KSU Proceedings on Cybersecurity Education, Research and Practice

2019 KSU Conference on Cybersecurity Education, Research and Practice

Oct 12th, 1:25 PM - 1:50 PM

Effectiveness of Tools in Identifying Rogue Access Points on a Wireless Network

Ryan VanSickle
University of North Georgia, ryan.vansickle@ung.edu

Tamirat Abegaz
University of North Georgia, tamirat.abegaz@ung.edu

Bryson Payne
University of North Georgia, bryson.payne@ung.edu

Abstract

Wireless access points have greatly improved users' ability to connect to the Internet. However, they often lack the security mechanisms needed to protect users. Malicious actors could create a rogue access point (RAP), using a device such as the WiFi Pineapple Nano, that could trick users into connecting to an illegitimate access point (AP). To make them look legitimate, adversaries tend to setup RAPs to include a captive portal. This is very effective, since most public networks use captive portals as a means to provide genuine access. The objective of this study is to examine the effectiveness of RAP identification tools in identifying WiFi Pineapple RAPs. Three common RAP identifications tools were used, namely Aircrack-ng, Kismet, and inSSIDer. The result indicated that RAPs could easily be identified through actively monitoring networks using tools such as Aircrack-ng, Kismet, and inSSIDer.

Location

KSU Center Rm 460

Disciplines

Information Security | Management Information Systems | Technology and Innovation

INTRODUCTION

Wireless local area networks (WLANs) are a growing trend as more devices become Internet-enabled and end-users favor the convenience of being able to browse the web without a wired connection. WLANs are based on IEEE 802.11 and provide users the ability to be mobile and still have network access (Souppaya & Scarfone, 2012, Dabrowski et. al, 2016). WLANs are client devices that are connected to a wired network infrastructure (Ghafir et. al, 2018). WLANs, by their broadcast nature, make them more prone to an attack. WLANs are less secure than wired networks because they are easier to connect to and weaker security configurations (Souppaya & Scarfone, 2012). WLANs are dangerous because an attacker only needs to be within the wireless network range, typical configurations put convenience over security, and can compromise the entire network (including LAN) and the devices on the network (Souppaya & Scarfone, 2012).

One device that can compromise a network is a rogue access point; however, it needs user interaction to work if a client device is not set up to automatically connect (Witemyre et. al, 2018). It can compromise a network by creating a backdoor that bypasses the security controls implemented on the network and opens up the possibility of an attack such as a man-in-the-middle attack (Souppaya & Scarfone, 2012). A man-in-the-middle attack occurs when the client receives a response from the attacker instead of the webserver it was attempting to reach and assumes the attacker's response is legitimate (Agarwal et. al, 2018). A rogue access point is an unauthorized access point that attempts to lure users to connect to it. A deauthentication attack requires spoofing the access points MAC address, otherwise known as EUI-48 or EUI-64, and copies the access points SSID so that when the user reconnects it will be to the rogue access point (Ghafir et. al, 2018). A rogue access point takes advantage of the convenience of devices remembering a network and automatically connecting to it.

RELATED WORK

A real-life example of why network security and monitoring networks are important is the TJ Maxx incident (Agrawal et. al, 2014). The TJ Maxx attack of 2005 where an attacker compromised the store’s network, stole 45 million customer records, and cost the store an estimated 1 billion dollars over an 18-month period (Anon. 2019, Agarwal et. al, 2018). The attack took advantage of the Wireless Privacy Equivalent (WEP) network TJ Maxx used instead of the more secure security standard Protected Access (WPA) or WPA2 and sending unencrypted data over the network. WEP was first cracked in 2001. This incident could have been prevented by actively monitoring the network, logging data and then reading the data daily, using SSL/TLS or IPSec to send data, and adhering to rules and regulations. The hackers stole 80 GB of data over a period of seven months (Tom Espiner, 2017, Kim 2017). TJ Maxx was aware of the high-level vulnerabilities it had based on an audit from 2004, but the company did not feel like the additional security was worth the cost (Tom Espiner).

The implementation of this experiment for any type of network is simply to connect a RAP to a computer and configure the RAP to mimic a legitimate access point. A successful RAP will have great signal strength, allow users to access the Internet, and be the most appealing AP in the area. One could jam or weaken APs near the RAP to be the most appealing and also set up the RAP in a location near the target. A deauthentication attack is one way to get targets off an AP and try to connect to it again. It would also take advantage of a user's inherent trust to connect to a network automatically and willingness to connect to a free open WiFi. One could also have a captive portal similar to a restaurant.

