

# Hacking Wireless Networks MODULE-16

 by Durgesh Thakare

# Wireless Network

Wireless Networks are the networks which don't need to connect to any Network Peripheral. For eg. Bluetooths, WIFI etc. These Wireless Network came into existence because when we were using physical networks, it was very difficult to maintain and to spend expenses on various physical mediums required for establishing connection with end users used in Physical Network. Physical Medium includes Switches, Hubs, Cables, Connections, and Maintenances etc.

- **WIFI ALLIANCE:**

- The WiFi Alliance is an organization that oversees the development and implementation of Wi-Fi technology. It ensures compliance with standards and interoperability among different devices.

- **IEEE 802.11 Standard:**

- The IEEE 802.11 standard establishes rules and regulations for wireless networks, including Wi-Fi, enabling the use of the Internet. The term "WIFI" itself stands for Wireless Fidelity.

- **Router and DHCP:**

- Wireless networks, such as Wi-Fi, are facilitated through routers equipped with DHCP (Dynamic Host Configuration Protocol). The router manages the assignment of IP addresses to devices on the network. DLINK was one of the first companies to introduce wireless routers.

- **Need for Wireless Security:**

- With the widespread use of smart devices on wireless networks, security becomes paramount.
- Inadequately secured networks can lead to unauthorized access, manipulation, and illegal use.
- Hackers can exploit vulnerabilities for data interception, spread viruses, worms, Trojan horses, and engage in identity theft.

## Wireless Security Protocols:

- **WEP (Wired Equivalent Privacy):**

- **Introduction:** Developed in 1997, WEP aimed to provide wireless networks with privacy protection comparable to wired networks.
- **Security Mechanisms:** WEP used the RC4 algorithm and DES encryption. However, its fixed key made it susceptible to attacks.
- **Vulnerabilities:** WEP suffered from significant security flaws, allowing for key recovery and making it easy to break.

- **WPA (WiFi Protected Access):**

- **Introduction:** Introduced in 2003 as an improvement over WEP, WPA enhanced authentication and encryption features.
- **Security Improvements:** WPA introduced extra security mechanisms and algorithms, providing more robust protection against unauthorized access.
- **RADIUS Support:** WPA required support from RADIUS servers for user authentication.

- **WPA2 (WiFi Protected Access 2):**

- **Introduction:** Released in 2004, WPA2 maintained the security features of WPA but aimed for stronger encryption.
- **Encryption Technologies:** WPA2 utilized Temporal Key Integrity Protocol (TKIP) and Advanced Encryption Standard (AES) with Pre-Shared Keys (PSK) for enhanced security.

# Wireless Encryption Technologies:

## **AES (Advanced Encryption Standard):**

**Description:** AES is a symmetric block cipher chosen by the U.S. government for protecting classified information. It operates on blocks of data and uses a symmetric key algorithm.

**Application:** Used for securing various types of data, including passphrases and classified information.

## **DES (Data Encryption Standard):**

**Description:** DES is an outdated symmetric-key encryption method. It encrypts and decrypts messages using the same private key, requiring both the sender and receiver to possess the identical key.

**Application:** Historically used for data encryption, DES is now considered obsolete due to its susceptibility to modern cryptographic attacks.

## **TKIP (Temporal Key Integrity Protocol):**

**Description:** TKIP is an encryption protocol included in the IEEE 802.11 standard for wireless LANs (WLANs). It was designed to address the vulnerabilities found in WEP.

**Application:** TKIP is used to enhance the security of wireless communications, providing a more robust encryption mechanism.

## **PSK (Pre-Shared Key):**

**Description:** PSK is used in Wi-Fi encryption protocols such as WEP, WPA, and WPA2. In the context of WPA, it is referred to as WPA-PSK or WPA2-PSK. The key is shared between parties through a secure channel before use.

**Application:** Commonly used for securing Wi-Fi networks, requiring users to enter a pre-shared key for authentication.

## **CCMP (Counter Mode Cipher Block Chaining Message Authentication Code Protocol):**

**Description:** CCMP is an advanced data cryptographic encapsulation mechanism designed to ensure data confidentiality. It was created to address the vulnerabilities present in WEP, an outdated and insecure protocol.

**Application:** Used in conjunction with WPA2, CCMP provides a secure encryption method for protecting wireless communication. These encryption technologies play a crucial role in securing wireless networks, safeguarding data from unauthorized access and potential cyber threats.

