|  |
| --- |
| ***Network Attack*** |
| Kaan Efe Öğüt  *ADLİ BİLİŞİM MÜHENDİSLİĞİ* |
| -WPA2 Korumalı bir wifi’nin şifresini nasıl ele geçirebiliriz bunun hakkında bilgi vermek istiyorum. |

**01.11.2021**

Kablosuz Ağ terimleri

SSID = Kablosuz Ağ İsmi

BSSID = Kablosuz Aygıtın Ethernet Mac adresidir.

Channel = Client ile AP'nin daha verimli haberleşebilmes için kullandığı kanal numarası

Client = İstemci

AP = Access Point erişim noktasını temsil eder.Ağ'ı yayan aygıt olarak düşünebiliriz. Bilgisayarlar,telefon vb cihazları ağa bağlar.

Airodump

-Çevremizdeki ağlardan bilgi toplama işlemi gerçekleştirmemizi sağlar.

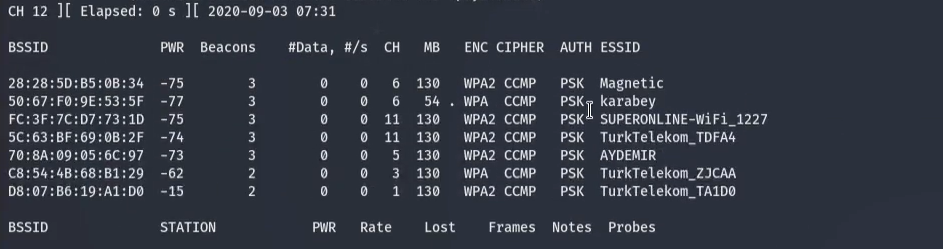


- Bu işlemler için ilk önce monitör moda geçiş yapıyorum.

-Monitor moda alma -> airmon-ng start wlan0



-Daha sonrasında İfconfig komutuyla kontrol ediyorum ve burada Wlan0mon'u görebiliyorum.



-"airodump-ng wlan0mon" Komutunu kullanarak etrafında ki modem hakkında bilgi sahibi olabiliyoruz.

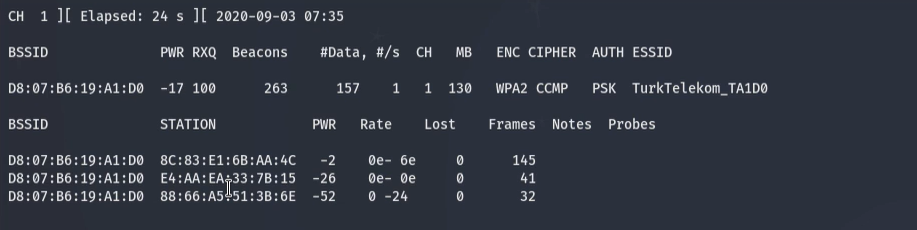
Güvenlik Protokolleri

WEB -> Bilgiler direk toplanıp bilgi toplama işlemi yapılabilir.

WPA-WPA2 -> Üzerinden bilgi toplamak için Ağdan birini düşürüp ardından tekrar bağlantı kurduğunda handshake yakalıyarak işlem gerçekleştirebiliriz.



-"airodump-ng wlan0mon --bssid "Saldırı gerçekleştireceğimiz BSSID" -c "Channel belirtilir".



- Ağ içerisinde bulunan cihazlar hakkında bilgi sahibi olmamızı sağladı.

