VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

Fakulta elektrotechniky
a komunikačních technologií

DIPLOMOVÁ PRÁCE

Brno, 2021 Bc. David Hirš

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ
FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION

ÚSTAV TELEKOMUNIKACÍ
DEPARTMENT OF TELECOMMUNICATIONS

SYSTÉM PREVENCE PRŮNIKŮ VYUŽÍVAJÍCÍ RASPBERRY PI
INTRUSION PREVENTION SYSTEM BASED ON RASPBERRY PI

DIPLOMOVÁ PRÁCE
MASTER'S THESIS

AUTOR PRÁCE — **Bc. David Hirš**
AUTHOR

VEDOUCÍ PRÁCE — **Ing. Zdeněk Martinásek, Ph.D.**
SUPERVISOR

BRNO 2021

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ

Diplomová práce

magisterský navazující studijní program **Informační bezpečnost**

Ústav telekomunikací

Student: Bc. David Hirš ***ID:*** 195151
Ročník: 2 ***Akademický rok:*** 2020/21

NÁZEV TÉMATU:

Systém prevence průniků využívající Raspberry Pi

POKYNY PRO VYPRACOVÁNÍ:

Hlavním cílem práce je návrh a implementace různých detekčních a prevenčích metod kybernetických útoků do sondy využívající platformu Raspberry Pi. V teoretické části prostudujte současný stav problematiky detekce kybernetických útoků na L2/L3 vrstvách a možnost jejich mitigace (prevence). Analyzujte možnosti detekce na základě vzorů a anomálií, které je možné implementovat a provozovat na výpočetně omezeném zařízení současně. Různé metody porovnejte z pohledu hardwarových požadavků a možné kooperace. Z výsledků analýzy vyberte nejméně 10 kybernetických útoků a pro jejich detekci naimplementujte mechanizmus. Detekční a následující prevenčí mechanismus musí být aktivní a plně automatizovaný bez zásahu uživatele, což představuje vlastní přínos práce. Navrhněte a implementujte programové vybavení umožňující správu detekčních mechanizmů. Výsledné řešení otestujte na experimentálním pracovišti.

DOPORUČENÁ LITERATURA:

[1] PFLEEGER, Charles P.; PFLEEGER, Shari Lawrence. Analyzing computer security: a threat/vulnerability/countermeasure approach. Prentice Hall Professional, 2012.

[2] GARCIA-TEODORO, Pedro, et al. Anomaly-based network intrusion detection: Techniques, systems and challenges. computers & security, 2009, 28.1-2: 18-28.

Termín zadání: 1.2.2021 ***Termín odevzdání:*** 24.5.2021

Vedoucí práce: Ing. Zdeněk Martinásek, Ph.D.
Konzultant: Leoš Jiřík (AŽD Praha s.r.o.)

doc. Ing. Jan Hajný, Ph.D.
předseda rady studijního programu

ABSTRAKT

Počet objevených zranitelností prudce stoupá. Například v roce 2019 bylo objeveno 20 362 zranitelností. Pravděpodobnost realizace kybernetických útoků je tedy vysoká. Z toho důvodu je nutné navrhnout a implementovat automatizované a levné systémy prevence či detekce narušení (IPS/IDS). Tato implementace se může zaměřit na domácí či malé firemní sítě. Hlavním cílem systému je detekovat nebo zmírnit dopad kybernetických útoků v co nejkratším čase. Diplomová práce navrhuje IPS/IDS založené na Raspberry Pi, které dokážou detekovat a předcházet různým kybernetickým útokům.
Obsah této práce je zaměřen na popis kybernetických útoků založených na linkové a síťové vrstvě referenčního modelu ISO/OSI. Dále je zde popis systémů IPS/IDS a jejich zástupců nabízející otevřený kód. Praktická část je zaměřena na experimentální pracoviště, hardwarové nároky vybraných detekčních systémů, scénáře kybernetických útoků a vlastní implementaci programu detekce. Program detekce je založen na těchto vybraných systémech a spojuje je do jednoho celku umožňující jejich snazší správu.

KLÍČOVÁ SLOVA

IDS, IPS, Raspberry Pi 4, kybernetické útoky

ABSTRACT

The number of discovered vulnerabilities rapidly increases. For example in 2019 there were discovered 20 362 vulnerabilities. The probability of cyber-attacks realization is high. Therefore it is necessary to propose and implement automated and low-cost Intrusion Prevention or Intrusion Detection Systems (IPS/IDS). This implemetation can focus on home use or small corporate networks. The main goal of the system is to detect or mitigate cyber-attack impact as fast as possible. The master's thesis proposes IPS/IDS based on Raspberry Pi that can detect and prevent various cyber-attacks.
Contents of this thesis are focus on description of cyber-attacks based on ISO/OSI model's Link and Network layers. Then there is description of IPS/IDS systems and theirs open source representatives. The practical part is focus on experimental workspace, hardware consumption of choosen detection systems, cyber-attacks scenarios and own implementation of detection program. Detection program is based on these chosen systems and puts them together to be easily manageable.

KEYWORDS

IDS, IPS, Raspberry Pi 4, cyber-attacks

HIRŠ, David. *Systém prevence průniků využívající Raspberry Pi*. Brno, 2021, 79 s. Diplomová práce. Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, Ústav telekomunikací. Vedoucí práce: Ing. Zdeněk Martinásek, Ph.D.

PROHLÁŠENÍ

Prohlašuji, že svou diplomovou práci na téma „Systém prevence průniků využívající Raspberry Pi“ jsem vypracoval samostatně pod vedením vedoucího diplomové práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou všechny citovány v práci a uvedeny v seznamu literatury na konci práce.

Jako autor uvedené diplomové práce dále prohlašuji, že v souvislosti s vytvořením této diplomové práce jsem neporušil autorská práva třetích osob, zejména jsem nezasáhl nedovoleným způsobem do cizích autorských práv osobnostních a/nebo majetkových a jsem si plně vědom následků porušení ustanovení § 11 a následujících autorského zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů, včetně možných trestněprávních důsledků vyplývajících z ustanovení části druhé, hlavy VI. díl 4 Trestního zákoníku č. 40/2009 Sb.

Brno ....

podpis autora

PODĚKOVÁNÍ

Rád bych poděkoval vedoucímu diplomové práce panu Ing. Zdeňku Martináskovi, Ph.D. za odborné vedení, konzultace, trpělivost a podnětné návrhy k práci.

Obsah

Seznam obrázků

Seznam tabulek

Úvod

Informační systémů dosahují hojného zastoupení napříč různými odvětvími. Přínos informačních systémů společnosti je bezpochyby nepopiratelný, avšak přináší i určitá rizika z pohledu kybernetické bezpečnosti. Kybernetické útoky mohou cílit na odepření služeb, odposlouchávání dat, jejich úprava nebo i ovládnutí uživatelova zařízení. Tato rizika existují ve veřejné, pracovní i domácí síti s cílem odcizit uživatelova aktiva či poškodit poskytovanou službu. Proti těmto hrozbám je nutné se bránit či alespoň snížit jejich dopad. Protiopatření proti kybernetickým útokům získává na důležitosti především kvůli automatizaci útoků a snížení složitosti při jejich provedení. Útočník nadále nemusí disponovat množstvím znalostí potřebných k realizaci kybernetického útoku. V některých situacích je použití běžného firewallu nedostačující a vznikají automatizované systémy detekce a prevence těchto útoků. Jedná se o systémy IDS (Intrusion Detection System) a IPS (Intrusion Prevention System). Jejich použití není široce rozšířené, avšak jedná se o systémy jejichž užívání snižuje dopad rostoucího počtu kybernetických útoků.

Hlavním cílem diplomové práce je vlastní návrh a implementace detektoru kybernetických útoků využívající výpočetně omezené zařízení Raspberry Pi 4 typ B. Jedná se o detektor jehož cílem je zabezpečit malé firemní sítě. Cílem teoretické části práce je zhodnocení současné problematiky kybernetických útoků zaměřených na linkovou a síťovou vrstvu referenčního modelu ISO/OSI a způsoby jejich detekce a mitigace. Tento cíl je dělen na popis kybernetických útoků, jejich detekce, mitigace a dále popis systémů sloužících k automatizované detekci kybernetických útoků. Vybrané kybernetické útoky lze realizovat v bezdrátových i kabelových sítích. Popis systémů automatizované detekce také obsahuje přehled současných systémů, ze kterých jsou vybrány konkrétní systémy pro realizaci praktické části diplomové práce. Cílem praktické realizace diplomové práce je vlastní návrh a implementace detektoru kybernetických útoků, který umožní detekci a prevenci nejméně deseti vybraných útoků. Ke splnění tohoto cíle je nutná tvorba experimentálního pracoviště, jehož účelem je testování hardwarových nároků vybraných systémů detekce a testování vlastní implementace detektoru. Pro testování detekčních schopností implementovaného detektoru je vytvořeno deset scénářů kybernetických útoků. Vlastní implementaci programu detektoru předchází jeho návrh spolu s vývojovým diagramem. Implementovaný program detektoru je testován dle vytvořených scénářů a dosažené výsledky detekce a prevence kybernetických útoků jsou dále popsány.

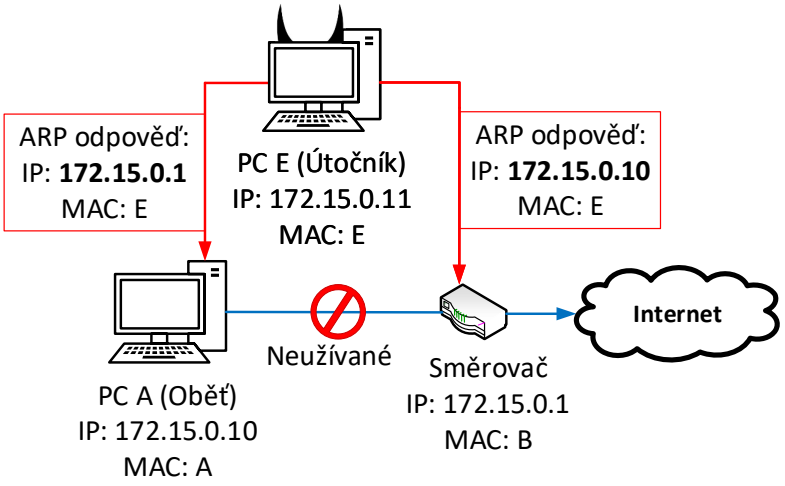
1 Analýza kybernetických útoků L2-L3

Následující text analyzuje kybernetické útoky, které jsou realizovány na vrstvách L2 až L3 modelu ISO/OSI [1]. Vytvořená analýza se zaměřuje výhradně na útoky, které je možné detekovat na základě vytvořených vzorů (detekce využívající signatury). Text také obsahuje metody protiopatření jednotlivých útoků. Popsané útoky jsou zaměřené na kabelové i bezdrátové sítě a jejich provedení lze v lokálních sítích převážně snadno uskutečnit. Jako součást diplomové práce vznikl vlastní článek analyzující současný stav kybernetických útoků [2].

1.1 Podvržení ARP zpráv

Protokol ARP (Address Resolution Protocol) slouží k získání linkové adresy síťového rozhraní (MAC - Media Access Control) příjemce ve stejné podsíti pomocí známé IP (Internet Protocol) adresy [3]. ARP nedisponuje bezpečnostním mechanismem (př. kontrola autentičnosti), a proto jeho všesměrové dotazy a odpovědi může kdokoli podvrhnout (útok ARP spoofing/poisoning). Útočník tímto způsobem získá přístup k datům uživatele, který je nevědomky odesílá útočníkovi.

Útoky založené na napadení ARP protokolu modifikují nebo vytváří falešné ARP zprávy (požadavky a odpovědi). Takto dochází k přesměrování komunikace uvnitř sítě LAN (Local Area Network) [4]. Útočník se může vydávat za zařízení s hledanou IP adresou a přesvědčit tak odesílatele, že on je hledaným příjemcem. Útočník toho může docílit dvojím způsobem, a to odesíláním ARP dotazu, nebo ARP odpovědi. Tyto podvržené zprávy musí být útočníkem periodicky odesílány, jinak dochází k samovolnému opravení ARP tabulky pomocí nepodvržených ARP zpráv v LAN. V případě, kdy útočník „otráví“ ARP tabulku obou uživatelů, veškerá jejich komunikace probíhá přes něj a stává se tak snadno čitelnou či modifikovatelnou. Výsledkem je realizace MitM (Man in the Middle). Schéma útoku MitM využívající otravu ARP tabulky je uveden na obrázku 1.1. Komunikující strany jsou označeny jako Oběť, Směrovač a Útočník. Útočník periodicky vysílá podvrženou ARP odpověď Oběti i Směrovači (označují červené šipky), čímž dosahuje MitM. Další případ představuje „otrávení“ ARP tabulky jednostranně (přesměrování pouze jednoho směru komunikace), například přesměrování Oběti na vlastní webový server. Útočník „otráví“ jen ARP tabulku Oběti a útok je označován jako „Host impersonation attack“. Dalším možným použitím tohoto útoku je realizace odepření služby. V tomto případě, útočník cíleně zahazuje datovou komunikaci uživatele pro specifickou službou, dopadem je že daná služba je pro uživatele nedostupná. Obecně jsou takovéto útoky označovány jako útoky cílené na odepření služeb (DoS - Denial of Service).



Obr. 1.1: Provedení MitM a následný odposlech či změna procházejících dat.

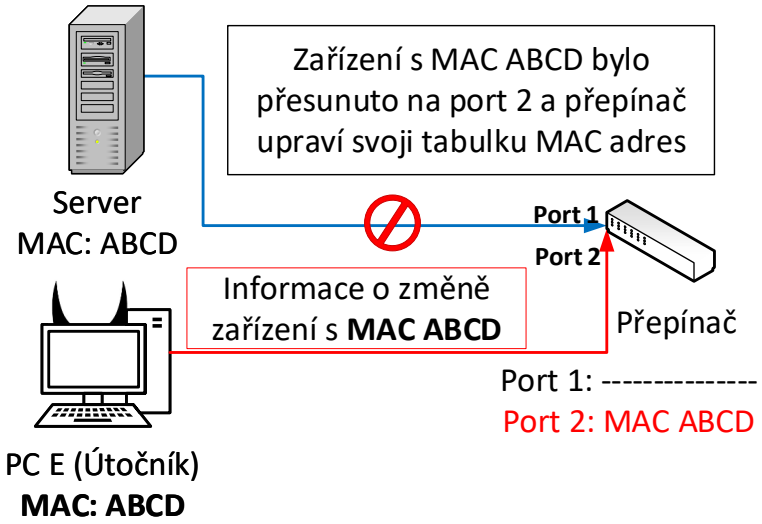
Protiopatření má za cíl zabránit modifikovanému ARP požadavku průchod sítí LAN. Lze využit bezpečnostní funkci síťových přepínačů nazývanou DHCP (Dynamic Host Configuration Protocol) Snooping [5]. Tato funkce primárně zabezpečuje protokol DHCP tím, že zahazuje DHCP rámce, které přichází od nedůvěryhodných DHCP serverů. DHCP Snooping může pomoci i při detekci modifikovaných ARP zpráv. Vytváří tzv. DHCP Snooping Binding table, což je tabulka obsahující svázané IP a MAC adresy jednotlivých zařízení v síti LAN, které byly přiřazeny důvěryhodným DHCP serverem. Dynamickou kontrolu ARP požadavků obstarává Dynamic ARP Inspection a jejich obsah porovnává s vytvořenou DHCP Snooping Binding table. Pokud obsah požadavku nesouhlasí, dochází k jeho zahození. Dynamic ARP Inspection pro kontrolu svázaných adres může využít také statickou tabulku, která je manuálně nakonfigurovaná. Manuální konfigurace je však časově náročná úloha a nevhodné řešení při středních a velkých sítích.

Další možnou formou protiopatření je úprava samotného ARP protokolu a vytvoření zabezpečeného S-ARP (Secure Address Resolution Protocol). Tento navržený protokol a bezpečnostní přístup byl představen v článku [6] roku 2003. Protokol S-ARP zajišťuje autentizaci zpráv za pomocí asymetrické kryptografie a infrastruktury veřejných klíčů PKI (Public Key Infrastructure). Veškerá zařízení v síti LAN disponují vlastním veřejným i soukromým klíčem a certifikátem pro ověření jejich identity. Identitu představuje IP adresa. Certifikát také obsahuje IP a MAC adresu důvěryhodné stanice, která představuje AKD (Authoritative Key Distributor), neboli certifikační autoritu distribuující klíče pro tento protokol. Odpověď na ARP požadavek je podepsána soukromým klíčem odpovídajícího uživatele. Dotazující se stanice ověří podpis veřejným klíčem uživatele obsaženým uvnitř jeho certifikátu. Pokud certifikát neobsahuje veřejný klíč, je vyžádán od AKD. Odpovědi AKD jsou

také podepsané. Pokud se podpis neshoduje, ARP odpověď je zahozena. Tvorbu digitálního podpis zajišťuje algoritmus DSA (Digital Signature Algorithm). Možnou hrozbu představuje Reply attack, avšak tomu je zamezeno pomocí časového údaje (razítka). Časové razítko distribuuje AKD a všechny stanice uvnitř sítě musí být časově synchronizovány.

1.2 Podvržení linkové adresy

Tyto útoky využívají možnosti snadného podvržení linkové adresy (MAC Address spoofing) a tím pádem se útočník vydává za někoho jiného. MAC adresa je teoreticky jedinečný identifikátor zařízení na L2 vrstvě, na jejímž základě lze doručit data od odesílatele k příjemci v LAN. Na základě tohoto chybného předpokladu, existence unikátního identifikátoru lze také řídit přístup do sítě LAN pomocí funkce filtrování na základě linkových adres (router má aktivovanou funkci MAC filtering). Tímto způsobem dojde k odepření přístupu do sítě zařízením, která nejsou uvedena v seznamu [7]. Toto zabezpečení lze jednoduše obejít právě pomocí útoku, který podvrhne linkovou adresu legitimního uživatele služby. Útočník nejprve odhalí MAC adresu legitimního uživatele s povoleným přístupem a to za pomoci softwarového nástroje např. Wireshark. V druhém kroku si útočník změní MAC adresu a vydává se za legitiního uživatele. Prakticky všechny operační systémy umožňují změnu MAC adesy. Podvržení linkové adresy lze také využít k provedení útoku na odepření služby. Útočník se vydává za stanici uvnitř sítě, ke které legitimní uživatelé hodlají přistoupit a daný požadavek o přístup zahodí [8]. Průběh útoku graficky znázorňuje obr. 1.2. Zde je červenou šipkou znázorněno odeslání informace o změně zařízení s MAC adresou ABCD, tedy adresou patřící Serveru.



Obr. 1.2: Princip útoku podvržením linkové adresy.

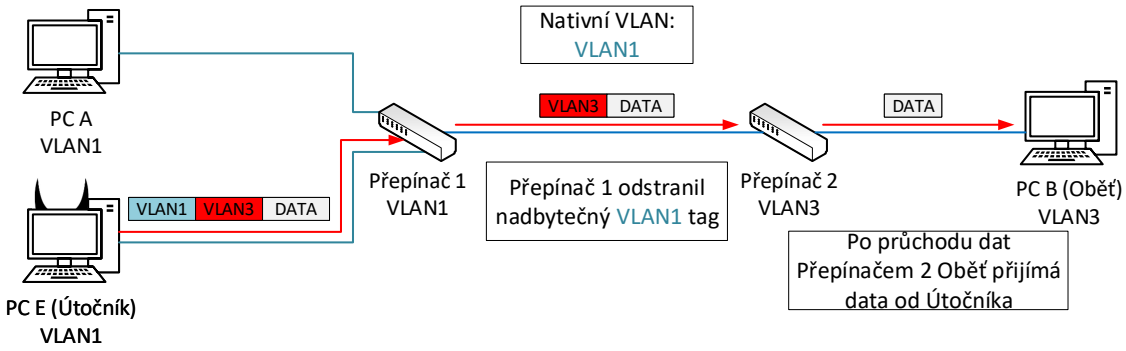
Protiopatřením je opět DHCP Snooping [5]. Tato funkce byla popsána v předešlé části 1.1, a proto již nebude znovu představena. Jediným rozdílem je funkce IP Source Guard, která zde nahrazuje Dynamic ARP Inspection. Pro odhalení MAC address spoofing je nutné kontrolovat a porovnávat všechny přijímané rámce obsahující MAC adresu s DHCP Snooping Binding table. IP Source Guard kontroluje IP i MAC adresy. Podvržení linkové adresy lze zabránit i pomocí „odlehčených autentizačních agentů“, jak popisuje práce [9]. Zabezpečení pro celou síť LAN nastavuje autentizační server a přístup do této sítě je povolen pouze s validním agentem na klientském zařízení.

1.3 Přeskakování virtuální LAN

VLAN (Virtual Local Area Network) představuje virtuální lokální síť [10]. LAN je takto rozdělena do více VLAN, které logicky rozdělují síť a zařízení uvnitř. Komunikace dvou zařízení uvnitř různých VLAN je zakázaná a přepínač uvnitř sítě tyto pakety zahazují. Kybernetický útok označovaný jako přeskakování VLAN (VLAN hopping) má za cíl oklamání přepínače v síti tak, aby útočník získal přístup do jiné VLAN, než do které sám přísluší. Přístupem je myšlena komunikace se zařízením jiné VLAN [11, 12].

