Jméno: _____ **Datum:** _____ **Body:** _____

Zabezpečení veřejné Wi-Fi a šifrování

Útoky man-in-the-middle, podvržené přístupové body, odposlech paketů, VPN tunely a šifrování HTTPS.

PŘEHLED VÝUKY: ZABEZPEČENÍ VEŘEJNÉ WI-FI

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 zabezpečením veřejných Wi-Fi. Prozkoumáte nešifrované sítě, útoky man-in-the-middle (MitM), falešné přístupové body, odposlech paketů, VPN tunely a zabezpečení přenosu HTTPS.

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/bezpecnost-verejne-wifi/

Váš studijní plán: bezpečnost na veřejné Wi-Fi

- Určete běžná rizika veřejné Wi-Fi včetně odchytávání paketů a podvodných přístupových bodů.
- Zavést šifrovací tunely VPN k zabezpečení dat při přenosu.
- Vynuťte HTTPS a zabezpečená nastavení webového prohlížeče pro vzdálené pracovníky.

POKYNY K PRŮVODCI ZABEZPEČENÍM VEŘEJNÉ WI-FI

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 zabezpečení vzdáleného přístupu. Zakončete bonusovou aktivitou Mysli rychle.

ZABEZPEČENÍ VEŘEJNÉ WI-FI A OCHRANA PŘI PŘENOSU (ÚVOD)

Nešifrované veřejné Wi-Fi hotspoty nechávají síťový provoz vystavený odposlechu paketů a podvržení Evil Twin. Vynucení provozu přes zabezpečené šifrované VPN tunely a vynucení pravidel HSTS pouze pro HTTPS chrání relace před zachycením v místní síti.

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

Kontrolní bod 1: Výzva s výběrem odpovědí

1 **1. Co je útok Man-in-the-Middle (MitM)?**

- A. Zachycování a pozměňování komunikace mezi dvěma stranami ve sdílené síti
- B. Technika extrakce dat z databáze cílící na uživatelské záznamy
- C. Zahlcování webových serverů požadavky síťového provozu
- D. Vymazání svazků místního pevného disku

2 **2. Co je falešný přístupový bod (Evil Twin)?**

- A. Škodlivý Wi-Fi hotspot nakonfigurovaný se stejným SSID jako legitimní síť
- B. Administrativní nástroj používaný ke sledování záloh databáze
- C. Konfigurace zabezpečené VPN brány
- D. DNS záznam mapující autorizované poštovní servery

3 **3. Jak VPN chrání provoz na veřejné Wi-Fi?**

- A. Balí všechny síťové pakety do šifrovaného tunelu, takže jsou pro sniffery nečitelné
- B. Automaticky blokuje všechny příchozí požadavky na připojení
- C. Mění MAC adresu fyzické síťové karty
- D. Maže kešované cookies ve webovém prohlížeči

4 **4. Co je odposlech paketů (packet sniffing)?**

- A. Použití hardwarových nebo softwarových nástrojů k zachycování a zaznamenávání síťových paketů
- B. Skenování místních adresářů kvůli duplicitním souborům
- C. Omezení práv ke čtení databáze podle rolí uživatelů
- D. Šifrování úložných disků klíči AES-256

5 **5. Jaká je role HTTPS?**

- A. Šifrování provozu relace mezi prohlížečem a webovým serverem
- B. Filtrování příchozích e-mailových zpráv na bráně
- C. Komprese obrázků pro rychlejší načítání stránek
- D. Správa souborových struktur v síťovém úložišti (NAS)

