VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ
ÚSTAV TELEKOMUNIKACÍ

FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION
DEPARTMENT OF TELECOMMUNICATIONS

ANALÝZA SKRYTÉ SLUŽBY V SÍTI TOR

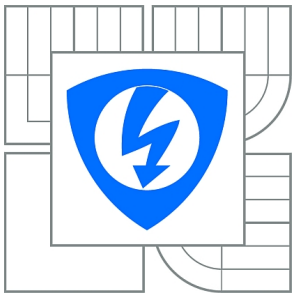
BAKALÁŘSKÁ PRÁCE
BACHELOR'S THESIS

AUTOR PRÁCE VLADIMÍR MESÍK
AUTHOR

BRNO 2015

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

BRNO UNIVERSITY OF TECHNOLOGY



FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ

ÚSTAV TELEKOMUNIKACÍ

FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION

DEPARTMENT OF TELECOMMUNICATIONS

ANALÝZA SKRYTÉ SLUŽBY V SÍTI TOR

THE ANALYSIS OF TOR'S HIDDEN SERVICE

BAKALÁŘSKÁ PRÁCE

BACHELOR'S THESIS

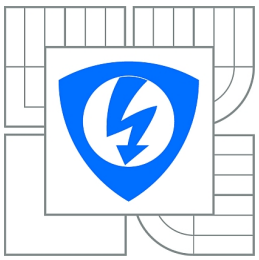
AUTOR PRÁCE — VLADIMÍR MESÍK

AUTHOR

VEDOUCÍ PRÁCE — Ing. MARTIN ROSENBERG

SUPERVISOR

BRNO 2015



VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

Fakulta elektrotechniky a komunikačních technologií

Ústav telekomunikací

Bakalářská práce

bakalářský studijní obor
Teleinformatika

Student: Vladimír Mesík ***ID:*** 146060
Ročník: 3 ***Akademický rok:*** 2014/2015

NÁZEV TÉMATU:

Analýza skryté služby v síti TOR

POKYNY PRO VYPRACOVÁNÍ:

Cílem bakalářské práce je podrobný popis funkčnosti a bezpečnosti serverů Hidden Service (Skrytá služba) pracujících v anonymní síti TOR (The Onion Routing). Student detailně popíše principy sítě, nakonfiguruje vlastní server a zaměří se na možnosti, které mohou vést k cílenému nebo náhodnému odhalení identity serveru a klienta. Výstupem práce bude nakonfigurovaný anonymní server určený pro úschovu a sdílení dat. Student vytvoří dvě laboratorní úlohy zaměřené na konfiguraci a bezpečnost Hidden Service.

DOPORUČENÁ LITERATURA:

PENG, Kun. Anonymous communication networks: protecting privacy on the web. 2014. ISBN 14-398-8157-X.

HENDERSON, Lance. Anonymous File Sharing & Darknet: How to be a Ghost in the Machine. CreateSpace Independent Publishing Platform, 2013. ISBN 1482323990.

Termín zadání: 9.2.2015 ***Termín odevzdání:*** 2.6.2015

Vedoucí práce: Ing. Martin Rosenberg
Konzultanti bakalářské práce:

doc. Ing. Jiří Mišurec, CSc.
Předseda oborové rady

UPOZORNĚNÍ:

ABSTRAKT

Táto práca sa zaoberá anonymitou v informačnej dobe, princípom cibuľového smerovania, anonymnou sieťou Tor a princípom fungovania skrytej služby v sieti Tor. Analyzuje bezpečnosť, anonymitu a možnosť deanonymizácie servera skrytej služby, riziko odhalenia jeho skutočnej IP adresy. Popisuje vybrané typy útokov na siet Tor s cieľom deanonymizácie. V praktickej časti popisuje postup inštalácie a konfigurácie skrytej služby v sieti Tor pod linuxom. Záverom praktickej časti je funkčný .onion server skrytej služby s možnosťou anonymného ukladania a zdielania súborov. Súčasťou práce je zostavenie dvoch laboratórnych úloh zameraných na konfiguráciu servera skrytej služby a zabezpečenia jeho anonymity spolu s bezpečnostnými pravidlami týkajúcich sa prevádzkovania skrytej služby.

KĽÚČOVÉ SLOVÁ

anonymná sieť Tor, skrytá služba v sieti Tor, analýza sieťovej komunikácie, cibuľové smerovanie, deanonymizácia siete Tor, útoky proti sieti Tor, bezpečnostné pravidlá v sieti Tor.

ABSTRACT

This work deals with problems concerning anonymity in the internet age, the principle of onion routing, Tor network, Tor's Hidden Service protocol. Analyzing security, anonymity and the possibility of Hidden Services deanonymisation, revealing the actual IP address of hidden service server. It describes selected types of attacks against Tor network in order to deanonymisation of nodes and hidden services. The practical part describes the process of installing and configuring hidden services under Linux. The final part of the practical part is operational and running .onion hidden service with anonymous service for file storing and sharing. Part of the work is the development of two laboratory tasks aimed at the server configuration and its security.

KEYWORDS

anonymous Tor network, hidden service, network traffic analysis, onion routing, deanonymisation of Tor network, attacks against Tor.

MESÍK, Vladimír *Analýza skryté služby v síti TOR*: bakalárska práca. Brno: Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, Ústav telekomunikací, 2015. 52 s. Vedúci práce bol Ing. Martin Rosenberg,

PREHLÁSENIE

Prehlasujem, že som svoju bakalársku prácu na tému „Analýza skryté služby v síti TOR“ vypracoval(a) samostatne pod vedením vedúceho bakalárskej práce, využitím odbornej literatúry a ďalších informačných zdrojov, ktoré sú všetky citované v práci a uvedené v zozname literatúry na konci práce.

Ako autor(ka) uvedenej bakalárskej práce ďalej prehlasujem, že v súvislosti s vytvorením tejto bakalárskej práce som neporušil(a) autorské práva tretích osôb, najmä som nezasiahol(-la) nedovoleným spôsobom do cudzích autorských práv osobnostných a/nebo majetkových a som si plne vedomý(-á) následkov porušenia ustanovenia § 11 a nasledujúcich autorského zákona č. 121/2000 Sb., o právu autorském, o právoch súvisejúcich s právom autorským a o zmeně niektorých zákonov (autorský zákon), vo znení neskorších predpisov, vrátane možných trestnoprávnych dôsledkov vyplývajúcich z ustanovenia časti druhé, hlavy VI. diel 4 Trestného zákoníka č. 40/2009 Sb.

Brno ....

podpis autora(-ky)

POĎAKOVANIE

Rád by som poďakoval vedúcemu bakalárskej práce pánovi Ing. Martinovi Rosenbergovi za odborné vedenie, konzultácie, trpezlivosť a podnetné návrhy k práci.

Brno ....

podpis autora(-ky)

Faculty of Electrical Engineering
and Communication
Brno University of Technology
Purkynova 118, CZ-61200 Brno
Czech Republic
http://www.six.feec.vutbr.cz

POĎAKOVANIE

Výzkum popsaný v tejto bakalárskej práci bol realizovaný v laboratóriách podporených projektom SIX; registračné číslo CZ.1.05/2.1.00/03.0072, operačný program Výzkum a vývoj pro inovace.

Brno . . . . . .

. . . . . .
podpis autora(-ky)

OBSAH

ZOZNAM OBRÁZKOV

ÚVOD

Bez Internetu si v dnešnej dobe nevieme predstaviť život. Stal sa našou súčasťou, bez neho sa cítime nekompletní a stratení. Vďaka Internetu máme okamžitý prístup ku zdanlivo nekonečnému zdroju informácií, pričom ich množstvo rastie každým dňom. Neaktuálne informácie sú nahrádzané aktuálnymi. Doba potrebná na distribúciu týchto informácií je minimálna, vďaka čomu sa internet stal tak populárnym. V momente tragédie o nej vie celý svet, nakoľko nadviazanie komunikácie medzi dvoma kontinentmi trvá len pár sekúnd. Prekonávanie neprekonateľného sa stalo každodennou realitou.

Na prvý pohľad sa Internet môže javiť ako bezpečné, priam anonymné miesto. Niektorí ho považujú za útočisko, iní za nástroj skazy. Naše fyzické proporcie, rysy tváre, vek či hlas, ostávajú pri komunikácií skryté, dávajúc nám mylný pocit súkromia a bezpečia. V bežnom živote si väčšina ľudí svoje súkromie dobre chráni a dôležité informácie zdieľajú len so svojimi najbližšími. Vo virtuálnom svete to ale neplatí, nakoľko používaním Internetu a hlavne rozvojom sociálnych sietí, záujem o ochranu súkromia na webe výrazne upadol. Mnoho užívateľov ani len netuší, aké informácie sa pri načítaní webovej stránky uložia na server a aké množstvo digitálnych stôp za nimi po neobozretnom surfovaní po webe ostáva. Na základe týchto informácií je potom možné spätne dohľadať konkrétneho užívateľa, či jeho lokáciu.

Táto bakalárska práca sa bude zaoberať problematikou anonymity na Internete, parciálnymi možnosťami ukrytia identity, ale hlavne sieťou Tor a jej službou Hidden Service (skrytá služba), riešením ich dostupnosti a bezpečnosti a možnosťami pripojenia. V neposlednom rade sa práca bude zaoberať konfiguráciou anonymného servera určeného pre anonymné zdielanie dát. Posledným krokom práce bude navrhnúť dve laboratórne úlohy zamerané na konfiguráciu a bezpečnosť Hidden Service.

1 ANONYMITA A SÚKROMIE NA INTERNETE

1.1 Anonymita všeobecne

Slovo Anonymita je odvodené z Gréckeho anonymia čo znamená „bez mena“. V informatike je definovaná ako „vlastnosť systému umožňujúca použitie zdrojov alebo služieb bez zistenia identity používateľa tohto systému[5].“ Nemožnosť dohľadať používateľa je teda najväčšou výhodou anonymity.

Na prvý pohľad môže internet vyzerať ako anonymné miesto. Naše fyzické proporcie, rysy tváre, vek či hlas ostávajú pri komunikácií neznámou, dávajúc nám milný pocit bezpečia. V bežnom živote si väčšina ľudí svoje súkromie dobre chráni a dôležité informácie zdieľajú len so svojimi najbližšími. Vo virtuálnom svete to ale neplatí, nakoľko používaním Internetu a hlavne rozvojom sociálnych sietí záujem o ochranu súkromia na webe výrazne upadol.

V minulosti, keď na internete prevládali diskusné fóra a klienti na interaktívne posielanie správ, bola identifikácia prostredníctvom prezývky samozrejmosťou. Človek, ktorý využíval svoje pravé meno a priezvisko bol označovaný buď za neskúseného používateľa alebo za súkromie nedbajúceho.

Dnes, jedna z viditeľných zmien správania internetových používateľov, je používanie reálnych mien. Zmena je spôsobená nástupom a rozmachom sociálnych sietí, založených na budovaní online profilov fyzických identít. Ľudia si privykli na vystupovanie pod reálnym menom a so skutočnou fotografiou.

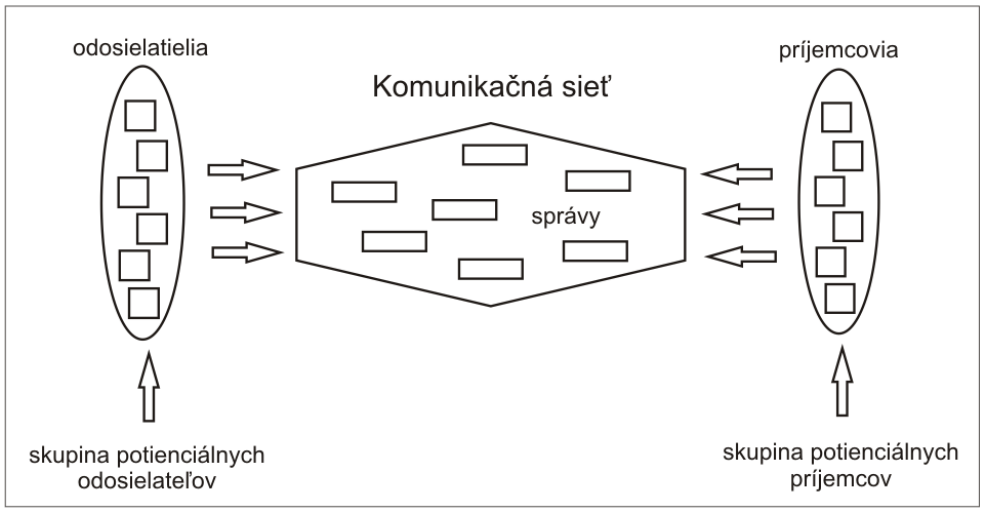
Neuvedomujúc si možné obštrukcie, zverejňujú na svojich profiloch fotky z dovolenky, reštaurácie, školy, domu, bytu či nového auta. Na základe týchto informácií si kriminálne živly môžu urobiť celkom dobrý obraz o finančnom zabezpečení danej entity, dennom harmonograme aj dobe neprítomnosti v obývanej nehnuteľnosti. Tieto informácie v kombinácii s menom sú pre nich jednoduchým kľúčom k úspechu.

Naše prejavy vôle, či už sa jedná o osobné názory, odborné rozpravy alebo kompromitujúce informácie sú na internete zálohované, indexované a ďalej kategorizované. Kým dnes nerozvážne činy 18-ročného mladíka nezaujimajú takmer nikoho, o pár rokov neskôr mu môžu stáť v ceste za vysnívanou karierou.

Práve preto by si mal každý vo svojom vlastnom záujme uvedomiť a prehodnotiť, čoho všetkého sa vlastne dobrovoľne chce vzdať. Spomenuli sme dobrovoľne, pretože existujú organizácie, špecializujúce sa na zber, dekódovanie a analýzu informácií. Najznámejšou a najčastejšie skloňovanou oganizáciou v oblasti súkromia je NSA.

