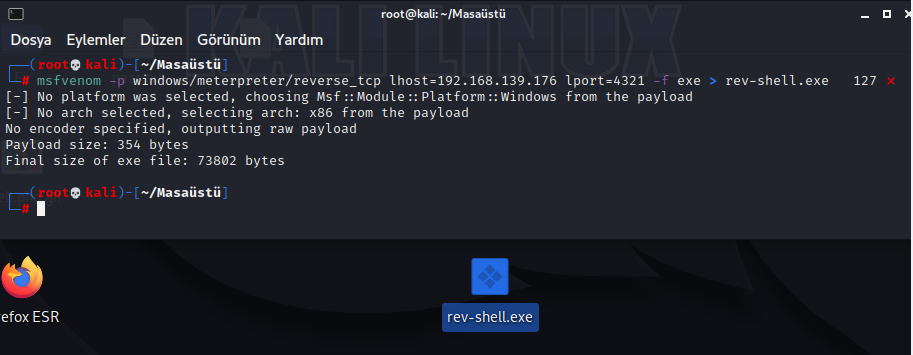
|  |
| --- |
| ***APT(Advanced Persisten Threat) Saldırıları*** |
| Kaan Efe Öğüt  *ADLİ BİLİŞİM MÜHENDİSLİĞİ* |
| Penetrasyon işlemlerinde en önemli faktörlerden olan gizlenme ve oluşturduğun backdoor’u gizli tutmak için yapılabilecek yöntemlerden bahsedeceğim. |

**27.12.2021**

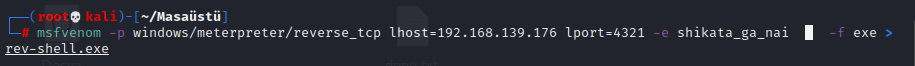
***Backdoor Oluşturma***

- Metasploit üzerinde hedefler üzerinde otomatik olarak işlem gerçekleştiriyorduk.

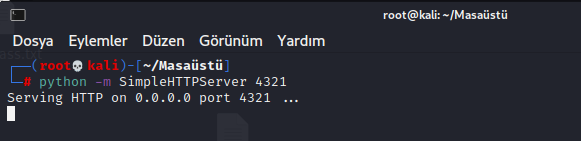
-Bu sefer kendimiz yine metasploit firmasına ait Linux üzerinde kurulu olarak gelen "msfvenom" aracı ile bu işlemleri gerçekleştireceğiz.



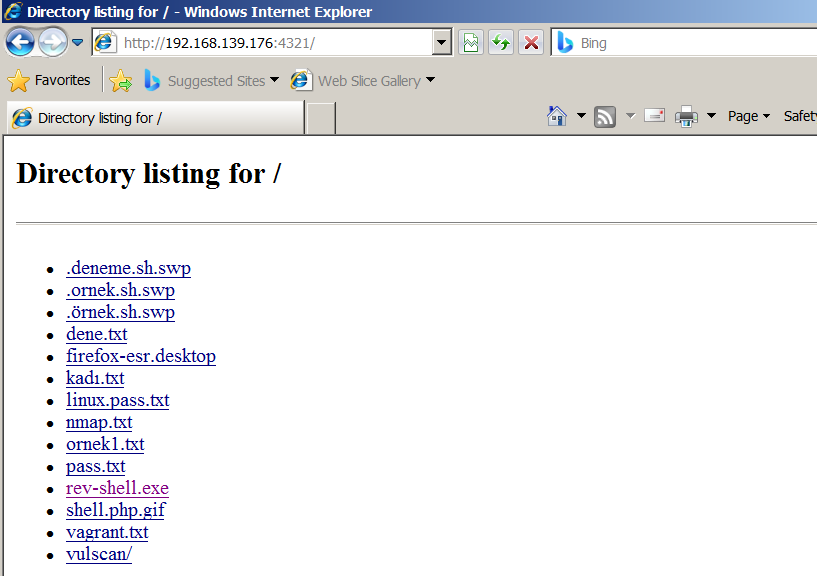
- "msfvenom" aracı ile "reverse\_tcp" için bir backdoor oluşturuyorum.



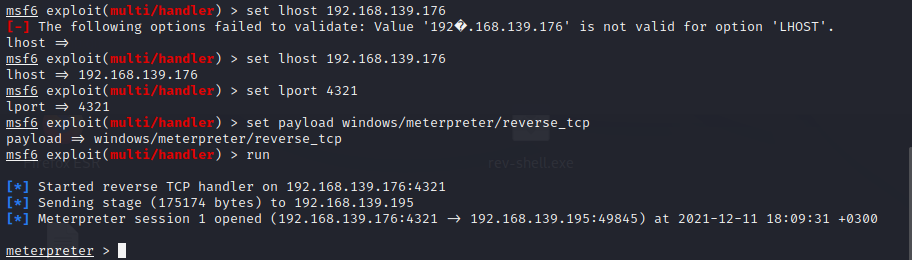
- Burada encode kullanarak oluşturduğumuz zararlı yazılımın tespit edilmesini engelliyorum.



- Aracın bulunduğu yer bir HTTPServer başlatıyorum.



- Ardından sunucu üzerine geçiş yapıyorum ve HTTP Server üzerinden oluşturduğum zararlı yazılımı indiriyorum.



