Traffic flow sonda s IDS/IPS postavená na platformě ARM

Bc. Šimon Boškovič

Diplomová práce
2020

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně

Fakulta aplikované informatiky

Ústav počítačových a komunikačních systémů

Akademický rok: 2019/2020

ZADÁNÍ DIPLOMOVÉ PRÁCE

(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení:	**Bc. Šimon Boškovič**
Osobní číslo:	**A18420**
Studijní program:	**N3902 Inženýrská informatika**
Studijní obor:	**Počítačové a komunikační systémy**
Forma studia:	**Kombinovaná**
Téma práce:	**Traffic flow sonda s IDS/IPS postavená na platformě ARM**
Téma práce anglicky:	**A Traffic Flow Probe with IDS/IPS – Based on the ARM Platform**

Zásady pro vypracování

1. Specifikujte funkční požadavky pro navrhovanou sondu.
2. Stanovte funkční omezení dle použité platformy.
3. Navrhěte funkce sondy a schéma komunikaci s centrálním prvkem pomocí netflow.
4. Nasazení navrženého systému v testovacím prostředí.
5. Ověření implementovaných funkcí v testovacím prostředí, zhodnocení návrhu.

Rozsah diplomové práce:
Rozsah příloh:
Forma zpracování diplomové práce: **tištěná/elektronická**

Seznam doporučené literatury:

1. HANES, David, Gonzalo SALGUEIRO, Patrick GROSSETETE, Robert BARTON a Jerome HENRY. *IoT fundamentals: networking technologies, protocols, and use cases for the Internet of things*. Indianapolis, Indiana, USA: Cisco Press, [2017]. Cisco Press fundamentals series. ISBN 1587144565.
2. SORIANO, Miguel. *Information and network security*. Prague: Czech Technical University, [2013]. ISBN 978-80-01-05297-6.
3. PETROVIČ, Michal a Michal KOSTĚNEC. *Bezpečnost počítačových sítí*. Plzeň: Západočeská univerzita v Plzni, 2012. ISBN 978-80-261-0117-8.
4. KADLEC, Jaroslav. *Systém detekce neoprávněného vniknutí pro virtuální komunikační síť: Intrusion detection system for virtual automation network : zkrácená verze habilitační práce*. Brno: VUTIUM, 2010. ISBN 978-80-214-4183-5.
5. KIM, Peter. *Hacking: praktický průvodce penetračním testováním*. Přeložil Jan POKORNÝ. Brno: Zoner Press, 2015. Encyklopedie Zoner Press. ISBN 978-80-7413-313-8.

Vedoucí diplomové práce: **Ing. David Malaník, Ph.D.**
Ústav informatiky a umělé inteligence

Datum zadání diplomové práce: **13. prosince 2019**
Termín odevzdání diplomové práce: **29. května 2020**

doc. Mgr. Milan Adámek, Ph.D.
děkan

Ing. Miroslav Matýsek, Ph.D.
ředitel ústavu

Ve Zlíně dne 9. prosince 2019

Prohlašuji, že

- beru na vědomí, že odevzdáním diplomové práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby;
- beru na vědomí, že diplomová práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk diplomové/bakalářské práce bude uložen v příruční knihovně Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně a jeden výtisk bude uložen u vedoucího práce;
- byl/a jsem seznámen/a s tím, že na moji diplomovou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- beru na vědomí, že podle § 60 odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- beru na vědomí, že podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – diplomovou práci nebo poskytnout licenci k jejímu využití jen připouští-li tak licenční smlouva uzavřená mezi mnou a Univerzitou Tomáše Bati ve Zlíně s tím, že vyrovnání případného přiměřeného příspěvku na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše) bude rovněž předmětem této licenční smlouvy;
- beru na vědomí, že pokud bylo k vypracování diplomové práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tedy pouze k nekomerčnímu využití), nelze výsledky diplomové/bakalářské práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem diplomové práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

- že jsem na diplomové práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně, dne 10.8.2020

Bc. Šimon Boškovič, v.r.
podpis diplomanta

ABSTRAKT

Diplomová práce se zabývá detekcí problému na sítí pomocí automatizovaného získávání síťových dat. Jsou zde ukázány příklady problému, s kterými se lze na síti setkat a které je možno pomocí analýzy dat odhalit. Jsou zde taktéž uvedeny hlavní možnosti využití Netflow pro síťovou analýzu. V závěrečném bodu práce je uveden postup, pomocí kterého lze docílit automatizovaného procesu získávání síťových dat.

Klíčová slova: Síť, Internet, Síťový analyzátor, Netflow, Pcap, SSH, OpenVPN, Konfigurační soubor, Skript.

ABSTRACT

The diplom thesis is focussed on detection network problems throught automated data collectioning. There is few examples of problems which you can detect throught network data anylysis. There is also presented main options why use Netflow for network analysis. In the final part of thesis in shown method that can be use to achieve an automated proccess of network data collectioning.

Keywords: Network, Internet, Network analyzator, Netflow, Pcap, SSH, OpenVPN, Config file, Script.

Velké poděkování patří hlavně panu Ing. Davidu Malaníkovi Ph.D. za pomoc při zpracování diplomové práce, cenné rády a bezproblémové jednání.

OBSAH

ÚVOD

Internet se stal v posledních desetiletích nedílnou součástí každodenního života lidí. Téměř každá domácnost má dnes již přístup k internetu a jen stěží si dokážeme život bez internetu vůbec představit. Používání internetových služeb a sociálních sítí je fenomén dnešní doby a pokud dojde jen k sebemenšímu výpadku, zanedlouho o tom ví celý svět. Aby bylo možné těmto výpadkům předejít, je potřeba sítě monitorovat a patřičně udržovat. Počet uživatelů se zvětšuje každým dnem, což znamená nutnost rozšiřovat výpočetní kapacity pro přenos, ukládání a zpracování dat. Rostou samozřejmě požadavky i na přenosy velkého množství dat s vysokou rychlostí a uživatelé předpokládají spolehlivý, bezpečný a neměnný přenos. Je proto nutností zajistit neustálý vývoj nových zařízení, která budou spravovat a monitorovat provoz v síti. Jakýkoliv problém může správce sítě včas detekovat a zaměřit se na odstranění vzniklých problémů. Tahle zařízení poskytují správcům také informace o využívání určitých služeb, která síť poskytuje, vytížení sítě v jednotlivé dny a v neposlední řadě mohou upozornit na útoky v síti.

Diplomová práce se bude zabývat detekcí problému a následnému řešení bezpečnostních incidentů v síti.

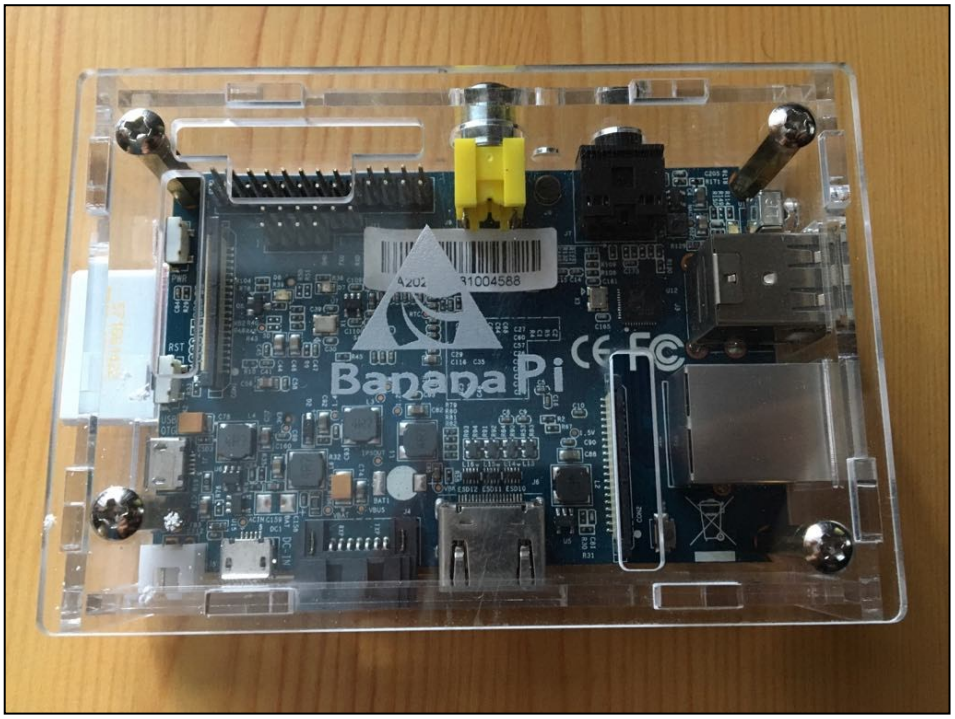
I. TEORETICKÁ ČÁST

1 VÝVOJOVÁ DESKA BANANAPI

Vznik projektu Banana Pi se datuje k začátku roku 2013 jako reakce na vývojovou desku Raspberry Pi. Jedná se o miniaturní počítač postavený na platformě ARM. Procesory postavené na platformě ARM se vyznačují nízkou spotřebou elektrické energie, vysokým výkonem a v neposlední řadě také nízkými nároky na aktivní chlazení procesoru.[1]

1.1 Banana Pi BPI-M1

Pro vypracování modelu Traffic-flow sondy bude použita vývojová deska Banana Pi BPI-M1. Deska disponuje dvoujádrovým procesorem Allwinner A20 Dual-core s frekvencí 1 GHz a operační pamětí 1 GB DDR3. Vývojová deska neobsahuje žádnou interní paměť, obsahuje však rozhraní SATA pro připojení pevného disku, slot pro SD kartu a také HDMI vstup pro připojení k monitoru. Internetové připojení je umožněno díky konektoru RJ45. Deska obsahuje dva USB vstupy pro připojení myši, klávesnice, nebo jiné periferie. Na oficiálních stránkách Banana Pi *http://wiki.banana-pi.org/Banana_Pi_BPI-M1* je možnost si vybrat mezi několika operačními systémy.[2]



Obrázek č. 1- Vývojová deska Banana Pi

1.1.1 Armbian

Armbian je operační systém, který se používá pro počítače postavené na platformě ARM. Pro instalaci je zapotřebí si na oficiálních stránkách armbianu najít pro příslušnou desku aktuální operační systém. Po stažení příslušeného obrazu operačního systému je nutno přes program Disk-Imager soubor zapsat na SD kartu, která se následně vloží do počítače. Po zapnutí si deska začne bootovat operační systém. Systém prověří, zda jsou všechny periferie funkční a následně spustí operační systém.

Obrázek č. 2 - Systém armbian [3]

Operační systém obsahuje nyní pouze základní nástroje (lze jej ovládat jenom přes command-line). Pro nainstalování uživatelského rozhraní je potřeba zpustit příkaz *sudo apt install xfce4,* který stáhne a nainstaluje nenáročné rozhraní *xfce4*. Po dokončení instalace je systém třeba restartovat příkazem *sudo reboot* a po znovu načtení systému a spuštění grafického serveru xorg s desktopovým rozhraním *xfce4*.

Obrázek č. 3 - Uživatelské rozhraní systému Armbian

2 FUNKČNÍ POŽADAVKY

První částí, kterou je potřeba pro realizaci udělat, je analýza a následná specifikace funkčních prvků sondy. Je potřeba si definovat místa a situace, ve kterých se budou testy provádět, jaký výstup se od nich bude očekávat, případně kdo tyhle testy bude provádět.

V prvním kroku je potřeba promyslet, jak komplexní daný systém má být. Uživatel určitě upřednostní systém, který je lehce ovladatelný a časově méně náročný, než systém, který vyžaduje komplexní znalosti dané problematiky.

U sondy je třeba zajistit, aby se daný systém ovládal jednoduše, samotná sonda by se mohla ovládat přes webové rozhraní a ke spuštění by mohlo dojit automaticky po zapnutí desky. Dále je třeba myslet na výstup, který nám systém vytvoří. Pro jednoduchost by informace o výsledku testování měly být v krátké a srozumitelné formě a to i pro člověka, který se v dané problematice nepohybuje. Uživatel určitě neocení zbytečné a nicneříkající informace o chybách, souborech atp. Výsledný soubor by tedy mohl obsahovat informace o počítačích, které se účastní komunikace, dále také jejich IP adresy, informace o přenesených paketech a třeba i graf, na kterém lze vidět hustotu přenesených souboru v uplynulém čase.

