Experiment 08

Learning Objective: Use of tools like Fluxion, Wifite, & WifiSlax OS to scan and test the Wi-Fi Security and perform Vulnerability Assessment and Penetration Testing.

Tools: Fluxion, Wifite, & WifiSlax OS.

Theory:

What is Fluxion?

Fluxion is a Wi-Fi Security analysis tool that can be used for WPA and WPA2 hacking or other Wi-Fi attacks using the **MITM** (Man in the Middle Attack) techniques. It is the future of Wi-Fi hacking and a combination of technical and social engineering techniques that force users to send Wi-Fi passwords to attackers in plain text. In short words, it's a social engineering framework using the following process.

How to Use Fluxion for WPA / WPA2 Hacking

Step 1: Scan the networks.

Step 2: Capture a handshake (can't be used without a valid handshake, it's necessary to verify the password)

Use WEB Interface *

Step 3: Launch a FakeAP instance to imitate the original access point.

Step 4: Spawns an MDK3 process, which deauthenticates all users connected to the target network, so they can be lured to connect to the FakeAP and enter the WPA password.

Step 5: A fake DNS server is launched in order to capture all DNS requests and redirect them to the host running the script.

Step 6: A captive portal is launched in order to serve a page, which prompts the user to enter their WPA password.

Step 7: Each submitted password is verified by the handshake captured earlier.

Step 8: The attack will automatically terminate, as soon as a correct password is submitted.

Installing Fluxion

Run the following commands to install fluxion in your Kali Linux:

~# **git clone https://github.com/wi-fi-analyzer/fluxion.git**

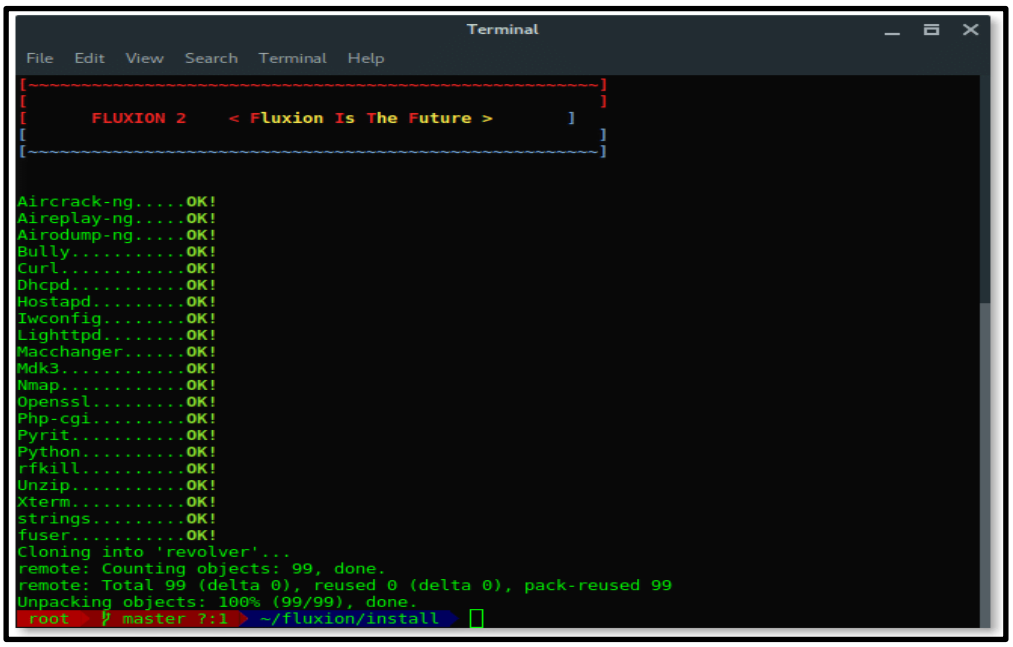
~# **cd fluxion/**

Update your Kali Linux system and install Fluxion dependencies packages by running install.sh script inside fluxion/install folder.

~# **cd install**

~# **./install.sh**

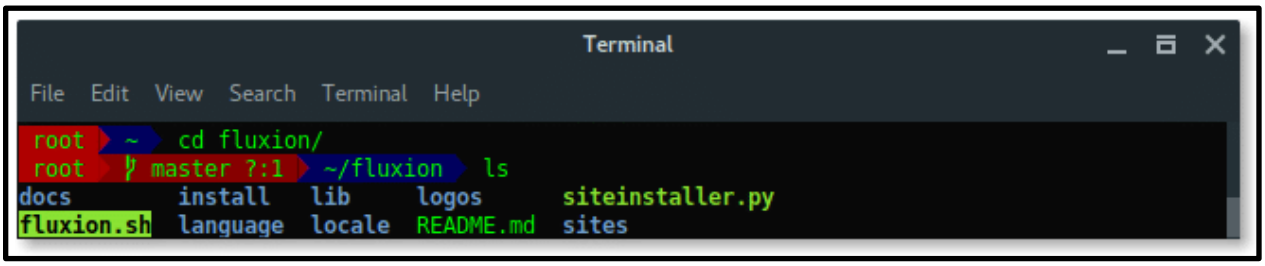
Once the installation succeeds, it should appear like this. Fluxion now is ready to use.



