

Text laboratorní úlohy

Laboratorní úloha č. 11

ANONYMIZAČNÍ SÍTĚ

Úvod k laboratorní úloze

Cílem této laboratorní úlohy je seznámit studenty s využitím anonymizačních sítí, jejich významem v oblasti ochrany soukromí a bezpečnosti online komunikace a objasnit jim základní principy jejich fungování. Hlavní pozornost bude věnována **anonymizační síti Tor** (z angl. *The Onion Routing*), která pro zajištění důvěrnosti, anonymity uživatelů a utajení komunikace mezi účastníky využívá techniku tzv. „cibulového“ směrování (*onion routing*). V rámci této úlohy budou vysvětleny základní principy fungování a účel anonymizačních sítí, představen bude hlavní koncept celosvětově známé anonymizační sítě Tor a objasněno bude také použití vrstevnatého směrování v tomto typu sítí.

V praktické části se studenti budou věnovat instalaci a konfiguraci nástroje Tor v prostředí Kali Linux, prohlížení internetu prostřednictvím sítě Tor a analýze síťové komunikace pomocí nástroje Wireshark. Studenti tak získají praktické dovednosti v oblasti anonymizace internetové komunikace a naučí se analyzovat tok dat v prostředí anonymizačních sítí.

Požadavky pro vypracování úlohy:

- software: VMware Workstation Player pro virtualizaci stanic,
- virtuální stroje: dva, resp. tři virtuální stroje s Kali Linux.

1. Teoretický úvod

V této laboratorní úloze zaměřené na problematiku anonymizačních sítí se seznámíte se základními principy jejich fungování, základní strukturou a také s procesem tzv. vícevrstvého („cibulového“) šifrování, který je typický právě pro dosažení anonymity koncových zařízení komunikujících prostřednictvím anonymizačních sítí.

1.1. Anonymizační síť

Anonymizační síť představují pokročilé bezpečnostní technologie navržené a používané za účelem **ochrany identity uživatelů a jejich soukromí** v digitálním prostředí současných počítačových sítí. Jedná se o speciální typy sítí určené k ochraně identity a polohy uživatelů, které prostřednictvím šifrování informací obsažených v přenášených datových jednotkách **umožňují anonymní prohlížení internetu**, resp. komunikaci, a tím i **skrytí identity** přístupujících uživatelů (resp. zařízení) napříč rozsáhlým konglomerátem vzájemně propojených sítí. Jejich cílem je minimalizovat možnost sledování zdrojové IP adresy, lokalizace či jiných identifikačních údajů uživatele. Mezi nejznámější anonymizační sítě patří například **Tor, I2P, Freenet** a i. V tomto úkolu bude největší pozornost věnována především anonymizační síti Tor (*The Onion Router*).

1.2. Tor (The Onion Router)

Tor je projekt vyvíjený s cílem poskytnout uživatelům internetu možnosti anonymního vystupování a komunikace v digitálním prostředí. Je založen na **principu tzv. „cibulového“ směrování (*onion routing*)**, kdy komunikace mezi klientem a cílovým serverem probíhá přes sérii náhodně vybraných zprostředkovatelů nazývaných „*Tor relé*“ (typicky se jedná o mezilehlé směrovače na přenosové trase). Každý takovýto mezilehlý uzel zná pouze bezprostředně předcházející a následující bod komunikace, díky čemuž je znemožněno sledování průběhu celé komunikace, včetně informací o koncových bodech. Anonymizační síť Tor je navržena tak, aby bylo možné:

- zajistit anonymitu klienta vůči cílové službě,
- například v případě tzv. skrytých služeb zajistit také anonymitu cíle vůči klientovi,
- zabránit třetím stranám (např. poskytovatelům internetového připojení, provozovatelům Wi-Fi sítí apod.) získat přehled o tom, jaké stránky uživatel navštěvuje nebo s kým v síti komunikuje.

Architektura sítě Tor

Pro další popis a vysvětlení principů tzv. „cibulového“ směrování jsou důležité dva základní pojmy: **vrstvy a uzly**. Při směrování datových jednotek (tzv. buněk) směrem k adresátovi s využitím „cibulového“ směrování každý mezilehlý uzel zapojený do komunikace dešifruje pouze jednu „vrstvu“ aplikovaného šifrování. Po dešifrování, tj. odstranění vnější vrstvy, se odhalí následující adresa na trase k příjemci datové jednotky, ostatní zůstávají stále chráněny, ukryty šifrováním. To představuje základní mechanismus zajištění anonymity uživatelů (resp. jednotlivých uzlů, zařízení).

Typická síť Tor se skládá z následujících **základních komponent (uzlů)**:

- **Tor klient** – aplikační rozhraní na straně uživatele využívající možnosti anonymního prohlížení, typicky ve formě Tor prohlížeče nebo systémového démona *tor*.
- **Tor směrovače (*Tor relays, onion routers*)** – mezilehlé uzly (zpravidla směrovače), jejichž úkolem je směrování datových jednotek (buněk) v síti Tor. Rozlišujeme:
 - **vstupní uzel (*Entry Node*)** – první bod (uzel) v komunikační síti, kde poprvé dochází k šifrování přenášených dat;
 - **relé uzly (*Relay Nodes*)** – mezilehlé¹ uzly, které přenášejí šifrovaná data, resp. je postupně (de)šifrují pomocí svých šifrovacích a dešifrovacích klíčů;

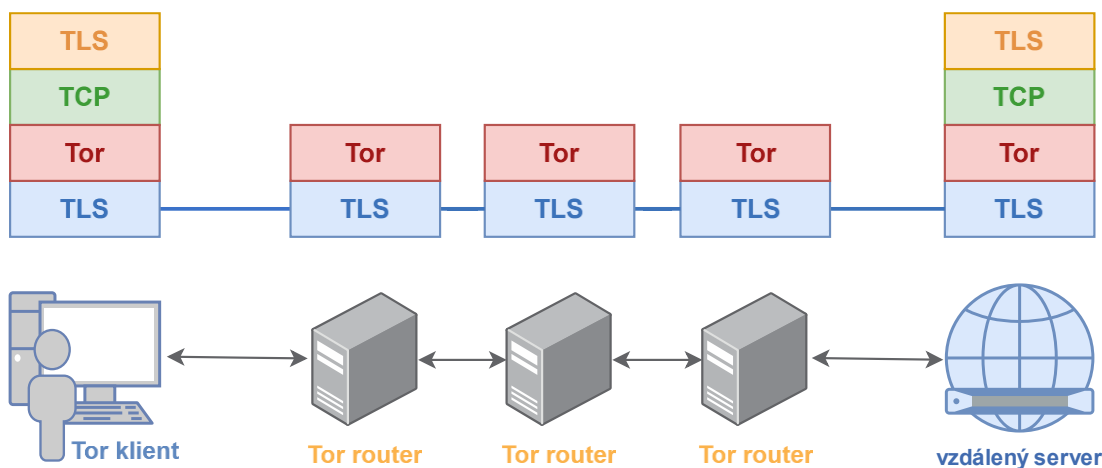
¹ Tyto mezilehlé *relay* uzly jsou zprostředkovateli přenosu šifrované datové komunikace mezi odesílatelem a příjemcem využívajícím anonymizační síť Tor.

