Nume: _____ **Data:** _____ **Punctaj:** _____

Securitatea și criptarea Wi-Fi public

Atacuri de tip man-in-the-middle, puncte de acces false, interceptarea pachetelor, tuneluri VPN și criptarea HTTPS.

PREZENTARE GENERALĂ DESPRE SECURITATEA WI-FI PUBLIC

SECURIZAT
CRIPTAREA DATELOR
Standardul AES pe 256 de biți

CONFORM
STANDARDE GLOBALE
Cadrele GDPR și CCPA

ZERO-TRUST
POLITICĂ DE ACCES
Autentificare multifactor

Bun venit! Acest pachet de activități te ghidează prin securitatea Wi-Fi public. Vei explora rețelele necriptate, atacurile de tip man-in-the-middle (MitM), punctele de acces fraudulos, interceptarea pachetelor, tunelurile VPN și securitatea tranzitului HTTPS.

PUNCTE DE CONTROL ALE FIȘEI DE LUCRU

- [ ] **Partea 1-4: Stăpânește securitatea cibernetică și prevenirea amenințărilor.**
- [ ] **Partea 5-7: Rezolvă puzzle-uri de tip cuvinte încrucișate și căutare de cuvinte.**
- [ ] **Partea 8-9: Rezolvă studii de caz și provocarea cu codul cifrat.**
- [ ] **Partea 10: Parcurge paginile de întrebări frecvente de bază și avansate.**
- [ ] **Partea 11: Explorează 10 fapte interesante din lumea reală.**
- [ ] **Bonus: provocarea Gândește repede.**

Deschide Ghidul VPN.com de securitate cibernetică

URL: https://www.vpn.com/ro/securitate-cibernetica/securitate-wifi-public/

Harta ta de învățare despre securitatea rețelelor Wi-Fi publice

- Identifică riscurile frecvente ale rețelelor Wi-Fi publice, inclusiv interceptarea pachetelor și punctele de acces false.
- Implementează tuneluri de criptare VPN pentru a securiza datele în tranzit.
- Impune HTTPS și setări securizate ale browserului web pentru angajații care lucrează la distanță.

INSTRUCȚIUNI PENTRU GHIDUL DE SECURITATE A WI-FI PUBLIC

Răspunde la întrebările cu alegere multiplă și adevărat/fals, completează propozițiile cu spații libere folosind banca de cuvinte, asociază definițiile și rezolvă cuvintele încrucișate și puzzle-ul de căutare a cuvintelor. Aplică ce ai învățat despre securitatea accesului la distanță. Încheie cu activitatea bonus Gândește repede.

SECURITATEA WI-FI PUBLIC ȘI PROTECȚIA TRANSMISIEI (INTRODUCERE)

Hotspot-urile Wi-Fi publice necriptate lasă traficul de rețea expus interceptării pachetelor și falsificării de tip Evil Twin. Forțarea traficului prin tuneluri de criptare VPN securizate și aplicarea regulilor HSTS doar HTTPS protejează sesiunile de interceptarea în rețeaua locală.

CITEȘTE ATENT FIECARE PUNCT DE CONTROL ȘI ALEGE SAU SCRIE RĂSPUNSUL CORECT.

Punct de control 1: Provocare cu alegere multiplă

1. Ce este un atac de tip Man-in-the-Middle (MitM)?

- A. Interceptarea și modificarea comunicațiilor dintre două părți într-o rețea partajată
- B. O tehnică de extragere a datelor din baze de date, care vizează înregistrările utilizatorilor
- C. Supraîncărcarea serverelor web cu cereri de trafic de rețea
- D. Ștergerea volumelor de stocare ale hard diskului local

2. Ce este un punct de acces fraudulos (Evil Twin)?

- A. Un hotspot Wi-Fi rău intenționat, configurat cu același SSID ca o rețea legitimă
- B. Un instrument administrativ folosit pentru monitorizarea copiilor de rezervă ale bazelor de date
- C. O configurație sigură de gateway VPN
- D. O înregistrare DNS care asociază serverele de e-mail autorizate

