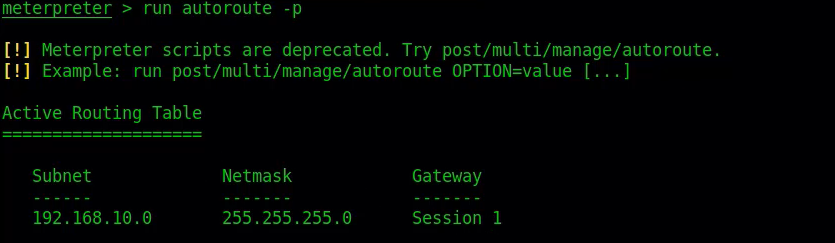
|  |
| --- |
| ***Covering Tracks*** |
| Kaan Efe Öğüt  *ADLİ BİLİŞİM MÜHENDİSLİĞİ* |
| Pentest sırasında yaptığımız saldırılar veya gerçekleştirdiğimiz işlemler sunucu üzerinde kayıt edilmektedir.Bu kayıtların bir kısmının nasıl silinebileceğini sizlere aktaracağım. |

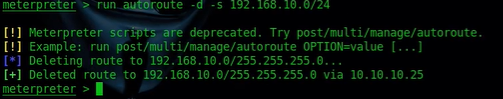
**07.01.2022**

***Route ve Port Yönlendirmelerinin Silinmesi***

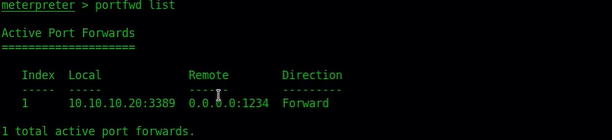
-Server üzerinde yapmış olduğumuz işlemleri geri almamız sisteme sızmamız kadar önemlidir.



- Öncelikle "autoroute" komutu ile oluşturmuş olduğum port yönlendirmesini temizlemek istiyorum.



- "run autoroute -d -s 192.168.10.0/24" komutu ile oluşturduğum yönlendirmeyi silebilirim.



- Bir diğer yaptığım işlem ise "portfwd" ile yönlendirme işlemi bunu list komutu ile görüntüleyebilirim.



- İki farklı yol ile bu yönlendirmeleri silebiliriz.

1.Yol olarak "portfwd delete" komutunu kullanabiliriz.



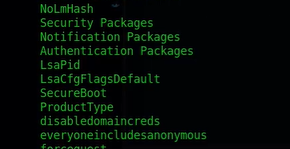
-2.Yol ise Index değeri ile silme işlemidir.

***Registry Girdilerinin Temizlenmesi***

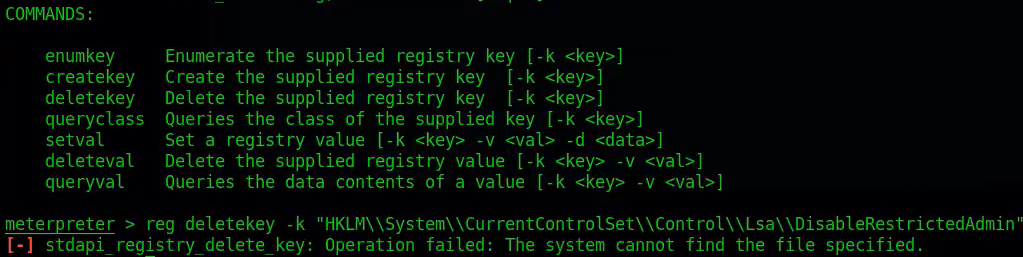
-Yaptığım örneklerde "reg add HKLM\System\CurrentControlSet\Control\Lsa -t REG\_DWORD -v DisableRestrictedAdmin -d 0x0 -f" komutu ile registry içerisine ekleme yapmıştık.

-Yaptığımız eklemeleri;

- Windows üzerinde Registry silme "reg delete HKLM\System\CurrentControlSet\Control\Lsa\DisableRestrictedAdmin" komutu ile temizleme işlemi gerçekleştirebiliriz.



