

ITA1466-ETHICAL HACKING

LAB MANUAL

Exercise No 1: Nmap Scan

NAME : P.yugendhar. Reg no:192111639
--

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:

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

```
[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
```

Step 3:-

To perform host discovery

```
[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

Step4:-

Port Specification

```
[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

Step 5:-

Service Version and OS Detection

```
[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
```

```
[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
```

Result:

Exercise No 2: Vulnerability Access Scan Using Nessus

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

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

Nessus

Downloads / Nessus

Nessus

1 Download and Install Nessus

Choose Download

Version: Nessus - 10.4.2 | Platform: Windows - x86_64

[Download](#) [Checksum](#)

[Download by curl >](#)

[Docker & Virtual Machines >](#)

2 Start and Setup Nessus

Open Nessus and follow setup wizard to finish setting up Nessus

3 Getting Started

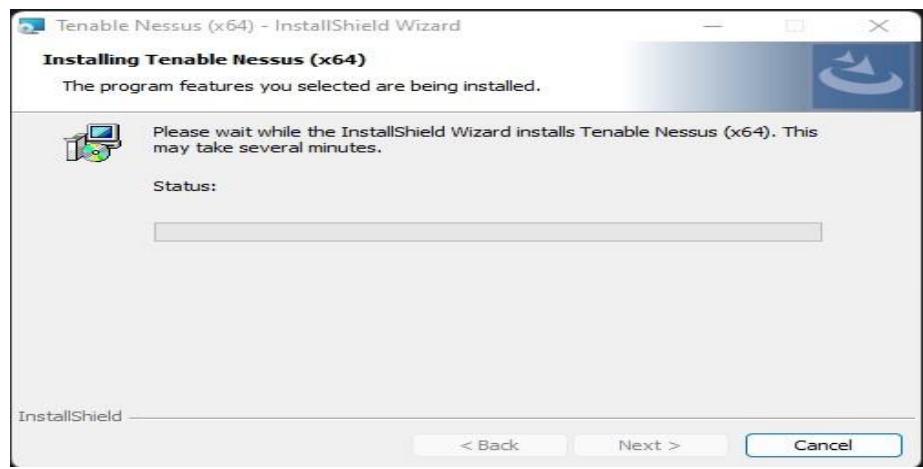
Summary

Release Date: Jan 18, 2023

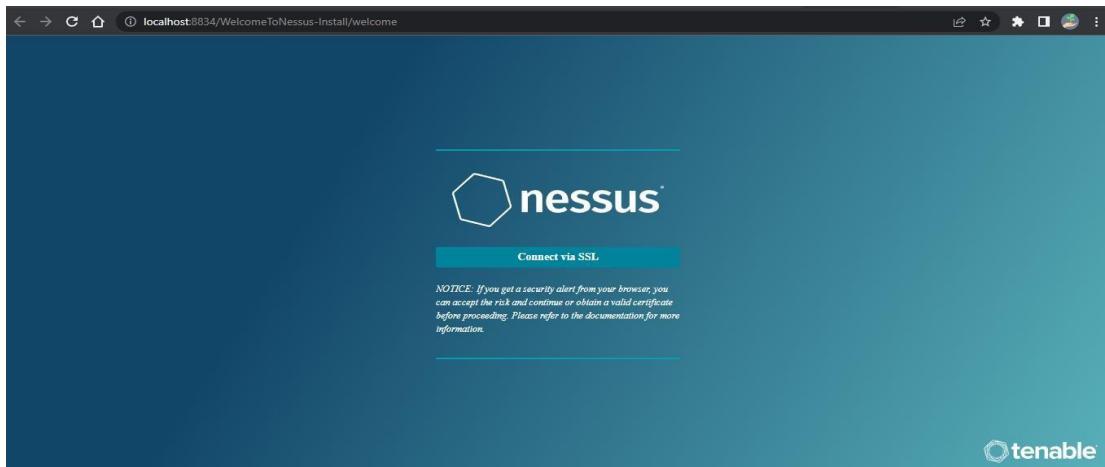
Release Notes: [Nessus 10.4.2 Release Notes](#)

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

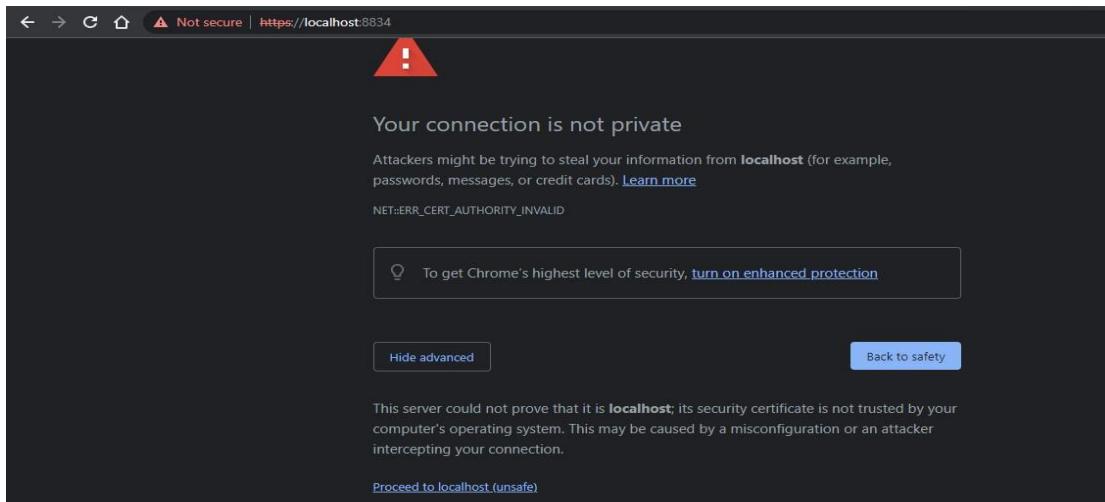
Step 2: Choose your OS and download , install



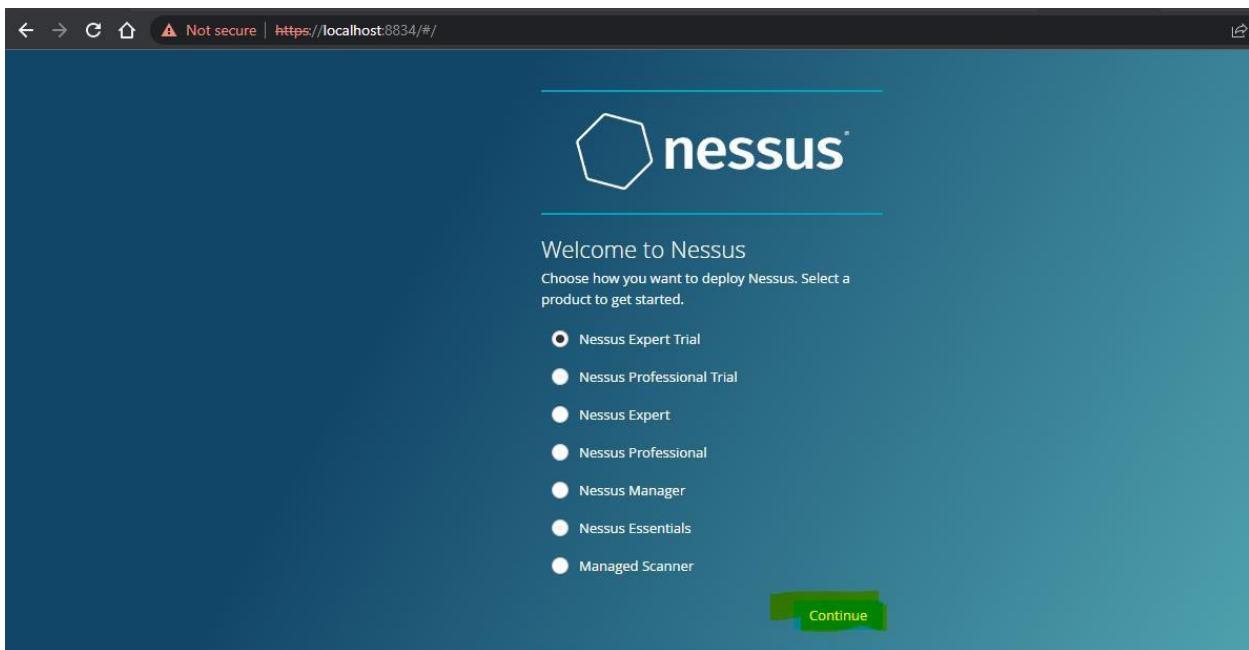
Step 3: Once installation is completed it will open in default browser



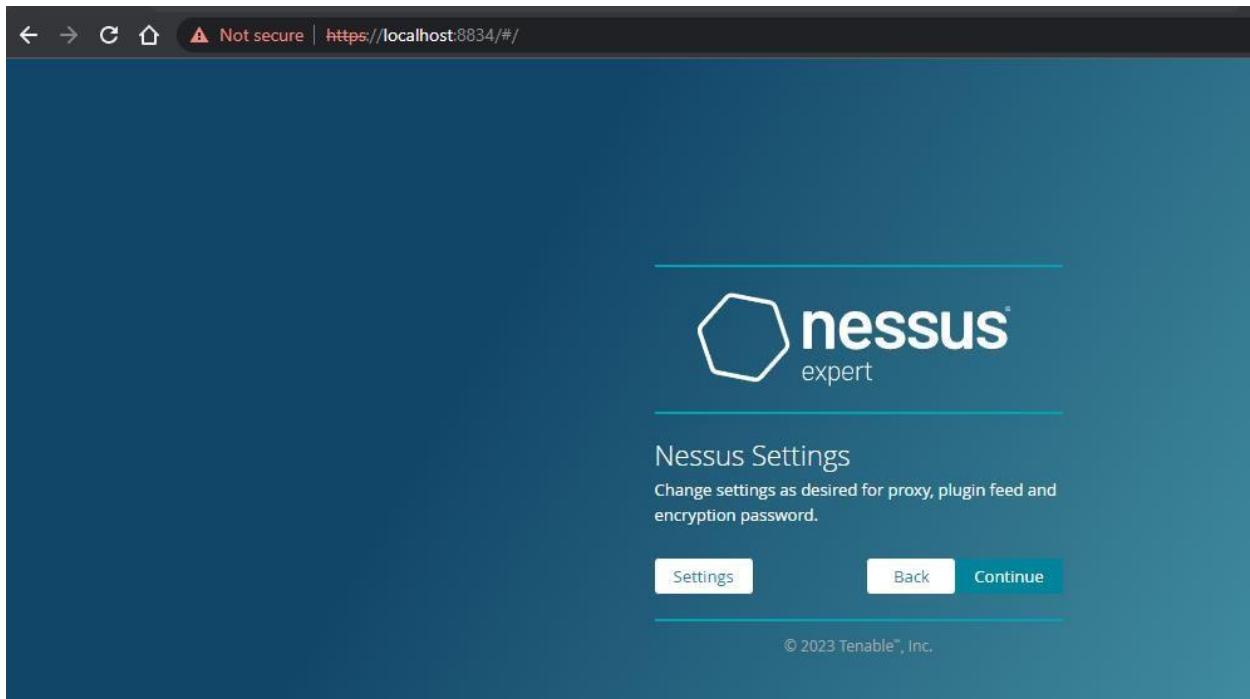
Step 5:- (click on the proceed to local host)



