|  |
| --- |
| ***Privelege Excalation Saldırıları*** |
| Kaan Efe Öğüt  *ADLİ BİLİŞİM MÜHENDİSLİĞİ* |
| -Exploitation aşamasında bulduğum açıklardan yararlanarak yetkilerimi yükseltmeye çalışacağım. |

**27.12.2021**

***Windows’ta Yetki Yükseltme(Otomatik)***

-İşlemlerimize yetki yükseltme ile devam edeceğiz.

-Bu işlem için öncelikle bir meterpreter bağlantısı almalıyım.



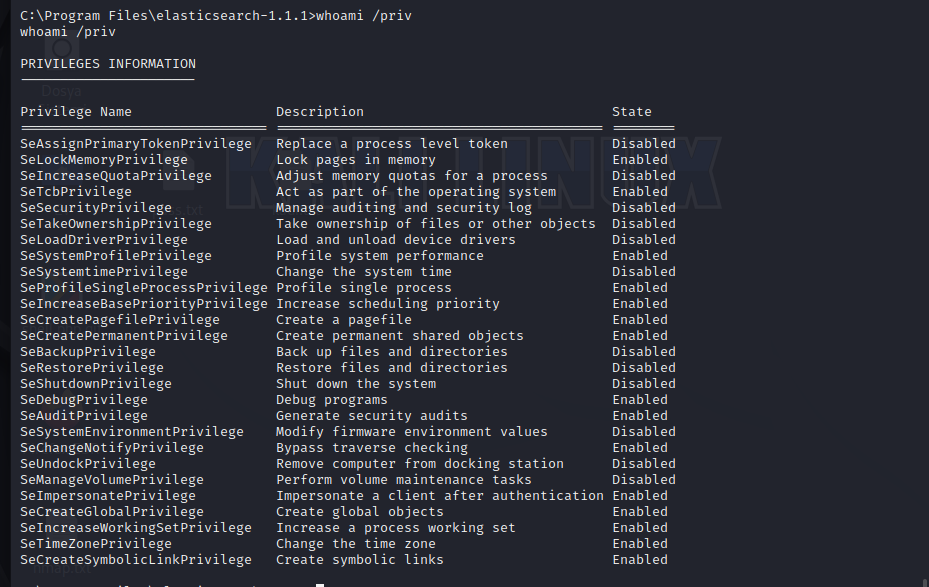
- Öncelikle "getuid" komutu ile yetkisini öğreniyorum.

-Burada eğer "NT AUTHORITY\SYSTEM" gözükür ise en yetkili olduğunu anlarım.

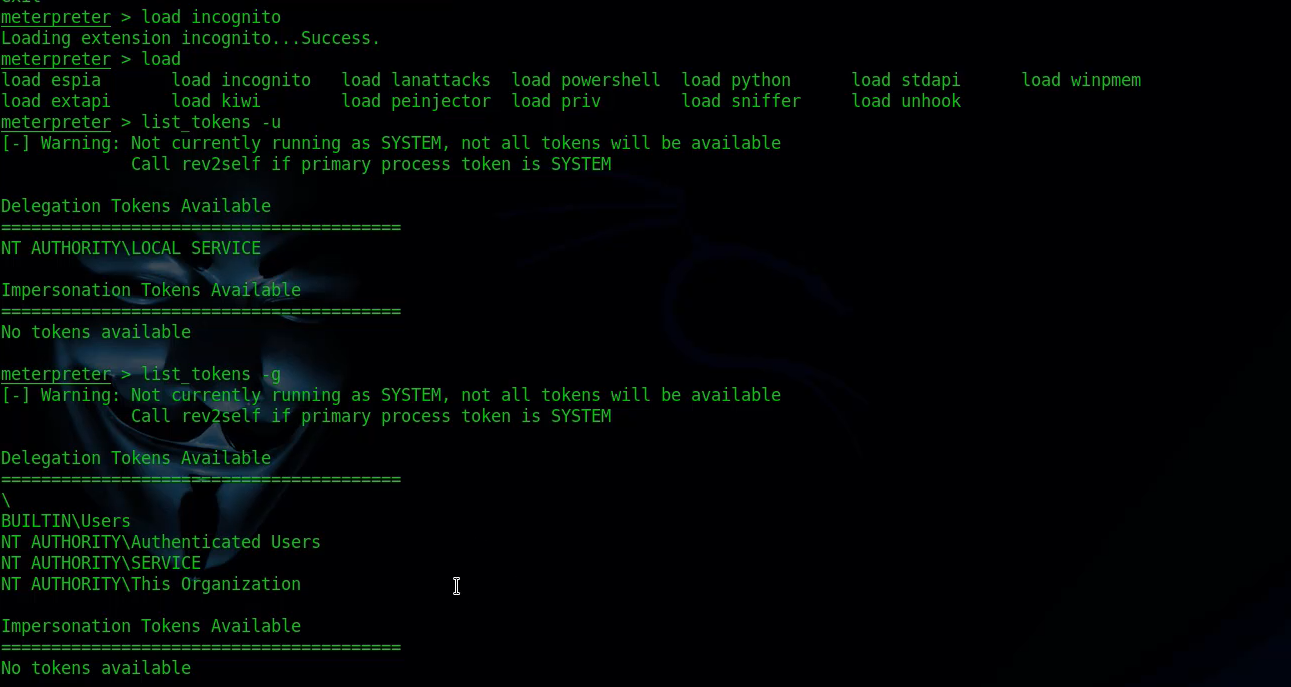
-Eğer "Local\_Service" görüntülersek sadece servislerle ilgilendiğini görüntülüyorum.



