

[illegible]

Name	WPA PSK Cracking
URL	https://www.attackdefense.com/challengedetails?cid=31
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 WPA-PSK.pcap

```
CH  0  ][ Elapsed: 28 s ][ 2018-11-03 13:08 ][ Finished reading input file WPA-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 . WPA  TKIP  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 WPA-PSK.pcap

Aircrack-ng 1.2 beta3

[00:00:04] 1000 keys tested (237.40 k/s)

KEY FOUND! [abcdefgh]

Master Key : 5D C0 A9 A5 B3 59 C2 72 C4 65 90 41 EC CA 2F D7
A6 D8 4E 97 DD A3 EC 22 C9 10 9B 21 F7 AD D1 B0

Transient Key : 5A 38 D3 16 70 55 E2 7C CF 7B ED 2A 41 CA A1 94
FC 44 91 2E 8E C8 F0 4B 8C F6 2E 4C 65 1A 9A 01
83 EF BC 06 97 1F B0 87 87 85 FE E0 51 44 5A 8A
D3 48 E0 EB FE AB 29 76 76 2F C9 B7 53 1F 89 76

EAPOL HMAC : B1 9C A6 F3 DF 16 1D 83 A5 F0 D3 1B 1B 7F 24 25

Flag: abcdefgh

References:

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