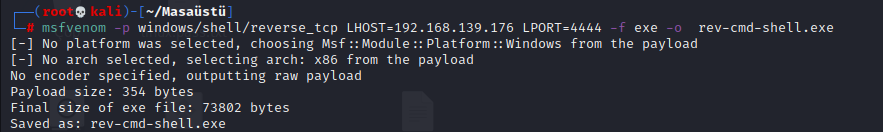
- Aracı çalıştırmadan önce backdoor üzerinde belirttiğim port'u dinlemeye alıyorum.

-Burada metasploit içerisinde bulunan multi handler aracından yararlanıyorum.

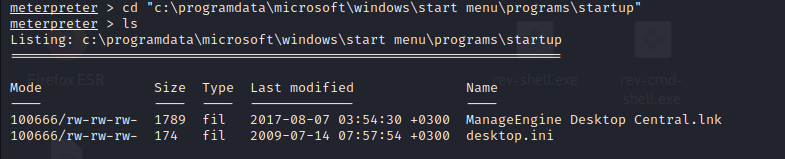
-Aracı çalıştırdığım da başarılı bir şekilde meterpreter bağlantısı kurabildim.

***Backdoor’u sistem açılışına yerleştirme***

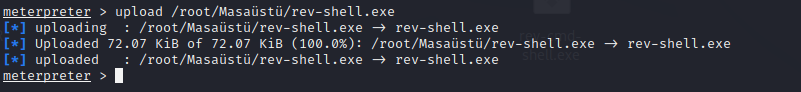
-Oluşturduğumuz backdoor'u sistem açılışına gizleyip her açıldığında aktif hale getirmeye çalışacağız.



- Bunun için ilk önce shell kullanan bir zararlı yazılım oluşturuyorum.

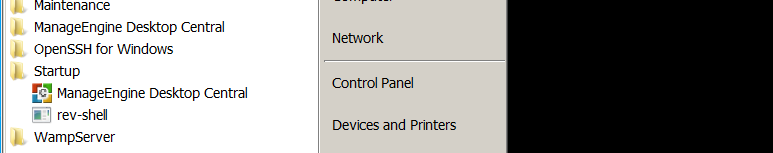


- Ardından zaten devam eden Meterpreter bağlantım üzerinden "startup" dosyasına geçiş yapıyorum.

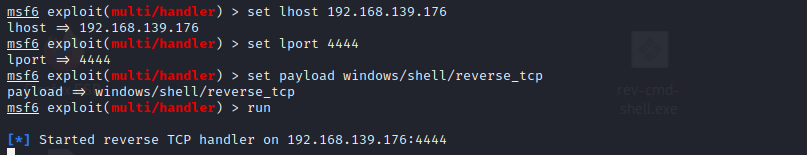


- "Startup" içerisine oluşturduğum shell'i ekliyorum.

-Ardından tüm bağlantılarımı kapatıyorum.



- Sunucu üzerinden de kontrol ettiğim de her açılışta aktif olacağını görüntülüyorum.



-Sunucumu kapatıyorum ve ardından metasploit üzerinde bulunan multi handler aracından yararlanıyorum.

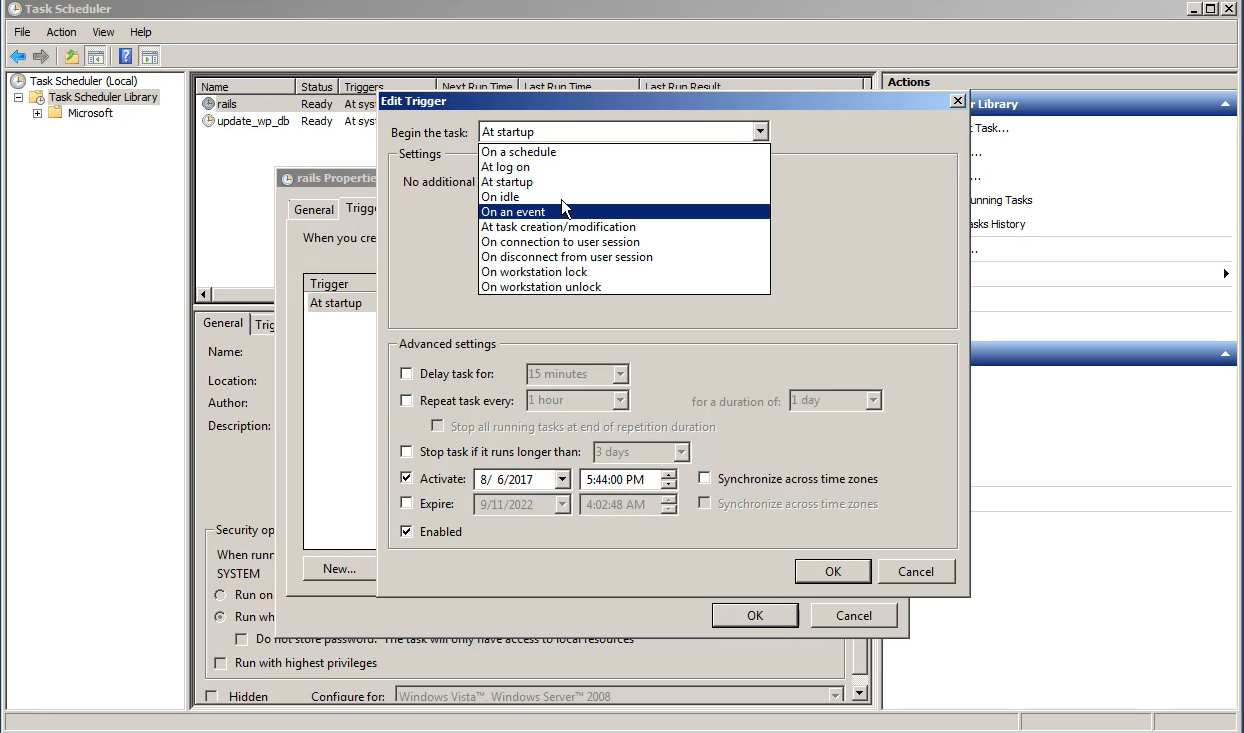
-Burada "msfvenom" ile oluşturduğum payload üzerinden işlem gerçekleştiriyorum.



