

ITA1471

ETHICAL HACKING FOR NETWORK HACKING



B. Siva sai kumar

192211164

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 -Pn 192.168.1.1
-sn	only host discover	nmap -sn 192.168.1.1
-PR	arp discovery on a local network	nmap -PR 192.168.1.1
-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:

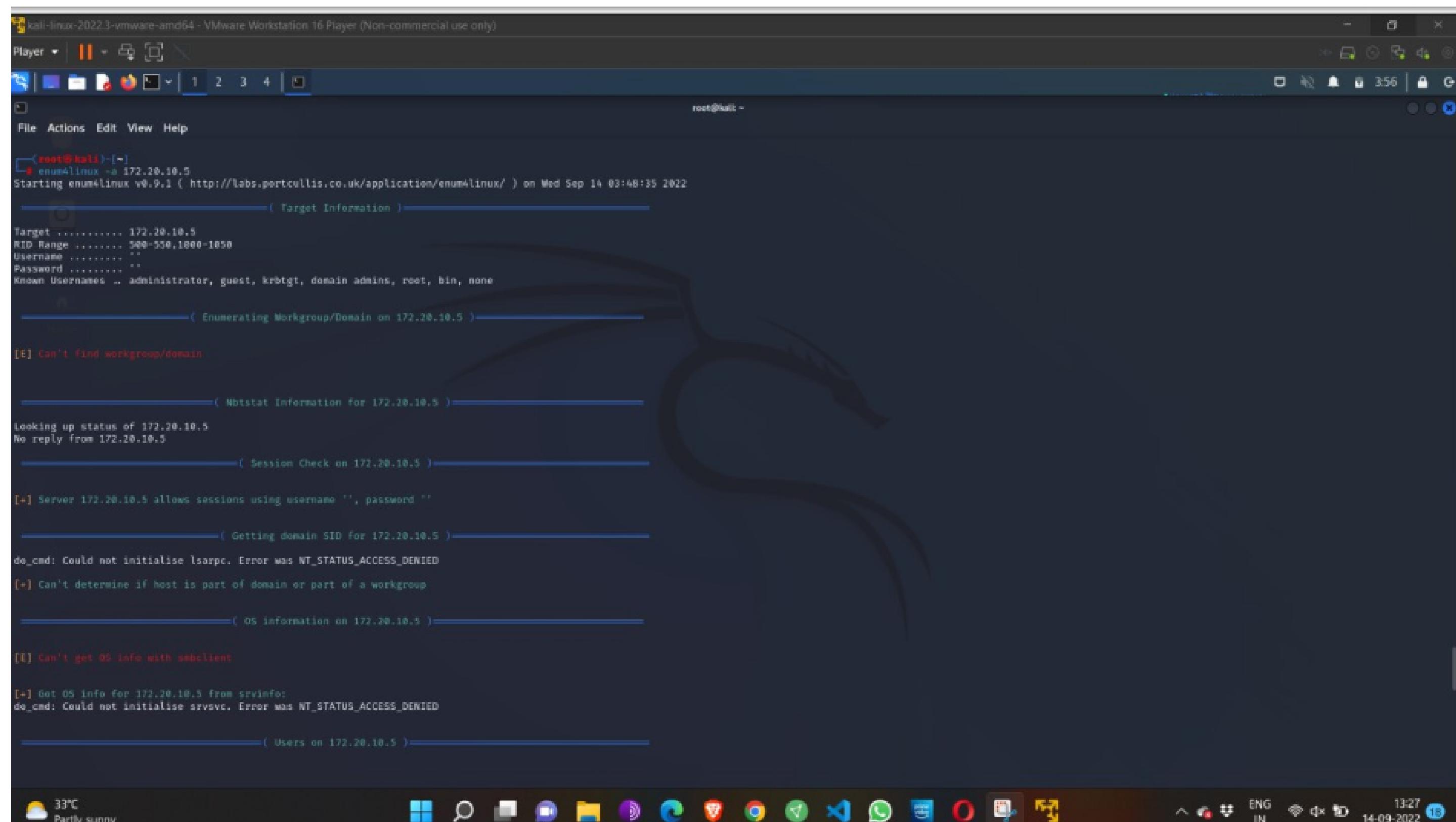
- Kali linux running as an attacker machine
- Windows 7 running as virtual machine

• 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 -v -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

7)

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



```
[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 ..... 500-550,1800-1850
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

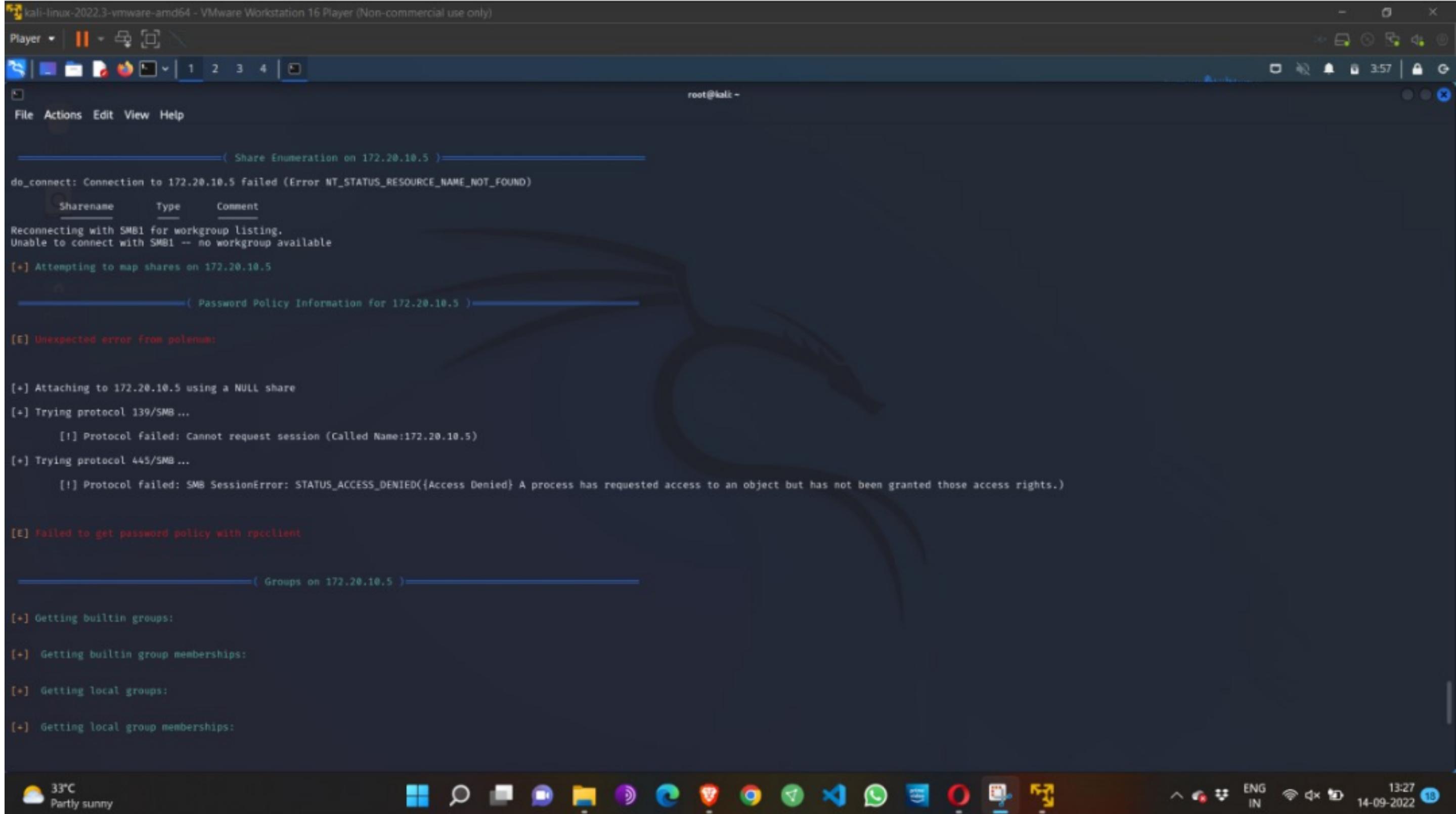
[+] Nbtstat Information for 172.20.10.5
Looking up status of 172.20.10.5
No reply from 172.20.10.5

[+] 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
[!] Can't get OS info with smbclient
[+] Got OS info for 172.20.10.5 from srvinf0:
do_cmd: Could not initialise svrsvc. Error was NT_STATUS_ACCESS_DENIED

[+] Users on 172.20.10.5
```

8) 

```
( 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:

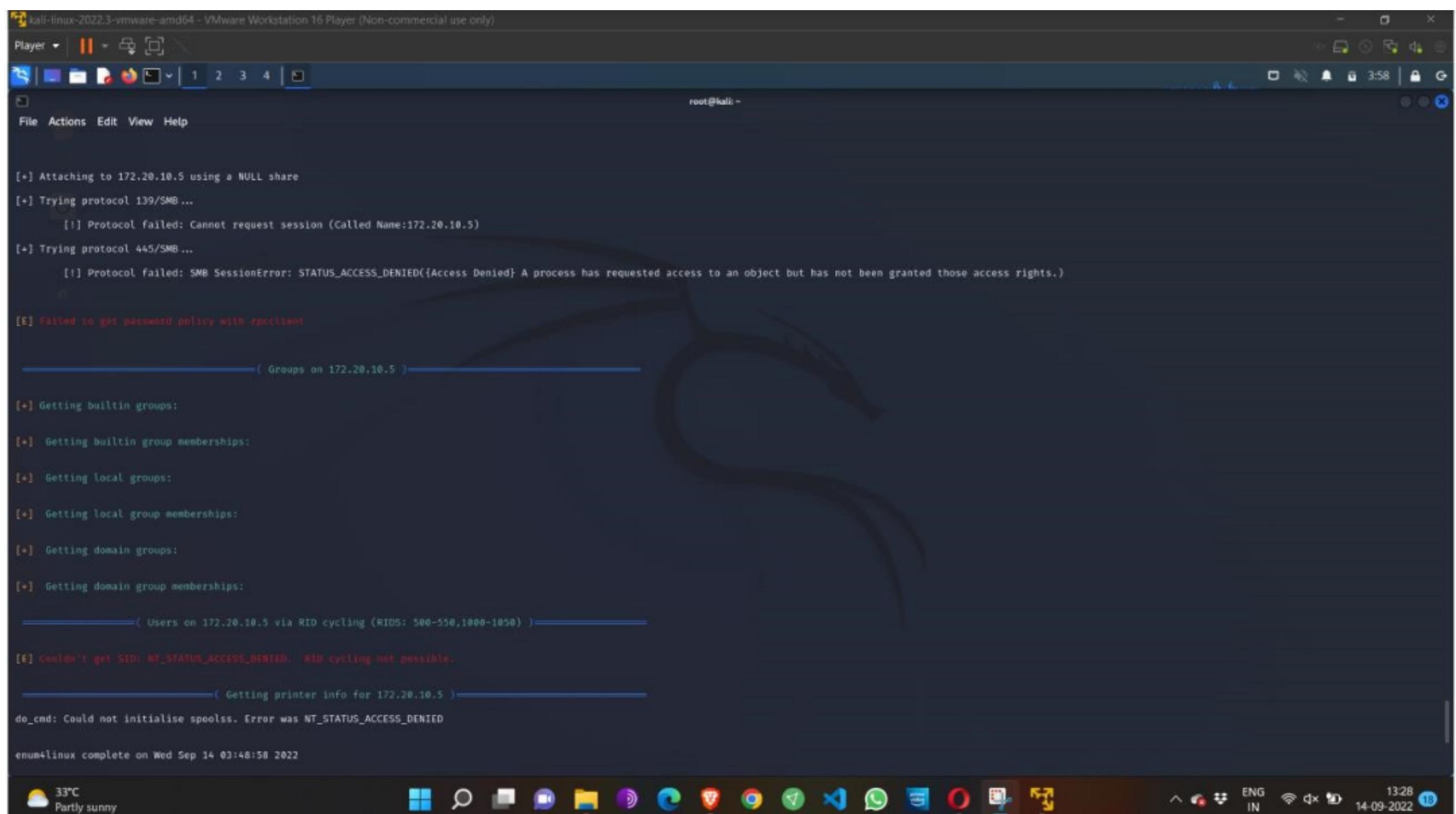
[+] Attaching to 172.20.10.5 using a NULL share
[+] Trying protocol 139/SMB ...
[!] Protocol failed: Cannot request session (Called Name:172.20.10.5)
[+] Trying protocol 445/SMB ...
[!] Protocol failed: SMB SessionError: STATUS_ACCESS_DENIED({Access Denied} A process has requested access to an object 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:

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



```
[+] 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

  33°C Partly sunny 13:28 14-09-2022 ENG IN
```

9)

