Jméno: _____ Datum: _____ Body: _____

Jak skrýt svou IP adresu Pracovní list

Skrývání IP adres, maskování polohy, proxy, Tor a prevence úniků DNS/WebRTC

VPN – PŘEHLED UČIVA

STUDENT
STUDENTSKÝ STATUS
Dráha obránce sítě

ZABEZPEČENÝ
STAV PŘIPOJENÍ
Stínění datových paketů

AKTIVNÍ
OCHRANA PROTI ÚNIKŮM
Ochrana proti únikům DNS a IPv6

Vítejte! Tento balíček aktivit vás provede základními principy virtuálních privátních sítí (VPN). Prozkoumáte, jak šifrované tunely zabezpečují vaše data, jak fungují síťové protokoly a jak rozpoznat a zmírnit úniky soukromí.

KONTROLNÍ BODY PRACOVNÍHO LISTU

- [ ] **Část 1-4: Zvládněte koncepty a protokoly VPN.**
- [ ] **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 VPN od VPN.com

URL: https://www.vpn.com/cs/vpn/

Váš studijní plán: VPN

- Vysvětlete, jak fungují IP adresy a jak prozrazují polohu.
- Porovnejte proxy, Tor a VPN pro maskování síťových adres.
- Určete metody detekce a prevence úniků DNS a WebRTC.
- Pochopte, jak weby sledují uživatele podle jejich veřejné IP.
- Vyhodnoťte multi-hop směrování a šifrované tunely pro ochranu duševního vlastnictví.

POKYNY K PRACOVNÍMU LISTU OCHRANY IP

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 skrytí IP adresy a prevenci úniků. Zakončete bonusovou aktivitou Mysli rychle.

SKRÝVÁNÍ VAŠÍ IP (ÚVOD)

Vaše IP adresa je digitální poštovní adresa, která odhaluje vaši fyzickou polohu a síťové návyky. Skrytí IP adresy je první linií obrany proti online sledování, cílenému profilování a geografickému blokování. Pochopení, jak adresu bezpečně maskovat, pomáhá chránit vaše soukromí online.

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

Kontrolní bod 1: Výzva s výběrem odpovědí

1. Co veřejná IP adresa zařízení prozrazuje webům, které navštívíte?
   - A. Číslo kreditní karty uživatele
   - B. Vaši přibližnou polohu a jméno vašeho ISP
   - C. Úplný místní adresář souborů
   - D. Nastavení jazyka klávesnice

2. Jaká metoda skryje vaši IP a šifruje veškerý provoz v celém systému?
   - A. Standardní webová proxy
   - B. Vymazání cookies v prohlížeči
   - C. Virtuální privátní síť (VPN)
   - D. Vypnutí nativního firewallu

3. Jaké je hlavní omezení soukromí při použití bezplatné webové proxy?
   - A. Nešifruje datový provoz ve veřejných sítích
   - B. Vyžaduje instalaci externího operačního systému
   - C. Je ve Spojených státech zcela nelegální
   - D. Vyžaduje vyhrazenou telefonní linku

4. Jak síť Tor poskytuje uživatelům vysokou anonymitu?
   - A. Zrychlováním připojení
   - B. Směrováním provozu přes tři dobrovolnicky provozované relaye
   - C. Registrací vašeho jména v globální databázi
   - D. Omezením přístupu jen na vládní agentury

5. Co je únik DNS?
   - A. Chyba spočívající v odeslání e-mailu na špatnou adresu
   - B. Když dotazy DNS obcházejí tunel VPN a jdou k ISP
   - C. Hardwarová porucha napájecího zdroje místního routeru
   - D. Aktualizace ovladače místního síťového adaptéru

Kontrolní bod 2: Výzva Pravda/Nepravda

6 Otázka 6

6. Proxy server šifruje provoz OS na pozadí stejně jako VPN.

○ Pravda ○ Nepravda

7 Otázka 7

7. Směrování Tor je vysoce bezpečné, ale snižuje rychlost prohlížení.

○ Pravda ○ Nepravda

8 Otázka 8

8. Úniky WebRTC mohou odhalit vaši skutečnou IP během aktivní VPN relace.

