Emri: _____ Data: _____ Pikët: _____

Web-i i errët kundër web-it të thellë: siguria dhe Dallimet

Indeksimi i motorëve të kërkimit, bazat e të dhënave të deep web, rrugëzimi onion i Tor, anonimiteti i rrjetit dhe rreziqet

PËRMBLEDHJE MËSIMORE PËR DARK WEB KUNDREJT DEEP WEB

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 dallimeve mes Internetit të Thellë dhe Internetit të Errët. Do të eksplorosh bazat e të dhënave të paindeksuara, Onion Routing të shfletuesit Tor, domenet kriptografike .onion dhe rreziqet e sigurisë së anonimitetit.

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/web-i-erret-vs-web-i-thelle/

Udhërrëfyesi yt mësimor për strategjinë e internetit të thellë dhe të errët

- Krahaso deep web-in (baza të dhënash të paindeksuara) me dark web-in (shërbimet onion).
- Kupto se si Onion Routing e enkripton dhe e përcjell trafikun e rrjetit.
- Vlerëso rreziqet e sigurisë të hyrjes në faqe të paverifikuara të rrjetit Tor.
- Zbato politika portash hyrëse të sigurta dhe sandboxing-u për eksplorimin e inteligjencës së kërcënimeve.
- Analizo formatin kriptografik të adresave të domeneve të shërbimeve onion.

UDHËZIME PËR UDHËZUESIN E WEB-IT TË THELLË DHE TË ERRËT

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 privatësinë në rrjetin e thellë dhe të errët (deep dhe dark web). Përfundo me aktivitetin bonus Mendo shpejt.

BAZAT E TË DHËNAVE TË WEB-IT TË THELLË KUNDËR RRUGËZIMIT ONION TË WEB-IT TË ERRËT (HYRJE)

Uebi i thellë përbëhet nga faqe të paindeksuara pas fjalëkalimeve dhe hyrjeve, si emailet private ose portalet bankare të korporatave. Uebi i errët është një nënbashkësi e uebit të thellë që fshihet qëllimisht dhe kërkon shfletues të specializuar (si Tor) dhe rrjete onion për t'u aksesuar në mënyrë anonime.

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

Pika e kontrollit 1: Sfida me zgjedhje të shumëfishtë

1. Çfarë e dallon deep web nga surface web?

- A. Faqet e uebit të thellë nuk indeksohen nga motorët publikë të kërkimit
- B. Trafiku i rrjetit të thellë (deep web) është i paligjshëm dhe monitorohet nga zbatimi i ligjit
- C. Faqet e rrjetit të thellë kërkojnë shfletues të specializuar si Tor për t'u hapur
- D. Faqet e deep web-it ngarkohen gjithmonë më shpejt se faqet e surface web-it

2. Si hyhet në dark web?

- A. Përmes shfletuesve të specializuar që përdorin rrjete drejtimi onion
- B. Duke konfiguruar cilësime DNS të personalizuara në router-a standardë
- C. Përmes konsolave private të kërkimit të sipërfaqes së uebit vetëm me ftesë
- D. Duke instaluar një zgjerim standard shfletuesi për bllokimin e reklamave

3. Cila strukturë përbën pjesën më të madhe të deep web?

- A. Baza të dhënash të përdoruesve të mbrojtura me fjalëkalim dhe llogari private
- B. Forume të paligjshme të tregut të zi që tregtojnë mallra të paligjshme
- C. Protokolle jo të enkriptuara të ndarjes së skedarëve peer-to-peer
- D. Bazat e të dhënave të cache-it të motorëve publikë të kërkimit

4. Çfarë i bën Onion Routing trafikut të rrjetit?

- A. Enkripton paketat dhe i drejton përmes disa releve
- B. Rrit shpejtësinë e shkarkimit duke anashkaluar nyjet e ISP-së
- C. Lidh numrat serialë të harduerit të pajisjes me regjistrimet IP
- D. Fshin cookie-t e shfletuesit pas çdo klikimi

5. Cila prapashtesë domeni përdoret ekskluzivisht në rrjetet Tor?

- A. Shtesa kriptografike e nivelit më të lartë .onion
- B. Shtesa standarde tregtare e vjetër .com
- C. Shtesa e decentralizuar Web3 .eth e blockchain-it
- D. Shtesa teknologjike .ai me kod shteti