- "getprivs" komutu ile kullanabileceğimiz yetkileri görüntülemekteyiz.

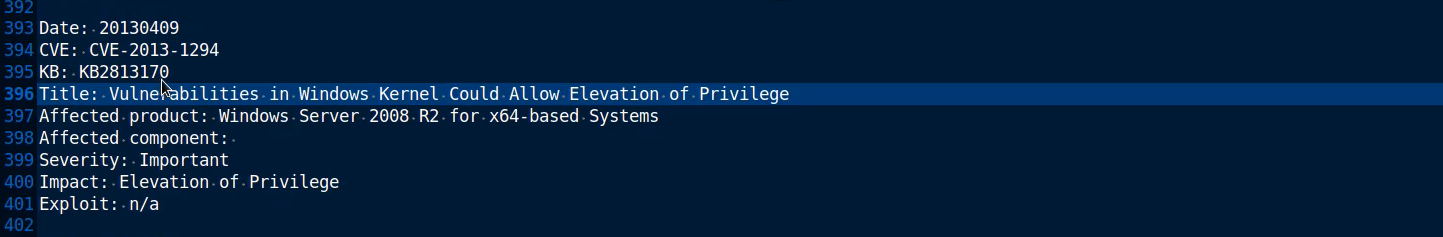


- Aynı şekilde "shell" komutu ile kabuk bağlantısı kurup kullanabileceğim servisleri görüntüleyebiliyorum.



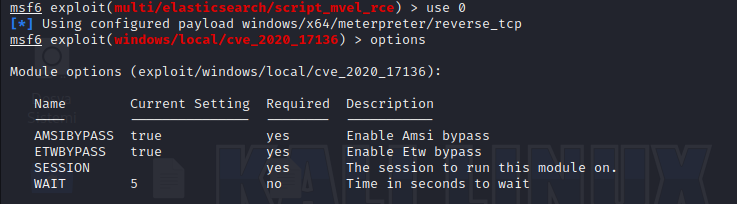
- "load incognito" komutu ile meterpreter üzerinde kullanabileceğim scriptleri kullanabilirim.

-Burada tokenlar üzerinden işlem gerçekleştirmeye çalıştığım da kullanabileceğim scriptler hakkında bilgi sahibi olabiliyorum.



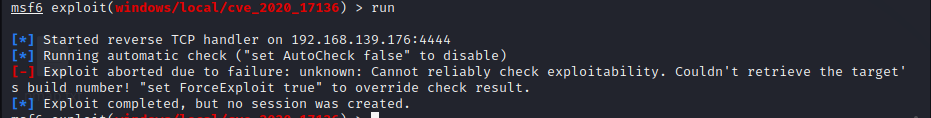
- Ayrıca daha önce suggester üzerinden elde ettiğim CVE numarası üzerinden bir açık taraması gerçekleştireceğim.

-Buradan bir yükseltme elde edebilirim.



- Metasploit aracı üzerinden bulduğum açık ile ilgili bir arama gerçekleştiriyorum.

-Scripti başlattığım da benden bir "session" bilgisi istemektedir.

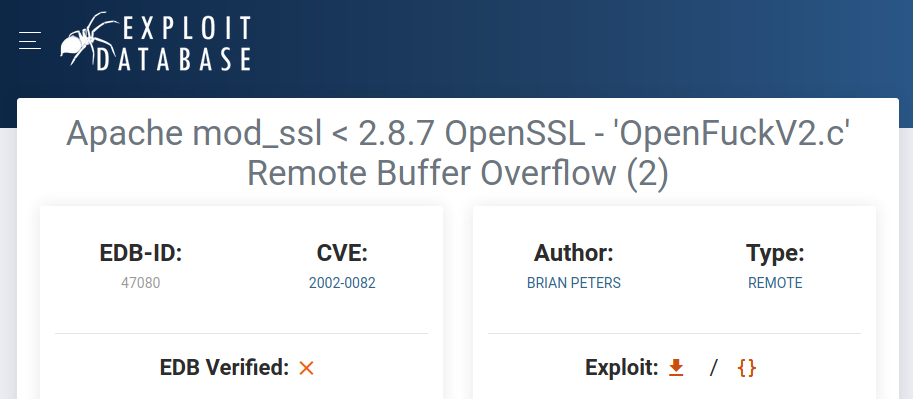


-Gerekli session bilgisini set ediyorum ve scripti çalıştırıyorum.

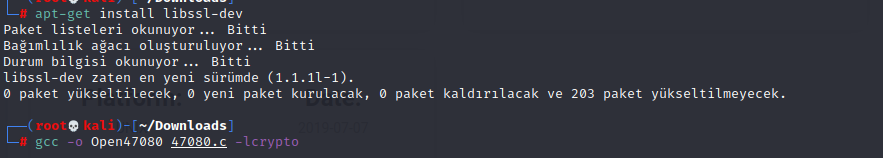
-Eğer burada "System" yetkisi ile çalışmıyor olsaydım başarılı bir şekilde yetki yükseltme gerçekleşirdi.