3. Cum protejează un VPN traficul din rețelele Wi-Fi publice?

- A. Împachetează toate pachetele de rețea într-un tunel criptat, făcându-le ilizibile pentru sniffere
- B. Blochează automat toate cererile de conexiune de intrare
- C. Schimbă adresa MAC a plăcii de rețea fizice
- D. Șterge cookie-urile din cache din browserul web

4. Ce este interceptarea pachetelor (packet sniffing)?

- A. Folosirea unor instrumente hardware sau software pentru a captura și înregistra pachetele de rețea
- B. Scanarea directoarelor locale pentru fișiere duplicate
- C. Restricționarea privilegiilor de citire din baza de date în funcție de rolurile utilizatorilor
- D. Criptarea unităților de stocare cu chei AES-256

5. Care este rolul HTTPS?

- A. Criptarea traficului sesiunii dintre browser și serverul web
- B. Filtrarea mesajelor de e-mail primite la nivelul gateway-ului
- C. Comprimarea imaginilor pentru încărcarea mai rapidă a paginilor
- D. Gestionarea structurilor de fișiere în stocarea atașată la rețea

Punct de control 2: Provocare Adevărat sau Fals

6 Întrebare 6

6. Utilizatorii conectați pot captura cu ușurință date în text simplu în rețelele Wi-Fi publice deschise.

- ○ Adevărat
- ○ Fals

7 Întrebare 7

7. Punctele de acces false (Evil Twins) sunt întotdeauna autorizate de administratorii de rețea.

- ○ Adevărat
- ○ Fals

8 Întrebare 8

8. Un VPN este ineficient în protejarea traficului împotriva interceptării pachetelor (packet sniffing) în rețelele publice.

- ○ Adevărat
- ○ Fals

9 Întrebare 9

9. HTTPS criptează doar calea URL, lăsând conținutul pachetelor în text simplu.

- ○ Adevărat
- ○ Fals

10 Întrebare 10

10. Hotspoturile Wi-Fi care folosesc securitatea WPA3 oferă o protecție mai puternică decât rețelele deschise, fără parolă.

- ○ Adevărat
- ○ Fals

Punct de control 3: Inserarea termenilor-cheie

Citește fiecare propoziție de mai jos și completează spațiul liber cu termenul corect din Banca de cuvinte.

1. Capturarea parolelor private într-un Wi-Fi public este o _____ a comunicațiilor.
2. Analizarea pachetelor brute într-o rețea locală folosește _____ de pachete.
3. Un hotspot fals care imită Wi-Fi-ul unui hotel este un _____ .
4. Securizarea transportului traficului web necesită criptare cu _____ .
5. Criptarea întregului trafic de rețea de ieșire folosește un _____ .
6. O cale de comunicare criptată prin rețele publice este un _____ .

BANCĂ DE CUVINTE DIN VOCABULAR

CLIENT VPN | EVIL TWIN | FIREWALL | HTTPS | INTERCEPTARE | SNIFFING | STANDARD WPA | TUNEL

Scrie răspunsurile aici:

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

Punct de control 4: Asocierea conceptelor despre securitate

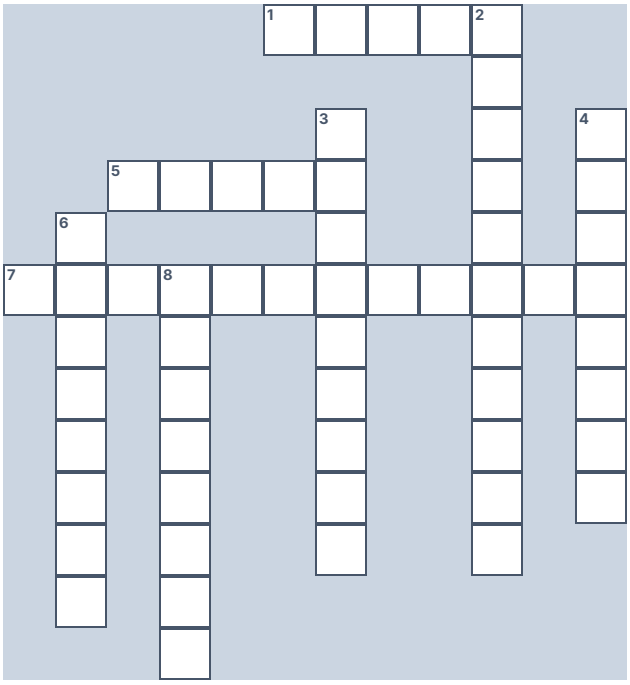
ASOCIEREA DEFINIȚIILOR

Asociază fiecare termen de vocabular din stânga cu definiția corectă din dreapta, scriind litera corespunzătoare (A-H) în câmpul de completare.

