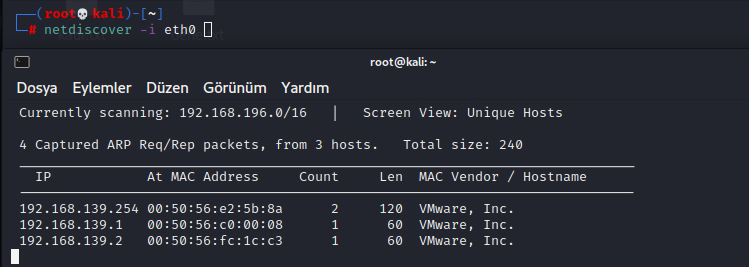
|  |
| --- |
| ***SCANNING*** |
| Kaan Efe Öğüt  *ADLİ BİLİŞİM MÜHENDİSLİĞİ* |
| Penetrasyon testlerinin ikinci aşaması olan tarama aşamasında kullanılan araçları göstereceğim. |

**13.12.2021**

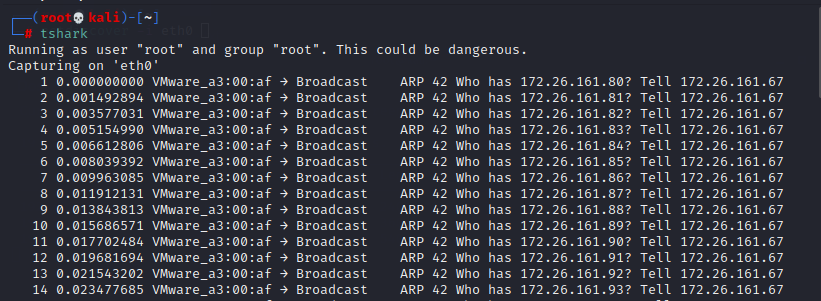
***Netdiscover & Nmap Scan ile Host Discovery***

-Bulunduğumuz ağ üzerinde bulunan cihazların tespiti için bu araçlar kullanılır.



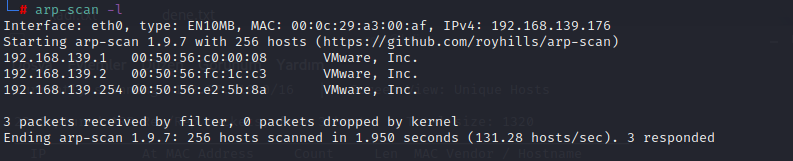
- Netdiscover aracı ile "eth0" üzerinde bulunan cihazların tespitini gerçekleştirdik.

-Bu araç ARP Paketi göndererek işlem yapmamıza olanak sağlar.



-"Tshark" üzerinden gelen giden paketleri kontrol ettiğimde ARP paketlerini de görüntüleyebiliyorum.

-Tshark->Wireshark aracının konsol üzerinden çalışanıdır.



-Bu işlemi "arp-scan" aracı ile de gerçekleştirebiliriz.

-"arp-scan -l" komutu ile host üzerinde bulunan cihazları görüntüleyebiliriz.

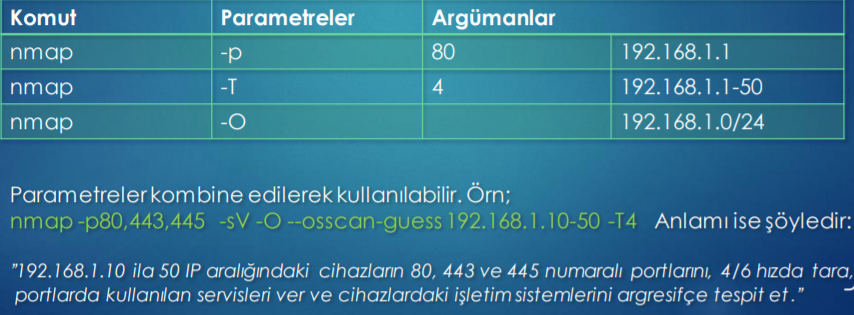
***Nmap Cheat Sheet***

Nmap Komut ve Parametreleri

-Nmap;penetration testleri sırasında en çok kullanacağımız araçlardan biridir.

-Bu araç,ağdaki cihazlar için tarama,tespit ve keşif yapabilen gelişmiş ve ünlü bir programdır.

-Kullanımıyla ilgili bir kaç tane görsel eklemek gerekirse;



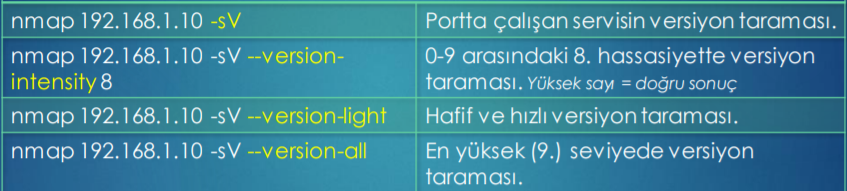
-Basit kullanım.



