

Wifi Hacking

GUI Based Automated Wifi cracking



FERN is a Wireless security auditing and attack software program written using the Python Programming Language and the Python Qt GUI library

The program is able to crack and recover WEP/WPA/WPS keys in a GUI based environment in a **click and forget** manner

FERN



WIFITE

Step- 1

- ❖ Prepare the dictionary file for FERN. Locate the dictionary file

> Locate rockyou

```
(kali@kali)-[~]
└─$ locate rockyou
/usr/share/hashcat/masks/rockyou-1-60.hcmask
/usr/share/hashcat/masks/rockyou-2-1800.hcmask
/usr/share/hashcat/masks/rockyou-3-3600.hcmask
/usr/share/hashcat/masks/rockyou-4-43200.hcmask
/usr/share/hashcat/masks/rockyou-5-86400.hcmask
/usr/share/hashcat/masks/rockyou-6-864000.hcmask
/usr/share/hashcat/masks/rockyou-7-2592000.hcmask
/usr/share/hashcat/rules/rockyou-30000.rule
/usr/share/john/rules/rockyou-30000.rule
/usr/share/wordlists/rockyou.txt.gz
```

Step- 1

❖ Now Un compress the file

- `gunzip /usr/share/wordlists/rockyou.txt.gz`
- `ls /usr/share/wordlists/`

```
(kali㉿kali)-[~]  
└─$ gunzip /usr/share/wordlists/rockyou.txt.gz
```

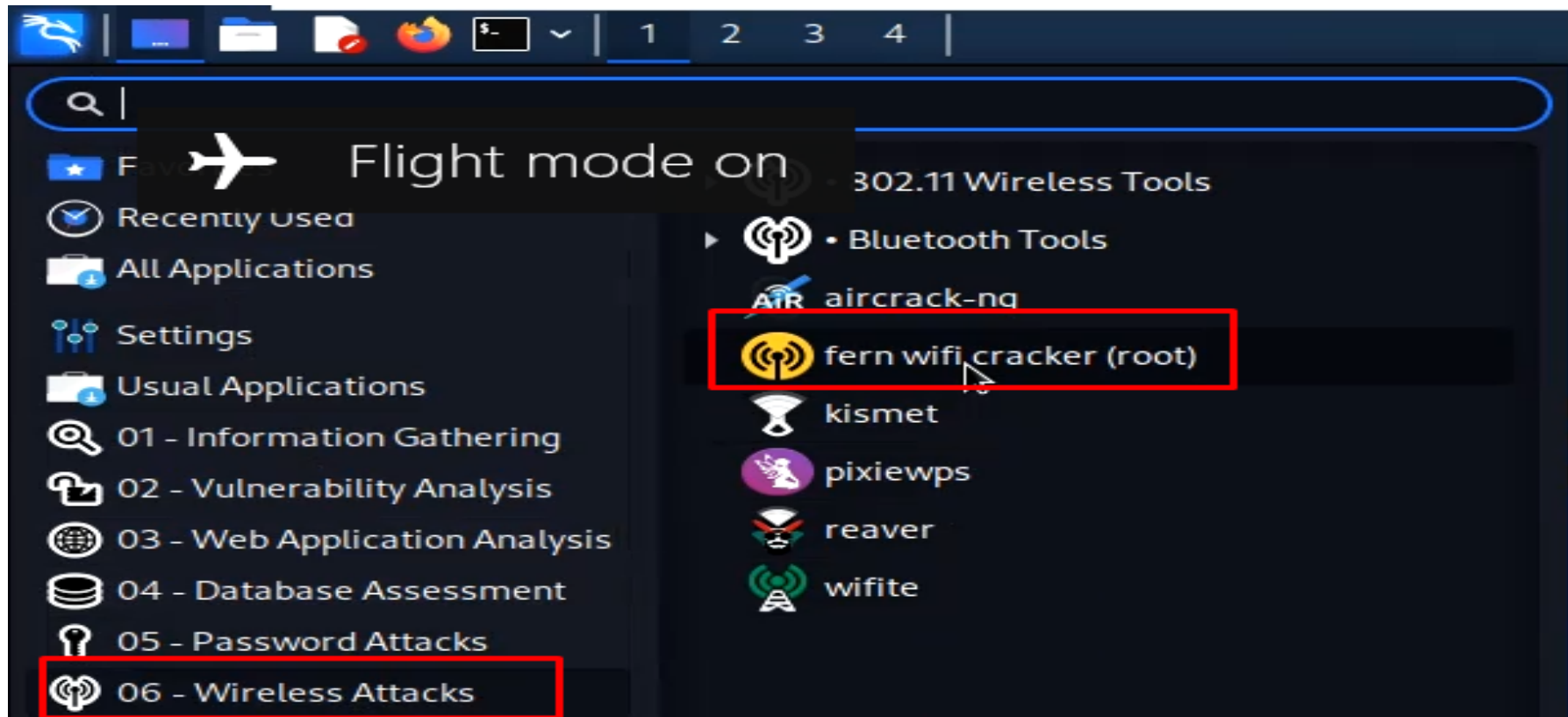
```
(kali㉿kali)-[~]  
└─$ ls /usr/share/wordlists/  
  
dirb  dirbuster  fasttrack.txt  fern-wifi  metasploit  nmap.lst  rockyou.txt  wfuzz
```