1.2 Relativita anonymity

Aby sme mohli hovoriť o anonymite subjektu, musí existovať vhodná skupina subjektov s potenciálne rovnakými vlastnosťami. Anonymita subjektu je potom definovaná ako „nemožnosť identifikovať subjekt v rámci danej skupiny subjektov, tiež nazývanej ako skupina anonymity.“ Odosielateľ môže byť anonymný len v rámci skupiny potencionálnych odosielateľov, ktorá môže byť podskupinou všetkých subjektov, ktorí kedy poslali správy. Rovnako to platí aj pre príjemcu, ktorý môže byť anonymný iba v rámci skupiny potenciálnych príjemcov (obr. 1.1). Nemožnosť identifikovať subjekt v rámci skupiny anonymity znamená, že iba použitím útočníkovi dostupných informácií, subjekt nie je odlíšiteľný od ostatných subjektov v danej skupine anonymity[5].



Obr. 1.1: Relativita anonymity.

1.3 Súkromie na internete

Sledovanie ľudí, ich správanie sa na internete, evidovanie každého jedného kliknutia a ich pohybu v online svete naberá na intenzite. V minulosti boli pokusy jednotlivcov, ktorí nabádali k väčšej ochrane súkromia, brané skôr s humorom. Po odhalení projektu PRISM v roku 2013[6], ktorý prevádzkuje od roku 2007 americká agentúra NSA (National Security Agency), sa otázka súkromia stala každodennou neoddeliteľnou súčasťou ľudí využívajúcich internet, či už pracovne alebo súkromne.

Do projektu PRISM boli postupne zapojené veľké nadnárodné internetové spoločnosti ako Microsoft, Google, Yahoo, Facebook, Apple, Dropbox, Skype a AOL[6]. Tieto spoločnosti museli agentúre NSA poskytovať informácie o svojich užívateľoch,

o ich komunikácii, fotkách, hlasových a video hovoroch, informácie o polohe užívateľov.

Počas uplynulých rokov ľudia stále viac a viac dôverujú vzdialeným službám, uverili výhodám cloud computingu. Vzdali sa kontroly nad svojimi údajmi v prospech služieb SaaSS (Service as a Software Substitute). Nevedia, čo sa deje s ich dátami, kto všetko má k nim prístup, kde sa nachádzajú servre cloud spoločností[14]. Pričom tieto spoločnosti sú zo zákona povinné sprístupniť všetky údaje vládnym agentúram, a to nielen v prípade podozrenia z páchania trestnej činnosti alebo kvôli obrane pred terorizmom.

Preto je z pohľadu ochrany súkromia potrebné vybudovať slobodnú decentralizovanú sieť s využitím súčasnej infraštruktúry internetu, ktorú nebude možné sledovať jednoduchým spôsobom, v ktorej budú užívatelia slobodní, nebudú sledovaní. Ich aktivity na internete nebudu zaznamenávané a ďalej poskytované nadnárodným internetovým spoločnostiam a štátnym inštitúciám.

Jednou z alternatív decentralizovanej anonymnej siete je anonymizačná služba Tor, ktorú odporúčajú mnohé organizácie, ktoré sa zaoberajú slobodou internetu, napr. EFF (Electronic Frontier Foundation). EFF odporúča Tor ako online nástroj na udržanie občianskej slobody.

1.4 Analýza sieťovej komunikácie (Traffic Analysis)

Sieťové pakety sa skladajú z dvoch častí: hlavička potrebná k smerovaniu paketu (routing header) a prenášané údaje (data payload). Prenášané údaje môžu byť akékoľvek: emailová správa, webová stránka alebo súbor. Aj v prípade, že prenášané údaje sú šifrované, analýzou hlavičky dokážeme stále zistiť množstvo údajov: zdrojová a cieľová adresa, veľkosť, čas, atď.

Základným problémom z pohľadu súkromia je skutočnosť, že príjemca komunikácie dokáže tieto informácie zistiť jednoduchým nahliadnutím do hlavičky. Rovnako to dokáže aj autorizovaná osoba, napr. ISP, alebo neautorizovaná osoba nachádzajúca sa medzi odosielateľom a príjemcom.

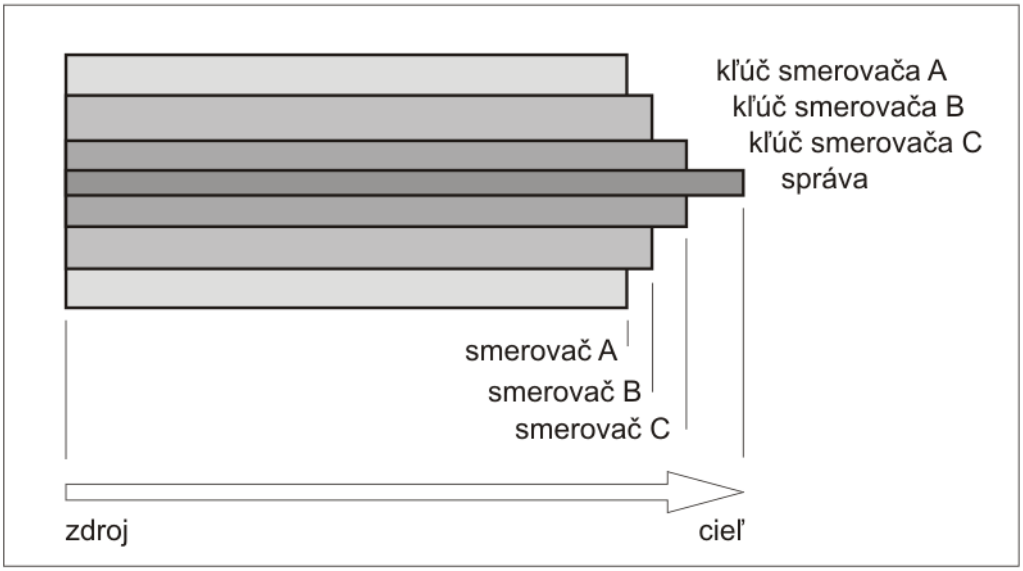
V súčasnosti sa používa omnoho sofistikovanejšia analýza prevádzky, pri ktorej sa sledujú viaceré časti internetu, využívajú sa štatistické modely na sledovanie správania sa organizácií a jednotlivcov. Šifrovanie v týchto prípadoch nepomáha, pretože šifrované sú len prenášane údaje, nie hlavičky.

2 SIEŤ TOR

2.1 Vznik siete Tor

Technika Onion Router (cibuľové smerovanie) bola pôvodne vyvinutá v U.S. Naval Research Laboratory pre potreby americkej armády. Hlavným dôvodom vzniku bola ochrana štátnej komunikácie. Po určitom čase si ale armáda uvedomila, že rozšírenie Toru medzi širokú verejnosť prispeje k zvýšeniu bezpečnosti, vďaka rozšíreniu skupiny potencionálnych odosieľateľov a prijímateľov[18].

Projekt Tor pozostáva z výskumu, navrhovania, stavby a analýzy anonymných komunikačných systémov. Dôraz je kladený na pripojenie s nízkou latenciou na báze Internetu a schopnosť odolávať analýze prevádzky, odpočúvaniu a ďalším útokom z vonkajšej (Internetové smerovače) alebo vnútornej strany systému (Onion smerovače). Cibuľové smerovanie zabraňuje transportnému médiu rozoznať, kto s kým komunikuje, sieť vie len to, že komunikácia prebieha. Okrem toho, obsah komunikácie je šifrovaný, skrytý pred odpočúvaním až do bodu, kde opúšťa sieť Tor[18]. Názov „cibuľové smerovanie“ je odvodený z princípu fungovania siete. Tak ako cibuľa, aj dáta prenášané v sieti Tor majú určitý počet vrstiev, ktoré sa odbaľujú na ceste ku finálnej destinácií (obr. 2.1).



Obr. 2.1: Princíp „cibuľového smerovania“ (Onion Router).

2.2 Všeobecný popis siete Tor

Tor tvorí sieť dobrovoľníkov, ktorí poskytujú svoje internetové pripojenie a počítače, aby vytvorili rozsiahlu sieť, ktorá umožňuje užívateľom siete Tor zvýšiť anonymitu a bezpečnosť na internete. Užívateľ teda namiesto priameho spojenia medzi svojím počítačom a cieľovým počítačom využije sieť uzlov, cez ktoré prebehne jeho komunikácia s cieľovým serverom. Týmto umožňuje jednotlivcom aj organizáciám zdieľať údaje cez verejný internet a pritom nekompromitovať svoje súkromie.

Užívatelia používajú Tor kvoli zabráneniu zbierania informácií veľkými servermi, ako napr. Facebook alebo Google, alebo tiež aby mohli využívať služby, ktoré majú blokované svojim poskytovateľom internetu.

Skryté služby Tor-u poskytujú užívateľom prevádzkovať internetové služby bez odhalenia polohy a informácií o majiteľovi alebo prevádzkovateľovi.

Anonymná služba Tor umožňuje ľuďom komunikovať privátne, bez narušenia súkromia. Pomocou nej je možné obchádzať cenzúru nastolenú poskytovaľom internetu alebo štátu. Táto cenzúra v súčasnosti nie je problémom len médiami podsúvaných krajín ako Irán alebo Čína. Čoraz viac sa týka krajín tzv. „slobodného sveta“ – „slobodné“ USA, „slobodná“ Európa.

Užívatelia zapojení do projektu Tor robia túto sieť slobodnejšou a bezpečnejšou. Čím viac ľudí sa do nej zapojí, tým viac uzlov bude funkčných a tým menej bude celá sieť zraniteľnejšia[19].

Používaním siete Tor sa chránime proti bežne používaným metódam sledovania internetu, známym ako analýza prenášaných údajov (traffic analysis). Touto analýzou sa zisťuje kto komunikuje s kým cez verejnú sieť. Sleduje sa správanie užívateľa na internete, jeho záujmy, jeho navštevované stránky, atď. Užívateľ odhaľuje krajinu svojho pôvodu, zamestnávateľa a mnoho ďalších dôverných a súkromných informácií, aj v prípade, že používa šifrovaný prenos údajov.

2.3 Prístup do siete Tor

Pripojiť sa do siete Tor je jednoduché a bezplatné, stačí si stiahnuť dostupnú verziu programu z oficiálnych stránok projektu https://www.torproject.org/. V prípade krajín so silnou cenzúrou, kde sú tieto stránky blokované alebo trestné, je možné komunikovať s automatickým GetTor robotom.

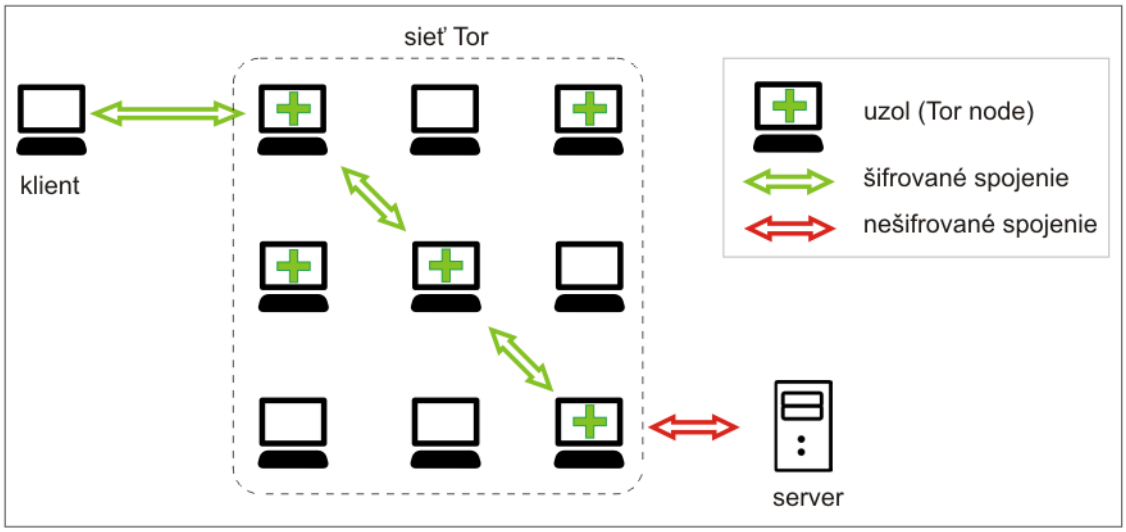
Užívateľ kontaktuje automatického robota emailovou správou. Najstabilnejším súčastným GetTor robotom je gettor@torproject.org. Podľa požadovaného operačného systému sa do tela správy uvedie iba jedno slovo: windows, linux alebo osx, pričom predmet správy nemá vplyv, môže ostať prázdny.

Robot na základe uvedeného operačného systému odošle užívateľovi správu s príslušným odkazom na stiahnutie programu z dropboxu a s prideleným digitálnym kľúčom pre overenie elektronického podpisu po rozbalení. V prípade, že užívateľ odošle správu s iným obsahom, robot odpovie pomocnou správou, v ktorej užívateľovi vysvetlí, ako správne komunikovať. Komunikácia prebieha len v anglickom jazyku.

2.4 Princíp fungovania siete Tor

Tor (The Onion Router) funguje na princípe mnohovrstvového smerovania – odtiaľ prirovnanie „cibuľový“ smerovač (obr. 2.1). O cibuľovom smerovaní bolo publikovaných už v minulosti niekoľko štúdií[16][17][13][7], návrhov siete a konceptov, žiadny projekt ale nebol nasadený pre verejné použitie ako práve projekt Tor[4].

Tor využíva distribuovanú anonymizačnú sieť, ktorú tvoria uzly – počítače dobrovoľníkov zapojených do projektu Tor. Komunikácia medzi užívateľom a uzlami siete je šifrovaná, záverečná časť cesty od výstupného uzla siete Tor po cieľový server už šifrovaná nie je (obr. 2.2).



Obr. 2.2: Princíp fungovania distribuovanej siete Tor cez uzly.

Tor pomáha redukovať možnosť jednoduchej aj sofistikovanej analýzy prenosu údajov distribuovaním komunikačného kanálu medzi niekoľko náhodne vybraných uzlov siete v rámci internetu. Náhodný pozorovateľ teda nemôže určiť, odkiaľ údaje prichádzajú a kam smerujú.

