Možnosti detekce narušitelů v bezdrátových sítích

Ján Ševčík

Bakalářská práce
2021

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
Ústav informatiky a umělé inteligence

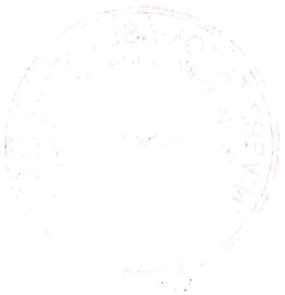
Akademický rok: 2020/2021

ZADÁNÍ BAKALÁŘSKÉ PRÁCE
(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení:	**Ján Ševčík**
Osobní číslo:	**A18079**
Studijní program:	**B3902 Inženýrská informatika**
Studijní obor:	**Softwarové inženýrství**
Forma studia:	**Prezenční**
Téma práce:	**Možnosti detekce narušitelů v bezdrátových sítích**
Téma práce anglicky:	**Possibilities of Intruder Detection in Wireless Networks**

Zásady pro vypracování

1. Specifikujte existující možnosti detekce narušitelů Wi-fi sítí.
2. Stanovte limity pro detekci narušitelů.
3. Proveďte návrh řešení pro detekci narušitelů Wi-Fi sítě.
4. Implementujte navržené řešení v testovacím prostředí.
5. Ověřte Vámi navržené řešení v testovací infrastruktuře.



Forma zpracování bakalářské práce: **Tištěná/elektronická**

Seznam doporučené literatury:

1. KHAN, Shafiullah a Al-Sakib Khan PATHAN, ed. Wireless networks and security: issues, challenges and research trends. Heidelberg: Springer, [2013], viii, 512 s. Signals and communication technology. ISBN 9783642361685.
2. DIOGENES, Yuri a Erdal OZKAYA. Cybersecurity – attack and defense strategies: infrastructure security with Red Team and Blue Team tactics. Birmingham: Packt, 2018, viii, 367 s. ISBN 9781788475297.
3. SAK, Brian a Jilumundi RAGHU RAM. Mastering Kali Linux wireless pentesting: test your wireless network's security and master advanced wireless penetration techniques using Kali Linux. Birmingham: Packt Publishing, 2016, xii, 285 s. Community experience distilled. ISBN 9781785285561.
4. ANMULWAR, S., S. SRIVASTAVA, S.P. MAHAJAN, A.K. GUPTA a V. KUMAR. Rogue access point detection methods: A review. International Conference on Information Communication and Embedded Systems (ICICES2014), Information Communication and Embedded Systems (ICICES), 2014 International Conference on [online]. 2014, , 1-6 [cit. 2020-12-01]. ISBN 9781479938353. ISSN edseee.IEEEConferenc. Dostupné z: doi:10.1109/ICICES.2014.7034106
5. FADYUSHIN, Vyacheslav a Andrey POPOV. Building a pentesting lab for wireless networks: build your own secure enterprise or home penetration testing lab to dig into the various hacking techniques. Birmingham: Packt Publishing, 2016, xii, 245 s. Community experience distilled. ISBN 9781785283154.

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

Datum zadání bakalářské práce: **15. ledna 2021**
Termín odevzdání bakalářské práce: **17. května 2021**

doc. Mgr. Milan Adámek, Ph.D. v.r.
děkan

UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ
Fakulta aplikované informatiky
DĚKAN
L.S.

prof. Mgr. Roman Jašek, Ph.D. v.r.
ředitel ústavu

Ve Zlíně dne 15. ledna 2021

Prohlašuji, že

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

Prohlašuji,

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

Ve Zlíně, dne Ján Ševčík v.r.

ABSTRAKT

Cieľom bakalárskej práce je vytvoriť systém pre detekciu narušiteľov v bezdrôtových sieťach. Teoretická časť sa zameriava na fungovanie sietí WLAN a ich bezpečnosť. Tiež sú v nej popísane útoky na siete WLAN a ich detekcia pomocou WIDS. Praktická časť je zameraná na vytvorenie návrhu systému pre detekciu narušiteľov, ktorý využíva nástroje Kismet a Snort. Návrh je implementovaný v testovacom prostredí a následne otestovaný rôznymi druhmi útokov na bezdrôtové siete WLAN.

Klíčová slova: WLAN, Wireless Intrusion Detection, Kismet, Snort, bezpečnosť, detekcia narušiteľov

ABSTRACT

The aim of the bachelor thesis is to create a system for detecting intruders in wireless networks. The theoretical part focuses on the operation of WLANs and their security. It also describes attacks on WLANs and their detection using WIDS. The practical part is focused on the design of an intruder detection system, that uses tools Kismet and Snort. The design is implemented in a test environment and subsequently tested with various types of attacks on wireless WLANs.

Keywords: WLAN, Wireless Intrusion Detection, Kismet, Snort, security, intruder detection

Moje poďakovanie patrí vedúcemu práce pánovi Ing. Davidovi Malaníkovi, Ph.D. za výber výbornej témy, za jeho užitočné rady a prínosné konzultácie, vďaka ktorým sa mi podarilo bakalársku prácu dokončiť.

OBSAH

ÚVOD

Bezdrôtové siete Wi-Fi sa stali súčasťou každodenného života ľudí naprieč celým svetom. Sú tak rozšírené, že by bolo skoro nemožné nájsť domácnosť alebo podnik, v ktorom sa takáto sieť nenachádza. Hlavnou príčinou tohto javu je, že oproti káblovej sieti, na bezdrôtovú sieť sa môžete pripojiť z hocijakého miesta a máte možnosť sa pohybovať a súčasne komunikovať so sieťou. Taktiež je bezdrôtová sieť veľmi jednoduchá na implementáciu i prevádzku, a zároveň finančne nenáročná. Keď si v dnešnej dobe zakúpite internet, provider k nemu automaticky poskytne aj router, ktorý už disponuje bezdrôtovou sieťovou kartou a anténami schopnými prevádzkovať bezdrôtovú sieť Wi-Fi. Rozšírenosť je badateľná aj na väčšine novodobých inteligentných zariadení, keďže sa skoro všetky fabrikujú s bezdrôtovými sieťovými kartami, ktoré majú schopnosť sa na siete Wi-Fi pripojiť.

Práve množstvo výhod bezdrôtových sietí Wi-Fi má za následok existenciu aj niekoľkých nevýhod, ktoré vznikajú práve kvôli ich flexibilite. Najzraniteľnejšou časťou je bezpečnosť. Bezpečnosť je veľmi dôležitá súčasť bezdrôtových sietí, keďže informácie sa na takejto sieti voľne šíria vzduchom a oproti káblovým sieťam, stačí byť narušiteľovi iba v dosahu signálu a dokáže ich získať. Aj napriek tomu, že sa zabezpečenie bezdrôtových sietí neustále vyvíja, doteraz sa vždy našlo niekoľko spôsobov, ako tieto siete napadnúť a získať citlivé informácie. Tento fakt si väčšina ľudí neuvedomuje a myslí si, že bezdrôtové siete sú dostatočne bezpečné a vôbec sa o ich bezpečnosť nezaujímajú.

Akonáhle sa niekto začne zaujímať o zabezpečenia bezdrôtových sietí, zistí, že ich bezpečnosť nie je dokonalá a samotná, ako taká, na ochranu siete nestačí. Bolo teda potrebné vyvinúť systémy, ktoré sú schopné monitorovať bezdrôtové siete a analyzovať ich prevádzku pre možné narušenia, čím sa ochrana bezdrôtových sietí posúva o ďalší level. Takéto detekčné systémy sa nazývajú WIDS (Wireless Intrusion Detecion Systems). Sú schopné detegovať narušenie bezpečnosti na sieti a instantne naň upozorniť. Nie sú veľmi rozšírené a využívajú sa väčšinou len v komerčnom prostredí, kde takéto narušenia môžu spôsobiť fatálne následky.

Na to, aby sme boli schopní pochopiť fungovanie systémov pre detekciu narušiteľov, je najskôr potrebné pochopiť a oboznámiť sa s tým, ako fungujú bezdrôtové siete WLAN, akým spôsobom na nich prebieha komunikácia a aké typy zabezpečenia môžu mať. Tiež je nutné pochopiť priebeh rôznych útokov na sieť, do akých kategórii sa zaraďujú, čo nimi narušiteľ môže získať a ako niektorým z nich môžme zabrániť. V neposlednom rade je tiež treba oboznámiť sa s tým, ako samotný systém na detekciu narušiteľov pracuje, aké ma komponenty, aké využíva technológie pre detekciu, ako analyzuje sieť a aké sú jeho limitácie.

I. TEORETICKÁ ČÁST

1 WIRELESS LOCAL AREA NETWORK (WLAN)

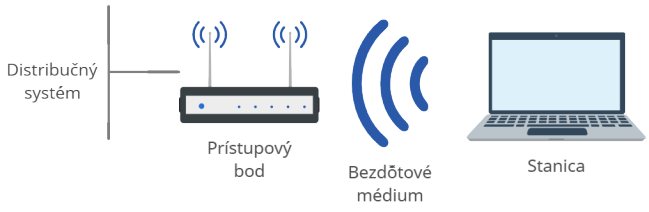
1.1 Úvod

Kapitola sa zaoberá fungovaním bezdrôtovej siete WLAN, opisuje zariadenia, aké sa na sieti WLAN nachádzajú a aké topológie tejto siete existujú. Venuje sa spôsobom, akými zariadenia na sieti WLAN navzájom komunikujú, a pravdaže, aj zabezpečeniam využívajúcim sa na sieti tohoto typu.

Wireless Local Area Network (WLAN) je sieť spájajúca dve alebo viaceré zariadenia, ktoré nie sú pripojené fyzicky pomocou kábla, ale pomocou rádiového signálu. Väčšinou slúži na prepojenie bezdrôtových zariadení do drôtovej siete LAN. Nejedná sa o veľkú sieť, zväčša pokrýva len menšiu geografickú oblasť, ktorá má rádovo niekoľko metrov, napríklad kanceláriu, budovu alebo celé bloky budov. V praxi sa WLAN skladá z dvoch druhov zariadení, a to z bezdrôtových klientov, ako sú napr. mobil alebo laptop, a z prístupového bodu, ako je napr. router. Na to, aby tieto zariadenia mohli byť na sieť WLAN pripojené a komunikovať v nej, musia byť vybavené bezdrôtovou sieťovou kartou [1] . Pre špecifikáciu tejto komunikácie existuje štandard IEEE 802.11, ktorý určuje rádiové štandardy a štandardy sieťového protokolu.

1.2 Terminológia a dizajn

Siete 802.11 sa skladajú zo 4 základných komponentov. [1]



Obrázek 1.1 Základné komponenty siete 802.11

1.2.1 Stanica

Stanice sú zariadenie, ktoré sú vybavené bezdrôtovou sieťovou kartou, čiže dokážu bezdrôtovo komunikovať. Väčšinou sa jedna práve o mobilné zariadenia, ako napr. laptop alebo telefón, avšak nie je to pravidlo. Stanicami môžu byť aj statické zariadenia, ku ktorým nechceme pripájať kábel a majú bezdrôtovú sieťovú kartu.

1.2.2 Prístupový bod

Prístupový bod nám vykonáva funkciu mosta, ktorý premosťuje komunikáciu z bezdrôtovej siete na drôtovú. Vykonáva viac funkcií, ale jeho najvýznamnejšou je práve premosťovanie.

1.2.3 Bezdrôtové médium

Bezdrôtové médium sa využíva pri prenose rámcov z jednej stanice na druhú. Tvoria ho rádiové vlny, ktoré sú vysielané na nelicencovaných frekvenčných pásmach 2,4 GHz a 5 GHz, ktoré sú rozdelené do jedenástich kanálov, z ktorých prvý, šiesty a jedenásty sa navzájom neprekrývajú.

1.2.4 Distribučný systém

Ak chceme pokryť väčšiu plochu niekoľkými prístupovými bodmi, potrebujeme, aby tieto prístupové body navzájom komunikovali a posielali si informácie o pohybe pripojených staníc. Práve distribučný systém sa zaoberá vzájomnou komunikáciou medzi prístupovými bodmi a slúži na to, aby sa rámce dostali vždy do cieľa.

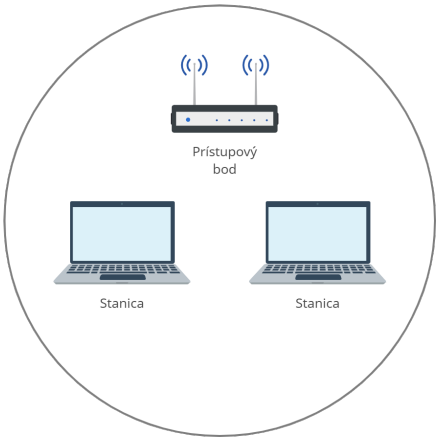
1.3 Topológie siete

IEEE 802.11 špecifikuje určitú štruktúru usporiadania komponentov v bezdrôtových sieťach. Takéto štruktúry sa nazývajú topológie. Rozsah topológií môže byť od veľmi jednoduchých, na ktorých je pripojených iba niekoľko zariadení, až po zložité, ktoré môžu byť teoreticky neobmedzene veľké. Vždy sú však potrebné minimálne 2 zariadenia pre vytvorenie siete [2].

1.3.1 Basic Service Set (BSS)

BSS je topológia pozostávajúca z jedného prístupového bodu a viacerých staníc, ktoré sú naň pripojené. Stanice navzájom komunikujú cez prístupový bod [3] .

- **Basic Service Set Identifier (BSSID) -** predstavuje MAC adresu prístupového bodu, ktorá ma 48bitov (xx.xx.xx.xx.xx.xx). Každá jedna stanica alebo prístupový bod ma unikátnu MAC adresu [3].
- **Service Set Identifier (SSID) -** je meno bezdrôtovej siete, ktoré si môžeme nastaviť na prístupovom bode. Na jeden prístupový bod môžeme nakonfigurovať niekoľko SSID, ktoré si zadáme [3].

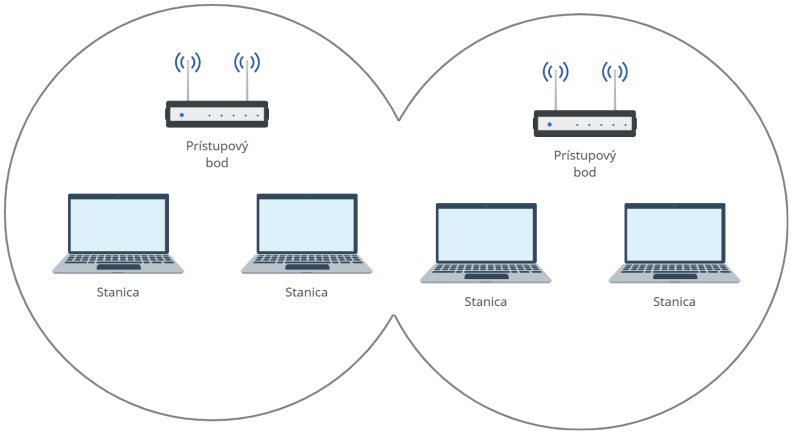


Obrázek 1.2 Basic Service Set

1.3.2 Extended Service Set (ESS)

ESS je topológia podobná ako BSS, avšak obsahuje niekoľko prístupových bodov, na ktorých je napojených niekoľko staníc, nie len jedna. Jednoducho povedané, je to niekoľko BSS prepojených pomocou distribučného systému. Stanice môžu bez problémov prechádzať medzi jednotlivými BSS bez stratenia konektivity. [1]

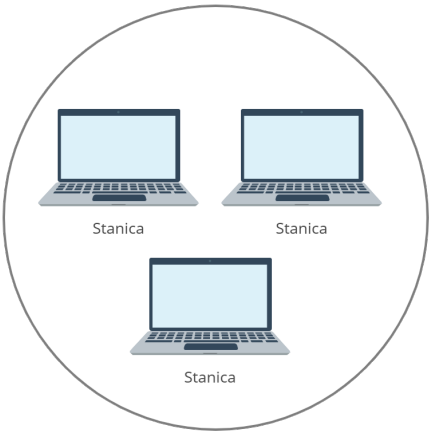
- **Extended Service Set Identifier (ESSID) -** ESSID a BSSID sú rovnaké topológie, avšak ESS môže obsahovať niekoľko prístupových bodov s rozličným BSSID pripojených na to isté ESS [3]. Prístupové body pripojené na rovnaký distribučný systém môžu taktiež mať vlastné SSID, ale stále sú súčasťou Extended Service Set.