Princip útoku využívajícího přidání druhé značky (Double tagging) [11, 12], zobrazuje obrázek 1.3. Útočník chce odeslat data do *VLAN 3*, která je za běžných podmínek nedosažitelná. Pokud by datové rámce poslal pouze se značkou *VLAN 3* (802.1Q *tag*), přepínač by je ihned zahodil. Z tohoto důvodu útočník přidá k datovým rámcům ještě jednu značku, datové rámce tak mají dvě značky *VLAN 1* (povolená) a *VLAN 3* (nepovolená). První, přepínačem kontrolovaná značka, bude platný pro útočníkovi příslušnou *VLAN 1* a to způsobí předání rámce dál a odstranění značky. Rámec ale stále nese druhou značku, která ukazuje na cílovou VLAN označenou *VLAN 3*. Následující přepínač detekuje značku nesoucí hodnotu *VLAN 3* a rámec předá do cílené *VLAN 3*. Pro tento útok je klíčové, aby cesta k cílovému uživateli vedla alespoň přes dva přepínače. Dalším požadavkem je, aby značka označující VLAN útočníka a nativní VLAN přepínače byla nastavena na stejnou VLAN, v tomto případě *VLAN 1*. Pokud jsou obě hodnoty stejné, přepínač vyhodnotí značku jako nadbytečnou, a proto dochází k jejímu odstranění. Útočník je v tomto případě značně omezený, protože data může skrze síť jen odesílat, a tak může přikročit například k DoS útoku. Obrázek znázorňuje předání útočníkem generovaná data skrze dva přepínače, které odstraní jim příslušnou značku.

Druhým útokem patřícím do kategorie přeskakování virtuální LAN je podvržení přepínače (Switch spoofing) [11]. Útočník se vydává za přepínač a sjednává přenosy, což mu umožní přijímat a přeposílat rámce mezi odlišnými VLAN. Rámce DTP



Obr. 1.3: Průchod rámce do nepřístupné VLAN pomocí Double tagging útoku.

(Dynamic Trunking Protocol) slouží pro určení módu, ve kterém bude probíhat přenos rámců mezi dvěma sousedními přepínači. Útočník odešle DTP rámce přepínači a snaží se jej přesvědčit, že je novým přepínačem v síti. Pokud je přesvědčovaný přepínač v módu *Dynamic Auto, Dynamic Desirable, Trunk*, schválí útočníka jako nový přepínač a naváže s ním spojení. Útočník nyní, nehledě na vlastní příslušnost určité VLAN, může odesílat rámce do kterékoliv VLAN. V takovémto případě je možné vytvořit spojení s „Obětí“, a komunikovat bez zabezpečovacích protokolů vyšší, 3. vrstvy ISO/OSI. Naopak útok není realizovatelný v případě, kdy je přepínač v módu *Access*, a tedy všechny příchozí DTP rámce sousedních přepínačů zahazuje.

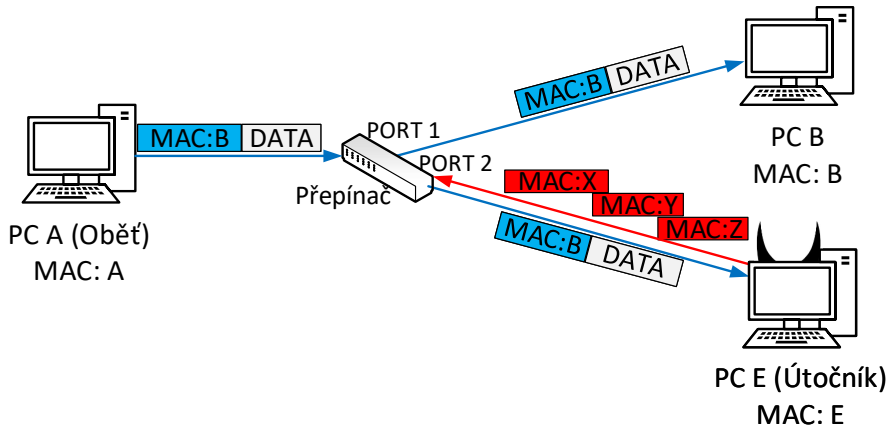
Protiopatření proti výše popsanému útoku lze realizovat definováním nepoužívané VLAN a její přiřazení jako nativní pro všechny přenosové cesty mezi přepínači [12, 13]. Toto nastavení způsobí, že všechny přepínače budou brát nativní značku nepoužívané VLAN. Útočník tak nemůže provést **Double tagging**, protože přepínač nevyhodnotí jeho *tag* jako redundantní. Další možností je změna protokolu používající *tag*, například na protokol ISL (InterSwitch Link Protocol) [12].

Protiopatření proti **Switch spoofing** již bylo zmíněno v popisu útoku. Nejsnazší možností je zamezení dynamickému ustanovení přepínačů skrze DTP a nastavit jejich mód na *access*.

1.4 Zahlcení směrovací tabulky CAM

CAM (Content Addressable Memory) je fyzická paměť přepínače obsahující stejnojmennou tabulku, na základě které přepínač přepíná datovou komunikaci [13]. Tato tabulka obsahuje svázané MAC adresy koncových zařízení s příslušnými fyzickými porty přepínače, na které jsou stanice připojena. Přepínač zpracovává příchozí rámce podle cílové MAC adresy obsažené v hlavičce datového rámce a to porovnáním s údaji obsažené v CAM tabulce a následným přepnutím rámce na cílový port. Každé nově připojené zařízení k portu přepínače je dynamicky přidáno do tabulky.

Útok cílený na zahlcení tabulky CAM (CAM overflow/MAC flooding) je realizován následujícím způsobem. Útočník je připojen k přepínači a generuje velké množství falešných MAC adres. Tímto oznamuje přepínači nově připojená zařízení do sítě umístěná na jeho portu. Každé toto oznámení nese jinou MAC adresu a přepínač si ukládá vždy nový záznam do tabulky CAM. Jakmile dojde k „zahlcení“ přepínače záplavou nových záznamů a přepínač nedisponuje již volnou pamětí, musí odstraňovat nejstarší záznamy uložené v CAM tabulce a nahrazovat je novými. Ve stejnou chvíli přechází směrovač do stavu *fail safe mode*, známého také jako *hub mode*. Kvůli přehlcení CAM tabulky dochází k degradaci přepínače na úroveň rozbočovače, přepínač není nadále schopen využívat svoji CAM tabulku a kopíruje veškeré příchozí datové rámce na všechny své porty. Útočník je nyní schopen pasivně odposlouchávat probíhající komunikaci na všech portech přepínače a získává citlivé informace o všech koncových zařízeních nacházejících se uvnitř stejné sítě LAN. Zmíněný útok lze také označit za útok hrubou silou [14]. Průběh útoku je znázorněn na obrázku 1.4, kde PC A a PC B jsou komunikující strany a PC E představuje útočníka. První útočníkův krok, kdy zasílá falešná oznámení o nových zařízeních, je označen červenou šipkou. Následně dochází k degradaci směrovače na rozbočovač. Oběť (PC A) následně odesílá data příjemci (PC B), která přechází skrze všechny porty směrovače (označeno modrou šipkou). Odeslaná data obdrží nejen příjemce (PC B), ale i útočník (PC E).



Obr. 1.4: Zaplavení přepínače a jeho následná degradace na rozbočovač.

Protiopatření může poskytovat rozšíření omezené kapacity CAM a zabránění jejího úplného využití. Toho lze dosáhnout nastavením zabezpečení portů, kdy lze připojit pouze omezené množství zařízení [5, 14]. Například přepínače od společnosti CISCO disponují vlastností nazvanou *Port Security*, pomocí které lze definovat maximální množství zařízení připojených k portům. Tato vlastnost umožňuje vybrat přepínačem realizovanou akci jako odpověď na porušení nastaveného pravidla jednoho z aktivních portů [15]. Na výběr jsou dvě základní reakce.

- **Restrict** - Po dovršení nastaveného limitu dochází k zahazování všech příchozích rámců s neznámou MAC adresou. Rámce nesoucí známou MAC adresu jsou povoleny. Incident je zaznamenán a dochází k vyvolání upozornění pro správce sítě.
- **Shutdown** - Chování stejné jako u předchozí akce, avšak po porušení pravidla je port vypnut a veškerá komunikace je zakázána.

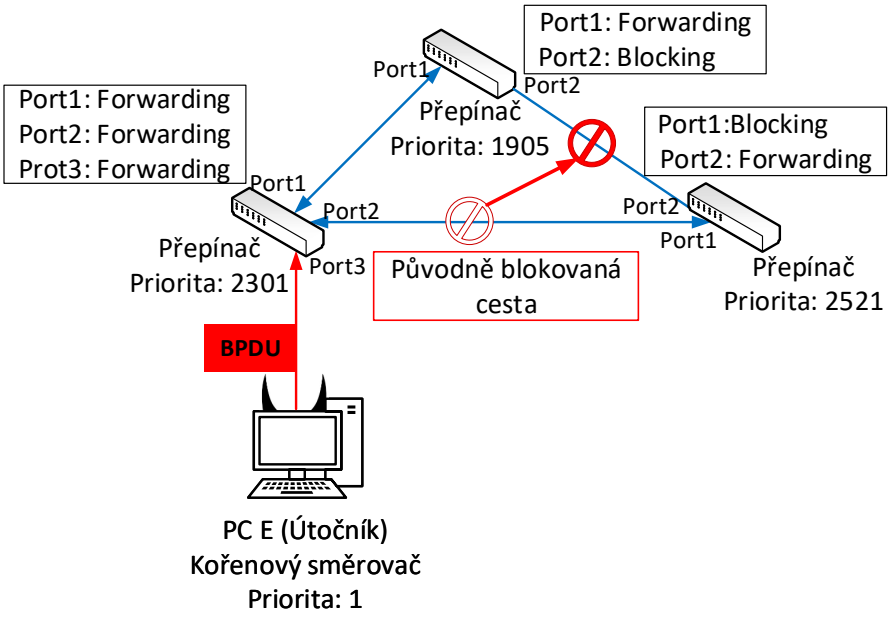
Zmíněného zvýšení kapacity CAM tabulky přepínače lze dosáhnout alokací paměti z fyzického serveru disponujícího velkými paměťovými možnostmi. Přepínač by takto mohl pracovat s CAM tabulkou umístěnou na serveru a v případě útoku by ohrožení oznámil správci sítě, který by mohl na jeho základě patřičně reagovat a provedení útoku zabránit. Ovšem definování zabezpečení portů je snazší, méně nákladné a nevyžaduje okamžitý zásah pověřené osoby.

1.5 Útok na Spanning Tree Protocol

STP (Spanning Tree Protocol) je síťový protokol zamezující tvorbě smyček v topologii sítě [16]. STP protokol neobsahuje opět žádné autentizační metody. Útočník tak může bez problémů odchytit všesměrově vysílaný BPDU (Bridge Protocol Data Unit) rámec a upravit jej za účelem získání nejvyšší priority, což povede k jeho zvolení jako **Root Bridge** a veškerá data budou předávána přes něj.

Nejvyšší prioritu uvnitř BPDU je hodnota 1 [17]. Odeslaný rámec je validní a přepínače útočníka přijmou jako nový **Root Bridge**. Útočník zvolený kořenovým přepínačem takto získá celou síť LAN, nebo konkrétní VLAN. Veškerá data prochází skrze **Root Bridge**, v tomto případě přes útočníka. Ten může rámce zachytávat a upravovat, tedy realizovat MitM. DoS přichází také v úvahu. V takovém případě by útočník blokoval veškeré rámce směřující k určité stanici nebo do konkrétní podsítě. Útočníkem vynucenou změnu **Root Bridge** znázorňuje obrázek 1.5. Zde je červenou šipkou znázorněno odeslání upraveného BPDU rámce. Přepínač dále předal BPDU a útočník byl ostatními přepínači zvolen jako **Root Bridge**. Výsledkem je změna blokované cesty, tedy přepnutí stavu portů u všech přepínačů.

Protiopatřením v tomto případě by mohlo být vypnutí STP, což není doporučováno. Cisco přepínače obsahují připravená protiopatření proti STP útoku [13]. Jedním je BPDU Guard. Hraniční přepínače mají na portech s uživateli nastavený mód PortFast. Tento mód zabraňuje zařízením připojeným k tomuto portu jakýmkoliv způsobem ovlivnit STP topologii. Pokud na port v módu PortFast příjde BPDU, přepínač změní stav na *Disabled*. Následně dojde k vytvoření záznamu o příchozím BPDU, který nepronikne dále do sítě. Druhou možností je Root Guard, která pracuje stejným způsobem a monitoruje port, na kterém pracuje. Pokud příjme BPDU o změně STP topologie, vypne daný port a záznam zanese do logu.



Obr. 1.5: Podvržené BPDU od útočníka.

1.6 Odposlouchávání rámců Linkové vrstvy

Odposlouchávání, neboli Eavesdropping, je pasivním typem útoku. U tohoto typu útoku nedochází k zásahu do obsahu zachycených rámců přenášených sítí LAN nebo vysílání jakkoliv upraveného rámce [18]. Existence útočníka je díky jeho chování velmi obtížně detekovatelná. Výsledkem útoku je získání informací obsažených v rámcích. V případě použití nezabezpečeného komunikačního protokolu lze získat veškerý odesílaný obsah.

Tento útok zasahuje do soukromí a důvěrnosti přenášených dat. Samotný útok lze s těží detekovat kvůli útočníkově pasivnímu přístupu. Pro realizaci útoku však útočník musí provést určité akce a splnit některé požadavky. Jedním z požadavků je jeho přístup do sítě LAN, ve které je i Oběť útoku. Dále je vhodné disponovat nástrojem pro monitorování síťového provozu. Útočníkovi však nejsou dostupná veškerá komunikační data. Všem uživatelům sítě jsou dostupná data odesílaná všesměrově. Další útočníkovou možností je zajistit situaci, kdy skrze něj prochází veškerá data. Tohoto stavu lze dosáhnout pomocí útok mužem uprostřed (MITM). Pokud dochází ke komunikaci přes nezabezpečený protokol Hypertext Transfer Protocol (HTTP), jsou veškerá odesílaná data dostupná v otevřené podobě. Útočník může fyzicky připojit do sítě rozbočovač, který zajistí přeposílání obdržených dat na veškeré své komunikační porty. Pokud je připojení rozbočovače nerealizovatelné, útočník může využít útoku Podvržení ARP zpráv popsaného v kapitole 1.1. Tento útok zajistí požadovaný přístup k odesílaným datům, avšak dojde k prozrazení útočníka.

Detekci tohoto útoku je nutné zaměřit na útočníkovu přípravu a metodu pro zachytávání přenášených dat. V tomto případě je nutné detekovat útok Podvržení ARP zpráv a na základě této detekce lze určit MAC adresu útočníka. Mitigace útoku spočívá v zajištění bezpečnosti dat šifrováním [19]. Tímto způsobem je zajištěn požadavek na důvěrnost dat a soukromí uživatelů.

1.7 Útoky cílené na odepření služeb

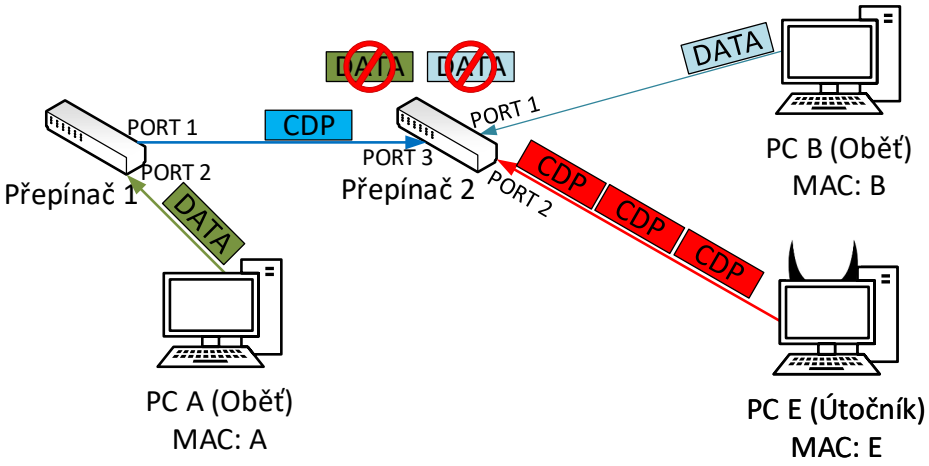
Pro poškození Oběti může útočník zvolit i způsob útoku cílený na odepření služeb, neboli DoS (Denial of Service). Tyto útoky mohou útočit například na poskytovatele aplikačních služeb, nebo na konkrétní prvek v síti. Při tomto útoku dochází většinou k zahlcení Oběti, vyčerpání výpočetního výkonu nebo jiných prostředků tak, že nebude schopna efektivně plnit svoji činnost. Útok DoS je realizovaný jednou stanicí, kdežto DDoS (Distributed Denial of Service) využívá více stanic k realizaci útoku.

1.7.1 Zneužití Cisco Discovery protokolu

Přepínače společnosti CISCO využívají protokol CDP (Cisco Discovery Protocol) pro sdílení informací o přímo připojených zařízeních [20]. CDP rámce jsou odesílané periodicky, na multicast adresu skrze každý port přepínače. Ihned po obdržení prvního CDP rámce si přepínač vytváří tabulku sousedících zařízení. Ve výchozím nastavení přepínačů jsou veškerá data CDP protokolu přenášena v otevřené podobě.

Útočníkovým cílem je upravení CDP zpráv a oznámit přepínači, že bylo připojeno do sítě nové zařízení. Útočník je následně považován za nový přepínač v síti. Přínosem pro útočníka jsou informace o přímo připojených zařízeních.

Cílem zneužití CDP protokolu je realizace DoS útoku a zahlcení sousedních zařízení [21]. Útočník vygeneruje záplavu CDP rámců a zahltí tak přepínač, který již nedokáže zpracovávat příchozí rámce. Uživatelům, jejichž komunikace prochází skrze napadený přepínač, budou veškeré služby nedostupné [22]. Výsledek tohoto útoku nemusí nutně končit jen odepřením služeb. Dle popisu v kapitole 1.4, zahlcený přepínač může být degradován na rozbočovač a následně rozesílá všesměrově veškerou komunikaci. Výsledek tohoto útoku je závislý na verzi operačního systému přepínače [21]. Tento útočníkův přístup způsobí škody pouze na jednom, přímo připojeném zařízení. Pokud by však získal přístup k přepínači, ke kterému jsou připojené další přepínače, rozsah škod bude násobný. Díky všesměrovému přeposílání CDP rámců by bylo možné zaplavit všechny okolní přepínače. Obrázek 1.6 znázorňuje útočníkem realizovaný DoS. Červeně jsou znázorněny útočníkem generované CDP rámce vedoucí k zahlcení přepínače 2. Přepínač 1 odesílá jeden korektní CDP rámec. Oběti (PC A i PC B) následně odesílají data přepínači 2, který je následně zahazuje.



Obr. 1.6: DoS jako výsledek zaplavení CDP rámci.

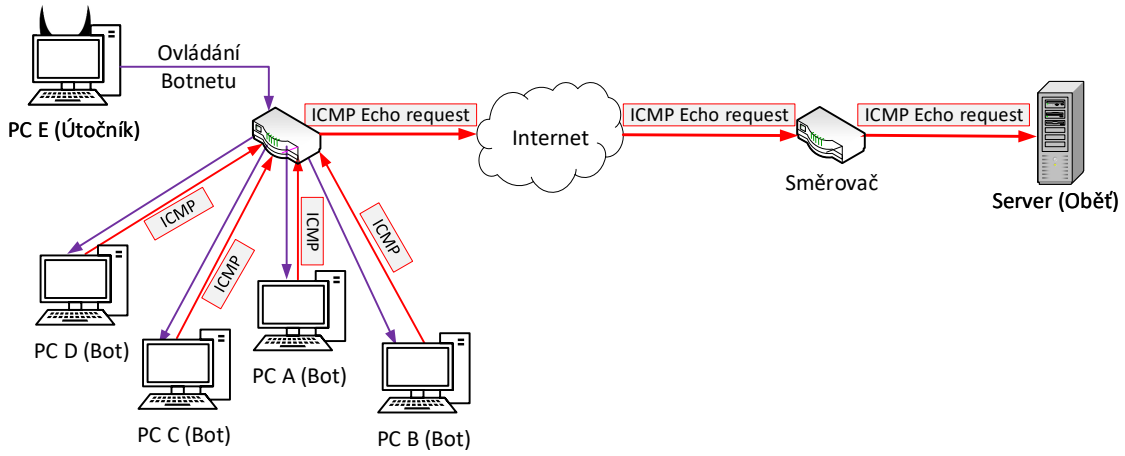
Protiopatření proti zneužití CDP je zakázat používání samotného CDP protokolu na přepínačích CISCO uvnitř sítě LAN [23]. Zakázání protokolu lze nastavit globálně pro všechna zařízení v síti, nebo na konkrétních portech jednoho přepínače. Koncové stanice, připojené na zabezpečený port, nemohou vysílat CDP rámce a ovlivnit tak přepínač. Pokud útočník získá fyzický přístup ke směrovači, může své zařízení přepojit na jiný port přepínače.

1.7.2 Záplava ICMP

Internet Control Message Protocol (ICMP) je protokol sloužící pro oznamování chybových stavů nebo dotazů síťové vrstvy ISO/OSI. Dotaz sestává z požadavku a odpovědi [24]. Útočník může protokol ICMP zneužít např. k zahlcení cílové stanice velkým množstvím PING dotazů. PING slouží jako nástroj pro ověření dostupnosti cílové stanice. Bez hlavičky IP protokolu dosahuje ve výchozím nastavení velikosti 32/64 bajtů. Cílem útoku je tedy vyslat množství ICMP paketů dostatečné k zahlcení Oběti a úspěšně realizovat DoS.