# SECURITY CONFIGURATIONS

chillypannerr@234 → c#i77YP4n333@234

## Length and Complexity:

Example: chillypannerr@234 Explanation: Use a password with a minimum of 8 characters, combining uppercase and lowercase letters, numbers, and special characters. A longer and more complex password enhances security.

## Alphanumeric Mix:

Example: pASSwOrD Explanation: Include a mix of uppercase and lowercase letters in your password. This makes it more resistant to brute-force attacks and improves overall complexity.  
Incorporate Numbers:

Example: p3\$\$w0rd Explanation: Integrate numbers into your password to increase its strength. Avoid using easily guessable sequences or personal information.

## Special Characters:

Example: c#i77YP4n333@234 Explanation: Use special characters like @, #, or \$ to add an extra layer of complexity. This makes your password more challenging for attackers to guess.

## Avoid Common Words:

Explanation: Avoid using easily guessable words, names, or phrases. Instead, create unique combinations of characters that are not present in dictionaries commonly used for attacks. Avoid Personal Information:

Explanation: Refrain from using easily accessible personal information, such as birthdays, names, or addresses. Attackers often attempt to exploit personal details.

## Regularly Update Passwords:


Explanation: Change your passwords regularly to minimize the risk associated with compromised credentials. Regular updates enhance security by preventing long-term unauthorized access.

## Password Manager Usage:

Explanation: Consider using a reputable password manager to generate, store, and manage complex passwords. Password managers can help you maintain strong and unique passwords for each account.

## Check Password Strength:

Website: How Secure Is My Password Explanation: Use online tools like "How Secure Is My Password"

 howsecureismypassword.net



### How Secure Is My Password?

How long it would take a computer to crack your password?

to assess the strength of your passwords. These tools provide insights into the time it would take for a computer to crack your password.

# WORDLISTS GENERATOR

Crunch is a powerful tool included in Kali Linux that allows you to create custom wordlists based on specified criteria. Here's a guide on how to use Crunch to generate wordlists:

**Step 1:** Open a Terminal Open a terminal on your Kali Linux system. T.

**Step 2:** Understand Crunch Syntax Crunch has a specific syntax for generating wordlists. The basic structure is:

```
crunch <minimum length> <maximum length> <character set> -o <output file>
```

```
crunch 6 6 abcdefghijklmnopqrstuvwxyz -o wordlist.txt
```

# WIFI HANDSHAKE

The WiFi handshake is a crucial part of the process that ensures a secure connection between a wireless access point (AP) and a client device. The four-way handshake is designed to establish a connection while proving the authenticity of both the access point and the client. Here's an overview of the steps involved:

1. **Access Point Sends Nonce Packet to the Client:** The process begins with the access point (AP) sending a Nonce Packet to the client. A Nonce (number used once) is a random value generated for a specific session.
2. **Client Uses Nonce Packet for Authentication:** The client receives the Nonce Packet from the access point. The client uses the Nonce along with the pre-shared key (PSK) or other authentication credentials to create an Authenticator.
3. **Access Point Responds with Broadcasting and Multicasting Messages:** The access point responds with Broadcasting and Multicasting Messages to authenticate itself to the client. These messages contain information that verifies the access point's identity and establishes the connection.
4. **Client Accepts Broadcasting Packet and Responds with ACK:** The client accepts the broadcasting and multicasting packets from the access point. The client then responds with an Acknowledgment Packet (ACK) to confirm the successful receipt of the authentication messages. The ACK finalizes the four-way handshake, and the connection is established.

**Importance of the Four-Way Handshake:**

- Security:** The handshake ensures that both the access point and the client are legitimate and have the correct credentials.
- Protection Against Replay Attacks:** Nonces and other elements in the handshake help protect against replay attacks, where an attacker captures and attempts to reuse authentication data.
- Establishment of Encryption Keys:** The four-way handshake is also used to establish the keys necessary for encrypting the data exchanged during the session.
- Security Considerations:** The security of the WiFi network relies on the strength of the pre-shared key (PSK) or other authentication methods used during the handshake. It's crucial to use strong, unique passwords or authentication credentials to prevent unauthorized access.

Understanding the WiFi handshake is essential for security professionals, as it provides insights into the process of securing wireless communications and the potential vulnerabilities that attackers might exploit.