Obrázek 1.3 Extended Service Set

1.3.3 Independent Basic Service Set (IBSS)

IBSS je topológia pozostávajúca iba zo staníc, ktoré sú pripojené navzájom medzi sebou. Neobsahuje žiadne prístupové body. Predstavuje ju niekoľko staníc v dosahu pripojených pomocou ad hoc mode.[1]



Obrázek 1.4 Independent Basic Service Set

1.4 Komunikácia

Na všetku komunikáciu medzi zariadeniami na sieti 802.11 sa používajú rámce. Rámce sú štandardizované štruktúry dát, ktoré obsahujú informácie o fyzických adresách, prenášaných dátach a kontrole integrity [1]. Štandard 802.11 užšie špecifikuje všetky typy a funkcie rámcov na správu pripojenia, prenos dát a riadenie linky, na ktorej sú prenášané.

1.4.1 Manažment rámce

Na drôtovej sieti sa môže stanica jednoducho pripojiť do siete tým, že pripojí kábel do portu prepínača. V bezdrôtových sieťach je pripojenie do siete o niečo zložitejšie, nakoľko stanicu nedokážeme fyzicky pripojiť, a preto musí existovať určitý mechanizmus, ktorý nám aj napriek tomu dovolí sa na sieť pripojiť. Práve tento mechanizmus majú na starosť manažment rámce, ktoré na stanici zabezpečujú funkciu pripojenia do bezdrôtovej siete. Taktiež sú tieto rámce zodpovedné za udržanie komunikácie medzi zariadeniami. Bez manažment rámcov by nebolo možné sa na bezdrôtové siete pripojiť. Manažment rámce rozdeľujeme na niekoľko druhov, tie najdôležitejšie sú popísané v tabuľke 1.1 [2] .

Tabulka 1.1 Manažment rámce

Rámec	**Popis**
Beacon frame	Vysielajú z prístupového bodu, aby oznámili svoju prítomnosť a inzerovali informácie o nakonfigurovaných sieťach.
Probe request	Posiela ich stanica v snahe kontaktovať inú stanicu a zhromaždiť o nej informácie. Príkladom toho je, keď klient hľadá prístupový bod.
Probe response	Sú odpovede na probe requests, stanica vysiela informácie o svojich schopnostiach.
Authentication	"Unicastujú"rámce zo stanice, ktoré sa používajú na určenie, či má klient príslušné schopnosti na pripojenie k bezdrôtovej sieti.
Deauthentication	Tieto rámce sa odosielajú, ak sa stanice rozhodnú ukončiť komunikáciu medzi sebou, napríklad, ak prístupový bod chce odpojiť klienta alebo ak sa klient rozhodne ukončiť pripojenie.
Association requests	Odosiela sa z klienta na opýtanie sa prístupového bodu, či sa môže pripojiť na určité SSID a posiela informácie o schopnostiach klienta.
Association responses	Odosiela sa ako odpoveď na association requests.
Reassociation requests	Odosiela sa, keď sa klient pohybuje medzi rôznymi prístupovými bodmi, ktoré sú v rovnakom ESSID alebo keď sa klient znova pripojí na prístupový bod po určitom čase.
Reassociation responses	Odosiela sa ako odpoveď na reassociation requests.

1.4.2 Dátové rámce

Dátové rámce slúžia na prenos dát z vyšších vrstiev medzi bezdrôtovými stanicami. Okrem štandardných dátových rámcov tu patria aj rámce so službou kvality a prázdne dátové rámce. [2]

Tabulka 1.2 Dátové rámce

Rámec	**Popis**
Data	Prenos dát medzi prístupovým bodom a stanicami.
Null Data	Oznámenie zmeny stavu zariadenia do módu šetrenia energie.
QoS Data	Prenos dát so zvýšenou kvalitou služieb.

1.4.3 Riadiace rámce

Riadiace rámce sa používajú na získanie a vyčistenie kanálu a ďalšie riadenia prenosu na bezdrôtovom médiu. Sú potrebné na správnu činnosť výmeny prenosu medzi klientskymi stanicami. [2]

Tabulka 1.3 Riadiace rámce

Rámec	**Popis**
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.

1.5 Bezpečnosť

Najväčšou slabinou bezdrôtových sietí je práve to, že všetky dáta sa posielajú vzduchom, čo v praxi znamená, že ktokoľvek v dosahu rádiovej frekvencie vysielajúceho prístupového bodu je schopný ich zachytiť a potenciálne pri prenose vidieť citlivé informácie. Preto je pre zabezpečenie súkromia týchto dát potrebné silné šifrovanie, ktoré ich znemožní tak jednoducho čítať. Keďže bezdrôtové siete väčšinou fungujú iba ako portál pre iné sieťové infraštruktúry, ako je napríklad 802.3 Ethernet, je potrebné zabezpečiť, aby sa na takúto sieť dostali iba zariadenia, ktoré sú autorizované [4]. Aj napriek tomu, že existuje niekoľko ochranných mechanizmov zavedených kvôli zabezpečeniu komunikácie v rámci bezdrôtovej siete, dokážu sa aj v sieti WLAN nájsť chyby, ktoré sa môžu využiť na to, aby sme komunikáciu na bezdrôtovej sieti narušili, ba dokonca boli schopní dostať sa až k dátam, ktoré sa na bezdrôtovej sieti odosielajú.

1.5.1 WEP

WEP je prvá zabezpečovacia technika, ktorá sa využíva v sieťach 802.11 a vyšla zarovno s týmto štandardom. Hlavným cieľom používania WEP je poskytnúť zabezpečenie bezdrôtovej siete WLAN ako drôtovej LAN. WEP pomáha zabezpečiť komunikáciu a poskytuje tajnú autentifikačnú schému medzi prístupovým bodom a koncovými stanicami, ktoré budú pristupovať na sieť WLAN [4] . V zásade je WEP implementovaný tak, že užívateľ nemôže mať prístup do siete bez správneho kľúča. Využíva symetricky šifrované kľúče pomocou RC4. Dĺžka týchto kľúčov sa pohybuje od 64 bitov po 128 bitov. Zvyčajne sa využíva rovnaký šifrovací kľúč pre všetky uzly v sieti a ten ich manuálne preposiela do každého uzlu, čo znamená, že nedokáže poskytnúť funkciu správy kľúčov. Poskytuje autentifikáciu pomocou metódy SKA (shared key authentication), pri ktorej stanice potrebujú dve veci na to, aby sa pripojili do siete WLAN, a to SSID a kľúč WEP, ktorý generuje prístupový bod [5].

1.5.2 WPA

Po odhalení nedostatkov štandardu WEP musel vzniknúť' nový a bezpečnejší spôsob ochrany WLAN komunikácie, ktorý vyriešil všetky problémy skoršej zabezpečovacej

techniky WEP. Preto vznikol WPA, ktorého primárnym cieľom bolo zaviesť bezpečnostné opatrenia pre hlavné zraniteľnosti WEP. Pri tvorbe tohoto protokolu bolo dôležité nielen odstrániť všetky významné bezpečnostné vady WEP, ale aj priniesť kompatibilitu pre zariadenia, ktoré doteraz poskytovali iba WEP zabezpečenie, resp. kompatibilitu na starší typ hardvéru [4]. Najväčším rozdielom medzi danými štandardmi je to, že WPA používa protokol TKIP (Temporary Key Integrity Protocol). Ten vytvára unikátny šifrovací kľuč pre každý rámec. TKIP nahradzuje jeden statický kľúč, ktorý sa využíval vo WEP, viacerými kľúčmi, ktoré sú dynamicky generované a distribuované autentifikačným serverom [5]. WPA sa využíva v dvoch rôznych módoch, a to:

- **Enterprise/commercial WPA:** Mód využívajúci centralizovaný komponent, ktorý je známy ako RADIUS server, je zodpovedný za autentifikáciu, autorizáciu a má zodpovednosť za stanice pripojené na prístupový bod.
- **Personal/WPA-PSK (pre shared key) WPA:** Mód, v ktorom sa nenachádza žiadny RADIUS server, ale funguje pomocou pre shared key, kedy užívateľovi stačí vedieť SSID siete, na ktorú sa chce napojiť a WPA kľuč, ktorý generujú prístupový bod na to, aby bol schopný sa pripojiť do siete.

1.5.3 WPA2

IEEE 802.11i, taktiež referovaný ako WPA2, je dodatočný štandard s cieľom celkového vylepšenia autentifikácie a šifrovania na sieťach WLAN. Architektúra WPA2 je úplne odlišná ako architektúra WEP a WPA, pretože využíva jediný komponent pre manažment kľúčov a integráciu správ, a to CCMP (Counter Cipher Mode with Block Chaining Message Authentication Code Protocol). CCMP je založený na AES (Advanced Encryption Standard) [5] . Stále si však zachováva 2 módy - Personal a Enterprise. Vo WPA2 je nový kľúč generovaný pre všetky šifrované dátové pakety, ktoré sú pripravené na bezdrôtové odoslanie s vlastným šifrovacím kľúčom. Používanie tejto techniky robí dekódovanie paketov v sieti zložitejším a pre neautorizovaného užívateľa je veľmi náročné takéto pakety dešifrovať [4] .

1.5.4 WPA3

Podobne ako jeho predchodcovia, taktiež WPA3 prichádza v dvoch režimoch - WPA3-Personal a WPA3-Enterprise. Využíva novú technológiu pri Personal móde, nazývanú Simultaneous Authentication of Equals (SAE), nový protokol pre bezpečnejšiu výmenu kľúčov medzi stanicou a prístupovým bodom. Enterprise mód sa od verzie WPA2-Personal zásadne nemení, ale namiesto neho sa zameriava na pridanie vylepšení a zvýšenie odolnosti proti útokom [6] .

2 ÚTOKY NA WLAN

2.1 Úvod

Kapitola sa zaoberá možnými útokmi, ktoré hrozia užívateľom v sieťach WLAN.

Útok je možné popísať rôznymi spôsobmi podľa toho, aký je cieľ útoku. Všeobecne útok môže byť pokus o zničenie, úpravu, odhalenie, krádež alebo, najčastejšie, získanie neoprávneného prístupu k sieti. Útok neovplyvní iba jedného užívateľa, ale môže ovplyvniť všetkých užívateľov, ktorí sú pripojení k rovnakej sieti a prípadne poškodiť celý systém [7]. Na rozdiel od káblových sietí, bezdrôtové siete nemôžu byť fyzicky zabezpečené, čo znamená, že médium nemôže byť opatrené ochranou, ktorá sa dá využiť fyzicky pri káblových sieťach. Kvôli tomu sú bezdrôtové siete ešte zraniteľnejšie voči rôznym druhom útokov. Základný element, ktorý činí bezdrôtové siete zraniteľnejšími je skutočnosť, že používatelia, ktorí sú pripojení k rovnakej sieti využívajú spoločné médium, čo znamená, že všetky dáta, ktoré si vymieňajú medzi zariadeniami sú verejné. Každý užívateľ pripojený k rovnakej sieti môže zachytiť prenos ktoréhokoľvek iného používateľa v sieti jednoduchým monitorovaním prenosu pomocou rôznych techník a softvéru. Útočník teda môže zhromaždiť rôzne typy informácií, či už sú to dôležité údaje, ako sú heslá, alebo citlivé údaje, ako je súkromný chat. Takéto útoky vôbec nie sú zložité, a preto človek, ktorý má čo i len základné vedomosti o neoprávnenom získavaní údajov v bezdrôtovej sieti, dokáže spraviť väčšinu útokov, ktoré sú v kapitole popísané.

2.2 Rozdelenie útokov

Útoky na bezdrôtové siete sa dajú rozdeliť do troch kategórií podľa toho, čo chce daným útokom narušiteľ dosiahnuť. Tieto typy útokov sa považujú za najpoužívanejšie v bezdrôtových sieťach:

- Útoky voči šifrovaniu
- Pasívne útoky
- Aktívne útoky

2.3 Útoky voči šifrovaniu

Jedná sa o útoky, ktorými sa útočník snaží prelomiť šifrovanie na sieti, aby sa mohol dostať k dátam, ktoré sú šifrované. Využívajú slabiny v bezpečnostných protokoloch WEP, WPA, WPA2, vďaka ktorým sa útočníci dostanú či už k heslu od siete, alebo priamo dešifrujú komunikáciu medzi stanicou a prístupovým bodom. V tejto časti sú

popísané iba útoky na WPA a WPA2, keďže WEP sa považuje za zastaralú technológiu, ktorá sa v dnešnej dobe už skoro vôbec nevyužíva.

