Jméno: _____ Datum: _____ Body: _____

Temný web vs. hluboký web: bezpečnost a Rozdíly

Indexace ve vyhledávačích, databáze hlubokého webu, onion routing sítě Tor, anonymita v síti a rizika

PŘEHLED VÝUKY: DARK WEB VS DEEP WEB

ZABEZPEČENO
ŠIFROVÁNÍ DAT
Standard 256bitového AES

VYHOVUJÍCÍ
GLOBÁLNÍ STANDARDY
Rámce GDPR a CCPA

ZERO-TRUST
ZÁSADY PŘÍSTUPU
Vícefaktorové ověřování

Vítejte! Tento balíček aktivit vás provede rozdíly mezi deep webem a dark webem. Prozkoumáte neindexované databáze, onion routing prohlížeče Tor, kryptografické domény .onion a bezpečnostní rizika anonymity.

KONTROLNÍ BODY PRACOVNÍHO LISTU

- [ ] **Část 1-4: Zvládněte kyberbezpečnost a prevenci hrozeb.**
- [ ] **Část 5-7: Vyřešte křížovku a osmisměrku.**
- [ ] **Část 8-9: Vyřešte případové studie a šifrovací výzvu.**
- [ ] **Část 10: Projděte si stránky se základními i pokročilými FAQ.**
- [ ] **Část 11: Prozkoumejte 10 zajímavých faktů z praxe.**
- [ ] **Bonus: výzva Mysli rychle.**

Otevřete průvodce kyberbezpečností od VPN.com

URL: https://www.vpn.com/cs/kyberneticka-bezpecnost/dark-web-vs-deep-web/

Váš studijní plán: strategie pro deep a dark web

- Porovnejte deep web (neindexované databáze) s dark webem (onion služby).
- Pochopte, jak onion routing šifruje a předává síťový provoz.
- Vyhodnoťte bezpečnostní rizika přístupu na neověřené stránky sítě Tor.
- Nasaďte zásady zabezpečené brány a sandboxu pro procházení threat intelligence.
- Analyzujte kryptografický formát adres domén služeb onion.

POKYNY K PRŮVODCI DEEP A DARK WEBEM

Odpovězte na otázky s výběrem odpovědí a otázky pravda/nepravda, doplňte věty s vynechanými slovy pomocí banky slov, přiřaďte definice a vyřešte křížovku a osmisměrku. Uplatněte své znalosti na soukromí na deep webu a dark webu. Zakončete bonusovou aktivitou Mysli rychle.

DATABÁZE DEEP WEBU VS ONION SMĚROVÁNÍ DARK WEBU (ÚVOD)

Deep web tvoří neindexované stránky za hesly a přihlášeními, jako jsou soukromé e-maily nebo firemní bankovní portály. Dark web je podmnožina deep webu, která je skryta záměrně a k anonymnímu přístupu vyžaduje specializované prohlížeče (jako Tor) a onion sítě.

PŘEČTĚTE SI POZORNĚ KAŽDÝ KONTROLNÍ BOD A VYBERTE NEBO NAPIŠTE SPRÁVNOU ODPOVĚĎ.

Kontrolní bod 1: Výzva s výběrem odpovědí

1. Co odlišuje deep web od surface webu?

- A. Stránky deep webu nejsou indexovány veřejnými vyhledávači
- B. Provoz na deep webu je nelegální a sledovaný orgány činnými v trestním řízení
- C. Weby na deep webu vyžadují k přístupu specializované prohlížeče jako Tor
- D. Stránky deep webu se vždy načítají rychleji než stránky povrchového webu

2. Jak se přistupuje na dark web?

- A. Prostřednictvím specializovaných prohlížečů využívajících onion routing
- B. Konfigurací vlastních nastavení DNS na běžných routerech
- C. Přes soukromé vyhledávací konzole povrchového webu jen na pozvánku
- D. Instalací běžného rozšíření prohlížeče pro blokování reklam

3. Jaká struktura tvoří největší část deep webu?

- A. Heslem chráněné uživatelské databáze a soukromé účty
- B. Nelegální fóra černého trhu obchodující s nezákonným zbožím
- C. Nešifrované protokoly peer-to-peer sdílení souborů
- D. Veřejné databáze cache vyhledávačů

4. Co dělá Onion Routing se síťovým provozem?

- A. Šifruje pakety a směruje je přes několik relé
- B. Zvyšuje rychlost stahování obcházením uzlů ISP
- C. Mapuje sériová čísla hardwaru zařízení na IP záznamy
- D. Maže cookies prohlížeče po každém kliknutí