- Ardından sunucumda oturum açıyorum ve karşıma bu şekilde bağlantı geliyor.

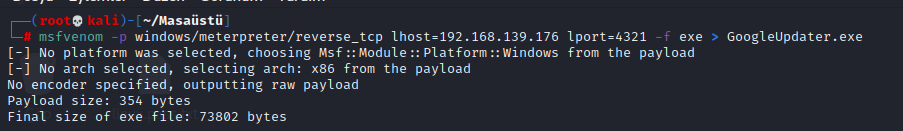
***Backdoor’u Görev Zamanlayıcıya Yerleştirme***

-Az önce yaptığımız işlemi "Task Scheduler" üzerine ekleyerek buradan sürekli shell almamızı sağlar.

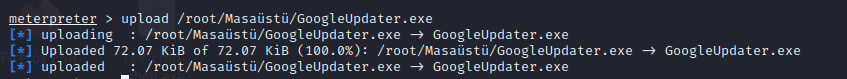


- Task scheduler'ı server üzerinde görüntülediğimizde böyle bir ekran izleri karşılıyor.

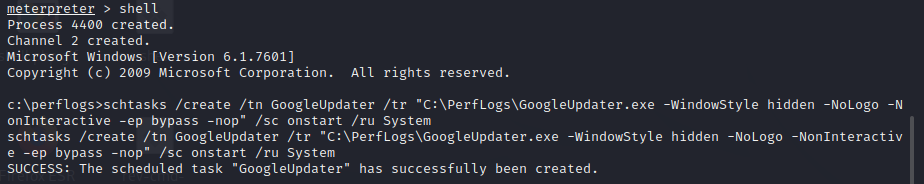
-Bu işlem için çok kullanılmayan bir dosya kullanılırsa daha iyi olur ben burada Perflogs dosyasını seçiyorum.



- Msfvenom ile ilk önce "GoogleUpdater" isimli bir meterpreter yazılımı yazıyorum.



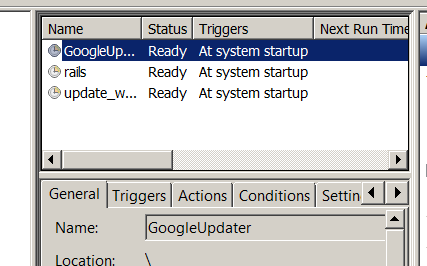
-Meterpreter bağlantısı üzerinden "perflogs" içerisine oluşturdum zararlı yazılımı ekliyorum.



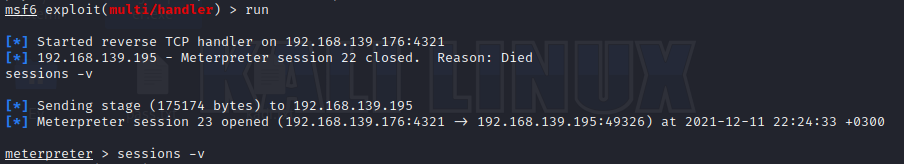
- Bu işlem için yazılmış bir script komutu kullanacağım.Bu scripti meterpreter üzerinden değil de shell bağlantısı üzerinden çalıştırıyorum.

-Burada öncelikle meterpreter bağlantım üzerinden işlem gerçekleştireceğim.

-Kodum bu şekildedir. "schtasks /create /tn GoogleUpdater /tr "C:\PerfLogs\GoogleUpdater.exe -WindowStyle hidden -NoLogo -NonInteractive -ep bypass -nop" /sc onstart /ru System"



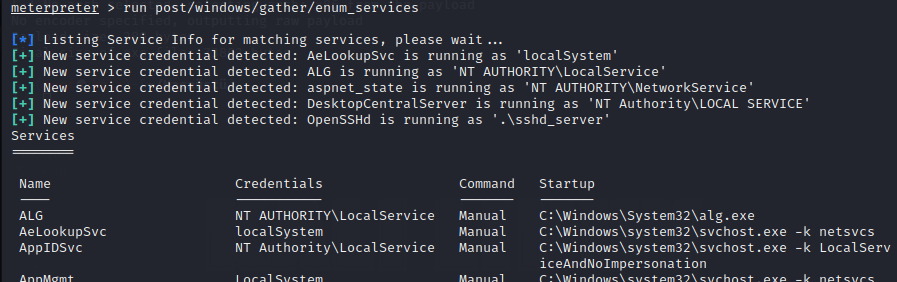
- Server üzerinde kontrol ettiğim de GoogleUpdater olarak kayıt edildiğini görüntülüyorum.



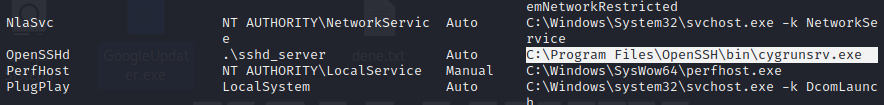
- Server'ı yeniden başlattığım da 120 saniye içerisinde "Task Scheduler" servisleri çalışır.