***Linux’ta Yetki Yükseltme(Manuel)***

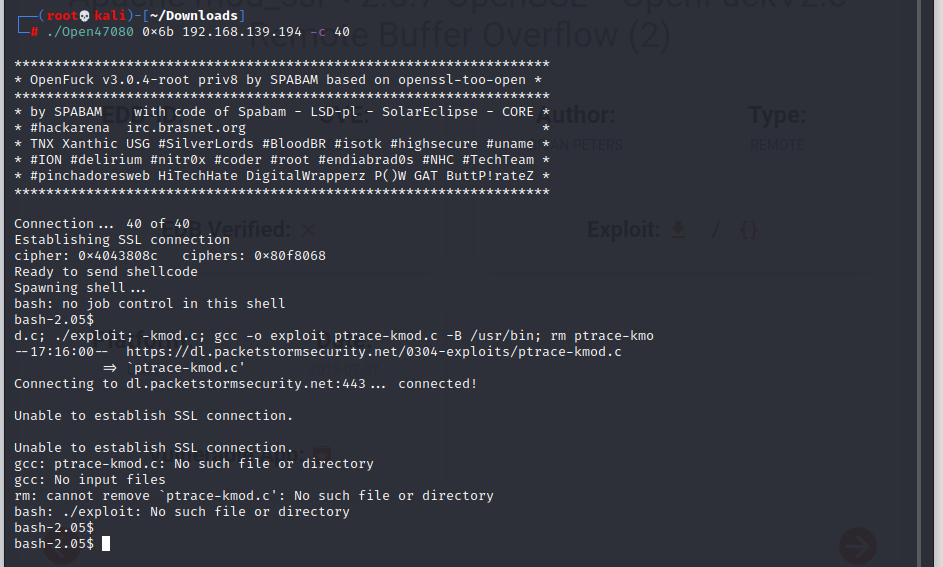
-"Kioptrix1" zafiyetli makinesi üzerinde bir exploit kullanıp yetkisini yükseltmeye çalışacağım.



-Öncelikle "exploit-db" üzerinde bulunan scripti indiriyorum.

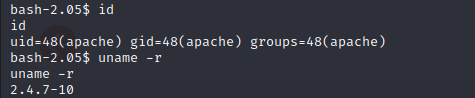


- Ardından gerekli kütüphaneyi kurup,"gcc" ile derliyorum.

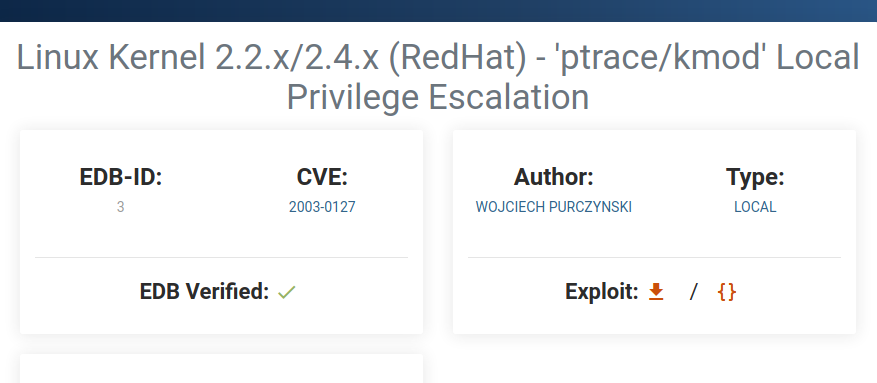


- Komutu kullanımına bakarak düzenliyorum ve Linux makineme saldırı gerçekleştiriyorum.

-Saldırı sonucunda başarılı bir şekilde shell alabildim.

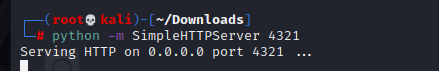


- Bağlantı sonrasında "id,uname -r" komutunu kullanarak kernel versiyonu ve yetkilerimi görüntüleyebiliyorum.

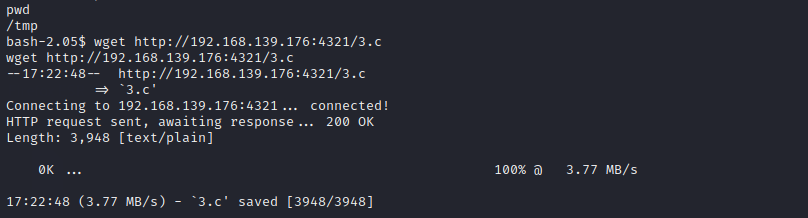


- Bulduğum çekirdek numarası ile bir exploit taraması gerçekleştiriyorum ve burada bir script buluyorum.

-C dilinde yazılan bu dosyayı indiriyorum fakat bu sefer server üzerinde compile edip çalıştıracağım.



- Bunun için indirdiğim dizin üzerinde bir SimpleHTTPServer başlatıyorum.

