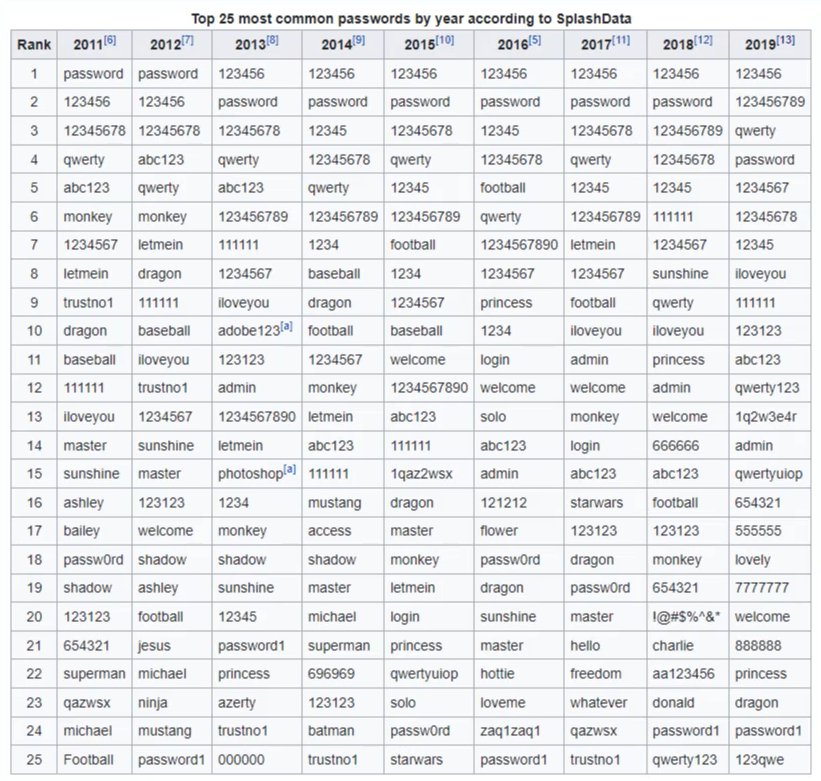
|  |
| --- |
| ***BruteForce Saldırıları*** |
| Kaan Efe Öğüt  *ADLİ BİLİŞİM MÜHENDİSLİĞİ* |
| -Pentest aşamalarında kullanılan Bruteforce Saldırılarıyla ilgili bilgi vereceğim. |

**13.12.2021**

***Dictionary Attack ve Wordlistler***

-Sözlük saldırıları metinsel girdileri hedefler,bunlar sadece şifre için değil veritabanı adları,dizin adları gibi yerlerde de kullanılır.

-Wordlistler programlar aracılığıyla oluşturulmuştur.



- Güncel olarak bilinen çoğu şifre bu kadar basit kullanılmaktadır.

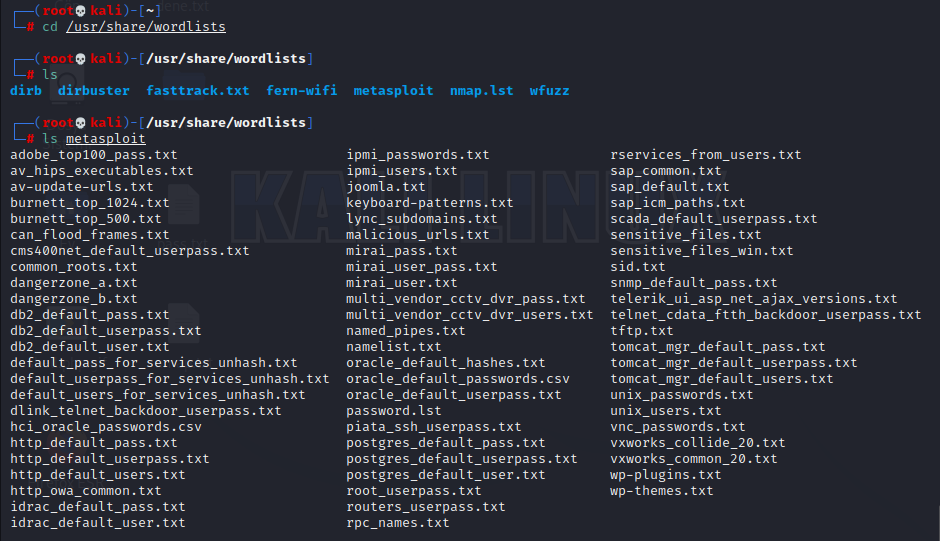


- Örnek olarak göstermek istediğim bir kaynak "https://github.com/xajkep/wordlists" bağlantısı üzerinde bulunmaktadır.

-Tarayıcı üzerinde wordlist araması yaptığımda çok daha fazlasını elde edebilirim.

***Lokal Wordlistler***

-Wordlistlere sadece tarayıcı üzerinden değil,linux üzerinde hazır olarak bulunan ve çoğu CTF'de kullanım gösterdiğimiz wordlistler de bulunmaktadır.



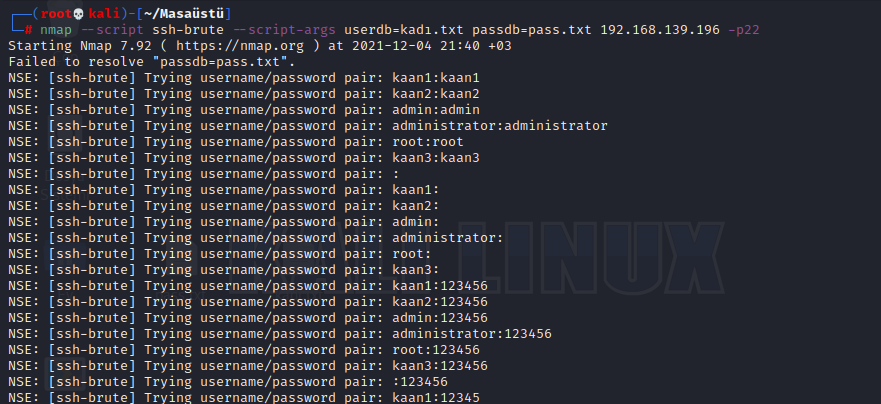
- "/usr/share/wordlists" dizininde çeşitli araçlar için kullanabileceğimiz wordlistler mevcuttur.

-------------------------------------------------------------------

Nmap ile Dictionary Attack(SSH)

-Linux üzerinde kurulu olarak bulunan Nmap aracı ile Dictionary Attack gerçekleştireceğiz.

-Bu işlemi Metasploitable-2 üzerinde bulunan SSH servisinde gerçekleştireceğim.



- Nmap üzerinde daha önce bu işlemi gerçekleştirdiğimiz için çok detaylı göstermeyeceğim.

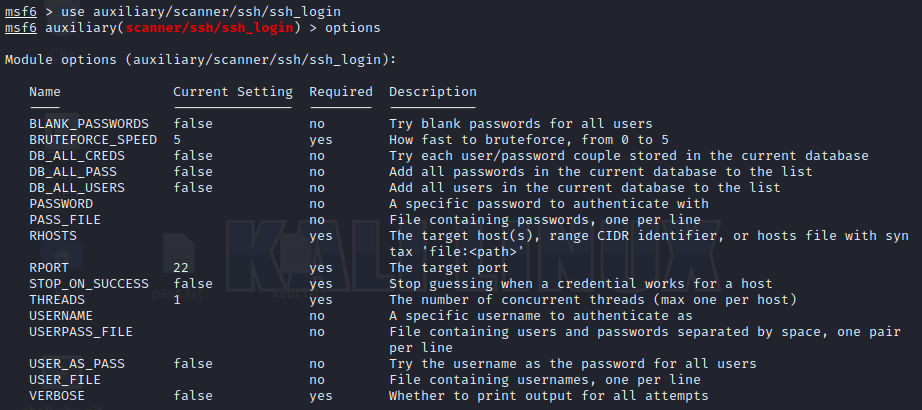
-Burada Kullanıcı adı ve şifre tutan wordlistler belirtiyorum ve ardından işlemi başlatıyorum.

