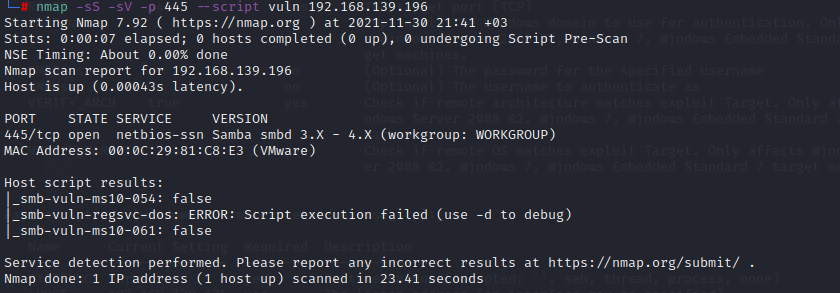
|  |
| --- |
| ***Exploit Saldırıları*** |
| Kaan Efe Öğüt  *ADLİ BİLİŞİM MÜHENDİSLİĞİ* |
| -Windows ve Linux ortamlarında bulunan servislere birlikte exploit saldırıları gerçekleştireceğiz. |

**13.12.2021**

Nmap ve Metasploit ile MS17-010 Açığı Kontrolü

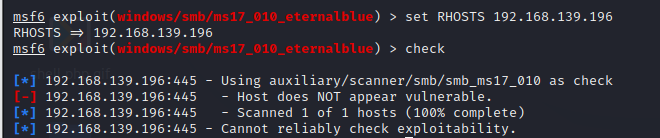
-Microsoftun meşhur güvenlik açığı olan MS17-010 Eternal Blue açığının bulunup bulunmadığını kontrol edeceğiz.

-Bu işlem için "Metasploitable" zafiyetli aracından yararlanacağım.



- İlk önce işlemi nmap üzerinden vuln scripti ile gerçekleştireceğim ve burada MS17-010 açığının aktif olmadığını görüntülüyorum.

-Ardından metasploit aracı ile bu işlemi yapmak istiyorum.



-"Msfconsole" ile aracı başlatıyorum.

-Ardından "search ms17" komutu ile kullanabileceğim exploitleri görüntülüyorum.

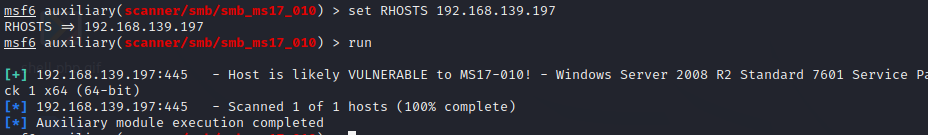
-İçerisine saldıracağım IP adresini set ediyorum.

-Ardından check komutu ile işlemi başlatıyorum.

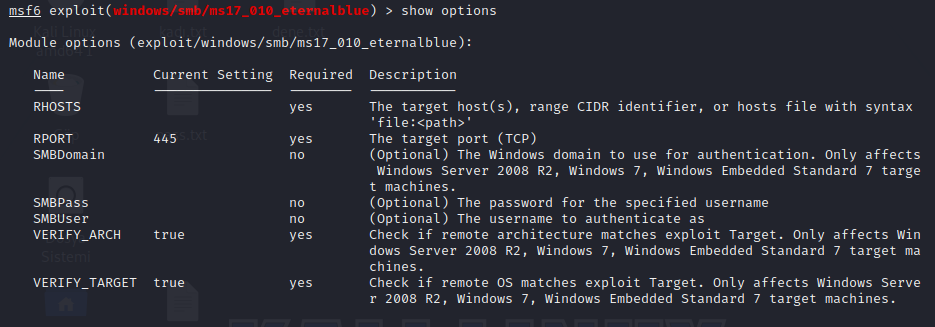
-Bu araç üzerinde açık bulunmadığını tarafıma aktarıyor.

***MS17-010 Açığına Exploit Saldırısı***

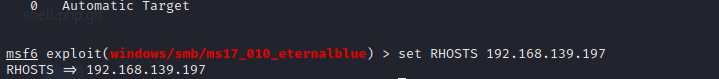
-Öncelikle MS17 açığının bulunup bulunmadığını kontrol etmek için Metasploit aracında buluna "smb\_ms17\_010" exploitini çalıştırıyorum.



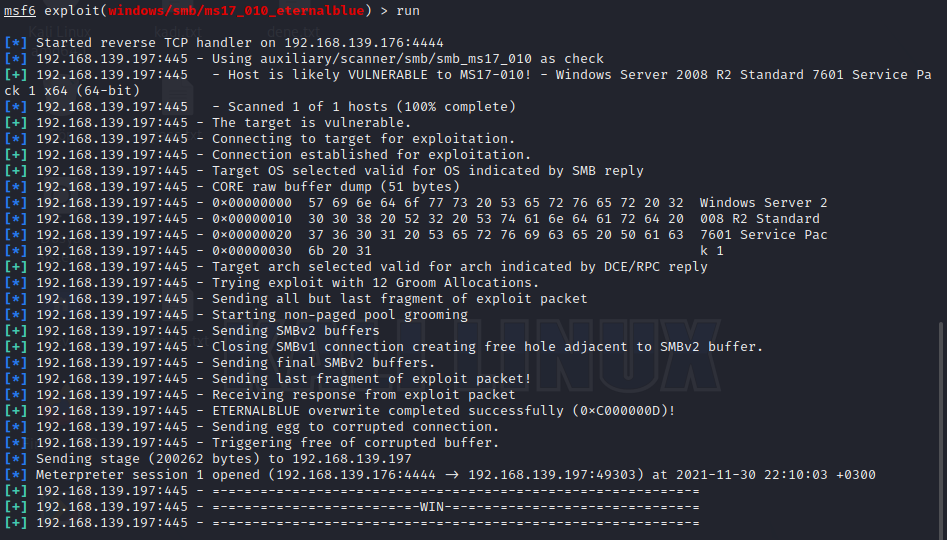
- Sonucuna baktığımda açığın bulunduğunu görüntülüyorum.



- Shell bağlantısı kurmak için "ms17\_010\_eternalblue" exploitini kullanıyorum.



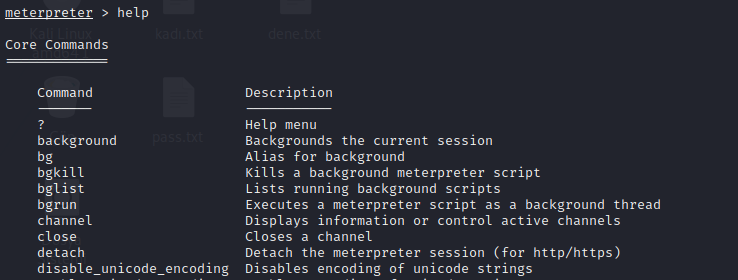
- İstediklerine baktığım da saldıracağım IP adresini set ediyorum.



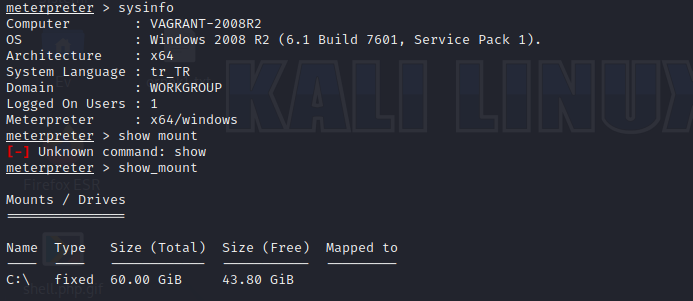
-Başarılı bir şekilde meterpreter üzerinden bağlantı kurabildim.

***Meterpreter ile Hedefte Sistem Keşfi***

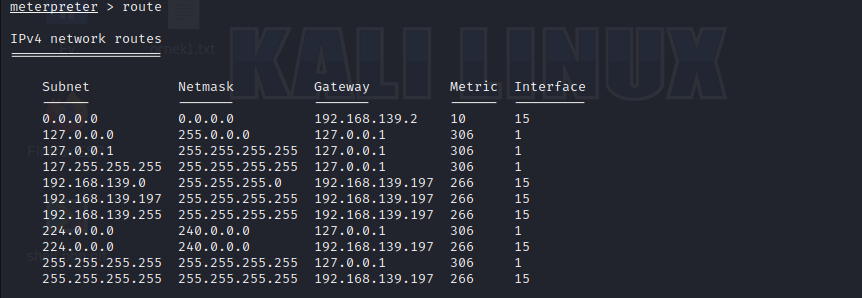
-Meterpreter üzerinden bağlantı kurduğum makine meterpreter komutları çalıştırabilirim.