Kontrolní bod 2: Výzva Pravda/Nepravda

6 Otázka 6

6. Připojení uživatelé mohou na otevřených veřejných Wi-Fi sítích snadno zachytávat data v prostém textu.

○ Pravda ○ Nepravda

7 Otázka 7

7. Falešné přístupové body (Evil Twins) jsou vždy autorizovány správci sítě.

○ Pravda ○ Nepravda

8 Otázka 8

8. VPN je neúčinná při ochraně provozu proti odposlechu paketů ve veřejných sítích.

○ Pravda ○ Nepravda

9 Otázka 9

9. HTTPS šifruje pouze cestu URL a obsah paketu nechává v otevřeném textu.

○ Pravda ○ Nepravda

10 Otázka 10

10. Wi-Fi hotspoty se zabezpečením WPA3 nabízejí silnější ochranu než otevřené sítě bez hesla.

○ Pravda ○ Nepravda

Kontrolní bod 3: Doplňování klíčových pojmů

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

1. Zachytávání soukromých hesel na veřejné Wi-Fi se označuje jako _____ komunikace.

2. Analýza surových paketů v místní síti se nazývá paketový _____ .

3. Falešný hotspot napodobující hotelovou Wi-Fi se nazývá _____ .

4. Bezpečný přenos webového provozu vyžaduje šifrování protokolem _____ .

5. Veškerý odchozí síťový provoz zašifruje klientská _____ .

6. Šifrovanou komunikační cestou skrz veřejné sítě je _____ .

ZÁSOBNÍK SLOV

EVIL TWIN | FIREWALL | HTTPS | ODPOSLECH | SNIFFING | TUNEL | VPN | WPA3

Sem napište své odpovědi:

1. | **2.**

3. | **4.**

5. | **6.**

Kontrolní bod 4: Přiřazování bezpečnostních pojmů

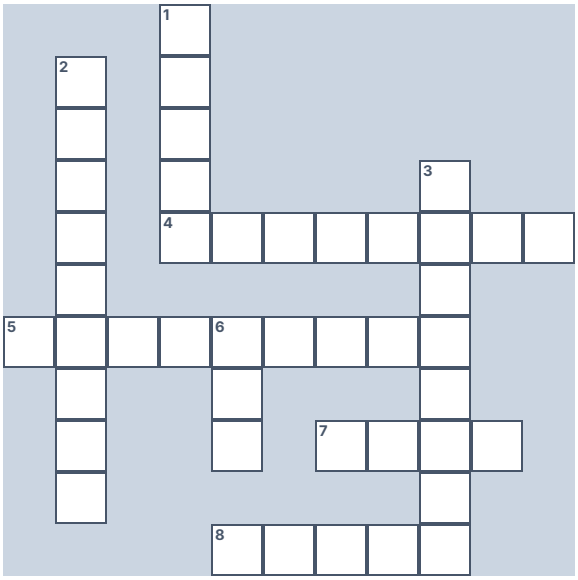
PŘIŘAZOVÁNÍ DEFINIC

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

☐	1. ODPOSLECH	A	Moderní bezpečnostní standard Wi-Fi.
☐	2. SNIFFING	B	Zabezpečená datová cesta při přenosu.
☐	3. EVIL TWIN	C	Filtrování příchozího provozu.
☐	4. HTTPS	D	Falešný hotspot napodobující Wi-Fi.
☐	5. VPN	E	Čtení provozu při přenosu.
☐	6. TUNEL	F	Zachytávání síťových datových paketů.
☐	7. WPA3	G	Šifrovaná virtuální privátní síť.
☐	8. FIREWALL	H	Zabezpečený webový přenos.

Kontrolní bod 5: Křížovka

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



VODOROVNÉ NÁPOVĚDY

4. Zachytávání síťových datových paketů. (8)

5. Falešný hotspot napodobující Wi-Fi. (9)

7. Moderní standard zabezpečení Wi-Fi. (4)

8. Zabezpečená datová cesta při přenosu. (5)

SVISLÉ NÁPOVĚDY

1. Zabezpečený webový přenos. (5)

2. Čtení provozu během přenosu. (9)

3. Filtrování příchozího provozu. (8)

6. Šifrovaná virtuální privátní síť. (3)

Kontrolní bod 5, alternativa: Přístupná zadání křížovky

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

VODOROVNÉ NÁPOVĚDY

4 vodorovně: Zachytávání síťových datových paketů. (8 písmen):

5 vodorovně: Falešný hotspot napodobující Wi-Fi. (9 písmen):

7 vodorovně: Moderní standard zabezpečení Wi-Fi. (4 písmen):

