

ITA1471

ETHICAL HACKING FOR NETWORK HACKING



G. HEMANTH

192224095

1st YEAR, AI&DS DEPARTMENT

LAB MANUAL

Exercise No 1: Nmap Scan

Aim:

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

Procedure:

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

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

Scanning Techniques

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

Step 3:-

To perform host discovery

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

Step4:-

Port Specification

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

Step 5:-

Service Version and OS Detection

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

Step 6:-

Timing and Performance

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

Output:

1)

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

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

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

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

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

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

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

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

2)

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

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

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

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

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

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

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

3)

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

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

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

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

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

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

4)

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

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

5)

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

Service detection performed. Please report any incorrect results at https://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.

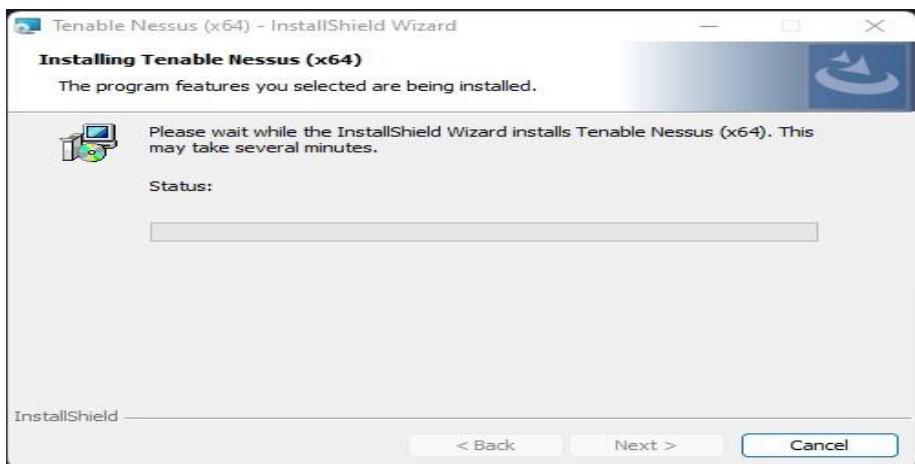
Exercise No 2: Vulnerability Access Scan Using Nessus

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

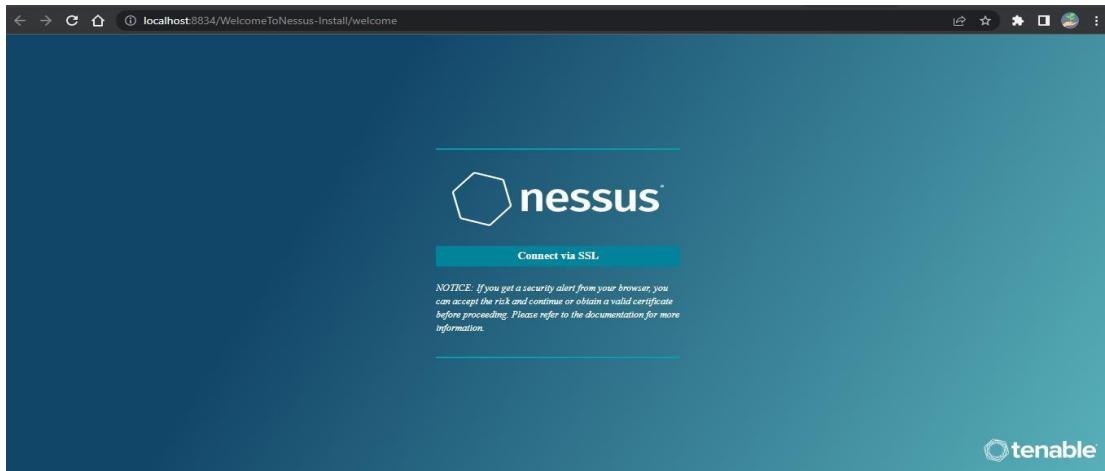
Step 1:- <https://www.tenable.com/downloads/nessus?loginAttempted=true>

The screenshot shows the Tenable Nessus download page. On the left, there's a sidebar with links like Nessus Agents, Nessus Network Monitor, Tenable.sc, Integrations, Sensor Proxy, Log Correlation Engine, Tenable Core, Tenable.ot, Tenable.ad, Web Application Scanning, Frictionless, Compliance & Audit, and Files. The main content area has a header 'Downloads / Nessus' and a title 'Nessus'. It features three numbered sections: 1. Download and Install Nessus (with 'Choose Download' dropdowns for Version 'Nessus - 10.4.2' and Platform 'Windows - x86_64'), 2. Start and Setup Nessus (with a link 'Open Nessus and follow setup wizard to finish setting up Nessus'), and 3. Getting Started. To the right is 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).

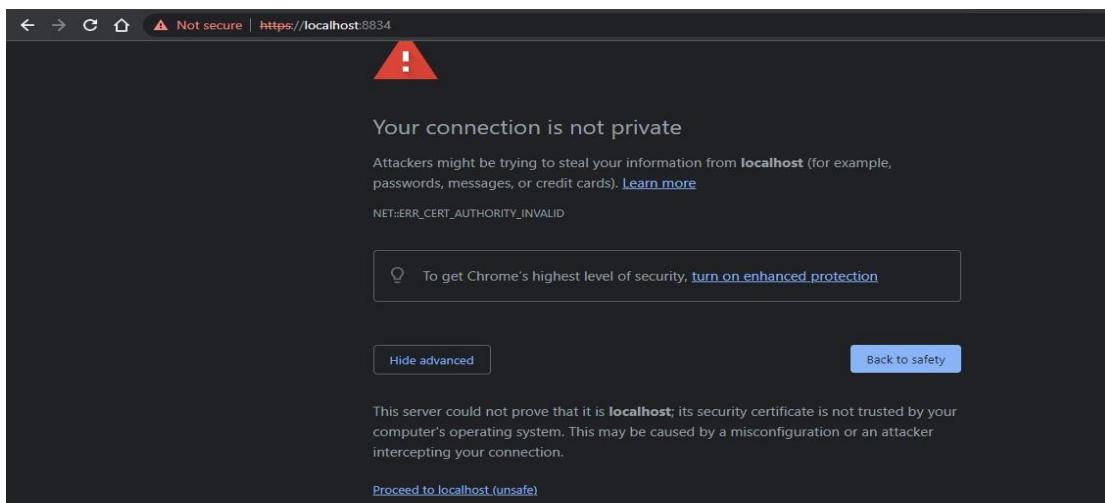
Step 2: Choose your OS and download , install



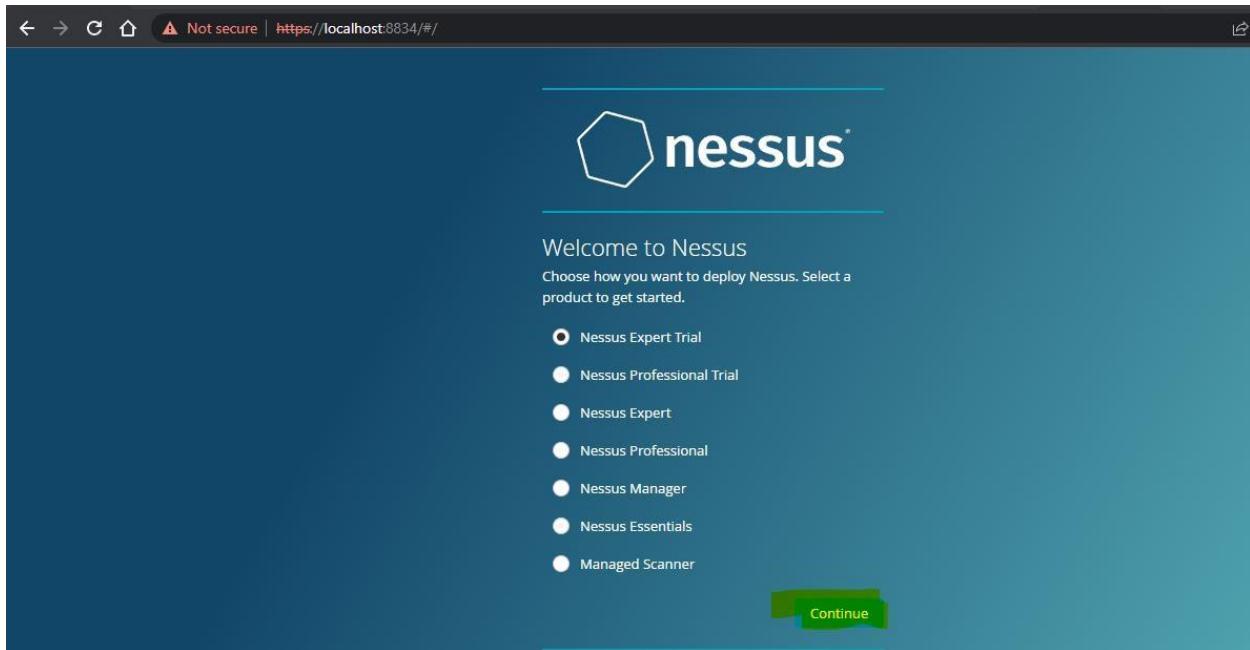
Step 3: Once installation is completed it will open in default browser



