Question **1**

Answer saved

Marked out of 2.50

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

'Beacons' are beacon frames, which are periodically transmitted by the AP. They contain the information about the network, used for announcing the presence of WLAN and synchronizing the users.

Question **2**

Answer saved

Marked out of 10.00

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]

I will send disassocate packets to one or more clients which are currently associated with a particular access point

aireplay-ng --deauth 0 -c [DEVICES MAC ADDRESS] -a [ROUTERS MAC ADDRESS] wlan0mon

The 0 represents an infinite amount of deauth attacks.
-c is the client, what you're attacking.
This is the devices MAC address. -a is the router, what is the router the victim is connected to.
wlan0mon is the name of the network card still in monitor mode.

Question **3**
Not yet answered
Marked out of 5.00

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]

aireplay-ng -0 0 -a [AP MAC ADDRESS] -c [Windows machine MAC address] wlan0

-0 means deauthentication attack mode
use 0 (the second zero) for infinite deauths
wlan0 is the NIC (Network Interface Card)

Question **4**
Answer saved
Marked out of 5.00

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

1. add more possible password in the dictionary
2. Capturing WPA/WPA2 handshakes by forcing clients to reauthenticate which can capture more handshake packets

Question **5**
Answer saved
Marked out of 5.00

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 for providing the transport and usage of keying material and parameters generated by EAP methods.
There are 5 types of EAPs that are supported by WPA/WPA2 which are:
EAP-TLS (originally certified protocol)
EAP-TTLS/MSCHAPv2
PEAPv0/EAP-MSCHAPv2
PEAPv1/EAP-GTC
EAP-SIM

Question **6**

Answer saved

Marked out of 2.50

- 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)

Wardriving is the act of searching for Wi-Fi wireless networks by a person usually in a moving vehicle, using a laptop or smartphone.

iStumbler
InSSIDer
Kismet
KisMAC

false
although turning off the SSID broadcast can be hidden, the communication between client and AP also can be detected by the tools above.

Question **7**

Answer saved

Marked out of 2.50

Briefly describe the process involved in cracking WEP?

(Common interview question, 5-7 lines)

Start the wireless interface in monitor mode on the specific AP channel
Test the injection capability of the wireless device to the AP
Use aireplay-ng to do a fake authentication with the access point
Start airodump-ng on AP channel with a bssid filter to collect the new unique IVs
Start aireplay-ng in ARP request replay mode to inject packets
Run aircrack-ng to crack key using the IVs collected

Question **8**

Answer saved

Marked out of 5.00

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

1.WPA2 requires you to enter a longer password than WPA requires.
2.WPA2 further improves the security of a network with its use of stronger encryption called AES.
I would like to use WPA2, cause it is safer than WPA, although the safer encryption may require more advanced encryption algorithms, however, the performance impact of WPA2 is negligible.

Question **9**

Not yet answered

Marked out of 5.00

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

The WPA Personal (WPA-PSK) uses 20 character key, compared to the WEP which uses 10 character key, it would have considerably more possibilities in combination. This will increase the difficulty of cracking WPA by brute force. In the lab, we use the dictionary to crack WPA network, which I have noticed that the size of the dictionary can be large (provide more possibility) and take more time to attack into it.

Question **10**

Answer saved

Marked out of 2.50

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

(CWSP exam question, research type)

Select one or more:

- [x] a. The SSID field is set to null in the beacon frame.
- [ ] b. The SSID field is set to null in the probe request frame.
- [x] c. The SSID field is set to null in the probe response frame.
- [ ] d. The AP stops transmitting beacon frames.
- [ ] e. The AP stops responding to probe request frames.

Question **11**

Answer saved

Marked out of 5.00

128-bit WEP encryption uses a _____ IV and a _____ static key.

(CWSP exam question, research type, lecture and lab material)

Select one:

- a. 64 bit and 64 bit
- b. 24 bit and 104 bit
- c. 28 bit and 100 bit
- d. 20 bit and 108 bit
- e. None of the above