ITA1471

ETHICAL HACKING FOR NETWORK HACKING

S .Charan Kumar

192211364

1St YEAR, CSE DEPARTMENT

ITA144-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)

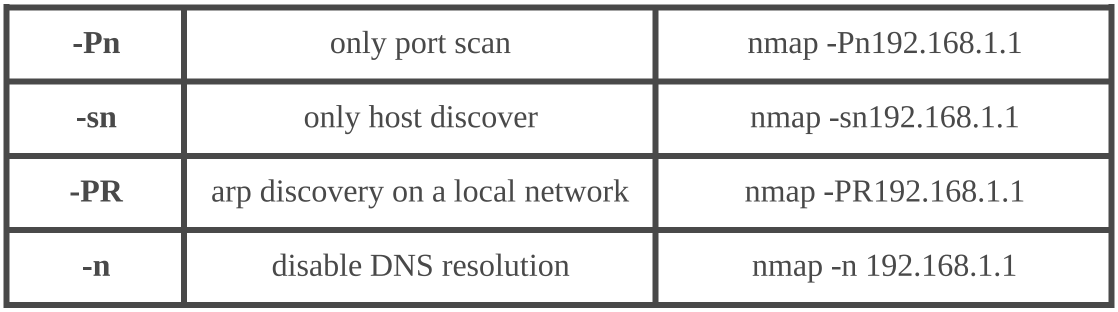
Step 2: Perform different types of scan (Tcp, Udp, Ack, Syn, Fin, Null, Xmas, Rpc, Idle)- scan types

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

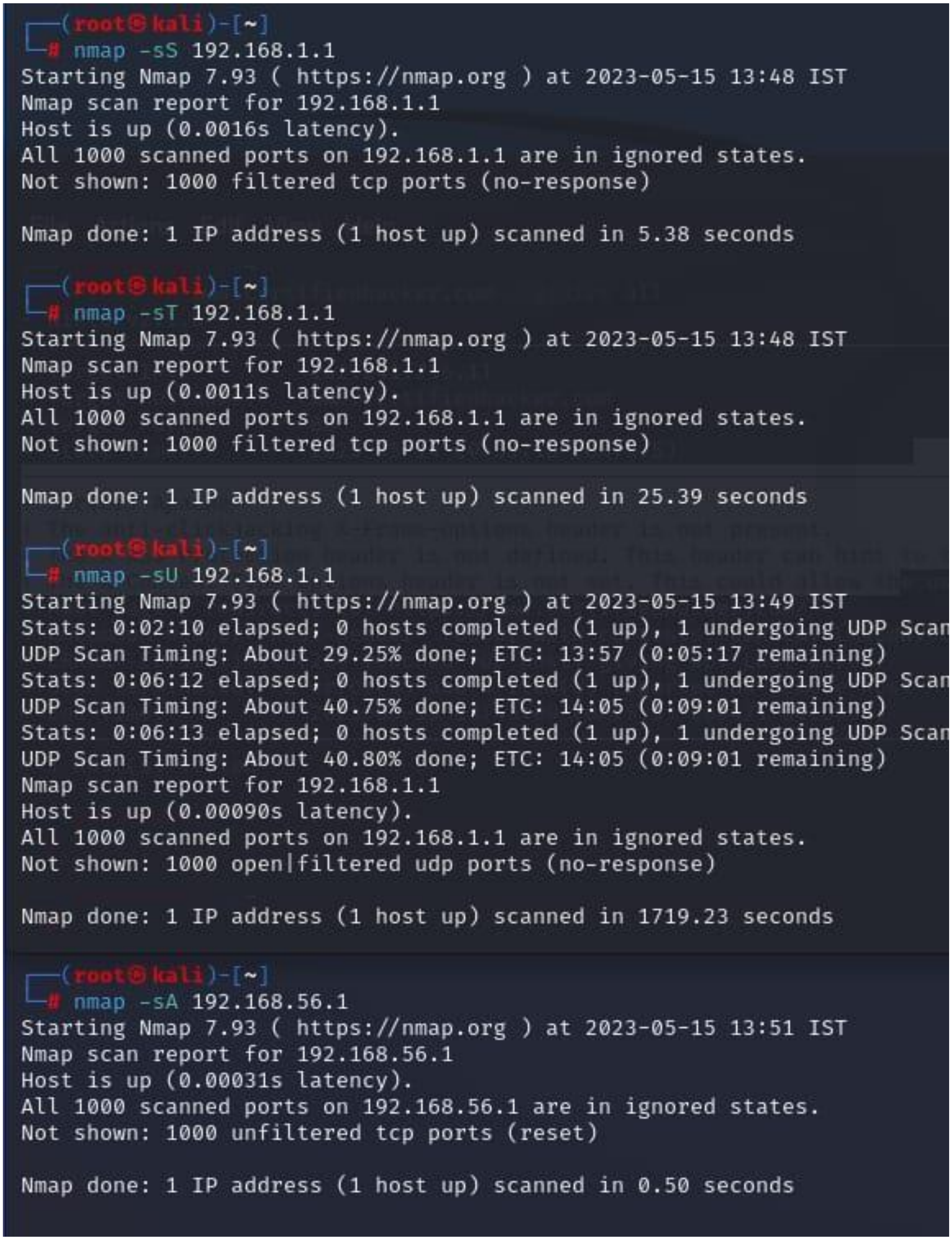
Step 6:-

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

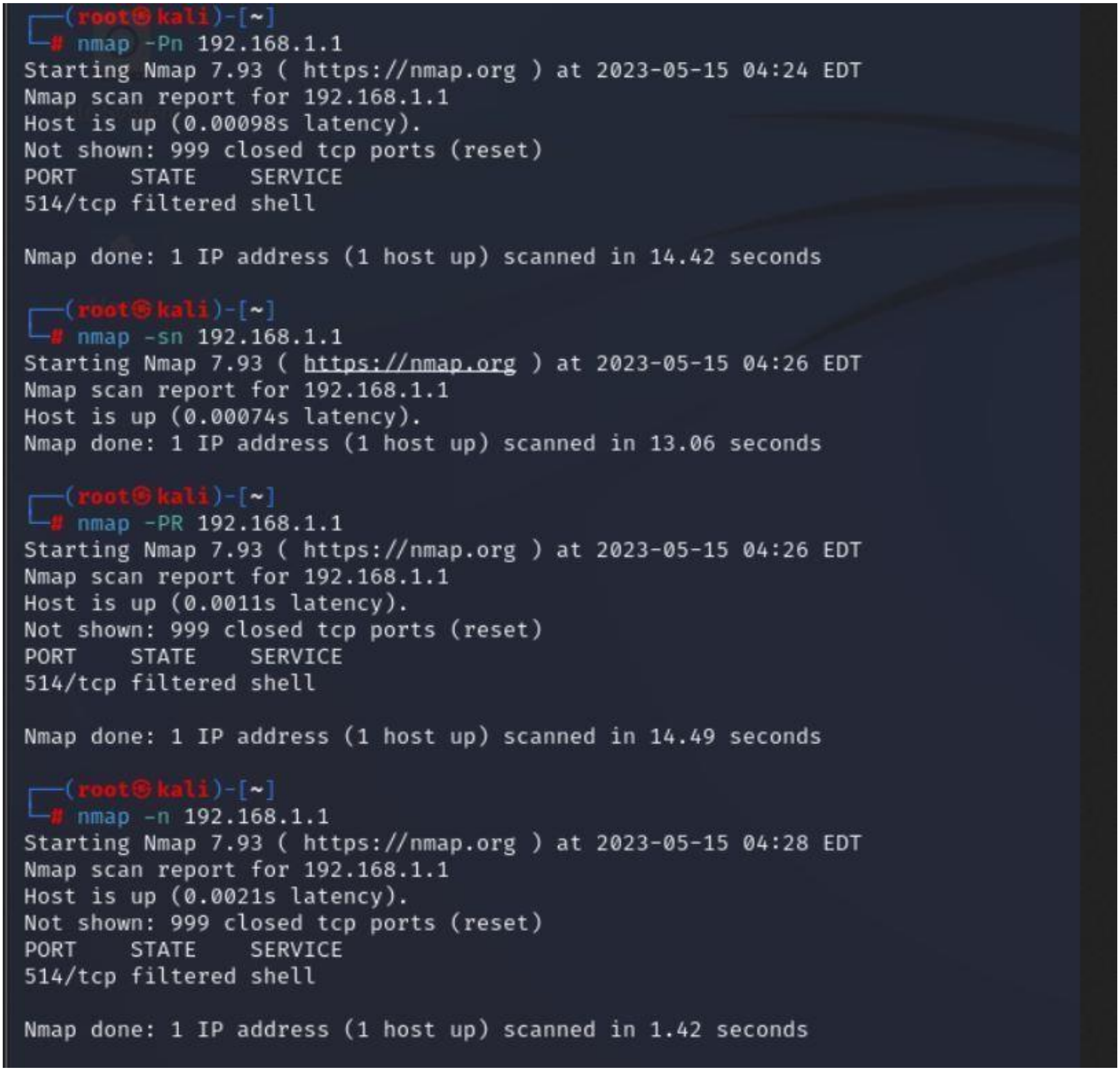
Output:

1)



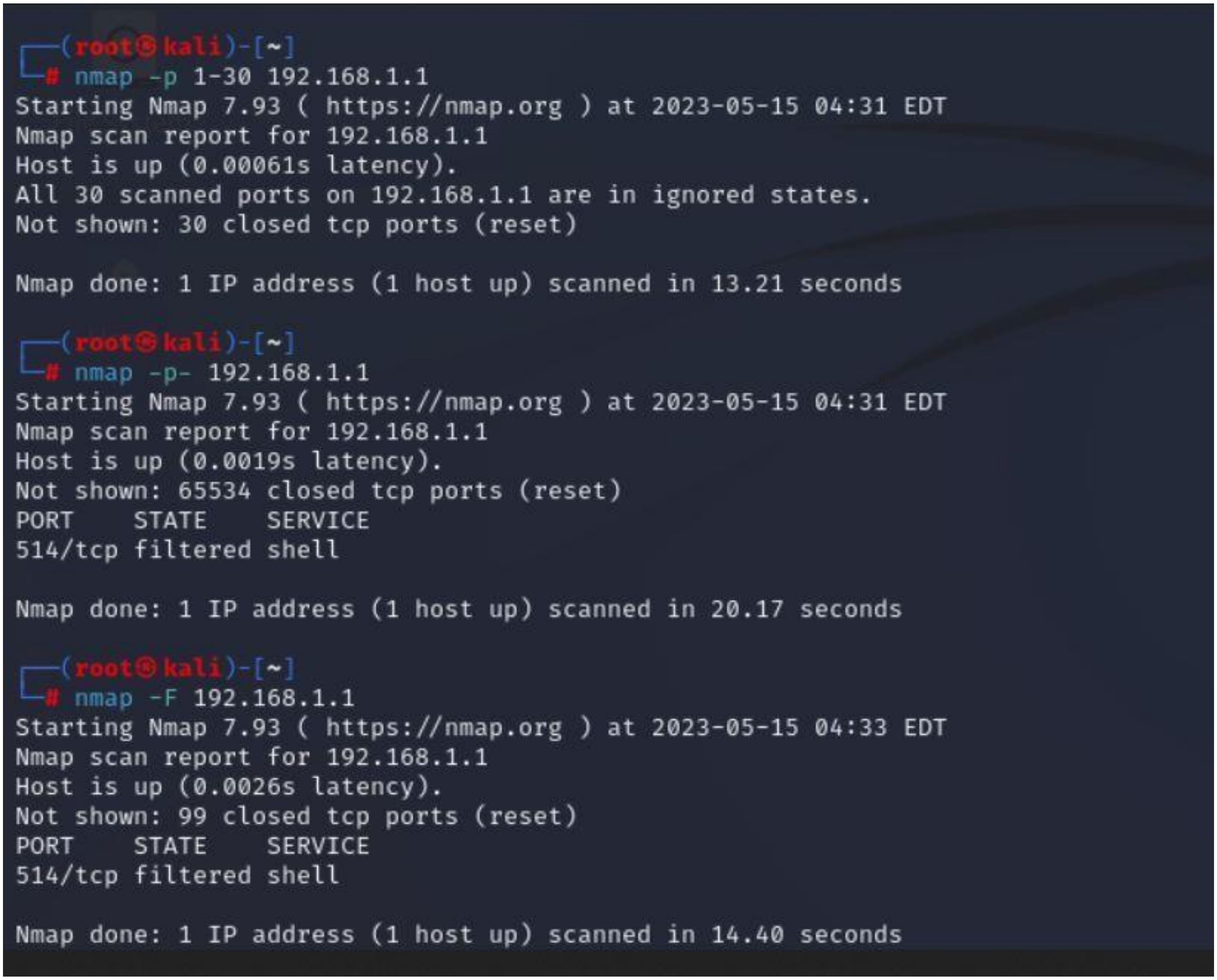
```
┌──(root㉿kali)-[~]
└─# nmap -sS 192.168.1.1
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-15 13:48 IST
Nmap scan report for 192.168.1.1
Host is up (0.0016s latency).
All 1000 scanned ports on 192.168.1.1 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap done: 1 IP address (1 host up) scanned in 5.38 seconds

┌──(root㉿kali)-[~]
└─# nmap -sT 192.168.1.1
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-15 13:48 IST
Nmap scan report for 192.168.1.1
Host is up (0.0011s latency).
All 1000 scanned ports on 192.168.1.1 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap done: 1 IP address (1 host up) scanned in 25.39 seconds

┌──(root㉿kali)-[~]
└─# nmap -sU 192.168.1.1
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-15 13:49 IST
Stats: 0:02:10 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 29.25% done; ETC: 13:57 (0:05:17 remaining)
Stats: 0:06:12 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 40.75% done; ETC: 14:05 (0:09:01 remaining)
Stats: 0:06:13 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 40.80% done; ETC: 14:05 (0:09:01 remaining)
Nmap scan report for 192.168.1.1
Host is up (0.00090s latency).
All 1000 scanned ports on 192.168.1.1 are in ignored states.
Not shown: 1000 open|filtered udp ports (no-response)

Nmap done: 1 IP address (1 host up) scanned in 1719.23 seconds

┌──(root㉿kali)-[~]
└─# nmap -sA 192.168.56.1
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-15 13:51 IST
Nmap scan report for 192.168.56.1
Host is up (0.00031s latency).
All 1000 scanned ports on 192.168.56.1 are in ignored states.
Not shown: 1000 unfiltered tcp ports (reset)

Nmap done: 1 IP address (1 host up) scanned in 0.50 seconds
```

2)



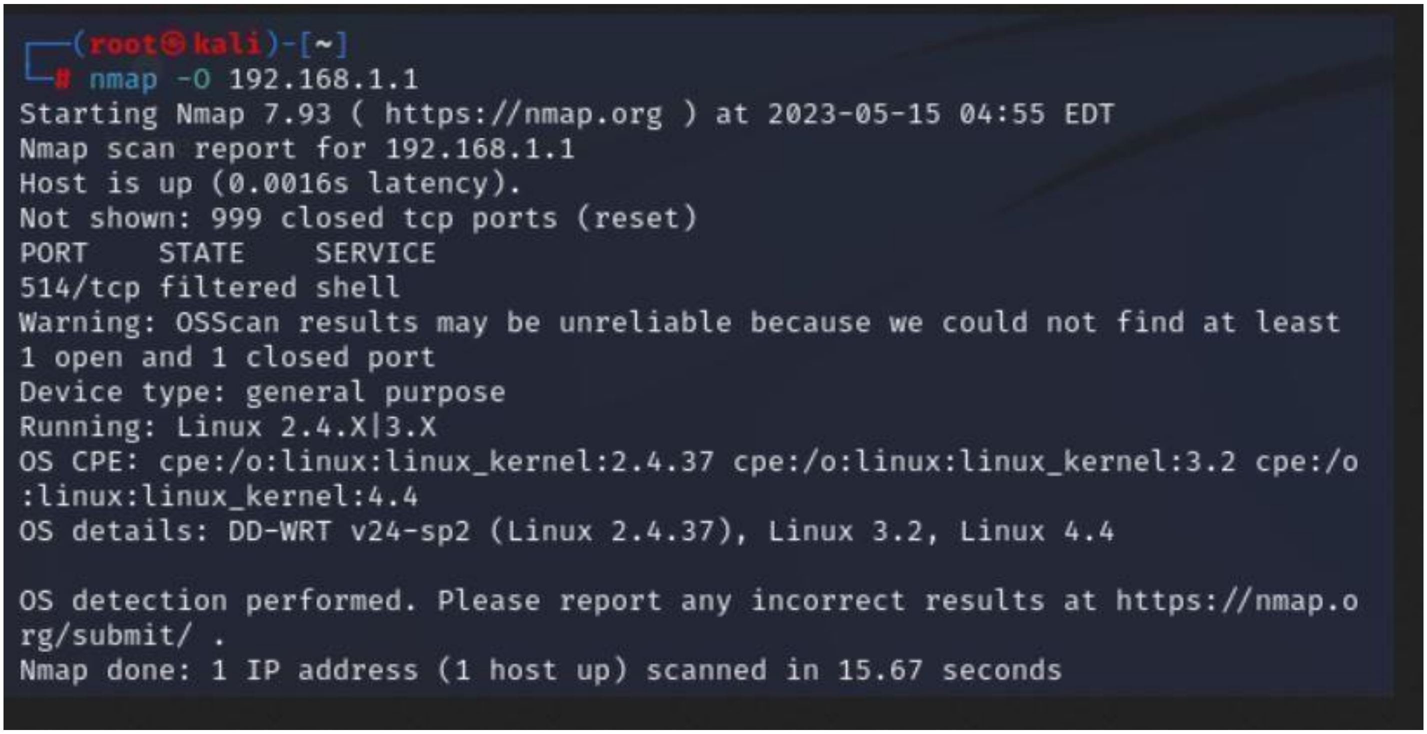
```
┌──(root㉿kali)-[~]
└─# nmap -Pn 192.168.1.1
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-15 04:24 EDT
Nmap scan report for 192.168.1.1
Host is up (0.00098s latency).
Not shown: 999 closed tcp ports (reset)
PORT    STATE    SERVICE
514/tcp filtered shell

Nmap done: 1 IP address (1 host up) scanned in 14.42 seconds

┌──(root㉿kali)-[~]
└─# nmap -sn 192.168.1.1
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-15 04:26 EDT
Nmap scan report for 192.168.1.1
Host is up (0.00074s latency).
Nmap done: 1 IP address (1 host up) scanned in 13.06 seconds

┌──(root㉿kali)-[~]
└─# nmap -PR 192.168.1.1
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-15 04:26 EDT
Nmap scan report for 192.168.1.1
Host is up (0.0011s latency).
Not shown: 999 closed tcp ports (reset)
PORT    STATE    SERVICE
514/tcp filtered shell

Nmap done: 1 IP address (1 host up) scanned in 14.49 seconds

┌──(root㉿kali)-[~]
└─# nmap -n 192.168.1.1
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-15 04:28 EDT
Nmap scan report for 192.168.1.1
Host is up (0.0021s latency).
Not shown: 999 closed tcp ports (reset)
PORT    STATE    SERVICE
514/tcp filtered shell

Nmap done: 1 IP address (1 host up) scanned in 1.42 seconds
```

3)



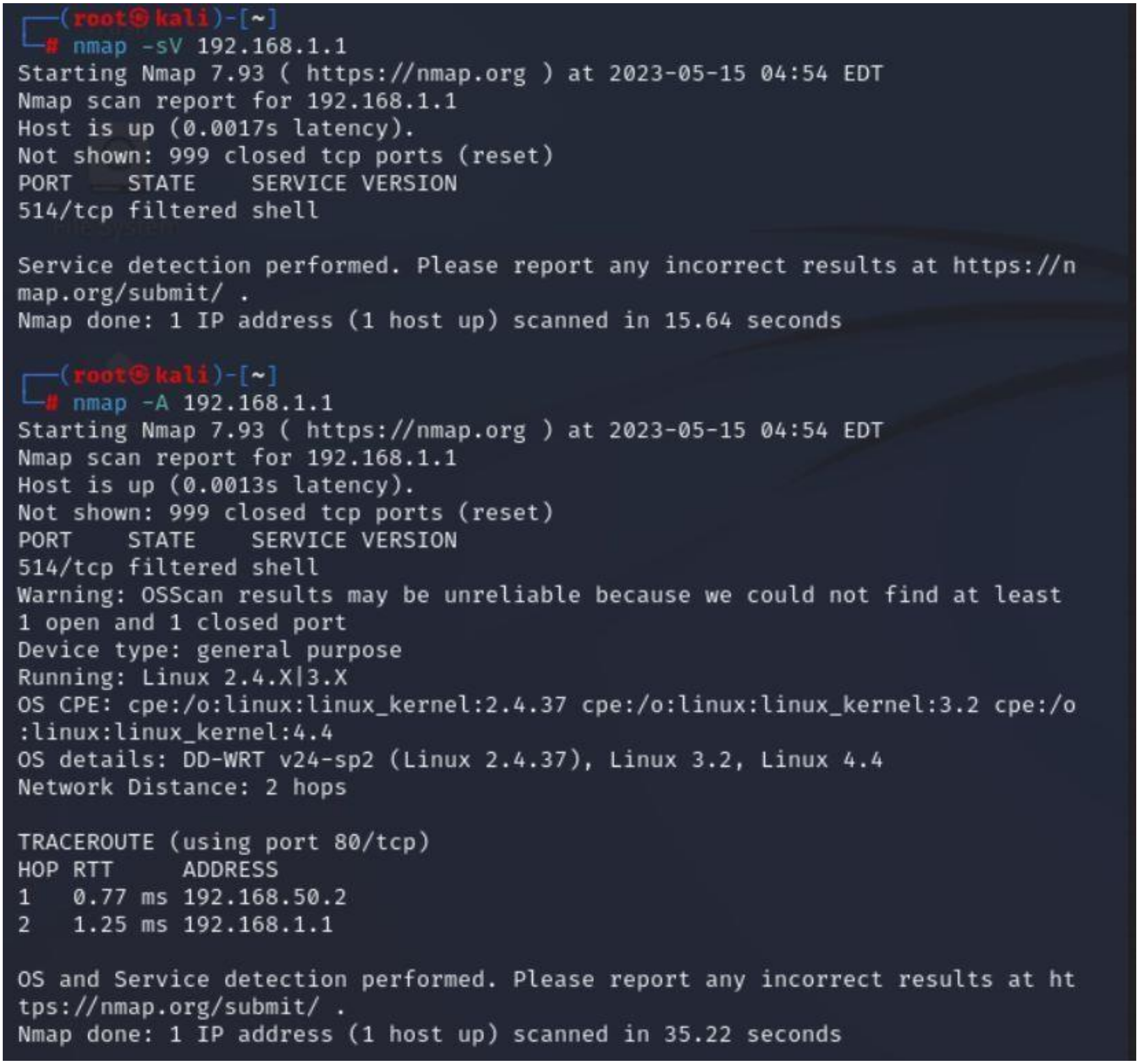
```
┌──(root㉿kali)-[~]
└─# nmap -p 1-30 192.168.1.1
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-15 04:31 EDT
Nmap scan report for 192.168.1.1
Host is up (0.00061s latency).
All 30 scanned ports on 192.168.1.1 are in ignored states.
Not shown: 30 closed tcp ports (reset)

Nmap done: 1 IP address (1 host up) scanned in 13.21 seconds

┌──(root㉿kali)-[~]
└─# nmap -p- 192.168.1.1
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-15 04:31 EDT
Nmap scan report for 192.168.1.1
Host is up (0.0019s latency).
Not shown: 65534 closed tcp ports (reset)
PORT    STATE    SERVICE
514/tcp filtered shell

Nmap done: 1 IP address (1 host up) scanned in 20.17 seconds

┌──(root㉿kali)-[~]
└─# nmap -F 192.168.1.1
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-15 04:33 EDT
Nmap scan report for 192.168.1.1
Host is up (0.0026s latency).
Not shown: 99 closed tcp ports (reset)
PORT    STATE    SERVICE
514/tcp filtered shell

Nmap done: 1 IP address (1 host up) scanned in 14.40 seconds
```

4)



```
┌──(root㉿kali)-[~]
└─# nmap -O 192.168.1.1
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-15 04:55 EDT
Nmap scan report for 192.168.1.1
Host is up (0.0016s latency).
Not shown: 999 closed tcp ports (reset)
PORT    STATE    SERVICE
514/tcp filtered shell
Warning: OSScan results may be unreliable because we could not find at least
1 open and 1 closed port
Device type: general purpose
Running: Linux 2.4.X|3.X
OS CPE: cpe:/o:linux:linux_kernel:2.4.37 cpe:/o:linux:linux_kernel:3.2 cpe:/o
:linux:linux_kernel:4.4
OS details: DD-WRT v24-sp2 (Linux 2.4.37), Linux 3.2, Linux 4.4

OS detection performed. Please report any incorrect results at https://nmap.o
rg/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 15.67 seconds
```

5)



```
┌──(root㉿kali)-[~]
└─# nmap -sV 192.168.1.1
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-15 04:54 EDT
Nmap scan report for 192.168.1.1
Host is up (0.0017s latency).
Not shown: 999 closed tcp ports (reset)
PORT    STATE    SERVICE VERSION
514/tcp filtered shell

Service detection performed. Please report any incorrect results at https://n
map.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 15.64 seconds

┌──(root㉿kali)-[~]
└─# nmap -A 192.168.1.1
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-15 04:54 EDT
Nmap scan report for 192.168.1.1
Host is up (0.0013s latency).
Not shown: 999 closed tcp ports (reset)
PORT    STATE    SERVICE VERSION
514/tcp filtered shell
Warning: OSScan results may be unreliable because we could not find at least
1 open and 1 closed port
Device type: general purpose
Running: Linux 2.4.X|3.X
OS CPE: cpe:/o:linux:linux_kernel:2.4.37 cpe:/o:linux:linux_kernel:3.2 cpe:/o
:linux:linux_kernel:4.4
OS details: DD-WRT v24-sp2 (Linux 2.4.37), Linux 3.2, Linux 4.4
Network Distance: 2 hops

TRACEROUTE (using port 80/tcp)
HOP RTT     ADDRESS
1   0.77 ms 192.168.50.2
2   1.25 ms 192.168.1.1

OS and Service detection performed. Please report any incorrect results at ht
tps://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 35.22 seconds
```

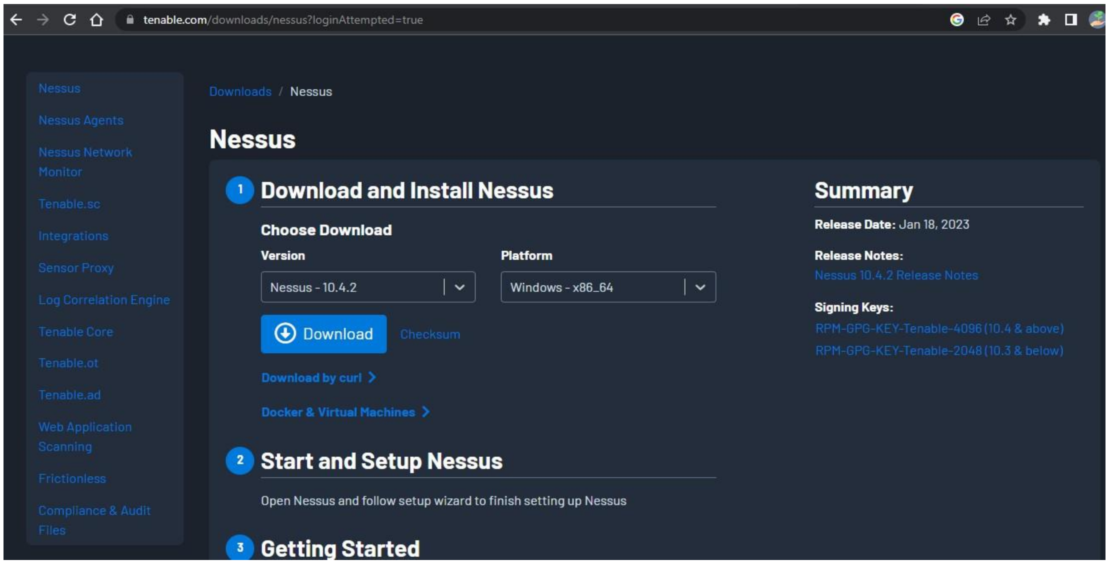
Result:

The following experiment is done using Nmap tool in root terminal in kali Linux server. I have used all the commands that are available in Nmap tool.

Exercise No 2: Vulnerability Access Scan Using Nessus

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

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



Nessus

1 Download and Install Nessus

Choose Download

Version: Nessus - 10.4.2

Platform: Windows - x86_64

2 Start and Setup Nessus

Open Nessus and follow setup wizard to finish setting up Nessus

3 Getting Started

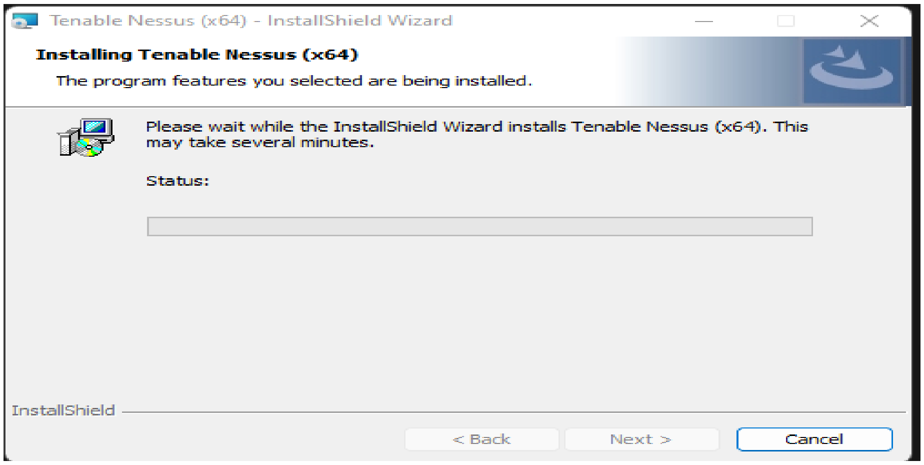
Summary

Release Date: Jan 18, 2023

Release Notes: Nessus 10.4.2 Release Notes

Signing Keys:
RPM-GPG-KEY-Tenable-4096 (10.4 & above)
RPM-GPG-KEY-Tenable-2048 (10.3 & below)

Step 2: Choose your OS and download , install



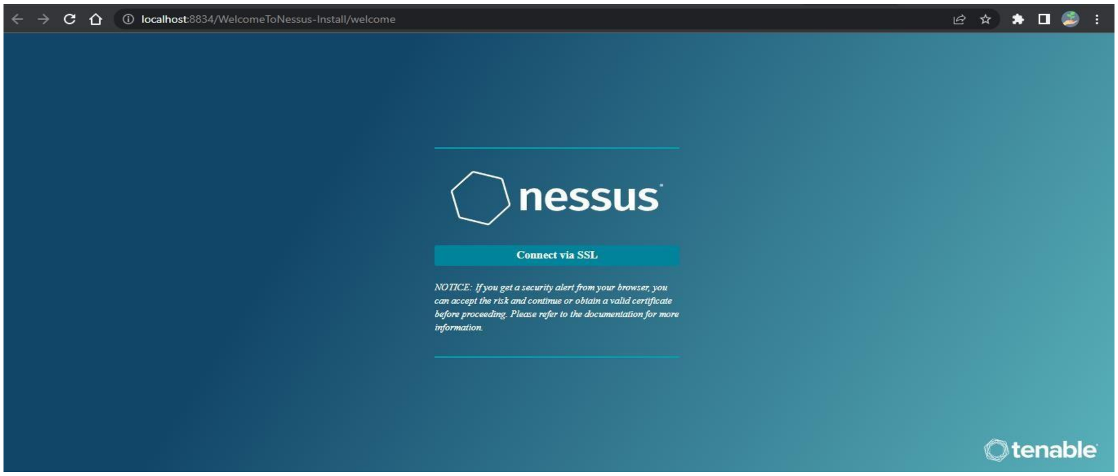
Installing Tenable Nessus (x64)

The program features you selected are being installed.

Please wait while the InstallShield Wizard installs Tenable Nessus (x64). This may take several minutes.

