Emri: _____ Data: _____ Pikët: _____

Siguria dhe enkriptimi i Wi-Fi publik

Sulme man-in-the-middle, pika aksesi të rreme, përgjim paketash, tunele VPN dhe enkriptim HTTPS.

PËRMBLEDHJE MËSIMORE PËR SIGURINË E WI-FI PUBLIK

I SIGURUAR
ENKRIPTIMI I TË DHËNAVE
Standardi AES 256-bit

I PËRPUTHSHËM
STANDARDET GLOBALE
Kornizat GDPR dhe CCPA

ZERO-TRUST
POLITIKA E QASJES
Autentikim me shumë faktorë

Mirë se vjen! Kjo paketë aktivitetesh të udhëheq përmes sigurisë së Wi-Fi-t publik. Do të eksplorosh rrjetet e paenkriptuara, sulmet man-in-the-middle (MitM), pikat e aksesit mashtruese, packet sniffing-un, tunelet VPN dhe sigurinë e tranzitit HTTPS.

PIKAT E KONTROLLIT TË FLETËS SË PUNËS

- [ ] **Pjesët 1-4: Zotëro sigurinë kibernetike dhe parandalimin e kërcënimeve.**
- [ ] **Pjesët 5-7: Zgjidh fjalëkryqe dhe enigma me kërkim fjalësh.**
- [ ] **Pjesët 8-9: Zgjidh studime rasti dhe sfidën e kodit.**
- [ ] **Pjesa 10: Shqyrto faqet e pyetjeve të shpeshta bazë dhe të avancuara.**
- [ ] **Pjesa 11: Eksploro 10 fakte interesante nga bota reale.**
- [ ] **Bonus: sfida Mendo shpejt.**

Hap Udhëzuesin VPN.com për sigurinë kibernetike

URL: https://www.vpn.com/sq/siguria-kibernetike/siguria-wifi-publik/

Udhërrëfyesi yt mësimor për sigurinë e Wi-Fi-t publik

- Identifiko rreziqet e zakonshme të Wi-Fi publik, përfshirë përgjimin e paketave dhe pikat e rreme të qasjes.
- Zbato tunele enkriptimi VPN për të siguruar të dhënat në tranzit.
- Zbato HTTPS dhe cilësime të sigurta të shfletuesit për punonjësit në distancë.

UDHËZIME PËR UDHËZUESIN E SIGURISË SË WI-FI PUBLIK

Përgjigju pyetjeve me zgjedhje të shumëfishtë dhe pyetjeve E vërtetë/E gabuar, plotëso fjalitë me vende bosh duke përdorur bankën e fjalëve, përputh përkufizimet dhe zgjidh fjalëkryqin dhe enigmën e kërkimit të fjalëve. Zbato njohuritë e tua për sigurinë e qasjes në distancë. Përfundo me aktivitetin bonus Mendo shpejt.

SIGURIA E WI-FI PUBLIK DHE MBROJTJA GJATË TRANSITIT (HYRJE)

Pikat publike Wi-Fi të paenkriptuara e lënë trafikun e rrjetit të ekspozuar ndaj përgjimit të paketave dhe falsifikimit Evil Twin. Detyrimi i trafikut përmes tuneleve të sigurta të enkriptimit të VPN-së dhe zbatimi i rregullave HSTS vetëm për HTTPS i mbrojnë seancat nga përgjimi në rrjetin lokal.

LEXO ÇDO PIKË KONTROLLI ME KUJDES DHE ZGJIDH OSE SHKRUAJ PËRGJIGJEN E SAKTË.

Pika e kontrollit 1: Sfida me zgjedhje të shumëfishtë

1. Çfarë është një sulm Man-in-the-Middle (MitM)?

- A. Përgjimi dhe ndryshimi i komunikimeve mes dy palëve në një rrjet të përbashkët
- B. Një teknikë nxjerrjeje nga baza e të dhënave që synon regjistrat e përdoruesve
- C. Mbingarkimi i serverëve të uebit me kërkesa trafiku rrjeti
- D. Fshirja e vëllimeve të ruajtjes së diskut të ngurtë lokal

2. Çfarë është një pikë aksesi mashtruese (Evil Twin)?

- A. Një hotspot Wi-Fi keqdashës i konfiguruar me të njëjtin SSID si një rrjet legjitim
- B. Një mjet administrativ i përdorur për të monitoruar kopjet rezervë të bazës së të dhënave
- C. Një konfigurim i sigurt i portës VPN
- D. Një regjistrim DNS që harton serverët e autorizuar të postës

3. Si e mbron një VPN trafikun e Wi-Fi publik?

- A. I mbështjell të gjitha paketat e rrjetit në një tunel të enkriptuar, duke i bërë të palexueshme për sniffer-at
- B. Bllokon automatikisht të gjitha kërkesat hyrëse për lidhje
- C. Ndryshon adresën MAC të kartës fizike të rrjetit
- D. Fshin cookie-t e ruajtura në shfletues

4. Çfarë është packet sniffing?

