|  |
| --- |
| ***PİVOTİNG*** |
| Kaan Efe Öğüt  *ADLİ BİLİŞİM MÜHENDİSLİĞİ* |
| Penetrasyon testlerinde sürekli karşımıza çıkan Pivoting kavramını sizlere uygulamalar ile açıklama çalışacağım. |

**07.01.2022**

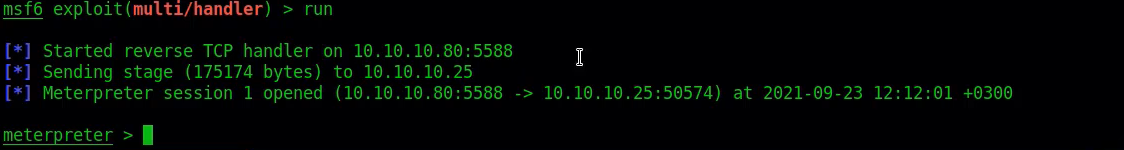
***PİVOTİNG Kavramı***

-Pivoting erişim sağlayamadığımız makinelere onlara erişebilen makineler üzerinden erişme işlemidir.

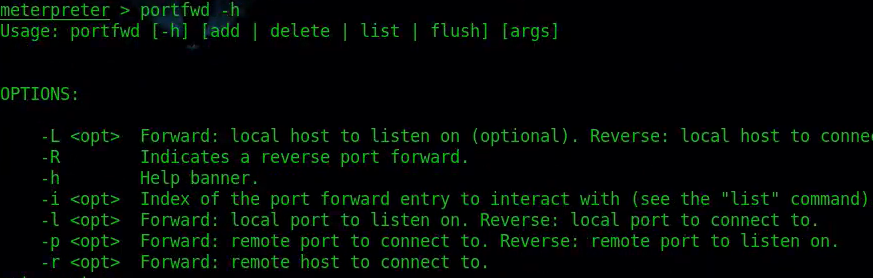
-Bu işlemi CTF üzerinde çokca kullanmaktayız.

-Bu terimi bir örnek ile göstermek istiyorum.Daha öncede kullandığımız Server ve Client üzerinden gideceğim.

-Burada amacım Server'a erişim sağlamak fakat buraya erişim için A.bilgi kullanıcısına erişim sağlayıp ardından servera erişim sağlayacağım.

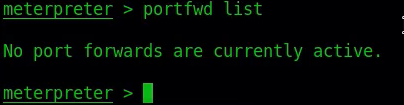


- Öncelikle a.bilgi kullanıcısın da bir shell alıp işlemlerime başlayacağım.



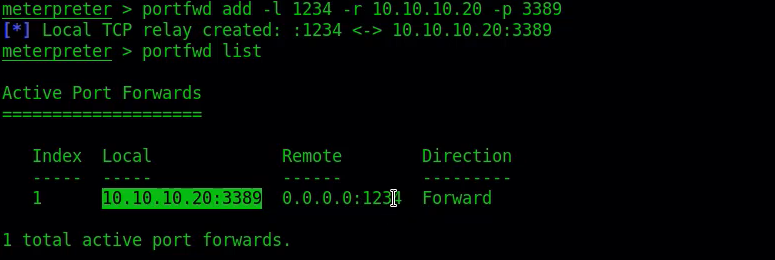
- "portfwd" ile işlemlerime devam edeceğim.

-Portwd yönlendirilmiş port bilgileri üzerinden Pivoting yapmama imkan sağlayabilir.



- "portfwd list" komutu ile öncelikle yönlendirme varsa listelemesini istiyorum.

-Burada bir yönlendirme işlemi görüntüleyemedim.



- Bilgiişlem üzerine "1234" portu üzerinden gelen paketleri 10.10.10.20 üzerinde bulunan 3389 portuna yönlendiriyorum.



- Burada hemen aklıma "rdesktop" üzerinden işlem gerçekleştirmek geliyor fakat burada hata alıyorum.

-Hata almamın sebebi tünellemeden dolayıdır.



