

Dokumentace pro vyučujícího k laboratorní úloze

Laboratorní úloha č. 11

ANONYMIZAČNÍ SÍTĚ

1. Základní informace k laboratorní úloze

Laboratorní úloha č. 11 je zaměřena na využití anonymizačních sítí pro zachování anonymity a ochranu soukromí uživatele internetu, a to zejména na **praktické seznámení se s použitím anonymizační sítě Tor prostřednictvím specializovaného prohlížeče Tor Browser** v systému Kali Linux. Cílem úlohy je tedy prakticky demonstrovat princip fungování sítě Tor, včetně základní konfigurace, přístupu na web prostřednictvím sítě Tor a porovnání s běžnou komunikací využívající aplikační protokol HTTPS. Studenti si ověří, jakým způsobem v síti Tor probíhá anonymizace přenosu dat, jak funguje vícevrstvé šifrování (*onion routing*) a jaká omezení či rizika jsou spojena s jeho použitím.

2. Očekávané výstupy práce studentů

Praktická činnost studentů v rámci této úlohy spočívala ve vlastním testování možnosti anonymního prohlížení v prostředí Kali Linux díky použití prohlížeče Tor Browser. Úkolem studentů je provést potřebnou konfiguraci na zařízení klienta tak, aby bylo možné k přístupu na internet využít právě Tor Browser. Na základě záznamu komunikace ve Wiresharku studenti analyzují průběh datové komunikace odeslané přes anonymizační síť Tor. Studenti by měli být schopni vysvětlit základní principy a průběh „cibulového směrování“ v anonymizační síti.

Po spuštění a nakonfigurování virtuálních strojů studenti provedou instalaci a spuštění prohlížeče Tor (Tor Browser) na jednom ze strojů (klient VM1), připojí se k anonymizační síti a navštíví webové stránky pomocí sítě Tor. Na příslušném stroji spustí nástroj Wireshark pro monitorování komunikace a její následnou analýzu, přičemž se zaměří na datové přenosy využívající Tor SOCKS proxy a konkrétní porty jako 9001 a 9050 a prozkoumají aplikované vrstvy šifrování (*onion routing*).

2.1. Řešení samostatné úlohy

Samostatná úloha studentů přímo navazuje na praktickou část a jejím cílem je **porovnat průběh datové komunikace s webovým serverem přes aplikační protokol HTTPS a šifrované komunikace přes síť Tor**. Pro tento účel mohou studenti využít další VM, který mají ve VMware k dispozici. Studenti budou pracovat se dvěma klientskými koncovými zařízeními, přičemž jeden klient bude k přístupu na internet a prohlížení webových stránek, konkrétně na stránku: <https://www.whatismyipaddress.com>, využívat protokol HTTPS, druhý bude přistupovat na internet prostřednictvím sítě Tor.

S využitím nástroje Wireshark porovnájí oba přístupy, přičemž se zaměří na hlavní rozdíly související s ochranou soukromí a anonymitou uživatelů, a také na rozdíly v šifrování přenášeného datového obsahu souvisejícího se zajištěním důvěrnosti probíhající komunikace. Studenti porovnájí rozdíly v přenášených informacích, velikosti

přenášených datových jednotek, obsahu jejich záhlaví, IP adresách komunikujících uzlů, šifrování a časové odezvě. Na vlastním příkladu zachycené komunikace ve Wiresharku studenti demonstrují zásadní rozdíly v podobě přenášených paketů, jako jsou např. skrytá, resp. šifrovaná IP adresa při přenosu přes síť Tor, viditelná, resp. nešifrovaná IP adresa při přenosu přes HTTPS apod.

Studenti by měli po zpracování samostatné úlohy dospět k následujícím závěrům:

- **Zobrazená IP adresa na stránce:** klient bez Toru (VM2) uvidí svou reálnou (univerzitní) veřejnou IP adresu z rozsahu akademické počítačové sítě CESNET, Tor klient (VM1) uvidí IP adresu výstupního uzlu sítě Tor.
- **WHOIS informace o přidělené IP adrese:** IP bez Toru bude registrována na akademickou nebo veřejnou instituci (např. CESNET, SANET), IP adresa výstupního uzlu Tor sítě bude patřit soukromému poskytovateli VPS nebo anonymnímu hostingu (např. QuxLabs, OVH), často v jiné zemi.
- **Analýza komunikace ve Wiresharku:** v komunikaci klienta bez Toru (VM2) jsou viditelné standardní HTTPS požadavky směřované přímo na cílový server, u Tor klienta komunikace směřuje nejprve na IP adresu výstupního uzlu a využívá porty typické pro Tor (např. 9000).
- **Velikosti přenášených dat:** v síti Tor jsou přenášeny Tor buňky s konstantní velikostí 512 bajtů na úrovni TLS *payload*, což snižuje možnost analýzy podle velikosti dat, bez použití Toru velikosti přenášených paketů závisí na konkrétních datech a mohou být během komunikace proměnlivé.
- **Viditelné IP adresy ve Wiresharku:** v komunikaci klienta bez Toru (VM2) je jasně viditelná cílová IP adresa navštívené webové stránky, naopak při komunikaci přes síť Tor je skutečný cíl spojení skryt – Tor klient (VM1) komunikuje pouze s IP adresou výstupního uzlu Toru.
- **Šifrování:** v obou případech je použito HTTPS, ale Tor navíc šifruje celou trasu mezi klientem a výstupním uzlem (aplikuje vícenásobné šifrování).