Dalším aspektem, který by mohla sonda mít, je filtrace výsledných dat, která uživateli umožňují filtrování dle několika uvedených parametrů. Větší množství dat by mohlo mít za následek nečitelnost výsledku. Testovací program by měl umožnit uložení výsledných dat do souboru pro jejich opětovné načtení a zobrazení historicky uložených dat v předešlých testech. Sonda by dále poskytla detekci podezřelých aktivit v síti, které by mohl vést k narušení bezpečnosti síťového provozu, veškeré podezřelé aktivity by zaznamenávala a po ukončení testu nahlásila.

Souhrn požadavků:

- Nízká komplexnost řešení
- Jednoduché ovládání
- Lehce čitelný výstup
- Rychlost prováděných testů
- Grafické zobrazení výsledků
- Export výsledných dat

3 OMEZUJÍCÍ VLASTNOSTI

Opačným stavem funkčních požadavků pro navrhovanou sondu je stanovení funkčních omezení navrhovaného systému. Je třeba se nad uvedeným řešením zamyslet a následně prozkoumat, zdali zde nejsou žádná omezení, která by mohla limitovat dosavadní řešení. V průběhu měřených testů by mohlo dojít k nečekané změně chování systému, zamrznutí, nebo vypnutí celé vývojové desky.

První omezující vlastnost je stabilita desky. Jakýkoliv větší výkyv napájecího napětí může bez větších problémů způsobit pád desky, a tak i ztrátu neuložených dat. Po připojení klávesnice a myši se deska několikrát sama vypnula a bylo nutné vše odpojit a desku znovu zapnout.

Taktéž je zde otázka stability operačního systému. Obecně se doporučuje použít operační systém Armbian, jelikož poslední verze systému Debian nejsou pro vývojovou desku Banana Pi BPI-M1 příliš stabilní a několikrát způsobily nečekaný pád desky. Pro takové případy by bylo vhodné použití záložního serveru pro ukládání dat. Po každém provedeném testu by se data zálohovala, čím by se předešlo nečekaným ztrátám dat z důvodu selhání desky, nebo operačního systému.

Dalším limitujícím faktorem je výpočetní výkon. Deska je vybavena pouze dvoujádrovým procesorem Allwinnder A20 a operační pamětí 1GB DDR3. Výpočetní výkon s jistotou nebude dostatečný pro hloubkovou analýzu sítě, nebo pro jakékoliv složitější operace. Výkon nebude dostačující ani pro analýzu sítě, která má desítky až stovky uživatelů. Systém by nestačil zpracovávat nepřeberné množství dat, která probíhají sítí a s největší pravděpodobností by se systém zasekl, nebo spadl. Hlubší analýza sítě by potřebovala alespoň 4 GB RAM pro běžící aplikace a čtyřjádrový procesor pro rychlejší zpracování instrukcí. Kapacitní úložiště je v případě použité konfigurace pro desku Banana Pi pouze 16GB, což není dostatečné, bylo by vhodnější použít kapacitní server, nebo cloud úložiště.

Problém bude s real-time sledováním provozu, který je velmi náročný na zpracování. V poslední řadě to mohou být např. DDOS útoky proti Banana Pi, které by dokázaly zahltit síť zbytečnými pakety a desku tímto odstavit. [4]

Souhrn omezujících požadavků

- Stabilita desky
- Výpočet výkon

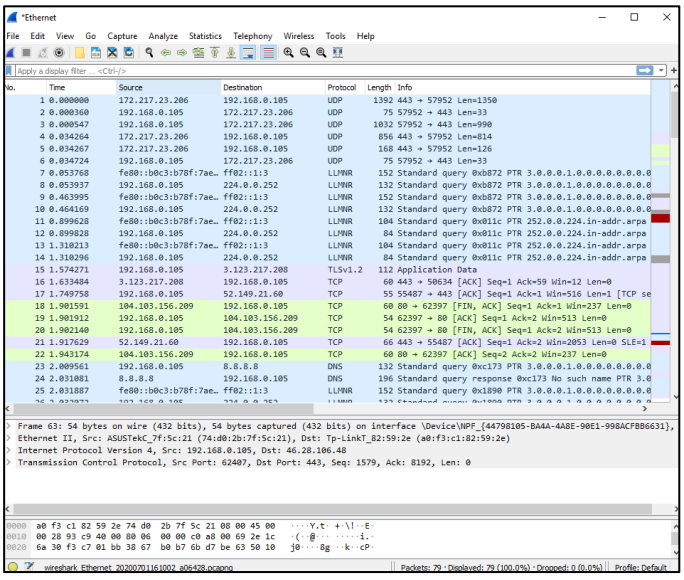
- Omezené úložiště
- Real-time monitoring
- Nebezpečí útoku

3.1 Síťové analyzátory

Analýza síťového toku slouží jako kolektor dat proudících po internetové síti. Pomocí ní lze získávat informace ohledně provozu, množství prošlých dat či detailní analýzu síťových paketů. Za pomocí síťových analyzátorů lze dále provádět např. monitorování stavu sítě, monitorování množství přenesených dat, detekce potenciálních útoků, přehled o využitelnosti sítě v závislosti na určujícím faktoru (např. den v týdnu, roční období) a další.

3.1.1 Zachycení pcap souborů

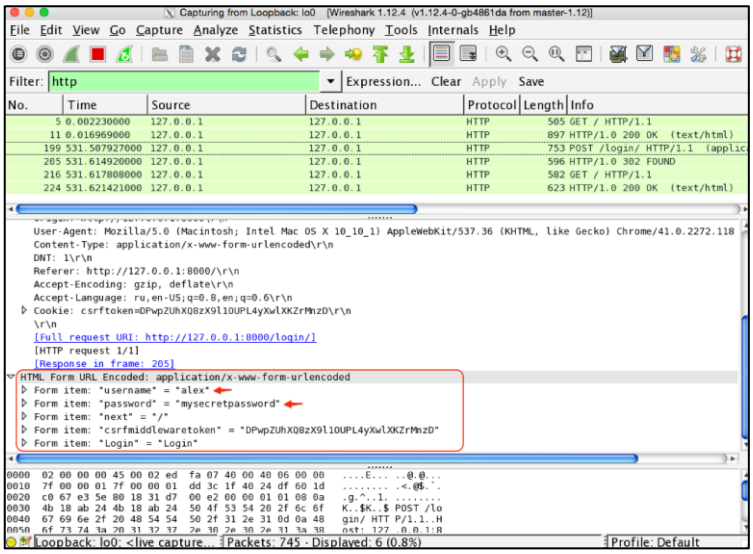
Analyzátor prochází hlavičky IP adres paketů, ze kterých lze následně získat porty nebo IP adresy. Pomocí získaných informací lze sledovat například využití šířky pásma, detekci malwaru, dále lze zjistit, která dvě zařízení mezi sebou komunikují, případně množství přenesených dat nebo použitý protokol. Pcap dále umožňuje filtrování zachycených paketů, které využívá řada programů pro síťový monitoring (např. tcpdump, snort, nmap nebo Wireshark).



Obrázek č. 4 - Ukázka paketového snifferu WireShark

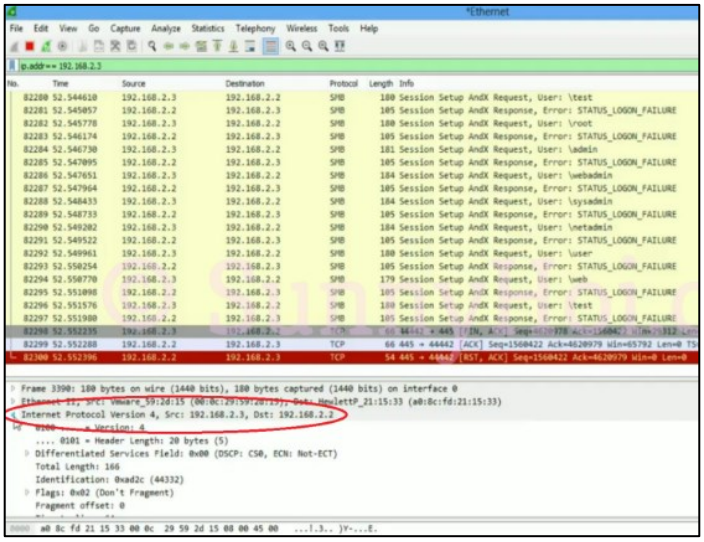
Na obrázku č. 4 je možné vidět ukázku zachycené komunikaci v programu Wireshark. Program zachycuje veškerý síťový provoz paketů TCP/IP a UDP. Provoz je možné filtrovat, podrobně zkoumat, nebo ukládat do .pcap souborů.[5][6]

Pomocí zachycené komunikace lze například zachytit nezabezpečené pakety HTTP, ze kterých můžeme následně vyčíst např. přihlašovací údaje uživatele.[7]



Obrázek č. 5 - Ukázka odchycení nezabezpečené komunikace [7]

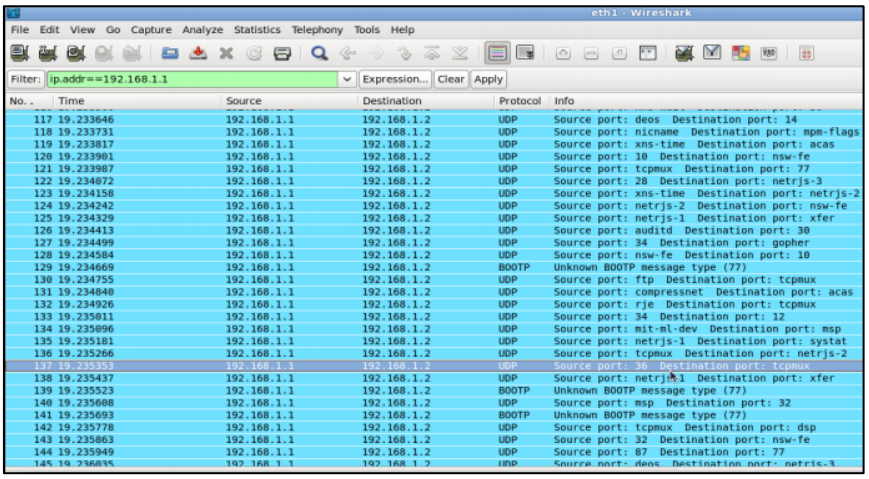
Na obrázku č. 6 je vidět odhalení útoku hrubou silou. Útok se vyznačuje větším množstvím paketů s negativní odpovědí. Jedná se tedy o náhodné pokusy, které mají za cíl např. uhodnutí přihlašovacích údajů uživatele.[8]



Obrázek č. 6 - Ukázka zachycení útoku hrubou silou [8]

Dalším typem útoku je DDOS útok. Jedná se o útok, který má za úkol zahltit server množstvím požadavků, který není schopen zpracovat, případně na požadavek odpovědět. Server se poté začne zpomalovat, nebo vypadne úplně. Útok je zachycen na obrázku č. 7, kde je

možno vidět velký počet paketů se stejným, nebo lehce odlišným obsahem pocházející ze stejného zdroje.[9]



Obrázek č. 7 - Ukázka zachycení DDOS útoku [9]

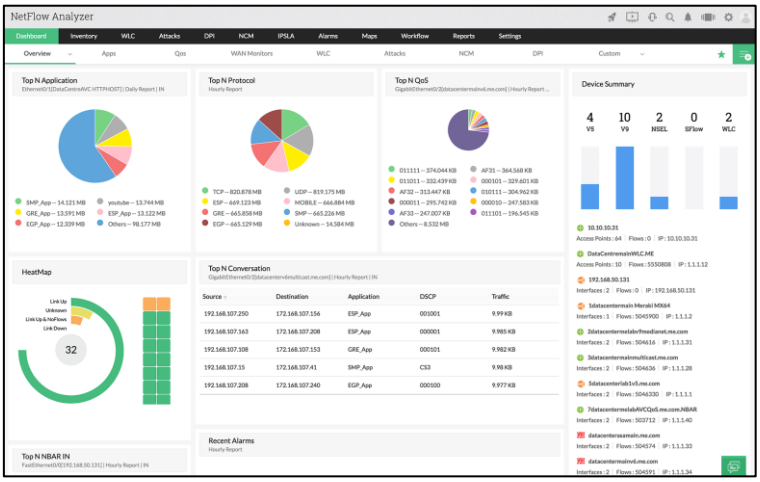
3.2 Netflow

Netflow patří v současné době k nejrozšířenějším standardům pro získávání statistik o datové komunikaci. Jedná se o protokol, který vynalezla společnost Cisco Systém za účelem monitorování síťového provozu. Nejpoužívanější verzí Netflow je verze č. 5.

