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

Dark web vs. web profund: securitate și Diferențe

Indexarea de către motoarele de căutare, bazele de date din deep web, rutarea Tor onion, anonimitatea în rețea și riscurile

PREZENTARE GENERALĂ A ÎNVĂȚĂRII: DARK WEB VS. DEEP WEB

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 diferențele dintre Deep Web și Dark Web. Vei explora bazele de date neindexate, rutarea Onion din browserul Tor, domeniile criptografice .onion și riscurile de securitate legate de anonimat.

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/dark-web-vs-deep-web/

Harta ta de învățare despre strategia pentru deep web și dark web

- Compară deep web-ul (baze de date neindexate) cu dark web-ul (servicii onion).
- Înțelege cum criptează și transmite traficul de rețea rutarea Onion.
- Evaluează riscurile de securitate ale accesării unor site-uri neverificate din rețeaua Tor.
- Implementează politici de gateway securizat și de sandboxing pentru crawlingul de informații despre amenințări.
- Analizează formatul adreselor criptografice ale domeniilor serviciilor onion.

GHID DESPRE WEB-UL PROFUND ȘI DARK WEB: INSTRUCȚIUNI

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 confidențialitatea pe web-ul profund și pe dark web. Încheie cu activitatea bonus Gândește repede.

BAZE DE DATE DIN WEB-UL PROFUND VS. RUTAREA ONION DIN DARK WEB (INTRODUCERE)

Deep web-ul este alcătuit din pagini neindexate, protejate prin parole și autentificări, precum e-mailurile private sau portalurile bancare corporative. Dark web-ul este un subset al deep web-ului, ascuns intenționat, care necesită browsere specializate (precum Tor) și rețele onion pentru a fi accesat anonim.

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

Punct de control 1: Provocare cu alegere multiplă

1. Ce deosebește deep web de surface web?

- A. Paginile deep web nu sunt indexate de motoarele de căutare publice
- B. Traficul din deep web este ilegal și monitorizat de forțele de ordine
- C. Site-urile din deep web necesită browsere specializate precum Tor pentru a fi accesate
- D. Paginile deep web se încarcă întotdeauna mai repede decât paginile din surface web

2. Cum se accesează dark web-ul?

- A. Prin browsere specializate care folosesc rețele de rutare onion
- B. Prin configurarea unor setări DNS personalizate pe routere standard
- C. Prin console de căutare web de suprafață private, doar pe bază de invitație
- D. Instalând o extensie de browser standard pentru blocarea reclamelor

3. Ce structură formează cea mai mare parte a deep web?

- A. Baze de date de utilizatori protejate prin parolă și conturi private
- B. Forumuri ilegale de piață neagră care tranzacționează bunuri ilicite
- C. Protocoale de partajare a fișierelor peer-to-peer necriptate
- D. Baze de date cu cache ale motoarelor de căutare publice

4. Ce face Onion Routing cu traficul de rețea?

- A. Criptează pachetele și le direcționează prin mai multe relee
- B. Crește vitezele de descărcare prin ocolirea nodurilor ISP
- C. Asociază numerele de serie hardware ale dispozitivelor cu înregistrări IP
- D. Șterge cookie-urile browserului web după fiecare clic

5. Ce sufix de domeniu este folosit exclusiv în rețelele Tor?

- A. Extensia criptografică de nivel superior .onion
- B. Extensia comercială clasică .com
- C. Extensia descentralizată Web3 .eth bazată pe blockchain
- D. Extensia tehnologică cu cod de țară .ai