Launch Fluxion

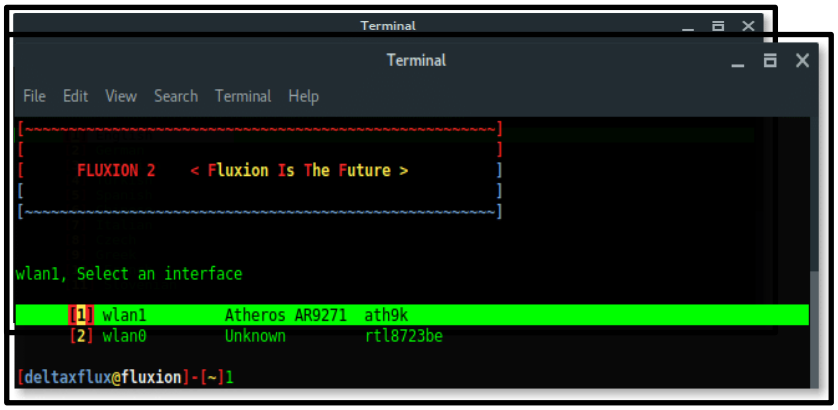
The main program of fluxion is fluxion.sh located under the main directory fluxion folder. To run fluxion, type:

~# **./fluxion.sh**



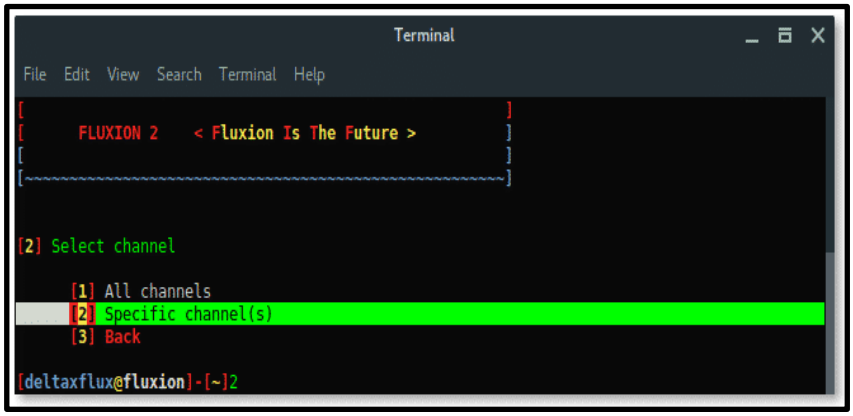
Setup & Configuration

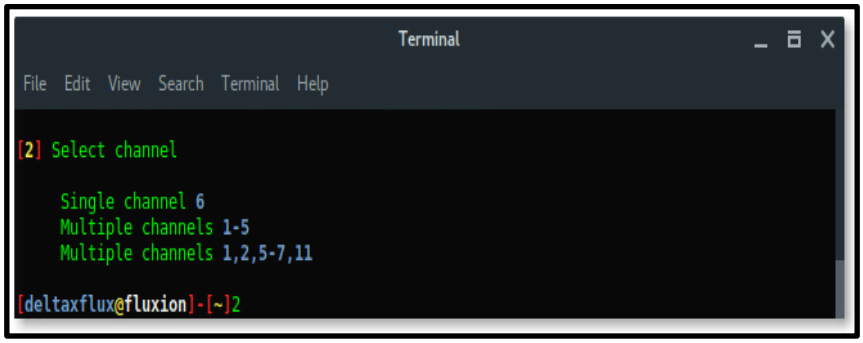
First, Fluxion will ask you to select language you preferred.



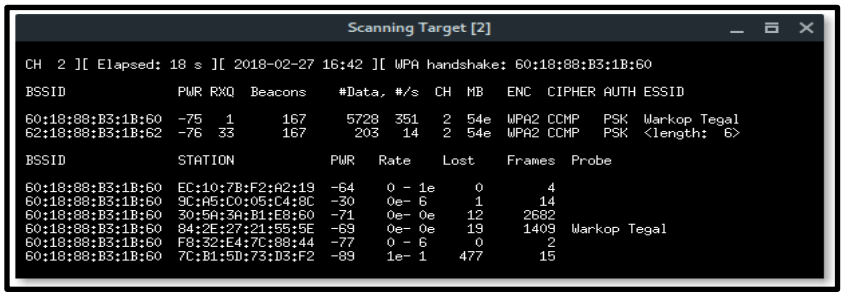
Then, select the **wireless card** you want to use, external wireless card is recommended.
Next, is select the channel, based on our target information above, the target is in channel 2. We choose Specific channel(s) then input the channel number.