8 vodorovně: Zabezpečená datová cesta při přenosu. (5 písmen):

SVISLÉ NÁPOVĚDY

1 svisle: Zabezpečený webový přenos. (5 písmen):

2 svisle: Čtení provozu během přenosu. (9 písmen):

3 svisle: Filtrování příchozího provozu. (8 písmen):

6 svisle: Šifrovaná virtuální privátní síť. (3 písmen):

Kontrolní bod 6: Hledání skrytých slov

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

Č	Š	I	Ě	O	S	N	H	R	Y	R	Ó	Č	U	T
Ť	E	L	Í	B	A	B	T	C	P	T	Y	L	J	Y
L	Y	3	U	K	Ď	Ř	T	N	J	U	D	I	O	Ň
E	K	A	R	Q	F	Ň	P	Ň	Ř	N	S	T	U	Ť
Č	F	P	C	T	O	R	S	Ó	H	E	Š	B	S	V
J	D	W	T	Z	D	Ů	C	Ž	V	L	Ě	K	N	G
O	Ž	D	Ň	Ď	P	Ř	X	F	Q	C	Ú	B	I	A
V	Ž	O	D	L	O	A	Ď	I	Ó	Ď	É	G	F	I
D	D	S	Ř	N	S	E	I	R	Š	Ž	T	É	F	Ř
É	Ů	E	A	Á	L	V	Ř	E	P	O	Q	U	I	Y
L	R	J	S	U	E	P	Š	W	Č	Ň	Ý	B	N	Ě
Z	Š	X	W	Í	C	N	A	A	S	Ž	Ý	Ý	G	L
F	I	N	S	J	H	N	M	L	Ť	P	G	R	Ř	G
Ž	Á	Ó	Ů	Ě	Ú	C	Ý	L	Š	Ý	B	G	M	Ž
F	J	Ó	Q	O	X	C	N	Ž	Z	Ě	Ý	P	W	Ú

SEZNAM SLOV

ODPOSLECH SNIFFING ZLÉDVOJČE HTTPS VPN TUNEL WPA3 FIREWALL

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. ODPOSLECH**
- **B. SNIFFING**
- **C. ZLÉDVOJČE**
- **D. HTTPS**
- **E. VPN**
- **F. TUNEL**
- **G. WPA3**
- **H. FIREWALL**

DEFINICE A POLE K PŘIŘAZENÍ

1. Moderní standard zabezpečení Wi-Fi.
2. Falešný hotspot napodobující Wi-Fi.
3. Zachytávání síťových datových paketů.
4. Zabezpečená datová cesta při přenosu.
5. Filtrování příchozího provozu.
6. Čtení provozu během přenosu.
7. Šifrovaná virtuální privátní síť.
8. Zabezpečený webový přenos.

Kontrolní bod 7: Výzva s přeházenými slovy

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

1. **LSODOECHP** _____
2. **EZČDLOJVÉ** _____
3. **NPV** _____
4. **3AWP** _____
5. **FINGFSNI** _____
6. **PHTST** _____
7. **ELTNU** _____
8. **EIWLFLAR** _____

Bonusová aktivita: Mysli rychle

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

1	Důvody, proč aktualizovat software			
2	Zařízení, která se automaticky připojují k Wi-Fi			
3	Informace, které byste nikdy neměli sdílet			
4	Bezpečné návyky, se kterými můžete začít už dnes			
5	Způsoby, jak zůstat v bezpečí v kavárně			
6	Zařízení, která lze hacknout			
7	Věci, které může hacker vidět na otevřené Wi-Fi			
8	Známky falešné sítě Wi-Fi			
9	Alternativy k veřejné Wi-Fi			
10	Varovné signály v e-mailu			
11	Věci, které na veřejné Wi-Fi neděláte			
12	Místa s Wi-Fi zdarma			
13	Způsoby, jak chránit své účty			
14	Známky toho, že je počítač nakažený			
15	Názvy Wi-Fi, které působí podezřele			

Kontrolní bod 8: Případové studie kyberbezpečnosti

Použijte naučené koncepty k vyřešení níže uvedených reálných scénářů.

