METASPOIT : METERPRETER

1)Introduction To Meterpreter :

Meterpreter is metasploit payload that supports penetration testing process with a valuable component.

Meterpreter will run on targer system and acts as an agent within a command and control architecture.

—HOW DOES METERPRETER WORK ?

Meterpreter runs on the target system but is not installed on it. It runs in memory and does not write itself to the disk on the target. This feature aims to avoid being detected during antivirus scans. By default, most antivirus software will scan new files on the disk (e.g. when you download a file from the internet) Meterpreter runs in memory (RAM - Random Access Memory) to avoid having a file that has to be written to the disk on the target system (e.g. meterpreter.exe). This way, Meterpreter will be seen as a process and not have a file on the target system.

Command :

1) getpid : This command return process ID with meterpreter is running.

2) ps : To list the processes which running on the target system.

3)to go a step further and look at DLLs (Dynamic-Link Libraries) used by the Meterpreter process

Command : tasklist /m /fi “pid eq 1304” (for ex :pid = 1304)

2)Meterpreter flavors :

We have used the msfvenom --list payloads command and grepped "meterpreter" payloads (adding | grep meterpreter to the command line), so the output only shows these. You can try this command on the AttackBox.

 The list will show Meterpreter versions available for the following platforms;

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

4)Meterpreter commands :

Meterpreter will provide you with three primary categories of tools;

* Built-in commands
* Meterpreter tools
* Meterpreter scripting

Core commands

* background: Backgrounds the current session
* exit: Terminate the Meterpreter session
* guid: Get the session GUID (Globally Unique Identifier)
* help: Displays the help menu
* info: Displays information about a Post module
* irb: Opens an interactive Ruby shell on the current session
* load: Loads one or more Meterpreter extensions
* migrate: Allows you to migrate Meterpreter to another process
* run: Executes a Meterpreter script or Post module
* sessions: Quickly switch to another session

File system commands

* cd: Will change directory
* ls: Will list files in the current directory (dir will also work)
* pwd: Prints the current working directory
* edit: will allow you to edit a file
* cat: Will show the contents of a file to the screen
* rm: Will delete the specified file
* search: Will search for files
* upload: Will upload a file or directory
* download: Will download a file or directory

Networking commands

* arp: Displays the host ARP (Address Resolution Protocol) cache
* ifconfig: Displays network interfaces available on the target system
* netstat: Displays the network connections
* portfwd: Forwards a local port to a remote service
* route: Allows you to view and modify the routing table

System commands

* clearev: Clears the event logs
* execute: Executes a command
* getpid: Shows the current process identifier
* getuid: Shows the user that Meterpreter is running as
* kill: Terminates a process
* pkill: Terminates processes by name
* ps: Lists running processes
* reboot: Reboots the remote computer
* shell: Drops into a system command shell
* shutdown: Shuts down the remote computer
* sysinfo: Gets information about the remote system, such as OS

Others Commands (these will be listed under different menu categories in the help menu)

* idletime: Returns the number of seconds the remote user has been idle
* keyscan\_dump: Dumps the keystroke buffer
* keyscan\_start: Starts capturing keystrokes
* keyscan\_stop: Stops capturing keystrokes
* screenshare: Allows you to watch the remote user's desktop in real time
* screenshot: Grabs a screenshot of the interactive desktop
* record\_mic: Records audio from the default microphone for X seconds
* webcam\_chat: Starts a video chat
* webcam\_list: Lists webcams
* webcam\_snap: Takes a snapshot from the specified webcam
* webcam\_stream: Plays a video stream from the specified webcam
* getsystem: Attempts to elevate your privilege to that of local system
* hashdump: Dumps the contents of the SAM database

5)Post-exploitation with meterpreter :

Meterpreter provides you with many useful commands that facilitate the post-exploitation phase.

-Help : This command will give you a list of all available commands in Meterpreter.

-Migrate : Migrating to another process will help Meterpreter interact with it. For example, if you see a word processor running on the target (e.g. word.exe, notepad.exe, etc.), you can migrate to it and start capturing keystrokes sent by the user to this process. Some Meterpreter versions will offer you the keyscan\_start, keyscan\_stop, and keyscan\_dump command options to make Meterpreter act like a keylogger. Migrating to another process may also help you to have a more stable Meterpreter session.

Command : migrate <pid>

-Hashdump : The hashdump command will list the content of the SAM database. The SAM (Security Account Manager) database stores user's passwords on Windows systems. These passwords are stored in the NTLM (New Technology LAN Manager) format.

-search : The search command is useful to locate files.

For ex : search –f flag.txt

-Shell : The shell command will launch a regular command-line shell on the target system. Pressing CTRL+Z will help you go back to the Meterpreter shell.

6)Post-exploitation Practical :

Questions :

1)What is the computer name?

Answer : use command : sysinfo : acme-test

2)What is the target domain?

Answer : flash

3)What is the name of the share likely created by the user?

Answer : use exploit : post/window/gather/enum\_shares

In that set session and run it : speedster

4)What is the NTLM hash of the jchambers user?

Answer : use hashdump : 69596c7aa1e8daee17f8e78870e25a5c

5)What is the cleartext password of the jchambers user?

Answer : use crackstation.net : trustno1

6)Where is the "secrets.txt"  file located? (Full path of the file)

Answer : use command : search –f secrets.txt : c:\Program Files (x86)\Windows Multimedia Platform\secrets.txt

7)What is the Twitter password revealed in the "secrets.txt" file?

Answer : KDSvbsw3849!

8)Where is the "realsecret.txt" file located? (Full path of the file)

Answer : c:\inetpub\wwwroot\realsecret.txt

9)What is the real secret?

Answer : The Flash is the fastest man alive