Velikost odeslaného ICMP paketu lze upravit. Útočník je schopný zvolit nejbližší maximálně možnou velikost paketu, což představuje 2^{16} bajtů. V tomto případě se však nejedná o záplavový útok, ale o tak zvaný PING of death, neboli PING smrti [25]. Zaplavit Oběť s využitím jednoho komunikačního uzlu, který útočník vlastní, je velmi obtížné. Přistoupí tedy k využití sítě Botnet, která představuje síť infikovaných zařízení. Takovouto síť má útočník pod kontrolou a využívá ji pro realizaci DDoS (Distributed Denial of Service) útoku. Realizace záplavy pakety ICMP (ICMP Flood) probíhá způsobem, kdy útočník z množství zařízení generuje ICMP pakety (například zmíněný PING). Velkým množstvím těchto paketů se snaží zahltit výpočetní prostředky kterými Oběť disponuje. Pokud je celková propustnost komunikační

linky využita pro přijímání ICMP dotazů a generování ICMP odpovědí, legitimní provoz nemá dostatek prostředků pro správnou funkci. Jedná-li se o službu serveru, ta se stane nedostupnou všem uživatelům snažícím se o přístup. Nastává útočníkem žádané odepření služby. Využití sítě Botnet znázorňuje obrázek 1.7. Zde je fialovou šipkou znázorněno ovládání Botnetu útočníkem. Nemusí se jednat jen o jednu lokální síť, která je infikovaná. Útočník tak může nakládat s více zařízeními napříč mnoha sítím. Každý Bot v síti odesílá ICMP paket, znázorněno červeně. Oběť zahlcená takovýmto množstvím paketů není nadále schopná provozu.



Obr. 1.7: Realizace zaplavení serveru ICMP žádostmi s pomocí Botnetu.

Protiopatření proti útoku záplavou ICMP pakety přináší například nastavení signatury, která představuje frekvenční pravidlo, tedy definovaný počet povolených ICMP zpráv za časový okamžik [26]. Síťové prvky jsou včetně firewallů nastaveny na filtraci ICMP provozu včetně neodpovídání na dotaz PING z důvodu možného použití k zesílení DoS útoku.

1.7.3 Vyčerpání DHCP

DHCP (Dynamic Host Configuration Protocol) poskytuje novým uživatelům v síti veškeré síťové parametry, které jsou nezbytné pro komunikaci s ostatními zařízeními. DHCP server má k dispozici pouze omezené množství IP adres, které může přidělit zařízením připojeným do lokální sítě. Cílem útočníka je vyčerpat všechny IP adresy legitimního DHCP serveru, což vede k odepření služeb poskytovaných DHCP serverem. Nově příchozí uživatelé nebudou mít možnost získání IP adresy a bude jim takto odepřena komunikace v síti. Dalším možným cílem útočníka může být poskytnutí vlastního DHCP serveru, který bude přidělovat IP adresy a označovat útočníka za výchozí bránu sítě. Možné následky jsou útok Mužem uprostřed (Man-in-the-middle) a přesměrování DNS (DNS hijacking).

Provedení tohoto útoku je umožněné absencí autentizace při přidělování síťových parametrů DHCP serverem. Útočník odesílá na server velké množství *DHCPDISCOVER* zpráv. Tímto druhem zpráv si uživatel vyžádá přidělení síťových parametrů. Útočník však modifikuje zdrojovou MAC adresu těchto zpráv. DHCP server takto přidělí IP adresu neexistujícím zařízením [27]. Realizace tohoto útoku v bezdrátových sítí není takto snadná. Úskalí realizace tohoto útoku představuje přístupový bod (AP) do vnitřní sítě. Jak také uvádí práce [27], veškeré příchozí zprávy od zařízení, která nejsou s AP asociována, jsou ihned zahozeny.

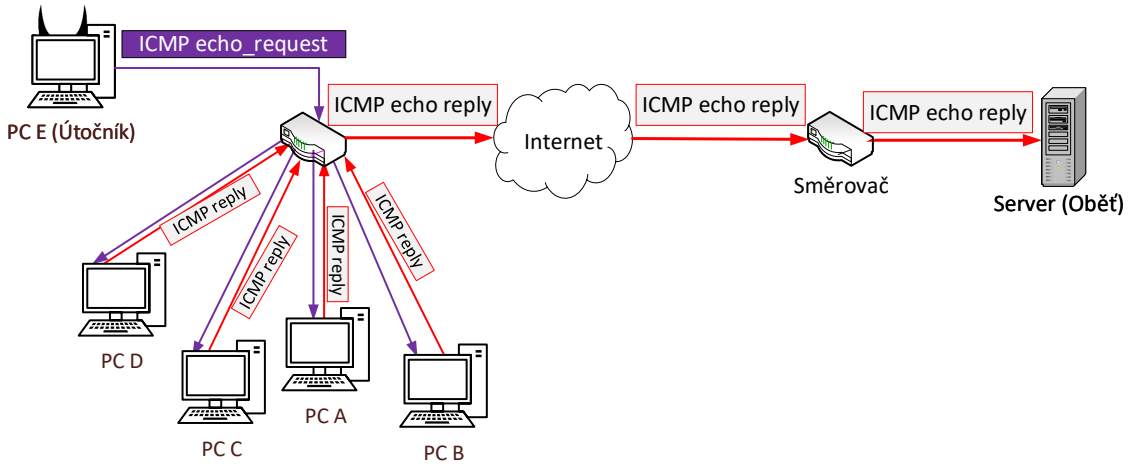
Protiopatření proti tomuto útoku představuje nastavení seznamu důvěryhodných MAC adres. Takto dojde k přidělení IP adresy pouze těm zařízením, které jsou uvedeny na tomto seznamu. Seznam důvěryhodných MAC adres se nachází přímo na DHCP serveru a útočník tak nebude schopný vyčerpat možné IP adresy. Toto řešení však není možné použít pro veřejně dostupné sítě, kdy není žádoucí definovat povolené uživatele. Další řešení, především pro zařízení společnosti CISCO, představuje nastavení funkce Port security. Tato funkce umožní definovat maximální možný počet komunikujících MAC adres na konkrétním rozhraní zařízení. Po překročení definovaného omezení lze nastavit následnou akci. Možnou akcí je například vypnutí konkrétního portu, že kterého došlo k porušení pravidla [28].

1.7.4 Útok Smurf

Útoky typu DoS vychází z jednoho počítače s cílem vyčerpat cílovou stanici tak, že nebude schopna odpovídat na požadavky klientů a nadále poskytovat své služby. DDoS představuje rozlohou větší útok a k jeho realizaci spolupracuje více zařízení. Dobrovolně (více útočníků), proti své vůli (útočníkem podmaněné stanice), či nevědomě. **Smurf** je útokem typu DDoS a využívá stanice uvnitř sítě, které nevědomě plní útočníkův cíl a zahlcují oběť útoku.

Funkcionality ICMP, jmenovitě *ICMP echo request*, zneužívá **Smurf** [29]. Po obdržení *ICMP echo request* stanice odpovídá odesílateli pomocí *ICMP echo reply*. Útočník však nestojí o získání odpovědi na odeslaný dotaz, proto podvrhne zdrojovou adresu obsaženou uvnitř *ICMP echo request*. Stanice přijímající tento požadavek, odpoví zařízení jehož IP adresa je uvedena uvnitř pole se zdrojovou adresou [30]. Útočník využívá převážně všesměrového vysílání (Broadcast). Odešle-li útočník *ICMP echo request* na všesměrovou adresu dané sítě (x.x.x.255). Směrovač zpracovávající požadavek jej předá všem zařízením uvnitř sítě, kterých je N. Všech N zařízení vygeneruje *ICMP echo reply* a odešle na útočníkem podvrženou zdrojovou adresu Oběti. Tímto způsobem může útočník využít více nezávislých sítí a dosáhnout násobně vyššího počtu *ICMP echo reply*. Průběh útoku zobrazuje obrázek 1.8. Fialovou barvou je znázorněn *ICMP echo request* odesílaný na směrovač, který jej

předá všem zařízením uvnitř sítě. Každé zařízení odpovídá *ICMP echo reply*, znázorněno červeně. Vygenerované množství odpovědí zahltí Oběť, která již není schopná zpracovávat jiné požadavky.



Obr. 1.8: Realizace DDoS útoku Smurf.

Protiopatření útoku je komplikované z pohledu použitého ICMP protokolu, který je vhodný pro diagnostiku sítě, avšak s výše popsaným rizikem. Řešením může být komponenta firewall filtrující ICMP pakety dle konfigurace, kdy například veškeré ICMP pakety jsou zahazovány [29]. Pravděpodobně nejvyšší váhu má konfigurace sítě od poskytovatele internetových služeb (ISP), kdy sám poskytovatel může vytvořit taková protiopatření, která zabrání útočníkovy jej realizovat. Pokud by ISP (Internet Service Provider) kontroloval zdrojovou adresu uvedenou uvnitř hlavičky příchozích paketů, může zajistit zahození paketu nenáležícího do vlastní sítě. Předejde tak realizaci DDoS útoku **Smurf** [31].

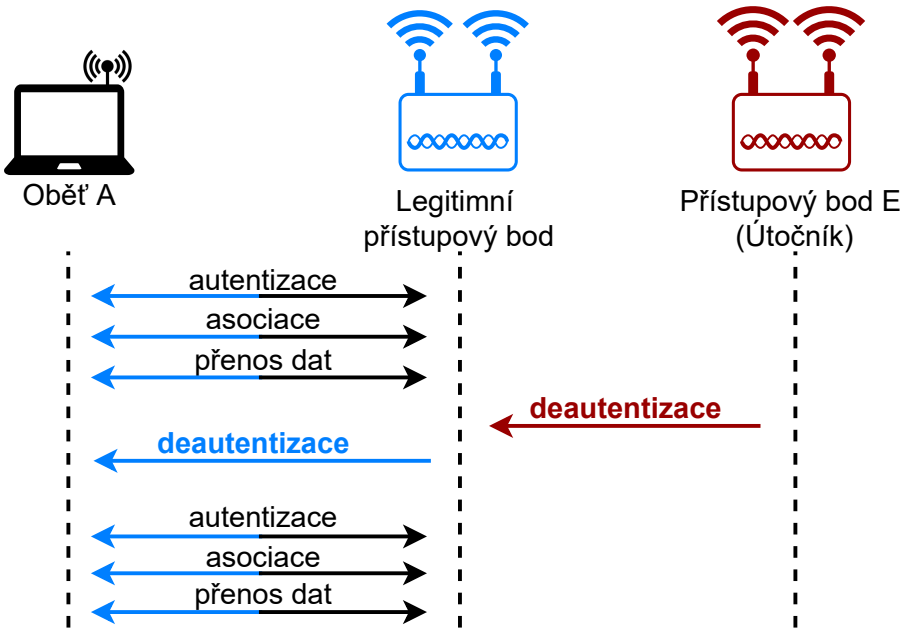
1.8 Útoky cílené na bezdrátová zařízení

Opomenuta nesmí být také bezdrátová zařízení a útoky na ně cílené. Četnost užívání bezdrátových zařízení uvnitř sítě roste a je tedy nutné znát rizika, která pro tato zařízení mohou nastat. Výhodou těchto zařízení je možnost volného pohybu při jejich užívání, avšak pro připojení do sítě potřebují přístupový bod (AP). Přístupový bod může oznamovat svoji dostupnost pomocí vysílání svého SSID (Service Set Identifier), což představuje jeho jméno. Například této skutečnosti může útočník využít pro realizaci útoku. Výsledkem útoku může být jak odepření služby, tak i odcizení soukromých dat Oběti.

1.8.1 Deautentizační útok

Pro komunikaci v bezdrátové síti, tedy síti označené jako WLAN (Wireless Local Area Network), je využívaný standard IEEE 802.11. Tento standard je rozšířený o množství modulací, které jsou označovány například písmeny a, b, g, n. Veškeré řídící rámce tohoto standardu jsou na druhé vrstvě ISO/OSI modelu odesílané v otevřeném formátu. Důvodem je možnost zjištění dostupných WLAN v okolí a vyžádání si přístupu do sítě. Naopak tato skutečnost dovolí uživateli zachytit tyto řídící rámce, upravit je a využít ve svůj prospěch. V tomto případě je útočník schopen upravit řídící zprávu tak, aby došlo k odpojení jednoho, nebo více uživatelů od konkrétního AP. Cílem může být donucení oběti k připojení do útočníkem vytvořené sítě.

Zachycené řídící rámce jsou útočníkem upraveny tak, aby je AP vyhodnotil jako pocházející od uživatele, v tomto případě od Oběti útoku. K tomuto útoku jsou využívány dva typy rámců, konkrétně DeAuth (deautentizace) a DisAssoc (disociace). Obdrží-li AP jeden z těchto dvou rámců, převede oběť ze stavu „autentizovaný“ do stavu, ve kterém Oběti není dovoleno komunikovat. Tyto rámce představují stav, kdy si uživatel již nepřeje nadále udržovat spojení s AP. Deautentizační rámce přináší větší škodu z pohledu časových nároků na opětovné připojení do sítě. Oběť se musí znovu autentizovat, což v případě disociace není nutné, a Oběti je odepřená komunikace o kratší časový úsek [32]. Ilustrací tohoto útoku je Obrázek 1.9, který znázorňuje navázání spojení Oběti s legitimním AP (modrý). V průběhu komunikace Oběti s AP odešle Útočník (červený) deautentizační rámec. Následně dojde k deautentizaci Oběti, která poté musí opět navázat spojení s legitimním AP.



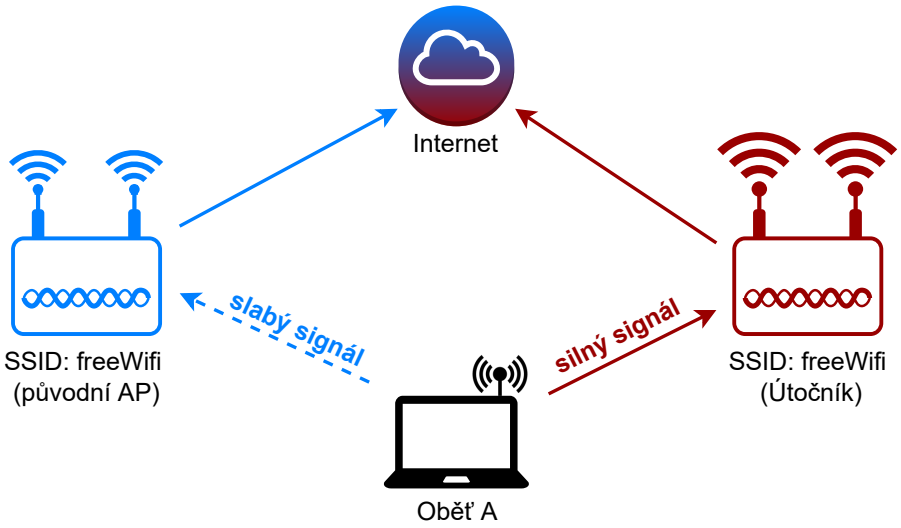
Obr. 1.9: Průběh deautentizačního útoku.

Detekce deautentizačního útoku je vybudována především na monitorování sítě a zaznamenávání přenesených DeAuth a DeAssoc rámců. Počet přenesených rámců je zaznamenán a porovnáván s vybranou hranicí za určený časový interval. Stanovení hranice nejčastěji probíhá dle zkušeností správce sítě a odhadu na základě běžné komunikace v síti. Dojde-li k překročení této hranice, poté je vygenerované oznámení o možném průběhu deautentizačního útoku [32].

1.8.2 Falešný přístupový bod

Jedná se o útok vytvořením falešného přístupového bodu, viditelného pro zařízení a hlavně volně dostupného. Tento falešný AP disponuje stejnou konfigurací, jakou má legitimní AP. Snahou tohoto útoku je ošálit Oběť tak, aby se k tomuto AP připojila a jakýmkoliv způsobem komunikovala. Útočníkovým cílem je zachytávání komunikace a odhalení soukromých údajů uživatele. Výsledkem je zisk přihlašovacích údajů, číslo kreditní karty či další, jinak hodnotné informace.

Útočníkovo zařízení nemusí poskytovat přístup do internetu, nebo do konkrétní lokální sítě. Pouze sbírá informace o zařízení Oběti, nebo disponuje staticky generovanými webovými stránkami, které by Oběť mohla navštívit a zachytává Obětí zadané informace. Nejčastějším využitím takto vytvořeného AP je útok mužem uprostřed. Útočník nakonfiguruje AP tak, aby vystupoval jako legitimní AP. Dle publikace [33], je provedení tohoto útoku velmi snadné a potřebná konfigurace sestává pouze ze stejného SSID legitimního zařízení. Útočníkovo zařízení poté předává veškeré požadavky uživatelů legitimnímu zařízení, které jejich požadavky vyhodnotí a odpovědí přeposílá zpět útočníkově zařízení. Veškerá komunikace může probíhat tak, že si Oběť ani nevšimne, že je připojena k jinému zařízení, než je obvyklé. Útočník nyní může pasivně čekat na přihlášení další Oběti, nebo aktivně deautentizovat uživatele z legitimního zařízení, kteří budou takto nuceni připojit se k podvrženému AP. V tomto případě je pro Útočníka důležité, aby ním vytvořený AP měl vyšší vysílací výkon, než legitimní zařízení. Tomuto útoku cíleného na veřejnost se přezdívá *zlé dvojče*, neboli Evil twin. Tento útok je odlišný do útoku anglicky zvaného *rogue AP*. Cílem tohoto útoku je připojení útočníkova AP do soukromé sítě a nalákat tak uživatele, kteří potřebují pracovat se síťovými prvky této lokální sítě. Oba útoky nesou podobnostní rysy ve formě duplikování legitimního bezdrátového AP a přinucení uživatelů se k tomuto zařízení připojit[34]. Pro získání informací je však nutné, aby Oběť navštěvovala nezabezpečené stránky, tedy stránky užívající protokol HTTP a nevyužívala VPN připojení [35]. Výše popsané útoky jsou často zaměňovány, či spojovány. Grafické znázornění falešného AP, konkrétně útoku Zlé dvojče, představuje Obrázek 1.10. Obrázek zobrazuje připojení Oběti na AP Útočníka (červený), který disponuje silnějším signálem, než původní AP (modrý) nazvaný „freeWifi“.



Obr. 1.10: Probíhající útok Zlé dvojče.

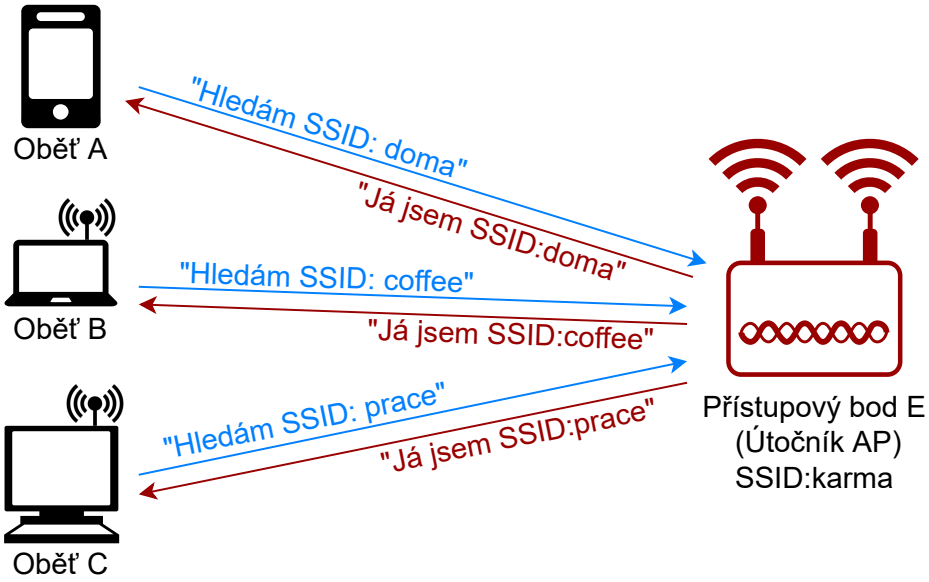
Detekce falešných AP může probíhat na základě několika typů parametrů. Prvním typem může být například doba, kterou paket musí urazit k cíli a zpět, neboli RTT (Round Trip Time). RTT pro kabelově připojená zařízení je odlišné od RTT pro bezdrátová zařízení. Při porovnání těchto dvou údajů, spolu se znalostí topologie sítě, je možné detekovat falešný AP. Další detekce může probíhat na základě fyzikálních parametrů vysílaného signálu [34, 35]. Také systém Kismet poskytuje detekci falešných AP, avšak na základě kontroly vysílaného SSID a staticky definovaných MAC adres zařízení, která toto SSID mohou vysílat [36].

1.8.3 Útok Karma

Karma představuje v bezdrátových sítí útok, který je podobný útoku s falešným přístupovým bodem a využívá situace, kdy zařízení zjišťuje dostupnost známého AP. Tento útok je založený na naslouchání dotazům na zjištění dostupnosti (probe request) konkrétního AP. Pokud se nachází útočníkem ovládaný AP v blízkosti dotazujícího se zařízení, Útočníkův AP odpoví na dotaz a vydává se za Oběti známé zařízení. Dotazující se zařízení (Oběť) po obdržení odpovědi vyšle autentizační požadavek. AP s Obětí naváže komunikaci a útočník takto může dosáhnout útoku muže uprostřed a odposlouchávat komunikaci Oběti.

Úspěšná realizace útoku Karma je závislá na nastavení zařízení Oběti. Oběť musí mít ve svém zařízení list preferovaných sítí, ke kterým se chce připojit a alespoň některé z nich nastavené na automatické připojení. Díky tomuto nastavení dochází k vysílání dotazu na dostupnost sítě, ke které se Oběť chce automaticky připojit. Útočníkův AP na tento požadavek reaguje, nehledě na to, že jeho původní SSID je

odlišné od požadovaného. Oběť se poté pokusí připojit k síti. V některých případech nemusí dojít ke kompletnímu připojení kvůli dotazování na další dostupné AP výše postavené v seznamu poreferovaných sítí. I na tyto požadavky útočník odpoví kladě a naváže s Obětí komunikaci. Předešle navázaná spojení budou Obětí ukončována, až dorazí k poslednímu záznamu preferovaných sítí. Nyní dojde k úplnému navázání spojení a Oběť bude komunikovat v síti útočníka v domnění, že se jedná o známou síť [37]. Obrázek 1.11 zobrazuje Útočníka odesílajícího odpovědi (označeny červeně) na všechny dotazy o dostupnosti známého AP (označeny modře).