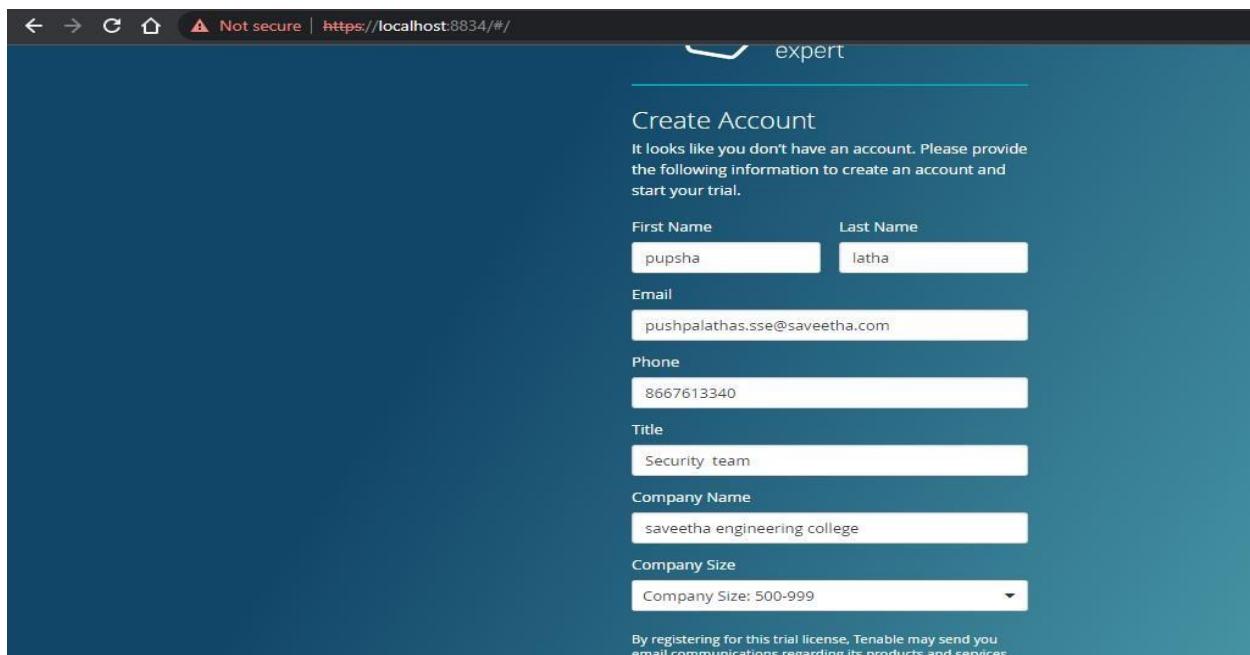
Step 6:- Please choose the Nessus Expert



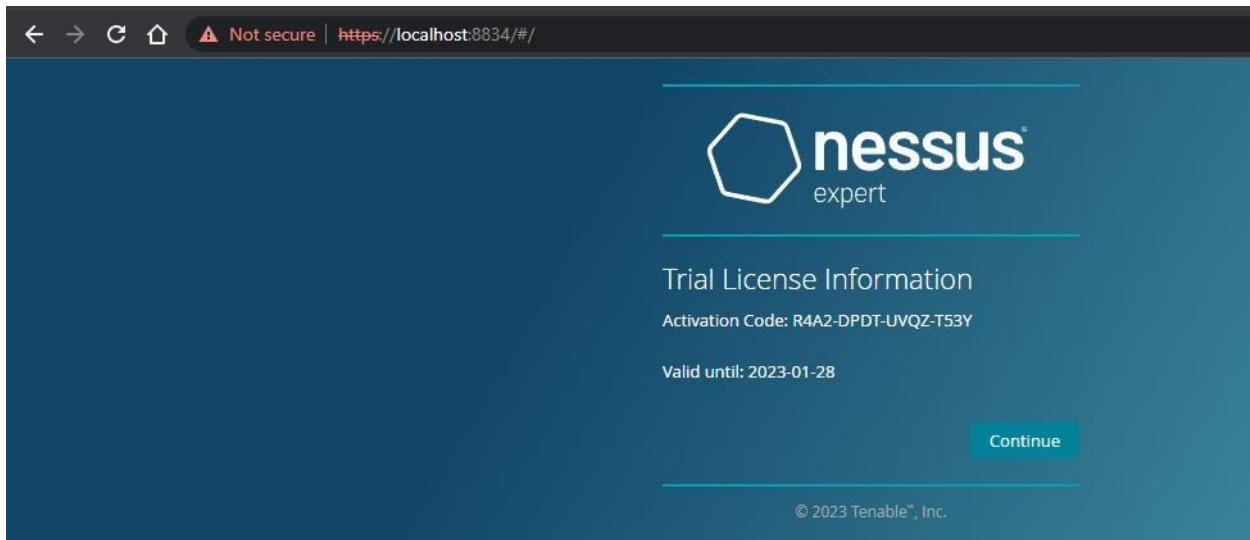
Step 7: Click on continue



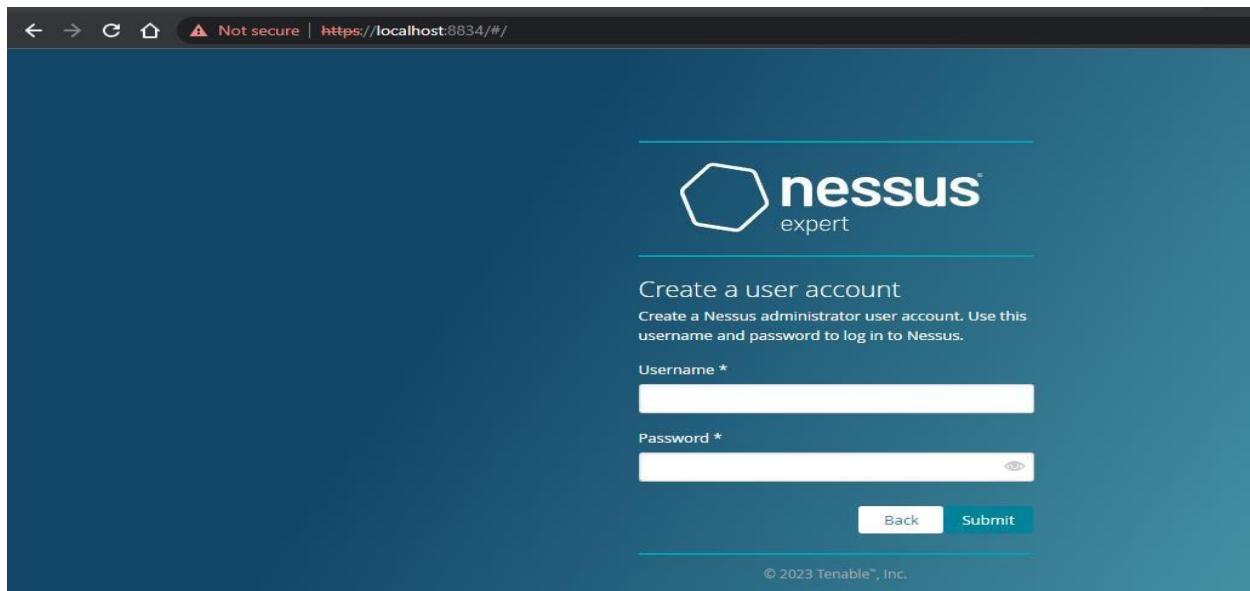
Step 8:- Register with your organizational email id



