ATTACK DEFENSE

by PentesterAcademy

Name	WiFi Recon I
URL	https://www.attackdefense.com/challengedetails?cid=1253
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.

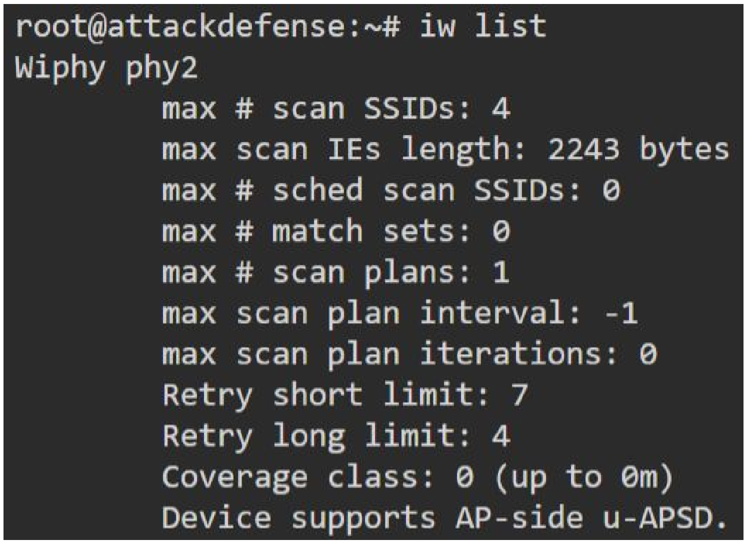
Q1: Is phy2 interface capable of transmitting beacon frames on channel 13?

Answer: No

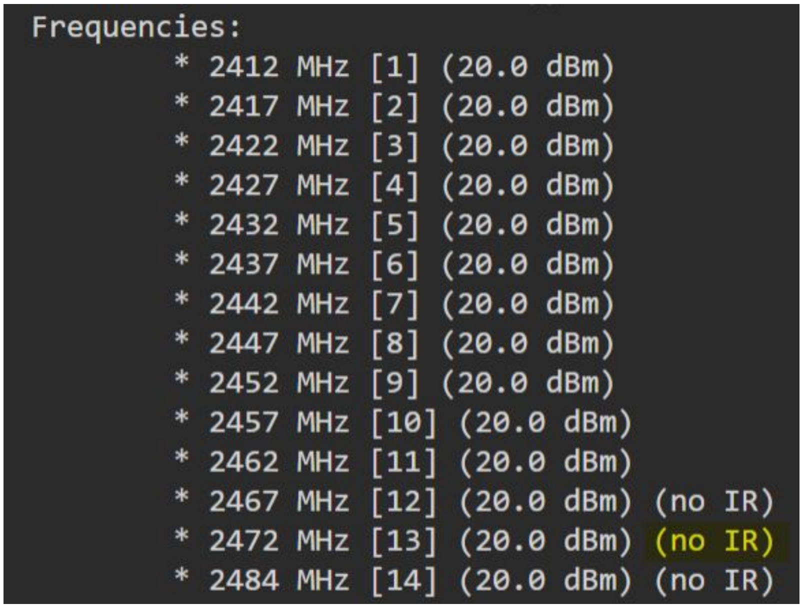
Solution:

Running iw list will show that NO_IR flag is set for channel 13 which means that the device cannot use modes of operation that require the device to initiate radiation first.

Command: iw list



```
root@attackdefense:~# iw list
Wiphy phy2
        max # scan SSIDs: 4
        max scan IEs length: 2243 bytes
        max # sched scan SSIDs: 0
        max # match sets: 0
        max # scan plans: 1
        max scan plan interval: -1
        max scan plan iterations: 0
        Retry short limit: 7
        Retry long limit: 4
        Coverage class: 0 (up to 0m)
        Device supports AP-side u-APSD.
```



```
Frequencies:
        * 2412 MHz [1] (20.0 dBm)
        * 2417 MHz [2] (20.0 dBm)
        * 2422 MHz [3] (20.0 dBm)
        * 2427 MHz [4] (20.0 dBm)
        * 2432 MHz [5] (20.0 dBm)
        * 2437 MHz [6] (20.0 dBm)
        * 2442 MHz [7] (20.0 dBm)
        * 2447 MHz [8] (20.0 dBm)
        * 2452 MHz [9] (20.0 dBm)
        * 2457 MHz [10] (20.0 dBm)
        * 2462 MHz [11] (20.0 dBm)
        * 2467 MHz [12] (20.0 dBm) (no IR)
        * 2472 MHz [13] (20.0 dBm) (no IR)
        * 2484 MHz [14] (20.0 dBm) (no IR)
```

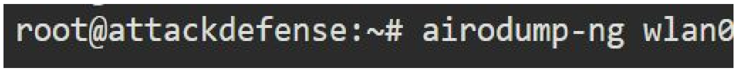
Q2: What is the BSSID of SSID "Home_Network"?

