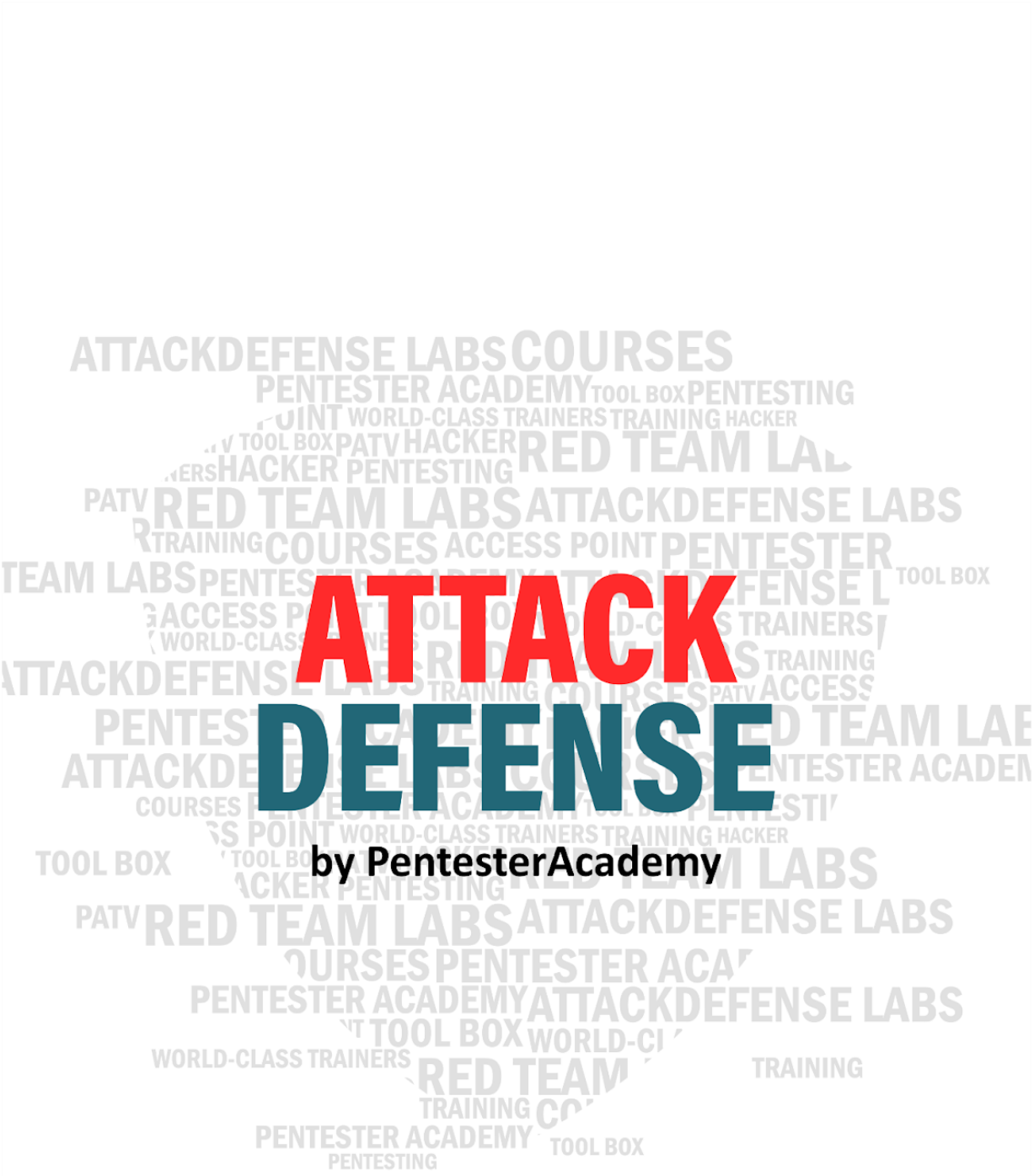
ATTACK
DEFENSE
by PentesterAcademy

Name	WiFi Recon II
URL	https://www.attackdefense.com/challengedetails?cid=1254
Type	Wi-Fi Attack-Defense : Reconnaissance

Important Note: This document illustrates all the important steps required to complete this lab. This is by no means a comprehensive step-by-step solution for this exercise. This is only provided as a reference to various commands needed to complete this exercise and for your further research on this topic. Also, note that the IP addresses and domain names might be different in your lab.

Q1: How many WiFi networks are present on channel 1?

Answer: 3

Solution:

Run airodump-ng on wlan0 on channel 1 and count the SSIDs in the list.

Command: airdump-ng wlan0 -c 1

```
CH  1 ][ Elapsed: 6 s ][ 2019-10-07 10:59

BSSID              PWR RXQ  Beacons    #Data, #/s  CH   MB   ENC CIPHER  AUTH ESSID

B8:0D:F7:83:79:BB  -28   0      132        0    0   1   11   WPA  TKIP   PSK  Forex_Magic
B8:0D:F7:D5:79:A9  -28   0      132        0    0   1   11   OPN              Airport-Free-WiFi
B8:0D:F7:6E:79:5A  -28   0      132        0    0   1   11   WPA2 CCMP   PSK  EvilCorp

BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes

(not associated)   02:00:00:00:08:00  -49    0 - 1     34         4         BAC-Community-college
```

Q2: Which WiFi network is using the WPA-PSK security scheme on channel 1?