İşlemin akışını bu şekilde görüntülüyebiliriz.

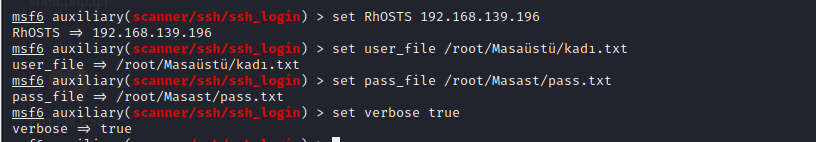
***Metasploit ile Dictionary Attack(SSH)***

-SSH servisi üzerine gerçekleştireceğim Dictionary Attack için Metasploit aracını kullanacağım.

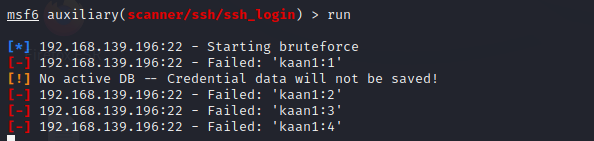
-Msfconsole komutu ile aracı başlatıyorum.



- "set RHOSTS" komutu ile saldırı gerçekleştireceğim IP adresini tanımlıyorum.Eğer birden fazla tanımlamak istersek bir ".txt" uzantılı dosyaya yazıp "set rhost file:" komutu ile tanımlayabiliriz.



--Burada ekstra olarak kullanıcı adı ve şifreleri set ediyorum ve verbose'u aktif edip yapılan işlemleri görüntülüyorum.

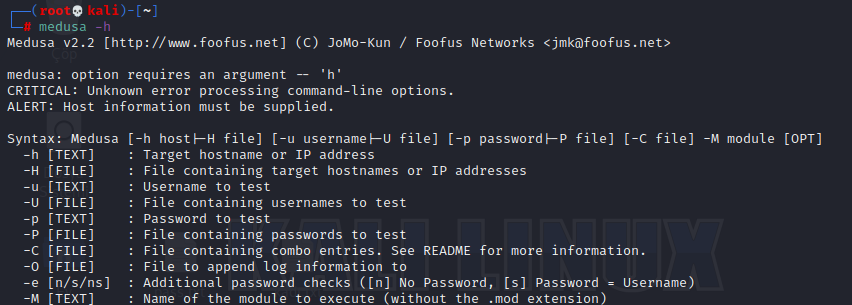


- İşlemi başlattığımda başarılı bir şekilde Bruteforce işlemi gerçekleştirdiğini görüntülüyorum.

***Medusa ile Dictionary Attack(SSH)***

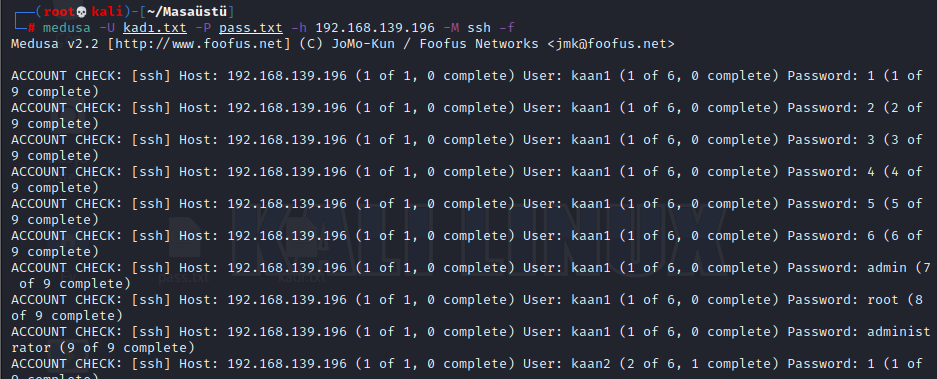
-Bu işlemleri hızlıca gerçekleştiren araçlardan bir olan medusa ile devam ediyoruz.

-Medusa linux sürümlerinde kurulu olarak gelmektedir.



-"medusa -h" komutu ile kullanımı hakkında bilgi sahibi olabilirim.

-"-u,-p,-h" harfleri ile tek index içeren saldırıları gerçekleştirebiliriz.Eğer birden fazla index var ise "-U,-P,-H" kullanılır.



-Örnek üzerinde göstermek gerekir ise;

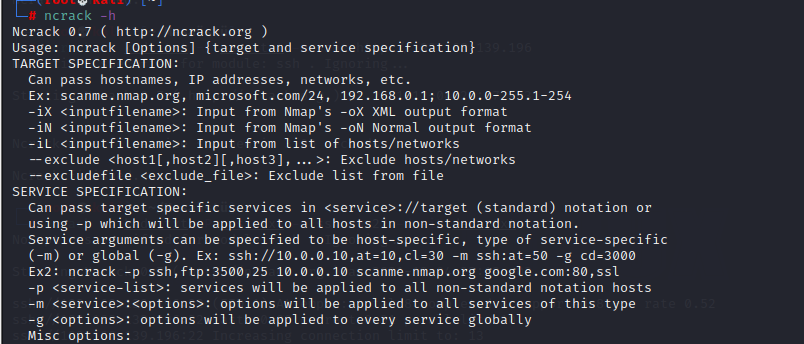
-"-M" ile saldırı gerçekleştireceğim servisi belirtmem gerekmektedir.

-"-n" ile farklı bir port üzerinde bulunuyor ise değiştirebilirim.

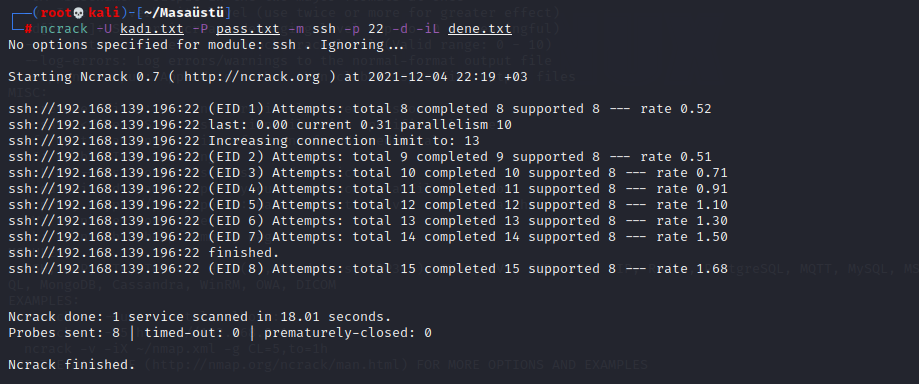
-Ayrıca "-f" komutu ile doğru kombinasyonu bulduğunda durur.

***Ncrack ile Dictionary Attack(SSH)***

-Bu işlemi en hızlı gerçekleştiren araçlardan biri olan ncrack ile işlemlerime devam ediyorum.



-ncrack -h komutu ile kullanımı hakkında bilgi sahibi olabilirim.



-Kullanım içeriği medusa ile benzer olduğu için açıklama yapmadan direk örnek olarak gösteriyorum.