Punct de control 2: Provocare Adevărat sau Fals

6 Întrebare adevărat/fals 6

6. Deep web-ul și dark web-ul se referă la același segment de rețea.

- ○ Adevărat
- ○ Fals

7 Întrebare adevărat/fals 7

7. Portalurile intranet corporative fac parte din deep web.

- ○ Adevărat
- ○ Fals

8 Întrebare adevărat/fals 8

8. Rutarea Onion decriptează complet pachetele de date la fiecare nod de tranzit.

- ○ Adevărat
- ○ Fals

9 Întrebare adevărat/fals 9

9. Accesarea dark web-ului expune dispozitivele la riscuri mari de malware.

- ○ Adevărat
- ○ Fals

10 Întrebare adevărat/fals 10

10. Motoarele de căutare web standard scanează și indexează site-urile onion.

- ○ 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. Portalurile bancare private se află în segmentul neindexat numit _____ .
2. Nodurile Tor specializate găzduiesc servicii ascunse din _____ .
3. Site-urile Tor folosesc extensia criptografică de nivel superior _____ .
4. Calea criptată, pe mai multe straturi, a traficului se numește _____ .
5. Motoarele de căutare de suprafață parcurg paginile accesibile public, adică pe cele _____ .
6. Rețelele onion criptează IP-urile clienților pentru a menține _____ utilizatorului.

BANCĂ DE CUVINTE DIN VOCABULAR

.ONION ANONIMAT BAZĂ DE DATE DARK WEB INDEXATE NOD DE INTRARE RUTARE ONION WEB PROFUND

Scrie răspunsurile aici:

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

Punct de control 4: Asocierea conceptelor despre securitate

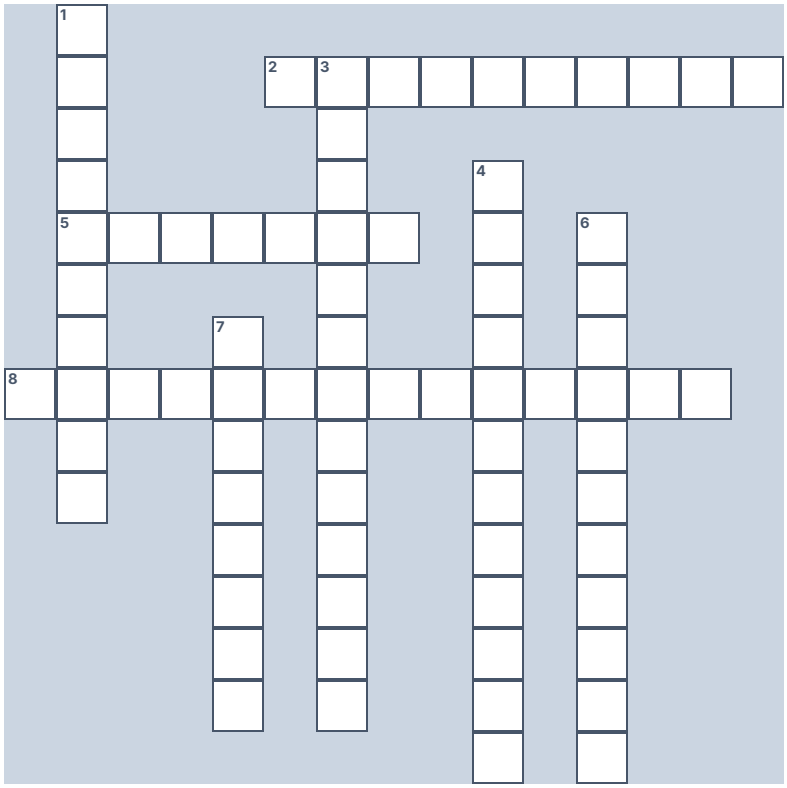
ASOCIEREA DEFINIȚIILOR

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

☐	1. Segmentul Deep Web	A	Segment de rețea criptat, accesibil doar prin browsere speciale.
☐	2. Portalul Dark Web	B	Criptarea datelor în straturi și retransmiterea lor prin trei noduri.
☐	3. Extensia Onion	C	Stocare backend securizată care găzduiește înregistrări de sistem neindexate.
☐	4. Rutare Tor	D	Sufix criptografic de domeniu de nivel superior folosit în rețelele Tor.
☐	5. Pagini indexate	E	Nodul-punct de intrare folosit pentru a accesa rețeaua Tor.
☐	6. Anonimatul utilizatorului	F	Conținut web de suprafață indexat și care poate fi căutat pe Google.
☐	7. Bază de date privată	G	Păstrarea adreselor IP publice ale clienților ascunse față de servere.
☐	8. Gateway de intrare	H	Conținut web neindexat, precum autentificări private, e-mailuri și înregistrări din baze de date.

