

**ITA1471**

# **ETHICAL HACKING FOR NETWORK HACKING**



**K.Phanindra**

**192211310**

**1<sup>st</sup> YEAR, CSE DEPARTMENT**

# ITA144-ETHICAL HACKING

## LAB MANUAL

### Exercise No 1: Nmap Scan

#### Aim:

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

#### Procedure:

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

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

#### Scanning Techniques

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

#### Step 3:-

To perform host discovery

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

Step4:-

**Port Specification**

<b><u>Flag</u></b>	<b><u>Use</u></b>	<b><u>Example</u></b>
<b>-p</b>	specify a port or port range	nmap -p 1-30 192.168.1.1
<b>-p-</b>	scan all ports	nmap -p- 192.168.1.1
<b>-F</b>	fast port scan	nmap -F 192.168.1.1

Step 5:-

***Service Version and OS Detection***

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

Step 6:-

**Timing and Performance**

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

Output:

1)

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

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

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

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

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

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

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

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

2)

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

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

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

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

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

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

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

3)

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

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

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

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

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

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



4)

```
(root@kali)-[~]  
# nmap -O 192.168.1.1  
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-15 04:55 EDT  
Nmap scan report for 192.168.1.1  
Host is up (0.0016s latency).  
Not shown: 999 closed tcp ports (reset)  
PORT      STATE      SERVICE  
514/tcp   filtered  shell  
Warning: OSScan results may be unreliable because we could not find at least  
1 open and 1 closed port  
Device type: general purpose  
Running: Linux 2.4.X|3.X  
OS CPE: cpe:/o:linux:linux_kernel:2.4.37 cpe:/o:linux:linux_kernel:3.2 cpe:/o:  
:linux:linux_kernel:4.4  
OS details: DD-WRT v24-sp2 (Linux 2.4.37), Linux 3.2, Linux 4.4  
  
OS detection performed. Please report any incorrect results at https://nmap.org/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 https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 35.22 seconds
```

### **Result:**

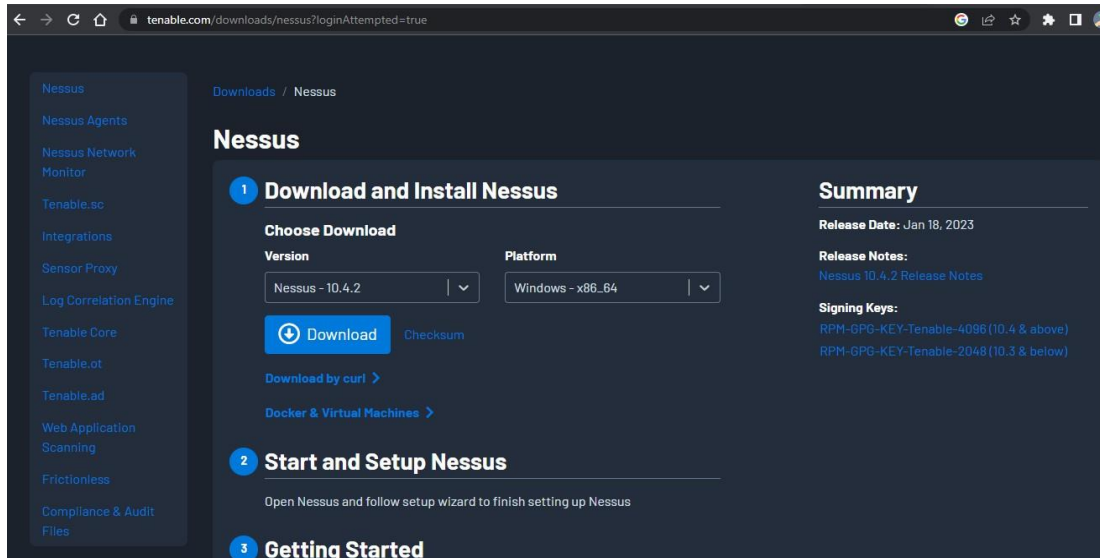
The following experiment is done using Nmap tool in root terminal in kali Linux server. I have used all the commands that are available in Nmap tool.



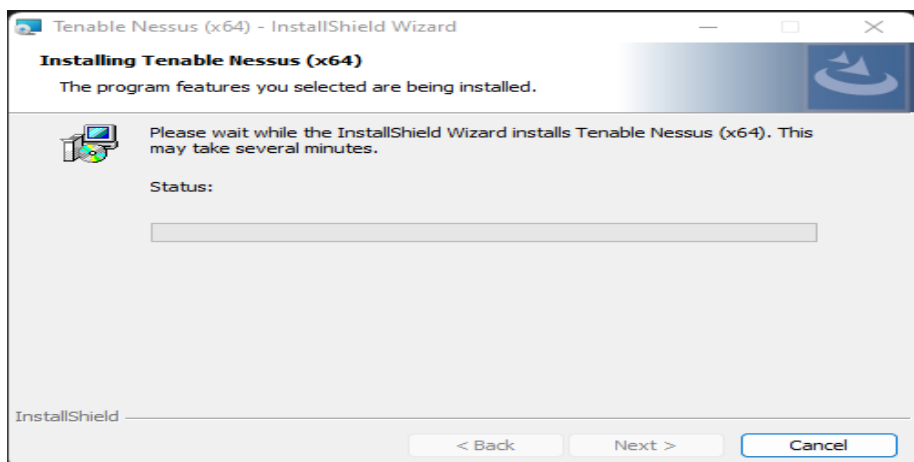
## Exercise No 2: Vulnerability Access Scan Using Nessus

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

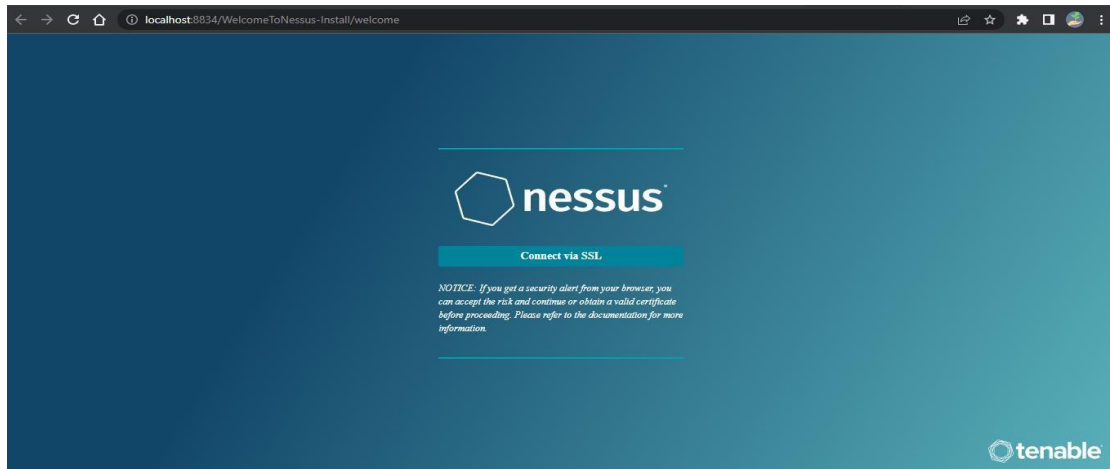
Step 1:- <https://www.tenable.com/downloads/nessus?loginAttempted=true>



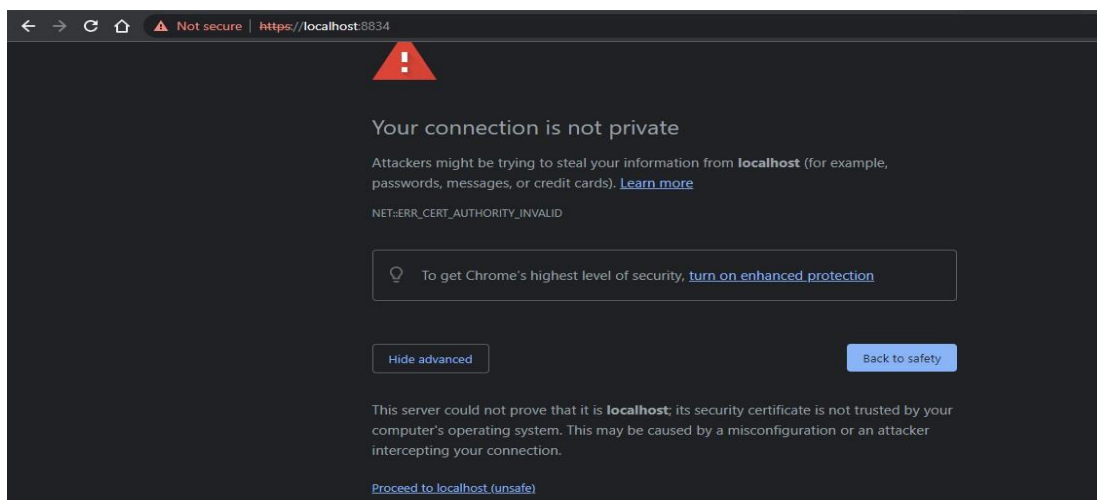
Step 2: Choose your OS and download , install



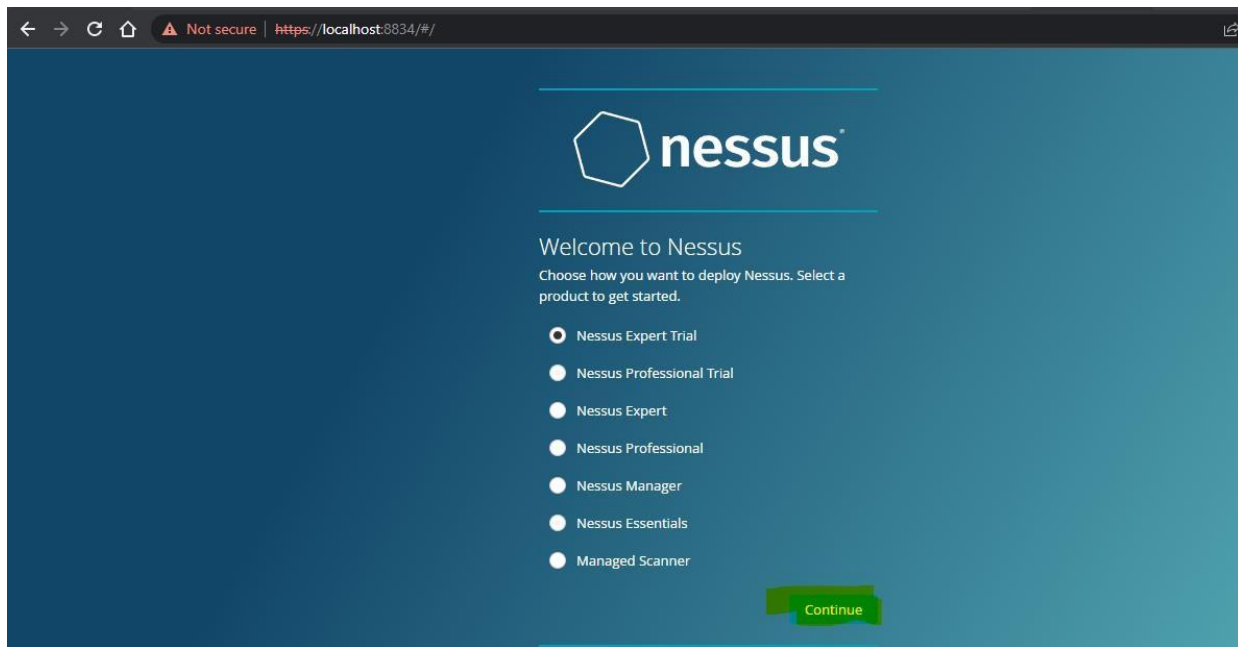
Step 3: Once installation is completed it will open in default browser