Best Alternate Word lists Collections.

- ✓ <https://weakpass.com/>
- ✓ <https://github.com/danielmiessler/SecLists/tree/master/Passwords/WiFi-WPA>
- ✓ <https://labs.nettitude.com/blog/rocktastic/>
- ✓ <https://github.com/kennyn510/wpa2-wordlists>

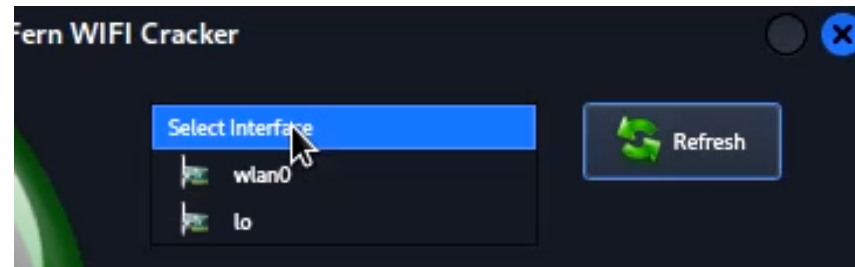
Step- 2

- ❖ Open FERN from Programs > Wireless Attacks > FERN



Step- 3

- ❖ Select your Interface, FERN will automatically put it in monitor mode



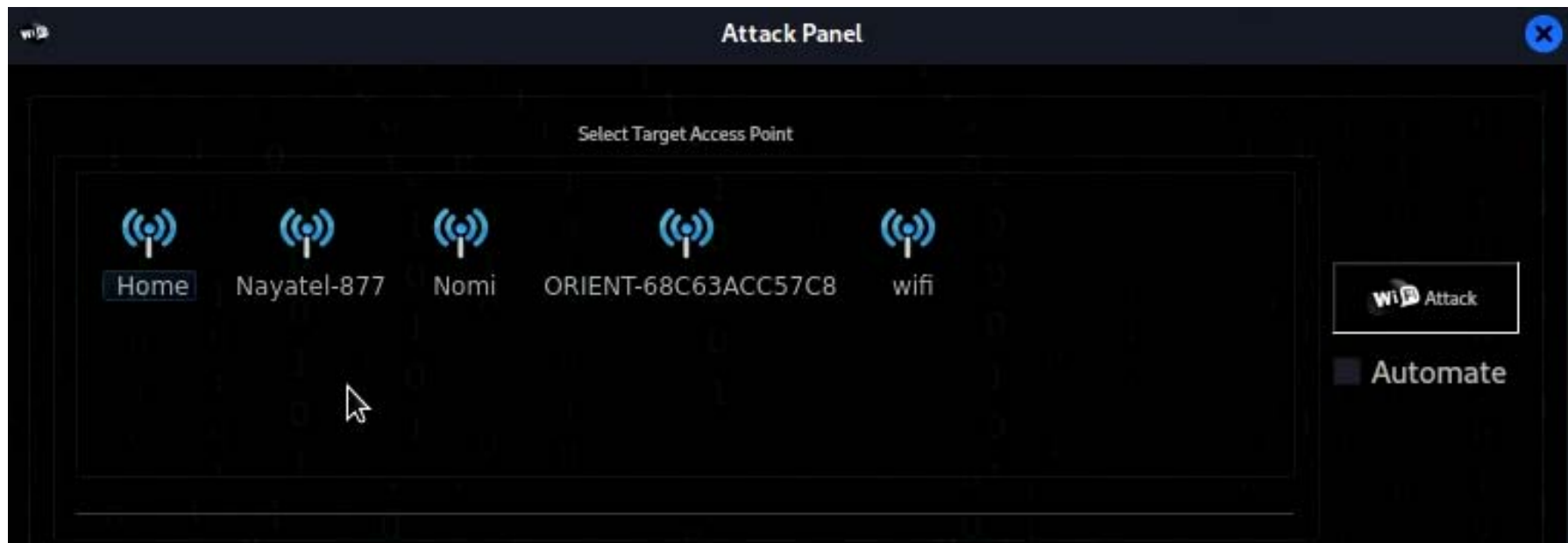
Step- 4

- ❖ Now Start Scanning, FERN will show the number of WEP and WPA networks that it finds



Step- 5

- ❖ Now Select WPA Networks and Here a new Window will appear listing all WPA/ WPA-2 networks



Step- 6

- ❖ Now you need to select the dictionary. Open the dictionary tab and select the Rockyou.txt from the following location