K vybudovaniu privátneho komunikačného kanálu vytvorí klientský softvér siete Tor šifrované spojenie medzi uzlami siete. Komunikácia medzi uzlami je šifrovaná, žiadny individuálny uzol nepozná kompletnú cestu, ktorou paket prešiel.

Akonáhle je kanál otvorený, môže byť použitý rôznymi druhmi aplikácií s podporou protokolu SOCKS. Pretože žiadny uzol nevidí ďalej ako po svoj najbližší uzol, komunikácia nemôže byť analyzovaná ani použitím kompromitovaného uzla.

Kvôli efektivite používa softvér Tor ten istý otvorený komunikačný kanál pre všetky spojenia počas určitého intervalu, najčastejšie 10 minút. Po uplynutí tohto časového intervalu sa vytvorí nový kanál.

2.5 Možnosti pripojenia

Pripojiť k sieti Tor sa dá tromi spôsobmi: ako klient, smerovač alebo premostenie. Klient je základná možnosť poskytujúca plnohodnotné využitie všetkých služieb siete hneď po nainštalovaní programu Tor Browser Bundle.

Užívateľ sa môže stať aktívnym uzlom siete Tor tak, že nastaví svoj program ako smerovač. Program vytvorí nový Tor smerovač, ktorí ihneď zaradí do databázy a odošle na adresárový server, aby ho mohli používať aj ostatní používatelia. Podľa povoleného použitia sa smerovače delia na dve základné skupiny, a to výstupné a nevýstupné. Výstupné smerovače nie sú limitované zákazom a teda môžu byť použité ako ktorýkoľvek smerovač, vstupný, prostredný či výstupný. Nevýstupné smerovače môžu byť použité len ako vstupné či prostredné smerovače, nikdy nie ako smerovače výstupné. Je to z dôvodu zachovania bezpečnosti vlastníka a ochrániť ho pred spájaním jeho IP adresy s premávkou v sieti Tor, a tým aj pred možnými problémami s úradmi v prípade odhalenia nevhodných praktík.

Treťou možnosťou je premostenie. Jedná sa o špeciálny typ smerovačov, ktoré sa nenachádzajú v adresárovej službe a neexistuje ich kompletný verejný zoznam. Premostenie sa najčastejšie využíva v krajinách, kde sa blokujú verejné smerovače Toru, ako napríklad v Číne. Ochrana pred blokovaním spočíva v použití obfsproxy. Tieto premostenia potom obsahujú extra mätúcu vrstvu a pozorovateľ tak uvidí len nevinne sa tváriacu transformovanú prevádzku, namiesto skutočnej Tor prevádzky.

2.6 Zachovanie anonymity v sieti Tor

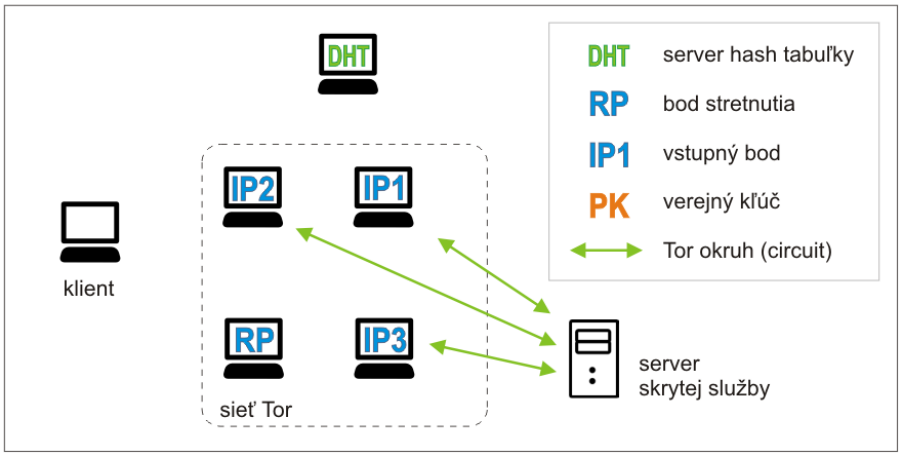
Tor nedokáže vyriešiť všetky problémy týkajúce sa anonymity. Je zameraný iba na zabezpečenie prenosu údajov cez internet. Užívateľom sa odporúča dodržiavať ďalšie všeobecné pravidlá pre zachovanie anonymity v sieti Tor:

- Používanie prehliadača Tor (Tor browser) – tento prehliadač je predkonfigurovaný na bezpečné používanie v sieti Tor.
- Nepoužívať torrent klienta v sieti Tor – veľa klientov obchádza Tor a odhaľuje tak skutočnú IP adresu užívateľa.
- Nepoužívať prídavné moduly v prehliadačoch (browser add-ons) – častokrát tieto moduly obchádzajú nastavenie siete Tor a deanonymizuju užívateľský počítač.
- Používať HTTPS verzie stránok, ak sú k dispozícii – komunikácia v sieti Tor medzi uzlami siete je šifrovaná, ale posledný úsek od výstupného uzla po cieľový server je závislý od použitého protokolu na prenos údajov.
- Neotvárať stiahnuté dokumenty počas aktívnej siete Tor – dokumenty ako napr. DOC alebo PDF môžu obsahovať externé odkazy, ktoré môžu obísť sieť Tor a odhaliť tak skutočnú IP adresu počítača.
- Využívať premostenie namiesto bežného pripojenia na vstupný uzol siete Tor – lokálny ISP môže analýzou prevádzky detekovať používanie siete Tor. Ak je to nežiadúce, je možné pripojenie do siete Tor cez premostenie (Tor Bridge Relay). V takom prípade ani ISP nedokáže rozpoznať využívanie siete Tor[19].

2.7 Skryté služby v sieti Tor

Tor ponúka okrem anonymizačnej siete aj službu pod názvom „skryté služby“ (Tor Hidden Services). Umožňuje tým užívateľom skryť polohu ich servera, na ktorom môžu poskytovať rôzne webové služby ako napr. internetové fórum, službu na zdielanie súborov, instant messaging server. Pomocou tzv. „rendezvous“ bodov sa na server skrytej služby dokážu pripojiť ostatní užívatelia siete Tor, bez toho, aby poznali skutočnú sieťovú identitu servera.

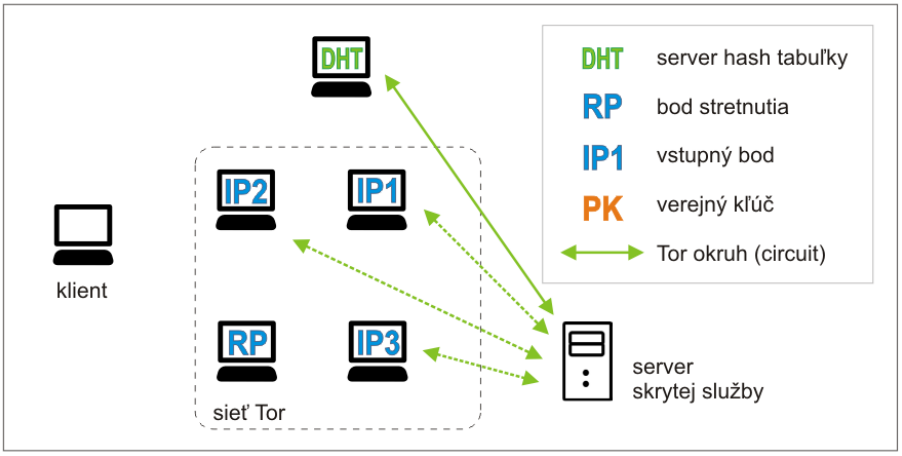
Skrytá služba musí poslať informáciu o svojej existencii v sieti Tor ešte predtým, ako sa na ňu dokážu pripojiť ostatní užívatelia. Kvôli tomu skrytá služba náhodne vyberie niekoľko uzlov siete, vytvorí k nim okruhy a požiada ich, aby sa stali vstupnými bodmi (introduction points) skrytej služby (introduction points) (obr. 2.3).



Obr. 2.3: Skrytá služba - vstupné body.

Týmto uzlom odošle skrytá služba svoj verejný šifrovací kľúč. Vybudovaním okruhu (označené zelenými spojnicami) namiesto priameho spojenia servera skrytej služby k vstupným bodom sa zabezpečí anonymita skrytej služby a bude zložité pre útočníka asociovať vstupný bod s reálnou IP adresou servera skrytej služby.

V druhom kroku vytvorí skrytá služba deskriptor (hidden service descriptor), ktorý obsahuje jej verejný kľúč a sumárne údaje o jej vstupných bodoch (introduction points). Tento deskriptor následne podpíše svojím súkromným kľúčom a odošle ho do verejne prístupnej databázy DHT (distributed hash table) (obr. 2.4).



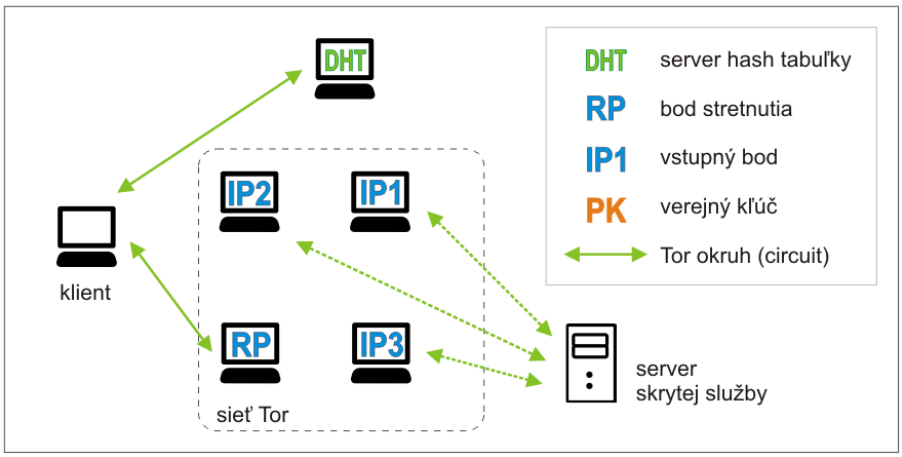
Obr. 2.4: Skrytá služba - odoslanie deskriptora na server DHT.

Deskriptor bude následne poskytnutý klientovi, ktorý si ho vyžiada na základe .onion adresy v tvare xyz.onion, kde xyz tvorí 16 znakov odvodených z verejného

kľúča skrytej služby. Po tomto kroku je skrytá služba vytvorená a jej adresa bude napr.: t4rvnpaleil3fnwl.onion.

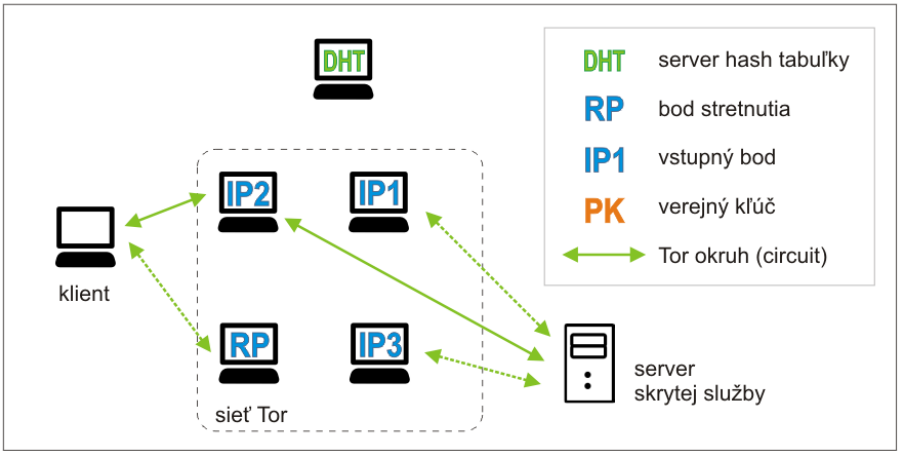
Aj keď sa zdá byť používanie adresy skrytej služby v tvare automaticky generovaného hash reťazca nepraktické, prináša to isté výhody: každý, kto komunikuje so skrytou službou, či už vstupný bod, adresárová služba hash tabuliek alebo samotný klient, si môže overiť, že komunikuje so správnou skrytou službou. V budúcnosti budú možno implementované návrhy ako napr. Petname[15], ktoré umožnia používanie ľudsky zrozumiteľnejších a zapamätateľnejších adries .onion.

Po úspešnom propagovaní skrytej služby a jej adresy .onion ju môžu kontaktovať klienti výhradne cez sieť Tor. Klient musí najskôr poznať adresu skrytej služby. Potom kontaktuje službu DHT a získa deskriptor skrytej služby, zoznam vstupných bodov a verejný kľúč skrytej služby (obr. 2.5). Zároveň klient otvorí okruh na náhodne zvolený uzol siete, ktorý požiada, aby vystupoval ako tzv. „rendezvous“ bod (bod stretnutia) pre spojenie so skrytou službou.



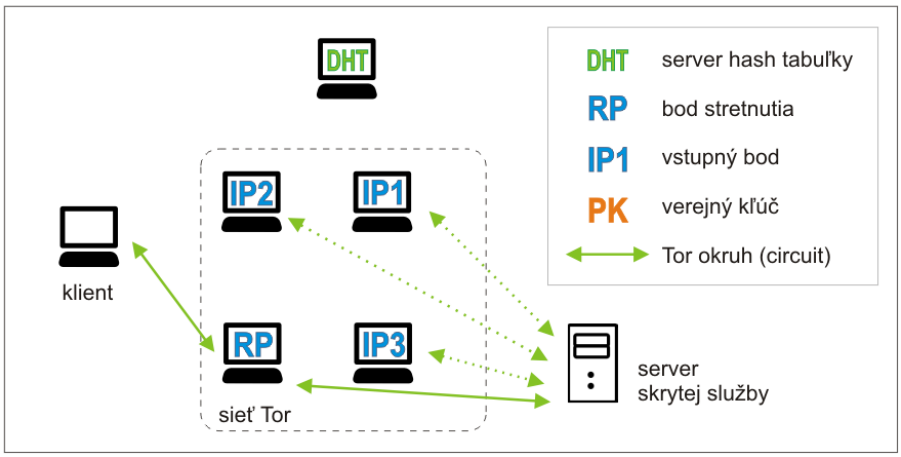
Obr. 2.5: Skrytá služba - výber bodu stretnutia (Rendezvous point).