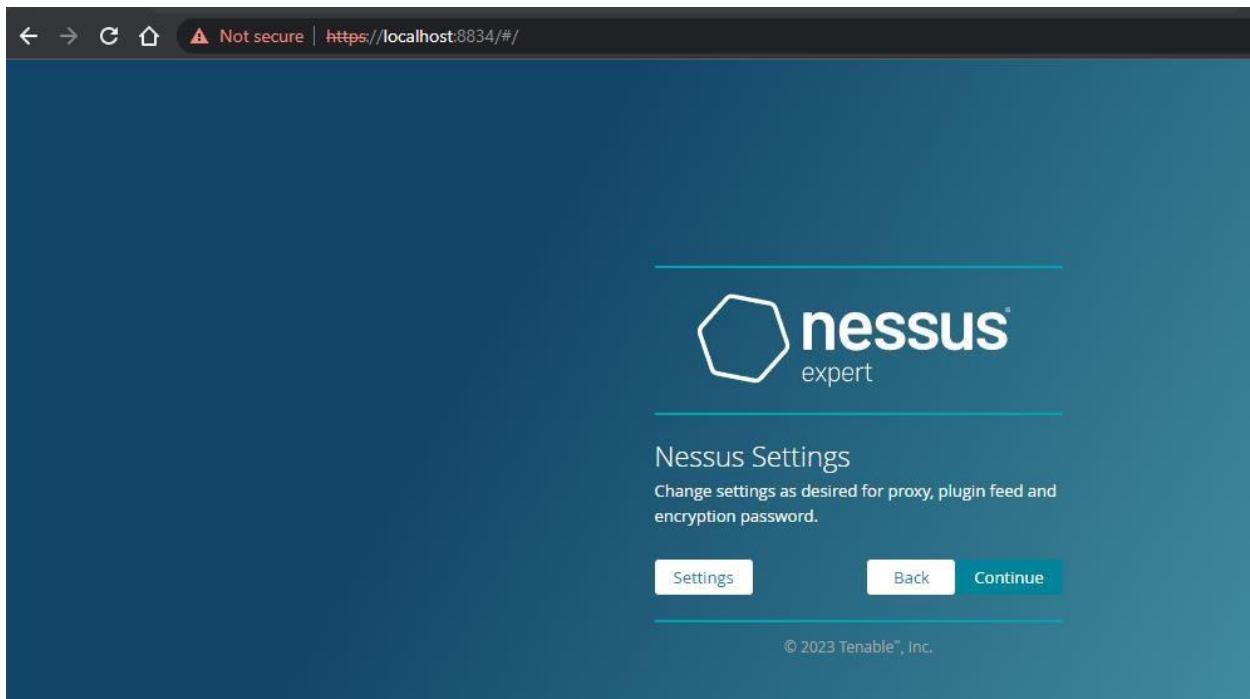
Step 5:- (click on the proceed to local host)



Step 6:- Please choose the Nessus Expert



Step 7: Click on continue



Step 8:- Register with your organizational email id

← → C ⌂ Not secure | <https://localhost:8834/#/>

expert

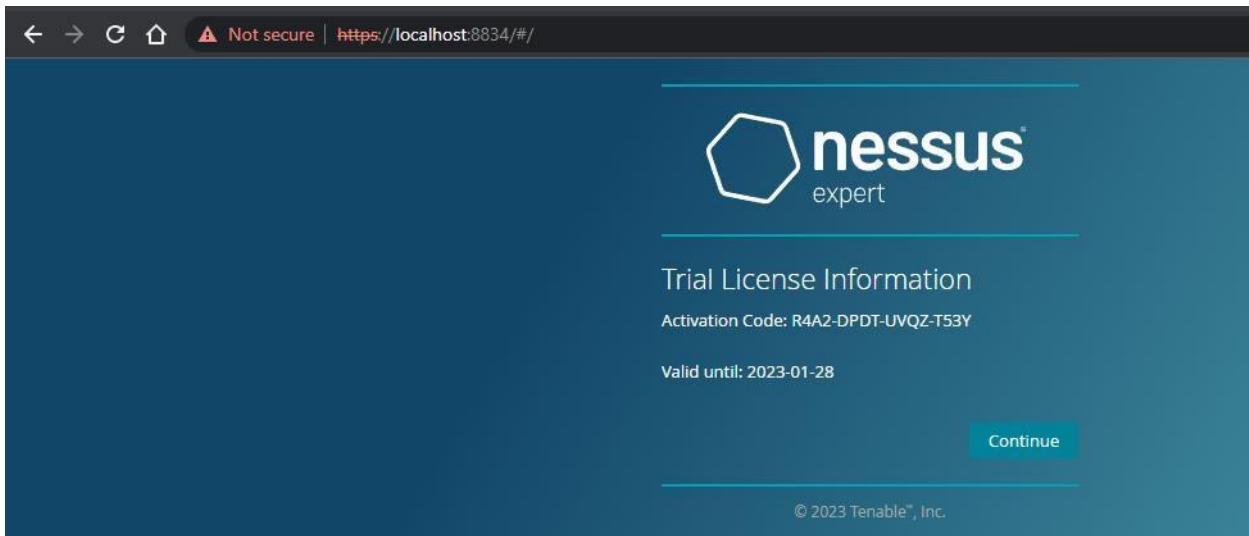
Create Account

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

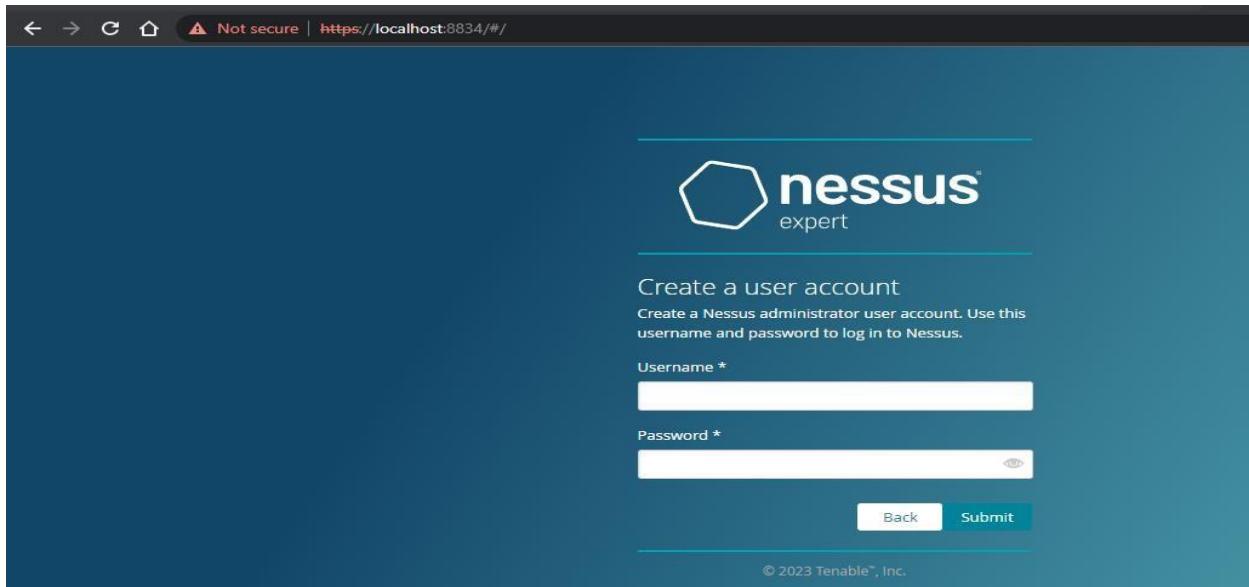
| | |
|--------------|-------------------------------|
| First Name | Last Name |
| pupsha | latha |
| Email | pushpalathas.sse@saveetha.com |
| Phone | 8667613340 |
| Title | Security team |
| Company Name | saveetha engineering college |
| Company Size | Company Size: 500-999 |

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

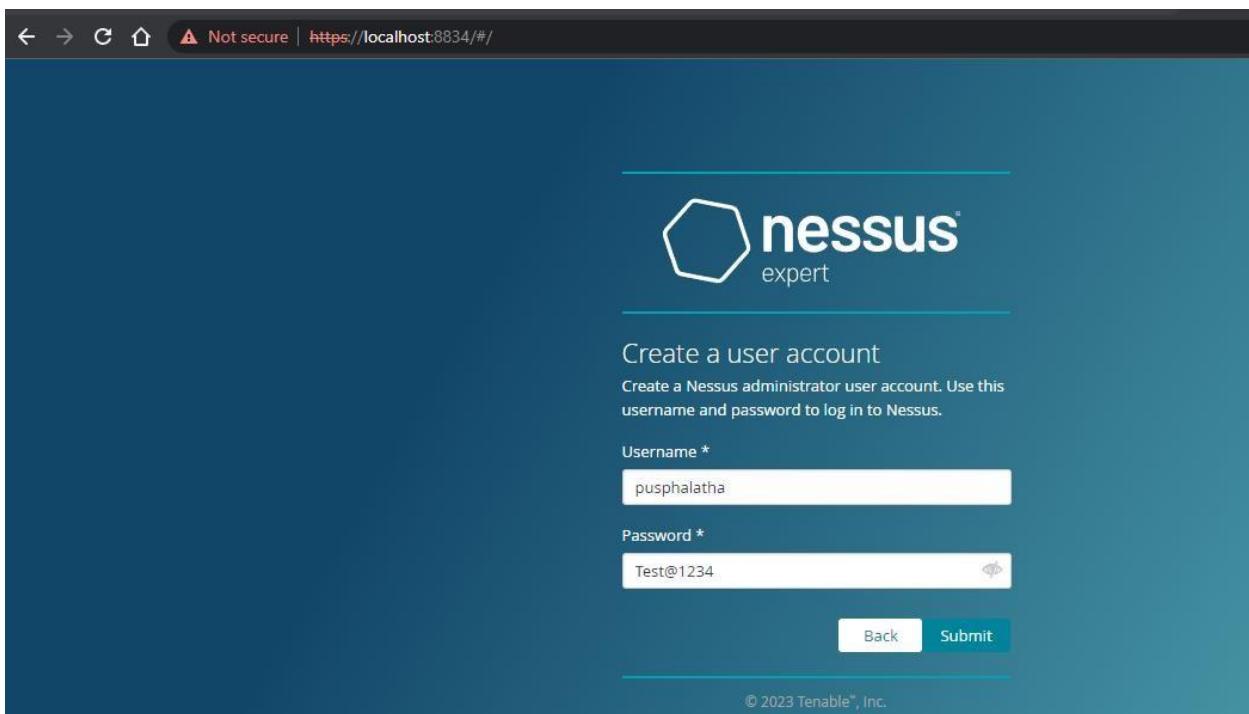
Step 9:- please note down the activation key



