**ITA14-ETHICAL HACKING**

**LAB MANUAL**

**Exercise No 1:** **Nmap Scan**

**Aim:**

To install and perform Nmap scan (note :- you may use ip address or website name)

**Procedure:**

Step 1: Open Nmap from Kali Linux (Goto Applications->select Information Gathering->select

Nmap)

Step 2: Perform different types of scan

(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 |

Step4:-

**Port Specification**

|  |  |  |
| --- | --- | --- |
| **Flag** | **Use** | **Example** |
| **-p** | **specify a port or port range** | **nmap -p 1-30 192.168.1.1** |
| **-p-** | **scan all ports** | **nmap -p- 192.168.1.1** |
| **F** | **fast port scan** | **nmap -F 192.168.1.1** |

Step 5:-

***Service Version and OS Detection***

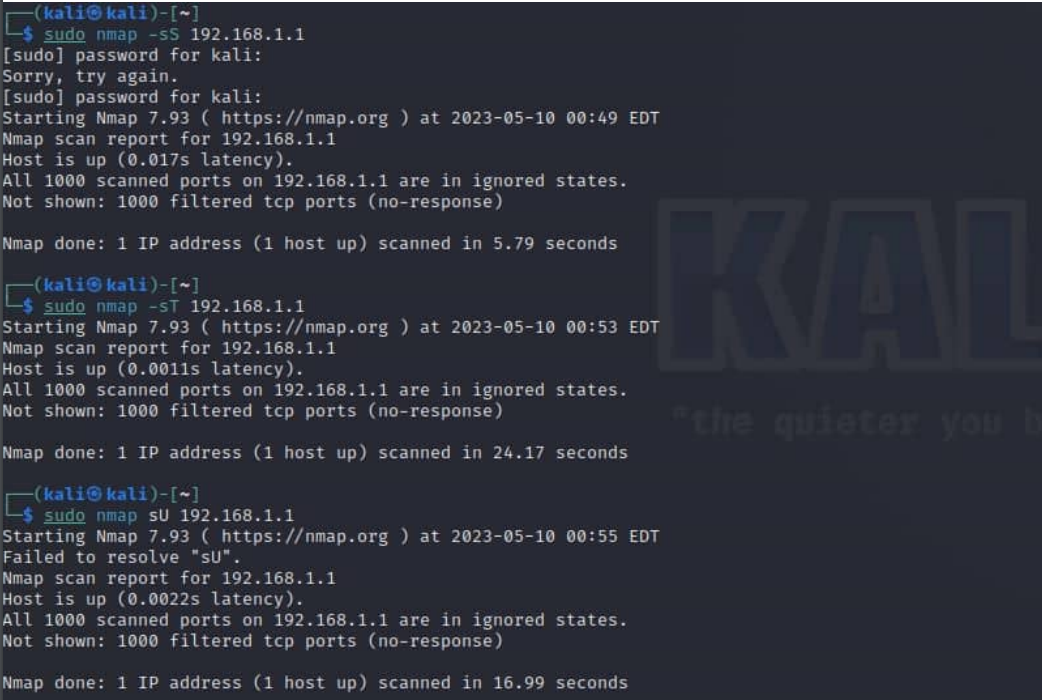
|  |  |  |
| --- | --- | --- |
| Flag | Use | Example |
| -sV | detect the version of services running | nmap -sV 192.168.1.1 |
| -A | aggressive scan | nmap -A 192.168.1.1 |
| -O | detect operating system of the target | nmap -O 192.168.1.1 |

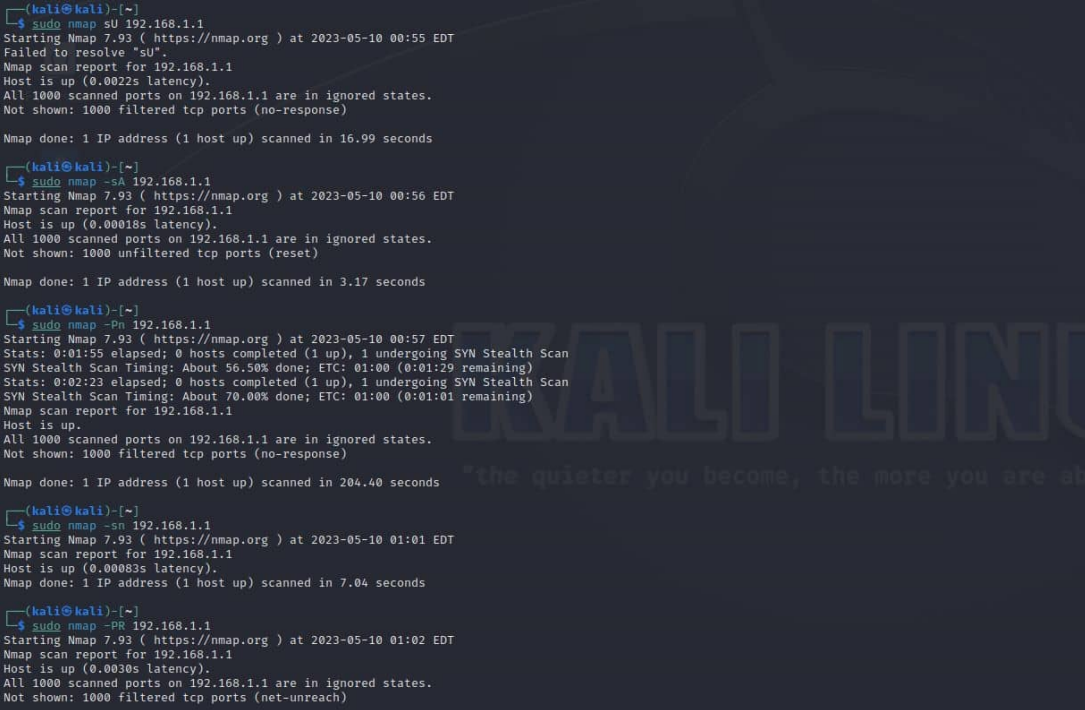
Step 6:-

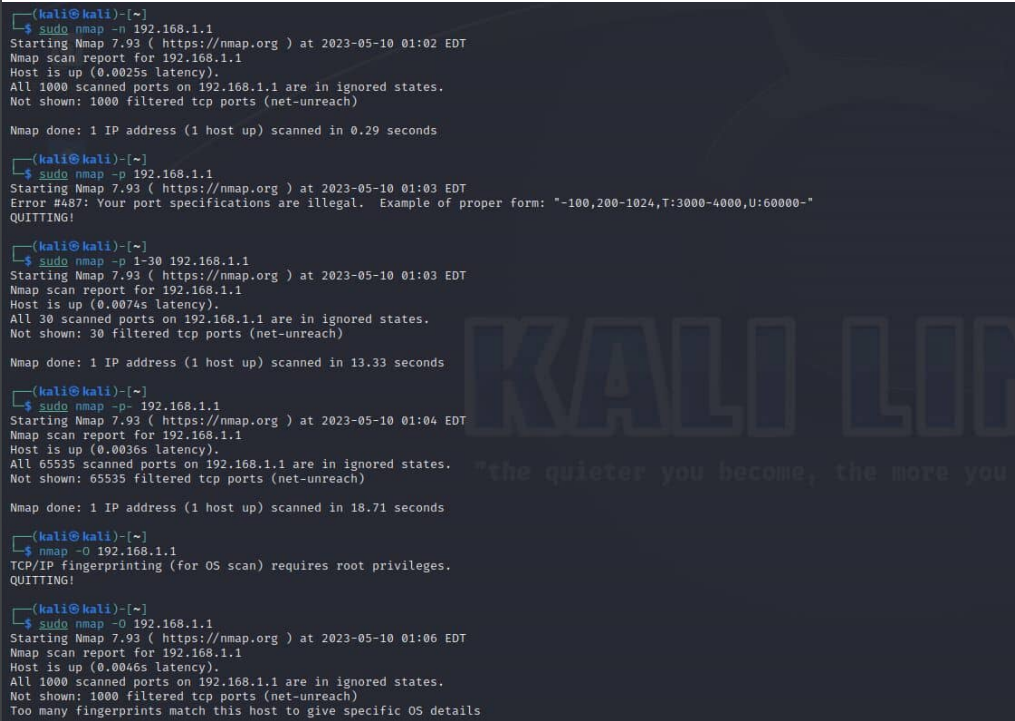
Timing and Performance

|  |  |  |
| --- | --- | --- |
| Flag | Use | Example |
| -T0 | paranoid IDS evasion | nmap -T0 192.168.1.1 |
| -T1 | sneaky IDS evasion | nmap -T1 192.168.1.1 |
| -T2 | polite IDS evasion | nmap -T2 192.168.1.1 |
| -T3 | normal IDS evasion | nmap -T3 192.168.1.1 |
| -T4 | aggressive speed scan | nmap -T4 192.168.1.1 |
| -T5 | insane speed scan | nmap -T5 192.168.1.1 |