- **výstupní uzel (*Exit Node*)** – poslední bod v síti, kde jsou data dešifrována a odeslána na cílovou adresu (příjemci);
- **Adresářové servery** – centrální uzly, které spravují seznam důvěryhodných Tor směrovačů a poskytují informace o dostupných uzlech ostatním prvkům v síti Tor.

Princip šifrování v anonymizační síti

Mechanismy sítě Tor pro zajištění anonymity uživatelů jsou aplikovány na úrovni síťové vrstvy, jak ji známe z TCP/IP modelu. Celková architektura sítě Tor se skládá z následujících vrstev:

- **Linková vrstva** – je realizována prostřednictvím TLS spojení mezi jednotlivými prvky sítě Tor, kde protokol TLS hraje zásadní roli při autentizaci prvků a ochraně důvěrnosti a integrity přenosu. Každý individuální úsek komunikace mezi dvěma sousedními uzly (např. klient ↔ OR1) je zabezpečen samostatným TLS tunelem.
- **Síťová vrstva** – je realizována protokolem Tor, který zajišťuje vytváření, přenos a směrování buněk, včetně jejich šifrování.
- **Transportní vrstva** – za účelem spolehlivosti přenosu a možnosti šifrování pomocí TLS využívá spojově orientovaný a spolehlivý protokol TCP.
- **Aplikační vrstva** – tvořena klientskými aplikacemi na straně koncového uživatele, které využívají transportní protokol TCP (např. HTTP, FTP).



Obrázek 1.1 Vrstvová architektura sítě Tor ².

V síti Tor probíhá komunikace ve formě **buněk (*cells*)**, které představují základní jednotku přenosu dat mezi klientem a uzly v síti. Každá buňka má **pevně danou velikost 512 bajtů**. Neměnná velikost buněk umožňuje minimalizovat možnost analýzy komunikace na základě velikosti přenášených datových jednotek. Všechny zprávy, bez

² Převzato z oficiálních výukových materiálů k přednáškám předmětu MPC-NSB – vypracoval garant předmětu a přednášející doc. Karel Burda, CSs. (viz též E-learning předmětu).

ohledu na jejich skutečný obsah nebo délku, jsou proto zapouzdřeny do stejně velkých buněk, čímž se snižuje riziko, že by pozorovatel (typicky útočník) mohl identifikovat vzorce komunikace nebo konkrétní typ dat.

Buňky Tor lze podle účelu jejich použití rozdělit na několik typů, například:

- **Buňky typu CREATE a CREATED** – slouží k vytváření šifrovaného okruhu mezi klientem a jednotlivými uzly (resp. mezi dvojicí sousedních uzlů v síti Tor).
- **Buňky označené jako RELAY, RELAY_EXTEND, RELAY_DATA** apod. – slouží k přenosu šifrovaných dat přes jednotlivé uzly v rámci okruhu.
- K ukončení okruhu se používá **buňka typu DESTROY**, která signalizuje, že daný komunikační okruh má být okamžitě zrušen a všechny navázané šifrovací klíče zneplatněny.

Každá buňka Tor má pevně definovaný formát a obsahuje více polí, která slouží k identifikaci, správě přenosu a samotnému přenosu dat. Přesný obsah buňky se může mírně lišit v závislosti na jejím typu. Struktura standardní buňky Tor je znázorněna na obr. 1.2, význam jednotlivých polí je následující:

- **Circuit ID** – identifikátor okruhu, ke kterému buňka náleží. Umožňuje multiplexování více okruhů přes jedno TCP spojení.
- **Command** – určuje typ buňky (např. CREATE, RELAY, DESTROY, atd.).
- **Payload** – tělo buňky, které je během přenosu v síti Tor šifrováno. Jeho obsah se liší podle konkrétního typu buňky.



Obrázek 1.2 Schematické znázornění struktury Tor buňky³.

Vytváření okruhů a princip cibulového směrování v síti Tor

Klíčovým mechanismem pro zajištění anonymity je vytváření tzv. **okruhů** (*circuits*) a používání techniky vícevrstvého šifrování, známé jako *onion routing*.

Tor vytváří mezi klientem a cílovým serverem vícevrstvový (tzv. „cibulový“⁴) šifrovaný kanál, prostřednictvím kterého jsou data, resp. datové pakety přesměrovány

³ Převzato z oficiálních výukových materiálů k přednáškám předmětu MPC-NSB – vypracoval garant předmětu a přednášející doc. Karel Burda, CSs. (viz též E-learning předmětu).

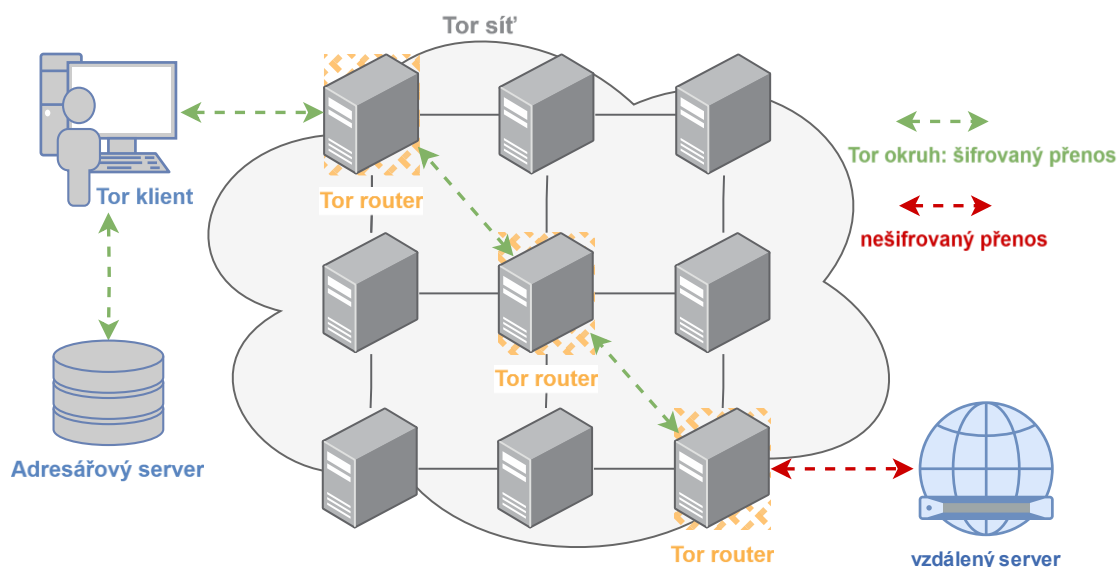
⁴ Označení je převzato z překladu angl. slova *onion*, které značí cibuli. Princip šifrování, resp. dešifrování paketů odesílaných přes Tor síť se podobá vrstvení cibule – a právě na základě této podobnosti byl vytvořen i její název.

přes několik náhodně vybraných uzlů v síti Tor. Jednotlivé uzly znají pouze odesílatele a příjemce své části trasy, nemají znalost o jiných uzlech, které byly nebo budou zapojeny do celé komunikace potřebné k doručení dané datové jednotky (buňky) od jejího odesílatele až k vybranému příjemci, což zajišťuje anonymitu.