3.2.1 Využití Netflow

1) Monitorování uživatelů – Pomocí datových toků lze získat detailní přehled využití sítě daným klientem. Lze také odhalit možná bezpečnostní rizika, nebo porušování pravidel síťového provozu.
2) Monitorování sítě – Netflow poskytuje velké možnosti monitoringu sítě v reálném čase. Za pomocí vizuálních analyzátorů datových toků lze získat velmi dobrý přehled z jednotlivých síťových přepínačů nebo směrovačů.
3) Ukládání dat – Získaná data z Netflow lze archivovat a poté použít pro datové analýzy. V případě potřeby mohou být z dat získány historické informace ohledně provozování sítě daným uživatelem.
4) Monitorování aplikací – Umožňuje monitorovat a získat přehled ohledně využití jednotlivých aplikací. Lze poté snadněji předpovídat a odhalovat budoucí vytížení sítě a jejich zdrojů.

5) Vyúčtování provozu – Za pomocí Netflow je možné použít účtovací služby. Provozovatel je schopen pomocí služeb účtovat např. za použití délky pásma, za uplynulý čas, nebo za množství stažených dat. [10][11]



Obrázek č. 8 - Ukázka Netflow analyzátoru [19]

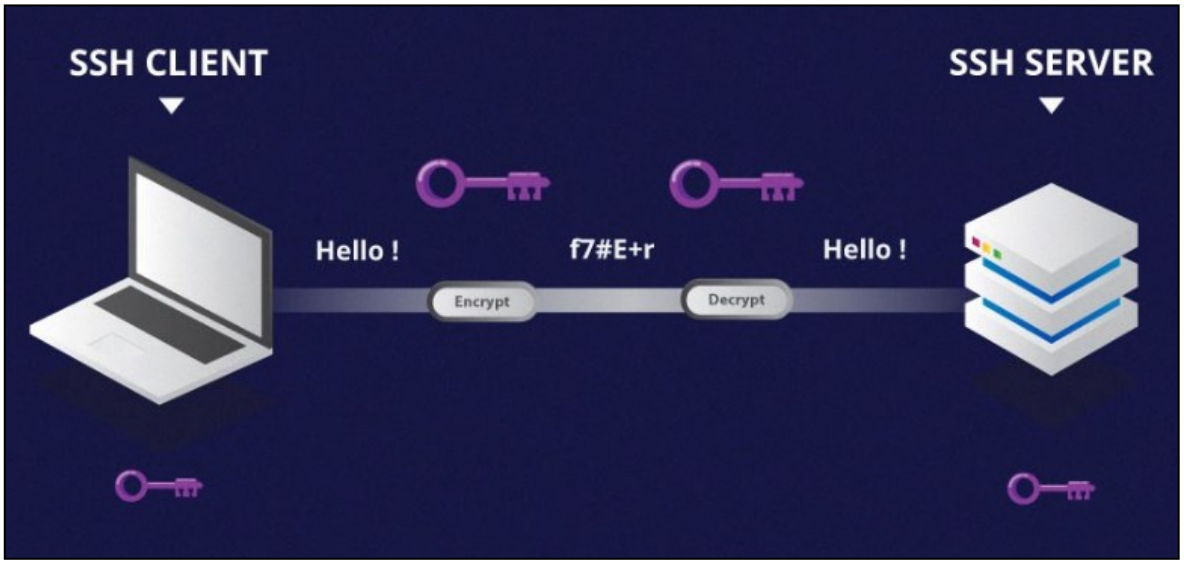
3.3 OpenVPN

OpenVPN je volně dostupný software, který pomocí technologie VPN vytváří v síti internet zabezpečené tunely, mezi kterými může uživatel komunikovat. Pomocí neplacené verze lze vytvořit klient-server a klient-klient propojení. Jedná se o nejrozšířeněji používaný program pro vytváření zabezpečených spojení. Je dostupný jak pro mobilní operační systémy iOS, Android, tak i pro desktopové počítače s operačním systémem Windows, iOS i linux. Mezi hlavní výhody programu patří jednoduchost, přehledné návody na internetu, i možnost rozšíření pomocí pluginů nebo skriptů. OpenVPN používá standardně protokol UDP (lze ale použít i protokol TCP), který funguje na transportní vrstvě a je považován za nespolehlivý protokol, jelikož nezaručí kontrolu doručených paketů a jejich doručení ve správném pořadí. Komunikace probíhá na specificky přiděleném portu 1194. Díky použití jednoho portu lze snadno nakonfigurovat síťový firewall tak, aby propouštěl pakety pouze na daném portu. Pro zabezpečení komunikace používá OpenVPN protokoly SSLv3/TLSv1 a také knihovnu OpenSSL, která podporuje nepřeberné množství kryptografických algoritmů jako Blowfish, AES, 3DES a další.[12][13]

3.4 SSH

SSH v doslovném překladu znamená bezpečná příkazová řádka. Jedná se o zabezpečený komunikační protokol, pomocí kterého lze získat přístup ke vzdálenému počítači. Původní myšlenka vznikla jako náhrada za již zastaralý telnet s nezabezpečenou komunikací. Rozdíl oproti předchůdci je také v tom, že veškerá komunikace probíhá pomocí protokolu SSH, který je šifrovaný, a tedy mnohem bezpečnější.

Protokol se skládá ze tří hlavních vrstev. Transportní protokol, který má na starost vytvoření zabezpečeného připojení, autentizační protokol, který zajišťuje autentizaci klienta a v poslední řadě protokol spojení, který zajišťuje správu logických kanálů v rámci jednoho spojení. Za pomocí klientského programu lze následně vytvořit spojení se vzdáleným počítačem. Pomocí IP adresy uživatele, jeho jména a hesla je možné se připojit pomocí příkazové řádky k počítači, kde mohou být spuštěny příkazy, případně lze přenášet soubory. SSH najde využití např. při administraci serverů přesměrovávání portů, nebo založení VPN. Při konfiguraci SSH je z bezpečnostních důvodů vhodné změnit původní port, jelikož právě tento port bývá častým terčem útoků hrubou silou. Je taktéž vhodné použití komplexnějšího hesla při přihlašování.



Obrázek č. 9 - Princip SSH komunikace [14]

Na obrázku č. 9 lze vidět princip fungování. Po připojení klienta k serveru odpoví server zasláním souboru s číslem verze. Klient následně ověří identitu serveru a dále pak odešle svou vlastní identifikaci zpět. Díky zmíněnému principu je ověřeno, že port je v pořádku a je zahájena komunikace. [15][16]

3.4.1 SSH autentizace

Autentizace uživatelů probíhá pomocí hesel (méně bezpečné), dále za pomocí SSH klíčů (velmi bezpečné) a v poslední řadě pomocí certifikátů.

V dnešní době jsou hesla nejslabší autentizační metodou. Oproti autentizaci veřejným klíčem se hesla přenáší přes síť. SSH má ve většině případů provoz mezi klientem a serverem šifrovaný, ovšem implementace SSH dovoluje i komunikaci bez šifrování. Za určitých podmínek se tedy může stát, že celý komunikační kanál šifrován není a heslo se tedy sítí přenáší nešifrované. Rovněž SSH server samotné heslo vidí, pokud tedy dojde k napadení serveru, útočník může heslo získat.

SSH umožňuje také autentizaci za pomocí klíčů postavenou na asymetrické kryptografii. Sada klíčů obsahuje veřejný (public key) a také privátní (private key). Veřejný klíč může uživatel svobodně sdílet na internetu, ovšem privátní klíč musí být bezpečně uchován a nesmí být nikomu prozrazen.

Pro použití autentizace za pomocí klíčů musí mít uživatel na svém lokálním počítači dvojici SSH klíčů. Veřejný klíč se zkopíruje na serveru do souboru, který se nachází v domovském adresáři *~/.ssh/authorized_keys*. V tomhle souboru se nachází seznam všech veřejných klíčů, které jsou použity k autorizaci uživatelů, kteří se k tomuhle serveru přihlašují. Pokud se tedy nějaký klient připojí k tomuto serveru a chce použít autentizaci pomocí SSH klíčů, tak kontaktuje server a sdělí mu, který z veřejných klíčů má pro autentizaci použít. Server následně zkontroluje, zda se veřejný klíč v adresáři authorized_keys nachází, poté vygeneruje náhodný řetězec znaků a zašifruje ho pomocí vybraného veřejného klíče. Server dále odešle zašifrovanou zprávu vybranému klientovi, ten po obdržení zprávy dešifruje obsah pomocí svého privátního klíče a zkombinuje rozšifrovaný řetězec s dříve dohodnutým ID relace a pošle zpět. Server následně porovná odeslaná a přijatá data. Pokud se data shodují, tak je umožněna komunikace.

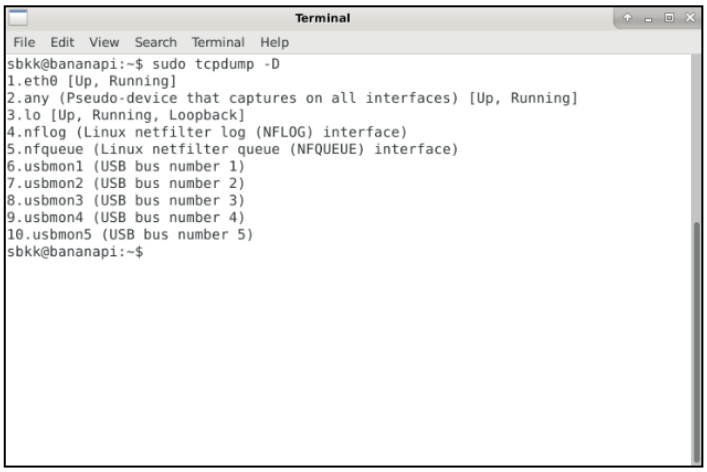
U SSH je taktéž možno použití certifikátů. Nevýhodou je, že SSH v základu neumožňuje použití X509 certifikátů, umožňuje pouze použití svých vlastních. Existují však tyto patche, díky kterým lze přidat podporu pro X509 certifikáty. Tyto patche však nejsou oficiální a mohou tedy obsahovat bezpečností riziko, jelikož zasahují přímo do kódu SSH. Takto pozměněný kód může obsahovat chyby, kvůli kterým může být použití certifikátů pro uživatele nebezpečné.[17][18]

I. PRAKTICKÁ ČÁST

3.4.2 Zachycení síťové komunikace

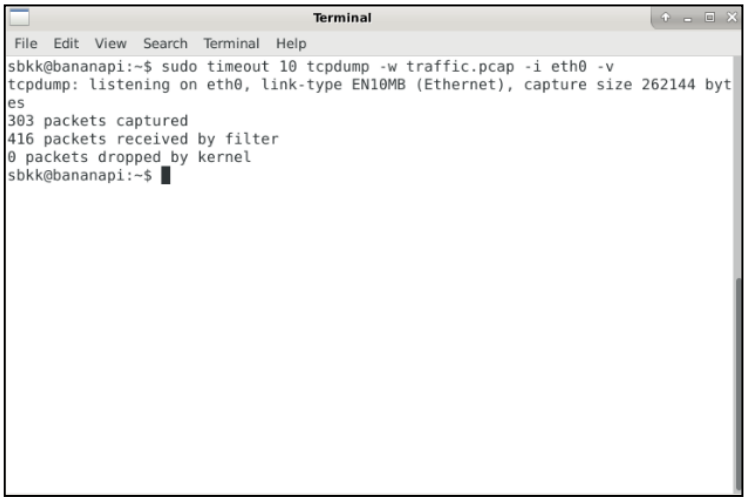
Sledování a následné zachycení síťového provozu bude prováděno pomocí paketového analyzéru *tcpdump.* Pomocí programu lze sítovou komunikaci sledovat, nastavovat filtry dle potřeby a také uložit sledovanou komunikaci do souboru s příponou *pcap*, kterou lze následně otevřít např. v programu Wireshark.

V prvním kroku bude zjištěno, jak velký soubor vznikne při plném vytížení sítě. Po nainstalování *tcpdump* je třeba vybrat správné síťové rozhraní.