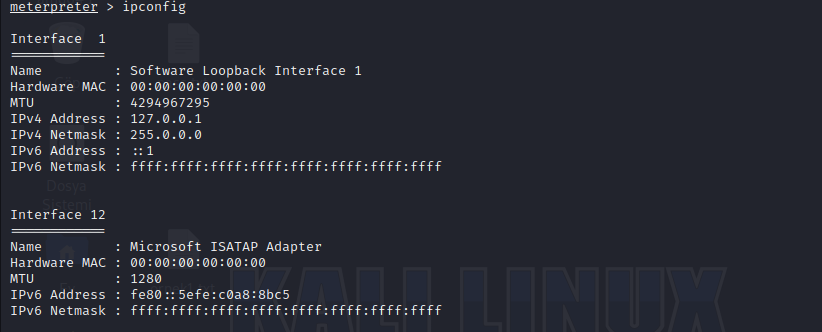
- Bu komutlara "help" yazarak erişim sağlayabilirim.



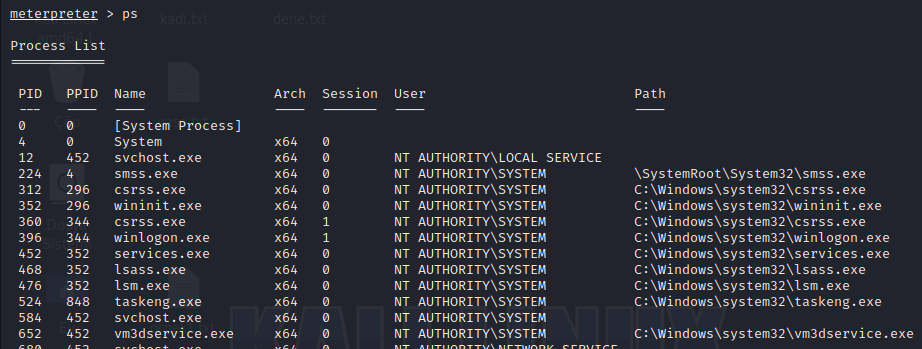
- Burada "sysinfo,show\_mount" gibi komutlar çalıştırarak erişim sağladığım zafiyetli makine üzerinden işlem sağlayabilirim.



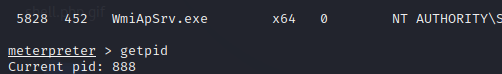
- Route komutu ile IPTables üzerinden işlem yapabilirim.



- Ipconfig ile Interface'ler hakkında bilgi sahibi olabilirim.

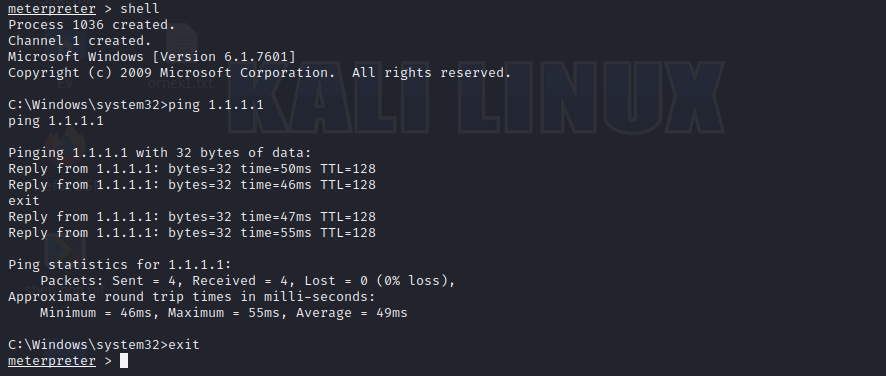


- "Ps" komutu ile çalışan processleri görüntüleyebilirim.



- "getpid" komutu ile arka planda çalıştığım process'i görüntüleyebiliyorum.

-Burada kill komutu ile istediğim processleri kapatabilirim.



- Ayrıca "shell" komutu ile işletim sistemine geçiş yapabilir.İşletim sistemi üzerinde bulunan komutları çalıştırabilirim.

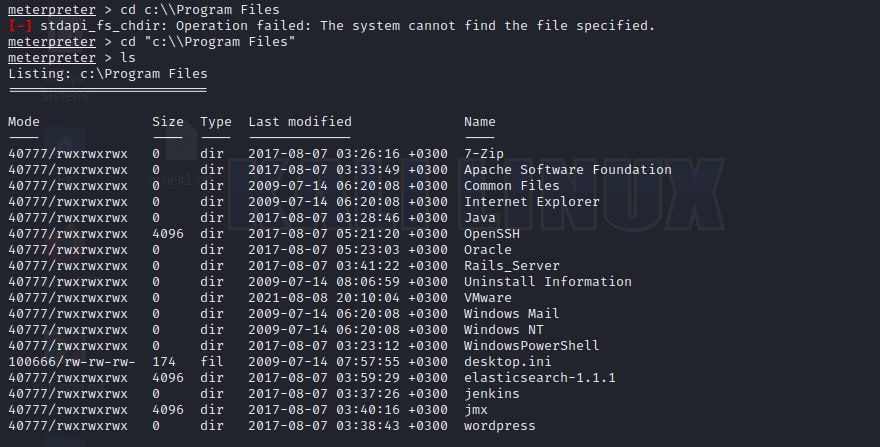
-Exit komutu ile shell komutundan çıkabilirim.

***Meterpreter ile Hedefte Dosya Dizin Yönetimi***

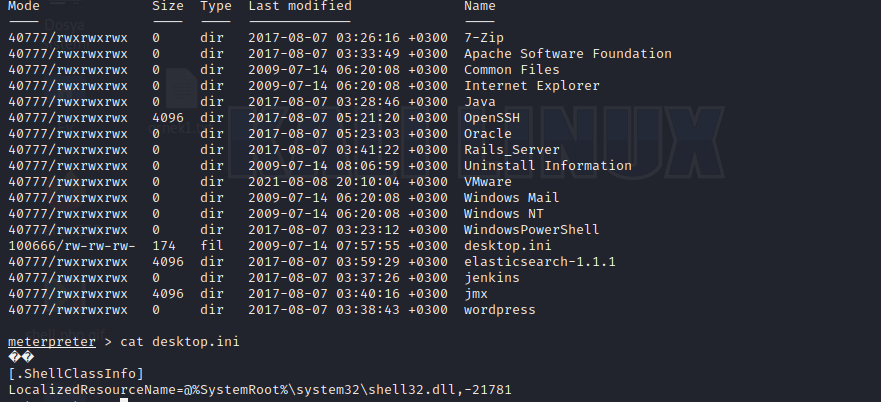


- Pwd komutu ile bulunduğum dosyayı görüntülüyorum.Her zaman system32 üzerinde başlamaz.Metasploit shell bulduğu yerden giriş yapmamı sağlar.

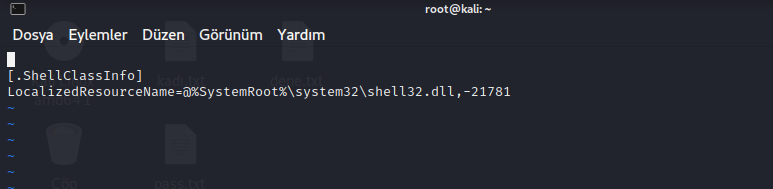
-Ayrıca ls komutu ile "C" diski üzerinde bulunan dizinleri görüntülüyorum.



- Örneğin "C" üzerinde bulunan Program Files dizinine erişim sağlamak için cd komutunu kullanırım fakat burada boşluk kullandığım için "" içerisinde işlem gerçekleştirmeliyim.



- "cat desktop.ini" komutu ile okuma iznimin bulunduğu bir dosyanın içeriğini görüntüleyebildim.



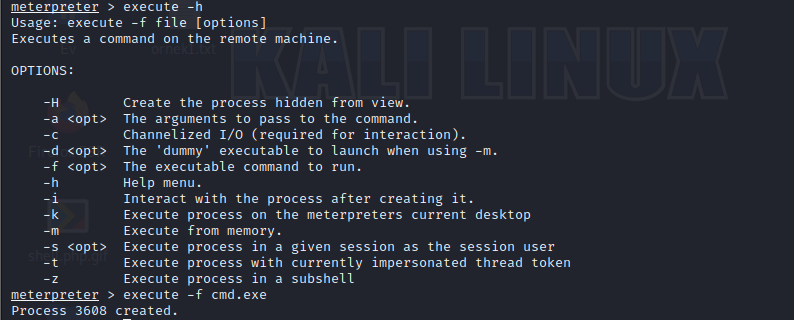
- "edit" komutu ile içeriğini Nano editörü ile açabilirim.

-Burada :q ile çıkış yapabilirim.

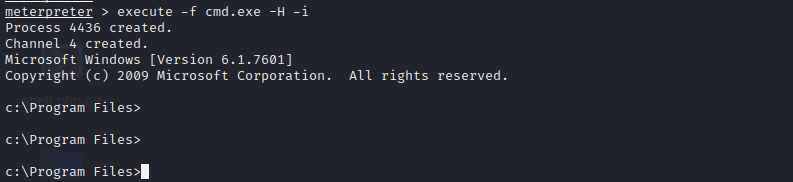


- Ayrıca burada "de" yazıp iki kere Tab yaptığım da kullanabileceğim fonksiyonları görüntüleyebilirim.