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

2. Conținut web neindexat, precum autentificări private, e-mailuri și înregistrări din baze de date (10)

5. Segment de rețea criptat, accesibil doar prin browsere speciale (7)

8. Conținut al web-ului de suprafață, compilat și care poate fi căutat pe Google (14)

VERTICAL

1. Stocare securizată în backend, care găzduiește înregistrări de sistem neindexate (10)

3. Sufix criptografic de domeniu de nivel superior, folosit în rețelele Tor (13)

4. Nodul de intrare folosit pentru a accesa rețeaua Tor (12)

6. Criptarea datelor pe straturi și retransmiterea lor prin trei noduri (11)

7. Păstrarea ascunsă față de servere a adreselor IP publice ale clientului (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

2 orizontal: Conținut web neindexat, precum autentificări private, e-mailuri și înregistrări din baze de date (10 litere):

5 orizontal: Segment de rețea criptat, accesibil doar prin browsere speciale (7 litere):

8 orizontal: Conținut al web-ului de suprafață, compilat și care poate fi căutat pe Google (14 litere):

VERTICAL

1 vertical: Stocare securizată în backend, care găzduiește înregistrări de sistem neindexate (10 litere):

3 vertical: Sufix criptografic de domeniu de nivel superior, folosit în rețelele Tor (13 litere):

4 vertical: Nodul de intrare folosit pentru a accesa rețeaua Tor (12 litere):

6 vertical: Criptarea datelor pe straturi și retransmiterea lor prin trei noduri (11 litere):

7 vertical: Păstrarea ascunsă față de servere a adreselor IP publice ale clientului (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.

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

LISTĂ DE CUVINTE DIN VOCABULAR

WEBPROFUND DARKWEB EXTENSIEONION RUTAREONION PAGINIINDEXATE
ANONIMAT BAZĂDEDATE NODDEINTRARE

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. WEBPROFUND**
- **B. DARKWEB**
- **C. EXTENSIEONION**
- **D. RUTAREONION**
- **E. PAGINIINDEXATE**
- **F. ANONIMAT**
- **G. BAZĂDEDATE**
- **H. NODDEINTRARE**

DEFINIȚII ȘI CÂMPURI DE ASOCIERE

_____ 1. Păstrarea ascunsă față de servere a adreselor IP publice ale clientului.

_____ 2. Stocare securizată în backend, care găzduiește înregistrări de sistem neindexate.

_____ 3. Criptarea datelor pe straturi și retransmiterea lor prin trei noduri.

_____ 4. Conținut web neindexat, precum autentificări private, e-mailuri și înregistrări din baze de date.

_____ 5. Segment de rețea criptat, accesibil doar prin browsere speciale.

_____ 6. Sufix criptografic de domeniu de nivel superior, folosit în rețelele Tor.

_____ 7. Nodul de intrare folosit pentru a accesa rețeaua Tor.

_____ 8. Conținut al web-ului de suprafață, compilat și care poate fi căutat pe Google.

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. NFOREWUDPB
2. ONXSTEIINONEE
3. PDATNEEXGINIAI
4. ETDEĂADBAZ
5. WBKRDEA
6. RNENOIRUOTA
7. ATIMANNO
8. TDEANENIORRD

Activitate bonus: Gândește repede

3 RĂSPUNSURI PE CATEGORIE. CÂȘTIGĂ CINE COMPLETEAZĂ PRIMUL LISTA.

1	Motive pentru care să eviți dark web-ul			
2	Lucruri pe care un motor de căutare nu le poate găsi			
3	Dispozitive care pot fi sparte			
4	Motive legale pentru a folosi Tor			
5	Motive pentru care ar trebui să actualizezi software-ul			
6	Semnale de avertizare într-un e-mail			
7	Lucruri vândute ilegal pe dark web			
8	Persoane pe care le poți întreba pentru ajutor IT			
9	Obiceiuri sigure pe care le poți începe de azi			
10	Lucruri de făcut după o scurgere de date			
11	Lucruri care fac parte din deep web			
12	Site-uri pe care le folosești cu autentificare			
13	Cuvinte legate de anonimat			
14	Informații pe care nu ar trebui să le dai niciodată			
15	Lucruri care se află „sub suprafață”			

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: IDENTIFICAREA UNEI SCURGERI DE DATE



Scenariu: Un audit de securitate corporativ descoperă că înregistrări sensibile din baza de date a clienților sunt tranzacționate pe o piață onion. Datele nu sunt indexate în Google.

