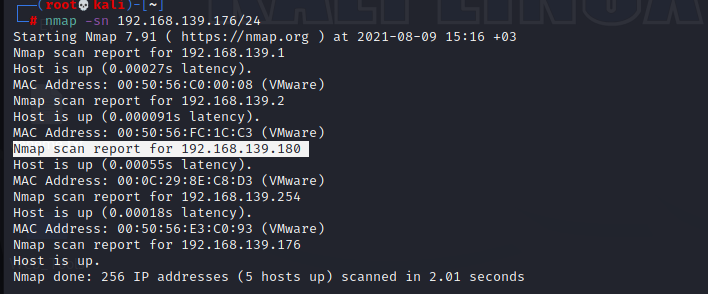
|  |
| --- |
| ***Typhoon*** |
| Kaan Efe Öğüt  *ADLİ BİLİŞİM MÜHENDİSLİĞİ* |
| -Nmap uygulamasında kullandığımız Typhoon zafiyetli makinesi üzerinden exploit kullanımı ve yetki yükselme işlemlerini birlikte yapacağız. |

***LOTUSCMS Exploit ve Yetki Yükseltme***

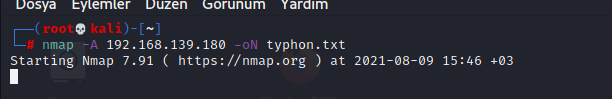
**10.08.2021**

-Daha öncesinde Typhoon makinesinin kurulumu hakkında bilgi vermiştik.

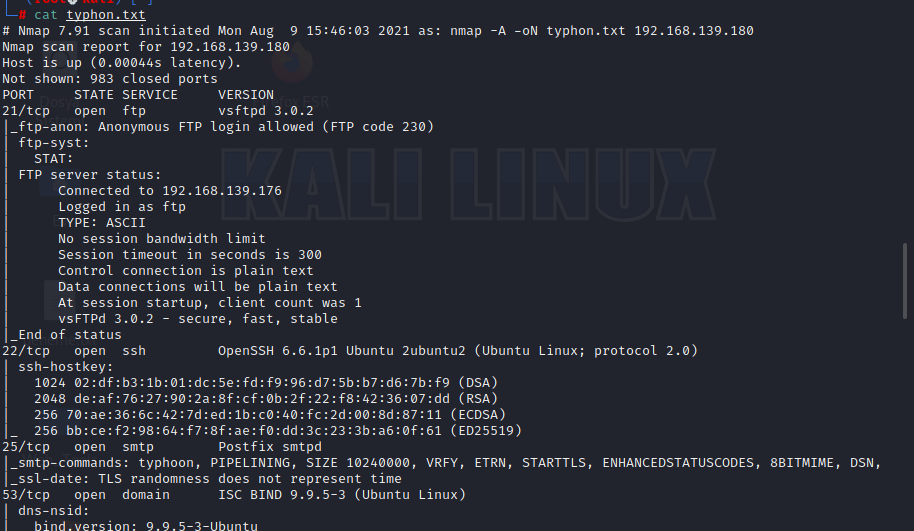
-Typhoon makinesinde bulunan zafiyetleri daha önce hiç görmedik.Bu sebeple bunu da çözmek istiyorum.



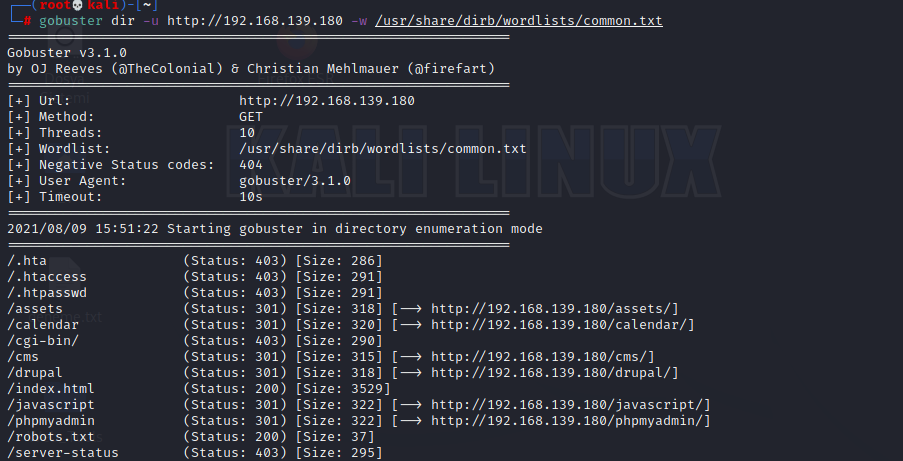
- Öncelikle typhoon makinemin IP adresini Nmap komutu ile buluyorum.