Output:







**Result:** Performing nmap scan using ip address is successful.

**EX.NO: 2**

**BATCH FILE EXECUTION**

**AIM:** To create a Windows batch file.

**PROCEDURE:**

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

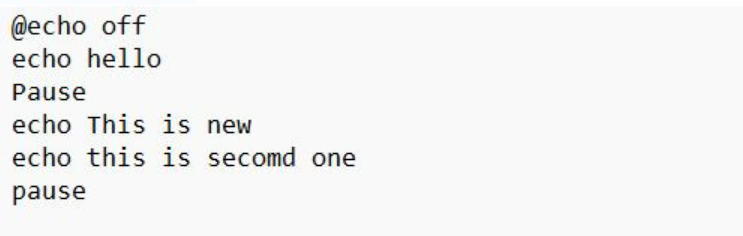
Step 2 : Add your commands, starting with @echo [off], followed by, each in a new line, title [title of your batch script], echo [first line], and pause

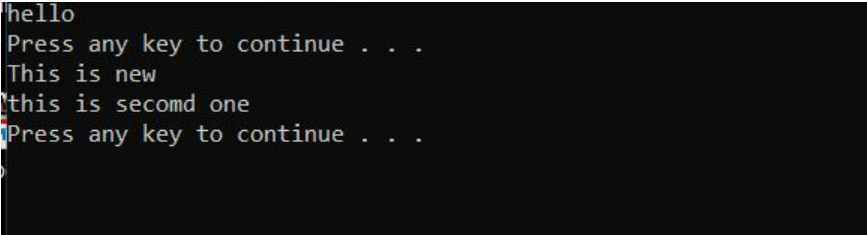
Step 3 : Save your file with the file extension BAT, for example, test.bat.

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. And here's the corresponding command window for the example above: 1.Create a New Text Document A batch file simplifies repeatable computer tasks using the Windows command prompt. Below is an example of a batch file responsible for displaying some text in your command prompt. Create a new BAT file by right-clicking an empty space within a directory and selecting New, then Text Document. 1.CODE Double-click this New Text Document to open your default text editor. Copy and paste the following code into your text entry. >> @echo off >> echo hello >> Pause >> echo This is new >> echo this is second one >> pause 1. TO SAVE a BAT File The above script echoes back the text "Welcome to batch scripting!" Save your file by heading to File > Save As, and then name your file what you'd like. End your file name with the added BAT extension, for example test.bat, and click OK. This will finalize the batch process. Now, double-click on your newly created batch file to activate it. 2.To RUN as BAT File Once you'd saved your file, all you need to do is double-click your BAT file. Instantly, your web pages will open. If you'd like, you can place this file on your desktop. This will allow you to access all of your favorite websites at once.

**OUTPUT-**

****

****

**RESULT-**

Creating a windows batch file is successful.

**Exercise No 3:** **Vulnerability Access Scan Using Nessus**

**Aim :** To Download and install Nessus tool and perform a Vulnerability Access scan in kali Linux Operating systems.

**PROCEDURE-**

Step 1:- <https://www.tenable.com/downloads/nessus?loginAttempted=true>

Step 2: Choose your OS and download , install

Step 3: Once installation is completed it will open in default browser

Step 5:- (click on the proceed to local host)

Step 6:- Please choose the Nessus Expert.

Step 7: Click on continue

Step 8:- Register with your organizational email id

Step 9:- please note down the activation.

Step 10:- set up your username & password

Step 11:-Type username and password

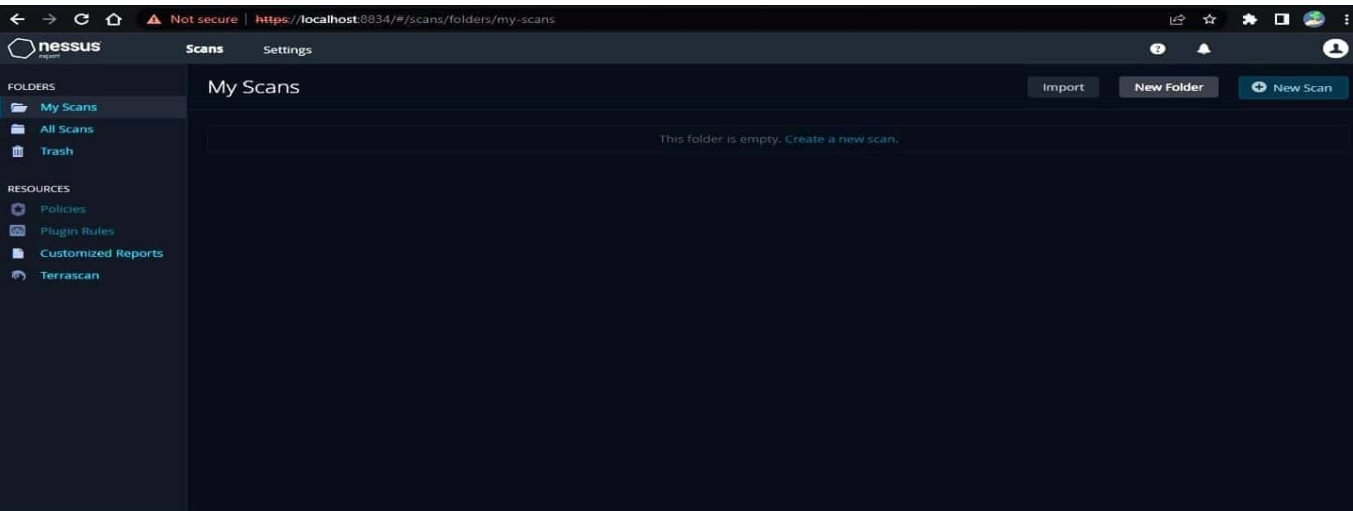
Step 12:- Please wait until download is completed

Step 13: Select My Scans

**OUTPUT-**

****

****

****

**RESULT-**

Using Nessus tool and performing Vulnerability Access scan in kali Linux Operating systems is

successful.