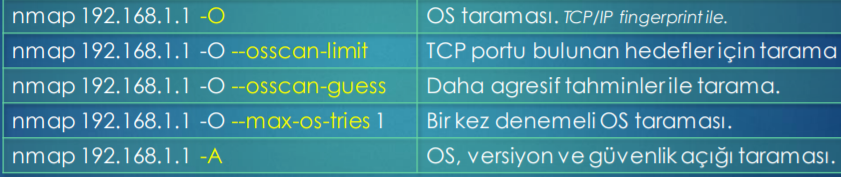
-Hedef tarama



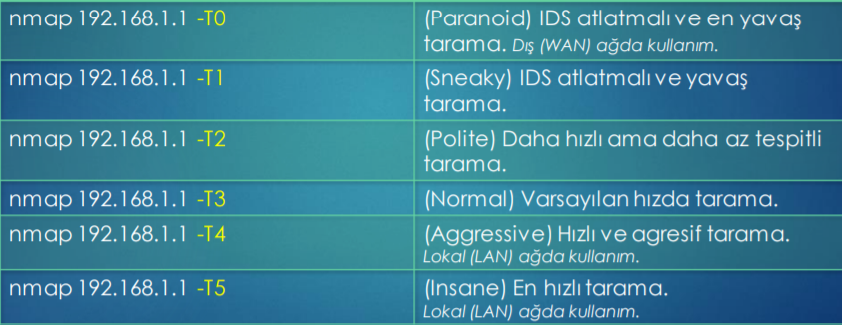
-Port tarama



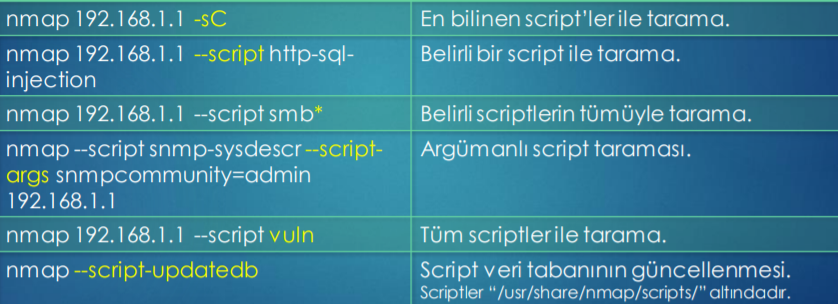
-Servis ve versiyon tarama



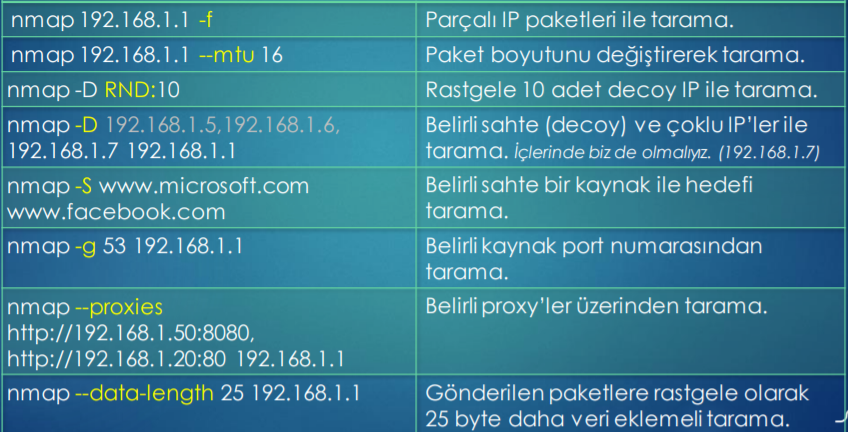
-OS Tespit Taraması



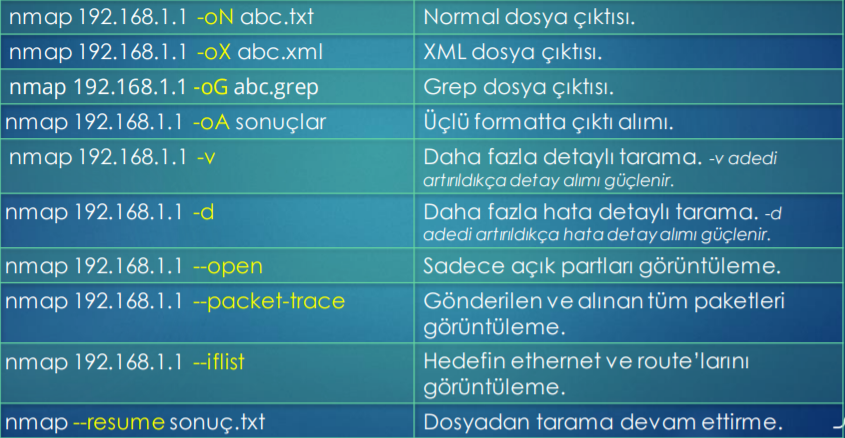
-Zaman ve performans ayarlı tarama



-Nmap Script Engine ile tarama

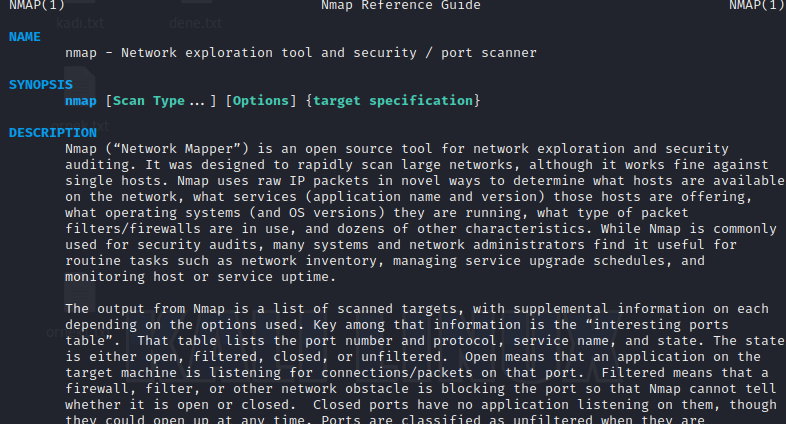


-Firewall ve IDS Atlatmalı Tarama

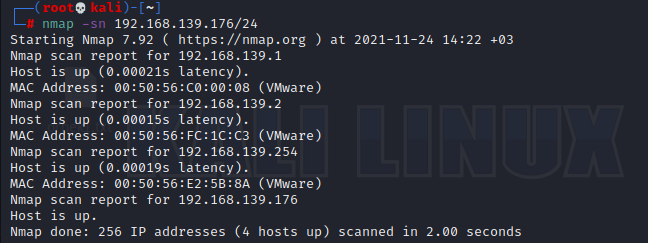


-Çıktı Alımlı Tarama

***Nmap Kullanımı ile Port,Servis ve OS Tespiti***



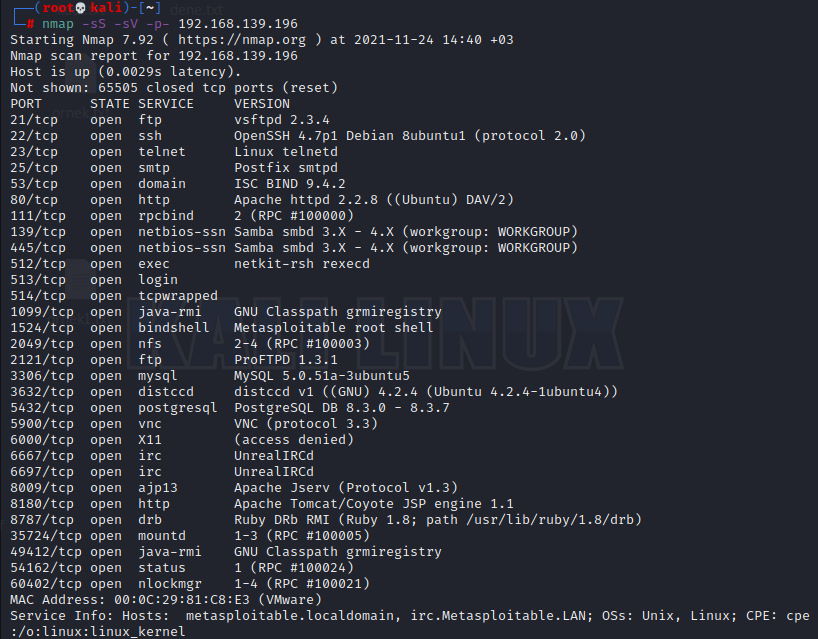
-"man nmap" komutu ile nmap aracının kullanımı hakkında bilgi sahibi olabiliriz.



-"nmap -sn IP" düzeni ile arama gerçekleştirdiğim de Ağ üzerinde bulunan hostlar hakkında bilgi sahibi olabiliyorum.



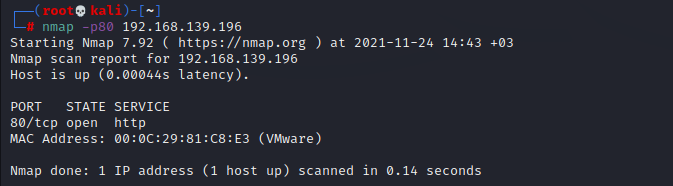
-"nmap -O IP -T4" komutu ile işletim sistemi hakkında bilgi sahibi olabiliriz.



-Bu yaptığım taramada tüm portlar üzerinde Syn paketi göndererek tüm portlar hakkında bilgi sahibi olmamı sağladı.

"-s" ile başlayanlar port taramasıdır.

"-p" ile balayan ise ping taramasıdır.



-Tüm portlar üzerinde işlem gerçekleştirebileceğim gibi tek port üzerinden de işlem gerçekleştirebilirim.

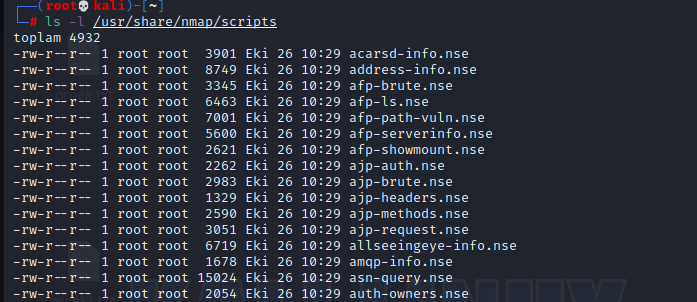


-Burada en kapsamlı top 100 port üzerinde agresif bir port taraması gerçekleştirdim.Burada ayrıca -A parametresi ile gerekli açıkları da bulmaya çalıştı.

-Nmap ile gerekli taramalardan sonra "NSE(Nmap Script Engine)" ile işlemlerimize devam ediyoruz.

***NSE Yardımı Alımı***

-NSE'yi verimli kullanabilmek için çeşitli scriptlerden yararlanırız.

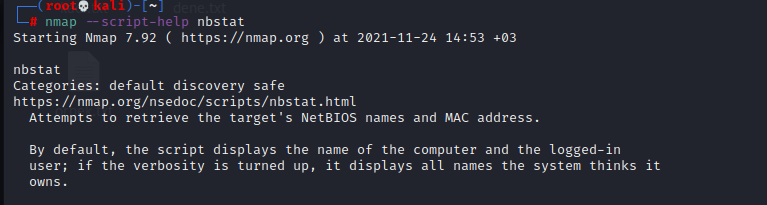


-Bu scriptler linux içerisinde "/usr/share/nmap/scripts" içerisinde bulunur.

-Sonlarına baktığımızda da ".nse" ile bittiğini görüntülüyorum.

-Burada istediğimiz Scripti " | grep" komutu ile de yakalayabiliriz.

-Ayrıca hiç konumu bilmediğimiz bir scripti locate komutu ile de tespit edebiliriz.



-Script hakkında bilgi almak içinde "nmap --script-help script\_adı" komutunu kullanabiliriz.

-Ayrıca bilgi kısmında verilen Tarayıcı üzerinden de gerekli bilgileri toplayabiliriz.

***NSE ile NETBIOS Discovery***



-Kullandığımız "nbstat" scripti ile BIOS versiyonu hakkında bilgi toplamamıza yardımcı oldu.

-Fakat burada bir hata gerçekleştirdim.Port belirtip işlem yaparsam bu işlem çok daha çabuk gerçekleşecektir.

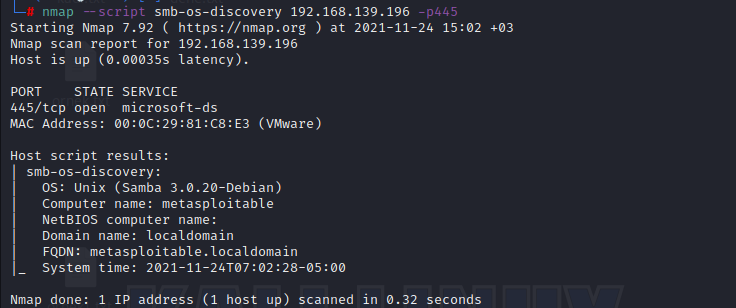
***NSE ile SMB Enumeration***

-SMB(Server Message Block) bu bir protokoldür.Ağdaki cihazların yazıcı vs paylaşmasını sağlar.

-SMB servisi 445 portu üzerinde çalışır.