○ Pravda ○ Nepravda

9 Otázka 9

9. Se zapnutou VPN a bez úniků váš ISP nevidí, které weby navštěvujete.

○ Pravda ○ Nepravda

10 Otázka 10

10. Skrytí vaší IP adresy blokuje sledování pomocí otisku prohlížeče (fingerprinting).

○ Pravda ○ Nepravda

Kontrolní bod 3: Doplňování klíčových pojmů

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

1. Obejití bezpečného tunelu, které odhalí vaše doménové dotazy, se nazývá _____ .

2. Komunikační API prohlížeče zvané _____ může nechtěně odhalit vaši skutečnou IP adresu.

3. Webová _____ přesměrovává provoz prohlížeče, ale obsah paketů nešifruje.

4. Vysokou míru anonymity poskytuje síť _____ založená na vícevrstvém šifrování.

5. Vaše veřejná _____ je přidělena telekomunikačním operátorem a prozrazuje vaši oblast.

6. Při obcházení regionálních mediálních blokád se maskuje vaše skutečná _____ .

ZÁSOBNÍK SLOV

IP ADRESA MASKOVÁNÍ POLOHA PROXY TOR ÚNIK DNS VPN TUNEL WEBRTC

Sem napište své odpovědi:

1. 2.

3. 4.

5. 6.

Kontrolní bod 4: Přiřazování síťových pojmů

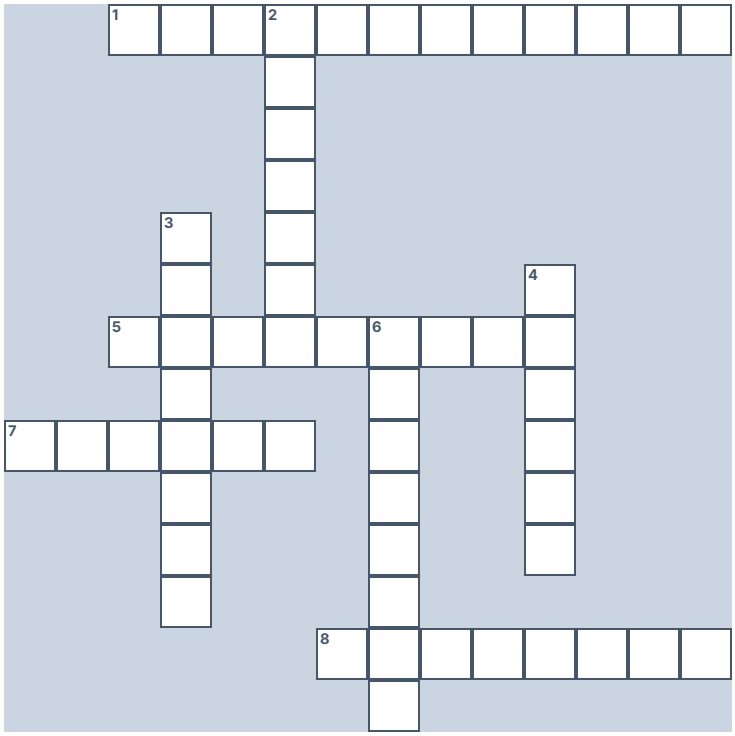
PŘIŘAZOVÁNÍ DEFINIC

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

☐	1. IP adresa	A	Šifruje veškerý provoz zařízení a směruje ho přes server VPN.
☐	2. VPN tunel	B	Směruje data přes tři dobrovolnické servery a v každém kroku šifruje vrstvy.
☐	3. Síť Tor	C	Směrování připojení přes server v jiné zemi k obejití geoblokací.
☐	4. Webová proxy	D	Jedinečné číselné označení identifikující rozhraní zařízení na internetu.
☐	5. Únik DNS	E	Přesměrovává provoz prohlížeče na aplikační vrstvě bez systémového šifrování.
☐	6. WebRTC API	F	Zaznamenávání cílů nešifrovaného internetového provozu vaším telekomunikačním operátorem.
☐	7. Maskování polohy	G	Dotazy překládané mimo VPN tunel, které odhalují navštívené domény ISP.
☐	8. Sledování ze strany ISP	H	Funkce prohlížeče pro hlas/video, která může obcházet tunely a odhalit skutečné IP adresy.