-Burada karşıma del komutunun çıkması bunu silebileceğim anlamına gelmektedir.



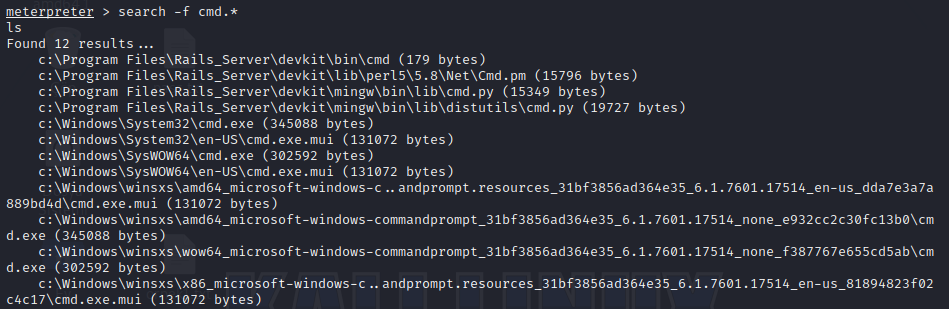
- İçerisinde bulunan dosyaları nasıl çalıştırabileceğimi "execute -h" komutu ile öğrenebilirim.



- "execute -f cmd.exe -H -i" komutunu kullanarak işleme geçiş yapabiliyorum.

Cmd üzerinde kullanabileceğim tüm komutları burada kullanabilirim.

-"exit" komutu ile çıkış yapabilirim.



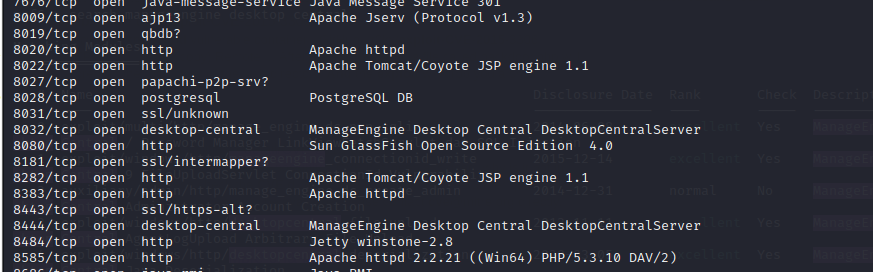
- "cmd" isimli dosyaları bu şekilde "search" komutu ile görüntüleyebilirim.



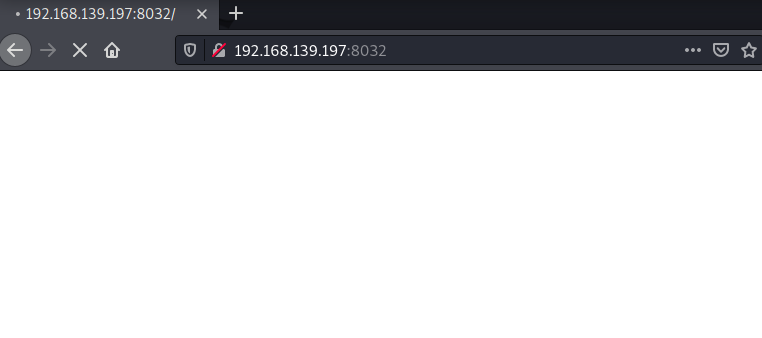
- Ayrıca sistem üzerinde bulunan bir dizini kendi bilgisayarıma "download" komutu ile indirebilirim.

-İndirme işlemi yapabileceğim gibi "upload -/Masaüstü/dene.txt" komut ile yükleme yapabilirim.

***Exploit Araştırması***



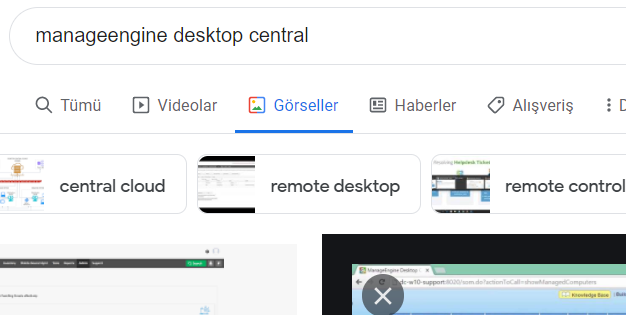
- Detaylı Nmap taraması gerçekleştirdiğim de burada DesktopCentralServer kısmı dikkatimi çekiyor.



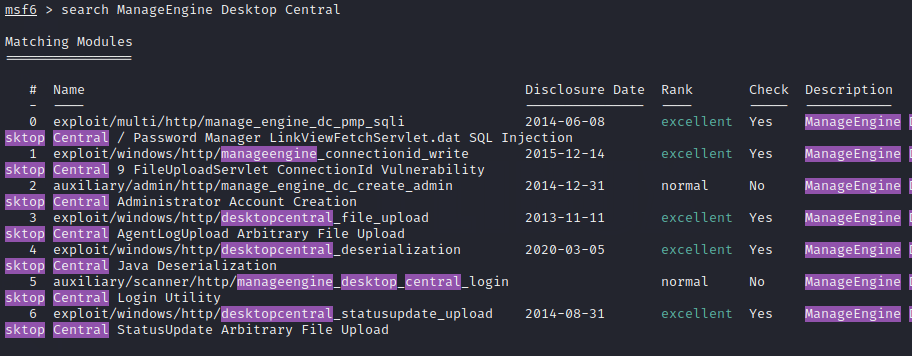
- Bu portları tarayıcı üzerinde görüntülemeye çalıştığımızda hiçbir dönüt alamayacağız.

-Bunun sebebi bunların Web servisi olmasıdır.Web sayfası da bir web servistir fakat bu insanla etkileşime geçmeyen kısımdır.

-Vulnerability olanlar HTTP üzerinden işlem gerçekleştirilir.



- "Manageengine Desktop Central" araması gerçekleştiriyorum ve 8020 portunda çalıştığını görüntülüyorum.



- Portu tespit ettikten sonra Metasploit aracımı çalıştırıyorum ve burada "search manageengine desktop central" komutu ile exploit taraması gerçekleştiriyorum.

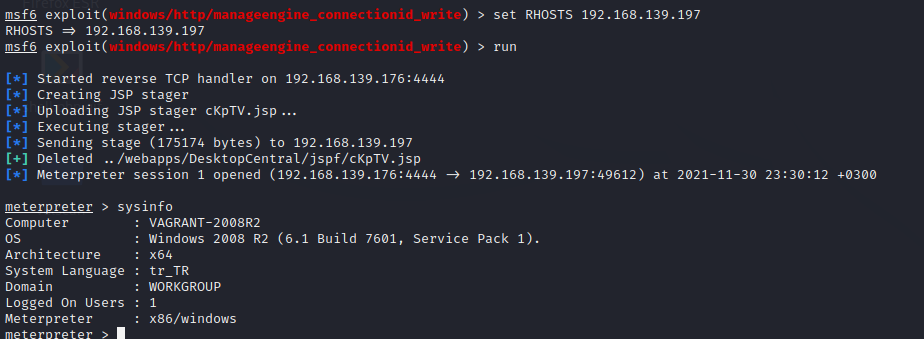
-Karşıma çıkan bu exploitleri Nessus gibi araçlar ile taratıp Cve'leri ve Versiyon numaralarını öğrenip onla işlem gerçekleştirebilirim.



- Tarayıcı üzerinde tarama gerçekleştirdiğimde "rapid7" sitesi üzerinde metasploit üzerinde kullanabileceğim exploit hakkında tüyo vermektedir.

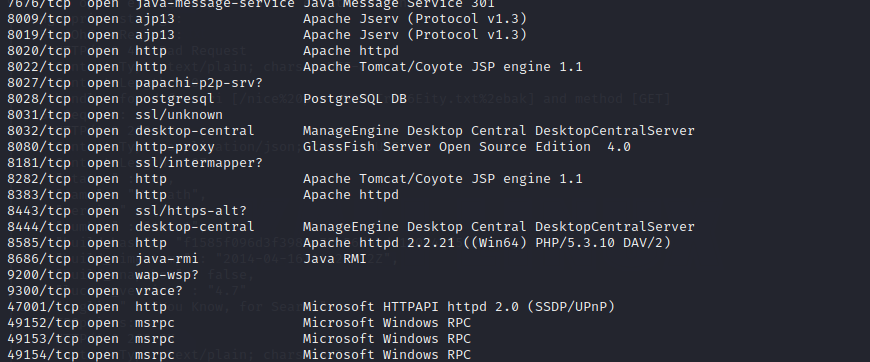
***ManageEngine’e Exploit Saldırısı***

-Burada versiyon bilgisi ile de tarama gerçekleştirip bu exploiti tespit edebilirdim.