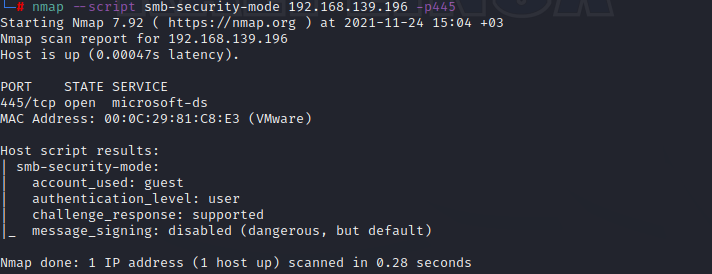


-SMB üzerinde kullanılan scriptleri görüntülemek için "locate \*smb\*.nse" komutunu kullanıyorum.



-"Smb-os-discovery" scriptini belirledikten sonra "445" portu üzerinde bir işlem gerçekleştiriyorum.

-Burada "Unix (Samba 3.0.20-Debian) olduğunu bana belirtti.



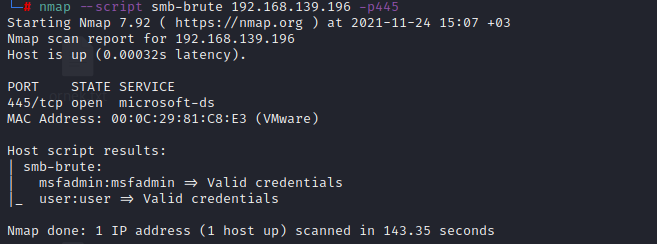
-Aynı işlemi "smb-security-mode" ile gerçekleştiriyorum.

-Burada giriş aptığı account hakkında bilgi sahibi oluyorum.

-Authentication level kısmına baktığımda burada user ve share olmak üzere 2 çeşittir.

-User-level ' Kullanıcı adı ve şifreyle giriş yapılır.

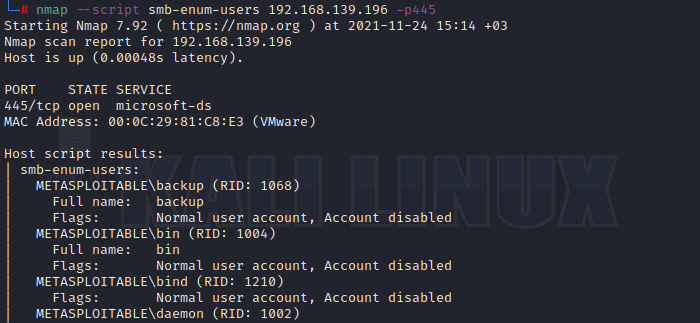
-Share-level 'Anonim olarak işlem yapılabilir.



-Aynı işlemi "smb-brute" ile gerçekleştiriyorum.

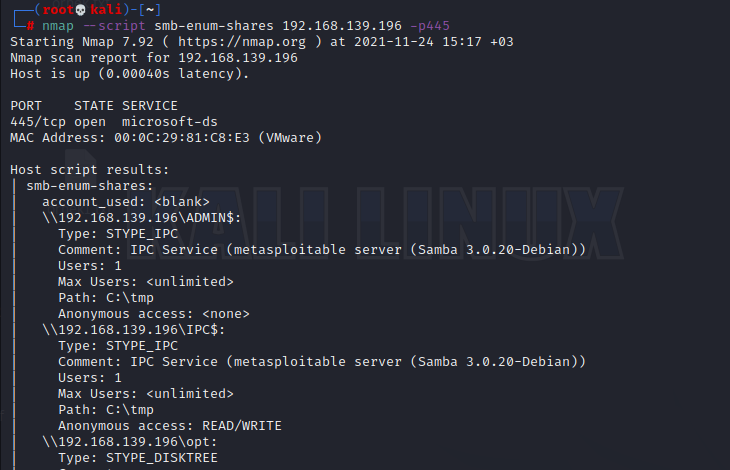
-Burada yaptığı Brute-force işlemi ile kullanıcı yakalamaya çalışıyorum.

-Eğer burada hata almış lsaydım "-d" parametresi ile verdiği hata hakkında bilgi sahibi olabilirdim.



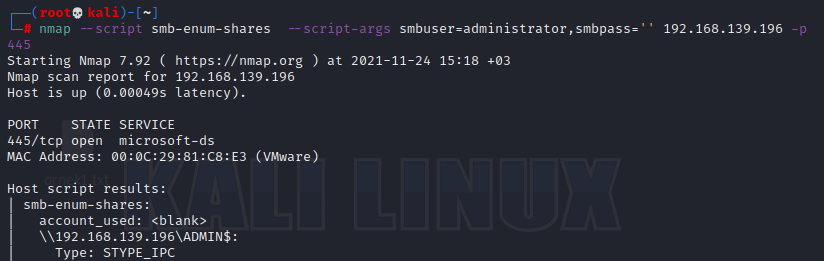
-Kullanıcılar hakkında tam detaylı bilgi sahibi olmak için "smb-enum-users"' scriptini kullanıyorum.

-Burada farklı kullanıcılar hakkında bana bilgi verdi.



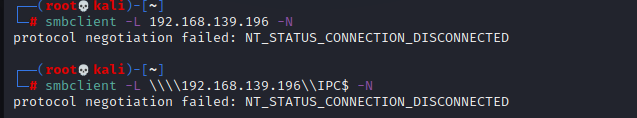
-"smb-enum-shares" ile yaptıkları paylaşımları görüntüleyebiliyorum.

-Burada yetkiler hakkında da bilgi sahibi olabiliriz.



-Aynı şekilde burada argüman belirtip kullanıcı adı ve şifre ile daha detaylı bilgi sahibi olmaya çalışabiliriz.

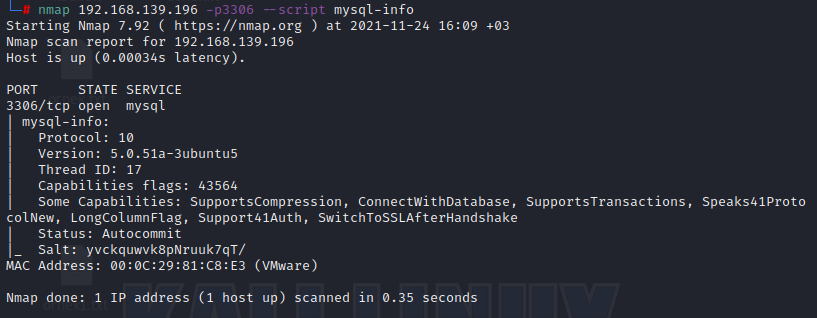
-Bunun ile izinsiz olarak erişim sağlayamadığımız servisler hakkında da bilgi sahibi olabiliriz.



-Burada eğer bağlantı protokolü aktif olsaydı sistem içerisine erişim sağlayabilirdik.

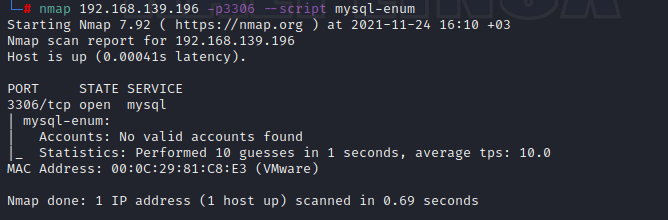
***NSE ile MYSQL Enumeration***

-3306 portunda bulunan "Mysql" için bilgi toplama işlemlerini gerçekleştireceğiz.



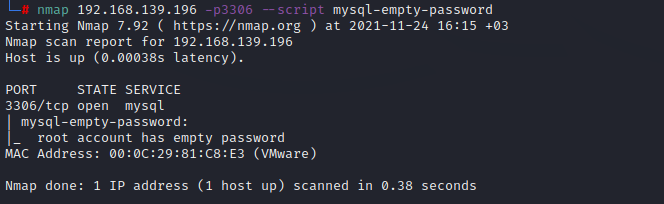
-Öncelikle "mysql-info" scriptini kullanarak bilgi almaya çalışacağım.

-Autocommit olduğu zaman üstünde yazma yaptığımızda diske de aynı şekilde işler.



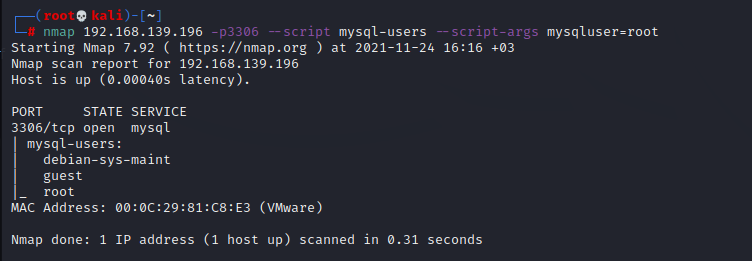
-"mysql-enum" scripti ile doğrulanmış hesaplar hakkında bilgi sahibi olabilirz.

-Burada eğer ":" görürsek sol taraf kullanıcı adı,sağ taraf ise şifredir.



-Bir önceki aramamda kullanıcı adı bulamamış olsa da boş şifre scripti ile bir deneme yapıyorum.