Obr. 1.11: Probíhající útok Karma.

Detekci útoku Karma lze založit na párování SSID a k němu příslušné BSSID (Basic Service Set Identifier) známého AP. BSSID představuje MAC adresu konkrétního AP. Pár SSID a BSSID je vytvořený při prvotním připojení k AP. Z těchto dvou údajů je vytvořený hash, který je uložený do databáze v zařízení. Při každém dalším připojení do sítě dojde k získání BSSID zařízení a vytvoří se nový hash. Takto získaný hash je porovnávaný s hodnotou v databázi a v případě neshody dojde k odpojení od sítě kvůli možnému útoku Karma. Tento postup byl navržen v publikaci [38]. Další možností je využití nástroje PiKarma, který naslouchá okolním AP v dosahu a zaznamenává jejich MAC adresu a příslušné SSID. Dojde-li k zaznamenání alespoň dvou odpovědí obsahující stejnou MAC adresu, ale odlišné SSID, poté bude daný AP vložený na černou listinu. Tento AP bude následně podroben deautentizačnímu útoku, aby došlo k odpojení již připojených uživatelů. Jedná se o nástroj publikovaný na GitHub s otevřeným zdrojovým kódem [39].

2 Automatizovaná detekce útoků

Spolu s nástrojem Firewall jsou zde i další způsoby, jak odhalit či kompletně zamezit možným útokům. Cílem nemusí být pouze koncová zařízení, ale celá síť. Kvůli většímu počtu kybernetických útoků, a jejich snižujícím se nárokům na znalosti útočníka, bylo nutné zavést automatizované nástroje pro jejich omezení. Zmíněnými nástroji jsou IDS a IPS. Nemusí se však jednat výlučně o dvě zařízení. Při použití IPS lze deaktivovat jejich funkce pro prevenci útoků a využít je pouze jako IDS zařízení.

Detekce průniku je proces monitorování nastalých událostí v počítačovém systému nebo síti. Následně probíhá analýza těchto událostí, zda nenaznačují možné bezpečnostní riziko, neboli incident. Tyto incidenty mohou představovat například prolomení či částečné prolomení bezpečnostních pravidel, pravidel užití nebo běžné bezpečnostní praktiky. Automatizovaná detekce hrozeb nedokáže dokonale odhalit veškeré incidenty. Dochází k vyvolání chybně pozitivních a chybně negativních stavů. Při pokusu o eliminaci jednoho stavu často dochází ke zvýšení stavu druhého. Některé organizace přikročí raději ke snížení chybně negativních stavů, což zvýší četnost odhalení incidentů. Toto řešení však má svoji cenu v podobě chybně označených benigních událostí jako incidenty [40].

Veškerá data získaná systémem detekce musí projít několika kroky než dojde k jejich vyhodnocení. V prvé řadě se jedná o uložení těchto dat na místo, ve kterém dojde k jejich filtraci. Filtrace zajistí, že budou vyhodnocena poza ta data, která obsahují užitečnou informaci. Následující proces normalizace zajistí, aby měla veškerá data stejný formát a dochází zde také ke kategorizaci dat. Normalizovaná data jsou sjednocena s dalšími daty, které k sobě náleží. Jedná se zde o korelaci, která pro detekční systémy znázorňuje vzájemný vztah na základě pravidel (signatury) či vytvořeného modelu (anomálie). Posledním krokem je oznámení o nalezené shodě s vytvořenými pravidly či modelem detekce kybernetických útoků [41].

2.1 Intrusion Detection System

Proces detekce průniku je automatizován softwarem, který tvoří výsledné IDS. Tento systém aktivně nezabraňuje vzniklým incidentům, pouze plní funkci ohlašování a upozorňování, například systémového administrátora. Může být umístěný za Firewall a v případě jeho „prolomení“ oznámí tuto skutečnost administrátoru, který následně podnikne potřebná opatření. Detekce incidentů je založena na kontrole jednotlivých paketů, které byly tímto systémem odchyceny a analyzovány. Tento proces není omezený použitým komunikačním protokolem, například TCP či UDP. Mezi hlavní funkce systému patří:

- ukládání informací spojených s probíhajícími událostmi,
- oznámení důležitých událostí administrátora systému,
- produkování výsledných hlášení.

Přednostní tohoto systému je možnost jeho úprav dle konkrétních potřeb. Naopak hlavní nevýhodou detekčních systémů je jejich neschopnost zpracovat šifrovanou komunikaci [42].

Metody detekce jsou děleny do následujících kategorií:

- **Detekce na bázi signatur** - Jedná se o ustálený postup při tvorbě incidentů, například obsah paketu změněný tak, aby vyvolal konkrétní incident. Tento postup útoku je známý a na jeho základě je probíhající incident porovnáván. Tato metoda je efektivní v případě odhalení již dříve známých hrozeb. Jedná se o velmi jednoduchou metodu, která je omezená pouze na definované hrozby.
- **Detekce na bázi anomálií** - Tento způsob je převážně založený na anomáliích obsažených v hlavičkách paketů, spolu se znaky abnormálních jevů. Je tedy nutné rozhodnout, zda jde o záměrně generované vytížení [43]. Systém má k dispozici profily, které charakterizují normální chování uživatelů, síťových připojení, aplikací atd. Výhodou tohoto typu detekce je přizpůsobení se novým, dříve neznámým hrozbám. V případě detekce anomálií existuje několik metod vytvoření modelu detekce. Kupříkladu lze přistoupit k vytvoření referenčního modelu, tedy modelu optimálního stavu síťového provozu. Referenční model je vypočítán za pomocí matematických rovnic. Jako první se vypočítá průměrná hodnota vybraného datového souboru, poté směrodatná odchylka a standardní hodnota chyby. Přesnost referenčního modelu závisí na množství dat, která byla použita při jeho tvorbě [44]. Veškerá odchýlení od tohoto modelu jsou zaznamenávány a zpracovávány. Dalším příkladem je frekvenční model, u jehož využití se počítá výskyt definovaného jevu za daný časový úsek.
- **Stateful Protocol Analysis** - V tomto případě dochází k porovnávání předdefinovaných profilů, které vychází z obecně uznaných definicí neškodné aktivity protokolů, proti probíhajícím událostem. Tato metoda spoléhá na obecné profily vyvinuté výrobcem, které specifikují, jak by jednotlivé protokoly měly či neměly být použity [40].

IDS jsou podrobněji dělené na základě jejich metod detekce, jak uvádí článek [45].

- **Behaviour-based** neboli založené na vlastnostech. Tato kategorie je také někdy označována jako statistická detekce anomálií. Jak název napovídá, jedná se o využití statistických technik k detekci incidentů. Techniky začínají určením normálního stavu pro daný systém. Následně jsou sbírána data, která se odchylují od stanoveného normálního stavu. Jakmile dojde k přesáhnutí stanovené hranice, systém spustí alarm. Úskalím je komplikovaná implementace a potřeba velkého množství zdrojů.

- **Knowledge-based** neboli založené na znalosti. Tento přístup je založený na signaturách. Jedná se o hledání incidentů na síti či aktivity v logovacích souborech. Tato metoda detekce je dále dělena dle jejího zaměření.
- **Network-based IDS** jsou IDS zaměřené na hledání signatur uvnitř síťového provozu. Zkráceně označené jako NIDS. Odhalení incidentů probíhá na úrovni paketů. Vyčleněná stanice disponující IDS systémem je připojená k síťovému provozu, který analyzuje. NIDS nesmí být lokalizovatelná uvnitř sítě, a proto rozhraní systému je nastavené jako skryté. Nevlastní IP adresu, pouze analyzuje provoz směrovaný skrz něj. Analýza je cílena na hlavičky jednotlivých paketů, tak i jejich samotný obsah. Získané informace porovnává se svojí databází známých signatur. Uvnitř sítě se také nachází řídící IDS systém, skrze který je NIDS spravována. Na tento řídící systém jsou také odesílané hlášení o odhaleném incidentu.
- **Host-based IDS** neboli HIDS představuje IDS zaměřující se na logovací soubory. Zde je systém IDS také umístěna na vyčleněné stanici, avšak není připojený do sítě a pracuje jako aplikace spuštěná v pozadí. Zaměřuje se na aplikace běžící na dané stanici. Oznámení o incidentech také odesílá na řídící IDS systém, který určí následující akce. HIDS od něj také přijímá administrační pokyny.

Odesílání zpráv oznamujících incident probíhá pro obě zmíněné metody stejně. Realizováno je pomocí SNMP (Simple Network Management Protocol). SNMP agenta zde představuje NIDS/HIDS a řídící IDS systém je SNMP manažer. Aby agent mohl odesílat SNMP zprávy, musí být vyzván manažerem. Pokud byl identifikován incident, agent bez vyzvání odešle SNMP zprávu manažeru, což je označováno pojmem *SNMP trap*.

2.2 Intrusion Prevention System

IPS systémy poskytují veškeré funkce dostupné u systémů IDS a rozšiřují je o pokusy aktivně zamezit možným bezpečnostním incidentům. Jedná se tedy o aktivní bezpečnostní prvek. Z důvodu velké podobnosti systémů IDS a IPS zde nebude duplicitně popsáno rozdělení a detekční metody systémů IPS. Naopak se tato podkapitola bude věnovat výhradně rozdílům mezi těmito systémy a dodatečným vlastnostem systémů IPS.

Hlavní rozdíl se nachází ve funkcích, které IPS nabízí. Oproti funkcím IDS systémů jsou zde další tři funkce, jak popisuje publikace [40]:

- zastavení samotného incidentu,
- změna bezpečnostního prostředí,
- změna obsahu incidentu.

- **Zastavení incidentu** představuje například situaci, kdy IPS ukončí připojení k síti, nebo navázané uživatelské spojení, které je zneužité k tvorbě incidentu. IPS také disponuje možností blokovat přístup k cíli incidentu na základě IP adres, uživatelského účtu či dalších parametrů. Dalším způsobem je blokování veškerého přístupu k cíli incidentu, ať už se jedná o koncové zařízení, službu, aplikaci či jiné zdroje.
- **Změna bezpečnostního prostředí** představuje změnu konfigurace jiných bezpečnostních opatření za účelem zamezení incidentu. Příkladem je změna konfigurace síťového prvku, jako je firewall, router apod. Některé IPS vydávají „záplaty“ pro koncové stanice v případě, že odhalí některé její zranitelnosti.
- **Změna obsahu incidentu** spočívá v odstranění či změně škodlivé části incidentu tak, aby jej učinili neškodným. Jednoduchým příkladem je odstranění škodlivé přílohy obsažené v emailu. Složitějším procesem je nastavení IPS jako proxy, kdy dochází k normalizaci příchozích požadavků. Tento proces může v některých případech vést ke kompletnímu zamezení incidentu.

2.3 Analýza současných systémů detekce

Existuje značné množství systémů detekce kybernetických útoku. Pro realizaci cílů diplomové práce je vhodné nejprve uvést možné varianty těchto systémů. Tato kapitola je zaměřena na výčet dostupných variant systémů detekce a jejich popisu. Jedná se pouze o některé systémy, které však umožňují svoji implementaci jako *NIDS*, nejsou komerčním řešením a jedná se o systémy s otevřeným zdrojovým kódem. Závěrem kapitoly je soupis vybraných systémů pro praktickou realizaci práce.

Snort

Systém Snort byl vyvinut v roce 1998 se zaměřením na analýzu paketů. Jedná se o systém podporující jednovláknové zpracování paketů. Snort je známý převážně pro své detekční schopnosti a stabilitu. Navzdory tomu však může nastat stav, kdy systém Snort nebude výkonnostně stíhat zpracovat veškerá příchozí data. Jmenovitě se jedná o zpracování 100-200 megabitů za vteřinu [46]. Z toho důvodu může dojít k jejich ignorování a tedy pozdržené, či žádné detekci kybernetického útoku. Modulární stavba tohoto systému dovoluje vývojářům přidání vlastních dodatečných funkcí bez nutnosti zásahu do jádra systému. Systém Snort je složený z analyzátoru paketů, preprocesoru, detekčního modulu využívající daná pravidla a oznámení či logování v případě shody pravidla [47]. V době psaní této části práce byla poslední oficiální verze systému 2.9.8. Probíhá však testování systému Snort 3.0, který již nabízí řadu

vylepšení předchozí verze, především multivláknové zpracování dat [48]. Avšak z důvodu, kdy tato verze ještě není oficiálně vydaná, je brána v úvahu především výše zmíněná verze 2.9.8.

Systém Snort lze do strážené sítě umístit jako *NIDS* zařízení, nebo nainstalovat na hostitelské zařízení (*HIDS*). Podporuje detekci na bázi signatur. Pravidla pro detekci jsou dostupná a lehce spravovat pomocí programu Oinkmaster. Jedná se o program pomocí kterého lze aktualizovat pravidla z vybraných zdrojů. Také lze vytvářet svá vlastní pravidla. Příkladem pravidla je obrázek 2.1 sloužící k zjištění konkrétního textu obsaženého v HTTP dotazu. Každé pravidlo je rozděleno na tři části. První částí je akce, která bude provedena po spojení analyzovaných dat s konkrétním pravidlem. Následuje část hlavičky pravidla. Tato část začíná určeným protokolem a následuje zdrojová adresa a port, poté cílová adresa a port. Poté je zde část možností pravidla. V této části je pravidlo blíže specifikováno [49].

```
alert tcp $EXTERNAL_NET any -> 10.200.0.0/24 80 (msg:"WEB-IIS CodeRed v2
root.exe access"; flow:to_server,established; uricontent:"/root.exe"; nocase;
classtype:web application-attack; reference:url,www.cert.org/advisories/CA-
2001 19.html; sid:1255; rev:7;)
```

Obr. 2.1: Příklad možného pravidla systému Snort [49].

Suricata

Dalším v pořadí je systém Suricata. Jedná se o systém dovolující více vláknové zpracování dat. Tato vlastnost je velice výhodná pro zařízení disponující více procesory a dovoluje rychlejší zpracování příchozích dat. V případě větší míry zátěže zřídka dochází k vynechání dat při porovnání se stanovenými pravidly detekce [47]. Systém Suricata také podporuje využití výkonu grafické karty za účelem akcelerace výkonu. Struktura tohoto systému je podobná struktuře systému Snort. Rozdíl je pouze u detekčního modulu, kdy dochází k vícevláknovému zpracování.

Tento systém lze umístit jako další zařízení do strážené sítě (*NIDS*) či nainstalovat přímo na zařízení (*HIDS*). Suricata také disponuje módy IDS či IPS. Jako soubor pravidel (signatur), lze využít již volně dostupný soubor pravidel (Emerging Threats Open ruleset). Ke správě a aktualizaci těch pravidel slouží nástroj *suricata-update*. Jedná se o oficiální a doporučovaný způsob zprávy těchto pravidel. Další možností získání pravidel detekce je využití pravidel nástroje Snort či tvorba vlastních. V případě pravidel systému Snort dochází k několika odlišnostem, avšak jejich použití je stále možné [50].

Pravidla systému Suricata se skládají z několika částí. Těmito částmi jsou *akce*, *hlavička* a *možnosti*. Akce definuje úkon ke kterému dojde v případě shody s definovaným pravidlem. Část hlavičky obsahuje protokol paketu, zdrojovou/cílovou adresu a port. Možnosti pravidla blíže specifikují jeho povahu a konkrétní zaměření. Lze například definovat, po jakém počtu stejných paketů daného časového úseku dojde ke shodě s pravidle a vyhlášení oznámení. Příklad takového pravidla zobrazuje Obrázek 2.2. Obrázek pochází z dokumentace systému Suricata [51]. Na tomto obrázku je červeně vyznačena část akce. Zelená část představuje hlavičku a modrá možnosti detekce. Dalším rozšířením jsou také klíčová slova, která se pojí s vybraným protokolem, který je uvedený v hlavičce pravidla. Tato klíčová slova se uvádí do části popisující možnosti detekce.

```
drop tcp $HOME_NET any -> $EXTERNAL_NET any (msg:"ET TROJAN Likely Bot Nick in IRC (USA +..)";
flow:established,to_server; flowbits:isset,is_proto_irc; content:"NICK "; pcre:"/NICK .*USA.*[0-9]
{3,}/i"; reference:url,doc.emergingthreats.net/2008124; classtype:trojan-activity; sid:2008124;
rev:2;)
```

Obr. 2.2: Příklad možného pravidla systému Suricata [51].

Zeek

Zeek představuje pasivní síťový monitorovací nástroj dříve nazývaný Bro. Tento nástroj je vyvíjen od roku 1990 a lze jej do sítě umístit pouze jako *NIDS*. Detekce kybernetických útoků probíhá na bázi signatur i anomálií. Jeho hlavním zaměřením je transportní a aplikační vrstva referenčního modelu ISO/OSI. Systém Zeek nepodporuje vícevláknové zpracování dat, ale je možné zpracování rozložit na několik současně běžících instancí systému Zeek [52].

Zjištěná hlášení jsou ukládána do logů nebo do plně přizpůsobitelného výstupu, který lze použít pro následné manuální či automatizované zpracování. Zeek dále poskytuje výkonnostní, auditorské, kapacitní a bezpečnostní služby. Vývoj tohoto systému je založený na vlastním skriptovacím jazyce Zeek. Veškeré detekční metody a způsoby detekce lze upravit. Žádná funkcionalita není pevně ukotvená v jádře systému a celý systém je tak plně modifikovatelný.

Logovací soubory obsahují veškeré informace, které je systém Zeek schopen zachytit. Jedná se o veškerá navázaná spojení a parametry protokolů aplikační vrstvy. Výsledná podoba těchto logovacích souborů může být buď jako tabulkově rozdělené záznamy, nebo data ve formátu JSON pro následné zpracování [53].

Kismet

Jedná se o systém zaměřený na analýzu a detekci v bezdrátových sítích (*WIDS*). Detekce je prováděná pasivně a je schopný pracovat s každou síťovou kartou, která podporuje přepnutí do monitorovacího módu. Díky pasivnímu přístupu systém Kismet dokáže odhalit i skryté bezdrátové sítě a sám nevysílá žádná data. Dokáže také zachytit přítomnost bezdrátového přístupového bodu (AP), bezdrátových klientů a jejich společnou asociaci. Možné je také nechat systém Kismet procházet dostupné vysílací kanály, či zaměřit jej pouze na jeden konkrétní. Systém Kismet je schopný logovat veškeré zachycené pakety a uložit je do souborů například ve formátu JSON. Další jeho vlastností je zjištění úrovně použitého šifrování u konkrétního přístupového bodu ve vysílacím dosahu [54, 55].

Tento systém je již v instalačním balíčku operačního systému Kali. Kismet také nabízí grafické rozhraní, avšak nebude v této práci nijak využito. Pro detekci kybernetických útoků tento systém již disponuje sadou pravidel a nabízí také detekci falešného AP pro jedno konkrétní BSSID. Detekční mechanismy pokrývají exploity několika známých chyb systémů, záplavové a DoS útoky [56].

Arpwatch

Arpwatch představuje systém zaměřený na ARP protokol. Tento systém monitoruje veškerý ARP provoz a vytváří si seznam zařízení. MAC adresa každého zařízení je v seznamu spojeno s IP adresou. Arpwatch tak dokáže zjistit, zda došlo k připojení nového zařízení do sítě, či změně MAC adresy kteréhokoliv dříve známého zařízení. Díky těmto vlastnostem je tento systém vhodný například pro detekci ARP spoofing útoku, neboli Podvržení ARP zpráv. Veškeré změny v síti oznamuje výpisem do systémových logů a umožňuje také nastavit e-mailovou adresu, na kterou budou tato oznámení odesílána [57].

Hodnocení systémů detekce

Pro začátek bylo nutné vybrat systémy zaměřené na ethernetová rozhraní. V tomto případě nebylo možné objektivně vybrat jediný systém pro praktickou realizaci této práce. Systém Zeek byl zamítnutý kvůli jeho způsobu detekce kybernetických útoků. Nabízí velké možnosti a tvorbu komplexních metod detekce útoků, avšak pro potřeby této práce by nebyly plně využity. Také by bylo nutné získat zkušenosti se samotným skriptovacím jazykem Zeek. Proto je možnost snadného přidání nových signatur zde dostačující a je nutné rozhodnou mezi systémy Suricata a Snort. Jedná se o velmi známé systémy detekce. Hlavním záporem u systému Snort je využívání pouze jednoho vlákna pro zpracování dat. Na základě výsledků článku [47] je systém

Snort vhodnou volbou pro méně výkonné procesory. Jedná se především o procesory s jedním jádrem. Přesnost detekce systému Snort mírně převyšuje výsledky systému Suricata, avšak v případě větší zátěže jsou výsledky opačné. Je tedy nutné provést důkladné rozhodnutí pro konkrétní potřeby této práce a zařízení Raspberry Pi. Zařízení Raspberry Pi 4 typ B disponuje čtyřjádrovým procesorem, z toho důvodu se systém Suricata jeví jako vhodná volba. Pro ověření této skutečnosti je nutné nástroje porovnat na realizovaném experimentálním pracovišti.

Výběr možných nekomerčních alternativ pro systém Kismet sestával převážně z variant poskytujících analýzu bezdrátových sítí, nikoliv detekci kybernetických útoků. Jako komerční varianta přicházel do úvahu systém Bastille, který nabízí detekci kybernetických útoků. Dalšími možnými variantami pro bezdrátové sítě jsou systémy Suricata a Snort, avšak dle teoretického návrhu realizovaného detektoru nebudou na tuto oblast zaměřeny. Z tohoto důvodu byl zvolen systém Kismet jako detektor kybernetických útoků v bezdrátových sítích.