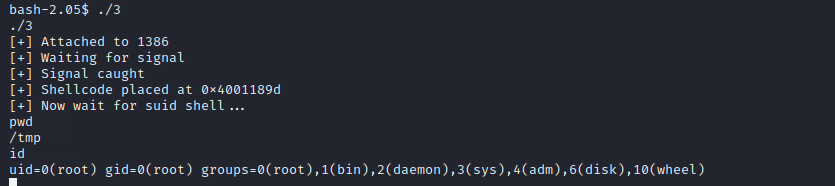


-Bu işlemi gerçekleştirmek için en doğru dizin TMP dosyasıdır.

-Dosyayı wget komutu ile indiriyorum.



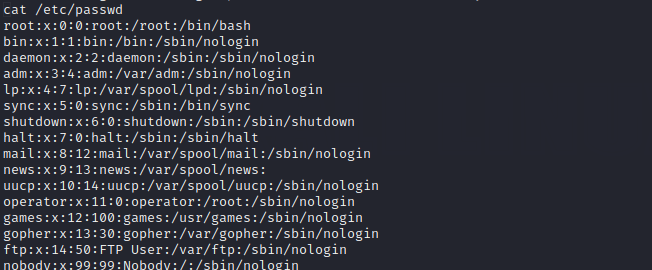
-Ardından "gcc" ile derleyip C kodunu çalışabilir hale getiriyorum.



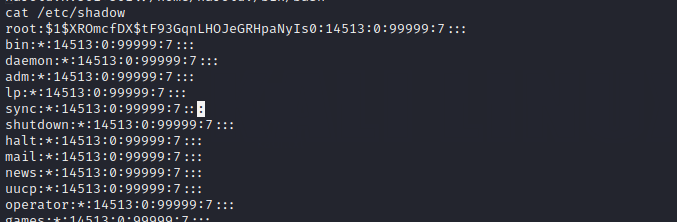
-Exploiti çalıştırdığımda başarılı bir şekilde root yetkisi alabildim.

***Linux’ta Hash Dump ve Crack***

-Yetki yükseltme işleminin ardından "Passwd ve Shadow" üzerinde ki hashli bilgileri çözmeye çalışacağım.



-"cat /etc/passwd" komutu ile kullanıcılar hakkında bilgi sahibi olabiliyorum.

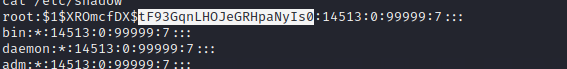


-Bir diğer kritik dosya olan shadow dosyasını görüntülüyorum.("cat /etc/shadow")

-Burada kullanıcı adları ve şifreleri şifrelenmiş bir biçimde görürüz.

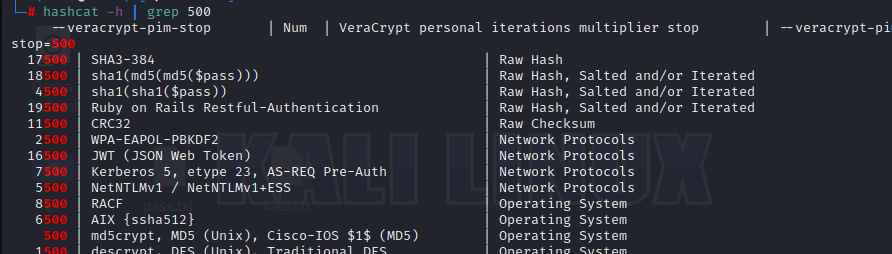
-"$1" ile başlayan kısım MD5 ile şifrelenmiştir.

-"$5" SHA 256'dır.Bunu program kullanarak çözebiliriz.



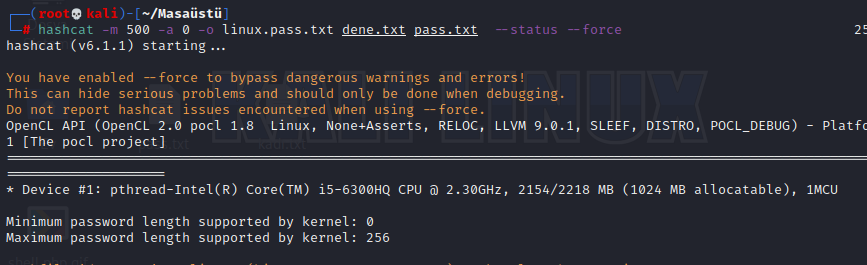
-Burada 2.Dolar işaretinden sonra ki kısım bizim için önemlidir.Burada şifre bilgileri tutulur.

-Burada bulduğum değerleri bir .txt dosyasına aktarıyorum.



-Kaydettiğim .txt üzerinde hashcat aracını kullanıyorum.

-Araç üzerinde "|grep 500" üzerinden bir arama gerçekleştiriyorum.Bu MD5 şifrelemeye aittir.



-Hashcat üzerinden şifreleme kırma işlemini başlatıyorum.