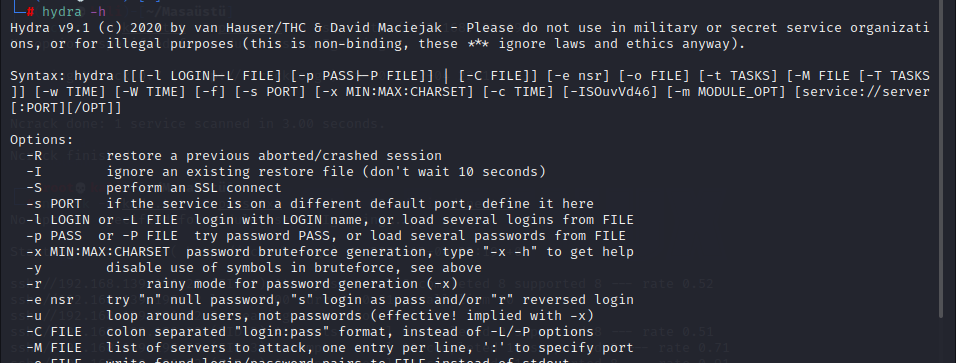
-Fark olarak "-iL" komutu ile hostların bulunduğu bir .txt dosyası belirtebiliriz.

-"-d" komutu ile de aldığımız hata mesajlarını görüntüleyebiliriz.

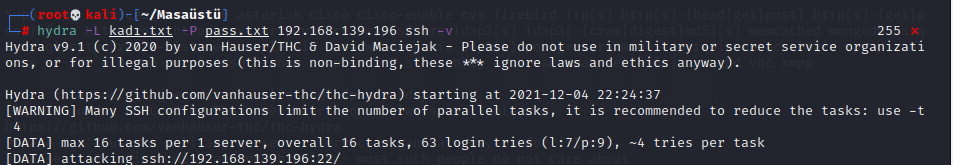
***Hydra ile Dictionary Attack(SSH)***

-Pentest aşamalarında en çok kullanılan hızlı araçlardan biridir.

-Birden fazla host üzerinde çok fazla etkili değildir.



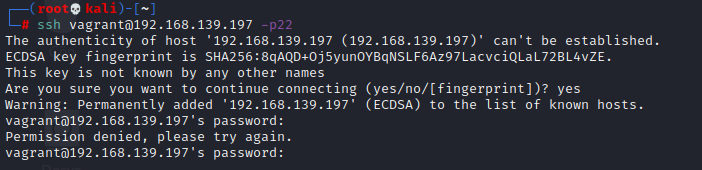
-"hydra -h" komutu ile kullanımı hakkında bilgi sahibi olabiliriz.



-Kullanımını bir örnek ile göstermek istiyorum.

***SSH Komutları***

-Bundan sonra çokça karşılaşacağımız SSH ile ilgili komutları göstermek isterim.



-Öncelikle SSH bağlantısını gerçekleştiriyorum.

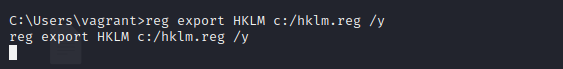


-"pwd" komutu ile bulunduğumuz dizini görebilirken;

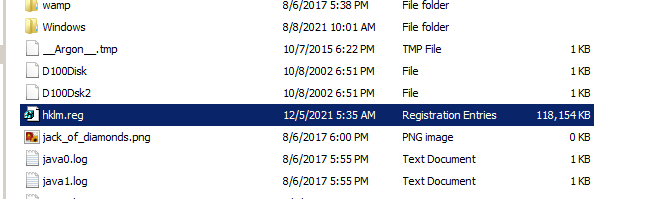
-"ls" komutu ile listeleme işlemlerini gerçekleştirebiliriz.



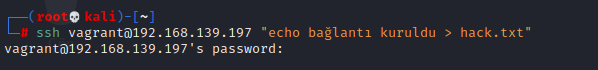
-"cmd" komutu ile işletim sistemini öğrenebiliriz.



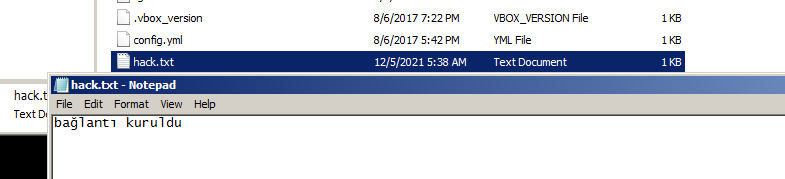
-Registry'deki HKEY\_LOCAL\_MACHINE'i C: altına hklm.reg dosyası adıyla kayıt eder.



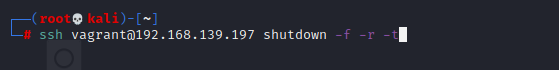
-Yapmış olduğu backup işlemini sunucum üzerinden de teyit ediyorum.



-SSH bağlantısı ile bir dosya üzerine yazma işlemi de gerçekleştirebilirim.



-Sunucu üzerinde kontrol ettiğim de dosyaya yazma işlemini gerçekleştirdiğimi görüntüleyebilirim.

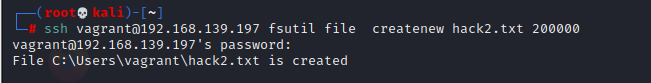


-Bu işlemlerin haricinde sunucuyu kapatmaya zorlayabiliriz.

-f(force) = Zorla.

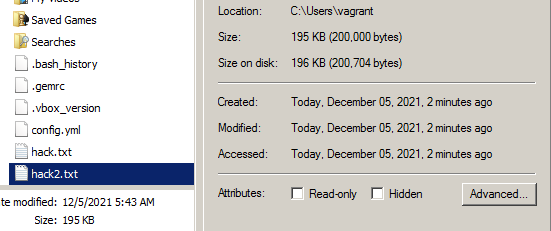
-r(restart) = Yeniden başlat.

-t(timeout) = 5 Saniye sonra.

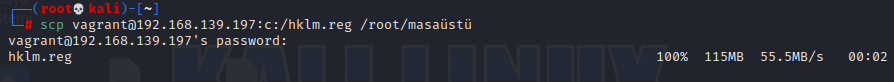


-Boyutunu kendimizin belirlediği bir dosya da yaratabiliriz.

-"fsutil file createnew hack2.txt 20000"



-Sunucu üzerinden kontrol sağladığım da başarılı bir şekilde işlem gerçekleştiğini görüntülüyorum.

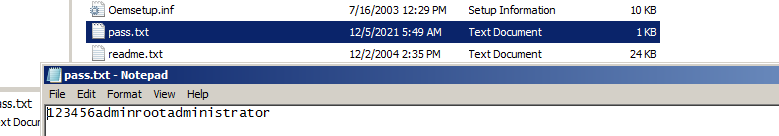


-Sunucu üzerinden dosya çekmek için "scp" komutu kullanılır.

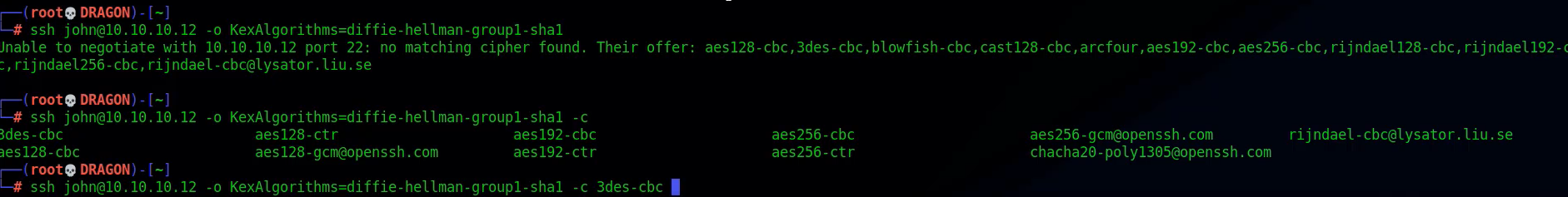
-Bu düzende istediğimiz dosyayı çekebiliriz.