Întrebare de discuție: Explică ce segmente ale web-ului sunt implicate și cum a avut loc această scurgere.

STUDIU DE CAZ 2: ANONIMAT VS. RISCURI MALWARE



Scenariu: Un analist vrea să verifice fluxurile de informații despre amenințări de pe un site Tor. Descarcă browserul Tor și accesează site-ul.

Întrebare de discuție: Evaluează avantajele anonimatului și descrie pe scurt pașii de reducere a riscului de malware.

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

19	2	22	24	21	7	1	31	2		1	17	18	17	11	16	1	24	26	15
19	21	11	17		21	26	24	1	21	7		18	17	11	18	17			
				22	11	9	26	21	2										

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: Ce este web-ul profund (deep web)?

Deep web-ul este alcătuit din toate paginile web pe care motoarele de căutare nu le pot indexa, inclusiv serviciile bancare online, bazele de date de e-mail și revistele cu acces contra cost.

Q2: Ce este dark web-ul?

Dark web-ul este un mic subset al deep web-ului, ascuns intenționat și accesibil doar prin browsere specializate care folosesc rețele onion.

Q3: Cum indexează motoarele de căutare paginile?

Motoarele rulează programe automate (spideri) pentru a urma linkurile publice, indexând paginile care nu blochează crawlingul prin directive robot.

Q4: De ce este considerată activitatea bancară online parte a deep web?

Portalurile bancare sunt protejate prin ecrane de autentificare și parole, ceea ce împiedică motoarele de căutare publice să indexeze paginile cu extrase de cont.

Q5: Ce este rutarea Onion din browserul Tor?

Rutarea Onion este o metodă de transmisie care criptează traficul în straturi și îl trece prin mai multe relee pentru a masca adresele IP ale utilizatorilor.

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

Parcurge întrebările și răspunsurile frecvente despre atenuarea amenințărilor online.

Q6: Este ilegal accesul la dark web?

Nu. Accesarea dark web-ului este legală în majoritatea țărilor, deși participarea la piețe ilegale sau la activități cibernetice ilegale este interzisă.

Q7: De ce se încarcă lent site-urile din dark web?

Traficul este rutat și decriptat prin cel puțin trei relee globale (intrare, intermediar, ieșire), ceea ce crește latența transmisiei.

Q8: Ce înseamnă sufixul de domeniu .onion?

Este un sufix specializat de domeniu de nivel superior folosit în rețelele Tor, care trimite către adrese generate criptografic, în loc de servere DNS standard.

Q9: Ce riscuri sunt asociate cu linkurile din dark web?

Site-urile nu au filtrare de securitate, expunând utilizatorii la rate mari de infectare cu malware, scripturi de phishing și escrocherii de tranzacții.

Q10: Cine a creat protocolul de rutare al rețelei Tor?

Tehnologia a fost dezvoltată inițial de Laboratorul de Cercetare Navală al SUA în anii 1990 pentru a proteja comunicațiile guvernamentale.

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 protejează nodurile intermediare anonimatul în Tor?

Fiecare nod decriptează un singur strat de date de rutare, aflând doar saltul anterior și pe cel următor, niciodată și sursa, și destinația.

Q2: Care este rolul nodului de ieșire?

Nodul de ieșire decriptează ultimul strat de criptare, trimițând traficul către serverul public de destinație sau către serverul onion.

Q3: Ce este un gateway cu punți Tor (Tor bridges)?

Bridge-urile sunt relee de intrare Tor nelistate, folosite pentru a ocoli blocajele ISP și cenzura în regiunile care restricționează accesul la browserul Tor.

Q4: Cum exploatează actorii din dark web criptomonedele?

Actorii folosesc criptomonede anonime pentru a executa tranzacții financiare pe piețe dark, evitând verificările bancare standard ale tranzacțiilor.

Q5: De ce nu reușesc motoarele de căutare obișnuite să acceseze bazele de date profunde?