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

6 Pyetje E/G 6

6. Uebi i thellë dhe uebi i errët i referohen të njëjtit segment të rrjetit.

E vërtetë E gabuar

7 Pyetje E/G 7

7. Portalet e intraneteve të korporatave janë pjesë e deep web-it.

E vërtetë E gabuar

8 Pyetje E/G 8

8. Rrugëzimi onion i deshifron plotësisht paketat e të dhënave në çdo nyje tranziti.

E vërtetë E gabuar

9 Pyetje E/G 9

9. Qasja në dark web i ekspozon pajisjet ndaj rreziqeve të larta nga malware-i.

E vërtetë E gabuar

10 Pyetje E/G 10

10. Motorët standardë të kërkimit në ueb i crawl-ojnë dhe i indeksojnë faqet onion.

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. Portalet private të bankave ndodhen në segmentin e paindeksuar _____ .
2. Nyjet e specializuara Tor strehojnë shërbime të fshehura të _____ .
3. Faqet e Tor përdorin shtesën kriptografike të nivelit të lartë _____ .
4. Rruga e trafikut të enkriptuar me shumë shtresa quhet _____ .
5. Motorët e kërkimit të sipërfaqes skanojnë faqe që janë publikisht të _____ .
6. Rrjetet Onion enkriptojnë IP-të e klientëve për të ruajtur këtë cilësi të përdoruesit: _____ .

BANKA E FJALËVE TË LEKSIKUT

ANONIMITET | BAZË TË DHËNASH | DARK WEB | DEEP WEB | INDEKSUARA | NYJË HYRËSE | ONION | RUTIM TOR

Shkruaj përgjigjet e tua këtu:

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

Pika e kontrollit 4: Përputhja e koncepteve të sigurisë

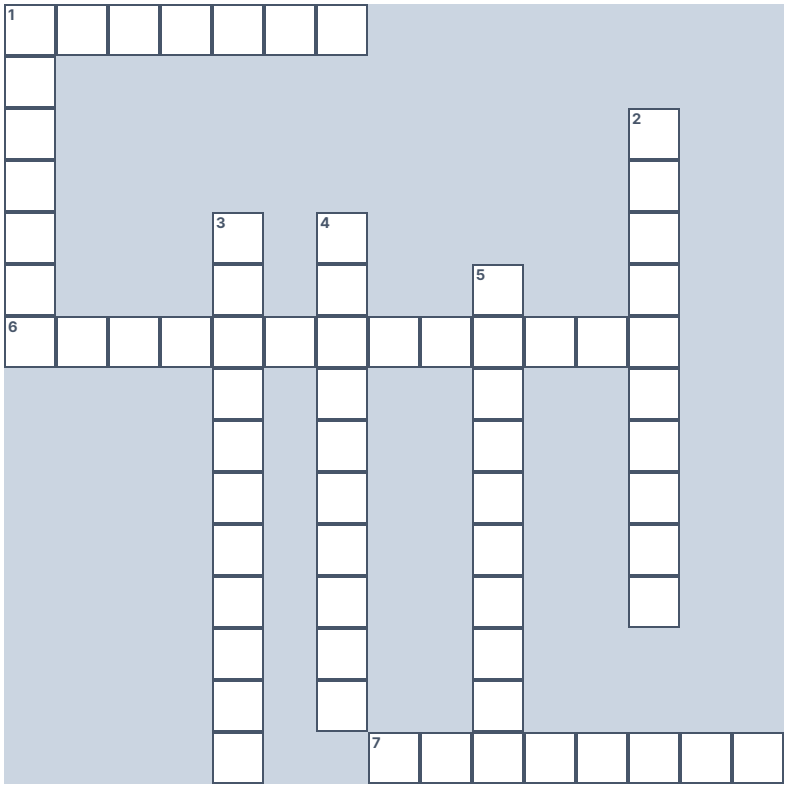
PËRPUTHJA E PËRKUFIZIMEVE

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. Segmenti i internetit të thellë	A	Segment i enkriptuar i rrjetit i qasshëm vetëm përmes shfletuesve të veçantë.
☐	2. Portali i internetit të errët	B	Enkriptimi i të dhënave në shtresa dhe transmetimi i tyre përmes tri nyjeve.
☐	3. Zgjerimi Onion	C	Ruajtje e sigurt në backend që strehon regjistrime të sistemit të paindeksuara.
☐	4. Drejtimi Tor	D	Prapashtesë kriptografike e domenit të nivelit të lartë e përdorur në rrjetet Tor.
☐	5. Faqet e indeksuara	E	Nyja e pikës hyrëse e përdorur për të hyrë në rrjetin Tor.
☐	6. Anonimiteti i përdoruesit	F	Përmbajtje e uebit sipërfaqësor e përpiluar dhe e kërkueshme në Google.
☐	7. Bazë e dhënash private	G	Fshehja e adresave publike IP të klientit nga serverët.
☐	8. Gateway-i i hyrjes	H	Përmbajtja e uebit e paindeksuar si hyrjet private, emailet dhe regjistrimet e bazave të të dhënave.

Pika e kontrollit 5: Fjalëkryq

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



HORIZONTALISHT

1. Segment i enkriptuar i rrjetit i qasshëm vetëm përmes shfletuesve të veçantë (7)

6. Ruajtje e sigurt e pjesës së prapme që strehon regjistrime sistemi të paindeksuara (13)

7. Enkriptimi i të dhënave në shtresa dhe përcjellja e tyre përmes tri nyjeve (8)

VERTIKALISHT

1. Përmbajtje uebi e paindeksuar si hyrjet private, email-et dhe regjistrimet e bazave të të dhënave (7)

2. Nyja e hyrjes që përdoret për të hyrë në rrjetin Tor (10)

3. Prapashtesë kriptografike e domenit të nivelit të lartë që përdoret në rrjetet Tor (11)

4. Përmbajtje e uebit të sipërfaqes e përpiluar dhe e kërkueshme në Google (10)

5. Mbajtja e adresave publike IP të klientit të fshehura nga serverët (10)

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

1 horizontalisht: Segment i enkriptuar i rrjetit i qasshëm vetëm përmes shfletuesve të veçantë (7 shkronja):

6 horizontalisht: Ruajtje e sigurt e pjesës së prapme që strehon regjistrime sistemi të paindeksuara (13 shkronja):

7 horizontalisht: Enkriptimi i të dhënave në shtresa dhe përcjellja e tyre përmes tri nyjeve (8 shkronja):

VERTIKALISHT

1 vertikalisht: Përmbajtje uebi e paindeksuar si hyrjet private, email-et dhe regjistrimet e bazave të të dhënave (7 shkronja):

2 vertikalisht: Nyja e hyrjes që përdoret për të hyrë në rrjetin Tor (10 shkronja):

3 vertikalisht: Prapashtesë kriptografike e domenit të nivelit të lartë që përdoret në rrjetet Tor (11 shkronja):

4 vertikalisht: Përmbajtje e uebit të sipërfaqes e përpiluar dhe e kërkueshme në Google (10 shkronja):

5 vertikalisht: Mbajtja e adresave publike IP të klientit të fshehura nga serverët (10 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.

A E N I M Ç L I C Ç F G B B N

N Q K O U B S N G Y E Y Q F X

O V G E P E S D M T I Q Ç S R

I K O J L W R E G I O G Y N K

N V T M Y K P K P B A J N L B

O J G E H R M S Y B Z Z Y B D

A L U X K A C U E N V O P X E

S F D Y C D V A K E F F Z V E

E C N P I V X R Q J Z A L Q P

T Z Q K Ë R V A Ë J V H B Y W

H B A Z Ë T Ë D H Ë N A S H E

S C C N Y J Ë H Y R Ë S E Y B

N T A N O N I M I T E T Z N Z

T S B G U O X C L K G O X Y Z

X R O T M I T U R F M H M Q V

LISTA E FJALËVE TË LEKSIKUT

DEEPWEB DARKWEB SHTESAONION RUTIMTOR INDEKSUARA ANONIMITET BAZËTËDHËNASH NYJËHYRËSE

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. DEEPWEB**
- **B. DARKWEB**
- **C. SHTESAONION**
- **D. RUTIMTOR**
- **E. INDEKSUARA**
- **F. ANONIMITET**
- **G. BAZËTËDHËNASH**
- **H. NYJËHYRËSE**

PËRKUFIZIME DHE FUSHA PËRPUTHJEJE

1. Mbajtja e adresave publike IP të klientit të fshehura nga serverët.
2. Ruajtje e sigurt e pjesës së prapme që strehon regjistrime sistemi të paindeksuara.
3. Enkriptimi i të dhënave në shtresa dhe përcjellja e tyre përmes tri nyjeve.
4. Përmbajtje uebi e paindeksuar si hyrjet private, email-et dhe regjistrimet e bazave të të dhënave.
5. Segment i enkriptuar i rrjetit i qasshëm vetëm përmes shfletuesve të veçantë.
6. Prapashtesë kriptografike e domenit të nivelit të lartë që përdoret në rrjetet Tor.
7. Nyja e hyrjes që përdoret për të hyrë në rrjetin Tor.
8. Përmbajtje e uebit të sipërfaqes e përpiluar dhe e kërkueshme në Google.

