UNIVERZITA KONŠTANTÍNA FILOZOFA V NITRE

FAKULTA PRÍRODNÝCH VIED

Tor: Tvorba wifi hotspotu pre anonymný web

Seminárna práca

Nitra 2021 Vlčák, Stranovská, Rusňák

# Obsah

[Tor: Tvorba wifi hotspotu pre anonymný web1](#_Toc71830044)

[Obsah2](#_Toc71830045)

[Zoznam ilustrácií a tabuliek4](#_Toc71830046)

[Úvod5](#_Toc71830047)

[1 Analýza súčasného stavu6](#_Toc71830048)

[1.1 Princíp anonymizácie6](#_Toc71830049)

[1.2 Tor7](#_Toc71830050)

[1.2.1 Tor sieť8](#_Toc71830051)

[1.2.2 Slabé stránky9](#_Toc71830052)

[1.2.3 Útoky na Tor9](#_Toc71830053)

[2 Ciele seminárnej práce11](#_Toc71830054)

[3 Riešenie seminárnej práce12](#_Toc71830055)

[3.1 Príprava WIFI hotspotu pre anonymné siete12](#_Toc71830056)

[3.1.1. Napálenie Raspbian OS12](#_Toc71830057)

[3.1.2. Inštalácia a konfigurácia „hostapd“13](#_Toc71830058)

[3.1.3. Inštalácia a konfigurácia „udhcpd“16](#_Toc71830059)

[3.1.4. Konfigurácia sieťového rozhrania17](#_Toc71830060)

[3.1.5. Inštalácia a konfigurácia „tor“18](#_Toc71830061)

[3.1.6. Konfigurácia „iptables“20](#_Toc71830062)

[3.1.7. Nastavenie IP forwarding20](#_Toc71830064)

[3.1.8. Zakázanie niektorých predvolených deamonov21](#_Toc71830065)

[3.1.9. Reštart zariadenia a kontrola21](#_Toc71830066)

[3.2 Testovanie23](#_Toc71830068)

[3.2.1 Check.torproject.org23](#_Toc71830069)

[3.2.2 IP chicken24](#_Toc71830070)

[3.2.3 DNS test priepustnosti26](#_Toc71830071)

[3.2.4 Browserleaks.com26](#_Toc71830072)

[3.2.5 Speedtest27](#_Toc71830073)

[3.2.6 Prístup do hidden services28](#_Toc71830074)

[3.2.7 Youtube29](#_Toc71830075)

[4 Výsledky riešenia a ich zhodnotenie30](#_Toc71830076)

[4.1 Dopad na rýchlosť30](#_Toc71830077)

[4.2 DNS test priepustnosti30](#_Toc71830078)

[4.3 Limitácie Siete31](#_Toc71830079)

[Záver32](#_Toc71830080)

[Zoznam bibliografických odkazov33](#_Toc71830081)

[Zoznam príloh36](#_Toc71830082)

# Zoznam ilustrácií a tabuliek

Obrázok 1 Porovnanie bežnej a anonymizovanej komunikácie 7

Obrázok 2 Sieť Tor 9

Obrázok 3 Slabiny Tor 9

Obrázok 4 Sieťový tok 11

Obrázok 5 Napálenie Rasbian OS 13

Obrázok 6 Konfiguračný súbor etc/hostapd/hostapd.conf 15

Obrázok 7 Konfiguračný súbor /etc/default/hostapd 15

Obrázok 8 Overenie funkčnosti služby po reštarte 16

Obrázok 9 Konfiguračný súbor /etc/udhcpd.conf 17

Obrázok 10 Konfiguračný súbor /etc/default/udhcpd 17

Obrázok 11 Overenie funkčnosti udhcpd 18

Obrázok 12 Konfiguračný súbor /etc/network/interfaces 19

Obrázok 13 Konfiguračný súbor /etc/tor/torrc 20

Obrázok 14 Konfiguračný súbor /etc/iptables.ipv4 21

Obrázok 15 Konfiguračný súbor /etc/sysctl.conf 22

Obrázok 16 Ukážka pripojenia 24

Obrázok 17 Torproject test pred pripojením do Tor siete 25

Obrázok 18 Torproject test po pripojením do Tor siete 25

Obrázok 19 IP chicken test pred pripojením do Tor siete 26

Obrázok 20 IP chicken test po pripojením do Tor siete 26

Obrázok 21 DNS test priepustnosti 27

Obrázok 22 Browserleaks test 28

Obrázok 23 Speedtest pred pripojením do Tor siete 29

Obrázok 24 Speedtest po pripojení do Tor siete 29

Obrázok 25 Hidden services test pred pripojením do Tor siete 30

Obrázok 26 Hidden services test po pripojenía do Tor siete 30

# Úvod

Slovo „internet“ sa stalo domáckym pojmom. Už aj malé dieťa dnes vie, ako sa pripojiť na sieť, alebo že informácia je „dostupná na internete“. To, čo bolo predtým nástroj iba pre seriózne vedecké publikum, sa stalo všadeprítomným. Dnes je možné nájsť sieťovo prepojené gadgety všade: počínajúc od počítačov, mobilných zariadení, až po rozmanité IoT zariadenia sprevádzajúce nás na každom kroku v dnešnej „Kultúre Internetu“ (Kirch, 1993).

Služby internetu využíva obrovské množstvo používateľov každý deň. S prepojenosťou zariadení a stúpajúcim množstvom „premávky“ na internete sa však vynárajú otázky. Je komunikácia na internete bezpečná? Kto všetko môže vidieť moju aktivitu? Je možné, že aj bez môjho vedomia, ISP - poskytovateľ internetových služieb - na rozkaz štátu cenzuruje, kam mám a kam nemám prístup? Na tieto otázky nebolo myslené, keď bol navrhnutý internet. Preto sa vynára otázka: Čo môžem spraviť pre ochranu svojho súkromia na internet?

V dnešnej dobe existujú mnohé technológiu slúžiace na zvyšovanie ochrany súkromia a samotná ENISA podporuje ich používanie vo svojom projekte s rovnomerným názvom PETs (privacy enhancing technologies).

Jedným z riešení dostupných zvyšovanie ochrany súkromia a anonymizácie komunikácie práve používanie siete Tor.

Tor, The Onion Router, je svetová sieť serverov vyvinutá americkým námorníctvom, ktorá agentom mala umožniť bezpečnejšiu, anonymnú komunikáciu. V súčasnej dobe Tor zastrešuje nezisková organizácia, ktorej hlavným účelom je výskum a vývoj online nástrojov na ochranu osobných údajov. Tor je jedným z najjednoduchších spôsobov anonymizácie. Za predpokladu, že poznáme pravidlá (plaintext je vždy len plaintext, či ide cez Tor alebo nie), stačí stiahnuť Tor prehliadač a o jednu vrstvu ochrany súkromia máme naviac.

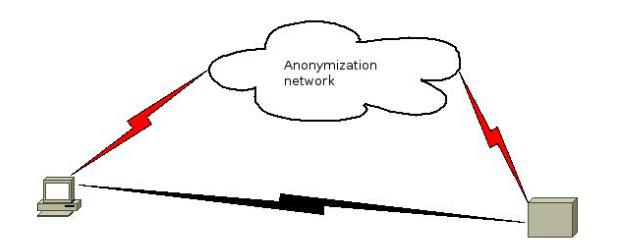
Ak chceme zabezpečiť Tor na viacerých zariadeniach, buď musíme nastaviť každé individuálne, alebo je možné použiť Raspberry Pi ako bezdrôtový prístupový bod a prevádzkovať samostatnú sieť, buď pomocou zabudovaných bezdrôtových funkcií Raspberry Pi 3 alebo Raspberry Pi Zero W. A práve tento princíp WiFi hotspotu pre anonymný web budeme skúmať v našej práci.

# 1 Analýza súčasného stavu

Danezis a Diaz definujú anonymitu ako „stav, keď nie je možné ju identifikovať v rámci súboru subjektov, súbor anonymity“. Táto definícia hovorí, že používateľ na internete by nemal byť identifikovateľný prostredníctvom svojho sieťového prenosu o nič viac ako ktorýkoľvek používateľ internetu, že by pri analýze sieťového prenosu nemal používať charakteristiky identity používateľa. Je potrebné poznamenať, že v sieťovom prenose identifikačné znaky, ako sú hlavičky IP a číslo portu sú používané, aby počítače na prijímacom konci boli schopné rozpoznať zdrojovú a cieľovú IP adresu. Vhodnejším pojmom pre systémy ako sú tieto, by mohla byť neprepojitelnosť, ktorá je definovaná tak, aby zabezpečila, že používateľ môže viacnásobne využívať zdroje alebo služby bez toho, aby ostatní boli schopní tieto použitia prepojiť. Neprepojitelnosť vyžaduje, aby používatelia alebo subjekty nedokázali určiť, či ten istý používateľ spôsobil určité špecifické operácie v systéme. Jednoducho povedané je definovaný ako rozloženie, pri ktorom nie je možné prepojiť sieťový prenos s konkrétnym používateľom, čo je presnejšie. na opísanie úrovne služieb, ktoré systémy poskytujú cez internet (Choudhary, Bhagat 2018).

## Princíp anonymizácie

Aby sa zabránilo zverejneniu IP adresy klienta, boli vyvinuté rôzne nástroje na anonymizáciu webu. Prakticky všetky sa zameriavajú na utajenie IP adresy IP, pretože utajenie druhej IP adresy na strane servera sa zdá byť nerealizovateľná kvôli vlastnostiam schém adresovania používaných v internete (predovšetkým služba DNS). Základný princíp anonymizačných nástrojov je znázornený na Obr.1. Medzi anonymizačnými nástrojmi je Tor (The Onion Routing project) jedným z najstarších a najznámejších. Zatiaľ čo pôvodnou myšlienkou Tor bolo pomáhať ľuďom žijúcim v štátoch s autoritatívnou vládou, jej dostupnosť tiež pomohla zločincom vylepšiť ich schopnosť skryť svoje aktivity pred políciou. Niektoré ďalšie nástroje ,ktoré sa neskôr objavili, menovite I2P a JAP/JonDo alebo VPN (Klimeš, Sochor 2018).