-Ardından kontrol ettiğimde başarılı bir şekilde bağlantı kurabildim.

***Kullanıcı Ekleme(Unquoted Service Path)***



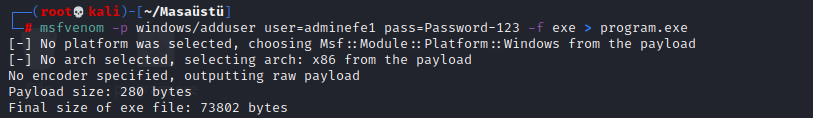
- Meterpreter bağlantısı sırasında kullanacağım "run post/windows/gather/enum\_services" komutu ile içerisinde bulunan servisleri görüntülüyorum.



- Burada dizin kısmında eğer boşluk var ise "" işareti kullanılmalıdır.

-Örnekte olduğu gibi boşluk olmasına rağmen tırnak işareti yoksa burada bir açık bulunmaktadır.

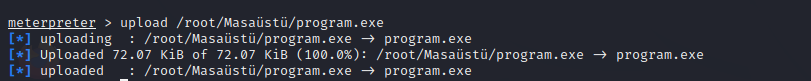
-Burada okurken boşluğa kadar gider ve eğer exe yoksa .exe gördüğü yere kadar gider.Burada araya girersek backdoorumuzu servis yetkisinde kullanabiliriz.



- Şuan gerçekleştireceğimiz çalışmaları yüksek yetki ile gerçekleştiriyoruz.Burada "tmp" içerisinde bulunan bir servis keşfedilerek işlem yapılırsa yetkisiz de aynı işlemler yapılabilir.

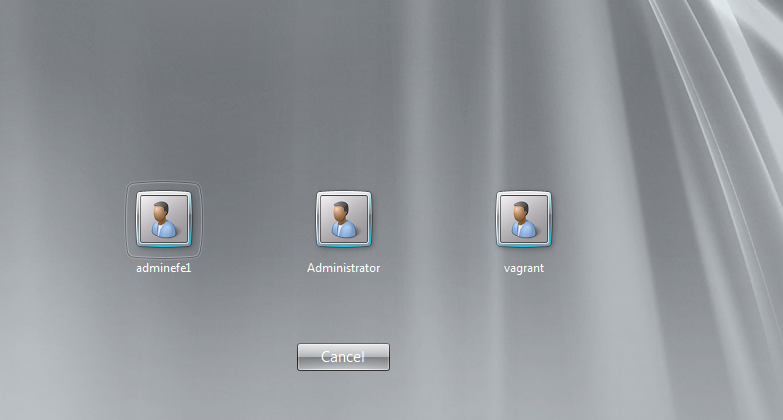
-Msfvenom ile zararlı yazılımı oluşturuyorum.

-Kulanıcı adı: "adminefe1" - Şifre:"Password-123" > Şifreyi güçlü vermek sistemin hata vermemesi için önemlidir.



- Meterpreter bağlantım üzerinden "C:\\" dizini altına oluşturduğum zararlı yazılımı ekliyorum.

-Burada C:\\ dizini altında .exe içeren bir dosya arıyacak ve bu aracı görüp çalıştırıcak.

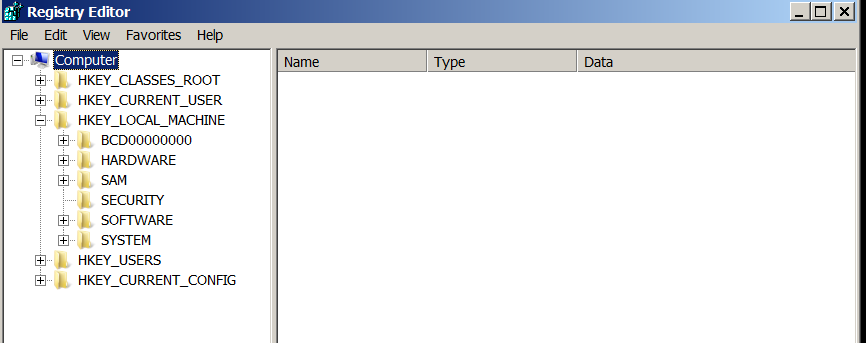


-Serveri yeniden kapatıp açtığım da kullanıcının eklendiğini görüntülüyorum.

***Registry ile Kullanıcı Girişi Gizleme***

-Oluşturduğumuz bu kullanıcıyı Registry üzerinden görünmez hale getirmeyi amaçlıyorum.

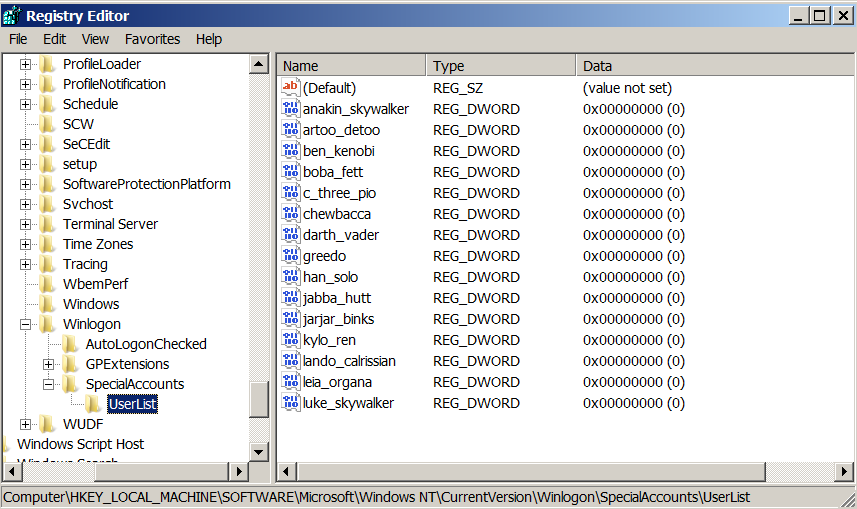
-Registry üzerinde işletim sistemiyle ilgili gerekli tüm ayarlar yer almaktadır.