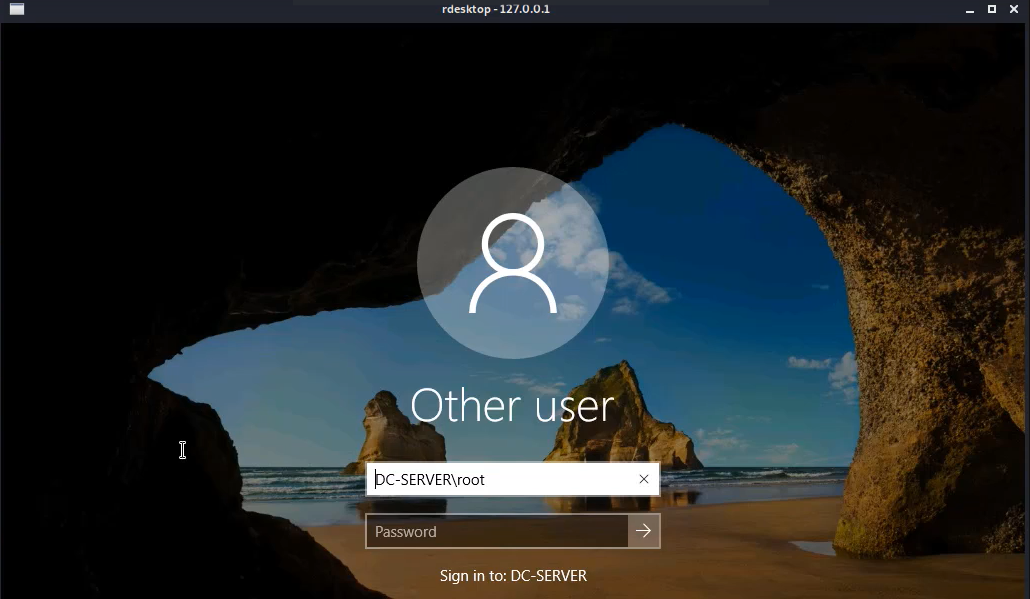
- "netstat -l" komutunu çalıştırdığım da kendi cihazım üzerinde ki yönlendirmeleri görüntüleyebiliyorum.

-Burada kendi IP adresim ve belirttiğim port üzerinden bir yönlendirme olduğunu görüntülüyorum.

-Kendi makinem üzerinde bir bağlantı oluştuğu için oradan gönderdiğim istek aslında ahmet makinesine düşecektir.



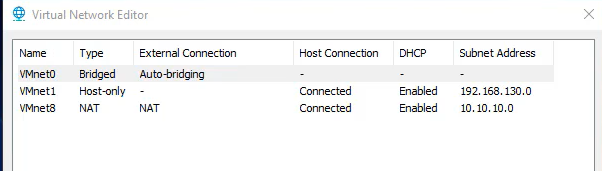
- "rdesktop" komutu ile kendi temsili Ip adresim üzerinden bir yönlendirme gerçekleştirdim.



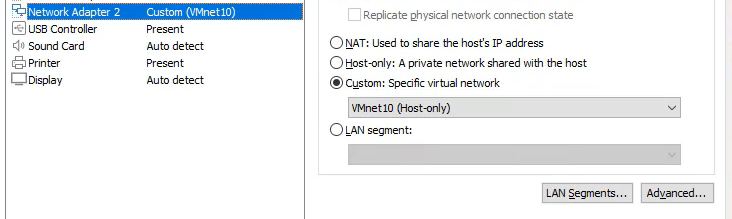
- Ardından oluşturduğum yönlendirme işlemini de başarıyla kullanıp Rdesktop üzerinden server'a bağlantı kurabildim.

***Yeni Network Oluşturma***

-Pivoting işlemi için bir başka olasılıkta Server içerisinde bulunan farklı Networkler üzerine erişim sağlamak.

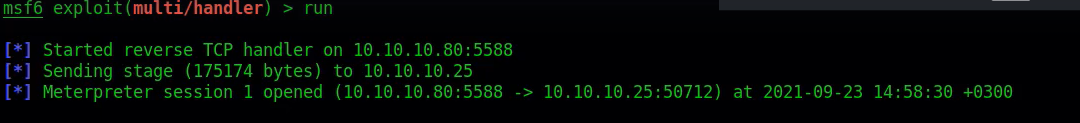


- Daha önce kurduğum server için Virtual Machine üzerinden yeni bir Network oluşturuyorum.



- Oluşturduğum Network'e Clientlerimi bağlıyorum ve burada farklı 2 network varmış gibi bir senaryo oluşturdum.

***Bilinmeyen Diğer Ağların ve Hedeflerin Tespiti***



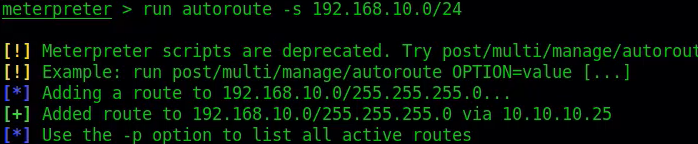
Öncelikle yine BİLGİİSLEM-PC üzerine bir meterpreter bağlantısı kuruyorum.

-Burada oluşturduğum Embed-Trojanları kullanabilirim.



- Meterpreter bağlantısı üzerinde "ipconfig" komutunu çalıştırıyorum.