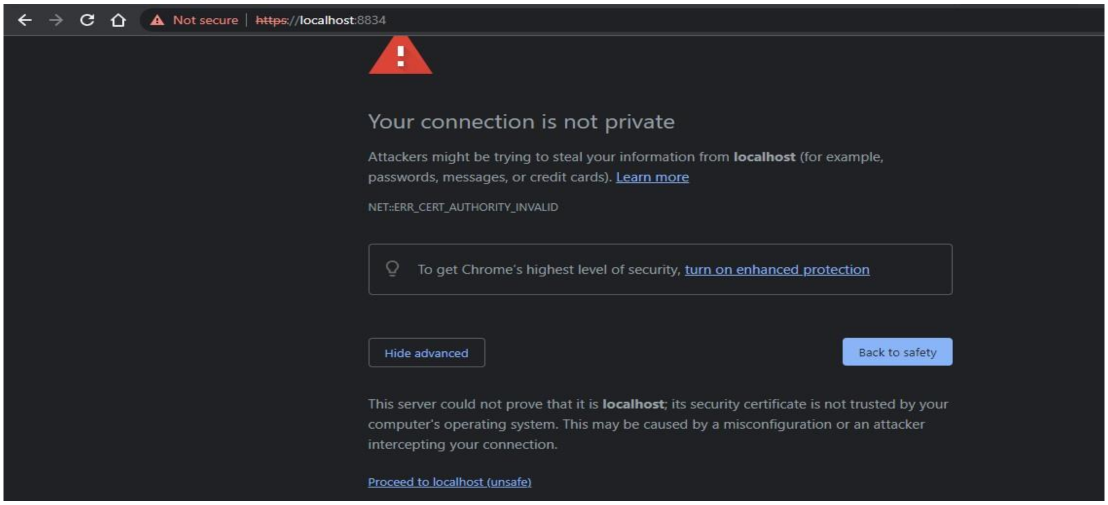
Status:

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



NOTICE: If you get a security alert from your browser, you can accept the risk and continue or obtain a valid certificate before proceeding. Please refer to the documentation for more information.

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



Your connection is not private

Attackers might be trying to steal your information from **localhost** (for example, passwords, messages, or credit cards). Learn more

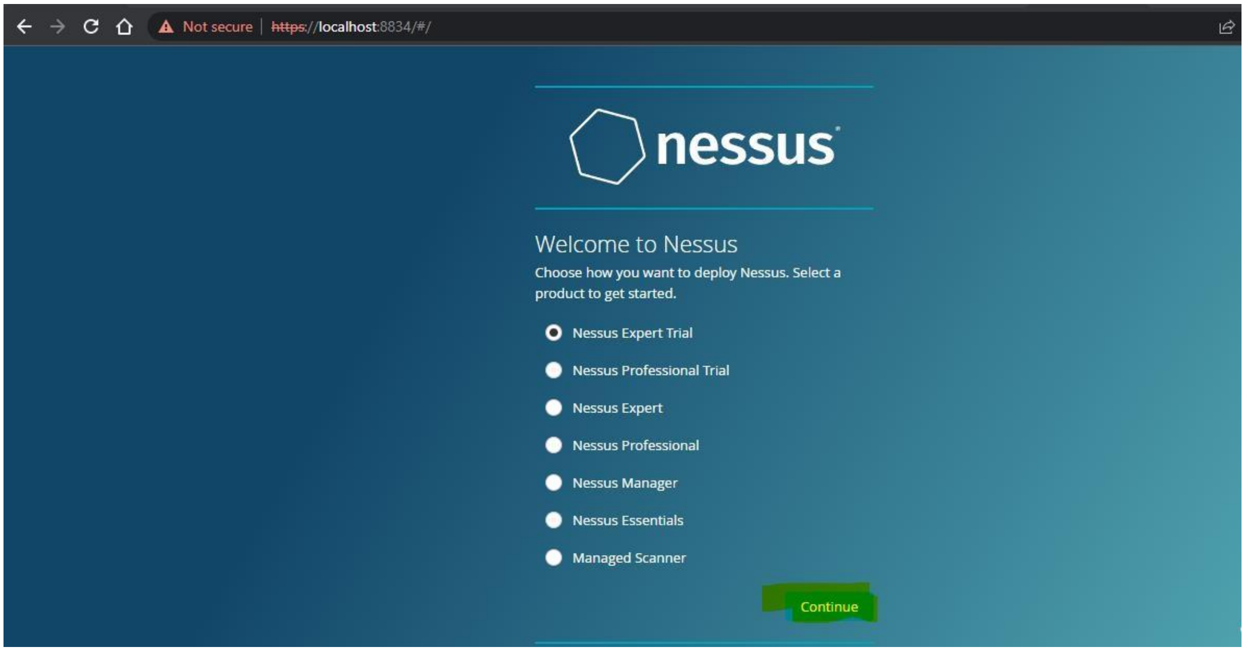
NET::ERR_CERT_AUTHORITY_INVALID

To get Chrome's highest level of security, turn on enhanced protection

This server could not prove that it is **localhost**; its security certificate is not trusted by your computer's operating system. This may be caused by a misconfiguration or an attacker intercepting your connection.

Proceed to localhost (unsafe)

Step 6:- Please choose the Nessus Expert

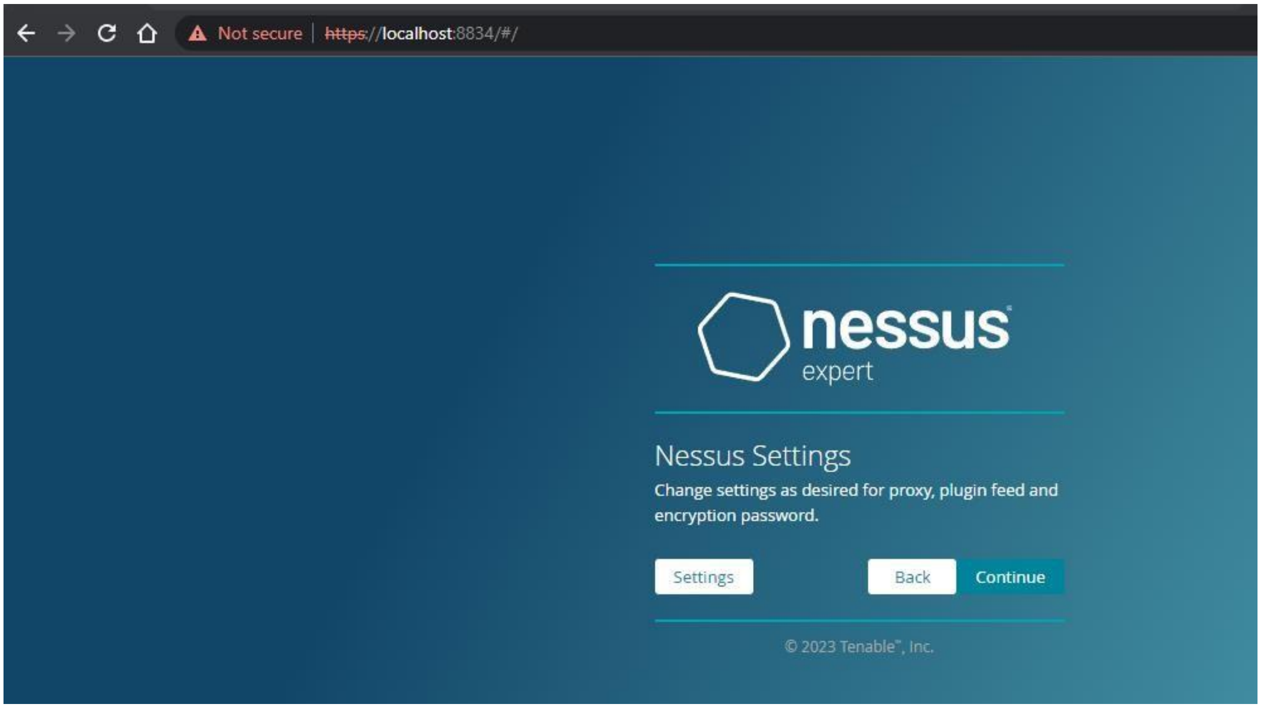


Welcome to Nessus

Choose how you want to deploy Nessus. Select a product to get started.

● Nessus Expert Trial
○ Nessus Professional Trial
○ Nessus Expert
○ Nessus Professional
○ Nessus Manager
○ Nessus Essentials
○ Managed Scanner

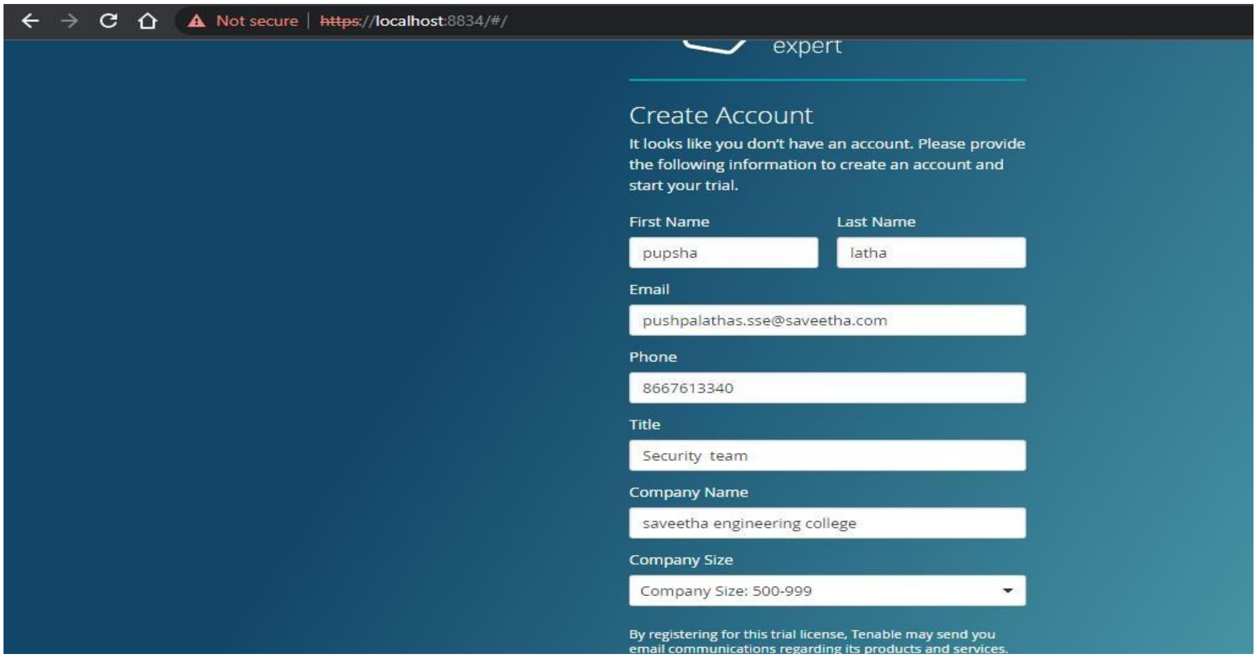
Step 7: Click on continue



Nessus Settings

Change settings as desired for proxy, plugin feed and encryption password.

Step 8:- Register with your organizational email id



Not secure | ~~https~~://localhost:8834/#/

expert

Create Account

It looks like you don't have an account. Please provide the following information to create an account and start your trial.

First Name: pupsha

Last Name: latha

Email: pushpalathas.sse@saveetha.com

Phone: 8667613340

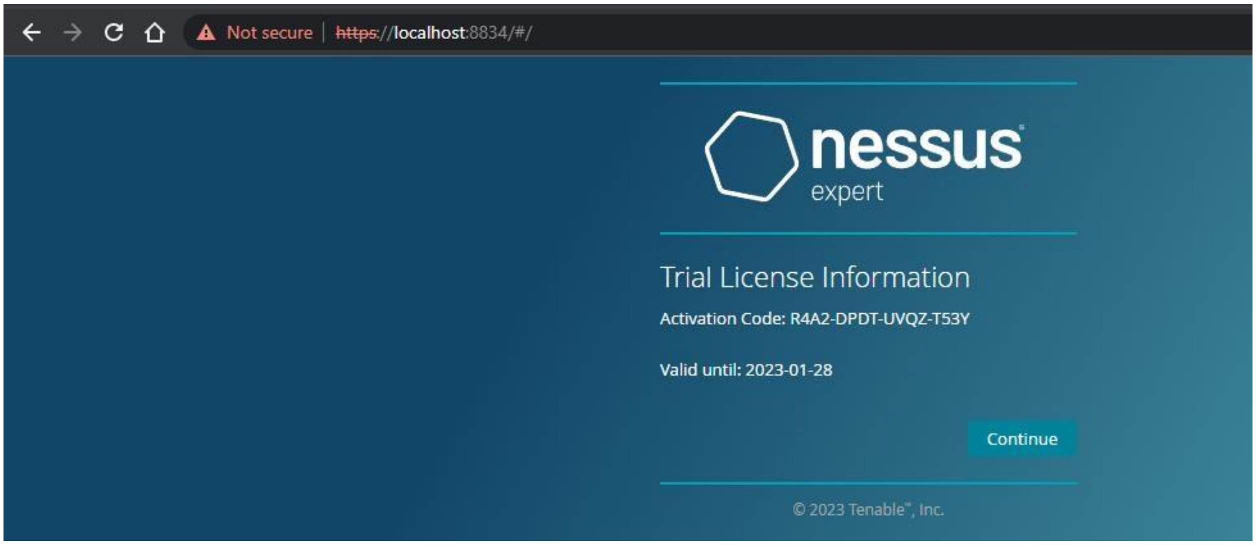
Title: Security team

Company Name: saveetha engineering college

Company Size: Company Size: 500-999

By registering for this trial license, Tenable may send you email communications regarding its products and services.

Step 9:- please note down the activation key



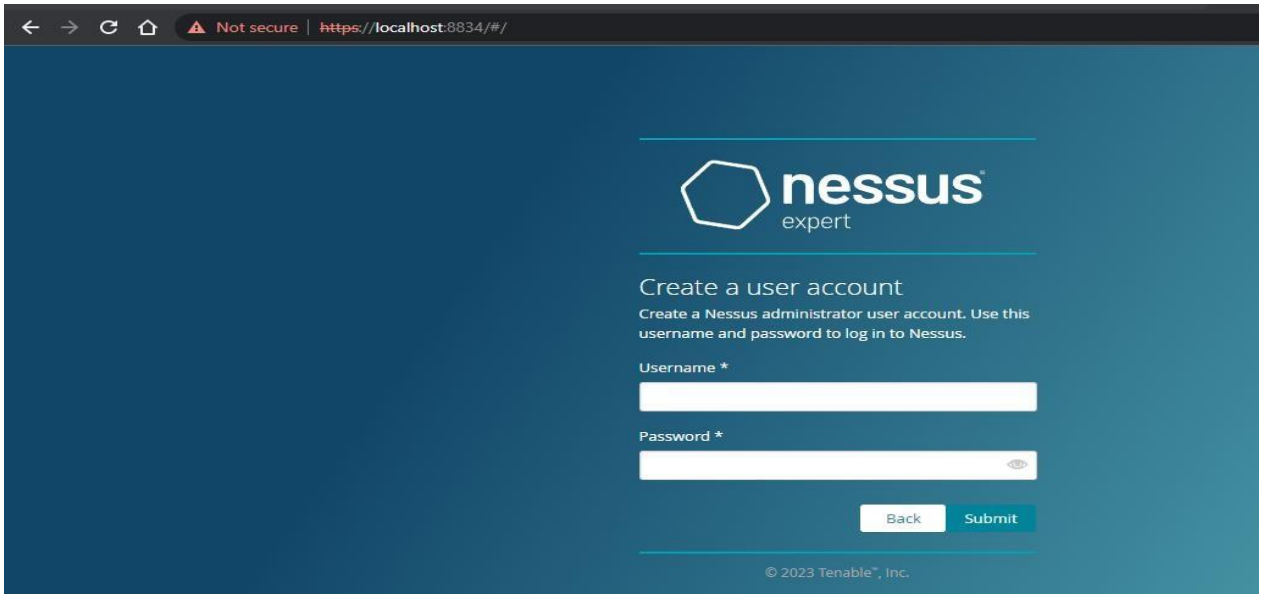
Not secure | ~~https~~://localhost:8834/#/

Trial License Information

Activation Code: R4A2-DPDT-UVQZ-T53Y

Valid until: 2023-01-28

Step 10:- set up your username & password



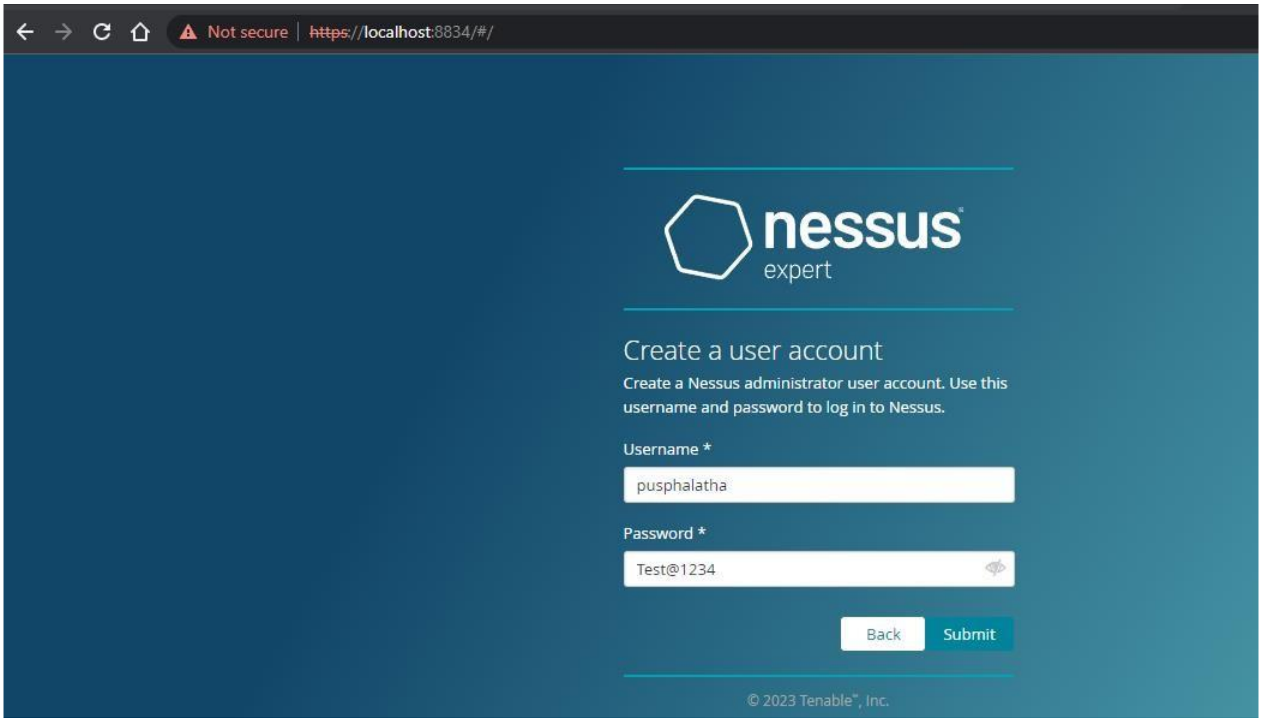
Create a user account

Create a Nessus administrator user account. Use this username and password to log in to Nessus.

Username *

Password *

Step 11:-Type username and password



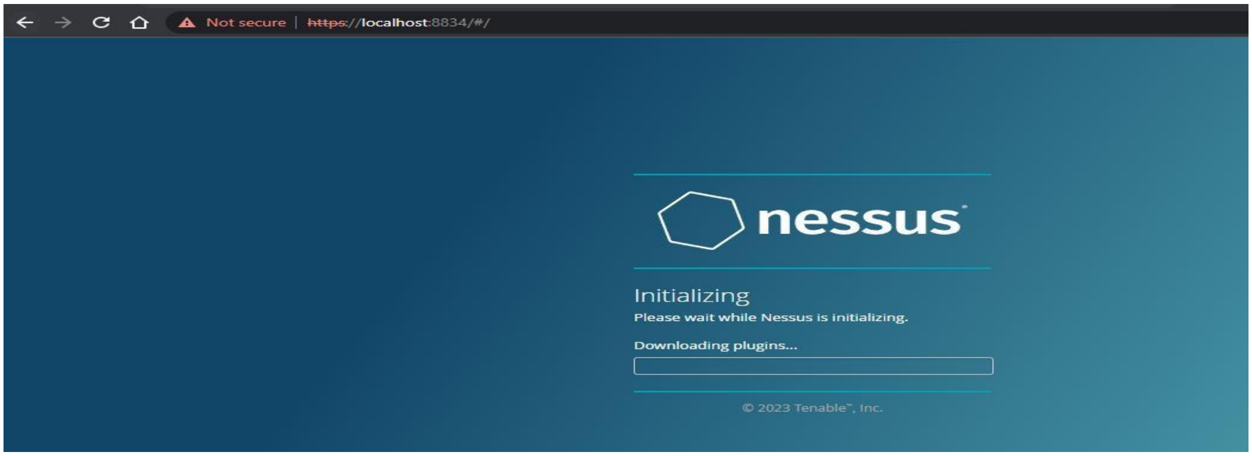
Create a user account

Create a Nessus administrator user account. Use this username and password to log in to Nessus.

Username * pusphalatha

Password * Test@1234

Step 12:- Please wait until download is completed



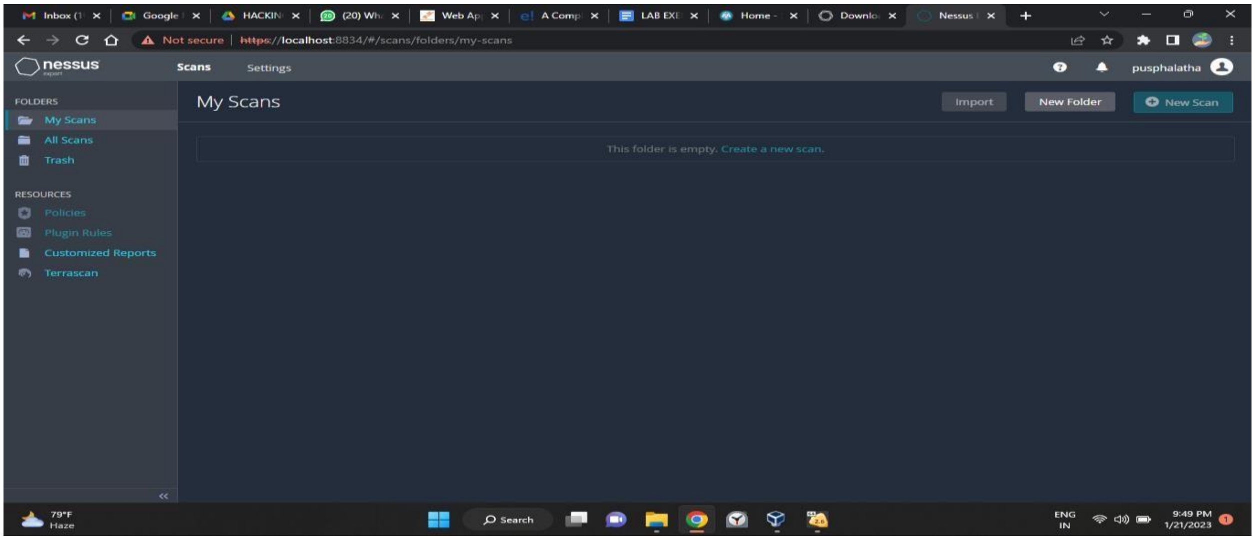
Initializing

Please wait while Nessus is initializing.

Downloading plugins...

© 2023 Tenable™, Inc.

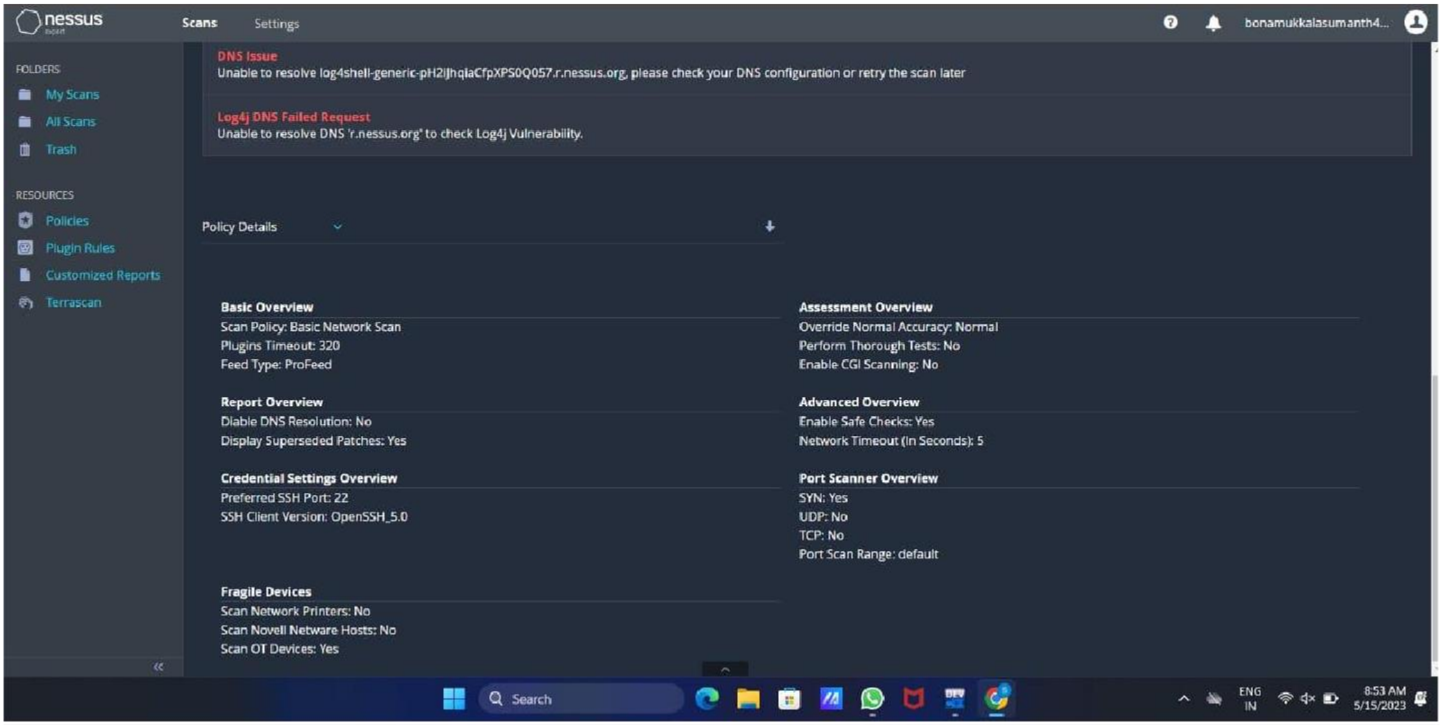
Step 13: Select My Scans



This folder is empty. Create a new scan.

Output:

1)



DNS Issue
Unable to resolve log4shell-generic-pH2iJhqlaCfpXPS0Q057.r.nessus.org, please check your DNS configuration or retry the scan later

Log4j DNS Failed Request
Unable to resolve DNS 'r.nessus.org' to check Log4j Vulnerability.

Policy Details

Basic Overview
Scan Policy: Basic Network Scan
Plugins Timeout: 320
Feed Type: ProFeed

Assessment Overview
Override Normal Accuracy: Normal
Perform Thorough Tests: No
Enable CGI Scanning: No

Report Overview
Diable DNS Resolution: No
Display Superseded Patches: Yes

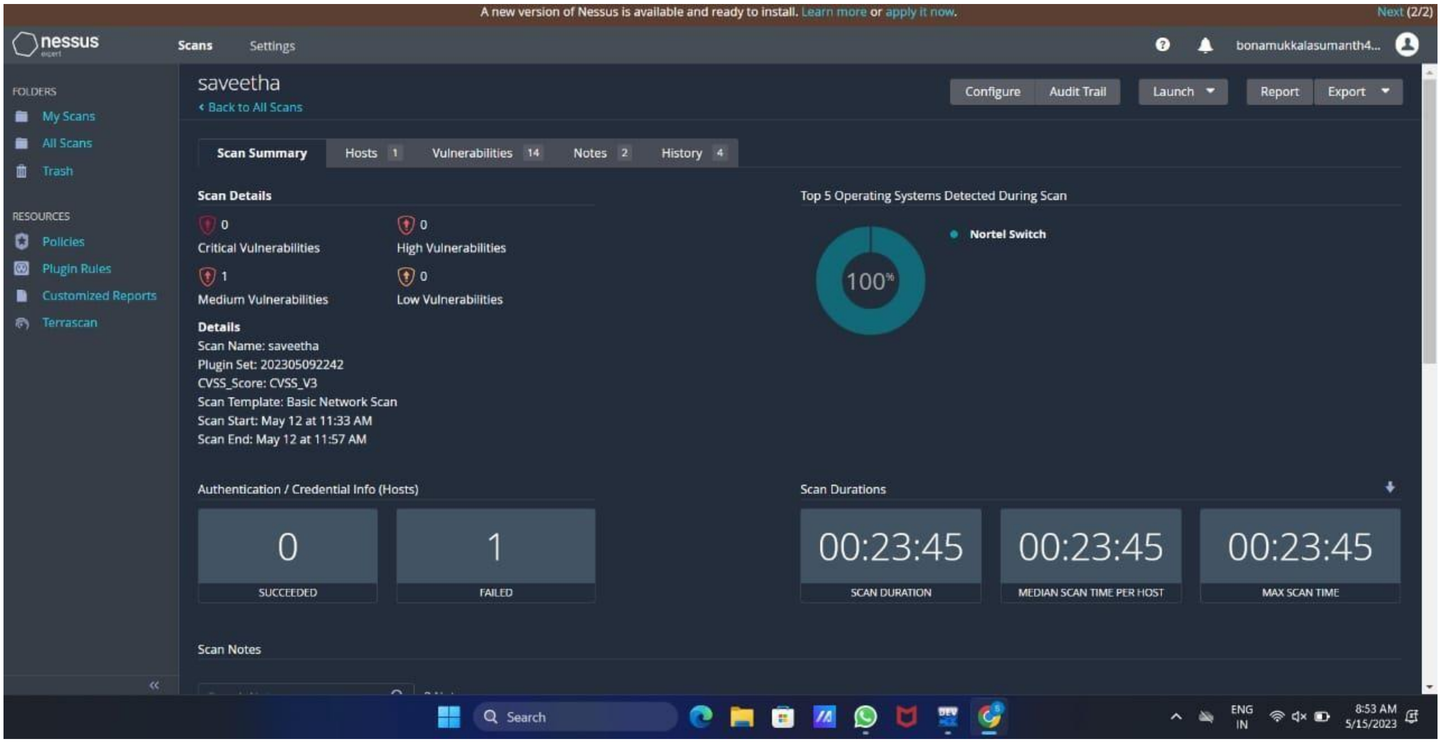
Advanced Overview
Enable Safe Checks: Yes
Network Timeout (In Seconds): 5

Credential Settings Overview
Preferred SSH Port: 22
SSH Client Version: OpenSSH_5.0

Port Scanner Overview
SYN: Yes
UDP: No
TCP: No
Port Scan Range: default

Fragile Devices
Scan Network Printers: No
Scan Novell Netware Hosts: No
Scan OT Devices: Yes

2)



A new version of Nessus is available and ready to install. Learn more or apply it now. Next (2/2)

saveetha
‹ Back to All Scans

Scan Details

0 Critical Vulnerabilities	0 High Vulnerabilities
1 Medium Vulnerabilities	0 Low Vulnerabilities

Top 5 Operating Systems Detected During Scan

Details
Scan Name: saveetha
Plugin Set: 202305092242
CVSS_Score: CVSS_V3
Scan Template: Basic Network Scan
Scan Start: May 12 at 11:33 AM
Scan End: May 12 at 11:57 AM

Authentication / Credential Info (Hosts)

SUCCEEDED	FAILED
0	1

Scan Durations

SCAN DURATION	MEDIAN SCAN TIME PER HOST	MAX SCAN TIME
00:23:45	00:23:45	00:23:45

Scan Notes

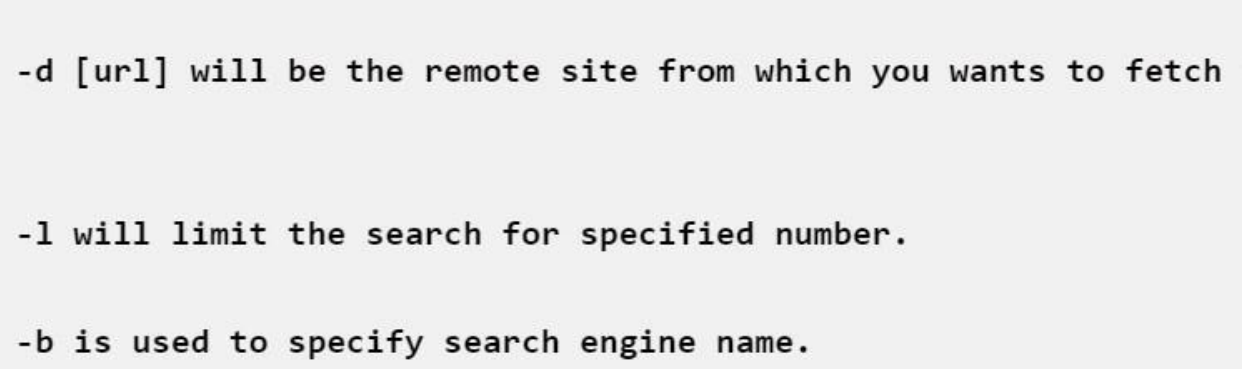
Result:

The following experiment is done using Nessus website in windows operating system. I have done this experiment in google chrome of windows operating system.

