CSC436 Lab 06

Take a screenshot of each of the commands you run in Meterpreter, and save them to a single Word or PDF document. **Please label all of your screenshots!**

This lab should be completed in the CSC436_Exploitation vApp.

Overview

After exploitation of a system, we'll then have a decision on what to do next. Often, we may choose to create a meterpreter session with the target host. This lab will expose you to many of the commands and features of meterpreter.

Get A Session

Using whatever method you choose, get a meterpreter shell on the Windows XP box at 192.168.1.11. You may wish to again exploit MS08-067. You may need to restart your XP VM to get a successful exploit. Be sure you choose a meterpreter payload.

Sysinfo

Run the *sysinfo* command in Meterpreter.

Process List

Run the *ps* command in Meterpreter. The output will be a list of the running processes on the victim. Having a list of processes on the system will become important for migration shortly.

Kill a process

Run the *kill* command to kill a process. For this lab, go ahead and kill the process for vmtoolsd.exe. You'll need to supply the Process ID (PID) to the kill command.

Get Process ID

The *getpid* command will list the process your Meterpreter session is currently connected to. This process will depend on the process that was exploited initially. **Run the *getpid* command. What is the name of the process you are connected to? Note this in your document to submit.**

Migrate

The *migrate* command will migrate your Meterpreter session to another session. Often, we'll want to change the process we are attached to, to a stable process, if it's not already. If we are attached to an internet explorer process, for example, when the user closes IE, our shell will be closed as well. **Run the *migrate* command, and migrate to explorer.exe.** The *migrate* command takes a PID as a parameter.

Get The Current Process's Username

The *getuid* command will get the username responsible for the current process. That is, the username associated with the current meterpreter session. This is the level of privileges you have on the system. **Run the *getuid* command**. Note the user we are running as.

Get System

NT AUTHORITY\SYSTEM is the highest privileged user on a Windows machine. Since we migrated to the explorer.exe process, we are now running as the DSU user. The *getsystem* command runs a script in an attempt to escalate privileges. The script will attempt every method available to it to run a privesc exploit. **Run the *getsystem* command**.

Keystroke Logging

To log keystrokes, you must be attached to the explorer.exe process. Verify you are running under that process. **Use the *keyscan_start* command** to begin recording keystrokes. Move over to your Windows XP VM, and type some things. **Use the *keyscan_dump* command to dump the currently captured keystrokes. Use the *keyscan_stop* command** to stop the capture of keystrokes.

User Interface Control

The *uictl* command allows you to disable or enable the keyboard or mouse. **Run the *uictl disable keyboard*** command to disable keyboard input. Attempt to type in a notepad document on the Windows XP machine. **Run the *uictl enable keyboard*** command to enable keyboard input. Verify you are able to type in the notepad document. You can additionally optionally try to disable the mouse.

Password Hashes

Use the *hashdump* command to display the native hashes for the system. We'll talk later in the semester how we can use these hashes.

Enumerate Desktops

Run the *enumdesktops* command to enumerate available desktops on the system. This can include remote connections as well. Default is the desktop/screen a user is logged into. Disconnect is the screensaver, or locked window. Winlogon is the login screen.

Currently Active Desktop

Use the *getdesktop* command to display the desktop that is currently active. A majority of the time this will be the Default desktop on session 0. If you wanted to use the keyboard sniffing to grab a password during login, you'd need to change the active desktop to 0\WinSta0\WinLogon

Idle Time

Use the *idletime* command to see how much time the user has been inactive. This could be useful for finding if the user is sitting at the computer, or it is just idle.

Meterpreter Scripts

A number of scripts are prepackaged with Meterpreter. Do a bit of research on the scripts here: https://www.offensive-security.com/metasploit-unleashed/existing-scripts/. **Select one script, and run it using the *run* command**.

Command Shell

Run the *shell* command to get an interactive shell on the target machine. For Windows, this will put you in the command prompt. Run the *exit* command to close the shell and return to meterpreter.

Clear Event Logs

Use the *clearev* command to clear the event logs on the Windows system. This will clear previous entries in these logs, though this isn't very stealthy.

Execute a File

The *execute* command can be used to execute a file on the target. You may wish to do things such as start an FTP server, an FTP client, create a backdoor using netcat, or any number of things. **Use the *execute* command to spawn a calculator**. *execute –f calc.exe*

Webcams

Use the *webcam_list* command to see if there are any webcams on the system. If there are, you can run the *webcam_snap* command to take a snapshot, and the *record_mic* command to record for a specified amount of time.

Search

The *search* command allows you to search the remote machine for specific files by supplying the –f option. **Search for the SAM file by running the *search –f SAM* command.**

Local Directory Traversal

You can use the following commands to traverse directories on your local (Kali) system:
lcd changes the local working directory
lpwd gets the local working directory
getlwd identical to *lpwd*

Downloading and Uploading Files

Use the *download* command to download the changes.txt file from the desktop of the target system. You may first need to use the *cd* command to change to the Desktop folder. You can upload files using the *upload* command as well.
download <srcFile> <destFile> (If destination is not supplied, it will default to the current directory)
upload <srcFile> <destFile>

Edit the Registry

You can use the *reg* command to interact with the target's registry. **Run the *reg* command** to see its usage.

Backgrounding Meterpreter

Run the *background* command to put the Meterpreter session in background mode. **Use *sessions -l*** to list the current sessions. **Use *sessions –i <sessionID>*** to interact with a backgrounded session.

Reboot and Shutdown

Use the *reboot* command to reboot the target system without warning the user. You can also use the *shutdown* command to shut down the system. If the reboot or shutdown fails, you may need to migrate to svchost.exe