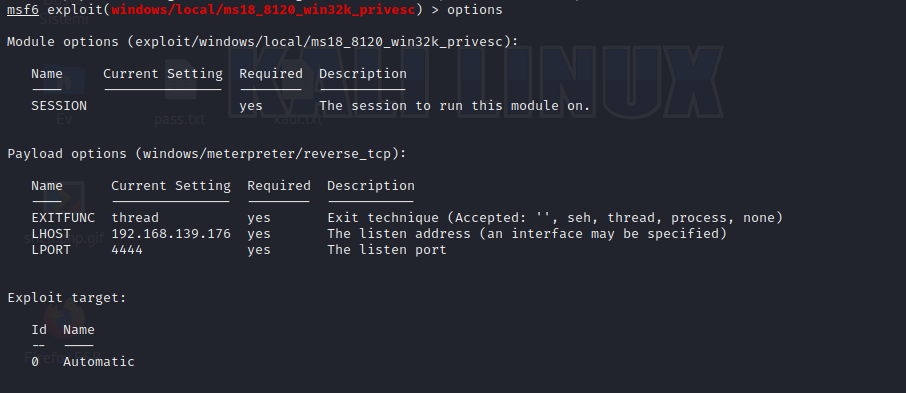


-Tarafıma bulduğu şifreleri bu şekilde aktardı.

***Windows’ta Hash Dump ve Crack***

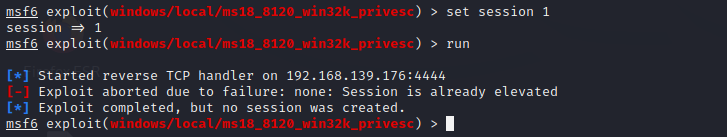
-Aynı işlemi bu sefer Windows makine üzerinde gerçekleştireceğim.

-Meterpreter bağlantısı kurulu bir şekilde işlemlerimi gerçekleştirmeye başlıyorum.



-"Metasploit" aracımı başlatıyorum.Ardından "windows/local/ms18\_8120\_win32k\_privesc" scriptini başlatıyorum.

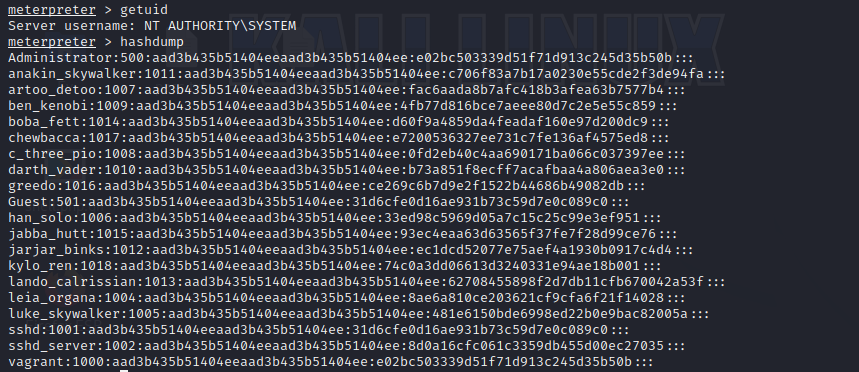
-Ayarlar kısmını görüntülediğim de burada bir "sessions" bilgisi vermem gerektiğini görüntülüyorum.



-Session bilgisini set ediyorum ve işlemi başlatıyorum.

-Burada benim bilgim üst düzey olduğu için hata almaktayım.

-Eğer yetkilerimiz kısıtlı ise bu adımlar yapılır.



-"hashdump" komutu ile sistem üzerinde bulunan kullanıcıların bilgilerine erişebiliyoruz.

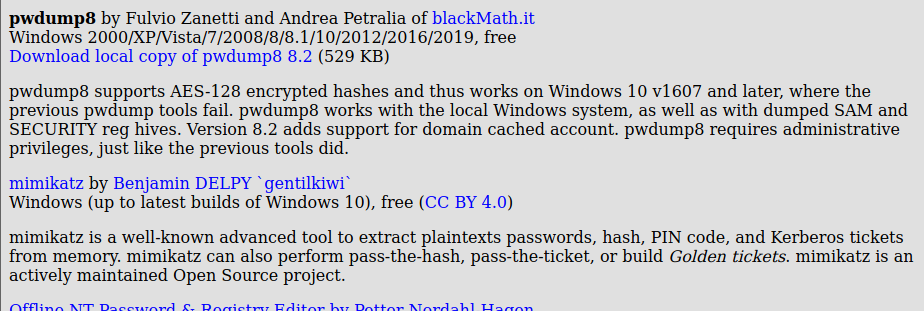
-Bu linux üzerinde bulunan "shadow" dosyasına benzemektedir.



-Burada bulduğum bilgileri kopyalıyorum ve bunları "hashcat & john" araçları ile kırmayı deneyebilirim.

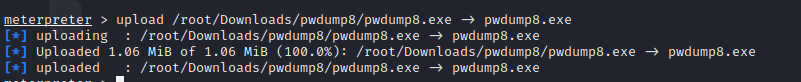
-Burada bu işlemi bırakıyorum.

-Eğer burada "hashdump" aracını kullanamamış olsaydım.Başka yapabileceğim yöntemlerde vardı.