Only choose All channels if you are not sure what the target channel is.

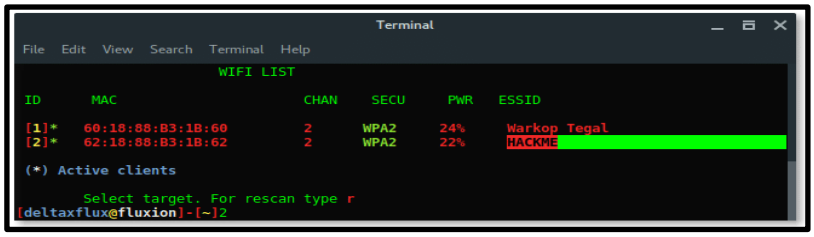




The xterm window will appear with airodump-ng program scanning the wireless network. Terminate by pressing **CTRL+C** whenever the target appears.

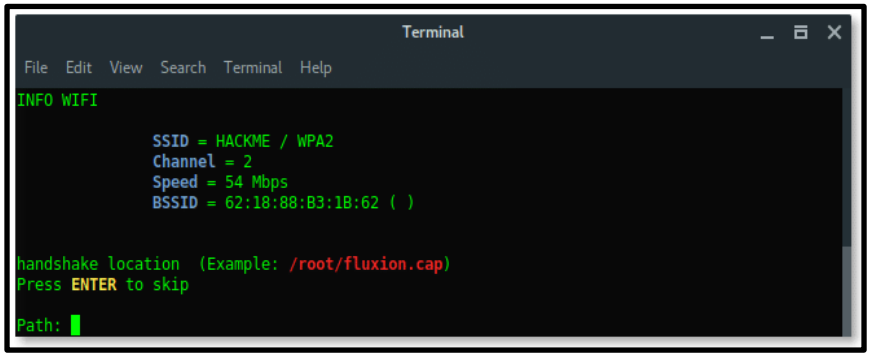


Fluxion will list all available targets. Choose the correct target based on the number in the list.



Next, select the FakeAP Attack Mode. Choose the recommended option **FakeAP – Hostapd**.

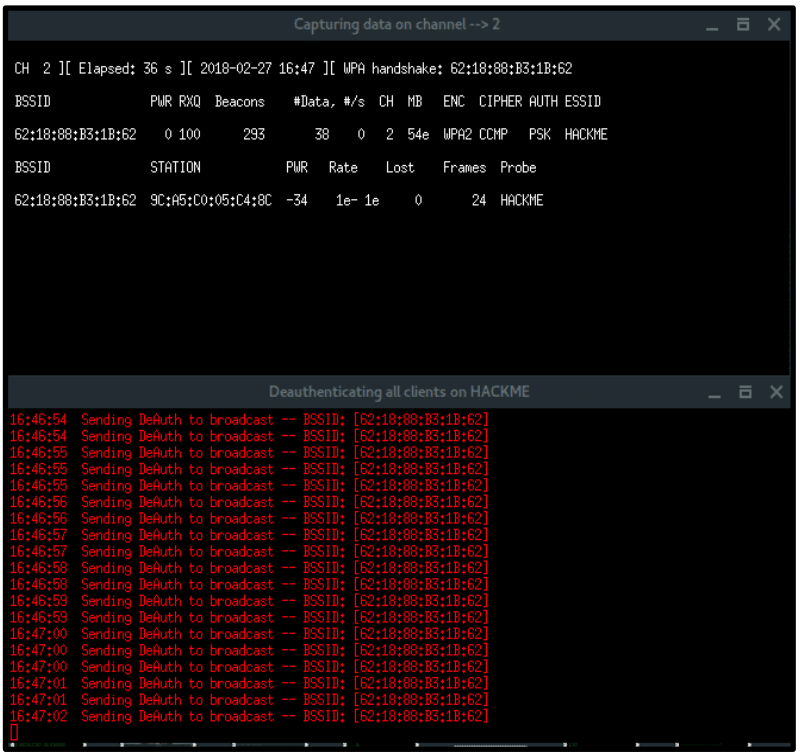
Then Fluxion will ask if we already have the handshake file. Just skip this process, let fluxion handle this for you, keep the file in place. Press **ENTER**.