Kontrolní bod 5: Křížovka

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



VODOROVNÉ NÁPOVĚDY

1. Logování cílů nešifrovaného internetového provozu vaším operátorem (12)

5. Směrování připojení přes server v jiné zemi k obejití geografických bloků (9)

7. Funkce prohlížeče pro hlas/video, která může obejít tunely a odhalit skutečné IP adresy (6)

8. Přesměrovává provoz prohlížeče na aplikační vrstvě bez systémového šifrování (8)

SVISLÉ NÁPOVĚDY

2. Dotazy překládané mimo VPN tunel, odhalující navštívené domény poskytovateli (7)

3. Jedinečný číselný identifikátor rozhraní zařízení na internetu (8)

4. Směruje data přes tři dobrovolnické servery a v každém kroku šifruje vrstvy (6)

6. Šifruje veškerý provoz zařízení a směruje jej přes VPN server (8)

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: Logování cílů nešifrovaného internetového provozu vaším operátorem (12 písmen):

5 vodorovně: Směrování připojení přes server v jiné zemi k obejití geografických bloků (9 písmen):

7 vodorovně: Funkce prohlížeče pro hlas/video, která může obejít tunely a odhalit skutečné IP adresy (6 písmen):

8 vodorovně: Přesměrovává provoz prohlížeče na aplikační vrstvě bez systémového šifrování (8 písmen):

SVISLÉ NÁPOVĚDY

2 svisle: Dotazy překládané mimo VPN tunel, odhalující navštívené domény poskytovateli (7 písmen):

3 svisle: Jedinečný číselný identifikátor rozhraní zařízení na internetu (8 písmen):

4 svisle: Směruje data přes tři dobrovolnické servery a v každém kroku šifruje vrstvy (6 písmen):

6 svisle: Šifruje veškerý provoz zařízení a směruje jej přes VPN server (8 písmen):

Kontrolní bod 6: Hledání skrytých slov

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

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

SEZNAM SLOV

IPADRESA VPNTUNEL SÍŤTOR WEBPROXY DNSÚNIK WEBRTC
MASKOVÁNÍ SLEDOVÁNÍISP

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. IPADRESA
B. VPNTUNEL
C. SÍŤTOR
D. WEBPROXY
E. DNSÚNIK
F. WEBRTC
G. MASKOVÁNÍ
H. SLEDOVÁNÍISP

DEFINICE A POLE K PŘIŘAZENÍ
1. Přesměrovává provoz prohlížeče na aplikační vrstvě bez systémového šifrování.
2. Směrování připojení přes server v jiné zemi k obejití geografických bloků.
3. Funkce prohlížeče pro hlas/video, která může obejít tunely a odhalit skutečné IP adresy.
4. Jedinečný číselný identifikátor rozhraní zařízení na internetu.
5. Směruje data přes tři dobrovolnické servery a v každém kroku šifruje vrstvy.
6. Logování cílů nešifrovaného internetového provozu vaším operátorem.
7. Dotazy překládané mimo VPN tunel, odhalující navštívené domény poskytovateli.
8. Šifruje veškerý provoz zařízení a směruje jej přes VPN server.

Kontrolní bod 7: Výzva s přeházenými slovy

Přeuspořádejte písmena níže a odhalte klíčové pojmy a termíny VPN. Odpovědi pište do vyplnitelných polí.

1. SDRIEPAA
2. RSŤOTÍ
3. ÚDNKSIN
4. OÍNKÁVMAS
5. UNPLTVEN
6. XYPOWREB
7. TWRCBE
8. NEOIÁPSVLSÍD

Bonusová aktivita: Mysli rychle

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

1	Důvody, proč používat VPN na cestách			
2	Prohlížeče, které znáte			
3	Věci, které VPN dokáže skrýt			
4	Slova související se soukromím			
5	Slova z tohoto pracovního listu, která si chcete zapamatovat			
6	Věci, které může web odhadnout z vaší IP adresy			
7	Čísla nebo symboly v IP adrese			
8	Mýty o VPN			
9	VPN služby, které znáte			
10	Věci, které vidí váš poskytovatel internetu			
11	Sliby, které dává dobrý poskytovatel VPN			
12	Věci, které mohou prozradit vaši skutečnou IP adresu			
13	Důvody, proč skrýt svou polohu			
14	Způsoby, jak skrýt svou IP adresu			
15	Zařízení, která mohou používat VPN			

Kontrolní bod 8: Případové studie VPN

Použijte naučené koncepty k vyřešení níže uvedených reálných scénářů.