Answer: D2:69:10:37:F5:94

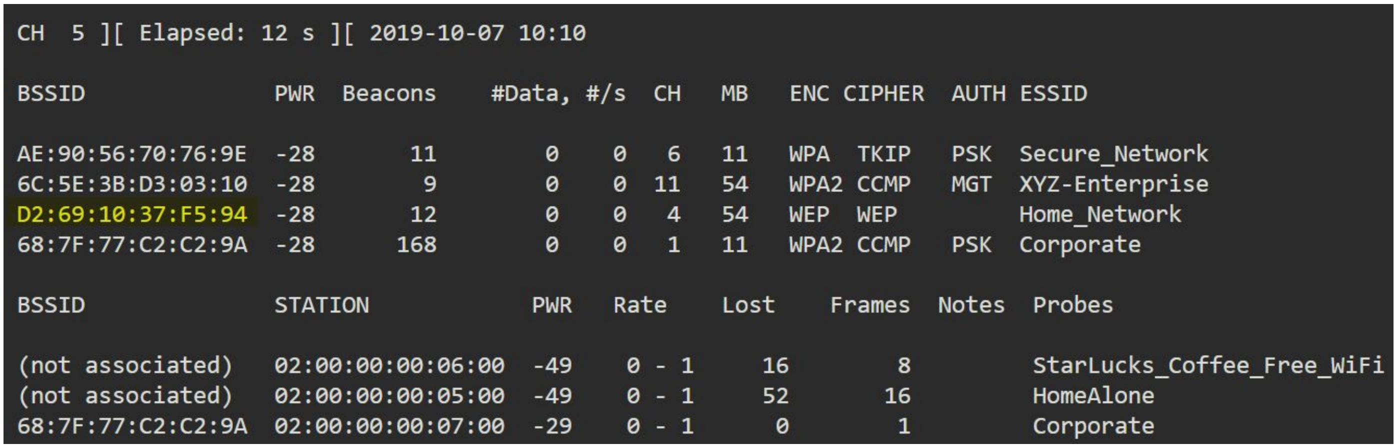
Solution:

As mentioned in the challenge description, a monitor mode capable WiFi interface is available on the machine. Run airodump-ng on it.

Command: airodump-ng wlan0



```
root@attackdefense:~# airodump-ng wlan0
```



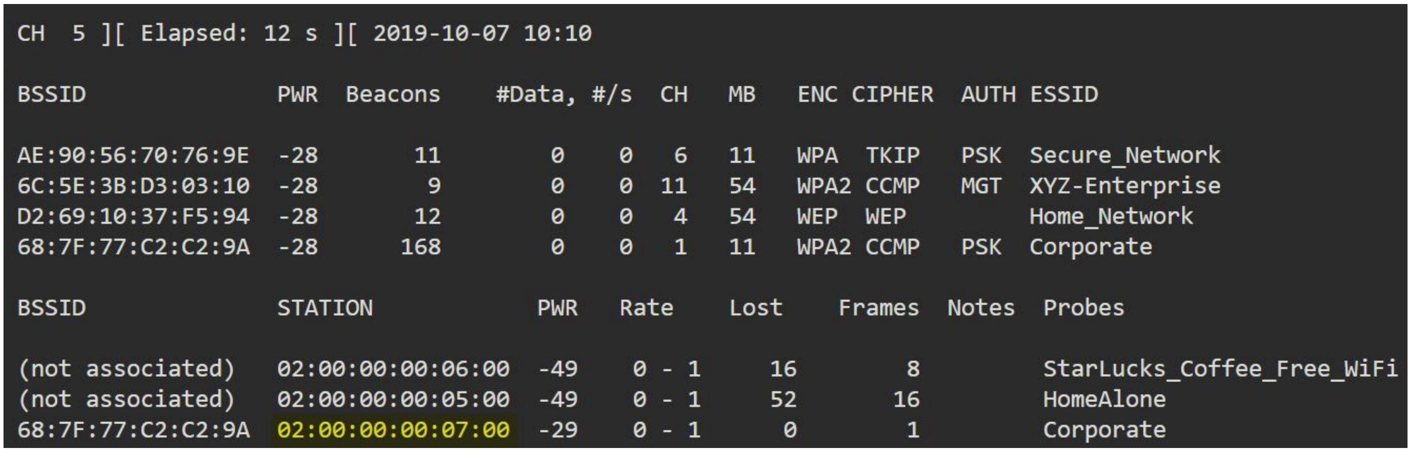
```
CH  5 ][ Elapsed: 12 s ][ 2019-10-07 10:10

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

AE:90:56:70:76:9E  -28       11        0    0   6   11   WPA  TKIP   PSK  Secure_Network
6C:5E:3B:D3:03:10  -28        9        0    0  11   54   WPA2 CCMP   MGT  XYZ-Enterprise
D2:69:10:37:F5:94  -28       12        0    0   4   54   WEP  WEP         Home_Network
68:7F:77:C2:C2:9A  -28      168        0    0   1   11   WPA2 CCMP   PSK  Corporate

BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes

(not associated)   02:00:00:00:06:00  -49    0 - 1     16        8         StarLucks_Coffee_Free_WiFi
(not associated)   02:00:00:00:05:00  -49    0 - 1     52       16         HomeAlone
68:7F:77:C2:C2:9A  02:00:00:00:07:00  -29    0 - 1      0        1         Corporate
```

Q3: What is the MAC address of the client connected to SSID "Corporate"?

