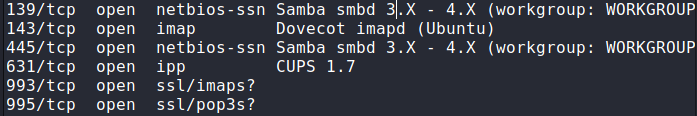
|  |
| --- |
| ***Searchsploit & Metasploit*** |
| Kaan Efe Öğüt  *ADLİ BİLİŞİM MÜHENDİSLİĞİ* |
| -Searchsploit ve Metasploit araçlarını kullanarak port zafiyetlerini kullanarak sunucu üzerinde sızma nasıl yapılır bunun hakkında bilgi vereceğim. |

**08.08.2021**

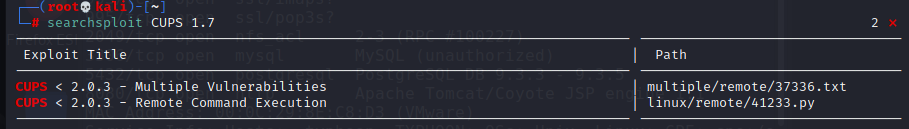
***Searchsploit ile Exploit bulma***

- Önceki yaptığımız uygulamalar da “typhoon.txt “ isimli bir txt oluşturmuştuk burada tarama sonuçlarını kayıt etmiştik.

-Searchsploit ile bir portta çalışan uygulamanın versiyonu veya adıyla zafiyet tarama işlemi gerçekleştireceğiz.



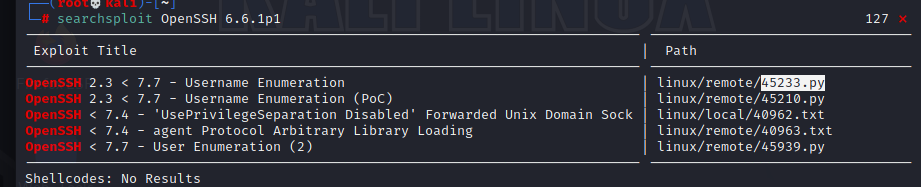
- Önce nmap taraması üzerinden elde ettiğim versiyon bilgilerine bakıyorum ve CUPS 1.7'yi kopyalıyorum.Bunun üzerinden bir sploit işlemi gerçekleştireceğim.



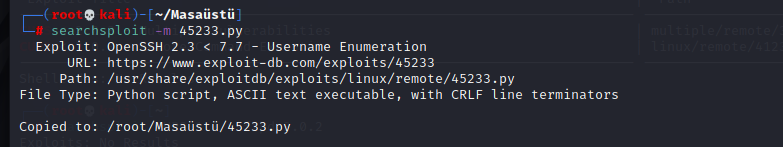
- Searcsploit kendi veritabanı üzerinden yaptığı sorgulama sonucunda bize zafiyet döndürmektedir.

-Hangi uygulama için işlem yapmak istiyorsak direk searchsploit yazılıp yanına sürüm bilgisi eklenir.

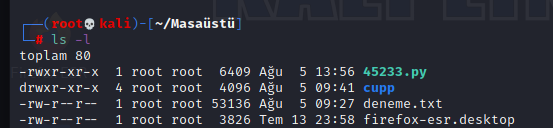
-Aynı işlemler Metasploit üzerinden de gerçekleştirilir fakat bu işlemler daha kapsamlı gerçekleşmektedir.



- OpenSSH ile ilgili bir arama gerçekleştirdim.Burada bulunan zafiyeti kullanmak istiyorum.Bunun için Path kısmında ki sadece (.py .txt) dosyalarından istediğimin adını kopyalıyorum.

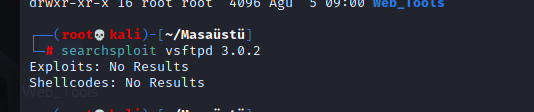


-"-m" parametresi ile istediğimiz scripti dizinimize indiriyoruz.



- İndirme işleminin ardından işlemin başarılı bir şekilde gerçekleştiğini ve yetkilerini de bu şekilde görüntüleyebiliyoruz.

-Searchploit üzerinde her zaman bilgi alıcaz diye bir şey söz konusu değildir.

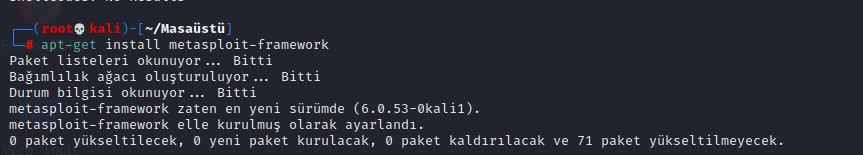


- Eğer buradan bilgi elde edemezsek tarayıcı üzerinden incelemeye devam edeceğiz.

***Metasploit Giriş***

-Metasploit aracını “Hacking,Bruteforce,Bilgi toplama” gibi işlemler için kullanıyoruz.

-Metasploit aracı Linux’un çoğu sürümünde kurulu olarak gelmektedir.

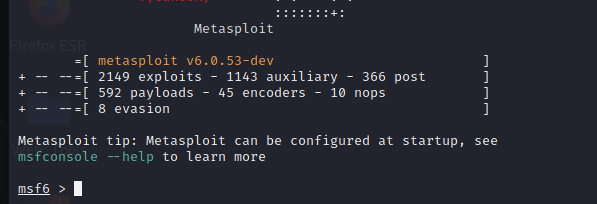


- Apt-get parametresi ile kurulum gerçekleştirebiliriz.

- Msfconsole ile Metasploit’i başlatabiliriz.