Obrázok 1 Porovnanie bežnej a anonymizovanej komunikácie[[1]](#footnote-2)

## Tor

Tor Project, Inc, sa stal neziskovou organizáciou v roku 2006, ale myšlienka onion routing začala v polovici 90. rokov. V 90. rokoch sa objavil problém nedostatku bezpečnosti na internete a jeho schopnosť využívať ho na sledovanie a sledovanie. V roku 1995 si David Goldschlag, Mike Reed a Paul Syverson z amerického laboratória pre námorný výskum (NRL) položili otázku, či existoval spôsob, ako vytvoriť internetové pripojenie, ktoré neodhaľuje, kto s kým komunikuje, dokonca ani niekto, kto sleduje sieť. Ich odpoveďou bolo vytvorenie a nasadenie prvých výskumných návrhov a prototypov onion routingu.

Cieľom onion routingu je nájsť spôsob, ako používať internet s čo najväčším súkromím, a myšlienkou bolo smerovať prenos cez viac serverov a šifrovať ho na každom kroku. Na začiatku roku 2000 začal Roger Dingledine pracovať na projekte onion routingu NRL s Paulom Syversonom. Na odlíšenie tejto pôvodnej práce v NRL od iných snáh onion routingu, ktoré sa začali objavovať inde, Roger nazval projekt Tor, ktorý znamenal The Onion Routing. Od svojho založenia v 90. rokoch bol onion routing koncipovaný tak, že sa spolieha na decentralizovanú sieť. Sieť museli prevádzkovať subjekty s rôznymi predpokladmi záujmov a dôvery a softvér musel byť slobodný a otvorený, aby sa maximalizovala transparentnosť a oddelenie. Preto v októbri 2002, keď bola sieť Tor pôvodne zavedená, bol jej kód vydaný na základe bezplatnej a otvorenej softvérovej licencie. Do konca roku 2003 mala sieť asi tucet dobrovoľníckych uzlov, väčšinou v USA, a jeden v Nemecku.

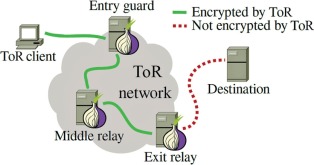
Tor si začal získavať popularitu medzi aktivistami a technicky zdatnými používateľmi zaujímajúcimi sa o súkromie, ale pre menej technicky zdatných ľudí bolo stále ťažké ich používať, a tak od roku 2005 začal vývoj nástrojov presahujúcich iba Tor proxy. Vývoj prehliadača Tor sa začal v roku 2008. Vďaka prehliadaču Tor, ktorý sprístupnil Tor bežným používateľom internetu a aktivistom, bol Tor nástrojom počas arabskej jari, ktorá sa začala koncom roka 2010. Nielenže chránil identitu ľudí online, ale umožňoval im prístup ku kritickým zdrojom, sociálnym médiám a webovým stránkam. ktoré boli zablokované (Tor 2021).

### Tor sieť

Tor anonymizuje vytvorením prekrývacej siete zloženej z uzlov, ktoré náhodne preposielajú údaje používateľov medzi pôvodcom (zdrojom) a cieľom. Tor preto funguje v tradičnej sieti TCP / IP, nastavuje prekrývajúcu sa sieť, ktorá skrýva identitu zdrojového aj cieľového uzla a zachováva dôvernosť prechádzajúcich paketov. Sieť Tor sa skladá z :

* *Klient Tor* je softvér nainštalovaný na zariadení každého používateľa Tor. Umožňuje používateľovi vytvoriť anonymizačný okruh Tor a spracovať všetky kryptografické kľúče potrebné na komunikáciu so všetkými uzlami v okruhu.
* *Vstupný uzol* je prvý uzol v okruhu, ktorý prijíma požiadavku klienta a preposiela ho druhému uzlu v sieti.
* *Výstupný uzol* je posledné relé Tor v obvode.

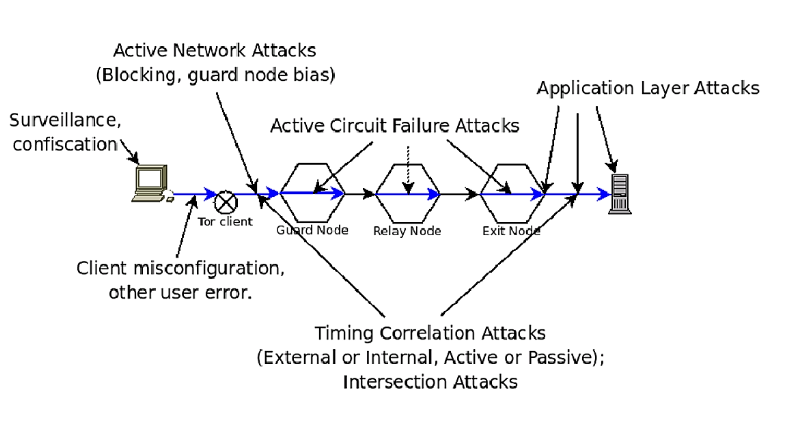
Akonáhle požiadavka na pripojenie opustí vstupný uzol, bude posielaná medzi všetkými uzly v obvode, kým nedosiahne výstupný uzol. Ten prijme žiadosť a odošle ju konečnému cieľu. Ako je znázornené na Obr. 2, spojenia v sieti Tor medzi vstupným a výstupným uzlom sú šifrované pomocou štandardu pokročilého šifrovania (AES). Spojenia medzi výstupným uzlom a konečným cieľom však nie sú šifrované Tor-om. To znamená, že ak relácia medzi klientom a cieľom nie je šifrovaná ako súčasť protokolu zabezpečenia vyššej vrstvy, ako je napríklad HTTPS, útočník s bydliskom v blízkosti cieľa bude môcť údaje zverejniť(Dobre, Xhafa 2016).



Obrázok 2 Sieť Tor[[2]](#footnote-3)

### Slabé stránky

Systém Tor nie je bez limitácii(Obrázok 3), jedným rozdielom medzi Tor a predchádzajúcimi pokusmi o anonymizáciu tokov prenosu je to, že netvrdí, že ponúka bezpečnosť dokonca ani voči pasívnym globálnym pozorovateľom. Tento problém je známy v projekte Tor, ktorý každému odporúča používať šifrovanie typu end-to-end. Táto limitácia vedie k tomu že útočník, ktorý môže pozorovať prúd komunikácie v dvoch rôznych bodoch, dokáže zistiť, že ide o rovnaký prenos. Toto je slabina, ktorú je možné zneužiť na narušenie anonymity systému Tor (Choudhary, 2018).



Obrázok 3 Slabiny Tor[[3]](#footnote-4)

### Útoky na Tor

Z hľadiska bezpečnosti Tor sieťe môžu byť útoky zamerané na tri rôzne subjekty

siete:

* *Klient*: v tomto prípade je cieľom útočníka zamerať sa na klienta Tor sieť;
* *Server*: v tomto prípade je útočník zameraný na skrytý server Tor;
* *Sieť*: v tomto prípade je útočníkom zameraná samotná sieť Tor.

Príkladom útoku na klienta môžu byť útoky založené na pluginoch. Tieto útoky sa vykonávajú s cieľom zacieliť na používateľa prostredníctvom internetového prehliadač, ktorý používa na navigáciu v sieti. Takéto hrozby využívajú externý softvér v prehliadaču (pluginy), ako sú Flash, Java a ovládacie prvky ActiveX. Tieto aplikácie fungujú ako samostatný softvér s používateľskými oprávneniami v operačnom systéme. Niektoré z týchto technológií, ako napríklad Java alebo Adobe Flash sa vykonávajú vo virtuálnych strojoch alebo frameworkoch obchádzajúcich nastavenia konfigurácie proxy nastavených prehliadačom Tor, teda priamo komunikujú v sieti internet bez použitia Toru. Útoky na prehľadávač môžu byť implementované nasledujúcimi spôsobmi prístupy :

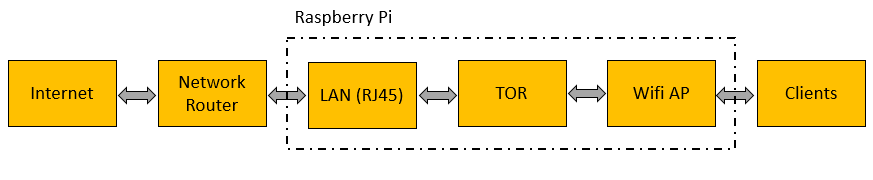
* pôsobením na verejnom internetovom serveri kontaktovanom klientom, prostredníctvom škodlivého serverového systému obsahujúceho napríklad Adobe Flash obsah na webovej stránke,
* prijatím zlého výstupného uzla a odpočúvaním komunikácie používateľov na nezašifrovaných kanáloch (napr. pripojenie HTTP) a vkladanie škodlivého obsahu súvisiaceho s doplnkami.

Z dôvodu možného prezradenia identity klientov kvôli použitiu doplnkov prehliadača, ako to prednastavujú anonymizačné prehliadače, sú pluginy, ktoré sú predvolené často deaktivované, aby sa zabránilo neanonymnej komunikácii v sieti Tor.

Ďalším príkladom útoku na sieť Tor je Sniper útok. Sniper využíva algoritmus riadenia toku Tor, tým, že vykoná DoS útok proti uzlu Tor, ničením procesu Tor na uzle. Toto sa dosiahne donútením uzla ukladať do vyrovnávacej pamäte veľké množstvo dát (využívajúci správy platného protokolu), kým nie je preťažený a prinútený byť offline. Útočník môže zaútočiť na obrovské množstvo uzlov a degradovať tak možnosti siete a zvýšiť šancu klienta vybrať si uzol útočníka (Cambiaso, 2019).