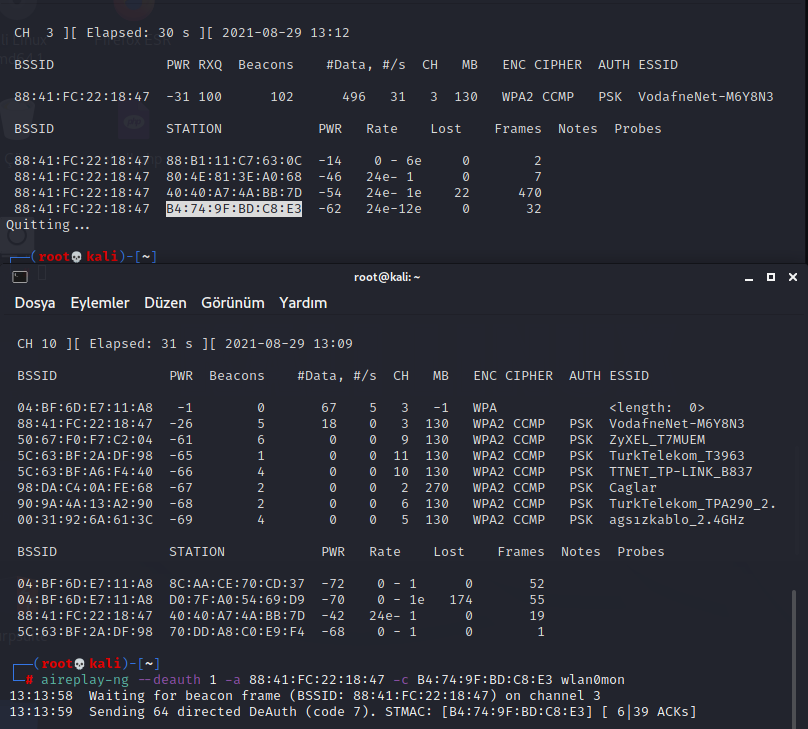
-Station bölümünde fiziksel adres gözükmektedir.

Ağda DOS ve Handshake yakalama

-Monitör mod üzerinde çalışırken bu işlem gerçekleştirilir.

-WPA ve WPA2 güvenlikli ağlarda bilgi toplayabilmek için handshake almamız gerekmektedir.Bu sebeple ilk etapta ağdan atmamız gerekmektedir.

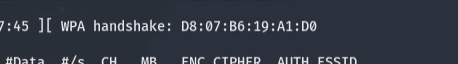
-Ağ içerisinde bulunan cihazların adresi üzerinden işlem yapacağım için öncelikle ağ içerisinde bilgi topluyorum.



- Bu işlem için Deauth saldırısı gerçekleştireceğiz.

-"aireplay-ng --deauth 3 -a "BSSID" -c "STATİON" ile ağdan düşürme işlemi gerçekleştiriyoruz.

-Handshake alabilmemiz için "airodump-ng wlan0mon --bssid "BSSID" -c 1 -w Kayıtyeri olarak çalıştırmamız gerekmektedir.

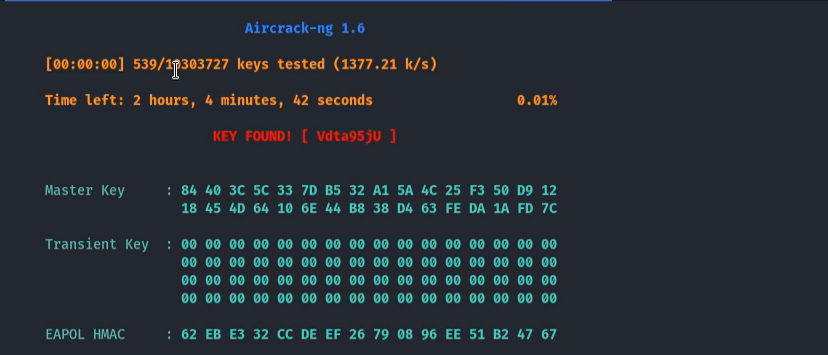


-Başarılı bir şekilde handshake elde edebildik.

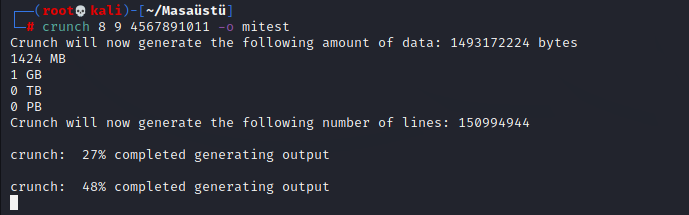
Aircrack

-Airmon ile bilgi topladığımız ve ardından aireplay ile aldığımız (.cap)handshake'i kullanarak bir bruteforce işlemi gerçekleştireceğiz.

