Ad Soyad: _____ **Tarih:** _____ **Puan:** _____

Karanlık Ağ ve Derin Ağ: Güvenlik ve Farklar

Arama motoru dizinleme, derin web veritabanları, Tor soğan yönlendirme, ağ anonimliği ve riskler

KARANLIK AĞ VE DERİN AĞ ÖĞRENME GENEL BAKIŞI

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 Derin Web ile Karanlık Web arasındaki farklar konusunda rehberlik eder. Dizinlenmemiş veri tabanlarını, Tor tarayıcısı Onion Yönlendirmesini, .onion kriptografik alan adlarını ve anonimlik güvenlik risklerini 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/karanlik-web-vs-derin-web/

Derin ve Karanlık Web Stratejisi Öğrenme Yol Haritan

- Derin ağı (dizine eklenmemiş veritabanları) ve karanlık ağı (onion hizmetleri) karşılaştır.
- Onion Routing'in ağ trafiğini nasıl şifrelediğini ve aktardığını anla.
- Doğrulanmamış Tor ağı sitelerine erişmenin güvenlik risklerini değerlendir.
- Tehdit istihbaratı taraması için güvenli geçit ve korumalı alan ilkelerini dağıt.
- Onion hizmeti alan adlarının kriptografik adres biçimini analiz et.

DERİN VE KARANLIK AĞ REHBERİ TALİMATLARI

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: derin ve karanlık ağ gizliliği. Hızlı Düşün bonus etkinliğiyle bitir.

DERİN AĞ VERİ TABANLARI VE KARANLIK AĞ SOĞAN YÖNLENDİRMESİ (GİRİŞ)

Deep web, özel e-postalar veya kurumsal banka portalları gibi parola ve oturum açma arkasındaki dizine eklenmemiş sayfalardan oluşur. Dark web ise deep web'in kasıtlı olarak gizlenmiş bir alt kümesidir; anonim erişim için özel tarayıcılar (Tor gibi) ve onion ağları gerektirir.

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

Kontrol Noktası 1: Çoktan seçmeli görev

1. Derin ağı yüzey ağından ayıran nedir?

- A. Derin web sayfaları herkese açık arama motorları tarafından dizinlenmez
- B. Derin ağ trafiği yasa dışıdır ve kolluk kuvvetlerince izlenir
- C. Derin web siteleri erişim için Tor gibi özel tarayıcılar gerektirir
- D. Derin ağ sayfaları her zaman yüzey ağ sayfalarından daha hızlı yüklenir

2. Dark web'e nasıl erişilir?

- A. Soğan yönlendirme ağlarını kullanan özel tarayıcılar aracılığıyla
- B. Standart yönlendiricilerde özel DNS ayarlarını yapılandırarak
- C. Yalnızca davetle girilen gizli yüzey web arama konsolları üzerinden
- D. Standart bir reklam engelleyici tarayıcı uzantısı kurarak

3. Derin ağın en büyük bölümünü hangi yapı oluşturur?

- A. Parola korumalı kullanıcı veritabanları ve özel hesaplar
- B. Yasa dışı mal ticareti yapan yasa dışı kara pazar forumları
- C. Şifrelenmemiş eşler arası dosya paylaşım protokolleri
- D. Herkese açık arama motoru önbellek veritabanları

4. Onion Routing ağ trafiğine ne yapar?

- A. Paketleri şifreler ve birden fazla röle üzerinden yönlendirir
- B. ISS düğümlerini atlayarak indirme hızlarını artırır
- C. Cihaz donanım seri numaralarını IP kayıtlarıyla eşleştirir
- D. Her tıklamadan sonra web tarayıcısı çerezlerini siler

5. Hangi alan adı uzantısı yalnızca Tor ağlarında kullanılır?

- A. Kriptografik .onion üst düzey uzantısı
- B. Standart eski .com ticari uzantısı
- C. Web3 merkeziyetsiz .eth blok zinciri uzantısı
- D. Ülke kodlu .ai teknoloji uzantısı

