

ITA1471

ETHICAL HACKING FOR NETWORK HACKING



A. INDDASENA REDDY

192225086

1st YEAR, AI&ML DEPARTMENT

ITA1471-ETHICAL HACKING

LAB MANUAL

Exercise No 1: Nmap Scan

Aim:

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

Procedure:

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

Step 2: Perform different types of scans
(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

```
[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-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
```

STEP-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
```

```
[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
```

```
[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.

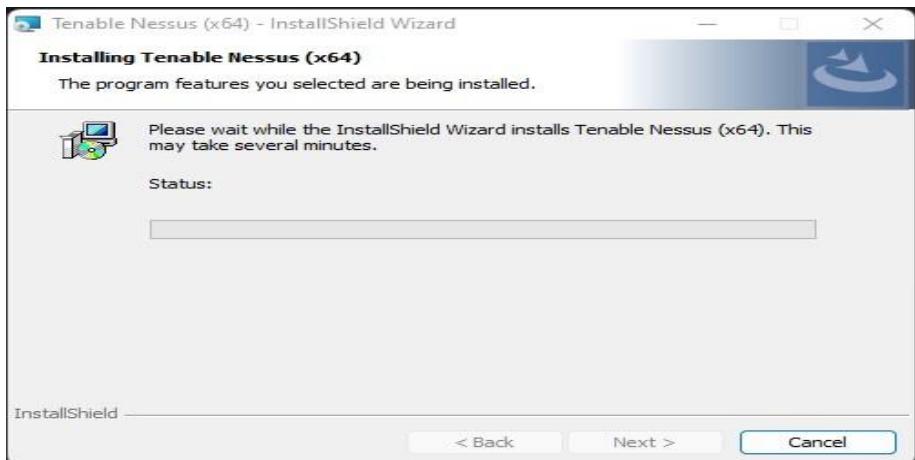
Exercise No 2: Vulnerability Access Scan Using Nessus

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 various links like Nessus, Nessus Agents, Nessus Network Monitor, etc. The main content area has a heading 'Nessus'. Below it, there are three numbered sections: 1. Download and Install Nessus, 2. Start and Setup Nessus, and 3. Getting Started. The first section contains a 'Choose Download' form with dropdowns for 'Version' (set to Nessus - 10.4.2) and 'Platform' (set to Windows - x86_64). It features a large blue 'Download' button with a circular arrow icon. To the right of this section is a 'Summary' box containing release information: 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).

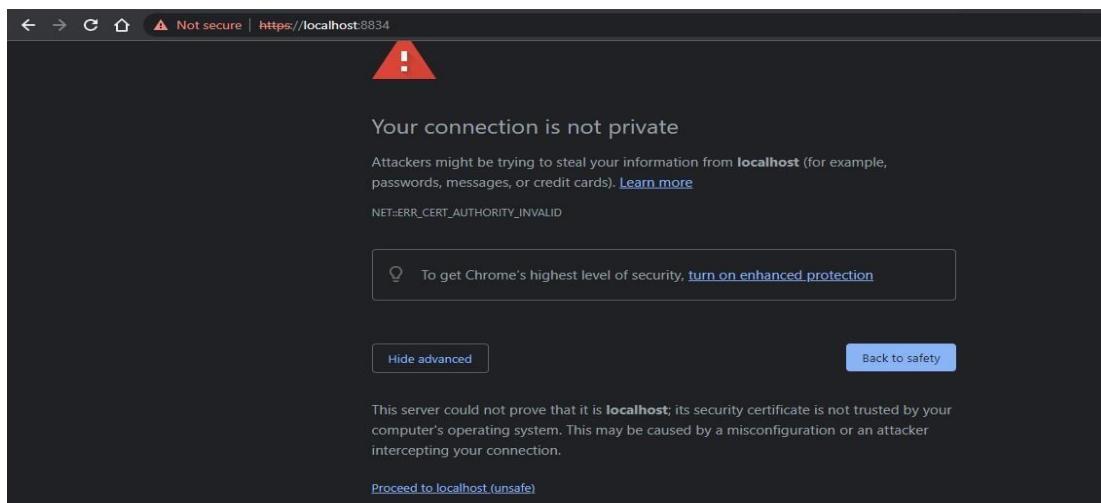
Step 2: Choose your OS and download, install



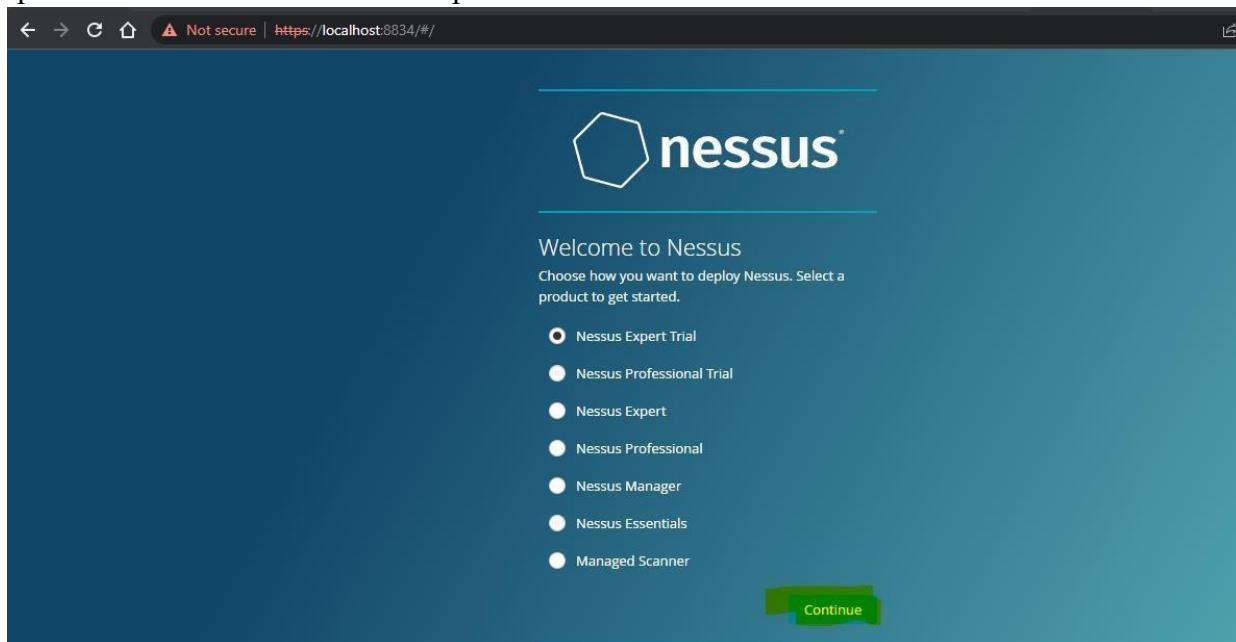
Step 3: Once installation is completed it will open in default browser



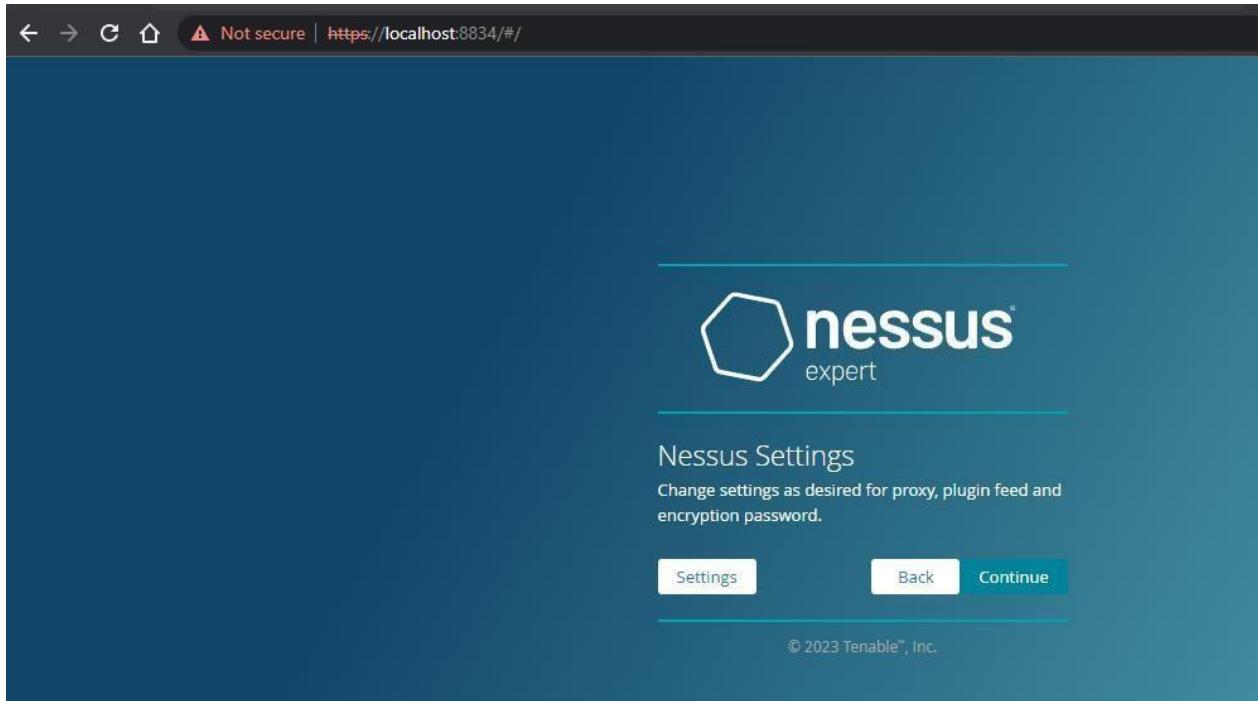
Step 5:- (click on the proceed to local host)



