|  |
| --- |
| ***NMAP*** |
| Kaan Efe Öğüt  *ADLİ BİLİŞİM MÜHENDİSLİĞİ* |
| Linux aracı üzerinde kurulu olarak gelen Nmap aracı ile IP adresini bildiğimiz bir sunucunun Ağ haritası hakkında nasıl bilgi toplayabiliriz bunun hakkında bilgi vereceğim. |

**09.08.2021**

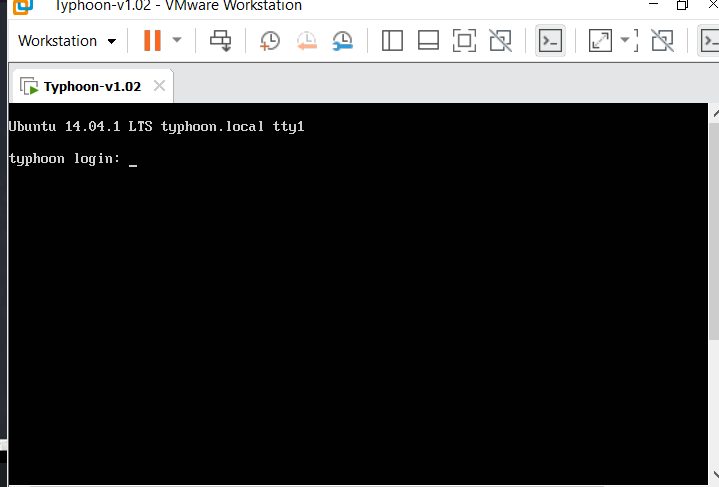
***Nmap’e Giriş***

-Öncelikle Nmap aracını kullanabileceğim zafiyet bulunan bir sanal makinaya ihtiyacım var.

- "https://drive.google.com/file/d/1fPGBGcmCgvoAejVUGtb-0PqGYnEDcdeB/view" bağlantısı üzerinden içerisinde zafiyet bulunan “Typhoon” isimli aracı indiriyorum.

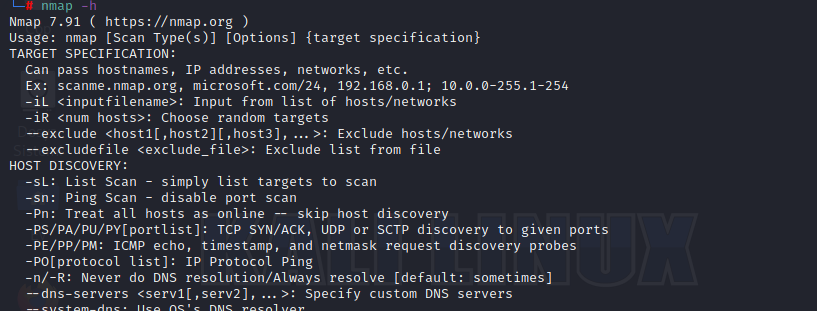
- Ağ bağlantısını hem sanal makine üzerinde NAT hem de typhoon aracı üzerinden NAT konumuna getirilmelidir.Aksi takdirde makineler birbirini görmeyecektir.

-



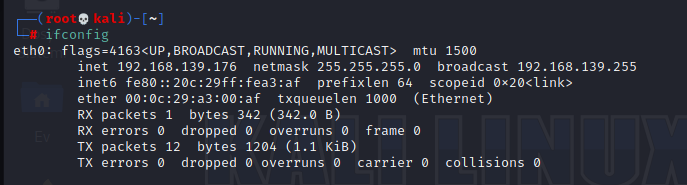
-Ardından sanal makineyi çalıştırıyorum ve hiçbir işlem gerçekleştirmeden bekliyorum.Tüm ayarların sonrasında login ekranı gelecektir.Bu ekran üzerinde arka planda çalışacak.,

-Linux makineme geçiş yapıyorum



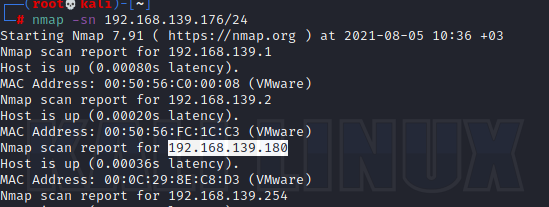
-Uç birim üzerinde "nmap -h" komutu ile nmap üzerinde gerçekleştirebileceğim fonksiyonları görüntülüyorum.

- Nmap ile typhoon aracı üzerinde bir tarama gerçekleştirmek istiyorum.



-Bu sebeple NAT bağlantısı yaptığım için önce Ip adresimi "ifconfig" ile öğreniyorum.

-Ip adresim üzerinden Nmap aracı ile bir tarama gerçekleştiriyorum.



-"nmap -sn Ip" ile Ip adresi üzerinde ki tüm cihazları görüntülüyorum.