Answer: Forex_Magic

Solution:

As mentioned in the challenge description, a monitor mode capable WiFi interface is available on the machine. Run airodump-ng on it and check for WPA TKIP in output.

Command: airodump-ng wlan0

```
CH 10 ][ Elapsed: 30 s ][ 2019-10-07 11:16

BSSID              PWR  Beacons    #Data, #/s  CH   MB   ENC CIPHER  AUTH ESSID

F2:A8:3E:C2:72:AC  -28       27        0    0   6   54   WPA2 CCMP   PSK  EvilCorp
F2:A8:3E:C2:9F:0C  -28       27        0    0   6   54   WEP  WEP         <length:  0>
B8:67:E3:34:9A:4B  -28       27        0    0  11   54   WPA2 CCMP   PSK  EvilCorp
B8:67:E3:57:D6:5C  -28       27        0    0  11   54   WPA2 CCMP   MGT  XYZ-Enterprise
B8:0D:F7:83:79:BB  -28      487        0    0   1   11   WPA  TKIP   PSK  Forex_Magic
B8:0D:F7:D5:79:A9  -28      487        0    0   1   11   OPN             Airport-Free-WiFi
B8:0D:F7:6E:79:5A  -28      487        0    0   1   11   WPA2 CCMP   PSK  EvilCorp

BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes

(not associated)   02:00:00:00:08:00  -49    0 - 1     16        24         BAC-Community-college
```

Q3: A hidden SSID is present in the vicinity. This network is operating on which channel?

Answer: 6

Solution:

From airodump-ng output, one can observe that the hidden network is operating on channel 6.

```
CH  9 ][ Elapsed: 2 mins ][ 2019-10-07 11:18

BSSID              PWR  Beacons    #Data, #/s  CH   MB   ENC CIPHER  AUTH ESSID

F2:A8:3E:C2:72:AC  -28      107        0    0   6   54   WPA2 CCMP   PSK  EvilCorp
F2:A8:3E:C2:9F:0C  -28      107        0    0   6   54   WEP  WEP         <length:  0>
B8:67:E3:34:9A:4B  -28      108        0    0  11   54   WPA2 CCMP   PSK  EvilCorp
B8:67:E3:57:D6:5C  -28      108        0    0  11   54   WPA2 CCMP   MGT  XYZ-Enterprise
B8:0D:F7:83:79:BB  -28     1778        0    0   1   11   WPA  TKIP   PSK  Forex_Magic
B8:0D:F7:D5:79:A9  -28     1778        0    0   1   11   OPN             Airport-Free-WiFi
B8:0D:F7:6E:79:5A  -28     1778        0    0   1   11   WPA2 CCMP   PSK  EvilCorp
```

Q4: What is the BSSID of the SSID "EvilCorp" operating on channel 1?

Answer: B8:0D:F7:6E:79:5A

Solution:

From airodump-ng output, one can observe that BSSID B8:0D:F7:6E:79:5A of SSID EvilCorp is operating on channel 1.

```
CH  9 ][ Elapsed: 2 mins ][ 2019-10-07 11:18

BSSID              PWR  Beacons    #Data, #/s  CH   MB   ENC CIPHER  AUTH ESSID

F2:A8:3E:C2:72:AC  -28      107        0    0   6   54   WPA2 CCMP   PSK  EvilCorp
F2:A8:3E:C2:9F:0C  -28      107        0    0   6   54   WEP  WEP         <length:  0>
B8:67:E3:34:9A:4B  -28      108        0    0  11   54   WPA2 CCMP   PSK  EvilCorp
B8:67:E3:57:D6:5C  -28      108        0    0  11   54   WPA2 CCMP   MGT  XYZ-Enterprise
B8:0D:F7:83:79:BB  -28     1778        0    0   1   11   WPA  TKIP   PSK  Forex_Magic
B8:0D:F7:D5:79:A9  -28     1778        0    0   1   11   OPN              Airport-Free-WiFi
B8:0D:F7:6E:79:5A  -28     1778        0    0   1   11   WPA2 CCMP   PSK  EvilCorp

BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes

(not associated)   02:00:00:00:08:00  -49    0 - 1     48       108         BAC-Community-college
```

Q5: How many BSSIDs are present for the SSID "EvilCorp" in total?

Answer: 5

Solution:

Run airodump-ng on both bands (2.4 GHz and 5 GHz) and count the total number of BSSIDs for SSID Evilcorp. Total count of BSSIDs is 5.