# 2 Ciele seminárnej práce

Cieľom tejto seminárnej práce je mať samostatnú bezdrôtovú sieť, do ktorej sa môžu všetky vaše zariadenia prihlásiť, a potom pomocou dostupného pripojenia LAN slúžiť sieťam pre vaše zariadenia z jedného bodu (Valley 2021). Nastavíme Raspberry Pi ako prístupový bod a potom filtrujeme všetku internetovú komunikáciu cez Tor. Vďaka použitiu transparentného proxy môžeme prehľadávať anonymne, iba za jednoduchého pripojenia zariadenia k sieti a o ostatné sa postará Pi.

[[4]](#footnote-5)

Obrázok 4 Sieťový tok

Sieťový tok na Obr.4 zreprodukujeme za použitia Raspberry Pi Zero W.

# 3 Riešenie seminárnej práce

## 3.1 Príprava WIFI hotspotu pre anonymné siete

* Napálenie Raspbian OS
* Inštalácia a konfigurácia „hostapd“
* Inštalácia a konfigurácia „udhcpd“,
* Konfigurácia sieťového rozhrania
* Inštalácia a konfigurácia „tor“
* Konfigurácia „iptables“
* Nastavenie IP forwarding
* Zakázanie niektorých predvolených deamonov

### 3.1.1. Napálenie Raspbian OS

Pre účely projektu je budeme pracovať s čerstvou inštaláciou operačného systému na SD kartu.

Ako prvý krok je potrebné si stiahnuť „Raspberry Pi Imager“, program, ktorý nahradil „NOOBS“ pri prvotnej inštalácii operačného systému Raspbian. „Imager“ ponúka možnosť formátovania SD karty, priameho stiahnutia a nahrania operačného systému na SD kartu, vybraného z dropdown ponuky. Pre naše účely sme „Raspberry Pi OS Lite“ (Raspberry.org, 2021), pretože obsahuje najmenej pred-inštalovaných súborov. Alternatívne je ho možné stiahnuť osobitne a potom Imageru dať presnú cestu kde sa súbor nachádza.

Následne sa spustí zápis. Ako vidíme na obrázku 5 prebieha zápis nového operačného systému.

Po ukončení inštalácie je možné vložiť SD kartu do zariadenia Raspberry Pi Zero W a spustiť prvotný boot.

Obrázok 5 Napálenie Rasbian OS

Na pokračovanie je potrebné mať možnosť pripojiť Raspberry Pi Zero W na monitor, klávesnicu a pripojiť k eternetovému sieťovému káblu. Prihlásime sa do zariadenia pomocou prednastavených prihlasovacích údajov ako užívateľ pi.

*log in: pi*

*password: raspberry*

V tomto momente je vhodné heslo zmeniť, cez raspi-config.

Následne si overíme, že máme prístup na internet cez eternetový sieťový kábel, updatneme a upgradneme zariadenie pomocou príkazov:

*$ sudo apt update && sudo apt upgrade*

### 3.1.2. Inštalácia a konfigurácia „hostapd“

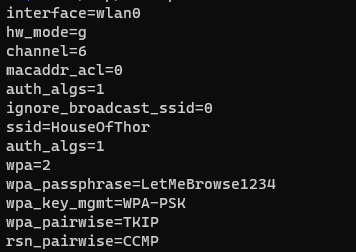
Ako prvý s linuxových deamonov, ktorý budeme potrebovať pri našom projekte je hostapd. Hostapd (Host access point daemon) je deamonom používateľského priestoru, ktorý je schopný premeniť bežné karty sieťového rozhrania na prístupový bod (AP) a autentifikačný server (Malinen 2009). Implementuje správu prístupových bodov podľa štandardu IEEE 802.11.

Program nainštalujeme jednoducho pomocou príkazu:

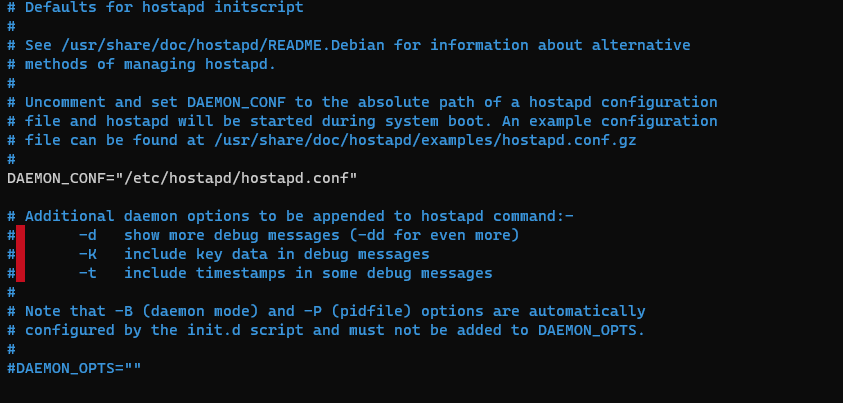
*$ sudo apt install hostapd*

Po inštalácii potrebujeme nastaviť ako sa má *hostapd* správať. Preto potrebujeme špecifikovať 2 konfiguračné subory a to *hostapd.conf* (Obrázok 6) a *hostapd* (Obrázok 7)*.*

Ako prvý potrebujeme vytvoriť súbor /etc/hostapd/hostapd.conf, konfiguračný súbor, ktorý bude špecifikovať ako Raspberry Pi Zero W bude implementovať IEEE 802.11 štandard a komunikovať s okolím. Kompletnú dokumentáciu k projektu nájdeme vo vývojárskej dokumentácii (Hostapd, 2021), ktorá vysvetľuje jednotlivé parametre a vstupné údaje, ktoré program prijíma. Pre naše potreby budeme používať iba časť dokumentácie týkajúcej sa konfigurácia súvisiaca s IEEE 802.11. V prílohe A je možné nájsť celý konfiguračný súbor s vysvetleniami pre jednotlivé riadky súboru vyobrazeného na obrázku 6.



Obrázok 6 Konfiguračný súbor etc/hostapd/hostapd.conf

Nasledujúcim krokom bola úprava súboru /default/hostapd, kde bolo nutné odkomentovať DEAMON\_CONF premennú a nastaviť absolútnu cestu k *hostapd.conf* súboru. Táto úprava zabezpečí automatický štart deamona pri boote / reboote a tým zabezpečí trvalý chod služby (obrázok 7). 

Obrázok 7 Konfiguračný súbor /etc/default/hostapd

Keďže hostapd nemá nakonfigurované predvolené nastavenia, vývojári daného balíčku sa rozhodli službu maskovať.

Preto pred ďalším použitím potrebujeme deamona odmaskovať, povoliť a reštartovať. Dané kroky je možné spraviť pomocou nasledujúcich príkazov:

*$ sudo systemctl unmask hostapd*

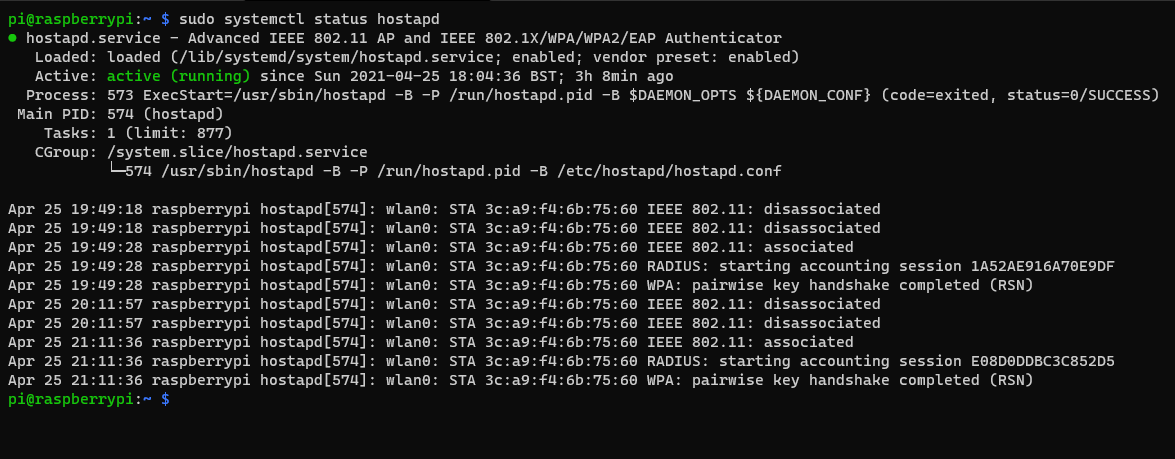
*$ sudo systemctl enable hostapd*

*$ sudo systemctl stop hostapd*

*$ sudo systemctl start hostapd*

Následne si overíme funkcionalitu pomocou:

*$ sudo systemctl status hostapd*



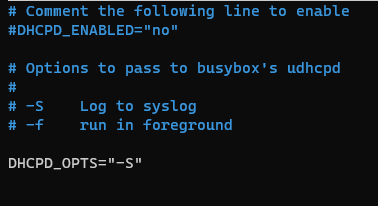
Obrázok 8 Overenie funkčnosti služby po reštarte

*hostapd* vytvára iba prístupový bod a nevie o protokole IP alebo o routingu, a preto potrebujeme nasledujúci balíček *udhcpd*, zaobstarávajúci práve tieto funkcie.