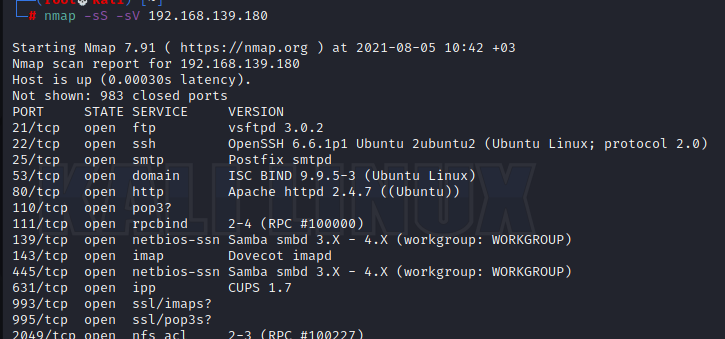
-Sonu 180 olan Typhoon aracımın Ip adresidir.



-Basit bir şekilde “sS” parametresi ile SYN taraması yapıyorum ve açık portları buluyorum.

-Bu bilgiler her zaman doğru değildir.Bu doğruluğu -sV komutu ekleyerek deneyelim.

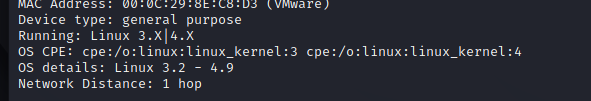
-“sV” parametresi versiyon bilgilerini görüntülüyorum.



-Versiyon bilgisi dönenler açık olduğu bilinenler dönmeyenler ise belirsizdir.

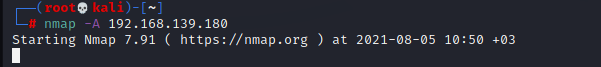
***Nmap Komutları-1***

-"nmap -O IP adress" düzeninde bir arama gerçekleştiriyorum.



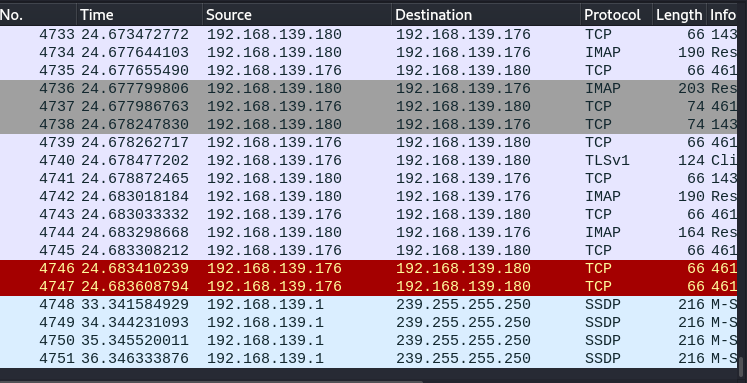
-Bu arama bana taramış olduğum sunucunun İşletim sistemi hakkında bilgi sahibi yapacaktır.

-Genellikle emin de olsa aralıklı şekilde bilgilendirme yapar.



-İşletim sistemi tespiti,Script taraması,Port-Version parametresi gibi işlemlerin hepsini ayrı ayrı yapmayıp tek seferde gerçekleştirmek için

-"nmap -A Ip adress" düzeni ile tarama işlemini başlatıyorum.Bu işlem biraz uzun sürecektir.

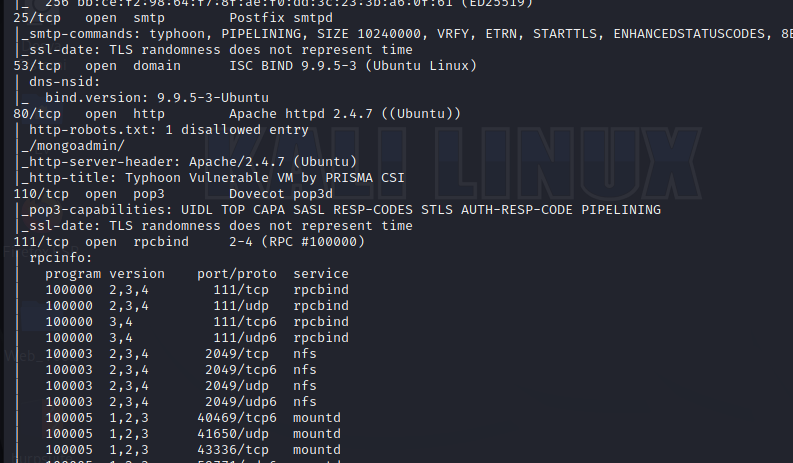


-Wireshark üzerinden işlem devam ederken inceleme yaptığımda sürekli istek gönderdiğini görüntülüyorum.

-Wireshark üzerinde inceleme yaparken Nmap aracımın yapmış olduğu tarama sonuçlandı.