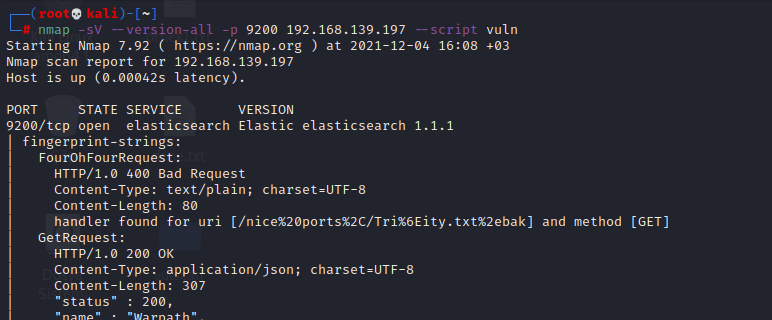


- Az önce bulduğum exploiti kullanarak başarılı bir şekilde meterpreter bağlantısı kurabildim.

***ElasticSearch’e Exploit Saldırısı***

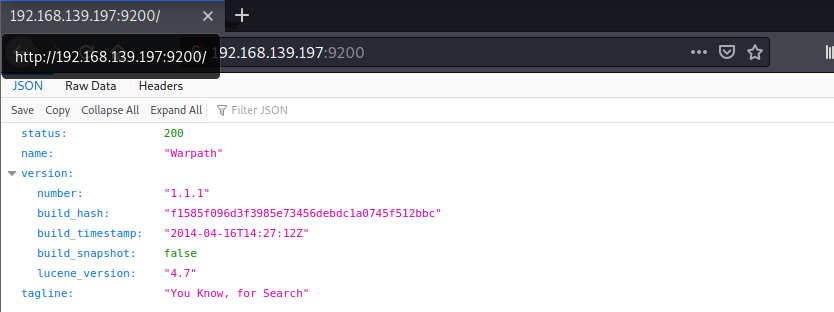


- Daha önce yaptığımız nmap taramasında 9200/tcp portunda versiyon tespiti yapamadı.



- Gözükmeyen versiyon bilgisini görebilmek için 9200 portuna bir tarama gerçekleştiriyorum.

-Burada ElasticSearch olduğunu görüntülüyorum.

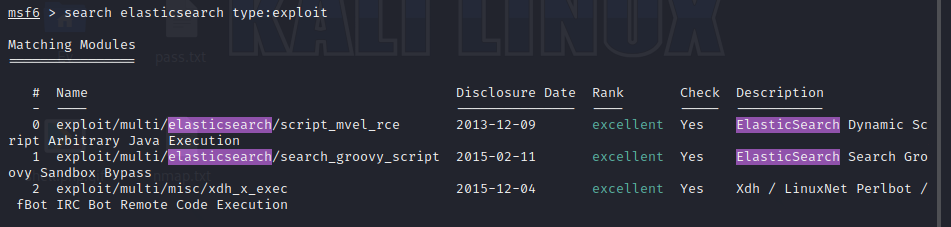


- Tarayıcı üzerinde çağırdığımda nmap üzerinde elde ettiğim bilgileri de görüntülüyorum.

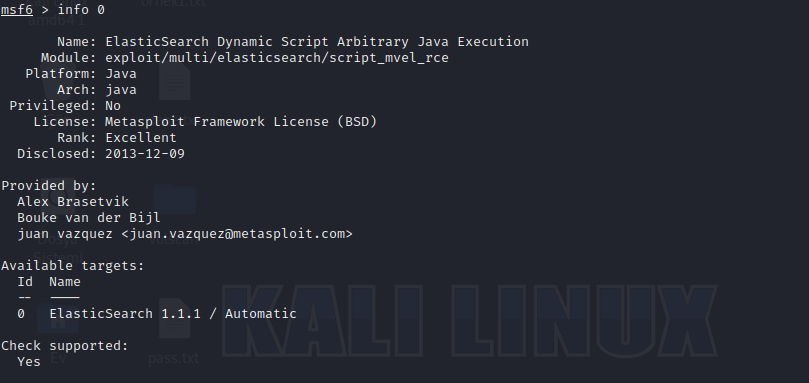


- Bu açık hakkında kullanabileceğim exploitlere erişim sağlamak için Metasploit üzerinde bir arama gerçekleştiriyorum.

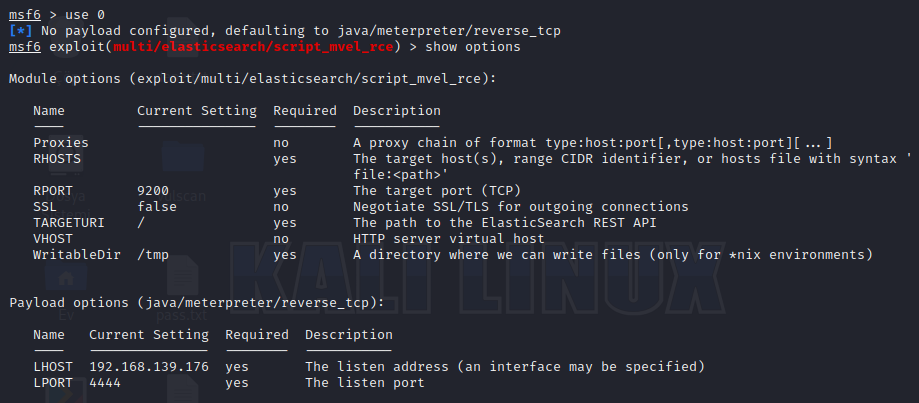
-Karşıma kullanabileceğim bu açıklar çıkmaktadır.



- Burada "type:exploit" şeklinde belirterek bir arama daha gerçekleştiriyorum ki karşıma sadece exploitler gelsin.

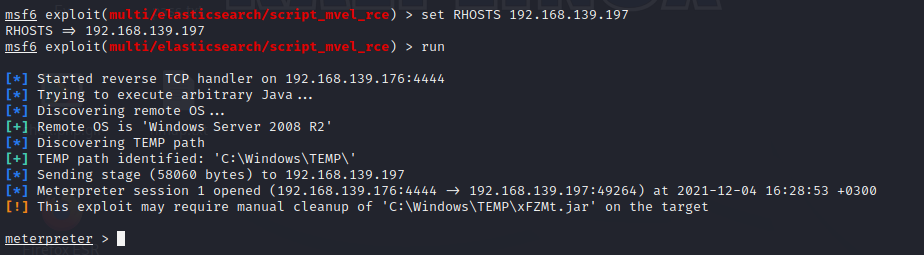


- "info 0" ile kullanabileceğim exploit'in versiyonunun da tuttuğunu görüntülüyorum ve exploitin yaptığı işlemleri de görüntülüyorum.



- "use 0" komutu ile "script\_mvel\_rce" isimli exploiti başlatıyorum.

-Ardından "show options" komutu ile set edeceğim ayarları görüntülüyorum.



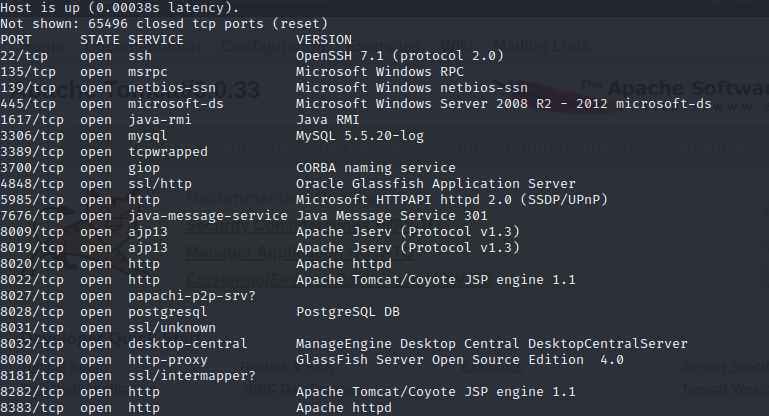
- Portum doğru olduğu için sadece "HOST" adresimi set ediyorum ve ardından işlemi başlattım.

-İşlemin sonucunda başarılı bir şekilde bağlantı kurabildim.

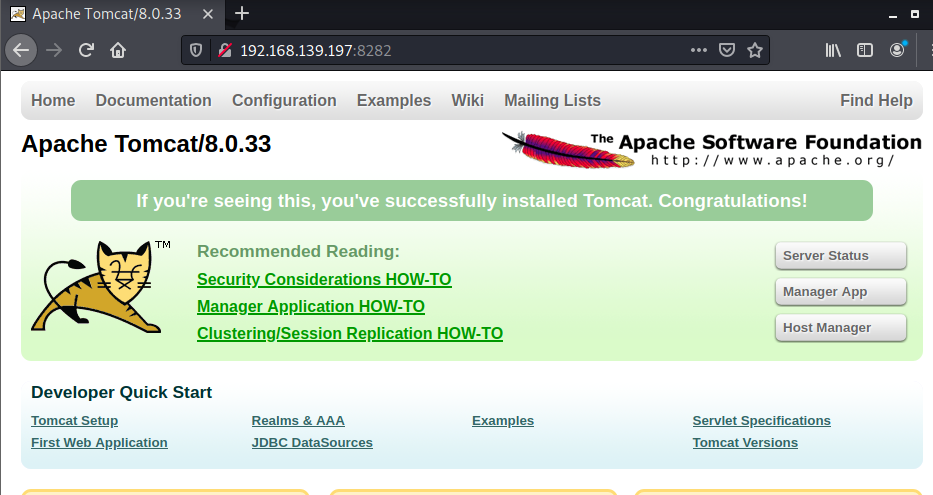
-İz silme aşamasında silmem gereken dosyayı tarafıma bildirdi.