Ak klient získa deskriptor skrytej služby (služba je online, klient má správnu adresu) a je pripravený okruh k bodu stretnutia, klient vytvorí úvodnú správu zašifrovanú pomocou verejného kľúča skrytej služby, v ktorej odošle informáciu o mieste stretnutia (obr. 2.6). Celá komunikácia prebieha v sieti Tor, takže klient ostáva anonymný voči skrytej službe.



Obr. 2.6: Skrytá služba - bod stretnutia (Rendezvous point).

V ďalšom kroku skrytá služba dekryptuje úvodnú správu od klienta a vyhľadá miesto stretnutia (rendezvous point), vybuduje k nemu okruh a vytvorí „rendezvous“ správu, ktorú odošle na toto miesto stretnutia (obr. 2.7).



Obr. 2.7: Skrytá služba - vytvorenie okruhov.

V poslednom kroku bod stretnutia informuje klienta o úspešnom vytvorení spojenia so skrytou službou. Následne klient aj skrytá služba použijú svoje okruhy k bodu stretnutia a môžu komunikovať navzájom. Bod stretnutia (rendezvous point) jednoducho preposiela šifrované dáta od klienta k skrytej službe a naopak.

Vo všeobecnosti, kompletné spojenie medzi klientom a serverom skrytej služby pozostáva zo šiestich uzlov: tri z nich boli zvolené klientom (jeden je rendezvous bod) a ďalšie tri vybrala skrytá služba.

2.8 Tor a jeho budúcnosť

Poskytnúť použiteľnú anonymizačnú sieť v rámci internetu je veľkou výzvou. Vývojári stojaci za projektom Tor sa snažia o vybudovanie čo najstabilnejšej siete s možnosťou pripojenia čo najviac užívateľov. Čím viac užívateľov sa stane súčasťou siete Tor, tým sa bude zvyšovať počet uzlov. To zvýši diverzifikáciu, anonymitu a bezpečnosť siete Tor pre všetkých[19].

3 ZRANITEĽNOSŤ SIETE TOR - DEANONYMIZÁCIA

3.1 Cielené útoky proti sieti Tor

Sieť Tor patrí medzi populárne anonymizačné siete a počet jej úžívateľov neustále narastá, je preto prirodzené, že rastie aj záujem o jej deanonymizáciu, hlavne zo strany vládnych agentúr (NSA, GCHQ). Za týmto účelom bolo vyvinutých niekoľko cielených útokov na infraštruktúru siete Tor, najmä na jej výstupné uzly. V nasledujúcej časti budú stručne popísané niektoré teoretické aj reálne útoky.

3.1.1 Sniper Attack

Sniper Attack je útok, ktorý za použitia vyrazne nízkych nákladov dokáže znefunkčniť najpoužívanejšie výstupné uzly siete Tor. Na dosiahnutie cieľa používa deštruktívny DoS útok proti týmto uzlom. Útok prebieha exploitnutím validných správ protokolu Tor, pomocou ktorých dokáže útočník zahltiť operačnú pamäť počítača. Experimenty ukázali, že útočník dokáže alokovať operačnú pamäť rýchlosťou 2187 KiB/s, pričom na to potrebuje prenosovú rýchlosť iba 92 KiB/s. Pri reálnom použití útoku došlo behom 29 minút k výpadku 20 najpoužívanejších výstupných uzlov siete. Tento útok dokáže deanonymizovať skryté služby (server .onion) selektívnym DoS útokom a prinútením .onion servera, aby použil uzol, ktorý je pod kontrolou útočníka[9].

DoS útok je smerovaný proti tzv. guarding relays, proti uzlom siete, ktoré chránia skrytú službu. Útočník dokáže deanonymizovať server skrytej služby behom niekoľkých dní s použitím bežného hardvéru a internetového pripojenia. Pri použití výkonejšieho vybavenia sa skráti čas potrebný na odhalenie na niekoľko hodín. Útok bol úspešne simulovaný v testovacom prostredí Shadow[8], bez ohrozenia reálnej prevádzky siete Tor.

Deanonymizačný útok prebieha v troch krokoch:

1. Identifikácia ochranných uzlov skrytej služby
2. Znefukčnenie týchto uzlov použitím Sniper Attack
3. Testovanie, či si skrytá služba vybrala náhradný uzol pod kontrolou útočníka. Ak nie, opakuje sa postup od kroku č.1.

3.1.2 RAPTOR

Útok RAPTOR (Routing Attacks on Privacy in Tor) využíva známu zraniteľnosť siete Tor, keď útočník sleduje kominukáciu na oboch stranách siete. Následným po-

rovnaním a koreláciou paketov, ich veľkosti a času, dokáže deanonymizovať klientov siete Tor[21].

Útok je realizovaný pomocou autonómnych systémov, ktoré zaznamenávajú prevádzku siete a realizujú koreláciu metadát z paketov. Často sú súčasťou siete Tor v pozícii výstupných uzlov. Veľké autonómne systémy ISP dokážu zbierať údaje o každom pakete v rámci ich siete. Ako poukázal Edward Snowden[1], agentúra NSA v projekte Marina ukladá meta informácie o komunikácií užívateľov počas jedného roku, obdobný projekt Tempora agentúry GCHQ ukladá meta informácie 30 dní a celé pakety ukladá 3 dni.

RAPTOR sa skladá z troch individuálnych útokov:

1. RAPTOR využíva asymetrický spôsob smerovania internetových paketov. Trasa BGP (Border Gateway Protocol) od zdrojového počítača po cieľový počítač sa môže líšiť od spätnej trasy BGP od cieľa ku zdroju. Asymetria v smerovaní zvyšuje šancu sledovania aspoň jedného smeru komunikácie.
2. RAPTOR využíva prirodzené zmeny v BGP trasách spôsobené výpadkom liniek alebo sieťových prvkov. Zmeny v BGP trasách umožňujú autonómnym systémom odsledovať dodatočnú komunikáciu a tým deanonymizovať zvýšený počet klintov v sieti Tor.
3. RAPTOR využíva vnútornú zraniteľnosť internet routingu – útočník môže manipulovať smerovanie pomocou techník ako BGP hijack voči sieti Tor.

3.1.3 Sybil Attack

Útok označovaný ako Sybil, nie je špecifický len pre sieť Tor, ale je všeobecne použiteľný pre akúkoľvek sieť peer-to-peer. V roku 2014 bol zaznamenaný veľký útok Sybil na sieť Tor, ktorý zatiaľ nebol úplne analyzovaný. Do siete Tor bolo prihlásených 115 nových rýchlych vnútorných uzlov (nie výstupných), ktoré boli pod kontrolou útočníka. Spolu tvorili približne 6% ochrannej kapacity siete. Po približne piatich mesiacoch sa z nich v rámci bežnej rotácie stali vstupné uzly pre významne vysoký počet užívateľov. Spolu s ďalším typom útoku s názvom „traffic confirmation attack“ sa podarilo deanonymizovať časť siete so skrytými službami[20].

3.2 Deanonymizácia spôsobená nevhodnou správou servera

Prevádzková bezpečnosť servera je dôležitou súčasťou celkovej bezpečnosti služby Hidden Service a jej dodržiavaním dokážeme vyznamne znížiť možnosť prezradenia skutočnej IP adresy servera skrytej služby. Prevádzkovatelia skrytej služby si často

neuvedomujú možné riziká, nemajú potrebné teoretické ani praktické skúsenosti. V nasledujúcej časti budú popísané možné riziká deanonymizácie skrytej služby, ktoré sú zapríčinené jej prevádzkou.

3.2.1 Infiltrácia agenta v prestrojení

Dôležitou súčasťou bezpečnosti Hidden Service je klásť veľký dôraz na preverenie nových ľudí, ktorí sú príjmaní medzi správcov servera. Pri veľkých a populárnych serveroch sa častokrát stáva, že súčasťou tímu je cudzí agent, čo vedie po určitej dobe nielen k prezradeniu identity prevádzkovateľa, ale aj zozbieraním vecných dôkazov proti nemu.

3.2.2 SQL injections

Množstvo Hidden Service serverov ponúka svoje služby a produkty cez nekvalitne naprogramované php / mysql online obchody, ktoré obsahujú veľa chýb a tým ponúkajú možnosť útoku typu SQL injections.

3.2.3 Deanonymizácia platobného systému

Väčšina serverov ponúka možnosť buď dobrovoľného príspevku (donation) na podporu svojej činnosti, alebo vyžaduje platbu za svoje služby alebo produkty. Preto je dôležité pre prevádzkovaľa zvoliť platobný systém, ktorý spĺňa podmienku anonymity. V dnešnej dobe patrí medzi najpoužívanejšie anonymné platobné systémy práve Bitcoin. Aj keď je Bitcoin všeobecne považovaný za anonymný, niekoľko prípadov a štúdií[2] z minulosti ukazuje, že aj pri jeho používaní je potrebné dbať na základné pravidlá dodržania anonymity.

3.2.4 Konfigurácia servera skrytej služby

Správna konfigurácia služieb bežiacich na serveri môže výrazne znížiť riziko odhalenia polohy alebo IP adresy. Je vhodné vypnúť chybové hlásenia web servera, ktoré by mohli prezradit informácie o systéme alebo časovom pásme. Tiež je potrebné vykonávať pravidelné bezpečnostné aktualizácie celého systému a používaných služieb. Na serveri sa neodporúča prevádzkovať mailový server.

3.2.5 Dedikovaný server pre skrytú službu

Vo všeobecnosti sa neodporúča prevádzkovať na jednom serveri skrytú službu spolu so službou Tor Relay, pretože uzly siete Tor sú verejné a z dlhodobého sledovania

ich prevádzky a prevádzky skrytej služby je možné deanonymizovať skrytú službu. Tiež platí pravidlo, že čím dlhšie beží skrytá služba, tým viac údajov o nej sa dá zozbierať, a tým väčšia je šancia na jej odhalenie.

3.3 Zlepšenie bezpečnosti a stability siete Tor

3.3.1 Škálovateľnosť

Súčasná architektúra siete Tor nepodporuje škálovateľnosť skrytej služby v dostatočnej miere. Premigrovať existujúce webové servery s vysokou návštevnosťou ako Hidden Services je problém. Vstupné body skrytej služby (introduction points) nie sú pripravené na veľké množstvo požiadaviek od návštevníkov, keďže ide len o obyčajné uzly siete (Tor Node). Do budúcnosti vývojári stojaci za projektom Tor plánujú vyriešiť tento problém tým, že správcovia navštevovanejších webov budú mať možnosť nastaviť počet vstupných bodov skrytej služby a tým rozložiť záťaž.

3.3.2 Zraniteľnosť voči DoS útokom

Ďalším problémom sú útoky DoS (Denial of Service), ktoré útočníkom slúžia na zahltenie vstupného bodu skrytej služby a tým zneprístupnenie obsahu bežným užívateľom. Môže ísť o snahu konkurencie alebo aj štátnej moci. Jedným z možných riešení je implementácia tzv. Valet uzlov[12]. Tieto uzly by stáli pred vstupným bodom skrytej služby a redukovali by zraniteľnosť voči DoS útokom a tiež by umožnili aplikovať QoS. V súčasnej dobe nie je toto riešenie implementované, hlavne kvôli časovej náročnosti.

3.3.3 Dĺžka kľúča

V súčasnosti používaný šifrovací pár kľúčov je RSA-1024, ktorý sa dnes už považuje z hľadiska bezpečnosti za nedostatočný. Implementácia dlhšieho kľúča je navrhnutá[10], ale zatiaľ nie je zrealizovaná. Jednou z príčin odkladania zavedenia nového kľúča je fakt, že časť verejného kľúča slúži ako názov .onion domény. Zmenou kľúča by došlo k zmene názvu, čo by mohol byť problém u zabehnutých serverov. Prechodným riešením by bolo súčasné používanie starého aj nového kľúča.

3.3.4 Obrana voči HSDir útokom

Skrytá služba odosiela svoj deskriptor uzlu siete s názvom HSDirs (Hidden Service Directory Servers). Užívatelia sa potom pripájajú na HSDirs a získavajú deskriptor

a následne sa pripájajú na danú skrytú službu. Štúdia z roku 2013[3] analyzovala možnosti služby HSDirs:

- ako zmerať popularitu skrytej služby bez spolupráce s jej prevádzkovateľom
- ako odmietnuť prístup ku skrytej službe pomocou HSDirs
- ako získať deskriptory všetkých skrytých služieb v sieti Tor za menej než 2 dni s použitím minimálnych nákladov
- ako odhaliť ochranné uzly (guard nodes) skrytej služby
- návrh deanonymizačného útoku, ktorý dokáže odhaliť IP adresy významne veľkému počtu serverov skrytej služby, v čase 1 roka.

3.3.5 Rýchlosť prístupu k serverom skrytej služby

Rýchlosť odozvy skrytej služby je v súčasnosti veľmi nízka. Môže to byť spôsobené napríklad komplikovaným spôsobom vybudovania okruhu. Jedným z navrhovaných riešení je jeho zjednodušenie eliminovaním potreby oddelených rendezvous spojení[11].

4 PRAKTICKÁ ČASŤ

V praktickej časti bude popísaný postup inštalácie skrytej služby v sieti Tor pod operačným systémom Debian Linux. Ďalej bude pre potreby tejto práce nainštalovaný web server Apache, MySQL server a PHP (LAMP) a opensource softvér ownCloud, ktorý umožňuje prevádzkovať vlastný cloud – plnohodnotné úložisko súborov s možnosťou ich zdielania.

Postup inštalácie bude rozdelený a popísaný v nasledujúcich krokoch:

1. 1. inštalácia operačného systému Debian Linux
2. 2. inštalácia web servera Apache, databázového servera MySQL a PHP
3. 3. inštalácia skrytej služby Tor
4. 4. inštalácia softvéru ownCloud

Celá inštalácia bola realizovaná lokálne.

