**ITA144-ETHICAL HACKING**

**NMAP**

**Exp no: 1**

**Aim:** To perform Nmap scan by using kali Linux.

**Procedure:**

Step 1: Open Nmap from Kali Linux

Step 2: Perform different types of scans

(Tcp, Udp, Ack, Syn, Fin, Null, Xmas, Rpc, Idle)- scan types

**Scanning Techniques**

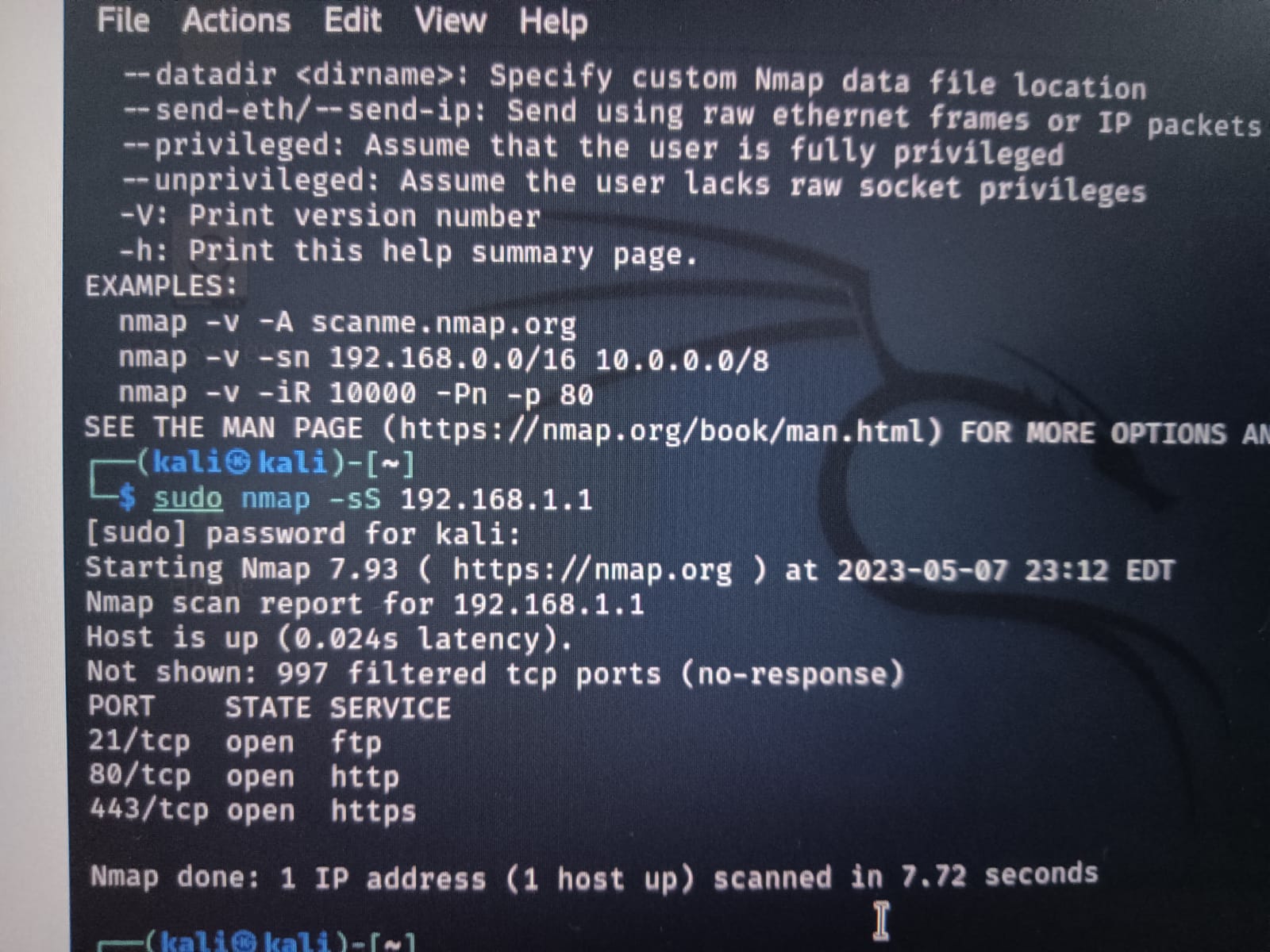
|  |  |  |
| --- | --- | --- |
| **Flag** | **Use** | **Example** |
| **-sS** | **TCP syn port scan** | **Nmap -sS 192.168.1.1** |
| **-sT** | **TCP connect port scan** | **Nmap -sT 192.168.1.1** |
| **-sU** | **UDP port scan** | **Nmap -sU 192.168.1.1** |
| **-sA** | **TCP ack port scan** | **Nmap -sA 192.168.1.1** |