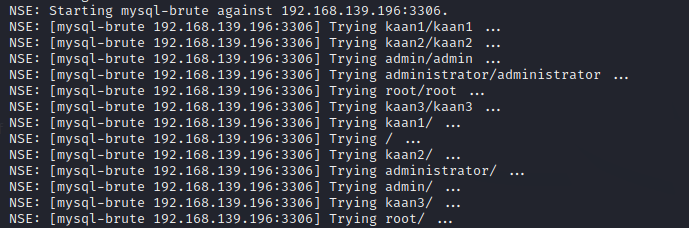
-Burada root kullanıcısına boş şifre ile giriş yaptığını görüntülüyorum.



-"mysql-users" scripti ie bir arama gerçekleştiriyorum.Burada kullanıcı adı olarak root kullanıcısını belirtiyorum.Şifre kısmı boş olduğu için şifre vermiyorum.



-Tarama modunda Brute işlemi gerçekleştirilmez.Burada IP'nin engellenmesi durumu gerçekleşebilir.



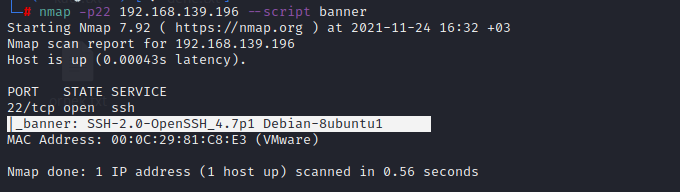
-Bu bruteforce işlemini sadece onun veritabanı ile değil kendi belirttiğim wordlist üzerinden de gerçekleştirebilirim.

-"nmap 192.168.139.196 -p3306 --script mysql-brute --script-args userdb='kadı.txt'" kullandığım komut budur.

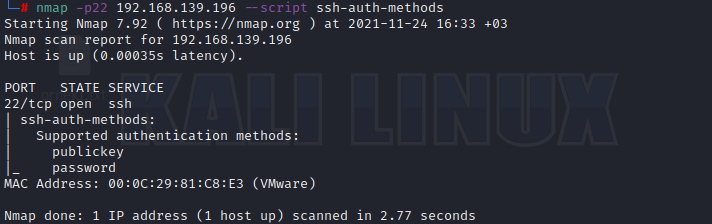
-Denemeleri bu şekilde görüntüleyebiliyorum.

***NSE ile SSH Enumeration***

-SSH servisi 22.Portta çalışmaktadır.



-Banner scripti ile SSH versiyonunu çıkarabildim.



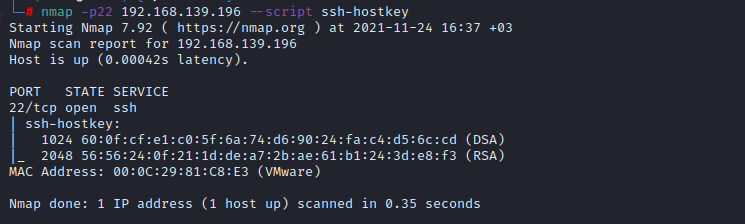
-"Auth" metodları hakkında bilgi sahibi olmak için "ssh-auth-methods" scriptini çalıştırıyorum.

-Password ile giriş yapılması çok güvenli değildir.MITM ve BruteForce işlemi gerçekleştirilebilir.



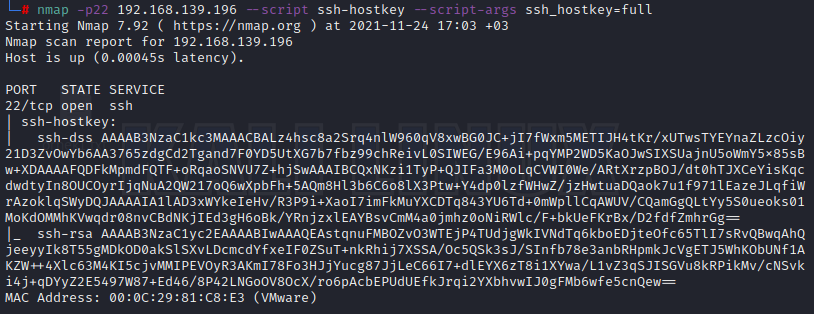
"ssh2-enum-algos" scripti ile SSH servisi üzerinde kullanılan algoritmalar hakkında bilgi sahibi olabiliriz.

-Burada MD5 olması güvensizdir.Eski bir teknoloji olduğunu gösterir.



-"ssh-hostkey" scripti ile giriş yapabileceğimiz keyler hakkında bilgi sahibi olabiliriz.

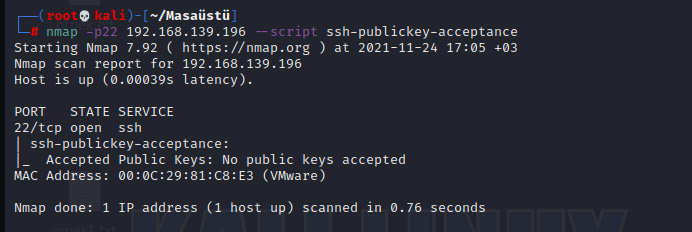
-Burada şifrelenmiş bir şekilde -RSA kısmını görebiliyoruz.



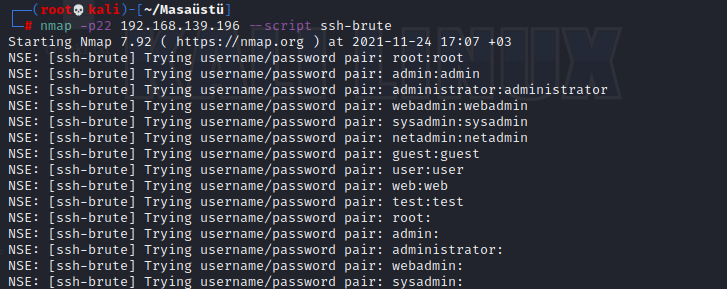
-"--script ssh-hostkey --script-args ssh\_hostkey=full" komutu ile şifrelenmemiş hallerini burada görebiliriz.



-Eğer hash değerlerinide görüntülemek istersek "--script ssh-hostkey --script-args ssh\_hostkey=all" komutu kullanılır.

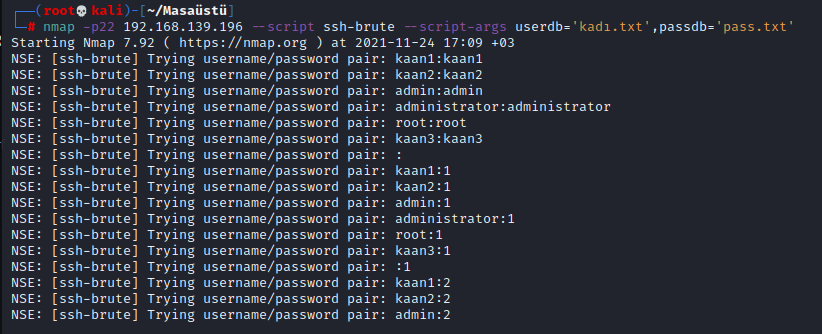


-Bulduğumuz public-keyleri "ssh-publickey-acceptance" komutu ile deneyebiliriz.



-"ssh-brute" scripti ile parola saldırı gerçekleştirebiliriz.

-Bu işlem sırasında nmap aracının içerisinde bulunan wordlistlerden yararlanılır.

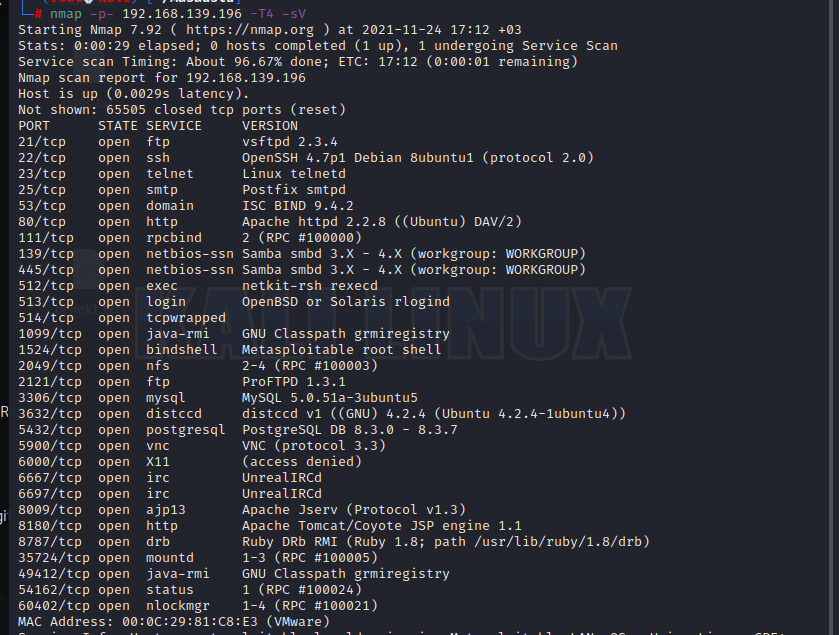


-Kendi sözlüğümü oluşturup buradan da bir saldırı gerçekleştirebilirim.

