**WPA2 Handshake Capture & Cracking Report**

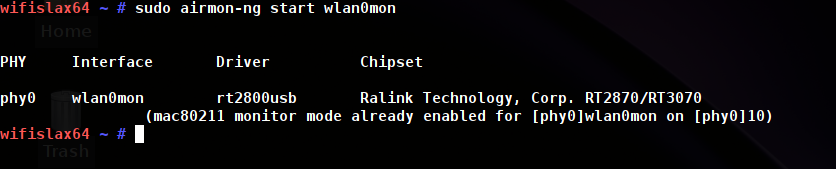
**Student Name:** M.Murtaza   
**Course:** Vulnerability assessment & reverse engineering  
**Instructor:** Muhammad Siddique  
**Date:** 3/23/2025

**1. Introduction**

This report documents the process of capturing a WPA2 handshake from a Wi-Fi network and subsequently cracking the password using dictionary attacks. The goal was to understand wireless security vulnerabilities and how attackers might exploit them.

**2. Tools Used**

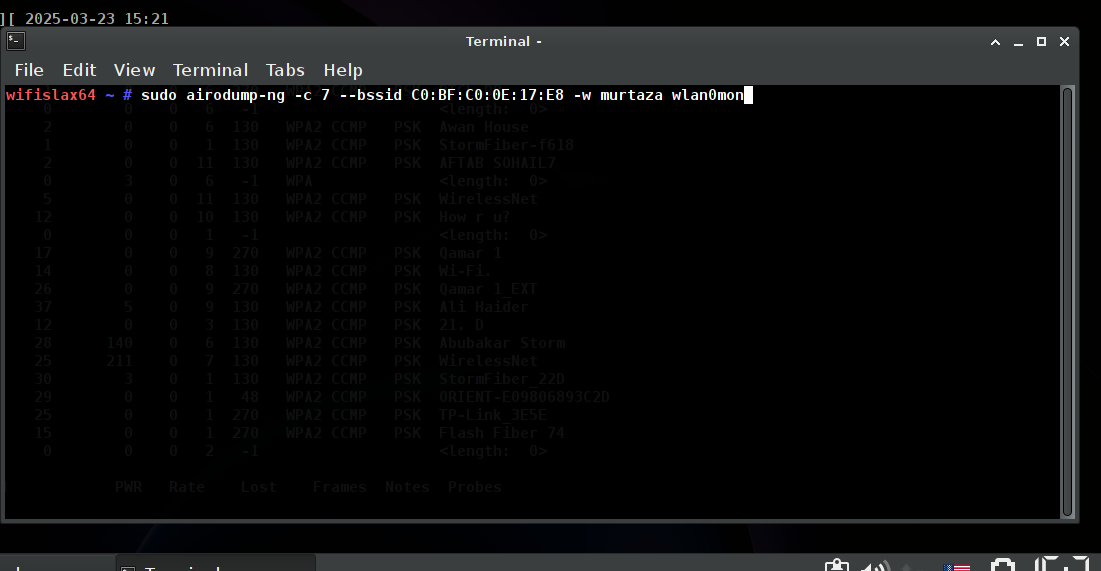
* **Operating System:** Kali Linux (Live Boot / Virtual Machine / Dual Boot)
* **Wi-Fi Adapter:** Alfa AWUS036NH (Supports Monitor Mode & Packet Injection)
* **Software Tools:**
  + airmon-ng (Enable monitor mode)
  + airodump-ng (Capture handshake)
  + aireplay-ng (Deauthentication attack)
  + aircrack-ng (Crack password using dictionary attack)
  + hashcat (Alternative GPU-based cracking tool)