A campus or enterprise network would require the attacker to bypass the implemented network security measures to avoid detection. The attacker must spoof a EUI-48 or EUI-64 address that looks legitimate and similar to the other devices on the network if there is address filtering. They may need to make the AP look like it has its regular traffic so the network/security team does not see any irregularities of its temporal traffic. A campus or enterprise network could have a flood guard and an ACL. The attacker would also need to choose a location that is near the AP target.

An access point is an object that allows devices on the network Internet access. These connections can be physical or wireless. A physical connection is a wired network, using cables, between an AP and a device. Usually, these devices are in a stationary position and plugged into an outlet. A wireless connection is between an AP and a device that does not require cables to make the connection. Wireless access points (WAPs) need to be secured by using authentication. It is important to change the default username and password for the WAP. WAPs signal strength is determined by how close the device is to the AP, with close having the best strength and losing strength as the distance between the device and AP increase

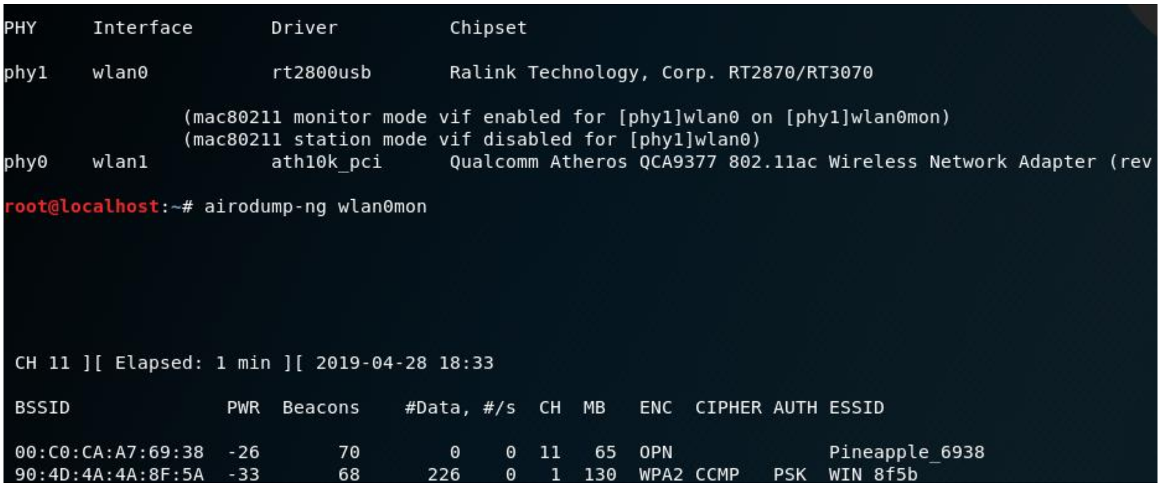
Rogue access point WiFi Pineapple Nano is a device that connects to any computer via USB, can be set up within minutes, and contains modules that allow penetration testers to perform attacks on connected devices such as a man-in-the-middle attack or a phishing attempt (2). Rogue access points provide an Internet connection and can also re-direct clients to a malicious website or steal their credentials (4). An easy method to get victims to connect to a rogue access point would be to set up a rogue access point in an area with free open WiFi with the best signal because most users trust that network to be legitimate and will not think twice about connecting to it (4). Aircrack-ng, Kismet, and insider tools are used to identify the presence of this rogue access point (Sagar, 2015, Anon 2019,

APPROACH

This experiment will work on any network; however, for this particular use-case, a home network is used (Fig. 2). We configured the WiFi Pineapple Nano networking settings and left the rest of the settings default (Fig. 3). We identified our wireless adapters using ifconfig. We configured one wireless adapter to managed mode and one wireless adapter to monitor mode. We then ran aircrack-ng, Kismet, and inSSIDer on our selected home network.