- A. Përdorimi i mjeteve harduerike ose softuerike për të kapur dhe regjistruar paketat e rrjetit
- B. Skanimi i direktorive lokale për skedarë dublikatë
- C. Kufizimi i privilegjeve të leximit të bazës së të dhënave sipas roleve të përdoruesve
- D. Enkriptimi i disqeve të ruajtjes duke përdorur çelësa AES-256

5. Cili është roli i HTTPS?

- A. Enkriptimi i trafikut të sesionit mes shfletuesit dhe serverit të uebit
- B. Filtrimi i mesazheve hyrëse të emailit në gateway
- C. Kompresimi i imazheve për ngarkim më të shpejtë të faqeve
- D. Menaxhimi i strukturave të skedarëve në ruajtjen e lidhur me rrjetin

Pika e kontrollit 2: Sfida: E vërtetë ose e gabuar

6 Pyetja 6

6. Përdoruesit e lidhur mund të kapin lehtësisht të dhëna në tekst të thjeshtë në rrjetet publike të hapura Wi-Fi.

- ○ E vërtetë
- ○ E gabuar

7 Pyetja 7

7. Pikat e rreme të qasjes (Evil Twins) autorizohen gjithmonë nga administratorët e rrjetit.

- ○ E vërtetë
- ○ E gabuar

8 Pyetja 8

8. Një VPN është joefektiv në mbrojtjen e trafikut nga përgjimi i paketave (packet sniffing) në rrjete publike.

- ○ E vërtetë
- ○ E gabuar

9 Pyetja 9

9. HTTPS enkripton vetëm shtegun e URL-së, duke e lënë payload-in e paketës në tekst të thjeshtë.

- ○ E vërtetë
- ○ E gabuar

10 Pyetja 10

10. Pikat e Wi-Fi që përdorin sigurinë WPA3 ofrojnë mbrojtje më të fortë se rrjetet e hapura pa fjalëkalim.

- ○ E vërtetë
- ○ E gabuar

Pika e kontrollit 3: Futja e termave kryesorë

Lexo secilën fjali më poshtë dhe plotëso vendin bosh me termin e saktë nga Banka e Fjalëve.

1. Kapja e fjalëkalimeve private në Wi-Fi publik është _____ i komunikimit.
2. Analizimi i paketave të papërpunuara në një rrjet lokal përdor _____ paketash.
3. Një hotspot i rremë që imiton Wi-Fi-n e një hoteli është një _____ .
4. Sigurimi i tranzitit të trafikut të uebit kërkon enkriptim me _____ .
5. Enkriptimi i të gjitha daljeve të rrjetit përdor një _____ .
6. Një rrugë e enkriptuar komunikimi nëpër rrjete publike është një _____ .

BANKA E FJALËVE TË LEKSIKUT

EVIL TWIN | FIREWALL | HTTPS | KLIENT VPN | PËRGJIM | SNIFFING | TUNEL | WPA3

Shkruaj përgjigjet e tua këtu:

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

Pika e kontrollit 4: Përputhja e koncepteve të sigurisë

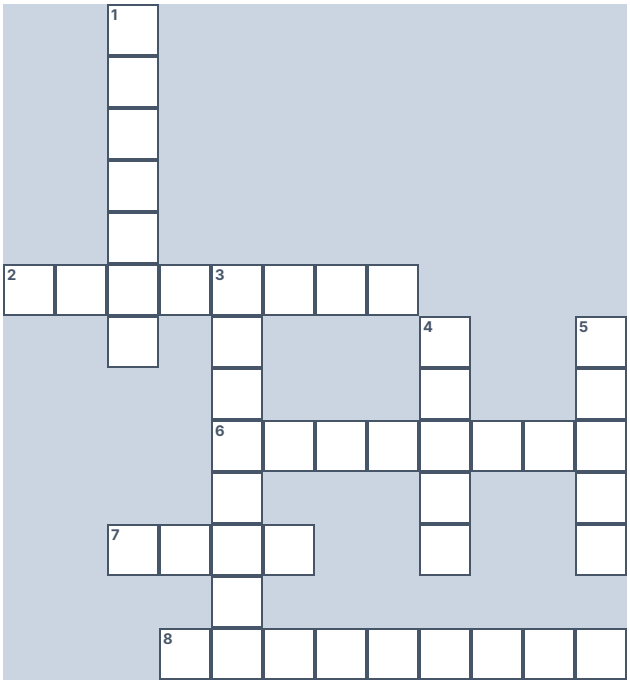
PËRPUTHJA E PËRKUFIZIMEVE

Përputh çdo term fjalori në të majtë me përkufizimin e tij të saktë në të djathtë, duke shkruar shkronjën përkatëse (A-H) në kutinë e plotësueshme.