5. Jaká doménová koncovka se používá výhradně v sítích Tor?

- A. Kryptografická přípona nejvyšší úrovně .onion
- B. Standardní tradiční komerční koncovka .com
- C. Decentralizovaná blockchainová koncovka .eth ze světa Web3
- D. Národní technologická koncovka .ai

Kontrolní bod 2: Výzva Pravda/Nepravda

6 Otázka tf 6

6. Deep web a dark web označují tentýž segment sítě.

- ○ Pravda
- ○ Nepravda

7 Otázka tf 7

7. Firemní intranetové portály jsou součástí deep webu.

- ○ Pravda
- ○ Nepravda

8 Otázka tf 8

8. Onion routing zcela dešifruje datové pakety v každém tranzitním uzlu.

- ○ Pravda
- ○ Nepravda

9 Otázka tf 9

9. Přístup na dark web vystavuje zařízení vysokým rizikům malwaru.

- ○ Pravda
- ○ Nepravda

10 Otázka tf 10

10. Standardní webové vyhledávače procházejí a indexují onion weby.

- ○ Pravda
- ○ Nepravda

Kontrolní bod 3: Doplňování klíčových pojmů

Přečtěte si každou větu níže a doplňte do vynechaného místa správný termín ze slovní banky.

1. Soukromé bankovní portály se nacházejí v neindexované části internetu zvané _____ .

2. Skryté služby hostované na specializovaných uzlech Tor tvoří část sítě známou jako _____ .

3. Adresy webů v síti Tor končí kryptografickou koncovkou nejvyšší úrovně zvanou _____ .

4. Vícevrstvé šifrované vedení provozu sítí Tor se nazývá cibulové _____ .

5. Povrchové vyhledávače procházejí stránky, které jsou veřejně _____ .

6. Sítě onion šifrují IP adresy klientů, aby byla zachována uživatelská _____ .

ZÁSOBNÍK SLOV

ANONYMITA | DARK WEB | DATABÁZE | DEEP WEB | INDEXOVANÉ | ONION | SMĚROVÁNÍ | VSTUPNÍ UZEL

Sem napište své odpovědi:

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

Kontrolní bod 4: Přiřazování bezpečnostních pojmů

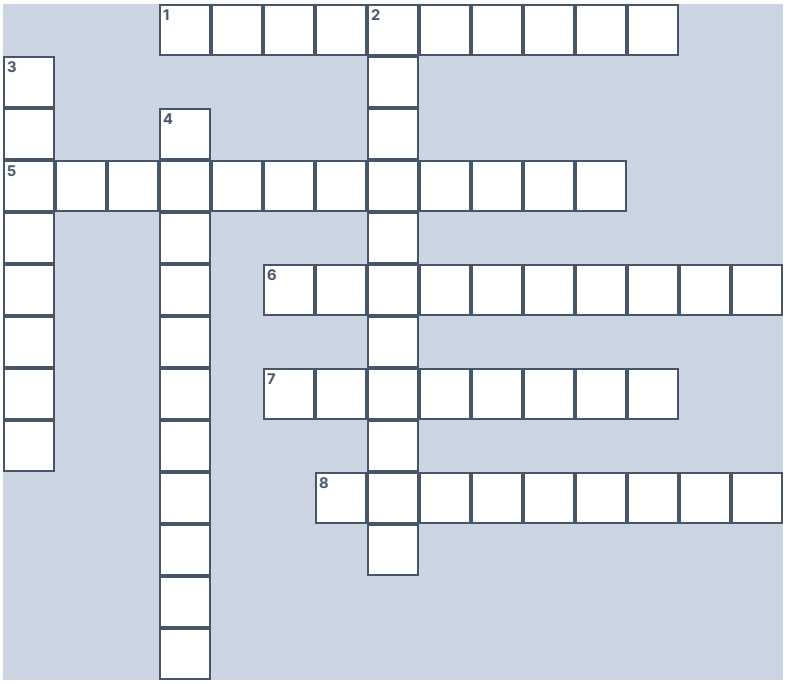
PŘIŘAZOVÁNÍ DEFINIC

Přiřaďte každý slovníčkový pojem vlevo k jeho správné definici vpravo zapsáním odpovídajícího písmene (A–H) do vyplnitelného pole.