Proces vytváření okruhu probíhá v několika etapách:

1. **Výběr uzlů:** klient si ze zveřejněného seznamu náhodně vybere vhodné uzly Tor. Výběr probíhá podle specifických pravidel – například vstupní uzly musí být stabilní a důvěryhodné.
2. **Dohoda na klíčích:** pomocí protokolu podobného výměně klíčů podle Diffie-Hellmana si klient postupně vytvoří s každým uzlem samostatný šifrovací klíč. Všechny tyto výměny probíhají přes vstupní uzel, přičemž klient navazuje spojení s dalšími uzly „skrze“ předchozí (šifrovaně).
3. **Postupné rozšíření okruhu:** nejprve se vytvoří šifrované spojení klienta se vstupním uzlem (pomocí buněk CREATE a CREATED), následně se přes tento uzel vytvoří šifrovaný tunel postupně ke všem dalším uzlům až nakonec k výstupnímu uzlu.

Takto vytvořený okruh slouží jako trasa, po které jsou dále přenášena šifrovaná data.



Obrázek 1.3 Komponenty Tor sítě a znázornění vytvořeného okruhu⁵.

Po vytvoření kompletního okruhu od odesílatele až k cílovému příjemci je možné zahájit přenos dat, který je podroben tzv. „cibulovému směrování“. Mechanismus tohoto vícevrstvého šifrování funguje následovně:

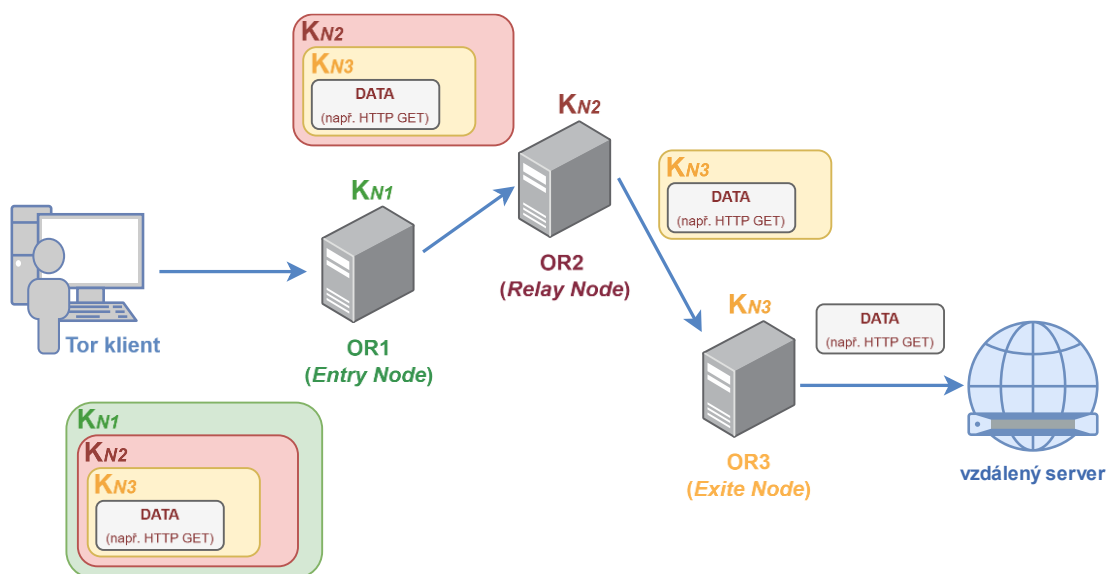
⁵ Převzato z [5].

1. Klient si nejprve připraví datovou jednotku (např. požadavek HTTP), kterou chce doručit na cílový server.
2. Tuto jednotku následně **vícekrát zašifruje** – každá vrstva šifrování je určena jednomu uzlu v pořadí od výstupního po vstupní:
 - nejprve pro výstupní uzel (vnitřní vrstva),
 - poté pro prostřední uzel,
 - nakonec pro vstupní uzel (vnější vrstva).
3. Když šifrovaná zpráva dorazí do vstupního uzlu, ten v procesu dešifrování odstraní pouze svou vrstvu (vnější) a odešle její obsah, který je zašifrován pomocí klíče pro další mezilehlý uzel v pořadí, dále směrem k tomuto uzlu ve vytvořeném okruhu.
4. Následující uzel opět odstraní jen svou vrstvu šifrování a odešle šifrovaná data dále.
5. Tento proces se opakuje, dokud buňka nedorazí k výstupnímu uzlu. Ten dešifruje poslední vrstvu a odešle původní požadavek vytvořený klientem, resp. odesílatelem, na cílový server na internetu (např. webovou stránku).
6. Při zpětné odpovědi se postupuje obdobně, pouze s tím rozdílem, že jednotlivé šifrovací klíče jsou aplikovány při vytváření vrstev v opačném pořadí – výstupní uzel odpověď zašifruje a pošle zpět přes tentýž okruh, přičemž každý uzel dešifruje pouze svou část, až se odpověď dostane zpět k původnímu klientovi.

Aplikace vícevrstvého šifrování na přenášena data je schematicky znázorněna na obr. 1.4. Popsaný mechanismus zajišťuje, že žádný z uzlů nemá úplnou znalost o celé komunikaci. Vstupní uzel zná IP adresu klienta, ale ne cílový server. Výstupní uzel naopak zná cíl, ale ne klienta. Všechny mezilehlé uzly znají pouze své bezprostřední sousedy.

Použití anonymizačních sítí přináší řadu výhod, mezi něž nepochybně patří skrytí IP adresy uživatelů, což je zároveň jeden ze základních předpokladů pro ochranu před nežádoucím sledováním a profilováním. Na druhou stranu, přenos dat prostřednictvím anonymizační sítě může být znatelně pomalejší, protože je nutné data přenášet přes více mezilehlých uzlů a zároveň je opakovaně šifrovat (resp. dešifrovat), což může vést ke zpomalení internetového připojení. Mezi další nevýhody a rizika anonymizačních sítí lze zařadit i možnost kompromitace výstupního uzlu směrem k příjemci dat (*exit node*) a také skutečnost, že použití anonymizačních sítí nezaručuje úplnou ochranu před všemi formami sledování komunikace v počítačových sítích – např. sledování časových korelací mezi datovými přenosy a jejich následná analýza. Stejně tak neposkytují ochranu před jinými typy síťových útoků nebo útoků na koncová zařízení, např. prostřednictvím škodlivého kódu (malwaru) na straně uživatele apod.

Více informací o konceptu anonymizačních sítí a o samotné síti Tor lze nalézt v publikacích [1], [2], [3], [4].



Obrázek 1.4 Schematické znázornění vrstveného šifrování v Tor síti⁶.

1.3. Použité nástroje

Tor v Kali Linux

Tor představuje jednoduchý softwarový nástroj umožňující **anonymní prohlížení internetu přes síť Tor**. Vytvoření, resp. simulaci vlastní anonymizační sítě založené na využití služby Tor lze realizovat i v prostředí systému Kali Linux, a to její instalací přímo prostřednictvím příkazového řádku (terminálu) pomocí příkazů:

```
sudo apt update  
sudo apt install tor
```

Po úspěšné instalaci následuje spuštění služby Tor:

```
sudo systemctl start tor  
sudo systemctl enable tor
```

Ověření, zda je služba aktivní, lze provést příkazem:

```
sudo systemctl status tor
```

⁶ Převzato z [6].