```
(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)-[~]
```

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.

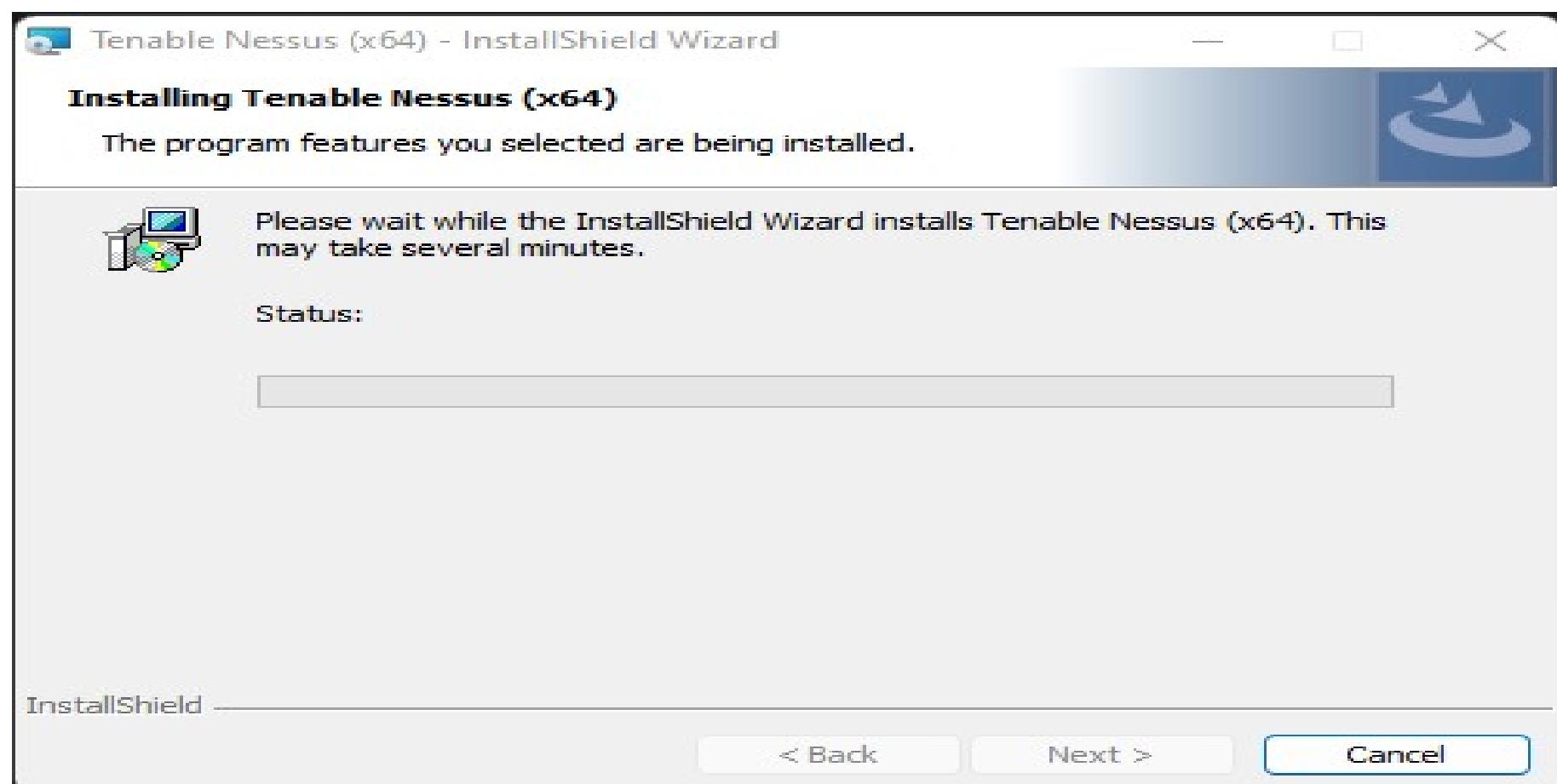
Exercise No 3: Vulnerability Access Scan Using Nessus

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. On the left, there's a sidebar with links like Nessus, Nessus Agents, Nessus Network Monitor, etc. The main content area has a heading 'Nessus' and three numbered steps: 1. Download and Install Nessus, 2. Start and Setup Nessus, and 3. Getting Started. Step 1 is expanded, showing 'Choose Download' fields for 'Version' (Nessus - 10.4.2) and 'Platform' (Windows - x86_64), a large blue 'Download' button, and links for 'Download by curl' and 'Docker & Virtual Machines'. To the right, there's a 'Summary' section with release details: Release Date: Jan 18, 2023, Release Notes: Nessus 10.4.2 Release Notes, and Signing Keys: RPM-GPG-KEY-Tenable-4096 (10.4 & above) and RPM-GPG-KEY-Tenable-2048 (10.3 & below).

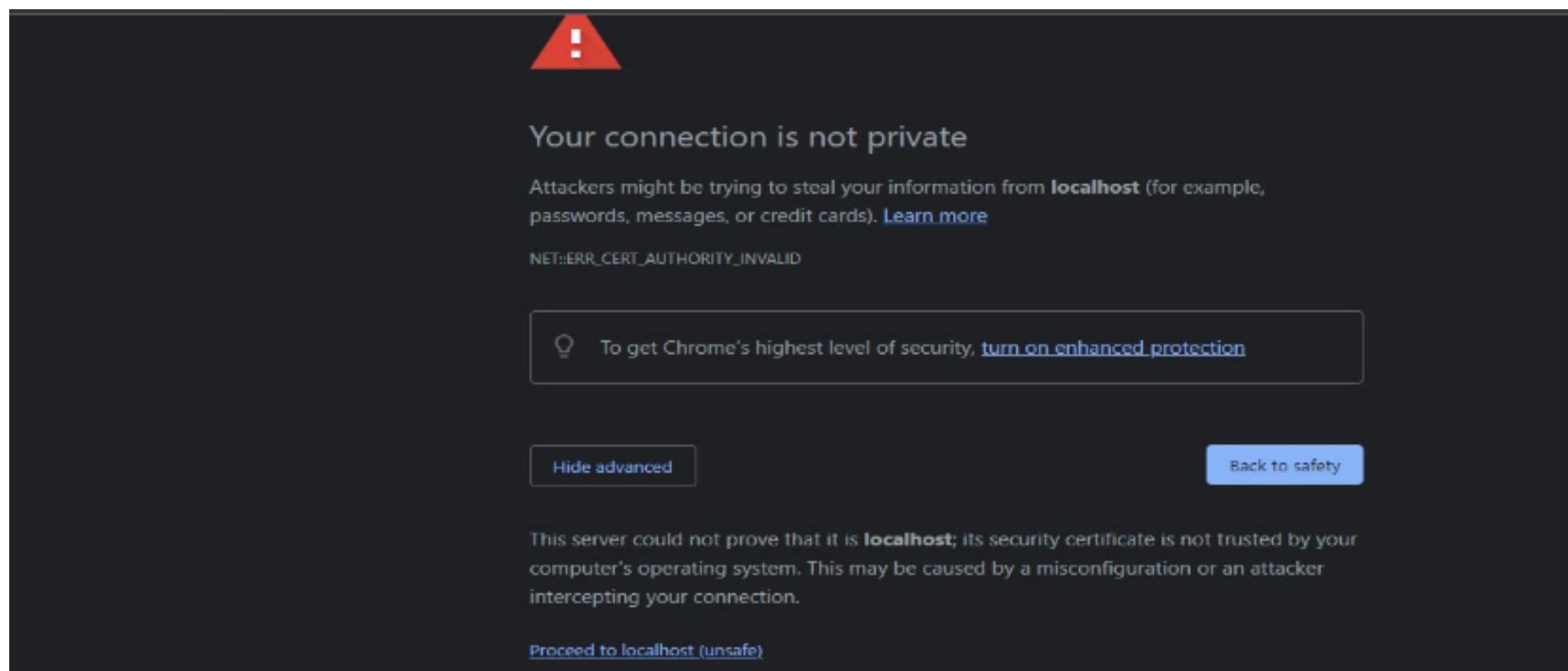
Step 2: Choose your OS and download , install



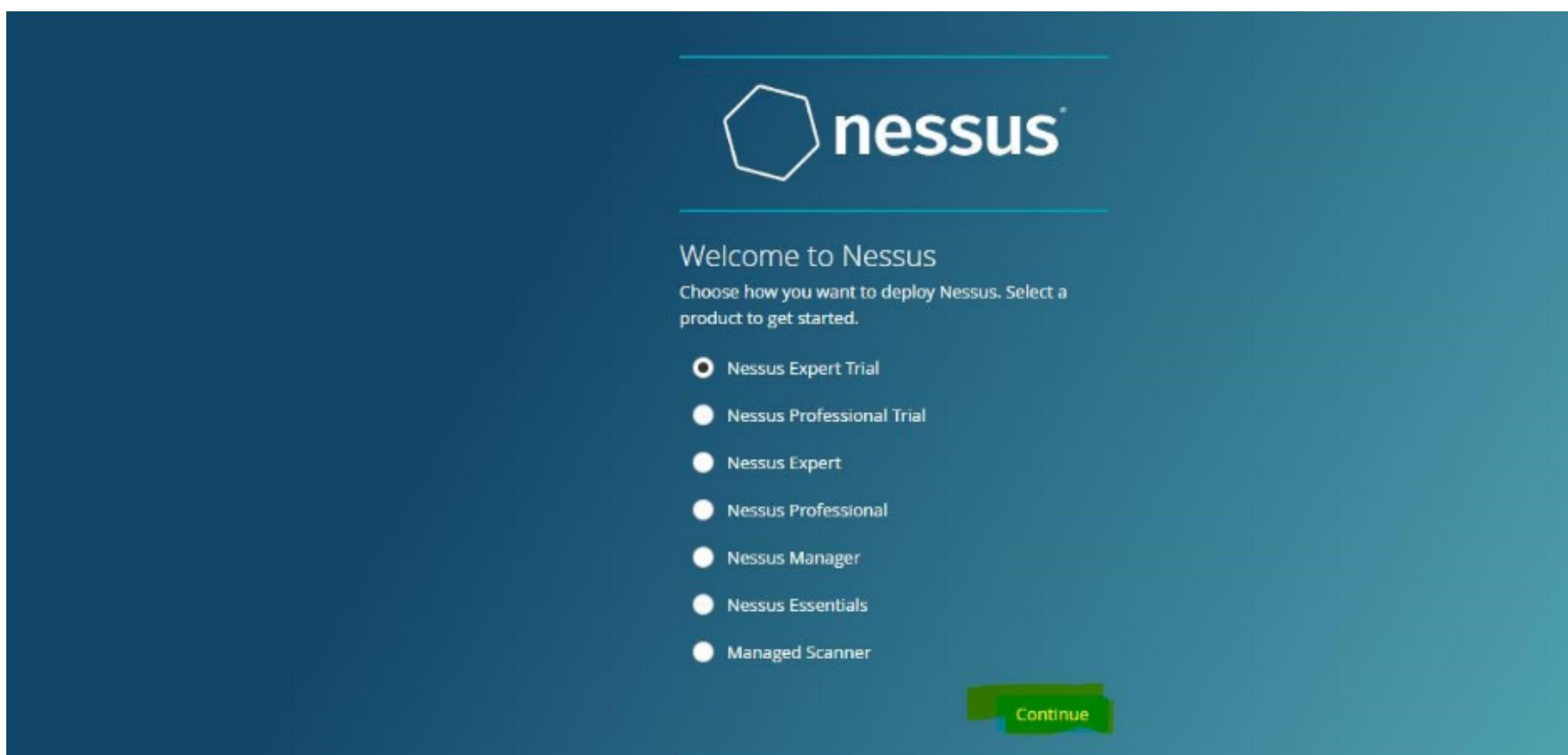
Step 3: Once installation is completed it will open in default browser



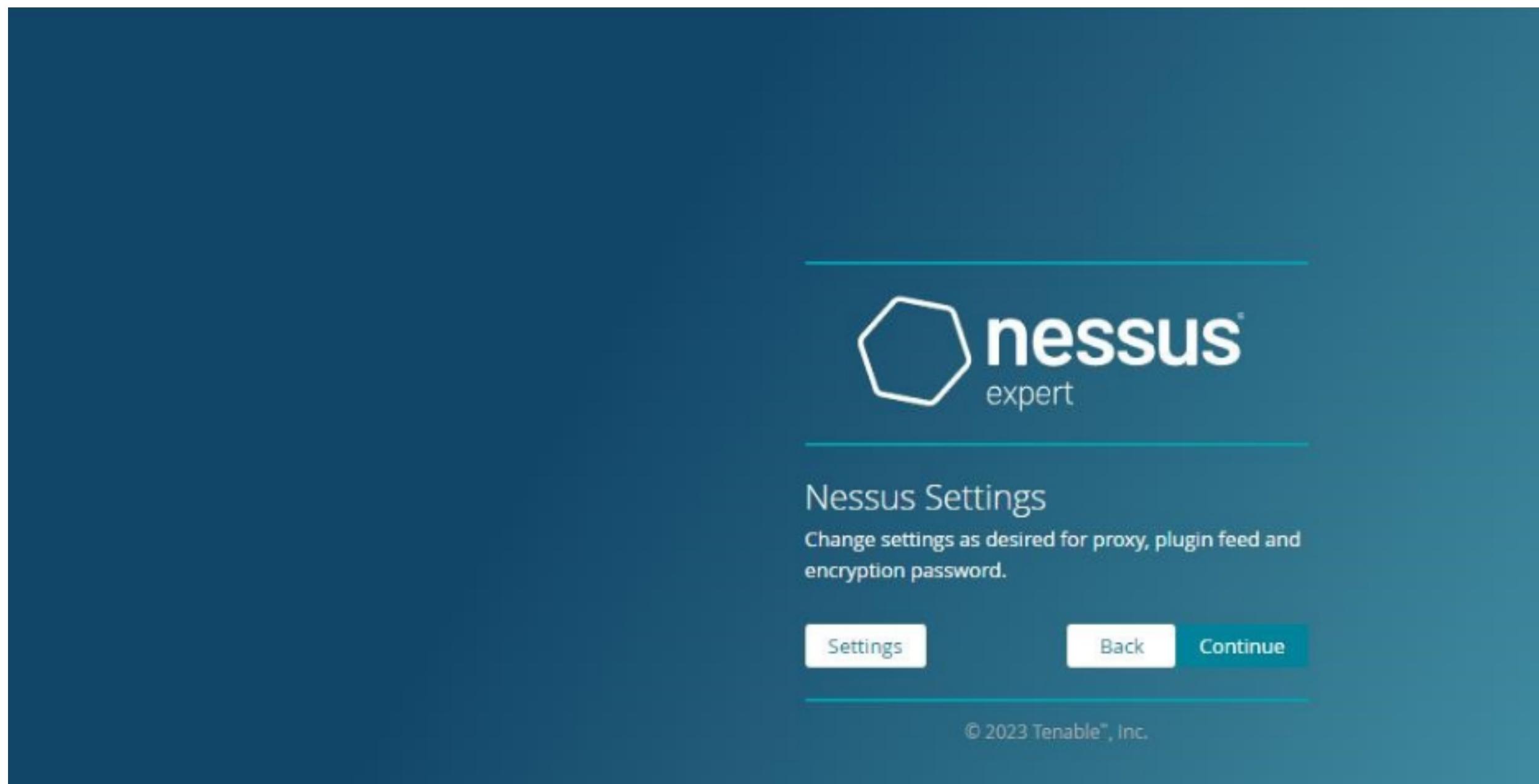
Step 5:- (click on the proceed to local host)



Step 6:- Please choose the Nessus Expert



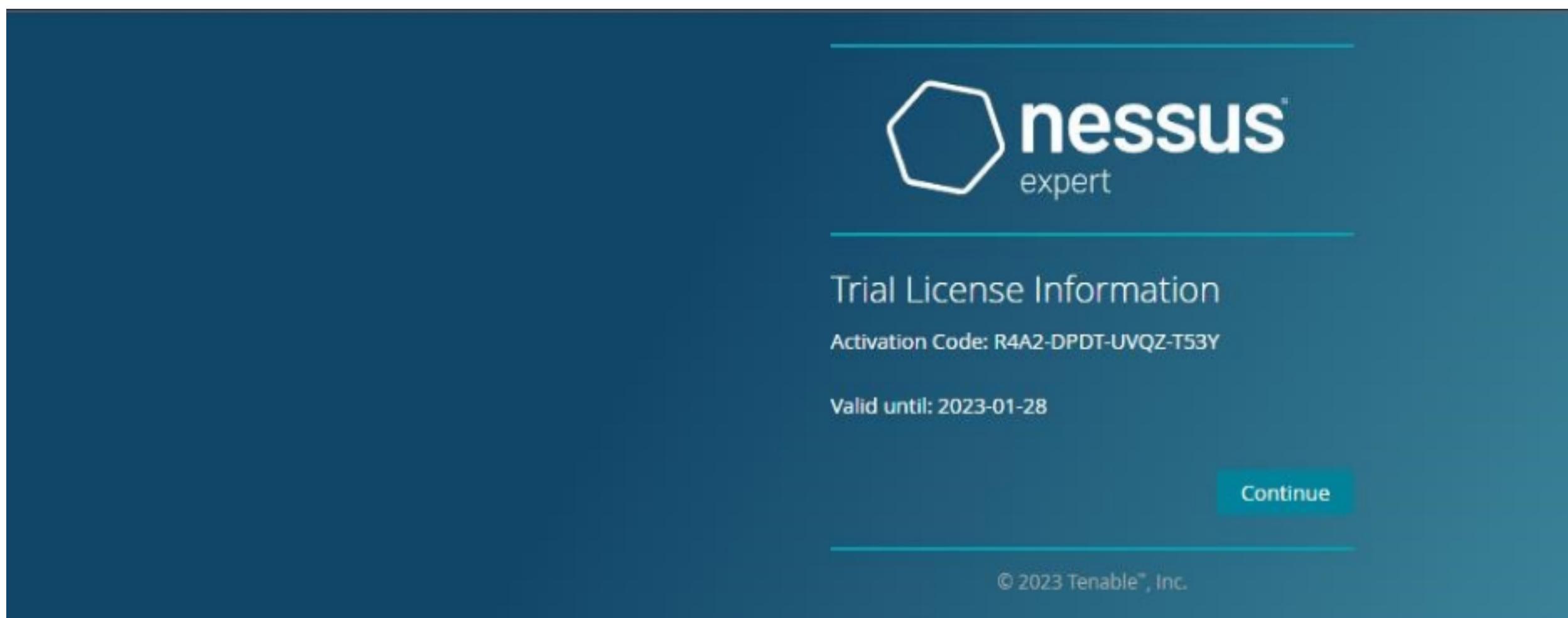
Step 7: Click on continue



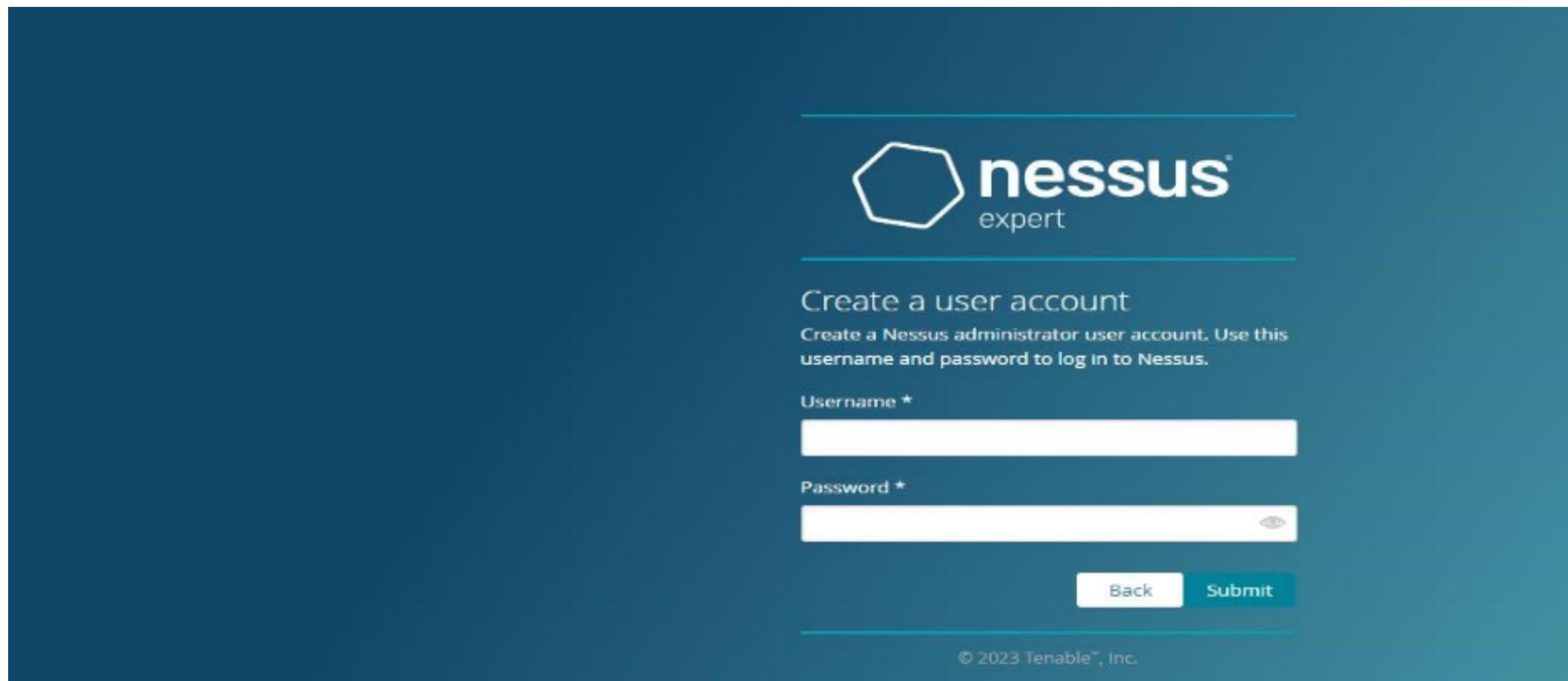
Step 8:- Register with your organizational email id

A screenshot of the Create Account form. The title is "Create Account" with a sub-instruction: "It looks like you don't have an account. Please provide the following information to create an account and start your trial." The form fields are: First Name (pupsha), Last Name (latha), Email (pushpalathas.sse@saveetha.com), Phone (8667613340), Title (Security team), Company Name (saveetha engineering college), and Company Size (Company Size: 500-999). At the bottom is a note: "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



