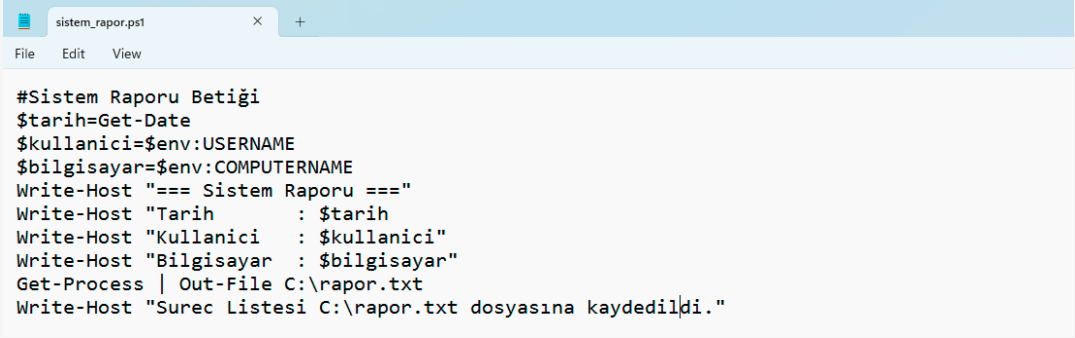
Tablo 3.30: PowerShell Betik Komutları

Komut	Açıklama	Örnek
$degisken = deger	Değişken tanımlar.	$ad = "Siber"
Write-Host $degisken	Değişken değerini ekrana yazdırır.	Write-Host $ad
if (koşul) { }	Koşullu işlem yapar.	if ($sayi -gt 5) { Write-Host "Büyük" }
foreach ($i in $liste) { }	Liste üzerinde döngü çalıştırır.	foreach ($s in Get-Process) { Write-Host $s.Name }
Get-Date	Sistem tarih ve saatini döndürür.	Get-Date
Out-File [dosya]	Çıktıyı dosyaya yazar.	Get-Process | Out-File rapor.txt

18. ÖRNEK UYGULAMA

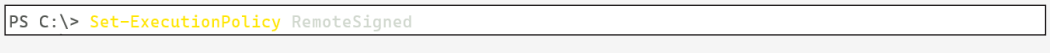
Aşağıdaki adımları izleyerek PowerShell betik dosyası oluşturunuz ve çalıştırınız.

1. Adım: Not Defteri'ni açınız ve Görsel 3.77'deki betik içeriğini giriniz. Dosyayı C:\sistem_rapor.ps1 olarak kaydediniz.



Görsel 3.77: Betik dosyasının oluşturulması

2. Adım: PowerShell'i yönetici olarak açınız ve yürütme ilkesini ayarlayınız (Görsel 3.78).



Görsel 3.78: Yürütme ilkesinin ayarlanması

3. Adım: **.\sistem_rapor.ps1** komutuyla betiği çalıştırınız ve çıktıyı inceleyiniz (Görsel 3.79).

```
PS C:\> .\sistem_rapor.ps1
=== Sistem Raporu ===
Tarih     : 06/14/2026 22:22:18
Kullanici : siber
Bilgisayar:
Surec Listesi c:\rapor.txt dosyasina kaydedildi.
```

Görsel 3.79: Betik çıktısı

4. Adım: **Get-Content C:\rapor.txt** komutuyla oluşturulan rapor dosyasını görüntüleyiniz (Görsel 3.80).

```
PS C:\> Get-Content C:\rapor.txt

Handles  NPM(K)    PM(K)      WS(K)     CPU(s)      Id  SI ProcessName
-------  ------    -----      -----     ------      --  -- -----------
    141       9     2576      13976       0,52    5468   0 AggregatorHost
    433      23    32904      75300       1,41    9068   1 ApplicationFrameHost
    240      11     6972      19404       0,09    1544   0 audiodg
    448      20     7212       3644       0,69    4528   1 backgroundTaskHost
    284      15    15460       3580       0,42    6136   1 backgroundTaskHost
    614      26     8956       3856       0,45    8328   1 backgroundTaskHost
    455      25    34896      75284       1,59    2720   1 CrossDeviceResume
    525      21     2468       8768       0,86     744   0 csrss
    477      20     2556       8340       1,38     824   1 csrss
```

Görsel 3.80: Rapor dosyasının içeriği

7. ETKİNLİK

Etkinlik Adı	PowerShell Betik Dosyası Hazırlama
Süre	25 dakika
Amaç	Değişken, açıklama satırı ve dosyaya yazma komutlarını kullanarak sistem bilgilerini raporlayan bir PowerShell betiği oluşturmak ve çalıştırmak
Yönerge	PowerShell ISE'yi yönetici olarak açınız. Aşağıdaki adımları sırasıyla gerçekleştiriniz. Her adımı tamamladığınızda Kontrol sütununa tik (✓) atarak işaretleyiniz.

Uygulama Adımları

Adım	Yapılacak İşlem	Kullanılan Komut	Kontrol
1	PowerShell ISE'yi yönetici olarak açınız ve betik çalıştırma iznini ayarlayınız.		☐ Tamamlandı
2	Sistem tarihini, etkin kullanıcı adını ve bilgisayar adını tutan üç değişken tanımlayınız.		☐ Tamamlandı
3	Her değişkenin üstüne o satırın ne yaptığını açıklayan bir açıklama satırı ekleyiniz.		☐ Tamamlandı
4	Tanımladığınız değişkenleri ekrana yazdırınız.		☐ Tamamlandı

5	Çalışan süreç listesini C:\Lab\surecler.txt dosyasına kaydediniz.		☐ Tamamlandı
6	Betiği lab_rapor.ps1 adıyla kaydediniz ve çalıştırınız.		☐ Tamamlandı
7	Oluşturulan dosyanın varlığını ve içeriğini doğrulayınız.		☐ Tamamlandı

Değerlendirme

Çalışmanız öğretmeniniz tarafından analitik dereceli puanlama anahtarına göre değerlendirilecektir. Çalışmanızı yaparken buradaki ölçütleri dikkate alınız. Analitik dereceli puanlama anahtarı formuna ulaşmak için karekodu okutunuz. Dijital yayınlarda karekodun üstüne tıklayarak içeriğe ulaşabilirsiniz.

3.1.5.6. Kapalı Kaynak Kodlu İşletim Sistemi Yönetim Araçları

Kapalı kaynak kodlu işletim sistemi, sistem durumunu izlemek, sorunları teşhis etmek ve yapılandırmaları yönetmek için çeşitli grafik tabanlı yönetim araçları sunar. Bu araçlar hem bireysel kullanıcılara hem de sistem yöneticilerine sistem üzerinde kapsamlı denetim imkânı sağlar.

Görev Yöneticisi

Görev Yöneticisi (Task Manager), çalışan uygulamaları, süreçleri ve sistem kaynak kullanımını anlık olarak izlemeye yarar. **Ctrl+Shift+Esc** kısayoluyla veya görev çubuğuna sağ tıklayarak açılır.

Görev Yöneticisi'nde beş temel sekme bulunur:

1. **İşlemler:** Çalışan uygulamalar ve arka plan süreçleriyle CPU, bellek, disk kullanımları görüntülenir.
2. **Performans:** CPU, bellek, disk ve ağ kullanımının anlık grafiklerini gösterir.
3. **Uygulama geçmişi:** Uygulamaların kaynak tüketim geçmişini gösterir.
4. **Başlangıç:** Sistem açılışında otomatik başlayan uygulamaları listeler ve devre dışı bırakmaya olanak tanır.
5. **Hizmetler:** Sistemde çalışan servisleri listeler.

SİBER GÜVENLİK PENCERESİ

Görev Yöneticisi'nde tanımadığınız bir süreç yüksek CPU veya bellek kullanıyorsa zararlı yazılım olabilir. Sürecin adını aratarak güvenilir bir kaynaktan doğrulayınız. Gereksiz başlangıç uygulamalarını devre dışı bırakmak hem güvenliği hem de sistem performansını artırır.

Olay Görüntüleyicisi

Olay Görüntüleyicisi (Event Viewer), sistemde gerçekleşen olayları, hataları ve uyarıları kayıt altına alır. Başlat menüsüne **eventvwr** yazılarak açılır.

Olay Görüntüleyicisi'nde üç temel günlük kategorisi bulunur:

1. **Uygulama:** Uygulamalar tarafından oluşturulan olayları içerir.
2. **Sistem:** İşletim sistemi bileşenlerine ait olayları içerir.
3. **Güvenlik:** Oturum açma, dosya erişimi gibi güvenlik olaylarını kaydeder.

SİBER GÜVENLİK PENCERESİ

Olay Görüntüleyicisi'ndeki Güvenlik günlükleri, başarısız oturum açma denemeleri ve yetkisiz erişim girişimlerini kaydeder. Siber saldırı sonrasında adli analiz yapılırken ilk incelenen kaynaklardan biridir. Bu nedenle günlük dosyaları düzenli olarak izlenmeli ve korunmalıdır.

Sistem Bilgisi

Sistem Bilgisi (System Information) aracı, donanım, yazılım ve sistem yapılandırmasına ilişkin ayrıntılı bilgi sunar. Başlat menüsüne **msinfo32** yazılarak açılır. İşlemci, bellek, işletim sistemi sürümü, kurulu sürücüler ve ağ bilgileri bu araçla görüntülenebilir.

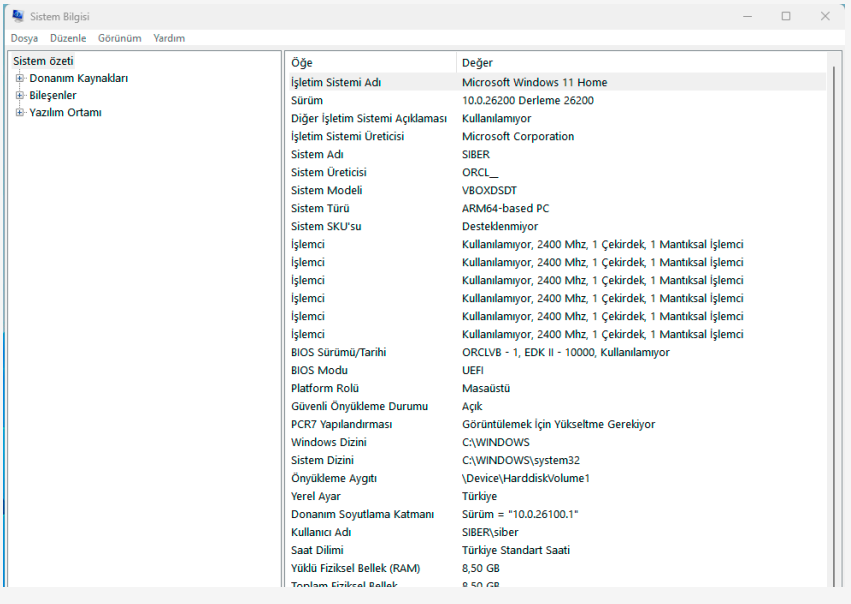
Kaynak İzleyicisi

Kaynak İzleyicisi (Resource Monitor), CPU, bellek, disk ve ağ kullanımını Görev Yöneticisi'ne kıyasla daha ayrıntılı biçimde izlemeye olanak tanır. Başlat menüsüne **resmon** yazılarak açılır.

19. ÖRNEK UYGULAMA

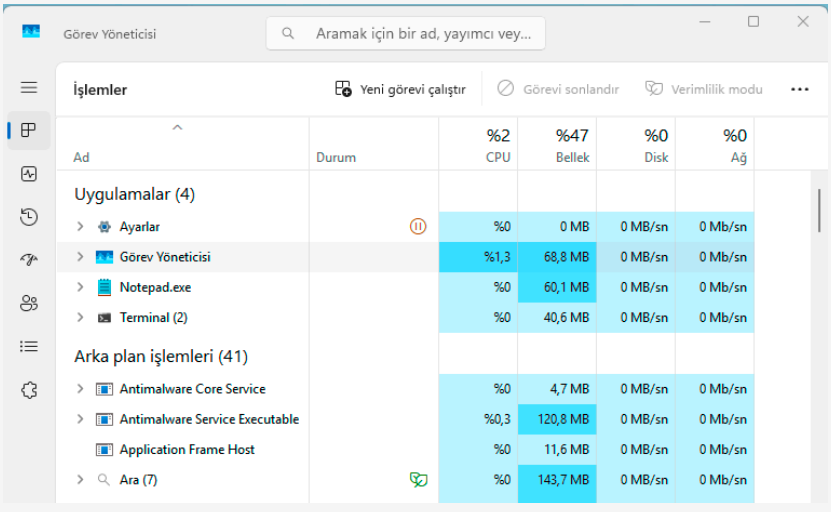
Aşağıdaki adımları izleyerek kapalı kaynak kodlu işletim sistemi yönetim araçlarını kullanarak sistemi izleyiniz ve rapor hazırlayınız.

1. Adım: Başlat menüsüne **msinfo32** yazarak **Sistem Bilgisi'**ni açınız. İşlemci, RAM ve işletim sistemi sürümünü not ediniz (Görsel 3.81).



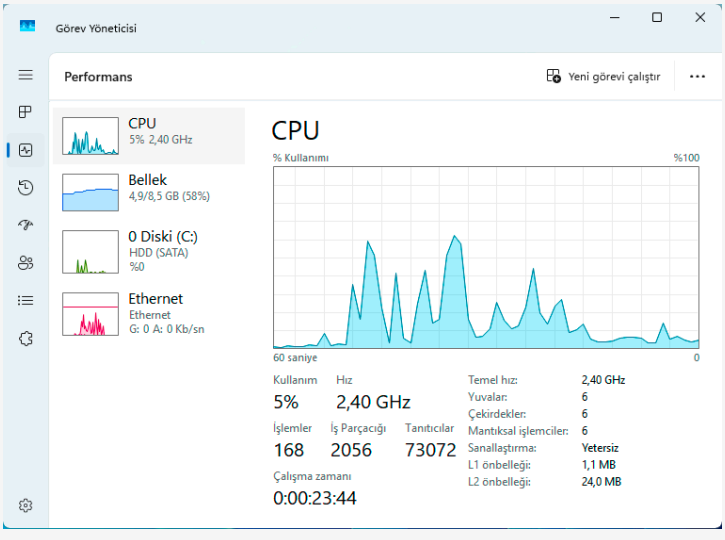
Görsel 3.81: Sistem Bilgisi aracı

2. Adım: **Ctrl+Shift+Esc** kısayoluyla **Görev Yöneticisi**'ni açınız. İşlemler sekmesinde en fazla CPU kullanan süreci not ediniz (Görsel 3.82).



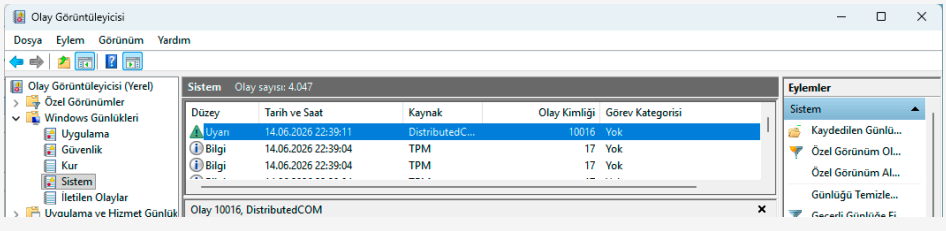
Görsel 3.82: Görev Yöneticisi - İşlemler sekmesi

3. Adım: Performans sekmesine geçiniz. CPU, bellek ve disk kullanım değerlerini not ediniz (Görsel 3.83).



Görsel 3.83: Görev Yöneticisi - Performans sekmesi

4. Adım: Başlat menüsüne eventvwr yazarak Olay Görüntüleyicisi'ni açınız. Windows Günlükleri > Sistem bölümünde son 5 olayı inceleyiniz (Görsel 3.84).



Görsel 3.84: Olay Görüntüleyicisi

5. Adım: Not Defteri'ni açınız. Topladığınız bilgileri Görsel 3.85'teki görülen başlıklar altında bir sistem raporu olarak düzenleyiniz ve kaydediniz.

```
========================================
        SİSTEM İZLEME RAPORU
========================================

Tarih          : ....../....../..........
Hazırlayan     : ..................................
Bilgisayar Adı : ..................................


--- 1. SİSTEM BİLGİLERİ ---

İşlemci        : ..................................
Toplam RAM     : ..................................
İşletim Sistemi: ..................................


--- 2. SÜREÇ İZLEME ---

En fazla CPU kullanan 3 süreç:

1. ............................ → %......
2. ............................ → %......
3. ............................ → %......


--- 3. PERFORMANS DEĞERLERİ ---

CPU Kullanımı  : %......
Bellek Kullanımı: ...... GB / ...... GB
Disk Kullanımı : %......


--- 4. SİSTEM OLAYI İNCELEMESİ ---

İncelenen son 5 olay:

1. Tarih: .......... | Düzey: .......... | Kaynak: ..........
2. Tarih: .......... | Düzey: .......... | Kaynak: ..........
3. Tarih: .......... | Düzey: .......... | Kaynak: ..........
4. Tarih: .......... | Düzey: .......... | Kaynak: ..........
5. Tarih: .......... | Düzey: .......... | Kaynak: ..........


--- 5. YORUM ---

Genel sistem durumunu kısaca değerlendiriniz:

................................................
................................................

========================================
```

Görsel 3.85: Sistem raporunun hazırlanması

8. ETKİNLİK

Etkinlik Adı	Sistem Tanılama Raporu
Süre	20 dakika
Amaç	Bir performans sorununu araştırmak için yönetim araçlarını doğru kullanmak ve toplanan verileri yorumlayarak belgelenmiş bir sistem tanılama raporu hazırlamak

Senaryo: Okulunuzdaki bilişim laboratuvarında bir bilgisayar son günlerde belirgin biçimde yavaşlamaktadır. Sorumlu teknisyen şu anda ulaşılabilir değildir; ilk incelemeyi siz yapacaksınız. Göreviniz, sistemi yönetim araçlarıyla incelemek, elde ettiğiniz bulguları tabloya kaydetmek ve bu verileri yorumlayarak kısa bir tanılama raporu hazırlamaktır.

Görev Tablosu

No.	Görev	Elde Edilen Veriler
1	Görev Yöneticisi'ni açarak en fazla CPU kullanan süreci belirleyiniz.	Süreç adı: ..... CPU: %.....
2	Performans sekmesinden bellek (RAM) kullanım değerini görüntüleyiniz.	..... / ..... GB (%.....)
3	Başlangıç sekmesinde otomatik başlayan uygulama sayısını not ediniz.	Uygulama sayısı: .....
4	Olay Görüntüleyicisi'nde Windows Günlükleri > Sistem bölümünde son hata veya uyarı olayını inceleyiniz.	Kaynak: ..... Düzey: .....
5	msinfo32 aracıyla işlemci adını ve toplam RAM miktarını alınız.	İşlemci: ..... RAM: ..... GB

Görev tablosunda topladığınız verilere dayanarak aşağıdaki soruları yanıtlayınız.

1. Tablonuzdaki verilere göre sistemi en çok hangi süreç zorluyor? Bu sürecin yüksek kaynak kullanmasının olası nedenleri neler olabilir?

   _____

   _____

2. Başlangıçta otomatik çalışan uygulama sayısı performansı nasıl etkiler? Bu uygulamalardan hangilerinin devre dışı bırakılması daha uygun olur? Gerekçenizi yazınız.

   _____

   _____

3. Olay Görüntüleyicisi'nde incelediğiniz olayın kaynağı ve düzeyine bakarak bu olayı nasıl yorumlarsınız? Sistemdeki yavaşlamayla bir bağlantısı olup olmadığını gerekçelendiriniz.

   _____

   _____

4. Tablodaki tüm bulgularınızı birlikte değerlendirerek yavaşlamanın en olası nedenini belirleyiniz ve teknisyene iletmek üzere bulgularınızı kısaca özetleyiniz.

   _____

   _____

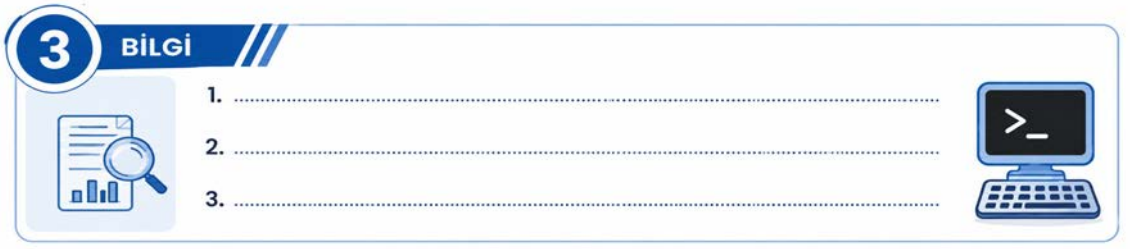
Değerlendirme

Çalışmanız öğretmeniniz tarafından kontrol listesine göre değerlendirilecektir. Çalışmanızı yaparken buradaki ölçütleri dikkate alınız. Kontrol listesi formuna ulaşmak için karekodu okutunuz. Dijital yayınlarda karekodun üstüne tıklayarak içeriğe ulaşabilirsiniz.

SIRA SİZDE

Açık kaynak kodlu ve kapalı kaynak kodlu işletim sistemlerinin terminal komutlarına ilişkin yaptığınız karşılaştırma ve uygulamalardan hareketle aşağıdaki **3-2-1 çıkış kartını** doldurunuz. Cevaplarınızı kısa, açık ve konuya uygun şekilde yazınız.

Her iki sistemin terminal komutlarıyla ilgili öğrendiğiniz üç komutu veya üç önemli bilgiyi yazınız.



Her iki sistemin terminal komutlarıyla ilgili merak ettiğiniz veya daha iyi anlamak istediğiniz iki soruyu yazınız.



Her iki sistemin terminal komutlarını karşılaştırdığınızda fark ettiğiniz bir benzerliği veya farklılığı yazınız.



3.2. SUNUCU İŞLETİM SİSTEMLERİ

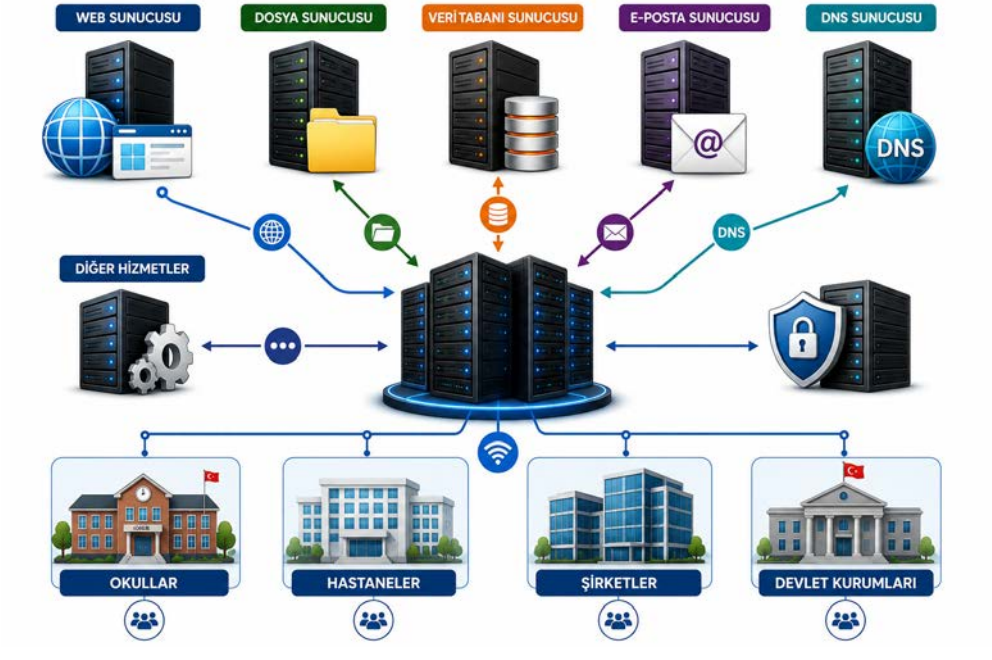
Bir şirketteki çalışanlar her sabah bilgisayarına oturup kurumsal dosyalara erişir, şirket içi e-posta gönderir ve ortak yazıcıya iş gönderir. Tüm bu işlemler arka planda kesintisiz çalışan ve hiçbir kullanıcının doğrudan görmediği bir sisteme dayanır. O sistem kapanırsa dosyalara ulaşmak, e-posta göndermek, hatta sisteme giriş yapmak mümkün olmaz. Bu görevi üstlenen yapıya **sunucu,** sunucunun tüm bu hizmetleri yönetmesini sağlayan yazılıma ise **sunucu işletim sistemi** denir.

Sunucu işletim sistemi, ağdaki diğer cihazlara dosya paylaşımı, web yayını, e-posta iletimi, kullanıcı kimlik doğrulama gibi hizmetleri kesintisiz olarak sunmak amacıyla tasarlanmış özel bir işletim sistemi türüdür. Masaüstü işletim sistemlerinin önceliği kullanıcı deneyimidir. Sunucu işletim sistemlerinin önceliği ise kararlılık, güvenlik ve kaynak verimliliğidir. Bu nedenle grafik arayüz çoğunlukla kullanılmaz ve sistem yalnızca komut satırı üzerinden yönetilir. Gereksiz bileşenlerden arındırılmış bu yapı hem kaynak tüketimini azaltır hem de sistemi daha kararlı ve güvenli kılar. Masaüstü ve sunucu işletim sistemleri arasındaki temel farklar Tablo 3.31'de verilmiştir.

Tablo 3.31: Masaüstü ve Sunucu İşletim Sistemlerinin Karşılaştırması

Özellik	Masaüstü İşletim Sistemi	Sunucu İşletim Sistemi
Temel amaç	Bireysel kullanıcı deneyimi	Ağ hizmetleri sunmak
Arayüz	Grafik arayüz	Çoğunlukla komut satırı
Çalışma süresi	Gerektiğinde açık	7/24 kesintisiz
Kullanıcı sayısı	Tek kullanıcı	Çok kullanıcı
Kaynak yönetimi	Kullanıcı uygulamaları öncelikli	Ağ hizmetleri öncelikli
Güvenlik önceliği	Orta	Yüksek

Sunucu işletim sistemleri; web sunucusu, dosya sunucusu, veri tabanı sunucusu, e-posta sunucusu, DNS [Domain Name Server (Alan Adı Sunucusu)] sunucusu gibi birçok farklı hizmet rolünü üstlenebilir. Okullar, hastaneler, şirketler, devlet kurumları gibi birden fazla kullanıcının aynı anda sisteme eriştiği her ortamda sunucu işletim sistemleri kullanılır (Görsel 3.86).



Görsel 3.86: Sunucu işletim sistemlerinin üstlenebileceği hizmet rolleri ve kullanım alanları

SİBER GÜVENLİK PENCERESİ

Sunucu işletim sistemleri, ağdaki tüm kullanıcılara hizmet verdiğinden siber saldırılar açısından öncelikli hedef hâline gelir. Yanlış yapılandırılmış bir sunucu; yetkisiz erişime, veri sızıntısına ve hizmet kesintisine yol açabilir. Varsayılan olarak gelen gereksiz servisler kapatılmalı, kullanıcı yetkileri en az ayrıcalık ilkesiyle tanımlanmalı ve güncellemeler düzenli olarak uygulanmalıdır. Güvenli bir sunucu kurulumu, teknik bilgi kadar sistematik bir yaklaşım da gerektirir.

BİLGİ KUTUSU : Pardus/Linux Sunucu

Pardus Sunucu, TÜBİTAK ULAKBİM tarafından geliştirilen yerli ve açık kaynaklı bir sunucu işletim sistemidir. Debian tabanlı olan bu sistem; kurumsal düzeyde güvenlik, performans ve yönetilebilirlik özellikleriyle kamu kurumları ve kuruluşlar için tasarlanmıştır. Türkçe dil desteği ve yerli yazılım ekosistemiyle öne çıkan Pardus Sunucu, Türkiye'nin yerli ve millî yazılım kullanımını yaygınlaştırma hedefine katkı sağlamaktadır.

KONTROL NOKTASI

Sunucu işletim sistemi seçerken yalnızca teknik özellikler değil lisans türü, topluluk desteği, güvenlik güncellemelerinin düzenli sağlanıp sağlanmadığı ve kurumun ihtiyacı da birlikte değerlendirilmelidir.

3.2.1. Sunucu İşletim Sistemi Kurulumu

Sunucu işletim sistemi kurulumu, masaüstü işletim sistemi kurulumundan birkaç temel noktada ayrılır. Grafik arayüz yerine metin tabanlı bir kurulum ekranıyla karşılaşılır. Ağ yapılandırması, disk bölümlendirme ve kullanıcı hesabı oluşturma adımları daha belirgin biçimde ön plana çıkar. Kurulum tamamlandığında sistem doğrudan komut satırına açılır ve masaüstü ortamı kurulmaz (kapalı kaynak kodlu sunucu dışında).

20. ÖRNEK UYGULAMA

Aşağıdaki adımları izleyerek açık kaynak kodlu sunucu işletim sistemi kurulumunu gerçekleştiriniz.

1. Adım: Sunucu işletim sistemi ISO dosyasını resmî web sitesinden indiriniz.

2. Adım: İndirilen ISO dosyasını kullanarak önyüklenebilir bir USB bellek hazırlayınız.

3. Adım: Hazırladığınız USB belleği bilgisayara takarak yeniden başlatınız. BIOS/UEFI ayarlarına giriniz ve ilk açılış aygıtını USB olarak ayarlayınız. Ayar kaydedildikten sonra bilgisayar yeniden başlar.

4. Adım: Kurulum ekranı açıldığında **Try or Install Ubuntu Server** seçeneğini seçiniz ve ilerleyiniz (Görsel 3.87).

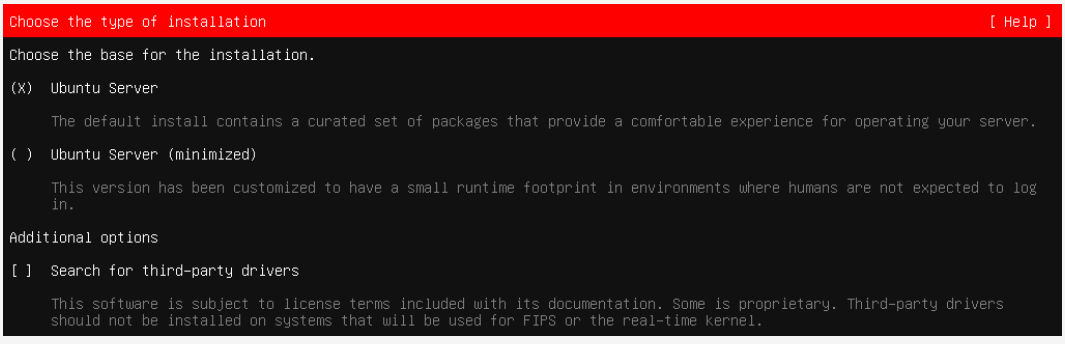


Görsel 3. 87: Ubuntu Server kurulum ekranı

5. Adım: Kurulum ekranı açıldığında dili English olarak seçiniz.

6. Adım: Klavye düzeni seçim ekranında Layout (Düzen) ve Variant (Tür) seçeneklerini Turkish (Türkçe) olarak ayarlayınız ve ilerleyiniz.

7. Adım: Kurulum türü olarak Ubuntu Server seçeneğini seçiniz (Görsel 3.88).



Görsel 3.88: Kurulum türü seçimi ekranı

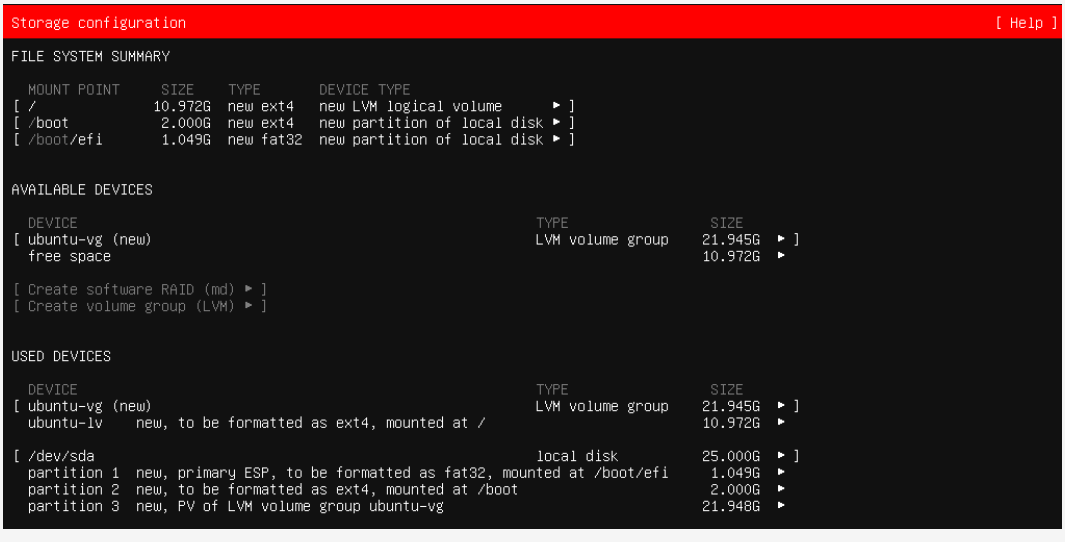
8. Adım: Ağ arayüzünü **(Network Configuration)** yapılandırınız.

9. Adım: Proxy yapılandırma ekranında **(Proxy Configuration)** proxy kullanmıyorsanız alanı boş bırakınız ve ilerleyiniz.

10. Adım: Arşiv yansıtıcısı yapılandırma ekranında **(Ubuntu Archive Mirror Configuration)** varsayılan ayna adresi olduğu gibi bırakınız ve ilerleyiniz.

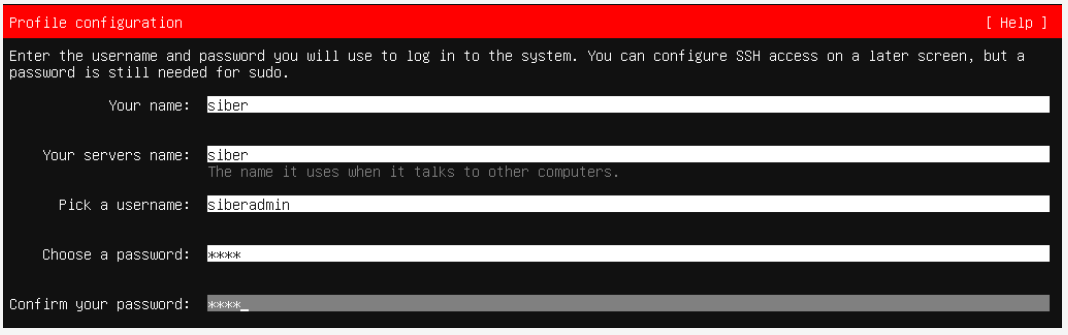
11. Adım: Disk yapılandırma ekranında **(Guided Storage Configuration)** Use an entire disk seçeneğini seçiniz ve ilerleyiniz.

12. Adım: Depolama yapılandırma özeti ekranında **(Storage Configuration)** disk bölümlendirme ayarlarını inceleyiniz ve ilerleyiniz (Görsel 3.89). Açılan onay penceresinde Continue seçeneğini seçiniz.



Görsel 3.89: Depolama yapılandırma özet ekranı

13. Adım: Profil yapılandırma ekranında **(Profile Configuration)** sunucu adını, kullanıcı adını ve parolayı belirleyerek hesap oluşturunuz (Görsel 3.90).



Görsel 3.90: Profil yapılandırma ekranı

14. Adım: Ubuntu Pro yükseltme ekranında **(Upgrade to Ubuntu Pro)** Skip for now seçeneğini seçiniz ve Continue ile ilerleyiniz.

15. Adım: SSH yapılandırma ekranında **(SSH Configuration)** Install OpenSSH server seçeneğini işaretleyiniz ve ilerleyiniz.

16. Adım: Ek yazılım seçim ekranında **(Featured Server Snaps)** herhangi bir seçim yapmadan devam ediniz.

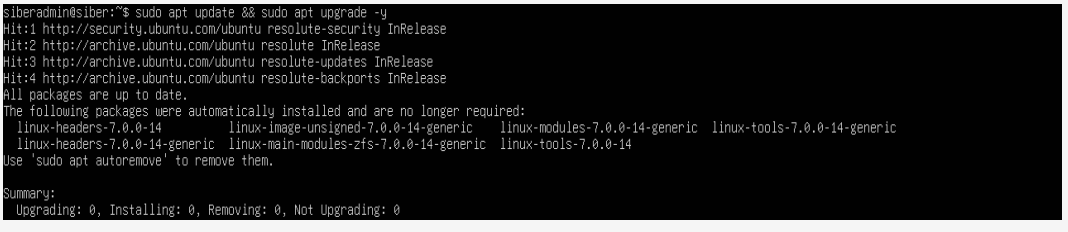
17. Adım: Kurulumun tamamlanmasını bekleyiniz. Ardından **Reboot Now** seçeneğiyle sistemi yeniden başlatınız.

18. Adım: USB belleği çıkarınız. Sistem açıldıktan sonra oluşturduğunuz kullanıcı adı ve parolayla oturum açınız (Görsel 3.91).



Görsel 3.91: Ubuntu Server oturum açma ekranı

19. Adım: **sudo apt update && sudo apt upgrade -y** komutunu çalıştırarak sistemi güncelleyiniz (Görsel 3.92).



Görsel 3.92: Sistem güncelleme komutunun çalıştırılması

9. ETKİNLİK

Etkinlik Adı	Açık Kaynak Kodlu Sunucu İşletim Sistemi Kurulumu
Süre	40 dakika
Amaç	Açık kaynak kodlu sunucu işletim sistemini fiziksel makineye adım adım kurarak sistemi kullanıma hazır hâle getirmek
Yönerge	Sınıf mevcuduna göre 3-4 kişilik gruplar oluşturunuz. Grubunuzla birlikte açık kaynak kodlu sunucu işletim sistemi kurulumunu gerçekleştiriniz. Her adımda iş bölümü yapınız. Tüm grup üyelerinin sürece aktif olarak katılması gerektiğini unutmayınız. Her adımı tamamladığınızda Kontrol sütununa tik (✓) atarak işaretleyiniz.

Uygulama Adımları

Adım	Yapılacak İşlem	Kontrol
1	Kurulum için ISO dosyasını resmî web sitesinden indiriniz ve önyüklenebilir USB bellek hazırlayınız.	☐ Tamamlandı
2	BIOS/UEFI ayarlarına girerek ilk açılış aygıtını USB olarak ayarlayınız.	☐ Tamamlandı
3	Kurulum ekranında Try or Install Ubuntu Server seçeneğini seçiniz ve Enter tuşuna basınız.	☐ Tamamlandı
4	Dili English olarak seçiniz.	☐ Tamamlandı
5	Klavye düzeni seçim ekranında Layout (Düzen) ve Variant (Değişken) seçeneklerini Turkish olarak ayarlayınız ve Done ile ilerleyiniz.	☐ Tamamlandı
6	Kurulum türü olarak Ubuntu Server seçeneğini seçiniz ve Done ile ilerleyiniz.	☐ Tamamlandı
7	Ağ arayüzünü yapılandırınız ve Done ile ilerleyiniz.	☐ Tamamlandı
8	Proxy yapılandırma ekranında (Proxy Configuration) alanı boş bırakınız ve Done ile ilerleyiniz.	☐ Tamamlandı
9	Arşiv yansıtıcısı yapılandırma ekranında (Ubuntu Archive Mirror Configuration) varsayılan ayna adresini olduğu gibi bırakınız ve Done ile ilerleyiniz.	☐ Tamamlandı
10	Disk yapılandırma ekranında (Guided Storage Configuration) Use an entire disk seçeneğini seçiniz ve Done ile ilerleyiniz.	☐ Tamamlandı
11	Depolama yapılandırma özeti ekranında (Storage Configuration) ayarları inceleyiniz, Done ile ilerleyiniz ve açılan onay penceresinde Continue seçeneğini seçiniz.	☐ Tamamlandı
12	Profil yapılandırma ekranında (Profile Configuration) sunucu adını, kullanıcı adını ve parolayı belirleyerek hesap oluşturunuz ve Done ile ilerleyiniz.	☐ Tamamlandı

Adım	Yapılacak İşlem	Kontrol
13	Ubuntu Pro yükseltme ekranında (Upgrade to Ubuntu Pro) Skip for now seçeneğini seçiniz ve Continue ile ilerleyiniz.	☐ Tamamlandı
14	SSH yapılandırma ekranında (SSH Configuration) Install OpenSSH server seçeneğini işaretleyiniz ve Done ile ilerleyiniz.	☐ Tamamlandı
15	Ek yazılım seçim ekranında (Featured Server Snaps) herhangi bir seçim yapmadan Done ile ilerleyiniz.	☐ Tamamlandı
16	Kurulumun tamamlanmasını bekleyiniz. Ardından Reboot Now seçeneğiyle sistemi yeniden başlatınız.	☐ Tamamlandı
17	USB belleği çıkarınız. Sistem açıldıktan sonra oluşturduğunuz kullanıcı adı ve parolayla oturum açınız.	☐ Tamamlandı
18	Sistemi güncelleyiniz.	☐ Tamamlandı

Değerlendirme

Çalışmanız öğretmeniniz tarafından kontrol listesine göre değerlendirilecektir. Çalışmanızı yaparken buradaki ölçütleri dikkate alınız. Kontrol listesi formuna ulaşmak için karekodu okutunuz. Dijital yayınlarda karekodun üstüne tıklayarak içeriğe ulaşabilirsiniz.

Arkadaşınızın öğrenme sürecine katkısını değerlendirmek için akran değerlendirme formunu doldurunuz. Formu tamamladıktan sonra öğretmeninizle paylaşınız veya EBA Portfolyo'ya yükleyiniz. Akran değerlendirme formuna ulaşmak için karekodu okutunuz. Dijital yayınlarda karekodun üstüne tıklayarak içeriğe ulaşabilirsiniz.

3.2.2. Sunucu İşletim Sistemi Yapılandırması

Kurulumu tamamlanan bir sunucu, henüz herhangi bir hizmet sunmaya hazır değildir. Ağdaki diğer cihazların sunucuya bağlanabilmesi, dosya alışverişi yapabilmesi veya uzaktan erişim sağlayabilmesi için sunucuya gerekli servislerin kurulması ve yapılandırılması gerekir. Bu işleme **servis yapılandırması** denir.

Servis yapılandırması, önce sunucunun hangi hizmetleri sunacağının belirlenmesiyle başlar. Ardından ilgili servis kurulur, çalıştırılır ve gerekli ayarlar yapılır. Her servisin kendine ait bir yapılandırma dosyası vardır. Bu dosyalar genellikle **/etc** dizini altında yer alır ve servisin nasıl davranacağını belirler.

KONTROL NOKTASI

Bir servisi kurmak, o servisin çalıştığı anlamına gelmez. Kurulum tamamlandıktan sonra servis mutlaka başlatılmalı, durumu kontrol edilmeli ve sistem yeniden başlatıldığında otomatik olarak devreye girmesi için etkinleştirilmelidir.

3.2.2.1. SSH Servisi

SSH [Secure Shell (Güvenli Kabuk)], ağ üzerindeki bir sunucuya uzaktan ve güvenli biçimde bağlanmayı sağlayan bir protokoldür. Bağlantı sırasında iletilen tüm veriler şifrelenir. Bu sayede kullanıcı adı, parola, komutlar gibi hassas bilgiler ele geçirilemez. Bu özelliği SSH'ı sunucu yönetiminde en yaygın kullanılan uzaktan erişim yöntemi hâline getirmiştir.

SSH bağlantısı iki bileşenden oluşur: Sunucu tarafında çalışan **SSH sunucusu (OpenSSH Server)** ve istemci tarafında kullanılan **SSH istemcisi.** Sunucuya bağlanmak isteyen istemci, SSH istemcisi aracılığıyla sunucuya bağlantı isteği gönderir. Sunucu bu isteği doğrulayarak güvenli bir oturum açar.

BİLGİ KUTUSU : Telnet ve SSH

SSH'tan önce sunuculara uzaktan bağlanmak için Telnet protokolü kullanılırdı. Telnet, verileri şifrelemeden düz metin olarak iletirdi. Bu durum kullanıcı adı, kullanıcı parolası gibi bilgilerin ağ üzerinde kolayca ele geçirilmesine yol açardı. SSH, Telnet'in bu güvenlik açığını gidermek amacıyla geliştirilmiştir. Bugün sunucu yönetiminde Telnet'in yerini tamamen SSH almıştır.

Açık kaynak kodlu sunucu işletim sisteminde SSH servisi **systemctl** komutu aracılığıyla yönetilir. systemctl; servisleri başlatmak, durdurmak, yeniden başlatmak ve sistem açılışında otomatik olarak devreye alınmasını sağlamak için kullanılan bir sistem yönetim aracıdır. SSH servisinin kurulumu ve yönetiminde kullanılan temel komutlar Tablo 3.32'de verilmiştir.

Tablo 3.32: SSH Servis Yönetimi Komutları

Komut	Açıklama	Örnek
sudo apt install openssh-server	SSH sunucusunu kurar.	sudo apt install openssh-server -y
sudo systemctl status ssh	SSH servisinin çalışma durumunu gösterir.	sudo systemctl status ssh
sudo systemctl start ssh	SSH servisini başlatır.	sudo systemctl start ssh
sudo systemctl stop ssh	SSH servisini durdurur.	sudo systemctl stop ssh
sudo systemctl restart ssh	SSH servisini yeniden başlatır.	sudo systemctl restart ssh
sudo systemctl enable ssh	SSH servisinin sistem açılışında otomatik başlamasını sağlar.	sudo systemctl enable ssh
sudo systemctl disable ssh	SSH servisinin sistem açılışında otomatik başlamasını devre dışı bırakır.	sudo systemctl disable ssh
ssh [kullanıcı]@[IP]	Belirtilen sunucuya SSH ile bağlanır.	ssh siber@192.168.1.10

SİBER GÜVENLİK PENCERESİ

SSH güvenli bir protokol olsa da yanlış yapılandırıldığında ciddi riskler doğurabilir. Root kullanıcısıyla doğrudan SSH bağlantısına izin vermek, zayıf parola kullanmak ve varsayılan port numarasını değiştirmemek en yaygın güvenlik hatalarındandır. SSH yapılandırması yapılırken bu noktalara özellikle dikkat edilmelidir.

21. ÖRNEK UYGULAMA

Aşağıdaki adımları izleyerek açık kaynak kodlu sunucu işletim sistemi üzerinde SSH servisini yapılandırınız.

1. Adım: Açık kaynak kodlu sunucu işletim sisteminde kullanıcı adı ve parolanızla oturum açınız.

2. Adım: **sudo apt update** komutuyla paket listesini güncelleyiniz (Görsel 3.93).

```
siberadmin@siber:~$ sudo apt update
Hit:1 http://archive.ubuntu.com/ubuntu resolute InRelease
Hit:2 http://security.ubuntu.com/ubuntu resolute-security InRelease
Hit:3 http://archive.ubuntu.com/ubuntu resolute-updates InRelease
Hit:4 http://archive.ubuntu.com/ubuntu resolute-backports InRelease
All packages are up to date.
```

Görsel 3.93: Paket listesinin güncellenmesi

3. Adım: **sudo systemctl status ssh** komutuyla SSH servisinin kurulu olup olmadığını kontrol ediniz (Görsel 3.94).

```
siberadmin@siber:~$ sudo systemctl status ssh
Unit ssh.service could not be found.
```

Görsel 3.94: SSH servisinin durum kontrolü

> **Not:** Kurulum sırasında **Install OpenSSH server** seçeneği işaretlendiyse SSH servisi zaten kurulu gelir ve servis durumu ekranda görüntülenir. Servis kurulu değilse bir sonraki adımı uygulayınız, kuruluysa 5. adıma geçiniz.

4. Adım: **sudo apt install openssh-server -y** komutuyla SSH servisini kurunuz.

5. Adım: **sudo systemctl start ssh** komutuyla SSH servisini başlatınız.

6. Adım: **sudo systemctl enable ssh** komutuyla SSH servisinin sistem açılışında otomatik olarak devreye girmesini sağlayınız (Görsel 3.95).

```
siberadmin@siber:~$ sudo systemctl start ssh
siberadmin@siber:~$ sudo systemctl enable ssh
Synchronizing state of ssh.service with SysV service script with /usr/lib/systemd/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable ssh
Created symlink '/etc/systemd/system/sshd.service' → '/usr/lib/systemd/system/ssh.service'.
Created symlink '/etc/systemd/system/multi-user.target.wants/ssh.service' → '/usr/lib/systemd/system/ssh.service'.
```

Görsel 3.95: SSH servisinin sistem açılışında otomatik başlatılması

7. Adım: **sudo systemctl status ssh** komutuyla SSH servisinin çalıştığını doğrulayınız (Görsel 3.96).

```
siberadmin@siber:~$ sudo systemctl status ssh
● ssh.service - OpenBSD Secure Shell server
     Loaded: loaded (/usr/lib/systemd/system/ssh.service; enabled; preset: enabled)
     Active: active (running) since Tue 2026-06-09 20:19:37 UTC; 50s ago
 Invocation: fcd613275daa48d3b3ba6da153543447
TriggeredBy: ● ssh.socket
       Docs: man:sshd(8)
             man:sshd_config(5)
   Main PID: 19748 (sshd)
      Tasks: 1 (limit: 2264)
     Memory: 1.1M (peak: 2M)
        CPU: 16ms
     CGroup: /system.slice/ssh.service
             └─19748 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"

Jun 09 20:19:37 siber systemd[1]: Starting ssh.service - OpenBSD Secure Shell server...
Jun 09 20:19:37 siber sshd[19748]: Server listening on 0.0.0.0 port 22.
Jun 09 20:19:37 siber sshd[19748]: Server listening on :: port 22.
Jun 09 20:19:37 siber systemd[1]: Started ssh.service - OpenBSD Secure Shell server.
```

Görsel 3.96: SSH servisinin çalışır olduğunun doğrulanması

8. Adım: **ip a** komutuyla sunucunun IP adresini öğreniniz (Görsel 3.97).

```
siberadmin@siber:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: enp0s8: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 08:00:27:3f:f8:86 brd ff:ff:ff:ff:ff:ff
    altname enx0800273ff886
    inet 10.0.2.15/24 metric 100 brd 10.0.2.255 scope global dynamic enp0s8
       valid_lft 85619sec preferred_lft 85619sec
    inet6 fd17:625c:f037:2:a00:27ff:fe3f:f886/64 scope global dynamic mngtmpaddr noprefixroute
       valid_lft 86158sec preferred_lft 14158sec
    inet6 fe80::a00:27ff:fe3f:f886/64 scope link proto kernel_ll
       valid_lft forever preferred_lft forever
```

Görsel 3.97: Sunucunun IP adresinin görüntülenmesi

10. ETKİNLİK

Etkinlik Adı	SSH Servis Yapılandırması
Süre	20 dakika
Amaç	Açık kaynak kodlu sunucu işletim sistemi üzerinde SSH servisini kurarak yapılandırmak ve servisin çalışır durumda olduğunu doğrulamak
Yönerge	Aşağıdaki adımları sırasıyla gerçekleştiriniz. Her adımı tamamladığınızda Kontrol sütununa tik (✓) atarak işaretleyiniz.

Uygulama Adımları

Adım	Yapılacak İşlem	Kontrol
1	Açık kaynak kodlu sunucu işletim sisteminde kullanıcı adı ve parolanızla oturum açınız.	☐ Tamamlandı
2	Paket listesini güncelleyiniz.	☐ Tamamlandı
3	SSH servisinin kurulu olup olmadığını kontrol ediniz.	☐ Tamamlandı
4	SSH servisi kurulu değilse kurunuz.	☐ Tamamlandı

Adım	Yapılacak İşlem	Kontrol
5	SSH servisini başlatınız.	☐ Tamamlandı
6	SSH servisinin sistem açılışında otomatik devreye girmesini sağlayınız.	☐ Tamamlandı
7	SSH servisinin çalıştığını doğrulayınız.	☐ Tamamlandı
8	SSH servisinin sistem açılışında otomatik devreye girmesini kapatınız.	☐ Tamamlandı
9	Sunucunun IP adresini öğreniniz.	☐ Tamamlandı

Değerlendirme

Çalışmanız öğretmeniniz tarafından kontrol listesine göre değerlendirilecektir. Çalışmanızı yaparken buradaki ölçütleri dikkate alınız. Kontrol listesi formuna ulaşmak için karekodu okutunuz. Dijital yayınlarda karekodun üstüne tıklayarak içeriğe ulaşabilirsiniz.

3.2.3. Sunucuda Veri Güvenliği

Bir sunucu ağa açıldığı andan itibaren çeşitli tehditlere maruz kalabilir. Yetkisiz erişim denemeleri, zayıf parolalar, gereksiz açık portlar ve güncellenmeyen yazılımlar sunucuyu savunmasız bırakır. Bu nedenle servis yapılandırması tamamlandıktan sonra güvenlik adımlarının uygulanması zorunludur.

Sunucuda veri güvenliği; yetkisiz erişimi engellemek, verilerin gizliliğini ve bütünlüğünü korumakla olası saldırılara karşı sistemi güçlendirmek amacıyla alınan önlemlerin bütünüdür. Bu önlemler tek seferlik yapılan işlemler değildir düzenli olarak gözden geçirilmesi ve güncellenmesi gereken sürekli bir süreçtir.

3.2.3.1. Sistem Güncellemeleri

Sunucuda yüklü olan yazılımlar zamanla güvenlik açıkları barındırabilir. Bu açıkların kapatılması için sistem ve paketlerin düzenli olarak güncellenmesi gerekir. Güncellenmemiş bir sistem, saldırganların kolayca istismar edebileceği bilinen zafiyetler içerebilir. Sunucu güncellemelerinde de açık kaynak kodlu işletim sistemlerinde kullanılan güncelleme komutları kullanılır.

3.2.3.2. Güvenlik Duvarı Yapılandırması

Güvenlik duvarı, sunucuya gelen ve sunucudan giden ağ trafiğini denetleyerek yalnızca izin verilen bağlantıların geçmesini sağlar. Açık kaynak kodlu sunucu işletim sisteminde güvenlik duvarı yönetimi için **UFW [Uncomplicated Firewall (Karmaşık Olmayan Güvenlik Duvarı)]** kullanılır. UFW, karmaşık güvenlik duvarı kurallarını basit komutlarla yönetmeyi sağlar (Tablo 3.33).

Tablo 3. 33: UFW Güvenlik Duvarı Komutları

Komut	Açıklama	Örnek
sudo ufw status	Güvenlik duvarının durumunu gösterir.	sudo ufw status
sudo ufw enable	Güvenlik duvarını etkinleştirir.	sudo ufw enable
sudo ufw disable	Güvenlik duvarını devre dışı bırakır.	sudo ufw disable
sudo ufw allow [port/servis]	Belirtilen port veya servise izin verir.	sudo ufw allow ssh

sudo ufw deny [port/servis]	Belirtilen port veya servisi engeller.	sudo ufw deny 23
sudo ufw allow [port]/tcp	Belirtilen TCP portuna izin verir.	sudo ufw allow 22/tcp
sudo ufw delete allow [port]	Daha önce tanımlanan izin kuralını siler.	sudo ufw delete allow 22

KONTROL NOKTASI

Güvenlik duvarını etkinleştirmeden önce SSH portuna (22) izin verildiğinden emin olunuz. Aksi hâlde sunucuya uzaktan bağlantı kesilir.

3.2.3.3. SSH Güvenlik Ayarları

SSH servisi varsayılan ayarlarıyla çalışmaya başlasa da bazı yapılandırma değişiklikleri güvenliği önemli ölçüde artırır. SSH yapılandırması **/etc/ssh/sshd_config** dosyası üzerinden yapılır. Bu dosyada yapılan değişiklikler SSH servisinin yeniden başlatılmasıyla geçerli olur. SSH güvenlik ayarlarında kullanılan temel parametreler ve komutlar Tablo 3.34'te verilmiştir.

Tablo 3.34: SSH Güvenlik Ayarları Komutları

Komut	Açıklama	Örnek
sudo nano /etc/ssh/ sshd_config	SSH yapılandırma dosyasını açar.	sudo nano /etc/ssh/ sshd_config
PermitRootLogin no	Root kullanıcısının SSH ile doğrudan bağlanmasını engeller.	PermitRootLogin no
Port 22	SSH'ın dinlediği port numarasını belirler. Varsayılan 22'dir.	Port 2222
MaxAuthTries 3	Başarısız giriş denemesi sayısını sınırlar.	MaxAuthTries 3
sudo systemctl restart ssh	Yapılandırma değişikliklerini uygulamak için SSH servisini yeniden başlatır.	sudo systemctl restart ssh

3.2.3.4. Kullanıcı Yetkilendirme

Açık kaynak kodlu işletim sistemlerinde her kullanıcının belirli yetkileri vardır. Sunucu güvenliği açısından her kullanıcıya yalnızca ihtiyaç duyduğu kadar yetki verilmesi gerekir. Bu ilke **en az ayrıcalık ilkesi** olarak bilinir. **Root** kullanıcısıyla doğrudan çalışmak yerine **sudo** yetkisine sahip standart bir kullanıcı hesabı kullanmak hem güvenliği artırır hem de olası hataların etkisini sınırlar (Tablo 3.35).

Tablo 3.35: Kullanıcı Yetkilendirme Komutları

Komut	Açıklama	Örnek
sudo adduser [kullanıcı]	Yeni kullanıcı oluşturur.	sudo adduser siber
sudo usermod -aG sudo [kullanıcı]	Kullanıcıya sudo yetkisi verir.	sudo usermod -aG sudo siber
sudo deluser [kullanıcı]	Kullanıcıyı siler.	sudo deluser siber
sudo passwd [kullanıcı]	Kullanıcı parolasını değiştirir.	sudo passwd siber

sudo passwd -l [kullanıcı]	Kullanıcı hesabını kilitler.	sudo passwd -l siber
id [kullanıcı]	Kullanıcının kimlik ve grup bilgilerini gösterir.	id siber

SİBER GÜVENLİK PENCERESİ

Sunucu güvenliğinin en kritik noktalarından biri root hesabının yönetimidir. Root kullanıcısı sistemde sınırsız yetkiye sahiptir, bu nedenle root hesabıyla SSH bağlantısına izin vermek ciddi bir güvenlik açığı oluşturur. Bunun yerine sudo yetkisine sahip standart bir kullanıcı hesabı kullanılmalı, root hesabıyla doğrudan SSH bağlantısı **/etc/ssh/sshd_config** dosyasında **PermitRootLogin no** parametresiyle engellenmelidir.

22. ÖRNEK UYGULAMA

Aşağıdaki adımları izleyerek açık kaynak kodlu sunucu işletim sistemi üzerinde veri güvenliği adımlarını uygulayınız.

1. Adım: **sudo apt update && sudo apt upgrade -y** komutuyla sistemi güncelleyiniz (Görsel 3.98).

```
siberadmin@siber:~$ sudo apt update && sudo apt upgrade -y
Hit:1 http://security.ubuntu.com/ubuntu resolute-security InRelease
Hit:2 http://archive.ubuntu.com/ubuntu resolute InRelease
Hit:3 http://archive.ubuntu.com/ubuntu resolute-updates InRelease
Hit:4 http://archive.ubuntu.com/ubuntu resolute-backports InRelease
All packages are up to date.
The following packages were automatically installed and are no longer required:
  linux-headers-7.0.0-14          linux-image-unsigned-7.0.0-14-generic    linux-modules-7.0.0-14-generic  linux-tools-7.0.0-14-generic
  linux-headers-7.0.0-14-generic  linux-main-modules-zfs-7.0.0-14-generic  linux-tools-7.0.0-14
Use 'sudo apt autoremove' to remove them.

Summary:
  Upgrading: 0, Installing: 0, Removing: 0, Not Upgrading: 0
```

Görsel 3.98: Sistem güncellemesinin yapılması

2. Adım: **sudo ufw status** komutuyla güvenlik duvarının durumunu kontrol ediniz (Görsel 3.99).

```
siberadmin@siber:~$ sudo ufw status
Status: inactive
```

Görsel 3.99: Güvenlik duvarı durumunun görüntülenmesi

3. Adım: **sudo ufw allow ssh** komutuyla SSH bağlantısına izin veriniz (Görsel 3.100).

```
siberadmin@siber:~$ sudo ufw allow ssh
Rules updated
Rules updated (v6)
```

Görsel 3.100: SSH bağlantısına izin verilmesi

4. Adım: **sudo ufw enable** komutuyla güvenlik duvarını etkinleştiriniz.

5. Adım: **sudo ufw status** komutuyla güvenlik duvarının aktif olduğunu ve SSH'a izin verildiğini doğrulayınız (Görsel 3.101).

```
siberadmin@siber:~$ sudo ufw enable
Firewall is active and enabled on system startup
siberadmin@siber:~$ sudo ufw status
Status: active

To                         Action      From
--                         ------      ----
22/tcp                     ALLOW       Anywhere
22/tcp (v6)                ALLOW       Anywhere (v6)
```

Görsel 3.101: Güvenlik duvarı kurallarının doğrulanması

6. Adım: **sudo nano /etc/ssh/sshd_config** komutuyla SSH yapılandırma dosyasını açınız (Görsel 3.102).

```
  GNU nano 8.7.1                                                /etc/ssh/sshd_config
# This is the sshd server system-wide configuration file.  See
# sshd_config(5) for more information.

# This sshd was compiled with PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games

# The strategy used for options in the default sshd_config shipped with
# OpenSSH is to specify options with their default value where
# possible, but leave them commented.  Uncommented options override the
# default value.

# In general, the first uncommented definition of an option takes precedence.
# For options that accept multiple values, like 'Port', subsequent definitions
# are appended to the configuration.
#
```

Görsel 3.102: SSH yapılandırma dosyasının açılması

7. Adım: Dosyada **PermitRootLogin** satırını bularak değerini **no** olarak ayarlayınız. **MaxAuthTries** değerini **3** olarak güncelleyiniz. Ctrl+O ve Enter ile kaydedip Ctrl+X ile çıkınız (Görsel 3.103).

```
# Authentication:

#LoginGraceTime 2m
#PermitRootLogin no
#StrictModes yes
#MaxAuthTries 3
#MaxSessions 10
```

Görsel 3.103: SSH güvenlik ayalarının yapılandırılması

8. Adım: **sudo systemctl restart ssh** komutuyla SSH servisini yeniden başlatarak değişiklikleri uygulayınız.

9. Adım: **sudo adduser testuser** komutuyla yeni bir kullanıcı oluşturunuz (Görsel 3.104).

```
siberadmin@siber:~$ sudo adduser testuser
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for testuser
Enter the new value, or press ENTER for the default
        Full Name []: Test User
        Room Number []: 1
        Work Phone []: 05XXXXXXXXX
        Home Phone []: 05XXXXXXXXX
        Other []:
Is the information correct? [Y/n] y
```

Görsel 3.104: Yeni kullanıcı oluşturulması

10. Adım: **sudo usermod -aG sudo testuser** komutuyla oluşturduğunuz kullanıcıya sudo yetkisi veriniz.

11. Adım: **id testuser** komutuyla kullanıcının kimlik ve grup bilgilerini görüntüleyerek sudo yetkisinin verildiğini doğrulayınız (Görsel 3.105).

```
siberadmin@siber:~$ sudo usermod -aG sudo testuser
siberadmin@siber:~$ id testuser
uid=1001(testuser) gid=1001(testuser) groups=1001(testuser),27(sudo),100(users)
```

Görsel 3.105: Kullanıcı kimlik ve grup bilgilerinin doğrulanması

11. ETKİNLİK

Etkinlik Adı	Sunucuda Veri Güvenliği
Süre	30 dakika
Amaç	Yeni teslim alınan bir sunucuda güvenlik açıklarını tespit ederek gerekli güvenlik adımlarını uygulamak
Yönerge	Aşağıdaki tabloda her adım için yapılacak işlem verilmiştir. Uygun komutu belirleyerek uygulayınız. Her adımı tamamladığınızda Kontrol sütununa tik (✓) atarak işaretleyiniz.

Senaryo: Kurumunuza yeni bir sunucu teslim alındı. Sunucunun ağa bağlanmadan önce güvenlik yapılandırmasının tamamlanması gerekmektedir. İlk incelemede güvenlik duvarının kapalı olduğu, root girişine izin verildiği ve test amaçlı oluşturulmuş bir kullanıcı hesabının sistemde hâlâ bulunduğu görüldü. Göreviniz bu açıkları gidererek sunucuyu güvenli hâle getirmektir.

Uygulama Adımları

Adım	Yapılacak İşlem	Kontrol
1	Sistemi güncelleyiniz.	☐ Tamamlandı
2	Güvenlik duvarının durumunu kontrol ediniz.	☐ Tamamlandı
3	SSH bağlantısına izin veriniz.	☐ Tamamlandı
4	Güvenlik duvarını etkinleştiriniz.	☐ Tamamlandı
5	Güvenlik duvarının aktif olduğunu ve SSH'a izin verildiğini doğrulayınız.	☐ Tamamlandı
6	SSH yapılandırma dosyasını açınız.	☐ Tamamlandı
7	Root girişini devre dışı bırakınız ve başarısız giriş denemesi sayısını 3 ile sınırlayınız. Değişiklikleri kaydedip dosyadan çıkınız.	☐ Tamamlandı
8	SSH servisini yeniden başlatarak değişiklikleri uygulayınız.	☐ Tamamlandı
9	testuser adlı kullanıcı hesabını ev diziniyle birlikte siliniz.	☐ Tamamlandı
10	Yeni bir kullanıcı oluşturunuz ve sudo yetkisi veriniz.	☐ Tamamlandı
11	Oluşturduğunuz kullanıcının kimlik ve grup bilgilerini görüntüleyerek sudo yetkisinin verildiğini doğrulayınız.	☐ Tamamlandı

Değerlendirme

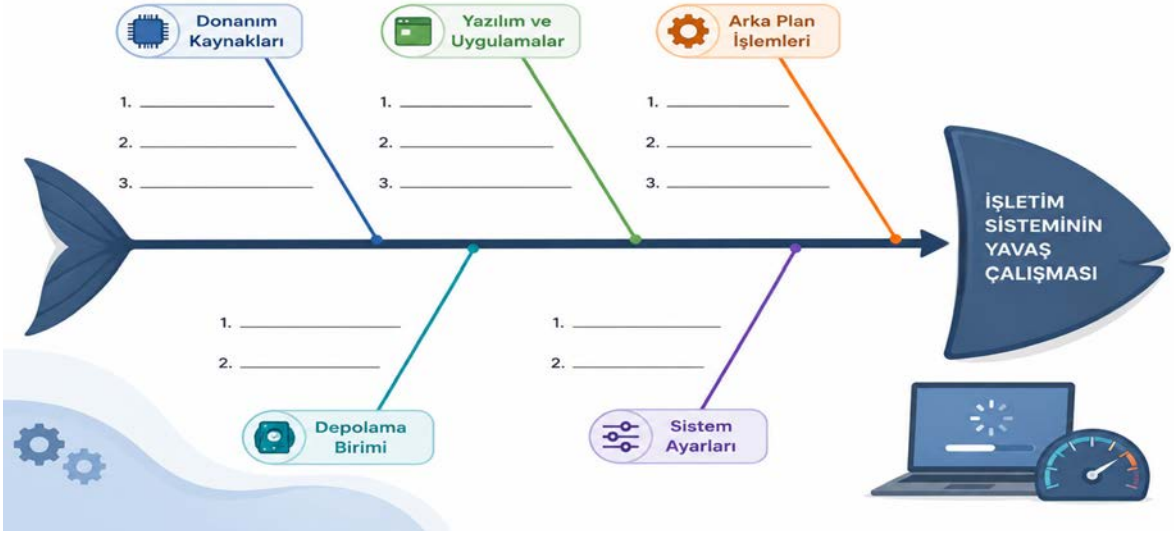
Çalışmanız öğretmeniniz tarafından kontrol listesine göre değerlendirilecektir. Çalışmanızı yaparken buradaki ölçütleri dikkate alınız. Kontrol listesi formuna ulaşmak için karekodu okutunuz. Dijital yayınlarda karekodun üstüne tıklayarak içeriğe ulaşabilirsiniz.

ÖLÇME VE DEĞERLENDİRME

A) Aşağıdaki T tablosunu doldurunuz. Her özellik için masaüstü ve sunucu işletim sistemlerinin nasıl farklılaştığını ilgili sütunlara yazınız.

Masaüstü İşletim Sistemi	Özellik	Sunucu İşletim Sistemi
	Temel amaç	
	Kullanıcı arayüzü	
	Çalışma süresi	
	Kullanıcı sayısı	
	Kaynak yönetimi önceliği	
	Güvenlik önceliği	
	Örnek işletim sistemleri	

B) Aşağıdaki balık kılçığı diyagramında ana problem "işletim sisteminin yavaş çalışması" olarak verilmiştir. Diyagramdaki her dal için işletim sisteminin yavaş çalışmasına neden olabilecek en az iki durum yazınız.



C) Aşağıda verilen işlevleri uygun komutlarla eşleştiriniz. Doğru komutun harfini işlevin başındaki boşluğa yazınız.

	İşlevler	Komutlar
	1. Dosya içinde belirli bir metni arar.	**A)** **ls -la**
	2. Kapalı kaynak kodlu işletim sisteminde ağ arayüzlerini ve IP adreslerini görüntüler.	**B)** chmod
	3. Zamanlanmış görev dosyasını düzenlemek için açar.	**C)** grep
	4. Dizin içeriğini ayrıntılı ve gizli dosyalarla listeler.	**Ç)** ip a
	5. Kullanıcıyı belirtilen gruba ekler.	**D)** crontab -e
	6. Açık kaynak kodlu işletim sisteminde ağ arayüzlerini ve IP adreslerini görüntüler.	**E)** ping
	7. Dosya veya dizin erişim izinlerini değiştirir.	**F)** net user
	8. Kapalı kaynak kodlu işletim sisteminde çalışan süreçleri listeler.	**G)** ipconfig
	9. Sistemdeki kullanıcıları listeler.	**H)** tasklist
	10. Kapalı kaynak kodlu işletim sisteminde tanımlanmış zamanlanmış görevleri listeler.	**I)** schtasksquery
		J) usermod -aG

Ç) Aşağıdaki soruların doğru cevabını işaretleyiniz.

1. Aşağıdakilerden hangisi SSH protokolünün Telnet'ten temel farkını doğru ifade eder?

A) SSH iletilen verileri şifreler, Telnet verileri şifrelemeden düz metin olarak iletir.

B) SSH yalnızca Linux sistemlerinde, Telnet yalnızca Windows sistemlerinde çalışır.

C) SSH yalnızca dosya aktarımı için, Telnet ise uzaktan oturum açmak için kullanılır.

D) SSH bağlantısı için grafik arayüz gerekir, Telnet ise komut satırıyla çalışır.

E) SSH yalnızca 443 numaralı portu, Telnet ise 22 numaralı portu kullanır.

2. **Aşağıdakilerden hangisi sunucu işletim sisteminin masaüstü işletim sisteminden temel farkını doğru ifade eder?**

A) Açık kaynaklı olarak geliştirilir.

B) Tek kullanıcıya hizmet verir.

C) Ağ hizmetleri sunmak için tasarlanmıştır.

D) Yalnızca büyük kurumlarda kullanılabilir.

E) Masaüstü uygulamalarını çalıştırmaz.

3. **Bir açık kaynak kodlu işletim sisteminde crontab -e komutu ne işe yarar?**

A) Sistemdeki mevcut zamanlanmış görevleri listeler.

B) Daha önce oluşturulmuş tüm zamanlanmış görevleri siler.

C) Sistemdeki tüm kullanıcıların cron görevlerini görüntüler.

D) Zamanlanmış görev dosyasını açarak düzenleme yapılmasını sağlar.

E) Zamanlanmış görevin son çalışma zamanını görüntüler.

4. **Bir açık kaynak kodlu işletim sisteminde chmod 644 rapor.txt komutu çalıştırıldığında dosyaya hangi izinler tanınmış olur?**

A) Sahibi dosyayı okuyabilir, çalıştırabilir ve dosyaya yazabilir; diğerleri dosyaya hiçbir işlem yapamaz.

B) Sahibi dosyayı okuyabilir ve dosyaya yazabilir; grup ve diğer kullanıcılar dosyayı yalnızca okuyabilir.

C) Tüm kullanıcılar dosyayı okuyabilir, çalıştırabilir ve dosyaya yazabilir.

D) Sahibi tüm izinlere sahiptir; diğerleri dosyayı yalnızca çalıştırabilir.

E) Sahibi dosyayı okuyabilir; grup ve diğer kullanıcılar dosyayı okuyabilir ve dosyaya yazabilir.

D) Senaryo temelli soruları cevaplayınız.

1-3. soruları aşağıdaki senaryoya göre cevaplayınız.

Bir okul, tüm öğrenci dosyalarını saklamak ve öğretmenlerin bu dosyalara ağ üzerinden erişmesini sağlamak amacıyla yeni bir sunucu kurmaktadır. Sistem yöneticisi sunucu için işletim sistemi seçimi yapacaktır. Değerlendirme ölçütleri sunucunun 7/24 kesintisiz çalışması, sunucuya çok kullanıcılı erişim, güvenlik güncellemelerinin düzenli sağlanması ve lisans maliyetidir.