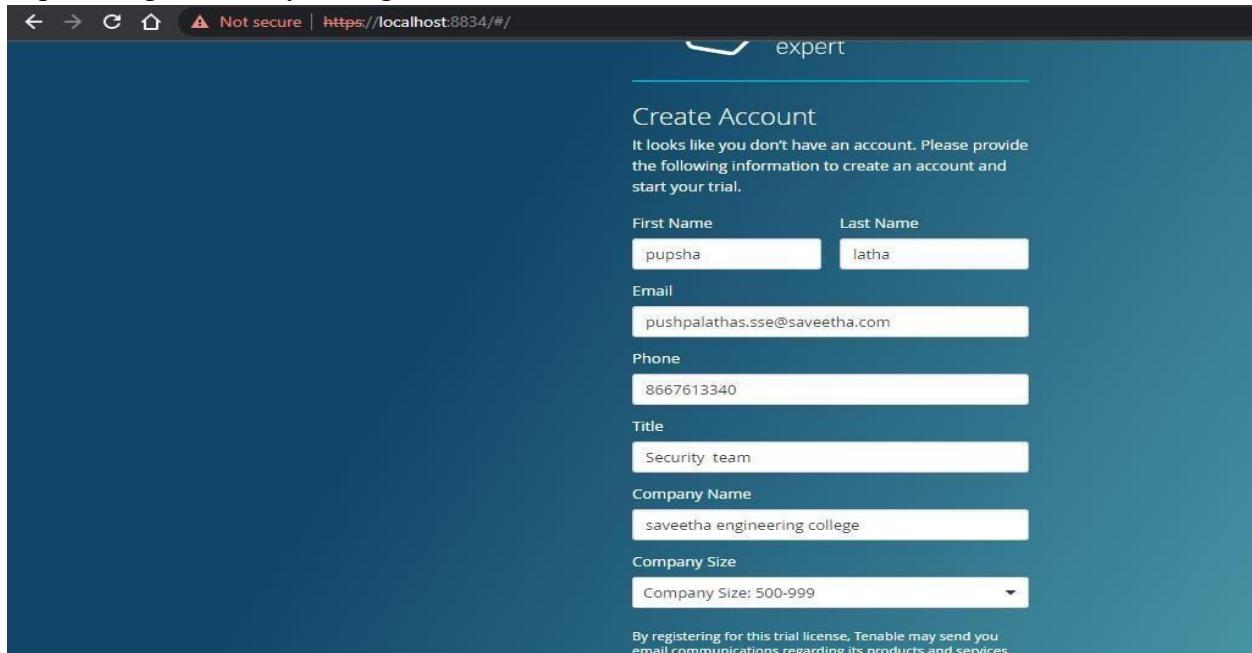
Step 6:- Please choose the Nessus Expert



Step 7: Click on continue



Step 8:- Register with your organizational email id



Step 9:- please note down the activation key

The screenshot shows a web browser window with the URL <https://localhost:8834/#/>. The page title is "Trial License Information". It displays an activation code "R4A2-DPDT-UVQZ-T53Y" and a valid until date "2023-01-28". A "Continue" button is visible at the bottom right.

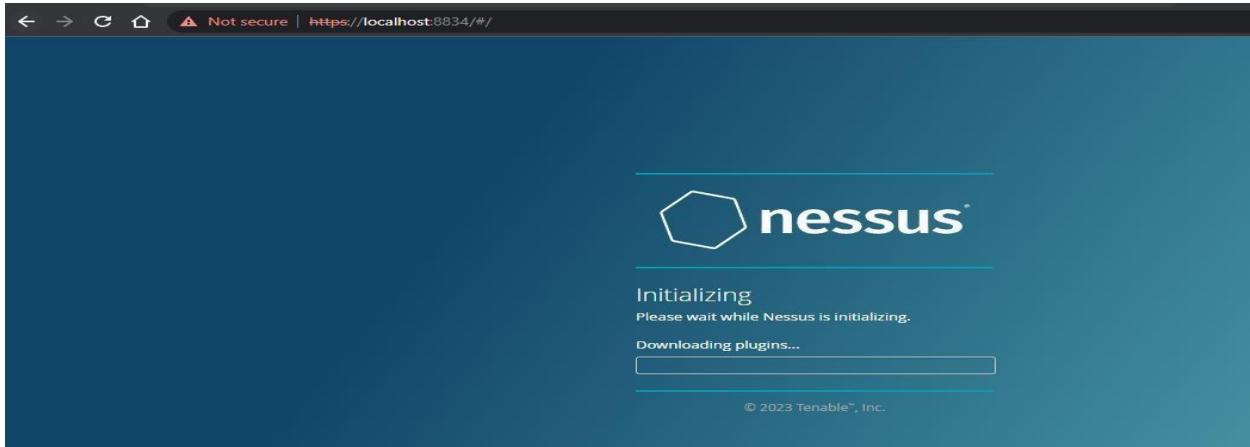
Step 10:- set up your username & password

The screenshot shows a web browser window with the URL <https://localhost:8834/#/>. The page title is "Create a user account". It instructs the user to "Create a Nessus administrator user account. Use this username and password to log in to Nessus." There are fields for "Username *" and "Password *". Below the fields are "Back" and "Submit" buttons. A copyright notice "© 2023 Tenable™, Inc." is at the bottom.

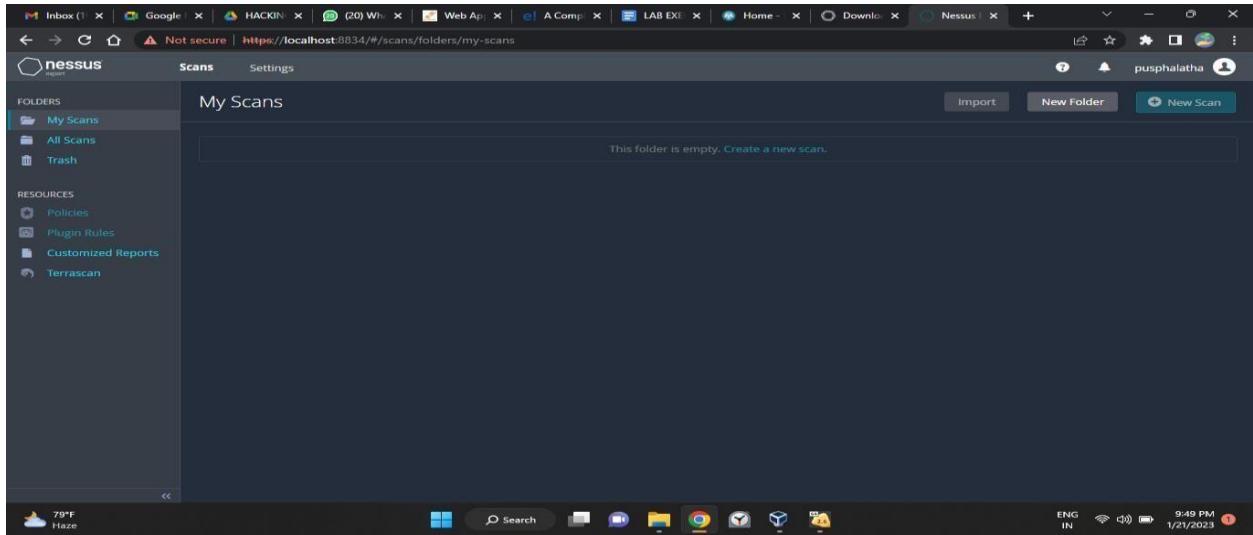
Step 11:-Type username and password

The screenshot shows a web browser window with the URL <https://localhost:8834/#/>. The page title is "Create a user account". It features the Nessus logo and the text "Create a Nessus administrator user account. Use this username and password to log in to Nessus." Below this are two input fields: "Username *" containing "pusphalatha" and "Password *" containing "Test@1234". At the bottom are "Back" and "Submit" buttons, and a copyright notice "© 2023 Tenable®, Inc."