Select the handshake verifier. Choose the recommended option **pyrit.**

Select deauth option, choose the safeway using Aireplay-ng option **[1] deauth all.**

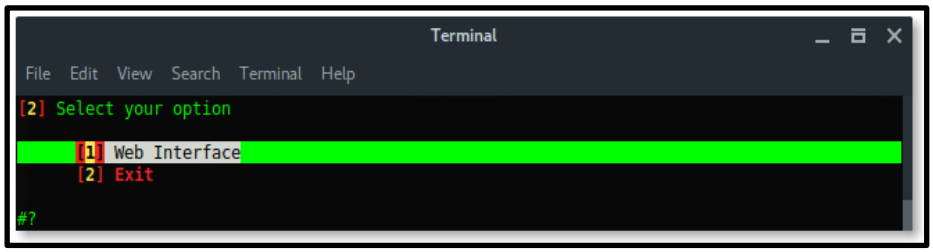
Then, another 2 xterm windows appear, first window is **airodump-ng** monitor which will try to capture handshake, while the second window is a **deauth attack** using aireplay-ng.



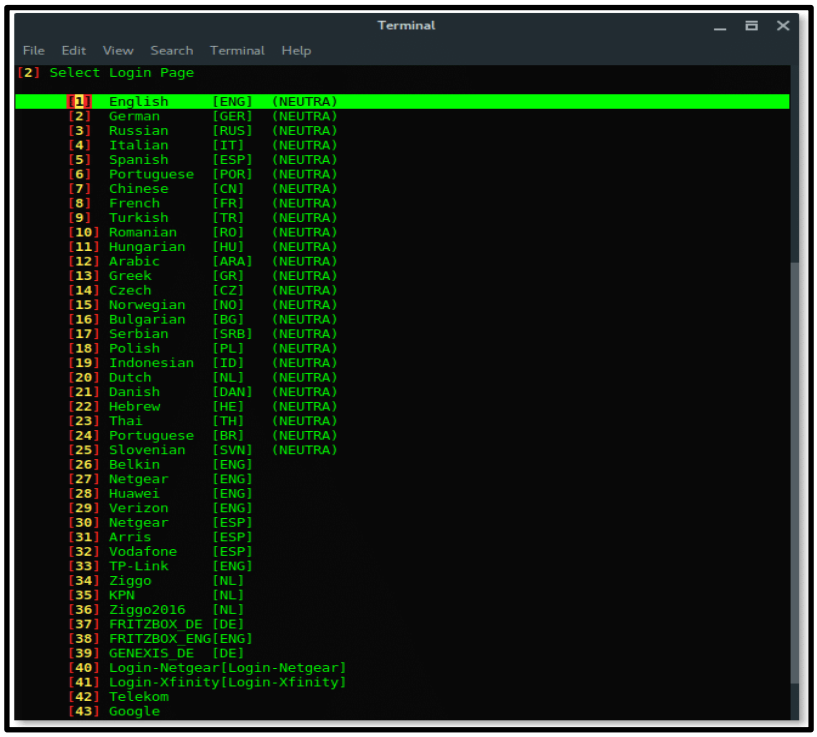
Notice, in the right-top corner of first window, when the handshake is captured (which says: **WPA HANDSHAKE xx:xx:xx:xx:yy:yy:yy**) just let these windows run in background. Back to the Fluxion window, choose option Check handshake to verify the handshake.If the handshake is valid, or corresponds to the target, then Fluxion will move to next process,

create SSL certificate for fake login.

Choose Web Interface. There are no other options, the only method is using a fake web login.

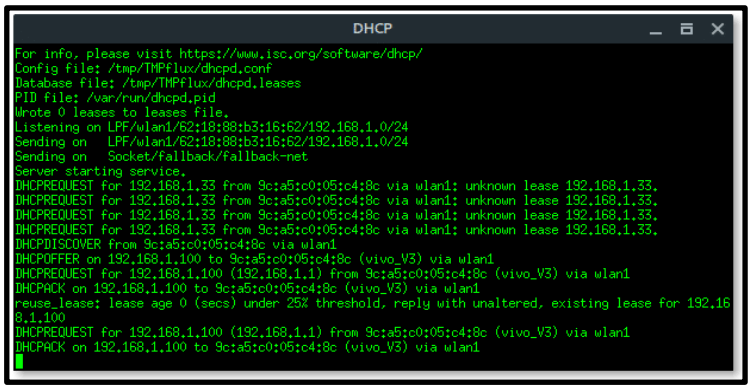


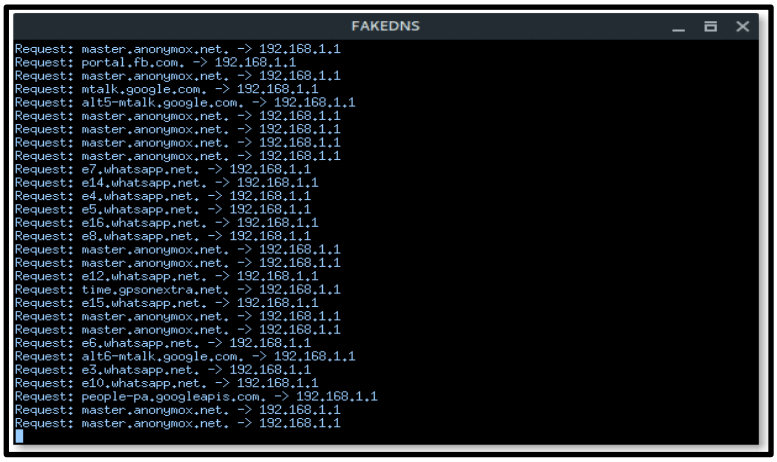
Next, choose the fake login template. To make your page look compromised set the proper template as the target firmware or region.