Step 9:- please note down the activation key



Step 10:- set up your username & password



Step 11:-Type username and password

← → ⌂ ⌄ ▲ Not secure | https://localhost:8834/#/



nessus
expert

Create a user account

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

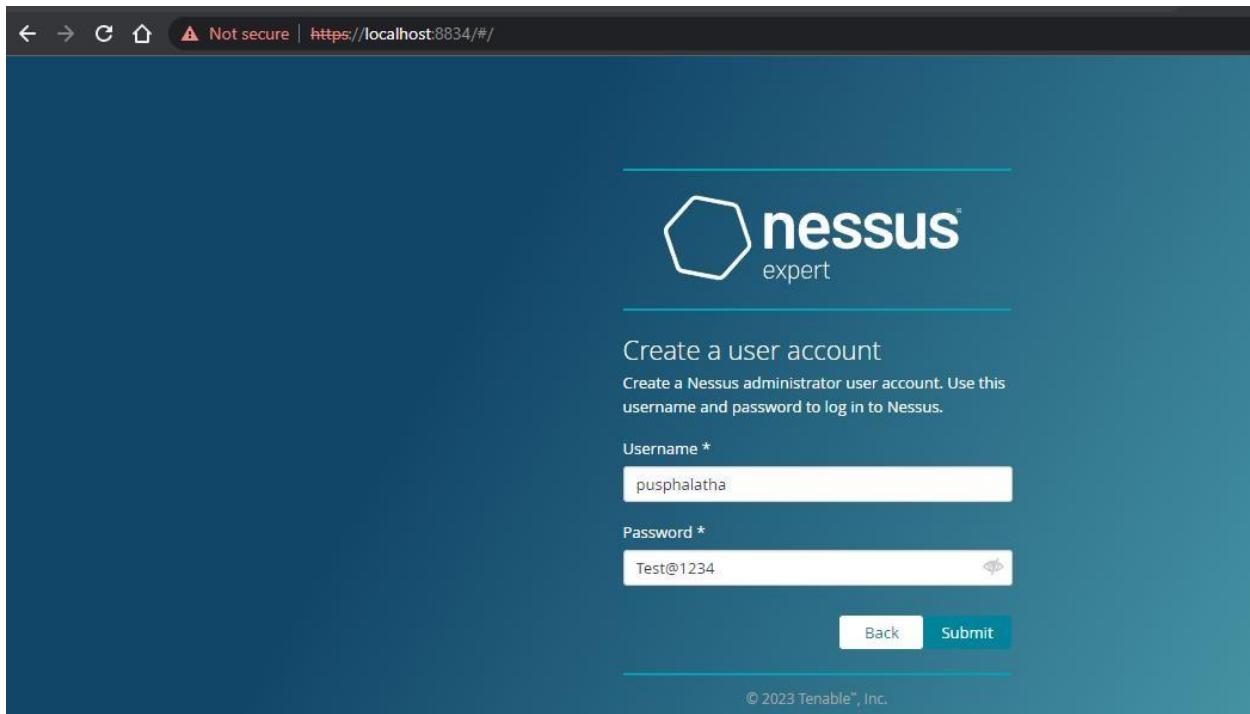
Username *

Password *

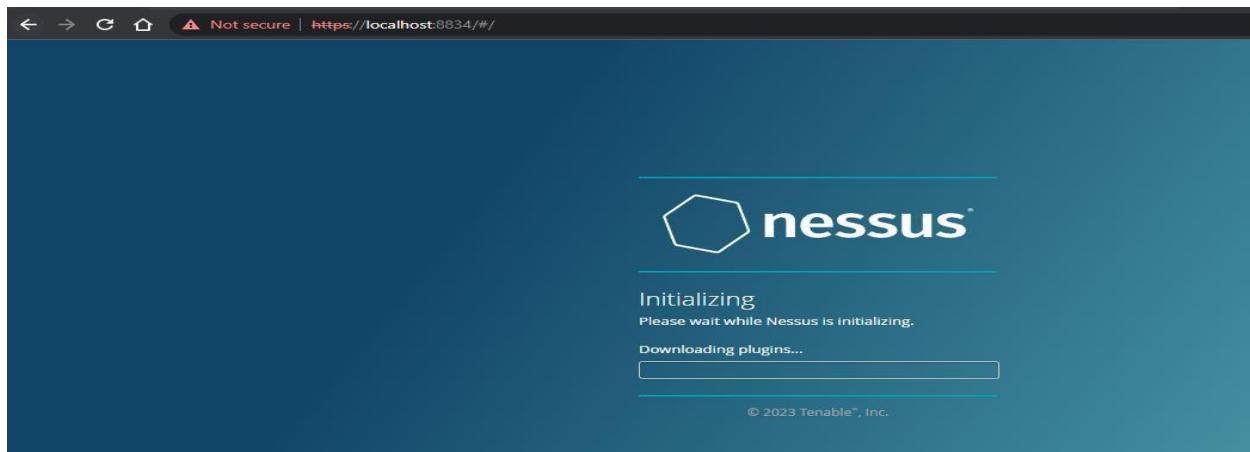
 

[Back](#) [Submit](#)

© 2023 Tenable™, Inc.



Step 12:- Please wait until download is completed



This screenshot shows the Nessus web interface. The left sidebar has sections for FOLDERS (My Scans, All Scans, Trash), RESOURCES (Policies, Plugin Rules, Customized Reports, Terrascan), and a status bar at the bottom showing '70°F Haze'. 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'.

Out Put:

A new version of Nessus is available and ready to install. [Learn more](#) or [apply it now](#).

Scans Settings

saveetha [Back to All Scans](#)

Scan Summary Hosts 1 Vulnerabilities 14 Notes 2 History 4

Scan Details

Critical Vulnerabilities	High Vulnerabilities
0	0

Medium Vulnerabilities	Low Vulnerabilities
1	0

Details

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

Top 5 Operating Systems Detected During Scan

Authentication / Credential Info (Hosts)

0 SUCCEEDED	1 FAILED
-------------	----------

Scan Durations

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

Scan Notes

The screenshot shows the Nessus application interface. On the left, there's a sidebar with 'Folders' (My Scans, All Scans, Trash), 'Resources' (Policies, Plugin Rules, Customized Reports, Terrascan), and a 'Scans' tab. The main area displays two 'DNS Issue' notifications: 'Unable to resolve log4shell-generic-pH2jjhqiaCfpXP50Q057.r.nessus.org, please check your DNS configuration or retry the scan later' and 'Log4j DNS Failed Request' with the message 'Unable to resolve DNS r.nessus.org' to check Log4j Vulnerability. Below these are sections for 'Policy Details' (Basic Overview, Report Overview, Credential Settings Overview, Fragile Devices), 'Assessment Overview' (Override Normal Accuracy: Normal, Perform Thorough Tests: No, Enable CGI Scanning: No), 'Advanced Overview' (Enable Safe Checks: Yes, Network Timeout (In Seconds): 5), and 'Port Scanner Overview' (SYN: Yes, UDP: No, TCP: No, Port Scan Range: default). At the bottom, there's a taskbar with icons for various applications like File Explorer, Edge, and Google Chrome.

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

```
[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 PentestTools.
[!] Missing API key for Securitytrail.
[!] Missing API key for ProjectDiscovery.
[!] Missing API key for Hunter.
[!] Missing API key for zoomeye.
[!] Missing API key for Censys ID and/or Secret.
[!] Missing API key for Intelx.
[!] Missing API key for RocketReach.

[+] Missing API key for Github.
[*] Searching tricase...
[*] Searching Rapid7...
[*] Searching Shodan...
[*] Searching VirusShare...
[*] Searching 0 results.
[*] Searching Shodan...
[*] Searching 100 results.
[*] Searching Omission...
[*] Searching Omission...
```