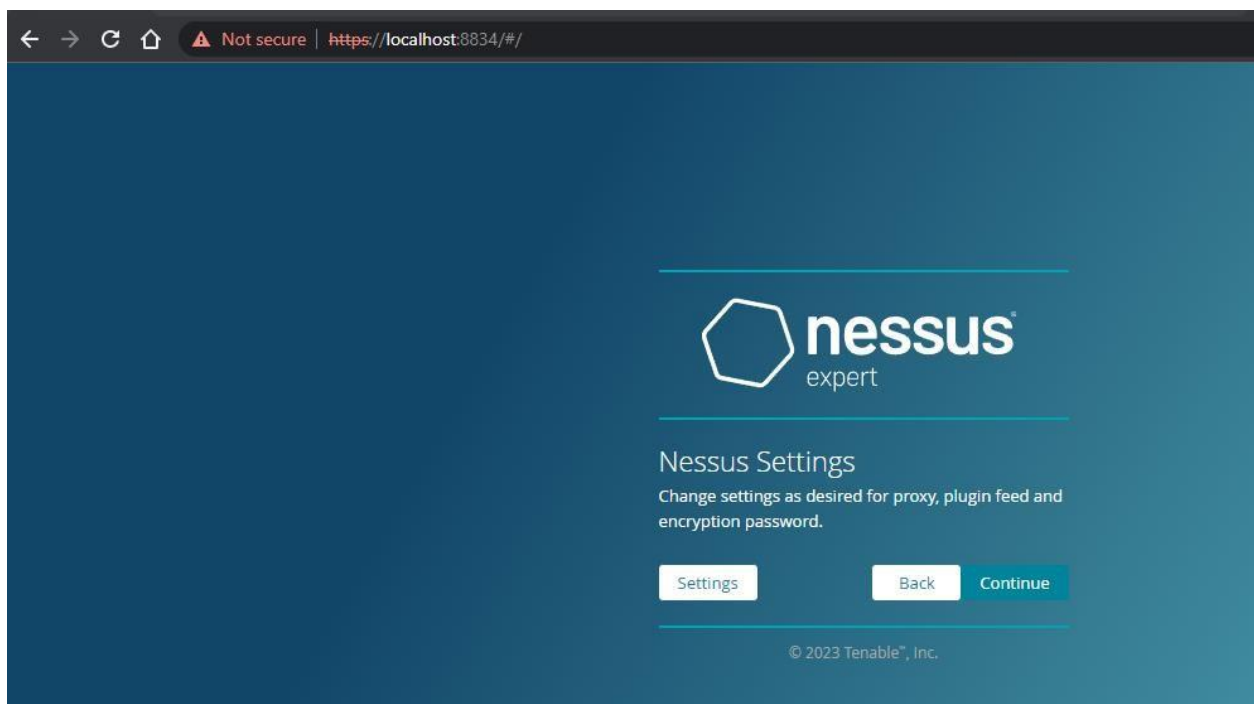
Step 5:- (click on the proceed to local host)



Step 6:- Please choose the Nessus Expert



Step 7: Click on continue



Step 8:- Register with your organizational email id

← → ↻ 🏠 ⚠ Not secure | https://localhost:8834/#/ expert

### Create Account

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

First Name  Last Name

Email

Phone

Title


Company Name

Company Size

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

Step 9:- please note down the activation key

---

← → ↻ 🏠 ⚠ Not secure | https://localhost:8834/#/ 

### Trial License Information

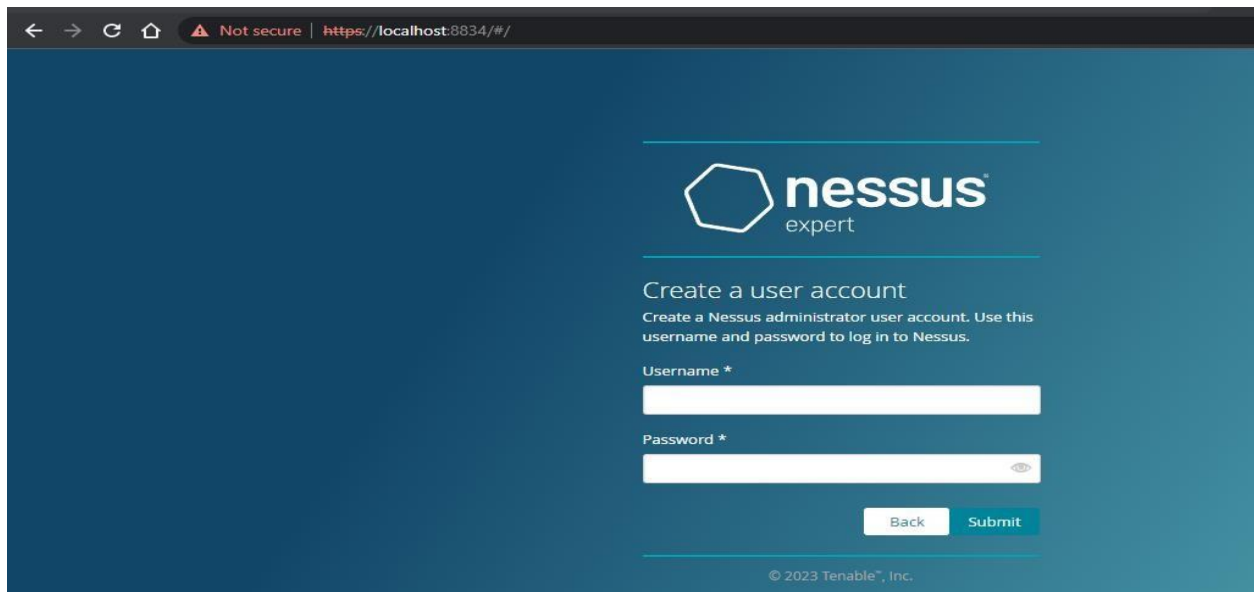
Activation Code: R4A2-DPDT-UVQZ-T53Y

Valid until: 2023-01-28

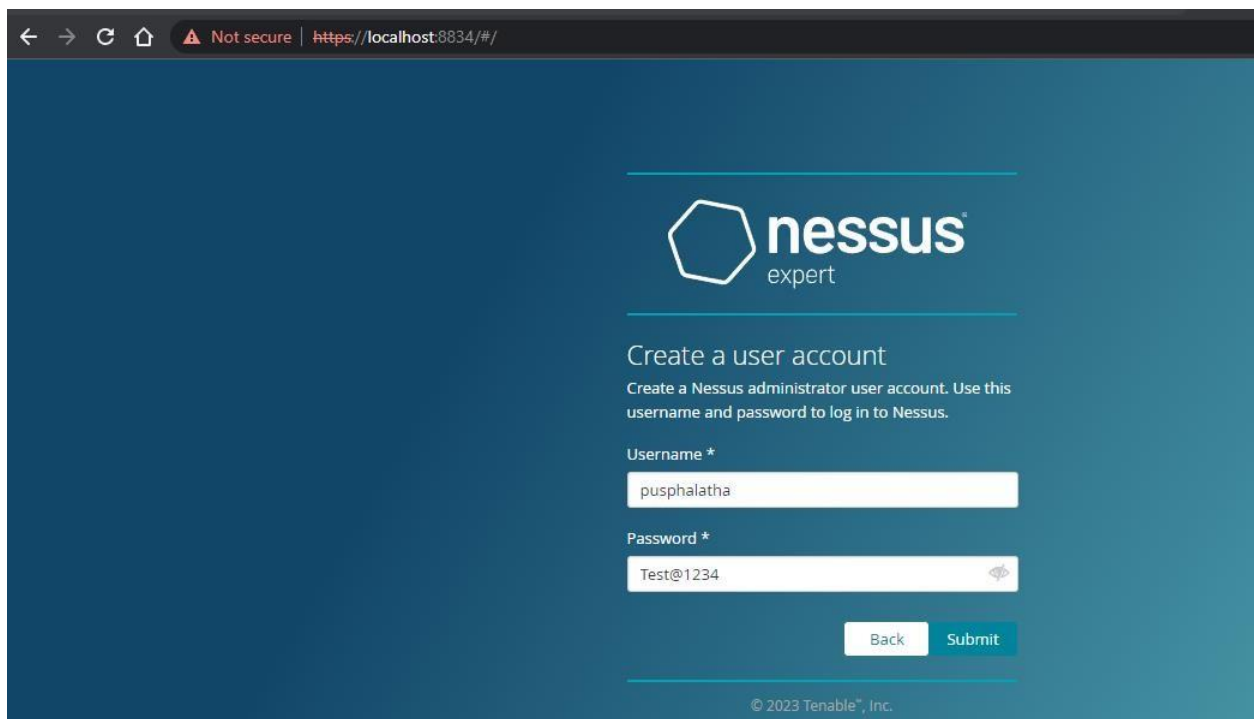
[Continue](#)

© 2023 Tenable™, Inc.

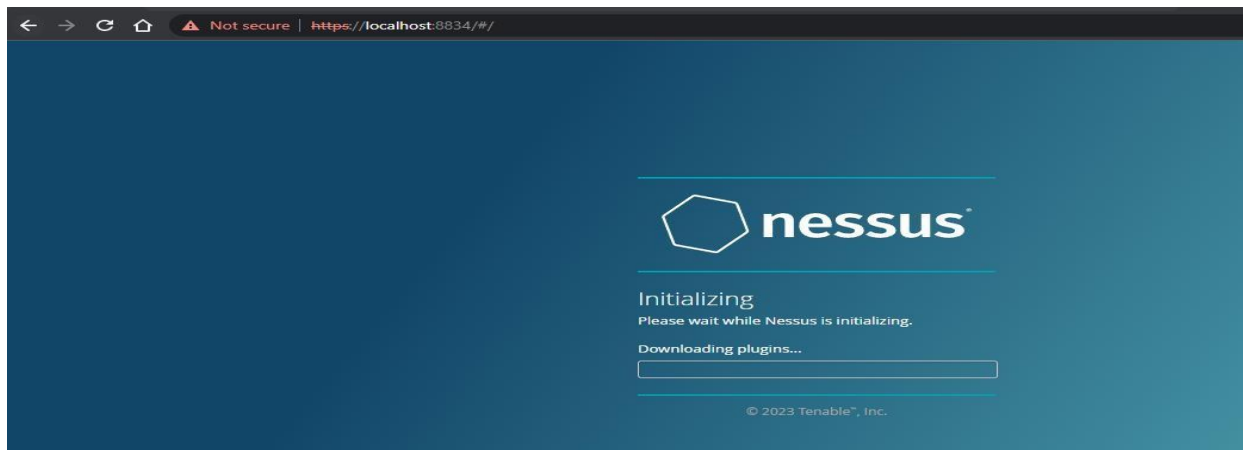
Step 10:- set up your username & password