Aircrack-ng

Aircrack-ng is a command-line suite of tools used to monitor networks by capturing packets, attack in a variety of ways including replay attacks, deauthentication, fake access points, cracking WEP and WPA1 and WPA2, and testing WiFi cards and driver capabilities (6). This program is available on several operating systems including Windows, Linux, OS X, and OpenBSD. For the scope of this experiment, the airmon-ng and airodump-ng commands will be used. The airmon-ng command puts the wireless access card into monitor mode which allows the card to listen to all packets. The airodump-ng command is used to discover networks (APs) and statistics about the network.



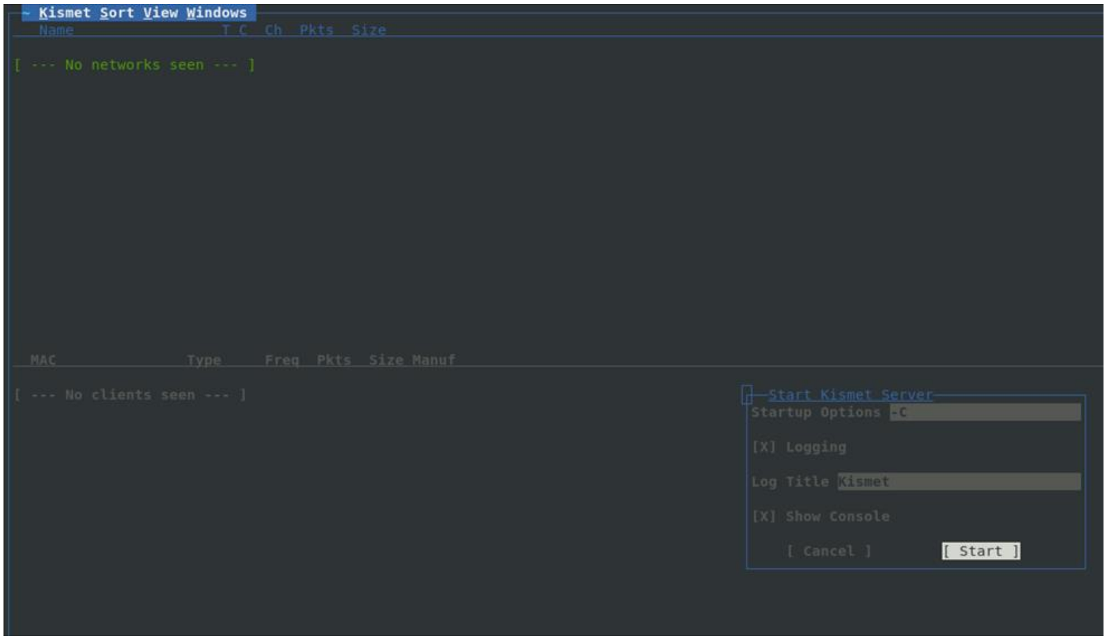
```
PHY     Interface       Driver          Chipset

phy1    wlan0           rt2800usb       Ralink Technology, Corp. RT2870/RT3070

                (mac80211 monitor mode vif enabled for [phy1]wlan0 on [phy1]wlan0mon)
                (mac80211 station mode vif disabled for [phy1]wlan0)
phy0    wlan1           ath10k_pci      Qualcomm Atheros QCA9377 802.11ac Wireless Network Adapter (rev

root@localhost:~# airodump-ng wlan0mon




 CH 11 ][ Elapsed: 1 min ][ 2019-04-28 18:33

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

 00:C0:CA:A7:69:38  -26       70        0    0  11   65  OPN              Pineapple_6938
 90:4D:4A:4A:8F:5A  -33       68      226    0   1  130  WPA2 CCMP   PSK  WIN 8f5b
```

Figure 1. Screenshot of the Aircrack-ng command

The first command used was ifconfig, which displays the list of wireless adapters. WLAN 0 was used as monitor mode and wlan1 was used as the wireless adapter in managed mode. Airmon-ng check kill command kills any process that might cause the program to run correctly. airmon-ng start wlan0 puts wlan0 into monitor mode allowing it to view network traffic. That changed the name to wlan0mon. Next, the airodump-ng command was used. This command caused the program to begin parsing network traffic. As shown in Figure 1, the airodump-ng wnlan0mon command displayed important information about the wireless access point. For instance, notice that the ESSID, which is the broadcast name, of Pineappple_6938 and BSSID, MAC address, channel 11, and no encryption indicating this the WiFi Pineapple Nano.