PŘÍPADOVÁ STUDIE 1: ZAMEZENÍ ODPOSLECHU PAKETŮ NA VEŘEJNÉ WI-FI



Scénář: Vzdálený obchodní manažer připojený k veřejné letištní síti Wi-Fi si všimne, že několik citlivých obchodních e-mailů uniklo krátce po jejich odeslání v nešifrované podobě.

Otázka k diskusi: Analyzujte rizika veřejných sítí a navrhněte řešení šifrování provozu.

PŘÍPADOVÁ STUDIE 2: OBRANA PROTI PODVRŽENÉMU HOTSPOTU EVIL TWIN



Scénář: Útočníci nasadí podvržený bezdrátový přístupový bod s názvem 'CoffeeShop_Guest', který napodobuje legitimní kavárenský hotspot a zachytává síťový provoz nic netušících hostů.

Otázka k diskusi: Popište ověřovací kroky k detekci a blokování falešných přístupových bodů.

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

29	14	11	26	32	16	30	8		24	26	22	35	22	40

35	8	27	8	16	20	9		36	14	11	14		24	22	19	22	4	15

35	24	20

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: Proč je veřejná Wi-Fi nezabezpečená?

Otevřená veřejná Wi-Fi nešifruje provoz vzduchem, takže ostatní v okolí mohou zachytit jakákoli nechráněná data. [2]

Q2: Co je odposlech paketů?

Paketový sniffer zachytává surová data proudící přes síťové rozhraní a odhaluje hesla v prostém textu a podrobnosti o provozu.

Q3: Co je Evil Twin?

Podvodný přístupový bod zřízený hackery, který napodobuje název a nastavení důvěryhodného místního Wi-Fi hotspotu.

Q4: Jak mě VPN chrání?

Směruje váš provoz šifrovaným tunelem a skrývá vaši aktivitu při prohlížení před místními síťovými odposlechy.

Q5: Chrání mě HTTPS na veřejné Wi-Fi?

Ano, šifruje data vyměňovaná mezi vaším prohlížečem a webovou stránkou a VPN přidává další vrstvu ochrany.

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

Projděte si časté otázky a odpovědi ohledně zmírňování online hrozeb.

Q6: Co je WPA3?

Moderní standard Wi-Fi Protected Access nabízející silnější šifrování a ochranu proti offline slovníkovým útokům. [1]

Q7: Může veřejná Wi-Fi doručit malware?

Ano, útočníci mohou zachytávat provoz a vkládat do relace vašeho prohlížeče škodlivé výzvy ke stažení (drive-by downloads).

Q8: Jaké je riziko sdílení souborů?

Pokud je povoleno sdílení souborů, ostatní uživatelé ve veřejné síti mohou číst nebo upravovat váš místní adresář složek.

Q9: Co je captive portál?

Přihlašovací stránka, kterou hotelové nebo kavárenské sítě používají k povolení přístupu k internetu a kterou mohou útočníci někdy podvrhnout.

Q10: Mám vypínat Wi-Fi, když ji nepoužívám?

Ano, vypnutí Wi-Fi zabrání zařízení v automatickém připojování k nedůvěryhodným sítím.

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

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

Q1: Jak útok man-in-the-middle zneužívá DNS?

Použitím DNS spoofingu na podvodném routeru k nasměrování cílových prohlížečů na podobně vypadající phishingové stránky místo cílových domén.

Q2: Co je únos relace?

Útočník odposlechne nešifrovanou cookie relace přes veřejnou Wi-Fi a importuje ji, aby obešel přihlášení pomocí údajů.

Q3: Co je SSL stripping?

Útok MitM, při kterém útočník sníží zabezpečený požadavek HTTPS uživatele na nešifrované HTTP a zachytává přihlašovací údaje v prostém textu.

Q4: Jak HSTS chrání před SSL strippingem?

HTTP Strict Transport Security nutí prohlížeče připojovat se pouze přes HTTPS a odmítat nešifrované HTTP alternativy. [3]

Q5: Co je split-tunnel VPN?