2.3.1 Slovníkový/Brute force útok

Skoro všetky siete WLAN používajú vopred zdieľaný kľúč alebo heslo počas celej komunikácie s prístupovým bodom. Princíp útoku tohto typu je založený na tom, že útočník odpočúva komunikáciu a snaží sa zachytiť handshake medzi stanicou a prístupovým bodom v nešifrovanej podobe. Následne útočník skúša dosadzovať testovací kľúč zo slovníka alebo, pri slabom hesle, skúša využiť techniku brute force. Akonáhle sa mu podarí nájsť správny kľúč v slovníku, získava prístup k sieti. Slovníkový alebo brute force útok možno zrealizovať len na sieťach typu WPA/WPA2 Personal, ktoré využívajú vopred zdieľaný kľuč. Útočník môže taktiež využiť aj útok Evil twin, pomocou ktorého od napadnutej stanice dostaneme všetky potrebné údaje. [8]

2.3.2 KRACK útok

Na vytvorenie šifrovaného spojenia WPA2 sa využíva 4-way handshake, avšak pri opätovnom pripojení sa využíva iba tretia časť handshake na to, aby sa mohlo zariadenie rýchlejšie pripojiť na už známe siete. Tu prichádza útočník, ktorý vytvorí klon siete, na ktorú sa stanica opätovne pripája a snaží sa danú stanicu donútiť, aby sa pripojila na narušiteľom vytvorený klon. Pri takomto pripájaní útočník stále odosiela tretiu časť handshake a každý raz, keď stanica prijme toto pripojenie, útočník dešifruje malú časť dát, ktorou sa potom snaží zistiť šifrovací kľúč. [9]

2.4 Pasívne útoky

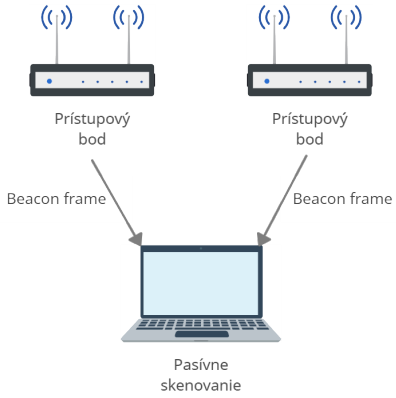
Pasívne útoky sa tykajú útočníkov, ktorí sa pokúšajú bezdrôtovú sieť analyzovať tým, že monitorujú sieťovú prevádzku medzi napojenými zariadeniami. Zahŕňa to zhromaždenie čo najväčšieho množstva informácií na rôzne účely [10] . Hocikto, kto ma bezdrôtový sieťový adaptér s podporou monitorovacieho módu, môže jednoducho zhromaždiť dáta, ktoré si ostatné zariadenia posielajú medzi sebou. Takéto jednoduché odpočúvanie možno použiť aj vďaka tomu, že bezdrôtové siete fungujú na nelicencovanom frekvenčnom spektre. To znamená, že každý, kto používa správnu frekvenciu, môže bez problémov preniknúť do súkromnej bezdrôtovej siete bez toho, aby to niekto spozoroval. Na rozdiel od káblových sietí, pri ktorých musí útočník byť pripojený fyzicky na sieť, pri bezdrôtových sieťach môže byť útočník vďaka prenosovému médiu aj niekoľko kilometrov ďaleko, ak použije správnu anténu a dobre ju nasmeruje. Takáto možnosť sieťovým administrátorom ešte viac sťažuje ochranu sietí pred pasívnymi útokmi. Útoky samotné nepredstavujú z hľadiska bezpečnosti pre užívateľov príliš veľké

riziko, ak na sieti využívame šifrovanie. Vďaka nemu informácie, ktoré útočník získa nebudú pre neho čitateľné. Riziko nastáva akonáhle sa útočníkovi podarí využiť niektorú zo zraniteľností v šifrovacom algoritme, čím sa takýto útok stáva omnoho väčším problémom a môže dôjsť ku kompromitácii siete. Previesť takýto útok nie je vôbec zložité, nakoľko existuje niekoľko open-source nástrojov, ako napr. `Kismet, TCPDump, Wireshark, airodump-ng`, ktoré to umožňujú a je úplne jednoduché ich nastaviť a začať používať [11] . Jediné, čo je k tomu potrebné je mať pri väčšine z nich len základné znalosti operačného systému Linux a, ako už bolo spomenuté vyššie, anténu, ktorá má možnosť byť v monitorovacom móde. Tá sa dá v dnešnej dobe kúpiť veľmi jednoducho a lacno.

2.4.1 Skenovanie siete

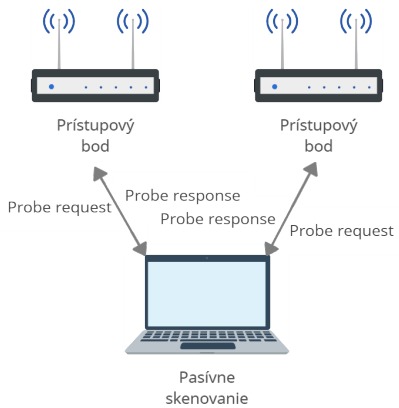
Skenovanie siete je prvou fázou útoku na bezdrôtovú sieť. Útočník počas nej zhromaždí dostatok informácií, ktoré je možné použiť v neskorších fázach útoku. Množstvo zhromaždených informácií v tejto fáze ovplyvňuje plán útoku a definuje ďalšie činnosti, ktoré útočník vykoná. Skenovanie siete sa môže rozdeliť do dvoch hlavných kategórií, a to aktívne skenovanie a pasívne skenovanie [2]. Pri pasívnom skenovaní útočník nenápadne objaví cieľovú sieť a v sieti nezanechá žiadne stopy ani dôkazy. Pri aktívnom skenovaní musí útočník začať so sieťou komunikovať na to, aby ju odhalil, tým pádom po sebe zanecháva stopy. Pasívne skenovanie je teda preferovaná metóda, nakoľko obeť nevie o tom, že skenovanie prebieha a nemá sa ako brániť. Pasívnym skenovaním však nemusíme dosiahnuť požadovaný výsledok, ak je sieť dobre nastavená a zabezpečená. V tom prípade je potrebné začať s aktívnym skenovaním, ktoré vie odhaliť viac.

Pasívne skenovanie Funguje tak, že zariadenie počúva komunikáciu a hľadá beacon frames od prístupového bodu. Tie sú odosielané v pravidelných intervaloch. Stanica najskôr počúva SSID nachádzajúce sa v zozname preferovaných sietí a akonáhle zistí, že SSID zo zoznamu sa nachádza v blízkosti, pokúsi sa vytvoriť pripojenie na sieť. V prípade, ak sa v dosahu nachádza viacero SSID zo zoznamu preferovaných sietí, pripojí sa na prístupový bod, ktorý ma najlepší signál. Pri pasívnom skenovaní zariadenie aktívne nehľadá cieľovú sieť. Jednou z hlavných limitácií pasívneho skenovanie je, že sa nám nemusí podariť nájsť prístupové body, ak aktívne nevysielajú beacon rámce. Z toho dôvodu väčšinou sieťoví administrátori preventívne vypínajú možnosť periodického vysielania beacon rámcov, a tak tieto siete nie sú ľahko detekovateľné. V takom prípade sa narušiteľovi pri používaní pasívneho skenovania nemusí podariť nájsť prístupové body v dosahu, avšak stále sa mu môže podariť ich nájsť pomocou detekcie komunikácie medzi inými stanicami a prístupovým bodom. Obrázok 2.1 zobrazuje, ako pasívne skenovanie prebieha. [2]



Obrázek 2.1 Ukážka pasívneho skenovania

Aktívne skenovanie Pri využívaní aktívneho skenovania sa rámce, na rozdiel od pasívneho, aj odosielajú, nie len prijímajú. Pri tomto skenovaní stanica odosiela probe request rámce, v ktorých je pole SSID buď SSID stanice, z ktorej ich odosielame, alebo je toto pole prázdne. Prístupové body v dosahu takejto stanice na dané rámce odpovedajú pomocou probe response rámcu, ktorý obsahuje rovnaké informácie ako beacon rámec. Na tento rámec odpovedajú aj prístupové body, ktoré nevysielajú beacon rámce, a tým dávajú najavo svoju existenciu. Preto pri aktívnom skenovaní dokážeme nájsť oveľa viac prístupových bodov. Ako protiopatrenie proti probe request rámcom, v ktorých nie je vyplnené SSID, existuje nastavenie, kedy prístupový bod na takéto rámce neodpovedá, vďaka čomu ho pomocou nich nemožno detegovať. V tom prípade iba stanice so správnou konfiguráciou SSID dokážu detegovať takýto prístupový bod a pripojiť sa naň. Obrázok 2.2 zobrazuje ako aktívne skenovanie prebieha. [2]



Obrázek 2.2 Ukážka aktívneho skenovania

2.4.2 Odpočúvanie

Odpočúvanie, alebo sniffing, je aktivita, pri ktorej útočník zachytáva a analyzuje komunikáciu na bezdrôtovej sieti, aby sa dostal k citlivým informáciám. Zachytávanie komunikácie na bezdrôtových sieťach nie je vôbec zložité. Ako už bolo uvedené vyššie, jediným potrebným zariadením je bezdrôtový sieťový adaptér v monitorovacom móde, ktorý dokáže monitorovať komunikáciu. Keďže väčšina bezdrôtových sietí v dnešnej dobe už využíva určitý druh šifrovania, nie je jednoduché takúto komunikáciu čítať, preto musí útočník najskôr využiť jednu zo slabín WEP alebo WPA/WPA2, aby mohol komunikáciu prečítať. [13]

2.5 Aktívne útoky

Aktívne útoky zahŕňajú získanie úplnej kontroly nad sieťou alebo vykonanie neautorizovanej zmeny na bezdrôtovej sieti. Na rozdiel od pasívnych útokov, kde sa útočník snaží odpočúvať prevádzku na sieti, aktívny útok zahŕňa monitorovanie prevádzky siete a následnú modifikáciu zachytených rámcov alebo dokonca vytvorenie nových rámcov, ktorými sa útočník snaží napadnúť prístupový bod či asociované stanice [10]. Aktívny útok začína väčšinou vtedy, keď už útočník získal dostatok informácií pre získanie kontroly nad sieťou z predchádzajúceho pasívneho útoku. Pri aktívnom útoku sa narušiteľ buď pokúsi obísť zabezpečenie a získať úplnú kontrolu nad sieťou, alebo začne ničiť komunikáciu na sieti tak, aby nebolo možné ju využívať. Takýto útok oproti pasívnemu predstavuje omnoho väčšiu hrozbu, pretože útočník môže na sieti získavať informácie od ostatných zariadení bez toho, aby potreboval ich vzájomnú komunikáciu, nakoľko je schopný ju vytvoriť sám. Na vytvorenie podobného útoku nepotrebuje útočník zložité vybavenie, stačí mu bezdrôtový sieťový adaptér s funkciou *packet injection*, ktorá mu poskytne modifikáciu rámcov na sieti aj možné vytvorenie vlastných [11]. Na vykonanie aktívnych útokov sú taktiež dostupné open-source nástroje, ako napr. `packetforge-ng, mdk3` , ktorými je možné jednoducho útok tohto typu zrealizovať.

2.5.1 Denial of Service (DoS)

Denial of Service je útok, na ktorý sa v porovnaní s ostatnými útokmi nesústreďuje toľká pozornosť, avšak stále môže predstavovať veľkú hrozbu, predovšetkým na bezdrôtových sieťach, kde sa využíva ako predvoj pre ďalšie útoky. Narušiteľ môže dočasne odstaviť bezdrôtovú sieť viacerými technikami a spôsobiť, že nebude funkčná pre bežných užívateľov. Vďaka prenosovému médiu a voľne dostupným frekvenciám, ktoré využívajú bezdrôtové siete je takýto útok ešte jednoduchší. Management rámce nedokážu ochrániť veľkú väčšinu bezdrôtových sietí a v takom prípade útočníkovi stačí využiť iba jeden rámec na to, aby odpojil klientsku stanicu z prístupového bodu [13]. Týmto

atakom síce nezíska žiadne citlivé údaje, ale ako je uvedené vyššie, funguje ako predvoj pre oveľa závažnejšie útoky, ako napríklad Evil Twin alebo Man-In-The-Middle, ktoré už citlivé informácie dokážu bez problémov získať.

2.5.2 Man-in-the-Middle

Man-in-the-middle je forma útoku využívajúca sniffing, na to aby sa útočník dostal medzi dve navzájom komunikujúce zariadenia a stal sa tretím, neviditeľným zariadením, ktoré riadi komunikáciu medzi obeťami prostredníctvom nezávislého spojenia s každou obeťou. Útočník preposiela komunikáciu medzi obeťami tak, aby si mysleli, že sú v spojení cez súkromnú komunikáciu. Na to, aby mohol narušiteľ vykonať daný útok, musí byť schopný zachytiť komunikáciu prechádzajúcu medzi dvoma obeťami a modifikovať ju natoľko, aby ich presvedčil, že komunikujú len navzájom. [12]

ARP poisoning je útok pracujúci na tretej vrstve OSI modelu a snaží sa meniť trasu komunikácie prebiehajúcej na sieti tak, aby prechádzala cez zariadenie útočníka. Útočník to chce dosiahnuť tým, že sa pokúša o manipuláciu s ARP tabuľkou napadnutého zariadenia, aby si myslelo že default gateway je zariadenie podstrčené útočníkom. [12]

DNS spoofing je typ útoku, pri ktorom sa útočník pokúša zmeniť DNS server napadnutej stanice, vďaka čomu potom poskytuje nesprávne informácie o mapovaní názvov domén na IP adresu. Dosiahne to relatívne jednoducho tak, že pri sniffingu zistí, že daná stanica žiada o mapovanie nejakej domény a útočníkov DNS server odpovie rýchlejšie ako ten pravý. Výsledkom je, že akonáhle sa chce napadnutá stanica dostať na normálnu webovú stránku, nepodarí sa jej to a DNS server ju presmeruje na stránku útočníka. Ten môže týmto spôsobom získať citlivé údaje, ako sú email, heslo, telefónne číslo a podobne. [12]

Rogue DHCP server predstavuje útok, ktorého princíp spočíva v tom, že sa narušiteľovi podarí zmeniť DHCP server za jeho vlastný, vďaka čomu je následne schopný nakonfigurovať pripojené zariadenia takým spôsobom, aby default gateway pre všetky pripojené zariadenia bola jeho podstrčená stanica. Na to, aby sa útočníkovi podarilo takýto útok previesť, je nutné, aby odstavil originálny DHCP server, ktorý už na sieti existuje a to buď tým, že využije DoS útok, alebo DHCP starvation attack alebo rychlejšie odpovedal na DHCP request. [12]

2.5.3 Evil Twin

Evil Twin, alebo aj zlé dvojča, je útok, pri ktorom útočník nakonfiguruje svoj bezdrôtový sieťový adaptér tak, aby fungoval ako prístupový bod. Na takomto prístupovom bode následne nastaví rovnaké SSID, aké používa sieť, na ktorej je obeť útoku pripojená. Prístupový bod útočníka je teda funkčný ako zlé dvojča originálneho prístupového bodu, má rovnaké SSID, ale vysiela na inom kanáli. Útočník potom odošle falošné disassociation a deauthentication rámce, ktoré prinútia stanicu klienta odpojiť sa z originálneho prístupového bodu na jeho zlé dvojča. V tomto štádiu už útočník úspešne uniesol napadnutú stanicu od originálneho prístupového bodu a dostáva sa ku komunikácii obete. Na takýto útok dokonca netreba použiť ani deauthentication rámce. Na prepojenie klienta na zlé dvojča nám postačí iba rušička rádiového signálu. [13]

3 WIRELESS INTRUSION DETECTION SYSTEM (WIDS)

3.1 Úvod

Ako bolo uvedené v predchádzajúcej kapitole, bezdrôtové siete WLAN majú stále niekoľko zraniteľností, kvôli ktorým dokážu byť terčom útokov aj napriek využitiu bezpečnostných opatrení, preto je potrebné ich chrániť aj ďalším stupňom ochrany. Predstavuje ho Wireless Intrusion Detection System, v preklade Bezdrôtový systém pre detekciu prienikov. Bol vyvinutý na to, aby chránil bezdrôtovú sieť pred už známymi útokmi a zraniteľnosťami. Keďže na začiatku používania bezdrôtových sietí WLAN bolo zabezpečenie veľmi obmedzené vzhľadom na tak široko otvorené prenosové médium, akým je rádiový signál, bolo potrebné vyvinúť systém takéhoto druhu, ktorý by dokázal ochrániť sieť pred existujúcimi zraniteľnosťami. Preto aj vývoj tohoto systému napredoval spoločne s vývojom bezdrôtových sietí WLAN. Wireless Intrusion Detection System neustále monitoruje prenosové médium a deteguje pokusy o zneužitie zraniteľností či nedodržiavanie bezpečnostných politík, ktoré sú na sieti nastavené. Pôsobí teda ako druhý stupeň ochrany bezdrôtovej siete WLAN a do istej miery poskytuje záruku, že v sieti nedôjde k škodlivému prenosu alebo neoprávnenej činnosti.