***NSE ile HTTP Enumeration***

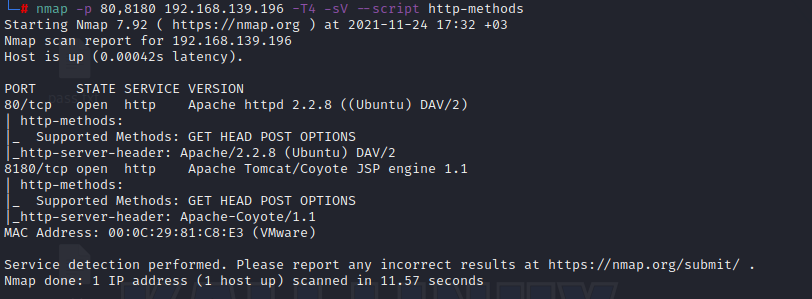
-HTTP server ile bağlantı kurmamızı sağlayan servistir.

-HTTP portu çok değişkenlik gösterdiği için tüm portlar üzerinde işlem gerçekleştiririm.



-Bunun için nmap üzerinden tüm portlar için bir tarama gerçekleştiriyorum.

-HTTP portlarının farklı portlar üzerinde çalıştığını gözlemledik.

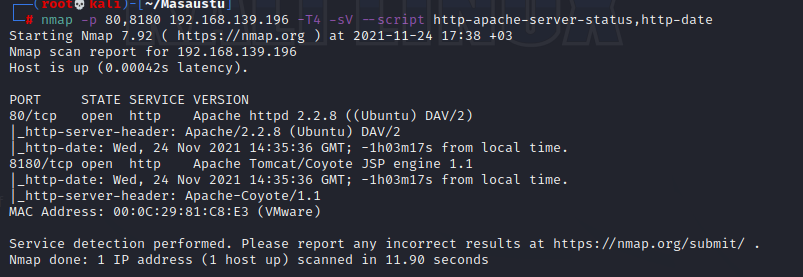


-Tarama işlemi gerçekleştirirken artık bu portlar üzerinden yapacağım.

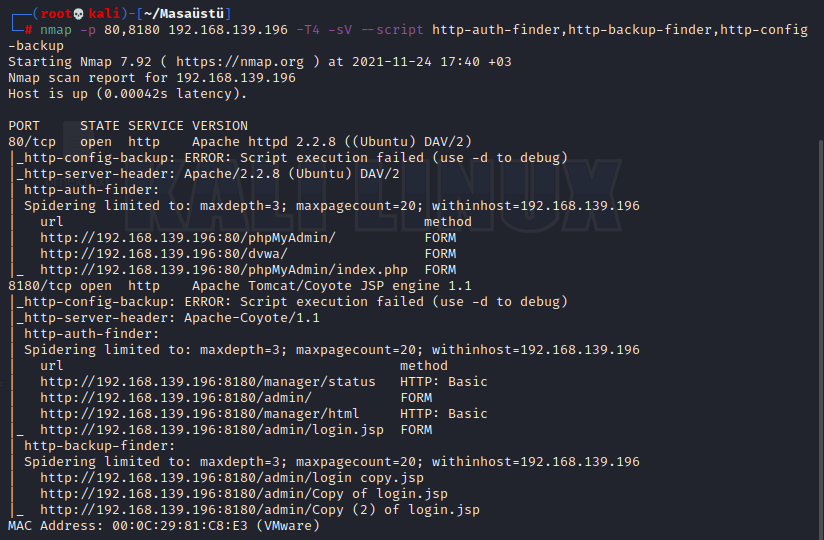
-HTTP servisinin 80 ve 8180 portunda olduğunu görüntülüyorum.

-Bu script sayesinde kullanılan methodların yanı sıra versiyon bilgilerini de görüntülüyorum.

-Bu methodlar içerisinde en çok kullanılan GET ve POST'tur.



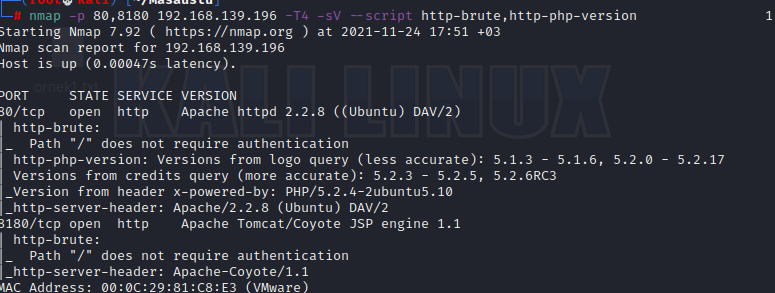
-Aynı anda birden fazla scripti'de kullanabiliriz.Server durumunu ve aynı anda kullandığı zaman dilimini çekerek bilgi sahibi olabilirim.



-Kullandığımız scriptler ile back-up dosyaları hakkında bilgi sahibi olmaya çalıştık.

-Burada "basic" kısımlı olan yerlerde bir giriş ekranı olduğunu görüntülüyorum.

-Ayrıca wordpress login ekranı gibi bilgileri de içermektedir.



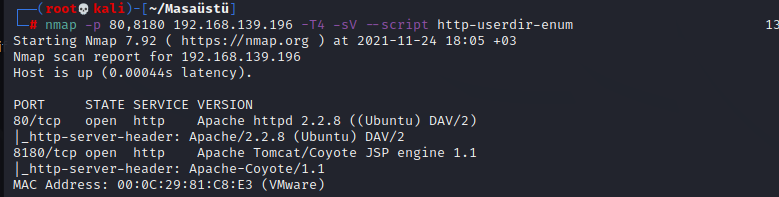
-"http-brute" ve "http-php-version" scriptleri ile bir işlem gerçekleştirdiğim de buradan bir bilgi edinemedim fakat başka pentest işlemlerinde bilgi edinebilirim.

-HSTS'in konfigure edilmediğini görüntüleyebilirim.Burada bir downgrade işlemi gerçekleştirip bilgi çıkarabilirim.

C:\Users\ogutk\AppData\Local\Microsoft\Windows\INetCache\Content.Word\6.png

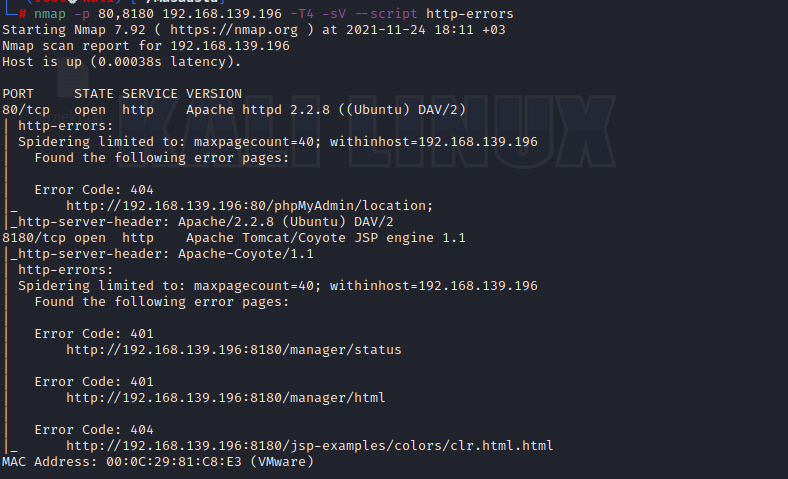
-Sunucunun DDOS saldırılarına karşı güvenilir olup olmadığını kontrol etmemizi sağlar.

-Burada devre dışı bırakabileceğimiz kısımları görmemizi sağlar.



-"http-userdir-enum" komutu ile kullanıcılar hakkında bilgi sahibi olaya çalışıyorum.

-Burada şuan da bilgi edinemedim fakat burada bir kullanıcı adı ve şifre elde edebilirdim.

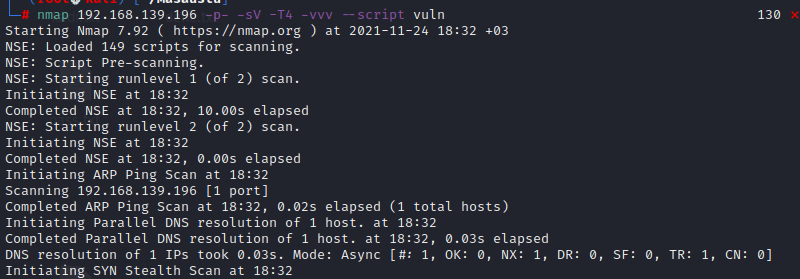


-Ayrıca "http-errors" scriptini çalıştırıp.