Step 3:

To perform host discovery

|  |  |  |
| --- | --- | --- |
| -Pn | only port scan | nmap -Pn192.168.1.1 |
| -sn | only host discover | nmap -sn192.168.1.1 |
| -PR | arp discovery on a local network | nmap -PR192.168.1.1 |
| -n | disable DNS resolution | nmap -n 192.168.1.1 |

Output:



Result:

Hence, we have successfully completed the nmap scan using kali Linux.

**BATCH FILE**

**Exp no:2**

**Aim:**

To create a Windows batch file.

**Procedure:**

Step 1: Open a text file, such as a Notepad or WordPad document.

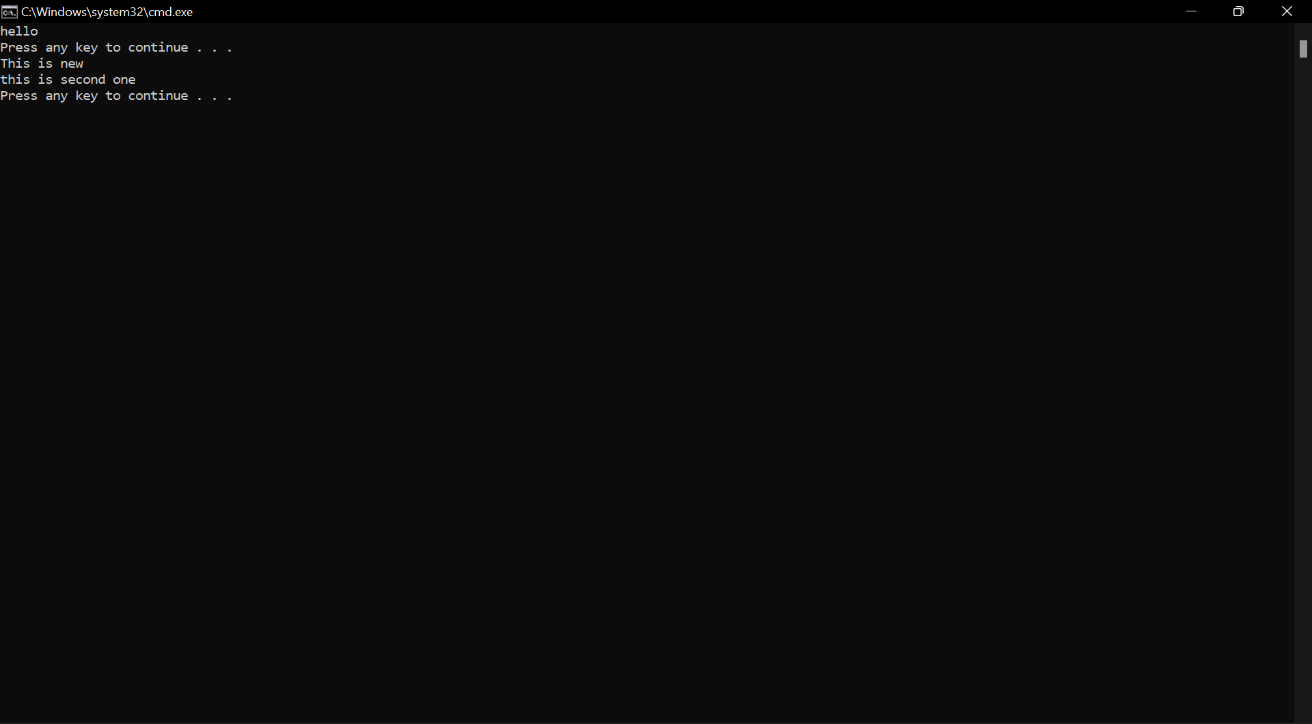
Step 2: Add your commands, starting with @echo [off], followed by, each in a new line, title [title of your batch script], echo [first line], and pause.