# CAPTURING WIRELESS COMMUNICATION PACKETS

In the context of wireless security and penetration testing, capturing wireless communication packets is a fundamental step in analyzing and assessing the security of a wireless network. Below are the details of capturing wireless packets using Kali Linux, a compatible external WiFi adapter, and essential tools such as Airmmon-ng and Airodump-ng.

**Attacker’s Machine:** Operating System: Kali Linux Wireless Adapter: Leoxsys External WiFi Adapter - 150HGN (<https://www.amazon.in/Leoxsys-150Mbps-Wireless-external-LEO-HG150N/dp/B00IWT1JA6>)

Tools: Airmmon-ng, Airodump-ng (Non-Graphical)

**Modes of Using a Wireless Adapter: Standard Mode |Managed Mode:**

This mode is used by the average user to connect to and use the services of a particular access point. In this mode, the wireless adapter functions as a regular client, connecting to WiFi networks.

**Monitoring Mode:**

Monitoring mode allows a computer with a wireless network interface controller to monitor all traffic received from the wireless network. In this mode, the adapter captures packets from all nearby devices, making it useful for security analysis and penetration testing.

**Terminologies:**

Understanding key terminologies related to wireless packet capture is crucial for effective analysis.

**Beacons:**

Number of beacons sent by the access point. Beacons are frames broadcast by access points to announce their presence.

**Data:**

Number of captured data packets, including data broadcast packets. In the context of WEP, this may refer to the unique IV (Initialization Vector) count.

**#s (Packets per Second):**

Number of data packets per second measured over the last 10 seconds. Indicates the data packet rate.

**CH (Channel):**

Channel number (taken from beacon packets). Represents the frequency channel used by the access point.

**MB (Maximum Speed):**

Maximum speed supported by the access point. May indicate short preamble support and QoS (Quality of Service) status.

**ENC (Encryption Algorithm):**

Indicates the encryption algorithm in use. Examples include OPN (no encryption), WEP, WPA, or WPA2.

**CIPHER:**

The cipher detected, such as CCMP, WRAP, TKIP, or WEP.

**AUTH (Authentication Protocol):**

The authentication protocol used, including MGT, SKA, or PSK.

**WPS (WiFi Protected Setup):**

Displayed when WPS (WiFi Protected Setup) is supported by the access point.

**ESSID (Extended Service Set Identifier):**

The name of the access point.

**BSSID (Basic Service Set Identifier):**

MAC address of the access point.

**Capturing Packets:**

Use Airmmon-ng to enable monitoring mode on the wireless adapter.

Use Airodump-ng to capture wireless packets, specifying the target access point's BSSID and channel.

The captured data is saved in files for further analysis. Capturing wireless communication packets is a foundational step in wireless security testing, allowing security professionals to assess vulnerabilities, analyze network traffic, and identify potential security risks.

# DEMONSTRATION

This demonstration outlines the steps for capturing wireless packets and subsequently cracking WEP and WPA/WPA2 WiFi passwords. The process involves using tools like Airmo-ng, Airodump-ng, Aireplay-ng, and Aircrack-ng on Kali Linux with a compatible wireless adapter.

### Opening Kali Machine and Using Tools:

Open a terminal in Kali Linux.

Use the following commands:

```
$ iwconfig
$ airmo-ng start wlan0 // Starting Monitoring Mode on wlan
$ airmo-ng kill PIDs
$ iwconfig - wlan0mon
```

### Start dumping packets using Airodump-ng:

```
$ airodump-ng wlan0mon // Start dumping on wlan0mon
$ airodump-ng --ssid -c -w wlan0mon // Start capturing and dumping packets, storing them on Kali OS.
```

**Requirements for Cracking Wireless Networks:** Operating System: Kali Linux Hardware Components: Wireless Adapter that supports Monitor Mode (Using "Leoxsys 150 HGN")

### Tools (CLI Tools Pre-Installed in Kali Linux):

- Airmo-ng: For enabling Monitor Mode.
- Airodump-ng: For dumping wireless fidelity packets.
- Aireplay-ng: For generating frames/packets and altering network packets. Aircrack-ng: For doing brute force attacks on WiFi captured packets using wordlists.