-Nmap ile Detaylı bir tarama başlatıyorum ve bunu da ” typhon.txt” olarak kayıt ediyorum.

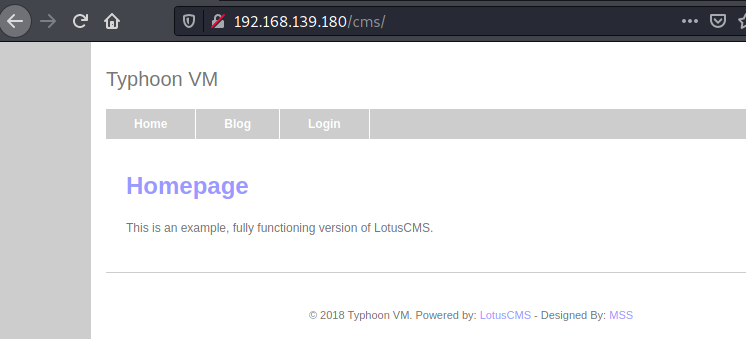


-Cat komutu ile “txt” dosyasını görüntülediğim de burada açıkları görüntüleyebiliyorum.



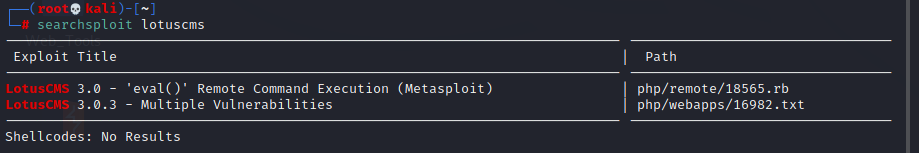
-Dirb aracına göre Gobuster daha hızlı olduğu için Gobuster ile bir tarama gerçekleştiriyorum.

-Burada açık olabilecek URL'leri görüntüleyebiliyorum.Bunların hepsine bakacağım.

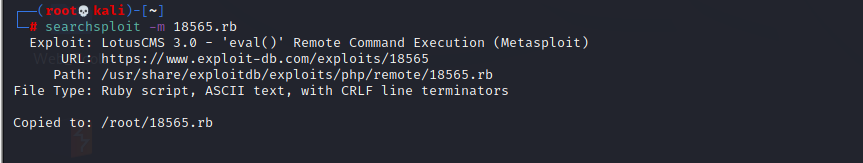


- CMS ile devam ediyorum burada sitenin görünümü bu şekildedir.

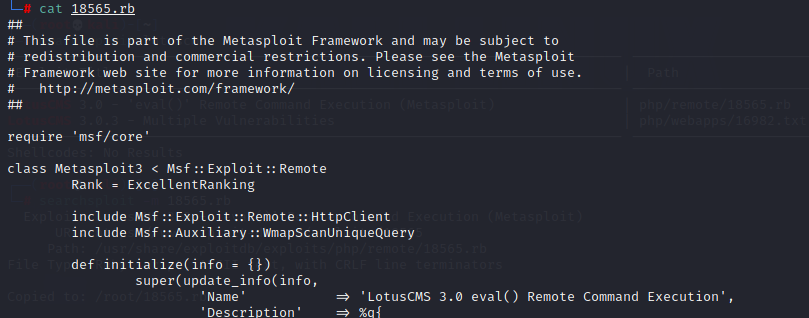
-Kaynak kodu üzerinden versiyon bilgisini öğrenmeye çalışıyorum fakat herhangi bir bilgiye rastlayamadım.