☐	1. PËRGJIMI	A	Standard modern i sigurisë Wi-Fi.
☐	2. PËRGJIMI I PAKETAVE	B	Shteg i sigurt i të dhënave gjatë transitit.
☐	3. EVIL TWIN	C	Filtrimi i trafikut hyrës.
☐	4. HTTPS	D	Hotspot i rremë që imiton Wi-Fi.
☐	5. VPN	E	Leximi i trafikut gjatë transmetimit.
☐	6. TUNELI	F	Kapja e paketave të të dhënave të rrjetit.
☐	7. WPA3	G	Rrjet privat virtual i enkriptuar.
☐	8. FIREWALL	H	Transmetim i sigurt në uebi.

Pika e kontrollit 5: Fjalëkryq

Zgjidhe fjalëkryqin duke shkruar shkronja në kutitë e bardha aktive. Numrat korrespondojnë me indiciet më poshtë.



HORIZONTALISHT

2. Kapja e paketave të të dhënave të rrjetit. (8)

6. Hotspot i rremë që imiton Wi-Fi. (8)

7. Standard modern sigurie për Wi-Fi. (4)

8. Rrjet privat virtual i enkriptuar. (9)

VERTIKALISHT

1. Leximi i trafikut gjatë tranzitit. (7)

3. Filtrimi i trafikut hyrës. (8)

4. Transmetim i sigurt në ueb. (5)

5. Rrugë e sigurt e të dhënave gjatë tranzitit. (5)

Pika e kontrollit 5, alternativa: Çelësa të aksesueshëm të fjalëkryqit

Përdoruesit e lexuesve të ekranit dhe të tastierës mund t'i shkruajnë përgjigjet e fjalëkryqit drejtpërdrejt në fushat e tekstit më poshtë.

HORIZONTALISHT

2 horizontalisht: Kapja e paketave të të dhënave të rrjetit. (8 shkronja):

6 horizontalisht: Hotspot i rremë që imiton Wi-Fi. (8 shkronja):

7 horizontalisht: Standard modern sigurie për Wi-Fi. (4 shkronja):

8 horizontalisht: Rrjet privat virtual i enkriptuar. (9 shkronja):

VERTIKALISHT

1 vertikalisht: Leximi i trafikut gjatë tranzitit. (7 shkronja):

3 vertikalisht: Filtrimi i trafikut hyrës. (8 shkronja):

4 vertikalisht: Transmetim i sigurt në ueb. (5 shkronja):

5 vertikalisht: Rrugë e sigurt e të dhënave gjatë tranzitit. (5 shkronja):

Pika e kontrollit 6: Kërkimi i fjalës së fshehur

Gjej 8 termat kyç të fjalorit të fshehur në rrjetën më poshtë. Fjalët mund të jenë horizontale, vertikale ose diagonale.

D J H B A B C N X J I Y J X S
I D P L I Ç G L L J P P O F L
L P Q R S S Ë C R O Ë M G Q B
U L L A W E R I F Ç R R Z T C
N L Z U Ë K I F Z Ç G L D P X
I E O C T L B S A Z J M Ç J A
W N D M D I E F N G I Ç Q P K
T U D G Q E Z R E I M P U E A
L T A P N N L O S X F P I Q S
I Q Ç L Y T H B Ë Q X F V H A
V Q Z Y Y V T J Ë G L W I P I
E K K S N P T F O P P F Z N A
N U Ë T C N P Y Q A Y B F K G
Z Ë I M O M S V 3 C K Z Y Ë Y
N V T J T O B M U S K F T Ç Y

LISTA E FJALËVE TË LEKSIKUT

PËRGJIM SNIFFING EVILTWIN HTTPS KLIENTVPN TUNEL WPA3 FIREWALL

Pika e kontrollit 6, alternativa: Përputhja e aksesueshme e fjalorit

Përputh secilin nga 8 termat e fjalorit nga Kërkimi i fjalëve me përkufizimin e saktë të tij, duke shkruar shkronjën (A-H) në vendin bosh.