Poslední oblastí detekce je Linková vrstva referenčního modelu ISO/OSI. Pro tento případ bylo nutné vybrat odlišný systém, který je zaměřený výhradně na tuto oblast. V průběhu hledání dostupných systémů zaměřených na tuto oblast byl k dispozici i systém XArp. Tento systém je zaměřený na útoky spojené s ARP protokolem. Jedná se však o systém, který nenabízí otevřený zdrojový kód a cílí na operační systémy Windows a Linux Ubuntu. Další nevýhodou pro tuto práci je jeho rozdělení na placenou a neplacenou verzi. Neplacená verze nabízí detekci útoků, avšak jeho konfigurace je omezená, nedovoluje zaměření na jedno síťové rozhraní a neodesílá e-mailová oznámení [58]. Z těchto důvodů byl vybrán systém Arpwatch, který poskytuje dostatečné vlastnosti a funkce pro praktickou realizaci této práce.

3 Vlastní návrh a implementace detektoru

Kapitola je věnována vlastní realizaci experimentálního pracoviště a popisu jeho částí. Pracoviště bylo vytvořeno za účelem otestování vybraných detekčních systémů a jejich hardwarových nároků. Vybrané detekční systémy jsou použity pro vlastní realizaci program detektoru. Realizovaný detektor je testován dle definovaných scénářů kybernetických útoků s využitím experimentálního pracoviště. Dále byla vytvořena dokumentace popisující možnosti instalace a použití programu detektoru. Cílem praktické části práce je:

- realizace experimentálního pracoviště,
- realizace scénářů kybernetických útoků,
- srovnání systémů detekce kybernetických útoků,
- vlastní návrh programu detektoru,
- implementace a testování programu detektoru,
- dokumentace programu detektoru.

3.1 Realizace experimentálního pracoviště

Experimentálním pracoviště zde slouží pro realizaci útoků popsaných v první kapitole práce. Tyto útoky představují incidenty, které budou zaznamenávány či kompletně přerušeny výsledným detektorem. Tato funkce detektoru je realizována pomocí vybraných IDS/IPS systémů.

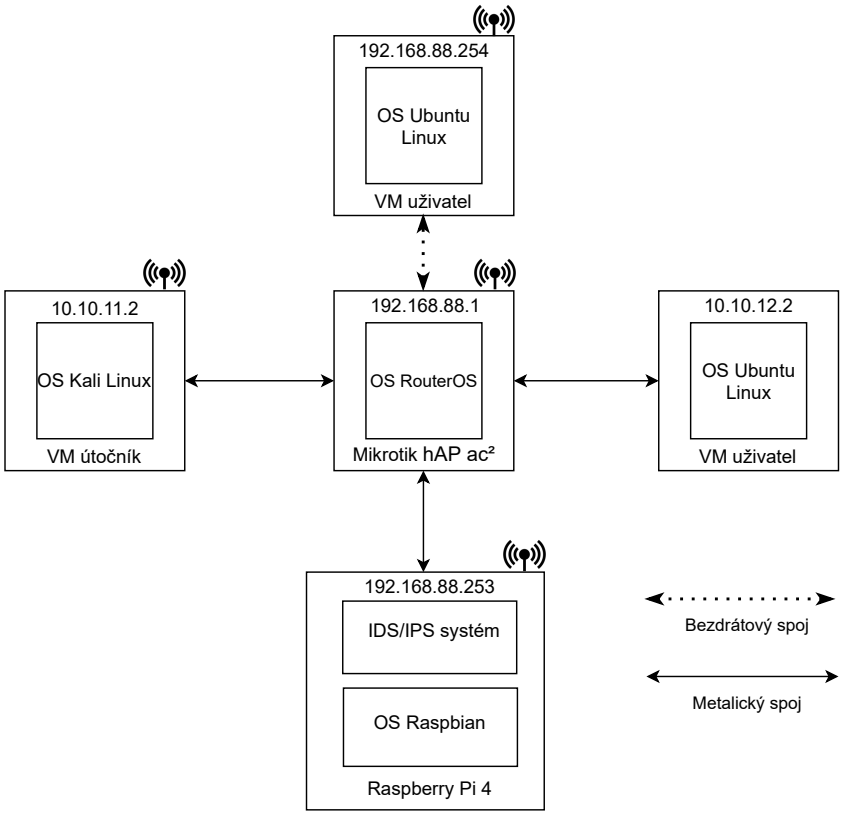
Útočníka zde představuje virtuální stroj s operačním systémem Kali Linux. Tento operační systém disponuje řadou nástrojů zaměřených na zátěžové a penetrační testování. Pro realizování útoků na bezdrátové sítě byl k tomuto stroji připojen USB Wi-Fi adaptér. Jedná se o adaptér s chipsetem Atheros AR9271, který nativně podporuje Linuxové distribuce. Používá frekvenci pouze 2.4 GHz s podporou standardů IEEE 802.11bgn.

Obětí generovaných útoků bude druhý virtuální stroj s operačním systémem Ubuntu. Tento operační systém slouží jako systém pro běžného uživatele a nemá konkrétnější určení, například jako zmíněný Kali Linux. Tento stroj tedy představuje uživatele generujícího běžný síťový provoz. Využitý bude také pro testování odolnosti detektoru na chybně vyhodnocené události.

Detektor bude realizován na zařízení Raspberry Pi 4. Jedná se o zařízení drobných rozměrů, které je možné umístit do budovy, aniž by poutalo nechtěnou pozornost. Lze jej označit jako jednodeskový osobní počítač. Na toto zařízení budou instalovány vybrané IDS/IPS systémy. Monitorovaný provoz zde bude vyhodnocován a na základě vyhodnocení budou provedeny příslušné akce.

Uvnitř topologie se také nachází přístupový bod (Access Point) Mikrotik, ze kterého bude zrcadlený veškerý provoz na detektor, tedy zařízení Raspberry Pi. Zrcadlení provozu je zde nastaveno z důvodu, kdy bude sám Mikrotik vystaven útokům a je žádané, aby i tato situace byla monitorována. I přes fakt, že se jedná o přístupový bod, použitý Mikrotik hAP ac^2 [59] poskytuje funkce směrovače a lze jej považovat za dostačující substitut.

Diagram experimentálního pracoviště zobrazuje Obrázek 3.1. Zde je naznačen směr komunikace mezi jednotlivými uzly realizované topologie a jejich IP adresy. V diagramu jsou stanice útočníka i uživatele vyobrazeny jako dva odlišné stroje, avšak se jedná o dva virtuální stroje lokalizované uvnitř jednoho fyzického zařízení. Raspberry Pi disponuje Wi-Fi přijímačem, který dovoluje bezdrátové připojení k zařízení Mikrotik. Toto spojení zde není nutné využít, avšak bylo vhodné jej naznačit jako dostupné. Hlavním zaměřením tohoto přijímače je monitorování okolní bezdrátové komunikace.



Obr. 3.1: Diagram experimentálního pracoviště

Kompletní přehled použitých zařízení a jejich hardwarových specifikací zde doplňuje Tabulka 3.1. Tato tabulka obsahuje název zařízení, v tabulce označené jako uzel, instalovaný operační systém, velikost operační paměti RAM a osazený procesor. U procesoru je vždy uvedený počet jader, architektura a typ.

Tab. 3.1: Hardwarové specifikace komunikujících uzlů vytvořené topologie

uzel [-]	Operační systém [-]	RAM [MB]	CPU [-]
VM útočník	Linux Kali 5.7.0-kali1-amd64	2048	Dual-Core AMD RYZEN 5 3600 3,6 GHz
VM uživatel	Linux Ubuntu 5.4.0-52-generic	2048	Dual-Core AMD RYZEN 5 3600 3,6 GHz
Mikrotik hAP ac^2	RouterOS	128	Quad-Core ARM 32bit IPQ-4018
Raspberry Pi 4 B	Raspberry Pi OS 5.4.72-v7l+	4096	Quad-Core ARM v8 Cortex-A72

Doplněním popisu realizovaného experimentálního pracoviště je fotografie pracoviště, viz Obrázek 3.2. Jak lze z fotky určit, Raspberry Pi je rozšířeno o USB síťový adaptér, skrze který je spojený jedním metalickým kabelem k přístupovému bodu Mikrotik. Rozšíření bylo přidáno z důvodu, kdy by bylo nutné připojit Raspberry Pi zároveň skrze metalický kabel i Wi-Fi. Mikrotik je dále spojený dalším metalickým kabelem k osobnímu počítači, na kterém je spuštěný systém útočníka, tedy Kali Linux, spolu s uživatelem, Ubuntu Linux.

Pro přesné splnění uvedené topologie v diagramu pracoviště, bylo nutné provést několik změn se síťovými adaptéry virtuálních zařízení. Správcem virtuálních strojů byl použit program Oracle VM VirtualBox. Síťové rozhraní každého virtuálního stroje bude nastaveno jako síťový most. Tento síťový most odkazuje na integrovanou síťovou kartu fyzického počítače, se kterou je metalickým kabelem připojena k přístupovému bodu Mikrotik. Mikrotik slouží pro jednotlivé stroje jako DHCP server a Raspberry Pi od něj získá IP adresu. IP adresy pro virtuální stroje byly nastavené jako statické. Oba virtuální stroje, útočník i uživatel jsou v různých sítích. Toto nastavení bylo nutné, aby veškerý provoz byl cílen na jejich výchozí bránu, Mikrotik, a zde zrcadlen na port s Raspberry Pi.

3.1.1 Srovnání systémů detekce kybernetických útoků

Tato kapitola popisuje IDS/IPS systémy, které byly vybrány a otestovány jako vhodné pro splnění cílů diplomové práce. Jedná se o systémy:

- Arpwatch - sledování ARP dotazů a zjištění nových zařízení v síti,
- Kismet - IDS systém pro bezdrátové komunikace,
- Suricata/Snort - oba systémy nabízí funkce IDS i IPS.

Systémy Suricata i Snort nabízí velmi podobné možnosti. Při testování hardwarového vytížení při monitorování sítě a zachycení útočníkem generovaného incidentu

Obr. 3.2: Fotografie experimentálního pracoviště

byly zaznamenány nároky na procesor (CPU) a operační paměť (RAM) zařízení Raspberry Pi. Útočník generoval útok záplavou ICMP paketů. Oba systémy pracovaly jako IDS zařízení. Pravidla pro monitorování sítě byla využita ta, která jsou volně poskytována samotnými organizacemi. Na základě výsledků byl vybrán systém Suricata verze 6.0.0.0. Převážnou váhu při rozhodování nesla také skutečnost, že systém Suricata umožňuje zpracování příchozích dat ve více vláknech. Samotné zpracování je tedy rychlejší a dokáže zpracovat více dat než systém Snort. Výsledky měření těchto dvou systémů obsahuje Tabulka 3.2, kde jsou zapsaný hodnoty i zbylých vybraných systémů. Hodnoty v tabulce představují průměr z naměřených hodnot při sledování Linuxového softwaru *top*.

Během testování softwaru **arpwatch** verze 2.1a15 bylo zjištěno několik rozdílností od běžného použití například na Linux Debian. Dle internetových návodů a fór je uváděno, že programu arpwatch zapisuje do souboru /var/log/messages. Při použití operačního systému Raspberry Pi OS dochází ke změně a arpwatch zapisuje do souboru **/var/log/syslog**. Nejvýznamnější problém však představuje skutečnost, kdy ARP protokol komunikuje pouze na druhé vrstvě modelu ISO/OSI. Aktuální nastavení experimentálního pracoviště tedy nedovoluje provedení ARP spoofing

Tab. 3.2: Hardwarové nároky vybraných systémů detekce

Systém a verze	Vytížení CPU [%]	Vytížení RAM [%]
Suricata 6.0.0.0	23,7	1,2
Snort 2.9.7.0 GRE	28,3	2,7
arpwatch 2.1a15	0,7	1,3
KISMET 2020-00-GIT	4,1	0,5
KISMET chromium web browser	42,9	5,4
Python skript	1,3	0,5

útoku z důvodu, kdy ARP pakety neprochází do jiné sítě. Úskalím je, že ze stejného důvodu nyní nedochází k přeposílání ARP paketů na směrovač a opakování těchto paketů na port s Raspberry Pi, aby došlo k jejich detekci. Opravu tohoto problému představuje přidání dalšího fyzického zařízení, kdy dojde ke sjednocení všech zařízení do jedné sítě a útok ARP spoofing již bude realizovatelný a detekovatelný. Do sítě bylo přidáno další fyzické zařízení v roli uživatele. Jednalo se o zařízení s operačním systémem s distribucí Linux. Toto zařízení bylo spojeno metalickým kabelem s Mikrotik přístupovým bodem. Z virtuálního stroje Kali byl generovaný útok ARP spoofing, který byl detekován na Raspberry Pi. V této situaci bylo měřeno hardwarové vytížení softwarem arpwatch a hodnoty obsahuje Tabulka 3.2.

Jako další byl testován síťový detektor a IDS systém **Kismet**. Jedná se o systém zaměřený na monitorování komunikace na bezdrátové síti. Aby bylo možné tento systém použít na zařízení Raspberry Pi, je nutné několik úprav. Instalace systému Kismet musela být provedena ze zdrojového kódu lokalizovaného v oficiálním GIT repozitáři skupiny Kismet Wireless. Pro spuštění nástroje Kismet bylo nutné uvést bezdrátový přijímač zařízení Raspberry Pi 4 do monitorovacího módu. Při ověření dostupných funkcí adaptéru nebyla funkce monitorování vypsána. Jedná se o nevhodnou konfiguraci ovladačů tohoto adaptéru nainstalovaných v zařízení Raspberry Pi. Bylo tedy nutné nainstalovat balíček Nexmon, který představuje soubor „záplat“ pro zařízení Raspberry Pi, který dovoluje uvést bezdrátový adaptér do monitorovacího módu. Tento balíček je určen konkrétně pro Broadcom čip, který je v Raspberry Pi využívaný. GIT repozitář Secure Mobile Networking Lab, zkráceně seemoo-lab, obsahuje návod pro instalaci Nexmon balíčku, spolu s podporovanými zařízeními a jejich verzemi operačních systémů. Na základě operačního systému a čipu síťového adaptéru byla vybrána verze firmwaru, která byla nainstalovaná. Konkrétně se jedná o čip **bcm43455c0**, operační systém **Raspberry Pi OS Kernel 5.4** a verzi firmwaru **7_45_206**. Po úspěšné instalaci a změně starých ovladačů síťového adaptéru za nové, již bylo možné adaptér uvést do monitorovacího módu. Tato skutečnost následně vedla k úspěšnému spuštění IDS systému Kismet. Hodnoty v Tabulce 3.2

byly naměřeny při monitorování síťového provozu z bytu panelového domu. Finální podoba detektoru nebude využívat grafické rozhraní tohoto systému. Dojde pouze ke spuštění systému Kismet z programovacího jazyka Python a čtení generovaných zpráv a oznámení.

Posledním testovaným byl skript psaný v programovacím jazyce Python. Jedná se o demonstraci, která má za cíl přiblížit možné hardwarové vytížení při využívání tohoto programovacího jazyka. Python byl vybrán na základě obliby mezi širokou veřejností a pozitivního ohlasu při jeho užití. Další rozhodující faktor představovalo IDE Thonny, které je součástí systému Raspbian. Díky tomuto IDE je možné programovat v jazyce Python bez nutnosti instalování dalších programů třetích stran. K tvorbě programového vybavení detektoru bylo použito IDE Thonny spolu s verzí 3.7.3 programovacího jazyku Python. Hodnoty v Tabulce 3.2 představují vytížení při spuštěném systému Kismet a odesílání oznámení o detekovaném Deautentizačním útoku. Oznámení je realizováno e-mailem.

3.1.2 Scénáře realizace a detekce útoků

Obsahem této kapitoly je postup realizace jednotlivých útoků, které byly popsané v teoretické části diplomové práce. Jedná se tedy o popis potřebných nástrojů a konkrétních příkazů sloužících ke spuštění útoku. Útoky budou realizované ze zařízení s operačním systémem Kali Linux, konkrétně tedy ze stanice útočníka v experimentálním pracovišti. Realizace těchto útoků je nutná ke zjištění a ověření možných způsobů, jak daným útokům zabránit a podrobně otestovat použité systémy. Vybrané útoky lze provést bez nutnosti nákladné přípravy. Převážně je dostačující pouze stažení a instalace vhodného nástroje. Jedná se tedy o velmi reálné riziko v lokální síti. Pro detekci útoku je předpokládána síť pokrývající malou firmu.

Provedení útoků cílených na bezdrátová zařízení je obdobné. Rozdílem je pouze nutnost disponovat s vhodným bezdrátovým adaptérem podporujícím monitorovací mód. V současné době se na trhu vyskytuje množství síťových adaptérů, které nepodporují tento monitorující mód. Vybraný adaptér pro realizaci útoků byl Qualcomm Atheros AR9271 viz kapitola 3.1. Bezdrátový adaptér je tedy nutné uvést do monitorovacího módu, což vytvoří nové rozhraní. Použitým nástrojem byl *airmon-ng*, který je součástí sady nástrojů *aircrack-ng*. Tato sada je součástí Kali Linux.

Podvržení ARP zpráv

Útok byl realizován za pomocí sady nástrojů *dsniff*, konkrétně nástroje *arpspoof*. Tento balíček je nutné stáhnout a nainstalovat. Spuštění útoku je následující:

```
kali@kali:~# sudo arpspoof -i [jméno rozhraní] -t [adresa Oběti] -r [adresa výchozí brány]
```

Tímto způsobem dojde ke konstantnímu oznamování změny MAC adresy pro adresu výchozí brány za MAC adresu útočníka. Veškerá komunikace, kterou Oběť odesílá, nyní prochází přes stanici útočníka. Cílem nebylo realizovat útok Man-in-the-Middle, proto není nutné tento útok cílit i na výchozí bránu sítě. Při současné podobě experimentálního pracoviště je nutné připojit nové fyzické zařízení do společné sítě s útočníkem. Důvodem je přeposílání ARP paketů skrz porty směrovače viz kapitole 3.1.1, kde je tento problém popsán.

Detekce útoku probíhá pomocí IDS nástroje *arpwatch*. Zaznamenaný útok je zapisován do logů. V tomto případě jsou logy kontrolovány a při zjištění oznámení útoku dojde k provedení příslušné akce.

Podvržení linkové adresy

Pro podvržení linkové adresy bude využitý nástroj *macchanger*. Tento nástroj byl již součástí použitého operačního systému Kali Linux. V případě potřeby je tento nástroj možné nainstalovat ve stejnojmenném balíčku. Změna MAC adresy probíhá pomocí příkazu:

```
kali@kali:~# sudo macchanger -m [nová MAC] [cílové rozhraní]
```

Dojde tedy k nastavení specifikované MAC adresy konkrétnímu síťovému rozhraní. Možné je také nechat nástroj nastavit MAC adresu náhodně.

Detekci útoku je možné založit na kontrole přenášených paketů a kontrole páru MAC a IP adresa. Pokud nastane situace, že bude použita jedna IP adresa u různých MAC adres, dojde k vyhodnocení útoku z důvodu změnění MAC adresy jedním zařízením. Také může nastat situace, kdy se v síti nachází zařízení se stejnou MAC adresou, ale jinou IP adresou. Zde se jedná o útočníkem záměrně změněnou MAC adresu na adresu patřící již do sítě připojenému zařízení. Tuto detekci však poskytuje i nástroj *arpwatch*, který si ukládá páry IP a MAC adres. Při změně MAC adresy dojde k porušení uloženého páru adres a dojde k ohlášení této změny.

Přeskakování virtuální LAN

Přeskakování virtuální LAN, neboli VLAN hopping útok lze provést pomocí nástroje *Yersinia*. Jedná se o nástroj zaměřený na útoky, testování či analýzu, jejichž cílem jsou protokoly linkové vrstvy síťového modelu ISO
OSI. Tento nástroj lze používat pomocí terminálu, ale nabízí i přehledné grafické prostředí, které bude pro provedení útoku využito. *Yersinia* však není součástí systému Kali Linux a je tedy nutné ji prvně nainstalovat. Instalace probíhá ze stejnojmenného balíčku. Po spuštění v grafickém rozhraní nástroj naslouchá na síti a zachytává

příslušné rámce, které lze využít k podporovaným útokům. Spuštění se provede následujícím příkazem:

```
kali@kali:~# sudo yersinia -G
```

Po spuštění nástroje je nutné přejít do záložky DTP (Dynamic Trunking Protocol). Z této záložky je nutné spustit *enable trunking* pomocí tlačítka *launch attack*. Po spuštění *enable trunking* začne *Yersinia* vysílat požadavky na zvolení útočníka jako *trunk*. Nyní je možné přejít do záložky *802.1Q* a spustit *sending 802.1Q double enc. packet*. Tímto dojde k označení odesílaných rámců dvěmi štítky a útočník takto může komunikovat napříč všemi VLAN tak, jako by byl sám jedním z přepínačů v lokální síti. Tento útok však není možné provést z důvodu DTP protokolu, který je proprietárním pro zařízení od společnosti CISCO.

Detekci tohoto útoku je možné založit na neustálém vysílání DTP rámců útočníkem. Dojde-li k zachycení většího množství DTP rámců, lze zdroj vysílání označit za útočníka. V praxi se nedoporučuje využívat DTP protokol, a proto by nemělo být možné jeho zneužitý.

Pro cíle diplomové práce tento útok nebude realizovaný z důvodu předpokládané zabezpečované infrastruktury. Předpokladem je lokální síť nerozdělená do více virtuálních lokálních sítí.

Zahlcení směrovací tabulky CAM

Realizace útoku zahlcením směrovací tabulky CAM probíhá pomocí nástroje *macof*. Tento nástroj je obsažen v balíčku *dsniff*, který byl také použitý pro instalaci nástroje *arpspoof*. Ke spuštění tohoto nástroje je nutné určit použité rozhraní parametrem *i* a adresu Oběti parametrem *d*. Výsledný příkaz má následující strukturu:

```
kali@kali:~# sudo macof -i [cílové rozhraní] -d [IP adresa Oběti]
```

Po spuštění příkazu dochází k neustálému vysílání záznamů o nových MAC adresách. Takto spuštěný útok je nutné manuálně zastavit. Výsledkem je zaplnění CAM tabulky směrovače MAC adresami.