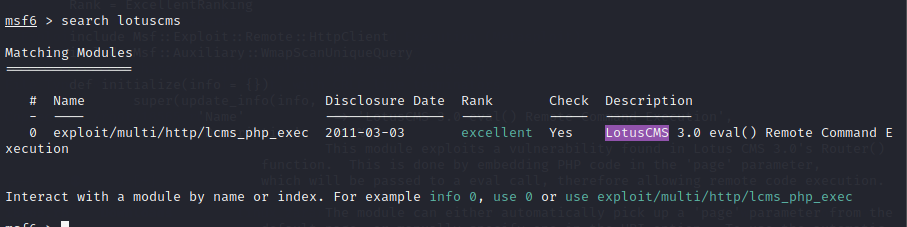
-Bu sebeple uçbirim üzerinde Searchsploit ile "lotuscms" üzerinde bir arama gerçekleştiriyorum.



-”rb” uzantılı Script’i indiriyorum ardından “cat” komutu ile görüntüleyeceğim.

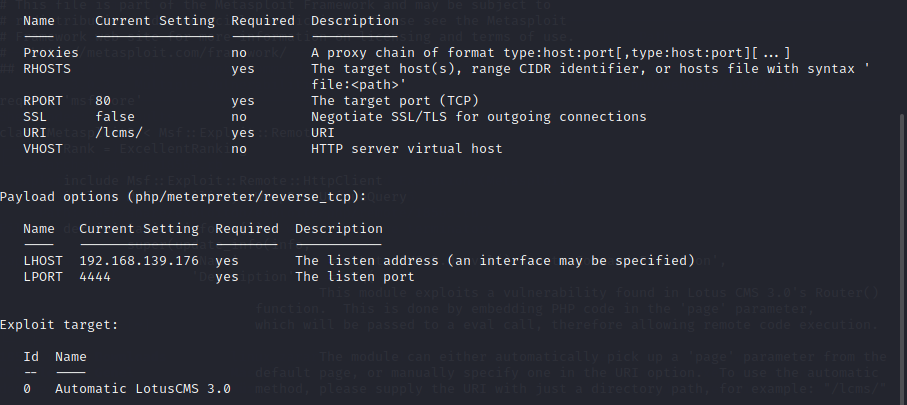


-Ayrıntılarına baktığımda “MS” için oluşturulduğunu görüntülüyorum Bu sebeple “msfconsole” komutu ile Metasploiti başlatıyorum.

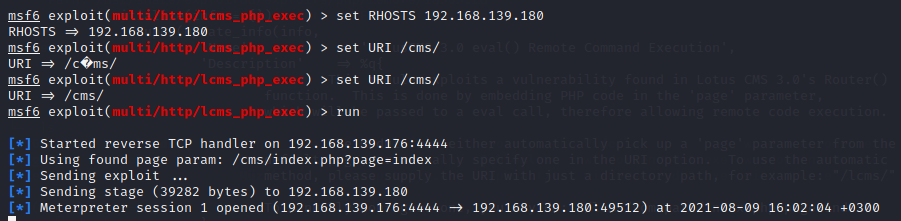


-Metasploit aracımı çalıştırıyorum burada exploit denemesi gerçekleştireceğim.

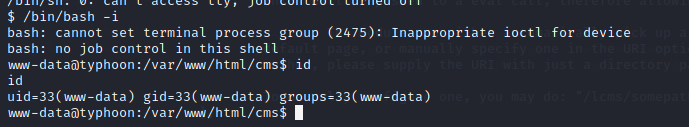
-"search lotuscms" komutu ile Exploit araması gerçekleştiriyorum.



-“Show options” ile görüntülediğim de burada gerekli bilgileri görüntülüyorum.

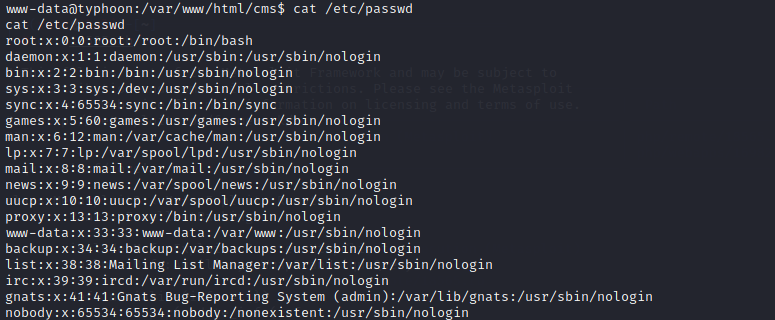


-Gerekli bilgileri set ettikten sonra işlemi başlatıyorum ve burada “Meterpreter” üzerinde bir açık elde ediyorum.