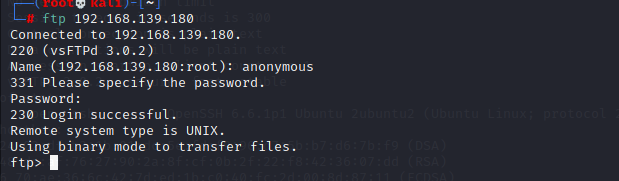


-Çıktıların hepsini gösteremesem de bir kısmını 1-2 SS ile göstermek istiyorum.



-Port taramasına kadar gerçekleştiğini görüntülüyorum.

-Ayrıca dikkatim Anonymous olarak giriş yaptığı çekiyor. (Bir önceki sayfada) ,



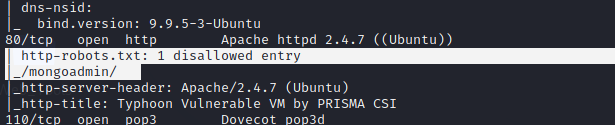
-FTP bağlantısı kullanarak Anonymous olarak giriş yapmaya çalışıyorum.

-Girişi başarılı olarak gerçekleştirdim.Burada linux komutlarını kullanabiliyorum.



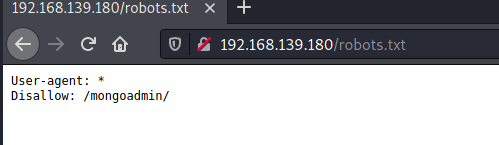
-Ftp bağlantısı kurduğumda LS komutunu çalıştırıyorum fakat dosya olmadığı için geri bir şey döndürmüyor.

-Ayrıca burada “back-up” dosyaları yer alabilirdi bu da tüm bilgilere erişim yapmama olanak sağlardı.



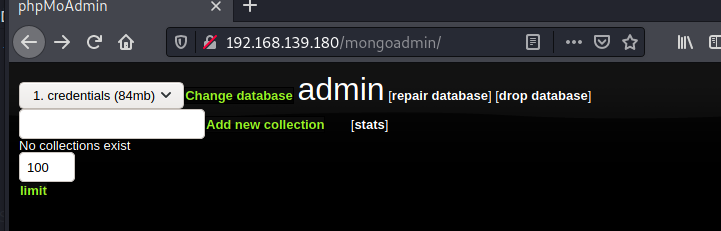
-İçerisinde robots.txt ve mangoadmin bulunduğunu görüntülüyorum.Buradan bir bilgi çekme işlemi gerçekleştirebilirim.

-Tarayıcı üzerinden “/robots.txt” uzantısını açıyorum.

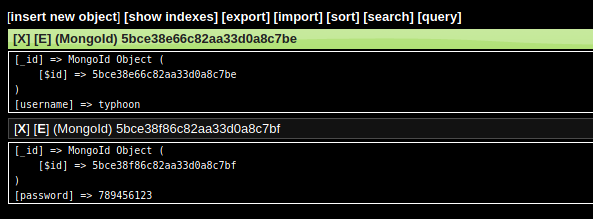


-Burada da ” mongoadmin” bilgisine erişiyorum.

-Tarayıcı üzerinden “/mongoadmin” uzantısını açıyorum.

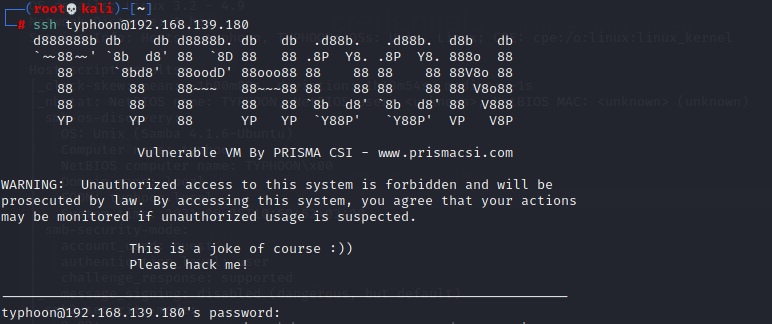


-Burada açılabilir sayfalar üzerinde bilgi arıyorum.

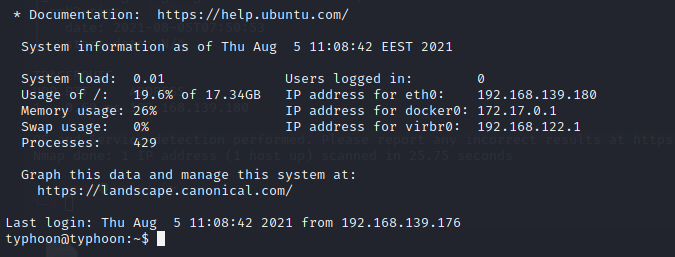


-Mongo admin üzerinde “Change database” üzerinden “credits” bölümüne geçiyorum ve burada bir kullanıcı adı ve şifre yakalıyorum.