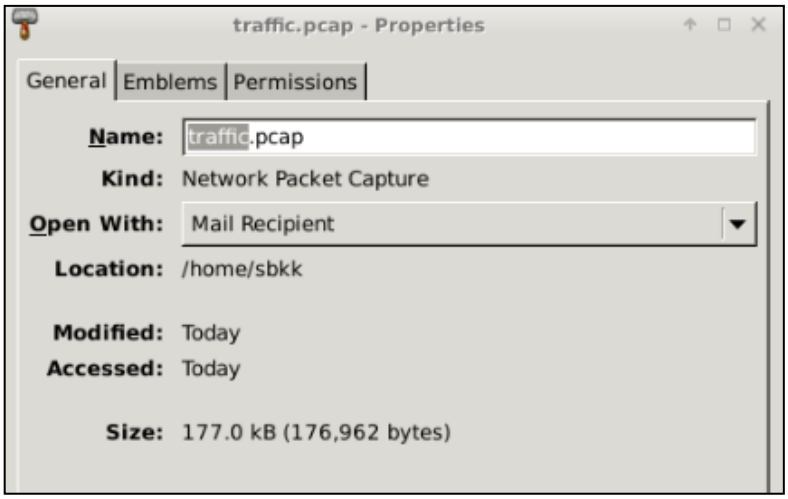
Obrázek č. 10 - Dostupná síťová rozhranní

Na obrázku č. 10 jsou zobrazena všechna dostupná zařízení. Pro sledování provozu sítě bude použito rozhraní *eth0*.



Obrázek č. 11 - Zachycená komunikace v rozhranní eth0

Na obrázku č. 11 je možné vidět zachycenou komunikaci na rozhraní *eth0.* Za dobu deseti vteřin bylo zachyceno 303 paketů.

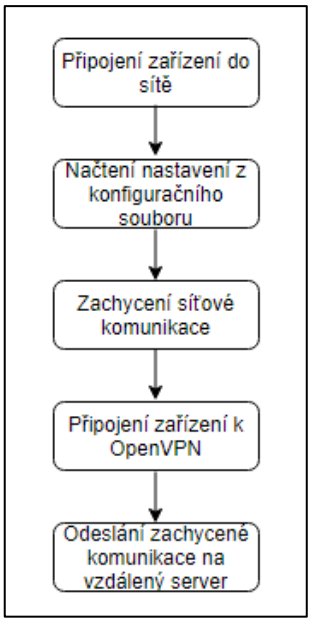


Obrázek č. 12 - Velikost souboru se zachycenou komunikací

Celková velikost souboru se zachycenou komunikací je 177 kB. Pokud by komunikace trvala delší dobu, tak by bylo vhodné použít datové úložiště, jelikož by výsledný soubor mohl mít řádově i stovky megabajtů.

4 FUNKCE SONDY

V následující sekci budou popsány funkce sondy. Je třeba definovat, jak bude samotná sonda fungovat, odkud se budou brát autorizační údaje, jak bude fungovat shromažďování a odesílání zachycené komunikace. Dále je třeba zajistit start běhu programu po spuštění samotné desky.



Obrázek č. 13 - Schéma komunikace

V prvním kroku návrhu je třeba zajistit konfigurační soubor. Konfigurační soubor je důležitý kvůli samotnému nastavení. Soubor bude připraven v předdefinované lokaci na pevném disku sondy a bude obsahovat všechny potřebné informace pro analýzu sítě. Pro lepší práci s konfiguračním souborem bude veškeré nastavení ve formátu JSON.

Obrázek č. 14 - Ukázka nastavení ve formátu JSON

4.1 Ovládací skript

V programovacím jazyku Python bude napsán skript, který konfigurační soubor po resetu zařízení otevře, následně přečte všechny potřebné parametry a uloží si je do proměnných. Python následně začne příkazy v systému spouštět.

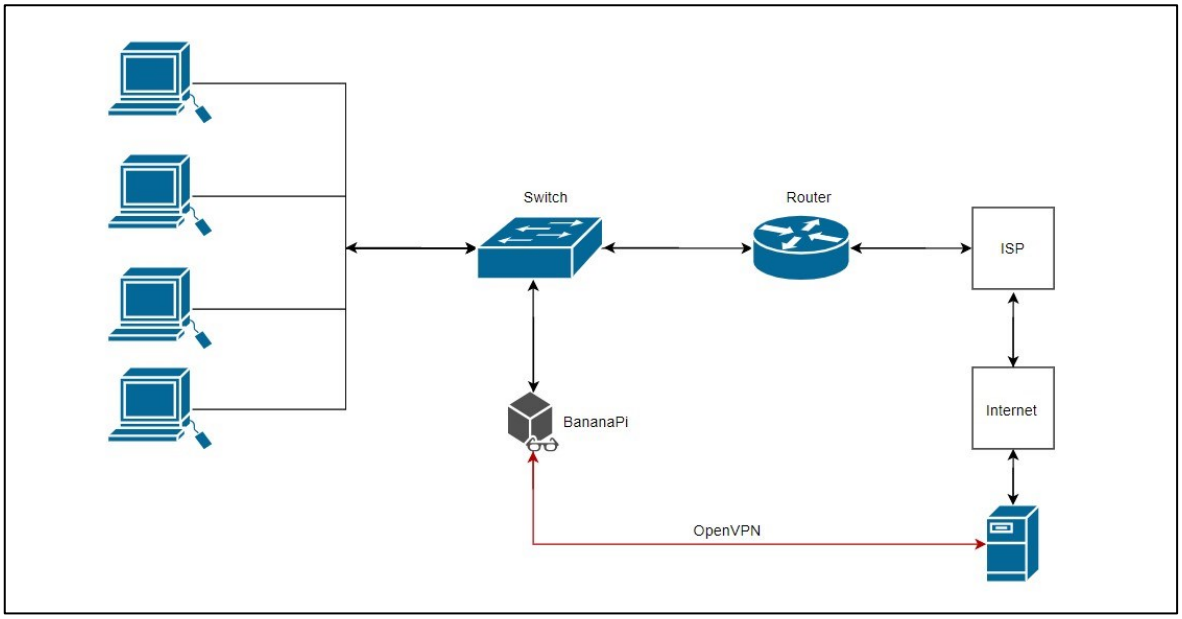
Samotný skript, který bude spouštět příkazy, bude umístěn v paměti zařízení. Jeho zapnutí bude provedeno pomocí softwarového démona *Cron,* ve kterém má uživatel možnost si nastavit skripty nebo příkazy, které se mají zapnout v určitý čas, nebo při nějaké události, např. zapnutí zařízení.

Z konfiguračního souboru se nejprve začnou získávat informace ohledně OpenVPN. Do JSONu je třeba zadat cestu k souboru, který obsahuje nastavení pro připojení k dané VPN. Pro spuštění OpenVPN se použije příkaz „*sudo open --config* + ‚cesta k souboru'". Je zde ovšem problém s linuxovým příkazem pro získání nadřazených práv uživatele „*sudo*". Po zadání již zmíněného příkazu je uživatel nucen ručně zadat heslo, až poté jsou mu přiděleny práva nadřazeného uživatele (samozřejmostí je zadání správného hesla). Pro případ sondy, kdy se má automaticky k OpenVPN připojit, je třeba zvolit variantu, kdy systém nevyžaduje zadání hesla. Spuštění OpenVPN bez nutnosti zadání hesla bude popsáno v sekci konfigurace zařízení.

Po úspěšném připojení začne sonda zachytávat pakety na vybraném internetovém rozhraní pomocí programu tcpdump, nebo začne zachytávat Netflow. Nastavení tcpdump se bude brát z konfiguračního souboru. Bude zde uvedeno internetové rozhraní, které se má použít, dále doba po jakou bude skenování probíhat a v poslední řadě název souboru s cestou, kde výsledný soubor uložit.

Zachycený soubor bude ve formátu „*cap_rok_den_měsíc".* Je ovšem třeba zajistit, aby se výsledný soubor nepřepisoval stále dokola v případě, že by bylo provedeno více analýz v jeden den. Ve skriptu bude proto část kódu, která se bude starat o to, aby se výsledný soubor nepřepisoval stále dokola, ale aby v případě nalezení souboru se stejným jménem za něj doplnil závorku s číslem, např. „*cap_2020_5_17(2)*".

4.2 Schéma sítě



Obrázek č. 15 - Schéma sítě

Na obrázku č. 15 je možno vidět schéma zapojení ve zkoumané síti. Sonda BananaPi je zde zapojená do switche, ke kterému jsou připojeny všechny ostatní počítače v síti. Switch je dále připojen přes router do internetové sítě. Sonda BananaPi je připojená přes VPN ke vzdálenému serveru.

Sonda tedy po připojení do soustavy začne shromažďovat data, která switchem prochází a následně je odešle přes zabezpečenou OpenVPN na vzdálený server. Pro zamezení vzdáleného připojení útočníka k sondě bude mít zařízení zavřené všechny porty kromě těch, které jsou potřebné pro komunikaci s OpenVPN. V poslední části bude proveden test, který oskenuje zařízení a bude zjišťovat, zda má sonda nějaké porty otevřené.

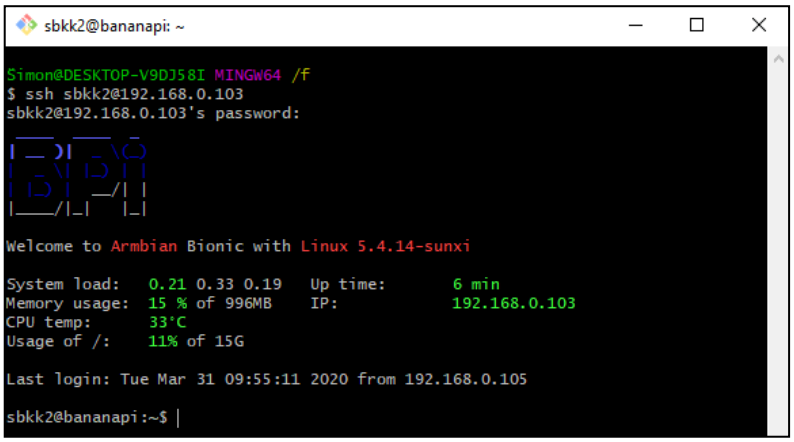
5 KONFIGURACE ZAŘÍZENÍ

Konfigurační nastavení zařízení bude uloženo v zařízení ve formátu JSON. Jak již bylo řečeno, formát JSON byl zvolen z důvodu jednoduššího získávání informací ze souboru. Tento konfigurační soubor však bude nutné přenést ze vzdáleného zařízení na sondu. Přenesení souboru bude provedeno pomocí Secure Copy (SCP), které slouží k bezpečnému přenosu dat mezi dvěma propojenými počítači na stejné síti pomocí protokolu SSH.

5.1 Nastavení SSH

Pro připojení přes SSH je potřeba mít na sondě nainstalovaného SSH klienta. Pokud se tedy uživatel připojuje ze zařízení, kde je použitý např. operační systém Windows, tak je třeba mít nainstalovaný OpenSSH Server.

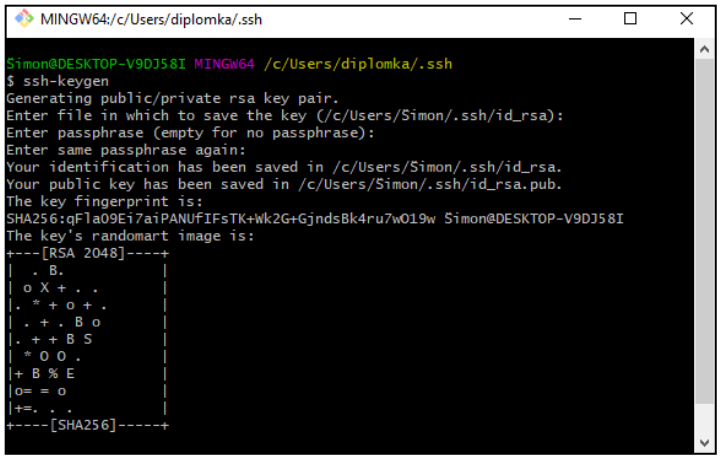
Pokud je na obou zařízeních správně nainstalované SSH, je poté umožněno se připojit z jednoho zařízení na druhé. Uživatel se připojí na druhé zařízení příkazem *ssh jménoPc@IPadresa*. Po zadání hesla je uživateli umožněno ovládat druhé zařízení pomocí příkazového řádku.