3.2 Komponenty

Systém WIDS na svoju prevádzku potrebuje niekoľko komponentov, ktoré typicky fungujú na distribuovanom klient-server modeli obsahujúcom tri základné komponenty. [14]

3.2.1 Server

Server funguje ako centrálny bod pre monitorovanie bezpečnosti, výkonu a zber dát. Na detekciu potencionálnej hrozby server využíva niekoľko techník, ktoré sú popísane v sekcii 3.4.

3.2.2 Konzola

Konzola slúži ako rozhranie pre WIDS, ktoré komunikuje so serverom. Používa sa na administratívu a konfiguráciu nastavení servera.

3.2.3 Senzory

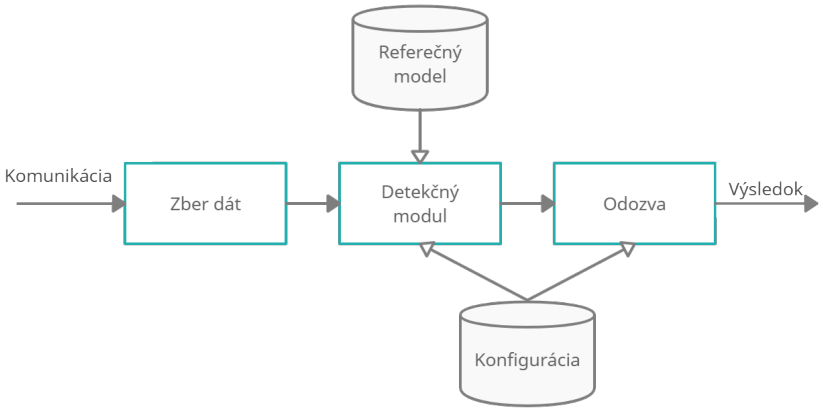
Senzory predstavujú zariadenia, ktoré by mali byť umiestnené strategicky, kvôli odpočúvaniu a odchytávaniu celej komunikácie na bezdrôtovej sieti. Senzory sú oči a uši monitorovacieho systému WIDS. Využívajú bezdrôtové sieťové karty v monitorovacom móde, čím sú schopné monitorovať prevádzku na sieti. Senzory neustále skenujú všetky

kanály, ktoré využíva štandard 802.11. Momentálne senzory nie sú schopné monitorovať všetku komunikáciu v pásme súčasne, preto musia monitorovanie medzi kanálmi stále striedať. Tu prichádza problém týchto zariadení, pretože akonáhle skenujú jeden kanál, na ostatných môže prebiehať škodlivá činnosť. Pre zníženie tohto problému snímajú každý kanál niekoľkokrát za sekundu. Senzory môžu mať rôznu formu, a preto si uvedieme ich jednotlivé typy [15]:

- **Dedikované:** sú priamo určené iba na monitorovanie bezdrôtovej siete. Na sieti nekomunikujú s ostatnými zariadeniami. Niektoré vykonávajú priamo analýzu monitorovanej siete, iné iba preposielajú monitorovanú komunikáciu na server, ktorý analýzu vykonáva. Tieto senzory sú zvyčajne pripojené pomocou kábla. Dedikované senzory sú najčastejšie určené pre jeden z dvoch typov nasadenia:
  - **Fixné:** senzor je nasadený na konkrétne miesto.
  - **Mobilné:** senzor je navrhnutý na použitie počas pohybu. Administrátor siete môže použiť mobilný senzor napríklad pri prechádzaní budovami pre nájdenie falošných prístupových bodov.
- **Vstavané do prístupového bodu:** sú priamo vstavané do prístupového bodu a ich nevýhodou je, že obvykle poskytujú menšiu ochranu, pretože potrebujú rozdeliť čas medzi komunikáciou na sieti a monitorovaním siete.

3.3 Proces detekcie

Pre pochopenie princípu fungovania WIDS si musíme ukázať, ako prebieha celý proces detekcie a jednotlivo popísať všetky fázy, ktoré sa vykonávajú pri využívaní systému WIDS. [16]



Obrázek 3.1 Proces detekcie

- **Zber dát:** v tejto fáze WIDS zhromažďuje nespracovaný prenos na bezdrôtovej sieti a prepracováva ho na čitateľný a použiteľný pre analýzu a identifikáciu prienikov, čo prebieha v ďalšej fáze - detekčným modulom.
- **Detekčný modul:** považuje sa za jadro procesu detekcie narušenia, kde WIDS analyzuje výsledok fázy zberu dát podľa algoritmov referenčného modelu na identifikáciu škodlivých aktivít.
- **Referečný model:** je databáza, v ktorej sa nachádza model normálneho a predpokladaného správania siete, signatúry útokov alebo špecifický profil využívajúci sa pri technikách analýzy.
- **Konfigurácia:** WIDS zvyčajne obsahuje konfiguračný súbor alebo nastavenia, ktoré možno použiť na konfiguráciu WIDS podľa charakteristík siete a použitých zariadení, ako aj na úpravu detekčného modulu a odozvu WIDS podľa bezpečnostnej politiky systému.
- **Odozva:** pri detekcii vniknutia WIDS generuje alerty buď pre informovanie správcu siete, alebo na vyvolanie doplnkového preventívneho protiopatrenia.

3.4 Techniky detekcie

Základný princíp detekcie narušenia je založený na predpoklade, že podozrivá činnosť sa zreteľne líši od bežnej, a teda je detegovateľná. Na základe toho vzniklo niekoľko techník k detekcii útokov, ktoré sa dajú rozdeliť do dvoch kategórií.

3.4.1 Detekcia na základe signatúr

Signatúra je vzor zodpovedajúci priebehu známeho útoku. Detekcia na základe signatúr analyzuje sieťovú komunikáciu a porovnáva ju so signatúrami známych útokov. Táto technika sa využíva na identifikáciu už známych signatúr útokov uložených v referenčnom modeli WIDS. Výzvy, ktorým čelia WIDS založené na detekcii signatúr, sú obtiažnosť zhromažďovania informácií o všetkých súčasných útokoch, ako aj potenciálne zlyhanie pri charakterizácii nových útokov alebo variáciách existujúcich. WIDS založené na detekcii signatúr majú teda problém pri detekcii nových alebo neznámych útokoch a tiež sú náchylné na falošne negatívnu identifikáciu útokov. [16] [17]

3.4.2 Detekcia na základe anomálií

Detekcia na základe anomálií predpokladá, že každá nežiaduca aktivita je vždy anomálna. Analyzuje prevádzku a identifikuje akúkoľvek odchýlku od vopred určeného

modelu bežnej a očakávanej prevádzky bezdrôtovej siete. Identifikuje anomálne správanie siete na základe historických ukazovateľov. Vďaka takejto identifikácii môžu byť objavené aj odchýlky, ktoré nemusia byť objavené inými technikami detekcie prienikov, čiže oproti analýze signatúr dokáže rozpoznať aj nové útoky, ako aj variácie už existujúcich útokov. Nevýhody tejto techniky sa prejavujú v nedostatku schopnosti detegovať útoky, ktoré nespôsobujú výrazné anomálie, ďalej v nesprávnej detekcii bežnej prevádzky, ktorá môže spôsobiť chvíľkovú anomáliu a v nedostatočnom rozpoznávaní typu delegovaných útokov. Preto sú WIDS založené na technike detekcie anomálií náchylné na veľké množstvo odhalenia falošne pozitívnych útokov. [16] [17]

3.5 Klasifikácia zariadení

Akékoľvek zariadenia založené na štandarde 802.11, ktoré komunikujú v pásme sledovanom senzormi sú detegovateľné. WIDS rozhodujú, o akú stanicu (prístupový bod, klientska stanica) sa jedná pomocou management rámcov, ktoré voľne vysielajú. Vo väčšine literatúr sa stretneme s kategorizáciou zariadení do štyroch základných skupín. [13]

3.5.1 Autorizované zariadenia

Autorizované zariadenia predstavujú všetky klientske stanice alebo prístupové body, ktoré sú členmi bezdrôtovej siete. Správca siete môže ručne označiť každú jednu rádiovú stanicu ako autorizované zariadenie siete alebo ich môže pridať automaticky pomocou importu MAC adries kariet všetkých zariadení, ktoré sa používajú na sieti.

3.5.2 Neautorizované zariadenia

Klasifikácia neautorizovaného zariadenia je priradená automaticky všetkým novým zariadeniam 802.11, ktoré boli detegované a nie sú klasifikované ako podvrhnuté zariadenia. Neznamená to, že zariadenia sú automaticky považované za neautorizované. Zvyčajne sú bližšie skúmané a zisťuje sa, či sa jedná o susedné zariadenia alebo potencionálnu hrozbu. Neskôr sa môžu manuálne klasifikovať na iný typ.

3.5.3 Susedné zariadenia

Susedné zariadenia sú všetky klientske stanice alebo prístupové body, ktoré senzor deteguje a ich identita je známa. Takéto označenie je manuálne priradené správcom siete. Sú to zariadenia, ktoré síce nepatria do danej siete, ale sú zariadeniami susedných sietí, ktorým správca dôveruje.

3.5.4 Rogue zariadenia

Rogue zariadenia sú prístupové body alebo klientske stanice, ktoré sú považované za rušiace zariadenia alebo potencionálnu hrozbu. Väčšina WIDS takéto zariadenia definuje ako tie, ktoré sú pripojené do siete a nie sú známe.

3.6 Stopovanie Rogue zariadení

Ako bolo spomenuté vyššie, na bezdrôtovej sieti sa nám nechcene môžu vyskytnúť aj zariadenia, ktoré môžu predstavovať potencionálnu hrozbu, preto je ich potrebné vyhľadať, odstrániť a následne zistiť, ako sa do uvedenej siete dostali a za akým účelom boli nainštalované. Na vystopovanie takýchto zariadení sa využíva niekoľko techník, ale väčšina z nich funguje na metóde RSSI(Received Signal Strengt Indicator), ktorá zisťuje silu prichádzajúceho signálu. [14]

3.6.1 Triangulácia RF

Triangulácia RF je najpoužívanejšia technika zistenia polohy bezdrôtového zariadenia využívajúca práve RSSI. Celý princíp je založený na tom, že v sieti existujú najmenej 3 senzory, ktoré majú pevnú polohu a sú zaznačené na mape. Práve k senzoru, kde je najvyššia hodnota RSSI sa najbližšie nachádza vyhľadávané zariadenie. Medián presnosti tejto techniky je 10 metrov.

3.6.2 RF odtlačok

RF odtlačok využíva databázu známych zariadení a ich RSSI a porovná ju s vyhľadávaným zariadením. Základným princípom fungovania RF odtlačku je, že v prípade, ak sa RSSI zhoduje zo známymi zariadeniami, je jednoznačné, že sa musí nachádzať blízko neho. Je presnejšia ako Triangulácia a dokáže znížiť veľkosť rozptylu z 10 na 2 až 1 meter.

3.6.3 Time Diference of Arrival (TDoA)

Ďalšou technikou na lokalizáciu zariadení je technika časového rozdielu príchodu. Využíva myšlienku časového príchodu rovnakého vysielaného signálu na tri alebo viac senzorov. Rýchlosť rádiových vĺn je známy fakt a každý zosynchronizovaný TDoA senzor hlási čas príchodu signálu. TDoA taktiež využíva uhol prichádzajúceho signálu (Angel of Arrival).

3.7 Limitácie WIDS

V zásade neexistujú žiadne bezpečnostné opatrenia, ktoré fungujú na 100% a vždy sa nájde nejaká slabosť, ktorú je možné využiť. Takýmto problémom trpia aj WIDS a majú hneď niekoľko limitácií. [16]

3.7.1 Falošné alerty

Jedným z najvýznamnejších problémov WIDS sú práve falošné alerty. Rozdeľujú sa do dvoch základných skupín, a to falošne negatívne a falošne pozitívne. Falošne negatívne alerty vznikajú, keď WIDS detekuje bežnú prevádzku na sieti ako útok a vytvorí falošný alert. Falošne pozitívne nastávajú vtedy, keď WIDS nedokáže detegovať útok a nevydá ani upozornenie, že nejaký útok na sieť prebieha. Najväčší problém WIDS je práve to, že bežná prevádzka sa veľmi neodlišuje od abnormálnej kvôli tomu, že topológia na sieti sa neustále mení, keďže zariadenia sú mobilné a môžu strácať konektivitu.

3.7.2 Redundantné alerty

Redundantné alerty nastávajú akonáhle WIDS označí veľké množstvo prevádzky za abnormálnu a generuje alert niekoľkokrát aj napriek tomu, že sa stále jedná o ten istý útok. To znemožní administrátorovi nájsť ten, ktorý je ozajstný. Daný problém sa dá vyriešiť správnym nastavením WIDS.

3.7.3 Slabá detekcia útokov

Aj napriek tomu, že WIDS má mechanizmus na rozpoznávanie útokov, veľmi často sa stáva, že nie je schopné ich správne detegovať, čo môže mať za následok kritické problémy.

3.7.4 Slabá bezpečnosť

Akonáhle WIDS využíva niekoľko senzorov komunikujúcich so serverom, môže nastať situácia, keď sa útočníkovi podarí túto komunikáciu znemožniť, čiže senzor nebude schopný odoslať nazbierané dáta serveru na to, aby ich spracoval. To vytvára útočníkovi možnosť sa dostať do siete bez toho, aby WIDS niečo zistilo, a tak môžu nastať vážne problémy.

II. PRAKTICKÁ ČÁST

4 NÁVRH

4.1 Úvod

Hlavným zadaním bakalárskej práce bol návrh systému pre detekciu narušiteľov v bezdrôtových sieťach, preto je praktická časť venovaná koncepčnému návrhu, ktorý je komponovaný tak, aby spĺňal potrebné zadané parametre. V nasledovnej časti bakalárskej práce sú popísané jednotlivé komponenty, software a hardware využité na vytvorenie systému, ktorý má mať schopnosť detekcie narušiteľov. Všetky využité technológie sú open-source, a preto si ich môže stiahnuť každý, kto by takýto systém potreboval využiť.