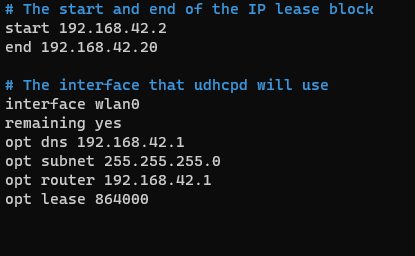
### 3.1.3. Inštalácia a konfigurácia „udhcpd“

Dynamic Host Configuration Protocol (DHCP) je protokol klient / server, ktorý automaticky poskytuje hosťovi IP adresu a ďalšie súvisiace informácie o konfigurácii, napríklad masku podsiete a predvolenú bránu a pod. (Singh 2017).

Udhcpc je veľmi malý klientsky program DHCP zameraný na zabudované systémy. Písmená sú skratkou pre Micro - DHCP - Client (μDHCPc). Program sa snaží byť plne funkčný a kompatibilný s RFC 2131 (Emanuele Aina a Anderson 2017), (Droms 1997).

Pre naše účely potrebujeme upraviť 2 súbory. Súbor */etc/udhcpd.conf* obsahujúci informácie o konfigurácii špecifické pre server *udhcp*. Formát konfiguračného súboru je kľúčové slovo konfigurácie na riadok, za ktorým by mali nasledovať príslušné informácie o konfigurácii (Canonical 2019). Celý konfiguračný súbor nájdeme aj s popisom na https://udhcp.busybox.net/udhcpd.conf .

Obrázok 9 Konfiguračný súbor /etc/default/udhcpd

Začiatočná a koncová IP adresa možná na prenájom zariadeniam v našom príklade bola stanovená na 18 zariadení, kvôli stabilite zariadenia. V prílohe A nájdeme podrobnejšie vysvetlenia k obrázku 9, ktoré objasňujú jednotlivé časti konfiguračného súboru. Avšak keďže sa jedná internú sieť, akýkoľvek blok privátnych adries môže byť špecifikovaný v tomto momente.Ďalším súborom, ktorý treba upraviť na je */default/udhcpd,* v ktorom je potrebné povoliť službu pri spustení odkomentovaním riadka DHCPD\_ENABLE=”no” (Obrázok 10). Bez týchto úprav sa deamon nespustí. Tento krok je v princípe rovnaký ako omaskovanie *hostapd* a zabezpečuje tiež trvalý prístup k službe a to, že bude bežať na pozadí.

Obrázok 10 Konfiguračný súbor /etc/udhcpd.conf

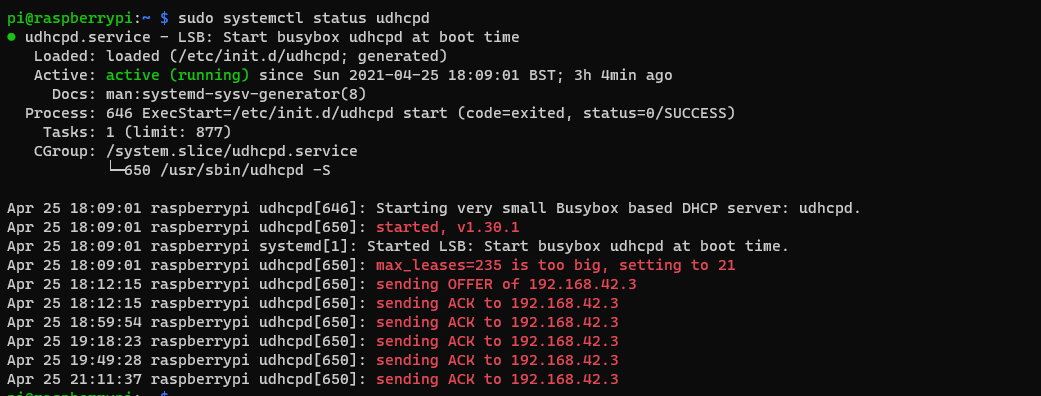
Podobne ako *hostapd* aj *udhcpd* je potrebné povoliť a následne reštartovať aby sa aplikovali zmeny.

*$ sudo systemctl stop udhcpd*

*$ sudo systemctl start udhcpd*

Následne si overíme funkcionalitu pomocou:

*$ sudo systemctl status udhcpd*



Obrázok 11 Overenie funkčnosti udhcpd

### 3.1.4. Konfigurácia sieťového rozhrania

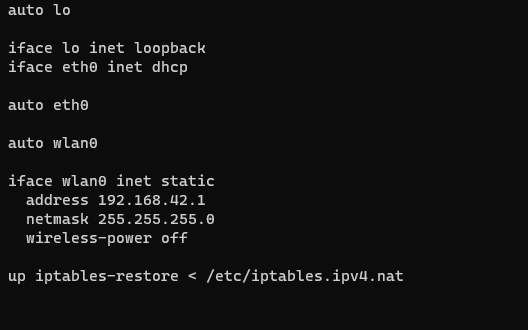
Neodkladnou súčasťou pri budovaní wifi hotspotu je definícia ako bude vyzerať konfigurácia sieťového rozhrania. V našom prípade nastavíme statické konfiguračné údaje manuálne pre bezdrôtové rozhranie (Wiki.debian 2021).

Ako môžeme vidieť na obrázku 12, wlan0 rozhranie obsahuje 3 dôležité údaje. Prvou je adresa predvolená brána, ktorý je nastavená na 192.168.42.1. Druhou je sieťová maska, rozdelí adresu IP na podsiete a určí dostupných hostiteľov siete. Treťou infomáciou je príkaz *wireless-power off,* ktorý zabezpečí, Raspberry sa nebude snažiť o automatickú správu napájania (Osbourn 2016)[.](https://tosbourn.com/stop-wireless-turning-off-raspberry-pi/)

Daľšie rozhrania, ktoré potrebujeme definovať je loopback a eth0. *Loopback (lo)* je špeciálne virtuálne sieťové rozhranie, ktoré počítač používa na komunikáciu sám so sebou (Juniper 2020).

Pomocou DHCP sa automaticky konfiguruje rozhranie eth0, ktoré bude komunikovať s vonkajším svetom (Wiki.debian 2021).

Ako poslednú vec potrebujeme nastaviť každé rozhranie na „auto“, pretože chceme ich mať dostupné pri štarte.



Obrázok 12 Konfiguračný súbor /etc/network/interfaces

Na záver konfiguračného súboru treba pridať príkaz, ktorý zabezpečí, že pri každom reštarte siete, iptables nastavenia sa nanovo načítajú zo súboru *iptables.ipv4.nat,* kde je definované ich správanie.

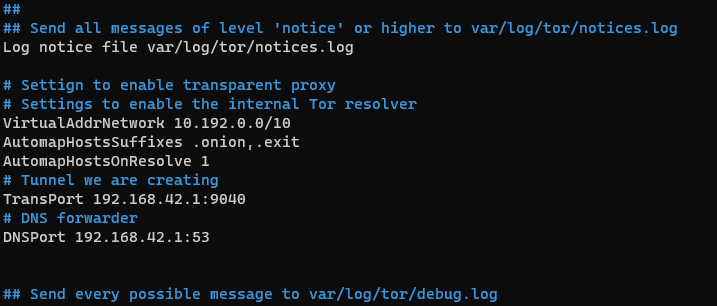
### 3.1.5. Inštalácia a konfigurácia „tor“

V tomto momente máme zariadenie pripravené na inštaláciu samostatného Toru.

*$ sudo apt install tor*

Inštalácia Toru na naše zariadenie spôsobí 2 veci. Jedna je nainštalovanie novej služby/deamona, ktorý bude obstarávať Tor, a druhá, že Tor vytvoril samostatného používateľa na našom zariadení s názvom „debian-tor“.

Prvým krokom po inštalácii je upraviť konfiguračný súbor *etc/tor/torrc*. Na obrázku 13 vidíme podrobnejší popis úprav. Pre naše potreby sme upravili iba 2 veci. Odkomentovali riadok hovoriaci, kde sa budu logovať upozornenia a pridali sme nastavenia pre transparentné proxy, vytvárajúce virtuálne prostredie pre našu sieť. Ako nastavenia hovoria, automatický každé zariadenie po pripojení bude súčasťou tejto virtuálnej siete a automaticky sa budú pripájať prípony .onion alebo .exit zabezpečujúce, že nikto „neunikne“ z Tor siete. Pre vytvorenie vlastného tunela a DNS resolvera použijeme statickú IP nášho default gateway so špecifikovanými portami cez ktoré sa bude komunikovať (FreedomBox/Configs/Tor - Debian Wiki, 2021).



Obrázok 13 Konfiguračný súbor /etc/tor/torrc

Po úprave *torrc* potrebujeme spaviť ešte pár úprav a to vytvoriť samostatný logovací súbor, ktorý sa v tomto momente nenachádza na našom zariadení, zmeniť vlastníctvo a prístup k tomuto súboru a pričleniť ho požívateľovi debian-tor pomocou:

*$ touch /var/log/tor/notices.log*

*$ chown debian-tor /var/log/tor/notices.log*

*$ chmod 640 /var/log/tor/notices.log*

Poslednou skutočnosťou je povolenie automatického reštartu Tor služby pri zlyhaní.

*$ sudo update-rc.d tor enable*

### 3.1.6. Konfigurácia „iptables“

Jedným z posledných krokov pri finalizácii nášho projektu je nastavenie iptables, kde sa budú definovať pravidlá sieťovej prevádzky (povolené/zakázané správanie). Je viacero spôsobov ako sa tieto pravidlá dajú nastaviť, ale keďže sme si predtým definovali v */etc/network/interfaces,* že pri každom reštarte sa načítajú iptables pravidlá zo súboru *iptables.ipv4.nat,* stačí ak vytvoríme tento súbor, zreštartujeme sieť a pravidlá budú aplikované.

Ako je vidno na obrázku 14 prijímame všetku sietovú aktivitu. Kedže sa jedná o vnútornú privátnu sieť, nepotrebujeme filtrovať aké porty komunikujú vnútri.

