VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

Fakulta elektrotechniky
a komunikačních technologií

BAKALÁŘSKÁ PRÁCE

Brno, 2020 Norbert Lővinger

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

DETEKCE FALEŠNÝCH PŘÍSTUPOVÝCH BODŮ
DETECTION OF FAKE ACCESS POINTS

BAKALÁŘSKÁ PRÁCE
BACHELOR'S THESIS

AUTOR PRÁCE — **Norbert Lővinger**
AUTHOR

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

BRNO 2020

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ

Bakalářská práce

bakalářský studijní program **Informační bezpečnost**

Ústav telekomunikací

Student: Norbert Lővinger ***ID:*** 197636
Ročník: 3 ***Akademický rok:*** 2019/20

NÁZEV TÉMATU:

Detekce falešných přístupových bodů

POKYNY PRO VYPRACOVÁNÍ:

Hlavním cílem práce je návrh a implementace detekčních metod kybernetických útoků v lokálních sítích LAN (Local Area Network). V teoretické části práce se seznamte s metodami pro detekci a mitigaci kybernetických útoků v LAN a vytvořte přehledný rozbor současného stavu problematiky (metody detekce na bázi signatur a anomálií pro jednotlivé typy útoků). Analýzu zaměřte zejména na bezdrátové lokální sítě WLAN (Wireless LAN, 802.11) a na metody detekce falešných přístupových bodů. V praktické části vytvořte experimentální pracoviště obsahující domácí směrovač Mikrotik, Raspbeery Pi (detektor) a osobní počítače představující legitimního uživatele a útočníka. Navrhněte a implementujte nejméně 5 metod detekce kybernetických útoků, funkčnost implementace ověřte na experimentálním pracovišti. Detektor bude využívat vlastní implementaci signatury pro systém Suricata nebo vlastní implementaci metody detekce v programovacím jazyku Python (anomálie nebo vzor).

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: 3.2.2020 ***Termín odevzdání:*** 8.6.2020

Vedoucí práce: Ing. Zdeněk Martinásek, Ph.D.

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

ABSTRAKT

Riziko kybernetických útokov v lokálnych sieťach sa stále zvyšuje v dôsledku podceňovania ich bezpečnosti. V bezdrôtových lokálnych sieťach útočník nevyžaduje fyzický prístup do siete a postrehnutie útoku je takmer nemožné. Typickým znakom falošného prístupového bodu je jeho rovnaká konfigurácia s legitímnym prístupovým bodom, čo zvyšuje efektivitu útoku. Na detekciu kybernetických útokov v lokálnych sieťach sa využívajú detekčné systémy, ktoré obsahujú pokročilé metódy na analýzu zachytenej sieťovej komunikácie. V tejto bakalárskej práci sú analyzované detekčné systémy Suricata a Kismet na základe ktorých je vytvorená vlastná implementácia detekčného systému v jazyku Python na cenovo dostupnom zariadení Raspberry Pi 4. Úspešnosť detekcie kybernetických útokov s využitím falošného prístupového bodu bola overená vytvorením 4 scenárov kybernetických útokov na experimentálnom pracovisku.

KĽÚČOVÉ SLOVÁ

falošný prístupový bod, detekčný systém, IDS, Suricata, Kismet, Scapy, Kali Linux, airmon-ng, útok s falošným prístupovým bodom, deautentizačný útok, KARMA útok, útok zahltením frekvencii

ABSTRACT

The risk of cyber-attacks in the local networks is constantly increasing due to the underestimation of their security. In wireless LANs, an attacker does not require physical access to the network. These types of attacks are almost impossible to spot. The typical signature of fake access point is the same configuration as the legitimate access point, which increases the effectivness of the attack. Detection systems are used to detect these cyber-attacks in local networks. Detection systems offer advanced methods for real-time analysis of captured network communication.

In this bachelor thesis two open detection systems – Suricata and Kismet are analysed and compared. Custom implementation of detection system is based on functionality analysis of these two detection systems. Custom implemetation is programmed in Python at an affordable Raspberry Pi 4. The success of detecting cyber-attacks using fake access point was tested in 4 different scenarios at the experimental testbed.

KEYWORDS

rogue access point, fake access point, Intrusion Detection System, Suricata, Kismet, Scapy, Kali Linux, airmon-ng, evil twin attack, deauth attack, KARMA attack, beacon flood attack

LÖVINGER, Norbert. *Detekce falešných přístupových bodů*. Brno, 2020, 74 s. Bakalárska práca. Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, Ústav telekomunikací. Vedúci práce: Ing. Zdeněk Martinásek, Ph.D.

VYHLÁSENIE

Vyhlasujem, že svoju bakalársku prácu na tému „Detekce falešných přístupových bodů“ som vypracoval samostatne pod vedením vedúceho bakalárskej práce, s využitím odbornej literatúry a ďalších informačných zdrojov, ktoré sú všetky citované v práci a uvedené v zozname literatúry na konci práce.

Ako autor uvedenej bakalárskej práce ďalej vyhlasujem, že v súvislosti s vytvorením tejto bakalárskej práce som neporušil autorské práva tretích osôb, najmä som nezasiahol nedovoleným spôsobom do cudzích autorských práv osobnostných a/alebo majetkových a som si plne vedomý následkov porušenia ustanovenia § 11 a nasledujúcich autorského zákona Českej republiky č. 121/2000 Sb., o práve autorskom, o právach súvisiacich s právom autorským a o zmene niektorých zákonov (autorský zákon), v znení neskorších predpisov, vrátane možných trestnoprávnych dôsledkov vyplývajúcich z ustanovenia časti druhej, hlavy VI. diel 4 Trestného zákonníka Českej republiky č. 40/2009 Sb.

Brno ....

podpis autora

POĎAKOVANIE

Rád by som sa poďakoval môjmu vedúcemu bakalárskej práce pánovi Ing. Zdeněkovi Martináskovi, Ph.D. za odborné vedenie, konštruktívne konzultácie, podnetné návrhy a komplexnejší pohľad na prácu.

Obsah

Zoznam obrázkov

Úvod

V posledných rokoch sa bezdrôtové siete stali bežnou súčasťou života každého človeka, ktorý sa chce pripojiť k internetu. Napriek rýchlemu rozvoju bezdrôtových technológií sa z pohľadu bežných používateľov nevenuje veľká pozornosť ich bezpečnosti. Takéto správanie má za následok zvýšenie počtu kybernetických útokov aj na lokálne bezdrôtové siete[1], nakoľko šanca útočníka na získanie citlivých údajov používateľov je pomerne vysoká.

Hlavným cieľom bakalárskej práce je spracovanie problematiky kybernetických útokov v lokálnych bezdrôtových sieťach a vytvorenie vlastnej implementácie detekčného systému s metódami na detekciu falošného prístupového bodu.

Teoretická časť bakalárskej práce sa zaoberá základným členením kybernetických útokov v lokálnych sieťach, ich detekciou a mitigáciou pomocou detekčných systémov. Detekčné systémy monitorujú sieťovú komunikáciu a upozorňujú používateľa na podozrivú aktivitu v sieti. Podľa funkcionality sa rozdeľujú na pasívne a aktívne s prvkami firewallu. Detekčný systém využíva dve základné metódy detekcie: na základe **signatúr** a **anomálií** v sieti. Práca sa ďalej zameriava na analýzu bezdrôtových lokálnych sietí a základnú funkcionalitu bezdrôtového prístupového bodu.

Kybernetické útoky s využitím falošného prístupového bodu v bezdrôtových lokálnych sieťach sú pre bežných používateľov nepostrehnuteľné a o to viac nebezpečné. V praktickej časti práce sú metódy detekcie kybernetických útokov otestované na vytvorenom experimentálnom pracovisku najprv pomocou dvoch voľne dostupných detekčných systémov Suricata a Kismet. Analýzou získaných výsledkov detekcie je vytvorený a otestovaný **vlastný návrh implementácie** detekčného systému na cenovo dostupnom zariadení **Raspberry Pi 4** s využitím programovacieho jazyka **Python 3**.

[1] Zoznam známych kybernetických útokov a zraniteľností za rok 2019. [1]

1 Kybernetické útoky v lokálnych sieťach

V následujúcich kapitolách bakalárskej práce sa vyskytujú špecifické technické pojmy preložené do Slovenského jazyka. Pre jednoduchšie porozumenie textu sú ich anglické preklady uvedené v zátvorkách.

Bezpečnosť lokálnych sietí je častokrát podceňovaná a riziko kybernetických útokov v dôsledku ich rozvoja a využívania používateľmi je vysoké. Používatelia častokrát nesprávne označujú malé lokálne siete za bezpečnejšie v porovnaní s geograficky väčšími sieťami. Pri bezdrôtových lokálnych sieťach útočník nevyžaduje fyzický prístup do siete a preto sú tieto typy útokov takmer nepostrehnuteľné. Útoky na lokálne siete sa rozdeľujú na **pasívne a aktívne**. [2, 3, 4]

1.1 Typy útokov v lokálnych sieťach

Pasívny **útok odposluchu a zbierania informácií** o sieti je pre bežného používateľa nepostrehnuteľný. Útočník zachytáva sieťovú komunikáciu pomocou monitorovacieho módu na rozhraní a špeciálneho nástroja (kapitola 3.1). Zachytené informácie sú využité na realizáciu ďalších kybernetických útokov. Detekcia a mitigácia pasívnych útokov je náročná a vyžaduje si pokročilé nastavenie sieťových zariadení, čo výrazne znižuje komfort používania lokálnej siete. [5]

Cieľom **deautentizačných útokov** je prerušenie existujúceho pripojenia a prinútenie používateľa o opätovnú autentizáciu k prístupovému bodu. Komunikáciu môže útočník zachytiť a využiť na ďalšie útoky iba v prípade nedostatočného zabezpečenia rámcov (kapitola 2.1). Deautentizačné útoky sú často využívané na pripojenie používateľov k falošnému prístupovému bodu (kapitola 2.3 a scenár 3.18). Detekcia a mitigácia deautentizačných útokov je vzhľadom na ich vysoký počet za pomerne krátky čas jednoduchá a efektívna. [6]

Aktívny **útok duplikáciou fyzickej adresy** (angl. MAC – Media access control) nachádza svoje uplatnenie pri pripájaní používateľa k prístupovému bodu, ktorý disponuje zoznamom povolených zariadení. Pomocou odposluchu prenášaných dát dokáže útočník zistiť fyzické adresy aktívnych zariadení v sieti a ich duplikovaním sa pripojiť k sieti. Prístupový bod nedokáže rozlíšiť skutočnú fyzickú adresu od duplikovanej a nastávajú sieťové kolízie z dôvodu pripojenia dvoch rovnakých fyzických adries do siete. Detekcia a mitigácia útoku duplikácie fyzických adries vyžaduje detekčný algoritmus, ktorý vytvára a porovnáva jedinečné odtlačky so signatúrami pripojených zariadení. [7]

Aktívny **útok na odopretie dostupnosti služieb** (angl. DoS – Denial-of-Service) pripojeným používateľom za účelom paralyzovania poskytovaných služieb v sieti. Cieľom útočníka je vyčerpanie sieťových a výpočtových zdrojov zariadenia

ako napríklad zahltenie vysielaného kanálu v bezdrôtovej lokálnej sieti (kapitola 2.3 a scenár 3.16). Metódy na detekciu a mitigáciu útokov DoS fungujú spoľahlivo, avšak ich úspešnosť vždy závisí na sile útoku. V bezdrôtových sieťach je jednou z možností mitigácie odpojenie konkrétneho zariadenia, ktoré DoS útok vykonáva. [8]

Najznámejší a najpoužívanejší aktívny útok na sieťovú komunikáciu medzi dvomi stranami je **útok s mužom uprostred** (angl. MitM – Man-in-the-Middle). Cieľom útočníka je zachytávať a modifikovať komunikáciu medzi pripojenými používateľmi a prístupovým bodom bez ich vedomia. Zachytené informácie môže následne využiť na ďalšie útoky v lokálnych sieťach, ktoré sú bližšie popísané aj s ich detekciou v kapitole 2.3.

Útok s vytvorením falošného bezdrôtového prístupového bodu je vo veľkej miere vykonávaný v slabo zabezpečených bezdrôtových sieťach. Cieľom útočníka je rovnako, ako v prípade útoku s mužom uprostred zachytávanie a modifikácia prenášaných dát v sieti (scenár 3.12). Detekcia a mitigácia falošného prístupového bodu je podrobnejšie popísaná v kapitolách 2.2 a 2.3.

1.2 Metódy pre detekciu kybernetických útokov

Na detekciu kybernetických útokov v lokálnej sieti sú využívané **detekčné systémy obsahujúce pokročilé monitorovacie metódy** s cieľom analýzy mimoriadnych udalostí v reálnom čase. Základným princípom je predpoklad odlišnosti normálnych a abnormálnych aktivít na sieti. Systémy pracujú v rôznych prostrediach, v dôsledku čoho je správne umiestnenie systému často rozhodujúci faktor pri detekcií a následnej mitigácií útokov. [2, 9, 10]

Detekčné systémy v závislostí na funkcionalite sa rozdeľujú na:

- **Pasívny detekčný systém** (angl. IDS – Intrusion Detection System), ktorého funkciou je zachytávanie a následné vyhodnocovanie komunikácie.
- **Aktívny systém s funkciami IDS a firewalu** (angl. IPS – Intrusion Prevention System), ktorý dynamicky reaguje na nežiadúce incidenty v monitorovanej sieti a vykonaním akcie ich mitiguje.

Typické umiestnenie detekčných systémov:

- **Detekčný systém na zariadení používateľa** (angl. HIDS – Host-Based IDS) analyzuje podozrivé činnosti, ako úpravy súborového systému alebo systémové volania.
- **Strategicky umiestnený detekčný systém v sieti** (angl. NIDS – Network-Based IDS) monitoruje aktivitu vyhradenej časti siete. Analyzuje získané informácie, ktoré vyhodnocuje a porovnáva s vytvorenými pravidlami. Typickým príkladom tohto systému je sieťový senzor.

- **Bezdrôtový detekčný systém v sieti** (angl. WIDS – Wireless IDS) je umiestnený v bezdrôtovej sieti bez nutnosti fyzického pripojenia. V porovnaní s NIDS dokáže monitorovať a analyzovať aktivitu v sieti iba na nižších vrstvách ISO/OSI modelu. Výhodou je jeho väčšia flexibilita.

Detekčné systémy pracujú s dvomi hlavnými metódami detekcie kybernetických útokov v lokálnych sieťach. Prvou metódou je **detekcia na základe signatúr**. Signatúry sú vzory nepriaznivej činnosti na sieti, ktoré detekčné systémy majú uložené v databáze a porovnávajú ich s aktuálnou situáciou na sieti. Signatúry sú väčšinou vytvárané manuálne na základe zachytenej sieťovej komunikácie alebo vzoru škodlivého kódu. **Výhodou je ich vysoká efektivita pri známych útokoch**, naopak schopnosť detekcie pri neznámych útokoch je veľmi nízka. Vo všeobecnosti platí, že úspešnosť detekcií závisí na kvalitnej databáze.

Techniky detekcie signatúr sa delia na:

- **Metódy založené na porovnávaní paketov** – Technika využívaná hlavne v detekčných systémoch umiestnených na sieti. Porovnávajú sa hlavičky a obsahy jednotlivých paketov za cieľom nájdenia zhody s nebezpečnou signatúrou. Výpočtovo a časovo náročná metóda, ktorá môže byť nahradená efektívnejšími metódami. [11]
- **Metódy definované pomocou pravidiel** – Najstaršia technika detekcie signatúr modeluje scenáre útokov prostredníctvom definovaných pravidiel. Výsledky sú porovnávané s aktuálnou situáciou na sieti a akákoľvek odchýlka predstavuje potencionálny útok. Hlavnou nevýhodou je nutnosť technických znalostí z oblasti na vytvorenie vhodnej definície pravidiel.
- **Metódy dolovania a analýzy dát** – Proces, v ktorom sú využívané na tvorbu modelov a zisťovania útokov klasifikačné algoritmy, ako napríklad neurónové siete. Na základe vstupnej trénovacej množiny dát algoritmus vytvorí pravidlá v podobe modelu. Nevýhodou je nutnosť tvorby trénovacej množiny obsahujúcej škodlivú komunikáciu a následne znížená schopnosť detekcie útokov. [12]

Druhou metódou je **detekcia kybernetických útokov na základe anomálií**. Anomálie sú neznáme udalosti a odchýlky, ktoré predstavujú nebezpečenstvo pre monitorovanú sieť. K vytvoreniu pravidiel na základe anomálií je nutný zber veľkého počtu dát o situáciach na sieti a ich triedenie do profilov, ktoré sú následne porovnávané s referenčným modelom[1]. Detekcia anomálií predstavuje učenie rôznych situácií a určenie ich hraníc normálnosti. Hlavnou **výhodou je lepšia detekcia neznámych útokov, avšak pri zvýšenom počte falošných poplachov**. Nevýhodou je neschopnosť detekcie skrytých útokov[2].

[1] Referenčný model obsahuje charakteristiku bežnej sieťovej aktivity za určitý časový okamih.

[2] Skryté útoky sa tvária ako bežná sieťová komunikácia a je ich ťažké odhaliť.

Techniky detekcie na základe anomálií sú:

- **Metódy definované pomocou pravidiel** – Podobný princíp metódy, ako u detekcií na základe signatúr. V tomto prípade sa špecifikuje správanie systému pomocou atribútov[3], pri ktorých je ich viacnásobné vykonávanie ohrozením monitorovanej siete.
- **Štatistické metódy** – Akákoľvek udalosť v monitorovanej sieti je zaznamenávaná a zaradená do profilu štatistického modelu, ktorý rozhoduje o jej bezpečnosti.
- **Metódy dolovania a analýzy dát** – Rovnaký princíp metódy, ako pri analýze signatúr. Jediným rozdielom je použitie bežnej sieťovej komunikácie bez vložených škodlivých dát, ako trénovacej množiny. Výhodou je presný model s jednoduchšou detekciou nebezpečnej aktivity. [13]

Kombinácia dvoch metód detekcií kybernetických útokov tvorí **hybridný detekčný systém spájajúci výhody oboch systémov**. Detekcia signatúr je využívaná na odhalenie známych útokov a naopak detekcia anomálií slúži na detekciu neznámych útokov. Cieľom je minimalizácia falošných poplachov pri vysokej úspešnosti ich detekcie.

Moderné detekčné systémy sú pomerne bežnými zariadeniami v lokálnych sieťach. Svoje **komerčné riešenia detekčných systémov** do domácich ale aj firemných sietí ponúkajú výrobcovia:

- **Cisco NGIPS** – Komerčné riešenie detekčného systému, ktorý využíva inteligentnú a pravidelne aktualizovanú databázu hrozieb, doplnenú o nástroje podporujúce automatizáciu zápisu udalostí za cieľom zvýšenia celkovej efektivity. Užívateľsky prívetivé prostredie umožňuje spracovanie veľkého počtu vstupných dát a ich následnú implementáciu. [14]
- **Palo Alto Networks NGFW** – Celosvetovo známa spoločnosť v oblasti kybernetickej bezpečnosti Palo Alto ponúka aplikačné firewally novej generácie. Spoločnosť priamo vyhlasuje, že ich riešenia sa odlišujú oproti bežným IPS a ponúkajú pridanú funkcionalitu ako napríklad sieťový anti-malware, URL filter, či zabezpečujúcu politiku na základe aplikácie a užívateľa. [15]
- **Bitdefender BOX 2** – Zariadenie na trhu od firmy Bitdefender dokáže zabezpečiť všetky pripojené zariadenia v domácnosti. Zariadenie po pripojení do rovnakej lokálnej siete plní úlohu hardvérového firewallu. Vďaka tomuto riešeniu dokáže BOX monitorovať prevádzku na sieti a upozorňovať na prípadné útoky, či iné anomálie. [16]

[3] Atribúty sú napríklad pokusy o prihlásenie do siete, pravidelná návšteva webovej stránky a pod.

- **Radware** – Filozofia spoločnosti Radware je založená na poskytovaní cloudových riešení systémov IPS. V minulosti získala významné ocenenia pri detekcií a mitigácií DoS útokov v reálnom čase. [17]
- **F-Secure SENSE** – Prémiový domáci bezdrôtový prístupový bod so smerovačom a ochranou dát pomocou analýzy vzoriek a ich porovnávania v cloudovej databáze. Mobilná aplikácia na správu siete umožňuje rýchle zmeny nastavení a monitorovanie siete v reálnom čase. [18]
- **Norton Core Router** – Dizajnový prístupový bod s ochranou domácej siete podporujúcej hlbokú analýzu prichádzajúcich a odchádzajúcich paketov. Jednoduchosť užívateľského prostredia zjednodušuje nastavenie širokého množstva funkcií a monitorovania siete. [19]

Na druhej strane **voľne dostupné nekomerčné detekčné systémy** sú využívané v menších domácich sieťach:

- **Suricata** – V súčasnej dobe najpoužívanejší voľne dostupný detekčný systém. Nadácia OISF[4] stojí za jej vývojom a v porovnaní so systémom Snort, pracuje s využitím viacerých vlákien súčasne, čo výrazne zvyšuje rýchlosť spracovania dát v reálnom čase[5]. Podporuje všetky známe operačné systémy a z jej základov sú vyvíjané aj ďalšie komerčné riešenia. [20, 21]
- **Kismet** – Detekčný systém pracujúci v bezdrôtových sieťach. Použitím pasívneho módu nezanecháva žiadne stopy pri skenovaní siete a dokáže pracovať so všetkými sieťovými kartami podporujúcich monitorovací mód. Má aktívnu komunitu používateľov a je rozšíriteľný pomocou rozšírení. Kismet je v základe distribuovaný v systémoch Kali Linux. [22, 23, 24]
- **Zeek** – Bezplatný sieťový systém v minulosti označovaný ako Bro je založený na oboch typoch detekcií – signatúr a anomálií. Môže byť využívaný ako riešenie NIDS s pridanou analýzou udalostí v reálnom čase, čím sa odlišuje od iných nekomerčných riešení. Nevýhodou systému Zeek je možnosť spustenia len na platforme operačných systémov Unix. [25, 26]
- **Snort** – Detekčný systém umiestnený na sieti – NIDS. Voľne dostupné riešenie od spoločnosti Cisco s podporou operačných systémov Linux a Windows. Systém realizuje odchytávanie paketov v sieti, ktoré sú následne analyzované v reálnom čase. Systém využíva vlastnú syntax na konfiguráciu pravidiel. [27, 28]

[4]Open Information Security Foundation

[5]Podporuje hardwarovú akceleráciu a dokáže využívať výkon grafickej karty na výpočty.