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. **PEDWBEE**
2. **SNHSOATINOE**
3. **ISRUNKAEAD**
4. **ËSËZHTHDANBAË**
5. **WBKRDEA**
6. **ORITRMUT**
7. **NNAIMTETIO**
8. **SËYENHYRËJ**

Aktivitet bonus: Mendo shpejt

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

1	Arsye për t'u larguar nga dark web-i			
2	Gjëra që një motor kërkimi nuk mund t'i gjejë			
3	Pajisje që mund të hakohen			
4	Arsye ligjore për të përdorur Tor			
5	Arsye për të përditësuar softuerin			
6	Shenja paralajmëruese në një email			
7	Gjëra që shiten në mënyrë të paligjshme në dark web			
8	Njerëz që mund t'i pyesësh për ndihmë me IT-në			
9	Zakone të sigurta që mund t'i fillosh sot			
10	Gjëra që bëhen pas një rrjedhjeje të dhënash			
11	Gjëra që i përkasin internetit të thellë (deep web)			
12	Faqe që i përdor me identifikim			
13	Fjalë që lidhen me anonimitetin			
14	Informacione që nuk duhet t'i ndash kurrë			
15	Gjëra që qëndrojnë 'nën sipërfaqe'			

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: IDENTIFIKIMI I RRJEDHJES SË TË DHËNAVE



Skenari: Një auditim sigurie i kompanisë zbulon se regjistrat e ndjeshëm të bazës së të dhënave të klientëve po tregtohen në një treg onion. Të dhënat nuk janë të indeksuara në Google.

Pyetje për diskutim: Shpjego cilat segmente të internetit përfshihen dhe si ndodhi kjo rrjedhje.

STUDIMI I RASTIT 2: ANONIMITETI KUNDREJT RREZIQEVE TË MALWARE-IT



Skenari: Një analist dëshiron të kontrollojë burimet e inteligjencës së kërcënimeve në një faqe Tor. Ai shkarkon shfletuesin Tor dhe hyn në faqe.

Pyetje për diskutim: Vlerëso përfitimet e anonimitetit dhe përshkruaj hapat për zbutjen e malware-it.

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

20	23	1	12		1	16	17	16	11	15	11	22	6	22	11	16		15	6

20	23	22	11	15	11	16		6		21	11	9	23	20	22

17	16	11	17	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: Çfarë është deep web?

Uebi i thellë përbëhet nga të gjitha faqet e uebit që motorët e kërkimit nuk mund t'i indeksojnë, përfshirë bankingun online, bazat e të dhënave të emailit dhe revistat me pagesë.

Q2: Çfarë është dark web?

Uebi i errët është një nënbashkësi e vogël e uebit të thellë, e fshehur qëllimisht dhe e aksesueshme vetëm përmes shfletuesve të specializuar që përdorin rrjete onion.

Q3: Si i indeksojnë motorët e kërkimit faqet?

Motorët ekzekutojnë programe automatike (spiders) për të ndjekur lidhjet publike, duke indeksuar faqet që nuk e bllokojnë eksplorimin me direktiva roboti.

Q4: Pse konsiderohet bankingu online pjesë e deep web?

Portalet bankare janë pas mureve të hyrjes dhe fjalëkalimeve, duke ua bllokuar motorëve publikë indeksimin e faqeve të pasqyrave të llogarisë.

Q5: Çfarë është ruterimi Onion i shfletuesit Tor?

Rrugëzimi onion është një metodë transmetimi që enkripton trafikun në shtresa dhe e kalon përmes disa relejesh për të maskuar adresat IP të përdoruesve.

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: A është i paligjshëm aksesi në dark web?

Jo. Aksesi në dark web është i ligjshëm në shumicën e vendeve, megjithëse përfshirja në tregje të paligjshme ose aktivitete kibernetike është e ndaluar.