☐	1. Segment hlubokého webu	A	Šifrovaný segment sítě přístupný pouze přes speciální prohlížeče.
☐	2. Portál dark webu	B	Šifrování dat ve vrstvách a jejich předávání přes tři uzly.
☐	3. Přípona onion	C	Zabezpečené backendové úložiště hostující neindexované systémové záznamy.
☐	4. Směrování přes Tor	D	Kryptografická přípona domény nejvyššího řádu používaná v sítích Tor.
☐	5. Indexované stránky	E	Vstupní uzel používaný pro přístup do sítě Tor.
☐	6. Anonymita uživatelů	F	Obsah povrchového webu shromážděný a vyhledatelný na Googlu.
☐	7. Soukromá databáze	G	Udržování veřejných IP adres klientů skrytých před servery.
☐	8. Vstupní brána	H	Neindexovaný webový obsah, jako jsou soukromá přihlášení, e-maily a databázové záznamy.

Kontrolní bod 5: Křížovka

Vyřešte křížovku zapisováním písmen do aktivních bílých políček. Čísla odpovídají nápovědám níže.



VODOROVNÉ NÁPOVĚDY

1. Neindexovaný webový obsah jako soukromá přihlášení, e-maily a databázové záznamy (10)

5. Šifrování dat ve vrstvách a jejich předávání přes tři uzly (12)

6. Obsah povrchového webu shromážděný a vyhledatelný na Googlu (10)

7. Šifrovaný segment sítě přístupný pouze přes speciální prohlížeče (8)

8. Udržování veřejných IP adres klientů skrytých před servery (9)

SVISLÉ NÁPOVĚDY

2. Kryptografická přípona domény nejvyšší úrovně používaná v sítích Tor (11)

3. Zabezpečené backendové úložiště hostící neindexované systémové záznamy (8)

4. Vstupní bod používaný pro přístup do sítě Tor (11)

Kontrolní bod 5, alternativa: Přístupná zadání křížovky

Uživatelé čteček obrazovky a klávesnice mohou odpovědi křížovky zapisovat přímo do textových polí níže.

VODOROVNÉ NÁPOVĚDY

1 vodorovně: Neindexovaný webový obsah jako soukromá přihlášení, e-maily a databázové záznamy (10 písmen):

5 vodorovně: Šifrování dat ve vrstvách a jejich předávání přes tři uzly (12 písmen):

6 vodorovně: Obsah povrchového webu shromážděný a vyhledatelný na Googlu (10 písmen):

7 vodorovně: Šifrovaný segment sítě přístupný pouze přes speciální prohlížeče (8 písmen):

8 vodorovně: Udržování veřejných IP adres klientů skrytých před servery (9 písmen):

SVISLÉ NÁPOVĚDY

2 svisle: Kryptografická přípona domény nejvyšší úrovně používaná v sítích Tor (11 písmen):

3 svisle: Zabezpečené backendové úložiště hostící neindexované systémové záznamy (8 písmen):

4 svisle: Vstupní bod používaný pro přístup do sítě Tor (11 písmen):

Kontrolní bod 6: Hledání skrytých slov

Najděte 8 klíčových pojmů skrytých v mřížce níže. Slova mohou být vodorovně, svisle nebo úhlopříčně.

K Ď L Ř Ň J A H Ě P K O Č Ň C
A D G I B Á P L S M Q V U I Ý
N Ě Z Š F Y W U H É S U Ó Ú K
É S D Ť T M Q B L Ň T H K Q H
M Z P M W Ú O O Ý Ř Ř Á Á V M
O Q Ň Á L I É K Í O Ý B Ž S D
D Ž Z B Ň Ů Y Ý N Č É P X T A
N R R Y G Ď Z W C W M E F U T
O G Ž W Č P Ř E J X Y S L P A
I Ž A Ň S Ž S B N F T W Ě N B
N T O R S M Ě R O V Á N Í Í Á
O M X A N O N Y M I T A J U Z
B Ý I N D E X O V A N É Č Z E
C Ý Ó Ů Ž P Ž Ú U B H V Q E Y
Č B E W Ý N M E T Ň N H Q L X

SEZNAM SLOV

HLUBOKÝWEB
TEMNÝWEB
ONIONDOMÉNA
TORSMĚROVÁNÍ
INDEXOVANÉ
ANONYMITA
DATABÁZE
VSTUPNÍUZEL

Kontrolní bod 6, alternativa: Přístupné přiřazování slovíček

Přiřaďte každý z 8 slovníčkových pojmů z osmisměrky k jeho správné definici zapsáním písmene (A–H) do prázdného pole.