4.1 Inštalácia – Debian Linux

Ako operačný systém bol zvolený Linux v distribúcii Debian vo verzii 8.0 Jessie. Samotná inštalácia operačného systému je užívateľsky jednoduchá a prehľadná. Kvôli potrebám tejto práce bolo nainštalované grafické rozhranie KDE. Verzia linuxu a jadra použitého v tejto bakalárskej práci:

```
# uname -a
Linux debian 3.16.0-4-686-pae \#1 SMP Debian 3.16.7-ckt9-2
(2015-04-13) i686 GNU/Linux
```

Aby boli pri inštalácii použité aktuálne verzie inštalačných balíkov, doplníme do súboru /etc/apt/sources.list:

```
# nano /etc/apt/sources.list
```

nasledovné riadky:

```
deb http://deb.torproject.org/torproject.org jessie main
deb-src http://deb.torproject.org/torproject.org jessie main
```

Po základnej inštalácii je vhodné doinštalovať balíky sudo a nano:

```
# apt-get install sudo nano
```

Nano je textový editor vhodný na editáciu konfiguračných súborov a sudo umožňuje spúšťanie príkazov s právami root. Kvôli bezpečnosti sa neodporúča v Linuxe pracovať pod správcovským účtom root. Preto bol použitý lokálny užívateľ s názvom peter. Nového užívateľa pridáme príkazom:

```
# adduser peter
```

Ďalej nastavíme lokálnemu užívateľovi práva používať príkaz sudo:

```
# sudo adduser peter sudo
```

a v konfiguračnom súbore /etc/sudoers:

```
# nano /etc/sudoers
```

doplníme riadok pre užívateľa peter:

```
peter  ALL=(ALL:ALL) ALL
```

4.2 Inštalácia – apache, mysql, php

Inštaláciu web servera Apache vykonáme príkazom:

```
$ sudo apt-get install apache2
```

Inštaláciu databázového servera MySQL spustíme príkazom:

```
$ sudo apt-get install mysql-server
```

V ďalšom kroku dokončíme inštaláciu príkazmi:

```
$ sudo mysql_install_db
$ sudo /usr/bin/mysql_secure_installation
```

Inštalácia PHP:

```
$ sudo apt-get install php5 php5-mysql libapache2-mod-php5
```

V konfiguračnom súbore povolíme .php súbory pre apache:

```
# nano /etc/apache2/mods-available/php5.conf
```

Upravíme riadky:

```
<FilesMatch "\.ph(p3?|tml)$">
    SetHandler application/x-httpd-php
    Require all granted
</FilesMatch>
```

4.3 Inštalácia Hidden Service

Inštaláciu vykonáme príkazom:

```
$ sudo apt-get install tor
```

Po nainštalovaní je potrebné upraviť konfiguračný súbor torrc:

```
$ sudo mv /etc/tor/torrc /etc/tor/torrc.bak
$ sudo nano /etc/tor/torrc
```

Pre fungovanie skrytej služby stačí do súboru vložiť len 3 riadky:

```
DataDirectory /var/lib/tor
HiddenServiceDir /var/lib/tor/hidden\_service/
HiddenServicePort 80 127.0.0.1:80
```

Nasleduje reštart služby tor:

```
$ sudo service tor reload
```

Po reštarte služby tor sa zapíše privátny kľúč do súboru /var/lib/tor/hidden_service/private_key a vygenerovaný názov .onion servera sa zapíše do súboru /var/lib/tor/hidden_service/hostname:

```
$ sudo cat /var/lib/tor/hidden\_service/hostname
t4rvnpaleil3fnwl.onion
```

4.4 Inštalácia – ownCloud

Inštaláciu programu ownCloud spustíme príkazom:

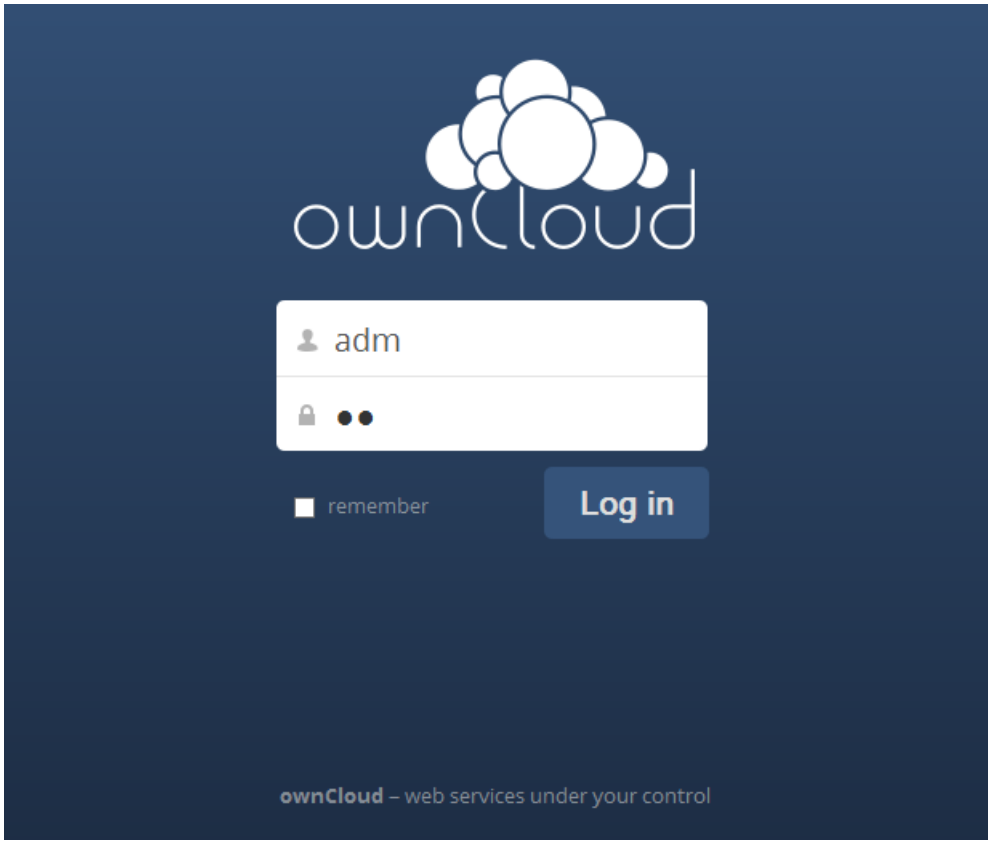
```
$ sudo apt-get install owncloud
```

Počas inštalácie bolo vytvorené užívateľské konto „adm“ s heslom „ma“.
Následne v prehliadači skontrolujeme funkčnosť inštalácie otvorením url:
http://localhost/owncloud

4.5 Pripojenie na server skrytej služby

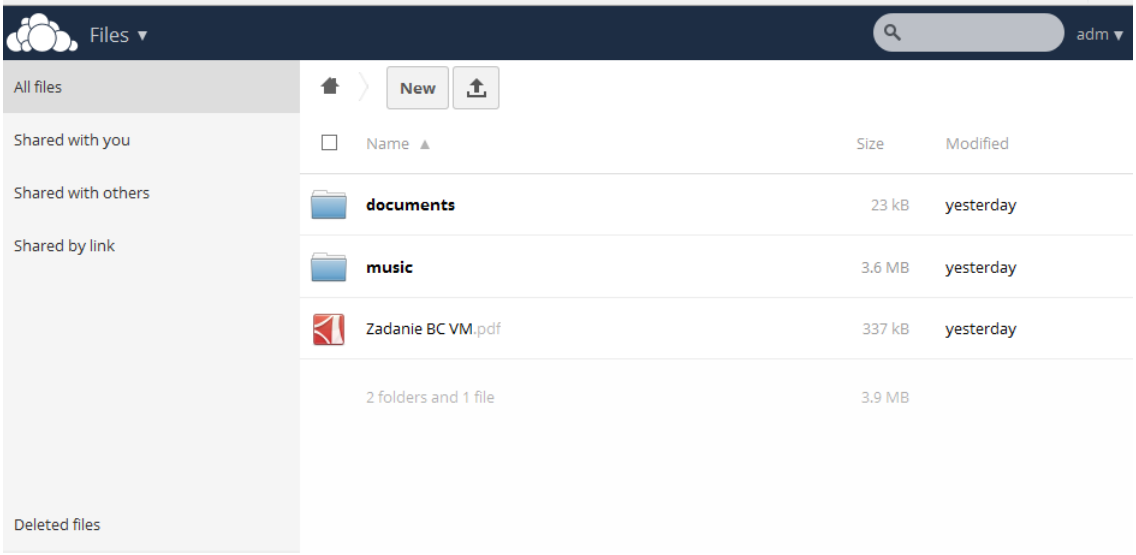
Na strane klienta (pod operačným systémom Windows 8.1) nainštalujeme balík Tor Browser Bundle. Tento balík je postavený na zdrojovom kóde prehliadača Mozilla Firefox, doplnený o klienta siete Tor a optimalizovaný na zachovanie anonymity počas prehliadania webových stránok.

Po spustení prehliadača Tor Browser a zadaní url .onion adresy na náš server skrytej služby (http://t4rvnpaleil3fnwl.onion/owncloud) sa otvorí prihlasovacie okno programu ownCloud (obr. 4.1)



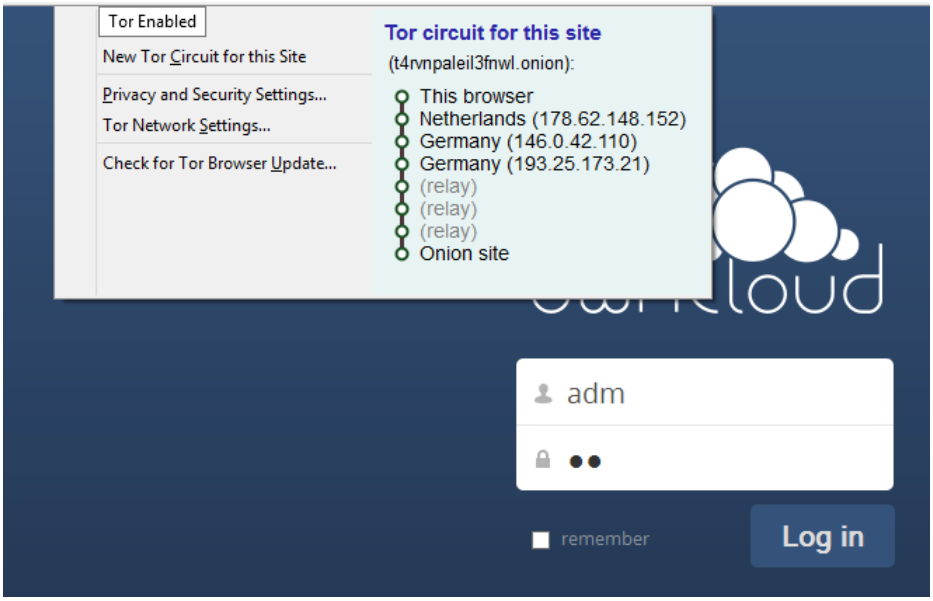
Obr. 4.1: OwnCloud - prihlasovacia stránka.

Po prihlásení sa dostaneme do základnej obrazovky programu ownCloud (obr. 4.2), kde je zoznam adresárov, súborov, so základnými možnosťami pre nahratie nového súboru (upload), stiahnutie alebo nastavenie zdielania pre požadovaný súbor.



Obr. 4.2: OwnCloud - základná obrazovka.

Po otvorení skrytej služby v prehliadači Tor Browser môžeme zobraziť informácie o okruhu od klienta ku skrytej službe (obr. 4.3).

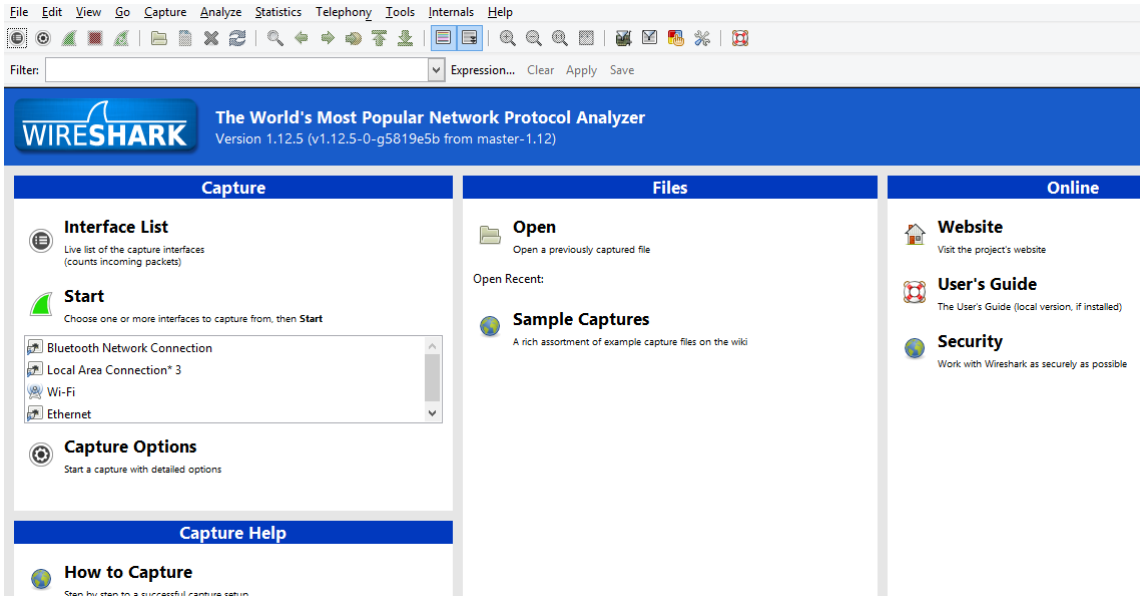


Obr. 4.3: Okruh k serveru skrytej služby (Tor Circuit).

Na obrázku vidíme 3 Tor uzly s IP adresou a 3 uzly bez IP adresy. Prvé tri uzly patria do okruhu klienta, pričom tretí je „rendezvous point“ (s IP adresou 193.25.173.21). Ďalšie tri patria do okruhu skrytej služby a ich IP adresy nie sú klientovi známe.