Q7: Pse ngarkohen ngadalë faqet e dark web?

Trafiku rrugëzohet dhe deshifrohet përmes të paktën tri releve globale (hyrëse, e ndërmjetme, dalëse), çka e rrit vonesën e transmetimit.

Q8: Çfarë do të thotë prapashtesa e domenit .onion?

Është një prapashtesë e specializuar e domenit të nivelit të lartë e përdorur në rrjetet Tor, që drejton te adresa të gjeneruara kriptografikisht në vend të serverëve standardë DNS.

Q9: Cilat rreziqe lidhen me lidhjet e dark web?

Faqet nuk kanë filtrim sigurie, duke i ekspozuar përdoruesit ndaj normave të larta infektimi me malware, skripteve phishing dhe mashtrimeve me transaksione.

Q10: Kush e krijoi protokollin e rrugëzimit të rrjetit Tor?

Teknologjia u zhvillua fillimisht nga Laboratori Kërkimor Detar i SHBA-së në vitet 1990 për të mbrojtur komunikimet qeveritare.

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 mbrojnë anonimitetin e Tor nyjet e ndërmjetme?

Çdo nyje dekripton vetëm një shtresë të të dhënave të rrugëzimit, duke mësuar vetëm hapin e mëparshëm dhe hapin pasardhës, kurrë burimin dhe destinacionin njëkohësisht.

Q2: Cili është roli i nyjes dalëse?

Nyja dalëse e deshifron shtresën e fundit të enkriptimit, duke e dërguar trafikun te serveri publik i destinacionit ose serveri onion.

Q3: Çfarë është një portë ndërlidhëse me urat e Tor (Tor bridges)?

Bridges janë rele hyrëse Tor të palistuara, të përdorura për të anashkaluar bllokimet e ISP-së dhe censurën në rajone që kufizojnë qasjen në shfletuesin Tor.

Q4: Si e shfrytëzojnë kriptovalutën aktorët e internetit të errët (dark web)?

Aktorët përdorin kriptovaluta anonime për të kryer tregtime financiare në tregjet e errëta, duke shmangur kontrollet standarde të transaksioneve bankare.

Q5: Pse dështojnë motorët e zakonshëm të kërkimit të kalojnë nëpër bazat e thella të të dhënave?

Crawler-at nuk mund të futin kredenciale hyrjeje, të zgjidhin CAPTCHA sigurie ose të ekzekutojnë skriptet e kërkesave SQL të backend-it të nevojshme për të hyrë në bazat e thella të të dhënave.

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: Çfarë është një server direktorie në rrjetet Tor?

Është një server i besuar që mban listën e rele-ve aktive hyrëse, të mesme dhe dalëse të përdorura nga klientët për të ndërtuar shtigjet e rrugëzimit.

Q7: Si e kryejnë aktorët keqdashës përgjimin në nyjën dalëse (exit node sniffing)?

Operatorët e nyjeve të rreme të daljes mund të përgjojnë trafikun e paenkriptuar HTTP teksa del nga rrjeti Tor, duke vjedhur emra përdoruesish dhe cookie.

Q8: Cili është ndryshimi mes Tor dhe I2P?

Tor përdor një direktori të centralizuar releve dhe nyje dalëse për qasjen në uebin publik, ndërsa I2P përdor një strukturë të decentralizuar peer-to-peer për hostim të brendshëm.

Q9: Si i gjurmojnë agjencitë e zbatimit të ligjit tregjet e dark web?

Agjencitë përdorin analizën blockchain, lokalizojnë konfigurimet fizike të hostimit të serverëve dhe kryejnë operacione karth për të identifikuar operatorët.

Q10: Si e kompromenton rrjedhja e DNS anonimitetin e klientit?

Rrjedhjet e DNS ndodhin kur kërkesat DNS të shfletuesit dërgohen drejtpërdrejt nëpërmjet ISP-së lokale në vend që të drejtohen nëpërmjet rrjetit të enkriptuar Tor.

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

Uebi i thellë është shumë më i madh se uebi sipërfaqësor i kërkueshëm, pasi pjesa më e madhe e përmbajtjes është pas hyrjeve dhe bazave të të dhënave.

2. PERSPEKTIVË PËR SIGURINË

Uebi i errët është një pjesë e vogël e fshehur qëllimisht e uebit të thellë, që arrihet me mjete si Tor.

