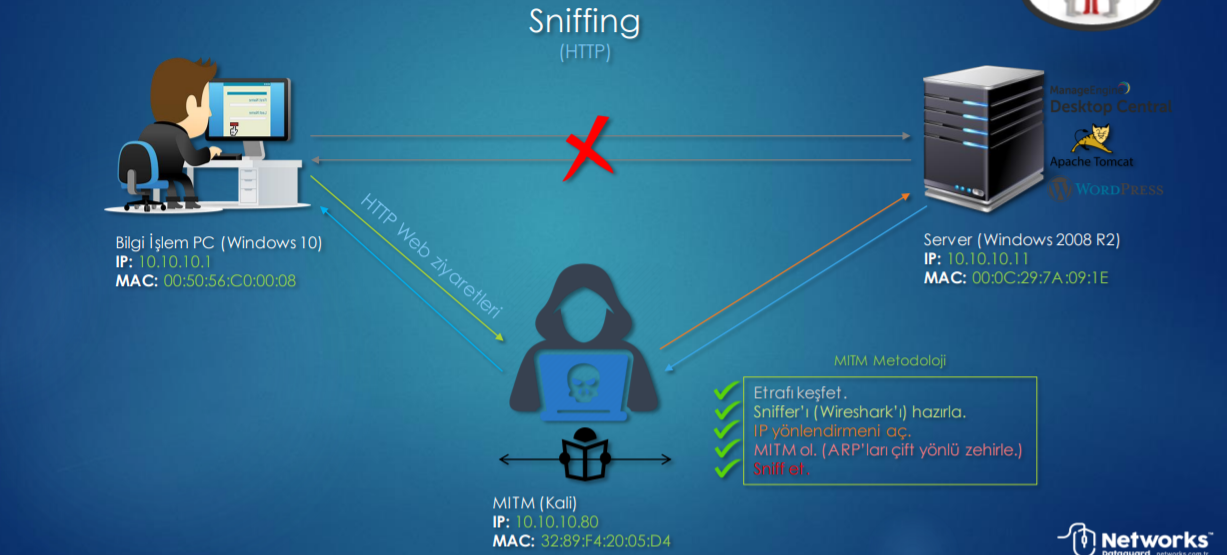
|  |
| --- |
| ***MITM Saldırıları*** |
| Kaan Efe Öğüt  *ADLİ BİLİŞİM MÜHENDİSLİĞİ* |
| Pentest aşamalarında çok fazla önemi olan MITM Saldırıları hakkında uygulama gerçekleştireceğim. |

**27.12.2021**

MITM Kavramı

- Ortadaki adam terimi, networkteki standart iletişim yöntemlerinin ve süreçlerinin manipüle edilmesi anlamındadır.

-Birden fazla manipülasyon çeşidi ve amacı vardır.



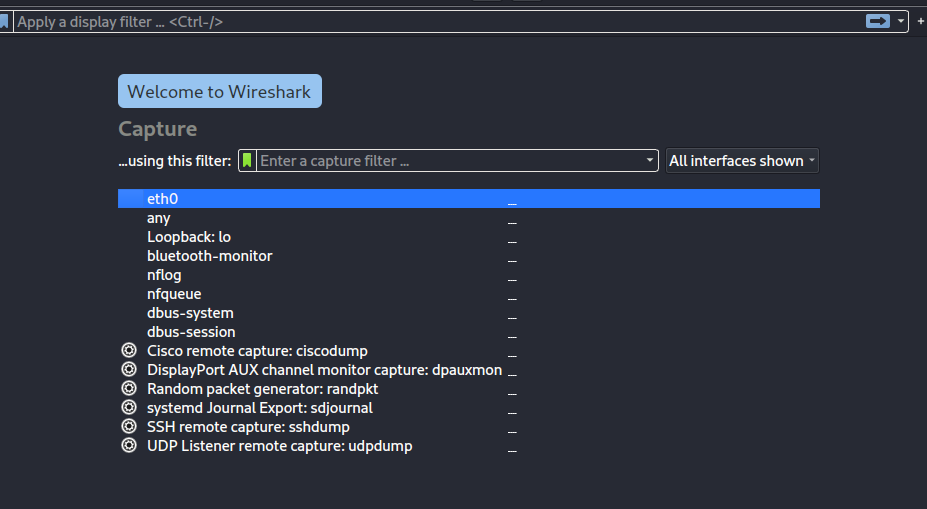
- Görsel olarak anlatmaya çalıştığımız da bu şekildedir.

-Örneklerle daha çok pekişecektir.

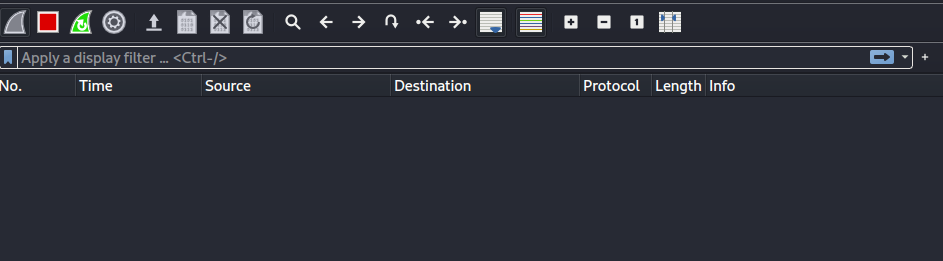
***Wireshark Kullanımı ve Paket Filtreleme***

-Wireshark network üzerinde paket analiz etme,hata analiz etme gibi işlemlerimizi gerçekleştirmemizi sağlar.

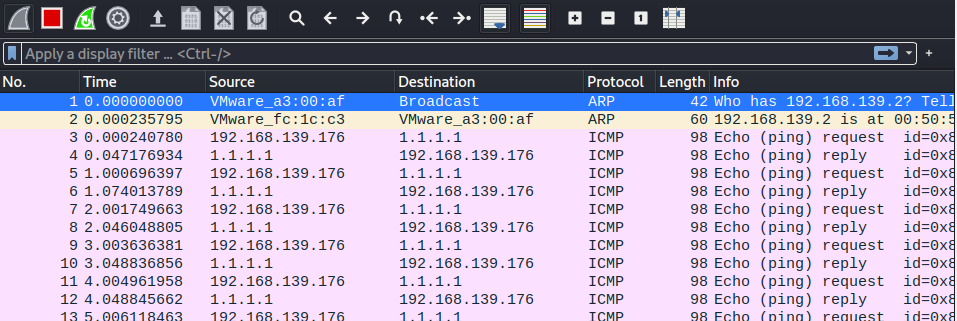
-Bu araç Linux üzerinde kurulu olarak gelmektedir.