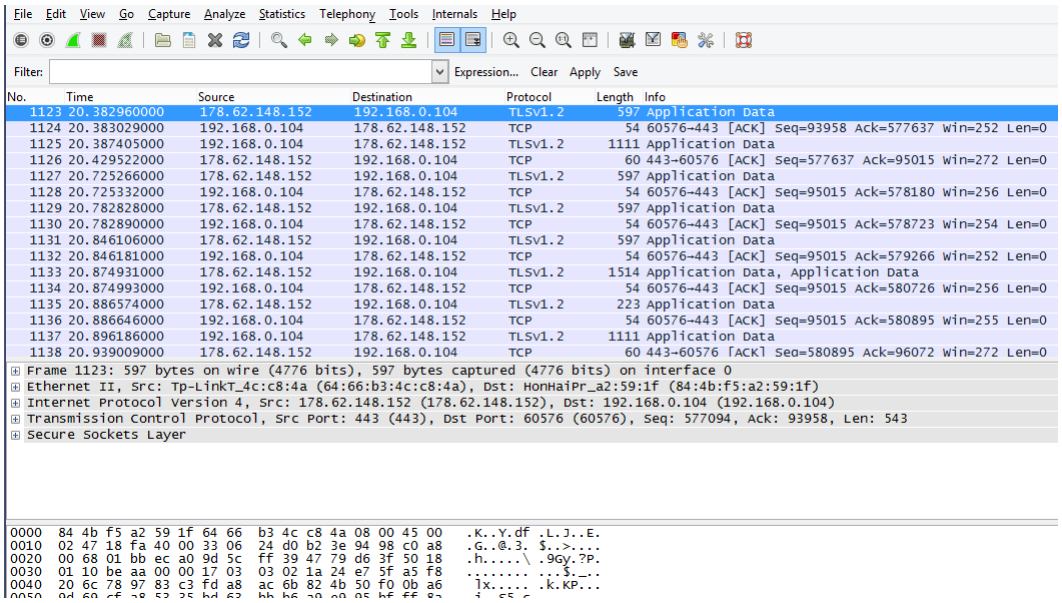
K analýze prenosu údajov medzi klientom a skrytou službou použijeme program Wireshark (http://wireshark.org). Wireshark je protokolový analyzér a paketový sniffer. Dokáže analyzovať veľké množstvo komunikačných protokolov a formátov. Dokáže prepnúť sieťovú kartu do tzv. promiskuitného režimu, v ktorom je možné odpočúvať celú sieťovú komunikáciu na danom rozhraní (napr. eth0). Poskytuje tiež prehľadné užívateľské rozhranie a patrí medzi najpoužívanejšie programy vo svojej triede.

Na úvodnej obrazovke programu Wireshark vyberieme sieťové rozhranie, ktoré chceme anyzovať (obr. 4.4) a spustíme záznam komunikácie.



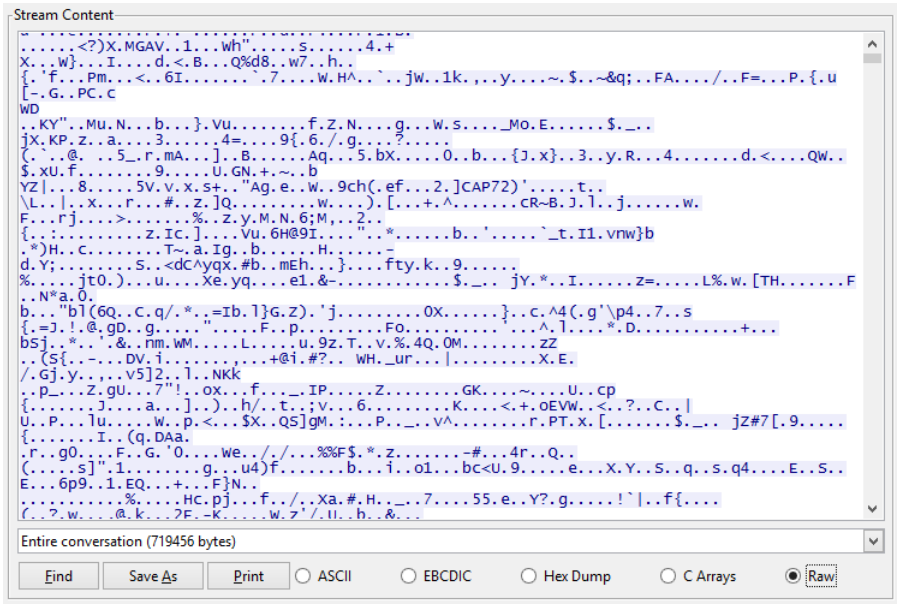
Obr. 4.4: Wireshark - úvodná obrazovka.

Následne otvoríme stránku ownCloud na našom .onion servery. Po načítaní stránky a prihlásení sa zastavíme zachytávanie paketov. Zo záznamu komunikácie je zrejmé, že Tor Browser komunikoval iba s uzlom, ktorého IP adresa bola 178.62.148.152 (obr. 4.5), teda s prvým uzlom nadviazaného okruhu.



Obr. 4.5: Wireshark - zachytená sieťová komunikácia.

Komunikácia s uzlom siete Tor prebieha šifrovane, cez kryptografický protokol TLS (Transport Layer Security) verzie 1.2, čo potvrdí aj zobrazenie celého streamu (obr. 4.6).



Obr. 4.6: Wireshark - TCP stream.

5 LABORATÓRNA ÚLOHA Č. 1

5.1 Účel cvičenia

Zoznámiť študentov s projektom Tor, priblížiť im fungovanie anonymnej siete Tor, princíp onion router-a, princíp skrytej služby. Ukázať inštaláciu a konfiguráciu servera skrytej služby v sieti Tor. Úloha je základom pre realizáciu nasledujúcich laboratórnych úloh.

5.2 Teoretický úvod

5.2.1 Onion Router – cibuľový smerovač

Tor (The Onion Router) funguje na princípe mnohovrstvového smerovania – odtiaľ prirovnanie „cibuľový“ smerovač. O cibuľovom smerovaní bolo publikovaných už v minulosti niekoľko štúdií, návrhov siete a konceptov, žiadny projekt ale nebol nasadený pre verejné použitie ako práve projekt Tor.

5.2.2 Anonymná sieť Tor

Tor využíva distribuovanú anonymizačnú sieť, ktorú tvoria uzly – počítače dobrovoľníkov zapojených do projektu Tor. Komunikácia medzi užívateľom a uzlami siete je šifrovaná, záverečná časť cesty od výstupného uzla siete Tor po cieľový server už šifrovaná nie je.

Tor pomáha redukovať možnosť jednoduchej aj sofistikovanej analýzy prenosu údajov distribuovaním komunikačného kanálu medzi niekoľko náhodne vybraných uzlov siete v rámci internetu. Náhodný pozorovateľ teda nemôže určiť, odkiaľ údaje prichádzajú a kam smerujú.

K vybudovaniu privátneho komunikačného okruhu vytvorí klientský softvér siete Tor šifrované spojenie medzi uzlami siete. Komunikácia medzi uzlami je šifrovaná, žiadny individuálny uzol nepozná kompletnú cestu, ktorou paket prešiel.

Akonáhle je kanál otvorený, môže byť použitý rôznymi druhmi aplikácií s podporou protokolu SOCKS. Pretože žiadny uzol nevidí ďalej ako po svoj najbližší uzol, komunikácia nemôže byť analyzovaná ani použitím kompromitovaného uzla.

5.2.3 Skryté služby v sieti Tor

Tor ponúka okrem anonymizačnej siete aj službu pod názvom „skryté služby“ (Tor Hidden Services). Umožňuje užívateľom skryť polohu ich servera, na ktorom môžu

poskytovať rôzne webové služby ako napr. internetové fórum, službu na zdielanie súborov, instant messaging server. Pomocou tzv. „rendezvous“ bodov sa na server skrytej služby dokážu pripojiť ostatní užívatelia siete Tor, bez toho, aby poznali skutočnú sieťovú identitu servera.

Skrytá služba musí poslať informáciu o svojej existencii v sieti Tor ešte predtým, ako sa na ňu dokážu pripojiť ostatní užívatelia. Kvôli tomu skrytá služba náhodne vyberie niekoľko uzlov siete, vytvorí k nim okruhy a požiada ich, aby sa stali vstupnými bodmi (introduction points) skrytej služby. Týmto uzlom odošle skrytá služba svoj verejný šifrovací kľúč. Vybudovaním okruhu namiesto priameho spojenia servera skrytej služby k vstupným bodom sa zabezpečí anonymita skrytej služby a bude zložité pre útočníka asociovať vstupný bod s reálnou IP adresou servera skrytej služby.

V druhom kroku vytvorí skrytá služba deskriptor (hidden service descriptor), ktorý obsahuje jej verejný kľúč a sumárne údaje o jej vstupných bodoch (introduction points). Tento deskriptor následne podpíše svojím súkromným kľúčom a odošle ho do verejne prístupnej databázy DHT (distributed hash table).

Deskriptor bude následne poskytnutý klientovi, ktorý si ho vyžiada na základe .onion adresy v tvare xyz.onion, kde xyz tvorí 16 znakov odvodených z verejného kľúča skrytej služby. Po tomto kroku je skrytá služba vytvorená a jej adresa bude napr.: t4rvnpaleil3fnwl.onion.

Aj keď sa zdá byť používanie adresy skrytej služby v tvare automaticky generovaného hash reťazca nepraktické, prináša to isté výhody: každý, kto komunikuje so skrytou službou, či už vstupný bod, adresárová služba hash tabuliek alebo samotný klient, si môže overiť, že komunikuje so správnou skrytou službou. V budúcnosti budú možno implementované návrhy ako napr. Petname, ktoré umožnia používanie ľudsky zrozumiteľnejších a zapamätateľnejších adries .onion.

Po úspešnom propagovaní skrytej služby a jej adresy .onion ju môžu kontaktovať klienti výhradne cez sieť Tor. Klient musí najskôr poznať adresu skrytej služby. Potom kontaktuje službu DHT a získa deskriptor skrytej služby, zoznam vstupných bodov a verejný kľúč skrytej služby. Zároveň klient otvorí okruh na náhodne zvolený uzol siete, ktorý požiada, aby vystupoval ako tzv. „rendezvous“ bod (bod stretnutia) pre spojenie so skrytou službou.

Ak klient získa deskriptor skrytej služby (služba je online, klient má správnu adresu) a je pripravený okruh k bodu stretnutia, klient vytvorí úvodnú správu zašifrovanú pomocou verejného kľúča skrytej služby, v ktorej odošle informáciu o mieste stretnutia. Celá komunikácia prebieha v sieti Tor, takže klient ostáva anonymný voči skrytej službe.

V ďalšom kroku skrytá služba dekryptuje úvodnú správu od klienta a vyhľadá miesto stretnutia (rendezvous point), vybuduje k nemu okruh a vytvorí „rendezvous“ správu, ktorú odošle na toto miesto stretnutia.

V poslednom kroku bod strednutia kontaktuje klienta o úspešnom vytvorení spojenia so skrytou službou. Následne klient aj skrytá služba použijú svoje okruhy k bodu stretnutia a môžu komunikovať navzájom. Bod stretnutia (rendezvous point) jednoducho preposiela šifrované dáta od klienta k skrytej službe a naopak.

Vo všeobecnosti, kompletné spojenie medzi klientom a serverom skrytej služby pozostáva zo šiestich uzlov: tri z nich boli zvolené klientom (jeden je rendezvous bod) a ďalšie tri vybrala skrytá služba.

5.3 Pokyny a postup pre vypracovanie

5.3.1 Inštalácia LAMP – Linux, Apache, MySQL, PHP

Úloha predpokladá už nainštalovaný server s operačným systémom Debian Linux a zvládnuté príkazy „sudo“, „nano“, a „apt-get“. V ďalších krokoch bude popísaný postup inštalácie balíkov apache2, mysql-server a php5. Prihláste sa do linuxu vzdialeným prístupom, buď cez ssh, telnet alebo cez lokálny terminál. Pre účely tejto úlohy môžete v linuxe pracovať pod účtom root, ale vo všeobecnosti sa odporúča pracovať pod užívateľským účtom a používať príkaz „sudo“.

Webový server Apache nainštalujete príkazom:

```
$ sudo apt-get install apache2
```

Inštaláciu databázového servera MySQL spustíme príkazom:

```
$ sudo apt-get install mysql-server
```

V ďalšom kroku dokončíme inštaláciu príkazmi:

```
$ sudo mysql_install_db
$ sudo /usr/bin/mysql_secure_installation
```

Inštalácia PHP:

```
$ sudo apt-get install php5 php5-mysql libapache2-mod-php5
```

V konfiguračnom súbore povolíme .php súbory pre apache:

```
$ sudo nano /etc/apache2/mods-available/php5.conf
```

Upravíme riadky podľa vzoru:

```
<FilesMatch "\.ph(p3?|tml)$">
    SetHandler application/x-httpd-php
    Require all granted
</FilesMatch>
```

Funkčnosť inštalácie overíme v prehliadači otvorením url: http//localhost

V prehliadači sa otvorí úvodná stránka Apache2 Debian Default Page. Správne fungovanie php overíme nasledovne:

v adresári /var/www/html/ vytvoríme súbor info.php

```
$ sudo nano /var/www/html/info.php
```

s obsahom:

```
<?php phpinfo(); ?>
```

V prehliadači otvoríme url: http://localhost/info.php

Zobrazí sa stránka s informáciou o systéme Linux, Apache, PHP a MySQL.