Exercise No 3: Information gathering using theHarvester

Aim: To demonstrate information gathering using theHarvester
Procedure:

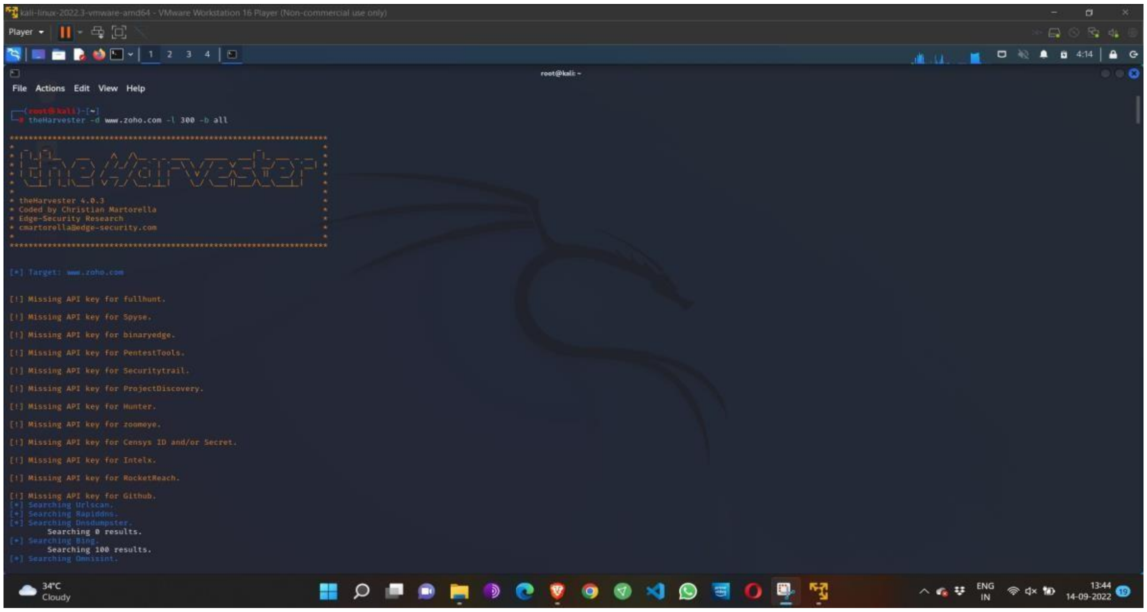
STEP 1: Open Terminal in the kali linux



```
-d [url] will be the remote site from which you wants to fetch


-l will limit the search for specified number.

-b is used to specify search engine name.
```

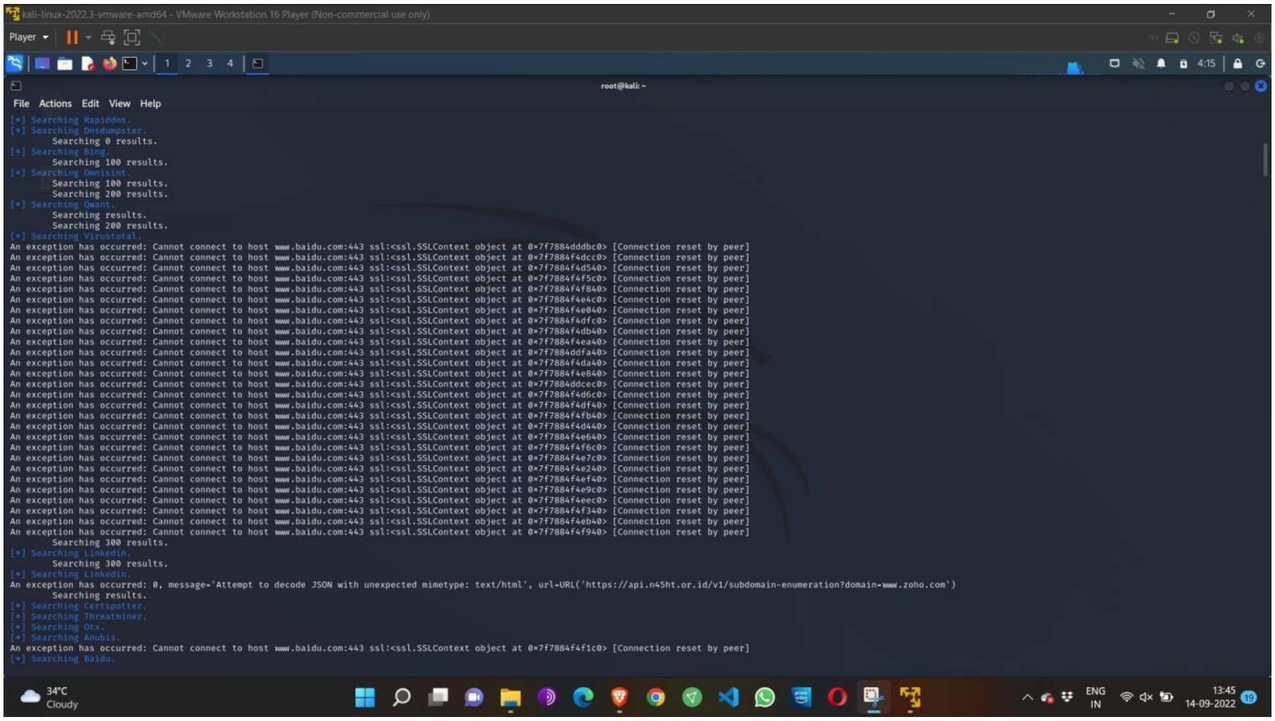
STEP 2: Run the following command

Command: theHarvester -d www.zoho.com -l 300 -b all

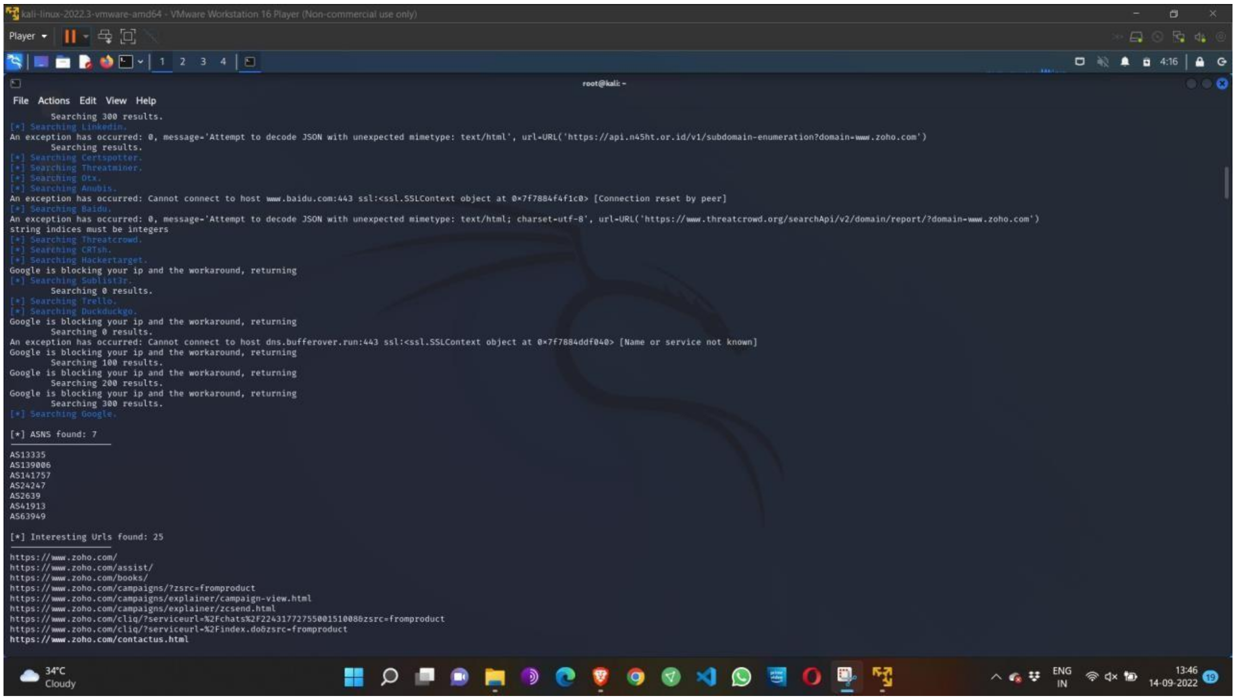


kali-linux-2022.3-vmware-amd64 - VMware Workstation 16 Player (Non-commercial use only)
Player
root@kali: ~
File Actions Edit View Help
34°C
Cloudy
ENG
IN
13:44
14-09-2022

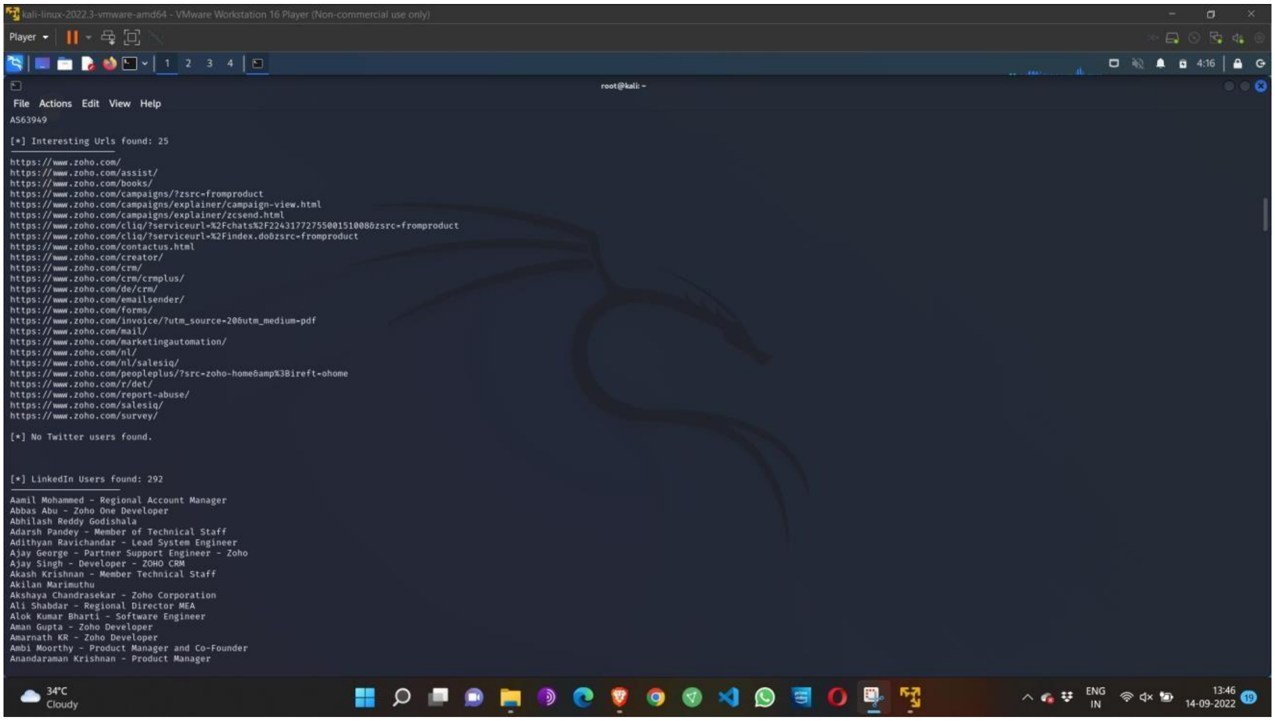
```
┌──(root㉿kali)-[~]
└─# theHarvester -d www.zoho.com -l 300 -b all

*******************************************************************
*                                                                 *
* theHarvester 4.0.3                                              *
* Coded by Christian Martorella                                   *
* Edge-Security Research                                          *
* cmartorella@edge-security.com                                   *
*                                                                 *
*******************************************************************


[*] Target: www.zoho.com


[!] Missing API key for fullhunt.

[!] Missing API key for Spyse.

[!] Missing API key for binaryedge.

[!] Missing API key for PentestTools.

[!] Missing API key for Securitytrail.

[!] Missing API key for ProjectDiscovery.

[!] Missing API key for Hunter.

[!] Missing API key for zoomeye.

[!] Missing API key for Censys ID and/or Secret.

[!] Missing API key for Intelx.

[!] Missing API key for RocketReach.

[!] Missing API key for Github.
[*] Searching Urlscan.
[*] Searching Rapiddns.
[*] Searching Dnsdumpster.
        Searching 0 results.
[*] Searching Bing.
        Searching 100 results.
[*] Searching Omnisint.
```


kali-linux-2022.3-vmware-amd64 - VMware Workstation 16 Player (Non-commercial use only)
Player
1 2 3 4
4:15
root@kali: ~
File Actions Edit View Help
34°C
Cloudy
ENG
IN
13:45
14-09-2022

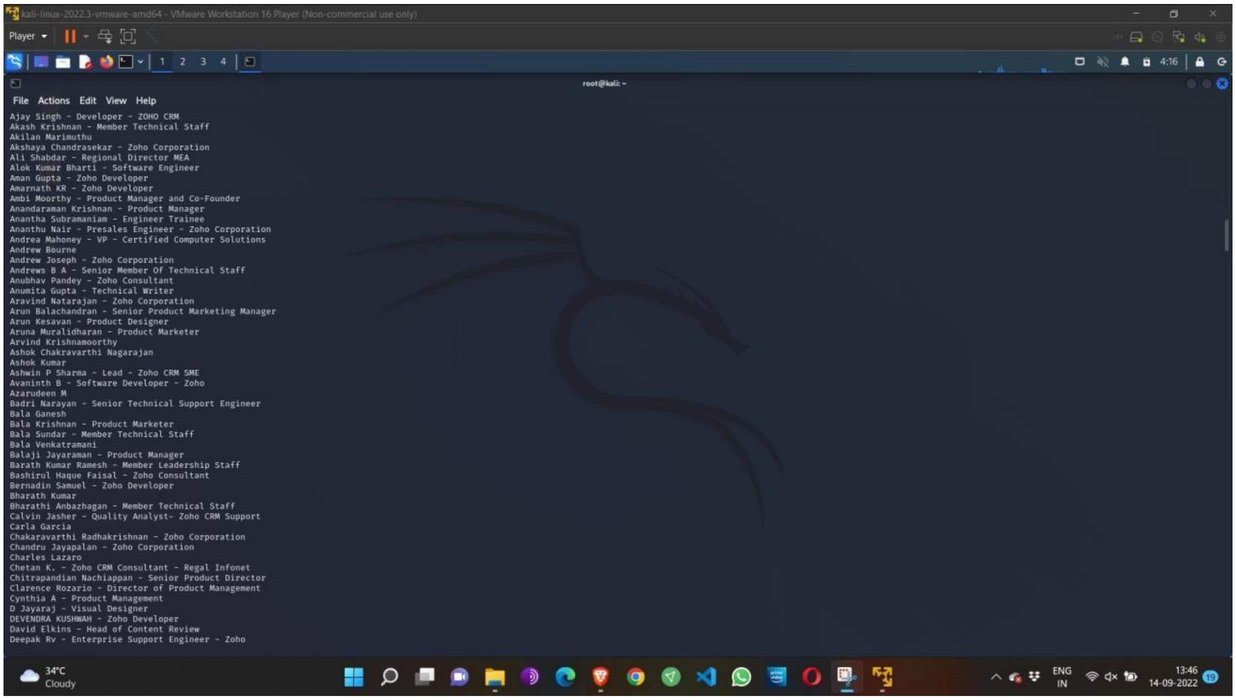
```
[*] Searching Rapiddns.
[*] Searching Dnsdumpster.
        Searching 0 results.
[*] Searching Bing.
        Searching 100 results.
[*] Searching Omnisint.
        Searching 100 results.
        Searching 200 results.
[*] Searching Qwant.
        Searching results.
        Searching 200 results.
[*] Searching Virustotal.
An exception has occurred: Cannot connect to host www.baidu.com:443 ssl:<ssl.SSLContext object at 0×7f7884dddbc0> [Connection reset by peer]
An exception has occurred: Cannot connect to host www.baidu.com:443 ssl:<ssl.SSLContext object at 0×7f7884f4dcc0> [Connection reset by peer]
An exception has occurred: Cannot connect to host www.baidu.com:443 ssl:<ssl.SSLContext object at 0×7f7884f4d540> [Connection reset by peer]
An exception has occurred: Cannot connect to host www.baidu.com:443 ssl:<ssl.SSLContext object at 0×7f7884f4f5c0> [Connection reset by peer]
An exception has occurred: Cannot connect to host www.baidu.com:443 ssl:<ssl.SSLContext object at 0×7f7884f4f840> [Connection reset by peer]
An exception has occurred: Cannot connect to host www.baidu.com:443 ssl:<ssl.SSLContext object at 0×7f7884f4e4c0> [Connection reset by peer]
An exception has occurred: Cannot connect to host www.baidu.com:443 ssl:<ssl.SSLContext object at 0×7f7884f4e040> [Connection reset by peer]
An exception has occurred: Cannot connect to host www.baidu.com:443 ssl:<ssl.SSLContext object at 0×7f7884f4dfc0> [Connection reset by peer]
An exception has occurred: Cannot connect to host www.baidu.com:443 ssl:<ssl.SSLContext object at 0×7f7884f4db40> [Connection reset by peer]
An exception has occurred: Cannot connect to host www.baidu.com:443 ssl:<ssl.SSLContext object at 0×7f7884f4ea40> [Connection reset by peer]
An exception has occurred: Cannot connect to host www.baidu.com:443 ssl:<ssl.SSLContext object at 0×7f7884ddfa40> [Connection reset by peer]
An exception has occurred: Cannot connect to host www.baidu.com:443 ssl:<ssl.SSLContext object at 0×7f7884f4da40> [Connection reset by peer]
An exception has occurred: Cannot connect to host www.baidu.com:443 ssl:<ssl.SSLContext object at 0×7f7884f4e840> [Connection reset by peer]
An exception has occurred: Cannot connect to host www.baidu.com:443 ssl:<ssl.SSLContext object at 0×7f7884ddcec0> [Connection reset by peer]
An exception has occurred: Cannot connect to host www.baidu.com:443 ssl:<ssl.SSLContext object at 0×7f7884f4d6c0> [Connection reset by peer]
An exception has occurred: Cannot connect to host www.baidu.com:443 ssl:<ssl.SSLContext object at 0×7f7884f4df40> [Connection reset by peer]
An exception has occurred: Cannot connect to host www.baidu.com:443 ssl:<ssl.SSLContext object at 0×7f7884f4fb40> [Connection reset by peer]
An exception has occurred: Cannot connect to host www.baidu.com:443 ssl:<ssl.SSLContext object at 0×7f7884f4d440> [Connection reset by peer]
An exception has occurred: Cannot connect to host www.baidu.com:443 ssl:<ssl.SSLContext object at 0×7f7884f4e640> [Connection reset by peer]
An exception has occurred: Cannot connect to host www.baidu.com:443 ssl:<ssl.SSLContext object at 0×7f7884f4f6c0> [Connection reset by peer]
An exception has occurred: Cannot connect to host www.baidu.com:443 ssl:<ssl.SSLContext object at 0×7f7884f4e7c0> [Connection reset by peer]
An exception has occurred: Cannot connect to host www.baidu.com:443 ssl:<ssl.SSLContext object at 0×7f7884f4e240> [Connection reset by peer]
An exception has occurred: Cannot connect to host www.baidu.com:443 ssl:<ssl.SSLContext object at 0×7f7884f4ef40> [Connection reset by peer]
An exception has occurred: Cannot connect to host www.baidu.com:443 ssl:<ssl.SSLContext object at 0×7f7884f4e9c0> [Connection reset by peer]
An exception has occurred: Cannot connect to host www.baidu.com:443 ssl:<ssl.SSLContext object at 0×7f7884f4eec0> [Connection reset by peer]
An exception has occurred: Cannot connect to host www.baidu.com:443 ssl:<ssl.SSLContext object at 0×7f7884f4f340> [Connection reset by peer]
An exception has occurred: Cannot connect to host www.baidu.com:443 ssl:<ssl.SSLContext object at 0×7f7884f4eb40> [Connection reset by peer]
An exception has occurred: Cannot connect to host www.baidu.com:443 ssl:<ssl.SSLContext object at 0×7f7884f4f940> [Connection reset by peer]
        Searching 300 results.
[*] Searching Linkedin.
        Searching 300 results.
[*] Searching Linkedin.
An exception has occurred: 0, message='Attempt to decode JSON with unexpected mimetype: text/html', url=URL('https://api.n45ht.or.id/v1/subdomain-enumeration?domain=www.zoho.com')
        Searching results.
[*] Searching Certspotter.
[*] Searching Threatminer.
[*] Searching Otx.
[*] Searching Anubis.
An exception has occurred: Cannot connect to host www.baidu.com:443 ssl:<ssl.SSLContext object at 0×7f7884f4f1c0> [Connection reset by peer]
[*] Searching Baidu.
```


kali-linux-2022.3-vmware-amd64 - VMware Workstation 16 Player (Non-commercial use only)
Player
1 2 3 4
4:16
root@kali: ~
File Actions Edit View Help
34°C
Cloudy
ENG
IN
13:46
14-09-2022

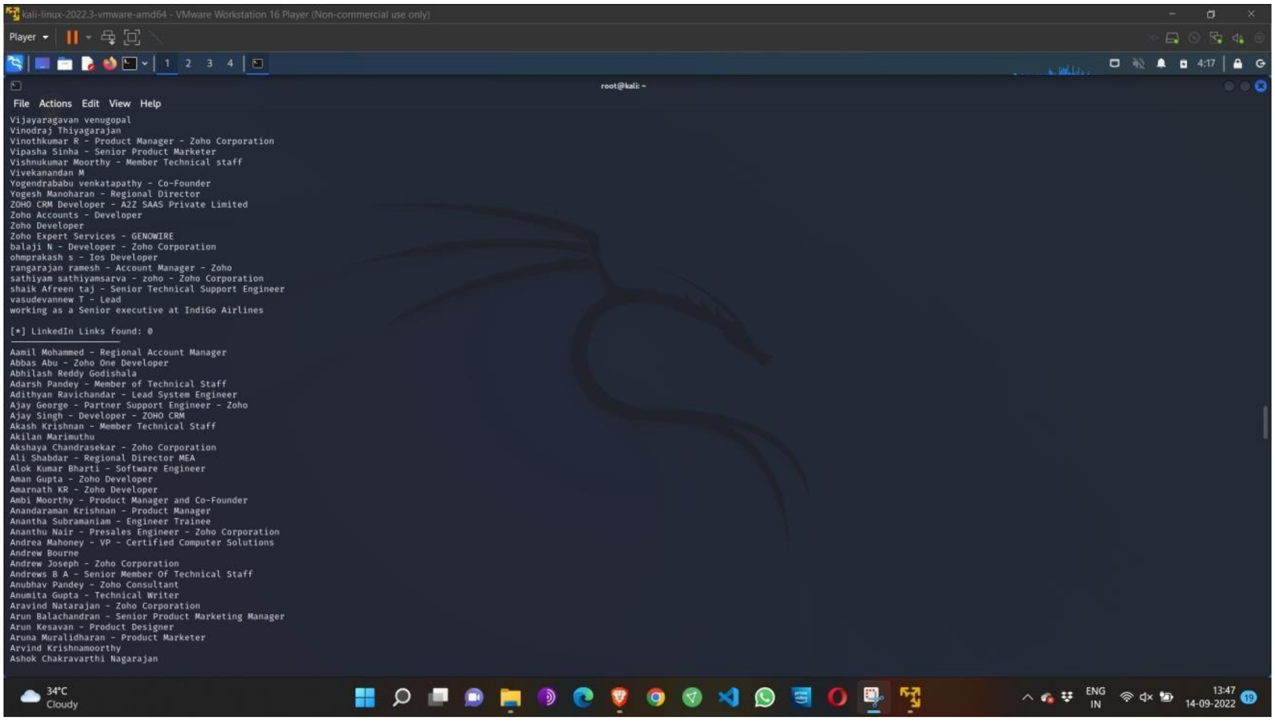
```
        Searching 300 results.
[*] Searching Linkedin.
An exception has occurred: 0, message='Attempt to decode JSON with unexpected mimetype: text/html', url=URL('https://api.n45ht.or.id/v1/subdomain-enumeration?domain=www.zoho.com')
        Searching results.
[*] Searching Certspotter.
[*] Searching Threatminer.
[*] Searching Otx.
[*] Searching Anubis.
An exception has occurred: Cannot connect to host www.baidu.com:443 ssl:<ssl.SSLContext object at 0×7f7884f4f1c0> [Connection reset by peer]
[*] Searching Baidu.
An exception has occurred: 0, message='Attempt to decode JSON with unexpected mimetype: text/html; charset=utf-8', url=URL('https://www.threatcrowd.org/searchApi/v2/domain/report/?domain=www.zoho.com')
string indices must be integers
[*] Searching Threatcrowd.
[*] Searching CRTsh.
[*] Searching Hackertarget.
Google is blocking your ip and the workaround, returning
[*] Searching Sublist3r.
        Searching 0 results.
[*] Searching Trello.
[*] Searching Duckduckgo.
Google is blocking your ip and the workaround, returning
        Searching 0 results.
An exception has occurred: Cannot connect to host dns.bufferover.run:443 ssl:<ssl.SSLContext object at 0×7f7884ddf040> [Name or service not known]
Google is blocking your ip and the workaround, returning
        Searching 100 results.
Google is blocking your ip and the workaround, returning
        Searching 200 results.
Google is blocking your ip and the workaround, returning
        Searching 300 results.
[*] Searching Google.

[*] ASNS found: 7
--------------------

AS13335
AS139006
AS141757
AS24247
AS2639
AS41913
AS63949

[*] Interesting Urls found: 25
--------------------

https://www.zoho.com/
https://www.zoho.com/assist/
https://www.zoho.com/books/
https://www.zoho.com/campaigns/?zsrc=fromproduct
https://www.zoho.com/campaigns/explainer/campaign-view.html
https://www.zoho.com/campaigns/explainer/zcsend.html
https://www.zoho.com/cliq/?serviceurl=%2Fchats%2F2243177275500151008&zsrc=fromproduct
https://www.zoho.com/cliq/?serviceurl=%2Findex.do&zsrc=fromproduct
https://www.zoho.com/contactus.html
```


kali-linux-2022.3-vmware-amd64 - VMware Workstation 16 Player (Non-commercial use only)
Player
root@kali: ~
File Actions Edit View Help
34°C
Cloudy
ENG
IN
13:46
14-09-2022

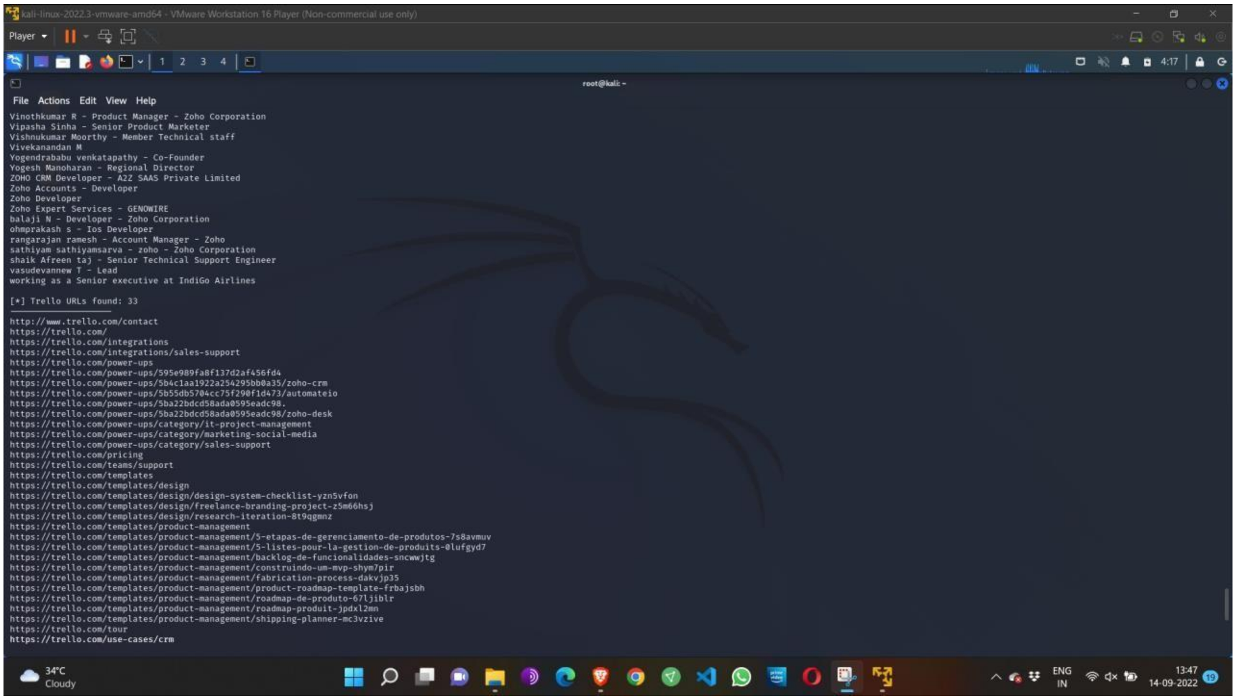
```
AS63949

[*] Interesting Urls found: 25
--------------------
https://www.zoho.com/
https://www.zoho.com/assist/
https://www.zoho.com/books/
https://www.zoho.com/campaigns/?zsrc=fromproduct
https://www.zoho.com/campaigns/explainer/campaign-view.html
https://www.zoho.com/campaigns/explainer/zcsend.html
https://www.zoho.com/cliq/?serviceurl=%2Fchats%2F2243177275500151008&zsrc=fromproduct
https://www.zoho.com/cliq/?serviceurl=%2Findex.do&zsrc=fromproduct
https://www.zoho.com/contactus.html
https://www.zoho.com/creator/
https://www.zoho.com/crm/
https://www.zoho.com/crm/crmplus/
https://www.zoho.com/de/crm/
https://www.zoho.com/emailsender/
https://www.zoho.com/forms/
https://www.zoho.com/invoice/?utm_source=20&utm_medium=pdf
https://www.zoho.com/mail/
https://www.zoho.com/marketingautomation/
https://www.zoho.com/nl/
https://www.zoho.com/nl/salesiq/
https://www.zoho.com/peopleplus/?src=zoho-home&amp%3Bireft=ohome
https://www.zoho.com/r/det/
https://www.zoho.com/report-abuse/
https://www.zoho.com/salesiq/
https://www.zoho.com/survey/

[*] No Twitter users found.


[*] LinkedIn Users found: 292
---------------------
Aamil Mohammed - Regional Account Manager
Abbas Abu - Zoho One Developer
Abhilash Reddy Godishala
Adarsh Pandey - Member of Technical Staff
Adithyan Ravichandar - Lead System Engineer
Ajay George - Partner Support Engineer - Zoho
Ajay Singh - Developer - ZOHO CRM
Akash Krishnan - Member Technical Staff
Akilan Marimuthu
Akshaya Chandrasekar - Zoho Corporation
Ali Shabdar - Regional Director MEA
Alok Kumar Bharti - Software Engineer
Aman Gupta - Zoho Developer
Amarnath KR - Zoho Developer
Ambi Moorthy - Product Manager and Co-Founder
Anandaraman Krishnan - Product Manager
```


kali-linux-2022.3-vmware-amd64 - VMware Workstation 16 Player (Non-commercial use only)
Player
root@kali: ~
File Actions Edit View Help
34°C
Cloudy
ENG
IN
13:46
14-09-2022