Crawlerele nu pot introduce credențiale de autentificare, nu pot rezolva CAPTCHA-uri de securitate și nu pot rula scripturile de interogare SQL din backend necesare pentru a accesa bazele de date din deep web.

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: Ce este un server director în rețelele Tor?

Este un server de încredere care întreține lista releelor active de intrare, intermediare și de ieșire folosite de clienți pentru a construi căile de rutare.

Q7: Cum realizează actorii rău intenționați interceptarea la nodul de ieșire (exit node sniffing)?

Operatorii nodurilor de ieșire rău intenționate pot intercepta traficul HTTP necriptat la ieșirea din rețeaua Tor, furând nume de utilizator și cookie-uri.

Q8: Care este diferența dintre Tor și I2P?

Tor folosește un director centralizat de relee și noduri de ieșire pentru acces la web-ul public, în timp ce I2P folosește o structură descentralizată peer-to-peer pentru găzduirea internă.

Q9: Cum urmăresc agențiile de aplicare a legii piețele din dark web?

Agențiile folosesc analiza blockchain, localizează configurațiile fizice de găzduire a serverelor și derulează operațiuni-momeală pentru a identifica operatorii.

Q10: Cum compromite scurgerea DNS anonimatul clientului?

Scurgerile DNS apar atunci când interogările DNS ale browserului sunt trimise direct prin furnizorul local de internet, în loc să fie direcționate prin rețeaua Tor criptată.

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

Deep web-ul este mult mai mare decât web-ul de suprafață care poate fi căutat, deoarece cea mai mare parte a conținutului se află în spatele autentificărilor și al bazelor de date.

2. INFORMAȚII DESPRE SECURITATE

Dark web-ul este o parte mică a deep web-ului, ascunsă intenționat, la care se ajunge cu instrumente precum Tor.

3. INFORMAȚII DESPRE SECURITATE

Rutarea Tor criptează pachetele de date de trei ori, dezvelind straturile de criptare ca pe cele ale unei cepe la fiecare nod releu.

4. INFORMAȚII DESPRE SECURITATE

Tor a apărut din proiectul de rutare onion al Laboratorului de Cercetare Navală al SUA, iar codul său a fost lansat ca software liber. [1]

5. INFORMAȚII DESPRE SECURITATE

Adresele Onion sunt șiruri alfanumerice de 56 de caractere, generate criptografic din perechi de chei publice.

6. INFORMAȚII DESPRE SECURITATE

Nodurile de ieșire pot citi traficul necriptat, ceea ce înseamnă că TLS/HTTPS este în continuare necesar pe Tor pentru datele securizate ale sesiunii.

7. PERSPECTIVĂ ASUPRA SECURITĂȚII

Site-urile intranet, unitățile cloud și bazele de date private reprezintă cele mai mari segmente de stocare a datelor din deep web.

8. PERSPECTIVĂ ASUPRA SECURITĂȚII

Motoare de căutare specializate precum DuckDuckGo găzduiesc portaluri onion pentru a permite căutări anonime în rețelele Tor.

9. PERSPECTIVĂ ASUPRA SECURITĂȚII

Peste 2 milioane de utilizatori se conectează zilnic la rețeaua Tor pentru a ocoli cenzura și a-și păstra confidențialitatea comunicațiilor.

10. INFORMAȚII DESPRE SECURITATE

Operațiunile globale ale forțelor de ordine (precum Operation Bayonet) au închis piețe întunecate importante prin confiscarea hardware-ului de găzduire.

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] 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

Barem: Punct de control 1 – Alegere multiplă

1 **Indexarea în motoarele de căutare** WEB PROFUND Răspuns corect: A

NOTĂ PENTRU PROFESOR

Paginile din web-ul profund se află în spatele unor bariere de autentificare și al unor baze de date, ceea ce îi împiedică pe crawlerii motoarelor de căutare să le parcurgă. Citare: IETF RFC 3986.

2 **Acces Tor** DARK WEB Răspuns corect: A

NOTĂ PENTRU PROFESOR

Dark web-ul este alcătuit din servicii onion ascunse, accesibile doar prin browsere precum Tor. Citare: IETF RFC 3986.