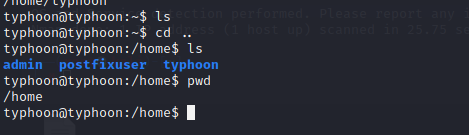
-Bu kullanıcı adı ve şifreyi kullanarak SSH bağlantısı kurabilirim.



-SSH "kadı@ıp" düzeni ile bir bağlantı isteği gönderiyorum.Bağlantı için tarafıma bir Password ekranı geliyor.



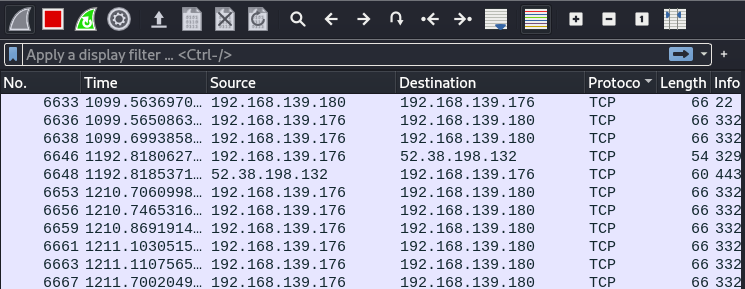
-Sisteme başarılı bir şekilde sızdım artık istediğim komutu gerçekleştirebilirim.



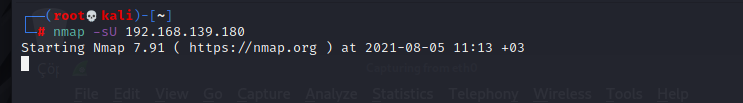
-Dizinler arasında geçiş işlemi yapıp istediğim bilgiyi toplayabilirim.

***Nmap ile TCP/UDP Taraması***

-Nmap tarama esnasında belirtmediğimiz sürece UDP taraması gerçekleştirmez.

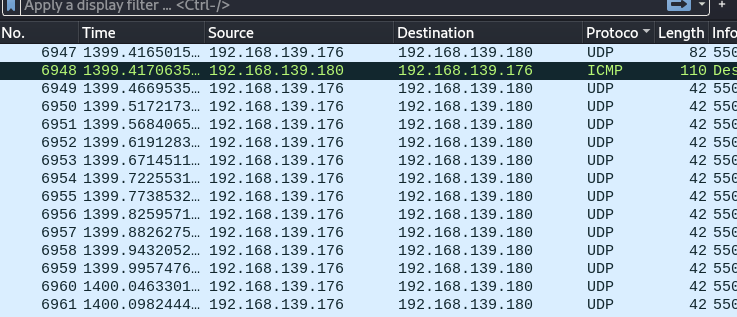


-Bunu wireshark üzerinden incelediğimizde görüntüleyebiliyoruz.

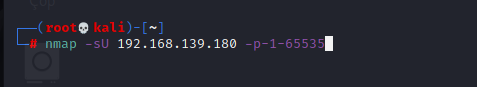


-UDP port taramasını Uçbirim üzerinden "nmap sU IP" şeklinde tarama başlatıyorum.Bu işlemi sT ile gerçekleştirseydim TCP paketi gönderecekti.

Ardından Wireshark üzerinde inceleme gerçekleştiriyorum.



-Wireshark üzerinde UDP taraması gerçekleştirdiğini görüntülüyorum.



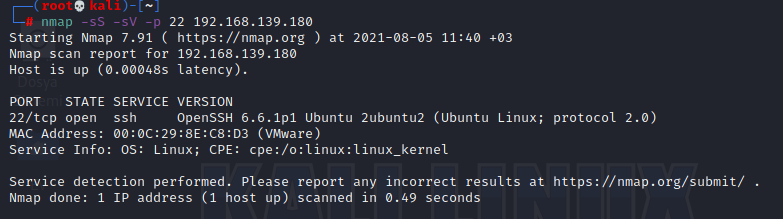
-İstediğimiz Portu tarama işlemini de -p-1-65535(Bu kısmı değiştirerek) gerçekleştirebiliriz.

-Hiç port belirtmezsek popüler olarak bulunan portları tarayacaktır.Bu port tablosunu kesinlikle bilmemiz gerekmektedir.

-Ayrıca Nmap üzerinde popüler portlar taranıp o düzene göre port değerleri değiştirilebilir.

-Bu sebeple tüm portları taramak çok daha mantıklı olacaktır.

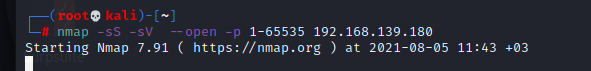
***Nmap Komutları -2***



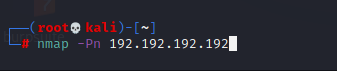
-Sadece SSH portunu sorguluyorum ve SSH hakkında çok detaylı bir bilgi sahibi olabiliyorum.