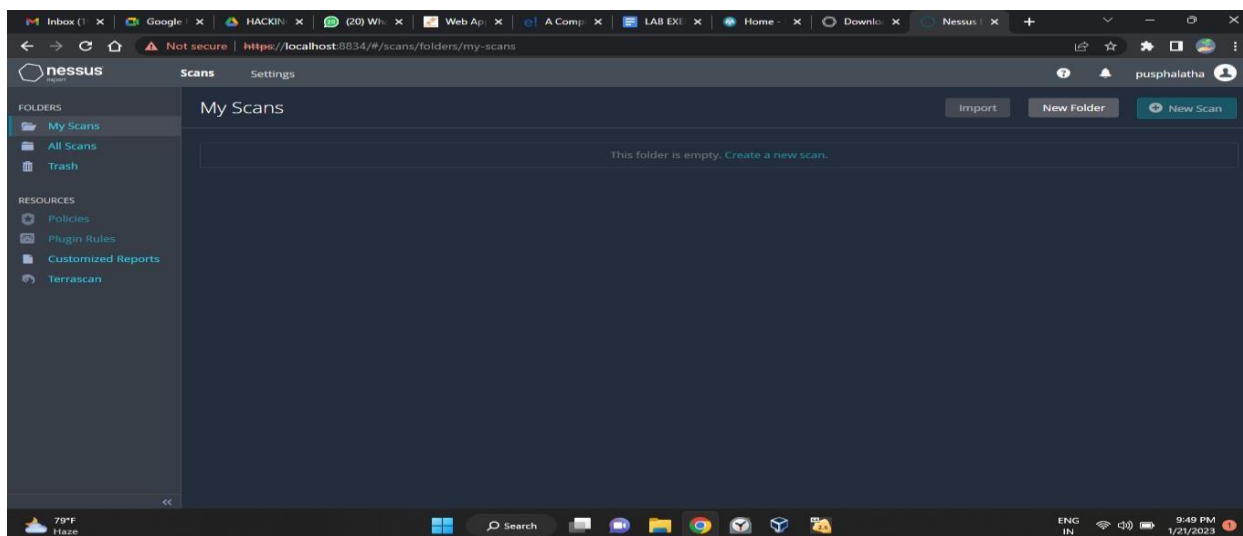
Step 11:-Type username and password



Step 12:- Please wait until download is completed



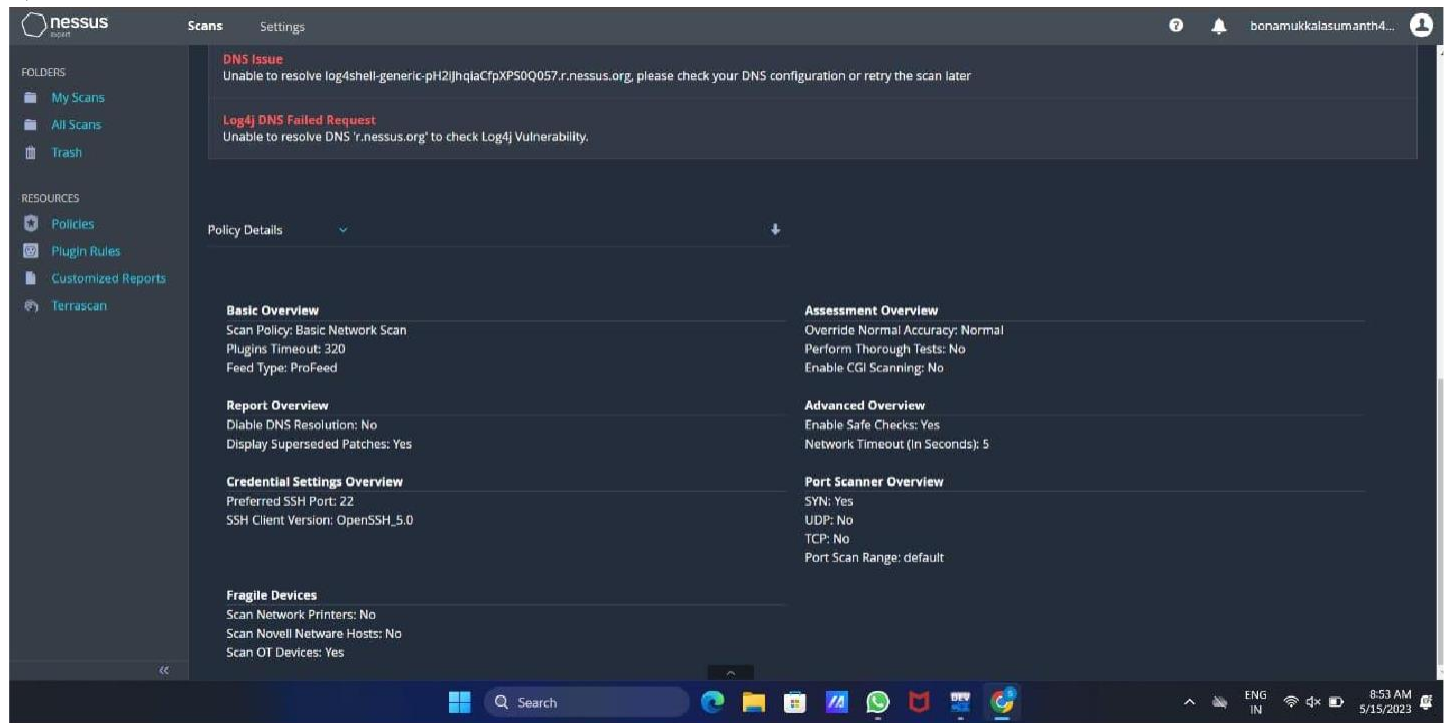
## Step 13: Select My Scans



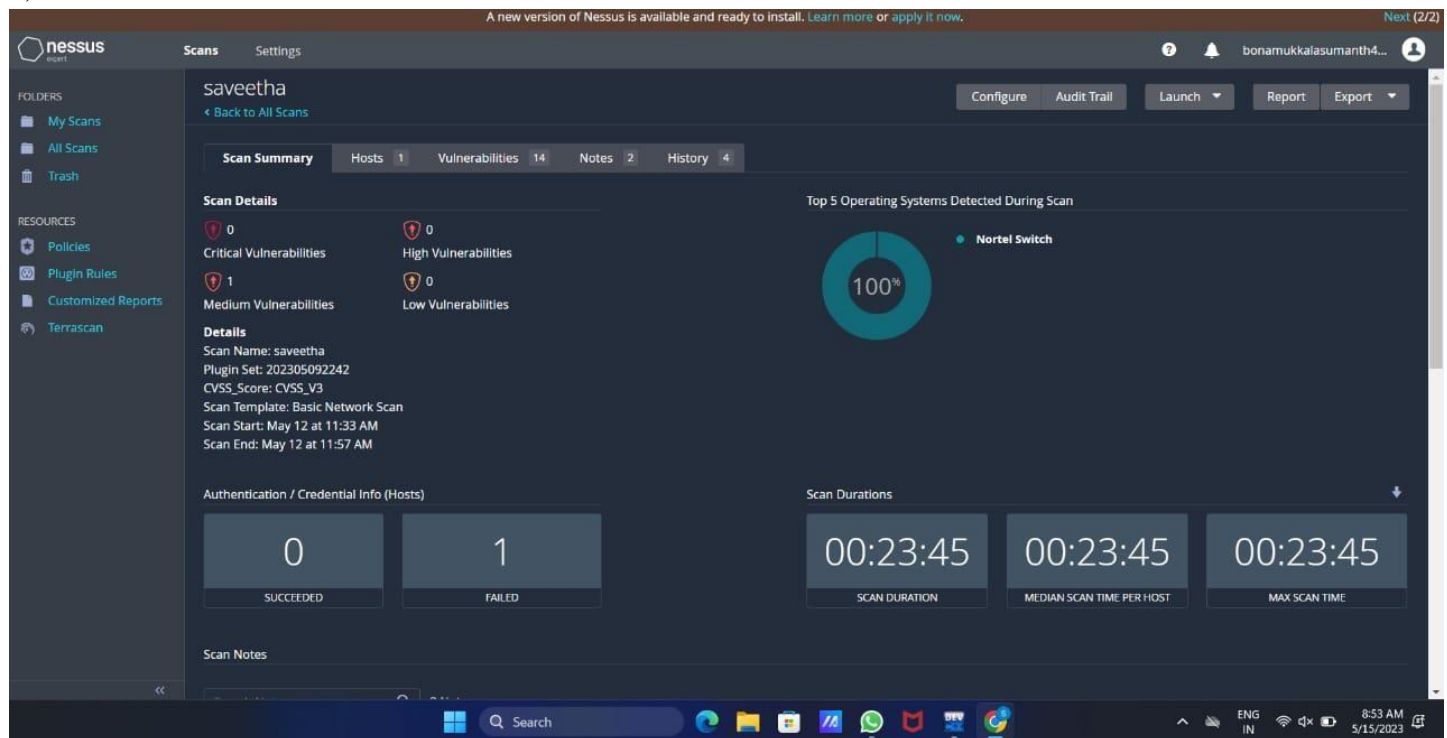


## Output:

1)



2)



## Result:

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

## Exercise No 3: Information gathering using theHarvester

**Aim:** To demonstrate information gathering using theHarvester

**Procedure:**

### STEP 1: Open Terminal in the kali linux

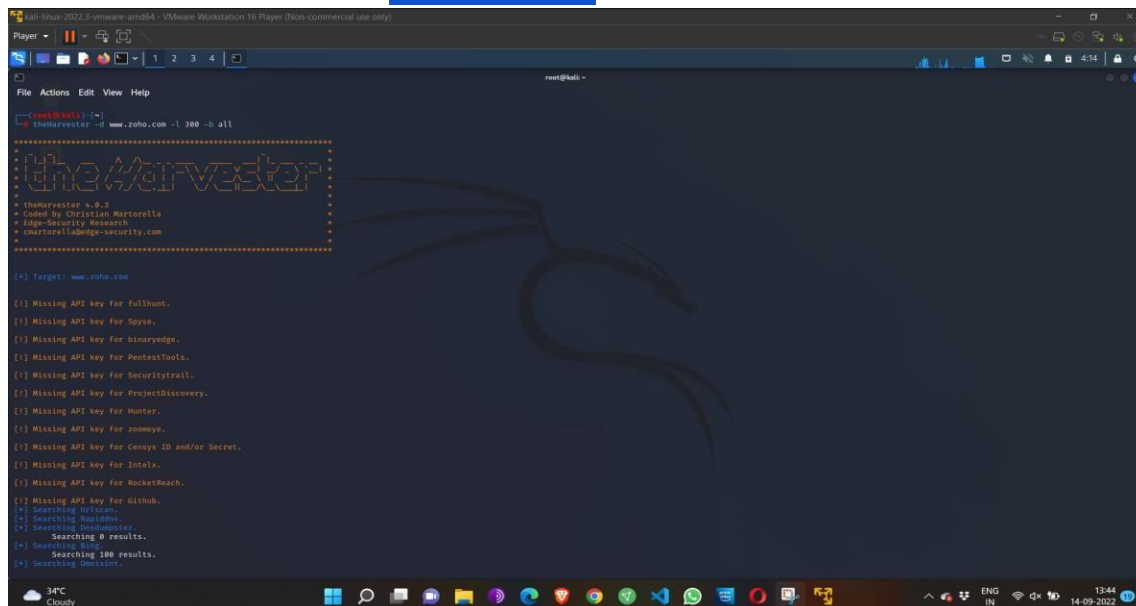
`-d [url]` will be the remote site from which you wants to fetch

`-l` will limit the search for specified number.

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

### STEP 2: Run the following command

**Command:** theHarvester -d [www.zoho.com](http://www.zoho.com) -l 300 -b all



```
kali-linux-2022.2-vmware-usb04 - VMware Workstation 16 Player (Non-commercial use only)
Player
File Actions Edit View Help
root@kali: ~
[+] theHarvester --d www.zoho.com -l 300 -b all

theHarvester
theHarvester 4.0.3
+ Coded By Christian Martorella
+ Edge-Security Research
+ chartwell@edge-security.com

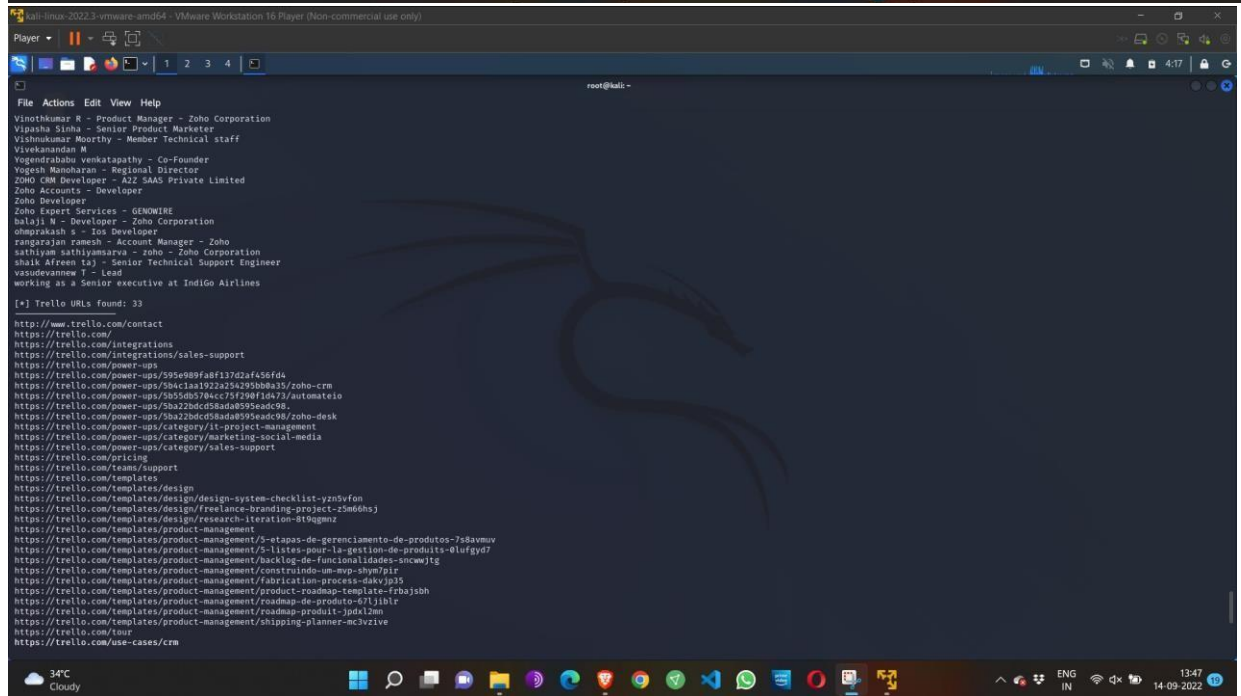
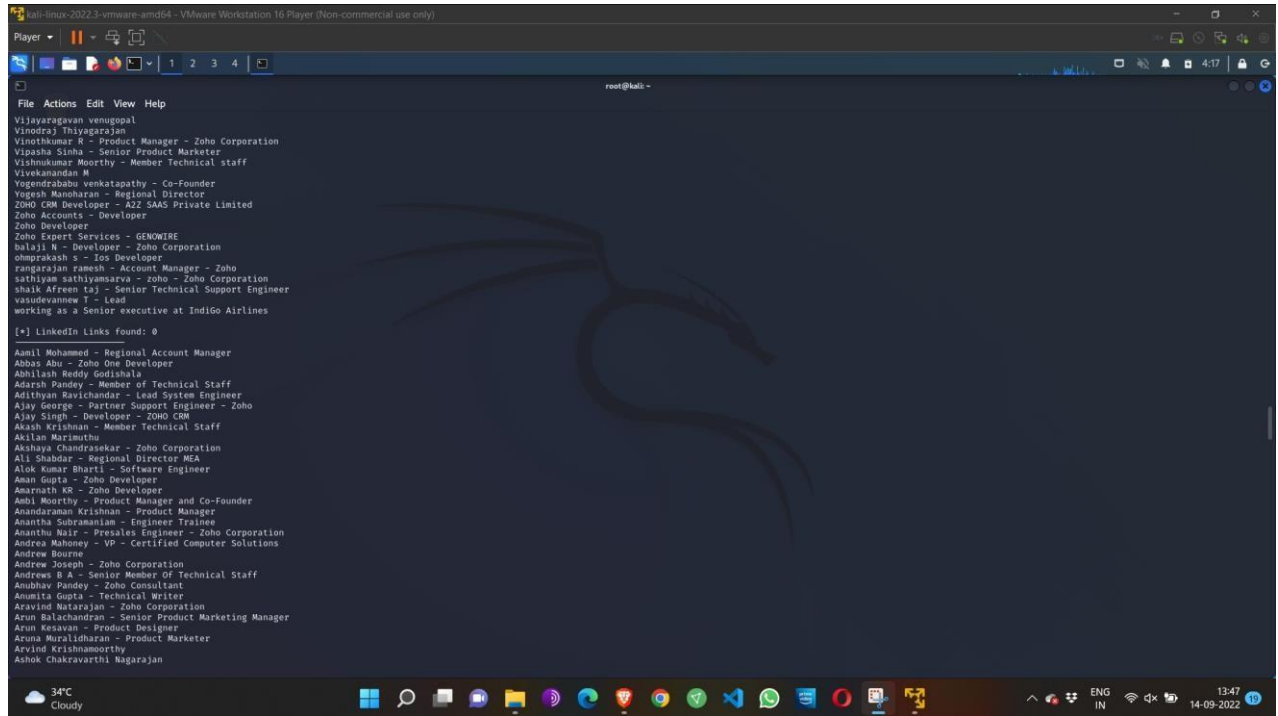
[*] target: www.zoho.com

[!] Missing API key for fullhunt.
[!] Missing API key for Spyse.
[!] Missing API key for binaryedge.
[!] Missing API key for PentestTools.
[!] Missing API key for Securitytrail.
[!] Missing API key for ProjectDiscovery.
[!] Missing API key for Hunter.
[!] Missing API key for Zoomeye.
[!] Missing API key for Censys ID and/or Secret.
[!] Missing API key for Intelx.
[!] Missing API key for RuckitReach.
[!] Missing API key for Github.
[*] Searching 0 results.
[*] Searching 0 results.
[*] Searching 0 results.
[*] Searching 0 results.
[*] Searching 100 results.
[*] Searching 0 results.
```