Step 3: Save your file with the file extension BAT, for example, test.bat.

Step 4: To run your batch file, double-click the BAT file you just created.

Step 5: To edit your batch file, right-click the BAT file and select Edit.

**Output:**

****

**Result:**

Thus, the Creation and execution of BATCH FILE was successfully completed.

**WHOIS**

Exp No:3

Aim:

To find out the Whois, DNS Records and Diagonstics for particular website by using Whois search.

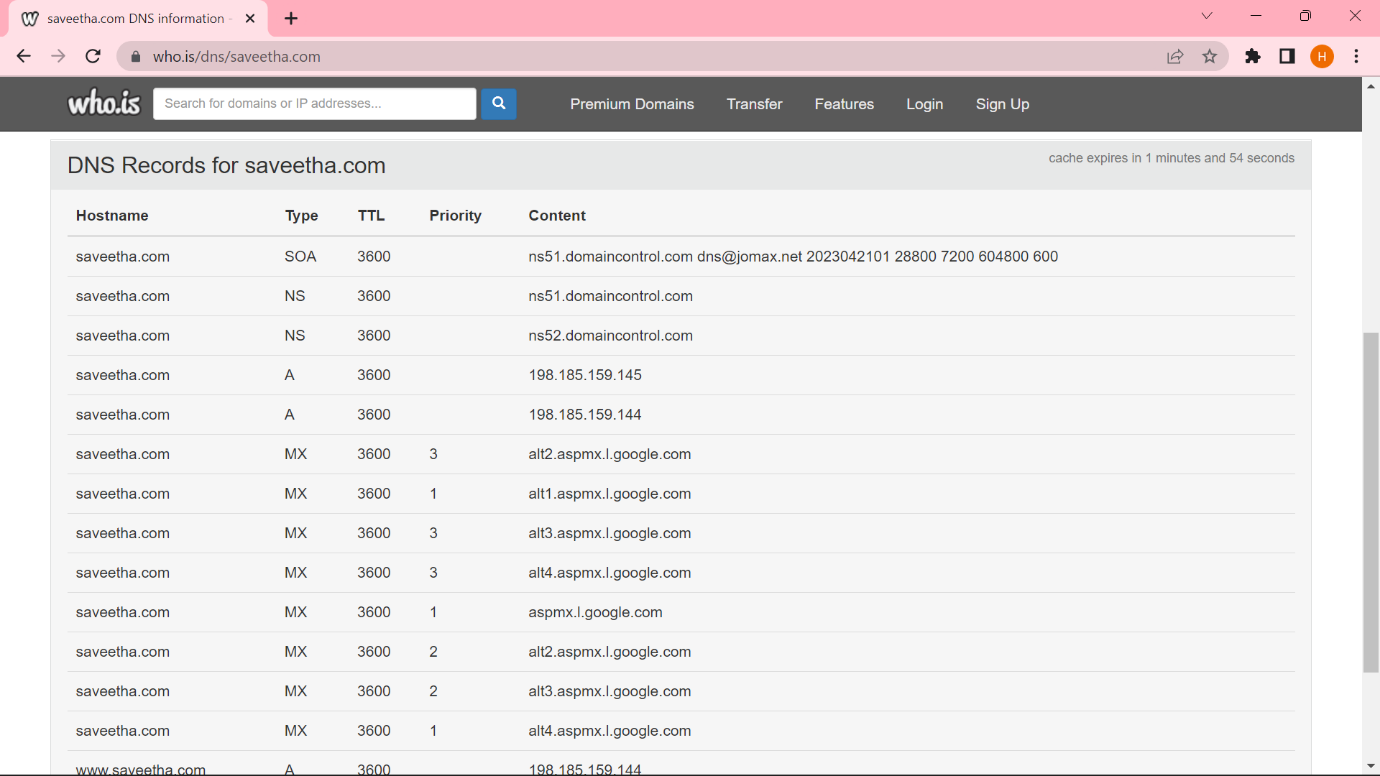
Procedure:

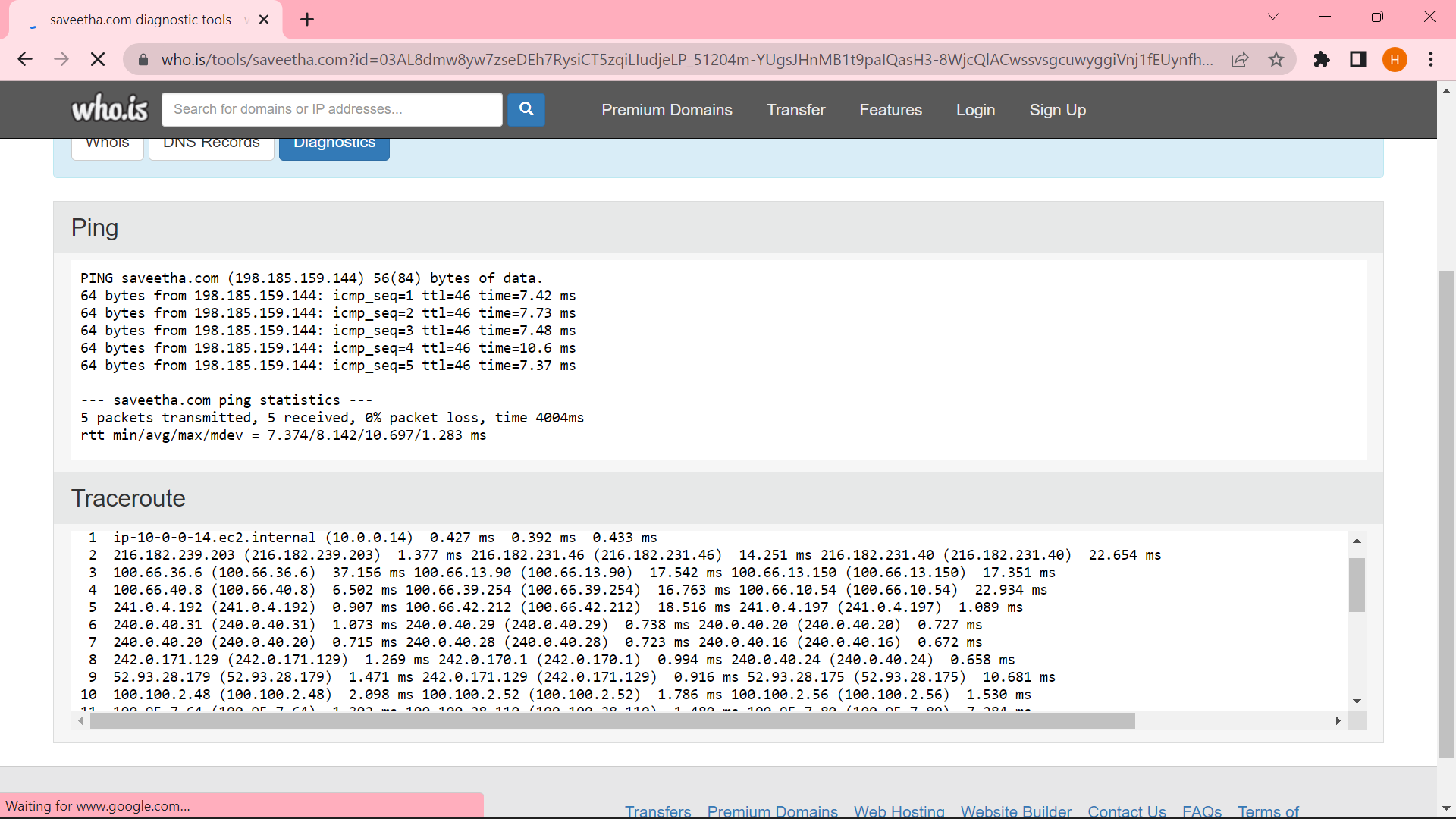
Step1: Open the WHO.is website

Step 2: Enter the website name in search bar and hit the “enter button”

Step 3: Show you information about [www.saveetha.com](http://www.saveetha.com)

**Output:**

****

****

**Result:**

Hence, we have successfully found out the Whois, DNS Records and Diagonstics for saveetha website by using Whois search.