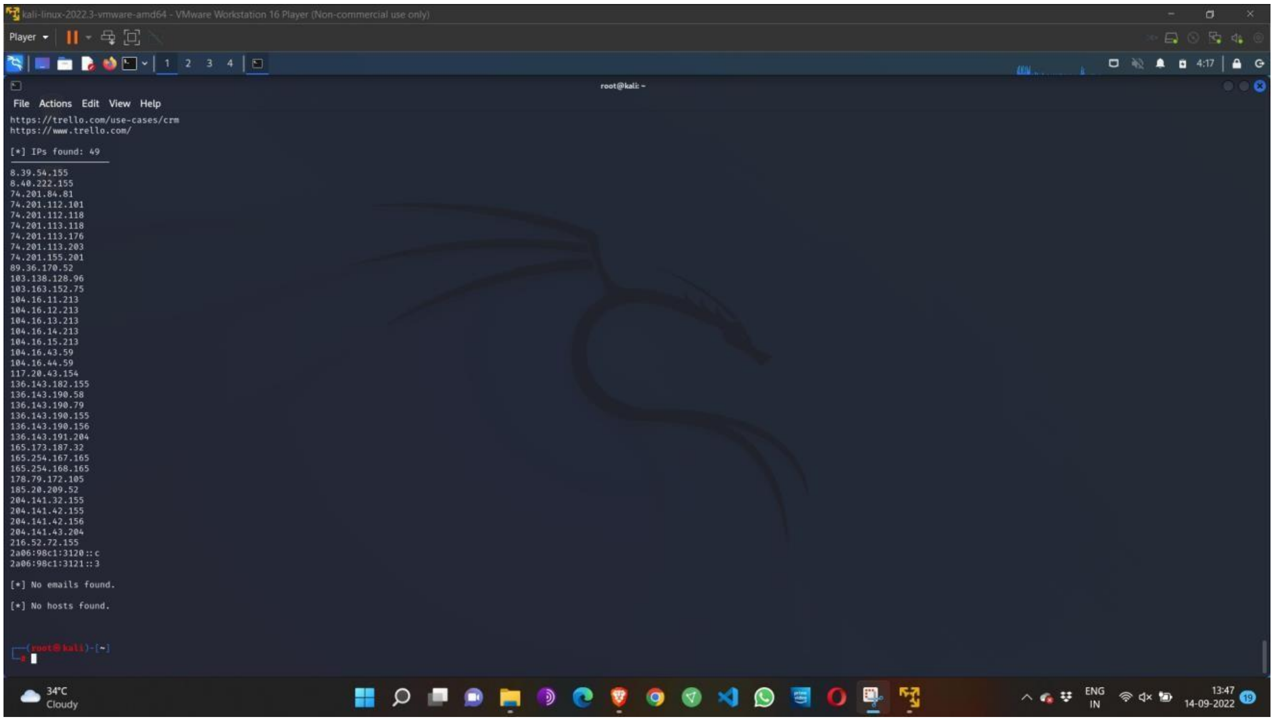
```
Ajay Singh - Developer - ZOHO CRM
Akash Krishnan - Member Technical Staff
Akilan Marimuthu
Akshaya Chandrasekar - Zoho Corporation
Ali Shabdar - Regional Director MEA
Alok Kumar Bharti - Software Engineer
Aman Gupta - Zoho Developer
Amarnath KR - Zoho Developer
Ambi Moorthy - Product Manager and Co-Founder
Anandaraman Krishnan - Product Manager
Anantha Subramaniam - Engineer Trainee
Ananthu Nair - Presales Engineer - Zoho Corporation
Andrea Mahoney - VP - Certified Computer Solutions
Andrew Bourne
Andrew Joseph - Zoho Corporation
Andrews B A - Senior Member Of Technical Staff
Anubhav Pandey - Zoho Consultant
Anumita Gupta - Technical Writer
Aravind Natarajan - Zoho Corporation
Arun Balachandran - Senior Product Marketing Manager
Arun Kesavan - Product Designer
Aruna Muralidharan - Product Marketer
Arvind Krishnamoorthy
Ashok Chakravarthi Nagarajan
Ashok Kumar
Ashwin P Sharma - Lead - Zoho CRM SME
Avaninth B - Software Developer - Zoho
Azarudeen M
Badri Narayan - Senior Technical Support Engineer
Bala Ganesh
Bala Krishnan - Product Marketer
Bala Sundar - Member Technical Staff
Bala Venkatramani
Balaji Jayaraman - Product Manager
Barath Kumar Ramesh - Member Leadership Staff
Bashirul Haque Faisal - Zoho Consultant
Bernadin Samuel - Zoho Developer
Bharath Kumar
Bharathi Anbazhagan - Member Technical Staff
Calvin Jasher - Quality Analyst- Zoho CRM Support
Carla Garcia
Chakaravarthi Radhakrishnan - Zoho Corporation
Chandru Jayapalan - Zoho Corporation
Charles Lazaro
Chetan K. - Zoho CRM Consultant - Regal Infonet
Chitrapandian Nachiappan - Senior Product Director
Clarence Rozario - Director of Product Management
Cynthia A - Product Management
D Jayaraj - Visual Designer
DEVENDRA KUSHWAH - Zoho Developer
David Elkins - Head of Content Review
Deepak Rv - Enterprise Support Engineer - Zoho
```


kali-linux-2022.3-vmware-amd64 - VMware Workstation 16 Player (Non-commercial use only)
Player
root@kali: ~
File Actions Edit View Help
4:17
34°C
Cloudy
ENG
IN
13:47
14-09-2022

```
Vijayaragavan venugopal
Vinodraj Thiyagarajan
Vinothkumar R - Product Manager - Zoho Corporation
Vipasha Sinha - Senior Product Marketer
Vishnukumar Moorthy - Member Technical staff
Vivekanandan M
Yogendrababu venkatapathy - Co-Founder
Yogesh Manoharan - Regional Director
ZOHO CRM Developer - A2Z SAAS Private Limited
Zoho Accounts - Developer
Zoho Developer
Zoho Expert Services - GENOWIRE
balaji N - Developer - Zoho Corporation
ohmprakash s - Ios Developer
rangarajan ramesh - Account Manager - Zoho
sathiyam sathiyamsarva - zoho - Zoho Corporation
shaik Afreen taj - Senior Technical Support Engineer
vasudevannew T - Lead
working as a Senior executive at IndiGo Airlines

[*] LinkedIn Links found: 0
────────────────────

Aamil Mohammed - Regional Account Manager
Abbas Abu - Zoho One Developer
Abhilash Reddy Godishala
Adarsh Pandey - Member of Technical Staff
Adithyan Ravichandar - Lead System Engineer
Ajay George - Partner Support Engineer - Zoho
Ajay Singh - Developer - ZOHO CRM
Akash Krishnan - Member Technical Staff
Akilan Marimuthu
Akshaya Chandrasekar - Zoho Corporation
Ali Shabdar - Regional Director MEA
Alok Kumar Bharti - Software Engineer
Aman Gupta - Zoho Developer
Amarnath KR - Zoho Developer
Ambi Moorthy - Product Manager and Co-Founder
Anandaraman Krishnan - Product Manager
Anantha Subramaniam - Engineer Trainee
Ananthu Nair - Presales Engineer - Zoho Corporation
Andrea Mahoney - VP - Certified Computer Solutions
Andrew Bourne
Andrew Joseph - Zoho Corporation
Andrews B A - Senior Member Of Technical Staff
Anubhav Pandey - Zoho Consultant
Anumita Gupta - Technical Writer
Aravind Natarajan - Zoho Corporation
Arun Balachandran - Senior Product Marketing Manager
Arun Kesavan - Product Designer
Aruna Muralidharan - Product Marketer
Arvind Krishnamoorthy
Ashok Chakravarthi Nagarajan
```


kali-linux-2022.3-vmware-amd64 - VMware Workstation 16 Player (Non-commercial use only)
Player
root@kali: ~
File Actions Edit View Help
4:17
34°C
Cloudy
ENG
IN
13:47
14-09-2022

```
Vinothkumar R - Product Manager - Zoho Corporation
Vipasha Sinha - Senior Product Marketer
Vishnukumar Moorthy - Member Technical staff
Vivekanandan M
Yogendrababu venkatapathy - Co-Founder
Yogesh Manoharan - Regional Director
ZOHO CRM Developer - A2Z SAAS Private Limited
Zoho Accounts - Developer
Zoho Developer
Zoho Expert Services - GENOWIRE
balaji N - Developer - Zoho Corporation
ohmprakash s - Ios Developer
rangarajan ramesh - Account Manager - Zoho
sathiyam sathiyamsarva - zoho - Zoho Corporation
shaik Afreen taj - Senior Technical Support Engineer
vasudevannew T - Lead
working as a Senior executive at IndiGo Airlines

[*] Trello URLs found: 33
────────────────────

http://www.trello.com/contact
https://trello.com/
https://trello.com/integrations
https://trello.com/integrations/sales-support
https://trello.com/power-ups
https://trello.com/power-ups/595e989fa8f137d2af456fd4
https://trello.com/power-ups/5b4c1aa1922a254295bb0a35/zoho-crm
https://trello.com/power-ups/5b55db5704cc75f290f1d473/automateio
https://trello.com/power-ups/5ba22bdcd58ada0595eadc98.
https://trello.com/power-ups/5ba22bdcd58ada0595eadc98/zoho-desk
https://trello.com/power-ups/category/it-project-management
https://trello.com/power-ups/category/marketing-social-media
https://trello.com/power-ups/category/sales-support
https://trello.com/pricing
https://trello.com/teams/support
https://trello.com/templates
https://trello.com/templates/design
https://trello.com/templates/design/design-system-checklist-yzn5vfon
https://trello.com/templates/design/freelance-branding-project-z5m66hsj
https://trello.com/templates/design/research-iteration-8t9qgmnz
https://trello.com/templates/product-management
https://trello.com/templates/product-management/5-etapas-de-gerenciamento-de-produtos-7s8avmuv
https://trello.com/templates/product-management/5-listes-pour-la-gestion-de-produits-0lufgyd7
https://trello.com/templates/product-management/backlog-de-funcionalidades-sncwwjtg
https://trello.com/templates/product-management/construindo-um-mvp-shym7pir
https://trello.com/templates/product-management/fabrication-process-dakvjp35
https://trello.com/templates/product-management/product-roadmap-template-frbajsbh
https://trello.com/templates/product-management/roadmap-de-produto-67ljiblr
https://trello.com/templates/product-management/roadmap-produit-jpdxl2mn
https://trello.com/templates/product-management/shipping-planner-mc3vzive
https://trello.com/tour
https://trello.com/use-cases/crm
```



kali-linux-2022.3-vmware-amd64 - VMware Workstation 16 Player (Non-commercial use only)
Player
root@kali: ~
File Actions Edit View Help
34°C
Cloudy
13:47
14-09-2022

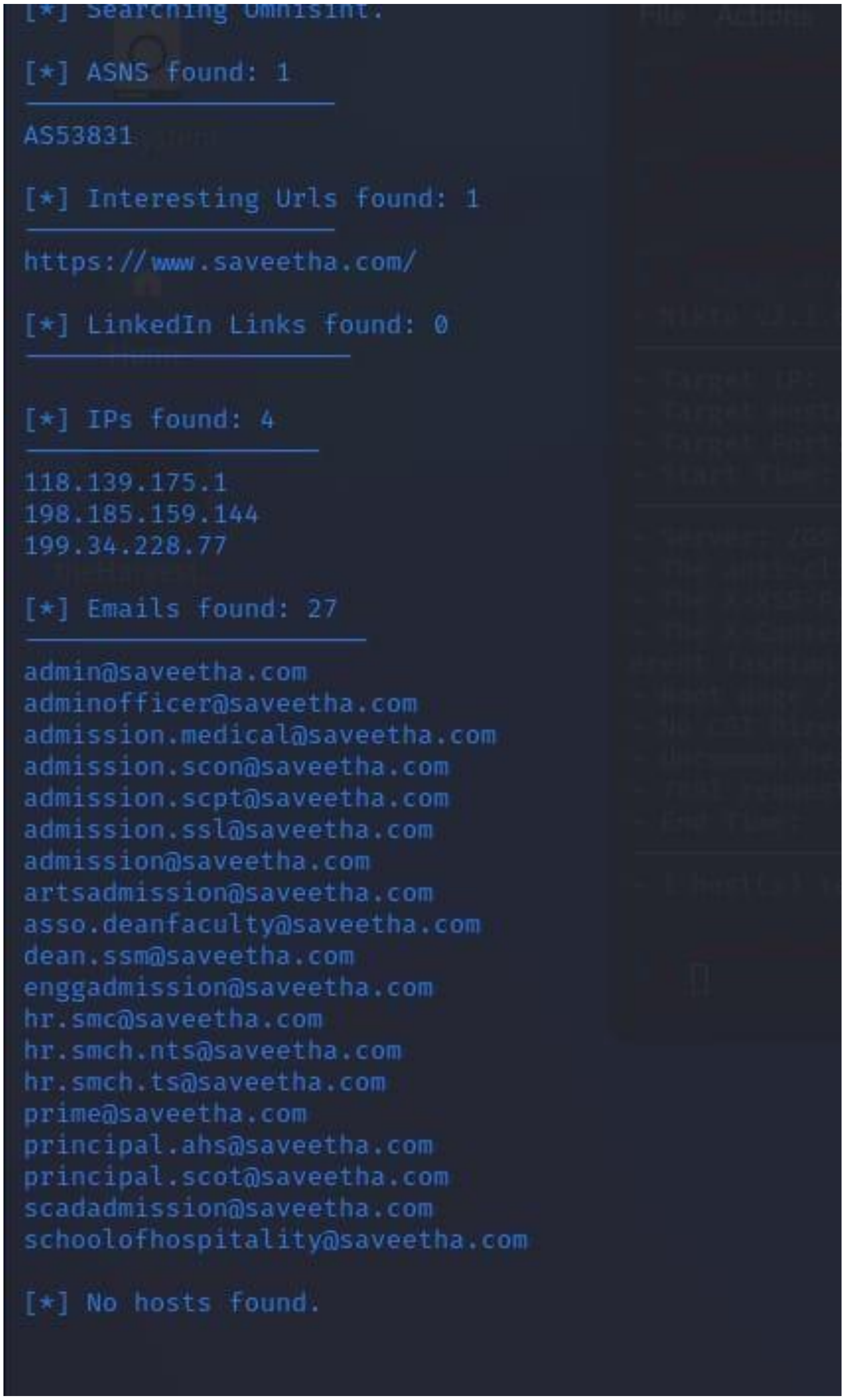
```
https://trello.com/use-cases/crm
https://www.trello.com/

[*] IPs found: 49
-------------------
8.39.54.155
8.40.222.155
74.201.84.81
74.201.112.101
74.201.112.118
74.201.113.118
74.201.113.176
74.201.113.203
74.201.155.201
89.36.170.52
103.138.128.96
103.163.152.75
104.16.11.213
104.16.12.213
104.16.13.213
104.16.14.213
104.16.15.213
104.16.43.59
104.16.44.59
117.20.43.154
136.143.182.155
136.143.190.58
136.143.190.79
136.143.190.155
136.143.190.156
136.143.191.204
165.173.187.32
165.254.167.165
165.254.168.165
178.79.172.105
185.20.209.52
204.141.32.155
204.141.42.155
204.141.42.156
204.141.43.204
216.52.72.155
2a06:98c1:3120::c
2a06:98c1:3121::3

[*] No emails found.

[*] No hosts found.


┌──(root㉿kali)-[~]
└─#
```

Step 4: run this command “**theHarvester -d 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:

1)



```
[*] Searching Omnisint.

[*] ASNS found: 1
--------------------
AS53831

[*] Interesting Urls found: 1
--------------------
https://www.saveetha.com/

[*] LinkedIn Links found: 0
---------------------


[*] IPs found: 4
-------------------
118.139.175.1
198.185.159.144
199.34.228.77

[*] Emails found: 27
----------------------
admin@saveetha.com
adminofficer@saveetha.com
admission.medical@saveetha.com
admission.scon@saveetha.com
admission.scpt@saveetha.com
admission.ssl@saveetha.com
admission@saveetha.com
artsadmission@saveetha.com
asso.deanfaculty@saveetha.com
dean.ssm@saveetha.com
enggadmission@saveetha.com
hr.smc@saveetha.com
hr.smch.nts@saveetha.com
hr.smch.ts@saveetha.com
prime@saveetha.com
principal.ahs@saveetha.com
principal.scot@saveetha.com
scadadmission@saveetha.com
schoolofhospitality@saveetha.com

[*] No hosts found.
```

Result:

The above-mentioned experiment is done using theHarvester in kali Linux server. The information is gathered using theHarvester.

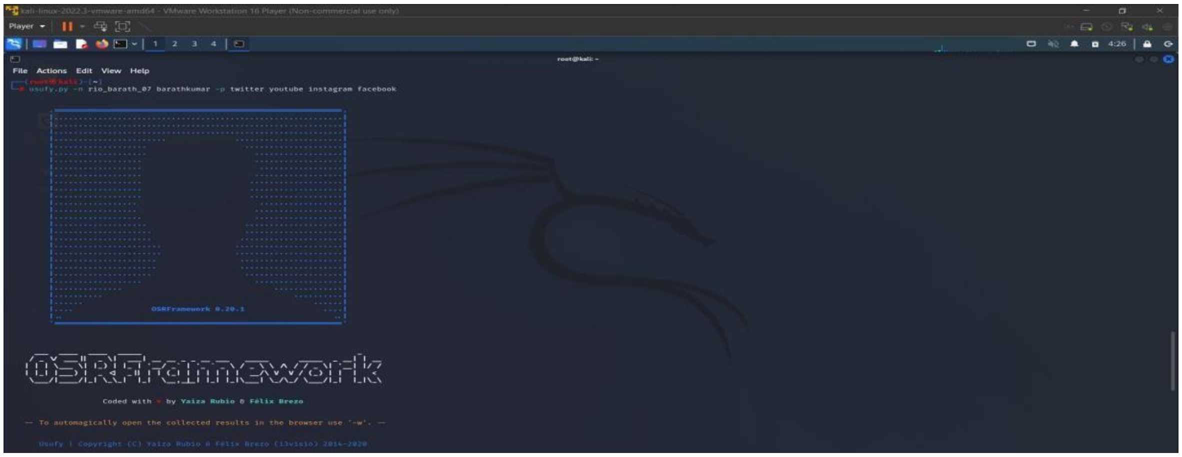
Exercise No 4 - Open Source Intelligence Gathering Using OSRFramework

Aim: To Checks for the Existence of a Profile for given user details in differentplatforms
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 twitterfacebook youtube
```

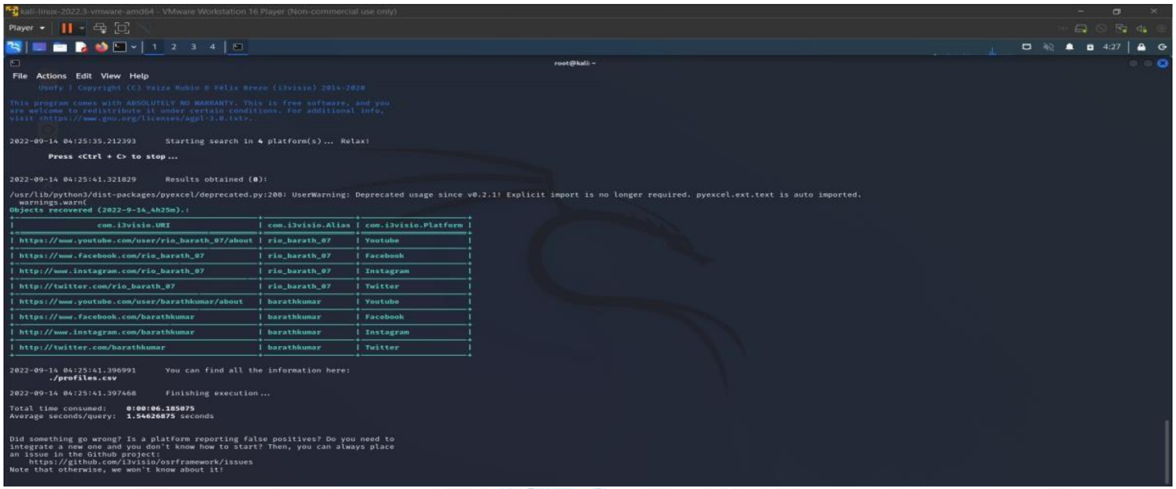


kali-linux-2022.3-vmware-amd64 - VMware Workstation 16 Player (Non-commercial use only)
Player
1
2
3
4
root@kali: ~
File
Actions
Edit
View
Help

```
┌──(root㉿kali)-[~]
└─# usufy.py -n rio_barath_07 barathkumar -p twitter youtube instagram facebook

                         OSRFramework 0.20.1

OSRFramework

                Coded with ♥ by Yaiza Rubio & Félix Brezo

 — To automagically open the collected results in the browser use '-w'. —

    Usufy | Copyright (C) Yaiza Rubio & Félix Brezo (i3visio) 2014-2020
```

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

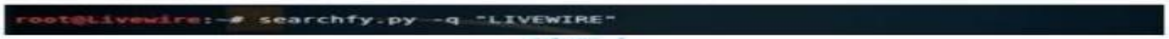
The usufy.py will search the user details in the mentioned platformand will provide you with the existence of the user


kali-linux-2022.3-vmware-amd64 - VMware Workstation 16 Player (Non-commercial use only)
Player
1
2
3
4
root@kali: ~
4:27
File
Actions
Edit
View
Help

```
      Usufy | Copyright (C) Yaiza Rubio & Félix Brezo (i3visio) 2014-2020

This program comes with ABSOLUTELY NO WARRANTY. This is free software, and you
are welcome to redistribute it under certain conditions. For additional info,
visit <https://www.gnu.org/licenses/agpl-3.0.txt>.


2022-09-14 04:25:35.212393      Starting search in 4 platform(s)... Relax!

        Press <Ctrl + C> to stop ...


2022-09-14 04:25:41.321829      Results obtained (8):

/usr/lib/python3/dist-packages/pyexcel/deprecated.py:208: UserWarning: Deprecated usage since v0.2.1! Explicit import is no longer required. pyexcel.ext.text is auto imported.
  warnings.warn(
Objects recovered (2022-9-14_4h25m).:
+-----------------------------------------------+-------------------+----------------------+
|                com.i3visio.URI                | com.i3visio.Alias | com.i3visio.Platform |
+===============================================+===================+======================+
| https://www.youtube.com/user/rio_barath_07/about | rio_barath_07  | Youtube              |
+-----------------------------------------------+-------------------+----------------------+
| https://www.facebook.com/rio_barath_07        | rio_barath_07     | Facebook             |
+-----------------------------------------------+-------------------+----------------------+
| http://www.instagram.com/rio_barath_07        | rio_barath_07     | Instagram            |
+-----------------------------------------------+-------------------+----------------------+
| http://twitter.com/rio_barath_07              | rio_barath_07     | Twitter              |
+-----------------------------------------------+-------------------+----------------------+
| https://www.youtube.com/user/barathkumar/about | barathkumar      | Youtube              |
+-----------------------------------------------+-------------------+----------------------+
| https://www.facebook.com/barathkumar          | barathkumar       | Facebook             |
+-----------------------------------------------+-------------------+----------------------+
| http://www.instagram.com/barathkumar          | barathkumar       | Instagram            |
+-----------------------------------------------+-------------------+----------------------+
| http://twitter.com/barathkumar                | barathkumar       | Twitter              |
+-----------------------------------------------+-------------------+----------------------+

2022-09-14 04:25:41.396991      You can find all the information here:
        ./profiles.csv

2022-09-14 04:25:41.397468      Finishing execution ...

Total time consumed:    0:00:06.185075
Average seconds/query:  1.54626875 seconds


Did something go wrong? Is a platform reporting false positives? Do you need to
integrate a new one and you don't know how to start? Then, you can always place
an issue in the Github project:
    https://github.com/i3visio/osrframework/issues
Note that otherwise, we won't know about it!
```

FIGURE. 8

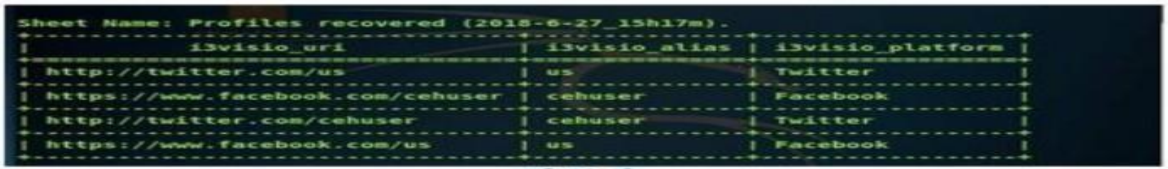
Step 5: Searchfy.py checks with the existing users of a page/handlers for given details in the all social networking platforms. Type searchfy.py -q <Page Name or Handler Name> and press Enter.



```
root@Livewire:~# searchfy.py -q "LIVEWIRE"
```

FIGURE. 9

Step 6: It will put out all the details who are subscribed to target social networking pages that are provided.



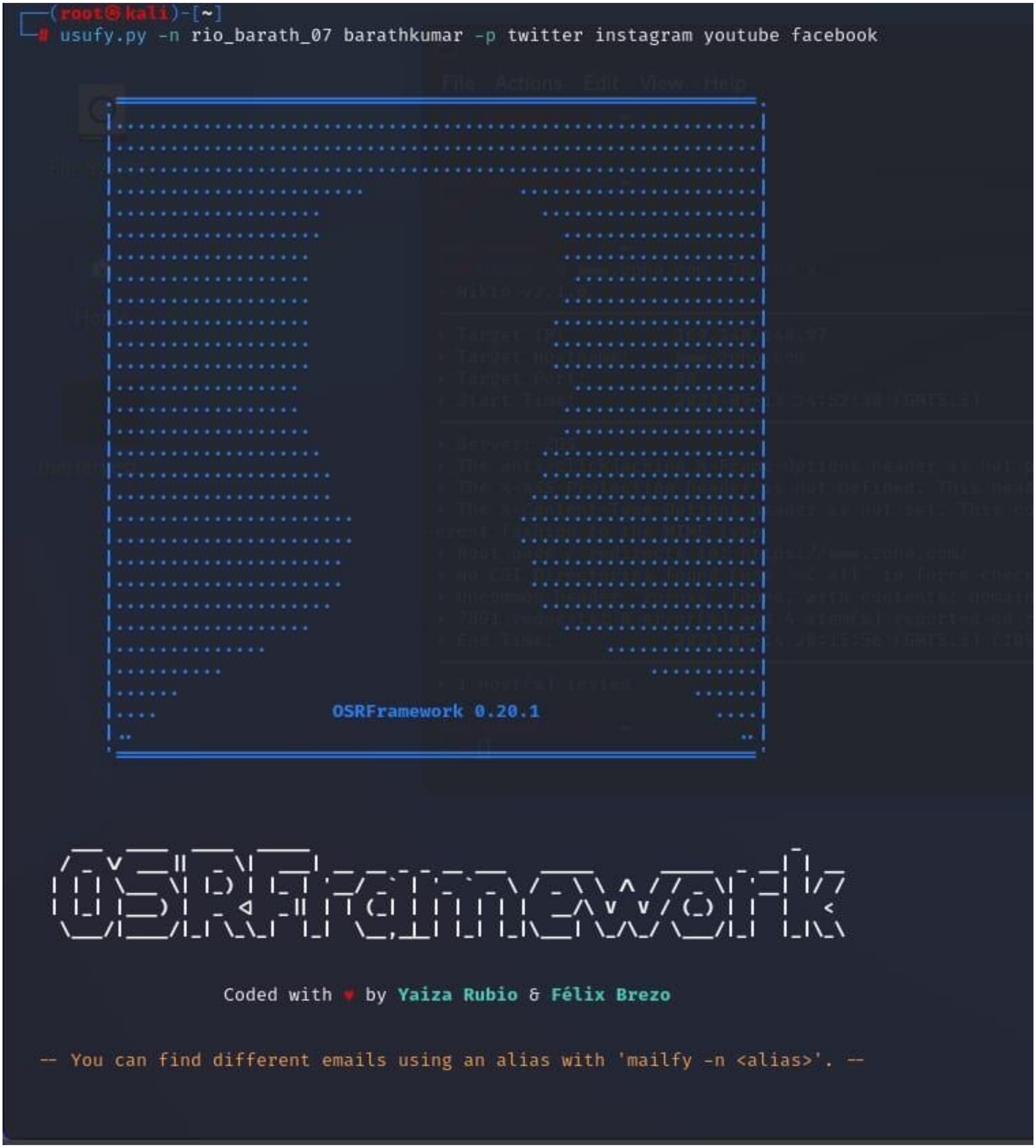
```
Sheet Name: Profiles recovered (2018-6-27_15h17m).
+----------------------------------+------------------+-----------------------+
|           i3visio_uri            |  i3visio_alias   |  i3visio_platform     |
+==================================+==================+=======================+
| http://twitter.com/us            | us               | Twitter               |
+----------------------------------+------------------+-----------------------+
| https://www.facebook.com/cehuser | cehuser          | Facebook              |
+----------------------------------+------------------+-----------------------+
| http://twitter.com/cehuser       | cehuser          | Twitter               |
+----------------------------------+------------------+-----------------------+
| https://www.facebook.com/us      | us               | Facebook              |
+----------------------------------+------------------+-----------------------+
```

FIGURE. 10

Collect and note the information disclosed about the target

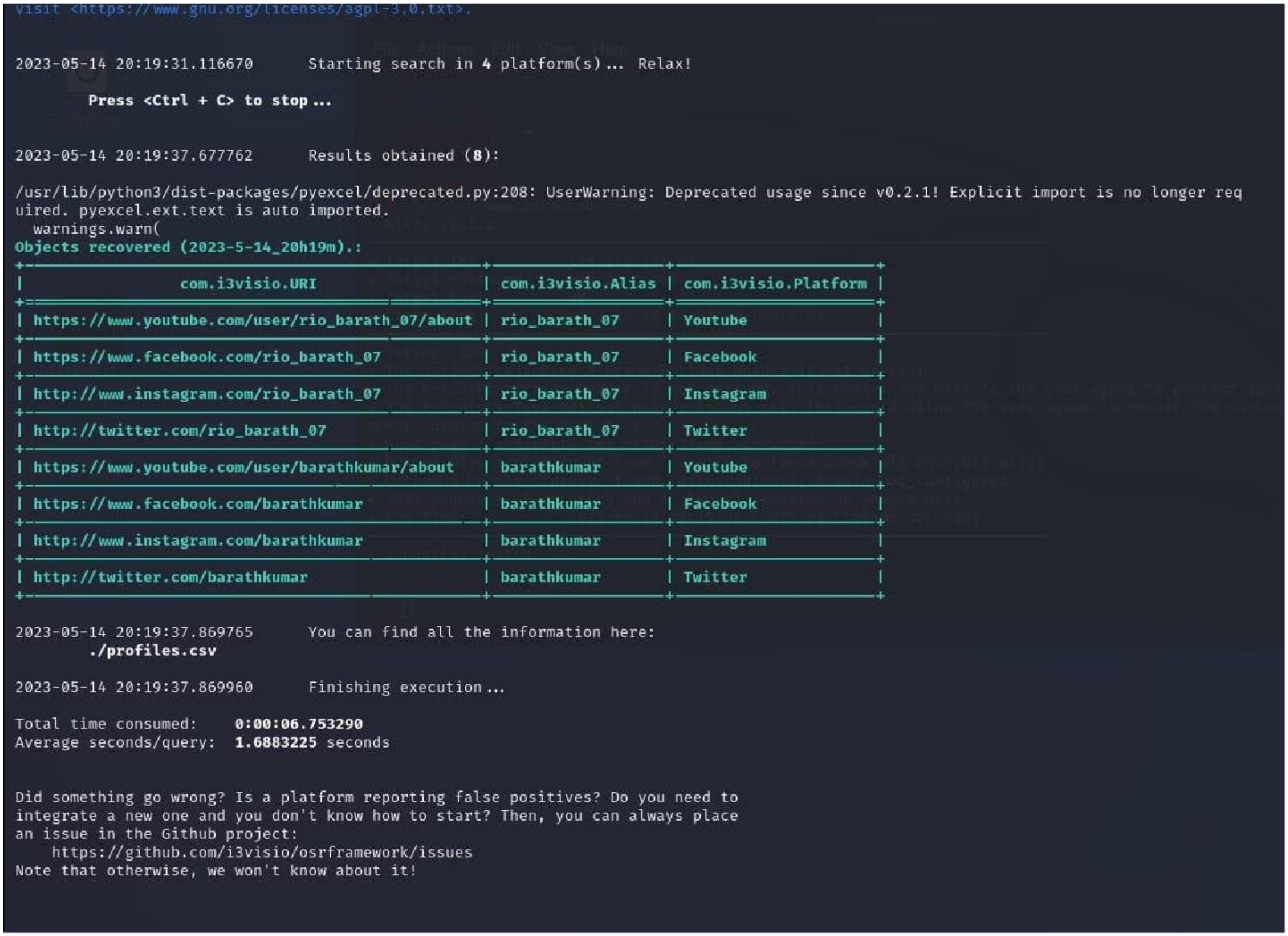
Output:

1)



```
┌──(root㉿kali)-[~]
└─# usufy.py -n rio_barath_07 barathkumar -p twitter instagram youtube facebook

                    OSRFramework 0.20.1

          Coded with ♥ by Yaiza Rubio & Félix Brezo

 -- You can find different emails using an alias with 'mailfy -n <alias>'. --
```

2)



```
visit <https://www.gnu.org/licenses/agpl-3.0.txt>.