5.3.2 Inštalácia Tor Hidden Service

Inštaláciu vykonáme príkazom:

```
$ sudo apt-get install tor
```

Po nainštalovaní je potrebné upraviť konfiguračný súbor torrc:

```
$ sudo mv /etc/tor/torrc /etc/tor/torrc.bak
$ sudo nano /etc/tor/torrc
```

Pre fungovanie skrytej služby stačí do súboru vložiť len 3 riadky:

```
DataDirectory /var/lib/tor
HiddenServiceDir /var/lib/tor/hidden_service/
HiddenServicePort 80 127.0.0.1:80
```

Nasleduje reštart služby tor:

```
$ sudo service tor reload
```

Po reštarte služby tor sa zapíše privátny kľúč do súboru /var/lib/tor/hidden_service/private_key a vygenerovaný názov .onion servera sa zapíše do súboru /var/lib/tor/hidden_service/hostname:

```
$ sudo cat /var/lib/tor/hidden_service/hostname
xyz.onion (pričom xyz bude jedinečný názov vašej .onion domény)
```

V poslednom kroku nainštalujte na pracovnú stanicu pod operačným systémom Linux klienta siete Tor – Tor Browser (zo stránkok www.torproject.org).

```
$ wget https://www.torproject.org/dist/torbrowser/4.5.1/
tor-browser-linux32-4.5.1_en-US.tar.xz
$ tar -xvJf tor-browser-linux32-4.5.1_en-US.tar.xz
$ cd tor-browser_en-US
$ ./start-tor-browser.desktop
```

Po spustení prehliadača Tor Browser otvorte url s názvom vašej .onion domény. Cez ikonu v tvare cibule zobrazte informáciu o aktuálne otvorenom okruhu (Tor Circuit) v sieti Tor.

5.4 Samostatná úloha

Otvorte v prehliadači Tor Browser stránku http://xyz.onion/info.php (xyz je vaša .onion doména) a uložte screenshot obrazovky do súboru. Po otvorení stránky zobrazte informáciu o aktuálnom okruhu (Tor Circuit) a uložte screenshot obrazovky do súboru. Otvorte v prehliadači ľubovoľnú stránku, napr. dsl.sk, zobrazte informácie o okruhu a uložte screenshot obrazovky.

6 LABORATÓRNA ÚLOHA Č. 2

6.1 Účel cvičenia

Zoznámiť študentov s rôznymi typmi útokov na sieť Tor za účelom deanonymizácie serverov skrytej služby. Popísať základné pravidlá, ktoré je nutné dodržiavať pri administrácii servera skrytej služby. Ukázať niekoľko možností, ako nakonfigurovať linux a služby, aby sa minimalizovalo riziko odhalenia. Overenie anonymity servera skrytej služby z úlohy č.1.

6.2 Teoretický úvod

Sieť Tor patrí medzi populárne anonymizačné siete a počet jej úžívateľov neustále narastá, je preto prirodzené, že rastie aj záujem o jej deanonymizáciu, hlavne zo strany vládnych agentúr (NSA, GCHQ). Za týmto účelom bolo vyvinutých niekoľko cielených útokov na infraštruktúru siete Tor, najmä na jej výstupné uzly. V nasledujúcej časti budú stručne popísané niektoré teoretické aj reálne útoky.

6.2.1 Sniper Attack

Sniper Attack je útok, ktorý za použitia vyrazne nízkych nákladov dokáže znefunkčniť najpoužívanejšie výstupné uzly siete Tor. Na dosiahnutie cieľa používa deštruktívny DoS útok proti týmto uzlom. Útok prebieha exploitnutím validných správ protokolu Tor, pomocou ktorých dokáže útočník zahltiť operačnú pamäť počítača. Experimenty ukázali, že útočník dokáže alokovať operačnú pamäť rýchlosťou 2187 KiB/s, pričom na to potrebuje prenosovú rýchlosť iba 92 KiB/s. Pri reálnom použití útoku došlo behom 29 minút k výpadku 20 najpoužívanejších výstupných uzlov siete. Tento útok dokáže deanonymizovať skryté služby (server .onion) selektívnym DoS útokom a prinútením .onion servera, aby použil uzol, ktorý je pod kontrolou útočníka.

DoS útok je smerovaný proti tzv. guarding relays, proti uzlom siete, ktoré chránia skrytú službu. Útočník dokáže deanonymizovať server skrytej služby behom niekoľkých dní s použitím bežného hardvéru a internetového pripojenia. Pri použití výkonejšieho vybavenia sa skráti čas potrebný na odhalenie na niekoľko hodín. Útok bol úspešne simulovaný v testovacom prostredí Shadow, bez ohrozenia reálnej prevádzky siete Tor.

Deanonymizačný útok prebieha v troch krokoch:

1. Identifikácia ochranných uzlov skrytej služby
2. Znefukčnenie týchto uzlov použitím Sniper Attack

3. Testovanie, či si skrytá služba vybrala náhradný uzol pod kontrolou útočníka. Ak nie, opakuje sa postup od kroku č.1.

6.2.2 RAPTOR

Útok RAPTOR (Routing Attacks on Privacy in Tor) využíva známu zraniteľnosť siete Tor, keď útočník sleduje kominukáciu na oboch stranách siete. Následným porovnaním a koreláciou paketov, ich veľkosti a času, dokáže deanonymizovať klientov siete Tor.

Útok je realizovaný pomocou autonómnych systémov, ktoré zaznamenávajú prevádzku siete a realizujú koreláciu metadát z paketov. Často sú súčasťou siete Tor v pozícii výstupných uzlov. Veľké autonómne systémy ISP dokážu zbierať údaje o každom pakete v rámci ich siete. Ako poukázal Edward Snowden, agentúra NSA v projekte Marina ukladá meta informácie o komunikácií užívateľov počas jedného roku, obdobný projekt Tempora agentúry GCHQ ukladá meta informácie 30 dní a celé pakety ukladá 3 dni.

RAPTOR sa skladá z troch individuálnych útokov:

1. RAPTOR využíva asymetrický spôsob smerovania internetových paketov. Trasa BGP (Border Gateway Protocol) od zdrojového počítača po cieľový počítač sa môže líšiť od spätnej trasy BGP od cieľa ku zdroju. Asymetria v smerovaní zvyšuje šancu sledovania aspoň jedného smeru komunikácie.
2. RAPTOR využíva prirodzené zmeny v BGP trasách spôsobené výpadkom liniek alebo sieťových prvkov. Zmeny v BGP trasách umožňujú autonómnym systémom odsledovať dodatočnú komunikáciu a tým deanonymizovať zvýšený počet klintov v sieti Tor.
3. RAPTOR využíva vnútornú zraniteľnosť internet routingu – útočník môže manipulovať smerovanie pomocou techník ako BGP hijack voči sieti Tor.

6.2.3 Sybil Attack

Útok označovaný ako Sybil, nie je špecifický len pre sieť Tor, ale je všeobecne použiteľný pre akúkoľvek sieť peer-to-peer. V roku 2014 bol zaznamenaný veľký útok Sybil na sieť Tor, ktorý zatiaľ nebol úplne analyzovaný. Do siete Tor bolo prihlásených 115 nových rýchlych vnútorných uzlov (nie výstupných), ktoré boli pod kontrolou útočníka. Spolu tvorili približne 6% ochrannej kapacity siete. Po približne piatich mesiacoch sa z nich v rámci bežnej rotácie stali vstupné uzly pre významne vysoký počet užívateľov. Spolu s ďalším typom útoku s názvom „traffic confirmation attack“ sa podarilo deanonymizovať časť siete so skrytými službami.

6.2.4 Deanonymizácia spôsobená nevhodnou správou servera

Prevádzková bezpečnosť servera je dôležitou súčasťou celkovej bezpečnosti služby Hidden Service a jej dodržiavaním dokážeme vyznamne znížiť možnosť prezradenia skutočnej IP adresy servera skrytej služby. Prevádzkovatelia skrytej služby si často neuvedomujú možné riziká, nemajú potrebné teoretické ani praktické skúsenosti. V nasledujúcej časti budú popísané možné riziká deanonymizácie skrytej služby, ktoré sú zapríčinené jej prevádzkou.

1. Infiltrácia agenta v prestrojení - Dôležitou súčasťou bezpečnosti Hidden Service je klásť veľký dôraz na preverenie nových ľudí, ktorí sú príjmaní medzi správcov servera. Pri veľkých a populárnych serveroch sa častokrát stáva, že súčasťou tímu je cudzí agent, čo vedie po určitej dobe nielen k prezradeniu identity prevádzkovateľa, ale aj zozbieraním vecných dôkazov proti nemu.
2. SQL injections Množstvo Hidden Service serverov ponúka svoje služby a produkty cez nekvalitne naprogramované php / mysql online obchody, ktoré obsahujú veľa chýb a tým ponúkajú možnosť útoku typu SQL injections.
3. Deanonymizácia platobného systému - Väčšina serverov ponúka možnosť buď dobrovoľného príspevku (donation) na podporu svojej činnosti, alebo vyžaduje platbu za svoje služby alebo produkty. Preto je dôležité pre prevádzkovaľa zvoliť platobný systém, ktorý spĺňa podmienku anonymity. V dnešnej dobe patrí medzi najpoužívanejšie anonymné platobné systémy práve Bitcoin. Aj keď je Bitcoin všeobecne považovaný za anonymný, niekoľko prípadov a štúdií z minulosti ukazuje, že aj pri jeho používaní je potrebné dbať na základné pravidlá dodržania anonymity.
4. Konfigurácia servera skrytej služby - Správna konfigurácia služieb bežiacich na serveri môže výrazne znížiť riziko odhalenia polohy alebo IP adresy. Je vhodné vypnúť chybové hlásenia web servera, ktoré by mohli prezradit informácie o systéme alebo časovom pásme. Tiež je potrebné vykonávať pravidelné bezpečnostné aktualizácie celého systému a používaných služieb. Na serveri sa neodporúča prevádzkovať mailový server.
5. Dedikovaný server pre skrytú službu - Vo všeobecnosti sa neodporúča prevádzkovať na jednom serveri skrytú službu spolu so službou Tor Relay, pretože uzly siete Tor sú verejné a z dlhodobého sledovania ich prevádzky a prevádzky skrytej služby je možné deanonymizovať skrytú službu. Tiež platí pravidlo, že čím dlhšie beží skrytá služba, tým viac údajov o nej sa dá zozbierať, a tým väčšia je šancia na jej odhalenie.

6.2.5 Zachovanie anonymity v sieti Tor

Tor nedokáže vyriešiť všetky problémy týkajúce sa anonymity. Je zameraný iba na zabezpečenie prenosu údajov cez internet. Užívateľom sa odporúča dodržiavať ďalšie všeobecné pravidlá pre zachovanie anonymity v sieti Tor:

- Používanie prehliadača Tor (Tor Browser) – tento prehliadač je predkonfigurovaný na bezpečné používanie v sieti Tor.
- Neopoužívať torrent klienta v sieti Tor – veľa klientov obchádza Tor a odhaľuje tak skutočnú IP adresu užívateľa.
- Nepoužívať prídavné moduly v prehliadačoch (browser add-ons) – častokrát tieto moduly obchádzajú nastavenie siete Tor a deanonymizuju užívateľský počítač.
- Používať HTTPS verzie stránok, ak sú k dispozícii – komunikácie v sieti Tor medzi uzlami siete je šifrovaná, ale posledný úsek od výstupného uzla po cieľový server je závislý od použitého protokolu na prenos údajov.
- Neotvárať stiahnuté dokumenty počas aktívnej siete Tor – dokumenty ako napr. DOC alebo PDF môžu obsahovať externé odkazy, ktoré môžu obísť sieť Tor a odhaliť tak skutočnú IP adresu počítača.
- Využívať premostenie namiesto bežného pripojenia na vstupný uzol siete Tor – lokálny ISP môže analýzou sieťovej prevádzky detekovať používanie siete Tor. Ak je to nežiadúce, je možné pripojenie do siete Tor cez premostenie (Tor Bridge Relay). V takom prípade ani ISP nedokáže rozpoznať využívanie siete Tor.

6.2.6 Pravidlá pre prevádzkovanie servera skrytej služby

1. Neprevádzkujte server skrytej služby na virtuálnych serveroch, pokiaľ nemáte kontrolu nad fyzickým hardvérom.
2. Je bezpečnejšie použiť dva fyzické servre, od dvoch rôznych poskytovateľov, môžu sa nachádzať aj v jednom datacentre. Na prvom serveri beží virtual machine. Host aj VM je chránená firewall-om, ktorý obmedzuje obojtranný prenos len na komunikáciu v sieti Tor a medzi druhým serverom. Druhý server obsahuje iba VM so skrytou službou. Spojenie medzi servermi by malo byť zabezpečené pomocou IPsec alebo OpenVPN. V prípade podozrenia, že prvý server bol kompromitovaný, druhý server by mal byť okamžite premiestnený (kópia VM image) a obidva servre vypnuté. Celý tento postup sa dá zrealizovať použitím Whonix (whonix.org).
3. Pre server skrytej služby nie je vhodné prenajať server v cloude. Je dôležité sledovať fyzické parametre servera a v prípade výpadku ho považovať za kompromitovaný, pretože nie je možné rozlíšiť jednoduchú hardvérovú poruchu od

útoku a kompromitácie.

4. Úvodná inštalácia servera u providera sa musí vykonať z ním povolených adries. Neodporúča sa prihlasovať na server z domu, z práce alebo z miesta, na ktorom ste boli už predtým.
5. Po inštalácii skrytej služby sa na ňu nikdy nepripájajte z otvorenej siete, vždy len zo siete Tor. V prípade núdze, ak je potrebný rýchly zásah, pripojte sa len z miesta, z ktorého sa v budúcnosti už nepripojíte.
6. Premiestňujte pravidelne server skrytej služby, aj keď nie je dôvod považovať server za kompromitovaný. Známe útoky na sieť Tor dokážu deanonymizovať sieť za niekoľko mesiacov. Preto je vhodné premiestňovať server tak často, ako to je len možné, minimálne raz za mesiac. Sieti Tor trvá približne hodinu, kým rozpozná novú polohu premiestneného servera.

6.3 Pokyny a postup pre vypracovanie

6.3.1 Konfigurácia webového servera Apache

Pri otvorení neexistujúcej stránky vypíše apache chybovú hlášku, ktorá obsahuje informáciu o systéme a verzii. Nasledovnou úpravou toto chybové hlásenie vypneme:

```
# nano /etc/apache2/conf-enabled/security.conf
```

Upravíme konfiguračný súbor podľa vzoru:

```
ServerSignature Off
ServerTokens Prod
```

Reštartujeme službu apache:

```
$ sudo service apache2 restart
```

6.3.2 Odinštalovanie nevhodných balíkov

Niektoré príkazy, ktoré poskytujú informácie o systéme, môžu byť zneužité za účelov získania informácií o systéme: wget, sendmail, postfix, exim (alebo iný MTA). Tiež je vhodné vypnúť logovanie (rsyslog).