Kontrol Noktası 2: Doğru/Yanlış görevi

6 Soru D/Y 6

6. Deep web ve dark web aynı ağ bölümünü ifade eder.

- ( ) Doğru
- ( ) Yanlış

7 Soru D/Y 7

7. Kurumsal intranet portalları derin ağın bir parçasıdır.

- ( ) Doğru
- ( ) Yanlış

8 Soru D/Y 8

8. Soğan yönlendirme, veri paketlerinin şifresini her geçiş düğümünde tamamen çözer.

- ( ) Doğru
- ( ) Yanlış

9 Soru D/Y 9

9. Dark web'e erişmek, cihazları yüksek kötü amaçlı yazılım risklerine maruz bırakır.

- ( ) Doğru
- ( ) Yanlış

10 Soru D/Y 10

10. Standart web arama motorları soğan sitelerini tarar ve dizine ekler.

- ( ) Doğru
- ( ) Yanlış

Kontrol Noktası 3: Anahtar terim yerleştirme

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

1. Özel banka portalları dizinlenmemiş _____ kesiminde yer alır.
2. Özel Tor düğümleri gizli _____ hizmetlerini barındırır.
3. Tor web siteleri, kriptografik bir üst düzey alan adı soneki olan _____ kullanır.
4. Şifrelenmiş, çok katmanlı trafik yolu oluşturmaya _____ denir.
5. Yüzey arama motorları, herkese açık biçimde _____ sayfaları tarar.
6. Onion ağları, kullanıcılara _____ sağlamak için istemci IP'lerini şifreler.

KELİME BANKASI

ANONİMLİK · DERİN WEB · DİZİNLENMİŞ · GİRİŞ DÜĞÜMÜ · KARANLIK WEB · ONION UZANTISI · TOR YÖNLENDİRME · VERİTABANI

Cevaplarını buraya yaz:

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

Kontrol Noktası 4: Güvenlik kavramı eşleştirme

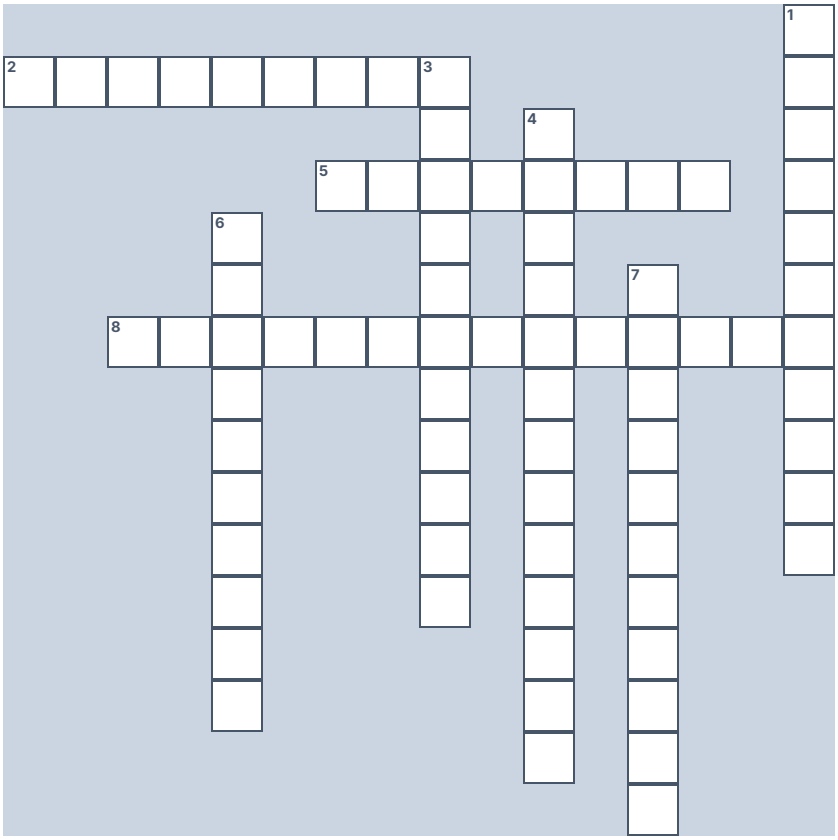
TANIM EŞLEŞTİRME

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

☐	1. Derin Web Kesimi	A	Yalnızca özel tarayıcılarla erişilebilen şifreli ağ bölümü.
☐	2. Karanlık Web Portalı	B	Verileri katmanlar halinde şifreleyip üç düğüm üzerinden iletme.
☐	3. Onion Uzantısı	C	Dizine eklenmemiş sistem kayıtlarını barındıran güvenli arka uç depolama.
☐	4. Tor Yönlendirmesi	D	Tor ağlarında kullanılan şifreleme tabanlı üst düzey alan adı soneki.
☐	5. Dizine Eklenmiş Sayfalar	E	Tor ağına erişmek için kullanılan giriş noktası düğümü.
☐	6. Kullanıcı Anonimliği	F	Google'da derlenmiş ve aranabilir yüzey web içeriği.
☐	7. Özel Veritabanı	G	İstemci genel IP adreslerini sunuculardan gizli tutma.
☐	8. Giriş Ağ Geçidi	H	Özel oturum açma bilgileri, e-postalar ve veri tabanı kayıtları gibi dizinlenmemiş web içeriği.

Kontrol Noktası 5: Bulmaca

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



SOLDAN SAĞA

2. İstemcilerin genel IP adreslerini sunuculardan gizli tutma (9)

5. Özel girişler, e-postalar ve veritabanı kayıtları gibi dizinlenmemiş web içeriği (8)

8. Veriyi katmanlar halinde şifreleyip üç düğüm üzerinden aktarma (14)

YUKARIDAN AŞAĞI

1. Google'da derlenmiş ve aranabilir yüzey web içeriği (11)

3. Yalnızca özel tarayıcılarla erişilebilen şifrelenmiş ağ kesimi (11)

4. Tor ağlarında kullanılan kriptografik üst düzey alan adı soneki (13)

6. Dizinlenmemiş sistem kayıtlarını barındıran güvenli arka uç depolama (10)

7. Tor ağına erişmek için kullanılan giriş noktası düğümü (11)

Kontrol Noktası 5, alternatif: Erişilebilir bulmaca ipuçları

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

SOLDAN SAĞA

2 soldan sağa: İstemcilerin genel IP adreslerini sunuculardan gizli tutma (9 harf):

5 soldan sağa: Özel girişler, e-postalar ve veritabanı kayıtları gibi dizinlenmemiş web içeriği (8 harf):

8 soldan sağa: Veriyi katmanlar halinde şifreleyip üç düğüm üzerinden aktarma (14 harf):

YUKARIDAN AŞAĞI

1 yukarıdan aşağı: Google'da derlenmiş ve aranabilir yüzey web içeriği (11 harf):

3 yukarıdan aşağı: Yalnızca özel tarayıcılarla erişilebilen şifrelenmiş ağ kesimi (11 harf):

4 yukarıdan aşağı: Tor ağlarında kullanılan kriptografik üst düzey alan adı soneki (13 harf):

6 yukarıdan aşağı: Dizinlenmemiş sistem kayıtlarını barındıran güvenli arka uç depolama (10 harf):

7 yukarıdan aşağı: Tor ağına erişmek için kullanılan giriş noktası düğümü (11 harf):

Kontrol Noktası 6: Gizli kelime bulmacası

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

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

KELİME LİSTESİ

DERİNWEB, KARANLIKWEB, ONIONUZANTISI, TORYÖNLENDİRME, DİZİNLENMİŞ, ANONİMLİK, VERİTABANI, GİRİŞDÜĞÜMÜ

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. DERİNWEB**
- **B. KARANLIKWEB**
- **C. ONIONUZANTISI**
- **D. TORYÖNLENDİRME**
- **E. DİZİNLENMİŞ**
- **F. ANONİMLİK**
- **G. VERİTABANI**
- **H. GİRİŞDÜĞÜMÜ**

TANIMLAR VE EŞLEŞTİRME ALANLARI

1. İstemcilerin genel IP adreslerini sunuculardan gizli tutma.
2. Dizinlenmemiş sistem kayıtlarını barındıran güvenli arka uç depolama.
3. Veriyi katmanlar halinde şifreleyip üç düğüm üzerinden aktarma.
4. Özel girişler, e-postalar ve veritabanı kayıtları gibi dizinlenmemiş web içeriği.
5. Yalnızca özel tarayıcılarla erişilebilen şifrelenmiş ağ kesimi.
6. Tor ağlarında kullanılan kriptografik üst düzey alan adı soneki.
7. Tor ağına erişmek için kullanılan giriş noktası düğümü.
8. Google'da derlenmiş ve aranabilir yüzey web içeriği.