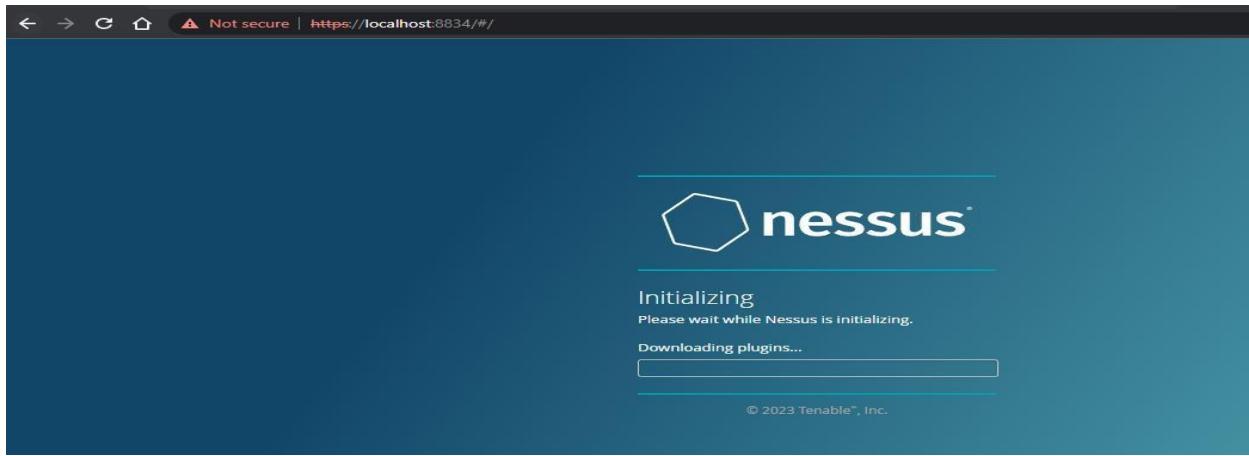
Step 10:- set up your username & password



Step 11:-Type username and password



Step 12:- Please wait until download is completed



Step 13: Select My Scans

A screenshot of the Nessus web interface. The left sidebar shows navigation options: FOLDERS (My Scans, All Scans, Trash), RESOURCES (Policies, Plugin Rules, Customized Reports, Terrascan). The main content area is titled "My Scans" and displays a message: "This folder is empty. Create a new scan." There are buttons for Import, New Folder, and New Scan. The top status bar shows multiple open tabs and the user "pushhalatha". The bottom taskbar includes icons for search, file operations, and system status.

Output:

1)

The screenshot shows the Nessus Expert interface. On the left sidebar, there are sections for FOLDERS (My Scans, All Scans, Trash), RESOURCES (Policies, Plugin Rules, Customized Reports, Terrascan), and a Policy Details dropdown. The main content area displays several error messages: 'DNS Issue' (unable to resolve log4shell-generic-pH2JhqlaCfpXPS0Q057.r.nessus.org), 'Log4j DNS Failed Request' (unable to resolve DNS 'r.nessus.org'), and 'Log4j DNS Failed Request' again. Below these are sections for Basic Overview, Report Overview, Credential Settings Overview, and Fragile Devices. The Basic Overview section includes details like Scan Policy: Basic Network Scan, Plugins Timeout: 320, and Feed Type: ProFeed. The Report Overview section includes Disable DNS Resolution: No and Display Superseded Patches: Yes. The Credential Settings Overview section includes Preferred SSH Port: 22 and SSH Client Version: OpenSSH_5.0. The Fragile Devices section includes Scan Network Printers: No, Scan Novell Netware Hosts: No, and Scan OT Devices: Yes.

2)

The screenshot shows the Nessus Expert interface with a completed scan named 'saveetha'. The main content area includes a 'Scan Summary' card with metrics: Hosts 1, Vulnerabilities 14, Notes 2, and History 4. Below this are sections for Scan Details (showing 0 Critical, 1 Medium, and 0 High vulnerabilities) and Scan Durations (showing 00:23:45 for Scan Duration, Median Scan Time per Host, and Max Scan Time). A pie chart indicates 100% detection for Nortel Switch. The interface also features a 'Scan Notes' section and navigation buttons for Configure, Audit Trail, Launch, Report, and Export.

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.

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

STEP 1: Open Terminal in the kali linux

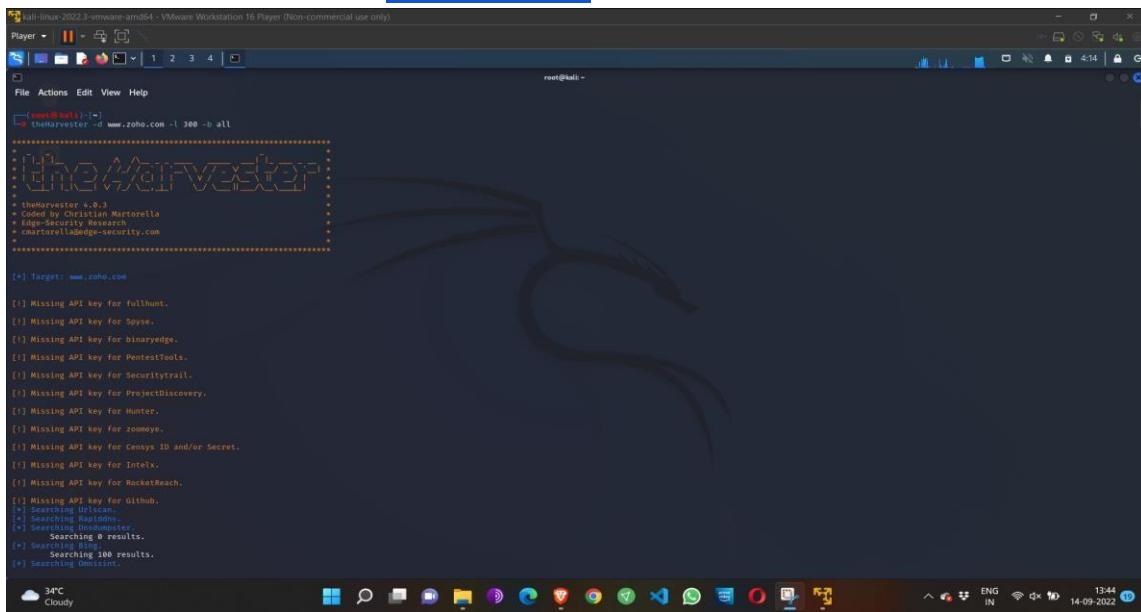
-d [url] will be the remote site from which you wants to fetch

-l will limit the search for specified number.

-b is used to specify search engine name.

