***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?***

ESSID: targetnetwork

Commands:

sudo airmon-ng

sudo airmon-ng start wlan0

sudo airmon-ng check kill

iwconfig (check monitor mode)

sudo airodump-ng wlan0mon

sudo airodump-ng -c 6 --bssid '' -w ~/wpafile1 wlan0 ??

??

***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 network card listens to every packet in the air. Managed mode is the default mode where the card will only capture packets that have its MAC address as the destination MAC.

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

WPA can be cracked when the network interface card can capture the handshake key. This means that it can launch an attack e.g. dictionary attack to try and crack the WPA key.

***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.***

***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]***

***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]***

***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 Processing powerful CPU

***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)***

***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)***

***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, wheras WPA uses 20 characters = 160 bits making it 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.