Tab. 1.1: Porovnanie komerčných a voľne dostupných detekčných systémov

	Výhody (+)	**Nevýhody (-)**
Komerčné riešenia	Komplexnosť podpory Pravidelnosť aktualizácií Jednoduchosť ovládania	Cena a licencovanie Rozšíriteľnosť
Nekomerčné riešenia	Cena Rozšíriteľnosť Otvorenosť	Zložitosť ovládania Žiadna oficiálna podpora Kompatibila HW

2 Bezdrôtové lokálne siete

Bezdrôtové lokálne siete (angl. WLAN – Wireless Local Area Network) boli primárne navrhnuté a využívané v priemyselnej oblasti. S odstupom času sa ich popularita zvýšila a nižšie výrobné náklady zariadení zapríčinili jej rozšírenie aj do bežných domácností.

Bezdrôtový prístupový bod (angl. AP – Access Point) je sieťové zariadenie, ktoré umožňuje bezdrôtovým používateľom rýchle a jednoduché pripojenie do lokálnej siete s využitím technológie Wi-Fi. Prístupový bod podporuje pripojenie viacerých zariadení súčasne. Pripojenie a následná komunikácia prebieha cez rádiové spojenie v bezlicenčnom pásme na frekvenciách podľa používaného protokolu. Najpoužívanejšími sieťovými štandardmi na bezdrôtovú komunikáciu sú protokoly rodiny IEEE 802.11, ktoré špecifikujú implementáciu prenosových protokolov na fyzickej a spojovej vrstve modelu ISO/OSI v bezdrôtových sieťach. [29]

Vysielaný **signál** je elektromagnetická vlna, ktorá je nositeľom informácie a umožňuje jej prenos medzi odosielateľom a prijímateľom. Signál pre komunikáciu v bezdrôtových sieťach prenáša informácie vo forme 0 a 1, ktoré sú pomocou modulácie vložené na nosnú vlnu. Sila signálu závisí na viacerých faktoroch[1] a je vyjadrená v jednotkách dBm (decibel-miliwatt).

Frekvenčný kanál je bližšie špecifikovaný rozsah rádiovej frekvencie bezlicenčného pásma. K najpoužívanejším frekvenciám, ktoré štandard 802.11 podporuje patria: 2,4 GHz, 5 GHz a 60 GHz[2]. Každá krajina môže tieto frekvencie regulovať v závislosti od ich využívania[3].

Hlavným viditeľným identifikátorom bezdrôtovej siete je SSID (Service Set Identifier), podľa ktorého sa používateľ rozhoduje o pripojení k lokálnej sieti. Identifikátor SSID sa skladá z 32bitového názvu siete, ktorý je vysielaný prístupovým bodom okolitým zariadeniam v určitých časových intervaloch. Toto vysielanie sa označuje ako beacon rámec (kapitola 2.1).

Unikátny identifikátor prístupového bodu BSSID (Basic Service Set Identifier) slúži na presnú identifikáciu bodu v sieti. Pozostáva zo 48bitového identifikátora pochádzajúceho z konverzie MAC adresy zariadenia. Vysielanie tohto identifikátora nie je možné bežnými spôsobmi konfigurovať a predstavuje bezpečnostnú slabinu pri útokoch o podvrhnutie prístupového bodu – **Rogue Access Point**. [30]

[1] Prostredie v blízkosti, vzdialenosť a prekážky v ceste, spotreba elektrickej energie vysielačom.
[2] Využívaná hlavne poskytovateľmi internetového pripojenia na krátke vzdialenosti do 1,5 km.
[3] Japonsko podporuje až 14 kanálov na frekvencii 2,4 GHz. EU 13 a USA 12.

2.1 Typy a funkcie rámcov štandardu 802.11

Základnou dátovou jednotkou prenášanou na spojovej vrstve ISO/OSI modelu je **rámec** (angl. frame). Rámec pozostáva zo štandardizovanej štruktúry dát, ktorá obsahuje informácie o fyzických adresách, prenášaných dátach a kontrole integrity. Štandard 802.11 bližšie špecifikuje typy a funkciu rámcov určených na správu pripojenia, prenos dát a riadenie linky, na ktorej sú prenášané. [31, 32]

Manažment rámce slúžia na správu pripojenia medzi bezdrôtovými zariadeniami a prístupovými bodmi. Vzhľadom na typ prenášaného média, ktorým je vzduch, je potrebné, aby správa fungovala bezchybne. Z tohto dôvodu štandard 802.11 rozdelil celý postup pripojenia k bezdrôtovej sieti na viaceré časti:

1. **Vyhľadávanie** – vyhľadávanie prístupového bodu pomocou beacon a probe rámcov.
2. **Autentizácia** – overenie identity a parametrov bezdrôtového zariadenia pomocou autentizačných rámcov.
3. **Asociácia** – získanie prístupu a pripojenie zariadenia do bezdrôtovej siete.

Tab. 2.1: Prehľad manažment rámcov.

Typ rámca	Smer vysielania	Účel prenosu
Beacon	Bod → Zariadenie	Oznamovanie prítomnosti bezdrôtovej siete okolitým zariadeniam
Probe	Zariadenie → Bod	Aktívna žiadosť zariadenia o pripojenie k bezdrôtovej sieti
Autentizácia	Zariadenie → Bod	Overenie a autentizácia pripájaného zariadenia k bezdrôtovej sieti
Asociácia	Zariadenie → Bod	Pripojenie zariadenia po vzájomnej výmene kompatibilných parametrov
Reasociácia	Zariadenie → Bod	Obnovenie pripojenia po dlhšej nečinnosti zariadenia
Deasociácia	Bod ↔ Zariadenie	Ukončenie pripojenia pri zmene vysielaných parametrov
Deautentizácia	Bod ↔ Zariadenie	Ukončenie komunikácie a odpojenie zariadenia

Beacon rámec slúži na oznamovanie dostupnosti bezdrôtovej siete okolitým bezdrôtovým zariadeniam podporujúcich rovnaký štandard. Beacon rámce sú považované za najdôležitejšie rámce v bezdrôtových sieťach, nakoľko pravidelne vysielajú všetky parametre o bezdrôtovej sieti.

Vysielané parametre sa rozdeľujú na:

- **Povinné** – časová značka, časový interval, identifikátor siete a základné prenosové rýchlosti.
- **Voliteľné** – krajina, rozšírené prenosové rýchlosti, zabezpečenie, kvalita služieb a iné.

Zodpovednosť za správne vysielanie rámcov má prístupový bod. Pravidelnosť, viditeľnosť a sila vysielaného rámca sa dá vo väčšine prístupových bodoch nakonfigurovať a docieliť tak zvýšenie zabezpečenia bezdrôtovej siete.

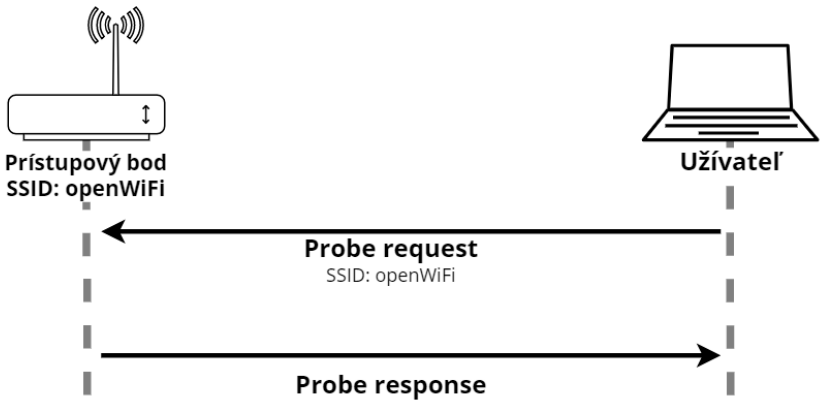
Obr. 2.1: Vysielanie beacon rámcov.

Probe rámec využívajú bezdrôtové zariadenia, ktoré aktívne skenujú okolie a vyhľadávajú bezdrôtové siete. Proces sa skladá z dvoch rámcov žiadosť – odpoveď:

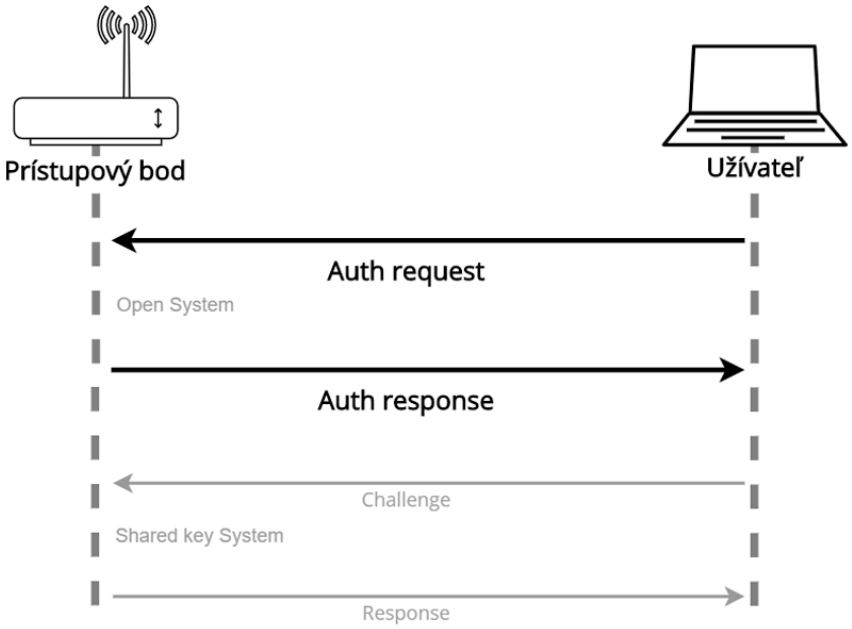
- **Žiadosť (Probe Request)** obsahuje informácie o identifikátore vyhľadávanej siete a podporovaných prenosových rýchlostiach. Prístupový bod spracovaním žiadosti rozhodne o pripojení bezdrôtového zariadenia.
- **Odpoveď (Probe Response)** obsahuje informácie o kompatibilných parametroch zariadenia a siete. V prípade potvrdenia parametrov je bezdrôtové zariadenie pripojené k prístupovému bodu a nasleduje autentizačný proces.

Autentizačný rámec slúži na autentizáciu bezdrôtového zariadenia pred pripojením k sieti. Proces autentizácie zariadenia pre otvorené siete (Open System) sa skladá z dvoch rámcov žiadosť – odpoveď. V prípade autentizácie k zabezpečenej sieti (Shared Key System) sa proces dopĺňa o ďalšie dva rámce výzva – odpoveď, ktoré zabezpečujú **komplexnejšiu autentizáciu zariadenia**.

- **Žiadosť o autentizáciu (Auth Request)** porovnáva typ a štandard 802.11 s prístupovým bodom.
- **Odpoveď (Auth Response)** obsahuje informácie o dohodnutom autentizačnom algoritme, sekvenčné číslo, stavový kód a prípadnú výzvu.



Obr. 2.2: Aktívne skenovanie a komunikácia probe rámcov.

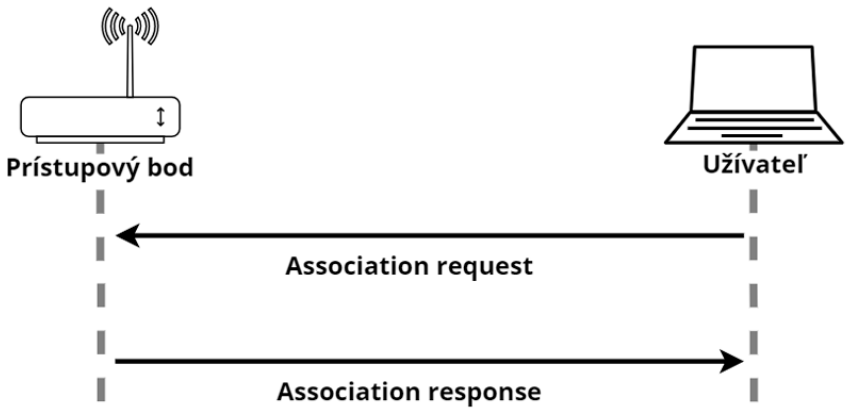


Obr. 2.3: Proces autentizácie zariadenia pre otvorené a zabezpečené siete.

Asociačný rámec slúži na pripojenie bezdrôtového zariadenia k prístupovému bodu. Proces sa skladá z výmeny dvoch rámcov žiadosť – odpoveď:

- **Asociačná žiadosť (Association Request)** môže byť vytvorená aj bez predchádzajúceho zachytenia beacon rámca a preto obsahuje aj žiadosť o parametre prístupového bodu (informácie o identifikátore SSID, podporované prenosové rýchlosti, informácie o napájaní, kvalita služieb a iné).
- **V asociačnej odpovedi (Association Response)** sa okrem vyžiadaných parametrov nachádza aj asociačné číslo – ID pre bezdrôtové zariadenie.

Reasociačný rámec je špeciálny typ asociačného rámca, ktorý umožňuje automatické obnovenie pripojenia medzi prístupovými bodmi počas pohybu zariadenia v rámci pokrytej oblasti. Znovupripojenie sa skladá z rovnakej žiadosti a odpovede ako pri asociácií.

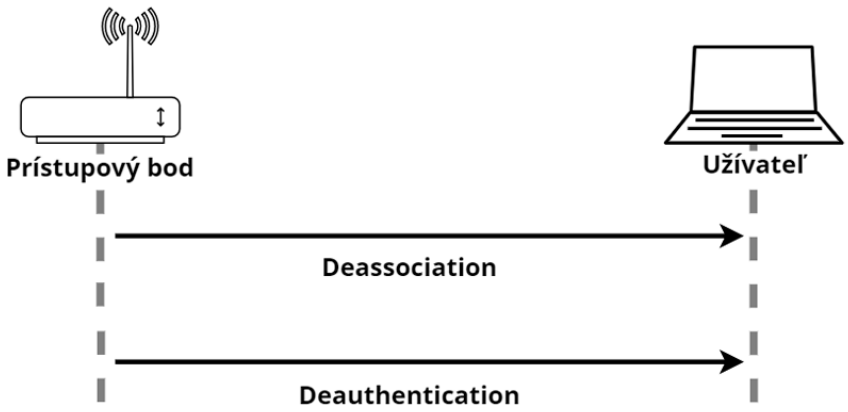


Obr. 2.4: Asociácia a reasociácia bezdrôtového zariadenia.

Deasociačný rámec slúži na ukončenie pripojenia medzi bezdrôtovým zariadením a prístupovým bodom. Telo rámca obsahuje informáciu o dôvode prerušenia pripojenia (Reason Code). Deasociačné rámce môžu byť vysielané konkrétnemu, alebo všetkým pripojeným bezdrôtovým zariadeniam.

Deautentizačný rámec môže byť vysielaný bezdrôtovým zariadením alebo prístupovým bodom za účelom prerušenia prebiehajúcej komunikácie. Telo rámca obsahuje informácie o dôvode ukončenia pripojenia (Reason Code), o MAC adresách dotknutých zariadení a o voliteľnom zabezpečení 802.11w. K bežným dôvodom prerušenia pripojenia patrí ručné odpojenie od siete, odpojenie z dôsledku neaktivity, alebo zmeny v nastaveniach zabezpečenia prístupového bodu. [33]

Deautentizačné rámce sú **najpoužívanejšou súčasťou bezdrôtových kybernetických útokov** muža uprostred alebo odopretia služby. Ochranou voči týmto typom útokov je zabezpečenie komunikácie manažment rámcov štandardom 802.11w.



Obr. 2.5: Ukončenie asociácie a autentizácie pripojeného zariadenia.

Štandard 802.11w označovaný ako ochrana manažment rámcov (angl. MFP – Management Frame Protection) slúži na zvýšenie bezpečnosti a integrity manažment rámcov v bezdrôtových sieťach. Narozdiel od prenášaných dát, **manažment rámce musia byť v otvorenej forme vysielané a prijímané všetkými bezdrôtovými zariadeniami v okolí**, čo z nich robí ideálnu možnosť na ich podvrhnutie. Patria sem predovšetkým deasociačné a deautentizačné rámce, ktoré umožňujú útočníkovi vykonať útoky odpojenia (Deauth Attack) alebo útoky opakovania (Replay Attack). Hlavnou výhodou pre podporované bezdrôtové zariadenia je ochrana pred neautorizovaným útokom na odpojenie, alebo odopretie služby, nakoľko pripojené zariadenie **akceptuje manažment rámce iba od legitímneho prístupového bodu**. Prístupové body naopak akceptujú asociačné a autorizačné požiadavky iba od nepripojených zariadení, čím znemožňujú útočníkovi vykonať útoky na odpojenie už pripojených zariadení. [34]

Dátové rámce obsahujú dáta z vyšších vrstiev, ktoré sú prenášané medzi bezdrôtovými zariadeniami. Okrem klasických dátových rámcov sem patria aj rámce so službou kvality (angl. QoS – Quality of Service) a prázdne dátové rámce (Null Data), ktoré slúžia na informovanie prístupového bodu o nedostupnosti zariadenia v dôsledku zapnutia módu šetrenia energie.

Tab. 2.2: Prehľad dátových rámcov.

Typ rámca	**Účel prenosu**
Data	Prenos dát medzi zariadením a prístupovým bodom
Null Data	Rámec označujúci zmenu stavu zariadenia do módu šetrenia energie
QoS Data	Prenos dát so zvýšenou kvalitou služieb

Riadiace rámce sa používajú v spojení s dátovými rámcami na zabezpečenie spoľahlivosti a celkovej kontroly linky, ktorá zahrňuje potvrdzovanie a správu prenosov, správu vysielanej frekvencie a pripojených zariadení. Štruktúra riadiacich rámcov obsahuje iba záhlavie a kontrolu integrity bez samotného tela rámca.

Tab. 2.3: Prehľad riadiacich rámcov.

Typ rámca	**Účel prenosu**
RTS	Žiadosť o prenos dát medzi zariadením a prístupovým bodom
CTS	Potvrdenie žiadostí o prenos dát a ochrana pred kolíziami
ACK	Potvrdzovací rámec prenosu dát
PS Pool	Informačný rámec o opätovnej dostupnosti zariadenia

Žiadosť o posielanie dát (angl. RTS – Request to Send) sa využíva na prebranie kontroly nad linkou pre ďalší prenos dát. Prístup k linke môže byť rezervovaný iba pre jednosmerné rámce.

Uzavrenie posielania dát (angl. CTS – Clear to Send) sa využíva v dvoch situáciách, ktoré nastávajú pri správe linky. Prvou situáciou je potvrdzovanie rámcov so žiadosťou o posielanie dát (RTS). Druhou situáciou je využitie ako ochranný mechanizmus proti kolíziám so staršími zariadeniami na linke.

Na **potvrdenie prenosu dát** na linke slúžia potvrdzovacie rámce (angl. ACK – Acknowledgment). Potvrdzovacie rámce ukončujú prenos dát, potvrdzujú prijatie riadiacich rámcov a uvoľňujú prenosovú linku pre ďalšie zariadenia.

Prebudenie z módu šetrenia energie (angl. Power-Saving mode) bezdrôtového zariadenia pri dlhšej neaktivite na sieti. Pozastavený je prenos a príjem rámcov pre toto zariadenie, ktoré po opätovnom prebudení a odoslaní rámca (angl. Power-Save Pool) informuje prístupový bod o svojom spustení. Ak existujú dátové rámce, ktoré boli prístupovým bodom zachytené počas nedostupnosti zariadenia, sú zariadeniu odoslané z vyrovnávacej pamäte.

2.2 Falošný prístupový bod

Neautorizovaný bezdrôtový prístupový bod v sieti, ktorý predstavuje bezpečnostné riziko pre používateľov. Typickým znakom je **rovnaká konfigurácia** s blízkym legitímnym prístupovým bodom. Cieľom útočníka je nalákanie používateľov na vysielanie rovnakého názvu siete a ich následné pripojenie k tomuto bodu za účelom ďalších útokov. Podvrhnutie falošného prístupového bodu je vzhľadom na jeho **jednoduchosť a vysokú efektívnosť** obľúbeným nástrojom útočníkov.

V tejto sekcií práce sú zahrnuté informácie o jeho vytvorení a detekcií známych útokov s využitím falošného prístupového bodu. [35]

Spôsobov vytvorenia falošného prístupového bodu je viac. Z technického hľadiska sa rozdeľuje na:

- **Soft AP** – Prístupový bod je vytvorený pomocou softvérového Wi-Fi adaptéru, ktorý zdieľa pripojenie k internetu – **tethering**. Ovládač Wi-Fi adaptéru musí podporovať operatívny mód. Vďaka funkcii Virtual Wi-Fi v operačných systémoch Windows 7 a vyššie sa možnosť vytvorenia prenosného prístupového bodu rozšírila viac medzi bežných používateľov.
- **Fake AP** – Špeciálny prístupový bod vytvorený a nakonfigurovaný znalým útočníkom, ktorý môže byť obsluhovaný na vzdialenosť aj niekoľko stoviek metrov s využitím antény s väčším dosahom[4]. Ovládač Wi-Fi adaptéru musí podporovať **monitorovací mód**, ktorý umožňuje rozhraniu zachytávať sieťovú komunikáciu v bezdrôtových sieťach. Primárne je táto funkcionalita blokovaná výrobcami a preto sú útočníkmi vo väčšine využívané niektoré externé Wi-Fi karty, ktoré tento mód podporujú.

Okrem technického rozdelenia falošného prístupového bodu sa môže deliť aj podľa technickej znalosti osoby, ktorá ho vytvorila:

- **Znalý útočník** – Prístupový bod je vytvorený za konkrétnym účelom a jeho konfigurácia je dôsledne premyslená. Zámer útočníka môže byť špionáž siete, vytvorenie **backdooru**[5], odopretie služieb, alebo krádež citlivých informácií od pripojených používateľov.
- **Bezpečnostný pracovník** – Takto vytvorený falošný prístupový bod slúži na bezpečnostné testovanie siete, jej robustnosti a zabezpečenia. Zo získaných analýz sú vykonané ďalšie bezpečnostné opatrenia v sieti. Zámerne vytvorený prístupový bod, bez ďalšieho pripojenia do siete, za účelom prilákania útočníkov sa označuje ako **honeypot**[6].
- **Neznalý používateľ** – Najväčší počet nežiaducich prístupových bodov je vytváraných bežnými používateľmi. Účel vytvorenia týchto prístupových bodov môže byť úmyselné vyhnutie sa nastavenej bezpečnostnej politiky pri pripojení na internet, alebo zvýšenie vysielaného signálu. Tieto nežiaduce prístupové body sa nazývajú **Rogue AP**[7] a patria sem aj zdieľané prístupové body z mobilného zariadenia.

[4]Wi-Fi Pineapple sa považuje za profesionálne zariadenie na bezpečnostný audit. [36]

[5]Zadná brána do lokálnej siete dostupná z vonkajšej siete.