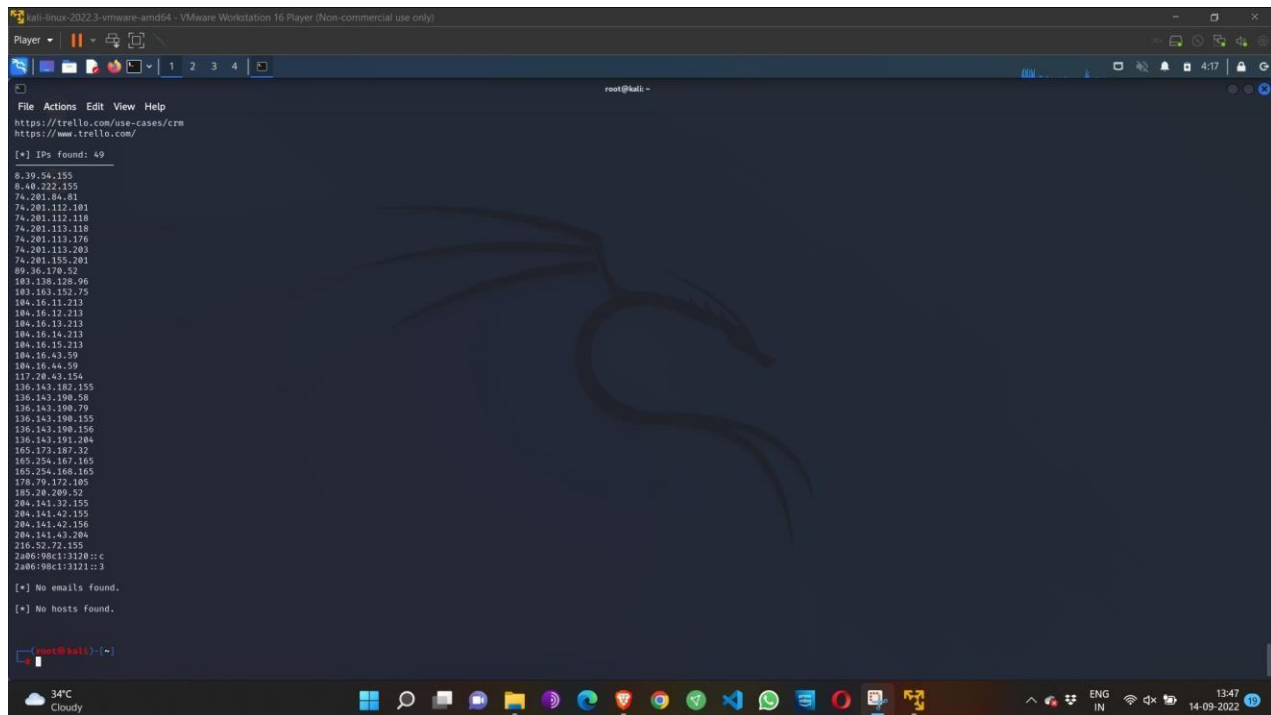


```
kali-linux-2022.3-vmware-amd64 - VMware Workstation 16 Player (Non-commercial use only)
Player
File Actions Edit View Help
AS63949
[*] Interesting Urls found: 25
https://www.zoho.com/
https://www.zoho.com/assist/
https://www.zoho.com/books/
https://www.zoho.com/campaigns/7zsrc=fromproduct
https://www.zoho.com/campaigns/explainer/campaign-view.html
https://www.zoho.com/campaigns/explainer/zcscend.html
https://www.zoho.com/cliq/?serviceurl=x2findex.d00zsrc=fromproduct
https://www.zoho.com/cliq/?serviceurl=x2findex.d00zsrc=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/dm/crm/
https://www.zoho.com/emailsender/
https://www.zoho.com/forms/
https://www.zoho.com/inswica/?utm_source=20butn_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&38ireft=ohome
https://www.zoho.com/rf/dex/
https://www.zoho.com/report-abuse/
https://www.zoho.com/salesiq/
https://www.zoho.com/survey/
[*] No Twitter users found.
[*] LinkedIn Users found: 292
Aamir Mohammed - Regional Account Manager
Abbas Abu - Zoho One Developer
Abhilash Reddy Godishala
Adarsh Pandey - Member of Technical Staff
Adithyan Ravichandrar - Lead System Engineer
Ajay George - Partner Support Engineer - Zoho
Ajay Singh - Developer - Zoho CRM
Akash Krishnan - Member Technical Staff
Akilan Marimuthu
Akshaya Chandrasekar - Zoho Corporation
Ali Shabdar - Regional Director MEA
Alok Kumar Bharti - Software Engineer
Aman Gupta - Zoho Developer
Amarnath KR - Zoho Developer
Ambi Moorthy - Product Manager and Co-Founder
Anandaraman Krishnan - Product Manager
```

```
kali-linux-2022.3-vmware-amd64 - VMware Workstation 16 Player (Non-commercial use only)
Player
File Actions Edit View Help
Ajay Singh - Developer - Zoho CRM
Akash Krishnan - Member Technical Staff
Akilan Marimuthu
Akshaya Chandrasekar - Zoho Corporation
Ali Shabdar - Regional Director MEA
Alok Kumar Bharti - Software Engineer
Aman Gupta - Zoho Developer
Amarnath KR - Zoho Developer
Ambi Moorthy - Product Manager and Co-Founder
Anandaraman Krishnan - Product Manager
Anantha Subramaniam - Engineer Trainee
Anantho Nair - Presales Engineer - Zoho Corporation
Andrea Mahoney - VP - Certified Computer Solutions
Andrew Bourne
Andrew Joseph - Zoho Corporation
Andrews B A - Senior Member Of Technical Staff
Anubhav Pandey - Zoho Consultant
Anumita Gupta - Technical Writer
Aravind Natarajan - Zoho Corporation
Arun Balachandran - Senior Product Marketing Manager
Arun Kesavan - Product Designer
Aruna Muralidharan - Product Marketer
Arvind Krishnamoorthy
Ashok Chakravarthi Nagarajan
Ashok Kumar
Ashwin P Sharma - Lead - Zoho CRM SME
Avaninth B - Software Developer - Zoho
Azarudeen M
Badr Narayan - Senior Technical Support Engineer
Bala Ganesh
Bala Krishnan - Product Marketer
Bala Sundar - Member Technical Staff
Bala Venkatramani
Balaji Jayaraman - Product Manager
Barath Kumar Ramesh - Member Leadership Staff
Bashirul Haque Faisal - Zoho Consultant
Bernadita Samuel - Zoho Developer
Bharath Kumar
Bharathi Ambazhagan - Member Technical Staff
Calvin Jasher - Quality Analyst- Zoho CRM Support
Carla Garcia
Chakravarthi Radhakrishnan - Zoho Corporation
Chandru Jayapalan - Zoho Corporation
Charles Lazaro
Chetan K. - Zoho CRM Consultant - Regal Infonet
Chitrapandian Nachappan - Senior Product Director
Clarence Rozaris - Director of Product Management
Cynthia A - Product Management
G Jayaraj - Visual Designer
DEVENDRA KUSHMAN - Zoho Developer
David Elkins - Head of Content Review
Deepak Rv - Enterprise Support Engineer - Zoho
```







Step 4: run this command “**theHarvester -d [www.zoho.com](https://www.zoho.com) -l 300 -b all -f test**” and hit enter to export the result as html file and xml file

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



## **Output:**

1)

```
[*] Searching Omnisint.
[*] ASNS found: 1
AS53831
[*] Interesting Urls found: 1
https://www.saveetha.com/
[*] LinkedIn Links found: 0
[*] IPs found: 4
118.139.175.1
198.185.159.144
199.34.228.77
[*] Emails found: 27
admin@saveetha.com
adminofficer@saveetha.com
admission.medical@saveetha.com
admission.scon@saveetha.com
admission.scpt@saveetha.com
admission.ssl@saveetha.com
admission@saveetha.com
artsadmission@saveetha.com
asso.deanfaculty@saveetha.com
dean.ssm@saveetha.com
enggadmission@saveetha.com
hr.smch@saveetha.com
hr.smch.nts@saveetha.com
hr.smch.ts@saveetha.com
prime@saveetha.com
principal.ahs@saveetha.com
principal.scot@saveetha.com
scadadmission@saveetha.com
schoolofhospitality@saveetha.com
[*] No hosts found.
```

## **Result:**

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

## Exercise No 4 - Open Source Intelligence Gathering Using OSRFramework

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

**Procedure:**

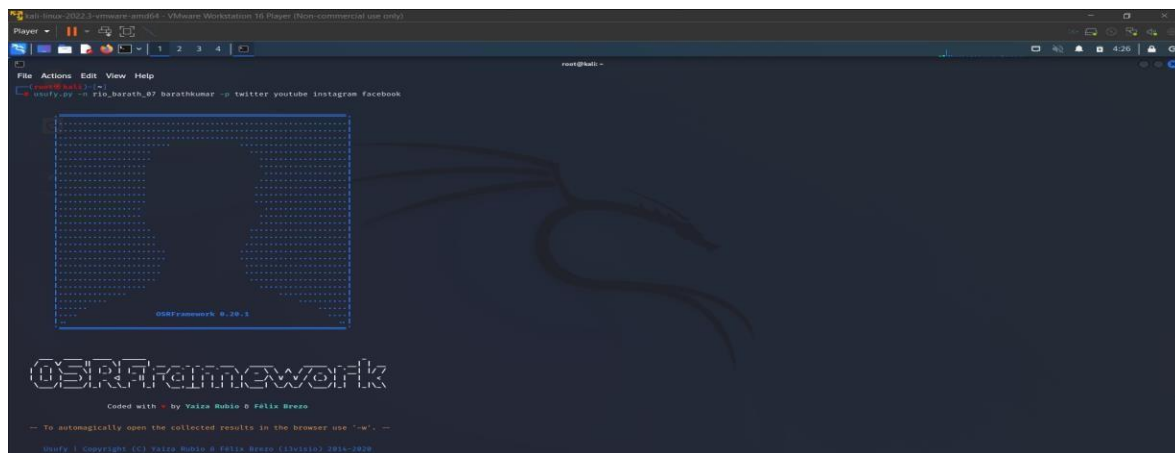
Step 1: Log into kali linux machine

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

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

**Command:**

Usufy.py -n <Target username or profile name> -p twitterfacebook youtube



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: ~
File Actions Edit View Help
Only 1 Copyright (C) 2018 Robin R. Fallis (i3visio) 2018/2018
This program comes with ABSOLUTELY NO WARRANTY. This is free software, and you
are welcome to redistribute it under certain conditions. For additional info,
visit https://www.gnu.org/licenses/agpl-3.0.txt.