-Linux üzerinden Sunucu üzerine de bu düzende dosya aktarımı yapabiliriz.



-Sunucu üzerinde teyit ettiğimde başarılı bir şekilde aktarım yaptığımı görüntülüyorum.

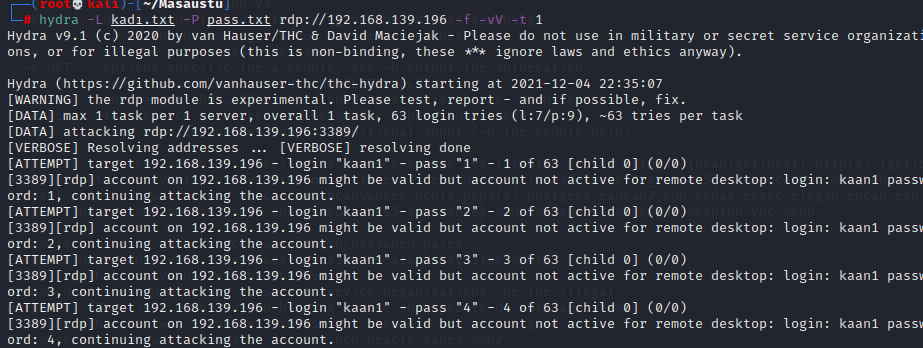


-Linux bir sunucu üzerinden encryption'lı giriş yapmak istersek tam olarak düzen bu şekildedir.

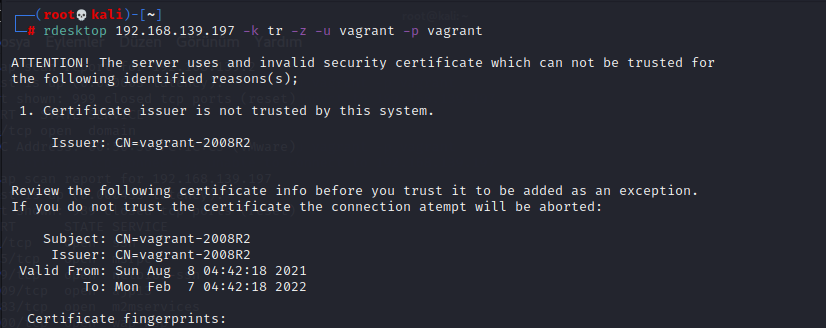
***RDP’ye Dictionary Attack ve RDesktop***

-RDP servisine bir Dictionary Attack gerçekleştireceğim.

-RDP "Remote Desktop Connection" Windows çalıştıran bir bilgisayara, Uzak Masaüstü Bağlantısı kullanarak, aynı ağa veya İnternet'e bağlı olan ve Windows çalıştıran başka bir bilgisayardan erişim sağlayabiliriz.



Hydra aracı ile başarılı bir şekilde şifresini kırabildik.



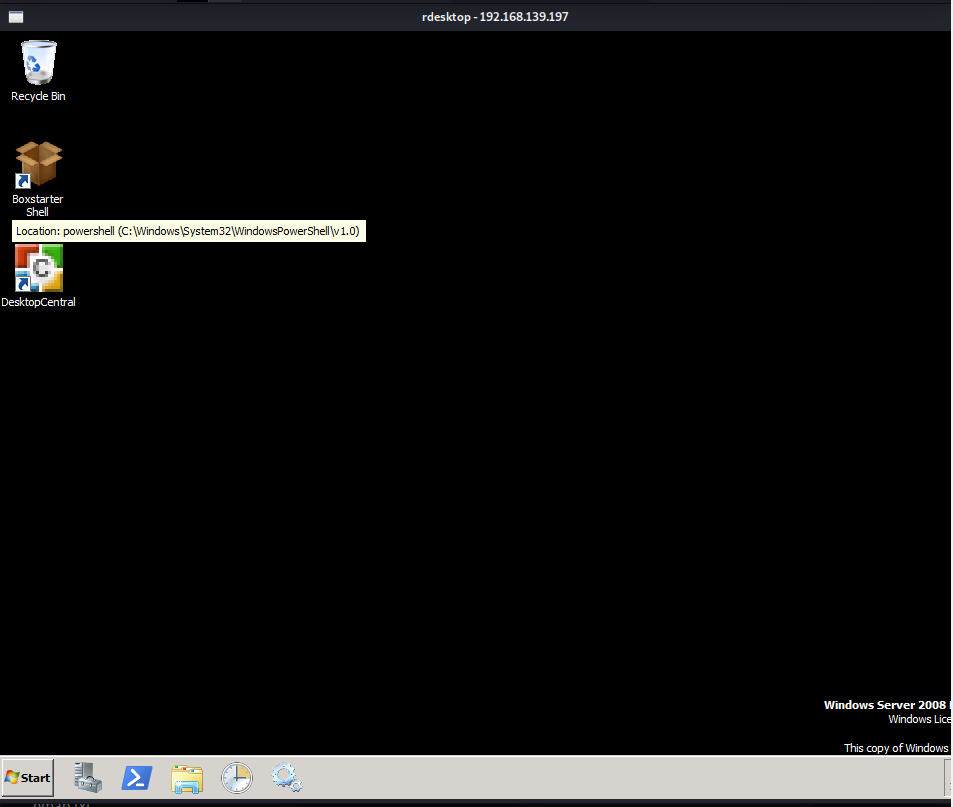
-Linux üzerinde kurulu olarak gelen "rdesktop" aracını kullanarak uzak bağlantı kurabiliriz.

-"-k" komutu ile klavye dilini belirtiyorum.

-"-z" ile işlemlerin daha hızlı gerçekleşmesini sağlıyorum.

-"-f" komutu ile tam ekran yapabiliyorum.

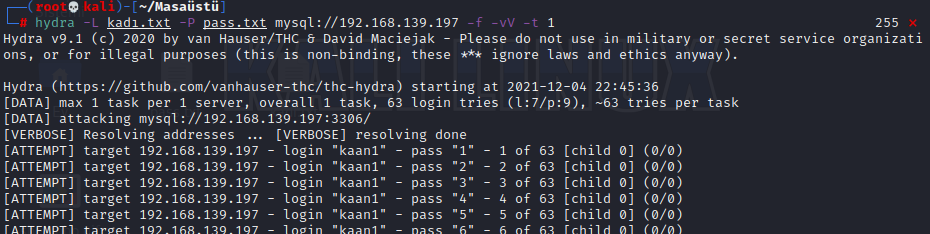
-"-u,-p" parametreleri ile kullanıcı adı ve şifreyi belirtiyorum.



-Başarılı bir şekilde uzak bağlantı kurabildim.

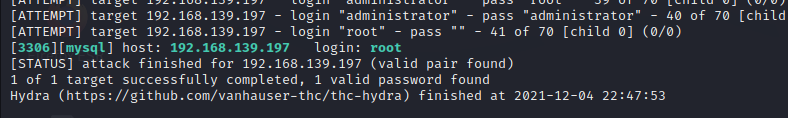
***MySQL’e Dictionary Attack ve Null Password***

-Aynı işlemi Hydra aracı ile Mysql servisine saldırı gerçekleştiriyorum.



-Hydra aracı ile bir önceki yaptığımız saldırılara benzer şekilde bir saldırı gerçekleştiriyorum.

-Burada şifresinin boş olmasından dolayı bulamadı.



-Komut satırının sonuna eklediğim "-e n" parametresi il artık boş şifreyi de deneyecek.