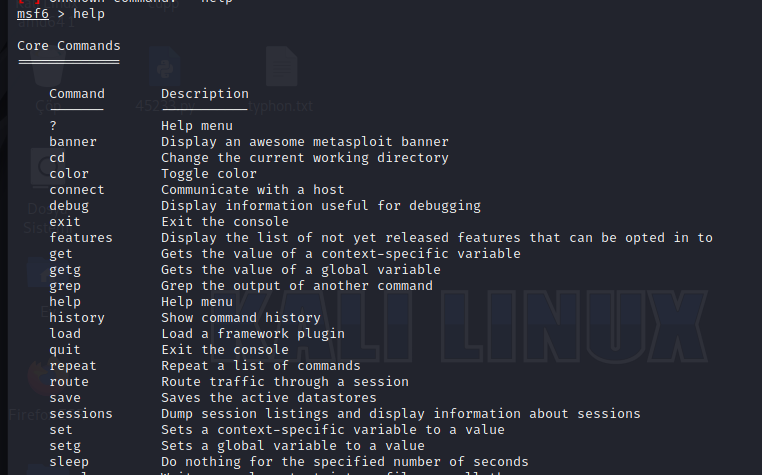


-Program başlatıldığında bu şekilde bir ekran bizi karşılar.



-İçeriğini bu şekilde görüntülüyoruz ve “-help” komutu ile bilgi sahibi olabiliriz.

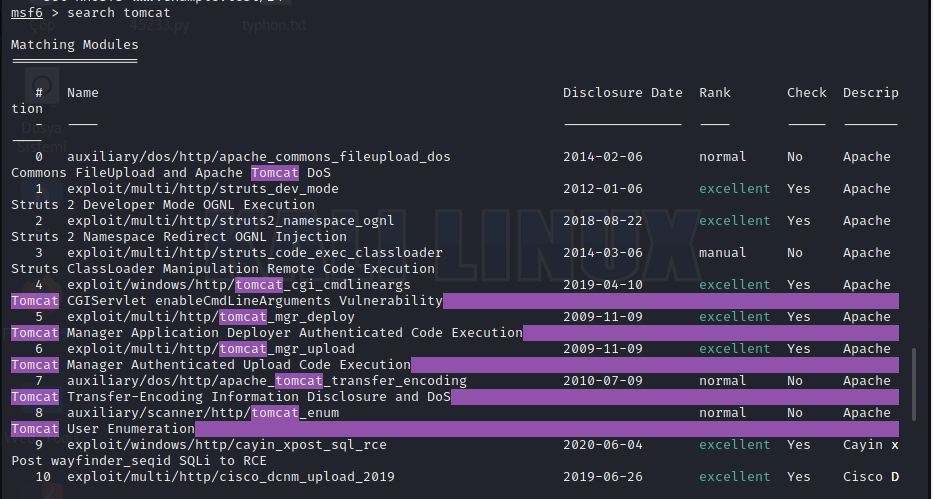
***Metasploit Komutları***



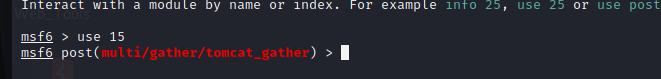
-Bu komutlara “msfconsole” üzerinden help komutu kullanılarak erişim sağlanabilir.

-Searchsploit üzerinden arama işlemi yaptığımız gibi Metasploit üzerinden de arama gerçekleştirebiliriz.

-Search komutu ile arama zafiyet bulunan yerde bir arama gerçekleştirebiliriz.

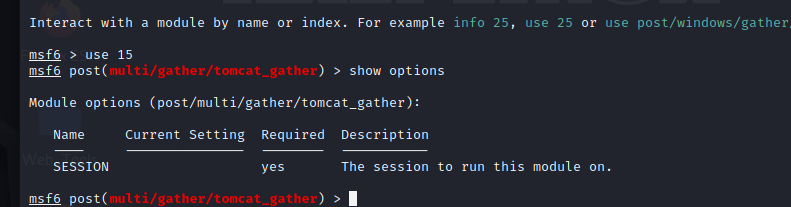


-“Tomcat” zafiyeti üzerinde bir arama gerçekleştirdiğim de hem exploit hem de post modüllerini döndürdüğünü görüntülüyoruz.



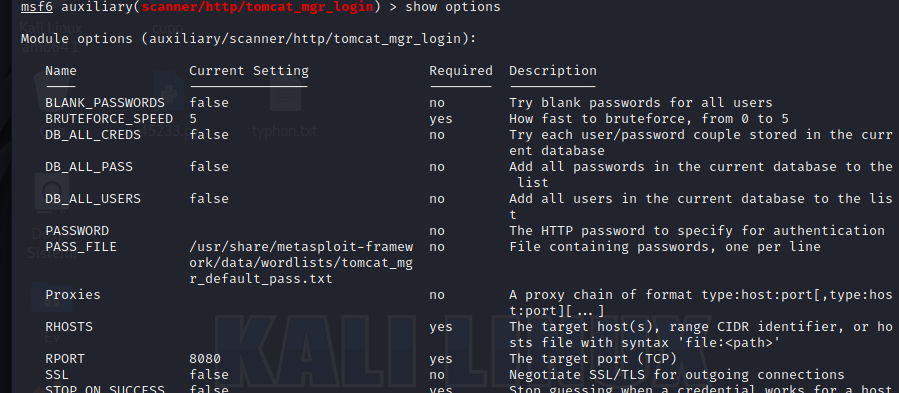
-Arama içerisinde bulunan sayıları kullanarak Scriptler hakkında bilgi sahibi olabiliriz.

-Burada dilersek dizini üzerinden de işlem başlatabiliriz.