SARAH (STUDENTKA V KAVÁRNĚ)

👩‍💻 "Ahoj! Sedím v Coffee & Bytes. Je tu nezabezpečená veřejná síť 'Free_Wi-Fi_No_Password'. Chci se přihlásit do školního e-mailu a nahrát úkol, ale bojím se hackerů. Jaká jsou rizika používání této sítě bez VPN a jak VPN zabezpečí moje data?"

ALEX (CESTUJÍCÍ STUDENT)

👩‍💻 "Ale ne! Cestuji kvůli projektu v zahraničí a snažím se sledovat biologický dokument hostovaný na serveru v mé domovské zemi. Web ale hlásí 'Toto video není ve vaší aktuální lokalitě dostupné.' Proč jsem blokován a jak mi VPN pomůže ho sledovat?"

Kontrolní bod 9: Dešifrování šifry

K dokončení výcviku maskování IP dešifrujte tuto tajnou zprávu o skrývání digitálních stop.

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

28	17	26	38	16	30	8		28	35	22	32		1	6	26	8	28	32
28	17	26	38	30	39	19		28	38	28	30	9	19	8	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 k VPN (část A)

Projděte si nejčastější otázky a odpovědi zájemců o používání virtuálních privátních sítí.

Q1: Co je VPN a jak funguje?

Virtuální privátní síť (VPN) šifruje vaše internetové připojení a směruje váš provoz přes zabezpečený vzdálený server. Tím maskuje vaši veřejnou IP adresu a omezuje, co mohou místní pozorovatelé sítě a váš ISP vidět o provozu vedeném tunelem VPN.

Q2: Proč bych měl používat VPN?

VPN chrání vaše digitální soukromí, zabezpečuje připojení na veřejných Wi-Fi sítích (například v kavárnách nebo na letištích), může omezit zpomalování podle typu aktivity, když ISP nedokáže identifikovat druh šifrovaného provozu, obchází geografická omezení pro přístup ke globálnímu obsahu a pomáhá zabezpečit prostředky pro práci na dálku.

Q3: Zajistí mi VPN na internetu úplnou anonymitu?

Ne. VPN sice skrývá vaši IP adresu a šifruje provoz, ale stále vás lze sledovat přes cookies prohlížeče, aktivní účty (jako Google nebo Facebook), otisk prohlížeče, nebo pokud váš poskytovatel VPN loguje vaše data.

Q4: Skryje webová proxy mou IP adresu?

Ano, ale jen pro provoz, který přes ni posíláte, obvykle váš prohlížeč. Většina webových proxy vaše data nešifruje, takže ISP nebo provozovatel sítě stále vidí, co odesíláte a přijímáte.

Q5: Je skrývání mé IP legální?

V mnoha zemích ano, ale některé VPN a jiné nástroje ke skrytí IP adresy omezují nebo zakazují. Skrytí IP nikdy nečiní nezákonný čin legálním, proto si před použitím ověřte místní zákony.

Kontrolní bod 10: Základní časté otázky k VPN (část B)

Projděte si nejčastější otázky a odpovědi zájemců o používání virtuálních privátních sítí.

Q6: Skryje Tor mou IP?

Ano. Tor posílá váš provoz přes tři dobrovolnická relé (vstupní, prostřední a výstupní), takže weby vidí adresu výstupního relé a žádné jednotlivé relé nezná zároveň to, kdo jste, i kam míříte. [1]

Q7: Co prozrazuje má IP?

Vaše veřejná IP obvykle odhaluje vašeho ISP a přibližnou polohu, například zemi nebo město. Weby ji také mohou použít k propojení vašich návštěv a k uplatnění geografických blokací.

Q8: Jak zkontroluji, že je skrytá?

Připojte se k VPN, poté navštivte web pro kontrolu IP a spusťte testy úniků DNS a WebRTC. Zobrazená IP a DNS servery mají patřit VPN, ne vašemu ISP. Pokud se objeví vaše skutečná IP, zapněte ochranu proti únikům.