Step 12:- Please wait until download is completed



Step 13: Select My Scans

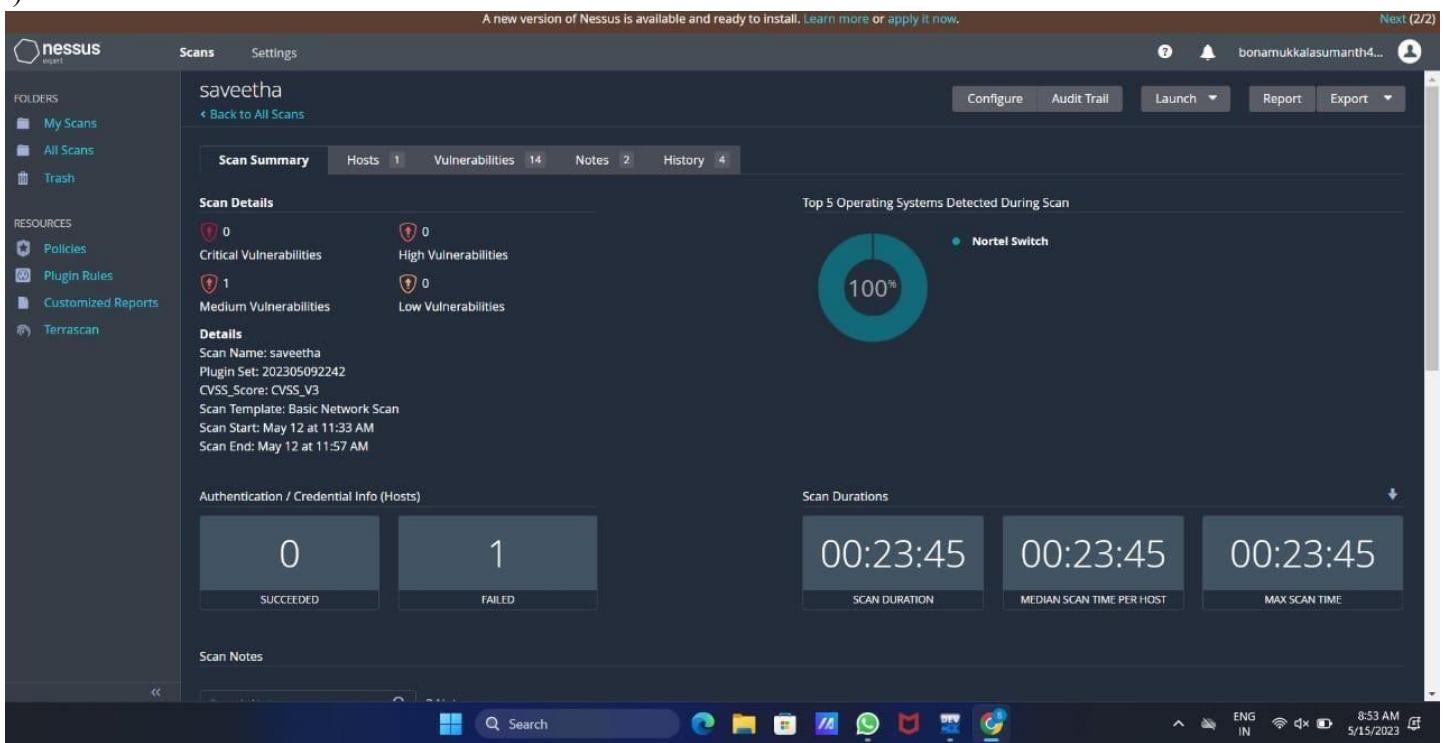


Output:

1)

A screenshot of the Nessus web interface showing policy details. The sidebar on the left includes 'FOLDERS' (My Scans, All Scans, Trash) and 'RESOURCES' (Policies, Plugin Rules, Customized Reports, Terrascan). The main content area displays 'Policy Details' with sections for 'Basic Overview' (Scan Policy: Basic Network Scan, Plugins Timeout: 320, Feed Type: ProFeed), 'Report Overview' (Disable DNS Resolution: No, Display Superseded Patches: Yes), 'Credential Settings Overview' (Preferred SSH Port: 22, SSH Client Version: OpenSSH_5.0), '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), 'Port Scanner Overview' (SYN: Yes, UDP: No, TCP: No, Port Scan Range: default), and 'Fragile Devices' (Scan Network Printers: No, Scan Novell Netware Hosts: No, Scan OT Devices: Yes). The bottom status bar shows system information.

2)



Result:

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

Exercise No 3: Information gathering using theHarvester

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

STEP 1: Open Terminal in the kali linux

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

-l will limit the search for specified number.

-b is used to specify search engine name.

STEP 2: Run the following command

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

The screenshot shows a terminal window on a Kali Linux desktop environment. The terminal title is '(root㉿kali)-[~]'. The command entered is 'theHarvester -d www.zoho.com -l 300 -b all'. The output of the command is displayed below the command line. It starts with the theHarvester logo and version information: 'theHarvester 4.0.3', 'Coded by Christian Martorella', 'Edge-Security Research', and 'source@edge-security.com'. The output then lists various search engines and their API keys: Fullhunt, Spyse, binaryedge, PentestTools, Securitytrail, ProjectDiscovery, Hunter, zoomeye, Consys ID, Intelx, RocketReach, GitHub, Utscan, Raidoo, and Omission. For each, it says 'Missing API key'. The search results for 'www.zoho.com' are then shown: 'Searching 0 results.' followed by 'Searching 100 results.' and 'Searching Omission.' The terminal window has a dark background with light-colored text. The desktop environment includes a taskbar with icons for various applications like a browser, file manager, and terminal, along with system status icons at the bottom.

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

[*] Target: www.zoho.com

[!] Missing API key for Fullhunt.
[!] Missing API key for Spyse.
[!] Missing API key for binaryedge.
[!] Missing API key for PentestTools.
[!] Missing API key for Securitytrail.
[!] Missing API key for ProjectDiscovery.
[!] Missing API key for Hunter.
[!] Missing API key for zoomeye.
[!] Missing API key for Consys ID and/or Secret.
[!] Missing API key for Intelx.
[!] Missing API key for RocketReach.

[!] Missing API key for GitHub.
[*] Searching Utscan...
[*] Searching Raidoo...
[*] Searching Omission...
    Searching 0 results.
[*] Searching 100 results.
[*] Searching Omission...
```



```
kali-linux-2022.3-vmware-amd64 - VMware Workstation 16 Player (Non-commercial use only)
Player | ||| | 1 2 3 4 | 
File Actions Edit View Help
AS63949
[*] Interesting URLs Found: 25
https://www.zoho.com/
https://www.zoho.com/assit/
https://www.zoho.com/books/
https://www.zoho.com/campaigns/?src=fromproduct
https://www.zoho.com/campaigns/explain/explain/view.html
https://www.zoho.com/campaigns/explain/explain/send.html
https://www.zoho.com/cliq/?serviceurl=%2Fchats%2F2431772755001510080zsrc=fromproduct
https://www.zoho.com/cliq/?serviceurl=%2Findex.dobzsrc=fromproduct
https://www.zoho.com/contactus.html
https://www.zoho.com/creator/
https://www.zoho.com/crm/
https://www.zoho.com/crm/rmplus/
https://www.zoho.com/crm/v/
https://www.zoho.com/emailsender/
https://www.zoho.com/forms/
https://www.zoho.com/invoice/?utm_source=200utm_medium-pdf
https://www.zoho.com/mail/
https://www.zoho.com/marketingautomation/
https://www.zoho.com/nl/salesiq/
https://www.zoho.com/rmplus/?src=zoho-home&amp%3Bref=ohome
https://www.zoho.com/report/dash/
https://www.zoho.com/report/abuse/
https://www.zoho.com/salesiq/
https://www.zoho.com/survey/
[*] No Twitter users found.

[*] LinkedIn Users Found: 292
Aamill Mohamed - Regional Account Manager
Abbas Abu - Zoho Developer
Abhilash Reddy Godishala
Adarsh Pandey - Member of Technical Staff
Adithyan Ravindraraj - Lead Product Engineer
Ajay Singh - Partner Software Engineer - Zoho
Ajay Singh - Developer - ZOHO CRM
Akash Krishnan - Member Technical Staff
Akash Krishnamoorthy - Zoho Corporation
Akshaya Chidrasekhar - Zoho Corporation
Ali Shabd - Regional Director MEA
Alok Kumar Bharti - Software Engineer
Aman Gupta - Zoho Developers
Amaravathi KR - Zoho Developer
Ambi Moorthy - Product Manager and Co-Founder
Anandaraman Krishnan - Product Manager