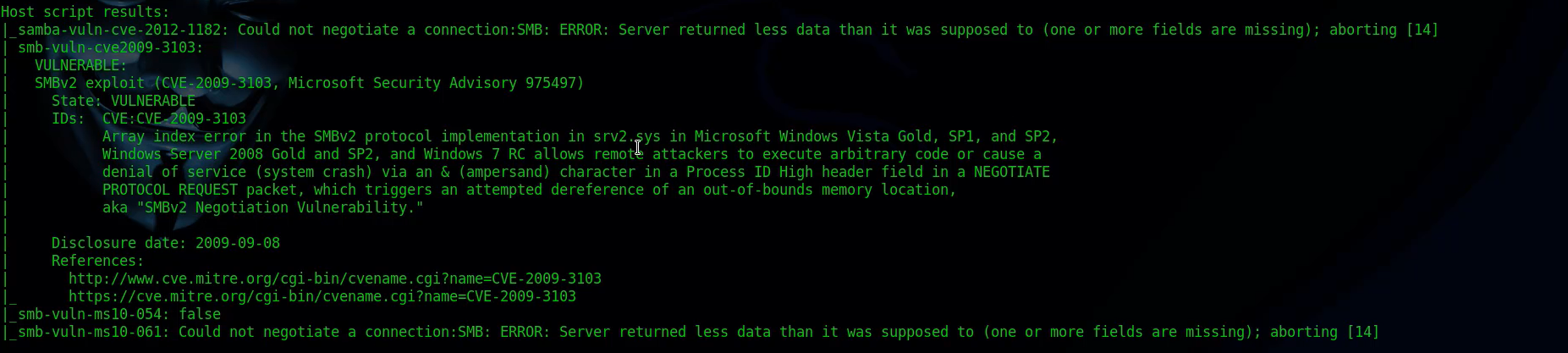
-Hata verdiği yerlerden bir bilgi çekmeye çalışabiliriz.

***NSE ile Güvenlik Açığı ve CVE Tespiti***

-CVE numaraları bize exploit edilip edilemeyeceği hakkında bilgi sahibi olmamızı sağlar.



-Açık bulunmuş halini sizler ile paylaşmak isterim.



Bir açık bulduğunda bu görselde olduğu gibi tarafımıza aktarım gerçekleştirir.

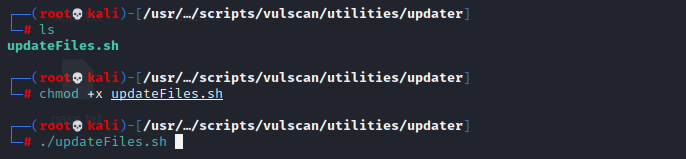
***Nmap Vulscan ile Güvenlik açığı ve CVE Tespiti***

-CVE tespit işlemini bu sefer Vulscan aracı ile gerçekleştireceğim.



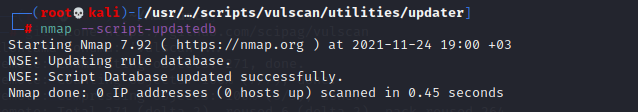
-Bu aracı github üzerinde bulunan "https://github.com/scipag/vulscan" bağlantı üzerinden indiriyoruz.

-Burada dikkat etmemiz gereken "/usr/share/nmap/scripts" içerisine bu dosyayı indirmemiz.

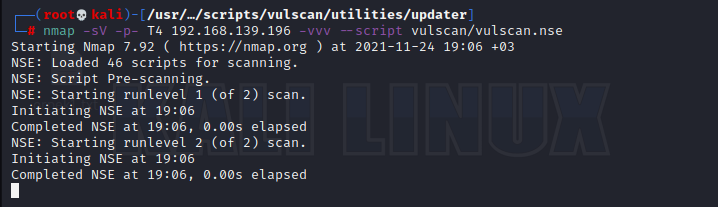


-İndirme işleminin ardından "updater" klasörüne geçiş yapıyorum ve burada chmod +x ile çalıştırma yetkisi verdiğim bu aracı çalıştırıyorum.

-Veritabanını da güncelledikten sonra çalışmaya hazır biçimdedir.



-Nmap üzerinde işlem yapmadan önce onunda veritabanını güncellememiz gerekmektedir.



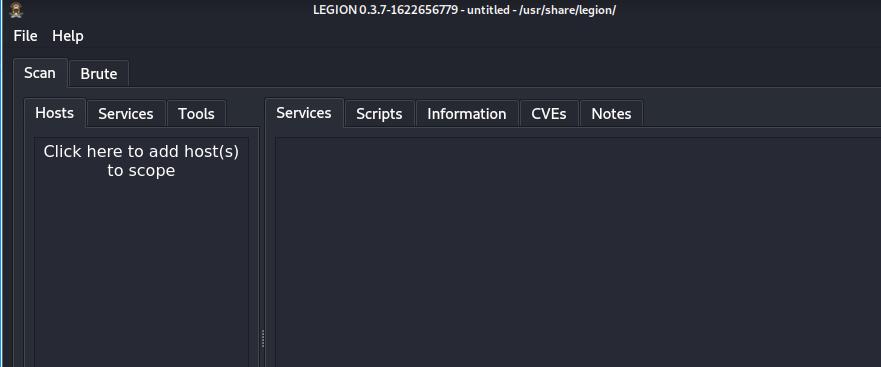
-Bir önceki başlık üzerinde yaptığımız işlemi farklı bir araç ile de gerçekleştirdik.

-Burada da açık bulduğunda bir önceki örneğe benzer bir çıktı vereceği için onu göstermedim.

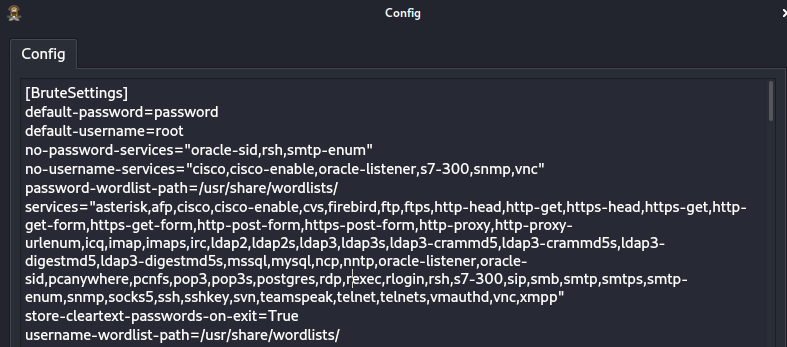
***LEGION(Nmap GUI) ile Tümleşik Arama***

Legion,nmap üzerinde yapılan işlemleri bize görsel olarak sunan bir araçtır.

-Bu araç Linux üzerinde kurulu olarak gelmektedir.

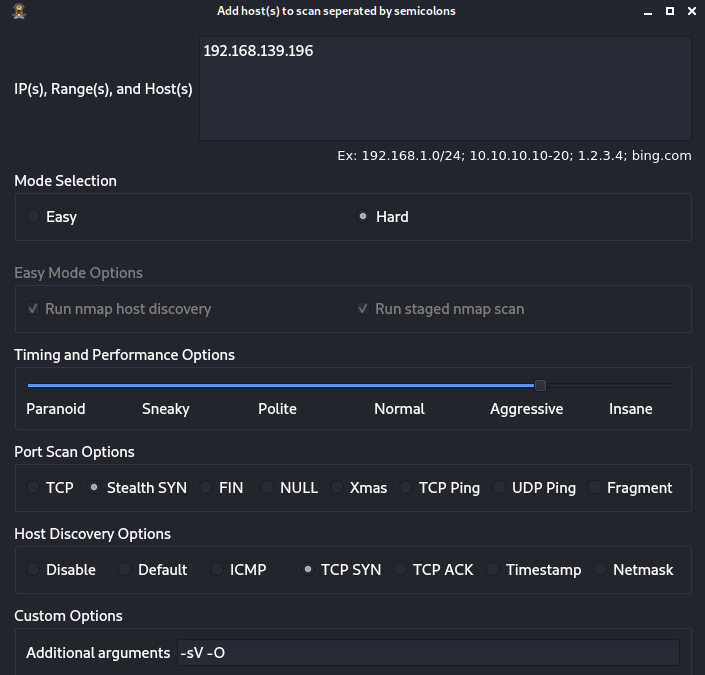


-Aracı çalıştırdığımda görsel olarak görüntüsü bu şekildedir.

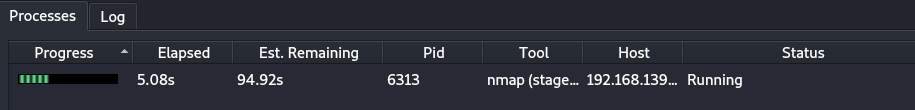


-Araç barından "Help>Config" kısmına girdiğimizde ayarlar hakkında bilgi sahibi olabiliriz.

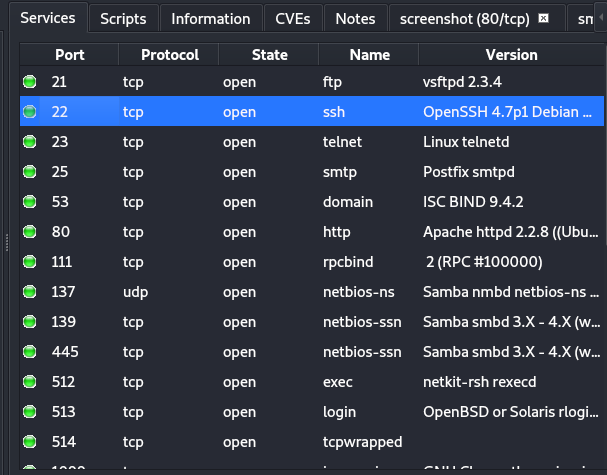
-Default ayarları gayet yeterli olduğu için değiştirmemize gerek yoktur.