Q9: Mohu VPN používat na telefonu i chytré televizi?

Ano. Moderní poskytovatelé VPN nabízejí vyhrazené aplikace pro iOS, Android, macOS, Windows, Linux a chytré televize a také nastavení na routeru pro ochranu všech zařízení ve vaší domácí síti.

Q10: Co je kill switch?

Kill switch je bezpečnostní funkce, která automaticky odpojí vaše zařízení od internetu, pokud spojení VPN vypadne. Tím zabraňuje úniku vašich nešifrovaných dat nebo skutečné IP adresy.

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

Prozkoumejte technické a strukturální aspekty virtuálních privátních sítí a zabezpečených tunelovacích protokolů.

Q1: Proč mě weby mohou sledovat i po skrytí mé IP adresy?

Skrytí vaší IP nezastaví fingerprinting prohlížeče. Sledovací nástroje mohou zkombinovat detaily jako rozlišení obrazovky, nainstalovaná písma a nastavení prohlížeče do identifikátoru a identifikovat vás mohou i cookies nebo přihlášené účty, proto používejte také prohlížeč zaměřený na soukromí. [3]

Q2: Co je dvojitá VPN neboli směrování Multi-Hop?

Multi-Hop směruje váš provoz postupně přes dva a více serverů VPN. Přidává tak druhou vrstvu šifrování a pomáhá udržet vaši skutečnou IP adresu skrytou před druhým skokem, pokud by byl jeden server kompromitován.

Q3: Co je únik WebRTC a jak mu VPN zabraňuje?

WebRTC je protokol prohlížeče, který může odhalit vaši skutečnou lokální i veřejnou IP adresu, i když je VPN aktivní. Prémiové VPN blokují nebo podvrhují požadavky WebRTC ve svých desktopových/mobilních aplikacích a rozšířeních prohlížeče.

Q4: Může provoz IPv6 prozradit mou skutečnou IP adresu?

Ano, pokud vaše VPN tuneluje pouze IPv4. Zařízení pak může posílat IPv6 provoz mimo tunel a odhalit adresu přidělenou vaším ISP. Používejte VPN, která IPv6 tuneluje nebo blokuje, a ověřte to testem úniků IPv6.

Q5: Jak obfuskace obchází blokování VPN?

Obfuskace (neboli „Stealth VPN“) maskuje pakety VPN provozu tak, aby vypadaly jako běžný webový provoz HTTPS (port 443). To pomáhá projít přes hloubkovou inspekci paketů (DPI), kterou vlády nebo školní/firemní sítě používají k blokování VPN.

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

Prozkoumejte technické a strukturální aspekty virtuálních privátních sítí a zabezpečených tunelovacích protokolů.

Q6: Prozrazuje split tunneling mou skutečnou IP adresu?

Ano, pro aplikace, které vyloučíte. Provoz mimo tunel používá vaši skutečnou IP a RFC 8828 uvádí, že WebRTC může odhalit adresu od ISP pod split-tunnel VPN, pokud to prohlížeč neomezí. [2]

Q7: Co je sdílená IP adresa a jak pomáhá soukromí?

Se sdílenou IP je online mnoho uživatelů VPN se stejnou adresou současně. Pro web je pak mnohem těžší spojit konkrétní návštěvu s vámi než u vyhrazené IP, kterou používáte jen vy.

Q8: Vidí můj ISP, že používám VPN ke skrytí IP?

Obvykle ano. Váš ISP vidí, že se připojujete k IP adrese VPN serveru, kdy se připojujete a kolik dat posíláte, ale ne navštěvované weby ani obsah uvnitř šifrovaného tunelu.

Q9: Co je ochrana proti únikům DNS?

Ochrana proti únikům DNS nutí vaše zařízení posílat dotazy na vyhledání webů (dotazy DNS) přes soukromé, šifrované DNS servery VPN místo serverů vašeho ISP. Tím brání vašemu ISP sledovat, které stránky navštěvujete.

Q10: Je pro skrytí mé IP lepší proxy, nebo VPN?

VPN je obvykle lepší. Skrývá vaši IP pro každou aplikaci na zařízení a šifruje provoz, zatímco webová proxy obvykle pokrývá jen prohlížeč a často nepřidává žádné šifrování.