34°C Cloudy
ENG IN 13:46 14-09-2022
```

```
kali-linux-2022.3-vmware-amd64 - VMware Workstation 16 Player (Non-commercial use only)
Player | ||| | 1 2 3 4 | 
File Actions Edit View Help
Ajay Singh - Developer - ZOHO CRM
Akash Krishnan - Member Technical Staff
Akila Umamirtham
Akshaya Chidrasekhar - Zoho Corporation
Ali Shabd - Regional Director MEA
Alok Kumar Bharti - Software Engineer
Aman Gupta - Zoho Developers
Amaravathi KR - Zoho Developer
Ambi Moorthy - Product Manager and Co-Founder
Anandaraman Krishnan - Product Manager
Ananthu Nair - Presales Engineer - Zoho Corporation
Andrea Mahoney - VP - Certified Computer Solutions
Andrew Bourne
Andrews B A - Zoho Corporation
Andrews B A - Senior Member Of Technical Staff
Anubhav Pandey - Zoho Consultant
Anumita Gupta - Technical Writer
Anusha Nagarajan - Zoho Corporation
Arun Balachandra - Senior Product Marketing Manager
Arun Kesavan - Product Designer
Arun Venkateswaran - Product Marketeer
Aryild Krishnamoorthy
Ashok Chakravarthi Nagarajan
Ashok Kumar
Ashwin Rama - Lead - Zoho CRM SME
Avanadithi B - Software Developer - Zoho
Azareedeen M
Balaji Barayam - Senior Technical Support Engineer
Bala Krishnan - Product Marketeer
Bala Sundar - Member Technical Staff
Bala Venkateswaran
BalaVijayaraman - Product Manager
Barath Kumar Raresh - Member Leadership Staff
Basitruul Haque Faisal - Zoho Consultant
Baskaran Sivivel - Zoho Developer
Bharath Kumar
Bharathi Ambazhagan - Member Technical Staff
Calvin Gopalan - Quality Analyst- Zoho CRM Support
Carla Garcia
Chakravarthi Radhakrishnan - Zoho Corporation
Chandru Jayapalan - Zoho Corporation
Chaitanya - Zoho
Chetan K. - Zoho CRM Consultant - Regal Infonet
Chitrapsundari Nachagpan - Senior Product Director
Clarence Rozario - Director of Product Management
Cynthia - Project Management
D Javaraj - Visual Designer
DEVENORA KUSHWHAH - Zoho Developer
David Elkins - Head of Content Review
Deepak RV - Enterprise Support Engineer - Zoho

34°C Cloudy
ENG IN 13:46 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
Vijayaraghavan venugopal
Vinodraju Thiyyarajan
Vinothkumar R - Product Manager - Zoho Corporation
Vipasha Sinha - Senior Product Marketer
Vishnukumar Murthy - Member Technical staff
Vivekanandan M
Yogendrababu venkatapathy - Co-Founder
Yogesh Manoharan - Regional Director
Zoho One Developer - A2Z SaaS Private Limited
Zoho Account - Developer
Zoho Developer
Zoho Expert Services - GENOWIRE
balaji - Developer - Zoho Corporation
omprakash s - Ios Developer
rangarajan ramesh - Account Manager - Zoho
sathiyam sathiyamarsa - zoho - Zoho Corporation
sasi k Afreen - Senior Technical Support Engineer
vasudevannew 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 Krishnamoorthy - Member 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 Balaji - Product Manager and Co-Founder
Anandaraman Krishnan - Project Manager
Anantha Subramanian - Engineer Trainee
Ananthu Nair - Presales Engineer - Zoho Corporation
Andrea Mahoney - VP - Certified Computer Solutions
Anil Kulkarni
Andrew Joseph - Zoho Corporation
Andrews B A - Senior Member Of Technical Staff
Anubha Patel - Zoho Corporation
anshulika gopta - Technical Writer
Aravind Nataraajan - Zoho Corporation
Arun Balachandran - Senior Product Marketing Manager
Arun Kesavamurthy - Product Designer
Arun Selvadharan - 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 | ||| | 1 2 3 4 | root@kali:~ |
File Actions Edit View Help
Vinothkumar R - Product Manager - Zoho Corporation
Vipasha Sinha - Senior Product Marketer
Vishnukumar Murthy - Member Technical staff
Vivekanandan M
Yogendrababu venkatapathy - Co-Founder
Yogesh Manoharan - Regional Director
Zoho One Developer - A2Z SaaS Private Limited
Zoho Account - Developer
Zoho Developer
Zoho Expert Services - GENOWIRE
balaji - Developer - Zoho Corporation
omprakash s - Ios Developer
rangarajan ramesh - Account Manager - Zoho
sathiyam sathiyamarsa - zoho - Zoho Corporation
sasi k Afreen - Senior Technical Support Engineer
vasudevannew T - Lead
working as a Senior executive at IndiGo Airlines
[*] Trello URLs found: 33
http://www.trello.com/contact
https://trello.com/
https://trello.com/integrations
https://trello.com/integrations/sales-support
https://trello.com/power-ups
https://trello.com/power-ups/595e9ffaf8f137d12f456fd8
https://trello.com/power-ups/5b0c1aa1922a254295b08a35/zoho-crm
https://trello.com/power-ups/5b5d5d5794cc75f290fd4d73/automateio
https://trello.com/power-ups/5b0c1aa1922a254295b08a35/zoho-crm
https://trello.com/power-ups/5b5d5d5794cc75f290fd4d73/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-yzn5vf0n
https://trello.com/templates/design/freelance-branding-project-zsm6dhs
https://trello.com/templates/design/research-iteration-8t9qgmz
https://trello.com/templates/design/ux-design-process-smcwwtg
https://trello.com/templates/product-management/5-etapes-de-gestionnement-de-produits-ts8avmuv
https://trello.com/templates/product-management/5-listes-pour-la-gestion-de-produits-0lfufgyd7
https://trello.com/templates/product-management/5-listes-pour-la-gestion-de-produits-0lfufgyd7
https://trello.com/templates/product-management/construction-d-un-plan-de-fonctionnement-mop-shyq7jg
https://trello.com/templates/product-management/fabrication-process-davkjps5
https://trello.com/templates/product-management/product-roadmap-template-fbajssh
https://trello.com/templates/product-management/project-planning-template-jiblr
https://trello.com/templates/product-management/readmap-product-jpd120m
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)
Player | ||| 1 2 3 4
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
74.201.113.101
74.201.112.118
74.201.113.118
74.201.113.178
74.201.113.203
74.201.155.201
89.36.170.52
103.138.128.96
103.138.129.70
104.16.11.213
104.16.12.213
104.16.13.213
104.16.14.213
104.16.15.213
104.16.43.59
104.16.44.50
104.16.45.54
104.163.182.155
136.143.198.58
136.143.198.79
136.143.198.155
136.143.198.156
136.143.191.284
165.173.187.32
165.254.168.165
165.254.168.165
178.79.172.105
185.28.289.52
204.141.42.155
204.141.42.156
204.141.43.204
204.141.43.205
2a06:98c1:3129::c
2a06:98c1:3121::3
[*] No emails found.
[*] No hosts found.

(rmert@kali)-[~]
Cloudy 34°C 13:47 14-09-2022 ENG IN
```

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.scpi@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.

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:

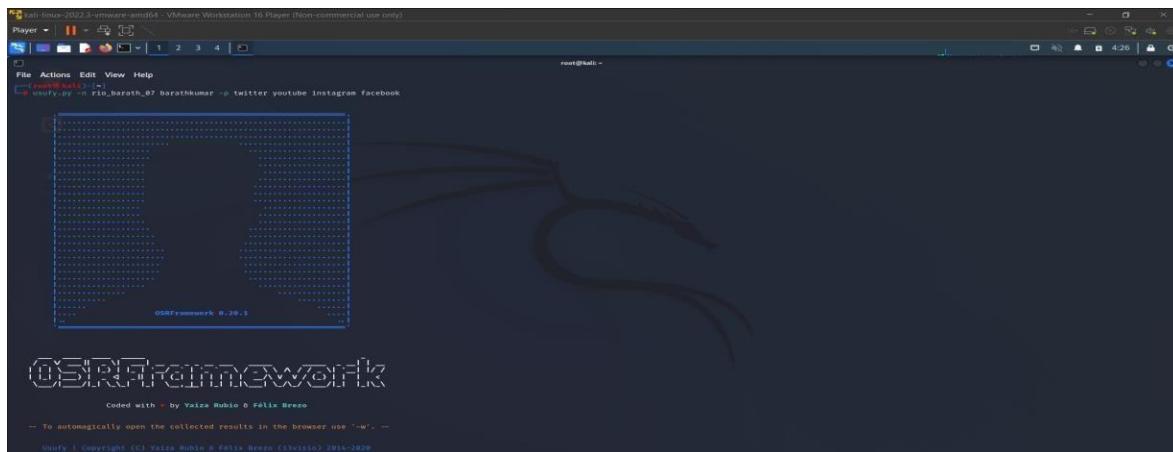
Step 1: Log into kali linux machine

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 twitterfacebook youtube
```



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

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

```

root@Livevisio:~# searchfy.py -q "LIVEWIRE"
2022-09-14 04:25:41.218299  Starting search in 4 platform(s) ... Relax!
Press Ctrl+C to stop ...
2022-09-14 04:25:41.218299  Results obtained (8):
/usr/lib/python3/dist-packages/xlsxwriter/deprecated.py:200: UserWarning: Deprecated usage since v0.2.1! Explicit import is no longer required. pyexcel.ext.text is auto imported.
  warnings.warn("Deprecated usage since v0.2.1! Explicit import is no longer required. pyexcel.ext.text is auto imported.", stacklevel=2)
Objects recovered (2022-09-14_042541.218299):
+-----+-----+-----+
| com.i3visio.URI | com.i3visio.Alias | com.i3visio.Platform |
+-----+-----+-----+
| https://www.youtube.com/user/rio_barath_07/about | rio_barath_07 | YouTube |
| https://www.facebook.com/rio_barath_07 | rio_barath_07 | Facebook |
| https://www.instagram.com/rio_barath_07 | rio_barath_07 | Instagram |
| http://twitter.com/rio_barath_07 | rio_barath_07 | Twitter |
| https://www.youtube.com/user/barathkumar/about | barathkumar | YouTube |
| https://www.facebook.com/barathkumar | barathkumar | Facebook |
| https://www.instagram.com/barathkumar | barathkumar | Instagram |
| http://twitter.com/barathkumar | barathkumar | Twitter |
+-----+-----+-----+
2022-09-14 04:25:41.390991  You can find all the information here:
2022-09-14 04:25:41.397468  Finishing execution...
Total time consumed: 0:00:06.189075
Average seconds/query: 1.14626875 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/srframework/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@Livevisio:~# searchfy.py -q "LIVEWIRE"
```