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. EİNDWEBR
2. SNNUIOIZINT AO
3. DELNZİİŞNMİ
4. ANTIİABVER
5. WAKIRBNLKE A
6. NLİÖRREMDT ONEY
7. MAİKLNNİO
8. ÜÜÜDRGŞİMĞ İ

Bonus etkinlik: Hızlı Düşün

HER KATEGORİ İÇİN 3 CEVAP. LİSTEYİ İLK TAMAMLAYAN KAZANIR.

1	Karanlık ağdan uzak durma nedenleri			
2	Arama motorunun bulamadığı şeyler			
3	Hacklenebilecek cihazlar			
4	Tor kullanmanın yasal nedenleri			
5	Yazılımı güncelleme nedenleri			
6	E-postadaki uyarı işaretleri			
7	Karanlık ağda yasa dışı satılan şeyler			
8	BT yardımı için sorabileceğin kişiler			
9	Bugün başlayabileceğin güvenli alışkanlıklar			
10	Veri sızıntısından sonra yapılacaklar			
11	Derin ağa ait olan şeyler			
12	Oturum açarak kullandığın siteler			
13	Anonimlikle ilgili sözcükler			
14	Asla paylaşmaman gereken bilgiler			
15	'Yüzeyin altında' kalan şeyler			

Kontrol Noktası 8: Siber güvenlik vaka çalışmaları

Öğrendiğin kavramları aşağıdaki gerçek dünya senaryolarını çözmek için uygula.

VAKA ÇALIŞMASI 1: VERİ SIZINTISINI TESPİT ETME



Senaryo: Kurumsal bir güvenlik denetimi, hassas müşteri veritabanı kayıtlarının bir onion pazarında alınıp satıldığını ortaya çıkarıyor. Veriler Google'da dizinlenmemiş.

Tartışma sorusu: Hangi web katmanlarının söz konusu olduğunu ve bu sızıntının nasıl gerçekleştiğini açıkla.

VAKA ÇALIŞMASI 2: ANONİMLİK VE KÖTÜ AMAÇLI YAZILIM RİSKLERİ



Senaryo: Bir analist, bir Tor web sitesindeki tehdit istihbaratı akışlarını kontrol etmek istiyor. Tor tarayıcısını indirip siteye erişiyor.

Tartışma sorusu: Anonimlik avantajlarını değerlendir ve kötü amaçlı yazılıma karşı önlem adımlarını özetle.

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

22	18	9	1	17		28	19	17	15	6	17	5	12	21	16	6		12	15	6

1	17	18	17	12	16	15	12	9	12	17	12		14	18	21	25

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: Derin web nedir?

Deep web, arama motorlarının dizine ekleyemediği tüm web sayfalarından oluşur; buna çevrimiçi bankacılık, e-posta veri tabanları ve ücretli dergiler dâhildir.

Q2: Dark web nedir?

Dark web, deep web'in küçük bir alt kümesidir; kasıtlı olarak gizlenmiştir ve yalnızca onion ağlarını kullanan özel tarayıcılarla erişilebilir.

Q3: Arama motorları sayfaları nasıl dizinler?

Arama motorları, herkese açık bağlantıları izlemek için otomatik programlar (örümcekler) çalıştırır ve robot yönergeleriyle taramayı engellemeyen sayfaları dizinler.

Q4: Çevrimiçi bankacılık neden derin ağın bir parçası sayılır?

Bankacılık portalları oturum açma duvarlarının ve parolaların arkasındadır; bu da genel arama motorlarının hesap ekstresi sayfalarını dizinlemesini engeller.

Q5: Tor tarayıcısı Soğan Yönlendirmesi (Onion Routing) nedir?

Soğan yönlendirme, trafiği katmanlar halinde şifreleyen ve kullanıcı IP adreslerini gizlemek için birden çok röleden geçiren bir iletim yöntemidir.

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

Çevrimiçi tehditlerin azaltılmasına ilişkin sık sorulan soruları ve cevapları incele.

Q6: Karanlık ağa erişmek yasa dışı mı?

Hayır. Dark web'e erişmek çoğu ülkede yasaldır, ancak yasadışı pazar yerlerine veya siber faaliyetlere katılmak yasaktır.