Command: theHarvester -d www.zoho.com -l 3

9
00 -ball

```
kali-linux-2022.3-vmware-amd64 - VMware Workstation 16 Player (Non-commercial use only)
Player | [ ] 1 2 3 4 | root@kali: ~

File Actions Edit View Help
    Searching 300 results.
[*] Searching LinkedIn.
An exception has occurred: 0, message='Attempt to decode JSON with unexpected mimetype: text/html', url=URL('https://api.n45ht.or.id/v1/subdomain-enumeration?domain=www.zoho.com')
[*] Searching Threatminer.
[*] Searching Crt.sh.
[*] Searching Baidu.
An exception has occurred: Cannot connect to host www.baidu.com:443 ssl<:ssl.SSLContext object at 0x7f7884f4fc0> [Connection reset by peer]
[*] Searching Threatcrowd.
[*] Searching CTF4.
[*] Searching VirusShare.
Google is blocking your ip and the workaround, returning
[*] Searching Sodinster.
    Searching 0 results.
[*] Searching Shodan.
[*] Searching Duckduckgo.
Google is blocking your ip and the workaround, returning
[*] Searching 0 results.
An exception has occurred: Cannot connect to host dns.bufferover.run:443 ssl<:ssl.SSLContext object at 0x7f7884ddfb40> [Name or service not known]
Google is blocking your ip and the workaround, returning
    Searching 100 results.
Google is blocking your ip and the workaround, returning
    Searching 200 results.
Google is blocking your ip and the workaround, returning
    Searching 300 results.
[*] Searching Google.
[*] ASNs found: 7
AS1335
AS139006
AS141757
AS3237
AS2639
AS41913
AS63949
[*] Interesting URLs Found: 25
https://www.zoho.com/
https://www.zoho.com/assist/
https://www.zoho.com/books/
https://www.zoho.com/campaigns/?zsrc=fromproduct
https://www.zoho.com/explainer/campaign-view.html
https://www.zoho.com/campaigns/explainer/zcsend.html
https://www.zoho.com/chats?serviceurl=%2Fchats%2F22431772755001510080zsrc=fromproduct
https://www.zoho.com/cliq/?serviceurl=%2Findex.dobzsrc=fromproduct
https://www.zoho.com/contactus.html
Cloudy 34°C 13:46 ENG IN 14-09-2022
```

```
kali-linux-2022.3-vmware-amd64 - VMware Workstation 16 Player (Non-commercial use only)
Player | [ ] 1 2 3 4 | root@kali: ~

File Actions Edit View Help
AS63949
[*] Interesting URLs Found: 25
https://www.zoho.com/
https://www.zoho.com/assist/
https://www.zoho.com/books/
https://www.zoho.com/campaigns/?zsrc=fromproduct
https://www.zoho.com/explainer/campaign-view.html
https://www.zoho.com/explainer/zcsend.html
https://www.zoho.com/chats?serviceurl=%2Fchats%2F2431772755001510080zsrc=fromproduct
https://www.zoho.com/cliq/?serviceurl=%2Findex.dobzsrc=fromproduct
https://www.zoho.com/contactus.html
https://www.zoho.com/contactus/error/
https://www.zoho.com/crm/
https://www.zoho.com/crmplus/
https://www.zoho.com/de/cm/
https://www.zoho.com/dmsender/
https://www.zoho.com/forms/
https://www.zoho.com/invoice/?utm_source=Z0Gutm_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/?zrc=zoho-home&amp%3Bireft=ohome
https://www.zoho.com/report-abuse/
https://www.zoho.com/salesiq/
https://www.zoho.com/survey/
[*] No Twitter users found.

[*] LinkedIn Users found: 292
Asael Mohammed - Regional Account Manager
Abbas Abu - Zoho One Developer
Abhilash Reddy Godishala
Adarsh Pandey - Member of Technical Staff
Adithyan Ravichandran - Lead System Engineer
Ajay Singh - Software Developer - Zoho
Ajay Singh - Developer - ZOHO CRM
Akash Krishnan - Member Technical Staff
Akilan Ramamirtham
Akash Chaitanya Sekar - Zoho Corporation
Ali Shaabdar - Regional Director MEA
Alok Kumar Bharti - Software Engineer
Aman Gupta - Zoho Developer
Anand Kumar - Zoho Developer
Ambi Moorthy - Product Manager and Co-Founder
Anandaraman Krishnan - Product Manager
Cloudy 34°C 13:46 ENG IN 14-09-2022
```

```
kali-linux-2022.3-vmware-amd64 - VMware Workstation 16 Player (Non-commercial use only)
Player | || | 1 2 3 4 | 
root@kali:~#
File Actions Edit View Help
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
Amaranth KR - Zoho Developer
Ambi Moorthy - Product Manager and Co-Founder
Anandaraman Krishnan - Product Manager
Ananthu Subramanian - Engineer Trainee
Ananthu Nair - Presales Engineer - Zoho Corporation
Andrea Mahoney - VP - Certified Computer Solutions
Andrew Bourne
Andrew Joseph - Zoho Corporation
Andrews B A - Senior Member Of Technical Staff
Anubhav Pandey - Zoho Consultant
Anumita Gupta - Technical Writer
Aravind Krishnamoorthy - Zoho Corporation
Arun Balachandran - Senior Product Marketing Manager
Arun Kesavan - Product Designer
Arun Selvamuthu - Product Marketer
Arvind Krishnamoorthy
Ashok Chakravarthi Nagarajan
Ashok Kumar
Ashwin Venkateswaran - Lead - Zoho CRM SME
Avinanth B - Software Developer - Zoho
Azarudeen M
Barati Haridasan - Senior Technical Support Engineer
Bala Balachch
Bala Krishnan - Product Marketer
Bala Sundar - Member Technical Staff
Balaji Sanketkraman
Balaji Venkateswaran - Product Manager
Barath Kumar Ramesh - Member Leadership Staff
Bashirul Haque Faisal - Zoho Consultant
Bennett Samuel - Zoho Developer
Bharath Kumar
Bharathi Anbazhagan - Member Technical Staff
Calvin Jasher - Quality Analyst- Zoho CRM Support
Carlton Dill
Chakravarthi Radhakrishnan - Zoho Corporation
Chandru Jayapalan - Zoho Corporation
Charles Diaz
Cheeta K - Zoho CRM Consultant - Regal Infonet
Chitrapandian Nachiapalan - Senior Product Director
Clarence Rozario - Director of Product Management
Comptech Infonet Management
D Jayaraaj - Visual Designer
DEVENDRA KUSHWAH - Zoho Developer
David Elkins - Head of Content Review
Deepak RV - Enterprise Support Engineer - Zoho
34°C
Cloudy
root@kali:~#
ENG IN 13:46 14-09-2022 19
```

```
kali-linux-2022.3-vmware-amd64 - VMware Workstation 16 Player (Non-commercial use only)
Player | || | 1 2 3 4 | 
root@kali:~#
File Actions Edit View Help
J Jayaraghavan venugopal
Vinothkumar R - Product Manager
Vinothkumar R - Product Manager - Zoho Corporation
Vipasha Sinha - Senior Product Marketer
Vishnukumar Moorthy - Member Technical staff
Vishwanand Venkateswaran
Yogendrababu venkatapathy - Co-Founder
Yogesh Manoharan - Regional Director
ZOHO CRM Developer - AZZ SAMS Private Limited
Eduardo Jose - Developer
Zoho Developer
Zoho Expert Services - GENOWIRE
balaji m - Developer - Zoho Corporation
bhupesh kumar - Developer
rangarajan ramesh - Account Manager - Zoho
sathiyam sathiyamarsva - zoho - Zoho Corporation
shaiq Afreen tal - Senior Technical Support Engineer
vaidheevanneewar - Senior Executive
working as a Senior executive at IndiGo Airlines
[*] LinkedIn Links found: 0
Aamil Mohammed - Regional Account Manager
Abbas Abu - Zoho One Developer
Abhilash Reddy Godishala
Adithyan Ravichandran - Member of Technical Staff
Adithyan Ravichandran - Lead System Engineer
Ajay George - Partner Support Engineer - ZOHO CRM
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
Amaranth KR - Zoho Developer
Ambi Moorthy - Product Manager and Co-Founder
Anandaraman Krishnan - Product Manager
Anantha Subramanian - Engineer Trainee
Ananthu Nair - Presales Engineer - Zoho Corporation
Andrea Mahoney - VP - Certified Computer Solutions
Andrew Bourne
Andrew Joseph - Zoho Corporation
Andrews B A - Senior Member Of Technical Staff
Anubhav Pandey - Zoho Consultant
Anumita Gupta - Technical Writer
Aravind Krishnamoorthy - Zoho Corporation
Arun Balachandran - Senior Product Marketing Manager
Arun Kesavan - Product Designer
Arun Selvamuthu - Product Marketer
Arvind Krishnamoorthy
Ashok Chakravarthi Nagarajan
34°C
Cloudy
root@kali:~#
ENG IN 13:47 14-09-2022 19
```

```
Vinothkumar R - Product Manager - Zoho Corporation
Vipasha Sinha - Senior Product Marketer
Visithkumar Moorthy - Member Technical staff
Visithkumar Moorthy - Member Technical staff
Yogendrababu venkatapathy - Co-Founder
Yogesh Manoharan - Regional Director
Zoho Cloud Developer - A2Z SaaS Private Limited
Zoho Account - Developer
Zoho Developer
Zoho Expert Services - GENOWIRE
Zoho Global Devops - Zoho Corporation
zheprakash v - iOS Developer
rangarajan ramesh - Account Manager - Zoho
satish sathiyamurthy - zoho - Zoho Corporation
shankar Afridi - Senior Technical Support Engineer
vasudevanne T - Lead
working as a Senior executive at IndiGo Airlines

[*] Trello URLs found: 33
http://www.trello.com/contact
http://www.trello.com/integrations
https://trello.com/integrations/sales-support
https://trello.com/power-ups
https://trello.com/power-ups/55e089fafaf17d2fa455fd4
https://trello.com/power-ups/594c1aa1922a254295bb0a35/zoho-crm
https://trello.com/power-ups/5b55db5704cc25f2981fd473/automateio
https://trello.com/power-ups/5ba22bdcd8adab995eadc98
https://trello.com/power-ups/5c1a2a2a254295bb0a35/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/privacy
https://trello.com/teams/support
https://trello.com/templates
https://trello.com/templates/design/design
https://trello.com/templates/design/design-system-checklist-yzn5vfon
https://trello.com/templates/design/freelance-branding-project-z5m6hsj
https://trello.com/templates/design/research-iteration-8thqmgz
https://trello.com/templates/product-management/3-etapas-de-gerenciamento-de-produtos-7s8avmvu
https://trello.com/templates/product-management/5-listes-pour-la-gestion-de-produits-0lufgyd7
https://trello.com/templates/product-management/7-etapes-de-gestion-de-produits-0n7snkwjt8
https://trello.com/templates/product-management/constindo-um-planilha-shynjpris
https://trello.com/templates/product-management/fabrication-process-dakyjp35
https://trello.com/templates/product-management/product-roadmap-template-frbabjsb
https://trello.com/templates/product-management/project-management-planifiable
https://trello.com/templates/product-management/roadmap-product-ipdk1x39
https://trello.com/templates/product-management/shipping-planner-mc3vzive
https://trello.com/tour
https://trello.com/use-cases/crm
```

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 .

Out Put:

```
[*] 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.
```

Exercise No 4- Open Source Intelligence Gathering Using OSRFramework

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

Procedure:

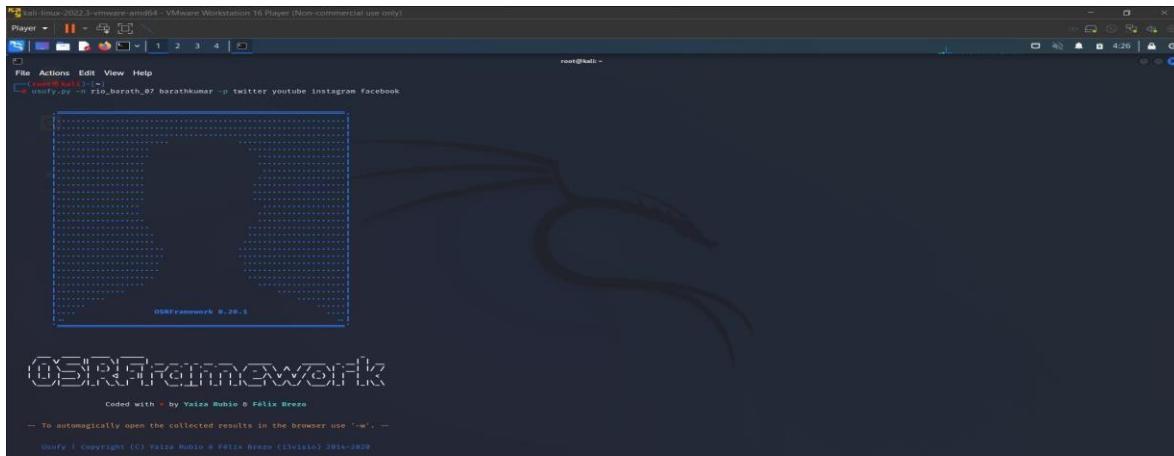
Step 1: Log into kali linux machine

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

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

Command:

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



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

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

```
root@halli:~# usufy.py -n rie_barath_07 barathkumar -p twitter youtube instagram facebook
2022-09-16 06:12:51.515293      Starting search in 4 platform(s) ... Relax!
Press Ctrl + C to stop...
2022-09-16 06:12:51.515293      Results obtained (4):
/usr/lib/python3/dist-packages/xpexcel/deprecated.py:208: UserWarning: Deprecated usage since v0.2.1! Explicit import is no longer required. pxcel.xlsx is auto imported.
  warnings.warn("Deprecated usage since v0.2.1! Explicit import is no longer required. pxcel.xlsx is auto imported.", UserWarning)
[Projects Recovered (2022-9-16, 0h23m):]
+-----+-----+-----+
| com.i3visio.Uri | com.i3visio.Alias | com.i3visio.Platform |
+-----+-----+-----+
| https://www.youtube.com/user/rie_barath_07/about | rie_barath_07 | YouTube |
| https://www.facebook.com/rie_barath_07 | rie_barath_07 | Facebook |
| https://www.instagram.com/rie_barath_07 | rie_barath_07 | Instagram |
| http://twitter.com/rie_barath_07 | rie_barath_07 | Twitter |
| https://www.youtube.com/user/barathkumar/about | barathkumar | YouTube |
| https://www.facebook.com/barathkumar | barathkumar | Facebook |
| https://www.instagram.com/barathkumar | barathkumar | Instagram |
| http://twitter.com/barathkumar | barathkumar | Twitter |
+-----+-----+-----+
2022-09-16 06:12:51.515293      You can find all the information here:
./profiles.csv
2022-09-16 06:12:51.515293      Finishing execution...
Total time consumed: 0:00:06.185075
Average seconds/query: 1.54626875 seconds

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

Out Put:

```

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

File Actions Edit View Help
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!