- Aracı çalıştırdığımız da karşımıza bu şekilde bir ekran gelmektedir.

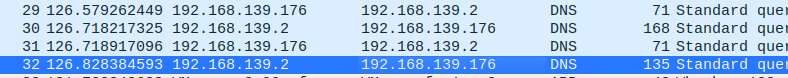


- Local üzerinde işlem gerçekleştirmek istediğim için "eth0" ile devam ediyorum.



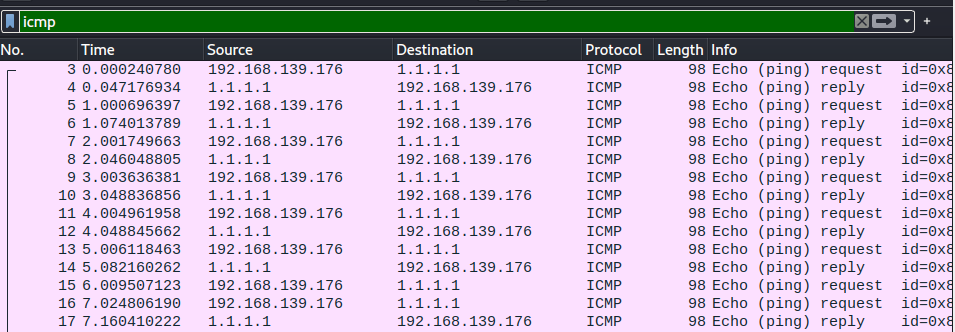
- Seçimi yaptıktan hemen sonra ağı dinlemeye başlar.

-Yukarıda yer alan buton(balık sırtı) ile işlemi başlatıp stop tuşu ile durdurabiliriz.

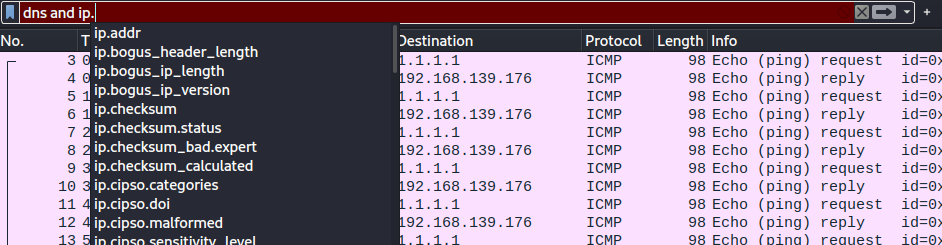


- Paket alıp verme işlemleri başladığında ekranımıza bu şekilde yüzlerce paket düşecektir.

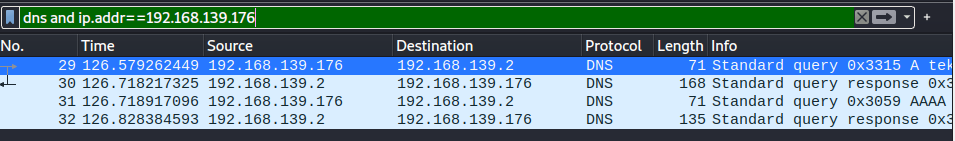
-Burada filtreleme işlemi gerçekleştirerek bilgi çekmeye çalışacağız.



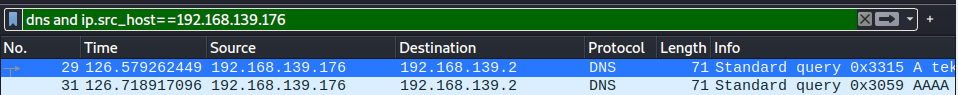
- Arka planda gerçekleştirdiğim bir DNS sorgusu ekrana bu şekilde düşmektedir.



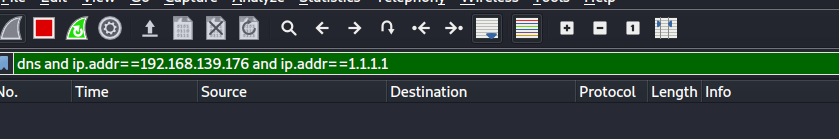
- Arama yerinde ICMP aratırsam sadece onunla ilgili tablolar gelmektedir.



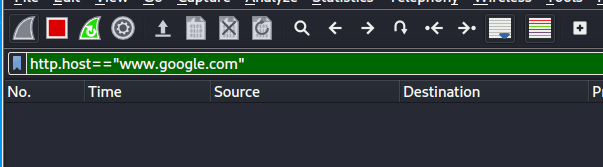
- Arama yerinde ayrıca "dns and ip." şeklinde bir arama gerçekleştireceğim de kod yazar gibi tamamlayabileceğim seçenekleri tarafıma sunar.



- Sadece kaynak kısmında aradığım IP olmasını istersem bu şekilde filtreleyebilirim.



- Sorguya birden çok "and" yapısı ekleyerek daha çok sorgulama gerçekleştirebilirim.



- HTTP metodu ile de bu şekilde çalışılabilir.

-Wireshark üzerinde gelen giden trafiği görüntüledik.

-Kendimizden geleni ve kendimizden gideni görüntüledik.

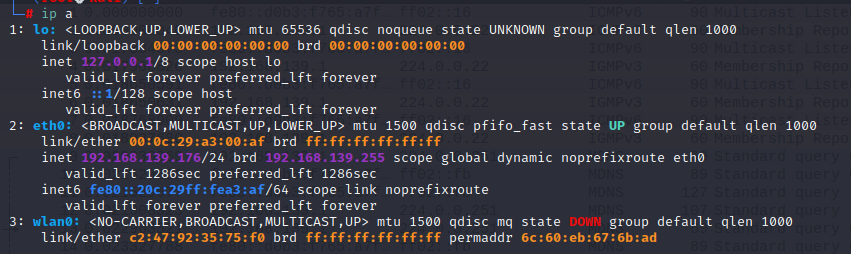
#Etrafta ki tüm paketleri nasıl görebilirim.#

-Switchlerin yeteneksiz olanları hub’tır ve Switchlerden önce yaygın kullanırdı.