Answer: 02:00:00:00:07:00

Solution:

From airodump-ng output, one can observe that the client with MAC 02:00:00:00:07:00 is connected to “Corporate” SSID.



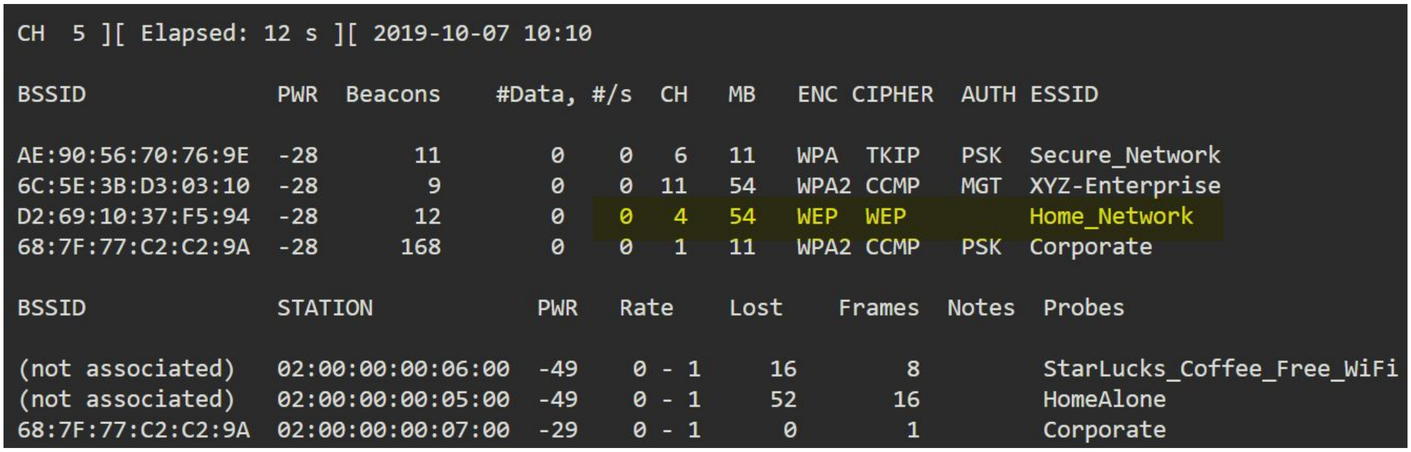
```
CH  5 ][ Elapsed: 12 s ][ 2019-10-07 10:10

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

AE:90:56:70:76:9E  -28       11        0    0   6   11   WPA  TKIP   PSK  Secure_Network
6C:5E:3B:D3:03:10  -28        9        0    0  11   54   WPA2 CCMP   MGT  XYZ-Enterprise
D2:69:10:37:F5:94  -28       12        0    0   4   54   WEP  WEP         Home_Network
68:7F:77:C2:C2:9A  -28      168        0    0   1   11   WPA2 CCMP   PSK  Corporate

BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes

(not associated)   02:00:00:00:06:00  -49    0 - 1     16        8         StarLucks_Coffee_Free_WiFi
(not associated)   02:00:00:00:05:00  -49    0 - 1     52       16         HomeAlone
68:7F:77:C2:C2:9A  02:00:00:00:07:00  -29    0 - 1      0        1         Corporate
```

Q4: WEP network is also present in the vicinity. This network is on which channel?

Answer: 4

Solution:

From airodump-ng output, one can observe that WEP network is operating on channel 4.



```
CH  5 ][ Elapsed: 12 s ][ 2019-10-07 10:10

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

AE:90:56:70:76:9E  -28       11        0    0   6   11   WPA  TKIP   PSK  Secure_Network
6C:5E:3B:D3:03:10  -28        9        0    0  11   54   WPA2 CCMP   MGT  XYZ-Enterprise
D2:69:10:37:F5:94  -28       12        0    0   4   54   WEP  WEP         Home_Network
68:7F:77:C2:C2:9A  -28      168        0    0   1   11   WPA2 CCMP   PSK  Corporate

BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes

(not associated)   02:00:00:00:06:00  -49    0 - 1     16        8         StarLucks_Coffee_Free_WiFi
(not associated)   02:00:00:00:05:00  -49    0 - 1     52       16         HomeAlone
68:7F:77:C2:C2:9A  02:00:00:00:07:00  -29    0 - 1      0        1         Corporate
```