Ad Soyad: _____ Tarih: _____ Puan: _____

Genel Wi-Fi güvenliği ve şifreleme

Ortadaki adam saldırıları, sahte erişim noktaları, paket koklama, VPN tünelleri ve HTTPS şifrelemesi.

GENEL WI-FI GÜVENLİĞİNE GENEL BAKIŞ

GÜVENCEDE
VERİ ŞİFRELEME
256 bit AES Standardı

UYUMLU
KÜRESEL STANDARTLAR
GDPR ve CCPA çerçeveleri

SIFIR GÜVEN
ERİŞİM POLİTİKASI
Çok Faktörlü Kimlik Doğrulama

Hoş geldin! Bu etkinlik paketi sana herkese açık Wi-Fi güvenliği konusunda rehberlik eder. Şifrelenmemiş ağları, ortadaki adam (MitM) saldırılarını, sahte erişim noktalarını, paket dinlemeyi, VPN tünellerini ve HTTPS iletim güvenliğini keşfedeceksin.

ÇALIŞMA KÂĞIDI KONTROL NOKTALARI

- [ ] **Bölüm 1-4: Siber güvenlikte ve tehdit önlemede ustalaş.**
- [ ] **Bölüm 5-7: Çapraz bulmaca ve kelime avı bulmacalarını çöz.**
- [ ] **Bölüm 8-9: Vaka çalışmalarını ve şifre görevini çöz.**
- [ ] **Bölüm 10: Temel ve ileri düzey SSS sayfalarını gözden geçir.**
- [ ] **Bölüm 11: 10 ilginç gerçek dünya gerçeğini keşfet.**
- [ ] **Bonus: Hızlı Düşün görevi.**

VPN.com siber güvenlik rehberini aç

URL: https://www.vpn.com/tr/siber-guvenlik/halka-acik-wifi-guvenligi/

Herkese Açık Wi-Fi Güvenliği Öğrenme Yol Haritan

- Paket dinleme ve sahte erişim noktaları dahil yaygın herkese açık Wi-Fi risklerini belirle.
- Aktarım halindeki verileri korumak için VPN şifreleme tünelleri uygula.
- Uzaktan çalışanlar için HTTPS'i ve güvenli web tarayıcı ayarlarını zorunlu kıl.

GENEL WI-FI GÜVENLİĞİ REHBERİ YÖNERGELERİ

Çoktan seçmeli ve doğru/yanlış sorularını cevapla, boşluk doldurma cümlelerini kelime bankasını kullanarak tamamla, tanımları eşleştir, çapraz bulmacayı ve kelime avı bulmacasını çöz. Bilgini şu konulara uygula: uzaktan erişim güvenliği. Hızlı Düşün bonus etkinliğiyle bitir.

GENEL WI-FI GÜVENLİĞİ VE AKTARIM KORUMASI (GİRİŞ)

Şifrelenmemiş herkese açık Wi-Fi erişim noktaları, ağ trafiğini paket dinlemeye ve Evil Twin sahteciliğine açık bırakır. Trafiği güvenli VPN şifreleme tünellerinden geçirmek ve yalnızca HTTPS'e izin veren HSTS kurallarını uygulamak, oturumları yerel ağ müdahalesine karşı korur.

HER KONTROL NOKTASINI DİKKATLE OKU VE DOĞRU CEVABI SEÇ YA DA YAZ.

Kontrol Noktası 1: Çoktan seçmeli görev

1 **1. Ortadaki adam (MitM) saldırısı nedir?**

- A. Ortak bir ağda iki taraf arasındaki iletişimi araya girerek yakalamak ve değiştirmek
- B. Kullanıcı kayıtlarını hedef alan bir veritabanı çekme tekniği
- C. Web sunucularını ağ trafiği istekleriyle boğmak
- D. Yerel sabit disk depolama birimlerini silmek

2 **2. Sahte erişim noktası (Evil Twin) nedir?**

- A. Meşru bir ağla aynı SSID ile yapılandırılmış kötü amaçlı Wi-Fi erişim noktası
- B. Veritabanı yedeklerini izlemek için kullanılan bir yönetim aracı
- C. Güvenli bir VPN ağ geçidi yapılandırması
- D. Yetkili posta sunucularını eşleyen bir DNS kaydı

3 **3. VPN, herkese açık Wi-Fi trafiğini nasıl korur?**

- A. Tüm ağ paketlerini şifreli bir tünele sarar ve koklayıcılar tarafından okunamaz hale getirir
- B. Gelen tüm bağlantı isteklerini otomatik olarak engeller
- C. Fiziksel ağ kartının MAC adresini değiştirir
- D. Web tarayıcısındaki önbelleğe alınmış çerezleri siler