-Ethernet kartında hedefin MAC ve IP adresi vardır fakat bu bütün portlardan herkese gönderir ve sahibi kimse alır.HUB bunu çevrede ki tüm cihazlara aktarırdı.

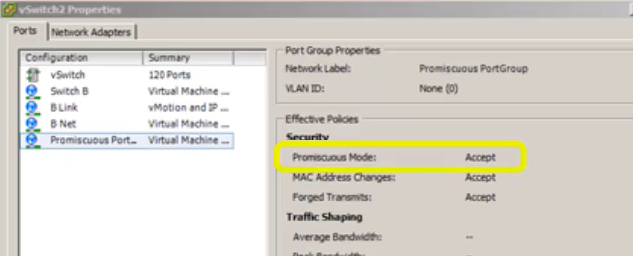
-Switch(Anahtarlayıcı) ile Kaynağı hedefe anahtarlayabilir hale geldiler.Burada HUB’un aksine herkese paket göndermek yerine istediğine gönderiyor.

-Switchler aynı HUB gibi davranıp paketi tüm ağ üzerine gönderebiliyor.Bu davranışa Promiscuous Mode denir.İlgilisine değil herkese gönderim yapar.



-Kullanılan ethernet kartınında bu mode'u açık ise paketleri yakalar.

-Wireshark gibi sniffer'lar ise bunları yorumlamamızı sağlar.

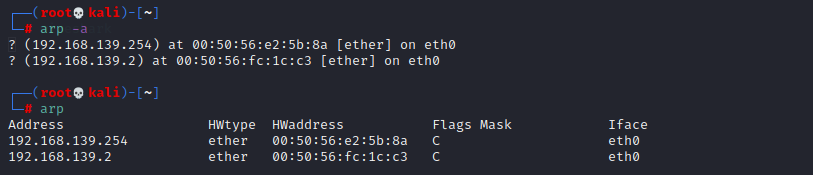


-Switch üzerinde güvenlik önlemi alınmadıysa ve ethernet kartı bu modu destekliyorsa Wireshark gibi sniffler o zaman devreye girer.

-Aslında bu işi yapan ethernet kartlarıdır.

***ARP***

-Bu işlemlere başlamadan önce "ARP" hakkında bilgilendirme yapmak istiyorum.



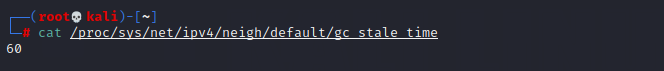
-"arp -a" & "arp" komutunu kullandığımızda civarda ki cihazlar hakkında bilgi alabiliyorduk.

-Fakat burada tüm cihazların olmadığını görüyoruz.

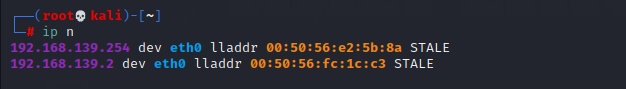


-A sınıfında yaklaşık olarak 16.777.214 adet host bulunmaktadır.

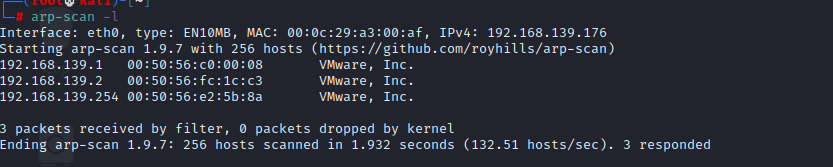
-Eğer ki cihazlar bunların hepsini görseydi bozulurlardı.



-Bu tablo 60 saniye de bir güncellenir.

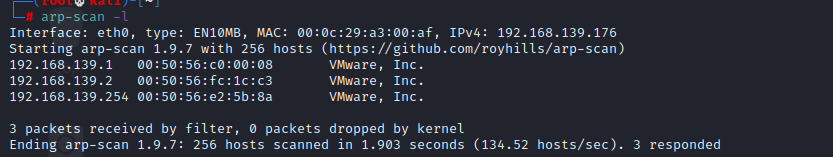


-"ip n" komutu ile erişilebilir veya erişilemez(kopmaya yakın) olanları görüntüleyebiliriz.

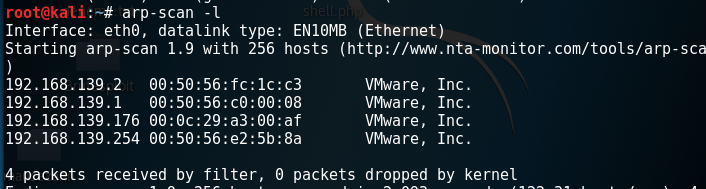


-Bu sebeple her zaman "arp-scan -l" komutu çalıştırılmalıdır.

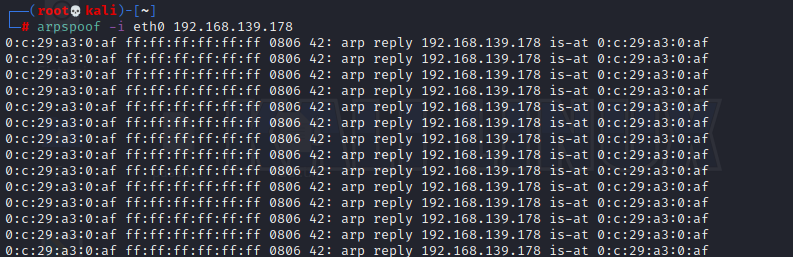
***ARP Zehirlenmesi***



-Öncelikle arp taraması gerçekleştiriyorum.



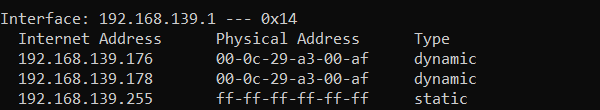
-Aynı işlemi farkı bir sürüm linux üzerinden de gerçekleştiriyorum.



