
ATTACK
DEFENSE
by PentesterAcademy

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.

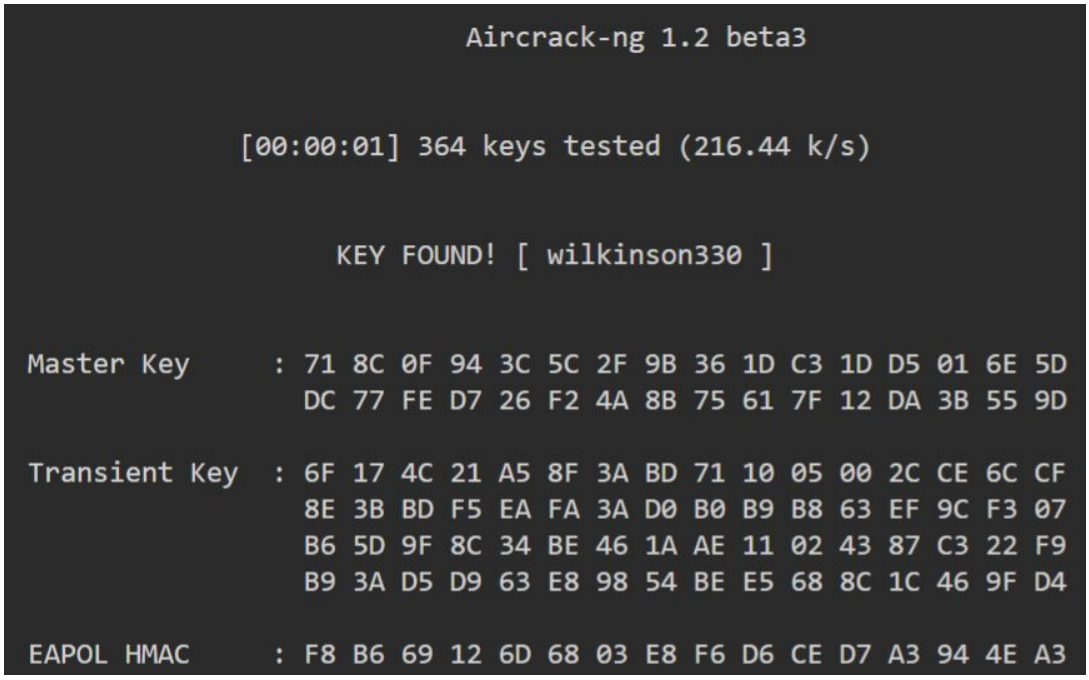
Command: airodump-ng -r WPA2-PSK.cap

```
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



Flag: wilkinson330

References:

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