***Apache Axis2’ye Exploit Saldırısı***

- Bu senaryomuzda 8282 portunda bulunan "Apache" servisi üzerinden bir erişim almaya çalışacağım.

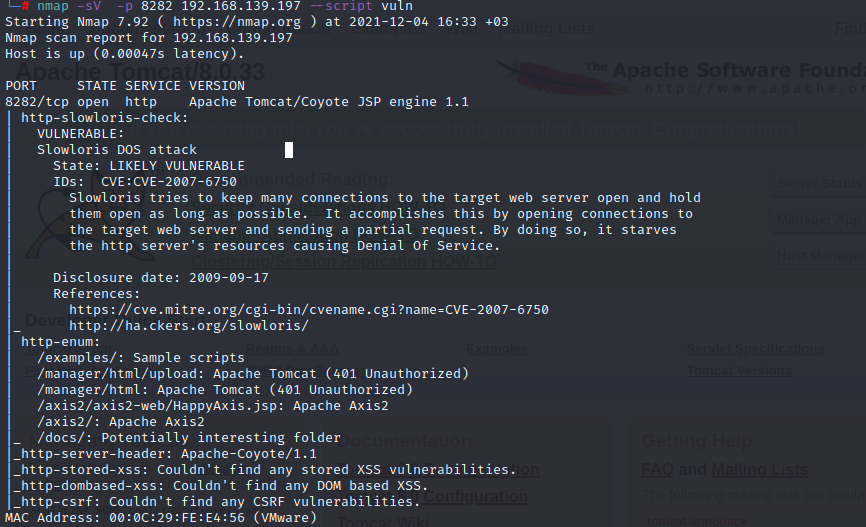


- Nmap sonuçlarına baktığımda http servisinde çalıştığını görüntülüyorum.



- Tarayıcı üzerinde görüntülemeye çalıştığım da version bilgilerine de erişim sağlıyorum.

-Eğer burada version bilgisi elde edemeseydim tek port üzerinde "vuln" scripti ile güven5lik açığı tespit edilmelidir.

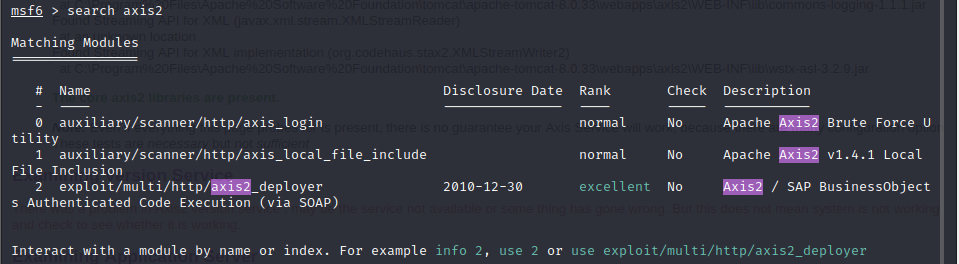


- Nmap taramasını yine de gerçekleştiriyorum ve burada Axis2 olduğunu tespit ediyorum.

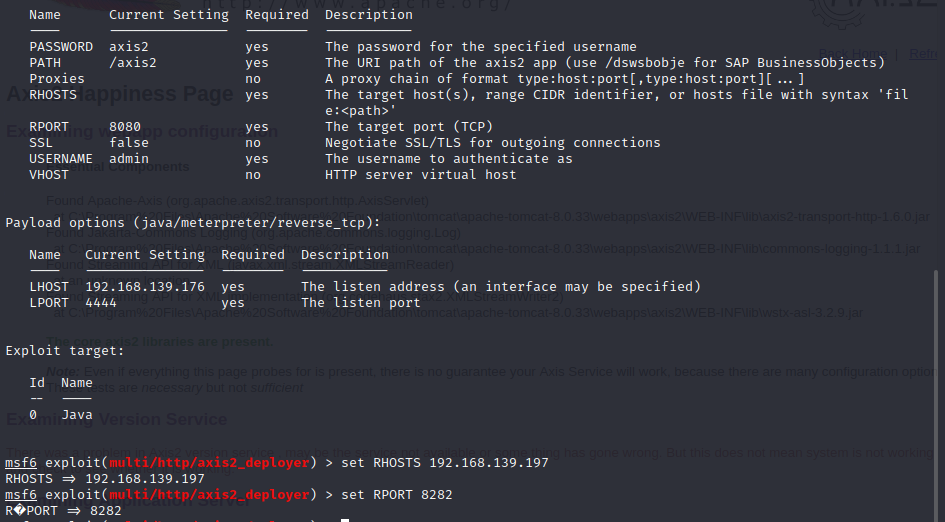


- Nmap üzerinde elde ettiğim bağlantı üzerinden de kontrolünü sağladığım da "Axis2" olduğunu tespit ediyorum.

- Diğer örneklerde yaptığım gibi metasploit aracını başlatıyorum ve burada "Axis2" ile ilgili bir tarama gerçekleştiriyorum.

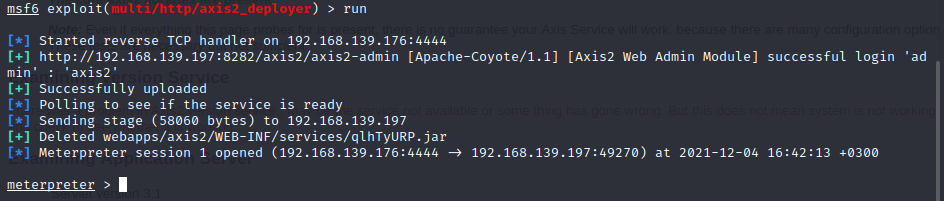


-2 Adet Auxliary ve 1 adet Exploit tespit ediyor.



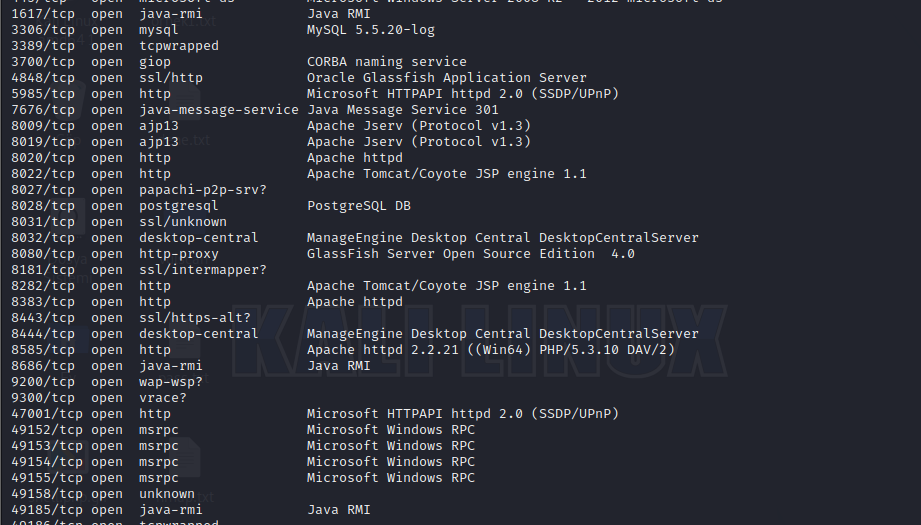
- Exploiti başlatıyorum ve burada gerekli olan RHOSTS bilgisini set ediyorum.

-Burada dikkat edilmesi gereken yer port adresinin yanlış oluşudur.

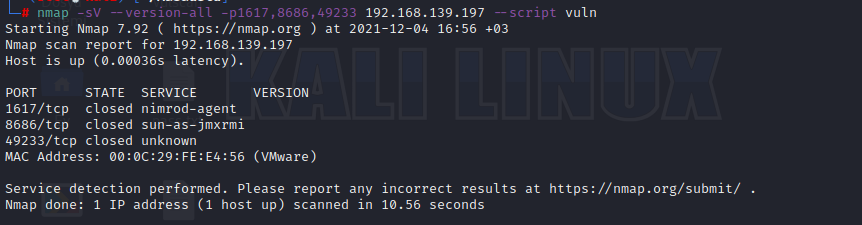


- Onu da düzelttikten sonra işlemi başlatıyorum ve başarılı bir şekilde bağlantı alabildim.