**Exercise No 4:** **Website Penetration Testing**

**Aim:** DEMONSTRATE BOOT SECTOR VIRUS USING KALI LINUX

**Procedure:**

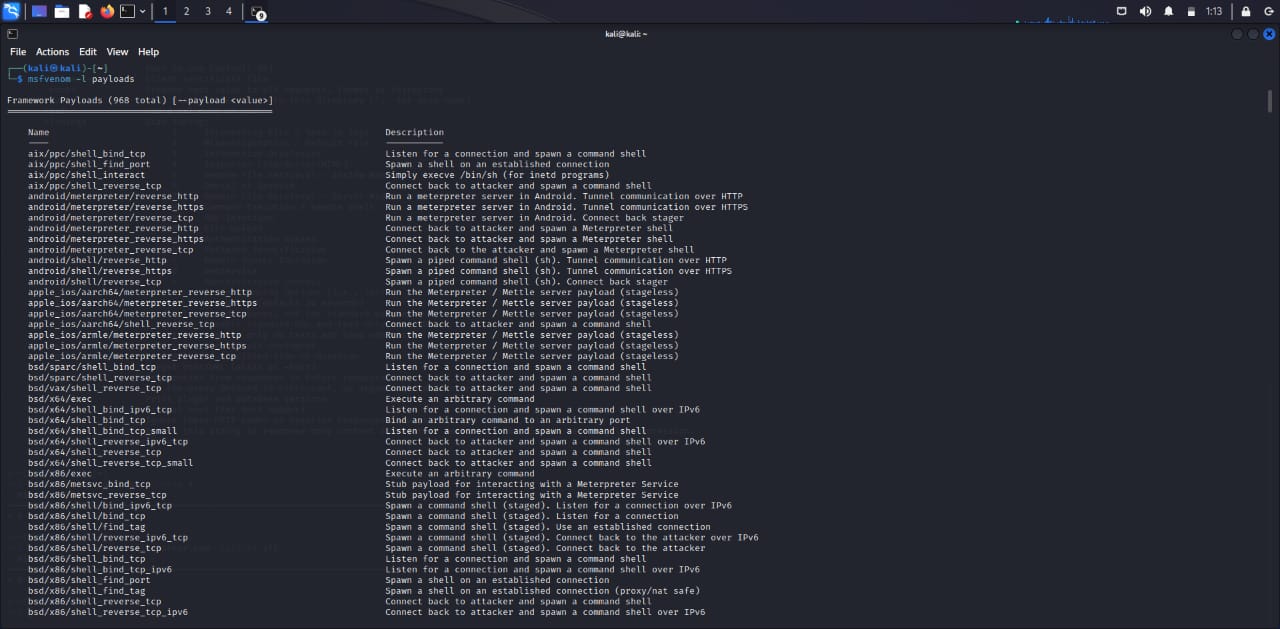
Step 1 – open oracle vmbox

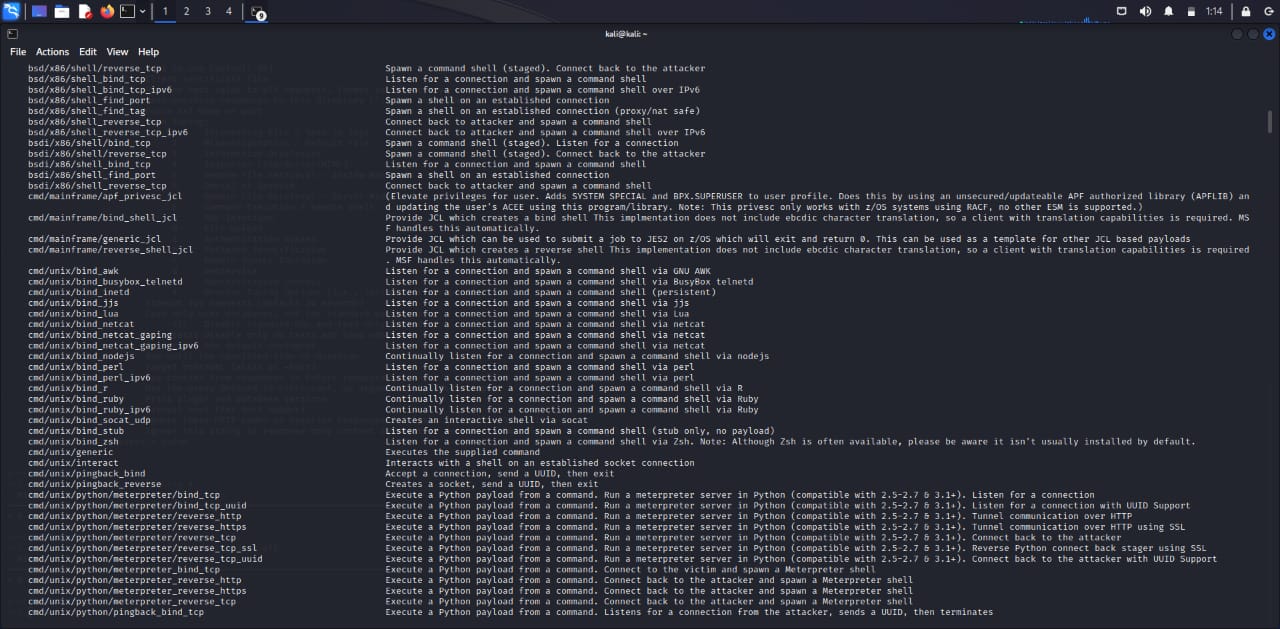
Step 2 – open kali linux

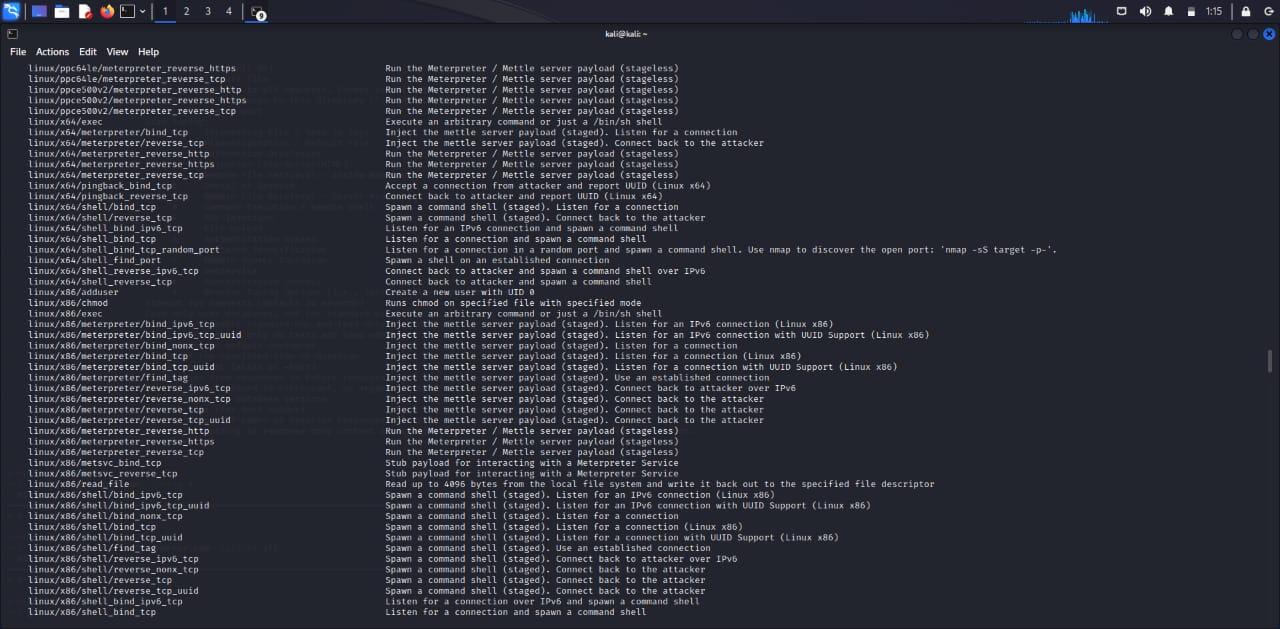
Step 3 – go to terminal

step 4 – enter “msfvenom -l payloads”

**OUTPUT-**







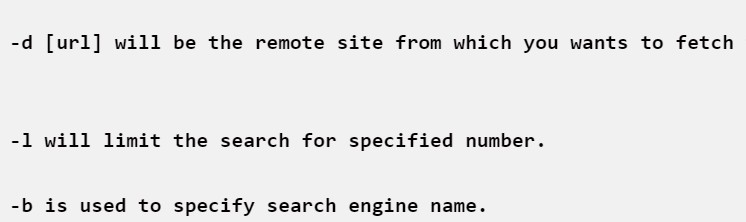
**RESULT-**

Demonstrating boot sector virus offered by Kali Linux is successful.

Exercise No 5: Information gathering using theHarvester

Aim: To demonstrate information gathering using theHarvester

Procedure:

STEP 1: Open Terminal in the kali linux

STEP 2: Run the following command

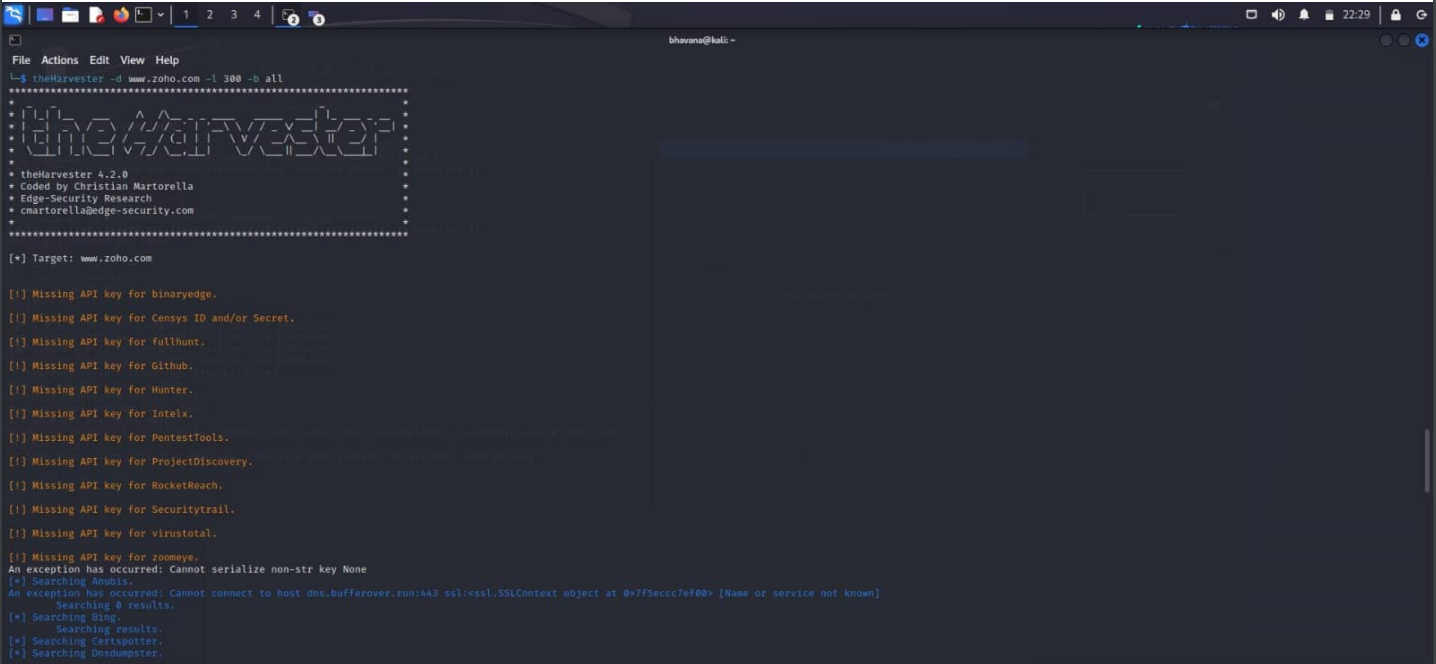
Command: theHarvester -d [www.zoho.com](http://www.zoho.com/) -l