Step 10:- set up your 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 *

Password *

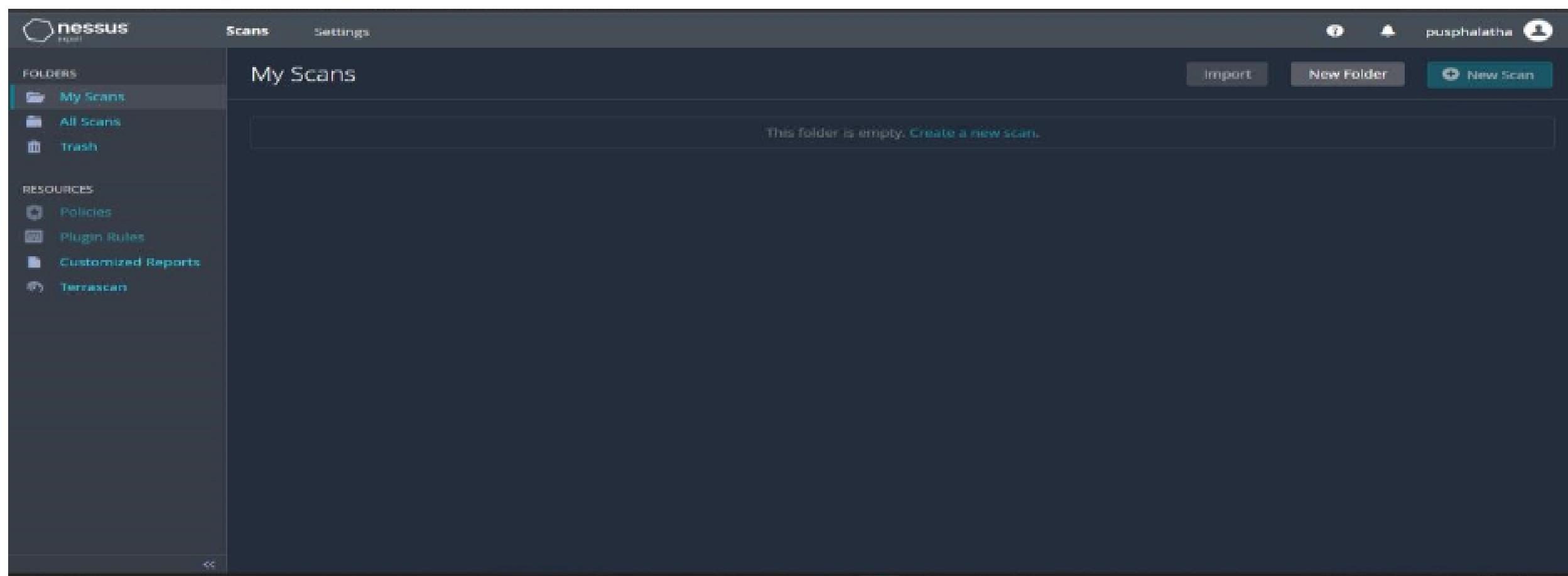
[Back](#) [Submit](#)

© 2023 Tenable®, Inc.

Step 12:- Please wait until download is completed

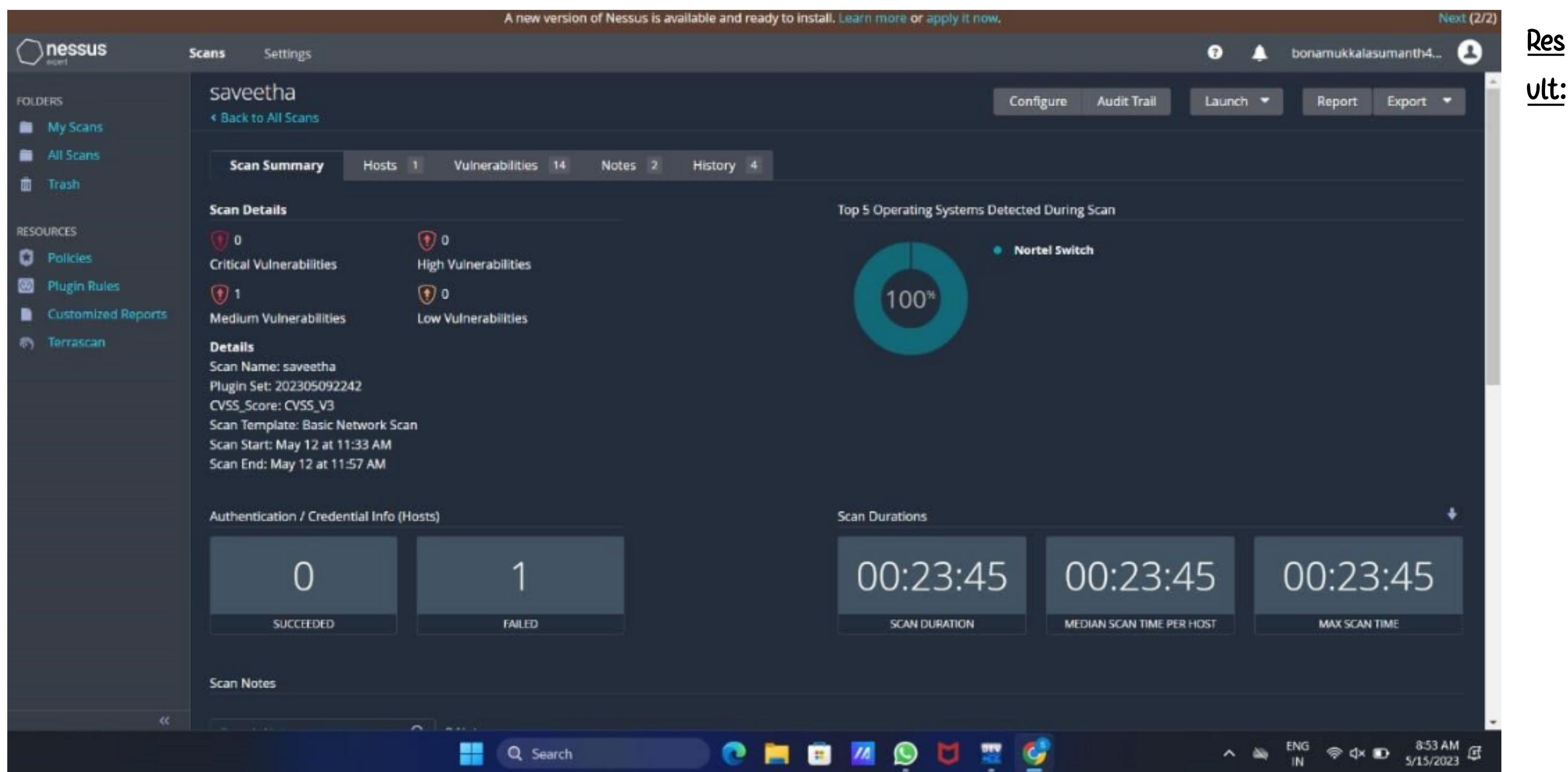


Step 13: Select My Scans



Output:

A screenshot of the Nessus interface showing policy details. The left sidebar includes 'Scans', 'Settings', 'FOLDERS' (with 'My Scans' selected), 'RESOURCES' (with 'Policies', 'Plugin Rules', 'Customized Reports', and 'Terrascan'), and a search bar. The main content area displays 'Policy Details' with sections for 'Basic Overview', 'Assessment Overview', 'Report Overview', 'Advanced Overview', 'Credential Settings Overview', 'Port Scanner Overview', and 'Fragile Devices'. It also shows network configuration details like 'Scan Policy: Basic Network Scan', 'Override Normal Accuracy: Normal', and 'Preferred SSH Port: 22'. The bottom of the screen shows a Windows taskbar with icons for File Explorer, Search, Task View, File, WhatsApp, Microsoft Edge, and Google Chrome, along with system status indicators.



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

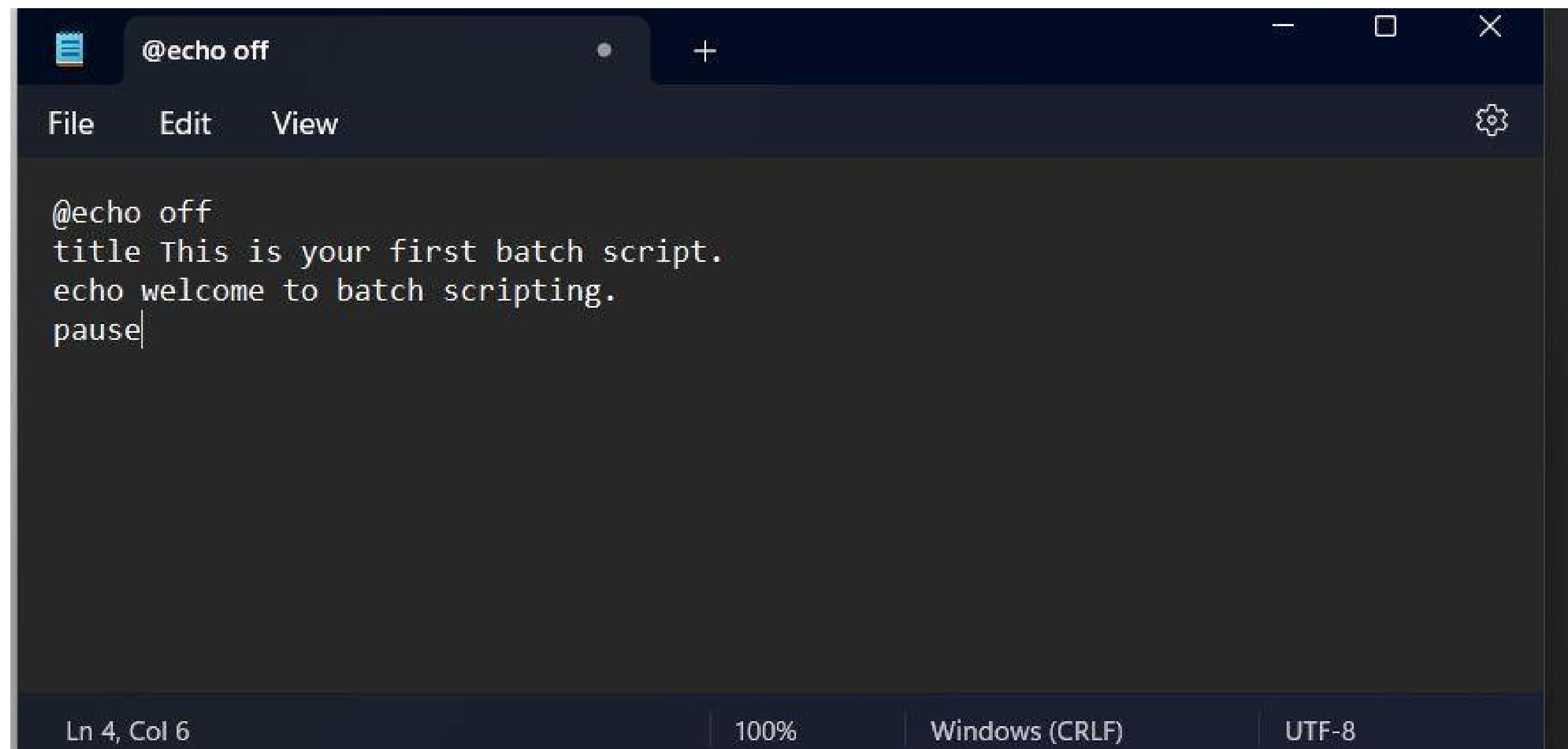
The above script echoes back the text "Welcome to batch scripting!" Save your file by heading to File > Save As, and then name your file what you'd like. End your file name with the added BAT extension, for example test.bat, and click OK. This will finalize the batch process. Now, double-click on your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

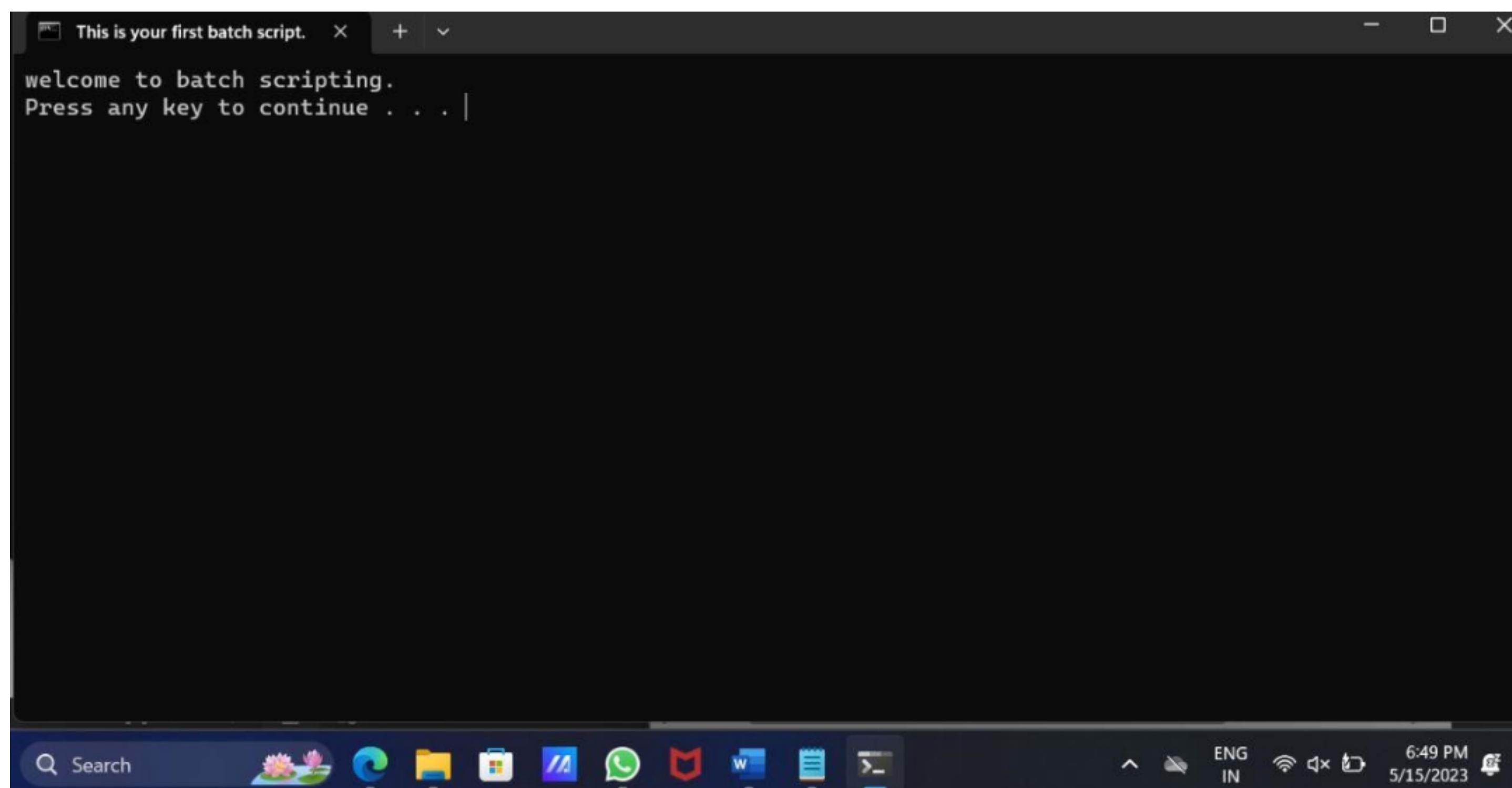
Result:



The screenshot shows a code editor window with a dark theme. The title bar says '@echo off'. The menu bar includes 'File', 'Edit', 'View', and a settings gear icon. The main area contains the following batch script code:

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

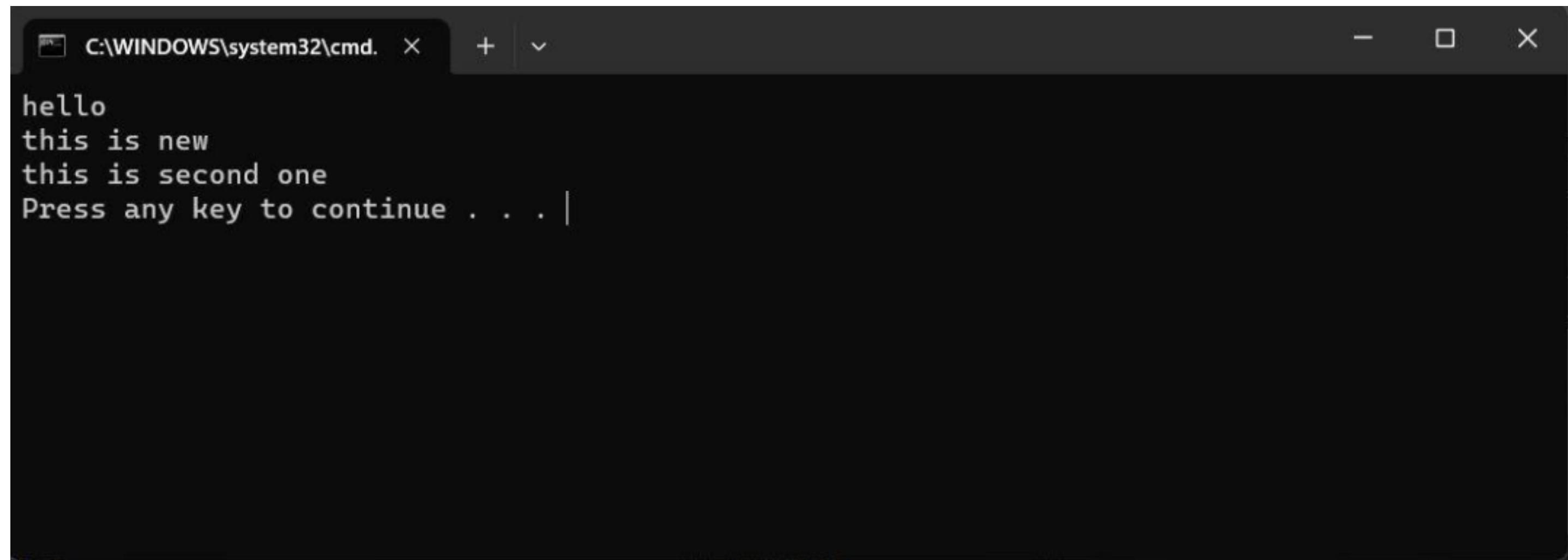
The status bar at the bottom shows 'Ln 4, Col 6' on the left, '100%' in the center, 'Windows (CRLF)' and 'UTF-8' on the right.



The screenshot shows a terminal window titled 'This is your first batch script.' The window displays the output of the batch script:

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

The taskbar at the bottom shows various pinned icons, including Microsoft Edge, File Explorer, and several productivity apps. The system tray in the bottom right corner shows the date and time as '6:49 PM 5/15/2023' along with other system status indicators.



A screenshot of a Windows Command Prompt window titled "C:\WINDOWS\system32\cmd.". 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

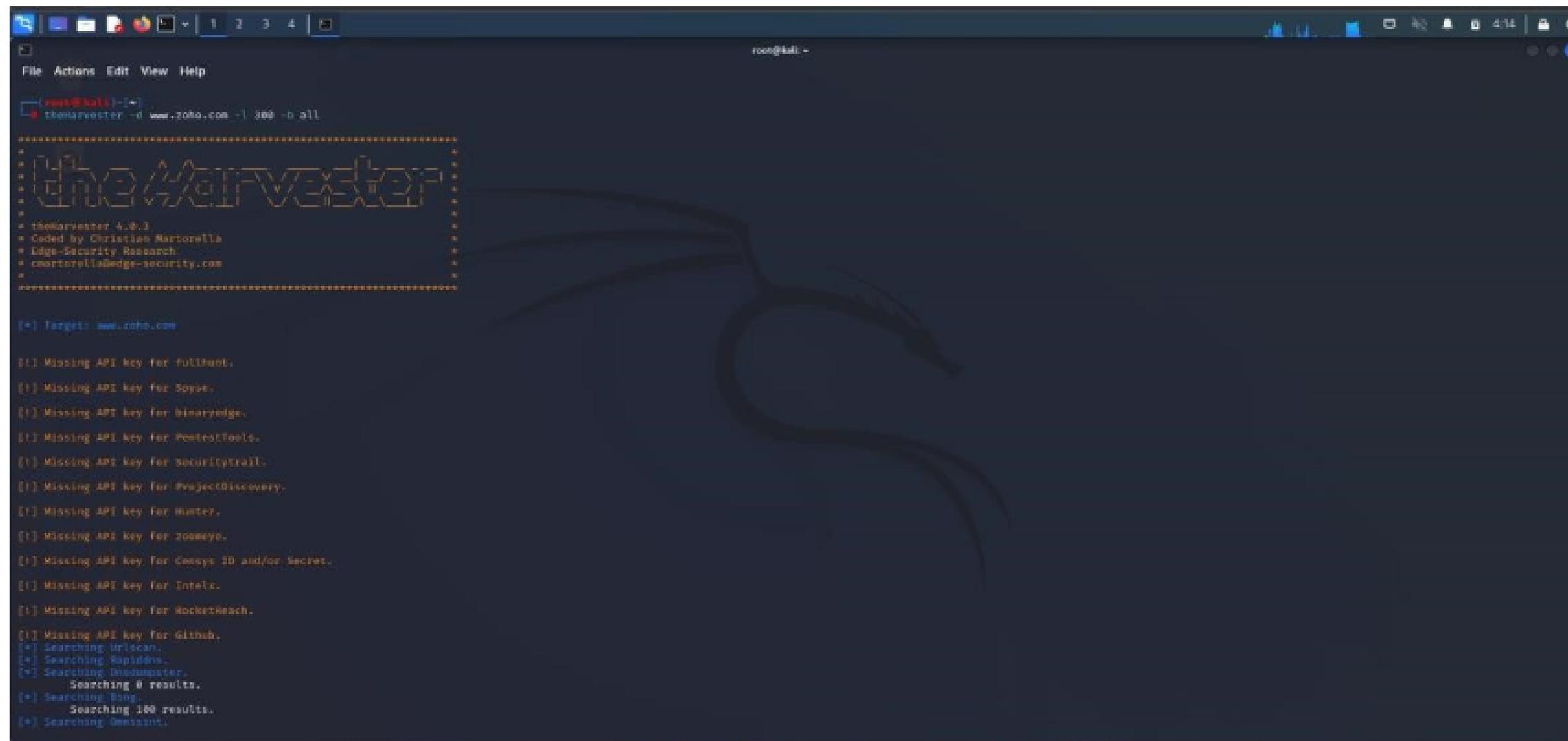
Aim: To demonstrate information gathering using theHarvester Procedure:

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



The screenshot shows a terminal window on a Kali Linux desktop. The title bar says "root@kali: ~". The command entered is "theHarvester -d www.zoho.com -l 300 -b all". The output is as follows:

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

[+] Target: www.zoho.com
[!] Missing API key for FullText.
[!] Missing API key for Sospe.
[!] Missing API key for binaryedge.
[!] Missing API key for PostalTools.
[!] Missing API key for securitytrails.
[!] Missing API key for ProjectDiscovery.
[!] Missing API key for Hunter.
[!] Missing API key for zonemoto.
[!] Missing API key for Censys IO and/or Secret.
[!] Missing API key for Intelis.
[!] Missing API key for RocketReach.
[!] Missing API key for Github.
(*) Searching Urlican.
(*) Searching Badlands.
(*) Searching Hunterster.
Searching 100 results.
(*) Searching Bing.
    Searching 100 results.
(*) Searching Omnisint.
```

```
root@kali:~
```