**Aireplay-ng:** Aireplay-ng is used to inject/replay frames, generating traffic for later use in Aircrack-ng.

### Aircrack-ng:

- Aircrack-ng is an 802.11 WEP and WPA/WPA2-PSK key cracking program.
- It can recover the WEP key once enough encrypted packets have been captured with Airodump-ng.
- Aircrack-ng uses statistical attacks, brute force, and dictionary methods to discover WEP and WPA/WPA2 keys.

## Workflow for Cracking WEP, WPA/WPA2:

### Check Wireless Adapter Name:

```
# iwconfig // Wireless Adapter Name wlan0
```

### Start Monitoring Mode:

```
# airmo-ng start wlan0 // Starting Monitoring Mode on Adapter
```

### Kill Processes:

```
# kill PID // Killing processes
```

### Check Adapter Name After Monitoring Mode:

```
# iwconfig // After Monotoring mode adapter name is : wlan0mon
```

### Start Dumping Packets:

```
# airodump-ng wlan0mon // Starting Dumping on Wireless Adapter
```

### Save Dumped Packets to a File:

```
# airodump-ng --ssid <Target Router's ssid> -c <channel number> -w wpa2 wlan0mon
```

Save the captured packets to a file (wpa2-01.cap) for further analysis.

- ssid: Router's MAC address
- c: Channel number
- w: Write/capture packets to a file

### Send Deauthentication Packets:

```
# aireplay-ng -0 10 -a <ssid of router> -c <ssid of client/user> wlan0mon
```

Send 10 deauthentication packets to the router's client/user. This action will prompt a reconnection, capturing the WiFi handshake.

- 0: Deauthentication packet
- a: MAC of the target router
- c: MAC of any connected client/user

### Start Dictionary Attack:

```
# aircrack-ng -w <path of dictionary> wpa2-01.cap
```

Initiate a dictionary attack using a wordlist (Rockyou.txt in this case) against the captured WiFi handshake packets.

- w: Path to the wordlist file
- wpa2-01.cap: Captured packets file



# Using Fern wifi cracker

## Key-Features of Fern WiFi Cracker:

WEP Cracking with Fragmentation,Chop-Chop, Caffè-Latte, Hirte, ARP Request Replay or WPS attack.

WPA/WPA2 Cracking with Dictionary or WPS based attacks. Automatic saving of key in database on successful crack.

Automatic Access Point Attack System.

Session Hijacking (Passive and Ethernet Modes).

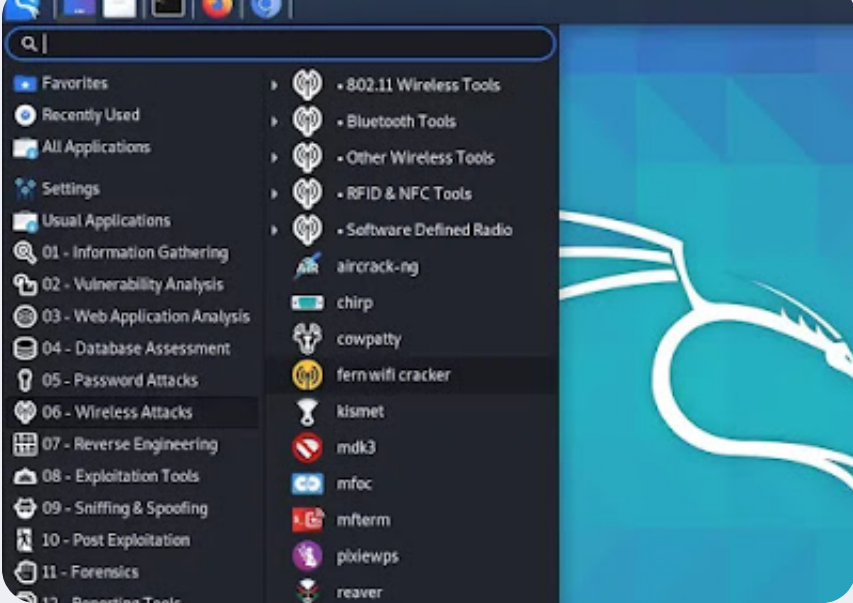
Access Point MAC Address Geo Location Tracking.

Internal MITM Engine.

Bruteforce Attacks (HTTP,HTTPS,TELNET,FTP).