☐	1. INTERCEPTARE	A	Standard modern de securitate Wi-Fi.
☐	2. SNIFFING	B	Cale de date securizată în tranzit.
☐	3. EVIL TWIN	C	Filtrarea traficului de intrare.
☐	4. HTTPS	D	Hotspot fals care imită Wi-Fi-ul.
☐	5. VPN	E	Citirea traficului în tranzit.
☐	6. TUNEL	F	Capturarea pachetelor de date din rețea.
☐	7. WPA3	G	Rețea privată virtuală criptată.
☐	8. FIREWALL	H	Transmisie web securizată.

Punct de control 5: Careu de cuvinte încrucișate

Rezolvă careul de cuvinte încrucișate tastând litere în căsuțele albe active. Numerele corespund indiciilor de mai jos.



ORIZONTAL

1. Transmisie web securizată. (5)

5. Cale securizată de date în tranzit. (5)

7. Citirea traficului aflat în tranzit. (12)

VERTICAL

2. Standard modern de securitate Wi-Fi. (11)

3. Rețea privată virtuală criptată. (9)

4. Filtrarea traficului de intrare. (8)

6. Capturarea pachetelor de date din rețea. (8)

8. Hotspot fals care imită un Wi-Fi legitim. (8)

Punct de control 5, variantă alternativă: Indicii accesibile pentru cuvinte încrucișate

Utilizatorii de cititoare de ecran și de tastatură pot introduce răspunsurile la cuvintele încrucișate direct în câmpurile de text de mai jos.

ORIZONTAL

1 orizontal: Transmisie web securizată. (5 litere):

5 orizontal: Cale securizată de date în tranzit. (5 litere):

7 orizontal: Citirea traficului aflat în tranzit. (12 litere):

VERTICAL

2 vertical: Standard modern de securitate Wi-Fi. (11 litere):

3 vertical: Rețea privată virtuală criptată. (9 litere):

4 vertical: Filtrarea traficului de intrare. (8 litere):

6 vertical: Capturarea pachetelor de date din rețea. (8 litere):

8 vertical: Hotspot fals care imită un Wi-Fi legitim. (8 litere):

Punct de control 6: Căutarea cuvintelor ascunse

Găsește în grila de mai jos cei 8 termeni cheie de vocabular ascunși. Cuvintele pot fi orizontale, verticale sau diagonale.

H T T P S I M S M J Q P G M M
A L Q R S T L N T F E Â Ș Q O
P L H S Â E V I C Ș V Y U Â Z
W A V F N J G F Z C I M C R W
D W P U Â Ț Ă F A Z L N C C J
R E T A C O C I E G T I C L R
A R Q L D I S N Z Ș W E R I U
D I D A A R O G M P I T X E Q
N F Î S T S B M Y Ă N F S N W
A W Î A R Z Y Y K F I M R T Î
T I N T E R C E P T A R E V L
S L T O G Q Q G Z A O U F P Ț
Â Y S Y Ă G L Z F Î N P N N W
Â L Z Y F X O V Ț J U P Ă N U
T L G U B X Ț J R Ă W Z X L S

LISTĂ DE CUVINTE DIN VOCABULAR

INTERCEPTARE SNIFFING EVILTWIN HTTPS CLIENTVPN TUNEL
STANDARDWPA FIREWALL

Punct de control 6, variantă alternativă: Asocierea accesibilă a vocabularului

Asociază fiecare dintre cei 8 termeni de vocabular din Căutarea de cuvinte cu definiția corectă, scriind litera (A-H) în spațiul liber.

TERMENI DE VOCABULAR
A. INTERCEPTARE
B. SNIFFING
C. EVILTWIN
D. HTTPS
E. CLIENTVPN
F. TUNEL
G. STANDARDWPA
H. FIREWALL

	DEFINIȚII ȘI CÂMPURI DE ASOCIERE
	1. Standard modern de securitate Wi-Fi.
	2. Hotspot fals care imită un Wi-Fi legitim.
	3. Capturarea pachetelor de date din rețea.
	4. Cale securizată de date în tranzit.
	5. Filtrarea traficului de intrare.
	6. Citirea traficului aflat în tranzit.
	7. Rețea privată virtuală criptată.
	8. Transmisie web securizată.

