|  |
| --- |
| ***EXPLOITATION*** |
| Kaan Efe Öğüt  *ADLİ BİLİŞİM MÜHENDİSLİĞİ* |
| -Penetrasyon aşamalarından biri olan Exploitation aşamasında yetkilerimizi yükseltecek açıklar bulmaya çalışacağım..Burada manuel işlemler gerçekleştireceğim gibi LinuxSuggester gibi otomatik araçlardan da yararlanacağım. |

**27.12.2021**

***EXPLOITATION***

-Şimdiye kadar hedefin uzağındaydık artık hedefin içinde olduğumuz için artık Local üzerinde işlem gerçekleştireceğiz.

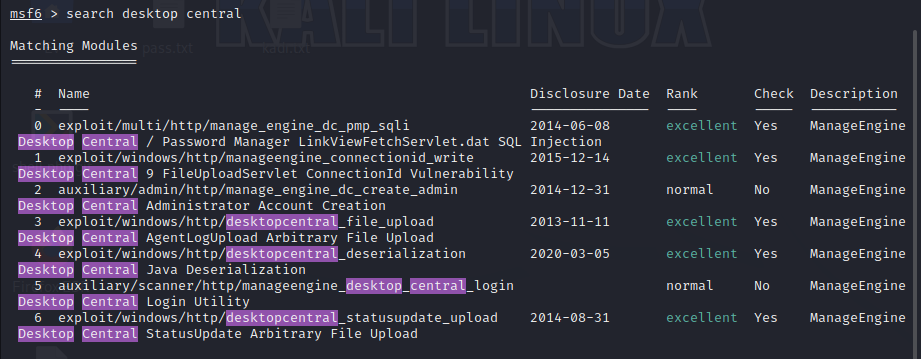
-Yetki yükseltme sadece burada bir daldır.

-Burada oldukça fazla açık bulunmaktadır.Bu açıkları da CTF çöze çöze göreceğiz.

***Windowsta Local Exploit Tespiti***

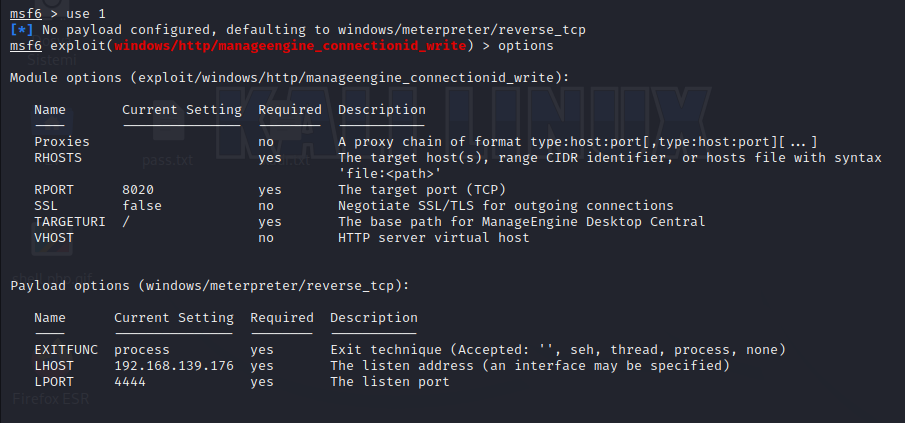


- Burada işlem gerçekleştirmek için Metasploit aracından yararlanacağım bu sebeple "Msfconsole" komutu ile Metasploit aracını başlatıyorum.



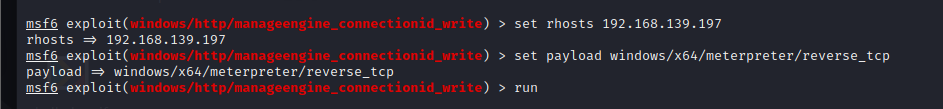
-Ardından "desktop central" üzerine bir arama gerçekleştiriyorum.

-Burada karşıma çıkan "connectionid write" scriptinden yararlanacağım.

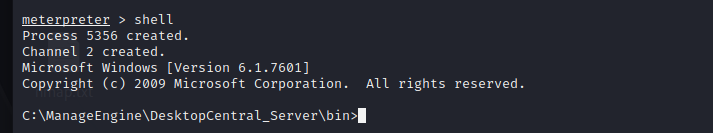


- Ardından kullandığım script içerisinde gerekli olan ayarları görüntülüyorum.

-Burada kullanacağımız Payload çok önemlidir.



- Gerekli ayarları set ediyorum ve işlemi başlatıyorum.