STEP 2: Run the following command

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



```
Kali-Linux-2023.3-vmware-11004 - VMware Workstation 16 Player (Non-commercial use only)
Player | II | X
File Actions Edit View Help
root@kali:~# theHarvester -d www.zoho.com -l 300 -b all
=====
[!] Target: www.zoho.com
[!] Missing API key for fullhunt.
[!] Missing API key for Spyse.
[!] Missing API key for binaryedge.
[!] Missing API key for PentesTools.
[!] 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 RockTheBeach.
[!] Missing API key for Github.
[!] Searching LinkedIn...
[!] Searching Maildom...
[!] Searching Shodan...
[!] Searching 0 results.
[!] Searching Bing...
[!] Searching 100 results.
[!] Searching Imdb...
```



```
kali-linux-2022.3-vmware-amd64 - VMware Workstation 16 Player (Non-commercial use only)
Player | ||| | 1 2 3 4 | 
File Actions Edit View Help
A563949
[*] Interesting URLs found: 25
http://www.zoho.com/
http://www.zoho.com/assit/
https://www.zoho.com/books/
https://www.zoho.com/campaigns/?zsrc=fromproduct
https://www.zoho.com/campaigns/leads/zcsandview.html
https://www.zoho.com/exalines/exalines/zcsandview.html
https://www.zoho.com/cliq/?serviceurl=>#Fchat#2F2431727550015100&zsrc=fromproduct
https://www.zoho.com/contactus.html
https://www.zoho.com/contactus.html
https://www.zoho.com/crm/
https://www.zoho.com/crmplus/
https://www.zoho.com/crm/
https://www.zoho.com/crmcalendar/
https://www.zoho.com/forms/
https://www.zoho.com/invoice/?utm_source=20&utm_medium=pdf
https://www.zoho.com/marketing/
https://www.zoho.com/marketingautomation/
https://www.zoho.com/nl/
https://www.zoho.com/nl/salesiq/
https://www.zoho.com/peopleplus/?zsrc=zoho-home&amp;zsrc=bireft->home
https://www.zoho.com/report-abuse/
https://www.zoho.com/salesiq/
https://www.zoho.com/survey/
[*] No Twitter users found.

[*] LinkedIn Users found: 292
Anil Mohamed - Regional Account Manager
Abba Abu - Zoho Developer
Abhishek Godishala
Adarsh Pandey - Member of Technical Staff
Adithyan Ravindrar - Lead Software Engineer
Ajay Singh - Partner Software Engineer - Zoho
Ajay Singh - Developer - ZOHO CRM
Akash Krishnan - Member Technical Staff
Akash Krishnamoorthy
Akshaya Chidrasekar - Zoho Corporation
Ali Shabdar - Regional Director MEA
Alok Kumar Bharti - Software Engineer
Aman Gupta - Zoho Developers
Amarjeet Kaur - Zoho Developer
Ambi Moorthy - Product Manager and Co-Founder
Anandaraman Krishnan - Product Manager
[*] Interesting URLs found: 292
[*] LinkedIn Users found: 292
Anil Mohamed - Regional Account Manager
Abba Abu - Zoho Developer
Abhishek Godishala
Adarsh Pandey - Member of Technical Staff
Adithyan Ravindrar - Lead Software Engineer
Ajay Singh - Partner Software Engineer - Zoho
Ajay Singh - Developer - ZOHO CRM
Akash Krishnan - Member Technical Staff
Akash Krishnamoorthy
Akshaya Chidrasekar - Zoho Corporation
Ali Shabdar - Regional Director MEA
Alok Kumar Bharti - Software Engineer
Aman Gupta - Zoho Developers
Aman Gupta - Zoho Developer
Ambi Moorthy - Product Manager and Co-Founder
Anandaraman Krishnan - Product Manager
[*] Interesting URLs found: 292
[*] LinkedIn Users found: 292
```

```
kali-linux-2022.3-vmware-amd64 - VMware Workstation 16 Player (Non-commercial use only)
Player | ||| | 1 2 3 4 | 
File Actions Edit View Help
A563949
[*] Interesting URLs found: 25
http://www.zoho.com/
http://www.zoho.com/assit/
https://www.zoho.com/books/
https://www.zoho.com/campaigns/?zsrc=fromproduct
https://www.zoho.com/campaigns/leads/zcsandview.html
https://www.zoho.com/exalines/exalines/zcsandview.html
https://www.zoho.com/cliq/?serviceurl=>#Fchat#2F2431727550015100&zsrc=fromproduct
https://www.zoho.com/contactus.html
https://www.zoho.com/contactus.html
https://www.zoho.com/crm/
https://www.zoho.com/crmplus/
https://www.zoho.com/crm/
https://www.zoho.com/crmcalendar/
https://www.zoho.com/forms/
https://www.zoho.com/invoice/?utm_source=20&utm_medium=pdf
https://www.zoho.com/marketing/
https://www.zoho.com/marketingautomation/
https://www.zoho.com/nl/
https://www.zoho.com/nl/salesiq/
https://www.zoho.com/peopleplus/?zsrc=zoho-home&amp;zsrc=bireft->home
https://www.zoho.com/report-abuse/
https://www.zoho.com/salesiq/
https://www.zoho.com/survey/
[*] No Twitter users found.

[*] LinkedIn Users found: 292
Anil Mohamed - Regional Account Manager
Abba Abu - Zoho Developer
Abhishek Godishala
Adarsh Pandey - Member of Technical Staff
Adithyan Ravindrar - Lead Software Engineer
Ajay Singh - Partner Software Engineer - Zoho
Ajay Singh - Developer - ZOHO CRM
Akash Krishnan - Member Technical Staff
Akash Krishnamoorthy
Akshaya Chidrasekar - Zoho Corporation
Ali Shabdar - Regional Director MEA
Alok Kumar Bharti - Software Engineer
Aman Gupta - Zoho Developers
Aman Gupta - Zoho Developer
Ambi Moorthy - Product Manager and Co-Founder
Anandaraman Krishnan - Product Manager
[*] Interesting URLs found: 292
[*] LinkedIn Users found: 292
Anil Mohamed - Regional Account Manager
Abba Abu - Zoho Developer
Abhishek Godishala
Adarsh Pandey - Member of Technical Staff
Adithyan Ravindrar - Lead Software Engineer
Ajay Singh - Partner Software Engineer - Zoho
Ajay Singh - Developer - ZOHO CRM
Akash Krishnan - Member Technical Staff
Akash Krishnamoorthy
Akshaya Chidrasekar - Zoho Corporation
Ali Shabdar - Regional Director MEA
Alok Kumar Bharti - Software Engineer
Aman Gupta - Zoho Developers
Aman Gupta - Zoho Developer
Ambi Moorthy - Product Manager and Co-Founder
Anandaraman Krishnan - Product Manager
[*] Interesting URLs found: 292
[*] LinkedIn Users found: 292
```

```
kali-linux-2022.3-vmware-amd64 - VMware Workstation 16 Player (Non-commercial use only)
Player | || v | 1 2 3 4 | x
File Actions Edit View Help
Vijayaraghavan Venugopal
Vinodraja 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
Zoheb Khan - Developer
Zoho Developer
Zoho Expert Services - GENOWIRE
balaji - Developer - Zoho Corporation
omprakash - Ios Developer
rangarajan ramesh - Account Manager - Zoho
sathiyam sathiyamsarya - zoho - Zoho Corporation
shuktik Afrin - Senior Technical Support Engineer
vasudevanew T - Lead
working as a Senior executive at IndiGo Airlines
[*] LinkedIn Links found: 0
Aamil Mohammed - Regional Account Manager
Abbas Abu - Zoho One Developer
Abhilash Reddy Godisala
Abhishek Chaturvedi - Member of Technical Staff
Adithyan Ravichandar - Lead System Engineer
Ajay George - Partner Support Engineer - ZOHO CRM
Ajay Singh - Developer - ZOHO CRM
Akash Krishnamoorthy - Member Technical Staff
Akilan Marimuthu
Akshaya Chandrasekar - Zoho Corporation
Alka Patel - Regional Director MEA
Alok Kumar Bhattacharya - Software Engineer
Aman Gupta - Zoho Developer
Amaranath KR - Zoho Developer
Anand Prabhakar - Product Manager and Co-Founder
Anandharuman Krishnan - Project Manager
Anantha Subramanian - Engineer Trainee
Ananthu Nair - Presales Engineer - Zoho Corporation
Andrea Mahoney - VP - Certified Computer Programmer
Anil Kulkarni
Andrew Joseph - Zoho Corporation
Andrews B A - Senior Member Of Technical Staff
Anilbabu Ponnuswamy - Zoho Corporation
Anuradha Gupta - Technical Writer
Aravind Nataraajan - Zoho Corporation
Arun Balachandran - Senior Product Marketing Manager
Arun Kesavam - Product Designer
Arun Selvamuthu - Product Marketer
Arvind Krishnamoorthy
Ashok Chakravarthi Nagarajan
34°C
Cloudy
ENG IN 13:47 14-09-2022
```

```
kali-linux-2022.3-vmware-amd64 - VMware Workstation 16 Player (Non-commercial use only)
Player | || v | 1 2 3 4 | x
File Actions Edit 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
Zoheb Khan - Developer
Zoho Developer
Zoho Expert Services - GENOWIRE
balaji - Developer - Zoho Corporation
omprakash - Ios Developer
rangarajan ramesh - Account Manager - Zoho
sathiyam sathiyamsarya - zoho - Zoho Corporation
shuktik Afrin - Senior Technical Support Engineer
vasudevanew T - Lead
working as a Senior executive at IndiGo Airlines
[*] Trello URLs found: 33
http://www.trello.com/contact
https://trello.com/integrations
https://trello.com/integrations/sales-support
https://trello.com/power-ups
https://trello.com/power-ups/595e99f8f137d2af4b6fd4
https://trello.com/power-ups/5b0c1aa1922a254295b0a35/zoho-crm
https://trello.com/power-ups/5b5d5074cc75f290fd47/automatio
https://trello.com/power-ups/5ba22ddc8b80a8959edc0
https://trello.com/power-ups/5b9a0a0a0a0a0a0a0a0a0a0a0a0a0a0a0/zoho-desk
https://trello.com/power-ups/category/it-project-management
https://trello.com/power-ups/category/marketing-social-media
https://trello.com/power-ups/category/sales-support
https://trello.com/pricing
https://trello.com/teams/support
https://trello.com/templates
https://trello.com/templates/design
https://trello.com/templates/design/design-system-checklist-yzn5yfon
https://trello.com/templates/design/freelance-branding-project-z5m6dhs
https://trello.com/templates/design/research-iteration-8t9qgnz
https://trello.com/templates/product-management
https://trello.com/templates/product-management/5-etapas-de-gerenciamento-de-produtos-7s8avmuv
https://trello.com/templates/product-management/5-listes-pour-la-gestion-de-produits-0lfufgyd7
https://trello.com/templates/product-management/acklog-de-funcionalidades-sncwwjtg
https://trello.com/templates/product-management/acklog-de-projetos-7t77g7s
https://trello.com/templates/product-management/fabrication-process-davkjps
https://trello.com/templates/product-management/product-roadmap-template-fbajjsbh
https://trello.com/templates/product-management/project-planning-template-jibfr
https://trello.com/templates/product-management/roadmap-project-t-jpd120
https://trello.com/templates/product-management/shipping-planner-mc3vzive
https://trello.com/tour
https://trello.com/use-cases/crm
34°C
Cloudy
ENG IN 13:47 14-09-2022
```



```
Kali-linux-2022.3-vmware-amd64 - VMware Workstation 16 Player (Non-commercial use only)
File Actions Edit View Help
https://trello.com/use-cases/crm
https://www.trello.com/
[*] IPs found: 49
8.39.54.155
8.40.222.155
74.201.84.81
74.201.112.101
74.201.113.118
74.201.113.118
74.201.113.176
74.201.113.176
74.201.155.201
89.36.170.52
103.138.128.96
103.138.128.97
104.16.11.213
104.16.12.213
104.16.13.213
104.16.14.213
104.16.43.213
104.16.43.59
104.16.44.59
117.20.42.154
120.117.187.155
136.143.198.58
136.143.198.79
136.143.198.155
136.143.198.156
136.143.191.284
165.173.187.32
166.254.166.165
166.254.166.165
178.79.172.105
185.28.209.52
208.113.145.155
208.141.42.155
208.141.42.156
208.141.43.204
216.95.225.253
230.69.91.1328::c
2a06:98c1:1321::3
[*] No emails found.
[*] No hosts found.

(rmett@kali)-[~]
Cloudy 34°C
```