4 **4. Paket dinleme (packet sniffing) nedir?**

- A. Ağ paketlerini yakalayıp kaydetmek için donanım veya yazılım araçları kullanmak
- B. Yinelenen dosyalar için yerel dizinleri taramak
- C. Veritabanı okuma ayrıcalıklarını kullanıcı rollerine göre kısıtlamak
- D. Depolama sürücülerini AES-256 anahtarlarıyla şifrelemek

5 **5. HTTPS'in rolü nedir?**

- A. Tarayıcı ile web sunucusu arasındaki oturum trafiğini şifrelemek
- B. Gelen e-posta iletilerini ağ geçidinde filtrelemek
- C. Daha hızlı sayfa yüklemeleri için görselleri sıkıştırmak
- D. Ağa bağlı depolamada dosya yapılarını yönetmek

Kontrol Noktası 2: Doğru/Yanlış görevi

6 Soru 6

6. Bağlı kullanıcılar, açık herkese açık Wi-Fi ağlarında düz metin verileri kolayca yakalayabilir.

○ Doğru ○ Yanlış

7 Soru 7

7. Sahte erişim noktaları (Evil Twin) her zaman ağ yöneticileri tarafından yetkilendirilir.

○ Doğru ○ Yanlış

8 Soru 8

8. VPN, herkese açık ağlarda paket koklamaya karşı trafiği korumada etkisizdir.

○ Doğru ○ Yanlış

9 Soru 9

9. HTTPS yalnızca URL yolunu şifreler, paket yükünü düz metin olarak bırakır.

○ Doğru ○ Yanlış

10 Soru 10

10. WPA3 güvenliği kullanan Wi-Fi erişim noktaları, açık ve parolasız ağlardan daha güçlü koruma sunar.

○ Doğru ○ Yanlış

Kontrol Noktası 3: Anahtar terim yerleştirme

Aşağıdaki her cümleyi oku ve boşluğu Kelime Bankası'ndaki doğru terimle doldur.

1. Genel Wi-Fi'da özel parolaları yakalamaya _____ denir.
2. Yerel ağdaki ham paketleri analiz etmeye _____ denir.
3. Bir otelin Wi-Fi ağını taklit eden sahte erişim noktası bir _____ olarak adlandırılır.
4. Web trafiğinin aktarımını güvence altına almak için _____ ile şifreleme gerekir.
5. Tüm ağ çıkışlarını şifrelemek için bir _____ kullanılır.
6. Genel ağlar üzerinden şifreli bir iletişim yoluna _____ denir.

KELİME BANKASI

ARA DİNLEME | GÜVENLİK DUVARI | HTTPS | KÖTÜ İKİZ | PAKET DİNLEME | TÜNEL | VPN İSTEMCİSİ | WPA3

Cevaplarını buraya yaz:

1.
2.
3.
4.
5.
6.

Kontrol Noktası 4: Güvenlik kavramı eşleştirme

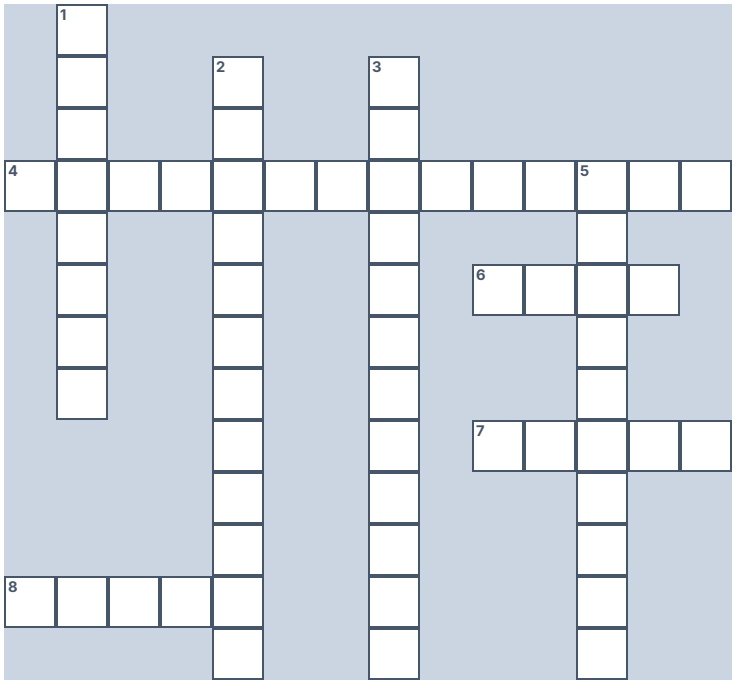
TANIM EŞLEŞTİRME

Soldaki her kelimeyi, doldurulabilir giriş kutusuna ilgili harfi (A-H) yazarak sağdaki doğru tanımıyla eşleştir.