3. PERSPEKTIVË PËR SIGURINË

Rrugëzimi Tor i enkripton paketat e të dhënave tri herë, duke hequr shtresat e enkriptimit si një qepë në secilën nyje rele.

4. PERSPEKTIVË PËR SIGURINË

Tor u zhvillua nga projekti i rrugëzimit onion i drejtuar nga Laboratori Kërkimor Detar i SHBA-së, dhe kodi i tij u publikua si softuer i lirë. [1]

5. PERSPEKTIVË PËR SIGURINË

Adresat onion janë vargje alfanumerike me 56 karaktere të gjeneruara kriptografikisht nga çifte çelësash publikë.

6. PERSPEKTIVË PËR SIGURINË

Nyjet e daljes mund të lexojnë trafikun në tekst të qartë, çka do të thotë se TLS/HTTPS kërkohet prapë në Tor për të dhënat e sigurta të seancës.

7. NJOHURI PËR SIGURINË

Faqet intranet, diskët cloud dhe bazat e të dhënave private përfaqësojnë segmentet më të mëdha të ruajtjes së të dhënave në deep web.

8. NJOHURI PËR SIGURINË

Motorë kërkimi të specializuar si DuckDuckGo operojnë portale onion për të lejuar kërkime anonime në rrjetet Tor.

9. NJOHURI PËR SIGURINË

Mbi 2 milionë përdorues lidhen çdo ditë me rrjetin Tor për të kapërcyer censurën dhe për të ruajtur privatësinë e komunikimit.

10. PERSPEKTIVË PËR SIGURINË

Operacionet globale të zbatimit të ligjit (si Operation Bayonet) mbyllën tregje kryesore të errëta duke konfiskuar harduerin e strehimit.

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] 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

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

1 **Indeksimi i kërkimit** WEB-I I THELLË **Përgjigjja e saktë: A**

SHËNIM PËR MËSUESIN

Faqet e web-it të thellë janë pas mureve të hyrjes me kyçje dhe pas bazave të të dhënave, duke i penguar robotët e kërkimit t'i eksplorojnë. Citim: IETF RFC 3986.

2 **Qasja në Tor** DARK WEB **Përgjigjja e saktë: A**

SHËNIM PËR MËSUESIN

Uebi i errët përbëhet nga shërbime të fshehura onion, të aksesueshme vetëm përmes shfletuesve si Tor. Citim: IETF RFC 3986.

3 **Baza të thella të dhënash** BAZA TË DHËNASH **Përgjigjja e saktë: A**

SHËNIM PËR MËSUESIN

Llogaritë e mbrojtura me fjalëkalim dhe të dhënat korporative përbëjnë segmentin më të madh të deep web. Citim: NIST Digital Identity.

4 **Rrugëzimi Onion** RRJETI TOR **Përgjigjja e saktë: A**

SHËNIM PËR MËSUESIN

Rrugëzimi onion i enkripton paketat e të dhënave në shtresa dhe i përcjell përmes disa nyjeve për anonimitet. Citim: IETF RFC 3986.

5 **Domen Onion** PRAPASHTESË **Përgjigjja e saktë: A**

SHËNIM PËR MËSUESIN

Prapashtesa kriptografike e domenit.onion e rrugëzon trafikun brenda Tor-it pa DNS publike. Citim: IETF RFC 3986.

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

6 **Segmentet e web-it** STRUKTURA — **Përgjigjja e saktë: E gabuar**

SHËNIM PËR MËSUESIN

Uebi i thellë mbulon të gjitha faqet e paindeksuara, ndërsa uebi i errët është një nënsegment i vogël onion i enkriptuar. Citim: IETF RFC 3986.

7 **Intranetet e korporatave** WEB-I I THELLË — **Përgjigjja e saktë: E vërtetë**

SHËNIM PËR MËSUESIN

Faqet intranet janë pas portaleve me fjalëkalim dhe nuk indeksohen, që do të thotë se i përkasin deep web-it. Citim: NIST Digital Identity.

8 **Enkriptimi me shtresa** RELE — **Përgjigjja e saktë: E gabuar**

SHËNIM PËR MËSUESIN

Releja onion e deshifrojnë vetëm një shtresë rrugëzimi për të mbrojtur anonimitetin e përdoruesit, kurrë paketën e plotë. Citim: IETF RFC 3986.