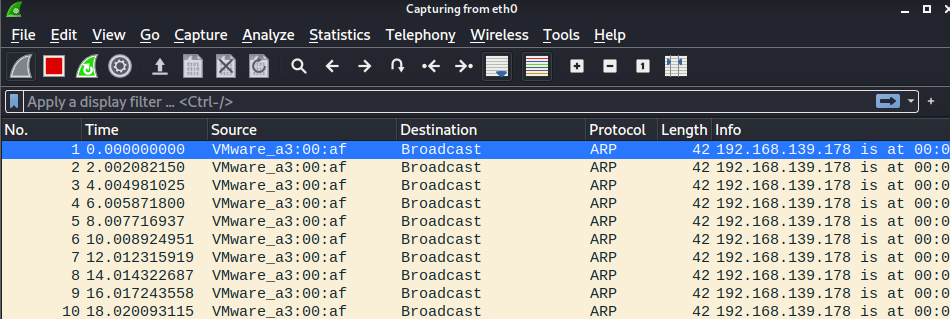
Arp zehirlemesi için "arpspoof" aracından yararlanacağım.

-"-i" komutu ile interface tanımlıyorum.

-Yapmış olduğum işlem sonucunda kendi adresimi saldırı gerçekleştirdiğim adrese atıyorum.



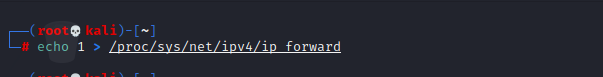
-Kontrolünü sağladığımda başarılı bir şekilde gerçekleştiğini görüyorum.



-Kontrolünü sağladığımda başarılı bir şekilde gerçekleştiğini görüyorum.

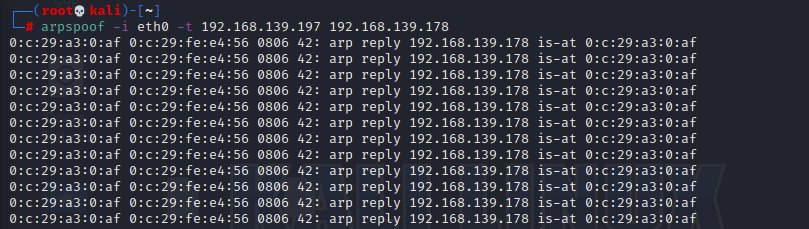
***ARP’nin kavranması ve IP Forwarding***

-MAC adresi atamadan sonra IP yönlendirmesi gerçekleştireceğim.

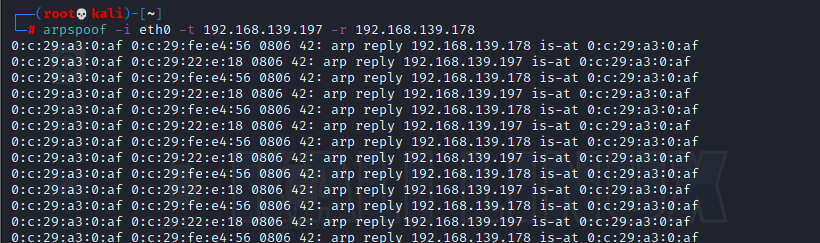


-“echo 1 > /proc/sys/net/ipv4/ip\_forward" komutu ile içerisine dosya yazmaya kapalı dizine bir yönlendirme yazıyorum.

-Artık IP adresleri içinde bir yönlendirme gerçekleştirebilirim.



-Öncelikle ARP saldırı gerçekleştireceğim IP adresini "-t" parametresi ile gösteriyorum ve daha sonrasında Fiziksel adresi atadığım cihazın IP adresini yazıyorum.



-Aynı işlemi "-r" komutu ile bir de tersine çalıştırıyorum.

-Artık Wireshark üzerinde kontrol ettiğimde ikisi arasında geçen bağlantıyı ele geçirmiş bulunuyorum.

***HTTP Packet Sniffing***

-ARP Poising ile ilgili bir alıştırma daha gerçekleştirmek istiyoruz.

-Bir adet Linux makinem var IP Adresi 192.168.139.178

-Bir adet sunucum var IP adresi 192.168.139.197

-Bir adette saldırı gerçekleştireceğim Linux Makinem var IP adresi 192.168.139.176

Sırasıyla;

-Etrafı Keşfet

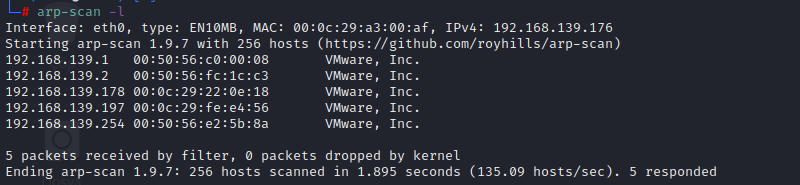
-Sniffer'ı hazırla(Wireshark)

-IP Yönlendirmeni aç.

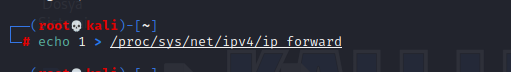
-MITM ol.(Arpları çift yönlü zehirle)

-Sniff et.

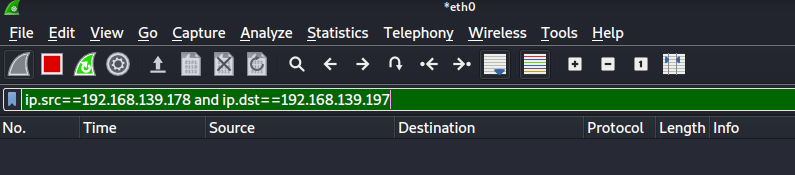
İşlemlerini uygulayacağım.



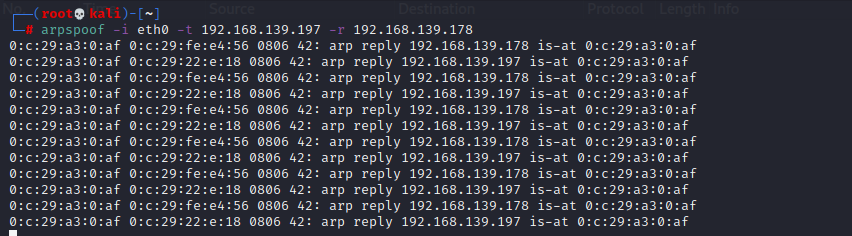
-Saldırı gerçekleştireceğim makine üzerinde bir "arp" taraması gerçekleştiriyorum.Burada makineleri görüntülüyorum.



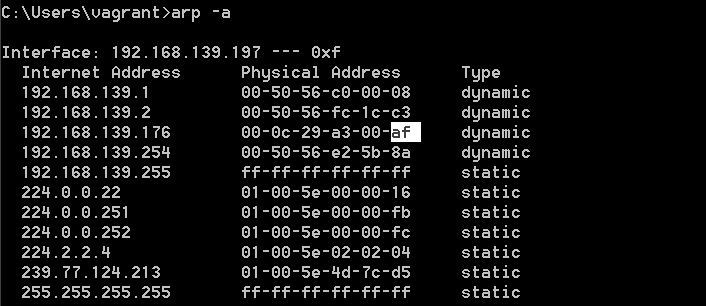
-IP yönlendirmesini aktif ettim.