POJMY SLOVNÍ ZÁSOBY

- **A. HLUBOKÝWEB**
- **B. TEMNÝWEB**
- **C. ONIONDOMÉNA**
- **D. TORSMĚROVÁNÍ**
- **E. INDEXOVANÉ**
- **F. ANONYMITA**
- **G. DATABÁZE**
- **H. VSTUPNÍUZEL**

DEFINICE A POLE K PŘIŘAZENÍ

1. Udržování veřejných IP adres klientů skrytých před servery.
2. Zabezpečené backendové úložiště hostící neindexované systémové záznamy.
3. Šifrování dat ve vrstvách a jejich předávání přes tři uzly.
4. Neindexovaný webový obsah jako soukromá přihlášení, e-maily a databázové záznamy.
5. Šifrovaný segment sítě přístupný pouze přes speciální prohlížeče.
6. Kryptografická přípona domény nejvyšší úrovně používaná v sítích Tor.
7. Vstupní bod používaný pro přístup do sítě Tor.
8. Obsah povrchového webu shromážděný a vyhledatelný na Googlu.

Kontrolní bod 7: Výzva s přeházenými slovy

Přeuspořádejte písmena níže a odhalte klíčové pojmy a termíny kybernetické bezpečnosti. Odpovědi pište do připravených polí.

1. EÝKOLHWBBU
2. NANONDIÉMOO
3. IONVNXÉEAD
4. AZEÁBDAT
5. ÝWEBNTEM
6. ÍMVÁĚNOTORRS
7. MATAINNYO
8. ZÍLNTVPSEUU

Bonusová aktivita: Mysli rychle

3 ODPOVĚDI V KAŽDÉ KATEGORII. VYHRÁVÁ, KDO PRVNÍ VYPLNÍ CELÝ SEZNAM.

1	Důvody, proč se dark webu vyhýbat			
2	Věci, které vyhledávač nenajde			
3	Zařízení, která lze hacknout			
4	Legální důvody pro používání Toru			
5	Důvody, proč aktualizovat software			
6	Varovné signály v e-mailu			
7	Věci, které se nelegálně prodávají na dark webu			
8	Lidé, které můžete požádat o pomoc s IT			
9	Bezpečné návyky, se kterými můžete začít už dnes			
10	Co udělat po úniku dat			
11	Věci, které patří do deep webu			
12	Weby, které používáte s přihlášením			
13	Slova související s anonymitou			
14	Informace, které byste nikdy neměli sdílet			
15	Věci, které leží „pod povrchem“			

Kontrolní bod 8: Případové studie kyberbezpečnosti

Použijte naučené koncepty k vyřešení níže uvedených reálných scénářů.

PŘÍPADOVÁ STUDIE 1: IDENTIFIKACE ÚNIKU DAT



Scénář: Firemní bezpečnostní audit zjistí, že citlivé záznamy klientské databáze se obchodují na onion tržišti. Data nejsou indexována na Googlu.

Otázka k diskusi: Vysvětlete, kterých segmentů webu se to týká a jak k tomuto úniku došlo.

PŘÍPADOVÁ STUDIE 2: ANONYMITA VS. RIZIKA MALWARU



Scénář: Analytik chce zkontrolovat zdroje threat intelligence na webu v síti Tor. Stáhne si prohlížeč Tor a web otevře.

Otázka k diskusi: Vyhodnoťte přínosy anonymity a nastíněte kroky ke zmírnění rizika malwaru.

Kontrolní bod 9: Dešifrování šifry

Profesionál v kyberbezpečnosti chrání síťová aktiva před online útočníky. Pomocí níže uvedeného klíče písmeno–číslo dešifrujte zprávu zapsáním odpovídajících písmen do prázdných polí.

ŠIFROVACÍ KLÍČ PÍSMENO–ČÍSLO

A=1 Á=2 B=3 C=4 Č=5 D=6 Ď=7 E=8 É=9 Ě=10 F=11 G=12 H=13 I=14
Í=15 J=16 K=17 L=18 M=19 N=20 Ň=21 O=22 Ó=23 P=24 Q=25 R=26 Ř=27 S=28
Š=29 T=30 Ť=31 U=32 Ú=33 Ů=34 V=35 W=36 X=37 Y=38 Ý=39 Z=40 Ž=41

40	1	4	13	22	35	8	16	30	8		1	20	22	20	38	19	14	30	32
4	14	3	32	18	22	35	39	19		28	19	10	26	22	35	2	20	15	19

Dešifrovaná zpráva:

TIP: KAŽDÉ ČÍSLO PŘEDSTAVUJE POZICI DANÉHO PÍSMENE V ABECEDĚ (NAPŘ. 1 = A, 2 = B, 41 = Ž).

Kontrolní bod 10: Základní časté otázky ke kyberbezpečnosti (část A)

Projděte si časté otázky a odpovědi ohledně zmírňování online hrozeb.