3 **Baze de date profunde** BAZE DE DATE Răspuns corect: A

NOTĂ PENTRU PROFESOR

Conturile protejate prin parolă și evidențele corporative formează cel mai mare segment al web-ului profund. Citație: NIST Digital Identity.

4 **Rutare Onion** REȚEAUA TOR Răspuns corect: A

NOTĂ PENTRU PROFESOR

Rutarea Onion criptează pachetele de date în straturi și le transmite prin mai multe noduri pentru anonimat. Citație: IETF RFC 3986.

5 **Domeniu Onion** SUFIX Răspuns corect: A

NOTĂ PENTRU PROFESOR

Sufixul de domeniu criptografic.onion rutează traficul intern în Tor, fără DNS public. Citare: IETF RFC 3986.

Barem: Punct de control 2 – Adevărat sau fals

6 **Segmente web** STRUCTURĂ — **Răspuns corect: Fals**

NOTĂ PENTRU PROFESOR

Deep web-ul cuprinde toate paginile neindexate, în timp ce dark web-ul este un mic subsegment onion criptat. Citare: IETF RFC 3986.

7 **Intraneturi corporative** WEB PROFUND — **Răspuns corect: Adevărat**

NOTĂ PENTRU PROFESOR

Site-urile intranet sunt în spatele unor portaluri protejate prin parolă și nu sunt indexate, ceea ce înseamnă că aparțin deep web-ului. Citare: NIST Digital Identity.

8 **Criptare pe straturi** RELEE — **Răspuns corect: Fals**

NOTĂ PENTRU PROFESOR

Releele Onion decriptează doar un strat de rutare pentru a proteja anonimatul utilizatorului, niciodată întregul pachet. Citație: IETF RFC 3986.

9 **Expunerea la software rău intenționat** AMENINȚĂRI — **Răspuns corect: Adevărat**

NOTĂ PENTRU PROFESOR

Piețele din dark web nu au filtrare de securitate și prezintă riscuri extreme de infectare cu software rău intenționat. Citare: Center for Internet Security (CIS).

10 **Întrebarea 10** — **Răspuns corect: Fals**

NOTĂ PENTRU PROFESOR

Crawlerele obișnuite ale motoarelor de căutare nu folosesc Tor, deci nu pot ajunge la site-urile .onion și nici nu le pot indexa.

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

H 1. Segmentul Deep Web	A 2. Portalul Dark Web	D 3. Extensia Onion	B 4. Rutare Tor
F 5. Pagini indexate	G 6. Anonimatul utilizatorului	C 7. Bază de date privată	E 8. Gateway de intrare

PUNCT DE CONTROL 3: BAREM – TERMENI-CHEIE

1 WEB PROFUND	2 DARK WEB	3 .ONION	4 RUTARE ONION
5 INDEXATE	6 ANONIMAT		

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

1 F – ANONIMAT	2 G – BAZĂDEDATE	3 D – RUTAREONION	4 A – WEBPROFUND
5 B – DARKWEB	6 C – EXTENSIEONION	7 H – NODDEINTRARE	8 E – PAGINIINDEXATE

NOTE DE DISCUȚIE PENTRU PROFESORI

Termeni-cheie:
Verifică dacă elevii pot explica Segmentul Deep Web, Portalul Dark Web și Extensia Onion 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.

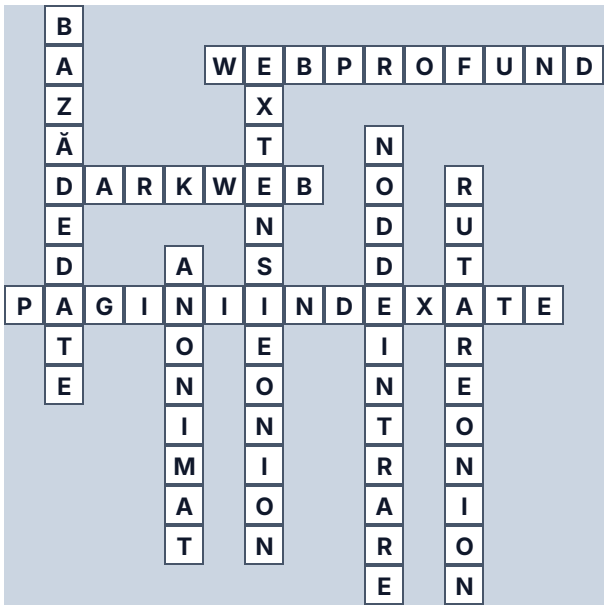
Evaluarea surselor:
Cere elevilor să verifice cel puțin o afirmație în sursele fișei și discutați de ce cifrele, prețurile și regulile se pot schimba în timp.