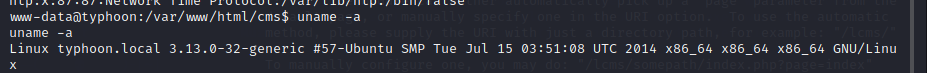


-Konsol üzerinde şuanda erişimi sağladım fakat şuan erişim sağladığım kullanıcı yetkili bir kullanıcı değil.(Burada ki sayıdan anlıyoruz)

-Bu sebeple bir yetki yükseltme işlemi gerçekleştirmeye çalışacağım.



-"cat /etc/passwd" komutu ile sistemde ki kullanıcıları görüntüleyebildim.



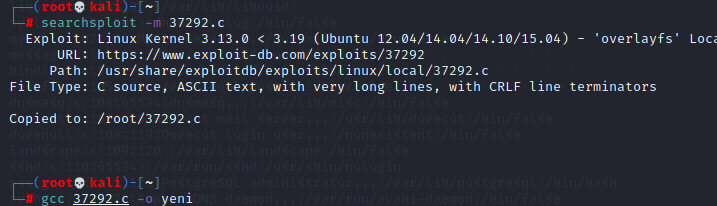
-"uname -a" komutu ile Linux sürümünü öğreniyorum.

-Bu Linux sürümü üzerinde bir zafiyet var mı bunu görüntüleyeceğim.



-Searchsploit üzerinde bir arama gerçekleştiriyorum.

-3.13 sürümü için bulduğu açık (C) dilinde yazılmış bir kod dizinidir.

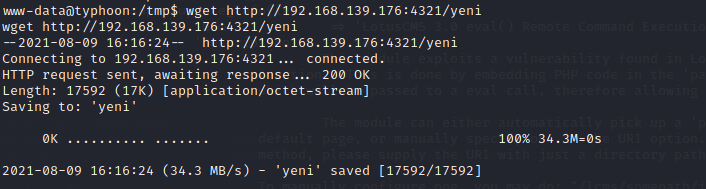


-Kodu indirme işlemini gerçekleştiriyorum ve ardından ismini değiştirip derliyorum.

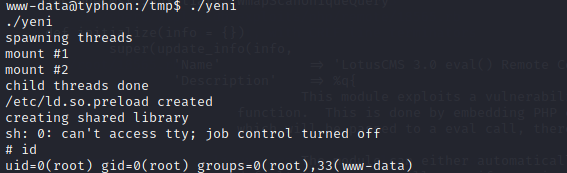
-Şimdi yapacağım işlem ise sunucunun “tmp” dosyalarının içerisine; indirdiğim exploit dosyasını aktarmak olacaktır.



-Python komutundan yararlanarak HTTP server'ı başlatıyorum ve sunucu üzerine indirme işlemi gerçekleştireceğim.



-Sunucuya indirme işlemini başarılı bir şekilde gerçekleştirdim.



-Yeni dosyasına "chmod +x yeni" komutu ile yetki veriyorum ve ardında çalıştırma işlemini gerçekleştiriyorum.

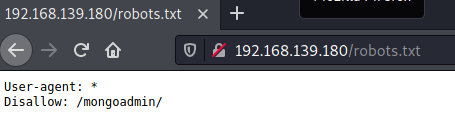
-Exploiti çalıştırdıktan sonra id ile kullanıcıma baktığımda Root olduğumu görüntülüyorum.

-Başarılı bir şekilde yetkiyi ele alabildim.

***Robots.txt & Mongoadmin Üzerinden Bilgi Çekme***

-Root yetkisi alma işlemini önceki uygulamamızda başarılı bir şekilde uygulamıştık.