***Java JMX’e Exploit Saldırısı***



-Nmap taraması üzerinde baktığım da birden fazla port üzerinde Java servisinin çalıştığını görüntülüyorum.



- Aynı şekilde nmap üzerinden "vuln" scripti ile bir açık yakalamaya çalışıyorum.

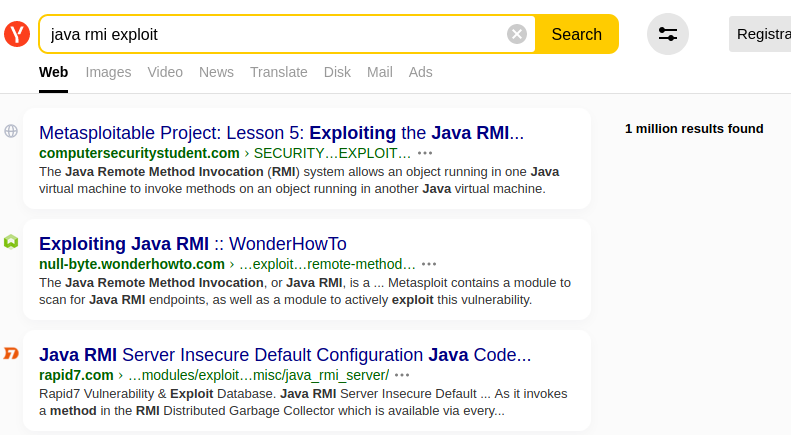
-Fakat yine bir bilgi elde edemiyorum.



- Bu yüzden metasploit aracı üzerinden bir arama gerçekleştireceğim.

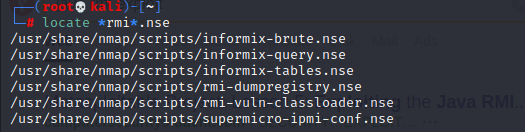
-Burada RMI olduğunu keşfettiğim için ona bağlı bir araştırma gerçekleştiriyorum.

-Fakat çıkan sonuçlara baktığımda 11 adet sonuç elde ediyorum.Bunları eğer tek tek denersem kesinlikle log kayıtlarına yakalanırım.



- Bu sebeplerden ötürü birazda google üzerinden arama gerçekleştiriyorum.

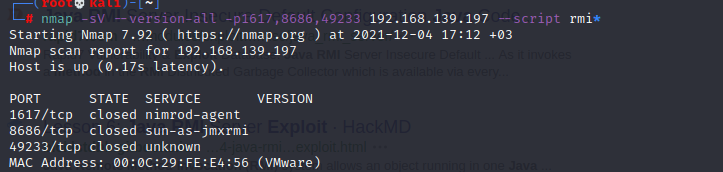
-Burada yapmış olduğum arama sonucunda birden fazla exploit ile karşılaştım fakat bunlarda aynı risklere sahiptir.



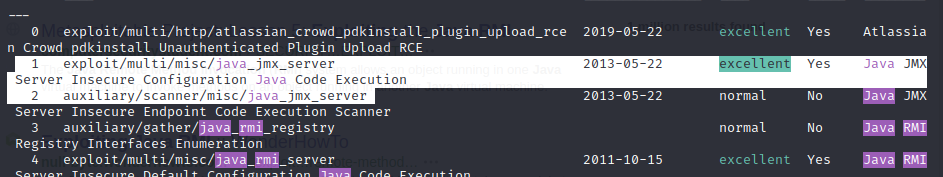
- Nmap aracı sadece güvenlik açığı taraması yapmıyordu.

-Bu sebeple locate komutu ile içinde "rmi" geçen ve uzantısı ".nse" ile biten dosyaları bulmaya çalışıyorum.

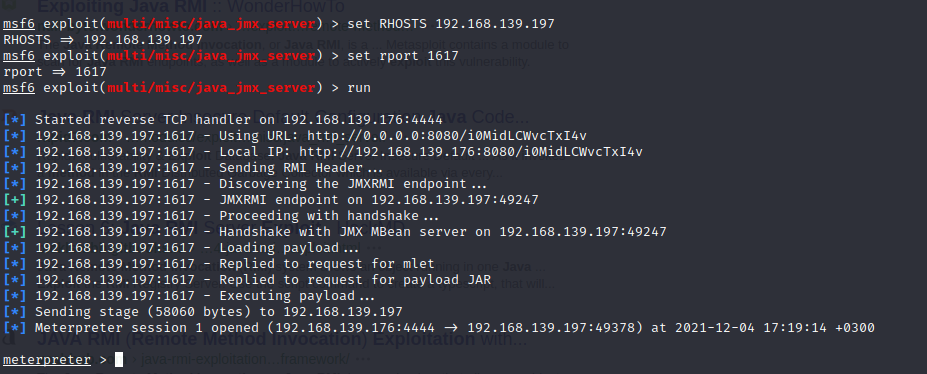
-Burada arama sonucunda 2 adet script karşıma çıkmaktadır.



- Burada da Java JMX diye bir bilgi elde ettim.



- Ardından tekrardan Metasploit üzerine geçiş yapıyorum ve JMX üzerinde kullanılan bir exploit buldum.

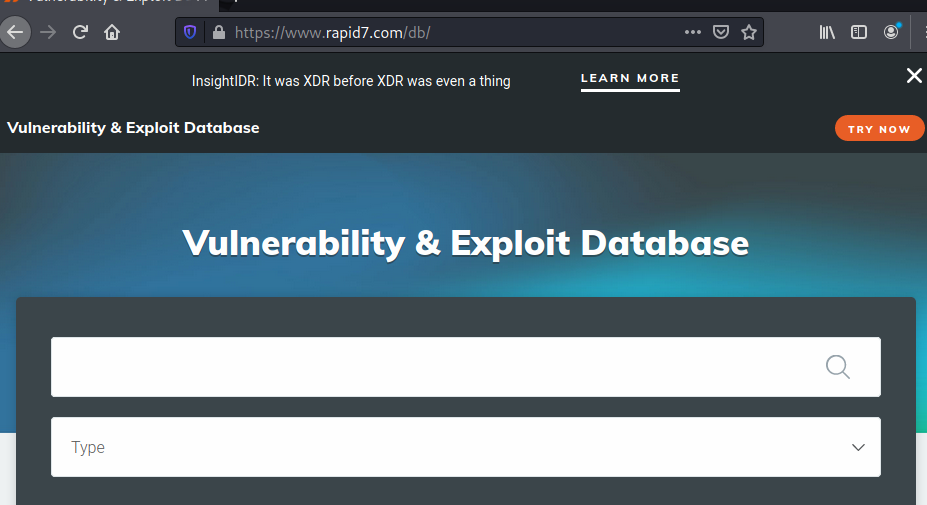


- Show options komutu ile görüntülediğim de RHOSTS ve RPORT bilgilerine ihtiyaç duyduğunu görüntüledim.

-İlk önce 1617 portu üzerinden bir deneme gerçekleştirdim ve bu port üzerinden başarılı bir şekilde bağlantı kurabildim.

***Exploit Veritabanları ve Kaynakları***

-Metasploit haricinde bilgi elde edebileceğimiz başka araçlara göz atacağız.



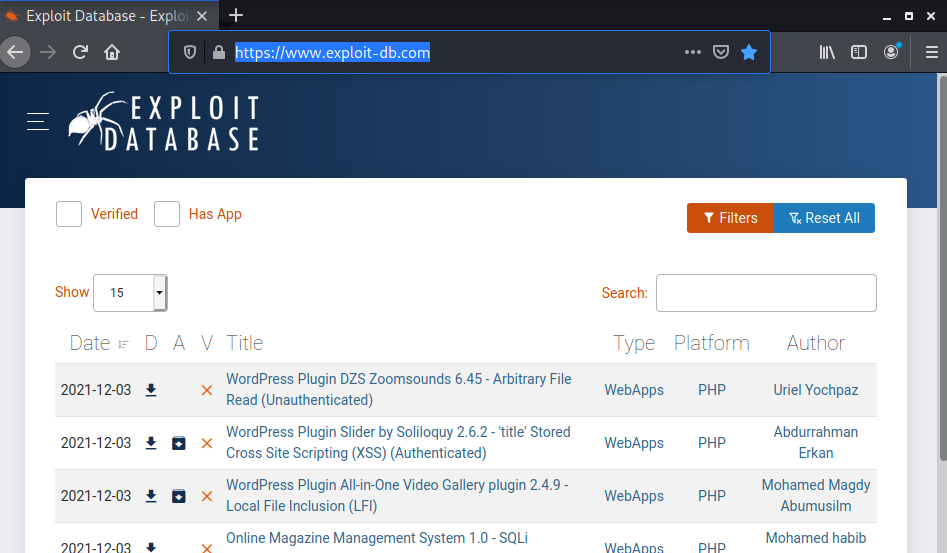
- "https://www.rapid7.com/db/" bağlantısı üzerinde bulunan bu sayfa ile başlıyoruz.