Část 11: 10 zajímavých faktů o VPN a poznatků z praxe

Projděte si tato velmi cenná fakta a poznatky z praxe o historii, trhu a technologii VPN.

1. PRVNÍ VPN PROTOKOL

PPTP (Point-to-Point Tunneling Protocol), raný VPN protokol od skupiny vedené Microsoftem z let po roce 1990, je dnes považován za nezabezpečený, takže moderní VPN používají WireGuard nebo OpenVPN.

2. FINGERPRINTING

Skrytí vaší IP nezastaví fingerprinting prohlížeče, který vás dokáže identifikovat podle detailů, jako je rozlišení obrazovky a nainstalovaná písma. [3]

3. REVOLUCE WIREGUARD

WireGuard má vysoce zjednodušenou kódovou základnu navrženou pro efektivitu, takže se snáze audituje na bezpečnostní zranitelnosti než tradiční protokoly.

4. ODHALENÍ ADRESY PŘES WEBRTC

RFC 8828 varuje, že WebRTC může odhalit veřejnou adresu VPN i adresu ISP, přes kterou VPN běží, pokud to prohlížeč neomezí. [2]

5. POČÁTKY ALIANCE 5 OČÍ

Zpravodajské partnerství Five Eyes mezi USA, Spojeným královstvím, Kanadou, Austrálií a Novým Zélandem vzniklo ze spolupráce spojenců v oblasti signálového zpravodajství za druhé světové války.

6. HLOUBKOVÁ INSPEKCE PAKETŮ

Pokročilé firewally nasazují hloubkovou inspekci paketů (DPI) k analýze metadat síťových paketů a blokování standardních charakteristik VPN připojení.

7. OPAKOVANÉ POUŽITÍ OKRUHŮ TOR

Tor používá stejný okruh přibližně deset minut a poté sestaví nový, což ztěžuje vzájemné propojení vaší aktivity prohlížení. [1]

8. DECENTRALIZOVANÉ VPN

Decentralizované VPN (dVPN) rozdělují provoz přes síť uzlů provozovaných jednotlivci, čímž snižují závislost na jediném centralizovaném poskytovateli.

9. ANONYMITA TOR VS. VPN

VPN tuneluje provoz přes jediného poskytovatele, zatímco Tor (The Onion Router) posílá provoz přes tři dobrovolnická relé (vstupní, prostřední, výstupní) pro maximalizaci soukromí. [1]

10. PROXY VS. VPN TUNELY

Webová proxy mění IP adresu, kterou web vidí u provozu vašeho prohlížeče, ale na rozdíl od VPN tento provoz obvykle nešifruje ani nepokrývá ostatní aplikace ve vašem zařízení. [5]

Technické reference a zdroje

Citované publikace, kryptografické specifikace a oficiální dokumentační standardy použité v celém tomto pracovním listu.

AKADEMICKÉ A OBOROVÉ REFERENCE

[1] Tor Project. (n.d.). Overview.
https://support.torproject.org/about-tor/how-tor-works/overview/

[2] IETF. (2021). RFC 8828: WebRTC IP Address Handling Requirements.
https://www.rfc-editor.org/rfc/rfc8828

[3] Electronic Frontier Foundation. (n.d.). Cover Your Tracks: Learn.
https://coveryourtracks.eff.org/learn

[4] Electronic Frontier Foundation. (2026). Choosing the VPN That's Right for You.
https://ssd.eff.org/module/choosing-vpn-thats-right-you

[5] Federal Trade Commission. (2018). FTC Provides Tips for Using VPN Apps.
https://www.ftc.gov/news-events/news/press-releases/2018/02/ftc-provides-tips-using-vpn-apps

Klíč odpovědí: Skrytí IP adresy, maskování polohy, proxy, Tor a prevence úniků DNS/WebRTC

1 Otázka 1

Správná odpověď: B

POZNÁMKA PRO VYUČUJÍCÍ

Co veřejná IP adresa zařízení prozrazuje webům, které navštívíte? → Vaši přibližnou polohu a jméno vašeho ISP

2 Systémové šifrování VPN LATENCE

Správná odpověď: C

POZNÁMKA PRO VYUČUJÍCÍ

Na rozdíl od proxy, které přesměrovávají jen provoz prohlížeče, vytváří VPN celosystémový šifrovaný tunel a zabezpečuje aplikace na pozadí, hry i dotazy OS.