Obrázek č. 16 - Připojení přes SSH pomocí hesla

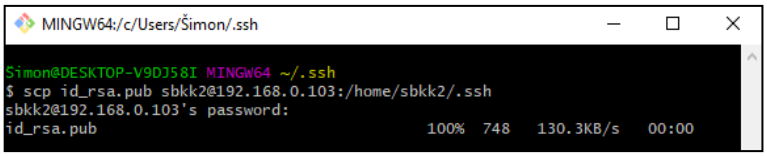
Na obrázku č. 16 je zobrazen příkazový řádek, pomocí kterého lze ovládat sondu. Uživatel může provádět libovolné operace pomocí příkazů, měnit nastavení, nebo přenášet data. Bohužel přihlašování pomocí hesla, jak již bylo řečeno v sekci SSH autentizace, není bezpečná, a proto zde bude použita autentizace pomocí klíčů. Již zmíněná metoda je daleko bezpečnější, navíc odpadá nutnost zadávání hesla ručně. Pokud zařízení prokáže svoji identitu, je mu zpřístupněn příkazový řádek.

Pro použití autentizace pomocí klíčů je potřeba na vzdáleném počítači vygenerovat v domovském adresáři *C:\Users\username\.ssh* veřejný a privátní klíč. K vygenerování klíčů slouží příkaz *ssh-keygen*. Po vygenerování vzniknou v již zmíněném adresáři dva soubory. Veřejný klíč s názvem *id_rsa.pub* a privátní klíč *id_rsa*.



Obrázek č. 17 - Generování veřejného a privátního klíče

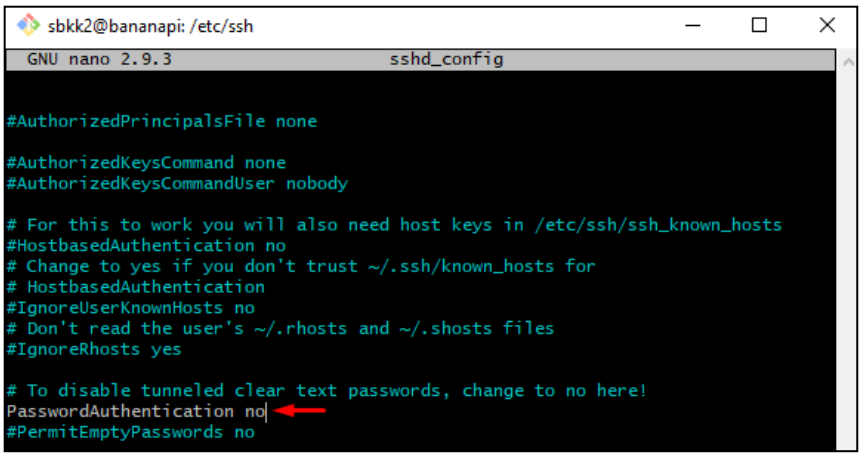
Dalším krokem je vytvoření stejné složky *.ssh* v domovském adresáři sondy. V nově vytvořené složce je třeba příkazem *touch ~/.ssh/authorized_keys* vytvořit soubor *authorized_keys,* který bude sloužit pro uchování veřejných klíčů všech zařízení, které se budou k sondě připojovat přes SSH. Veřejný klíč je nutno překopírovat do souboru *authorized_keys*. Je zde více možností, jak toho dosáhnout. Pro jednoduchost zde bude uveden postup, kdy se přes příkaz *scp* veřejný klíč nakopíruje do již zmíněné složky a poté se klíč umístí do souboru s veřejnými klíči.



Obrázek č. 18 - Kopírování veřejného klíče do adresáře sondy

Obrázek č. 19 - Překopírování veřejného klíče do souboru authorized_keys

Na obrázku č. 18 a č. 19 je zobrazeno překopírování veřejného klíče vzdáleného zařízení do domovského adresáře sondy a následné zapsání klíče do souboru *authorized_keys*.
V posledním kroku je třeba v konfiguračním souboru SSH vypnout ověřování pomocí hesla. Konfigurační soubor se nachází v adresáři */etc/ssh/sshd_config*.

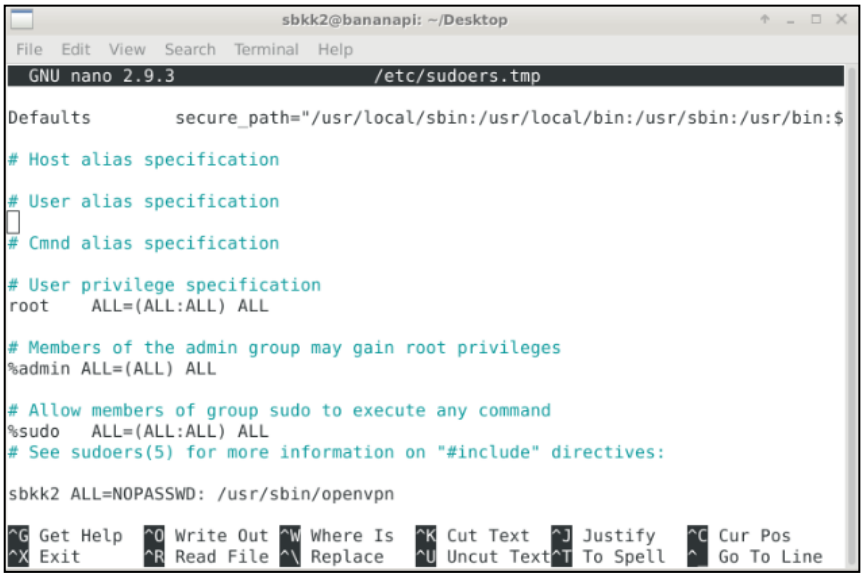


Obrázek č. 20 - Úprava konfiguračního souboru

Po úpravě konfiguračního souboru je nutno službu SSH restartovat. Verifikovaný uživatel se poté může přihlásit bez nutnosti zadávání hesla.

5.2 Nastavení oprávnění pro OpenVPN

V linuxovém adresáři */etc*, v souboru *sudoers.tmp* lze nastavit oprávnění pro jednotlivé uživatele. Lze zde tedy zakázat zadání hesla pro příkazy, kde je nutnost vyšších oprávnění.



Obrázek č. 21 - Soubor sudoers.tmp

Na obrázku č. 21 je zobrazen obsah souboru. Na poslední řádek byl přidán příkaz, který zruší potřebu zadání hesla pro spuštění OpenVPN na daném uživateli. Kdykoliv tedy uživatel zadá příkaz pro připojení k OpenVPN, systém nebude vyžadovat heslo a automaticky se připojí.

5.3 Nastavení konfiguračního souboru

Jak již bylo řečeno, v konfiguračním souboru bude uloženo veškeré nastavení. Tohle nastavení lze změnit jak na vzdáleném zařízení, tak i na sondě (za předpokladu, že soubor byl překopírován do adresáře sondy).

```
"name": "BananaPI-ConfigFile",
"version": "0.0.1",
"bananaPi": {
  "captured-files-directory": "/home/sbkk2/captured-files/"
},
"remote-server-info": {
  "server-name": "diplomka",
  "server-ip-address": "192.168.0.105",
  "cap-file-location": "C:/Users/diplomka/Desktop"
},
"OpenVPN": {
  "path": "/home/sbkk2/openvpn/ceske-vpn.ovpn"
},
"network-analyze-info": {
  "send-pcapFiles": "true",
  "send-NetFlow": "false"
},
```

Obrázek č. 22 - Nastavení konfiguračního souboru

Na obrázku č. 22 je zobrazeno základní nastavení, které bude použito pro analýzu sítě. Jsou zde uvedeny informace o adresáři, kde soubory na sondě ukládat. Dále informace o vzdáleném serveru, kde soubory zasílat a cesta k adresáři se souborem k OpenVPN.

Konfigurační soubor je třeba přenést do adresáře sondy */home/sbkk2/device-settings.* Skript, který bude po startu zařízení spuštěný, bude hledat konfigurační soubor v tomhle adresáři. Pokud skript soubor nenajde, nebude provedená analýza sítě.

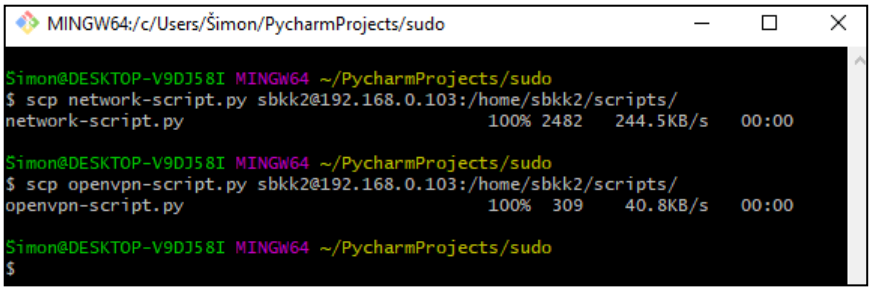
```
MINGW64:/c/Users/Šimon/PycharmProjects/helloWorld
Simon@DESKTOP-V9DJ58I MINGW64 ~/PycharmProjects/helloWorld
$ scp device-settings.json sbkk2@192.168.0.103:/home/sbkk2/device-settings
device-settings.json                          100%  865   110.8KB/s   00:00

Simon@DESKTOP-V9DJ58I MINGW64 ~/PycharmProjects/helloWorld
$
```

Obrázek č. 23 - Přenesení konfiguračního souboru

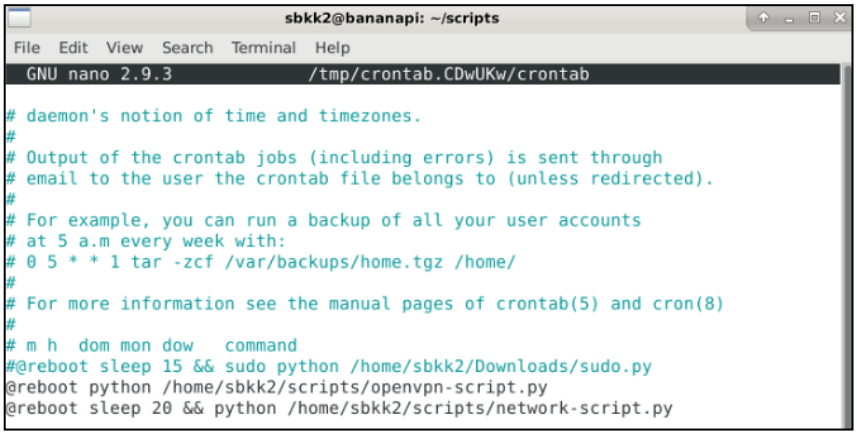
5.4 Nastavení spuštění skriptu

V posledním bodě konfigurace zařízení je nutné zajistit spuštění skriptu po startu zařízení. Pro tenhle účel bude použit softwarový démon *Cron.*



Obrázek č. 24 - Přenesení skriptů

Do adresáře */home/sbkk2/scripts/* byly přeneseny dva skripty. První skript slouží pro analýzu sítě a druhý je zde pro připojení k OpenVPN. Příkazem *crontab –e* se uživatel dostane do plánovacího nástroje, pomocí kterého lze automatizovat spouštění příkazů, programů atd.



Obrázek č. 25 - Nastavení spouštění skriptů

Nastavení automatického spuštění skriptů je znázorněno na obrázku č. 25. První je spuštěn skript, který zařízení propojí k OpenVPN. V souboru je dále nastavena prodleva dvaceti vteřin z toho důvodu, aby se zařízení stihlo připojit k OpenVPN před tím, než bude spuštěna analýza sítě. Skript pro analýzu sítě si načte konfigurační soubor ze kterého přečte veškerá nastavení, která jsou nutná k zachycení komunikace a jejímu odeslání na vzdálené zařízení. Konfigurační soubor bude moci uživatel přes SSH libovolně upravovat. Bude zde možnost nastavit, jak dlouho má analýza sítě probíhat, dále místo, kde zachycené soubory ukládat, nebo zda má sonda zachytávat pakety pomocí TCPdump, nebo zasílat netflow pakety.