TERMA LEKSIKORË

- **A. PËRGJIM**
- **B. SNIFFING**
- **C. EVILTWIN**
- **D. HTTPS**
- **E. KLIENTVPN**
- **F. TUNEL**
- **G. WPA3**
- **H. FIREWALL**

PËRKUFIZIME DHE FUSHA PËRPUTHJEJE

1. Standard modern sigurie për Wi-Fi. ____
2. Hotspot i rremë që imiton Wi-Fi. ____
3. Kapja e paketave të të dhënave të rrjetit. ____
4. Rrugë e sigurt e të dhënave gjatë tranzitit. ____
5. Filtrimi i trafikut hyrës. ____
6. Leximi i trafikut gjatë tranzitit. ____
7. Rrjet privat virtual i enkriptuar. ____
8. Transmetim i sigurt në ueb. ____

Pika e kontrollit 7: Sfida e fjalëve të përzier

Rirenditi shkronjat më poshtë për të zbuluar konceptet dhe termat kryesorë të sigurisë kibernetike. Shkruaji përgjigjet në kutitë e dhëna.

1. **GIPJMRË** _____
2. **LENVIWTI** _____
3. **KTNLVNEPI** _____
4. **3AWP** _____
5. **FINGFSNI** _____
6. **PHTST** _____
7. **ELTNU** _____
8. **EIWLFLAR** _____

Aktivitet bonus: Mendo shpejt

3 PËRGJIGJE PËR ÇDO KATEGORI. FITON KUSH E PLOTËSON I PARI LISTËN.

1	Arsye për të përditësuar softuerin			
2	Pajisje që lidhen automatikisht me Wi-Fi			
3	Informacione që nuk duhet t'i ndash kurrë			
4	Zakone të sigurta që mund t'i fillosh sot			
5	Mënyra për të qëndruar i sigurt në një kafene			
6	Pajisje që mund të hakohen			
7	Gjëra që mund të shohë një haker në Wi-Fi të hapur			
8	Shenja të një rrjeti Wi-Fi të rremë			
9	Alternativa ndaj Wi-Fi-t publik			
10	Shenja paralajmëruese në një email			
11	Gjëra që nuk i bën në Wi-Fi publik			
12	Vende me Wi-Fi falas			
13	Mënyra për të mbrojtur llogaritë e tua			
14	Shenja që një kompjuter është i infektuar			
15	Emra Wi-Fi që duken të dyshimtë			

Pika e kontrollit 8: Studime rasti për sigurinë kibernetike

Zbato konceptet që ke mësuar për të zgjidhur skenarët reale më poshtë.

STUDIMI I RASTIT 1: PËRMBAJTJA E PËRGJIMIT TË PAKETAVE NË WI-FI PUBLIK



Skenari: Një ekzekutiv shitjesh në distancë, i lidhur me rrjetin publik Wi-Fi të një aeroporti, vëren se disa email të ndjeshëm biznesi rrjedhin menjëherë pasi i dërgon në tekst të thjeshtë.

Pyetje për diskutim: Analizo rreziqet e rrjeteve publike dhe përshkruaj një zgjidhje enkriptimi të trafikut.

STUDIMI I RASTIT 2: MBROJTJA NGA HOTSPOT-I I RREMË EVIL TWIN



Skenari: Sulmuesit vendosin një pikë qasjeje valore të rreme me emrin 'CoffeeShop_Guest' që imiton pikën legjitime të një kafeneje, duke kapur trafikun e rrjetit të mysafirëve që nuk dyshojnë.

Pyetje për diskutim: Përshkruaj në detaje hapat e verifikimit për të zbuluar dhe bllokuar pikat e rreme të qasjes.

Pika e kontrollit 9: Deshifrimi i kodit

Një profesionist i sigurisë kibernetike mbron asetet e rrjetit nga aktorët e kërcënimeve online. Përdor çelësin shkronjë-numër më poshtë për të deshifruar mesazhin duke shkruar shkronjat përkatëse në hapësirat e zbrazëta.

ÇELËSI I ENKRIPTIMIT SHKRONJË-NË-NUMËR

A=1 B=2 C=3 Ç=4 D=5 E=6 Ë=7 F=8 G=9

H=10 I=11 J=12 K=13 L=14 M=15 N=16 O=17 P=18

Q=19 R=20 S=21 T=22 U=23 V=24 X=25 Y=26 Z=27

6	16	13	20	11	18	22	17		22	20	1	8	11	13	23	16		6

20	20	12	6	22	11	22		18	23	2	14	11	13		15	6		24	18	16

Mesazhi i deshifruar:

KËSHILLË: ÇDO NUMËR PËRFAQËSON POZICIONIN E ASAJ SHKRONJE NË ALFABET (P.SH. 1 = A, 2 = B, 27 = Z).

Pika e kontrollit 10: Pyetje të shpeshta bazë për sigurinë kibernetike (Pjesa A)

Rishiko pyetje dhe përgjigje të zakonshme për zbutjen e kërcënimeve në internet.

Q1: Pse nuk është i sigurt Wi-Fi publik?

Wi-Fi publik i hapur nuk e enkripton trafikun në ajër, kështu që të tjerët aty pranë mund të kapin çdo të dhënë të pambrojtur. [2]

Q2: Çfarë është përgjimi i paketave (packet sniffing)?