FIGURE. 9

Step 6: It will put out all the details who are subscribed to target social networking pages that are provided.

| Sheet Name: Profiles recovered (2018-6-27_15h17m). | | |
|--|---------------|------------------|
| i3visio.uri | i3visio.alias | i3visio.platform |
| http://twitter.com/us | us | Twitter |
| https://www.facebook.com/cehuser | cehuser | Facebook |
| http://twitter.com/cehuser | cehuser | Twitter |
| https://www.facebook.com/us | us | Facebook |

FIGURE. 10

Collect and note the information disclosed about the target

Output:

1)

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

File Actions Edit View Help
```

The screenshot shows the OSRFramework interface running in a terminal window. The title bar includes 'File', 'Actions', 'Edit', 'View', and 'Help'. The main area displays a search results window with a grid of user profiles. Each profile card contains a small thumbnail image, a name, and some descriptive text. A vertical sidebar on the left lists various search parameters and options. At the bottom of the interface, the text 'OSRFramework 0.20.1' is visible.

```
Target IP: 192.168.1.127
Target Port: 80
Target Threads: 10
Start Time: 2023-07-10 14:52:10 (UTC+0)
End Time: 2023-07-10 14:56:10 (UTC+0)
Time Elapsed: 00:04:00
OSRFramework 0.20.1
```

OSRFramework

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

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

2)

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

2023-05-14 20:19:31.116670      Starting search in 4 platform(s) ... Relax!
Press <Ctrl + C> to stop ...

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

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

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

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

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

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

Result:

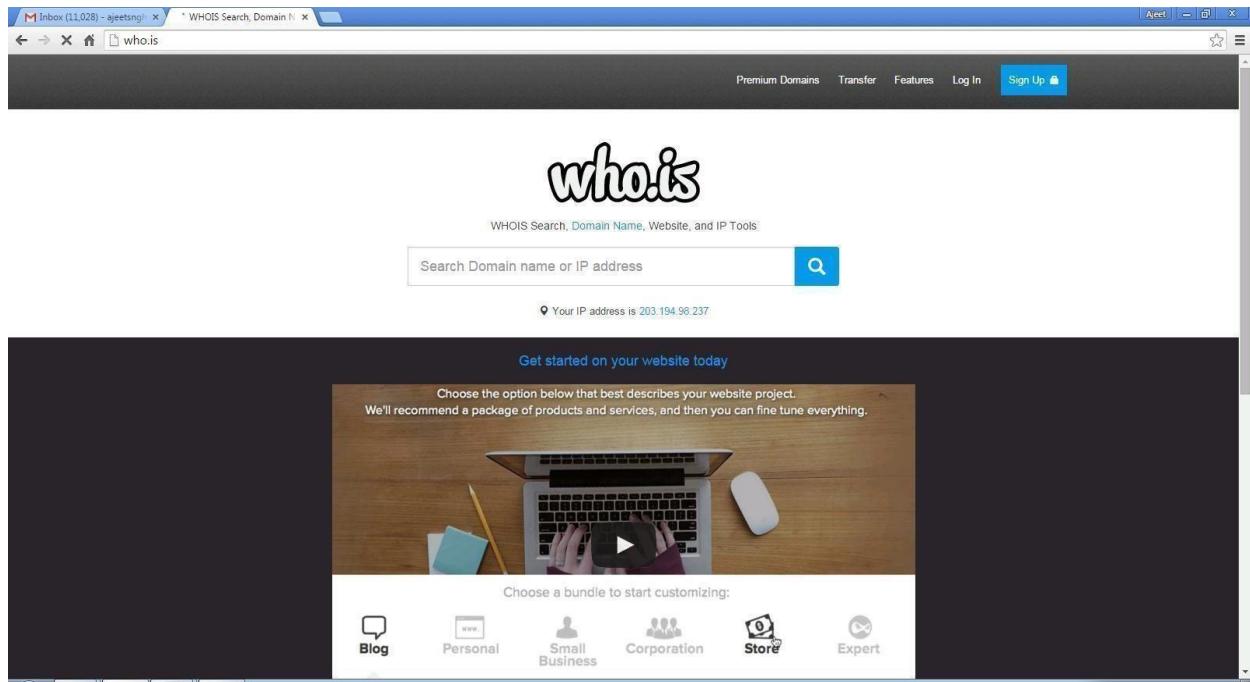
The current experiment is about Open-Source Intelligence Gathering is done using OSR Framework. This experiment is done to check for the Existence of a Profile for given user details in different platforms. This experiment is executed in root terminal using kali linux operating system.

Exercise NO 5: Use Google and Whois for Reconnaissance.

Aim: To find out the Whois, DNS Records and 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 interface includes a navigation bar with links for Premium Domains, Transfer, Features, Log in, and Sign Up. The main content area displays the following information:

- Registrar Info:**
 - Name: PDR Ltd. db/a PublicDomainRegistry.com
 - Whois Server: whois.publicdomainregistry.com
 - Referral URL: www.publicdomainregistry.com
 - Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
- Important Dates:**
 - Expires On: 2023-06-18
 - Registered On: 2001-06-18
 - Updated On: 2022-05-27
- Name Servers:**

| | |
|------------------------|---------------|
| ns51.domaincontrol.com | 97.74.105.26 |
| ns52.domaincontrol.com | 173.201.73.26 |
- Similar Domains:** A list of domains including `save-beard.gen.in`, `savee-energy.com`, `savee.biz`, `savee.cloud`, `savee.co`, `savee.co.jp`, `savee.co.uk`, `savee.com`, `savee.com.au`, `savee.com.br`, `savee.com.cn`, `savee.de`, `savee.dk`, `savee.earth`, `savee.energy`, `savee.eu`, `savee.host`, `savee.info`, `savee.it`, and `savee.lt`.
- Registrar Data:**
 - We will display stored WHOIS data for up to 30 days.
 - Refresh button.
 - Make Private Now button.
- Site Status:**

| |
|--------------------------|
| Status: Active |
| Server Type: Squarespace |
- Suggested Domains for `saveetha.com`:**
 - `save-etha.live` \$2.99
 - `saveethas.live` \$2.99
 - `freeetha.live` \$2.99
 - `rescueetha.live` \$2.99
 - `guardetha.live` \$2.99
- Purchase Selected Domains** button.

Output:

The screenshot shows a web browser window with the title "WHOIS search results". The URL in the address bar is "in.godaddy.com/whois/results.aspx?domain=www.saveetha.com". The main content area displays the "WHOIS search results" for the domain "SAVEETHA.COM". The results include the following information:

- Domain Name: SAVEETHA.COM
- Registry Domain ID: 72789528_DOMAIN_COM-VRSN
- Registrar WHOIS Server: whois.PublicDomainRegistry.com
- Registrar URL: http://www.publicdomainregistry.com
- Updated Date: 2022-05-27T12:35:41Z
- Creation Date: 2001-06-18T13:41:02Z
- Registry Expiry Date: 2023-06-18T13:41:02Z
- Registrar: PDR Ltd. d/b/a PublicDomainRegistry.com
- Registrar IANA ID: 303
- Registrar Abuse Contact Email: abuse-contact@publicdomainregistry.com
- 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/

Below the results, there is a notice about the expiration date and a link to the ICANN Whois Inaccuracy Complaint Form. To the right of the main content, there is a sidebar titled "Find your Domain" with a search bar and a button.

Result:

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

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

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

Procedure:

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

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

C:\Users\barat>tracert saveetha.com

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

 1  11 ms    4 ms    4 ms  172.18.64.1
 2  9 ms     2 ms    9 ms  172.22.3.1
 3  9 ms     17 ms   8 ms  172.22.7.2
 4  12 ms    9 ms   10 ms  ptp1-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

```

nuse1:-# 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 | 52.238.84.217: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)

```
A Command Prompt x + 
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.
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 WhatsApp Ethical Hacking Lab psiphon3 qBittorrent

inet0      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:0 errors:0 dropped:0 overrun:0 frame:0
          TX packets:0 errors:0 dropped:0 overrun:0 carrier:0
          R bytes:0 T bytes:0 (0.0 bps) TX bytes:0 (0.0 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:0 errors:0 dropped:0 overrun:0 frame:0
          TX packets:0 errors:0 dropped:0 overrun:0 carrier:0
          R bytes:0 T bytes:0 (0.0 bps) TX bytes:0 (0.0 Kb)

2:09 PM 5/13/2023
```