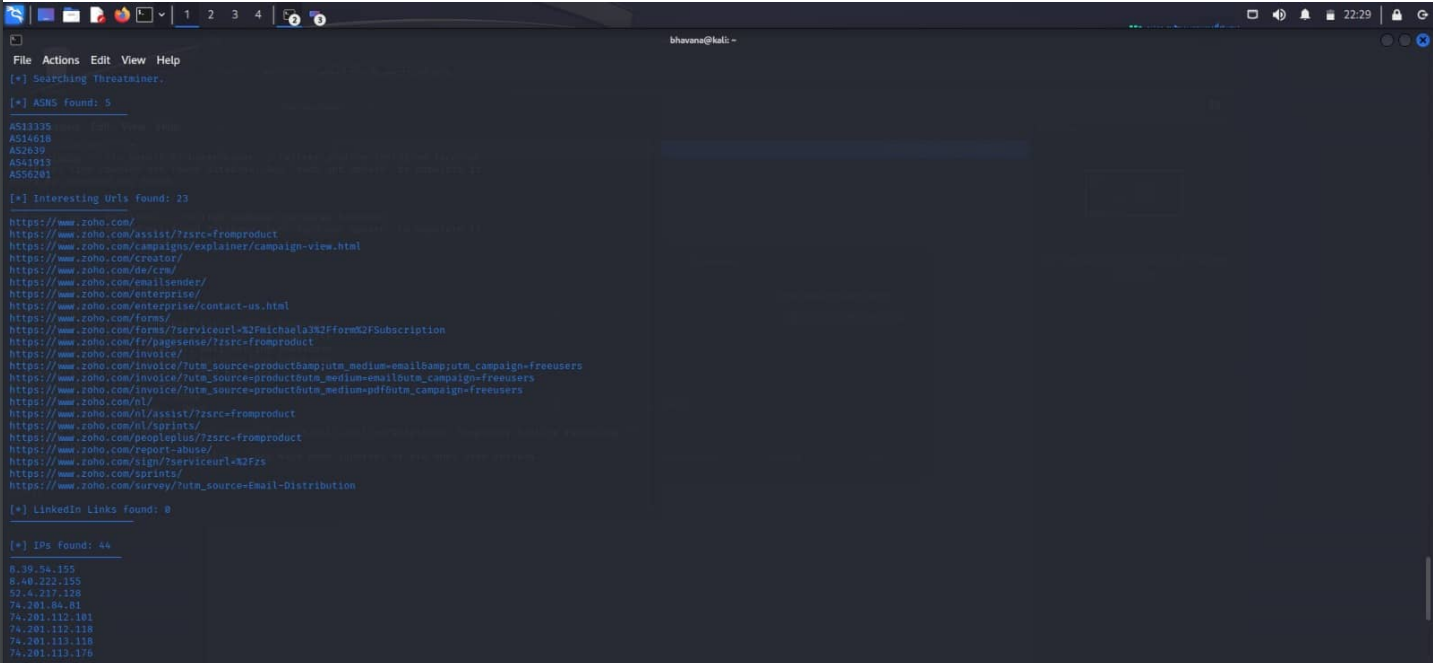
Step 4: run this command “**theHarvester -d** [**www.zoho.com**](http://www.zoho.com/) **-l 300 -b all -f test” and** hit enter

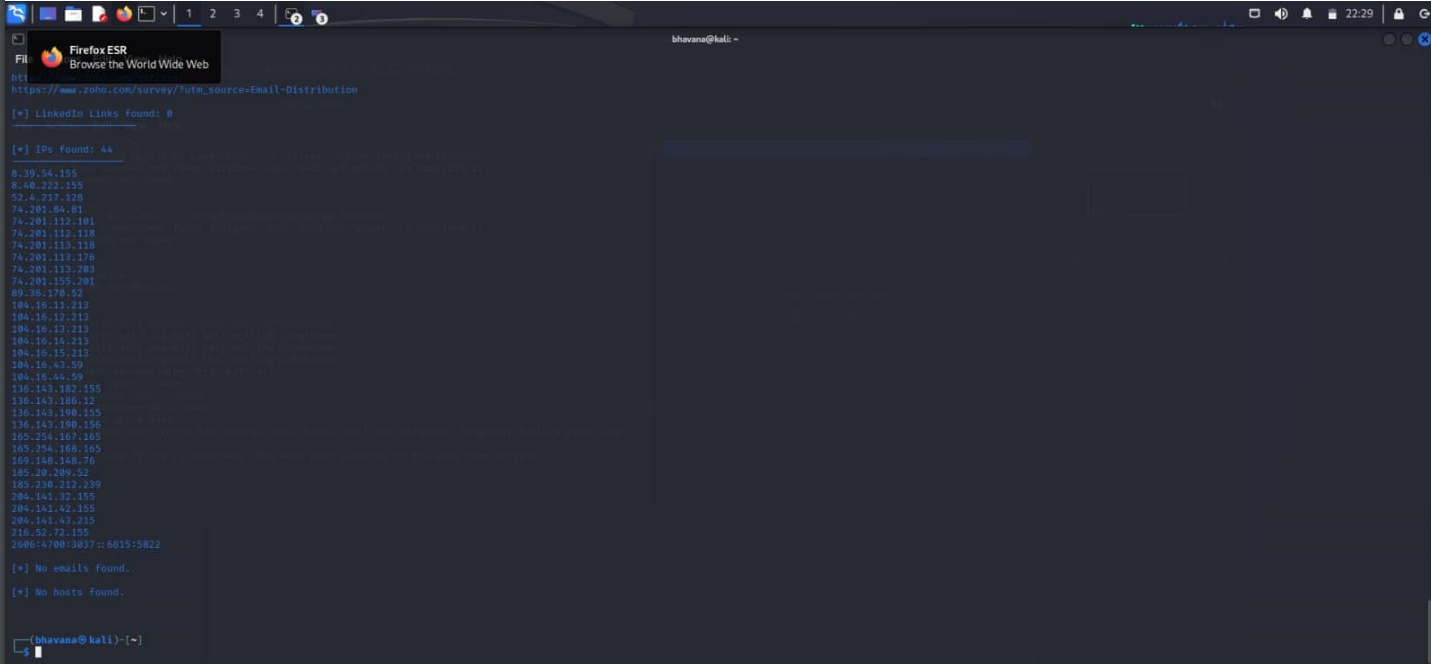
to export the result as html file and xml file.

Step 5: now close the terminal and navigate the home folder and search for test file .

**OUTPUT-**

****

****



**RESULT-**

Demonstrating information gathering using theHarvester is successful.