Q7: Karanlık ağ siteleri neden yavaş yüklenir?

Trafik en az üç küresel aktarıcı (giriş, orta, çıkış) üzerinden yönlendirilir ve şifresi çözülür; bu da iletim gecikmesini artırır.

Q8: .onion alan adı uzantısı ne anlama gelir?

Tor ağlarında kullanılan, standart DNS sunucuları yerine kriptografik olarak üretilmiş adreslere işaret eden özel bir üst düzey alan adı sonekidir.

Q9: Karanlık ağ bağlantılarıyla ilişkili riskler nelerdir?

Sitelerde güvenlik taraması yoktur; bu da kullanıcıları yüksek kötü amaçlı yazılım bulaşma oranlarına, kimlik avı betiklerine ve işlem dolandırıcılıklarına maruz bırakır.

Q10: Tor ağı yönlendirme protokolünü kim geliştirdi?

Teknoloji ilk olarak 1990'larda hükümet iletişimini korumak için ABD Deniz Araştırma Laboratuvarı tarafından geliştirildi.

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: Ara düğümler Tor anonimliğini nasıl korur?

Her düğüm yönlendirme verisinin yalnızca bir katmanının şifresini çözer ve yalnızca bir önceki ve bir sonraki atlamayı öğrenir; kaynağı ve hedefi asla birlikte öğrenmez.

Q2: Çıkış düğümünün rolü nedir?

Çıkış düğümü şifrelemenin son katmanının şifresini çözer ve trafiği genel hedef sunucuya veya onion sunucusuna gönderir.

Q3: Tor köprüsü ağ geçidi nedir?

Köprüler, Tor tarayıcı erişimini kısıtlayan bölgelerde ISS engellerini ve sansürü aşmak için kullanılan listelenmemiş Tor giriş rölesidir.

Q4: Karanlık ağ aktörleri kripto parayı nasıl istismar eder?

Aktörler, bankacılık işlem kontrollerinden kaçınarak karanlık pazarlarda finansal işlemler yapmak için anonim kripto paralar kullanır.

Q5: Standart arama motorları derin veritabanlarını neden tarayamaz?

Tarayıcı botları, derin veritabanlarına erişmek için gereken oturum açma kimlik bilgilerini giremez, güvenlik CAPTCHA'larını çözemez veya arka uç SQL sorgu komut dosyalarını çalıştıramaz.

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: Tor ağlarında dizin sunucusu nedir?

İstemcilerin yönlendirme yolları oluşturmak için kullandığı etkin giriş, orta ve çıkış röle listesini tutan güvenilir bir sunucudur.

Q7: Kötü niyetli kişiler çıkış düğümü dinlemesini (exit node sniffing) nasıl yapar?

Sahte çıkış düğümü operatörleri, şifresiz HTTP trafiğini Tor ağından çıkarken ele geçirebilir ve kullanıcı adlarını ile çerezleri çalabilir.

Q8: Tor ile I2P arasındaki fark nedir?

Tor, herkese açık web erişimi için merkezî bir aktarıcı dizini ve çıkış düğümleri kullanırken I2P, dahili barındırma için merkezî olmayan eşler arası bir yapı kullanır.

Q9: Kolluk kuvvetleri karanlık ağ pazarlarını nasıl izler?

Kurumlar, işletmecileri belirlemek için blok zinciri analizi kullanır, fiziksel sunucu barındırma düzenlerini bulur ve tuzak operasyonlar yürütür.

Q10: DNS sızıntısı istemci anonimliğini nasıl zayıflatır?

DNS sızıntıları, tarayıcı DNS sorgularının şifreli Tor ağı üzerinden yönlendirilmek yerine doğrudan yerel İSS üzerinden gönderilmesiyle oluşur.

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

Deep web, aranabilir yüzey web'inden çok daha büyüktür; çünkü içeriğin çoğu oturum açma ekranlarının ve veri tabanlarının arkasındadır.

2. GÜVENLİK İPUCU

Dark web, deep web'in küçük ve kasıtlı olarak gizlenmiş bir parçasıdır; Tor gibi araçlarla erişilir.

3. GÜVENLİK İPUCU

Tor yönlendirmesi veri paketlerini üç kez şifreler ve her aktarım düğümünde şifreleme katmanlarını bir soğan gibi soyar.