1. **Sistem yöneticisinin bu okul için işletim sistemi seçiminde öncelikle göz önünde bulundurması gereken ölçüt aşağıdakilerden hangisidir?**

   A) 7/24 kesintisiz ve kararlı çalışması

   B) Grafik arayüzünün gelişmiş olması

   C) Tek kullanıcılı erişimi desteklemesi

   D) Yüksek multimedya performansı sunması

   E) Yalnızca kablolu ağlarda çalışabilmesi

2. **Sistem yöneticisi lisans maliyetini de göz önünde bulundurursa bağlamdaki okul için aşağıdakilerden hangisi <u>en uygun</u> olur?**

   A) Ticari lisanslı masaüstü işletim sistemi

   B) Yalnızca mobil cihazlar için geliştirilmiş işletim sistemi

   C) Tek kullanıcılı masaüstü işletim sistemi

   D) Grafik arayüz odaklı bireysel kullanım işletim sistemi

   E) Açık kaynaklı sunucu işletim sistemi

3. **Kurulan sunucuya ağ üzerinden güvenli uzaktan erişim sağlamak için aşağıdaki adımlardan hangisi öncelikle yapılmalıdır?**

   A) Sunucuya grafik arayüz kurulmalıdır.

   B) Güvenlik duvarı devre dışı bırakılmalıdır.

   C) SSH servisi kurularak yapılandırılmalıdır.

   D) Tüm kullanıcılara root yetkisi verilmelidir.

   E) Sunucu yeniden başlatılmalıdır.

4-6. soruları aşağıdaki senaryoya göre cevaplayınız.

Bir sistem yöneticisi, bilgisayar hakkında temel bilgileri ekrana yazdıran ve çalışan süreçleri bir dosyaya kaydeden PowerShell betiği yazmıştır. Betik; sistem tarihini, aktif kullanıcı adını ve bilgisayar adını değişkenlere atayarak ekrana yazdırmakta ardından o an çalışan tüm süreçleri **C:\Lab\surecler.txt** dosyasına kaydetmektedir.

```
$tarih = Get-Date
$kullanici = $env:USERNAME
$bilgisayar = $env:COMPUTERNAME
Write-Host "Tarih: $tarih"
Write-Host "Kullanıcı: $kullanici"
Write-Host "Bilgisayar: $bilgisayar"
Get-Process | Out-File C:\Lab\surecler.txt
```

4. **Betikteki $tarih, $kullanici ve $bilgisayar ifadelerinin kullanım amacı aşağıdakilerden hangisidir?**

A) Betik dosyasına açıklama satırı eklemek

B) Dosyaya veri yazmayı sağlamak

C) Betik çalışma iznini ayarlamak

D) Ağ bağlantısını kontrol etmek

E) Sistem bilgilerini geçici olarak saklamak

5. **Get-Process | Out-File C:\Lab\surecler.txt satırı çalıştırıldığında aşağıdakilerden hangisi gerçekleşir?**

A) Sistemdeki tüm dosyalar listelenir ve ekrana yazdırılır.

B) Çalışan süreçler listelenerek belirtilen dosyaya kaydedilir.

C) Belirtilen dizindeki dosyalar silinir.

D) Sistem servisleri durdurularak bir rapora aktarılır.

E) Ağ bağlantıları kontrol edilerek dosyaya yazılır.

6. Bu betiğin çalıştırılabilmesi için öncelikle yapılması gereken ayar aşağıdakilerden hangisidir?

A) SSH servisinin etkinleştirilmesi

B) Güvenlik duvarı kurallarının güncellenmesi

C) Kullanıcı hesabının yeniden oluşturulması

D) PowerShell betik çalıştırma izninin ayarlanması

E) Sistem güncellemelerinin tamamlanması

7-8. soruları aşağıdaki senaryoya göre cevaplayınız.

Utku, bir şirkette sistem yöneticisi olarak çalışmaktadır. Şirkete yeni bir açık kaynak kodlu sunucu işletim sistemi kurulmuş ve Utku'dan bu sunucuyu güvenli biçimde yapılandırması istenmiştir. Utku aşağıdaki komutları sırasıyla çalıştırmıştır:

```
sudo ufw status
sudo ufw allow ssh
sudo ufw enable
sudo nano /etc/ssh/sshd_config
```

sshd_config dosyasını açtığında şu satırları görmüştür:

```
Port 22
PermitRootLogin yes
MaxAuthTries 6
```

7. Utku'nun **sudo ufw allow ssh** komutunu **sudo ufw enable** komutundan önce çalıştırmasının nedeni nedir? Sıra değiştirilseydi ne olurdu?

8. **sshd_config** dosyasındaki hangi ayarlar güvenlik açığı oluşturmaktadır? Bu ayarların nasıl ve neden değiştirilmesi gerektiğini açıklayınız.

4. ÖĞRENME BİRİMİ

SANALLAŞTIRMA VE BULUT BİLİŞİM











KONULAR

4.1. SANALLAŞTIRMA
4.2. BULUT BİLİŞİM

ANAHTAR KAVRAMLAR

- bulut bilişim
- hipervizör
- IaaS
- konteyner
- Kubernetes
- PaaS
- SaaS
- sanal makine
- sanallaştırma

Bu öğrenme biriminde sizden

- sanallaştırma teknolojisinin temel kavramlarını, mimarisini ve bileşenlerini analiz ederek uygun senaryolara göre sanallaştırma ihtiyaçlarını belirlemeniz
- hipervizör türlerini yapısal ve performans yönünden karşılaştırarak, kurumsal veya bireysel ihtiyaçlara uygun hipervizör teknolojisini seçmeniz
- sanal makine oluşturma ve yönetme işlemlerini gerçekleştirmeniz
- bulut bilişim teknolojisinin temel yapı ve hizmet modellerini (IaaS, PaaS, SaaS) kurumsal mimarideki işlevlerine göre sınıflandırmanız ve ihtiyaca uygun bulut modelini projelendirmeniz
- sanallaştırma ile bulut bilişim arasındaki teknolojik bağı kurarak, sanallaştırılmış bir altyapıyı bulut servis modeline (IaaS/PaaS) dönüştürme süreçlerini açıklamanız ve planlamanız

beklenmektedir.

HAZIRLIK ÇALIŞMASI

1. Bilgisayarınıza yüklü bir yazılım (çevrim dışı) ve internet üzerinden kullandığınız bir uygulamayı (çevrim içi) ele alınız. Bu iki yöntemin kullanım özelliklerini karşılaştırınız.
2. Çevrim dışı ve çevrim içi uygulamaları erişim hızı, veri depolama ve kullanım kolaylığı ölçütlerine göre değerlendiriniz.
3. Çevrim dışı ve çevrim içi uygulama başlıklarının etrafındaki noktalı yerlere bu kavramların zihninizde çağrıştırdığı sözcükleri yazınız.

..... **Çevrim Dışı Uygulama**	..... **Çevrim İçi Uygulama** .....

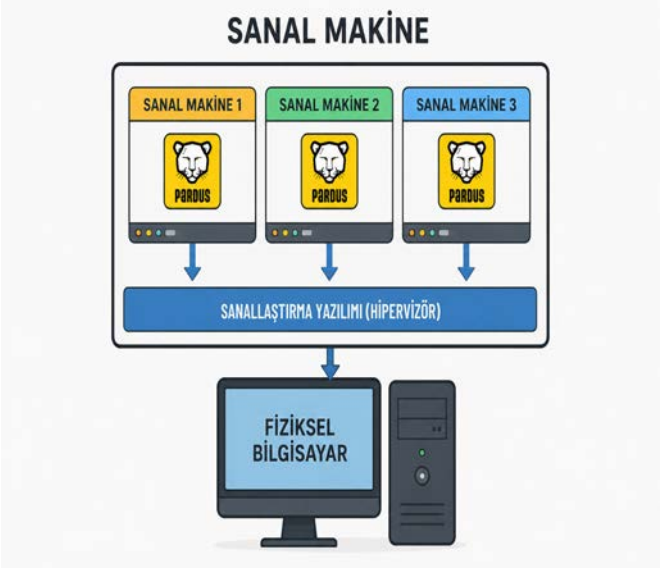
BAŞLARKEN

Sanallaştırma ve bulut bilişim teknolojileri, bilişim dünyasının temel yapı taşlarından biridir ve hem bireysel hem de kurumsal düzeyde yaygın olarak kullanılır. Sanallaştırma teknolojisi sayesinde tek bir fiziksel donanım üzerinde birden fazla işletim sistemi ve uygulama çalıştırılabilirken bu durumla donanım kaynaklarının daha verimli kullanılması sağlanır. Hipervizör yapıları, sanal makineler ve konteynerler bu teknolojinin temelini oluşturarak sistemlerin esnek, güvenli ve yönetilebilir olmasına katkı sağlar.

Bulut bilişim ise verilerin ve uygulamaların internet üzerinden erişilebilir hâle gelmesini sağlayarak kullanıcıların her yerden hizmet alabilmesine imkân tanır. IaaS, PaaS, SaaS gibi hizmet modelleri, farklı ihtiyaçlara yönelik çözümler sunarken bilişim altyapılarının daha ölçeklenebilir ve ekonomik olmasını sağlar. Sanallaştırma ve bulut bilişim arasındaki güçlü ilişki, modern veri merkezlerinin ve dijital hizmetlerin temelini oluşturur.

4.1. SANALLAŞTIRMA

Sanallaştırma (Virtualization); tek bir fiziksel donanımın yazılım ile mantıksal alanlara bölünerek birbirinden bağımsız birden fazla işletim sisteminin veya uygulamanın aynı anda çalıştırılmasını sağlayan teknolojidir. Sanallaştırmada kullanılan en önemli kavramlardan biri de **sanal makinedir [Virtual Machine (VM)]**. Sanal makine ile fiziksel bir cihaz yazılımla taklit edilir ve sanki gerçek bir cihaz çalışıyor gibi davranan sanal ortam oluşturulur (Görsel 4.1).



Görsel 4.1: Tek donanımda üç işletim sistemi çalıştıran sanal makineler

4.1.1. Hipervizör Türleri

Tek bir donanım üzerinde birbirinden bağımsız ve farklı işletim sistemlerinin kurulabilmesi için birden fazla sanal makine (virtual machine) oluşturulması en kolay yöntemdir. Sanal makineler oluşturmak için kullanılan yazılım katmanına **hipervizör** denir. Hipervizör özellikle işlemci, bellek, ağ gibi donanım kaynaklarını yönetir ve bu donanımları sanal makinelere paylaştırır. Bu sayede her sanal makine kendi işletim sistemine ve donanımına sahipmiş gibi bağımsız çalışır ancak gerçekte sadece tek bir donanım üzerinde işlemler gerçekleşir. Hipervizörün temel görevleri şunlardır:

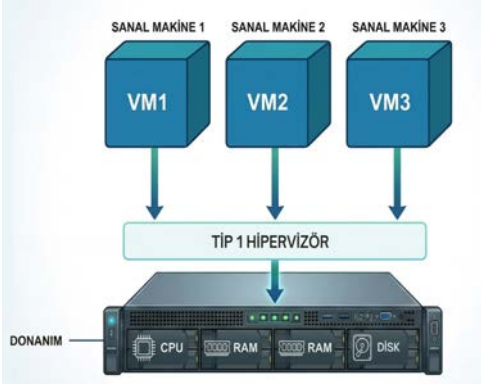
- İşlemci, bellek ve ağ donanımlarını paylaştırmak
- Sanal makinelerin birbirinden bağımsız çalışmasını sağlamak
- Belleğin verimli yönetilmesini sağlamak
- İşlemci paylaşım zamanlamasını düzenlemek
- Sanal makinelerin başlatılması, durdurulması ve izlenmesini sağlamak

Bunlar sağlandığında tek bir fiziksel donanım üzerinde farklı işletim sistemleri aynı anda çalışabilir. Hipervizör yazılımları, donanıma erişim yöntemine göre iki temel türe ayrılır:

- Tip 1 Hipervizör (Bare-Metal Hypervisor)
- Tip 2 Hipervizör (Hosted Hypervisor)

Tip 1 hipervizör, donanıma doğrudan kurularak çalışır. Dolayısıyla arada başka katman olmadığı için kısıtlamalarla karşı karşıya kalmaz (Görsel 4.2). Bu erişim şekli, yüksek çalışma performansı ve güvenilirlik sağlar. Tip 1 hipervizör özellikle dev ölçekli firmalarda, büyük veri merkezlerinde, bulut servis sağlayıcılarında ve yüksek performanslı uygulamalarda tercih edilir. En çok kullanılan açık kaynak kodlu Tip 1 hipervizör uygulamaları şunlardır:

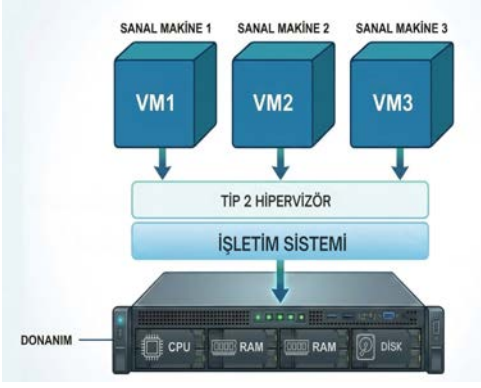
- Xen
- KVM
- Proxmox VE



Görsel 4.2: Tip 1 hipervizör

Tip 2 hipervizör, donanıma doğrudan kurulmaz. İşletim sistemi üzerine kurulur dolayısıyla donanıma direkt erişmez (Görsel 4.3). Donanıma erişmek için işletim sistemini kullanması gerektiği için bazı kısıtlamalara uğrar. Tip 2 hipervizörler, düşük performanslı yazılımlar ve test ortamları için uygundur. Küçük ölçekli firmalar ile kişisel kullanıcıların ihtiyaçlarında veya eğitim ortamlarında tercih edilir. Bunların kurulumu ve kullanımı basittir. En çok kullanılan açık kaynak kodlu Tip 2 hipervizör uygulamaları şunlardır:

- VirtualBox
- QEMU



Görsel 4.3: Tip 2 hipervizör

SIRA SİZDE

Aşağıdaki yapılandırılmış gridde numaralandırılmış kutucuklarda **Tip 1** ve **Tip 2 hipervizörlere** ait özellikler verilmiştir. Soruların cevaplarını kutucuk numaralarını kullanarak ilgili boşluklara yazınız (Her kutucuğu cevap için bir kez kullanabilirsiniz).

1	2	3	4
Donanıma doğrudan kurulur.	Bir işletim sistemi üzerine kurulur.	Yüksek performans sağlar.	Düşük performanslıdır.
5	**6**	**7**	**8**
Veri merkezlerinde kullanılır.	Bireysel amaçlı kullanılır.	Kaynakları doğrudan yönetir.	Kurulumu kolaydır.
9	**10**	**11**	**12**
Güvenilirliği yüksektir.	Test ortamlarında kullanılır.	İşletim sistemi kısıtlamalarıyla karşı karşıyadır.	İşletim sistemi kısıtlamalarına tabi değildir.

	Sorular
A)	Kutucuklarda verilen özelliklerden hangileri Tip 1 (Bare-Metal) Hipervizör kavramı ile ilişkilidir?
	Cevap:.....
B)	Kutucuklarda verilen özelliklerden hangileri Tip 2 (Hosted / Barındırılan) Hipervizör kavramı ile ilişkilidir?
	Cevap: .....

BİLGİ KUTUSU : Hostname (FQDN)

Bir bilgisayarın veya sunucunun ağ üzerindeki tam alan adıdır ve hostname ile domain adının birleşmesinden oluşur.

KONTROL NOKTASI

Donanım Sanallaştırma: BIOS üzerinden Virtualization Technology (VT-x veya AMD-V) özelliğinin **Enabled (Etkin)** olması gerekir.

1. ÖRNEK UYGULAMA

Tip 1 hipervizör yazılımının kurulumunu aşağıdaki adımları izleyerek gerçekleştiriniz.

1. Adım: Tip 1 hipervizör yazılımının imaj dosyasını resmî web sitesinden indiriniz.

2. Adım: İndirilen imaj dosyasını önyüklenebilir olarak USB belleğe yazdırınız.

3. Adım: BIOS/UEFI menüsünden ilk açılış cihazı olarak USB seçiniz.

4. Adım: USB bellek bilgisayara takılıyken cihazı yeniden başlatınız.

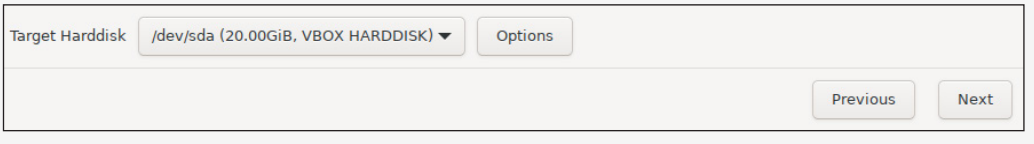
5. Adım: Açılan ekranda Install (Graphical) seçeneği işaretliyken Enter tuşuna basınız (Görsel 4.4).



Görsel 4.4: Açılış ekranı

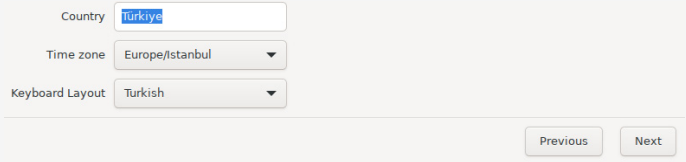
6. Adım: Lisans sözleşmesini kabul etmek için **I agree (Kabul ediyorum.)** düğmesine tıklayınız.

7. Adım: Kurulumun gerçekleştirileceği depolama birimini seçiniz (Görsel 4.5).



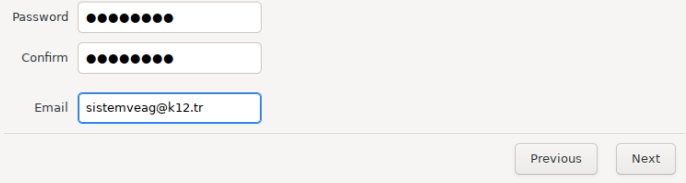
Görsel 4.5: Kurulumun yapılacağı depolama biriminin seçilmesi

8. Adım: Yerelleştirme (Ülke, Zaman dilimi ve Klavye dili) ayarlarını yapınız (Görsel 4.6).



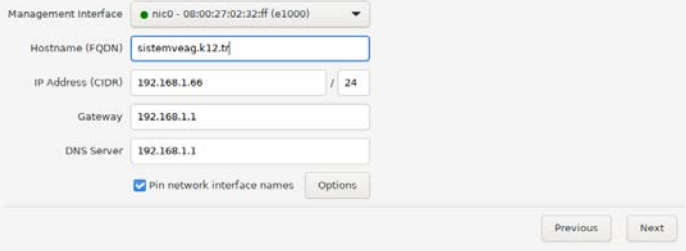
Görsel 4.6: Yerelleştirme ayarları

9. Adım: Yönetici parolası ve e-posta bilgilerini giriniz (Görsel 4.7).



Görsel 4.7: Yönetici parolası ve e-posta girişinin yapılması

10. Adım: Sunucu cihazın ağ yapılandırmasını yapınız (Görsel 4.8).



Görsel 4.8: Sanallaştırma programı ağ ayarları

11. Adım: Kurulum işlemi bitince cihazı yeniden başlatarak açılış ekranını görüntüleyiniz.

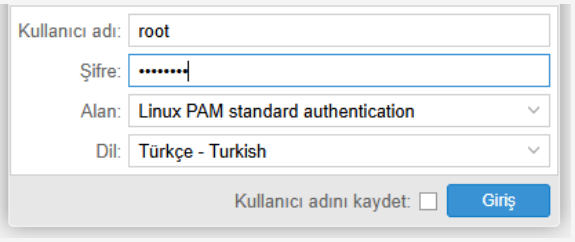
12. Adım: Sunucu bilgisayarın statik IP adresini aynı ağda olmak şartıyla başka bir bilgisayarın web tarayıcısına yazarak sunucu paneline erişim sağlayınız.

13. Adım: Web sayfasındaki Gelişmiş seçeneklerinden **192.168.1.66 adresine devam edin (Güvenli değil)** bağlantısına tıklayarak geçiniz (Görsel 4.9).



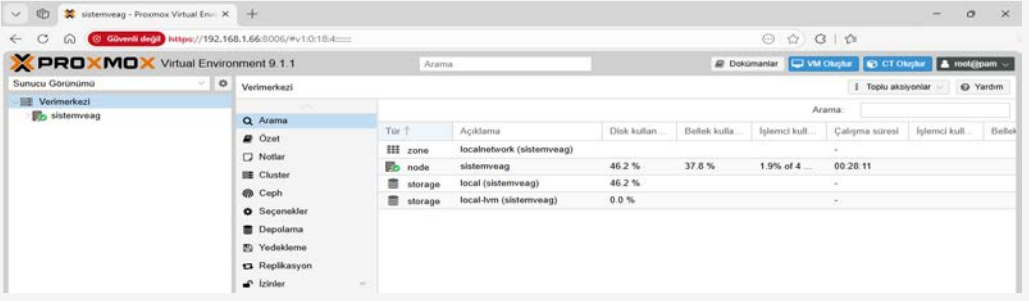
Görsel 4.9: Sanallaştırma programına erişimde güvenlik uyarısı

14. Adım: Sunucu paneline bağlanmak için root kullanıcı adını ve önceden belirlenen parolayı giriniz (Görsel 4.10).



Görsel 4.10: Sanallaştırma programı oturumunun açılması

15. Adım: Açılan sunucu panelini inceleyiniz (Görsel 4.11).



Görsel 4.11: Sanallaştırma programı yönetim paneli

1. ETKİNLİK

Etkinlik Adı	Alternatif Tip 1 Hipervizör Yazılımının Kurulumu ve Sunumu
Süre	Kurulum uygulaması + sunum hazırlama (ders dışı) | 15 dakika sunum
Amaç	Tip 1 hipervizör yazılımının kurulum sürecini adım adım uygulayarak sistemi kullanıma hazır hâle getirmek
Yönerge	Öğretmeniniz Tip 1 hipervizör kurulum sürecini adım adım gösterdikten sonra aşağıdaki adımları izleyerek farklı bir Tip 1 Hipervizör kurunuz. Her adım tamamlandığında **Kontrol** sütununa (✓) işaretleyiniz.

⚠ **İş Sağlığı ve Güvenliği Kuralları**

Elektrik Güvenliği

- Elektrik prizleri, güç kabloları ve uzatma kabloları güvenli şekilde kullanınız; hasarlı ekipman kullanmayınız.
- Kurulum sırasında elektrik kesintisi riskine karşı mümkünse priz koruyucu veya UPS kullanınız.
- USB bellek takma-çıkarma işlemlerini dikkatli yapınız.

Donanım Güvenliği

- USB kurulum belleğini zorlamadan doğru yönde takınız.
- Bilgisayar açılırken BIOS/UEFI ayarlarında yanlış işlem yapmamaya dikkat ediniz.
- Kurulum sırasında depolama birimini yanlışlıkla biçimlendirmemek için disk seçimini dikkatli yapınız.

Çalışma Alanı Düzeni

- Çalışma alanını düzenli tutunuz.
- Kablolar üzerinde yürümeyiniz, takılma ve düşme riskine karşı dikkatli olunuz.
- USB bellek, güç kabloları ve ağ kablolarını gelişigüzel bırakmayınız.
- Grup üyeleri arasında görev paylaşımı yapınız.

Kurulum Adımları

Adım	Yapılacak İşlem	Kontrol
1	Tip 1 hipervizör yazılımının imaj dosyasını indiriniz.	☐ Tamamlandı
2	İndirilen imaj dosyasını önyüklenebilir olarak USB belleğe yazdırınız.	☐ Tamamlandı
3	BIOS/UEFI menüsünden ilk açılış cihazı olarak USB seçiniz.	☐ Tamamlandı
4	USB bellek bilgisayara takılıyken cihazı yeniden başlatınız.	☐ Tamamlandı
5	Tip 1 hipervizör yazılımının kurulumunu yapınız.	☐ Tamamlandı
6	Kurulum adımlarının ekran görüntülerini alınız.	☐ Tamamlandı
7	Bu ekran görüntülerini kullanarak kurulum sunumu hazırlayınız.	☐ Tamamlandı

Sunumda Yer Alacak Bölümler

Bölüm	*İçerik*
1. Hazırlık	ISO dosyasının indirilmesi ve önyüklenebilir USB hazırlama adımları
2. Kurulum Adımları	BIOS/UEFI ayarı, disk seçimi, yönetici oluşturma, ağ yapılandırma
3. Kurulum Sonrası	Sistemin çalışır durumda olduğunu gösteren ekran görüntüsü
4. Sorunlar ve Çözümler	Kurulum sırasında karşılaşılan sorunlar ve nasıl çözüldüğü

Değerlendirme

Çalışmanız öğretmeniniz tarafından analitik dereceli puanlama anahtarına göre değerlendirilecektir. Çalışmanızı yaparken buradaki ölçütleri dikkate alınız. Analitik dereceli puanlama anahtarı formuna ulaşmak için karekodu okutunuz. Dijital yayınlarda karekodun üstüne tıklayarak içeriğe ulaşabilirsiniz.

Öz değerlendirme formunu uygulama sürecinizi dikkate alarak doldurunuz. Formu tamamladıktan sonra öğretmeninizle paylaşınız veya EBA Portfolyo'ya yükleyiniz. Öz değerlendirme formuna ulaşmak için karekodu okutunuz. Dijital yayınlarda karekodun üstüne tıklayarak içeriğe ulaşabilirsiniz.

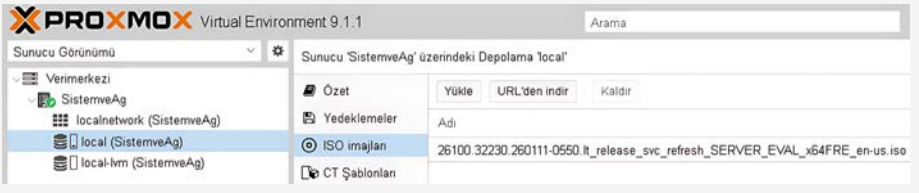
2. ÖRNEK UYGULAMA

Tip 1 hipervizör yazılımı üzerinde sanal makine oluşturma ve sunucu işletim sistemi kurulumunu aşağıdaki adımları izleyerek gerçekleştiriniz.

1. Adım: Sunucu işletim sisteminin ISO kurulum dosyasını resmî web sitesinden indiriniz.

2. Adım: Web tarayıcısından sanallaştırma programı yönetim paneline bağlanınız.

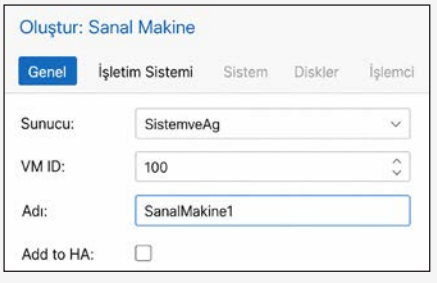
3. Adım: Sanallaştırma programının sol taraftaki menüsünden sanal makine işletim sistemi kurulumu için gerekli ISO dosyasını yerel depolama alanına [local (SistemveAg)] yükleyiniz (Görsel 4.12).



Görsel 4.12: İşletim sistemi ISO dosyasının yüklenmesi

4. Adım: Sanallaştırma programı panelinin sağ üst kısmında bulunan **VM Oluştur** düğmesine tıklayınız.

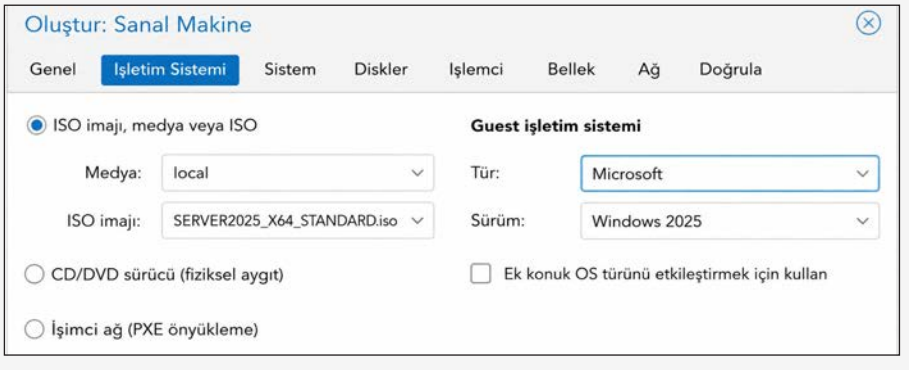
5. Adım: Açılan Genel sekmesinde Sunucu, VM ID ve Adı değerleri değiştirilebilir. Varsayılan değerlerle devam etmek için **İleri** düğmesine tıklayınız (Görsel 4.13).



Görsel 4.13: Genel sekmesi

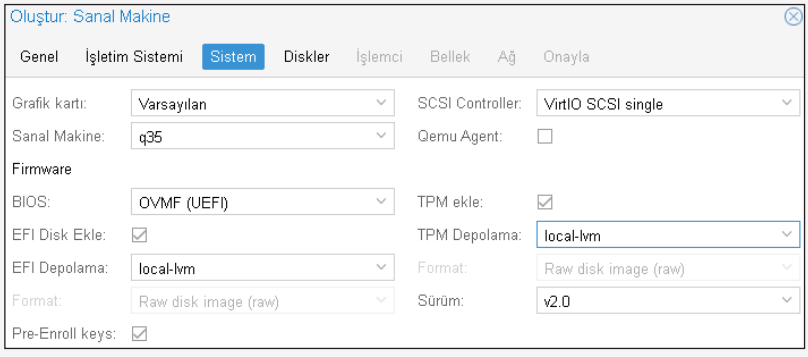
6. Adım: İşletim Sistemi sekmesinde **Disk İmajı (ISO):** kutusuna daha önce yüklenen ISO dosyasını seçiniz.

7. Adım: **Misafir işletim sistemi Tür ve Sürüm** kutusuna seçtiğiniz ISO dosyasına uygun bilgiler girilmiş ise **İleri** düğmesine tıklayınız (Görsel 4.14).



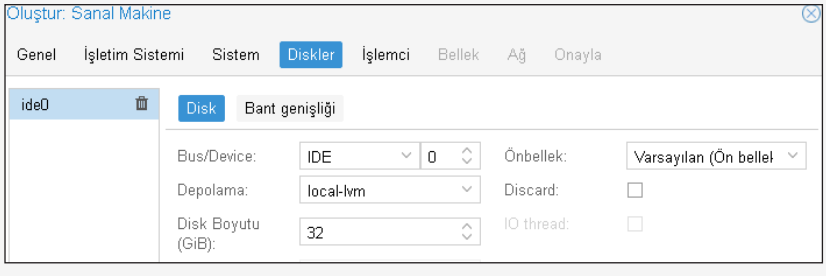
Görsel 4.14: İşletim Sistemi sekmesi

8. Adım: **Sistem** sekmesinde **Grafik kartı, Sanal Makine, BIOS ve SCSI Controller** kutularını kullanarak ayarlar yapılabilir. Varsayılan değerlerle devam etmek için **İleri** düğmesine tıklayınız (Görsel 4.15).



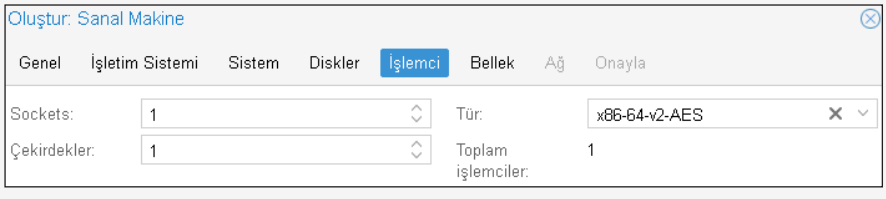
Görsel 4.15: Sistem sekmesi

9. Adım: **Diskler** sekmesinde sanal disk ayarları yapılabilir. Varsayılan değerlerle devam etmek için **İleri** düğmesine tıklayınız (Görsel 4.16).



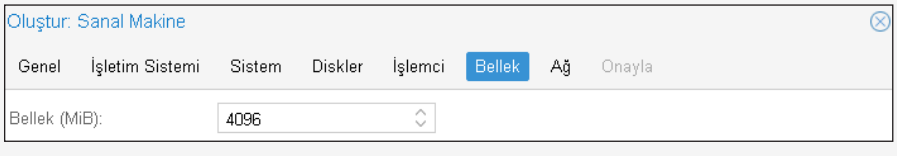
Görsel 4.16: Diskler sekmesi

10. Adım: İşlemci sekmesinde sanal makine için uygun işlemci türü, çekirdek sayısı gibi bilgiler değiştirilebilir. Varsayılan değerlerle devam etmek için **İleri** düğmesine tıklayınız (Görsel 4.17).



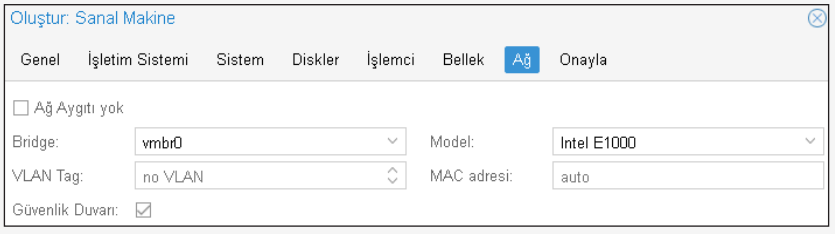
Görsel 4.17: İşlemci sekmesi

11. Adım: **Bellek** sekmesinde sanal makine için ayrılacak bellek (RAM) miktarı belirlenebilir. Değişiklik yapmadan devam etmek için **İleri** düğmesine tıklayınız (Görsel 4.18).



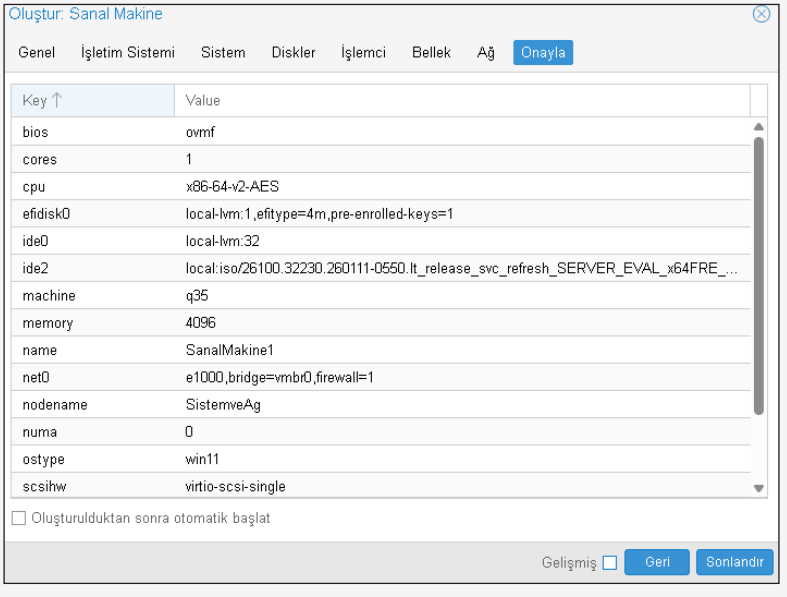
Görsel 4.18: Bellek sekmesi

12. Adım: **Ağ** sekmesinde sanal makine şebeke bağlantı ayarları düzenlenebilir. Varsayılan ayarlarla devam etmek için **İleri** düğmesine tıklayınız (Görsel 4.19).



Görsel 4.19: Ağ sekmesi

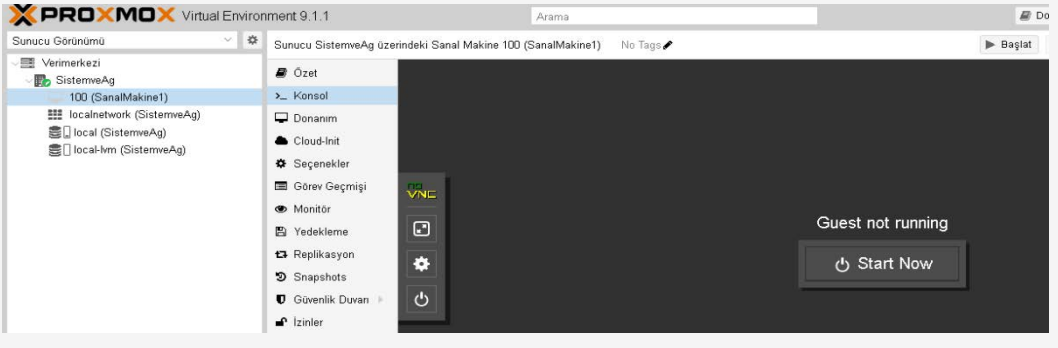
13. Adım: Tüm ayarlar düzenlendikten sonra **Sonlandır** düğmesine tıklayınız (Görsel 4.20).



Görsel 4.20: Onayla sekmesi

14. Adım: Oluşturulan sanal makineyi sol menüden seçiniz.

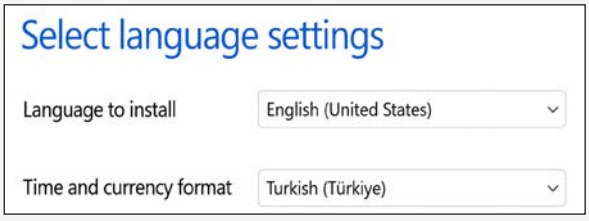
15. Adım: Üst seçeneklerde bulunan **Başlat** düğmesine tıklayınız (Görsel 4.21).



Görsel 4.21: Sanal makineyi başlatma

16. Adım: Konsol ekranında sunucu işletim sistemi kurulum ekranını görüntüleyiniz.

17. Adım: Yerelleştirme ayarlarını düzenledikten sonra **Next (İleri)** düğmesine tıklayınız (Görsel 4.22).

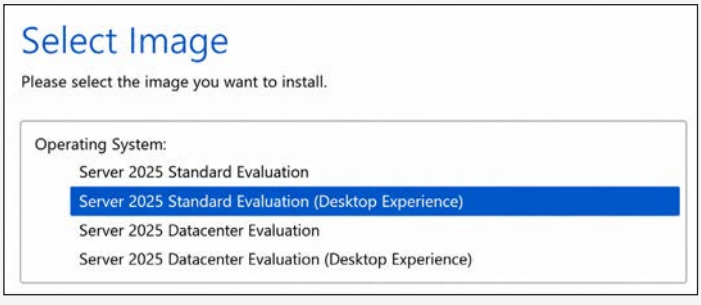


Görsel 4.22: Yerelleştirme ayarları

18. Adım: **Keyboard or input method (Klavye veya giriş metodu)** belirleyiniz.

19. Adım: **Install Server (Sunucu Kur)** seçiliyken **Next (İleri)** düğmesine tıklayınız.

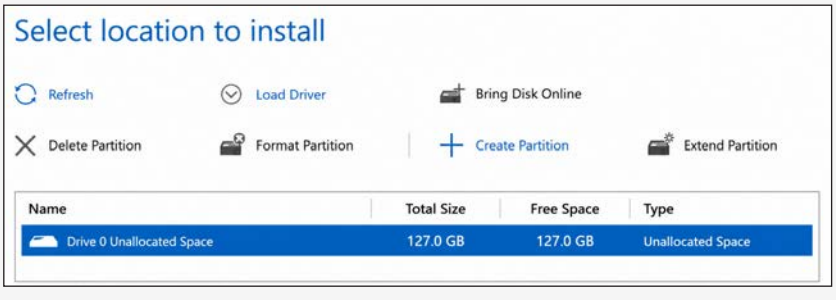
20. Adım: Kurulumu yapılacak sunucu işletim sistemi sürümünü seçiniz (Görsel 4.23).



Görsel 4.23: Sunucu işletim sistemi sürüm seçimi

21. Adım: Lisans sözleşmesi penceresini **Accept (Kabul)** düğmesine tıklayarak geçiniz.

22. Adım: Kurulumun gerçekleşeceği sanal diski seçerek **Next** düğmesine tıklayınız (Görsel 4.24).

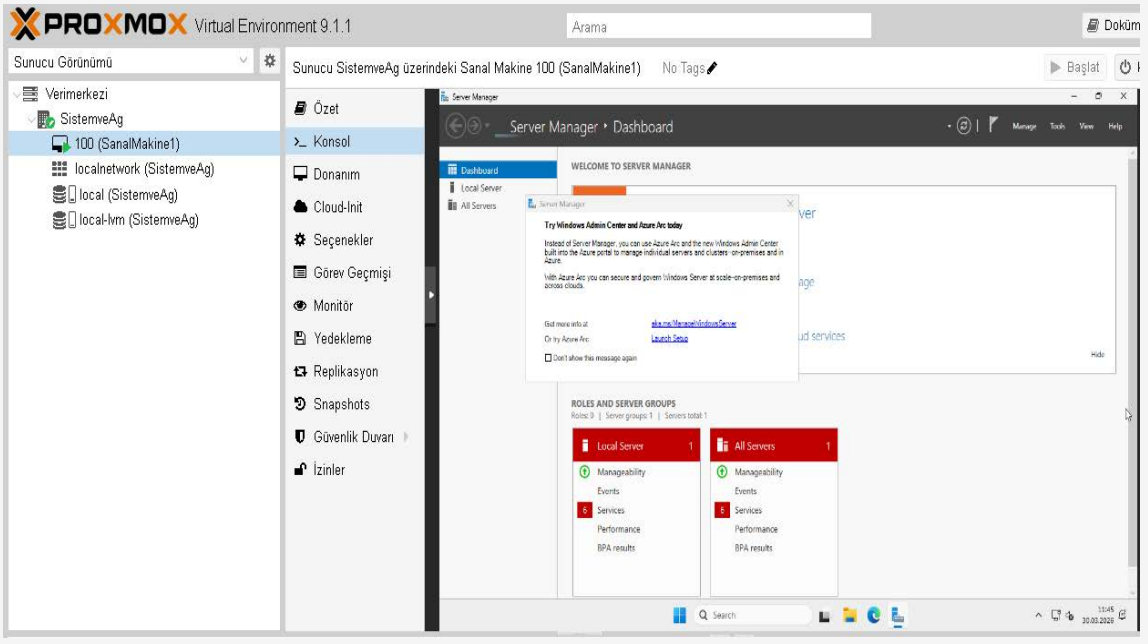


Görsel 4.24: Kurulum diski seçimi

23. Adım: **Ready to install (Kuruluma hazır)** penceresi görüntülenecektir. **Install** düğmesine tıklayınız.

24. Adım: Sunucu işletim sistemi kurulumu başlayacaktır. Kurulum tamamlandığında sistem otomatik olarak yeniden başlatılır. Sistem açıldığında **Administrator (Yönetici)** hesabı için parola belirleyiniz.

25. Adım: Sunucu işletim sisteminin kullanıcı arayüzünü inceleyiniz (Görsel 4.25).



Görsel 4.25: Sunucu işletim sistemi

3. ÖRNEK UYGULAMA

Tip 2 hipervizör yazılımıyla oluşturulmuş sanal makineye açık kaynak işletim sisteminin kurulumunu verilen adımlar doğrultusunda yapınız.

1. Adım: Resmî web sayfasından sanallaştırma yazılımını indirip kurulumu başlatınız.

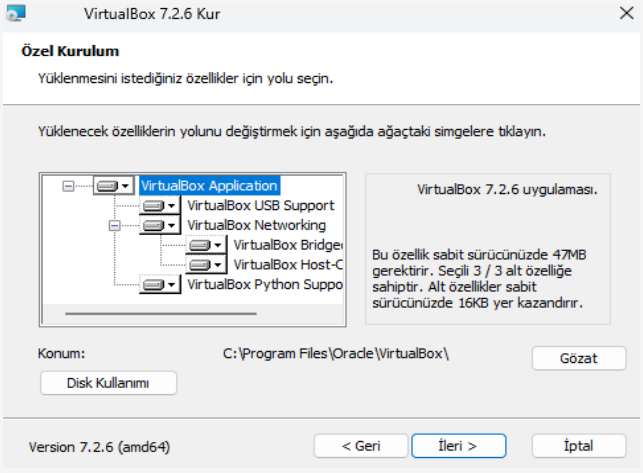
2. Adım: Karşılama penceresinde **İleri** düğmesine tıklayınız (Görsel 4.26).



Görsel 4.26: Tip 2 hipervizör yazılımı kurulum karşılama ekranı

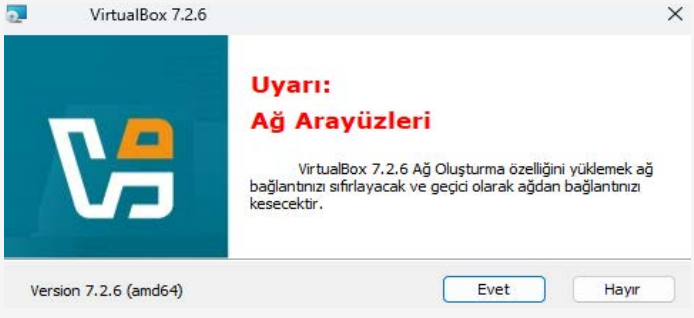
3. Adım: Lisans sözleşmesinin şartlarını kabul edip **İleri** düğmesine tıklayınız.

4. Adım: Yüklemek istenilen özellikler ve yolları belirlenip **İleri** düğmesine tıklayınız (Görsel 4.27).



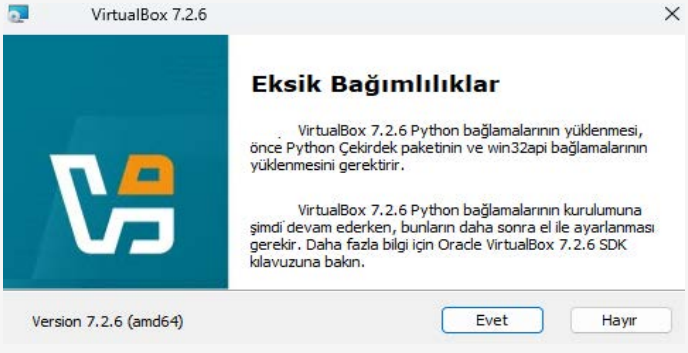
Görsel 4.27: Yüklenecek özellikler ve yollarını belirleme

5. Adım: Kurulum sırasında ağ bağlantısının kısa süreli kesileceğini belirten uyarı penceresinde **Evet** düğmesine tıklayınız (Görsel 4.28).



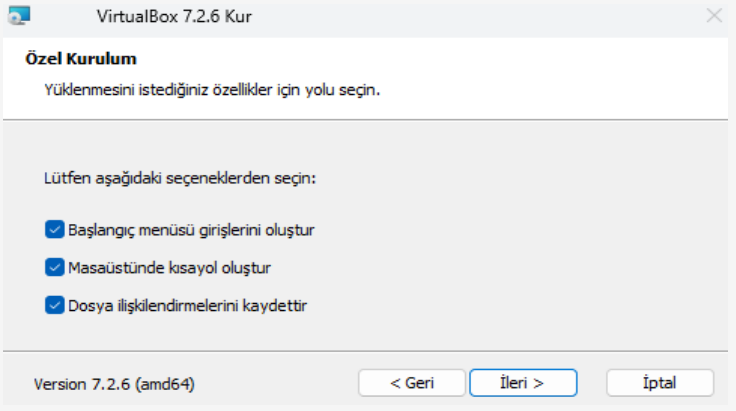
Görsel 4.28: Ağ bağlantısı kesilecek uyarısı

6. Adım: Sanallaştırma programı kurulumu sırasında Eksik Bağımlılıklar uyarısı gelebilir. Bu uyarı sanal makine oluşturma ve işletim sistemi yükleme işlemlerini engellemez. İleri düzey kullanımlarda bunların yüklü olması gerektiğini hatırlatır. **Evet** diyerek kuruluma devam ediniz (Görsel 4.29).



Görsel 4.29: Eksik Bağımlılıklar penceresi

7. Adım: Özel Kurulum penceresindeki seçenekler kullanılarak **Başlangıç menüsü girişlerini oluştur, Masaüstünde kısayol oluştur, Dosya ilişkilendirmelerini kaydettir** kutucuklarına onay işareti koyup, **İleri** düğmesine tıklayarak devam ediniz (Görsel 4.30).

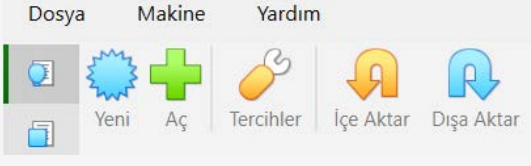


Görsel 4.30: Özel kurulum penceresi

8. Adım: **Yüklemek için hazır** penceresinde **Yükle** düğmesine tıklayarak kurulumu başlatınız.

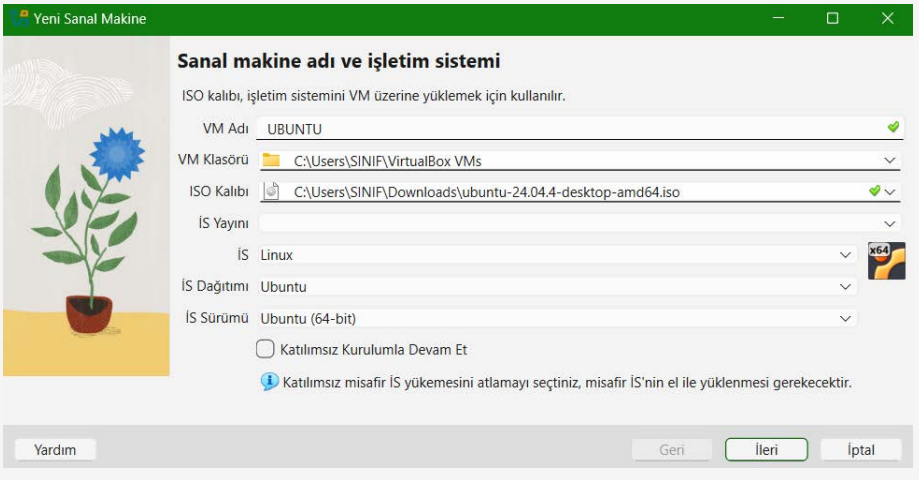
9. Adım: Kurulum tamamlandıktan sonra gelen pencerede **Bitir** düğmesine tıklayınız.

10. Adım: Sanallaştırma yazılımı çalıştıktan sonra yeni bir sanal makine oluşturmak için araçlar bölümünden **Yeni** simgesini tıklayınız (Görsel 4.31).



Görsel 4.31: Sanallaştırma yazılımı Yeni simgesi

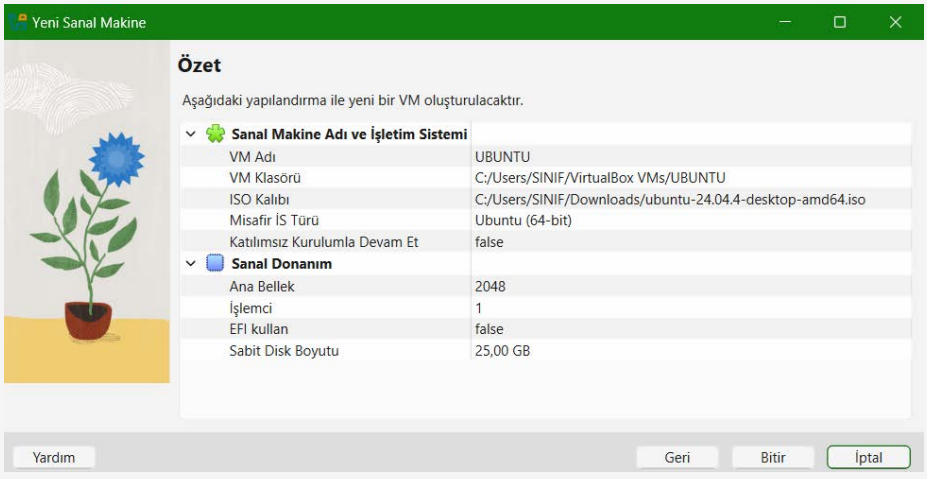
11. Adım: Sanal makineye işletim sistemi kurulumu için gerekli ISO dosyasının yolunu ve gerekli bilgileri girdikten sonra **İleri** düğmesine tıklayınız (Görsel 4.32).



Görsel 4.32: ISO dosyasının yolu ve kurulum ayarları

12. Adım: Sanal makine için bellek miktarı, işlemci sayısı ve depolama kapasitesini belirledikten sonra **İleri** düğmesine tıklayınız.

13. Adım: Sanal makine Özet penceresini inceledikten sonra **Bitir** düğmesini tıklayınız (Görsel 4.33).



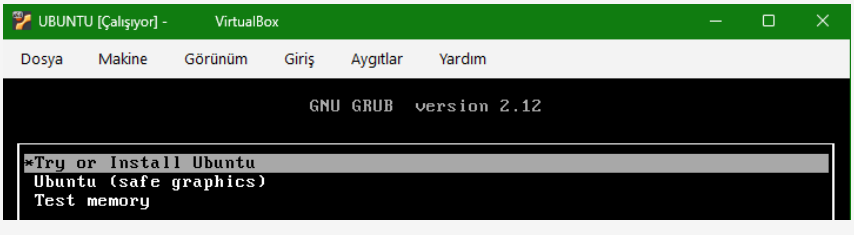
Görsel 4.33: Özet penceresi

14. Adım: Sanal makineyi çalıştırıp kurulumu başlatmak için iki yöntem kullanılabilir. Birincisi UBUNTU sanal makinesine çift tıklanır. İkincisi **Başlat** simgesine tıklanır (Görsel 4.34). Bu yöntemlerden birini seçiniz.



Görsel 4.34: Başlat simgesi

15. Adım: **Try or Install Ubuntu** seçip **Enter** tuşuna basınız (Görsel 4.35).



Görsel 4.35: Kurulum başlangıç ekranı

16. Adım: Dili Türkçe seçip **Sonraki** düğmesini tıklayınız.

17. Adım: Erişim özelliklerinin seçildiği pencerede **Sonraki** düğmesine tıklayınız.

18. Adım: Klavye düzenini Türkçe seçip **Sonraki** düğmesine tıklayınız.

19. Adım: İnternet bağlantı ayarlarını yapıp **Sonraki** düğmesine tıklayınız.

20. Adım: Şimdi güncelle penceresini **Atla** düğmesine tıklayarak geçiniz.

21. Adım: Ubuntu Kur seçeneğini işaretleyerek **Sonraki** düğmesine tıklayınız.

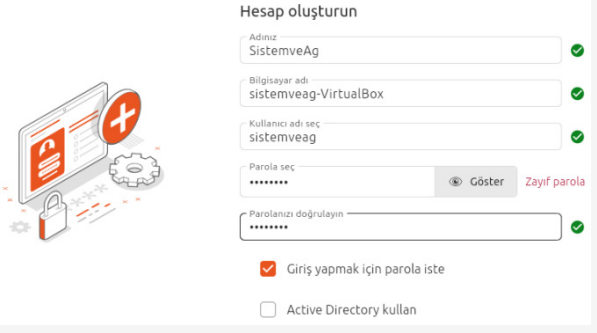
22. Adım: Kurulumun etkileşimli olması için **Interactive installation** seçeneğini işaretleyerek **Sonraki** düğmesine tıklayınız.

23. Adım: Başlangıç uygulamaları için **Tam kurulum** seçeneğini işaretleyerek **Sonraki** düğmesine tıklayınız.

24. Adım: Grafik, kablosuz cihazlar ve ek ortam biçimleri için üçüncü taraf yazılımları yükleme penceresinde **Sonraki** düğmesine tıklayınız.

25. Adım: **Diski sil ve Ubuntu kur** seçeneği işaretlenerek **Sonraki** düğmesine tıklayınız.

26. Adım: Sanal makine için kullanıcı adı, makine adı ve parola bilgilerini girip **Sonraki** düğmesine tıklayınız (Görsel 4.36).

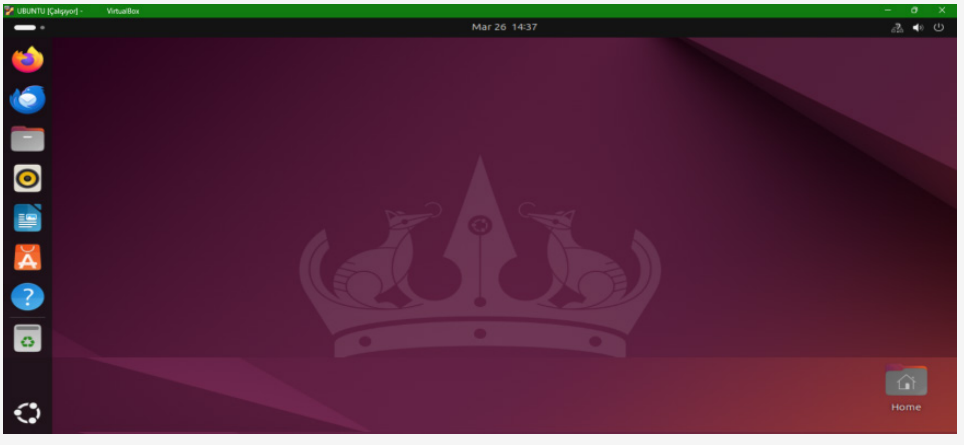


Görsel 4.36: Hesap oluşturma penceresi

27. Adım: Zaman dilimi için bulunduğunuz bölgeyi seçip **Sonraki** düğmesine tıklayınız.

28. Adım: Şimdi yeniden başlat seçeneğine tıklayarak kurulumun tamamlanması için sanal makineyi yeniden başlatınız.

29. Adım: İşletim sistemi masaüstünü inceleyiniz (Görsel 4.37).



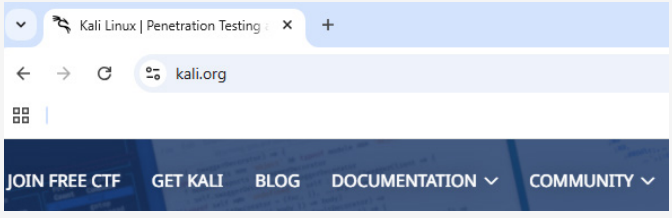
Görsel 4.37: İşletim sistemi masaüstü görüntüsü

4. ÖRNEK UYGULAMA

Tip 2 hipervizör yazılımını kullanarak hazır bir sanal makine imajını yükleme işlemini verilen adımlar doğrultusunda gerçekleştiriniz.

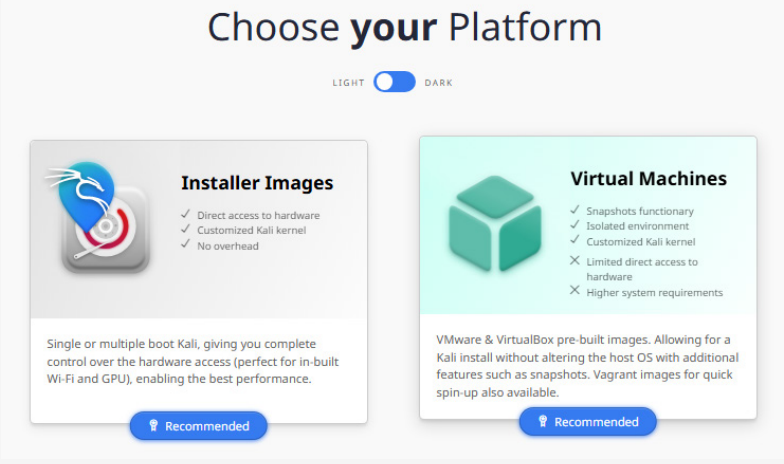
1. Adım: Yüklenecek işletim sisteminin resmî web sayfasına gidiniz.

2. Adım: GET KALI (Kali işletim sistemini al) bağlantısına tıklayınız (Görsel 4.38).



Görsel 4.38: İşletim sistemi indirme bağlantısı

3. Adım: Virtual Machines (Sanal Makineler) seçeneğini tıklayınız (Görsel 4.39).



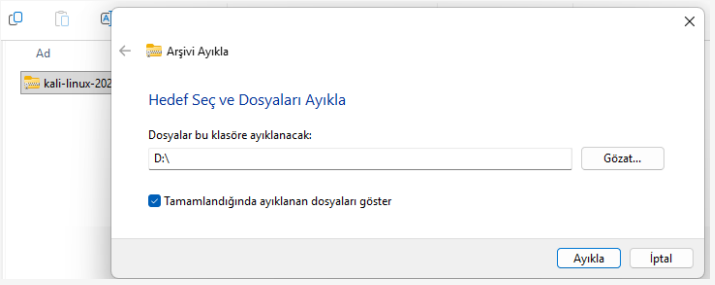
Görsel 4.39: Farklı platformlar için işletim sistemi imajlar penceresi

4. Adım: Sanal makine yazılımınıza uygun hazır işletim sistemi imaj dosyasını indiriniz (Görsel 4.40).



Görsel 4.40: Sanal makine yazılımına uygun imaj seçimi

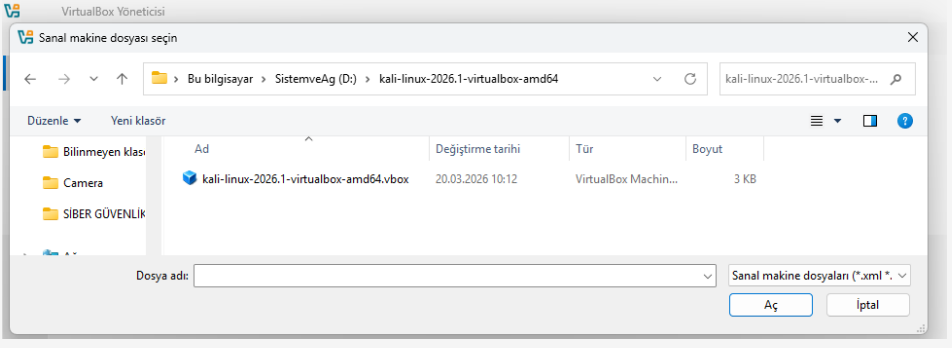
5. Adım: Sıkıştırılmış olarak indirilen imaj dosyasını yerel sürücüde uygun bir yere açınız (Görsel 4.41).



Görsel 4.41: Sıkıştırılmış imaj dosyasının açılması

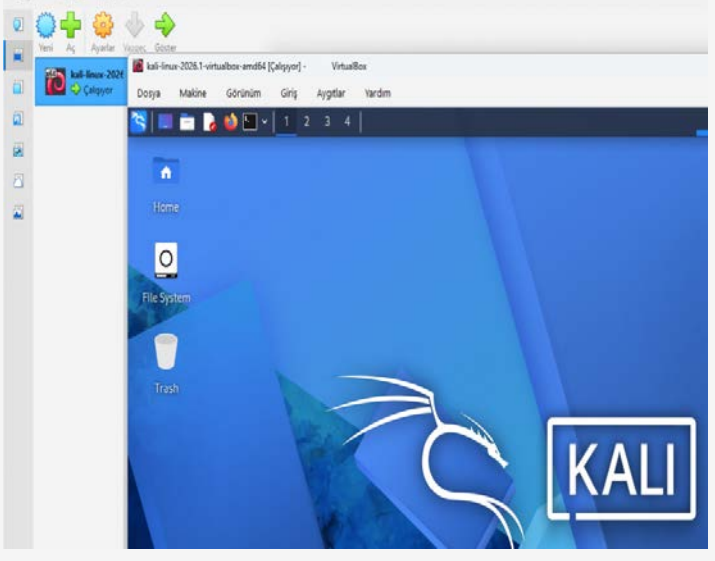
6. Adım: Sanal makine yazılımını çalıştırınız.

7. Adım: Sanal makine yazılımında **Aç** seçeneğinden yerel sürücüye açılan dosyayı seçiniz (Görsel 4.42).



Görsel 4.42: Hazır sanal makine ekleme

8. Adım: Sanal makine yazılımında eklenen makineyi çift tıklayarak çalıştırınız (Görsel 4.43).



Görsel 4.43: Çalıştırılan hazır sanal makine

2. ETKİNLİK

Etkinlik Adı	Tip 2 Hipervizör Yazılımında Mint İşletim Sistemi Kurulumu ve Afiş Hazırlama
Süre	40-80 dakika
Amaç	Mint işletim sistemini doğru adımlarla kurmak, temel sistem ayarlarını yapmak, sürücü ve ağ bağlantılarını kontrol ederek sistemi kullanıma hazır hâle getirmek
Yönerge	Öğretmeniniz işletim sistemi kurulum sürecini adım adım gösterdikten sonra grubunuzla birlikte aşağıdaki adımları izleyerek Mint işletim sistemini kurunuz. Her adımda iş bölümü yapınız ve tüm grup üyelerinin sürece aktif katılımını sağlayınız. Her adım tamamlandığında **Kontrol** sütununa (✓) işaretleyiniz.

⚠ **İş Sağlığı ve Güvenliği Kuralları**

Elektrik Güvenliği

- Elektrik prizleri, güç kabloları ve uzatma kabloları güvenli şekilde kullanınız; hasarlı ekipman kullanmayınız.
- Kurulum sırasında elektrik kesintisi riskine karşı mümkünse priz koruyucu veya UPS kullanınız.
- USB bellek takma-çıkarma işlemlerini dikkatli yapınız.

Donanım Güvenliği

- USB kurulum belleğini zorlamadan doğru yönde takınız.
- Bilgisayar açılırken BIOS/UEFI ayarlarında yanlış işlem yapmamaya dikkat ediniz.
- Kurulum sırasında depolama birimini yanlışlıkla biçimlendirmemek için disk seçimini dikkatli yapınız.

Çalışma Alanı Düzeni

- Çalışma alanını düzenli tutunuz.
- Kablolar üzerinde yürümeyiniz, takılma ve düşme riskine karşı dikkatli olunuz.
- USB bellek, güç kabloları ve ağ kablolarını gelişigüzel bırakmayınız.
- Grup üyeleri arasında görev paylaşımı yapınız.

Kurulum Adımları

Adım	Yapılacak İşlem	Kontrol
1	İşletim sistemi ISO dosyasını indiriniz.	☐ Tamamlandı
2	Sanal makine yazılımında ISO dosyasını kurulum için seçiniz.	☐ Tamamlandı
3	Sanal makineyi çalıştırınız.	☐ Tamamlandı
4	İşletim sistemi kurulum işlemlerini yapınız.	☐ Tamamlandı
5	Kurulum aşamalarını gösteren afiş hazırlayınız.	☐ Tamamlandı

Değerlendirme

Çalışmanız öğretmeniniz tarafından kontrol listesine göre değerlendirilecektir. Çalışmanızı yaparken buradaki ölçütleri dikkate alınız. Kontrol listesi formuna ulaşmak için karekodu okutunuz. Dijital yayınlarda karekodun üstüne tıklayarak içeriğe ulaşabilirsiniz.

Çalışmanızı tamamladıktan sonra grup değerlendirme formunu doldurarak grup üyelerinin çalışmaya katkı düzeylerini değerlendiriniz. Grup değerlendirme formuna ulaşmak için karekodu okutunuz. Dijital yayınlarda karekodun üstüne tıklayarak içeriğe ulaşabilirsiniz.

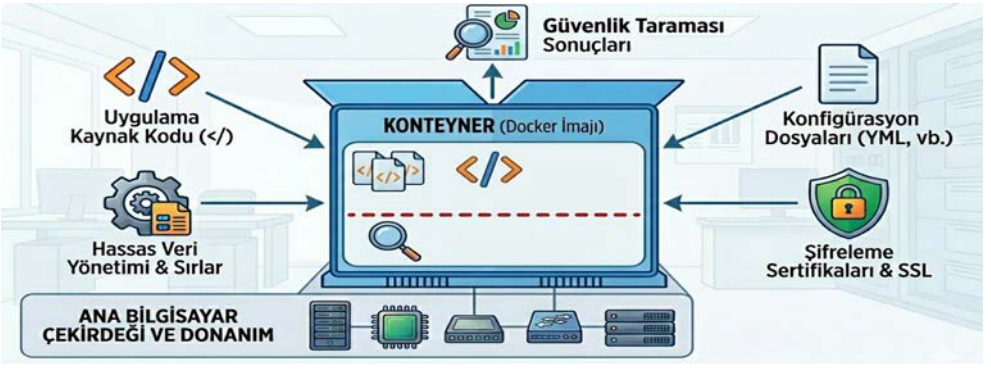
Çalışmanızın öğrenme sürecinize katkısını değerlendirmek için öz değerlendirme formunu doldurunuz. Formu tamamladıktan sonra öğretmeninizle paylaşınız veya EBA Portfolyo'ya yükleyiniz. Öz değerlendirme formuna ulaşmak için karekodu okutunuz. Dijital yayınlarda karekodun üstüne tıklayarak içeriğe ulaşabilirsiniz.

4.1.2. Konteyner Mimarisi

Konteyner mimarisi, uygulamaların ihtiyaç duyduğu tüm bileşenlerle birlikte yalıtılmış bir ortamda çalıştırılmasını sağlayan bir sanallaştırma yöntemidir. Her uygulama, bu mimaride şu şekilde oluşturulur:

- Kendi bağımlılıklarıyla birlikte paketlenir.
- Aynı işletim sisteminin çekirdeğini paylaşır.
- Birbirinden yalıtılmış şekilde çalışır.

Aynı apartmandaki daireler düşünüldüğünde bunlar birbirinden yalıtılmış ve bağımsızdır ancak aynı binada bulunur. Konteyner mimarisinde de her uygulama birbirinden bağımsız ve yalıtılmış olmasına rağmen aynı işletim sistemini kullanır. Uygulamanın çalışması için gerekli tüm kütüphaneler, bağımlılıklar ve ayarlar konteyner içinde saklanır (Görsel 4.44). Saklanan bu paket sayesinde farklı sistemler ve platformlar arasında oluşabilecek uyum sorunları ortadan kaldırılır. Ayrıca her konteyner birbirinden bağımsız çalıştığı için birinin güvenlik sorunları diğerini etkilemez.



Görsel 4.44: Tek bir konteyner yapısı

Her ne kadar konteyner ve sanal makinelerin çalışma biçimi birbirine benzese de her sanal makine için ayrı bir işletim sistemine ihtiyaç duyulurken konteyner için tek işletim sistemi yeterlidir. Dolayısıyla sanal makineler çok daha fazla donanım kaynağına ihtiyaç duyar. Konteynerler ise tek bir işletim sistemi kullandıkları için daha verimli donanım kaynağı kullanır.

Sanal makineler donanım seviyesinde yalıtım sağlarken konteynerler işletim sistemi düzeyinde yalıtım sağlar (Tablo 4.1).

Tablo 4.1: Sanal Makine ve Konteyner Karşılaştırması

Ölçütler	Sanal Makine (VM)	Konteyner
Başlatma Süresi	Uzun (dakikalar)	Çok kısa (saniyeler)
Kaynak Kullanımı	Yüksek	Düşük (ortak çekirdek)
Disk Kullanımı	Fazla	Daha az
Performans	Orta	Yüksek
İzolasyon	Güçlü (donanım seviyesinde)	Orta (İşletim sistemi seviyesinde)
Taşınabilirlik	Sınırlı	Çok yüksek
Ölçeklenebilirlik	Zor	Kolay ve hızlı
Kurulum Süresi	Uzun	Kısa
Güncelleme	Daha karmaşık	Daha kolay
Yoğunluk (Density)	Aynı donanımda daha az sanal makine	Aynı donanımda daha fazla konteyner

Konteyner mimarisinin yaygınlaşmasıyla birlikte uygulamaların yönetimi için Docker ve Kubernetes olmak üzere iki önemli teknoloji ortaya çıkmıştır.

- Docker, konteyner oluşturma ve çalıştırma için kullanılır.
- Kubernetes, konteynerleri yönetme ve ölçeklendirme için kullanılır.

Konteyner mimarisindeki bu teknolojiler basitleştirerek şu şekilde örneklendirilebilir: Docker, restoranda yemek yapma eylemidir; Kubernetes, yemek yapılan bu restoranı yönetmektir.

SIRA SİZDE

Aşağıda bir yazılım şirketinin, çalıştıracağı yazılımlar için hangi teknolojinin kullanılacağı kararını konu alan bir senaryo verilmiştir.

Senaryo

Bir yazılım şirketi, farklı özelliklere sahip dört yazılım çalıştırmak istemektedir. Teknik ekip, her yazılım için en uygun çalışma ortamının konteyner mi yoksa sanal makine mi olacağına karar verecektir.

1. Yazılım

- Küçük ölçekli bir web form uygulamasıdır.
- Hızlı başlatılması gerekir.
- Güncellemeler sık yapılacaktır.
- Aynı sunucuda birçok benzer uygulama çalışacaktır.

2. Yazılım

- Banka işlemleri benzeri yüksek güvenlik gerektirir.
- İzolasyon çok önemlidir.
- Sistem kararlılığı önceliklidir.
- Donanım kaynakları yeterlidir.

3. Yazılım

- Eski teknoloji ile yazılmış büyük bir uygulamadır.
- İşletim sistemi bağımlılığı yüksektir.
- Yeniden yazılması mümkün değildir.
- Kurulum süreci karmaşıktır.

4. Yazılım

- Çok sayıda küçük servislerden oluşur.
- Sürekli güncellenir.
- Hızlı ölçeklenebilirlik gerekir.
- Hafif ve taşınabilir yapı tercih edilir.

Aşağıdaki soruları senaryo metnine dayanarak yanıtlayınız. Kararlarınızı teknik gerekçelerle destekleyiniz.

Sorular

1. Birinci yazılım için hangi mimari daha uygundur? Gerekçesini yazınız.

☐ Konteyner ☐ Sanal Makine	**Gerekçeniz:**

2. İkinci yazılım için hangi mimari daha uygundur? Gerekçesini yazınız.

☐ Konteyner ☐ Sanal Makine	**Gerekçeniz:**

3. Üçüncü yazılım için hangi mimari daha uygundur? Gerekçesini yazınız.