Punct de control 7: Provocare cu cuvinte amestecate

Descifrează literele de mai jos pentru a dezvălui conceptele și termenii-cheie de securitate cibernetică. Scrie răspunsurile în casetele de introducere furnizate.

1. TCPRNEAIRTEE
2. LENVIWTI
3. CTNLVNEPI
4. RPAAADWDSTN
5. FINGFSNI
6. PHTST
7. ELTNU
8. EIWLFLAR

Activitate bonus: Gândește repede

3 RĂSPUNSURI PE CATEGORIE. CÂȘTIGĂ CINE COMPLETEAZĂ PRIMUL LISTA.

1	Motive pentru care ar trebui să actualizezi software-ul			
2	Dispozitive care se conectează automat la Wi-Fi			
3	Informații pe care nu ar trebui să le dai niciodată			
4	Obiceiuri sigure pe care le poți începe de azi			
5	Moduri de a rămâne în siguranță într-o cafenea			
6	Dispozitive care pot fi sparte			
7	Lucruri pe care le poate vedea un hacker într-o rețea Wi-Fi deschisă			
8	Semne ale unei rețele Wi-Fi false			
9	Alternative la Wi-Fi-ul public			
10	Semnale de avertizare într-un e-mail			
11	Lucruri pe care nu le faci într-o rețea Wi-Fi publică			
12	Locuri cu Wi-Fi gratuit			
13	Moduri de a-ți proteja conturile			
14	Semne că un calculator este infectat			
15	Nume de rețele Wi-Fi care par suspecte			

Punct de control 8: Studii de caz despre securitatea cibernetică

Aplică conceptele pe care le-ai învățat pentru a rezolva scenariile reale de mai jos.

STUDIU DE CAZ 1: LIMITAREA INTERCEPTĂRII PACHETELOR PE WI-FI PUBLIC



Scenariu: Un agent de vânzări care lucrează la distanță, conectat la o rețea Wi-Fi publică dintr-un aeroport, observă că mai multe e-mailuri de afaceri sensibile sunt scurse la scurt timp după ce au fost trimise în text simplu.

Întrebare de discuție: Analizează riscurile rețelelor publice și descrie pe scurt o soluție de criptare a traficului.

STUDIU DE CAZ 2: APĂRAREA ÎMPOTRIVA UNUI HOTSPOT FALS DE TIP EVIL TWIN



Scenariu: Atacatorii instalează un punct de acces wireless fals, numit „CoffeeShop_Guest”, care imită hotspot-ul unei cafenele legitime și captează traficul de rețea al oaspeților neavizați.

Întrebare de discuție: Detaliază pașii de verificare pentru detectarea și blocarea punctelor de acces false.

Punct de control 9: Descifrează codul

Un profesionist în securitate cibernetică protejează activele rețelei de actorii amenințărilor online. Folosește cheia literă–număr de mai jos pentru a descifra mesajul, scriind literele corespunzătoare în spațiile libere.

CHEIE DE CRIPTARE LITERĂ-NUMĂR

A=1 Ă=2 Â=3 B=4 C=5 D=6 E=7 F=8 G=9 H=10 I=11

Î=12 J=13 K=14 L=15 M=16 N=17 O=18 P=19 Q=20 R=21 S=22

Ș=23 T=24 Ț=25 U=26 V=27 W=28 X=29 Y=30 Z=31

5	21	11	19	24	7	1	31	2		24	21	1	8	11	5	26	15

28	11	8	11		19	26	4	15	11	5		5	26		26	17		27	19	17

Mesaj descifrat:

SFAT: FIECARE NUMĂR REPREZINTĂ POZIȚIA ACELEI LITERE ÎN ALFABET (DE EX. 1 = A, 2 = B, 31 = Z).

Punct de control 10: Întrebări frecvente de bază despre securitatea cibernetică (Partea A)

Parcurge întrebările și răspunsurile frecvente despre atenuarea amenințărilor online.