Q1: Co je deep web?

Deep web tvoří všechny webové stránky, které vyhledávače nemohou indexovat, včetně internetového bankovnictví, e-mailových databází a odborných časopisů za paywallem.

Q2: Co je dark web?

Dark web je malá podmnožina deep webu, záměrně skrytá a dostupná jen prostřednictvím specializovaných prohlížečů využívajících onion sítě.

Q3: Jak vyhledávače indexují stránky?

Vyhledávače spouštějí automatizované programy (roboty), které sledují veřejné odkazy a indexují stránky, jež procházení neblokují direktivami pro roboty.

Q4: Proč se internetové bankovnictví považuje za součást deep webu?

Bankovní portály jsou za přihlašovacími stěnami a hesly, což veřejným vyhledávačům brání indexovat stránky s výpisy z účtů.

Q5: Co je Onion Routing v prohlížeči Tor?

Onion routing je metoda přenosu, která šifruje provoz ve vrstvách a posílá jej přes více uzlů, aby zamaskovala IP adresy uživatelů.

Kontrolní bod 10: Základní časté otázky ke kyberbezpečnosti (část B)

Projděte si časté otázky a odpovědi ohledně zmírňování online hrozeb.

Q6: Je přístup na dark web nezákonný?

Ne. Přístup na dark web je ve většině zemí legální, zapojení do nelegálních tržišť či kybernetických aktivit je však zakázané.

Q7: Proč se stránky dark webu načítají pomalu?

Provoz je směrován a dešifrován přes nejméně tři globální relé (vstupní, prostřední, výstupní), což zvyšuje latenci přenosu.

Q8: Co znamená doménová koncovka .onion?

Je to specializovaná doménová přípona nejvyššího řádu používaná v sítích Tor, odkazující na kryptograficky generované adresy místo standardních DNS serverů.

Q9: Jaká rizika jsou spojena s odkazy na dark webu?

Weby nemají žádnou bezpečnostní kontrolu, což uživatele vystavuje vysoké míře malwarových infekcí, phishingovým skriptům a transakčním podvodům.

Q10: Kdo vytvořil směrovací protokol sítě Tor?

Technologii původně vyvinula americká Naval Research Laboratory v letech po roce 1990 k ochraně vládní komunikace.

Kontrolní bod 10: Pokročilé časté otázky k bezpečnosti (část C)

Prozkoumejte pokročilé technické aspekty bezpečnostních rámců, analýzy malwaru a datové compliance.

Q1: Jak prostřední uzly chrání anonymitu Toru?

Každý uzel dešifruje jen jednu vrstvu směrovacích dat a zná pouze předchozí a následující skok, nikdy zdroj i cíl zároveň.

Q2: Jaká je role výstupního uzlu?

Výstupní uzel dešifruje poslední vrstvu šifrování a odesílá provoz na veřejný cílový server nebo onion server.

Q3: Co je brána Tor bridges?

Bridge jsou neveřejné vstupní relaye Toru používané k obcházení blokací ISP a cenzury v regionech omezujících přístup k prohlížeči Tor.

Q4: Jak aktéři dark webu zneužívají kryptoměny?

Aktéři používají anonymní kryptoměny k provádění finančních obchodů na temných tržištích a vyhýbají se standardním bankovním kontrolám transakcí.

Q5: Proč běžné vyhledávače nedokážou procházet hluboké databáze?

Crawlery nedokážou zadávat přihlašovací údaje, řešit bezpečnostní CAPTCHA ani spouštět backendové SQL dotazy potřebné k přístupu do hlubokých databází.

Kontrolní bod 10: Pokročilé časté otázky k bezpečnosti (část D)

Prozkoumejte pokročilé technické aspekty bezpečnostních rámců, analýzy malwaru a datové compliance.

Q6: Co je adresářový server v sítích Tor?

Je to důvěryhodný server udržující seznam aktivních vstupních, prostředních a výstupních relé, které klienti používají k sestavování směrovacích cest.

Q7: Jak zlomyslní aktéři odposlouchávají výstupní uzly?

Provozovatelé zákeřných výstupních uzlů mohou zachytávat nešifrovaný HTTP provoz opouštějící síť Tor a krást uživatelská jména a cookies.

Q8: Jaký je rozdíl mezi Torem a I2P?

Tor používá centralizovaný adresář relé a výstupní uzly pro přístup k veřejnému webu, zatímco I2P používá decentralizovanou peer-to-peer strukturu pro interní hostování.