-“p1-65535” komutu ile Tüm portları tarayabiliriz.

-Tüm portları tarama işlemini başlatıyorum.



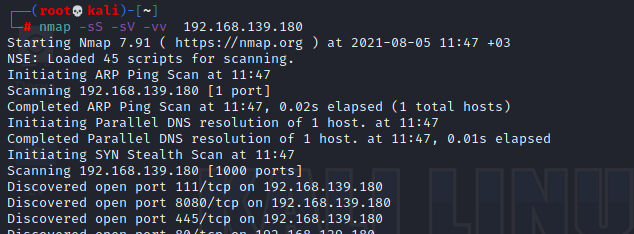
-"-open" komutunu ekleyerek sadece açık olan portlar hakkında bilgi sahibi olabiliriz.



-Tarayacağımız sunucu üzerinden bir Firewall olabilir ve bu da ping gönderme işlemi sırasına bize bilgi dönmesini engelliyor.

-Burada nmap aracı -Pn parametresini kullanmamızı önerecektir.

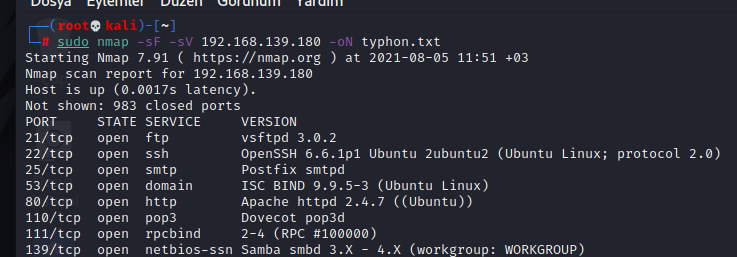
-Bu parametre ile ping göndermeden bir tarama gerçekleştirebiliriz.



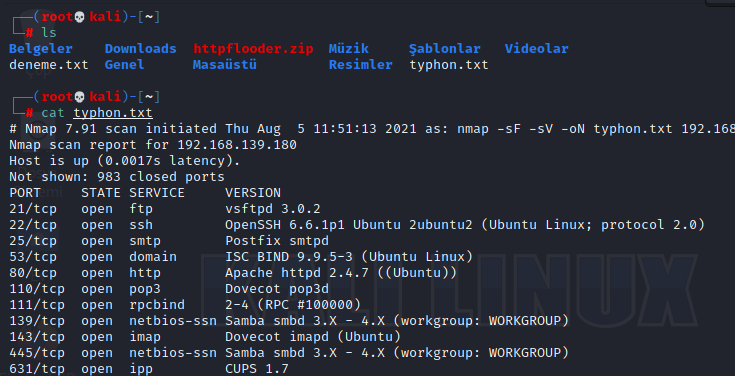
-"-vv" parametresi ile sistemde gelişen tüm olayları görüntüleyebiliriz.Bu metasploit üzerinde ki “verbose” işlemidir.

***Nmap Komutları -3***

-Bu sefer FIN paketi gönderme işlemi gerçekleştireceğiz.



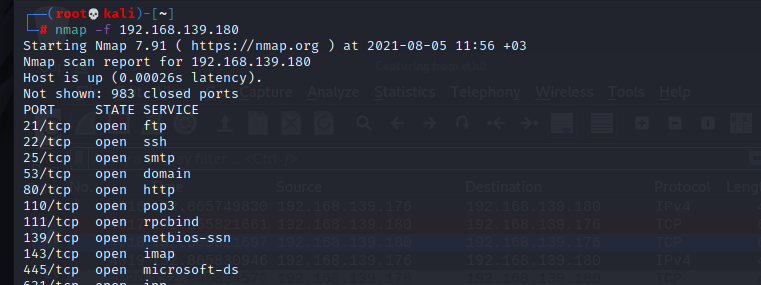
-"-oN" parametresi ile tarama işlemi sonucu denen işlemleri bu txt dosyasına yazacaktır.



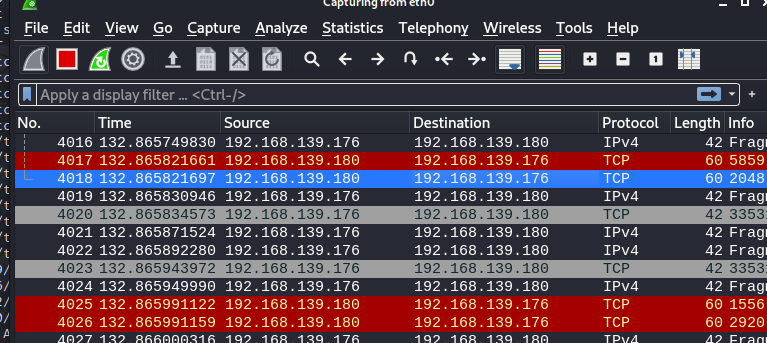
-Nmap’i çalıştırdığım dizin üzerinde bu işlemin sonuçları kayıt edilecektir.