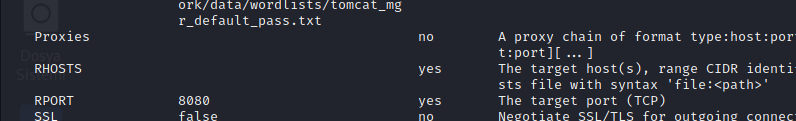


-Scripti başlattıktan sonra içerisinde istediği bilgiler ile ilgili bir dönüt görüntülüyorum.

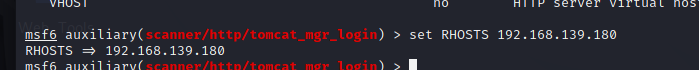
-Bu Script üzerinde çok fazla işlem olmadığı için Bruteforce için kullanılan “\_mgr\_login” Scriptini başlatıyorum.



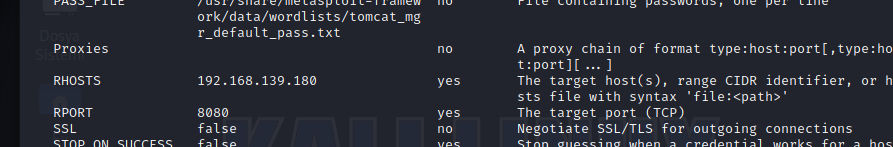
­-Required kısmında YES bulunuyorsa bizim buraya bir bilgi vermemiz gerekmektedir.



-RHOST kısmını görüntülediğimizde buraya bilgi girilmesi gerektiğini görüntülüyorum.



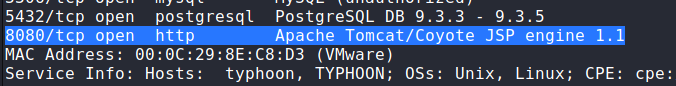
-Set ile RHOSTS kısmına “typhoon” sanalımın IP adresini set ediyorum.



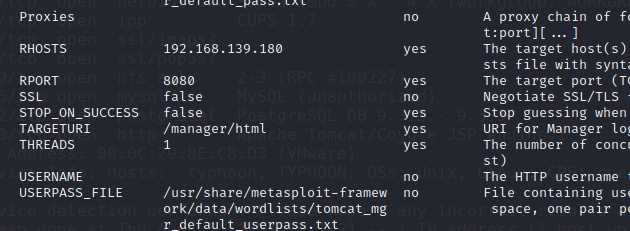
-Tekrardan show options ile baktığımda RHOST kısmına eklemiş olduğum bilgilerin geldiğini görüntülüyorum.

-Teorik olarak biraz bilgi sahibi olduktan sonra;

-Nmap taramasında kaydettiğim .txt yi açıyorum ve burada “Tomcat” hakkında bilgi topluyorum.



-Tomcat'in 8080 portunda çalıştığını görüntülüyorum.

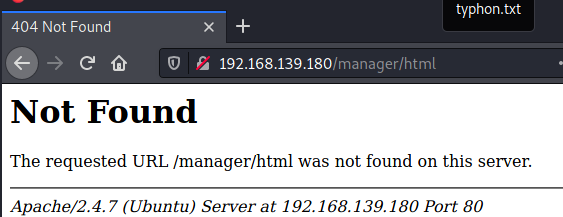


-Tekrardan Metasploit üzerine geçiş yaptığımda burada ki bilgileri inceliyorum.

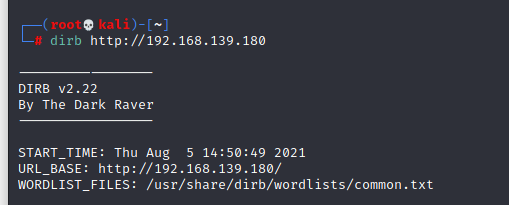
-Port değerinin doğru olduğu görüntülüyorum

-SSL ile işlem yapmayacağım için False durumunda bırakıyorum.

-TARGETURI değerini teyit etmek için tarayıcı üzerinde görüntülüyorum.

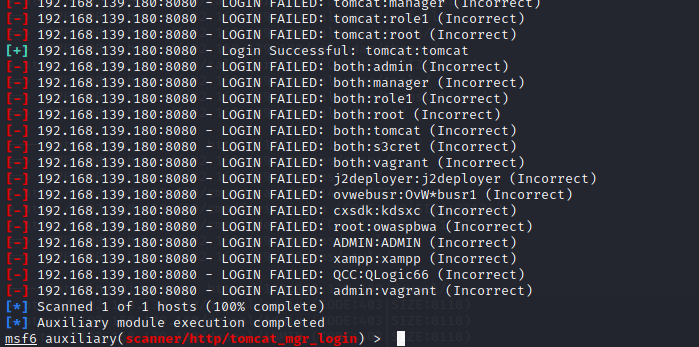


-Tarayıcı üzerinde görüntülediğim de 404 not found hatası alıyorum bu sebeple Typhoon adresini Dirb ile tarıyorum.



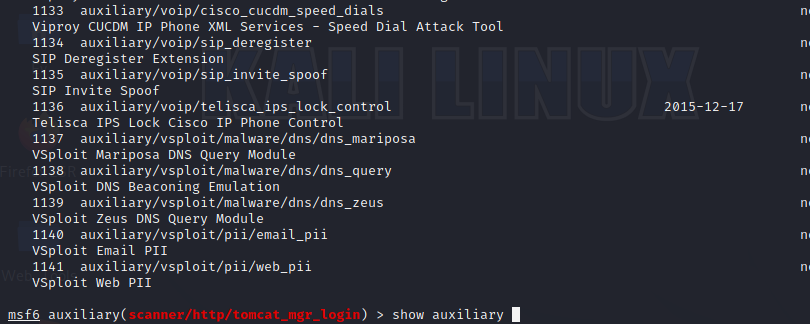
-Dirb ile işlemi başlattım.