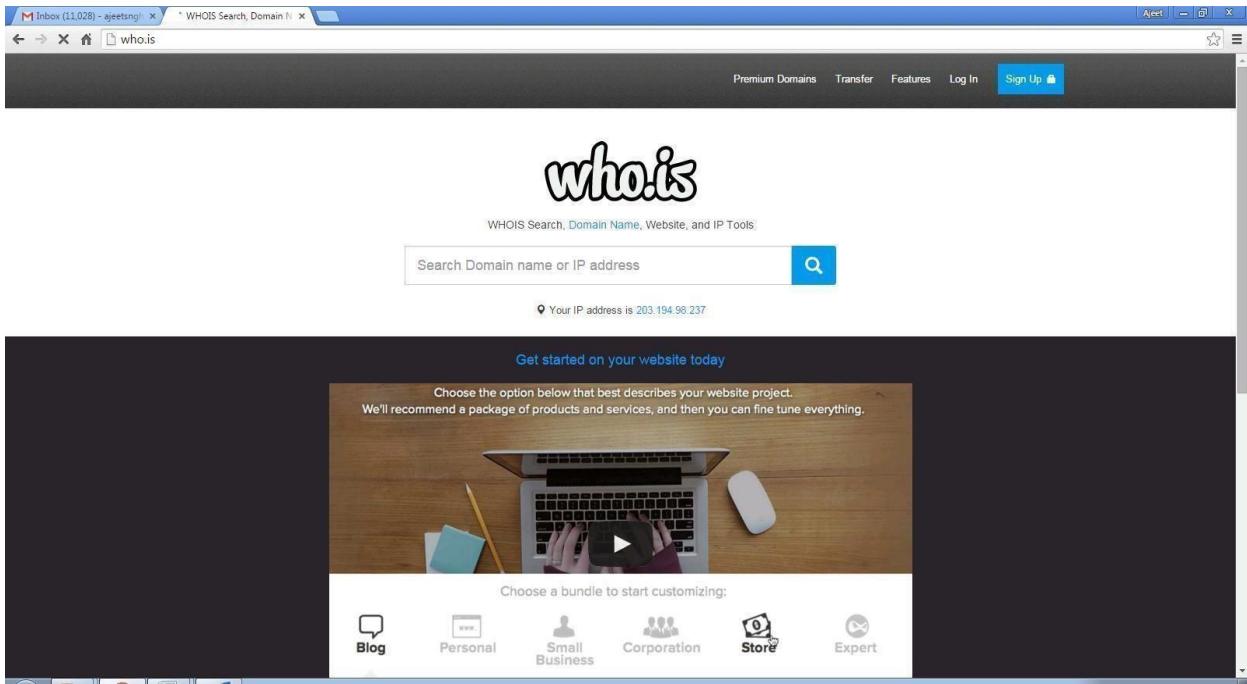
```

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 who.is WHOIS search results for the domain `saveetha.com`. The page includes sections for Registrar Info, Important Dates, Name Servers, Similar Domains, Registrar Data, Site Status, and Suggested Domains.

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:

Name Server	IP Address
ns51.domaincontrol.com	97.74.105.26
ns52.domaincontrol.com	173.201.73.26

Similar Domains:

- savee-board.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

Registrant Contact Information:

Name	Organization	Address
Dr N.H.Veeraiyan	Saveetha Dental College & Hosp.	Saveetha University Saveetha Nagar, Thandaim Campus

Site Status:

Status	Active
Server Type	Squarespace

Suggested Domains for saveetha.com

Domain	Price
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.

Out Put:

The screenshot shows the in.godaddy.com WHOIS search results for the domain `www.saveetha.com`. The page features a search bar at the top and a main content area with a "WHOIS search results" section and a "Find your Domain" sidebar.

WHOIS search results:

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

Find your Domain

Find your perfect domain

ENG IN 2:03 PM 5/13/2023

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-vsln.net.in [14.141.20.165]
 7  12 ms    10 ms   *     172.31.167.45
 8  10 ms   11 ms    8 ms  ix-ae-4-2.tcore1.cxr-chennai.as6453.net [180.87.36.9]
 9  43 ms    *       *     if-be-34-2.ecore2.esin4-singapore.as6453.net [180.87.36.41]
10  42 ms   45 ms   50 ms  if-be-10-2.ecore2.svq-singapore.as6453.net [180.87.107.0]
11  *       *       *     Request timed out.
12  *       *       *     Request timed out.
13  *       *       *     Request timed out.
14  *       *       *     Request timed out.
15  *       *       *     Request timed out.
16  *       *       *     Request timed out.
17  *       *       *     Request timed out.
18  *       *       *     Request timed out.
19  *       *       *     Request timed out.
20  *       *       *     Request timed out.
21  *       *       *     Request timed out.
22  *       *       *     Request timed out.
23  *       *       *     Request timed out.
24  *       *       *     Request timed out.
25  *       *       *     Request timed out.
26  *       *       *     Request timed out.
27  *       *       *     Request timed out.
28  *       *       *     Request timed out.
29  *       *       *     Request timed out.
30  *       *       *     Request timed out.

Trace complete.
```

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

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

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

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

Step 3: Type ifconfig command

```
suse1:-# ifconfig
eth0      Link encap:Ethernet HWaddr 00:0C:29:17:1B:27
          inet addr:192.168.208.133 Bcast:192.168.208.255 Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe17:1b27/64 Scope:Link
            UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
            RX packets:195 errors:0 dropped:0 overruns:0 frame:0
            TX packets:189 errors:0 dropped:0 overruns:0 carrier:0
            collisions:0 txqueuelen:1000
            RX bytes:21313 (20.8 Kb) TX bytes:16778 (16.3 Kb)

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

Step 4: Type netstat c

```
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
```

Out Put:

```
A Command Prompt + 36351101.r24f.6eh0.0401.54d7... X
Shop Microsoft Windows [Version 10.0.22621.1555]
(c) Microsoft Corporation. All rights reserved.

Th C:\Users\Sumanth>tracert saveetha.com
SI
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.
G  5 SumanthReddy [192.168.226.91] reports: Destination host unreachable.

C Trace complete.

I C:\Users\Sumanth>ping 192.185.159.145
Y Pinging 192.185.159.145 with 32 bytes of data:
Request timed out.
Request timed out.
gog 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>
Audacity VLC media player old WhatsApp Hacking La...
P psiphon3 qBittorrent
Link encap:Local Loopback
inet addr: fe80::2c0:2ff%1 brd fe80::ff:ff%1 Mask:255.0.0.0
inet6 addr: ::1/128 Scope:Host
UP LOOPBACK RUNNING MTU:16496 Metric:1
RX packets:109 errors:0 dropped:0 overruns:0 frame:0
collisions:0 txqueuelen:1000
bytes:21319 (20.8 Kb) Tx bytes:16778 (16.3 Kb)
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:16496 Metric:1
RX packets:18 errors:0 dropped:0 overruns:0 frame:0
bytes:1419 (1.4 Kb) Tx bytes:1419 (1.4 Kb)
C: \Users\Sumanth>
C: \Users\Sumanth>
C: \Users\Sumanth>
Windows Search 2:09 PM 5/13/2023 ENG IN
```

```
A Command Prompt + 36351101.r24f.6eh0.0401.54d7... X
Shop Microsoft Windows [Version 10.0.22621.1555]
(c) Microsoft Corporation. All rights reserved.

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

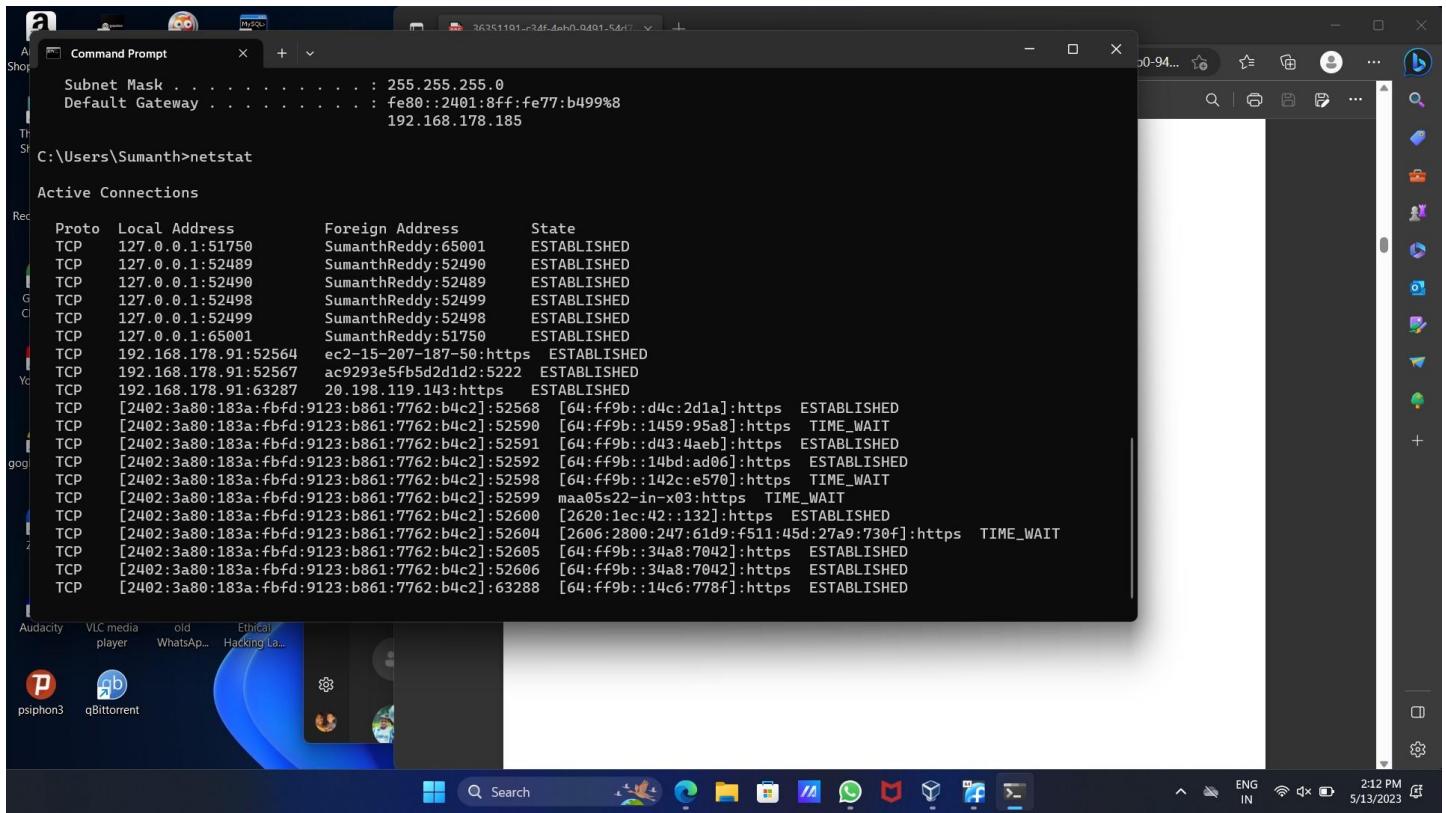
C: \Users\Sumanth>ipconfig
Windows IP Configuration

