**Lab #2 Learn Fluxion- one of Kali Linux Security Tools**

**Last Name: \_\_\_\_\_\_ First Name:** \_\_\_\_\_\_\_

**Objective:** Hand-On lab to carry out for students to understand how Kali Linux security tools work. The aim for this lab is to is to gain knowledge in using a man in the middle attack on WPA/WPA2 wireless networks.??? Need more about Fluxion

**Scenario:??? I donot think this is the scenario, this is background** you need to create a scenario

**Background**: Kali Linux is a multiplatform, Debian-based Linux distribution aimed at advanced Penetration Testing and Security Auditing. Kali Linux contains many tools that are fixed on towards different information tasks such as Security Research, Computer Forensics and more. Linux was developed through rewriting of Backtrack by Mati Aharoni and Devon Keams of Offensive Security. Linux contains over six hundred different preinstalled penetration applications that can be discovered. Each program in Kali Linux has its own unique flexibility and case uses. Kali separates these useful utilities into the following categories: Information Gathering, Vulnerability Analysis, Wireless Attacks, Web Applications, Exploitation Tools, Stress Testing, Forensics Tools, Sniffing & Spoofing, Password Attacks, Maintaining Access, Reverse Engineering, Reporting Tools, and Hardware Hacking. ?? Which category Fluxion belong to?

Fluxion is a rescript attack that is used to trick inexperienced users into revealing the password/passphrase of the network. Fluxion is a special tool due to the use of a WPA handshake special able to control the behavior of login page but the behavior of the entire script. Fluxion is a combination of technical and social engineering automation that tricks a user into handing over the Wi-fi password in a matter of keystrokes. It is a social engineering structure using an opposite twin access point, integrated jamming, and handshake capture functions. It compresses the original network and creates a clone of the network with the extract name, causing the disconnected individual to join the network again. This tool causes the networks to present a fake login page indicating the router needs a restart or load firmware and requests the network password to proceed. Then the tool uses a captured to check the password entered and continues to jam the target AP until the correct password is entered.

**Goals:**

The students will learn: The following are concepts ??? you need to redesign it

* Learn what Kali Linux is
* Learn what are the different tools that are found in Kali Linux
* Learn what is social engineering attack and man in the middle attack
* Learn what fluxion attack is and what happens during a fluxion attack
* Learn what WPA/WPA2 is
* Learn the layers application of computer security

**Tools**

* Kali Linux Virtual Machine
* Laptop/Desktop
* GitHub
* Ethernet Cable

**Tasks: task #1—task #3 are combined as ONE task**

**Task #1: Installing/Preparing/Starting Kali Linux Virtual Machine**

1. Install the VMware with default options from the website (https://my.vmware.com/en/web/vmware/free#desktop\_end\_user\_computing/vmware\_workstation\_player/15  
   \_0) if you are using a PC or VMware Fusion or Virtual Box if you are using MAC OS operating system.
2. In a search engine, go to <https://www.offensive-security.com/kali-linux-vmware-virtualbox-image-download/> website where you will click the Kali Linux VMware 64 bit to get the current version of the computer application. Then unzip the download file.
3. Navigate to the Kali VM that was unzipped and start the virtual machine.
4. Log in to Kali with the username kali and password of Kali.
5. In your own words explain what is a kali Linux and what is the use of kali Linux?

|  |
| --- |
|  |
|  |
|  |
|  |

1. Where do you go to download the latest version of kali Linux on a PC and MAC OS operating system?

|  |
| --- |
|  |
|  |
|  |

1. List the several types of tools that can be performed by Kali Linux?

|  |
| --- |
|  |
|  |
|  |
|  |

**Task #2: Installing the Fluxion Program**

1. In the terminal window, type in this command to download the latest version of the program into Kali Linux: **git clone** [**https://www.github.com/FluxionNetwork/fluxion.git**](https://www.github.com/FluxionNetwork/fluxion.git)
2. Then switch tool’s directory by typing this command: **cd fluxion**.
3. Run the fluxion program by typing this command: **./fuxion.sh**.
4. In your own words, explain what a fluxion attack is and how a fluxion attack is performed?

|  |
| --- |
|  |
|  |
|  |
|  |

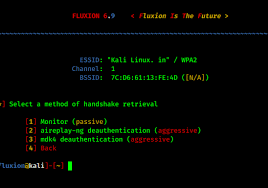
1. In your own words, explain what is a social engineering attack and give example of social engineering attack?

|  |
| --- |
|  |
|  |
|  |
|  |
|  |

1. In your own words, explain what is a man in the middle attack and explain what happens during an attack like that?

|  |
| --- |
|  |
|  |
|  |
|  |

**Task #3: Running of the Fluxion Program**



1. By scanning for a target wireless network.
2. Launch the Handshake Snooper attack.
3. Capture a handshake for password verification.
4. Launch a Captive attack which will lead to a sequence of actions
5. Spawns a rogue (fake) AP, imitating the original access point:
6. Spawns a DNS server, redirecting all requests to the attacker's host running the captive portal.
7. Spawns a web server, serving the captive portal which prompts users for their WPA/WPA2 key.
8. Spawns a jammer, de-authenticating all clients from original AP and luring them to the rogue AP.
9. All authentication attempts at the captive portal are checked against the handshake file captured earlier.
10. The attack will automatically terminate once a correct key has been submitted.
11. The key will be logged, and clients will be allowed to reconnect to the target access point.
    1. In your own words, explain what is a WPA/WPA2 key and what is the difference between both keys.

|  |
| --- |
|  |
|  |
|  |
|  |

* 1. Explain what is a Handshake Snooper and Captive attack?

|  |
| --- |
|  |
|  |
|  |
|  |

* 1. Explain what a DNS server and web servers are and explain the difference between each server.

|  |
| --- |
|  |
|  |
|  |
|  |

* 1. How many digits is a WPA key?

|  |
| --- |
|  |
|  |
|  |
|  |

* 1. How long is WPA/WPA2 password?

|  |
| --- |
|  |
|  |
|  |
|  |

* 1. What is the definition of WPA/WPA?

|  |
| --- |
|  |
|  |
|  |
|  |