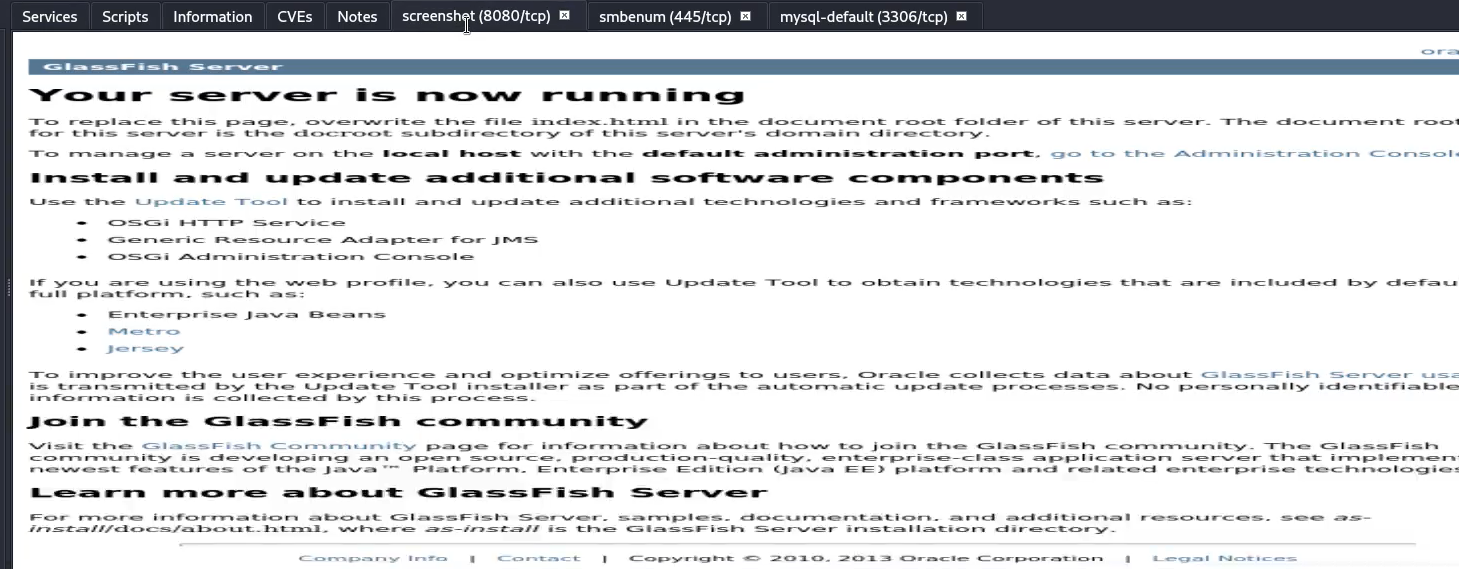
-Bir scope aralığı belirtirsek burada istediğimiz ayar üzerinden işlemlerimizi başlatabiliriz.



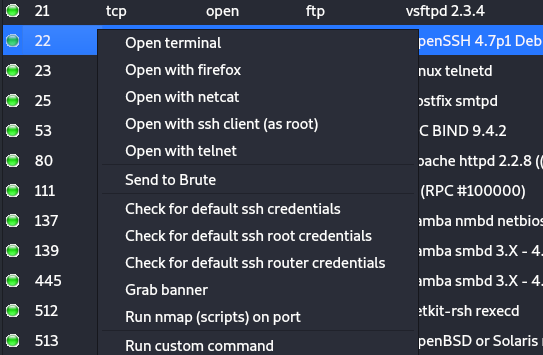
-İşlemi başlattığımızda alt kısımdan takibini yapabiliriz.



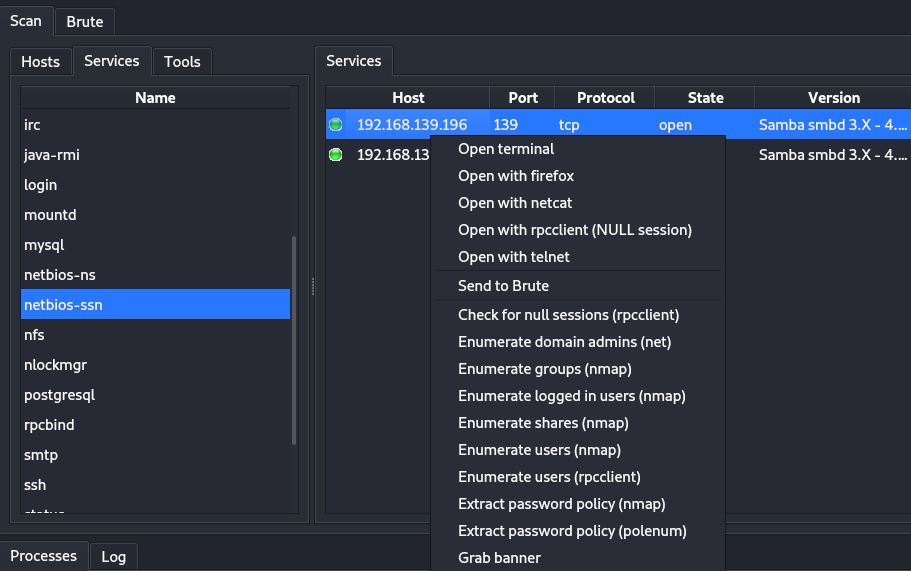
-Ayrıca bulduğu sonuçları ekran üzerinden takip edebilirim.



-Bulduğu sonuçlar haricinde Screenshot sekmesinden aldığı ekran görüntülerini görüntüleyebilirim.

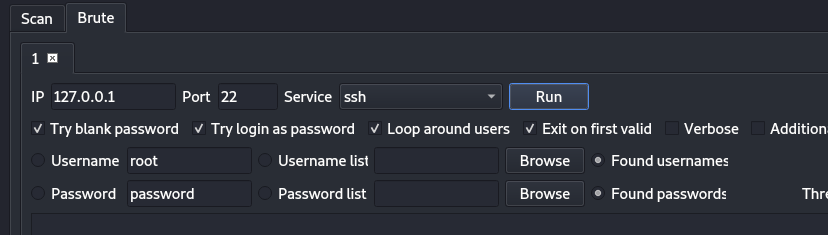


-Ayrıca bulduğu servis üzerinde sağ tıkladığımda yapabileceğim diğer işlemleri görüntüleyebiliyorum.



-Sol taraftan servis bölümünde bulduğu servisleri ve gerekli bilgileri tarafıma aktarıyor.

-Burada işlem yapabileceğim -enumerate'leri görüntüleyebiliyorum.

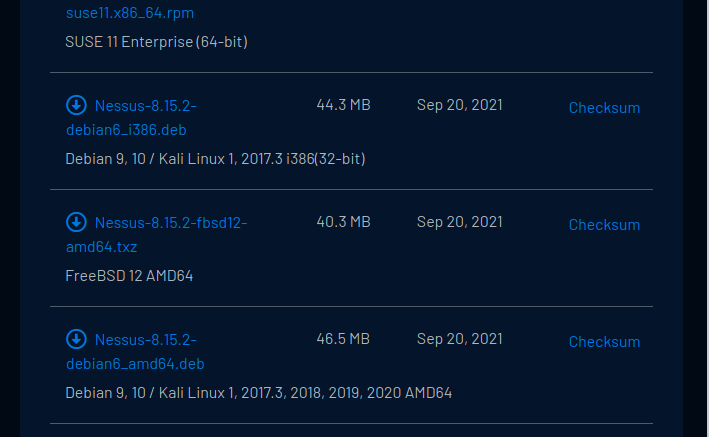


-Ayrıca "Brute" kısmına geçiş yaptığımda verdiğim wordlistler aracılığıyla bir Bruteforce işlemi gerçekleştirilebilir.

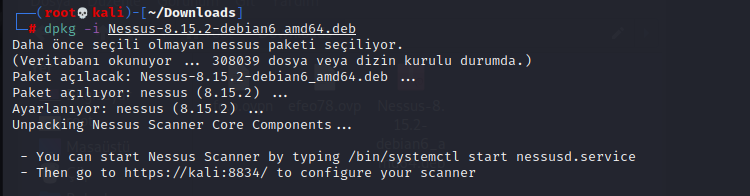
***Nessus ile Güvenlik Açığı Tespiti***

-Nessus aracı da pentest sırasında kullanacağımz araçlardan biridir.

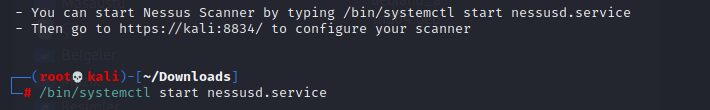
-Bu "tenable" şirketine bağlı aracı tarayıcı üzerinden indirebiliriz.