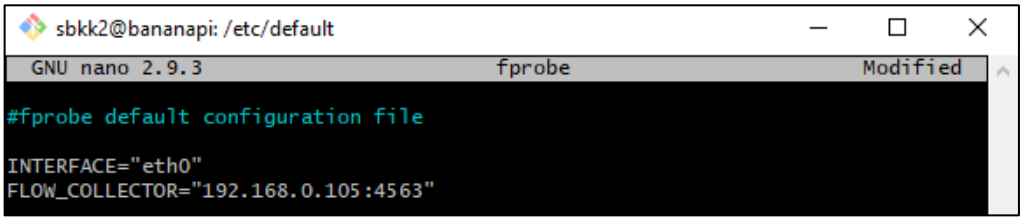
5.5 Zapojení zařízení do infrastruktury

Do zařízení byly přeneseny veškeré potřebné soubory a také bylo provedeno nastavení konfiguračního souboru. Zařízení je nyní třeba připojit do struktury v síti, kterou chce daný uživatel sledovat. K připojení do sledované sítě je třeba napájecí a ethernetový kabel. Zařízení se pro připojení napájecího kabelu zapne a naběhne základní linuxový systém armbian. Systém zařízení lze ovládat pomocí příkazové řádky.

Po naběhnutí systému se začnou zpracovávat instrukce softwarového démona Cron. V prvním bodě se zapíná skript, který vyhledá konfigurační soubor a najde v něm adresu souboru pro připojení k OpenVPN. Adresa k souboru poslouží jako cílový parametr k příkazu, který spouští připojování. Pomocí skriptu se zařízení připojí k OpenVPN a zároveň proběhne ping na vnitřní adresu sítě pro ověření, zda bylo zařízení úspěšně připojeno do nastavené sítě. Pokud připojení proběhlo v pořádku, je spuštěn druhý skript.

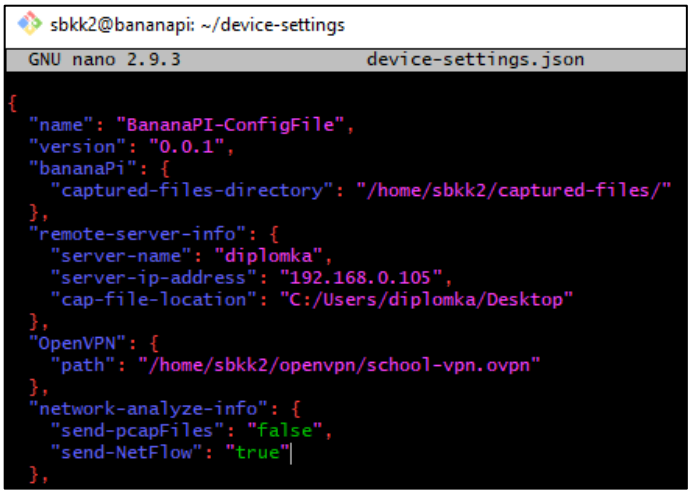
Pomocí druhého skriptu je provedená nastavená analýza sítě. Skript si znovu vyhledá konfigurační soubor a uloží si nastavené hodnoty do proměnných. Dle nastavených hodnot je provedena analýza sítě. Zařízení je schopné zachytávat síťovou komunikaci, nebo posílat Netflow na vzdálený server. Pokud je zařízení nastaveno na zachycení komunikace, tak je na vybraném síťovém rozhraní spuštěn tcpdump. Délka analýzy sítě je určená parametrem v konfiguračním souboru. Po uplynutí stanovené doby se zachycená komunikace uloží do souboru a odešle se na vzdálený server. Na vzdáleném zařízení je možné soubor analyzovat např. pomocí programu Wireshark.

V případě, že je v konfiguračním souboru povolena možnost zasílat Netflow, tak zařízení emituje zachycené Netflow na vzdálený server. Posílání Netflow je umožněno pomocí emitoru „*fprobe*“. Nastavení sondy je uloženo v adresáři „*/etc/default/fprobe*“. Zde je nutné nastavit rozhraní, na kterém je Netflow zachytáváno a také adresu a port kolektoru dat. Na vzdáleném zařízení je třeba zapnout odposlouchávání na portu 4563.



Obrázek č. 26 - Nastavení fprobe – nastavení serveru

Sondu BananaPi lze ovládat pomocí SSH ze vzdáleného zařízení. Pomocí připojení lze měnit např. konfigurační soubor. Na obrázku č. 27 je možné vidět změnu ze zachytávání síťové komunikace za pomocí programu tcpdump na zasílání Netflow. Zařízení je poté nutno příkazem „*sudo reboot*“ restartovat.



Obrázek č. 27 - Změna nastavení konfiguračního souboru

Ve čtvrté části bylo vysvětleno, jak probíhá konfigurace zařízení. Bylo popsáno, jakým způsobem vygenerovat privátní a veřejný klíč, který slouží pro SSH autentizaci bez nutností zadání hesla. V další části byl uveden postup, jak nevyžadovat heslo pro příkazy, kde je nutnost vyšších oprávnění. V poslední části je popsáno, jakým způsobem docílit spuštění obou skriptů po startu zařízení.

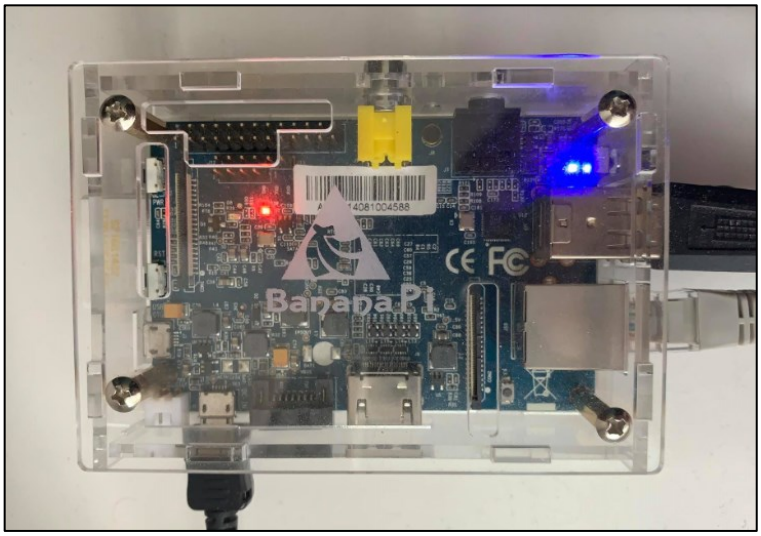
Zařízení je v současné době připraveno k nasazení do reálného provozu. V další části bude ověřeno, zda implementované funkce fungují v reálném prostředí. Zařízení bude zapojeno do místní sítě a bude zachytávat síťový provoz, který následně bude odesílat na vzdálené zařízení.

V první částí testování bude nutné zařízení znova nakonfigurovat pro chod v dané síti. Bude třeba zjistit přidělené IP adresy pro obě zařízení a dle nich nastavit konfigurační soubor. Dále bude třeba do konfiguračního nastavit jméno vzdáleného serveru a adresář, kde budou zaslány soubory se zachycenou komunikací. Po nastavení všech potřebných parametrů budou provedeny testy implementovaných funkcí. Bude taktéž ověřeno, zda se na zařízení nebude dát připojit ze sledované sítě, tj. že zařízení bude mít zavřeny všechny komunikační porty. V případě otevřených komunikačních portů by mohl potenciální hacker zařízení napadnout.

6 OVĚŘENÍ IMPLEMENTOVANÝCH FUNKCÍ ZAŘÍZENÍ

Sonda BananaPi bude připojena do místní internetové sítě. Jakožto vzdálené zařízení bude zvolen server UTB, na který budou zasílána data. V následující části bude nutno zařízení nakonfigurovat pro komunikaci se vzdáleným serverem.

6.1 Nastavení BananaPi



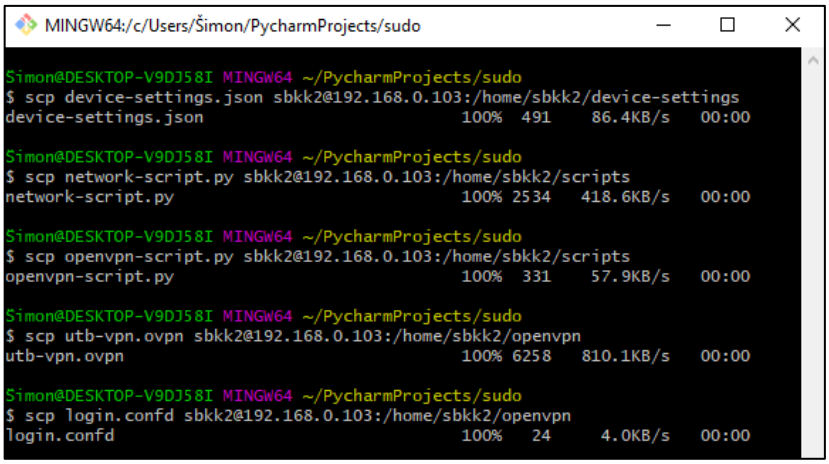
Obrázek č. 28 - Sonda připojená k místní síti

device-settings.json

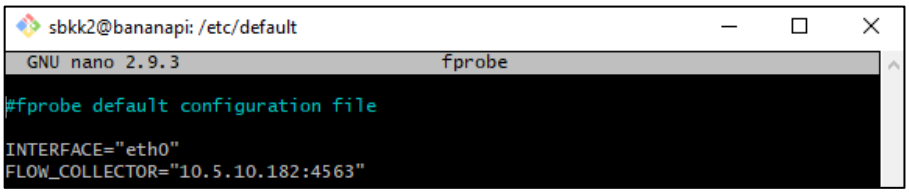
```
{
  "name": "BananaPI-ConfigFile",
  "version": "0.0.1",
  "bananaPi": {
    "captured-files-directory": "/home/sbkk2/captured-files/"
  },
  "remote-server-info": {
    "server-name": "root",
    "server-ip-address": "10.5.10.182",
    "cap-file-location": "pcap",
    "netflow-file-location": "netflow"
  },
  "OpenVPN": {
    "path": "/home/sbkk2/openvpn/utb-vpn.ovpn"
  },
  "network-analyze-info": {
    "send-pcapFiles": "true",
    "send-NetFlow": "false",
    "duration": 60
  }
}
```

Obrázek č. 29 - Nastavení konfiguračního souboru

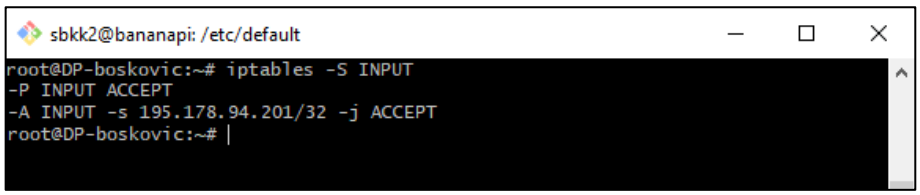
Na obrázku č. 28 je zobrazena sonda připojená do místní sítě. Konfigurace souboru proběhla na obrázku č. 29, jsou zde nastaveny všechny informace, které jsou nutné pro síťovou analýzu. V další části proběhne přenesení všech potřebných komponent do paměti sondy.



Obrázek č. 30 - Přenesení souborů do paměti sondy



Obrázek č. 31 - Nastavení Netflow emitoru



Obrázek č. 32 - Přidání IP adresy zařízení do iptables

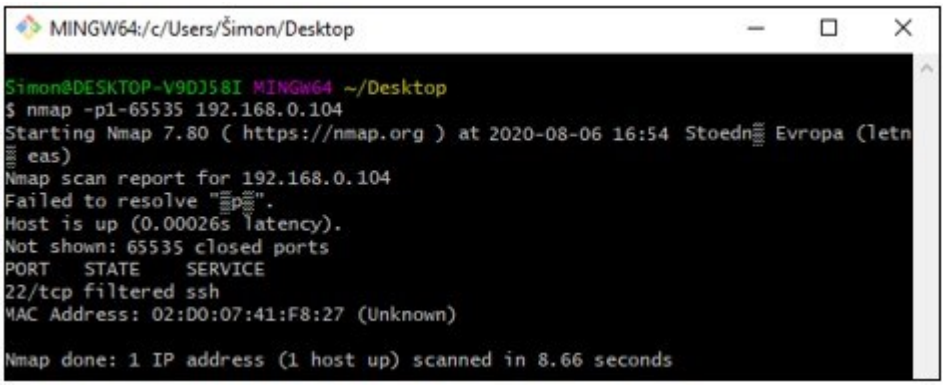
Zařízení je v současné chvíli připraveno na ověření implementovaných funkcí z předešlých kapitol. V následující sekci budou provedeny celkově čtyři testy. Dva pro zachycení a odeslání pcap souboru a dále dva pro odeslání Netflow.

6.2 Nastavení vzdáleného serveru

Jakožto vzdálené zařízení byl zvolen server UTB, k serveru je možné se připojit pomoci SSH za předpokladu, že je zařízení přepojeno na příslušnou OpenVPN. Na serveru bude třeba vytvořit jednu složku pro pcap soubory a druhou pro Netflow.