Q1: De ce nu este sigur Wi-Fi-ul public?

Wi-Fi-ul public deschis nu criptează traficul în aer, așa că persoanele aflate în apropiere pot capta orice date neprotejate. [2]

Q2: Ce este captarea pachetelor (packet sniffing)?

Un packet sniffer capturează datele brute care circulă printr-o interfață de rețea, expunând parole în text clar și detalii despre trafic.

Q3: Ce este un Evil Twin?

Un punct de acces fals configurat de hackeri, care imită numele și setările unui hotspot Wi-Fi local de încredere.

Q4: Cum mă protejează un VPN?

Îți direcționează traficul printr-un tunel criptat, ascunzându-ți activitatea de navigare față de dispozitivele de interceptare din rețeaua locală.

Q5: Mă protejează HTTPS în rețelele Wi-Fi publice?

Da, criptează datele schimbate între browserul tău și site, iar un VPN adaugă un strat suplimentar de protecție.

Punct de control 10: Întrebări frecvente de bază despre securitatea cibernetică (Partea B)

Parcurge întrebările și răspunsurile frecvente despre atenuarea amenințărilor online.

Q6: Ce este WPA3?

Standardul modern Wi-Fi Protected Access, care oferă criptare mai puternică și protecție împotriva atacurilor de tip dicționar offline. [1]

Q7: Poate Wi-Fi-ul public să livreze software rău intenționat?

Da, atacatorii pot intercepta traficul și pot injecta în sesiunea ta de browser solicitări de descărcare rău intenționate (descărcări drive-by).

Q8: Care este riscul partajării de fișiere?

Dacă partajarea fișierelor este activată, alți utilizatori din rețeaua publică pot citi sau modifica directorul tău local de foldere.

Q9: Ce este un captive portal?

Pagina de autentificare pe care o folosesc rețelele din hoteluri sau cafenele pentru a acorda acces la internet și care poate fi uneori falsificată de atacatori.

Q10: Ar trebui să opresc Wi-Fi-ul când nu îl folosesc?

Da, dezactivarea Wi-Fi împiedică dispozitivul tău să se conecteze automat la rețele nesigure.

Punct de control 10: Întrebări frecvente avansate despre securitate (Partea C)

Explorează aspecte tehnice avansate ale cadrelor de securitate, ale analizei software-ului rău intenționat și ale conformității datelor.

Q1: Cum exploatează DNS-ul un atac Man-in-the-Middle?

Prin folosirea DNS spoofing pe un router fals pentru a direcționa browserele țintă către pagini de destinație de phishing asemănătoare, în loc de domeniile țintă.

Q2: Ce este deturnarea sesiunii (session hijacking)?

Un atacator care interceptează un cookie de sesiune necriptat în Wi-Fi public și îl importă pentru a ocoli autentificarea cu date de acces.

Q3: Ce este SSL stripping?

Un atac MitM în care un atacator degradează cererea HTTPS securizată a unui utilizator la HTTP necriptat, captând datele de autentificare în text clar.

Q4: Cum protejează HSTS împotriva SSL stripping?

HTTP Strict Transport Security obligă browserele să se conecteze doar prin HTTPS, refuzând revenirile la HTTP necriptat. [3]

Q5: Ce este un VPN cu split tunneling?

O configurație care direcționează prin VPN doar traficul corporativ, trimițând direct datele de internet publice, ceea ce poate crea riscul expunerii prin scurgeri pe calea de rutare.

Punct de control 10: Întrebări frecvente avansate despre securitate (Partea D)

Explorează aspecte tehnice avansate ale cadrelor de securitate, ale analizei software-ului rău intenționat și ale conformității datelor.

Q6: De ce este WPA2 vulnerabil la KRACK?

Atacul Key Reinstallation exploatează handshake-ul în patru pași WPA2 pentru a decripta pachetele fără parola Wi-Fi.

Q7: Ce este izolarea clienților?

O setare de securitate a routerului care împiedică dispozitivele Wi-Fi conectate să comunice direct între ele, blocând interceptarea locală.

Q8: Cum folosesc atacatorii servere DNS false?

Configurează routere false pentru a atribui clienților servere DNS false, ceea ce le permite să intercepteze și să rescrie toate căutările web.