Pro ověření připojení k síti Tor lze použít např. níže uvedený příkaz:

```
curl --socks5-hostname 127.0.0.1:9050  
https://check.torproject.org/
```

Uvedený příkaz spustí odeslání jednoduché HTTP GET požadavky na stránku <https://check.torproject.org>⁷ přes vytvořenou Tor síť. Pozn.: TCP port 9050 je výchozím portem pro klienta Tor běžícího na Kali Linuxu. Síť Tor v tomto případě funguje jako proxy server, resp. zprostředkovatel komunikace mezi klientem na vašem zařízení a dotazovaným cílovým serverem – veškerá komunikace je tedy přesměrována právě přes síť Tor.

Po odeslání požadavku server **check.torproject.org** analyzuje vaši IP adresu a vrátí odpověď, zda komunikace probíhá přes Tor. Pokud je použití sítě Tor správně nastaveno, v terminálu se zobrazí hláška:

"Congratulations. This browser is configured to use Tor."

Tor Browser

Jedná se o upravenou verzi webového prohlížeče nakonfigurovanou pro anonymní používání s využitím sítě Tor za účelem **zajištění soukromí a anonymity uživatelů** v online prostředí. Tor Browser je navržen tak, aby bylo možné skrýt nejen samotnou identitu uživatele, ale také jeho polohu a aktivitu na internetu.

Tor Browser realizuje šifrování přenášených uživatelských dat v několika vrstvách. Datové přenosy jsou kompletně šifrovány a odesílány přes síť Tor, která se skládá z velkého množství (typicky tisíců) *relay* uzlů zprostředkujících přenos zabezpečené šifrované komunikace. Každý *relay* uzel na cestě přenosu dat směrem k příjemci vždy dešifruje pouze jednu (vnější) vrstvu, díky čemuž nikdy nezíská úplnou, kompletní informaci o daném přenosu, a anonymita komunikujících stran tak zůstává zachována.

Wireshark

Wireshark je síťový analyzátor, který umožňuje sledovat datové přenosy. V případě sítě Tor je možné zachytit šifrované pakety a analyzovat jejich strukturu, avšak jejich obsah zůstává chráněn šifrováním.

Použití nástroje Wireshark jste si prakticky vyzkoušeli již v rámci několika předchozích laboratorních úloh, a proto jeho podrobnější popis nebude dále uváděn.

⁷ Více o filosofii a struktuře projektu Tor, jehož cílem je poskytování specializovaného prohlížeče Tor Browser pro anonymní prohlížení, je možné nalézt na oficiálních stránkách: [7].

2. Praktická část

V rámci praktické části úlohy si vyzkoušíte **anonymní prohlížení prostřednictvím anonymizačního webového prohlížeče Tor Browser**. Následně budete analyzovat zachycený tok dat v anonymizační síti pomocí nástroje Wireshark, na základě čehož získáte přehled o výhodách, nevýhodách a rizicích spojených s použitím prostředků pro anonymizaci v dnešních počítačových sítích.

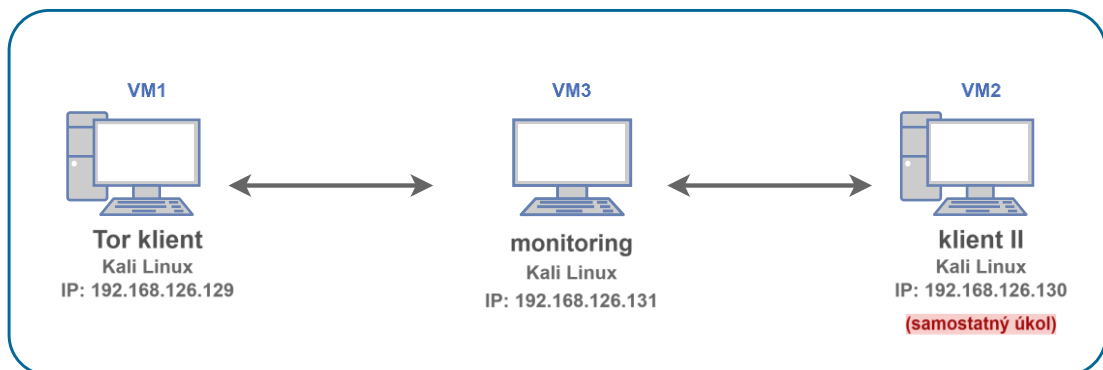
2.1. Topologie virtuální sítě a nastavení virtuálních strojů

Vytvořená síť bude sestávat ze tří virtuálních strojů:

- **klient pro anonymní prohlížení** a přístup na internet přes síť Tor,
- **klient II** – simulace klasického připojení, tj. běžné připojení bez použití Tor (využití v části **Samostatný úkol**),
- **monitorovací zařízení**, které bude sloužit pro účely sledování a následné analýzy probíhající komunikace v síti.

Síťová konfigurace:

- Tor klient (VM1): 192.168.126.129
- klient II (VM2): 192.168.126.130
- monitorovací zařízení (VM3): 192.168.126.131



Obrázek 2.1 Topologie sítě laboratorní úlohy.

2.2. Seznámení se s použitými nástroji

Přehled základních příkazů pro jednotlivé používané nástroje

- Uvedení základních příkazů pro práci se službou Tor na klientském zařízení a pro instalaci a následné **použití prohlížeče Tor Browser** pro anonymní prohlížení internetu bylo součástí teoretického úvodu, a z tohoto důvodu se jejich opakovaný přehled dále neuvádí. Všechny potřebné příkazy budou uvedeny následně v praktické části v jednotlivých krocích pro vypracování laboratorního úkolu.

Použití Wiresharku pro analýzu komunikace přes síť Tor

- V rámci analýzy zaznamenané komunikace je vhodné použít filtr:

```
tcp.port == 9050
```

Použití uvedeného filtru zajistí zobrazení TCP komunikace na příslušném portu, tj. 9050 – což je port využívaný na straně klienta pro komunikaci se SOCKS proxy pro její další přesměrování přes anonymizovanou síť Tor.

2.3. Postup pro vypracování laboratorní úlohy

A) Příprava prostředí

Spuštění virtuálních strojů:

- Otevřete VMware Workstation Pro (zástupce na ploše).
- Postupně spusťte všechny tři virtuální stroje s Kali Linux.
- Zkontrolujte, že všechny VMs jsou připojeny ke stejné virtuální síti (nastavení např. NAT nebo Host-Only).
- Přihlaste se do prostředí Kali Linux na všech VMs.

VM „Tor klient“ – přihlašovací údaje: **Username:** klient, **Password:** kali

VM „Klient II“ – přihlašovací údaje: **Username:** server, **Password:** kali

VM „monitoring“ – přihlašovací údaje: **Username:** kali, **Password:** kali

- Zkontrolujte síťovou konektivitu mezi stroji (pomocí příkazu **ping**).

B) Příprava klienta pro využití anonymizované sítě

Instalace Tor na klientském VM:

- Na jednom z VM, který bude v simulované síti zastávat roli klienta, otevřete terminál kliknutím na ikonu umístěnou v záhlaví hlavního pracovního okna nebo v menu zvolte **Applications > System Tools > Terminal**. Otevře se okno s příkazovým řádkem.
- Aktualizujte balíčky Kali Linux příkazem:

```
sudo apt update && sudo apt upgrade -y
```

- Pomocí následujících příkazů nainstalujte službu Tor:

```
sudo apt update  
sudo apt install tor
```

Po úspěšné instalaci běží služba Tor automaticky na pozadí systému.