## Using Fern in Kali Linux

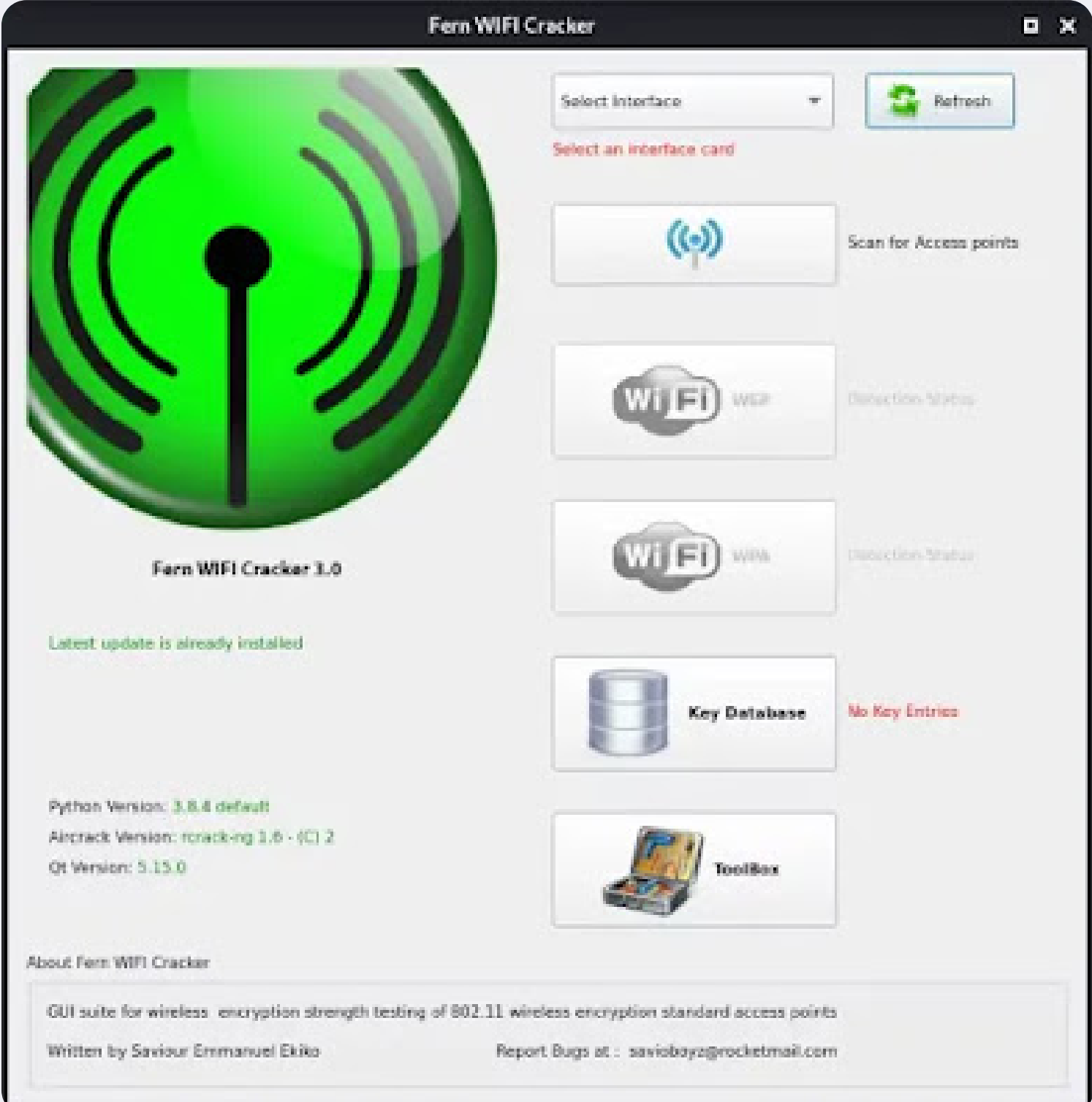
Fern WiFi cracker comes pre-installed with Kali Linux latest full version. We can run it from the Kali Linux application menu Wireless **Attacks > fern wifi cracker**.