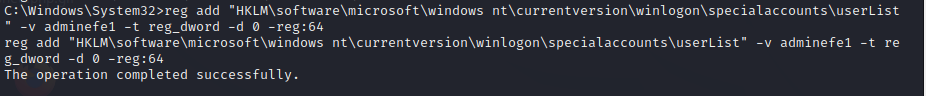
- "Local-Machine" içerisinde makineyle ilgili ayarlar.

-"Current-User" içerisinde oturum açılan kullanıcıya ait ayarlar.

-"USERS" kısmında ise tüm kullanıcılara ait ayarlar yer almaktadır.

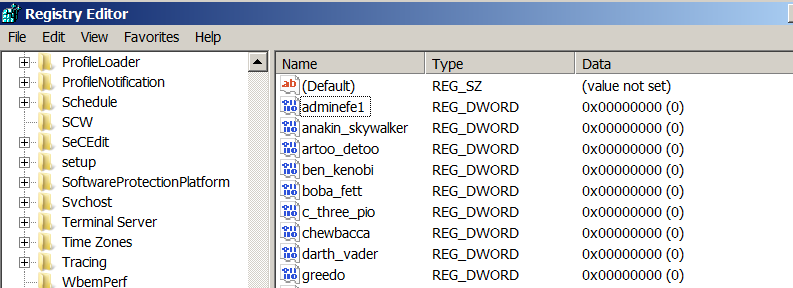


- Registry üzerinde "UserList" bölümüne geldiğim de burada giriş kısmında gizlenmiş kullanıcılara erişim sağlayabiliyorum.



- Meterpreter bağlantım üzerinden "System32" kısmına geliyorum.

-Burada "reg add "HKLM\software\microsoft\windows nt\currentversion\winlogon\specialaccounts\userList" -v adminefe1 -t reg\_dword -d 0 -reg:64" komutunu çalıştırıyorum.



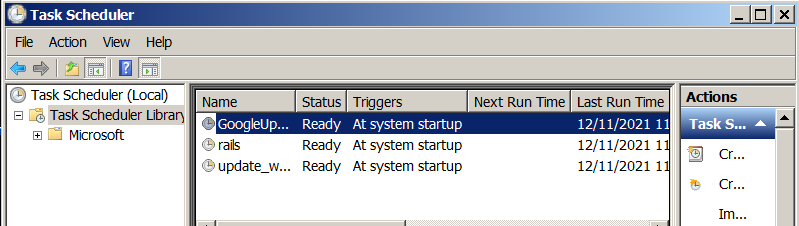
- Registry üzerinden de kontrol ettiğim de burada "adminefe1" kullanıcısının da eklendiğini görüntülüyorum.



-Ardından Server'ı kapatıp açıyorum ve kullanıcı kısmında artık "adminefe1" yazmıyor.

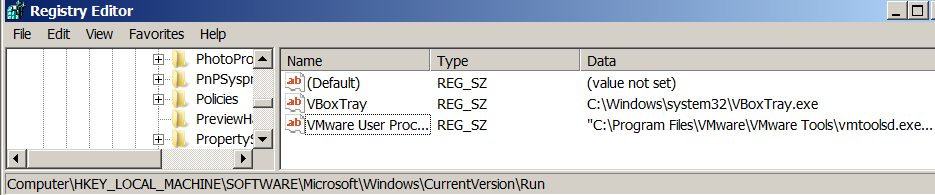
***Registry ile Açılışa Exe Yerleştirme***

-Önceki örneklerimizde eklediğimiz GoogleUpdater servisini gizlemeye çalışacağım.

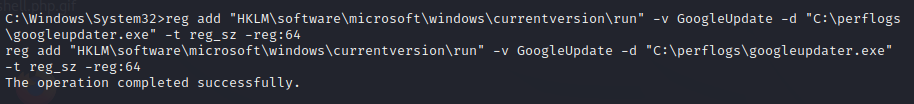


- "Tash Scheduler" üzerine geçiş yaptığım da burada GoogleUpdater servisini görüntülüyorum.

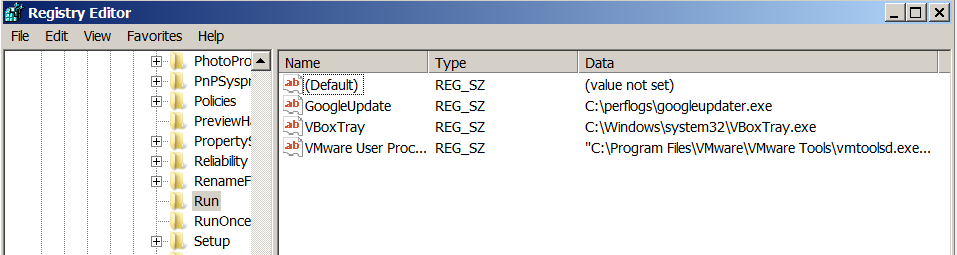
-Buradan silinme durumuna karşılık regedit içerisine ekleme gerçekleştirebiliriz.