☐	1. DİNLEME	A	Modern Wi-Fi güvenlik standardı.
☐	2. PAKET DİNLEME	B	Aktarım sırasında güvenli veri yolu.
☐	3. KÖTÜ İKİZ	C	Gelen trafiği filtreleme.
☐	4. HTTPS	D	Wi-Fi'ı taklit eden sahte erişim noktası.
☐	5. VPN	E	Aktarım halindeki trafiği okumak.
☐	6. TÜNEL	F	Ağ veri paketlerini yakalama.
☐	7. WPA3	G	Şifreli sanal özel ağ.
☐	8. GÜVENLİK DUVARI	H	Güvenli web iletimi.

Kontrol Noktası 5: Bulmaca

Bulmacayı, etkin beyaz kutulara harf yazarak çöz. Sayılar aşağıdaki ipuçlarına karşılık gelir.



SOLDAN SAĞA

4. Gelen trafiği filtreleme (14)

6. Modern Wi-Fi güvenlik standardı (4)

7. Aktarım sırasında güvenli veri yolu (5)

8. Güvenli web iletimi (5)

YUKARIDAN AŞAĞI

1. Wi-Fi'yi taklit eden sahte erişim noktası (8)

2. Şifreli sanal özel ağ (12)

3. Ağ veri paketlerini yakalama (12)

5. Aktarım halindeki trafiği okuma (10)

Kontrol Noktası 5, alternatif: Erişilebilir bulmaca ipuçları

Ekran okuyucu ve klavye kullanıcıları, bulmaca cevaplarını aşağıdaki metin alanlarına doğrudan yazabilir.

SOLDAN SAĞA

4 soldan sağa: Gelen trafiği filtreleme (14 harf):

6 soldan sağa: Modern Wi-Fi güvenlik standardı (4 harf):

7 soldan sağa: Aktarım sırasında güvenli veri yolu (5 harf):

8 soldan sağa: Güvenli web iletimi (5 harf):

YUKARIDAN AŞAĞI

1 yukarıdan aşağı: Wi-Fi'yi taklit eden sahte erişim noktası (8 harf):

2 yukarıdan aşağı: Şifreli sanal özel ağ (12 harf):

3 yukarıdan aşağı: Ağ veri paketlerini yakalama (12 harf):

5 yukarıdan aşağı: Aktarım halindeki trafiği okuma (10 harf):

Kontrol Noktası 6: Gizli kelime bulmacası

Aşağıdaki ızgarada gizlenmiş 8 temel kelimeyi bul. Kelimeler yatay, dikey veya çapraz olabilir.

E O M Ü C K Z Y F V N U T J T

M O E M E L N İ D A R A B M U

E S K G T Ç Y T İ P B Ü Z V K

L P Ö V H N D A Ç İ H T T P S

N Ö U Ü Ü J I T Ğ Ş Ğ F B E H

İ İ S R U P Z Ü W E Ğ E R C A

D J O C Z K İ N U P P Ş A R Ü

T I K K G Ğ L E Ğ P A F J S J

E P Ü Ğ B Ş F L Y M Y 3 Ü R Ğ

K S V A Z İ K İ Ü T Ö K O T M

A G Ü V E N L İ K D U V A R I

P M Z N H O S Ğ O T Ş N Ş Ş İ

A E V P N İ S T E M C İ S İ N

L J B M T F G O Ö Ü Y I İ T I

Y U V O İ H Z H I L A E H B S

KELİME LİSTESİ

ARADİNLEME PAKETDİNLEME KÖTÜİKİZ HTTPS VPNİSTEMCİSİ TÜNEL WPA3 GÜVENLİKDUVARI

Kontrol Noktası 6, alternatif: Erişilebilir kelime eşleştirme

Kelime Bulmaca'daki 8 kelimenin her birini, boşluğa harfi (A-H) yazarak doğru tanımıyla eşleştir.

KELİME TERİMLERİ

- **A. ARADİNLEME**
- **B. PAKETDİNLEME**
- **C. KÖTÜİKİZ**
- **D. HTTPS**
- **E. VPNİSTEMCİSİ**
- **F. TÜNEL**
- **G. WPA3**
- **H. GÜVENLİKDUVARI**

TANIMLAR VE EŞLEŞTİRME ALANLARI

1. Modern Wi-Fi güvenlik standardı. ____
2. Wi-Fi'yi taklit eden sahte erişim noktası. ____
3. Ağ veri paketlerini yakalama. ____
4. Aktarım sırasında güvenli veri yolu. ____
5. Gelen trafiği filtreleme. ____
6. Aktarım halindeki trafiği okuma. ____
7. Şifreli sanal özel ağ. ____
8. Güvenli web iletimi. ____

Kontrol Noktası 7: Karışık harflerden kelime bulma görevi

Temel siber güvenlik kavramlarını ve terimlerini ortaya çıkarmak için aşağıdaki harfleri doğru sıraya diz. Cevaplarını verilen giriş kutularına yaz.