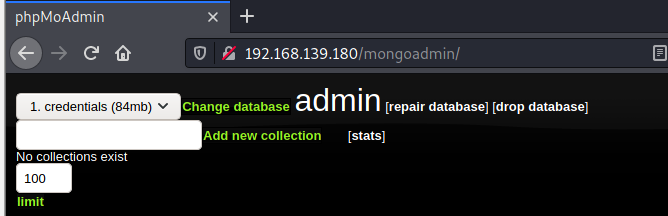
-Şimdi ise “Gobuster” uygulaması üzerinden yaptığımız taramada Robots.txt ve Mongoadmin kısmı dikkatimizi çekmişti.Buradan bir bilgi ifşası yapmayı deneyeceğiz.



- Öncelikle "/robots.txt" sayfasını görüntülüyorum.Burada karşıma “mongoadmin” dosyası çıkıyor.

-Burada “Google” tarafından indexlenmesini istediğini fakat indexlenmediğini görüntülüyorum.

-Buradan bir bilgi zafiyeti yapabilirim.



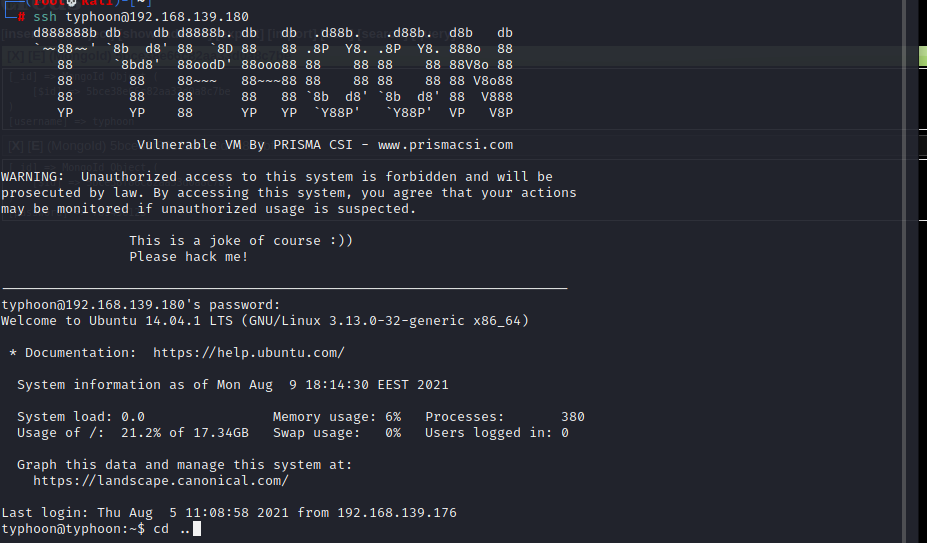
- Önce mongoadmin sayfasını görüntülüyorum.

-Sayfa üzerinde ki stats bölümünden bir bilgi edinebileceğimi düşünüyorum.



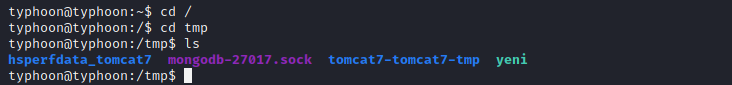
- Daha sonrasında karşıma çıkan sayfada bir kullanıcı adı ve şifre parametresi beni karşılıyor.

-Sunucuya bir “SSH” bağlantısı kurarak bir işlem gerçekleştirebileceğimizi düşünüyorum.



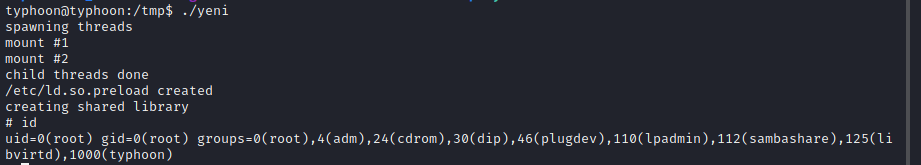
- SSH bağlantısını başarılı bir şekilde kurdum.

-Artık sunucu üzerinde istediğimi yapabilirim fakat burada da önceki uygulamamızda olduğu gibi bir yetki yükseltme işlemi gerçekleştirmek istiyorum.



- Bir önceki uygulamamda bir “Sploit” eklemiştim ve burada görüntüleniyor.

