

ITA1471

ETHICAL HACKING FOR NETWORK HACKING



B. Jaswanth

192211084

1st YEAR, CSE DEPARTMENT

ITA1471-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

<u>Flag</u>	<u>Use</u>	<u>Example</u>
-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:

```
└─(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://nmap.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.

6)

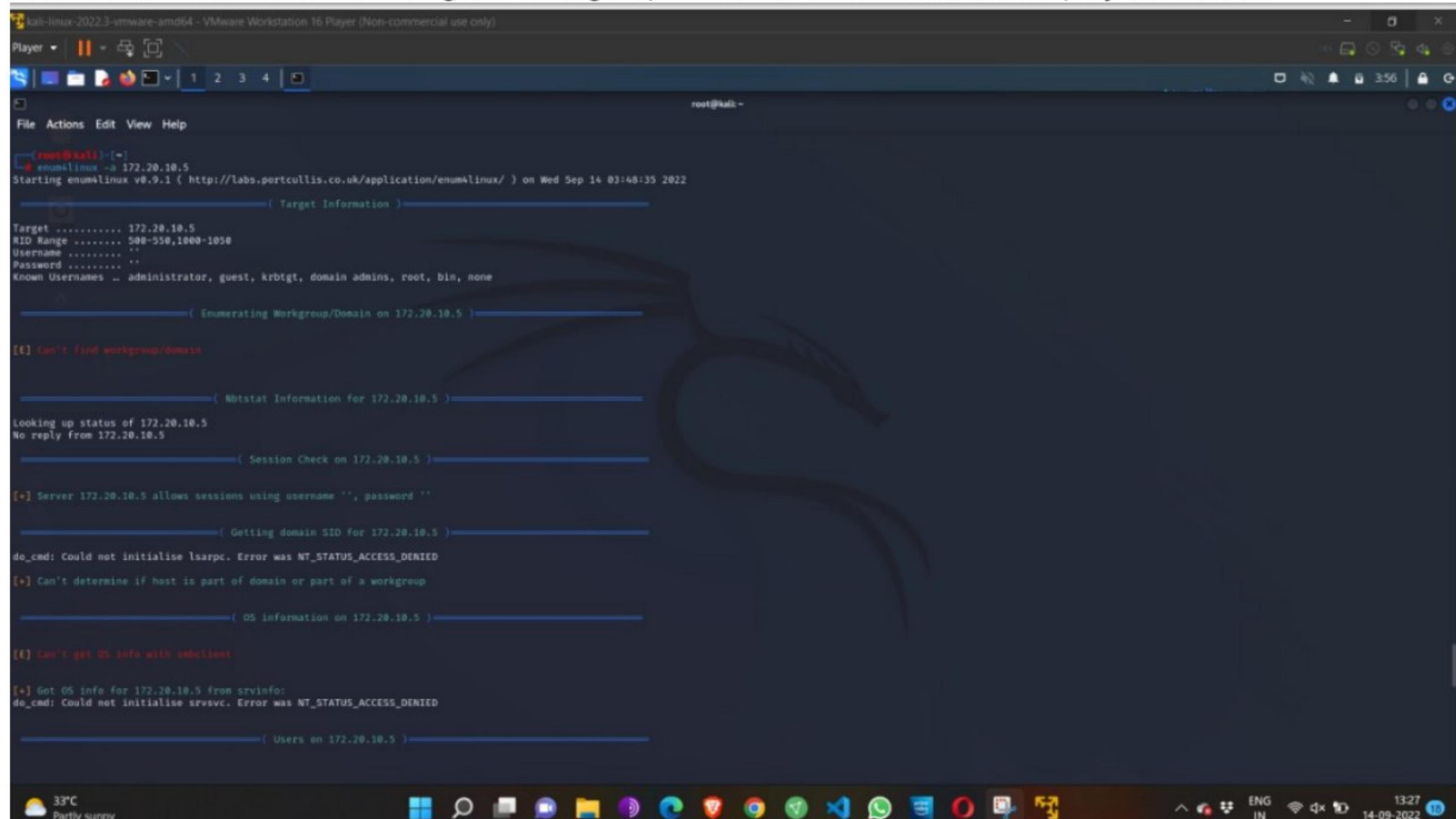
Ex. No.2 – ENUMERATION - Enumerating information from windows and Samba Host Using Enum4linux

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



```
[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 subclient

[*] Got OS info for 172.20.10.5 from svrinfo:
do_cmd: Could not initialise svrsvc. Error was NT_STATUS_ACCESS_DENIED

[+] Users on 172.20.10.5
```

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

```
7) kali-linux-2022.3-vmware-amd64 - VMware Workstation 16 Player (Non-commercial use only)
Player | 1 2 3 4 | 
File Actions Edit View Help

[+] 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 credential.

[+] Groups on 172.20.10.5
[+] Getting builtin groups:
[+] Getting builtin group memberships:
[+] Getting local groups:
[+] Getting local group memberships:

33°C Partly sunny 13:27 14-09-2022 ENG IN 3:57 G
```

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

[+] 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 credential.

[+] 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
33°C Partly sunny 13:28 14-09-2022 ENG IN 3:58 G
```

8)

```
[root@kali:~]# enum4linux -a 172.20.10.5
Starting enum4linux v0.9.1 ( http://labs.portcallis.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:~]
```

Output:

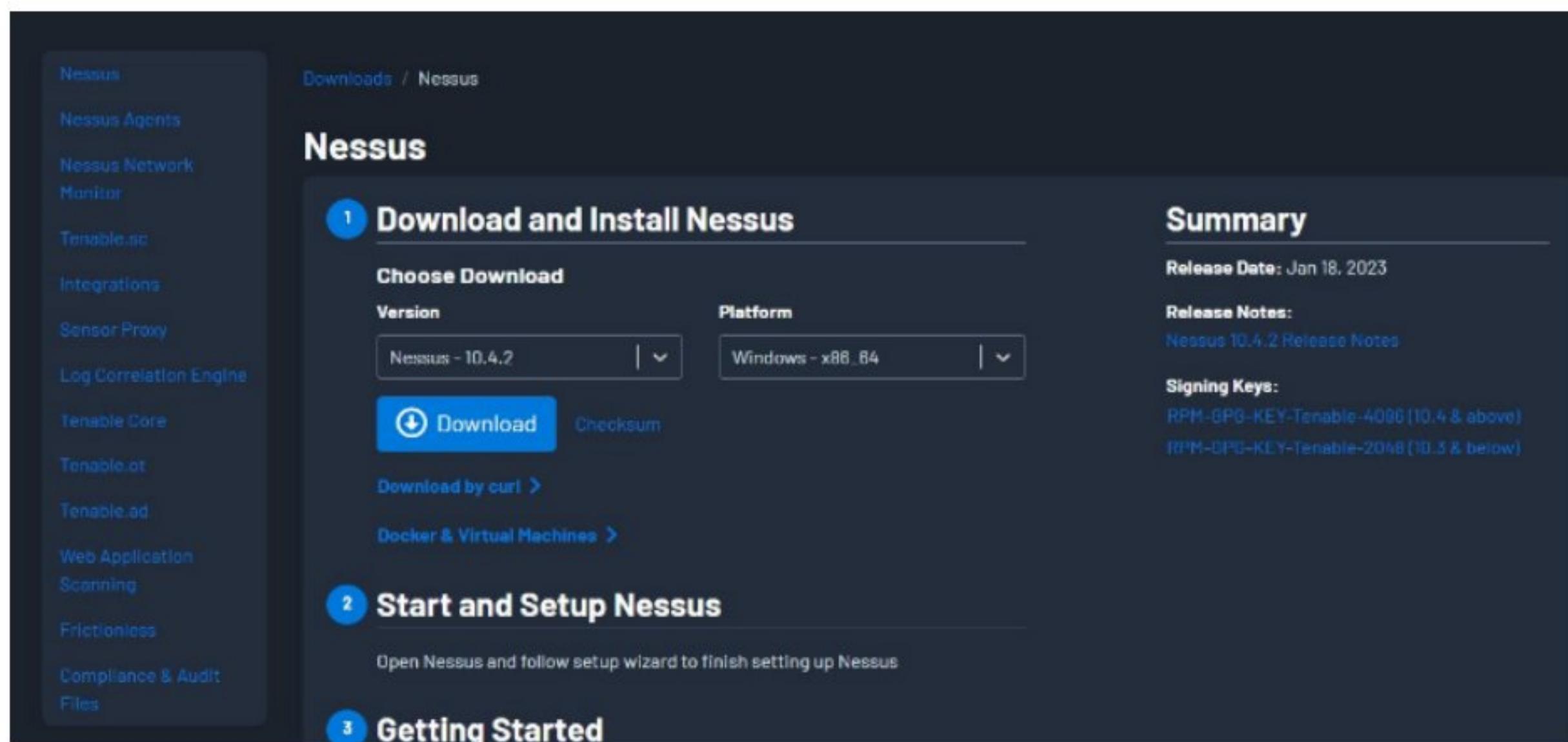
Result:

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.

Exercise No 3: Vulnerability Access Scan Using Nessus

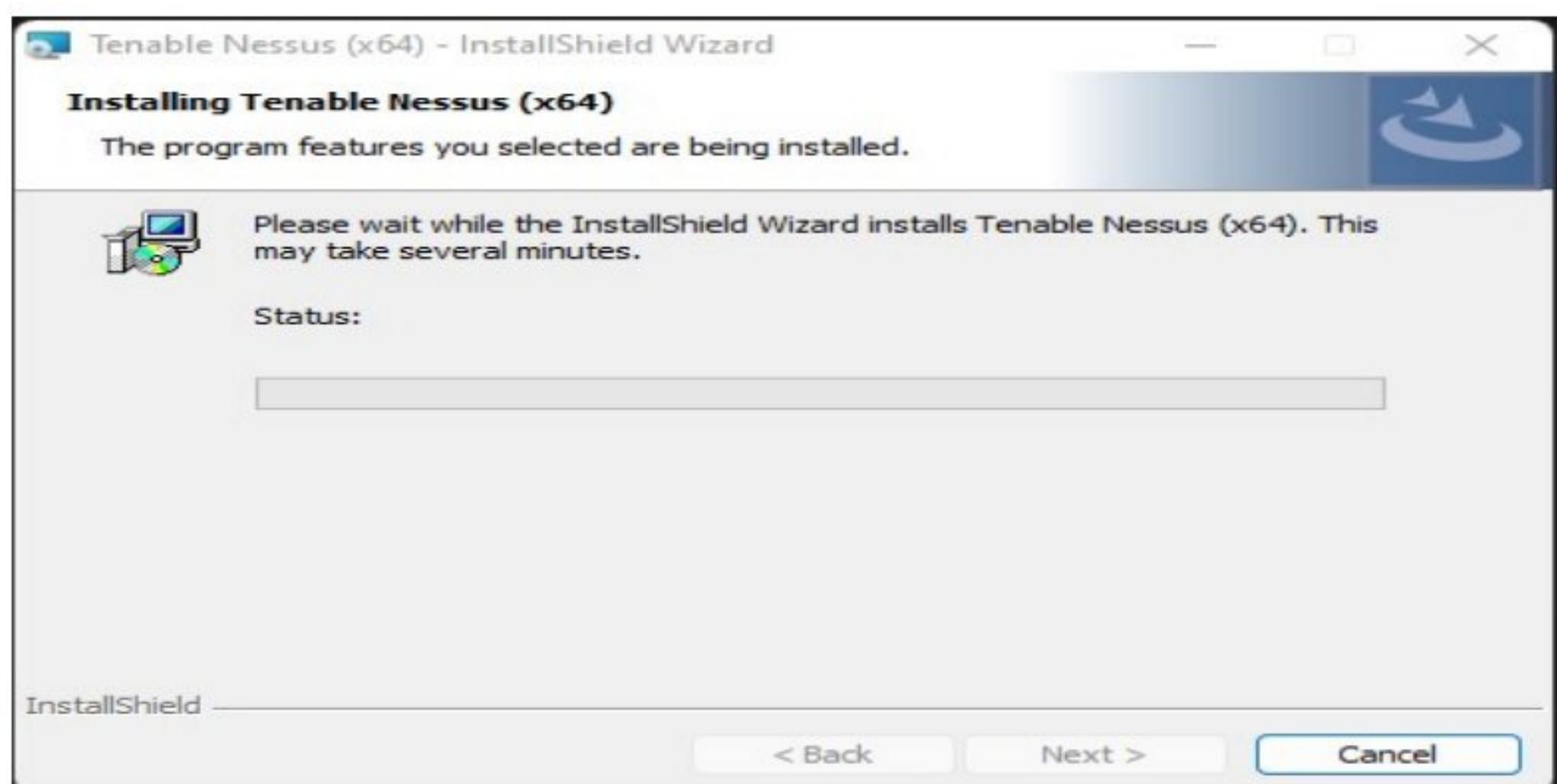
Aim : To Download and install Nessus tool and perform a Vulnerability Access scan in kali Linux Operating systems.

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



The screenshot shows the 'Downloads / Nessus' page on the Tenable website. The left sidebar lists various Tenable products: Nessus, Nessus Agents, Nessus Network Monitor, Tenable.sc, Integrations, Sensor Proxy, Log Correlation Engine, Tenable Core, Tenable.ot, Tenable.ad, Web Application Scanning, Frictionless, and Compliance & Audit Files. The main content area is titled 'Nessus' and contains three numbered sections: 1. 'Download and Install Nessus' (with 'Choose Download' dropdowns for 'Version' (Nessus - 10.4.2) and 'Platform' (Windows - x86_64)), a 'Download' button, and links for 'Download by curl' and 'Docker & Virtual Machines'. 2. 'Start and Setup Nessus' (with the text 'Open Nessus and follow setup wizard to finish setting up Nessus'). 3. 'Getting Started' (with the text 'Install and run Nessus to begin your security assessment'). To the right, a 'Summary' section provides the 'Release Date' (Jan 18, 2023), 'Release Notes' (Nessus 10.4.2 Release Notes), and 'Signing Keys' (RPM-GPG-KEY-Tenable-4098 (10.4 & above) and RPM-GPG-KEY-Tenable-2048 (10.3 & below)).