Q9: Jak orgány činné v trestním řízení sledují tržiště na dark webu?

Agentury využívají analýzu blockchainu, lokalizují fyzická serverová hostingová řešení a provádějí klamné operace k identifikaci operátorů.

Q10: Jak únik DNS ohrožuje anonymitu klienta?

K únikům DNS dochází, když jsou dotazy DNS prohlížeče odesílány přímo přes místního ISP, místo aby byly směrovány přes šifrovanou síť Tor.

Část 11: 10 faktů a poznatků o kyberbezpečnosti z praxe

Projděte si fakta z praxe o bezpečnostních incidentech, obranných mechanismech a standardech souladu.

1. BEZPEČNOSTNÍ POSTŘEH

Deep web je mnohem větší než prohledávatelný povrchový web, protože většina obsahu je za přihlášeními a v databázích.

2. BEZPEČNOSTNÍ POSTŘEH

Dark web je malá, záměrně skrytá část deep webu, dostupná nástroji jako Tor.

3. BEZPEČNOSTNÍ POSTŘEH

Směrování Tor šifruje datové pakety třikrát a na každém relay uzlu odlupuje vrstvy šifrování jako u cibule.

4. BEZPEČNOSTNÍ POSTŘEH

Tor vzešel z projektu onion routingu americké Naval Research Lab a jeho kód byl uvolněn jako svobodný software. [1]

5. BEZPEČNOSTNÍ POSTŘEH

Onion adresy jsou 56znakové alfanumerické řetězce generované kryptograficky z párů veřejných klíčů.

6. BEZPEČNOSTNÍ POSTŘEH

Výstupní uzly mohou číst nešifrovaný provoz, takže TLS/HTTPS je na Toru pro zabezpečení relací stále nutné.

7. POSTŘEH K BEZPEČNOSTI

Intranetové weby, cloudové disky a soukromé databáze představují největší segmenty ukládání dat na deep webu.

8. POSTŘEH K BEZPEČNOSTI

Specializované vyhledávače jako DuckDuckGo provozují onion portály umožňující anonymní vyhledávání v sítích Tor.

9. POSTŘEH K BEZPEČNOSTI

Přes 2 miliony uživatelů se denně připojují k síti Tor, aby obešli cenzuru a udrželi soukromí komunikace.

10. BEZPEČNOSTNÍ POSTŘEH

Globální operace orgánů činných v trestním řízení (jako operace Bayonet) uzavřely velká temná tržiště zabavením hostingového hardwaru.

Technické reference a zdroje

Studijní příručka a interaktivní hádanky jsou sestaveny z globálních standardů NIST, OWASP a předpisů o ochraně osobních údajů.

AKADEMICKÉ A OBOROVÉ REFERENCE

[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

Klíč odpovědí: Kontrolní bod 1 - Výběr z možností

1 **Indexace vyhledávání** DEEP WEB — Správná odpověď: A

POZNÁMKA PRO VYUČUJÍCÍ

Stránky hlubokého webu jsou za přihlašovacími stěnami a databázemi, což brání vyhledávacím robotům v jejich procházení.

2 **Přístup k Toru** DARK WEB — Správná odpověď: A

POZNÁMKA PRO VYUČUJÍCÍ

Dark web tvoří skryté onion služby dostupné pouze prohlížeči jako Tor.

3 **Hluboké databáze** DATABÁZE — Správná odpověď: A

POZNÁMKA PRO VYUČUJÍCÍ

Heslem chráněné účty a firemní záznamy tvoří největší segment deep webu.

4 **Onion routing** SÍŤ TOR — Správná odpověď: A

POZNÁMKA PRO VYUČUJÍCÍ

Onion routing šifruje datové pakety ve vrstvách a předává je přes více uzlů kvůli anonymitě.

5 **Doména onion** PŘÍPONA — Správná odpověď: A

POZNÁMKA PRO VYUČUJÍCÍ

Kryptografická doménová přípona.onion směruje provoz interně v síti Tor bez veřejného DNS.

Klíč odpovědí: Kontrolní bod 2 - Pravda, nebo nepravda

6 **Webové segmenty** STRUKTURA — **Správná odpověď: Nepravda**

POZNÁMKA PRO VYUČUJÍCÍ

Deep web pokrývá všechny neindexované stránky, zatímco dark web je malý šifrovaný onion podsegment.

7 **Firemní intranety** DEEP WEB — **Správná odpověď: Pravda**

POZNÁMKA PRO VYUČUJÍCÍ

Intranetové weby jsou za heslovými portály a nejsou indexovány, což znamená, že patří do deep webu.