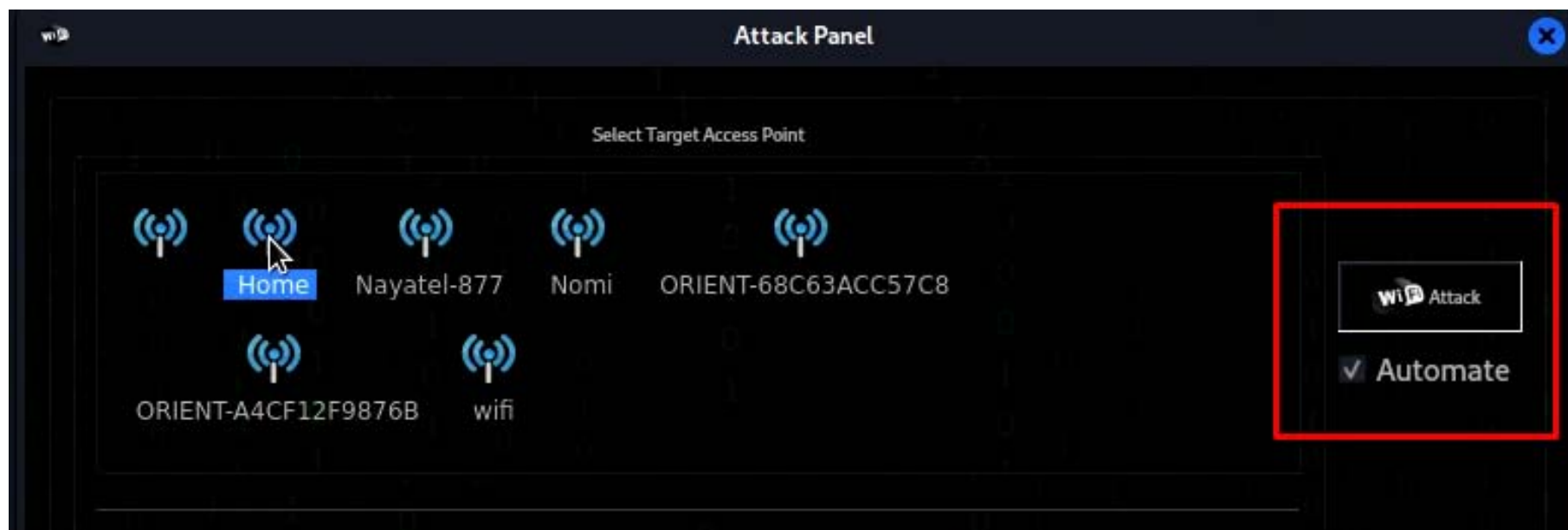
➤ /usr/share/wordlists/



The screenshot shows a dark-themed interface for configuring a network attack. The 'Access Point Details' section displays: ESSID: Home, BSSID: C0:F6:C2:5E:8D:20, Channel: 6, Power: -78, Encryption: WPA, and Supports WPS. Under 'Attack Option', 'Regular Attack' is selected. The 'Probing Access Point' section shows 'rockyou.txt' and a 'Browse' button, which is highlighted with a red box. Below this, 'Deauthentication Status', 'Handshake Status' (FC:19:99:58:48:73), and 'Bruteforcing Encryption' are