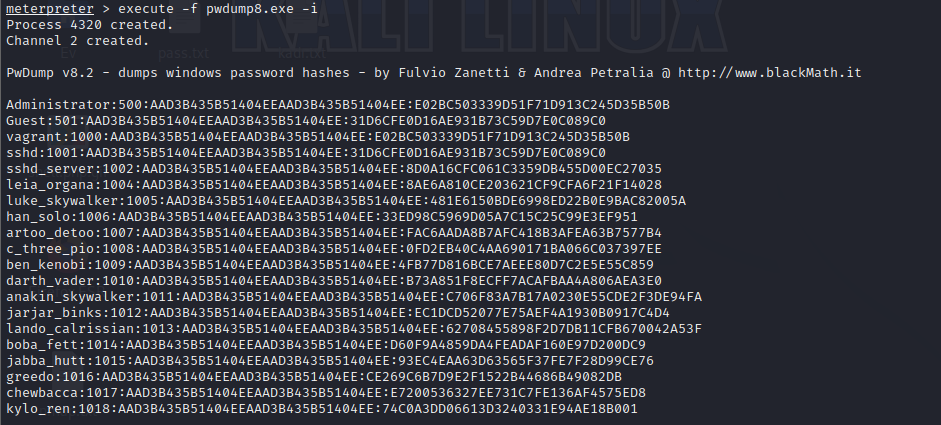
-Burada devreye "pwdump8" aracı girmektedir.Bu aracı "openwall" sitesi üzerinden indirebiliriz.

-Bunu sunucuya göndermeyi de zaten öğrenmiştik.



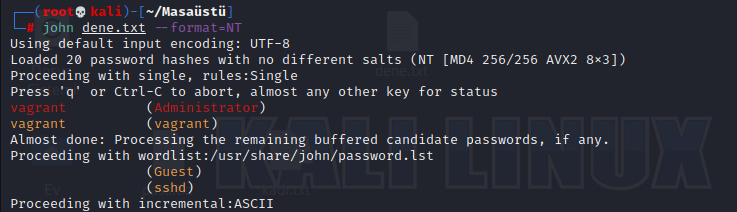
-Burada meterpreter bağlantısı kurduğum için bağlantı üzerinden gönderdim.

-HTTP server-ApacheServer üzerinden gönderim yapabilirdim.



Server üzerinde "pwdump8" aracını çalıştırıyorum.Burada "-i" komutu ile process üzerinde değil sonuçları interaktif olarak bana göndermesini sağladım.

-Bu araç sadece üst yetkilerde olduğum zaman işlev gösterir.



-John aracı ile şifreyi kırmaya çalışıyorum ve bulduğu şifreleri tarafıma aktarıyor.

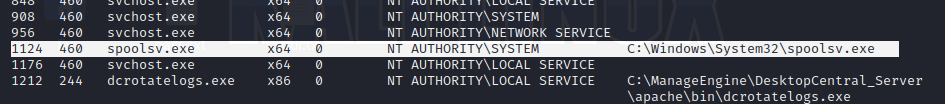
***Migration(Göç) İşlemi***

-Migration işleminin yapılmasının nedeni birden fazladır.

-Bu işlem için de önceden bir meterpreter bağlantısı kurulmalıdır.



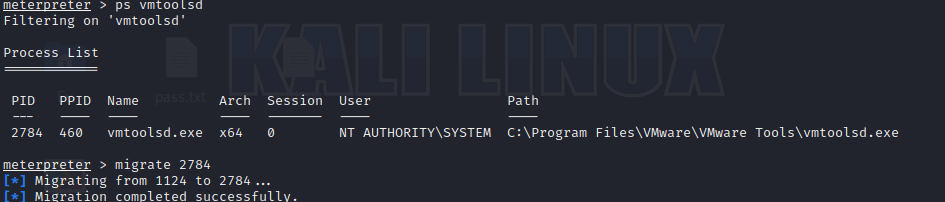
-"getpid" komutu ile şuan hangi process üzerinde çalıştığımı görüntülüyorum.



-"ps" komutu ile baktığım da şuanda farklı bir isim ile yer aldığımı görüntülüyorum.

-Burada fark edilip işlemimin sonlandırılmasını istemem.

-Ayrıca en büyük sebeplerinden biri de uyum sorununu ortadan kaldırmaktır.



-Burada gizlenecek en güzel yerlerden biri "explorer" dosyasıdır.

-Eğer burada gizlenemezsek "winlogon" üzerinde gizlenmemiz bizler için iyi olur.

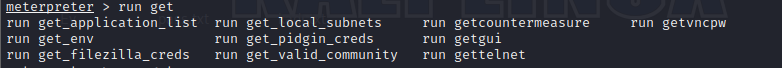
-Sanal makine üzerinde çalıştırılıyorsa "vmtoolsd.exe" process'i bulunmaktadır.

-Ayrıca kendi kullanıcıma denk işlemlere geçiş yapabilirim.

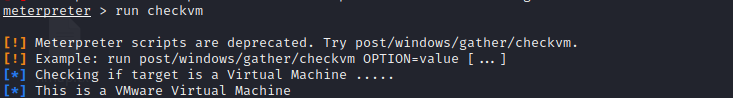
-Vmtoolsd.exe arkasına şuan da saklandım eski process işlemim son bulsa da artık sistemden düşmem.