4. GÜVENLİK İPUCU

Tor, ABD Deniz Araştırma Laboratuvarı'nın yürüttüğü onion yönlendirme projesinden doğmuştur ve kodu özgür yazılım olarak yayımlanmıştır. [1]

5. GÜVENLİK İPUCU

Onion adresleri, açık anahtar çiftlerinden kriptografik olarak üretilen 56 karakterlik alfasayısal dizelerdir.

6. GÜVENLİK İPUCU

Çıkış düğümleri açık metin trafiğini okuyabilir; bu da güvenli oturum verileri için Tor'da TLS/HTTPS'in hâlâ gerekli olduğu anlamına gelir.

7. GÜVENLİK İÇGÖRÜSÜ

İntranet siteleri, bulut sürücüleri ve özel veri tabanları, derin web'deki en büyük veri depolama bölümlerini oluşturur.

8. GÜVENLİK İÇGÖRÜSÜ

DuckDuckGo gibi özel arama motorları, Tor ağlarında anonim aramalara izin vermek için soğan portalları işletir.

9. GÜVENLİK İÇGÖRÜSÜ

Her gün 2 milyondan fazla kullanıcı, sansürü aşmak ve iletişim gizliliğini korumak için Tor ağına bağlanır.

10. GÜVENLİK İPUCU

Küresel kolluk operasyonları (Operation Bayonet gibi), barındırma donanımına el koyarak büyük karanlık pazar yerlerini kapattı.

Teknik Referanslar ve Kaynaklar

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

AKADEMİK VE SEKTÖREL KAYNAKLAR

[1] Tor Project. (n.d.). Why is it called Tor?
https://support.torproject.org/about/why-is-it-called-tor/

[2] Tor Project. (n.d.). How do Onion Services work?
https://community.torproject.org/onion-services/overview/

[3] Tor Project. (n.d.). Users – Tor Metrics.
https://metrics.torproject.org/userstats-relay-country.html

[4] CISA. (n.d.). Malware, Phishing, and Ransomware.
https://www.cisa.gov/topics/cyber-threats-and-advisories/malware-phishing-and-ransomware

[5] 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

Cevap Anahtarı: Kontrol Noktası 1 - Çoktan Seçmeli

1 **Arama Dizinleme** DERİN AĞ — Doğru cevap: A

ÖĞRETMEN NOTU

Derin ağ sayfaları giriş duvarlarının ve veri tabanlarının arkasındadır ve arama örümceklerinin bunları taramasını engeller. Kaynak: IETF RFC 3986.

2 **Tor Erişimi** KARANLIK AĞ — Doğru cevap: A

ÖĞRETMEN NOTU

Dark web, yalnızca Tor gibi tarayıcılarla erişilebilen gizli onion hizmetlerinden oluşur. Kaynak: IETF RFC 3986.

3 **Derin Veri Tabanları** VERİTABANLARI — Doğru cevap: A

ÖĞRETMEN NOTU

Parola korumalı hesaplar ve kurumsal kayıtlar, derin web'in en büyük bölümünü oluşturur. Kaynak: NIST Digital Identity.

4 **Soğan yönlendirme (Onion Routing)** TOR AĞI — Doğru cevap: A

ÖĞRETMEN NOTU

Soğan yönlendirme, veri paketlerini katmanlar halinde şifreler ve anonimlik için birden çok düğüm üzerinden iletir. Kaynak: IETF RFC 3986.

5 **Onion alan adı** UZANTI — Doğru cevap: A

ÖĞRETMEN NOTU

Kriptografik.onion alan adı soneki, trafiği genel DNS olmadan Tor içinde yönlendirir. Kaynak: IETF RFC 3986.

Cevap Anahtarı: Kontrol Noktası 2 - Doğru veya Yanlış

6 **Web segmentleri** YAPI — Doğru cevap: Yanlış

ÖĞRETMEN NOTU

Deep web dizine eklenmemiş tüm sayfaları kapsar; dark web ise bunun küçük, şifreli bir onion alt kesimidir. Kaynak: IETF RFC 3986.

7 **Kurumsal İntranetler** DERİN AĞ — Doğru cevap: Doğru

ÖĞRETMEN NOTU

İntranet siteleri parola portallarının arkasındadır ve dizinlenmez; bu da onların derin web'e ait olduğu anlamına gelir. Kaynak: NIST Digital Identity.