Konfigurace směrující přes VPN pouze firemní provoz, zatímco veřejná internetová data jdou přímo, což může přinášet riziko expozice únikové cesty.

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

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

Q6: Proč je WPA2 zranitelné vůči KRACK?

Útok Key Reinstallation Attack zneužívá čtyřcestný handshake WPA2 k dešifrování paketů bez znalosti hesla Wi-Fi.

Q7: Co je izolace klientů?

Bezpečnostní nastavení routeru, které brání připojeným Wi-Fi zařízením v přímé vzájemné komunikaci a blokuje místní odposlech.

Q8: Jak útočníci využívají falešné DNS servery?

Konfigurují podvodné routery tak, aby klientům přidělovaly falešné DNS servery, což jim umožňuje zachytávat a přepisovat všechny webové dotazy.

Q9: Skryje VPN mou lokální MAC adresu?

Ne. Adresy MAC jsou lokální identifikátory vrstvy 2; použijte místo toho vestavěnou randomizaci MAC (soukromou adresu) svého zařízení.

Q10: Co je útok podvržením captive portálu?

Útočník hostující falešný ověřovací portál na podvodném hotspotu, aby pod záminkou bezplatné Wi-Fi ukradl přihlašovací údaje.

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

Vzdálení pracovníci často používají Wi-Fi v kavárnách, hotelech a na letištích, kde nemohou ovlivnit zabezpečení sítě.

2. BEZPEČNOSTNÍ POSTŘEH

Podvodný hotspot Evil Twin dokáže zkopírovat přesný název i MAC adresu důvěryhodné sítě a zmást zařízení.

3. BEZPEČNOSTNÍ POSTŘEH

Software pro odposlech paketů, jako je Wireshark, je zdarma a dokáže zobrazit nešifrovaná HTTP hesla v čitelné podobě.

4. BEZPEČNOSTNÍ POSTŘEH

Zabezpečení WPA3 využívá Simultaneous Authentication of Equals (SAE) k ochraně před lokálními útoky hrubou silou.

5. BEZPEČNOSTNÍ POSTŘEH

Útoky SSL stripping obcházejí základní ochranu HTTPS zachycením prvotních HTTP přesměrování na bráně.

6. BEZPEČNOSTNÍ POSTŘEH

Hlavičky odpovědi HTTP Strict Transport Security (HSTS) brání prohlížečům v návratu k nešifrovaným HTTP připojením. [3]

7. POSTŘEH K BEZPEČNOSTI

Vypnutí funkce 'Auto-Connect' zabrání chytrým telefonům připojovat se na veřejných místech k podvodným sítím s podobným názvem.

8. POSTŘEH K BEZPEČNOSTI

Podnikové konfigurace VPN typu always-on nutí veškerý síťový provoz vzdálených pracovníků procházet firemními firewally.

9. POSTŘEH K BEZPEČNOSTI

Falešné přístupové body mohou rozdávat podvržené DNS odpovědi a přesměrovávat cílové domény na phishingové servery.

10. BEZPEČNOSTNÍ POSTŘEH

Bez VPN mohou ostatní uživatelé na otevřeném hotspotu vidět, které weby a servery vaše zařízení kontaktuje.

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] 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

Klíč odpovědí: Kontrolní bod 1 - Výběr z možností

1 Otázka 1 — **Správná odpověď: A**

POZNÁMKA PRO VYUČUJÍCÍ

Co je útok Man-in-the-Middle (MitM)? → Zachycování a pozměňování komunikace mezi dvěma stranami ve sdílené síti

2 Otázka 2 — **Správná odpověď: A**

POZNÁMKA PRO VYUČUJÍCÍ

Co je falešný přístupový bod (Evil Twin)? → Škodlivý Wi-Fi hotspot nakonfigurovaný se stejným SSID jako legitimní síť

3 Otázka 3 — **Správná odpověď: A**

POZNÁMKA PRO VYUČUJÍCÍ

Jak VPN chrání provoz na veřejné Wi-Fi? → Balí všechny síťové pakety do šifrovaného tunelu, takže jsou pro sniffery nečitelné