-Arka planda bu işlem ilerlerken Metasploitimi çalıştırmak istiyorum.

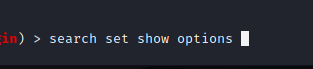


-Dönen sonuçlar bu şekildedir burada yapılan işlem TARGETURI'yi aldı.

-Burada USERFILE ve USERPASSFILE üzerinde bulunan payloadları tek tek denedi.



-"show auxiliary" ile burada kullanılabilecek scriptlerle ilgili bilgi alabiliyoruz.



-Bu komutlar bizim metasploit üzerinde en çok kullanacağımız ayarlardır.

-Verbose ile işlemleri adım adım izleyebiliriz.

-Bulduğumuz exploitlerde kullanıcını İşletim sistemine göre kullanım göstereceğiz.

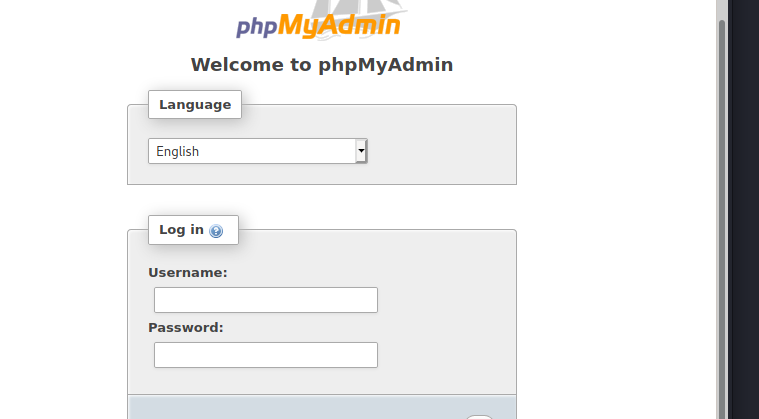
-Dirb araması ile de dizin taraması gerçekleştirip dizinler hakkında bilgi sahibi olabiliriz.

***Metasploit Auxliary Modülü Kullanımı***

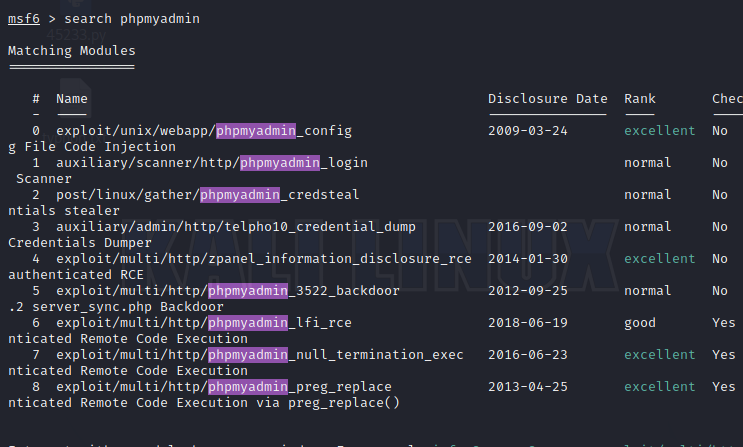
-Bu uygulamamızda Auxiliary üzerinden Brute Force işlemi hakkında çalışma gerçekleştireceğiz.

-Linux makineme geçiş yapıyorum ve burada msfconsole'u başlatıyorum.

-Dizin tarama işlemi sonucunda “typhoon” üzerinde bir giriş ekranı bulmuştuk.(/phpmyadmin)Bu dizin üzerinden işlem gerçekleştireceğim.

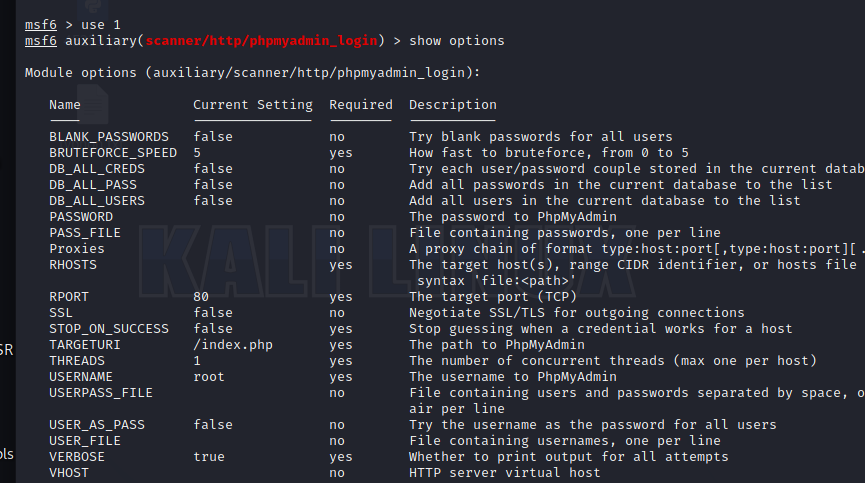


-“/phpmyadmin” URL'sini tarayıcı üzerinde görüntülediğimde böyle bir ekranla karşılaşıyorum.