8 **Katmanlı Şifreleme** AKTARICILAR — Doğru cevap: Yanlış

ÖĞRETMEN NOTU

Onion röleleri, kullanıcı anonimliğini korumak için yalnızca bir yönlendirme katmanının şifresini çözer, paketin tamamının asla. Kaynak: IETF RFC 3986.

9 **Kötü Amaçlı Yazılıma Maruz Kalma** TEHDİTLER — Doğru cevap: Doğru

ÖĞRETMEN NOTU

Karanlık ağ pazar yerlerinde güvenlik filtresi yoktur ve çok yüksek kötü amaçlı yazılım bulaşma riski taşır. Kaynak: Center for Internet Security (CIS).

10 **Soru 10** — Doğru cevap: Yanlış

ÖĞRETMEN NOTU

Sıradan arama motoru tarayıcıları Tor kullanmaz, bu yüzden .onion sitelerine ulaşamaz ve onları dizinleyemez.

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

H 1. Derin Web Kesimi	A 2. Karanlık Web Portalı	D 3. Onion Uzantısı	B 4. Tor Yönlendirmesi
F 5. Dizine Eklenmiş Sayfalar	G 6. Kullanıcı Anonimliği	C 7. Özel Veritabanı	E 8. Giriş Ağ Geçidi

KONTROL NOKTASI 3: CEVAP ANAHTARI – ANAHTAR TERİMLER

1 DERİN WEB	2 KARANLIK WEB	3 ONION UZANTISI	4 TOR YÖNLENDİRME
5 DİZİNLENMİŞ	6 ANONİMLİK		

KONTROL NOKTASI 6, ALTERNATİF: CEVAP ANAHTARI – KELİME EŞLEŞTİRME

1 F – ANONİMLİK	2 G – VERİTABANI	3 D – TORYÖNLENDİRME	4 A – DERİNWEB
5 B – KARANLIKWEB	6 C – ONIONUZANTISI	7 H – GİRİŞDÜĞÜMÜ	8 E – DİZİNLENMİŞ

EĞİTMENLER İÇİN TARTIŞMA NOTLARI

Anahtar terimler:
Öğrencilerin Derin Web Kesimi, Karanlık Web Portalı ve Onion Uzantısı terimlerini kendi sözcükleriyle açıklayıp her biri için bir örnek verebildiğini kontrol et.

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

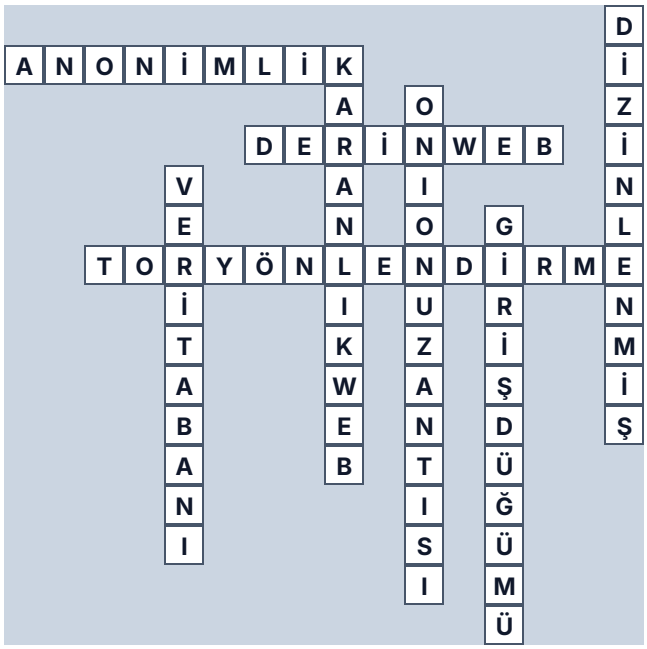
Kaynakların değerlendirilmesi:
Öğrencilerden çalışma kâğıdının kaynaklarında en az bir iddiayı doğrulamalarını iste ve rakamların, fiyatların ve kuralların zamanla neden değişebileceğini tartışın.