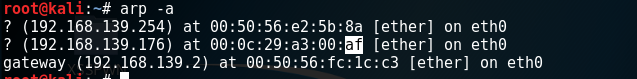
-Wireshark'ı da aktif hale getiriyorum.



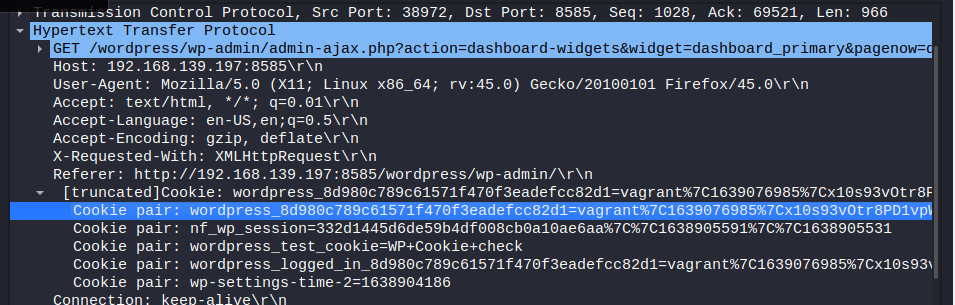
-Zehirleme işlemini başlatıyorum.



-Server üzerinden "arp -a" ile arp tablosuna bakıyorum ve başarılı bir şekilde adres değiştiğimi görüntülüyorum.



-Aynı işlemi Linux makinemde'de gerçekleştiriyorum ve burada da başarılı bir şekilde adres değişikliği sağlanmış.



-Wireshark üzerinde kontrol sağladığım da başarılı bir şekilde girilen bilgilere erişebildim.

***DNS Spoofing***

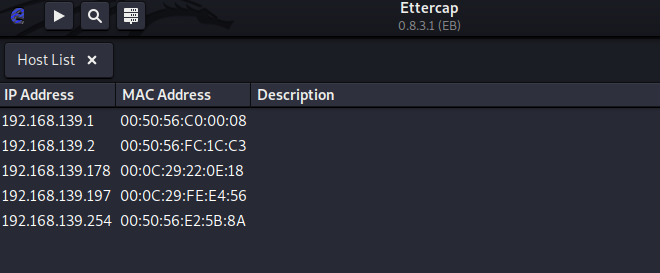
-DNS Spoofing işlemi ile devam ediyoruz.

-Bilgisayarlar isimlerden birşey anlamıyor.Burada IP'ler üzerinden işlemler yapılır.DNS Sunuculardan gelen bilgiler ile gerçekleştiriyor.

-Bu işlemi evlerde de olduğu gibi Gateway(254) üstlenir.Burada Gateway yerine geçip bilgi sızdırmaya çalışacağız.

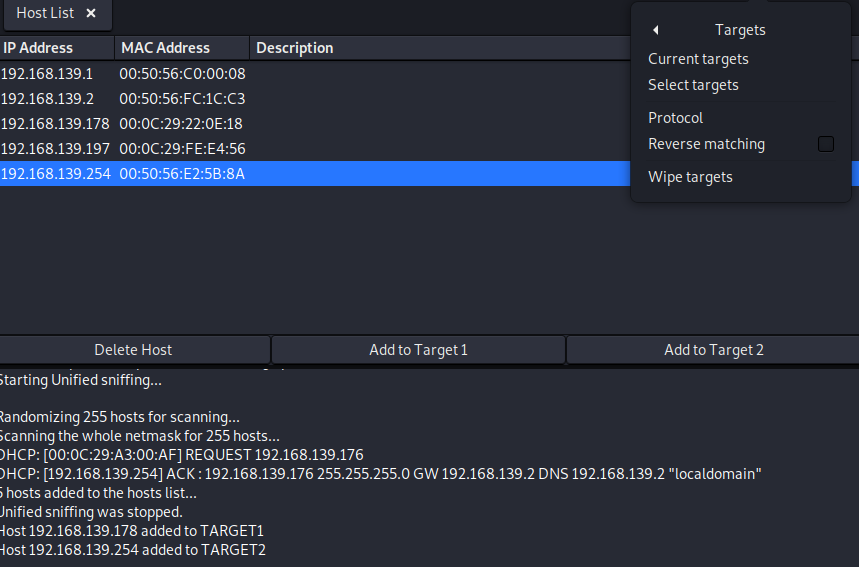


-Bu işlem için Linux üzerinde kurulu olarak gelen "Ettercap" aracından yararlanacağız.



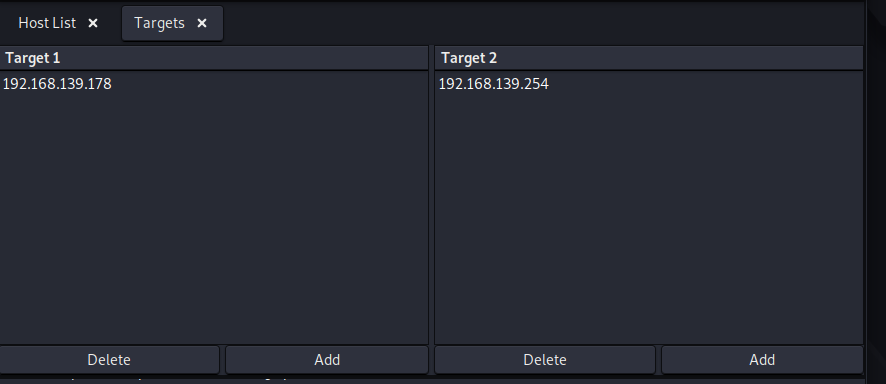
-"Arama" butonu üzerinden bir ARP taraması gerçekleştiriyorum.

-Karşıma "arpscan -l" tarama sonucuna benzer bir sonuç geldi.