2023-05-14 20:19:31.116670      Starting search in 4 platform(s)...  Relax!

        Press <Ctrl + C> to stop...


2023-05-14 20:19:37.677762      Results obtained (8):

/usr/lib/python3/dist-packages/pyexcel/deprecated.py:208: UserWarning: Deprecated usage since v0.2.1! Explicit import is no longer req
uired. pyexcel.ext.text is auto imported.
  warnings.warn(
Objects recovered (2023-5-14_20h19m).:
+--------------------------------------------------+-------------------+----------------------+
|                 com.i3visio.URI                  | com.i3visio.Alias | com.i3visio.Platform |
+==================================================+===================+======================+
| https://www.youtube.com/user/rio_barath_07/about | rio_barath_07     | Youtube              |
+--------------------------------------------------+-------------------+----------------------+
| https://www.facebook.com/rio_barath_07           | rio_barath_07     | Facebook             |
+--------------------------------------------------+-------------------+----------------------+
| http://www.instagram.com/rio_barath_07           | rio_barath_07     | Instagram            |
+--------------------------------------------------+-------------------+----------------------+
| http://twitter.com/rio_barath_07                 | rio_barath_07     | Twitter              |
+--------------------------------------------------+-------------------+----------------------+
| https://www.youtube.com/user/barathkumar/about   | barathkumar       | Youtube              |
+--------------------------------------------------+-------------------+----------------------+
| https://www.facebook.com/barathkumar             | barathkumar       | Facebook             |
+--------------------------------------------------+-------------------+----------------------+
| http://www.instagram.com/barathkumar             | barathkumar       | Instagram            |
+--------------------------------------------------+-------------------+----------------------+
| http://twitter.com/barathkumar                   | barathkumar       | Twitter              |
+--------------------------------------------------+-------------------+----------------------+

2023-05-14 20:19:37.869765      You can find all the information here:
        ./profiles.csv

2023-05-14 20:19:37.869960      Finishing execution...

Total time consumed:    0:00:06.753290
Average seconds/query:  1.6883225 seconds


Did something go wrong? Is a platform reporting false positives? Do you need to
integrate a new one and you don't know how to start? Then, you can always place
an issue in the Github project:
    https://github.com/i3visio/osrframework/issues
Note that otherwise, we won't know about it!
```

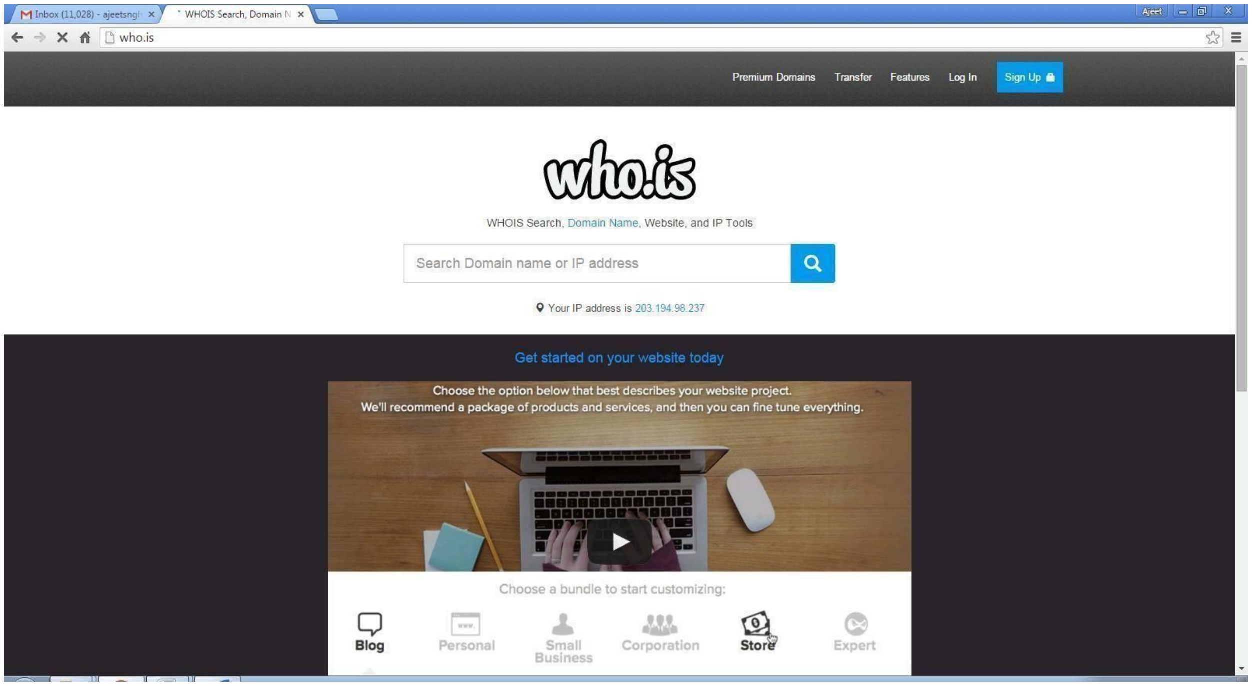
Result:

The current experiment is about Open-Source Intelligence Gathering is done using OSR Framework. This experiment is done to check for the Existence of a Profile for given user details in different platforms. This experiment is executed in root terminal using kali linux operating system.

Exercise NO 5: Use Google and Whois for Reconnaisasance.

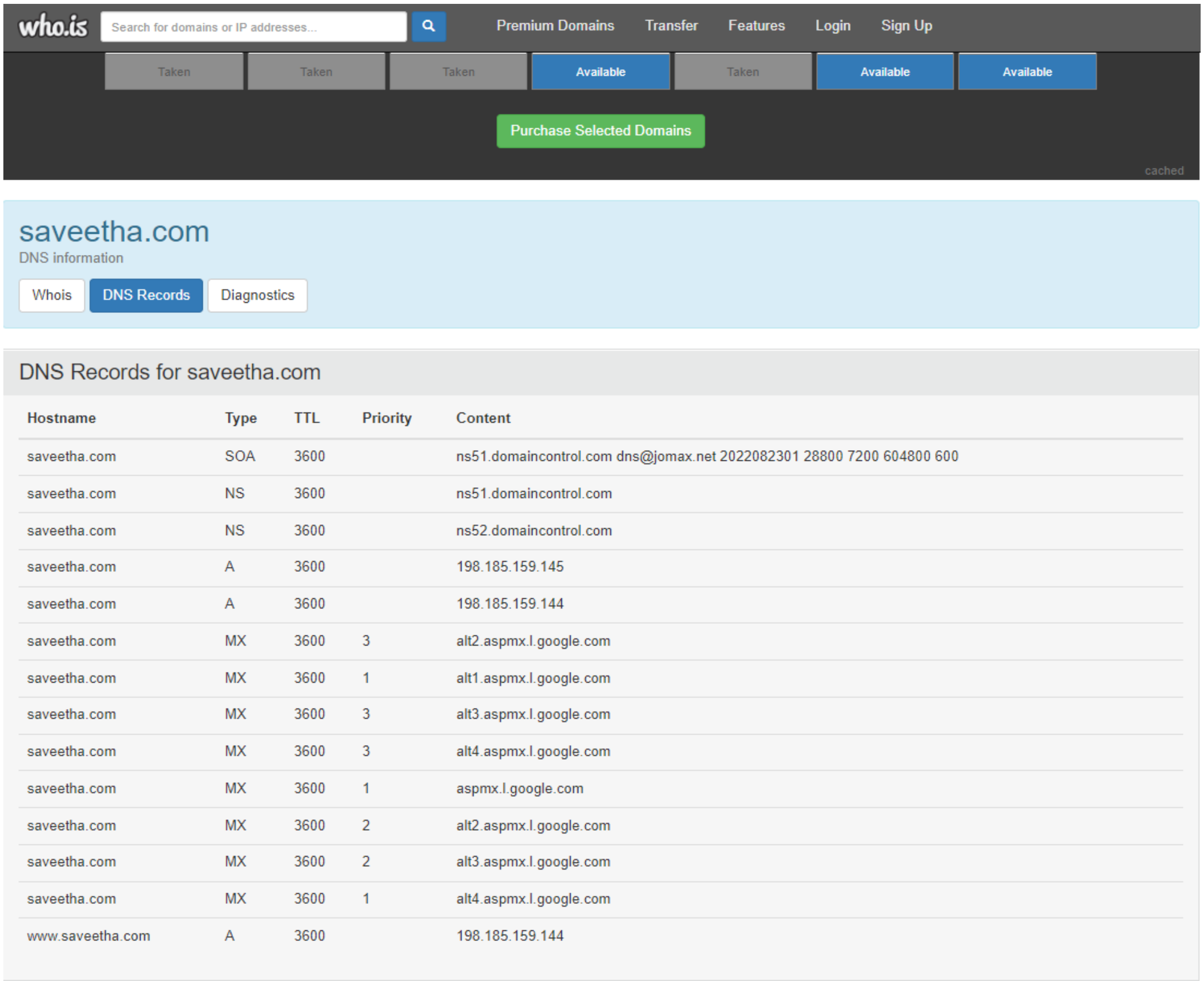
Aim: To find out the Whois, DNS Records and Diagonstics for particular website by using Whois search.
Procedure:

Step1: Open the WHO.is website


Inbox (11,028) - ajeetsngh
WHOIS Search, Domain N
Ajeet
who.is
Premium Domains
Transfer
Features
Log In
Sign Up
who.is
WHOIS Search, Domain Name, Website, and IP Tools
Search Domain name or IP address
Your IP address is 203.194.98.237
Get started on your website today
Choose a bundle to start customizing:
Blog
Personal
Small Business
Corporation
Store
Expert

Choose the option below that best describes your website project.
We'll recommend a package of products and services, and then you can fine tune everything.

Step 2: Enter the website name in search bar and hit the “Enter button”.
Step 3: Show you information about www.saveetha.com

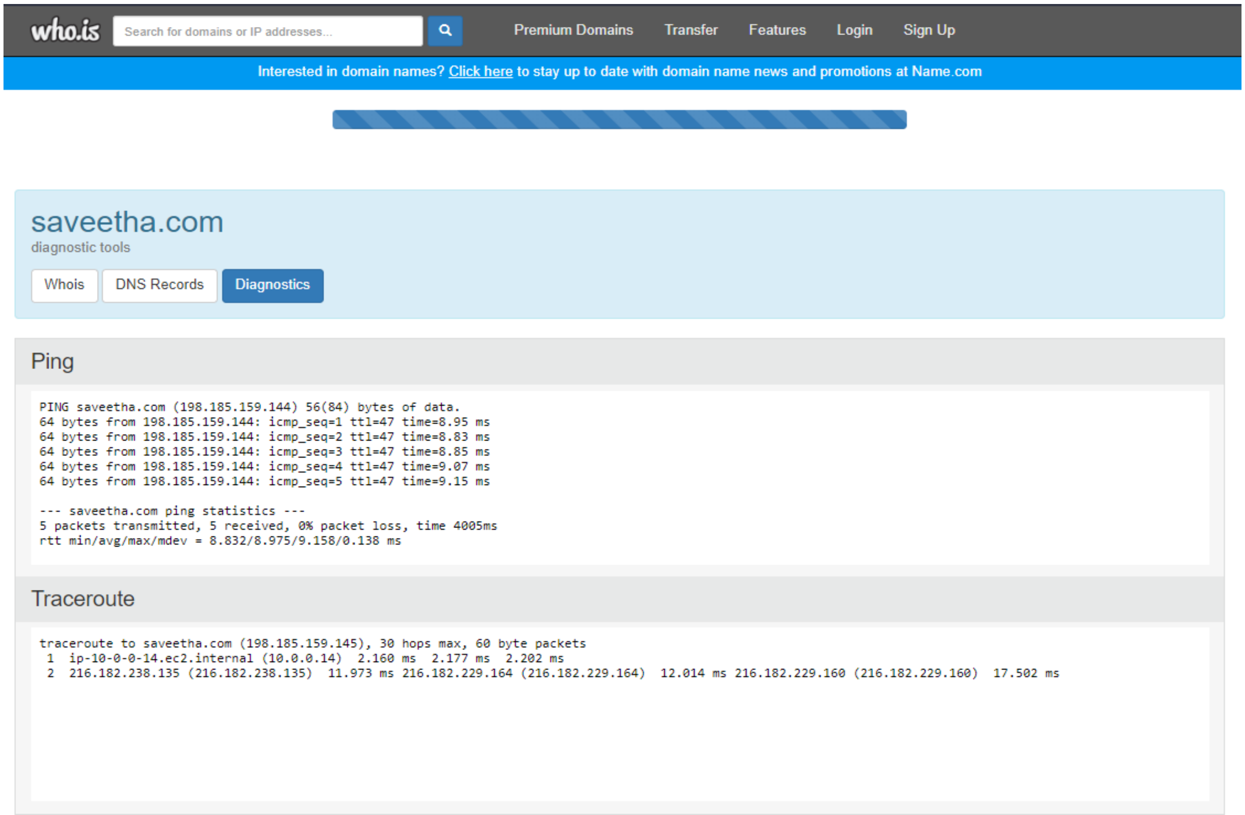


saveetha.com

DNS information

DNS Records for saveetha.com

Hostname	Type	TTL	Priority	Content
saveetha.com	SOA	3600		ns51.domaincontrol.com dns@jomax.net 2022082301 28800 7200 604800 600
saveetha.com	NS	3600		ns51.domaincontrol.com
saveetha.com	NS	3600		ns52.domaincontrol.com
saveetha.com	A	3600		198.185.159.145
saveetha.com	A	3600		198.185.159.144
saveetha.com	MX	3600	3	alt2.aspmx.l.google.com
saveetha.com	MX	3600	1	alt1.aspmx.l.google.com
saveetha.com	MX	3600	3	alt3.aspmx.l.google.com
saveetha.com	MX	3600	3	alt4.aspmx.l.google.com
saveetha.com	MX	3600	1	aspmx.l.google.com
saveetha.com	MX	3600	2	alt2.aspmx.l.google.com
saveetha.com	MX	3600	2	alt3.aspmx.l.google.com
saveetha.com	MX	3600	1	alt4.aspmx.l.google.com
www.saveetha.com	A	3600		198.185.159.144



Interested in domain names? Click here to stay up to date with domain name news and promotions at Name.com

saveetha.com

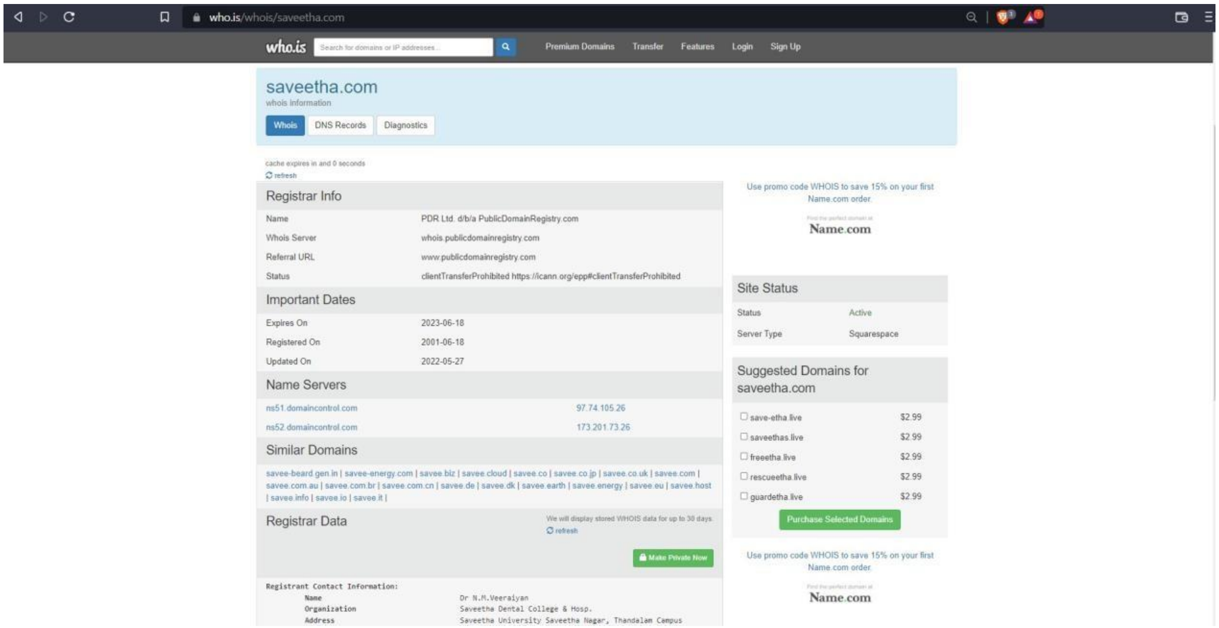
diagnostic tools

Ping

```
PING saveetha.com (198.185.159.144) 56(84) bytes of data.
64 bytes from 198.185.159.144: icmp_seq=1 ttl=47 time=8.95 ms
64 bytes from 198.185.159.144: icmp_seq=2 ttl=47 time=8.83 ms
64 bytes from 198.185.159.144: icmp_seq=3 ttl=47 time=8.85 ms
64 bytes from 198.185.159.144: icmp_seq=4 ttl=47 time=9.07 ms
64 bytes from 198.185.159.144: icmp_seq=5 ttl=47 time=9.15 ms

--- saveetha.com ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4005ms
rtt min/avg/max/mdev = 8.832/8.975/9.158/0.138 ms
```

Traceroute

```
traceroute to saveetha.com (198.185.159.145), 30 hops max, 60 byte packets
 1  ip-10-0-0-14.ec2.internal (10.0.0.14)  2.160 ms  2.177 ms  2.202 ms
 2  216.182.238.135 (216.182.238.135)  11.973 ms 216.182.229.164 (216.182.229.164)  12.014 ms 216.182.229.160 (216.182.229.160)  17.502 ms
```


who.is/whois/saveetha.com
who.is
Search for domains or IP addresses...
Premium Domains
Transfer
Features
Login
Sign Up
Whois
DNS Records
Diagnostics
refresh
Make Private Now
Purchase Selected Domains
Find the perfect domain at
Name.com

saveetha.com

whois information

cache expires in and 0 seconds

Registrar Info

Name	PDR Ltd. d/b/a PublicDomainRegistry.com
Whois Server	whois.publicdomainregistry.com
Referral URL	www.publicdomainregistry.com
Status	clientTransferProhibited https://icann.org/epp#clientTransferProhibited

Important Dates

Expires On	2023-06-18
Registered On	2001-06-18
Updated On	2022-05-27

Name Servers

ns51.domaincontrol.com	97.74.105.26
ns52.domaincontrol.com	173.201.73.26

Similar Domains

savee-beard.gen.in | savee-energy.com | savee.biz | savee.cloud | savee.co | savee.co.jp | savee.co.uk | savee.com | savee.com.au | savee.com.br | savee.com.cn | savee.de | savee.dk | savee.earth | savee.energy | savee.eu | savee.host | savee.info | savee.io | savee.it |

Registrar Data

We will display stored WHOIS data for up to 30 days.

```
Registrant Contact Information:
        Name                                Dr N.M.Veeraiyan
        Organization                        Saveetha Dental College & Hosp.
        Address                             Saveetha University Saveetha Nagar, Thandalam Campus
```

Use promo code WHOIS to save 15% on your first Name.com order.

Site Status

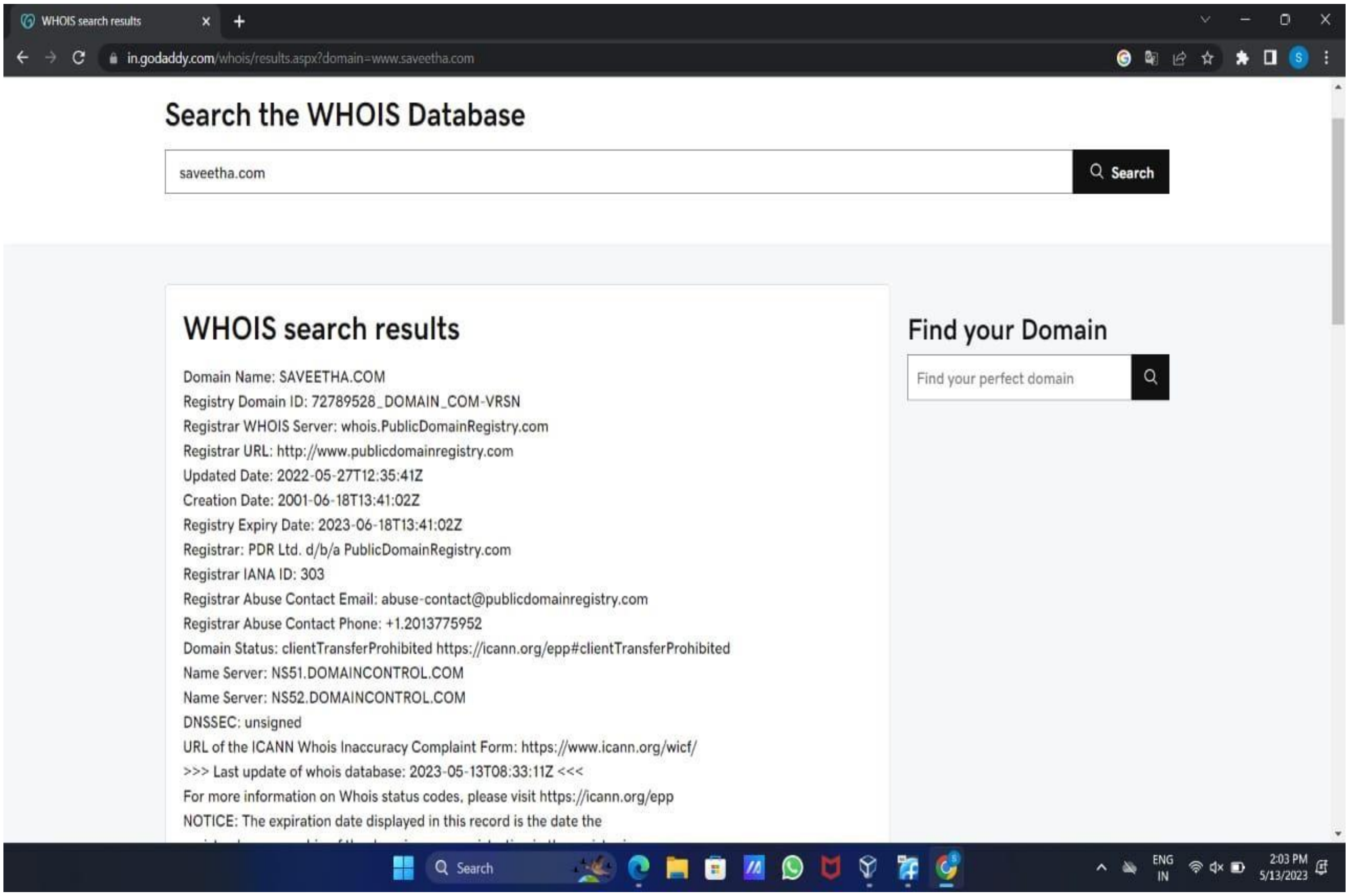
Status	Active
Server Type	Squarespace

Suggested Domains for saveetha.com

□ save-etha.live	$2.99
□ saveethas.live	$2.99
□ freeetha.live	$2.99
□ rescueetha.live	$2.99
□ guardetha.live	$2.99

Use promo code WHOIS to save 15% on your first Name.com order.

Output:



WHOIS search results

```
Domain Name: SAVEETHA.COM
Registry Domain ID: 72789528_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.PublicDomainRegistry.com
Registrar URL: http://www.publicdomainregistry.com
Updated Date: 2022-05-27T12:35:41Z
Creation Date: 2001-06-18T13:41:02Z
Registry Expiry Date: 2023-06-18T13:41:02Z
Registrar: PDR Ltd. d/b/a PublicDomainRegistry.com
Registrar IANA ID: 303
Registrar Abuse Contact Email: abuse-contact@publicdomainregistry.com
Registrar Abuse Contact Phone: +1.2013775952
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Name Server: NS51.DOMAINCONTROL.COM
Name Server: NS52.DOMAINCONTROL.COM
DNSSEC: unsigned
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2023-05-13T08:33:11Z <<<
For more information on Whois status codes, please visit https://icann.org/epp
NOTICE: The expiration date displayed in this record is the date the
```

Result:

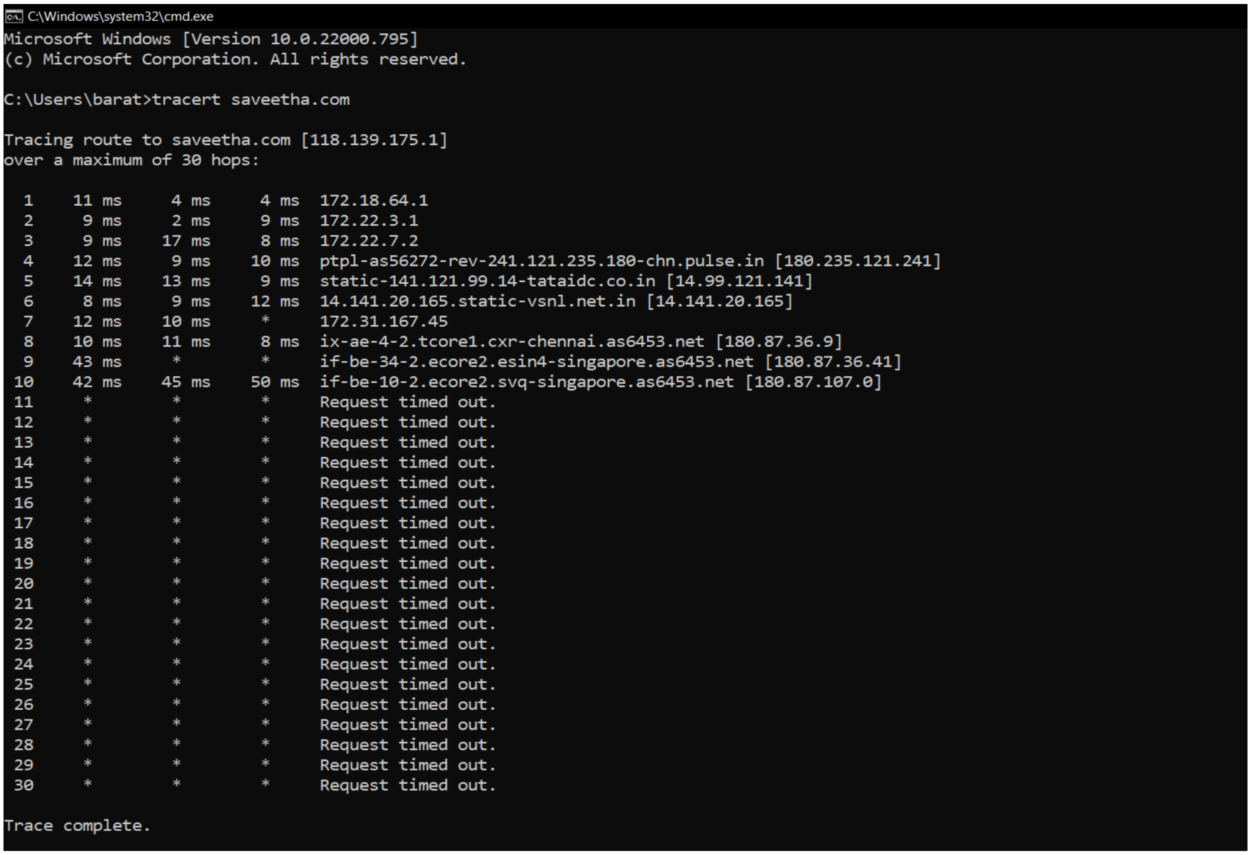
WHOIS is tool to check for the domain names, domain address and IP addresses. This experiment was done using the google and WHOIS.com website. We got the results such as domain name, domain ID, website creation date, name server and so on.

Exercise No 6: TraceRoute, ping, ifconfig, ipconfig, netstat

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

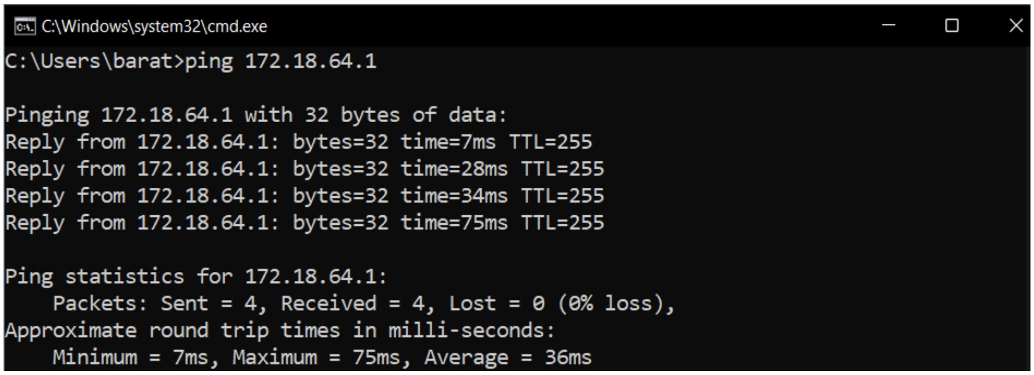
Procedure:

Step 1: open windows command prompt and Type tracert command and type tracert www.saveetha.com -> “Enter”



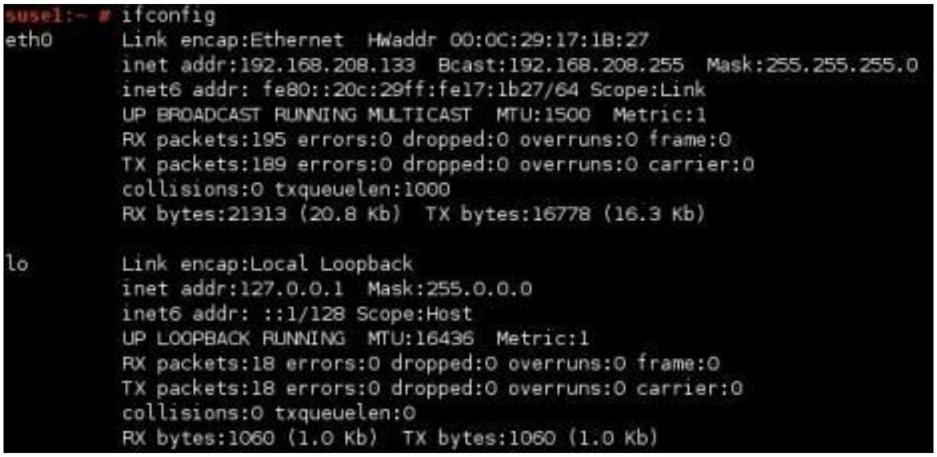
```
C:\Windows\system32\cmd.exe
Microsoft Windows [Version 10.0.22000.795]
(c) Microsoft Corporation. All rights reserved.