3 Absence šifrování u proxy ZABEZPEČENÍ WI-FI

Správná odpověď: A

POZNÁMKA PRO VYUČUJÍCÍ

Webové proxy pouze předávají provoz prohlížeče bez šifrování obsahu paketů, takže provozovatel sítě nebo ISP může váš obsahový provoz stále sledovat.

4 Otázka 4

Správná odpověď: B

POZNÁMKA PRO VYUČUJÍCÍ

Jak síť Tor poskytuje uživatelům vysokou anonymitu? → Směrováním provozu přes tři dobrovolnicky provozované relaye

5 Úniky z tunelu DNS SOUKROMÍ

Správná odpověď: B

POZNÁMKA PRO VYUČUJÍCÍ

K úniku DNS dochází, když požadavky na překlad doménových jmen obcházejí tunel VPN a jdou přímo na resolvery vašeho ISP, čímž odhalují záznamy o navštívených doménách.

Klíč odpovědí: Kontrolní bod 2 - Pravda, nebo nepravda

6 **Podrobnosti omezení proxy** MASKOVÁNÍ IP

Správná odpověď: Nepravda

POZNÁMKA PRO VYUČUJÍCÍ

Proxy fungují na aplikační vrstvě a postrádají celosystémovou integraci síťového ovladače, kterou má VPN tunel.

7 **Otázka 7**

Správná odpověď: Pravda

POZNÁMKA PRO VYUČUJÍCÍ

Přeposílání provozu přes tři dobrovolnické relaye s vrstveným šifrováním přidává latenci, takže Tor je obvykle pomalejší než přímé připojení.

8 **Otázka 8**

Správná odpověď: Pravda

POZNÁMKA PRO VYUČUJÍCÍ

WebRTC může odhalit místní adresy a u některých konfigurací VPN i veřejnou IP přidělenou ISP pod tunelem (RFC 8828).

9 **Otázka 9**

Správná odpověď: Pravda

POZNÁMKA PRO VYUČUJÍCÍ

Bez úniků DNS nebo WebRTC vidí ISP jen šifrovaný provoz k serveru VPN, ne weby, které navštěvujete.

10 **Limity fingerprintingu** NO-LOGS

Správná odpověď: Nepravda

POZNÁMKA PRO VYUČUJÍCÍ

Fingerprinting cílí na konfigurační metriky zařízení (rozlišení obrazovky, fonty, doplňky), které zůstávají viditelné, i když je IP skrytá.

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

D 1. IP adresa	A 2. VPN tunel	B 3. Síť Tor	E 4. Webová proxy
G 5. Únik DNS	H 6. WebRTC API	C 7. Maskování polohy	F 8. Sledování ze strany ISP

KONTROLNÍ BOD 3: KLÍČ KE KLÍČOVÝM POJMŮM

1 ÚNIK DNS	2 WEBRTC	3 PROXY	4 TOR
5 IP ADRESA	6 POLOHA		

KONTROLNÍ BOD 6, ALTERNATIVA: KLÍČ K PŘIŘAZOVÁNÍ SLOV

1 D – WEBPROXY	2 G – MASKOVÁNÍ	3 F – WEBRTC	4 A – IPADRESA
5 C – SÍŤTOR	6 H – SLEDOVÁNÍISP	7 E – DNSÚNIK	8 B – VPNTUNEL

POZNÁMKY K DISKUSI PRO VYUČUJÍCÍ

Klíčové pojmy:
Ověřte, že studenti umí vlastními slovy vysvětlit pojmy IP adresa, VPN tunel a Síť Tor a ke každému uvést příklad.