Pro detekci tohoto útoku lze využít systém Suricata. Tento systém bude aktivně naslouchat provozu uvnitř lokální sítě. Realizovaný útok bude spojený s definovaným pravidlem systému Suricata a dojde k oznámení a zastavení probíhajícího útoku.

Útok na Spanning Tree Protocol

Jedná se o útok realizovatelný nástroje *Yersinia*, stejně jako tomu bylo u útoku Přeskakování virtuální LAN 3.1.2. Z tohoto důvodu zde nebude popsána instalace a spuštění nástroje. Rozdílem je vybraná záložka nástroje *Yersinia*, která je v tomto

případě STP. Z této záložky je nutné zvolit *Claiming Root Role* po stisku tlačítka *launch attack*. Po spuštění dojde ke změně kořenového zařízení, kterým bude nyní útočníkovo zařízení.

Detekce útoku na Spanning Tree Protocol je obtížná z důvodu, kdy informace o změně kořenového směrovače mohou být legitimní. V takovém případě by mohlo docházet k chybnému vyhodnocení útoku. Vhodným řešením je tedy konfigurovat kořenový směrovač manuálně a nastavit na zařízení pravidlo, které bude ignorovat veškerá oznámení o změně kořenového směrovače. Detekci útoku by však bylo možné založit na získávání BPDU rámců. Pokud by došlo v krátkém časovém okamžiku k několika takovýmto oznámením, lze vypsat várování o možném útoku.

I zde se jedná o útok, který nebude uskutečněný na realizovaném experimentálním pracovišti. Důvodem je použití STP protokolu, který je výhodný pro velké sítě a tedy pro malou firemní síť je tento protokol téměř nevyužitelný.

Odposlouchávání rámců Linkové vrstvy

Tento útok je založený na Podvržení ARP zpráv a následné realizaci Muže uprostřed (MITM). Samotné provedení závisí na úspěšné změně ARP tabulky Oběti. Postup realizace je tedy stejný, viz scénář 3.1.2. Pro monitorování zachycených dat lze využít nástroj Wireshark. Dále je nutné nastavení IPtables systému tak, aby příchozí data přeposílal legitimnímu směrovači uvnitř sítě. Veškeré tyto úkony však lze zajistit pomocí nástroje *Ettercap*. Tento nástroj naslouchá komunikujícím zařízením přes vybrané rozhraní a dovolí útočníkovy zvolit Oběť útoku. Pro spuštění nástroje Ettercap v grafickém rozhraní slouží příkaz:

```
kali@kali:~# sudo ettercap -G
```

Detekce odposlouchávání rámců Linkové vrstvy je tedy založena na detekci uskutečněného útoku Podvržení ARP zpráv. Implementovaný detekční systém ARPwatch detekuje Podvržení ARP zpráv a na této detekci dojde k samotnému oznámení.

Zneužití Cisco Discovery protokolu

Jedná se o záplavový útok realizovaný nástrojem *Yersinia*. Popis nástroje je obsažený v předchozích scénářích a nebude tu opakován. Pro realizaci tohoto útoku je nutné pracovat se záložkou označenou CDP. Po stisknutí tlačítka *launch attack* je nutné vybrat možnost *flooding CDP table*.

Z důvodu, že se jedná o záplavový útok, je detekce tohoto útoku možná na základě kontrolování síťového provozu. Detekce je možná pomocí systému Suricata. Tento nástroj zjištění útoku oznámí a umožní zastavení odhaleného útoku.

Realizace tohoto útoku však není na experimentálním pracovišti možná. Důvodem je absence směrovačů Cisco, které tento protokol využívají.

Záplava ICMP

Realizace útoku Záplavou ICMP probíhá pomocí nástroje *hping3*. Tento nástroj není součástí použitého operačního systému Kali Linux a je tedy nutné jej nainstalovat pomocí stažení stejnojmenného balíčku. Spuštění útoku probíhá pomocí příkazu:

```
kali@kali:~# sudo hping3 [IP adresa oběti] --icmp --faster
```

Parametr *–icmp* představuje použitý protokol a parametr *–fast* počet odeslaných paketů za vteřinu. Pro parametr *–fast* se jedná o rychlost 10 paketů za vteřinu a parametr *–faster* 100 paketů za vteřinu.

Detekce tohoto útoku probíhá pomocí nástroje Suricata, který tento záplavový útok je schopný detekovat. Realizovaná detekce je založená na definovaném pravidle pro klasifikaci útoku. V případě tohoto útoku je možné vytvořit pravidlo do Firewallu směrovače Miktoritik na blokování zdrojové IP adresy, protože zde nedochází k jejím změnám.

Útok Smurf

Útoku Smurf je také realizovatelný nástrojem *hping3*, jako tomu bylo předešlému útoku Záplavou ICMP 3.1.2. Příkaz k provedení útoku je také obdobný příkazu pro Záplavu ICMP. Změnou je však uvedená IP adresa cíle, což v tomto případě se jedná o všesměrovou adresu. Nutné je upravit zdrojovou adresu, což je realizováno parametrem *-a*. Příklad výsledného příkazu pro realizaci útoku je následující:

```
kali@kali:~# sudo hping3 [všesměrová adresa] -a [IP adresa oběti] --icmp --faster
```

Protokol je určený parametrem *–icmp* a *–fast* počet odeslaných paketů za vteřinu.

Detekce tohoto útoku probíhá pomocí nástroje Suricata, který tento záplavový útok je schopný detekovat. Realizovaná detekce je založená na definovaném pravidle pro klasifikaci útoku. Tento útok má stejné charakteristiky jako Záplava ICMP, rozdílem je změna zdrojové adresy za adresu oběti a cílovou adresou je všesměrová adresa. Na základě těchto informací lze detekci upravit tak, aby docházelo ke kontrole cílové IP adresy v případě, že dojde k detekci útoku Záplavou ICMP.

Vyčerpání DHCP

Vyčerpání DHCP serveru lze realizovat pomocí nástroje *Yersinia* a *DHCPig*. Popis nástroje *Yersinia* je popsaný v předchozích scénářích a nebude tu opakován. Pro realizaci tohoto útoku je nutné pracovat se záložkou označenou DHCP. Po stisknutí

tlačítka *launch attack* je nutné vybrat možnost *sending DISCOVER packet*. *DHCPig* představuje nástroj psaný v jazyce Python. Ke spuštění slouží příkaz:

```
kali@kali:~# sudo pig.py [cílové rozhraní]
```

Následně dojde k vysílání dhcp discover zpráv na vybrané rozhraní. Nástroj čeká na odpověď DHCP serveru, čímž dojde k jeho zjištění. Poté dojde k zaplavení DHCP serveru a vyčerpání dostupných IP adres. K realizaci tohoto útoku byl využitý nástroj *Yersinia*.

Tento útok spadá do kategorie záplavových útoku, detekce je tedy možná na základě kontrolování síťového provozu a počítání přijatých DHCP zpráv. DHCP protokol komunikuje na porty s číslem 67 a 68. Je nutné určit maximální hranici DHCP discover zpráv za časový úsek. Po překročení stanovené hranice dojde k oznámení možného útoku a provedení příslušné akce. Jedná se tedy o vytvoření pravidla v detekčním systému Suricata.

Deautentizační útok

Deautentizační útok na bezdrátové sítě lze provést pomocí nástroje *aireplay-ng* z balíčku *aircrack-ng*. Pro realizaci tohoto útoku je nutné znát BSSID přístupového bodu a MAC adresu Oběti. Tyto informace lze zjistit pomocí nástroje *airodump-ng*. Kompletní příkaz pro realizaci útoku má následující podobu:

```
kali@kali:~# sudo aireplay-ng --deauth [počet deautentizačních rámců] -a [BSSID] -c [MAC
  ↪adresa Oběti] [cílové rozhraní]
```

Parametr *––deauth* oznamuje odesílání dautentizačních zpráv následovaný jejich celkovým počtem. Při zvolení hodnoty 0, dojde k neustálému odesílání deautentizačních zpráv. Parametr *–a* slouží pro identifikaci cílového přístupového bodu určeného pomocí BSSID. Následuje parametr *–c*, který definuje konkrétní Oběť připojenou k přístupovému bodu. Pokud není parametr *–c* definovaný, dojde k deautentizaci všech uživatelů. Posledním definovaným parametrem je cílové rozhraní, které však není v monitorovacím módu a musí být spuštěno na stejném vysílacím kanálu, který využívá Oběť.

Detekci útoku je možné založit na počtu přijatých deautentizačních zpráv, ovšem pouze při definování jejich většího počtu, nebo nepřetržitého odesílání. Při realizaci tohoto útoku došlo k vyslání deseti deautentizačních zpráv a detekce je založena na nástroji Kismet. Po detekci prvního rámce dochází k oznámení o odpojení všech uživatelů a možném ukončení zařízení. Další zjištěné deautentizační zprávy vyvolají oznámení o probíhající záplavě deautentizačními či disociačními zprávami.

Falešný přístupový bod

Pro realizaci tohoto útoku lze využít velké množství nástrojů. Zvolenými nástroji jsou *websploit* a *airbase-ng*, převážně pro jejich snadné spuštění a manipulaci. Nástroj *websploit* není ve výchozím stavu obsažený v systému Kali Linux a je tedy nutné jej nainstalovat. Spuštění probíhá vyvoláním tohoto nástroje přímo z konzole. Protože se jedná o celý framework, je nutná navigace napříč celým tímto nástrojem. Pro realizaci útoku falešného AP byl vybrán nástroj *airbase-ng* z důvodu snadného spuštění útoku. Spuštění útoku probíhá s následujícími parametry:

```
kali@kali:~# sudo airbase-ng -e [SSID] -c [číslo kanálu] [rozhraní]
```

Parametr *–e* značí název podvrženého AP a parametr *–c* dovoluje určit cílový vysílací kanál. Tyto údaje se musí shodovat s původním AP. Posledním vybraným parametrem je určení rozhraní, které budou vysílat oznámení a je spuštěno v monitorovacím módu. Monitorovací mód je zde nutný z důvodu možné reakce na příchozí data uživatelů a požadavky na připojení.

Detekce falešného bodu je prováděna pomocí IDS nástroje Kismet. Tento systém poskytuje detekci falešných AP na základě kontroly vysílaného SSID a definovaných MAC adres zařízení, která toto SSID mohou vysílat. Dostupné sítě jsou neustále monitorovány a při zjištění nového přístupového bodu s parametry stráženého AP dojde ke generování oznámení o falešném AP.

Útok Karma

Realizování útoku Karma lze docílit pomocí nástroje *airbase-ng*, nebo nástroje *Simple Karma Attack*. *Simple Karma Attack*, neboli SKA představuje Shell skript, který slouží pro realizaci Karma útoku a dovoluje také realizovat útok Falešného AP. Po stažení nástroje z GitHub a spuštění je nutné vybrat rozhraní použité pro útok. Následně nástroj čeká na Oběť, která se bude dotazovat na dostupnost známé sítě. Jakmile dojde k odchycení tohoto dotazu, nástroj nastaví své SSID i kanál na odpovídající hodnoty. Oběť je následně připojena na falešné AP. Nástroj dále přesměruje veškeré HTTP dotazy na falešné stránky a zachytává Obětí zadané údaje. Útok je pak nutné manuálně ukončit.

Při použití nástroje *airbase-ng* je nutné nastavit móde, který je definovaný parametrem *–P*. Tento parametr určí, že vytvořený přístupový bod bude odpovídat na veškeré dotazy o dostupnosti hledaného zařízení. Dále je nutné definovat i parametr *–C* s hodnotou ve vteřinách. Tento parametr určí, jak dlouho po odchyceném dotazu o dostupnosti od uživatele bude falešný přístupový bod oznamovat dotazované ESSID. Následně je vhodné určit kanál, na kterém bude falešné AP vysílat, pomocí parametru *–c* a čísla kanálu. Další parametr *–y* zakáže falešnému AP odpovídat

na obecné dotazy o tom, které AP jsou v dosahu dotazovaného zařízení. Poslední parametr určí rozhraní, které pracuje v monitorovacím módu a bude použito pro vysílání. Výsledný příkaz má tedy následující strukturu:

```
kali@kali:~# sudo airbase-ng -P -C [vteřiny] -c [číslo kanálu] -y [vybrané rozhraní]
```

Detekce tohoto útoku je založena na kontrole dostupnosti dotazovaného AP a kontrole, zda nedošlo k odpovědi na tento dotaz, nebo kontrola odpovědí na neexistující AP od jednoho zařízení za krátký časový úsek. Systém Kismet oznámí možné nebezpečí na základě chování dostupných zařízení například v situaci, kdy existující AP za provozu změní své vlastnosti. Tímto dojde k vyhlášení probíhajícího útoku Karma. Oznámení však neobsahuje konkrétně útok Karma, avšak indikuje podvržení AP a podvodné zosobnění daného AP.

3.2 Návrh programového vybavení detektoru

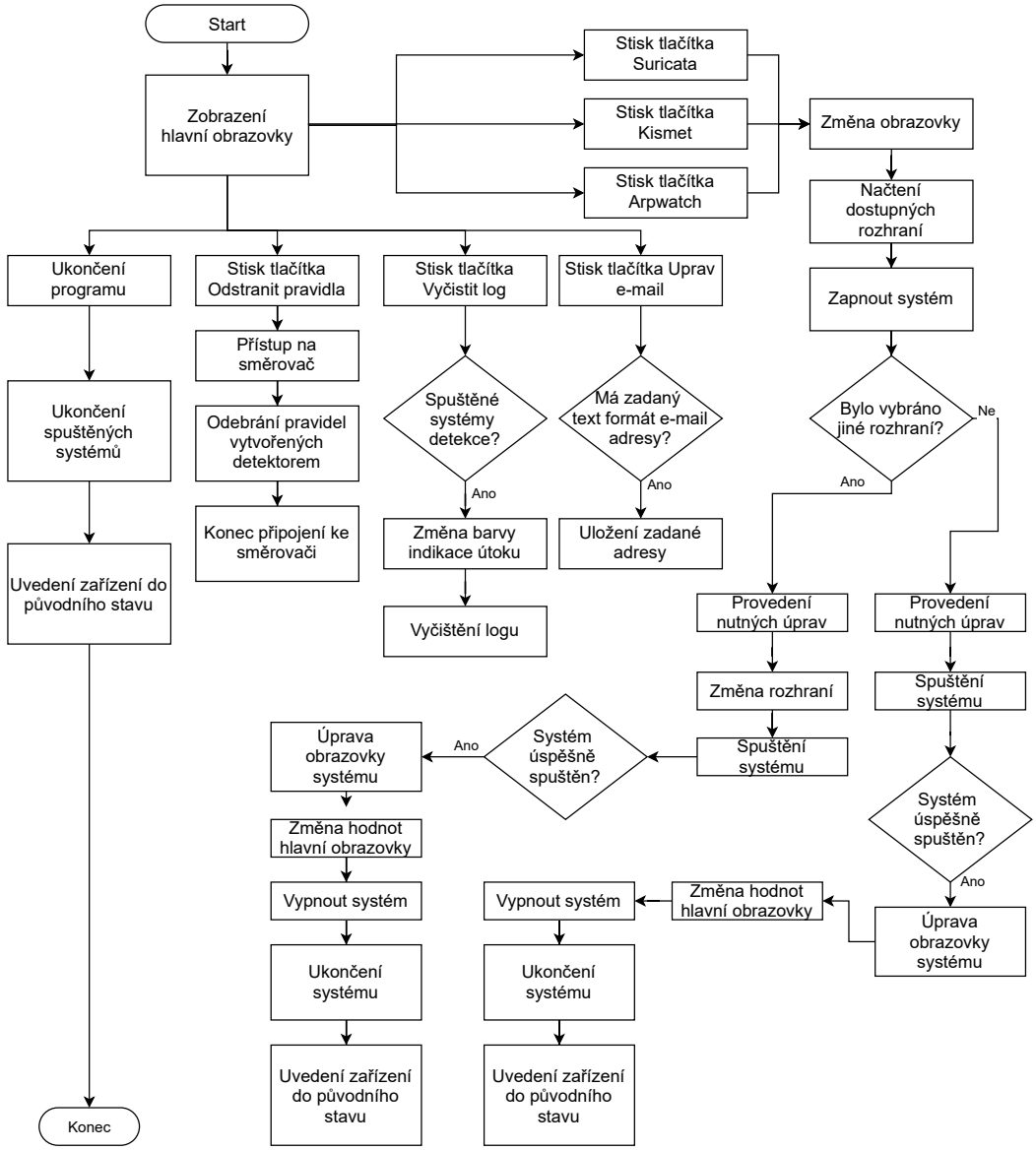
Hlavním přínosem diplomové práce je automatizovaný IDSIPS systém, který detekuje kybernetické útoky. V situacích, kdy je možné konkrétně určit zdroj útoku, dojde k jeho zablokování na základě IP adresy a přidání příslušného pravidla do firewallu směrovače. Tímto dojde k realizaci prevenční povahy detektoru. Uživatel programu detektoru je schopný zvolit konkrétní detekční systém a cílové rozhraní. Kýženým výsledkem je tedy jeden program, který bude ovládat vybrané detekční systémy. Detekované útoky a možné hrozby jsou vypsány do textového pole umístěného v hlavním menu programu, zapsány do logovacího souboru detekčního systému a oznámeny e-mailem. K odeslání e-mailu dojde pouze tehdy, pokud je dostupné připojení k síti Internet a nejedná se o již jednou oznámený útok. Opětovná oznámení jsou odesílána pouze jednou za dvě minuty z důvodu, aby nedocházelo k zahlcení určené e-mailové schránky.

Detekce kybernetických útoků je tedy založena na třech vybraných detekčních systémech. Také systém Suricata je spuštěn pouze v režimu IDS z důvodu zachování veškeré kontroly nad komunikací v režii vytvořeného programu. Systém Suricata je zaměřen na metalické spojení v síti společně se systémem Arpwatch. Arpwatch je však určený na kontrolu dat druhé vrstvy referenčního modelu ISO/OSI a tedy slouží pro detekci změny MAC adres, nově připojených zařízení a útoku Podvržení ARP zpráv. Na bezdrátovou komunikaci je zaměřený systém Kismet. U každého systému je uživatel schopný zvolit dostupné komunikační rozhraní s ohledem na určení daného systému. Pro systém Kismet je tedy možné zvolit pouze dostupná bezdrátová komunikační rozhraní. U systémů Suricata a Arpwatch lze zvolit pouze dostupná ethernetová rozhraní.

Program detektoru je nutné spouštět jako superuživatel. Práva superuživatele jsou zde vyžadována například pro uvedení bezdrátového rozhraní do monitorovacího módu. Samotný program disponuje grafických rozhraním pro zvýšení přehlednosti a intuitivní práce. Po spuštění programu dojde k zobrazení hlavní obrazovky. Tato obrazovka obsahuje přehledovou tabulku dostupných systémů detekce, jejich stav, zvolené rozhraní a zda došlo k detekci útoku. Dále je zde možnost nastavit e-mailovou adresu, na kterou jsou odesílána hlášení o detekovaných kybernetických útocích. Následuje část výběru detekčního systému. Tento výběr představují tři tlačítka, která přepnou hlavní obrazovku programu na obrazovku příslušnou vybranému systému. Každá tato obrazovka dovoluje vybrat komunikační rozhraní na kterém bude systém spuštěný. Dále je zde umístěno textové pole obsahující důležité soubory pro konkrétní systém a cesty k těmto souborům. Po návratu na hlavní obrazovku programu dojde k vizuální změně stavu systému, byl-li uživatelem zapnut. Další tlačítko v menu programu dovoluje uživateli odebrat veškerá přidaná pravidla do FW směrovače. Nedojde k odstranění všech pravidel, pouze těch, která byla přidána detektorem. Poslední částí této obrazovky je textové pole do které jsou zapsána hlášení o detekovaných kybernetických útocích. Pod tímto textovým polem je umístěno tlačítko po jehož stlačení dojde k vyčištění veškerého obsahu pole a změně barevné indikace ohlášení útoku.

Po zapnutí vybraného detekčního systému dojde k upravení konkrétní obrazovky a dovolí systém vypnout. Při zapnutí systému Kismet dojde nejprve k přepnutí bezdrátového rozhraní do monitorovacího módu a poté k zapnutí detekčního systému. Vypnutí tohoto systému má tedy opačný průběh, kdy dojde k vypnutí systému a uvedení bezdrátového rozhraní zpět do původního módu. Pokud jde jen o vypnutí jednoho nebo dvou systémů, je vhodné použít tento manuální postup. V případě, že je požadováno vypnutí celého programu detektoru, lze zmáčknout křížek okna programu. Tato akce je programem zachycena a dojde ke kontrole spuštěných systémů. Zjištěný spuštěný systém bude následně ukončen a veškeré potřebné změny pro správný chod systému uvedeny do původního stavu.

Z důvodu rozšíření konfigurovatelnosti programu a generalizace pro více prostředí je vytvořen konfigurační soubor. Tento soubor dovoluje uživateli nastavit parametry užívaného směrovače a emailového účtu určeného pro program detektoru. Lze nastavit podobu odeslaného e-mailu, parametry pro přihlášení ke směrovači a další parametry. Je tedy vhodné upravit hodnoty konfiguračního souboru před prvním spuštěním programu detektoru. Po spuštění programu jsou veškeré uvedené hodnoty načteny. Pro správný chod programu nesmí být tento konfigurační soubor odstraněn. Také nesmí být změněny názvy parametrů, jinak nedojde k načtení uvedených hodnot. Obrázek 3.3 zobrazuje grafickou podobu a funkce implementovaného programu.



Obr. 3.3: Diagram programu detektoru kybernetických útoků.