C:\Users\barat>tracert saveetha.com

Tracing route to saveetha.com [118.139.175.1]
over a maximum of 30 hops:

  1    11 ms     4 ms     4 ms  172.18.64.1
  2     9 ms     2 ms     9 ms  172.22.3.1
  3     9 ms    17 ms     8 ms  172.22.7.2
  4    12 ms     9 ms    10 ms  ptpl-as56272-rev-241.121.235.180-chn.pulse.in [180.235.121.241]
  5    14 ms    13 ms     9 ms  static-141.121.99.14-tataidc.co.in [14.99.121.141]
  6     8 ms     9 ms    12 ms  14.141.20.165.static-vsnl.net.in [14.141.20.165]
  7    12 ms    10 ms     *     172.31.167.45
  8    10 ms    11 ms     8 ms  ix-ae-4-2.tcore1.cxr-chennai.as6453.net [180.87.36.9]
  9    43 ms     *        *     if-be-34-2.ecore2.esin4-singapore.as6453.net [180.87.36.41]
 10    42 ms    45 ms    50 ms  if-be-10-2.ecore2.svq-singapore.as6453.net [180.87.107.0]
 11     *        *        *     Request timed out.
 12     *        *        *     Request timed out.
 13     *        *        *     Request timed out.
 14     *        *        *     Request timed out.
 15     *        *        *     Request timed out.
 16     *        *        *     Request timed out.
 17     *        *        *     Request timed out.
 18     *        *        *     Request timed out.
 19     *        *        *     Request timed out.
 20     *        *        *     Request timed out.
 21     *        *        *     Request timed out.
 22     *        *        *     Request timed out.
 23     *        *        *     Request timed out.
 24     *        *        *     Request timed out.
 25     *        *        *     Request timed out.
 26     *        *        *     Request timed out.
 27     *        *        *     Request timed out.
 28     *        *        *     Request timed out.
 29     *        *        *     Request timed out.
 30     *        *        *     Request timed out.

Trace complete.
```

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



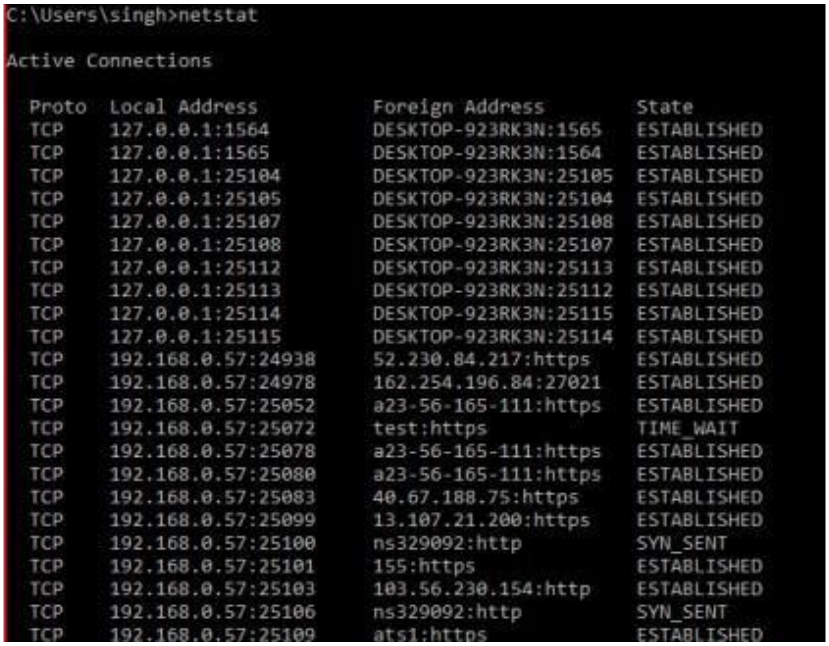
```
C:\Windows\system32\cmd.exe
C:\Users\barat>ping 172.18.64.1

Pinging 172.18.64.1 with 32 bytes of data:
Reply from 172.18.64.1: bytes=32 time=7ms TTL=255
Reply from 172.18.64.1: bytes=32 time=28ms TTL=255
Reply from 172.18.64.1: bytes=32 time=34ms TTL=255
Reply from 172.18.64.1: bytes=32 time=75ms TTL=255

Ping statistics for 172.18.64.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 7ms, Maximum = 75ms, Average = 36ms
```

Step 3: Type ifconfig command



```
susel:~ # ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0C:29:17:1B:27
          inet addr:192.168.208.133  Bcast:192.168.208.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe17:1b27/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:195 errors:0 dropped:0 overruns:0 frame:0
          TX packets:189 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:21313 (20.8 Kb)  TX bytes:16778 (16.3 Kb)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:18 errors:0 dropped:0 overruns:0 frame:0
          TX packets:18 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:1060 (1.0 Kb)  TX bytes:1060 (1.0 Kb)
```

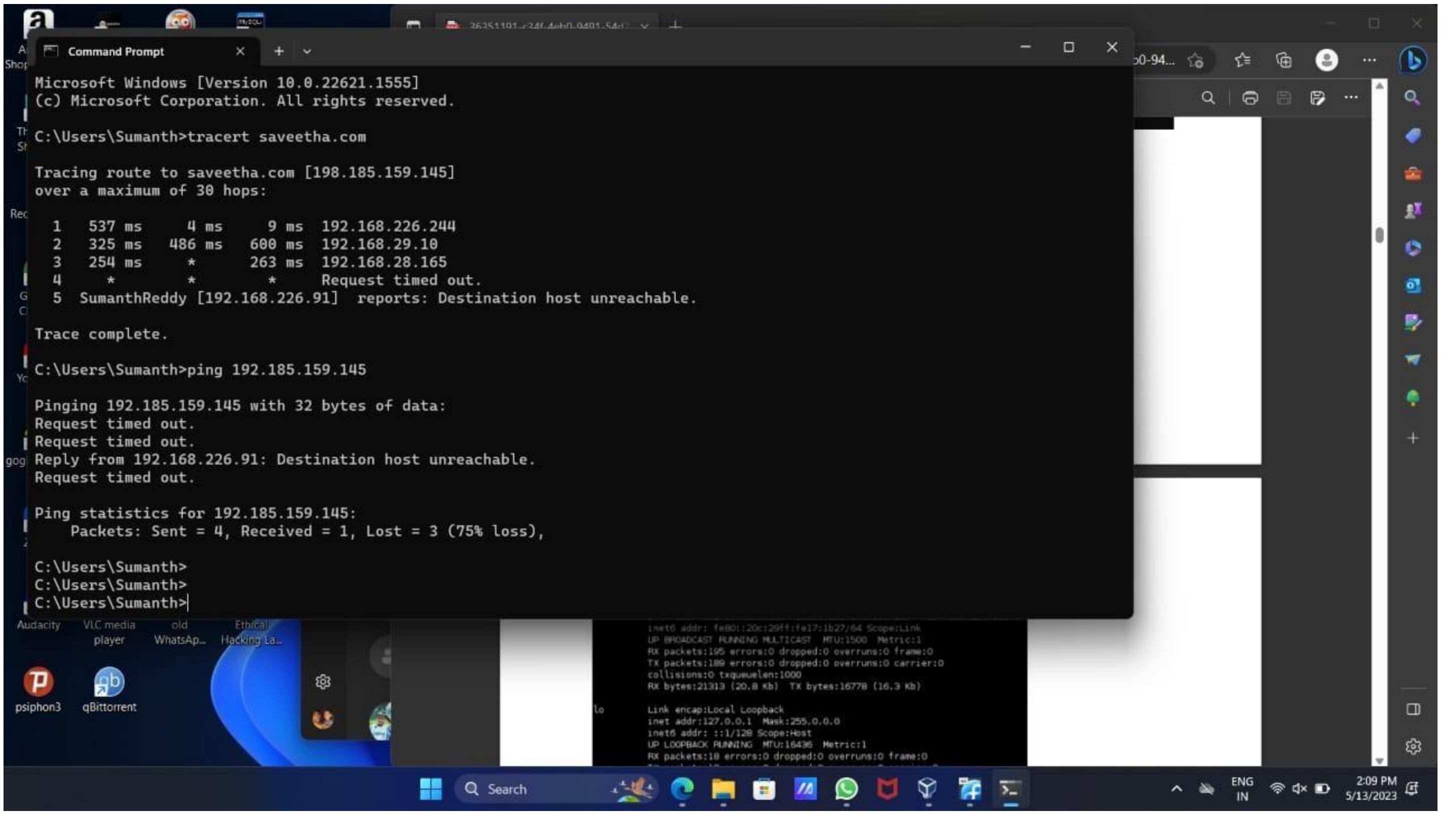
Step 4: Type netstat command



```
C:\Users\singh>netstat

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    127.0.0.1:1564         DESKTOP-923RK3N:1565   ESTABLISHED
  TCP    127.0.0.1:1565         DESKTOP-923RK3N:1564   ESTABLISHED
  TCP    127.0.0.1:25104        DESKTOP-923RK3N:25105  ESTABLISHED
  TCP    127.0.0.1:25105        DESKTOP-923RK3N:25104  ESTABLISHED
  TCP    127.0.0.1:25107        DESKTOP-923RK3N:25108  ESTABLISHED
  TCP    127.0.0.1:25108        DESKTOP-923RK3N:25107  ESTABLISHED
  TCP    127.0.0.1:25112        DESKTOP-923RK3N:25113  ESTABLISHED
  TCP    127.0.0.1:25113        DESKTOP-923RK3N:25112  ESTABLISHED
  TCP    127.0.0.1:25114        DESKTOP-923RK3N:25115  ESTABLISHED
  TCP    127.0.0.1:25115        DESKTOP-923RK3N:25114  ESTABLISHED
  TCP    192.168.0.57:24938     52.230.84.217:https    ESTABLISHED
  TCP    192.168.0.57:24978     162.254.196.84:27021   ESTABLISHED
  TCP    192.168.0.57:25052     a23-56-165-111:https   ESTABLISHED
  TCP    192.168.0.57:25072     test:https             TIME_WAIT
  TCP    192.168.0.57:25078     a23-56-165-111:https   ESTABLISHED
  TCP    192.168.0.57:25080     a23-56-165-111:https   ESTABLISHED
  TCP    192.168.0.57:25083     40.67.188.75:https     ESTABLISHED
  TCP    192.168.0.57:25099     13.107.21.200:https    ESTABLISHED
  TCP    192.168.0.57:25100     ns329092:http          SYN_SENT
  TCP    192.168.0.57:25101     155:https              ESTABLISHED
  TCP    192.168.0.57:25103     103.56.230.154:http    ESTABLISHED
  TCP    192.168.0.57:25106     ns329092:http          SYN_SENT
  TCP    192.168.0.57:25109     ats1:https             ESTABLISHED
```

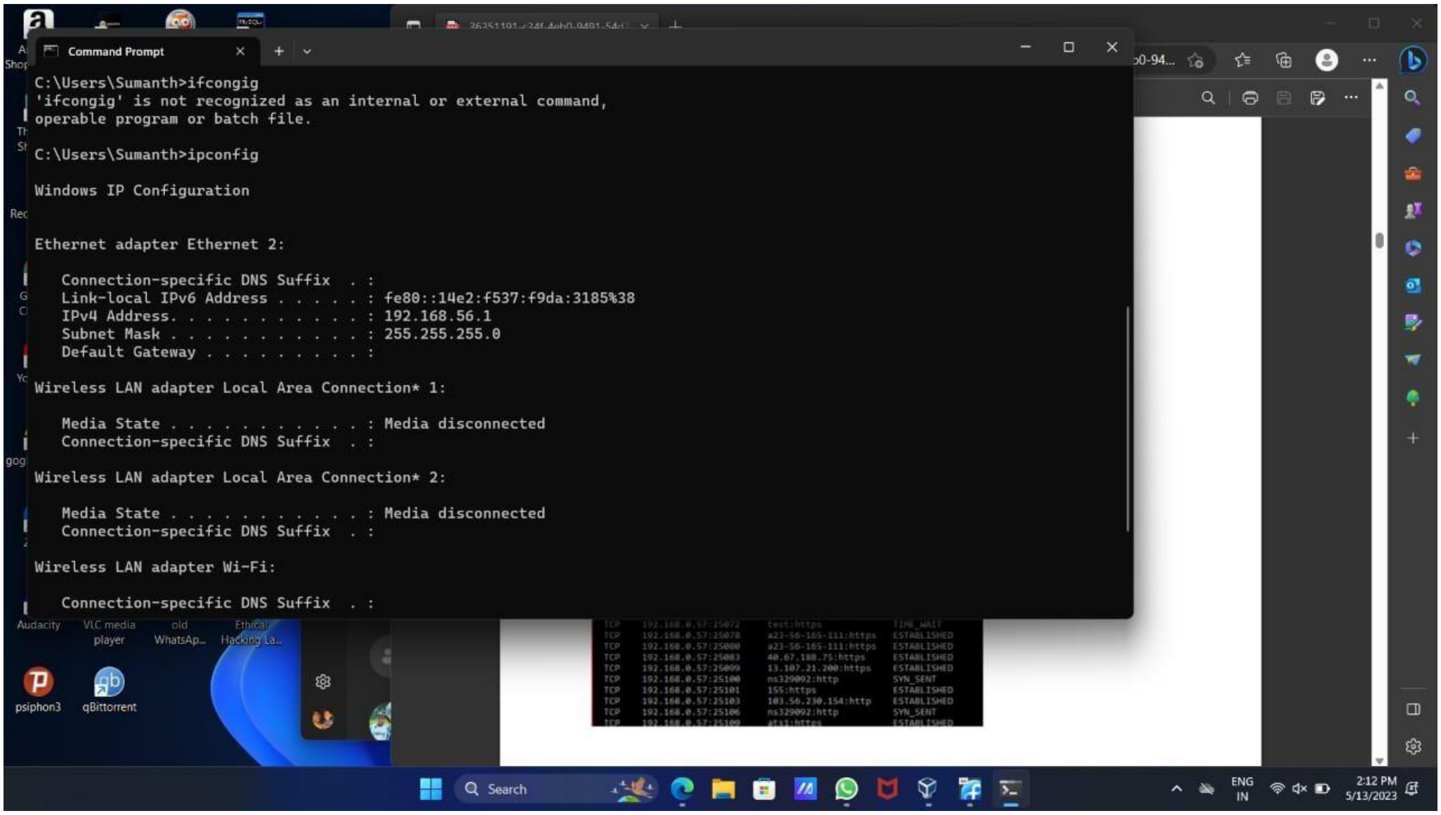
Output:

1)



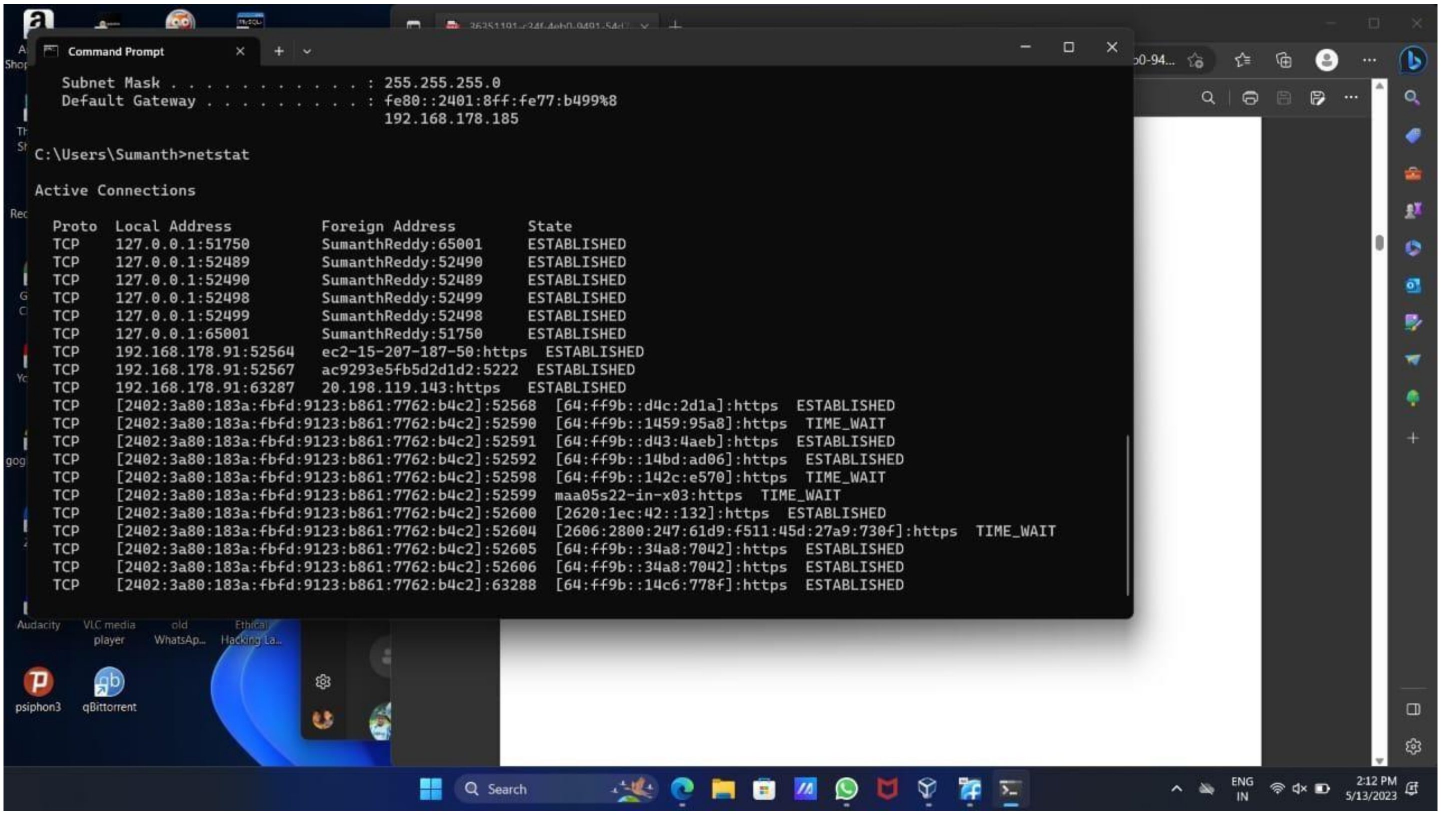
```
Microsoft Windows [Version 10.0.22621.1555]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Sumanth>tracert saveetha.com

Tracing route to saveetha.com [198.185.159.145]
over a maximum of 30 hops:

  1   537 ms     4 ms     9 ms  192.168.226.244
  2   325 ms   486 ms   600 ms  192.168.29.10
  3   254 ms     *      263 ms  192.168.28.165
  4     *        *        *     Request timed out.
  5  SumanthReddy [192.168.226.91]  reports: Destination host unreachable.

Trace complete.

C:\Users\Sumanth>ping 192.185.159.145

Pinging 192.185.159.145 with 32 bytes of data:
Request timed out.
Request timed out.
Reply from 192.168.226.91: Destination host unreachable.
Request timed out.

Ping statistics for 192.185.159.145:
    Packets: Sent = 4, Received = 1, Lost = 3 (75% loss),

C:\Users\Sumanth>
C:\Users\Sumanth>
C:\Users\Sumanth>
```

2)



```
C:\Users\Sumanth>ifcongig
'ifcongig' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\Sumanth>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet 2:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::14e2:f537:f9da:3185%38
   IPv4 Address. . . . . . . . . . . : 192.168.56.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

Wireless LAN adapter Local Area Connection* 1:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 2:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
```

3)



```
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : fe80::2401:8ff:fe77:b499%8
                                       192.168.178.185

C:\Users\Sumanth>netstat

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    127.0.0.1:51750        SumanthReddy:65001     ESTABLISHED
  TCP    127.0.0.1:52489        SumanthReddy:52490     ESTABLISHED
  TCP    127.0.0.1:52490        SumanthReddy:52489     ESTABLISHED
  TCP    127.0.0.1:52498        SumanthReddy:52499     ESTABLISHED
  TCP    127.0.0.1:52499        SumanthReddy:52498     ESTABLISHED
  TCP    127.0.0.1:65001        SumanthReddy:51750     ESTABLISHED
  TCP    192.168.178.91:52564   ec2-15-207-187-50:https  ESTABLISHED
  TCP    192.168.178.91:52567   ac9293e5fb5d2d1d2:5222  ESTABLISHED
  TCP    192.168.178.91:63287   20.198.119.143:https   ESTABLISHED
  TCP    [2402:3a80:183a:fbfd:9123:b861:7762:b4c2]:52568  [64:ff9b::d4c:2d1a]:https  ESTABLISHED
  TCP    [2402:3a80:183a:fbfd:9123:b861:7762:b4c2]:52590  [64:ff9b::1459:95a8]:https  TIME_WAIT
  TCP    [2402:3a80:183a:fbfd:9123:b861:7762:b4c2]:52591  [64:ff9b::d43:4aeb]:https  ESTABLISHED
  TCP    [2402:3a80:183a:fbfd:9123:b861:7762:b4c2]:52592  [64:ff9b::14bd:ad06]:https  ESTABLISHED
  TCP    [2402:3a80:183a:fbfd:9123:b861:7762:b4c2]:52598  [64:ff9b::142c:e570]:https  TIME_WAIT
  TCP    [2402:3a80:183a:fbfd:9123:b861:7762:b4c2]:52599  maa05s22-in-x03:https  TIME_WAIT
  TCP    [2402:3a80:183a:fbfd:9123:b861:7762:b4c2]:52600  [2620:1ec:42::132]:https  ESTABLISHED
  TCP    [2402:3a80:183a:fbfd:9123:b861:7762:b4c2]:52604  [2606:2800:247:61d9:f511:45d:27a9:730f]:https  TIME_WAIT
  TCP    [2402:3a80:183a:fbfd:9123:b861:7762:b4c2]:52605  [64:ff9b::34a8:7042]:https  ESTABLISHED
  TCP    [2402:3a80:183a:fbfd:9123:b861:7762:b4c2]:52606  [64:ff9b::34a8:7042]:https  ESTABLISHED
  TCP    [2402:3a80:183a:fbfd:9123:b861:7762:b4c2]:63288  [64:ff9b::14c6:778f]:https  ESTABLISHED
```

Result:

I have carried out the above experiment using Microsoft windows command prompt. I have used the commands TraceRoute, ping, ifconfig, ipconfig, netstat in this experiment. I have got the results for each command like ping, IP addresses, LAN connections.

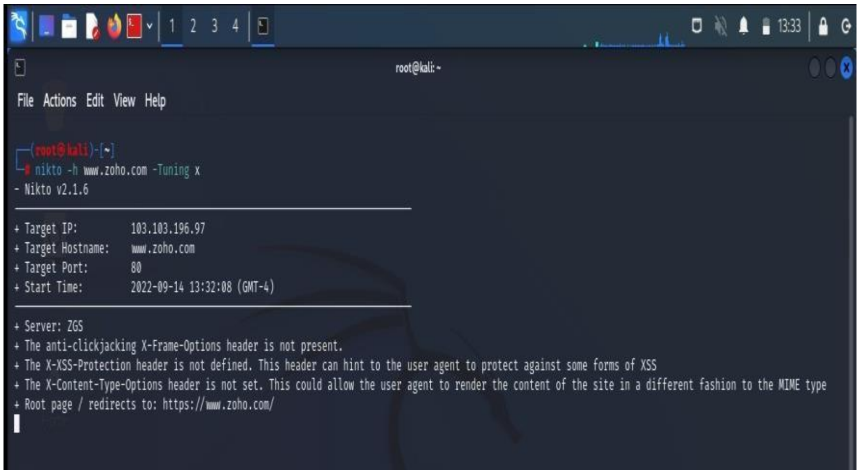
Exercise No 7:VULNERABILITY ANALYSIS - CGI Scanning with Nikto

Aim:To perform vulnerability Analysis using CGI Scanning with Nikto

Procedure:

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

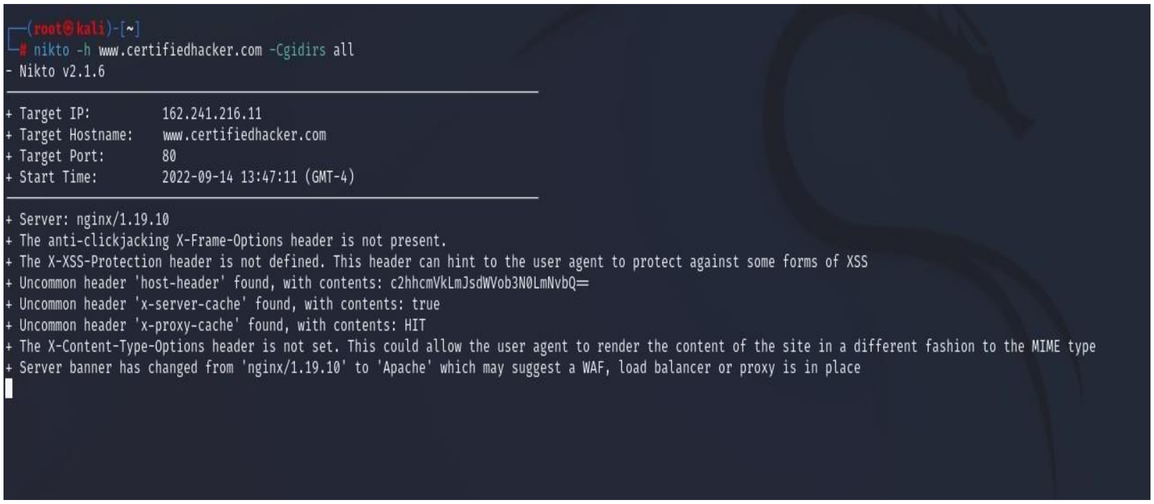
Step 2: Type nikto –h <website> Tuning x and press enter



```
┌──(root㉿kali)-[~]
└─# nikto -h www.zoho.com -Tuning x
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          103.103.196.97
+ Target Hostname:    www.zoho.com
+ Target Port:        80
+ Start Time:         2022-09-14 13:32:08 (GMT-4)
---------------------------------------------------------------------------
+ Server: ZGS
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
+ Root page / redirects to: https://www.zoho.com/
```

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

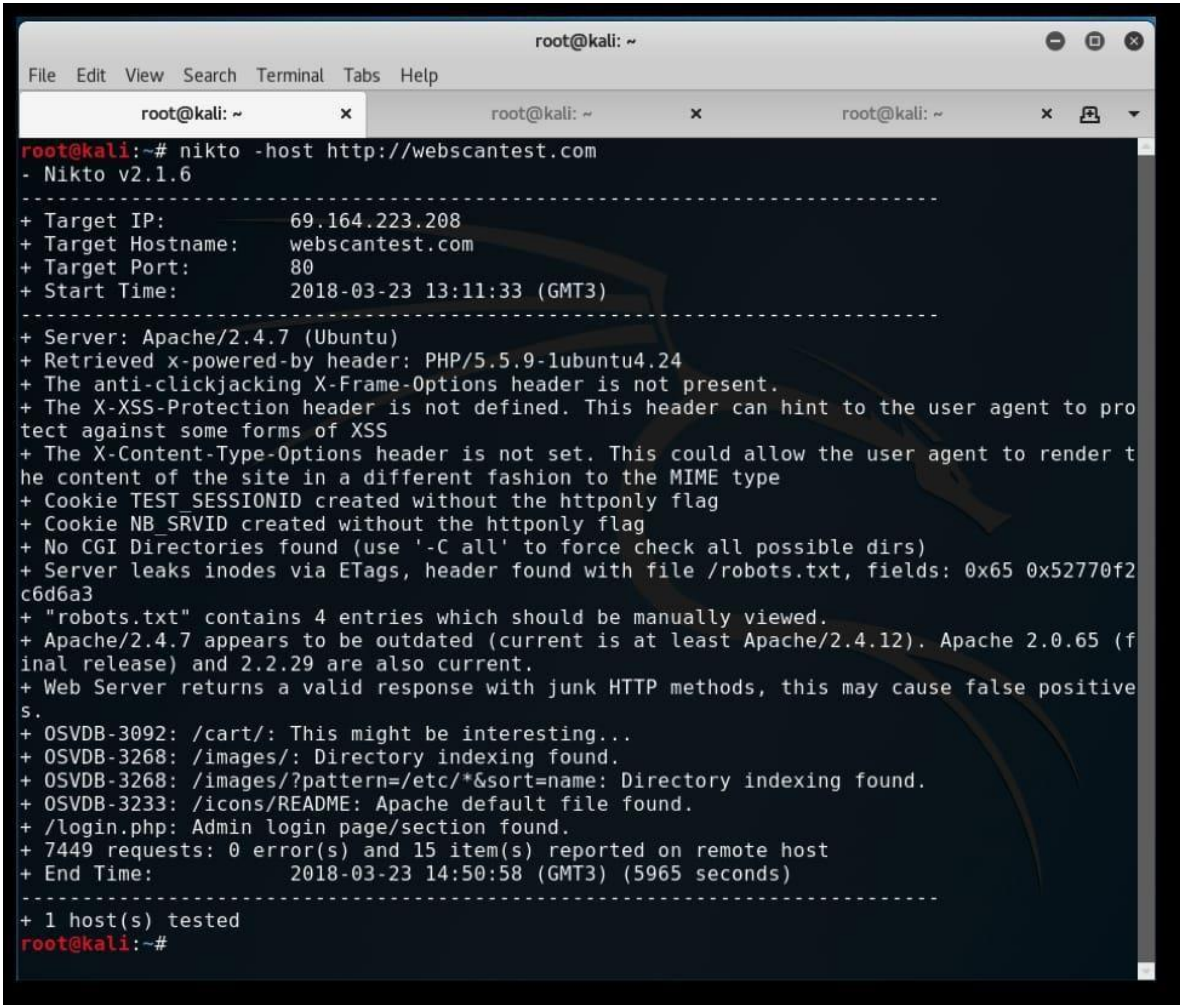


```
┌──(root㉿kali)-[~]
└─# nikto -h www.certifiedhacker.com -Cgidirs all
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          162.241.216.11
+ Target Hostname:    www.certifiedhacker.com
+ Target Port:        80
+ Start Time:         2022-09-14 13:47:11 (GMT-4)
---------------------------------------------------------------------------
+ Server: nginx/1.19.10
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ Uncommon header 'host-header' found, with contents: c2hhcmVkLmJsdWVob3N0LmNvbQ==
+ Uncommon header 'x-server-cache' found, with contents: true
+ Uncommon header 'x-proxy-cache' found, with contents: HIT
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
+ Server banner has changed from 'nginx/1.19.10' to 'Apache' which may suggest a WAF, load balancer or proxy is in place
```

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

Output:

1)