***Meterpreter Scriptleri ve şifrelerin elde edilmesi***

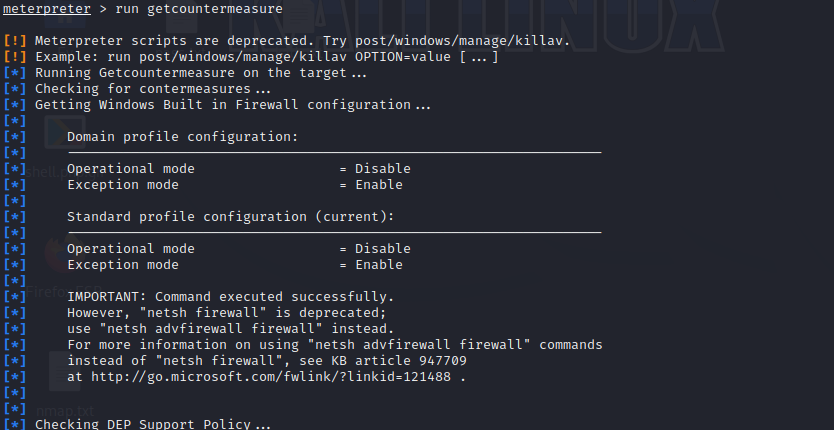
-Birazda meterpreter komutlarından bahsetmek istiyorum.



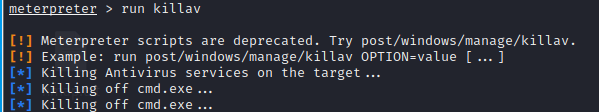
-"run get" komutunu kullanıp 2 kere tab tuşuna basarsak bana kullanabileceğim scriptleri verir.



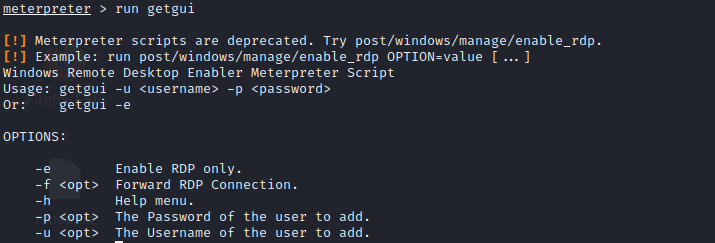
-"run checkvm" komutu ile sistemin sanal makine olup olmadığını görüntüleyebilirim.



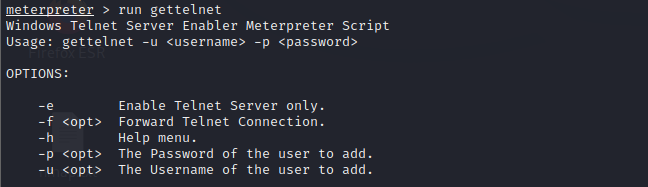
-"run getcountermeasure" komutu ile firewall konfigurelerini görüntüleyebiliriz.



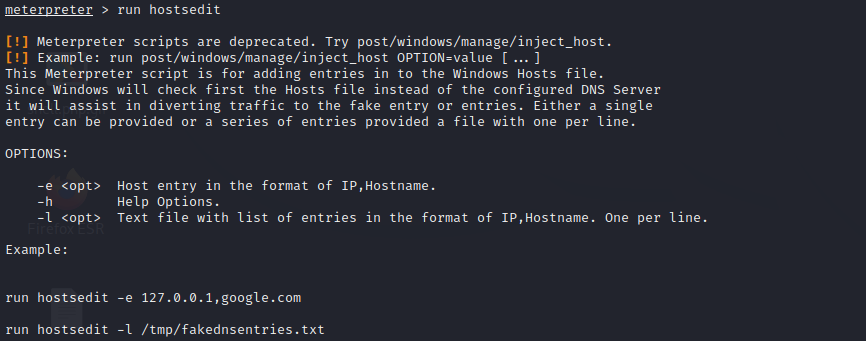
-"run killav" komutu ile açık olan antivirüsleri devre dışı bırakabiliriz.



-"run getgui" remote desktop'ı açmaya çalışabiliriz.

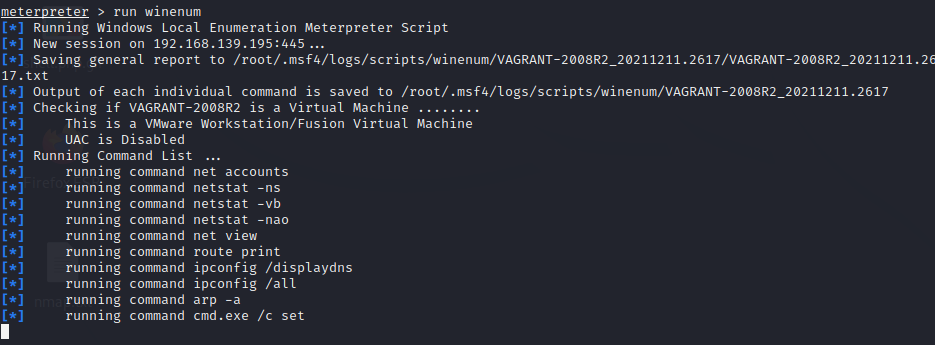


-"run gettelnet" komutu ile Telnet servisini açmaya çalışabiliriz.