4.2 Návrh systému

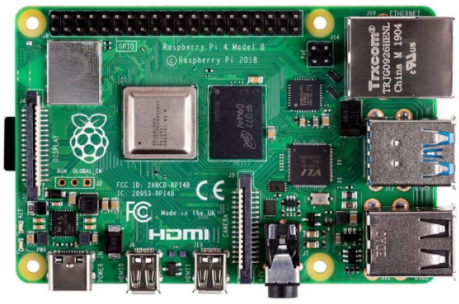
Návrh detekčného systému bol zameraný na to, aby nebol nákladný a využíval iba open-source nástroje, čiže aby nebolo potrebné platiť za žiadny software, ktorý detekciu narušiteľov umožňuje. Existuje niekoľko nástrojov, ktoré je možné využiť bezplatne a v niektorých prípadoch sú dokonca lepšie ako platené verzie. Jadro tohto systému bude tvoriť WIDS a NIDS, ktorý funguje na tom istom princípe len je pripojený priamo do siete. Funkcie a vlastnosti WIDS boli bližšie popísané v časti 3. Konkrétne sa bude jednať o nástroje `Kismet` a `Snort` nainštalované na operačnom systéme `Kali Linux`. Taktiež bolo pri návrhu systému pre detekciu narušiteľov myslené na to, že je potrebné, aby bežal na zariadení schopnom tento systém prevádzkovať neustále bez problémov, kvôli čomu bol vybraný práve Raspberry Pi 4 Model B, ktoré by malo byť schopné daný systém bezproblémovo zvládnuť. Ďalšou jeho nespornou výhodou je jeho veľkosť a mobilita. Na to, aby takýto systém vôbec fungoval bude potrebný aj špeciálny hardware schopný zachytávať všetku komunikáciu na bezdrôtovej sieti, čo znamená, že je potrebné využiť bezdrôtovú sieťovú kartu, ktorá dokáže pracovať v monitorovacom móde, a tak je schopná monitorovať prevádzku na sieti aj v okolí siete.

4.3 Hardware

4.3.1 Raspberry Pi 4 Model B

Celý navrhnutý systém pre detekciu narušiteľov bude bežať práve na Raspberry Pi 4 Model B. Jedná sa o miniatúrny počítač o veľkosti kreditnej karty, ktorý bol vyvinutý s cieľom poskytnúť plne funkčný výpočtový nástroj za nízku cenu. Raspberry Pi 4 je najnovší a najvýkonnejší počítač z dielne Raspberry Pi Foundantion a má byť schopný nahradiť desktopové počítače. Je vybavený procesorom Broadcom BCM2711 architektúry ARMv8, ktorý ma štyri jadrá a frekvenciu 1.8GHz. Vyrába sa v niekoľkých variantoch - 1 GB, 2 GB, 4GB, 8GB. V práci sa bude využívať verzia so 4 GB

LPDDR4 RAM, ktorá nebude mať žiadny problém s prevádzkovaním navrhnutého systému. Má dva porty USB 2.0 a dva porty USB 3.0, Bluetooth 5.0, výstup HDMI a slot na kartu micro SD (tá sa využíva ako pevný disk). Taktiež má bezdrôtovú sieťovú kartu podporujúcu frekvencie 2,4GHz a 5GHz aj Gigabit Ethernet kartu, ktoré budú potrebné pre implementáciu návrhu [18].



Obrázek 4.1 Raspberry Pi 4 Model B

4.3.2 Bezdrôtová sieťová karta RTL8812AU

Pre funkčnosť WIDS je potrebná bezdrôtová sieťová karta, ktorá dokáže poskytnúť využitie monitorovacieho módu potrebného pre monitorovanie celej prevádzky na sieti aj v jej okolí. Keďže integrovaná bezdrôtová sieťová karta v Raspberry Pi 4 nie je schopná monitorovacieho módu, treba využiť neintegrovanú s možnosťou takého využitia. Z tohto dôvodu sme začali vyhľadávať karty so schopnosťou využitia monitorovacieho módu, čo nás priviedlo ku kartám s chipsetom RTL8812AU, ktorého driver sa dá bezproblémovo nainštalovať na `Kali Linux` a je stále aktualizovaný. Taktiež je podporovaná aj vybraným WIDS, ktorým je Kismet[19]. Ďalšou výhodou je, že je ako jedna z mála schopná monitorovať vo všetkých pásmach a frekvenciách štandardu 802.11 a je tiež schopná aj `packet-injection` [20].

Obrázek 4.2 Raspberry Pi s pripojeným adaptérom RTL8812AU

4.4 Software

4.4.1 Kali Linux

Na to, aby sme mohli využívať navrhnutý systém je potrebný operačný systém. Keďže vybraným WIDS v našej práci je Kismet fungujúci iba na Linuxe, bolo potrebné vybrať vhodnú distribúciu. Pristúpili sme k výberu práve Kali Linux, na ktorom už je Kismet predinštalovaný a taktiež ma vytvorený image špeciálne pre Raspberry Pi, priamo určený na ARM procesory. Kali Linux je open-source operačný systém založený na Debanie, ktorý je vyvíjaný a financovaný spoločnosťou Offensive Security zaoberajúcou sa informatickou bezpečnosťou. Je špeciálne zameraný na pokročilé penetračné testovanie a bezpečnostné audity [26]. Poskytuje širokú ponuku bezpečnostných nástrojov, ktoré neskôr budeme používať na testovanie navrhnutého systému.

4.4.2 Kismet

Základným prvkom detekčného systému bude práve Kismet, ktorý zodpovedá za detekciu a tvorbu upozornení o prípadných narušiteľoch. Kismet je open-source bezdrôtový sieťový analyzátor fungujúci v operačnom systéme Linux. Je pasívnym skenerom, ktorý sa používa na detekciu bezdrôtových sietí. Dokáže objaviť aj skryté siete a funguje na druhej vrstve OSI. Na to, aby získaval informácie o všetkých sieťach, neustále preskakuje medzi kanálmi 802.11. Jednou z možností, ako sa dá využiť, je práve WIDS [20]. K využitiu Kismetu je potrebný taký adaptér, ktorý pracuje s monitor-mode a uvedie bezdrôtovú sieťovú kartu do stavu, aby dokázala monitorovať všetku prevádzku. Monitor-mode, narozdiel od promiskuitného módu, sa nepotrebuje asociovať so žiadnym prístupovým bodom. Skladá sa z niekoľkých komponentov, ako každé WIDS.

- **Kismet drone:** funguje na princípe senzora, alebo agenta, odpočúvajúceho všetku komunikáciu a následne ju odosiela na server. Je možné ho nainštalovať na hocijaké zariadenie s operačným systémom Linux, ktoré má bezdrôtovú sieťovú kartu schopnú monitorovacieho módu. Všetky jeho nastavenia sa nachádzajú v konfiguračnom súbore `kismet_drone.conf` [22].

- **Kismet server:** spracováva všetky informácie a dáta, ktoré sú mu odosielané z pripojených dronov a následne ich vyhodnocuje. Tak isto aj on môže fungovať ako drone, ak sa na ňom nachádza bezdrôtová sieťová karta podporujúca monitorovací mód. Ak má už zmienenú kartu, nie je nutné, aby využíval drony, ale môže fungovať aj samostatne. Všetky jeho nastavenia vieme nájsť v konfiguračnom súbore `kismet.conf` [22].

- **Kismet klient:** slúži ako rozhranie a jeho hlavnou úlohou je prehľadne zobrazovať informácie, ktoré mu odosiela server. Nenastavuje sa pomocou žiadneho

konfiguračného súboru, ale pomocou rozhrania [23].

Alert Ak chceme využívať Kismet ako WIDS, potrebujeme, aby bol schopný informovať nás o možných útokoch alebo problémoch na sieti. Sú to tzv. alerty, ktoré umožňujú, aby WIDS na niečo také dokázal upozorňovať. Alerty je možné konfigurovať pomocou `alert=` v konfiguračnom súbore `kismet_alerts.conf`. Sú konfigurované menom alertu a parametrami `throttle`, ktorý určuje, koľko alertov sa môže vytvoriť za určitý čas (sekundy,minúty) a `burst`, ktorý zase určuje, koľko je potrebných alertov pre rýchle nasledovanie. Všetky alerty sú uvedené na odkaze [23].

4.4.3 Snort

Keďže Kismet funguje iba pasívne a nie je pripojený priamo na sieť, je potrebné využiť aj NIDS (Network Intrusion Detection System), ktorý je priamo pripojený na sieť a dokáže na nej monitorovať prevádzku. Problém pri využití samotného WIDS by nastal akonáhle by sa narušiteľovi podarilo pripojiť do siete bez detekcie narušenia a začal by vytvárať útoky priamo na nej. Preto bude využitý aj Snort, ktorý je schopný detegovať útoky prebiehajúce už priamo na sieti, a to pomocou karty v promiskuitnom móde. Snort je open-source NIDS vyvíjaný firmou Cisco, schopný analyzovať sieťovú prevádzku v reálnom čase [27]. Tak isto ako Kismet využíva alerty, ktoré sa nastavujú pomocou `rules` v konfiguračnom súbore `snort.conf`, kde sa nachádza niekoľko predinštalovaných `rules` vytvorených komunitou, z ktorých je možné vybrať tie, ktoré budú zapnuté.

Rules Veľmi dôležitou časťou Snort sú rules. Jedná sa o pravidlá, ktorými sa Snort riadi pri detekcii útokov. Závisí od nich schopnosť detekcie a pri zlom nastavení môžu spôsobiť zahltenie alebo dokonca nefunkčnosť. Tieto pravidlá nie je jednoduché vytvoriť a je potrebné presne vedieť, ako daný útok funguje. Každé z týchto `rules` sa skladá z hlavičky a tela, ktoré môžme vidieť v obecnom formáte [28].

```
akcia protokol IP_zdroj port_zdroj smer IP_ciel port_ciel (telo)
```

- **Akcia:** Definuje, akým spôsobom sa má Snort zachovať, keď nájde paket zodpovedajúci pravidlu.
- **Protokol:** Protokol, ktorý má Snort zanalyzovať. V súčasnosti podporuje štyri protokoly - TCP, UDP, ICMP, a IP.
- **IP_zdroj:** Zdrojová IP adresa, odkiaľ prichádza komunikácia.
- **Port_zdroj:** Zdrojový port, z ktorého prichádza komunikácia.

- **Smer:** Smer, ktorým komunikácia prebieha. Určuje sa operátormi `->` a `<-`.
- **IP_cieľ:** Cieľová adresa, kam komunikácia smeruje.
- **Port_cieľ:** Cieľový port, na ktorý prichádza komunikácia.

5 IMPLEMENTÁCIA

5.1 Úvod

Nasledujúca kapitola sa zaoberá implementáciou návrhu systému na detekciu narušiteľov. Sú v nej podrobne popísané jednotlivé kroky priebehu implementácie, aké problémy pri implementácii tohoto systému nastali a spôsoby riešenia daných problémov. V kapitole taktiež detailnejšie popisujeme konfiguráciu a nastavenia jednotlivých komponentov nachádzajúcich sa v systéme.

5.2 Inštalácia Kali Linux na Raspberry Pi

Ako už bolo uvedené vyššie, na to, aby nám vybraný WIDS Kismet fungoval, je nutná inštalácia Kali Linux, ktorý je už v tejto distribúcii predinštalovaný. Prvým potrebným krokom je teda nainštalovanie Kali Linux na Raspberry Pi. Keďže Raspberry Pi využíva ARM architektúru, je potrebný špeciálny image, ktorý je na ňu určený. Tento image je možné stiahnuť priamo zo stránky Offensive Security [24]. Ak chceme dostať Kali Linux na Raspberry Pi, je nutné image nainštalovať na microSD kartu, ktorá bude fungovať ako pevný disk. K tomu poslúži nastroj `Raspberry Pi Imager`, ktorý ho na kartu nainštaluje. Potom stačí už len vložiť microSD kartu do Raspberry Pi.

Obrázek 5.1 Raspberry Pi Imager

5.3 Konfigurácia Kali Linux

5.3.1 Základné nastavenie

Po inštalácii Kali Linux je na Raspberry Pi potrebné pripojiť monitor, klávesnicu a myšku a následne ho môžme nakonfigurovať. Ďalším krokom je pripojenie Raspberry Pi do siete, aby sme ho neskôr dokázali využívať vzdialene a nemuseli vždy zapájať periférie. Najjednoduchším spôsobom je nastaviť aby sa automaticky pripájal na Wi-Fi sieť. Na to treba upraviť súbor `/etc/network/interfaces` na nastavenie automatického pripojenia, a to pridaním týchto nastavení:

```
auto wlan0
allow-hotplug wlan0
iface wlan0 inet dhcp
wpa-conf /etc/wpa_supplicant/wpa_supplicant.conf
iface default inet dhcp
```

Taktiež je nutné nastaviť súbor `/etc/wpa_supplicant/wpa_supplicant.conf`, v ktorom sa nachádzajú údaje o bezdrôtovej sieti, na ktorú sa má Raspberry Pi pripojiť.

```
network={
ssid="WiFi"
psk="heslo"
proto=RSN
key_mgmt=WPA-PSK
pairwise=CCMP
auth_alg=OPEN
}
```

Následne je potrebné umožniť vzdialene ovládať Raspberry Pi. Na to by pokojne stačilo SSH, ale nakoľko Kismet má výborný web interface, rozhodli sme sa použiť nástroj XRDP, ktorý umožňuje pripojiť sa na Linux zariadenia cez protokol RDP (Remote Desktop Protokol) a zabezpečuje zdieľanie grafického rozhrania.

```
# apt-get install xrdp
# service xrdp start
# service xrdp-sesman start
# update-rc.d xrdp enable
```

Nakoniec už iba stačí otvoriť klient, ktorý využíva RDP a zadaním IP adresy a prihlasovacích údajov sa dostaneme do grafického rozhrania Kali Linux zo vzdialeného počítača.

5.3.2 Konfigurácia bezdrôtovej sieťovej karty

K využívaniu monitor-mode na karte RTL8812AU je potrebné nainštalovať upravený ovládač, ktorý je toho schopný. Existuje niekoľko druhov ovládačov na danú kartu. V našom prípade sme však zvolili ten, ktorý je vytvorený aircrack-ng. Predtým, ako sa nainštaluje samotný ovládač, je potrebné aktualizovať niekoľko dôležitých vecí. Najskôr treba aktualizovať všetky balíčky nachádzajúce sa v Kali Linux, a to pomocou príkazu `apt dist-upgrade`. Na to, aby bolo možné driver skompilovať, je potrebné nainštalovať `Linux-headers`, pretože ovládač bude pracovať s hlavičkami kernelu.

```
# apt-get install raspberrypi-kernel-headers build-essential
# apt-get install kalipi-kernel-headers build-essential
```

V ďalšom kroku je treba stiahnuť už zmieňovaný ovládač, ktorý jednoducho naklonujeme z Githubu aircrack-ng príkazom

```
git clone https://github.com/aircrack-ng/rtl8812au
```

Ako bolo spomenuté vyššie, tento ovládač je potrebné skompilovať. Najskôr je však nutné nainštalovať nástroj `dkms` zaisťujúci podporu inštalácie pre moduly kernelu [24]. Po kompilácii bude treba reštartovať operačný systém.

```
# apt-get install dkms
# make dkms_install
# reboot
```

Ak chceme začať kartu využívať v `monitor-mode`, musíme ešte túto možnosť zapnúť, a to pomocou príkazu `airmon-ng start wlan1`. Ten zapne `monitor-mode` na `wlan1`, ktorá je naša vybraná karta.