Një packet sniffer kap të dhënat e papërpunuara që rrjedhin përmes një ndërfaqeje rrjeti, duke ekspozuar fjalëkalime në tekst të thjeshtë dhe detaje të trafikut.

Q3: Çfarë është një Evil Twin?

Një pikë qasjeje e rreme e ngritur nga hakerat që imiton emrin dhe cilësimet e një hotspot-i të besuar Wi-Fi lokal.

Q4: Si më mbron një VPN?

E rrugëzon trafikun tënd përmes një tuneli të enkriptuar, duke fshehur aktivitetin tënd të shfletimit nga përgjuesit e rrjetit lokal.

Q5: A më mbron HTTPS në Wi-Fi publik?

Po, enkripton të dhënat e shkëmbyera mes shfletuesit tënd dhe faqes së internetit, dhe një VPN shton një shtresë tjetër mbrojtjeje.

Pika e kontrollit 10: Pyetje të shpeshta bazë për sigurinë kibernetike (Pjesa B)

Rishiko pyetje dhe përgjigje të zakonshme për zbutjen e kërcënimeve në internet.

Q6: Çfarë është WPA3?

Standardi modern Wi-Fi Protected Access, që ofron enkriptim më të fortë dhe mbrojtje ndaj sulmeve fjalori jashtë linje. [1]

Q7: A mund të përhapë malware Wi-Fi publik?

Po, sulmuesit mund të përgjojnë trafikun dhe të injektojnë kërkesa dëmtuese shkarkimi (drive-by downloads) në sesionin tënd të shfletuesit.

Q8: Cili është rreziku i ndarjes së skedarëve?

Nëse ndarja e skedarëve është e aktivizuar, përdoruesit e tjerë në rrjetin publik mund të lexojnë ose modifikojnë direktorinë tënde lokale të dosjeve.

Q9: Çfarë është një portal kapës (captive portal)?

Faqja e hyrjes që rrjetet e hoteleve ose kafeneve përdorin për të dhënë qasje në internet, e cila ndonjëherë mund të falsifikohet nga sulmuesit.

Q10: A duhet ta çaktivizoj Wi-Fi kur nuk e përdor?

Po, çaktivizimi i Wi-Fi-t e pengon pajisjen tënde të lidhet automatikisht me rrjete të pabesueshme.

Pika e kontrollit 10: Pyetje të shpeshta të avancuara për sigurinë (Pjesa C)

Eksploro aspektet e avancuara teknike të kornizave të sigurisë, analizës së malware-it dhe pajtueshmërisë me të dhënat.

Q1: Si e shfrytëzon një sulm Man-in-the-Middle DNS-në?

Duke përdorur DNS spoofing në një router të rremë për të drejtuar shfletuesit e synuar te faqe uljeje phishing të ngjashme në vend të domeneve të synuara.

Q2: Çfarë është rrëmbimi i seancës (session hijacking)?

Një sulmues që përgjon një cookie sesioni të pa enkriptuar nëpër Wi-Fi publik dhe e importon për të anashkaluar identifikimet me kredenciale.

Q3: Çfarë është SSL stripping?

Një sulm MitM ku sulmuesi e ul një kërkesë të sigurt HTTPS të përdoruesit në HTTP të pa enkriptuar, duke kapur kredencialet e hyrjes në tekst të thjeshtë.

Q4: Si mbron HSTS nga SSL stripping?

HTTP Strict Transport Security i detyron shfletuesit të lidhen vetëm përmes HTTPS, duke refuzuar kthimet te HTTP i paenkriptuar. [3]

Q5: Çfarë është një VPN me split tunneling?

Një konfigurim që drejton përmes VPN-së vetëm trafikun korporativ, ndërsa e dërgon drejtpërdrejt të dhënat e internetit publik, çka mund të rrezikojë ekspozim përmes rrugëve të rrjedhjes.

Pika e kontrollit 10: Pyetje të shpeshta të avancuara për sigurinë (Pjesa D)

Eksploro aspektet e avancuara teknike të kornizave të sigurisë, analizës së malware-it dhe pajtueshmërisë me të dhënat.

Q6: Pse është WPA2 i cenueshëm ndaj KRACK?

Key Reinstallation Attack shfrytëzon shtrëngimin e duarve me katër hapa të WPA2 për të deshifruar paketat pa fjalëkalimin e Wi-Fi.

Q7: Çfarë është izolimi i klientit?

Një cilësim sigurie i router-it që i pengon pajisjet Wi-Fi të lidhura të komunikojnë drejtpërdrejt me njëra-tjetrën, duke bllokuar përgjimin lokal.