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

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

Output:

1)

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

Result:

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

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

Procedure:

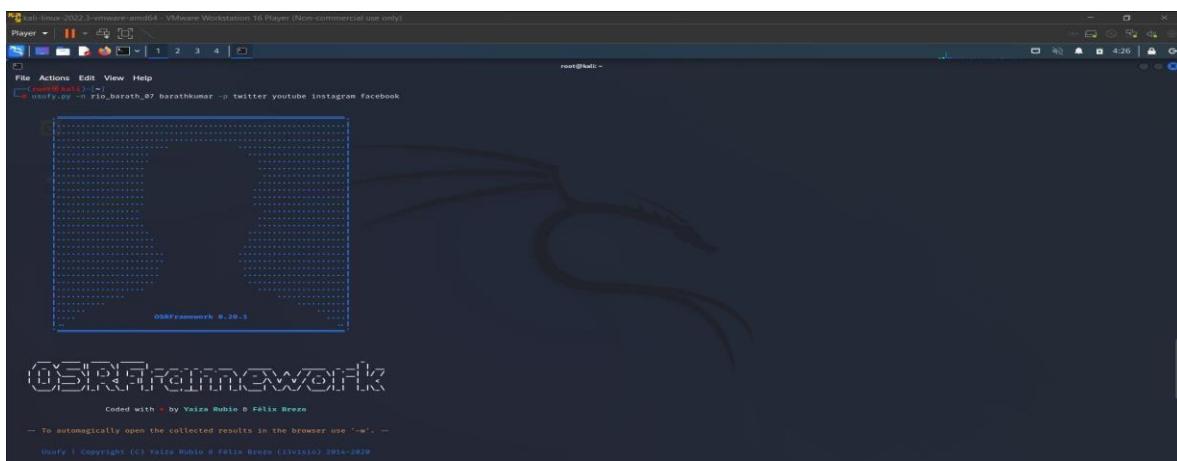
Step 1: Log into kali linux machine

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

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

Command:

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



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

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

```

root@LiveWire:~# ./searchfy.py -q "LIVEWIRE"
[...]
2022-09-14 04:25:11.216299    Starting search in 4 platform(s) ... Relax!
Press Ctrl+C to stop...
2022-09-14 04:25:11.216299    Results obtained (8):
[...]
com.iVisio.URI | com.iVisio.Alias | com.iVisio.Platform |
| https://www.youtube.com/user/rio_barath_07/about | rio_barath_07 | YouTube
| https://www.facebook.com/rio_barath_07 | rio_barath_07 | Facebook
| http://www.instagram.com/rio_barath_07 | rio_barath_07 | Instagram
| http://twitter.com/rio_barath_07 | rio_barath_07 | Twitter
| https://www.youtube.com/user/barathkumar/about | barathkumar | YouTube
| https://www.facebook.com/barathkumar | barathkumar | Facebook
| http://www.instagram.com/barathkumar | barathkumar | Instagram
| http://twitter.com/barathkumar | barathkumar | Twitter
[...]
2022-09-15 04:25:11.390091    You can find all the information here: ./profiles.csv
2022-09-15 04:25:11.397468    Finishing execution...
Total time consumed: 0:00:06.189475
Average seconds/query: 1.14462675 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 repository:
https://github.com/iVisio/osrfframework/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 allsocial 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). | | |
|--|--------------|-----------------|
| iVisio.uri | iVisio.alias | iVisio.platform |
| http://twitter.com/us | us | Twitter |
| https://www.facebook.com/cehuser | cehuser | Facebook |
| http://twitter.com/cehuser | cehuser | Twitter |
| https://www.facebook.com/us | us | Facebook |

FIGURE. 10

Collect and note the information disclosed about the target.

Output:

1)

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

File Actions Edit View Help
OSRFramework 0.20.1
```

```
-- 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:

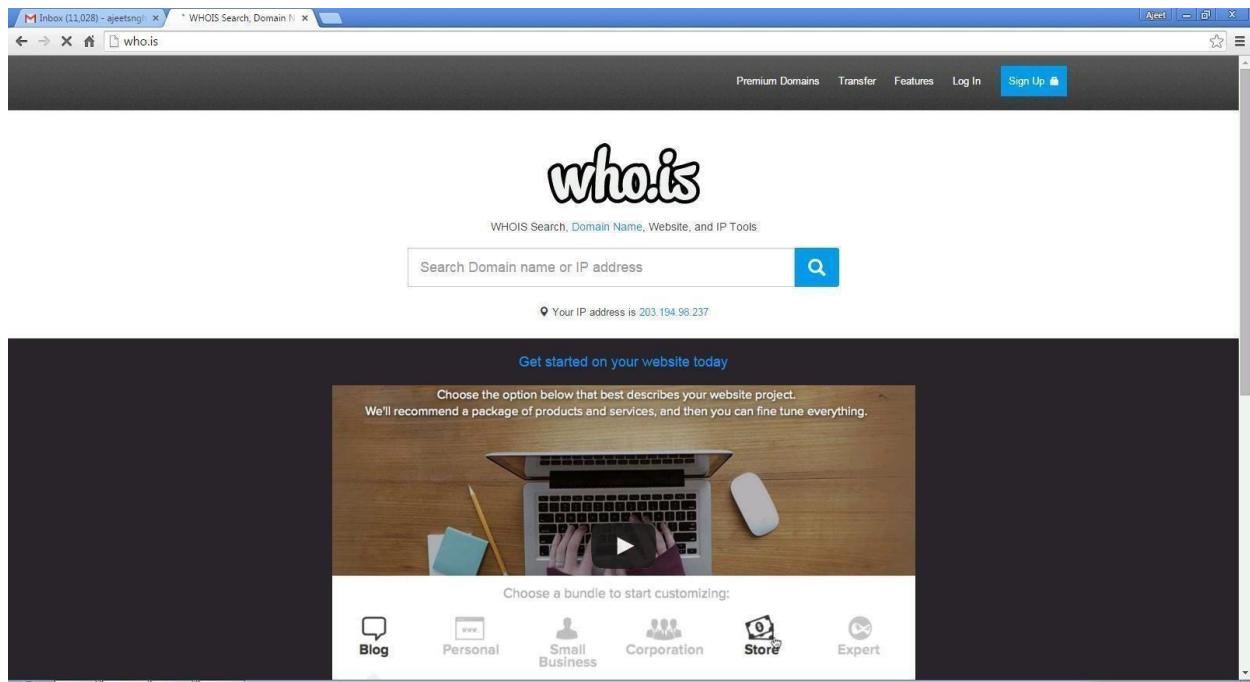
The current experiment is about Open-Source Intelligence Gathering is done using OSR Framework. This experiment is done to check for the Existence of a Profile for given user details in different platforms. This experiment is executed in root terminal using kali linux operating system.

Exercise NO 5: Use Google and Whois for Reconnaissance.

Aim: To find out the Whois, DNS Records and 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 | 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 |

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=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
```

The screenshot shows the whois.is website interface. At the top, there's a search bar with the URL "whois.is/whois/saveetha.com". Below the search bar, there's a navigation menu with links for "Premium Domains", "Transfer", "Features", "Login", and "Sign Up". The main content area displays the WHOIS information for the domain "saveetha.com". The "Whois" tab is selected. Key details shown include:

- Registrar Info:** PDR Ltd. d/b/a PublicDomainRegistry.com, whois.PublicDomainRegistry.com
- 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:** A list of domains like save-energy.com, savee.biz, savee.cloud, savee.co.jp, savee.co.uk, savee.com, savee.com.au, savee.com.br, savee.com.cn, savee.de, savee.dk, savee.eu, savee.host, savee.info, savee.io, and savee.it.
- Registrar Data:** Registrant Contact Information: Name - Dr N.H. Veeraiyan, Organization - Saveetha Dental College & Hosp., Address - Saveetha University, Saveetha Nagar, Thandlem Campus.

On the right side, there are promotional banners for Name.com and suggestions for similar domains like "save-etha.live", "saveetha.live", "freeetha.live", "rescueetha.live", and "guardetha.live".

Output:

The screenshot shows the GoDaddy WHOIS search results for the domain "www.saveetha.com". The page has a header "Search the WHOIS Database" with a search bar containing "saveetha.com" and a "Search" button. The main content area is titled "WHOIS search results" and contains the following information:

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

Result:

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

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

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

Procedure:

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

```

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

C:\Users\barat>tracert saveetha.com

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

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

Trace complete.