Dôležité sú pravidlá, ktoré nám definujú ako bude komunikovať bezdrôtové rozhranie. Nastavili sme 2 pravidlá a to, že iba zariadenia, ktoré sú už pripojené na našej sieti majú možnosti SSH do Raspberry (nevyhnutnosť riešenia problémov bez možnosti pripojiť sa na externý monitor) a pravidlo komunikácie s vonkajším svetom. Je povolená iba TCP komunikácia, keďže Tor nie je postavený na zvládnutie UDP komunikácie. Problém s DNS požiadavkami sme vyriešili v predošlých nastaveniach a preto máme istotu, že nedôjde k DNS úniku.



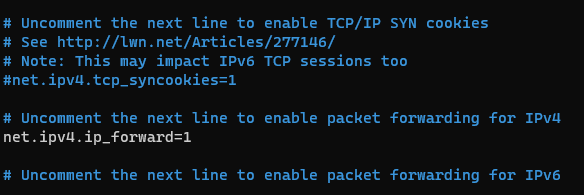
Obrázok 14 Konfiguračný súbor /etc/iptables.ipv4

### 3.1.7. Nastavenie IP forwarding

Posledný konfiguračný súbor, ktorému potrebujeme venovať pozornosť je */etc/sysctl.conf*  (Kerrisk 2020). Jedná jednoduchý súbor obsahujúci hodnoty sysctl, ktorý má byť načítaný a nastavený sysctl. Pre naše potreby potrebujeme otvoriť súbor:

*$ sudo nano /etc/systcl.conf*

A odkomentovať riadok *net.ipv4.ip\_forward=1 .* V tomto momente sme umožnili tok dát medzi našou internou sieťou a internetom.



Obrázok 15 Konfiguračný súbor /etc/sysctl.conf

### 3.1.8. Zakázanie niektorých predvolených deamonov

Finálnym krokom je zakázanie prednastavených deamonov, ktoré sa snažia o pomoc DHCP pre Rasbperry a Avahi - démon mDNS / DNS-SD implementujúci architektúru Zeroconf spoločnosti Apple (avahi-daemon(8): Avahi mDNS/DNS-SD daemon - Linux man page, 2021).

*$ sudo systemctl disable dhcpcd*

*$ sudo systemctl disable avahi-daemon*

### 3.1.9. Reštart zariadenia a kontrola

V tomto momente máme všetky nastavenia v poriadku a zariadenie by malo fungovať. Pre kontrolu správnosti a aplikáciu spravených nastavení zariadenie zreštarujeme:

*$ sudo shutdown -r now*

Po reboote skontrolujmeme, či iptables sa načítali:

*$ sudo iptable -n -L -t nat*

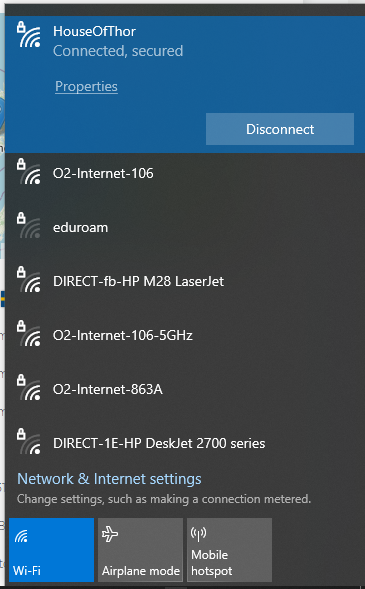
Ďaľším testom cez príkazový riadok:

*$ dig A www.google.com @192.168.42.1*

Ak príkaz fungoval znamená to, že rozlíšenie DNS pracuje zodpovedajúcim spôsobom prostredníctvom siete Tor so zadaním zo súboru *torrc* Trans DNS.

## 3.2 Testovanie

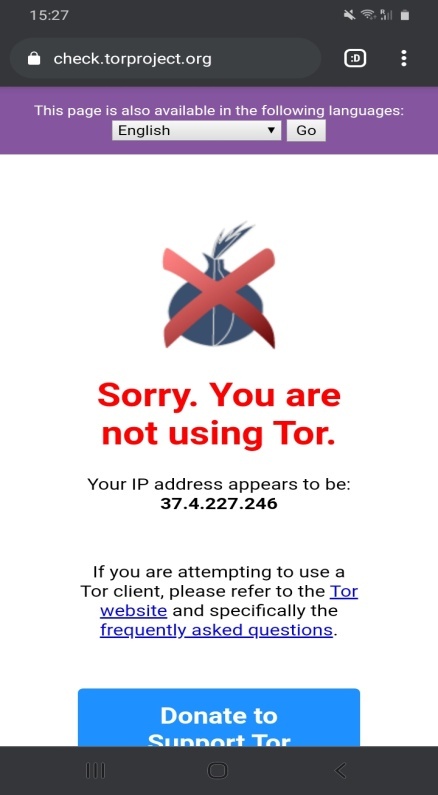
Na našom zariadení si skontrolujeme dostupné wifi siete a nájdeme našu Raspberry Pi sieť. Pripojíme sa na túto sieť pomocou hesla, ktorého sme si zadávali v konfiguračnom súbore. Následne sme vykonali viacero testov aby sme skontrolovali správnu funkčnosť nášho pripojenia a taktiež, aby sme overili či je toto pripojenie skutočne bezpečné.



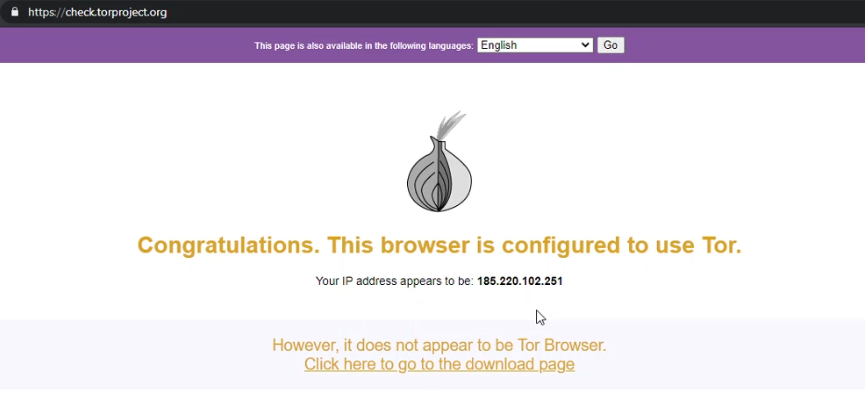
Obrázok 16 Ukážka pripojenia

### Check.torproject.org

Prvým testom bol test na check.torproject.org. Na prvom obrázku vidíme ako je stránka zobrazená na našom normálnom pripojení a na druhom zobrazenie po pripojení na našu Tor sieť. Ako môžeme vidieť tak naša IP adresa sa zmenila a test nám potvrdzuje, že využívame pripojenie cez Tor sieť.



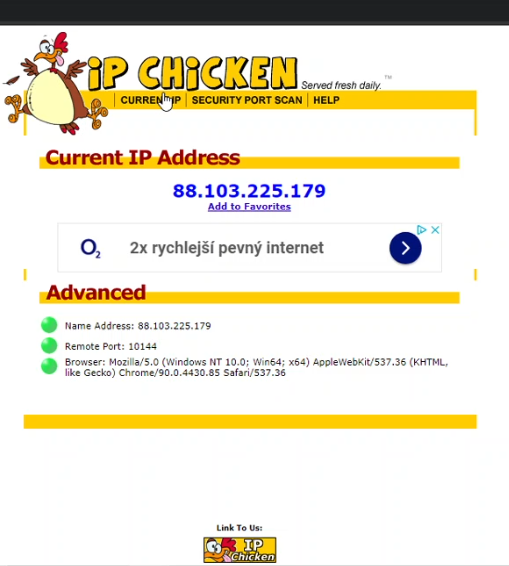
Obrázok 17 Torproject test pred pripojením do Tor siete



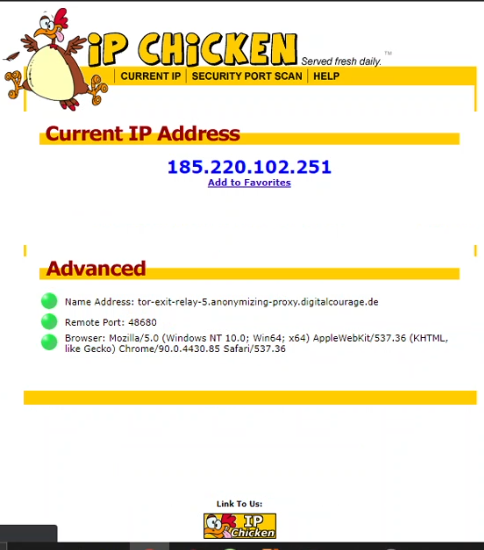
Obrázok 18 Torproject test po pripojením do Tor siete

### IP chicken

Ďalší vykonaný test bol pomocou stránky [www.ipchicken.com](http://www.ipchicken.com/), ktorá nám zobrazí IP adresu tak ako ju vidí server a zobrazí taktiež meno domény. Môžeme vidieť, že IP adresa nie je totožná s IP od nášho internetového providera. Taktiež si môžeme všimnúť, že keď stránku načítame znova tak sa tieto údaje zmenia (Adafruit 2013).