2)

```
A Command Prompt x + 
C:\Users\Sumanth>ifconig
'ifconig' 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 . :

inet0      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:0 errors:0 dropped:0 overrun:0 frame:0
          TX packets:0 errors:0 dropped:0 overrun:0 carrier:0
          R bytes:0 T bytes:0 (0.0 bps) TX bytes:0 (0.0 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:0 errors:0 dropped:0 overrun:0 frame:0
          TX packets:0 errors:0 dropped:0 overrun:0 carrier:0
          R bytes:0 T bytes:0 (0.0 bps) TX bytes:0 (0.0 Kb)

2:12 PM 5/13/2023
```

3)

The screenshot shows a Microsoft Windows desktop environment. In the center, a Command Prompt window is open with the following text:

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

C:\Users\Sumanth>netstat

Active Connections

Rec 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 maa85s22-in-x03:https TIME_WAIT
TCP   [2402:3a80:183a:fbfd:9123:b861]:7762:[b4c2]:52600 [2620:1ec:42::132]:https ESTABLISHED
TCP   [2402:3a80:183a:fbfd:9123:b861]:7762:[b4c2]:52604 [2606:2800:247:61d9:f511:45d:27a9:730f]:https TIME_WAIT
TCP   [2402:3a80:183a:fbfd:9123:b861]:7762:[b4c2]:52605 [64:ff9b::34a8:7042]:https ESTABLISHED
TCP   [2402:3a80:183a:fbfd:9123:b861]:7762:[b4c2]:52606 [64:ff9b::34a8:7042]:https ESTABLISHED
TCP   [2402:3a80:183a:fbfd:9123:b861]:7762:[b4c2]:63288 [64:ff9b::14c6:778f]:https ESTABLISHED
```

The desktop taskbar at the bottom shows icons for Audacity, VLC media player, old WhatsApp, Ethical Hacking Lab, psiphon3, and qBittorrent. The system tray indicates the date and time as 5/13/2023, 2:12 PM, with ENG IN language settings.

Result:

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

Exercise No 7: VULNERABILITY ANALYSIS - CGI Scanning with Nikto

Aim:To perform vulnerability Analysis using CGI Scanning with Nikto

Procedure:

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

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



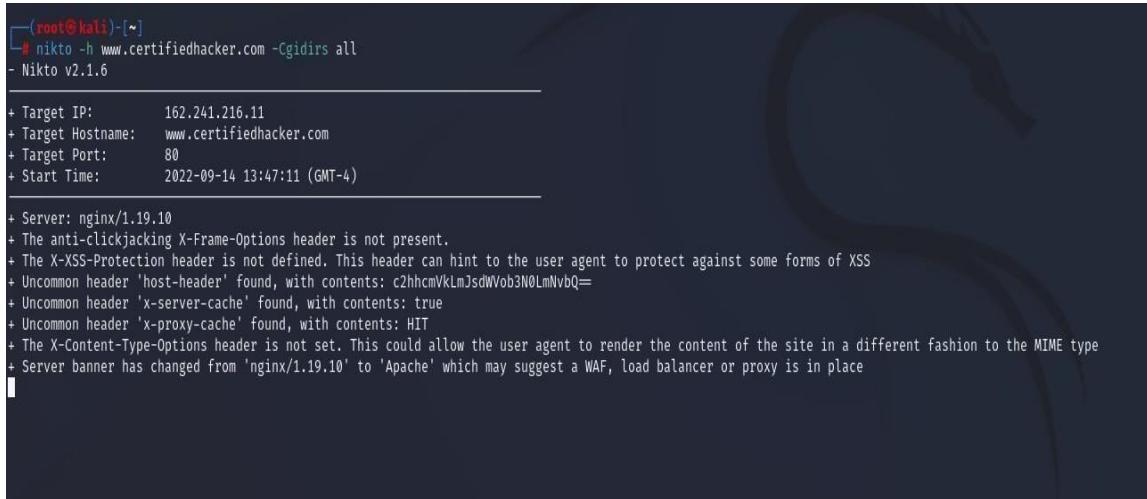
```
(root@kali)-[~]
# nikto -h www.zoho.com -Tuning x
- Nikto v2.1.6

+ 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: c2hhcmVlMjsdWob3N0LmNvbQ=
+ Uncommon header 'x-server-cache' found, with contents: true
+ Uncommon header 'x-proxy-cache' found, with contents: HIT
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
+ Server banner has changed from 'nginx/1.19.10' to 'Apache' which may suggest a WAF, load balancer or proxy is in place
```

Step 5. Nikto will scan the webserver as it looks vulnerable CGI directories. It scans the webserver and list out the directories

Output:

1)