Kismet

Kismet is a tool that passively acts as a network detector, sniffer, wireless intrusion detection framework, and wardriving (7). Passively in this instance means that it will not send any logging packets. Kismet works by placing the wireless access card into monitor mode and will then be able to see all packets. Kismet can capture Bluetooth and replay pcap or pcap-ng files. Kismet also allows users to remotely capture packets. It can also use GPS to give a general idea of where a receiver target is located. Kismet also allows users to filter based on MAC addresses and other things. Figure 2 shows the start screen for Kismet. Through subsequent steps, users configure the Kismet server with options, the name of the log file, and to monitor traffic.



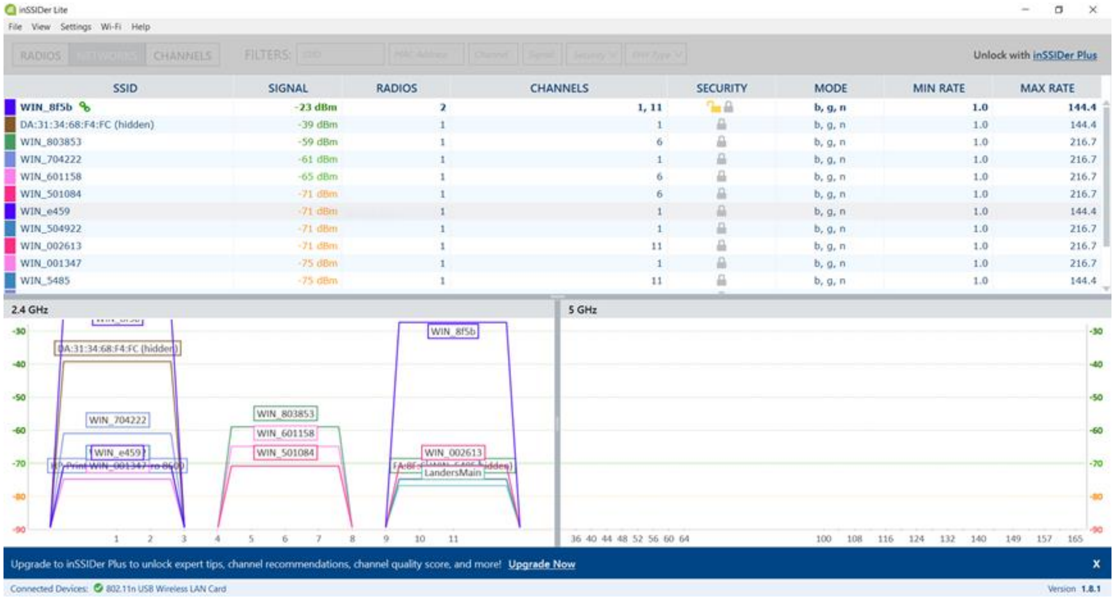
```
  Name                    T C  Ch  Pkts  Size

[ --- No networks seen --- ]

  MAC                Type     Freq  Pkts  Size Manuf

[ --- No clients seen --- ]
                                   Start Kismet Server
                                   Startup Options -c
                                   [X] Logging
                                   Log Title Kismet
                                   [X] Show Console
```

Figure 2. Screen displayed when starting Kismet.

inSSIDer

inSSIDer is a tool that analyzes WiFi environments and helps users see details of a network work such as channel placement, signal strength, security type, give aliases to APs, network overlap, and even spot RAPs (8). inSSIDer only works on Windows operating systems and provides a GUI. inSSIDer provides filtering and coloring in order to help one narrow down the relevant data. It also allows both physical and logical grouping. inSSIDer also provides graphs which can be useful when comparing network utilization over a period of time.

InSSIDer did not require any setup. Users open the program up and select a network they would like to know more about. In this particular case, we would like to know more about the two WIN_8f5b networks. The link symbol indicates that there are multiple networks with that SSID. Looking at the screen, we can see that one of those networks is configured like the WiFi Pineapple Nano. Figure 3 showed the output if the InSSIDer tool