9 **Ekspozimi ndaj malware-it** KËRCËNIMET — **Përgjigjja e saktë: E vërtetë**

SHËNIM PËR MËSUESIN

Tregjet e web-it të errët nuk kanë filtrim sigurie dhe sjellin rreziqe ekstreme infektimi me malware. Citim: Center for Internet Security (CIS).

10 **Pyetja 10** — **Përgjigjja e saktë: E gabuar**

SHËNIM PËR MËSUESIN

Crawler-at e zakonshëm të motorëve të kërkimit nuk përdorin Tor, ndaj nuk mund t'i arrijnë ose t'i indeksojnë faqet .onion.

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

H 1. Segmenti i internetit të thellë	A 2. Portali i internetit të errët	D 3. Zgjerimi Onion	B 4. Drejtimi Tor
F 5. Faqet e indeksuara	G 6. Anonimiteti i përdoruesit	C 7. Bazë e dhënash private	E 8. Gateway-i i hyrjes

PIKA E KONTROLLIT 3: ÇELËSI – TERMAT KRYESORË

1 DEEP WEB	2 DARK WEB	3 ONION	4 RUTIM TOR
5 INDEKSUARA	6 ANONIMITET		

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

1 F – ANONIMITET	2 G – BAZËTËDHËNASH	3 D – RUTIMTOR	4 A – DEEPWEB
5 B – DARKWEB	6 C – SHTESAONION	7 H – NYJËHYRËSE	8 E – INDEKSUARA

SHËNIME PËR DISKUTIM PËR MËSUESIT

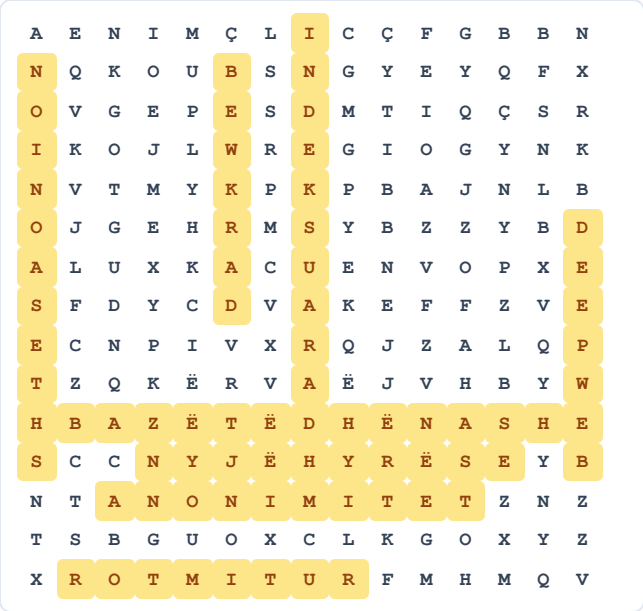
Termat kryesorë:
Kontrollo nëse nxënësit mund të shpjegojnë Segmenti i internetit të thellë, Portali i internetit të errët dhe Zgjerimi Onion me fjalët e tyre dhe të japin një shembull për secilin.

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

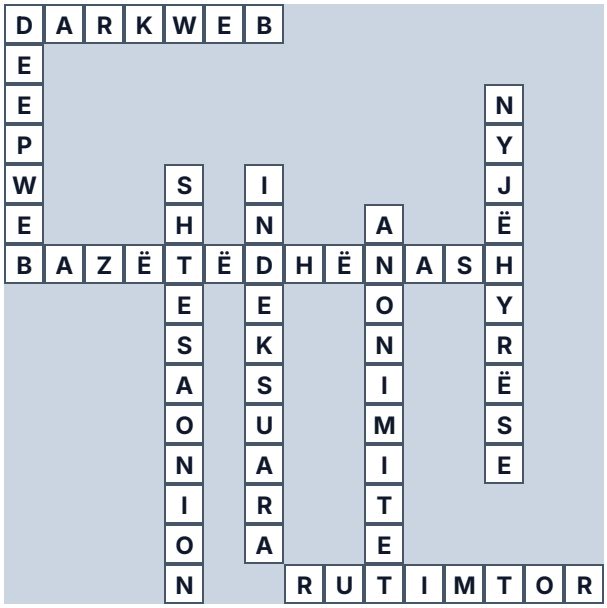
Vlerësimi i burimeve:
Kërkoju nxënësve të verifikojnë të paktën një pohim në burimet e fletës dhe diskutoni pse numrat, çmimet dhe rregullat mund të ndryshojnë me kalimin e kohës.