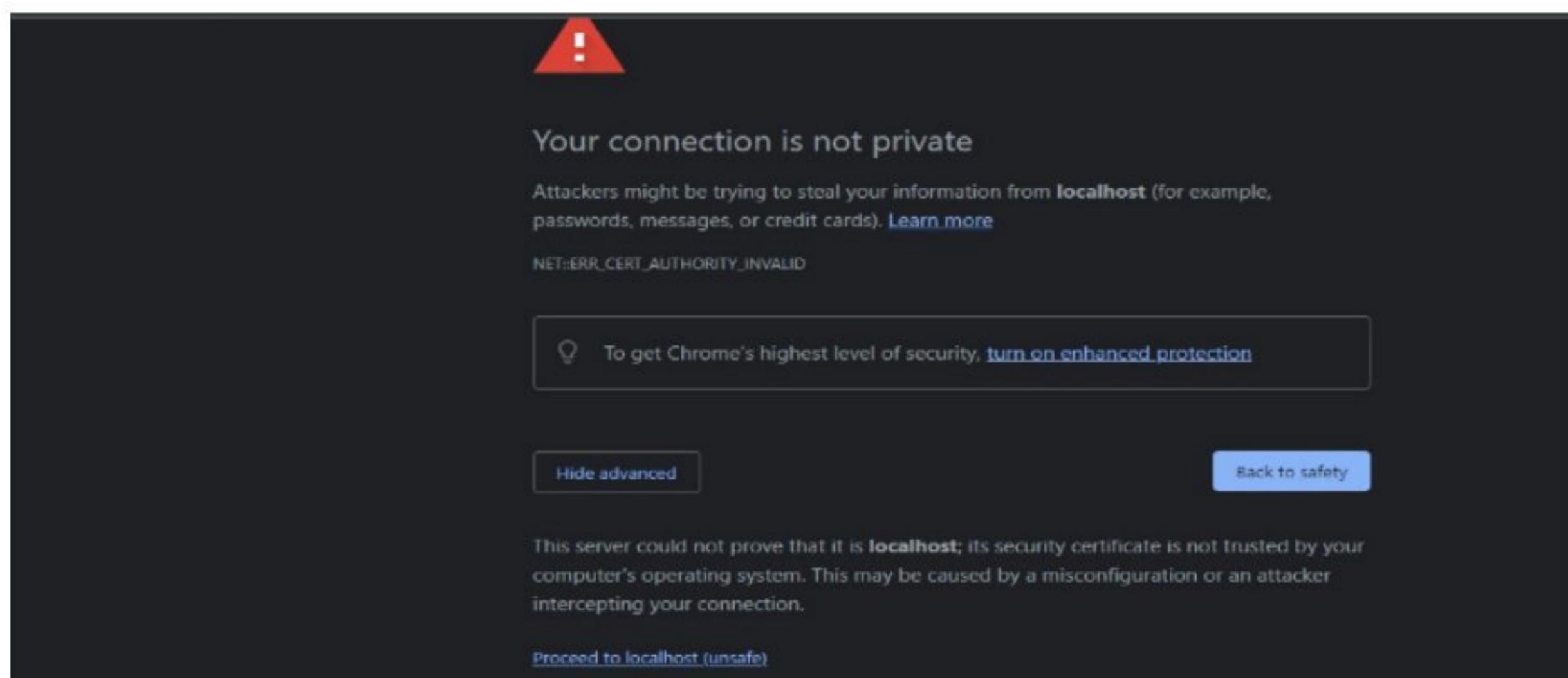
Step 2: Choose your OS and download , install



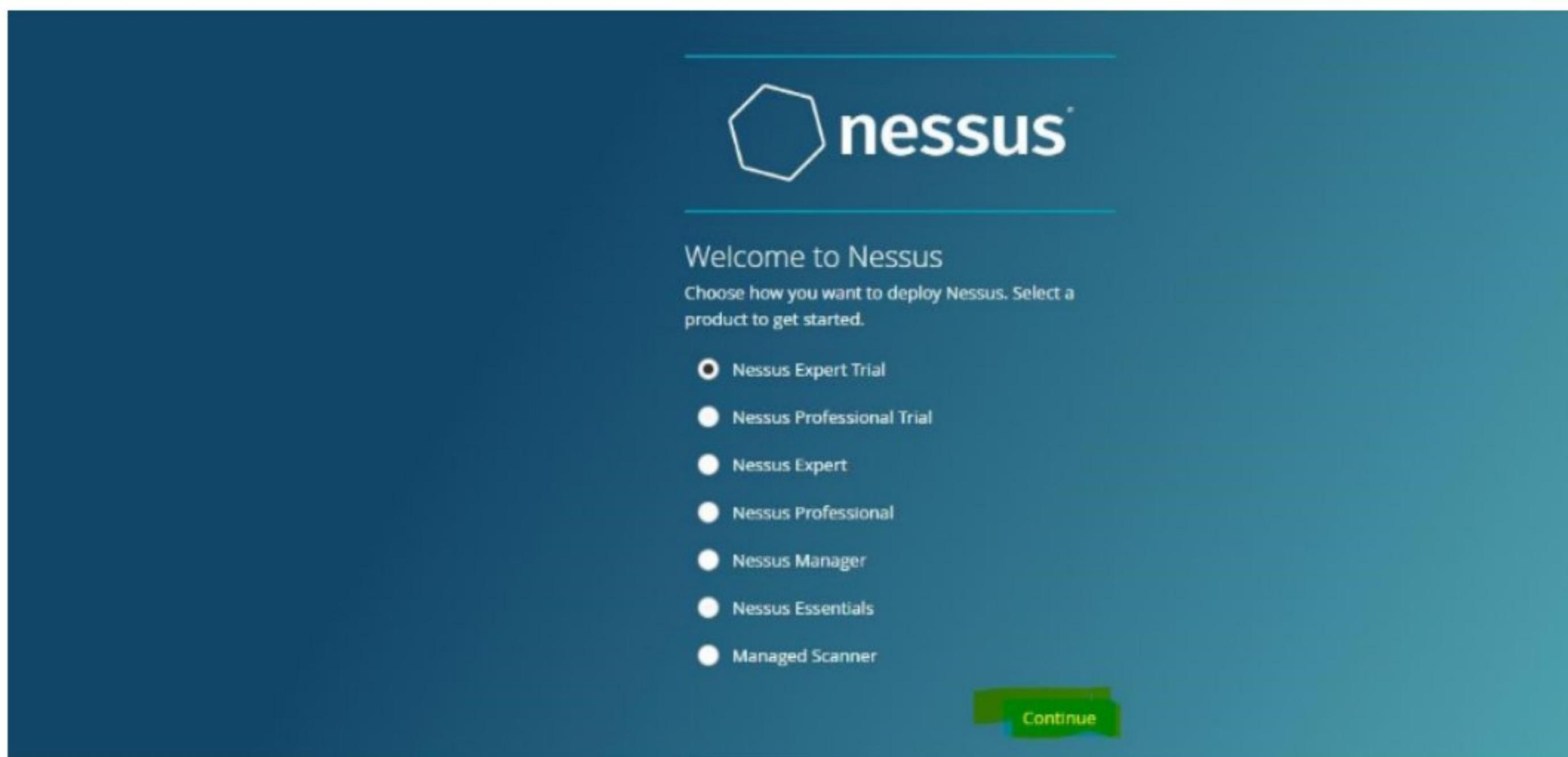
Step 3: Once installation is completed it will open in default browser



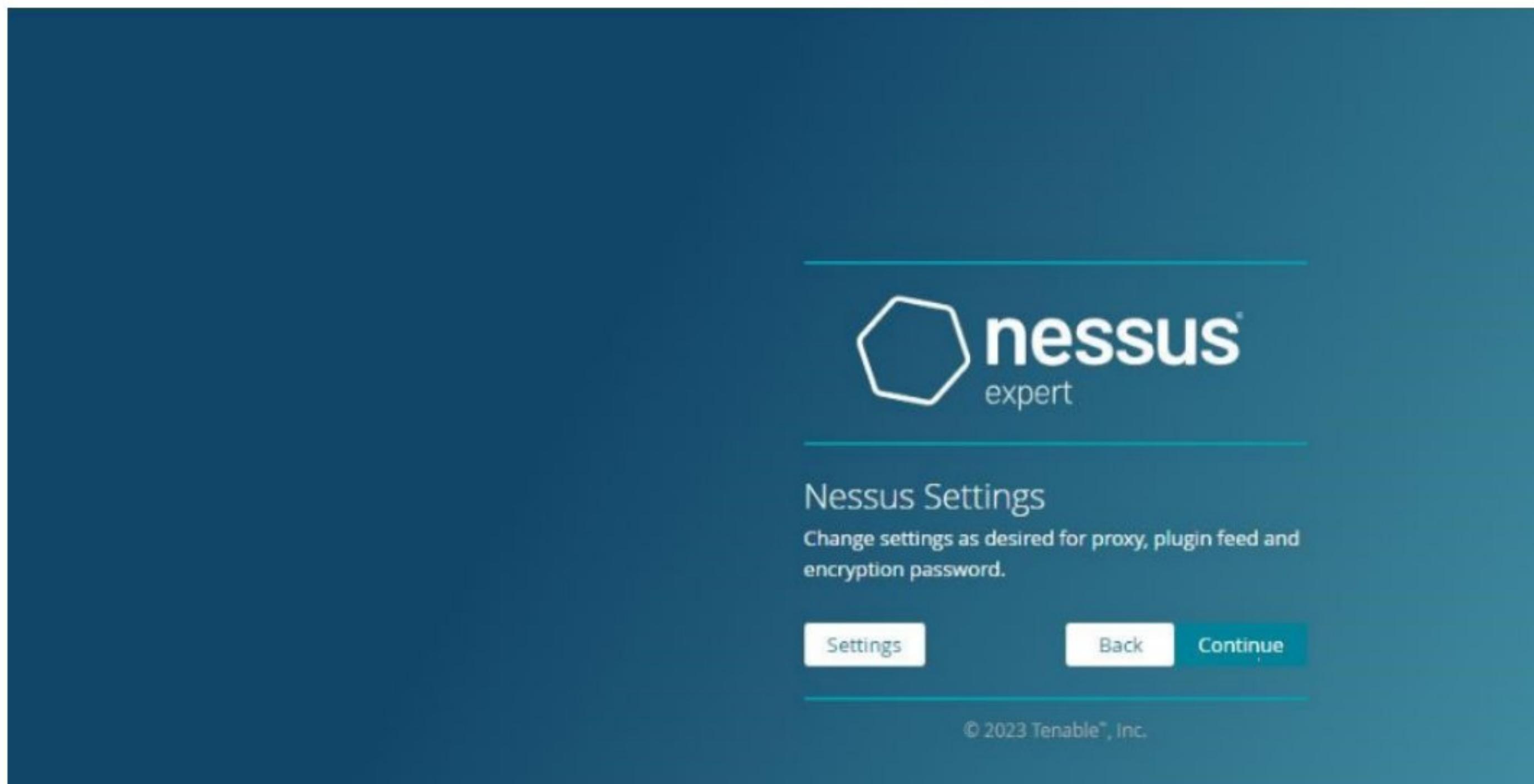
Step 5:- (click on the proceed to local host)



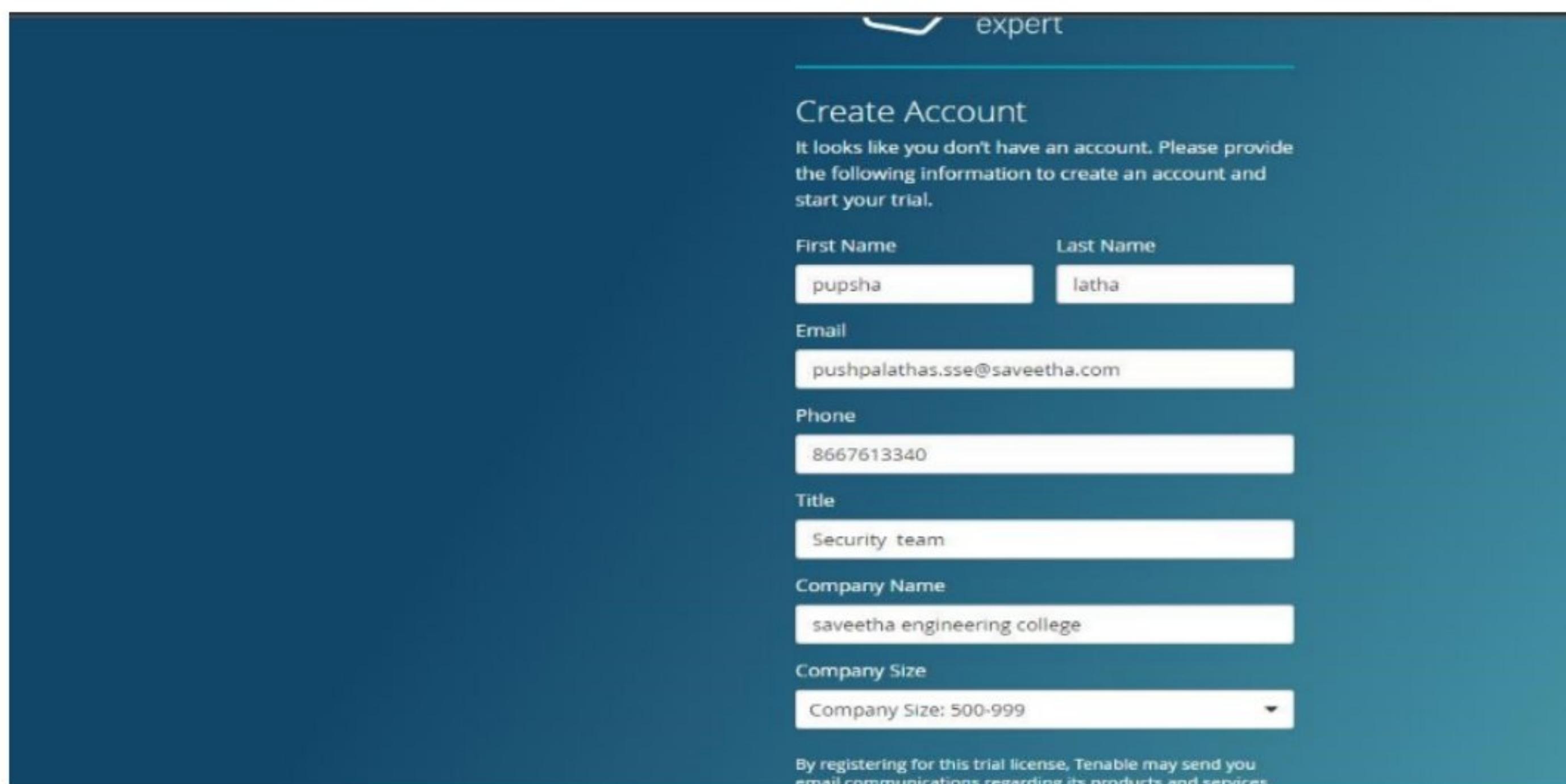
Step 6:- Please choose the Nessus Expert



Step 7: Click on continue



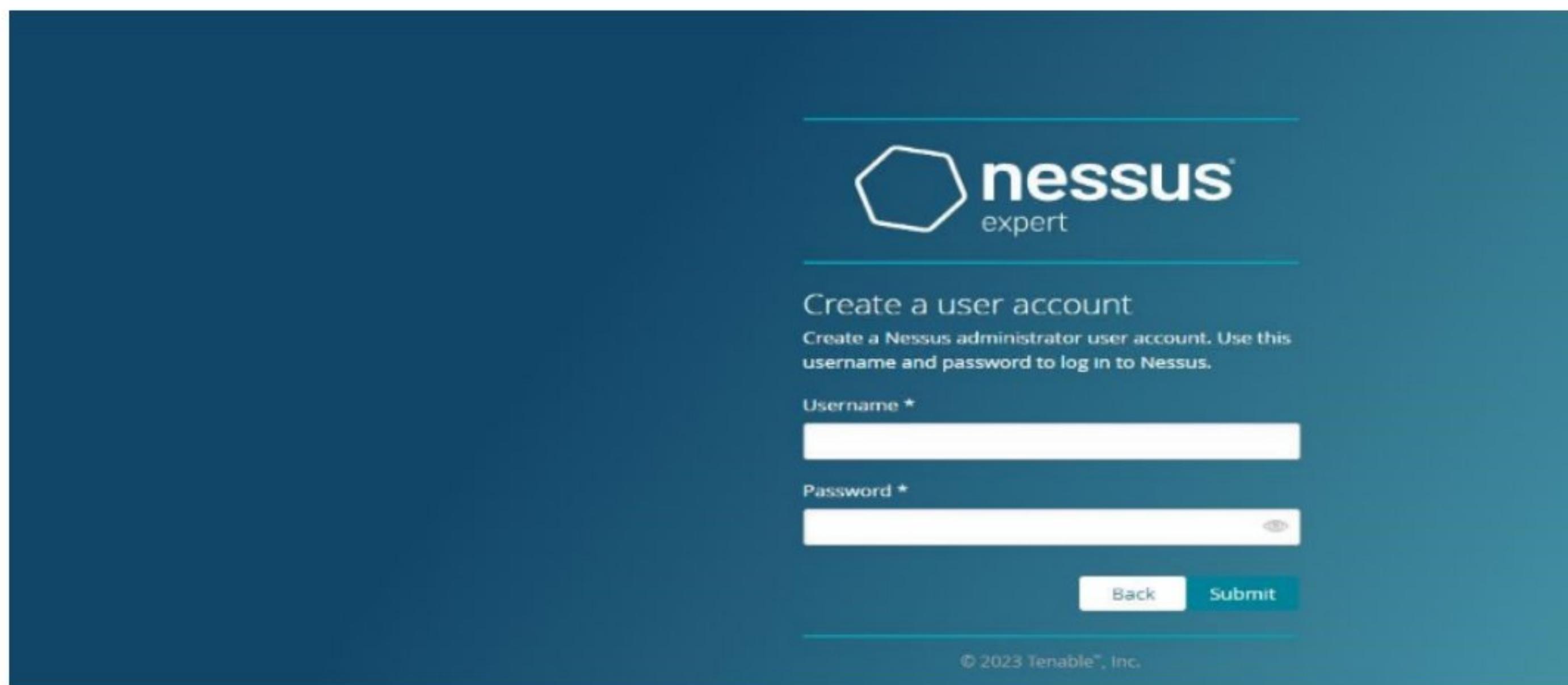
Step 8:- Register with your organizational email id