-Başka bir sunucu üzerinde bir işlem gerçekleştirmiş olsaydık.Burada bu dosya bulunmayacaktı.Bu sebeple bir önceki uygulamamızda olduğu gibi tekrardan bir indirme işlemi gerçekleştirecektik.

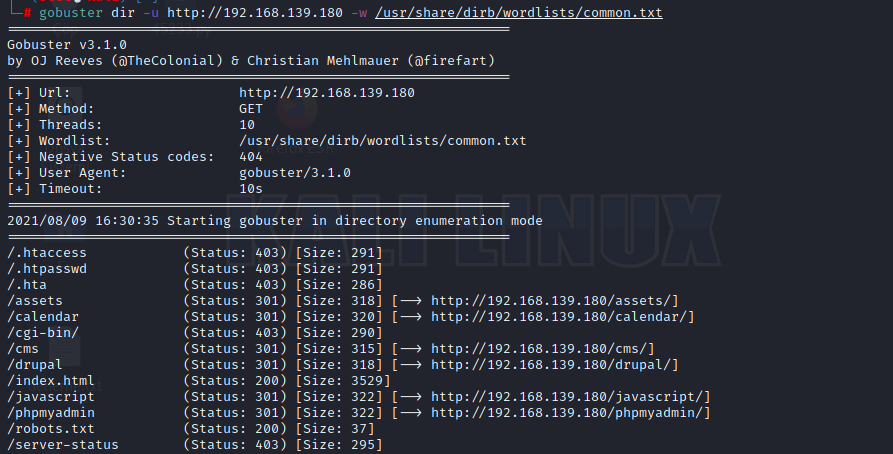


- "yeni" dosyasını çalıştırdığımda “root” olma işlemini tekrardan başarılı bir şekilde gerçekleştirdim.

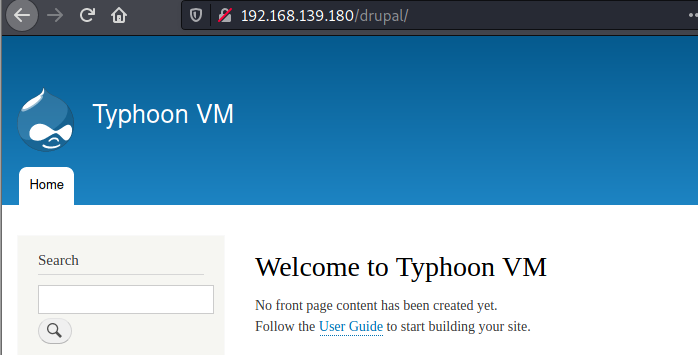
***Drupal Exploit ve Yetki Yükseltme***

- Lotuscms üzerinde gerçekleştirdiğimiz zafiyeti bu sefer Drupal üzerinde gerçekleştirip yetki yükseltme işlemini gerçekleştireceğiz.

-Drupal dizininde ki zafiyeti tekrardan görüntüleyelim.

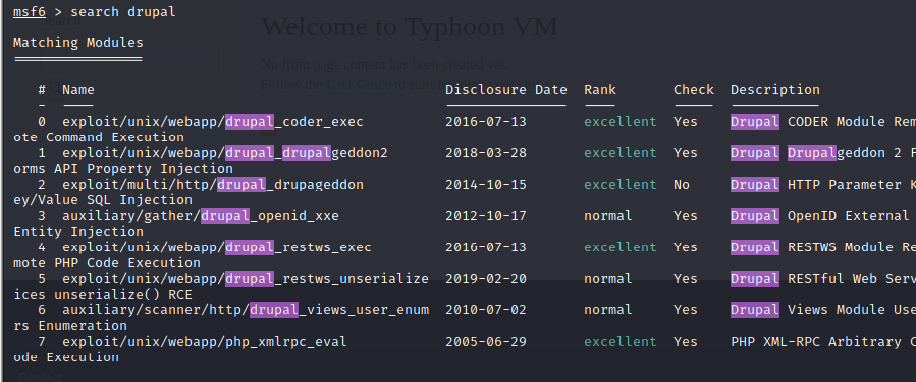


- Gobuster aracı ile dizin taraması gerçekleştiriyorum ve burada açığı görüntülüyorum.



