

# **Dokumentácia pre vyučujúceho k laboratórnej úlohe**

Laboratórna úloha č. 11

## **ANONYMIZAČNÉ SIETE**

# 1. Základné informácie k laboratórnej úlohe

Laboratórna úloha č. 11 je venovaná použitiu anonymizačných sietí pre zachovanie anonymity a ochranu súkromia používateľa internetu, a to najmä **na praktické zoznámenie sa s využitím anonymizačnej siete Tor prostredníctvom špecializovaného prehliadača Tor Browser** v Kali Linux. Cieľom úlohy je teda prakticky demonštrovať princíp fungovania siete Tor, vrátane základnej konfigurácie, prístupu na web prostredníctvom siete Tor a porovnania s bežnou komunikáciou využívajúcou aplikačný protokol HTTPS. Študenti si overia, akým spôsobom v sieti Tor prebieha anonymizácia prenosu dát, ako funguje viacvrstvové šifrovanie (*onion routing*) a aké obmedzenia alebo riziká sa viažu na jeho použitie.

## 2. Očakávané výstupy práce študentov

Praktická činnosť študentov v rámci tejto úlohy spočívala vo vlastnom testovaní možnosti anonymného prehliadania v prostredí Kali Linux vďaka použitiu prehliadača Tor Browser. Úlohou študentov je uskutočniť potrebnú konfiguráciu na zariadení klienta tak, aby bolo možné pre prístup k internetu využiť práve Tor Browser. Na základe záznamu komunikácie na Wiresharku študenti analyzujú priebeh dátovej komunikácie odoslanej cez anonymizačnú sieť Tor. Študenti by mali byť schopní vysvetliť základné princípy a priebeh „cibuľového smerovania“ v anonymizačnej sieti.

Po spustení a nakonfigurovaní virtuálnych strojov študenti vykonajú inštaláciu a spustenie Tor prehliadača (Tor Browser) na jednom zo strojov (klient VM1), pripoja sa k anonymizačnej sieti a prístupia na webové stránky pomocou Tor. Na príslušnom stroji spustia nástroj Wireshark pre monitorovanie komunikácie a jej následnú analýzu, pričom sa zamerajú na dátové prenosy využívajúce Tor SOCKS proxy a konkrétne porty ako 9001 a 9050 a preskúmajú aplikované vrstvy šifrovania (*onion routing*).

### 2.1. Riešenie samostatnej úlohy

Samostatná úloha študentov priamo nadväzuje na praktickú časť a jej cieľom je **porovnať priebeh dátovej komunikácie s webovým serverom cez aplikačný protokol HTTPS a šifrovanej komunikácie cez Tor sieť**. Pre tento účel môžu študenti využiť ďalší VM, ktorý majú vo VMware k dispozícii. Študenti budú pracovať s dvoma klientskymi koncovými zariadeniami, pričom jeden klient bude pre prístup k internetu a webové prehliadanie, konkrétne na webovú stránku: <https://www.whatismyipaddress.com>, využívať protokol HTTPS, druhý bude na internet pristupovať prostredníctvom siete Tor. S využitím nástroja Wireshark porovnajú oba prístupy, pričom sa zamerajú na hlavné rozdiely súvisiace s ochranou súkromia a anonymity používateľov a tiež na rozdiely v šifrovaní prenášaného dátového obsahu súvisiaceho so zaistením dôvernosti prebiehajúcej komunikácie. Študenti porovnajú rozdiely v prenášaných informáciách,

veľkosti prenášaných dátových jednotiek, obsahu ich záhlaví, IP adresách komunikujúcich uzlov, šifrovaní a časovej odozve. Na vlastnom príklade zachytenej komunikácie vo Wiresharku študenti demonštrujú zásadné rozdiely v podobe prenášaných paketov ako sú napr. skrytá, resp. šifrovaná IP adresa pri prenose cez sieť Tor, viditeľná, resp. nešifrovaná IP adresa pri prenose cez HTTPS apod.