[6]Pre útočníka na prvý pohľad zraniteľné miesto v sieti, na ktoré sa "nalepí".

[7]Takto vytvorené prístupové body zahlcujú pásmo, čím môžu znížiť rýchlosť pripojenia.

Z pohľadu typu pripojenia do siete sú rozdelené na:

- **Bez pripojenia** – Prístupové body bez pripojenia do siete využívajú na získanie citlivých informácií sociálne inžinierstvo a nevedomosť používateľa. Podvrhnutím známych webových stránok môže útočník získať prihlasovacie údaje používateľa, alebo vytvorením falošného prihlasovacieho portálu k pripojeniu na internet dokáže získať heslo k existujúcej bezdrôtovej sieti bez nutnosti jeho dešifrovania. [37]
- **Neautorizované** – Tieto prístupové body sú fyzicky pripojené do internej siete a umožňujú neautorizovaný a nemonitorovaný prístup. Rogue AP nie sú spravované administrátorom siete čo umožňuje útočníkovi využiť takto vytvorený falošný prístupový bod na útok s mužom uprostred (kapitola 2.3).
- **Podvrhnuté** – Prístupové body poskytujúce úplný prístup do siete za účelom zbierania dát a informácií o jej prevádzke a pripojených používateľoch. Často sú podvrhnuté prístupové body doplnené o špeciálne nástroje na dešifrovanie komunikácie či zachytenie rôznych privátnych kľúčov[8].

Detekcia falošných prístupových bodov vzhľadom na ich úmyselnú konfiguráciu za legitímny prístupový bod **je dosť obtiažna**. V praxi sa pri detekcií využívajú dve detekčné metódy, ktoré pod sebou zahrňujú konkrétne technické podrobnosti a mali by sa navzájom dopĺňať.

Každý prístupový bod zanecháva jedinečnú stopu v sieti – **signatúru**. Pri detekcií falošných prístupových bodov sa vyhľadávajú a porovnávajú parametre, ktoré sú **vysielané prístupovým bodom vždy** a bez jednoduchej možnosti modifikácie útočníkom. Patria sem signatúry:

- MAC adresa prístupového bodu.
- Časové značky, ktoré informujú používateľov ako dlho prístupový bod vysiela od posledného zapnutia.
- Sila signálu s kombináciou frekvencie, zvoleného kanálu a iných parametrov, ktoré sú ťažko reprodukovateľné vzhľadom na konkrétnu polohu.
- Signatúry konkrétneho výrobcu zariadenia ako názov, či špecifická kombinácia fyzického nastavenia[9].

Anomálie sú vhodnou metódou na detekciu falošných prístupových bodov už v existujúcej infraštruktúre. Pri falošných prístupových bodoch môžu vzniknúť anomálie v prípade:

- Zvýšenia počtu vysielaných SSID v sieti.
- Vysielania dvoch rovnakých BSSID v sieti.

[8]Nástroj SSLstrip umožňuje degradovať zabezpečenú komunikáciu do otvorenej formy. [35]

[9]Podporované rýchlosti, pracovné pásma, zabezpečenia a pod.

- Zvýšenia sily signálu nad priemernú hodnotu pridaním silnejšej antény, alebo posunu prístupového bodu bližšie k detektoru.
- Zvýšenie počtu deautentizačných požiadavkov na odpájanie pripojených používateľov v sieti.

Vysoká efektivita kybernetických útokov s využitím falošného prístupového bodu **priamo súvisí s nízkymi technickými znalosťami bežných používateľov**, ktorí častokrát nepoznajú riziká pripojenia sa k neznámym prístupovým bodom.

Bezpečnostné odporúčania pre používateľov sú nasledovné:

- **Nepripájanie sa k neznámym a nezabezpečeným Wi-Fi sieťam**
- **Používanie šifrovacích algoritmov a silných hesiel**
- **Používanie špeciálnej aplikácie na sledovanie podozrivej aktivity**
- **Pravidelná bezpečnostná aktualizácia zariadení**
- **Vypínanie Wi-Fi pripojenia na zariadeniach počas ich nečinnosti**

2.3 Kybernetické útoky s využitím falošného prístupového bodu

Falošný prístupový bod je útočníkmi využívaný ako úvodný krok k ďalším typom kybernetických útokov. Najčastejšie útoky a ich detekcie s využitím falošného prístupového bodu sú:

- **Útok s mužom uprostred**.
- **Útok zlé dvojča**.
- **KARMA útok**.
- **Deautentizačný útok**.
- **Útok zahltenia frekvencii**.

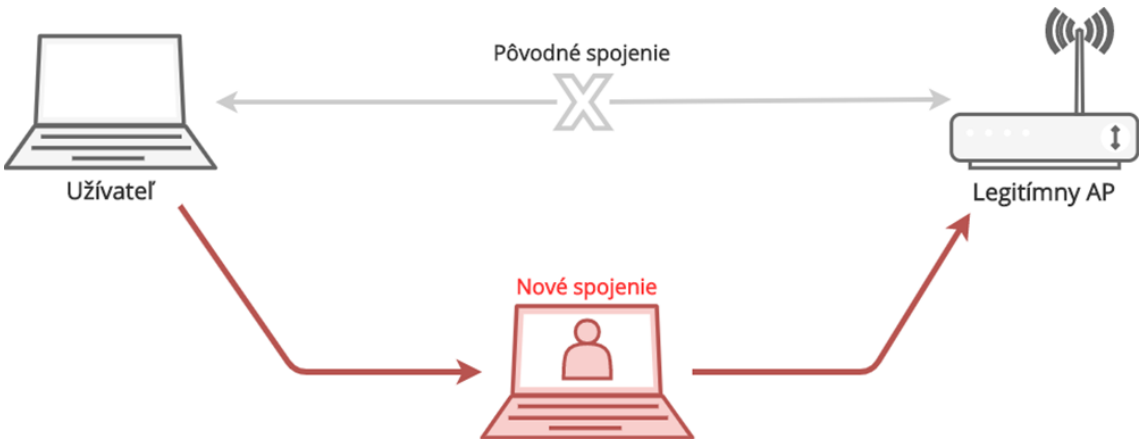
Útok s mužom uprostred

Základnou myšlienkou **útoku s mužom uprostred** je vloženie útočníka do komunikácie medzi používateľa a legitímny prístupový bod. Útočník sfalšovaním MAC adries zariadení dokáže existujúce pripojenie rozdeliť a presmerovať ho cez seba. Cieľom útoku je **odpočúvanie a úprava komunikácie za účelom získania citlivých informácií od používateľa**. Verzií útoku je viac a rozlišujú sa využitím zraniteľnosti protokolu: [35, 38]

- **DNS – Domain Name Server** – Služba mapujúca preklady doménových mien na IP adresy. Protokol pracuje na aplikačnej vrstve ISO/OSI modelu a útok spočíva vo falošnom presmerovaní používateľa na podvrhnuté webové stránky.

- **ARP – Address Resolution Protocol** – Protokol pracuje na sieťovej vrstve ISO/OSI modelu a prekladá IP adresy na príslušné MAC adresy podľa ARP tabuľky. Podvrhnutím ICMP (Internet Control Message Protocol) požiadavky na úpravu údajov v tabuľke na používateľskom zariadení sa útočník dokáže vložiť do komunikácie medzi používateľa a prístupový bod.
- **SSL/TLS – Secure Sockets Layer/Transport Layer Security** – Kryptografický protokol na prezentačnej vrstve ISO/OSI modelu, ktorý má za úlohu vytvoriť zabezpečené pripojenie medzi dvomi stranami. Útočník dokáže HTTPS (Hypertext Transfer Protocol Secure) pripojenie degradovať na nezabezpečené HTTP, alebo pomocou falošných certifikátov prinútiť používateľa používať útočníkom vygenerovaný certifikát.
- **DHCP – Dynamic Host Configuration Protocol** – Protokol na aplikačnej vrstve ISO/OSI modelu je využívaný na distribúciu sieťových nastavení na zariadenia v sieti. Útočník s využitím vlastného DHCP serveru dokáže efektívne zmeniť adresu východzej brány a vložiť sa do prebiehajúcej komunikácie.

Pri **detekcií útoku s mužom uprostred** platí, že útočník sa snaží svoju existenciu skryť a k tomu prispôsobuje aj svoje chovanie v sieti. V bezdrôtových sieťach na fyzickej a spojovej vrstve je **detekcia útoku možná iba s využitím vysielaných informácií od okolitých prístupových bodov**, ktoré analyzuje detekčný systém v reálnom čase. Jednotlivé metódy detekcie sú viac popísané pri konkrétnych útokoch. [39]



Obr. 2.6: Schéma útoku s mužom uprostred.

Útok zlé dvojča

Najznámejší útok s použitím falošného prístupového bodu označovaný ako zlé dvojča (Evil Twin) má za cieľ presmerovať používateľa na podvrhnuté webové stránky a získať jeho citlivé údaje. Signatúry falošného prístupového bodu sú dôsledne klonované podľa známych signatúr zo zachytených manažment rámcov legitímneho prístupového bodu. Takto vytvorený falošný prístupový bod je pre bezdrôtové zariadenia takmer nerozpoznateľný. Spôsoby zapojenia falošného prístupového bodu sú do lokálnej siete (Obr. 2.7A) alebo do vlastnej siete (Obr. 2.7B).

V minulosti operačné systémy umožňovali na základe prijatia rovnakých informácií o prístupovom bode automaticky pripojiť používateľa k bodu, ktorý vysiela silnejší signál. Väčšina dnešných operačných systémov si už vytvára vlastné signatúry o bezdrôtových sieťach a preto k úspešnému **prepojeniu používateľa na falošný prístupový bod je nutné využiť útok zahltenia legitímneho prístupového bodu deautentizačnými požiadavkami** (kapitola 2.3, scenár 3.12 a 3.18).

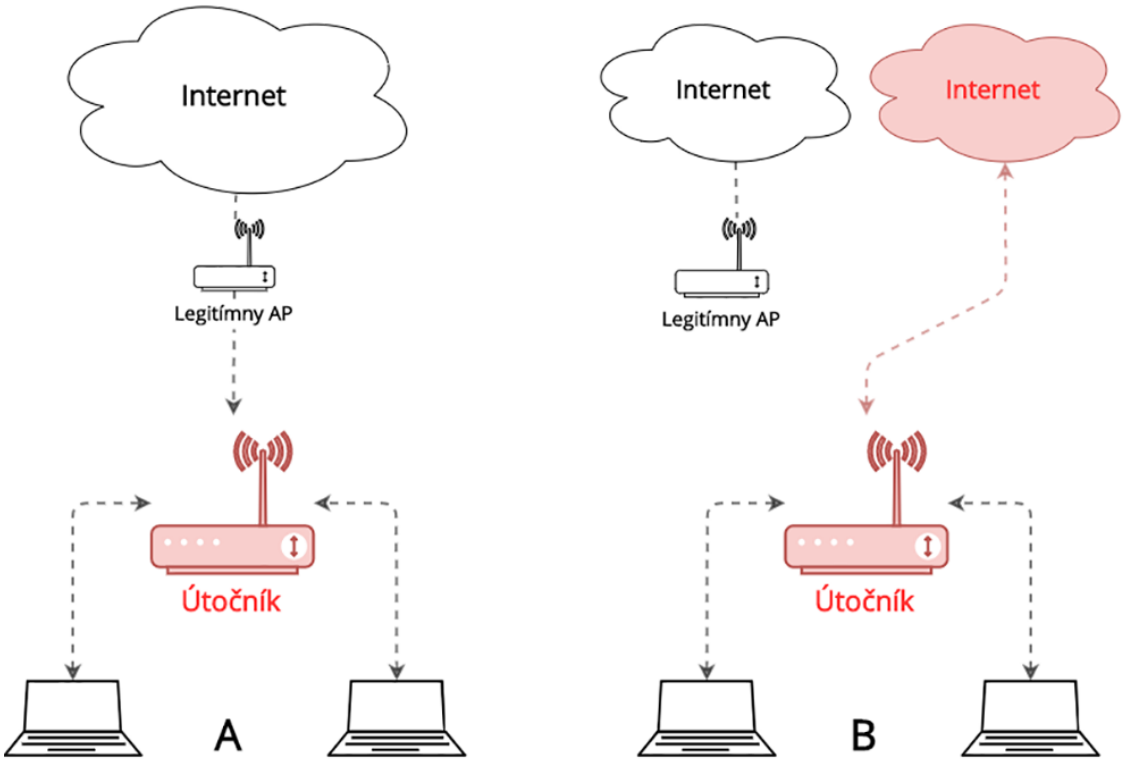
Úspešnosť detekcie útoku zlé dvojča závisí na konfigurácií falošného prístupového bodu a sieti, v ktorej je umiestnený. Spôsoby detekcie sa rozdeľujú na administrátorsky a používateľsky orientované riešenia. Administrátor zvyčajne disponuje zoznamom autorizovaných prístupových bodov v sieti, ktorý pomocou špeciálnych nástrojov a techník aktívne monitoruje. Ku známym metódam detekcie patrí:

- Monitorovanie signatúr prístupových bodov pomocou sieťových detektorov.
- Vytvorenie odtlačkov na základe vysielaných rádiových frekvencií. [40]
- Porovnávanie výrobcov bezdrôtových rozhraní v prístupových bodoch.
- Porovnávanie prijatých a vypočítaných časových synchronizačných značiek prístupového bodu. [41, 42]

V poslednej dobe sa viac rozširujú **používateľsky orientované riešenia detekcie**, ktoré využívajú voľne dostupné informácie od prístupových bodov v okolí. Výhodou je detekcia priamo na zariadení používateľa s minimálnymi výpočtovými nárokmi. Negatívom je vyšší počet falošných upozornení v dôsledku využívania metód založených na čase, či nutnosť úpravy existujúcich protokolov. Používateľsky orientované metódy detekcie sú:

- Výpočet časovej odozvy RTT (Round Trip Time) medzi používateľom a DNS serverom. [43]
- Aktívny mechanizmus s použitím štatistiky pre meranie IAT (Interpacket Arrival Time) medzi legitímnym a falošným prístupovým bodom. [44]
- Odoslanie a monitorovanie špeciálne označených rámcov na server. [45]

Z dôvodu viacerých nedostatkov detekčných metód má každý väčší výrobca prístupových bodov pre firemné siete vytvorené vlastné riešenie[10].



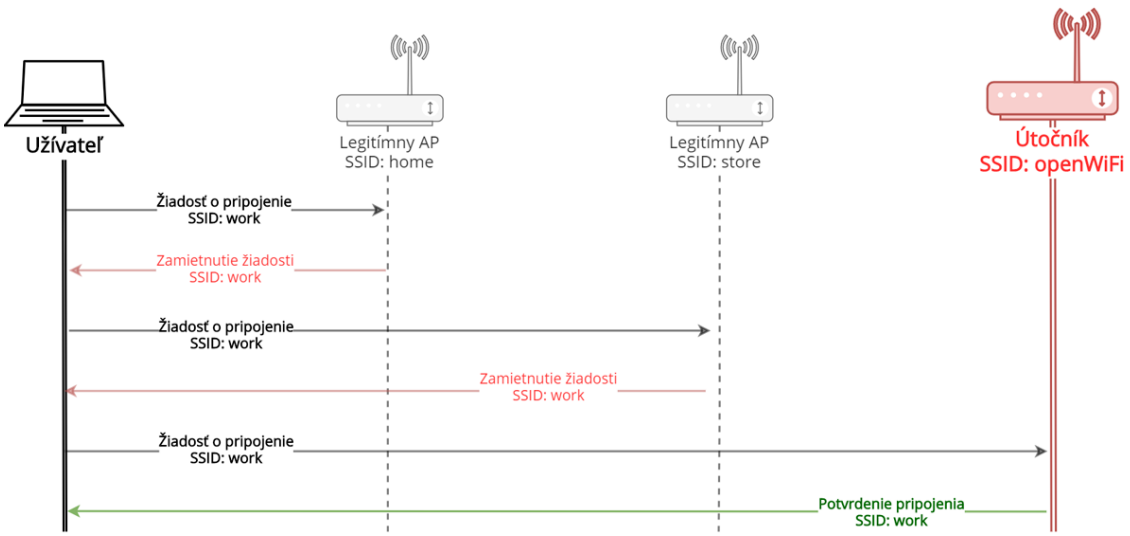
Obr. 2.7: Schéma zapojenia falošného prístupového bodu typu zlé dvojča.

Útok KARMA

KARMA (angl. KARMA Attacks Radioed Machines Automatically) využíva zraniteľnosť metódy aktívneho vyhľadávania prístupových bodov. Aktívne skenovanie funguje na odosielaní požiadavku o pripojenie – **Probe Request od používateľa** k legitímnemu prístupovému bodu. Požiadavka o pripojenie obsahuje signatúry siete, ktoré sú potrebné pre pripojenie k sieti so skrytým vysielaním. Pomocou automatizovaných nástrojov dokáže útočník vysielané požiadavky zachytiť a **podvrhnutím odpovede – Probe Response** donúti používateľa pripojiť sa na vytvorený falošný prístupový bod. Na rozdiel od útoku zlé dvojča, pri ktorom útočník vytvorí falošný prístupový bod a čaká na automatické prepojenie používateľa, útok KARMA je **pre útočníka efektívnejší a bezpečnejší** (scenár 3.14).

[10]Cisco – Rogue Location Discovery Protocol, UniFi – Rogue AP Detection, HP Enterprise – Rogue AP Isolation.

Samotná **detekcia útoku KARMA** vzhľadom na aktívnu interakciu používateľa a prístupových bodov je možná iba komplexnou analýzou sieťovej komunikácie s použitím detekčného systému. Porovnaním odpovedí prístupových bodov, ktoré odosielajú informácie o SSID a BSSID vie detekčný systém vyhodnotiť podozrivú aktivitu. Pokiaľ sa v monitorovanej sieti nachádzajú dve rovnaké odpovede pre jedného používateľa, útok bol úspešne detekovaný. Od roku 2004, keď bol útok KARMA publikovaný sa stále nájdu bezdrôtové zariadenia, ktoré sú zraniteľné aj v dnešnej dobe. [46]



Obr. 2.8: Schéma komunikácie pri útoku KARMA.

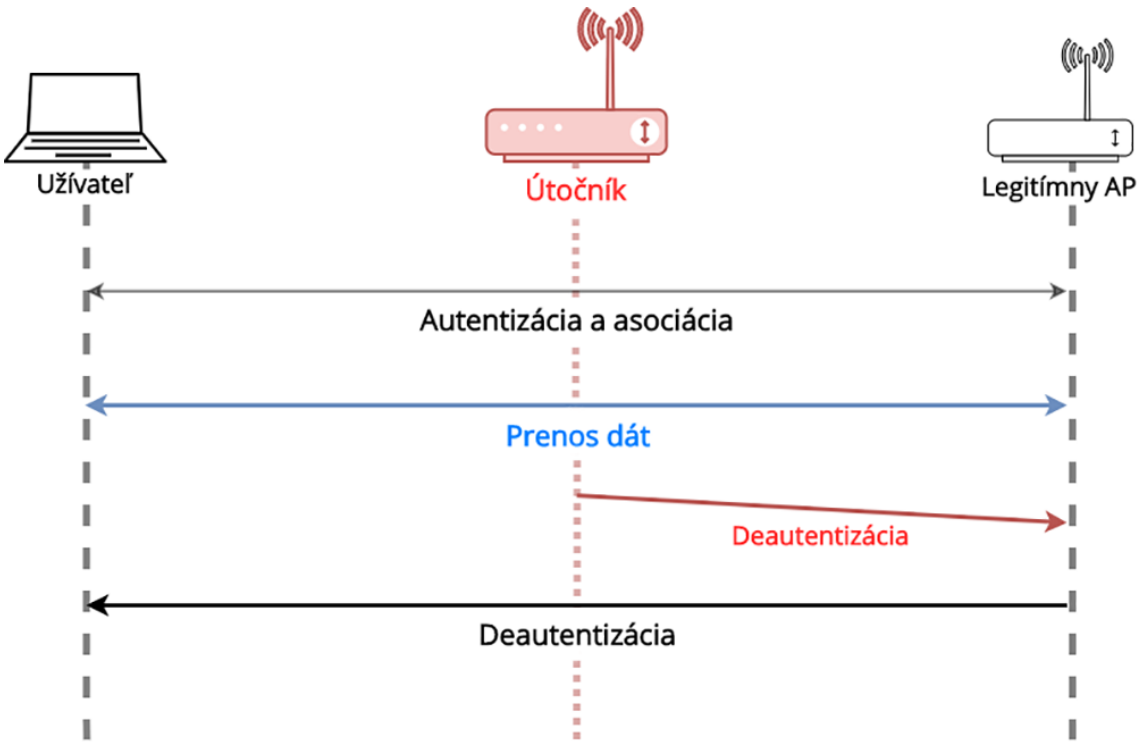
Deautentizačný útok

Deautentizačný útok je **typ útoku odopretia služby**. Útočník využíva podvrhnutie nezabezpečených deautentizačných a deasociačných rámcov, ktoré sú vysielané z falošného prístupového bodu[11] na MAC adresu legitímneho prístupového bodu. V dôsledku ich vysokého počtu a intenzite sú odopreté všetky spojenia.

Deautentizačné a deasociačné rámce môžu byť vysielané buď na konkrétneho používateľa s použitím jeho MAC adresy alebo všetkým pripojeným používateľom s využitím všesmerovej (Broadcast) adresy. Následnou stratou pripojenia sú používatelia automaticky pripojení na falošný prístupový bod, ktorý ich operačný systém vyhodnotil ako stabilné pripojenie k sieti (scenár 3.18).

[11] Štandard 802.11w určuje spôsob šifrovania manažment rámcov, avšak vzhľadom na časovo zložité kryptografické výpočty je rýchlosť pripojenia výrazne znížená čo je dôsledkom jeho nevyužitia.