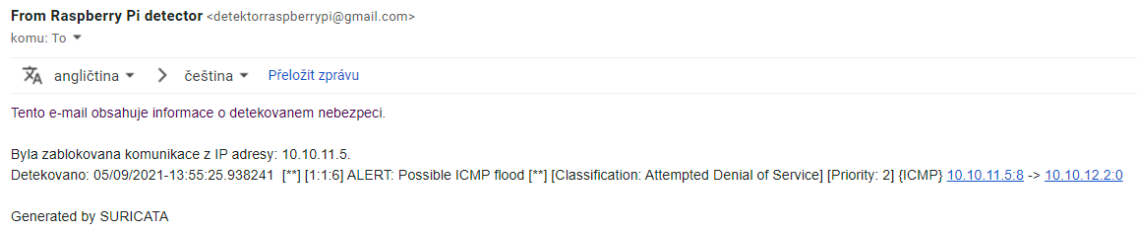
3.3 Vlastní implementace a testování detektoru

Pro praktickou realizaci programu detektoru byl zvolen programovací jazyk Python verze 3.7.3. Z důvodu výpočetního omezení zařízení Raspberry Pi bylo nutné vybrat vývojové prostředí (IDE), které neklade vysoké nároky na výpočetní prostředky zařízení. Nebylo možné vyvíjet program na výkonnějším zařízení kvůli snížení efektivity při testování. Kvůli těmto požadavkům bylo vybráno vývojové prostředí Thonny. Jedná se o prostředí, které již zařízení Raspberry PI obsahuje. Prostředí Thonny je blízce podobné náročnějším IDE, avšak poskytuje méně funkcí usnadňující práci. Pro vývoj programu detektoru bylo toto prostředí dostačující, avšak časově tak došlo k drobné prodlevě. Vývoj grafického uživatelského rozhraní probíhal za pomocí gra-

fického designeru Qt Designer. Tento designer nabízí intuitivní tvorbu uživatelského rozhraní s možností integrace a spojení s programovacím jazyce Python. Propojení vytvořeného grafického návrhu a programovacího jazyka bylo dosaženo knihovnou PyQt5. Knihovna dovoluje načíst návrhy uložené do souboru s koncovkou *.ui* bez nutnosti převodu na soubory s příponou *.py*.

Vytvořený program detektoru dovoluje spuštění vybraných systémů detekce sloužící pro zachycení a oznámení všech kybernetických útoků popsaných v kapitole 3.1.2. Pro dosažení tohoto výsledku bylo nutné přidat vlastní pravidla do seznamu pravidel systému Suricata. Konkrétně se jedná o pravidla pro detekci útoků *Záplava ICMP* a *Vyčerpání DHCP*. Konkrétní podoba pravidel je uvedena v předchozí kapitole 3.4. Na základě pravidla pro detekování záplavy ICMP je založena detekce útoku *SMURF*. Systém Suricata vyhodnotí příchozí rámce jako útok Záplavou ICMP, avšak cílem ICMP dotazů je všesměrová adresa. To vyvolá hlášení o útoku SMURF. K detekci ostatních útoků již slouží detekční systémy bez dodatečných úprav.

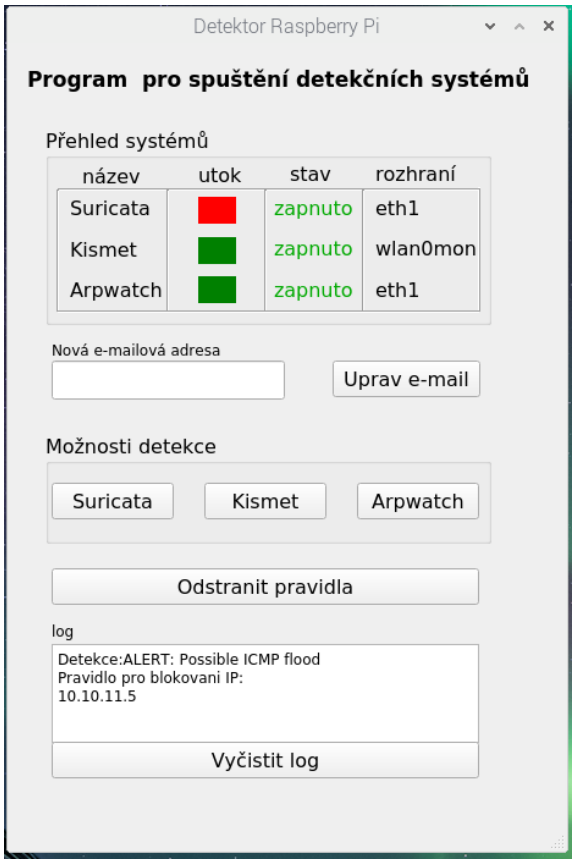
Veškerá oznámení o detekovaném kybernetickém útoku jsou odesílána e-mailem na uživatelem zvolenou adresu, zapsán do logovacího souboru nebo oznámený v hlavním menu programu. Hlášení jsou v případě odesílání e-mailem předané pomocí SSL protokolu na e-mailový server a není tak možné číst obsah odesílaného hlášení. Příkladem generovaného e-mailu je Obrázek 3.4. Odesílání e-mailů je omezené na časový úsek pro ta hlášení, která již byla oznámena. Jedná se o protiopatření, kdy by mohlo dojít k zahlcení cílové e-mailové schránky. Ke každému hlášení je přidán aktuální čas a na jeho základě je kontrolováno, zda dojde k opětovnému odeslání hlášení či nikoliv. Tomuto stavu docházelo například při detekci útoku *Zahlcení Směrovací tabulky CAM* 3.1.2. Opětovné oznámení výstrahy probíhá jednou za dvě minuty. Pokud nebyl detekovaný útok již jednou oznámen, dojde k odeslání hlášení.



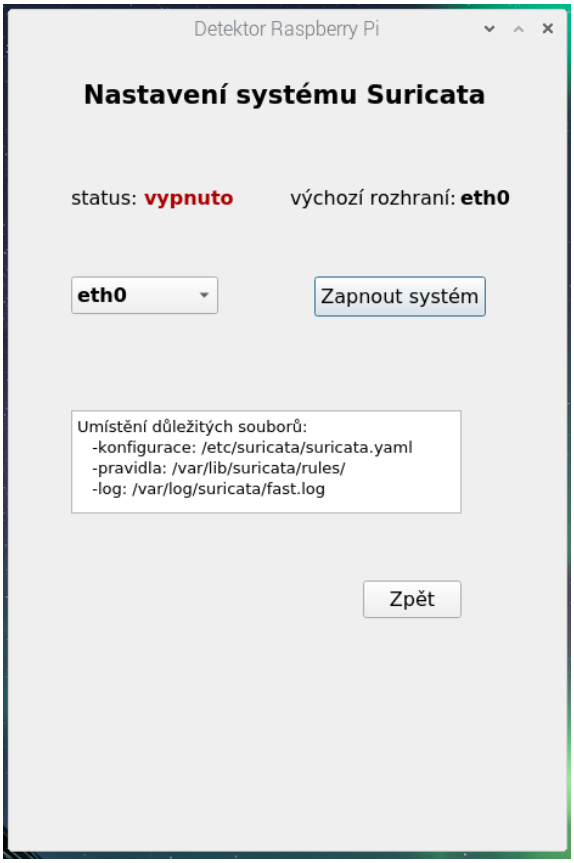
Obr. 3.4: Generované e-mailové hlášení detektoru

Při testování programu detektoru došlo systémem Suricata k vyhodnocení odchozí komunikace detektoru jako potenciálně škodlivé. Na základě této detekce bylo vytvořeno pravidlo blokování veškeré komunikace detektoru. Jednalo se o ojedinělou situaci, avšak bylo nutné této skutečnosti zabránit. Při tvorbě pravidla je zdrojová IP adresa u hlášení kontrolována. Pokud se shoduje s adresou, která náleží detektoru,

k vytvoření pravidla nedojde. Konečnou podobu hlavního menu detektoru znázorňuje Obrázek 3.5. V přehledové části okna lze spatřit stav *zapnuto* u všech tří vybraných systémů detekce. S tímto stavem je spojen sloupec *útok*. Pro vypnutý systém je barva pole šedá a pro zapnutý systém zelená. Pokud dojde systémem k detekci útoku, je barva pole změněna na červenou. Tímto dojde k vizuálnímu upozornění uživatele a zapsáním detekovaného útoku do textového pole umístěného v dolní části obrazovky. Po stisknutí tlačítka *vyčistit log* je změněna barva oznámení útoku zpět na zelenou a textové pole je vyčištěno. Uživatel tímto dává najevo, že detekovanou hrozbu vzal na vědomí a pokud je to nutné, podnikne potřebné akce. Toto pole také slouží pro ohlášení zjištěných chyb. Může se jednat o chyby při spouštění detekčního systému, odesílání hlášení e-mailem či připojení ke směrovači. Obrazovku nastavení a spuštění detekčního systému zobrazuje Obrázek 3.6.



Obr. 3.5: Hlavní okno programu detektoru oznamující detekovaný útok



Obr. 3.6: Obrazovka nastavení systému Suricata

Při zapnutí systému detekce na konkrétním rozhraní dojde k přepsání této hodnoty i do přehledové tabulky hlavní obrazovky programu. Uživateli je poskytnut list zařízení, která jsou aktuálně dostupná. Nejedná se tedy o pevně zadaný seznam. Takovéto řešení by bylo značně nepraktické a takřka nepoužitelné. Po stisknutí tla-

čítka *zapnout systém* na obrazovce systémů detekce dojde ke kontrole, zda se jedná o aktivní komunikační rozhraní či nikoliv. Pokud neexistuje záznam o odeslaných či přijatých datech daného rozhraní v souboru */proc/net/dev*, je vytvořeno informační okno obsahující tuto skutečnost. Tímto způsobem je uživatel obeznámen s faktem, že na daném rozhraní nebyla detekována žádná data a může se tak jednat o nepřipojené rozhraní. Oznámení je také vytvořeno v případě, že detektor není připojen k síti Internet a nebude tak možné odesílat e-mailová oznámení.

Konečný přehled dosažených výsledků poskytuje Tabulka 3.3. První sloupec tabulky obsahuje názvy kybernetických útoků, které jsou detailněji popsány v teoretické části této práce. Následující sloupec obsahuje informaci o tom, zda k detekci tohoto útoku docházelo bez potřebných úprav či tvorby vlastních pravidel vybraných systémů detekce. Poslední sloupec tabulky slouží jako přehled kybernetických útoků, které současné implementované řešení dokáže detekovat.

Dochází tedy převážně k plnění cílů IDS systémů. Cílem práce bylo také zamezení probíhajících útoků. K tomu dochází v případě útoku Záplavou ICMP. Jedná se o útok, při kterém lze konkrétně určit zdrojová IP adresa útočníka a lze tak útok zablokovat. Zde dochází ke kompletnímu blokování komunikace z dané IP adresy. Pro zamezení probíhajícího kybernetického útoku by bylo možné využít také blokování komunikace z daného síťového rozhraní. K tomuto řešení však nebylo přistoupeno z důvodu, kdy veškerá komunikace experimentálního pracoviště pochází právě z jednoho síťového rozhraní. Došlo by tak k blokování komunikace většiny uživatelských zařízení v lokální síti, což by vedlo k vysoké neefektivitě při současné podobě experimentálního pracoviště. Z toho důvodu byla implementována možnost blokování komunikace pouze na základě zjištěné IP adresy. Pro správné blokování komunikace však musel být přidán mechanismus, který rozhoduje o tom, jaké pravidlo bude do Firewallu přidáno. Pokud útok cílí na směrovač, jedná se o pravidlo kategorie *INPUT*. V případě, že je cílem jiné zařízení, bude přidáno pravidlo do kategorie *FORWARD*. Při útoku na směrovač dojde k zablokování pouze útočníkovi komunikace se směrovačem, avšak komunikace s jinými zařízeními bude nadále možná.

Detekce kybernetických útoků není omezena pouze na vybrané útoky a jejich scénáře. K detekci a oznámení útoků také dochází v případě, kdy systém Kismet zjistí shodu se svými pravidly detekce kybernetických útoků. Stejným způsobem se chová systém Suricata, avšak zde bylo nutné oznámení omezit. Suricata disponuje rozsáhlým seznamem komunitních pravidel, avšak všechny nejsou cílené na detekci kybernetických útoků a jsou roztříděny do skupin dle přiřazené priority. Program detektoru tedy oznámí pouze taká hlášení, která nesou prioritu dva a jedna. Pokud se jedná o hlášení s prioritou tři a čtyři, k oznámení nedojde. Toto rozhodnutí bylo učiněno na základě testování detekčního systému, kdy docházelo ke zbytečným

Tab. 3.3: Detekované kybernetické útoky

Scénáře kyb. útoků	Detektor v.1	Detektor v.2
Podvržení ARP zpráv	✓	✓
Podvržení linkové adresy	✓	✓
Zahlcení směrovací tabulky CAM	✓	✓
Odposlouchávání rámců linkové vrstvy	✓	✓
Záplava ICMP	✗	✓
Útok SMURF	✗	✓
Vyčerpání DHCP	✗	✓
Deautentizační útok	✓	✓
Falešný přístupový bod	✓	✓
Útok Karma	✓	✓

hlášením i falešným poplachům. V případě systému Arpwatch zde také dochází ke generování dodatečného oznámení, a to v situaci, kdy je do sítě přidáno nové zařízení. Během kontroly dosažených výsledků této práce bylo zjištěno oficiální vydání systému Snort 3. K vydání systému došlo v polovině ledna tohoto roku. Jedná se o systém disponující řadou vylepšení oproti systému Snort verze 2.9.8, jakou je třeba vícevláknové zpracování dat. Tato skutečnost by mohla vést ke změně detekčního systému Suricata, avšak bylo by nutné provést nová měření a testy. Jedná se však o možné zvýšení efektivity realizovaného detektoru.

3.4 Manuál ke spuštění programu detektoru

Tato kapitola popisuje možnosti spuštění programu detektoru. Popis je rozdělený do dvou částí, kdy první část je věnována popisu přenesení samotného programu detektoru. V tomto případě již uživatel musí mít nainstalované detekční systémy. Tento způsob je vhodný pro případ, kdy uživatel užívá zařízení Raspberry Pi s požadovaných operačním systémem a nechce ztratit vlastní nastavení a modifikace. Druhá část je věnována stažení obrazu operačního systému. Tento obraz obsahuje požadované detekční systémy a veškeré úpravy systému pro správný chod programu. Jedná se o doporučený postup, jak využít realizovaný program detektoru.

Užití samostatného programu detektoru

Program detektoru byl vytvořený jako samostatná (standalone) aplikace **detectorRaspberry** za pomocí programu *PyInstaller*. Výsledkem je tedy aplikace již

obsahující veškeré závislosti na použité externí knihovny. Vše je obsaženo v jednom adresáři nazvaném *detectorRaspberry*, ve kterém tento program také musí být spuštěný. Tento adresář obsahuje podadresář *logs* obsahující záznamy generované jednotlivými detekčními systémy. Uvnitř hlavního adresáře je také umístěný soubor *configDetector.yaml*. Tento soubor obsahuje veškerou konfiguraci definovatelnou uživatelem. Doporučené je pouze upravovat hodnoty jednotlivých polí, nikoliv samotnou strukturu a názvy polí. Tento konfigurační soubor zde musí vždy existovat. Vyžadované prerekvizity programu:

- práva superuživatele,
- IDS Suricata,
- auditorský systém Kismet,
- bezdrátové rozhraní pro monitorovací mód,
- systém Arpwatch,
- připojení k internetu.

Bez výše vypsaných požadavků nelze dosáhnout plné funkčnosti programu detektoru. Pro případ nutnosti upravení bezdrátového rozhraní pro uvedení do monitorujícího módu byl tento postup zmíněn v předešlé kapitole 3.1.1 části popisující systém Kismet. Výjimkou prerekvizit je přístup k internetu, kdy bude detektor stále plně funkční, avšak bez možnosti odesílání e-mailových oznámení o detekovaném.

Získaný komprimovaný adresář *detectorRaspberry.tar.gz* je nutné nejdříve extrahovat. Extrakci lze provést příkazem:

```
pi@raspberrypi:~ $ tar -xvzf detectorRaspberry.tar.gz
```

Takto dojde k extrahovaní adresáře do aktuální složky. Výsledkem je stejnojmenný adresář obsahující soubory potřebné pro správný chod programu a spustitelný soubor. Tento soubor je nutné spouštět jako superuživatel, aby samotný program mohl provádět veškeré potřebné akce a nedošlo k jeho omezení či nežádoucím chybám. Práva superuživatele jsou vyžadována například pro převod bezdrátového rozhraní do monitorovacího módu a plynulého chodu programu.

Před prvním spuštěním je vhodné upravit soubor *configDetector.yaml*. Tento konfigurační soubor obsahuje důležité informace o směrovači a používaném e-mailovém účtu. U směrovače je nutné nastavit jeho IP adresu a přihlašovací údaje, aby bylo možné přidávat pravidla do FW směrovače. Pro tuto úpravu slouží pole:

- **ipRouter** - IP adresa směrovače,
- **usernameRouter** - přihlašovací jméno uživatele směrovače,
- **passwordRouter** - heslo vybraného uživatele.

Druhá část, konfigurace e-mailu, obsahuje nastavení následujících polí:

- **emailSmtpServer** - adresa užívaného SMTP serveru,
- **emailServerPort** - číslo SSL portu,

- **emailSender** - e-mailová adresa pro odesílaní hlášení (slouží pro přihlášení programu do e-mailového účtu),
- **emailPassword** - heslo k e-mailovému účtu použitému pro odesílání hlášení,
- **emailReceiver** - e-mailová adresa příjemce generovaných hlášení,
- **emailMessageTemplate** - šablona hlášení o zjištěném nebezpečí.

E-mailová adresa příjemce může být změněna v hlavním menu programu a dojde pouze k jednorázové změně. Ke spuštění detektoru je vhodné přejít do samotného adresáře a spustit program detektoru příkazem:

```
pi@raspberrypi:~/detectorRaspberry $ sudo ./detectorRaspberry
```

Pro detekci útoků Záplavou ICMP a Vyčerpání DHCP je nutné přidat nové pravidla do souboru pravidel detekčního systému Suricata. Tato pravidla byla vytvořena s ohledem na průběh kybernetických útoků dle stanovených scénářů. Pro detekci Záplavou ICMP byla stanovena hranice deseti tisíc přenesených paketů za jednu vteřinu. Detekce Vyčerpání DHCP upřesňuje zdrojový a cílový port DHCP paketu a celkový počet přenesených paketů za jednu vteřinu. Jedná se o tato dvě pravidla:

```
alert icmp any any -> any any (msg:"ALERT: Possible ICMP flood"; threshold: type both,
  ↪track by_src, count 10000, seconds 1; icode:0; itype:8; sid:1; rev:1; classtype:
  ↪attempted-dos)
alert dhcp any 68 -> any 67 (msg:"ALERT: Possible DHCP starvation"; threshold: type both,
  ↪track by_src, count 1000, seconds 1; icode:0; itype:8; sid:11; rev:1; classtype:
  ↪attempted-dos)
```

Je nutné zmínit, že výsledný program lze spustit pouze na takovém operačním systému, ve kterém byl samotný program vygenerován. Žádoucí je tedy brát v úvahu cílovou platformu. V současné době je dostupná pouze jedna verze programu detektoru určena pro o operační systém Raspbian.

Užití obrazu operačního systému

Výše uvedený popis spuštění slouží pro případ, kdy byl předán pouze samotný program detektoru a uživatel již vlastní operační systém Raspbian se všemi prerekvizitami. Pro případ, kdy uživatel těmito prvky nedisponuje, byl vytvořený obraz operačního systému Raspbian obsahující všechny nutné prerekvizity. Uživatel si pouze stáhne komprimovaný archív s tímto obrazem systému. Pro použití tohoto obrazu je nutné vlastnit SD kartu a čtečku těchto SD karet. Vložení na SD kartu lze uskutečnit například pomocí programu **win32diskimager**. Tento program slouží pro práci s těmito obrazy disku. Uvnitř programu je nutné vybrat označení jednotky čtečky SD karet, stažený obraz operačního systému a spustit zápis na SD kartu. Po úspěšném zápisu na SD kartu je systém použitelný bez dalších příprav, stačí jen vložit SD kartu do zařízení Raspberry Pi a spustit.

Po spuštění systému je na ploše umístěna ikona programu detektoru nazvaná **Detector RaspberryPi**. Spuštění lze provést dvojklikem na ikonu programu. Poté dojde ke spuštění s právy superuživatele. Jedná se pouze o zástupce programu a pracovní složka je umístěna v domovském adresáři uživatele *pi*. Celá cesta k tomuto adresáři je */home/pi/python_code/*. Uvnitř tohoto adresáře jsou obsažené zdrojové kódy detektoru spolu s konfiguračním souborem, který je detailně popsaný v předcházející části této kapitoly. Dále je zde i složka s názvem *logs*, obsahující logy systémů detekce, a *dist*. Složka *dist* zde obsahuje vytvořený samostatný program detektoru jemuž je věnovaná předchozí část kapitoly.

Závěr

Diplomová práce byla zaměřena na vlastní návrh a implementaci detektoru kybernetických útoků využívající výpočetně omezené zařízení Raspberry Pi 4 typ B. Cílem byla úspěšná detekce a prevence kybernetických útoků bezdrátové i kabelové sítě zaměřených na linkovou a síťovou vrstvu modelu ISO/OSI. Teoretická část práce byla věnována popisu realizace, detekce a možnosti mitigace kybernetických útoků spadající do zmíněné kategorie. Následoval popis systémů detekce, jejich rozdělení a výběr současných detekčních systémů pro vlastní implementaci detektoru. Tímto byl analyzován současný stav problematiky detekce kybernetických útoků.

Praktická část práce byla zaměřena na tvorbu experimentálního pracoviště obsahující výpočetně omezené zařízení Raspberry Pi 4 typ B, směrovač Mikrotik a dvě virtuální uživatelská zařízení. Z důvodu omezeného výpočetního výkonu zařízení Raspberry Pi bylo provedeno srovnání hardwarových nároků dostupných detekčních systémů. Na základě výsledků byly vybrány systémy Suricata, Kismet a Arpwatch.