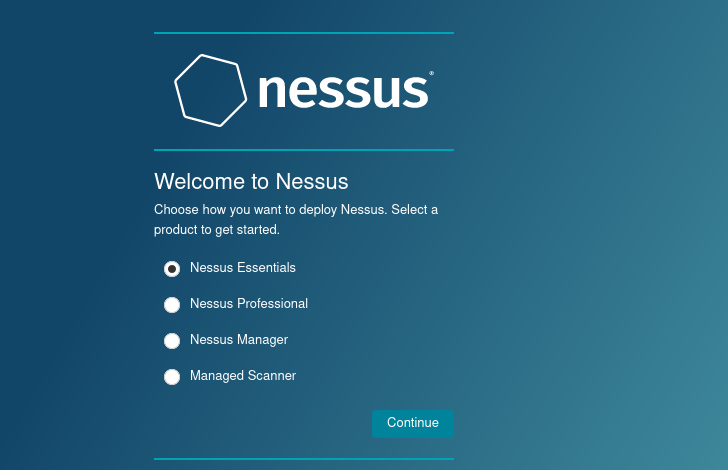
-Kendi sanalıma uygun olan versiyonunu indiriyorum.



-".deb" uzantılı aracı indiriyorum ve ardından "dpkg" kütüphanesi ile kurulum gerçekleştiriyorum.



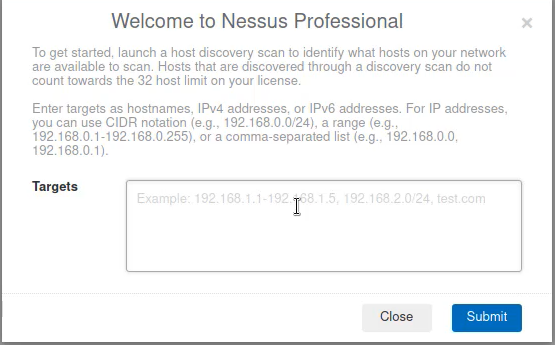
-Kurulumun ardından söylediği gibi service'i başlatıyorum.



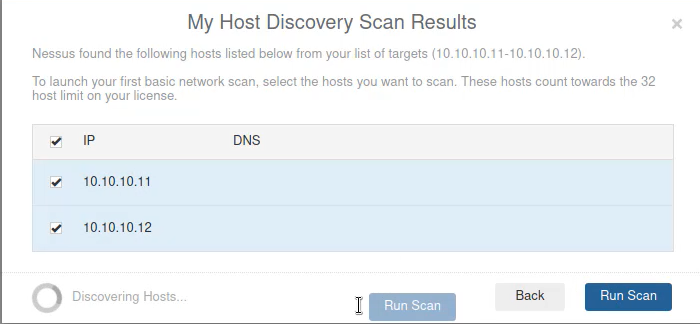
-Sonrasında tarayıcı üzerine geçiş yapıyorum ve verdiği bağlantı üzerinden nessus aracını başlatıyorum.

-Burada free versiyon ile işlemlerime devam ediyorum.

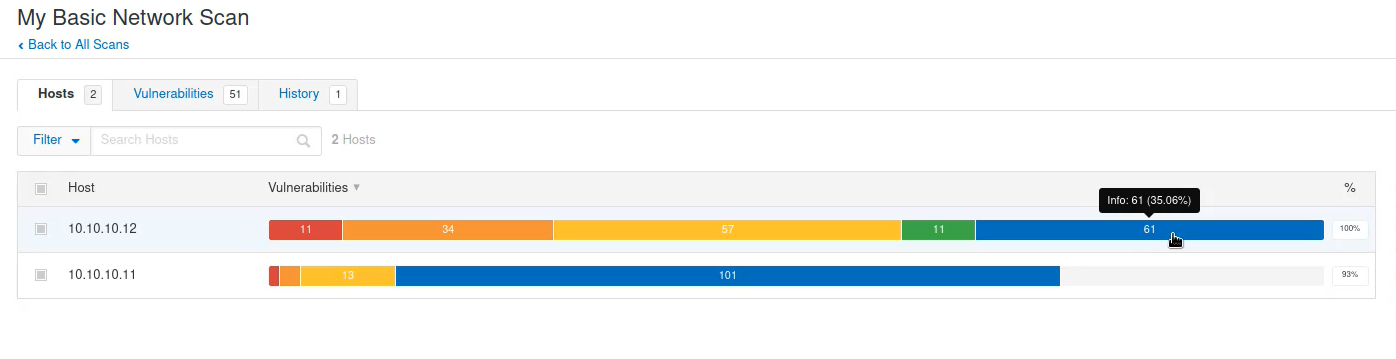
-Vermiş olduğum mail adresi üzerinden gelen aktivasyon kodu ile üyeliğimi tamamlayıp aracı açıyorum.



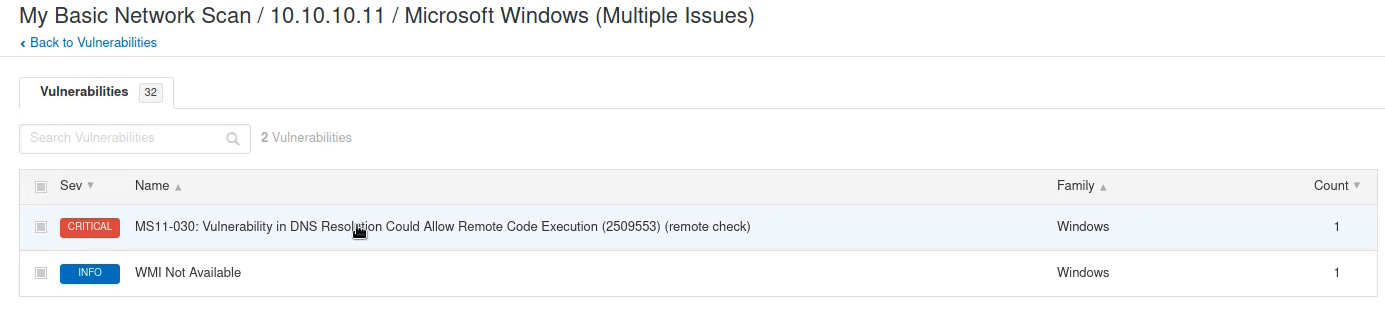
-Araç çalıştığında ilk önce bizden bir adres istemektedir.



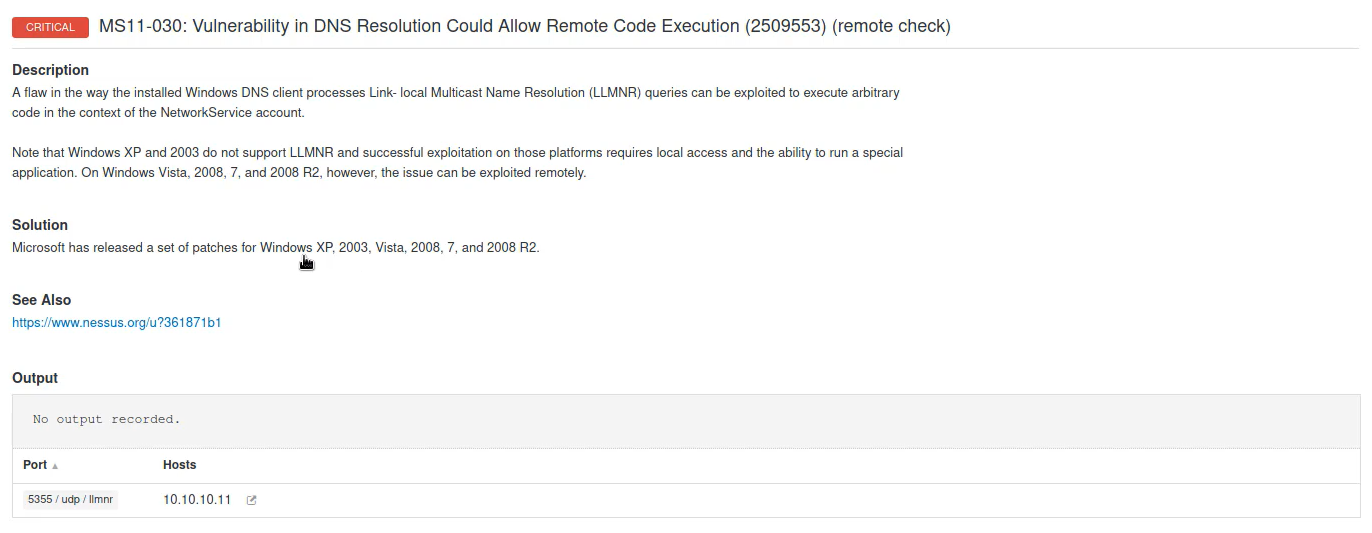
-Verdiğim IP adreslerini başarılı bir şekilde buldu burada taramalarına aynı şekilde devam etmektedir.



-Verdiğim IP adresleri üzerinde yapmış olduğu tarama sonuçlarını tarafıma bu şekilde aktarmaktadır.



-Verdiği açıklardan bir tanesine girdiğim de sürüm kaynaklı bir açık bulunduğunu tarafıma aktardı.



-Açığı tam olarak görüntülediğim de burada açığı kapatmak için yapılabilecek işlemlere kadar göstermektedir.

-Aracın kullanımı bu şekildedir. Kesinlikle Penetration testlerinde kullanılmalıdır.