DETECTION OF FAKE ACCESS POINTS

Norbert Lővinger

Bachelor Degree Programme (3rd), FEEC BUT

E-mail: xlovin00@vutbr.cz

Supervised by: Zdeněk Martinásek

E-mail: martinasek@feec.vutbr.cz

Abstract: Wireless networks have become a common part of our everyday life. This paper describes the cyber-attacks that employ fake access points. These types of attacks are dangerous for users due open communication medium and automatic connection of end stations. In order to prevent attacks, we can implement Wireless Intrusion Detection System to monitor a wireless network. In this article, we analyze Kismet system in experimental testbed that prevents fake access points attacks.

Keywords: Wi-Fi, Fake Access Points, Rouge AP, WIDS, Kismet

1 ÚVOD DO PROBLEMATIKY

Bezdrôtové siete sa stali bežnou súčasťou každodenného života. Prinášajú veľa pozitív, ale málokto vie, že skrývajú aj negatíva. Jedným z nich sú možné kybernetické útoky na užívateľov, ktoré sú vďaka dostupnosti bezdrôtového prenosového média veľmi efektívnym nástrojom útočníkov. Tento príspevok sa zaoberá kybernetickými útoky, ktoré využívajú metódy falošného prístupového bodu. V rámci výskumu bolo realizované experimentálne pracovisko, v ktorom bol otestovaný detekčný systém Kismet. Pre detekciu ďalších typov kybernetických útokov je vyvíjaná vlastná implementácia v programovacom jazyku Python.

2 KYBERNETICKÉ ÚTOKY - FALOŠNÝ PRÍSTUPOVÝ BOD

Falošný prístupový bod *(angl. Fake Access Point)* je neautorizované zariadenie v bezdrôtovej sieti, ktoré vysiela rovnaké parametre ako legitímny prístupový bod. Takto podvrhnuté zariadenie predstavuje bezpečnostné riziko pre bezdrôtových používateľov v dosahu vysielaného signálu. Vzhľadom na jeho jednoduchosť vytvorenia a vysokú efektívnosť je obľúbeným nástrojom útočníkov, ktorí ho používajú pri rôznych kybernetických útokoch so snahou o prvotný prienik do privátnej lokálnej siete a odcudzenie citlivých informácií. [1]

Medzi najviac využívané kybernetické útoky s využitím falošného prístupového bodu patria:

- *Man-in-the-Middle Attack* – vloženie útočníka do komunikácia medzi používateľa a legitímny prístupový bod alebo pripojenie do lokálnej siete. Účelom je získanie citlivých informácií používateľa. [2]
- *Evil Twin Attack* – vytvorenie úplne rovnakej kópie legitímneho prístupového bodu za účelom pripojenia používateľov a získania citlivých údajov.
- *KARMA Attack* – využitie aktívneho skenovania požiadaviek bezdrôtových zariadení o pripojenie – tzv. Probe Request, za účelom podvrhnutia falošnej bezdrôtovej siete. Nutná je aktívna interakcia používateľov.
- *Deauthentication Attack* – vytváranie veľkého počtu deautentizačných rámcov, za účelom odoprenia služby používateľa od legitímneho prístupového bodu a následné pripojenie na falošný prístupový bod.

3 BEZDRÔTOVÝ DETEKČNÝ SYSTÉM

Monitorovací systém umiestnený v bezdrôtovej sieti *(angl. WIDS – Wireless Intrusion Detection System)* v reálnom čase analyzuje a vyhodnocuje sieťovú komunikáciu, či sa nejedná o kybernetický útok. Detekcia útokov využíva dve základné metódy - na základe signatúr a na základe anomálií.

Signatúry sú vytvorené vzory nepriaznivej činnosti na sieti, ktoré sú uložené v databáze systému. Výhodou je vysoká efektivita pri známych útokoch. Naopak pri nových útokoch je schopnosť detekcie takmer nulová. Tento problém rieši druhýýý spôsob detekcie pomocou anomálií.

Anomálie sú neznáme udalosti a odchýlky sieťovej komunikácie, ktoré sú zbierané a radené do profilov. Nevýhodou je možný vysoký počet falošných hlásení a nutná doba učenia za účelom vytvorenia modelu. Aktuálne detekčné systémy sú tzv. hybridné systémy, ktoré kombinujú výhody z oboch metód, čím sa zvyšuje úspešnosť detekcie útokov. [3]

4 EXPERIMENTÁLNE PRACOVISKO

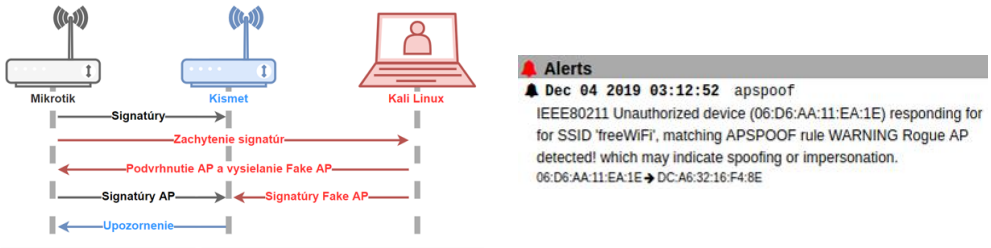
Hlavným cieľom tejto práce je vytvoriť bezdrôtový detekčný systém využívajúci cenovo dostupný detektor, ktorý je schopný detekovať kybernetické útoky v bezdrôtovej sieti. Detekčný systém bol vyvíjaný a skúmaný v experimentálnom pracovisku, ktorého bloková schéma a skutočná podoba je zobrazená na **obr. 1**. Pracovisko predstavuje bežný model bezdrôtovej lokálnej siete na ktorom boli testované kybernetické útoky s využitím falošného prístupového bodu a voľne dostupné bezdrôtové detekčné systémy na jeho detekciu. Pracovisko obsahovalo nasledovné zariadenia s nainštalovaným softvérom:

- Legitímny prístupový bod - *Mikrotik hAP^2 router.*
- Cenovo dostupný *detektor Raspberry Pi 4 s* operačným systémom *Raspbian* s nainštalovaným bezdrôtovým detekčným systémom *Kismet 2019-09-01.* [4]
- Zariadenie legitímneho používateľa s operačným systémom *Windows 10 Pro.*
- Zariadenie útočníka s virtualizovaným *Kali Linux 2019.3* a externou bezdrôtovou kartou TP-Link, ktorá simulovala falošný prístupový bod pomocou nástrojov z balíka **aircrack-ng**.

Obrázek 1: Schéma zapojenia detektoru a experimentálne pracovisko

Po zapojení pracoviska, inštalácií operačných systémov a nástrojov bol spustený detekčný systém Kismet, ktorý monitoroval sieťovú aktivitu cez monitorovací mód integrovanej bezdrôtovej karty Raspberry. Spustením a nastavením vysielania legitímneho prístupového bodu Mikrotik, boli získané jeho základné signatúry (SSID,BSSID), ktoré boli vložené do konfiguračného súboru detekčného systému Kismet s využitím funkcie **apspoof**.

Po uložení a reštarte detekčného systému bol spustený falošný prístupový bod, ktorý si pomocou analýzy beacon rámcov zistil vysielané signatúry legitímneho bodu, ktoré s využitím nástroju **airbase-ng** podvrhol. Bezdrôtový detekčný systém zareagoval na vysielanie v reálnom čase a zobrazil varovnú notifikáciu používateľovi na **obr. 2**, v ktorej informoval o podvrhnutom bode so zhodnými signatúrami zapísanými v konfiguračnom súbore. [5]



Obrázek 2: Schéma podvrhnutia prístupového bodu a upozornenie

5 ZHRNUTIE

Príspevok detailne popisuje podceňovanú problematiku falošných bezdrôtových prístupových bodov, ktoré sú čoraz častejšie využívané útočníkmi na miestach s vysokou hustotou bezdrôtových používateľov. Vzhľadom na ich jednoduchosť implementácie a vysokú úspešnosť sú bežným nástrojom na vykonanie ďalších kybernetických útokov. Účinná ochrana spočíva vo využívaní detekčných systémov založených na metódach porovnávania signatúr a anomálií okolitých bezdrôtových sietí. Medzi takéto systémy patrí aj voľne dostupný detekčný systém - **Kismet**, ktorý umožňuje jednoduché monitorovanie blízkych bezdrôtových sietí s upozornením na ich podozrivú aktivitu. V experimentálnom pracovisku bol detekčný systém otestovaný na detekciu falošného prístupového bodu vytvoreného s rovnakými signatúrami ako legitímny prístupový bod. Jeho výsledkom bola pozitívna zhoda zachytených signatúr v reálnom čase a následné upozornenie používateľa. Pre detekciu ďalších typov kybernetických útokov sa ďalšia časť práce bude zaoberať tvorbou vlastného návrhu a implementácie riešenia bezdrôtového detektoru v programovacom jazyku Python.

POĎAKOVANIE

Výskum bol podporený projektom MVČR VI20192022149 s názvom *Systém distribuovaného dohledu nad síťovým provozem L2/L3* podľa vyhlášky č. 317/2014 Sb. a zákona 181/2014 Sb..

REFERENCE

[1] DVORSKÝ, Radovan. *Detekce útoků na wifi sítě pomocí získávaní znalostí* [online]. Brno, 2014 [cit. 19. 2. 2020]. Dostupné z URL: https://www.vutbr.cz/www_base/zav_prace_soubor_verejne.php?file_id=119310

[2] PLCH, Matej. *Practical man-in-the-middle attacks in computer networks* [online]. Brno, 2015 [cit. 19. 2. 2020]. Dostupné z URL: https://is.muni.cz/th/s8uf2/thesis.pdf

[3] POLJAK, Peter. *IDS pro WiFi sítě* [online]. Brno, 2013 [cit. 19. 2. 2020]. Dostupné z URL: https://is.muni.cz/th/qhqx2/praca.pdf

[4] *Kismet* [online]. 2019 [cit. 19. 2. 2020]. Dostupné z URL: https://www.kismetwireless.net/

[5] THEJDEEP. G, SHIVA SAGAR. B, SIDDARTHA. L. K a B. R. CHANDAVARKAR. *Detecting Rogue Access Points using Kismet.* 2015 International Conference on Communications and Signal Processing (ICCSP) [online]. IEEE, 2015, 0172-0175 [cit. 19. 2. 2020]. DOI: 10.1109/ICCSP.2015.7322813. ISBN 978-1-4799-8081-9. Dostupné z URL: http://ieeexplore.ieee.org/document/7322813/