2022-09-14 04:25:15.21203 Starting search in 4 platform(s)... Relax!
Press <Ctrl + C> to stop ...

2022-09-14 04:25:41.22129 Results obtained (8):
/usr/lib/python3/dist-packages/pyexcel/deprecated.py:288: UserWarning: Deprecated usage since v0.2.1: Explicit import is no longer required. pyexcel.ext.text is auto imported.
  warnings.warn
Objects recovered (2022-9-14_4h25m):
+-----+-----+-----+
| com.i3visio.uri | com.i3visio.alias | com.i3visio.platform |
+-----+-----+-----+
| https://www.youtube.com/user/rin_harath_07/about | rin_harath_07 | Youtube |
| https://www.facebook.com/rin.harath.07 | rin_harath_07 | Facebook |
| http://www.instagram.com/rin_harath_07 | rin_harath_07 | Instagram |
| http://twitter.com/rin_harath_07 | rin_harath_07 | Twitter |
| https://www.youtube.com/user/harathkumar/about | harathkumar | Youtube |
| https://www.facebook.com/harathkumar | harathkumar | Facebook |
| http://www.instagram.com/harathkumar | harathkumar | Instagram |
| http://twitter.com/harathkumar | harathkumar | Twitter |
+-----+-----+-----+

2022-09-14 04:25:41.208991 You can find all the information here:
./genlive.sh

2022-09-14 04:25:41.397468 Finishing execution ...
Total time consumed: 0:00:00.185075
Average seconds/query: 1.54626875 seconds

Did something go wrong? Is a platform reporting false positives? Do you need to
integrate a new one and you don't know how to start? Then, you can always place
an issue in the Github project!
https://github.com/i3visio/i3visioframework/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

1)

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

# OSKAR COMPANY

Coded with ❤ by **Yaiza Rubio** & **Félix Brezo**

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

2)

```
visit <https://www.gnu.org/licenses/agpl-3.0.txt>.
2023-05-14 20:19:31.116670      Starting search in 4 platform(s)... Relax!
      Press <Ctrl + C> to stop...

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

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

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

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

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

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

## Result:

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

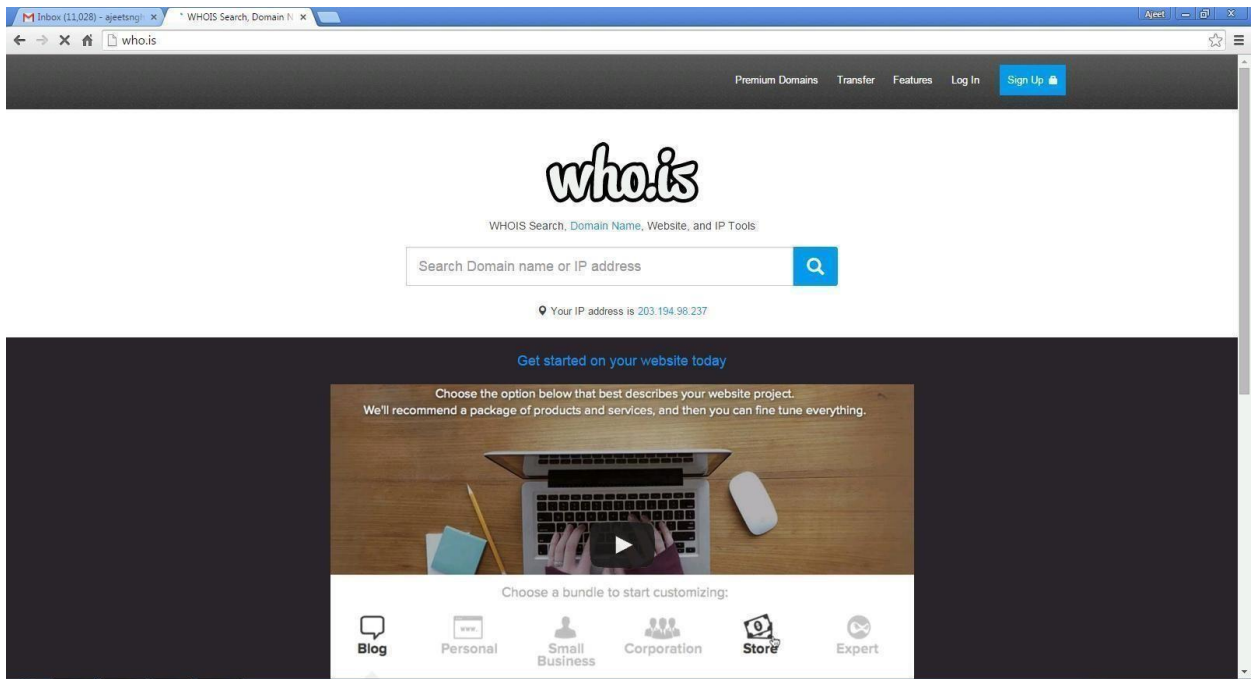


## Exercise NO 5: Use Google and Whois for Reconnaissance.

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

**Procedure:**

Step1: Open the WHO.is website



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

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



who.is

Search for domains or IP addresses...

Q

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

## 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=9.07 ms  
64 bytes from 198.185.159.144: icmp_seq=5 ttl=47 time=9.15 ms  
  
--- saveetha.com ping statistics ---  
5 packets transmitted, 5 received, 0% packet loss, time 4005ms  
rtt min/avg/max/mdev = 8.832/8.975/9.158/0.138 ms
```

### Traceroute

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

who.is

Search for domains or IP addresses...

Q

Premium Domains

Transfer

Features

Login

Sign Up

whois/whois/saveetha.com

saveetha.com

whois information

Whois

DNS Records

Diagnostics

cache expires in and 0 seconds

refresh

Registrar Info

Name

PDR Ltd. d/b/a PublicDomainRegistry.com

Whois Server

whois.publicdomainregistry.com

Referral URL

www.publicdomainregistry.com

Status

clientTransferProhibited https://icann.org/epp/clientTransferProhibited

Important Dates

Expires On

2023-06-18

Registered On

2001-06-18

Updated On

2022-05-27

Name Servers

ns51.domaincontrol.com

97.74.105.26

ns52.domaincontrol.com

173.201.73.26

Similar Domains

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

Registrar Data

We will display stored WHOIS data for up to 30 days

refresh

Make Private Here

Registrant Contact Information:

Name

Dr. N.R.Veeraiyan

Organization

Saveetha Dental College & Hosp.

Address

Saveetha University, Saveetha Nagar, Thandian Campus

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

Find the perfect domain at

Name.com

Site Status

Status

Active

Server Type

Squarespace

Suggested Domains for saveetha.com

☐ save-etha.live

\$2.99

☐ saveethas.live

\$2.99

☐ freeetha.live

\$2.99

☐ rescueetha.live

\$2.99

☐ guardetha.live

\$2.99

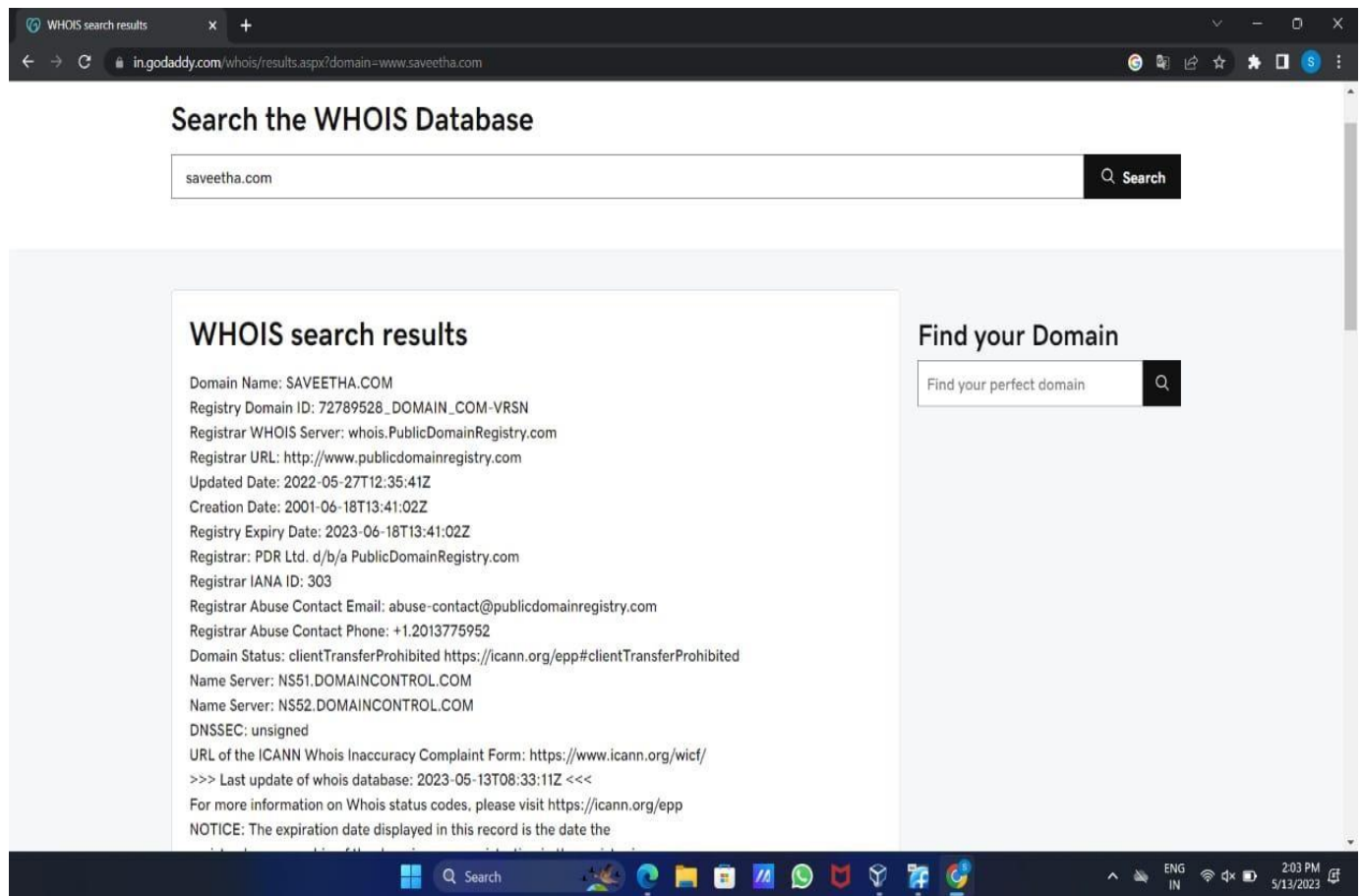
Purchase Selected Domains

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 address bar displaying "in.godaddy.com/whois/results.aspx?domain=www.saveetha.com". The page title is "Search the WHOIS Database". A search bar contains the text "saveetha.com" and a "Search" button. Below the search bar, the "WHOIS search results" are displayed for the domain "SAVEETHA.COM". The results include the following information:

- 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](mailto:abuse-contact@publicdomainregistry.com)
- Registrar Abuse Contact Phone: +1.2013775952
- Domain Status: clientTransferProhibited <https://icann.org/epp#clientTransferProhibited>
- Name Server: NS51.DOMAINCONTROL.COM
- Name Server: NS52.DOMAINCONTROL.COM
- DNSSEC: unsigned
- URL of the ICANN Whois Inaccuracy Complaint Form: <https://www.icann.org/wicf/>
- >>> Last update of whois database: 2023-05-13T08:33:11Z <<<
- For more information on Whois status codes, please visit <https://icann.org/epp>
- NOTICE: The expiration date displayed in this record is the date the

To the right of the search results, there is a section titled "Find your Domain" with a search bar containing the text "Find your perfect domain" and a search button.

## Result:

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

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

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

### Procedure:

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

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

C:\Users\barat>tracert saveetha.com

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

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

Trace complete.
```

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

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

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

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

### Step 3: Type ifconfig command

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

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

### Step 4: Type netstat command

```
C:\Users\singh>netstat

Active Connections

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

# Output:

1)

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

C:\Users\Sumanth>tracert saveetha.com

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

  0  1  537 ms  4 ms  9 ms  192.168.226.244
  1  2  325 ms  486 ms  600 ms  192.168.29.10
  2  3  254 ms  *  263 ms  192.168.28.165
  3  4  *  *  *  Request timed out.
  4  5  SumanthReddy [192.168.226.91] reports: Destination host unreachable.

Trace complete.