Při měření dosažené přenosové rychlosti a latence datových přenosů obou klientů by studenti měli pozorovat, že klient s Torem (VM1) bude mít výrazně nižší přenosovou rychlost a vyšší latenci než klient bez Toru (VM2). Důvodem je struktura sítě Tor, kdy každá odeslaná datová jednotka je několikanásobně šifrována a prochází přes několik mezilehlých uzlů (Tor směrovačů). Použitý způsob směrování a vícevrstvého šifrování (*onion routing*) výrazně zpomaluje přenos a zvyšuje odezvu.

Dalším faktorem, který může měření ovlivnit, je skutečnost, že některé testovací stránky nemusí být optimalizovány pro použití Toru a mohou vykazovat nestabilní výsledky.

2.2. Odpovědi na 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 meziuzel 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 směruje 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 ☒

2.3. Doplnující otázky

Níže uvedené otázky mohou být využity při kontrole výstupů samostatné práce studentem s cílem ověřit, zda skutečně porozuměli řešené problematice v praktické části laboratorní úlohy.

1. Vysvětlete, co je anonymizační síť a jaký je hlavní účel jejího použití.

- Anonymizační síť představuje technologii určenou k zajištění ochrany soukromí a anonymity uživatelů během jejich online aktivity v prostředí internetu. Jejím hlavním cílem je utajit IP adresu koncového uživatele a směřovat veškerou jeho komunikaci přes více zprostředkovatelů (mezilehlých uzlů) tak, aby nebylo možné v žádném bodě přenosu jednoznačně identifikovat původce (a případně i adresáta) odeslané datové jednotky.

2. Popište princip „cibulového směrování“ v síti Tor.

- Síť Tor funguje na principu tzv. *onion routingu*, tedy mechanismu šifrování spočívajícím ve vícenásobném šifrování přenášených dat, která jsou během přenosu postupně dešifrována na jednotlivých mezilehlých uzlech. Data jsou odeslána přes sérii uzlů, přičemž každý uzel dokáže dešifrovat pouze jednu („vnější“) vrstvu, a tím zná pouze předchozí a následující uzel, což je základní předpoklad pro zajištění anonymity koncového uživatele.

3. Jaká je úloha *Entry Node* a *Exit Node* v Tor síti?

- *Entry Node* (vstupní uzel) je první bod v síti Tor, který přijímá zašifrovaná data od klienta. *Exit Node* (výstupní uzel) je poslední uzel, který data dešifruje a odesílá je na cílový server. *Entry Node* zná IP adresu klienta, ale nezná adresáta komunikace. Naopak *Exit Node* zná cílovou IP adresu (adresáta), ale nikoli původce dat.

4. Jakým způsobem dochází k zajištění anonymity uživatele při využití anonymizační sítě?

- Anonymita je dosažena vrstvením šifrování a směrováním komunikace přes několik uzlů, kdy každý zná pouze část přenosové trasy. Tím se znemožní sledování celé komunikace, včetně jednoznačného určení koncových bodů přenosu.

5. Jaké jsou hlavní výhody a nevýhody používání sítě Tor?

- Výhody: vysoká úroveň anonymity uživatele, ochrana před sledováním, ochrana soukromí koncového uživatele.
- Nevýhody: nižší přenosová rychlost, možné blokování některých služeb, riziko kompromitace výstupních uzlů, omezená podpora některých aplikací.

6. Pomocí jakého filtru ve Wiresharku je možné zobrazit pouze komunikaci přenášenou anonymizační sítí Tor? Existuje konkrétní filtr pro zobrazení zpráv (resp. buněk) Tor protokolu?

- Komunikace v anonymizační síti Tor sice nevyužívá žádný konkrétní aplikační protokol označený např. jako „tor“, který by sloužil přímo k zajištění anonymity uživatelů, ale je možné použít vhodné filtry pro filtrování komunikace na úrovni transportní vrstvy. Příklady možného filtrování zachycené komunikace na základě portů:

```
tcp.port == 9001 || tcp.port == 9050 || tcp.port == 443
```

(pokud je využíván i HTTPS)

7. Demonstrujte na praktickém příkladu (můžete využít např. část zaznamenané komunikace ve Wiresharku) rozdíly mezi běžnou šifrovanou HTTPS komunikací a komunikací přes síť Tor.

- V případě šifrované komunikace přes HTTPS je ve Wiresharku zřejmá IP adresa klienta i cílového serveru, zatímco při přenosu přes Tor nejsou IP adresy koncových zařízení na jednotlivých uzlech sítě viditelné, resp. nejsou přenášeny IP hlavičky v otevřené, čitelné podobě.

8. Jaké rozdíly lze pozorovat při měření rychlosti připojení mezi klientem používajícím Tor a klientem bez Tor? Uveďte hlavní důvod tohoto rozdílu.

- Klient používající Tor (VM1) bude mít nižší přenosovou rychlost a vyšší latenci. Důvodem je, že Tor směruje šifrovanou komunikaci přes více mezilehlých uzlů, což způsobuje zpoždění a snižuje dosaženou přenosovou rychlost a celkovou propustnost spojení.

9. Z jakého rozsahu byla přidělena IP adresa klientovi bez použití Toru (VM2)?

- IP adresa klienta bez Toru (VM2) byla přidělena z veřejného rozsahu sítě organizace CESNET, konkrétně se jedná o rozsah 147.251.0.0/16, který je registrován pro Vysoké učení technické v Brně (VUT v Brně).