"aircrack-ng "Elde ettiğimiz Handshake" -w /rockyou.txt(Wordlist belirtiyoruz).



Wordlist Oluşturma

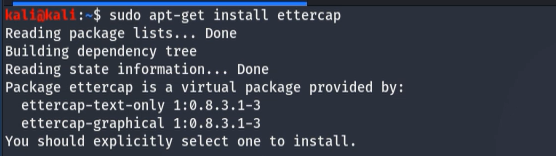


- -Daha önceden çalıştığım Crunch'ı kullanacağım.

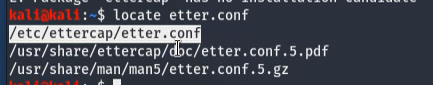
-Genellikle modemler en az 8 karakterli şifreler kullanır ben şifreyi bildiğim için bu şekilde oluşturdum.

Ağa dahil olduktan sonra IP Spoofing

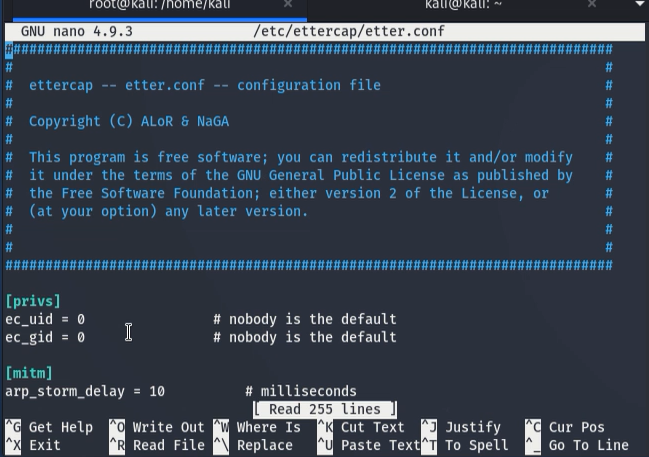
- Ağa başarılı bir şekilde dahil olabilmiştik bu sefer MITM içerisinde bulunan ARP Spoofing ile HTTP mesajlarımızı okuyabilir.



-Bu işlem için ettercap aracını kullanacağız.Eğer yüklü değil ise bu komutları kullanarak yükleme işlemi yapılabilir.



- Bu işlem için ilk önce etter.conf uzantılı dosyada bir işlem gerçekleştirmemiz gerekmektedir.Bu sebeble locate komutuyla bu dosyayı arıyorum.



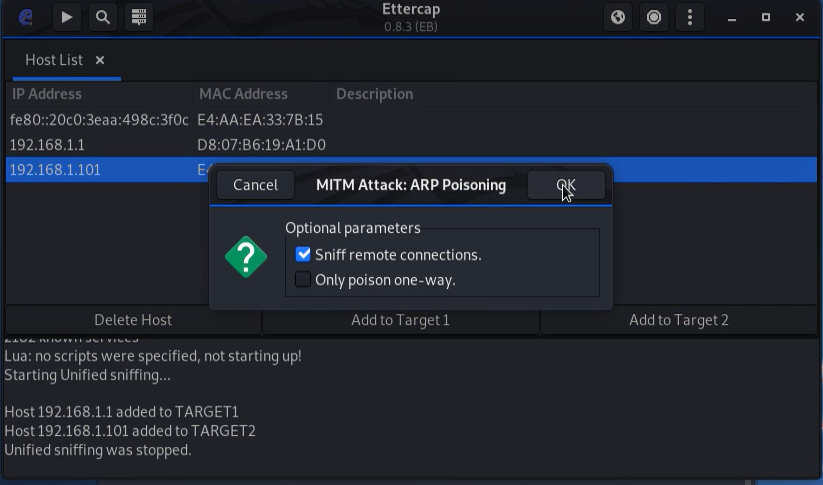
- Daha sonrasında nano komutu ile dosyayı görüntülüyorum.Burada yer alan "ec\_uid,ec\_guid" değerlerini 0 yapıyorum.