Detekcia deautentizačného útoku je možná monitorovaním a následnou analýzou sieťovej komunikácie pomocou špeciálnych nástrojov. Keďže manažment rámce sú vysielané v otvorenej forme s využitím už existujúcich metód je detekcia dostatočne rýchla a presná[12]. Napriek tomu sa jedná o jeden z najefektívnejších útokov v bezdrôtových sieťach. [47]



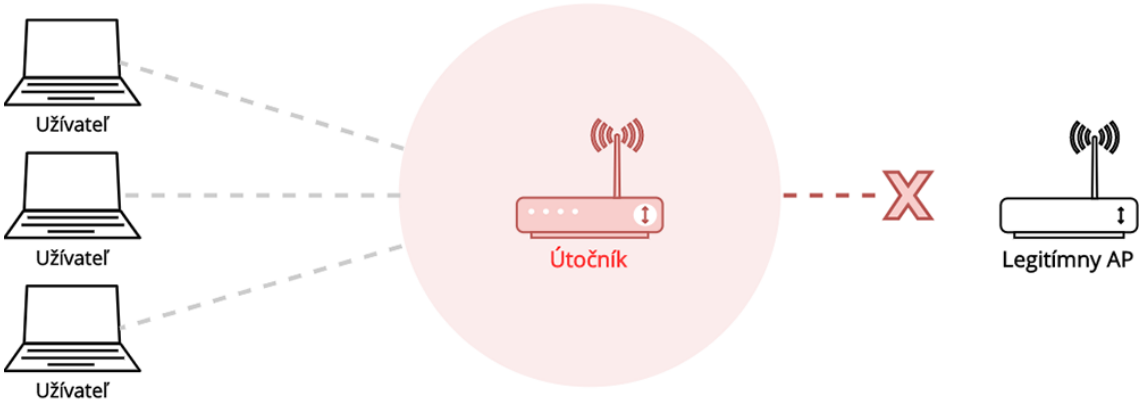
Obr. 2.9: Schéma komunikácie pri deautentizačnom útoku s využitím falošného prístupového bodu.

Útok zahltením frekvencií

Agresívny útok na odopretie služieb (Radio Frequency Jamming) s cieľom zahltenia rádiových frekvencií štandardu Wi-Fi pomocou vysoko-výkonného šumu, alebo vytvorením falošnej komunikácie. Útok zahltenia frekvencie môže byť vytvorený falošnými prístupovými bodmi ale aj zariadeniami, ktoré zdieľajú rovnakú vysielanú frekvenciu (mikrovlnky, mikrofóny, bluetooth zariadenia a iné). Jedná sa o veľmi efektívny útok a vzhľadom na prekrývanie jednotlivých kanálov dokáže ovplyvniť bezdrôtové siete na viacerých kanáloch súčasne.

[12]Založené na programovacom jazyku Python, ktorý umožňuje jednoduché nasadenie na rôzne zariadenia. [48]

Detekcia útoku zahltením frekvencii je možná monitorovaním viacerých metrík ako sila signálu, šum a úspešnosť prenosu dát na prístupových bodoch. Detekcia útokov sa dá zautomatizovať aj s využitím strojového učenia. [49]



Obr. 2.10: Útok vysielania šumu pomocou falošného prístupového bodu.

3 Praktická časť práce

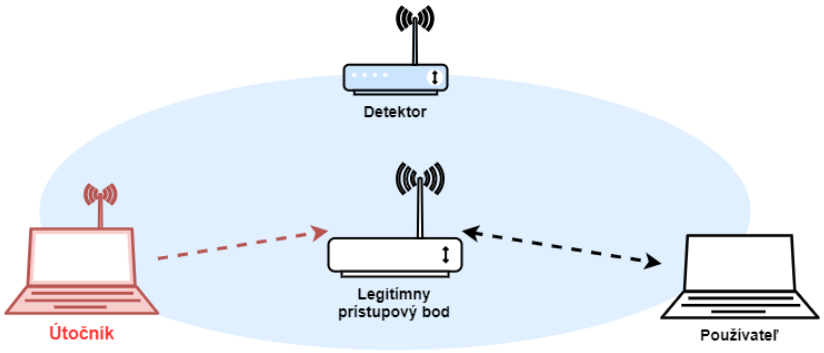
Cieľom praktickej časti práce je vytvorenie experimentálneho pracoviska, zapojenie a konfigurácia zariadení, vytvorenie vlastného návrhu a implementácie metód detekčného systému zameraného na detekciu falošného prístupového bodu v bezdrôtovej lokálnej sieti.

Funkčnosť vlastnej implementácie je otestovaná vo vytvorených scenároch kybernetických útokov. Zo získaných výsledkov práce je vyhodnotený záver doplnený o ďalšie možnosti rozvoja. Vlastný prínos práce uzatvára dotazník o problematike falošných prístupových bodov, ktorý je vyhodnotený z odpovedí 90 respondentov.

3.1 Experimentálne pracovisko

Experimentálne pracovisko predstavuje **model bežnej lokálnej bezdrôtovej siete** vytvorený legitímnym prístupovým bodom doplneným o detektor falošných prístupových bodov. Lokálna bezdrôtová sieť je vytvorená iba za účelom demonštrácie a nedisponuje prístupom k internetu.

- Počítač vpravo predstavuje **bežného používateľa** pripojeného k legitímnemu prístupovému bodu v strede.
- **Útočník** na ľavej strane zachytáva vysielané signatúry legitímneho prístupového bodu a následne vykonáva útoky na odpojenie používateľa a podvrhnutie prístupového bodu.
- **Detektor monitoruje komunikáciu bezdrôtovej siete pomocou integrovaného Wi-Fi adaptéru. Bez nutnosti pripojenia k bezdrôtovej sieti v reálnom čase vyhodnocuje podozrivú aktivitu s prednastavenými signatúrami a informuje používateľa o podozrivých aktivitách.** Poloha detektoru je flexibilná vrámci dosahu vysielaného signálu bezdrôtovej siete.



Obr. 3.1: Schéma zapojenia pracoviska.

Obr. 3.2: Reálne zapojenie pracoviska.

Vytvorenie experimentálneho pracoviska

V experimentálnom pracovisku boli zapojené nasledovné zariadenia:

- **Legitímny prístupový bod Mikrotik** od Lotyšskej spoločnosti patrí medzi najlepšie zariadenia na trhu v pomere cena a výkon. Verzia **hAP ac**^{2} podporuje súčasné vysielanie na frekvenciách 2,4 GHz a 5 GHz, 4 lokálne Gigabit Ethernet porty a samostatný USB port pre pripojenie ľubovolného zariadenia. Prístupový bod MikroTik predstavuje v zapojení legitímny bezdrôtový prístupový bod, na ktorom je pripojený používateľ. Pre jednoduchšiu administráciu zariadenia sa využíva **aplikácia WinBox** (kapitola 3.1).
- **Detektor Raspberry Pi** je jednodoskový počítač s architektúrou ARM určený primárne na edukatívne účely. Vďaka svojej praktickej veľkosti a širokej rozšíriteľnosti je jeho využitie takmer neobmedzené. Operačným systémom je upravená open-source Unix distribúcia **Kali Linux ARM**, ktorý obsahuje upravené ovládače sieťovej karty podporujúcej monitorovací mód. Raspberry Pi predstavuje v schéme zapojenia **bezdrôtovo orientovaný detekčný systém – WIDS**, ktorý na základe pravidelných intervalov monitoruje a analyzuje komunikáciu v nastavenej bezdrôtovej sieti. V prípade detekcie nebezpečnej aktivity v sieti vyvolá upozornenie do konzoly a zaznamená informácie do logovacieho súboru.

- **Falošný prístupový bod s externou Wi-Fi kartou** podporujúcou monitorovací mód od spoločnosti TP-Link[1] predstavuje ideálne zariadenie na vytvorenie a vysielanie falošného prístupového bodu. Hlavnou výhodou je jej jednoduché plug-and-play použitie a široká kompatibilita ovládačov vo väčšine operačných systémov. Ako útočníkov systém je zvolený rovnako **Kali Linux** (kapitola 3.1), ktorý beží vo virtualizovanom prostredí[2]. V schéme zapojenia je externá Wi-Fi karta pripojená do zariadenia útočníka, ktorý vytvára falošný prístupový bod.
- **Prenosný počítač s Windows 10 Pro** predstavuje zariadenie bežného používateľa pripojeného do bezdrôtovej siete. Bezdrôtová komunikácia prebieha na frekvencií 2,4 GHz s využitím integrovanej Wi-Fi karty[3]. Používateľ je podľa schémy pripojený na legitímny prístupový bod a vytvára bežnú sieťovú komunikáciu.

Zoznam **použitých nástrojov** v experimentálnom pracovisku:

- **Kali Linux verzia 2020.1** – Špeciálna distribúcia operačného systému Linux zameraná na penetračné testovanie. Ponúka širokú kolekciu predinštalovaných nástrojov a ovládačov k bezdrôtovým kartám. Patria sem aj populárne sieťové nástroje `aircrack-ng`, ktoré slúžia na analýzu bezdrôtových sietí štandardu 802.11. Samotná konfigurácia falošného prístupového bodu pomocou nástroja `airbase-ng` je popísaná v kapitole 3.1.
- **WinBox verzia 3.23** – Oficiálny nástroj od spoločnosti MikroTik na konfiguráciu legitímneho prístupového bodu. Automatickým pripojením na predvolenú IP adresu `192.168.88.1` sa zobrazí jednoduché grafické používateľské rozhranie, pomocou ktorého je možné prístupový bod nastaviť. Pripojenie používateľa a následná konfigurácia prebieha v bezpečnej šifrovanej forme. Nastavenie prístupového bodu je popísané v kapitole 3.1.
- **Suricata verzia 5.0.3** – Sieťovo orientovaný monitorovací systém, ktorý analyzuje a vyhodnocuje podozrivú sieťovú komunikáciu na základe vytvorených pravidiel a signatúr. Suricata ponúka široké možnosti nastavenia a v ich závislosti dokáže pracovať ako IDS, IPS a NSM (Network Security Monitoring). Štandardným výstupom systému sú záznamy o prevádzke v sieti v otvorenom formáte JSON (JavaScript Object Notation) pre lepšiu integráciu s ďalšími systémami. Inštalácia a bližšia konfigurácia systému Suricata je popísaná v kapitole 3.2.

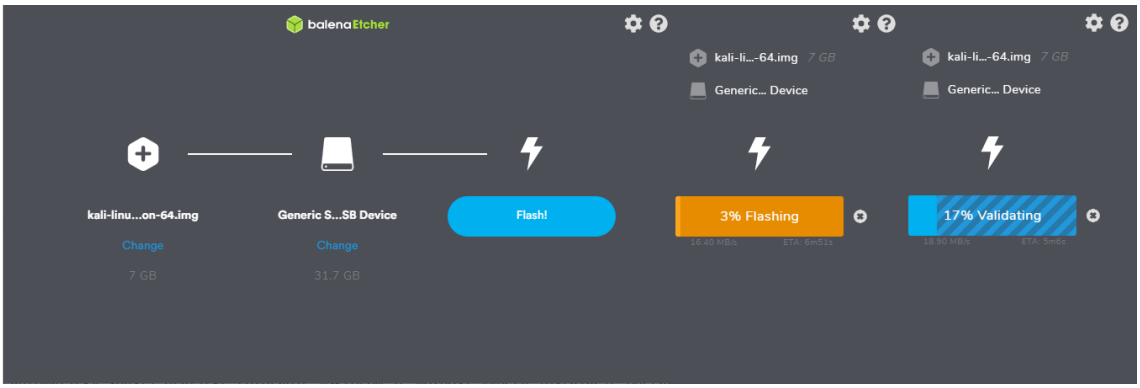
[1] Model TL-WN722N vo verzií 1.
[2] Program Oracle WM VirtualBox v 6.0.20.
[3] Intel® Dual Band Wireless-AC 8260.

- **Kismet verzia 2020-04-R2** – Bezdrôtový sieťový detekčný systém monitorujúci komunikáciu na spojovej vrstve ISO/OSI modelu. Skladá sa z troch častí – jadro, klient a server, čo mu umožňuje použitie viacerých detektorov v monitorovanej sieti pripojených na jeden server. Hlavnou výhodou systému Kismet je pasívne skenovanie siete. V porovnaní so systémom Suricata dokáže pracovať aj s rámcami na spojovej vrstve, ktoré sú vysielané bezdrôtovými prístupovými bodmi. Od verzie 2019 obsahuje aj prehľadné webové rozhranie. Pre zachytávanie a analýzu rámcov je však nutná bezdrôtová karta podporujúca monitorovací mód. Dôvody a nastavenie systému Kismet je popísané v kapitole 3.2.

Konfigurácia experimentálneho pracoviska

Zariadenie Raspberry Pi 4 predstavuje ideálny prenosný detektor prístupových bodov. Pre **základnú inštaláciu a úvodné nastavenie Raspberry Pi** je ho však nutné zapojiť k monitoru, k perifériám, do napájania a samozrejme pripojiť k internetu. Inštalácia systému Kali Linux ARM vyžaduje externý počítač s prístupom k internetu, pamäťovú kartu s kapacitou aspoň 8 GB a program **Etcher**[4].

Prvým krokom je stiahnutie a overenie kópie systému **Kali Linux Raspberry Pi 2020.1a** z oficiálnej stránky Offensive Security[5]. Vložením pamäťovej karty do počítača sa stiahnutý obraz systému pomocou programu Etcher prekonvertuje na plnohodnotný operačný systém Kali Linux ARM spustiteľný z pamäťovej karty.

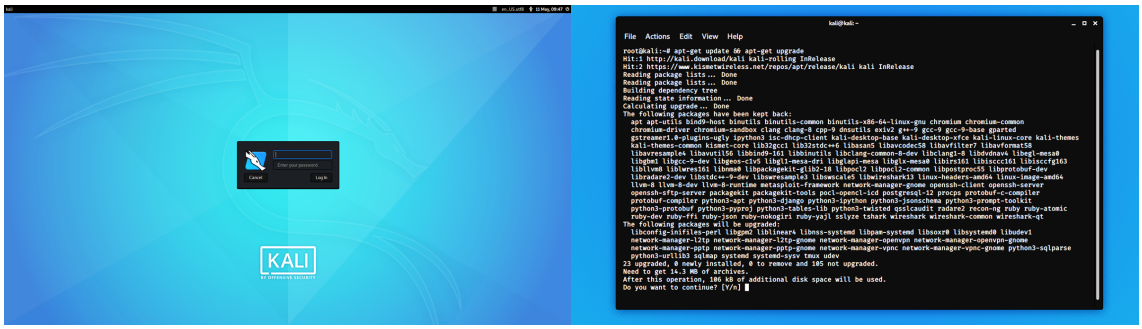


Obr. 3.3: Inštalačný nástroj Etcher.

Pre prvé zapnutie operačného systému Kali Linux ARM je nutné vložiť pamäťovú kartu do Raspberry Pi a zapojením napájania sa po chvíli automaticky spustí grafické rozhranie. Ak sa nevyskytla žiadna komplikácia, operačný systém automaticky

[4]https://www.balena.io/etcher/
[5]https://www.offensive-security.com/kali-linux-arm-images/

zobrazí grafické prihlásenie do systému. Po zadaní a zmene základného hesla príkazom `passwd` je nutné Raspberry Pi pripojiť k internetu a príkazom `sudo apt-get update && apt-get upgrade` automaticky stiahnuť najnovšie balíčky.



Obr. 3.4: Prihlasovacia obrazovka a konzola systému Kali Linux ARM.

Nastavenie monitorovacieho módu na integrovanej Wi-Fi karte je potrebné pre pasívne zachytávanie prenášaných rámcov v bezdrôtovej sieti. Existujú dve možnosti nastavenia.

Prvou je pripojenie externej Wi-Fi karty, ktorá monitorovací mód podporuje. V prípade použitia bežného operačného systému je nutné nainštalovať dodatočné ovládače, ktoré tento mód odomknú. Avšak **väčšina výrobcov externých Wi-Fi kariet zámerne nepodporuje túto funkcionalitu** a preto získanie a nainštalovanie kompatibilných ovládačov je častokrát nemožné.

V takomto prípade prichádza na rad použitie špeciálneho nástroja **Nexmon**, ktorý umožňuje prepísanie originálnych ovládačov a tým odomknúť monitorovací mód aj na integrovanej Wi-Fi karte, čím sa zvyšuje flexibilita detektoru. Projekt Nexmon je voľne dostupný a podporuje viaceré zariadenia. [52]

V zozname podporovaných zariadení sa nachádza aj Raspberry Pi B4 s kernelom 4.19, ktorého verzia sa overí zadaním príkazu `uname -a`. Pre konkrétny Wi-Fi čip s označením `bcm43455c0` je v tabuľke (obr. 3.5) uvedená verzia ovládača `7_45_189` a jeho podporované módy.

Funkčnosť nástroja Nexmon bola otestovaná v rámci semestrálneho projektu, pri ktorom bola na zariadení Raspberry Pi 4 nainštalovaná verzia operačného systému Raspbian. Základné ovládače tohto systému nepodporujú monitorovací mód na integrovanej Wi-Fi karte a **použitím ovládačov Nexmon vznikala vysoká nestabilita a nutnosť pravidelného reštartovania detektoru**.

Po konzultácií vzniknutých problémov bol vymenený operačný systém za Kali Linux ARM. Tento operačný systém už v sebe integruje ovládače podporujúce monitorovací mód a sú priamo kompatibilné so zariadením Raspberry Pi 4. Inštalácia operačného systému Kali Linux je popísaná v kapitole 3.1.

Supported Devices

The following devices are currently supported by our nexmon firmware patch.

WiFi Chip	Firmware Version	Used in	Operating System	M	RT	I	FP	UC	CT
bcm43430a1[1]	7_45_41_26	Raspberry Pi 3 and Zero W	Raspbian 8	X	X	X	X	X	O
bcm43430a1[1]	7_45_41_46	Raspberry Pi 3 and Zero W	Raspbian Stretch	X	X	X	X	X	O
bcm43455c0	7_45_154	Raspberry Pi B3+/B4	Raspbian Kernel 4.9/14/19	X	X		X	X	
bcm43455c0	7_45_189	Raspberry Pi B3+/B4	Raspbian Kernel 4.14/19	X	X		X	X	
bcm4356	7_35_101_5_sta	Nexus 6	Android 7.1.2	X	X		X	X	O
bcm4358	7_112_200_17_sta	Nexus 6P	Android 7 Stock	X	X		X	X	O
bcm4358	7_112_201_3_sta	Nexus 6P	Android 7.1.2 Stock	X	X		X	X	O
bcm4358[2]	7_112_300_14_sta	Nexus 6P	Android 8.0.0 Stock	X	X	X	X	X	O

Obr. 3.5: Tabuľka podporovaných zariadení Nexmon.

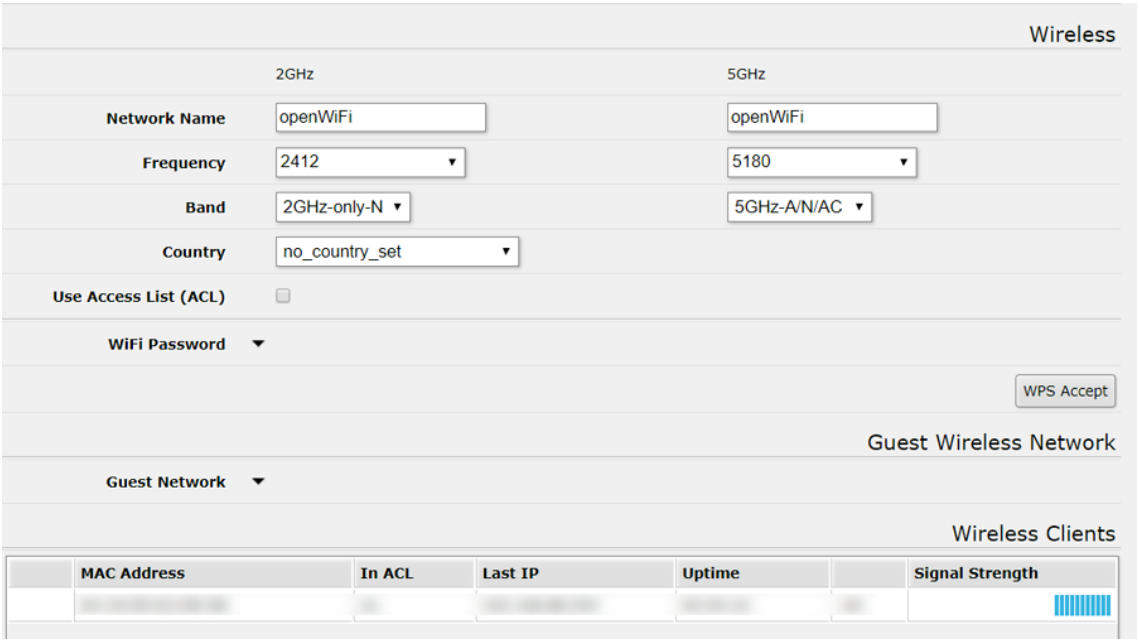
Vytvorenie legitímneho prístupového bodu na zariadení Mikrotik hAP ac[2]. Tieto prístupové body sú dodávané s predvoleným nastavením, ktoré vysiela bezdrôtovú sieť ihneď po zapojení do napájania. Konfigurácia zariadenia je možná ako káblovým pripojením cez Ethernet port, tak aj pomocou pripojenia na vysielanú sieť. Pri každom pripojení na prístupový bod sa overuje dostupnosť najnovšieho systému RouterOS[6]. Po pripojení do vysielanej siete a zadaním IP adresy `192.168.88.1` do webového prehliadača sa zobrazí bez nutnosti zadania prístupových údajov administrácia zariadenia s oknom rýchleho nastavenia – **Quick Set** (obr. 3.6). Pokročilejšia administrácia sa nazýva **WebFig**, ktorá je grafickou nadstavbou terminálu. [51]

Rozhranie WebFig slúži na rozšírenú konfiguráciu legitímneho prístupového bodu (príloha A.2). Pod položkou v hlavnom menu **Wireless** – **wlan1** sú zobrazené informácie o bezdrôtovej sieti s názvom `openWiFi`. Prístupový bod vysiela na frekvencií 2,4 GHz, so šírkou pásma 20 MHz, v štandarde 802.11n a s MAC adresou `C4:AD:34:03:24:DD`.

Zabezpečenie bezdrôtovej siete nie je nastavené a slúži iba za účelom simulácie bežného prístupového bodu na mieste s vysokým počtom pripojených používateľov.

Pre **vytvorenie falošného prístupového bodu** je dôležitá konfigurácia na základe znalostí zachytených signatúr legitímneho prístupového bodu. Vhodným nástrojom v operačnom systéme Kali Linux je balík **aircrack-ng**, ktorý umožňuje vytvorenie falošného prístupového bodu zadaním pár príkazov. [50]

[6] Aktuálna verzia v dobe písania práce je 6.46.6



Obr. 3.6: Webové rozhranie konfigurácie – Quick Set.

Po spustení systému Kali Linux vo virtualizovanom prostredí[7] je ďalším krokom pripojenie a spustenie externej Wi-Fi karty podporujúcej monitorujúci mód. Nasledovnými príkazmi sa vytvorí virtuálne rozhranie na pripojenej Wi-Fi karte a spustí sa zachytávanie sieťovej komunikácie.