Q9: Poate un VPN să îmi ascundă adresa MAC locală?

Nu. Adresele MAC sunt identificatori locali de nivel 2; folosește în schimb setarea integrată a dispozitivului pentru randomizarea MAC (adresă privată).

Q10: Ce este un atac de falsificare a portalului captiv?

Un atacator care găzduiește un portal fals de autentificare pe un hotspot fals pentru a fura datele de autentificare sub pretextul accesului gratuit la Wi-Fi.

Partea 11: 10 fapte și perspective din lumea reală despre securitatea cibernetică

Parcurge fapte din lumea reală despre breșele de securitate, mecanismele de apărare și standardele de conformitate.

1. INFORMAȚII DESPRE SECURITATE

Lucrătorii la distanță folosesc adesea Wi-Fi în cafenele, hoteluri și aeroporturi, unde nu pot controla securitatea rețelei.

2. INFORMAȚII DESPRE SECURITATE

Un hotspot fals de tip Evil Twin poate copia exact numele și adresa MAC ale unei rețele de încredere, derutând dispozitivele.

3. INFORMAȚII DESPRE SECURITATE

Software-ul de captare a pachetelor, precum Wireshark, este gratuit și poate afișa în text clar parolele HTTP necriptate.

4. INFORMAȚII DESPRE SECURITATE

Securitatea WPA3 folosește Simultaneous Authentication of Equals (SAE) pentru a proteja împotriva atacurilor locale de tip forță brută.

5. INFORMAȚII DESPRE SECURITATE

Atacurile de tip SSL stripping ocolesc protecțiile HTTPS de bază interceptând redirecționările HTTP inițiale la nivelul gateway-ului.

6. INFORMAȚII DESPRE SECURITATE

Anteturile de răspuns HTTP Strict Transport Security (HSTS) împiedică browserele să revină la conexiuni HTTP necriptate. [3]

7. PERSPECTIVĂ ASUPRA SECURITĂȚII

Dezactivarea opțiunii „Auto-Connect” împiedică smartphone-urile să se conecteze la rețele false asemănătoare în spații publice.

8. PERSPECTIVĂ ASUPRA SECURITĂȚII

Configurațiile VPN „always-on” pentru întreprinderi forțează tot traficul de rețea al angajaților care lucrează la distanță să treacă prin firewall-urile corporative.

9. PERSPECTIVĂ ASUPRA SECURITĂȚII

Punctele de acces false pot oferi răspunsuri DNS falsificate, redirecționând domeniile țintă către servere de phishing.

10. INFORMAȚII DESPRE SECURITATE

Fără un VPN, alți utilizatori dintr-un hotspot deschis pot vedea ce site-uri și servere contactează dispozitivul tău.

Referințe tehnice și surse

Ghidul de studiu și puzzle-urile interactive sunt alcătuite pe baza standardelor globale NIST, OWASP și de conformitate privind confidențialitatea datelor.

REFERINȚE ACADEMICE ȘI DIN INDUSTRIE

[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

Barem: Punct de control 1 – Alegere multiplă

1 Întrebarea 1 **Răspuns corect: A**

NOTĂ PENTRU PROFESOR

Ce este un atac de tip Man-in-the-Middle (MitM)? → Interceptarea și modificarea comunicațiilor dintre două părți într-o rețea partajată

2 Întrebarea 2 **Răspuns corect: A**

NOTĂ PENTRU PROFESOR

Ce este un punct de acces fraudulos (Evil Twin)? → Un hotspot Wi-Fi rău intenționat, configurat cu același SSID ca o rețea legitimă

3 Întrebarea 3 **Răspuns corect: A**

NOTĂ PENTRU PROFESOR

Cum protejează un VPN traficul din rețelele Wi-Fi publice? → Împachetează toate pachetele de rețea într-un tunel criptat, făcându-le ilizibile pentru sniffere

4 Întrebarea 4 **Răspuns corect: A**

NOTĂ PENTRU PROFESOR

Ce este interceptarea pachetelor (packet sniffing)? → Folosirea unor instrumente hardware sau software pentru a captura și înregistra pachetele de rețea

5 Întrebarea 5 **Răspuns corect: A**

NOTĂ PENTRU PROFESOR

Care este rolul HTTPS? → Criptarea traficului sesiunii dintre browser și serverul web

Barem: Punct de control 2 – Adevărat sau fals

6 **Întrebarea 6** — **Răspuns corect: Adevărat**

NOTĂ PENTRU PROFESOR

Utilizatorii conectați pot captura cu ușurință date în text simplu în rețelele Wi-Fi publice deschise.