5.4 Implementácia Kismet

5.4.1 Konfigurácia

Po tom, ako sa podarilo nainštalovať ovládače na bezdrôtovú sieťovú kartu a je možné ju spustiť v `monitor-mode`, prichádza na rad samotný WIDS `Kismet`. Ten ani nie je nutné inštalovať, keďže je v Kali Linux v základnom balíčku. Pred prvým spustením je ho však potrebné nastaviť v konfiguračnom súbore `kismet.conf`. Najskôr si musíme určiť zdroj, ktorým bude práve bezdrôtová sieťová karta, a to pomocou `source=interface` . V našom prípade je interface práve `wlan1`, ktorý je karta RTL8812AU. Ak chceme, aby Kismet skenoval na všetkých kanáloch, je nutné nastaviť `channel_hop=true`. V prípade, že by sme chceli zvoliť odpočúvanie iba jedného kanálu, tak nastavíme parameter na `false`, vyberieme si kanál pomocou `channel=` a zadáme číslo kanálu. Ak skenujeme viac kanálov, je potrebné aj nastaviť, ako často bude Kismet medzi nimi preskakovať, a to pomocou `channel_hop_speed=time/sec`, kde môžeme nastaviť čas buď v `sec`, alebo `min`. Ďalšou možnosťou je `randomized_hopping=true`, ktorá umožňuje náhodne vyberať skenované kanály. Naše nastavenia teda vyzerajú nasledovne:

```
source=wlan1
channel_hop=true
channel_hop_speed=10/sec
randomized_hopping=true
```

Ako sme spomenuli v časti 4.4.2, Kismet využíva alerty a tie je potrebné vhodne nastaviť, aby nám nevznikali redundantné alerty, bližšie popísané v 3.7.2. Nastavenia alertov sa nachádzajú práve v konfiguračnom súbore `kismet_alerts.conf`, ktorý je opäť potrebné pred spustením nastaviť. Ako bolo uvedené vyššie, existuje niekoľko desiatok alertov, avšak nie je potrebné nastavovať všetky. Zamerali sme sa iba na tie, ktoré sú využívané pri testovaní.

- `apspoof` - nejedná sa priamo o alert, ale o nastavenie známych zariadení. Zadávajú sa do neho prístupové body, ktoré poznáme a ich MAC adresa. Dokáže jednoducho odhaliť Evil Twin attack vďaka tomu, že pozná MAC adresu autorizovaných prístupových bodov.
- `DEAUTHFLOOD` - využíva sa na detekciu DoS útoku, ktorý väčšinou býva predvoj

iných útokov, ako Man-In-The-Middle. Tento alert je priamo zameraný na typ útoku, kedy sa útok vykonáva zahltením siete deauthentication rámcami.

- `CRYPTODROP` – alert slúžiaci na detekciu útoku Evil Twin, zapne sa akonáhle stanica zmení svoje šifrovanie na horšie, čo by sa bežne nemalo stať.
- `ADVCRYPTCHANGE` - alert určený na detekciu prístupových bodov, ktoré z ničoho nič zmenia svoje zabezpečenie, čo môže naznačovať pokúšanie sa o vytvorenie útoku Evil Twin.
- `NONCEREUSE` - taktiež alert slúžiaci na detekciu útoku voči šifrovaniu, ale tentokrát útoku KRACK. Snaží sa detegovať handshake, ktorý sa pokúša využiť znova to isté nonce. Opäť je predvolene vypnutý pre obtiažnu detekciu a časté vytváranie falošne pozitívnych alertov.

Konfigurácia upravených alertov bude teda vyzerať nasledovne:

```
apspoof=Test:ssid="F8:1A:67:EB:9B:AE",validmacs="F8:1A:67:EB:9B:AE"
alert=DEAUTHFLOOD,5/min,2/sec
alert=CRYPTODROP,5/min,1/sec
alert=ADVCRYPTCHANGE,5/min,1/sec
alert=NONCEREUSE,5/min,1/sec
```

5.4.2 Spustenie

Po konfigurácii Kismet je potrebné pristúpiť k ďalšiemu kroku, a tým je spustenie. Kismet je možné zapnúť dvoma rôznymi spôsobmi, a to buď ako service, alebo jednoducho ho spustiť cez konzolu, ako aplikáciu. WIDS potrebuje, kvôli čo najlepším výsledkom, neustále skenovanie, preto by malo bežať stále a zapínať sa automaticky. Z toho vyplýva, že Kismet využijeme ako service bežiaci na pozadí a bude sa spúšťať priamo pri spustení Kali Linux. Na spustenie Kismet ako service je najskôr potrebné stiahnuť alebo vytvoriť súbor `kismet.service`, ktorý sa bude využívať na spustenie `systemd service`. Stiahnuť ho je možné z Github Kismet, kde sa nachádza ukážkový súbor. V ňom stačí prepísať používateľa, ktorý bude daný service využívať.

```
# cd /lib/systemd/system/
# curl https://raw.githubusercontent.com/kismetwireless/kismet/master/
  packaging/systemd/kismet.service.in --output filename kismet.service
# sudo systemctl edit kismet
```

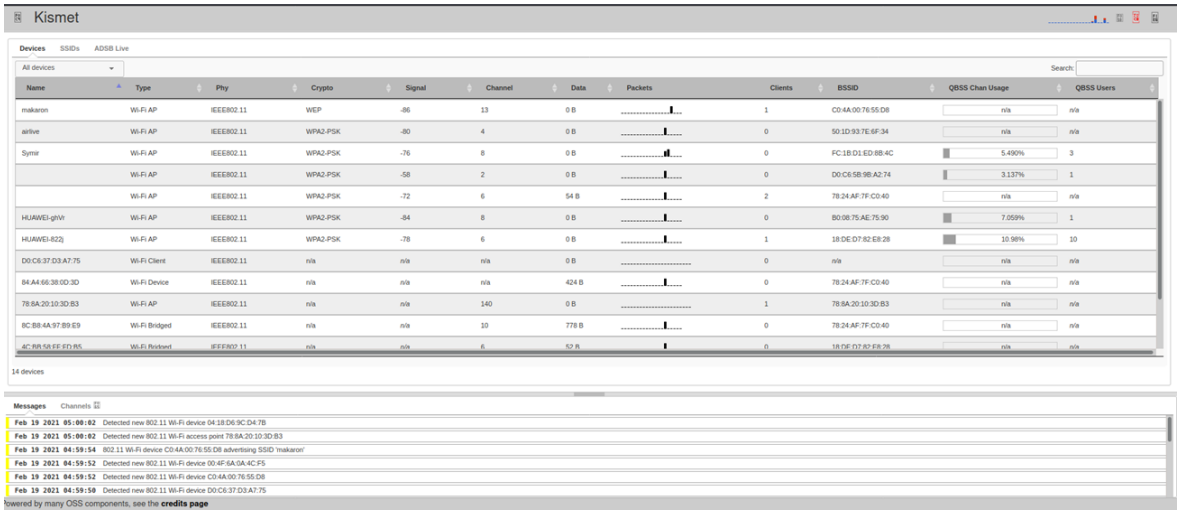
Keďže využívame Kali Linux, prepíšeme používateľa na `kali` a skupinu ponecháme `kismet`.

```
[Service]
 User=kali
 Group=kismet
```

Následne stačí už iba Kismet service spustiť a nastaviť ho na automatické zapnutie pri štarte.

```
# sudo service kismet start
# sudo systemctl enable kismet
```

Po spustení nasmerujeme prehliadač na stránku `http://localhost:2501`, ktorá obsahuje webové rozhranie nástroju Kismet slúžiace na zobrazovanie všetkých naskenovaných staníc, konfiguráciu a samotné alerty WIDS.



Obrázek 5.2 Webové rozhranie nástroju Kismet

5.5 Implementácia Snort

5.5.1 Inštalácia

Snort sa na rozdiel od Kismet nenachádza v základom balíku Kali Linux, a preto je najskôr potrebné ho nainštalovať. Inštalácia nie je zložitá, pretože aj keď nie je základnou súčasťou Kali Linux, nachádza sa v jeho repozitári aplikácií. Postačí iba využiť príkaz `apt install snort`, ktorý Snort stiahne aj s ďalšími nástrojmi potrebnými na jeho fungovanie.

5.5.2 Konfigurácia

Ďalším krokom po inštalácii je nastaviť samotný Snort, a to v konfiguračnom súbore `snorf.conf`. Najskôr treba nastaviť IP adresu subsiete, pomocou `ipvar HOME_NET 192.168.1.0/24`. Následne, pre správne fungovanie systému, je potrebné nastaviť už spomínané `rules`, ktoré sa budú využívať. Najskôr treba zadať cestu, kde sa `rules` súbory nachádzajú a to pomocou `var RULE_PATH /etc/snort/rules`. Netreba vytvárať nové `rules` ani ich nijako nastavovať, pretože sú dostupné komunitné, ktoré sa stiahli pri inštalácii a pre naše potreby úplne stačia. Jediné, čo treba spraviť je od komentovať

tie, ktoré sa budú využívať.

```
include $RULE_PATH/attack-response.rules
include $RULE_PATH/backdoor.rules
include $RULE_PATH/bad-traffic.rules
include $RULE_PATH/dns.rules
include $RULE_PATH/dos.rules
include $RULE_PATH/exploit.rules
include $RULE_PATH/finger.rules
include $RULE_PATH/scan.rules
include $RULE_PATH/snmp.rules
include $RULE_PATH/icmp.rules
```

5.5.3 Spustenie

Tak isto ako WIDS Kismet, tak aj Snort je potrebné pre najlepšie výsledky mať spustený neustále, a to znova pomocou `systemd service`, ktorý umožní automatické zapnutie pri štarte a bežanie na pozadí. Tentoraz však nie je možnosť stiahnutia ukážkového súboru, ktorý stačí prepísať, ale je nutnosť ho vytvoriť a nastaviť.

```
nano /lib/systemd/system/snort.service
```

Do tohto súboru je nutné vpísať nastavenia, ako sa má Snort zapnúť a nastaviť pomocou parametru `-c` konfiguračný súbor a parametru -i interface, na ktorom bude prebiehať odpočúvanie.

```
[Unit]
 Description=Snort Service
 After=syslog.target network.target
[Service]
 Type=simple
 ExecStart=/usr/local/bin/snort -q -c /etc/snort/snort.conf -i eth0
[Install]
 WantedBy=multi-user.target
```

Následne už stačí iba povoliť service na spustenie pri štarte a zapnúť ho.

```
systemctl enable snort
systemctl start snort
```

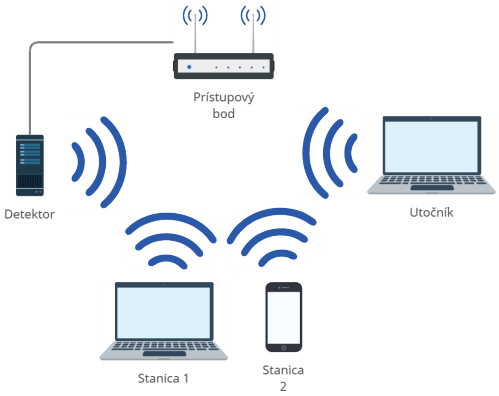
6 TESTOVANIE

6.1 Úvod

Funkčnosť každého navrhnutého riešenia je potrebné aj overiť. Preto sa táto kapitola zaoberá samotným testovaním navrhnutého systému pre detekciu narušiteľov. Cieľom testovania je určiť, či je daný systém možné využívať v reálnom živote a je schopný zachytiť útoky voči bezdrôtovým sieťam.

6.2 Testovacie prostredie

Keďže je potrebné uskutočniť útoky na bezdrôtovú sieť, ktoré budú mať za následok závažné problémy s pripojením, komunikáciou a bezpečnosťou, nie je možné využiť pre testovanie bežnú bezdrôtovú sieť, na ktorej prebieha prevádzka. Musíme vytvoriť testovacie prostredie, v ktorom sa tieto útoky budú odohrávať a budú v ňom využité iba zariadenia určené práve na testovanie. Testovacie prostredie bude pozostávať zo 4 základných prvkov - prístupový bod, stanica 1, stanica 2, systém pre detekciu narušiteľov a v neposlednom rade, narušiteľ. Každý z týchto prvkov zohráva pri testovaní určitú úlohu. Tieto zariadenia budú úplne odlúčené od bežnej siete, aby na nej nedošlo k problémom.



Obrázek 6.1 Testovacie prostredie

- **Prístupový bod:** Wi-Fi router TL-WR1042ND zodpovedný za prevádzku na sieti.
- **Detekčný systém:** Raspberry Pi, na ktorom beží Kali Linux, WIDS Kismet a IDS Snort pre detekciu narušiteľov.
- **Stanica 1:** notebook s operačným systémom Windows 10 komunikujúci s prístupovým bodom.

- **Stanica 2:** mobilný telefón s operačným systémom Android 10 komunikujúci s prístupovým bodom.
- **Útočník:** stanica, na ktorej beží Kali Linux a bude pracovať ako narušiteľ.

6.3 Útočník

Pre testovanie navrhnutého riešenia je nutné využiť špeciálny hardware aj software, ktorým útočník napadne bezdrôtovú sieť. Ako bolo uvedené vyššie, stanica útočníka bude fungovať na operačnom systéme Kali Linux, bližšie popísanom v 4.4.1, pretože už v základnom balíku ponúka množstvo predinštalovaných nástrojov na penetračné testovanie bezdrôtových sietí a nie je nutné ich sťahovať a inštalovať. Na to, aby sme na bezdrôtové siete mohli útočiť, bude znovu potrebný adaptér, ktorý je schopný `monitor-mode` aj `packet-injection`. V tomto prípade je využitá bezdrôtová sieťová karta s čipsetom RT5370 podporujúcim obidve funkcie. Dokonca nie je nutné inštalovať ani externý ovládač, pretože táto karta je podporovaná. Jediným problémom uvedenej karty je, že funguje iba na 2.4GHz a nie je tak silná ako karta využitá v detekčnom systéme.

6.4 Testovanie

V úvode bolo spomenuté, že táto kapitola sa venuje testovaniu navrhnutého riešenia. Testovanie systému pre detekciu narušiteľov bude prebiehať tým spôsobom, že útočník sa bude snažiť útočiť na testovaciu sieť s názvom `Test`, ktorá bude pre každý útok špecificky nastavená, aby bolo možné vyskúšať útoky rôzneho druhu a úlohou navrhnutého systému bude útoky detegovať. Výsledkom testov bude zistenie schopnosti detekcie útokov a prienikov navrhnutým systémom.

6.5 Skenovanie

6.5.1 Návrh testu

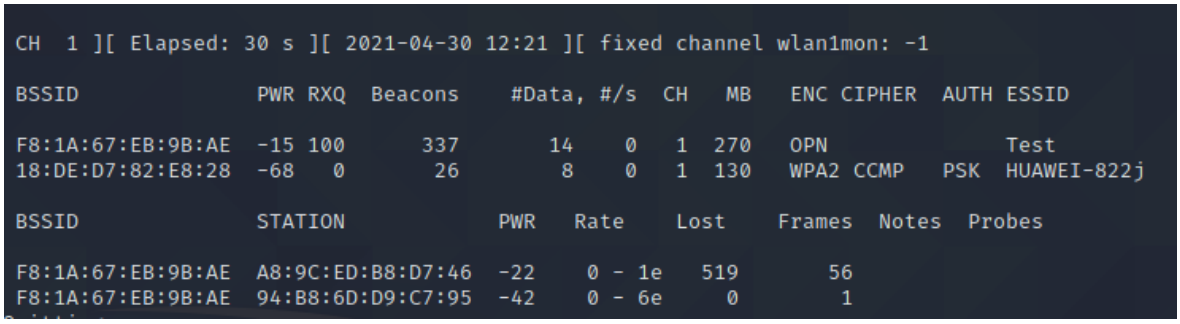
Nasledovný test má za úlohu zistiť, do akej miery dokáže navrhnutý systém detegovať skenery. Pre správne otestovanie systému sa využijú dva nástroje schopné skenovať, a to `airodump-ng` a `Kismet`. Obidva fungujú iba ako pasívne skenery. Test prebehne tak, že *Útočník* zapne skener v dosahu systému a bude skenovať. Úlohou systému bude zistiť, že skenovanie prebieha.