Obrázok 19 IP chicken test pred pripojením do Tor siete

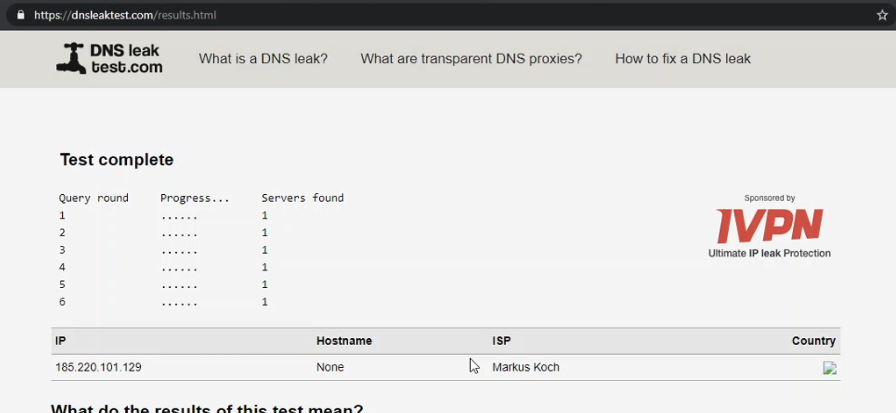


Obrázok 20 IP chicken test po pripojením do Tor siete

### **DNS test priepustnosti**

Pri používaní anonymizačnej služby je mimoriadne dôležité, aby bola všetka komunikácia pochádzajúca z vášho počítača smerovaná cez anonymnú sieť. Ak dôjde k úniku akejkoľvek prenosovej aktivity mimo zabezpečeného pripojenia k sieti, každý útočník monitorujúci vašu prenosovú kapacitu bude môcť zaznamenať vašu aktivitu. Za určitých podmienok bude operačný systém, aj keď je pripojený k anonymnej sieti, naďalej používať svoje predvolené servery DNS namiesto anonymných serverov DNS priradených k vášmu počítaču anonymnou sieťou. Úniky DNS sú hlavnou hrozbou ochrany osobných údajov, pretože anonymná sieť môže poskytovať falošný pocit bezpečia, zatiaľ čo unikajú súkromné údaje.

Z tohto dôvodu sme teda vykonali tento test pomocou stránky [https://www.dnsleaktest.com](https://www.dnsleaktest.com/) **,** vďaka ktorému sme zistili, že nenastal žiaden únik (Campbell 2021).

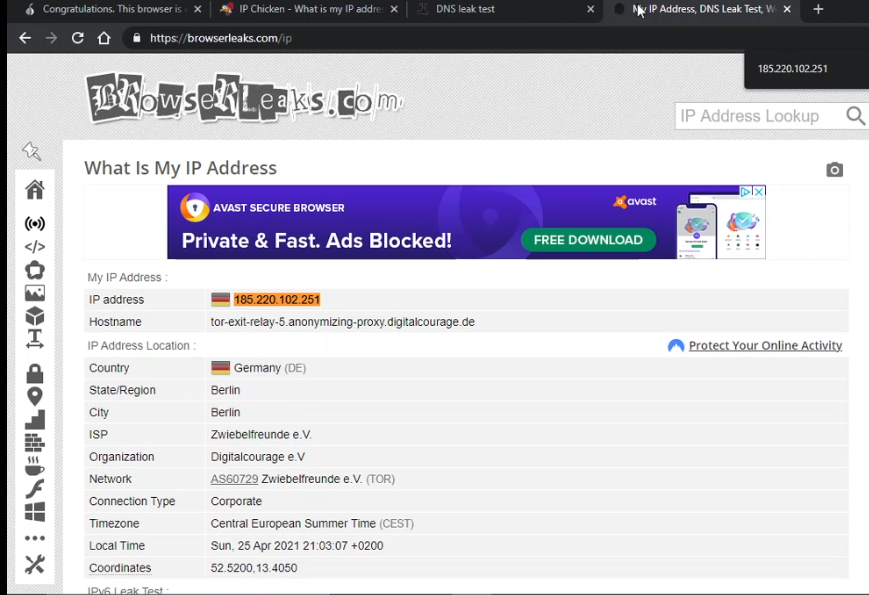


Obrázok 21 DNS test priepustnosti

### Browserleaks.com

Ďalší test bol vykonaný pomocou stránky browserleaks.com. Dlho sa verilo, že IP adresy a cookies sú jedinými spoľahlivými digitálnymi odtlačkami prstov, ktoré sa používajú na online sledovanie ľudí. V súčasnosti už existuje veľké množstvo moderných webových technológii, ktoré umožnili zainteresovaným organizáciám používať nové spôsoby identifikácie a sledovania používateľov bez ich vedomia a bez možnosti vyhnúť sa im.

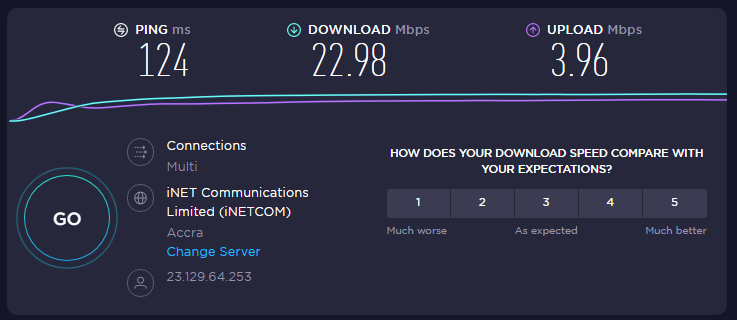
Na tejto stránke je veľké množstvo testov ktoré nám môžu odhaliť tieto potencionálne slabiny našej siete. Konkrétne sme tu vyskúšali IP test. Tento test ilustruje schopnosti servera odhaliť identitu používateľa. Má základné funkcie, ako napríklad zobrazovanie vašej adresy IP a hlavičiek HTTP, geolokácia na základe adresy IP (GeoIP) , určuje vašu krajinu, štát, mesto a tak ďalej.



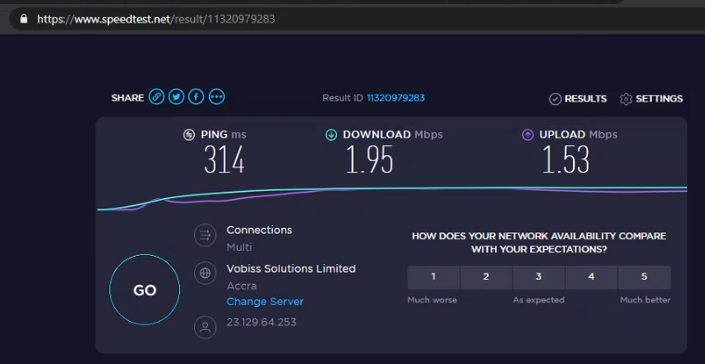
Obrázok 22 Browserleaks test

### **Speedtest**

Na určenie rýchlosti našej siete sme vykonali viacero Speedtestov. Výsledky sa líšili v závislosti od vzdialenosti, ktorou boli packety posielané. Vo všeobecnosti môžeme vidieť masívne spomalenie rýchlosti našej siete.



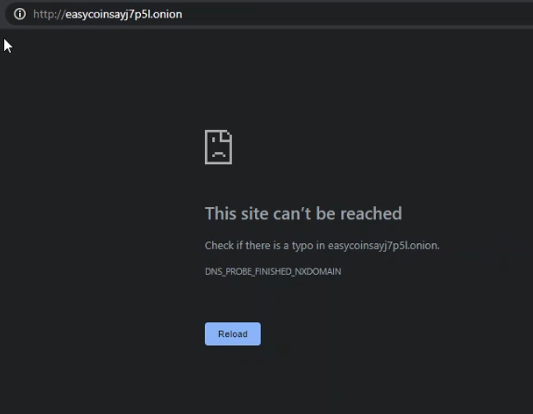
Obrázok 23 Speedtest pred pripojením do Tor siete



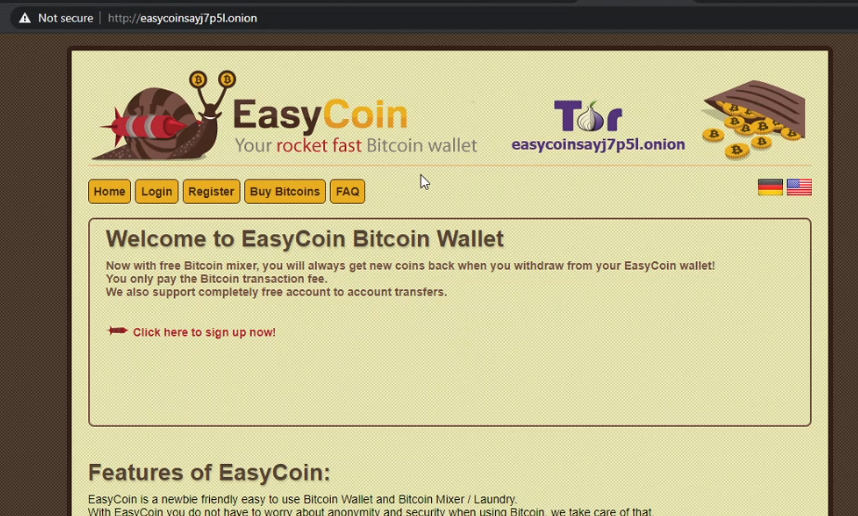
Obrázok 24 Speedtest po pripojení do Tor siete

### **Prístup do hidden services**

Tor hidden services je špeciálny typ webových stránok, ktoré je možné navštíviť iba pomocou služby Tor, ktorý sa snaží čo najviac zabezpečiť našu digitálnu stopu. My konkrétne skúšame prístup na Easycoin Bitcoin Wallet. Môžeme vidieť, že keď nie sme pripojený cez Tor tak sa nám stránka nezobrazí, po pripojení na Tor sieť už funguje normálne.



Obrázok 25 Hidden services test pred pripojením do Tor siete



Obrázok 26 Hidden services test po pripojenía do Tor siete

### **Youtube**

Posledný vykonaný test bol kontrola rýchlosti prehrávania full HD videí na stránke youtube. Tento test je ukázaný na video dokumentácií, ktorú poskytujeme spolu s ostatnými materiálmi. Môžeme avšak povedať, že kvôli obmedzeniu rýchlosti prehrávanie videí vo vysokom rozlíšení alebo sťahovanie väčších súborov je značne spomalené.