**TRACEROUTE, PING, IFCONFIG, IPCONFIG(WINDOWS), AND NETSAT COMMAND**

**Exp No:4**

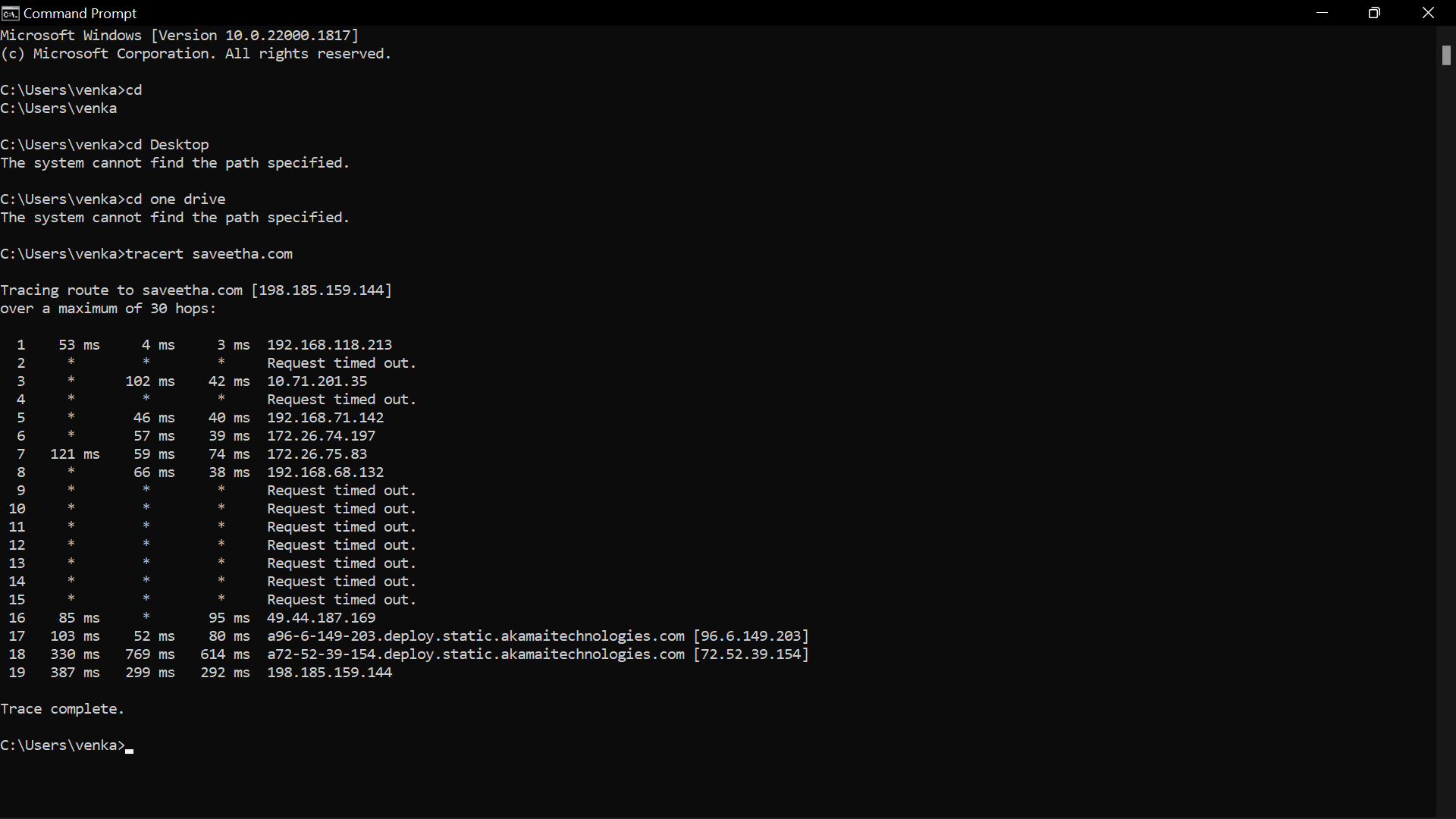
**Aim:**

Using Traceroute, ping, ifconfig (LINUX), ipconfig (WINDOWS), and netstat Command.