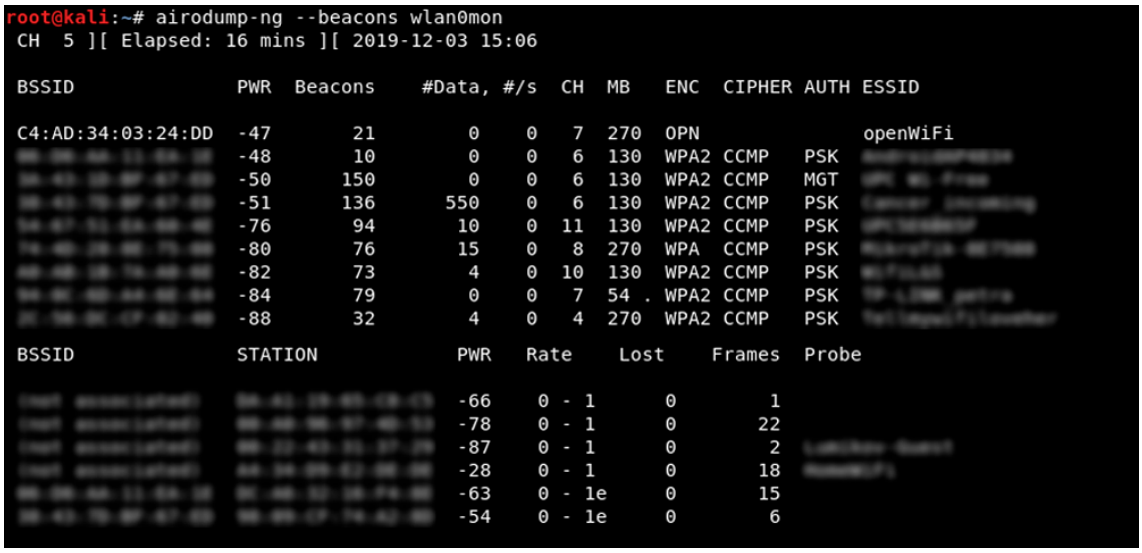
```
sudo airmon-ng check kill
sudo airmon-ng start wlan0
sudo airodump-ng wlan0mon
```

Zachytená komunikácia zobrazuje všetky fyzické adresy prístupových bodov a pripojených používateľov v reálnom čase. Po zachytení rámcov legitímneho prístupového bodu s vysielaným SSID `openWiFi` sa nástrojom **airbase-ng vytvorí falošný prístupový bod** na vytvorenom rozhraní `wlan0mon` s rovnakými signatúrami:

```
sudo airbase-ng -a C4:AD:34:03:24:DD --essid
'openWiFi' -c 7 wlan0mon
```

DHCP služba **dnsmasq** umožňuje úspešné pripojenie používateľov na vytvorený falošný prístupový bod. Konfigurácia služby sa skladá z vytvorenia rozsahu ponúkaných IP adries, vytvorenia sieťovej cesty a nastavenia presmerovania komunikácie cez nástroj **iptables**. Parametre v súbore `dnsmasq.conf` popisujú výber falošného rozhrania, rozsah adries, predvolenej brány a DNS serverov.

[7]Voľne dostupný na URL adrese `https://www.offensive-security.com/kali-linux-vm-vmware-virtualbox-image-download/`



Obr. 3.7: Zachytená sieťová komunikácia nástrojom `airodump-ng`.

```
interface=at0
dhcp-range=192.168.0.10, 192.168.0.250,
   255.255.255.0, 12h
dhcp-option=3, 192.168.0.1
dhcp-option=6, 192.168.0.1
server=8.8.8.8
listen-address=127.0.0.1
```

Spustenie a nastavenie falošného rozhrania ako predvolenej brány:

```
sudo ifconfig at0 up
sudo ifconfig at0 192.168.0.1 netmask 255.255.255.0
```

Nastavenie nemaskovaného presmerovania sieťovej komunikácie z virtuálneho rozhrania na `wlan0mon`:

```
sudo route add -net 192.168.0.0 netmask 255.255.255.0
    gw 192.168.0.1
sudo iptables -P FORWARD ACCEPT
sudo iptables -t nat -A POSTROUTING -o wlanm0mon -j
   MASQUERADE
sudo echo 1 > /proc/sys/net/ipv4/ip_forward
```

Posledným príkazom sa spustí služba DHCP z vytvoreného konfiguračného súboru:

```
sudo dnsmasq -C /dnsmasq.conf -d
```

3.2 Detekcia kybernetických útokov pomocou systémov Suricata a Kismet

Systém Suricata

Prvá implementácia detekčného systému je zameraná podľa zadania práce na voľne dostupný detekčný systém **Suricata**. Inštalácia systému Suricata sa skladá z oficiálneho inštalačného balíka a otvorenej databázy signatúr známych útokov[8].

```
sudo apt-get install suricata
sudo apt-get install suricata-update
```

V prehľadnom konfiguračnom súbore `suricata.yaml` vytvoreným **značkovacím jazykom YAML** sa nachádzajú základné nastavenia:

- Rozsah IP adries monitorovanej siete označenej ako `HOME_NET`.
- Rozhranie na monitorovanie sieťovej komunikácie.
- Pripojenie súborov s vytvorenými pravidlami.
- Vytvorenie log súborov v rôznych formátoch.

Detekčný systém Suricata na svoju činnosť potrebuje aktualizovanú databázu pravidiel, ktoré popisujú určitú signatúru podozrivej aktivity.

```
sudo suricata-update
sudo systemctl restart suricata
```

Zobrazenými príkazmi sa stiahne aktuálna databáza signatúr, ktorá tvorí súbor `suricata.rules`[9] a po reštartovaní systému Suricata sa pravidlá aplikujú. Súbor obsahujúci pravidlá je predvoleným zdrojom signatúr pre systém. Na **pridanie vlastných signatúr je nutné vytvoriť vlastný súbor** a jeho súborovú cestu vložiť do hlavného konfiguračného súboru.

```
default-rule-path: /etc/suricata/rules
rule-files:
 - suricata.rules
 - custom.rules
```

Obr. 3.8: Konfigurácia pravidiel v súbore `suricata.yaml`.

Jednotným príkazom sa detekčný systém Suricata spustí a načíta základné nastavenia zo súboru `suricata.yaml`. Parameterom `-i wlan0mon` sa zvolí rozhranie, na ktorom bude detekčný systém spustený a parametrom `-vvvv` zas debugovací mód.

```
sudo suricata -i wlan0mon -vvvv
```

[8] Emerging Threats Open Ruleset

[9] Súboru obsahuje vyše 28-tisíc signatúr útokov a jeho prvotná veľkosť je vyše 15 MB.

Výsledkom detekcie detekčného systému Suricata sú logovacie súbory, ktoré obsahujú informácie o podozrivej komunikácií. Systém každým spustením vytvára hneď niekoľko súborov, ktoré sú v reálnom čase aktualizované. Súbor `suricata.log` obsahuje informácie o aktuálnej konfigurácií systému. Súbor `fast.log` zachytáva aktuálnu komunikáciu, ktorú následne prepisuje do súboru `stats.log`. Podľa konfigurácie `suricata.yaml` je možné do súboru `eve.json` zapísať zachytené podozrivé udalosti v otvorenom formáte JSON.

Systém Kismet

Druhou implementáciou na detekciu falošných prístupových bodov je voľne dostupný **detekčný systém Kismet**, ktorý dokáže pracovať s bezdrôtovými rámcami na spojovej vrstve ISO/OSI modelu.

Inštalácia systému Kismet je rovnako jednoduchá ako pri systéme Suricata. Po pridaní cesty k repozitáru[10] sa jednotným príkazom stiahne a nainštaluje najnovšia verzia[11], ktorá pre svoju plnú funkcionalitu vyžaduje bezdrôtové sieťové rozhranie podporujúce monitorovací mód, ktorého inštalácia je popísaná v predchádzajúcej kapitole 3.1.

```
sudo apt-get install kismet
```

Pred spustením systému Kismet je nutné zapnúť virtuálne rozhranie `wlan0mon` na monitorovanie siete.

```
sudo kismet -c wlan0mon
```

Príkazom sa spustí detekčný systém Kismet pod administrátorskými privilégiami[12] s monitorovaním vytvoreného virtuálneho rozhrania. Zachytená sieťová komunikácia je vysielaná na lokálny webový server `http://localhost:2501`.

Konfigurácia detekčného systému je možná **úpravou konfiguračných súborov** umiestnených v priečinku `/etc/kismet/`. Na nastavenie upozornení systému nielen na detekciu falošného prístupového bodu slúži súbor `kismet_alerts.conf`. Pre vytvorenie pravidla je využitá funkcia **apspoof**, ktorá zo zadaných parametrov[13] vytvorí jedinečnú signatúru, ktorú následne detekčný systém porovnáva so zachytenou komunikáciou. Pri každej aktualizácií pravidiel je nutné detekčný systém Kismet reštartovať.

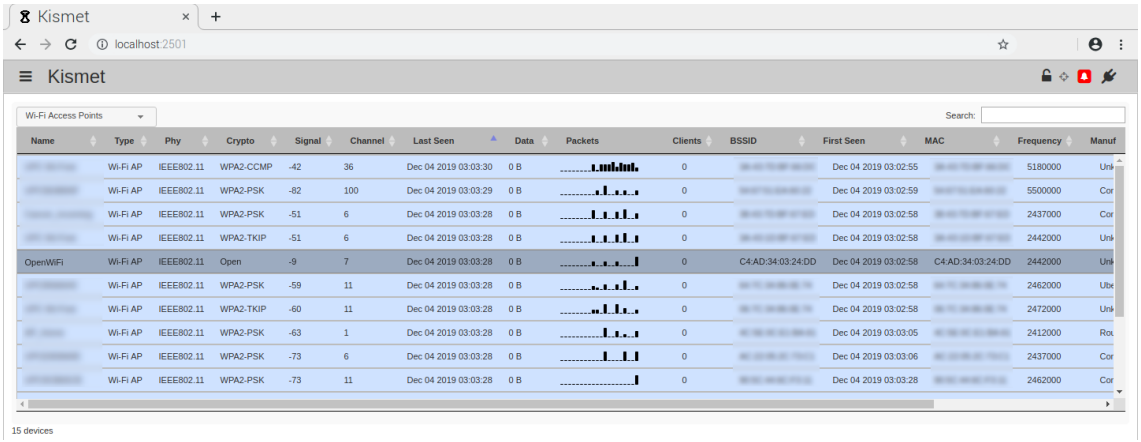
V prípade výskytu zhody so zadaným pravidlom, **systém Kismet upozorní používateľa zobrazením varovnej notifikácie** s informáciami o detekcií falošného prístupového bodu v konzolovom riadku a pod položkou upozornenia.

[10] `https://www.kismetwireless.net/docs/readme/packages/`

[11] Kismet 2020-04-R2

[12] Bez použitia príkazu `sudo` nie je možné monitorovanie komunikácie na zvolenom rozhraní.

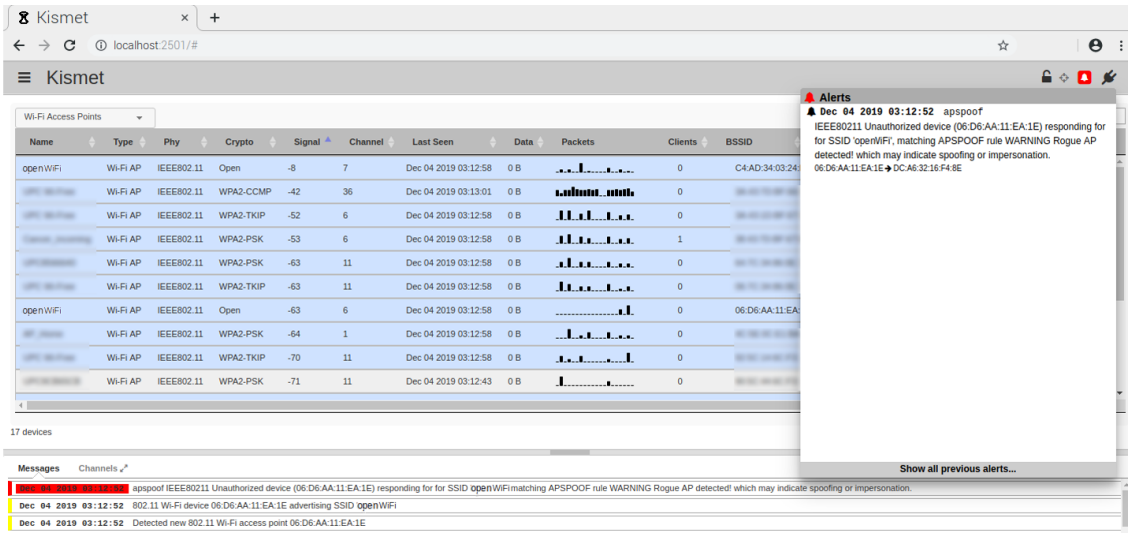
[13] Názov pravidla, SSID vysielanej siete a BSSID adresa prístupového bodu.



Obr. 3.9: Webové rozhranie systému Kismet.

```
apspoof=WARNING Rogue AP detected!:ssid="openWiFi",validmacs="C4:AD:34:03:24:DD"
```

Obr. 3.10: Pravidlo na detekciu falošného prístupového bodu.



Obr. 3.11: Detekcia falošného prístupového bodu.

Výsledky implementácie systémov Suricata a Kismet

Po dlhom testovaní konfiguračných nastavení sa ukázalo, že **detekčný systém Suricata nedokáže pracovať so zachytenou komunikáciou na spojovej vrstve** ISO/OSI modelu. Pre detekciu kybernetických útokov na spojovej vrstve nie je vhodný a preto nesplňuje zadanie práce. V rámci ďalšieho výskumu sa ako vhodným riešením ukázal voľne dostupný detekčný systém Kismet, ktorý ponúkal široké možnosti monitorovania bezdrôtových sietí aj na spojovej vrstve a čiastočne spĺňal zadanie práce. Avšak vzhľadom na absenciu pokročilej detekcie útokov s využitím falošného prístupového bodu bola práca zameraná na **návrh a vytvorenie vlastnej implementácie** detekčného systému v programovacom jazyku Python.

3.3 Vlastná implementácia

Analýzou získaných výsledkov z predchádzajúcich detekčných systémov Suricata a Kismet bol **vytvorený vlastný návrh implementácie** detekčného systému s viacerými metódami na detekciu kybernetických útokov s využitím falošného prístupového bodu na spojovej vrstve. Vlastný návrh funkcionality detekčného systému sa skladá z viacerých modulov, ktoré sú zobrazené v podobe diagramu (príloha B.1).

Zoznam implementovaných modulov:

- **Správa bezdrôtového rozhrania** – obsluha bezdrôtovej karty s monitorovacím módom a jej pravidelná zmena zachytávaných frekvencii.
- **Skenovanie bezdrôtových sietí v okolí** – pasívne získavanie informácií o prenášaných rámcoch, ktoré systém ďalej spracúva.
- **Analýza rámcov** – filtrovanie zachytených rámcov protokolu 802.11 pre spracovanie potrebných signatúr.
- **Tvorba odtlačkov signatúr** – vytváranie a ukladanie jedinečných odtlačkov zo zachytených signatúr prvých rámcov do globálnej databázy.
- **Spracovanie signatúr a detekcia útokov** – detekčný algoritmus porovnávania signatúr zachytených rámcov (príloha B.2).
- **Logovanie informácií** – zobrazenie dôležitých informácii do konzoly a ich zápis do logovacieho súboru.

Pri **realizácií vlastnej implementácie** bol podľa zadania, zvoleným **programovacím jazykom Python 3.8**. Vďaka jeho hlavným výhodám ako sú rýchlosť, prenositeľnosť medzi zariadeniam a nenáročnosť na výpočtový výkon, bola realizácia detekčného systému na architektúre ARM zariadenia Raspberry Pi 4 bezproblémová.

Vlastný **návrh predstavoval vhodnú škálovateľnosť dosiahnutú pomocou jednotlivých modulov**. Ich funkcionalitu zabezpečovali importované balíky, ktoré boli rozdelené na:

Externé balíky – nutnosť dodatočnej inštalácie z externých knižníc:

- **airmon-ng**[14] – nástroj na správu monitorovacieho módu bezdrôtovej karty.
- **scapy**[15] – efektívny nástroj na prácu so sieťovou komunikáciou, ktorý umožňuje zachytávať, modifikovať a dekódovať protokol 802.11 pre všetky rámce na spojovej vrstve.
- **netifaces**[16] – jednoduchý nástroj na správu aktuálnych sieťových rozhraní.

Interné balíky – implementované priamo v oficiálnych knižniciach:

- **logging**[17] – systém na logovanie vzniknutých udalostí, ktorý umožňoval priamy výpis do konzoly, vytvorenie logovacieho súboru a zápis upozornenia.
- **datetime**[18] **a time**[19] – moduly, ktoré spravovali aktuálny dátum a čas.
- **argparse**[20] – modul, ktorý spracovával argumenty zadávané pri spustení programu, na základe ktorých boli nastavené globálne premenné.
- **hashlib**[21] – implementácia hašovacích nástrojov, ktoré vytvárali odtlačky zachytených rámcov.
- **threading**[22] – modul na viacvláknový beh systému.

Moduly systému boli programované postupne. Prvým najdôležitejším modulom bola správa bezdrôtového rozhrania, ktorá riešila kontrolu pripojených rozhraní, výber, otestovanie, zapnutie monitorovacieho módu a zmenu kanálu frekvencii.

Po overení podporovaného rozhrania, bol načítaný modul pre správu zadaných argumentov a hodnôt globálnych premenných. Globálne premenné slúžili ako úložisko zadaných hodnôt s prístupom pre všetky moduly programu. Ak spracovanie načítaných parametrov bolo úspešné, program spustil pasívne zachytávanie sieťovej komunikácie na spojovej vrstve.

Modul na analýzu rámcov rozdeľoval zachytenú komunikáciu podľa obsahu na beacon rámce, probe rámce a deautentizačné rámce (kapitola 2.1). Signatúry beacon rámcov prístupového bodu boli uložené do lokálnej pamäte a z nich bol vytvorený **jedinečný odtlačok pomocou hašovacej funkcie o veľkosti 256 bitov**. Spracovávané signatúry beacon rámcu boli **SSID, BSSID, Kanál, Zabezpečenie, Krajina a základné prenosové rýchlosti**.

[14] `https://www.aircrack-ng.org/doku.php?id=airmon-ng`
[15] `https://scapy.readthedocs.io/en/latest/introduction.html`
[16] `https://pypi.org/project/netifaces/`
[17] `https://docs.python.org/3/library/logging.html`
[18] `https://docs.python.org/3/library/datetime.html`
[19] `https://docs.python.org/3/library/time.html`
[20] `https://docs.python.org/3/library/argparse.html`
[21] `https://docs.python.org/3/library/hashlib.html`
[22] `https://docs.python.org/3/library/threading.html`

Následne boli spracované údaje vložené do globálneho slovníkového poľa, ktoré sledovalo integritu a duplicitu údajov. Kľúčom bola zvolená signatúra fyzickej adresy prístupového bodu – **BSSID**. Hodnotou zas pole údajov prístupového bodu a odtlačok. V prípade zachytenia probe alebo deautentizačných rámcov boli ich signatúry spracované a uložené do lokálnej pamäte.

Druhým najdôležitejším modulom programu bol **algoritmus na porovnávanie signatúr a detekciu útokov**. Modul nadväzuje na zachytávanie a rozdeľovanie rámcov, z ktorých porovnával ďalšie zachytené signatúry so signatúrami v globálnej databáze. Algoritmus tak v **reálnom čase vyhodnocoval zachytené signatúry a detegoval potencionálny útok**.

Po zachytení kybernetického útoku bol **vytvorený záznam s určitým stupňom priority**. Všetky záznamy boli zobrazované do konzoly a zapisované do vytvoreného logovacieho súboru. Ukončenie programu nastalo po prerušení zachytávania rámcov používateľom. Výsledný logovací súbor s aktuálnym dátumom bol uložený do lokálneho priečinku.

Testovanie systému prebiehalo súbežne s jeho realizáciou. Jednotlivé moduly boli navrhnuté tak, aby používateľ nemohol svojou neodbornou činnosťou program znefunkčniť. V prípade výskytu akejkoľvek chyby počas behu programu, vzniklo upozornenie, ktoré bolo vypísané do konzoly a program sa bezpečne ukončil.

Testovanie detekcie útokov (kapitola 2.3) prebiehalo v nasledovných scenároch:

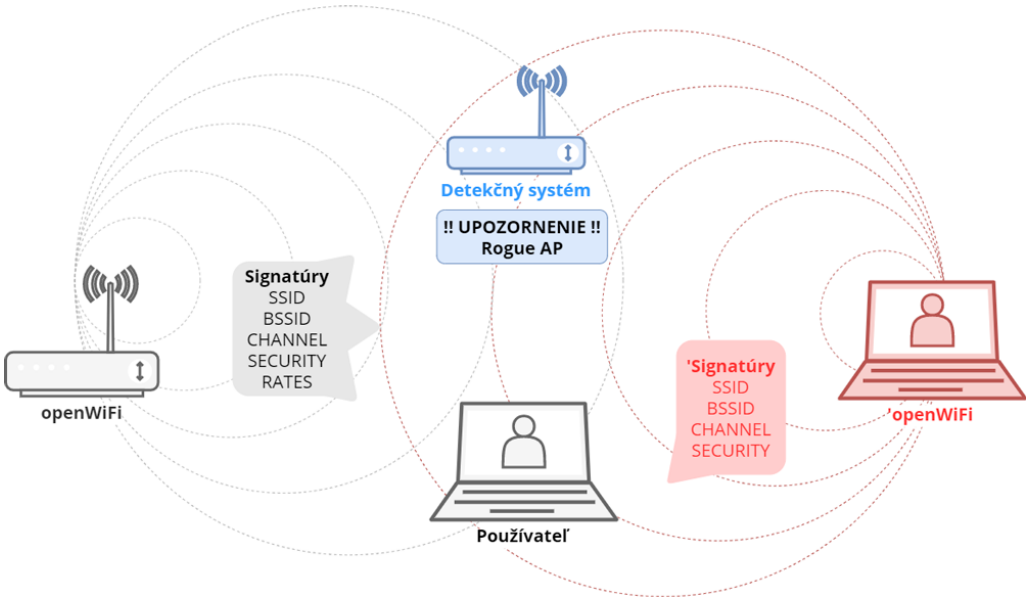
1. **Scenár útoku s podvrhnutím falošného prístupového bodu**.
2. **Scenár KARMA útoku**.
3. **Scenár útoku zahltenia frekvencie beacon rámcami**.
4. **Scenár deautentizačného útoku**.