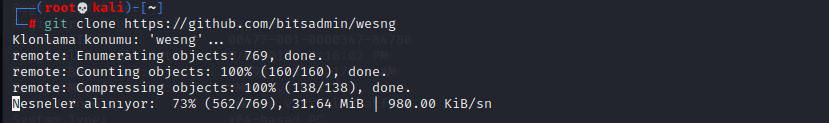
-Ardından başarılı bir şekilde shell bağlantısı kurabildim.



- "bin>cd c:\\" komutu ile C dizini üzerinde komut kullanabilir hale geldim.

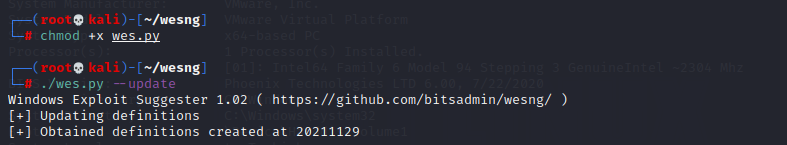
-Ardından "systeminfo" komutu ile system hakkında bilgi topluyorum.

-Burada yüklenen güvenlik yamalarını görüntüleyebilirim.



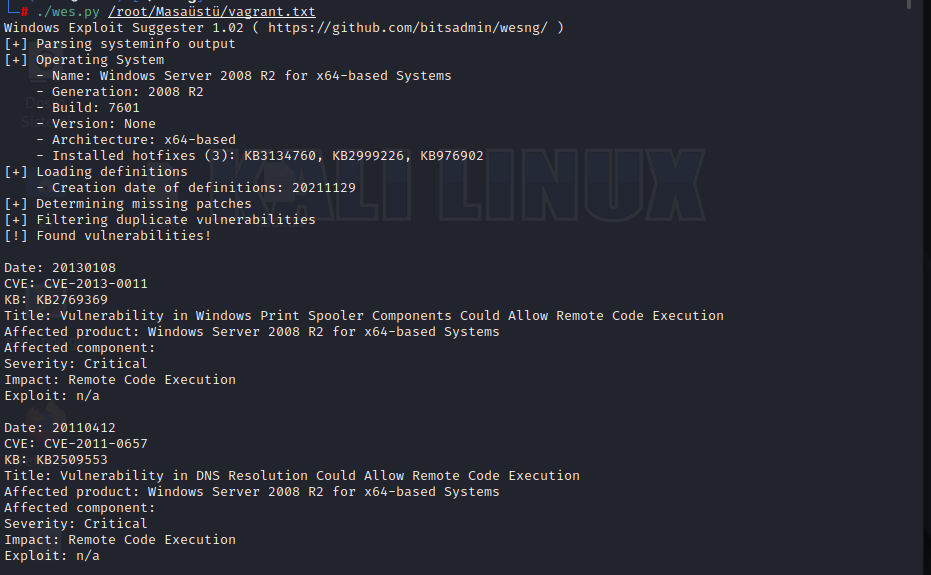
-Bu işlemi bizim için yapan Suggester'lar vardır.

-Github üzerinde bu suggesterlardan birini yüklüyorum.Bağlantı adresi "https://github.com/bitsadmin/wesng" ‘dir.



Ardından indirdiğim klasöre geçiş yapıyorum ve burada öncelikle çalışma izni veriyorum.

-Çalıştırma öncesinde Update işlemini de sağlıyorum.



- Araç artık çalışır duruma gelmiş bulunmaktadır.

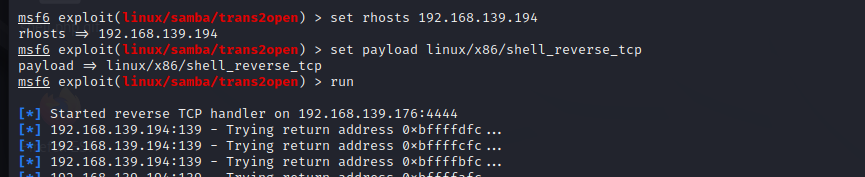
-Systeminfo komutu ile aldığım çıktıyı bir .txt dosyasına yazıyorum ve bu dosya üzerinden tarama başlatıyorum.

-Bulduğu açıkları tarafıma bu şekilde aktarmaktadır.

-Karşıma burada exploit.db üzerinde bulduğu scriptleri karşıma aktarıyor.

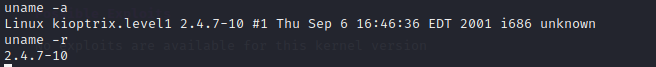
***Linux’ta Local(Kernel) Exploit Tespiti***

-Az önce yaptığımız işlemi Linux işletim sistemli bir yapı üzerinde deniyorum.