***Nmap Firewall ve IDS Atlatma***

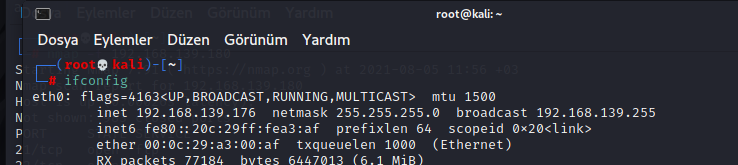
-Eğer sistemde IPS/IDS sistemleri var ise bunları nasıl atlatabileceğimizi inceleyelim.



-“-f” Parametresi : Firewall 2000 Bayt üzerinde ki rakamları kabul etmiyor(Sunucuda böyle ayarlanmış).

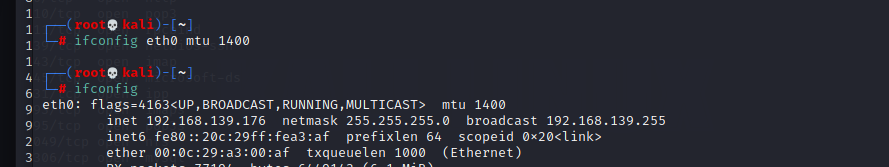


-Bu işlemi Wireshark üzerinde izlediğimiz zaman paketleri böldüğü için diğer Nmap taramalarına göre daha çok paket gönderdiğini görüntülüyoruz.

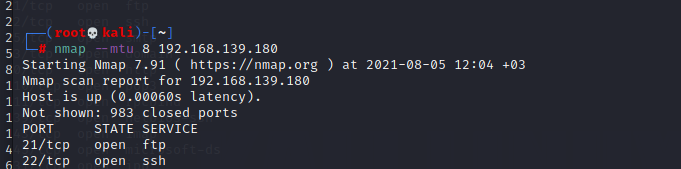


-Ifconfig işlemini gerçekleştirdiğimde burada bir MTU değeri görüntülüyorum bu değer gönderilebilecek en yüksek paket boyutudur.

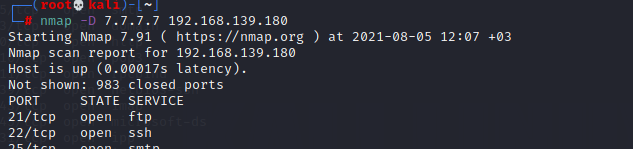
-Bu paket boyutunu ayarlayıp nmap üzerinden ona göre bir işlem gerçekleştirebiliriz.



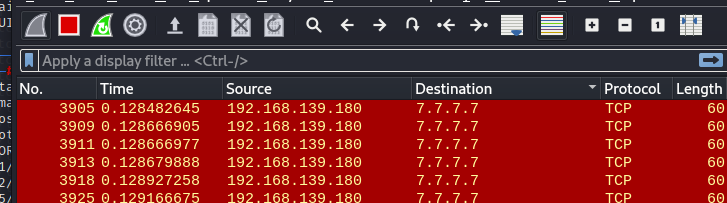
-Ayrıca bu sunucu üzerinde ki mtu değerini de bu şekilde değiştirebiliriz.



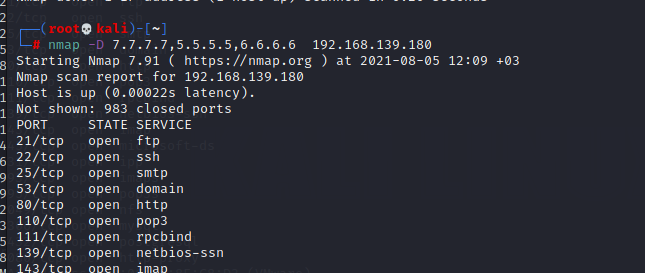
-"nmap --mtu 8 192.168.139.180" komutu ile mtu değerini 8 parçaya bölüp paketleri gönderme işlemi gerçekleştirebiliriz.



-IP Adresimizin gizlenmesini istersek.Bunu "-D Host" ile gerçekleştirebiliriz.



-Bu giden paketleri Wireshark üzerinde incelediğimiz zaman giden paketlerin 7.7.7.7 adresi üzerinden gittiğini görüntülüyorum.



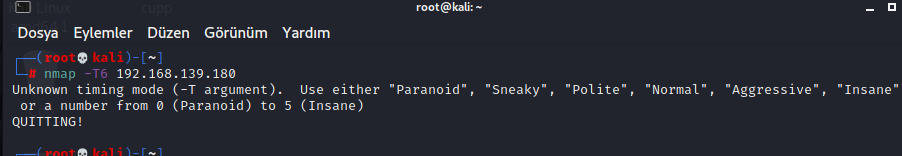
-Bu işlem tamamen kafa karıştırmak amaçlıdır. 7.7.7.7,6.6.6.6,5.5.5.5 Ip adresleri ile işlem gerçekleşebilir.Burada Firewall şaşırabilir.