C:\Users\Sumanth>ping 192.185.159.145

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

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

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

2)

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

C:\Users\Sumanth>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet 2:

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

Wireless LAN adapter Local Area Connection* 1:

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

Wireless LAN adapter Local Area Connection* 2:

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

Wireless LAN adapter Wi-Fi:

    Connection-specific DNS Suffix  . : 

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 48-67-188-75:https ESTABLISHED
TCP 192.168.0.57:25090 13-187-21-200:https ESTABLISHED
TCP 192.168.0.57:25100 m320902:https SYN_SENT
TCP 192.168.0.57:25101 155:https ESTABLISHED
TCP 192.168.0.57:25103 183-56-230-154:https ESTABLISHED
TCP 192.168.0.57:25106 m320902:https SYN_SENT
TCP 192.168.0.57:25109 443:https ESTABLISHED
```



3)

The screenshot shows a Windows 10 desktop with a Command Prompt window open. The Command Prompt displays the following network configuration:

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

Below the configuration, the user has entered the command `netstat`, and the output shows active connections:

```
Active Connections

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

The desktop background is a blue abstract image. The taskbar at the bottom shows the Start button, a search bar, and several pinned applications including VLC media player, WhatsApp, and qBittorrent. The system tray on the right shows the date and time as 2:12 PM on 5/13/2023.

## Result:

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

## Exercise No 7:VULNERABILITY ANALYSIS - CGI Scanning with Nikto

**Aim:**To perform vulnerability Analysis using CGI Scanning with Nikto

### Procedure:

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

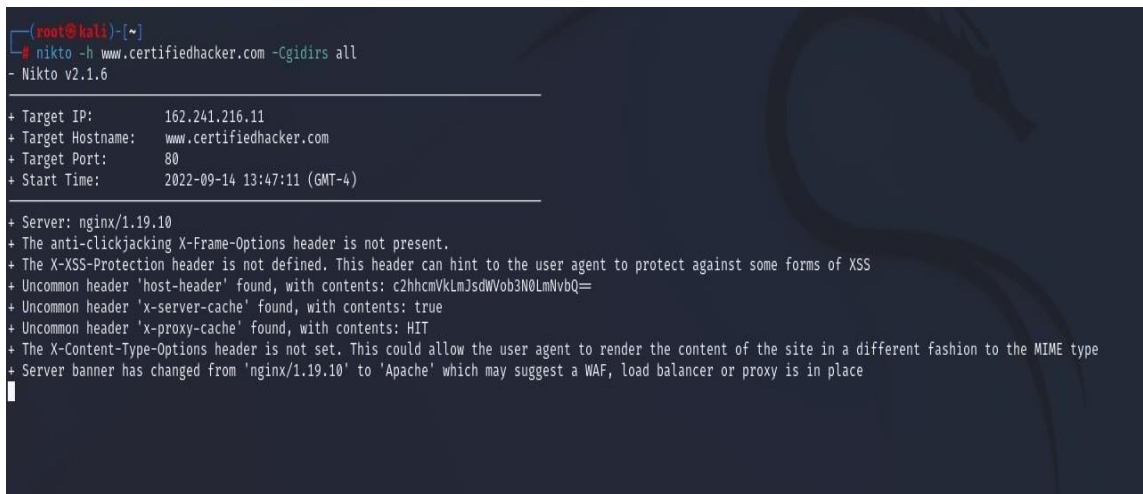
Step 2: Type nikto -h <website> Tuning x and press enter



```
root@kali: ~  
File Actions Edit View Help  
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

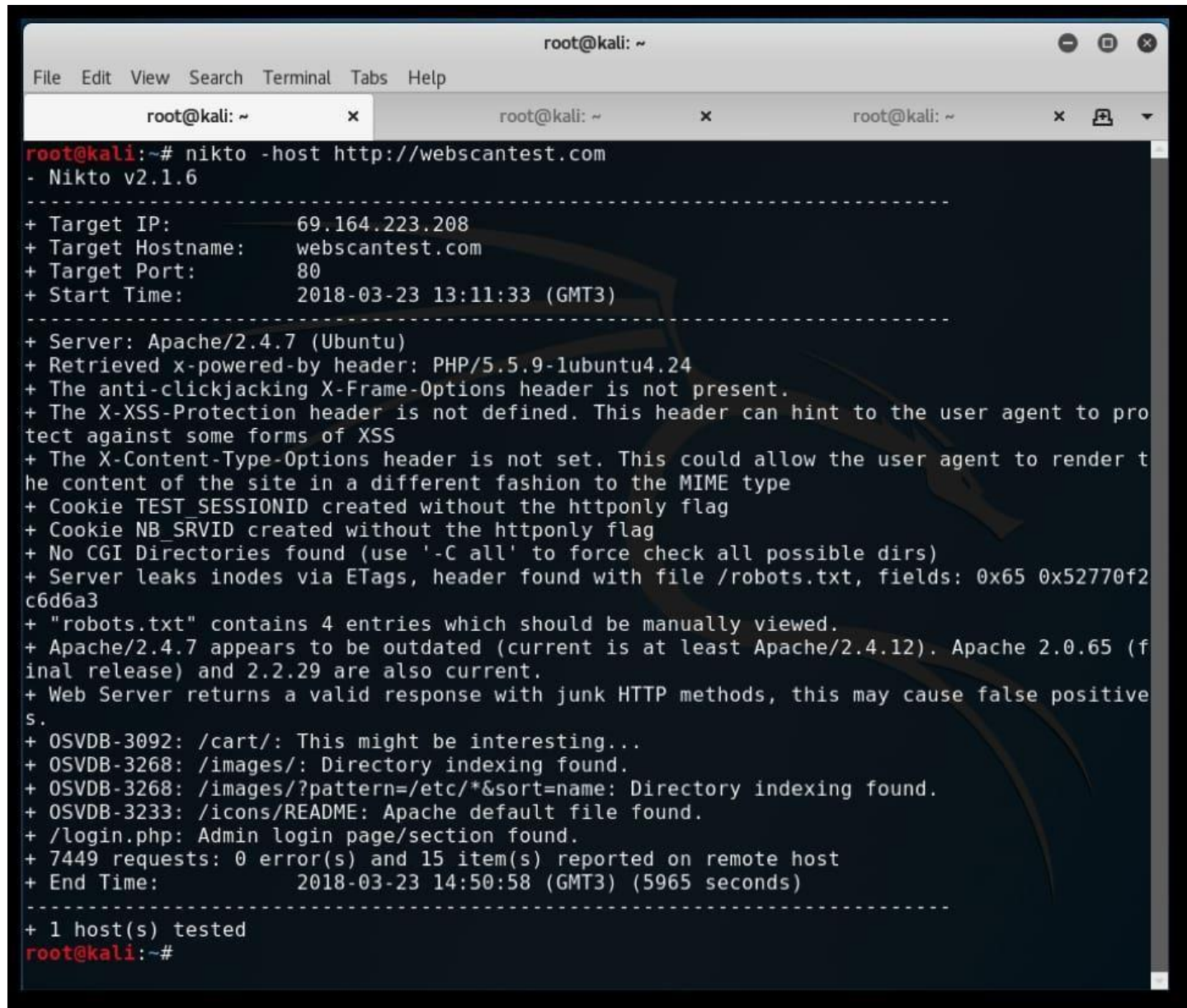


```
root@kali:~  
# nikto -h www.certifiedhacker.com -Cgidirs all  
- Nikto v2.1.6  
  
+ Target IP: 162.241.216.11  
+ Target Hostname: www.certifiedhacker.com  
+ Target Port: 80  
+ Start Time: 2022-09-14 13:47:11 (GMT-4)  
  
+ Server: nginx/1.19.10  
+ The anti-clickjacking X-Frame-Options header 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: c2hhcmVVLmJsdWVob3N0LmVvbQ==  
+ 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 0x52770f2c6d6a3  
+ "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:

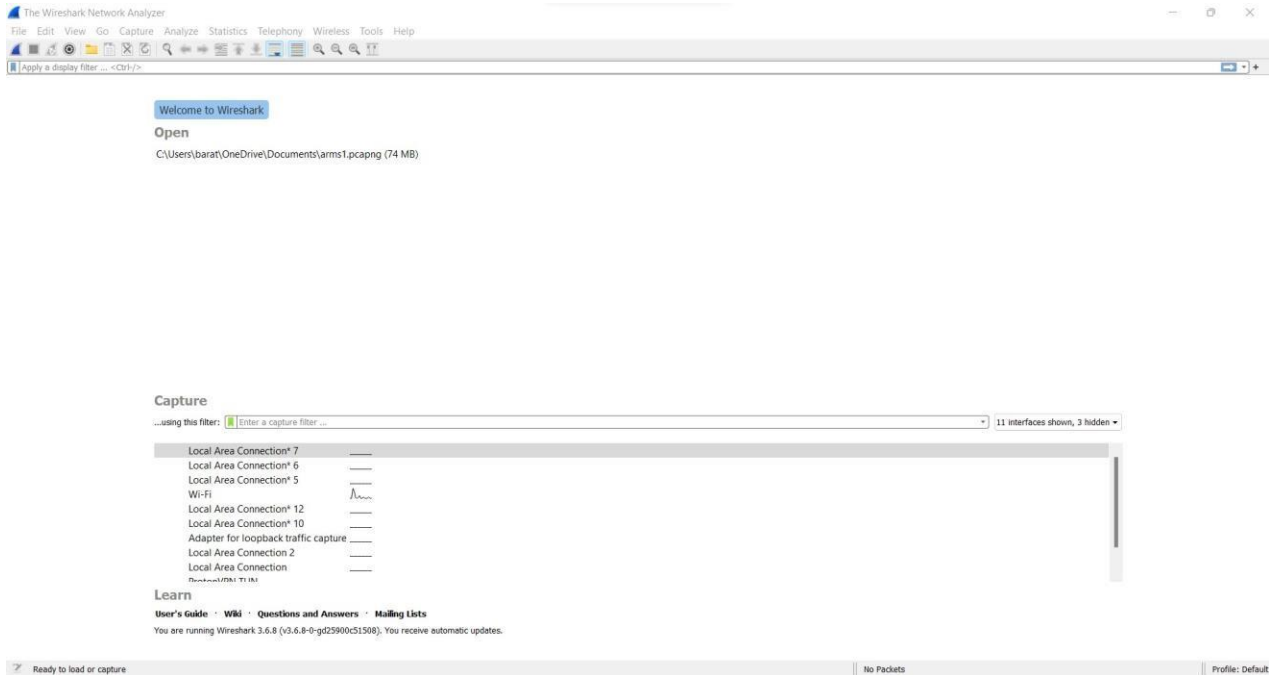
The above experiment is about VULNERABILITY ANALYSIS - CGI Scanning with Nikto. We can retrieve information like server name, headers and etc. This is done in root terminal using kali linux OS.