```
root@kali: ~
File Edit View Search Terminal Tabs Help
root@kali: ~          root@kali: ~          root@kali: ~
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:~#
```

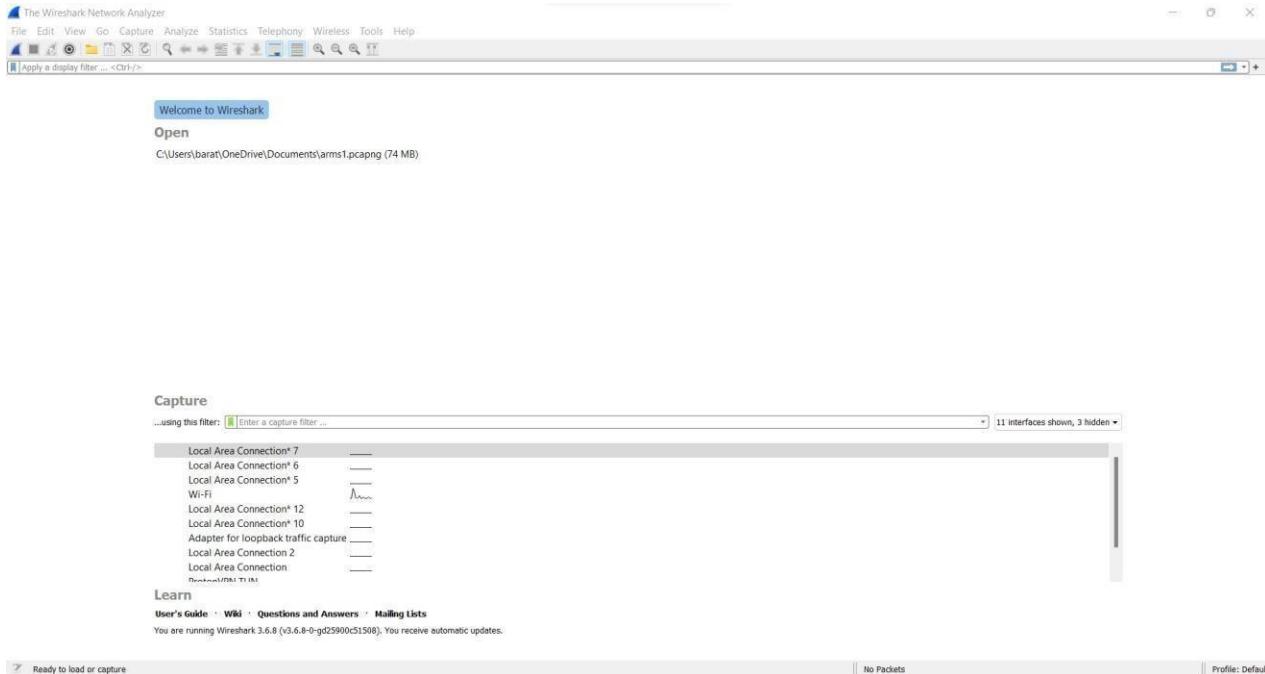
Result:

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

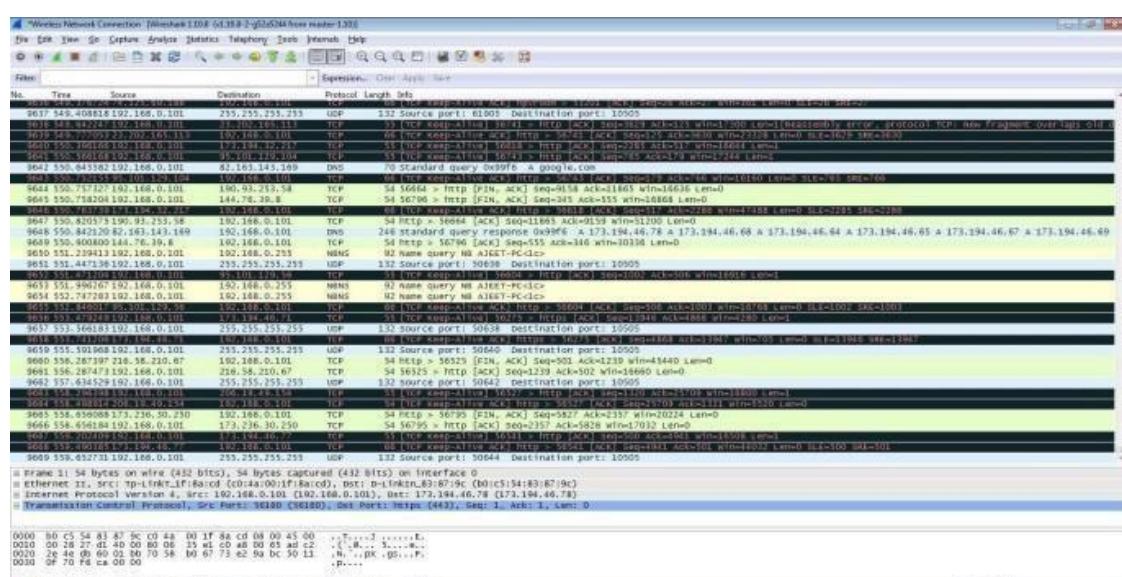
Aim: Use Wireshark sniffer to capture network traffic and analyze. Procedure:

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 ifneeded.

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 HTTP packets. The browser window displays a 'Sign In' page for 'SAVEETHA SCHOOL OF ENGINEERING'. The user has entered 'admin' for the username and 'password' for the password. An error message at the bottom of the page states: 'The username and password you entered is invalid'. The URL in the browser is 'arms.sse.saveetha.com'.

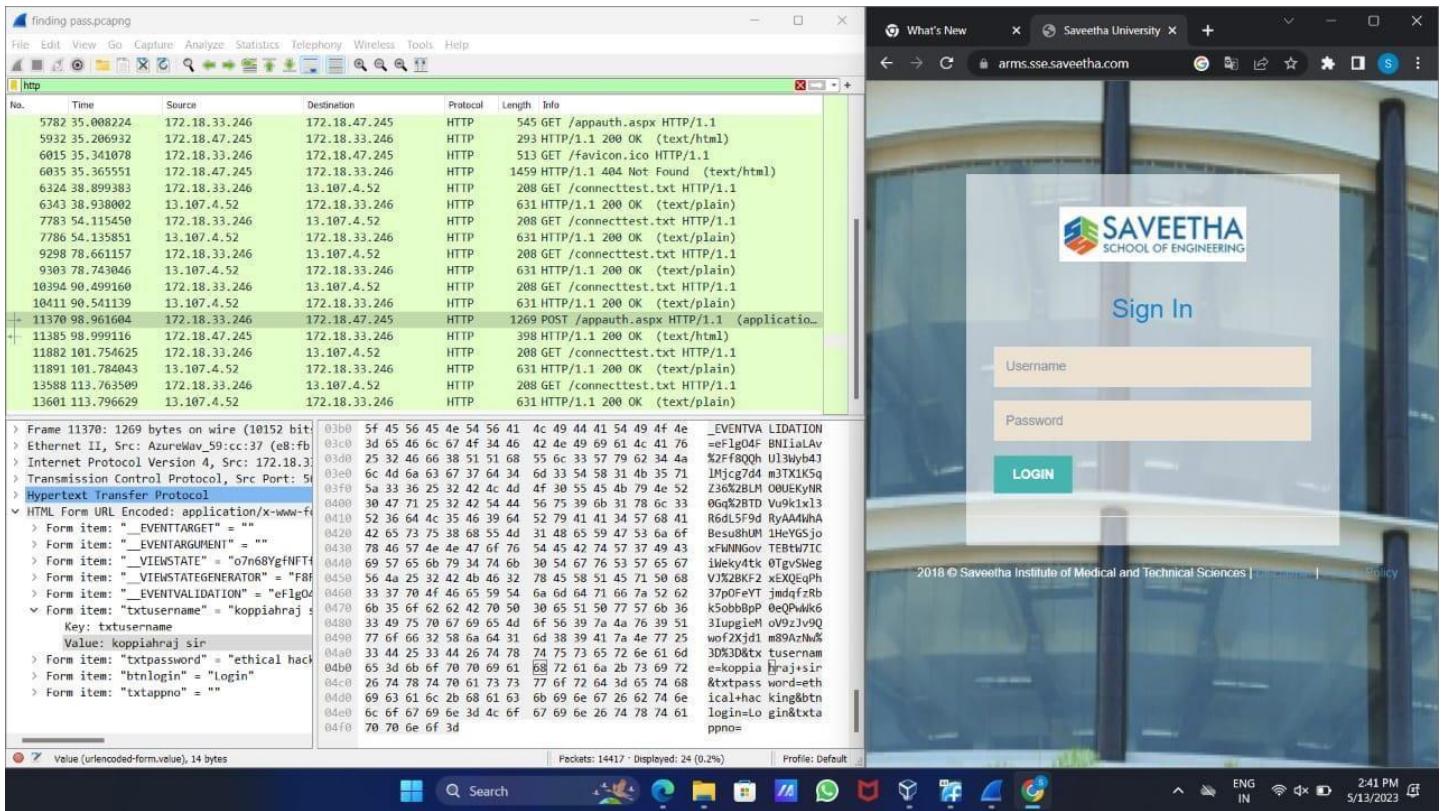
This screenshot is similar to the previous one, showing the Wireshark capture and the browser sign-in page. However, the browser page now shows a red error message: 'The username and password you entered is invalid'. The captured packet details show a POST request from the user's IP (172.18.75.157) to the server (172.18.47.245). The packet payload contains the form data: 'username=admin&password=password'. The browser window URL is 'arms.sse.saveetha.com'.

Step 10: Find the post methods for username and passwords

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

Output:

1)



Result:

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

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 ..... 172.20.10.5
[+] Port(s) .... 445,585,591,1000-1050
[+] Username .... ''
[+] Password .... ''
[+] Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none

[+] ( Enumerating Workgroup/Domain on 172.20.10.5 )

[E] Can't find workgroup/domain

[+] ( Nbtstat Information for 172.20.10.5 )
Looking up status of 172.20.10.5
No reply from 172.20.10.5
[+] ( Session Check on 172.20.10.5 )

[+] Server 172.20.10.5 allows sessions using username '', password ''

[+] ( Getting domain SID for 172.20.10.5 )
do_cmd: Could not initialise lsarpc. Error was NT_STATUS_ACCESS_DENIED
[+] Can't determine if host is part of domain or part of a workgroup
[+] ( OS Information on 172.20.10.5 )

[E] Can't get OS Info with smbdclient
[+] 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
```

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

[+] Share Enumeration on 172.20.10.5
do_connect: Connection to 172.20.10.5 Failed (Error NT_STATUS_RESOURCE_NAME_NOT_FOUND)
  Sharename      Type      Comment
Reconnecting with SMB1 for workgroup listing.
Unable to connect with SMB1 -- no workgroup available
[*] Attempting to map shares on 172.20.10.5
[+] Password Policy Information for 172.20.10.5
[E] Unexpected error from polenum:
[*] Attaching to 172.20.10.5 using a NULL share
[*] Trying protocol 139/SMB...
  [!] Protocol failed: Cannot request session (Called Name:172.20.10.5)
[*] Trying protocol 445/SMB...
  [!] Protocol failed: SMB SessionError: STATUS_ACCESS_DENIED({Access Denied} A process has requested access to an object but has not been granted those access rights.)
[E] Failed to get password policy with rpcclient
[+] Groups on 172.20.10.5
[*] Getting builtin groups:
[*] Getting builtin group memberships:
[*] Getting local groups:
[*] Getting local group memberships:
[*] 33°C Partly sunny
[+] 13:27 14-09-2022 ENG IN
```

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

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

[E] Failed to get password policy with rpcclient
[+] Groups on 172.20.10.5
[*] Getting builtin groups:
[*] Getting builtin group memberships:
[*] Getting local groups:
[*] Getting local group memberships:
[*] Getting domain groups:
[*] Getting domain group memberships:
[+] Users on 172.20.10.5 via RID cycling (RIDs: 500-550,1000-1050)
[E] Couldn't get SID! NT_STATUS_ACCESS_DENIED. RID cycling not possible.
[+] Getting printer info for 172.20.10.5
do_cmd: Could not initialise spoolss. Error was NT_STATUS_ACCESS_DENIED
enum4linux complete on Wed Sep 14 03:48:58 2022
[*] 33°C Partly sunny
[+] 13:58 14-09-2022 ENG IN
```

Output:

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

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

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

[E] Can't Find workgroup/domain

=====
( Nbtstat Information for 172.20.10.5 )

Looking up status of 172.20.10.5
No reply from 172.20.10.5
=====
( Session Check on 172.20.10.5 )