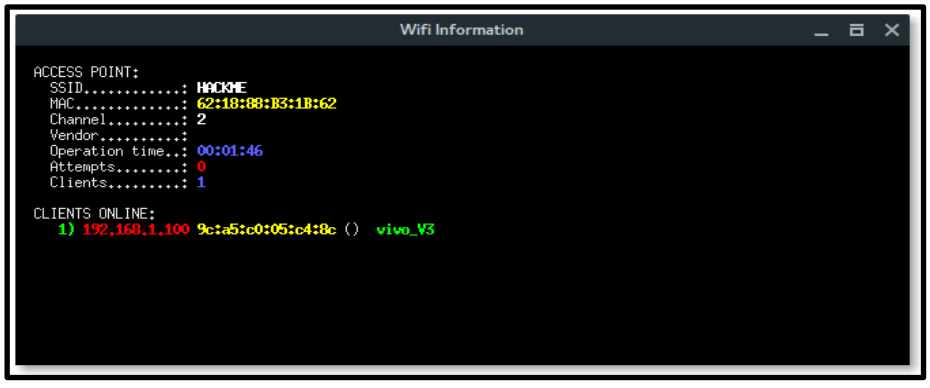


Alright, the setup is done. Now fluxion is ready to fish. Fluxion will make Fake AP, which has the same Wi-Fi information as the target, it is also called Evil Twin AP attack, but without any encryption or Open Connection. Let's read the log file and reveal the password.

More xterm windows will appear, DHCP server, DNS server, Deauth program, and the Wi-Fi information. Here, the deauth is to make sure the target clients are unable to connect to the original access point.





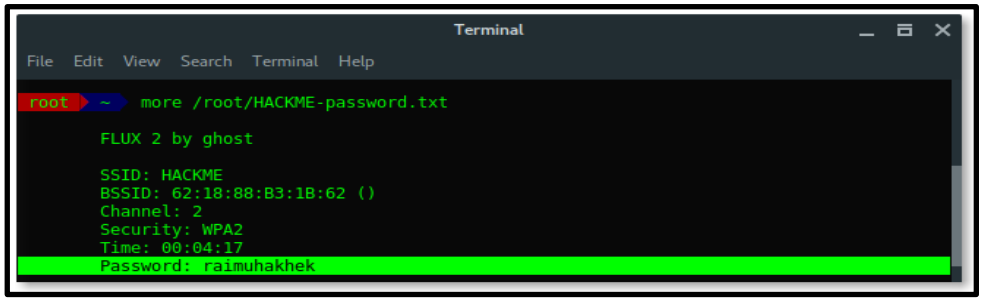


On the target client's side, they will notice there are two of the same "HACKME" Wi-Fi network, one is password protected (original), the other one is Open (Fake AP). If the target connects into

the Fake AP, especially if the user is using a mobile phone, it will redirect-automatically opening the Web Fake login like this.

Based on the result above, fluxion saves the log under **/root/[ESSID]-password.txt**.

Let's read the log file and reveal the password.



We have succeeded to reveal the hidden ESSID (access point name) and also the password using Fluxion in Kali Linux.

What is Wifite?

Wifite is a command-line tool, available on Kali Linux, to crack wireless network passwords. It's included with the essentials tools and can be used directly on a fresh installation of Kali Linux.

Wifite relies on different older tools, mostly the Aircrack-NG suite, making the process of scanning, auditing, and detecting Wi-Fi clients easier than ever. It can also be used to attempt password cracking using different methods.

Wifite supports cracking of WPA/WPA2, WEP and WPS networks, and the good news is that it can also be used to attack multiple networks at once.

In short, it's a simple and efficient tool that is commonly used by security professionals and ethical hackers to test the security of wireless networks. Let's see how it works now.

How to Install WiFite on Kali Linux

Run the following command to install WiFite:

sudo apt-get install wifite

It will install the WiFite and all packages.

Also, you can install WiFite onto your computer (from any terminal) by running:

sudo python setup.py install

In this way, you have installed wifite to /user/bin/wifite which is in your terminal path.