1. MLNİRAEEDA
2. ÜKZÖİKİT
3. VPMESCNTİSİİ
4. 3AWP
5. AENİEKTLDPME
6. PHTST
7. ELTNÜ
8. EKALDUÜIGİVRVN

Bonus etkinlik: Hızlı Düşün

HER KATEGORİ İÇİN 3 CEVAP. LİSTEYİ İLK TAMAMLAYAN KAZANIR.

1	Yazılımı güncelleme nedenleri			
2	Wi-Fi'a otomatik bağlanan cihazlar			
3	Asla paylaşmaman gereken bilgiler			
4	Bugün başlayabileceğin güvenli alışkanlıklar			
5	Kafede güvende kalma yolları			
6	Hacklenebilecek cihazlar			
7	Açık Wi-Fi'da bir hackerın görebileceği şeyler			
8	Sahte Wi-Fi ağının işaretleri			
9	Herkese açık Wi-Fi'a alternatifler			
10	E-postadaki uyarı işaretleri			
11	Herkese açık Wi-Fi'da yapmadığın şeyler			
12	Ücretsiz Wi-Fi olan yerler			
13	Hesaplarını koruma yolları			
14	Bir bilgisayarın virüslü olduğunu gösteren işaretler			
15	Şüpheli görünen Wi-Fi adları			

Kontrol Noktası 8: Siber güvenlik vaka çalışmaları

Öğrendiğin kavramları aşağıdaki gerçek dünya senaryolarını çözmek için uygula.

VAKA ÇALIŞMASI 1: HERKESE AÇIK WI-FI'DE PAKET DİNLEMEYİ KONTROL ALTINA ALMA



Senaryo: Herkese açık bir havalimanı Wi-Fi ağına bağlı olan uzaktaki bir satış yöneticisi, düz metin olarak gönderilen birkaç hassas iş e-postasının gönderildikten kısa süre sonra sızdırıldığını fark ediyor.

Tartışma sorusu: Herkese açık ağ risklerini analiz et ve bir trafik şifreleme çözümünü özetle.

VAKA ÇALIŞMASI 2: EVIL TWIN SAHTE HOTSPOT SAVUNMASI



Senaryo: Saldırganlar, meşru bir kafe erişim noktasını taklit eden 'CoffeeShop_Guest' adlı sahte bir kablosuz erişim noktası kurarak habersiz misafirlerin ağ trafiğini yakalıyor.

Tartışma sorusu: Sahte erişim noktalarını tespit etmek ve engellemek için doğrulama adımlarını ayrıntılı anlat.

Kontrol Noktası 9: Şifreyi Çöz

Bir siber güvenlik uzmanı, ağ varlıklarını çevrimiçi tehdit aktörlerine karşı korur. Aşağıdaki Harf-Sayı anahtarını kullanarak, eşleşen harfleri boşluklara yazıp mesajın şifresini çöz.

HARFTEN SAYIYA ŞİFRELEME ANAHTARI

A=1 B=2 C=3 Ç=4 D=5 E=6 F=7 G=8 Ğ=9 H=10

I=11 İ=12 J=13 K=14 L=15 M=16 N=17 O=18 Ö=19 P=20

R=21 S=22 Ş=23 T=24 U=25 Ü=26 V=27 Y=28 Z=29

8	6	17	6	15		14	1	2	15	18	22	25	29		1	9
24	21	1	7	12	9	12	17	12		27	20	17		12	15	6
					23	12	7	21	6	15	6					

Çözülen mesaj:

İPUCU: HER SAYI, O HARFİN ALFABEDEKİ SIRASINI GÖSTERİR (ÖR. 1 = A, 2 = B, 29 = Z).

Kontrol Noktası 10: Siber güvenlik hakkında sık sorulan sorular – temel düzey (Bölüm A)

Çevrimiçi tehditlerin azaltılmasına ilişkin sık sorulan soruları ve cevapları incele.

Q1: Genel Wi-Fi neden güvensizdir?

Açık genel Wi-Fi, trafiği havada şifrelemez; bu yüzden yakındaki kişiler korumasız verileri yakalayabilir. [2]

Q2: Paket koklama nedir?

Paket koklayıcı, ağ arayüzünden geçen ham veriyi yakalar ve düz metin parolaları ile trafik ayrıntılarını açığa çıkarır.

Q3: Evil Twin nedir?