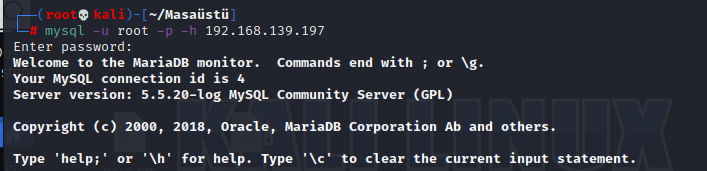
-Burada başarılı bir şekilde şifreyi bulabildim.

---------------------------------------------------------------------------------------------------------------

MySQL Komutları,Kullanımı ve DBDump

-Pentest sırasında çokca karşımıza çıkacak olan SQL veritabanlarıdır.

-Mysql veritabanının komutları hakkında biraz bilgi vermek istiyorum.



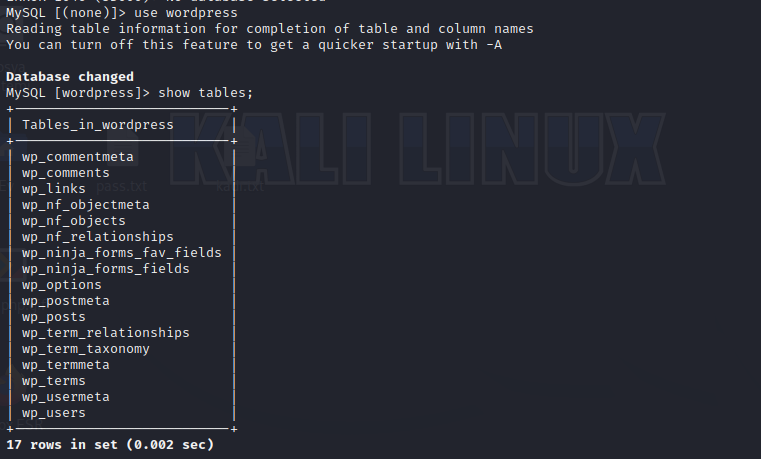
-Öncelike Mysql üzerinden bağlantı alıyorum.

-Burada passwd kısmını boş bırakıyorum.

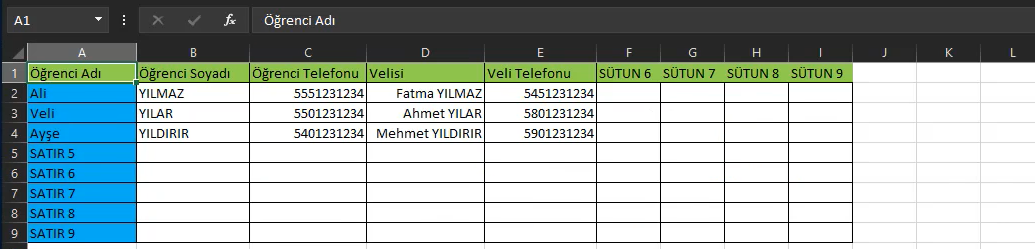
-Eğer port adresini belirtmek istersek "-P" kullanabiliriz.



-"show databases;" komutu ile sistemde yer alan veritabanlarını görüntüleyebiliriz.



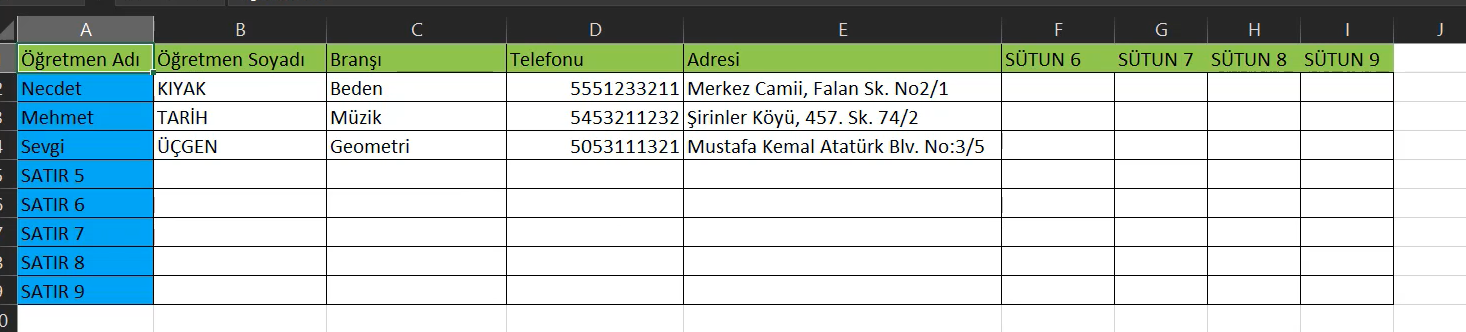
-Seçtiğimiz veritabanı üzerinde bulunan tabloları "show tables;" komutu ile görüntüleyebiliriz.



-Veritabanı yapısını basit bir şekilde göstermek gerekirse;

-Bunu wordpress veritabanı olarak düşünebilirim.

-Burada gördüğümüz 1 tablodur.Burada birden fazla tablo olabilir.

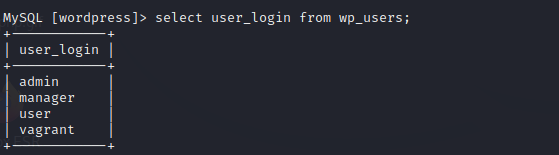


-Aynı sunucu içerisinde farklı bir veritabanına geçiş yapıyorum.

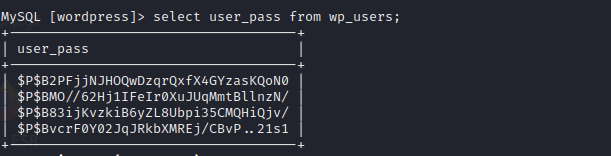
-Burada da aynı şekilde birden fazla tablo bulunabilir.



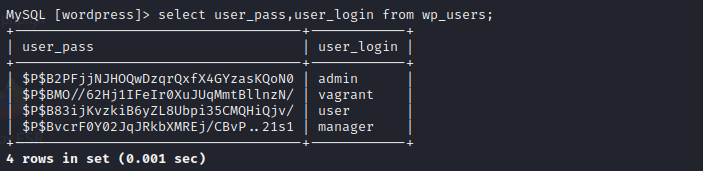
-"desc wp\_users;" komutu ile tablonun yapısı hakkında bilgi sahibi olabilirim.



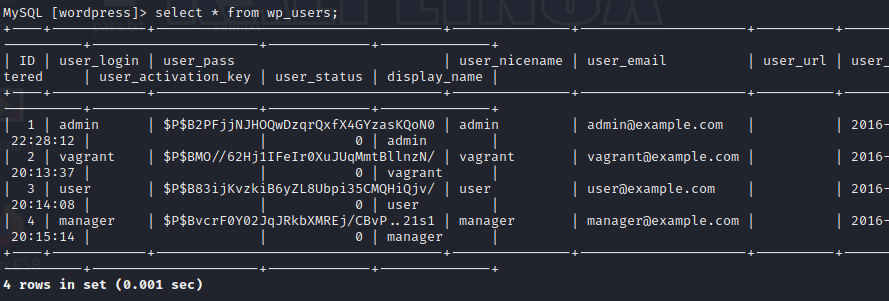
-"user\_login" sutununun içinde ki bilgileri çekiyorum.



-"user\_pass" sutununun içinde ki bilgileri çekiyorum.