File Actions Edit View Help

[*] Searching Rapiddns.
[*] Searching Dnsdumpster.
 Searching 0 results.
[*] Searching Bing.
 Searching 100 results.
[*] Searching Omnisint.
 Searching 100 results.
 Searching 200 results.
[*] Searching Quant.
 Searching results.
 Searching 200 results.
[*] Searching VirusTotal.
An exception has occurred: Cannot connect to host www.baidu.com:443 ssl<:ssl.SSLContext object at 0x7f78044ddbc0> [Connection reset by peer]
An exception has occurred: Cannot connect to host www.baidu.com:443 ssl<:ssl.SSLContext object at 0x7f78044fdcc0> [Connection reset by peer]
An exception has occurred: Cannot connect to host www.baidu.com:443 ssl<:ssl.SSLContext object at 0x7f78044fd540> [Connection reset by peer]
An exception has occurred: Cannot connect to host www.baidu.com:443 ssl<:ssl.SSLContext object at 0x7f78044f5c0> [Connection reset by peer]
An exception has occurred: Cannot connect to host www.baidu.com:443 ssl<:ssl.SSLContext object at 0x7f78044fb40> [Connection reset by peer]
An exception has occurred: Cannot connect to host www.baidu.com:443 ssl<:ssl.SSLContext object at 0x7f78044f64c0> [Connection reset by peer]
An exception has occurred: Cannot connect to host www.baidu.com:443 ssl<:ssl.SSLContext object at 0x7f78044fa040> [Connection reset by peer]
An exception has occurred: Cannot connect to host www.baidu.com:443 ssl<:ssl.SSLContext object at 0x7f78044fd4c0> [Connection reset by peer]
An exception has occurred: Cannot connect to host www.baidu.com:443 ssl<:ssl.SSLContext object at 0x7f78044fd4b0> [Connection reset by peer]
An exception has occurred: Cannot connect to host www.baidu.com:443 ssl<:ssl.SSLContext object at 0x7f78044f6a40> [Connection reset by peer]
An exception has occurred: Cannot connect to host www.baidu.com:443 ssl<:ssl.SSLContext object at 0x7f78044fdff40> [Connection reset by peer]
An exception has occurred: Cannot connect to host www.baidu.com:443 ssl<:ssl.SSLContext object at 0x7f78044fd4d0> [Connection reset by peer]
An exception has occurred: Cannot connect to host www.baidu.com:443 ssl<:ssl.SSLContext object at 0x7f78044fd4b0> [Connection reset by peer]
An exception has occurred: Cannot connect to host www.baidu.com:443 ssl<:ssl.SSLContext object at 0x7f78044fd4a0> [Connection reset by peer]
An exception has occurred: Cannot connect to host www.baidu.com:443 ssl<:ssl.SSLContext object at 0x7f78044fd480> [Connection reset by peer]
An exception has occurred: Cannot connect to host www.baidu.com:443 ssl<:ssl.SSLContext object at 0x7f78044fd460> [Connection reset by peer]
An exception has occurred: Cannot connect to host www.baidu.com:443 ssl<:ssl.SSLContext object at 0x7f78044fd4e0> [Connection reset by peer]
An exception has occurred: Cannot connect to host www.baidu.com:443 ssl<:ssl.SSLContext object at 0x7f78044fd4c0> [Connection reset by peer]
An exception has occurred: Cannot connect to host www.baidu.com:443 ssl<:ssl.SSLContext object at 0x7f78044fd4b0> [Connection reset by peer]
An exception has occurred: Cannot connect to host www.baidu.com:443 ssl<:ssl.SSLContext object at 0x7f78044fd490> [Connection reset by peer]
An exception has occurred: Cannot connect to host www.baidu.com:443 ssl<:ssl.SSLContext object at 0x7f78044fd470> [Connection reset by peer]
An exception has occurred: Cannot connect to host www.baidu.com:443 ssl<:ssl.SSLContext object at 0x7f78044fd450> [Connection reset by peer]
An exception has occurred: Cannot connect to host www.baidu.com:443 ssl<:ssl.SSLContext object at 0x7f78044fd430> [Connection reset by peer]
An exception has occurred: Cannot connect to host www.baidu.com:443 ssl<:ssl.SSLContext object at 0x7f78044fd410> [Connection reset by peer]
An exception has occurred: Cannot connect to host www.baidu.com:443 ssl<:ssl.SSLContext object at 0x7f78044fd490> [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.n4ght.or.id/v1/subdomain-enumeration?domain=www.zoho.com')
 Searching results.
[*] Searching Certspotter.
[*] Searching ThreatMiner.
[*] Searching Onix.
[*] Searching Anubis.
An exception has occurred: Cannot connect to host www.baidu.com:443 ssl<:ssl.SSLContext object at 0x7f7804f6f1c0> [Connection reset by peer]
[*] Searching Baidu.

```
root@kali:~
```

File Actions Edit View Help

Searching 300 results.

[*] Searching LinkedIn.
An exception has occurred: 0, message='Attempt to decode JSON with unexpected mimetype: text/html', url=URL('https://api.n4ght.or.id/v1/subdomain-enumeration?domain=www.zoho.com')
 Searching results.
[*] Searching Certspotter.
[*] Searching ThreatMiner.
[*] Searching Onix.
[*] Searching Anubis.
An exception has occurred: Cannot connect to host www.baidu.com:443 ssl<:ssl.SSLContext object at 0x7f7804f6f1c0> [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 CHTsh.
[*] Searching Hackertarget.
Google is blocking your ip and the workaround, returning
[*] Searching CHTsh.
 Searching 0 results.
[*] Searching Threatcrowd.
Google is blocking your ip and the workaround, returning
[*] Searching Google.

[*] ASNs found: 7

AS32225
AS319986
AS311757
AS23247
AS2039
AS41913
AS63949

[*] InterestingUrls Found: 25

<https://www.zoho.com/>
<https://www.zoho.com/assistant/>
<https://www.zoho.com/assistant/>
<https://www.zoho.com/campaigns/?src=fromproduct>
<https://www.zoho.com/campaigns/explainer/campaign-view.html>
<https://www.zoho.com/campaigns/explainer/createm.html>
<https://www.zoho.com/campaigns/?src=fromproduct&id=2243172755001510000zsrc=fromproduct>
<https://www.zoho.com/campaigns/contactus.html>

```
File Actions Edit View Help
AS63949
[*] Interesting URLs Found: 25
https://www.zoho.com/
https://www.zoho.com/assists/
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/zsend.html
https://www.zoho.com/clickservicecurl-%Fchats%2F224377255801510886zsrc=fromproduct
https://www.zoho.com/clickservicecurl-%Findex.phpzsrc=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/crm/crm/
https://www.zoho.com/emailsender/
https://www.zoho.com/forms/
https://www.zoho.com/invoicer/?utm_source=206utm_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;ZBleft=show
https://www.zoho.com/nl/det/
https://www.zoho.com/report-abuse/
https://www.zoho.com/salesiq/
https://www.zoho.com/survey/
[*] No Twitter users found.

[*] LinkedIn Users Found: 392
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
Amoli Moorthy - Product Manager and Co-Founder
Anandarajan Krishnan - Product Manager
[*] No LinkedIn users found.
```

```
File Actions Edit View Help
root@kali:~
[*] LinkedIn Users Found: 392
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
Amoli Moorthy - Product Manager and co-Founder
Anandarajan Krishnan - Product Manager
Ananthu Subramanian - Engineer Trainee
Ananthu Hair - PreSales Engineer - Zoho Corporation
Andrea Manomey - VP - Certified Computer Solutions
Andrew Beaume
Andrew John - Zoho Corporation
Andrew J A - Senior Member Of Technical Staff
Anilayaa Pandit - Zoho Consultant
Anurita Gupta - Technical Writer
Anupendu Narasimhan - Zoho Corporation
Anup Balachandran - Senior Product Marketing Manager
Arun Koenig - Product Designer
Aruna Muraleedharan - Product Marketer
Aryadeep Krishnamoorthy
Ashok Chakravarthy Nagaraajan
Ashok Kumar
Ashwin P Sharma - Lead - Zoho CRM SME
Avinanth B - Software Developer - Zoho
Avaradeen N
Badril Rajayan - Senior Technical support engineer
Balaji Ganesh
Balaji Krishnan - Product Marketer
Balaji Sundar - Member Technical Staff
Balaji Venkatasramani
Balaji Jayaraman - Product Manager
Bareeth Kumar Ramish - Member Leadership Staff
Bashirul Haque Faisal - Zoho Consultant
Bennudin Samuel - Zoho Developer
Bharath Kumar
Bharathi Ambarzagan - Member Technical Staff
Calvin Jaster - Quality Analyst- Zoho CRM Support
Carla Garcia
Chakravarthy Radhakrishnan - Zoho Corporation
Chandru Jayapalan - Zoho Corporation
Charles Lazaro
Chetan K. - Zoho CRM Consultant - Regal Infonet
Chitravandian Nachiappa - Senior Product Director
Clarence Rorario - Director of Product Management
Cynthia A - Product Management
D Jayaram - Visual Designer
DEVEROMA KUSHWAH - Zoho Developer
David Elkins - Head of Content Review
Deepak RV - Enterprise Support Engineer - Zoho
```

```
File Actions View Help
Vijayragavan venugopal
Vinothnai Thiagarajan
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
Chandrakalash S - iOS Developer
Ranganathan Ramesh - Account Manager - Zoho
Sathiyam Sathiyammarva - zoho - Zoho Corporation
Shakil Afreen Taj - Senior Technical Support Engineer
Visudevanneew T - Lead
working as a Senior executive at Indigo Airlines
[*] LinkedIn Links Found: 8
Aamil Mohammed - Regional Account Manager
Abbas Abu - Zoho One Developer
Abhilash Reddy Godishala
Adarsh Pandey - Member of Technical Staff
Adithyan Ravichandran - 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
Amar Nath KR - Zoho Developer
Amoli Moorthy - Product Manager and Co-Founder
Anandarasan 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
Anubhav Pandey - Zoho consultant
Anumita Gupta - Technical Writer
Aravinda Natarajan - Zoho Corporation
Arun Balachandran - Senior Product Marketing Manager
Arun Kesavan - Product Designer
Aruna Muralidharan - Product Marketer
Arvind Krishnamoorthy
Ashok Chakravarthi Nagarajan
```

```
File Actions View Help
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
Chandrakalash S - iOS Developer
Ranganathan Ramesh - Account Manager - Zoho
Sathiyam Sathiyammarva - zoho - Zoho Corporation
Shakil Afreen Taj - Senior Technical Support Engineer
Visudevanneew 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/593e989fa8f137d2af458fd4
https://trello.com/power-ups/584c1aa1922a25429b66635/zoho-crm
https://trello.com/power-ups/5b05db5704c75f29bf1d475/automateio
https://trello.com/power-ups/5ba22b6cd5ada0f95e4dc98
https://trello.com/power-ups/5a22bd6d5ada0f95e4dc98/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/reviews/support
https://trello.com/templates
https://trello.com/templates/design
https://trello.com/templates/design/design-system-checklist-yzn5ufon
https://trello.com/templates/design/freelance-branding-project-zm66dsjy
https://trello.com/templates/design/research-iteration-8f9qgnz
https://trello.com/templates/product-management
https://trello.com/templates/product-management/5-estapas-de-gestionamiento-de-productos-7s8avmv
https://trello.com/templates/product-management/7-listas-para-la-gestion-de-productos-blufgy87
https://trello.com/templates/product-management/backlog-de-funcionalidades-snmcwjtg
https://trello.com/templates/product-management/combinando-un-mvp-snyq7p
https://trello.com/templates/product-management/facilizar-las-ideas-davivj95
https://trello.com/templates/product-management/product-roadmap-template-frbjabsbh
https://trello.com/templates/product-management/roadmap-de-produto-67jiblr
https://trello.com/templates/product-management/roadmap-product-jpdxi2nn
https://trello.com/templates/product-management/shipping-planner-mclvzive
https://trello.com/tour
https://trello.com/use-cases/crm
```

```

root@kali: ~
File Actions Edit View Help
https://trello.com/use-cases/crm
https://www.trello.com/
[*] IPs found: 49
8.39.54.155
8.48.222.81
74.205.84.81
74.205.112.101
74.205.112.118
74.205.113.118
74.205.113.176
74.205.113.203
74.205.155.201
89.16.178.52
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
136.14.1.182.195
136.14.1.198.58
136.14.3.190.79
136.14.3.190.155
136.14.3.190.156
136.14.1.191.204
185.171.187.32
185.254.167.105
185.254.168.105
178.79.172.105
185.20.289.52
204.141.32.155
204.141.42.155
204.141.62.156
204.141.62.194
236.52.72.155
2886:98c1:3128::c
2886:98c1:3121::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)

```

[*] Receiving connections...
[*] ASNs Found: 4
ASNS:4
[*] Interesting URLs Found: 1
https://www.zaveetha.com/
[*] LinkedIn Links Found: 0