visible. A 'Current Phrase' field is at the bottom, and a 'Finished' status is indicated at the very bottom.

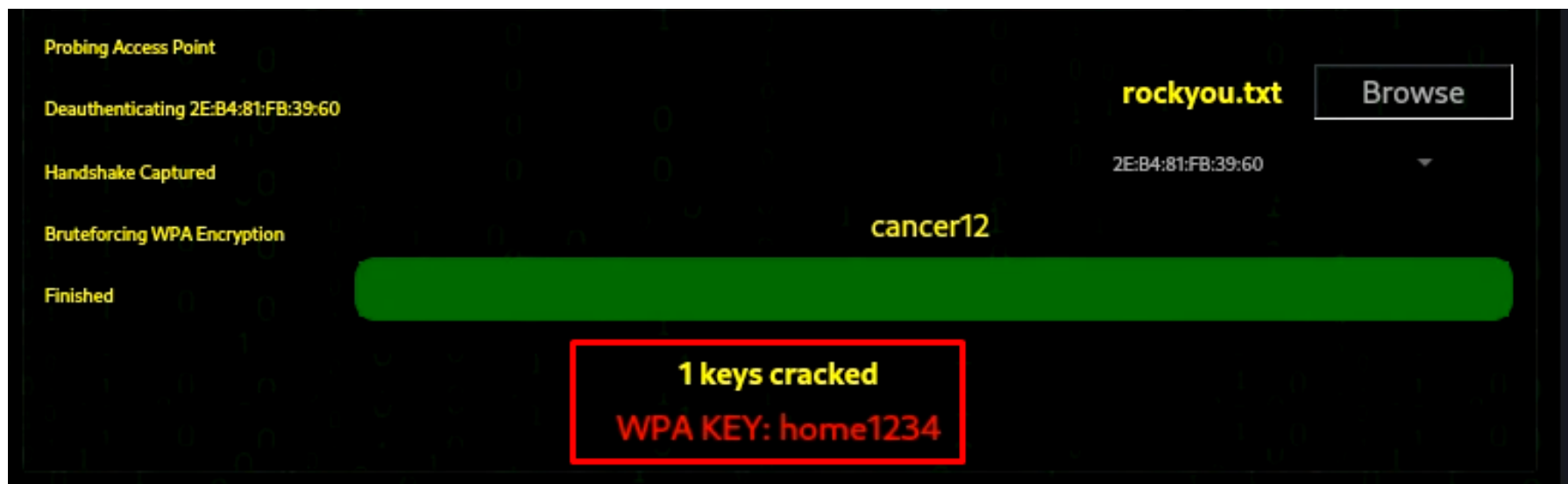
Step- 7

- ❖ Now Select the target network, select option to automate and click attack



Step- 8

- ❖ FERN will automatically disassociate the clients, capture the handshake and then crack the handshake. Once cracked, the password will be displayed





DEMO

A photograph of a body of water with mountains in the background and a small structure on the right. The word 'THANKS' is overlaid in the center.

THANKS