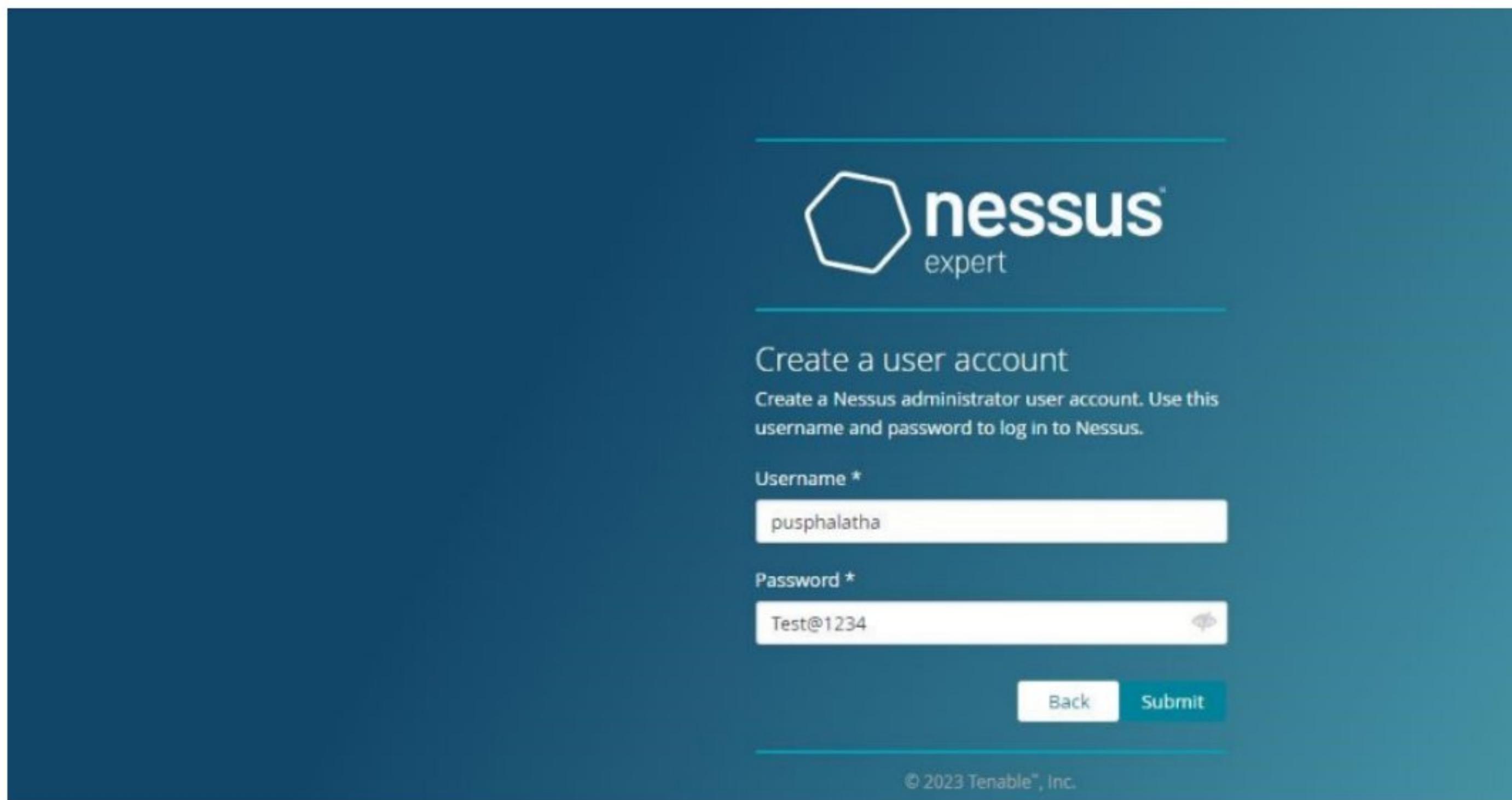
Step 9:- please note down the activation key



Step 10:- set up your username & password



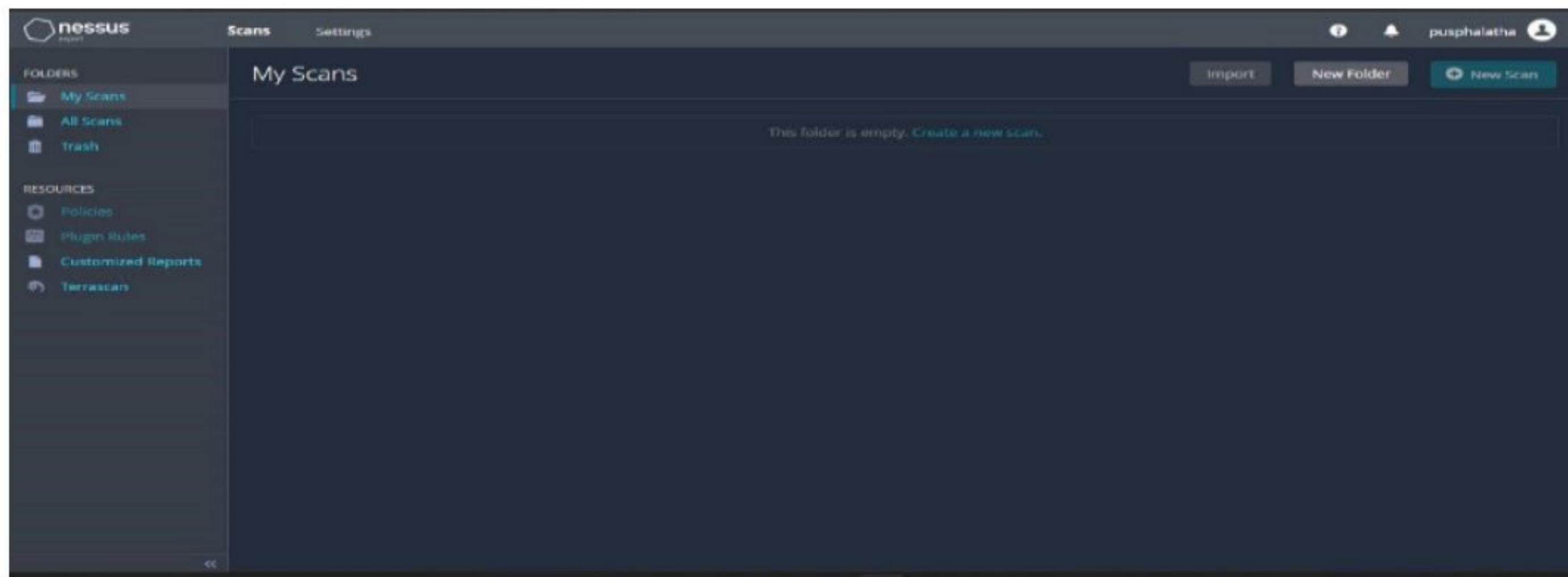
Step 11:-Type username and password



Step 12:- Please wait until download is completed

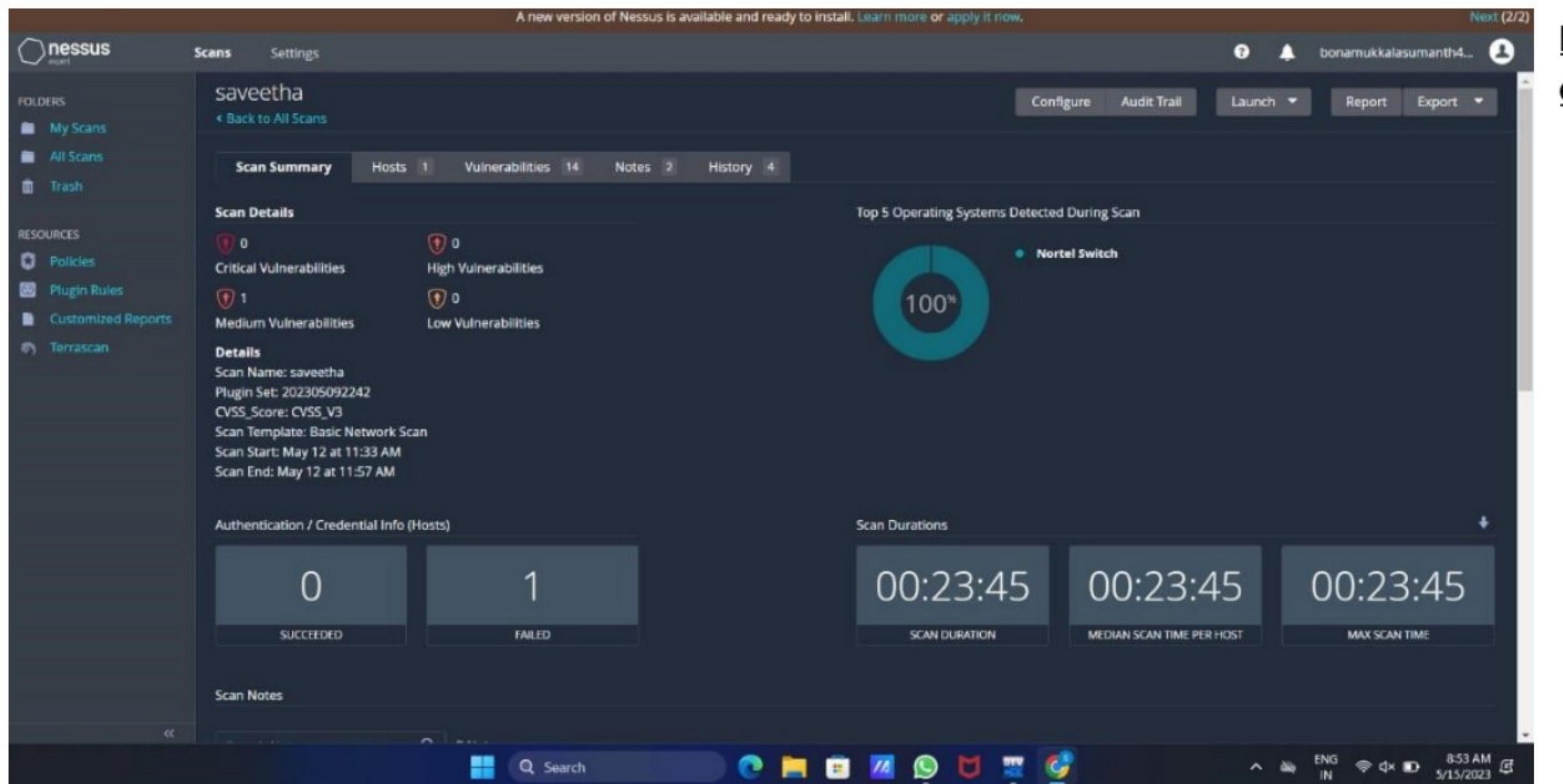


Step 13: Select My Scans



Output:

A screenshot of the Nessus web interface showing policy details for a scan. The top navigation bar includes the Nessus logo, 'Scans', 'Settings', and a user profile for 'bonamukkalasumanth4...'. The left sidebar has sections for 'FOLDERS' (My Scans, All Scans, Trash) and 'RESOURCES' (Policies, Plugin Rules, Customized Reports, Terrascan). The main content area displays policy details. It includes sections for 'DNS Issue' (unable to resolve log4shell-generic-pH2jhqlaCfpXPS0Q057.r.nessus.org), 'Log4j DNS Failed Request' (unable to resolve DNS 'r.nessus.org' to check Log4j Vulnerability), and 'Policy Details' (Basic Overview, Assessment Overview, Advanced Overview, Port Scanner Overview, and Fragile Devices). The bottom of the screen shows a taskbar with various icons and the system tray.



ult:

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

EX.NO: 4 BATCH FILE EXECUTION

AIM:

To create a Windows batch file.

PROCEDURE:

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

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

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

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

Step 5: To edit your batch file, right-click the BAT file and select Edit. And here's the corresponding command window for the example above:

1.Create a New Text Document:

A batch file simplifies repeatable computer tasks using the Windows command prompt. Below is an example of a batch file responsible for displaying some text in your command prompt.

Create a new BAT file by right-clicking an empty space within a directory and selecting New, then Text Document.

1.CODE:

Double-click this New Text Document to open your default text editor. Copy and paste the following code into your text entry:

```
>> @echo off
>> echo hello
>> Pause
>> echo This is new
>> echo this is second
one >> pause
```

1. TO SAVE a BAT File

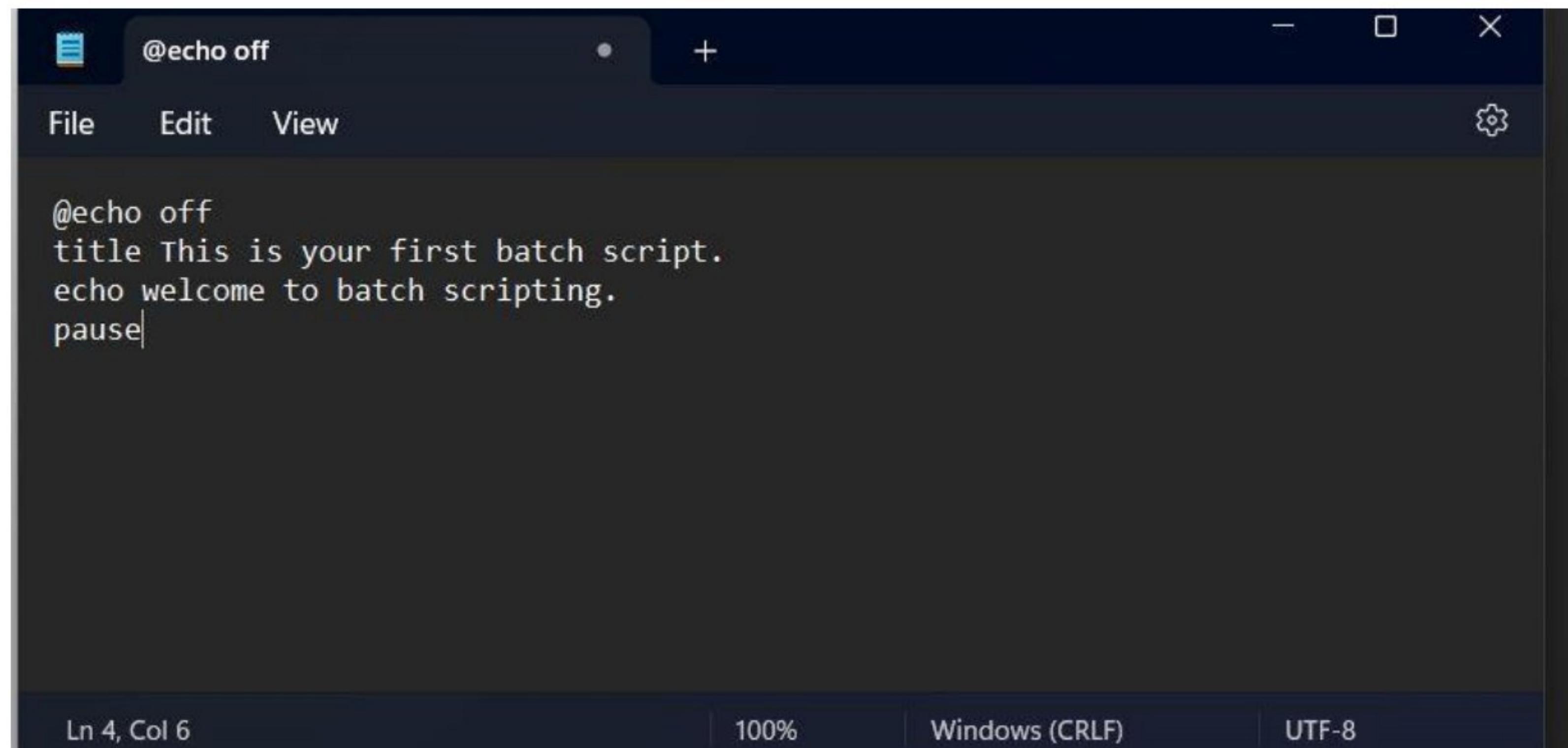
The above script echoes back the text "Welcome to batch scripting!" Save your file by heading to File > Save As, and then name your file what you'd like. End your file name with the added BAT extension, for example test.bat, and click OK. This will finalize the batch process. Now, double-click on your newly created batch file to activate it.