```

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

```

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

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

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

```

Step 3: Type ifconfig command

```

$use1:-# 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)

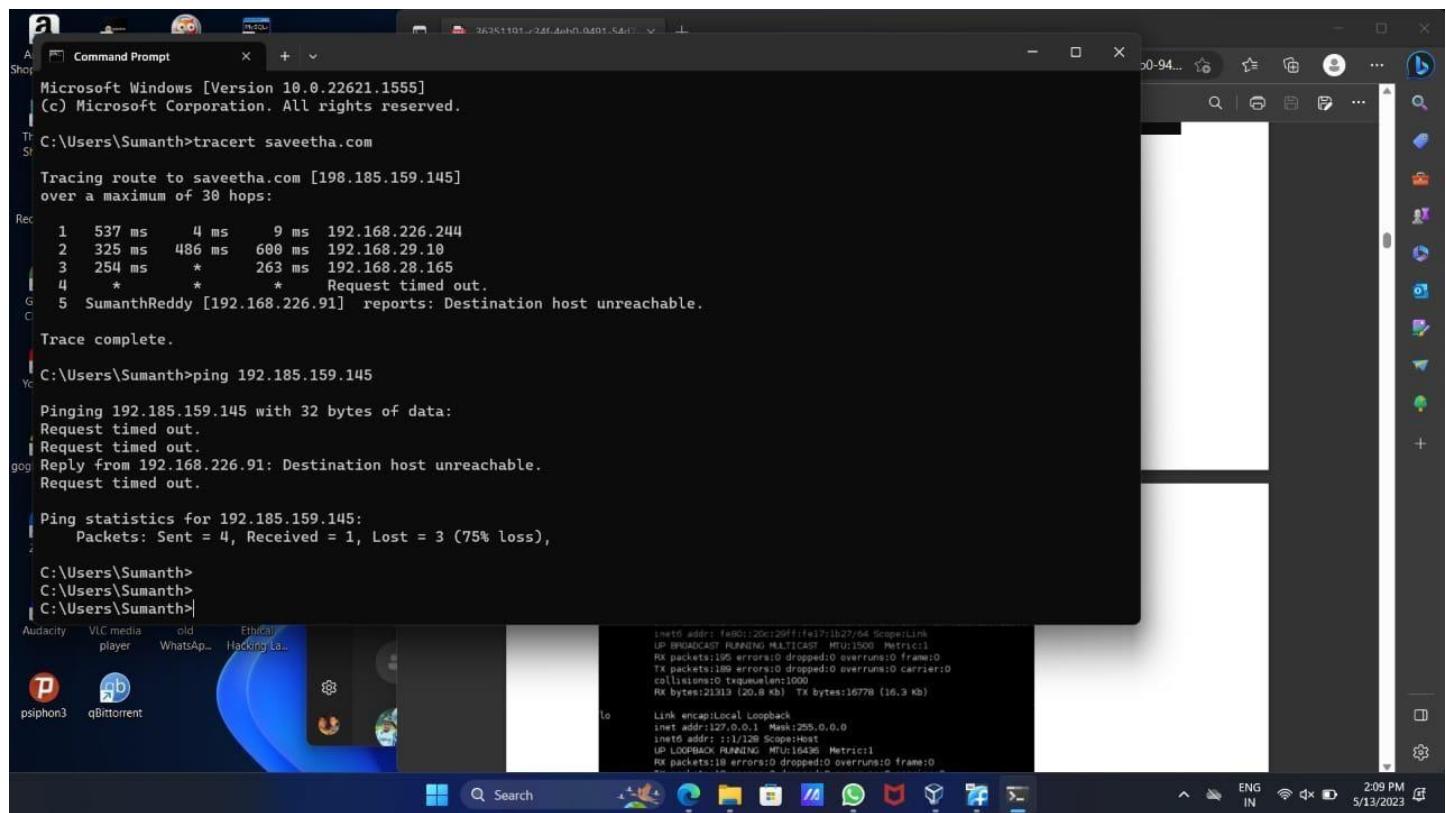
```

Step 4: Type netstat command

| 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:

```

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

Trace complete.

```

C:\Users\Sumanth>ping 192.185.159.145

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

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

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

Autoplay

psiphon3 VLC media player WhatsApp Hacking Lab

Link encap:Local Loopback
inet addr:127.0.0.1 Mask:255.0.0.0
inet addr: ::1/128 Scope:Host
Link encap:Local Loopback MTU:16436 Metric:1
inet addr:127.0.0.1 Mask:255.0.0.0

2)

3)

```
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 192.168.0.1:25072 test:https TIME_WAIT
TCP 192.168.0.57:25078 a23-50-165-111:https ESTABLISHED
TCP 192.168.0.57:25089 a23-50-165-111:https ESTABLISHED
TCP 192.168.0.57:25083 48.67.188.75:https ESTABLISHED
TCP 192.168.0.57:25099 11.11.21.21.200:https ESTABLISHED
TCP 192.168.0.57:25100 n329092: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 n329092:http SYN_SENT
TCP 192.168.0.57:25107 11.11.21.200:https ESTABLISHED
```

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

C:\Users\Sumanth>netstat

Active Connections

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

Result:

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

Exercise No 7:VULNERABILITY ANALYSIS - CGI Scanning with Nikto

Aim:To perform vulnerability Analysis using CGI Scanning with Nikto

Procedure:

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

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



The screenshot shows a terminal window on a Kali Linux desktop environment. The title bar says 'root@kali:~' and the status bar shows the time as 13:33. The terminal menu bar includes File, Actions, Edit, View, Help. The command entered is 'nikto -h www.zoho.com -Tuning X'. The output shows the following information:

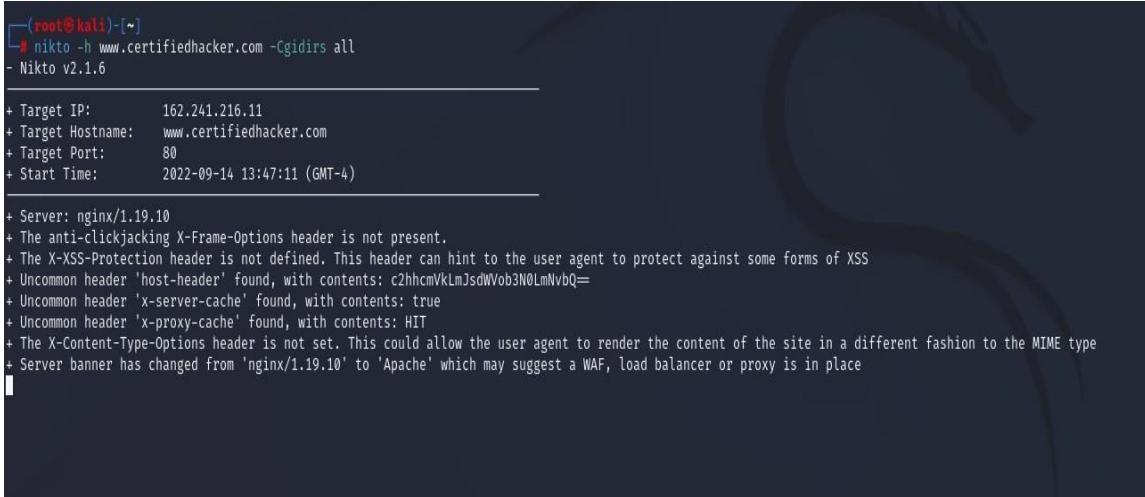
```
(root@kali)-[~]
# nikto -h www.zoho.com -Tuning X
- Nikto v2.1.6

+ 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

A screenshot of a terminal window titled '(root㉿kali)-[~]'. The command entered is '# nikto -h www.certifiedhacker.com -Cgidirs all'. The output shows the following information:

```
[# 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: c2hhcmVklmJsdWob3N0LmNvbQ=
+ Uncommon header 'x-server-cache' found, with contents: HIT
+ 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-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 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 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:

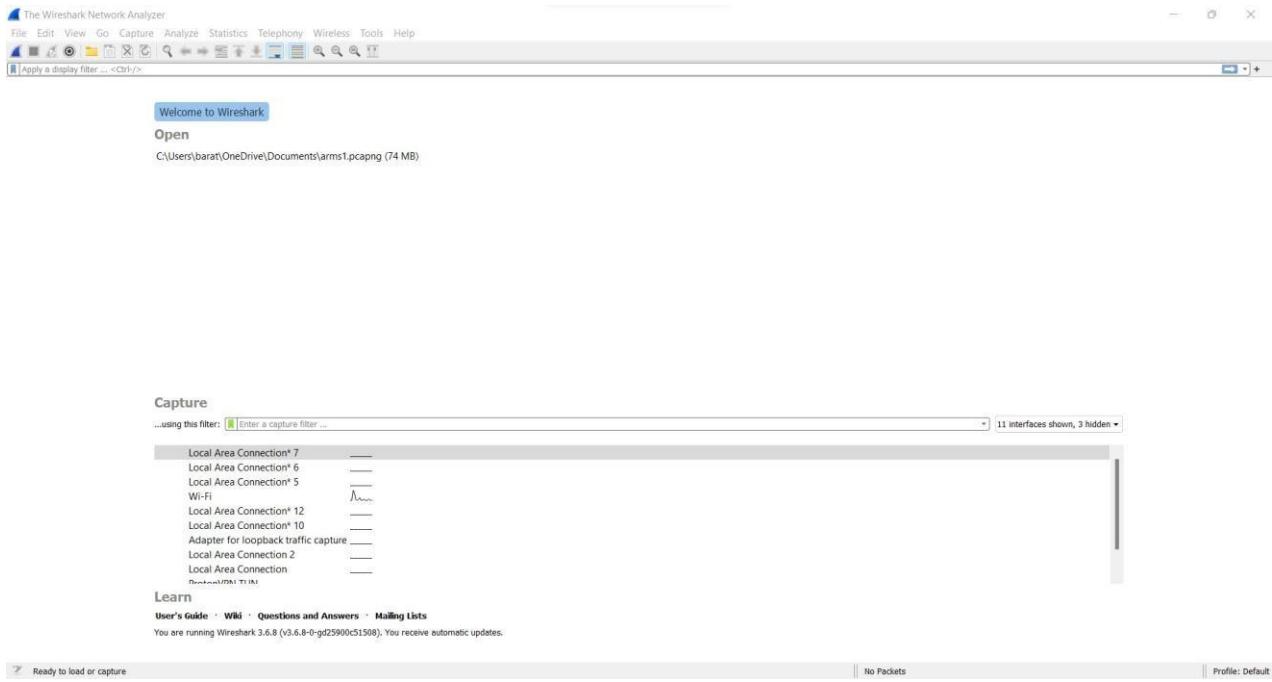
The above experiment is about VULNERABILITY ANALYSIS - CGI Scanning with Nikto. We can retrieve information like server name, headers and etc. This is done in root terminal using kali linux OS.