1. Scenár útoku s podvrhnutím falošného prístupového bodu

1. Legitímny prístupový bod (Mikrotik) vysielal beacon rámce používateľovi (Windows 10) s prednastavenými signatúrami.
2. Rovnaké signatúry zachytil detekčný systém (Raspberry Pi), ktorý si vytvoril záznam a uložil ho do databázy.
3. Útočník (Kali Linux) zachytil signatúry a nástrojom **airbase-ng** vytvoril falošný prístupový bod s rovnakým SSID, BSSID, kanálom a zabezpečením.

```
sudo airbase-ng -a C4:AD:34:03:24:DD --essid
   'openWiFi' -c 7 wlan0mon
```

4. **Detekčný systém zaznamenal vysielanie rovnakých signatúr** pomocou monitorovacieho módu karty a implementované moduly na zachytenie signatúr prístupového bodu, vytvorenie jedinečného odtlačku a algoritmus na porovnávanie signatúr vyhlásili upozornenie na falošný prístupový bod.



Obr. 3.12: Schéma prvého testovacieho scenára.

```
WARNING: ROGUE AP DETECTION! [c4:ad:34:03:24:dd]
WARNING: ROGUE AP DETECTION! [c4:ad:34:03:24:dd] Different channel: 7≠4
WARNING: ROGUE AP DETECTION! [c4:ad:34:03:24:dd] Different rates: [2, 4, 11, 22, 140, 18, 24, 36]≠[2, 4, 11,22]
```

Obr. 3.13: Upozornenie na falošný prístupový bod s rovnakými signatúrami.

```
def analystAP(AP.key, AP.values):
    if not database_AP:
            database_AP[AP.key] = AP.values
            loggingLevels('AP found', 20)
    else:
        if not AP.key in database_AP.keys():
                database_AP[AP.key] = AP.values
                loggingLevels('AP found', 20)
        else:
            database_AP.values[4] != AP.values[4]:
            loggingLevels('ROGUE AP DETECTION', 40)
```

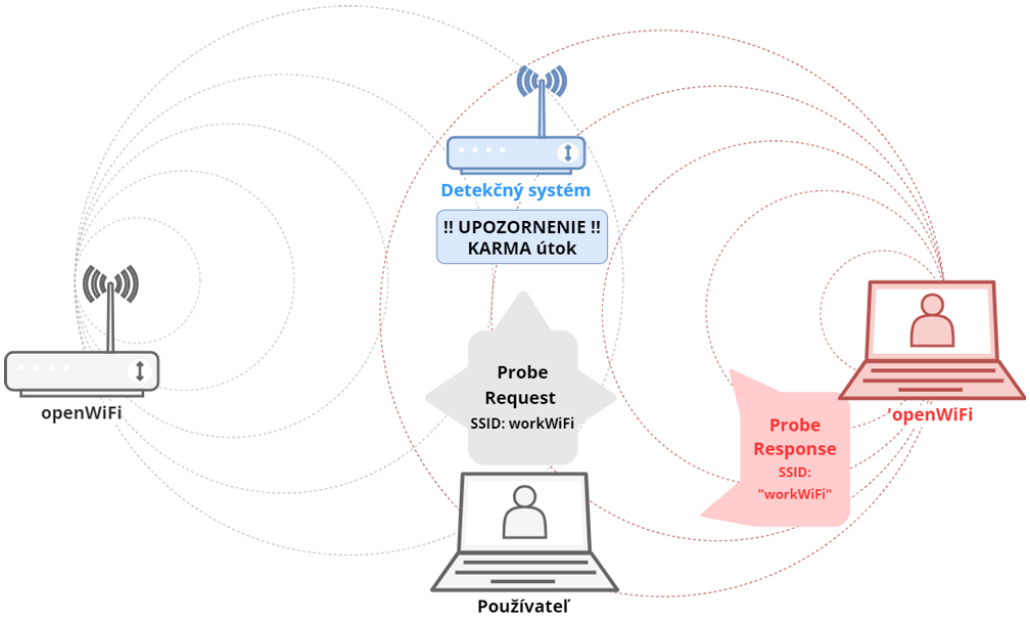
Výpis 3.1: Ukážka pseudo kódu na detekciu falošného prístupového bodu s rovnakými signatúrami.

2. Scenár útoku KARMA

1. Používateľ (Windows 10) vysielal žiadosti o pripojenie (Probe request) k bezdrôtovej sieti, ktorá sa nenachádzala vo fyzickej blízkosti k zariadeniu.
2. Detekčný systém zachytil žiadosti o pripojenie k neexistujúcej sieti a jej signatúry si uložil do databázy. Následne čakal na zachytenie rámca odpovede (Probe response).
3. Útočník (Kali Linux) pomocou nástroja **airbase-ng** zachytil žiadosti používateľa a odoslal mu odpoveď, v ktorej sa vydáva za hľadanú bezdrôtovú sieť.

```
sudo airbase-ng -c 7 -P -C10 -y wlan0mon
```

4. Modul detekčného systému zachytil v krátkom časovom úseku (2 sek.) vysoké množstvo odpovedí na používateľovu žiadosť o pripojenie do neexistujúcej siete. Keďže sa **hľadaná bezdrôtová sieť v globálnej databáze nenachádzala, vyhlásil upozornenie na KARMA útok**.



Obr. 3.14: Schéma druhého testovacieho scenára.

```
Probe req STA: 04:d6:aa:11:ea:1e sending to AP: ff:ff:ff:ff:ff:ff SSID: default
Probe resp AP: 84:16:f9:19:81:6d sending to STA: 84:d6:aa:11:ea:1e SSID: default
WARNING: KARMA ATTACK DETECTION! [84:16:f9:19:81:6d]
WARNING: KARMA ATTACK DETECTION! [84:16:f9:19:81:6d] STA: 04:d6:aa:11:ea:1e SSID: default
```

Obr. 3.15: Upozornenie na falošný prístupový bod s rovnakými signatúrami.

```
sniff(iface=interface,prn=karmaDetection,timeout=2)
```

```
def karmaDetection(frame):
    if frame.haslayer(Dot11ProbeResp):
        bssidAP = frame.addr2
        ssidAP = frame.info.decode('utf-8')
        if bssidAP in databse_KARMA_AP.keys() and ssidAP
           in databse_KARMA_AP.values():
            loggingLevels('KARMA ATTACK DETECTION', 40)
```

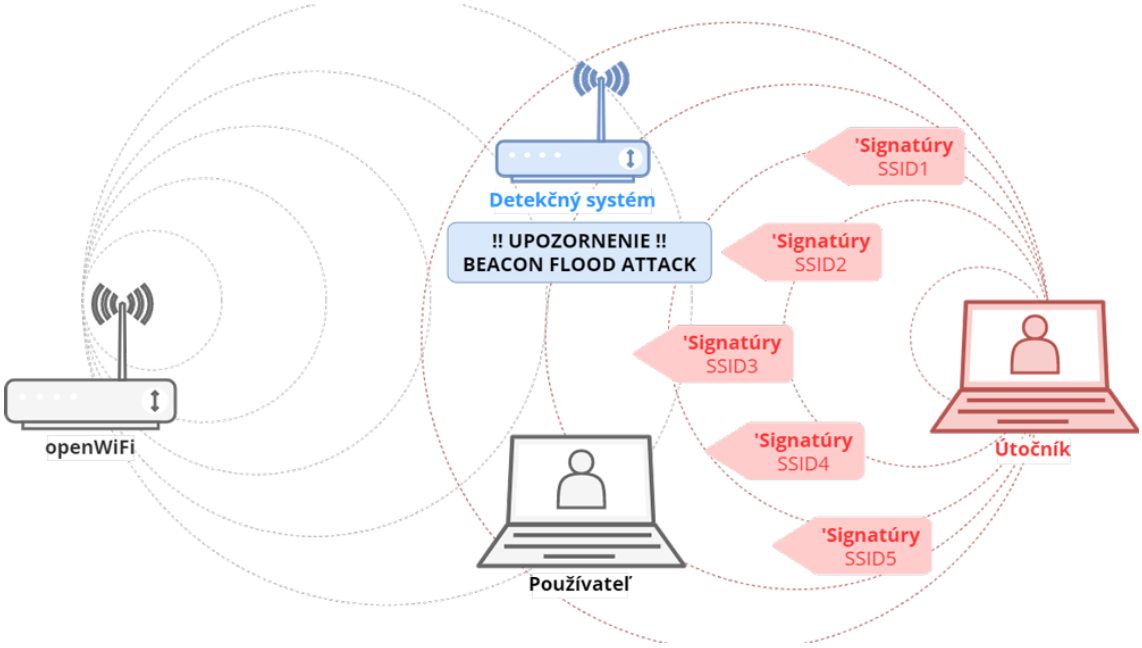
Výpis 3.2: Ukážka pseudo kódu na detekciu útoku KARMA.

3. Scenár útoku zahltenia frekvencie beacon rámcami

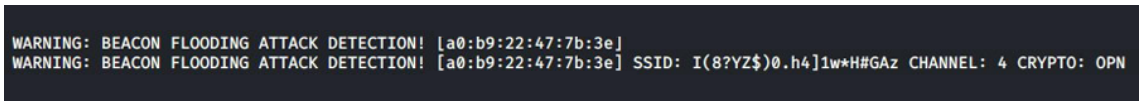
1. Útočník (Kali Linux) pomocou nástroja **mdk3** začal vysielať na rovnakej frekvencii vysoké množstvo falošných beacon rámcov oznamujúcich novú sieť.

```
sudo apt-get install mdk3
sudo mdk3 wlan0mon b
```

2. Moduly detekčného systému zachytili v krátkom časovom úseku (0.3 sek.) vysoké množstvo nových beacon rámcov, ktorých identifikátory siete SSID obsahujú nepovolené znaky a **vyhlásil upozornenie na útok zahltenia frekvencie beacon rámcami**.



Obr. 3.16: Schéma tretieho testovacieho scenára.



Obr. 3.17: Upozornenie na útok zahltenia frekvencie falošnými beacon rámcami.

```
sniff(iface=interface,prn=beaconFloodDetection,timeout
   =0.3)
def beaconFloodDetection(frame):
    if frame.haslayer(Dot11Beacon):
        beaconscounter += 1
        if beaconscounter > 30:
            loggingLevels('BEACON FLOODING ATTACK
               DETECTION', 40)
            beaconscounter = 0
def beaconFloodDetection2(foundAP):
    regex = ';:,<>/\"#_\|{}[]()&‘~@$%^='
    ssid = foundAP[0]
    crypto = foundAP[1]
    if any((r in regex)for r in ssid and crypto == 'OPN':
        loggingLevels('BEACON FLOODING ATTACK DETECTION',
            40)
```

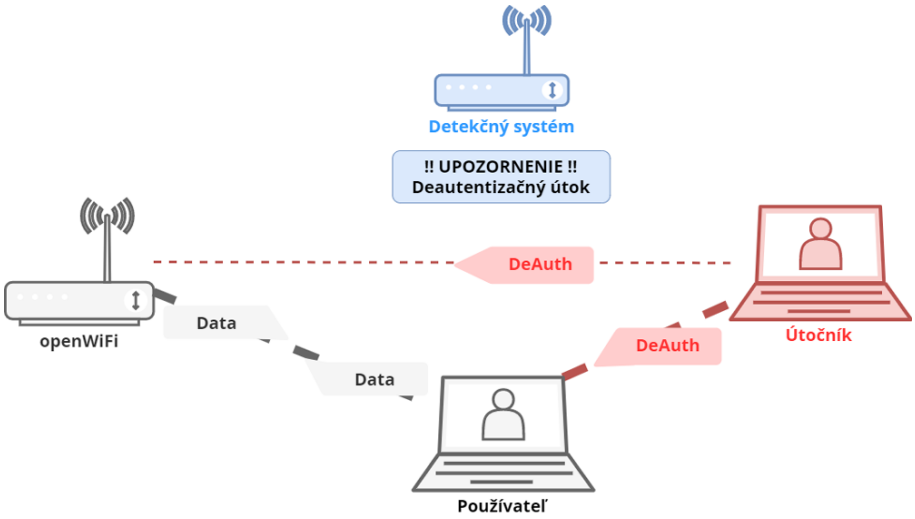
Výpis 3.3: Ukážka dvoch metód pseudo kódu na zachytenie beacon flood útoku.

4. Scenár deautentizačného útoku

1. Používateľ (Windows 10) bol pripojený k legitímnemu prístupovému bodu (Mikrotik) a vytváral sieťovú komunikáciu.
2. Rovnaké signatúry zachytil detekčný systém (Raspberry Pi), ktorý si vytvoril záznam a uložil ho do databázy.
3. Útočník (Kali Linux) pomocou monitorovacie módu karty zachytil signatúry prístupového bodu a nástrojom **aireplay-ng** následne spustil deautentizačný útok na všetkých pripojených používateľov.

```
sudo iwconfig wlan0mon channel 7
sudo aireplay-ng -0 0 -a C4:AD:34:03:24:DD
   wlan0mon
```

4. Detekčný modul systému (Raspberry Pi) zachytil **vysoké množstvo deautentizačných rámcov, ktoré boli vysielané z rovnakej fyzickej adresy v krátkom časovom úseku** a vyhlásil upozornenie na deautentizačný útok.



Obr. 3.18: Schéma štvrtého testovacieho scenára.

```
WARNING: DEAUTH ATTACK DETECTION! [c4:ad:34:03:24:dd]
WARNING: DEAUTH ATTACK DETECTION! [c4:ad:34:03:24:dd]: from: ff:ff:ff:ff:ff:ff reason: Class 3 Frame received
 from nonassociated STA
```

Obr. 3.19: Upozornenie na deautentizačný útok.

```
sniff(iface=interface,prn=deauth, timeout=1)
def deauth(frame):
    if frame.type == 0 and frame.subtype == 12:
        deauthcounter += 1
        if deauthcounter == 200:
            loggingLevels('DEAUTH ATTACK DETECTION',
               40)
```

Výpis 3.4: Ukážka pseudo kódu na detekciu deautentizačného útoku

Pri vývoji vlastnej implementácie detekčného systému **vznikli nasledovné problémy**, ktoré zabrali veľa času a úsilia na ich odstránenie:

- **Nestabilný ovládač pre integrovanú bezdrôtovú kartu na zariadení Raspberry Pi** – monitorovací mód karty je oficiálnymi ovládačmi blokovaný a v dôsledku toho bolo potrebné využiť nástroj **Nexmon**, ktorý ponúkal upravený ovládač pre niektoré podporované karty (obr. 3.5). Vzhľadom na vysokú nestabilitu ovládača, riešením bola nútená zmena operačného systému Raspbian na Kali Linux ARM, ktorý integruje iné upravené ovládače. Napriek tejto zmene bolo správanie integrovanej bezdrôtovej karty aj naďalej nezvyčajné, na čo nadväzuje ďalší problém.

- **Mód šetrenia energie na virtuálnom monitorovacom rozhraní** – pri zapínaní monitorovacieho módu nástrojom `airmon-ng` bolo vytvorené virtuálne rozhranie `wlan0mon`, ktoré v základnom nastavení malo predvolený mód šetrenia energie. Ten spôsoboval vypínanie virtuálneho rozhrania po nejakom čase, čím z neho urobil nepoužiteľné zariadenie na dlhšie monitorovanie a detekciu bezdrôtových sietí. Vhodným riešením sa ukázalo použitie externej bezdrôtovej karty, čo však spôsobuje nižšiu prenositeľnosť detektoru a vyššie prevádzkové náklady.
- **Pravidelnosť zmeny frekvencie monitorovacieho rozhrania** – na úplné pokrytie sieťovej komunikácie v okolí bolo nutné pravidelne meniť frekvenčný kanál na monitorovacom rozhraní nakoľko rozhranie dokázalo spracovať komunikáciu súbežne iba na jednom frekvenčnom pásme. Zmena pásma bola náhodná a častokrát nastala situácia, že rozhranie skákalo po niektorých frekvenciách častejšie ako po iných. Riešením by bola vhodná implementácia algoritmu, ktorý by rozlišoval viac a menej využívané frekvencie a následne by tomu prispôsobil zmenu frekvenčného pásma pre bezdrôtové rozhranie.

Výsledok vlastnej implementácie detekčného systému vznikol na základe vlastnej analýzy voľne dostupných detekčných systémov Suricata a Kismet. Jednotlivé moduly detekčného systému boli otestované na experimentálnom pracovisku, kde v 4 rôznych scenároch útokov dokázal detegovať útoky s využitím falošného prístupového bodu, čím bolo splnené zadanie praktickej časti práce.

Počas vlastnej realizácie vznikli ďalšie **návrhy na vylepšenie**, ktoré môžu byť v budúcnosti zapracované. Patria sem napríklad:

- Optimalizácia pre viaceré bezdrôtové karty.
- Komplexná konfigurácia detekcie všetkých vrstiev ISO/OSI modelu so systémom Suricata.
- Špecifikácia detekcie útokov a správa vlastných signatúr.
- Jednoduché grafické rozhranie.

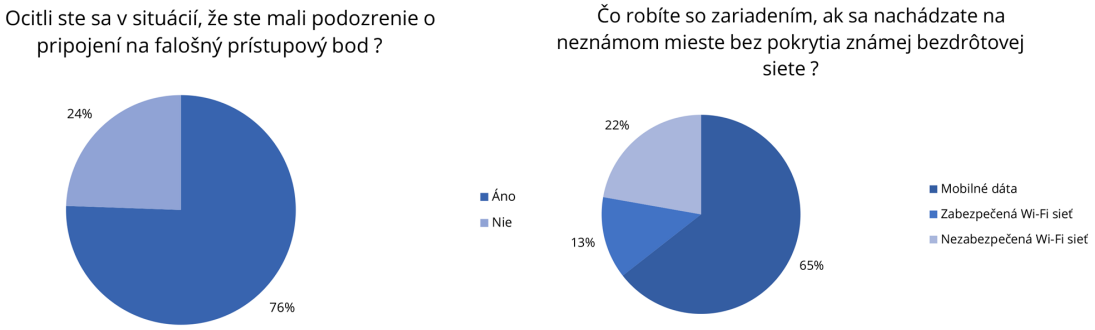
3.4 Analýza znalostí problematiky – Dotazník

Cieľom dotazníka bolo získanie všeobecného prehľadu a názorov nad porozumením problematiky falošných prístupových bodov z pohľadu bežných používateľov bezdrôtových sietí. V dotazníku odpovedalo **v časovom rozmedzí 2 mesiacov, 90 respondentov na 11 povinných a 1 doplňujúcu otázku**.

Zvolené otázky boli rozdelené do troch oblastí, ktoré obsahovali otvorené a zatvorené odpovede. Pre ich porozumenie postačovala základná znalosť technických termínov z oblasti bezdrôtových sietí.

Prvá oblasť otázok sa zamerala na používané zariadenia respondentov a ich zabezpečenie. Druhá časť zisťovala bežné správanie a návyky respondentov v určitých modelových situáciach. V poslednej časti mohli respondenti ohodnotiť svoje znalosti a zanechať svoj názor k otázke problematiky bezpečnosti pripojenia k bezdrôtovým sieťam.

Analýza získaných odpovedí a názorov poukázala na pomerne zaujímavé výsledky. Viac ako 58 % opýtaných respondentov ohodnotilo svoje znalosti z oblasti bezpečnosti pripájania do bezdrôtových sietí a komunikácie na sieti za vynikajúce (1) a veľmi dobré (2). Napriek tomu až 31 % opýtaných respondentov nemá nainštalovaný na svojom bezdrôtovom zariadení žiadny typ antivírusovej ochrany, 44 % ponecháva zapnuté bezdrôtové pripojenie, aj keď nie sú v dosahu známej bezdrôtovej sieti a 22 % vyhľadáva na neznámom mieste nezabezpečenú bezdrôtovú sieť.



Obr. 3.20: Grafické znázornenie odpovedí z dotazníku.

Každý opýtaný respondent sa pripája do známej bezdrôtovej siete s telefónom (100 %) a osobným počítačom (78 %), z toho 94 % automaticky bez ich potvrdenia. V čase vyplňovania dotazníku, ich bolo pripojených do bezdrôtovej siete 79 % opýtaných. Najčastejšie sa respondenti pripájajú do domácej bezdrôtovej siete (88 %), avšak pri pripojení k neoverenej sieti až 76 % z nich využíva dodatočné zabezpečenie. Potencionálnym rizikom je skutočnosť, že až 76 % z opýtaných respondentov nemalo nikdy podozrenie o ich pripojení k falošnému prístupovému bodu.

Analýzou odpovedí respondentov vyplýva fakt, že napriek dodržiavaniu bežných bezpečnostných pravidiel a postupov pri práci s bezdrôtovými sieťami, o samotnom nebezpečenstve vo forme falošných prístupových bodoch **respondenti nemajú dostatočné znalosti**. Celkové znenie dotazníka vrátane otázok, odpovedí a jeho grafického vyhodnotenia sa nachádza v priloženej prílohe C.

Záver

Cieľom bakalárskej práce zameranej na kybernetické útoky v bezdrôtových sieťach s využitím falošného prístupového bodu bola detailná analýza a spracovanie problematiky zahrňujúcej veľké množstvo informácií z oblasti informačnej bezpečnosti a sietí. Cieľom praktickej časti bakalárskej práce bolo vytvorenie a otestovanie vlastnej implementácie detekčného systému. Získané znalosti boli spracovávané a porovnávané spolu so získanými výsledkami z anonymného prieskumu medzi opýtanými respondentmi.

V teoretickej časti práce boli popísané typy kybernetických útokov v lokálnej sieti, ich detekcia pomocou detekčných systémov využívajúcich metódy signatúr a anomálií, bezdrôtové siete, funkcia bezdrôtového prístupového bodu v sieti, rozdelenie a spôsoby vytvorenia **falošného prístupového bodu**, a najznámejšie útoky s jeho využitím.

Praktická časť práce obsahovala vytvorenie a nastavenie experimentálneho pracoviska, ktoré simulovalo bežnú bezdrôtovú sieť. Na experimentálnom pracovisku boli otestované dva voľne dostupné detekčné systémy **Suricata a Kismet**. Zhrnutím výsledkov sa ako čiastočne vhodným riešením ukázal detekčný systém Kismet, ktorý dokázal spracovať zachytávané rámce aj na spojovej vrstve.

Vzhľadom na vyžadovanú pokročilú implementáciu metód detekcie kybernetických útokov s použitím falošného prístupového bodu bola **navrhnutá a vytvorená vlastná implementácia** detekčného systému v programovacom jazyku Python. Systém dokázal zachytávať signatúry jednotlivých rámcov na spojovej vrstve, ktoré boli ďalej spracované a analyzované. Implementované moduly detekčného systému vyhodnocovali nebezpečenstvo kybernetických útokov na základe získaných informácií. V rámci testovania vlastnej implementácie boli vytvorené **4 scenáre kybernetických útokov, ktoré detekčný systém dokázal detegovať** a upozorniť používateľa.