Güvenilir bir yerel Wi-Fi erişim noktasının adını ve ayarlarını taklit eden, bilgisayar korsanlarınca kurulmuş sahte erişim noktası.

Q4: VPN beni nasıl korur?

Trafiğini şifreli bir tünel üzerinden yönlendirir ve gezinme etkinliğini yerel ağ dinleyicilerinden gizler.

Q5: HTTPS beni herkese açık Wi-Fi'da korur mu?

Evet, tarayıcın ile web sitesi arasında değiş tokuş edilen verileri şifreler ve VPN ek bir koruma katmanı ekler.

Kontrol Noktası 10: Siber güvenlik hakkında sık sorulan sorular – temel düzey (Bölüm B)

Çevrimiçi tehditlerin azaltılmasına ilişkin sık sorulan soruları ve cevapları incele.

Q6: WPA3 nedir?

Çevrimdışı sözlük saldırılarına karşı daha güçlü şifreleme ve koruma sunan modern Wi-Fi Protected Access standardı. [1]

Q7: Herkese açık Wi-Fi kötü amaçlı yazılım bulaştırabilir mi?

Evet, saldırganlar trafiği araya girerek ele geçirebilir ve tarayıcı oturumuna kötü amaçlı indirme istemleri (drive-by indirmeler) enjekte edebilir.

Q8: Dosya paylaşımının riski nedir?

Dosya paylaşımı etkinse herkese açık ağdaki diğer kullanıcılar yerel klasör dizinini okuyabilir veya değiştirebilir.

Q9: Oturum açma portalı (captive portal) nedir?

Otel veya kafe ağlarının internet erişimi vermek için kullandığı, bazen saldırganlar tarafından taklit edilebilen giriş sayfası.

Q10: Kullanmadığımda Wi-Fi'ı kapatmalı mıyım?

Evet, Wi-Fi'yi kapatmak cihazının güvenilmeyen ağlara otomatik olarak bağlanmasını engeller.

Kontrol Noktası 10: Güvenlik hakkında sık sorulan sorular – ileri düzey (Bölüm C)

Güvenlik çerçevelerinin, kötü amaçlı yazılım analizinin ve veri uyumluluğunun ileri düzey teknik yönlerini keşfet.

Q1: Ortadaki Adam saldırısı DNS'i nasıl istismar eder?

Hedef tarayıcıları hedef alan adları yerine benzer görünen kimlik avı iniş sayfalarına yönlendirmek için sahte bir yönlendiricide DNS sahteciliği kullanarak.

Q2: Oturum ele geçirme nedir?

Bir saldırganın herkese açık Wi-Fi üzerinden şifrelenmemiş bir oturum çerezini koklaması ve kimlik bilgisi girişlerini atlamak için içe aktarması.

Q3: SSL stripping nedir?

Saldırganın kullanıcının güvenli HTTPS isteğini şifrelenmemiş HTTP'ye düşürerek oturum açma bilgilerini düz metin olarak yakaladığı bir MitM saldırısı.

Q4: HSTS, SSL stripping'e karşı nasıl koruma sağlar?

HTTP Strict Transport Security, tarayıcıları yalnızca HTTPS ile bağlanmaya zorlar ve şifrelenmemiş HTTP'ye geri dönüşü reddeder. [3]

Q5: Bölünmüş tünelli VPN nedir?

Yalnızca kurumsal trafiği VPN üzerinden yönlendirip genel internet verisini doğrudan gönderen ve sızıntı yolu riski doğurabilen bir yapılandırma.

Kontrol Noktası 10: Güvenlik hakkında sık sorulan sorular – ileri düzey (Bölüm D)

Güvenlik çerçevelerinin, kötü amaçlı yazılım analizinin ve veri uyumluluğunun ileri düzey teknik yönlerini keşfet.

Q6: WPA2 KRACK'e karşı neden savunmasızdır?

Key Reinstallation Attack, Wi-Fi parolasını bilmeden paketlerin şifresini çözmek için WPA2 dört yönlü el sıkışmasından yararlanır.

Q7: İstemci yalıtımı nedir?

Bağlı Wi-Fi cihazlarının birbirleriyle doğrudan iletişim kurmasını engelleyen, yerel koklamayı durduran yönlendirici güvenlik ayarı.

Q8: Saldırganlar sahte DNS sunucularını nasıl kullanır?

İstemcilere sahte DNS sunucuları atamak için sahte yönlendiriciler yapılandırır; böylece tüm web aramalarını yakalayıp yeniden yazabilirler.

Q9: VPN yerel MAC adresimi gizleyebilir mi?

Hayır. MAC adresleri yerel katman-2 tanımlayıcılarıdır; bunun yerine cihazının yerleşik MAC rastgeleleştirme (özel adres) ayarını kullan.