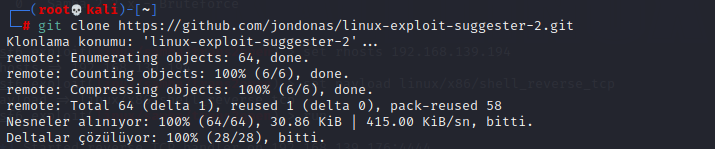


- Bu işlem için yine metasploit aracını kullanıyorum.

-"linux/samba/trans2open" scriptini kullanarak bir shell almaya çalışıyorum.



- Burada "uname -a","uname -r" komutları ile bilgi toplamaya çalışıyorum ve çekirdek bilgisine erişim sağladım.



- İşlemleri otomatize etmeye odaklandığım için burada da "Linux exploit suggester" aracından yararlanacağım.

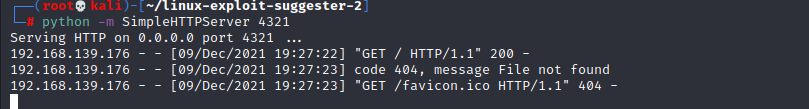
-"https://github.com/jondonas/linux-exploit-suggester-2.git" bağlantısında bulunan aracı indiriyorum.



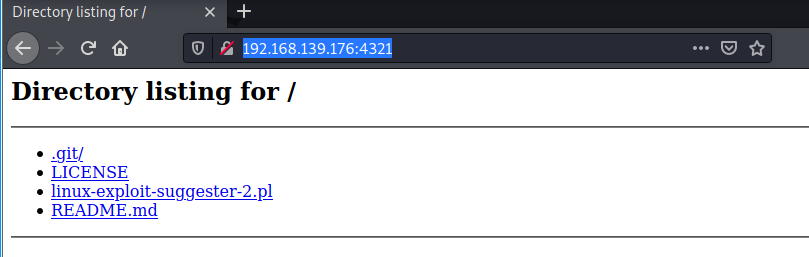
- Çekirdek sürümü üzerinden arama gerçekleştirdiğim de 3 adet açık bulmaktadır.

-Ayrıca bu dosyayı sızdığım sistem içerisine gönderip işlem gerçekleştirebiliriz.

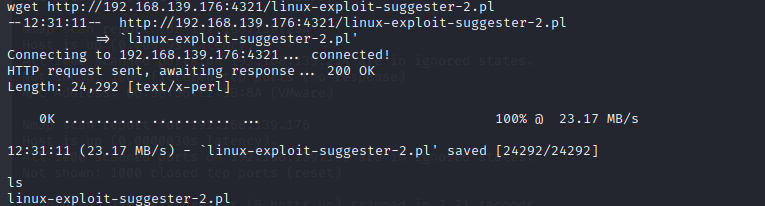
***Linux’a Dosya Çekerek Kernel Exploit Tespiti***



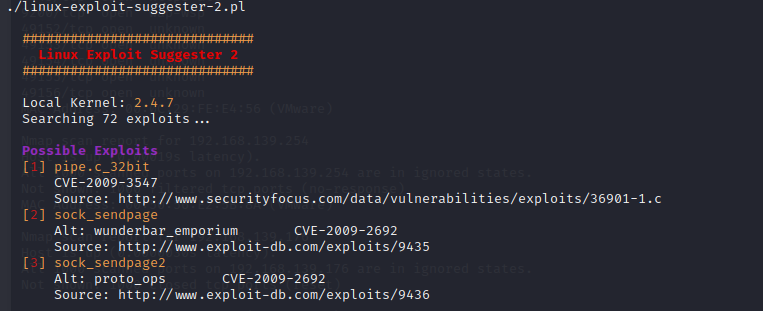
-İlk önce Linux üzerinde LinuxSuggester aracının bulunduğu yerde Python ile bir HTTPserver başlatıyorum ki buradan dosyayı çekebileyim.



- Tarayıcı üzerinde de kontrolünü sağladığım da başarılı şekilde paylaştığımı görüntülüyorum.

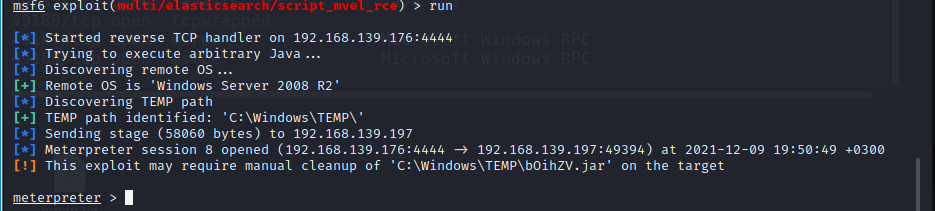


-Bunu Linux üzerine çekmek için "wget" komutunu genellikle kullanırız.Genellikle bulunduğumuz dizin üzerinde yetkimiz bulunmaz bu sebeple "tmp" klasörü içerisine bu dosyayı çekeriz.