Use the commands below to install dependencies:

sudo apt-get install

sudo apt-get install aircrack-ng

sudo apt-get install reaver

sudo apt-get install pyrit

sudo apt-get install tshark

How To Run WiFite on Kali Linux

Type the following command to run WiFite:

git clone https://github.com/derv82/wifite2.git

cd wifite2

sudo ./Wifite.py

Usage of Wifite

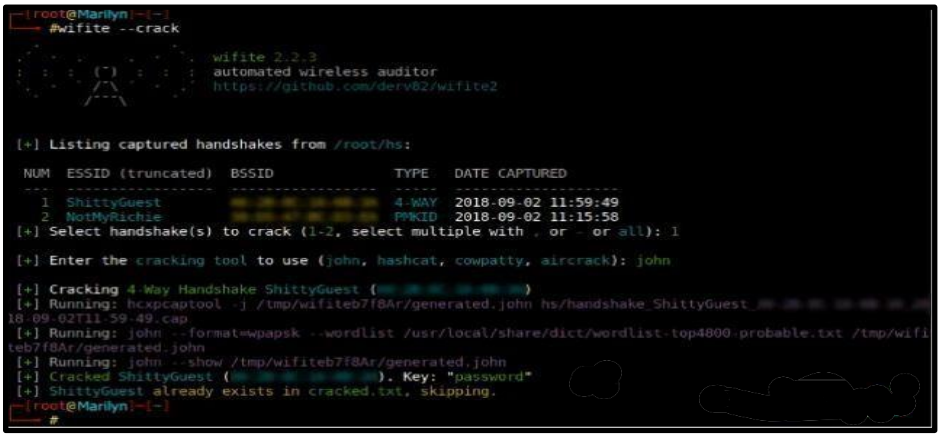
1- Cracking WPS PIN using reaver ‘s Pixie-Dust attack, then fetching WPA key using bully

2- Cracking WPA key using PMKID attack

3- Deauth and cracking a hidden access point

4- Cracking a weak WEP password

5- Cracking a pre-captured handshake using John the Ripper



What is WifiSlax?

Wifislax is a Slackware based-Linux distribution operating system (OS). It is designed for penetration testing on Wi-Fi and for practice of ethical hacking. It contains variety of Wi-Fi pentesting tools like Fluxion, Kismet, Aircarck, Airgeddon, MITM and lots of other tools in it.

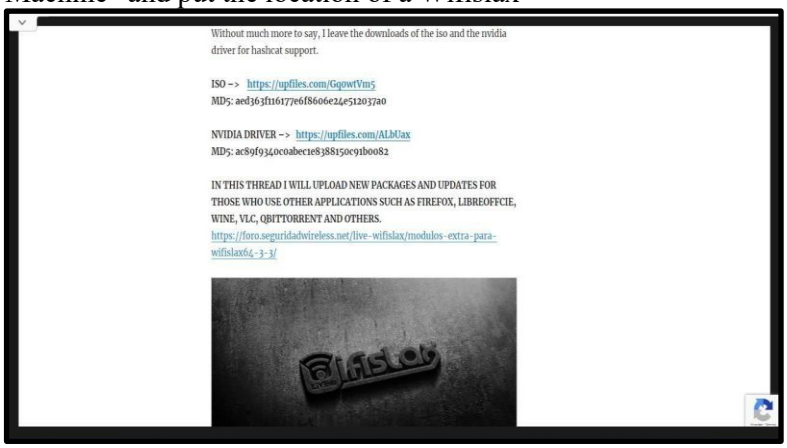
It can crack WEP, WPA, WPA2 protected Wi-Fi Networks. It has a command line interface. WPA Security is difficult to crack but still possible. WEP Networks are very easy to Crack. That's why, Nowadays, All Wi-Fi are WPA Supported.

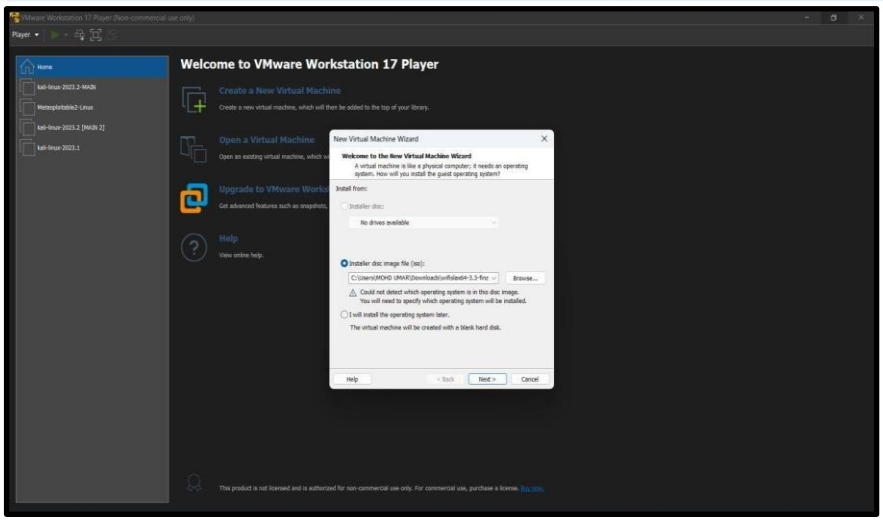
You can download Wifislax OS from official site www.wifislax.com and use it.