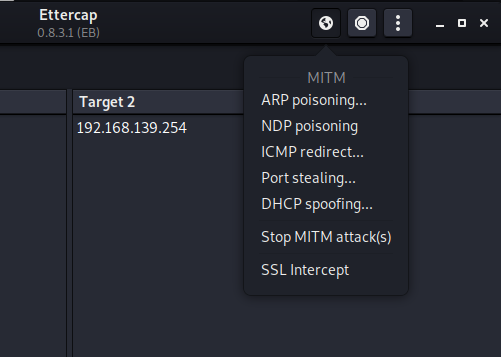


-İletişim kuracak makineyi "Target1",Gateway adresini de "Target2" olarak set ettim.

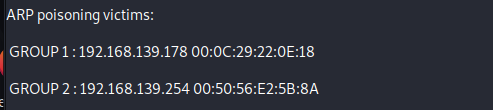
-Ardından sağ tarafta ki buton'dan target kısmından kontrol sağlıyorum.



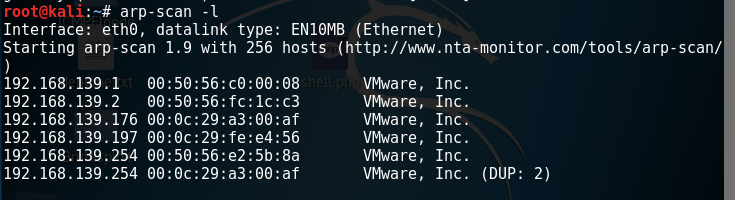
-İşlemin başarılı bir şekilde gerçekleştiğini görüntülüyorum.



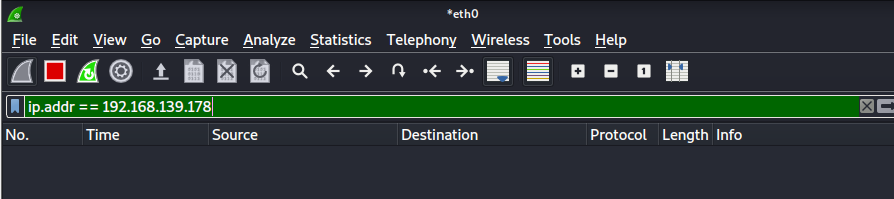
-"Dünya" butonuna basıyorum ve açılan sekmeden ARP Poisoning ile devam ediyorum.



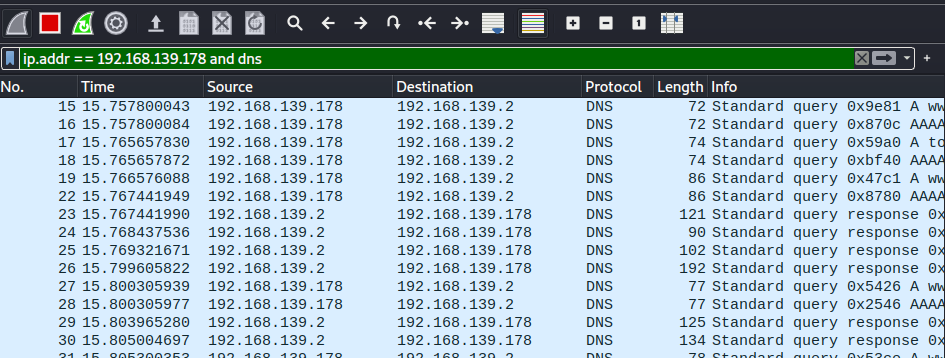
-İşlem sonrasında alt tarafta bulunan bilgilendirme kısmından zehirlendi diye bildirim gelmektedir.



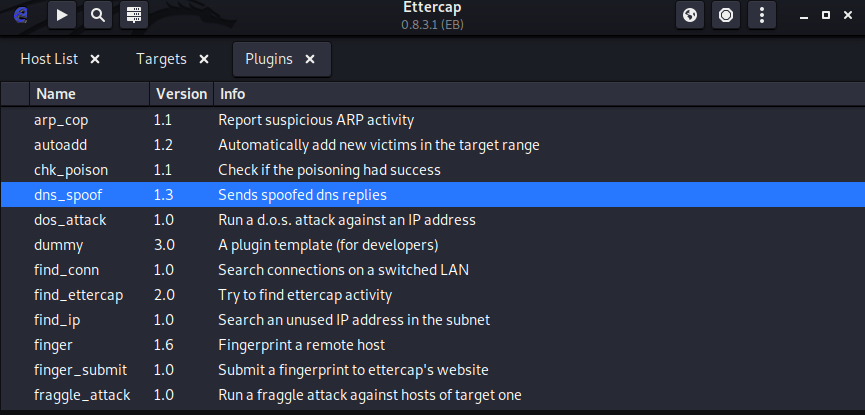
-Kontrol sağladığımda zehirlenme işleminin gerçekleştiğini burada görüntülüyorum.



-Sniff aracımı hazır konuma getiriyorum.



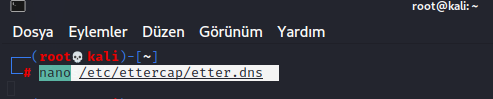
-Ardından Zehirlediğim Linux üzerinden bir tarama gerçekleştiriyorum ve gerekli bilgiler Wireshark üzerine düşüyor.



-Ettercap üzerine geçiyorum ve işlemi durduruyorum.

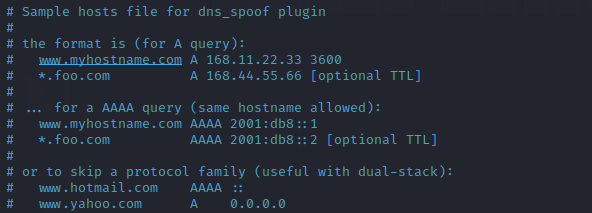
-Ardından ayarlar kısmına geçiyorum ve oradan Plugins bölümüne giriyorum.

-Plugins bölümünde yer alan "DNS Spoofing"e çift tıklıyorum ve başlatıyorum.



-Plugin üzerinde ayarlama yapılması gerektiği için Uçbirime geçiş yapıyorum.

-"nano /etc/ettercap/etter.dns" komutu ile açıyorum.