## Exercise No 8: WireShark sniffer

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

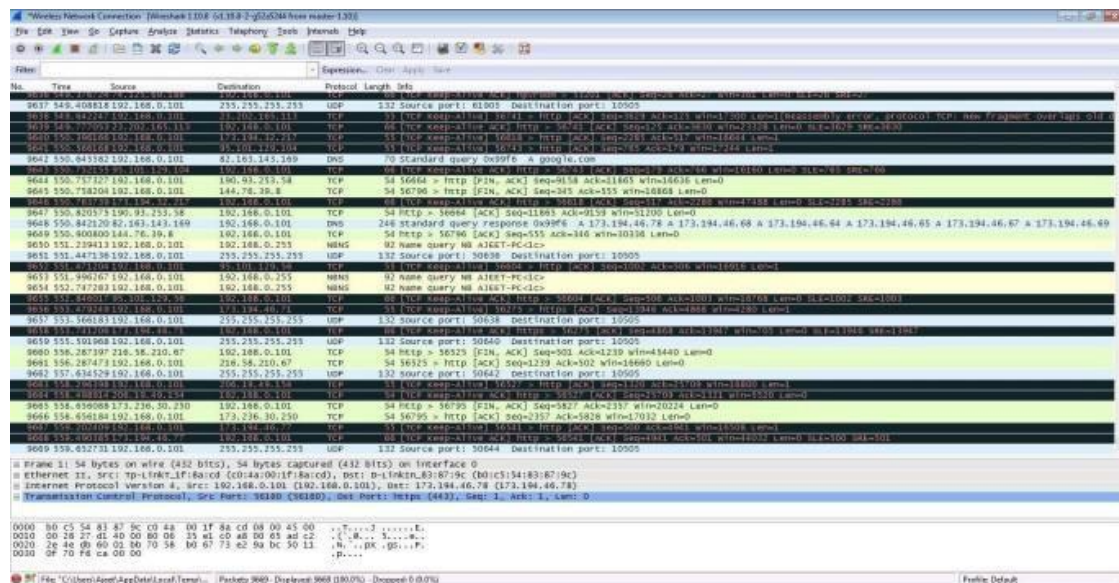
**Procedure:**

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





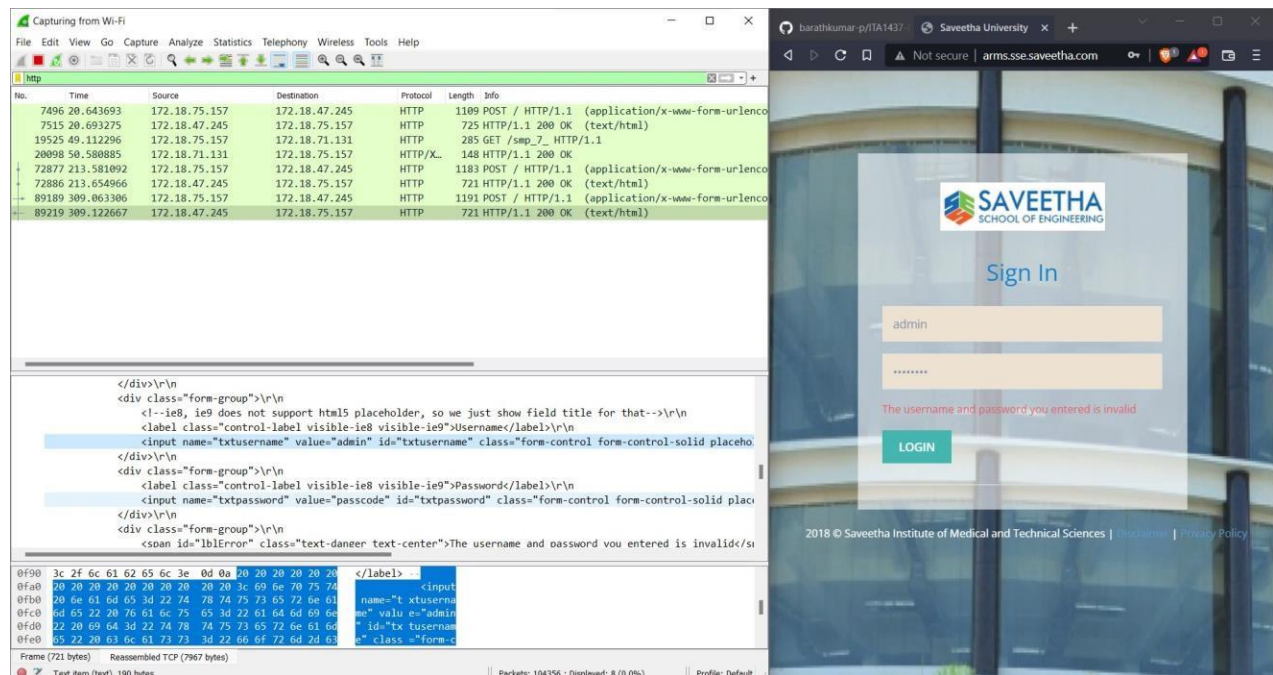
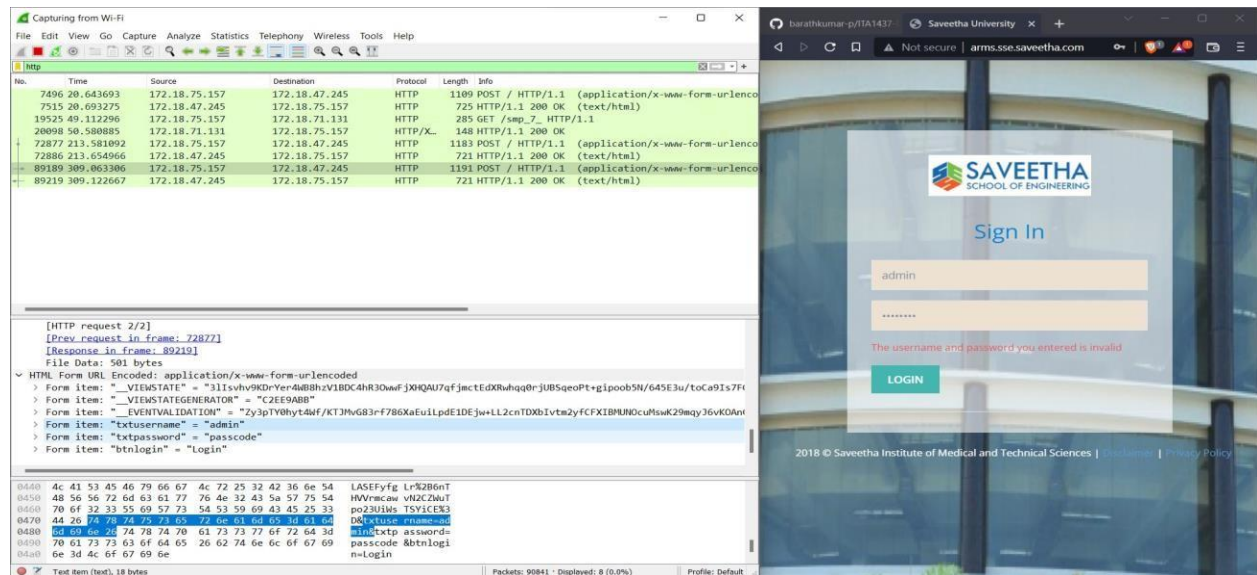
Step 4: Open a website in a new window and enter the user id and password. Register if needed.

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

## Output:

1)

The screenshot displays a network traffic analysis using Wireshark on the left and a web browser (Google Chrome) on the right. The Wireshark interface shows a list of captured packets, with the selected packet (No. 11370) expanded to show its details. The details pane highlights the 'Hypertext Transfer Protocol' section, revealing an HTML form URL encoded as 'application/x-www-form-urlencoded'. The form data includes a 'txtusername' field with the value 'koppiahraja sir' and a 'txtpassword' field with the value 'ethical hacker'. The browser window on the right shows the 'Sign In' page of the Saveetha University website, with the 'LOGIN' button highlighted. The browser's address bar shows the URL 'arms.sse.saveetha.com'.

No.	Time	Source	Destination	Protocol	Length	Info
5782	35.008224	172.18.33.246	172.18.47.245	HTTP	545	GET /appauth.aspx HTTP/1.1
5932	35.206932	172.18.47.245	172.18.33.246	HTTP	293	HTTP/1.1 200 OK (text/html)
6015	35.341078	172.18.33.246	172.18.47.245	HTTP	513	GET /favicon.ico HTTP/1.1
6035	35.365551	172.18.47.245	172.18.33.246	HTTP	1459	HTTP/1.1 404 Not Found (text/html)
6324	38.899383	172.18.33.246	13.107.4.52	HTTP	208	GET /connecttest.txt HTTP/1.1
6343	38.930002	13.107.4.52	172.18.33.246	HTTP	631	HTTP/1.1 200 OK (text/plain)
7783	54.115450	172.18.33.246	13.107.4.52	HTTP	208	GET /connecttest.txt HTTP/1.1
7786	54.135851	13.107.4.52	172.18.33.246	HTTP	631	HTTP/1.1 200 OK (text/plain)
9298	78.661157	172.18.33.246	13.107.4.52	HTTP	208	GET /connecttest.txt HTTP/1.1
9303	78.743046	13.107.4.52	172.18.33.246	HTTP	631	HTTP/1.1 200 OK (text/plain)
10394	90.499160	172.18.33.246	13.107.4.52	HTTP	208	GET /connecttest.txt HTTP/1.1
10411	90.541139	13.107.4.52	172.18.33.246	HTTP	631	HTTP/1.1 200 OK (text/plain)
11370	98.961604	172.18.33.246	172.18.47.245	HTTP	1269	POST /appauth.aspx HTTP/1.1 (application/x-www-form-urlencoded)
11385	98.999116	172.18.47.245	172.18.33.246	HTTP	398	HTTP/1.1 200 OK (text/html)
11882	101.754625	172.18.33.246	13.107.4.52	HTTP	208	GET /connecttest.txt HTTP/1.1
11891	101.784043	13.107.4.52	172.18.33.246	HTTP	631	HTTP/1.1 200 OK (text/plain)
13588	113.763509	172.18.33.246	13.107.4.52	HTTP	208	GET /connecttest.txt HTTP/1.1
13601	113.796629	13.107.4.52	172.18.33.246	HTTP	631	HTTP/1.1 200 OK (text/plain)

Frame 11370: 1269 bytes on wire (10152 bits) captured on interface 0x...  
Ethernet II, Src: AzureWav\_59:cc:37 (e8:fb:60:5d:4e:37), Dst: 172.18.33.246  
Internet Protocol Version 4, Src: 172.18.33.246, Dst: 172.18.47.245  
Transmission Control Protocol, Src Port: 54113, Dst Port: 80  
Hypertext Transfer Protocol  
HTML Form URL Encoded: application/x-www-form-urlencoded  
Form item: "EVENTTARGET" = ""  
Form item: "EVENTARGUMENT" = ""  
Form item: "VIEWSTATE" = "o7n68YgfnFT4" (unencoded-form-value)  
Form item: "VIEWSTATEGENERATOR" = "F8F8F8F8" (unencoded-form-value)  
Form item: "EVENTVALIDATION" = "eF1gO4" (unencoded-form-value)  
Form item: "txtusername" = "koppiahraja sir" (unencoded-form-value)  
Form item: "txtpassword" = "ethical hacker" (unencoded-form-value)  
Form item: "btnlogin" = "Login" (unencoded-form-value)  
Form item: "txtappno" = "" (unencoded-form-value)

## Result:

The current experiment is about Wireshark sniffer. Using Wireshark sniffer, we can capture network traffic and can be able to analyze it. This experiment was executed using Google Chrome.



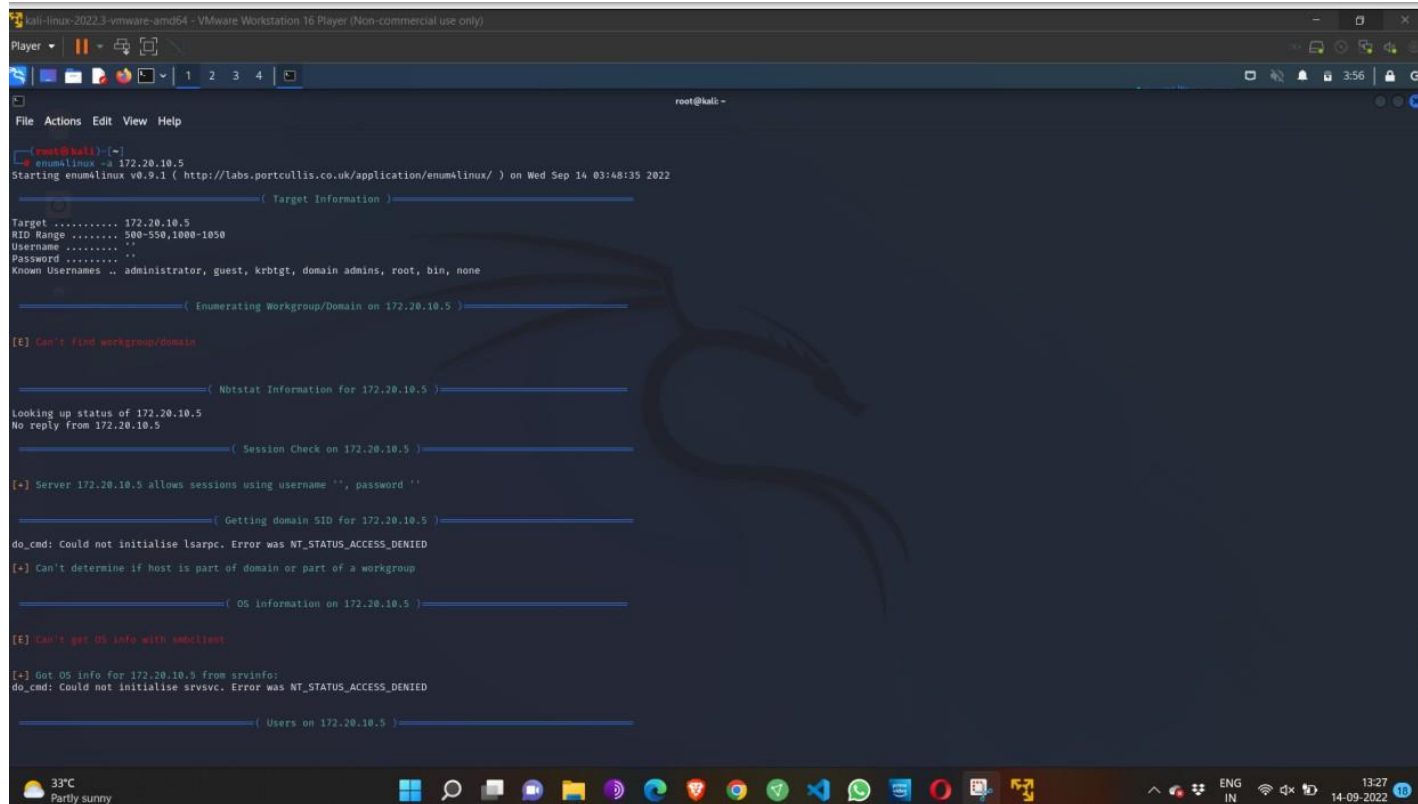
## Ex. No.9 – ENUMERATION - Enumerating information from windows and Samba Host Using Enum4linux