☐ Konteyner ☐ Sanal Makine	**Gerekçeniz:**

4. Dördüncü yazılım için hangi mimari daha uygundur? Gerekçesini yazınız.

☐ Konteyner ☐ Sanal Makine	**Gerekçeniz:** _____ _____

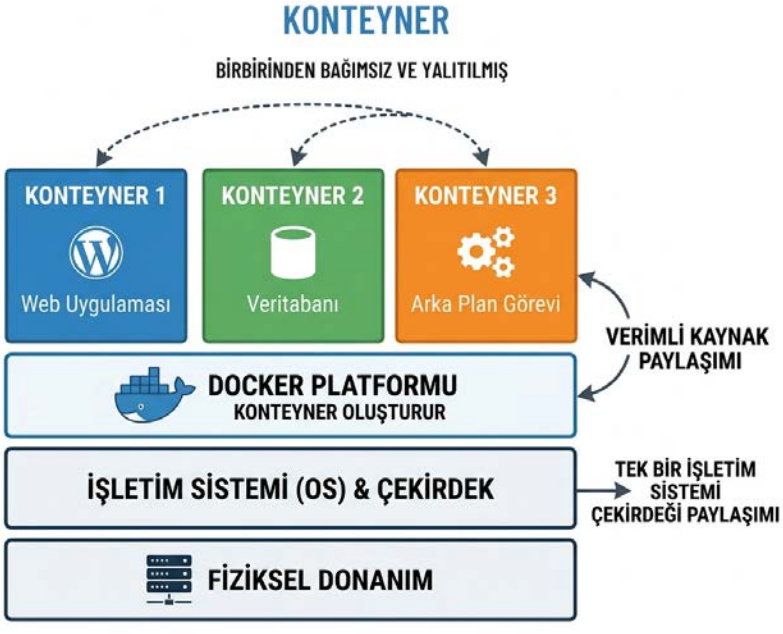
Değerlendirme

Çalıştırılacak bir yazılımın hangi özelliklerine bakarak sanal makine veya konteyner teknolojisini seçersiniz? Dört tanesini yazınız?

1	
2	
3	
4	

4.1.2.1. Docker

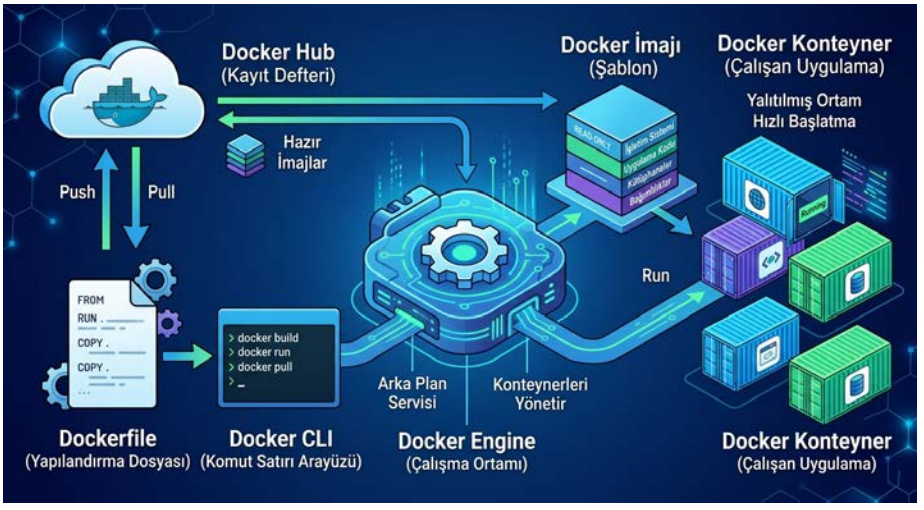
Tek bir işletim sistemi kaynaklarını verimli bir biçimde paylaştırarak birbirinden bağımsız ve yalıtılmış olarak uygulamaların çalıştırılmasını sağlayan açık kaynak yazılım platformlarından biri de **Docker** programıdır. İşletim sisteminin çekirdeğinde çalışır ve konteyner oluşturulmasını sağlar. Yaygın olarak kullanılan bir teknolojidir (Görsel 4.45).



Görsel 4.45: Konteyner yapısı

4.1.2.2. Docker Bileşenleri

Docker'ın temel bileşenlerini altıya ayırmak mümkündür. Bunlar; Docker Engine (Çalıştırma Ortamı), Docker Image (İmaj), Docker Container (Konteyner), Dockerfile, Docker Hub (Registry), Docker CLI [Command Line Interface (Komut Satırı Arayüzü)] olarak sıralanır (Görsel 4.46).



Görsel 4.46: Konteyner bileşenleri

Docker Engine: Docker'ın çalışmasını sağlayan ana bileşendir. Konteynerleri oluşturur ve çalıştırır. Komutların işlenmesini sağlar. Arka planda çalışan servistir.

Docker Image: Uygulamanın çalışması için gerekli tüm dosyaları içeren bir tür şablondur. İçeriğinde işletim sistemi dosyaları, uygulama kodları, kütüphaneler ve bağımlılıklar bulunur. Konteynerin oluşturulmasını sağlar.

Docker Container: Docker imajından oluşturulan çalışan uygulamadır. Yalıtılmış ortamda bağımsız olarak uygulamayı çalıştırır, donanım kaynaklarını sanal makineye göre yoğun kullanmaz ve hızlı açılır.

Dockerfile: Docker imajı oluşturmak için kullanılan komut dosyasıdır. Adım adım yapılandırmayı içerir ve otomatik olarak imaj oluşturmayı sağlar. Bu dosyada yaygın olarak kullanılan komutlar vardır (Tablo 4.2).

Tablo 4.2: Yaygın Olarak Kullanılan Dockerfile Komutları

Komut	Açıklama	Örnek
FROM	Kullanılacak temel imajı belirtir.	FROM ubuntu
WORKDIR	Çalışma klasörünü belirler.	WORKDIR /app
COPY	Dosyaları konteynere kopyalar.	COPY app.py .
ADD	Dosya veya klasör ekler.	ADD dosya.txt /app
RUN	İmaj oluşturulurken komut çalıştırır.	RUN apt update
CMD	Konteyner çalışınca varsayılan komutu çalıştırır.	CMD ["python","app.py"]
ENTRYPOINT	Konteynerin ana çalıştırma komutunu belirler.	ENTRYPOINT ["python"]
EXPOSE	Kullanılacak portu belirtir.	EXPOSE 80
ENV	Ortam değişkeni tanımlar.	ENV PORT=80
LABEL	İmaja açıklama bilgisi ekler.	LABEL version="1.0"

Docker Hub: Docker imajlarının saklandığı ve paylaşıldığı platformdur. Hazır imajlar burada bulunur. Kullanıcılar kendi imajlarını buraya yükleyebilir. Buradaki imajları kendi konteynerlerine çekebilir.

Docker CLI: Komut satırı arayüzüdür. Kullanıcının Docker ile iletişim kurmasını ve komutlarını çalıştırmasını sağlayan uç birimdir.

SIRA SİZDE

Senaryo başlığında belirtilen kullanım senaryolarını okuyunuz. O senaryo için en uygun bileşeni aşağıdan seçerek, önündeki harfi **Yanıt** sütununa yazıp doğru senaryo ile eşleştiriniz.

A: Docker Volume	**B:** Docker Container	**C:** Docker CLI	**Ç:** Docker Hub	**D:** Docker Engine

Senaryo	Yanıt
1. Bir şirket, bilgisayarlarındaki uygulamaların birbirinden yalıtılmış şekilde çalışmasını ve çalıştırılabilir hâle gelmesini istiyor.	
2. Bir geliştirici, web uygulamasında konteyner silinse bile verilerin kalıcı olarak saklanmasını istiyor.	
3. Bir geliştirici, hazır Docker imajlarını indirerek kendi projesine hızlıca entegre etmek istiyor.	
4. Bir sistem yöneticisi, komut satırı kullanarak Docker ile iletişim sağlamak istiyor.	

4.1.2.3. Docker Çalışma Ortamı

Kullanıcılar Docker'ı iki şekilde kullanabilir. Çevrimiçi platform üzerinden veya masaüstü uygulaması kurularak çalışma ortamı üzerinden kullanılabilir. Konteyner oluşturmak için imajlara ihtiyaç duyulacağı için öncelikle Docker Hub'da hesap oluşturulur. İstenirse bu imajlar kişisel cihaza indirilip yerel olarak da kullanılabilir.

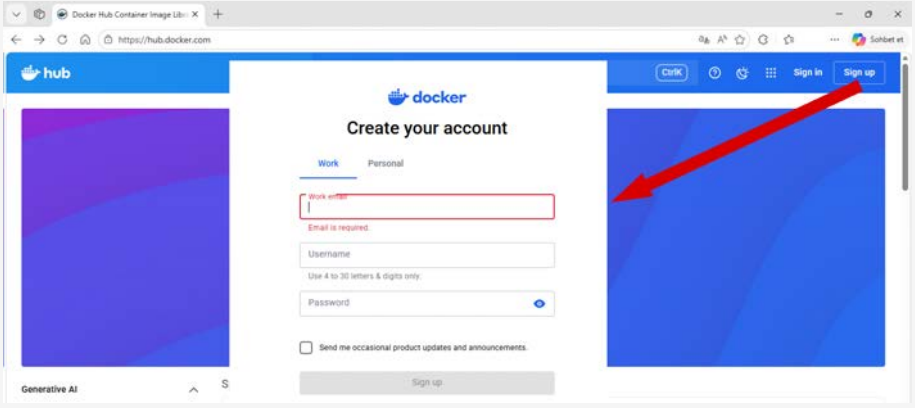
5. ÖRNEK UYGULAMA

Docker Hub'da imaj indirip konteyner oluşturabilmek veya oluşturulan imajları yüklemek için hesap açma işlemlerini aşağıdaki adımları takip ederek gerçekleştiriniz.

1. Adım: Hesap açılacak Docker Hub resmî web sayfasına gidiniz.

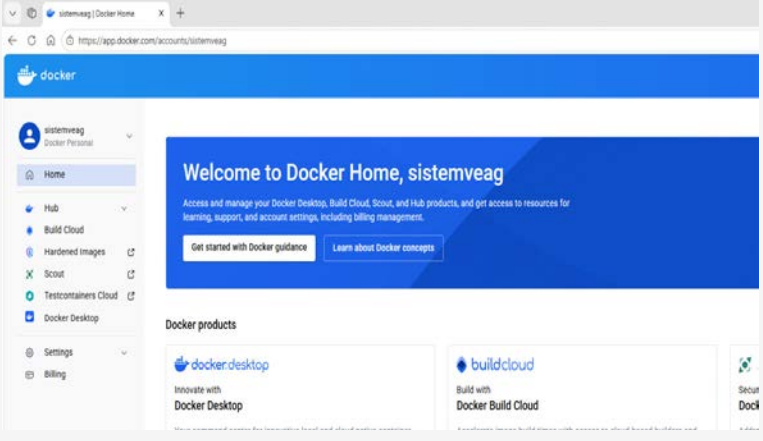
2. Adım: Web sayfasında Sign up (Kaydolmak) düğmesine tıklayınız.

3. Adım: İstenen bilgileri giriniz (Görsel 4.47).



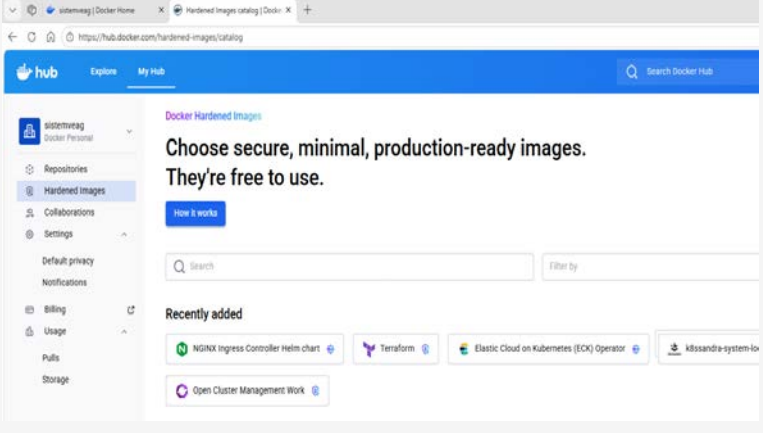
Görsel 4.47: Hesap oluşturma

4. Adım: E-postanızı onaylamak için e-postanıza gelen doğrulama koduyla hesaba giriş yapınız (Görsel 4.48).



Görsel 4.48: Karşılama penceresi

5. Adım: Sol menüden **Hardened Images** (Güçlendirilmiş, güvenlik zaafları azaltılmış ve gereksiz bileşenlerden arındırılmış imajlar) seçeneğini tıklayarak imajları inceleyiniz (Görsel 4.49).



Görsel 4.49: İmajlar

6. ÖRNEK UYGULAMA

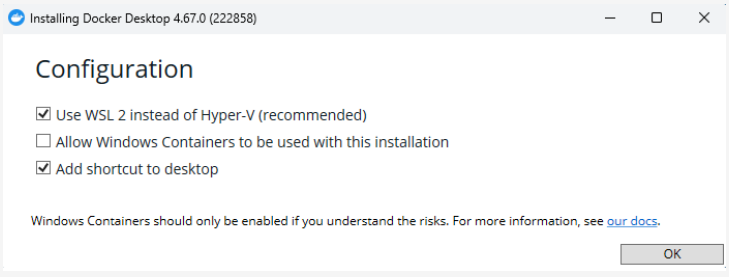
Docker Desktop kurulumunu aşağıdaki adımları takip ederek gerçekleştiriniz.

1. Adım: Docker'ın resmî web sayfasına gidiniz.

2. Adım: İşletim sisteminize uygun kurulum dosyasını indiriniz.

3. Adım: İndirilen kurulum dosyasına çift tıklayınız.

4. Adım: Kurulum sihirbazında Görsel 4.50'deki iki seçeneği işaretleyiniz.



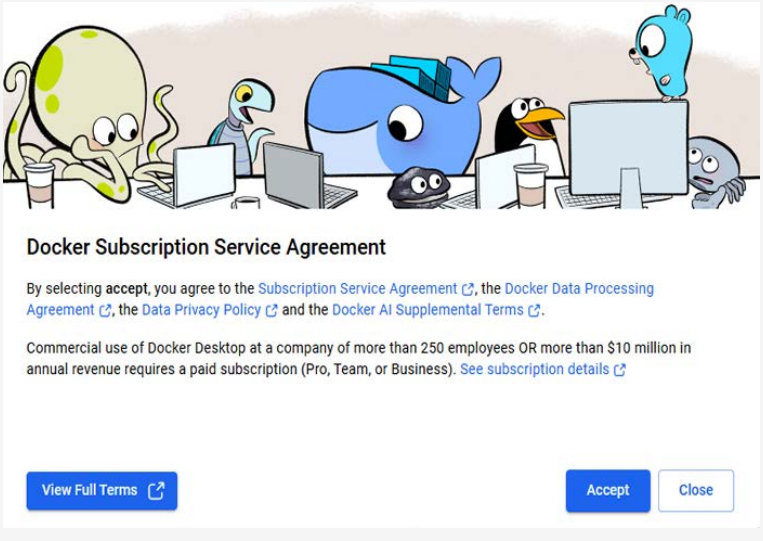
Görsel 4.50: Kurulum sihirbazı

5. Adım: OK (Tamam) düğmesine tıklayarak kurulumu başlatınız.

6. Adım: Kurulum bittiğinde Close and restart (Kapat ve yeniden başlat) düğmesine tıklayınız.

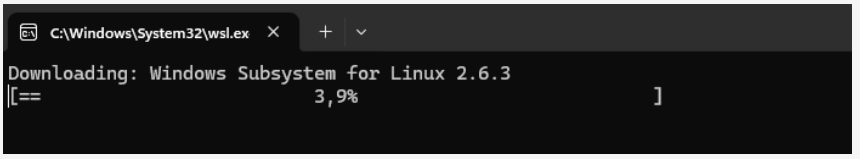
7. Adım: Bilgisayar tekrar açıldığında Docker Desktop uygulamasını başlatınız.

8. Adım: Docker Subscription Service Agreement (Hizmet Sözleşmesi) ekranı gelirse Accept düğmesine basınız (Görsel 4.51).



Görsel 4.51: Hizmet sözleşmesi

9. Adım: WSL 2 eksikse Docker size bir uyarı vererek gerekli güncellemeyi yapmanız için bir link sunacaktır. Bu durumda WSL 2 Linux çekirdeği güncelleme paketini indirip kurunuz (Görsel 4.52).



Görsel 4.52: Güncelleme paketini yükleme

10. Adım: Docker Desktop penceresini inceleyiniz.

BİLGİ KUTUSU : Komut İstemi Üzerinden Kontrol

Komut istemi veya PowerShell açarak şu komutu yazınız:

docker - -version

Ekranda Docker version 2x.xx.x gibi bir çıktı görüyorsanız kurulum başarılıdır.

4.1.2.4. Temel Komutlar

Docker komutları, işletim sisteminin komut arayüzünden (CLI) veya Docker Desktop uygulamasının görsel arayüzünden çalıştırılabilir. Bu komutlar kullanılarak konteyner oluşturulur, başlatılır, durdurulur, silinir. Kullanıcı tarafından komut arayüzünde yazılan komutun çalıştırılması için Docker Daemona (dockerd) aktarılır. Komutlar çalıştırıldıktan sonra sonuç tekrardan kullanıcı ekranına gönderilir. Docker komutları, genel komutlar ve konteyner komutları olmak üzere iki grupta incelenir. Genel komutlar; konteyner çalıştırma, durdurma, imaj yükleme, imaj görüntüleme gibi konteyner genel işlemlerini yönetmek için kullanılır. Konteyner komutları ise belirli bir konteyner üzerinde işlem yapılmasını sağlamak için kullanılır. Bu komutlar genellikle konteyner tanımlayıcı numarası (container_id) ile birlikte kullanılır (Tablo 4.3).

BİLGİ KUTUSU : Komut seçeneği (flag) veya parametre

Komutun çalışma şeklini değiştiren veya genişleten ifadelerdir. Genellikle komutun ardından "-" (kısa çizgi) veya "- -" (iki kısa çizgi) ile kullanılırlar.

Tablo 4.3: Docker Genel Komutları

Komut	Açıklama	Parametre
docker ps	Çalışan konteynerleri listeler.	-a: Çalışan tüm konteynerleri gösterir. -q: Sadece konteyner ID'lerini gösterir. -n: En son oluşturulan n sayıdaki konteynerleri gösterir.

Komut	Açıklama	Parametre
docker run	Yeni bir konteyner oluş-turur ve çalıştırır.	-d: Bir konteynerin arka planda çalışmasını sağlar. -p: Konteynere ait bir portu dış erişime açar. —name: Konteynere isim vermek için kullanılır. -v: Bir konteynere depolama için volume tanımlaması yapar.
docker pull	Docker Hub'dan imaj çeker.	-
docker images	Yüklenmiş imajları gösterir.	-
docker stop	Çalışan bir konteyneri durdurur.	-t: Konteyneri durdurmadan önce sinyal gönderir.
docker start	Durdurulmuş bir konteyneri başlatır.	-a: Konteynerin çıktılarını terminale gönderir. -i: Konteyneri etkileşimli modda başlatır.
docker restart	Konteyneri yeniden başlatır.	-t: Konteyneri yeniden başlatmadan önce sinyal gönderir.
docker rm	Durdurulmuş konteyneri siler.	-f: Bir konteyneri silmeye zorlar. -v: Bir konteynere ait veri tabanı kayıtlarını da siler.

Docker'da konteyner ile ilgili işlemler için örnek komutlar şunlardır:

- docker run nginx
  nginx imajını kontrol eder yoksa indirir. Konteyner oluşturur ve çalıştırır.
- docker run -d nginx
  -d komut seçeneği ile konteynerin arka planda çalışmasını sağlar.
- docker run -d -p 8080:80 nginx
  nginx web sunucusunu konteynerde çalıştırır ve 8080 portuna yönlendirir.
- docker run -d -p 8081:80 httpd
  Apache web sunucusunu konteynerde çalıştırır ve 8081 portuna yönlendirir.
- docker run -d -p 8082:3306 mysql
  MySQL very tabanı sunucusunu konteynerde çalıştırır ve 8082 portuna yönlendirir.
- docker ps
  Sadece çalışan konteynerleri listeler.
- docker ps -a
  Çalışan veya durdurulmuş tüm konteynerleri listeler.

Konteyner komutlar; belirli bir konteyner üzerinde işlem yapılmasını sağlamak için kullanılır. Bu komutlar genellikle konteyner tanımlayıcı numarası (container_id) ile birlikte kullanılır (Tablo 4.4).

Tablo 4.4: Docker Konteyner Komutları

Komut	Açıklama	Örnek Kullanım
docker container ls	Çalışan konteynerleri listeler.	docker container ls
docker container start	Bir konteyneri başlatır.	docker container start <container_id>
docker container stop	Bir konteyneri durdurur.	docker container stop <container_id>
docker container pause	Bir konteyneri duraklatır.	docker container pause <container_id>
docker container unpause	Duraklatılmış bir konteyneri tekrar çalıştırır.	docker container unpause <container_id>
docker container attach	Bir konteynerin terminal ekranına bağlanır.	docker container attach <container_id>
docker container exec	Çalışan bir konteynerde komut çalıştırır.	docker container exec -it <container_id>
docker container kill	Bir konteyneri doğrudan durdurur.	docker container kill <container_id>
docker container inspect	Bir konteynerin detaylı bilgilerini gösterir.	docker container inspect <container_id>

Docker konteynerlerde yapılan işlemlere ait örnek komutlar şunlardır:

- docker exec -it [konteyner_id] bash
  Belirtilen konteyner tanımlayıcı numarasına sahip konteynerin terminal ekranına bağlanır.
- docker exec -it [konteyner_id] ls
  Belirtilen konteyner tanımlayıcı numarasına sahip konteynerin dosya yapısını listeler.
- docker stop [konteyner_id]
  Belirtilen konteyner tanımlayıcı numarasına sahip konteynerin çalışmasını durdurur.
- docker rm [konteyner_id]
  Belirtilen konteyner tanımlayıcı numarasına sahip konteyneri siler.
- docker inspect [konteyner_id]
  Belirtilen konteyner tanımlayıcı numarasına sahip konteynerin detaylı bilgilerini görüntüler.

4.1.2.5. Docker Volume (Veri Birimi)

Docker konteynerleri geçici yapıya sahiptir. Docker konteynerleri durdurulup başlatıldığında veriler korunur ancak konteyner silinirse veriler kaybolur. Konteyner silinse dahi veriler kalsın istenirse Docker Volume kullanılması gerekir.

Bilgi işlem sistemlerinde uygulamalar veri saklama durumuna göre ikiye ayrılır:

- Stateless (Durumsuz)
- Stateful (Durumlu)

Stateless uygulamalar; kullanıcıya ait herhangi bir bilgiyi saklamaz. Her istek bağımsızdır ve önceki işlemler hatırlanmaz. Bu uygulamaların özellikleri; veriler saklanmaz, her işlem sıfırdan başlar ve ölçeklenmesi kolaydır. Konteynerde kolay çalışır.

Stateful uygulamalar; kullanıcıya ait bilgileri saklar. İşlemler arasında ilişki kurar. Bu uygulamaların özellikleri; verileri saklar, kullanıcı oturum bilgilerini tutar ve daha karmaşıktır. Konteynerde çalışmaları için Docker Volume gerekir.

Docker Volume kullanmak şu özellikleri sağlar:

- Oluşturulan Docker Volume birden fazla konteyner tarafından kullanılabilir.
- Docker imaj güncellemesi yapılsa bile Docker Volume'deki veriler değişmez.
- Docker Volume ile veriler taşınabilir ve kolaylıkla yedeklenebilir.
- Komut satırı arayüzü ve Docker Desktop ile yönetimi oldukça basittir.
- Hem açık kaynak kodlu işletim sistemi hem kapalı kaynak kodlu işletim sistemi konteynerlerde kullanılabilir.
- Docker Volume'ler ana makine dizininde oluşturulduğu için konteynerde hacim artışı olmaz.

SIRA SİZDE

Aşağıda bir okulda çalıştırılacak yazılımlar için Docker Volume kullanılıp kullanılmayacağı kararını konu alan bir senaryo verilmiştir.

Senaryo

Bir okulun bilişim laboratuvarında iki farklı yazılım kullanılmaktadır. Bu sistemlerde oluşan verilerin saklanması için **Docker Volume kullanılıp kullanılmaması** konusunda teknik bir karar verilmesi gerekmektedir.

1. Yazılım Öğrenci Takip Sistemi

- Öğrencilerin not ve devamsızlık bilgileri tutulmaktadır.
- Veriler sürekli güncellenmektedir.
- Sistem sık sık güncellenip yeniden başlatılmaktadır.
- Veri kaybı kesinlikle kabul edilmemektedir.

2. Yazılım Deneme Ortamı

- Öğrencilerin deneme amaçlı kullandığı bir yazılımdır.
- Test verileri geçicidir.
- Her ders sonunda sistem sıfırlanmaktadır.
- Verilerin saklanmasına gerek yoktur.

Aşağıdaki soruları senaryo metnine dayanarak yanıtlayınız. Kararlarınızı teknik gerekçelerle destekleyiniz.

Sorular

1. Birinci yazılımda Docker Volume kullanılmalı mıdır? Gerekçesini yazınız.

☐ Evet ☐ Hayır	**Gerekçeniz:** _____

2. İkinci yazılımda Docker Volume kullanılmalı mıdır? Gerekçesini yazınız.

☐ Evet ☐ Hayır	**Gerekçeniz:** _____

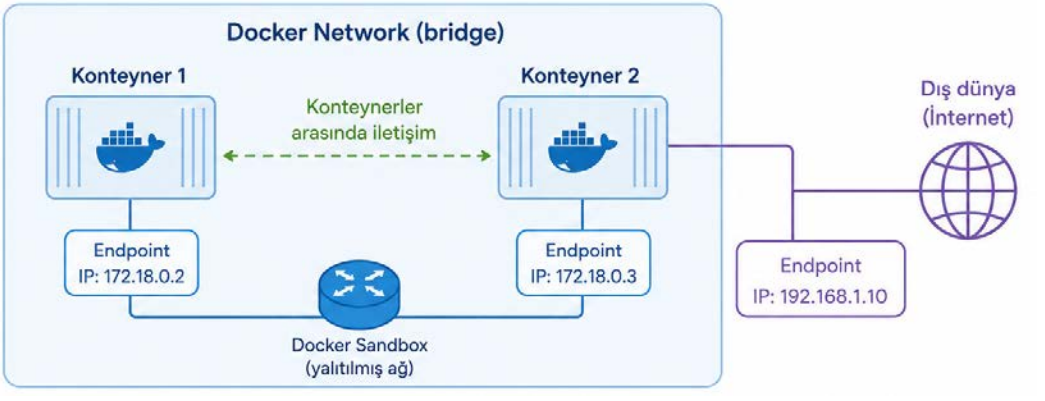
Değerlendirme

Docker Volume kullanılmasını gerektiren iki durumu aşağıya yazınız.

1	
2	

4.1.2.6. Docker Network (Ağ Yapısı)

Docker konteynerlerinin birbiriyle ve dış dünya ile iletişim kurabilmesi için **Docker Network** kullanılır. Bu sayede konteynerler arasında hem veri alışverişi yapılabilir hem de servislerin birbirine bağlanması sağlanabilir. Konteynerlerin bağımsız ve yalıtılmış çalışma şekli ağ ortamında da geçerlidir. Her bir konteynerin kendine ait ağ bağlantısı vardır. **Docker Sandbox** olarak isimlendirilen bu yapı, yalıtılmış ağ ortamını ifade eder. Konteynerler çalıştırıldığında kendilerine ait sanal bir ağ kartı **Endpoint** tanımlanır. Endpoint, IP adresi ve ağ bilgilerini içerir. Bir konteyner birden fazla ağa bağlanabilir. Her bağlantı için ayrı bir endpoint oluşur. Konteynerlerin ağ yapılandırma bilgileri, bağlı olduğu fiziksel sunucudan alınır. **Network,** konteynerlerin bağlı olduğu ağın tamamını ifade eder (Görsel 4.53).



Görsel 4.53: Ağ yapısı

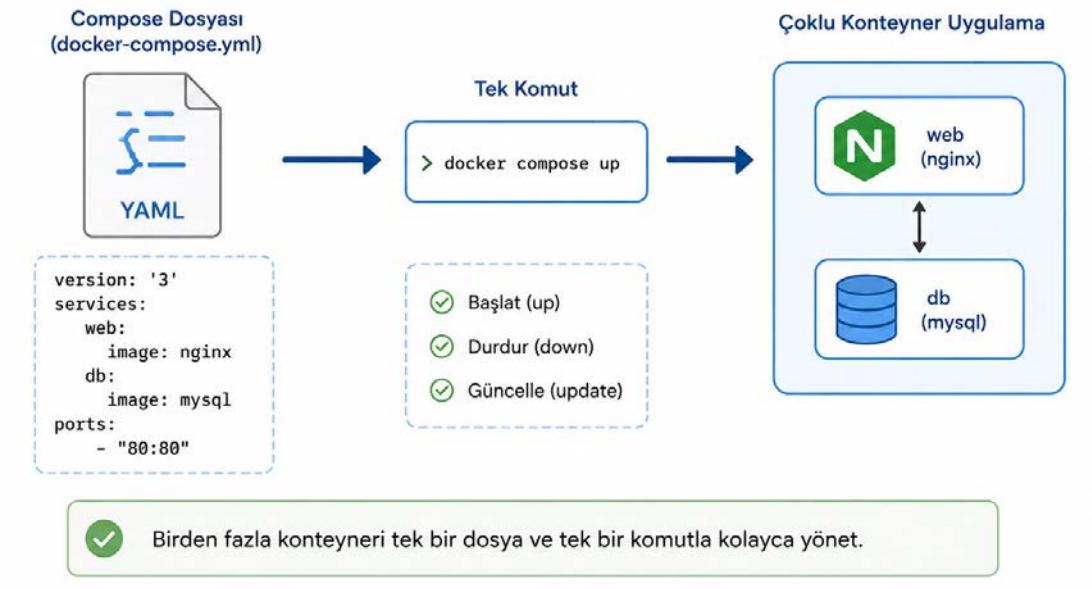
Docker, konteynerlerin farklı ihtiyaçlarına göre iletişim kurabilmesi için çeşitli ağ türleri sunar. En yaygın kullanılan ağ türleri şunlardır:

- Bridge Network (Köprü Ağı)
- Host Network (Ana Makine Ağı)
- Overlay Network (Üst Katman Ağı)
- Macvlan Network (Fiziksel Adres Tabanlı Sanal Ağ)

Ağ yapılandırmaları, sürücü yazılımları, IP adresleri, port yönlendirme, ağ izleme gibi işlemler Docker Engine tarafından yönetilir. **Network Driver,** docker ağının işleyişini yöneten yazılım bileşenidir. **IPAM Driver** ise IP adreslerinin yönetimini ve dağıtımını gerçekleştirir.

4.1.2.7. Docker Compose (Çoklu Konteyner Yönetimi)

Docker Compose, çoklu konteyner ortamlarında uygulamaların yönetilmesini sağlayan bir Docker aracıdır. Tek bir yapılandırma dosyası her bir konteynerin yapılandırmasını, bağlantılarını ve bağımlılıklarını içerir. **YAML** biçiminde hazırlanan Docker Compose dosyası **docker-compose.yml** adıyla kaydedilir. Kullanıcılar birden fazla konteynerin tek bir komutla başlatılmasını, durdurulmasını veya güncellenmesini bu sayede yönetebilir (Görsel 4.54).



Görsel 4.54: Çoklu konteyner yönetimi

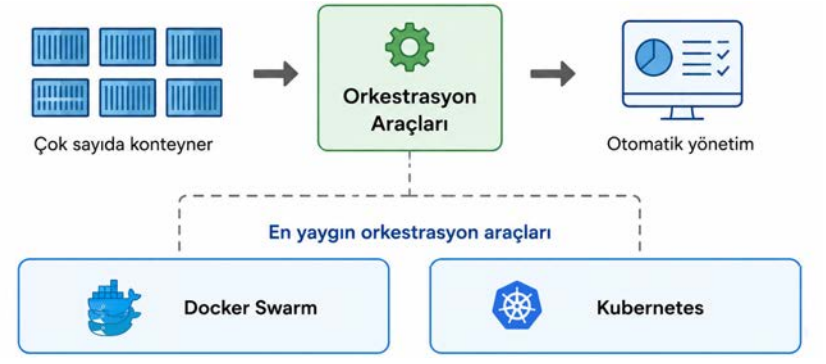
BİLGİ KUTUSU : YAML [Yet Another Markup Language (Yine Bir İşaretleme Dili)]

YAML; yapılandırma dosyalarında kullanılan, okunması anlaşılır ve sade bir veri formatıdır. Veriler girintili bir yapıda ve hiyerarşik olarak yazılır.

4.1.2.8. Docker Swarm ve Kubernetes

Konteyner teknolojisinin gelişmesiyle birlikte çok sayıda konteynerin yönetilmesi zorlaşmıştır. Bu nedenle konteynerleri otomatik olarak yöneten sistemler geliştirilmiştir. Bu sistemlere **orkestrasyon araçları** denir (Görsel 4.55). En yaygın kullanılan orkestrasyon araçları şunlardır:

- Docker Swarm
- Kubernetes



Görsel 4.55: Çoklu konteyner orkestrasyon araçları

Docker Swarm, Docker tarafından geliştirilen basit bir orkestrasyon aracıdır. Kurulumu kolaydır, Docker ile bütünleşik çalışır, küçük ve orta ölçekli sistemler için uygundur. İki temel bileşenden oluşur. Bu bileşenlerden **Swarm Node,** konteynerlerin içinde bulunduğu Docker Engine yapısını temsil eder. **Swarm Manager** ise kullanıcıların komut arayüzünden gelen taleplerine göre Swarm Node'ların yönetilmesini ve organize edilmesini sağlar.

Kubernetes, büyük ve karmaşık sistemlerde konteynerleri yönetmek için kullanılan gelişmiş bir açık kaynak orkestrasyon aracıdır. Otomatik ölçeklendirme, yük dengeleme, hata durumunda otomatik yeniden başlatma ve geniş ekosistem özelliklerine sahiptir. Worker Node (Çalışma Düğümü), Control Plane (Kontrol Düzlemi) gibi iki temel bileşenden oluşur. Bu bileşenlerden **Worker Node**; konteynerler, Container Runtime, Kubelet ve Kube Proxy bileşenlerinden oluşan bir düğümdür. **Container Runtime** yazılımıyla konteynerler çalıştırılır. **Kubelet** düğüm üzerindeki ajan yazılımdır ve podların çalışmasını sağlar. **Kube Proxy** ise ağ trafiğini yönetir ve servisler arası iletişimi sağlar. Temel bileşenlerden ikincisi Control Plane'de ise API Server, etcd, Controller Manager ve Scheduler kısımları yer alır. **API Server** tüm işlemlerin giriş noktasıdır ve kullanıcı ile sistem isteklerini alır. **etcd** tüm yapılandırma verilerini saklayan ve kümenin hafızası olan veri tabanıdır. **Controller Manager** sistem durumunu sürekli kontrol eder ve gerekli düzeltmeleri yapar. **Scheduler** podların hangi düğümlerde çalışacağını belirler. Her iki orkestrasyon aracının özelliklerinin karşılaştırılması Tablo 4.5'te gösterilmiştir.

Tablo 4.5: Docker Swarm ve Kubernetes Karşılaştırması

Özellik	Docker Swarm	Kubernetes
Kurulum	Kolay	Daha karmaşık
Öğrenme	Kolay	Zor
Ölçeklenebilirlik	Orta	Çok yüksek
Özellikler	Temel	Gelişmiş
Kullanım Alanı	Küçük projeler	Büyük sistemler

7. ÖRNEK UYGULAMA

Docker ile Python konteyner uygulamasını verilen adımlar doğrultusunda gerçekleştiriniz.

1. Adım: Docker Desktop uygulamasını çalıştırınız ve programın aktif hâle gelmesini bekleyiniz.

2. Adım: Bilgisayarda python-docker isimli dizin oluşturunuz.

3. Adım: Bu dizin içinde oluşturulan app.py isimli dosyaya aşağıdaki kodu yazınız.

```
print("Docker içinde çalışan Python uygulaması")
```

4. Adım: Aynı klasör içindeki Dockerfile isimli dosyaya aşağıdaki kodları yazınız.

```
FROM python:3.12
WORKDIR /app
COPY app.py .
CMD ["python", "app.py"]
```

5. Adım: Terminal veya komut isteminde proje klasörüne geçmek için aşağıdaki kodu giriniz ve enter tuşuna basınız.

```
cd python-docker
```

6. Adım: Aşağıdaki komut ile Docker imajını oluşturunuz.

```
docker build -t python-ilk-uygulama
```

7. Adım: Oluşturulan imajı aşağıdaki komut ile çalıştırınız.

```
docker run python-ilk-uygulama
```

8. Adım: Ekranda oluşan çıktıyı inceleyiniz.

9. Adım: Docker imajlarını listelemek için aşağıdaki komutu çalıştırınız.

```
docker image ls
```

10. Adım: Çalışan veya durmuş konteynerleri görüntülemek için aşağıdaki komutu çalıştırınız.

```
docker ps -a
```

3. ETKİNLİK

Etkinlik Adı	Docker Konteyner Tabanlı Deneme Sınavı Uygulaması
Süre	40-80 dakika
Amaç	Docker konteyner üzerinde çalışan deneme sınav uygulamasını yapmak
Yönerge	Öğretmeniniz Docker tabanlı sınav deneme uygulamasını gösterdikten sonra grubunuzla birlikte aşağıdaki adımları uygulayınız. Her adımda görev paylaşımı yapınız ve tüm grup üyelerinin aktif katılımını sağlayınız. Her adım tamamlandığında **Kontrol** sütununa (✓) işaretleyiniz.

⚠ **İş Sağlığı ve Güvenliği Kuralları**

Elektrik Güvenliği

- Elektrik prizleri, güç kabloları ve uzatma kabloları güvenli şekilde kullanınız; hasarlı ekipman kullanmayınız.
- Kurulum sırasında elektrik kesintisi riskine karşı mümkünse priz koruyucu veya UPS kullanınız.
- USB bellek takma-çıkarma işlemlerini dikkatli yapınız.

Donanım Güvenliği

- USB kurulum belleğini zorlamadan doğru yönde takınız.
- Bilgisayar açılırken BIOS/UEFI ayarlarında yanlış işlem yapmamaya dikkat ediniz.
- Kurulum sırasında depolama birimini yanlışlıkla biçimlendirmemek için disk seçimini dikkatli yapınız.

Dijital Güvenlik

- Docker konteyner işlemleri dikkatli yapılır.
- Yanlış konteyner silme / durdurma işlemlerinden kaçınılır.
- Sistem kaynakları kontrollü kullanılır.

Veri Güvenliği

- Kullanıcı bilgileri paylaşılmaz.
- Test verileri izinsiz değiştirilmez.
- Sistem çıktıları doğru şekilde kaydedilir.

Çalışma Alanı Düzeni

- Çalışma alanını düzenli tutunuz.
- Kablolar üzerinde yürümeyiniz, takılma ve düşme riskine karşı dikkatli olunuz.
- USB bellek, güç kabloları ve ağ kablolarını gelişigüzel bırakmayınız.
- Grup üyeleri arasında görev paylaşımı yapınız.

Kurulum Adımları

Adım	Yapılacak İşlem	Kontrol
1	Docker ortamının hazır olup olmadığını kontrol ediniz.	☐ Tamamlandı
2	Deneme sınavı uygulamasına ait Docker imajını çalıştırınız.	☐ Tamamlandı
3	Container'ın aktif ve doğru çalıştığını doğrulayınız.	☐ Tamamlandı
4	Deneme sınavını başlatıp süreci takip ediniz.	☐ Tamamlandı
5	Sınav sonuç ekranını inceleyerek raporlayınız.	☐ Tamamlandı

Değerlendirme

Çalışmanız öğretmeniniz tarafından kontrol listesine göre değerlendirilecektir. Çalışmanızı yaparken buradaki ölçütleri dikkate alınız. Kontrol listesi formuna ulaşmak için karekodu okutunuz. Dijital yayınlarda karekodun üstüne tıklayarak içeriğe ulaşabilirsiniz.

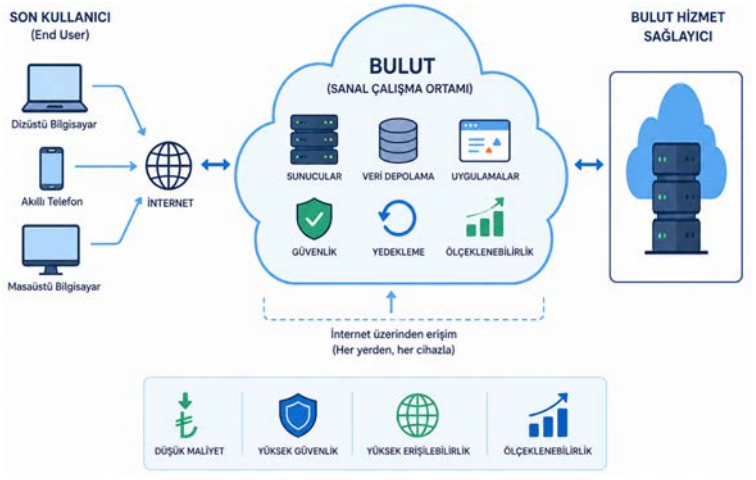
Çalışmanızı tamamladıktan sonra grup değerlendirme formunu doldurarak grup üyelerinin çalışmaya katkı düzeylerini değerlendiriniz. Grup değerlendirme formuna ulaşmak için karekodu okutunuz. Dijital yayınlarda karekodun üstüne tıklayarak içeriğe ulaşabilirsiniz.

Çalışmanızın öğrenme sürecinize katkısını değerlendirmek için öz değerlendirme formunu doldurunuz. Formu tamamladıktan sonra öğretmeninizle paylaşınız veya EBA Portfolyo'ya yükleyiniz. Öz değerlendirme formuna ulaşmak için karekodu okutunuz. Dijital yayınlarda karekodun üstüne tıklayarak içeriğe ulaşabilirsiniz.

4.2. BULUT BİLİŞİM

Bulut bilişim (Cloud computing); bilgisayar kaynaklarının (sunucu, depolama, yazılım vb.) ağ üzerinden sunulmasıdır. Bu sayede kullanıcıların fiziksel donanım bağımlılığı azalır. Klasik anlamda bilişim teknolojileri altyapısında ihtiyaç duyulan ağ kaynakları fiziksel olarak kurulur ve yönetilir fakat bu fiziksel ortamlar; yüksek kurulum maliyeti, yüksek güncelleme maliyeti, ölçeklendirme zorluğu, yönetim ve bakım hizmetlerinin sorumluluğu, yerel depolamada güvenlik açıkları gibi çeşitli olumsuz yönler içerir. Bu olumsuz yönlerle birlikte kullanıcının artan ihtiyaçları ve teknolojideki ilerlemeler bulut bilişime olan ihtiyacı artırmıştır. Bulut bilişim teknolojisinde kullanıcıların tüm ihtiyaçları internet üzerinden giderilmeye çalışılır ve kullanıcının tüm verileri de yine internetteki sanal depolarda saklanır. Bulut ortamına erişim; bulut servis sağlayıcılarının uygulamaları, web arayüzü veya uygulama programları (API - Application Programming Interface) kullanılarak gerçekleştirilir. Bulut bilişim hizmetleri internet ortamında yer aldığı için yüksek donanım maliyetlerini azaltır, veri güvenliği, yedekleme, erişilebilirlik ve ölçeklenebilirlik konusunda üst düzey hizmetler sunar. Son kullanıcı (end user) bulut adı verilen sanal çalışma ortamında güç kaynakları, sunucular, uygulamalar, veri depolama ve yazılımlara internet aracılığıyla ulaşır.

Bulut hizmet sağlayıcıları da kullanıcıların buluta ulaşmasını internet yoluyla sağlamakla görevlidir. Kullanıcılar, internet bağlantısı olan her ortamda istediği cihazla bu hizmetlere bağlanır ve bunları kullanır (Görsel 4.56).



Görsel 4.56: Bulut bilişim

Bulut bilişim sistemlerinin bileşenleri şunlardır:

- **Veri Merkezleri (Data Centers),** bulut hizmetlerinin altyapısını oluşturan fiziksel sunucuların bulunduğu yerdir.
- **Sunucular (Servers),** verilerin işlendiği ve uygulamaların çalıştığı ortamdır.
- **Depolama Sistemleri (Storage),** yedeklemenin yapıldığı ve güvenliği sağlanan verilerin saklandığı alanlardır.
- **Ağ Altyapısı (Network),** fiziksel sunucular ile kullanıcı arasında bağlantıyı sağlayan yapılardır.
- **Sanallaştırma Teknolojileri,** fiziksel kaynakların birden fazla kullanıcıya sanal olarak paylaştırılmasını sağlayan hizmetlerdir.

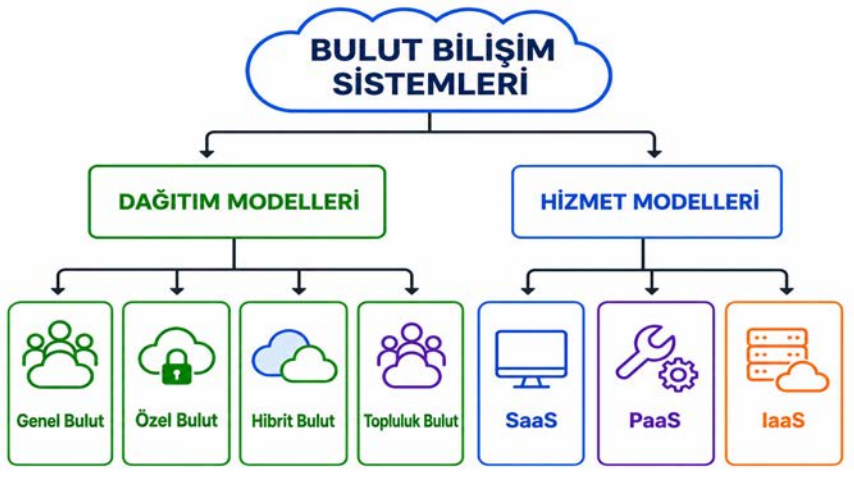
SIRA SİZDE

Aşağıdaki senaryolarda kurumların veya şirketlerin hedefleri verilmiştir. Bu hedefleri sağlayacak bulut bilişim sistemleri bileşenlerini yazınız. Yanıtlarınızı sınıfta paylaşınız.

Kullanıcı ve Senaryo	Uygun Bulut Bileşeni
1. Bir şirket, farklı şehirlerdeki kullanıcıların aynı uygulamaya internet üzerinden hızlı ve kesintisiz erişmesini istiyor.	
2. Büyük bir e-ticaret firması, milyonlarca ürün verisini güvenli şekilde saklamak ve gerektiğinde geri yüklemek istiyor.	
3. Bir bulut sağlayıcısı, tek bir fiziksel sunucu üzerinde birden fazla işletim sistemini aynı anda çalıştırarak kaynak kullanımını artırıyor.	
4. Bir oyun şirketi, oyuncuların yüksek grafik işlem gücü gerektiren oyunları internet üzerinden oynamasını sağlıyor.	
5. Dev bir teknoloji firması, dünya genelindeki tüm sunucularını tek merkezden yönetilen büyük bir tesis içinde barındırıyor.	

4.2.1. Bulut Bilişim Sistemleri

Bulut bilişim sistemleri, bulut sisteminin kim tarafından kullanıldığına göre **Dağıtım Modelleri (Deployment Models)** ve ikincisi bulut sisteminde hangi hizmetlerin sunulduğuna göre **Hizmet Modelleri (Service Models)** olmak üzere iki temel yapıya göre incelenir (Görsel 4.57).



Görsel 4.57: Bulut bilişim temel yapısı

Dağıtım modelleri, bulut hizmetlerine kullanıcıların erişim şeklini belirler. Farklı dağıtım modelleri şunlardır:

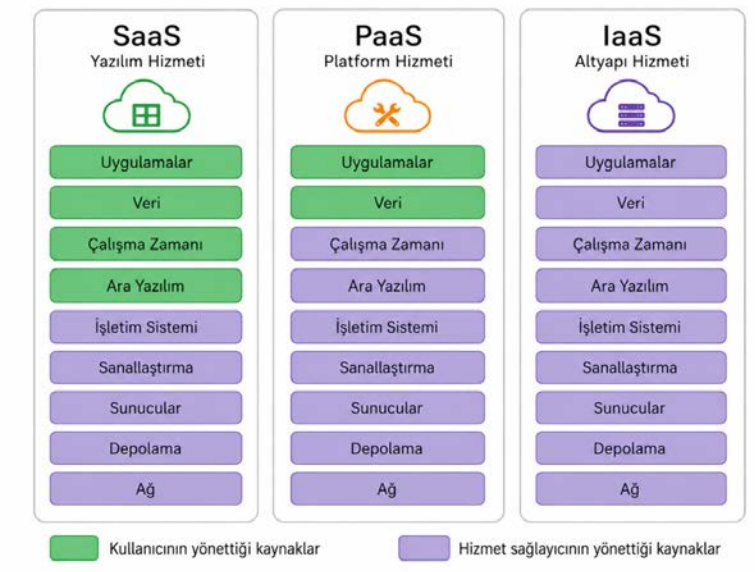
- **Genel Bulut (Public Cloud),** herkesin internet üzerinden ulaşabildiği hizmet sağlayıcılarının yönettiği modeldir. Kullanıcılar, ihtiyacı olan kaynaklara kolaylıkla erişir ve kullandıkları kadar ödeme yapabilir veya ücretsiz hizmet alabilir. Küçük ve orta ölçekli işletmelerin depolama, uygulama ve veri tabanı ihtiyaçlarına çözümler üretir.
- **Özel Bulut (Private Cloud)**, altyapı kaynaklarının sadece bir kuruluşa ayrılarak kullanıma sunulan bulut dağıtım modelidir. Güvenlik bu modelde yüksektir. Sadece yetkili kişiler verileri yönetebilir ve verilere ulaşabilir.
- **Hibrit Bulut (Hybrid Cloud),** genel bulut ve özel bulutun birlikte kullanıldığı esnek modeldir. Kuruluşlar, hassas verilerini ve uygulamalarını özel bulutta saklarken herkesin erişebileceği verilerini ve hizmetlerini genel bulutta saklar. Her iki modelin olumlu yönlerini bir araya getirerek uygun çözümler sunar.
- **Topluluk Bulut (Community Cloud),** benzer kurumların ortak ihtiyaçlarını ve gereksinimlerini karşılayan paylaşımlı bir modeldir. Kuruluşlar bulut yapısını ve politikalarını birlikte tanımlar. Topluluk bulutu, altyapıyı paylaşan kuruluşlar veya hizmet sağlayıcı tarafından yönetilir.

Hizmet modelleri, bulut bilişimde kullanıcılara sunulan hizmet türlerini ifade eder. Farklı hizmet modelleri şunlardır:

- **IaaS [Infrastructure as a Service (Hizmet Olarak Altyapı)],** bulut sağlayıcıları tarafından sağlanan altyapı modelidir. Bilişim teknolojileri altyapısında ihtiyaç duyulan gereksinimler, sanal olarak bulut ortamında sağlanır. Kullanıcılar, fiziksel donanımları değil de sanal kaynakları kiralar ve ihtiyaç duyduğu altyapıyı oluşturur. Bilgisayar, sunucu, depolama alanı, yazılım gibi bileşenleri bulut ortamında sanal olarak yapılandırır ve yönetir. Altyapının bakımı, yönetimi ve güvenliği ise hizmet sağlayıcısına aittir.
- **PaaS [Platform as a Service (Hizmet Olarak Platform)],** bu modelde yazılım ve uygulama geliştiricilere yazılım, uygulama ve test etme ortamları için gerekli geliştirme araçları, diller, veri tabanı uygulamaları gibi platformlar sağlanır. Geliştiriciler sunucu yönetimi, işletim sistemi yapılandırması gibi detaylarla uğraşmaz. Birden fazla kullanıcı birlikte bu platformda çalışabilir.

- **SaaS [Software as a Service (Hizmet Olarak Yazılım)],** kullanıcıların bir yazılımı cihazına kurmadan internet üzerinden kullanmasını sağlayan modeldir. Yazılımları abonelik yöntemiyle kiralayabilirler. Yazılımlar hazır olarak bulut üzerinde yer alır. Kullanıcılar internet erişimi olan her ortamda istediği cihazla bu yazılıma ulaşır. Yazılım güvenliği, güncelleme, yedekleme gibi işlemler hizmet sağlayıcıları tarafından yapılır.

Bulut bilişim hizmet modellerinde yönetim sorumlulukları, kullanıcı ve hizmet sağlayıcı arasında paylaşılır. Bu paylaşım, Görsel 4.58'de gösterilmiştir.



Görsel 4.58: Yönetim sorumluluk paylaşımı

SIRA SİZDE

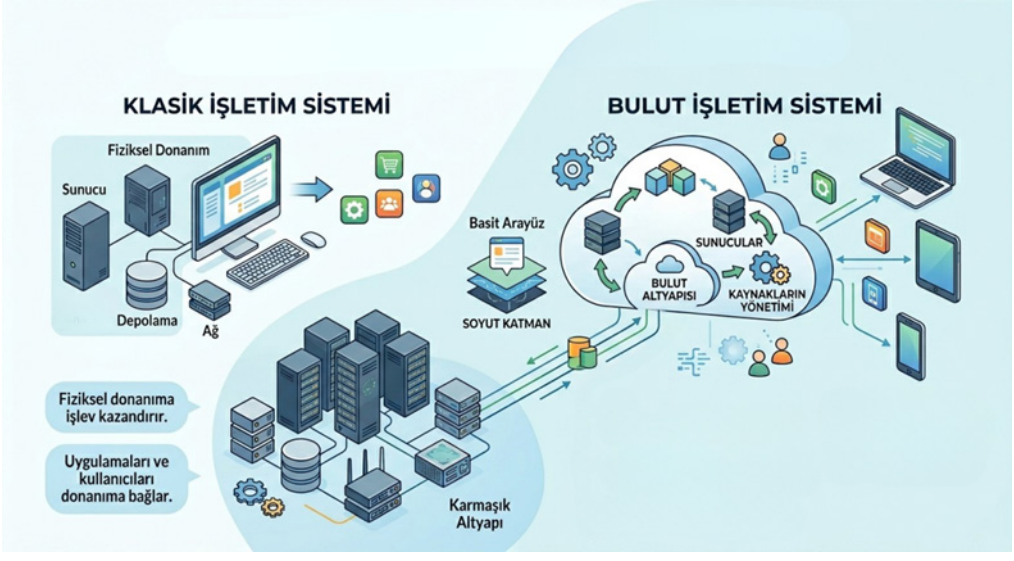
Senaryo başlığında belirtilen kullanım senaryolarını okuyunuz. O senaryo için en uygun tanımı aşağıdan seçerek, önündeki harfi **Yanıt** sütununa yazıp doğru senaryo ile eşleştiriniz.

A: Genel Bulut	B: Özel Bulut	C: Hibrit Bulut	Ç: Topluluk Bulutu

Senaryo	Yanıt
1. Ülkedeki tüm üniversiteler ortak bilimsel projeler yürütmek, akademik makaleleri paylaşmak ve ortak bir öğrenci otomasyon altyapısı kullanmak için bir araya gelip kendi sunucu sistemini kuruyor.	
2. Ulusal ölçekte hizmet veren büyük bir devlet bankası; müşteri gizliliği, kimlik numaraları ve kredi kartı bilgilerini gizli tutmak için kendi sunucu sistemini oluşturur.	
3. Milyonlarca kullanıcısı olan büyük bir e-ticaret sitesi, müşteri kayıtlarını kendi sunucularında barındırırken alışveriş sayfalarını kiraladığı sunucularda tutar.	
4. Yeni kurulan ve bütçesi kısıtlı olan bir mobil oyun girişim şirketi, oyunun veri tabanını ve görsellerini barındırmak için büyük bir sunucu yatırımı yapmak yerine alan kiralar.	

4.2.2. Bulut Bilişim İşletim Sistemleri

Bulut bilişim işletim sistemleri, veri merkezlerinde bulunan donanım kaynaklarını (sunucu, depolama, ağ vb.) yöneterek bulut hizmetlerini sağlayan yazılımlardır. Klasik işletim sistemleri fiziksel donanıma işlev kazandırıp uygulamaların ve kullanıcının hizmetine sunarken bulut işletim sistemleri sanal makineler, sunuclar, bulut altyapısı ve kaynaklarının verimli yönetilmesini sağlar. Bulut işletim sistemi soyut bir katman oluşturarak, kullanıcıların karmaşık altyapı düzenlemeleriyle uğraşmadan uygulama geliştirmelerini sağlar (Görsel 4.59).



Görsel 4.59: İşletim sistemlerini karşılaştırma

8. ÖRNEK UYGULAMA

Bulut ortamında eş zamanlı basit sohbet uygulamasını açık kaynak kodlu işletim sisteminde aşağıda verilen adımlar doğrultusunda gerçekleştiriniz.

1. Adım: Terminal ekranında paket güncellemesi için sudo apt update komutunu giriniz.

2. Adım: Konteyner yazılımı, javascript çalıştırma ortamı ve Node.js paket yöneticisi kurulumu için sudo apt install docker.io nodejs npm -y komutunu giriniz.

3. Adım: Docker servisini başlatmak için sudo systemctl start docker komutunu giriniz.

4. Adım: "sohbetoda" isminde dizin oluşturmak için mkdir sohbetoda komutunu giriniz.

5. Adım: Bu dizinin içine girmek için cd sohbetoda komutunu giriniz.

6. Adım: Dizine girdikten sonra npm init -y komutunu giriniz.

7. Adım: npm install express socket.io komutunu giriniz.

8. Adım: **nano server.js** komutuyla oluşturulan dosyaya aşağıdaki kodları girip Ctrl + O tuşuyla kaydediniz.

```
const express = require("express");
const app = express( );
const http = require("http").createServer(app);
const io = require("socket.io")(http);
app.use(express.static("public"));
io.on("connection", (socket) => {
  console.log("Yeni kullanıcı bağlandı");
  socket.on("chat message", (msg) => {
    io.emit("chat message", msg);
  });
  socket.on("disconnect", ( ) => {
    console.log("Kullanıcı ayrıldı");
  });
});
http.listen(3000, ( ) => {
  console.log("Sunucu 3000 portunda çalışıyor");
});
```

9. Adım: **Public** isminde dizin oluşturmak için **mkdir public** komutunu giriniz.

10. Adım: **Public** isimli dizine girmek için **cd public** komutunu giriniz.

11. Adım: **nano index.html** komutuyla oluşturulan dosyaya aşağıdaki kodları girip Ctrl + O tuşuyla kaydediniz.

```
<!DOCTYPE html><html><head> <title>Canlı Sohbet</title></head>
<body><h2>Canlı Mesajlaşma Uygulaması</h2>
<input id="msg" placeholder="Mesaj yaz">
<button onclick="send( )">Gönder</button>
<ul id="messages"></ul>
<script src="/socket.io/socket.io.js"></script>
<script>
const socket = io( );
    function send( ) {
      const msg = document.getElementById("msg").value;
      socket.emit("chat message", msg);
    }

    socket.on("chat message", function(msg) {
      const li = document.createElement("li");
      li.textContent = msg;
      document.getElementById("messages").appendChild(li);
    });

  </script></body></html>
```

12. Adım: **cd ..** komutuyla bir üst dizine geçiniz.

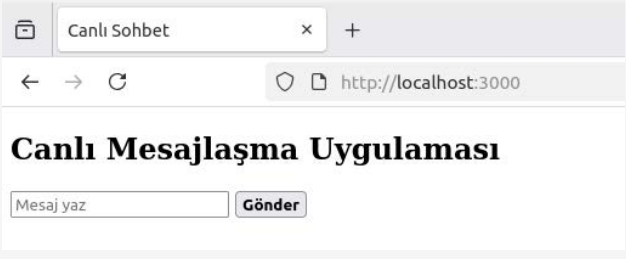
13. Adım: **nano dockerfile** komutuyla oluşturulan dosyaya aşağıdaki kodları girip Ctrl + O tuşuyla kaydediniz.

```
FROM node:18
WORKDIR /app
COPY package*.json ./
RUN npm install
COPY . .
EXPOSE 3000
CMD ["node", "server.js"]
```

14. Adım: **sudo docker build -t sohbetoda .** komutuyla imaj oluşturunuz.

15. Adım: **sudo docker run -p 3000:3000 sohbetoda** komutuyla konteyneri çalıştırınız.

16. Adım: Tarayıcıda **http://localhost:3000** adresine bağlanıp sohbet uygulamasını görüntüleyiniz (Görsel 4.60).



Görsel 4.60: Uygulama ekranı

4. ETKİNLİK

Etkinlik Adı	Docker Konteyner ile Bulut Tabanlı Okul Klasör ve Dizin Paylaşım Sistemi
Süre	40-80 dakika
Amaç	Docker konteyner kullanarak okul ortamında çalışan bulut tabanlı dosya / klasör paylaşım sistemini kurmak, erişmek ve temel kullanım işlemlerini gerçekleştirmek
Yönerge	Öğretmeniniz Docker üzerinde bulut tabanlı dosya paylaşım sistemini gösterdikten sonra aşağıdaki adımları uygulayınız. Her adımda görev paylaşımı yapınız ve tüm grup üyelerinin aktif katılımını sağlayınız. Her adım tamamlandığında Kontrol sütununa (✓) işaretleyiniz.

⚠ **İş Sağlığı ve Güvenliği Kuralları**

Elektrik Güvenliği

- Elektrik prizleri, güç kabloları ve uzatma kabloları güvenli şekilde kullanınız; hasarlı ekipman kullanmayınız.
- Kurulum sırasında elektrik kesintisi riskine karşı mümkünse priz koruyucu veya UPS kullanınız.
- USB bellek takma-çıkarma işlemlerini dikkatli yapınız.

Donanım Güvenliği

- USB kurulum belleğini zorlamadan doğru yönde takınız.
- Bilgisayar açılırken BIOS/UEFI ayarlarında yanlış işlem yapmamaya dikkat ediniz.
- Kurulum sırasında depolama birimini yanlışlıkla biçimlendirmemek için disk seçimini dikkatli yapınız.

Dijital Güvenlik

- Docker konteyner işlemleri dikkatli yapılır.
- Yanlış konteyner silme / durdurma işlemlerinden kaçınılır.
- Sistem kaynakları kontrollü kullanılır.

Veri Güvenliği

- Kullanıcı bilgileri paylaşılmaz.
- Test verileri izinsiz değiştirilmez.
- Sistem çıktıları doğru şekilde kaydedilir.

Çalışma Alanı Düzeni

- Çalışma alanını düzenli tutunuz.
- Kablolar üzerinde yürümeyiniz, takılma ve düşme riskine karşı dikkatli olunuz.
- USB bellek, güç kabloları ve ağ kablolarını gelişigüzel bırakmayınız.
- Grup üyeleri arasında görev paylaşımı yapınız.

Kurulum Adımları

Adım	Yapılacak İşlem	Kontrol
1	Docker ortamının hazır olup olmadığını kontrol ediniz.	☐ Tamamlandı
2	Bulut dosya paylaşım sistemine ait Docker imajını çalıştırınız.	☐ Tamamlandı
3	Container'ın çalıştığını ve ağ üzerinden erişilebilir olduğunu doğrulayınız.	☐ Tamamlandı
4	Web arayüzüne giriş yaparak kullanıcı oluşturunuz.	☐ Tamamlandı
5	Okul klasör yapısını oluşturunuz(örneğin Öğrenciler / Öğretmenler / Dersler).	☐ Tamamlandı

6	Dosya yükleme ve paylaşma işlemlerini gerçekleştiriniz.	☐ Tamamlandı
7	Paylaşılan klasöre başka bir kullanıcı ile erişim testini yapınız.	☐ Tamamlandı

Değerlendirme

Çalışmanız öğretmeniniz tarafından kontrol listesine göre değerlendirilecektir. Çalışmanızı yaparken buradaki ölçütleri dikkate alınız. Kontrol listesi formuna ulaşmak için karekodu okutunuz. Dijital yayınlarda karekodun üstüne tıklayarak içeriğe ulaşabilirsiniz.

Çalışmanızı tamamladıktan sonra grup değerlendirme formunu doldurarak grup üyelerinin çalışmaya katkı düzeylerini değerlendiriniz. Grup değerlendirme formuna ulaşmak için karekodu okutunuz. Dijital yayınlarda karekodun üstüne tıklayarak içeriğe ulaşabilirsiniz.

BİLGİ KUTUSU : Veri Merkezleri, Sanallaştırma ve Su Verimliliği

Bulut hizmetleri, web siteleri ve çevrim içi uygulamalar dünyanın farklı yerlerindeki veri merkezlerinde çalışır. Bu merkezlerde çok sayıda sunucu kesintisiz olarak görev yapar. Sunucular çalışırken elektrik tüketir ve ısı üretir. Bu ısının kontrol altında tutulması için soğutma sistemlerinden yararlanılır. Bazı soğutma sistemlerinde su da kullanılabildiği için veri merkezlerinde su verimliliği önemli bir konu hâline gelmiştir.

Sanallaştırma teknolojisi, aynı fiziksel donanım üzerinde birden fazla sanal sistemin çalıştırılmasını sağlar. Bu sayede daha az fiziksel sunucuyla daha fazla işlem yapılabilir. Fiziksel sunucu sayısının azalması; elektrik tüketiminin, ısı üretiminin ve soğutma ihtiyacının düşmesine katkı sağlayabilir.

Bu nedenle sanallaştırma yalnızca donanım kaynaklarını verimli kullanmayı sağlayan bir teknoloji değildir. Aynı zamanda enerji ve su kaynaklarının daha bilinçli kullanılmasına destek olan sürdürülebilir bir yaklaşımdır.

ÖLÇME VE DEĞERLENDİRME

A) Aşağıda verilen tanımlar ve bunların karşıladığı kavramları uygun harfleri kavramın önündeki parantezin içine yazarak eşleştiriniz.

1.

Kavram	Tanım
1. ( ) Hipervizör	**A)** Doğrudan fiziksel donanım üzerinde çalışan hipervizör türüdür.
2. ( ) Sanal Makine	**B)** Mevcut bir işletim sistemi üzerinde çalışan hipervizör türüdür.
3. ( ) Tip 1 Hipervizör	**C)** İşletim sistemi ve uygulamaların izole şekilde çalıştığı sanal bilgisayardır.
4. ( ) Tip 2 Hipervizör	**Ç)** Bir fiziksel sunucu üzerinde birden fazla sanal makinenin çalışmasını sağlayan yazılım katmanıdır.
	D) Bilgisayar kaynaklarının (sunucu, depolama, yazılım vb.) ağ üzerinden sunulmasıdır.

2.

Kavram	Tanım
1. ( ) IaaS	**A)** Konteyner orkestrasyonu ve yönetimidir.
2. ( ) PaaS	**B)** Uygulamaların konteyner mantığıyla çalıştırılmasıdır.
3. ( ) SaaS	**C)** Yalnızca tek kurum tarafından kullanılan bulut altyapısıdır.
4. ( ) Genel Bulut	**Ç)** Bir fiziksel sunucu üzerinde birden fazla sanal makinenin çalışmasını sağlayan yazılım katmanıdır.
5. ( ) Özel Bulut	**D)** Yazılım geliştirme ortamı ve araçlarının hizmet olarak sağlandığı modeldir.
6. ( ) Docker	**E)** Kullanıcının yalnızca uygulamayı kullandığı; altyapı ve platform yönetiminin servis sağlayıcıda olduğu modeldir.
7. ( ) Kubernetes	**F)** Sunucu, depolama ve ağ altyapısının hizmet olarak sunulduğu modeldir.
	G) Bulut hizmetlerinin altyapısını oluşturan fiziksel sunucuların bulunduğu yerdir.

B) Aşağıdaki soruların doğru cevabını işaretleyiniz.

1. **Fiziksel bir sunucunun kaynaklarını (CPU, RAM, Disk) yazılımsal olarak parçalara ayırıp birden fazla işletim sisteminin aynı anda çalışmasını sağlayan teknolojiye verilen ad aşağıdakilerden hangisidir?**

A) Sanallaştırma
B) Ağ Anahtarlama
C) Veri tabanı Yönetimi
D) Veri Madenciliği
E) İmaj oluşturma

2. **Doğrudan fiziksel donanım üzerine kurulan ve işletim sistemine ihtiyaç duymadan sanal makineleri yöneten hipervizör türü aşağıdakilerden hangisidir?**

A) Yazılım Tanımlı Depolama
B) Konteyner
C) Yerel Depolama
D) Tip 1 Hipervizör
E) Tip 2 Hipervizör

3. **Aşağıdakilerden hangisi sanallaştırmanın sağladığı temel avantajlardan biri <u>değildir</u>?**

A) Enerji tasarrufu sağlaması
B) Donanım maliyetlerini düşürmesi
C) Merkezi yönetim kolaylığı
D) Bakım süresinin azalması
E) Fiziksel alan ihtiyacını artırması

4. **Bulut bilişimde, kullanıcının sadece bir web tarayıcısı üzerinden hazır bir uygulamayı (örneğin e-posta, ofis) kullandığı hizmet modeli aşağıdakilerden hangisidir?**

A) BaaS
B) FaaS
C) IaaS
D) PaaS
E) SaaS

5. Sadece belirli bir kuruma veya şirkete özel olarak tahsis edilen, internete kapalı veya güvenli bağlantıyla erişilen bulut türü aşağıdakilerden hangisidir?

A) Hibrit Bulut
B) Genel Bulut
C) Özel Bulut
D) Topluluk Bulut
E) Çoklu Bulut

6. Konteyner silinse bile içindeki verilerin (örneğin veritabanı kayıtları) kaybolmaması için kullanılan yapı aşağıdakilerden hangisidir?

A) Docker Engine
B) Docker Network
C) Docker Volume
D) Docker Compose
E) Docker Hub

7. Docker'da çalışan konteynerleri listelemek için aşağıdaki komutlardan hangisi kullanılır?

A) docker pull
B) docker ps
C) docker sh
D) docker read
E) docker images

8. Durdurulmuş bir konteyneri silmek için aşağıdaki komutlardan hangisi kullanılır?

A) docker rm
B) docker stop
C) docker start
D) docker run
E) docker restart

9. Docker Hub'dan yeni bir imaj indirmek için kullanılan komut aşağıdakilerden hangisidir?

A) docker download
B) docker build
C) docker get
D) docker pull
E) docker push

10. **Aşağıdakilerden hangisi bir konteynerin detaylı bilgilerini gösteren komuttur?**

A) docker container attach <container_id>

B) docker container inspect <container_id>

C) docker container exec <container_id>

D) docker container pause <container_id>

E) docker container logs <container_id>

C) 1-8. soruları aşağıdaki senaryoya göre cevaplayınız.

Senaryo

Bir şirket; yüksek enerji tüketimi, artan bakım maliyetleri ve eskiyen donanımlar nedeniyle on adet fiziksel sunucu yerine, güçlü bir fiziksel sunucu üzerinde çalışan on adet sanal makine kullanmaya karar vermiştir. Ayrıca şirket, yeni bir uygulamayı kullanıma almadan önce sanal makine üzerinde test etmeyi planlamaktadır. Şirket bu sayede enerji tasarrufu sağlamayı, bakım işlemlerini kolaylaştırmayı ve ihtiyaç duyulduğunda yeni sanal sunucuları hızlıca oluşturmayı hedeflemektedir ancak bilgi işlem yöneticisi; ana sunucunun arızalanması, düzenli yedekleme yapılmaması, kaynakların yanlış planlanması, güvenlik açıkları gibi durumların tüm sistemi etkileyebileceği konusunda planlamayı yapan ekibi uyarmıştır.

1. On adet eski fiziksel sunucunun mu yoksa tek bir güçlü sunucuda on adet sanal makinenin mi sürekli çalıştırılması enerji tüketimi açısından avantajlıdır? Gerekçenizi yazınız.

.....
.....
.....

2. On yerine bir tane sunucu kullanmak bakım işlerini nasıl kolaylaştırır? Açıklayınız.

.....
.....
.....

3. Tek bir sunucuya birçok sanal makine kurmak ne gibi bir risk oluşturur? Kısaca yorumlayınız.

.....
.....
.....

4. Şirket, ilerleyen dönemde yeni bir sunucuya ihtiyaç duyarsa sanallaştırma ortamında bu ihtiyacı karşılamak fiziksel sunucu satın almaya göre neden daha kolaydır? Açıklayınız.

.....
.....
.....

5. Sunucuda çalışan sanal makinelerden biri zararlı yazılım nedeniyle etkilenirse bu durum diğer sanal makineleri nasıl etkileyebilir? Alınabilecek bir önlemi yazınız.

.....
.....
.....
.....

6. Şirket, sanallaştırma sisteminde düzenli yedekleme yapmamaktadır. Ana sunucunun arızalanması durumunda ne gibi sorunlar yaşanabilir? Açıklayınız.

.....
.....
.....
.....

7. Şirketin bilgi işlem yöneticisi, sanal makinelerin işlemci (CPU), bellek (RAM) ve depolama kaynaklarını doğru planlamazsa ne tür performans sorunları ortaya çıkabilir? Kısaca açıklayınız.

.....
.....
.....
.....

8. Şirket, sunuculardan birinde çalışan bir uygulamayı test etmek istemektedir. Bu testin sanal makine üzerinde yapılması, doğrudan fiziksel sunucuda yapılmasına göre hangi avantajları sağlar? Açıklayınız.

.....
.....
.....
.....