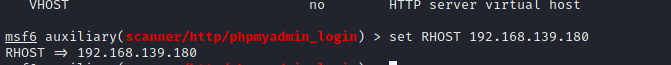


-Ardından Metasploit aracıma geçiyorum ve burada” search phpmyadmin” aramasını gerçekleştiriyorum

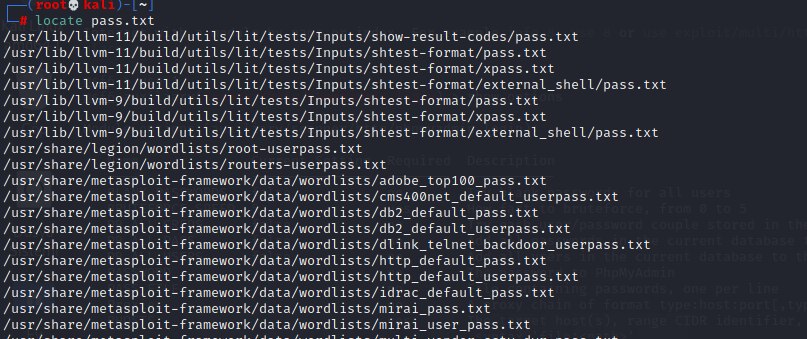
-Kullanabileceğim scriptler hakkında bilgi sahibi oluyorum.



-“phpmyadmin\_login" ile devam ediyorum.Burada show options diyip ayarları görüntülüyorum.

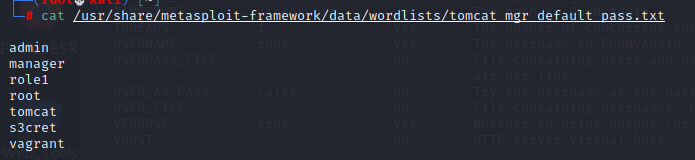


-Önce atak gerçekleştireceğim adresi “MS” üzerine set ediyorum.



-Ayarlar kısmından gerekli olan bilgilere baktığımda “pass\_list” set etmem gerekli burada diğer araçlar gibi liste bulunmadığı için;

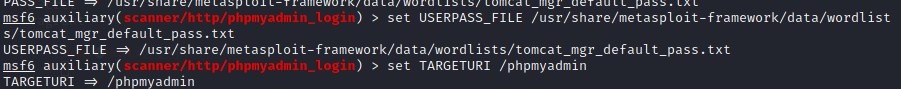
-Linux içerisinde hazır bulunan Listler ile işlem gerçekleştireceğim.



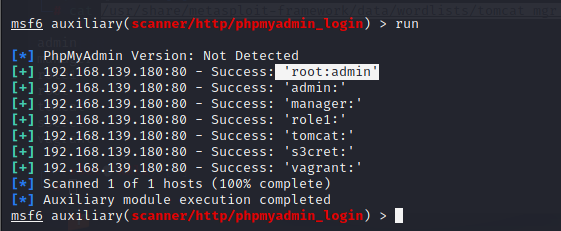
-Linux içerisinde hazır bulunan “Tomcat “ listi ile devam edeceğim içeriği bu şekildedir.



-PASS\_FİLE a kullanacağım txt dosyasını set ediyorum.

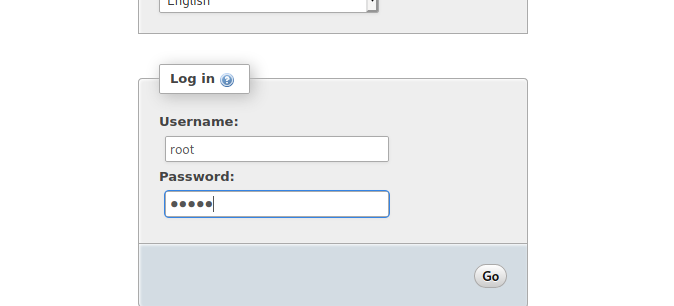


-Aynı txt dosyasını USERPASS içinde kullanıyorum ayrıca TARGETURI’yi kontrol ettiğimde yanlış olduğunu görüntülüyorum bunu da “/phpmyadmin” olarak set ediyorum.

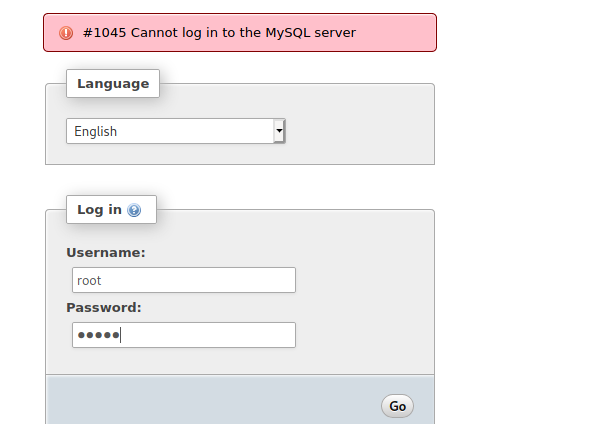


-Gerekli ayarları yaptıktan sonra işlemimi RUN veya EXPLOİT ile başlatıyorum.İşlem bittiğin de tarafıma denemiş olduğu Scriptlerin sonucunu bu şekilde aktardı.

-Burada kullanıcı adı ve şifre bölümünü “root-admin” şeklinde olduğunu görüntüledim