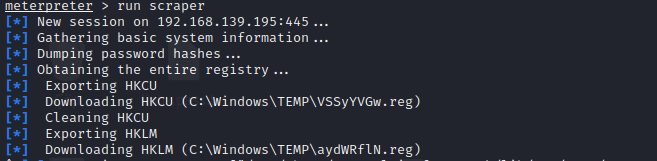


-"run hostedit" komutu ile host dosyasına müdahele de bulunabiliriz.

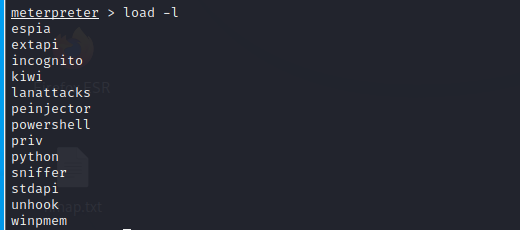
-DNS'e sorgu atılmadan önce kontrol edilen servis.



-"run winenum" komutu ile işletim sistemi hakkında daha fazla bilgi edinebiliriz.

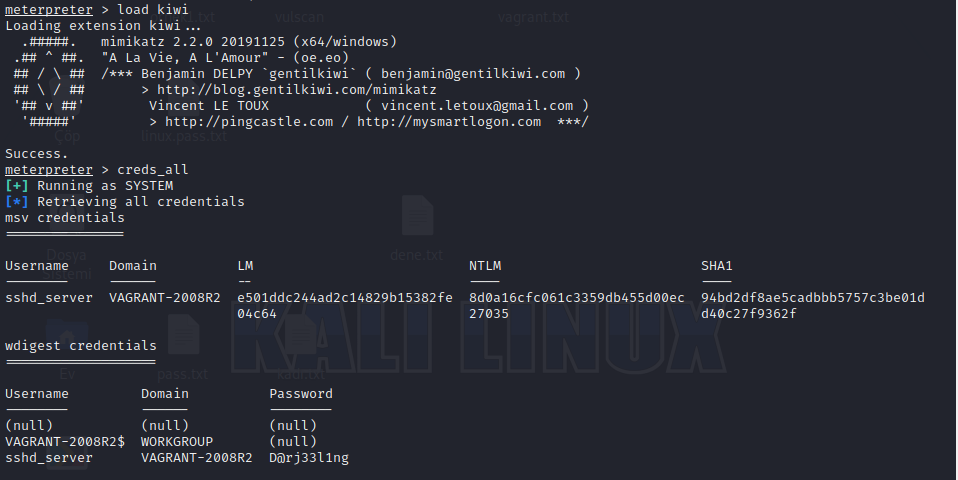


-"run scraper" komutu ile kayıt defterinde bulunan bilgileri tarafıma çekmeye çalışır.



-"load -l" komutu ile meterpreter üzerinde kullanabileceğim pluginleri görüntüleyebilirim.

-"kiwi" pluginini kurup ardından "creds\_all" komutunu kullanarak sistem üzerinde bulunan kullanıcı adı ve şifrelere erişebiliriz.

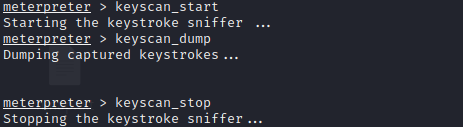


-Yüksek yetkide olmazsak bu işlemi gerçekleştiremeyiz.

***Hedefte Keylogger çalıştırma***

-Sistem üzerinde keylogger çalıştırıp tüm klavye işlemlerini kayıt edebiliriz.

-Bu işlem öncesinde process'imizi migrate etmemiz gerekmektedir.



-keyscan\_start" komutu ile keylogger aracını başlatıyorum.

-"keyscan\_dump" komutu ile bulduğum sonuçları kaydeder.

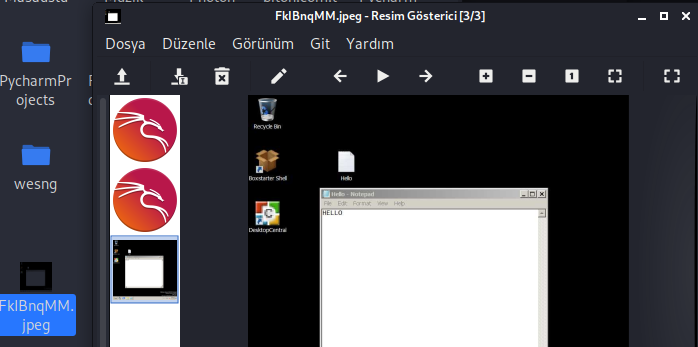
-"keyscan\_stop" komutu ile aracı sonlandırır.

***Hedefin Ekran Görüntüsünü Alma***

-Erişim aldığımız process'i yine migrate komutu ile gizlememiz gerekmektedir.



-Ardından "screenshot" komutu ile ekran görüntüsünü kendi işletim sistemimize alabiliriz.



-Ekran görüntüsünü de bu şekilde görüntüleyebiliriz.