### Requirements:

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

### Procedure:

- 1.Start the kali linux machine and open a terminal window
- 2.Type “sudo apt-get update” command
- 3.Now type enum4linux-h and hit enter to get help options With the help options conduct the enumeration on target machine
- 4.In the terminal window type enum4linux -u -p -U and hit enter to run this tool using the user list options
- 5.Enum4linux starts enumerating the workgroups/domain names first and display the results
- 6.To enumerate all the information Use this command enum4linux -a.



```
root@kali: ~  
* enum4linux -a 172.20.10.5  
Starting enum4linux v0.9.1 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Wed Sep 14 03:48:35 2022  
  
----- ( Target Information ) -----  
Target ..... 172.20.10.5  
RID Range ..... 500-550,1000-1050  
Username ..... ''  
Password ..... ''  
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none  
  
----- ( Enumerating Workgroup/Domain on 172.20.10.5 ) -----  
[E] Can't find workgroup/domain  
  
----- ( Nbtstat Information for 172.20.10.5 ) -----  
Looking up status of 172.20.10.5  
No reply from 172.20.10.5  
  
----- ( Session Check on 172.20.10.5 ) -----  
[+] Server 172.20.10.5 allows sessions using username '', password ''  
  
----- ( Getting domain SID for 172.20.10.5 ) -----  
do_cmd: Could not initialise lsarpc. Error was NT_STATUS_ACCESS_DENIED  
[+] Can't determine if host is part of domain or part of a workgroup  
  
----- ( OS Information on 172.20.10.5 ) -----  
[E] Can't get OS info with smbclient  
[+] Got OS info for 172.20.10.5 from srvinfo:  
do_cmd: Could not initialise srvsvc. Error was NT_STATUS_ACCESS_DENIED  
  
----- ( Users on 172.20.10.5 ) -----
```

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

===== ( 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
```

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

[*] 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
```

## Output:

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

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

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

[E] Can't Find workgroup/domain

===== ( Nbtstat Information for 172.20.10.5 ) =====
Looking up status of 172.20.10.5
No reply from 172.20.10.5

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

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

(root@kali)~[~]
```

## Result:

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

## **EX.NO: 10 BATCH FILE EXECUTION**

### **AIM:**

To create a Windows batch file.

### **PROCEDURE:**

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

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

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

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

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

#### **1.Create a New Text Document:**

A batch file simplifies repeatable computer tasks using the Windows command prompt. Below is an example of a batch file responsible for displaying some text in your command prompt. Create a new BAT file by right-clicking an empty space within a directory and selecting New, then Text Document.

### **1.CODE:**

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

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

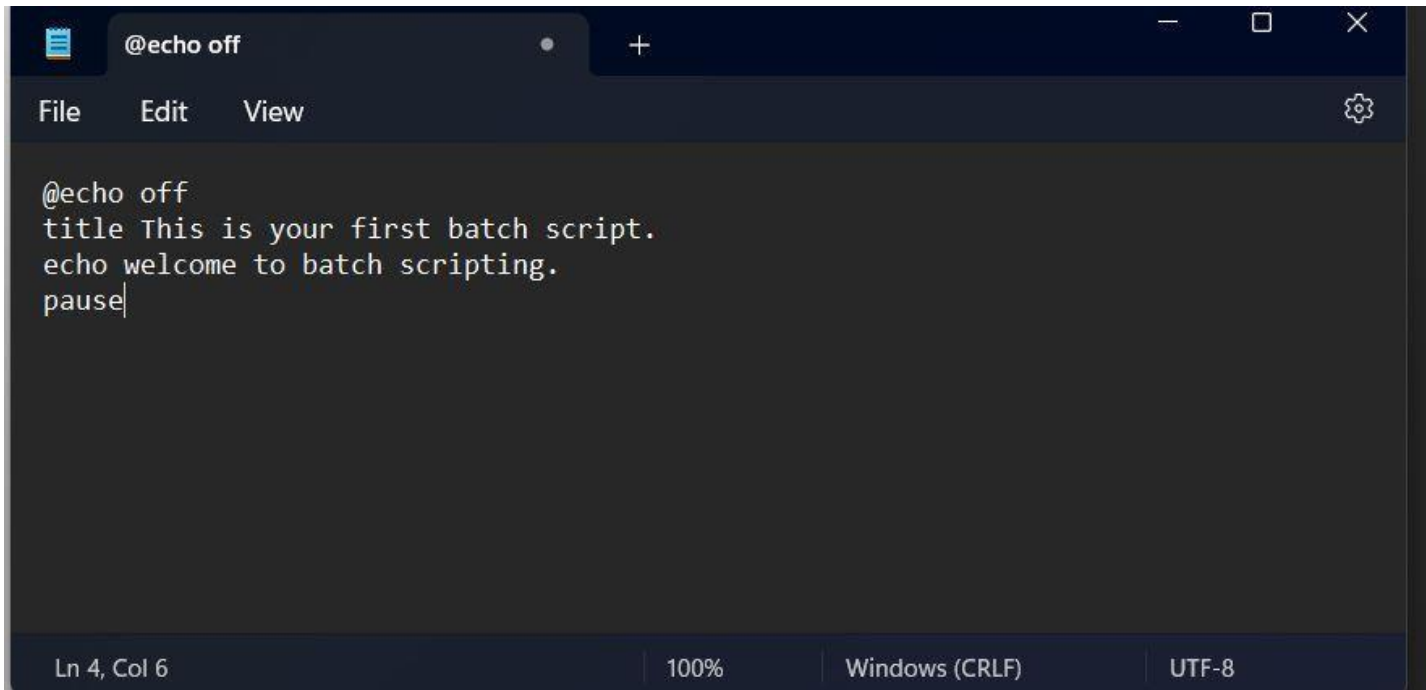
#### **1. TO SAVE a BAT File**

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

## 2.To RUN as BAT File

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

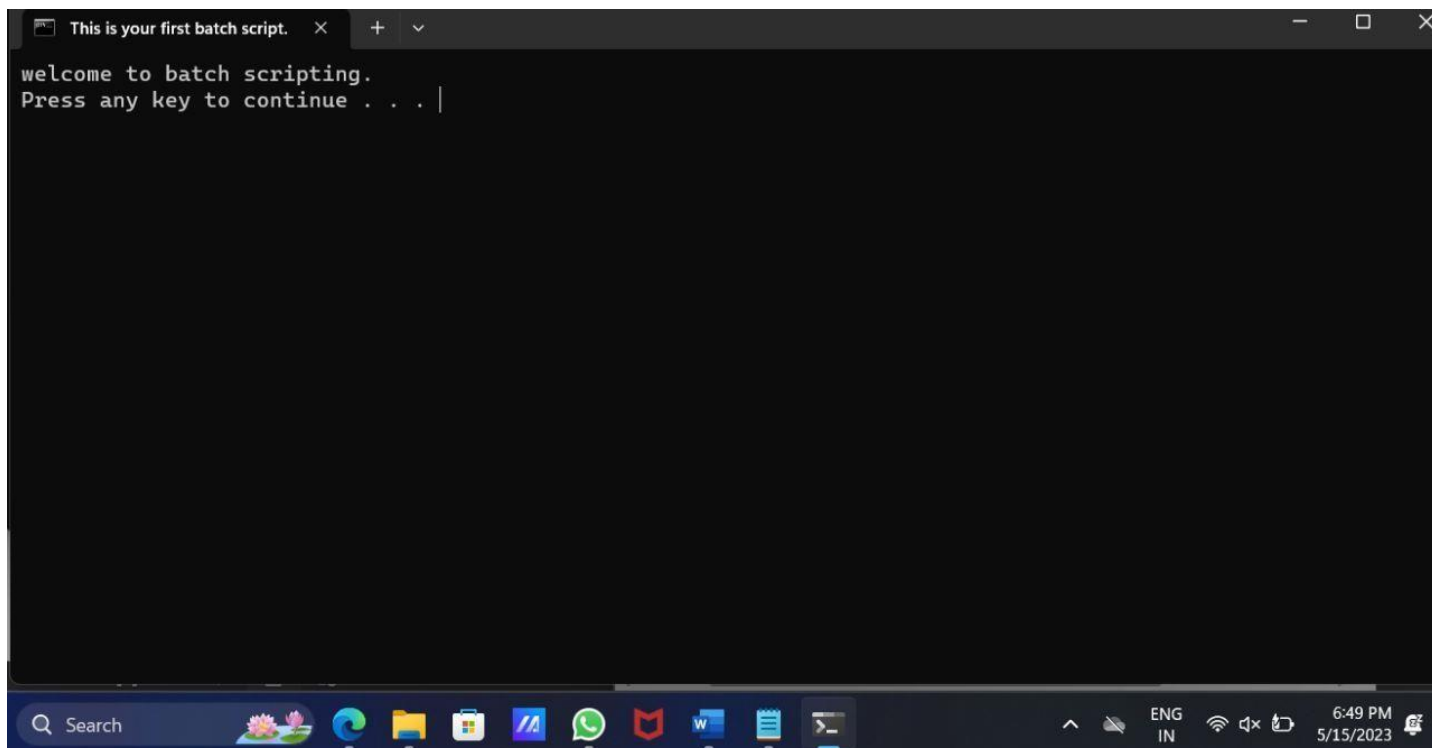
## OUTPUT:



A screenshot of a Notepad++ editor window. The title bar shows the file name as "@echo off". The menu bar includes "File", "Edit", and "View". The text area contains the following batch script code:

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

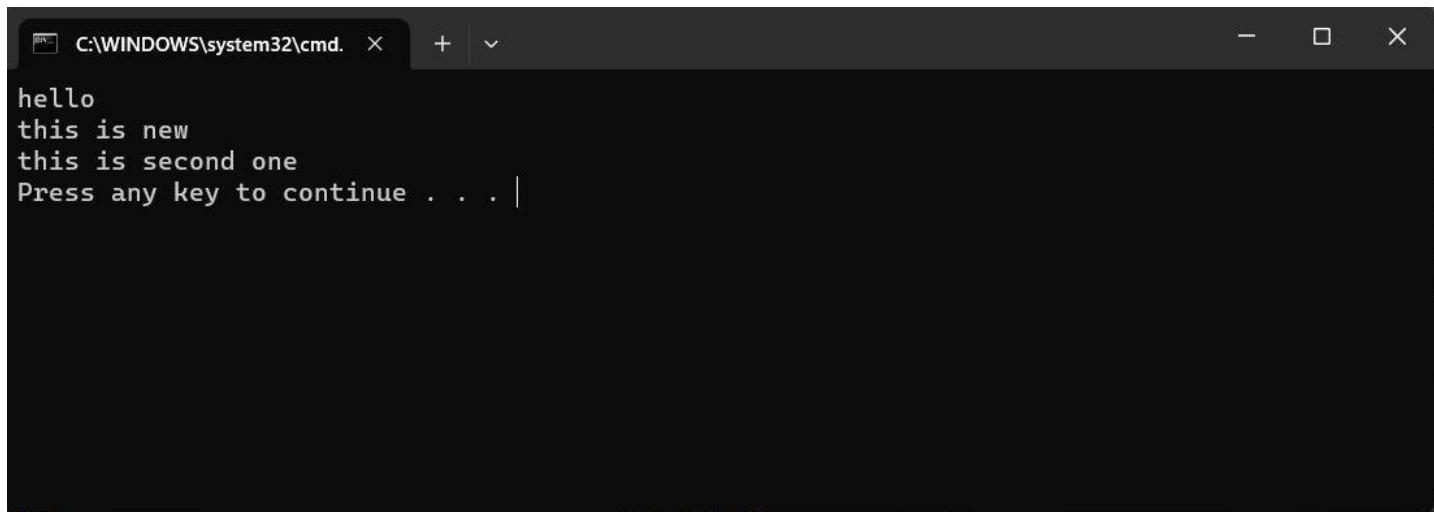
The status bar at the bottom indicates the cursor is at "Ln 4, Col 6", the zoom is "100%", the encoding is "Windows (CRLF)", and the character set is "UTF-8".



A screenshot of a Windows command prompt window. The title bar shows the window title as "This is your first batch script.". The text area displays the output of the batch script:

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

The Windows taskbar is visible at the bottom, showing the search bar, task view button, and several application icons including Edge, File Explorer, Task Manager, WhatsApp, and others. The system clock in the bottom right corner shows "6:49 PM" and "5/15/2023".

A screenshot of a Windows Command Prompt window. The title bar shows the path 'C:\WINDOWS\system32\cmd.' and standard window controls. The command prompt displays the following text: 'hello', 'this is new', 'this is second one', and 'Press any key to continue . . . |'. The text is in a monospaced font on a black background.

```
C:\WINDOWS\system32\cmd. X + v  
hello  
this is new  
this is second one  
Press any key to continue . . . |
```

### **Result:**

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