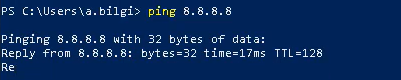
- Meterpreter üzerinde "reg enumkey -k "HKLM\\System\\CurrentControlSet\\Control\\Lsa"" komutu ile Registry üzerinde ki kayıtları görüntüleyebiliriz.



- Silme işlemi içinse;"reg deletekey -k "HKLM\\System\\CurrentControlSet\\Control\\Lsa\\DisableRestrictedAdmin" komutu kullanılabilir.

***Powershell Geçmişini Silme***

-Hedef makinede Trojan veya RDP kullanılarak işlem gerçekleştiğin de bunlar arka planda kayıt altına alınır.

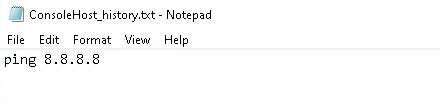


- Bunu bir örnek ile göstermek istiyorum bu sebeple önce;

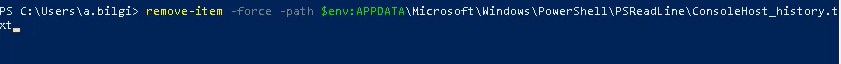
-"ping" komutunu kullanarak bir komut çalıştırıyorum.



-Dizini üzerinde bulunan .txt içerisinde daha önce çalıştırdığım Powershell komutları bulunmaktadır.



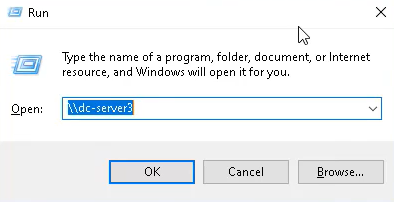
- ".txt" içeriğini de bu şekilde görüntüleyebiliriz.



-".txt" dosyasını silmek bir çözüm olduğu gibi powershell içerisinde "remove-item -force -path $env:APPDATA\Microsoft\Windows\PowerShell\PSReadLine\ConsoleHost\_history.txt" çalıştırdığım bu komut ile de silme işlemi gerçkelştirebilirim.

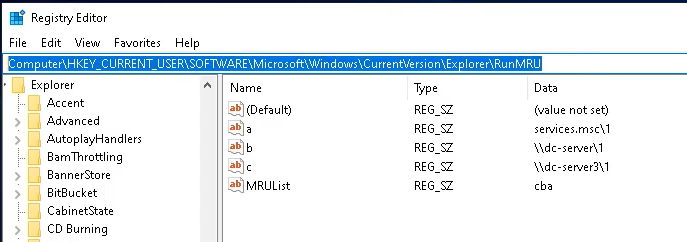
***Run Geçmişinin Temizlenmesi***

-Makine üzerinde çalışırken "Çalıştır(Win+R)" kısmını kullanmışsak burada da yaptığımız aramalar kayıt altına alınmaktadır.



- Çalıştır aracını bu şekilde görüntüleyebiliyoruz.

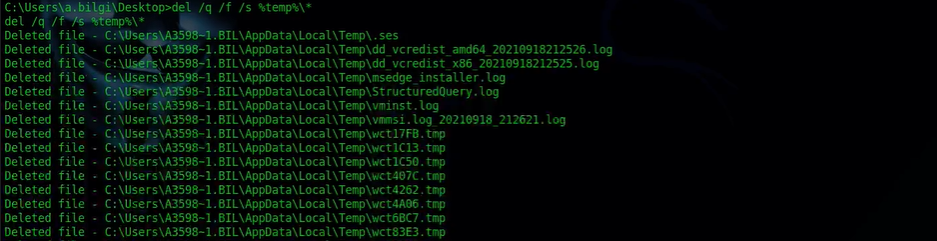
-Ayrıca burada mause ortasını hareket ettirerek daha önceki aramalarımı görüntüleyebiliyorum.



-Registry içerisinde tutulduğu dizinde bulunan kayıtları silerek arama kayıtlarını temizleyebilirim.