**Exercise No 6 - Open Source Intelligence Gathering Using OSRFramework**

**Aim:** To Checks for the Existence of a Profile for given user details in different platforms

**Procedure:**

Step 1: Log into kali linux machine

Step 2: Launch a command line terminal by clicking on terminal icon from taskbar

Step 3: Usufy.py checks for the existence of a profile for given user details in different

platforms

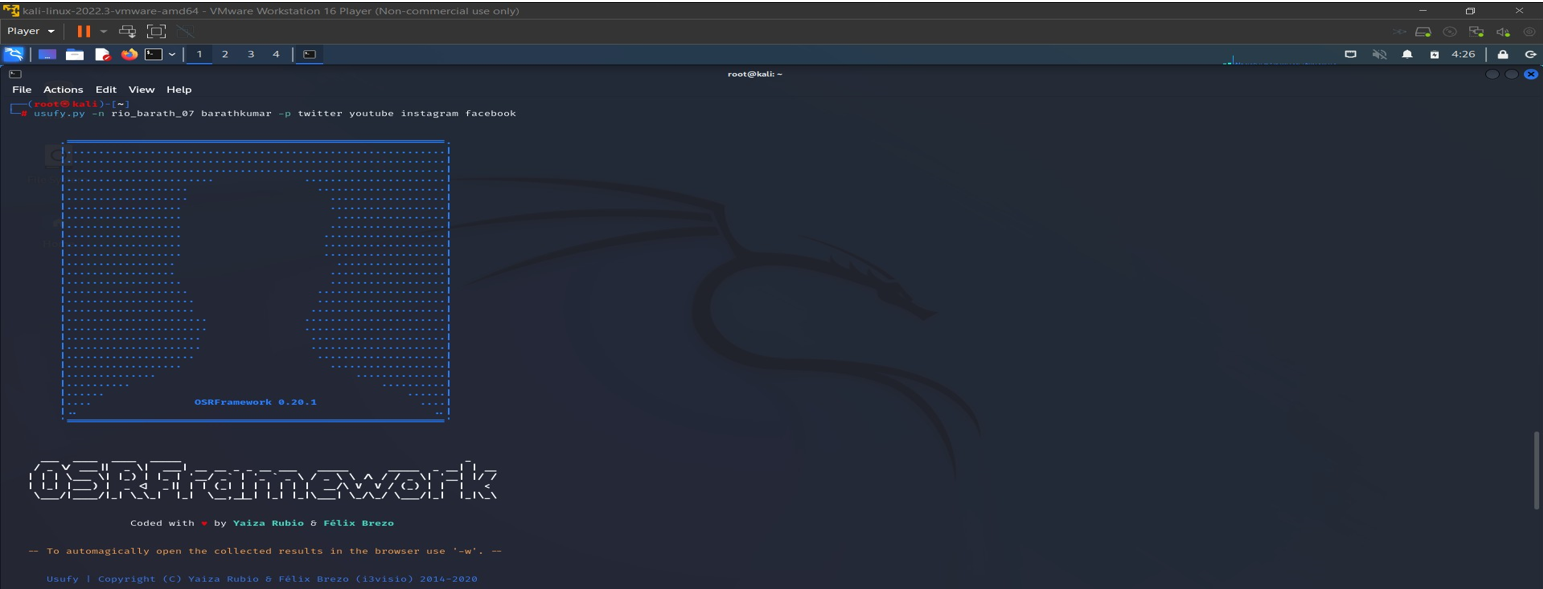
**Command:**

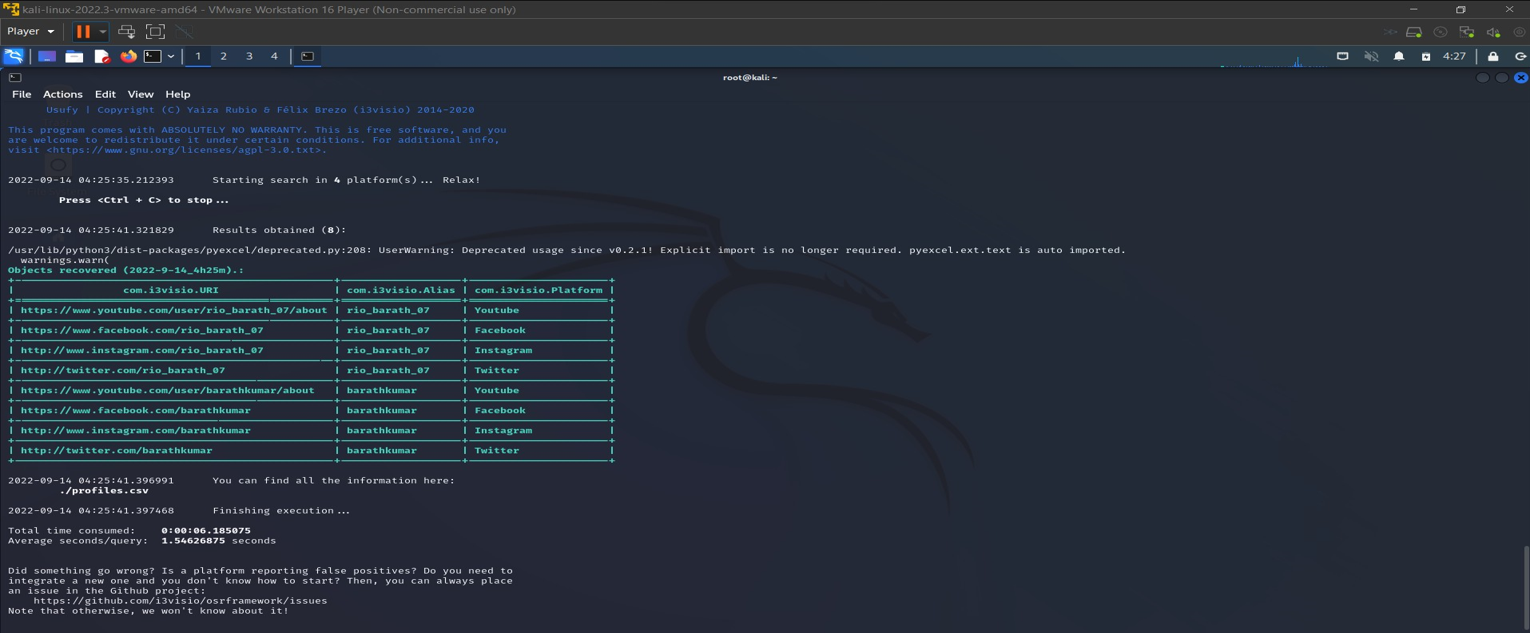
## Usufy.py -n <Target username or profile name> -p twitter facebook youtube

If any error occurs Try this command: **Sudo apt-getupdate**

## The usufy.py will search the user details in the mentioned platform and will provide you with the existence of the user

**OUTPUT-**





**RESULT-**

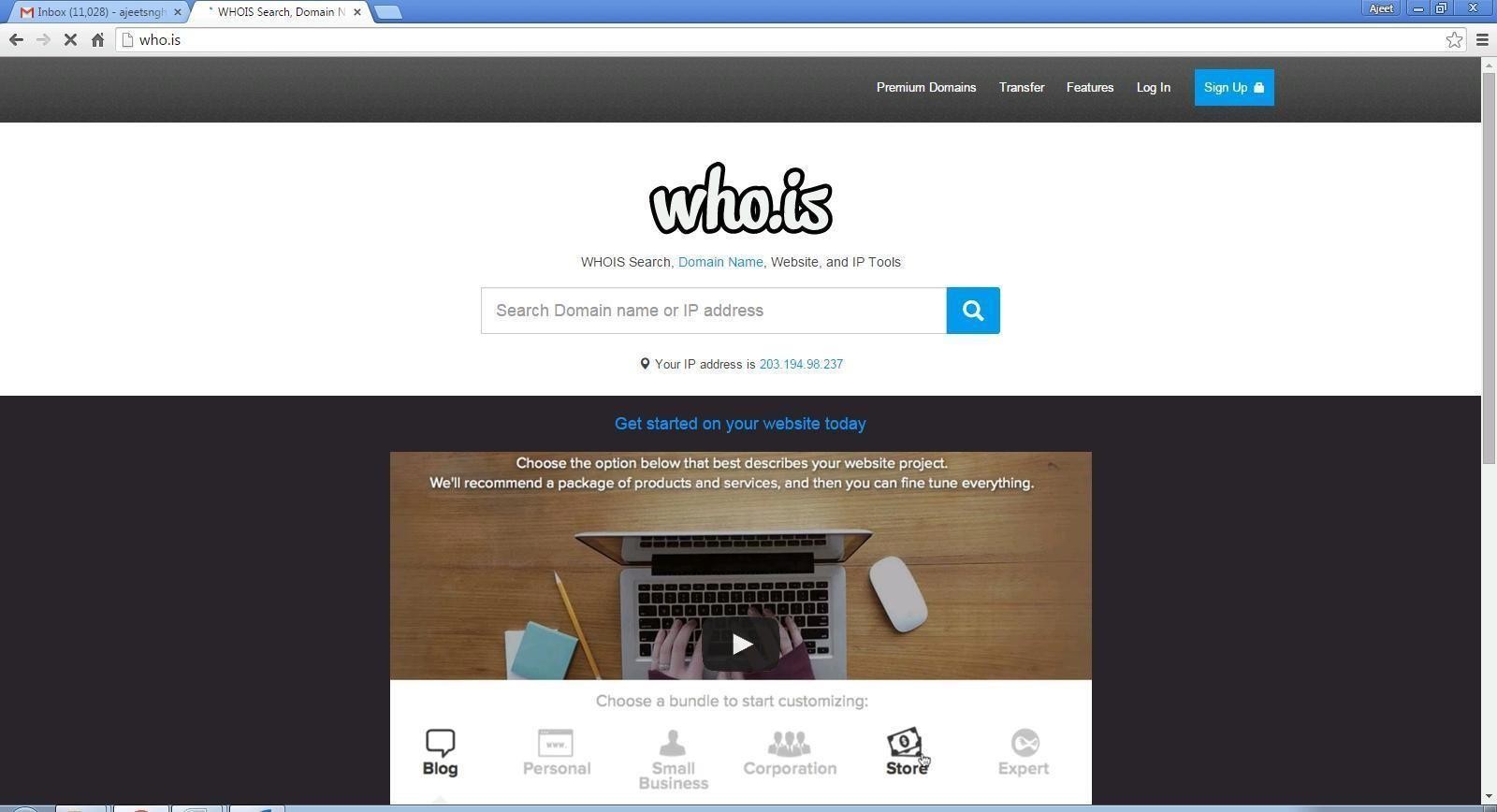
Checking for the Existence of a Profile for given user details in different platforms is successful.