SSID	SIGNAL	RADIOS	CHANNELS	SECURITY	MODE	MIN RATE	MAX RATE
WIN_8f5b	-23 dBm	2	1, 11	🔓🔒	b, g, n	1.0	144.4
DA:31:34:68:F4:FC (hidden)	-39 dBm	1	1	🔒	b, g, n	1.0	144.4
WIN_803853	-59 dBm	1	6	🔒	b, g, n	1.0	216.7
WIN_704222	-61 dBm	1	1	🔒	b, g, n	1.0	216.7
WIN_601158	-65 dBm	1	6	🔒	b, g, n	1.0	216.7
WIN_501084	-71 dBm	1	6	🔒	b, g, n	1.0	216.7
WIN_e459	-71 dBm	1	1	🔒	b, g, n	1.0	144.4
WIN_504922	-71 dBm	1	1	🔒	b, g, n	1.0	216.7
WIN_002613	-71 dBm	1	11	🔒	b, g, n	1.0	216.7
WIN_001347	-75 dBm	1	1	🔒	b, g, n	1.0	216.7
WIN_5485	-75 dBm	1	11	🔒	b, g, n	1.0	144.4

Upgrade to inSSIDer Plus to unlock expert tips, channel recommendations, channel quality score, and more! Upgrade Now

Connected Devices: 802.11n USB Wireless LAN Card

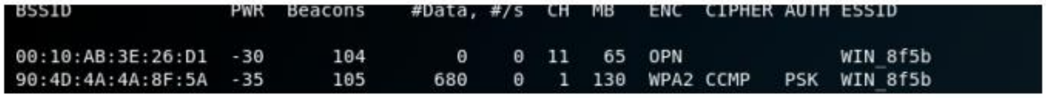
Version 1.8.1

Figure 3. Screen displayed when starting Kismet.

RESULTS

Aircrack-ng was the first tool we used to detect the WiFi Pineapple Nano using the configuration stated in section 3.1 Aircrack-ng was able to identify the RAP (see Fig. 4). The following steps were followed: plug the WiFi Pineapple Nano into a computer, use ifconfig to identify our wireless adapters, configure the wireless adapter into monitor mode, detect networks and traffic using the airodumg-ng command, and identify the RAP by using the BSSID (MAC address) or ESSID

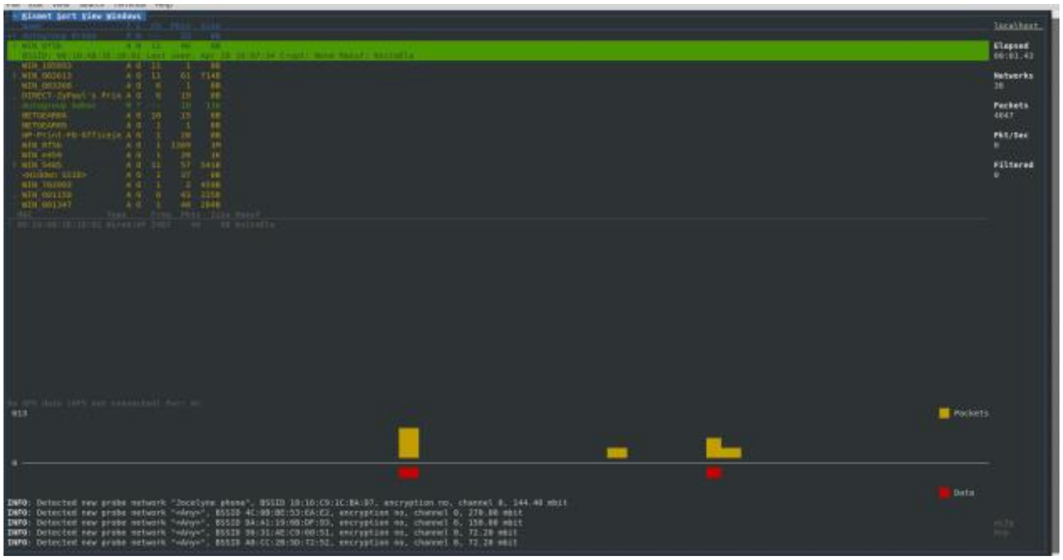
(SSID). Once done monitoring, be sure to exit monitor mode. As shown in Figure 4, the BSSID is the mac address of the WiFi Pineapple Nano, ESSID is the Service Set Identifier, CH is what channel the network is own, Data is how much data is being broadcast on the network, ENC is what type of encoding protocol the network uses, and MB is the maximum throughput.