Vlastným prínosom práce bolo aj vytvorenie dotazníku na analýzu znalostí problematiky falošného prístupového bodu medzi odbornou verejnosťou. Dotazník obsahoval 12 otázok na ktoré odpovedalo 90 respondentov. Konkrétne otázky a odpovede dotazníku sú v prílohe C. Posledným vlastným prínosom práce bolo vytvorenie príspevku s názvom *Detection of Fake Access Points* na konferenciu študentských prác EEICT. Všetky stanovené ciele bakalárskej práce boli týmto splnené.

Literatúra

[1] CIMPANU, Catalin. *The scariest hacks and vulnerabilities of 2019.* In: *ZDNet* [online]. 28. 10. 2019 [cit. 8. 12. 2019]. Dostupné z URL: <https://www.zdnet.com/article/the-scariest-hacks-and-vulnerabilities-of-2019/>.

[2] DVORSKÝ, Radovan. *DETEKCE ÚTOKŮ NA WIFI SÍTĚ POMOCÍ ZÍSKÁVANÍ ZNALOSTÍ* [online]. Brno, 2014 [cit. 19. 11. 2019]. Dostupné z URL: <https://www.vutbr.cz/www_base/zav_prace_soubor_verejne.php?file_id=119310>

[3] HRÁČEK, Jiří. *Perspektivy zabezpečení bezdrátových komunikačních sítí* [online]. Brno, 2008 [cit. 8. 12. 2019]. Dostupné z URL: <https://www.vutbr.cz/www_base/zav_prace_soubor_verejne.php?file_id=6271>

[4] HUSÁR, Michal. *Analýza a demonstrace vybraných bezdrátových útoků pod OS Windows* [online]. Brno, 2012 [cit. 8. 12. 2019]. Dostupné z URL: <https://www.vutbr.cz/www_base/zav_prace_soubor_verejne.php?file_id=118258>

[5] OREBAUGH, Angela. *Ethereal: packet sniffing* [online]. Rockland: Syngress, 2004, 1-38 s. [cit. 25. 5. 2020]. ISBN 978-1-932266-82-5. Dostupné z URL: <https://www.sciencedirect.com/book/9781932266825/ethereal-packet-sniffing>

[6] CHAN AUNG, May Aye a Khin Phyo THANT. *Detection and mitigation of wireless link layer attacks.* In: 2017 IEEE 15th International Conference on Software Engineering Research, Management and Applications (SERA) [online]. London, UK: IEEE, 2017, s. 173-178 [cit. 25. 5. 2020]. DOI: 10.1109/SERA.2017.7965725. ISBN 978-1-5090-5756-6. Dostupné z URL: <https://ieeexplore.ieee.org/document/7965725/>

[7] BENZAÏD, Chafika, Abderrahman BOULGHERAIF, Fatma Zohra DAHMANE, Ameer AL-NEMRAT a Khaled ZERAOULIA. *Intelligent detection of MAC spoofing attack in 802.11 network.* In: Proceedings of the 17th International Conference on Distributed Computing and Networking - ICDCN '16 [online]. New York, USA: ACM Press, 2016, s. 1-5 [cit. 25. 5. 2020]. DOI: 10.1145/2833312.2850446. ISBN 9781450340328. Dostupné z URL: <https://dl.acm.org/doi/pdf/10.1145/2833312.2850446>

[8] XU, Yi a Wenye WANG. *Detecting and Mitigating DoS Attacks in Wireless Networks without Affecting the Normal Behaving Nodes.* In: MILCOM 2007 -

IEEE Military Communications Conference [online]. Orlando, FL, USA: IEEE, 2007, s. 1-7 [cit. 25. 5. 2020]. DOI: 10.1109/MILCOM.2007.4454838. ISBN 978-1-4244-1512-0. Dostupné z URL: <http://ieeexplore.ieee.org/document/4454838/>

[9] JACKO, Michal. *Metody klasifikace síťového provozu* [online]. Brno, 2017 [cit. 8. 12. 2019]. Dostupné z URL: <https://www.vutbr.cz/www_base/zav_prace_soubor_verejne.php?file_id=158967>

[10] POLJAK, Peter. *IDS pro WiFi sítě* [online]. Brno, 2013 [cit. 8. 12. 2019]. Dostupné z URL: <https://is.muni.cz/th/qhqx2/praca.pdf>

[11] BOUKHTOUTA, Amine, Serguei A. MOKHOV, Nour-Eddine LAKHDARI, Mourad DEBBABI a Joey PAQUET. *Network malware classification comparison using DPI and flow packet headers.* In: Journal of Computer Virology and Hacking Techniques [online]. 2016, 12(2), s. 69-100 [cit. 8. 12. 2019]. DOI: 10.1007/s11416-015-0247-x. ISSN 2263-8733. Dostupné z URL: <http://link.springer.com/10.1007/s11416-015-0247-x>

[12] KARATAS, Gozde a Ozgur Koray SAHINGOZ. *Neural network based intrusion detection systems with different training functions.* 2018 6th International Symposium on Digital Forensic and Security (ISDFS) [online]. IEEE, 2018, 1-6 [cit. 8. 12. 2019]. DOI: 10.1109/ISDFS.2018.8355327. ISBN 978-1-5386-3449-3. Dostupné z URL: <https://ieeexplore.ieee.org/document/8355327/>

[13] JYOTHSNA, Veeramreddy a Koneti MUNIVARA PRASAD. *Anomaly-Based Intrusion Detection System.* Computer and Network Security [online]. IntechOpen, 2019, 11. 6. 2019 [cit. 8. 12. 2019]. DOI: 10.5772/intechopen.82287. Dostupné z URL: <https://www.intechopen.com/online-first/anomaly-based-intrusion-detection-system>

[14] *Next-Generation Intrusion Prevention System (NGIPS). Cisco* [online]. 2019 [cit. 8. 12. 2019]. Dostupné z URL: <https://www.cisco.com/c/en/us/products/security/ngips/index.html>

[15] *IPS as part of a Platform.* In: Palo Alto Networks [online]. 2018, 14. 12. 2018 [cit. 8. 12. 2019]. Dostupné z URL: <https://www.paloaltonetworks.com/resources/whitepapers/ips-as-platform>

[16] *Bitdefender BOX* [online]. 2019 [cit. 8. 12. 2019]. Dostupné z URL: <https://www.bitdefender.com/box/v2>

[17] *DefensePro DDoS Defense & DDoS Prevention Device. Radware* [online]. 2019 [cit. 8. 12. 2019]. Dostupné z URL: <https://www.radware.com/products/defensepro/>

[18] *F-Secure SENSE.* [online]. 2019 [cit. 8. 12. 2019]. Dostupné z URL: <https://www.f-secure.com/en/web/home_global/sense/technology>

[19] *NORTON CORE* [online]. 2019 [cit. 8. 12. 2019]. Dostupné z URL: <https://us.norton.com/core-secure-router-features>

[20] SCHREIBER J., LANGSTON R. *Open Source IDS Tools: Comparing Suricata, Snort, Bro (Zeek), Linux* [online]. 26. 11. 2018 [cit. 8. 12. 2019]. Dostupné z URL: <https://cybersecurity.att.com/blogs/security-essentials/open-source-intrusion-detection-tools-a-quick-overview>

[21] *Suricata* [online]. 2019 [cit. 8. 12. 2019]. Dostupné z URL: <https://suricata-ids.org/>

[22] THEJDEEP. G, SHIVA SAGAR. B, SIDDARTHA. L. K a B. R. CHANDAVARKAR. *Detecting Rogue Access Points using Kismet.* 2015 International Conference on Communications and Signal Processing (ICCSP) [online]. IEEE, 2015, 0172-0175 [cit. 8. 12. 2019]. DOI: 10.1109/ICCSP.2015.7322813. ISBN 978-1-4799-8081-9. Dostupné z URL: <http://ieeexplore.ieee.org/document/7322813/>

[23] *Kismet* [online]. 2019 [cit. 8. 12. 2019]. Dostupné z URL: <https://www.kismetwireless.net/>

[24] KERSHAW, Mike. *Kismet Package Description.* KALI TOOLS [online]. 18. 2. 2014 [cit. 8. 12. 2019]. Dostupné z URL: <https://tools.kali.org/wireless-attacks/kismet>

[25] SOMMER, Robin. Bro: *An Open Source Network Intrusion Detection System* [online]. Berlin, 2003 [cit. 8. 12. 2019]. Dostupné z URL: <https://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.60.5410> TU Mníchov.

[26] SOMMER, Robin. *Zeek 3.0.0.* Zeek.org [online]. 23. 9. 2019 [cit. 8. 12. 2019]. Dostupné z URL: <https://blog.zeek.org/2019/09/zeek-300.html>

[27] *Snort* [online]. 2019 [cit. 8. 12. 2019]. Dostupné z URL: <https://www.snort.org/>

[28] *Understanding and Configuring Snort Rules.* RAPID7 Blog [online]. 9. 12. 2016 [cit. 8. 12. 2019]. Dostupné z URL: <https://blog.rapid7.com/2016/12/09/understanding-and-configuring-snort-rules/>

[29] IEEE *IEEE 802.11 WIRELESS LOCAL AREA NETWORKS: The Working Group for WLAN Standards* [online]. 2019 [cit. 19. 11. 2019]. Dostupné z URL: <http://www.ieee802.org/11/>

[30] JUNIPER NETWORKS. *Understanding the Network Terms SSID,BSSID and ESSID* [online]. 12.2.2015 [cit. 19. 11. 2019]. Dostupné z URL: <https://www.juniper.net/documentation/en_US/junos-space-apps/network-director2.0/topics/concept/wireless-ssid-bssid-essid.html>

[31] IEEE *802.11-2016 – Standard for Information technology—Telecommunications and information exchange between systems Local and metropolitan area networks—Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications.* In: IEEE [online]. 2016, s. 1-3534 [cit. 25. 5. 2020]. DOI: 10.1109/IEEESTD.2016.7786995. ISBN 978-1-5044-3645-8. Dostupné z URL: <https://ieeexplore.ieee.org/document/7786995/>

[32] GAST, Matthew. *802.11 Wireless Networks: The Definitive Guide* [online]. 2nd edition. O'Reilly Media, 2005, s. 654 [cit. 25. 5. 2020]. ISBN 978-0-596-10052-0. Dostupné z URL: <https://www.oreilly.com/library/view/80211-wireless-networks/0596100523/>

[33] LAKSHMANAN, Saravanan. *802.11 Association Status, 802.11 Deauth Reason codes.* Cisco Community [online]. 29.8.2017 [cit. 25. 5. 2020]. Dostupné z URL: <https://community.cisco.com/t5/wireless-mobility-documents/802-11-association-status-802-11-deauth-reason-codes/ta-p/3148055>

[34] IEEE *802.11w-2009 – IEEE Standard for Information technology - Telecommunications and information exchange between systems - Local and metropolitan area networks - Specific requirements. Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 4: Protected Management Frames* In: IEEE [online]. 2009, s. 1-111 [cit. 25. 5. 2020]. DOI: 10.1109/IEEESTD.2009.5278657. ISBN 978-0-7381-6048-1. Dostupné z URL: <Dostupnéz:https://ieeexplore.ieee.org/document/5278657>

[35] PLCH, Matej. *Practical man-in-the-middle attacks in computer networks* [online]. Brno, 2015 [cit. 8. 12. 2019]. Dostupné z URL: <https://is.muni.cz/th/s8uf2/thesis.pdf>

[36] *WIFI PINEAPPLE* [online]. Hak5, 2019 [cit. 8. 12. 2019]. Dostupné z URL: <https://shop.hak5.org/products/wifi-pineapple>

[37] SMITH, Brian a George CHATZISOFRONIOU. *Wifiphisher: rogue Access Point framework* [online]. 2020 [cit. 25. 5. 2020]. Dostupné z URL: <https://github.com/wifiphisher/wifiphisher>

[38] WANG, Le. *Detection of Man-in-the-middle Attacks Using Physical Layer Wireless Security Techniques* [online]. Worcester, USA, 2013 [cit. 8. 12. 2019]. Dostupné z URL: <https://web.wpi.edu/Pubs/ETD/Available/etd-082713-125108/unrestricted/thesis.pdf>

[39] HALIL SARUHAN, Ibrahim. *Detecting and Preventing Rogue Devices on the Network* [online]. Online: SANS Institute, 8. 8. 2007 [cit. 8. 12. 2019].Dostupné z URL: <https://www.sans.org/reading-room/whitepapers/detection/detecting-preventing-rogue-devices-network-1866>

[40] Bahl, P., Chandra, R., Padhye, J., Ravindranath, L., Singh, M., Wolman, A., Zill, B. *Enhancing the security of corporate Wi-Fi networks using DAIR* [online]. MobiSys 2006 - Fourth International Conference on Mobile Systems, Applications and Services, 2006 [cit. 8. 12. 2019]. Dostupné z URL: <https://dl.acm.org/citation.cfm?doid=1134680.1134682>

[41] JADHAV, Swati, S.B. VANJALE a P.B. MANE. *Illegal Access Point detection using clock skews method in wireless LAN.* In: 2014 International Conference on Computing for Sustainable Global Development (INDIACom) [online]. IEEE, 2014, 2014, s. 724-729 [cit. 8. 12. 2019]. DOI: 10.1109/IndiaCom.2014.6828057. ISBN 978-93-80544-12-0. Dostupné z URL: <http://ieeexplore.ieee.org/document/6828057/>

[42] KAO, Kuo Fong, Wen Ching CHEN, Jui Chi CHANG a Heng Te CHU. *An Accurate Fake Access Point Detection Method Based on Deviation of Beacon Time Interval.* In: 2014 IEEE Eighth International Conference on Software Security and Reliability-Companion [online] IEEE, 2014, 2014, s. 1-2 [cit. 8. 12. 2019]. DOI: 10.1109/SERE-C.2014.13. ISBN 978-1-4799-5843-6. Dostupné z URL: <https://ieeexplore.ieee.org/document/6901631>

[43] HAN, Hao, Bo SHENG, Chiu C. TAN, Qun LI a Sanglu LU. *A Timing-Based Scheme for Rogue AP Detection.* In: IEEE Transactions on Parallel

and Distributed Systems [online]. 2011, 22(11), s. 1912-1925 [cit. 8. 12. 2019]. DOI: 10.1109/TPDS.2011.125. ISSN 1045-9219. Dostupné z URL: <http://ieeexplore.ieee.org/document/6007016/>

[44] SONG, Yimin, Chao YANG a Guofei GU. *Who is peeping at your passwords at Starbucks? — To catch an evil twin access point* [online]. In: IEEE, 2010, 2010, s. 323-332 [cit. 8. 12. 2019]. DOI: 10.1109/DSN.2010.5544302. ISBN 978-1-4244-7500-1. Dostupné z URL: <http://ieeexplore.ieee.org/document/5544302/>

[45] MÓNICA, Diogo a Carlos RIBEIRO. *WiFiHop - Mitigating the Evil Twin Attack through Multi-hop Detection.* Computer Security – ESORICS 2011 [online]. Berlin, Heidelberg: Springer Berlin Heidelberg, 2011, 2011, , 21-39 [cit. 8. 12. 2019]. Lecture Notes in Computer Science. DOI: 10.1007/978−3−642−23822−2_2. ISBN 978-3-642-23821-5. Dostupné z URL: <http://link.springer.com/10.1007/978-3-642-23822-2_2>

[46] DORMANN, Will. *Instant KARMA Might Still Get You.* In: Carnegie Mellon University [online] 2015, 11. 4. 2015 [cit. 8. 12. 2019]. Dostupné z URL: <https://insights.sei.cmu.edu/cert/2015/08/instant-karma-might-still-get-you.html>

[47] HAITHAM AMEEN, Noman, Abdullah SHAHIDAN M. a Mohammed HAYDAR IMAD. *An Automated Approach to Detect Deauthentication and Disassociation Dos Attacks on Wireless 802.11 Networks.* In: IJCSI International Journal of Computer Science Issues [online]. IJCSI, 2015, 4. 7. 2015, s. 107-112 [cit. 8. 12. 2019]. ISSN 1694-0784. Dostupné z URL: <https://pdfs.semanticscholar.org/e41e/8f773e44232fb6ff3e4c827282b5cd50a735.pdf>

[48] MOHIT, Raj. *The Deauthentication Attack.* In: Medium [online]. 25.10.2018 [cit. 8. 12. 2019]. Dostupné z URL: <https://medium.com/@Packt_Pub/the-deauthentication-attack-7872c916ed2a>

[49] FENG, Zhutian a Cunqing HUA. *Machine Learning-based RF Jamming Detection in Wireless Networks.* 2018 Third International Conference on Security of Smart Cities, Industrial Control System and Communications (SSIC) [online]. IEEE, 2018, 1-6 [cit. 8. 12. 2019]. DOI: 10.1109/SSIC.2018.8556709. ISBN 978-1-5386-8187-9. Dostupné z URL: <https://ieeexplore.ieee.org/document/8556709/>

[50] *Aircrack-ng* [online]. 2019 [cit. 8. 12. 2019]. Dostupné z URL: <https://www.aircrack-ng.org/>

[51] *Manual:Winbox.* MikroTik Documentation [online]. 2. 10. 2019 [cit. 8. 12. 2019]. Dostupné z URL: <https://wiki.mikrotik.com/wiki/Manual:Winbox>

[52] SCHULZ, Matthias, Daniel WEGEMER a Matthias HOLLICK. *Nexmon: The C-based Firmware Patching Framework.* GitHub [online]. 2017 [cit. 8. 12. 2019]. Dostupné z URL: <https://nexmon.org>

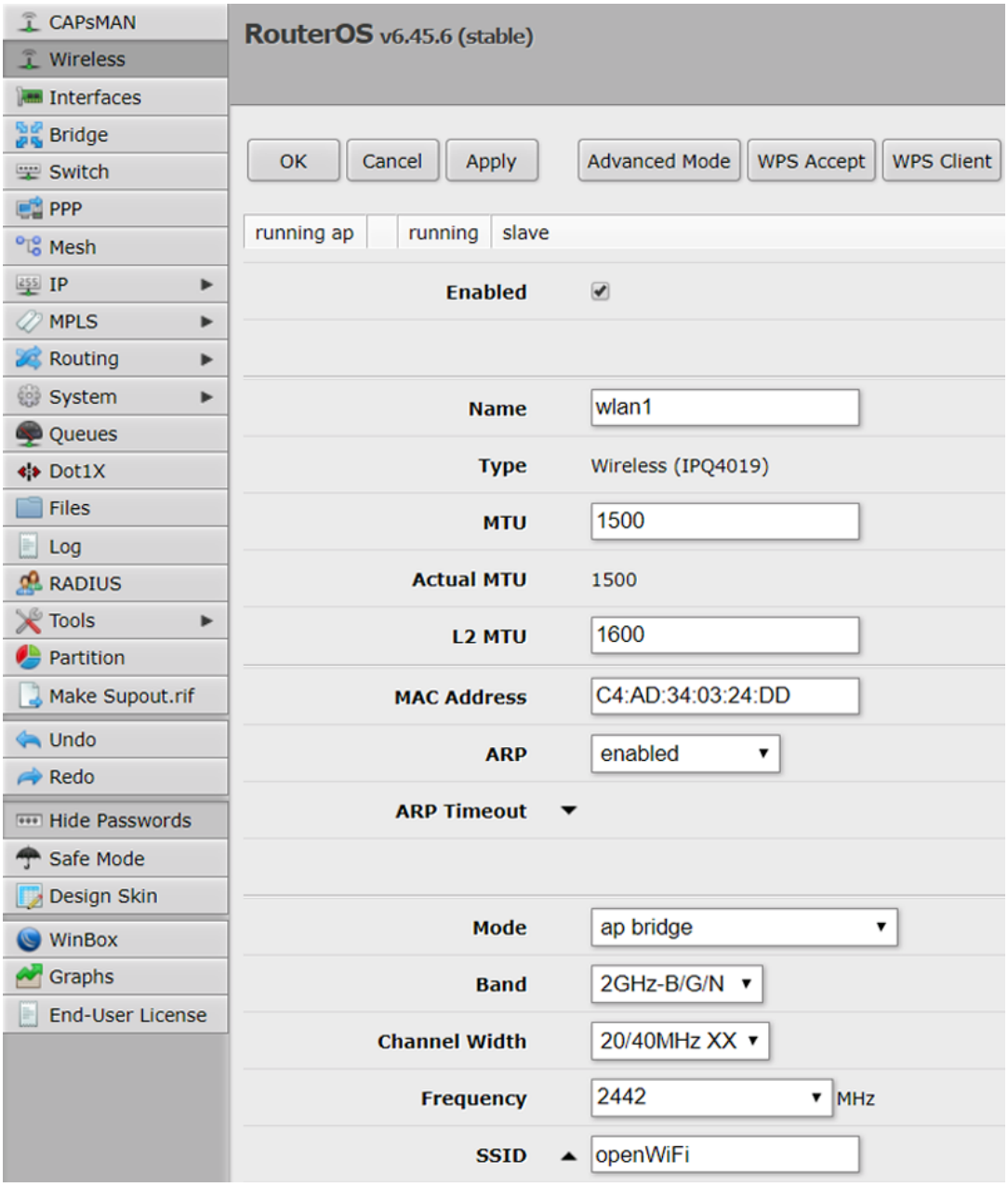
Zoznam príloh

A Experimentálne pracovisko

A.1 Návod na spustenie pracoviska

1. Zapojenie a nastavenie legitímneho prístupového bodu cez WinBox.
2. Pripojenie používateľa k legitímnemu prístupovému bodu.
3. Vytvorenie virtualizovaného prostredia Kali Linux a pripojenie externej bezdrôtovej karty.
4. Inštalácia Kali Linux ARM na zariadenie Raspberry Pi, zapnutie monitorovacieho módu na integrovanej karte a spustenie detektoru cez príkazový riadok.

