

[illegible]

Name	WEP Cracking
URL	https://www.attackdefense.com/challengedetails?cid=30
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: Explore the PCAP file and look at the WEP networks in it.

Command: airodump-ng -r WEP-Cracking.cap

```
CH  0  ][ Elapsed: 28 s ][ 2018-11-03 05:24 ][ Finished reading input file WEP-Cracking.cap.

BSSID                PWR  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID
00:21:91:D2:8E:25    0      1      18774    0   1  54e. WEP  WEP   SKA  SecurityTube

BSSID                STATION            PWR   Rate    Lost    Frames  Probe
00:21:91:D2:8E:25  60:FB:42:D5:E4:01   0     0e- 0      0    41414  SecurityTube
```

We see that there is only 1 WEP network with the BSSID 00:21:91:D2:8E:25 and SSID SecurityTube.

Step 2: Start the cracking process with aircrack

Command: aircrack-ng -b 00:21:91:d2:8e:25 WEP-Cracking.cap

```
Aircrack-ng 1.2 beta3

[00:00:02] Tested 47135 keys (got 18755 IVs)

KB  depth  byte(vote)
0   0/ 7    12(26112) 89(25344) 95(24576) A2(24576) 83(24320) E1(23808) C2(23552) 29(23296) 76(23296) E7(23040) 06(22528) D6(22528)
1   1/ 44   34(23296) 7B(23040) 8D(23040) A7(23040) 17(23040) 1F(23040) 81(22784) BD(22784) 27(22784) 5C(22528) 8A(22528) 92(22528)
2  15/ 18   25(22272) 10(22016) 9C(22016) CC(22016) 01(21760) 2D(21760) 8B(21760) 8F(21760) 9D(21760) 9E(21760) AE(21760) AF(21760)
3   0/ 9    78(24832) 50(24320) C9(23808) 1A(23296) 42(23296) 73(23040) 20(23040) 86(22784) C8(22784) 17(22272) 35(22272) 6B(22272)
4   0/ 1    90(33792) 85(24576) 57(24064) B7(23552) 7E(22784) 17(22528) 54(22528) 89(22528) BC(22528) D6(22528) A0(22272) DE(22272)

KEY FOUND! [ 12:34:56:78:90 ]
Decrypted correctly: 100%
```

Flag: 12:34:56:78:90

References:

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