5. ÖĞRENME BİRİMİ

SİBER GÜVENLİĞE GİRİŞ











KONULAR

5.1. ETİK VE YASAL SORUMLULUKLAR
5.2. GENEL GÜVENLİK KONSEPTİ
5.3. FİZİKSEL GÜVENLİK
5.4. DİJİTAL ARŞİVLEME

ANAHTAR KAVRAMLAR

- bütünlük
- çevre güvenliği
- dijital arşivleme
- erişilebilirlik
- fiziksel güvenlik
- FSEK
- gizlilik
- hacker türleri
- risk
- siber zorbalık
- sızma testi (pentest)
- sosyal mühendislik
- tehdit
- tehdit istihbaratı
- varlık
- zafiyet
- zafiyet testi
- zero-day saldırısı

Bu öğrenme biriminde sizden

- siber güvenlik alanındaki etik ilkelere, gizlilik kurallarına ve yasal mevzuata göre hareket ederek güvenli dijital vatandaşlık ve mesleki sorumluluk bilinci kazanmanız
- bilgi güvenliğinin temel saçayağı olan gizlilik, bütünlük, erişilebilirlik ilkelerini kavramanız, güçlü parola standartlarını ve bütünlük kontrolü uygulamalarını gerçekleştirmeniz
- hacker türlerini, tehdit aktörlerini (APT), zararlı yazılımları, sıfırıncı gün (zero-day) ve sosyal mühendislik saldırılarını tanımanız, bu tehditlere karşı korunma yöntemlerini uygulamanız
- siber saldırı yaşam döngüsünü ve uluslararası tehdit istihbaratı yöntemlerini açıklamanız
- varlık, tehdit, zafiyet ve risk kavramlarını analiz ederek Risk Değerlendirme Diyagramı oluşturmanız, zafiyet testi ile sızma testi (pentest) farklarını ayırt etmeniz
- siber güvenlik takımlarının görevlerini karşılaştırmanız ve güvenlik kontrollerini sınıflandırmanız
- bilgi güvenliği standartları ile uluslararası çerçeveleri öğrenerek kariyer hedeflerinize uygun sertifika programlarını tanımanız
- bilişim sistemleri ve veriler için fiziksel güvenliğin önemini değerlendirerek erişim kontrolü, çevre güvenliği, yangın, sel gibi durumlara karşı alınacak fiziksel önlemleri açıklamanız
- fiziksel ve dijital arşivlemenin avantaj / dezavantajlarını karşılaştırarak, uçtan uca dijital arşivleme adımlarını (tarama, indeksleme, depolama, yedekleme, erişim kontrolü ve güvenlik) planlamanız

beklenmektedir.

HAZIRLIK ÇALIŞMASI

1. Günlük hayatta kullandığınız sosyal medya, e-posta veya internet bankacılığı hesaplarında güvenliğiniz için hangi önlemleri alıyorsunuz? Arkadaşlarınızla paylaşınız.
2. Daha önce karşılaştığınız bir sahte mesaj, sahte bağlantı veya dolandırıcılık amaçlı sosyal mühendislik girişimini nasıl fark ettiğinizi açıklayınız.
3. İnternette başkasına ait fotoğraf, video veya yazıları izinsiz paylaşmanın hangi etik ve yasal sorunlara yol açabileceğini değerlendiriniz.
4. Siber zorbalık ve hacker kavramlarının etrafındaki noktalı alanlara bu kavramlarla ilgili aklınıza gelen sözcükleri yazınız.

..... **Siber zorbalık**	..... **Hacker** .....

BAŞLARKEN

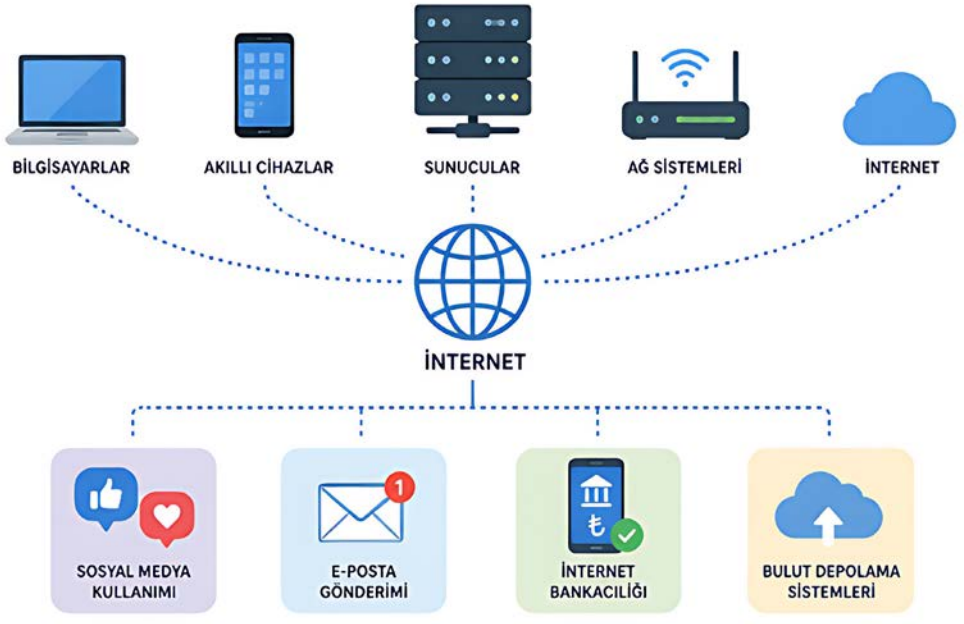
Siber güvenlik, dijital sistemlerin korunmasını sağlayan önemli bir bilişim alanıdır. Günümüzde bilgi güvenliği, gizlilik ve güvenli dijital vatandaşlık kavramları bireyler ve kurumlar için büyük önem taşımaktadır.

Siber güvenlikte etik kurallar, yasal sorumluluklar ve bilgi güvenliği standartları önemli yer tutar. Güçlü parola kullanımı, erişim kontrolü, bütünlük doğrulama, sosyal mühendislik saldırılarından korunma gibi uygulamalar sistem güvenliğini artırır. Ayrıca hacker türleri, zararlı yazılımlar, siber saldırılar ve tehdit aktörleri hakkında bilgi sahibi olmak güvenlik risklerini azaltmaya yardımcı olur.

5.1. ETİK VE YASAL SORUMLULUKLAR

Siber kelimesi; bilgisayar sistemleri, dijital teknolojiler, internet ortamı ve ağ yapılarıyla ilgili alanları ifade etmek için kullanılır. Bilişim cihazlarının ve internet kullanımının artmasıyla iletişim, eğitim, bankacılık, sağlık, kamu hizmetleri gibi birçok işlem siber ortamda gerçekleştirilmektedir.

Siber ortam; bilgisayarlar, akıllı cihazlar, sunucular, ağ sistemleri ve internet üzerinden birbirine bağlı dijital yapılardan oluşur. Sosyal medya kullanımı, e-posta gönderimi, internet bankacılığı, bulut depolama sistemleri siber ortamın kullanımına örneklerdir (Görsel 5.1).



Görsel 5.1: Siber ortam

Siber saldırı; siber ortamın kullanılmasının artmasıyla bilgisayar sistemlerine, ağlara veya verilere zarar vermek, bilgi çalmak, sistemi durdurmak ya da yetkisiz erişim sağlamak amacıyla gerçekleştirilen kötü niyetli saldırılardır. Siber güvenlik alanında teknik bilgi kadar etik kurallar, gizlilik ve bilgi güvenliği ilkeleri de büyük önem taşır.

SIRA SİZDE

Aşağıda verilen siber kavramları inceleyiniz. Soldaki her bir kavramın üst satırda yer alan ayırt edici özellikleri taşıyıp taşımadığını belirleyerek, ilgili kutucukları X işareti ile doldurunuz.

Kavramlar	Dijital Ağ ve Akıllı Cihazları Kapsar	Kötü Niyet, Zarar Verme ve Yetkisiz Erişim Amacı Taşır	Etik, Gizlilik ve Bilgi Güvenliği İlkelerini Barındırır
Siber Ortam			
Siber Saldırı			
Siber Güvenlik			

5.1.1. Etik İlkeleri

Etik, kelime anlamı olarak **ahlak bilimi** olarak tanımlanır ve bireylerin sosyal ilişkilerinde doğru ve yanlış davranışları belirleyen normları ve standartları içerir. Dürüstlük, adalet, ahlak, vicdan, onur ve sorumluluk en temel etik ilkelerdir. **Siber güvenlikte etik** ise daha çok siber ortamda davranış biçimlerini düzenleyen ve belirleyen bir disiplin olarak tanımlanır. Siber güvenlik dünyasında bilgi, tek başına bir güçtür ancak bu gücün ne yönde kullanılacağını belirleyen etiktir. Bilişim cihazlarına sızma, zafiyet bulma ve veri analizi yapma yeteneği, sınırları çok keskin çizilmiş ahlaki ve yasal kurallara dayanmalıdır. Aksi durumda savunma amaçlı öğrenilen bir bilgi kolayca yıkıcı bir araca dönüşebilir. Uluslararası bilişim dünyasında uyulması gereken kurallar şöyledir:

- Bilişim cihazları başkalarına zarar vermek için kullanılmaz.
- Diğer kişi veya kurumlara ait veriler izinsiz incelenmez.
- Diğer kişilerin geliştirdiği projeler izinsiz kurcalanmaz.
- Bilişim teknolojileri hırsızlık için kullanılmaz.
- Bilişim teknolojileri sahte delil üretmek ve yalancı şahitlik için kullanılmaz.
- Lisanssız, zararlı, kopya ya da kırılmış yazılımlar kullanılmaz.
- Diğer kişilerin bilişim teknolojilerinde geliştirdiği projeler sahiplenilemez.
- Güvenlik açıkları kötüye kullanılamaz.
- Yasalara ve mevzuatlara uygun davranılır.

SIRA SİZDE

Aşağıdaki sol sütunda siber dünyada karşılaşılabilecek Gerçek Hayat Senaryoları, sağ sütunda ise Siber Etik Kuralları verilmiştir. Senaryoları dikkatle okuyarak hangi durumun hangi etik kuralı doğrudan ihlal ettiğini eşleştiriniz ve doğru harfi parantez içine yazınız.

	Gerçek Hayat Senaryoları	Siber Etik Kuralları
(....)	1. Bir web geliştiricisinin, internette açık kaynak olarak paylaşılan bir e-ticaret kodunu tamamen kopyalayıp, üzerine kendi adını yazarak müşterisine satması	**A)** Güvenlik açıkları kötüye kullanılamaz.
(....)	2. Bir sistem uzmanının, çalıştığı kurumun sunucusunda tesadüfen bulduğu bir arka kapıyı (zafiyeti) yönetime bildirmek yerine, sistemden veri sızdırmak için kullanması	**B)** Diğer kişilerin bilişim teknolojilerinde geliştirdiği projeler sahiplenilemez.
(....)	3. Bir öğrencinin, ödev hazırlarken pahalı bir grafik tasarım programının orijinalini satın almak yerine, internetten "crack" edilmiş (kırılmış) sürümünü indirip bilgisayarına kurması	**C)** Diğer kişi veya kurumlara ait veriler izinsiz incelenmez.
(....)	4. Bir ağ yöneticisinin, mesai saatleri dışında merakından dolayı şirket genel müdürünün e-posta kutusuna girip gelen ve giden özel mesajları okuması	**Ç)** Lisanssız, zararlı, kopya ya da kırılmış yazılımlar kullanılmaz.
		D) Bilişim teknolojileri hırsızlık için kullanılmaz.

5.1.2. Mahremiyet (Gizlilik) İlkeleri

Mahremiyet, bireyin kendisine ait kişisel bilgilerinin nasıl toplandığı, kullanıldığı, saklandığı ve paylaşıldığı üzerinde kontrol sahibi olmasıdır. **Mahremiyet**, kişinin özel yaşamının korunmasını ve kişisel verilerinin izinsiz kullanılmamasını ifade eder. Mahremiyet kapsamındaki bilgiler şunlardır:

- T.C. kimlik numarası
- Telefon numarası
- Adres bilgisi
- Fotoğraf ve videolar
- Konum bilgisi
- Sağlık bilgileri
- Sosyal medya paylaşımları

Mahremiyeti korumak için yapılması gerekenler şunlardır:

- Kişisel bilgileri herkese açık paylaşmamak
- Güvenilmeyen sitelere bilgi girmemek
- Sosyal medya gizlilik ayarlarını düzenlemek
- Uygulama izinlerini kontrol etmek
- Ortak cihazlarda oturumları kapatmak

Bir kişinin izni olmadan fotoğrafının sosyal medyada paylaşılması, mahremiyet ihlaline örnek olarak verilebilir.

5.1.3. Bilgi Güvenliğiyle İlgili Yasal Zorunluluklar

Bilişim teknolojilerinin hızlı gelişimi, siber ortamların yaygınlaşması ve internet üzerinde verilerin çoğalmasıyla birlikte bilgi sistemlerine yönelik siber saldırılar artış gösterir. Bilgi güvenliğini sağlayabilmek ve siber saldırganları caydırmak için dünyada ve ülkemizde yasal düzenlemelerin yapılması kaçınılmaz hâle gelir. Türkiye'de ve dünyada bilgi güvenliğiyle ilgili yürürlükte olan yasal düzenlemelerden bazıları şunlardır:

- **Türkiye Cumhuriyeti Anayasası:** Haberleşme özgürlüğü, özel hayatın gizliliği ve kişisel verilerin korunması ile ilgili temel hakları içerir.
- **5237 Sayılı Türk Ceza Kanununun 243, 244 ve 245. Maddeleri:** Bilişim sistemlerine izinsiz erişim, veri bozma, banka ve kredi kartı suçları gibi bilişim suçlarını düzenler.
- **5846 Sayılı Fikir ve Sanat Eserleri Kanunu (FSEK):** Yazılım, dijital içerik ve diğer fikrî eserlerin telif hakkını korur.
- **6698 Sayılı Kişisel Verilerin Korunması Kanunu (KVKK):** Kişisel verilerin işlenmesi, saklanması ve korunmasına ilişkin kuralları belirler.
- **Genel Veri Koruma Tüzüğü [General Data Protection Regulation (GDPR)]:** Avrupa Birliği tarafından hazırlanan ve kişisel verilerin korunmasını amaçlayan bir veri koruma düzenlemesidir.
- **5809 Sayılı Elektronik Haberleşme Kanunu:** Elektronik haberleşme hizmetleri ve iletişim güvenliği ile ilgili düzenlemeleri kapsar.

- **5070 Sayılı Elektronik İmza Kanunu:** Elektronik imzanın kullanımını ve hukuki geçerliliğini düzenler.
- **5651 Sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun:** İnternet ortamında yapılan yayınların düzenlenmesi ve internet üzerinden işlenen suçlarla mücadele edilmesini amaçlar.
- **Elektronik Haberleşme Sektöründe Şebeke ve Bilgi Güvenliği Yönetmeliği:** Elektronik haberleşme altyapılarında bilgi güvenliği tedbirlerini düzenler.
- **Sanal Ortamda İşlenen Suçlar Sözleşmesi:** Avrupa Konseyi tarafından hazırlanan ve Türkiye'nin de taraf olduğu uluslararası siber suç sözleşmesidir.
- **Bilgi ve İletişim Güvenliği Tedbirleri Genelgesi (2019):** Kamu kurumlarında bilgi ve iletişim güvenliği için alınması gereken temel tedbirleri açıklar.
- **Bilgi ve İletişim Güvenliği Rehberi (2020):** Cumhurbaşkanlığı Dijital Dönüşüm Ofisi tarafından yayımlanan bilgi güvenliği uygulama rehberidir.
- **Bilgi ve İletişim Güvenliği Denetim Rehberi (2021):** Bilgi güvenliği süreçlerinin denetlenmesi ve değerlendirilmesine yönelik esasları açıklar.
- **7545 Sayılı Siber Güvenlik Kanunu (2025):** Türkiye'de siber güvenliğin güçlendirilmesi amacıyla hazırlanan yasal düzenlemedir. Kanun; kamu kurumları, özel sektör kuruluşları ve kritik altyapıların siber tehditlere karşı korunmasını amaçlamaktadır.

5.1.4. Telif Hakkı

Telif hakkı, bir kişinin veya kişilerin ortaya çıkardığı fikir, eser, yazılım, müzik, kitap, fotoğraf, video veya benzeri çalışmalar üzerindeki yasal kullanım ve koruma hakkıdır. Eseri oluşturan kişi **eser sahibi** olarak kabul edilir ve bu eser üzerindeki haklar kanunlarla korunur. Türkiye'de telif hakları, 5846 Sayılı Fikir ve Sanat Eserleri Kanunu (FSEK) kapsamında korunmaktadır. Korsan yazılım kullanmak, internette izinsiz film veya müzik paylaşmak, başkasına ait görsel veya yazıyı kaynak göstermeden kullanmak telif hakkı ihlallerine örneklerdir. Telif hakkı eser sahibinin emeğini korur, dijital içeriklerin izinsiz kullanılmasını engeller, yasal ve etik kullanım alışkanlığı kazandırır.

5.1.5. Dijital Vatandaşlık

Dijital vatandaşlık, bireyin dijital dünyada güvenli, etik ve sorumlu bir şekilde hareket etmesini sağlar. Bu bilinç hem bireysel güvenliği artırır hem de daha güvenli bir dijital toplum oluşmasına katkı sağlar.



ARAŞTIRMA

Telif hakkı ile korunan üç farklı eser örneğini genel ağda araştırınız. Elde ettiğiniz bilgilere göre aşağıdaki tabloyu doldurunuz.

Eser Türü	Örnek Eser / Sahibi	Kaynak (Site Adı)

5.1.5.1. Güvenli Dijital Vatandaşlık

Güvenli dijital vatandaşlık; bireylerin siber ortamı bilinçli, sorumlu ve güvenli şekilde kullanmasıdır. Bu kavram hem kişisel bilgilerin korunmasını hem de dijital ortamda etik davranış sergilemeyi kapsar. Siber vatandaşlık veya e-vatandaşlık olarak da ifade edilir. Güvenli dijital vatandaşlık dokuz temel kavramdan oluşur (Görsel 5.2).



Görsel 5.2: Güvenli dijital vatandaşlık kavramları

Güvenli dijital vatandaşlıkla ilgili kavramların açıklamaları şunlardır:

Dijital iletişim; internet, e-posta, sosyal medya, mesajlaşma uygulamaları, video konferans gibi dijital araçlar kullanılarak bilgi ve verinin aktarılması sürecidir.

Dijital erişim; bireylerin bilgisayar, akıllı telefon, tablet gibi teknolojik cihazları kullanabilme ve dijital ortamlara ulaşabilme becerisidir.

Dijital okuryazarlık, dijital ortamlarda karşılaşılan bilgilerin doğru olup olmadığını değerlendirme ve güvenilir kaynaklardan bilgiye ulaşabilme becerisidir. Bilgi kirliliğine karşı bilinçli olmayı sağlar.

Dijital güvenlik, kullanıcıların dijital ortamda kendilerini korumak için aldığı önlemleri kapsar.

Dijital etik; dijital ortamda saygılı, sorumlu ve empatik davranmayı ifade eder.

Dijital haklar, bireylerin internet ortamında sahip olduğu özgürlüklerdir. **Dijital sorumluluklar** ise bu hakları kullanırken uyulması gereken kurallardır.

Dijital kanun, internet ortamında işlenen suçların yasal karşılıklarının olduğunu ifade eder.

Dijital sağlık, uzun süreli teknoloji kullanımının fiziksel ve ruhsal etkilerini ifade eder.

Dijital ticaret; alışveriş, bankacılık gibi işlemlerin internet üzerinden yapılmasıdır.

SIRA SİZDE

Aşağıda günlük hayattan dijital kullanım senaryoları verilmiştir. Bu senaryoların güvenli dijital vatandaşlığın hangi boyutuna girdiğini yandaki sütunlardan bularak X ile işaretleyiniz.

Günlük Hayattan Dijital Senaryolar	Dijital Okuryazarlık	Dijital Sağlık	Dijital Ticaret	Dijital Güvenlik	Dijital İletişim
1. İnternetteki bir haberin doğruluğunu teyit etmek için farklı kaynakları araştırmak					
2. Mobil bankacılık uygulaması üzerinden elektrik faturasını ödemek					
3. Bilgisayar başında dik oturmaya özen gösterip ekran sürelerini kısıtlamak					
4. Sınıf arkadaşlarıyla dönem ödevi için video konferans üzerinden toplantı yapmak					
5. Sosyal medya hesaplarında iki aşamalı doğrulamayı (2FA) aktif hâle getirmek					

5.1.5.2. Siber Zorbalık

Siber zorbalık, siber ortamlar üzerinden kişilere karşı bilerek zarar verme davranışıdır. Sosyal medya, mesajlaşma uygulamaları, oyun sunucuları, cep telefonları gibi bilişim teknolojileri araçları kullanılarak gerçekleştirilen dijital saldırıdır. Bu saldırıyı gerçekleştiren kişiye **zorba,** saldırıya hedef olan kişiye ise **kurban** denir. Siber zorba, kurbanına zarar vermek için siber güvenlik araçlarını ve açıklarını kullanır. Siber zorbalığa maruz kalan kurbanlarda depresyon, anksiyete, sosyal izolasyon, özgüven kaybı, akademik başarısızlık, huzursuzluk, sürekli tehdit algısı gibi etkilere rastlanır. Bu etkiler çok olumsuz sonuçlara yol açabilir o yüzden göz ardı edilmemelidir.

Siber zorbalık davranışları şunlardır:

- Hakaret veya kötü mesaj göndermek
- Sosyal medyada alay etmek
- Küçük düşürücü yorum yapmak
- İzinsiz fotoğraf veya video paylaşmak
- Sahte hesap açmak
- Tehdit ve rahatsız edici mesajlar göndermek
- Çevrim içi gruplardan dışlamak
- Yalan bilgi ve dedikodu yaymak
- Özel bilgileri paylaşmak
- Oyunlarda aşağılayıcı konuşmak

- Hesaplara zarar vermek
- İnsanları korkutmak veya kışkırtmak

Siber zorbalığa karşı kurbanlar tarafından alınacak önlemler şunlardır:

- Zorbalık yapan kişiye cevap vermemek
- Mesaj, ekran görüntüsü ve kanıtları saklamak
- Zorbalık yapan kişiyi engellemek
- Güvenilir bir yetişkinden yardım istemek
- Öğretmen, aile veya rehber öğretmene durumu bildirmek
- Şifreleri güçlü tutmak ve kimseyle paylaşmamak
- Kişisel bilgileri internette paylaşmamak
- Sosyal medya gizlilik ayarlarını kullanmak
- Gerekirse ilgili platforma şikâyette bulunmak
- Kendini güvende hissetmediğinde resmî kurumlara başvurmak

SIRA SİZDE

Aşağıda verilen balık kılçığı diyagramındaki 6 ana kategoriyi inceleyip, bu probleme yol açan nedenleri belirleyerek ilgili kutucuklara maddeler hâlinde yazınız. Analizinizi tamamladıktan sonra balık kılçığının en altında yer alan **çözüm önerileri** bölümüne siber zorbalığı engellemeye yönelik en etkili çözüm adımlarını ekleyiniz.



5.1.6. Siber Güvenlik Uzmanı

Siber güvenlik uzmanı; bilişim cihazlarını, ağları, yazılımları ve verileri siber saldırılara karşı koruyan kişidir. Bilişim korsanlarının, kötü niyetli yazılımların ve siber tehditlerin neden olduğu güvenlik açıklarını tespit etmek, önlemek ve zafiyetlere karşı çözüm üretmek için çalışır. Siber güvenlik uzmanının temel sorumlulukları şunlardır:

- Yasalara ve etik kurallara uygun çalışmak
- Fikrî mülkiyet haklarının ve ticari sırların ihlalinden kaçınmak
- Güncel yazılım ve uygulamaların kullanılmasını teşvik etmek ve sistemleri sürekli güncel tutmak
- Mesleki faaliyet sırasında elde edilen bilgilerin gizliliğini korumak ve kendi menfaati için kullanmamak
- Güvenlik açıklarını ve ihlalleri yetkililere bildirmek
- Sızma testi için verilen izin ve yetki kapsamında güvenlik testlerini yapmak
- Sistemleri siber saldırılardan korumak için güvenlik önlemlerini almak

SIRA SİZDE

Aşağıdaki yapılandırılmış gridde (numaralandırılmış kutucuklar) siber güvenlik uzmanının temel sorumlulukları ve yapmaması gerekenler verilmiştir. Kutucuk numaralarını kullanarak soruları cevaplayınız. Bir kutucuk numarasını birden fazla soru için kullanabilirsiniz.

1	Yasalara ve etik kurallara uygun çalışmak	2	Sistemleri ve yazılımları sürekli güncel tutmak	3	Tespit ettiği açıkları internet forumlarında paylaşmak	4	Fikrî mülkiyet haklarının ihlalinden kaçınmak
5	Siber saldırılara karşı koruyucu önlemler almak	6	Elde ettiği gizli bilgileri kendi menfaati için kullanmak	7	Sızma testlerini yazılı izin ve yetki kapsamında yapmak	8	Ticari sırları korumak ve ihlalinden kaçınmak
9	Sistemlerdeki zafiyetlere karşı pratik çözümler üretmek	10	Güvenlik açıklarını ve ihlalleri yetkililere bildirmek	11	Kurumlardan habersiz sistemlere sızma testi uygulamak	12	Güncel yazılım ve uygulamaların kullanımını teşvik etmek

	Sorular
A)	Bir siber güvenlik uzmanının mesleğini icra ederken uyması gereken **etik ve yasal** sorumluluklar hangi numaralı kutularda bulunmaktadır?
	Cevap:.....
B)	Bir siber güvenlik uzmanının sahada aktif olarak yerine getirdiği **teknik ve koruyucu** görevler hangi numaralı kutularda bulunmaktadır?
	Cevap: .....
C)	Metne ve siber güvenlik ilkelerine göre bir uzmanın **asla yapmaması gereken (etik / yasal ihlale giren)** hatalı davranışlar hangi kutularda bulunmaktadır?
	Cevap: .....

5.2. GENEL GÜVENLİK KONSEPTİ

Genel güvenlik konsepti; bireylerin, kurumların ve sistemlerin karşılaşabileceği fiziksel veya dijital tehditlere karşı korunmasını amaçlayan temel güvenlik anlayışıdır. Amaç; can, mal, bilgi ve sistem güvenliğini sağlayarak oluşabilecek riskleri en aza indirmektir. Bu anlayış kapsamında şunlar hedeflenir:

- Risklerin belirlenmesi
- Tehditlerin analiz edilmesi
- Güvenlik önlemlerinin alınması
- Olası saldırı ve tehlikelere karşı hazırlıklı olunması

5.2.1. Güvenlik Kavramları

Siber güvenlik; bilgisayar sistemlerini, ağları, yazılımları, cihazları ve verileri siber saldırılara, yetkisiz erişimlere, veri kaybına ve dijital tehditlere karşı koruma çalışmalarının tümüdür. Siber güvenliğin temel amacı; bilgilerin korunması, sistemlerin güvenli çalışması, yetkisiz erişimlerin engellenmesi, veri kaybının önlenmesi ve dijital ortamın güvenli hâle getirilmesidir.

Bilgi güvenliği; bilginin yetkisiz kişilerin eline geçmesini, yayılmasını, değiştirilmesini veya kaybolmasını önlemek için alınan teknik ve idari önlemlerin bütünüdür. Verilerin anlamlı kullanılabilir hâle getirilmiş biçimine **bilgi** denir. Örnek olarak 90 ve Matematik birer veridir. Öğrencinin matematik notu 90'dır, ifadesi ise bilgidir.

Bilgi güvenliğinin üç temel ilkesi vardır. **Gizlilik (Confidentiality), Bütünlük (Integrity)** ve **Erişebilirlik (Availability)** bu ilkeler tam olarak uygulandığında bilgi güvenliği sağlanmış olur. Bu ilkeler bilgi güvenliğinin temelini oluşturur. Bu üç bilgi güvenlik ilkesine kısaltılarak **CIA üçlüsü** ismi verilir (Görsel 5.3).



Görsel 5.3: Bilgi güvenliği ilkeleri

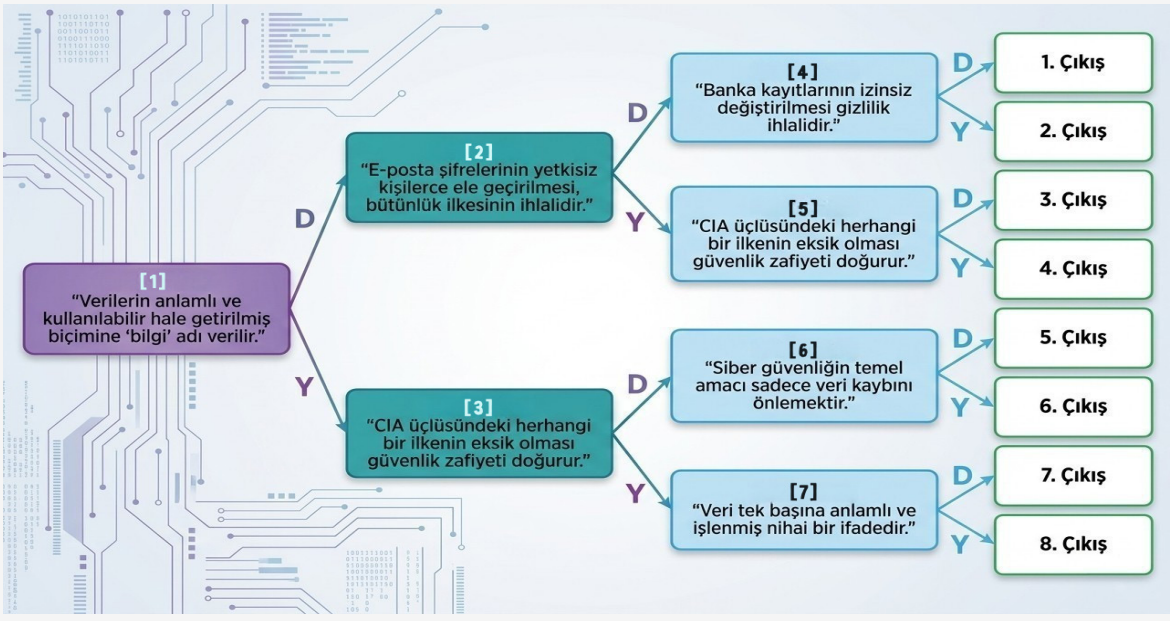
Gizlilik: Bilginin sadece yetkili kişiler tarafından erişilebilir olmasıdır. Diğer bir ifade ile bilginin yetkisiz kişiler tarafından elde edilmesinin engellenmesidir. İnternet bankacılığı erişim bilgileri, sosyal medya ve e-posta şifreleri gibi bilgilerin yetkisiz kişilerce ele geçirilmesi gizlilik ilkesinin ihlal edilmesine örnek gösterilebilir.

Bütünlük: Bilginin izinsiz olarak değiştirilememesi, silinememesi ve doğruluğunun korunmasıdır. Siber saldırganın; banka kayıtlarına erişip değiştirmesi, silmesi veya yeni bilgiler eklemesi bütünlük ilkesinin ihlal edilmesine örnek gösterilebilir.

Erişilebilirlik: Yetkili kişilerin bilgiye ihtiyaç duyduklarında erişebilmesidir. Siber saldırganın bir web sayfasını erişilmez hâle getirmesi erişilebilirlik ilkesinin ihlal edilmesine örnek gösterilebilir.

SIRA SİZDE

Tanılayıcı ağaç diyagramını inceleyiniz. En soldaki ifadeden başlayarak doğru (D) veya yanlış (Y) olduğuna karar verip okları takip ediniz. Yapacağınız her doğru seçim sizi siber güvenlik açısından farklı bir duruma ulaştıracaktır. Hatasız bir analiz zinciriyle ulaşmanız gereken doğru çıkışı bulunuz.



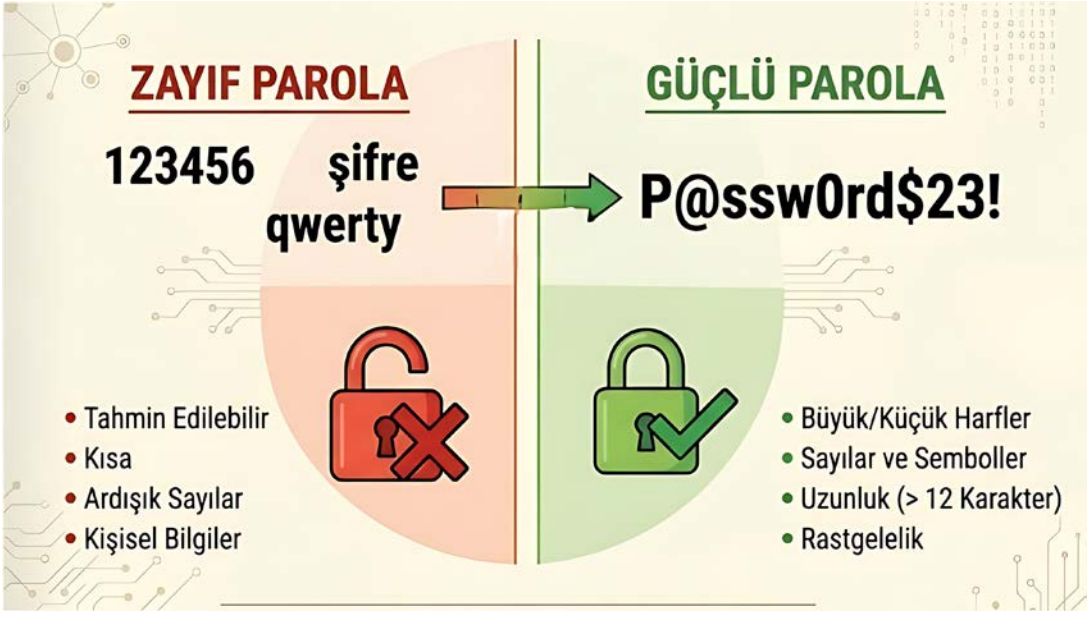
Ulaşılan Çıkış: .....

5.2.2. Güçlü Parola ve Bütünlük Kontrolü

Bilgi güvenliği ilkelerinden gizliliği sağlamanın en temel yöntemlerinden bir tanesi siber ortamda kullanılan hesaplara güçlü ve güvenli parola belirlemektir. Bu sayede yetkisiz kişilerin bilgilere ulaşması zorlaştırılır. Bilgi güvenliği ilkelerinden bütünlüğü sağlamanın yöntemlerinden bir tanesi bütünlük kontrolüdür. **Güçlü parola;** tahmin edilmesi zor, güvenli ve kırılması uzun süren paroladır. Güçlü parola belirlerken şu özelliklerde olmasına dikkat edilmelidir:

- En az 12 karakter olmalı
- Büyük harf içermeli
- Küçük harf içermeli
- Rakam içermeli
- Özel karakter içermeli (`!, ?, *, #, @` gibi)

Güçlü parola belirlendikten sonra aynı parolayı farklı hesaplarda kullanmamak, parolayı kimseyle paylaşmamak, doğum tarihi gibi tahmini kolay parolalar kullanmamak ve iki aşamalı doğrulama kullanmak gizlilik ilkesi açısından önemlidir (Görsel 5.4).



Görsel 5.4: Zayıf ve güçlü parola

Bütünlük kontrolü; bir bilginin veya dosyanın değiştirilip değiştirilmediğini kontrol etme işlemidir. Bu işlem sayesinde bilginin doğru kalması, dosyanın bozulup bozulmadığının anlaşılması ve yetkisiz değişiklerin fark edilmesi sağlanır. Bütünlük kontrolünde kullanılan en yaygın yöntemler şunlardır:

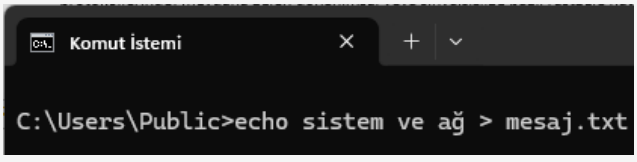
- **Kriptografik Özet Fonksiyonları (Hashing):** Bütünlük kontrolü denildiğinde akla gelen ilk ve en güçlü yöntemdir. Veri, boyutu ne olursa olsun matematiksel bir fonksiyondan geçirilerek sabit uzunlukta özet bir parmak izi (hash) oluşturulur. Eğer veride tek bir bit bile değişirse oluşan özet tamamen farklı olur (Buna çığ etkisi denir). En yaygın algoritmalar SHA-256, SHA-3, MD5 ve SHA-1'dir.
- **Mesaj Doğrulama Kodları (MAC ve HMAC):** Sadece verinin değişmediğini değil aynı zamanda verinin doğru kaynaktan gelip gelmediğini de kontrol etmek için kullanılır. Gizli bir anahtar (secret key) ile hash fonksiyonunun birleştirilmesiyle (HMAC) çalışır. Anahtara sahip olmayan biri veriyi değiştirse bile geçerli bir doğrulama kodu üretemez.
- **Dijital İmzalar (Digital Signatures):** Asimetrik şifreleme (açık ve gizli anahtar çifti) kullanarak hem bütünlüğü hem de kimlik doğrulamayı sağlar. Ek olarak inkâr edilememezlik (non-repudiation) ilkesini garanti eder. Başka bir ifadeyle veriyi imzalayan kişi bu veriyi ben göndermedim, diyemez.
- **Kontrol Toplamı (Checksum):** Genellikle ağ üzerinden veri iletimi sırasında (örneğin TCP/IP protokollerinde) meydana gelen donanımsal veya sinyal bozulması ve iletim hatalarına bağlı rastgele hataları tespit etmek için kullanılır.
- **Dosya Bütünlüğü İzleme [FIM (File Integrity Monitoring)]:** Sistemlerdeki kritik işletim sistemi dosyalarının, yapılandırma dosyalarının veya uygulama klasörlerinin durumunu sürekli tarayan yazılımsal çözümlerdir.
- **Erişim Kontrolleri ve Sürüm Yönetimi:** Verinin bütünlüğünü bozulmadan önce korumaya yönelik proaktif yöntemlerdir.

1. ÖRNEK UYGULAMA

Bir dosyanın bütünlük kontrolünü aşağıdaki adımları izleyerek gerçekleştiriniz.

1. Adım: Komut istemi penceresini açınız.

2. Adım: mesaj.txt dosyasını oluşturmak için echo sistem ve ağ > mesaj.txt komutunu girip Enter tuşuna basınız (Görsel 5.5).



Görsel 5.5: Dosya oluşturma

3. Adım: Dosyanın hash değerini certutil -hashfile mesaj.txt SHA256 komutuyla alınız (Görsel 5.6).

```
C:\Users\Public>certutil -hashfile mesaj.txt SHA256
SHA256 hash of mesaj.txt:
b57d5727575f0608f0131dabf4228e8226d53654c010175fdb094b721143bbf9
CertUtil: -hashfile command completed successfully.
```

Görsel 5.6: Hash değerini öğrenme

4. Adım: mesaj.txt dosyasının içeriğini değiştirmek için tekrar echo Sistem ve ağ > mesaj.txt komutunu girip Enter tuşuna basınız (Görsel 5.7).

```
C:\Users\Public>echo Sistem ve ağ > mesaj.txt
```

Görsel 5.7: Dosya içeriğini değiştirme

5. Adım: Dosyanın hash değerini certutil -hashfile mesaj.txt SHA256 komutuyla alınız (Görsel 5.8).

```
C:\Users\Public>certutil -hashfile mesaj.txt SHA256
SHA256 hash of mesaj.txt:
b7b6ac176c7816aee5aacd9aa2c15b75d8d4f92fdc50f711ae5cea0f2c509d08
CertUtil: -hashfile command completed successfully.
```

Görsel 5.8: İçerik değiştikten sonra hash değerini öğrenme

6. Adım: Önceki hash değeri ile sonraki hash değerini karşılaştırınız.

5.2.3. Hacker Kavramı

Hacker (bilgisayar korsanı) kavramı genellikle siber suçluları çağrıştırsa da aslında siber ortam konusunda ileri düzeyde teknik bilgiye sahip, sistemlerin sınırlarını zorlayan ve sorun çözen kişileri de ifade eder. Hacker kavramı geçmişte teknolojiyi alışılmışın dışında farklı yollarla kullanan bilişim uzmanları için bir övgü olarak kullanılırken zamanla güvenlik açıklarından faydalanan kişileri tanımlamak için de kullanılmaya başlanmıştır.

Hackerlar; taşıdıkları niyet, etik değerler ve yasallık durumuna göre temelde üç ana türe ayrılır (Görsel 5.9).



Görsel 5.9: Hacker türleri

1. Siyah Şapkalı Hacker: Siber ortama izinsiz giriş yapan, verileri ele geçiren, silen veya değiştiren amacı zarar vermek veya maddi kazanç sağlamak olan kişileri ifade eder.

2. Beyaz Şapkalı Hacker (Etik Hacker): Siber ortamların güvenliğini artırmak, zayıf noktalarını tespit etmek ve bu zayıf noktaları ortadan kaldırmak, saldırıları önlemek ve tespit etmek için çalışan, sızma testi yapan iyi niyetli hackerlardır. Faaliyetlerini izin alarak gerçekleştirirler ve bulundukları yerde siber güvenlik uzmanı olarak görev yapar.

3. Gri Şapkalı Hacker: Siyah şapkalı hacker ile beyaz şapkalı hacker arasında bir yerde durur. Sistemlere izinsiz giriş yapabilir. Sistemlere zarar verebileceği gibi zarar vermeden zafiyetin düzeltilmesini de sağlayabilir.

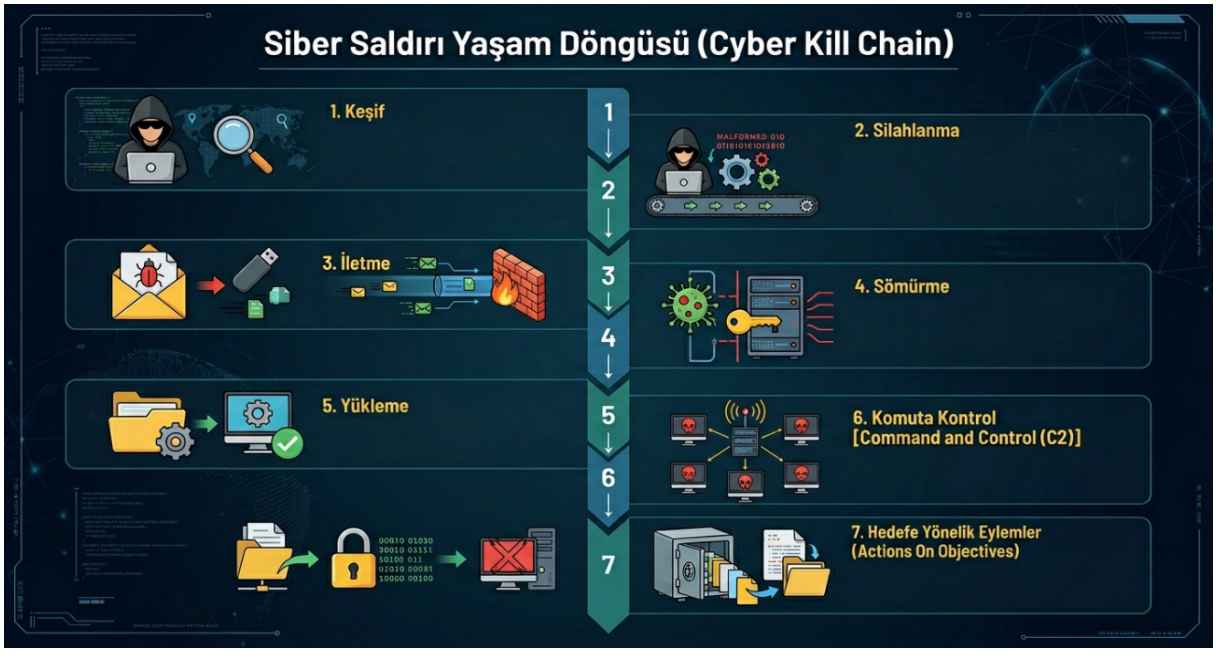
SIRA SİZDE

Siber dünyada ileri düzey teknik bilgiye sahip olan hacker kavramının alt türlerini inceleyiniz. Aşağıdaki tabloda boş bırakılan özellikleri, bu hacker türlerinin niyet, yasallık-izin durumu ve temel amaçlarını dikkate alarak doldurunuz.

Karşılaştırma Kriteri	Siyah Şapkalı Hacker	Beyaz Şapkalı Hacker	Gri Şapkalı Hacker
Temel Amacı / Niyeti	Zarar vermek veya maddi kazanç sağlamak		
Sistemlere Giriş İzni		Her zaman izinli / yetkili çalışır.	
Keşfedilen Açığa Ne Yapılır?	Verileri siler, değiştirir veya ele geçirir.		Zafiyetin düzeltilmesini sağlayabilir veya zarar verebilir.
Siber Güvenlikteki Rolü	Siber suçlu / Saldırgan		Duruma göre değişir.

5.2.4. Siber Saldırı Yaşam Döngüsü

Siber saldırılar; siber ortamlarda var olan zayıflıkları kullanarak bilişim sistemlerine, ağlara veya dijital verilere zarar vermek, bilgi çalmak ya da sistemi çalışamaz hâle getirmek amacıyla yapılan kötü niyetli işlemlerdir. Bu işlemler gerçekleştirilirken takip edilen planlı aşamalara **siber saldırı yaşam döngüsü (Cyber Kill Chain)** denir (Görsel 5.10).



Görsel 5.10: Siber saldırı yaşam döngüsü

Siber saldırı yaşam döngüsü şu aşamalardan oluşur:

- **Keşif (Reconnaissance):** Hedef siber ortamda güvenlik açıklarını bulmak için yapılan keşif faaliyetleridir.
- **Silahlanma (Weaponization):** Keşif aşamasında tespit edilen güvenlik açıklarına yönelik hangi zararlı yazılımı veya aracı kullanacağına karar verilen aşamadır. Zararlı yazılım veya siber saldırı aracı bu aşamada geliştirilir.
- **İletme (Delivery):** Hazırlanan zararlı yazılım veya siber saldırı araçları hedef sisteme e-posta, USB bellek vb. yöntemler kullanılarak iletilir.
- **Sömürme (Exploitation):** Siber saldırganın hedef sisteme gönderdiği zararlı yazılımı veya siber saldırı aracını çalıştırmaya başladığı aşamadır.
- **Yükleme (Installation):** Zararlı yazılımın hedef sisteme kalıcı olarak kurulduğu aşamadır.
- **Komuta Kontrol [Command and Control (C2)]:** Yüklenen zararlı yazılım uzaktan kontrol edilerek hedef sistemin ele geçirildiği aşamadır.
- **Hedefe Yönelik Eylemler (Actions on Objectives):** Siber saldırganın hedef sistemde verileri elde etme, değiştirme, silme, şifreleme vb. zararlı faaliyetleri gerçekleştirdiği aşamadır.

SIRA SİZDE

Bir siber saldırgan, hedef seçtiği bir kuruma veya sisteme doğrudan sızamaz, planlı ve aşamalı bir yol izler. Aşağıda sol sütunda bir siber saldırganın gerçek hayatta gerçekleştirdiği operasyonel eylemler (senaryolar), sağ sütunda ise siber saldırı yaşam döngüsünün aşamaları karışık olarak verilmiştir. Öğrendiğiniz bilgileri dikkate alarak, her bir senaryonun döngünün hangi aşamasına ait olduğunu bulunuz ve ilgili harfi parantez içine yazınız.

	Gerçek Hayat Senaryoları	Döngünün Aşamaları
(....)	**1.** Saldırganın, şirketin insan kaynakları departmanına içinde "Özgeçmiş" süsü verilmiş bir fidye yazılımı (ransomware) barındıran e-posta göndermesi	**A)** Keşif
(....)	**2.** İnsan kaynakları çalışanının e-postadaki dosyayı indirmesiyle birlikte, zararlı kodun bilgisayardaki yazılım açığını tetikleyip çalışmaya başlaması	**B)** Silahlanma
(....)	**3.** Saldırganın, hedef şirketin web sitesini, çalışanların sosyal medya hesaplarını ve açık portlarını tarayarak zafiyet araması	**C)** İletme
(....)	**4.** Sisteme yerleşen yazılımın, saldırganın yurt dışındaki sunucusuyla gizli bir bağlantı kurarak uzaktan komut almaya hazır hâle gelmesi	**Ç)** Sömürme
(....)	**5.** Saldırganın, tespit ettiği güvenlik açığına özel olarak veri tabanını ele geçirecek bir siber saldırı aracı / kodu geliştirmesi	**D)** Yükleme
(....)	**6.** Uzaktan kontrolü tamamen ele geçiren saldırganın, şirketin tüm müşteri veri tabanını şifreleyip fidye talep etmesi	**E)** Komuta Kontrol
(....)	**7.** Tetiklenen zararlı yazılımın, bilgisayarın arka planına kendini fark ettirmeden kalıcı olarak kurması ve yerleşmesi	**F)** Hedefe Yönelik Eylemler
		G) Depolama

5.2.5. Siber Saldırı Türleri

Siber saldırganlar, hedef siber ortamların zafiyetlerini kullanmak için farklı teknikler kullanır.

Zararlı yazılım (Malware-Malicious Software) saldırıları; siber ortama veya kullanıcılara zarar vermek, önemli verileri çalmak, yetkisiz erişim sağlamak veya sistemin işleyişini engellemek amacıyla özel olarak geliştirilmiş her türlü kod veya programın kullanıldığı saldırılardır.

Web uygulaması ve enjeksiyon saldırıları; web sayfalarının kodlama hatalarından ve veri tabanı açıklarından faydalanarak yapılan saldırılardır. SQL enjeksiyon (SQLi), web sitelerindeki girdi alanlarına zararlı SQL komutları göndererek arka plandaki veri tabanından yetkisiz veri çekme, değiştirme, silme veya yönetici yetkileri elde etme saldırısıdır. Siteler arası betik çalıştırma (XSS), web sitelerine zararlı JavaScript kodları enjekte ederek, o siteyi ziyaret eden kurbanların tarayıcı bilgilerini ve oturum çerezlerini (session cookie) çalma yöntemidir.

Hizmet engelleme (Erişilebilirlik) saldırıları; bilgi güvenliğinin **erişilebilirlik** ilkesini doğrudan hedef alan, siber ortamları hizmet dışı bırakmayı amaçlayan saldırılardır. DoS ve DDoS, web sunucusuna veya ağ cihazına kaldırabileceğinden fazla yapay trafik ve istek göndererek sistemin kilitlenmesini ve gerçek kullanıcılara hizmet veremez hâle gelmesini sağlayan saldırılardır. DDoS saldırılarında binlerce zombi bilgisayar, sunucu ve IoT cihazdan oluşan bir ordu kullanılır.

Sosyal mühendislik ve insan odaklı saldırılar; siber ortamlardan ziyade, sistemin en zayıf halkası olan insan unsurunu, güven duygusunu ve dikkatsizliği hedef alan saldırılardır. Oltalama başlıca sosyal mühendislik saldırılarındandır.

Ağ ve iletişim katmanı saldırıları; bilgisayar ağlarında veri iletimini hedef alan ve iletişimin gizliliğini, bütünlüğünü veya erişilebilirliğini bozmaya yönelik saldırılardır. Bu saldırılar ağ cihazlarını, iletişim protokollerini veya veri paketlerini hedef alabilir. En yaygın ağ ve iletişim katmanı saldırıları ortadaki adam [Man-in-the-middle (MITM)], ARP sahteciliği (ARP Spoofing), DNS sahteciliği (DNS Spoofing) ve paket dinlemedir (Sniffing).

Kaba kuvvet saldırıları (Brute Force); siber saldırganların bir sisteme yetkisiz erişim sağlamak amacıyla hedef kullanıcıya ait şifreleri tahmin etmek için gerçekleştirdiği deneme-yanılma yöntemidir. Bu saldırı türünde yazılımlar aracılığıyla binlerce kullanıcı adı ve parola kombinasyonu arka arkaya test edilerek doğru olan bulunmaya çalışılır. Özellikle tahmini kolay, kısa ve yaygın olarak tercih edilen zayıf parolalar bu saldırılara karşı savunmasızdır. Güçlü parola, iki aşamalı doğrulama, başarısız giriş denemelerini sınırlandırmak, zararlı IP engelleme yöntemleri ile kaba kuvvet saldırılarından korunulabilir.

Sıfırıncı gün saldırıları (Zero-Day Attacks); yazılım ya da sistem üzerinde var olan ancak üretici firma veya siber güvenlik uzmanları tarafından henüz keşfedilmemiş güvenlik açıklarına "sıfırıncı gün açığı" denir. Bu gizli boşlukları üreticiden önce fark eden saldırganların düzenlediği siber eylemlere ise "sıfırıncı gün saldırısı" adı verilir. İsmini, sistem üreticisinin bu açığı kapatmak veya bir yama geliştirmek için henüz "0" (sıfır) güne sahip olmasından alır. Bu tehlikeli saldırı türünden korunmanın en etkili yolu, zafiyet tespit edildiği an üretici tarafından çok hızlı bir şekilde güvenlik güncellemelerinin (yamaların) hazırlanıp sisteme uygulanmasıdır.

Gelişmiş sürekli tehditler [APT (Advanced Persistent Threat)]; siber saldırganların hedef seçtikleri bir ağa gizlice sızıp, kendilerini fark ettirmeden çok uzun süreler boyunca sistemde kalmasını amaçlayan son derece karmaşık ve planlı siber saldırı operasyonlarıdır. APT saldırıları, sıradan siber eylemlerden çok farklıdır. Genellikle siber alanda rekabet eden devletler, askerî kurumlar ya da küresel organizasyonlar tarafından yürütülür. Bu operasyonların gerçekleştirilebilmesi için çok yüksek düzeyde teknik uzmanlık, sabır ve büyük maddi kaynak (bütçe) gerekir.

ARAŞTIRMA

Siber saldırı türlerinden en çok karşılaşılan ilk üçünü genel ağda araştırınız. Elde ettiğiniz bilgilere göre aşağıdaki tabloyu doldurunuz.

Siber Saldırı Türü	Kısa Açıklaması	Kaynak (Site Adı)

SIRA SİZDE

Aşağıda bir kurumun bilgi işlem merkezinde veya kullanıcılarında gerçek hayatta yaşanabilecek 6 farklı siber olay senaryosu verilmiştir. Bu olayların hangi siber saldırı türüne karşılık geldiğini bularak altlarındaki boşluklara yazınız.

Vaka / Senaryo	Saldırı Türü
1. Bir kamu kurumunun resmî web sitesine aynı saniyede dünya genelindeki binlerce virüslü "zombi" bilgisayardan yapay istekler gönderilmiş, sunucu aşırı yükten dolayı kilitlenmiş ve vatandaşlar siteye saatlerce erişememiştir.	
2. Bir yazılım devi, işletim sistemindeki çok gizli bir kodlama hatasını henüz fark etmemişken siber suçlular bu açığı üreticiden önce bulmuş ve dünya genelindeki sistemlere yama çıkana kadar sızmayı başarmıştır.	
3. Bir siber saldırgan, hedef şirketin web sitesindeki "Kullanıcı Giriş" paneline otomatik bir yazılım bağlamış, saniyede yüzlerce kez "123456", "password", "admin" gibi yaygın şifre kombinasyonlarını deneyerek sisteme sızmaya çalışmıştır.	
4. Bir e-ticaret sitesinin arama çubuğuna özel kodlar gönderen bir saldırgan, veri tabanındaki güvenlik mekanizmasını aşarak arka planda duran tüm müşteri kredi kartı bilgilerini ve adres verilerini ekrana dökmeyi başarmıştır.	
5. Halka açık, şifresiz bir kafe Wi-Fi ağına bağlanan bir şirket çalışanının ağ trafiğine gizlice sızan bir hacker, çalışanın web tarayıcısı üzerinden gönderdiği kullanıcı adlarını ve kurumsal şifreleri havada yakalamıştır.	
6. Bir devletin nükleer tesisindeki endüstriyel kontrol sistemlerini sabote etmek amacıyla, çok yüksek bütçeli, devlet destekli uzman bir siber grup tarafından sisteme gizlice sızılmış ve yıllarca fark edilmeden veri sızdırılmıştır.	

5.2.6. Zararlı Yazılım ve Kullanım Yerleri

Zararlı yazılımlar; gösterdikleri davranışlara, yayılma yöntemlerine ve hedeflerine göre farklı kategorilere ayrılır.

Virüs (Virus): Biyolojik virüslere benzer şekilde, tek başlarına bağımsız bir şekilde çalışamazlar; yürütülebilir bir dosyaya, programa veya makro içeren dokümanlara (`.exe`, `.bat`, `.docm` vb.) tutunarak sisteme sızarlar. Kullanıcı enfekte olmuş bu dosyayı çalıştırdığında virüs aktif hâle gelir, sistem belleğine yerleşir ve diğer dosyalara bulaşarak yayılır. Genellikle dosyaları bozma, silme veya işletim sistemini kararsız hâle getirme amacı taşırlar.

Solucan (Worm): Virüslerden farklı olarak yayılmak için bir dosyaya ihtiyaç duymaz. Ağ zafiyetlerini (vulnerabilities) kullanarak bilgisayardan bilgisayara kendi kendini kopyalar. Kullanıcı etkileşimine ihtiyaç duymadığı için hızlı bir şekilde birçok bilişim cihazını etkileyebilir. Solucanlar; işletim sistemlerinde olabilecek zafiyetleri hedefleyerek e-posta eklentileri, USB bellekler, FTP, HTTP ve P2P ağ paylaşımlarıyla sistemlere bulaşabilir. Bant genişliğini (network bandwidth) tüketmek, sistem kaynaklarını sömürmek ve ağ trafiğini yavaşlatmak veya çökertmek gibi zararlı etkilere sahiptir.

Fidye Yazılımı (Ransomware): Bulaştığı sistemdeki değerli dosyaları (dokümanlar, fotoğraflar, veri tabanları) güçlü algoritmalarla şifreleyen ve bu şifrelenen dosyaların çözülmesi karşılığında fidye olarak kripto para talep eden zararlı yazılımdır. Kripto para istemesinin nedeni ülkeler arası para transferinin kolay olması nedeniyledir. Fidye ödemesinin yapılması da her zaman şifreli dosyaların çözüleceği veya şifrenin verileceği anlamına gelmez.

Arka Kapı (Backdoor): Doğrudan bir zararlı yazılım değildir. Zararlı yazılımların kullanıldığı bir saldırı yöntemi olup siber saldırganların hedef sistemlere izinsiz ve fark edilmeden erişmesine olanak tanır. Bir bilişim sistemine, ağa, veri tabanına veya yazılıma, normal kimlik doğrulama (kullanıcı adı, şifre, 2FA vb.) prosedürleri atlatılarak gizlice erişim sağlama yöntemidir. Siber saldırganlar, hedef sistemi ele geçirdikten sonra o sistemde kalıcı olabilmek ve gelecekte istedikleri an tekrar giriş yapabilmek için arka kapıları kullanır. Arka kapı, Truva atları ile oluşturulabilir. Yazılımlarda XSS ve SQL enjeksiyon saldırılarına uygun zafiyetlerin bulunması, sistemde açılan yeni port üzerinden veri çıkışlarının olması arka kapı yöntemine kolaylık sağlar.

Tuş Kaydedici (Keylogger): Kullanıcının klavyeden bastığı her tuşu siber saldırganlara ileten bir yazılımdır. Bu sayede kullanıcıların şifreleri, kişisel verileri, kredi kartı bilgileri ve klavye kullanılarak ortaya çıkan tüm önemli bilgiler karşıya iletilir. Tuş kaydedici yazılımlar; güvenilir olmayan web sitelerden indirilen dosyalar, lisanssız programlar, e-posta eklentileri, USB bellekler ve ağ paylaşımlarıyla bulaşabilir.

Botnet: Tam olarak bir zararlı yazılım değildir. Siber saldırganların ağa bağlı milyonlarca cihazı (bilgisayar, IoT cihazı vb.) Truva atları vasıtasıyla ele geçirmesi ve tek bir merkezden yönetmesiyle oluşan ağlardır. Bu ağa dâhil edilen her cihaza **zombi** denilir. Büyük ölçekli siber saldırılar gerçekleştirmek veya toplu spam e-posta göndermek için kullanılan yöntemdir.

Korku Yazılımı (Scareware): Siber ortamda kullanıcılara korku ve endişe oluşturmak için geliştirilmiş zararlı yazılımdır. Sahte güvenlik uyarılarıyla olmayan bir tehlikeli durumu gerçekleşiyormuş hissi oluşturur. Bu sahte tehlikeli durumdan kurtulmak için kullanıcılara çözümler ve ücretli hizmetler sunar. Bu şekilde kazanç sağlamayı hedefler.

Truva Atı (Trojan Horse): Mitolojideki Truva atından adını alır. Kendisini yararlı, güvenli veya meşru bir yazılım gibi göstererek kullanıcının şüphelenmeden sisteme yüklemesini sağlar. Arka planda ise siber saldırganlara sisteme sızmalarını sağlayacak arka kapı oluşturur. Siber saldırganların sistemi uzaktan kontrol etmesini ve veri sızdırmasını sağlar.

Reklam Yazılımı (Adware): Kullanıcının cihazında web tarayıcı çalıştırıldığında açılır pencerelerde reklam gösteren zararlı yazılımlardır. Sadece reklam bile gösterse sistemin yavaşlamasına ve donanım kaynaklarının sömürülmesine neden olur. Kullanıcı bu reklamlara tıkladığında siber saldırgana maddi kazanç sağlayabilir.

Casus Yazılımı (Spyware): Kullanıcının bilgisi ve izni olmaksızın arka planda çalışan, kişisel verileri, sistem aktivitelerini ve kullanıcı alışkanlıklarını siber saldırgana gönderen yazılımdır.

Kök Kullanıcı Takımı (Rootkit): Siber saldırganlara bir sisteme uzaktan erişim ve kontrol izni vermek için kullanılan yazılımlardır. Rootkitler, işletim sisteminin çekirdeğine gizlenir. Dolayısıyla zararlı yazılım tespit programlarıyla tespiti güçtür. Gizli kaldıkları sürece siber saldırganlar sistemlere sızıp zarar verebilir.

SIRA SİZDE

Aşağıdaki yapılandırılmış gridde (numaralandırılmış kutucuklar) zararlı yazılım türleri verilmiştir. Kutucuk numaralarını kullanarak soruları cevaplayınız. Bir kutucuk numarasını birden fazla soru için kullanabilirsiniz.

1	Solucan (Worm)	**2**	Truva Atı (Trojan)	**3**	Kök Kullanıcı Takımı (Rootkit)	**4**	Zombi Bilgisayar
5	Virüs (Virus)	**6**	Fidye Yazılımı (Ransomware)	**7**	Korku Yazılımı (Scareware)	**8**	Reklam Yazılımı (Adware)
9	Tuş Kaydedici (Keylogger)	**10**	Casus Yazılım (Spyware)	**11**	Arka Kapı (Backdoor)	**12**	Botnet

	Sorular
A)	Yukarıdaki kutucuklardan hangileri, kullanıcıyı bir **dosyayı çalıştırmaya, bağlantıya tıklamaya veya bir program yüklemeye** ikna ederek sisteme bulaşan zararlı yazılım türleridir?
	Cevap:.....
B)	Yukarıdaki kutucuklardan hangileri, kullanıcı **bilgilerini gizlice toplayarak saldırganlara iletmek** amacıyla kullanılan zararlı yazılım türleridir?
	Cevap: .....
C)	Yukarıdaki kutucuklardan hangileri, saldırganların **ele geçirdikleri sistemler üzerinde uzaktan kontrol sağlamalarına** yardımcı olan yapı veya yazılım türleridir?
	Cevap: .....
Ç)	Yukarıdaki kutucuklardan hangileri, güvenlik yazılımlarından **saklanmak veya zararlı faaliyetleri gizlemek amacıyla** kullanılan gelişmiş zararlı yazılım türleridir?
	Cevap: .....
D)	Yukarıdaki kutucuklardan hangileri, sistem performansını düşürerek **ağ veya bilgisayar kaynaklarını yoğun şekilde tüketen** zararlı yazılım ve yapılar arasında yer alır?
	Cevap: .....
E)	Yukarıdaki kutucuklardan hangileri, kullanıcıların **korku, panik veya maddi kayıp yaşamasına neden olarak** kazanç elde etmeyi amaçlayan zararlı yazılım türleridir?
	Cevap: .....
F)	Yukarıdaki kutucuklardan hangileri, **başka zararlı yazılımların sisteme yerleşmesine veya çalışmasına** zemin hazırlayabilen zararlı türleridir?
	Cevap: .....

5.2.7. Sosyal Mühendislik Saldırı Türleri

Sosyal mühendislik; saldırganların insanların duygularını, düşüncelerini ya da davranışlarını (güven, korku, merak, açgözlülük, otoriteye itaat vb.) kontrol ederek yahut sosyal teknikleri kullanıp gizli bilgileri ele geçirme veya sisteme sızma yöntemidir.

En çok kullanılan sosyal mühendislik saldırı türleri şunlardır:

Oltalama (Phishing), sahte e-posta veya taklit web siteleriyle kullanıcı adı, parola ve banka bilgilerini ele geçirme yöntemidir.

Sesli oltalama (Vishing), telefon yoluyla yapılan sosyal mühendislik saldırısıdır. Kendisini polis, savcı, banka görevlisi gibi tanıtarak korku ve aciliyet duygusu oluşturarak kurbandan gizli bilgileri alma yöntemidir.

SMS oltalama (Smishing), sahte SMS mesajlarıyla kötü amaçlı bağlantılara göndermeyi hedefleyen yöntemdir.

Yemleme (Baiting); kurbanın merak, açgözlülük, **yüksek kazanç beklentisi gibi zaaflarını kullanarak ücretsiz verilen hediye, bedava USB vb. cihazların kullanılmasını sağlar**. Bu ücretsiz hediyeye yerleştirilen dinleme unsurlarıyla veya USB'de bulunan bilgisayarı ele geçirme yazılımıyla sistemlere sızma yöntemidir.

Omuz dikizleme (Shoulder Surfing), kurbanın yakınında bulunarak ekranında bulunan veya klavyede yazılan bilgilere erişme yöntemidir.

Taklit etme (Pretexting), daha önce kurgulanan bir senaryoda saldırganın kendisini yetkili biri gibi tanıtarak kurbandan bilgi istemesidir.

Çöp karıştırma (Dumpster Diving), imha edilmeden çöpe atılan belgeler veya cihazlar üzerinden bilgi toplanması yöntemidir.

Korkutma yazılımı (Scareware), sahte virüs gibi uyarılarla kurbana zararlı yazılım yüklemeye yönlendirme yöntemidir.

SIRA SİZDE

Aşağıda sol sütunda siber saldırganların gerçek hayatta gerçekleştirdiği operasyonel senaryolar (vakalar), sağ sütunda ise sosyal mühendislik saldırı türleri karışık olarak verilmiştir. Her bir vakanın hangi saldırı türüne ait olduğunu bulunuz ve ilgili harfi parantez içine yazınız. Bir harfi sadece bir kez kullanabilirsiniz.

	Gerçek Hayat Senaryoları	Sosyal Mühendislik Saldırı Türleri
(....)	1. Bir okulun bilgi işlem odasının dışındaki atık kutusunu inceleyen bir saldırganın, üzerinde eski sistem şifreleri ve personel isimleri yazılı olan imha edilmemiş kâğıt notları ele geçirmesi	**A)** Oltalama

	Gerçek Hayat Senaryoları	Sosyal Mühendislik Saldırı Türleri
(....)	**2.** Bir çalışanın cep telefonuna "Kargonuz adres yetersizliği nedeniyle teslim edilememiştir. Adresinizi güncellemek için tıklayın:" şeklinde gelen ve içinde zararlı bağlantı barındıran kısa mesaj	**B)** Sesli Oltalama
(....)	**3.** Bankamatikte sıra bekleyen bir kişinin, önündeki kullanıcının el hareketlerini ve ekranını gizlice takip ederek kart şifresini zihnine kaydetmesi	**C)** SMS Oltalama
(....)	**4.** Bir siber saldırganın, bir şirketin otoparkına üzerinde "Maaş Zam Oranları Gizli Raporu" yazan zararlı kod yüklü birkaç adet şık USB belleği bilerek düşürmesi ve meraklı bir çalışanın bunu bilgisayarına takmasını beklemesi	**Ç)** Yemleme
(....)	**5.** Bir personeli telefonla arayıp kendisini "Merkez Cumhuriyet Savcısı" olarak tanıtan, arkadan telsiz sesleri dinleterek bir siber suça karışıldığını söyleyip, korkutarak anne kızlık soyadını ve e-devlet şifresini isteyen saldırgan	**D)** Omuz Dikizleme
(....)	**6.** Muhasebe çalışanına "Şirket Genel Müdürü" maskeli sahte bir e-posta adresinden "Çok acil, ekteki faturayı inceleyip muhasebe paneline giriş yaparak onaylayın!" şeklinde gelen ve taklit bir web sitesine yönlendiren mesaj	**E)** Taklit Etme
(....)	**7.** Kendisini kargo kuryesi olarak tanıtan ve "Bina yönetiminden geliyorum, sistem güncellemesi için sistem odasındaki personelin dâhilî numaralarını acilen listelemeniz gerekiyor." diyerek kurgulanmış bir hikâyeyle bilgi toplayan saldırgan	**F)** Çöp Karıştırma
		G) Korkutma

1. ETKİNLİK

Etkinlik Adı	Sosyal Mühendislik Saldırılarından Korunma Yöntemleri
Süre	80 dakika
Amaç	Sosyal mühendislik (oltalama, sahte kimlik vb.) saldırı tekniklerini tanımak, analiz etmek ve kurumsal veya bireysel sistemleri bu saldırılara karşı koruyacak güvenlik yapılandırmalarını gerçekleştirmek
Yönerge	Aşağıdaki tabloda her adım için yapılacak işlem verilmiştir. İlgili koruma yöntemini, analiz aracını veya komutu belirleyerek uygulayınız. Her adımı tamamladığınızda Kontrol sütununa tik (✓) atarak işaretleyiniz.

Senaryo

Okulunuzun bilişim laboratuvarındaki öğretmen ve öğrencilere yönelik son zamanlarda yoğun **oltalama (phishing)** e-postaları geldiği tespit edilmiştir. Laboratuvardaki bilgisayarları ve kullanıcıları bu tür sosyal mühendislik saldırılarına karşı korumak, gelen şüpheli bağlantıları analiz etmek ve sistem güvenliğini artırmak için gerekli adımları uygulamanız istenmektedir.

Güvenli Kullanım Uyarısı: Bu uygulamada şüpheli bağlantı analizi ve simülasyon adımları yalnızca öğretmeninizin belirlediği güvenli laboratuvar ortamında ve yasal analiz araçları (VirusTotal vb.) kullanılarak yapılmalıdır. Gerçek kişilere yönelik izinsiz oltalama simülasyonu veya veri toplama faaliyetleri yapılmamalıdır.

Uygulama Adımları

Adım	Yapılacak İşlem	Kontrol
1	Örnek şüpheli bir e-postanın kaynak (header) bilgilerini inceleyerek gönderici IP adresini ve sahtecilik durumunu analiz ediniz.	☐ Tamamlandı
2	E-postada yer alan kısaltılmış veya şüpheli bir URL bağlantısını tıklamadan, güvenli bir çevrim içi analiz aracıyla taratınız.	☐ Tamamlandı
3	Tarayıcıda sosyal mühendislik ve kimlik avı koruma özelliklerini (Güvenli Tarama / SmartScreen) aktif hâle getiriniz.	☐ Tamamlandı
4	İşletim sisteminde gizli dosya uzantılarını görünür yaparak, sosyal mühendislikte sık kullanılan çift uzantılı tuzakları tespit ediniz.	☐ Tamamlandı
5	Sosyal mühendislerin sistemde oturum açma denemelerini engellemek için güçlü bir Hesap Kilitleme Politikası (Account Lockout Policy) yapılandırınız.	☐ Tamamlandı
6	Sosyal mühendislik yoluyla ele geçirilen şifrelerin kırılmasını zorlaştırmak için Parola Karmaşıklığı (Password Complexity) politikasını aktif ediniz.	☐ Tamamlandı
7	Sosyal mühendislerin hedef belirlemek için kullandığı sistem bilgilerini gizlemek amacıyla, ağda bilgisayarın görünürlüğünü (ağ bulma) kapatınız.	☐ Tamamlandı

Adım	Yapılacak İşlem	Kontrol
8	Tarayıcı önbelleğinde biriken ve oturum çalma (Session Hijacking) saldırılarına zemin hazırlayan çerezleri (Cookies) temizleyiniz.	☐ Tamamlandı
9	Oltalama e-postalarındaki sahte destek hatlarına karşı, bilgisayara izinsiz uzaktan bağlantı yapılmasını engellemek için Uzak Masaüstü bağlantılarını kapatınız.	☐ Tamamlandı
10	Kurumsal kimlik avını önlemek için laboratuvardaki e-posta hesaplarında **İki Adımlı Doğrulama (2FA/MFA)** ayarlarını aktif ediniz.	☐ Tamamlandı
11	Sosyal mühendislerin insanları kandırarak USB bellek takılmasını sağladığı (Baiting) saldırılara karşı, bilgisayarda Otomatik Kullan (AutoRun) özelliğini devre dışı bırakınız.	☐ Tamamlandı
12	Sosyal mühendislik saldırısına uğradığını fark eden bir öğrencinin, zararlı yazılımın merkeze veri sızdırmasını önlemek amacıyla bilgisayarın ağ bağlantısını (Ethernet/Wi-Fi) hızla kesmesi simülasyonunu yapınız.	☐ Tamamlandı

Değerlendirme

Çalışmanız öğretmeniniz tarafından kontrol listesine göre değerlendirilecektir. Çalışmanızı yaparken buradaki ölçütleri dikkate alınız. Kontrol listesi formuna ulaşmak için karekodu okutunuz. Dijital yayınlarda karekodun üstüne tıklayarak içeriğe ulaşabilirsiniz.

5.2.8. Tehdit Aktörleri

Siber güvenlik tehdit aktörleri; siber ortama zarar vermek, veri çalmak, hizmetleri aksatmak veya çıkar elde etmek amacıyla siber saldırı gerçekleştiren kişi ya da gruplardır (Görsel 5.11).