6.5.2 Test

Najskôr sa využije práve `airodump-ng`, ktorý nemá grafické rozhranie.

```
# airmon-ng start wlan1
# airodump-ng wlan1mon
```

Výstupom tohto nástroja je nasledujúca tabuľka prístupových bodov a pripojených zariadení.



Obrázek 6.2 Airodump-ng

Použije sa aj nástroj Kismet, ktorého rozhranie je možné vidieť na 4.4.2. Tenkokrát bude spustený iba ako aplikácia a nie service, a to príkazom `kismet -c wlan1mon`.

6.5.3 Výsledok

Navrhnutý systém nebol schopný zistiť, že prebieha skenovanie ani pri jednom z využitých nástrojov, a to aj napriek viacerým pokusom skenovania, čo je spôsobené tým, že obidva tieto sieťové skeneri pracujú pasívne.

6.6 Slovníkový útok na WPA2

6.6.1 Návrh testu

Tento test má za úlohu zistiť, či je navrhnutý systém schopný detekcie snifferov. Počas testu sa bude *Stanica 1* snažiť pripojiť na sieť `Test` nastavenú so zabezpečením WPA2-PSK a jednoduchým heslom `password`. Cieľom narušiteľa bude zachytiť 4-way handshake, a to pomocou nástroja `airodump-ng` a následne zistiť kľúč pomocou nástroja `aircrack-ng` a slovníku. Tento 4-way handshake sa vytvorí počas toho, ako sa itStanica 1 bude na sieť `Test` pripájať.

6.6.2 Test

Stačí poznať BSSID a kanál siete zistené v predošlom teste a následne zapnúť nástroj `airodump-ng`, ktorý bude odpočúvať.

```
# airodump-ng wlan1mon -c 1 --bssid F8:1A:67:EB:9B:AE -w test/wpacrack
```

Akonáhle sa *Stanica 1* začne pripájať na sieť `Test`, podarí sa získať 4-way handshake a potom už iba stačí využiť slovník a nástroj `aircrack-ng`, ktorému zadáme cestu k zachytenému handshake a slovníku.

```
CH  1 ][ Elapsed: 48 s ][ 2021-05-04 13:03 ][ WPA handshake: F8:1A:67:EB:9B:AE

BSSID              PWR RXQ  Beacons    #Data, #/s  CH   MB   ENC CIPHER  AUTH ESSID

F8:1A:67:EB:9B:AE  -40 100      507       17    3   1  270   WPA2 CCMP   PSK  Test

BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes

F8:1A:67:EB:9B:AE  A8:9C:ED:B8:D7:46  -42    1e- 1e    80       30  EAPOL  Test
```

Obrázek 6.3 Airodump-ng

```
# sudo aircrack-ng wpacrack-01.cap -w /usr/share/wordlists/rockyou.txt
```

V momente, keď sa nástroju `aircrack-ng` podarí nájsť kľúč, vráti výstup, v ktorom ho zobrazí.

```
                          Aircrack-ng 1.6

[00:00:00] 12/10303727 keys tested (112.64 k/s)

Time left: 1 day, 1 hour, 24 minutes, 33 seconds                0.00%

                         KEY FOUND! [ password ]


Master Key     : 04 22 1A 7D 2B B5 2B 87 08 D9 6E A2 F5 AC 3E 0F
                 E2 60 9A 34 DD FC 16 A3 C9 F4 64 D2 F5 A7 85 0D

Transient Key  : BF C6 51 CA 9E 83 0C 23 B8 F8 95 EF 7A 5D 46 96
                 19 74 DB 95 2F 69 D3 72 0B 4B 93 D7 2E 41 42 37
                 65 F2 BA 45 CA 46 16 68 20 3B 50 7E D0 53 A5 8E
                 FD 80 74 A3 52 BD 6E D7 90 F9 88 D1 2F 00 F6 9F

EAPOL HMAC     : 0C BD 3D 4E EA 20 DD CE C3 A2 92 EE FE 5C 3C 75
```

Obrázek 6.4 Aircrack-ng

6.6.3 Výsledok

Navrhnutý systém nebol schopný detegovať prebiehajúci sniffing, nakoľko sa znovu jednalo len o pasívny útok.

6.7 Deauthentication útok

6.7.1 Návrh testu

Úlohou ďalšieho testu bude zistiť, či je navrhnutým systémom možné detegovať Deauthentication útok. Test prebehne tak, že na prístupový bod, na ktorom je sieť `Test` bude pripojená *Stanica 2* a tá s ním bude komunikovať. Narušiteľ sa bude snažiť zariadenie *Stanica 2* nedobrovoľne odpojiť pomocou DoS útoku a využije naň podvrhnuté deauthentication rámce, v ktorých sa bude vydávať za zariadenie *Stanica 2* a bude ich odosielať na prístupový bod. Tento prístupový bod si následne bude myslieť, že *Stanica 2* sa snaží zo siete `Test` odpojiť, a preto zariadenie odpojí.

6.7.2 Test

Na vytvorenie tohto útoku znova stačí poznať len BSSID siete `Test` a zariadenia *Stanica 2*. Využije sa nástroj `aireplay-ng`, ktorý slúži na vytváranie falošnej komunikácie na sieti. Deauthentication útok nastavíme pomocou parametra `-0`.

```
# sudo aireplay-ng -0 0 -a F8:1A:67:EB:9B:AE
  -c A8:9C:ED:B8:D7:46 wlan1mon
```

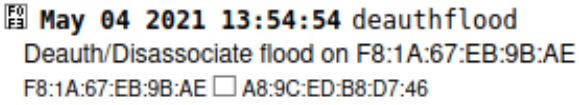
Po zapnutí sa zobrazí, ako sa odosielajú deauthentication rámce.

```
13:54:50  Waiting for beacon frame (BSSID: F8:1A:67:EB:9B:AE) on channel -1
13:54:51  Sending 64 directed DeAuth (code 7). STMAC: [A8:9C:ED:B8:D7:46] [ 0|61 ACKs]
13:54:52  Sending 64 directed DeAuth (code 7). STMAC: [A8:9C:ED:B8:D7:46] [ 0|60 ACKs]
13:54:52  Sending 64 directed DeAuth (code 7). STMAC: [A8:9C:ED:B8:D7:46] [ 0|61 ACKs]
13:54:53  Sending 64 directed DeAuth (code 7). STMAC: [A8:9C:ED:B8:D7:46] [ 2|64 ACKs]
13:54:53  Sending 64 directed DeAuth (code 7). STMAC: [A8:9C:ED:B8:D7:46] [12|47 ACKs]
```

Obrázek 6.5 Aircrack-ng

6.7.3 Výsledok

Navrhnutý systém bol schopný detegovať tenko útok za veľmi krátky čas, a to pomocou Kismet alertu `DEAUTHFLOOD`, ako je vidieť na obrázku nižšie.



Obrázek 6.6 Kismet alert DEAUTHFLOOD

6.8 Evil Twin útok

6.8.1 Návrh testu

Úlohou tohto testu bude opäť overenie systému, tentokrát, či je schopný detegovať útok Evil Twin. Počas testu budú na sieť `Test` pripojené zariadenia *Stanica 1* a *Stanica 2*. Úlohou útočníka bude vytvoriť kópiu siete `Test` a prebrať tieto zariadenia na jeho okopírovanú sieť. Po vytvorení kópie tejto siete sa útočník bude pokúšať odpojiť zariadenia *Stanica 1* a *Stanica 2* z originálnej siete na jeho okopírovanú sieť a to znova využitím Deauthentication útoku.

6.8.2 Test

Ako pri všetkých doterajších testoch, tak aj pri tomto treba poznať BSSID a taktiež aj ESSID, aby sme mohli vytvoriť kópiu siete. Tá sa jednoducho vytvorí pomocou nástroja `airbase-ng`, ktorý je určený na útoky voči klientom a prístupovým bodom.

```
# sudo airbase-ng -a F8:1A:67:EB:9B:AE --essid Test -c 1 wlan1mon
```

Po použití príkazu môžme vidieť, že sa podarilo vytvoriť kópiu siete `Test`.

```
13:30:37  Created tap interface at0
13:30:37  Trying to set MTU on at0 to 1500
13:30:37  Trying to set MTU on wlan1mon to 1800
13:30:37  Access Point with BSSID F8:1A:67:EB:9B:AE started.
```

Obrázek 6.7 Airbase-ng

Teraz treba opäť využiť nástroj `aireplay-ng`, podobne ako v predošlom teste na vytvorenie Deauthentication útoku.

```
# sudo aireplay-ng -0 0 -a F8:1A:67:EB:9B:AE
  -c A8:9C:ED:B8:D7:46 wlan1mon
```

Po tom, ako sa podarí odpojiť zariadenia *Stanica 2* pomocou Deauthentication útoku od originálnej siete `Test`, zobrazí nám nástroj `airbase-ng`, že sa na okopírovaný prístupový bod napája práve *Stanica 2*. Tento istý postup by sa využil aj na únos zariadenia *Stanica 1*.

```
13:42:41  Client A8:9C:ED:B8:D7:46 associated (unencrypted) to ESSID: "Test"
```

Obrázek 6.8 Airbase-ng

6.8.3 Výsledok

Navrhnutý systém bol schopný detegovať útok Evil Twin skoro instantne, a to pomocou hneď niekoľkých Kismet alertov `APSPOOF`, `CRYPTODROP`, `DOT11D`, `ADVCRYPTCHANGE`, ako je vidieť na obrázku nižšie. Nie je teda ani nutnosť manuálne nastavovať alert `APSPOOF` pre každé autorizované zariadenie, pretože Kismet má aj ďalšie alerty, ktoré vedia rozpoznať útok Evil Twin.

May 05 2021 13:30:40 advcryptchange
IEEE80211 Access Point BSSID F8:1A:67:EB:9B:AE SSID "Test" changed advertised encryption from none to WPA2 WPA2-PSK AES-CCMP which may indicate AP spoofing/impersonation
F8:1A:67:EB:9B:AE ☐ FF:FF:FF:FF:FF:FF

May 05 2021 13:30:40 cryptodrop
IEEE80211 Access Point BSSID F8:1A:67:EB:9B:AE SSID "Test" changed advertised encryption from WPA2 WPA2-PSK AES-CCMP to Open which may indicate AP spoofing/impersonation
F8:1A:67:EB:9B:AE ☐ FF:FF:FF:FF:FF:FF

May 05 2021 13:30:40 dot11d
IEEE80211 Access Point BSSID F8:1A:67:EB:9B:AE SSID "Test" advertised conflicting 802.11d information which may indicate AP spoofing/impersonation
F8:1A:67:EB:9B:AE ☐ FF:FF:FF:FF:FF:FF

May 05 2021 13:30:40 apspoof
IEEE80211 Unauthorized device (1C:BF:CE:4D:65:46) advertising for SSID 'Test', matching APSPOOF rule Test which may indicate spoofing or impersonation.
1C:BF:CE:4D:65:46 ☐ FF:FF:FF:FF:FF:FF

Obrázek 6.9 Kismet detekcia útoku Evil Twin

6.9 ARP Poisoning

6.9.1 Návrh testu

Test má za úlohu preveriť schopnosť navrhnutého systému na detekciu útoku ARP Poisoning. Test bude opäť prebiehať na sieti `Test`, na ktorú bude tentokrát priamo

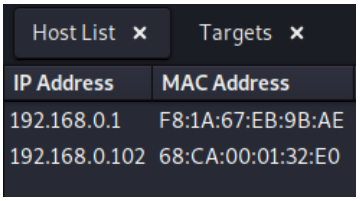
pripojený aj útočník. Cieľom útočníka bude zmeniť ARP tabuľku zariadenia *Stanica 1* tak, aby si myslelo, že zariadenie útočníka je default gateway.

6.9.2 Test

Na vytvorenie útoku ARP Poisoning bude využitý `Ettercap`. Je to nástroj využívajúci sa na vytváranie útokov Man-In-The-Middle. Nástroj je možné spustiť v grafickom rozhraní, a to pomocou parametru `-G`.

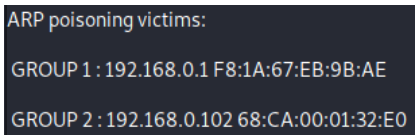
```
# ettercap -G
```

Po spustení nástroja si vyberieme interface wlan1 a spustíme skenovanie siete.



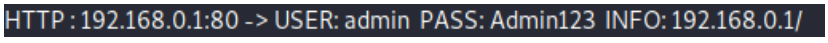
Obrázek 6.10 Sken nástroju Ettercap

Sken našiel 2 zariadenia, a to *Prístupový bod*, ktorý má IP adresu `192.168.0.1` a zariadenie *Stanica 1* s IP adresou `192.168.0.102`. Tieto zariadenia vyberieme ako targety a následne spustíme Man-In-The-Middle útok ARP Poisoning.



Obrázek 6.11 ARP Poisoning

Po úspešnom útoku ARP Poisoning už iba nástroj `Ettercap` odpočúva komunikáciu a podarí sa mu získať údaje, počas toho ako sa zariadenie *Stanica 1* pripája do nastavení zariadenia *Prístupový bod* nešifrovanou komunikáciou protokolu HTTP.



Obrázek 6.12 Získanie údajov

6.9.3 Výsledok

Navrhnutý systém bol schopný detegovať útok ARP Poisoning. Keďže sa jednalo o útok prebiehajúci priamo na sieti, Kismet nemá schopnosť takýto útok detegovať, nakoľko nie je pripojený na sieť. Kvôli tomu sa využil aj NIDS Snort, ktorý bol schopný daný útok detegovať hneď pri skenovaní zariadení a potom aj následnej exekúcii útoku.

```
ICMP PING NMAP [**] [Classification: Attempted Information Leak] [Priority: 2] {ICMP} 192.168.0.1 → 192.168.0.102
ICMP PING [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.0.1 → 192.168.0.102
ICMP Echo Reply [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.0.102 → 192.168.0.1
(spp_arpspoof) Attempted ARP cache overwrite attack [**]
ICMP Echo Reply [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.0.1 → 192.168.0.102
(spp_arpspoof) Attempted ARP cache overwrite attack [**]
```

Obrázek 6.13 Detekcia ARP Poisoning

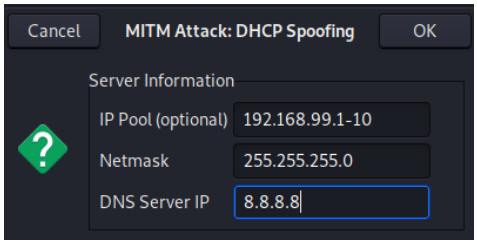
6.10 Rogue DHCP server

6.10.1 Návrh testu

Cieľom testu je overenie schopnosti detekcie navrhnutého systému na útok Rogue DHCP Server. Celý test bude opätovne prebiehať na sieti `Test`. Na uvedenej sieti sa bude nachádzať DHCP server bežiaci na zariadení *Prístupový bod* s IP adresou `192.168.0.1`. Narušiteľ bude mať na sieti tiež zariadenie, ktoré sa bude tváriť ako DHCP server a bude sa snažiť presvedčiť stanice, aby využili jeho a nie originálny DHCP server. Počas testu sa sieť pripojí *Stanica 1*, ktorá má zapnuté nastavenie adresy IP pomocou DHCP. Narušiteľ sa pokúsi tomuto zariadeniu pomocou Rogue DHCP servera nastaviť jeho IP nastavenia.