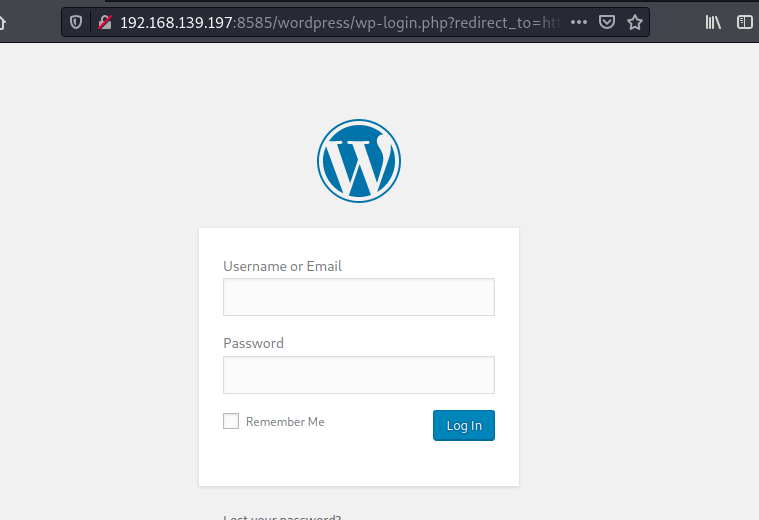
-İstediğim iki sutunu da bu şekilde getirebilirim.



-Tüm bilgileri çekmek istersem "select \* from wp\_users" komutunu kullanabilirim.

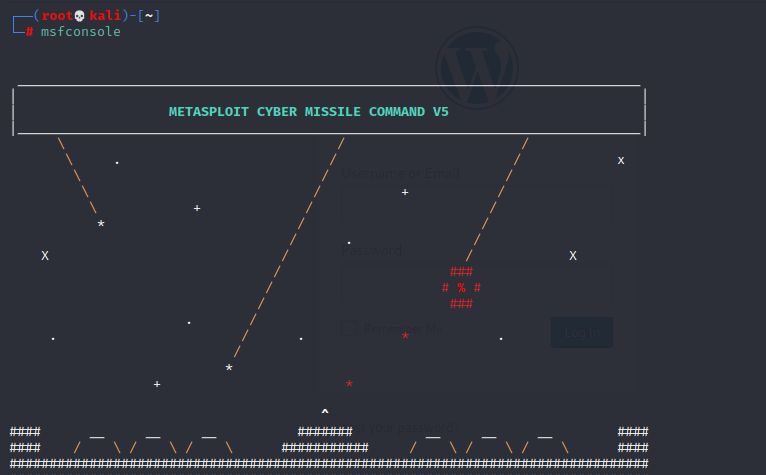
***Wordpress Login Attack***

-Çok fazla kullanılan Wordpress site arayüzüne Bruteforce ile bir saldırı gerçekleştirip login almaya çalışacağız.



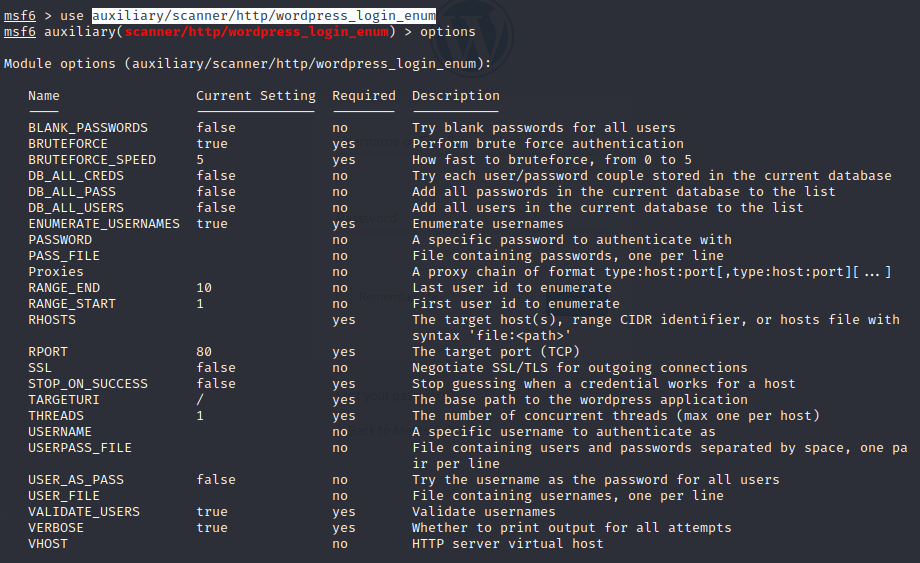
-Daha önce yaptığım nmap taramalarında "8585" portunu kullandığını biliyorum.

-Tarayıcı üzerinde bunu görüntülüyorum.



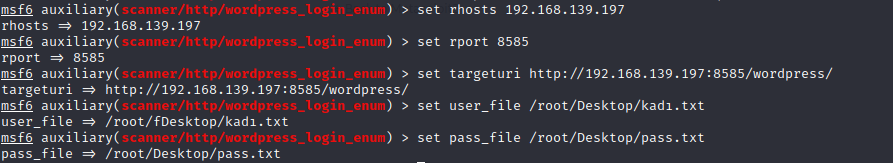
-Burada saldırı için metasploit içerisinde bulunan bir auiliary kullanacağım.

-Bu sebeple msfconsole ile metasploit'i başlatıyorum.



-"use auxiliary/scanner/http/wordpress\_login\_enum" komutu ile scriptimi başlatıyorum.

-Ardından "options" komutu ile istediği ayarları görüntülüyorum.



-Wordpress URL'sini,Wordlistlerimi ve portumu set ediyorum.

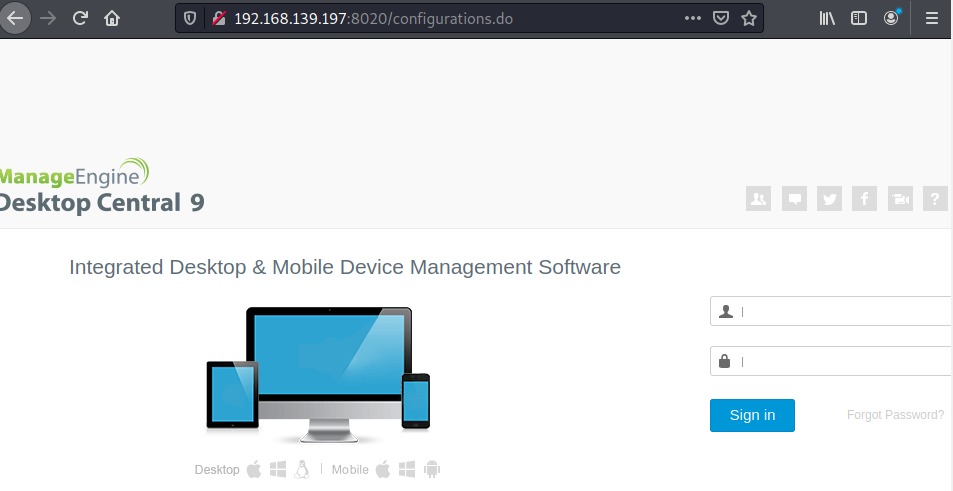


-Verbose'u da aktif hale getirip işlemi başlatıyorum

-İşlem sırasında şifreler çok basic olduğu için bu kadar basit bir wordlist ile bile şifre tespiti yapabildim.