Instalace Tor Browseru

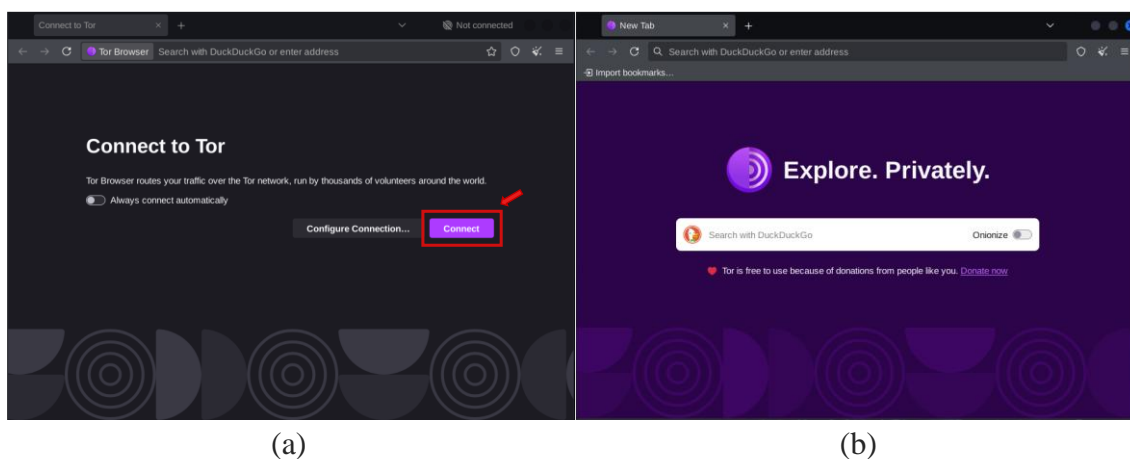
- Stáhněte instalační balíček Tor Browser ze stránek projektu:

```
sudo apt install torbrowser-launcher -y
```

- Po stažení spusťte Tor Browser zadáním níže uvedeného příkazu do terminálu (nebo v menu: **Applications** → **Internet** → **Tor Browser Launcher**):

```
torbrowser-launcher
```

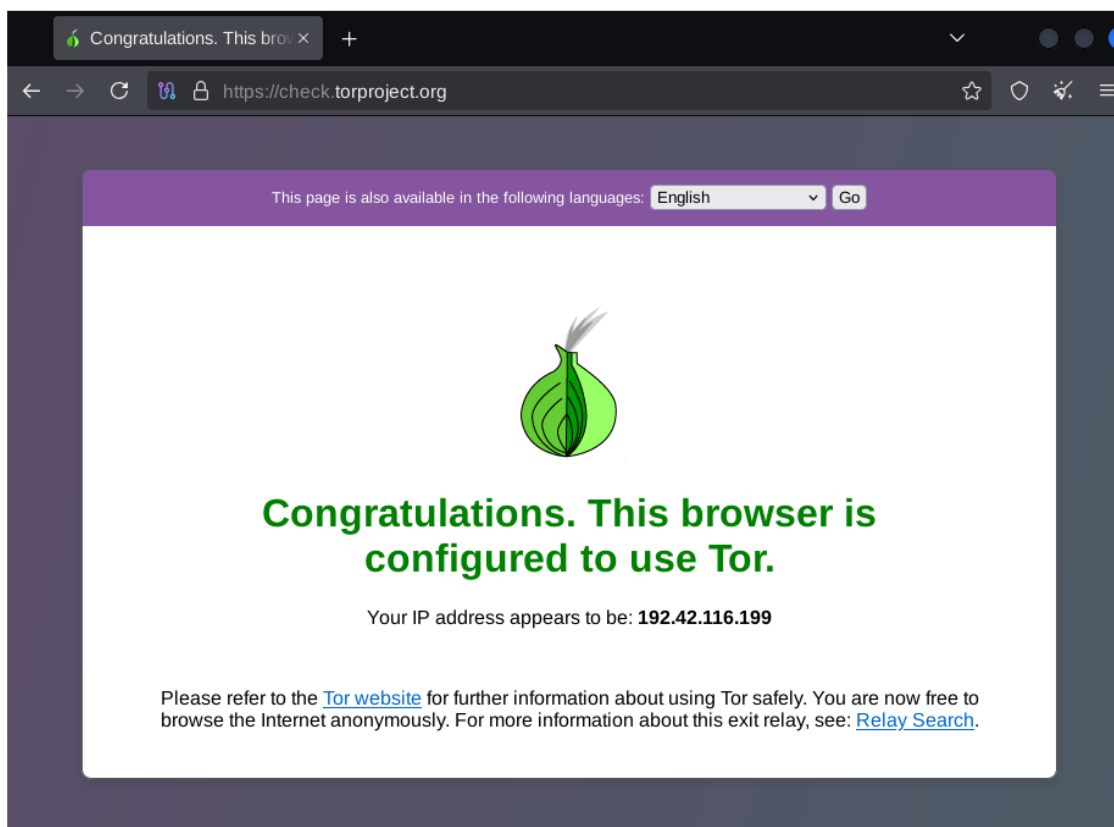
- Po spuštění akceptujte podmínky, potvrďte a nechte proběhnout aktualizaci, pokud je dostupná, a následně klikněte na **Connect**.
- Po úspěšném připojení se otevře anonymní prohlížeč okno, což značí, že **Tor Browser** je připraven k anonymnímu prohlížení.



Obrázek 2.2 Připojení k prohlížeči Tor Browser (a), načtení úvodní domovské stránky (b).

Připojení k síti Tor a ověření funkčnosti

- Po spuštění Tor Browseru by se měla automaticky otevřít stránka (viz obr. 2.3): <https://check.torproject.org/>
- V případě úspěšného připojení se zobrazí hláška: "Congratulations. This browser is configured to use Tor."
- Pokud nedojde k automatickému načtení stránky, zkuste kliknout na možnost **Connect** nebo restartujte Tor Browser.



Obrázek 2.3 Úvodní stránka – potvrzení úspěšného připojení.

C) Sledování síťového provozu

Sledování příchozí komunikace ve Wiresharku na VM3

- Přejděte na VM3.
- Otevřete nové terminálové okno a spusťte nástroj Wireshark:

```
sudo wireshark &
```

- Vyberte správné síťové rozhraní (např. `eth0`).
- Aplikujte vhodný filtr pro zachytávání komunikace probíhající přes síť Tor, např.:

```
tcp.port == 9001 || tcp.port == 443
```

- Spusťte zachytávání síťové komunikace na zvoleném rozhraní kliknutím na **Start Capturing**.
- V běžícím Tor Browseru na klientovi (VM1) se pokuste přistoupit na webovou stránku <https://whatismyipaddress.com> a sledujte průběh zaznamenané komunikace ve Wiresharku na monitorovacím zařízení (VM3). **Zaznamenejte si IP adresu zobrazenou stránkou.**

- Výsledkem by měl být záznam komunikace, ve kterém lze pozorovat velké množství TCP spojení, avšak **nebude možné dále analyzovat přenášený obsah**, a to konkrétně HTTP/HTTPS požadavky v čitelné podobě, jelikož se jedná o **šifrovaný přenos skrze vytvořenou síť Tor**. Věnujte pozornost **velikosti datových jednotek**.

Pozn.: standardní velikost Tor buňky je 512 B. Tato buňka je však následně zapouzdřena do TLS záznamu (TLS record), který kromě datové části (= Tor buňky) obsahuje i další řídicí informace. Z tohoto důvodu je možné vidět v záznamu komunikace jinou velikost datové jednotky (např. 590 B), důležitá je však její neměnnost v průběhu komunikace.