7 **Întrebarea 7** — **Răspuns corect: Fals**

NOTĂ PENTRU PROFESOR

Fals: un Evil Twin este un hotspot neautorizat, creat de un atacator pentru a imita unul real.

8 **Întrebarea 8** — **Răspuns corect: Fals**

NOTĂ PENTRU PROFESOR

Fals: un VPN criptează traficul într-un tunel, deci sniffer-ele locale nu îl pot citi.

9 **Întrebarea 9** — **Răspuns corect: Fals**

NOTĂ PENTRU PROFESOR

Fals: HTTPS criptează întregul schimb HTTP, inclusiv calea URL și conținutul paginii.

10 **Întrebarea 10** — **Răspuns corect: Adevărat**

NOTĂ PENTRU PROFESOR

Hotspoturile Wi-Fi care folosesc securitatea WPA3 oferă o protecție mai puternică decât rețelele deschise, fără parolă.

Chei de vocabular și grilă de notare

Barem de notare pentru profesor: Acordă 1 punct pentru fiecare asociere corectă (8 puncte în total) și pentru fiecare termen din context (6 puncte în total).

PUNCT DE CONTROL 4: BAREM – ASOCIEREA CONCEPTELOR

E 1. INTERCEPTARE	F 2. SNIFFING	D 3. EVIL TWIN	H 4. HTTPS
G 5. VPN	B 6. TUNEL	A 7. WPA3	C 8. FIREWALL

PUNCT DE CONTROL 3: BAREM – TERMENI-CHEIE

1 INTERCEPTARE	2 SNIFFING	3 EVIL TWIN	4 HTTPS
5 CLIENT VPN	6 TUNEL		

PUNCT DE CONTROL 6, VARIANTĂ ALTERNATIVĂ: BAREM – ASOCIEREA CUVINTELOR

1 G – STANDARDWPA	2 C – EVILTWIN	3 B – SNIFFING	4 F – TUNEL
5 H – FIREWALL	6 A – INTERCEPTARE	7 E – CLIENTVPN	8 D – HTTPS

NOTE DE DISCUȚIE PENTRU PROFESORI

Termeni-cheie:
Verifică dacă elevii pot explica INTERCEPTARE, SNIFFING și EVIL TWIN cu propriile cuvinte și pot da câte un exemplu pentru fiecare.

Studii de caz:
Cere elevilor să își susțină recomandările cu fapte din fișă, nu cu presupuneri.

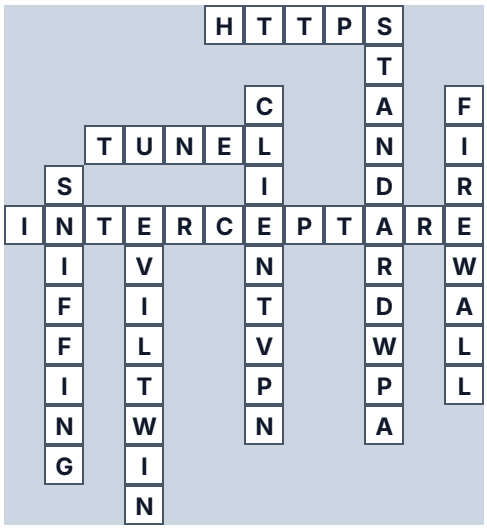
Evaluarea surselor:
Cere elevilor să verifice cel puțin o afirmație în sursele fișei și discutați de ce cifrele, prețurile și regulile se pot schimba în timp.