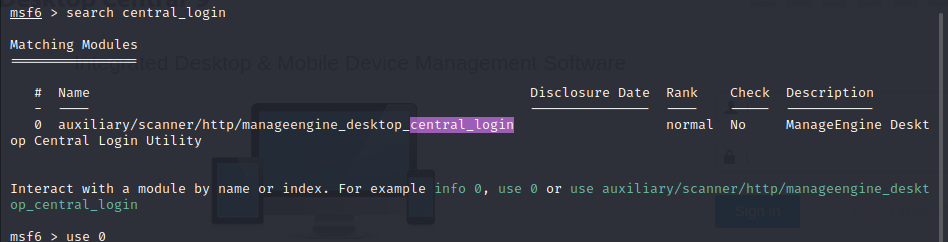
***ManageEngine Login’e Attack***

-ManageEngine servisinde bulunan login sayfasına bir bruteforce denemesi gerçekleştireceğim.



-Tarayıcı üzerinde login ekranını görüntülüyorum.

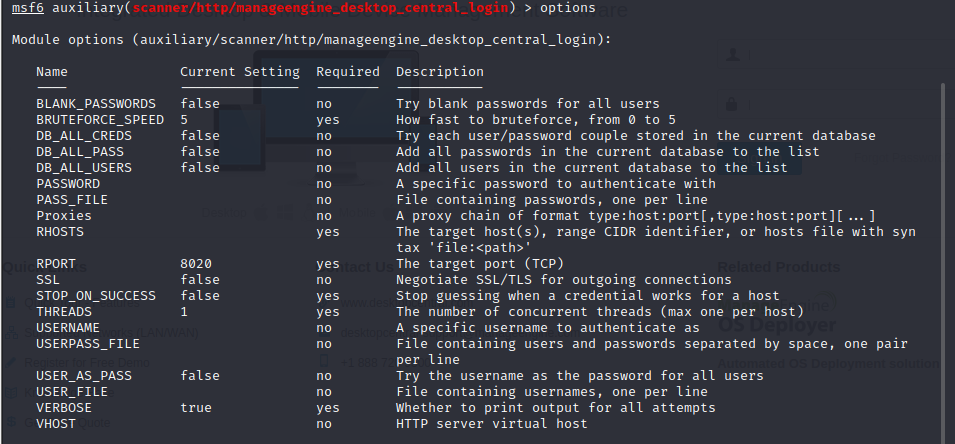
-Bu servis 8020 portunda çalışmaktadır.



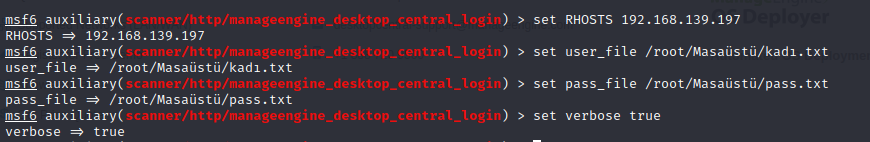
-Bu işlem içinde metasploit aracından yararlanacağım.

-Aracı başlattıktan sonra search komutu ile bir arama gerçekleştiriyorum.

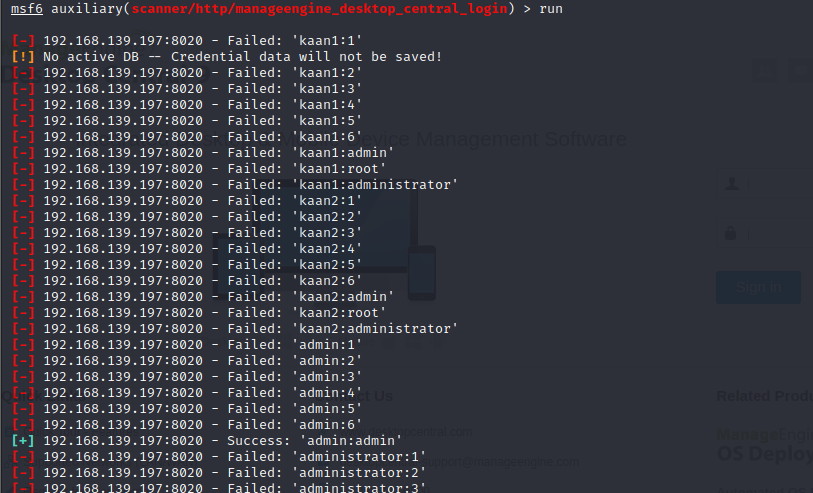
-Ardından bulduğum exploit'i başlatıyorum.



-"options" komutu ile istediği ayarları görüntülüyorum.



-Gerekli ayarları set ediyorum.



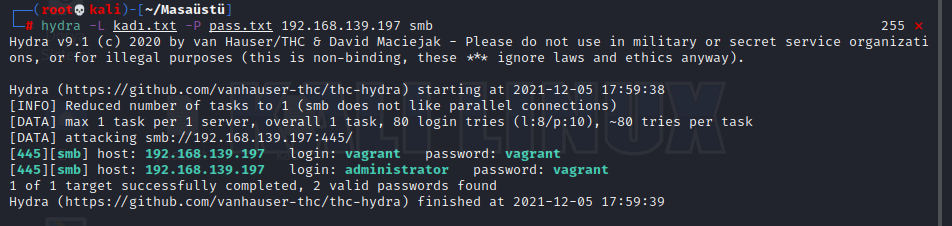
-Ardından işlemi başlatıyorum.

-Başarılı bir şekilde şifreyi buluyorum.

***SMB’ye Attack – Exploit***

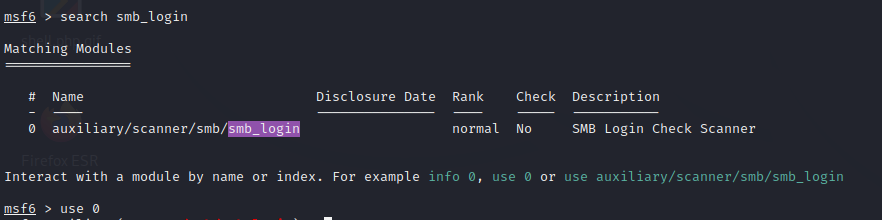
-SMB servisine bir Bruteforce işlemi gerçekleştireceğim.

-Bu işlemi Hydra aracı ile gerçekleştireceğim.



-Hydra aracı ile bir Bruteforce denemesi yapıyorum.

-Başarılı bir şekilde şifreyi elde edebildim.

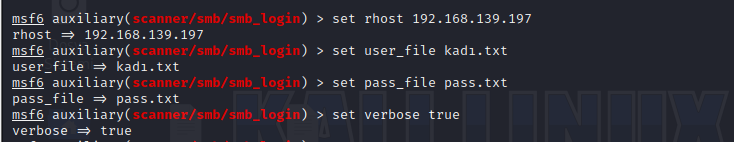


-Aynı işlemi metasploit üzerinden de gerçekleştirmek istiyorum.

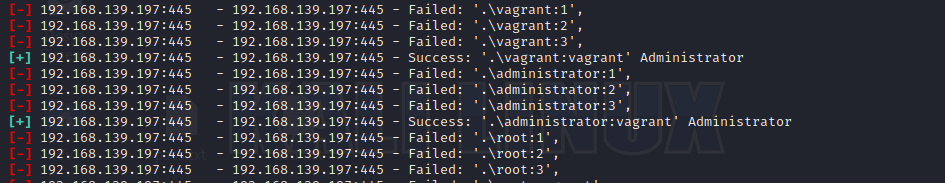
-Burada "smb\_login" scriptini kullanacağım.



-"Options" komutu ile istediği ayarları görüntülüyorum.