Görsel 5.11: Başlıca tehdit aktörleri

Başlıca tehdit aktörleri şunlardır:

Siber Suçlular: Maddi kazanç elde etmek amacıyla siber saldırı yapan birey veya gruplardır. Banka hesabı dolandırıcılığı, kimlik hırsızlığı, fidye yazılımı saldırıları ve kredi kartı bilgisi çalma yaygın olarak tercih eder.

Hacktivistler: Siyasi, sosyal veya ideolojik amaçlarla siber saldırı yapan gruplardır. Bir kurumu protesto etmek, kamuoyu oluşturmak veya internet sitelerini erişime kapatmak gibi yöntemleri tercih eder.

Devlet Destekli Siber Saldırganlar: Bir devlet adına çalışan profesyonel siber saldırı ekipleridir. APT [Advanced Persistent Threat (Gelişmiş Kalıcı Tehdit)] adı verilen gruplar da devlet destekli siber saldırganlar arasında yer alır. Bu APT grupları siber güvenlik ortamında en tehlikeli ve en organize tehdit aktörleri arasında yer alır. Casusluk, kritik altyapıları hedef alma ve askerî veya ekonomik bilgi toplama gibi amaçları vardır.

İç Tehditler: Siber ortamın içinde çalışan veya yetkili erişimi bulunan kişilerin oluşturduğu tehditlerdir. İki şekilde tehdit gerçekleşir. Kasıtlı zarar verme veya istenmeden yapılan güvenlik ihlali. Şifre paylaşımı, yetkisiz veri kopyalama, taşınabilir cihazlarla veri sızdırma gibi örnekleri vardır.

Betik Amatörler (Script Kiddies): Teknik bilgisi sınırlı olup hazır araçlarla siber saldırı yapan kişilerdir. Hazır siber saldırı yazılımları kullanır, merak veya gösteriş amacı taşır ve basit sistemleri hedef alır.

Siber Teröristler: Toplumda korku ve kaos oluşturmak amacıyla kritik sistemlere saldırı düzenleyen gruplardır. Bu grupların hedefinde elektrik şebekeleri, ulaşım sistemleri ve haberleşme altyapıları önde gelir.

Endüstriyel Casuslar: Rakiplerinin ticari sırlarını ele geçirmek amacıyla çalışan kişi veya gruplardır. Ar-Ge bilgileri, müşteri verileri veya üretim planları hedefleri arasındadır.

Tehdit aktörleri çoğunlukla oltalama, zararlı yazılım, sosyal mühendislik, DDoS saldırıları, şifre kırma saldırıları veya veri sızdırma gibi yöntemleri tercih eder.

5.2.9. Siber Tehdit İstihbaratı ve Yöntemleri

Siber tehdit istihbaratı [CTI (Cyber Threat Intelligence)], siber saldırganların kimliklerini, motivasyonlarını, yöntemlerini ve altyapılarını önceden analiz ederek olası saldırıları engellemeyi veya zararlarını en aza indirmeyi amaçlayan bilgi üretim sürecidir. Başlıca siber tehdit istihbaratı yöntemleri şunlardır:

Açık kaynak istihbaratı [OSINT (Open Source Intelligence)], internet siteleri, forumlar, sosyal medya, haber kaynakları ve herkese açık verilerden tehdit bilgisi toplama yöntemidir.

İnsan kaynaklı istihbarat [HUMINT (Human Intelligence)], siber tehditlerle ilgili verilere doğrudan insan üzerinden ulaşılmasıdır.

Teknik istihbarat (Technical Intelligence); zararlı yazılım örnekleri, IP adresleri, alan adları, hash değerleri, ağ trafiği gibi teknik verilerin analiz edilmesidir.

Karanlık ağ (Dark Web) izleme, dark web üzerindeki veri sızıntıları, yasa dışı satışlar ve siber saldırı planlarının takip edilmesidir.

Güvenlik günlüğü (Log) analizi, sistem ve uygulama kayıtlarının incelenerek anormal davranışların belirlenmesidir.

Balküpü (Honeypot) ve Baltuzağı (Honeynet) kullanımı, siber saldırganların dikkatini çeken sahte sistemler kurularak saldırı yöntemlerinin gözlemlenmesidir.

Tehdit avcılığı, sistemlerde gizlenmiş tehditlerin sürekli olarak araştırılmasıdır.

Siber tehdit paylaşım platformları, kurumlar arasında tehdit bilgisi paylaşımı sağlayan ortamlardan veri alınmasıdır.

MITRE ATT&CK çerçevesi, siber saldırganların kullandığı taktik ve tekniklerin sınıflandırılarak incelenmesidir.

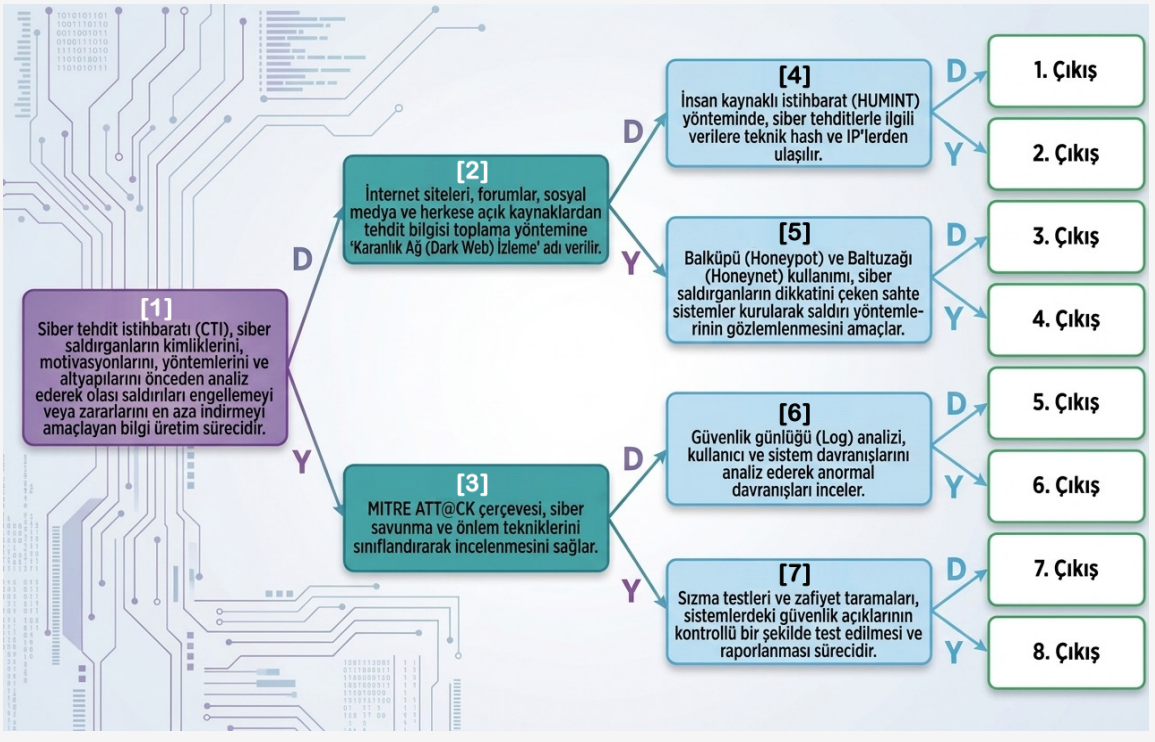
MITRE D3FEND kullanımı, savunma tekniklerini sınıflandırarak uygun güvenlik önlemlerinin belirlenmesini sağlayan yöntemdir.

Davranış analizi (Behavior Analytics), kullanıcı ve sistem davranışlarının analiz edilerek olağan dışı hareketlerin belirlenmesidir.

Sızma testleri ve zafiyet taramaları, sistemlerdeki güvenlik açıklarının kontrollü şekilde test edilmesi ve raporlanmasıdır.

SIRA SİZDE

Tanılayıcı ağaç diyagramını inceleyiniz. En soldaki ifadeden başlayarak Doğru (D) veya Yanlış (Y) olduğuna karar verip okları takip ediniz. Yapacağınız her doğru seçim sizi siber güvenlik açısından farklı bir duruma ulaştıracaktır. Hatasız bir analiz zinciriyle ulaşmanız gereken doğru çıkışı bulunuz.



Ulaşılan Çıkış: .....

5.2.10. Tehdit ve Risk

Siber güvenlikte tehdit ve risk kavramları sıklıkla birbirinin yerine kullanılsa da aralarında neden-sonuç ilişkisi vardır. Güvenlik sistemlerini doğru organize edebilmek için tehdit, risk, varlık ve zafiyet kavramlarını bir bütün olarak ele almak gerekir. Varlık, denizdeki bir gemi; zafiyet, geminin gövdesindeki hasar ve yırtık yelkenler; tehdit, yaklaşan fırtına ve kayalıklar; risk, fırtına ve kayalıkların gemiye zarar verme ihtimalidir (Görsel 5.12).



Görsel 5.12: Varlık, tehdit, zafiyet ve risk kavramları arasındaki ilişki

Bu kavramlar arasında ilişkiyi ve temel tanımları şu şekilde ifade etmek gerekir:

Varlık (Asset): Kurum veya kişi için değeri olan ve korunması gereken her türlü bileşendir. **Fiziksel varlıklar**; sunucular, bilgisayarlar, ağ cihazları ve veri depolama birimleridir. **Dijital varlıklar**; kaynak kodları, müşteri bilgileri, web uygulamaları gibi yazılımsal içeriklerdir. **Süreçsel varlıklar** ise kurum personeli, marka itibarı ve iş sürekliliğidir.

Tehdit (Threat): Bir kuruluşun varlıklarına zarar verme potansiyeli olan her türlü durumdur. Doğal afetler, çalışanların kasıtlı veya kasıtsız etkileri, zayıf güvenlik önlemleri, yazılım hataları, sistem veya donanım arızaları tehdittir.

Zafiyet (Vulnerability): Açık olarak da ifade edilir. Tehditler tarafından kullanılabilecek varlıklarda yer alan zayıflıklar, eksiklikler veya hatalardır. Güncellenmemiş bir işletim sistemindeki açık, teknik zafiyettir. Sistem odasının kapısının kilitlenmemesi fiziksel zafiyettir. Personelin sosyal mühendislik saldırılarına karşı eğitimsiz olması ise insani zafiyettir.

Risk: Bir tehdidin, sistemdeki bir zafiyeti suistimal ederek bir varlığa zarar verme olasılığı ve bu zararın yaratacağı etkinin bileşimidir. **Risk değerlendirme süreci**, kurum veya sistemlerde oluşabilecek tehditleri belirlemek, analiz etmek ve uygun önlemleri planlamak amacıyla yapılan sistematik çalışmadır. Sürece ait başlıklar ve açıklamaları şöyledir:

- **Varlıkları Belirleme:** Korunması gereken tüm varlıklar belirlenir.
- **Tehditleri Belirleme:** Varlıklara zarar verebilecek tehditler tespit edilir.
- **Zafiyetleri Belirleme:** Sistemlerdeki güvenlik açıkları ve eksiklikler incelenir.

- **Risk Analizi Yapma:** Tehditlerin gerçekleşme olasılığı ve etkisi değerlendirilir.
- **Risk Seviyesini Belirleme:** Riskler düşük, orta veya yüksek şeklinde sınıflandırılır.
- **Kontrol Önlemlerini Planlama:** Riskleri azaltmak için güvenlik tedbirleri belirlenir.
- **Riskleri İzleme ve Güncelleme:** Yeni tehditler ve sistem değişiklikleri düzenli olarak takip edilir.

SIRA SİZDE

A) Siber güvenlikte risk, kendi kendine var olmaz. Bir tehdidin, var olan bir zafiyeti sömürerek değerli bir varlığa zarar vermesiyle oluşur. Aşağıdaki tabloda siber güvenliğe dair 4 farklı gerçek hayat durumu verilmiştir. Bu durumların varlık, tehdit, zafiyet veya risk kavramlarından hangisine karşılık geldiğini bularak ilgili sütuna yazınız.

Gerçek Hayat Güvenlik Durumu	Karşılık Gelen Kavram
1. Şirketin tüm müşteri verilerinin, muhasebe kayıtlarının ve ticari sırlarının tutulduğu ana veri tabanı sunucusu.	.....
2. Şirket sunucusunda çalışan işletim sisteminin 2 yıldır hiç güncellenmemiş olması ve kaynak kodlarında hata barındırması.	.....
3. Bölgede meydana gelebilecek şiddetli bir deprem veya siber suçlular tarafından sisteme yapılabilecek bir siber saldırı olasılığı.	.....
4. Güncellenmemiş sunucu açığından faydalanan bir saldırganın müşteri verilerini şifrelemesi sonucu şirketin maddi zarara uğraması ve marka itibarını kaybetmesi ihtimali.	.....

B) Risk değerlendirme süreci, kurumlarda siber olaylar yaşanmadan önce önlem almayı sağlayan sistematik bir çalışmadır. Aşağıda bir bilgi işlem sorumlusunun risk değerlendirmesi yaparken attığı adımlar karışık olarak verilmiştir. Risk Değerlendirme Süreci aşamalarını dikkate alarak, bu adımları mantıksal ve kronolojik olarak 1'den 5'e kadar sıralayınız.

Gerçek Hayat Güvenlik Durumu
(...) Kurum personeline sosyal mühendislik eğitimi verilmesi ve sunuculara güvenlik duvarı kurulması için bütçe ve plan hazırlanması
(...) Kurumun web uygulamasında sızma testi yapılarak kaynak kodlarındaki girdi doğrulama (SQLi) hatalarının raporlanması
(...) Kurum bünyesinde bulunan kaynak kodlarının, personel bilgisayarlarının ve marka itibarının listelenerek değerlerinin belirlenmesi
(...) Tespit edilen web açığının siber suçlular tarafından kullanılma olasılığı ile veri tabanının çalınması durumunda oluşacak zararın boyutunun hesaplanması
(...) Kurumun dijital varlıklarına zarar verme potansiyeli olan APT gruplarının, siber suçluların ve olası elektrik kesintilerinin listelenmesi

2. ETKİNLİK

Etkinlik Adı	Siber Güvenlik Risk Değerlendirme Diyagramı Oluşturma
Süre	40 dakika
Amaç	Kurumsal varlıkları, tehditleri ve risk puanlarını analiz ederek standartlara uygun bir Siber Güvenlik Risk Değerlendirme Diyagramı ve Risk Matrisi yapılandırmak
Yönerge	Draw.io uygulamasını tarayıcınızda açarak boş bir proje başlatınız. Aşağıdaki tabloda her adım için yapılması gereken çizim, siber güvenlik mantığı veya araç yapılandırma işlemi verilmiştir. Adıma en uygun Draw.io özelliğini-eylemini belirleyerek uygulayınız. Her adımı tamamladığınızda Kontrol sütununa tik (✓) atarak işaretleyiniz.

Senaryo

Okulunuzun veya kurumunuzun bilişim altyapısına yeni bir sunucu ve veri tabanı sistemi entegre edildi. Bu yeni yapının siber güvenlik risklerini analiz etmek, önceliklendirmek ve yönetim kuruluna sunmak amacıyla Draw.io (diagrams.net) platformu üzerinden profesyonel bir süreç akış diyagramı ve risk matrisi hazırlamanız istenmektedir.

Güvenli Kullanım Uyarısı: Bu uygulamada modelleyeceğiniz varlıklar, tehditler ve zafiyet senaryoları tamamen simülasyon amaçlıdır. Gerçek kurumsal ağlara ait hassas IP adresleri, canlı şifre mimarileri veya gizli zafiyet raporları gibi kritik veriler Draw.io gibi bulut tabanlı halka açık ücretsiz araçlar üzerinde ham / şifresiz şekilde şemalaştırılmamalıdır.

Uygulama Adımları

Adım	Yapılacak İşlem	Kontrol
1	Draw.io üzerinde siber güvenlik ikonlarını (kilit, firewall, sunucu vb.) etkinleştiriniz.	☐ Tamamlandı
2	Sürecin başlangıç noktasını gösteren diyagram elemanını ekleyiniz.	☐ Tamamlandı
3	Korunacak varlıkları (Varlık Envanteri) listelemek için ilk süreci ekleyiniz.	☐ Tamamlandı
4	Olası siber tehditleri (Phishing, Zararlı Yazılım vb.) şemaya dâhil ediniz.	☐ Tamamlandı
5	Risk puanının hesaplanacağı bir karar (Eşkenar Dörtgen) mekanizması kurunuz.	☐ Tamamlandı
6	Hesaplanan risk skorunun kritik seviyede olması durumundaki yönlendirmeyi çiziniz.	☐ Tamamlandı
7	Yüksek riskler için alınacak acil siber güvenlik önlemini şemalaştırınız.	☐ Tamamlandı
8	Kabul edilebilir (düşük) riskler için ayrılan ikinci yolu çiziniz.	☐ Tamamlandı

Adım	Yapılacak İşlem	Kontrol
9	Düşük riskler için yapılması gereken pasif güvenlik eylemini tanımlayınız.	☐ Tamamlandı
10	Şemadaki iki farklı yolu (Kritik ve Düşük) ortak bir bitiş sürecinde birleştiriniz.	☐ Tamamlandı
11	Çizimin arka planına risk seviyelerini görselleştirmek için 5 x 5 boyutlarında bir matris alanı ekleyiniz.	☐ Tamamlandı
12	Matrisin dikey eksenini siber güvenlik risk kriterlerine göre adlandırınız.	☐ Tamamlandı
13	Matrisin yatay eksenini siber güvenlik iş etkisi kriterlerine göre adlandırınız.	☐ Tamamlandı
14	En yüksek olasılık ve en yüksek etkiye sahip 5 x 5 hücreyi siber güvenlik standartlarına göre renklendiriniz.	☐ Tamamlandı
15	En düşük olasılık ve en düşük etkiye sahip 1 x 1 hücreyi siber güvenlik standartlarına göre renklendiriniz.	☐ Tamamlandı
16	Risklerin hangi departmanlar tarafından yönetileceğini (Yönetim, BT, Güvenlik) katmanlara ayırınız.	☐ Tamamlandı

Değerlendirme

Çalışmanız öğretmeniniz tarafından kontrol listesine göre değerlendirilecektir. Çalışmanızı yaparken buradaki ölçütleri dikkate alınız. Kontrol listesi formuna ulaşmak için karekodu okutunuz. Dijital yayınlarda karekodun üstüne tıklayarak içeriğe ulaşabilirsiniz.

5.2.11. Zafiyet Testi ve Sızma Testi

Zafiyet testi (Vulnerability Assessment), siber ortamdaki bilinen zafiyetlerin otomatik araçlar ile taranması, tespit edilmesi ve listelenmesi sürecidir. Yaygın olarak kullanılan ücretsiz ve açık kaynak zafiyet testi araçları Tablo 5.1'de listelenmiştir.

Tablo 5.1: Zafiyet Testi Araçları

Araç	Açıklama	Kullanım Alanı
OpenVAS	Açık kaynak güvenlik açığı tarama sistemi	Ağ ve sistem taraması
Nmap	Ağ keşfi ve port tarama aracı	Ağ analizi
Nikto	Web sunucularındaki güvenlik açıklarını tarar.	Web güvenliği
OWASP ZAP	Web uygulaması güvenlik testi aracı	Web uygulama testi
Wapiti	Web uygulamalarında açık taraması yapar.	Web güvenliği
SQLmap	SQL Injection açıklarını test eder.	Veri tabanı güvenliği
Lynis	Linux sistem güvenlik denetimi yapar.	Sistem güvenliği

Araç	Açıklama	Kullanım Alanı
OpenSCAP	Güvenlik uyumluluk ve zafiyet taraması	Sistem denetimi
Aircrack-ng	Kablosuz ağ güvenlik testleri yapar.	Wi-Fi güvenliği
Wireshark	Ağ trafiği analiz aracı	Ağ güvenliği
ClamAV	Açık kaynak antivirüs çözümü	Zararlı yazılım tarama
Nuclei	Şablon tabanlı güvenlik açığı tarama aracıdır.	Ağ ve web güvenliği

Sızma testi (Pentest-Penetration Test), gerçek siber saldırganın davranışlarını taklit ederek kontrollü şekilde saldırı yapılması işlemidir. Yaygın olarak kullanılan ücretsiz ve açık kaynak sızma testi araçları Tablo 5.2'de listelenmiştir.

Tablo 5.2: Sızma Testi Araçları

Araç	Açıklama	Kullanım Alanı
Metasploit Framework	Güvenlik açıklarını test etmek ve istismar etmek için kullanılır.	Genel sızma testi
Kali Linux	Yüzlerce güvenlik aracını içeren Linux dağıtımı	Pentest platformu
Parrot Security OS	Güvenlik ve adli bilişim odaklı Linux sistemi	Pentest ve adli analiz
Nmap	Ağ keşfi ve port taraması yapar.	Ağ analizi
Wireshark	Ağ trafiğini analiz eder.	Paket analizi
Hydra	Parola test ve brute-force işlemleri yapar.	Kimlik doğrulama testleri
John the Ripper	Parola güvenliği testi yapar.	Parola denetimi
Aircrack-ng	Kablosuz ağ güvenliği testleri yapar.	Wi-Fi pentest
SQLmap	SQL Injection açıklarını test eder.	Web güvenliği
OWASP ZAP	Web uygulama güvenlik testleri yapar.	Web pentest
Nikto	Web sunucu açıklarını analiz eder.	Web sunucu testi
Burp Suite Community Edition	Web uygulama güvenlik testleri için kullanılır	Web uygulama testi
Responder	Ağ içi kimlik bilgisi yakalama testleri yapar	İç ağ testleri
BeEF	Tarayıcı güvenliği testleri yapar	İstemci tarafı testleri
CrackMapExec	Active Directory ve ağ testleri yapar	Kurumsal ağ pentest
Recon-ng	Bilgi toplama süreçlerinde kullanılır	Keşif (Reconnaissance)

Zafiyet testi ve sızma testi arasındaki farklar Tablo 5.3'te gösterilmiştir.

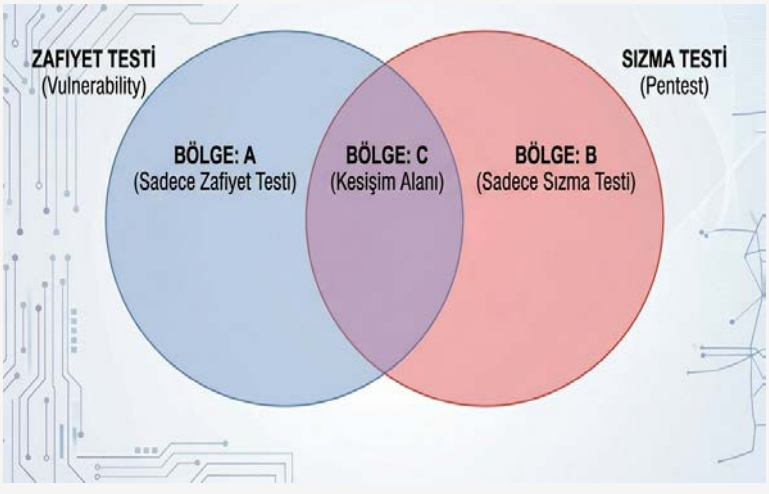
Tablo 5.3: Zafiyet ve Sızma Testi Farkları

Özellik	Zafiyet Testi	Sızma Testi
Amaç	Açıkları bulmak	Açıkları kullanarak sistemi test etmek
Yöntem	Tarama ve analiz	Kontrollü saldırı
Saldırı Simülasyonu	Yok	Var
Risk Seviyesi	Düşük	Daha yüksek
Süre	Daha kısa	Daha uzun
Derinlik	Genel tarama	Detaylı inceleme
Sonuç	Açık listesi	Açıkların etkisi ve istismar sonucu

SIRA SİZDE

Zafiyet testi ile sızma testi süreçlerini analiz ediniz. Aşağıda verilen Venn diyagramı üzerindeki A alanı sadece zafiyet testine özgü durumları, B alanı sadece sızma testine özgü durumları, kesişim alanı (C) ise her iki sürecin de ortak noktalarını temsil etmektedir. Maddeler hâlinde verilen özellikleri analiz ederek, diyagramdaki doğru alanların (A, B veya C) altına numarasını yazarak yerleştiriniz.

Gerçek Hayat Güvenlik Durumu
1. Sadece bilinen güvenlik açıklarını otomatik yazılımlarla tarar ve bir liste sunar.
2. Sisteme sızmak için keşfedilen açıkları aktif olarak istismar eder (saldırı simülasyonu yapar).
3. Sürecin yürütülmesi esnasında hedef sistemlerin kararlılığı açısından daha yüksek risk barındırır.
4. Kurumun siber güvenlik duruşunu iyileştirmek, açıkları kapatmak ve siber direnci artırmak amacıyla yapılır.
5. Nmap, SQLmap, Wireshark ve OWASP ZAP gibi açık kaynaklı araçlardan faydalanabilir.
6. Genellikle çok daha kısa sürede tamamlanan genel ve yüzeysel bir tarama faaliyetidir.



5.2.12. Siber Saldırılara Karşı Güvenlik Takımları

Genelde bir kurumun dijital varlıklarını korumak, saldırıları simüle etmek ve olaylara müdahale etmek için oluşturduğu uzman ekipleri ifade eder (Görsel 5.13).



Görsel 5.13: Siber güvenlik takımları

Blue Team [Mavi Takım (Savunma Ekibi)]: Sistemi koruyan ve izleyen ekiptir.

Red Team [Kırmızı Takım (Saldırı Simülasyon Ekibi)]: Gerçek bir hacker gibi davranarak sistemi sızma testine tabi tutar.

Purple Team [Mor Takım (Köprü Ekip)]: Red ve blue team arasında iş birliği sağlar.

SIRA SİZDE

Aşağıdaki yapılandırılmış gridde (numaralandırılmış kutucuklar) siber güvenlik takımları ve takımların sorumlulukları verilmiştir. Kutucuk numaralarını kullanarak soruları cevaplayınız. Bir kutucuk numarasını birden fazla soru için kullanabilirsiniz.

1	Red Team (Kırmızı Takım)	2	Güvenlik Günlüğü (Log) İzleme ve Analizi	3	Sızma Testi ve İstismar (Exploit)
4	Blue Team (Mavi Takım)	5	Purple Team (Mor Takım)	6	Zafiyet Taraması ve Sistem Sıkılaştırma
7	Ortak Tatbikat ve Bilgi Paylaşımı Köprüsü	8	Gerçek Bir Siber Saldırganı Simüle Etme	9	Olay Müdahalesi (Incident Response)

	Sorular	
A)	Bir kurumun siber güvenlik altyapısını korumakla görevli olan, ağ trafiğini sürekli izleyen ve bir saldırı anında ilk olay müdahalesini (incident response) gerçekleştiren savunma takımı ile bu takımın birincil görevleri hangi kutucuklarda yer almaktadır?	
	Cevap:.....	
B)	Kurumun güvenlik duvarlarını ve savunma mekanizmalarını test etmek amacıyla gerçek bir hacker gibi davranarak sisteme kontrollü sızma operasyonları düzenleyen ofansif (saldırı) takımı ve bu takımın doğrudan yürüttüğü faaliyetler hangileridir?	
	Cevap:	
C)	Saldırı ve savunma ekiplerinin birbirlerinin açıklarını kapatmasını sağlayan, iki takım arasında bir iş birliği ve bilgi paylaşım köprüsü kurarak kurumun siber direncini en üst seviyeye çıkaran entegrasyon takımı hangisidir?	
	Cevap:	

5.2.13. Siber Güvenlik Kontrolleri

Siber güvenlik kontrolleri, bir kurumun dijital varlıklarını korumak, siber riskleri azaltmak ve olası tehditlere karşı savunma hattı oluşturmak amacıyla kullanılan idari, fiziksel ve teknik önlemler bütünüdür.

Bu kontroller saldırı anındaki işlevlerine (önleyici, tespit edici ve düzeltici) göre sınıflandırılır. Siber güvenlik kontrolleri, bir siber olayın veya tehdidin hangi aşamasında devreye girdiğine bağlı olarak üç ana grupta incelenir:

1. Önleyici Kontroller (Preventive Controls): Bir güvenlik ihlalinin veya siber saldırının gerçekleşmeden önce durdurulmasını amaçlar. Tehditleri kapıda engellemeye odaklanan proaktif önlemlerdir. Örnek önlemler güvenlik duvarları (Firewall), çok faktörlü kimlik doğrulama (MFA), güçlü parola politikaları ve erişim yetkilendirmeleridir.

2. Tespit Edici Kontroller (Detective Controls): Önleyici engelleri aşarak sisteme sızan ya da içeride meydana gelen şüpheli ve zararlı aktiviteleri fark etmek için kullanılır. Saldırıyı doğrudan durdurmaz, alarm üreterek savunma ekiplerini uyarır. Örnek önlemler saldırı tespit sistemleri (IDS), güvenlik bilgisi ve olay yönetimi (SIEM), log analizi araçları, güvenlik kameraları ve dosya bütünlüğü kontrol sistemleridir.

3. Düzeltici Kontroller (Corrective Controls): Bir güvenlik ihlali tespit edildikten sonra devreye girer. Amacı, hasarı sınırlamak, sistemi tekrar güvenli hâle getirmek ve eski kararlı durumuna döndürmektir. Örnek uygulamalar yedeklerin geri yüklenmesi (Backup), sistem yamalarının uygulanması (Patch Management) ve etkilenen cihazların ağdan izole edilmesidir.

SIRA SİZDE

Aşağıdaki tabloda sol sütunda kurumlarda uygulanan bazı siber güvenlik tedbirleri ve senaryoları verilmiştir. Her bir tedbirin **Önleyici Kontrol**, Tespit Edici Kontrol veya Düzeltici Kontrol kavramlarından hangisine ait olduğunu belirleyerek ilgili kutucuğu X işareti ile doldurunuz. Her satır için sadece bir kutucuk işaretleyiniz.

Siber Güvenlik Tedbiri / Senaryosu	Önleyici Kontrol	Tespit Edici Kontrol	Düzeltici Kontrol
1. Bir şirketin ana sunucusuna yapılan yetkisiz giriş denemelerini izleyen SIEM sisteminin, gece yarısı şüpheli bir IP adresi için alarm üretmesi			
2. Çalışanların e-posta hesaplarına giriş yaparken sadece şifre yazmalarının yetmemesi, telefonlarına gelen onay kodunu (MFA) girmek zorunda olmaları			
3. Ransomware (Fidye yazılımı) saldırısına uğrayan ve dosyaları şifrelenen bir veri tabanının, siber olay müdahale ekibi tarafından dün gece alınan temiz yedeklerden geri yüklenmesi			
4. Bir sistem yöneticisinin, Windows sunucularda bulunan kritik bir sıfırıncı gün açığını kapatmak amacıyla en son yayınlanan güvenlik yamasını (Patch) tüm sisteme uygulaması			
5. Bilgi işlem odasının giriş kapısına yerleştirilen güvenlik kameralarının ve hareket sensörlerinin odaya izinsiz giren yabancı bir kişiyi kaydetmesi			
6. Şirket ağının dış dünya ile olan sınırına kurulan güvenlik duvarının, gelen zararlı ve şüpheli ağ trafiklerini daha içeri girmeden kapıda bloke etmesi			

5.2.14. Bilgi Güvenliği Standartları

Bilgi güvenliği standartları, kurumların dijital ve fiziksel varlıklarını korumak, riskleri yönetmek ve güvenliği küresel olarak kabul görmüş en iyi uygulamalarla yapılandırmak için rehberlik eder. Bu alanda en çok kabul gören standartlar, ISO (Uluslararası Standartlar Teşkilatı) ve IEC (Uluslararası Elektroteknik Komisyonu) tarafından ortaklaşa yayınlanan standart aileleridir. En temel üç bilgi güvenliği standardı vardır.

ISO 27001 Bilgi Güvenliği Yönetim **Sistemi (BGYS),** organizasyonların güvenlik stratejilerini belirleme, uygulama ve sürekli olarak yapılandırma süreçlerine yön verir. Bu sayede bilgi ve bilgi varlıklarının korunması ile doğru şekilde yönetilmesi güvence altına alınır. Olası tehditleri ortadan kaldırmayı veya zararlarını en aza indirmeyi hedefleyen bu idari süreçte Görsel 5.14'te gösterilen PUKÖ (Planla, Uygula, Kontrol et, Önlem al) modeli, temel metodoloji olarak benimsenmiştir.



Görsel 5.14: PUKÖ modeli

ISO 27002 Bilgi Güvenliği Kontrolleri, ISO 27000 ailesinin bir parçasıdır. Bilgi güvenliği yönetiminde en iyi uygulamaları ve kontrolleri barındıran uluslararası bir standarttır. ISO 27001 ile ayrılmaz bir bütün hâlinde kullanılır. ISO 27001 standardı "Ek A" bölümünde güvenlik kontrollerini yalnızca bir liste olarak sunarken ISO 27002 bu kontrollerin nasıl hayata geçirileceğini detaylandırarak kapsamlı bir kılavuzluk yapar. Kısacası ISO 27001 sistemin temel kurallarını ve şartlarını belirler, ISO 27002 ise bu kuralların nasıl uygulanacağını gösterir. 2022 yılındaki son güncellemesiyle birlikte ISO 27002, 4 ana başlık altında toplanan toplam 93 kontrolden oluşmaktadır (Görsel 5.15).



Görsel 5.15: ISO 27002 kontrolleri

ISO 27032 Siber Güvenlik Kılavuzu, ISO 27000 serisinin bir parçasıdır. Organizasyonların siber güvenlik seviyelerini artırmak amacıyla ISO 27001 ile entegre şekilde kullanılan uluslararası bir standarttır. Bu standart; temelde bilgi güvenliği, ağ ve internet güvenliği ile kritik bilgi altyapılarının korunması alanlarına odaklanarak kurumlara rehberlik sağlar.

SIRA SİZDE

A) Aşağıdaki tabloda sol sütunda kurumsal siber güvenlik süreçlerinde yaşanan senaryolar, sağ sütunda ise bu senaryolarda kılavuz olarak kullanılan ISO Standartları karışık olarak verilmiştir. Her bir senaryonun hangi standartla doğrudan ilişkili olduğunu bularak ilgili harfi parantez içine yazınız.

	Kurumsal Siber Güvenlik Senaryoları / İhtiyaçları	Bilgi Güvenliği Standartları
(....)	**1.** Bir firmanın, internet ağ altyapısını korumak, siber uzaydan gelebilecek karmaşık saldırılara karşı seviyesini artırmak ve kritik bilgi altyapılarını güvenceye almak için özel bir rehbere ihtiyaç duyması.	**A)** ISO 27001 (BGYS)
(....)	**2.** Bir bilgi işlem yöneticisinin, kurum bünyesinde uluslararası geçerliliğe sahip bir Bilgi Güvenliği Yönetim Sistemi kurmak, güvenlik stratejilerini belirlemek ve yasal şartları sağlamak amacıyla PUKÖ modelini devreye alması	**B)** ISO 27002
(....)	**3.** Güvenlik sorumlusunun, şirketteki güçlü parola politikasının ve erişim yetkilendirmelerinin teknik olarak nasıl hayata geçirileceğini 4 ana başlık altındaki 93 kontrolü inceleyerek detaylı bir kılavuz eşliğinde uygulaması	**C)** ISO 27032
		Ç) KVKK

B) ISO 27001 standardının temel metodolojisi olan PUKÖ modeli; Planla, Uygula, Kontrol Et ve Önlem Al aşamalarından oluşan sürekli bir döngüdür. Aşağıda bir kurumun bilgi güvenliği yönetim sistemini kurarken attığı adımlar verilmiştir. Bu adımların PUKÖ modelindeki hangi aşamaya (Planla, Uygula, Kontrol Et, Önlem Al) karşılık geldiğini boşluklara yazınız.

Kurumsal Siber Güvenlik Senaryoları / İhtiyaçları	Karşılık Gelen Aşama
A) Kurumda tespit edilen siber güvenlik risklerini azaltmak için firewall kurulması, MFA (Çok Faktörlü Kimlik Doğrulama) politikasının aktif edilmesi ve personellere siber güvenlik eğitimi verilmesi süreci	(.....)
B) Kurumun korunması gereken tüm dijital / fiziksel varlıklarının listelenmesi, olası tehditlerin belirlenmesi ve risk analizlerinin yapılarak güvenlik politikalarının kağıt üzerinde tasarlanması süreci	(.....)
C) Alınan tüm güvenlik önlemlerinin işe yarayıp yaramadığını görmek amacıyla sızma testleri (pentest) yaptırılması, logların incelenmesi ve iç denetim mekanizmalarıyla sistemin gözden geçirilmesi süreci	(.....)
Ç) Yapılan denetimlerde ve testlerde ortaya çıkan yeni güvenlik açıklarını kapatmak, sistemi daha kararlı hale getirmek ve değişen tehditlere göre politikaları kalıcı olarak güncelleme süreci	(.....)

5.2.15. Uluslararası Siber Güvenlik Çerçeveleri

Uluslararası siber güvenlik çerçeveleri; kurumların dijital varlıklarını korumak, siber riskleri yönetmek ve saldırılara karşı dayanıklı olmak için kullandıkları küresel rehberler ve standartlar bütünüdür. En yaygın kullanılan temel çerçeveler şunlardır:

NIST siber güvenlik çerçevesi (NIST Cybersecurity Framework), ABD Ulusal Standartlar ve Teknoloji Enstitüsü (NIST) imzası taşıyan bu model, kurumların siber alandaki risk durumlarını analiz etmesi ve bu tehditleri minimize etmesi amacıyla yapılandırılmıştır. Stratejik bir yol haritası sunan çerçeve; Tanımlama, Koruma, Algılama, Yanıt ve Kurtarma olmak üzere birbiriyle entegre beş temel boyuttan meydana gelir.

CIS (Center for Internet Security) kontrolleri, Center for Internet Security imzasını taşıyan bu metodoloji, kurumların siber savunma hatlarını güçlendirmek amacıyla hayata geçirebilecekleri önemli tedbirleri sıralar. Söz konusu yönergeler, dijital sistemlerin siber saldırılara karşı yüksek düzeyde direnç kazanmasında kritik bir rol oynar.

ISO/IEC 27000 Standart Ailesi, Uluslararası Standartlar Teşkilatı (ISO) ve Uluslararası Elektroteknik Komisyonu (IEC) tarafından ortaklaşa geliştirilen bu seri, bilgi güvenliği yönetiminde dünya çapındaki en prestijli standarttır.

SIRA SİZDE

Aşağıdaki tabloda sol sütunda kurumlarda siber güvenliği yapılandırmak isteyen yöneticilerin ihtiyaçları, sağ sütunda ise bu ihtiyaçlara cevap veren Küresel Çerçeveler / Standartlar karışık olarak verilmiştir. Doğru eşleştirmeleri yaparak harfleri parantez içine yazınız.

	Kurumsal Siber Güvenlik İhtiyacı	Küresel Çerçeve / Standart
(....)	**1.** Kurumunda dünya çapında en prestijli, denetlenebilir ve sertifikalandırılabilir bütüncül bir Bilgi Güvenliği Yönetim Sistemi (BGYS) kurmak isteyen bir şirketin seçeceği standart ailesi	**A)** NIST Siber Güvenlik Çerçevesi
(....)	**2.** Dijital sistemlerin ve ağ altyapısının siber saldırılara karşı yüksek düzeyde direnç kazanması için doğrudan uygulanabilecek teknik ve pratik önlemleri liste halinde arayan bir uzmanın rehberi	**B)** CIS Kontrolleri
(....)	**3.** Siber olayları sadece engellemeye değil; aynı zamanda siber olay anında nasıl algılama, yanıt ve kurtarma süreçleri yürüteceğine dair 5 boyutlu stratejik bir yol haritası çizmek isteyen kurumun seçimi	**C)** ISO/IEC 27000 Standart Ailesi
		Ç) KVKK

5.2.16. Siber Güvenlik Sertifikasyon Süreçleri

Siber güvenlik sertifika programları, bu alanda kariyer yapmayı hedefleyen veya mevcut yetkinliklerini bir üst seviyeye taşımak isteyen kişilere pratik ve teorik beceriler kazandıran nitelikli eğitim süreçleridir. Bu eğitimler; ağ yapılarının emniyete alınması, sistem açıklarının belirlenmesi, siber tehditlerin bertaraf edilmesi gibi kritik alanlarda profesyoneller yetiştirmeyi amaçlar.

Akademik kurumlar, küresel sertifikasyon otoriteleri ve yetkili eğitim merkezleri tarafından sunulan bu programların ardından adaylar, resmî bir yeterlilik sınavına tabi tutulur. Baraj puanını aşan katılımcılar, iş başvurularında ve kurumsal terfi süreçlerinde kendilerini öne çıkaracak uzmanlık sertifikasına sahip olur.

Sektörün dinamik yapısına bağlı olarak sürekli güncellenen bu programlar arasında seçim yaparken, bireyin teknik altyapısı, ilgi alanları ve kariyer planlaması göz önünde bulundurulmalıdır.

Bilgisayar Ağ Temelleri Sertifika Programı: Ağ mühendisliği ve yönetimi alanında ilerlemek isteyenler ile siber güvenliğe güçlü bir başlangıç yapmayı amaçlayanlar için tasarlanmış temel seviye bir eğitimdir. Müfredat kapsamı şunlardır:

1. **Temel Protokoller ve Modeller:** OSI Referans Mimarisi, TCP/IP Protokol Ailesi ile ağ katmanlarında çalışan servisler (HTTP, HTTPS, FTP, TFTP, DHCP, DNS, SMTP, TCP, UDP, IPv4, IPv6, ETHERNET, WIFI ve PPP)
2. **Ağ Anahtarlama ve Yapılandırma:** Anahtarlama esasları, VLAN mimarisi ve konfigürasyonu, WLAN tasarımı
3. **Yönlendirme Teknikleri:** Statik yönlendirme yöntemleri (Static, Default ve Floating), dinamik yönlendirme protokolleri (OSPF)
4. **Ağ Güvenliği Önlemleri:** Popüler ağ saldırı türleri, Switch Port güvenliği, Dinamik ARP Denetimi (DAI) ve DHCP Snooping (İzleme)
5. **Erişim ve Altyapı Yönetimi:** Standart ve Genişletilmiş Erişim Kontrol Listeleri (ACL), NAT/PAT entegrasyonları
6. **Modern Ağ Teknolojileri:** Ağ yedeklilik sistemleri ve Yazılım Tanımlı Ağlar (SDN)

Siber Güvenlik Temelleri Sertifika Programı: Siber güvenlik dünyasına adım atanlar için genel bir vizyon ve temel savunma mekanizmalarını öğreten, giriş seviyesi uzmanlık kazanımlarına odaklanan bir programdır. Müfredat kapsamı şunlardır:

1. **Bilgi ve Altyapı Güvenliği:** Bilgi ve ağ güvenliği esasları, sanallaştırma teknolojileri, mobil ve bulut bilişim güvenliği, telsiz (kablosuz) ağ mimarileri
2. **Erişim ve Kimlik Denetimi:** Kimlik doğrulama metotları ve erişim kontrol mekanizmaları
3. **Tehdit ve Korunma Teknolojileri:** Güncel siber saldırılar ve tehdit modelleri, zararlı yazılım (malware) türleri
4. **Savunma Sistemleri:** Saldırı Tespit Sistemleri (IDS), Sanal Özel Ağ (VPN) çözümleri ve genel güvenlik uygulamaları
5. **Kriptografi ve İzleme:** Şifreleme biliminin temelleri ile siber olay izleme ve log yönetimi süreçleri

Beyaz Şapkalı Hacker (Etik Hacker) Sertifika Programı: Yasal sınırlar ve bilişim etiği çerçevesinde kalarak kurumsal sistemlerin, ağların ve yazılımların zafiyetlerini tıpkı bir saldırgan gözüyle analiz eden uzmanlar yetiştirmeyi hedefler. Müfredat kapsamı şunlardır:

1. **Keşif ve Sızma Öncesi:** Etik hacker profili, hedef hakkında bilgi toplama (keşif) ve detaylı ağ tarama faaliyetleri
2. **Zafiyet ve Sistem Analizi:** Güvenlik açığı analizleri, sistem ele geçirme (hacking) aşamaları
3. **Saldırı Teknikleri:** Zararlı yazılımlar, ağ trafiği koklama (sniffing), sosyal mühendislik yöntemleri, DoS/DDoS (Servis dışı bırakma) ve oturum çalma (hijacking) atakları
4. **Sistem Atlatma:** Güvenlik duvarları (Firewall), IDS ve Balküpü (Honeypot) tuzaklarını devre dışı bırakma teknikleri
5. **Platform ve Web Tabanlı Ataklar:** Web sunucu ve web uygulaması zafiyetleri, SQL enjeksiyonu, kablosuz ağlar, mobil cihazlar ve IoT (Nesnelerin İnterneti) sistemlerine yönelik saldırılar
6. **Bulut ve Şifreleme:** Bulut bilişim güvenliği ile gelişmiş kriptografi uygulamaları

Siber Olaylara Müdahale Ekibi (SOME) Sertifika Programı: Kurumlarda meydana gelebilecek olası siber krizleri ve ihlalleri planlı bir şekilde kontrol altına alabilecek, ataklara karşı hızlı ve organize aksiyon geliştirebilecek uzmanlar yetiştirir. Müfredat kapsamı şunlardır:

1. **Yönetimsel Süreçler:** Olay müdahale süreçlerinin planlanması, adli bilişim süreçlerine uyumluluk ve olay anındaki ilk yanıt stratejileri
2. **Kategori Bazlı Müdahale Yöntemleri:** Ağ ve altyapı güvenliği ihlalleri, zararlı yazılım bulaşma senaryoları, e-posta ve oltalama (phishing) vakaları, web uygulaması odaklı siber saldırılar, bulut mimarilerindeki veri sızıntıları
3. **İç Tehditler:** Kurum içinden kaynaklanan kasıtlı veya kasıtsız tehlikelerin analizi ve yönetimi

Ofansif Güvenlik Sertifika Programı: Siber güvenlik alanında yetenekli profesyonellerin yetiştirilmesini amaçlayan bir eğitim programıdır. Bu sertifikayı alanlar, bilişim sistemlerine sızma testi yapacak düzeyde bilgi ve yetkinliğe sahip olur. Müfredat kapsamı şunlardır:

1. **Penetrasyon Esasları ve İşletim Sistemi:** Sızma testi metodolojileri, Kali Linux platformu kullanımı ve temel siber araç setleri
2. **Bilgi Toplama ve Tarama:** Pasif ve aktif bilgi toplama teknikleri, sistem zafiyet taramaları
3. **İstismar ve Sızma:** Exploit (istismar kodu) kullanımı, bellek taşırma (Buffer Overflow) saldırıları, dosya transfer yöntemleri
4. **Hedef Odaklı Ataklar:** Web uygulamalarına ve istemci tarafına (client-side) yönelik saldırılar, parola kırma stratejileri
5. **Altyapı ve Atlatma Teknikleri:** Port yönlendirme, tünelleme protokolleri, Metasploit Framework kullanımı ve güvenlik yazılımlarını (Antivirüs vb.) atlatma yöntemleri

Adli Bilişim Uzmanlığı Sertifika Programı: Siber suçlar veya ihlaller sonrasında dijital ortamlardaki delillerin hukuka uygun araçlarla toplanması, incelenmesi ve adli makamlara sunulmak üzere raporlanması süreçlerini kapsayan uzmanlık eğitimidir. Müfredat kapsamı şunlardır:

1. **Hukuk ve Etik Temelleri:** Adli bilişim prensipleri, siber güvenlik kavramları, bilişim etiği ve Türkiye'deki güncel bilişim hukuku mevzuatları
2. **Aktörler ve Tehditler:** Siber saldırgan (hacker) profilleri, hacker türleri, güncel saldırı metotları ve zararlı yazılımlar
3. **Sistemsel Bilgiler:** İşletim sistemlerinin mimari özellikleri ile kimlik doğrulama mekanizmaları.
4. **Teknik İnceleme ve Veri Yönetimi:** Şifreleme ve şifre çözme teknikleri, veri kurtarma, güvenli veri saklama ve kalıcı veri silme işlemleri
5. **Delil Analiz Süreci:** Depolama birimlerinin (disk vb.) adli imajlarının (kopyalarının) alınması, dijital delillerin analizi, çözümlenmesi ve adli süreçlerin işletilmesi
6. **Donanım, Yazılım ve Raporlama:** Adli bilişim laboratuvarlarında kullanılan donanımsal ve yazılımsal araçlar ile mahkemelere sunulacak resmi bilirkişi raporunun hazırlanması

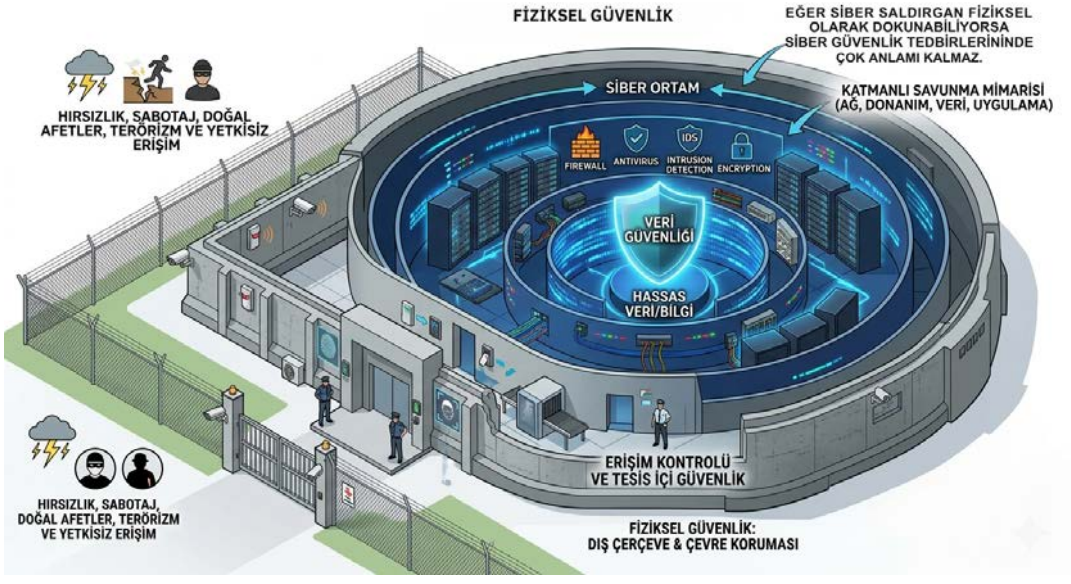
SIRA SİZDE

Aşağıdaki tabloda siber güvenliğe dair 6 farklı gerçek hayat kurumsal senaryosu ve mesleki hedef verilmiştir. İlgili senaryoları ve siber güvenlik rollerini inceleyerek bu durumların hangi sertifika programına karşılık geldiğini bulunuz ve boşluklara yazınız.

Kurumsal Durum / Mesleki Hedef	Sertifika Programı
1. Bir bankanın bilişim alt yapısında çalışacak, ağ katmanındaki OSPF yönlendirme protokollerini yapılandıracak, VLAN mimarisini kuracak ve DHCP Snooping ile ağ güvenliğini sağlayacak bir uzman aranmaktadır.	.....
2. Bir e-ticaret şirketi, bir siber saldırıya uğradıktan sonra delillerin bozulmadan toplanmasını, disklerin adli imajlarının (kopyalarının) alınmasını ve mahkemeye sunulmak üzere resmi bilirkişi raporu hazırlanmasını istemektedir.	.....
3. Bir kamu kurumunda çalışan ve olası bir fidye yazılımı (ransomware) veya oltalama (phishing) krizi anında ilk yanıt stratejilerini uygulayarak etkilenen sistemleri ağdan izole edecek dinamik bir ekip kurulacaktır.	.....
4. Bilişim sektörüne yeni adım atmış bir lise mezunu; sanallaştırma teknolojileri, bulut bilişim esasları, VPN çözümleri ve şifreleme biliminin temelleri hakkında genel bir savunma vizyonu kazanmak istemektedir.	.....
5. Bir siber güvenlik firmasında sızma testi (pentest) uzmanı olarak çalışmak isteyen bir yazılımcı, Kali Linux platformunu derinlemesine öğrenmek, Metasploit Framework kullanmak ve Buffer Overflow (bellek taşırma) açıklarını istismar etmek istemektedir.	.....
6. Bir holding, sistemlerinin güvenliğini test etmek amacıyla yasal sınırlar ve bilişim etiği çerçevesinde kalarak tıpkı bir saldırgan gözüyle web sunucu zafiyetlerini (SQL enjeksiyonu vb.) ve sosyal mühendislik açıklarını bulacak bir uzman istihdam edecektir.	.....

5.3. FİZİKSEL GÜVENLİK

Fiziksel güvenlik; siber ortamın hırsızlık, sabotaj, doğal afetler, terörizm, yetkisiz erişim gibi fiziksel tehditlere karşı koruma sürecidir. Siber saldırgan, bilişim sistemleri, ağlar, donanımlar ve verilerin bulunduğu ortama fiziksel olarak dokunabiliyorsa siber güvenlik tedbirlerinizin çok bir anlamı kalmamış demektir. Siber ortamı korumak için katmanlı bir savunma mimarisi uygulanır. Güvenlik önlemleri dış çerçeveden başlar ve en içteki veriye kadar uzanır (Görsel 5.16).



Görsel 5.16: Fiziksel güvenlik

5.3.1. Erişim Kontrol Sistemleri (Kayıt ve Yetkilendirme)

Erişim kontrol sistemleri, siber ortama veya kritik bilişim sistemlerine yetkisiz kişilerin fiziksel olarak erişmesini engellemek amacıyla alınan tedbirleri ifade eder. Bu tedbirlerden bazıları şunlardır:

- **Biyometrik Sistemler:** Parmak izi, yüz tanıma veya retina tarayıcılar gibi aldatılması zor olan kişisel doğrulama yöntemleri kullanılır.
- **Akıllı Kartlar ve PIN:** Siber ortamda çalışanların ünvanına ve yetkisine göre programlanmış RFID kartlar ve şifreli kapılar kullanılır.
- **Giriş-Çıkış Günlükleri (Loglama):** Siber ortama kimin, hangi gün ve saatte girdiğinin dijital olarak kayıt altına alınmasıdır.

5.3.2. Çevre Güvenliği

Çevre güvenliği, siber ortam çevresinin **güvenli** hâle getirilmesini ifade eder. Yetkisiz kişinin hedef cihaza ulaşmasını engelleyen ilk savunma hattıdır. **Çevre güvenliği için önemli unsurlardan bazıları şunlardır:**

- Güçlü kapı ve pencereler
- Kilitli kabinetler
- Güvenlik çitleri
- Nem ve sıcaklık kontrolü

5.3.3. Kamera ve İzleme Sistemleri (CCTV)

Kamera ve izleme sistemleri, siber ortamın sürekli izlenmesini ve kaydedilmesini sağlar. Bunun için dikkate alınması gereken bazı unsurlar şunlardır:

- **Kesintisiz Kayıt:** Kameralar siber ortamın girişini, içini ve koridorları kör nokta kalmayacak şekilde izlemesidir.
- **Hareket Sensörleri:** Mesai saatleri dışında veya ıssız alanlarda hareket algılandığında güvenlik personeline alarm gönderen sistemler entegre edilmelidir.

5.3.4. Yangın, Sel ve Çevresel Önlemler

Siber ortamlar sadece insanlardan değil doğadan ve çevre şartlarından da korunması gerekir. Bunun için dikkate alınması gereken bazı unsurlar şunlardır:

- **Yangın Söndürme Sistemleri:** Siber ortamlarda su bazlı söndürme yerine oksijeni azaltarak donanımlara zarar vermeyen gazlı sistemler kullanılır.
- **İklimlendirme:** Siber ortamlarda donanımların aşırı ısınması, özellikle sunucularda performans kaybına ve donanım arızalarına neden olabilir. Bu sebeple ortam sıcaklığını ve nem oranını sabit tutan endüstriyel klimalar kullanılır.
- **Yükseltilmiş Taban:** Kabloların zeminden geçerek karmaşa yaratmasını önlemek ve olası bir su sızıntısında cihazların ıslanmasını engellemek için zemin yükseltilir.

5.3.5. Enerji Güvenliği

Elektriksel dalgalanmalar veya kesintiler donanımlara fiziksel olarak zarar verebilir ve veri kaybına yol açar. Bunun için dikkate alınması gereken bazı unsurlar şunlardır:

- **Kesintisiz Güç Kaynakları (UPS):** Elektrik kesildiği anda sistemlerin kapanmasını önleyerek aküler üzerinden besleme sağlar.
- **Jeneratörler:** Uzun süreli elektrik kesintilerinde devreye girerek sistem odasının ve güvenlik kameralarının çalışmaya devam etmesini sağlar.

SIRA SİZDE

A) Aşağıda bir bilgi işlem merkezinde yaşanabilecek olası risk durumları ve siber güvenlik zafiyetleri verilmiştir. Bu riskleri sıfıra indirmek veya engellemek için hangi fiziksel güvenlik alt başlığındaki (Erişim Kontrolü, Çevre Güvenliği, CCTV, Çevresel Önlemler ve Enerji Güvenliği) tedbirlerin devreye alınması gerektiğini karşılarındaki boşluklara yazınız.

Yaşanan Fiziksel Risk / Zafiyet Durumu	Alınması Gereken Fiziksel Güvenlik Tedbiri
1. Şehir şebekesinde meydana gelen ani bir voltaj dalgalanması sebebiyle ana omurga anahtarının (switch) yanması veya elektriğin kesilmesiyle veri tabanının zarar görmesi	.....
2. Binadaki ana su borusunun patlaması sonucu sistem odasının tabanını su basması ve yerde duran yedekleme ünitelerinin kısa devre yaparak kullanılmaz hâle gelmesi	.....

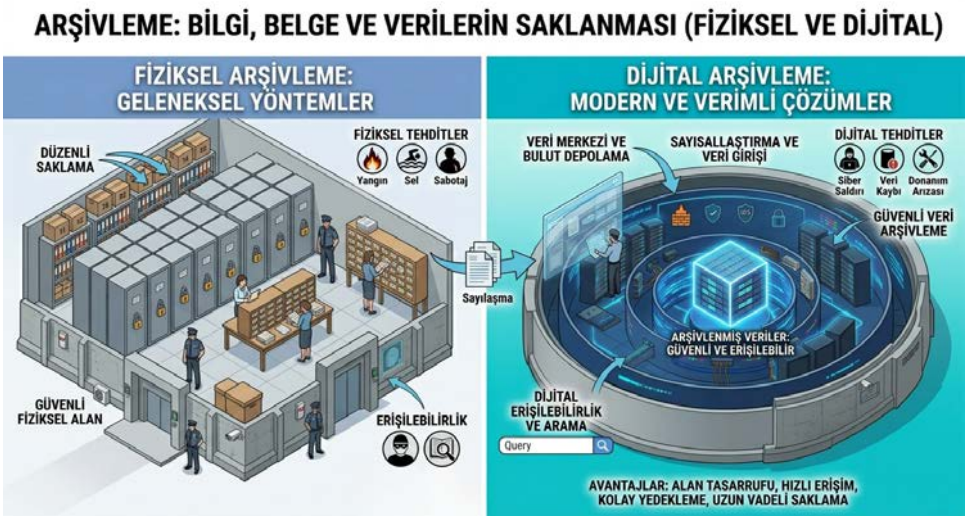
Yaşanan Fiziksel Risk / Zafiyet Durumu	Alınması Gereken Fiziksel Güvenlik Tedbiri
3. Eski personelin işten ayrılmasına rağmen elindeki eski giriş kartını turnikeye okutarak hiçbir engele takılmadan doğrudan sunucu odasına kadar yürüyebilmesi	.....
4. Sistem odasına giriş yapan kişilerin kimlik doğrulaması yapılmadığından, yetkisiz kişilerin sunuculara fiziksel olarak erişebilmesi ve donanımlara müdahale edebilmesi	.....
5. Sistem odasındaki sunucuların (server) yaz aylarında aşırı yük altında çalışırken ortamın havalandırılamaması nedeniyle aşırı ısınması ve işlemcilerin yanarak sistemin çökmesi	.....

B) Aşağıdaki yanıtlı soruları teknik gerekçeleri dikkate alarak kendi cümlelerinizle cevaplandırınız.

1. Sistem odalarında çıkan bir yangında neden okul koridorlarındaki gibi su bazlı otomatik fıskiyeler yerine gazlı söndürme sistemleri tercih edilmelidir? Gerekçesini açıklayınız.
Cevap:
2. Bir kurumda sadece "Kesintisiz Güç Kaynağı (UPS)" kullanılması uzun süreli elektrik kesintilerinde (örneğin 1-2 gün süren büyük arızalarda) neden tek başına yeterli olmaz? Yanına hangi fiziksel donanımın eklenmesi gerekir?
Cevap:

5.4. DİJİTAL ARŞİVLEME

Arşivleme; bilgi, belge ve verilerin düzenli, güvenli ve erişilebilir bir şekilde saklanma işlemidir. Arşivleme saklandığı ortama göre ikiye ayrılır (Görsel 5.17).



Görsel 5.17: Fiziksel arşivleme ve dijital arşivleme

Fiziksel arşivleme; kâğıt, mikrofilm, harita veya fotoğraf gibi somut belgelerin raf, dolap vb. ortamlarda saklanmasıdır. **Dijital arşivleme**, somut belgelerin tarayıcılar aracılığıyla dijital dosya formatlarına çevrilerek saklanmasıdır. Her iki arşivleme yönteminin kendine has avantajları ve dezavantajları vardır (Tablo 5.4).

Tablo 5.4: Fiziksel ve Dijital Arşivleme

Fiziksel Arşivleme	Dijital Arşivleme
Avantajları	
Elektrik olmadan kullanılabilir.	Daha az fiziksel alan kullanır.
Orijinal belgeler korunur.	Belgelere hızlı erişim sağlar.
Kullanımı basittir.	Kolay yedekleme yapılır.
Siber risklerlerden uzaktır.	Belgeler hızlı paylaşılır.
	Arama işlemleri kolaydır.
	Uzaktan erişim imkânı sağlar.
Dezavantajları	
Çok yer kaplar.	Siber saldırı riski vardır.
Belge aramak zaman alır.	Elektrik ve internet bağımlılığı olabilir.
Yangın, sel ve yıpranma riski vardır.	Sistem arızalarında veri kaybı yaşanabilir.
Kopyalama ve paylaşım zordur.	Güvenlik önlemleri gerektirir.
Belgeler kaybolabilir.	Teknik bilgi gerektirebilir.

Dijital arşivlemede belgeler elektronik ortama aktarılırken şu aşamalardan geçer:

Tarama (Dijitalleştirme): Fiziksel belgeler tarayıcılar aracılığıyla dijital dosya formatlarına dönüştürülür. Bu aşamada belgenin okunabilir ve kaliteli olması önemlidir.

İndeksleme: Fiziksel belgelerin dijital ortama aktarılmasından sonra kolay bulunabilmesi için etiketlenmesi ve sınıflandırılması işlemidir.

Depolama: Dijital ortama aktarılmış belgelerin sunucularda, bulut sistemlerinde saklanması sürecidir. Düzenli bir klasör yapısıyla veritabanlarında bu belgeler depolanmış olur.

Yedekleme: Dijital belgelerde siber saldırılarda veya beklenmeyen durumlarda veri kaybı olmaması için oluşturulan kopyalarının farklı ortamlarda tutulma işlemidir.

Erişim Kontrolü: Dijital belgelere kimlerin erişebileceğinin, kullanıcı adı, parola ve yetki seviyesinin belirlendiği aşamadır.

Güvenlik Önlemleri: Siber güvenlik politikalarına uygun olarak antivirus yazılımları, şifreleme ve güvenlik duvarı **işlemlerinin gerçekleştiği aşamadır.**

SIRA SİZDE

Aşağıda bir kurumun arşiv yöneticisinin karşı karşıya kaldığı 4 farklı operasyonel durum veya ihtiyaç verilmiştir. Verilerinden ve bilgilerden hareketle bu durumlara en uygun çözümün Fiziksel Arşivleme mi yoksa Dijital Arşivleme mi olduğunu belirleyerek karşılarındaki boşluğa yazınız ve tercihinizin temel avantaj-dezavantaj gerekçesini kısaca belirtiniz.

1. Durum: Kurumun Ankara, İstanbul ve İzmir şubelerinde çalışan proje yöneticilerinin, aynı teknik şartname belgesine aynı anda ulaşıp inceleme ve üzerinde hızlıca geri bildirim verme ihtiyacı
En Uygun Yöntem: ..... **Nedeni:**.....
2. Durum: Deprem riski yüksek bir bölgede bulunan resmi bir dairenin, tarihi el yazması beratları ve ıslak imzalı orijinal tapu senetlerini biyolojik yıpranmaya ve doğal afetlere karşı koruma altına alma zorunluluğu
En Uygun Yöntem: ..... **Nedeni:**.....
3. Durum: Kurumun bodrum katındaki geniş bir odada saklanan binlerce klasörlük eski personel özlük dosyaları arasında, 10 yıl önce işten ayrılmış bir çalışanın maaş bordrosunun acilen bulunması gerekmesi
En Uygun Yöntem: ..... **Nedeni:**.....
4. Durum: Bölgede yaşanan çok büyük ve uzun süreli bir enerji altyapısı arızası ile internet kesintisi sırasında, kurum içindeki temel çalışma talimatlarına acilen göz atılması ihtiyacı
En Uygun Yöntem: ..... **Nedeni:**.....

ÖLÇME VE DEĞERLENDİRME

A) Aşağıda verilen tanımlar ve bunların karşıladığı kavramları uygun harfleri kavramın önündeki parantezin içine yazarak eşleştiriniz.

1.

Kavram	Tanım
1. ( ) Siyah Şapkalı Hacker	A) Ulusal veya uluslararası düzeyde telif haklarını, sinema, müzik ve yazılımları koruyan kanundur.
2. ( ) Beyaz Şapkalı Hacker	B) İyi niyetli olan, bulduğu açıkları sisteme zarar vermeden kapatılması için kuruma bildiren güvenlik uzmanıdır.
3. ( ) FSEK (Fikir ve Sanat Eserleri Kanunu)	C) Yasaları çiğneyerek tamamen kişisel çıkar, maddi kazanç veya zarar verme motivasyonuyla siber saldırı gerçekleştiren kişidir.
4. ( ) TCK 243 (Türk Ceza Kanunu)	Ç) Bir bilişim sistemine yetkisiz olarak girme ve orada kalma suçunu düzenleyen kanun maddesidir.
	D) Kurumların dijital varlıklarını korumak, siber riskleri yönetmek ve saldırılara karşı dayanıklı olmak için kullandıkları küresel rehberler ve standartlar bütünüdür.

2.

Kavram	Tanım
1. ( ) Varlık	A) Dijital arşivlemede belgelerin gelecekte kolayca aranıp bulunabilmesi için etiketlenmesi ve sınıflandırılması adımıdır.
2. ( ) Tehdit	B) Kuruma veya sistemlere zarar verme potansiyeli olan her türlü unsur veya saldırgandır.
3. ( ) Zafiyet	C) Kurum için değeri olan ve korunması gereken her türlü veri, donanım, yazılım veya insan kaynağıdır.
4. ( ) Risk	Ç) Tehditlerin sistemdeki açıklıkları kullanarak kuruma zarar verme olasılığı ve bu zararın yaratacağı etkidir.
5. ( ) İndeksleme	D) Önleyici ve tespit edici kontrollere rağmen meydana gelen bir siber olayın etkilerini gidermek için uygulanan (örn: yedekten dönme) kontroldür.
6. ( ) Düzeltici Kontrol	E) Sistemlerde bulunan, saldırganların sızmasına zemin hazırlayan güvenlik açığı veya zayıflıktır.
	F) Fiziksel belgeler tarayıcılar aracılığıyla dijital dosya formatlarına dönüştürülmesidir.

B) Aşağıdaki soruların doğru cevabını işaretleyiniz.

1. **Türkiye'de kişisel verilerin korunmasını amaçlayan ve siber güvenlik uzmanlarının teknik önlemleri alırken uymakla yükümlü olduğu temel yasal mevzuat aşağıdakilerden hangisidir?**

A) FSEK
B) TCK 243
C) KVKK
D) GDPR
E) ISO 27001

2. **Bilgi güvenliğinde verinin yetkisiz kişilerin eline geçmesini engellemeyi (Gizlilik), izinsiz değiştirilmesini önlemeyi (Bütünlük) ve ihtiyaç duyulduğunda hazır olmasını (Erişilebilirlik) ifade eden üçlü model aşağıdakilerden hangisidir?**

A) Cyber Kill Chain
B) MITRE ATT&CK
C) CIA Üçlüsü
D) D3FEND Framework
E) Risk Matrisi

3. **Bir sisteme sızmak amacıyla herhangi bir zafiyet aramadan, tamamen insan ilişkilerini, manipülasyonu ve güveni suistimal ederek yetkisiz erişim sağlama yöntemine ne ad verilir?**

A) Zero Day Saldırısı
B) Sosyal Mühendislik
C) APT Saldırısı
D) Brute Force
E) Ransomware

4. **Yazılım üreticisi dâhil hiç kimse tarafından henüz fark edilmemiş ve yaması yayınlanmamış güvenlik açıklarını kullanan tehlikeli siber saldırı türü aşağıdakilerden hangisidir?**

A) Dosya Silme
B) Zero Day (Sıfırıncı Gün)
C) Phishing
D) Man-in-the-Middle
E) DDOS

5. **Siber güvenlik takımlarından, sistemlerin savunmasını yapan, logları inceleyen ve tehditleri tespit edip engelleyen "Savunma (Defensive)" odaklı takım aşağıdakilerden hangisidir?**

A) Kırmızı Takım
B) Mor Takım
C) Beyaz Şapkalı Takım
D) Mavi Takım
E) Gri Şapkalı Takım

6. **Saldırganların bir kuruma sızmak için kullandıkları taktik, teknik ve prosedürleri (TTP) listeleyen, siber tehdit istihbaratında küresel standart olarak kullanılan bilgi tabanı çerçevesi aşağıdakilerden hangisidir?**

A) ISO/IEC 27032
B) Cyber Kill Chain
C) MITRE ATT&CK
D) GDPR
E) FSEK

7. **Kurumun siber güvenlik risklerini azaltmak amacıyla veri merkezinin girişine biyometrik (parmak izi / yüz tanıma) sistemler kurulması ve yangın söndürme sistemlerinin yenilenmesi hangi güvenlik kontrolü türüne girer?**

A) Fiziksel
B) Mantıksal
C) Düzeltici
D) İdari
E) Dijital

8. **Bir dosyanın iletim veya depolama sırasında değişip değişmediğini, bütünlüğünün bozulup bozulmadığını kontrol etmek için aşağıdaki matematiksel değerlerden hangisi karşılaştırılır?**

A) Parola Karmaşıklığı
B) Kriptografik Hash (Özet) Değeri
C) IP Adresi
D) Port Numarası
E) Dijital Sertifika

9. **Devlet destekli olan, belirli bir hedefi uzun süre boyunca fark ettirmeden izleyen ve sistemlerden veri sızdıran gelişmiş organize tehdit aktörlerine ne ad verilir?**

A) Siyah Şapkalı Hacker
B) Gri Şapkalı Hacker
C) APT (Gelişmiş Sürekli Tehdit) Grupları
D) Siber Zorbalar
E) Betik Amatörler

10. Kurumların bilgi güvenliği yönetim sistemini (BGYS) kurması, yönetmesi ve uluslararası standartlara uygun olarak belgelendirmesi için uyması gereken temel ISO standardı hangisidir?

A) ISO 9001
B) ISO 14001
C) ISO/IEC 27001
D) ISO/IEC 27032
E) ISO 22301

C) 1, 2 ve 3. soruları aşağıdaki senaryoya göre cevaplayınız.

Senaryo

Bir e-ticaret firması, müşteri verilerinin güvenliğini artırmak ve yeni yasal mevzuatlara uyum sağlamak amacıyla altyapısını gözden geçirmektedir. Firma bünyesinde hassas kişisel veriler barındıran bir veri tabanı sunucusu bulunmakta, fiziksel arşivler dijital ortama aktarılmakta ve sisteme sızma testleri (pen-test) planlanmaktadır.

1. Firmanın müşteri verilerini barındırdığı ana sunucunun donanımsal arıza yapması veya bir fidye yazılımı (ransomware) tarafından şifrelenmesi, Bilgi Güvenliğinin temel ilkelerinden (Gizlilik, Bütünlük, Erişilebilirlik) hangisini doğrudan ihlal eder? Gerekçenizi yazınız.

.....
.....
.....

2. Firmanın bu süreçte fiziki ortamda tuttuğu eski fatura ve müşteri formlarını dijital arşivleme adımlarına uygun olarak sisteme aktarması planlanmaktadır. Dijital arşivleme sürecinin veri güvenliği ve operasyonel verimlilik açısından sağladığı temel avantajları açıklayınız.

.....
.....
.....

3. Firma siber güvenlik duruşunu test etmek için haricî bir siber güvenlik firmasıyla anlaşmıştır. Bu firmanın yapacağı "Zafiyet Testi (Vulnerability Assessment)" ile "Sızma Testi (Pentest)" arasındaki temel fark nedir? Kısaca yorumlayınız.

.....
.....
.....