[*] IPs Found: 4
198.139.175.1
198.189.159.144
199.34.228.77

[*] Emails Found: 27
admin@saveetha.com
adminoffice@ssaveetha.com
admission.medical@ssaveetha.com
admission.scon@ssaveetha.com
admission.scp@ssaveetha.com
admission.sxl@ssaveetha.com
admission@ssaveetha.com
artsadmission@ssaveetha.com
asso.deanfaculty@ssaveetha.com
dean.ssm@ssaveetha.com
enggadmin@sion@ssaveetha.com
hr.smc@ssaveetha.com
hr.smt@ssaveetha.com
hr.smt@sion@ssaveetha.com
hr.smt@sion@ssaveetha.com
prime@ssaveetha.com
principal.sht@ssaveetha.com
principal.sco@ssaveetha.com
schooladmission@ssaveetha.com
schoolofhospitality@ssaveetha.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:**

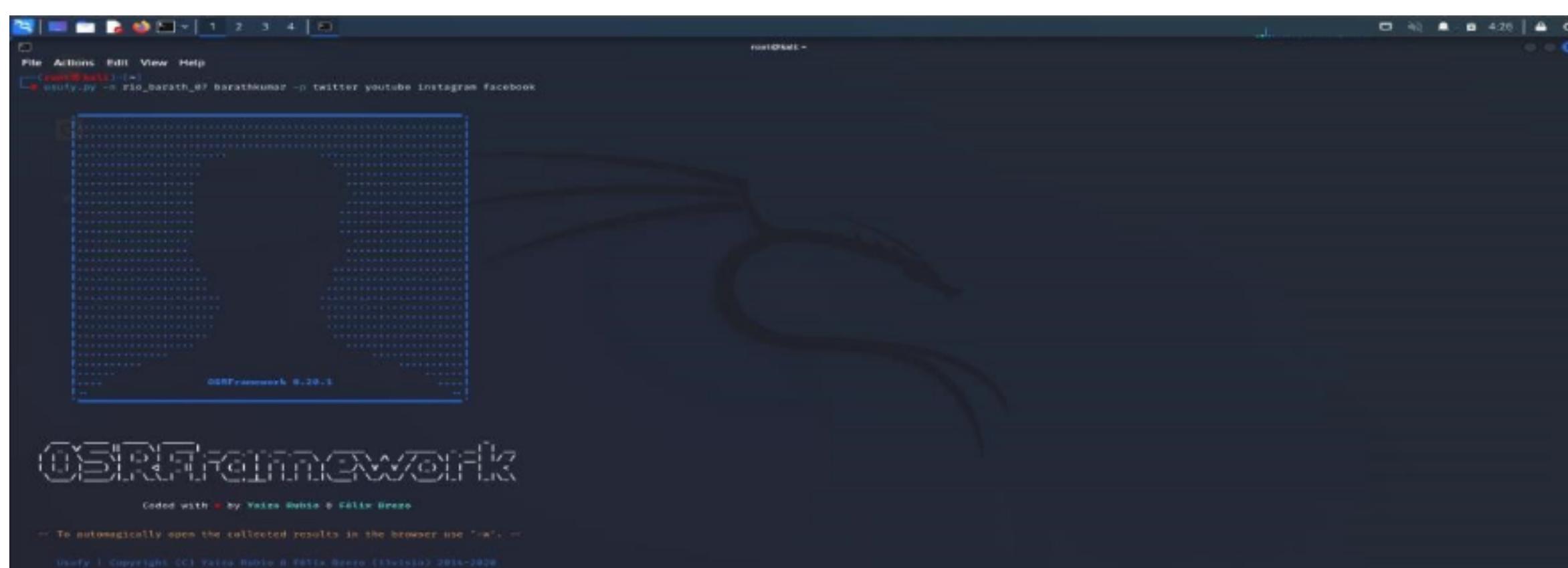
Step 1: Log into kali linux machine

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 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@kali:~# ./searchfy.py -q "LIVEWIREFRAMEWORK"
2022-09-14 04:25:35.212393      Starting search in 4 platform(s) ... Relax!
Press <Ctrl + C> to stop ...

2022-09-14 04:25:41.521829      Results obtained (4):
/usr/lib/python3/dist-packages/pyexcel/Deprecated.py:200: 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, 04:25:41.521829):
+-----+-----+-----+
| 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 |
| https://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/barathikumar/about | barathikumar | YouTube |
| https://www.facebook.com/barathikumar | barathikumar | Facebook |
| https://www.instagram.com/barathikumar | barathikumar | Instagram |
| http://twitter.com/barathikumar | barathikumar | Twitter |
+-----+-----+-----+
2022-09-14 04:25:41.598091      You can find all the information here:
./profiles.csv
2022-09-14 04:25:41.597460      Finishing execution ...
Total time consumed: 0:00:00.388075
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 our GitHub project:
https://github.com/livewireframework/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 "LIVEWIREFRAMEWORK"
```

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
+-----+	+-----+-----+	+-----+
	us	Twitter
+-----+	+-----+-----+	+-----+
	cehuser	Facebook
+-----+	+-----+-----+	+-----+
	cehuser	Twitter
+-----+	+-----+-----+	+-----+
	us	Facebook
+-----+	+-----+-----+	+-----+

FIGURE. 10

Collect and note the information disclosed about the target.

Output:

1)

Result:

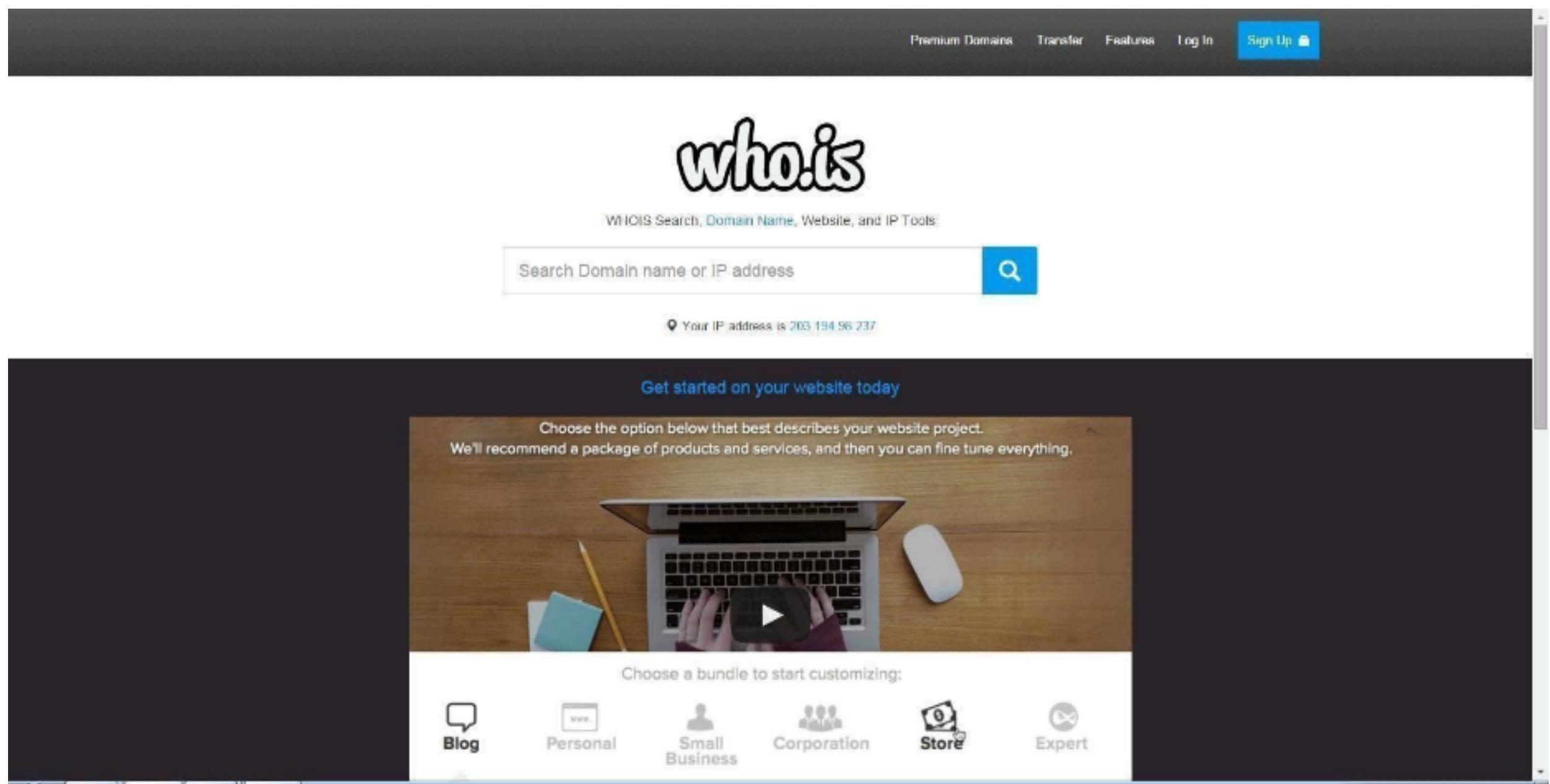
2)

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 cached

saveetha.com

DNS Information

Whois DNS Records Diagnostics

DNS Records for saveetha.com

Hostname	Type	TTL	Priority	Content
saveetha.com	A	3600	10	198.185.159.144
www.saveetha.com	CNAME	3600	10	saveetha.com

who.is Search for domains or IP addresses... Premium Domains Transfer Features Login Sign Up

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

saveetha.com

diagnostic tools

Whois DNS Records Diagnostics

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=8.07 ms
64 bytes from 198.185.159.144: icmp_seq=5 ttl=47 time=8.15 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 who.is/whois/saveetha.com

who.is Search for domain or IP addresses...

Premium Domains Transfer Features Login Sign Up

saveetha.com

whois Information

Whois DNS Records Diagnostics

cache expires in and 0 seconds
↻ refresh

Registrar Info

Name	PDR Ltd. dba PublicDomainRegistry.com
Whois Server	whois.publicdomainregistry.com
Referral URL	www.publicdomainregistry.com
Status	clientTransferProhibited https://icann.org/avpp#clientTransferProhibited

Important Dates

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

Name Servers

ns51.domaincontrol.com	97.74.165.26
ns52.domaincontrol.com	173.29.1.73.26

Similar Domains

savee-board.gov.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.
↻ refresh

Registrant Contact Information:

Name	Dr. H.P. Beereddy
Organization	Saveetha Dental College & Hospital
Address	Plot No. 100, Sector No. 10, Kukatpally, Hyderabad, Andhra Pradesh - 500072, India

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

Find the perfect domain at **Name.com**

OUTPUT:

The screenshot shows a web browser window with the title "WHOIS search results". The URL in the address bar is "in.godaddy.com/whois/results.aspx?domain=www.saveetha.com". The main content area displays "Search the WHOIS Database" with a search bar containing "saveetha.com" and a "Search" button. To the right, there is a sidebar with the heading "Find your Domain" and a search bar for "Find your perfect domain". The central content area is titled "WHOIS search results" and lists various domain registration details for "SAVEETHA.COM". Key information includes:

- 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/

At the bottom of the results, it says: "">>>> Last update of whois database: 2023-05-13T08:33:11Z <<<" and "For more information on Whois status codes, please visit https://icann.org/epp". A notice states: "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 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    192.168.0.57:25088   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 [108.165.150.145]
over a maximum of 20 hops.
  1  *        0 ms.   0 ms.   0 ms.  192.168.0.1:102
  2  *        514 ms.  620 ms.  192.168.20.10
  3  *        *        *        Request timed out.
  4  *        1012 ms.  293 ms.  192.160.31.24
  5  *xxxx  *        *        192.168.31.27
  6  *        *        *        Request timed out.
  7  *        *        *        Request timed out.
  8  *        *        *        Request timed out.
  9  *xxxx  *        *        127.73.248.228
 10  270 ms.  266 ms.  *        avo-e-100-w2.deploy.static.akamaitechnologies.com [50.6.100.21]
 11  *        *        *        Request timed out
 12  *        *        14017 ms.  192.168.108.170

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=36ms TTL=64
Reply from 192.168.53.42: bytes=32 time=36ms TTL=64

Ping statistics for 192.168.53.42:
    Packets: Sent = 3, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milliseconds:
        Minimum = 36ms, 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.

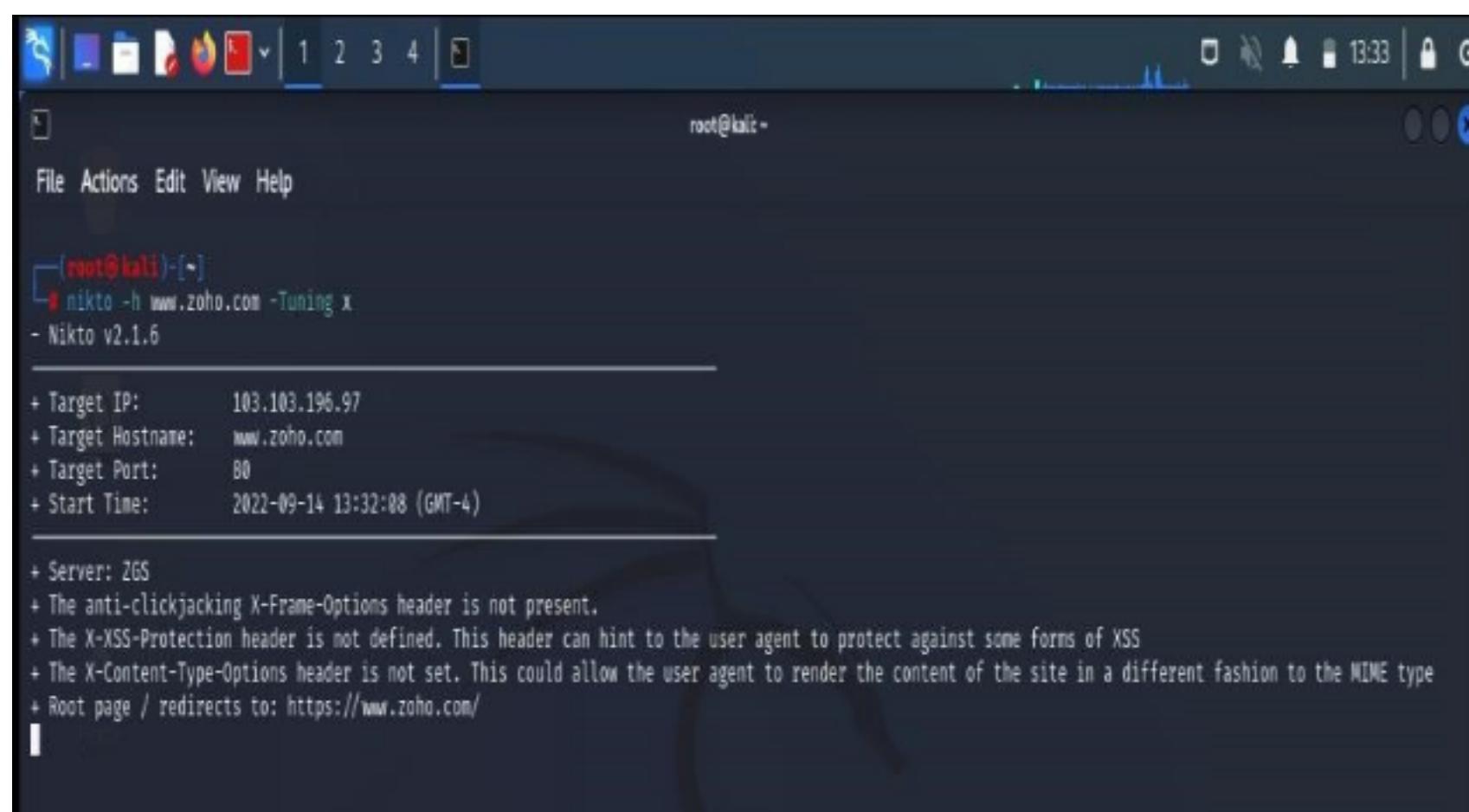
Exercise No 9:VULNERABILITY ANALYSIS - CGI Scanning with Nikto

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



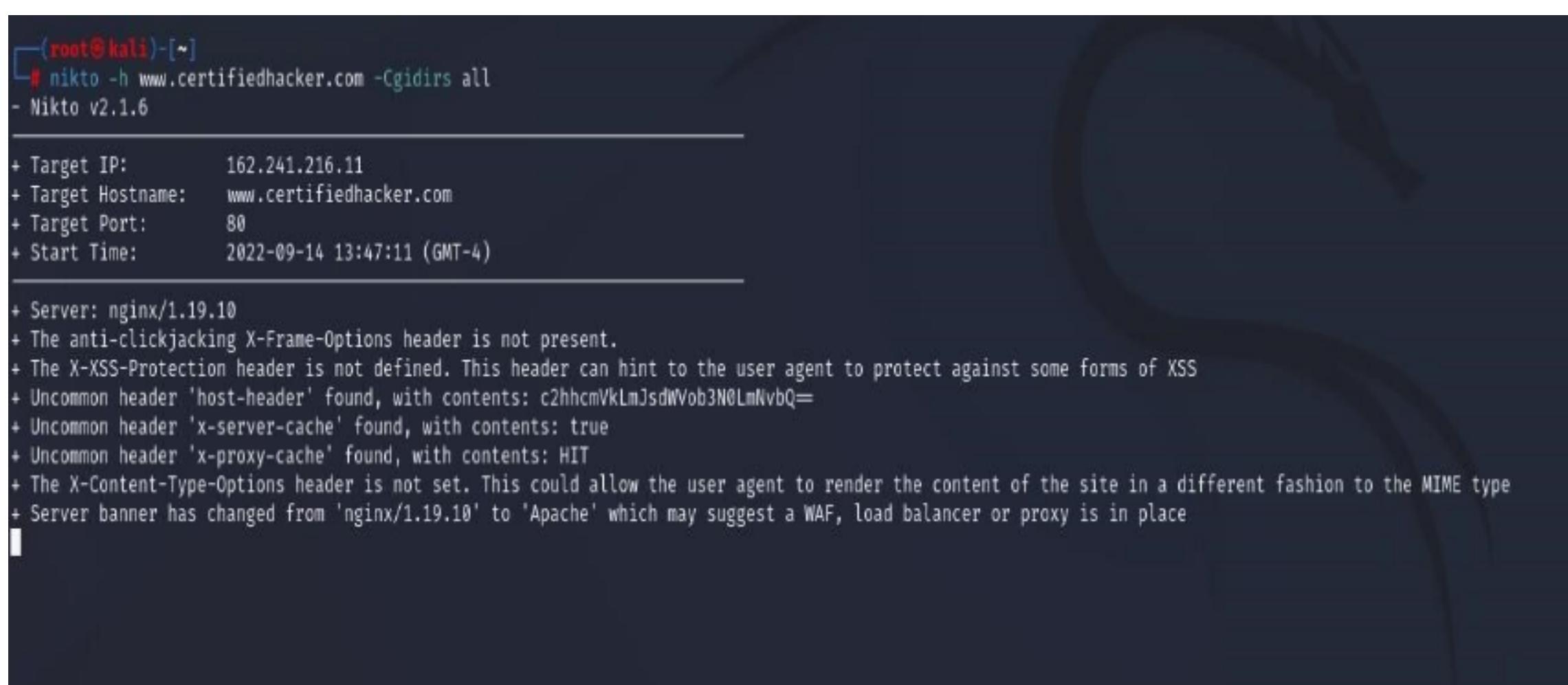
```
(root@kali)-[~]
# nikto -h www.zoho.com -Tuning x
- Nikto v2.1.6