Exercise No 8: Wireshark Sniffer

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

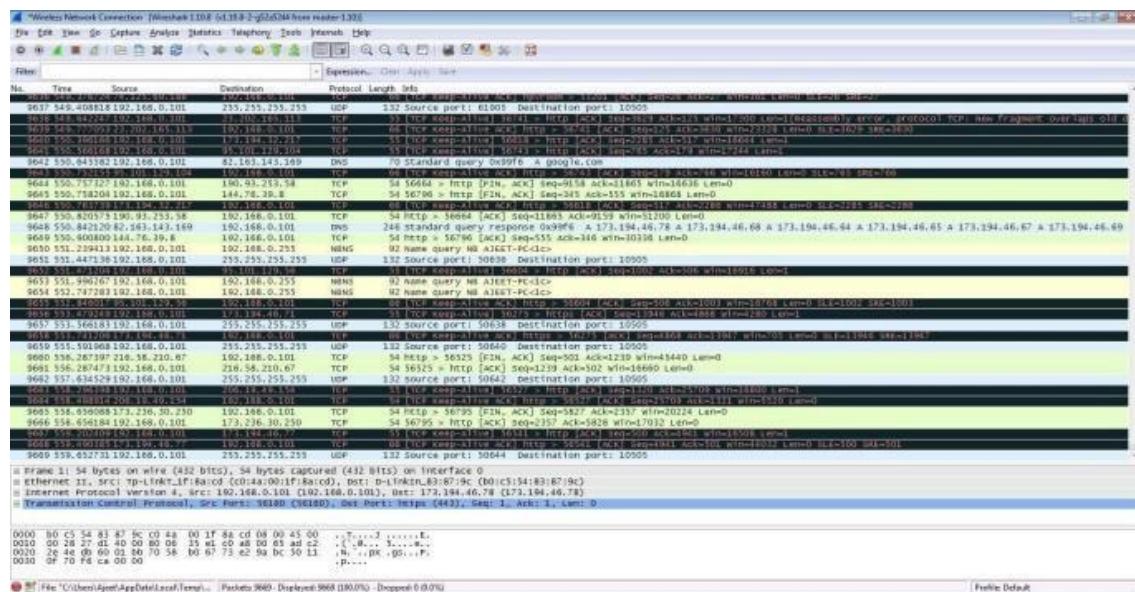
Procedure:

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

The screenshot shows NetworkMiner capturing traffic from Wi-Fi. A POST request to `http://arms.sse.saveetha.com` is selected, showing the raw data: [HTTP request 2/2] [Prev request in frame: 72877] [Response in frame: 89219]. The raw data includes form items like `_VIEWSTATE`, `_VIEWSTATEGENERATOR`, `_EVENTVALIDATION`, `txtusername`, `txtpassword`, and `btnlogin`. The browser window shows a 'Sign In' page for 'SAVEETHA SCHOOL OF ENGINEERING'. The user has entered 'admin' for the username and '*****' for the password. An error message 'The username and password you entered is invalid' is displayed below the login fields.

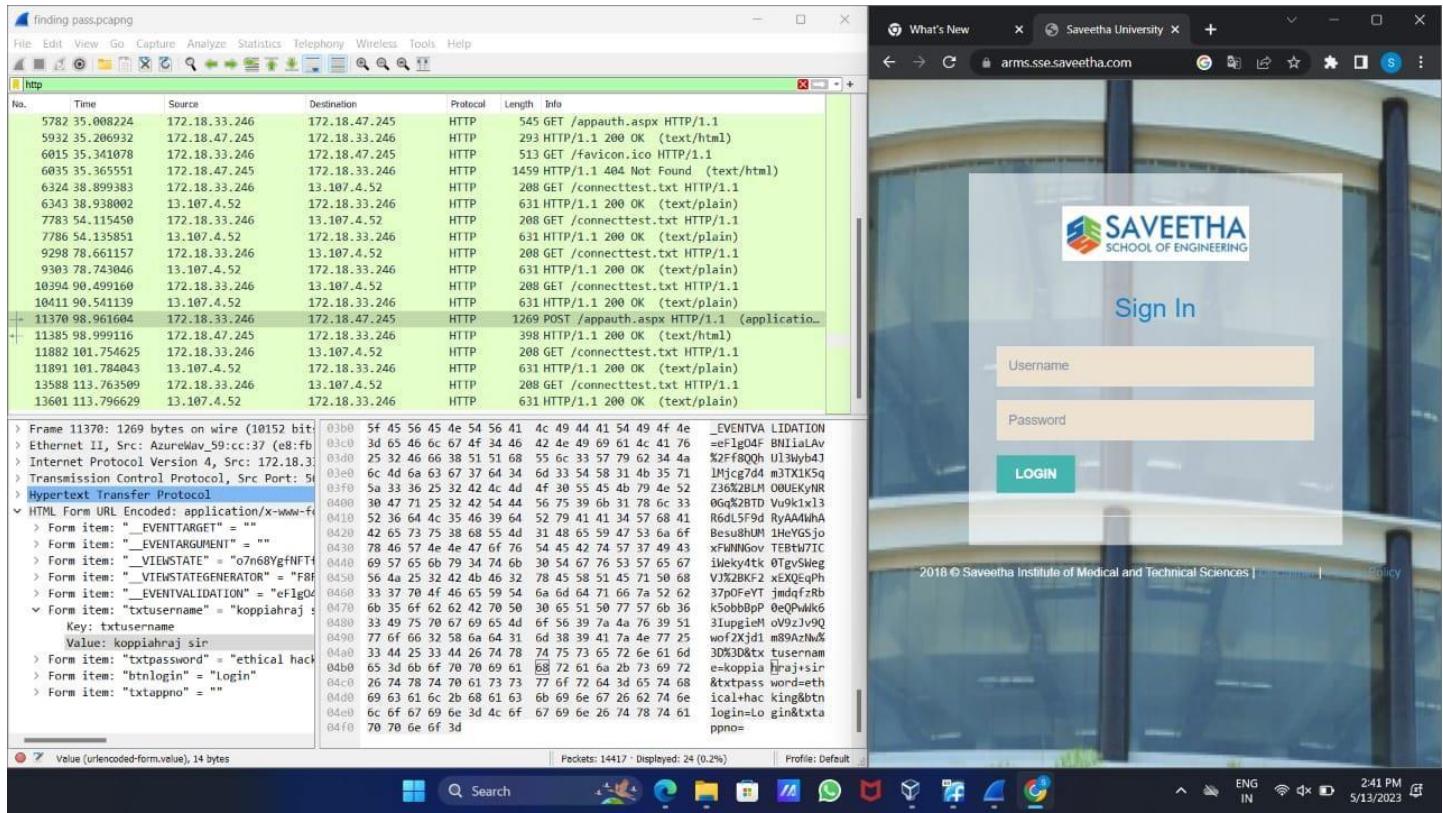
This screenshot shows a different session in NetworkMiner. A POST request to `http://arms.sse.saveetha.com` is selected, showing the raw data: [HTTP request 2/2] [Prev request in frame: 72877] [Response in frame: 89219]. The raw data includes form items like `_VIEWSTATE`, `_VIEWSTATEGENERATOR`, `_EVENTVALIDATION`, `txtusername`, `txtpassword`, and `btnlogin`. The browser window shows a 'Sign In' page for 'SAVEETHA SCHOOL OF ENGINEERING'. The user has entered 'admin' for the username and '*****' for the password. An error message 'The username and password you entered is invalid' is displayed below the login fields.