Rec
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 . :
Audacity VLC media player old WhatsApp Hacking La...
P psiphon3 qBittorrent
TCP 192.168.0.57:25072 test:https TIME_WAIT
TCP 192.168.0.57:25078 a23-56-105-111:https ESTABLISHED
TCP 192.168.0.57:25080 10.0.0.1:443 https ESTABLISHED
TCP 192.168.0.57:25083 46.67.108.75:https ESTABLISHED
TCP 192.168.0.57:25099 13.107.21.200:https ESTABLISHED
TCP 192.168.0.57:25101 13.107.21.200:https ESTABLISHED
TCP 192.168.0.57:25103 103.56.230.154:http ESTABLISHED
TCP 192.168.0.57:25106 ns32992:https SYN_SENT
TCP 192.168.0.57:25109 x11:https ESTABLISHED
C: \Users\Sumanth>
C: \Users\Sumanth>
C: \Users\Sumanth>
Windows Search 2:12 PM 5/13/2023 ENG IN
```



Exercise No 7:VULNERABILITY ANALYSIS - CGI Scanning with Nikto

Aim:To perform vulnerability Analysis using CGI Scanning with Nikto

Procedure:

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

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



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

+ Target IP:      103.103.196.97
+ Target Hostname: www.zoho.com
+ Target Port:    80
+ Start Time:    2022-09-14 13:32:08 (GMT-4)

+ Server: ZGS
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
+ Root page / redirects to: https://www.zoho.com/
```

Step 3: Nikto starts web server scanning with all tuning options enabled.

Step4:In the terminal window type “nikto –h <website>-Cgidirs all”and hit enter



```
(root㉿kali)-[~]
# nikto -h www.certifiedhacker.com -Cgidirs all
- Nikto v2.1.6

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

+ Server: nginx/1.19.10
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ Uncommon header 'host-header' found, with contents: c2hhcmVklmJsdWob3N0LmNvbQ=
+ 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 **Out Put:**

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

+ Target IP:          169.148.148.97
+ Target Hostname:    www.zoho.com
+ Target Port:        80
+ Start Time:        2023-05-14 20:46:15 (GMT5.5)
_____
+ 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/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Uncommon header 'zproxy' found, with contents: domain_not_configured
```

```
(root㉿kali)-[~]
# nikto -h www.certifiedhacker.com -Cgidirs all
- Nikto v2.1.6

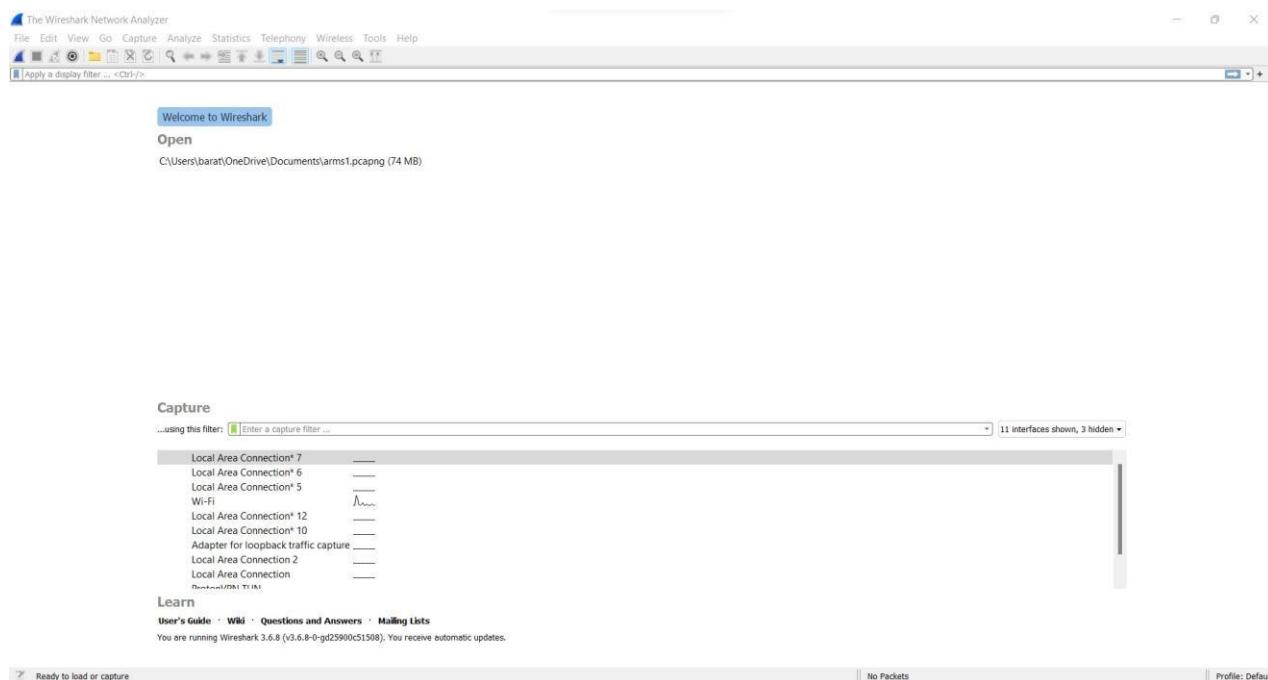
+ Target IP:          162.241.216.11
+ Target Hostname:    www.certifiedhacker.com
+ Target Port:        80
+ Start Time:        2023-05-14 20:55:18 (GMT5.5)
_____
+ Server: Apache
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header 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.certifiedhacker.com/
```

Exercise No 8: Wireshark sniffer

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

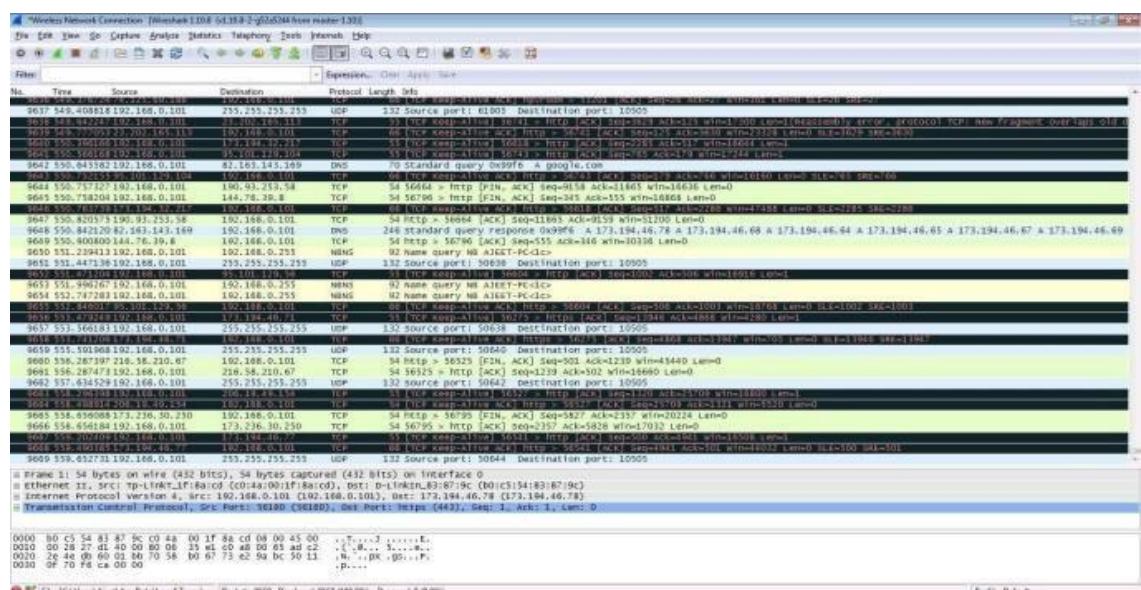
Procedure:

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

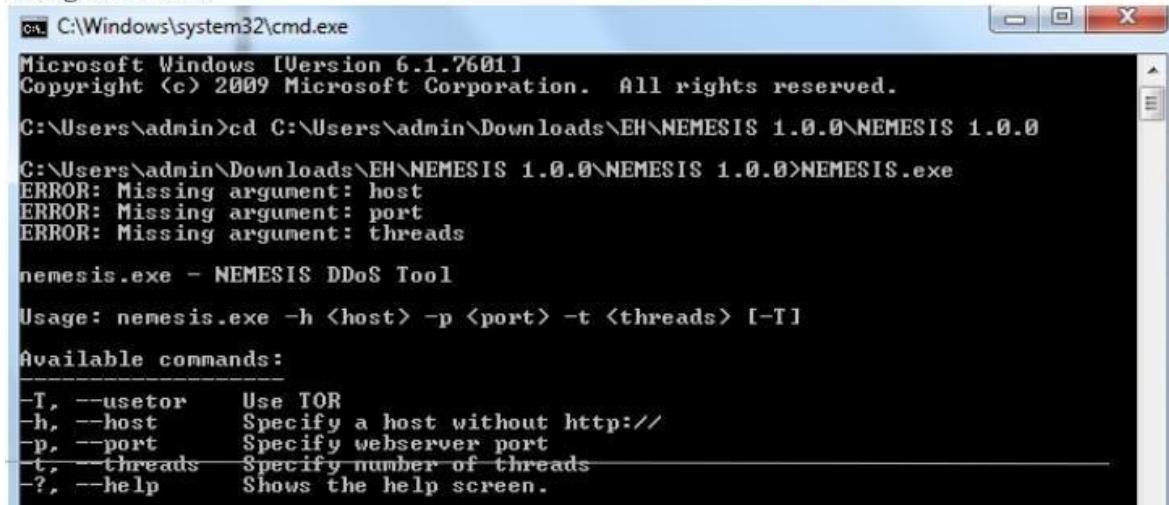
The screenshot shows the Wireshark interface with a list of captured packets. A specific packet is selected, showing its details and bytes panes. The packet details pane shows an HTTP POST request to 'http://arms.sse.saveetha.com'. The bytes pane displays the raw hex and ASCII data of the request, which includes form-encoded data for username ('admin') and password ('passcode'). To the right, a browser window shows a 'Sign In' page for 'SAVEETHA SCHOOL OF ENGINEERING'. The user has entered 'admin' in the username field and '*****' in the password field. An error message 'The username and password you entered is invalid' is displayed below the fields. The browser's address bar shows the URL 'http://arms.sse.saveetha.com'.

This screenshot is similar to the previous one but with some fields highlighted in blue. In the browser's sign-in form, the 'username' field ('admin') and the 'password' field ('passcode') are highlighted. This visual cue identifies the specific fields being transmitted in the captured network traffic. The rest of the interface, including the Wireshark window and the browser's status bar, remains the same.

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.

DOS Using NEMESIS



```
C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright <c> 2009 Microsoft Corporation. All rights reserved.

C:\Users\admin>cd C:\Users\admin\Downloads\EH\NEMESIS 1.0.0\NEMESIS 1.0.0
C:\Users\admin\Downloads\EH\NEMESIS 1.0.0\NEMESIS 1.0.0>NEMESIS.exe
ERROR: Missing argument: host
ERROR: Missing argument: port
ERROR: Missing argument: threads

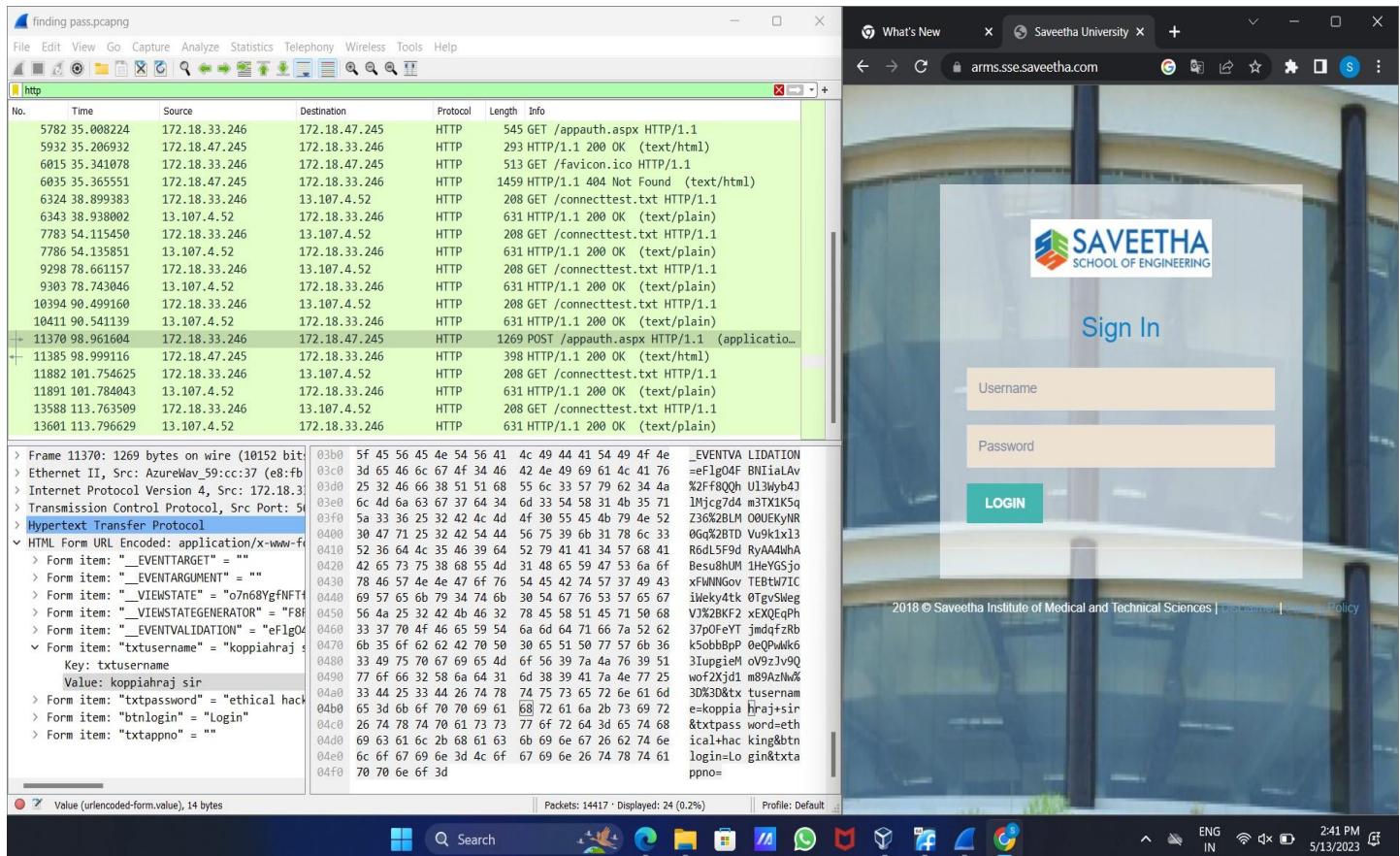
nemesis.exe - NEMESIS DDoS Tool

Usage: nemesis.exe -h <host> -p <port> -t <threads> [-T]

Available commands:

-T, --usetor      Use TOR
-h, --host        Specify a host without http://
-p, --port        Specify webserver port
-t, --threads     Specify number of threads
-?, --help         Shows the help screen.
```

Out Put:



The screenshot displays two windows. On the left, NetworkMiner is running with a list of captured network packets. The table shows columns for No., Time, Source, Destination, Protocol, Length, and Info. Several packets are highlighted in green, indicating they are related to the 'Sign In' process. On the right, a web browser window is open to the URL arms.sse.saveetha.com. The page features the Saveetha School of Engineering logo and a 'Sign In' form with fields for 'Username' and 'Password'. Below the form, a copyright notice reads: "2018 © Saveetha Institute of Medical and Technical Sciences | [Disclaimer](#) | [Privacy Policy](#)". The bottom of the screen shows the Windows taskbar with various pinned icons.

No.	Time	Source	Destination	Protocol	Length	Info
5782	35.0088224	172.18.33.246	172.18.47.245	HTTP	545	GET /appauth.aspx HTTP/1.1
5932	35.206932	172.18.47.245	172.18.33.246	HTTP	293	HTTP/1.1 200 OK (text/html)
6015	35.341078	172.18.33.246	172.18.47.245	HTTP	513	GET /favicon.ico HTTP/1.1
6035	35.365551	172.18.47.245	172.18.33.246	HTTP	1459	HTTP/1.1 404 Not Found (text/html)
6324	38.899383	172.18.33.246	13.107.4.52	HTTP	208	GET /connecttest.txt HTTP/1.1
6343	38.938002	172.18.33.246	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	98.961600	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	101.780443	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), 1269 bytes captured (10152 bits) on interface
> Frame 11370: 1269 bytes on wire (10152 bits), 1269 bytes captured (10152 bits) on interface
> Ethernet II, Src: AzureWav_59:cc:37 (e8:fb)
> Internet Protocol Version 4, Src: 172.18.33.246, Dst: 13.107.4.52
> Transmission Control Protocol, Src Port: 5444, Dst Port: 443
> Hypertext Transfer Protocol
HTTP Form URL Encoded: application/x-www-form-urlencoded
> Form item: "__EVENTTARGET" = ""
> Form item: "__VIEWSTATE" = "07n68YgfnFT4"
> Form item: "__EVENTARGUMENT" = "F8F"
> Form item: "__EVENTVALIDATION" = "eflg0Q"
> Form item: "txtusername" = "koppiahraj sir"
Key: txtusername
Value: koppiahraj sir
> Form item: "txtpassword" = "ethical hacker"
> Form item: "btnlogin" = "Login"
> Form item: "txtnappo" = ""

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 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)-[~]
```

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
```