**Exercise NO 7: Use Google and Whois for Reconnaisasance.**

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

Procedure:

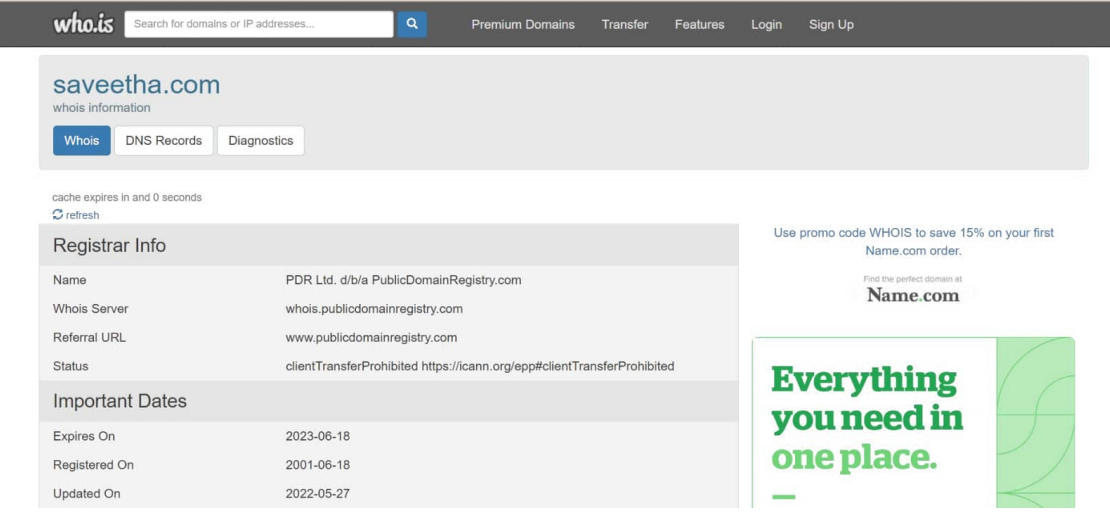
Step1: Open the WHO.is website

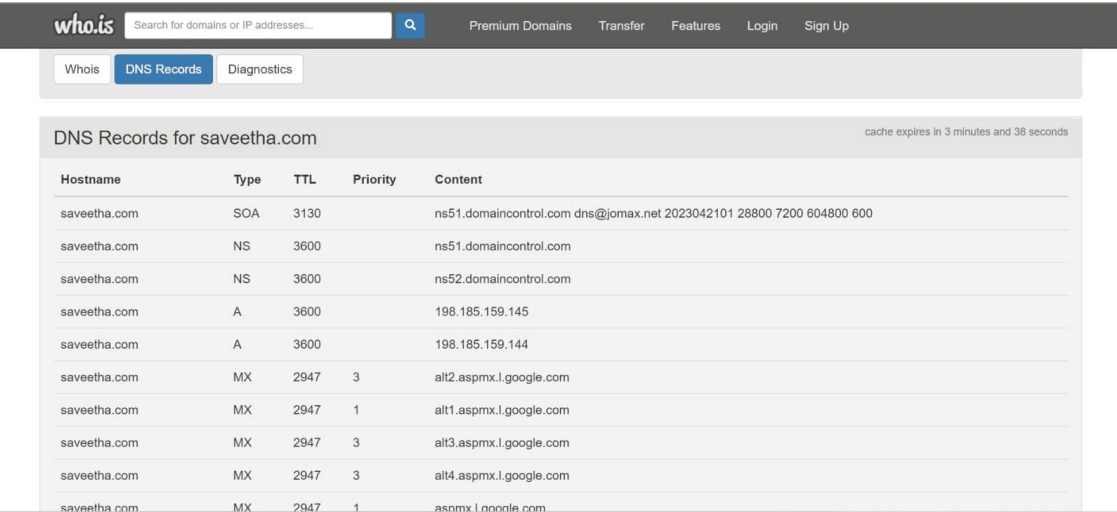


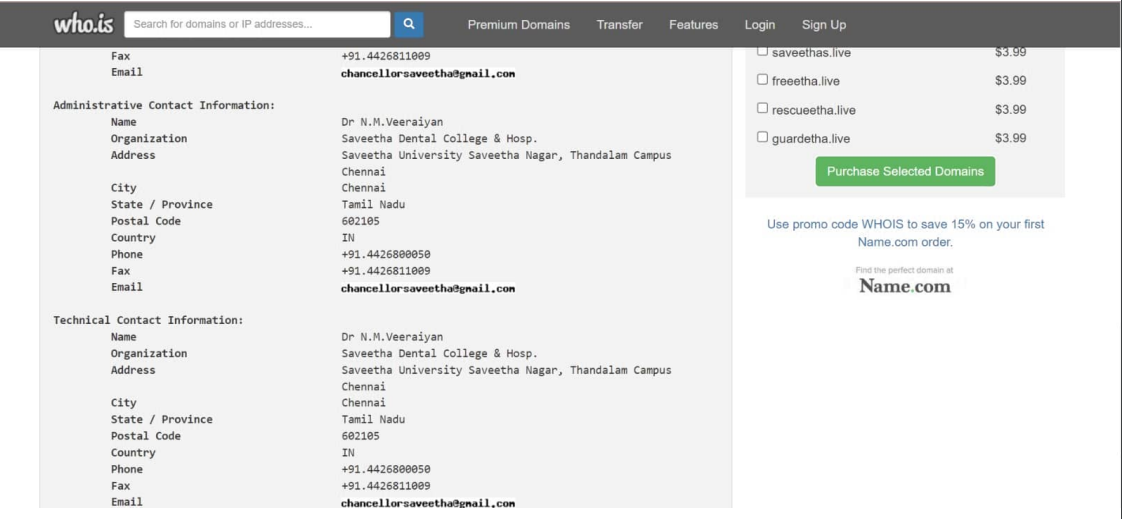
Step 2: Enter the website name in search bar and hit the “Enter button”.

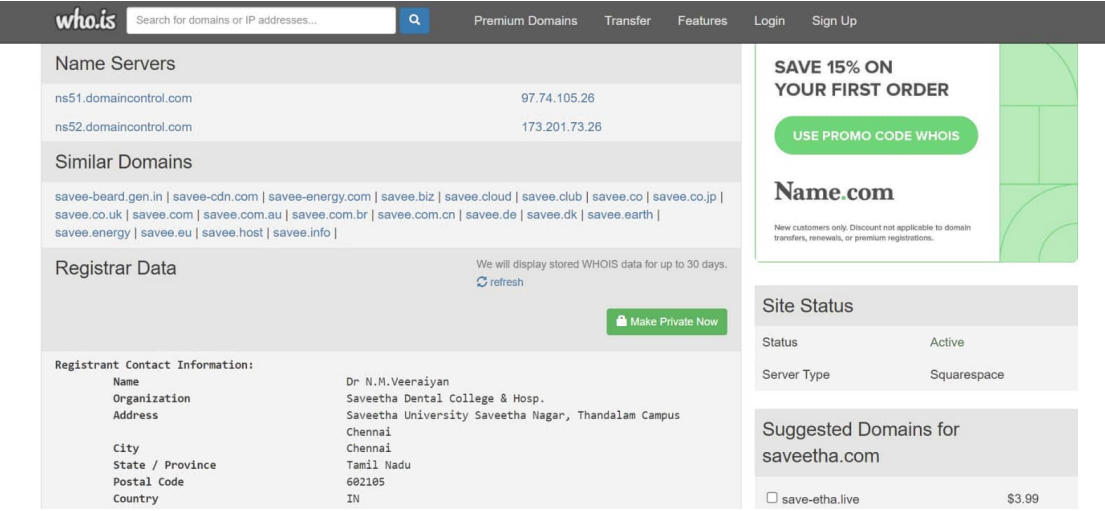
Step 3: Show you information about [www.saveetha.com](http://www.saveetha.com/)

**OUTPUT-**









RESULT-: To find out the Whois, DNS Records and Diagonstics for particular website by using Whois search is successful.