Q10: Captive portal sahteciliği saldırısı nedir?

Bir saldırganın, ücretsiz Wi-Fi erişimi görüntüsü altında kimlik bilgilerini çalmak için sahte erişim noktasında sahte bir kimlik doğrulama portalı barındırması.

Bölüm 11: Siber güvenlikle ilgili 10 gerçek dünya gerçeği ve içgörüsü

Güvenlik ihlalleri, savunma mekanizmaları ve uyumluluk standartlarıyla ilgili gerçek dünya bilgilerini incele.

1. GÜVENLİK İPUCU

Uzaktan çalışanlar çoğunlukla kafelerde, otellerde ve havalimanlarında, ağın güvenliğini denetleyemedikleri Wi-Fi'lar kullanır.

2. GÜVENLİK İPUCU

Evil Twin sahte erişim noktası, güvenilir bir ağın adını ve MAC adresini birebir kopyalayarak cihazları yanıltabilir.

3. GÜVENLİK İPUCU

Wireshark gibi paket koklama yazılımları ücretsizdir ve şifrelenmemiş HTTP parolalarını düz metin olarak gösterebilir.

4. GÜVENLİK İPUCU

WPA3 güvenliği, yerel kaba kuvvet saldırılarına karşı korunmak için Eşitlerin Eşzamanlı Kimlik Doğrulaması'nı (SAE) kullanır.

5. GÜVENLİK İPUCU

SSL şeritleme saldırıları, ağ geçidinde ilk HTTP yönlendirmelerini ele geçirerek temel HTTPS korumalarını aşar.

6. GÜVENLİK İPUCU

HTTP Strict Transport Security (HSTS) yanıt başlıkları, tarayıcıların şifrelenmemiş HTTP bağlantılarına geri dönmesini önler. [3]

7. GÜVENLİK İÇGÖRÜSÜ

'Otomatik Bağlan' seçeneğini kapatmak, akıllı telefonların halka açık alanlardaki benzer görünümlü sahte ağlara bağlanmasını önler.

8. GÜVENLİK İÇGÖRÜSÜ

Kurumsal 'her zaman açık' VPN yapılandırmaları, tüm uzaktan çalışan ağ trafiğini kurumsal güvenlik duvarlarından geçmeye zorlar.

9. GÜVENLİK İÇGÖRÜSÜ

Sahte erişim noktaları sahte DNS yanıtları verebilir ve hedef alan adlarını kimlik avı sunucularına yönlendirebilir.

10. GÜVENLİK İPUCU

VPN olmadan, açık bir erişim noktasındaki diğer kullanıcılar cihazının hangi sitelerle ve sunucularla iletişim kurduğunu görebilir.

Teknik Referanslar ve Kaynaklar

Çalışma kılavuzu ve etkileşimli bulmacalar, küresel NIST, OWASP ve veri gizliliği uyum standartlarından derlenmiştir.

AKADEMİK VE SEKTÖREL KAYNAKLAR

[1] Wi-Fi Alliance. (n.d.). Security.

https://www.wi-fi.org/discover-wi-fi/security

[2] Federal Trade Commission. (2023). Are Public Wi-Fi Networks Safe? What You Need To Know.

https://consumer.ftc.gov/articles/are-public-wi-fi-networks-safe-what-you-need-know

[3] MDN Web Docs. (n.d.). Strict-Transport-Security header.

https://developer.mozilla.org/en-US/docs/Web/HTTP/Reference/Headers/Strict-Transport-Security

[4] CISA. (2023). Phishing Guidance: Stopping the Attack Cycle at Phase One.

https://www.cisa.gov/resources-tools/resources/phishing-guidance-stopping-attack-cycle-phase-one

[5] CISA. (n.d.). Malware, Phishing, and Ransomware.

https://www.cisa.gov/topics/cyber-threats-and-advisories/malware-phishing-and-ransomware

Cevap Anahtarı: Kontrol Noktası 1 - Çoktan Seçmeli

1 Soru 1 Doğru cevap: A

ÖĞRETMEN NOTU

Ortadaki adam (MitM) saldırısı nedir? → Ortak bir ağda iki taraf arasındaki iletişimi araya girerek yakalamak ve değiştirmek

2 Soru 2 Doğru cevap: A

ÖĞRETMEN NOTU

Sahte erişim noktası (Evil Twin) nedir? → Meşru bir ağla aynı SSID ile yapılandırılmış kötü amaçlı Wi-Fi erişim noktası

3 Soru 3 Doğru cevap: A

ÖĞRETMEN NOTU

VPN, herkese açık Wi-Fi trafiğini nasıl korur? → Tüm ağ paketlerini şifreli bir tünele sarar ve koklayıcılar tarafından okunamaz hale getirir