# 4 Výsledky riešenia a ich zhodnotenie

Výsledkom našej práce je Tor router, vytvorený pomocou jednodoskového počítača Raspberry Pi Zero W, ktorý nám vytvára zabezpečenú možnosť využívania internetu. Používateľ sa jednoducho môže pripojiť na náš router pomocou Wifi. Taktiež odporúčame využívať VPN spolu s našim routerom, aby sme sa vyhli potencionálnym útokom na naše súkromie. Aj keď existuje viacero nevýhod, ktoré bližšie opíšeme v tejto kapitole tak sme preukázali, že sieť Tor nás naozaj ochraňuje pred nechceným pozorovaním.

## 4.1 Dopad na rýchlosť

Aby sme určili dopad na rýchlosť tak sme vykonali viacero testov – so zapnutým a vypnutým pripojením cez Tor sieť. Zistili sme, že všeobecne bola rýchlosť sťahovania ovplyvnená viacej ako rýchlosť nahrávania dát. Vo všeobecnosti bola naša rýchlosť sťahovania približne 23 Mbps, rýchlosť nahrávania približne 4Mbps a náš ping bol 124 ms. Po pripojení na Tor sieť naša rýchlosť sťahovania spadla na 1.95 Mbps, naša rýchlosť nahrávania bola 1.53 Mbps a nás ping stúpol na 314 ms.

Táto zmena rýchlosti bola očakávaná z dôvodu viacerých šifrovaní a dešifrovaní a taktiež kvôli tomu ako je packet smerovaný. Taktiež, celková rýchlosť pripojenia je obmedzená najpomalším uzlom v reťazci. Tento problém môže byť riešený iba zvýšením priepustnosti pre všetky servery Tor. Ako si môžeme všimnúť tak efektivita našej siete je zredukovaná na úkor bezpečnosti.

## 4.2 DNS test priepustnosti

Následne sme vykonali DNS test priepustnosti aby sme overili či náš Tor router spracoval DNS dotazy správne. Tento test je nevyhnutný aby sme mohli zabezpečiť používateľské údaje o prehľadávaní. Ak pôvodca nepoužíva služby DNS siete Tor na dokončenie požiadaviek DNS, dôjde k úniku. Úniky DNS umožňujú externej strane sledovať webové stránky, ktoré používateľ navštívil. Keď používateľ zadá požiadavku DNS na vyhľadanie IP adresy webovej stránky, ktorú chce navštíviť, tak zvyčajne použije svoj miestny server DNS, ktorý potom môže kontaktovať koreňový server DNS, za ktorým nasleduje server domény najvyššej úrovne a za ním autoritatívny server. Každé z pripojení k týmto serverom je možné odpočúvať, za účelom získať viac informácií o zvykoch používateľa online. Používaním bežných serverov DNS na dotazy na webové stránky používateľ nevyužíva šifrovania siete Tor, za účelom zistenia IP adresy webovej stránky, ktorú chce navštíviť. Aj keď týmto spôsobom nie je vidno, ktoré konkrétne časti webovej stránky používateľ navštívil, ukazuje to, kde bol alebo tam, kam chce ísť (Barberis et al. 2018). Takéto informácie možno použiť na profilovanie používateľa. Test úniku DNS ukázal, že náš router neprepúšťal požiadavky DNS. Namiesto toho boli využite DNS služby našej Tor siete za účelom dokončenia DNS požiadaviek.

## 4.3 Limitácie Siete

Tor je užitočný nástroj pri udržiavaní anonymity, avšak má niektoré nevýhody.

Prvá nevýhoda je dopad na rýchlosť prehľadávania, ktorú sme si už spomenuli v predchádzajúcich kapitolách. Využívanie preto Tor siete na sledovanie videí vo vysokom rozlíšení alebo sťahovanie väčších súborov nie je najlepší nápad.

Ďalšou nevýhodou je, že neposkytuje end-to-end šifrovanie. Tor šifruje vaše údaje, keď vstúpia do Tor siete, nie však pred tým ani potom. To znamená, že niekto, kto vás špehuje, môže vidieť všetko, čo je v obyčajnom textovom formáte, napríklad vaše používateľské meno a heslo k rôznym stránkam. Po tretie, pripájanie aplikácií k Tor sieti býva väčšinou komplikované.

Jednoduchým spôsobom, ako tieto obmedzenia prekonať, je použitie VPN spolu s Tor. Sieť VPN poskytuje šifrovanie typu end-to-end a podporuje aplikácie, takže predstavuje dobrú opravu uvedených problémov, okrem nízkej rýchlosti prehliadania.

Dôvodom prečo nepoužívať iba VPN je, že vás neurobí anonymným v pravom zmysle slova, pretože poskytovateľ VPN vás môže technicky sledovať

Ak chcete úplnú anonymitu, Tor je vaše najlepšie riešenie. A ak chcete prekonať jeho inherentné obmedzenia, jeho kombinácia s VPN je najlepším riešením (Wardini 2016).

# Záver

V tejto seminárnej práci sme sa zaoberali vytvorením Tor routeru prostredníctvom jednodoskového počítača Raspberry Pi Zero W. Práca sa zaoberá analýzou siete Tor, návrhom a vytvorením Tor routera, ktorý nám umožní prístup k internetu za účelom zabezpečeného prezerania internetu.

V kapitole analýza súčasného stavu sme si bližšie priblížili princíp anonymizácie, opísali sme si riešenia, ktoré sú momentálne dostupné a bližšie sme opísali sieť Tor. Opísali sme si históriu tejto siete, jej fungovanie a slabé stránky. Ďalej sme sa zaoberali potencionálnymi útokmi, ktoré môžu ohroziť túto sieť.

V práci sme sa po stanovení jednotlivých podcieľov pre dosiahnutie hlavného cieľa venovali návrhu nášho riešenia. Jadrom našej práce bolo vytvorenie zabezpečeného wifi hotspotu pomocou Raspberry Pi Zero W. Priblížili sme si vytvorenie tohto hotspotu a následne sme testovali či je naše pripojenie na internet pomocou tohto hotspotu naozaj zabezpečené.

Na záver sme prezentovali naše výsledky a opísali sme slabiny a nedostatky tejto siete. Najväčšou nevýhodou takéhoto pripojenia je obmedzenie rýchlosti spôsobené tým, ako packet cestuje po sieti. Ostatné inherentné nedostatky takéhoto pripojenia môžeme vyriešiť využitím VPN spolu so sieťou Tor, poprípade inými dodatkovými službami na zvýšenie ochrany a pokrytie slabín Toru. Vďaka testovaniu sme zistili, že takéto pripojenie je naozaj bezpečné a používateľské dáta sú zabezpečené.

# Zoznam bibliografických odkazov

ADAFRUIT, 2013. *Adafruit* [online]. Dostupné na: https://learn.adafruit.com/ONION-PI/

BARBERIS, Adrian, Danny RADOSEVICH, Wyatt EMERY a Mike BOROWCZAK, 2018. Portable tor router: Easily enabling web privacy for consumers. *2018 IEEE International Conference on Consumer Electronics, ICCE 2018* [online]. 2018, roč. 2018-Janua, s. 1–6. Dostupné na: doi:10.1109/ICCE.2018.8326333

CAMPBELL, Jeremy, 2021. DNS leak test [online]. 2021. Dostupné na: https://www.dnsleaktest.com/what-is-a-dns-leak.html

CANONICAL, 2019. *Ubuntu Manpage Repository* [online]. Dostupné na: http://manpages.ubuntu.com/manpages/bionic/man5/udhcpd.conf.5.html

CAMBIASO E. a i. 2019. *Darknet Security: A Categorization of Attacks to the Tor Network.* [online]. 2021. [cit. 2021-02-20]. Dostupné na internete: http://ceur-ws.org/Vol-2315/paper10.pdf.

CHOUDHARY D.. 2018. *The Onion Routing-The Good and The Bad.* [online]. 2021. [cit. 2021-02-20]. Dostupné na internete: https://www.researchgate.net/publication/327867486\_The\_Onion\_Routing-The\_Good\_and\_The\_Bad.

CHOUDHARY, D. BHAGAT R. 2018. *The Onion routing.* [online]. 2021. [cit. 2021-02-20]. Dostupné na internete: https://www.researchgate.net/publication/328388655\_The\_Onion\_Routing.

DROMS, R., 1997. *Dynamic Host Configuration Protocol* [online]. Dostupné na: https://www.ietf.org/rfc/rfc2131

DOBRE, C. XHAFA F. 2016. Chapter 1 – On preserving privacy in computing using ToR**.**   
In : *Pervasive Computing. Academic Press 2016.* Elsevier Science Publishing Co Inc, 2008. 548 s. ISBN 978-0-12-803663-1.