6. ÖĞRENME BİRİMİ

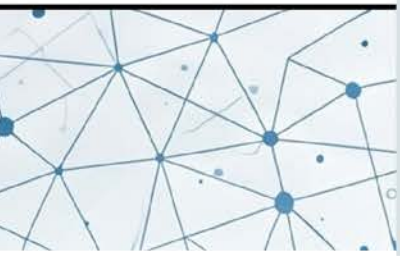
KRİPTOGRAFİ











KONULAR

6.1. KRİPTOLOJİ TEMELLERİ
6.2. KLASİK KRİPTOGRAFİ
6.3. ÖZET FONKSİYONLARI
6.4. SİMETRİK KRİPTOGRAFİ
6.5. ASİMETRİK KRİPTOGRAFİ
6.6. DİJİTAL İMZA VE SERTİFİKALAR
6.7. VERİ GİZLEME

ANAHTAR KAVRAMLAR

- AES
- anahtar
- Base64
- bcrypt
- Diffie-Hellman
- dijital imza
- dijital sertifika
- encoding
- frekans analizi
- hash
- kriptanaliz
- kriptografi
- RSA
- salt
- Sezar şifreleme
- steganografi
- SSL/TLS
- steghide
- şifreleme
- Vernam Cipher
- Vigenere

Bu öğrenme biriminde sizden

- kriptografi ve kriptanaliz kavramlarını açıklamanız
- kodlama ile şifreleme arasındaki farkı ayırt etmeniz
- klasik kriptografi yöntemlerini uygulamanız
- hash ve salting mantığını açıklamanız
- simetrik ve asimetrik kriptografi uygulamalarını gerçekleştirmeniz
- dijital imza ve dijital sertifikaların işleyişini analiz etmeniz
- steganografi araçlarıyla test verisi gizleme ve çıkarma uygulaması yapmanız

beklenmektedir.

HAZIRLIK ÇALIŞMASI

Aşağıda dijital ortamda karşılaşılabilecek bir metin verilmiştir.

Bir öğrenci, arkadaşının gönderdiği bağlantıya tıklayarak bir dosya indirmek ister. Bağlantının açıldığı web sitesinde kilit simgesi bulunduğunu görür. Aynı gün kullandığı bir çevrim içi araç, dosyasını kontrol edebilmek için yüklemesini ve hesap parolasını girmesini ister. Öğrenci, işlem yapmadan önce nelere dikkat etmesi gerektiğini düşünür.

Verilen metne göre aşağıdaki soruları cevaplayınız.

1. Siz bu öğrencinin yerinde olsaydınız işlem yapmadan önce nelere dikkat ederdiniz?

   .....

2. Bir web sitesinde kilit simgesi görmeniz, siteyle ilgili kararınızı nasıl etkiler? Düşüncenizi açıklayınız.

   .....

3. Bir çevrim içi araç sizden parolanızı veya özel bir dosyanızı isterse nasıl davranırsınız? Neden?

   .....

4. Dijital ortamda paylaştığınız dosyaları ve bilgileri korumak için günlük hayatınızda hangi önlemleri alıyorsunuz?

   .....

BAŞLARKEN

Günlük yaşamda arkadaşlarla mesajlaşma, web sitelerine giriş, dosya indirme, hesaplar için parola oluşturma, bazı belgeleri elektronik ortamda onaylama gibi birçok işlem dijital ortamda yapılır. Bu işlemler sırasında bilgilerin korunması, dosyaların değiştirilip değiştirilmediğinin anlaşılması ve işlem yapan kişinin doğrulanması önemlidir. Bu noktada devreye kriptografi kavramı girer. Bu öğrenme biriminde kriptografinin temel kavramlarından steganografi ile veri gizleme uygulamalarına kadar birçok konu incelenecektir.

6.1. KRİPTOLOJİ TEMELLERİ

Kriptografi; bilginin gizliliğini korumak, değiştirilip değiştirilmediğini kontrol etmek, kimlik doğrulamaya yardımcı olmak ve inkâr edilemezliği desteklemek için kullanılan yöntemleri inceleyen alandır. Kriptografi denildiğinde akla ilk olarak şifreleme gelir. Bir mesajı herkesin okuyabileceği açık hâlinden çıkarıp yalnızca yetkili kişinin anlayabileceği bir biçime dönüştürme işlemine şifreleme denir. Şifrelenmiş mesajın tekrar okunabilir hâle getirilmesine ise şifre çözme denir. Örneğin MERHABA kelimesi herkes tarafından okunabilen bir bilgidir. Bu bilgi belirli bir kurala ve anahtara göre değiştirilirse dışarıdan bakan kişi, mesajın ne olduğunu anlayamaz. Mesajı tekrar anlamlı hâle getirmek için kullanılan kuralın veya anahtarın bilinmesi gerekir.

Kriptografi yalnızca şifreleme işleminden oluşmaz. Kriptografide kullanılan bazı temel kavramlar Tablo 6.1'de görülür.

Tablo 6.1: Kriptografide Temel Kavramlar

Kavram	Açıklama
Düz metin (Plaintext/Cleartext)	Şifrelenmeden önceki okunabilir mesajdır.
Şifreli metin (Ciphertext)	Şifreleme işleminden sonra oluşan, doğrudan okunamayan mesajdır.
Anahtar (Key)	Şifreleme veya şifre çözme işleminde kullanılan özel bilgidir.
Şifreleme (Encryption)	Düz metni şifreli metne dönüştürme işlemidir.
Şifre çözme (Decryption)	Şifreli metni tekrar düz metne dönüştürme işlemidir.

Kriptografi, Tablo 6.2'de görülen farklı güvenlik amaçları için kullanılabilir.

Tablo 6.2: Kriptografinin Desteklediği Güvenlik Amaçları

Kriptografinin Desteklediği Güvenlik Amacı	Anlamı	Günlük Yaşam Örneği
Gizlilik	Bilginin yalnızca yetkili kişiler tarafından okunabilmesidir.	Bir mesajın sadece alıcı tarafından okunması
Bütünlük	Bilginin değiştirilip değiştirilmediğinin anlaşılabilmesidir.	İndirilen bir dosyanın hash değeriyle kontrol edilmesi
Kimlik doğrulama	Bir kişinin, cihazın veya web sitesinin gerçekten iddia ettiği kişi ya da sistem olduğunun kontrol edilmesidir.	Bir web sitesinin sertifika bilgisiyle doğrulanması
İnkâr edilemezlik	Bir işlemi yapan kişinin daha sonra bu işlemi yaptığını reddetmesini zorlaştıran güvenlik özelliğidir.	Dijital imzalı bir belgenin kimin tarafından imzalandığının doğrulanması

Web sitelerinde görülen kilit simgesi genellikle bağlantının HTTPS ile şifrelendiğini gösterir. Bu durum, tarayıcı ile web sitesi arasındaki veri iletiminin başkaları tarafından okunmasını zorlaştırır ancak kilit simgesi, web sitesinin tamamen güvenilir olduğunu tek başına kanıtlamaz. Bir site HTTPS kullanıyor olsa bile sahte, yanıltıcı veya zararlı içerik barındırabilir. Bu nedenle web adresi, site içeriği ve işlem yapılan sayfanın güvenilirliği ayrıca dikkatle kontrol edilmelidir. Parola güvenliği de kriptografiyle yakından ilişkilidir ancak parolaların güvenli saklanması, doğrudan parolayı şifreleyip saklamak şeklinde düşünülmemelidir. Parolaların sistemlerde nasıl daha güvenli saklanabileceğini anlamak için hashleme ve salting kavramlarının bilinmesi gerekir.

Kriptografi ile kullanılan bir diğer kavram da kriptanalizdir. **Kriptanaliz**, şifreli bilgiyi çözmeye veya kullanılan şifreleme yönteminin zayıf yönlerini bulmaya yönelik çalışmaları ifade eder. Kriptografi bilgiyi korumaya çalışırken kriptanaliz, bu korumanın ne kadar güçlü olduğunu anlamaya çalışır.

Düz metinden şifreli metne dönüşüm süreci Görsel 6.1'de gösterilmiştir.



Görsel 6.1: Düz metinden şifreli metne dönüşüm süreci

SIRA SİZDE

Aşağıdaki durumları okuyunuz. Her durumun hangi kriptografi amacıyla ilişkili olduğunu belirleyiniz. Tabloda yer alan **İlgili Kriptografi Amacı** sütununa uygun amacı, **Gerekçe** sütununa ise seçiminizin nedenini yazınız.

Cevaplarınızı tamamladıktan sonra sınıfta arkadaşlarınızla karşılaştırınız.

Bu çalışmada kullanacağınız kriptografi amaçları şunlardır: **gizlilik, bütünlük, kimlik doğrulama, inkâr edilemezlik**. Bu kavramlar, tablodaki durumları eşleştirmek için verilen cevap seçenekleridir. Her kavramı yalnızca bir durum için kullanınız.

No.	Durum	İlgili Kriptografi Amacı	Gerekçe
1	Bir arkadaşınıza yalnızca onun okuyabilmesini istediğiniz özel bir mesaj göndermek istiyorsunuz.		
2	Öğretmeninizin gönderdiği dosyanın sonradan değiştirilip değiştirilmediğini kontrol etmek istiyorsunuz.		
3	İnternet üzerinden işlem yapacağınız web sitesinin gerçekten ilgili kuruma ait olup olmadığını kontrol etmek istiyorsunuz.		
4	Elektronik ortamda onaylanan bir belgenin daha sonra işlemi yapan kişi tarafından reddedilmesini zorlaştırmak istiyorsunuz.		

6.1.1. Kriptografi, Kriptanaliz ve Kodlama

Kriptografiyle birlikte kriptanaliz, kodlama, Base64 ve frekans analizi kavramlarının bilinmesi, şifreleme yöntemlerini anlamak ve basit şifre çözme işlemlerine hazırlık yapmak için önemlidir.

Kriptografi, bilgiyi korumak için kullanılan yöntemleri inceler. Bir mesajın yetkisiz kişiler tarafından okunmasını zorlaştırmak, verinin değiştirilip değiştirilmediğini kontrol etmek ve dijital ortamda güven sağlamak kriptografinin çalışma alanına girer. Kriptanaliz ise kullanılan şifreleme yöntemlerini inceleyerek bu yöntemlerin güçlü

ve zayıf yönlerini anlamaya çalışır. Kriptanaliz yalnızca kötü niyetli saldırılarla ilişkili değildir. Güvenlik uzmanları da bir şifreleme yönteminin ne kadar dayanıklı olduğunu anlamak için kriptanalizden yararlanır.

Kriptografi, sağlam bir kilit tasarlamaya benzer. Kriptanaliz ise bu kilidin hangi durumlarda açılabileceğini ve zayıf bir noktası olup olmadığını incelemeye benzer. Şifreleme, okunabilir durumdaki düz metnin bir anahtar veya belirli bir kurala göre şifreli metne dönüştürülmesi işlemidir. Şifre çözme ise şifreli metnin uygun anahtar veya yöntem kullanılarak yeniden anlamlı ve okunabilir hâle getirilmesidir. Böylece kriptografi bilgiyi korumaya yönelik genel yaklaşımı ifade ederken şifreleme ve şifre çözme bu yaklaşımın temel işlem basamaklarını oluşturur.

Kriptografinin Tarihî Örnekleri

İnsanlar tarih boyunca askerî, diplomatik ve resmî yazışmalarda bilgiyi gizlemek için farklı yöntemler kullanmıştır. Bunlardan bazıları şunlardır:

Sezar Şifresi: Harflerin belirli bir sayı kadar kaydırılması mantığına dayanır. Örneğin bir harf yerine alfabede ondan sonra gelen başka bir harf yazılır. Bu yöntem, klasik şifreleme örneklerinden biridir.

El-Kindî: Kriptanaliz tarihinde önemli bir isimdir. Harflerin bir dilde farklı sıklıklarla kullanıldığını fark etmiş ve bu bilgiden yararlanarak şifreli metinleri çözmeye yönelik çalışmalar yapmıştır. Bu yaklaşım, **frekans analizi** olarak bilinen yöntemin temelini oluşturur.

İbn Adlan: Şifreli metinlerin çözümlenmesiyle ilgilenen tarihî isimlerdendir. Onun çalışmaları, şifreli metinlerdeki örüntüleri fark etmenin ve dil özelliklerini kullanmanın önemini gösterir.

Osmanlı Şifre Kalemi: Osmanlı Devleti'nde resmî ve diplomatik yazışmaların güvenliği için şifreli haberleşmeden yararlanılmıştır. Bu amaçla şifreleme ve şifre çözme işleriyle ilgilenen birimler oluşturulmuştur. Osmanlı Şifre Kalemi, bu tarihî uygulamalara örnek olarak verilebilir.

SIRA SİZDE

Aşağıdaki açıklamaları okuyunuz. Her açıklamanın hangi tarihî örnekle ilişkili olduğunu belirleyiniz. Tabloda yer alan **İlgili Tarihî Örnek** sütununa uygun cevabı yazınız. Cevaplarınızı tamamladıktan sonra sınıfta arkadaşlarınızla karşılaştırınız.

Bu çalışmada kullanacağınız tarihî örnekler şunlardır: **Sezar Şifresi, El-Kindî, İbn Adlan, Osmanlı Şifre Kalemi**. Bu ifadeler, tablodaki açıklamaları eşleştirmek için verilen cevap seçenekleridir. Her ifadeyi yalnızca bir açıklama için kullanınız.

No.	Açıklama	İlgili Tarihî Örnek
1	Harflerin belirli bir sayı kadar kaydırılması mantığına dayanan klasik şifreleme yöntemidir.	
2	Harflerin kullanım sıklığından yararlanarak şifreli metinleri çözmeye yönelik çalışmalar yapmıştır.	
3	Şifreli metinlerdeki örüntülerin ve dil özelliklerinin çözüm sürecindeki önemini gösteren çalışmalar yapmıştır.	
4	Resmî ve diplomatik yazışmaların güvenliği amacıyla şifreleme ve şifre çözme işleriyle ilişkilidir.	

Encoding

Encoding, Türkçede genellikle **kodlama** olarak ifade edilir. **Kodlama**, verinin başka bir gösterim biçimine dönüştürülmesidir. Amaç, veriyi gizlemek değil verinin farklı sistemlerde uygun biçimde taşınmasını, saklanmasını veya gösterilmesini sağlamaktır. Bu nedenle encoding ile şifreleme aynı şekilde değerlendirilmemelidir. Şifreleme, bilgiyi yetkisiz kişilerin anlamasını zorlaştırmayı amaçlar. Kodlama ise verinin biçimini değiştirir ancak çoğu durumda kodlanan veri kolayca geri dönüştürülebilir. Örneğin bir metni **Base64** biçimine dönüştürmek, o metni güvenli hâle getirmez. Sadece metnin farklı bir veri gösterimiyle yazılmasını sağlar. Encoding ve şifreleme kavramlarının karşılaştırması Tablo 6.3'te görülür.

Tablo 6.3: Encoding ve Şifreleme Karşılaştırması

Özellik	Encoding / Kodlama	Şifreleme
Temel amaç	Veriyi farklı biçimde temsil etmektir.	Bilgiyi yetkisiz kişilerden korumak
Gizlilik sağlar mı?	Genellikle sağlamaz.	Doğru yöntem ve anahtarla sağlayabilir.
Anahtar gerekir mi?	Genellikle gerekmez.	Çoğu şifreleme yönteminde gerekir.
Geri dönüştürme	Kolayca yapılabilir.	Anahtar veya yöntem bilinmeden zordur.
Örnek	Base64, URL Encoding	Sezar, AES, RSA gibi şifreleme yöntemleri

Base64 Çalışma Mantığı

Base64, veriyi gizlemek için değil veriyi farklı karakterlerle temsil etmek için kullanılan bir kodlama yöntemidir. Bu nedenle Base64 bir şifreleme yöntemi değildir. Base64 işleminde gizli anahtar kullanılmaz ve kodlanan veri uygun bir Base64 çözme aracıyla tekrar eski hâline dönüştürülebilir. Bilgisayarlar; harfleri, sayıları ve sembolleri doğrudan insanın gördüğü biçimde saklamaz. Her karakter bilgisayar içinde belirli bir sayısal kodla temsil edilir. Bu kodlama sistemlerinden biri **ASCII**'dir. ASCII, özellikle İngilizce harfler, rakamlar ve bazı semboller için kullanılan temel karakter kodlama sistemlerinden biridir. Örneğin ASCII tablosunda büyük "O" harfinin sayısal karşılığı 79'dur. Bu sayı bilgisayarda 8 bitlik ikilik değerle gösterilir.

Karakter	ASCII Değeri	8 Bitlik Gösterim
O	79	01001111
K	75	01001011
U	85	01010101

Bu durumda **OKU** metni, bilgisayar tarafından şu bit dizisiyle temsil edilir:

01001111 01001011 01010101

Burada her karakter 8 bit olduğu için üç karakter, toplam 24 bit eder. Base64, bu 24 bitlik veriyi 6 bitlik parçalara ayırır.

010011 110100 101101 010101

Her 6 bitlik parça 0 ile 63 arasında bir sayısal değere karşılık gelir. Base64 tablosunda toplam 64 karakter bulunduğu için her 6 bitlik grup, bu tablodaki bir karakterle gösterilir.

6 Bitlik Grup	Sayısal Değer	Base64 Karakteri
010011	19	T
110100	52	0
101101	45	t
010101	21	V

Böylece **OKU** metninin Base64 ile kodlanmış hâli şu şekilde olur:

OKU → T0tV

Bulunan sonuç, gizli bir şifre değildir. Base64 tablosunu kullanan bir araç, **T0tV** ifadesini tekrar **OKU** metnine dönüştürebilir. Bu işlem için gizli anahtar gerekmediğinden Base64 şifreleme olarak kabul edilmez.

Base64 tablosunda A-Z, a-z, 0-9, +(artı) ve /(eğik çizgi) karakterleri kullanılır. Bu karakterlerin toplamı 64 olduğu için yönteme **Base64** adı verilir. Base64 veriyi genellikle 3 baytlık gruplar hâlinde işler. 3 bayt, 24 bit eder. 24 bit ise dört tane 6 bitlik gruba ayrılır. Bu nedenle 3 baytlık veri, Base64 sonucunda dört karakterle temsil edilir.

3 bayt veri = 24 bit

24 bit = 6 bit + 6 bit + 6 bit + 6 bit

4 adet 6 bitlik grup = 4 Base64 karakteri

Kodlanacak veri 3 bayta tam bölünmezse Base64 çıktısının sonunda **"="** veya **"=="** işareti görülebilir. Bu işaretler şifre değildir. Yalnızca eksik kalan bölümü tamamlamak için kullanılan dolgu işaretleridir.

Örnek

OKU → T0tV

OKUL → T0tVTA==

OKUL metninde karakter sayısı 3'ün katı olmadığı için Base64 sonucunun sonunda **==** işareti görülür.

NOT: Bu bölümdeki ilk örneklerde Türkçe karakter içermeyen metinler kullanılmıştır çünkü **ç**, **ğ**, **ı**, **ö**, **ş**, **ü** gibi Türkçe karakterler ASCII kapsamında değildir. Bunlar bugün genellikle Unicode/UTF-8 gibi karakter kodlama sistemleriyle temsil edilir ve bazı durumlarda birden fazla bayt kullanabilir. Bu nedenle Türkçe karakter içeren metinlerin Base64 sonuçları, kullanılan karakter kodlama biçimine göre farklı görünebilir.

URL Encoding

İnternet adreslerinde kullanılan bazı karakterler, doğrudan yazıldığında farklı anlamlara gelebilir veya veri aktarımı sırasında sorun oluşturabilir. Bu nedenle boşluk, Türkçe karakter ve bazı özel semboller belirli gösterimlerle temsil edilir. Bir karakterin internet adreslerinde kullanılmaya uygun biçime dönüştürülmesi işlemine **URL Encoding** denir.

URL Encoding işleminde dönüştürülen karakterler genellikle % işareti ve bu işareti takip eden iki onaltılık sayı ile gösterilir. Örneğin bir metinde bulunan boşluk karakteri %20 biçiminde temsil edilir.

Düz Metin	URL Encoding ile Gösterimi
SISTEM VE AG	SISTEM%20VE%20AG
TEST DOSYASI	TEST%20DOSYASI
A+B	A%2BB

URL Encoding bir şifreleme yöntemi değildir. Bu yöntemde amaç, bilgiyi yetkisiz kişilerden gizlemek değil verinin internet adreslerinde ve web uygulamalarında uygun biçimde aktarılmasını sağlamaktır. URL Encoding işleminde gizli anahtar kullanılmaz. Kodlanan veri, uygun bir araçla tekrar eski biçimine dönüştürülebilir.

SIRA SİZDE

Bir okulun web uygulamasında aşağıdaki adresler kullanılmıştır. Ancak bazı özel karakterler URL içerisinde kodlanmadan yazıldığı için adreslerin tarayıcı veya sunucu tarafından yanlış yorumlanma ihtimali bulunmaktadır.

Adres	İncelenecek Parametre Değeri
https://okul.edu.tr/arama?q=siber guvenlik	siber guvenlik
https://okul.edu.tr/dosya?ad=proje&rapor.pdf	proje&rapor.pdf
https://okul.edu.tr/dogrulama?kod=A+B=C	A+B=C

Aşağıdaki çalışmaları gerçekleştiriniz.

1. Adreslerde yanlış yorumlanmaya neden olabilecek boşluk ve özel karakterleri belirleyiniz.

Parametre Değeri	Kodlanması Gereken Karakterler
siber güvenlik	.....
proje&rapor.pdf	.....
A+B=C	.....

2. Aşağıdaki kod karşılıklarından yararlanarak parametre değerlerini URL kodlama yöntemine uygun biçimde yeniden yazınız.

- Boşluk → %20
- + → %2B
- & → %26
- = → %3D

Parametre Değeri	URL Kodlanmış Biçimi
siber güvenlik	.....
proje&rapor.pdf	.....
A+B=C	.....

1. UYGULAMA

Uygulama Adı	Base64 ve URL Encoding Yöntemlerinin Karşılaştırması
Süre	20 dakika
Amaç	Verilen test metnini Base64 ve URL Encoding yöntemleriyle kodlamak, elde edilen sonuçları karşılaştırmak
Yönerge	Aşağıdaki uygulama adımlarını tamamlayınız. Verilen test metnini Base64 ve URL Encoding yöntemleriyle kodlayınız. Elde ettiğiniz sonuçları karşılaştırınız ve kodlama ile şifreleme arasındaki farkı yorumlayınız. Gerçek parola, kişisel bilgi, özel dosya veya başkalarıyla paylaşılmaması gereken herhangi bir veri kullanmayınız.

Uygulama Adımları

A) Test Metnini Belirleme

Aşağıdaki test metnini kullanınız.

SISTEM VE AG

B) Base64 Kodlaması Yapma

Öğretmeninizin belirlediği güvenli çevrim içi veya çevrim dışı aracı kullanarak test metnini Base64 biçimine dönüştürünüz. Elde ettiğiniz sonucu aşağıdaki tabloya yazınız.

İşlem	Sonuç
Kullanılan düz metin	SISTEM VE AG
Base64 ile kodlanmış metin	
Gizli anahtar kullanıldı mı?	
Kodlanan metin tekrar eski hâline dönüştürülebildi mi?	

C) URL Encoding İşlemi Yapma

Aynı test metnini URL Encoding biçimine dönüştürünüz. Elde ettiğiniz sonucu aşağıdaki tabloya yazınız.

İşlem	Sonuç
Kullanılan düz metin	SISTEM VE AG
URL Encoding ile kodlanmış metin	
Boşluk karakteri hangi gösterime dönüştü?	
Gizli anahtar kullanıldı mı?	
Kodlanan metin tekrar eski hâline dönüştürülebildi mi?	

C) URL Encoding İşlemi Yapma

Aynı test metnini URL Encoding biçimine dönüştürünüz. Elde ettiğiniz sonucu aşağıdaki tabloya yazınız.

İşlem	Sonuç
Kullanılan düz metin	SISTEM VE AG
URL Encoding ile kodlanmış metin	
Boşluk karakteri hangi gösterime dönüştü?	
Gizli anahtar kullanıldı mı?	
Kodlanan metin tekrar eski hâline dönüştürülebildi mi?	

Ç) Sonuçları Karşılaştırma

Aşağıdaki tabloyu tamamlayınız.

Karşılaştırma Ölçütü	Base64	URL Encoding
Verinin gösterim biçimini değiştirir mi?		
Gizli anahtar gerektirir mi?		
Temel amacı veriyi gizlemek midir?		
Uygun araçla kolayca geri dönüştürülebilir mi?		

Sonuç Soruları

1. Base64 ve URL Encoding yöntemleri neden şifreleme olarak değerlendirilmez?

.....
.....
.....

2. URL Encoding işleminde boşluk karakterinin %20 biçiminde gösterilmesinin amacı nedir?

.....
.....
.....

3. Karmaşık görünen bir metin neden her zaman güvenli veya şifrelenmiş olarak değerlendirilmemelidir?

.....
.....
.....

Değerlendirme

Çalışmanız öğretmeniniz tarafından kontrol listesine göre değerlendirilecektir. Çalışmanızı yaparken buradaki ölçütleri dikkate alınız. Kontrol listesi formuna ulaşmak için karekodu okutunuz. Dijital yayınlarda karekodun üstüne tıklayarak içeriğe ulaşabilirsiniz.

Frekans Analizi Yöntemi

Bazı dillerde bazı harfler diğerlerinden daha sık kullanılır. Bir şifreleme yönteminde aynı harf her geçtiğinde aynı şifreli harfle değiştiriliyorsa şifreli metindeki tekrarlar çözüm için ipucu verebilir. Frekans analizi, şifreli metindeki harflerin veya sembollerin kaç kez geçtiğini belirleyerek şifre çözmeye yardımcı olan bir yöntemdir. Bu yöntem özellikle basit yerine koyma şifrelerinde işe yarayabilir ancak frekans analizi her şifreli metni kesin olarak çözmez; yalnızca çözüm sürecine katkı sağlar. Modern şifreleme yöntemleri ise bu tür basit analizlere karşı çok daha dayanıklıdır.

Örnek

Aşağıdaki şifreli metni inceleyiniz.

X Y X Y X Y X Z X Z

Öncelikle metindeki harflerin kaçar kez geçtiğini sayınız.

Harf	Geçme Sayısı
X	5
Y	3
Z	2

Bu durumda en sık kullanılan harf X, en az kullanılan harf ise Z'dir. En sık geçen harf, şifreli metindeki önemli ipuçlarından biri olabilir ancak bu bilgi tek başına kesin çözüm sağlamaz. Daha uzun metinlerde harf tekrarları, kelime yapısı ve dil özellikleri birlikte değerlendirilir.

Örnek

Düz Metin Harfi	Şifreli Harf
A	M
G	T
L	P
A	M
R	S

Bu durumda

Düz Metin Harfi	Şifreli Harf
AGLAR	MTPMS

Dikkat edilirse düz metindeki **A** harfi iki kez geçmiştir ve her iki durumda da **M** harfine dönüşmüştür. Bu tür tekrarlar, frekans analizi ve örüntü incelemesi için ipucu oluşturabilir.

SIRA SİZDE

Aşağıdaki çalışmaları bireysel olarak tamamlayınız. Önce verilen durumların hangi kavramla ilişkili olduğunu belirleyiniz ve seçiminizin gerekçesini yazınız. Bu çalışmada kullanacağınız kavramlar şunlardır: **kriptografi, kriptanaliz, encoding, şifreleme, frekans analizi**. Ardından Base64 ile ilgili verilen ifadeyi okuyarak düşüncenizi gerekçesiyle açıklayınız. Son olarak verilen şifreli metindeki harflerin kaç kez geçtiğini sayınız ve frekans analiziyle ilgili soruları cevaplayınız. Cevaplarınızı tamamladıktan sonra sınıfta arkadaşlarınızla karşılaştırınız.

No.	Durum	İlgili Kavram	Kısa Gerekçe
1	Bir mesajı anahtar yardımıyla okunamaz hâle getirmek		
2	Şifreli bir metinde en sık geçen harfleri saymak		
3	Bir metni Base64 biçimine dönüştürmek		
4	Bir şifreleme yönteminin zayıf yönlerini incelemek		
5	Bilgiyi korumaya yönelik yöntemler geliştirmek		

Aşağıdaki ifadeyi okuyunuz ve düşüncenizi gerekçesiyle yazınız.

"Base64 ile dönüştürülen bir metin karmaşık görünür. Bu yüzden Base64 güvenli bir şifreleme yöntemidir."

Bu ifadeye katılıyor musunuz? Neden?

.....

.....

Aşağıdaki şifreli metindeki harflerin kaç kez geçtiğini sayınız.

Şifreli metin: **M M M K K T M K T M**

Harf	Geçme Sayısı
M	
K	
T	

Aşağıdaki soruları cevaplayınız.

1. En sık kullanılan harf hangisidir?

   .....

2. Bu bilgi şifre çözmede nasıl bir ipucu verebilir?

   .....

3. Bu ipucu tek başına kesin çözüm sağlar mı? Neden?

   .....

2. UYGULAMA

Uygulama Adı	Frekans Analiziyle Şifreli Metindeki İpuçlarını Bulmak
Süre	25 dakika
Amaç	Şifreli bir metindeki harf tekrarlarını incelemek ve frekans analiziyle ipuçları elde etmek
Yönerge	Aşağıdaki şifreli metni inceleyiniz. İşlem yaparken Türkçe karakter içermeyen Latin alfabesini kullanınız. Harflerin tekrar sayılarını belirleyiniz ve kelime yapılarını karşılaştırınız. Elde ettiğiniz ipuçlarından yararlanarak basit bir klasik şifreleme yöntemiyle oluşturulan metni çözmeye çalışınız.

Uygulama Adımları

A) Şifreli Metni İnceleme

Aşağıdaki şifreli metin, sabit kaydırma kuralı kullanılarak oluşturulmuştur.

YHUL JXYHQOLJL YHULBL NRUXU

B) Harflerin Tekrar Sayılarını Belirleme

Şifreli metindeki harflerin kaç kez geçtiğini sayınız. En sık karşılaştığınız harfleri aşağıdaki tabloya yazınız.

Şifreli Harf	Geçme Sayısı

C) Tekrar Eden Örüntüleri Bulma

Aşağıdaki soruları cevaplayınız.

1. Şifreli metinde tekrar eden veya birbirine benzeyen kelimeler var mıdır?

   .....

2. Tekrar eden kelimeler, şifreli metni çözmek için nasıl bir ipucu verebilir?

   .....

3. Şifreli metinde en sık kullanılan harf hangisidir?

   .....

Ç) Kaydırma Kuralını Deneme

Metindeki harfleri alfabede üç harf geri kaydırarak çözmeye çalışınız.

Şifreli Metin	Uygulanan Kural	Çözülen Düz Metin
YHUL	Her harfi üç harf geri kaydırınız.	
JXYHQOLJL	Her harfi üç harf geri kaydırınız.	
YHULBL	Her harfi üç harf geri kaydırınız.	
NRUXU	Her harfi üç harf geri kaydırınız.	

D) Düz Metni Yazma

Bulduğunuz düz metni aşağıdaki alana yazınız.

.....

.....

Sorular

1. Frekans analizi tek başına her şifreli metni kesin olarak çözebilir mi? Neden?

   .....

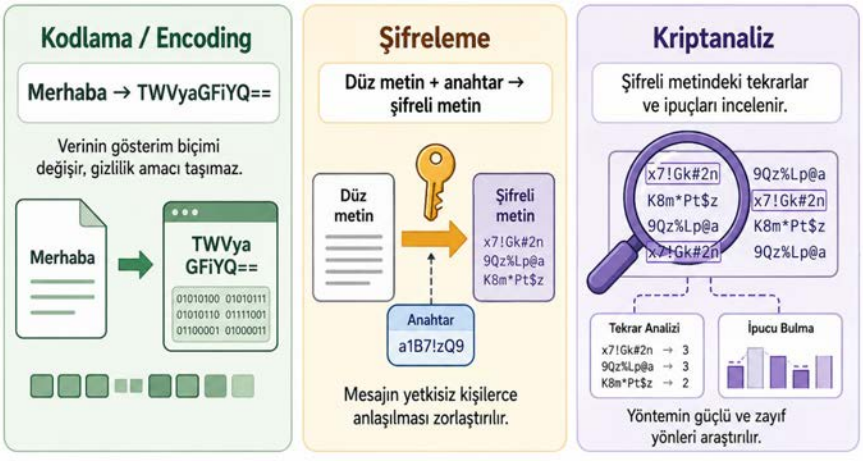
2. Tekrar eden kelimeler ve harfler, şifre çözme sürecinde nasıl kullanılabilir?

   .....

Değerlendirme

Çalışmanız öğretmeniniz tarafından kontrol listesine göre değerlendirilecektir. Çalışmanızı yaparken buradaki ölçütleri dikkate alınız. Kontrol listesi formuna ulaşmak için karekodu okutunuz. Dijital yayınlarda karekodun üstüne tıklayarak içeriğe ulaşabilirsiniz.

Kodlama, şifreleme ve kriptanaliz arasındaki fark Görsel 6.2'de belirtilmiştir.



Görsel 6.2: Kodlama, şifreleme ve kriptanaliz arasındaki fark

6.2. KLASİK KRİPTOGRAFİ

Klasik kriptografi sistemleri, modern bilgisayar sistemlerinden önce kullanılan temel şifreleme yöntemlerini kapsar. Bu yöntemlerde genellikle harflerin yerleri değiştirilir, harfler başka harflerle eşleştirilir veya belirli bir anahtara göre mesaj dönüştürülür.

Klasik Kriptografi: Mesajları gizlemek için kullanılan eski ve temel şifreleme yöntemlerini ifade eder. Bu yöntemler genellikle harfler, semboller ve basit kurallar üzerinden çalışır. Klasik kriptografide bulunan üç temel unsur ve bunların açıklamaları Tablo 6.4'te gösterilmiştir.

Tablo 6.4: Klasik Kriptografide Temel Unsurlar

Unsur	Açıklama
Düz metin	Şifrelenmeden önceki okunabilir mesajdır.
Anahtar / Kural	Mesajın nasıl değiştirileceğini belirleyen bilgidir.
Şifreli metin	Şifreleme işleminden sonra oluşan mesajdır.

Örneğin **OKUL** kelimesi düz metindir. Bu kelimedeki harfler belirli bir kurala göre değiştirilirse şifreli bir metin elde edilir. Klasik şifreleme yöntemleri, kriptografi mantığını öğrenmek için oldukça faydalıdır ancak bu yöntemler bugünün dijital güvenliği için tek başına yeterli değildir çünkü çoğu klasik şifreleme yöntemi, harf tekrarları ve dil özellikleri incelenerek çözülebilir.

6.2.1. Sezar Şifreleme Algoritması

Sezar şifreleme algoritması, harflerin alfabede belirli bir sayı kadar kaydırılması mantığına dayanır. Kaydırma miktarı bu yöntemde anahtar gibi kullanılır. Bu örnekte işlem kolaylığı sağlamak için Türkçe karakter içermeyen Latin alfabesi kullanılmıştır. Alfabe harfleri şu şekilde numaralandırılır:

Harf	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Değer	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Şifreleme işlemi şu mantıkla yapılır:

Şifreli Değer = (Düz metin harfinin değeri + Anahtar) mod 26

Şifre çözme işlemi ise ters yönde yapılır.

Düz metin değeri = (Şifreli harfin değeri - Anahtar) mod 26

Örnek

Düz Metin: NETWORK

Anahtar: **+ 4**

Sezar şifreleme yöntemine göre yapılan işlemler Tablo 6.5'te gösterilmiştir.

Tablo 6.5: Sezar Şifreleme İşlemi

Düz Metin Harfi	Harf Değeri	İşlem	Şifreli Değer	Şifreli Harf
N	13	13 + 4 = 17	17	R
E	4	4 + 4 = 8	8	I
T	19	19 + 4 = 23	23	X
W	22	22 + 4 = 26 → 0	0	A
O	14	14 + 4 = 18	18	S
R	17	17 + 4 = 21	21	V
K	10	10 + 4 = 14	14	O

Tablodan çıkarılan sonuç şöyledir:

Düz Metin	Anahtar	Şifreli Metin
NETWORK	+4	RIXASVO

Şifre çözmek için aynı anahtar ters yönde uygulanır. Bir başka ifadeyle her harf 4 adım geri kaydırılır.

Şifreli Metin	Anahtar	Çözülen Düz Metin
RIXASVO	-4	NETWORK

SIRA SİZDE

Aşağıdaki kelimeleri verilen kaydırma kuralına göre defterinizde şifreleyiniz. İşlem yaparken Türkçe karakter içermeyen Latin alfabesini kullanınız.

Düz Metin	Kaydırma Kuralı	Şifreli Metin
CRYPTOGRAPHY	Her harfi 5 harf ileri kaydırınız.	
KEY	Her harfi 7 harf ileri kaydırınız.	

Cevabınızı tamamladıktan sonra seçtiğiniz harflerin alfabede doğru yönde kaydırılıp kaydırılmadığını kontrol ediniz.

6.2.2. Vigenere Şifreleme Algoritması

Vigenere şifreleme algoritması, Sezar şifrelemesine benzer ancak Sezar yönteminde tüm harfler aynı miktarda kaydırılır. Vigenere yönteminde kaydırma miktarı anahtar kelimeye göre değişebilir. Bu yöntemde bir anahtar kelime seçilir. Anahtar kelime, düz metnin altına tekrar edecek şekilde yazılır. Böylece her harf için farklı bir kaydırma yapılabilir. Vigenere şifreleme örneği, Tablo 6.6'da verilmiştir. Bu örnekte işlem kolaylığı sağlamak için Türkçe karakter içermeyen Latin alfabesi kullanılmıştır. Harf değerleri A = 0, B = 1, C = 2 şeklinde düşünülmüştür.

Tablo 6.6: Vigenere Şifreleme Örneği

Düz Metin	K	O	D	L	A
Anahtar	A	B	C	A	B
Kaydırma Miktarı	0	+ 1	+ 2	0	+ 1
Şifreli Metin	K	P	F	L	B

Örnekte O harfi, anahtardaki B harfine karşılık geldiği için 1 harf ileri kaydırılmış ve P olmuştur. D harfi ise anahtardaki C harfine karşılık geldiği için 2 harf ileri kaydırılmış ve F olmuştur. Vigenere şifrelemesinde her harf, anahtar harfinin gösterdiği kaydırma miktarına göre dönüştürülür.

Düz Metin	**Anahtar Kelime**	**Şifreli Metin**
KODLA	ABCAB	KPFLB

Vigenere şifrelemesinde aynı harf, anahtarın durumuna göre farklı harflere dönüşebilir. Bu nedenle Sezar şifrelemesine göre daha güçlü bir klasik yöntemdir. Anahtar kısa veya tahmin edilebilir olursa yöntem zayıflayabilir. Bugünün güvenlik riskleri için tek başına yeterli kabul edilmez.

BİLGİ KUTUSU

Sezar şifrelemesinde aynı harf aynı kaydırma kuralıyla her zaman aynı harfe dönüşür. Vigenere şifrelemesinde ise anahtar harfleri değiştiği için aynı düz metin harfi farklı şifreli harflere dönüşebilir.

Aşağıdaki örnekte anahtar harfleri şu şekilde düşünülmüştür:

A = 0 kaydırma

B = + 1 kaydırma

C = + 2 kaydırma

D = + 3 kaydırma

Düz Metin	**M**	**A**	**M**	**A**
Anahtar	A	B	C	D
Kaydırma	0	+1	+2	+3
Şifreli Harf	M	B	O	D

Bu durumda sonuç şöyledir:

Düz Metin	Anahtar	Şifreli Metin
MAMA	ABCD	MBOD

Örnekte M harfi birinci sırada M olarak kalmış, üçüncü sırada ise O harfine dönüşmüştür çünkü aynı harf, farklı anahtar harfleriyle işlenmiştir. Şifre çözme işleminde ise anahtarın gösterdiği kaydırma miktarı ters yönde uygulanır.

Şifreli Metin	**M**	**B**	**O**	**D**
Anahtar	A	B	C	D
Ters Kaydırma	0	-1	-2	-3
Düz Metin	M	A	M	A

Bu durumda sonuç şöyledir:

Şifreli Metin	Anahtar	Çözülen Düz Metin
MBOD	ABCD	MAMA

SIRA SİZDE

Aşağıdaki kelimeleri verilen anahtar ve kaydırma mantığına göre defterinizde şifreleyiniz. İşlem yaparken Türkçe karakter içermeyen Latin alfabesini kullanınız. Harf değerlerini A = 0, B = 1, C = 2 şeklinde düşününüz.

Düz Metin	Anahtar	Kaydırma Mantığı	Şifreli Metin
ROTA	ABCA	0, +1, +2, 0	
MOLA	BCAA	+1, +2, 0, 0	

Cevabınızı tamamladıktan sonra her harfin, karşısındaki anahtar harfine göre doğru miktarda kaydırılıp kaydırılmadığını kontrol ediniz.

6.2.3. Yerine Koyma Şifrelemesi

Düz metindeki her harf başka bir harfle değiştirilir. Bu işlem için bir eşleştirme tablosu kullanılır. Aynı düz metin harfi, metin boyunca aynı şifreli harfe dönüşür. Örneğin Tablo 6.7 gibi bir sistem oluşturulabilir.

Tablo 6.7: Yerine Koyma Şifrelemesi Örneği

Düz Metin Harfi	Şifreli Harf
D	M
E	T
R	K
S	A

Bu tabloya göre DERS ifadesi şöyle şifrelenebilir.

Düz Metin	Kural	Şifreli Metin
DERS	Her harfi tablodaki karşılığıyla değiştir.	MTKA

Yerine koyma şifrelemesinde aynı düz metin harfi, her zaman aynı şifreli harfe dönüşürse şifreli metindeki tekrarlar ipucu verebilir. Bu nedenle frekans analizi gibi yöntemlerle bu tür şifrelerin zayıf yönleri incelenebilir.

6.2.4. Vernam Şifrelemesi

Vernam şifrelemesi (vernam cipher), her karakter için ayrı bir anahtar kullanma mantığına dayanır. Bu yöntemde anahtarın mesajla aynı uzunlukta olması, rastgele seçilmesi ve yalnızca bir kez kullanılması önemlidir. Bu nedenle Vernam Cipher, tek kullanımlık anahtar fikriyle ilişkilidir. Anahtar gerçekten rastgele seçilir, mesajla aynı uzunlukta olur, gizli tutulur ve sadece bir defa kullanılırsa yöntem çok güçlü olabilir ancak anahtarın güvenli biçimde paylaşılması ve tekrar kullanılmaması gerekir. Bu da uygulamada dikkat isteyen bir durumdur. Vernam Cipher'da temel işlem **XOR** işlemidir. **XOR** işleminde iki bit karşılaştırılır. Bitler aynıysa sonuç 0, farklıysa sonuç 1 olur. XOR işlemi şu şekildedir:

Düz Metin Biti	Anahtar Biti	XOR Sonucu
0	0	0
0	1	1
1	0	1
1	1	0

Örnek

Düz Metin: VERI

Anahtar: FGBD

Harfler sayısal değerlere dönüştürülmüştür. Bu örnekte A = 0, B = 1, C = 2 şeklinde düşünülmüştür.

Harf	Sayısal Değer	5 Bitlik Gösterim
V	21	10101
E	4	00100
R	17	10001
I	8	01000

Anahtar Harfleri

Anahtar Harfi	Sayısal Değer	5 Bitlik Gösterim
F	5	00101
G	6	00110
B	1	00001
D	3	00011

Her düz metin biti ile aynı sıradaki anahtar biti XOR işlemine tabi tutulur (Tablo 6.8).

Tablo 6.8: Vernam Cipher XOR İşlemi

Düz Metin Harfi	Düz Metin Biti	Anahtar Harfi	Anahtar Biti	XOR Sonucu	Şifreli Harf
V	10101	F	00101	10000	Q
E	00100	G	00110	00010	C
R	10001	B	00001	10000	Q
I	01000	D	00011	01011	L

Bu durumda ortaya şu sonuç çıkar:

Düz Metin	Anahtar	Şifreli Metin
VERI	FGBD	QCQL

Şifre çözme işleminde ise aynı anahtar tekrar XOR işleminde kullanılır. Şifreli metin ile aynı anahtar yeniden XOR işlemine sokulduğunda düz metne ulaşılır.

Şifreli Metin	Anahtar	Düz Metin
QCQL	FGBD	VERI

6.2.5. Klasik Şifreleme Yöntemlerinin Güçlü ve Zayıf Yönleri

Klasik şifreleme yöntemleri, kriptografinin temel mantığını öğrenmek için kullanışlıdır ancak bu yöntemler bugünün dijital sistemlerini korumak için yeterli değildir. Çünkü klasik yöntemlerde genellikle harflerin yerleri değiştirilir veya harfler başka harflerle eşleştirilir. Şifreli metinde tekrar eden harfler, kelime yapıları ve dil özellikleri incelenerek ipuçları bulunabilir.

1. ETKİNLİK

Etkinlik Adı	Mesaja Uygun Şifreleme Yöntemini Seçme
Süre	30 dakika
Amaç	Verilen kısa test mesajını inceleyerek klasik şifreleme yöntemlerinden uygun olanını seçmek
Yönerge	Aşağıda verilen test mesajını inceleyiniz. Sezar, Vigenere veya yerine koyma yöntemlerinden birini seçiniz. Seçtiğiniz yöntemin neden uygun olduğunu gerekçelendiriniz. Ardından mesajı belirlediğiniz anahtar veya kurala göre şifreleyiniz. Şifrelediğiniz mesajı tekrar çözerek işleminizin doğru olup olmadığını kontrol ediniz.

A) Test Mesajını İnceleme

Şifrelenecek test mesajı

BILGI

B) Yöntemlerin Özelliklerini Karşılaştırma

Şifreleme Yöntemi	Temel Mantığı	Bu Mesaj İçin Tercih Edilebilir mi?	Gerekçeniz
Sezar Şifreleme	Harfler sabit miktarda kaydırılır.		
Vigenere Şifreleme	Harfler anahtar kelimeye göre farklı miktarlarda kaydırılır.		
Yerine Koyma Şifrelemesi	Her harf belirlenen başka bir harfle değiştirilir.		

C) Yönteminizi Belirleme

İncelenecek Alan	Cevabınız
Seçtiğiniz şifreleme yöntemi	
Kullanacağınız anahtar veya kural	
Bu yöntemi seçme nedeniniz	

Ç) Mesajı Şifreleme

Düz Metin	Seçilen Yöntem	Anahtar veya Kural	Şifreli Metin
BILGI			

D) Şifreli Metni Çözme

Şifrelediğiniz metni aynı yöntemin ters işlemini kullanarak tekrar çözünüz.

Şifreli Metin	Kullanılan Ters İşlem	Çözülen Düz Metin

Sorular

1. Seçtiğiniz yöntemin güçlü yönü nedir?

   .....
   .....

2. Seçtiğiniz yöntemin zayıf yönü nedir?

   .....
   .....

3. Şifreli metni tekrar çözebildiniz mi? Ulaştığınız sonuç ilk test mesajıyla aynı mıdır?

   .....
   .....

4. Klasik şifreleme yöntemleri neden günümüzde tek başına yeterli kabul edilmez?

   .....
   .....

Değerlendirme

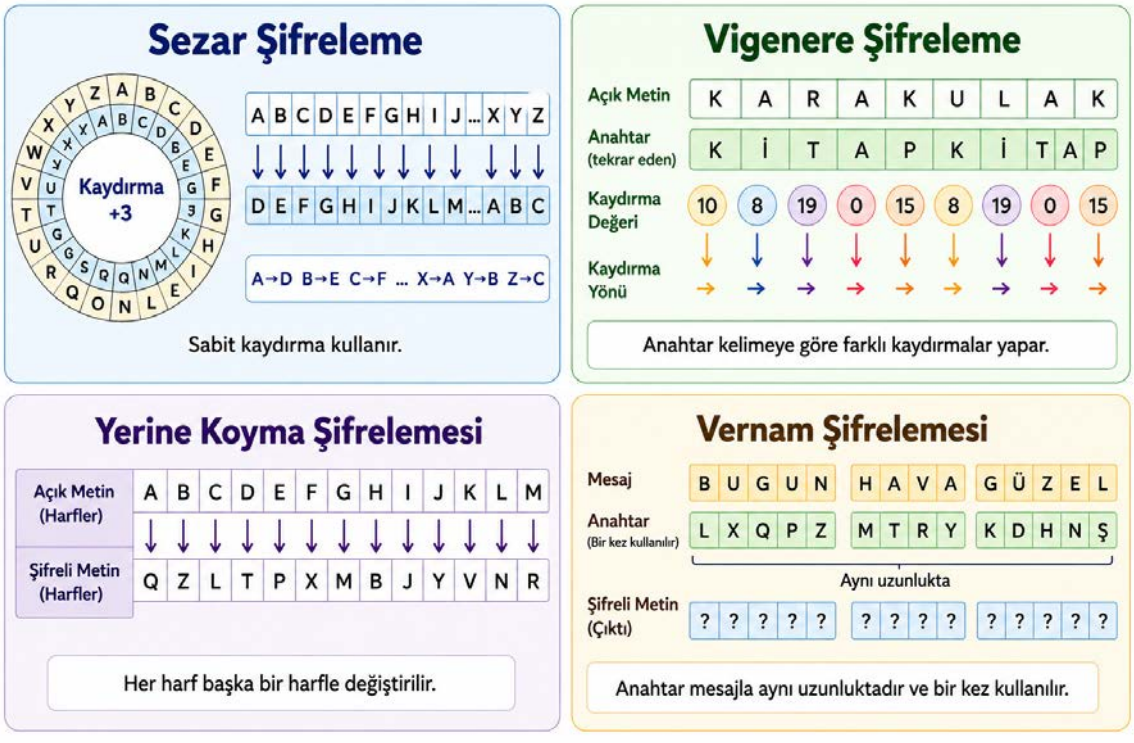
Çalışmanız öğretmeniniz tarafından kontrol listesine göre değerlendirilecektir. Çalışmanızı yaparken buradaki ölçütleri dikkate alınız. Kontrol listesi formuna ulaşmak için karekodu okutunuz. Dijital yayınlarda karekodun üstüne tıklayarak içeriğe ulaşabilirsiniz.

Klasik şifreleme yöntemlerinin güçlü ve zayıf yönleri Tablo 6.9'da görülür.

Tablo 6.9: Klasik Şifreleme Yöntemlerinin Güçlü ve Zayıf Yönleri

Yöntem	Temel Mantık	Güçlü Yönü	Zayıf Yönü
Sezar Şifreleme	Harfleri sabit miktarda kaydırır.	Öğrenmesi ve uygulaması kolaydır.	Kaydırma miktarı denenerek kolayca çözülebilir.
Vigenere Şifreleme	Anahtar kelimeye göre farklı kaydırmalar yapar.	Sezar yöntemine göre daha güçlüdür.	Anahtar kısa veya tahmin edilebilir olursa zayıflar.
Yerine Koyma Şifrelemesi	Her harfi başka bir harfle değiştirir.	Basit mesajları gizlemek için kullanılabilir.	Harf tekrarları frekans analiziyle ipucu verebilir.
Vernam Şifreleme	Mesaj uzunluğunda tek kullanımlık anahtar kullanır.	Anahtar rastgele, gizli ve tek kullanımlıysa çok güçlü olabilir.	Anahtarın güvenli paylaşılması ve tekrar kullanılmaması gerekir.

Klasik şifreleme algoritmaları Görsel 6.3'te toplu bir şekilde verilmiştir.



Görsel 6.3: Klasik şifreleme yöntemleri

2. ETKİNLİK

Etkinlik Adı	Klasik Şifreleme Yöntemlerini Uygulamak
Süre	40 dakika
Amaç	Sezar, Vigenere, yerine koyma ve Vernam şifreleme yöntemlerinin temel mantığını kâğıt-kalem yöntemiyle uygulamak ve sonuçları yorumlamak
Yönerge	Aşağıdaki alt görevleri defterinizde tamamlayınız. İşlemlerde yalnızca verilen test kelimelerini ve örnek anahtarları kullanınız.

A) Sezar Yöntemiyle Şifreleme

Aşağıdaki kelimeyi verilen kurala göre şifreleyiniz.

Düz Metin	Anahtar / Kural	Şifreli Metin
MASA	Her harfi + 2 kaydırınız.	

B) Vigenere Yöntemiyle Şifreleme

Aşağıdaki tabloyu tamamlayarak KALE kelimesini verilen anahtara göre şifreleyiniz.

	1. Harf	2. Harf	3. Harf	4. Harf
Düz Metin	K	A	L	E
Anahtar	A	B	A	B
Kaydırma Miktarı	0	+1	0	+1
Şifreli Metin				

Şifreli Metin: .....

C) Yerine Koyma Yöntemiyle Şifreleme veya Çözme

Aşağıdaki tabloyu kullanarak KALEM kelimesini şifreleyiniz.

Düz Metin Harfi	Şifreli Harf
K	Z
A	M
L	P
E	R
M	T

Şifreli Metin: .....

Ç) Vernam Mantığını Yorumlama

Aşağıdaki soruyu gerekçesini belirterek cevaplayınız.

Vernam şifreleme yönteminde her karakter için ayrı anahtar kullanılması neden önemlidir?

.....

D) Sezar Yöntemiyle Şifre Çözme

Aşağıdaki şifreli metni verilen kurala göre çözünüz. İşlem yaparken Türkçe karakter içermeyen Latin alfabesini kullanınız.

Şifreli Metin	Şifre Çözme Kuralı	Çözülen Düz Metin
OCUC	Her harfi iki harf geri kaydırınız.	

Cevabınızı tamamladıktan sonra elde ettiğiniz düz metindeki her harfin doğru yönde kaydırılıp kaydırılmadığını kontrol ediniz.

E) Vigenere Yöntemiyle Şifre Çözme

Aşağıdaki şifreli metni verilen anahtara göre çözünüz. Harf değerlerini A = 0, B = 1, C = 2 şeklinde düşününüz.

	1. Harf	2. Harf	3. Harf	4. Harf
Şifreli Metin	K	B	L	F
Anahtar	A	B	A	B
Ters Kaydırma Miktarı	0	-1	0	-1
Çözülen Düz Metin				

Çözülen Düz Metin: .....

Cevabınızı tamamladıktan sonra çözdüğünüz metni yeniden şifreleyerek sonucun ilk şifreli metinle aynı olup olmadığını kontrol ediniz.

Değerlendirme

Çalışmanız öğretmeninizin tarafından kontrol listesine göre değerlendirilecektir. Çalışmanızı yaparken buradaki ölçütleri dikkate alınız. Kontrol listesi formuna ulaşmak için karekodu okutunuz. Dijital yayınlarda karekodun üstüne tıklayarak içeriğe ulaşabilirsiniz.

SIRA SİZDE

Aşağıdaki çalışmayı yönergelere uygun olarak tamamlayınız. Sezar, Vigenere, yerine koyma ve Vernam şifreleme yöntemlerini dikkate alarak önce açıklamaların hangi klasik şifreleme yöntemiyle ilişkili olduğunu belirleyiniz. Ardından verilen durumları inceleyerek her durum için uygun yöntemi ve gerekçenizi yazınız. Cevaplarınızı tamamladıktan sonra yöntemlerin özellikleriyle verdiğiniz cevapların uyumlu olup olmadığını kontrol ediniz.

Açıklama	**İlgili Yöntem**
Harflerin belirli bir sayı kadar kaydırılmasıyla çalışır.	
Anahtar kelimeye göre farklı kaydırmalar yapılabilir.	
Her harf başka bir harfle eşleştirilir.	
Mesajla aynı uzunlukta tek kullanımlık anahtar kullanılır.	

Durum	Uygun Yöntem	Gerekçe
Çok kısa bir mesajı harfleri 3 ileri kaydırarak gizlemek istiyorsunuz.		
Aynı harfin her zaman aynı harfe dönüşmediği bir yöntem kullanmak istiyorsunuz.		
Harfler için önceden belirlenmiş bir eşleştirme tablosu kullanıyorsunuz.		
Mesajla aynı uzunlukta ve yalnızca bir kez kullanılan anahtar kullanıyorsunuz.		

6.3. ÖZET FONKSİYONLARI

Dijital ortamda bir bilginin değişip değişmediğini anlamak, indirilen bir dosyanın bütünlüğünü kontrol etmek veya parolaları daha güvenli biçimde saklamak için hash fonksiyonları kullanılır. Hash fonksiyonları, bir veriden sabit uzunlukta bir özet değer üretir. Bu özet değer, verinin dijital parmak izi gibi düşünülebilir. Veride çok küçük bir değişiklik yapılsa bile oluşan hash değeri büyük ölçüde değişir.

6.3.1. Hash Fonksiyonu

Hash fonksiyonu bir metni, dosyayı veya veriyi alarak sabit uzunlukta bir özet değer üretir. Bu özet değere hash değeri, özet değer veya dijital parmak izi denebilir. Örneğin bir dosyanın içeriği hash fonksiyonundan geçirilirse o dosyaya ait özel bir özet değer oluşur. Dosyada tek bir karakter bile değişirse hash değeri tamamen farklı bir değer gibi görünebilir. Hash fonksiyonlarının temel özellikleriyle açıklamaları Tablo 6.10'da görülür.

Tablo 6.10: Hash Fonksiyonlarının Temel Özellikleri

Özellik	Açıklama
Tek yönlüdür.	Hash değerinden ilk veriye geri dönülmesi beklenmez.
Sabit uzunlukta çıktı üretir.	Veri kısa veya uzun olsa da kullanılan algoritmaya göre belirli uzunlukta hash değeri oluşur.
Aynı veri aynı hash değerini üretir.	Aynı algoritma ve aynı veri kullanılırsa sonuç aynı olur.
Küçük değişiklik büyük fark oluşturur.	Veride küçük bir değişiklik yapılsa bile hash değeri değişir.

Örnek

Veri	Hash mantığı açısından sonuç
Okul	Belirli bir hash değeri üretir.
Okul.	Nokta eklendiği için farklı bir hash değeri üretir.
okul	Büyük / küçük harf değiştiği için farklı bir hash değeri üretir.

Soru

Yukarıdaki bilgiye göre bir dosyada yalnızca bir harf değişirse hash değerinin değişmesi neden önemlidir?

.....

Hash ile Şifreleme Arasındaki Fark

Hash ve şifreleme birbirine karıştırılmamalıdır. İkisi de kriptografiyle ilişkilidir ancak amaçları ve çalışma biçimleri farklıdır.

Şifreleme, veriyi gizlemek için kullanılır. Şifrelenen veri, uygun anahtar ve yöntemle tekrar okunabilir hâle getirilebilir. **Hashleme** ise veriden tek yönlü bir özet değer üretir. Hash değerinden ilk veriye geri dönülmesi amaçlanmaz.



SIRA SİZDE

Verilen durumların hashleme veya şifreleme ile ilişkisini belirleyerek gerekçenizi yazınız. Metinlerin hash değerlerinin aynı olup olmayacağını tahmin edip nedenini açıklayınız. Son olarak salt kullanımının hash değerlerine etkisini belirtiniz.

Durum	Hashleme / Şifreleme	Kısa Gerekçe
Bir dosyanın değiştirilip değiştirilmediğini kontrol etmek		
Bir mesajı yalnızca alıcının okuyabileceği hâle getirmek		
Parolanın açık hâlini saklamadan doğrulama yapmak		
Şifreli mesajı doğru anahtarla tekrar okunabilir hâle getirmek		
İndirilen dosyanın yayımlanan özet değeriyle eşleşip eşleşmediğini kontrol etmek		

Metin	Hash değeri aynı mı olur?	Neden?
Okul		
Okul.		
okul		

İki öğrenci salt kullanmadan aynı test parolasını kullanırsa aynı hash değeri oluşabilir. Salt kullanmak bu durumu nasıl değiştirir?

.....

.....

Hash Değerinin Kullanım Alanı

Hash değerleri birçok alanda kullanılabilir. Hash değerinin kullanım alanı Tablo 6.11'de görülür.

Tablo 6.11: Hash Değerinin Kullanım Alanları

Kullanım Alanı	Açıklama
Dosya bütünlüğü kontrolü	Dosyanın değiştirilip değiştirilmediğini anlamaya yardımcı olur.
Parola saklama	Parolaların doğrudan saklanması yerine hashleme ve salt mantığı kullanılır.
Veri karşılaştırma	Büyük dosyaların veya metinlerin aynı olup olmadığını hızlıca kontrol etmeye yardımcı olabilir.
Yazılım indirme kontrolü	İndirilen dosyanın yayımlanan hash değeriyle eşleşip eşleşmediği kontrol edilebilir.

Dosya Bütünlüğünün Kontrolü

Dosya bütünlüğü, bir dosyanın değiştirilip değiştirilmediğini anlamakla ilgilidir. Bir dosyanın hash değeri daha önce kaydedilmişse daha sonra aynı dosyanın hash değeri tekrar hesaplanabilir. İki değer aynıysa dosyanın yüksek olasılıkla değişmediği düşünülebilir. Değerler farklıysa dosyada değişiklik olmuş olabilir.

Örnek

Bir öğretmen, öğrencilerine **ag_guvenligi_notlari.txt** adlı bir dosya göndermiştir. Öğretmen dosyanın SHA-256 hash değerini de paylaşır ve öğrencilerden Tablo 6.12'ye göre dosya bütünlüğünü kontrol etmelerini ister.

Tablo 6.12: Dosya Bütünlüğü Kontrolü Örneği

Durum	Açıklama
Öğretmenin paylaştığı SHA-256 değeri	Dosyanın ilk hâline ait özet değer
Öğrencinin hesapladığı SHA-256 değeri	Öğrencinin indirdiği dosyanın özet değeri
İki değer aynıysa	Dosyanın yüksek olasılıkla değişmediği düşünülebilir.
İki değer farklıysa	Dosyada değişiklik olmuş olabilir.

Örnek Durum

Kontrol	Sonuç
Paylaşılan hash değeri	A1B2C3...
Öğrencinin hesapladığı hash değeri	A1B2C3...
Yorum	Hash değerleri aynı görünüyor. Dosya bütünlüğü korunmuş olabilir.



BİLGİ KUTUSU

Dosyada yalnızca küçük bir değişiklik yapılsa bile SHA-256 değeri tamamen farklı görünebilir. Bu özellik, dosya bütünlüğü kontrolünde kullanılır ancak hash değeri dosyanın kendisi değildir yalnızca dosyadan üretilmiş tek yönlü bir özet değerdir.

Bu uygulamada dosya bütünlüğünü kontrol etmek için SHA-256 özet değeri kullanılacaktır. SHA-256 ve diğer özet algoritmaları bir sonraki başlıkta daha ayrıntılı olarak ele alınacaktır.

3. UYGULAMA

Uygulama Adı	Dosya Hash Değeri ve Bütünlük Kontrolü
Süre	20 dakika
Amaç	Bir test dosyasının SHA-256 hash değerini hesaplamak
Yönerge	Aşağıdaki işlem basamaklarını öğretmen rehberliğinde tamamlayınız. Komutlarda kullanılan dosya adları örnektir. Uygulama sırasında yalnızca öğretmeninizin verdiği test dosyasını kullanınız. Gerçek kişisel dosya, özel belge, parola, okul hesabı bilgisi veya hassas veri kullanmayınız. Test dosyasının SHA-256 hash değerini hesapladıktan sonra dosyada küçük bir değişiklik yapınız. Değişiklikten önceki ve sonraki hash değerlerini karşılaştırınız. Elde ettiğiniz sonucu dosya bütünlüğü açısından yorumlayınız.

Uygulamada Kullanılabilecek Komutlar

Dosya hash değeri hesaplama işlemi farklı işletim sistemlerinde farklı komutlarla yapılabilir. Aşağıda Windows ve Linux ortamlarında SHA-256 hash değeri hesaplamak için kullanılabilecek temel komutlar ve örnek ekran çıktıları verilmiştir. Amaç, test dosyasına ait hash değerinin nasıl hesaplandığını gözlemlemektir.

Kapalı Kaynak Kodlu İşletim Sisteminde certutil ile SHA-256 Hesaplama

certutil -hashfile ornek.txt SHA256

Bu komut, ornek.txt adlı test dosyasının SHA-256 hash değerini hesaplamak için kullanılabilir. certutil ile SHA-256 hesaplama örneği Görsel 6.4'te verilmiştir.

```
C:\Users\ozrek> cd C:\Users\ozrek\OneDrive\Masaüstü

C:\Users\ozrek\OneDrive\Masaüstü>certutil -hashfile ornek.txt SHA256
SHA256 hash of ornek.txt:
398237c44768fb34eb59138e29845f1d2abdbdabfd3c9eaa5c2b1195428018bad
CertUtil: -hashfile command completed successfully.

C:\Users\ozrek\OneDrive\Masaüstü> _
```

Görsel 6.4: certutil ile SHA-256 hesaplama

PowerShell ile Get-FileHash Kullanımı

Get-FileHash .\ornek.txt -Algorithm SHA256

Bu komut, PowerShell ortamında ornek.txt adlı test dosyasının SHA-256 hash değerini göstermek için kullanılabilir.

PowerShell Get-FileHash kullanımı Görsel 6.5'te verilmiştir.

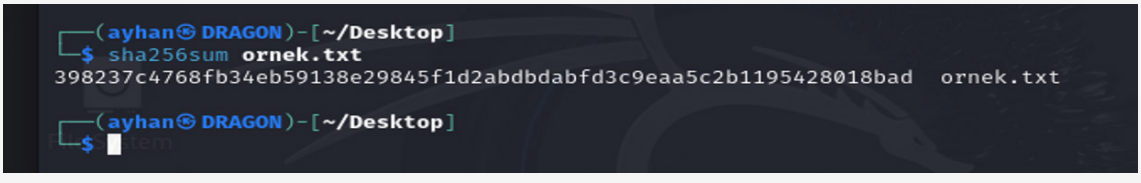


Görsel 6.5: PowerShell Get-FileHash kullanımı

Açık Kaynak Kodlu İşletim Sisteminde sha256sum Kullanımı

sha256sum ornek.txt

Bu komut, açık kaynak kodlu işletim sistemlerinde ornek.txt adlı test dosyasının SHA-256 hash değerini hesaplamak için kullanılabilir. sha256sum kullanımı Görsel 6.6'da verilmiştir.



Görsel 6.6: sha256sum kullanımı

Uygulama Adımları

1. Adım: Öğretmeninizin verdiği test dosyasını belirlenen klasöre kaydediniz.

2. Adım: Dosyanın SHA-256 hash değerini uygun komutla hesaplayınız.

3. Adım: İlk hash değerini tabloya yazınız.

4. Adım: Dosyanın sonuna bir nokta, boşluk veya kısa bir test kelimesi ekleyiniz.

5. Adım: Dosyayı yeniden kaydediniz.

6. Adım: Dosyanın SHA-256 hash değerini tekrar hesaplayınız.

7. Adım: İlk ve ikinci hash değerlerini karşılaştırınız.

8. Adım: Dosya bütünlüğü açısından sonucu yorumlayınız.

İşlem	SHA-256 Değeri / Gözlem
Dosyanın ilk hâli	
Dosyada yapılan küçük değişiklik	
Dosyanın değiştirilmiş hâli	
Hash değerleri aynı mı?	
Dosya bütünlüğü açısından yorum	

Değerlendirme

Çalışmanız öğretmeniniz tarafından kontrol listesine göre değerlendirilecektir. Çalışmanızı yaparken buradaki ölçütleri dikkate alınız. Kontrol listesi formuna ulaşmak için karekodu okutunuz. Dijital yayınlarda karekodun üstüne tıklayarak içeriğe ulaşabilirsiniz.

6.3.2. MD5, SHA-1, SHA-256 ve SHA-512 Algoritmaları

Hash üretmek için farklı algoritmalar kullanılabilir. Bu algoritmaların bazıları eski ve zayıf kabul edilirken bazıları güncel kullanımlarda daha güçlü kabul edilir. MD5, SHA-1, SHA-256 ve SHA-512 karşılaştırması Tablo 6.13'te görülür.

Tablo 6.13: MD5, SHA-1, SHA-256 ve SHA-512 Karşılaştırması

Algoritma	Ürettiği Özet Uzunluğu	Güvenlik Durumu	Açıklama
MD5	128 bit	Güvenlik açısından zayıf kabul edilir.	Çakışma zafiyetleri nedeniyle güvenlik amaçlı kullanım için uygun değildir.
SHA-1	160 bit	Güvenlik açısından zayıf kabul edilir.	Çakışma riskleri nedeniyle güvenlik açısından önerilmez.
SHA-256	256 bit	Güncel kullanımlarda güçlü kabul edilen SHA-2 ailesindendir.	Dosya bütünlüğü gibi işlemlerde yaygın olarak kullanılır.
SHA-512	512 bit	Güncel kullanımlarda güçlü kabul edilen SHA-2 ailesindendir.	Daha uzun özet değeri üretir, kullanım amacına göre tercih edilebilir.

Çakışma

Çakışma, iki farklı verinin aynı hash değerini üretmesi durumudur. Güvenli hash algoritmalarında bu ihtimalin çok düşük olması beklenir. Örneğin iki farklı dosyanın aynı hash değerini üretmesi, dosya bütünlüğü açısından risk oluşturabilir. Bu nedenle MD5, SHA-1 gibi zayıflıkları bilinen algoritmalar güvenlik amaçlı işlemler için uygun kabul edilmez. SHA-256, SHA-512 gibi daha güçlü algoritmalar ise dosya bütünlüğü gibi işlemlerde daha güvenilir seçenekler olarak değerlendirilir.

4. UYGULAMA

Uygulama Adı	MD5, SHA-256 ve SHA-512 Hash Değerlerini Karşılaştırmak
Süre	30 dakika
Amaç	Verilen test dosyasının MD5, SHA-256 ve SHA-512 özet değerlerini online ve offline araçlarla hesaplamak ve çıktı uzunluklarını karşılaştırmak
Yönerge	Verilen test dosyasının MD5, SHA-256 ve SHA-512 hash değerlerini çevrim içi ve çevrim dışı araçlarla hesaplayınız. Elde ettiğiniz değerleri ve çıktı uzunluklarını karşılaştırarak ilgili tablolara yazınız. Yalnızca öğretmeninizin verdiği test dosyasını kullanınız.

Uygulama Adımları

A) Test Dosyasını Oluşturma

Aşağıdaki komutu çalıştırarak bir test dosyası oluşturunuz.

echo Bu bir test dosyasidir. > test_dosyasi.txt

Bu komut, yalnızca sınıf içi uygulamada kullanılmak üzere test_dosyasi.txt adlı örnek bir dosya oluşturur.

B) Online Araçla Hash Değerlerini Hesaplama

Öğretmeninizin belirlediği güvenli online hash hesaplama aracını açınız. Online araç dosya yükleme özelliği sunuyorsa test_dosyasi.txt dosyasını kullanınız. Araç yalnızca metin girişi kabul ediyorsa verilen test metnini dikkatli biçimde giriniz

Online araçta test dosyası veya test metni için **MD5**, **SHA-256** ve **SHA-512** hash değerlerini hesaplayınız. Elde ettiğiniz sonuçları aşağıdaki tabloya yazınız.

Kullanılan Araç	Algoritma	Elde Edilen Hash Değeri	Onaltılık Karakter Sayısı
Online hash aracı	MD5		
Online hash aracı	SHA-256		
Online hash aracı	SHA-512		

C) Offline Araçla Hash Değerlerini Hesaplama

Aynı test dosyasının hash değerlerini bu kez offline komut satırı aracıyla hesaplayınız.

MD5 hash değerini hesaplamak için aşağıdaki komutu çalıştırınız.

certutil -hashfile test_dosyasi.txt MD5

Elde ettiğiniz MD5 hash değerini tabloya yazınız.

SHA-256 hash değerini hesaplamak için aşağıdaki komutu çalıştırınız.

certutil -hashfile test_dosyasi.txt SHA256

Elde ettiğiniz SHA-256 hash değerini tabloya yazınız.

SHA-512 hash değerini hesaplamak için aşağıdaki komutu çalıştırınız.

certutil -hashfile test_dosyasi.txt SHA512

Elde ettiğiniz SHA-512 hash değerini tabloya yazınız.

Kullanılan Araç	Algoritma	Elde Edilen Hash Değeri	Onaltılık Karakter Sayısı
certutil	MD5		
certutil	SHA-256		
certutil	SHA-512		

Ç) Online ve Offline Sonuçları Karşılaştırma

Online araçla ve offline komutla elde ettiğiniz hash değerlerini karşılaştırınız.

Karşılaştırma Ölçütü	Gözlem
Online ve offline MD5 değerleri aynı mı?	
Online ve offline SHA-256 değerleri aynı mı?	
Online ve offline SHA-512 değerleri aynı mı?	
Aynı veri için aynı algoritma kullanıldığında sonuçlar neden aynı olmalıdır?	
Sonuçlar farklı çıktıysa bunun nedeni ne olabilir?	

D) Dosyada Küçük Bir Değişiklik Yapma

Test dosyasının sonuna kısa bir ifade ekleyiniz.

echo test >> test_dosyasi.txt

Ardından dosyanın SHA-256 değerini yeniden hesaplayınız.

certutil -hashfile test_dosyasi.txt SHA256

Elde ettiğiniz yeni SHA-256 değerini, değişiklikten önceki SHA-256 değeriyle karşılaştırınız.

Karşılaştırma Ölçütü	Değişiklikten Önce	Değişiklikten Sonra
SHA-256 hash değeri		
İki hash değeri aynı mı?		

E) Sonuçları Yorumlama

Hash değerlerinin uzunluklarını ve dosyada yapılan küçük değişikliğin SHA-256 sonucuna etkisini inceleyiniz. Aynı dosya için aynı algoritma kullanıldığında online ve offline araçlardan elde edilen sonuçların aynı olması beklenir. Sonuçlar farklı çıkarsa dosya içeriği, boşluk, satır sonu veya kullanılan veri girişi farklı olabilir.

Sorular

1. Aynı dosya için kullanılan farklı hash algoritmaları neden farklı uzunluklarda sonuçlar üretmiştir?

   .....
   .....

2. Online ve offline araçlarla elde edilen hash değerleri aynı çıktı mı? Cevabınızı açıklayınız.

   .....
   .....

3. Dosyaya yalnızca kısa bir ifade eklenmesi SHA-256 değerini nasıl etkilemiştir?

   .....
   .....

4. Hash değerleri dosya bütünlüğünü kontrol etmek için nasıl kullanılabilir?

   .....
   .....