Odinštalujte potenciálne nebezpečné balíky:

```
$ sudo apt-get remove --purge rsyslog
$ sudo apt-get remove --purge wget
$ sudo apt-get remove --purge exim
$ sudo apt-get remove --purge postfix
$ sudo apt-get remove --purge sendmail
```

Ak plánujete využívať na vzdialené pripojenie ssh, je vhodné vypnúť „Debian banner“, ktorý poskytuje verziu Debian-u.

Do konfiguračného súboru /etc/ssh/ssh_config:

```
$ nano /etc/ssh/ssh_config
```

vložíme riadok:

```
DebianBanner  no
```

6.3.3 Overenie anonymity komunikácie klient-server

Na pracovnej stanici pod operačným systémom Linux spustite Tor Browser. Ak nie je nainštalovaný, stiahnite aktuálnu verziu tor-browser zo stránok www.torproject.org a postupujte nasledovne:

```
$ wget https://www.torproject.org/dist/torbrowser/4.5.1/
tor-browser-linux32-4.5.1_en-US.tar.xz
$ tar -xvJf tor-browser-linux32-4.5.1_en-US.tar.xz
$ cd tor-browser_en-US
$ ./start-tor-browser.desktop
```

Nainštalujte a spustite program tshark (konzolová verzia programu Wireshark). Ide o paketový analyzér určený na zachytávanie sieťovej komunikácie. Pomocou parametru w zaznam.pcap"budú zachytené údaje zapísané do súboru zaznam.pcap:

```
$ sudo apt-get install tshark
$ sudo tshark -w zaznam.pcap
```

Po spustení zachytávania paketov otvorte v prehliadači Tor Browser adresu vášho .onion servera. Po načítaní úvodnej stránky skrytej služby zastavte zachytávanie paketov klávesmi CTRL+C. Zapísané údaje zobrazte príkazom:

```
$ sudo tshark -r zaznam.pcap
```

Výstup bude vyzerať nasledovne:

```
1 0.000000000 192.168.0.104 -> 255.255.255.255
 UDP 126 Source port: 65451  Destination port: 10505
2 2.004046000 192.168.0.104 -> 255.255.255.255
 UDP 126 Source port: 65452  Destination port: 10505
3 4.011516000 192.168.0.104 -> 255.255.255.255
```

```
 UDP 126 Source port: 65453  Destination port: 10505
4 4.870549000 147.102.216.242 -> 192.168.0.102
 TCP 609 8995→56007 [PSH, ACK] Seq=1 Ack=1 Win=6985
 Len=543 TSval=725797987 TSecr=24589287
5 4.870622000 192.168.0.102 -> 147.102.216.242
 TCP 66 56007→8995 [ACK] Seq=1 Ack=544 Win=2693
 Len=0 TSval=24648960 TSecr=725797987
6 4.884840000 192.168.0.102 -> 147.102.216.242
 TCP 609 56007→8995 [PSH, ACK] Seq=1 Ack=544 Win=2693
 Len=543 TSval=24648963 TSecr=725797987
7 4.991449000 147.102.216.242 -> 192.168.0.102
 TCP 66 8995→56007 [ACK] Seq=544 Ack=544 Win=6985
 Len=0 TSval=725798018 TSecr=24648963
8 4.991480000 192.168.0.102 -> 147.102.216.242
 TCP 609 56007→8995 [PSH, ACK] Seq=544 Ack=544 Win=2693
 Len=543 TSval=24648990 TSecr=725798018
9 5.059028000 147.102.216.242 -> 192.168.0.102
 TCP 66 8995→56007 [ACK] Seq=544 Ack=1087 Win=6952
 Len=0 TSval=725798035 TSecr=24648990
10 5.068285000 147.102.216.242 -> 192.168.0.102
 TCP 609 8995→56007 [PSH, ACK] Seq=544 Ack=1087 Win=6985
 Len=543 TSval=725798037 TSecr=24648990
11 5.074969000 192.168.0.102 -> 147.102.216.242
 TCP 609 56007→8995 [PSH, ACK] Seq=1087 Ack=1087 Win=2693
 Len=543 TSval=24649011 TSecr=725798037
12 5.145333000 147.102.216.242 -> 192.168.0.102
 TCP 609 8995→56007 [PSH, ACK] Seq=1087 Ack=1630 Win=6952
 Len=543 TSval=725798056 TSecr=24649011
13 5.147217000 192.168.0.102 -> 147.102.216.242
 TCP 609 56007→8995 [PSH, ACK] Seq=1630 Ack=1630 Win=2693
 Len=543 TSval=24649029 TSecr=725798056
```

V našom prípade klient komunikoval s Tor uzlom s IP adresou 147.102.216.242.

Rovnakým spôsobom sa môžeme presvedčiť, že server skrytej služby komunikuje len s prvým uzlom vo svojom okruhu. K tomu účelu potrebujeme nainštalovať aj na server program Wireshark alebo konzolovú verziu tshark.

Analýza sieťovej komunikácie na strane klienta aj na strane servera potvrdzuje fakt, že klient a server ostávajú anonymní aj navzájom voči sebe, komunikujú spolu výhradne len cez sprostredkovateľa - tzv. rendezvous point.

6.4 Samostatná úloha

Otvorte v prehliadači Tor Browser neexistujúcu stránku napr. http://xyz.onion/4.php (xyz je vaša .onion doména). Presvedčte sa, že chybové hlásenie, ktoré vygeneruje apache, neobsahuje informácie o vašom systéme. Uložte screenshot obrazovky do súboru.

Zobrazte všetky aktívne procesy v linuxe príkazom:

```
$ sudo ps -A
```

Pokúste sa identifikovať procesy, ktoré nie sú potrebné pre správne fungovanie skrytej služby, a ktoré by bolo možné vypnúť alebo odinštalovať. Zoznam vybratých procesov zapíšte do súboru.

7 ZÁVER

Cieľom tejto bakalárskej práce bol podrobný popis služby Hidden Service v sieti Tor. V teoretickej časti bol stručne popísaný princíp fungovania anonymnej siete Tor a užívateľsky vysvetlený komunikačný protokol skrytej služby. Ďalej boli popísané niektoré typy útokov na sieť Tor za účelom deanonymizácie serverov skrytých služieb a odhalenia ich skutočnej IP adresy. Niektoré útoky boli navrhnuté len teoreticky a testované v prostredí Shadow, nie v reálnej sieti Tor. Tvorcovia projektu Tor vedia o týchto nedostatkoch a slabých miestach v sieti a protokole, snažia sa ich opraviť, prípadne implentovať obranu proti známym typom útokov.

V ďalšej časti práce sme sa zamerali na možnosť deanonymizácie skrytej služby nesprávnou prevádzkou webových stránok alebo iných služieb bežiacich na serveri skrytej služby. Realita ukázala, že práve toto bezpečnostné zlyhanie ma vysoký podiel na odhalení serverov skrytých služieb. Preto je mimoriadne dôležité venovať tejto problematike zvýšenú pozornosť. A to nielen správnemu nastaveniu servera, ale aj následnej administrácii služieb na ňom bežiacich.

V praktickej časti bol nakonfigurovaný server skrytej služby bežiaci pod operačným systémom Linux, s web serverom Apache, databázovým serverom MySQL a PHP. Na testovací server bol nainštalovaný softvér ownCloud, ktorý umožňuje nahrávanie, zálohovanie a zdielanie súborov cez prehliadač. Funkčný server skrytej služby a ownCloud je dostupný na adrese http://t4rvnpaleil3fnwl.onion/owncloud.

Na záver bola zrealizovaná analýza sieťovej prevádzky v programe Wireshark. Analyzovaná bola reálna komunikácia medzi klientom (Tor Browser pod operačným systémom Windows) a serverom skrytej služby. Výsledok analýzy potvrdil princíp fungovania siete Tor a skrytej služby popísanej v teoretickej časti.

Súčasťou bakalárskej práce sú dve laboratórne úlohy zamerané na inštaláciu a konfiguráciu skrytej služby v sieti Tor a celkovú bezpečnosť skrytej služby. Absolvovaním úloh si študenti osvoja poznatky potrebné pre zachovanie najcennejšej komodity dnešnej doby, súkromia.

LITERATÚRA

[1] BALL, J. *NSA stores metadata of millions of web users for up to a year, secret files show.* [online]. 2013, [cit. 15. 5. 2015]. Dostupné z URL: <http://www.theguardian.com/world/2013/sep/30/nsa-americans-metadata-year-documents>.

[2] BIRYUKOV, A. *Deanonymisation of clients in Bitcoin P2P network.* [online]. 2014, [cit. 15. 5. 2015]. Dostupné z URL: <http://arxiv.org/pdf/1405.7418v3>.

[3] BIRYUKOV, A. *Trawling for Tor Hidden Services: Detection, Measurement, Deanonymization.* [online]. 2013, [cit. 15. 5. 2015]. Dostupné z URL: <http://www.ieee-security.org/TC/SP2013/papers/4977a080.pdf>.

[4] DINGLEDINE, R. *Tor: The Second-Generation Onion Router.* [online]. 2004, [cit. 15. 5. 2015]. Dostupné z URL: <http://www.onion-router.net/Publications/tor-design.pdf>.

[5] FEDERRATH, H. *Designing privacy enhancing technologies: International Workshop on Design Issues in Anonymity and Unobservability.* 2001, 18-65, 230 p. ISBN 35-404-1724-9.

[1] FEDERRATH, Hannes. Designing privacy enhancing technologies: International Workshop on Design Issues in Anonymity and Unobservability, Berkeley, CA, USA, July 25-26, 2000 : proceedings. New York: Springer, 2001, 18-65, 230 p. ISBN 35-404-1724-9.

[6] GELLMAN, B. *US Intelligence Mining Data from Nine U.S. Internet Companies in Broad Secret Program.* [online]. 2013, [cit. 15. 5. 2015]. Dostupné z URL: <http://www.washingtonpost.com/investigations/us-intelligence-mining-data/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html>.

[7] GOLDSCHLAG, D.M. *Hiding routing information.* In R. Anderson, editor, Information Hiding, First International Workshop , pages 137–150. Springer- Verlag, LNCS 1174, May 1996.

[8] JANSEN, R. *Shadow: Running Tor in a Box for Accurate and Efficient Experimentation.* [online]. 2011, [cit. 15. 5. 2015]. Dostupné z URL: <http://www.robgjansen.com/publications/shadow-ndss2012.pdf>.

[9] JANSEN, R. *The Sniper Attack: Anonymously Deanonymizing and Disabling the Tor Network.* 2014. ISBN 1-891562-35-5.

[10] MATHEWSON, N. *Initial thoughts on migrating Tor to new cryptography.* [online]. 2010, [cit. 15. 5. 2015]. Dostupné z URL: <https://gitweb.torproject.org/torspec.git/tree/proposals/ideas/xxx-crypto-migration.txt>.

[11] OVERLIER, L. *Improving Efficiency and Simplicity of Tor Circuit Establishment and Hidden Services.* 2007. ISBN 978-3-540-75550-0

[12] OVERLIER, L. *Valet Services: Improving Hidden Servers with a Personal Touch.* [online]. 2006, [cit. 15. 5. 2015]. Dostupné z URL: <http://www.onion-router.net/Publications/valet-services.pdf>.

[13] REED, M.G. *Anonymous connections and onion routing.* IEEE Journal on Selected Areas in Communications, 16(4):482–494, May 1998.

[14] ROGOFF, Z. *Protect your freedom and privacy; join us in creating an Internet that's safer from surveillance.* [online]. 2013, [cit. 15. 5. 2015]. Dostupné z URL: <https://www.fsf.org/campaigns/surveillance>.

[15] STIEGLER, M. *An Introduction to Petname Systems.* [online]. 2010, [cit. 15. 5. 2015]. Dostupné z URL: <http://www.skyhunter.com/marcs/petnames/IntroPetNames.html>.

[16] SYVERSON, P. *Onion Routing access configurations.* In DARPA Information Survivability Conference and Exposition (DISCEX 2000) , volume 1, pages 34–40. IEEE CS Press, 2000.

[17] SYVERSON, P. *Towards an Analysis of Onion Routing Security.* In H. Federrath, editor, Designing Privacy Enhancing Technologies: Workshop on Design Issue in Anonymity and Unobservability, pages 96–114. Springer-Verlag, LNCS 2009, July 2000.

[18] TOR PROJECT. *Hidden Service Protocol.* [online]. 2015, [cit. 15. 5. 2015]. Dostupné z URL: <https://www.torproject.org/docs/hidden-services.html.en>.

[19] TOR PROJECT. *Tor Project: Overview.* [online]. 2015, [cit. 15. 5. 2015]. Dostupné z URL: <https://www.torproject.org/about/overview>.

[20] TOR PROJECT. *Tor security advisory: Relay early traffic confirmation attack.* [online]. 2014, [cit. 15. 5. 2015]. Dostupné z URL: <https://blog.torproject.org/blog/tor-security-advisory-relay-early-traffic-confirmation-attack>.

[21] YIXIN, S. *RAPTOR: Routing Attacks on Privacy in Tor.* [online]. 2015, [cit. 15. 5. 2015]. Dostupné z URL: <http://arxiv.org/pdf/1503.03940v1.pdf>.

ZOZNAM SYMBOLOV, VELIČÍN A SKRATIEK

Tor	The Onion Router
SaaSS	Service as a Software Substitute
ISP	internet service provider
NSA	National Security Agency, USA
GCHQ	Government Communications Headquarters, UK
EFF	Electronic Frontier Foundation
SOCKS	Socket Secure
BGP	Border Gateway Protocol
DoS	Denial of Service
QoS	Quality of Service
HSDir	Hidden Service Directory Servers
SSH	Secure Shell
DHT	Distributed Hash Table
TLS	Transport Layer Security
MTA	Mail Transfer Agent