Q8: Si i përdorin sulmuesit serverët e rremë DNS?

Konfigurojnë ruterë mashtrues që t'u caktojnë klientëve serverë DNS të rremë, duke u mundësuar të përgjojnë dhe të ripërshkruajnë të gjitha kërkimet e uebit.

Q9: A mund ta fshehë një VPN adresën time lokale MAC?

Jo. Adresat MAC janë identifikues lokalë të shtresës 2; përdor në vend të tyre cilësimin e integruar të pajisjes për randomizimin e MAC-it (adresë private).

Q10: Çfarë është një sulm i falsifikimit të captive portal?

Një sulmues që strehon një portal të rremë autentikimi në një hotspot të rremë për të vjedhur kredenciale nën pretekstin e qasjes falas në Wi-Fi.

Pjesa 11: 10 fakte dhe njohuri nga bota reale për sigurinë kibernetike

Rishiko fakte reale për shkeljet e sigurisë, mekanizmat e mbrojtjes dhe standardet e pajtueshmërisë.

1. PERSPEKTIVË PËR SIGURINË

Punëtorët në distancë shpesh përdorin Wi-Fi në kafene, hotele dhe aeroporte, ku nuk mund ta kontrollojnë sigurinë e rrjetit.

2. PERSPEKTIVË PËR SIGURINË

Një hotspot i rremë Evil Twin mund të kopjojë emrin dhe adresën MAC të saktë të një rrjeti të besuar, duke ngatërruar pajisjet.

3. PERSPEKTIVË PËR SIGURINË

Softueri i gjurmimit të paketave si Wireshark është falas dhe mund të shfaqë fjalëkalimet HTTP të paenkriptuara në tekst të qartë.

4. PERSPEKTIVË PËR SIGURINË

Siguria WPA3 përdor Simultaneous Authentication of Equals (SAE) për t'u mbrojtur nga sulmet lokale me forcë brutale.

5. PERSPEKTIVË PËR SIGURINË

Sulmet SSL stripping anashkalojnë mbrojtjet bazë HTTPS duke përgjuar ridrejtimet fillestare HTTP në gateway.

6. PERSPEKTIVË PËR SIGURINË

Titujt e përgjigjes HTTP Strict Transport Security (HSTS) ua ndalojnë shfletuesve kthimin te lidhjet HTTP të paenkriptuara. [3]

7. NJOHURI PËR SIGURINË

Çaktivizimi i 'Auto-Connect' i pengon smartfonët të lidhen me rrjete mashtruese të ngjashme në hapësira publike.

8. NJOHURI PËR SIGURINË

Konfigurimet VPN 'always-on' të ndërmarrjeve e detyrojnë gjithë trafikun e rrjetit të punonjësve në distancë të kalojë nëpër firewall-et e korporatës.

9. NJOHURI PËR SIGURINË

Pikat e rreme të qasjes mund të japin përgjigje të falsifikuara DNS, duke ridrejtuar domenet e synuara te serverë phishing.

10. PERSPEKTIVË PËR SIGURINË

Pa një VPN, përdoruesit e tjerë në një hotspot të hapur mund të shohin cilat faqe dhe servera kontakton pajisja jote.

Referenca teknike dhe burime

Udhëzuesi i studimit dhe enigmat interaktive janë përpiluar nga standardet globale të NIST, OWASP dhe të pajtueshmërisë me privatësinë e të dhënave.

REFERENCA AKADEMIKE DHE TË INDUSTRISË

[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

Çelësi i përgjigjeve: Pika e kontrollit 1 - Zgjedhje e shumëfishtë

1 **Pyetja 1** — **Përgjigjja e saktë: A**

SHËNIM PËR MËSUESIN

Çfarë është një sulm Man-in-the-Middle (MitM)? → Përgjimi dhe ndryshimi i komunikimeve mes dy palëve në një rrjet të përbashkët

2 **Pyetja 2** — **Përgjigjja e saktë: A**

SHËNIM PËR MËSUESIN

Çfarë është një pikë aksesi mashtruese (Evil Twin)? → Një hotspot Wi-Fi keqdashës i konfiguruar me të njëjtin SSID si një rrjet legjitim

3 **Pyetja 3** — **Përgjigjja e saktë: A**

SHËNIM PËR MËSUESIN

Si e mbron një VPN trafikun e Wi-Fi publik? → I mbështjell të gjitha paketat e rrjetit në një tunel të enkriptuar, duke i bërë të palexueshme për sniffer-at

4 **Pyetja 4** — **Përgjigjja e saktë: A**

SHËNIM PËR MËSUESIN

Çfarë është packet sniffing? → Përdorimi i mjeteve harduerike ose softuerike për të kapur dhe regjistruar paketat e rrjetit

5 **Pyetja 5** — **Përgjigjja e saktë: A**

SHËNIM PËR MËSUESIN

Cili është roli i HTTPS? → Enkriptimi i trafikut të sesionit mes shfletuesit dhe serverit të uebit

Çelësi i përgjigjeve: Pika e kontrollit 2 - E vërtetë ose e gabuar

6 **Pyetja 6** **Përgjigjja e saktë: E vërtetë**

SHËNIM PËR MËSUESIN

Përdoruesit e lidhur mund të kapin lehtësisht të dhëna në tekst të thjeshtë në rrjetet publike të hapura Wi-Fi.