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

00:10:AB:3E:26:D1  -30      104        0    0  11   65  OPN              WIN_8f5b
90:4D:4A:4A:8F:5A  -35      105      680    0   1  130  WPA2 CCMP   PSK  WIN_8f5b
```

Figure 4. Aircrack-ng identification result

Kismet was the next tool we used and it was able to detect the WiFi Pineapple Nano as well (See Figure 5). Kismet required more setup than Aircrack-ng, but we found it easier to use and had more features. We plugged in the WiFi Pineapple Nano and opened Kismet using the -C switch for capture mode. There Kismet guided me through the setup which included adding a wireless adapter and setting it up into monitor mode. Once set up, Kismet quickly found the RAP and even displayed when it was last accessed.

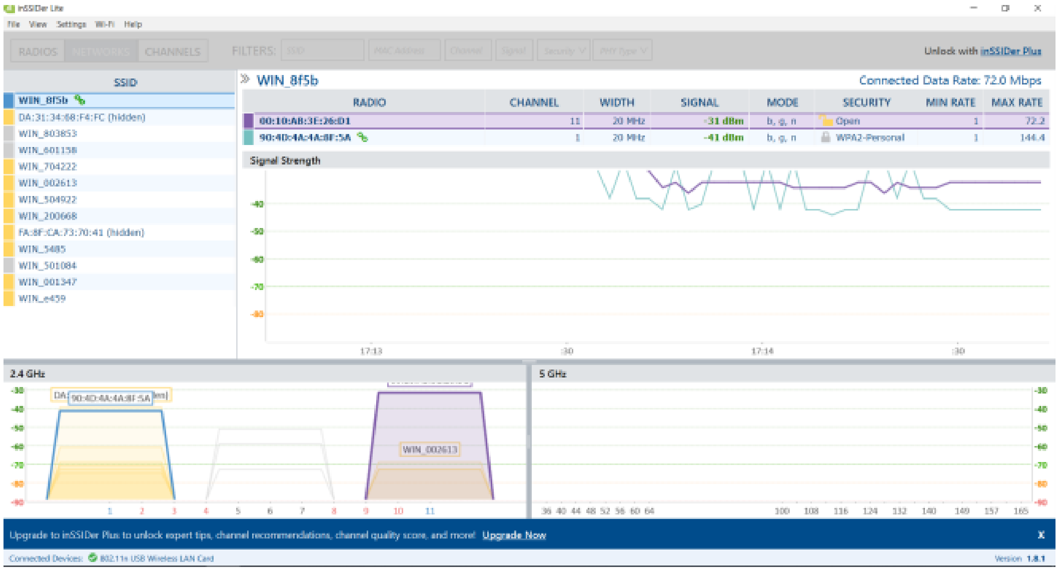