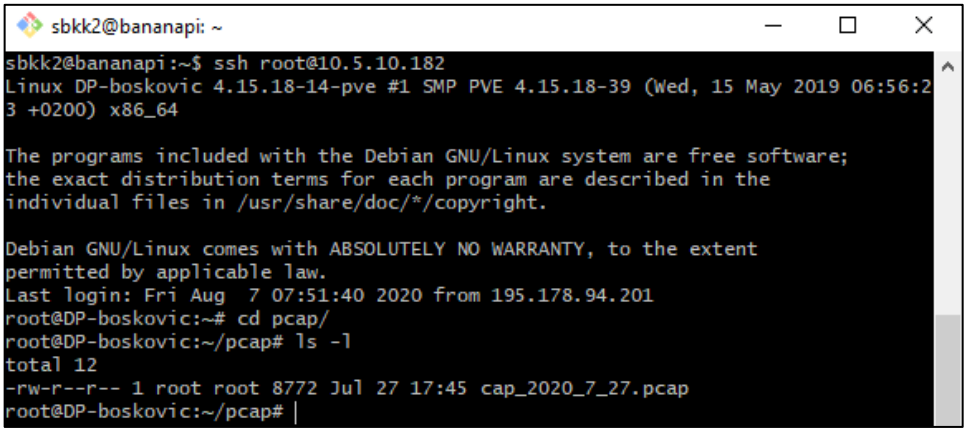
Obrázek č. 33 - Vytvoření složek na serveru

6.3 První test – zachycení a odeslání pcap souborů



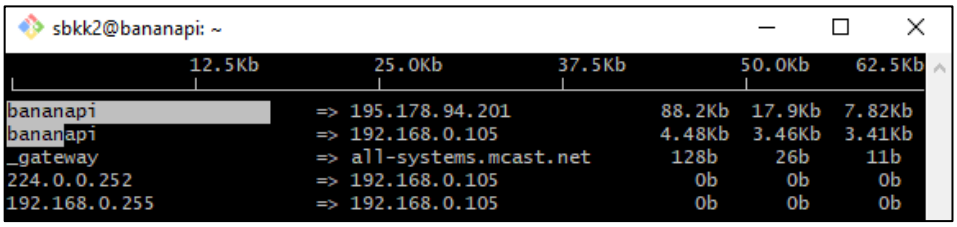
Obrázek č. 34 - Sken otevřených portů zařízení

Na obrázku č. 33 je znázorněn sken všech portů zařízení. Všechny komunikační porty zařízení musí být zavřeny z důvodu bezpečnosti. Pomocí příkazu „*nmap -p- IP-Adresa*“ se naskenují porty v rozsahu 1 – 65 535 a zobrazí se ty, které jsou otevřené. Po úspěšném oskenování portů bylo zařízení restartováno a následně se počkalo na vykonání skriptu.



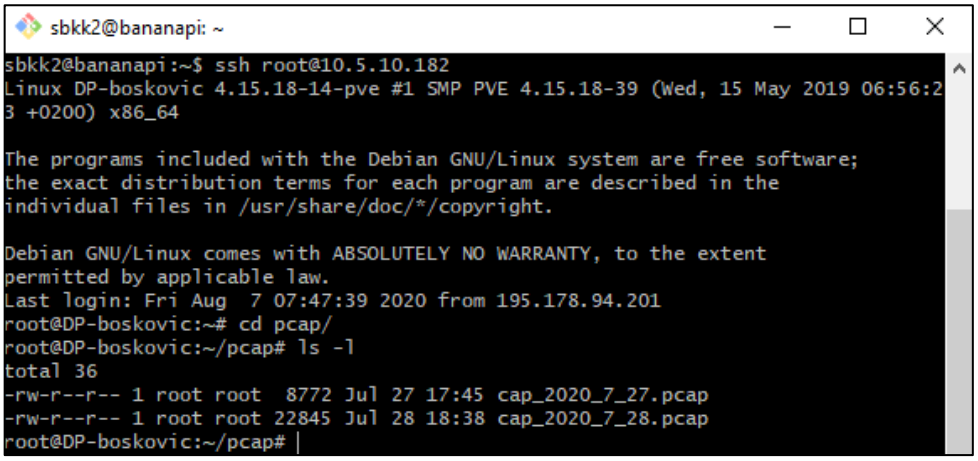
Obrázek č. 35 - Odesláné soubory na vzdálené zařízení v testu č. 1

Na obrázku č. 34 jsou zobrazena zachycená data, která byla zaslána na vzdálený server. Všechny části skriptu tedy proběhly úspěšně. V případě jakékoliv chyby (např. chybějící odezvě na vnitřní adresu OpenVPN, nebo špatně zadané IP adresy) by soubor zaslán nebyl. Na obrázku č. 35 jsou vyobrazeny velikosti přenesených souborů na vzdálené zařízení.

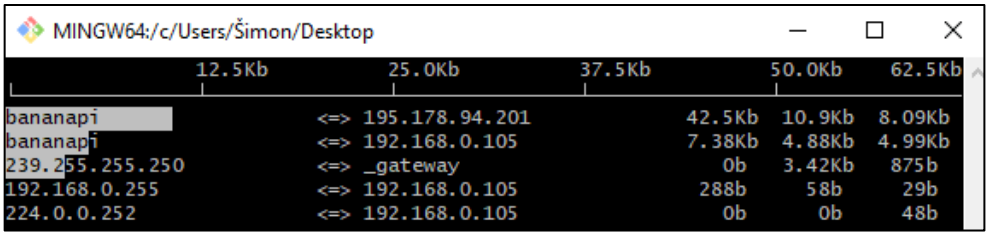


Obrázek č. 36 - Velikosti přenesených souborů v testu č. 1

6.4 Druhý test - zachycení a odeslání pcap souborů



Obrázek č. 37 - Odesláné soubory na vzdálené zařízení v testu č. 2

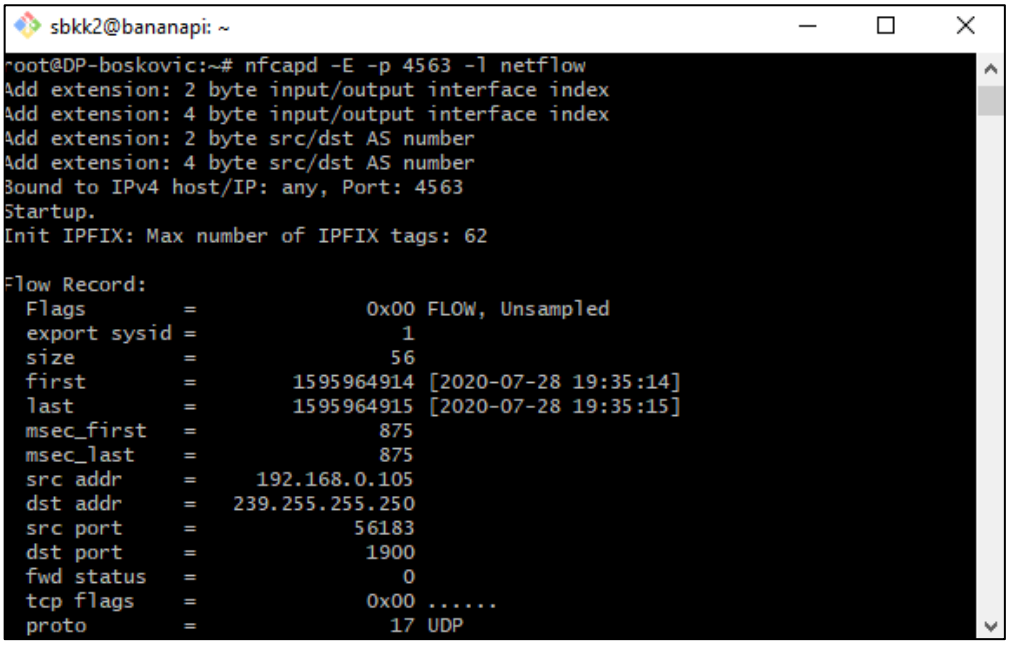


Obrázek č. 38 - Velikosti přenesených souborů v testu č. 2

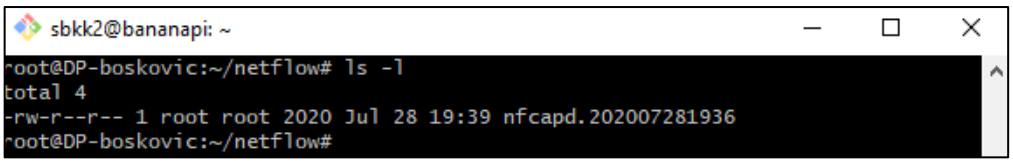
Provedené testy ukázaly správnou funkčnost první implementované části skriptu. Zařízení se po startu úspěšně připojilo k OpenVPN a začalo na lokální síti zachytávat za pomocí síťového snifferu pakety. Výsledný soubor byl uložen do paměti zařízení a poté překopírován na vzdálený server.

V další části testování bude provedeno posílání Netflow na vzdálený server. Na vzdáleném serveru je nainstalován nfcapd, který slouží pro sběr Netflow dat. Pomocí nfcap bude na serveru otevřen port (4563), na který bude sonda emitovat zachycené Netflow. Výsledný soubor bude poté uložen do paměti serveru.

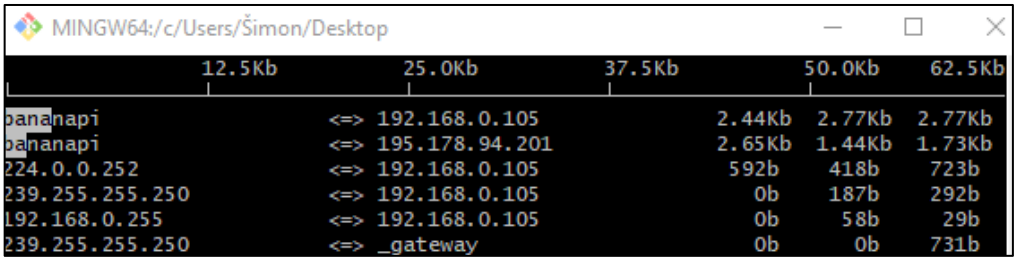
6.5 První test – posílání Netflow na vzdálené zařízení



Obrázek č. 39 - Otevření portu 4563 v testu č. 3



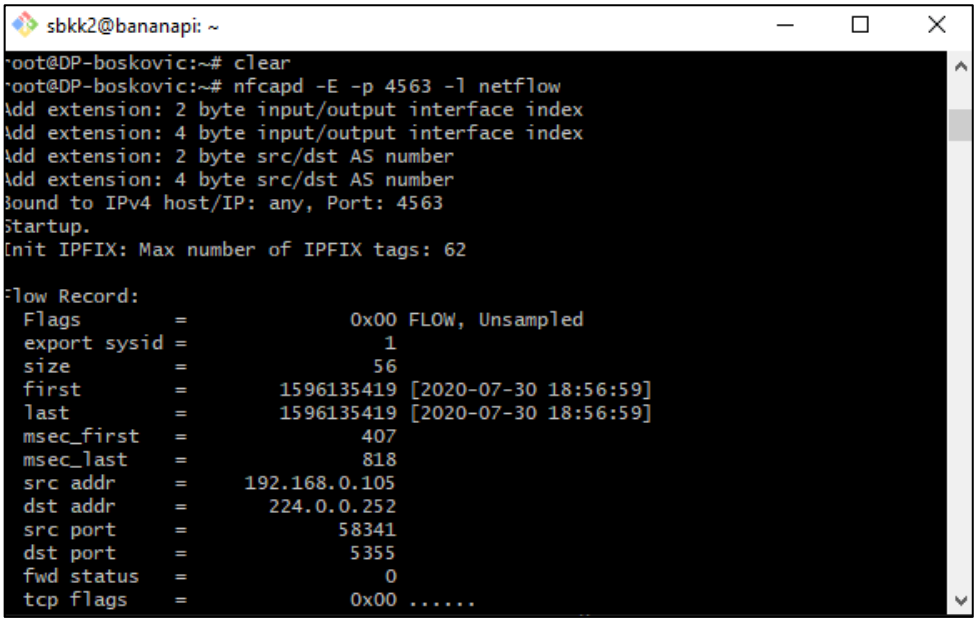
Obrázek č. 40 - Zachycené soubory v testu č. 3



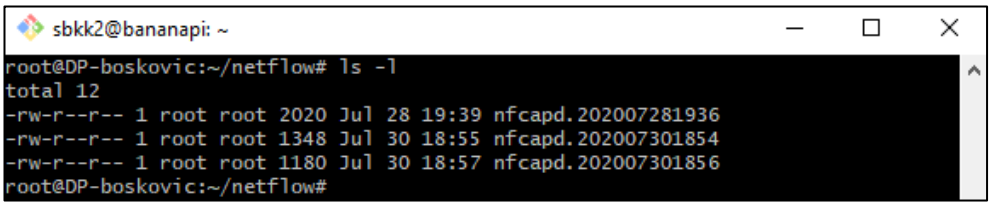
Obrázek č. 41 - Velikosti přenesených souborů v testu č. 3

V první testu byl na vzdáleném zařízení, na portu č. 4563 zapnut kolektor nfcapd, který zachytával emitované Netflow ze sondy. Po dokončení kolekce dat program vygeneruje soubor a uloží jej do složky /netflow v domovském adresáři. Na obrázku č. 40 lze vidět množství přenesených dat ze sondy na vzdálené zařízení (IP adresa 195.178.94.201).