5. MD5 algoritması neden günümüzde güvenli işlemler için önerilmemektedir?

   .....
   .....

Değerlendirme

Çalışmanız öğretmeniniz tarafından kontrol listesine göre değerlendirilecektir. Çalışmanızı yaparken buradaki ölçütleri dikkate alınız. Kontrol listesi formuna ulaşmak için karekodu okutunuz. Dijital yayınlarda karekodun üstüne tıklayarak içeriğe ulaşabilirsiniz.

6.3.3. Parola Saklama, Hashleme ve Salting

Parolalar, sistemlerde doğrudan açık hâlde saklanmamalıdır çünkü bir veri tabanı ele geçirilirse açık hâlde saklanan parolalar kolayca görülebilir. Parola güvenliğinde amaç, parolanın kendisini saklamak yerine paroladan üretilen hash değerini saklamaktır. Kullanıcı giriş yaptığında sistem, kullanıcının yazdığı paroladan tekrar hash değeri üretir ve kayıtlı hash değeriyle karşılaştırır ancak yalnızca hash kullanmak her zaman yeterli değildir. Aynı parolayı kullanan kişiler için aynı hash değeri üretilebilir. Bu durumu zorlaştırmak için salt kullanılır.

Salt, parolaya eklenen rastgele bir değerdir. Salt sayesinde aynı parola kullanılsa bile farklı hash değerleri oluşabilir. Saltın temel görevi, aynı parolaların aynı hash değerini üretmesini zorlaştırmaktır. Salt değeri gizli anahtar gibi düşünülmemelidir, parola hashleme sürecini güçlendiren ek bir rastgele değerdir.

Örnek Senaryo: Aynı Parola, Farklı Salt

Aşağıdaki örnek, parola saklamada salt değerinin neden kullanıldığını anlamak için hazırlanmıştır.

1. Kullanıcı A test parolası olarak **test123** ifadesini kullanmış olsun.
2. Kullanıcı B de aynı test ifadesini kullanmış olsun.
3. Salt kullanılmazsa aynı parola aynı hash değerini üretebilir. Bu durum, aynı parolayı kullanan hesapların fark edilmesini kolaylaştırabilir.
4. Her kullanıcı için farklı ve rastgele salt değeri eklendiğinde aynı parola farklı girdiler hâline gelir.

Örnek Mantık: test123 + SaltA → farklı hash değeri, test123 + SaltB → başka bir hash değeri.

Bu örnek, salt değerinin parolayı gizli bir anahtar gibi saklamak için değil aynı parolaların aynı hash değerine dönüşmesini zorlaştırmak için kullanıldığını gösterir.

Parola saklama mantığının adımları ve açıklamaları Tablo 6.14'te görülür.

Tablo 6.14: Parola Saklama Mantığı

Adım	Açıklama
1. Kullanıcı parola belirler.	**Örneğin Test Amaçlı:** ornek123
2. Sistem rastgele salt üretir.	**Örneğin:** X7pQ
3. Parola ve salt birlikte işlenir.	ornek123 + X7pQ
4. Hash değeri üretilir.	Ortaya özet değer çıkar.
5. Sistemde parola değil, hash ve salt bilgisi saklanır.	Parolanın açık hâli saklanmaz.

UYARI

Uygulamalarda gerçek kişisel parola, kimlik bilgisi, okul hesabı, e-posta parolası, özel metin veya hassas veri kullanılmamalıdır. Yalnızca verilen test metinleri, öğretmenin belirlediği örnek dosyalar veya sınıf içi kullanım için oluşturulan test verileri kullanılmalıdır.

6.3.4. Rainbow Table Mantığı

Rainbow table, çok sayıda yaygın parola ve bunlara karşılık gelen hash değerlerinden oluşan hazır liste gibi düşünülebilir. Amaç, bir hash değerinin hangi yaygın parolaya ait olabileceğini hızlıca tahmin etmektir. Örneğin çok yaygın kullanılan bir test metni her zaman aynı hash değerini üretirse bu hash değeri daha önce hazırlanmış listelerde bulunabilir. Bu nedenle yalnızca hash kullanmak her durumda yeterli olmayabilir. Salt, bu noktada önem kazanır. Aynı parola farklı salt değerleriyle işlendiğinde farklı hash çıktıları oluşabilir. Böylece hazır parola-hash listelerinin doğrudan işe yaraması zorlaşır (Tablo 6.15).

Tablo 6.15: Salt Kullanımının Hash Sonuçlarına Etkisi

Durum	Sonuç
Aynı test metni, salt kullanılmadan hashlenirse	Aynı hash değeri oluşabilir.
Aynı test metni, farklı salt değerleriyle hashlenirse	Farklı hash değerleri oluşabilir.
Hazır parola-hash listeleri kullanılırsa	Salt kullanılmayan zayıf yapılarda tahmin kolaylaşabilir.
Salt kullanılırsa	Aynı parolaların aynı hash değerini üretmesi zorlaşır.

6.3.5. Bcrypt, Scrypt ve Argon2 Mantığı

Parola saklama için sıradan hash algoritmaları her zaman yeterli değildir çünkü hızlı çalışan hash algoritmaları, saldırganların çok sayıda parola tahminini kısa sürede denemesine imkân verebilir. Bu nedenle parola hashleme için özel olarak geliştirilmiş yaklaşımlar kullanılır. Bcrypt, scrypt ve Argon2 bu amaçla kullanılan daha güvenli parola hashleme yaklaşımlarına örnek verilebilir. Bu yaklaşımların karşılaştırması Tablo 6.16'da görülür.

Tablo 6.16: Bcrypt, scrypt ve Argon2 Karşılaştırması

Yaklaşım	Kısa Açıklama
Bcrypt	Parola hashleme için yaygın kullanılan bir yöntemdir. İşlemi bilinçli olarak yavaşlatabilir.
Scrypt	Parola tahmin saldırılarını zorlaştırmak için işlem gücüyle birlikte bellek kullanımını da dikkate alır.
Argon2	Modern parola hashleme yaklaşımlarından biridir. Zaman ve bellek kullanımı ayarlanabilir.

Not: Belirtilen yöntemlerin ortak amacı, parolaların doğrudan saklanmasını önlemek ve parola tahmin denemelerini zorlaştırmaktır.

Salt kullanımının temel mantığı açıklandıktan sonra, bu yapının parola saklama süreçlerinde nasıl kullanıldığını gözlemlemek için bcrypt algoritması üzerinden uygulama yapılacaktır.

5. UYGULAMA

Uygulama Adı	Bcrypt ile Salt Kullanımını Gözlemlemek
Süre	30 dakika
Amaç	Aynı test ifadesini bcrypt algoritmasıyla birden fazla kez işlemek, farklı salt değerleri nedeniyle oluşan çıktıları karşılaştırmak ve parola doğrulama mantığını gözlemlemek
Yönerge	Aşağıdaki uygulama adımlarını tamamlayınız. Kendi parolanızı, okul hesabınıza ait bilgileri veya başka bir kişiye ait verileri kesinlikle kullanmayınız.

NOT: Uygulama öncesinde öğretmeniniz tarafından Python ortamı ve gerekli bcrypt kütüphanesi hazırlanacaktır.

Uygulama Adımları

A) Test Dosyasını Oluşturma

Bir metin düzenleyici açınız. Aşağıdaki kodu yazınız ve dosyayı bcrypt_test.py adıyla kaydediniz.

```
import bcrypt

test_ifadesi = b"ORNEK_PAROLA"

hash_1 = bcrypt.hashpw(test_ifadesi, bcrypt.gensalt())
hash_2 = bcrypt.hashpw(test_ifadesi, bcrypt.gensalt())

print("Birinci bcrypt ciktisi:")
print(hash_1.decode())
print("\nIkinci bcrypt ciktisi:")
print(hash_2.decode())
print("\nBirinci cikti ile dogrulama:")
print(bcrypt.checkpw(test_ifadesi, hash_1))
print("\nIkinci cikti ile dogrulama:")
print(bcrypt.checkpw(test_ifadesi, hash_2))
```

B) Python Dosyasını Çalıştırma

Komut satırını açınız. Dosyanın bulunduğu klasöre gidiniz ve aşağıdaki komutu çalıştırınız.

```
python bcrypt_test.py
```

C) Sonuçları Gözlemleme

Programın ürettiği iki bcrypt çıktısını aşağıdaki tabloya yazınız.

İncelenecek Alan	Birinci İşlem	İkinci İşlem
Kullanılan test ifadesi	ORNEK_PAROLA	ORNEK_PAROLA
Bcrypt çıktısı		
Çıktılar birbiriyle aynı mı?		
Doğrulama sonucu		

Ç) Sonuçları Yorumlama

Aynı test ifadesi kullanılmasına rağmen iki bcrypt çıktısının birbirinden farklı olup olmadığını kontrol ediniz. Ardından aşağıdaki soruları cevaplayınız.

Sorular

1. Aynı test ifadesi kullanılmasına rağmen bcrypt çıktıları neden farklı oluşmuştur?

   .....

   .....

   .....

2. Farklı çıktılar elde edilmesine rağmen doğrulama işlemleri neden başarılı olmuştur?

   .....

   .....

   .....

3. Salt kullanımı, aynı parolayı kullanan iki kişinin kayıtlarının karşılaştırılmasını neden zorlaştırır?

   .....

   .....

   .....

4. Parolaların doğrudan okunabilir metin biçiminde saklanması neden güvenli değildir?

   .....

   .....

   .....

5. Bu uygulamada gerçek parola kullanılmamasının nedeni nedir?

   .....

   .....

   .....

Değerlendirme

Çalışmanız öğretmeniniz tarafından kontrol listesine göre değerlendirilecektir. Çalışmanızı yaparken buradaki ölçütleri dikkate alınız. Kontrol listesi formuna ulaşmak için karekodu okutunuz. Dijital yayınlarda karekodun üstüne tıklayarak içeriğe ulaşabilirsiniz.

Hash fonksiyonları, verilen bir veriden sabit uzunlukta bir özet değer üretir. Veride yapılan küçük bir değişiklik, oluşan hash değerinin tamamen farklı görünmesine neden olabilir. Parola saklama süreçlerinde ise salt kullanımı, aynı test metninden veya aynı paroladan farklı hash değerleri elde edilmesine yardımcı olur.

3. ETKİNLİK

Etkinlik Adı	Hash Kullanım Alanlarını İncelemek
Süre	40 dakika
Amaç	Hash fonksiyonlarının farklı kullanım alanlarını incelemek, hashleme ile şifreleme arasındaki farkı açıklamak ve parola saklama süreçlerinde salt kullanımının önemini değerlendirmek
Yönerge	Sınıfta 3-4 kişilik gruplar oluşturunuz. Grubunuzla aşağıdaki durumlardan birini seçiniz. Seçtiğiniz durumu verilen sorular doğrultusunda inceleyiniz. Hash değerinin kullanım amacını, hashleme ile şifreleme arasındaki farkı ve uygun durumlarda salt kullanımının önemini değerlendiriniz. Ortak cevaplarınızı ilgili tabloya yazınız ve çalışmanızı sınıfta kısa bir sunumla paylaşınız.

İncelenecek Durumlar

- Bir yazılım dosyasının değiştirilip değiştirilmediğini kontrol etmek
- Öğrenci proje dosyasının aynı kalıp kalmadığını kontrol etmek
- Test amaçlı bir parolanın hash ve salt mantığıyla nasıl saklanabileceğini modellemek
- MD5, SHA-1, SHA-256 ve SHA-512 algoritmalarını karşılaştırmak

Etkinlik Adımları

1. Grubunuzla inceleyeceğiniz durumu seçiniz.
2. Seçtiğiniz durumun hash kavramıyla ilişkisini belirleyiniz.
3. Hashleme ile şifreleme arasındaki farkı grup içinde tartışınız.
4. Seçtiğiniz durumda salt kullanımının gerekli olup olmadığını değerlendiriniz.
5. MD5, SHA-1, SHA-256 ve SHA-512 algoritmalarını güvenlik açısından karşılaştırınız.
6. Aşağıdaki soruları grup içinde tartışınız.
7. Ortak cevaplarınızı tabloya yazınız.
8. Çalışmanızı sınıfta kısa bir sunumla paylaşınız.

Sorular

1. Seçtiğiniz durumda hash değeri ne işe yarar?
2. Hashleme ile şifreleme karıştırılırsa hangi yanlış anlaşılma oluşabilir?
3. Seçtiğiniz durumda salt kullanılması gerekir mi? Gerekçenizi yazınız.

4. MD5 veya SHA-1 bu işlem için güvenli kabul edilir mi? Neden?
5. SHA-256 veya SHA-512 hangi durumlarda daha uygun olabilir?

İncelenen Durum	Grubun Cevabı
Seçtiğimiz durum	
Hash değerinin kullanım amacı	
Hashleme ile şifreleme arasındaki fark	
Salt kullanımı gerekli mi? Gerekçesi	
MD5 ve SHA-1 hakkındaki değerlendirmemiz	
SHA-256 veya SHA-512 hakkındaki değerlendirmemiz	

Değerlendirme

Çalışmanız öğretmeninizin tarafından analitik dereceli puanlama anahtarına göre değerlendirilecektir. Çalışmanızı yaparken buradaki ölçütleri dikkate alınız. Analitik dereceli puanlama anahtarı formuna ulaşmak için karekodu okutunuz. Dijital yayınlarda karekodun üstüne tıklayarak içeriğe ulaşabilirsiniz.

Çalışmanızı tamamladıktan sonra grup değerlendirme formunu doldurarak grup üyelerinin çalışmaya katkı düzeylerini değerlendiriniz. Grup değerlendirme formuna ulaşmak için karekodu okutunuz. Dijital yayınlarda karekodun üstüne tıklayarak içeriğe ulaşabilirsiniz.

6.4. SİMETRİK KRİPTOGRAFİ

Simetrik kriptografi, aynı anahtarın hem şifreleme hem de şifre çözme işleminde kullanıldığı kriptografi türüdür. Bu yöntemde mesajı gönderen kişi ile mesajı alan kişinin aynı anahtarı bilmesi gerekir. Simetrik şifreleme yöntemleri genellikle hızlı çalışır. Bu nedenle dosya, metin veya veri şifreleme işlemlerinde kullanılabilir ancak bu yöntemde en önemli konu, anahtarın güvenli biçimde paylaşılması ve gizli tutulmasıdır. Anahtar yetkisiz kişilerin eline geçerse şifreli veri çözülebilir. Örneğin bir dosyayı şifrelemek için öğretmenin verdiği örnek bir test anahtarı kullanıldığında, bu dosyayı tekrar okunabilir hâle getirmek için de aynı test anahtarı gerekir.

6.4.1. Simetrik Şifrelemenin Çalışma Mantığı

Simetrik şifreleme sürecinde düz metin, belirlenen şifreleme algoritması ve gizli anahtar kullanılarak doğrudan okunamayan şifreli metne dönüştürülür. Şifreli verinin yeniden okunabilir hâle getirilmesi için şifreleme işleminde kullanılan anahtarın aynısı kullanılır. Bu nedenle anahtarın yalnızca yetkili kişiler tarafından bilinmesi, güvenli bir yolla paylaşılması ve gizli tutulması gerekir. Simetrik şifreleme algoritmaları hızlı çalıştıkları için dosya, disk ve ağ üzerinden aktarılan büyük miktardaki verilerin korunmasında tercih edilir. Ancak anahtarın yetkisiz kişilerin eline geçmesi durumunda şifreli veriler çözülebileceğinden yöntemin güvenliği büyük ölçüde anahtarın korunmasına bağlıdır.

BİLGİ KUTUSU

Tarih boyunca bilgileri gizlemek için farklı yöntemler geliştirilmiştir. Antik dönemlerde kullanılan Scytale, belirli kalınlıktaki bir çubuğun çevresine şerit sarılması ve mesajın bu şerit üzerine yazılması mantığına dayanır. Şerit çubuktan çıkarıldığında harflerin sırası bozulur ve mesaj doğrudan okunamaz. Mesajı okuyabilmek için benzer kalınlıktaki bir çubuğun kullanılması gerekir.

Scytale gibi tarihî yöntemler, şifreleme mantığını anlamak açısından önemlidir ancak günümüzdeki dijital verilerin korunması için yeterli değildir. Günümüzde bilgisayarlarda çok daha büyük miktardaki verilerin hızlı ve güvenli biçimde korunması gerekir. Bu nedenle AES gibi modern simetrik şifreleme algoritmaları kullanılmaktadır.

6. UYGULAMA

Uygulama Adı	Online Araç ve OpenSSL ile AES Simetrik Şifreleme
Süre	40 dakika
Amaç	Verilen test metnini online araç ve OpenSSL kullanarak AES algoritmasıyla şifrelemek, aynı test anahtarıyla yeniden çözmek, yanlış anahtar kullanımında ortaya çıkan sonucu gözlemlemek ve iki ortamda elde edilen sonuçları karşılaştırmak
Yönerge	Aşağıdaki uygulama adımlarını tamamlayınız. Bu uygulamada yalnızca verilen test metnini ve öğretmeninizin belirlediği test anahtarını kullanınız. Gerçek kişisel dosya, özel belge, okul hesabı bilgisi, e-posta parolası veya hassas veri kullanmayınız. Online araç kullanılırken yalnızca sınıf içi test verileriyle işlem yapılmalıdır.

Uygulama Adımları

A) Test Metnini ve Test Anahtarını Belirleme

Aşağıdaki test metnini kullanınız.

SISTEM VE AG GUVENLIGI

Aşağıdaki test anahtarını kullanınız.

ORNEK_TEST_ANAHTARI

Aşağıdaki tabloyu doldurunuz.

İncelenecek Alan	Bilgi
Kullanılan test metni	SISTEM VE AG GUVENLIGI
Kullanılan test anahtarı	ORNEK_TEST_ANAHTARI
Kullanılacak simetrik algoritma	AES

B) Online Araçla AES Şifreleme Yapma

Öğretmeninizin belirlediği güvenli online AES şifreleme aracını açınız. Online araçta yalnızca verilen test metnini ve test anahtarını kullanınız.

Online araçta şu işlemleri yapınız:

1. Test metnini ilgili alana yazınız.
2. Şifreleme yöntemi olarak AES seçiniz.
3. Test anahtarını ilgili alana yazınız.
4. Şifreleme işlemini başlatınız.
5. Oluşan şifreli metni aşağıdaki tabloya yazınız.

İşlem	Sonuç
Kullanılan online araç	
Kullanılan algoritma	AES
Kullanılan test metni	SISTEM VE AG GUVENLIGI
Kullanılan test anahtarı	ORNEK_TEST_ANAHTARI
Oluşan şifreli metin	

C) Online Araçla Şifre Çözme Yapma

Online araçta bu kez şifre çözme işlemini seçiniz. Bir önceki adımda elde ettiğiniz şifreli metni ve aynı test anahtarını kullanarak şifre çözme işlemini yapınız.

İşlem	Sonuç
Şifre çözmede kullanılan anahtar	ORNEK_TEST_ANAHTARI
Çözülen metin	
Çözülen metin ilk test metniyle aynı mı?	

Ç) OpenSSL İçin Test Dosyası Oluşturma

Komut satırını açınız. Aşağıdaki komutu çalıştırarak bir test dosyası oluşturunuz.

echo SISTEM VE AG GUVENLIGI > simetrik_test.txt

Dosyanın içeriğini kontrol etmek için aşağıdaki komutu çalıştırınız.

```
type simetrik_test.txt
```

D) OpenSSL ile AES Şifreleme Yapma

Aşağıdaki komutu kullanarak test dosyasını AES-256-CBC yöntemiyle şifreleyiniz.

openssl enc -aes-256-cbc -salt -pbkdf2 -in simetrik_test.txt -out simetrik_test.enc -pass

pass: ORNEK_TEST_ANAHTARI

Bu komuttan sonra simetrik_test.enc adlı şifreli dosya oluşacaktır. Şifreli dosya doğrudan okunabilir bir metin gibi görünmeyebilir.

Aşağıdaki tabloyu doldurunuz.

İncelenecek Alan	Cevap
Kullanılan araç	OpenSSL
Kullanılan algoritma	AES-256-CBC
Kullanılan giriş dosyası	simetrik_test.txt
Oluşan şifreli dosya	simetrik_test.enc
Şifreli dosya doğrudan okunabiliyor mu?	

E) OpenSSL ile Şifre Çözme Yapma

Şifreli dosyayı aynı test anahtarıyla tekrar çözmek için aşağıdaki komutu çalıştırınız.

openssl enc -d -aes-256-cbc -pbkdf2 -in simetrik_test.enc -out simetrik_test_cozulmus.txt -pass

pass: ORNEK_TEST_ANAHTARI

Çözülen dosyanın içeriğini görmek için aşağıdaki komutu çalıştırınız.

type simetrik_test_cozulmus.txt

Aşağıdaki tabloyu doldurunuz.

İşlem	Sonuç
Şifre çözmede kullanılan anahtar	ORNEK_TEST_ANAHTARI
Çözülen dosya	simetrik_test_cozulmus.txt
Çözülen metin ilk test metniyle aynı mı?	

F) Yanlış Anahtarla Şifre Çözmeyi Deneme

Bu kez yanlış bir test anahtarı kullanarak şifre çözmeyi deneyiniz.

openssl enc -d -aes-256-cbc -pbkdf2 -in simetrik_test.enc -out yanlis_anahtar.txt -pass

pass:YANLIS_ANAHTAR

Aşağıdaki tabloyu doldurunuz.

İncelenecek Alan	Gözlem
Yanlış anahtarla dosya doğru çözüldü mü?	
Hata mesajı veya okunamayan çıktı oluştu mu?	
Bu durum simetrik şifrelemede anahtarın önemini nasıl gösterir?	

G) Online Araç ve OpenSSL Sonuçlarını Karşılaştırma

Online araçla ve OpenSSL ile yaptığınız işlemleri karşılaştırınız.

Karşılaştırma Ölçütü	Online Araç	OpenSSL
Kullanılan veri		
Kullanılan test anahtarı		
Şifreleme yapılabildi mi?		
Aynı anahtarla şifre çözme yapılabildi mi?		
Yanlış anahtar kullanıldığında doğru sonuç elde edildi mi?		

Not: Online araçla ve OpenSSL ile elde edilen şifreli çıktılar birebir aynı olmayabilir. Bunun nedeni kullanılan araç ayarları, şifreleme modu, salt veya başlangıç değeri gibi teknik farklılıklar olabilir. Bu uygulamada asıl amaç, simetrik şifrelemede aynı anahtarın hem şifreleme hem de şifre çözme işleminde kullanıldığını gözlemlemektir.

Sonuç Soruları

1. AES neden simetrik şifreleme algoritması olarak değerlendirilir?

   .....
   .....

2. Aynı test anahtarı kullanıldığında şifreli dosya neden tekrar okunabilir hâle gelmiştir?

   .....
   .....

3. Yanlış anahtar kullanıldığında dosyanın doğru çözülememesi neyi gösterir?

   .....
   .....

4. Online araç kullanırken neden gerçek parola, kişisel bilgi veya özel dosya kullanılmamalıdır?

   .....
   .....

5. Online araç ve OpenSSL ile elde edilen şifreli çıktıların birebir aynı olmaması hangi nedenlerden kaynaklanabilir?

   .....
   .....

Değerlendirme

Çalışmanız öğretmeniniz tarafından kontrol listesine göre değerlendirilecektir. Çalışmanızı yaparken buradaki ölçütleri dikkate alınız. Kontrol listesi formuna ulaşmak için karekodu okutunuz. Dijital yayınlarda karekodun üstüne tıklayarak içeriğe ulaşabilirsiniz.

6.4.2. DES, 3DES, AES ve RC4 Algoritmaları

Simetrik kriptografide farklı algoritmalar kullanılmıştır. Bazıları tarihsel ve öğretici örneklerdir, bazıları ise bugün daha yaygın ve güçlü kabul edilir. DES, 3DES, AES ve RC4 karşılaştırması Tablo 6.17'de görülür.

Tablo 6.17: DES, 3DES, AES ve RC4 Karşılaştırması

Algoritma	Türü	Güncel Durumu	Kısa Açıklama
DES	Blok şifreleme	Modern güvenlik için yetersiz kabul edilir.	Tarihsel açıdan önemlidir, ancak anahtar uzunluğu günümüz için zayıf kalmıştır.
3DES	Blok şifreleme	Artık modern sistemlerde tercih edilmez.	DES'in üç kez uygulanması mantığına dayanır. DES'e göre daha güçlü olsa da güncel kullanım için önerilmez.
AES	Blok şifreleme	Günümüzde yaygın ve güçlü kabul edilir.	Farklı anahtar uzunluklarıyla kullanılabilir. Birçok güvenlik sisteminde tercih edilir.
RC4	Akış şifreleme	Güvenlik zayıflıkları nedeniyle önerilmez.	Eski sistemlerde kullanılmıştır, modern güvenlikte tercih edilmemelidir.

BİLGİ KUTUSU

Simetrik şifreleme yöntemleri genel olarak iki farklı yaklaşımla incelenebilir. **Blok şifreleme**, veriyi belirli büyüklükteki parçalar hâlinde işler. AES bu gruba örnek verilebilir. **AES**, veriyi 128 bitlik bloklar hâlinde işleyen bir blok şifreleme algoritmasıdır. AES-128, AES-192 ve AES-256 ifadeleri ise blok boyutunu değil kullanılan anahtar uzunluğunu gösterir. **Akış şifreleme** ise veriyi daha küçük birimler hâlinde, akış gibi işleme mantığına dayanır. RC4 eski bir akış şifreleme örneğidir ancak güvenlik zayıflıkları nedeniyle modern sistemlerde önerilmez.

Blok şifreleme ile akış şifrelemenin temel özellikleri Tablo 6.18'de karşılaştırılmıştır.

Tablo 6.18: Blok Şifreleme ve Akış Şifrelemenin Karşılaştırılması

Özellik	Blok Şifreleme	Akış Şifreleme
Çalışma mantığı	Veri bloklar hâlinde işlenir.	Veri akış gibi parça parça işlenir.
Örnek	AES	RC4
Güvenlik durumu	Doğru ayarlarla güçlü olabilir.	RC4 gibi eski örnekler önerilmez.
Öğrenme amacı	Modern simetrik şifrelemeyi anlamaya yardımcı olur.	Akış şifreleme mantığını tanımaya yardımcı olur.

NOT: AES güçlü kabul edilen simetrik şifreleme algoritmalarından biridir ancak tek başına mutlak güvenlik sağlamaz. Güvenli kullanım; güçlü anahtar seçimi, anahtarın gizli tutulması ve aracın doğru ayarlarla kullanılmasına bağlıdır.

6.4.3. AES ile Simetrik Şifreleme Mantığı

AES, bugün yaygın ve güçlü kabul edilen simetrik şifreleme algoritmalarından biridir. AES, veriyi belirli büyüklükteki bloklar hâlinde işler. Bu nedenle blok şifreleme algoritması olarak adlandırılır. AES farklı anahtar uzunluklarıyla kullanılabilir. Örneğin AES-128, AES-192 ve AES-256 ifadeleri, kullanılan anahtar uzunluğunu gösterir. Anahtar uzunluğu arttıkça güvenlik seviyesi de artabilir ancak güvenlik yalnızca anahtar uzunluğuna bağlı değildir.

Örnek Senaryo: Simetrik Anahtarın Korunması

Bir öğrenci, öğretmeninin verdiği test_notu.txt adlı örnek dosyayı AES ile şifrelemek ister. Bunun için öğretmenin belirlediği bir test anahtarı kullanılır. Dosya şifrelendiğinde içeriği doğrudan okunamaz. Aynı dosyanın tekrar okunabilir hâle gelmesi için aynı test anahtarı gerekir ancak test anahtarı başkasıyla paylaşılırsa o kişi de şifreli dosyayı çözebilir. Bu nedenle simetrik şifrelemede yalnızca algoritmanın güçlü olması yeterli değildir. Anahtarın gizli tutulması da gerekir. AES ile simetrik şifreleme senaryosunun aşamaları Tablo 6.19'da verilmiştir.

Tablo 6.19: AES ile Simetrik Şifreleme Senaryosunun Aşamaları

Aşama	Açıklama
Düz dosya	test_notu.txt
Kullanılan yöntem	AES ile simetrik şifreleme
Anahtar	Öğretmenin verdiği örnek test anahtarı
Şifreli dosya	test_notu.enc
Şifre çözme	Aynı test anahtarıyla yapılır.

7. UYGULAMA

Uygulama Adı	Test Dosyasını Simetrik Yöntemle Şifreleme ve Çözme
Süre	30 dakika
Amaç	Verilen test dosyasını simetrik şifreleme yöntemiyle şifrelemek ve aynı test anahtarıyla tekrar çözmek
Yönerge	Aşağıdaki uygulama adımlarını öğretmen rehberliğinde tamamlayınız. Verilen test dosyasını kullanarak simetrik şifreleme işlemini gerçekleştiriniz. Şifrelenmiş dosyayı aynı test anahtarıyla tekrar çözünüz. Daha sonra doğru ve yanlış test anahtarı kullanıldığında ortaya çıkan sonuçları gözlemleyiniz. Şifreleme ve şifre çözme işlemlerinden elde ettiğiniz sonuçları ilgili tabloya yazınız.

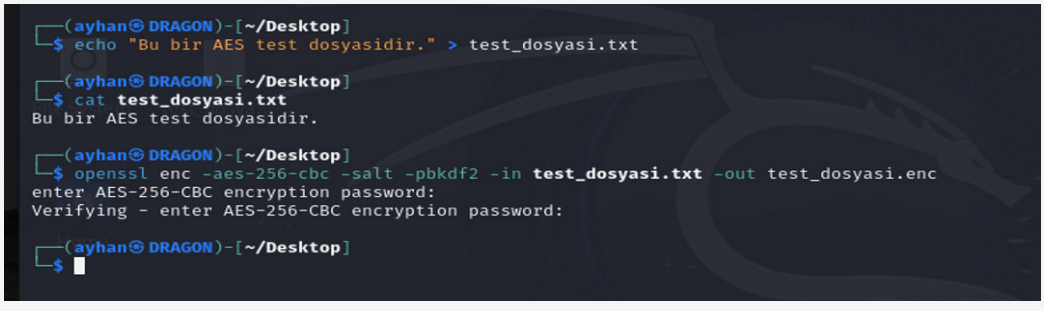
Uygulama Adımları

A) Test Dosyasını Şifreleme

Öğretmeninizin verdiği test_dosyasi.txt adlı test dosyasını kullanınız. Dosyayı AES-256-CBC yöntemiyle şifrelemek için aşağıdaki komutu çalıştırınız (Görsel 6.7).

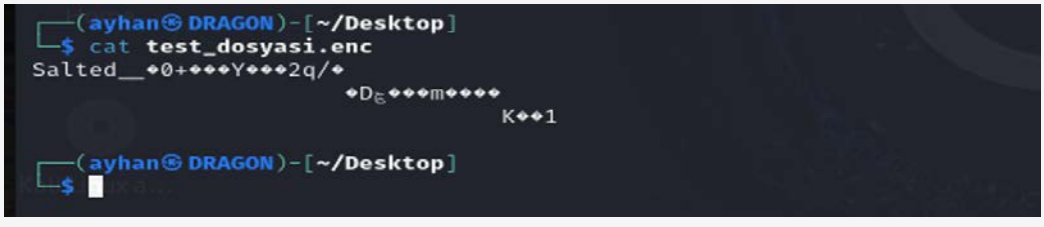
```
openssl enc -aes-256-cbc -salt -pbkdf2 -in test_dosyasi.txt -out test_dosyasi.enc
```

Bu komut, test_dosyasi.txt adlı test dosyasını şifreleyerek test_dosyasi.enc adlı şifreli dosyayı oluşturur. Komut çalıştırıldığında sizden test anahtarı veya geçiş ifadesi girmeniz istenebilir.



Görsel 6.7: Test dosyasını şifreleme

Şifreli dosyanın içeriğini doğrudan okumayı deneyiniz. Anlamlı bir metin yerine okunması güç karakterler veya anlamsız bir çıktı görülmesi beklenir (Görsel 6.8).



Görsel 6.8: Şifrelenmiş metin

B) Şifreli Dosyayı Çözme

Şifreli dosyayı çözmek için aşağıdaki komutu çalıştırınız (Görsel 6.9).

```
openssl enc -d -aes-256-cbc -pbkdf2 -in test_dosyasi.enc -out test_dosyasi_cozulmus.
txt
```

Bu komut, test_dosyasi.enc adlı şifreli dosyayı doğru test anahtarıyla tekrar okunabilir hâle getirerek test_dosyasi_cozulmus.txt adlı dosyayı oluşturur. Komut çalıştırıldığında şifreleme işleminde kullandığınız örnek test anahtarını giriniz.



Görsel 6.9: Şifreli dosyayı çözme

C) Sonuçları Karşılaştırma

1. test_dosyasi.enc adlı şifreli dosyanın doğrudan okunup okunamadığını kontrol ediniz.
2. Doğru test anahtarıyla oluşturulan test_dosyasi_cozulmus.txt dosyasını açınız.
3. Çözülen dosyanın içeriğini ilk test dosyasıyla karşılaştırınız.
4. Öğretmeninizin yönergesine göre yanlış bir test anahtarı kullanarak çözme işlemini tekrar deneyiniz.
5. Yanlış test anahtarı kullanıldığında işlemin başarısız olup olmadığını veya anlamlı bir çıktı oluşup oluşmadığını gözlemleyiniz.

Bulgularınızı aşağıdaki tabloya yazınız.

Kontrol Sorusu	Gözlem
Şifreli dosya doğrudan okunabiliyor mu?	
Doğru test anahtarıyla dosya tekrar çözülebiliyor mu?	
Çözülen dosyanın içeriği ilk test dosyasıyla aynı mı?	
Yanlış test anahtarı kullanıldığında işlem başarılı oluyor mu?	
Yanlış test anahtarı kullanıldığında anlamlı bir çıktı oluşuyor mu?	

Sorular

1. Simetrik şifrelemede aynı anahtarın hem şifreleme hem de şifre çözme işleminde kullanılması ne anlama gelir?

   .....
   .....

2. Şifreleme anahtarının yetkisiz kişilerin eline geçmesi hangi riski oluşturur?

   .....
   .....

3. Yanlış test anahtarı kullanıldığında dosyanın doğru biçimde çözülememesi neden önemlidir?

   .....
   .....

4. Şifreli dosya ile hash değeri aynı şey midir? Neden?

   .....
   .....

Değerlendirme

Çalışmanız öğretmeniniz tarafından kontrol listesine göre değerlendirilecektir. Çalışmanızı yaparken buradaki ölçütleri dikkate alınız. Kontrol listesi formuna ulaşmak için karekodu okutunuz. Dijital yayınlarda karekodun üstüne tıklayarak içeriğe ulaşabilirsiniz.

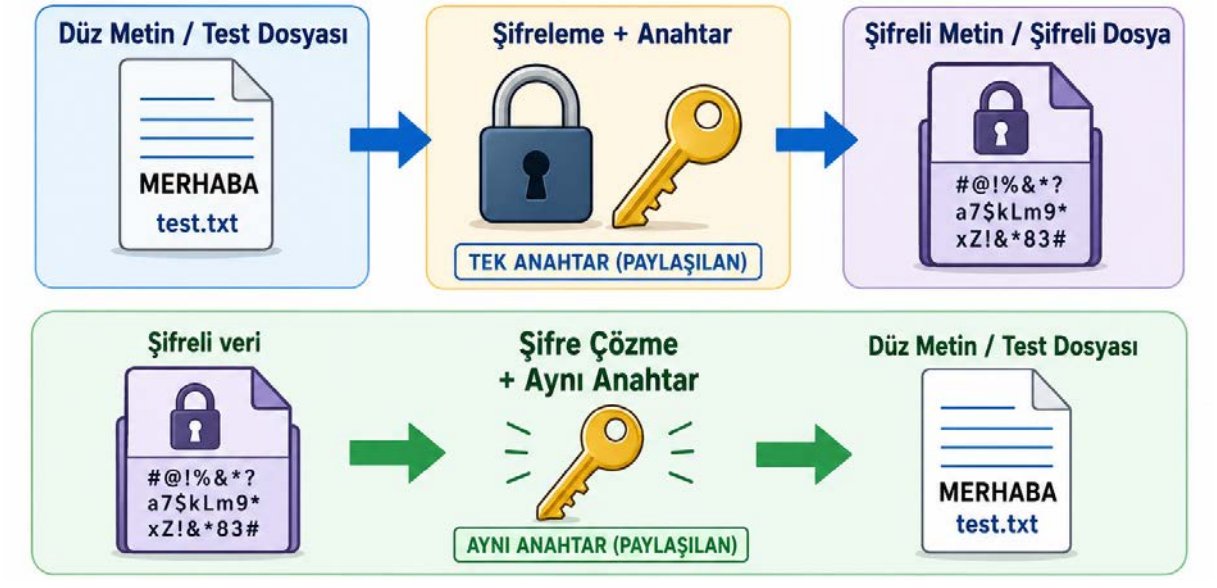
6.4.4. Simetrik Şifreleme Yöntemlerini Karşılaştırma

Simetrik şifreleme algoritmaları kullanım amaçlarına, hızlarına, güvenlik düzeylerine ve güncelliklerine göre farklılık gösterebilir. Simetrik şifreleme yöntemlerinin karşılaştırması Tablo 6.20'de görülür.

Tablo 6.20: Simetrik Şifreleme Yöntemlerini Karşılaştırma

Karşılaştırma Ölçütü	DES	3DES	AES	RC4
Genel tür	Blok şifreleme	Blok şifreleme	Blok şifreleme	Akış şifreleme
Günümüzde kullanım durumu	Tarihsel / Öğretici	Eski / Tercih edilmez.	Yaygın ve güçlü	Eski / Önerilmez.
Güvenlik durumu	Zayıf kabul edilir.	Güncel kullanım için uygun değildir.	Güçlü kabul edilir, doğru kullanım ayarları önemlidir.	Zayıflıkları bilinir.
Öğrenme açısından önemi	Simetrik şifrelemenin tarihsel gelişimini gösterir.	DES'in geliştirilmiş eski biçimini gösterir.	Modern simetrik şifrelemeyi anlamaya yardımcı olur.	Eski akış şifreleme örneğidir.

Simetrik şifrelemede tek anahtar mantığı Görsel 6.10'da gösterilmiştir.



Görsel 6.10: Simetrik şifrelemede tek anahtar mantığı

SIRA SİZDE

Aşağıdaki çalışmaları bireysel olarak tamamlayınız.

A) Kavramları Ayırt Edelim

Aşağıdaki durumları okuyunuz. Her durumla ilişkili kavramı **İlgili Kavram** sütununa, seçiminizin nedenini ise **Gerekçe** sütununa yazınız.

Kullanılacak Kavramlar: simetrik şifreleme, anahtar, şifreleme, şifre çözme, AES

Durum	İlgili Kavram	Gerekçe
Aynı anahtarın hem veriyi şifrelemek hem de şifreli veriyi çözmek için kullanılması		
Düz metnin okunamaz hâle getirilmesi		
Şifreli metnin doğru anahtarla tekrar okunabilir hâle getirilmesi		
Bugün yaygın kullanılan güçlü simetrik şifreleme algoritmalarından biri		
Şifreleme ve şifre çözme işlemlerinde kullanılan gizli bilgi		

B) Hashleme mi, Simetrik Şifreleme mi?

Aşağıdaki durumları okuyunuz. Hangi durumun hashleme veya simetrik şifrelemeyle ilişkili olduğunu belirleyiniz. Seçiminizi **Hashleme / Simetrik Şifreleme** sütununa, seçiminizin nedenini ise **Gerekçe** sütununa yazınız.

Durum	Hashleme / Simetrik Şifreleme	Gerekçe
Bir dosyanın değiştirilip değiştirilmediğini kontrol etmek		
Bir dosyayı doğru anahtarla tekrar açılabilecek şekilde gizlemek		
Veriden tek yönlü özet değer üretmek		
Aynı anahtarla şifreleme ve şifre çözme işlemlerini yapmak		

6.5. ASİMETRİK KRİPTOGRAFİ

Simetrik kriptografide aynı anahtar hem şifreleme hem de şifre çözme için kullanılır. **Asimetrik kriptografi**de ise birbiriyle ilişkili iki anahtar kullanılır. Bunlar **açık anahtar (public key)** ve **gizli anahtar (private key)** olarak adlandırılır. Açık anahtar paylaşılabilir. Gizli anahtar ise yalnızca sahibinde bulunmalı ve kesinlikle gizli tutulmalıdır. Bu yapı, güvenli iletişimde ve anahtar paylaşımı problemini azaltmada önemli bir rol oynar.

Asimetrik kriptografide açık anahtarla yapılan bir işlem, ilişkili gizli anahtar olmadan geri çözülemez ancak gerçek sistemlerde güvenlik yalnızca algoritmanın adına bağlı değildir. Doğru algoritma, doğru anahtar uzunluğu, güvenli dolgulama / yapılandırma ve güvenilir uygulama ayarları birlikte değerlendirilmelidir.

Açık Anahtar ve Gizli Anahtar Mantığı

Asimetrik kriptografide açık anahtar ve gizli anahtar arasındaki ilişki, günlük yaşamdan bir posta kutusu örneğiyle açıklanabilir. Bir posta kutusuna herkes mektup bırakabilir ancak kutunun içindeki mektuplara

yalnızca anahtarı bulunan kişi ulaşabilir. Bu örnekte posta kutusuna mektup bırakma imkânı açık anahtara, kutuyu açmak için kullanılan anahtar ise gizli anahtara benzetilebilir. Açık anahtar ve gizli anahtar arasındaki ilişki Tablo 6.21'de verilmiştir.

Tablo 6.21: Açık Anahtar ve Gizli Anahtar Benzetmesi

Günlük Yaşam Benzetmesi	Asimetrik Kriptografide Karşılığı
Herkesin mektup bırakabildiği posta kutusu	Açık anahtar
Kutuyu yalnızca sahibinin açabilmesi	Gizli anahtar
Mektubun kutuya bırakılması	Açık anahtarla koruma işlemi
Kutunun sahibi tarafından açılması	Gizli anahtarla çözme işlemi

Bu benzetme, asimetrik kriptografinin temel mantığını anlamaya yardımcı olur. Gerçek kriptografik sistemlerde ise bu işlemler matematiksel algoritmalarla gerçekleştirilir.

BİLGİ KUTUSU

Açık anahtar gerçekten doğru kişiye mi ait?

Asimetrik kriptografide açık anahtar paylaşılabilir. Ancak önemli olan, kullanılan açık anahtarın gerçekten doğru kişiye veya kuruma ait olduğundan emin olmaktır. Yanlış kişiye ait bir açık anahtar kullanılırsa, gönderilen veri istenmeyen bir kişi tarafından çözülebilecek şekilde korunmuş olabilir.

Simetrik ve Asimetrik Kriptografi Arasındaki Fark

Simetrik ve asimetrik kriptografi birbirine karıştırılmamalıdır. İki yöntemde de amaç bilgiyi güvenli biçimde korumaktır ancak kullanılan anahtar yapısı farklıdır (Tablo 6.22).

Tablo 6.22: Simetrik ve Asimetrik Kriptografi Karşılaştırması

Özellik	Simetrik Kriptografi	Asimetrik Kriptografi
Anahtar yapısı	Tek anahtar kullanılır.	Açık anahtar ve gizli anahtar çifti kullanılır.
Şifreleme / çözme	Aynı anahtar kullanılır.	Açık anahtar ve gizli anahtar birlikte çalışır.
Anahtar paylaşımı	Anahtarın güvenli paylaşılması gerekir.	Açık anahtar paylaşılabilir; gizli anahtar saklanır.
Hız	Genellikle daha hızlıdır.	Genellikle daha yavaştır.
Kullanım amacı	Büyük veri veya dosya şifrelemede kullanışlıdır.	Anahtar paylaşımı, güvenli iletişim ve kimlik doğrulama süreçlerinde önemli rol oynar.

BİLGİ KUTUSU

Hashleme de kriptografiyle ilişkilidir ancak hashleme şifreleme değildir. Hashleme tek yönlü özet üretir. Simetrik ve asimetrik şifrelemede ise uygun anahtarlarla verinin korunması veya tekrar okunabilir hâle getirilmesi söz konusudur.

RSA Algoritmasının Temel Mantığı

RSA, asimetrik kriptografi denildiğinde sık karşılaşılan algoritmalardan biridir. RSA'da bir açık anahtar ve bir gizli anahtar bulunur. RSA'nın temel mantığı şu şekilde özetlenebilir:

1. Bir anahtar çifti oluşturulur.
2. Açık anahtar paylaşılabilir.
3. Gizli anahtar yalnızca sahibinde kalır.
4. Açık anahtarla korunan veri, ilişkili gizli anahtar olmadan çözülemez.
5. Gizli anahtar güvenli biçimde saklanmalıdır.

BİLGİ KUTUSU

Şifreleme tek başına kimliği garanti etmez.

Bir verinin şifrelenmiş olması, o verinin kesin olarak doğru kişi veya kurumdan geldiğini tek başına göstermez. Güvenli sistemlerde verinin korunmasının yanında, gönderen tarafın doğrulanması ve verinin değiştirilmediğinin kontrol edilmesi de önemlidir.

RSA İçin Örnek Senaryo

Ali, kendisine güvenli bir test mesajı gönderilmesini istesin. Ali bir açık anahtar ve gizli anahtar çifti oluşturur. Açık anahtarını arkadaşlarıyla paylaşır. Gizli anahtarını ise kimseyle paylaşmaz. Tablo 6.23'te RSA ile ilgili örnek bir senaryo verilmiştir.

Tablo 6.23: RSA İçin Örnek Senaryo

Aşama	Açıklama
Ali anahtar çifti oluşturur.	Açık anahtar ve gizli anahtar oluşur.
Ali açık anahtarını paylaşır.	Arkadaşları bu anahtarı kullanabilir.
Arkadaşı test mesajını açık anahtarla korur.	Mesaj doğrudan okunamaz hâle gelir.
Ali mesajı gizli anahtarıyla çözer.	Mesajı yalnızca gizli anahtara sahip olan Ali okuyabilir.

Gerçek sistemlerde RSA gibi asimetrik kriptografi yöntemleri; doğru algoritma seçimi, uygun anahtar uzunluğu, güvenli yapılandırma ve güvenilir uygulama ayarlarıyla birlikte değerlendirilmelidir. Bu nedenle "RSA kullanıldıysa her durumda kesin güvenlidir." şeklinde düşünülmemelidir.

Diffie-Hellman Anahtar Değişimi

Diffie-Hellman, doğrudan mesaj şifreleme algoritması gibi düşünülmemelidir. Diffie-Hellman, mesajın kendisini

şifrelemek için değil iki tarafın ortak gizli anahtar oluşturabilmesi için kullanılır. Diffie-Hellman'ın amacı, iki kişinin herkesin görebileceği bir ortamda bazı bilgileri paylaşarak sonunda yalnızca kendilerinin bildiği ortak bir gizli değer oluşturabilmesidir. Diffie-Hellman'ın temel fikri, iki tarafın ortak bir gizli değer oluşturmasıdır. Burada önemli nokta, tarafların gizli bilgilerini doğrudan karşı tarafa göndermemesidir (Tablo 6.24). Basit bir benzetmeyle açıklanacak olursa Ali ve Zeynep herkesin bildiği ortak bir başlangıç bilgisi kullanır. Ali kendi gizli bilgisini, Zeynep kendi gizli bilgisini bu başlangıç bilgisiyle birleştirir. Daha sonra bazı ara bilgiler paylaşılır. Dışarıdan bakan biri bu ara bilgileri görebilir, ancak Ali'ye ve Zeynep'e ait olan gizli bilgileri bilmediği için son ortak gizli değeri kolayca elde edemez. Bu ortak gizli değer, daha sonra simetrik şifreleme için kullanılabilecek bir oturum anahtarının oluşturulmasına yardımcı olabilir.

BİLGİ KUTUSU

Diffie-Hellman doğrudan mesaj şifreleme yöntemi değildir. Mesajın kendisini şifrelemek için değil iki tarafın ortak gizli anahtar oluşturabilmesi için kullanılır.

Tablo 6.24: Diffie-Hellman Günlük Yaşam Benzetmesi

Benzetme	Diffie-Hellman'daki Karşılığı
Ortak başlangıç rengi	Herkesin bildiği ortak bilgi
Her öğrencinin gizli rengi	Her tarafın gizli bilgisi
Karıştırılmış ara renkler	Paylaşılan ara değerler
Son ortak renk	Ortak gizli anahtar

ECC Algoritmasının Temel Mantığı

ECC, açılımı "Elliptic Curve Cryptography" olan modern bir asimetrik kriptografi yaklaşımıdır. Türkçede Eliptik Eğri Kriptografisi olarak ifade edilebilir.

ECC, uygun şekilde kullanıldığında daha kısa anahtarlarla güçlü güvenlik sağlayabilen modern bir asimetrik kriptografi yaklaşımıdır. Bu nedenle bazı sistemlerde daha az işlem gücü ve daha küçük anahtarlarla güvenli yapıların kurulmasına yardımcı olabilir. Bilinmesi gereken temel nokta şudur: ECC de açık anahtar ve gizli anahtar mantığına dayanan asimetrik kriptografi yaklaşımlarından biridir.

BİLGİ KUTUSU

ECC, eliptik eğri kriptografisi anlamına gelir. ECC ailesinde farklı amaçlarla kullanılan yaklaşımlar bulunur.

Kavram	Kısa Açıklama
ECDH	Eliptik eğri temelli anahtar değişimi yaklaşımıdır. Diffie-Hellman fikrinin ECC ile kullanılan türü olarak düşünülebilir.
ECDSA	Eliptik eğri temelli dijital imza yaklaşımıdır. Dijital imza oluşturma ve doğrulama süreçleriyle ilişkilidir.

Bilinmesi gereken temel nokta şudur: ECC uygun şekilde kullanıldığında daha kısa anahtarlarla güçlü güvenlik sağlayabilen modern bir asimetrik kriptografi yaklaşımıdır ancak hiçbir yöntem tek başına mutlak güvenlik sağlamaz.

BİLGİ KUTUSU

Gerçek sistemlerde simetrik ve asimetrik şifreleme yöntemleri çoğu zaman birlikte kullanılır. Bunun nedeni, simetrik şifrelemenin büyük miktardaki verileri şifrelemede hızlı olması; asimetrik şifrelemenin ise anahtar paylaşımı sorununu azaltmaya yardımcı olmasıdır.

Örneğin bir dosya AES ile şifrelenebilir. AES için kullanılan anahtar ise alıcının açık anahtarıyla RSA kullanılarak korunabilir. Alıcı, kendi gizli anahtarıyla AES anahtarını elde eder ve dosyayı AES ile çözer. Bu yaklaşımda RSA, dosyanın tamamını doğrudan şifrelemek için kullanılmaz. RSA'nın görevi, AES anahtarının güvenli biçimde iletilmesine yardımcı olmaktır. Dosyanın şifrelenmesi ve çözülmesi işlemlerinde ise AES kullanılır.

8. UYGULAMA

Uygulama Adı	Küçük Test Mesajını Açık Anahtarla Şifreleyip Gizli Anahtarla Çözmek
Süre	30 dakika
Amaç	Asimetrik kriptografide açık anahtar ve gizli anahtar ilişkisinin temel mantığını küçük bir test mesajı üzerinde gözlemlemek; doğru ve yanlış test anahtarı kullanıldığında ortaya çıkan sonuçları karşılaştırmak
Yönerge	Aşağıdaki uygulama adımlarını öğretmen rehberliğinde tamamlayınız. İşlem sırasında yalnızca öğretmeninizin verdiği kısa test mesajını ve sınıf içi uygulama için oluşturulan test anahtarlarını kullanınız. Gözlemlerinizi ilgili tabloya yazınız ve sonuç sorularını cevaplayınız.

Uygulama Adımları

A) Test Anahtar Çiftini Oluşturma

Aşağıdaki komutla sınıf içi uygulamada kullanılacak test gizli anahtarını oluşturunuz.

openssl genpkey -algorithm RSA -pkeyopt rsa_keygen_bits:2048 -out test_gizli_anahtar.pem

Bu komut, test amacıyla bir RSA gizli anahtarı oluşturur.

Aşağıdaki komutla gizli anahtarla ilişkili açık anahtarı oluşturunuz.

openssl rsa -in test_gizli_anahtar.pem -pubout -out test_acik_anahtar.pem

Bu komut, test gizli anahtarından ilişkili açık anahtarı üretir.

B) Küçük Test Mesajını Oluşturma

Öğretmeninizin belirlediği kısa test mesajını kullanınız. Gerekli durumlarda aşağıdaki komutla örnek bir test mesajı oluşturabilirsiniz.

echo MERHABA > test_mesaj.txt

Bu mesaj yalnızca sınıf içi uygulama amacıyla kullanılmalıdır. Gerçek kişisel bilgi yazılmamalıdır.

C) Test Mesajını Açık Anahtarla Şifreleme

Aşağıdaki komutla test mesajını açık anahtar kullanarak şifreleyiniz.

openssl pkeyutl -encrypt -pubin -inkey test_acik_anahtar.pem -in test_mesaj.txt -out test_mesaj.sifreli

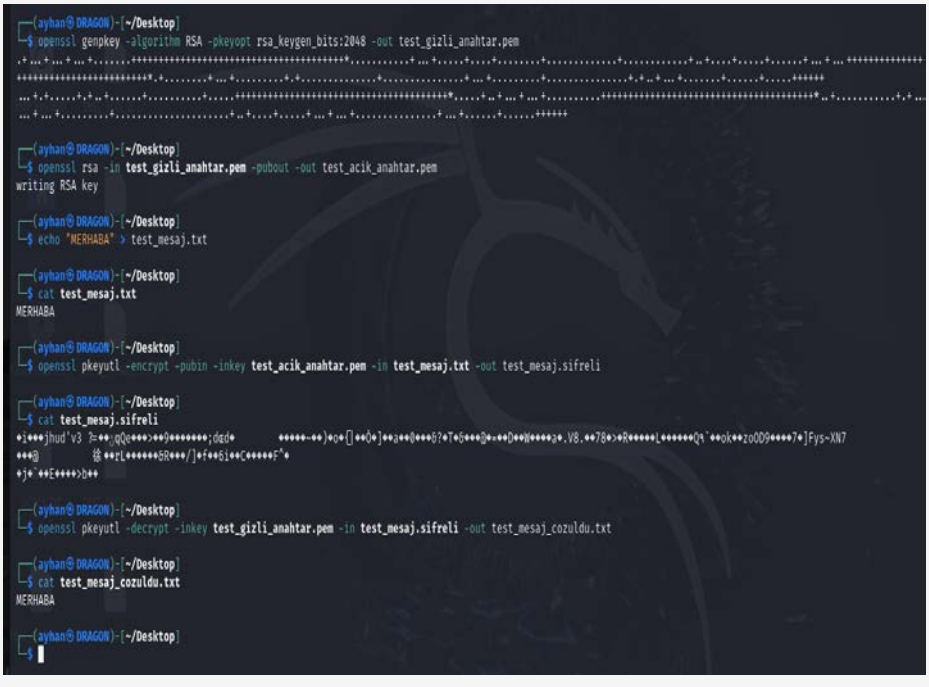
Bu işlemde açık anahtar kullanılır. Amaç, test mesajının doğrudan okunamayan bir çıktıya dönüştüğünü gözlemlemektir.

Ç) Test Mesajını Gizli Anahtarla Çözme

Aşağıdaki komutla şifreli test mesajını ilişkili gizli anahtar kullanarak çözünüz.

openssl pkeyutl -decrypt -inkey test_gizli_anahtar.pem -in test_mesaj.sifreli -out test_mesaj_cozuldu.txt

Bu işlemde gizli anahtar kullanılır. Doğru gizli anahtar kullanıldığında test mesajının yeniden okunabilir hâle gelmesi beklenir. Test mesajını şifreleme ve çözme işlemi Görsel 6.11'de gösterilmiştir.



Görsel 6.11: Test mesajını şifreleme ve çözme işlemi

D) Sonuçları Karşılaştırma

1. Açık anahtarın ve gizli anahtarın rollerini not ediniz.
2. test_mesaj.sifreli adlı dosyanın doğrudan okunup okunamadığını kontrol ediniz.
3. test_mesaj_cozuldu.txt adlı dosyanın içeriğini ilk test mesajıyla karşılaştırınız.

4. Öğretmeninizin yönergesine göre ilişkili olmayan farklı bir test anahtarı kullanarak çözme işlemini yeniden deneyiniz.
5. Yanlış test anahtarı kullanıldığında işlemin başarısız olup olmadığını gözlemleyiniz.

Kontrol Sorusu	Gözlem
Test açık anahtarı oluşturuldu mu?	
Test gizli anahtarı oluşturuldu mu?	
Açık anahtar paylaşılabilir mi?	
Gizli anahtar paylaşılmalı mı?	
Test mesajı açık anahtarla şifrelendi mi?	
Şifreli test mesajı doğrudan okunabiliyor mu?	
Doğru gizli anahtarla test mesajı çözülebildi mi?	
Çözülen mesaj ilk test mesajıyla aynı mı?	
Yanlış test anahtarı kullanıldığında işlem başarılı oldu mu?	
Bu yöntem büyük dosyaları doğrudan şifrelemek için kullanılmalı mı?	

Sorular

1. Açık anahtar neden başkalarıyla paylaşılabilir?

   .....

2. Gizli anahtar neden korunmalı ve başkalarıyla paylaşılmamalıdır?

   .....

3. Yanlış test anahtarı kullanıldığında mesajın doğru biçimde çözülememesi neden önemlidir?

   .....

4. Bu uygulamada RSA neden yalnızca küçük bir test mesajı üzerinde kullanılmıştır?

   .....

5. Gerçek sistemlerde RSA ve AES neden birlikte kullanılabilir?

   .....

6. Diffie-Hellman neden doğrudan mesaj şifreleme yöntemi olarak değerlendirilmez?

   .....

Değerlendirme

Çalışmanız öğretmeniniz tarafından kontrol listesine göre değerlendirilecektir. Çalışmanızı yaparken buradaki ölçütleri dikkate alınız. Kontrol listesi formuna ulaşmak için karekodu okutunuz. Dijital yayınlarda karekodun üstüne tıklayarak içeriğe ulaşabilirsiniz.

9. UYGULAMA

Uygulama Adı	Diffie-Hellman ile Ortak Gizli Değer Oluşturmak
Süre	40 dakika
Amaç	İki tarafın gizli anahtarlarını doğrudan paylaşmadan ortak bir gizli değer oluşturabilmesini gözlemlemek ve Diffie-Hellman anahtar değişiminin temel mantığını açıklamak
Yönerge	Aşağıdaki uygulama adımlarını tamamlayınız. İşlem sırasında yalnızca sınıf içi uygulama amacıyla oluşturulan test anahtarlarını kullanınız. Oluşturulan dosyaları gerçek sistemlerde kullanmayınız. Gizli anahtar dosyalarını başkalarıyla paylaşmayınız.

NOT: Diffie-Hellman parametrelerinin oluşturulması bazı bilgisayarlarda zaman alabilir. Bu nedenle dh_parametre.pem adlı test parametre dosyası öğretmeniniz tarafından önceden hazırlanarak sınıf ortamında paylaşılabilir.

Uygulama Adımları

A) Ali İçin Test Anahtarlarını Oluşturma

Aşağıdaki komutu çalıştırarak Ali'ye ait test gizli anahtarını oluşturunuz.

openssl genpkey -paramfile dh_parametre.pem -out ali_gizli.pem

Ardından Ali'ye ait açık anahtarı oluşturunuz.

openssl pkey -in ali_gizli.pem -pubout -out ali_acik.pem

B) Zeynep İçin Test Anahtarlarını Oluşturma

Aşağıdaki komutu çalıştırarak Zeynep'e ait test gizli anahtarını oluşturunuz.

openssl genpkey -paramfile dh_parametre.pem -out zeynep_gizli.pem

Ardından Zeynep'e ait açık anahtarı oluşturunuz.

openssl pkey -in zeynep_gizli.pem -pubout -out zeynep_acik.pem

C) Ali'nin Ortak Gizli Değeri Oluşturması

Ali'nin gizli anahtarı ile Zeynep'in açık anahtarını birlikte kullanarak ortak gizli değeri oluşturunuz.

openssl pkeyutl -derive -inkey ali_gizli.pem -peerkey zeynep_acik.pem -out ali_ortak_gizli.bin

Ç) Zeynep'in Ortak Gizli Değeri Oluşturması

Zeynep'in gizli anahtarı ile Ali'nin açık anahtarını birlikte kullanarak ortak gizli değeri oluşturunuz.

openssl pkeyutl -derive -inkey zeynep_gizli.pem -peerkey ali_acik.pem -out zeynep_ortak_gizli.bin

D) Ortak Gizli Değerlerin Hash Sonuçlarını Karşılaştırma

Ali tarafından oluşturulan ortak gizli değerin SHA-256 hash sonucunu hesaplayınız.

openssl dgst -sha256 ali_ortak_gizli.bin

Zeynep tarafından oluşturulan ortak gizli değerin SHA-256 hash sonucunu hesaplayınız.

openssl dgst -sha256 zeynep_ortak_gizli.bin

E) Gözlem Tablosunu Tamamlama

İncelenecek Alan	Ali	Zeynep
Oluşturulan gizli anahtar dosyası		
Oluşturulan açık anahtar dosyası		
Ortak gizli değer dosyası		
Ortak gizli değerin SHA-256 sonucu		

Sorular

1. Ali ve Zeynep tarafından oluşturulan ortak gizli değerlerin SHA-256 sonuçları aynı mıdır?

   .....

2. Ali ortak gizli değeri oluştururken hangi dosyaları kullanmıştır?

   .....

3. Zeynep ortak gizli değeri oluştururken hangi dosyaları kullanmıştır?

   .....

4. Ali ve Zeynep gizli anahtarlarını doğrudan birbirleriyle paylaşmış mıdır?

   .....

5. Açık anahtarların paylaşılabilir olmasına rağmen gizli anahtarların korunması neden gereklidir?

   .....

6. Diffie-Hellman neden doğrudan mesaj şifreleme yöntemi olarak değerlendirilmez?

   .....

7. Oluşturulan ortak gizli değer daha sonra hangi amaçla kullanılabilir?

   .....

Değerlendirme

Çalışmanız öğretmeniniz tarafından kontrol listesine göre değerlendirilecektir. Çalışmanızı yaparken buradaki ölçütleri dikkate alınız. Kontrol listesi formuna ulaşmak için karekodu okutunuz. Dijital yayınlarda karekodun üstüne tıklayarak içeriğe ulaşabilirsiniz.

Asimetrik Şifreleme Yöntemlerini Karşılaştırma

Asimetrik kriptografi yaklaşımları farklı amaçlarla kullanılabilir. RSA, Diffie-Hellman ve ECC aynı şey değildir. Bu yöntemlerin temel mantıkları ve kullanım amaçları birbirinden ayrılmalıdır (Tablo 6.25).

Tablo 6.25: RSA, Diffie-Hellman ve ECC Karşılaştırması

Yöntem	Temel Amacı	Anahtar Mantığı	Kısa Açıklama
RSA	Açık / gizli anahtar yapısıyla veri koruma işlemlerinde kullanılabilir.	Açık anahtar + gizli anahtar	Açık anahtarla korunan veri, ilişkili gizli anahtar olmadan çözülemez.
Diffie-Hellman	Ortak gizli anahtar oluşturmak	Her taraf kendi gizli bilgisini kullanır.	Doğrudan mesaj şifreleme yöntemi değildir. Anahtar değişimi yöntemidir.
ECC	Modern asimetrik kriptografi yaklaşımı	Açık anahtar + gizli anahtar	Uygun şekilde kullanıldığında daha kısa anahtarlarla güçlü güvenlik sağlayabilen yaklaşım olarak bilinir.

Asimetrik kriptografi yalnızca veriyi korumak için kullanılmaz. Dijital imza işlemleri de açık anahtar ve gizli anahtar mantığıyla ilişkilidir.

SIRA SİZDE

Aşağıdaki çalışmaları bireysel olarak tamamlayınız.

A) Kavramları Ayırt Edelim

Aşağıdaki durumları okuyunuz. Her durumla ilişkili kavramı **İlgili Kavram** sütununa, seçiminizin nedenini ise **Kısa Gerekçe** sütununa yazınız. Her kavramı bir kez kullanınız.

Kullanılacak Kavramlar: açık anahtar, gizli anahtar, RSA, Diffie-Hellman, ECC

Durum	İlgili Kavram	Kısa Gerekçe
Başkalarıyla paylaşılabilen anahtar		
Kesinlikle gizli tutulması gereken anahtar		
Açık anahtar ve gizli anahtar çiftiyle çalışan yaygın asimetrik şifreleme algoritması		
İki tarafın ortak gizli anahtar oluşturmasına yardımcı olan yöntem		
Uygun şekilde kullanıldığında daha kısa anahtarlarla güçlü güvenlik sağlayabilen modern asimetrik kriptografi yaklaşımı		

B) Simetrik mi, Asimetrik mi?

Aşağıdaki durumları okuyunuz. Her durumun simetrik kriptografi veya asimetrik kriptografiden hangisiyle daha çok ilişkili olduğunu belirleyiniz. Cevabınızı **İlgili Kriptografi Türü** sütununa, seçiminizin nedenini ise **Kısa Gerekçe** sütununa yazınız. Cevaplarınızı tamamladıktan sonra sınıfta arkadaşlarınızla karşılaştırınız.

No.	Durum	İlgili Kriptografi Türü	Kısa Gerekçe
1	Aynı anahtarla şifreleme ve şifre çözme işlemleri yapılır.		
2	Açık anahtar paylaşılabilir, gizli anahtar saklanır.		
3	Birbiriyle ilişkili iki anahtardan oluşan anahtar çifti kullanılır.		
4	Büyük miktardaki verilerin hızlı biçimde şifrelenmesi için genellikle daha uygundur.		
5	Anahtar paylaşımı sorununu azaltmaya yardımcı olur.		

BİLGİ KUTUSU

Açık anahtar paylaşılabilir, gizli anahtar paylaşılamaz. Asimetrik kriptografide açık anahtar başkalarıyla paylaşılabilir ancak gizli anahtar yalnızca sahibinde kalmalıdır. Gizli anahtarın başkalarının eline geçmesi, güvenliği tehlikeye atar.

6.6. DİJİTAL İMZA VE SERTİFİKALAR

Dijital ortamda bir dosyanın kim tarafından gönderildiğini, dosyanın değiştirilip değiştirilmediğini ve yapılan işlemin sonradan reddedilip reddedilemeyeceğini anlamak önemlidir. Bu amaçla **dijital imza** ve **dijital sertifika** kavramları kullanılır.

Dijital imza, mesajı veya dosyayı gizlemek için kullanılan bir yöntem değildir. Dijital imzanın temel amacı; kimlik doğrulama, veri bütünlüğü ve inkâr edilemezliği desteklemektir.

6.6.1. Dijital İmza

Dijital imza, bir dijital verinin belirli bir kişi veya kurumla ilişkilendirilebilmesini ve bu verinin sonradan değiştirilip değiştirilmediğinin kontrol edilebilmesini sağlayan kriptografik bir yöntemdir. Dijital imza ıslak imzaya benzetilebilir ancak teknik olarak kriptografik işlemlerle oluşturulur. Islak imza kâğıt üzerinde elle atılır. Dijital imza ise hash değeri, gizli anahtar, açık anahtar gibi kriptografik bileşenlerle çalışır. Dijital imza sayesinde bir dosya için Tablo 6.26'daki sorulara cevap aranabilir.

Tablo 6.26: Dijital İmzanın Cevap Aradığı Sorular

Soru	Dijital İmzayla İlişkisi
Bu dosyayı gerçekten kim imzaladı?	Kimlik doğrulama
Dosya imzalandıktan sonra değiştirilmiş mi?	Veri bütünlüğü
İmzayı atan kişi daha sonra "Ben imzalamadım." diyebilir mi?	İnkâr edilemezlik

Dijital İmzanın Sağladığı Güvenlik Özellikleri

Dijital imza üç temel güvenlik özelliğini destekler: kimlik doğrulama, veri bütünlüğü ve inkâr edilemezlik. Bu özellikler Tablo 6.27'de gösterilmiştir.

Tablo 6.27: Dijital İmzanın Sağladığı Güvenlik Özellikleri

Güvenlik Özelliği	Ne Anlama Gelir?	Günlük Yaşam Örneği
Kimlik doğrulama	İmzanın gerçekten ilgili kişiye veya kuruma ait olup olmadığını kontrol etmeye yardımcı olur.	Öğretmenin gönderdiği dosyanın gerçekten öğretmenden geldiğini doğrulamak
Veri bütünlüğü	İmzalanan verinin sonradan değiştirilip değiştirilmediğini anlamaya yardımcı olur.	İmzalı dosyada sonradan değişiklik yapılırsa doğrulamanın başarısız olması
İnkâr edilemezlik	İmza sahibinin yaptığı işlemi sonradan reddetmesini zorlaştırır.	Dijital olarak imzalanan bir belgenin kimin tarafından imzalandığının doğrulanması

Dijital imza bu özellikleri desteklerken **hash** ve **asimetrik kriptografi** birlikte kullanılır. Dosyanın önce hash değeri oluşturulur. Bu işlemden sonra hash değeri imzalayan kişinin gizli anahtarıyla imzalanır. Doğrulama işleminde ise ilgili açık anahtar kullanılır.

Dijital İmza ile Şifreleme Arasındaki Fark

Dijital imza ile şifrelemenin farkları vardır. İkisi de kriptografiyle ilişkilidir ancak amaçları farklıdır. Bu farklar Tablo 6.28'de gösterilmiştir.

Tablo 6.28: Dijital İmza ile Şifreleme Arasındaki Fark

Özellik	Dijital İmza	Şifreleme
Temel amaç	Kimlik doğrulama, bütünlük ve inkâr edilemezliği desteklemektir.	Veriyi yetkisiz kişilerden gizlemektir.
Veri gizlenir mi?	Hayır, temel amaç gizleme değildir.	Evet, doğru anahtar kullanılırsa veri gizlenir.
Hangi anahtar kullanılır?	İmzalama için gizli anahtar, doğrulama için açık anahtar kullanılır.	Kullanılan yönteme göre anahtar yapısı değişir.
Sonuç	İmza dosyası veya imza bilgisi oluşur.	Şifreli veri oluşur.
Kontrol işlemi	Açık anahtarla imza doğrulanır.	Doğru anahtarla veri çözülür.

Dijital İmza Sürecinin Temel Adımları

Dijital imza oluşturma ve doğrulama süreci sade biçimde Tablo 6.29'da açıklanmıştır.

Tablo 6.29: Dijital İmza Sürecinin Temel Adımları

Adım	İşlem	Açıklama
1	Dosyanın hash değeri oluşturulur.	Dosyanın tek yönlü özet değeri hesaplanır.
2	Hash değeri gizli anahtarla imzalanır.	İmza sahibinin gizli anahtarı kullanılır.
3	Dosya ve imza karşı tarafa gönderilir.	Alıcı, dosyayı ve imza bilgisini alır.
4	Alıcı, dosyanın hash değerini yeniden hesaplar.	Dosyanın alıcıdaki hâli kontrol edilir.
5	Açık anahtarla imza doğrulanır.	İmzanın ilgili gizli anahtarla oluşturulup oluşturulmadığı ve dosyanın değişip değişmediği kontrol edilir.

Bu süreçte **gizli anahtar** imza oluşturmak için kullanılır. **Açık anahtar** ise imzayı doğrulamak için kullanılır. Bu nedenle gizli anahtar kesinlikle paylaşılmamalıdır.

Dijital imza oluşturma ve doğrulama işlemleri, öğretmen rehberliğinde ve yalnızca test dosyalarıyla yapılmalıdır.

6.6.2. Elektronik İmza ve 5070 Sayılı Elektronik İmza Kanunu

Elektronik imza, elektronik ortamda kimlik doğrulama ve imzalama amacıyla kullanılan genel bir kavramdır. Türkiye'de elektronik imza konusu 5070 sayılı Elektronik İmza Kanunu ile düzenlenmiştir. Bu kanuna göre güvenli elektronik imza, elle atılan imza ile aynı hukuki sonucu doğurabilir ancak bu durum her elektronik onayın, her dijital işaretin veya her basit elektronik imza kullanımının aynı hukuki sonucu doğuracağı anlamına gelmediği Tablo 6.30'da gösterilmiştir. Burada kastedilen, kanunda belirtilen şartları taşıyan güvenli elektronik imzadır.

Tablo 6.30: Dijital İmza, Elektronik İmza ve Güvenli Elektronik İmza

Kavram	Kısa Açıklama
Dijital imza	Kriptografik imzalama ve doğrulama yöntemidir.
Elektronik imza	Elektronik ortamda imza amacıyla kullanılan daha genel kavramdır.
Güvenli elektronik imza	Kanunda belirtilen şartları taşıdığında elle atılan imzayla aynı hukuki sonucu doğurabilir.

6.6.3. Dijital Sertifika

Dijital sertifika, bir kişi, kurum veya web sitesinin açık anahtarını kimlik bilgileriyle ilişkilendiren dijital belgedir.

Bir dijital sertifika şu soruya cevap arar:

"Bu açık anahtar gerçekten bu kişiye, kuruma veya web sitesine mi ait?"

Dijital sertifikalar, açık anahtarın güvenilir bir kimlikle ilişkilendirilmesine yardımcı olur. Böylece kullanıcılar, karşı tarafın gerçekten iddia ettiği kişi veya sistem olup olmadığını daha güvenilir biçimde kontrol edebilir. Ayrıca Dijital sertifikada bulunabilecek bilgiler Tablo 6.31'de gösterilmiştir.