**Step 1: Enabling Monitor Mode** sudo airmon-ng start wlan0   
  


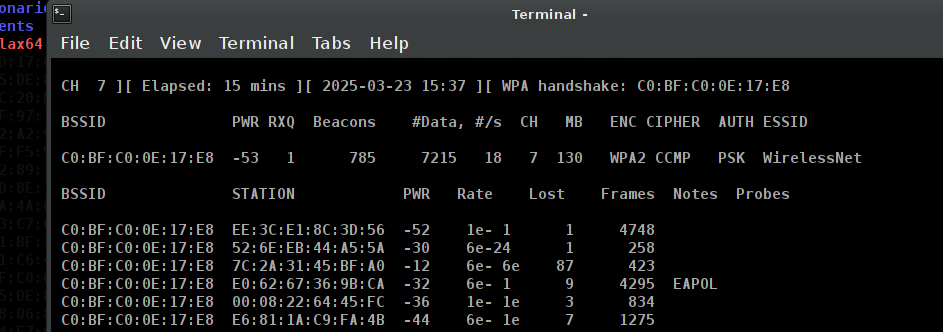
**Step 2: Capturing Handshake**

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

* <channel> refers to the Wi-Fi channel of the target network.
* <BSSID> is the MAC address of the target Wi-Fi.



**Step 4: Verifying Handshake Capture**



**4. Cracking the Captured Handshake**

**Using Aircrack-ng with a Dictionary Attack**

aircrack-ng -a2 -b <BSSID> -w rockyou.txt handshake.cap

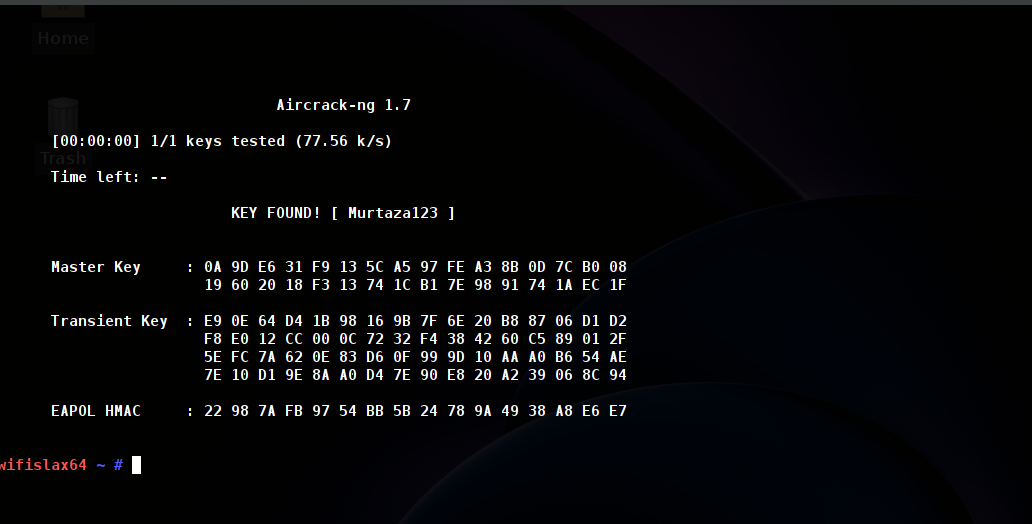
* -a2 specifies WPA2.
* -w rockyou.txt is the wordlist used for cracking.

**Using a Custom Wordlist**

If the password is not in rockyou.txt, a custom wordlist can be used:

echo "Murtaza123" > mylist.txt

aircrack-ng -a2 -b <BSSID> -w mylist.txt handshake.cap



**5. Results & Observations**

* The handshake was successfully captured after forcing a client to reconnect.
* The first dictionary attack failed because rockyou.txt did not contain the correct password.
* The password was successfully cracked after adding Murtaza123 to the custom wordlist.

**6. Conclusion & Security Recommendations**

This exercise demonstrated how WPA2 handshakes can be captured and cracked using dictionary attacks. To protect against such attacks, users should:

* Use a strong password (at least 12+ characters, including special symbols).
* Enable **WPA3** security if available.
* Use MAC address filtering to restrict device connections.
* Enable **Protected Management Frames (PMF)** to prevent deauthentication attacks.
* Regularly monitor for unauthorized connections using security tools.

**7. References**

1. Aircrack-ng Documentation: https://www.aircrack-ng.org/
2. Hashcat WPA2 Cracking Guide: https://hashcat.net/wiki/
3. Wireless Security Best Practices: https://www.cisa.gov/

**End of Report**