```
INFO: Detected new probe network "Jocelyns phone", BSSID 10:16:C9:1C:BA:97, encryption no, channel 0, 144.40 mbit
INFO: Detected new probe network "<Any>", BSSID 4C:09:0E:53:EA:E2, encryption no, channel 0, 270.00 mbit
INFO: Detected new probe network "<Any>", BSSID 0A:41:19:68:DF:93, encryption no, channel 0, 150.00 mbit
INFO: Detected new probe network "<Any>", BSSID 98:31:AE:C9:60:51, encryption no, channel 0, 72.20 mbit
INFO: Detected new probe network "<Any>", BSSID A8:CC:20:9D:72:52, encryption no, channel 0, 72.20 mbit
```

Figure 5. Kismet identification result

inSSIDer was the last tool we used to detect the WiFi Pineapple Nano. This was by far the easiest to use because it is GUI based and displays all the networks within your WiFi range with WIN_8f5b having the strongest signal. Here one can see that the WIN_8f5b SSID has two radios, two channels, two items in the security column, and a link symbol indicating there are multiple APs with the same SSID.

All of those indicators are signs that multiple APs are being used, which might be the case in a large network environment, or there is a RAP on that network. Double-clicking an SSID allows a more detailed look at the AP as shown below. (Fig. 6) Kismet also found the RAP and is consistent with aircrack-ng's findings. inSSIDer also found the RAP and was consistent with the other two programs in what they found. The BSSID is the mac address of the WiFi Pineapple Nano, ESSID is the Service Set Identifier, CH is what channel the network is own, Data is how much data is being broadcast on the network, ENC is what type of encoding protocol the network uses, and MB is the maximum throughput. The RAP is the first network



SSID

- WIN_8f5b
- DA:31:34:68:F4:FC (hidden)
- WIN_803853
- WIN_601158
- WIN_704222
- WIN_002613
- WIN_504922
- WIN_200668
- FA:8F:CA:73:70:41 (hidden)
- WIN_5485
- WIN_501084
- WIN_001347
- WIN_e459

WIN_8f5b Connected Data Rate: 72.0 Mbps

RADIO	CHANNEL	WIDTH	SIGNAL	MODE	SECURITY	MIN RATE	MAX RATE
00:10:AB:3E:26:D1	11	20 MHz	-31 dBm	b, g, n	Open	1	72.2
90:4D:4A:4A:8F:5A	1	20 MHz	-41 dBm	b, g, n	WPA2-Personal	1	144.4

Upgrade to inSSIDer Plus to unlock expert tips, channel recommendations, channel quality score, and more!

Connected Devices: 802.11n USB Wireless LAN Card Version 1.8.1

Figure 6. inSSIDer identification result

CONCLUSIONS AND FUTURE WORK

Security often is overlooked in the name of convenience. For instance, technology providers allow to automatically connect devices to an available network. Malicious actors could create a rogue access point (RAP) using a device, such as the WiFi Pineapple Nano, that would trick users into connecting to an illegitimate access point (AP) which could compromise a network. RAPs can be set up to include a captive portal that could be used for malicious intent. This is useful in creating a RAP in a public network like in restaurants that have a captive portal on the genuine access point and in attacking users that have a VPN access since users need to authenticate before obtaining Internet access. Actively monitoring a network and educating users are the best ways to make secure a network. Education is critical in preventing security incidents from occurring and that education must be continuous, to make sure users are up to date, as new exploits are being developed, with the latest best practices and also to help them from compromising a network unintentionally.

REFERENCES

Adrian Dabrowski, Georg Merzdovnik, Nikolaus Kommenda, and Edgar Weippl. 2016. *Browser History Stealing with Captive Wi-Fi Portals*. (May 2016). Retrieved May 4, 2019 from https://ieeexplore.ieee.org/abstract/document/7527774

Agrawal, Manish, Alex Campoe, and Eric Pierce. *Information security and IT risk management*. Wiley Publishing, 2014.

Agarwal, M., Biswas, S., & Nandi, S. (2018). *An Efficient Scheme to Detect Evil Twin Rogue Access Point Attack in 802.11 Wi-Fi Networks*. International Journal of Wireless Information Networks, 25(2), 130-145. Networks. International Journal of Wireless Information Networks, 1-16.

Anon. Kismet. *(A, 2019). Retrieved March 28, 2019 from https://www.kismetwireless.net/*

Anon. 2019. inSSIDer Plus: *Visualize Your WiFi Environment. (2019).* Retrieved March 28, 2019 from https://www.metageek.com/products/inssider/

Anon. 2019. *Omnipeek is more than an impressive collection of packet analysis*. (2019). Retrieved March 28, 2019 from https://www.liveaction.com/products/omnipeek/

B. Sagar, K. Siddartha, and R. Chandavarkar. 2015. Detecting Rogue Access Points using Kismet. (2015). Retrieved January 21, 2019

Ghafir, I., Kyriakopoulos, K. G., Aparicio-Navarro, F. J., Lambotharan, S., Assadhan, B., & Binsalleeh, H. (2018). *A basic probability assignment methodology for unsupervised wireless intrusion detection. IEEE Access*, 6, 40008-40023.

Kim Zetter. 2017. *TJX Hacker Gets 20 Years in Prison*. (June 2017). Retrieved April 25, 2019 from https://www.wired.com/2010/03/tjx-sentencing/

Souppaya, M., & Scarfone, K. (2012). *Guidelines for securing wireless local area networks (WLANs). NIST Special Publication*, 800, 153.

Tom Espiner. 2007. *Wi-Fi hack caused TK Maxx security breach. (May 2007).* Retrieved April 25, 2019 from https://www.zdnet.com/article/wi-fi-hack-caused-tk-maxx-security-breach/

Witemyre, S., Abegaz, T., Payne, B.R., Mady, A.N. (2018). Hacking Wireless Communications with WiFi Pineapple NANO. *Proceedings of the 2018 Conference on Cybersecurity Education, Research and Practice*.