7 **Pyetja 7** **Përgjigjja e saktë: E gabuar**

SHËNIM PËR MËSUESIN

E gabuar: një Evil Twin është një hotspot i paautorizuar i ngritur nga një sulmues për të imituar një të vërtetë.

8 **Pyetja 8** **Përgjigjja e saktë: E gabuar**

SHËNIM PËR MËSUESIN

E gabuar: një VPN e enkripton trafikun në një tunel, ndaj sniffer-at lokalë nuk mund ta lexojnë.

9 **Pyetja 9** **Përgjigjja e saktë: E gabuar**

SHËNIM PËR MËSUESIN

E gabuar: HTTPS e enkripton gjithë shkëmbimin HTTP, përfshirë shtegun e URL-së dhe përmbajtjen e faqes.

10 **Pyetja 10** **Përgjigjja e saktë: E vërtetë**

SHËNIM PËR MËSUESIN

Pikat e Wi-Fi që përdorin sigurinë WPA3 ofrojnë mbrojtje më të fortë se rrjetet e hapura pa fjalëkalim.

Çelësat e fjalorit dhe rubrika e vlerësimit

Rubrika e vlerësimit për mësuesin: Jep 1 pikë për çdo përputhje të saktë (8 pikë gjithsej) dhe term konteksti (6 pikë gjithsej).

PIKA E KONTROLLIT 4: ÇELËSI – PËRPUTHJA E KONCEPTEVE

E 1. PËRGJIMI	F 2. PËRGJIMI I PAKETAVE	D 3. EVIL TWIN	H 4. HTTPS
G 5. VPN	B 6. TUNELI	A 7. WPA3	C 8. FIREWALL

PIKA E KONTROLLIT 3: ÇELËSI – TERMAT KRYESORË

1 PËRGJIM	2 SNIFFING	3 EVIL TWIN	4 HTTPS
5 KLIENT VPN	6 TUNEL		

PIKA E KONTROLLIT 6, ALTERNATIVA: ÇELËSI – PËRPUTHJA E FJALËVE

1 G – WPA3	2 C – EVILTWIN	3 B – SNIFFING	4 F – TUNEL
5 H – FIREWALL	6 A – PËRGJIM	7 E – KLIENTVPN	8 D – HTTPS

SHËNIME PËR DISKUTIM PËR MËSUESIT

Termat kryesorë:
Kontrollo nëse nxënësit mund të shpjegojnë PËRGJIMI, PËRGJIMI I PAKETAVE dhe EVIL TWIN me fjalët e tyre dhe të japin një shembull për secilin.

Studimet e rastit:
Kërkoju nxënësve t'i mbështesin rekomandimet me fakte nga fleta, jo me supozime.

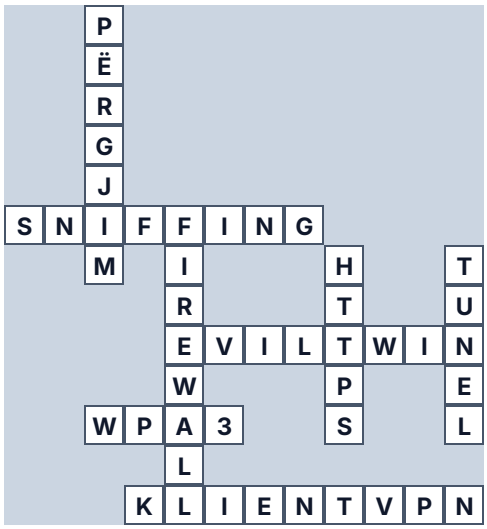
Vlerësimi i burimeve:
Kërkoju nxënësve të verifikojnë të paktën një pohim në burimet e fletës dhe diskutoni pse numrat, çmimet dhe rregullat mund të ndryshojnë me kalimin e kohës.