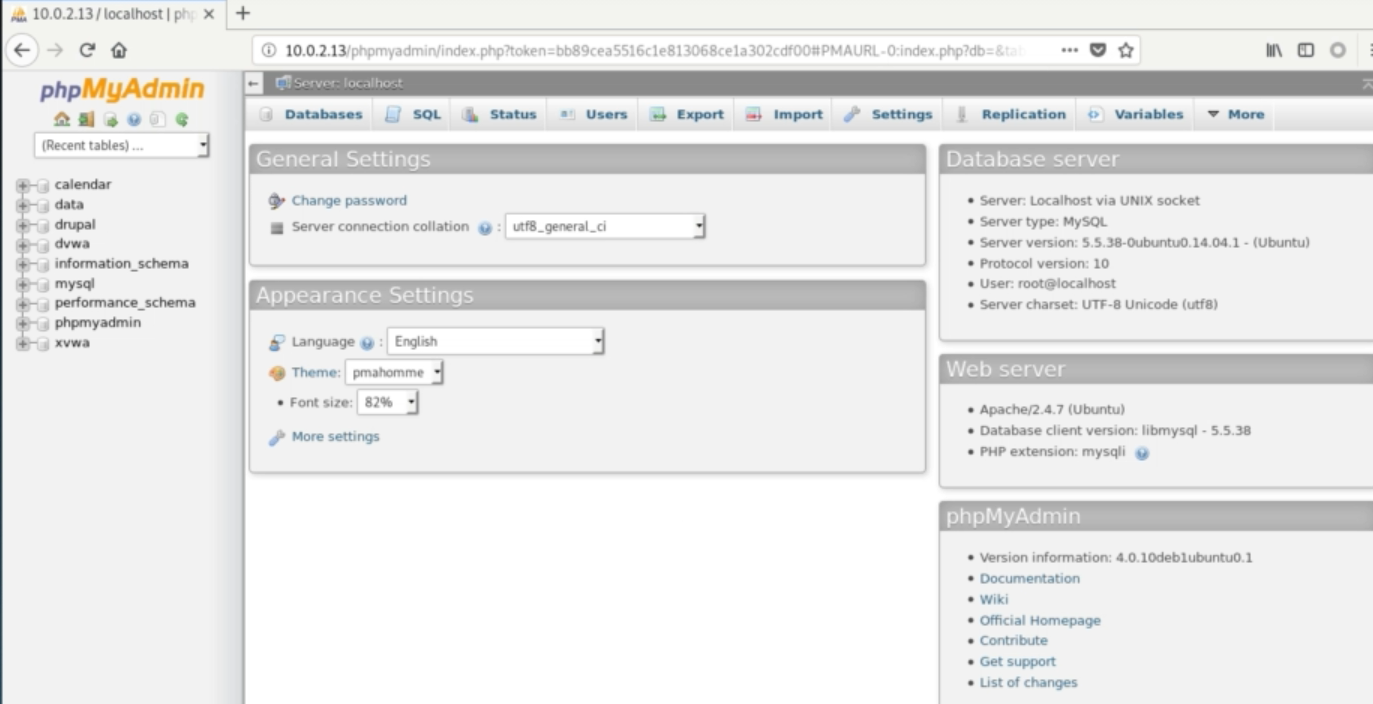


-Tarayıcıya geçiş yapıyorum ve burada bulmuş olduğum kullanıcı adı ve şifreyi deniyorum.



-Girilen bilgiler doğru olmasına rağmen sisteme giriş yapamadım bu yüzden işlemi Verbose ayarını açıp bir daha başlatacağım.

-Bu sayede nerede hata aldığımı görüntüleyeceğim.



-Linuxtan kaynaklı bir hata olduğunu görüntüledim.Bu sebeple birkaç kere daha bu işlemi denedim ve sisteme giriş yapabildim.

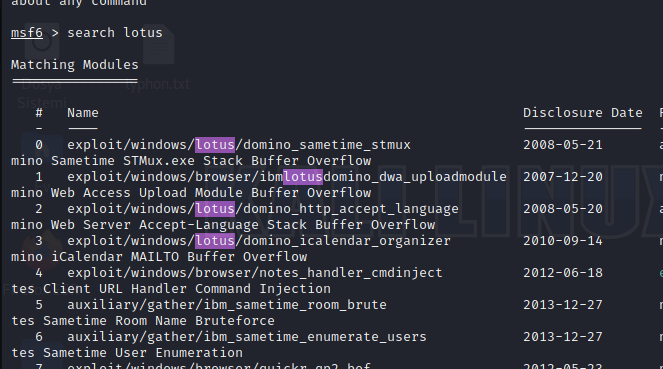
-Kullanıcı adı ve şifreyi Bruteforce saldırısı ile başarılı bir şekilde bulabildim.

***Metasploit Exploit-Payload Modülleri***

-Exploit ve Metasploit Payload modülleri ile kullanılır.

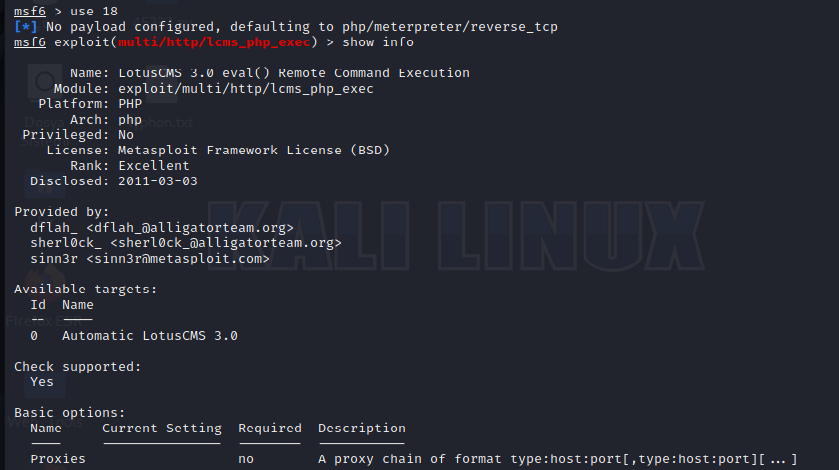
-Exploit tetikler payload ise terminal erişimi kurmamızı sağlar.

-Linux makinemde uçbirimi açıyorum ve burada msfconsole ile Metasploiti başlatıyorum.