+ 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: ZFS
+ 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

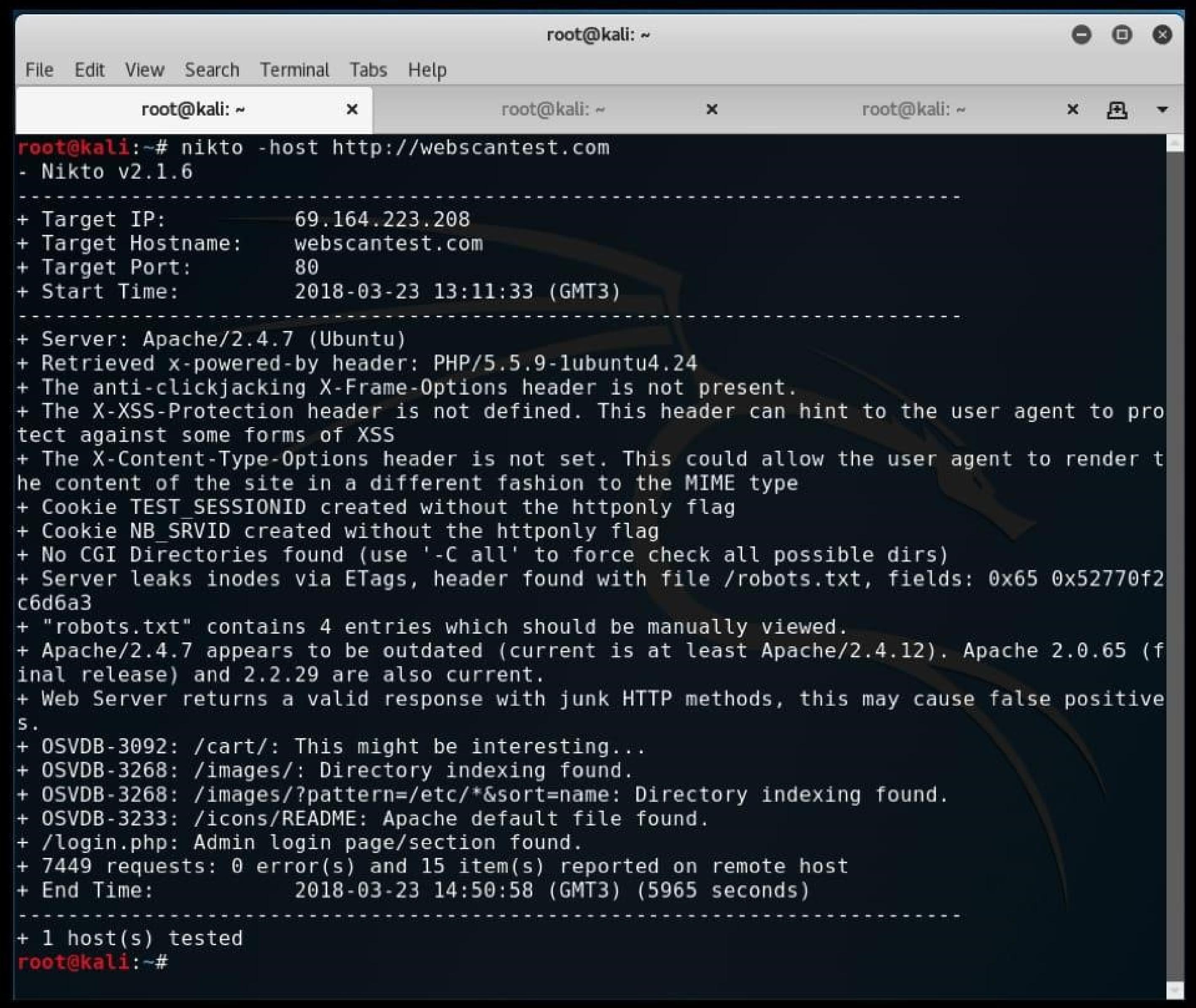
+ Target IP:      162.241.216.11
+ Target Hostname: www.certifiedhacker.com
+ Target Port:    80
+ Start Time:    2022-09-14 13:47:11 (GMT-4)

+ 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 webserver and list out the directories

Output:

1)