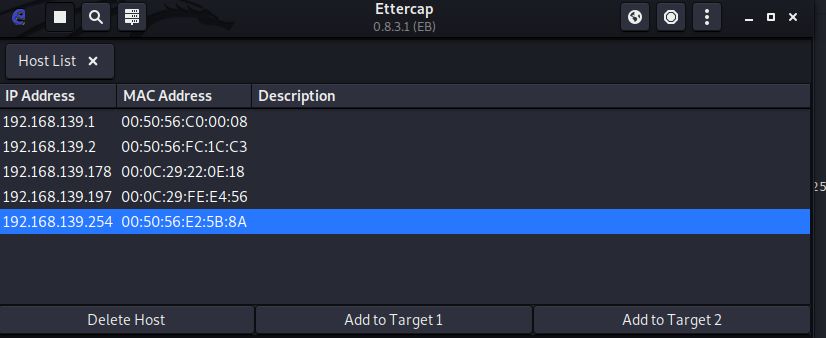


-Burada karşıma örnek olarak verilmiş bir kaç tane yapı çıkmaktadır.

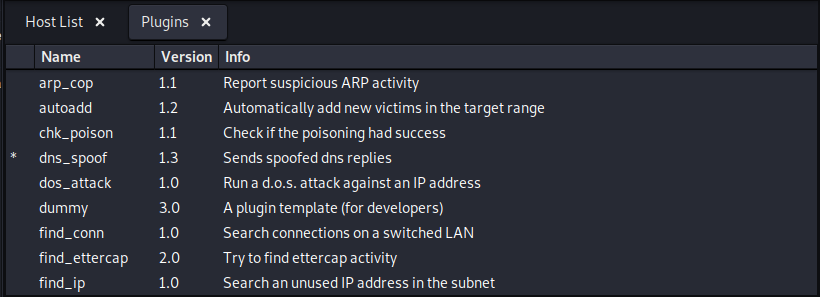


-Bu örneklerde olduğu gibi en alt kısmına bende ekleme gerçekleştiriyorum.

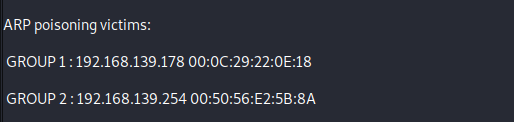
-Burada rastgele iki adet websitesi yerleştiriyorum ve kaydediyorum.



-Ettercap aracımı tekrardan başlatıyorum ve burada yine aynı ayarlamaları yapıyorum.

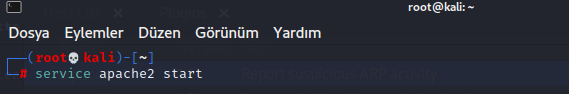


-Ardından burada plugin kısmından "DNS Spoof" işlemini aktif hale getiriyorum.

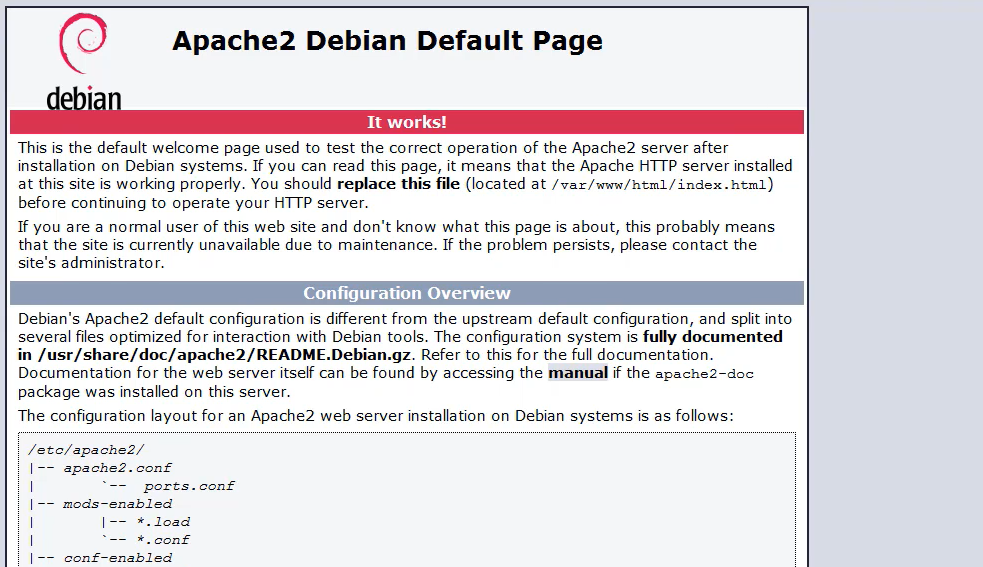


-Gerekli ayarlamalardan sonra işlemi başlatıyorum.

-Burada zehirlendiğini görüntülüyorum.



-Zehirleme işleminin ardından benden yönlendirme alabilmesi için "Apache2" servisini başlatıyorum.



-Zehirlenen makineme geçiş yapıyorum ve Yönlendirici kısmında verdiğim web sitelere buradan erişim sağlıyorum.

-Yaptığım zehirleme sonucu istediğim yere yönlendirme gerçekleştirebildim.

***DHCP Spoofing(Rogue Server) Saldırısı***

-Ortamda DHCP olup paket yakalamayı hedefleyeceğiz.



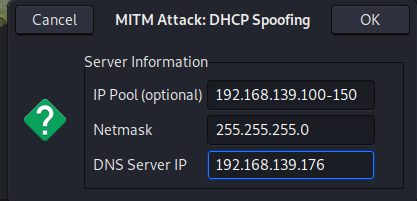
-Öncelikle DHCP süreçlerini hatırlatmak isterim.

-Bunları "DORA" olarakta hatırlayabiliriz.



-Bu işlem için yine "Ettercap" aracından yararlanacağız.

-Aracı başlattıktan sonra DHCP spoofing ile devam edeceğiz.

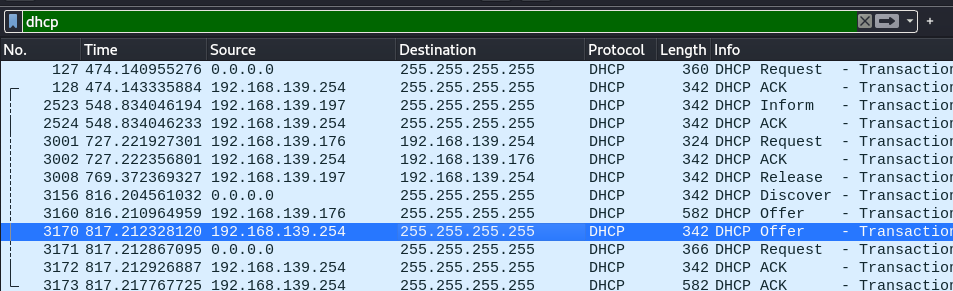


-Burada IP havuzunu rastgele belirliyorum.