***Temp’in Temizlenmesi***

-Pentest aşamalarında genellikle trojan veya kullandığımız zararlı yazılımları bu klasör içerisine enjekte ederiz.



Shell bağlantısı kurduğum Metasploit aracı sayesinde bu dosyayı temizleyebilirim.

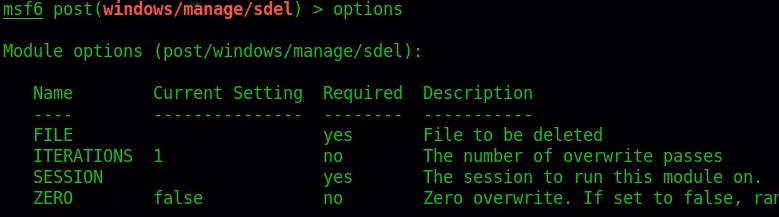
-"del" komutu ile sileceğimi belirtiyorum.

-"/q" komutu ile sessiz bir şekilde işlemi gerçekleştireceğini belirtiyorum.

-"/s" komutu ile de sileceğim dizini belirtiyorum.

***Üzerine yazarak yok etme***

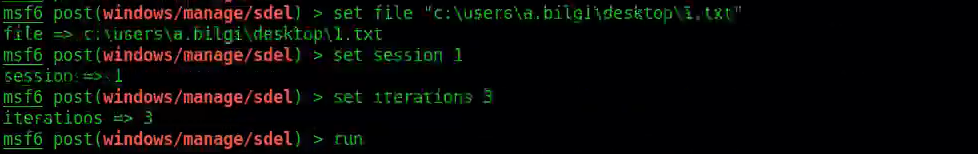
-Bu işlemleri manuel olarak yapmanın haricinde otomatize hale getirip işlem gerçekleştirebiliriz.



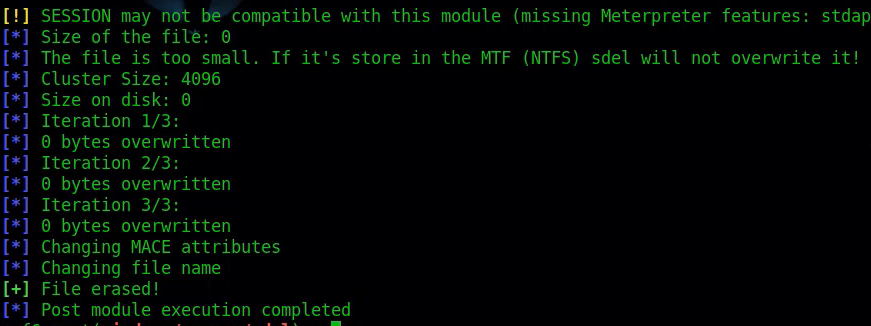
-Bu işlem için metasploit aracında bulunan "sdell" exploitini kullanacağım.

-Bu exploiti kullanmam için yine arka planda çalışan bir session'a ihtiyacım vardır.

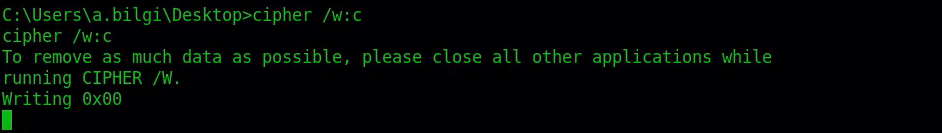
-Exploitin istediği diğer ayarlar ise bu şekildedir.



- Silmek istediğim dosyayı,Kaç kere silme işlemi gerçekleştireceğini ve session'ımı set edip işlemi başlatıyorum.