Chei de rezolvare ale puzzle-urilor și note pentru profesor

SOLUȚIA JOCULUI DE CĂUTARE DE CUVINTE

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

SOLUȚIA CUVINTELOR ÎNCRUCIȘATE



GHID PENTRU PROFESOR: SOLUȚIILE LA CUVINTELE ÎNCRUCIȘATE

ORIZONTAL

2 orizontal: WEBPROFUND Conținut web neindexat, precum autentificări private, e-mailuri și înregistrări din baze de date (10 litere)

5 orizontal: DARKWEB Segment de rețea criptat, accesibil doar prin browsere speciale (7 litere)

8 orizontal: PAGINIINDEXATE Conținut al web-ului de suprafață, compilat și care poate fi căutat pe Google (14 litere)

VERTICAL

1 vertical: BAZĂDEDATE Stocare securizată în backend, care găzduiește înregistrări de sistem neindexate (10 litere)

3 vertical: EXTENSIEONION Sufix criptografic de domeniu de nivel superior, folosit în rețelele Tor (13 litere)

4 vertical: NODDEINTRARE Nodul de intrare folosit pentru a accesa rețeaua Tor (12 litere)

6 vertical: RUTAREONION Criptarea datelor pe straturi și retransmiterea lor prin trei noduri (11 litere)

7 vertical: ANONIMAT Păstrarea ascunsă față de servere a adreselor IP publice ale clientului (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. N F O R E W U D P B — **WEBPROFUND**
2. O N X S T E I I N O N E E — **EXTENSIEONION**
3. P D A T N E E X G I N I A I — **PAGINIINDEXATE**
4. E T D E Ă A D B A Z — **BAZĂDEDATE**
5. W B K R D E A — **DARKWEB**
6. R N E N O I R U O T A — **RUTAREONION**
7. A T I M A N N O — **ANONIMAT**
8. T D E A N E N I O R R D — **NODDEINTRARE**

BAREMUL PROVOCĂRII CU CODUL SECRET

"PĂSTREAZĂ ANONIMATUL PRIN RUTARE ONION SIGURĂ"

Barem pentru studiile de caz

A Studiu de caz 1: Identificarea unei scurgeri de date

Soluția profesorului

GHID DE NOTARE

Răspunsurile elevilor ar trebui să acopere următoarele puncte:

- Analiza scenariului: Un audit de securitate corporativ descoperă că înregistrări sensibile din baza de date a clienților sunt comercializate pe o piață onion. Datele nu sunt indexate în Google.
- Strategie și soluție recomandată: Segmentele implicate: Baza de date privată aparține deep web (neindexat, dar securizat). Piața care comercializează datele furate se află pe dark web (rețeaua onion). Cum s-a întâmplat: Hackerii au ocolit apărările serverului, au furat baza de date din deep web și au listat-o anonim pe dark web pentru a scăpa de urmărirea autorităților.

B Studiu de caz 2: Anonimat vs. riscuri malware

Soluția profesorului

GHID DE NOTARE

Răspunsurile elevilor ar trebui să acopere următoarele puncte:

- Analiza scenariului: Un analist vrea să verifice fluxuri de informații despre amenințări pe un site Tor. Descarcă browserul Tor și accesează site-ul.
- Strategie și soluție recomandate: Beneficii: Tor direcționează traficul prin trei noduri, mascând IP-ul corporativ al analistului. Riscuri și atenuare: Linkurile din dark web nu au nicio filtrare reputațională. Analiștii trebuie să ruleze Tor în mașini virtuale (VM) izolate, să dezactiveze JavaScript în setările Tor și să evite descărcarea oricăror fișiere pentru a proteja rețeaua corporativă.