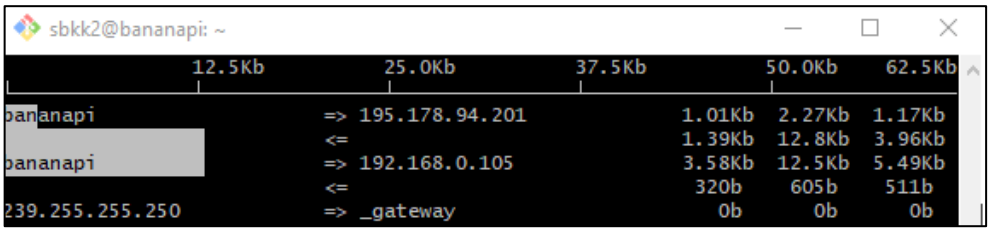
6.6 Druhý test - posílání Netflow na vzdálené zařízení



Obrázek č. 42 - Otevření portu 4563 v testu č. 4



Obrázek č. 43 - Zachycené soubory v testu č. 4



Obrázek č. 44 - Velikosti přenesených souborů v testu č. 4

Oba testy zasílání Netflow dopadly stejně. V obou případech bylo na serveru úspěšně zachyceno odeslání komunikace ze sondy. Lze tedy říci, že je možné zařízení použít i na rozlehlejší sítě pro zkoumání a analýzu bezpečnostních incidentů. Po správném nakonfigurování je zařízení schopno samostatně pracovat (zachytávat pcap soubory, nebo zasílat Netflow na vzdálené zařízení). I zde se ovšem mohou vyskytnout různé komplikace s řešením, které bylo implementováno. Nejedná se ovšem o chyby, které by nějak zásadně omezovaly chod zařízení na síti. V poslední části bude provedeno hodnocení implementovaného návrhu.

7 ZHODNOCENÍ NÁVRHU

V předchozích částech bylo popsáno, jakým způsobem probíhá konfigurace a následné nasazení zařízení do reálného provozu. Implementované funkce byly následně otestovány v předešlé částí. Podle výsledků testů lze vyvodit, že zařízení funguje v reálných podmínkách, ovšem i zde lze najít komplikace, které se vyskytly při vývoji a testování požadovaných funkcí.

V prvním kroku bylo nastaveno SSH pro vzdálené ovládání zařízení. Na obou zařízeních bylo nutno mít zapnutého SSH klienta. Dále byly vygenerovány na vzdáleném zařízení pomocí příkazu „*ssh-keygen*“ dva klíče, jeden veřejný a druhý soukromý. Veřejný klíč se umístil do adresáře „*/.ssh/authorized_keys“*. V konfiguračním souboru SSH bylo pro povolení přihlašování bez hesla nutno vypnout „*PasswordAuthentication*“. SSH bylo při vývoji mnohokrát použito a nebyla zde nalezena žádná komplikace.

Pro síťovou analýzu byl vytvořen skript a konfigurační soubor. Oba soubory šlo vzdáleně modifikovat pomocí přístupu přes SSH, nebo přímo v zařízení. Při testování nebyly nalezeny žádné problémy, které by se týkaly konfiguračního souboru, nebo skriptu. Je ovšem jisté, že pokud by byl konfigurační soubor nastaven špatně (tj. špatná IP adresa, nebo neexistující lokace na disku), tak by skript nefungoval správně.

Pro připojení k OpenVPN bylo nutno zrušit ruční zadávání hesla. Do souboru *sudoers.tmp* v adresáři */etc* byly přidány všechny programy, u kterých bylo zrušeno zadávání hesla. Samostatné spouštění skriptů obstarával plánovací nástroj crontab. V jednom z případů se stalo, že po restartu zařízení se uvedené hodnoty smazaly a bylo nutno je znova zadat.

Při testování implementovaných funkcí bylo jakožto vzdálené zařízení využito serveru UTB, na který se zasílala, nebo emitovala data. Při zasílání Netflow byl pro ukázku manuálně zapnut kolektor nfcapd na vzdáleném serveru. Po nasazení na jakoukoliv další síť, se již bude kolektor dat zapínat automaticky.

ZÁVĚR

Cílem diplomové práce bylo vytvořit sondu, která je schopná samostatně pracovat v internetové síti. V úvodu byly uvedeny omezující vlastnosti a také funkční požadavky, které by měla sonda poskytovat.

Další část teoretické práce se zaměřovala na vysvětlení přínosu síťových analyzátorů pro řešení bezpečnostních, nebo i jiných problémů, které na síti mohou vznikat. Bylo taktéž vysvětleno, k čemu slouží Netflow a pro jaké účely se vyplatí jej shromažďovat. V poslední části teoretické stránky byly uvedeny základní nástroje, které byly poté použity pro realizaci praktické částí diplomové práce.

Praktická část se věnovala především implementaci funkcí, které byly popsány v části teoretické. V úvodu bylo uvedeno, jakou velikost paměti si alokuje program pro zachytávání síťových paketů v závislosti na čase. Jelikož je velikost paměti zařízení omezená, mohly by zde vznikat problémy s časově náročnější analýzou.

Funkční řešení je uvedeno na obrázku č. 13. Je zde graficky vyobrazeno blokové schéma, kterým se sonda při síťové analýze řídí. Bylo popsáno, jakým způsobem probíhá nastavení OpenVPN a také konfigurace pro připojení pomocí SSH ze vzdáleného zařízení k sondě. Bylo ukázáno, jakým způsobem probíhá přenesení veřejných klíčů a jejich překopírování do potřebného souboru.

V posledním bodě bylo zařízení zapojeno do reálného provozu, kde byla následně ověřena funkčnost implementovaných funkcí. Bylo ověřeno, že zařízení dokáže v dané síti samostatně pracovat. V průběhu jednotlivých testů nedošlo v žádném z případů k nečekanému vypnutí, nebo zaseknutí sondy. Dá se tedy říci, že sonda je schopna spolehlivého provozu na síti. Při posílání Netflow byl z důvodu ukázky funkčnosti manuálně zapnout na vzdáleném zařízení kolektor dat. Lze tedy říci, že všechny funkcionality, tedy připojení k OpenVPN, zapnutí skriptu pro síťovou analýzu, zachycení dat a také přenos souborů pomocí SSH, se úspěšně podařilo automatizovat.

SEZNAM POUŽITÉ LITERATURY

[1] Banana Pi. *Wikipedia* [online]. San Francisco: Wikimedia Foundation, 2020 [cit. 2020-02-05]. Dostupné z: https://en.wikipedia.org/wiki/Banana_Pi

[2] Banana Pi BPI-M1. *Wikipedia* [online]. San Francisco: Wikimedia Foundation, 2020 [cit. 2020-02-05]. Dostupné z: http://wiki.banana-pi.org/Banana_Pi_BPI-M1

[3] Armbian. *Wikipedia* [online]. Slovinsko: Prima produkcija, 2020 [cit. 2020-02-05]. Dostupné z: https://www.armbian.com/

[4] MITCHELL, Robin. *Understanding the Differences Between ARM and x86 Processing Cores* [online]. 2017 [cit. 2020-04-10]. Dostupné z: https://www.allaboutcircuits.com/news/understanding-the-differences-between-arm-and-x86-cores/

[5] OREBAUGH, Angela. *Wireshark a Ethereal: kompletní průvodce analýzou a diagnostikou sítí*. Brno: Computer Press, 2008. ISBN 978-80-251-2048-4.

[6] *Wireshark* [online]. [cit. 2020-04-10]. Dostupné z: https://www.wireshark.org/docs/wsug_html/#ChIntroWhatIs

[7] EVSEEV, Alexey. *Listen wifi with wireshark* [online]. 2015 [cit. 2020-04-10]. Dostupné z: http://www.lexev.org/en/2015/listen-wifi-with-wireshark/

[8] SUNNY, Hoi. *How To Detect Nmap SMB Brute-Force Attack Using Wireshark* [online]. 2019 [cit. 2020-06-15]. Dostupné z: https://www.1337pwn.com/how-to-detect-nmap-smb-brute-force-attack-using-wireshark/

[9] *DoS and DDoS Attacks: How They're Executed, Detected, and Prevented* [online]. [cit. 2020-06-15]. Dostupné z: https://thecybersecurityman.com/2018/03/05/dos-and-ddos-attacks-how-theyre-executed-detected-and-prevented/

[10] *Introduction to Cisco IOS NetFlow - A Technical Overview* [online]. Corporate Headquarters 170 West Tasman Dr., 2012 [cit. 2020-06-15]. Dostupné z: https://www.cisco.com/c/en/us/products/collateral/ios-nx-os-software/ios-netflow/prod_white_paper0900aecd80406232.html

[11] *Cisco Netflow Collection Engine: NetFlow Services Solutions Guide* [online]. Corporate Headquarters 170 West Tasman Dr., 2011 [cit. 2020-06-25]. Dostupné z: https://www.cisco.com/en/US/technologies/tk648/tk362/technologies_white_paper09186a00800a3db9.html

[12] *Srovnání VPN Protokolů: PPTP vs. L2TP vs. OpenVPN vs. SSTP vs. IKEv2* [online]. [cit. 2020-07-15]. Dostupné z: https://cs.vpnmentor.com/blog/srovnani-vpn-protokolu-pptp-vs-l2tp-vs-openvpn-vs-sstp-vs-ikev2/

[13] HLADÍK, Radek. *OpenVPN – VPN jednoduše* [online]. Praha 6, 11. 10. 2004 [cit. 2020-07-15]. Dostupné z: https://www.root.cz/clanky/openvpn-vpn-jednoduse/

[14] AMAN, L. *How Does SSH Work: What is SSH* [online]. 2020 [cit. 2020-08-04]. Dostupné z: https://www.hostinger.com/tutorials/ssh-tutorial-how-does-ssh-work

[15] *SSH – bezpečné používání vzdáleného počítače a kopírování dat* [online]. [cit. 2020-08-04]. Dostupné z: https://www.dsl.cz/jak-na-to/jak-na-ssh

[16] YLONEN, T., LONVICK, Chris, ed. *The Secure Shell (SSH) Authentication Protocol* [online]. Helsinki, 2006 [cit. 2020-08-10]. Dostupné z: https://www.ietf.org/rfc/rfc4252.txt

[17] KRČMÁŘ, Petr. *Jak se přihlašovat na SSH bez zadávání hesla* [online]. Praha 6, 15.4.2010 [cit. 2020-08-04]. Dostupné z: https://www.root.cz/clanky/jak-se-prihlasovat-na-ssh-bez-zadavani-hesla/

[18] MALONE, Mike. *If you're not using SSH certificates you're doing SSH wrong* [online]. 11.9.2019 [cit. 2020-08-10]. Dostupné z: https://smallstep.com/blog/use-ssh-certificates/

[19] *ManageEngine NetFlow Analyzer* [online]. California [cit. 2020-08-10]. Dostupné z: https://www.manageengine.com/products/netflow/index-new.html

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

IP INTERNET PROTOCOL

DDOS DISTRIBUTED DENIAL OF SERVICE

HTTP HYPERTEXT TRANSFER PROTOCOL

SSH SECURE SHELL

VPN VIRTUAL PRIVATE NETWORK

SEZNAM OBRÁZKŮ

SEZNAM PŘÍLOH