2. To RUN as BAT File

Once you'd saved your file, all you need to do is double-click your BAT file. Instantly, your web pages will open. If you'd like, you can place this file on your desktop. This will allow you to access all of your favorite websites at once.

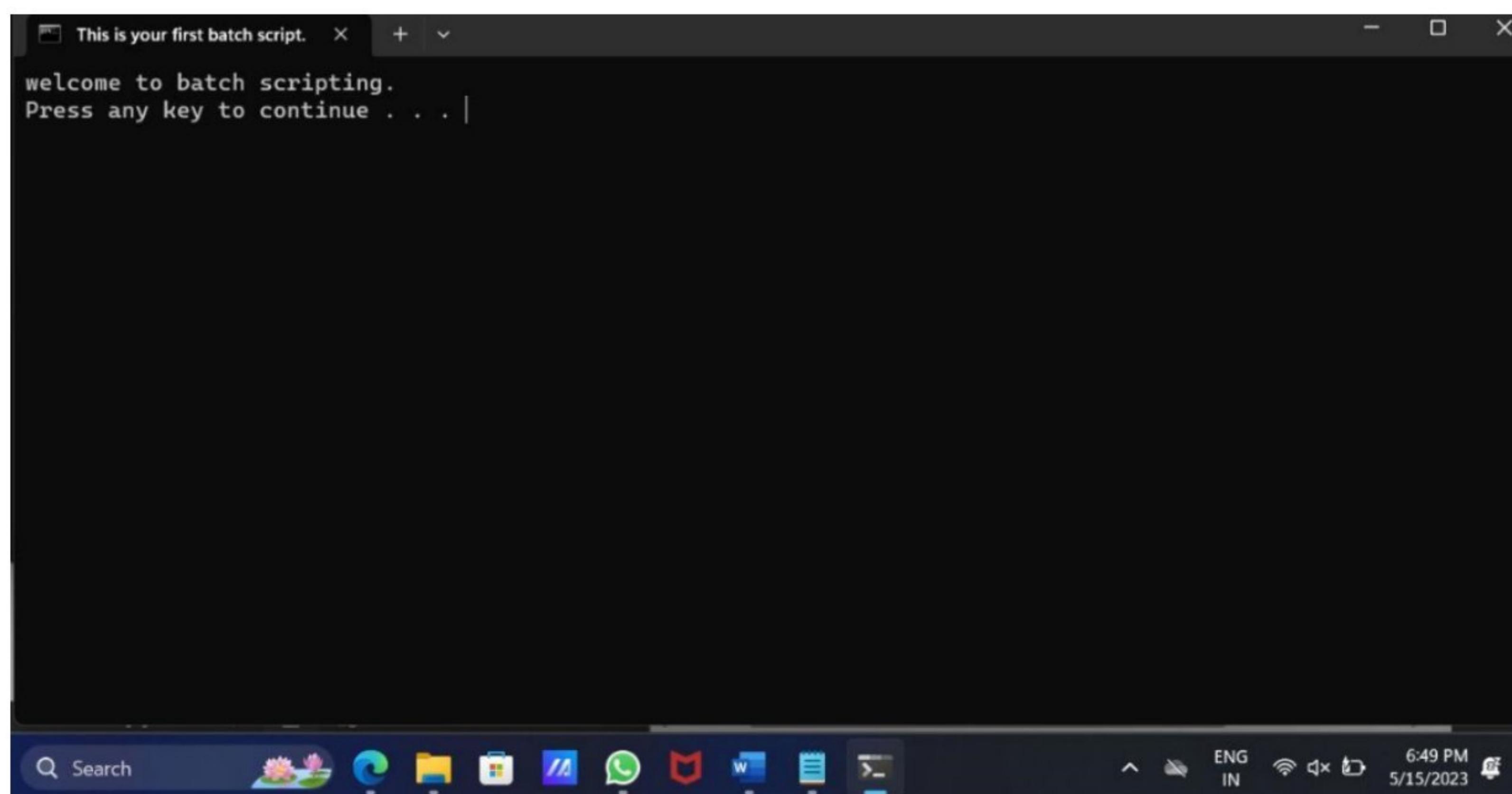
OUTPUT:

Result:



The screenshot shows a code editor window with a dark theme. The title bar says '@echo off'. The menu bar includes 'File', 'Edit', and 'View'. The status bar at the bottom shows 'Ln 4, Col 6', '100%', 'Windows (CRLF)', and 'UTF-8'. The main editor area contains the following batch script code:

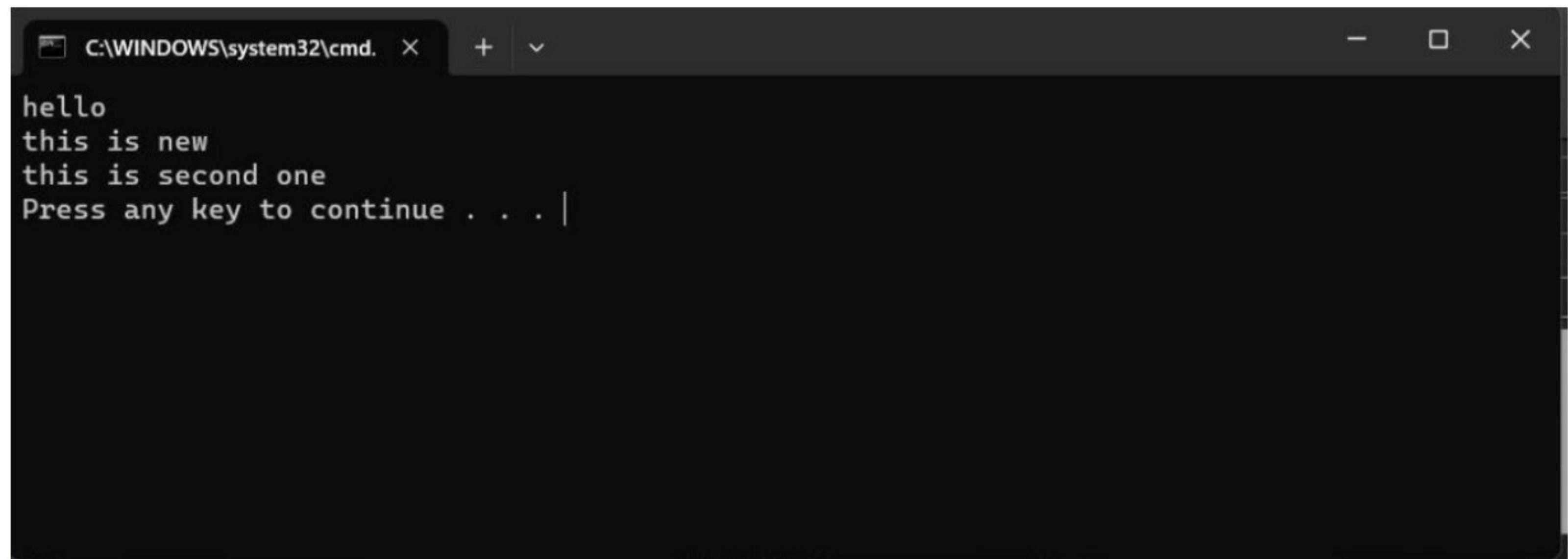
```
@echo off
title This is your first batch script.
echo welcome to batch scripting.
pause
```



The screenshot shows a terminal window with a dark theme. The title bar says 'This is your first batch script.'. The main window displays the output of the batch script:

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

The taskbar at the bottom shows various icons for Windows applications like File Explorer, Edge, and File History. The system tray shows the date and time as '5/15/2023 6:49 PM'.

A screenshot of a Windows Command Prompt window. The title bar reads "C:\WINDOWS\system32\cmd. x". The window contains the following text:

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

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.

Exercise No 5: Information gathering using theHarvester

Aim: To demonstrate information gathering using theHarvester

Procedure:

STEP 1: Open Terminal in the kali linux

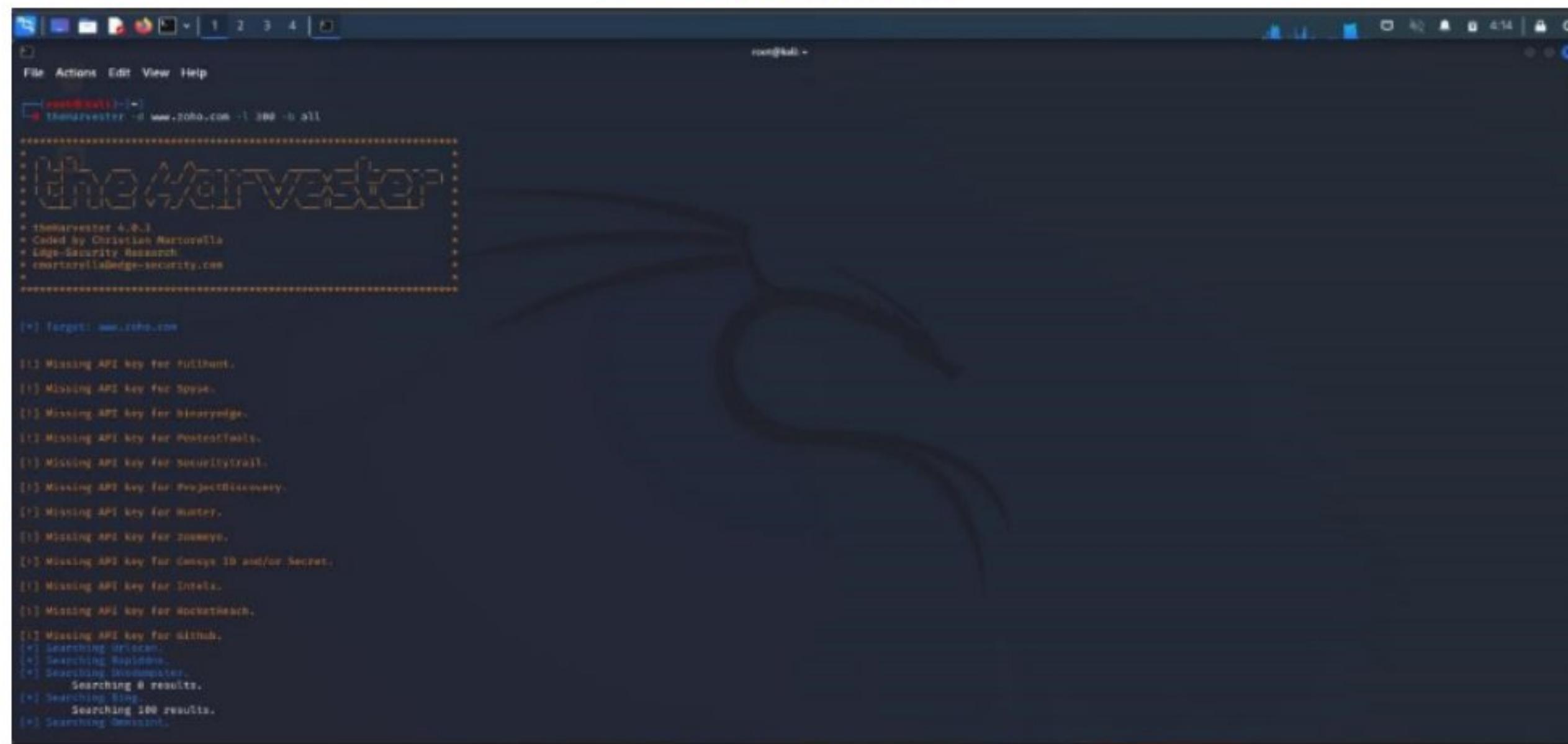
`-d [url]` will be the remote site from which you wants to fetch

`-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`



```
theHarvester 4.0.1
Coded by Christian Martorella
Edge-Security Research
crypticrededge-security.com

[*] Target: www.zoho.com
[*] Missing API key for Fulltext.
[*] Missing API key for Sogou.
[*] Missing API key for Baidu.
[*] Missing API key for ProjectD.
[*] Missing API key for Securitytrail.
[*] Missing API key for ProjectDiscovery.
[*] Missing API key for Hunter.
[*] Missing API key for Zmeye.
[*] Missing API key for Google ID and/or Secret.
[*] Missing API key for Shodan.
[*] Missing API key for Rocketchat.
[*] Missing API key for GitHub.
[*] Searching 8 results.
[*] Searching 300 results.
[*] Searching 100 results.
[*] Searching 200 results.
[*] Searching 0 results.
```

```
root@kali: ~
File Actions Edit View Help
  Searching 300 results.
[*] Searching LinkedIn.
An exception has occurred: B, message='Attempt to decode JSON with unexpected mimetype: text/html', url=URL('https://api.linkedin.com/v1/subdomain-enumeration?domain=www.zoho.com')
  Searching results.
[*] Searching Certspotter.
[*] Searching Threatminer.
[*] Searching DGA.
[*] Searching Analytics.
An exception has occurred: Cannot connect to host www.baidu.com:443 ssl:ssl.SSLContext object at 0x7f7804f471c0 [Connection reset by peer]
[*] Searching Baidu.
An exception has occurred: B, 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 CIRCL.
[*] Searching NetworkMiner.
Google is blocking your IP and the workaround, returning
[*] Searching Sodinokibi.
  Searching 0 results.
[*] Searching Trillian.
[*] Searching DuckDuckGo.
Google is blocking your IP and the workaround, returning
  Searching 0 results.
An exception has occurred: Cannot connect to host des.bufferover.run:443 ssl:ssl.SSLContext object at 0x7f7804d8f040 [Name or service not known]
Google is blocking your IP and the workaround, returning
  Searching 0 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
AS12225
AS139808
AS141797
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=$2Pchats82F22431727558013100882zrc=fromproduct
https://www.zoho.com/cliq/?serviceurl=$2Findex.d06zsrc=fromproduct
https://www.zoho.com/contactus.html
```

```
File Actions Edit View Help
AS63949
[*] Interesting URLs Found: 25
https://www.zoho.com/
https://www.zoho.com/assistant/
https://www.zoho.com/leads/
https://www.zoho.com/campaigns/?src=fromproduct
https://www.zoho.com/campaigns/explainer/campaign-view.html
https://www.zoho.com/campaigns/explainer/zzend.html
https://www.zoho.com/campaigns/explainer/?src=fromproduct
https://www.zoho.com/crm/serviceurl=42Fchats%2F243172755001510000zsrc=fromproduct
https://www.zoho.com/crm/index.doczsrc=fromproduct
https://www.zoho.com/contactus.html
https://www.zoho.com/calculator/
https://www.zoho.com/crm/
https://www.zoho.com/crm/crmplus/
https://www.zoho.com/crm/
https://www.zoho.com/excellerator/
https://www.zoho.com/forms/
https://www.zoho.com/voice/?utm_source=200utm_medium=pdf
https://www.zoho.com/lead/
https://www.zoho.com/marketingautomation/
https://www.zoho.com/leads/
https://www.zoho.com/leadsplus/?src=zoho-home&amp;X3Bireft=phose
https://www.zoho.com/retail/
https://www.zoho.com/report-abuse/
https://www.zoho.com/salesiq/
https://www.zoho.com/survey/
```

[*] No Twitter users found.