Chei de rezolvare ale puzzle-urilor și note pentru profesor

SOLUȚIA JOCULUI DE CĂUTARE DE CUVINTE

H	T	T	P	S	I	M	S	M	J	Q	P	G	M	M
A	L	Q	R	S	T	L	N	T	F	E	Â	Ș	Q	O
P	L	H	S	Â	E	V	I	C	Ș	V	Y	U	Â	Z
W	A	V	F	N	J	G	F	Z	C	I	M	C	R	W
D	W	P	U	Â	Ț	Ă	F	A	Z	L	N	C	C	J
R	E	T	A	C	O	C	I	E	G	T	I	C	L	R
A	R	Q	L	D	I	S	N	Z	Ș	W	E	R	I	U
D	I	D	A	A	R	O	G	M	P	I	T	X	E	Q
N	F	Î	S	T	S	B	M	Y	Ă	N	F	S	N	W
A	W	Î	A	R	Z	Y	Y	K	F	I	M	R	T	Î
T	I	N	T	E	R	C	E	P	T	A	R	E	V	L
S	L	T	O	G	Q	Q	G	Z	A	O	U	F	P	Ț
Â	Y	S	Y	Ă	G	L	Z	F	Î	N	P	N	N	W
Â	L	Z	Y	F	X	O	V	Ț	J	U	P	Ă	N	U
T	L	G	U	B	X	Ț	J	R	Ă	W	Z	X	L	S

SOLUȚIA CUVINTELOR ÎNCRUCIȘATE



GHID PENTRU PROFESOR: SOLUȚIILE LA CUVINTELE ÎNCRUCIȘATE

ORIZONTAL

1 orizontal: HTTPS Transmisie web securizată. (5 litere)

5 orizontal: TUNEL Cale securizată de date în tranzit. (5 litere)

7 orizontal: INTERCEPTARE Citirea traficului aflat în tranzit. (12 litere)

VERTICAL

2 vertical: STANDARDWPA Standard modern de securitate Wi-Fi. (11 litere)

3 vertical: CLIENTVPN Rețea privată virtuală criptată. (9 litere)

4 vertical: FIREWALL Filtrarea traficului de intrare. (8 litere)

6 vertical: SNIFFING Capturarea pachetelor de date din rețea. (8 litere)

8 vertical: EVILTWIN Hotspot fals care imită un Wi-Fi legitim. (8 litere)

Cuvinte amestecate și barem pentru codul cifrat

Barem pentru activitatea de descifrare a cuvintelor de vocabular și pentru provocarea Codul secret.

BAREMUL PENTRU DESCIFRAREA CUVINTELOR

1. TCPRNEAIRTEE — **INTERCEPTARE**
2. LENVIWTI — **EVILTWIN**
3. CTNLVNEPI — **CLIENTVPN**
4. RPAAADWDSTN — **STANDARDWPA**
5. FINGFSNI — **SNIFFING**
6. PHTST — **HTTPS**
7. ELTNU — **TUNEL**
8. EIWLFLAR — **FIREWALL**

BAREMUL PROVOCĂRII CU CODUL SECRET

"CRIPTEAZĂ TRAFICUL WIFI PUBLIC CU UN VPN"

Barem pentru studiile de caz

A Studiu de caz 1: Limitarea interceptării pachetelor pe Wi-Fi public

Soluția profesorului

GHID DE NOTARE

Răspunsurile elevilor ar trebui să acopere următoarele puncte:

- Analiza scenariului: Un executiv de vânzări la distanță, conectat la o rețea Wi-Fi publică dintr-un aeroport, observă că mai multe e-mailuri de afaceri sensibile sunt scurse la scurt timp după ce au fost trimise în text simplu.
- Strategie și soluție recomandată: Impune utilizarea unui client VPN enterprise pe toate stațiile de lucru la distanță. Impune extensii de browser doar HTTPS și blochează protocoalele necriptate (precum HTTP și FTP) la firewall-ul clientului.

B Studiu de caz 2: Apărarea împotriva unui hotspot fals de tip Evil Twin

Soluția profesorului

GHID DE NOTARE

Răspunsurile elevilor ar trebui să acopere următoarele puncte:

- Analiza scenariului: Atacatorii instalează un punct de acces wireless fals numit „CoffeeShop_Guest”, care imită hotspot-ul unei cafenele legitime și captează traficul de rețea al clienților nebănuiți.
- Strategie și soluție recomandate: Auditează adresele MAC BSSID ale punctelor de acces pentru a verifica autenticitatea rețelei. Impune validarea posturii clientului pentru a bloca conectarea la rețele deschise și cere hotspot-uri celulare pentru munca sensibilă.