Před vlastní implementací programu detektoru byl vytvořen návrh programového vybavení detektoru popisující chování programu a jeho funkce. Cílem byla tvorba intuitivního programu dovolujícího uživateli výběr jednotlivých systémů detekce k čemuž přispívá i grafické rozhraní. Pro zobecnění programu detektoru byl vytvořený konfigurační soubor obsahující uživatelem volitelné parametry. Snazší orientaci v návaznostech funkcí programu detektoru umožňuje vlastní vývojový diagram.

Dle prvotního testování vlastní implementace detektoru bylo nutné přidat nová pravidla pro systém Suricata za účelem dosažení úspěšné detekce všech vybraných kybernetických útoků. Dále bylo nutné přidat rozhodovací mechanismy pro jednoznačné určení konkrétního útoku definovaného v této práci, avšak se snahou neomezit detekční schopnosti systému Suricata. Testování detekčních schopností implementovaného programu probíhalo dle definovaných scénářů kybernetických útoků. Úskalím byla prevence kybernetických útoků, kdy nebylo možné vybudovat prevenční mechanismus pro všechny stanovené kybernetické útoky. Jedná se převážně o podstatu daného kybernetického útoku, kdy není možné přesně určit zdroj tohoto útoku. V případě přesného určení zdroje útoku dochází k zablokování útočníkovy IP adresy ve firewallu směrovače. Dosažené výsledky splňují stanovené cíle diplomové práce.

Na závěr byla vytvořena dokumentace popisující spuštění realizovaného detektoru. Byly vytvořeny dva způsoby, z toho první představuje využití pouze samotného programu detektoru, avšak uživatel již musí vlastnit detekční systémy užívané v této práci. Druhou možností je stažení a instalace obrazu operačního systému Raspbian. V tomto případě musí uživatel disponovat SD kartou, na kterou operační systém umístí. Toto řešení již obsahuje veškeré prerekvizity pro spuštění programu detekce a již nejsou nutné další úpravy operačního systému.

Literatura

[1] VERSCHUREN, Jan, René GOVAERTS and Joos VANDEWALLE. 1993. ISO-OSI security architecture. PRENEEL, Bart, René GOVAERTS and Joos VANDEWALLE (eds.). Computer Security and Industrial Cryptography [online]. Berlin, Heidelberg: Springer Berlin Heidelberg, p. 179-192. Lecture Notes in Computer Science. Available at: http://link.springer.com/10.1007/3-540-57341-0_62

[2] HIRŠ, D.; MARTINÁSEK, Z. Přehled kybernetických útoků na linkové a transportnívrstvě. Elektrorevue - Internetový časopis (http://www.elektrorevue.cz), 2020, roč. 22, č. 1, s. 1-15. ISSN: 1213-1539

[3] XIA, Jing, Zhiping CAI, Gang HU and Ming XU. 2019. An Active Defense Solution for ARP Spoofing in OpenFlow Network. Chinese Journal of Electronics [online]. 28(1), 172-178. Available at: https://digital-library.theiet.org/content/journals/10.1049/cje.2017.12.002

[4] BHIRUD, S. G. and Vijay KATKAR. 2011. Light weight approach for IP-ARP spoofing detection and prevention. In: 2011 Second Asian Himalayas International Conference on Internet (AH-ICI) [online]. IEEE, p. 1-5. Available at: http://ieeexplore.ieee.org/document/6113951/

[5] BHAIJI, Yusuf. 2009. Understanding, Preventing, and Defending Against Layer 2 Attacks [online]. Available at: https://www.cisco.com/c/dam/global/en_ae/assets/exposaudi2009/assets/docs/layer2-attacks-and-mitigation-t.pdf

[6] BRUSCHI, D., A. ORNAGHI and E. ROSTI. 2003. S-ARP: a secure address resolution protocol. In: 19th Annual Computer Security Applications Conference, 2003. Proceedings [online]. IEEE, p. 66-74. Available at: http://ieeexplore.ieee.org/document/1254311/

[7] HOFFMAN, Chris. 2017. Why You Shouldn't Use MAC Address Filtering On Your Wi-Fi Router. How-To Geek [online]. Available at: https://www.howtogeek.com/204458/why-you-shouldn%E2%80%99t-use-mac-address-filtering-on-your-wi-fi-router/

[8] BUHR, Andrew, Dale LINDSKOG, Pavol ZAVARSKY and Ron RUHL. 2011. Media Access Control Address Spoofing Attacks against Port Security. In: Proceedings of the 5th USENIX Conference on Offensive Technologies

[online]. WOOT'11. San Francisco, CA: USENIX Association. Available at: http://dl.acm.org/citation.cfm?id=2028052.2028053

[9] HUANG, I-Hsuan, Ko-Chen CHANG, Yu-Chi LU and Cheng-Zen YANG. 2010. Countermeasures against MAC address spoofing in public wireless networks using lightweight agents. In: The 5th Annual ICST Wireless Internet Conference (WICON) [online]. Available at: https://ieeexplore.ieee.org/document/5452667

[10] FAN, Huipu, Yizhou DONG, Ming YU and Leonard TUNG. 2013. Security Threats against the Communication Networks for Traffic Control Systems. In: 2013 IEEE International Conference on Systems, Man, and Cybernetics [online]. IEEE, p. 4783-4788. Available at: http://ieeexplore.ieee.org/document/6722569/

[11] ALABADY, Salah A. Jaro. 2008. Design and Implementation of a Network Security Model using Static VLAN and AAA Server. In: 2008 3rd International Conference on Information and Communication Technologies: From Theory to Applications [online]. IEEE, p. 1-6. Available at: http://ieeexplore.ieee.org/document/4530276/

[12] LOMNICKÝ, Marek. Analýza a demonstrace vybraných L2 útoků [online]. Brno, 2009 [cit. 2019-10-02]. Dostupné z: http://hdl.handle.net/11012/53857. Diplomová práce. Vysoké učení technické v Brně. Fakulta informačních technologií. Ústav informačních systémů. Vedoucí práce Ondřej Ryšavý.

[13] BULL, Ronny L. ACritical ANALYSIS OF LAYER 2 NETWORK SECURITY IN VIRTUALIZED ENVIRONMENTS. 2016. PhD Thesis. CLARKSON UNIVERSITY. Available at: https://people.clarkson.edu/ bullrl/bullrl_dissertation.pdf

[14] XU, Tong, Deyun GAO, Ping DONG, Chuan Heng FOH and Hongke ZHANG. 2017. Mitigating the Table-Overflow Attack in Software-Defined Networking. IEEE Transactions on Network and Service Management [online]. 14(4), 1086-1097. Available at: http://ieeexplore.ieee.org/document/8057280/

[15] Catalyst 4500 Series Switch Cisco IOS Software Configuration Guide, 12.2(25)EW: Configuring Port Security. Cisco - Global Home Page [online]. Available at: https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst4500/12-2/25ew/configuration/guide/conf/port_sec.html

[16] Understanding and Configuring Spanning Tree Protocol (STP) on Catalyst Switches. 2006. Cisco Systems [online]. Available at: https://www.cisco.com/c/en/us/support/docs/lan-switching/spanning-tree-protocol/5234-5.html

[17] TREJO, Luis A., Rául MONROY and Rafael LÓPEZ MONSALVO. 2006. Spanning Tree Protocol and Ethernet PAUSE Frames DDoS Attacks: Their Efficient Mitigation [online]. , 1-13. Available at: https://www.semanticscholar.org/paper/Spanning-Tree-Protocol-and-Ethernet-PAUSE-Frames-%3A-Trejo-Monroy/008339f322de9564d8a74f96f7aee670f6ec0cd9

[18] MOHAMMADI, Shahriar and Hossein JADIDOLESLAMY. 2011. A Comparison of Link Layer Attacks on Wireless Sensor Networks. International Journal on Applications of Graph Theory In wireless Ad Hoc Networks And sensor Networks [online]. 3(1), 35-56. Available at: http://www.airccse.org/journal/graphhoc/papers/3111jgraph03.pdf

[19] YORK, Dan. c2010. Seven deadliest Unified Communications attacks. Burlington, MA: Syngress. Syngress seven deadliest attacks series.

[20] Cisco Discovery Protocol Configuration Guide, Cisco IOS Release 15M&T. Cisco Systems [online]. Available at: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/cdp/configuration/15-mt/cdp-15-mt-book/nm-cdp-discover.html

[21] Cisco CDP Advisory. Phenoelit [online]. Available at: http://www.phenoelit.org/fr/misc.html

[22] TANCESKA, Biljana, Mitko BOGDANOSKI and Aleksandar RISTESKI. Simulation Analysis of DoS, MITM and CDP Security Attacks and Countermeasures. Future Access Enablers for Ubiquitous and Intelligent Infrastructures [online]. p. 197-203. Available at: http://link.springer.com/10.1007/978-3-319-27072-2_25

[23] CDP (Cisco Discovery Protocol). Flylib [online]. Available at: https://flylib.com/books/en/3.418.1.78/1/

[24] UDHAYAN, J. and R. ANITHA. 2009. Demystifying and Rate Limiting ICMP hosted DoS/DDoS Flooding Attacks with Attack Productivity Analysis. In: 2009 IEEE International Advance Computing Conference [online]. IEEE, p. 558-564. Available at: http://ieeexplore.ieee.org/document/4809072/

[25] YIHUNIE, Fekadu, Eman ABDELFATTAH and Ammar ODEH. 2018. Analysis of ping of death DoS and DDoS attacks. In: 2018 IEEE Long Island Systems, Applications and Technology Conference (LISAT) [online]. IEEE, p. 1-4. Available at: https://ieeexplore.ieee.org/document/8378010/

[26] CHANG, R.K.C. 2002. Defending against flooding-based distributed denial-of-service attacks: a tutorial. IEEE Communications Magazine [online]. 40(10), 42-51. Available at: http://ieeexplore.ieee.org/document/1039856/

[27] HUBBALLI, Neminath and Nikhil TRIPATHI. 2017. A closer look into DHCP starvation attack in wireless networks. Computers & Security [online]. 65, 387-404. Available at: https://linkinghub.elsevier.com/retrieve/pii/S0167404816301262

[28] MUKHTAR, Husameldin, Khaled SALAH and Youssef IRAQI. 2012. Mitigation of DHCP starvation attack. Computers & Electrical Engineering [online]. 38(5), 1115-1128. Available at: https://linkinghub.elsevier.com/retrieve/pii/S0045790612001140

[29] KUMAR, Sanjeev. 2007. Smurf-based Distributed Denial of Service (DDoS) Attack Amplification in Internet. In: Second International Conference on Internet Monitoring and Protection (ICIMP 2007) [online]. IEEE, p. 25-25. Available at: http://ieeexplore.ieee.org/document/4271771/

[30] ZARGAR, Gholam Reza and Peyman KABIRI. 2009. Identification of effective network features to detect Smurf attacks. In: 2009 IEEE Student Conference on Research and Development (SCOReD) [online]. IEEE, p. 49-52. Available at: http://ieeexplore.ieee.org/document/5443345/

[31] NAZARIO, Jose. 2008. DDoS attack evolution. Network Security [online]. 2008(7), 7-10. Available at: linkinghub.elsevier.com/retrieve/pii/S1353485808700862

[32] MILLIKEN, Jonny, Valerio SELIS, Kian Meng YAP and Alan MARSHALL. 2013. Impact of Metric Selection on Wireless DeAuthentication DoS Attack Performance. IEEE Wireless Communications Letters [online]. 2(5), 571-574. Available at: http://ieeexplore.ieee.org/document/6574904/

[33] YANG, Chao, Yimin SONG and Guofei GU. 2012. Active User-Side Evil Twin Access Point Detection Using Statistical Techniques. IEEE Transactions on Information Forensics and Security [online]. 7(5), 1638-1651. Available at: http://ieeexplore.ieee.org/document/6236067/

[34] HSU, Fu-Hau, Yu-Liang HSU and Chuan-Sheng WANG. 2019. A solution to detect the existence of a malicious rogue AP. Computer Communications [online]. 142-143, 62-68. Available at: https://linkinghub.elsevier.com/retrieve/pii/S0140366418306005

[35] WANG, Le and Alexander M. WYGLINSKI. 2016. Detection of man-in-the-middle attacks using physical layer wireless security techniques. Wireless Communications and Mobile Computing [online]. 16(4), 408-426. Available at: http://doi.wiley.com/10.1002/wcm.2527

[36] Alerts and WIDS. © 2021. Kismet [online]. Jekyll & Minimal Mistakes. Available at: https://www.kismetwireless.net/docs/readme/alerts_and_wids/

[37] MARTIN, Jeremy, Travis MAYBERRY, Collin DONAHUE, Lucas FOPPE, Lamont BROWN, Chadwick RIGGINS, Erik C. RYE and Dane BROWN. 2017. A Study of MAC Address Randomization in Mobile Devices and When it Fails. Proceedings on Privacy Enhancing Technologies [online]. 2017(4), 365-383. Available at: http://content.sciendo.com/view/journals/popets/2017/4/article-p365.xml

[38] BAMBANG SETIADJI, Muhammad Yusuf, Ramadhan IBRAHIM and Amiruddin AMIRUDDIN. 2019. Lightweight Method for Detecting Fake Authentication Attack on Wi-Fi. In: 2019 6th International Conference on Electrical Engineering, Computer Science and Informatics (EECSI) [online]. IEEE, p. 280-285. Available at: https://ieeexplore.ieee.org/document/8976975/

[39] ALTINOK, Besim. PiKarma: Detects wireless network attacks performed by KARMA module. In: GitHub [online]. Available at: https://github.com/WiPi-Hunter/PiKarma

[40] SCARFONE, Karen and Peter MELL. 2012. Guide to Intrusion Detection and Prevention Systems (IDPS). In: NIST Special Publication (SP) 800-94 [online]. Gaithersburg, MD: National Institute of Standards and Technology, p. 1-111. Available at: https://csrc.nist.gov/publications/detail/sp/800-94/rev-1/draft

[41] KENT, Karen and Murugiah SOUPPAYA. 2006. NIST Special Publication (SP) 800-92 [online]. , 1 - 72. Available at: https://csrc.nist.gov/publications/detail/sp/800-92/final

[42] COULIBALY, Keturahlee. An overview of Intrusion Detection and Prevention Systems. ArXiv:2004.08967v1 [online]. (abs/2004.08967), 1-4. Available at: https://arxiv.org/abs/2004.08967

[43] NASEER, Sheraz, Yasir SALEEM, Shehzad KHALID, Muhammad Khawar BASHIR, Jihun HAN, Muhammad Munwar IQBAL and Kijun HAN. 2018. Enhanced Network Anomaly Detection Based on Deep Neural Networks. IEEE Access [online]. 6, 48231-48246. Available at: https://ieeexplore.ieee.org/document/8438865/

[44] BOERO, Luca, Marco CELLO, Mario MARCHESE, Enrico MARICONTI, Talha NAQASH and Sandro ZAPPATORE. 2017. Statistical fingerprint-based intrusion detection system (SF-IDS). International Journal of Communication Systems [online]. 30(10). Available at: http://doi.wiley.com/10.1002/dac.3225

[45] FUCHSBERGER, Andreas. 2005. Intrusion Detection Systems and Intrusion Prevention Systems. Information Security Technical Report [online]. 10(3), 134-139. Available at: https://linkinghub.elsevier.com/retrieve/pii/S1363412705000415

[46] ALBIN, Eugene. September 2011. A Comparative Analysis of the Snort and Suricata Intrusion-Detection Systems [online]. Monterey, California. Available at: https://apps.dtic.mil/sti/citations/ADA552115. Master's thesis. Naval postgraduate school Monterey.

[47] PARK, Wonhyung and Seongjin AHN. 2017. Performance Comparison and Detection Analysis in Snort and Suricata Environment. Wireless Personal Communications [online]. 94(2), 241-252. Available at: http://link.springer.com/10.1007/s11277-016-3209-9

[48] Snort 3 officially released. Snort Blog [online]. Available at: https://blog.snort.org/2021/01/snort-3-officially-released.html

[49] Writing Effective Snort Rules with Examples [Best Practices]. Coralogix [online]. Available at: https://coralogix.com/blog/writing-effective-snort-rules-for-the-sta/

[50] Differences From Snort. Read the Docs: Suricata User Guide [online]. Available at: https://suricata.readthedocs.io/en/suricata-6.0.0/rules/differences-from-snort.html

[51] Rules Format. Read the Docs: Suricata User Guide [online]. Available at: https://suricata.readthedocs.io/en/suricata-6.0.0/rules/differences-from-snort.html

[52] SOMMER, Robin. Bro: An Open Source Network Intrusion Detection System. Security, E-learning, E-Services, 17. DFN-Arbeitstagung über Kommunikationsnetze [online]. Gesellschaft für Informatik e.V., 17, 273-288. Available at: https://subs.emis.de/LNI/Proceedings/Proceedings44/article1225.html

[53] About Zeek. Read the Docs: Zeek documentation [online]. Available at: https://docs.zeek.org/en/lts/about.html

[54] SINGH, Rupinder and Jatinder SINGH. 2012. A Performance Metrics Scorecard Based Approach to Intrusion Detection System Evaluation for Wireless Network. Global Journal of Computer Science and Technology [online]. , 1-11. Available at: https://computerresearch.org/index.php/computer/article/view/579

[55] MURRAY, Jason. 2009. An Inexpensive Wireless IDS using Kismet and OpenWRT. SANS Institute [online]. , 1-50. Available at: https://www.sans.org/reading-room/whitepapers/detection/inexpensive-wireless-ids-kismet-openwrt-33103

[56] Alerts and WIDS. Kismet wireless [online]. Available at: https://www.kismetwireless.net/docs/readme/alerts_and_wids/

[57] Arpwatch - keep track of ethernet/ip address pairings. FreeBSD Manual Pages [online]. Available at: https://www.freebsd.org/cgi/man.cgi?query=arpwatch&apropos=0&sektion=0&manpath=FreeBSD+5.3-RELEASE+and+Ports&format=html

[58] XArp – Advanced ARP Spoofing Detection [online]. Available at: http://www.xarp.net/

[59] Mikrotik model hAP ac² specification. Mikrotik [online]. [cit. 2020-11-18]. Dostupné z:<https://mikrotik.com/product/hap_ac2>

Seznam symbolů, veličin a zkratek

ARP protokol pro překlad adres – Address Resolution Protocol

S-ARP zabezpečený protokol pro překlad adres – Secure Address Resolution Protocol

MAC fyzická adresa zařízení – Media Access Control

LAN lokální síť – Local Area Network

IP internetový protokol – Internet Protokol

MitM útok mužem uprostřed – Man in the Middle

DoS útok odepřením služeb – Denial of Service

DDoS distribuovaný útok odepřením služeb – Distributed Denial of Service

DHCP protokol pro automatickou konfiguraci počítačů v síti – Dynamic Host Configuration Protocol

PKI infrastruktura pro správu a distribuci veřejných klíčů – Public Key Infrastructure

AKD certifikační autorita distribuující klíče – Authoritative Key Distributor

DSA algoritmus pro tvorbu digitálních podpisů – Digital Signature Algorithm

VLAN virtuální lokální síť – Virtual Local Area Network

DTP protokol pro sjednání přenosového kanálu mezi dvěma VLAN přepínači – Dynamic Trunking Protocol

ISL protokol sloužící k udržování VLAN informací v Ethernetových rámcích – InterSwitch Link Protocol

CAM fyzická paměť přepínače – Content Addressable Memory

STP protokol zamezující vzniku smyček síťové topologie – Spanning Tree Protocol

BPDU rámce nesoucí informace o STP – Bridge Protocol Data Unit

RIP směrovací protokol uvnitř sítě – Routing Information Protocol

OSPF směrovací protokol uvnitř sítě – Open Shortest Path First

BGP směrovací protokol mezi sítěmi – Border Gateway Protocol

LSA pakety obsahující informace o topologii sítě – Link-State Advertisement

TCP spojově orientovaný protokol transportní vrstvy – Transmission Control Protocol

UDP nespojově orientovaný protokol transportní vrstvy – User Datagram Protocol

AES algoritmus symetrické kryptografie – Advanced Encryption System

CDP protokol pro sdílení informací o přímo připojených zařízeních – Cisco Discovery Protocol

ICMP protokol oznamující chybové stavy v síti – Internet Control Message Protocol

ISP poskytovatel internetových služeb – Internet Service Provider

IDS systém detekce kybernetických hrozeb – Intrusion Detection System

IPS systém prevence kybernetických hrozeb – Intrusion Prevention System

NIDS síťový systém detekce kybernetických hrozeb – Network Intrusion Detection System

HIDS systém detekce kybernetických hrozeb zaměřený na koncové zařízení – Host Intrusion Detection System

SNMP protokol sloužící pro správu sítě – Simple Network Management Protocol

AP přístupový bod do vnitřní sítě – Access Point

A Přílohy

A.1 Obsah elektronické přílohy

Příloha obsahuje odkaz na Google Disk. Obsahem Google Disku je komprimovaný archív obsahující zdrojové kódy programu detektoru psané v jazyce Python verze 3.7.3 (programDetektoruSrc.rar). Dále je zde textový soubor obsahující použité příkazy pro realizaci kybernetických útoků (prikazyUtoky.txt) a video záznam použití programu detektoru (programDetektoruVideo.mp4). Následující archív obsahuje zkompilovaný a spustitelný program detektoru (programDetektoruSpustitelny.tar.gz). Posledním souborem je komprimovaný archív obsahující obraz celého systému Raspbian (raspberryPiOS.img.gz). Jedná se o obraz systému, který obsahuje použité detekční systémy, zdrojové kódy detektoru a spustitelný soubor odkazující na program detektoru. Stažení celého operačního systému Raspbian a instalace na SD kartu je doporučeným postupem pro využití programu detektoru.