4 Soru 4 Doğru cevap: A

ÖĞRETMEN NOTU

Paket dinleme (packet sniffing) nedir? → Ağ paketlerini yakalayıp kaydetmek için donanım veya yazılım araçları kullanmak

5 Soru 5 Doğru cevap: A

ÖĞRETMEN NOTU

HTTPS'in rolü nedir? → Tarayıcı ile web sunucusu arasındaki oturum trafiğini şifrelemek

Cevap Anahtarı: Kontrol Noktası 2 - Doğru veya Yanlış

6 **Soru 6** — **Doğru cevap: Doğru**

ÖĞRETMEN NOTU

Bağlı kullanıcılar, açık herkese açık Wi-Fi ağlarında düz metin verileri kolayca yakalayabilir.

7 **Soru 7** — **Doğru cevap: Yanlış**

ÖĞRETMEN NOTU

Yanlış: Evil Twin, bir saldırganın gerçek bir erişim noktasını taklit etmek için kurduğu yetkisiz bir erişim noktasıdır.

8 **Soru 8** — **Doğru cevap: Yanlış**

ÖĞRETMEN NOTU

Yanlış: bir VPN trafiği bir tünelde şifreler, bu yüzden yerel dinleyiciler onu okuyamaz.

9 **Soru 9** — **Doğru cevap: Yanlış**

ÖĞRETMEN NOTU

Yanlış: HTTPS, URL yolu ve sayfa içeriği dahil tüm HTTP alışverişini şifreler.

10 **Soru 10** — **Doğru cevap: Doğru**

ÖĞRETMEN NOTU

WPA3 güvenliği kullanan Wi-Fi erişim noktaları, açık ve parolasız ağlardan daha güçlü koruma sunar.

Kelime anahtarları ve puanlama ölçeği

Öğretmen notlandırma ölçeği: 1 puan ver — doğru her eşleştirme için (toplam 8 puan) ve her bağlam terimi için (toplam 6 puan).

KONTROL NOKTASI 4: CEVAP ANAHTARI – KAVRAM EŞLEŞTİRME

E 1. DİNLEME	F 2. PAKET DİNLEME	D 3. KÖTÜ İKİZ	H 4. HTTPS
G 5. VPN	B 6. TÜNEL	A 7. WPA3	C 8. GÜVENLİK DUVARI

KONTROL NOKTASI 3: CEVAP ANAHTARI – ANAHTAR TERİMLER

1 ARA DİNLEME	2 PAKET DİNLEME	3 KÖTÜ İKİZ	4 HTTPS
5 VPN İSTEMCİSİ	6 TÜNEL		

KONTROL NOKTASI 6, ALTERNATİF: CEVAP ANAHTARI – KELİME EŞLEŞTİRME

1 G – WPA3	2 C – KÖTÜİKİZ	3 B – PAKETDİNLEME	4 F – TÜNEL
5 H – GÜVENLİKDUVARI	6 A – ARADİNLEME	7 E – VPNİSTEMCİSİ	8 D – HTTPS

EĞİTMENLER İÇİN TARTIŞMA NOTLARI

Anahtar terimler:
Öğrencilerin DİNLEME, PAKET DİNLEME ve KÖTÜ İKİZ terimlerini kendi sözcükleriyle açıklayıp her biri için bir örnek verebildiğini kontrol et.

Vaka çalışmaları:
Öğrencilerden önerilerini varsayımlarla değil, çalışma kâğıdındaki bilgilerle desteklemelerini iste.

Kaynakların değerlendirilmesi:
Öğrencilerden çalışma kâğıdının kaynaklarında en az bir iddiayı doğrulamalarını iste ve rakamların, fiyatların ve kuralların zamanla neden değişebileceğini tartışın.

Bulmaca anahtarları ve öğretmen notları

KELİME BULMACA ÇÖZÜMÜ

E	O	M	Ü	C	K	Z	Y	F	V	N	U	T	J	T
M	O	E	M	E	L	N	İ	D	A	R	A	B	M	U
E	S	K	G	T	Ç	Y	T	İ	P	B	Ü	Z	V	K
L	P	Ö	V	H	N	D	A	Ç	İ	H	T	T	P	S
N	Ö	U	Ü	Ü	J	I	T	Ğ	Ş	Ğ	F	B	E	H
İ	İ	S	R	U	P	Z	Ü	W	E	Ğ	E	R	C	A
D	J	O	C	Z	K	İ	N	U	P	P	Ş	A	R	Ü
T	I	K	K	G	Ğ	L	E	Ğ	P	A	F	J	S	J
E	P	Ü	Ğ	B	Ş	F	L	Y	M	Y	3	Ü	R	Ğ
K	S	V	A	Z	İ	K	İ	Ü	T	Ö	K	O	T	M
A	G	Ü	V	E	N	L	İ	K	D	U	V	A	R	I
P	M	Z	N	H	O	S	Ğ	O	T	Ş	N	Ş	Ş	İ
A	E	V	P	N	İ	S	T	E	M	C	İ	S	İ	N
L	J	B	M	T	F	G	O	Ö	Ü	Y	I	İ	T	I
Y	U	V	O	İ	H	Z	H	I	L	A	E	H	B	S