[*] LinkedIn users found: 292

```
Asnil Muhammed - Regional Account Manager
Abhay 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
All Shabdar - Regional Director MEA
Alok Kumar Bharti - Software Engineer
Aman Gupta - Zoho Developer
Anamruth KR - Zoho Developer
Anil Moorthy - Product Manager and Co-Founder
Anandaraman Krishnan - Product Manager
Ananthu Subramanian - Engineer Trainee
Ananthu Nair - Product Engineer - Zoho Corporation
Andrew Mahoney - VP - Certified Computer Solutions
Andrew Bourne
Andrew Jusagh - Zoho Corporation
Andrew B A - Senior Member Of Technical Staff
Anupama Jayaram - Zoho Consultant
Anupita Gupta - Technical Writer
Anurajnd Natarajan - Zoho Corporation
Anurun Balachandran - Senior Product Marketing Manager
Anurun Neawan - Product Designer
Anurun Muralidharan - Product Marketer
Anvind Krishnamoorthy
Ashok Chakravarthi Nagarajan
Ashok Kumar
Ashwin P Sharma - Lead - Zoho CRM SME
Avanindh B - Software Developer - Zoho
Azamudeen R
Badril Narayan - Senior Technical Support Engineer
Bala Banesh
Bala Krishnan - Product Marketer
Bala Sunder - Member Technical Staff
Balaji Venkataswami
Balaji Jayaraman - Product Manager
Barath Kumar Narend - Member Leadership staff
Bashirul Haque Faisal - Zoho Consultant
Bernard Samuel - Zoho Developer
Bharath Kumar
Bharathi Ambazhagan - Member Technical Staff
Calvin Jasher - Quality Analyst- Zoho CRM Support
Carla Garcia
Chakravarthi Mudhukrishnan - Zoho Corporation
Chandru Jayapal - Zoho Corporation
Charles Lazro
Candan K - Zoho CRM Consultant - Regal Infonet
Chidirupaniam Nachiaappan - Senior Product Director
Chiranjeevi R - Director of Product Management
Cynthia A - Product Management
D Jayaram - Visual Designer
DEVENDRA KUSHWAHA - Zoho Developer
David Elkins - Head of Content Review
Deepak RV - Enterprise Support Engineer - Zoho
```

```
File Actions Edit View Help
root@kali: ~
[*] Interesting URLs Found: 25
Ajay Singh - Developer - ZOHO CRM
Akash Krishnan - Member Technical Staff
Akilan Marimuthu
Akshaya Chandrasekar - Zoho Corporation
All Shabdar - Regional Director MEA
Alok Kumar Bharti - Software Engineer
Aman Gupta - Zoho Developer
Anamruth KR - Zoho Developer
Anil Moorthy - Product Manager and Co-Founder
Anandaraman Krishnan - Product Manager
Ananthu Subramanian - Engineer Trainee
Ananthu Nair - Product Engineer - Zoho Corporation
Andrew Mahoney - VP - Certified Computer Solutions
Andrew Bourne
Andrew Jusagh - Zoho Corporation
Andrew B A - Senior Member Of Technical Staff
Anupama Jayaram - Zoho Consultant
Anupita Gupta - Technical Writer
Anurajnd Natarajan - Zoho Corporation
Anurun Balachandran - Senior Product Marketing Manager
Anurun Neawan - Product Designer
Anurun Muralidharan - Product Marketer
Anvind Krishnamoorthy
Ashok Chakravarthi Nagarajan
Ashok Kumar
Ashwin P Sharma - Lead - Zoho CRM SME
Avanindh B - Software Developer - Zoho
Azamudeen R
Badril Narayan - Senior Technical Support Engineer
Bala Banesh
Bala Krishnan - Product Marketer
Bala Sunder - Member Technical Staff
Balaji Venkataswami
Balaji Jayaraman - Product Manager
Barath Kumar Narend - Member Leadership staff
Bashirul Haque Faisal - Zoho Consultant
Bernard Samuel - Zoho Developer
Bharath Kumar
Bharathi Ambazhagan - Member Technical Staff
Calvin Jasher - Quality Analyst- Zoho CRM Support
Carla Garcia
Chakravarthi Mudhukrishnan - Zoho Corporation
Chandru Jayapal - Zoho Corporation
Charles Lazro
Candan K - Zoho CRM Consultant - Regal Infonet
Chidirupaniam Nachiaappan - Senior Product Director
Chiranjeevi R - Director of Product Management
Cynthia A - Product Management
D Jayaram - Visual Designer
DEVENDRA KUSHWAHA - Zoho Developer
David Elkins - Head of Content Review
Deepak RV - Enterprise Support Engineer - Zoho
```

```
File Actions Edit View Help
Vijayaraghavan venugopal
Vinodraj Thiagarajan
Vineethkumar 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 R - Developer - Zoho Corporation
Chennakrishna S - Zoho Developer
Nagarajan Ramesh - Account Manager - Zoho
Sathiyam Sathiyamurthy - Zoho - Zoho Corporation
Shakir Afrreen Taj - Senior Technical Support Engineer
Vasudevanan T - Lead
Working as a Senior executive at IndiGo Airlines

[*] LinkedIn Links Found: 0
Anil Mohamed - Regional Account Manager
Abbas Abu - Zoho One Developer
Abhilash Reddy Gottihala
Adarsh Pandey - Member of Technical Staff
Adithyan Ravichandar - Lead System Engineer
Alay George - Partner Support Engineer - Zoho
Alay Singh - Developer - Zoho CRM
Akash Krishnan - Member Technical Staff
Akilan Marimuthu
Akshaya Chandrasekar - Zoho Corporation
All Shabdar - Regional Director MEA
Atoli Kumar Bharti - Software Engineer
Anan Gupta - Zoho Developer
Ananthu KR - Zoho Developer
Anil Moorthy - Product Manager and Co-Founder
Anandarajan Krishnan - Product Manager
Anantha Subramanian - 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
Anudhav Pandey - Zoho Consultant
Anumita Gupta - Technical Writer
Aravind Natarajan - Zoho Corporation
Arini Balachandran - Senior Product Marketing Manager
Arini Kesavan - Product Designer
Aruna Muralidharan - Product Marketer
Arvind Krishnamoorthy
Ashok Chakravarthi Nagarajan
```

```
File Actions Edit View Help
Vineethkumar 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
Chennakrishna S - Zoho Developer
Nagarajan Ramesh - Account Manager - Zoho
Sathiyam Sathiyamurthy - Zoho - Zoho Corporation
Shakir Afrreen Taj - Senior Technical Support Engineer
Vasudevanan T - Lead
Working as a Senior executive at IndiGo Airlines

[*] Trello URLs Found: 33
https://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/299e0997a8f127d2af4bf4
https://trello.com/power-ups/29a11aa2922a254295006025/zoho-crm
https://trello.com/power-ups/3b55d578cc75f290fd677/automate
https://trello.com/power-ups/3ba27bdc058ada095eadc98
https://trello.com/power-ups/3ba27bdc058ada095eadc98/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/urging
https://trello.com/teams/support
https://trello.com/templates
https://trello.com/templates/design
https://trello.com/templates/design/design-system-checklist-yn5vfm
https://trello.com/templates/design/freelance-branding-project-zm66haj
https://trello.com/templates/design/research-iteration-0tqgmxz
https://trello.com/templates/product-management
https://trello.com/templates/product-management/3-étapes-de-gestionnement-des-produits-78avmzv
https://trello.com/templates/product-management/3-listes-pour-la-gestion-des-produits-0lufy07
https://trello.com/templates/product-management/balayage-de-luminalidades-sncwqjtg
https://trello.com/templates/product-management/planification-de-projet-myph
https://trello.com/templates/product-management/fabrication-planification-v923
https://trello.com/templates/product-management/product-roadmap-template-frhajbh
https://trello.com/templates/product-management/roadmap-produit-9d1jblr
https://trello.com/templates/product-management/roadmap-produit-9d1jblr
https://trello.com/templates/product-management/shipping-planner-mcv7vte
https://trello.com/tour
https://trello.com/use-cases/crm
```

```
File Actions Edit View Help
https://trello.com/use-cases/crm
https://www.trello.com/
[*] IPs found: 69
8.39.54.155
8.40.222.155
74.203.04.81
74.203.112.181
74.203.112.188
74.203.113.118
74.203.113.176
74.203.113.203
74.203.155.201
89.36.178.52
103.128.128.96
103.169.152.75
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
137.20.43.154
136.143.182.155
136.143.198.58
136.143.198.79
136.143.198.155
136.143.198.156
136.143.191.284
165.173.187.32
165.254.167.165
165.254.168.165
178.79.172.185
185.20.289.52
204.141.32.155
204.141.42.155
204.141.42.156
204.141.43.284
236.52.72.155
2a06:98c1:3120::4
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)

```
[*] IP Address: 192.168.1.111
[*] ASNs Found: 1
AS56353
[*] Interesting URLs Found: 1
https://www.savveetha.com/
[*] LinkedIn Links Found: 0
[*] TPs Found: 4
118.139.175.1
198.185.159.144
199.34.228.77
[*] Emails Found: 27
admin@msavveetha.com
admin@officer@savveetha.com
admission.medical@savveetha.com
admission.scott@savveetha.com
admission.scrub@savveetha.com
admission.sex1@savveetha.com
admission@savveetha.com
artsadmission@savveetha.com
asso.dean@faculty@savveetha.com
dean.ssm@savveetha.com
enggadmission@savveetha.com
hr.smc@savveetha.com
hr.smc1.1@savveetha.com
pmmed@savveetha.com
principal.ash@savveetha.com
principal.scott@savveetha.com
ssuadmission@savveetha.com
schoolofhospitality@savveetha.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 6 - Open Source Intelligence Gathering Using OSRFramework

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

Procedure:

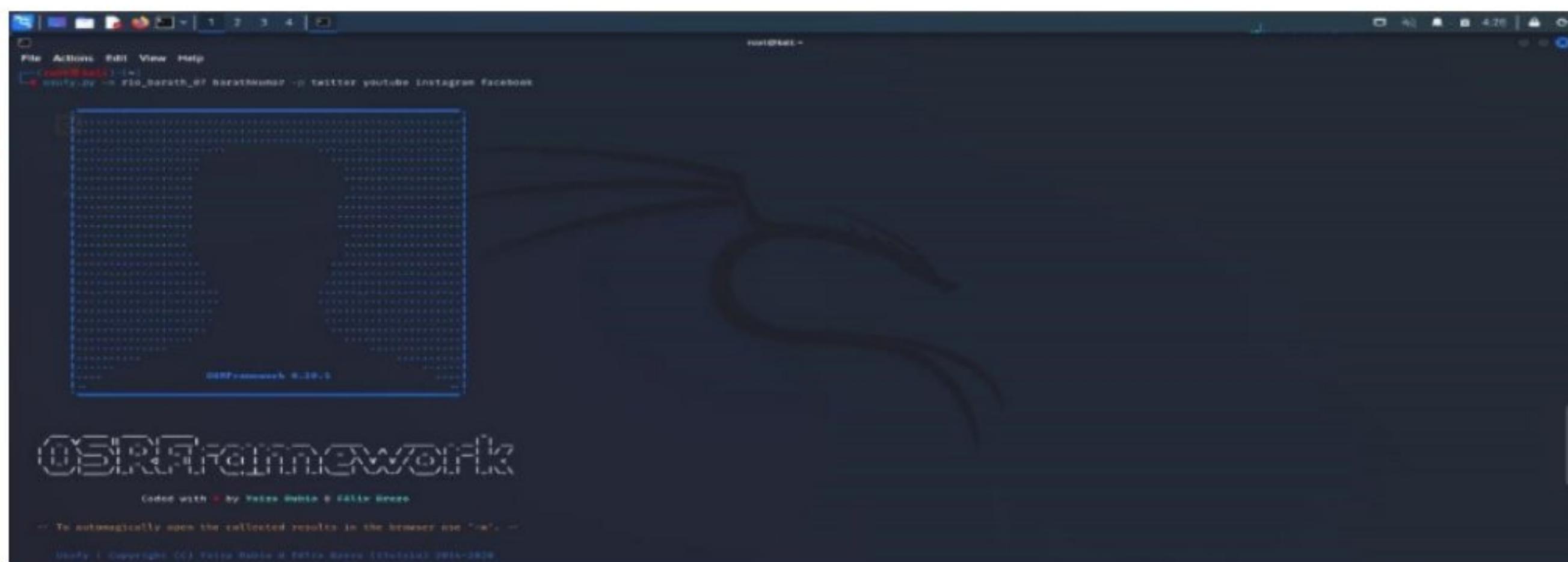
Step 1: Log into kali linux machine

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

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

Command:

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



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

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

```

root@i3visio-OptiPlex-5090:~/Desktop$ ./searchfy.py -q "i3visio"
2022-09-16 04:25:35.232993  Starting search in 4 platforms(s) ... Ready!
Please <Ctrl + C> to stop...
2022-09-16 04:25:41.921029  results obtained (4):
/usr/lib/python3/dist-packages/pymysql/depcreact.py:208: UserWarning: Deprecated usage since v0.2.1! Explicit import is no longer required, pymysql.cursors is auto imported.
warnings.warn("Objects recovered (2022-9-16, 04:25:41.921029).")
+-----+-----+-----+
| i3visio.uri | i3visio.alias | i3visio.platform |
+-----+-----+-----+
| https://www.youtube.com/user/rie_barath_07/about | rie_barath_07 | YouTube |
| https://www.facebook.com/rie_barath_07 | rie_barath_07 | Facebook |
| https://www.instagram.com/rie_barath_07 | rie_barath_07 | Instagram |
| https://twitter.com/rie_barath_07 | rie_barath_07 | Twitter |
| https://www.youtube.com/user/barathkumar/about | barathkumar | YouTube |
| https://www.facebook.com/barathkumar | barathkumar | Facebook |
| https://www.instagram.com/barathkumar | barathkumar | Instagram |
| https://twitter.com/barathkumar | barathkumar | Twitter |
+-----+-----+-----+
2022-09-16 04:25:41.998991  You can find all the information here: ./profiles.csv
2022-09-16 04:25:41.998991  Finishing execution...
Total time consumed: 0:00:05.184975
Message seconds/query: 1.2448873 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/i3visio-framework/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)

Result:

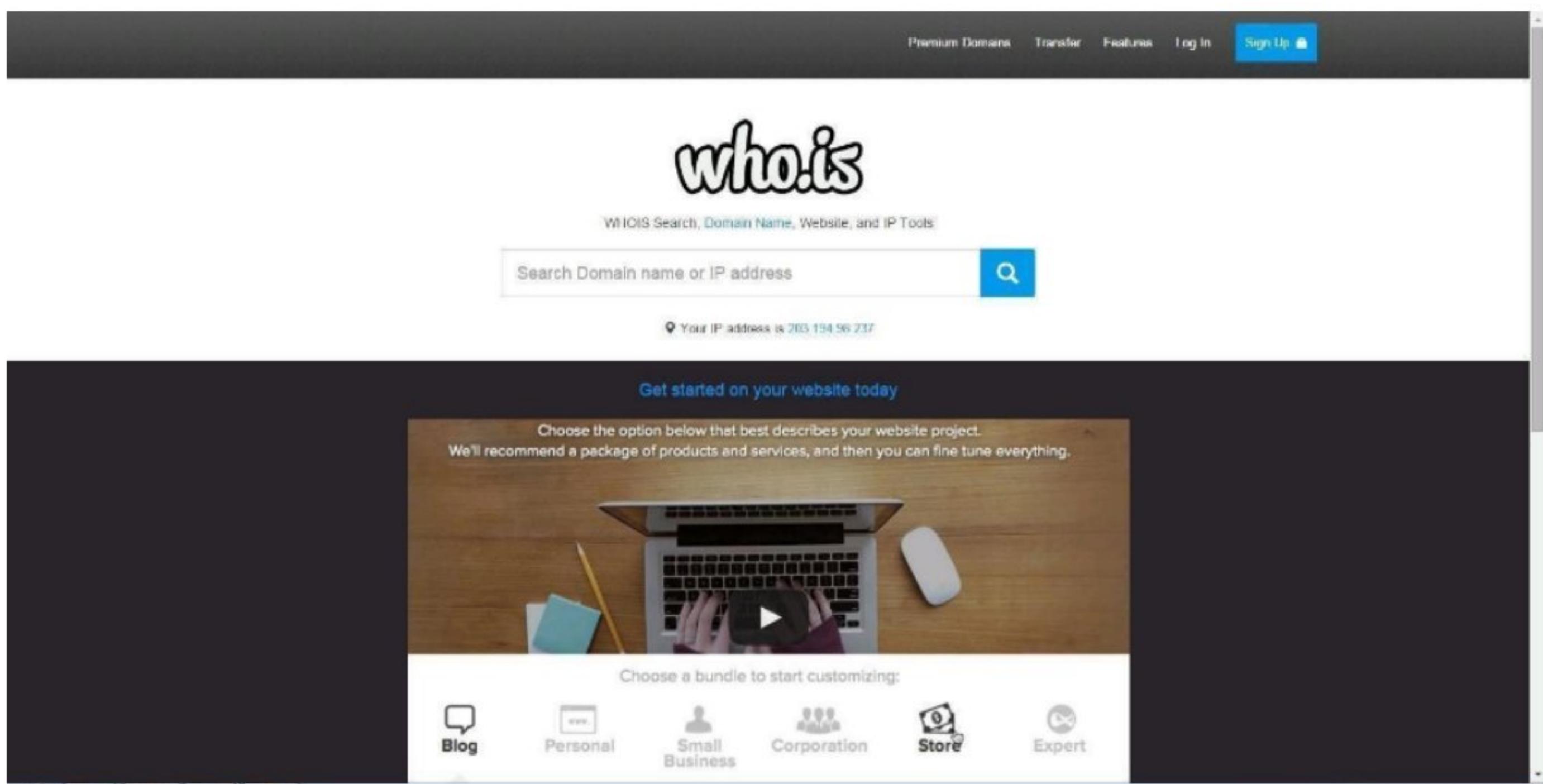
2)

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 7: Use Google and Whois for Reconnaissance.

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

Step1: Open the WHO.is website



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

who.is

Search for domains or IP addresses...

Premium Domains Transfer Features Login Sign Up

Taken Taken Taken Available Taken Available Available

Purchase Selected Domains

saveetha.com

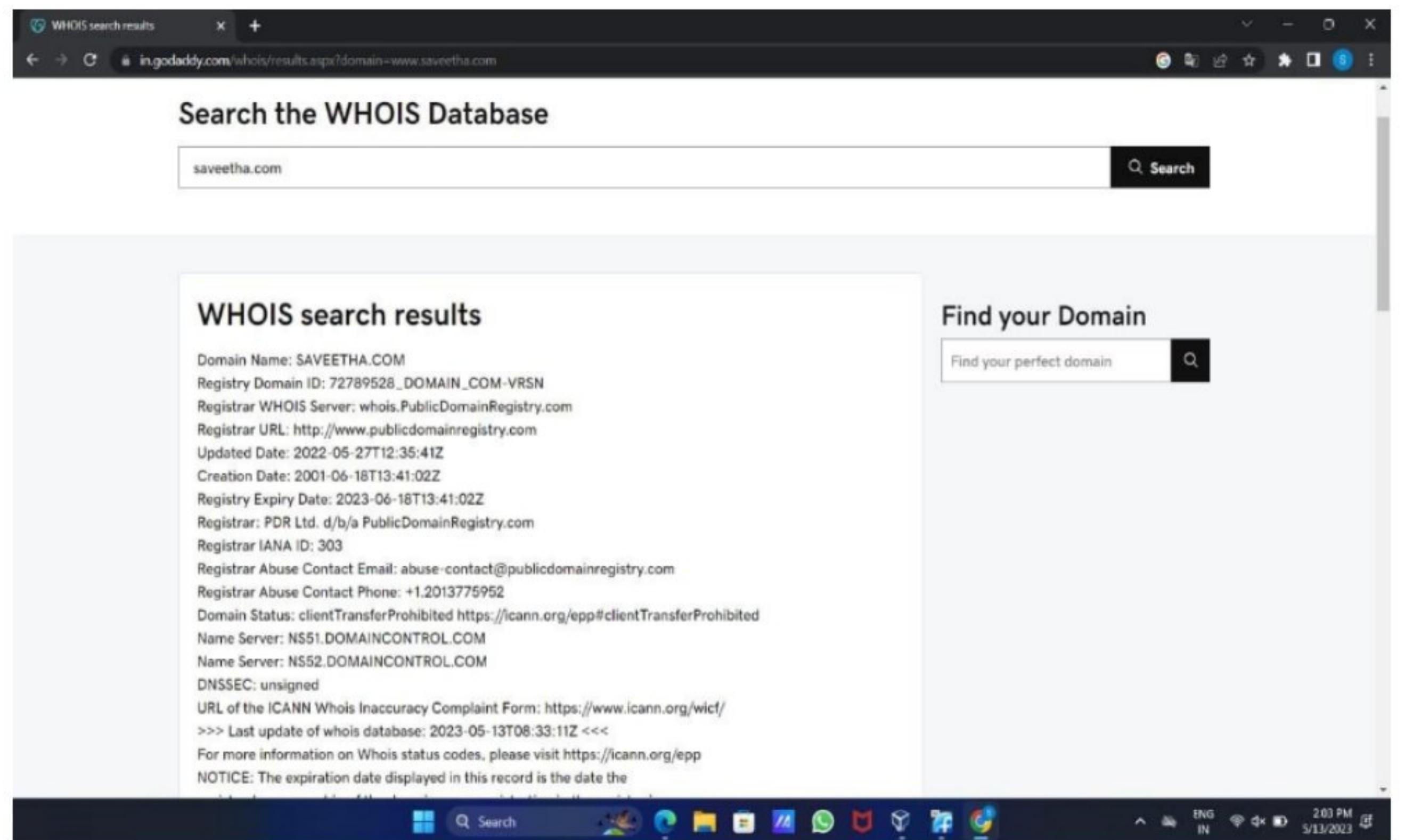
DNS Information

Whois DNS Records Diagnostics

DNS Records for saveetha.com

Hostname	Type	TTL	Priority	Content
saveetha.com	A	3600		198.185.159.144
ns1	NS			ns1.name.com
ns2	NS			ns2.name.com
ns3	NS			ns3.name.com
ns4	NS			ns4.name.com
ns5	NS			ns5.name.com
ns6	NS			ns6.name.com
ns7	NS			ns7.name.com
ns8	NS			ns8.name.com
ns9	NS			ns9.name.com
ns10	NS			ns10.name.com
ns11	NS			ns11.name.com
ns12	NS			ns12.name.com
ns13	NS			ns13.name.com
ns14	NS			ns14.name.com
ns15	NS			ns15.name.com
ns16	NS			ns16.name.com
ns17	NS			ns17.name.com
ns18	NS			ns18.name.com
ns19	NS			ns19.name.com
ns20	NS			ns20.name.com
ns21	NS			ns21.name.com
ns22	NS			ns22.name.com
ns23	NS			ns23.name.com
ns24	NS			ns24.name.com
ns25	NS			ns25.name.com
ns26	NS			ns26.name.com
ns27	NS			ns27.name.com
ns28	NS			ns28.name.com
ns29	NS			ns29.name.com
ns30	NS			ns30.name.com
ns31	NS			ns31.name.com
ns32	NS			ns32.name.com
ns33	NS			ns33.name.com
ns34	NS			ns34.name.com
ns35	NS			ns35.name.com
ns36	NS			ns36.name.com
ns37	NS			ns37.name.com
ns38	NS			ns38.name.com
ns39	NS			ns39.name.com
ns40	NS			ns40.name.com
ns41	NS			ns41.name.com
ns42	NS			ns42.name.com
ns43	NS			ns43.name.com
ns44	NS			ns44.name.com
ns45	NS			ns45.name.com
ns46	NS			ns46.name.com
ns47	NS			ns47.name.com
ns48	NS			ns48.name.com
ns49	NS			ns49.name.com
ns50	NS			ns50.name.com
ns51	NS			ns51.name.com
ns52	NS			ns52.name.com
ns53	NS			ns53.name.com
ns54	NS			ns54.name.com
ns55	NS			ns55.name.com
ns56	NS			ns56.name.com
ns57	NS			ns57.name.com
ns58	NS			ns58.name.com
ns59	NS			ns59.name.com
ns60	NS			ns60.name.com
ns61	NS			ns61.name.com
ns62	NS			ns62.name.com
ns63	NS			ns63.name.com
ns64	NS			ns64.name.com
ns65	NS			ns65.name.com
ns66	NS			ns66.name.com
ns67	NS			ns67.name.com
ns68	NS			ns68.name.com
ns69	NS			ns69.name.com
ns70	NS			ns70.name.com
ns71	NS			ns71.name.com
ns72	NS			ns72.name.com
ns73	NS			ns73.name.com
ns74	NS			ns74.name.com
ns75	NS			ns75.name.com
ns76	NS			ns76.name.com
ns77	NS			ns77.name.com
ns78	NS			ns78.name.com
ns79	NS			ns79.name.com
ns80	NS			ns80.name.com
ns81	NS			ns81.name.com
ns82	NS			ns82.name.com
ns83	NS			ns83.name.com
ns84	NS			ns84.name.com
ns85	NS			ns85.name.com
ns86	NS			ns86.name.com
ns87	NS			ns87.name.com
ns88	NS			ns88.name.com
ns89	NS			ns89.name.com
ns90	NS			ns90.name.com
ns91	NS			ns91.name.com
ns92	NS			ns92.name.com
ns93	NS			ns93.name.com
ns94	NS			ns94.name.com
ns95	NS			ns95.name.com
ns96	NS			ns96.name.com
ns97	NS			ns97.name.com
ns98	NS			ns98.name.com
ns99	NS			ns99.name.com
ns100	NS			ns100.name.com
ns101	NS			ns101.name.com
ns102	NS			ns102.name.com
ns103	NS			ns103.name.com
ns104	NS			ns104.name.com
ns105	NS			ns105.name.com
ns106	NS			ns106.name.com
ns107	NS			ns107.name.com
ns108	NS			ns108.name.com
ns109	NS			ns109.name.com
ns110	NS			ns110.name.com
ns111	NS			ns111.name.com
ns112	NS			ns112.name.com
ns113	NS			ns113.name.com
ns114	NS			ns114.name.com
ns115	NS			ns115.name.com
ns116	NS			ns116.name.com
ns117	NS			ns117.name.com
ns118	NS			ns118.name.com
ns119	NS			ns119.name.com
ns120	NS			ns120.name.com
ns121	NS			ns121.name.com
ns122	NS			ns122.name.com
ns123	NS			ns123.name.com
ns124	NS			ns124.name.com
ns125	NS			ns125.name.com
ns126	NS			ns126.name.com
ns127	NS			ns127.name.com
ns128	NS			ns128.name.com
ns129	NS			ns129.name.com
ns130	NS			ns130.name.com
ns131	NS			ns131.name.com
ns132	NS			ns132.name.com
ns133	NS			ns133.name.com
ns134	NS			ns134.name.com
ns135	NS			ns135.name.com
ns136	NS			ns136.name.com
ns137	NS			ns137.name.com
ns138	NS			ns138.name.com
ns139	NS			ns139.name.com
ns140	NS			ns140.name.com
ns141	NS			ns141.name.com
ns142	NS			ns142.name.com
ns143	NS			ns143.name.com
ns144	NS			ns144.name.com
ns145	NS			ns145.name.com
ns146	NS			ns146.name.com
ns147	NS			ns147.name.com
ns148	NS			ns148.name.com
ns149	NS			ns149.name.com
ns150	NS			ns150.name.com
ns151	NS			ns151.name.com
ns152	NS			ns152.name.com
ns153	NS			ns153.name.com
ns154	NS			ns154.name.com
ns155	NS			ns155.name.com
ns156	NS			ns156.name.com
ns157	NS			ns157.name.com
ns158	NS			ns158.name.com
ns159	NS			ns159.name.com
ns160	NS			ns160.name.com
ns161	NS			ns161.name.com
ns162	NS			ns162.name.com
ns163	NS			ns163.name.com
ns164	NS			ns164.name.com
ns165	NS			ns165.name.com
ns166	NS			ns166.name.com
ns167	NS			ns167.name.com
ns168	NS			ns168.name.com
ns169	NS			ns169.name.com
ns170	NS			ns170.name.com
ns171	NS			ns171.name.com
ns172	NS			ns172.name.com
ns173	NS			ns173.name.com
ns174	NS			ns174.name.com
ns175	NS			ns175.name.com
ns176	NS			ns176.name.com
ns177	NS			ns177.name.com
ns178	NS			ns178.name.com
ns179	NS			ns179.name.com
ns180	NS			ns180.name.com
ns181	NS			ns181.name.com
ns182	NS			ns182.name.com
ns183	NS			ns183.name.com
ns184	NS			ns184.name.com
ns185	NS			ns185.name.com
ns186	NS			ns186.name.com
ns187	NS			ns187.name.com
ns188	NS			ns188.name.com
ns189	NS			ns189.name.com
ns190	NS			ns190.name.com
ns191	NS			ns191.name.com
ns192	NS			ns192.name.com
ns193	NS			ns193.name.com
ns194	NS			ns194.name.com
ns195	NS			ns195.name.com
ns196	NS			ns196.name.com
ns197	NS			ns197.name.com
ns198	NS			ns198.name.com
ns199	NS			ns199.name.com
ns200	NS			ns200.name.com
ns201	NS			ns201.name.com
ns202	NS			ns202.name.com
ns203	NS			ns203.name.com
ns2				

OUTPUT:



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 8: TraceRoute, ping, ifconfig, ipconfig, netstat

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

Procedure:

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

```
suse1:~ # 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)

```
Tracing route to saveetha.com [192.168.150.145]
over a maximum of 30 hops:
  1  *        0 ms    0 ms    0 ms  192.168.150.10
  2  *        514 ms    620 ms  192.160.20.10
  3  *        *        *        Request timed out.
  4  *        1012 ms    293 ms  192.160.31.24
  5  XXX  ms    XXX ms    XXX ms  192.168.31.27
  6  *        *        *        Request timed out.
  7  *        *        *        Request timed out.
  8  *        *        *        Request timed out.
  9  XXX  ms    *        *        192.70.248.228
  10  275 ms    266 ms    *        206-0-150-0.deploy.static.akamaitechnologies.com [206.0.150.0]
  11  *        *        *        Request timed out
  12  *        *        1287 ms  192.160.150.145

Trace complete.
```

2)

```

Pinging 192.168.53.42 with 32 bytes of data:
Request timed out.
Reply from 192.168.53.42: bytes=32 time=1500ms TTL=64
Reply from 192.168.53.42: bytes=32 time=30ms TTL=64

Ping statistics for 192.168.53.42:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milliseconds:
        Minimum = 30ms, Maximum = 1500ms, Average = 530ms

```

3)

Active Connections

Proto	Local Address	Foreign Address	State
TCP	127.0.0.1:49674	LAPTOP-0400I8EB:49676	ESTABLISHED
TCP	127.0.0.1:49676	LAPTOP-0400I8EB:49674	ESTABLISHED
TCP	192.168.53.109:49409	20.198.119.84:https	ESTABLISHED
TCP	192.168.53.109:58125	20.198.119.84:https	ESTABLISHED
TCP	192.168.53.109:59567	a23-215-215-241:https	CLOSE_WAIT
TCP	192.168.53.109:59568	a23-215-215-241:https	CLOSE_WAIT
TCP	192.168.53.109:59569	a23-215-215-241:https	CLOSE_WAIT
TCP	192.168.53.109:59570	a23-215-215-241:https	CLOSE_WAIT
TCP	192.168.53.109:59572	a-0001:https	ESTABLISHED
TCP	192.168.53.109:59576	a-0001:https	ESTABLISHED
TCP	[2401:4900:6297:efe5:9872:41f9:7f06:fa55]:59595	[2001:1900:2381:4::1fe]:http	ESTABLISHED
TCP	[2401:4900:6297:efe5:9872:41f9:7f06:fa55]:59598	[2001:1900:2381:d01::1fe]:http	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.