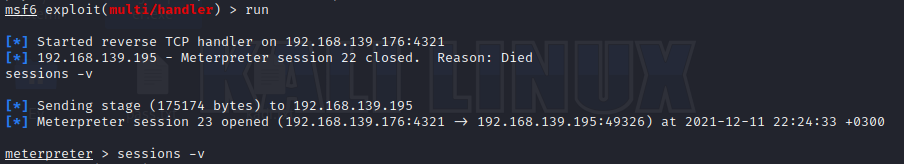
- Regedit içerisinde "Run" klasörünü görüntülüyoruz.Burada gizlenen ögeler bulunmaktadır.



- Shell bağlantısı üzerinden sisteme yazacağımız bu kod ile "Run" dizinine ekleme gerçekleştireceğiz.



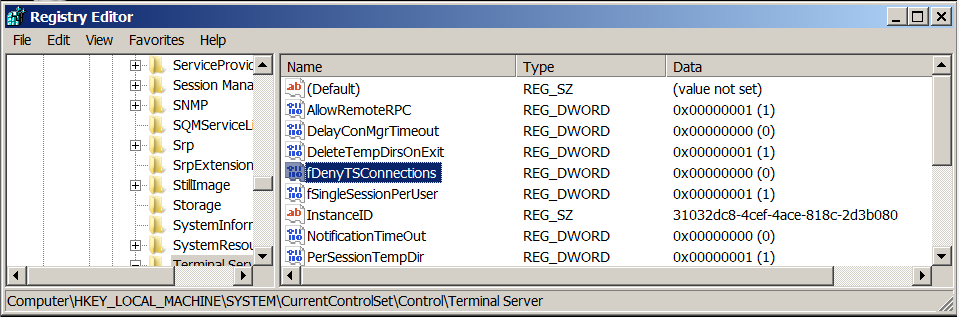
- Kayıt Defteri üzerinden kontrol ettiğimde burada "Googupdate" aracının eklendiğini görüntülüyorum.



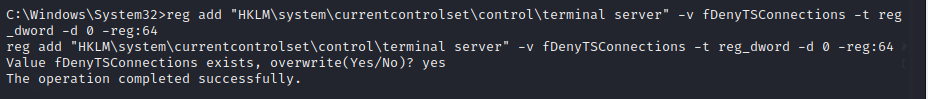
- Sistemi yeniden başlattığımda aynı şekilde meterpreter üzerinden bağlantı alabildiğimi görüntülüyorum.

***Registry ile RemoteDesktop aktif etme***

-Registry üzerinden RemoteDesktop kapalı olsaydı nasıl açabilirdik bunu görüntüleyeceğiz.

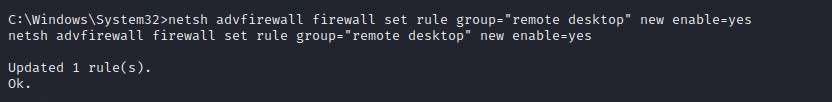


- Registry üzerinde bulunan "fDenyTSConnections" ayarının değeri "0" ise sistemin uzaktan erişime açık olduğunu anlıyorum.



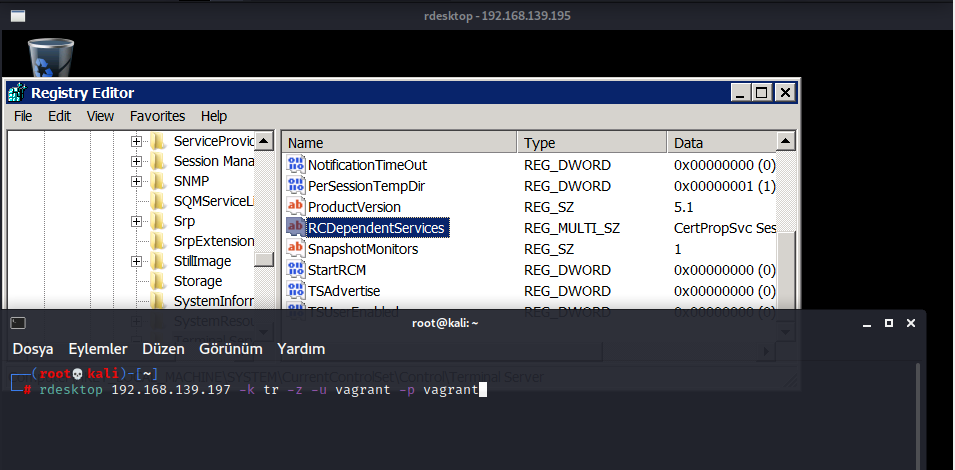
- Bu değeri dışarıdan kullanacağım "script" ile değiştirmek isteseydim;

-"reg add "HKLM\system\currentcontrolset\control\terminal server" -v fDenyTSConnections -t reg\_dword -d 0 -reg:64" komutunu shell üzerinde çalıştırırdım.



- Ardından firewall üzerinde bulunan değeri de değiştirmem gerekmektedir.

-Bu değeri de "netsh advfirewall firewall set rule group="remote desktop" new enable=yes" komutu ile değiştiriyorum.