8 **Vrstvené šifrování** RELAYE — **Správná odpověď: Nepravda**

POZNÁMKA PRO VYUČUJÍCÍ

Onion uzly dešifrují pouze jednu směrovací vrstvu, aby chránily anonymitu uživatele, nikdy celý paket.

9 **Vystavení malwaru** HROZBY — **Správná odpověď: Pravda**

POZNÁMKA PRO VYUČUJÍCÍ

Tržiště na temném webu nemají žádné bezpečnostní filtrování a nesou extrémní riziko nákazy malwarem.

10 **Otázka 10** — **Správná odpověď: Nepravda**

POZNÁMKA PRO VYUČUJÍCÍ

Běžné crawlery vyhledávačů nepoužívají Tor, takže se k webům .onion nedostanou ani je nemohou indexovat.

Klíče slovní zásoby a hodnoticí rubrika

Hodnoticí rubrika pro vyučující: Udělte 1 bod za každé správné přiřazení (celkem 8 bodů) a kontextový termín (celkem 6 bodů).

KONTROLNÍ BOD 4: KLÍČ K PŘIŘAZOVÁNÍ POJMŮ

H 1. Segment hlubokého webu	A 2. Portál dark webu	D 3. Přípona onion	B 4. Směrování přes Tor
F 5. Indexované stránky	G 6. Anonymita uživatelů	C 7. Soukromá databáze	E 8. Vstupní brána

KONTROLNÍ BOD 3: KLÍČ KE KLÍČOVÝM POJMŮM

1 DEEP WEB	2 DARK WEB	3 ONION	4 SMĚROVÁNÍ
5 INDEXOVANÉ	6 ANONYMITA		

KONTROLNÍ BOD 6, ALTERNATIVA: KLÍČ K PŘIŘAZOVÁNÍ SLOV

1 F – ANONYMITA	2 G – DATABÁZE	3 D – TORSMĚROVÁNÍ	4 A – HLUBOKÝWEB
5 B – TEMNÝWEB	6 C – ONIONDOMÉNA	7 H – VSTUPNÍUZEL	8 E – INDEXOVANÉ

POZNÁMKY K DISKUSI PRO VYUČUJÍCÍ

Klíčové pojmy:
Ověřte, že studenti umí vlastními slovy vysvětlit pojmy Segment hlubokého webu, Portál dark webu a Přípona onion a ke každému uvést příklad.

Případové studie:
Požádejte studenty, aby svá doporučení zdůvodnili fakty z pracovního listu, nikoli domněnkami.

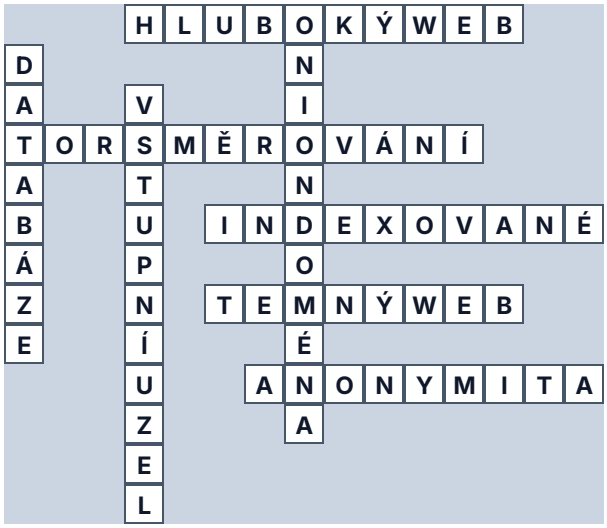
Práce se zdroji:
Nechte studenty ověřit alespoň jedno tvrzení proti referencím v pracovním listu a proberte, proč se čísla, ceny a pravidla mohou v čase měnit.