The screenshot shows a Kali Linux terminal window with three tabs open, all titled "root@kali: ~". The active tab displays the output of the Nikto web scanner. The command run was "nikto -host http://webscantest.com". The output provides detailed information about the target server, including its IP (69.164.223.208), hostname (webscantest.com), port (80), and start time (2018-03-23 13:11:33 GMT3). It also lists various security findings such as Apache version (2.4.7), PHP version (5.5.9), and specific vulnerabilities like OSVDB-3092 and OSVDB-3268. The scan concludes with 1 host tested.

```
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-lubuntu4.24
+ 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 positives.
+ 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:

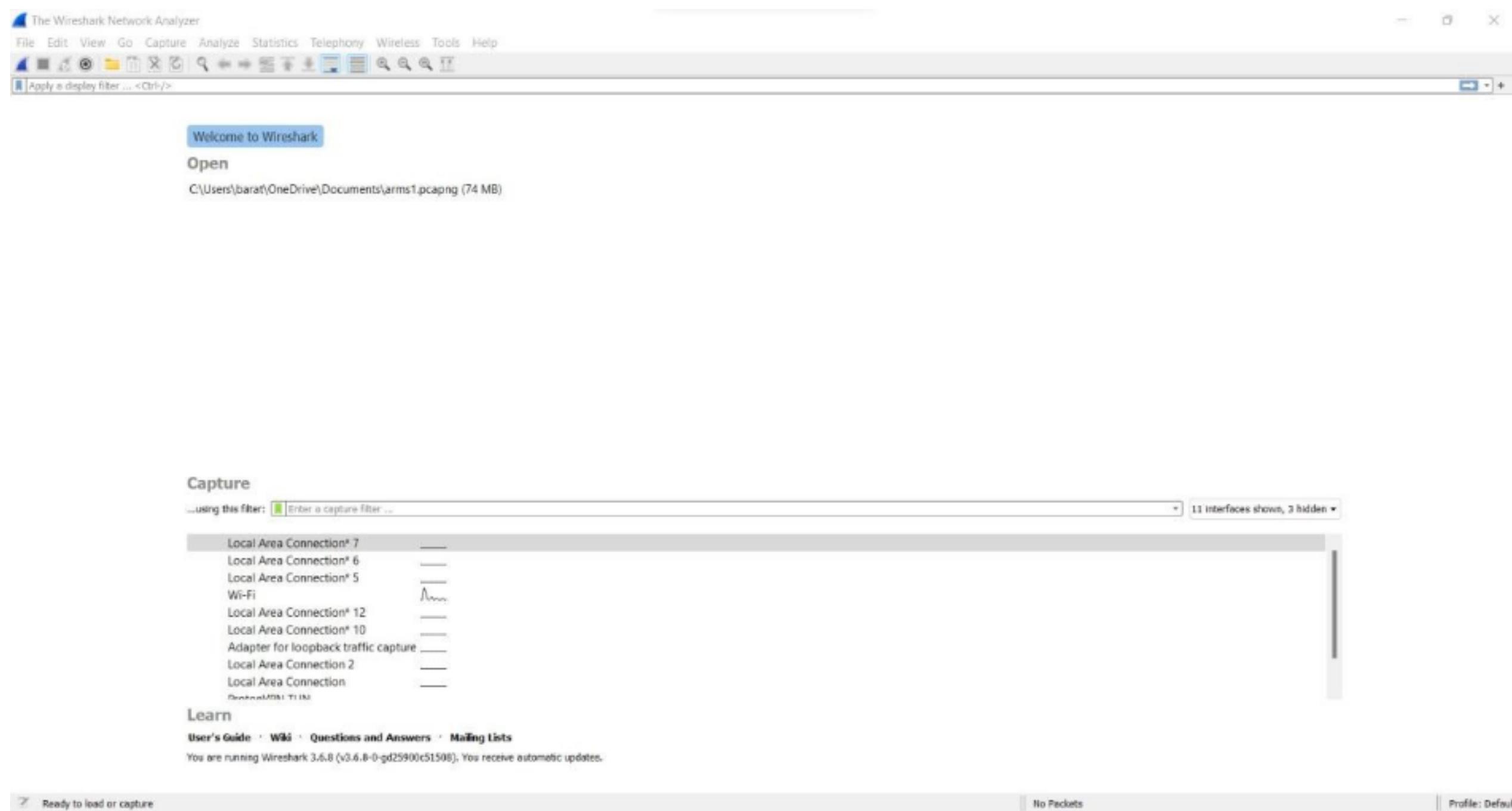
The above experiment is about VULNERABILITY ANALYSIS - CGI Scanning with Nikto. We can retrieve information like server name, headers and etc. This is done in root terminal using kali linux OS.

Exercise No 10: Wireshark sniffer

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

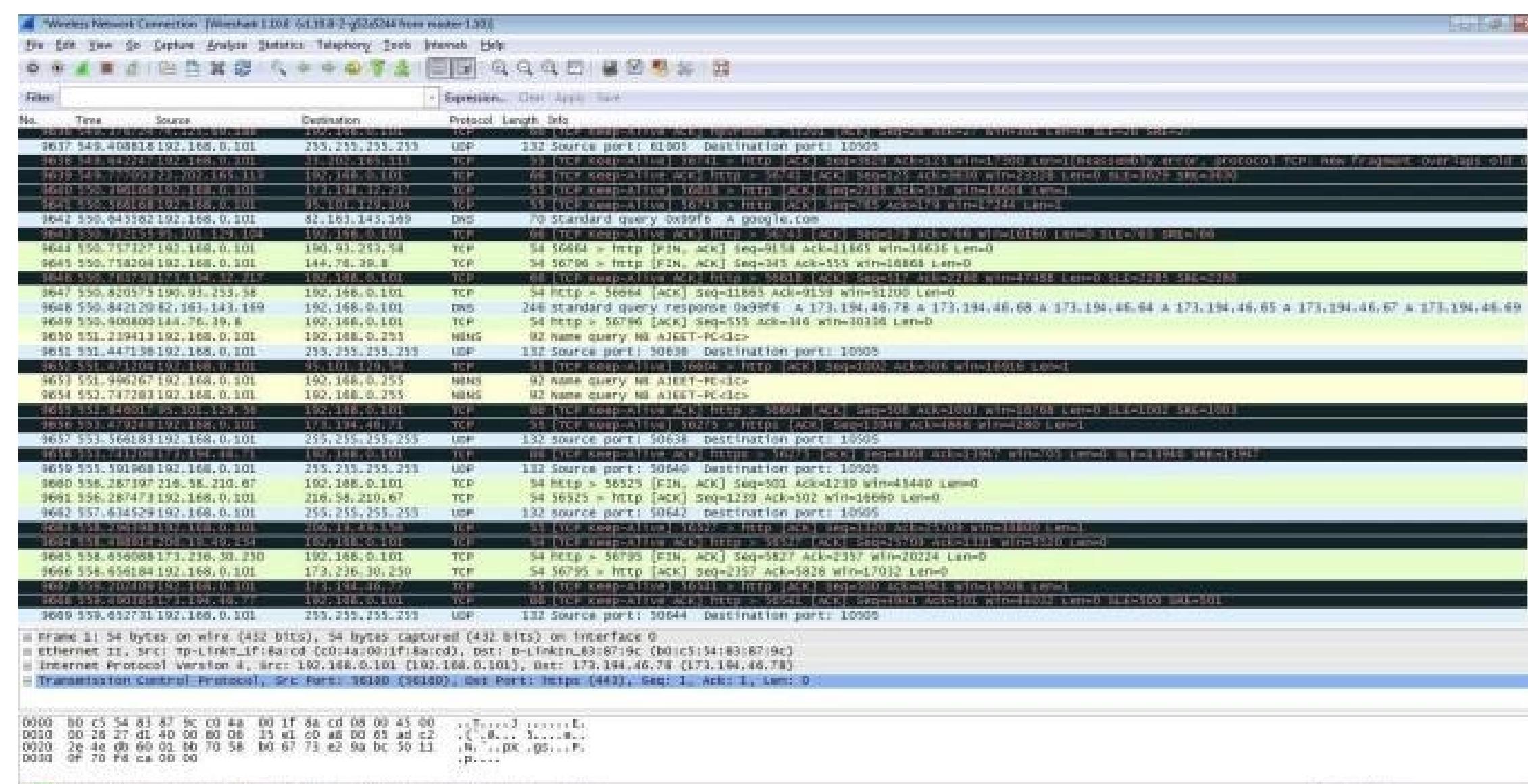
Procedure:

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



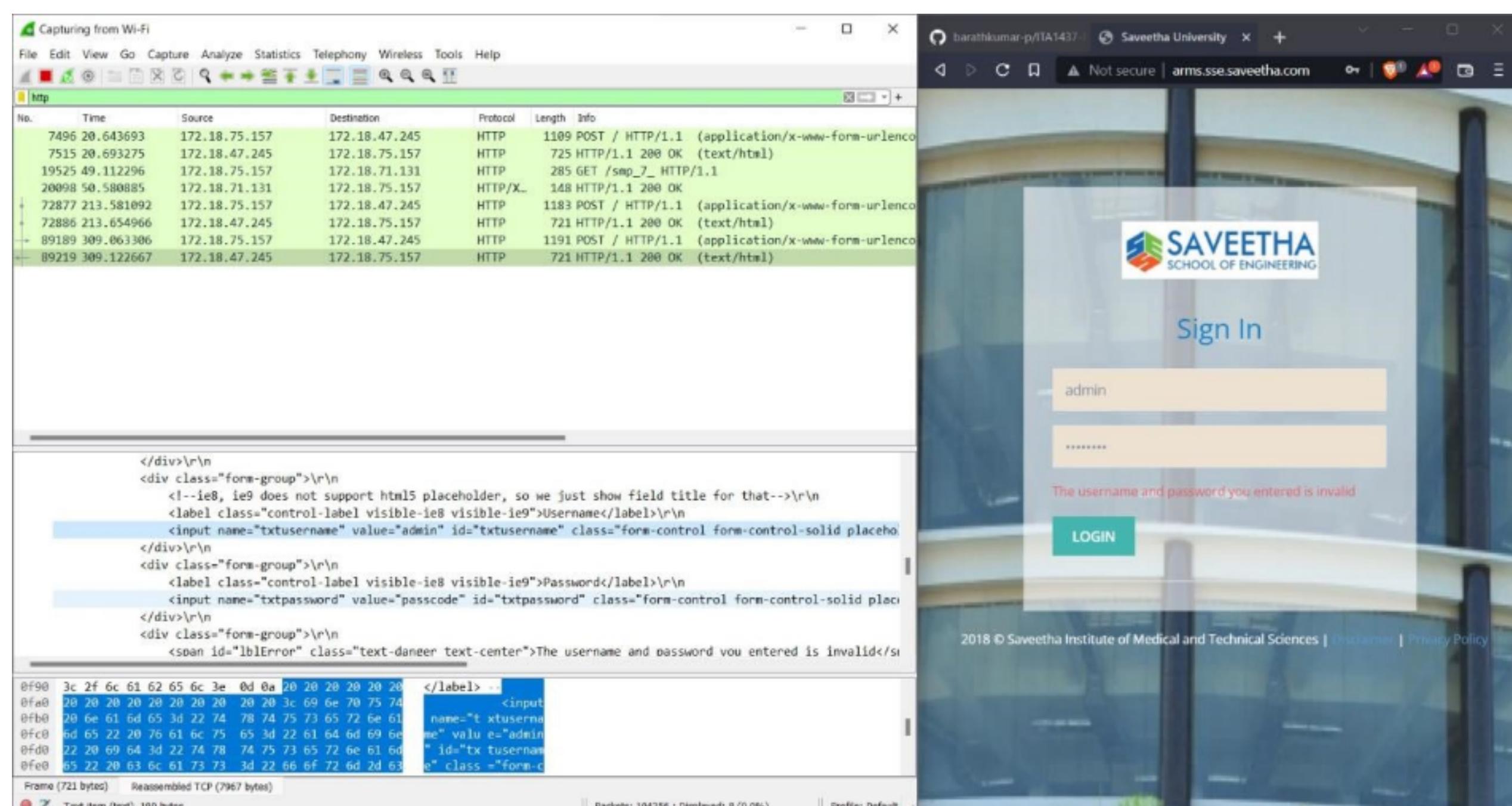
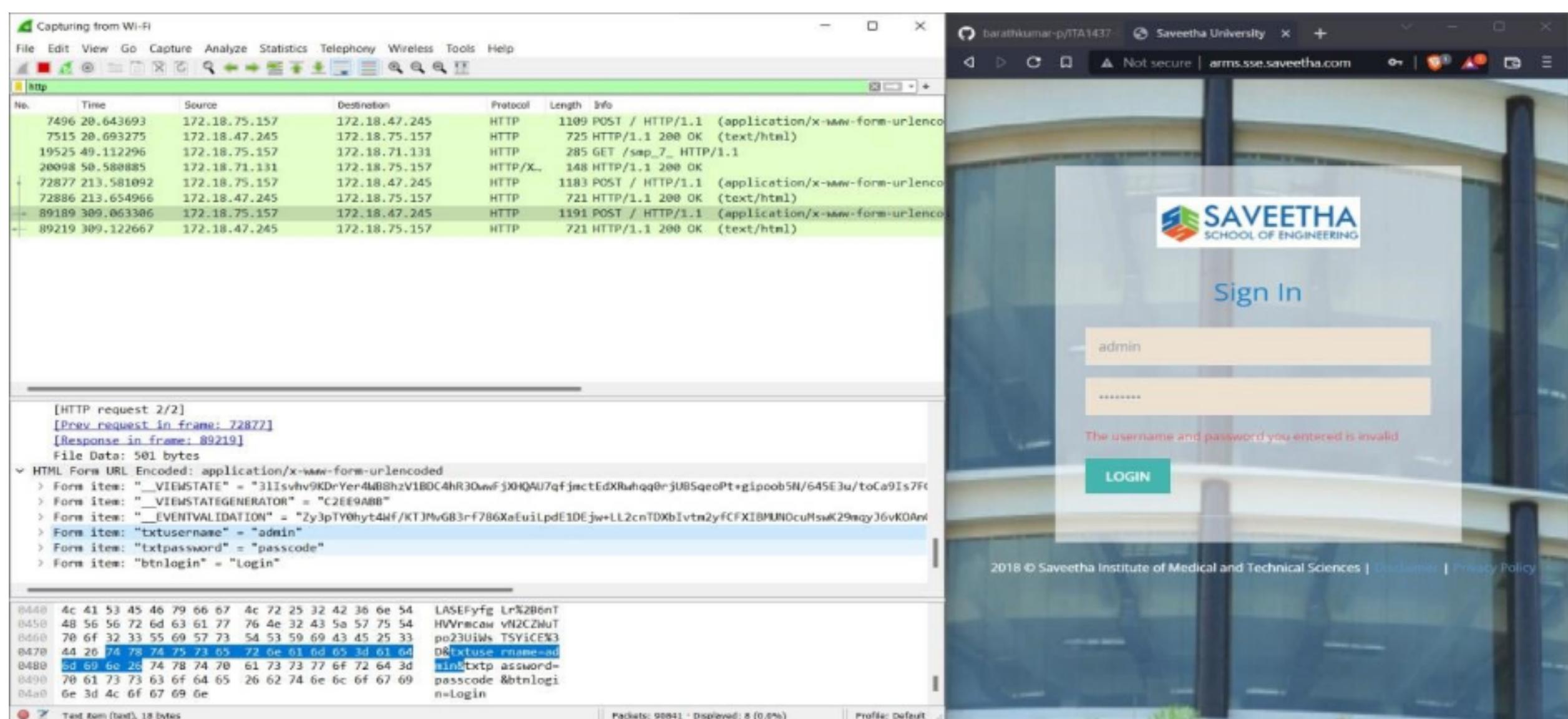
Step 1: Open a website in a new window and enter the user id and password. Register if needed.

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

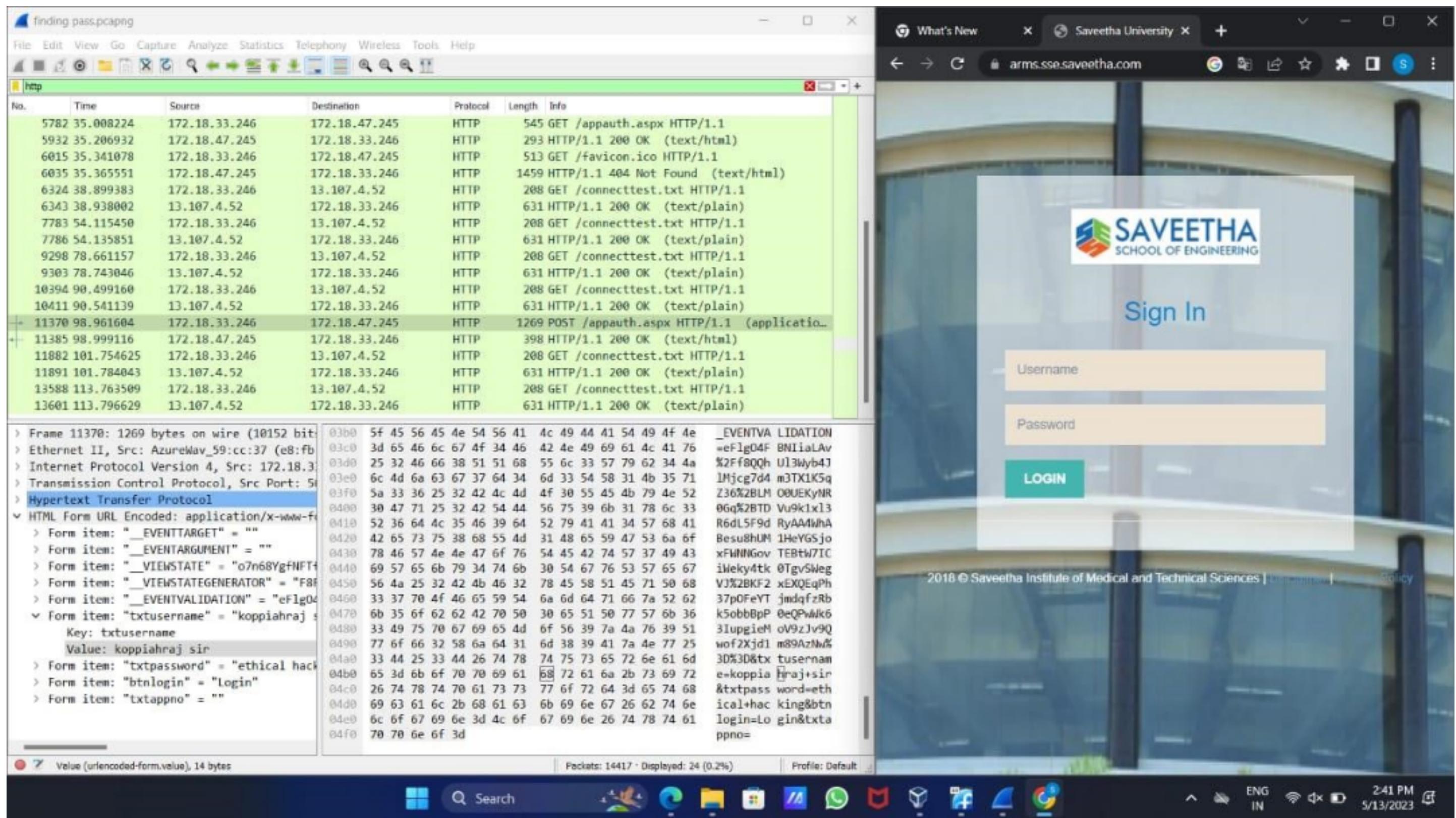


Step 10: Find the post methods for username and password

Step 11: You 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.