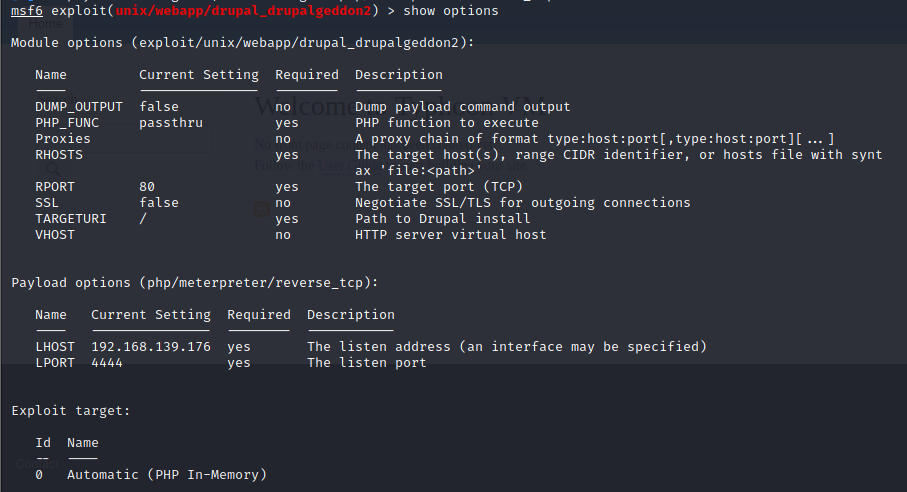
- Drupal uzantısını network üzerinde bu şekilde görüntüleyebiliyorum.

-Drupal'in versiyonu hakkında bir bilgi bulamıyorum.

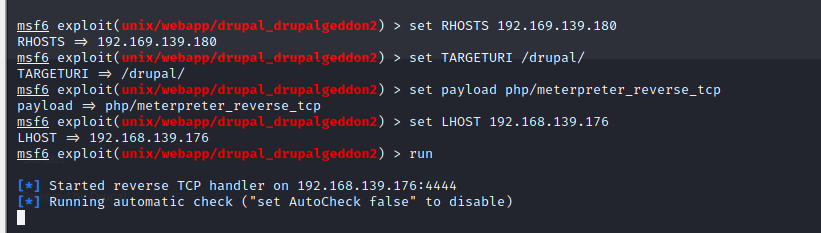


- Msfconsole ile Metasploit'i başlatıyorum.Burada bir Drupal için sploit arama işlemi gerçekleştireceğim.

-Sploit arama işlemini tamamladığım da 7 adet Sploit görüntülüyorum içlerinden "drupal geddon2" ile işlemi gerçekleştireceğim.

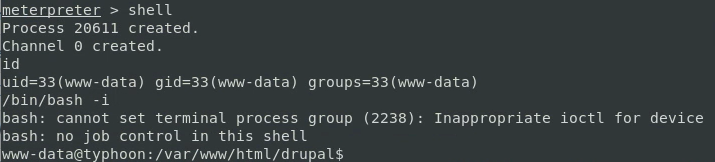


- “Show options” seçeneği ile istediği bilgileri görüntülüyorum.İçerisine sadece bir RHOST bilgisi vermem yeterli olacaktır.

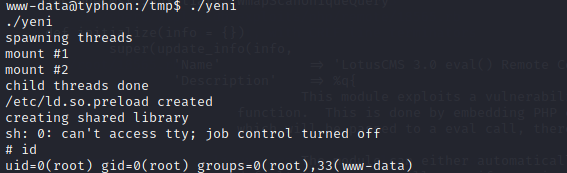


- Gerekli bilgileri set ettikten sonra işlemi başlatıyorum.

-Daha sonrasında bir Meterpreter açığı görüntülüyorum ve işlemlerime devam ediyorum.



- Shell bağlantısı kuruyorum ve burada tekrardan bir yetki yükseltme işlemi gerçekleştireceğim.



- Daha önceden sunucu üzerine indirdiğim "yeni" isimli dosyayı çalıştırıyorum ve root yetkilerini elde ediyorum.