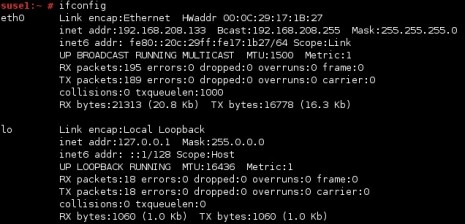
Procedure:

Step 1: Open windows command prompt and Type tracert command and tracert

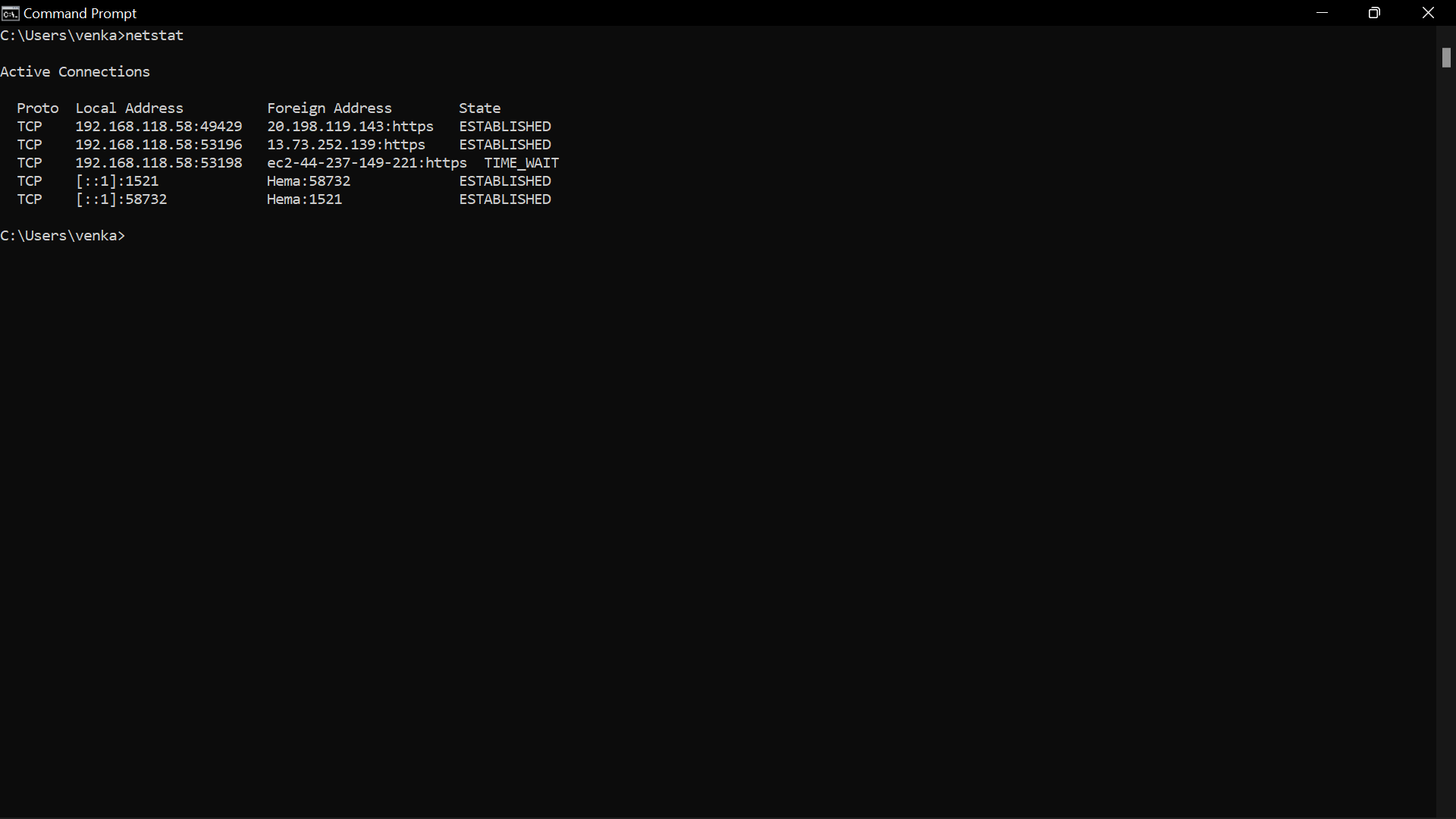
[www.saveetha.com](http://www.saveetha.com/) -> “Enter”