BULMACA ÇÖZÜMÜ

	K						P							
	Ö			V			A							
	T			P										
G	Ü	V	E	N	L	İ	K	D	U	V	A	R	I	
	İ			İ			E				R			
	K			S			T		W	P	A	3		
	İ			T			D				D			
	Z			E			İ				İ			
				M			N		T	Ü	N	E	L	
				C			L				L			
				İ			E				E			
H	T	T	P	S			M				M			
				İ			E				E			

BULMACA ÇÖZÜMLERİ İÇİN ÖĞRETMEN REHBERİ

SOLDAN SAĞA

4 soldan sağa: GÜVENLİKDUVARI Gelen trafiği filtreleme (14 harf)

6 soldan sağa: WPA3 Modern Wi-Fi güvenlik standardı (4 harf)

7 soldan sağa: TÜNEL Aktarım sırasında güvenli veri yolu (5 harf)

8 soldan sağa: HTTPS Güvenli web iletimi (5 harf)

YUKARIDAN AŞAĞI

1 yukarıdan aşağı: KÖTÜİKİZ Wi-Fi'yi taklit eden sahte erişim noktası (8 harf)

2 yukarıdan aşağı: VPNİSTEMCİSİ Şifreli sanal özel ağ (12 harf)

3 yukarıdan aşağı: PAKETDİNLEME Ağ veri paketlerini yakalama (12 harf)

5 yukarıdan aşağı: ARADİNLEME Aktarım halindeki trafiği okuma (10 harf)

Karışık Kelimeler ve Şifre Çözüm Anahtarı

Kelime karıştırma etkinliği ve Gizli Şifre Görevi için notlandırma anahtarı.

KELİME KARIŞTIRMA ANAHTARI

1.	MLNİRAEEDA	ARADİNLEME	5.	AENİEKTLDPME	PAKETDİNLEME
2.	ÜKZÖİKİT	KÖTÜİKİZ	6.	PHTST	HTTPS
3.	VPMESCNTİSİİ	VPNİSTEMCİSİ	7.	ELTNÜ	TÜNEL
4.	3AWP	WPA3	8.	EKALDUÜIGİVRVN	GÜVENLİKDUVARI

GİZLİ ŞİFRE GÖREVİ CEVAP ANAHTARI

"GENEL KABLOSUZ AĞ TRAFİĞİNİ VPN İLE ŞİFRELE"

Vaka çalışmaları cevap anahtarı

A Vaka Çalışması 1: Herkese Açık Wi-Fi'de Paket Dinlemeyi Kontrol Altına Alma

Öğretmen çözümü

NOTLANDIRMA YÖNERGESİ

Öğrenci cevapları şu noktaları kapsamalıdır:

- Senaryo analizi: Halka açık bir havalimanı Wi-Fi ağına bağlı uzaktaki bir satış yöneticisi, şifrelenmemiş olarak gönderilen birkaç hassas iş e-postasının gönderildikten kısa süre sonra sızdığını fark eder.
- Önerilen Strateji ve Çözüm: Tüm uzak iş istasyonlarında kurumsal bir VPN istemcisi kullanımını zorunlu kıl. Yalnızca HTTPS kullanan tarayıcı eklentilerini zorunlu kıl ve HTTP ile FTP gibi şifresiz protokolleri istemci güvenlik duvarında engelle.

B Vaka Çalışması 2: Evil Twin Sahte Hotspot Savunması

Öğretmen çözümü

NOTLANDIRMA YÖNERGESİ

Öğrenci cevapları şu noktaları kapsamalıdır:

- Senaryo analizi: Saldırganlar, meşru bir kafenin erişim noktasını taklit eden 'CoffeeShop_Guest' adlı sahte bir kablosuz erişim noktası kuruyor ve habersiz konukların ağ trafiğini yakalıyor.
- Önerilen strateji ve çözüm: Ağın gerçekliğini doğrulamak için erişim noktası BSSID MAC adreslerini denetle. Açık ağlara bağlanmayı engellemek için istemci duruş doğrulamasını zorunlu kıl ve hassas işler için hücresel erişim noktalarını (hotspot) zorunlu tut.