No.	Time	Source	Destination	Protocol	Length	Info
62	10.077992000	94.23.148.66	192.168.126.129	TCP	60	9800 → 57774 [ACK] Seq=5990 Ack=5323 Win=64240 Len=0
70	10.152799950	94.23.148.66	192.168.126.129	TLSv1.3	590	Application Data
71	10.156462772	192.168.126.129	94.23.148.66	TLSv1.3	590	Application Data
72	10.156627722	94.23.148.66	192.168.126.129	TCP	60	9800 → 57774 [ACK] Seq=6526 Ack=5859 Win=64240 Len=0
74	10.194594018	94.23.148.66	192.168.126.129	TLSv1.3	590	Application Data
75	10.196556267	192.168.126.129	94.23.148.66	TLSv1.3	590	Application Data
76	10.196556477	94.23.148.66	192.168.126.129	TCP	60	9800 → 57774 [ACK] Seq=7062 Ack=6395 Win=64240 Len=0
81	10.226632002	94.23.148.66	192.168.126.129	TLSv1.3	590	Application Data
82	10.228445962	192.168.126.129	94.23.148.66	TLSv1.3	590	Application Data
83	10.228446252	94.23.148.66	192.168.126.129	TCP	60	9800 → 57774 [ACK] Seq=7598 Ack=6931 Win=64240 Len=0
84	10.294087187	94.23.148.66	192.168.126.129	TLSv1.3	590	Application Data
85	10.294598838	192.168.126.129	94.23.148.66	TLSv1.3	590	Application Data
86	10.294598948	94.23.148.66	192.168.126.129	TCP	60	9800 → 57774 [ACK] Seq=8134 Ack=7467 Win=64240 Len=0

Frame 70: 590 bytes on wire (4720 bits), 590 bytes captured (4720 bits) on interface eth0, id 0
 Ethernet II, Src: VMware_f6:fa:ad (00:50:56:f6:fa:ad), Dst: VMware_b4:03:a2 (00:0c:29:b4:03:a2)
 Destination: VMware_b4:03:a2 (00:0c:29:b4:03:a2)
 Source: VMware_f6:fa:ad (00:50:56:f6:fa:ad)
 Type: IPv4 (0x0800)
 [Stream index: 1]
 Internet Protocol Version 4, Src: 94.23.148.66, Dst: 192.168.126.129
 Transmission Control Protocol, Src Port: 9800, Dst Port: 57774, Seq: 5990, Ack: 5323, Len: 536
 Transport Layer Security
 TLSv1.3 Record Layer: Application Data Protocol: Application Data
 Opaque Type: Application Data (23)
 Version: TLS 1.2 (0x0303)
 Length: 531
 Encrypted Application Data [...]: 532e4b8464a7bd6197ae318d77b04b67698c17ebcaa856b033a3a8077b7d4ce288b3816f498d6f5cdd8f97fc03554ae3b3

Obrázek 2.4 Ukázka zachycené komunikace: využití Tor Browseru pro anonymní prohlížení⁸.

- K ověření informací o přidělené IP adrese⁹ použijte službu **whois** a analyzujte zjištěné informace:

```
whois 193.189.100.201
```

IP adresa, kterou uvidíte na stránce jako např. whatismyipaddress.com, je **IP adresa výstupního Tor uzlu**, který kontaktuje cílový server na konci vytvořeného Tor okruhu. Cílový server tak nemá povědomí o tom, jaký konkrétní klient jej svým požadavkem kontaktoval, což názorně demonstruje způsob, jakým Tor umožňuje zajistit anonymitu klientů.

⁸ Ve výstupu můžete vidět komunikaci klienta s uzlem s IP adresou 94.23.148.66 – jedná se o IP adresu, která pravděpodobně patří jednomu z uzlů sítě Tor. Komunikace na portu 9000 je pro tuto síť typická. Tor standardně pro mezilehlé uzly (*relays*) využívá porty jako 9001, 9003 apod., avšak vzhledem k tomu, že síť Tor je dynamická a uzly se mohou měnit, je běžné, že klient naváže spojení s různými IP adresami na různých portech, jako například právě 9000, 9001 nebo 9003.

⁹ Při zadávání příkazu do terminálového okna použijte IP adresu přidělenou **vašemu klientovi na VM1**.

Time	192.168.126.129	94.23.148.66	Comment
9.748423723	57774 → 9000 [SYN] Seq=0 Win=0 Len=0	9000	TCP: 57774 → 9000 [SYN] Seq=0 Win=64240 Len=0 MSS
9.768111029	57774 ← 9000 [SYN, ACK] Seq=0 Ack=1 Win=64240	9000	TCP: 9000 → 57774 [SYN, ACK] Seq=0 Ack=1 Win=64240
9.768456270	57774 → 9000 [ACK] Seq=1 Ack=1 Win=64240 Len=0	9000	TCP: 57774 → 9000 [ACK] Seq=1 Ack=1 Win=64240 Len=0
9.781625301	57774 → 9000 [ACK] Seq=1 Ack=1 Win=64240 Len=0	9000	TCP: 57774 → 9000 [ACK] Seq=1 Ack=1 Win=64240 Len=0
9.781625351	57774 ← 9000 [ACK] Seq=1 Ack=518 Win=64240 Len=0	9000	TCP: 9000 → 57774 [ACK] Seq=1 Ack=518 Win=64240 Len=0
9.803170438	57774 → 9000 [ACK] Seq=518 Ack=1169 Win=65535 Len=0	9000	TCP: 57774 → 9000 [ACK] Seq=518 Ack=1169 Win=65535 Len=0
9.803452035	57774 ← 9000 [ACK] Seq=1169 Ack=598 Win=64240 Len=0	9000	TCP: 9000 → 57774 [ACK] Seq=1169 Ack=598 Win=64240 Len=0
9.810071096	57774 → 9000 [ACK] Seq=1169 Ack=631 Win=65535 Len=0	9000	TCP: 57774 → 9000 [ACK] Seq=1169 Ack=631 Win=65535 Len=0
9.810140880	57774 ← 9000 [ACK] Seq=1327 Ack=631 Win=65535 Len=0	9000	TCP: 9000 → 57774 [ACK] Seq=1327 Ack=631 Win=65535 Len=0
9.810585387	57774 → 9000 [ACK] Seq=1327 Ack=631 Win=65535 Len=0	9000	TCP: 57774 → 9000 [ACK] Seq=1327 Ack=631 Win=65535 Len=0
9.810585577	57774 ← 9000 [ACK] Seq=1327 Ack=631 Win=65535 Len=0	9000	TCP: 9000 → 57774 [ACK] Seq=1327 Ack=631 Win=65535 Len=0
9.829499085	57774 → 9000 [ACK] Seq=1327 Ack=631 Win=65535 Len=0	9000	TCP: 57774 → 9000 [ACK] Seq=1327 Ack=631 Win=65535 Len=0
9.848758025	57774 ← 9000 [ACK] Seq=1327 Ack=631 Win=65535 Len=0	9000	TCP: 9000 → 57774 [ACK] Seq=1327 Ack=631 Win=65535 Len=0
9.849586326	57774 → 9000 [ACK] Seq=1327 Ack=631 Win=65535 Len=0	9000	TCP: 57774 → 9000 [ACK] Seq=1327 Ack=631 Win=65535 Len=0
9.853747568	57774 ← 9000 [ACK] Seq=1327 Ack=631 Win=65535 Len=0	9000	TCP: 9000 → 57774 [ACK] Seq=1327 Ack=631 Win=65535 Len=0
9.873075962	57774 → 9000 [ACK] Seq=1327 Ack=631 Win=65535 Len=0	9000	TCP: 57774 → 9000 [ACK] Seq=1327 Ack=631 Win=65535 Len=0

Obrázek 2.5 *Flow Graph*¹⁰ komunikace mezi Tor klientem a vzdáleným serverem.