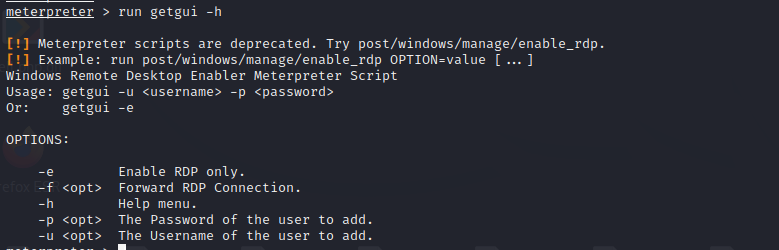


- Linux üzerinden bir "rdesktop" bağlantısı gerçekleştirdiğim de bağlantıyı kurabiliyorum.

***Metasploit ile Remote Desktop Aktif etme***

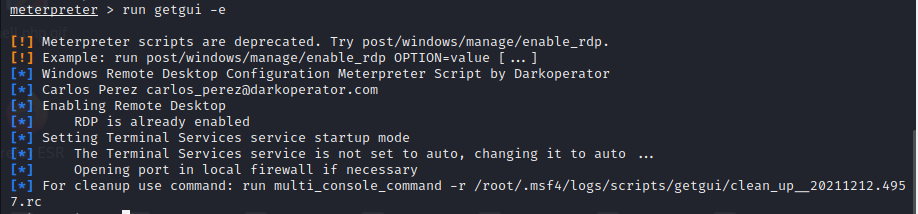
-Remote desktop'ı aktif etme işlemini her zaman "Meterpreter" olmayacağı için shell üzerinden gerçekleştirmeyi görmüştük.

-Bu sefer işlemi kolay yoldan metasploit aracı ile gerçekleştireceğiz.

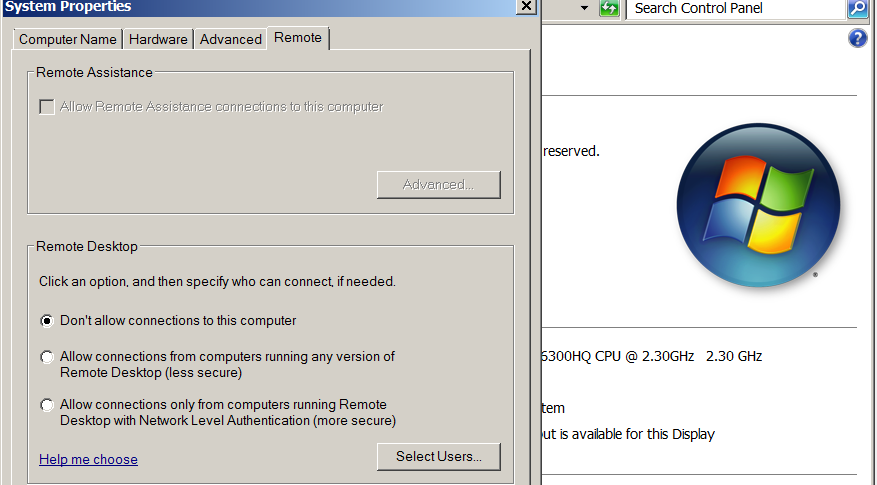


- Meterpreter bağlantım üzerinden işlemler gerçekleştireceğim.

-Burada "run getgui" üzerinden işlem gerçekleştireceğim.

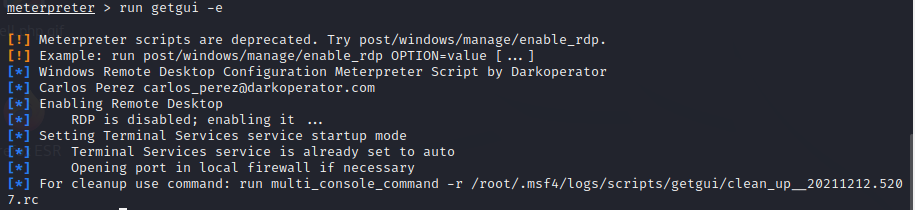


- "run getgui -e" komutu ile aktif hale getirmeye çalışıyorum fakat server üzerinde aktif olduğu için tekrardan aktif hale gelemiyor.

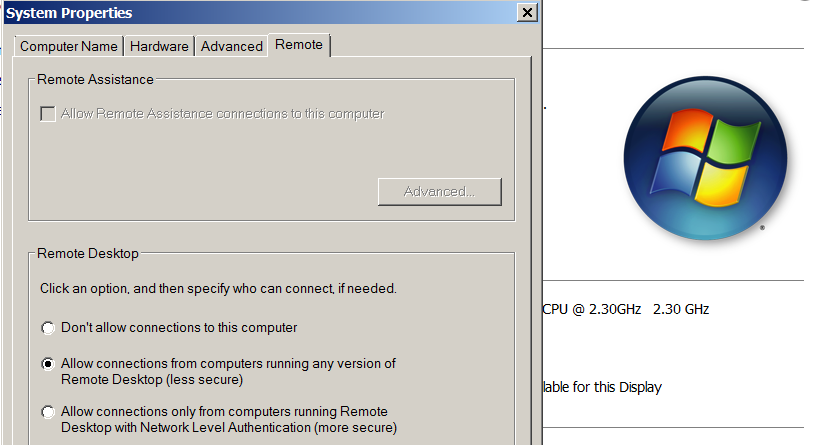


- Bu sebeple server üzerine geçiş yapıyorum ve buradan aktif hale getiriyorum.