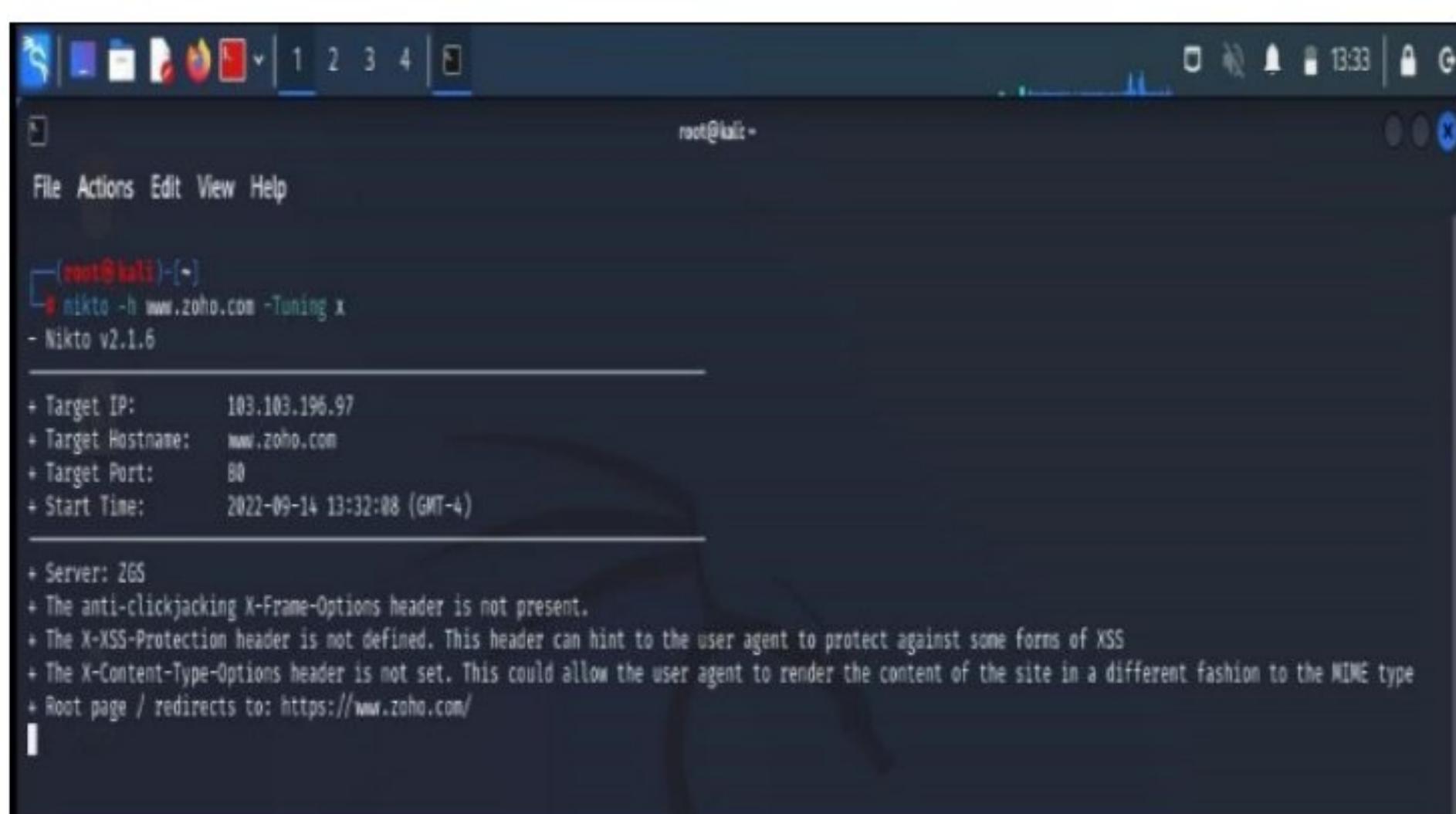
Exercise No 9:VULNERABILITY ANALYSIS - CGI Scanning with Nikto

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



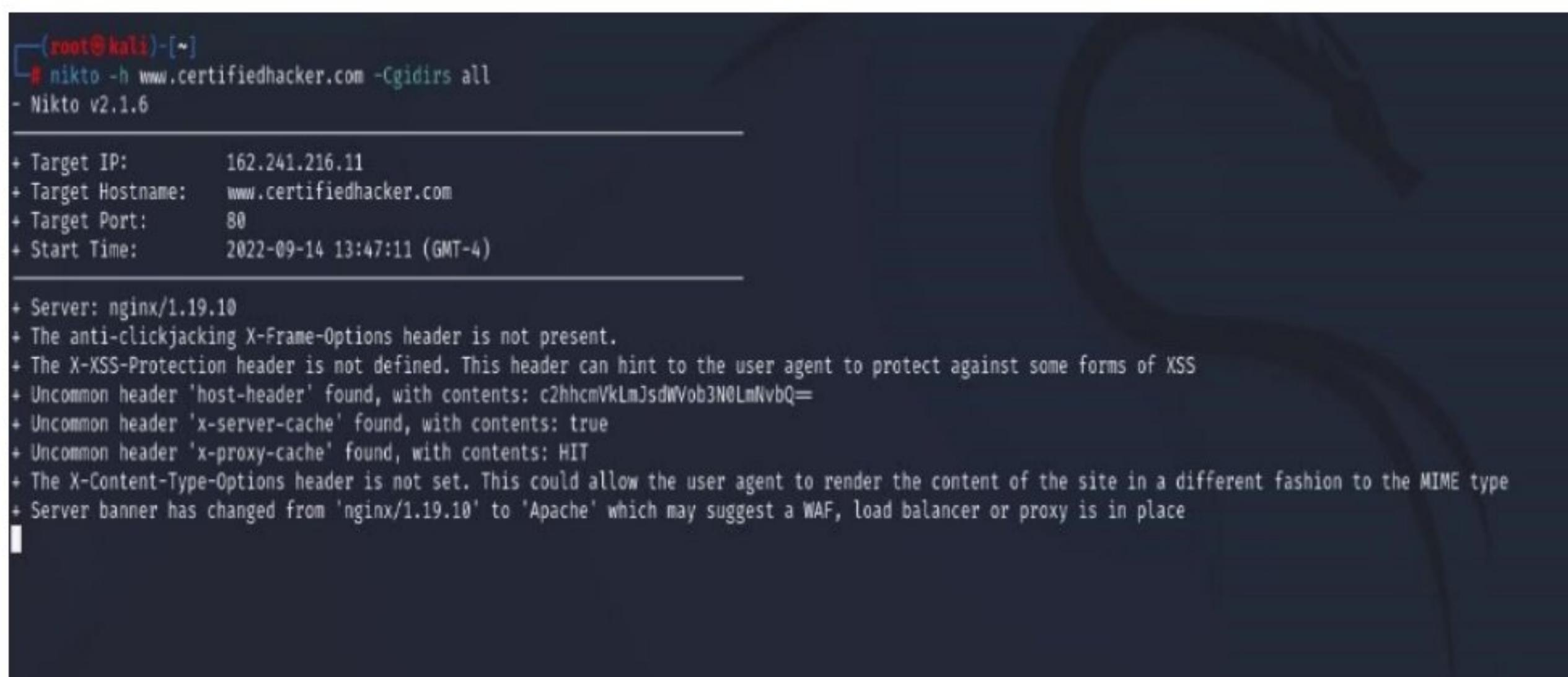
```
(root㉿kali)-[~]
# nikto -h www.zoho.com -Tuning x
- Nikto v2.1.6

+ 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

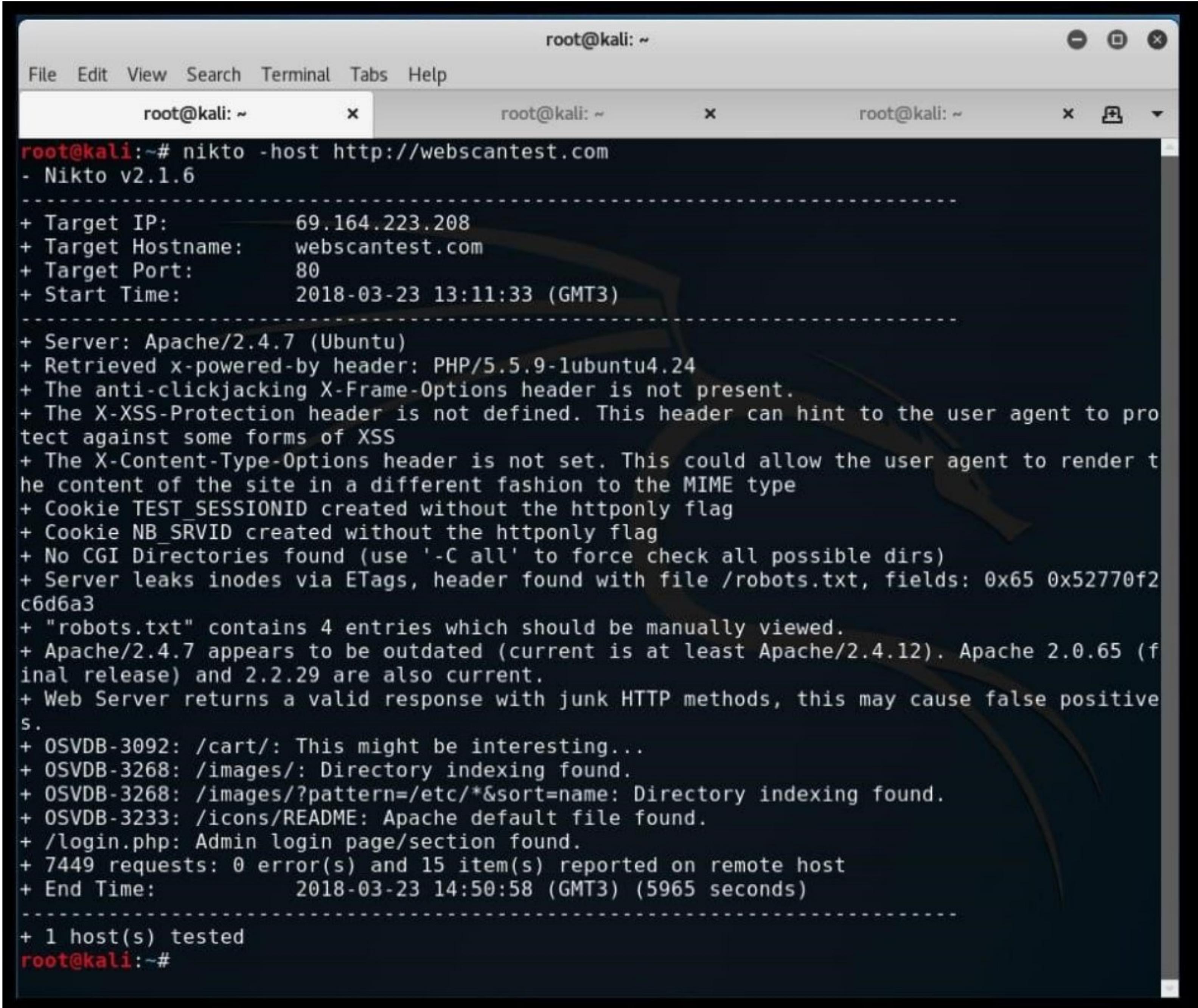
+ Target IP:      162.241.216.11
+ Target Hostname: www.certifiedhacker.com
+ Target Port:    80
+ Start Time:    2022-09-14 13:47:11 (GMT-4)

+ 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: c2hhcmVLMj5dWVob3N0LmNvbQ=
+ 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 webserver and list out the directories

Output:

1)



root@kali: ~

File Edit View Search Terminal Tabs Help

root@kali: ~ x root@kali: ~ x root@kali: ~ x

```
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 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
+ 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 (final 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:

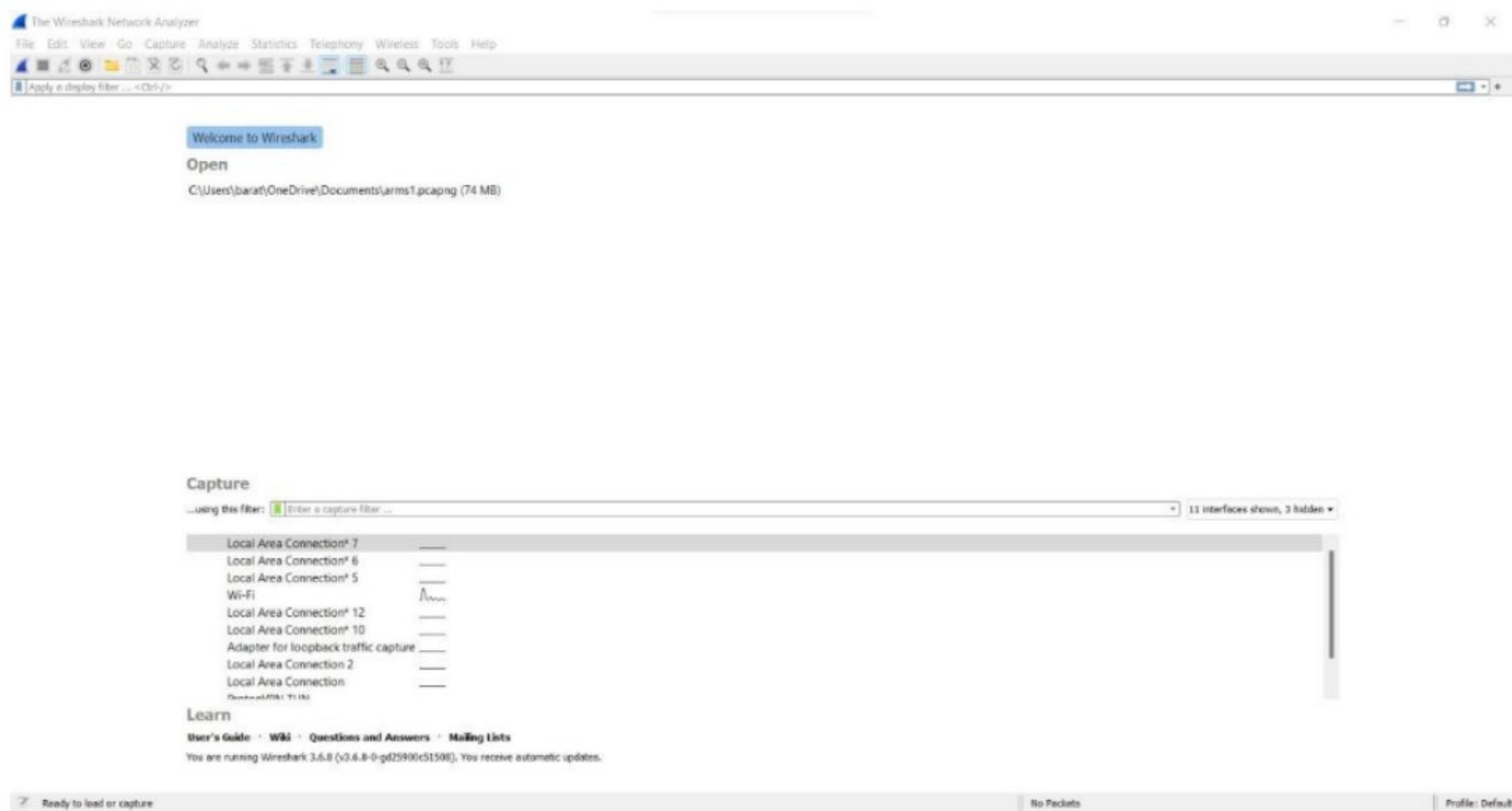
The above experiment is about VULNERABILITY ANALYSIS - CGI Scanning with Nikto. We can retrieve information like server name, headers and etc. This is done in root terminal using kali linux OS.