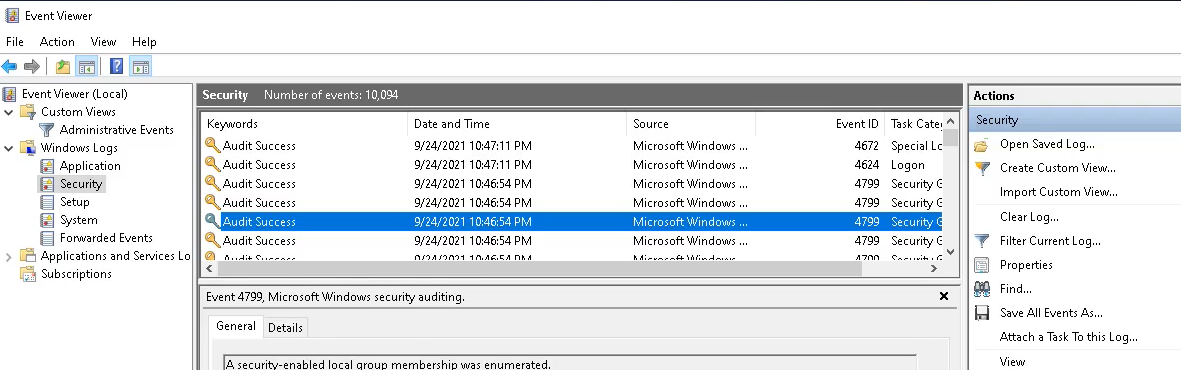
- Ardından işlemi 3 kere gerçekleştirdiğini ve sildiğini görüntülüyorum.



- Bu işlemin haricinde "cipher /w:c" komutu ile harddiskdeki boş olan değerleri kullanılamaz hale getirir.

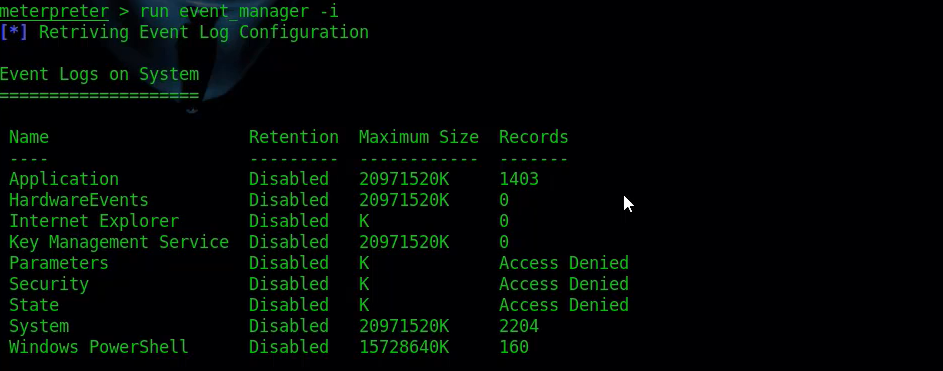
***Log Kayıtlarının Yok Edilmesi***

-Sunucu üzerinde bulunan EventWiewer(Olay Görüntüleyici) ile giriş işlemleri kayıt altına alınabilir.



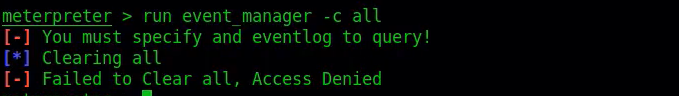
-Kurduğum server üzerinde bulunan Olay Görüntüleyici'yi bu şekilde görüntülüyorum.

-Burada giriş kayıtlarını,kullanıcı hareketlerini de ayrıca görüntüledim.



Bu kayıtları silmek için meterpreter üzerinde "event manager -i" komutunu çalıştırıyorum.

-System üzerinde ki etkinlikleri görüntülüyorum.



- "run eventmanager -c all" komutu ile sistem üzerinde ki kayıtları silmeye çalışıyorum.

-Bu işlem için üstdüzey yetkilere sahip olmak gerekmektedir.

-Eğer meterpreter bağlantımız yoksa Shell üzerinde ayrıca "for /F "tokens=\*" %1 in ('wevtutil.exe el') DO wevtutil.exe cl "%1" " komutunu çalıştırarak log kayıtları temizlenebilir.