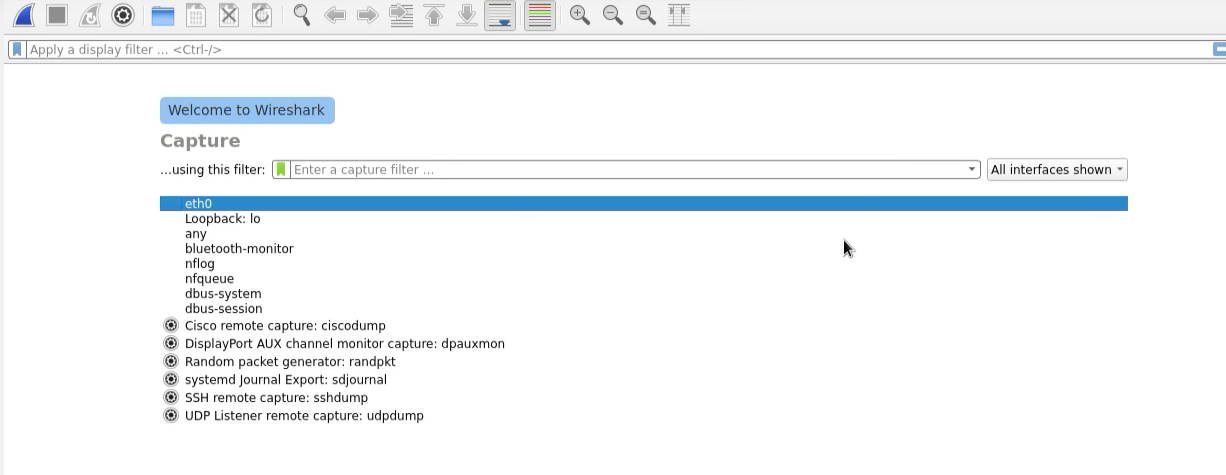
-"ettercap -G" komutu ile aracı başlatıyorum.Karşıma böyle bir arayüz çıkıyor.



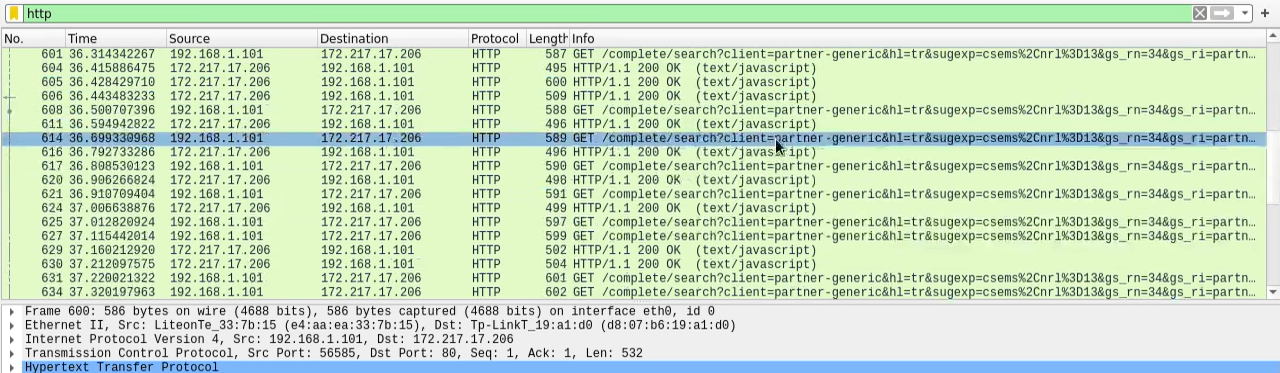
- Sniffing işlemini başlattığımda bu ağ üzerinde bulunan cihazların IP ve MAC adreslerini görüntüleyebiliriz.



