WIFI HACKING 101

EXP.NO: 13

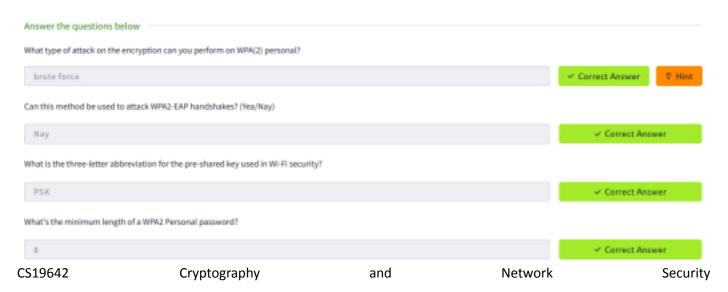
AIM:

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:



How do you put the interface "wlan0" into monitor mode with Aircrack tools? (Full command) ✓ Correct Answer airmon-ng start wlan0 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 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 9 Hint And to set the channel? --channel ✓ Correct Answer 0 Hint And how do you tell it to capture packets to a file? ✓ Correct Answer What flag do we use to specify a BSSID to attack? ✓ Correct Answer What flag do we use to specify a wordlist? Correct Answer 0 Hint How do we create a HCCAPX in order to use hashcat to crack the password? Correct Answer 0 Hint Using the rockyou wordlist, crack the password in the attached capture. What's the password? greeneggsandham ✓ Correct Answer 0 Hint Where is password cracking likely to be fastest, CPU or GPU?

RESULT:

GPU

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.

✓ Correct Answer