How to install Wifislax OS into our system with the help of VMware.

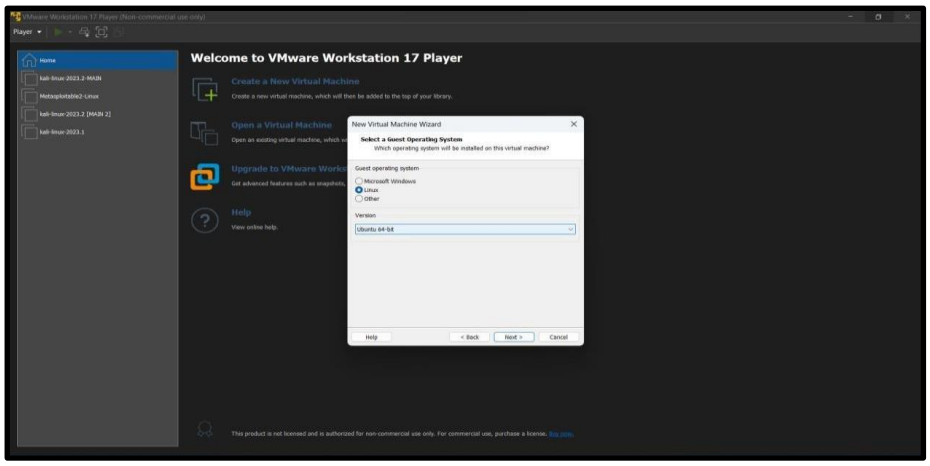
Step 01: First, we need to install **wifislax iso (.iso)** file for VMware from the WifiSlax official website → https://www.wifislax.com/

Step 02: After the file is download, open the VMware and select on the "Create a New Virtual Machine" and put the location of a Wifislax

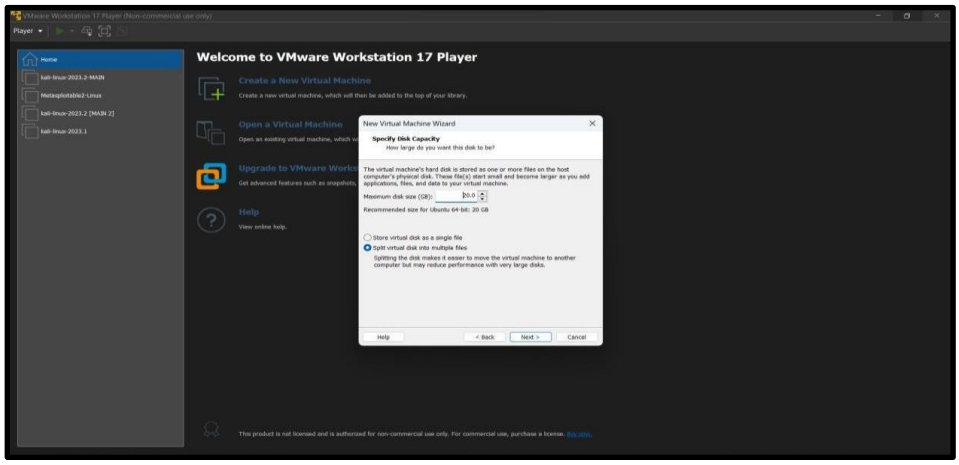




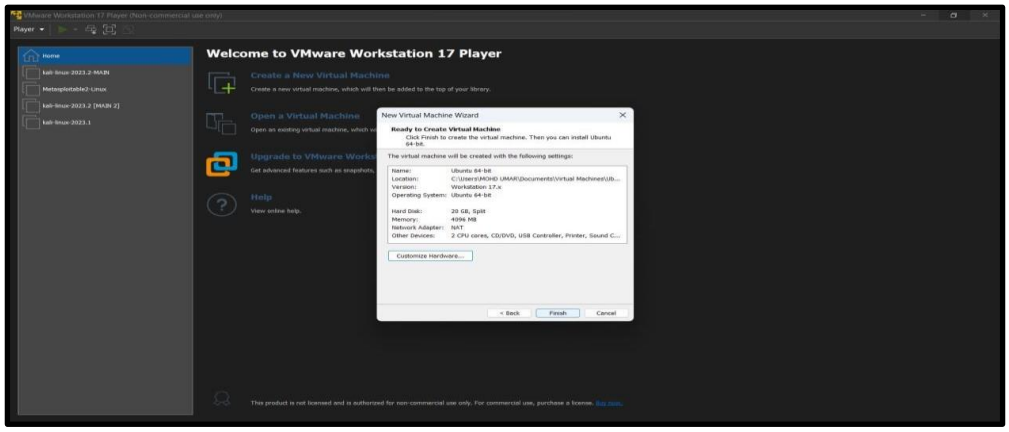
Step 03: Now, select the Linux Operating system and the "Ubuntu 64-bit" version and click "Next".