***Nmap Timing Ve Performance Komutları***

***Timing***

-Bu komut ile saniyede gönderilecek paketlerin hızlarını belirtiyoruz.

-Tarama hızlarını görüntüleyebiliyoruz.

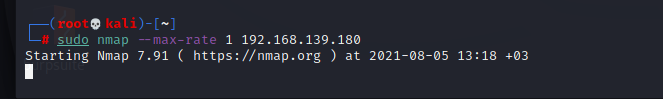


-Tarama hızları arttıkça sunucuya yapılan yüklenme o oranla artacaktır.O sebepten ötürü tarama hızı olarak 3 önerilmektedir.

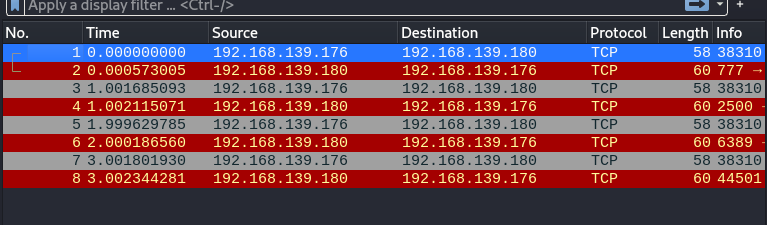
-Sürekli istek gönderdiğimizde Firewall'ın algılaması da söz konusudur.

***Max&Min Rate***

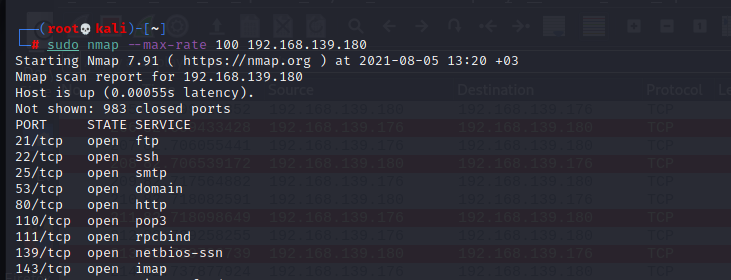
-Yanına verdiğimiz sayı ile saniyede gönderilecek max veya min. paket sayısını ayarlayabiliyoruz.



-Yazımı bu şekilde olup işlem başladıktan sonra Wireshark üzerinde inceleme yapıyorum.

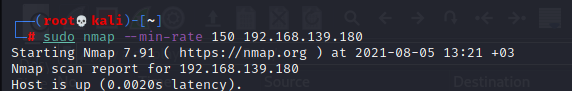


-Saniyede bir paket gönderimi yaptığını görüntülüyorum.



-Ayrıca bu ayarı saniyede 100 paket gönderecek biçimde ayarlayabiliyorum.

-Maksimum gönderebileceği paket sayısını ayarlayabildiğimiz gibi minimum gidecek paket sayısını da ayarlayabiliyoruz.



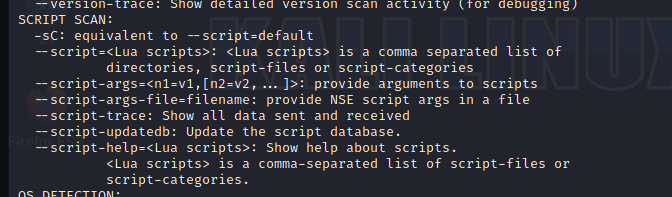
-Saniyede en az 150 paket gönderim işlemi gerçekleştiriyorum.

-Bu işlem sunucuya çok yük yükleyeceği için çökebilir veya ağ alt yapımız iyi değilse çökme işlemiyle karşılaşabiliriz.

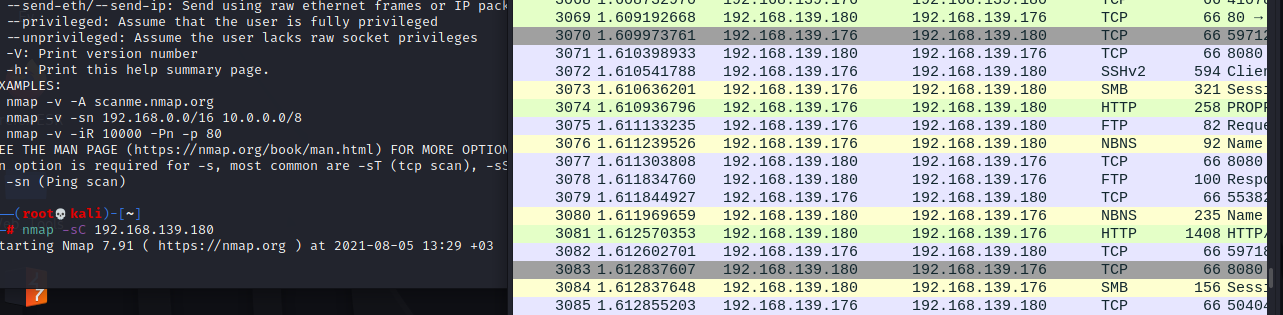
***Nmap Script Kullanımı***

-Scriptler BruteForce,Zafiyet tespiti,Kritik bilgileri ifşa etmek için kullanılır.