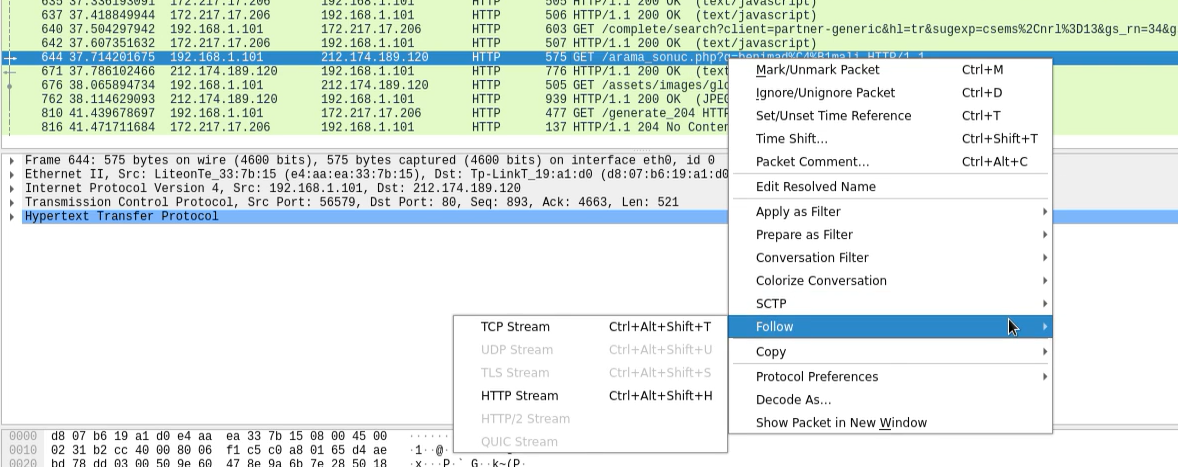
-Yönlendirici ile Cihazı add to target komtu ile ekliyorum.Daha sonrasında ARP Poising işlemini başlatıyorum.



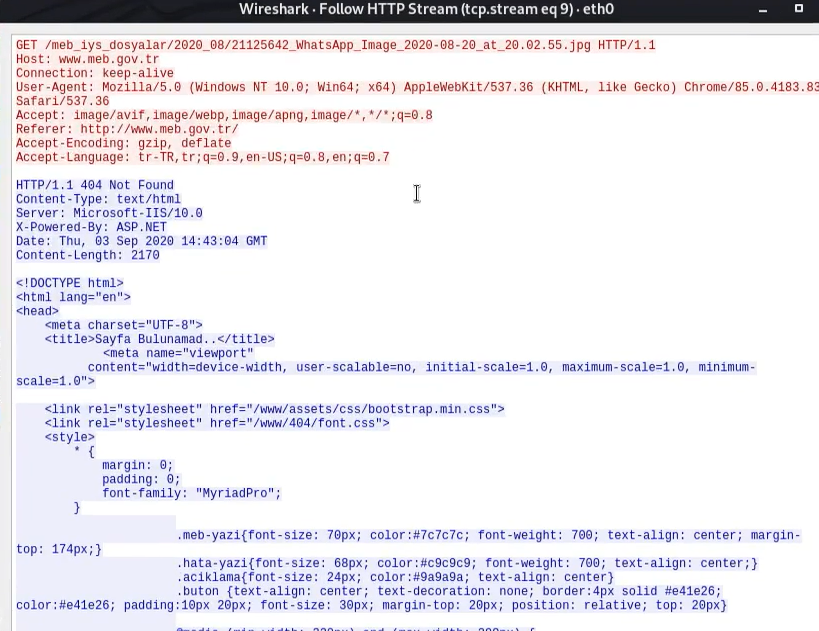
- İşlemi başlattıktan sonra Wireshark üzerine geçiş yapıyorum ve eth0 üzerinden ağı dinlemeye başlıyorum.



- HTTP filtrelemesi üzerinden bilgi elde etmeye çalışıyorum.



- HTTP filtrelemesi üzerinden bir sonuca geçiş yapıyorum ve "Follow -> Stream" seçeneği ile ayrıntılarını görüntüleyebiliyorum.



-Burada baktığımda site üzerine giriş yapılan yerlerde başarılı bir şekilde bilgi elde edinebilirim.