6.10.2 Test

Aj v tomto prípade sa využije nástroj `Ettercap`, ktorý je schopný vytvoriť Rogue DHCP server. Na spustenie servera stačí rozsah IP adries, sieťovú masku a DNS.



Obrázek 6.14 Nastavenie DHCP servera

Po zapnutí DHCP servera sa spustí sniffer, ktorý bude odpočúvať komunikáciu. Ako vidieť na obrázku nižšie, po pripojení zariadenia *Stanica 1* na sieť mu Rogue DHCP server ponúkne jeho IP nastavenia a *Stanica 1* ich prijme.

```
DHCP spoofing: fake OFFER [94:B8:6D:D9:C7:95] offering 192.168.99.1
DHCP: [192.168.0.101] OFFER : 192.168.99.1 255.255.255.0 GW 192.168.0.101 DNS 8.8.8.8
DHCP: [94:B8:6D:D9:C7:95] REQUEST 192.168.99.1
DHCP spoofing: fake ACK [94:B8:6D:D9:C7:95] assigned to 192.168.99.1
DHCP: [192.168.0.101] ACK : 192.168.99.1 255.255.255.0 GW 192.168.0.101 DNS 8.8.8.8
```

Obrázek 6.15 Komunikácia DHCP

6.10.3 Výsledok

Navrhnutý systém bol schopný útok detegovať, ale až po vytvorení špeciálneho `rule`, ktoré malo nastavené vytvoriť alert vždy, keď sa DHCP Server komunikujúci na sieti nerovnal originálnemu s IP adresou `192.168.0.1` .

```
alert udp !192.168.0.1 67 -> 255.255.255.255 any
(msg: "Rogue DHCP Server"; sid:1000001;)
```

Po vytvorení tohto `rule`, Snort okamžite zaznamenal, že sa na sieti nachádza Rogue DHCP Server.

```
[**] [1:1000001:0] Rogue DHCP Server  [**] [Priority: 0] {UDP} 192.168.0.101:67 → 255.255.255.255:68
```

Obrázek 6.16 Detekcia Rogue DHCP server

6.11 Výsledok testovania

Výsledkom testovania je zistenie, že navrhnutý systém na detekciu narušiteľov je schopný detegovať všetky aktívne útoky, ktoré boli testované, avšak nie je schopný detegovať práve tie pasívne. Ďalším zistením je, že v prípade prebiehajúceho pasívneho skenovania, nie je možné toto skenovanie nijakým spôsobom detegovať, tak isto ako odpočúvanie pri slovníkovom útoku na WPA2-PSK. Práve preto je potrebné sieť zabezpečiť zložitým heslom, v ktorom sa nachádzajú veľké písmená, malé písmená, čísla a znaky, čo útočníkovi veľmi sťažuje nájdenie kľúča a potreboval by vysoký výpočtový výkon, aby bol schopný dané heslo zistiť. Aj napriek neschopnosti detekcie pasívnych útokov by bolo možné navrhnutý systém implementovať v reálnom prostredí, kde dané útoky môžu prebiehať.

ZÁVĚR

Cieľom bakalárskej práce bolo navrhnúť systém, ktorý bude schopný detegovať narušenie bezdrôtovej siete, navrhnutý systém implementovať v testovacom prostredí a následne implementáciu tohto systému overiť a zistiť schopnosť detekcie na rôzne druhy útokov, ktoré sa pre narušenie siete dajú využiť.

V teoretickej časti práce sa čitateľ zoznámil so všetkými podrobnosťami potrebnými na pochopenie fungovania detekčného systému. Bolo v nej podrobne popísané, ako fungujú bezdrôtové siete WLAN, aké sú ich základné prvky, ako takéto siete vyzerajú, akým spôsobom na takýchto sieťach prebieha komunikácia a aká je bezpečnosť na sieťach. Taktiež sa v nej čitateľ oboznámil s útokmi, ktoré možno na sieti WLAN uskutočniť, ako sa rozdeľujú a čo jednotlivé útoky robia. Je v nej popísaná aj najdôležitejšia časť návrhu systému pre detekciu narušiteľov, a to práve WIDS. Boli opísané komponenty systému WIDS, ako funguje proces detekcie, aké techniky na detekciu sa využívajú, ako sa stopujú podvrhnuté zariadenia, ale aj limitácie systému WIDS.

Praktická časť obsahovala niekoľko kapitol, a to: návrh, implementácia a testovanie. Na vytvorenie návrhu bolo potrebné vyhľadať správne nástroje, ktoré sú schopné vykonávať úlohy takéhoto systému. Tiež bolo nutné zistiť, ako dané nástroje fungujú, aké majú nastavenia a ako ich správne nakonfigurovať. Vybranými nástrojmi boli práve Kismet, ktorý bol WIDS, a Snort, ktorý fungoval ako NIDS, pre prípad, že by sa útočník dostal do siete.

Na základe návrhu detekčného systému bolo podľa zadania vytvorené testovacie prostredie, ktoré sa skladalo z bezdrôtovej siete so zariadeniami schopnými využiť vybrané nástroje. Na vytvorenie tohto prostredia bolo nutné využiť špeciálny hardware, schopný monitorovať prevádzku na sieti. Ďalej, pre Kismet bezdrôtovú sieťovú kartu v monitorovacom móde, pre Snort sieťovú kartu v promiskuitnom móde. Tu nastali problémy pri zapnutí monitorovacieho módu, keďže Kismet po spustení monitorovacieho módu pomocou airmon-ng nenašiel žiadne zariadenia. Stačilo daný mód vypnúť a Kismet znovu zapnúť, aby si nastavil monitorovací mód sám.

Otestovanie implementácie navrhnutého systému znovu prebehlo v testovacom prostredí, do ktorého sa však pridalo aj zariadenie útočníka. To vykonávalo útoky popísané v teoretickej časti práce. Po vykonaní niektorých z týchto útokov bolo potrebné navrhnutý systém upraviť tak, aby ich bol schopný detegovať.

Návrh by pre implementáciu systému v reálnom prostredí bolo možné ešte vylepšiť, a to využitím ďalšieho nástroja, ktorý by dokázal Kismet aj Snort alerty ukazovať v jednom rozhraní, čo by zjednodušilo prácu sieťovým administrátorom a nemuseli by sledovať dve rozhrania a všetky alerty by mali na jednom mieste.

Veľmi prekvapujúce sú práve výsledky jednotlivých testov a zistenie, že útoky na bezdrôtové siete nie je vôbec ťažké vytvoriť. Útočník potrebuje mať iba základné znalosti o sieťach na to, aby bol schopný niektoré z týchto útokov vykonať. Preto sa ponúka otázka, či by nebolo vhodné systémy pre detekciu narušiteľov využívať vo väčšej miere.

SEZNAM POUŽITÉ LITERATURY

[1] GAST, Matthew. *802.11 Wireless Networks: The Definitive Guide, Second Edition. 2nd edition.* O'Reilly Media, 2005. ISBN 9780596001834.

[2] SAK, Brian a Jilumundi RAGHU RAM. *Mastering Kali Linux wireless pentesting: test your wireless network's security and master advanced wireless penetration techniques using Kali Linux.* Packt Publishing, 2016. ISBN 9781785285561.

[3] JUNIPER, *Understanding the Network Terms SSID, BSSID, and ESSID* [online]. 2015 [cit. 2021-04-16]. Dostupný z: `https://www.juniper.net/documentation/en_US/junos-space-apps/network-director2.0/topics/concept/wireless-ssid-bssid-essid.html`

[4] OSTERHAGE, Wolfgang. *Wireless Network Security.*Boca Raton: CRC Press, 2018. ISBN 978-0367781293.

[5] BENTON, Kevin. *The Evolution of 802.11 Wireless Security* [online]. 2010 [cit. 2021-04-17]. Dostupný z: `https://benton.pub/research/benton_wireless.pdf`

[6] ALLIANCE, Wi-Fi. *Wi-Fi CERTIFIED WPA3™ Technology Overview* [online]. 2021. [cit. 2021-04-17]. Dostupný z: `https://www.wi-fi.org/downloads-registered-guest/Wi-Fi_CERTIFIED_WPA3_Technology_Overview_202101.pdf/35521`

[7] DIOGENES, Yuri a Erdal OZKAYA. *Cybersecurity - attack and defense strategies: infrastructure security with Red Team and Blue Team tactics.* Birmingham: Packt, 2018. ISBN 9781788475297.

[8] TECHGE. *Typical Wi-Fi attacks* [online]. 2020 [cit. 2021-04-18]. Dostupný z: `https://splone.com/blog/2020/10/13/typical-wi-fi-attacks/`

[9] CLOUDFLARE. *What is a KRACK Attack?* [online]. 2020 [cit. 2021-04-18]. Dostupný z: `https://www.cloudflare.com/learning/security/what-is-a-krack-attack/`

[10] FADYUSHIN, Vyacheslav a Andrey POPOV. *Building a pentesting lab for wireless networks: build your own secure enterprise or home penetration testing lab to dig into the various hacking techniques.* Birmingham: Packt Publishing, 2016. ISBN 9781785283154.

[11] EIAN, Isaac Chin. *Wireless Networks: Active and Passive Attack Vulnerabilities and Privacy Challenges* [online]. Selangor, 2020 [cit. 2021-04-18]. Dostupný z: https://www.preprints.org/manuscript/202010.0018/v1/download

[12] PLCH, Matěj. *Praktické útoky typu man-in-the-middle v počítačových sítích* [online]. Brno, 2015 [cit. 2021-04-19]. Dostupné z: https://theses.cz/id/anp4zs/. Bakalářská práce. Masarykova univerzita, Fakulta informatiky. Vedoucí práce RNDr. Jiří Kůr, Ph.D.

[13] COLEMAN, David. *CWNA Certified Wireless Network Administrator Study Guide: Exam CWNA-108.* 6th Edition. WILEY-SYBEX, 2021. ISBN 978-1-119-73450-5.

[14] COLEMAN, David. *CWSP: certified wireless security professional official: study guide.* Indianapolis: Wiley, 2010. ISBN 978-0470438916.

[15] SCARFONE, Karen a Peter MELL. *Guide to Intrusion Detection and Prevention Systems (IDPS)* [online]. 2012 [cit. 2021-04-18]. Dostupný z: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-94.pdf

[16] NASR, Khalid. *Performance Analysis of Wireless Intrusion Detection Systems* [online]. [cit. 2021-04-18]. 2014. Dostupný z: https://oatao.univ-toulouse.fr/14136/1/Nasr.pdf.

[17] GHORBANI, Ali A., LU, Wei a TAVALLAEE, Mahbod. *Network Intrusion Detection and Prevention Concepts and Techniques.* New York: Springer US, 2010. ISBN 978-0-387-88771-5

[18] RASPBERY PI FOUNDATION. *Raspberry Pi Documentation* [online]. 2021 [cit. 2021-04-20]. Dostupný z: https://www.raspberrypi.org/documentation

[19] KISMET. *Wi-Fi sources: Supported Hardware* [online]. 2021 [cit. 2021-04-20]. Dostupný z: https://www.kismetwireless.net/docs/readme/datasources_wifi/

[20] WIRELESSHACKS. *Best Kali Linux Compatible USB Adapters 2021* [online]. 2021 [cit. 2021-04-20]. Dostupný z: https://www.wirelesshack.org/best-kali-linux-compatible-usb-adapter-dongles.html

[21] KISMET. *Kismet* [online]. 2021 [cit. 2021-04-20]. Dostupný z: https://www.kismetwireless.net/

[22] DD-WRT. *Kismet Server/Drone* [online]. 2021 [cit. 2021-04-20]. Dostupný z: https://wiki.dd-wrt.com/wiki/index.php/Kismet_Server/

[23] KISMET. *Alerts and WIDS* [online]. 2021 [cit. 2021-04-20]. Dostupný z: `https://www.kismetwireless.net/docs/readme/alerts_and_wids/`

[24] OFFENSIVE SECURITY. *Kali Linux ARM Images* [online]. 2021 [cit. 2021-04-22]. Dostupný z: `https://www.offensive-security.com/kali-linux-arm-images/`

[25] DELL. *Dynamic Kernel Module System* [online]. 2021 [cit. 2021-04-23]. Dostupný z: `https://github.com/dell/dkms`

[26] KALI. *What is Kali Linux?* [online]. 2021 [cit. 2021-04-23]. Dostupný z: `https://www.kali.org/docs/introduction/what-is-kali-linux/`

[27] SNORT. *What is Snort?* [online]. 2021 [cit. 2021-04-23]. Dostupný z: `https://www.snort.org/faq/what-is-snort`

[28] SNORT. *Snortology 101* [online]. 2021 [cit. 2021-04-23]. Dostupný z: `https://snort-org-site.s3.amazonaws.com/production/document_files/files/000/000/116/original/Snort_rule_infographic.pdf`

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

WLAN	Wireless Local Area Network
BSS	Basic Service Set
IEEE	Institute of Electrical and Electronics Engineers
BSSID	Basic Service Set Identifier
SSID	Service Set Identifier
ESS	Extended Service Set
MAC	Media Access Control
ESSID	Extended Service Set Identifier
IBSS	Independent Basic Service Set
RTS	Request To Send
CTS	Clear To Send
ACK	Acknowledgement
WEP	Wired Equivalent Privacy
LAN	Local Area Network
SKA	Shared Key Authentication
WPA	Wi-Fi Protected Access
TKIP	Temporal Key Integrity Protocol
CCMP	Counter Mode CBC-MAC Protocol
AES	Advanced Encryption Standard
SAE	Simultaneous Authentication of Equals
DoS	Denial Of Service
ARP	Address Resolution Protocol
OSI	Open Systems Interconnection model
DNS	Domain Name System
DHCP	Dynamic Host Configuration Protocol
WIDS	Wireless Intrusion Detection System
RSSI	Received Signal Strength Indication
RF	Radio Frequency
TDoA	Time Diference of Arrival
SSH	Secure Shell Protocol
RDP	Remote Desktop Protocol
NIDS	Network Intrusion Detection System

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

SEZNAM PŘÍLOH

PŘÍLOHA P I. CD-ROM

Bakalárska práca má CD prílohu, ktorá obsahuje:

- `fulltext.pdf` - bakalárska práca vo formáte PDF
- `kismet` - zložka so súbormi nástroja Kismet
  - `kismet.conf` - nastavenia nástroja
  - `kismet_alerts.conf` - nastavenia alertov
  - `kismet.service` - súbor na spustenie nástroja ako service
- `snort` - zložka so súbormi nástroja Snort
  - `snort.conf` - nastavenia nástroja
  - `rules` - zložka s pravidlami
  - `snort.service` - súbor na spustenie nástroja ako service