WIFI HACKING 101

EXP.NO: 13   **DATE:08-04-2025**

AIM:

        To understand and demonstrate how to capture and crack WPA/WPA2 personal Wi-Fi passwords using Aircrack-ng tools.

ALGORITHM:

1. Put the wireless interface into monitor mode.

2. Capture the 4-way handshake using airodump-ng.

3. (Optional) Deauthenticate a connected client to trigger handshake.

4. Use aircrack-ng with a wordlist to brute-force the password.

5. (Optional) Convert capture to HCCAPX format for GPU-based cracking with Hashcat.

OUTPUT:

Answer the questions below

What type of attack on the encryption can you perform on WPA(2) personal?

| brute force | ✓ Correct Answer | ♀ Hint |

Can this method be used to attack WPA2-EAP handshakes? (Yea/Nay)

| Nay | ✓ Correct Answer |

What is the three-letter abbreviation for the pre-shared key used in Wi-Fi security?

| PSK | ✓ Correct Answer |

What's the minimum length of a WPA2 Personal password?

| 8 | ✓ Correct Answer |

How do you put the interface "wlan0" into monitor mode with Aircrack tools? (Full command)

airmon-ng start wlan0   ✓ Correct Answer

What is the new interface name likely to be after you enable monitor mode?

wlan0mon   ✓ Correct Answer

What do you do if other processes are currently trying to use that network adapter?

airmon-ng check kill   ✓ Correct Answer   ♀ Hint

What tool from the aircrack-ng suite is used to create a capture?

airodump-ng   ✓ Correct Answer

What flag do you use to set the BSSID to monitor?

--bssid   ✓ Correct Answer   ♀ Hint

And to set the channel?

--channel   ✓ Correct Answer   ♀ Hint

And how do you tell it to capture packets to a file?

-w   ✓ Correct Answer   ♀ Hint

What flag do we use to specify a BSSID to attack?

-b   ✓ Correct Answer   ♀ Hint

What flag do we use to specify a wordlist?

-w   ✓ Correct Answer   ♀ Hint

How do we create a HCCAPX in order to use hashcat to crack the password?

-j   ✓ Correct Answer   ♀ Hint

Using the rockyou wordlist, crack the password in the attached capture. What's the password?

greeneggsandham   ✓ Correct Answer   ♀ Hint

Where is password cracking likely to be fastest, CPU or GPU?

GPU   ✓ Correct Answer   ♀ Hint

RESULT:

In this experiment, we demonstrated the process of capturing and cracking WPA2 Passwords using tools like Air cracking and Hashcat. The experiment also highlighted that GPU-based cracking is faster than CPU-based cracking.