Exercise No 10: Wireshark sniffer

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

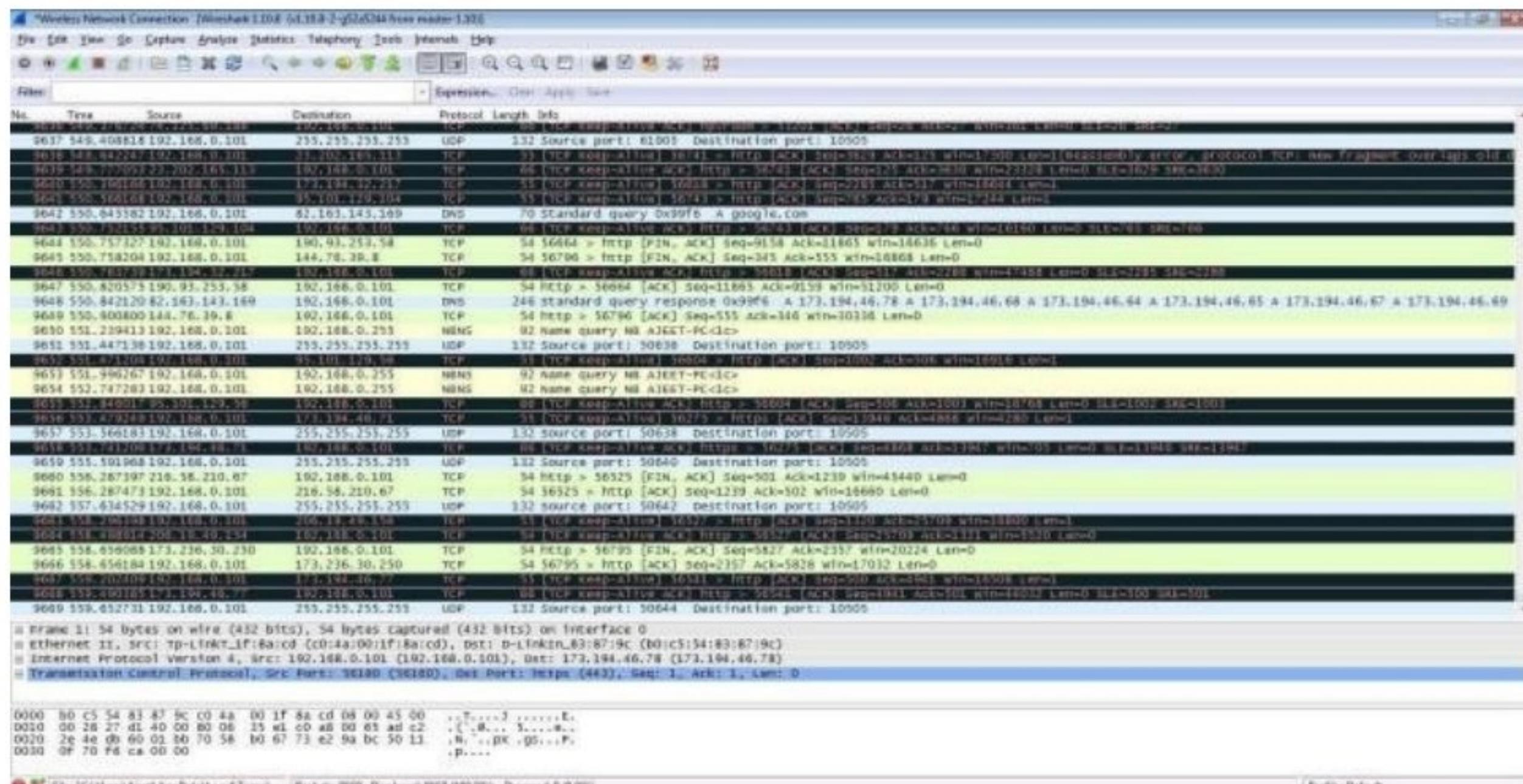
Procedure:

Step 1: Install and open Wireshark .



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

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



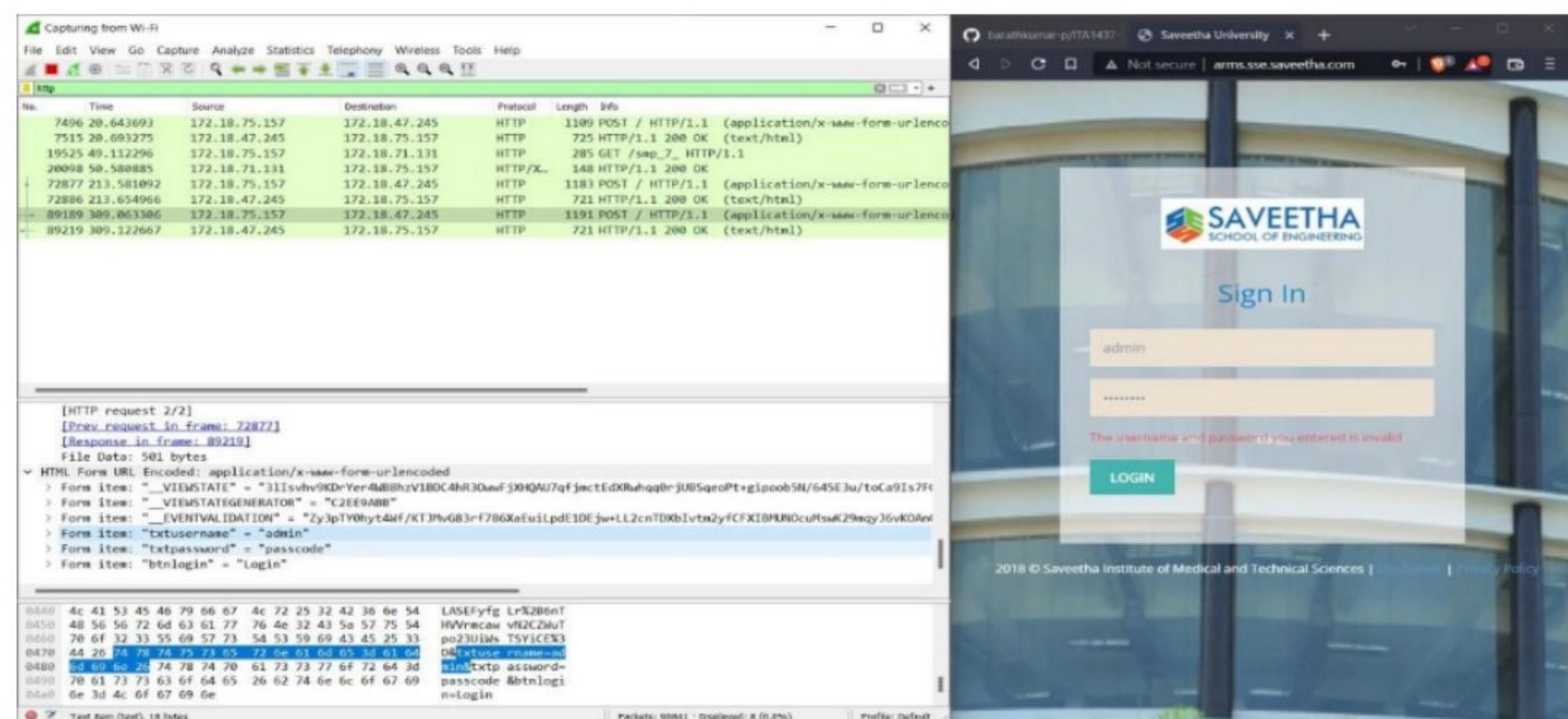
Step 4: Open a website in a new window and enter the user id and password. Register if needed.

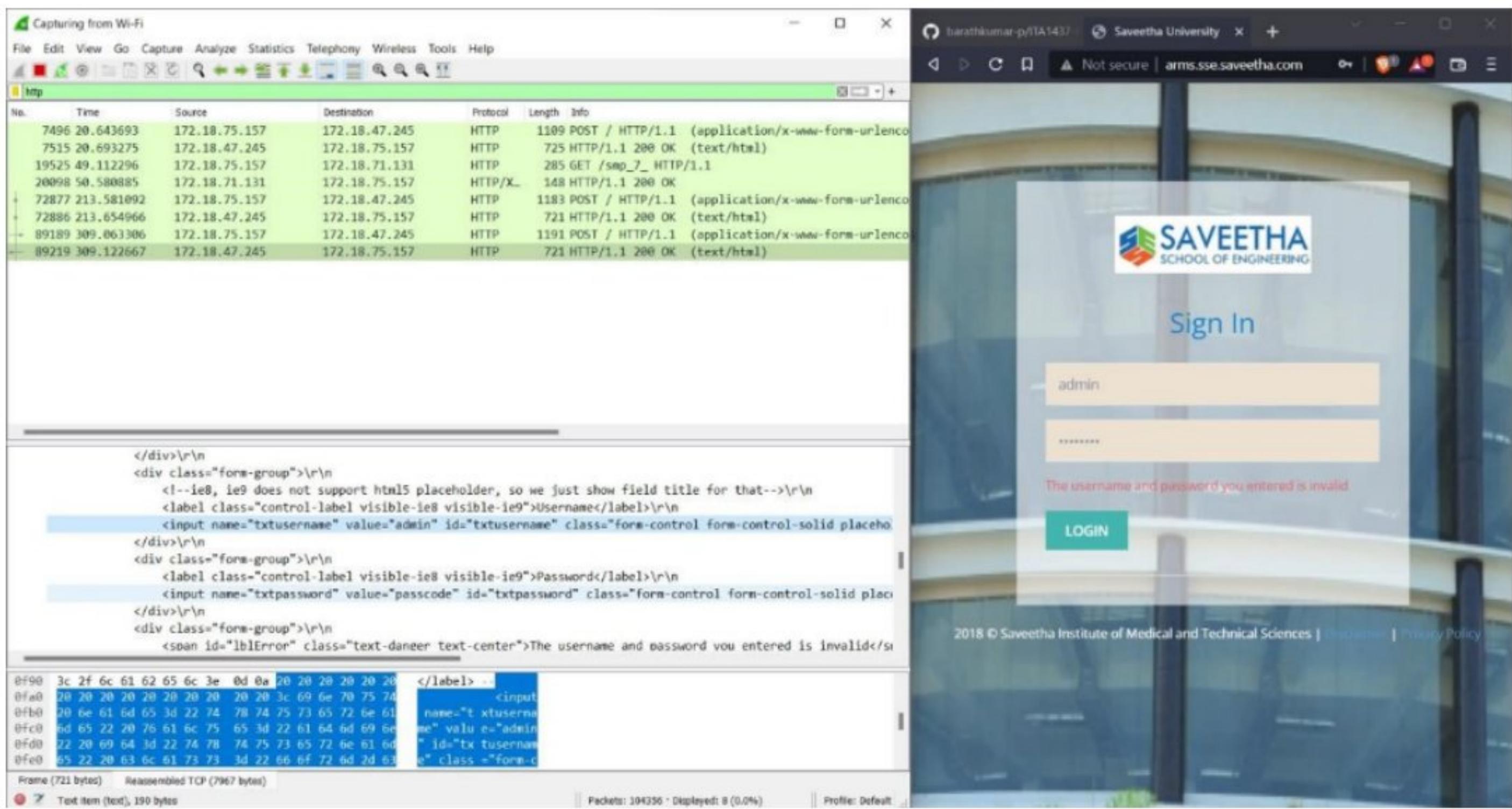
Step 5: Enter the credentials and then sign in

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

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

apply. Step 9: Now stop the tool to stop recording



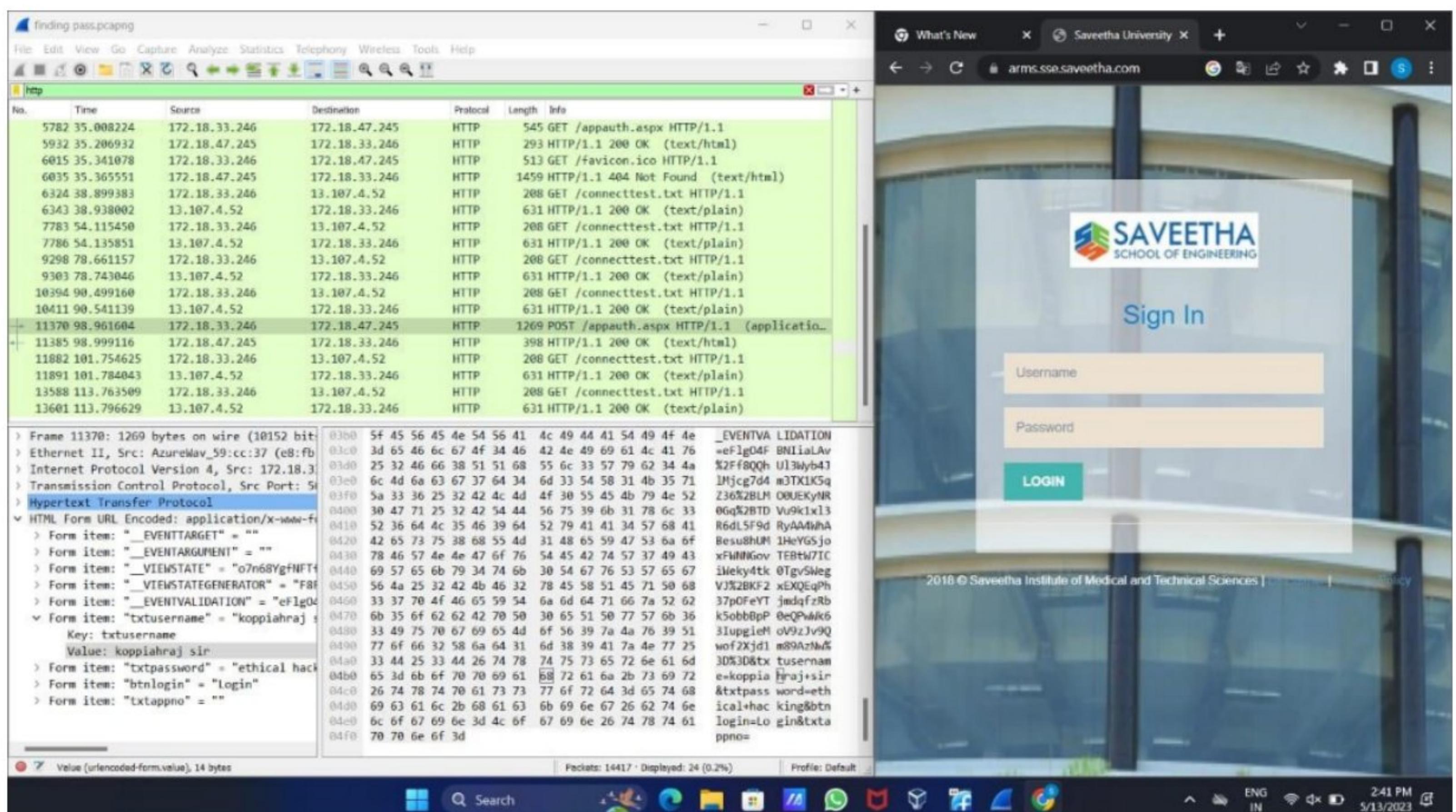


Step 10: Find the post methods for username and passwords

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

Output:

1)



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.