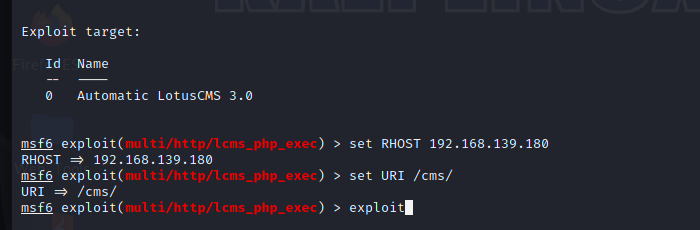
-MS üzerinde Search komutu ile php zafiyeti olan lotus u açarak başlıyorum.

-Bu zafiyeti dirb aracı ile tespit etmiştik.



-Burada php.exec scripti ile işlemlerime devam edeceğim.

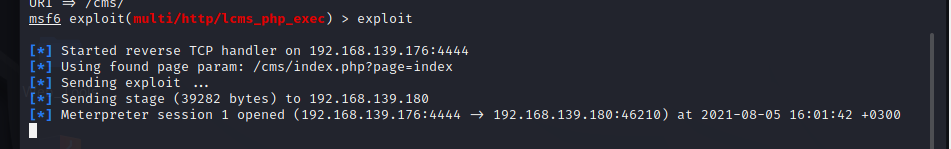
-Php.exec üzerinde showinfo komutu ile devam edersem burada bu script hakkında bilgi edinebiliriz.



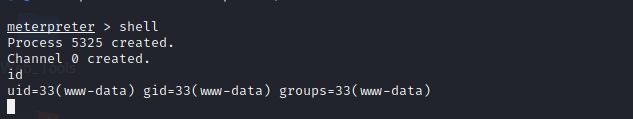
-Show options seçeneği ile devam ediyorum ve burada önce RHOST'umu set ediyorum.

-Ardından URI kısmına /cms/ 'yi set ediyorum

-Set etme işlemlerinin ardından Exploit ile işlemi başlatıyorum.

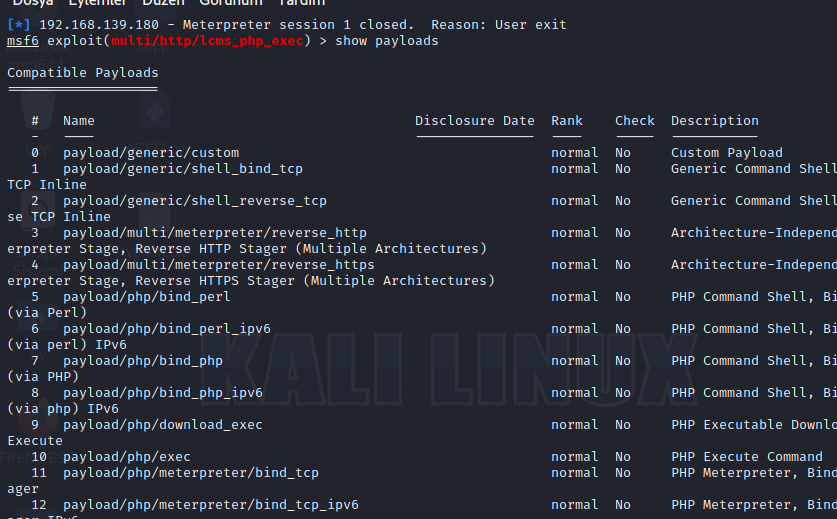


-Sonuçlara baktığımda tamda görmek istediğim gibi "Meterpreter session 1 opened" dönüşünü alıyorum.Meterpreter bana bir Shell kapısı oluşturacaktır.



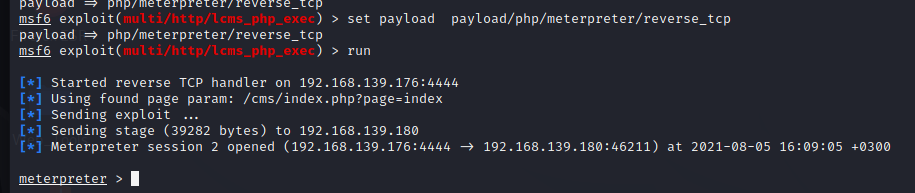
-İlerleyen uygulamalarda Meterpreter hakkında bilgi vereceğim ama en azından şuanlık görmenizi istedim.

-Burada “Shell” komutu ile yetkileri alıyorum ve artık istediğim komutu kullanabilirim.



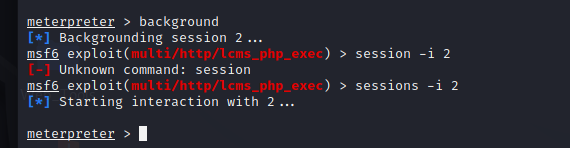
-Show Payloads ile payloadlara erişim sağlıyorum.Bu zafiyet için kullanılan payloadlar bunlardır.

-Buradan herhangi bir payload’ı seçiyorum.



-“Reverse\_tcp” payloadını seçtim bunu “set payload” ile set edip çalıştırıyorum.

-Meterpreter bağlantısını tekrardan kurduğumu görüntülüyorum.



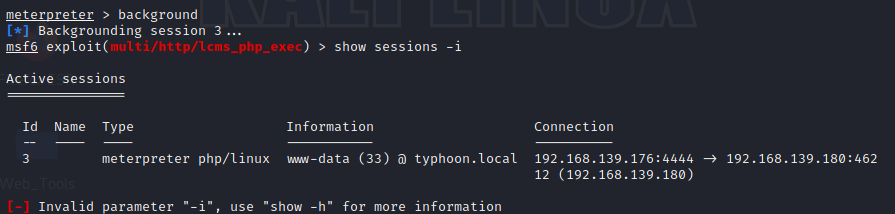
-Background komutu ile meterpreter'i arka plana alabildim ve sessions -i 2(sessions değeri) ile tekrardan dönüş yapabildim.