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

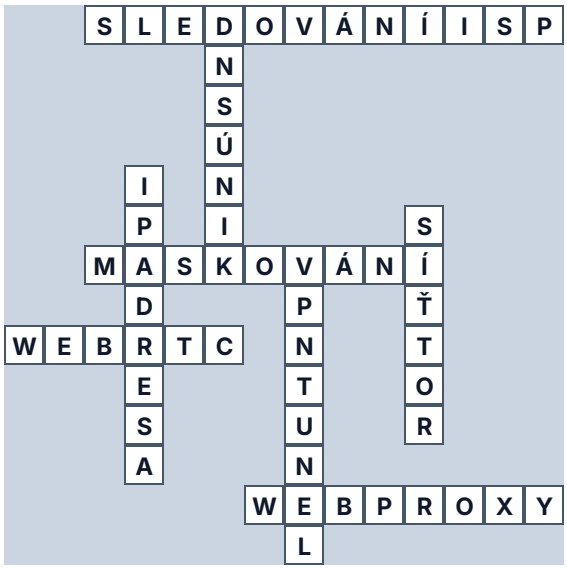
Práce se zdroji:
Nechte studenty ověřit alespoň jedno tvrzení proti referencím v pracovním listu a proberte, proč se čísla, ceny a pravidla mohou v čase měnit.

Klíče k úlohám a poznámky pro vyučující

ŘEŠENÍ OSMISMĚRKY

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

ŘEŠENÍ KŘÍŽOVKY



PRŮVODCE PRO VYUČUJÍCÍ K ŘEŠENÍ KŘÍŽOVKY

VODOROVNÉ NÁPOVĚDY

1 vodorovně: SLEDOVÁNÍISP Logování cílů nešifrovaného internetového provozu vaším operátorem (12 písmen)

5 vodorovně: MASKOVÁNÍ Směrování připojení přes server v jiné zemi k obejití geografických bloků (9 písmen)

7 vodorovně: WEBRTC Funkce prohlížeče pro hlas/video, která může obejít tunely a odhalit skutečné IP adresy (6 písmen)

8 vodorovně: WEBPROXY Přesměrovává provoz prohlížeče na aplikační vrstvě bez systémového šifrování (8 písmen)

SVISLÉ NÁPOVĚDY

2 svisle: DNSÚNIK Dotazy překládané mimo VPN tunel, odhalující navštívené domény poskytovateli (7 písmen)

3 svisle: IPADRESA Jedinečný číselný identifikátor rozhraní zařízení na internetu (8 písmen)

4 svisle: SÍŤTOR Směruje data přes tři dobrovolnické servery a v každém kroku šifruje vrstvy (6 písmen)

6 svisle: VPNTUNEL Šifruje veškerý provoz zařízení a směruje jej přes VPN server (8 písmen)

Klíč řešení přesmyček a šifry

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

KLÍČ K PŘESMYČKÁM

1.	SDRIEPAA	IPADRESA	5.	UNPLTVEN	VPNTUNEL
2.	RSŤOTÍ	SÍŤTOR	6.	XYPOWREB	WEBPROXY
3.	ÚDNKSIN	DNSÚNIK	7.	TWRCBE	WEBRTC
4.	OÍNKÁVMAS	MASKOVÁNÍ	8.	NEOIÁPSVLSÍD	SLEDOVÁNÍISP

KLÍČ TAJNÉ ŠIFROVACÍ VÝZVY

"SKRYJTE SVOU ADRESU SKRYTÝM SYSTÉMEM"

Klíč k případovým studiím

A Scénář A: Bezpečnost na veřejné síti

SNIFFING A ŠIFROVÁNÍ | Sarahino dilema

POKYNY K HODNOCENÍ

Odpovědi studentů by měly pokrýt následující body:

- Rizika: Odposlech paketů (sniffing), zachycení dat a útoky man-in-the-middle. Někdo na stejné kavárenské síti by mohl zachytit její přihlašovací údaje nebo soubor s úkolem.
- Ochrana VPN: Šifruje obsah síťových paketů, takže zachycený tunelový provoz je pro pasivní odposlech v místní síti nečitelný, je-li VPN správně nakonfigurována.

B Scénář B: Přístup k blokovaným zdrojům

GEOBLOKACE A IP ADRESY | Alexovo dilema

POKYNY K HODNOCENÍ

Odpovědi studentů by měly pokrýt následující body:

- Proč blokováno: Streamovací služba používá geoblokaci, která mapuje cestovatelovu lokální IP adresu na jeho fyzickou zemi a blokuje ji na základě územních licencí.
- Jak VPN pomáhá: Maskuje jeho skutečnou polohu směrováním provozu přes server v jeho domovské zemi. Web vidí IP adresu domovské země a umožní přístup.