Çelësat e enigmave dhe shënimet për mësuesin

ZGJIDHJA E LOJËS ME FJALË



ZGJIDHJA E FJALËKRYQIT



UDHËZUES PËR MËSUESIN PËR ZGJIDHJET E KRYQËZËS

HORIZONTALISHT

1 horizontalisht: DARKWEB Segment i enkriptuar i rrjetit i qasshëm vetëm përmes shfletuesve të veçantë (7 shkronja)

6 horizontalisht: BAZËTËDHËNASH Ruajtje e sigurt e pjesës së prapme që strehon regjistrime sistemi të paindeksuara (13 shkronja)

7 horizontalisht: RUTIMTOR Enkriptimi i të dhënave në shtresa dhe përcjellja e tyre përmes tri nyjeve (8 shkronja)

VERTIKALISHT

1 vertikalisht: DEEPWEB Përmbajtje uebi e paindeksuar si hyrjet private, email-et dhe regjistrimet e bazave të të dhënave (7 shkronja)

2 vertikalisht: NYJËHYRËSE Nyja e hyrjes që përdoret për të hyrë në rrjetin Tor (10 shkronja)

3 vertikalisht: SHTESAONION Prapashtesë kriptografike e domenit të nivelit të lartë që përdoret në rrjetet Tor (11 shkronja)

4 vertikalisht: INDEKSUARA Përmbajtje e uebit të sipërfaqes e përpiluar dhe e kërkueshme në Google (10 shkronja)

5 vertikalisht: ANONIMITET Mbajtja e adresave publike IP të klientit të fshehura nga serverët (10 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.	PEDWBEE	DEEPWEB	5.	WBKRDEA	DARKWEB
2.	SNHSOATINOE	SHTESAONION	6.	ORITRMUT	RUTIMTOR
3.	ISRUNKAEAD	INDEKSUARA	7.	NNAIMTETIO	ANONIMITET
4.	ËSËZHTHDANBAË	BAZËTËDHËNASH	8.	SËYENHYRËJ	NYJËHYRËSE

ÇELËSI I SFIDËS SË KODIT TË FSHEHTË

"RUAJ ANONIMITETIN ME RUTIMIN E SIGURT ONION"

Çelësi i studimeve të rastit

A Studimi i rastit 1: Identifikimi i rrjedhjes së të dhënave

Zgjidhja për mësuesin

UDHËZUES VLERËSIMI

Përgjigjet e studentëve duhet të mbulojnë pikat e mëposhtme:

- Analiza e skenarit: Një auditim sigurie korporativ zbulon se regjistrime të ndjeshme të bazës së të dhënave të klientëve po tregtohen në një treg onion. Të dhënat nuk janë të indeksuara në Google.
- Strategjia dhe zgjidhja e rekomanduar: Segmentet e përfshira: Baza e të dhënave private i përket deep web (e paindeksuar por e sigurt). Tregu që tregton të dhënat e vjedhura është në dark web (rrjeti onion). Si ndodhi: Hakerat anashkaluan mbrojtjet e serverit, vodhën bazën e të dhënave nga deep web dhe e listuan në mënyrë anonime në dark web për t'i shpëtuar gjurmimit nga organet e zbatimit të ligjit.

B Studimi i rastit 2: Anonimiteti kundrejt rreziqeve të malware-it

Zgjidhja për mësuesin

UDHËZUES VLERËSIMI

Përgjigjet e studentëve duhet të mbulojnë pikat e mëposhtme:

- Analiza e skenarit: Një analist dëshiron të kontrollojë burimet e inteligjencës së kërcënimeve në një faqe Tor. Ai shkarkon shfletuesin Tor dhe hyn në faqe.
- Strategjia dhe zgjidhja e rekomanduar: Përfitimet: Tor e drejton trafikun përmes tre nyjeve, duke maskuar IP-në korporative të analistit. Rreziqet dhe zbutja: Lidhjet e dark web nuk kanë filtrim reputacioni. Analistët duhet ta ekzekutojnë Tor brenda makinave virtuale (VM) të izoluara, ta çaktivizojnë JavaScript në cilësimet e Tor dhe të shmangin shkarkimin e çdo skedari për të mbrojtur rrjetin korporativ.