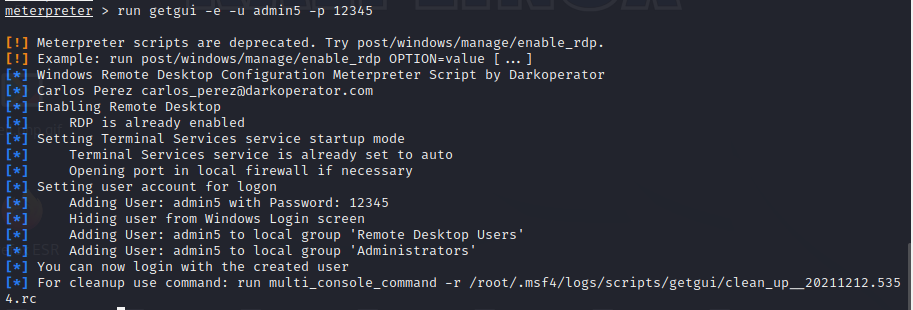
-Sistem ayarlarından RDP'yi kapatıyorum.



- Kapatma işleminin ardından bir kere daha "run getgui -e" komutunu çalıştırıyorum.Burada remote desktop'u aktif hale getirmeye çalıştığını belirtiyor.



- Server üzerinden kontrollerini sağlıyorum ve Aktif hale getirdiğini görüntülüyorum.



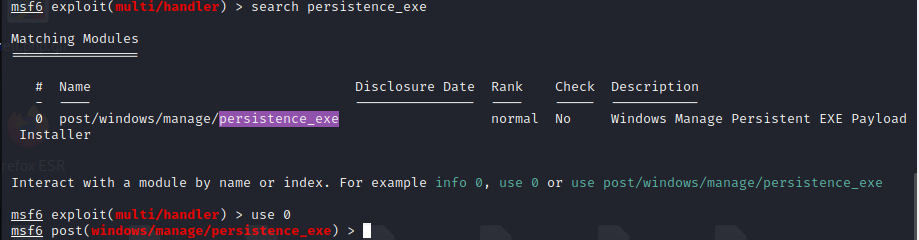
- Ardından "run getgui" aracı ile "admin5-12345" kullanıcı adı ve şifreli bir kullanıcı oluşturuyorum.Sistem içerisinde otomatik olarak bu gizlenir.



- ServerManager üzerinden kontrol sağladığım da buraya eklendiğini görüntülüyorum.

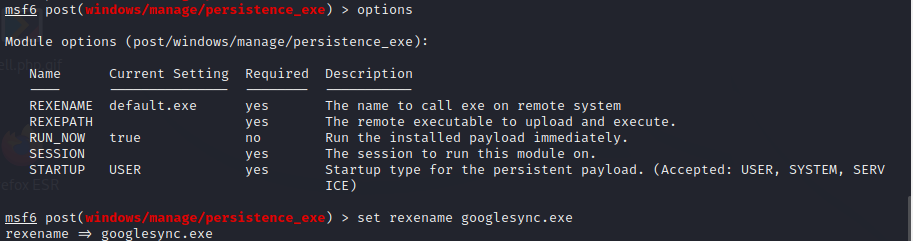
***Metasploit ile Açılışa Exe Yerleştirme***

-Metasploit üzerinde bulunan bir script ile açılışa bir .exe yerleştireceğiz.



- Bu işlem için "persistence\_exe" scriptinden yararlanacağım.

-Ayrıca burada arka planda yüksek yetki ile çalışan bir bağlantıya ihtiyacım vardır.

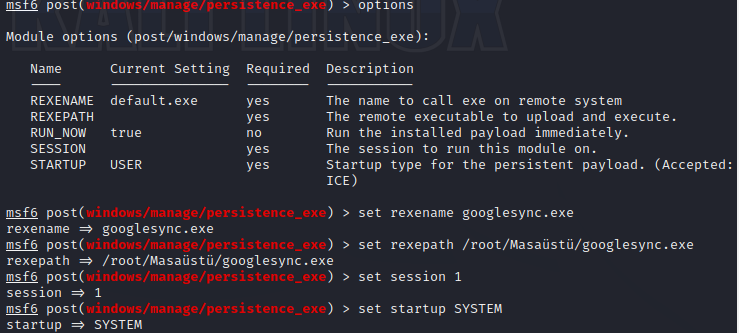


- Ayarlarına geçiş yaptığım da burada arka plana gizlenecek bir .exe ismi belirtiyorum.

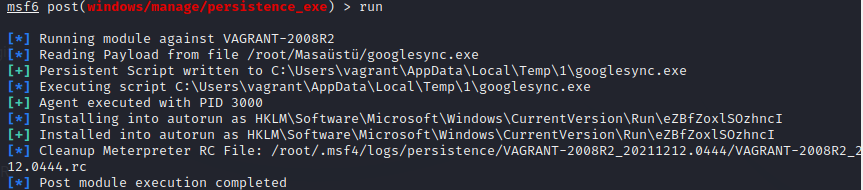
-Burada bir zararlı yazılım yolu istediği için msfvenom aracıma geçiş yapıyorum.



-Msfvenom aracı ile "meterpreter" bağlantısı kurmamı sağlayacak "googlesyn.exe" isimli bir zararlı yazılım oluşturuyorum.



- Gerekli ayarları tam olarak set ettikten sonra işlemi başlatabilirim.



- Manuel olarak gerçekleştirdiğim tüm işlemleri otomatize bir şekilde gerçekleştirdi.