-Linux makinemiz üzerinde uç birimi açıyoruz.

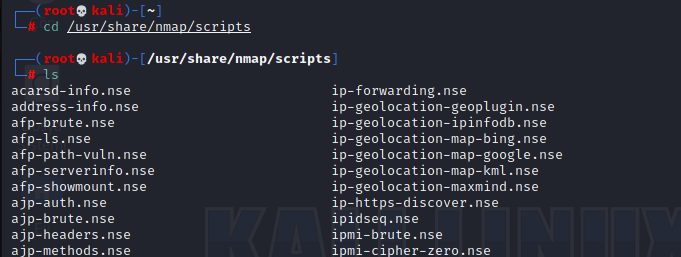


-Uçbirime yazdığımız “nmap –h” komutu ile script kullanımı hakkında bilgi ediniyoruz.



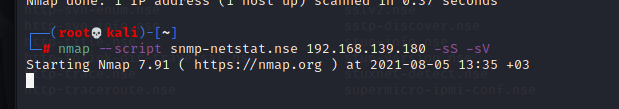
-“Nmap -sC IP” düzeni ile Nmap üzerinde ki tüm scriptler denenecektir.Bu çok fazla trafik yaratacaktır yan tarafta Wiresharkı da açıp trafiği görüntüleyelim.

-İlla default olarak aynı script üzerinde işlem gerçekleştireceğiz diye bir zorunluluk yok burada “Nmap/script” içerisinde bulunan scriptleri kullanabiliriz.

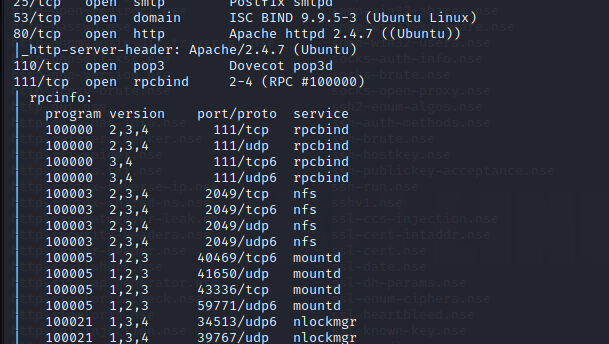


-Cd komutu ile Nmap'in scriptlerinin olduğu kısıma geliyorum ve burada scriptleri görüntülüyorum.

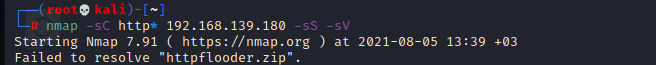
-Buradan istediğimiz scripti kullanabiliriz.



-Bu scripti kullanıp işlem gerçekleştirebiliriz.Eğer bu işlem sırasında bir açık bulunursa tarafımıza döndürecektir.

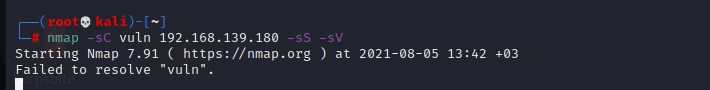
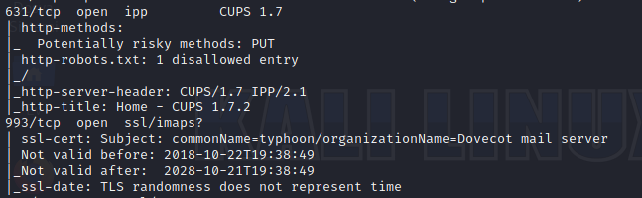


-Burada görüntülediğimiz de açık olan dosyalarla ilgili bilgi sahibi oluyorum.



-Bu şekilde arama yapmak yerine istediğimiz alan üzerinde script denemesi yapmak istersek;

-HTTP alanında bir Script çalışması gerçekleştirmek istersek öncelikle Port Numarasını öğreniyorum.



- Ayrıca bu işlemi Vuln& Vuln\* parametresi ile de gerçekleştirebiliriz.

-Vuln içerisinde bulunan tüm parametreleri deneyecektir.



- Saldırı yaptığımız alanda Firewall'la ilgili bir açık bulundu bunun hakkında bir bilgimiz yok ise bu komut ile bilgi sahibi olabiliriz.