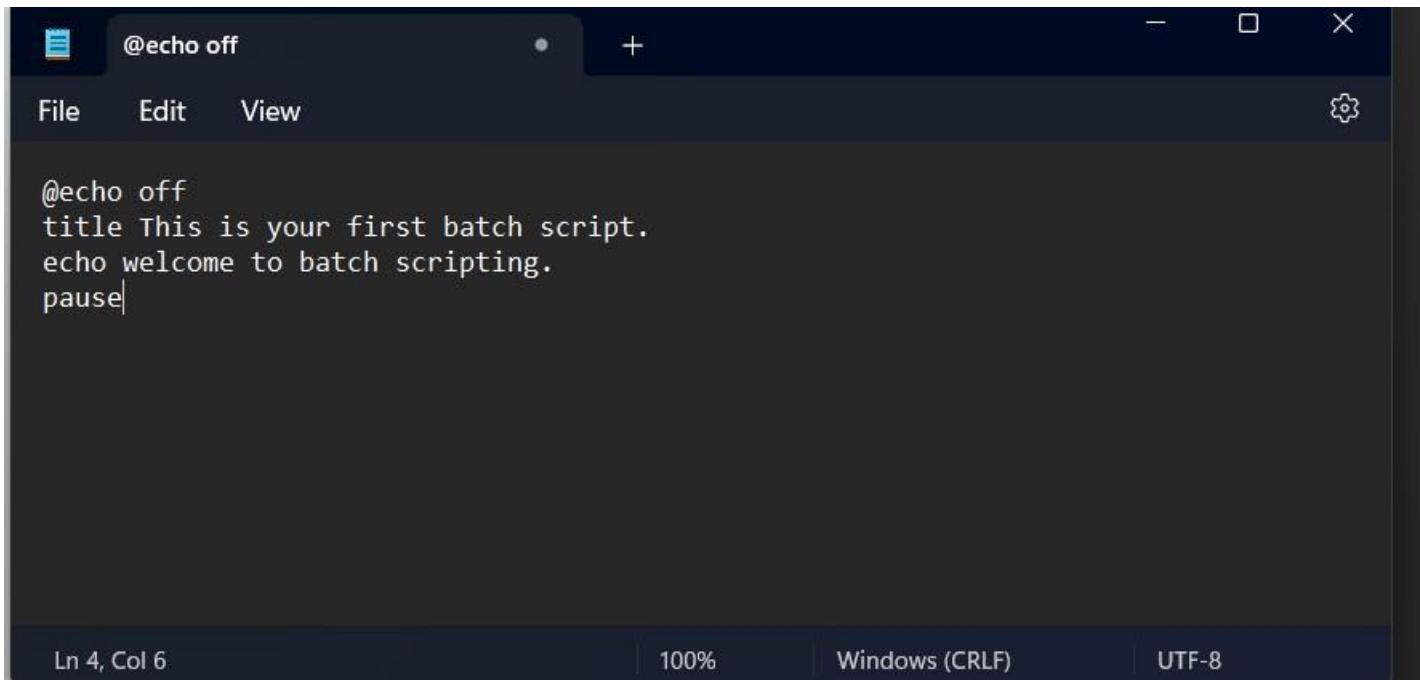
1. TO SAVE a BAT File

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.

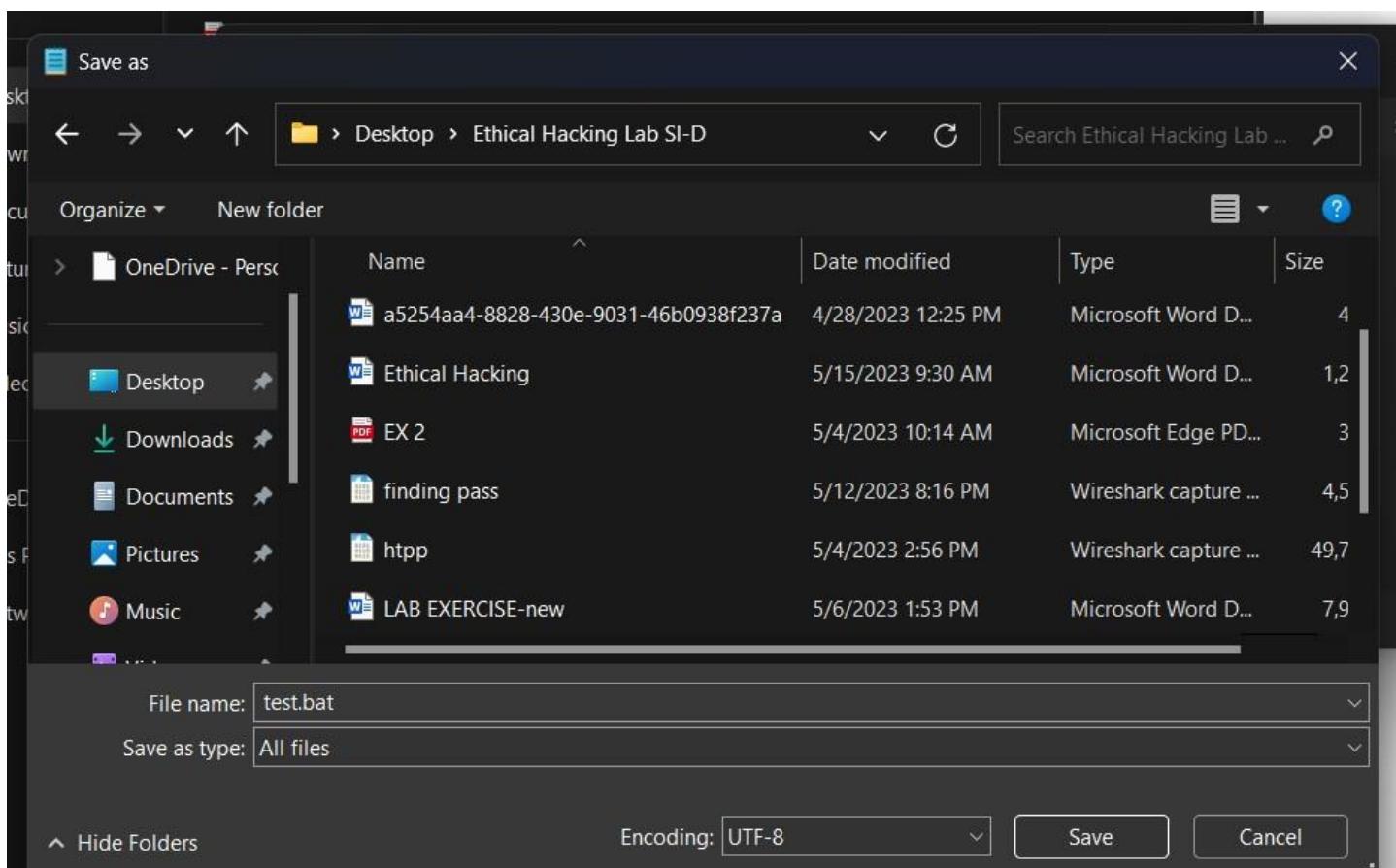
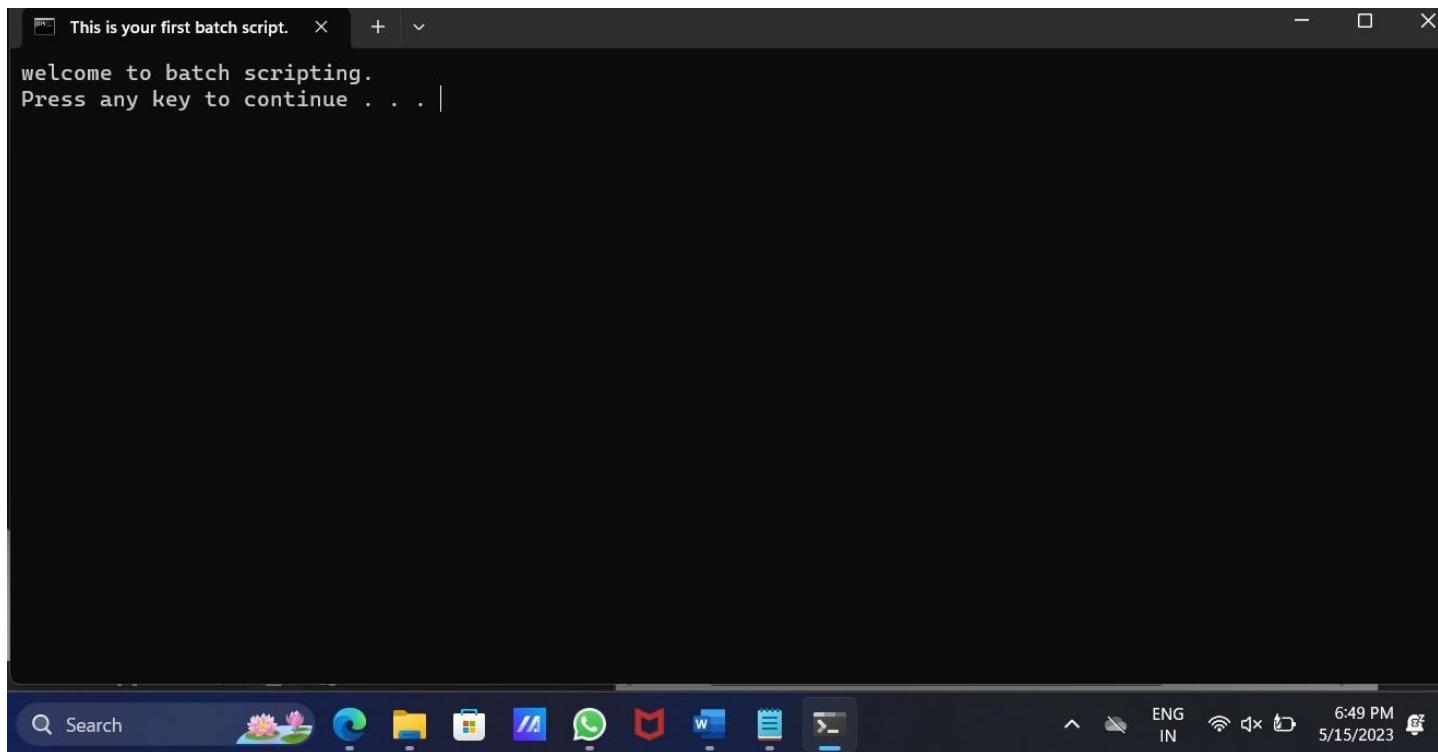
OUT PUT:



A screenshot of a code editor window displaying a batch script. The window has a dark theme with a top bar showing file icons and a title bar with a minimize, maximize, and close button. Below the title bar is a menu bar with 'File', 'Edit', and 'View' options. On the right side of the menu bar is a gear icon. The main area of the window contains the following text:

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

At the bottom of the window, there is a status bar with the following information: 'Ln 4, Col 6', '100%', 'Windows (CRLF)', and 'UTF-8'.



RESULT:

Thus the Creation and execution of BATCH FILE was successfully completed.