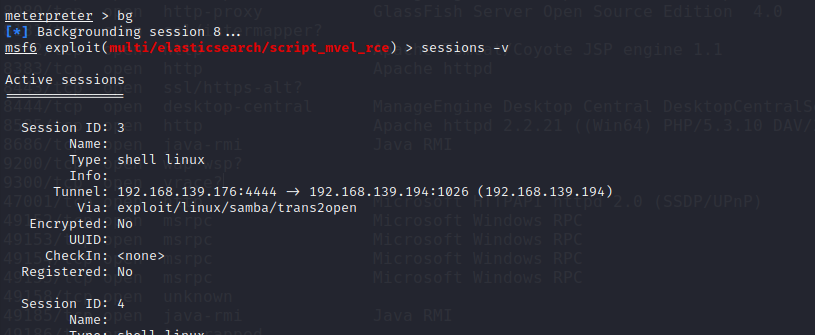


- Aracı sunucu içerisinde çalıştırıyorum ve burada da bulduğu açıkları görüntülüyorum.

***Metasploit Çoklu Oturum Yönetimi***

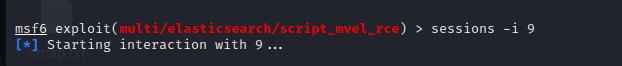


-Öncelikle bir meterpreter bağlantısı alıyorum.

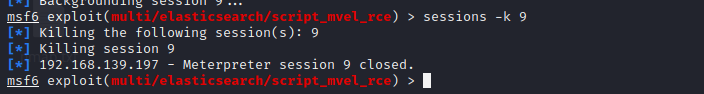


- Ardından "bg" komutu ile bunu background'a atıyorum.

-BG'ları sessions -v komutu ile görüntüleyebiliyorum.



-Sessions -i "session-id" komutu ile meterpreter bağlantısını geri alıyorum.

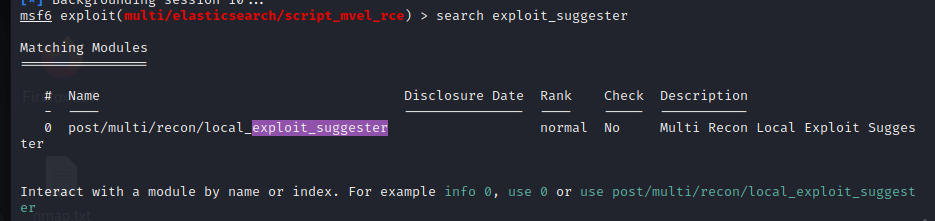


-Ayrıca "Sessions -k "sessiond-id" komutu ile mevcut olan bağlantıyı koparabiliyorum.

***Metasploit ile Local Exploit Tespiti***

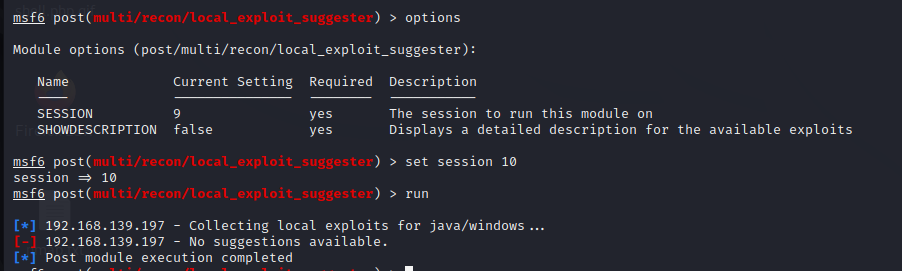
-Meterpreter bağlantısı kuruluyken arka plana session olarak gönderiyoruz.

-Ardından metasploit aracını başlatıyoruz.Burada "exploit\_suggester" ile bir tarama gerçekleştireceğiz.



- Metasploit aracını başlatıyorum.

-Ardından "search exploit\_suggester" komutu ile arama gerçekleştiriyorum.



- Ardından buraya "session id" bilgisini set ediyorum ve işlemi başlatıyorum.

-Bu işlem ile açık bulduğum session üzerinde bir tarama gerçekleştirip bulduğu açıkları tarafıma bildirecektir.