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

[root㉿kali)-[~]
```

Result:

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

EX.NO: 10 BATCH FILE EXECUTION

AIM:

To create a Windows batch file.

PROCEDURE:

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

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

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

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

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

1.Create a New Text Document:

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

1.CODE:

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

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

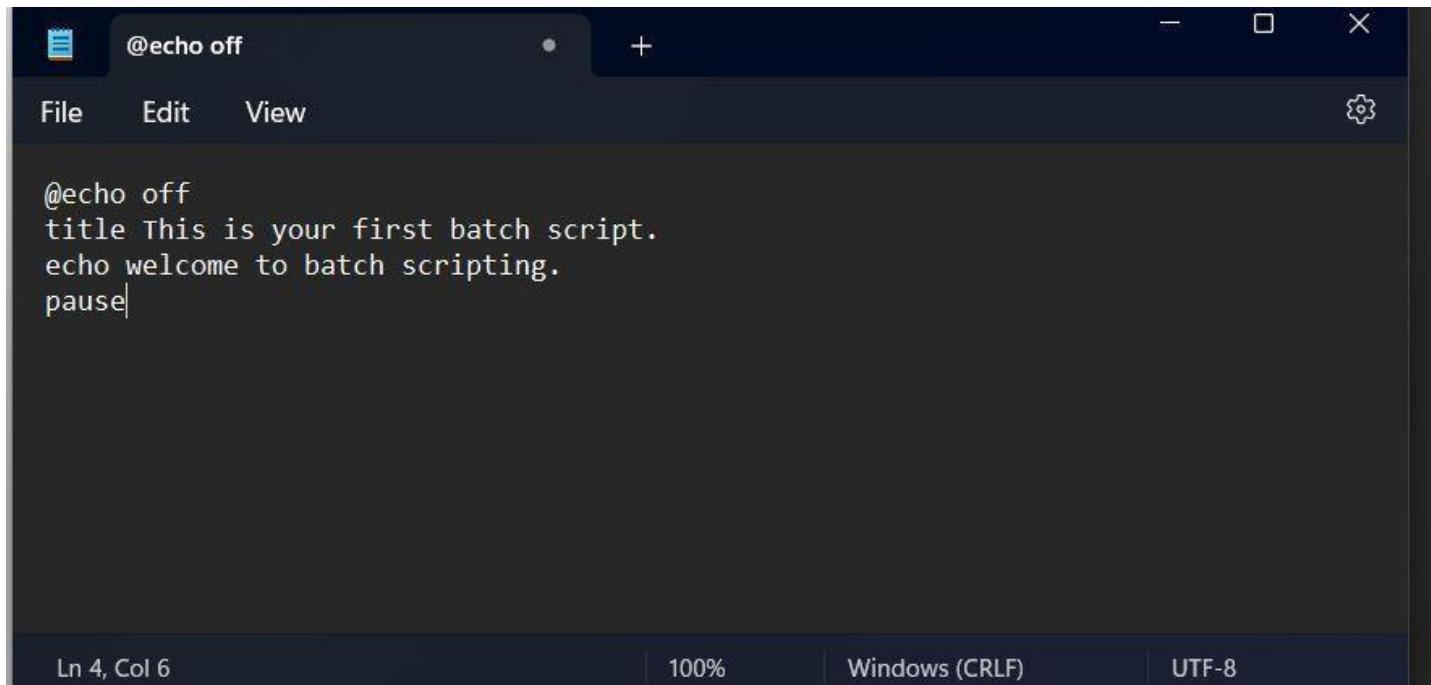
1. TO SAVE a BAT File

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

2.To RUN as BAT File

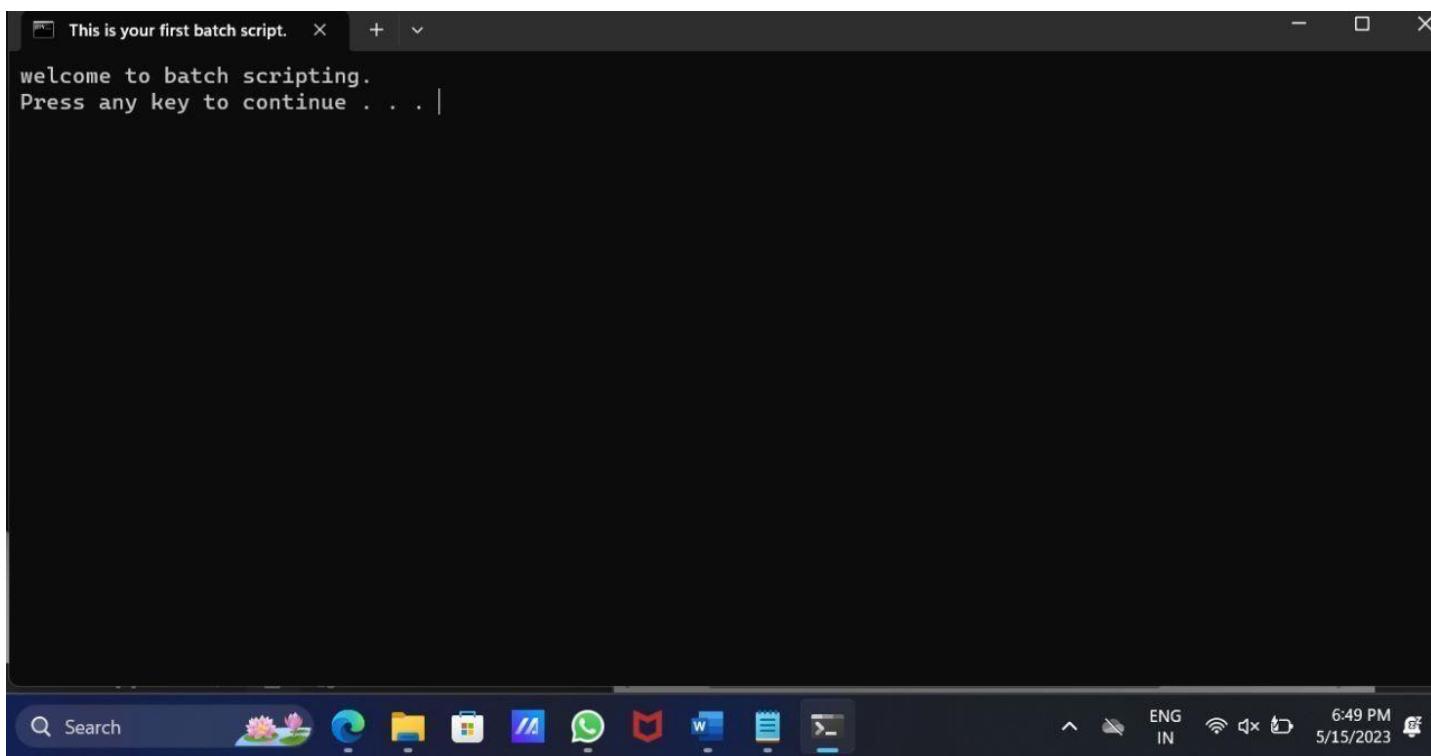
Once you'd saved your file, all you need to do is double-click your BAT file. Instantly, your web pages will open. If you'd like, you can place this file on your desktop. This will allow you to access all of your favorite websites at once.

OUTPUT:

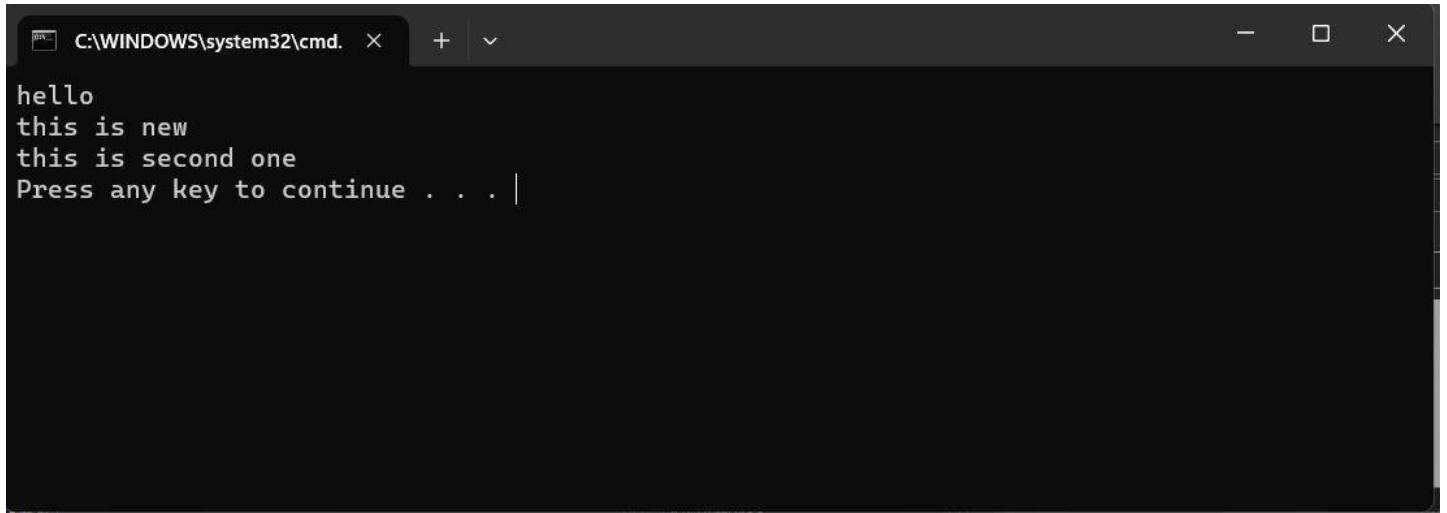


A screenshot of a code editor window titled '@echo off'. The menu bar includes 'File', 'Edit', and 'View'. The status bar at the bottom shows 'Ln 4, Col 6', '100%', 'Windows (CRLF)', and 'UTF-8'. The main area contains the following batch script code:

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



A screenshot of a terminal window titled 'This is your first batch script.'. The window displays the output of the batch script: 'welcome to batch scripting.' followed by 'Press any key to continue . . . |'. The taskbar at the bottom shows various application icons and the system tray with network and battery status.



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 . . . |

Result:

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