Klíče k úlohám a poznámky pro vyučující

ŘEŠENÍ OSMISMĚRKY

K	Ď	L	Ř	Ň	J	A	H	Ě	P	K	O	Č	Ň	C
A	D	G	I	B	Á	P	L	S	M	Q	V	U	I	Ý
N	Ě	Z	Š	F	Y	W	U	H	É	S	U	Ó	Ú	K
É	S	D	Ť	T	M	Q	B	L	Ň	T	H	K	Q	H
M	Z	P	M	W	Ú	O	O	Ý	Ř	Ř	Á	Á	V	M
O	Q	Ň	Á	L	I	É	K	Í	O	Ý	B	Ž	S	D
D	Ž	Z	B	Ň	Ů	Y	Ý	N	Č	É	P	X	T	A
N	R	R	Y	G	Ď	Z	W	C	W	M	E	F	U	T
O	G	Ž	W	Č	P	Ř	E	J	X	Y	S	L	P	A
I	Ž	A	Ň	S	Ž	S	B	N	F	T	W	Ě	N	B
N	T	O	R	S	M	Ě	R	O	V	Á	N	Í	Í	Á
O	M	X	A	N	O	N	Y	M	I	T	A	J	U	Z
B	Ý	I	N	D	E	X	O	V	A	N	É	Č	Z	E
C	Ý	Ó	Ů	Ž	P	Ž	Ú	U	B	H	V	Q	E	Y
Č	B	E	W	Ý	N	M	E	T	Ň	N	H	Q	L	X

ŘEŠENÍ KŘÍŽOVKY



PRŮVODCE PRO VYUČUJÍCÍ K ŘEŠENÍ KŘÍŽOVKY

VODOROVNÉ NÁPOVĚDY

1 vodorovně: HLUBOKÝWEB Neindexovaný webový obsah jako soukromá přihlášení, e-maily a databázové záznamy (10 písmen)

5 vodorovně: TORSMĚROVÁNÍ Šifrování dat ve vrstvách a jejich předávání přes tři uzly (12 písmen)

6 vodorovně: INDEXOVANÉ Obsah povrchového webu shromážděný a vyhledatelný na Googlu (10 písmen)

7 vodorovně: TEMNÝWEB Šifrovaný segment sítě přístupný pouze přes speciální prohlížeče (8 písmen)

8 vodorovně: ANONYMITA Udržování veřejných IP adres klientů skrytých před servery (9 písmen)

SVISLÉ NÁPOVĚDY

2 svisle: ONIONDOMÉNA Kryptografická přípona domény nejvyšší úrovně používaná v sítích Tor (11 písmen)

3 svisle: DATABÁZE Zabezpečené backendové úložiště hostící neindexované systémové záznamy (8 písmen)

4 svisle: VSTUPNÍUZEL Vstupní bod používaný pro přístup do sítě Tor (11 písmen)

Klíč řešení přesmyček a šifry

Klíč k hodnocení aktivity s přesmyčkami slovní zásoby a výzvy Tajná šifra.

KLÍČ K PŘESMYČKÁM

1. E Ý K O L H W B B U — **HLUBOKÝWEB**
2. N A N O N D I É M O O — **ONIONDOMÉNA**
3. I O N V N X É E A D — **INDEXOVANÉ**
4. A Z E Á B D A T — **DATABÁZE**
5. Ý W E B N T E M — **TEMNÝWEB**
6. Í M V Á Ě N O T O R R S — **TORSMĚROVÁNÍ**
7. M A T A I N N Y O — **ANONYMITA**
8. Z Í L N T V P S E U U — **VSTUPNÍUZEL**

KLÍČ TAJNÉ ŠIFROVACÍ VÝZVY

"ZACHOVEJTE ANONYMITU CIBULOVÝM SMĚROVÁNÍM"

Klíč k případovým studiím

A Případová studie 1: Identifikace úniku dat

Řešení pro vyučující

POKYNY K HODNOCENÍ

Odpovědi studentů by měly pokrýt následující body:

- Analýza scénáře: Firemní bezpečnostní audit zjistí, že citlivé záznamy klientské databáze se obchodují na onion tržišti. Data nejsou indexována na Googlu.
- Doporučená strategie a řešení: Dotčené segmenty: Soukromá databáze patří do deep webu (neindexovaná, ale zabezpečená). Tržiště obchodující s ukradenými daty je na dark webu (síť onion). Jak k tomu došlo: Hackeři obešli obranu serveru, ukradli databázi z deep webu a anonymně ji nabídli na dark webu, aby unikli sledování orgány činnými v trestním řízení.

B Případová studie 2: Anonymita vs. rizika malwaru

Řešení pro vyučující

POKYNY K HODNOCENÍ

Odpovědi studentů by měly pokrýt následující body:

- Analýza scénáře: Analytik chce zkontrolovat threat intelligence kanály na webu v síti Tor. Stáhne prohlížeč Tor a na web přistoupí.
- Doporučená strategie a řešení: Přínosy: Tor směruje provoz přes tři uzly a maskuje firemní IP analytika. Rizika a zmírnění: Odkazy na dark webu neprocházejí žádným reputačním prověřením. Analytici musí spouštět Tor v izolovaných virtuálních strojích (VM), vypnout Javascript v nastavení Toru a nestahovat žádné soubory, aby ochránili firemní síť.