Tablo 6.31: Dijital Sertifikada Bulunabilecek Bilgiler

Sertifikada Bulunabilecek Bilgiler	Açıklama
Sertifika sahibi	Kişi, kurum veya web sitesi bilgisi
Açık anahtar	Sertifika sahibine ait açık anahtar
Sertifikayı veren kurum	Sertifika otoritesi bilgisi
Geçerlilik süresi	Sertifikanın hangi tarihler arasında geçerli olduğu
İmza bilgisi	Sertifikanın doğrulanmasına yardımcı olan bilgi

6.6.4. X.509 Sertifikaları, Sertifika Otoritesi ve Güven Zinciri

Dijital sertifikalarda yaygın kullanılan yapılardan biri X.509 sertifikasıdır. X.509 sertifikaları; sertifika sahibine ait kimlik bilgilerini, açık anahtarı, geçerlilik süresini ve sertifikayı veren kurumla ilgili bilgileri içerebilir. Sertifika Otoritesi (kısaca CA), dijital sertifika düzenleyen ve sertifikanın güvenilirliğini destekleyen kuruluştur. CA, bir sertifikayı imzalayarak "Bu açık anahtar bu kişi, kurum veya web sitesiyle ilişkilidir." bilgisini destekler.

Güven zinciri, bir sertifikanın güvenilir bir kök sertifikaya kadar doğrulanabilmesi mantığıdır. Web tarayıcıları, bir web sitesinin sertifikasını kontrol ederken bu güven zincirinden yararlanır.

Bu kavramların tamamı Tablo 6.32'de birlikte verilmiştir.

Tablo 6.32: X.509 Sertifikası, Sertifika Otoritesi ve Güven Zinciri

Kavram	Açıklama
X.509 sertifikası	Açık anahtar ve kimlik bilgilerini içeren dijital sertifika yapısıdır.
Sertifika otoritesi / CA	Sertifika düzenleyen ve doğrulamaya yardımcı olan güvenilir kuruluştur.
Güven zinciri	Sertifikanın güvenilir bir kaynağa kadar doğrulanabilmesi mantığıdır.

6.6.5. SSL/TLS Sertifikalarının Web Sitelerinde Kimlik Doğrulamadaki Rolü

Bir web sitesine girildiğinde adres çubuğunda kilit simgesi görülebilir. Bu simge genellikle bağlantının HTTPS kullandığını ve tarayıcıyla web sitesi arasındaki iletişimin şifrelendiğini gösterir. Kilit simgesi ve sertifika bilgileri, bağlantı güvenliği ve kimlik doğrulama hakkında bilgi verir ancak sitenin tamamen güvenilir olduğunu tek başına kanıtlamaz. Bir web sitesi HTTPS kullanıyor olsa bile sahte olabilir veya zararlı içerik barındırabilir. Bu nedenle web adresi, kurum adı ve yapılan işlemin güvenilirliği ayrıca kontrol edilmelidir.

Örnek: Bir öğrenci, okuluyla ilgili bir web sitesine girmek istiyor. Adres çubuğunda kilit simgesi görünmesi, bağlantının HTTPS ile korunduğunu gösterebilir ancak öğrenci yine de web adresinin doğru olup olmadığını kontrol etmelidir. Çünkü saldırganlar da HTTPS kullanan sahte siteler oluşturabilir.

Örnek Senaryo: Sertifika Kontrolünün Yapılması

Bir öğrenci, okuluyla ilgili bir web sayfasına girmeden önce adres çubuğundaki kilit simgesine tıklar ve sertifika bilgilerini inceler. Öğrenci şu üç soruya cevap arar: Alan adı doğru mu, sertifika güvenilir bir sertifika otoritesi

tarafından verilmiş mi ve sertifikanın geçerlilik süresi devam ediyor mu? Bu kontroller Tablo 6.33'te bağlantı güvenliği hakkında fikir verir ancak sitenin içeriğinin tamamen güvenilir olduğunu tek başına kanıtlamaz. Bu nedenle web adresi ve istenen bilgilerin gerekliliği ayrıca değerlendirilmelidir.

Tablo 6.33: Web Sitesi Sertifikasında Kontrol Edilecek Noktalar

Kontrol Edilecek Nokta	Neden Önemlidir?
Web adresi doğru mu?	Sahte site riskini azaltır.
Kilit simgesi var mı?	Bağlantının HTTPS ile korunduğunu gösterebilir.
Sertifika bilgileri tutarlı mı?	Sitenin kimlik bilgilerini kontrol etmeye yardımcı olur.
Site sizden gereksiz bilgi istiyor mu?	Kimlik avı riskini fark etmeye yardımcı olur.

BİLGİ KUTUSU

Bir web sitesine HTTPS ile bağlanıldığında tarayıcı ve web sitesi arasında güvenli iletişim kurulmaya çalışılır. Bu süreçte şu üç temel fikir öne çıkar:

Sertifika Kontrolü: Tarayıcı, web sitesinin sertifikasını kontrol ederek sitenin kimliği hakkında bilgi edinir.

Anahtar Değişimi: Tarayıcı ve web sitesi, iletişimde kullanılacak ortak güvenli bilgiyi oluşturmak için anahtar değişimi yapar.

Oturum Anahtarı: Görüşme sırasında verileri hızlı ve güvenli biçimde şifrelemek için kullanılan geçici anahtar olarak düşünülebilir.

10. UYGULAMA

Uygulama Adı	OpenSSL ile Dijital İmza Oluşturma ve Doğrulama
Süre	40 dakika
Amaç	Verilen test dosyası için dijital imza oluşturmak ve imzayı açık anahtarla doğrulamak
Yönerge	Aşağıdaki uygulama adımlarını öğretmen rehberliğinde tamamlayınız. Verilen test metnini kullanarak bir test dosyası oluşturunuz. Önce dosyanın dijital imzasını oluşturup açık anahtarla doğrulayınız. Daha sonra test dosyasında küçük bir değişiklik yaparak aynı imza dosyasıyla doğrulama işlemini tekrar ediniz. İlk doğrulama sonucu ile dosya değiştirildikten sonraki doğrulama sonucunu karşılaştırarak gözlem tablosuna yazınız.

A) Test Gizli Anahtarını Oluşturma

openssl genpkey -algorithm RSA -pkeyopt rsa_keygen_bits:2048 -out test_gizli_anahtar.pem

Bu komut, sınıf içi uygulamada kullanılmak üzere bir test gizli anahtarı oluşturur.

B) Test Açık Anahtarını Oluşturma

openssl rsa -in test_gizli_anahtar.pem -pubout -out test_acik_anahtar.pem

Bu komut, gizli anahtarla ilişkili açık anahtarı oluşturur.

C) Test Dosyasını Oluşturma

Bu uygulamada aşağıdaki test metni kullanılacaktır.
Bu bir test dosyasidir.
Test metnini içeren dosyayı oluşturmak için aşağıdaki komutu kullanınız.
echo Bu bir test dosyasidir. > test_dosya.txt

Ç) Test Dosyasını Gizli Anahtarla İmzalama

openssl dgst -sha256 -sign test_gizli_anahtar.pem -out test_imza.bin test_dosya.txt
Bu işlemde test dosyasının SHA-256 özet değeri üzerinden dijital imza oluşturulur.

D) Açık Anahtarla İmzayı Doğrulama

openssl dgst -sha256 -verify test_acik_anahtar.pem -signature test_imza.bin test_dosya.txt

Doğrulama başarılıysa imzanın ilgili açık anahtarla doğrulanabildiği ve dosyanın değiştirilmediği gözlemlenir.

E) Dosyayı Değiştirip Tekrar Doğrulama

Dijital imza, dosyanın imzalandıktan sonra değiştirilip değiştirilmediğini anlamaya yardımcı olur. Bunu gözlemlemek için test dosyasının sonuna şu kısa ifadeyi ekleyiniz:

echo test >> test_dosya.txt

Ardından aynı imza dosyasını kullanarak doğrulama işlemini tekrar ediniz.

openssl dgst -sha256 -verify test_acik_anahtar.pem -signature test_imza.bin test_dosya.txt

Dosyanın içeriği değiştiği için doğrulama işleminin başarısız olması beklenir. Bu durum, dosya içeriğinde yapılan küçük bir değişikliğin dijital imza doğrulama sonucunu etkilediğini gösterir (Görsel 6.12).



Görsel 6.12: OpenSSL ile dijital imza oluşturma ve doğrulama uygulaması

Kontrol Sorusu	Gözlem
İlk doğrulama başarılı oldu mu?	
Dosyada hangi değişikliği yaptınız?	
Dosya değiştirildikten sonra doğrulama sonucu ne oldu?	
Bu sonuç veri bütünlüğüyle nasıl ilişkilidir?	
Dijital imza dosyanın içeriğini gizledi mi?	

Sorular

1. Dosyada küçük bir değişiklik yapılması doğrulama sonucunu neden etkiledi?

   .....

2. Dijital imza ile veri bütünlüğü arasında nasıl bir ilişki vardır?

   .....

3. Dijital imza dosyanın içeriğini gizler mi? Neden?

   .....

Değerlendirme

Çalışmanız öğretmeniniz tarafından kontrol listesine göre değerlendirilecektir. Çalışmanızı yaparken buradaki ölçütleri dikkate alınız. Kontrol listesi formuna ulaşmak için karekodu okutunuz. Dijital yayınlarda karekodun üstüne tıklayarak içeriğe ulaşabilirsiniz.

BİLGİ KUTUSU

Dosya değiştiğinde imza doğrulamasının başarısız olması beklenebilir. Çünkü dijital imza, dosyanın imzalandığı andaki hash değeriyle ilişkilidir. Dosya değişirse hash değeri de değişir ve doğrulama sonucu başarısız olabilir.

6.6.6. Dijital İmza ve Sertifikaları Karşılaştırma

Dijital imza ve dijital sertifika birbirine bağlı kavramlardır ancak aynı şey değildir. Bu kavramlar Tablo 6.34'te verilmiştir.

Tablo 6.34: Dijital İmza ve Sertifikaları Karşılaştırma

Kavram	Temel Amacı	Kısa Açıklama
Dijital imza	Dosyanın kim tarafından imzalandığını ve değişip değişmediğini kontrol etmeye yardımcı olur.	Gizli anahtarla oluşturulur, açık anahtarla doğrulanır.
Dijital sertifika	Açık anahtarı kişi, kurum veya web sitesi kimliğiyle ilişkilendirir.	Sertifika otoritesi tarafından desteklenebilir.
Sertifika otoritesi / CA	Sertifika düzenler ve güven ilişkisini destekler.	Güven zincirinin kurulmasına yardımcı olur.
SSL/TLS sertifikası	Web sitesi bağlantısında kimlik ve bağlantı güvenliği kontrolüne yardımcı olur.	Kilit simgesiyle ilişkilidir ancak sitenin tamamen güvenilir olduğunu tek başına kanıtlamaz.

BİLGİ KUTUSU

Dijital imza mesajı gizlemez. Dijital imza, bir dosyanın kim tarafından imzalandığını ve imzadan sonra değişip değişmediğini kontrol etmeye yardımcı olur. Mesajı gizlemek için şifreleme yöntemleri kullanılır. Dijital imza ise kimlik doğrulama, veri bütünlüğü ve inkâr edilemezliği destekler.

SIRA SİZDE

Aşağıdaki çalışmaları bireysel olarak tamamlayınız.

A) Kavramları Ayırt Edelim

Aşağıdaki durumları okuyunuz. Her durumla ilişkili kavramı **İlgili Kavram** sütununa, seçiminizin nedenini ise **Kısa Gerekçe** sütununa yazınız.

Kullanılacak Kavramlar: dijital imza, dijital sertifika, sertifika otoritesi, güven zinciri, SSL/TLS sertifikası

Durum	İlgili Kavram	Kısa Gerekçe
Bir dosyanın, imzalayan kişiyle ilişkilendirilmesine yardımcı olur.		
Açık anahtarı bir kişi, kurum veya web sitesinin kimlik bilgileriyle ilişkilendirir.		
Sertifika düzenleyen güvenilir kuruluşu ifade eder.		
Sertifikanın güvenilir bir kaynağa kadar doğrulanabilmesi mantığıdır.		
Web sitelerinde HTTPS bağlantısıyla ilişkilidir.		

B) Dijital İmza mı, Şifreleme mi?

Aşağıdaki durumları okuyunuz. Her durumun dijital imza veya şifreleme ile ilişkili olduğunu belirleyiniz. Seçiminizi **Dijital İmza / Şifreleme** sütununa, seçiminizin nedenini ise **Kısa Gerekçe** sütununa yazınız.

Durum	Dijital İmza / Şifreleme	Kısa Gerekçe
Dosyanın değiştirilip değiştirilmediğini kontrol etmek		
Mesajın içeriğini yetkisiz kişilerden gizlemek		
İmza sahibinin kimliğini doğrulamaya yardımcı olmak		
Şifreli veriyi doğru anahtarla yeniden okunabilir hâle getirmek		
Bir işlemin inkâr edilemezliğini desteklemek		

Cevaplarınızı tamamladıktan sonra sınıfta arkadaşlarınızla karşılaştırınız.

6.7. VERİ GİZLEME

Dijital ortamda bazı bilgiler yalnızca şifrelenerek korunmaz. Bazen bilginin varlığının fark edilmemesi de istenebilir. Bu noktada steganografi kavramı ortaya çıkar. **Steganografi**, bir mesajı ya da dosyayı başka bir dosyanın içinde gizleme yöntemidir. Örneğin bir görsel dosyasının içine kısa bir metin yerleştirilebilir. Dışarıdan bakıldığında dosya normal bir görsel gibi görünebilir ancak içinde gizlenmiş bir veri bulunabilir.

6.7.1. Steganografi

Steganografi; bir bilginin başka bir dosya, metin, görüntü, ses veya video içine gizlenmesi yöntemidir. Steganografinin temel amacı, mesajın içeriğini anlaşılmaz hâle getirmekten çok, mesajın varlığını fark edilmez hâle getirmeye çalışmaktır. Örneğin bir görsel dosyasının içine kısa bir test mesajı gizlenebilir. Görsel dışarıdan normal görünebilir; ancak uygun araçla incelendiğinde içindeki gizli test mesajı çıkarılabilir. Steganografide genellikle iki unsur bulunur ve bu unsurlar Tablo 6.35'te gösterilmiştir.

Tablo 6.35: Steganografide Temel Unsurlar

Unsur	Açıklama
Taşıyıcı dosya	İçine veri gizlenecek dosyadır. Örneğin resim, ses veya video dosyası
Gizlenecek veri	Taşıyıcı dosyanın içine yerleştirilecek test mesajı veya test dosyasıdır.

6.7.2. Steganografi ile Kriptografi Arasındaki Fark

Kriptografi ve steganografi benzer değildir. Kriptografinin şifreleme yönü, mesajın içeriğini yetkisiz kişiler için anlaşılmaz hâle getirmeye çalışır. Steganografi ise mesajın varlığını gizlemeye çalışır.

Şifreleme, "Bu mesaj okunamasın." derken steganografi, "Bu mesajın burada olduğu fark edilmesin." der. Bu özelliklerin tamamı Tablo 6.36'da verilmiştir.

Tablo 6.36: Kriptografi ve Steganografi Arasındaki Fark

Özellik	Kriptografi / Şifreleme Yönü	Steganografi
Temel amaç	Mesajın içeriğini anlaşılmaz hâle getirmektir.	Mesajın varlığını gizlemeye çalışmaktır.
Sonuç	Şifreli metin veya şifreli dosya oluşur.	Normal görünen bir taşıyıcı dosya içinde gizli veri bulunabilir.
Ana soru	"Bu mesaj nasıl okunamaz hâle gelir?"	"Bu mesajın varlığı nasıl fark edilmez?"
Örnek	Bir metni anahtarla şifrelemek	Bir görsel içine kısa test mesajı gizlemek
Sınırlılık	Anahtar güvenliği önemlidir.	Gizli veri fark edilirse çıkarılmaya çalışılabilir.

Tabloda kriptografinin özellikle şifreleme yönü dikkate alınmaktadır. Kriptografi; hash, dijital imza, sertifika gibi farklı konuları da kapsar. Bu tabloda amaç, şifreleme ile steganografi arasındaki temel farkı göstermektir.

6.7.3. Dijital Watermarking ve Steganaliz

Steganografiyle karıştırılabilecek kavramlardan biri dijital watermarkingdir. **Dijital watermarking**; bir görsel, ses veya video dosyasına sahiplik, doğrulama veya izleme bilgisi eklemek için kullanılabilir. **Steganografi** ise taşıyıcı dosyayı asıl gizli mesajı fark ettirmeden taşımak için kullanır. **Steganaliz** ise bir dosyada gizli veri bulunup bulunmadığını araştırmaya yönelik inceleme sürecidir. Karşılaştırmaları Tablo 6.37'de verilmiştir.

Tablo 6.37: Steganografi, Dijital Watermarking ve Steganaliz Karşılaştırması

Kavram	Temel Amaç	Örnek
Steganografi	Gizli mesajın varlığını fark ettirmeden taşımaya çalışır.	Bir test görselinin içine mesaj.txt dosyasını gizlemek
Dijital watermarking	Sahiplik, doğrulama veya izleme bilgisi eklemeye yardımcı olur.	Bir görsele telif, kurum ya da doğrulama bilgisi gömmek
Steganaliz	Bir dosyada gizli veri olup olmadığını araştırır.	Orijinal görsel ile stego görselin boyut, yapı veya istatistiksel özelliklerini karşılaştırmak

Üç kavram birbiriyle ilişkilidir ancak aynı anlama gelmez. Steganografi gizli mesajı taşımaya, dijital watermarking medya dosyasına anlamlı bir işaret eklemeye, steganaliz ise gizleme izlerini araştırmaya odaklanır.

Steganografide Temel Kavramlar

Steganografi uygulamalarında verinin hangi dosyanın içine yerleştirildiğini, gizleme işlemi sonucunda hangi dosyanın oluştuğunu ve gizlenen verinin hangi koşullarda geri çıkarılabildiğini doğru anlamak önemlidir. Bu süreçte kullanılan temel kavramlar ve açıklamaları Tablo 6.38'de verilmiştir.

Tablo 6.38: Steganografide Temel Kavramlar

Kavram	Açıklama
Taşıyıcı dosya	İçine veri gizlenecek dosyadır. Örneğin test_gorsel.jpg.
Gizlenecek veri	Taşıyıcı dosyanın içine yerleştirilecek test mesajı veya test dosyasıdır.
Stego dosya	İçine veri gizlenmiş çıktı dosyasıdır. Örneğin test_gorsel_stego.jpg.
Test geçiş ifadesi	Veriyi gömme veya çıkarma sırasında kullanılan sınıf içi örnek ifadedir. Gerçek parola değildir.

11. UYGULAMA

Uygulama Adı	LSB Mantığını İncelemek
Süre	20 dakika
Amaç	Dijital görüntülerde RGB renk değerlerinin en sağındaki bit değiştirilerek küçük test verilerinin nasıl saklanabileceğini incelemek
Yönerge	Tablo 6.39'u inceleyiniz. Her renk kanalında gizlenecek bitin, ikilik değerin en sağındaki bite nasıl yerleştirildiğini gözlemleyiniz. Ardından soruları cevaplayınız.

Uygulama Adımları

1. Tabloda verilen ilk RGB değerlerini inceleyiniz.
2. Her renk kanalının ikilik karşılığını kontrol ediniz.
3. Gizlenecek bit ile ilk ikilik değerin en sağındaki biti karşılaştırınız.
4. Gerekli değişiklik yapıldıktan sonra oluşan yeni ikilik değeri inceleyiniz.
5. Yeni ikilik değerin onluk sayı sistemindeki karşılığını karşılaştırınız.
6. İlk ve yeni RGB değerleri arasındaki farkı yorumlayınız

Tablo 6.39: LSB ile Bir Pikselde Test Verisi Gösterimi

Renk Kanalı	İlk Değer	İlk Ikilik Değer	Gizlenecek Bit	Yeni İkilik Değer	Yeni Değer
R	212	11010100	1	11010101	213
G	171	10101011	0	10101010	170
B	237	11101101	0	11101100	236

İşlem öncesinde piksel değeri RGB (212, 171, 237) biçimindedir. Gizlenecek bitler yerleştirildikten sonra piksel değeri RGB (213, 170, 236) hâline gelir.

Renk değerlerindeki değişiklik küçük olduğu için görsel üzerindeki fark gözle kolayca anlaşılamayabilir ancak bu durum, değişikliğin hiçbir yöntemle tespit edilemeyeceği anlamına gelmez. Dosya boyutu, dosya yapısı veya uygun analiz araçlarının çıktıları incelendiğinde değişiklik fark edilebilir.

Sorular

1. RGB değerlerinde hangi değişiklikler yapılmıştır?

   .....

2. Her renk kanalında yalnızca en sağdaki bitin değiştirilmesi ne sağlamıştır?

   .....

3. İlk piksel değeri ile yeni piksel değeri arasında büyük bir fark var mıdır?

   .....

4. Küçük renk değişikliklerinin gözle kolay fark edilememesi, gizlenen verinin hiçbir zaman tespit edilemeyeceği anlamına gelir mi? Neden?

.....

Değerlendirme

Çalışmanız öğretmeniniz tarafından kontrol listesine göre değerlendirilecektir. Çalışmanızı yaparken buradaki ölçütleri dikkate alınız. Kontrol listesi formuna ulaşmak için karekodu okutunuz. Dijital yayınlarda karekodun üstüne tıklayarak içeriğe ulaşabilirsiniz.

Steghide Parametreleri

Steghide, bazı görsel ve ses dosyaları içine test verisi gizlemek ve gizlenen veriyi çıkarmak için kullanılabilen bir araçtır. Bu aracın yaygın kullanılan parametreleri Tablo 6.40'ta verilmiştir.

Tablo 6.40: Yaygın Kullanılan Steghide Parametreleri

Komut / Parametre	Görevi
embed	Veri dosyasını taşıyıcı dosyanın içine gömmek için kullanılır.
extract	Gizlenmiş veriyi stego dosyadan çıkarmak için kullanılır.
-cf	Taşıyıcı dosyayı belirtir.
-ef	Gizlenecek veri dosyasını belirtir.
-sf	Oluşturulacak veya kullanılacak stego dosyayı belirtir.
-p	Test geçiş ifadesini belirtir.
-xf	Çıkarılan verinin kaydedileceği dosya adını belirtir.

SIRA SİZDE

Aşağıdaki Steghide komut parçalarını (Tablo 6.41) inceleyiniz. Her komut parçasının görevini **Görevi** sütununa yazınız.

Tablo 6.41: Steghide Komut Parçalarını Eşleştirme

Komut Parçası	Görevi
-cf test_gorsel.jpg	.....
-ef mesaj.txt	.....
-sf test_gorsel_stego.jpg	.....
-p test123	.....
extract	.....

12. UYGULAMA

Uygulama Adı	Kali Linux'ta Steghide ile Görsel İçine Test Mesajı Gizleme ve Geri Çıkarma
Süre	40 dakika
Amaç	Öğretmenin verdiği test görselinin içine kısa bir test mesajı gizlemek, içine veri gizlenmiş yeni görsel dosyasını oluşturmak ve gizlenen test mesajını görselden geri çıkarmak
Yönerge	Aşağıdaki uygulama adımlarını öğretmen rehberliğinde tamamlayınız. Uygulamada kullanılacak test dosyaları ve açıklamaları Tablo 6.42'de verilmiştir. İşlem sırasında yalnızca öğretmeninizin verdiği test görselini, test mesajını ve örnek test geçiş ifadesini kullanınız. Oluşturduğunuz dosyaları inceleyerek Tablo 6.43'ü doldurunuz ve sonuç sorularını cevaplayınız.

Tablo 6.42: Steghide Uygulamasında Kullanılacak Test Dosyaları

Dosya / Bilgi	Açıklama
test_gorsel.jpg	Öğretmenin verdiği test görselidir.
mesaj.txt	Görsel içine gizlenecek test mesajını içerir.
test_gorsel_stego.jpg	İçine test mesajı gizlenmiş yeni görsel dosyasıdır.
test_ifadesi	Sınıf içi uygulamada kullanılacak örnek test geçiş ifadesidir. Gerçek parola değildir.

Uygulama Adımları

A) Steghide Kurulumunu Kontrol Etme

Steghide aracının bilgisayarda kurulu olup olmadığını şu komutla kontrol ediniz:

steghide –version

Steghide aracının sürüm bilgisinin görüntülendiği örnek ekran çıktısı Görsel 6.13'te verilmiştir.

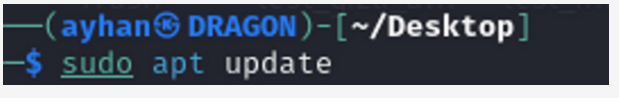


Görsel 6.13: Steghide kurulumunu kontrol etme

Steghide aracı kurulu değilse öğretmen rehberliğinde aşağıdaki komutları çalıştırınız.

```
sudo apt update
```

Sistem paket listesinin güncellenmesine ilişkin örnek ekran çıktısı Görsel 6.14'te verilmiştir.



Görsel 6.14: Sistemi güncelleme

```
sudo apt install steghide –y
```

Steghide aracının kurulmasına ilişkin örnek ekran çıktısı Görsel 6.15'te verilmiştir.



Görsel 6.15: Steghide aracını kurma

B) Uygulama Klasörünü Oluşturma

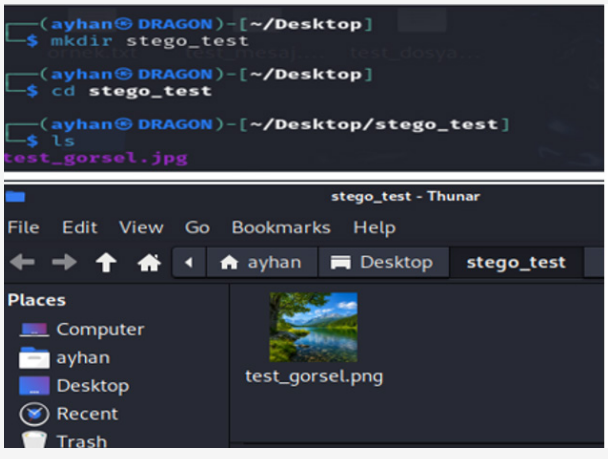
Uygulama dosyalarını düzenli biçimde saklamak için aşağıdaki komutlarla bir klasör oluşturunuz ve bu klasöre geçiniz.

```
mkdir stego_test
cd stego_test
```

Öğretmeninizin verdiği test_gorsel.jpg dosyasını bu klasöre kopyalayınız. Klasördeki dosyaları şu komutla kontrol ediniz.

```
ls
```

Uygulama klasörünün oluşturulmasına ilişkin örnek ekran çıktısı Görsel 6.16'da verilmiştir.



Görsel 6.16: Uygulama klasörü oluşturma

C) Test mesajı dosyasını Oluşturma

Şu komutla kısa bir test mesajı oluşturunuz:

```
echo “Bu bir steganografi test mesajidir.” > mesaj.txt
```

Oluşturduğunuz test mesajını görüntülemek için şu komutu çalıştırınız:

```
cat mesaj.txt
```

Test mesajı dosyasının oluşturulmasına ilişkin örnek ekran çıktısı Görsel 6.17'de verilmiştir.



Görsel 6.17: Test mesaj dosyasını oluşturma

Ç) Test Mesajını Görsel İçine Gizleme

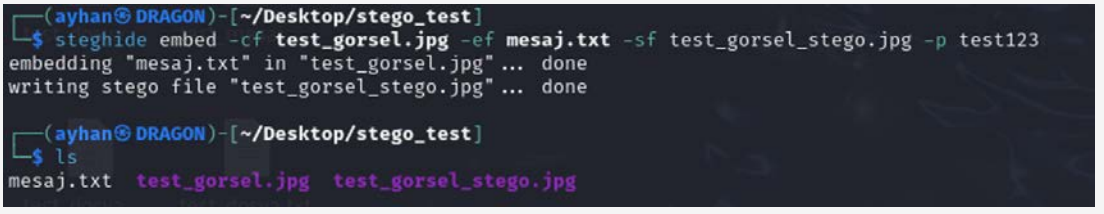
Şu komutla mesaj.txt dosyasındaki test mesajını test_gorsel.jpg adlı taşıyıcı görselin içine gizleyiniz:

```
steghide embed -cf test_gorsel.jpg -ef mesaj.txt -sf test_gorsel_stego.jpg -p test_ifadesi
```

İşlem tamamlandıktan sonra klasördeki dosyaları şu komutla kontrol ediniz:

```
ls
```

Klasörde test_gorsel.jpg, mesaj.txt ve test_gorsel_stego.jpg dosyalarının bulunması beklenir. Test mesajının görsel içine gizlenmesine ilişkin örnek ekran çıktısı Görsel 6.18'de verilmiştir.



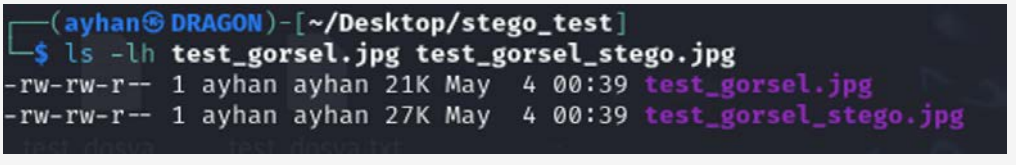
Görsel 6.18: Test mesajını görsel içine gizleme

D) Orijinal Görsel ile Yeni Görseli Karşılaştırma

Orijinal görsel ile içine test mesajı gizlenmiş stego görselin dosya boyutlarını şu komutla inceleyiniz:

ls -lh test_gorsel.jpg test_gorsel_stego.jpg

Dosya boyutlarının karşılaştırılmasına ilişkin örnek ekran çıktısı Görsel 6.19'da verilmiştir.



Görsel 6.19: Orijinal görsel ile yeni görseli karşılaştırma

Her iki görseli açarak dışarıdan bakıldığında fark görülüp görülmediğini kontrol ediniz. Gözlemlerinizi Tablo 6.43'e yazınız.

Tablo 6.43: Orijinal Görsel ve Stego Görsel Karşılaştırması

Dosya	Dosya Boyutu	Görsel Olarak Fark Var Mı?
test_gorsel.jpg	.....	.....
test_gorsel_stego.jpg	.....	.....

E) Gizlenen Test Mesajını Geri Çıkarma

Görsel içine gizlenen test mesajının geri çıkarılabildiğini gözlemlemek için önce uygulama klasöründeki ilk mesaj dosyasını siliniz. Böylece oluşturacağınız yeni dosyanın gerçekten stego görselden çıkarıldığını kontrol edebilirsiniz.

DİKKAT

Silme işleminden önce stego_test klasöründe bulunduğunuzdan emin olunuz. Yalnızca uygulama amacıyla oluşturduğunuz mesaj.txt adlı test dosyasını siliniz. Kişisel dosyalarınızı veya özel belgelerinizi silmeyiniz.

Uygulama klasöründeki dosyaları kontrol ediniz.

```
ls
```

Uygulama amacıyla oluşturduğunuz mesaj.txt dosyasını siliniz.

```
rm mesaj.txt
```

Dosyanın silindiğini kontrol ediniz:

```
ls
```

Stego görselden test mesajını geri çıkarmak için şu komutu çalıştırınız.

```
steghide extract –sf test_gorsel_stego.jpg –p test_ifadesi –xf cikarilan_mesaj.txt
```

Çıkarılan dosyanın oluşup oluşmadığını kontrol ediniz.

```
ls
```

Çıkarılan test mesajını görüntüleyiniz.

```
cat cikarilan_mesaj.txt
```

Beklenen çıktı şudur:

Bu bir steganografi test mesajidir.

Test mesajının stego görselden geri çıkarılmasına ilişkin örnek ekran çıktısı Görsel 6.20'de verilmiştir.



Görsel 6.20: Gizlenen test mesajını geri çıkarma

Sorular

1. Orijinal görsel ile içine test mesajı gizlenmiş stego görsel arasında gözle görülebilen bir fark var mıdır?

   .....

2. Görselde fark görülmemesi, görselin içinde veri bulunmadığını kanıtlar mı? Neden?

   .....

3. Orijinal görsel ile stego görselin dosya boyutları aynı mıdır?

.....

4. Steganografi mesajın içeriğini mi gizler, yoksa mesajın varlığını mı gizlemeye çalışır?

.....

5. Taşıyıcı dosya ile stego dosya arasındaki fark nedir?

.....

6. Bu uygulamada mesaj.txt dosyasının silinmesi neden istenmiştir?

.....

7. cikarilan_mesaj.txt dosyası oluşturuldu mu? İçeriği beklenen test mesajıyla aynı mıdır?

.....

8. Doğru test geçiş ifadesi kullanılmadığında veri çıkarma işlemi nasıl etkilenir?

.....

Değerlendirme

Çalışmanız öğretmeniniz tarafından kontrol listesine göre değerlendirilecektir. Çalışmanızı yaparken buradaki ölçütleri dikkate alınız. Kontrol listesi formuna ulaşmak için karekodu okutunuz. Dijital yayınlarda karekodun üstüne tıklayarak içeriğe ulaşabilirsiniz.

Steganaliz

Steganografi, gizli mesajın varlığını fark ettirmemeye çalışır ancak bu, gizlenen verinin hiçbir zaman tespit edilemeyeceği anlamına gelmez. Dosya boyutu, dosya yapısı, renk değerlerinin dağılımı veya özel analiz araçları incelenerek gizleme izleri araştırılabilir. Bu tür inceleme çalışmalarına **steganaliz** denir.

SIRA SİZDE

mesaj.txt dosyasını silmenize rağmen mesajı test_gorsel_stego.jpg dosyasından geri çıkarabilmeniz neyi gösterir?

.....

13. UYGULAMA

Uygulama Adı	Çevrim İçi Araçla Görsel İçine Görsel Gizleme ve Geri Çıkarma
Süre	30 dakika
Amaç	Öğretmenin belirlediği güvenli çevrim içi araçla bir test görselinin içine başka bir test görseli gizlemek, gizleme işleminde kullanılan temel ayarları incelemek ve gizlenen görseli geri çıkarmak
Yönerge	Aşağıdaki uygulama adımlarını öğretmen rehberliğinde tamamlayınız. İşlem sırasında yalnızca öğretmeninizin verdiği test görsellerini kullanınız. Gizleme işleminden sonra oluşan görsel ile taşıyıcı görseli karşılaştırınız. Ardından gizlenen görseli geri çıkararak sonuç sorularını cevaplayınız.

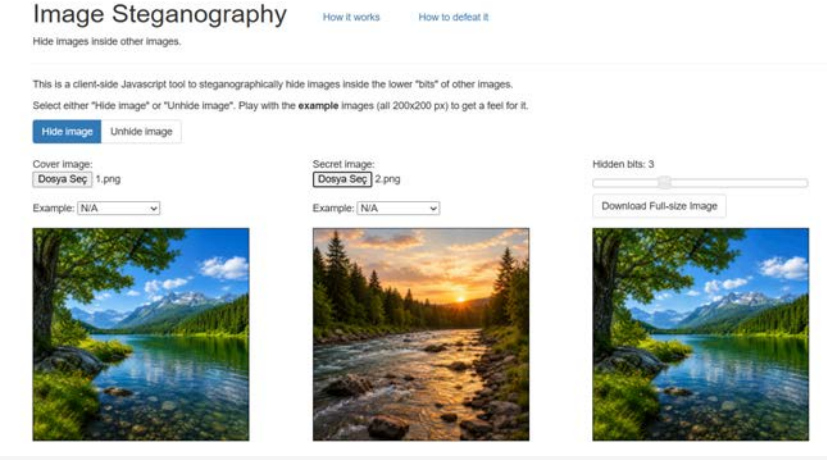
BİLGİ KUTUSU

Görsel içine görsel gizleme işlemlerinde kalite kaybı oluşturmayan dosya türleri tercih edilmelidir. PNG gibi kayıpsız dosya türleri bu tür işlemler için daha uygundur. JPG gibi sıkıştırmalı dosya türlerinde ise gizlenen veri zarar görebilir veya beklenen sonuç elde edilemeyebilir.

Uygulama Adımları

A) Taşıyıcı Görseli Seçme

Öğretmeninizin belirlediği güvenli çevrim içi aracı açınız. Araçta Cover Image bölümünü bulunuz ve öğretmeninizin verdiği taşıyıcı test görselini seçiniz.
Cover Image, içine başka bir görsele ait verilerin yerleştirileceği ana görseldir. İşlem tamamlandığında çıktı dosyası dışarıdan normal bir görsel gibi görünebilir.
Taşıyıcı görselin seçildiği bölüm Görsel 6.21'de verilmiştir.



Görsel 6.21: Taşıyıcı ve gizlenecek görseli seçme

B) Gizlenecek Görseli Seçme

Araçta Secret Image bölümünü bulunuz ve öğretmeninizin verdiği ikinci test görselini seçiniz.
Secret Image, taşıyıcı görselin içine gizlenecek görseldir. Gizleme işlemi tamamlandıktan sonra bu görsel doğrudan görünmez; ancak uygun veri çıkarma işlemiyle yeniden görüntülenebilir.

C) Gizlenecek Bit Sayısını Belirleme

Araçta **Hidden Bits** ayarını inceleyiniz. Öğretmeninizin yönergesine göre uygun bit sayısını seçiniz.

Hidden Bits, taşıyıcı görselin renk değerlerinde kaç bitlik alanın kullanılacağını belirler. Düşük bit değeri seçildiğinde taşıyıcı görseldeki değişiklik daha az fark edilebilir ancak gizlenen görselin kalitesi düşebilir. Bit değeri yükseltildiğinde gizlenen görsel daha belirgin hâle gelebilir. Buna karşılık taşıyıcı görselde bozulma oluşabilir.

Ç) Görsel İçine Görsel Gizleme

Gerekli seçimleri tamamladıktan sonra gizleme işlemini başlatınız. İşlem sonunda oluşan yeni görsel dosyasını yalnızca sınıf içi uygulama amacıyla kaydediniz.

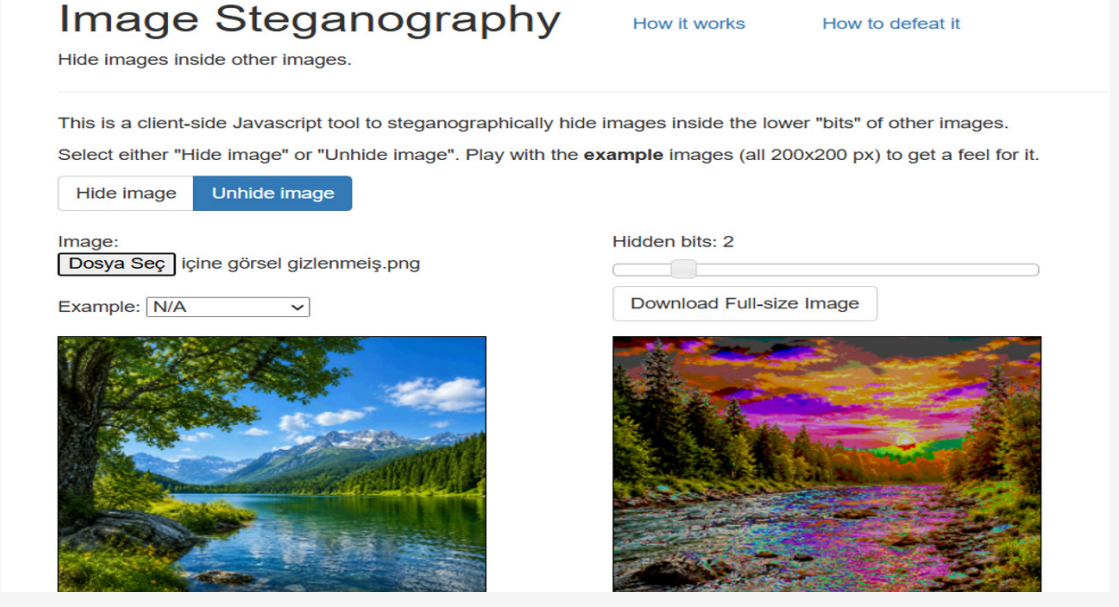
Oluşturulan çıktı dosyasını taşıyıcı görselle karşılaştırınız. Dışarıdan bakıldığında belirgin bir farklılık görülüp görülmediğini not ediniz.

Kontrol Sorusu	Gözlem
Taşıyıcı görsel seçildi mi?	
Gizlenecek test görseli seçildi mi?	
Kullanılan Hidden Bits değeri nedir?	
Gizleme işlemi tamamlandı mı?	
Oluşturulan çıktı görselinde gözle fark edilebilen bir değişiklik var mı?	

D) Gizlenen Görseli Geri Çıkarma

Araçta gizlenen görseli ortaya çıkarmak için kullanılan bölümü açınız. Gizleme işlemi sonucunda oluşturduğunuz çıktı dosyasını ilgili alana yükleyiniz. Öğretmeninizin yönergesine göre veri çıkarma işlemini başlatınız.

Gizlenmiş görselin geri çıkarılmasına yönelik araç arayüzü Görsel 6.22'de verilmiştir.



Görsel 6.22: Gizlenmiş görseli geri çıkarma

Sonuç Soruları

1. Taşıyıcı görsel ile gizlenecek görsel arasındaki fark nedir?

   .....
   .....

2. Hidden Bits değerinin artırılması veya azaltılması görselleri nasıl etkileyebilir?

   .....
   .....

3. Görsel içine görsel gizleme işleminde PNG gibi kayıpsız dosya türlerinin tercih edilmesi neden önemlidir?

   .....
   .....

4. Oluşturulan çıktı görselinde gözle fark edilebilen bir değişiklik bulunmaması, görselin içinde gizli veri bulunmadığını kanıtlar mı? Neden?

   .....
   .....

5. Çevrim içi araçlarla gerçekleştirilen veri gizleme uygulamalarında neden yalnızca öğretmenin verdiği test dosyaları kullanılmalıdır?

   .....
   .....

Değerlendirme

Çalışmanız öğretmeniniz tarafından kontrol listesine göre değerlendirilecektir. Çalışmanızı yaparken buradaki ölçütleri dikkate alınız. Kontrol listesi formuna ulaşmak için karekodu okutunuz. Dijital yayınlarda karekodun üstüne tıklayarak içeriğe ulaşabilirsiniz.

Steganografi Yöntemlerinin Avantajları ve Sınırlılıkları

Steganografi, mesajın varlığını gizlemeye yardımcı olabilir; ancak tek başına güçlü güvenlik sağlamaz. Yöntemin başarısı; kullanılan dosya türüne, taşıyıcı dosyanın kapasitesine ve gizlenen veri miktarına göre değişebilir. Steganografi yöntemlerinin başlıca avantajları ve sınırlılıkları Tablo 6.44'te verilmiştir.

Tablo 6.44: Steganografi Yöntemlerinin Avantajları ve Sınırlılıkları

Özellik	Avantaj	Sınırlılık
Görsel fark	Küçük değişiklikler gözle fark edilmeyebilir.	Özel analiz araçlarıyla değişiklik anlaşılabilir.
Uygulama	Test dosyalarıyla kolayca gözlemlenebilir.	Dosya formatı ve araç desteği önemlidir.
Gizleme mantığı	Mesajın varlığını saklamaya çalışır.	Mesajın içeriğini tek başına güçlü biçimde korumaz.
Kapasite	Taşıyıcı dosyada küçük veriler saklanabilir.	Gizlenecek veri büyüdükçe bozulma veya fark edilme riski artabilir.

BİLGİ KUTUSU

Steganografi mesajı şifrelemez, mesajın varlığını gizlemeye çalışır. Kriptografinin şifreleme yönü ise mesajın içeriğini anlaşılmaz hâle getirmeyi amaçlar. Steganografi tek başına güçlü güvenlik sağlamayabilir. Bu nedenle uygulamalar yalnızca test dosyalarıyla, etik ve yasal sınırlar içinde yapılmalıdır.

SIRA SİZDE

Aşağıdaki çalışmaları bireysel olarak tamamlayınız.

A) Kavramları Ayırt Etmek

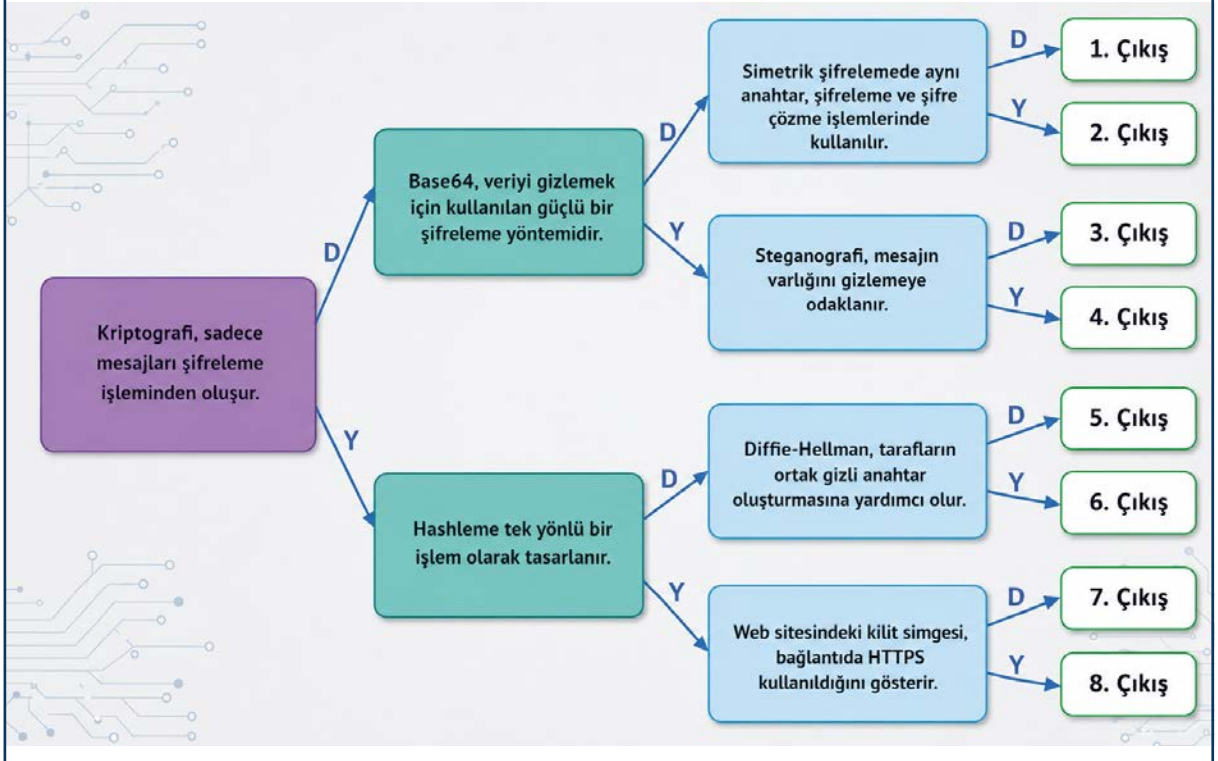
Aşağıdaki durumları okuyunuz. Her durumla ilişkili kavramı **İlgili Kavram** sütununa, seçiminizin nedenini ise **Kısa Gerekçe** sütununa yazınız. Her kavramı bir kez kullanınız.

Kullanılacak Kavramlar: steganografi, kriptografi, dijital filigranlama (digital watermarking), steganaliz, taşıyıcı dosya, gizlenen veri, stego dosya, veri çıkarma

Durum	İlgili Kavram	Kısa Gerekçe
Bir mesajın varlığını fark ettirmemek amacıyla mesajı başka bir dosyanın içine yerleştirmek		
Mesajın içeriğini yetkisiz kişilerin anlayamayacağı hâle getirmeye yönelik yöntemleri incelemek		
Bir görsele sahiplik veya doğrulama amacıyla ayırt edici bir işaret eklemek		
Bir dosyada gizlenmiş veri bulunup bulunmadığını araştırmak		
Test mesajını gizlemek için kullanılan başlangıç görseli		
Taşıyıcı dosyanın içine yerleştirilen test mesajı		
Gizleme işlemi tamamlandıktan sonra oluşturulan yeni çıktı dosyası		
Stego dosyanın içindeki test mesajını geri almak		

ÖLÇME VE DEĞERLENDİRME

A) **Aşağıda Doğru (D) / Yanlış (Y) önermeleri içeren tanılayıcı dallanmış ağaç verilmiştir. Verilen önermenin doğru olduğunu düşünüyorsanız (D), yanlış olduğunu düşünüyorsanız (Y) seçeneğini işaretleyiniz. İlk önermeden başlayarak yapacağınız seçimlerle oklar yönünde ilerleyiniz ve ulaştığınız çıkış noktasını belirleyiniz.**



B) Aşağıdaki yapılandırılmış gridde numaralandırılmış kutucuklarda kriptografiyle ilgili bazı kavramlar verilmiştir. Soruların cevaplarını kutucuk numaralarını kullanarak ilgili boşluklara yazınız. Aynı kutucuk numarasını birden fazla cevap için kullanabilirsiniz.

❶ RSA	❷ Salt	❸ Encoding	❹ Steghide
❺ AES	❻ Dijital sertifika	❼ Hash	❽ LSB
❾ Açık anahtar	❿ Base64	⓫ Dijital imza	⓬ bcrypt
⓭ Gizli anahtar	⓮ Steganografi	⓯ Diffie-Hellman	⓰ Kriptografi

1. Bilginin gizliliğini, bütünlüğünü ve güvenliğini destekleyen yöntemleri inceleyen genel alan hangisidir?

   Cevap: .....

2. Veriyi gizlemek amacıyla değil, farklı bir gösterim biçimine dönüştürmek amacıyla kullanılan kavramlar hangileridir?

   Cevap: .....

3. Tek yönlü özet üretme ve parolaların daha güvenli saklanması süreciyle ilişkili kavramlar hangileridir?

   Cevap: .....

4. Aynı anahtarın hem şifreleme hem de şifre çözme işleminde kullanıldığı simetrik şifreleme algoritması hangisidir?

   Cevap: .....

5. Açık ve gizli anahtar ilişkisiyle veya ortak gizli anahtar oluşturma mantığıyla ilişkili kavramlar hangileridir?

   Cevap: .....

6. Dijital imza oluşturma ve doğrulama süreciyle doğrudan ilişkili kavramlar hangileridir?

   Cevap: .....

7. Açık anahtarı bir kişi, kurum veya web sitesi kimliğiyle ilişkilendirmeye yardımcı olan kavram hangisidir?

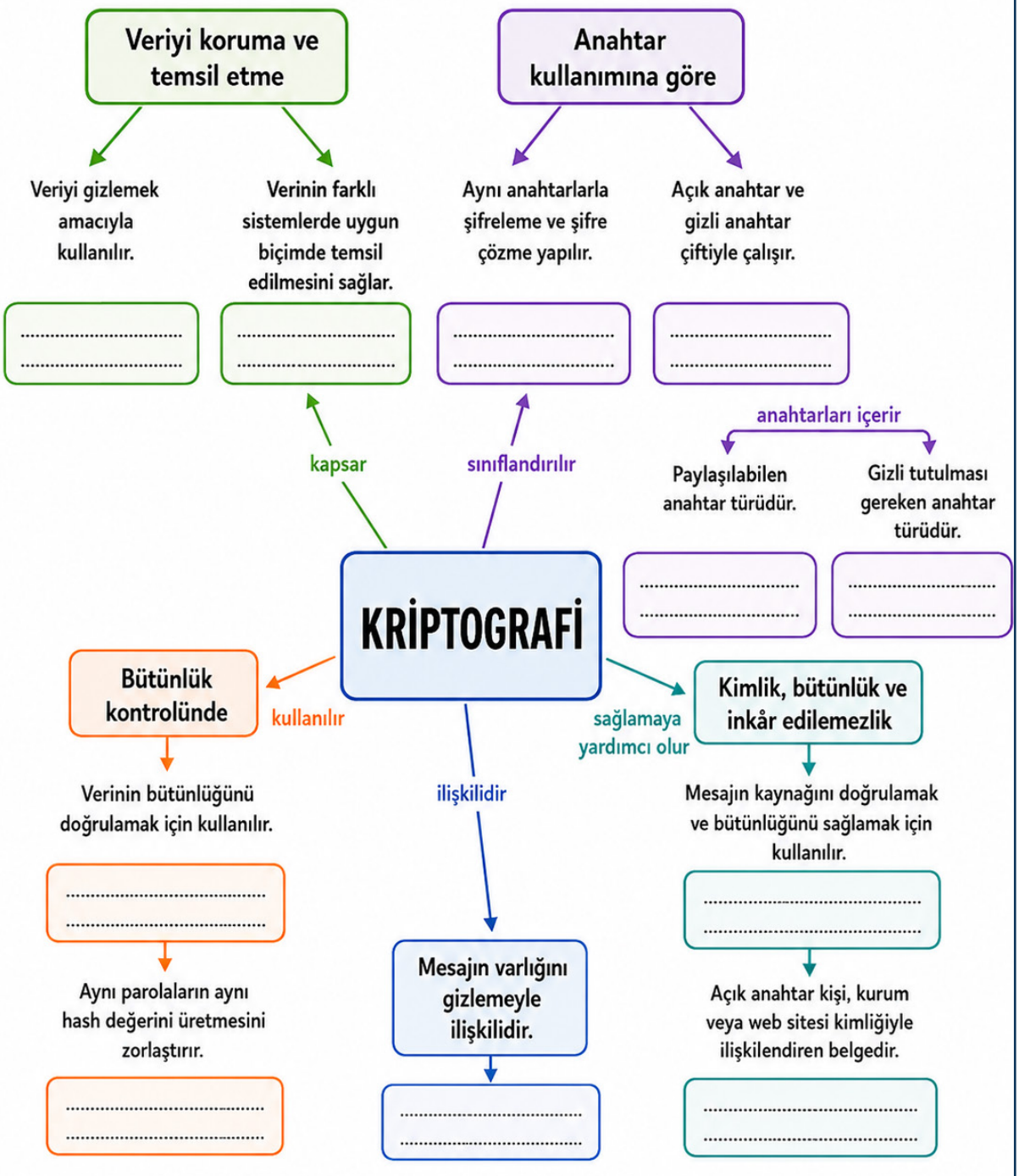
   Cevap: .....

8. Görsel içerisine veri gizleme süreciyle ilişkili kavramlar hangileridir?

   Cevap: .....

C) Aşağıdaki kavramları uygun boşluklara yerleştirerek kavram haritasını tamamlayınız.

şifreleme | hash | salt | simetrik kriptografi | asimetrik kriptografi | açık anahtar | gizli anahtar | dijital imza | dijital sertifika | steganografi | encoding



Ç) 1-4. soruları aşağıda verilen metne göre cevaplayınız.

Bir öğrenci, öğretmeninin paylaştığı **ag_guvenligi_test.pdf** adlı test dosyasını indirir. Öğretmeni dosyanın SHA-256 hash değerini sınıfta paylaşmıştır. Öğrenci dosyanın hash değerini kendi bilgisayarında hesapladığında öğretmenin verdiği değerle aynı olduğunu görür. Daha sonra dosyanın bir kopyasına tek bir nokta ekleyip hash değerini tekrar hesaplar ve hash değerinin değiştiğini fark eder.

1. İlk hash değerinin öğretmenin verdiği değerle aynı çıkması ne anlama gelir?

   .....

2. Dosyaya tek bir nokta eklendiğinde hash değerinin değişmesi neyi gösterir?

   .....

3. Bu işlem şifreleme midir, hashleme midir? Gerekçesiyle yazınız.

   .....

4. Bu uygulamada gerçek kişisel dosya kullanmak doğru mudur? Neden?

   .....

KAYNAKÇA

- Adam, M., Hammoudeh, M., Alrawashdeh, R., & Alsulaimy, B. (2024). A survey on security, privacy, trust, and architectural challenges in IoT systems. IEEE Access.
- Agham, V. (2016, April). Unified threat management. International Research Journal of Engineering and Technology (IRJET).
- Ağ Mimarisi Güvenliği Kılavuzu. (2015). Ankara: TÜBİTAK BİLGEM Bilişim ve Bilgi Güvenliği İleri Teknolojiler Araştırma Merkezi.
- Aliero, M. S., Shamaki, B. I., Abubakar, I., Kalgo, B. S., & Bello, A. M. (2020, September). Web application firewall: Review. International Journal of Contemporary Innovative Research and Analysis Studies.
- Altunay, H. C. (2024, September). Analysis of cyber attacks using honeypot. Black Sea Journal of Engineering and Science.
- Arslan, Y. (2021). Deploying data loss prevention (DLP) systems in big environments. Yönetim Bilişim Sistemleri Dergisi.
- Arvind, S., & Narayanan, V. A. (2019). An overview of security in CoAP: Attack and analysis. In Proceedings of the 5th International Conference on Advanced Computing & Communication Systems (pp. 655–660). Piscataway, NJ: IEEE.
- Bray, S. W. (2020). Implementing cryptography using Python. Indianapolis, IN: Wiley Publishing.
- Browning, P. (2022). 101 Labs CompTIA Network+ (Version 2). Reality Press Ltd.
- Browning, P. ve Tafa, F. (2020). 101 Labs Cisco Certified Network Associate (CCNA): Hands-on practical labs for the Implementing and Administering Cisco Solutions (CCNA) 200-301 exam. Reality Press Ltd.
- Bulut, A. (2023). Sıfır güven ağ erişim mimarisinde anomali tespiti (Yayımlanmamış yüksek lisans tezi). İstanbul Ticaret Üniversitesi, İstanbul.
- Cheddad, A., Condell, J., Curran, K. ve Mc Kevitt, P. (2010). Digital image steganography: Survey and analysis of current methods. Signal Processing, 90(3), 727–752. DOI: 10.1016/j.sigpro.2009.08.010
- Cisco Networking Academy. CCNA 1: Introduction to Networks v7.0 (ITN) [Ders materyali]. Cisco.
- Cisco Networking Academy. (2025). Bilişim teknolojilerinin temelleri kurs dokümanları.
- Cprime. (2024). Security by design: 7 principles you need to know. Retrieved January 25, 2025, from https://www.cprime.com/resources/blog/security-by-design-7-principles-you-need-to-know/
- Çavdar, T., & Öztürk, E. (2018). Nesnelerin interneti için yeni bir mimari tasarımı. Sakarya Üniversitesi Fen Bilimleri Enstitüsü Dergisi, 22(1), 39–48. doi:10.16984/saufenbilder.285444
- Daldoul, Y., & Berrima, M. (2024). A robust certificate management system to prevent evil twin attacks in IEEE 802.11 networks. International Journal of Information Technology, 1–11.
- Dlodlo, N., & Gatsheni, B. (2015). A brief history of IoT. In T. Karim (Ed.), Internet of Things and wireless sensor networks (pp. 1–16). Cham: Springer. doi:10.1007/978-3-031-39650-2_1
- Elektronik İmza Kanunu (Kanun No. 5070). (2004, 23 Ocak). T.C. Resmî Gazete (Sayı: 25355).
- Emmungil, L. (2010). Bilgisayar donanımı. İstanbul: Kodlab Yayınları.

- Eroğlu, E., Ataizi, M., Yüksel, N. A., & Yüksel, A. H. (2013). Etkili iletişim teknikleri. Eskişehir: Anadolu Üniversitesi Yayınları.
- Forouzan, B. A. (2007). Data communications and networking (4th ed.). New York, NY: McGraw-Hill.
- Gupta, A., Ninawe, S., Bariyekar, V., & Asati, R. (2019, February). Network intrusion prevention system. International Journal of Advanced Research in Computer and Communication Engineering.
- Josefsson, S. (2006). The Base16, Base32, and Base64 data encodings (RFC 4648). RFC Editor. DOI: 10.17487/RFC4648
- Kurose, J. F., & Ross, K. W. (2021). Computer networking: A top-down approach (8th ed.). Boston, MA: Pearson.
- Kurose, J. F. ve Ross, K. W. (2022). Computer networking: A top-down approach (8. bs., Global ed.). Pearson Education Limited.
- Mao, W. (2003). Modern cryptography: Theory and practice. Upper Saddle River, NJ: Prentice Hall PTR.
- Menezes, A. J., van Oorschot, P. C. ve Vanstone, S. A. (1996). Handbook of applied cryptography. CRC Press.
- Millî Eğitim Bakanlığı. (2024). Türkiye Yüzyılı Maarif Modeli ortak metni. Millî Eğitim Bakanlığı.
- Millî Eğitim Bakanlığı [MEB]. (2026). Siber güvenlik alanı çerçeve öğretim programı. Ankara: T.C. Millî Eğitim Bakanlığı.
- Millî Eğitim Bakanlığı [MEB]. (2026). Siber güvenlik alanı ders bilgi formu. Ankara: T.C. Millî Eğitim Bakanlığı.
- National Institute of Standards and Technology [NIST]. (2015). Secure Hash Standard (SHS) (FIPS PUB 180-4). U.S. Department of Commerce. DOI: 10.6028/NIST.FIPS.180-4
- National Institute of Standards and Technology [NIST]. (2023). Advanced Encryption Standard (AES) (FIPS PUB 197-upd1). U.S. Department of Commerce. DOI: 10.6028/NIST.FIPS.197-upd1
- Nelson, R. B., & Wallick, J. B. (1999). Sunuş yapma (E. S. Yarmalı, Çev.). İstanbul: Hayat Yayınları.
- Paar, C., & Pelzl, J. (2009). Understanding cryptography: A textbook for students and practitioners. Berlin: Springer.
- Pakin, S., & Rieffel, E. G. (2021, November 15). Introduction to quantum computing (LA-UR-19-31426) [Tutorial slides]. SC21 Tutorial. Los Alamos National Laboratory & NASA Ames Research Center.
- Sağıroğlu, Ş., & Akleylek, S. (2020). Siber güvenlik ve savunma: Biyometrik ve kriptografik uygulamalar. Ankara.
- Sağıroğlu, Ş., & Akleylek, S. (2021). Siber güvenlik ve savunma: Blok zincir ve kriptoloji. Ankara.
- Sağıroğlu, Ş., & Akleylek, S. (2022). Siber güvenlik ve savunma: Siber güvenlik ontolojisi, tehditler ve çözümler. Ankara.
- Sağıroğlu, Ş., & Alkan, M. (2018). Siber güvenlik ve savunma: Farkındalık ve caydırıcılık. Ankara.
- Sağıroğlu, Ş., & Şenol, M. (2019). Siber güvenlik ve savunma: Problemler ve çözümler. Ankara.
- Sequeira, A. (2022). CompTIA Network+ N10-008 cert guide. Pearson IT Certification.
- Serengil, S. (2011). Attacking Turkish texts encrypted by homophonic cipher. doi:10.13140/RG.2.1.3706.7608

- Shinde, O., Kulkarni, V., Patani, H., Rajput, A., & Jaiswal, R. C. (2024). A survey: Network attack detection and mitigation techniques. In International Conference on Smart Computing and Communication (pp. 263–275). Singapore: Springer Nature.
- Shiu, H.-J., Yang, C.-T., Tsai, Y.-R., Lin, W.-C., & Lai, C.-M. (2023). Maintaining secure level on symmetric encryption under quantum attack. Applied Sciences, 13(11), 6734. doi:10.3390/app13116734
- Singh, G. D. (2022). The ultimate Kali Linux book: Perform advanced penetration testing using Nmap, Metasploit, Aircrack-ng, and Empire. Birmingham: Packt Publishing.
- Stallings, W. (2006). Cryptography and network security: Principles and practice (4th ed.). Upper Saddle River, NJ: Pearson Prentice Hall.
- Stallings, W. (2017). Cryptography and network security: Principles and practice (7th ed.). Boston, MA: Pearson.
- Stinson, D. R. (1995). Cryptography: Theory and practice. Boca Raton, FL: CRC Press.
- Sun, P., Shen, S., Wan, Y., Wu, Z., Fang, Z., & Gao, X. Z. (2024). A survey of IoT privacy security: Architecture, technology, challenges, and trends. IEEE Internet of Things Journal.
- Temoshok, D., Fenton, J., Choong, Y.-Y., Lefkovitz, N., Regenscheid, A., Galluzzo, R. ve Richer, J. (2025). Digital identity guidelines: Authentication and authenticator management (NIST SP 800-63B-4). National Institute of Standards and Technology. DOI: 10.6028/NIST.SP.800-63b-4
- Türk Dil Kurumu. (2019). Türkçe sözlük. Atatürk Kültür, Dil ve Tarih Yüksek Kurumu Türk Dil Kurumu Yayınları.
- Türk Dil Kurumu. (2023). Yazım kılavuzu (28. baskı). Atatürk Kültür, Dil ve Tarih Yüksek Kurumu Türk Dil Kurumu Yayınları.
- Wobst, R., & Shafir, A. (2007). Cryptology unlocked. Chichester: John Wiley & Sons.
- Wong, T. G. (2022). Introduction to classical and quantum computing. Rooted Grove.
- Yılmaz, H. (2014). TS ISO/IEC 27001 bilgi güvenliği yönetimi standardı kapsamında bilgi güvenliği uygulamaları. Ankara.
- Yürekten, Ö., & Sağıroğlu, Ş. (Yıl belirtilmemiş). Güvenli yazılım geliştirme ve tehdit modelleme. In International Symposium on Digital Forensics and Security.

* Kaynakça, APA 6 referans gösterme sistemiyle hazırlanmıştır.

CEVAP ANAHTARLARI KAREKODU

Cevap anahtarlarına bu karekodu okutarak ulaşabilirsiniz.

Dijital dokümanlarda karekodun üzerine tıklayarak içeriğe ulaşabilirsiniz.



GENEL AĞ, GÖRSEL, E-İÇERİK KAYNAKÇASI KAREKODU

Materyalin görsel kaynakçası, genel ağ kaynakçası ve e-içerik kaynakçasına bu karekodu okutarak ulaşabilirsiniz.

Dijital dokümanlarda karekodun üzerine tıklayarak içeriğe ulaşabilirsiniz.




ROMANYA
UKRAYNA
RUSYA FEDERASYONU
HAZAR DENİZİ
BULGARİSTAN
KARADENİZ
GÜRCİSTAN
YUNANİSTAN
ERMENİSTAN
AZERBAYCAN
İRAN
SURİYE
IRAK
LİBYA
MISIR
AKDENİZ
EGE DENİZİ
MARMARA DENİZİ
KUZEY KIBRIS TÜRK CUMHURİYETİ
GÜNEY KIBRIS RUM YÖNETİMİ
LÜBNAN
İSRAİL
FİLİSTİN
Sofya
Bükreş
Atina
Beyrut
Şam
Bağdat
Tel Aviv
Lefkoşa
Erenköy
Tiflis
Erivan
Sinop
Samsun
Trabzon
Rize
Artvin
Ordu
Giresun
Gümüşhane
Bayburt
Kars
Ağrı
Iğdır
Erzurum
Erzincan
Tunceli
Bingöl
Muş
Bitlis
Van
Hakkâri
Şırnak
Siirt
Batman
Diyarbakır
Mardin
Şanlıurfa
Gaziantep
Adıyaman
Kilis
Osmaniye
Hatay
Adana
Mersin
Antalya
Karaman
Konya
Aksaray
Niğde
Nevşehir
Kayseri
Kahramanmaraş
Malatya
Elazığ
Sivas
Yozgat
Kırşehir
Kırıkkale
Ankara
Çankırı
Çorum
Amasya
Tokat
Yozgat
Eskişehir
Bilecik
Bursa
Çanakkale
Balıkesir
Kütahya
Afyonkarahisar
Uşak
Manisa
İzmir
Aydın
Denizli
Muğla
Burdur
Isparta
Yalova
Sakarya
Bolu
Düzce
Kocaeli
İstanbul
Tekirdağ
Kırklareli
Edirne
Gökçeada
Zonguldak
Bartın
Karabük
Kastamonu
Tuz Gölü
Van Gölü
Urumiye Gölü
Tuna N.
Meriç N.
Sakarya N.
Kızılırmak N.
Yeşilırmak N.
Çoruh N.
Kura N.
Aras N.
Fırat N.
Dicle N.
Göksu N.
Seyhan N.
Ceyhan N.
Büyük Menderes N.
Küçük Menderes N.
Gediz N.
Nil N.
Süveyş K.
ACARA Ö.C.
NAHÇIVAN Ö.C. (AZERBAYCAN)
TÜRKİYE'NİN MÜLKİ İDARE BÖLÜMLERİ İLE KARA VE DENİZ KOMŞULARI HARİTASI
BAŞKENT
Ankara
İL MERKEZİ
Elazığ
GÖL
ÜLKE SINIRI
ÖZERK BÖLGE SINIRI
AKARSU
0 50 100 200 300 400
Km


TÜRK DÜNYASI HARİTASI
Bağımsız Türk Devletleri
Türk Cumhuriyetleri, Türk Bölgeleri
Türk Toplulukları
0 250 500 1,000 1,500 2,000 Km
TÜRK CUMHURİYETLERİ, TÜRK BÖLGELERİ
1 GAGAVUZ YERİ
2 KARAÇAY-ÇERKESYA
3 KABARDİN-BALKARYA C.
4 DAĞISTAN C.
5 ÇUVAŞİSTAN C.
6 TATARİSTAN C.
7 BAŞKURT C.
8 KARAKALPAKİSTAN C.
9 ALTAY C.
10 HAKASYA C.
TÜRK TOPLULUKLARI
a Avrupa'daki Türkler
b Kosova Türkleri
c Yunanistan Türkleri
ç Bulgaristan Türkleri
d Romanya Türkleri
e Suriye Türkmenleri
f Irak Türkmenleri
g İran Türkleri
h Afganistan Türkmenleri
ı Pakistan Türkmenleri
i Hindistan Türkmenleri
j Çin H. C. Türkleri
k Moğolistan Türkleri
l Rusya Federasyonu Türkleri
ÜLKE KISALTMALARI
ARNAVUTLUK ARN
BELÇİKA BEL
BOSNA - HERSEK BH
GÜNEY KIBRIS RUM YÖNETİMİ GKRY
HIRVATİSTAN HRV
İSVİÇRE İS
KARADAĞ KD
KOSOVA KS
KUZEY KIBRIS TÜRK CUMHURİYETİ KKTC
KUZEY MAKEDONYA KMKD
LİHTENŞTAYN LİH
SIRBİSTAN SR
RUSYA FEDERASYONU
TÜRKİYE
KAZAKİSTAN
MOĞOLİSTAN
İRAN
AFGANİSTAN
PAKİSTAN
HİNDİSTAN
ÇİN HALK CUMHURİYETİ
SAHA (YAKUT) C.
TUVA C.
SİNCAN UYGUR ÖZERK BÖLGESİ
Norveç Denizi
Barents Denizi
Kara Denizi
Bering Denizi
Ohotsk Denizi
Akdeniz
Karadeniz
Hazar Denizi
Umman Denizi
Yemen Denizi
Kızıldeniz
Akdeniz
Tiren Denizi
Adriyatik Denizi
Ege Denizi
Marmara Denizi
Kuzey Denizi
Baltık Denizi
Manş Denizi
İrlanda Denizi
İzlanda
Norveç
İsveç
Finlandiya
Rusya Federasyonu
Almanya
Fransa
İspanya
Portekiz
İtalya
Yunanistan
Bulgaristan
Romanya
Moldova
Ukrayna
Belarus
Polonya
Gürcistan
Azerbaycan
Ermenistan
Türkmenistan
Özbekistan
Tacikistan
Kırgızistan
Moğolistan
Çin H. C.
Hindistan
Pakistan
Afganistan
İran
Irak
Suriye
Lübnan
Ürdün
İsrail
Filistin
Mısır
Libya
Tunus
Cezayir
Fas
Çad
Sudan
Nijer
Suudi Arabistan
Kuveyt
Katar
Birleşik Arap Emirlikleri
Umman
Yemen
Bangladeş
Kuzey Kıbrıs Türk Cumhuriyeti
Güney Kıbrıs Rum Yönetimi
Moskova
Astana
Ankara
Bişkek
Taşkent
Aşkabat
Duşanbe
Kabil
İslamabad
Yeni Delhi
Pekin
Ulanbator
Trablus
Lefkoşa
Şam
Amman
Bağdat
Tahran
Riyad
Doha
Abu Dabi
Muskat
Sana
Dakka
Cebeltarık B.
Kattegat
Skagerrak
Helsinki
Oslo
Kopenhag
Berlin
Varşova
Paris
Londra
Dublin
Madrid
Lizbon
Roma
Viyana
Budapeşte
Belgrad
Sofya
Atina
Kiev
Minsk
Kişinev
Tiflis
Bakü
Erivan
Aşkabat
Taşkent
Bişkek
Duşanbe
Kabil
İslamabad
Yeni Delhi
Pekin
Ulanbator
Astana
Moskova
Ural N.
Ob N.
Lena N.
Yenisey N.
İrtiş N.
Volga N.
Don N.
Dinyeper N.
Tuna N.
Ren N.
Elbe N.
Vistül N.
Nil N.
Fırat N.
Dicle N.
Sarı N.
Yangtze N.
Mekong N.
Ganj N.
Hint. N.
Amur N.
Hatanga K.
Laptev D.
Doğu Sibirya D.
Çukçi D.
Beaufort D.
Grönland D.
Labrador D.
Hudson K.
Baffin K.
Davis K.
Grönland
Kanada
ABD
Meksika
Küba
Jamaika
Haiti
Dominik Cum.
Porto Riko
Trinidad ve Tobago
Venezuela
Kolombiya
Panama
Kosta Rika
Nikaragua
Honduras
Salvador
Guatemala
Belize
Ekvador
Peru
Brezilya
Bolivya
Paraguay
Şili
Arjantin
Uruguay
Falkland Adaları
Güney Georgia
Güney Sandwich Adaları
Kuzey Kutup Dairesi
Yengeç Dönencesi
Ekvator
Oğlak Dönencesi
Güney Kutup Dairesi
30° 20° 10° 0° 10° 20° 30° 40° 50° 60° 70° 80° 90° 100° 110° 120° 130° 140° 150° 160° 170° 180°
40° 30° 20° 10°
50° 40° 30° 20° 10°
30° 40° 50° 60° 70° 80° 90° 100° 110° 120°