Command: airodump-ng --band abg wlan0

```
CH 165 ][ Elapsed: 1 min ][ 2019-10-07 11:25

BSSID              PWR  Beacons    #Data, #/s  CH   MB   ENC CIPHER  AUTH ESSID

D2:A4:4F:E3:28:B5  -28       30        0    0 132   54   WPA2 CCMP   PSK  EvilCorp
68:7F:77:C2:C2:9A  -28       30        0    0 104   54   WPA2 CCMP   PSK  EvilCorp-covert
DE:67:E3:34:9A:4B  -28       30        0    0  36   54   WPA  TKIP   PSK  EvilCorp
F2:A8:3E:C2:72:AC  -28       18        0    0   6   54   WPA2 CCMP   PSK  EvilCorp
F2:A8:3E:C2:9F:0C  -28       18        0    0   6   54   WEP  WEP         <length:  0>
B8:67:E3:34:9A:4B  -28       18        0    0  11   54   WPA2 CCMP   PSK  EvilCorp
B8:67:E3:57:D6:5C  -28       18        0    0  11   54   WPA2 CCMP   MGT  XYZ-Enterprise
B8:0D:F7:83:79:BB  -28     1302        0    0   1   11   WPA  TKIP   PSK  Forex_Magic
B8:0D:F7:D5:79:A9  -28     1302        0    0   1   11   OPN              Airport-Free-WiFi
B8:0D:F7:6E:79:5A  -28     1302        0    0   1   11   WPA2 CCMP   PSK  EvilCorp

BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes

(not associated)   02:00:00:00:08:00  -49    0 - 1      0        64         BAC-Community-college
```

Q6: What is the MAC address of the client associated with SSID "EvilCorp"?

Answer:

Solution:

As per the question, a client is associated with associated with SSID EvilCorp but no such client is visible on airodump-ng output. This might be due to non-activity (packet activity) between BSSID and client.

Fix airmon-ng on each channel on which EvilCorp SSID is operating, one by one. Then send a deauth broadcast for EvilCorp SSID. This will disconnect the client and while reconnecting with the BSSID, airodump-ng might pick it up.

Start with channel 1

Command: airodump-ng -c 1 wlan0

```
CH  1 ][ Elapsed: 24 s ][ 2019-10-07 11:31

BSSID              PWR RXQ  Beacons    #Data, #/s  CH   MB   ENC CIPHER  AUTH ESSID

B8:0D:F7:83:79:BB  -28 100      376        0    0   1   11   WPA  TKIP   PSK  Forex_Magic
B8:0D:F7:D5:79:A9  -28 100      376        0    0   1   11   OPN              Airport-Free-WiFi
B8:0D:F7:6E:79:5A  -28   0      376        0    0   1   11   WPA2 CCMP   PSK  EvilCorp

BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes

(not associated)   02:00:00:00:08:00  -49    0 - 1     34       12         BAC-Community-college
```

Send deauth packets for EvilCorp network

Command: aireplay-ng -0 100 -e EvilCorp wlan0

```
root@attackdefense:~# aireplay-ng -0 100 -e EvilCorp wlan0
11:30:51  Waiting for beacon frame (ESSID: EvilCorp) on channel 1
Found BSSID "B8:0D:F7:6E:79:5A" to given ESSID "EvilCorp".
NB: this attack is more effective when targeting
a connected wireless client (-c <client's mac>).
11:30:51  Sending DeAuth (code 7) to broadcast -- BSSID: [B8:0D:F7:6E:79:5A]
11:30:52  Sending DeAuth (code 7) to broadcast -- BSSID: [B8:0D:F7:6E:79:5A]
11:30:53  Sending DeAuth (code 7) to broadcast -- BSSID: [B8:0D:F7:6E:79:5A]
11:30:53  Sending DeAuth (code 7) to broadcast -- BSSID: [B8:0D:F7:6E:79:5A]
```

Check if airodump-ng is showing any such client.

Repeat for channel 6, 11, 36,104

Finally, while doing it for channel 36

Command: airodump-ng --band a -c 36 wlan0

```
CH 36 ][ Elapsed: 54 s ][ 2019-10-07 11:48

BSSID              PWR RXQ  Beacons    #Data, #/s  CH   MB   ENC CIPHER  AUTH ESSID

DE:67:E3:34:9A:4B  -28   0      581        0    0  36   54   WPA  TKIP   PSK  EvilCorp
B8:0D:F7:83:79:BB  -28 100      832        0    0   1   11   WPA  TKIP   PSK  Forex_Magic
B8:0D:F7:D5:79:A9  -28 100      832        0    0   1   11   OPN              Airport-Free-WiFi
B8:0D:F7:6E:79:5A  -28 100      832        0    0   1   11   WPA2 CCMP   PSK  EvilCorp

BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes

(not associated)   02:00:00:00:08:00  -49    0 - 6     58        56         BAC-Community-college
DE:67:E3:34:9A:4B  02:00:00:00:07:00  -29    0 - 6      0         2         EvilCorp
```

While sending deauths on channel 36, ignore the errors.

Command: aireply-ng -0 100 -e EvilCorp wlan0

```
root@attackdefense:~#
root@attackdefense:~# aireplay-ng -0 100 -e EvilCorp wlan0
11:48:05  Waiting for beacon frame (ESSID: EvilCorp) on channel 36
Found BSSID "B8:0D:F7:6E:79:5A" to given ESSID "EvilCorp".
11:48:05  wlan0 is on channel 36, but the AP uses channel 1
root@attackdefense:~#
```