Or we can run following command on our terminal to open Fern.

```
fern-wifi-cracker
```

It will ask us the sudo password to run because fern needs superuser access to do it's work. After providing it will run and we got it's main menu like following screenshot

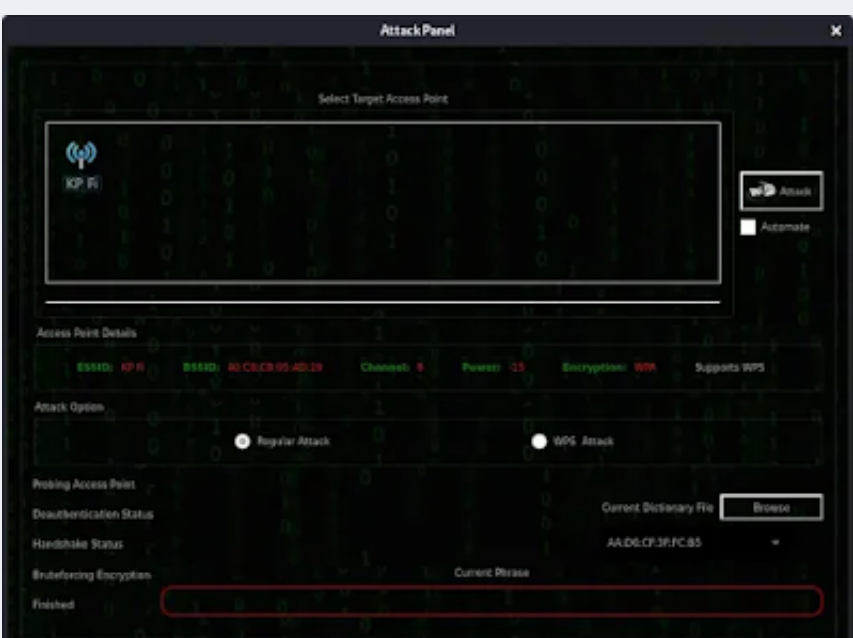


Now we select the network interface. Usually our devices internal WiFi is the wlan0 interface and to use monitor modes from our external WiFi adapter we need to select wlan1 interface, as we did in the following screenshot:

Now we need to click on the "Scan for Access Point" button then it will scan for nearby WiFi networks (WEP and WAP type of wireless protocols).



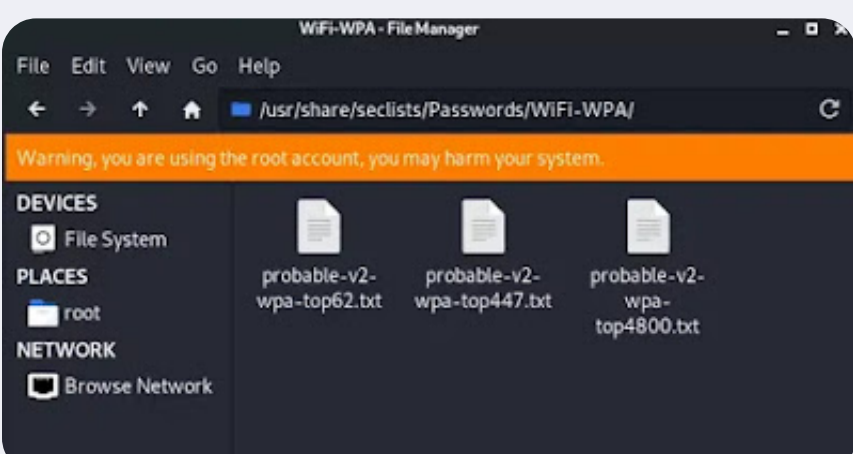
In the above screenshot we click on the on the 1 detected WiFi WPA button and we got the attack interface as following screenshot:



Now here we need to choose options to perform attack. We choose the attack type to "Regular attack". Then we choose the dictionary file to crack the WiFi password.