**Exercise No 8: TraceRoute, ping, ifconfig, ipconfig, netstat**

**Aim:** Using TraceRoute, ping, ifconfig(LINUX), ipconfig(WINDOWS), and netstat

Command.

Procedure:

Step 1: open windows command prompt and Type tracert command and type tracert

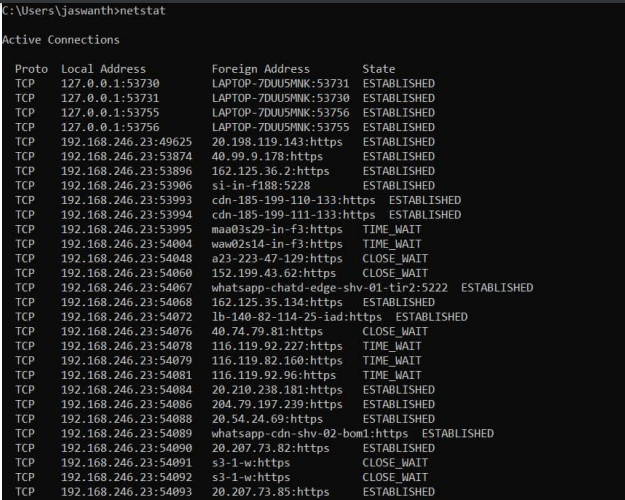
[www.saveetha.com](http://www.saveetha.com/) -> “Enter”

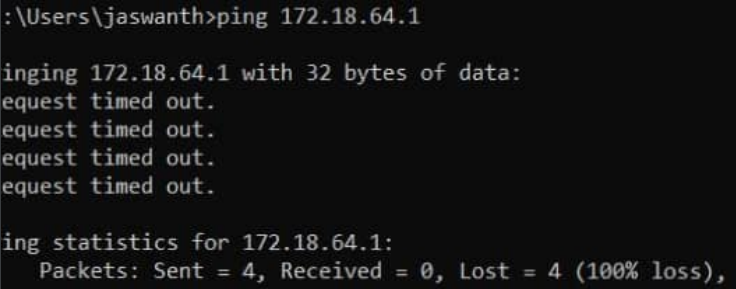
Step 2: Type ping command and type IP Address press “Enter”

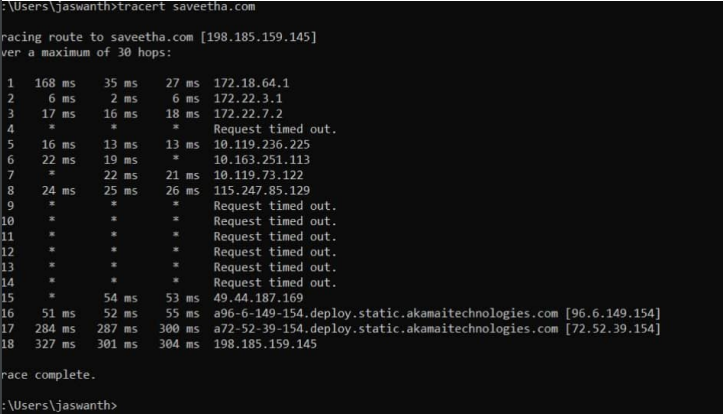
Step 3: Type ifconfig command

Step 4: Type netstat command

**OUTPUT-**

****

****

****

**RESULT-**

Using TraceRoute, ping, ifconfig(LINUX), ipconfig(WINDOWS), and netstat

Command is successful.

Exercise No 8:VULNERABILITY ANALYSIS - CGI Scanning with Nikto

Aim:To perform vulnerability Analysis using CGI Scanning with Nikto

Procedure:

Step 1: open a terminal window and type nikto –H and press enter

Step 2: Type nikto –h <website> Tuning x and press enter

Step 3: Nikto starts web server scanning with all tuning options enabled.

Step4:In the terminal window type “nikto –h <website>-Cgidirs all”and hit enter

Step 5. Nikto will scan the webserver as it looks vulnerable CGI directories. It scans the webserver and list out the directories

**OUTPUT-**



**RESULT-**

To perform vulnerability Analysis using CGI Scanning with Nikto is successful.

**Exercise No 9: WireShark sniffer**

**Aim:** Use WireShark sniffer to capture network traffic and analyze.

Procedure:

Step 1: Install and open WireShark .

Step 2: Go to Capture tab and select Interface option. Here Wifi connection is chosen

Step 3: The source, Destination and protocols of the packets in the Wifi network are displayed

Step 4: Open a website in a new window and enter the user id and password. Register if needed.

Step 5:Enter the credentials and then sign in

Step 6: The wireshark tool will keep recording the packets.

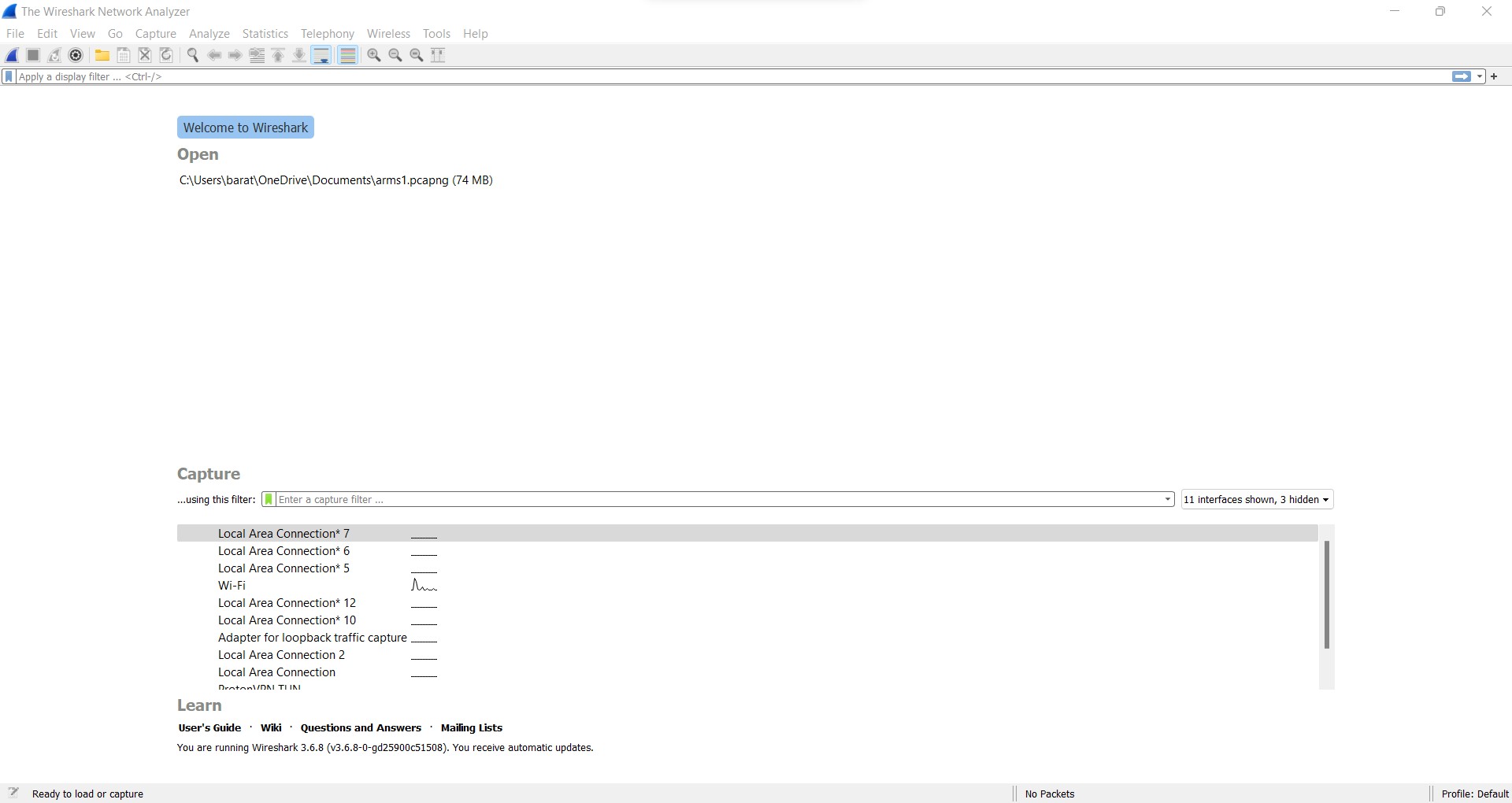
Step 7: Select filter as http to make the search easier and click on apply.