Çelësat e enigmave dhe shënimet për mësuesin

ZGJIDHJA E LOJËS ME FJALË

D	J	H	B	A	B	C	N	X	J	I	Y	J	X	S
I	D	P	L	I	Ç	G	L	L	J	P	P	O	F	L
L	P	Q	R	S	S	Ë	C	R	O	Ë	M	G	Q	B
U	L	L	A	W	E	R	I	F	Ç	R	R	Z	T	C
N	L	Z	U	Ë	K	I	F	Z	Ç	G	L	D	P	X
I	E	O	C	T	L	B	S	A	Z	J	M	Ç	J	A
W	N	D	M	D	I	E	F	N	G	I	Ç	Q	P	K
T	U	D	G	Q	E	Z	R	E	I	M	P	U	E	A
L	T	A	P	N	N	L	O	S	X	F	P	I	Q	S
I	Q	Ç	L	Y	T	H	B	Ë	Q	X	F	V	H	A
V	Q	Z	Y	Y	V	T	J	Ë	G	L	W	I	P	I
E	K	K	S	N	P	T	F	O	P	P	F	Z	N	A
N	U	Ë	T	C	N	P	Y	Q	A	Y	B	F	K	G
Z	Ë	I	M	O	M	S	V	3	C	K	Z	Y	Ë	Y
N	V	T	J	T	O	B	M	U	S	K	F	T	Ç	Y

ZGJIDHJA E FJALËKRYQIT



UDHËZUES PËR MËSUESIN PËR ZGJIDHJET E KRYQËZËS

HORIZONTALISHT

2 horizontalisht: SNIFFING Kapja e paketave të të dhënave të rrjetit. (8 shkronja)

6 horizontalisht: EVILTWIN Hotspot i rremë që imiton Wi-Fi. (8 shkronja)

7 horizontalisht: WPA3 Standard modern sigurie për Wi-Fi. (4 shkronja)

8 horizontalisht: KLIENTVPN Rrjet privat virtual i enkriptuar. (9 shkronja)

VERTIKALISHT

1 vertikalisht: PËRGJIM Leximi i trafikut gjatë tranzitit. (7 shkronja)

3 vertikalisht: FIREWALL Filtrimi i trafikut hyrës. (8 shkronja)

4 vertikalisht: HTTPS Transmetim i sigurt në ueb. (5 shkronja)

5 vertikalisht: TUNEL Rrugë e sigurt e të dhënave gjatë tranzitit. (5 shkronja)

Çelësi i fjalëve të përzierura dhe i zgjidhjes së kodit

Çelësi i vlerësimit për aktivitetin e rirenditjes së fjalorit dhe për Sfidën e Kodit të Fshehtë.

ÇELËSI I RIRENDITJES SË FJALËVE

1. GIPJMRË — **PËRGJIM**
2. LENVIWTI — **EVILTWIN**
3. KTNLVNEPI — **KLIENTVPN**
4. 3AWP — **WPA3**
5. FINGFSNI — **SNIFFING**
6. PHTST — **HTTPS**
7. ELTNU — **TUNEL**
8. EIWLFLAR — **FIREWALL**

ÇELËSI I SFIDËS SË KODIT TË FSHEHTË

"ENKRIPTO TRAFIKUN E RRJETIT PUBLIK ME VPN"

Çelësi i studimeve të rastit

A Studimi i rastit 1: Përmbajtja e përgjimit të paketave në Wi-Fi publik

Zgjidhja për mësuesin

UDHËZUES VLERËSIMI

Përgjigjet e studentëve duhet të mbulojnë pikat e mëposhtme:

- Analiza e skenarit: Një përgjegjës shitjesh në distancë, i lidhur me një rrjet Wi-Fi publik në aeroport, vëren se disa email-e të ndjeshme biznesi rrjedhin menjëherë pasi dërgohen në tekst të thjeshtë.
- Strategjia dhe zgjidhja e rekomanduar: Bëj të detyrueshëm përdorimin e një klienti VPN të ndërmarrjes në të gjitha stacionet e punës në distancë. Zbato zgjerime shfletuesi vetëm për HTTPS dhe blloko protokollet e paenkriptuara (si HTTP dhe FTP) në firewall-in e klientit.

B Studimi i rastit 2: Mbrojtja nga hotspot-i i rremë Evil Twin

Zgjidhja për mësuesin

UDHËZUES VLERËSIMI

Përgjigjet e studentëve duhet të mbulojnë pikat e mëposhtme:

- Analiza e skenarit: Sulmuesit vendosin një pikë qasjeje wireless mashtruese me emrin 'CoffeeShop_Guest', që imiton hotspotin e një kafeneje të ligjshme, duke kapur trafikun e rrjetit të mysafirëve të pakujdesshëm.
- Strategjia dhe zgjidhja e rekomanduar: Audito adresat MAC BSSID të pikave të aksesit për të verifikuar vërtetësinë e rrjetit. Zbato vlerësimin e qëndrimit të klientit për të bllokuar lidhjen me rrjete të hapura dhe kërko hotspot-e celulare për punë të ndjeshme.