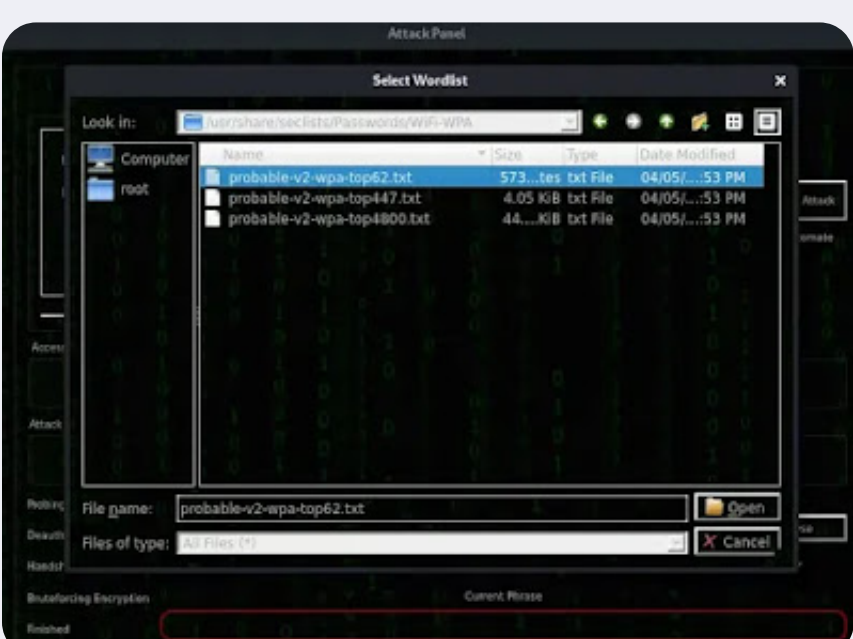
Here we need a dictionary file. A dictionary file/wordlist is a text file that contains lots of passwords. Our attack will follow the brute-force method first it capture the handshake file from the WiFi network then it try to crack the handshake file by brute-force method from our given password file. We will discuss about how it works later.

A bigger dictionary file or wordlist file provides us higher success rate but it may consume time. We can find a good dictionary file or wordlist file from the internet.



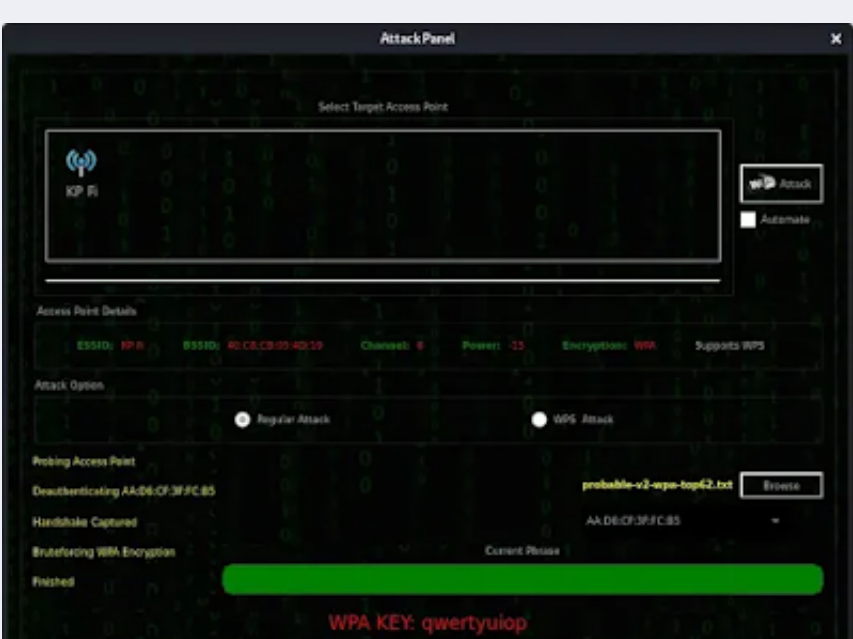
For our this example tutorial we are going to use one of these password lists.

So in the attack pane we choose one wordlist from this directory and click on open to select it.



Now we just need to click on the attack button. Rest everything will be done automatically.

After some time we got our targeted networks WiFi password.



Yes, we did it. We can see the password in red bold line on above screenshot.

Sometime after using this tool our network manager might down. To solve this we can do a restart or use following command:

```
sudo service network-manager restart
```

# Using Fluxion

```
git clone git@github.com:FluxionNetwork/fluxion.git
```

## Switch to tool's directory

```
cd fluxion
```

## Run fluxion (missing dependencies will be auto-installed)

```
./fluxion.sh
```

- Scan for a target wireless network.
- Launch the Handshake Snooper attack.
- Capture a handshake (necessary for password verification).
- Launch Captive Portal attack.
- Spawns a rogue (fake) AP, imitating the original access point.
- Spawns a DNS server, redirecting all requests to the attacker's host running the captive portal.
- Spawns a web server, serving the captive portal which prompts users for their WPA/WPA2 key.
- Spawns a jammer, deauthenticating all clients from original AP and luring them to the rogue AP.
- All authentication attempts at the captive portal are checked against the handshake file captured earlier.
- The attack will automatically terminate once a correct key has been submitted.
- The key will be logged and clients will be allowed to reconnect to the target access point.