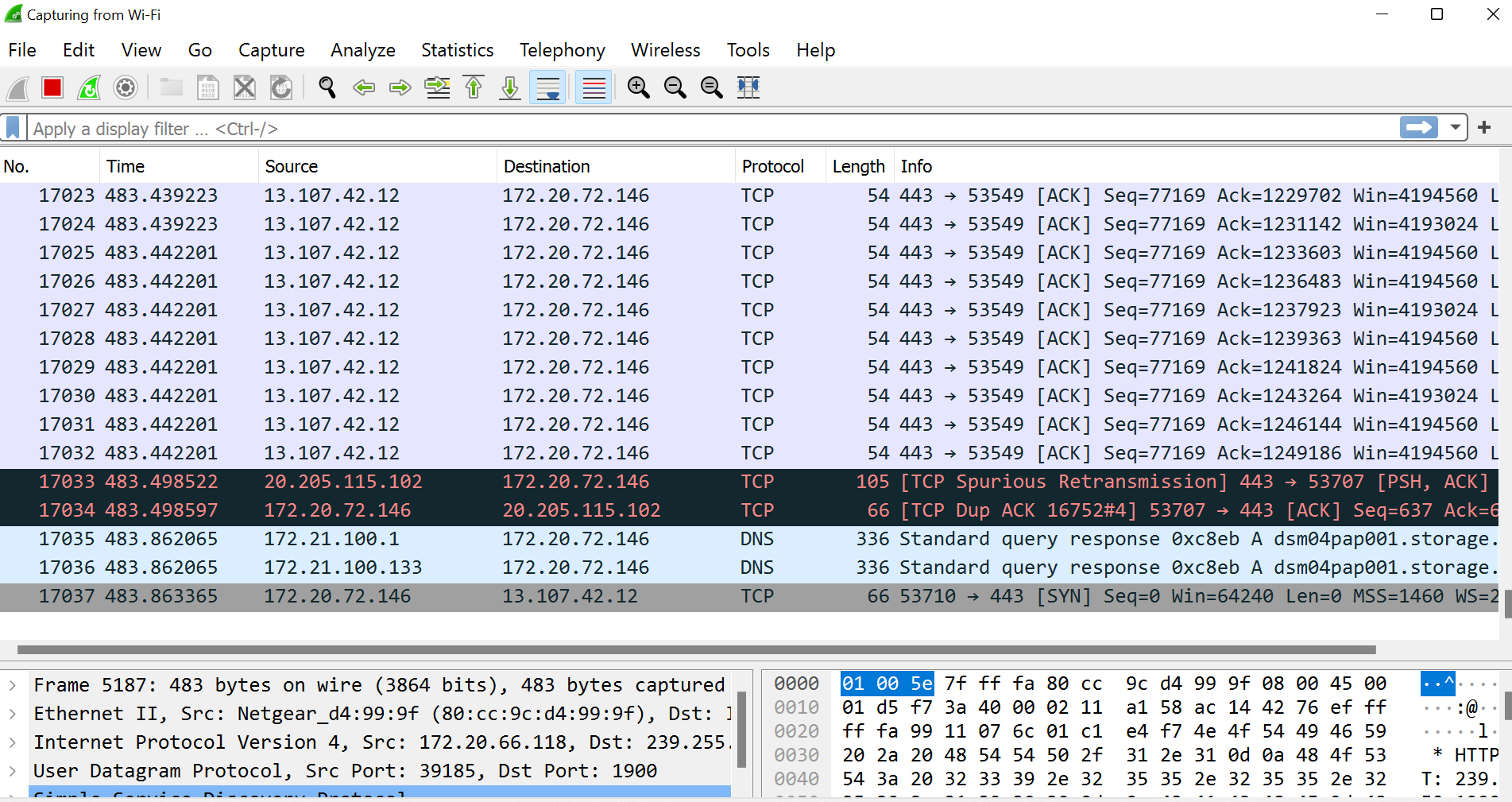
Step 9: Now stop the tool to stop recordin

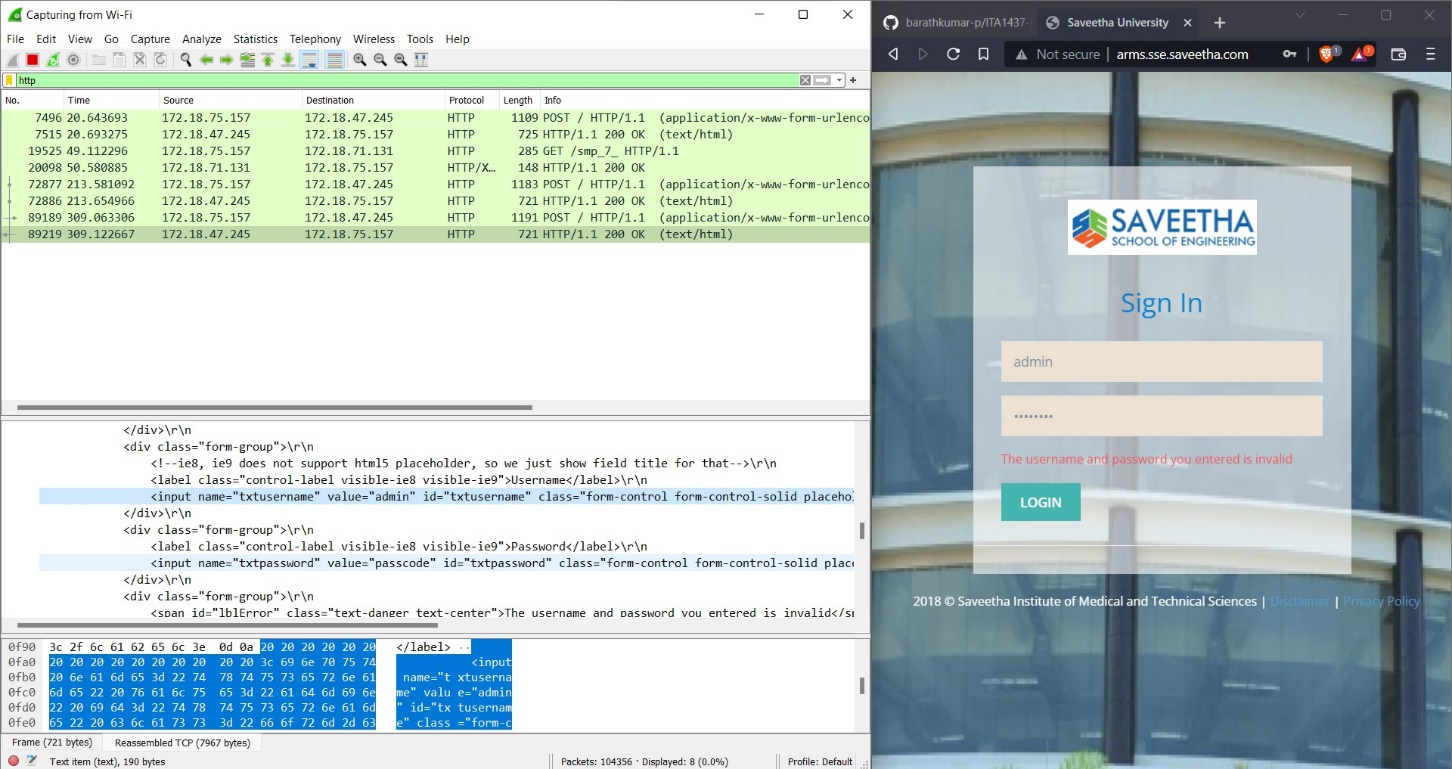
Step 10: Find the post methods for username and passwords

Step 11: U will see the email- id and password that you used to log in.

**OUTPUT-**







**RESULT-**

Using WireShark sniffer to capture network traffic and analyze is successful.