Študenti by mali po spracovaní samostatnej úlohy dospieť k nasledujúcim záverom:

- **Zobrazená IP adresa na stránke:** klient bez Toru (VM2) uvidí svoju reálnu (univerzitnú) verejnú IP adresu z rozsahu akademickej počítačovej siete CESNET, Tor klient (VM1) uvidí IP adresu výstupného uzla Tor siete.
- **WHOIS informácie o pridelení IP adrese:** IP bez Toru bude registrovaná na akademickú alebo verejnú inštitúciu (napr. CESNET, SANET), IP adresa výstupného Tor uzla bude patriť súkromnému poskytovateľovi VPS alebo anonymnému hostingu (napr. QuxLabs, OVH), často v inej krajine.
- **Analýza komunikácie vo Wiresharku:** v komunikácii klienta bez Toru (VM2) sú viditeľné štandardné HTTPS požiadavky smerované priamo na cieľový server, pri Tor klientovi komunikácia smeruje najskôr na IP adresu výstupného uzla a využíva porty typické pre Tor (napr. 9000).
- **Veľkosti prenášaných dát:** v Tor sieti sú prenášané Tor bunky s konštantnou veľkosťou 512 bajtov na úrovni TLS *payload*, čo znižuje možnosť analýzy pomocou veľkosti dát, bez použitia Toru veľkosti prenášaných paketov závisia od konkrétnych dát a môžu byť počas komunikácie premenlivé.
- **Viditeľné IP adresy vo Wiresharku:** v komunikácii klienta bez Toru (VM2) je jasne viditeľná cieľová IP adresa navštívenej webovej stránky, naopak pri komunikácii cez Tor sieť nie je skutočný cieľ spojenia zrejmý – Tor klient (VM1) komunikuje iba s IP adresou výstupného uzla Toru.
- **Šifrovanie:** v oboch prípadoch je použité HTTPS, ale Tor navyše šifruje celú trasu medzi klientom a výstupným uzlom (aplikuje viacnásobné šifrovanie).

Pri meraní dosiahnutých prenosových rýchlostí a latencie dátových prenosov oboch klientov by mali študenti pozorovať, že klient s Torom (VM1) bude mať výrazne nižšiu prenosovú rýchlosť a vyššiu latenciu než klient bez Toru (VM2). Dôvodom je štruktúra Tor siete, kedy každá odoslaná dátová jednotka je niekoľkonásobne šifrovaná a prechádza cez niekoľko medzilahlých uzlov (Tor smerovačov). Použitý spôsob smerovania a viacvrstvového šifrovania (*onion routing*) výrazne spomaľuje prenos a zvyšuje odozvu.

Ďalší faktor, ktorý môže merania ovplyvniť, je skutočnosť, že niektoré testovacie stránky nemusia byť optimalizované pre použitie Tor a môžu vykazovať nestabilné výsledky.

## 2.2. Odpovede na kontrolné otázky

1. Čo je hlavným cieľom využívania anonymizačných sietí?
  - A) Dosiahnuť vysokú prenosovú rýchlosť komunikácie
  - B) Zamedziť identifikácii používateľa v celosvetovej sieti ☒
  - C) Šifrovať komunikáciu a zabezpečiť dôvernosť prenosu medzi klientom a cieľovým serverom
  - D) Zaistiť anonymitu používateľa pri prístupe k internetu ☒
2. Na akom princípe funguje tzv. „cibuľové smerovanie“ (*onion routing*)?
  - A) Každý medziľahlý uzol na ceste od klienta k serveru pozná vždy celú trasu prenosu až k cieľu
  - B) Dáta sú šifrované v niekoľkých vrstvách a dešifrované postupne na každom uzle ☒
  - C) Každý uzol na prenosovej trase musí poznať IP adresu cieľového servera
  - D) Dáta sú prenášané pomocou transportného protokolu UDP
3. Označte nesprávne tvrdenia o medziľahlých uzloch prenosu (*Tor Nodes*):
  - A) Vstupný Tor uzol (*Entry Node*) je prvým bodom kontaktu medzi klientom a Tor sieťou
  - B) Komunikujú medzi sebou s využitím transportného protokolu UDP ☒
  - C) Každý uzol pozná IP adresu klienta ☒
  - D) Tor Exit Node smeruje dáta na cieľový server a pozná IP adresu klienta ☒
4. Ktoré z nasledujúcich charakteristík platia pre Tor bunky (*cells*)?
  - A) Majú pevne stanovenú veľkosť 512 bajtov ☒
  - B) Vždy obsahujú riadiace aj dátové informácie
  - C) Ich prenos na transportnej vrstve zabezpečuje protokol UDP
  - D) V záhlaví IP protokolu obsahujú zdrojovú IP adresu klienta
5. Aké rozdiely možno pozorovať medzi bežným HTTPS prístupom a prístupom cez Tor v nástroji Wireshark?
  - A) V prípade použitia Tor sú IP adresy výstupných uzlov odlišné od zdrojovej IP adresy klienta ☒
  - B) HTTPS nezahŕňa žiadne mechanizmy pre šifrovanie, Tor používa pre zaistenie dôvernosti prenosu TLS
  - C) Tor používa fixnú veľkosť buniek ☒
  - D) Tor umožňuje sledovanie zdrojovej IP adresy klienta rovnako ako HTTPS