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)



Result:

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

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

Requirements:

- Kali linux running as an attacker machine

- Windows 7 running as virtual machine

- Admin privileges **Procedure:**

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

- 2.Type “sudo apt-get update” command

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

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

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

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

```

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, bim, 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 svrsvc. Error was NT_STATUS_ACCESS_DENIED
[+] Users on 172.20.10.5

 33°C
Partly sunny
  ENG
  IN
  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:~[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 polonium:
[*] 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 ENG IN 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 ENG IN 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

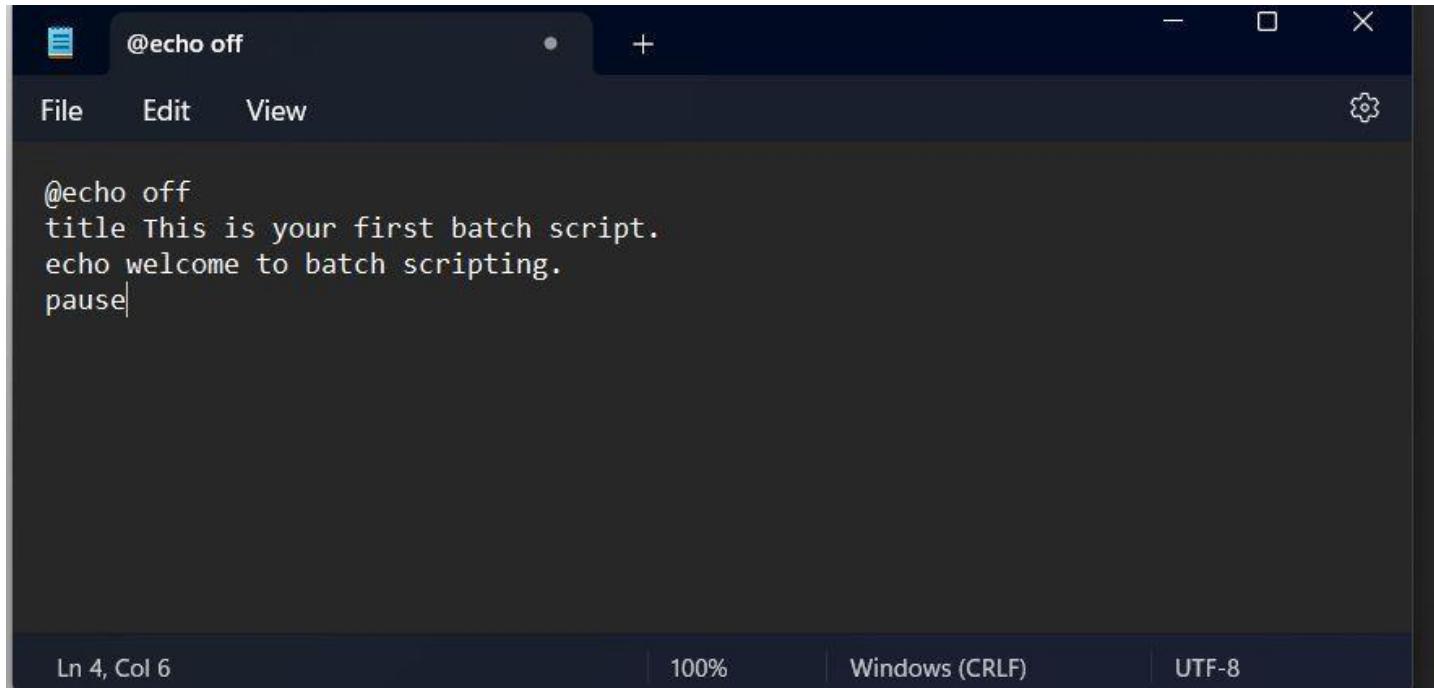
The above script echoes back the text "Welcome to batch scripting!" Save your file by heading to File > Save As, and then name your file what you'd like. End your file name with the added BAT extension, for example test.bat, and click OK. This will finalize the batch process. Now, double-click on your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

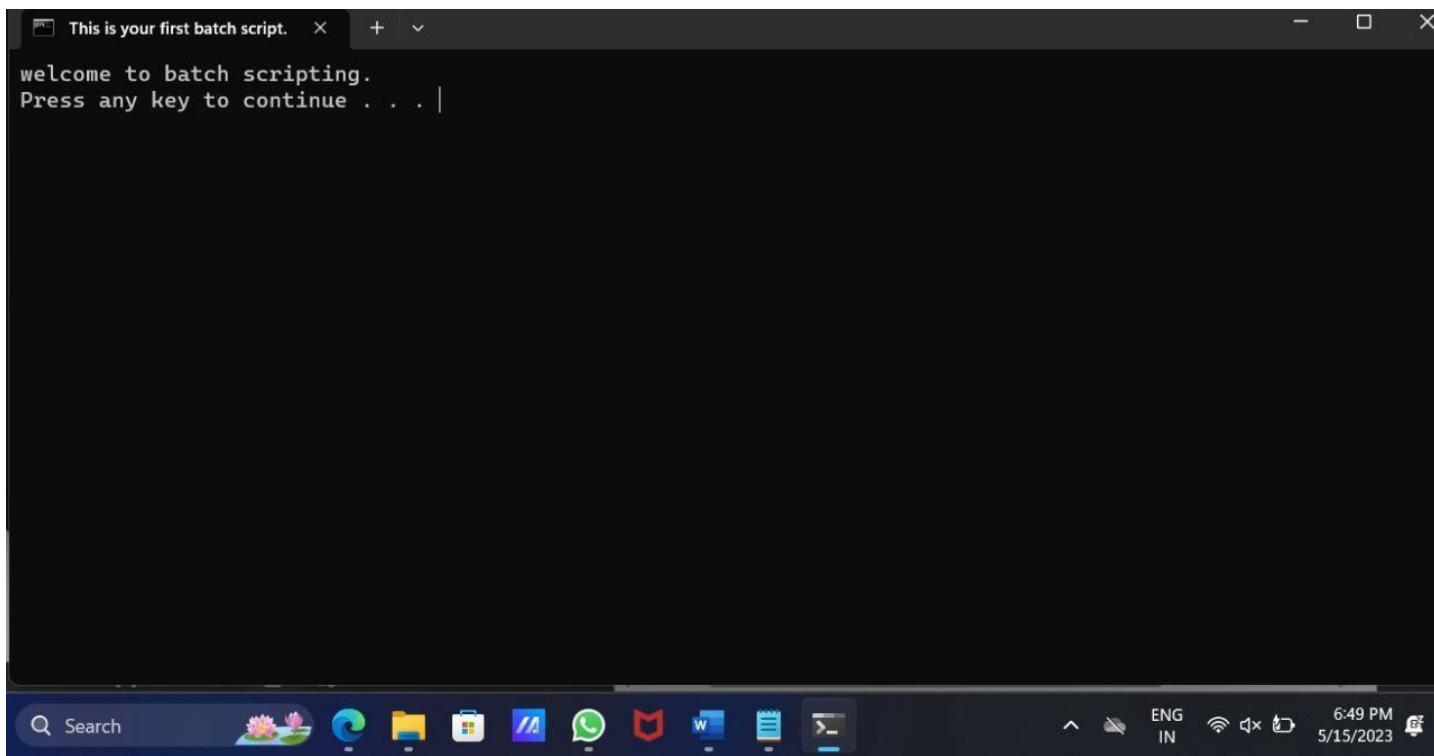
Result:



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 text:

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

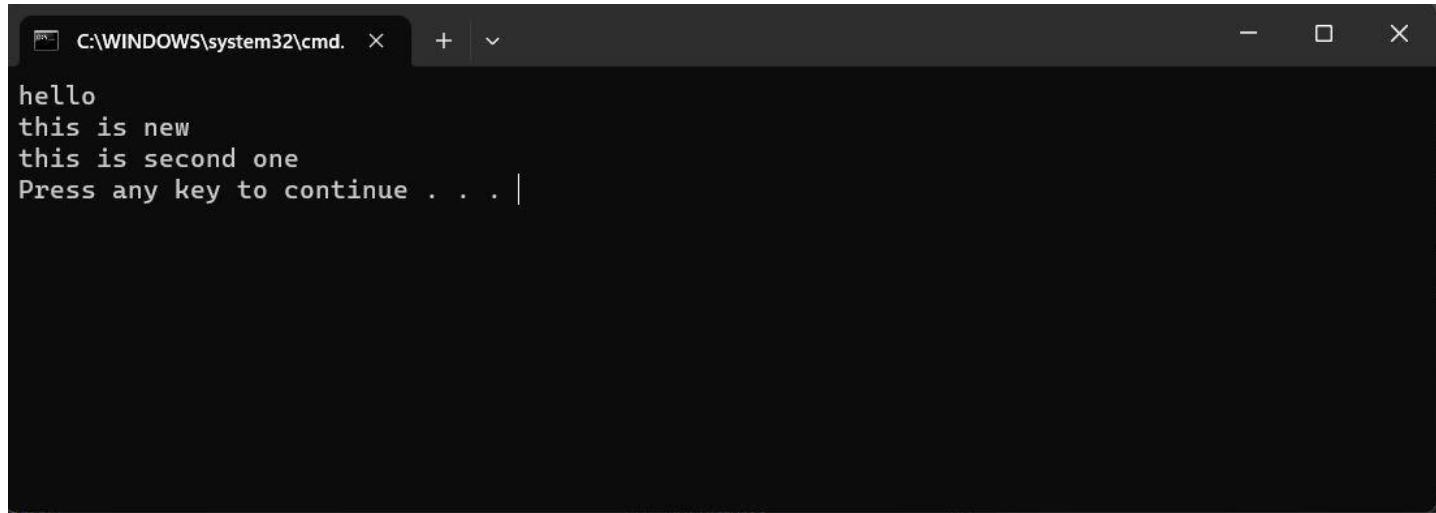
The status bar at the bottom shows 'Ln 4, Col 6' on the left, '100%' in the center, and 'Windows (CRLF)' and 'UTF-8' on the right.



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

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

The taskbar at the bottom shows various pinned icons, including a search bar, file explorer, and messaging apps. The system tray shows the date and time as '5/15/2023 6:49 PM'.



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.