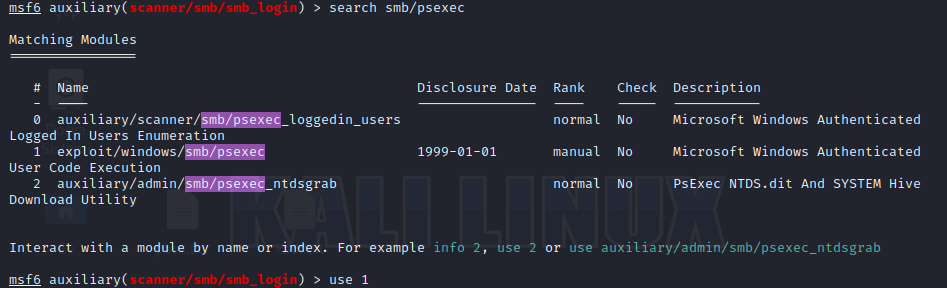


-Gerekli ayarları set ediyorum.



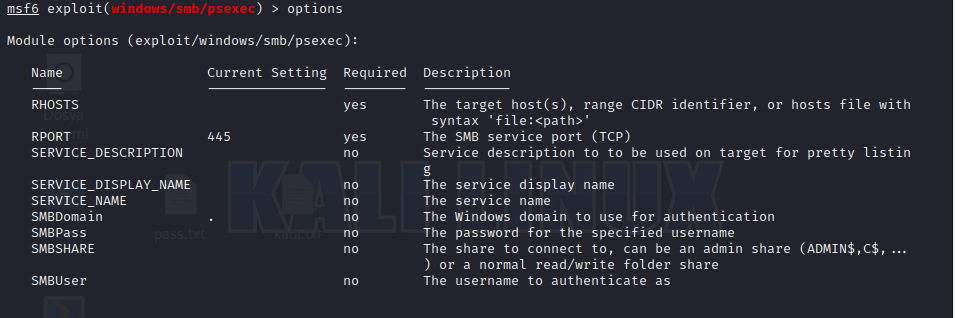
-Gerekli ayarlardan sonra işlemi başlatıyorum.

-Başarılı bir şekilde kullanıcı adı ve şifreyi bulabildim.

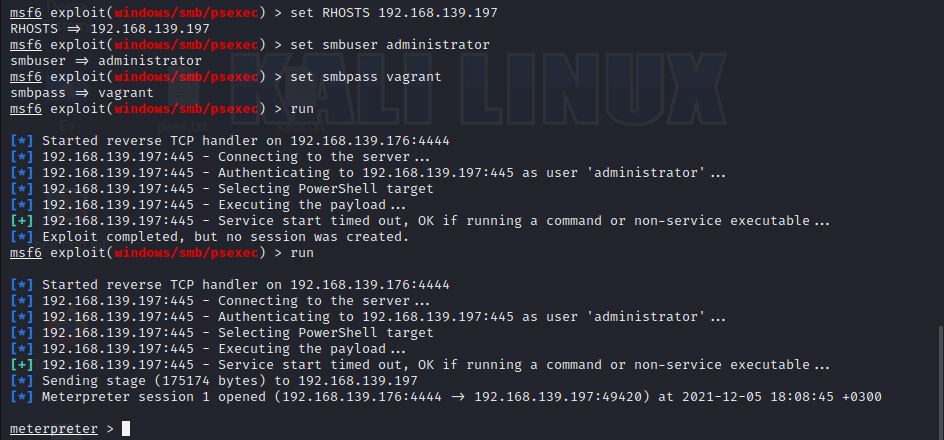


-Exploit kurabilmem için bir script arıyorum.

-Burada aklıma "psexec" scripti geliyor ve bu scripti başlatıyorum.



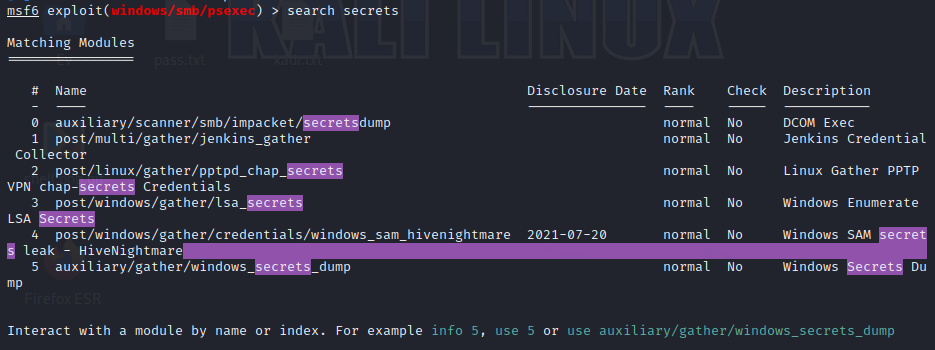
-"options" komutu ile gerekli ayarları görüntülüyorum.



-Gerekli ayarları set ediyorum ve scripti çalıştırıyorum.

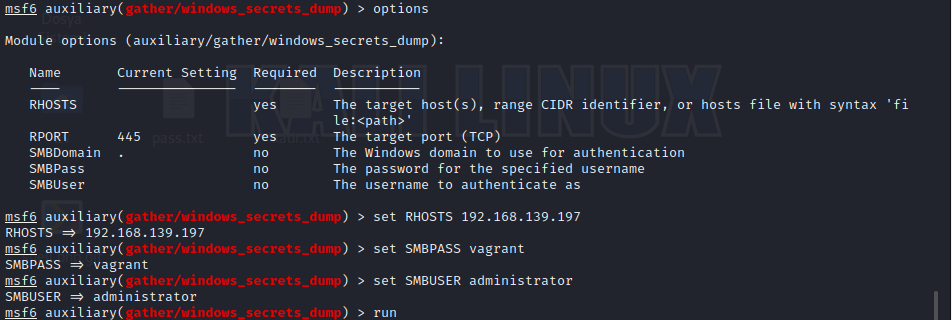
-Burada 2 kere deneme yaptım fakat birincisinde başarılı olamadım.

-Bu sebeple birden çok deneme yapmak bizi avantajlı kılabilir.

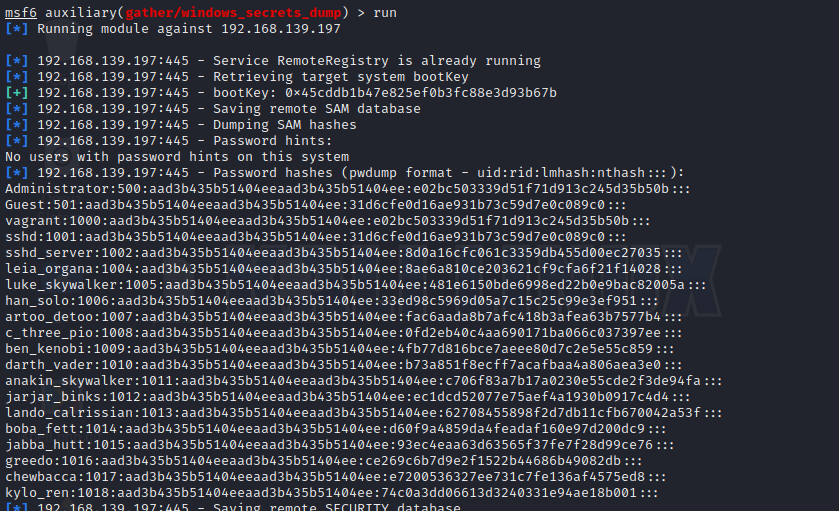


-Kullanıcı adı ve şifreyi biliyorken "secretdump" scripti ile sistem içerisinde bulunan tüm şifrelere hashli bir şekilde erişim sağlayabiliriz.

-SAM içerisinden bu bilgiler çekilir.



-Scriptin içerisine gerekli ayarları set ediyorum ve ardından işlemi başlatıyorum.



-İşlemin sonucunda sistem üzerinde ki tüm şifreleri bana hash'li bir şekilde aktardı.