****

Step 2: Type ping command and type IP address press “Enter”.

Step 3: Type ifconfig command

Step 4: Type netset command

****

**Result:**

Hence, we have used Traceroute, ping, ifconfig (LINUX), ipconfig (WINDOWS), and netsat command successfully.

**BOOT SECTOR**

**Exp No:5**

**Aim:**

To implement boot sector virus.

**Procedure:**

**Step 1:** Select Root Terminal Emulator and Update and Upgrade Kali Linux with the

commands sudo apt-get update, 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**

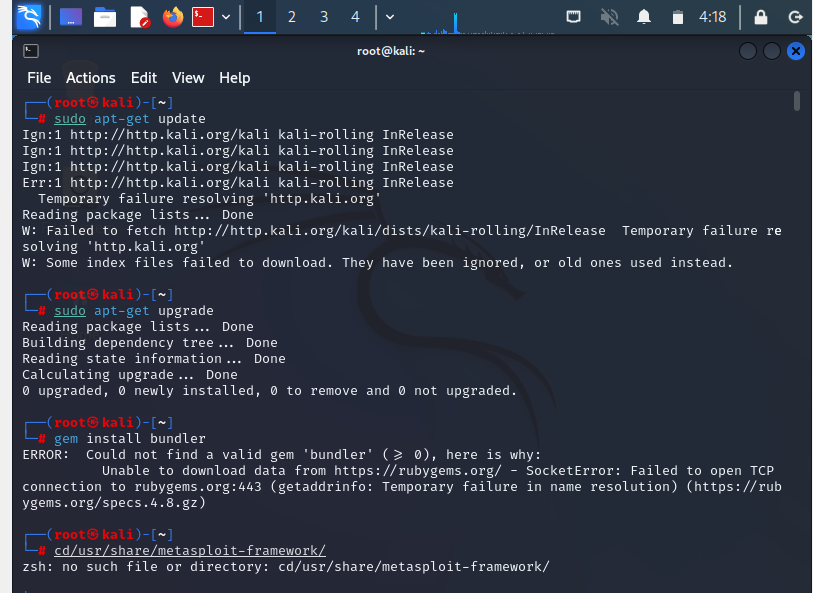
**Step 4:** Choose our payload ,To see a list of payloads : msfvenom -l payloads