```
root@kali:~# nikto -host http://webscantest.com
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          69.164.223.208
+ Target Hostname:    webscantest.com
+ Target Port:        80
+ Start Time:         2018-03-23 13:11:33 (GMT3)
---------------------------------------------------------------------------
+ Server: Apache/2.4.7 (Ubuntu)
+ Retrieved x-powered-by header: PHP/5.5.9-1ubuntu4.24
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to pro
tect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render t
he content of the site in a different fashion to the MIME type
+ Cookie TEST_SESSIONID created without the httponly flag
+ Cookie NB_SRVID created without the httponly flag
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Server leaks inodes via ETags, header found with file /robots.txt, fields: 0x65 0x52770f2
c6d6a3
+ "robots.txt" contains 4 entries which should be manually viewed.
+ Apache/2.4.7 appears to be outdated (current is at least Apache/2.4.12). Apache 2.0.65 (f
inal release) and 2.2.29 are also current.
+ Web Server returns a valid response with junk HTTP methods, this may cause false positive
s.
+ OSVDB-3092: /cart/: This might be interesting...
+ OSVDB-3268: /images/: Directory indexing found.
+ OSVDB-3268: /images/?pattern=/etc/*&sort=name: Directory indexing found.
+ OSVDB-3233: /icons/README: Apache default file found.
+ /login.php: Admin login page/section found.
+ 7449 requests: 0 error(s) and 15 item(s) reported on remote host
+ End Time:           2018-03-23 14:50:58 (GMT3) (5965 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
root@kali:~#
```

Result:

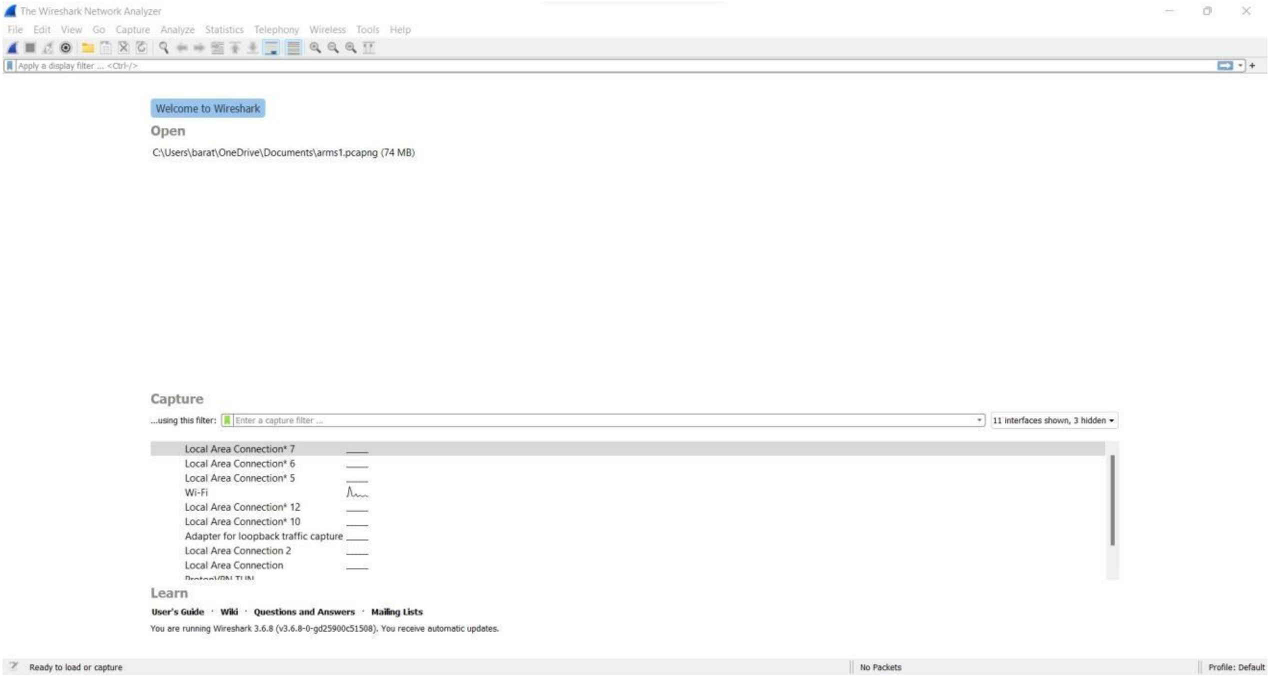
The above experiment is about VULNERABILITY ANALYSIS - CGI Scanning with Nikto. We can retrieve information like server name, headers and etc. This is done in root terminal using kali linux OS.

Exercise No 8: WireShark sniffer

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

Procedure:

Step 1: Install and open WireShark .



The Wireshark Network Analyzer

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter … <Ctrl-/>

Welcome to Wireshark

Open

C:\Users\barat\OneDrive\Documents\arms1.pcapng (74 MB)

Capture

…using this filter: Enter a capture filter … 11 interfaces shown, 3 hidden

- Local Area Connection* 7
- Local Area Connection* 6
- Local Area Connection* 5
- Wi-Fi
- Local Area Connection* 12
- Local Area Connection* 10
- Adapter for loopback traffic capture
- Local Area Connection 2
- Local Area Connection
- ProtonVPN TUN

Learn

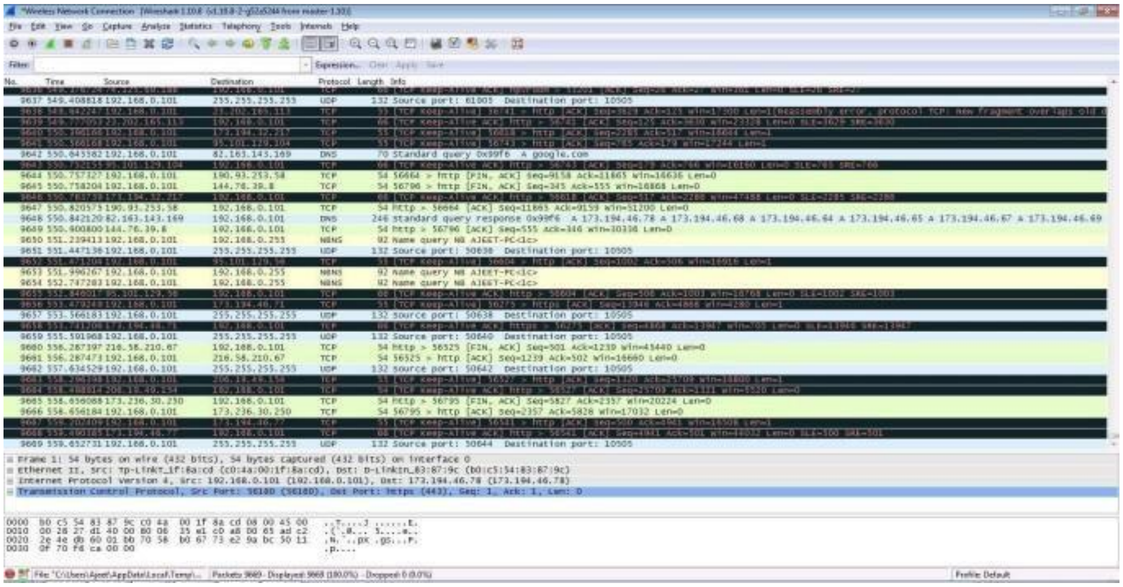
User's Guide · Wiki · Questions and Answers · Mailing Lists

You are running Wireshark 3.6.8 (v3.6.8-0-gd25900c51508). You receive automatic updates.

Ready to load or capture | No Packets | Profile: Default

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



*Wireless Network Connection [Wireshark 1.10.8 (v1.10.8-2-g52a5244 from master-1.10)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: Expression... Clear Apply Save

```
No.  Time       Source          Destination      Protocol Length Info
9637 549.408818 192.168.0.101   255.255.255.255  UDP      132 Source port: 61005  Destination port: 10505
9638 549.842247 192.168.0.101   23.202.165.113   TCP       55 [TCP Keep-Alive] 56741 > http [ACK] Seq=3629 Ack=125 Win=17300 Len=1[Reassembly error, protocol TCP: New fragment overlaps old d
9639 [illegible] 23.202.165.113 192.168.0.101    TCP       66 [TCP Keep-Alive ACK] http > 56741 [ACK] Seq=125 Ack=3630 Win=23328 Len=0 SLE=3629 SRE=3630
9640 [illegible] 192.168.0.101  173.194.32.217   TCP       55 [TCP Keep-Alive] 56818 > http [ACK] Seq=2285 Ack=517 Win=16684 Len=1
9641 [illegible] 192.168.0.101  95.101.129.104   TCP       55 [TCP Keep-Alive] 56743 > http [ACK] Seq=785 Ack=179 Win=17244 Len=1
9642 550.645582 192.168.0.101   82.163.143.169   DNS       70 Standard query 0x99f6  A google.com
9643 550.732155 95.101.129.104  192.168.0.101    TCP       66 [TCP Keep-Alive ACK] http > 56743 [ACK] Seq=179 Ack=786 Win=16160 Len=0 SLE=785 SRE=786
9644 550.757327 192.168.0.101   190.93.253.58    TCP       54 56664 > http [FIN, ACK] Seq=9158 Ack=11865 Win=16636 Len=0
9645 550.758204 192.168.0.101   144.76.39.8      TCP       54 56796 > http [FIN, ACK] Seq=345 Ack=555 Win=16868 Len=0
9646 550.783739 173.194.32.217  192.168.0.101    TCP       66 [TCP Keep-Alive ACK] http > 56818 [ACK] Seq=517 Ack=2286 Win=47488 Len=0 SLE=2285 SRE=2286
9647 550.820575 190.93.253.58   192.168.0.101    TCP       54 http > 56664 [ACK] Seq=11865 Ack=9159 Win=51200 Len=0
9648 550.842120 82.163.143.169  192.168.0.101    DNS      246 Standard query response 0x99f6  A 173.194.46.78 A 173.194.46.68 A 173.194.46.64 A 173.194.46.65 A 173.194.46.67 A 173.194.46.69
9649 550.900800 144.76.39.8     192.168.0.101    TCP       54 http > 56796 [ACK] Seq=555 Ack=346 Win=30336 Len=0
9650 551.239413 192.168.0.101   192.168.0.255    NBNS      92 Name query NB AJEET-PC<1c>
9651 551.447138 192.168.0.101   255.255.255.255  UDP      132 Source port: 50638  Destination port: 10505
9652 551.471204 192.168.0.101   95.101.129.58    TCP       55 [TCP Keep-Alive] 56604 > http [ACK] Seq=1002 Ack=506 Win=16916 Len=1
9653 551.996267 192.168.0.101   192.168.0.255    NBNS      92 Name query NB AJEET-PC<1c>
9654 552.747283 192.168.0.101   192.168.0.255    NBNS      92 Name query NB AJEET-PC<1c>
9655 552.840017 95.101.129.58   192.168.0.101    TCP       66 [TCP Keep-Alive ACK] http > 56604 [ACK] Seq=506 Ack=1003 Win=16768 Len=0 SLE=1002 SRE=1003
9656 553.479248 192.168.0.101   173.194.40.71    TCP       55 [TCP Keep-Alive] 56275 > https [ACK] Seq=13946 Ack=4868 Win=4280 Len=1
9657 553.566183 192.168.0.101   255.255.255.255  UDP      132 Source port: 50638  Destination port: 10505
9658 553.741708 173.194.40.71   192.168.0.101    TCP       66 [TCP Keep-Alive ACK] https > 56275 [ACK] Seq=4868 Ack=13947 Win=705 Len=0 SLE=13946 SRE=13947
9659 555.591968 192.168.0.101   255.255.255.255  UDP      132 Source port: 50640  Destination port: 10505
9660 556.287397 216.58.210.67   192.168.0.101    TCP       54 http > 56525 [FIN, ACK] Seq=501 Ack=1239 Win=43440 Len=0
9661 556.287473 192.168.0.101   216.58.210.67    TCP       54 56525 > http [ACK] Seq=1239 Ack=502 Win=16660 Len=0
9662 557.634529 192.168.0.101   255.255.255.255  UDP      132 Source port: 50642  Destination port: 10505
9663 [illegible] 192.168.0.101  [illegible]      TCP       55 [TCP Keep-Alive] 56527 > http [ACK] Seq=1120 Ack=25709 Win=16800 Len=1
9664 [illegible] [illegible]    192.168.0.101    TCP       66 [TCP Keep-Alive ACK] http > 56527 [ACK] Seq=25709 Ack=1121 Win=5520 Len=0
9665 558.656088 173.236.30.250  192.168.0.101    TCP       54 http > 56795 [FIN, ACK] Seq=5827 Ack=2357 Win=20224 Len=0
9666 558.656184 192.168.0.101   173.236.30.250   TCP       54 56795 > http [ACK] Seq=2357 Ack=5828 Win=17032 Len=0
9667 [illegible] 192.168.0.101  173.194.46.77    TCP       55 [TCP Keep-Alive] 56541 > http [ACK] Seq=500 Ack=4961 Win=16508 Len=1
9668 [illegible] 173.194.46.77  192.168.0.101    TCP       66 [TCP Keep-Alive ACK] http > 56541 [ACK] Seq=4961 Ack=501 Win=44032 Len=0 SLE=500 SRE=501
9669 559.652731 192.168.0.101   255.255.255.255  UDP      132 Source port: 50644  Destination port: 10505
```

```
⊞ Frame 1: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface 0
⊞ Ethernet II, Src: Tp-LinkT_1f:8a:cd (c0:4a:00:1f:8a:cd), Dst: D-LinkIn_83:87:9c (b0:c5:54:83:87:9c)
⊞ Internet Protocol Version 4, Src: 192.168.0.101 (192.168.0.101), Dst: 173.194.46.78 (173.194.46.78)
⊟ Transmission Control Protocol, Src Port: 56180 (56180), Dst Port: https (443), Seq: 1, Ack: 1, Len: 0
```

```
0000  b0 c5 54 83 87 9c c0 4a  00 1f 8a cd 08 00 45 00   ..T....J ......E.
0010  00 28 27 d1 40 00 80 06  35 e1 c0 a8 00 65 ad c2   .('.@... 5....e..
0020  2e 4e db 60 01 bb 70 58  b0 67 73 e2 9a bc 50 11   .N.`..pX .gs...P.
0030  0f 70 fd ca 00 00                                  .p....
```

File: "C:\Users\Ajeet\AppData\Local\Temp\... | Packets: 9669 · Displayed: 9668 (100.0%) · Dropped: 0 (0.0%) | Profile: Default

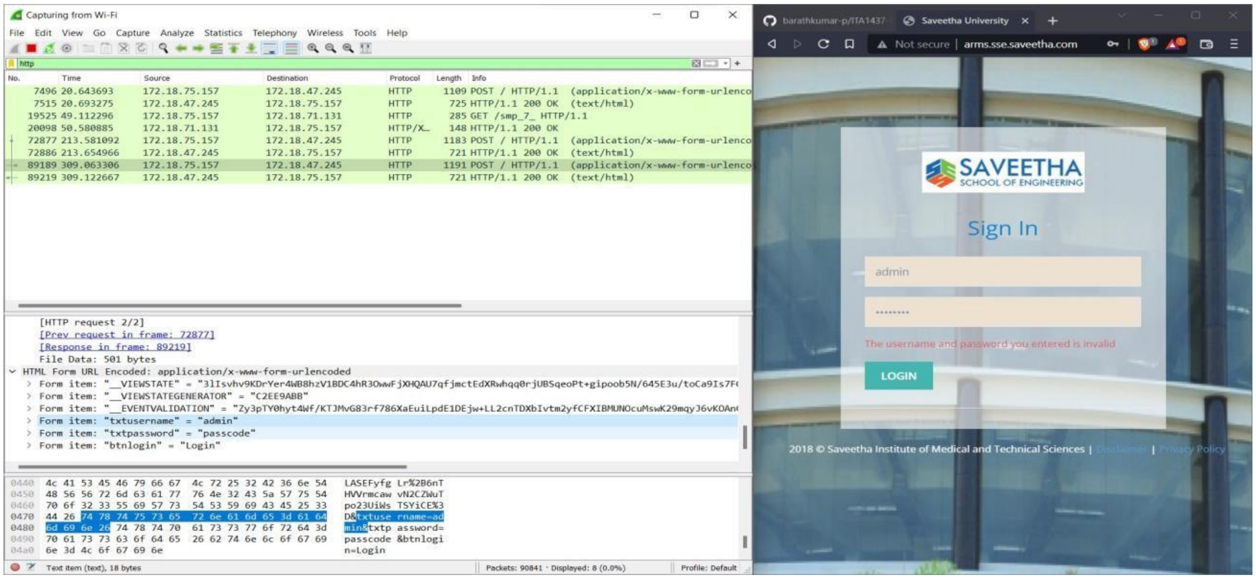
Step 4: Open a website in a new window and enter the user id and password. Register ifneeded.

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 recording



Capturing from Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

```
No.    Time        Source         Destination    Protocol  Length Info
 7496  20.643693   172.18.75.157  172.18.47.245  HTTP      1109 POST / HTTP/1.1  (application/x-www-form-urlenco
 7515  20.693275   172.18.47.245  172.18.75.157  HTTP       725 HTTP/1.1 200 OK  (text/html)
19525  49.112296   172.18.75.157  172.18.71.131  HTTP       285 GET /smp_7_ HTTP/1.1
20098  50.580885   172.18.71.131  172.18.75.157  HTTP/X…    148 HTTP/1.1 200 OK
72877  213.581092  172.18.75.157  172.18.47.245  HTTP      1183 POST / HTTP/1.1  (application/x-www-form-urlenco
72886  213.654966  172.18.47.245  172.18.75.157  HTTP       721 HTTP/1.1 200 OK  (text/html)
89189  309.063306  172.18.75.157  172.18.47.245  HTTP      1191 POST / HTTP/1.1  (application/x-www-form-urlenco
89219  309.122667  172.18.47.245  172.18.75.157  HTTP       721 HTTP/1.1 200 OK  (text/html)
```

```
    [HTTP request 2/2]
    [Prev request in frame: 72877]
    [Response in frame: 89219]
    File Data: 501 bytes
v HTML Form URL Encoded: application/x-www-form-urlencoded
  > Form item: "__VIEWSTATE" = "3lIsvhv9KDrYer4WB8hzV1BDC4hR3OwwFjXHQAU7qfjmctEdXRwhqq0rjUBSqeoPt+gipoob5N/645E3u/toCa9Is7F(
  > Form item: "__VIEWSTATEGENERATOR" = "C2EE9ABB"
  > Form item: "__EVENTVALIDATION" = "Zy3pTY0hyt4Wf/KTJMvG83rf786XaEuiLpdE1DEjw+LL2cnTDXbIvtm2yfCFXIBMUNOcuMswK29mqyJ6vKOAn(
  > Form item: "txtusername" = "admin"
  > Form item: "txtpassword" = "passcode"
  > Form item: "btnlogin" = "Login"
```

```
0440  4c 41 53 45 46 79 66 67  4c 72 25 32 42 36 6e 54   LASEFyfg Lr%2B6nT
0450  48 56 56 72 6d 63 61 77  76 4e 32 43 5a 57 75 54   HVVrmcaw vN2CZWuT
0460  70 6f 32 33 55 69 57 73  54 53 59 69 43 45 25 33   po23UiWs TSYiCE%3
0470  44 26 74 78 74 75 73 65  72 6e 61 6d 65 3d 61 64   D&txtuse rname=ad
0480  6d 69 6e 26 74 78 74 70  61 73 73 77 6f 72 64 3d   min&txtp assword=
0490  70 61 73 73 63 6f 64 65  26 62 74 6e 6c 6f 67 69   passcode &btnlogi
04a0  6e 3d 4c 6f 67 69 6e                                n=Login
```

Text item (text), 18 bytes | Packets: 90841 · Displayed: 8 (0.0%) | Profile: Default

barathkumar-p/ITA1437 | Saveetha University

Not secure | arms.sse.saveetha.com

SAVEETHA SCHOOL OF ENGINEERING

Sign In

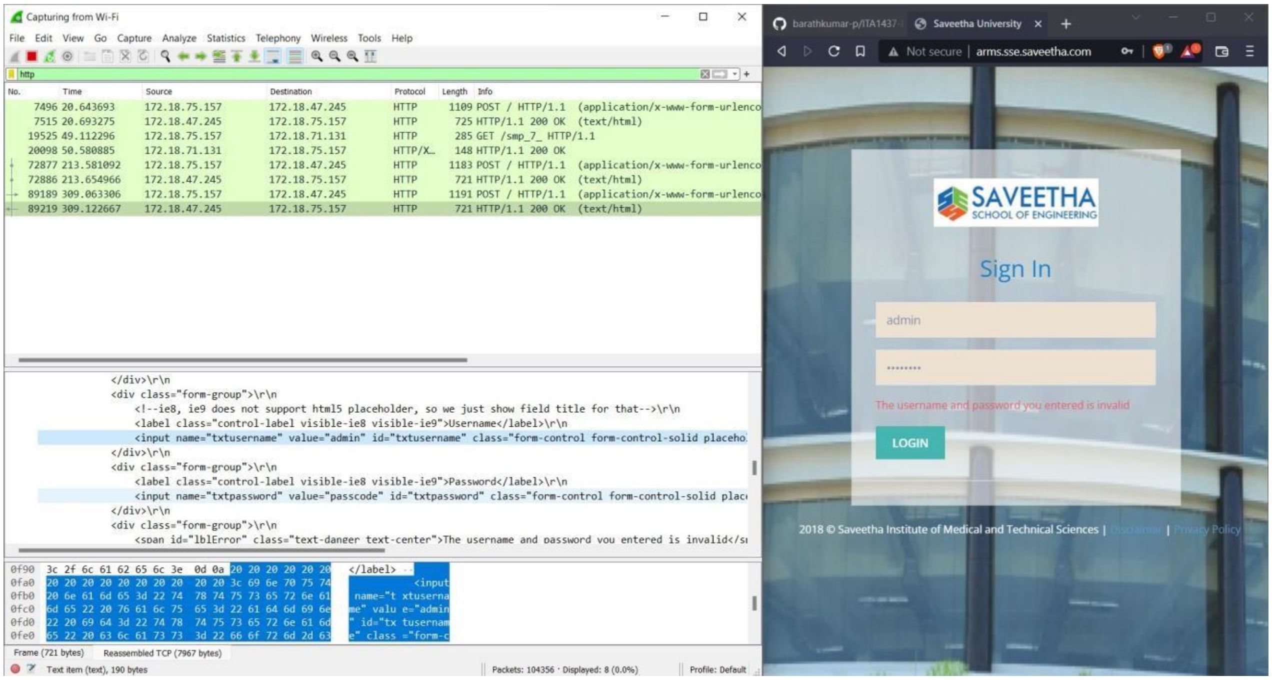
admin

••••••••

The username and password you entered is invalid

LOGIN

2018 © Saveetha Institute of Medical and Technical Sciences | Disclaimer | Privacy Policy



Capturing from Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

```
No.    Time        Source         Destination    Protocol  Length Info
 7496  20.643693   172.18.75.157  172.18.47.245  HTTP      1109 POST / HTTP/1.1  (application/x-www-form-urlenco
 7515  20.693275   172.18.47.245  172.18.75.157  HTTP       725 HTTP/1.1 200 OK  (text/html)
19525  49.112296   172.18.75.157  172.18.71.131  HTTP       285 GET /smp_7_ HTTP/1.1
20098  50.580885   172.18.71.131  172.18.75.157  HTTP/X…    148 HTTP/1.1 200 OK
72877  213.581092  172.18.75.157  172.18.47.245  HTTP      1183 POST / HTTP/1.1  (application/x-www-form-urlenco
72886  213.654966  172.18.47.245  172.18.75.157  HTTP       721 HTTP/1.1 200 OK  (text/html)
89189  309.063306  172.18.75.157  172.18.47.245  HTTP      1191 POST / HTTP/1.1  (application/x-www-form-urlenco
89219  309.122667  172.18.47.245  172.18.75.157  HTTP       721 HTTP/1.1 200 OK  (text/html)
```

```
        </div>\r\n
        <div class="form-group">\r\n
            <!--ie8, ie9 does not support html5 placeholder, so we just show field title for that-->\r\n
            <label class="control-label visible-ie8 visible-ie9">Username</label>\r\n
            <input name="txtusername" value="admin" id="txtusername" class="form-control form-control-solid placeho:
        </div>\r\n
        <div class="form-group">\r\n
            <label class="control-label visible-ie8 visible-ie9">Password</label>\r\n
            <input name="txtpassword" value="passcode" id="txtpassword" class="form-control form-control-solid plac(
        </div>\r\n
        <div class="form-group">\r\n
            <span id="lblError" class="text-danger text-center">The username and password you entered is invalid</s
```

```
0f90  3c 2f 6c 61 62 65 6c 3e  0d 0a 20 20 20 20 20 20   </label> ··
0fa0  20 20 20 20 20 20 20 20  20 20 3c 69 6e 70 75 74             <input
0fb0  20 6e 61 6d 65 3d 22 74  78 74 75 73 65 72 6e 61    name="t xtuserna
0fc0  6d 65 22 20 76 61 6c 75  65 3d 22 61 64 6d 69 6e   me" valu e="admin
0fd0  22 20 69 64 3d 22 74 78  74 75 73 65 72 6e 61 6d   " id="tx tusernam
0fe0  65 22 20 63 6c 61 73 73  3d 22 66 6f 72 6d 2d 63   e" class ="form-c
```

Frame (721 bytes) | Reassembled TCP (7967 bytes)

Text item (text), 190 bytes | Packets: 104356 · Displayed: 8 (0.0%) | Profile: Default

barathkumar-p/ITA1437 | Saveetha University

Not secure | arms.sse.saveetha.com

SAVEETHA SCHOOL OF ENGINEERING

Sign In

admin

••••••••

The username and password you entered is invalid

LOGIN

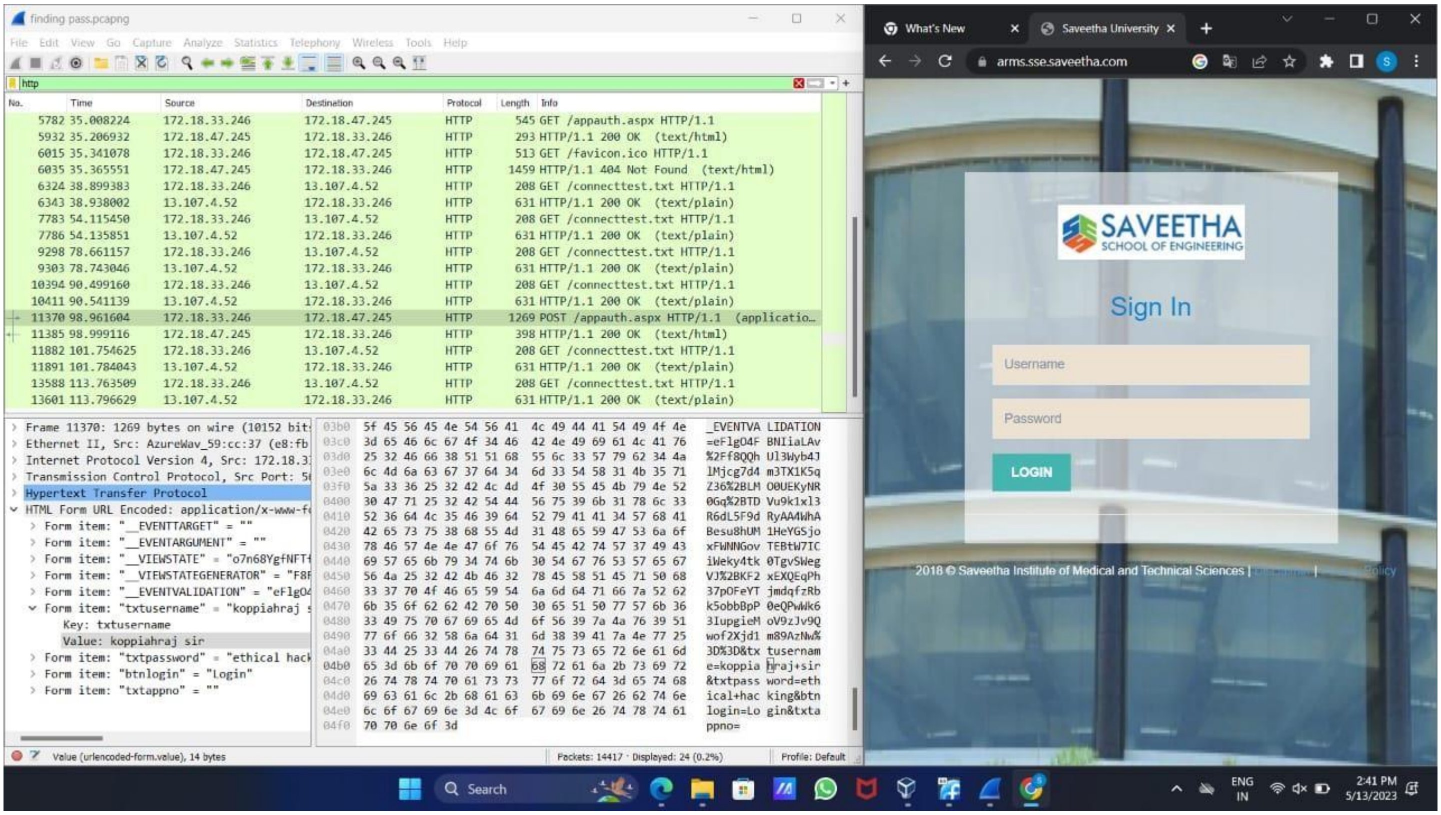
2018 © Saveetha Institute of Medical and Technical Sciences | Disclaimer | Privacy Policy

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:

1)



finding pass.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http

```
No.   Time        Source         Destination    Protocol Length Info
 5782 35.008224   172.18.33.246  172.18.47.245  HTTP      545 GET /appauth.aspx HTTP/1.1
 5932 35.206932   172.18.47.245  172.18.33.246  HTTP      293 HTTP/1.1 200 OK  (text/html)
 6015 35.341078   172.18.33.246  172.18.47.245  HTTP      513 GET /favicon.ico HTTP/1.1
 6035 35.365551   172.18.47.245  172.18.33.246  HTTP     1459 HTTP/1.1 404 Not Found  (text/html)
 6324 38.899383   172.18.33.246  13.107.4.52    HTTP      208 GET /connecttest.txt HTTP/1.1
 6343 38.938002   13.107.4.52    172.18.33.246  HTTP      631 HTTP/1.1 200 OK  (text/plain)
 7783 54.115450   172.18.33.246  13.107.4.52    HTTP      208 GET /connecttest.txt HTTP/1.1
 7786 54.135851   13.107.4.52    172.18.33.246  HTTP      631 HTTP/1.1 200 OK  (text/plain)
 9298 78.661157   172.18.33.246  13.107.4.52    HTTP      208 GET /connecttest.txt HTTP/1.1
 9303 78.743046   13.107.4.52    172.18.33.246  HTTP      631 HTTP/1.1 200 OK  (text/plain)
10394 90.499160   172.18.33.246  13.107.4.52    HTTP      208 GET /connecttest.txt HTTP/1.1
10411 90.541139   13.107.4.52    172.18.33.246  HTTP      631 HTTP/1.1 200 OK  (text/plain)
11370 98.961604   172.18.33.246  172.18.47.245  HTTP     1269 POST /appauth.aspx HTTP/1.1  (applicatio…
11385 98.999116   172.18.47.245  172.18.33.246  HTTP      398 HTTP/1.1 200 OK  (text/html)
11882 101.754625  172.18.33.246  13.107.4.52    HTTP      208 GET /connecttest.txt HTTP/1.1
11891 101.784043  13.107.4.52    172.18.33.246  HTTP      631 HTTP/1.1 200 OK  (text/plain)
13588 113.763509  172.18.33.246  13.107.4.52    HTTP      208 GET /connecttest.txt HTTP/1.1
13601 113.796629  13.107.4.52    172.18.33.246  HTTP      631 HTTP/1.1 200 OK  (text/plain)
```

```
> Frame 11370: 1269 bytes on wire (10152 bit
> Ethernet II, Src: AzureWav_59:cc:37 (e8:fb
> Internet Protocol Version 4, Src: 172.18.3
> Transmission Control Protocol, Src Port: 5
> Hypertext Transfer Protocol
v HTML Form URL Encoded: application/x-www-f
  > Form item: "__EVENTTARGET" = ""
  > Form item: "__EVENTARGUMENT" = ""
  > Form item: "__VIEWSTATE" = "o7n68YgfNFT
  > Form item: "__VIEWSTATEGENERATOR" = "F8F
  > Form item: "__EVENTVALIDATION" = "eFlgO4
  v Form item: "txtusername" = "koppiahraj s
      Key: txtusername
      Value: koppiahraj sir
  > Form item: "txtpassword" = "ethical hack
  > Form item: "btnlogin" = "Login"
  > Form item: "txtappno" = ""
```