Step 04: Now Specify the Disk capacity that would be 20 GB or 10 GB.

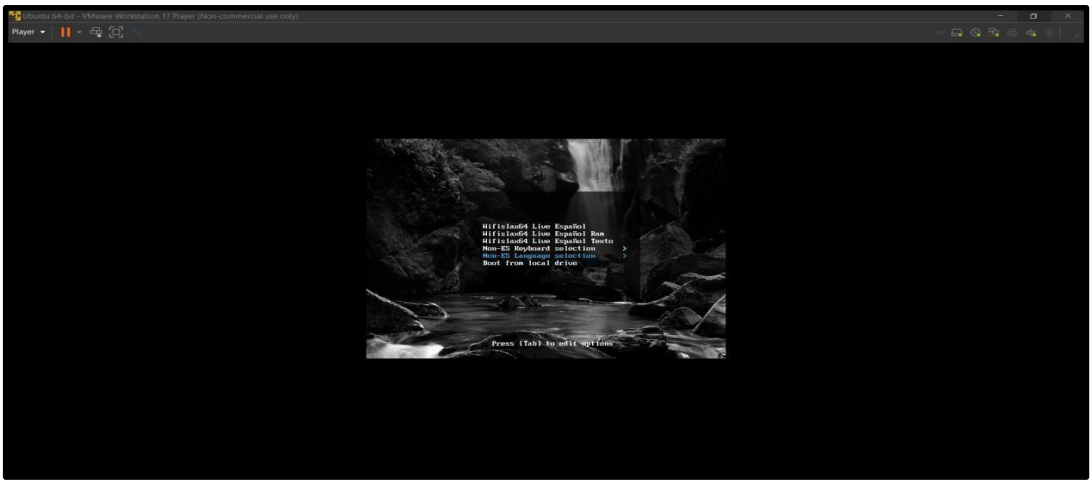


Step 05: After that you can Customize Hardware that would be RAM, CORE, etc.



Virtual Machine". It will run the WifiSlax.

Step 07: Now, go to the "Language Selection".



Step 08: Select the "British" language

Step 09: This interface will be shown when u first start or run the OS. You can change the display ratio.

Step 10: In window option you can see the "Wifislax" in that there are all the tools are there. Which we can use while performing wireless testing.

Usage of Wifislax OS.

WiFiSlax OS is primarily used for wireless penetration testing and security assessments of Wi-Fi networks. It provides a range of tools and utilities that can help security professionals, researchers, and ethical hackers identify vulnerabilities, weaknesses, and potential exploits in wireless networks. Here are some common use cases for WiFiSlax:

Wireless Network Assessment: WiFiSlax allows you to evaluate the security posture of wireless networks by detecting vulnerabilities such as weak encryption, default passwords, misconfigured access points, and other potential weaknesses.

Penetration Testing: Ethical hackers and penetration testers can use WiFiSlax to simulate real-world attacks on wireless networks in order to identify and fix security vulnerabilities before malicious actors exploit them.

Auditing and Compliance: WiFiSlax can be used to perform audits and compliance checks on wireless networks to ensure they adhere to industry standards and regulations, such as the Payment Card Industry Data Security Standard (PCI DSS) or other security frameworks.

Password Cracking: WiFiSlax provides tools that can be used to test the strength of Wi-Fi passwords and crack weak passwords, helping administrators identify and secure access points with inadequate security measures.

Network Monitoring: WiFiSlax includes tools for monitoring and capturing network traffic, which can be useful for analyzing network behavior, identifying suspicious activities, and understanding the flow of data within the network.

Security Research: Researchers can use WiFiSlax to experiment with and explore various wireless security concepts, protocols, and attacks in controlled environments.

Educational Purposes: WiFiSlax can be used for educational purposes, such as teaching students about wireless security, network vulnerabilities, and ethical hacking techniques in a hands-on manner.

Learning Outcomes: The student should have the ability to:

LO1: Perform Wi-Fi hacking using Fluxion tool.

LO2: Perform Wi-Fi hacking using Wifite tool.

LO3: Understand usage of WifiSlax OS.

Course Outcomes: Upon completion of the course students will be able to understand the concept of Wi-Fi hacking and Wireless Pentesting skills.

Conclusion: Through this experiment we learned the concept of Wi-Fi hacking and Wireless Pentesting using Fluxion and Wifite tool.

For Faculty Use:

Correction Parameters	Formative Assessment [40%]	Timely completion of Practical [40%]	Attendance / Learning Attitude [20%]	
Marks Obtained				