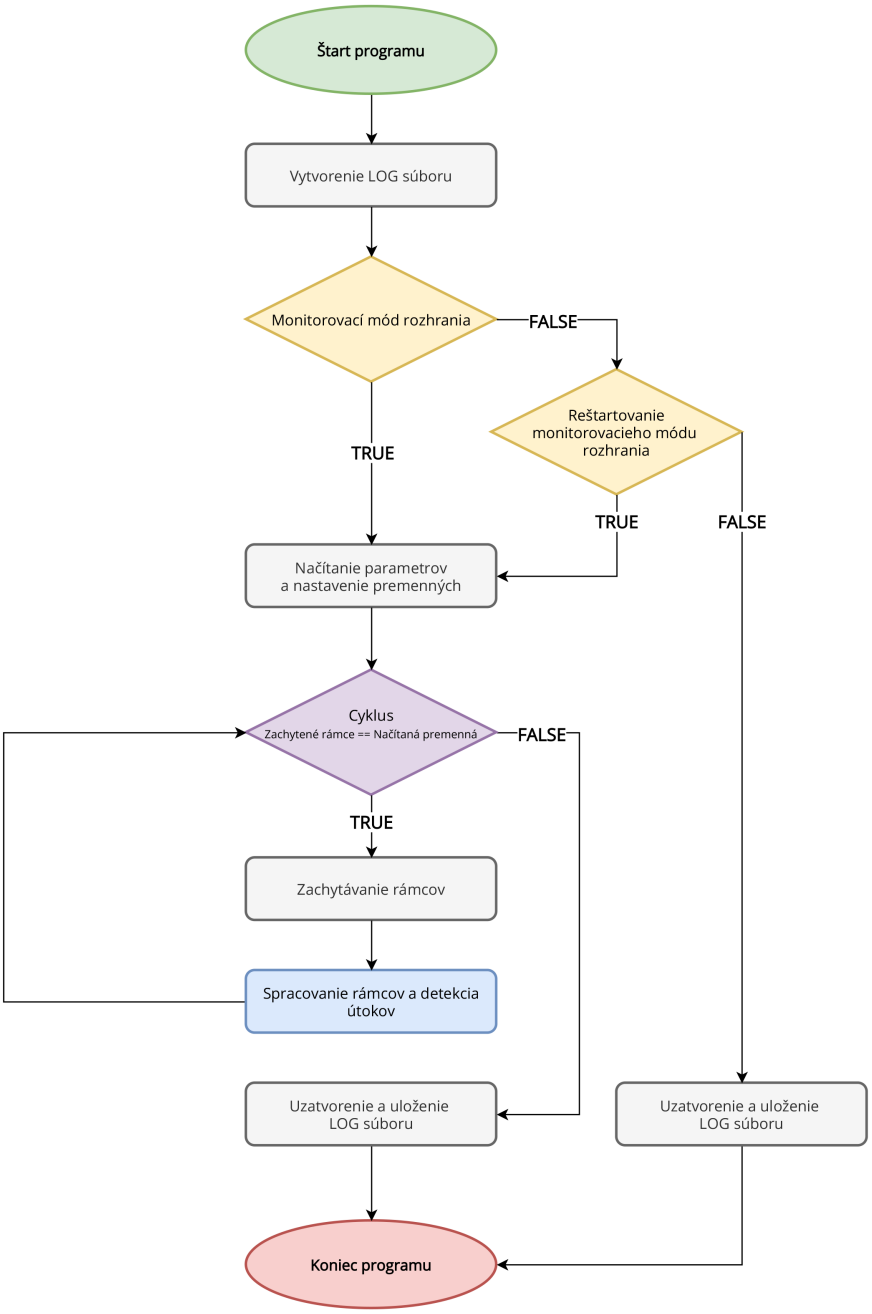
A.2 Rozšírené nastavenie prístupového bodu



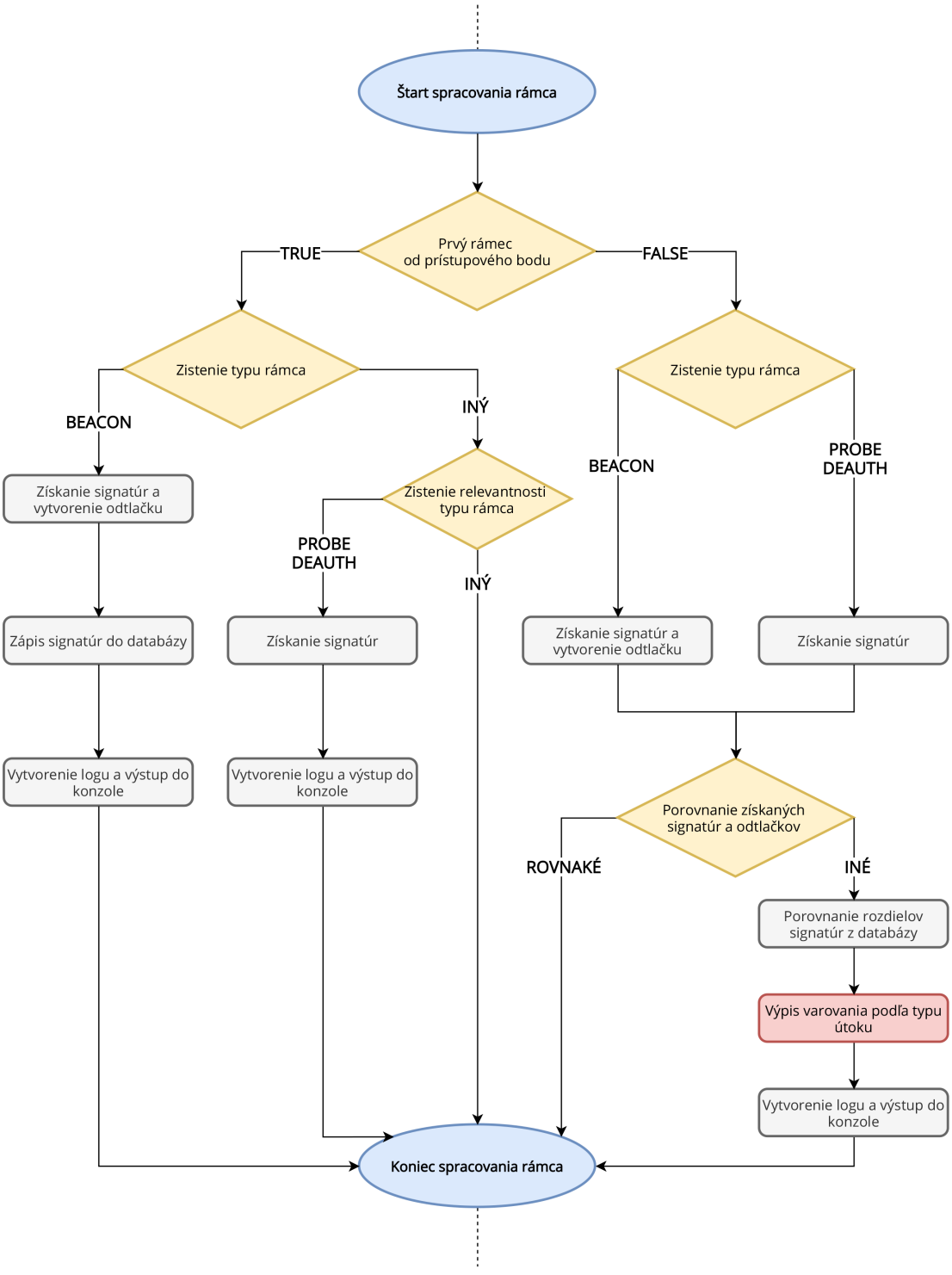
Obr. A.1: Rozšírené nastavenie prístupového bodu Mikrotik.

B Vlastná implementácia

B.1 Diagramy modulov vlastnej implementácie



Obr. B.1: Celkový diagram vlastnej implementácie detekčného systému.



Obr. B.2: Diagram modulu spracovania a analýzy zachyteného rámcu.

B.2 Návod na spustenie vlastnej implementácie

1. Spustenie Raspberry Pi a prihlásenie sa do systému Kali Linux ARM.
2. Vytvorenie virtuálneho monitorovacieho rozhrania v príkazovom riadku cez nástroj `airmon-ng`.
3. Prepnutie sa príkazovým riadkom do priečinku `/home/kali/PycharmProjects/bp_wids_final/`.
4. Spustenie detekcie `wids.py` s parametrami `-i wlan0mon -m False` (pre základný mód) alebo `-m True` (pre plný mód – spomaľuje výpis a celkovú detekciu útokov).
5. Ukončenie programu klávesovou skratkou `Control+C`.
6. Zobrazenie výsledného log súboru v priečinku `/log` v adresári projektu.

B.3 Zdrojový kód vlastnej implementácie

Modul na správy bezdrôtového rozhrania

```
def checkingMonitorMod():
    found = False
    monitor_interface = ''
    for i in netifaces.interfaces():
        if 'mon' in i:
            found = True
            monitor_interface = str(i)
        if i == 'wlan0' and 'wlan0mon' not in netifaces.
           interfaces():
            restartMonitorMod('wlan0')
            found = True
            monitor_interface = 'wlan0mon'
            break
        if 'mon' not in i:
            found = False
    return found
```

Modul na správu a výpis logov s rôznymi stupňami upozornení

```
def creatingLog():
    LOG_FILE = ('log/wids.log')
    logging.basicConfig(format='[%(asctime)s] - %(
       levelname)s - %(message)s',filename="LOG_FILE",
       filemode='w',level=logging.DEBUG, datafmt='%d.%m.%
       Y %H:%M:%S')

def loggingLevels(msg,lvl):
    if lvl == 10:
        logging.DEBUG(str(msg))
        print('DEBUG: '+str(msg))
    elif lvl == 20:
        logging.INFO(str(msg))
        print('INFO: '+str(msg))
    else:
        print('Incorrect value '+lvl)
```

Modul na správu argumentov a globálnych hodnôt

```
def arguments():
    parser = argparse.ArgumentParser(description='
       Arguments')
    parser.add_argument('--interface','-i',help='select
       interface')
    parser.add_argument('--fullmode','-m',help='fullmode'
       )
    args = parser.parse_args()

    if args.interface:
        interface = args.interface
    if args.fullmode:
        fullmode = True
```

Modul na zachytenie signatúr a vytvorenie odtlačku

```
def signaturesAP(frame):
    bssid = frame.addr2
    ssid = frame.info
    channel = str((frame[Dot11Beacon].network_stats()).
       get('channel')
    crypto = str((frame[Dot11Beacon].network_stats()).get
       ('crypto')[2:-2]
    rates = str(frame[Dot11Beacon].rates)
    county = str(frame[Dot11EltCountry].county_string)
       [2:-2]

def fingerprintAP(ssid,rates,country,crypto):
    try:
        values = ssid+rates+country+crypto
        fingerprint = hashlib.sha3_256(values.encode('utf
           -8').hexdigest())
        return fingerprint
    except ValueError:
        print('Empty values')
```

Modul na detekciu falošného prístupového bodu

```
def analystAP(AP):
    if AP.keys()
        if not database_AP:
            database_AP[AP.key] = AP.values
            loggingLevels('AP found', 20)
        else:
            if not AP.key in database_AP.keys():
                database_AP[AP.key] = AP.values
                loggingLevels('AP found', 20)
            else:
                if database_AP.values[4] != AP.values[4]:
                    loggingLevels('ROGUE AP DETECTION',
                       40)
```

Modul na detekciu KARMA útoku

```
sniff(iface=interface,prn=karmaDetection, timeout=2)

def karmaDetection(frame):
    if frame.haslayer(Dot11ProbeResp):
        bssidAP = frame.addr2
        ssidAP = frame.info.decode('utf-8')
        if bssidAP in databse_KARMA_AP.keys() and ssidAP
           in databse_KARMA_AP.values():
            loggingLevels('KARMA ATTACK DETECTION', 40)
```

Modul na detekciu záplavy falošných beacon rámcov

```
sniff(iface=interface,prn=beaconFloodDetection, timeout
   =0.3)

def beaconFloodDetection(frame):
    if frame.haslayer(Dot11Beacon):
        beaconscounter += 1
        if beaconscounter > 30:
            loggingLevels('BEACON FLOODING ATTACK
               DETECTION', 40)
            beaconscounter = 0

def beaconFloodDetection2(foundAP):
    regex = ';:,<>/\"#_\|{}[]()&`~@$%^='
    ssid = foundAP[0]
    crypto = foundAP[1]
    if any((r in regex)for r in ssid and crypto == 'OPN':
        loggingLevels('BEACON FLOODING ATTACK DETECTION',
            40)
```

Modul na detekciu deautentizačného útoku

```
sniff(iface=interface,prn=deauthAttackDetection, timeout
   =1)

def deauthAttackDetection(frame):
    if frame.type == 0 and frame.subtype == 12:
        deauthcounter += 1
        if deauthcounter == 200:
            loggingLevels('DEAUTH ATTACK DETECTION', 40)
```

C Analýza problematiky – Dotazník

C.1 Zoznam otázok a odpovedí dotazníku

1. Využívate pripojenie do bezdrôtových sietí ?
   Áno (90), Nie (0)
2. V akom prostredí sa najčastejšie pripájate do bezdrôtovej siete ?
   Doma (Privátna sieť) (79), Škola (Verejná sieť) (7), Práca (Organizácia) (4)
3. S akými zariadeniami sa pravidelne pripájate do bezdrôtovej siete ?
   Viac možných odpovedí: Telefón (90), Tablet (20), Osobný počítač (70), Herná konzola (10), Televízor (21), Iné (1)
4. Máte nainštalovaný anti-vírusový program na zariadení, s ktorým sa pripájate do bezdrôtovej siete ?
   Áno, mám neplatený (free) program (34), Áno, mám platený (paid) program (28), Nie, nemám žiadny program (27), Neviem (1)
5. Pripojí sa Vaše zariadenie automaticky ku bezdrôtovej sieti, ktorú pozná/má uloženú ?
   Áno, pripojí sa automaticky (85), Nie, pripájam ho vždy manuálne (5)
6. Čo robíte so zariadením, ak ste sa vzdialili od miesta s pokrytím známej bezdrôtovej siete ?
   Ručne vypnem bezdrôtové pripojenie na zariadení (50), Nechám zapnuté bezdrôtové pripojenie na zariadení (38), Iné (2)
7. Čo robíte so zariadením, ak sa nachádzate na neznámom mieste bez pokrytia známej bezdrôtovej siete ? *(Dovolenka, verejné priestranstvá, letiská, nemocnice a iné.)*
   Prepnem zariadenie na mobilné dáta / mobilný hotspot (aj za vyšší poplatok) (55), Vyhľadávam a pripájam sa iba na zabezpečené bezdrôtové siete (aj za poplatok) (12), Vždy vyhľadávam a pripájam sa na nezabezpečené (free) bezdrôtové siete (20), Iné (3)
8. Ak ste pripojený na neoverenú bezdrôtovú sieť, využívate dodatočné zabezpečenie pripojenia ? (VPN, SSL, HTTPS)
   Áno (68), Nie (22)
9. Ocitli ste sa v situácií, že ste mali podozrenie o pripojení na falošný prístupový bod ? *(divné správanie napr. časté presmerovania, nižšia prenosová rýchlosť, formulár na zadanie platobných údajov za účelom pripojenia a pod.)*
   Áno(22), Nie (68)
10. Ste práve pripojený na bezdrôtovú sieť ?

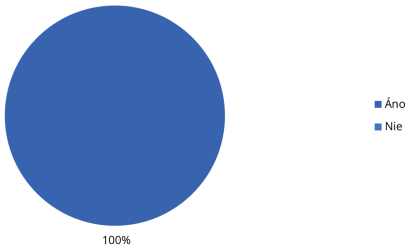
Áno (71), Nie (19)

11. Ako by ste ohodnotili Vaše znalosti v problematike bezpečnosti na sieti ? *(Bezpečné pripojenie do siete, bezpečné používanie zariadení (telefón,počítač..), znalosť štandardov bezdrôtových sietí a ich nastavenie na zariadeniach (napr. domáci Wi-Fi router)*

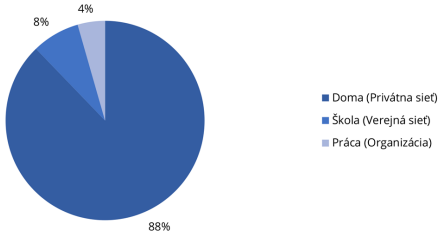
    1 (20), 2 (33), 3 (17), 4 (10), 5 (10)

C.2 Grafické vyhodnotenie odpovedí dotazníku

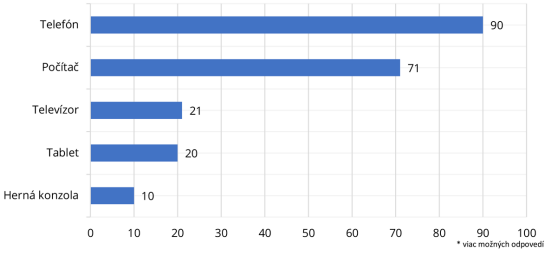
1. Využívate pripojenie do bezdrôtových sietí ?



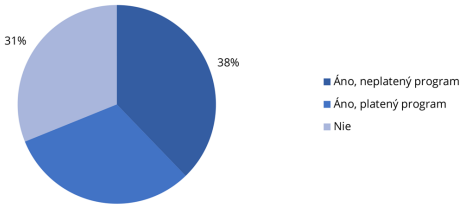
2. V akom prostredí sa najčastejšie pripájate do bezdrôtovej siete ?



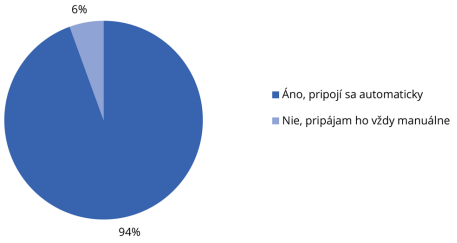
3. S akými zariadeniami sa pravidelne pripájate do bezdrôtovej siete* ?



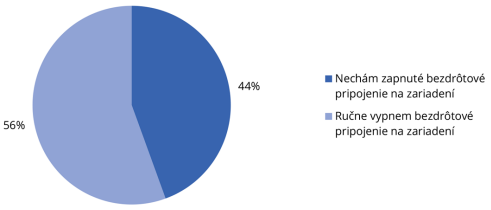
4. Máte nainštalovaný anti-vírusový program na zariadení, s ktorým sa pripájate do bezdrôtovej siete ?



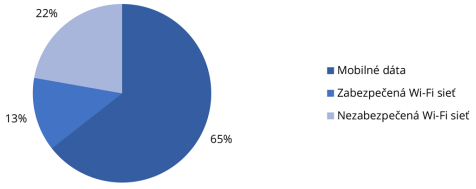
5. Pripojí sa Vaše zariadenie automaticky ku bezdrôtovej sieti, ktorú pozná/má uloženú ?



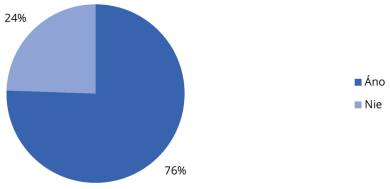
6. Čo robíte so zariadením, ak ste sa vzdialili od miesta s pokrytím známej bezdrôtovej siete ?



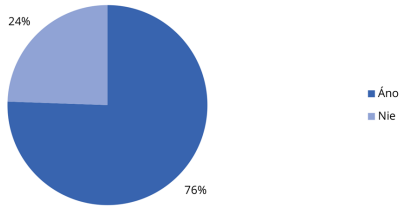
7. Čo robíte so zariadením, ak sa nachádzate na neznámom mieste bez pokrytia známej bezdrôtovej siete ?



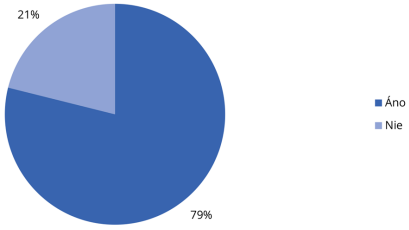
8. Ak ste pripojený na neoverenú bezdrôtovú sieť, využívate dodatočné zabezpečenie pripojenia ? (VPN, SSL, HTTPS)

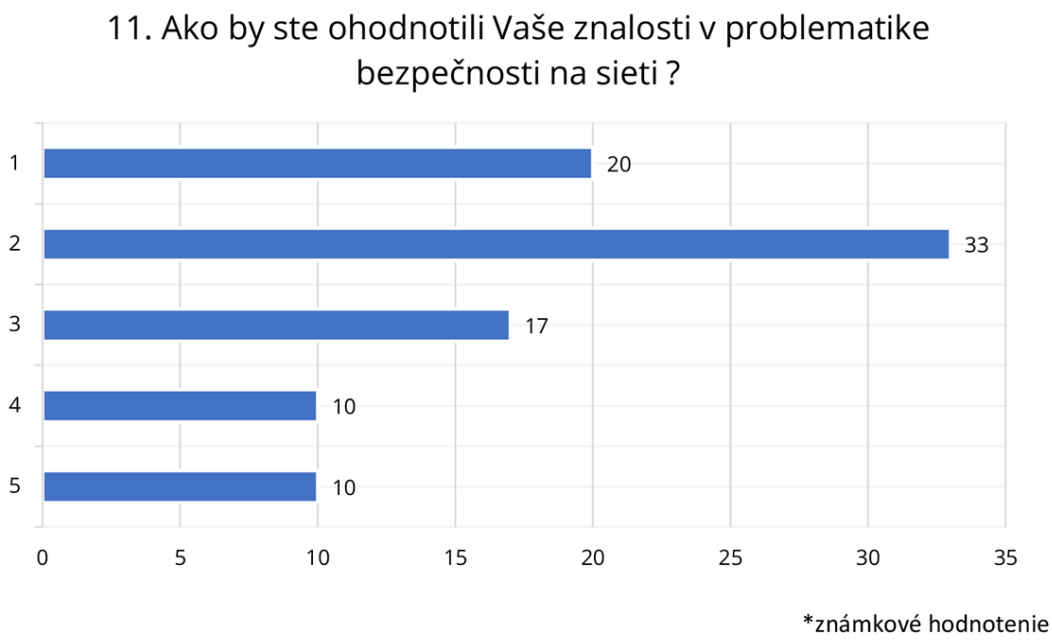


9. Ocitli ste sa v situácií, že ste mali podozrenie o pripojení na falošný prístupový bod ?



10. Ste práve pripojený na bezdrôtovú sieť ?




11. Ako by ste ohodnotili Vaše znalosti v problematike bezpečnosti na sieti ?
1
2
3
4
5
20
33
17
10
10
0
5
10
15
20
25
30
35
*známkové hodnotenie

D Obsah priloženého nosiča

- `OS` ..... exportované operačné systémy
  - `utocnik-kali-linux-2020.ova`
  - `detektor-kali-linux-sdcardimage.zip`
  - `attacks.txt`
- `skript` ..... skript detekčného systému
  - `xlovin00_bp_wids.zip`
- `video` ..... video detekcie kybernetických útokov
  - `attack_scheme_beacon_flood_easymode_detection.mp4`
  - `attack_scheme_beacon_flood_fullmode_detection.mp4`
  - `attack_scheme_deauth_easymode_detection.mp4`
  - `attack_scheme_deauth_fullmode_detection.mp4`
  - `attack_scheme_karma_easymode_detection.mp4`
  - `attack_scheme_karma_fullmode_detection.mp4`
  - `attack_scheme_rogueap_easymode_detection.mp4`
  - `attack_scheme_rogueap_fullmode_detection.mp4`
- `BP_detekcia_fakeAP_xlovin00.pdf` ..... text bakalárskej práce vo formáte PDF
- `EEICT_clanok_xlovin00.pdf` ..... článok konferencie EEICT 2020 vo formáte PDF
- `README.txt` ..... návod na spustenie