4 Otázka 4 — **Správná odpověď: A**

POZNÁMKA PRO VYUČUJÍCÍ

Co je odposlech paketů (packet sniffing)? → Použití hardwarových nebo softwarových nástrojů k zachycování a zaznamenávání síťových paketů

5 Otázka 5 — **Správná odpověď: A**

POZNÁMKA PRO VYUČUJÍCÍ

Jaká je role HTTPS? → Šifrování provozu relace mezi prohlížečem a webovým serverem

Klíč odpovědí: Kontrolní bod 2 - Pravda, nebo nepravda

6 **Otázka 6** **Správná odpověď: Pravda**

POZNÁMKA PRO VYUČUJÍCÍ

Připojení uživatelé mohou na otevřených veřejných Wi-Fi sítích snadno zachytávat data v prostém textu.

7 **Otázka 7** **Správná odpověď: Nepravda**

POZNÁMKA PRO VYUČUJÍCÍ

Nepravda: Evil Twin je neautorizovaný hotspot zřízený útočníkem, aby napodobil skutečný.

8 **Otázka 8** **Správná odpověď: Nepravda**

POZNÁMKA PRO VYUČUJÍCÍ

Nepravda: VPN šifruje provoz v tunelu, takže místní odposlechy ho nemohou číst.

9 **Otázka 9** **Správná odpověď: Nepravda**

POZNÁMKA PRO VYUČUJÍCÍ

Nepravda: HTTPS šifruje celou výměnu HTTP, včetně cesty URL i obsahu stránky.

10 **Otázka 10** **Správná odpověď: Pravda**

POZNÁMKA PRO VYUČUJÍCÍ

Wi-Fi hotspoty se zabezpečením WPA3 nabízejí silnější ochranu než otevřené sítě bez hesla.

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

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

KONTROLNÍ BOD 3: KLÍČ KE KLÍČOVÝM POJMŮM

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

KONTROLNÍ BOD 6, ALTERNATIVA: KLÍČ K PŘIŘAZOVÁNÍ SLOV

1 G – WPA3	2 C – ZLÉDVOJČE	3 B – SNIFFING	4 F – TUNEL
5 H – FIREWALL	6 A – ODPOSLECH	7 E – VPN	8 D – HTTPS

POZNÁMKY K DISKUSI PRO VYUČUJÍCÍ

Klíčové pojmy:
Ověřte, že studenti umí vlastními slovy vysvětlit pojmy ODPOSLECH, SNIFFING a EVIL TWIN a ke každému uvést příklad.

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

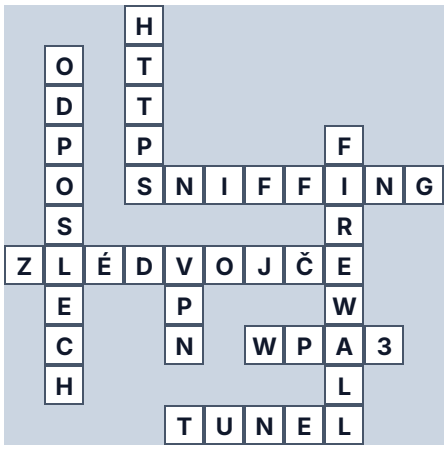
Práce se zdroji:
Nechte studenty ověřit alespoň jedno tvrzení proti referencím v pracovním listu a proberte, proč se čísla, ceny a pravidla mohou v čase měnit.