The screenshot shows the homepage of WhatIsMyIPAddress.com. The main content area displays the user's IP address as 193.189.100.201 (IPv4) and 2a0f:df00:0:255::201 (IPv6). Below this, it shows IP information including ISP (KeFF Networks Ltd), Services (Suspected Network, Sharing Device), City (Stockholm), Region (Stockholms lan), and Country (Sweden). A red button labeled 'HIDE MY IP ADDRESS NOW' is prominent. To the right, there is a map showing the location near Stockholm, Sweden, with a note 'Location not accurate? Update My IP Location'. The top navigation bar includes links for ABOUT, PRESS, PODCAST, and SUPPORT.

Obrázek 2.6 Tor klient: ukázka výstupu po přístupu na webové stránky whatismyipaddress.com - (přidělení IP adresy).

¹⁰ *Flow Graph* záznamu komunikace si můžete zobrazit přes volbu **Statistics > Flow Graph** v záhlaví panelu nástrojů hlavního okna nástroje Wireshark.

- Po zjištění IP adresy klienta s Tor (např. pomocí whatismyipaddress.com nebo z výpisu ve Wiresharku) ověřte, zda tato přidělená IP adresa skutečně náleží některému z výstupních uzlů sítě Tor pomocí některé z následujících stránek:
 - <https://www.dan.me.uk/tornodes> – webová stránka poskytuje aktuální seznam výstupních (*exit*) uzlů sítě Tor včetně jejich IP adres, portů a zemí. Nabízí možnosti filtrování a vyhledávání konkrétních adres.
 - <https://www.netify.ai/resources/tor> – webová stránka obsahuje podrobné informace o síti Tor, včetně její struktury, identifikace provozu a aktuálního seznamu výstupních uzlů.
- Pokud se přidělená IP adresa nachází v některém ze seznamů, jedná se skutečně o výstupní uzel (*exit node*). Všimněte si také dalších údajů, jako jsou země, port a název sítě. Tyto informace si zaznamenejte a porovnejte s výsledkem získaným pomocí služby `whois`.
- Otestujte funkčnost připojení na `.onion` adresu prostřednictvím prohlížeče Tor Browser – tyto adresy představují speciální domény určené pro webové služby dostupné pouze prostřednictvím anonymizované sítě Tor. Zajišťují anonymitu nejen uživatele, ale také cílového serveru. Jejich cílem je skrýt fyzické umístění služby a znemožnit běžné sledování provozu. V prohlížeči na klientovi s Tor (VM1) otevřete následující odkaz:

<https://duckduckgogg42xjoc72x3sjasowoarfbgcmvfimaftt6twagswzczad.onion/>
- Jedná se o speciální verzi vyhledávače DuckDuckGo pro síť Tor. Vyzkoušejte vyhledat klíčové slovo `"Tor exit node"` a sledujte, zda se načítají výsledky. Můžete také porovnat rychlost, strukturu a vzhled stránky se standardní verzí DuckDuckGo.

2.4. Samostatný úkol

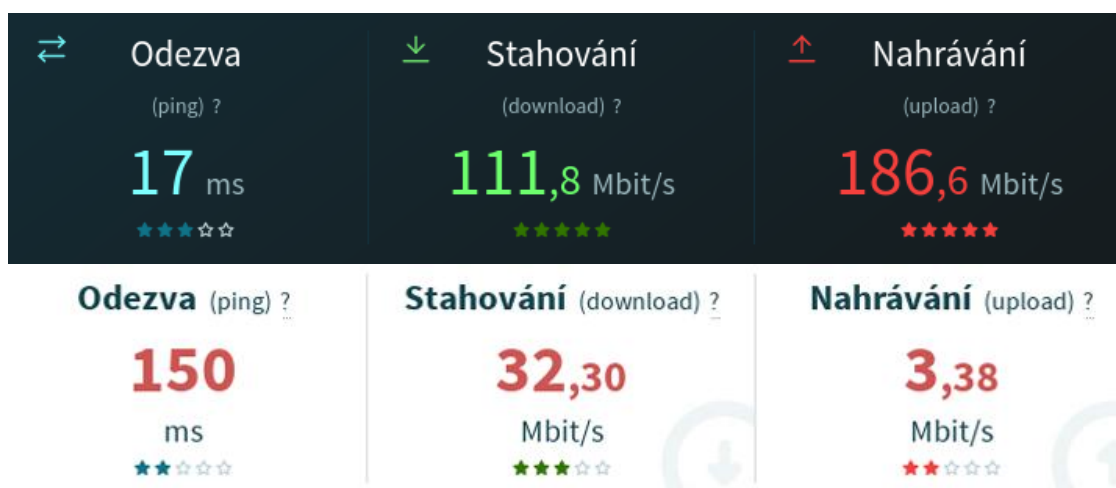
V závěrečné části laboratorního úkolu provedete **porovnání šifrované komunikace**, resp. přenosu datových jednotek standardním způsobem (tj. s využitím aplikačního protokolu HTTPS) a prostřednictvím sítě Tor. Na základě analýzy datové komunikace ve Wiresharku porovnáte rozdíly mezi uvedenými způsoby datového přenosu.

A) Cílem vaší samostatné práce bude s využitím VM2 (nového klienta) přistupovat k internetu „klasicky“ (tj. bez použití sítě Tor), kdy bude pro datový přenos použit protokol HTTP, resp. zabezpečený HTTPS, a následně porovnat zásadní rozdíly v anonymitě, struktuře přenosu, velikosti datových jednotek a viditelnosti dat při použití prohlížeče Tor Browser (sítě Tor) a běžného prohlížeče využívajícího připojení přes HTTPS.

B) Na základě záznamu komunikace ve Wiresharku analyzujte hlavní rozdíly v zabezpečení identity při použití Tor vs. klasického HTTPS připojení a porovnejte výhody, resp. nevýhody obou přístupů. Zároveň analyzujte rozdíly v IP adresách, které cílový server přidělí klientům na VM1 a VM2 (můžete využít nástroj whois).

C) Nakonec proveďte měření přenosové rychlosti a latence obou klientů. Doporučeno je využít stránku: <https://www.rychlost.cz>.

Sledujte parametry rychlosti stahování/odesílání a latenci (doba odezvy – ping), následně naměřené výsledky obou klientů vzájemně porovnejte.



Obrázek 2.7 Porovnání výsledků měření přenosových parametrů: klient bez Tor (nahore) vs. klient s Tor (dole).

3. Závěr

V tomto laboratorním úkolu jste se seznámili se základními principy fungování anonymizačních sítí a jejich významem pro ochranu soukromí a zachování anonymity uživatelů při komunikaci na internetu.