-Eğer background alınmazsa geri dönüş yapılamaz.

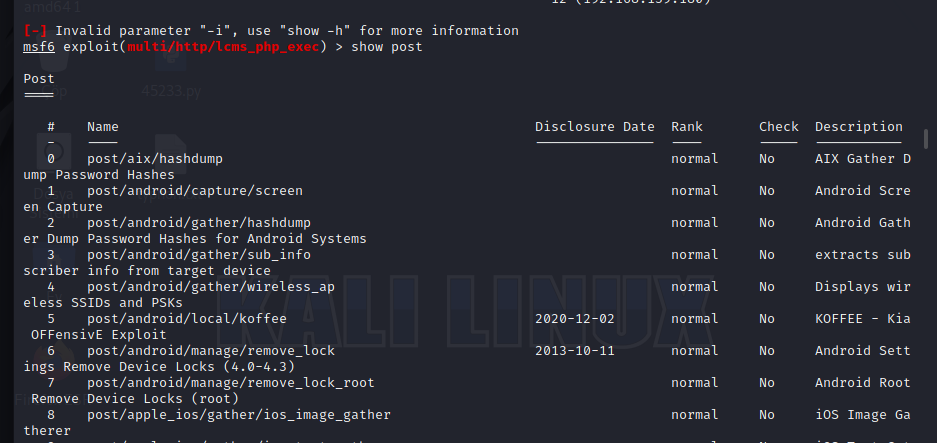
***Metasploit Post Modülleri***

-Post modülü için öncelikle önceki uygulamamdan devam ediyorum.

-Meterpreter içerisinde bir background alıyorum.

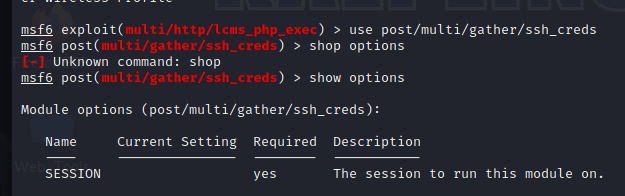


-"show sessions -i" komutu ile arka planda çalışan işlemleri görüntülüyorum.



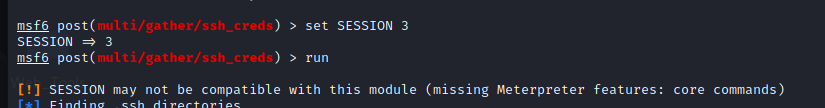
-Ardından "show post" ile ediyorum.Burada kullanabileceğim post modüllerini görüntülüyorum.

-Typhoon aracımın Linux işletim sistemini kullandığını biliyorum bunun için Linux işletim sisteminde kullanabileceğim modülleri arıyorum.



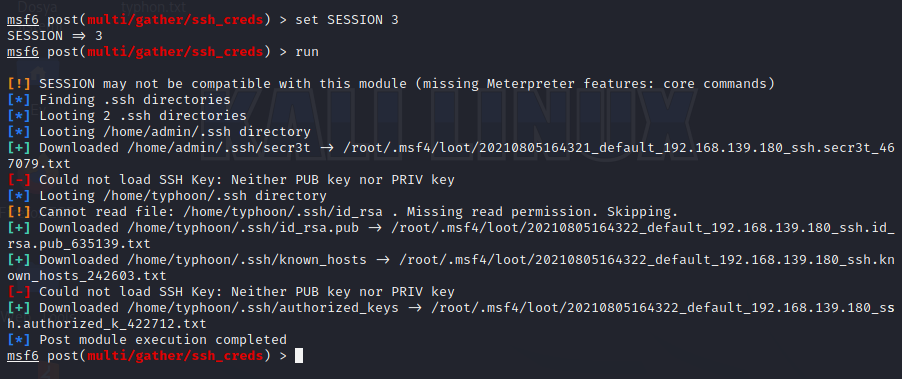
-"ssh\_creds" modülünü çalıştırdıktan sonra Show\_options bölümü ile istediği ayarları görüntülüyorum.

-Burada modül benden bir “Session” istemektedir.



-Background aldığım Session’umun ID numarası 3 bunu set ediyorum.

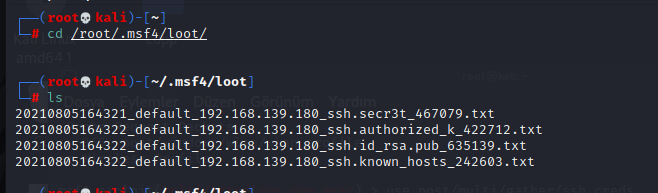
-Ardından işlemimi run komutu ile başlatıyorum.



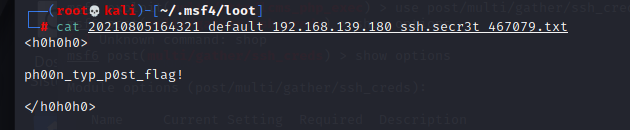
-Post sonuçlarını bu şekilde görüntülüyorum.

- “/home/admin/.ssh/secr3t” dizininde ki dosyayı kendi cihazıma indirdiğimi ve Erişim keylerini de aynı şekilde kaydettiğini görüntülüyorum.

-İndirdiği dizini kopyalıyoruz ve cd komutu ile geçiş yapıyorum.



-Dizine geçiş yaptığımda burada sunucudan indirmiş olduğu .txt uzantılı dosyaları görüntüleyebiliyorum.



-Secret içeriğine baktığımda bir bayrak değeri döndürdüğünü görüntülüyorum.

-Bunun sebebi bunun CTF içinde kullanılıyor olmasıdır.