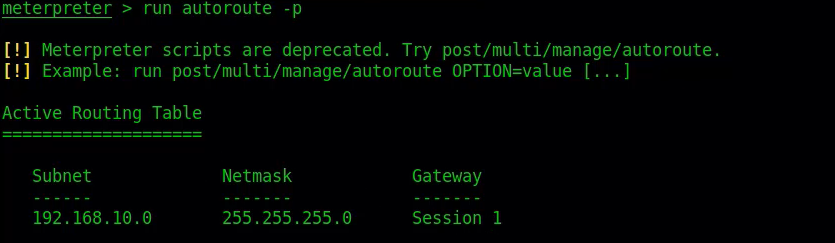
-Burada IP adreslerini görüntülediğim de iki farklı IP adresi türü olduğunu görüntülüyorum aklıma direk farklı 2 Network olabileceği geliyor.



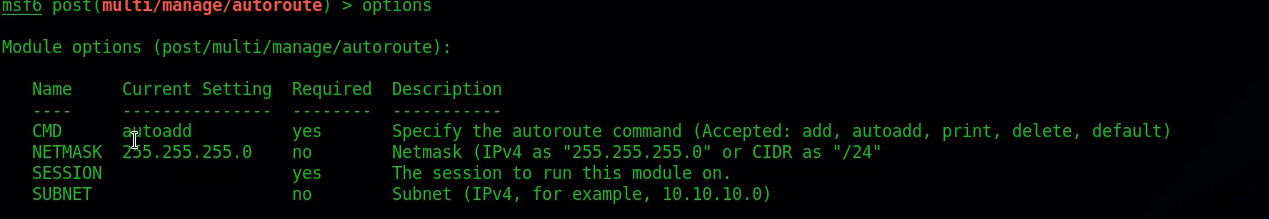
- Burada meterpreter üzerinde bulunan "autoroute" scriptini kullanarak kendime bir yönlendirme alacağım.

-"run autoroute -s 192.168.10.0/24" komutu ile bir yönlendirme işlemi gerçekleştiriyorum.

-Bu aracın kullanım süresi bitmiş ise "post/multi/manage/autoroute" kullanılabilir.

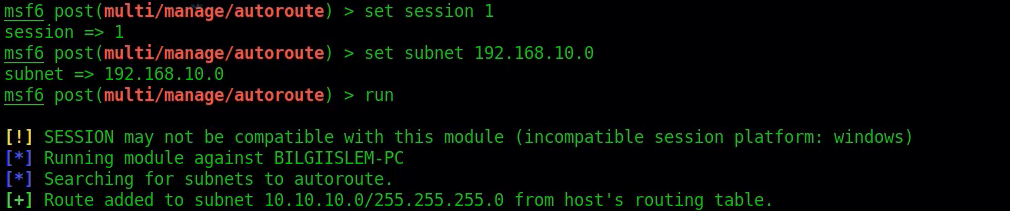


- "run autoroute -p" komutu ile bu ayarı kalıcı hale getirebilirim ve daha önceki kuralları da görüntüleyebilirim.



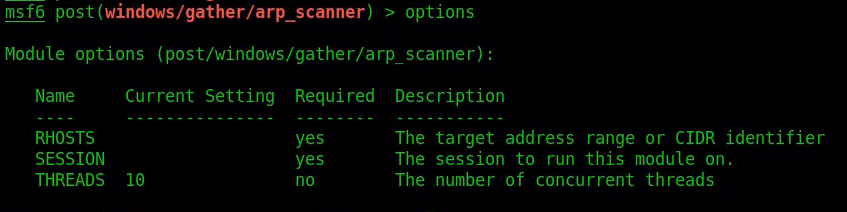
- Metasploit içerisinde bulunan "post/multi/manage/autoroute" exploiti ile de işlem sağlamak istiyorum.

-Exploiti başlatıyorum ve burada daha önceden bir session elde etmiş olmam gerekmektedir.



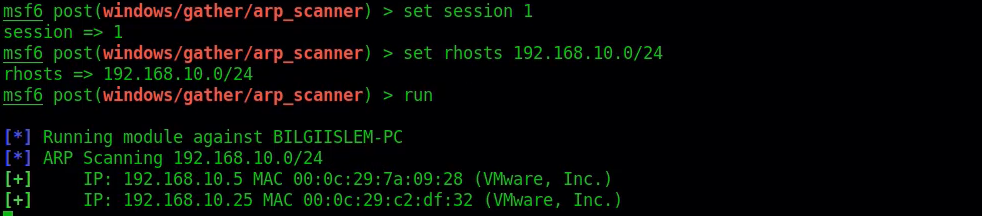
-Gerekli ayarları set ediyorum ve çalıştırıyorum.

-Burada IPtable içerisine yönlendirmemi ekleyebildim.



- Metasploit içerisinde bulunan "Arp-Scanner" exploitini kullanarak diğer ağlarda bulunan cihazlar hakkında bilgi toplamaya çalışacağım.

-Exploitin istediklerini görüntülüyorum.



- Arp Scanner exploitini çalıştırıyorum ve ve farklı network üzerinde bulunan cihazlar hakkında da artık bilgi sahibi olabilirim.

-İstediğim cihaz üzerinden işlem gerçekleştirebilirim.