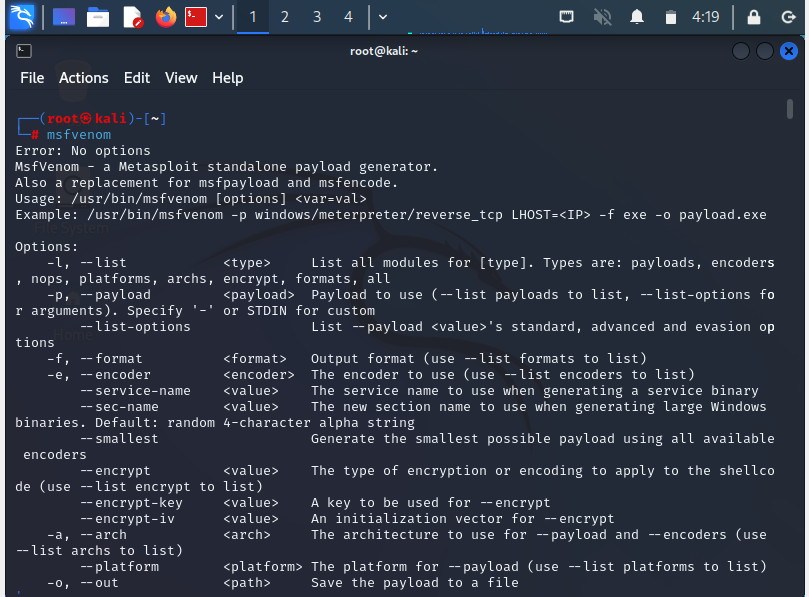
**Step 5:** Customize our payload

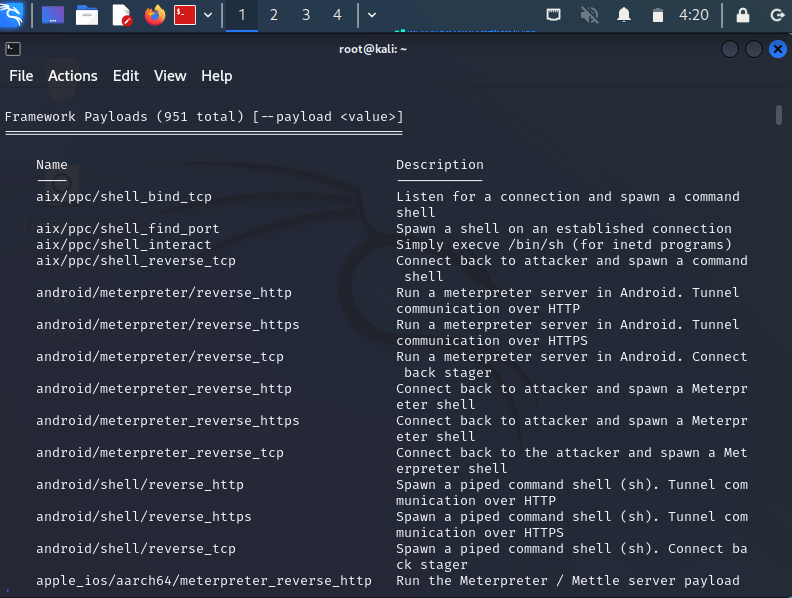
msfvenom –list-options -p windows/meterpreter/reverse\_tcp

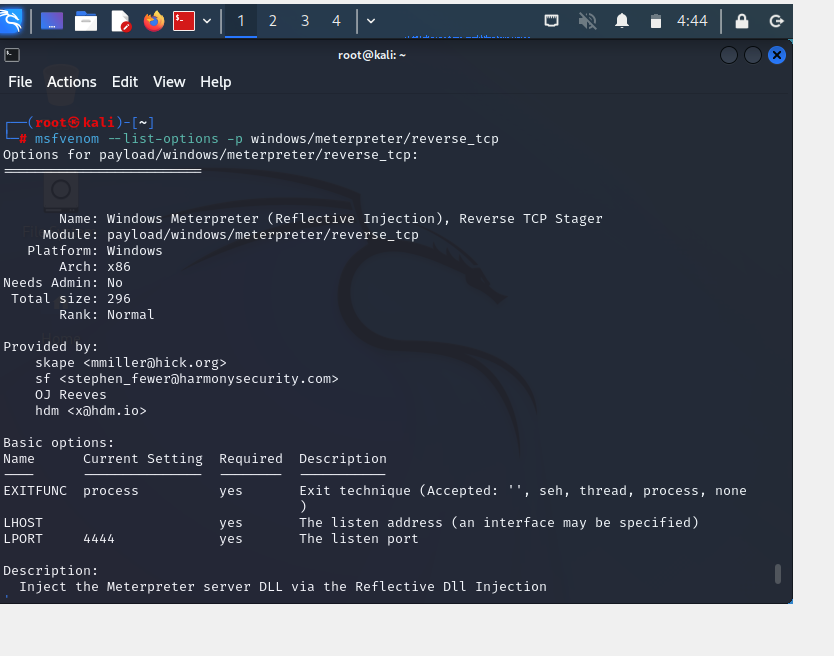
**Step 6:** Generate the virus

**Output:**

****

****

****

****

**Result:**

Thus the implementation of boot sector virus executed successfully.