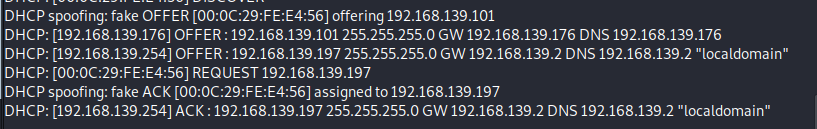
-Netmask'ı belirtiyorum.

-DNS Server IP bölümüne ise kendi IP adresimi yazıyorum.

-Ardından saldırıyı başlatıyorum.



-Wireshark üzerinde "dhcp" üzerine bir tarama gerçekleştirdiğim de karşıma gelip giden paketler çıkıyor.



-Ettercap üzerinden de istenen paketleri görüntüleyebiliyoruz.

***DHCP Starvation Saldırısı***

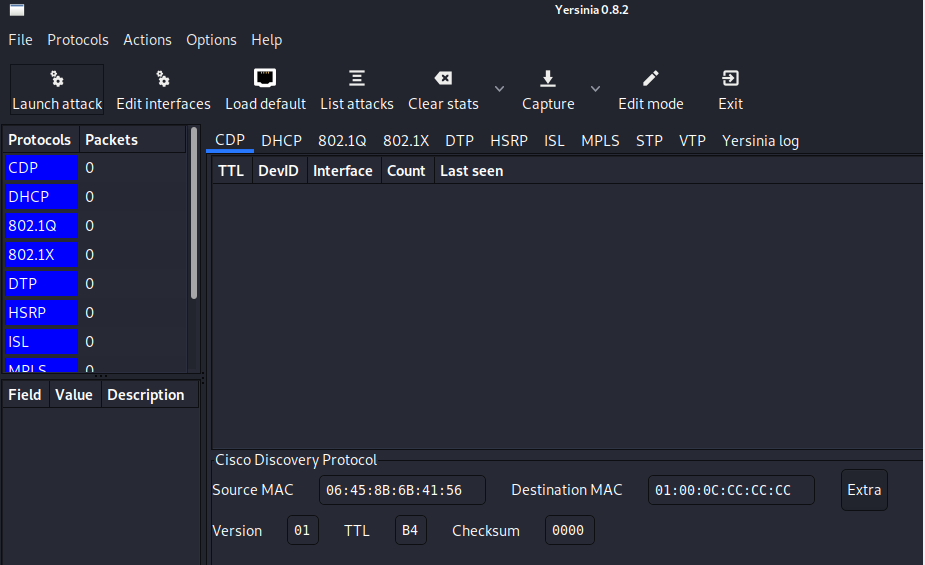
-Bu atak ile ortama sürekli Discover paketi göndereceğiz bunu almaya çalışan DHCP Server ise meşgul hale gelicek.

-DHCP Server'a DOS Attack bu şekilde gerçekleştirilebilir.

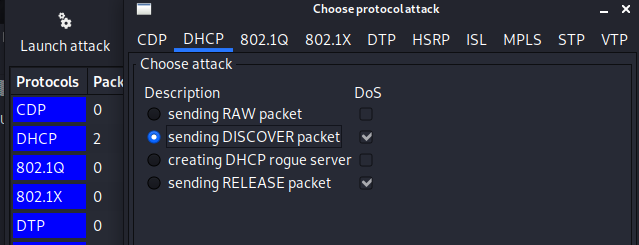


-Bu işlem için Linux üzerinde kurulu olarak bulunan "yersinia" aracını kullanacğım.

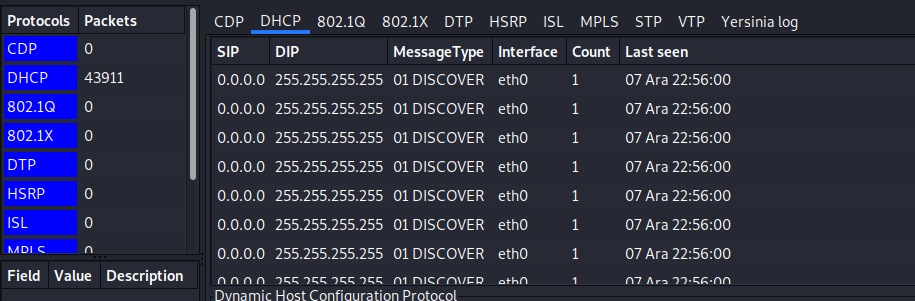
-"yersinia -h" ile kullanımıyla ilgili bilgi sahibi olabiliriz.



-"yersinia -G" ile grafik moduna geçiş yapıyorum.

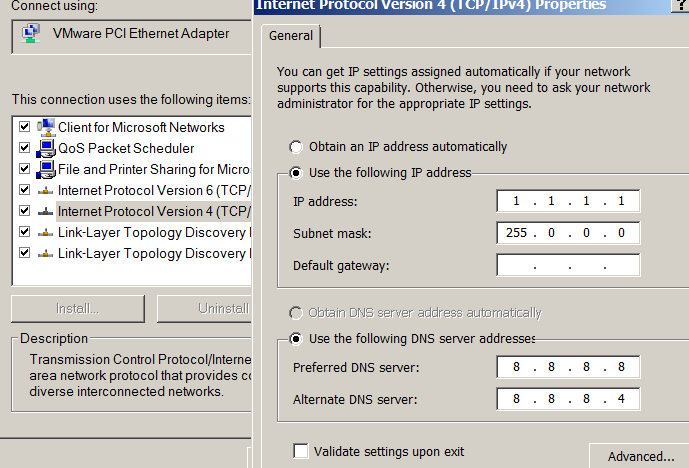


-Ardından "launch attack" butonuna basıyorum ve burada "DHCP" protokolü üzerinde "Discover" paketleri göndereceğimi belirtiyorum.



-Ortama gönderdiğim paket miktarını şuan da görüntüleyebiliyorum.

-Bu miktar git gide artmaktadır.



-Ortama gönderdiği paketlerin etkisini görmek için sunucuya statik olarak bir Ip adresi tanımladım.

-Saldırı işleminin ardından bu değerleri otomatik olarak almasını isteyeceğim.



-Otomatik olarak IP almasını istediğim de IP alamadığını görüntülüyorum.