-Sayfanın görüntüsü bu şekildedir.



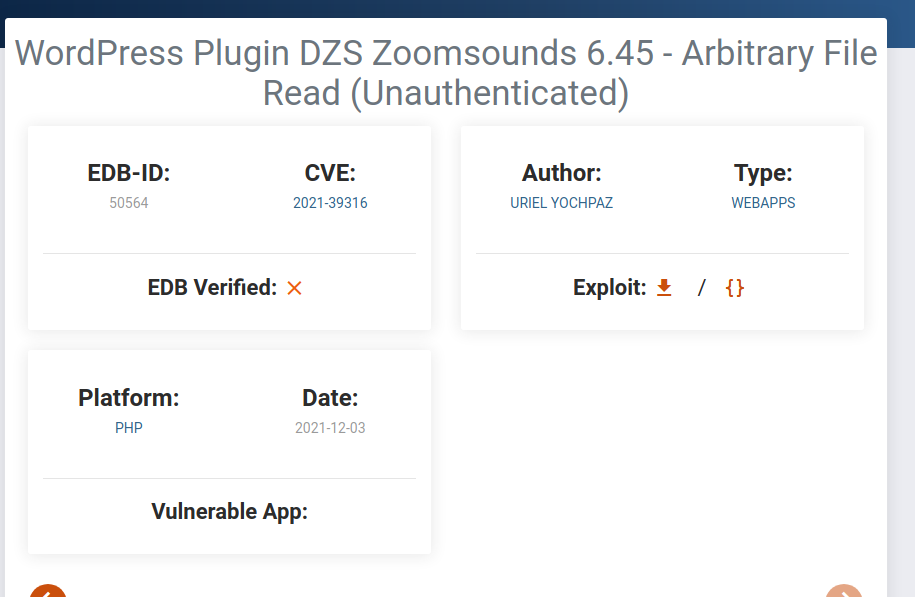
- Sayfanın alt taraflarına indiğimde burada çeşitli açıklar görünmektedir.

-Rastgele birine girdiğim de burada CVE numarası ve İşletim sistemi bilgilerinin verildiği ve kullanımıyla ilgili bilgilerinde yer aldığını görüntülüyorum.



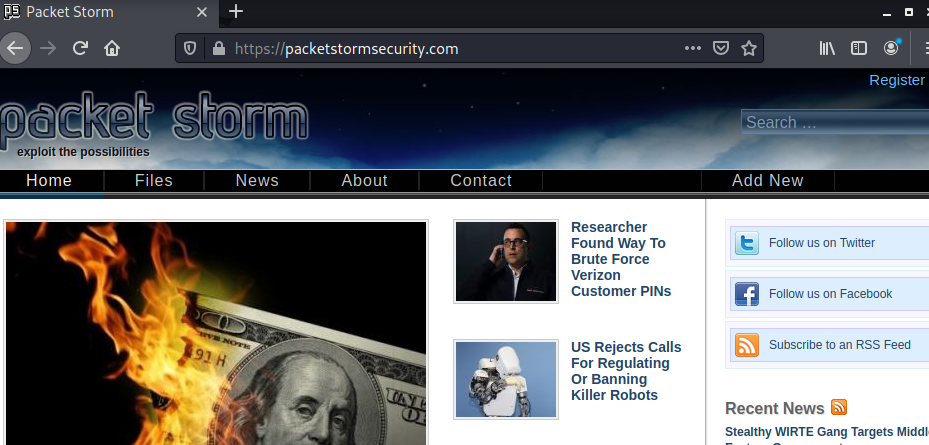
- Benzer işlemleri gerçekleştiren bir diğer sayfa ise "https://www.exploit-db.com/"'dir.

-Sayfanın görüntüsü bu şekildedir.



- Bir önceki örnekte olduğu gibi rastgele bir exploit'i görüntülüyorum ve "EDB Verified" kısmında kullanabilirliğinin doğrulanıp doğrulanmadığı ve bunların haricinde yazarı ve platformu hakkında bilgi sahibi olabiliriz.

-İndirme işlemi gerçekleştirdiğimizde çoğu zaman .txt şeklinde verse de bazen çalıştırılabilir şekilde de verebilir.



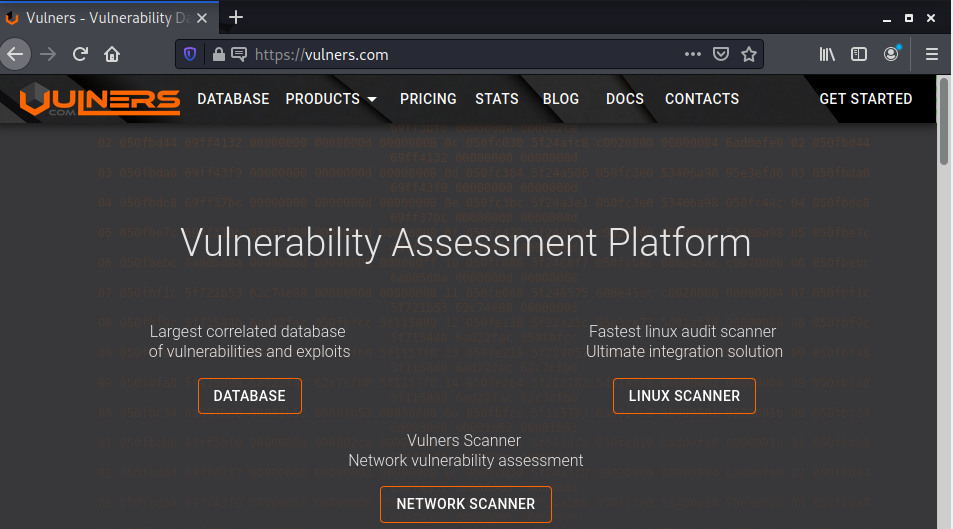
- Bir diğer sayfamız ise "https://packetstormsecurity.com/" bağlantısı üzerinde bulunmaktadır.

-Sayfanın görüntüsü bu şekildedir.Diğer sayfalar hakkında verdiğim bilgiler burada da geçerlidir.



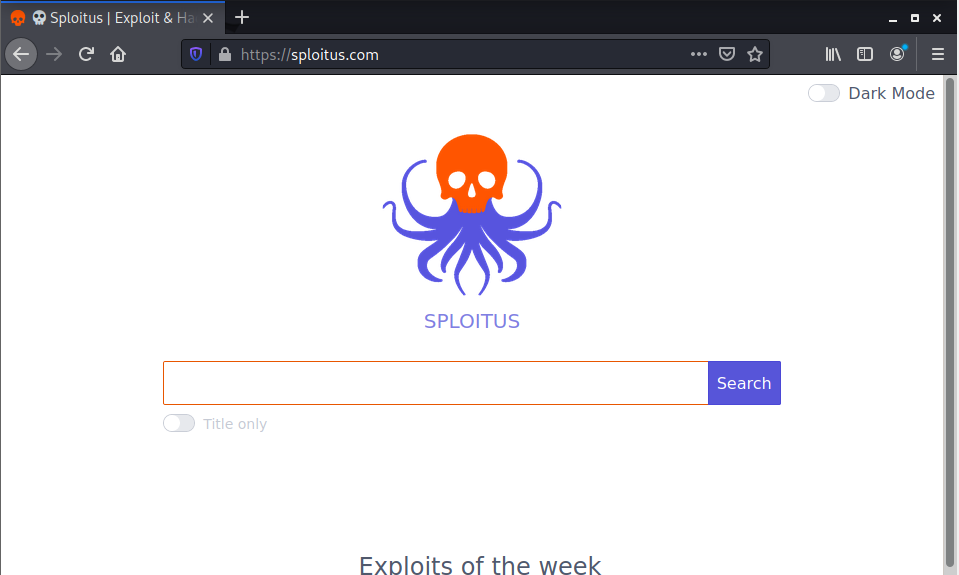
- Benzer işlemleri gerçekleştiren bir diğer sayfamız ise "https://cxsecurity.com/" bağlantısı üzerinde bulunmaktadır.

-Sayfanın görüntüsü bu şekildedir.Diğer sayfalar hakkında verdiğim bilgiler burada da geçerlidir.



- Benzer işlemleri gerçekleştiren bir diğer sayfamız ise "https://vulners.com/" bağlantısı üzerinde bulunmaktadır.

-Sayfanın görüntüsü bu şekildedir.Diğer sayfalar hakkında verdiğim bilgiler burada da geçerlidir.