Klíče k úlohám a poznámky pro vyučující

ŘEŠENÍ OSMISMĚRKY

Č	Š	I	Ě	O	S	N	H	R	Y	R	Ó	Č	U	T
Ť	E	L	Í	B	A	B	T	C	P	T	Y	L	J	Y
L	Y	3	U	K	Ď	Ř	T	N	J	U	D	I	O	Ň
E	K	A	R	Q	F	Ň	P	Ň	Ř	N	S	T	U	Ť
Č	F	P	C	T	O	R	S	Ó	H	E	Š	B	S	V
J	D	W	T	Z	D	Ů	C	Ž	V	L	Ě	K	N	G
O	Ž	D	Ň	Ď	P	Ř	X	F	Q	C	Ú	B	I	A
V	Ž	O	D	L	O	A	Ď	I	Ó	Ď	É	G	F	I
D	D	S	Ř	N	S	E	I	R	Š	Ž	T	É	F	Ř
É	Ů	E	A	Á	L	V	Ř	E	P	O	Q	U	I	Y
L	R	J	S	U	E	P	Š	W	Č	Ň	Ý	B	N	Ě
Z	Š	X	W	Í	C	N	A	A	S	Ž	Ý	Ý	G	L
F	I	N	S	J	H	N	M	L	Ť	P	G	R	Ř	G
Ž	Á	Ó	Ů	Ě	Ú	C	Ý	L	Š	Ý	B	G	M	Ž
F	J	Ó	Q	O	X	C	N	Ž	Z	Ě	Ý	P	W	Ú

ŘEŠENÍ KŘÍŽOVKY



PRŮVODCE PRO VYUČUJÍCÍ K ŘEŠENÍ KŘÍŽOVKY

VODOROVNÉ NÁPOVĚDY

4 vodorovně: SNIFFING Zachytávání síťových datových paketů. (8 písmen)

5 vodorovně: ZLÉDVOJČE Falešný hotspot napodobující Wi-Fi. (9 písmen)

7 vodorovně: WPA3 Moderní standard zabezpečení Wi-Fi. (4 písmen)

8 vodorovně: TUNEL Zabezpečená datová cesta při přenosu. (5 písmen)

SVISLÉ NÁPOVĚDY

1 svisle: HTTPS Zabezpečený webový přenos. (5 písmen)

2 svisle: ODPOSLECH Čtení provozu během přenosu. (9 písmen)

3 svisle: FIREWALL Filtrování příchozího provozu. (8 písmen)

6 svisle: VPN Šifrovaná virtuální privátní síť. (3 písmen)

Klíč řešení přesmyček a šifry

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

KLÍČ K PŘESMYČKÁM

1.	LSODOECHP	ODPOSLECH	5.	FINGFSNI	SNIFFING
2.	EZČDLOJVÉ	ZLÉDVOJČE	6.	PHTST	HTTPS
3.	NPV	VPN	7.	ELTNU	TUNEL
4.	3AWP	WPA3	8.	EIWLFLAR	FIREWALL

KLÍČ TAJNÉ ŠIFROVACÍ VÝZVY

"ŠIFRUJTE PROVOZ VEŘEJNÉ WIFI POMOCÍ VPN"

Klíč k případovým studiím

A Případová studie 1: Zamezení odposlechu paketů na veřejné Wi-Fi

Řešení pro vyučující

POKYNY K HODNOCENÍ

Odpovědi studentů by měly pokrýt následující body:

- Analýza scénáře: Vzdálený obchodní manažer připojený k veřejné letištní Wi-Fi zjistí, že několik citlivých obchodních e-mailů uniklo krátce po jejich odeslání v plaintextu.
- Doporučená strategie a řešení: Nařiďte použití podnikového VPN klienta na všech vzdálených stanicích. Vynucujte rozšíření prohlížeče pouze pro HTTPS a na klientském firewallu blokujte nešifrované protokoly (jako HTTP a FTP).

B Případová studie 2: Obrana proti podvrženému hotspotu Evil Twin

Řešení pro vyučující

POKYNY K HODNOCENÍ

Odpovědi studentů by měly pokrýt následující body:

- Analýza scénáře: Útočníci nasadí podvržený bezdrátový přístupový bod s názvem 'CoffeeShop_Guest' napodobující legitimní hotspot kavárny a zachytávají síťový provoz nic netušících hostů.
- Doporučená strategie a řešení: Auditujte MAC adresy BSSID přístupových bodů k ověření pravosti sítě. Vynuťte validaci stavu klienta, která zablokuje připojení k otevřeným sítím, a pro citlivou práci nařiďte mobilní hotspoty.