```
03b0  5f 45 56 45 4e 54 56 41  4c 49 44 41 54 49 4f 4e   _EVENTVA LIDATION
03c0  3d 65 46 6c 67 4f 34 46  42 4e 49 69 61 4c 41 76   =eFlgO4F BNIiaLAv
03d0  25 32 46 66 38 51 51 68  55 6c 33 57 79 62 34 4a   %2Ff8QQh Ul3Wyb4J
03e0  6c 4d 6a 63 67 37 64 34  6d 33 54 58 31 4b 35 71   lMjcg7d4 m3TX1K5q
03f0  5a 33 36 25 32 42 4c 4d  4f 30 55 45 4b 79 4e 52   Z36%2BLM O0UEKyNR
0400  30 47 71 25 32 42 54 44  56 75 39 6b 31 78 6c 33   0Gq%2BTD Vu9k1xl3
0410  52 36 64 4c 35 46 39 64  52 79 41 41 34 57 68 41   R6dL5F9d RyAA4WhA
0420  42 65 73 75 38 68 55 4d  31 48 65 59 47 53 6a 6f   Besu8hUM 1HeYGSjo
0430  78 46 57 4e 4e 47 6f 76  54 45 42 74 57 37 49 43   xFWNNGov TEBtW7IC
0440  69 57 65 6b 79 34 74 6b  30 54 67 76 53 57 65 67   iWeky4tk 0TgvSWeg
0450  56 4a 25 32 42 4b 46 32  78 45 58 51 45 71 50 68   VJ%2BKF2 xEXQEqPh
0460  33 37 70 4f 46 65 59 54  6a 6d 64 71 66 7a 52 62   37pOFeYT jmdqfzRb
0470  6b 35 6f 62 62 42 70 50  30 65 51 50 77 57 6b 36   k5obbBpP 0eQPwWk6
0480  33 49 75 70 67 69 65 4d  6f 56 39 7a 4a 76 39 51   3IupgieM oV9zJv9Q
0490  77 6f 66 32 58 6a 64 31  6d 38 39 41 7a 4e 77 25   wof2Xjd1 m89AzNw%
04a0  33 44 25 33 44 26 74 78  74 75 73 65 72 6e 61 6d   3D%3D&tx tusernam
04b0  65 3d 6b 6f 70 70 69 61  68 72 61 6a 2b 73 69 72   e=koppia hraj+sir
04c0  26 74 78 74 70 61 73 73  77 6f 72 64 3d 65 74 68   &txtpass word=eth
04d0  69 63 61 6c 2b 68 61 63  6b 69 6e 67 26 62 74 6e   ical+hac king&btn
04e0  6c 6f 67 69 6e 3d 4c 6f  67 69 6e 26 74 78 74 61   login=Lo gin&txta
04f0  70 70 6e 6f 3d                                     ppno=
```

Value (urlencoded-form.value), 14 bytes   Packets: 14417 · Displayed: 24 (0.2%)   Profile: Default

Result:

The current experiment is about wireshark sniffer. Using WireShark sniffer, we can capture network traffic and can be able analyze it. This experiment executed using google chrome.

Ex. No.9 – ENUMERATION - Enumerating information from windows and Samba Host Using Enum4linux

Requirements:

- Kali linux running as an attacker machine
- Windows 7 running as virtual machine
- Admin privileges

Procedure:

1.Start the kali linux machine and open a terminal window

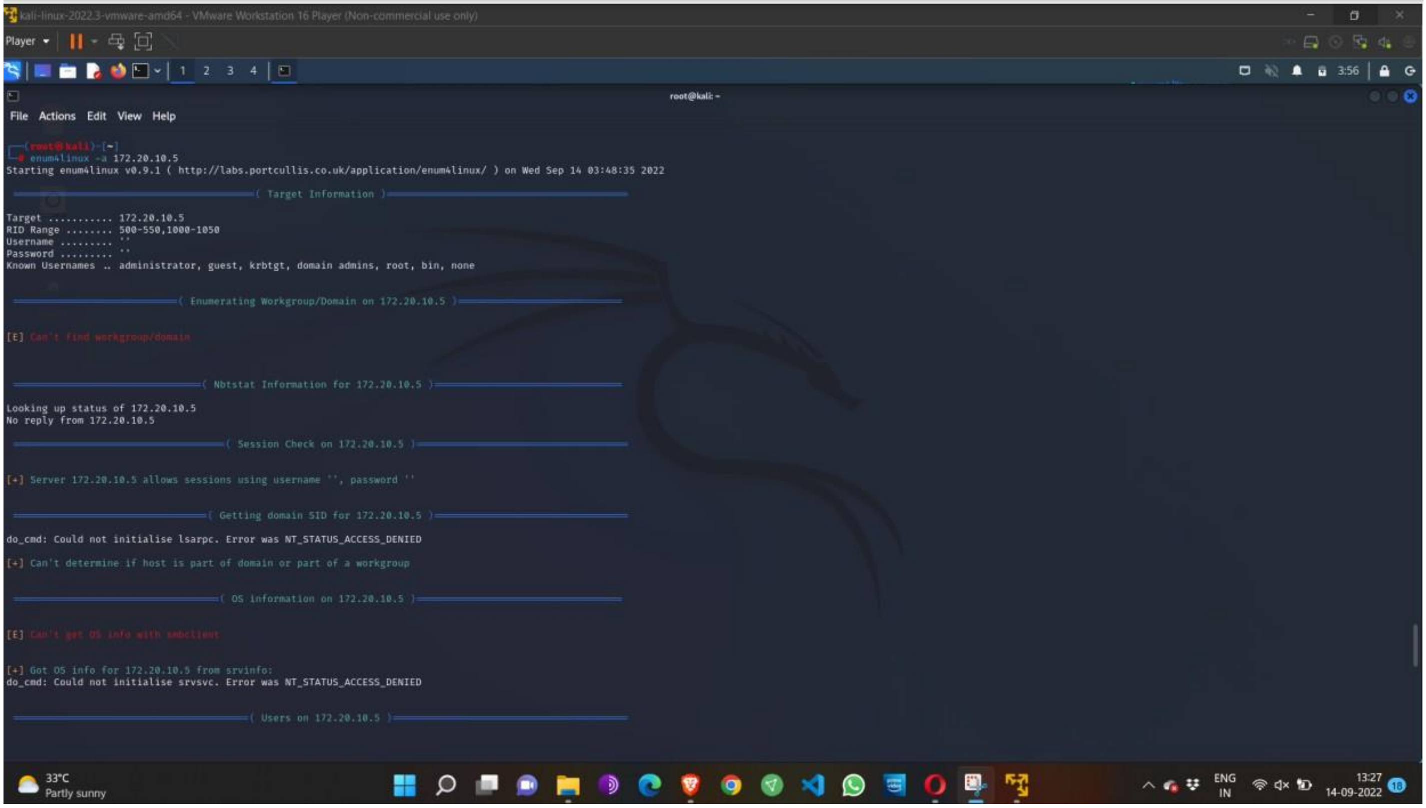
2.Type “sudo apt-get update” command

3.Now type enum4linux-h and hit enter to get help options With the help options conduct the enumeration on target machine

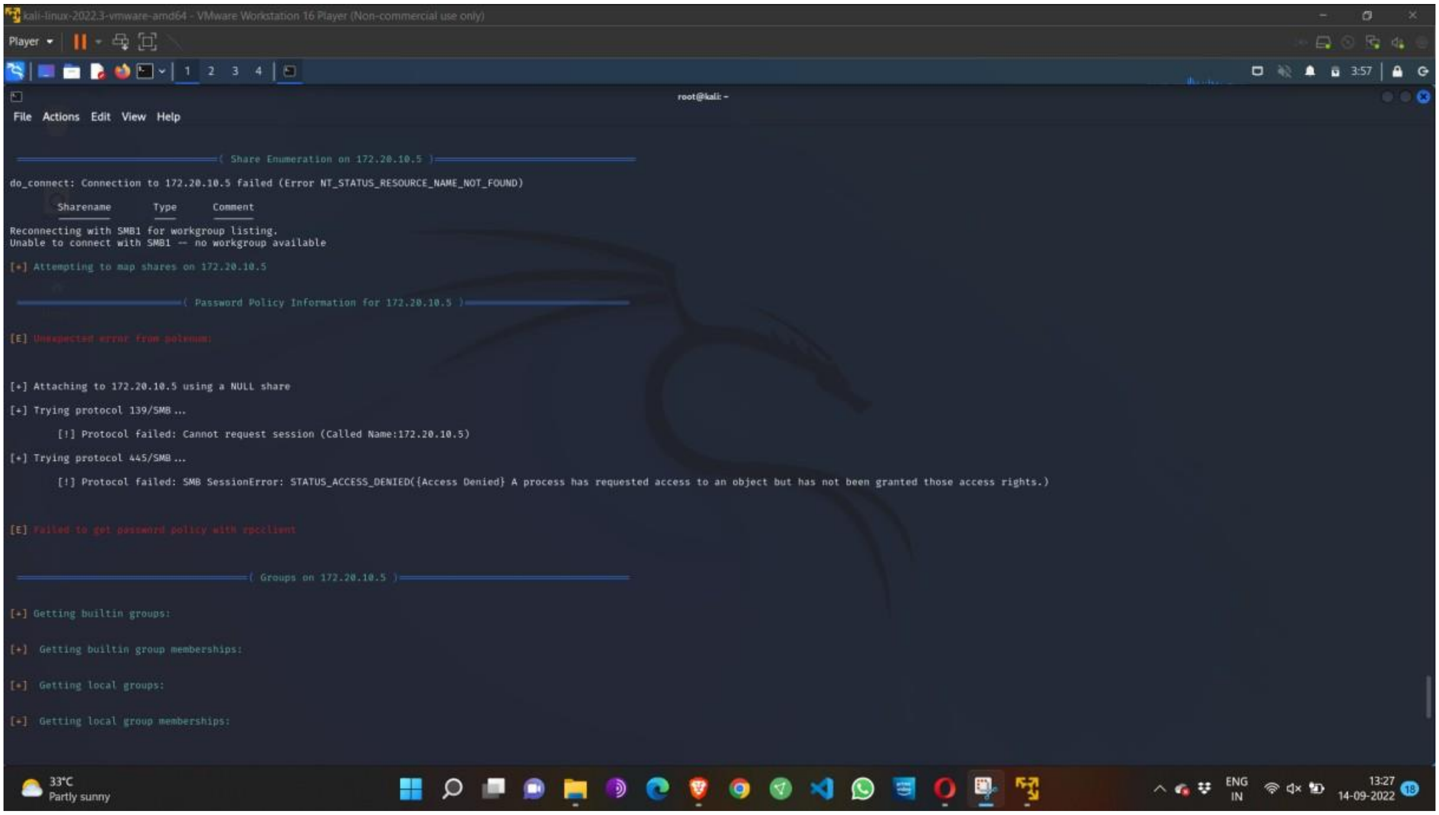
4.In the terminal window type enum4linux -u -p -U and hit enter to run this tool using the user list options

5.Enum4linux starts enumerating the workgroups/domain names first and display the results

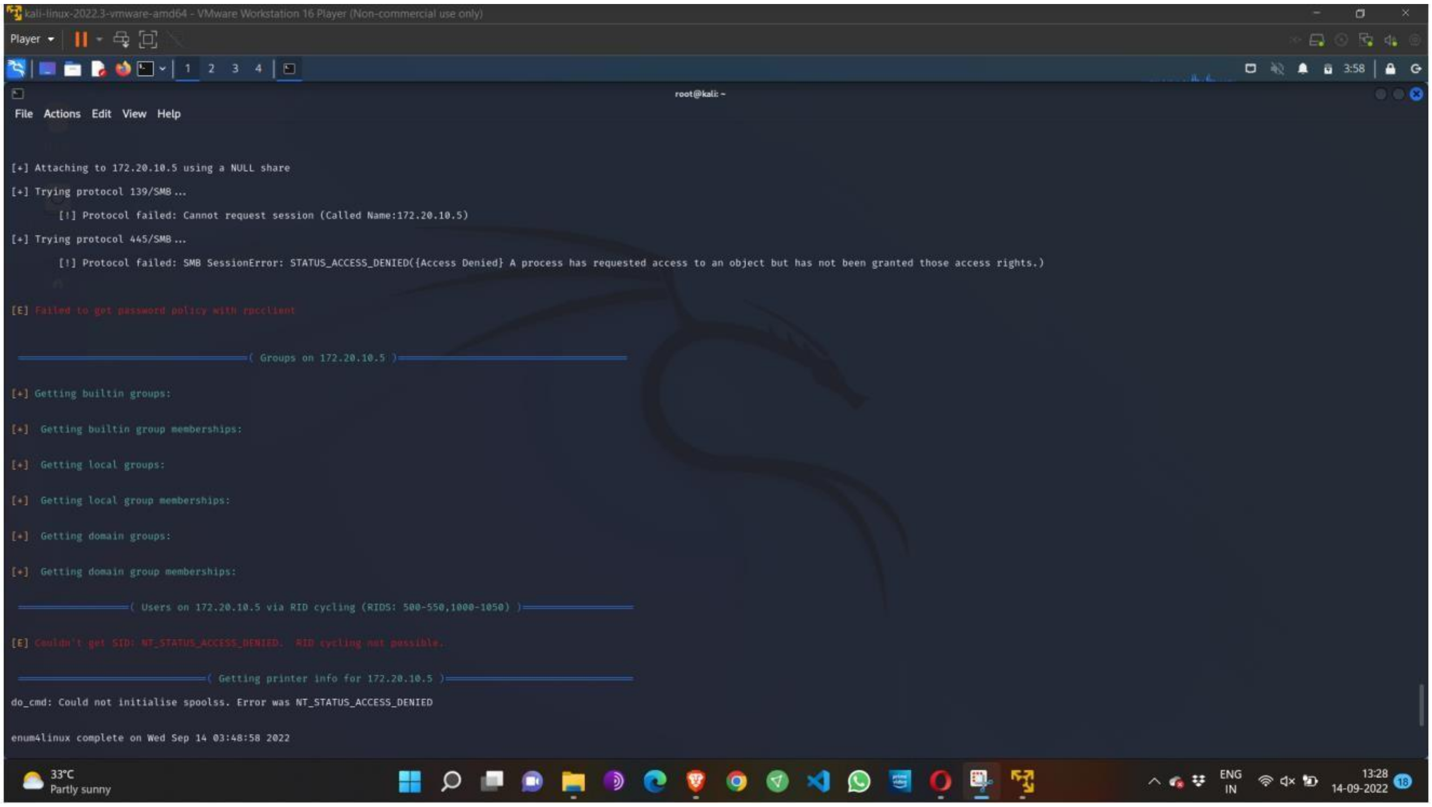
6.To enumerate all the information Use this command enum4linux -a.


kali-linux-2022.3-vmware-amd64 - VMware Workstation 16 Player (Non-commercial use only)
Player
1 2 3 4
3:56
root@kali: ~
File Actions Edit View Help
33°C
Partly sunny
ENG
IN
13:27
14-09-2022

```
┌──(root㉿kali)-[~]
└─# enum4linux -a 172.20.10.5
Starting enum4linux v0.9.1 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Wed Sep 14 03:48:35 2022

 =========================( Target Information )=========================

Target ........... 172.20.10.5
RID Range ........ 500-550,1000-1050
Username ......... ''
Password ......... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none


 ===================( Enumerating Workgroup/Domain on 172.20.10.5 )===================


[E] Can't find workgroup/domain



 ======================( Nbtstat Information for 172.20.10.5 )======================

Looking up status of 172.20.10.5
No reply from 172.20.10.5

 ==========================( Session Check on 172.20.10.5 )==========================


[+] Server 172.20.10.5 allows sessions using username '', password ''


 =======================( Getting domain SID for 172.20.10.5 )=======================

do_cmd: Could not initialise lsarpc. Error was NT_STATUS_ACCESS_DENIED

[+] Can't determine if host is part of domain or part of a workgroup


 =========================( OS information on 172.20.10.5 )=========================


[E] Can't get OS info with smbclient


[+] Got OS info for 172.20.10.5 from srvinfo:
do_cmd: Could not initialise srvsvc. Error was NT_STATUS_ACCESS_DENIED


 =============================( Users on 172.20.10.5 )=============================
```

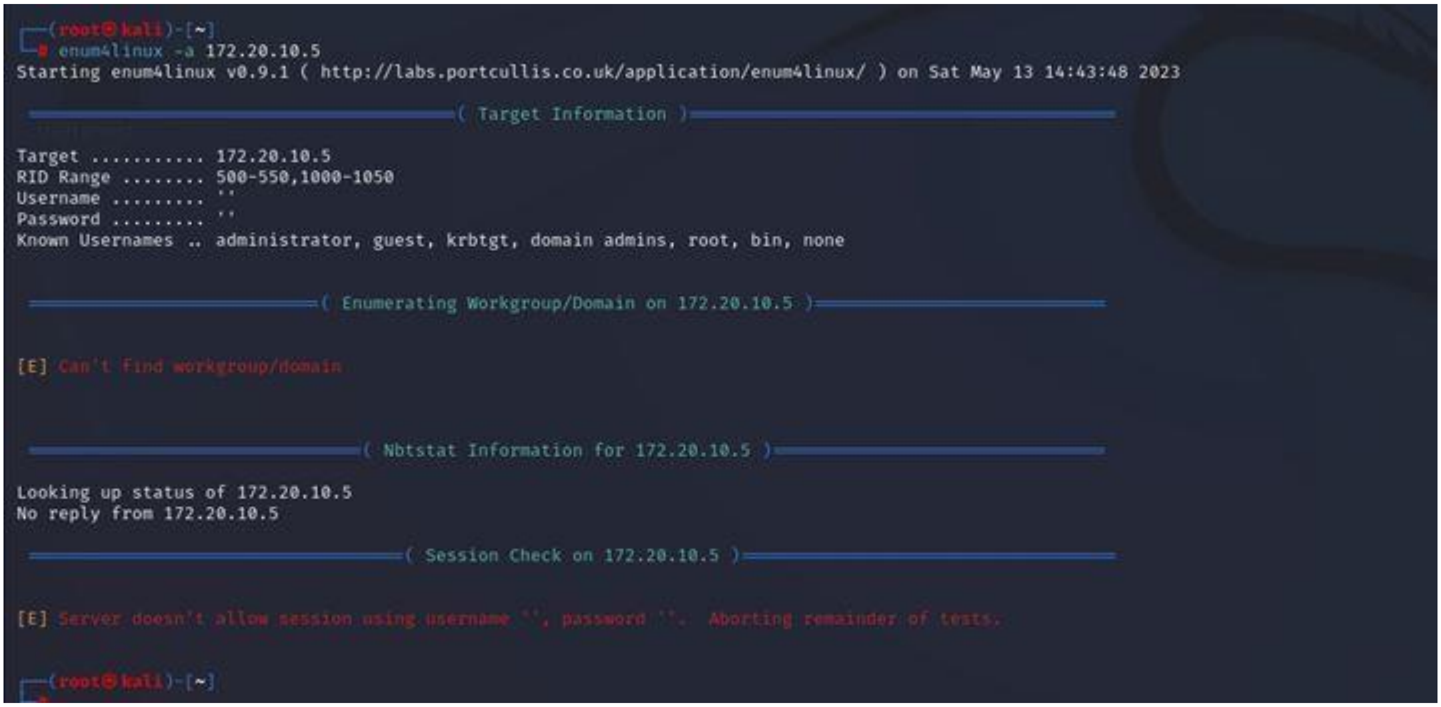

kali-linux-2022.3-vmware-amd64 - VMware Workstation 16 Player (Non-commercial use only)
Player
root@kali: ~
File Actions Edit View Help
3:57
33°C
Partly sunny
ENG
IN
13:27
14-09-2022

```
 ============================( Share Enumeration on 172.20.10.5 )============================

do_connect: Connection to 172.20.10.5 failed (Error NT_STATUS_RESOURCE_NAME_NOT_FOUND)

        Sharename       Type      Comment

Reconnecting with SMB1 for workgroup listing.
Unable to connect with SMB1 -- no workgroup available

[+] Attempting to map shares on 172.20.10.5

 ===========================( Password Policy Information for 172.20.10.5 )===========================

[E] Unexpected error from polenum:


[+] Attaching to 172.20.10.5 using a NULL share

[+] Trying protocol 139/SMB ...

        [!] Protocol failed: Cannot request session (Called Name:172.20.10.5)

[+] Trying protocol 445/SMB ...

        [!] Protocol failed: SMB SessionError: STATUS_ACCESS_DENIED({Access Denied} A process has requested access to an object but has not been granted those access rights.)


[E] Failed to get password policy with rpcclient


 ======================================( Groups on 172.20.10.5 )======================================

[+] Getting builtin groups:

[+]  Getting builtin group memberships:

[+]  Getting local groups:

[+]  Getting local group memberships:
```


kali-linux-2022.3-vmware-amd64 - VMware Workstation 16 Player (Non-commercial use only)
Player
root@kali: ~
File Actions Edit View Help
3:58
33°C
Partly sunny
ENG
IN
13:28
14-09-2022

```
[+] Attaching to 172.20.10.5 using a NULL share

[+] Trying protocol 139/SMB ...

        [!] Protocol failed: Cannot request session (Called Name:172.20.10.5)

[+] Trying protocol 445/SMB ...

        [!] Protocol failed: SMB SessionError: STATUS_ACCESS_DENIED({Access Denied} A process has requested access to an object but has not been granted those access rights.)


[E] Failed to get password policy with rpcclient


 ======================================( Groups on 172.20.10.5 )======================================

[+] Getting builtin groups:

[+]  Getting builtin group memberships:

[+]  Getting local groups:

[+]  Getting local group memberships:

[+]  Getting domain groups:

[+]  Getting domain group memberships:

 ==================( Users on 172.20.10.5 via RID cycling (RIDS: 500-550,1000-1050) )==================

[E] Couldn't get SID: NT_STATUS_ACCESS_DENIED.  RID cycling not possible.

 ===============================( Getting printer info for 172.20.10.5 )===============================

do_cmd: Could not initialise spoolss. Error was NT_STATUS_ACCESS_DENIED


enum4linux complete on Wed Sep 14 03:48:58 2022
```

Output:



```
┌──(root㉿kali)-[~]
└─# enum4linux -a 172.20.10.5
Starting enum4linux v0.9.1 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Sat May 13 14:43:48 2023

 ===========================================( Target Information )===========================================

Target ........... 172.20.10.5
RID Range ........ 500-550,1000-1050
Username ......... ''
Password ......... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none


 ==============================( Enumerating Workgroup/Domain on 172.20.10.5 )==============================


[E] Can't find workgroup/domain



 ==================================( Nbtstat Information for 172.20.10.5 )==================================

Looking up status of 172.20.10.5
No reply from 172.20.10.5

 =====================================( Session Check on 172.20.10.5 )=====================================


[E] Server doesn't allow session using username '', password ''.  Aborting remainder of tests.


┌──(root㉿kali)-[~]
```

Result:

The above experiment is done using enum4linux command. This experiment is about Enumerating information from windows and Samba Host Using Enum4linux. This experiment is carried out in root terminal using kali linux Operating System.

EX.NO: 10 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
```

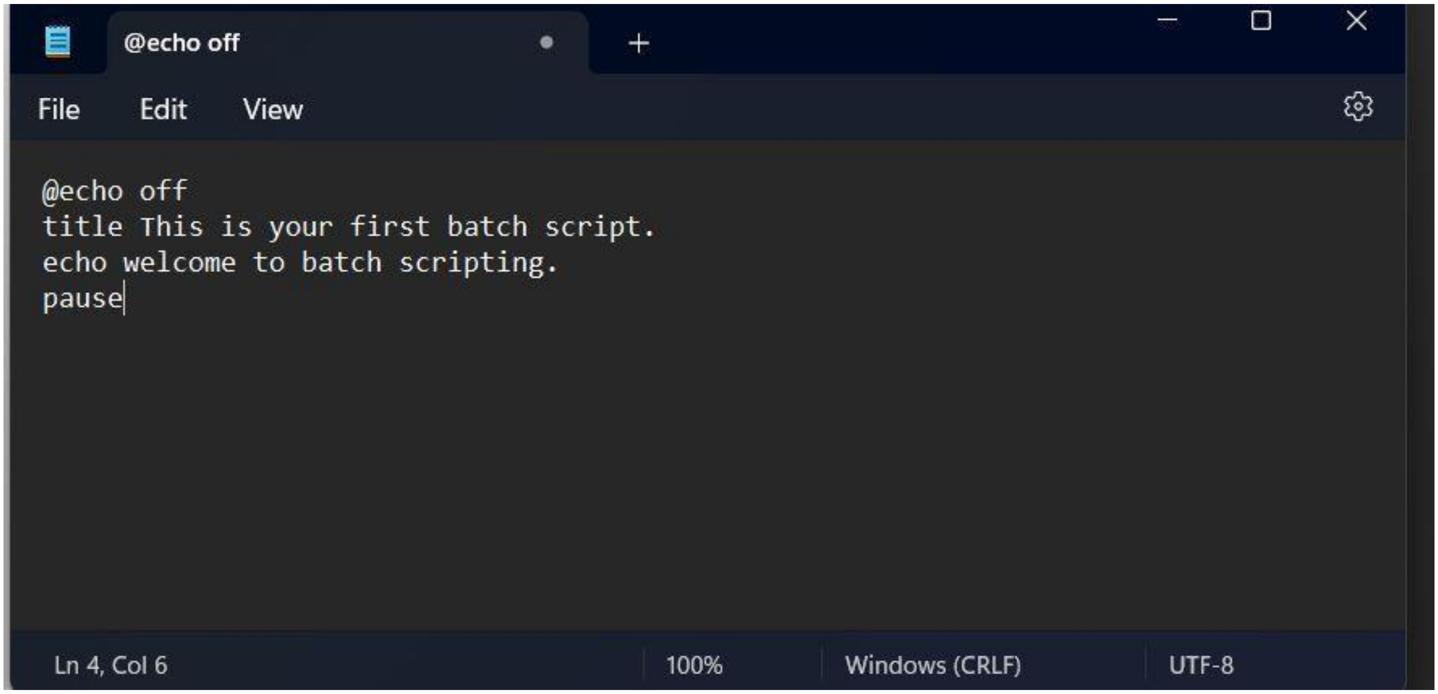
1. TO SAVE a BAT File

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.

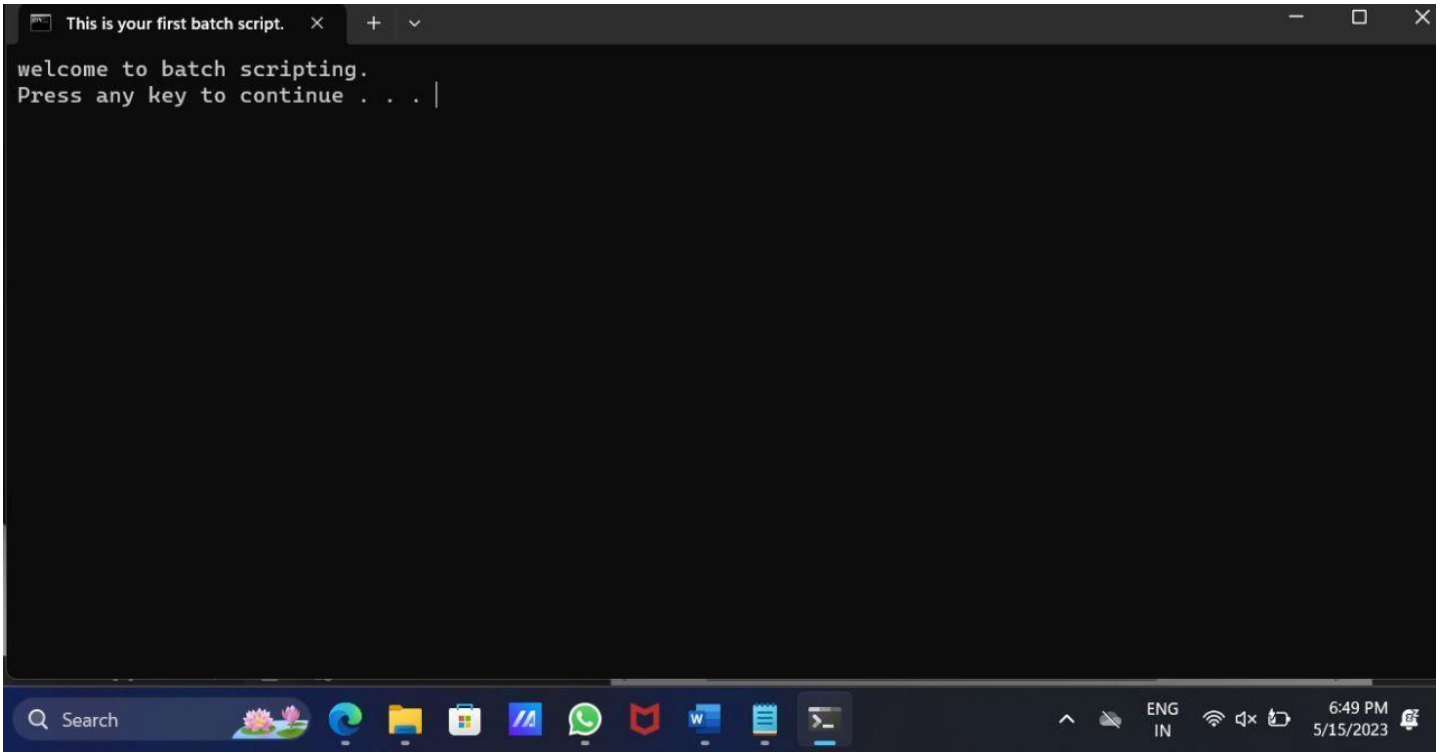
2.To RUN as BAT File

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.

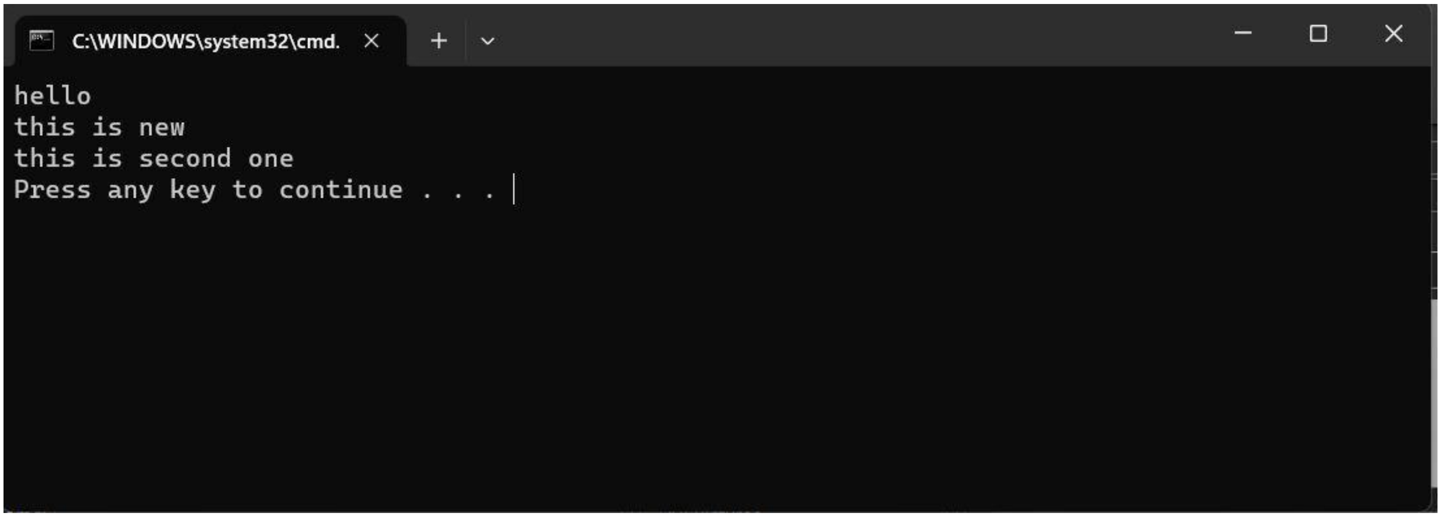
OUTPUT:



```
@echo off
title This is your first batch script.
echo welcome to batch scripting.
pause
```



```
welcome to batch scripting.
Press any key to continue . . .
```



```
hello
this is new
this is second one
Press any key to continue . . .
```

Result:

The above experiment is carried out using windows command prompt. The main aim of this experiment is to create a windows batch file using batch file extension. After this experiment, I was able to create a windows batch file using sufficient data.