6. Z akého dôvodu je pripojenie cez Tor zvyčajne pomalšie než priame pripojenie k internetu?
- A) Dáta sa prenášajú cez niekoľko medziľahlých uzlov ☒
  - B) Používateľ (klient) musí pred odoslaním dát tieto dáta najskôr elektronicky podpísať pomocou asymetrického kryptosystému
  - C) Tor používa zastaraný kryptografický algoritmus
  - D) Každý medziľahlý uzol musí uskutočniť viacnásobné operácie šifrovania (resp. dešifrovania) ☒
7. Čo je .onion adresa?
- A) Doména bežne dostupná pri klasickom internetovom prehliadaní
  - B) IP adresa výstupného uzla Tor siete
  - C) Špeciálna adresa určená pre skryté služby v sieti Tor ☒
  - D) Označuje cieľovú službu, ktorá je dostupná len pri znalosti IP adresy cieľového servera tejto služby
8. Na základe akých znakov je možné identifikovať vo Wiresharku, že komunikácie prebieha prostredníctvom Tor siete?
- A) Použitím filtra tcp.port == 9001 ☒
  - B) Vyhľadáním EAPoL správ
  - C) Identifikáciou TLS paketov s fixnou veľkosťou dát ☒
  - D) Zhodou zdrojových a cieľových IP adries pre všetky pakety prislúchajúce k rovnakému dátovému toku
9. Vyberte správne tvrdenia o výstupnom uzle Tor siete (Exit Node):
- A) Je posledným uzlom vo vytvorenom Tor okruhu ☒
  - B) Odosiela dešifrovanú komunikáciu na cieľovú službu ☒
  - C) Ako jediný pozná IP adresu používateľa (klienta)
  - D) Zabezpečuje TLS šifrovanie medzi klientom a serverom
10. Čo je úlohou adresárového servera v sieti Tor?
- A) Zabezpečuje šifrovanie prenosu dát medzi uzlami v sieti
  - B) Poskytuje IP adresy užívateľov v sieti
  - C) Obsahuje informácie o dostupných Tor uzloch ☒
  - D) Pridáva nové vrstvy šifrovania pre každú odoslanú Tor bunku
11. Aké zásadné rozdiely ste pozorovali pri meraní rýchlosti pripojenia cez anonymnú sieť Tor a bez použitia Tor?
- A) Vyššiu latenciu cez Tor ☒
  - B) Prenosovú rýchlosť bola približne rovnaká
  - C) Nižšiu rýchlosť downloadu pri použití Tor ☒
  - D) Nižšiu latenciu prenosu v prípade bežného pripojenia ☒

## 2.3. Dopĺňujúce otázky

Nižšie uvedené otázky môžu byť využité pri kontrole výstupov samostatnej práce študentom s cieľom overiť, či skutočne porozumeli riešenej problematike v praktickej časti laboratórnej úlohy.

### 1. Vysvetlite, čo je anonymizačná sieť a aký je hlavný účel jej použitia.

- Anonymizačná sieť predstavuje technológie určenú k zaistieniu ochrany súkromia a anonymity používateľov počas ich online aktivity v prostredí internetu. Jej hlavným cieľom je utajiť IP adresu koncového používateľa a smerovať všetku jeho komunikáciu cez viacero sprostredkovateľov (medziľahlých uzlov) tak, aby nebolo možné v žiadnom bode prenosu jasne identifikovať pôvodcu (a príp. i adresáta) zaslanej dátovej jednotky.