EMANUELE AINA, Erik Andersen a Laurence ANDERSON, 2017. *Busybox* [online]. Dostupné na: https://manpages.debian.org/stretch/udhcpd/udhcpd.8

HOSTAPD, 2021. *hostapd* [online]. Dostupné na: https://w1.fi/cgit/hostap/plain/hostapd/hostapd.conf

JUNIPER, 2020. *Understanding the Loopback Interface* [online]. Dostupné na: https://www.juniper.net/documentation/en\_US/junos/topics/concept/interface-security-loopback-understanding.html

KERRISK, Michael, 2020. *Linux manual page* [online]. Dostupné na: https://man7.org/linux/man-pages/man5/sysctl.conf.5.html

KIRCH, Olaf , 1993. *Linux Network Administrators Guide.* [online]. 2021. Dostupné na: https://tldp.org/LDP/nag2/f3.html

KLIMEŠ C. SOCHOR, T. 2018. *Overview of Web Anonymization.* [online]. 2021. [cit. 2021-02-21]. Dostupné na internete: https://www.researchgate.net/publication/322981530\_Overview\_of\_Web\_Anonymization

LINUX.DIE.NET, 2021. *avahi-daemon(8): Avahi mDNS/DNS-SD daemon - Linux man page.* [online] Available at: https://linux.die.net/man/8/avahi-daemon

MALINEN, Jouni, 2009. *hostapd* [online]. Dostupné na: http://w1.fi/hostapd/devel/index.html

OSBOURN, Toby, 2016. *Stopping your wireless from turning off on your Raspberry Pi* [online]. Dostupné na: https://tosbourn.com/stop-wireless-turning-off-raspberry-pi/

RASPBERRYPI.ORG. 2021. *Operating system images.* [online] Dostupné na: https://www.raspberrypi.org/software/operating-systems/

SINGH, Pradeep, 2017. *Configure Tiny Core Linux as DHCP Server using udhcpd* [online]. Dostupné na: https://iotbytes.wordpress.com/configure-dhcp-server-on-microcore-tiny-linux/

TOR. 2021. *History.* [online]. 2021. Dostupné na internete: https://www.torproject.org/about/history/.

VALLEY, Raspberry, 2021. *Raspberry Pi Tor Access Point* [online]. Dostupné na: http://raspberry-valley.azurewebsites.net/Raspberry-Pi-Tor-Access-Point/#raspberry-pi-tor-access-point

WARDINI, Josh, 2016. cloudtweaks [online]. 2016. Dostupné na: https://cloudtweaks.com/2020/01/tor-its-privacy-limitations/

WIKI.DEBIAN., 2021. *FreedomBox/Configs/Tor - Debian Wiki.* [online] Dostupné na: https://wiki.debian.org/FreedomBox/Configs/Tor.

WIKI.DEBIAN, 2021. *wiki.debian.org* [online]. Dostupné na: https://wiki.debian.org/NetworkConfiguration

# Zoznam príloh

Príloha A – Konfiguračné súbory

Príloha A

Konfiguračný súbor hostapd.conf

# the interface used by the access point

interface=wlan0

# "g" stands for 2.4ghz band

hw\_mode=g

# the channel to use

channel=6

# station mac address -based authentication

# please note that this kind of access control requires a driver that uses

# hostapd to take care of management frame processing and as such, this can be

# used with driver=hostap or driver=nl80211, but not with driver=atheros.

# 0 = accept unless in deny list

# 1 = deny unless in accept list

# 2 = use external radius server (accept/deny lists are searched first)

macaddr\_acl=0

auth\_algs=1

# send empty ssid in beacons and ignore probe request frames that do not

# specify full ssid, i.e., require stations to know ssid.

# default: disabled (0)

ignore\_broadcast\_ssid=0

# the name of the access point

ssid=houseofthor

# 1=wpa, 2=wep, 3=both

auth\_algs=1

wpa=2

wpa\_passphrase=letmebrowse1234

wpa\_key\_mgmt=wpa-psk

wpa\_pairwise=tkip

rsn\_pairwise=ccmp

Konfiguračný súbor default/hostapd

# Defaults for hostapd initscript

#

# See /usr/share/doc/hostapd/README.Debian for information about alternative

# methods of managing hostapd.

#

# Uncomment and set DAEMON\_CONF to the absolute path of a hostapd configuration

# file and hostapd will be started during system boot. An example configuration

# file can be found at /usr/share/doc/hostapd/examples/hostapd.conf.gz

#

DAEMON\_CONF="/etc/hostapd/hostapd.conf"

# Additional daemon options to be appended to hostapd command:-

# -d show more debug messages (-dd for even more)

# -K include key data in debug messages

# -t include timestamps in some debug messages

#

# Note that -B (daemon mode) and -P (pidfile) options are automatically

# configured by the init.d script and must not be added to DAEMON\_OPTS.

#

#DAEMON\_OPTS=""

Konfiguračný súbor udhcpd.conf

# The start and end of the IP lease block

start 192.168.42.2

end 192.168.42.20

# The interface that udhcpd will use

interface wlan0

# If remaining is true (default), udhcpd will store the time

# remaining for each lease in the udhcpd leases file. This is

# for embedded systems that cannot keep time between reboots.

# If you set remaining to no, the absolute time that the lease

# expires at will be stored in the dhcpd.leases file.

remaining yes

# The remainer of options are DHCP options and can be specifed with the

# keyword 'opt' or 'option'. If an option can take multiple items, such

# as the dns option, they can be listed on the same line, or multiple

# lines. The only option with a default is 'lease'.

opt dns 192.168.42.1

opt subnet 255.255.255.0

opt router 192.168.42.1

opt lease 864000 # 10 days of seconds

Konfiguračný súbor default/udhcpd

# Comment the following line to enable

#DHCPD\_ENABLED="no"

# Options to pass to busybox's udhcpd

#

# -S Log to syslog

# -f run in foreground

DHCPD\_OPTS="-S"

Konfiguračný súbor network/interfaces

# interfaces(5) file used by ifup(8) and ifdown(8)

# Please note that this file is written to be used with dhcpcd

# For static IP, consult /etc/dhcpcd.cong and 'man dhcpcd.conf'

auto lo

iface lo inet loopback

iface eth0 inet dhcp

auto eth0

auto wlan0

# Adding static adress to wlan0 which will be default gateway as well as DNS

# for our hotspot

# 'wireless-power off' will make sure that Raspberry does noy try for own power management

# it will stop wireless from turing off the Raspberry Pi

iface wlan0 inet static

address 192.168.42.1

netmask 255.255.255.0

wireless-power off

# Apply iptables rules, internet sharing (NAT)

up iptables-restore < /etc/iptables.ipv4.nat

Konfiguračný súbor torrc

Log notice file /var/log/tor/notices.log

# Settings to enable transparent proxy

# Settings to enable the internal Tor resolver

VirtualAddrNetwork 10.192.0.0/10

AutomapHostsSuffixes .onion,.exit

AutomapHostsOnResolve 1

TransPort 192.168.42.1:9040

DNSPort 192.168.42.1:53

Konfiguračný súbor iptables.ipv4.nat

\*nat

:PREROUTING ACCEPT [0:0]

:POSTROUTING ACCEPT [0:0]

:INPUT ACCEPT [0:0]

:OUTPUT ACCEPT [0:0]

-A PREROUTING -i wlan0 -p tcp -m tcp -d 192.168.42.1 --dport 22 -j ACCEPT

-A PREROUTING -i wlan0 -p tcp -m tcp --tcp-flags FIN,SYN,RST,ACK SYN -j REDIRECT --to-ports 9040

COMMIT

Konfiguračný súbor sysctl.conf

# /etc/sysctl.conf - Configuration file for setting system variables

# See /etc/sysctl.d/ for additional system variables.

# See sysctl.conf (5) for information.

#

#kernel.domainname = example.com

# Uncomment the following to stop low-level messages on console

kernel.printk = 3 4 1 3

##############################################################3

# Functions previously found in netbase

#

# Uncomment the next two lines to enable Spoof protection (reverse-path filter)

# Turn on Source Address Verification in all interfaces to

# prevent some spoofing attacks

#net.ipv4.conf.default.rp\_filter=1

#net.ipv4.conf.all.rp\_filter=1

# Uncomment the next line to enable TCP/IP SYN cookies

# See http://lwn.net/Articles/277146/

# Note: This may impact IPv6 TCP sessions too

#net.ipv4.tcp\_syncookies=1

# Uncomment the next line to enable packet forwarding for IPv4

net.ipv4.ip\_forward=1

# Uncomment the next line to enable packet forwarding for IPv6

# Enabling this option disables Stateless Address Autoconfiguration

# based on Router Advertisements for this host

#net.ipv6.conf.all.forwarding=1

###################################################################

# Additional settings - these settings can improve the network

# security of the host and prevent against some network attacks

# including spoofing attacks and man in the middle attacks through

# redirection. Some network environments, however, require that these

# settings are disabled so review and enable them as needed.

#

# Do not accept ICMP redirects (prevent MITM attacks)

#net.ipv4.conf.all.accept\_redirects = 0

#net.ipv6.conf.all.accept\_redirects = 0

# \_or\_

# Accept ICMP redirects only for gateways listed in our default

# gateway list (enabled by default)

# net.ipv4.conf.all.secure\_redirects = 1

#

# Do not send ICMP redirects (we are not a router)

#net.ipv4.conf.all.send\_redirects = 0

#

# Do not accept IP source route packets (we are not a router)

#net.ipv4.conf.all.accept\_source\_route = 0

#net.ipv6.conf.all.accept\_source\_route = 0

#

# Log Martian Packets

#net.ipv4.conf.all.log\_martians = 1

#

###################################################################

# Magic system request Key

# 0=disable, 1=enable all >1 bitmask of sysrq functions

# See https://www.kernel.org/doc/html/latest/admin-guide/sysrq.html

# for what other values do

#kernel.sysrq=438

# The vm.swappiness is a modifier that changes the balance between swapping

# out file cache pages in favour of anonymous pages.

vm.swappiness=1

# This is used to force the Linux VM to keep a minimum number

of kilobytes free

vm.min\_free\_kbytes = 8192

1. Zdroj Obrázok 1: https://bit.ly/3umqX4y [↑](#footnote-ref-2)
2. Zdroj Obrázok 2: https://www.sciencedirect.com/science/article/pii/B9780128036631000012 [↑](#footnote-ref-3)
3. Zdroj Obrázok 3: https://www.researchgate.net/publication/327867486\_The\_Onion\_Routing-The\_Good\_and\_The\_Bad [↑](#footnote-ref-4)
4. Zdroj Obrázok 4: http://raspberry-valley.azurewebsites.net/Raspberry-Pi-Tor-Access-Point/#raspberry-pi-tor-access-point [↑](#footnote-ref-5)