Bulmaca anahtarları ve öğretmen notları

KELİME BULMACA ÇÖZÜMÜ

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

BULMACA ÇÖZÜMÜ



BULMACA ÇÖZÜMLERİ İÇİN ÖĞRETMEN REHBERİ

SOLDAN SAĞA

2 soldan sağa: ANONİMLİK İstemcilerin genel IP adreslerini sunuculardan gizli tutma (9 harf)

5 soldan sağa: DERİNWEB Özel girişler, e-postalar ve veritabanı kayıtları gibi dizinlenmemiş web içeriği (8 harf)

8 soldan sağa: TORYÖNLENDİRME Veriyi katmanlar halinde şifreleyip üç düğüm üzerinden aktarma (14 harf)

YUKARIDAN AŞAĞI

1 yukarıdan aşağı: DİZİNLENMİŞ Google'da derlenmiş ve aranabilir yüzey web içeriği (11 harf)

3 yukarıdan aşağı: KARANLIKWEB Yalnızca özel tarayıcılarla erişilebilen şifrelenmiş ağ kesimi (11 harf)

4 yukarıdan aşağı: ONIONUZANTISI Tor ağlarında kullanılan kriptografik üst düzey alan adı soneki (13 harf)

6 yukarıdan aşağı: VERİTABANI Dizinlenmemiş sistem kayıtlarını barındıran güvenli arka uç depolama (10 harf)

7 yukarıdan aşağı: GİRİŞDÜĞÜMÜ Tor ağına erişmek için kullanılan giriş noktası düğümü (11 harf)

Karışık Kelimeler ve Şifre Çözüm Anahtarı

Kelime karıştırma etkinliği ve Gizli Şifre Görevi için notlandırma anahtarı.

KELİME KARIŞTIRMA ANAHTARI

1.	EİNDWEBR	DERİNWEB	5.	WAKIRBNLKEA	KARANLIKWEB
2.	SNNUIOIZINTAO	ONIONUZANTISI	6.	NLİÖRREMDTONEY	TORYÖNLENDİRME
3.	DELNZİİŞNMİ	DİZİNLENMİŞ	7.	MAİKLNNİO	ANONİMLİK
4.	ANTIİABVER	VERİTABANI	8.	ÜÜÜDRGŞİMĞİ	GİRİŞDÜĞÜMÜ

GİZLİ ŞİFRE GÖREVİ CEVAP ANAHTARI

"SOĞAN YÖNLENDİRME İLE ANONİMLİĞİNİ KORU"

Vaka çalışmaları cevap anahtarı

A Vaka Çalışması 1: Veri Sızıntısını Tespit Etme

Öğretmen çözümü

NOTLANDIRMA YÖNERGESİ

Öğrenci cevapları şu noktaları kapsamalıdır:

- Senaryo analizi: Bir kurumsal güvenlik denetimi, hassas müşteri veritabanı kayıtlarının bir onion pazar yerinde satıldığını ortaya çıkarır. Veriler Google'da dizinlenmemiştir.
- Önerilen Strateji ve Çözüm: İlgili Bölümler: Özel veritabanı derin ağa aittir (dizinlenmemiş ama güvenli). Çalınan verilerin ticaretinin yapıldığı pazar yeri karanlık ağdadır (onion ağı). Nasıl Gerçekleşti: Bilgisayar korsanları sunucu savunmalarını aştı, veritabanını derin ağdan çaldı ve kolluk kuvvetlerinin takibinden kaçmak için anonim olarak karanlık ağda listeledi.

B Vaka Çalışması 2: Anonimlik ve Kötü Amaçlı Yazılım Riskleri

Öğretmen çözümü

NOTLANDIRMA YÖNERGESİ

Öğrenci cevapları şu noktaları kapsamalıdır:

- Senaryo analizi: Bir analist, bir Tor sitesindeki tehdit istihbaratı akışlarını kontrol etmek istiyor. Tor tarayıcısını indirir ve siteye erişir.
- Önerilen strateji ve çözüm: Faydalar: Tor trafiği üç düğümden geçirerek analistin kurumsal IP'sini gizler. Riskler ve azaltma: Karanlık ağ bağlantılarında itibar taraması yoktur. Analistler Tor'u yalıtılmış sanal makinelerde (VM) çalıştırmalı, Tor ayarlarında JavaScript'i devre dışı bırakmalı ve kurumsal ağı korumak için hiçbir dosya indirmemelidir.