### 2. Popíšte princíp „cibuľového smerovania“ v sieti Tor.

- Sieť Tor pracuje na princípe tzv. *onion routing*, t. j. mechanizme šifrovania spočívajúcom vo viacnásobnom šifrovaní prenášaných dát, ktoré sú počas prenosu postupne dešifrované na jednotlivých medziľahlých uzloch. Dáta sú odoslané cez sériu uzlov, pričom každý uzol dokáže dešifrovať len jednu („vonkajšiu“) vrstvu, čím pozná len predchádzajúci a nasledujúci uzol, čo je základný predpoklad k tomu, aby mohla byť zaistená anonymita koncového používateľa.

### 3. Čo je úlohou *Entry Node* a *Exit Node* v Tor sieti?

- *Entry Node* (vstupný uzol) je prvý bod v Tor sieti, ktorý prijíma zašifrované dáta od klienta. *Exit Node* (výstupný uzol) je posledný uzol, ktorý dáta dešifruje a posiela ich na cieľový server. *Entry Node* pozná IP klienta, ale nemá vedomosť o tom, kto je cieľovým adresátom komunikácie. Naopak *Exit Node* pozná cieľovú IP adresu (t. j. adresáta), ale nie pôvodcu dát.

### 4. Akým spôsobom dochádza k zaistieniu anonymity používateľa pri využití anonymizačnej siete?

- Anonymita je dosiahnutá vrstvením šifrovania a smerovaním komunikácie cez niekoľko uzlov, kde každý pozná len časť prenosovej trasy. Tým sa znemožní sledovanie úplnej komunikácie, vrátane jednoznačného určenia koncových bodov komunikácie.

### 5. Aké sú hlavné výhody a nevýhody používania siete Tor?

- Výhody: vysoká úroveň anonymity používateľa, ochrana pred sledovaním ochrana súkromia koncového užívateľa.
- Nevýhody: nižšia rýchlosť prenosu, potenciálne nežiadúce blokovanie niektorých služieb, možnosť kompromitácie výstupných uzlov, obmedzená podpora niektorých aplikácií.

**6. Pomocou akého filtra vo Wiresharku je možné zobrazit' len komunikáciu prenášanú anonymizačnou sieťou Tor? Existuje konkrétny filter pre zobrazenie správ (resp. buniek) Tor protokolu?**

- Komunikácia v anonymizačnej sieti Tor síce nevyužíva žiadny konkrétny aplikačný protokol označený napr. ako "tor", ktorý by slúžil práve pre potreby zaistenia anonymity užívateľov, ale je možné použiť vhodné filtre pre filtrovanie komunikácie na úrovni transportnej vrstvy. Príklady možného filtrovania zachytenej komunikácie na základe portov:

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

*(ak sa používa aj HTTPS)*

**7. Demonštrujte na praktickom príklade (môžete využiť napr. časť zaznamenananej komunikácie vo Wiresharku) rozdiely medzi bežnou šifrovanou HTTPS komunikáciou a komunikáciou cez sieť Tor.**

- V prípade šifrovanej komunikácie cez HTTPS je vo Wiresharku zrejmé IP adresa klienta aj cieľového servera, zatiaľ čo pri prenose cez Tor nie sú IP adresy koncových zariadení na jednotlivých uzloch siete viditeľné, resp. nie sú prenášané IP záhlaví v otvorenej, čitateľnej podobe.

**8. Aké rozdiely možno pozorovať pri meraní rýchlosti pripojenia medzi klientom používajúcim Tor a klientom bez Tor? Uveďte hlavný dôvod tohto rozdielu.**

- Klient používajúci Tor (VM1) bude mať nižšiu prenosovú rýchlosť a vyššiu latenciu. Dôvodom je, že Tor smeruje šifrovanú komunikáciu cez viacero medziľahlých uzlov, čo má za následok vznik oneskorenia a zníženie dosiahnutej prenosovej rýchlosti a celkovej priepustnosti spojenia.

**9. Z akého rozsahu bola pridelená IP adresa klientovi bez použitia Toru (VM2)?**

- IP adresa klienta bez Toru (VM2) bola pridelená z verejného rozsahu siete organizácie CESNET, konkrétne ide o rozsah 147.251.0.0/16, ktorý je registrovaný pre Vysoké učení technické v Brně (VUT v Brně).