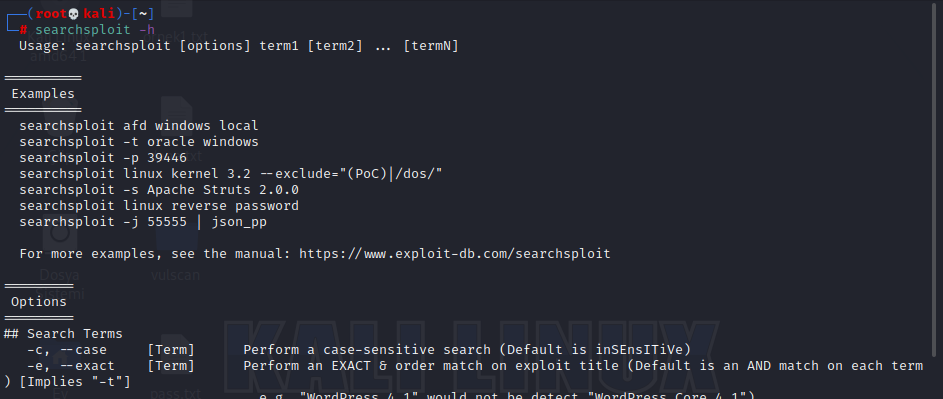


-Benzer işlemleri gerçekleştiren son sayfamız ise "https://sploitus.com/" bağlantısında bulunan tarayıcı sayfasıdır.

-Sayfanın görüntüsü bu şekildedir.Diğer sayfalar hakkında verdiğim bilgiler burada da geçerlidir.

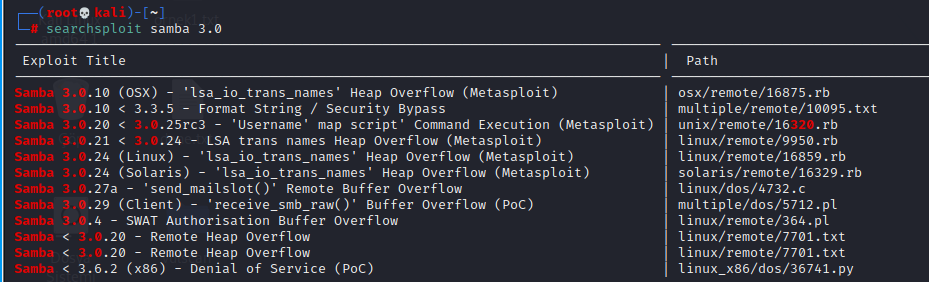
***Searchspoit ile Exploit-DB Kullanımı***

- Linux üzerinde kurulu olarak bulunan "Searchsploit" aracı exploit-db veritabanı üzerinde bulunan bilgiler üzerinde tarama gerçekleştirip bizim tarafımıza aktarır.

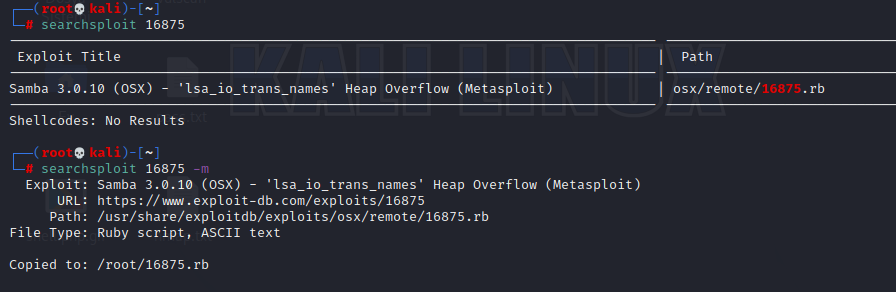


- "searchsploit -h" komutu ile kullanımı hakkında bilgi sahibi olabiliriz.

Ayrıca -u parametresi ile güncelleme yapılabilir.



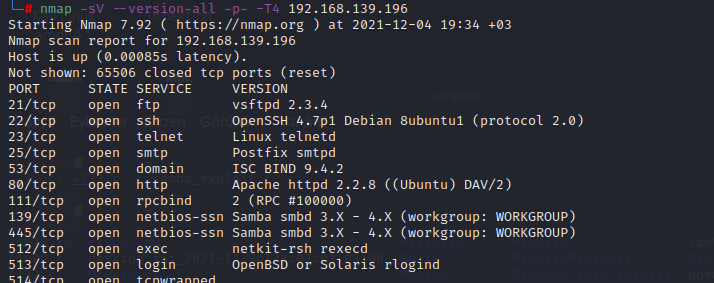
- Burada "samba 3.0" ile bir arama gerçekleştirdiğim de karşıma kullanabileceğim exploitleri vermektedir.



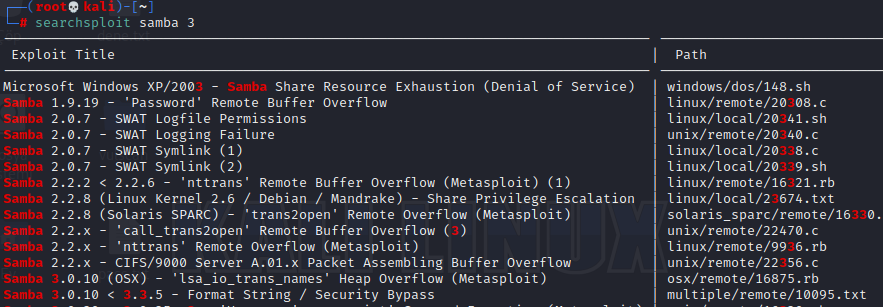
- "Searchsploit" üzerinde bir arama gerçekleştiriyorum ve "-m" parametresi ile bu exploiti kendi makineme çekiyorum.

***Manuel Exploit ile Apache’ye Saldırı***

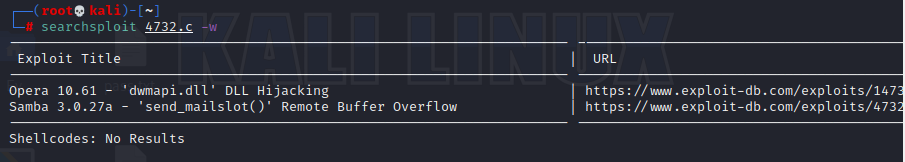
-139 Portunda bulunan Samba servisine searchsploit aracı üzerinden indirdiğimiz script ile sızmayı deneyeceğiz.



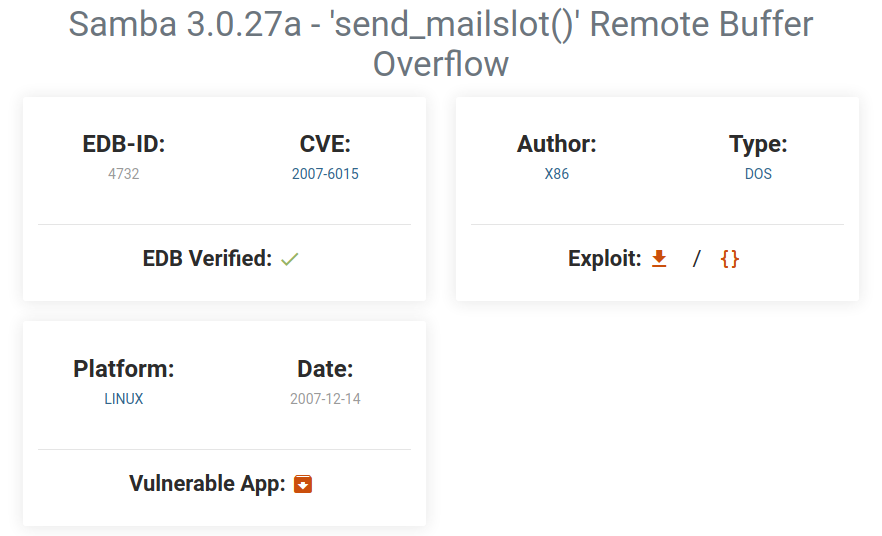
- Nmap taraması üzerinden de port doğrulaması gerçekleştiriyorum.



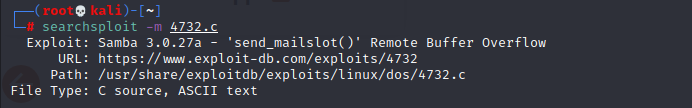
- Ardından searchsploit üzerinden bir tarama gerçekleştiriyorum.



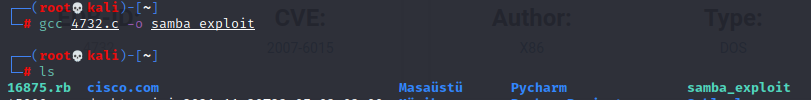
- "-w" parametresi ile web sitesine erişim sağlıyorum.



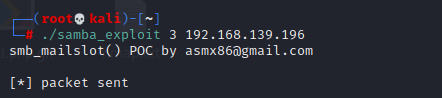
- Web sitesi üzerinde baktığımda gereksinim olarak bir kütüphane kurmamı istemiyor.



- Searchsploit üzerinden "id" numarasını bildiğim scripti indiriyorum.



- Ardından C kodunu gcc ile derliyorum ve çalıştırılabilir hale getiriyorum.



-Burada Netbios adını rastgele veriyorum.

-Asıl amacımız nasıl derlenip çalışacağını görmek.