Prakticky jste si vyzkoušeli **instalaci Tor klienta** v systému Kali Linux a také použití **prohlížeče Tor Browser** speciálně přizpůsobeného pro anonymní prohlížení, navázání spojení přes síť Tor a rovněž anonymní prohlížení internetu. Součástí úkolu byla také analýza zachycené komunikace pomocí nástroje Wireshark, kde jste mohli sledovat fázi navazování spojení (*handshake*) se sítí Tor a následné šifrované přenosy dat. V rámci samostatného úkolu jste dále provedli **porovnání průběhu šifrované komunikace prostřednictvím protokolu HTTPS a komunikace odesílané právě přes anonymizační síť Tor** a sledovali významné rozdíly porovnáním obou uvedených přístupů. Při vzájemném porovnání jste rovněž provedli měření přenosových parametrů, během kterého jste mohli pozorovat delší dobu odezvy a nižší přenosové rychlosti při použití Tor.

3.1. Kontrolní otázky

1. Co je hlavním cílem využívání anonymizačních sítí?
 - A) Dosáhnout vysoké přenosové rychlosti komunikace
 - B) Zamezit identifikaci uživatele v celosvětové síti
 - C) Šifrovat komunikaci a zajistit důvěrnost přenosu mezi klientem a cílovým serverem
 - D) Zajistit anonymitu uživatele při přístupu k internetu
2. Na jakém principu funguje tzv. „cibulové směrování“ (*onion routing*)?
 - A) Každý mezilehlý uzel na cestě od klienta k serveru zná vždy celou trasu přenosu až k cíli
 - B) Data jsou šifrována v několika vrstvách a dešifrována postupně na každém uzlu
 - C) Každý uzel na přenosové trase musí znát IP adresu cílového serveru
 - D) Data jsou přenášena pomocí transportního protokolu UDP
3. Označte nesprávná tvrzení o mezilehlých uzlech přenosu (*Tor Nodes*):
 - A) Vstupní Tor uzel (*Entry Node*) je prvním bodem kontaktu mezi klientem a sítí Tor
 - B) Komunikují mezi sebou s využitím transportního protokolu UDP
 - C) Každý uzel zná IP adresu klienta
 - D) Tor *Exit Node* směřuje data na cílový server a zná IP adresu klienta

4. Které z následujících charakteristik platí pro Tor buňky (*cells*)?
- A) Mají pevně stanovenou velikost 512 bajtů
 - B) Vždy obsahují řídicí informace i uživatelská data
 - C) Přenos na transportní vrstvě zajišťuje protokol UDP
 - D) V záhlaví IP protokolu obsahují zdrojovou IP adresu klienta
5. Jaké rozdíly lze pozorovat mezi běžným HTTPS přístupem a přístupem přes Tor v nástroji Wireshark?
- A) V případě použití Tor jsou IP adresy výstupních uzlů odlišné od zdrojové IP adresy klienta
 - B) HTTPS nezahrnuje žádné mechanismy pro šifrování, Tor používá pro zajištění důvěrnosti přenosu TLS
 - C) Tor používá fixní velikost buněk
 - D) Tor umožňuje sledování zdrojové IP adresy klienta stejně jako HTTPS
6. Z jakého důvodu je připojení přes Tor obvykle pomalejší než přímé připojení k internetu?
- A) Data se přenášejí přes několik mezilehlých uzlů
 - B) Uživatel (klient) musí před odesláním dat tato data nejprve elektronicky podepsat pomocí asymetrického kryptosystému
 - C) Tor používá zastaralý kryptografický algoritmus
 - D) Každý meziuzel musí provést vícenásobné šifrovací (resp. dešifrovací) operace
7. Co je .onion adresa?
- A) Doména běžně dostupná při klasickém internetovém prohlížení
 - B) IP adresa výstupního uzlu sítě Tor
 - C) Speciální adresa určená pro skryté služby v síti Tor
 - D) Označuje cílovou službu, která je dostupná jen při znalosti IP adresy cílového serveru této služby
8. Na základě jakých znaků lze identifikovat ve Wiresharku, že komunikace probíhá prostřednictvím sítě Tor?
- A) Použitím filtru `tcp.port == 9001`
 - B) Vyhledáním EAPoL zpráv
 - C) Identifikací TLS paketů s fixní velikostí dat
 - D) Shodou zdrojových a cílových IP adres pro všechny pakety náležící ke stejnému datovému toku
9. Vyberte správná tvrzení o výstupním uzlu sítě Tor (*Exit Node*):
- A) Je posledním uzlem ve vytvořeném Tor okruhu
 - B) Odesílá dešifrovanou komunikaci na cílovou službu
 - C) Jako jediný zná IP adresu uživatele (klienta)
 - D) Zajišťuje TLS šifrování mezi klientem a serverem

10. Co je úlohou adresářového serveru v síti Tor?
- A) Zajišťuje šifrování přenosu dat mezi uzly v síti
 - B) Poskytuje IP adresy uživatelů v síti
 - C) Obsahuje informace o dostupných uzlech sítě Tor
 - D) Přidává nové vrstvy šifrování pro každou odeslanou Tor buňku
11. Jaké zásadní rozdíly jste pozorovali při měření rychlosti připojení přes anonymní síť Tor a bez použití Tor?
- A) Vyšší latenci přes Tor
 - B) Přenosová rychlost byla přibližně stejná
 - C) Nižší rychlost stahování při použití Tor
 - D) Nižší latenci přenosu v případě běžného připojení

4. Literatura

- [1] Dingledine, Roger, Mathewson, Nick and Syverson, Paul *Tor: The Second Generation Onion Router*. In: Paul Syverson, vol. 13, 2004. Dostupné z: <https://ieeexplore.ieee.org/document/10330539> [cit. 2024-12-02].
- [2] Rahman, Mohammad Saidur and Diadamo, Stephen and Mehic, Miralem and Fleming, Charles. *Quantum Secure Anonymous Communication Networks*. 2024. [online]. Dostupné z: https://www.researchgate.net/figure/Three-layer-encrypted-message-in-a-Tor-network_fig1_380600931 [cit. 2024-12-02].
- [3] MURDOCH, Steven J. a George DANEZIS. *Low-cost traffic analysis of Tor*. In: Proceedings of the 2005 IEEE Symposium on Security and Privacy. IEEE, 2005, s. 183–195. ISBN 0-7695-2339-0. [cit. 2025-04-25].
- [4] DINGLEDINE, Roger, Nick MATHEWSON a Paul SYVERSON. *Tor: The second-generation onion router*. In: Proceedings of the 13th USENIX Security Symposium. San Diego: USENIX Association, 2004, s. 303–320. Dostupné tiež z: <https://www.usenix.org/legacy/events/sec04/tech/dingledine.html>
- [5] MYRA SECURITY. *What is the Tor Network?* [online]. Myra Security, [cit. 2025-05-04]. Dostupné z: <https://www.myrasecurity.com/en/knowledge-hub/tor-network/>
- [6] PALLOTTI, Massimo a KULSHRESTHA, Mayank. *Tor Traffic in Enterprise Networks: Risks and Realities* [online]. Unit 42 – Palo Alto Networks, 2023. [cit. 2025-05-04]. Dostupné z: <https://unit42.paloaltonetworks.com/tor-traffic-enterprise-networks/>
- [7] TOR PROJECT. *Anonymity Online*. [online]. 2025 [cit. 2024-12-07]. Dostupné z: <https://www.torproject.org/>