

ITA144-ETHICAL HACKING

LAB MANUAL

Exercise No 1: Nmap Scan

Aim:

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

Procedure:

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

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

Scanning Techniques

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

Step 3:-

To perform host discovery

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

Step4:-

Port Specification

<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

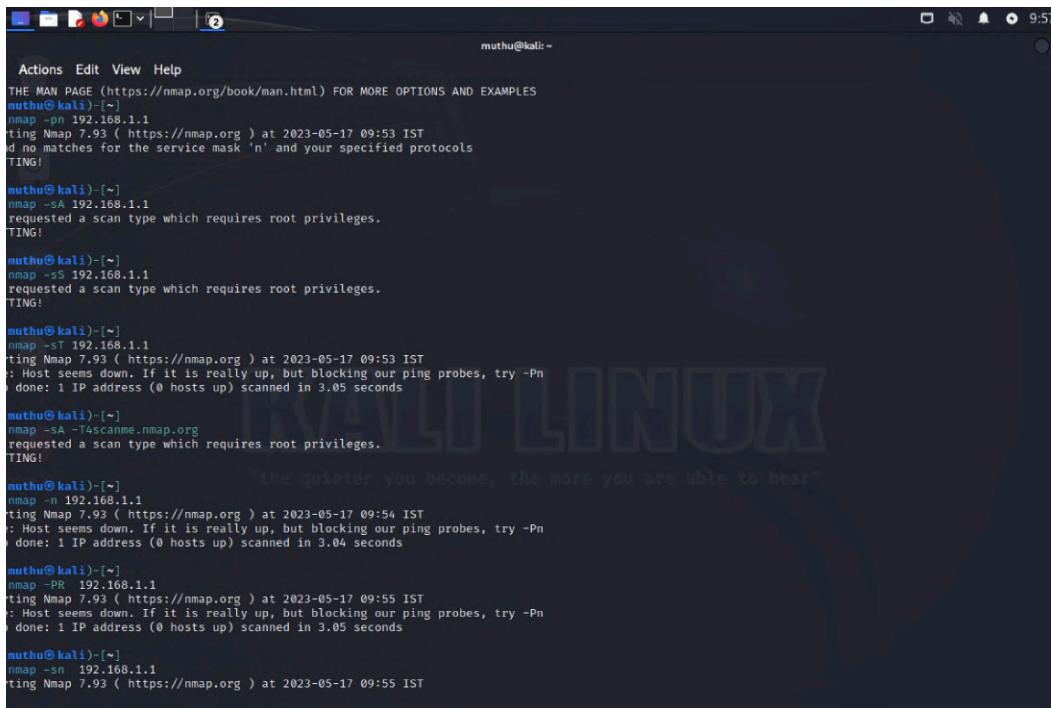
Flag	Use	Example
-sV	detect the version of services running	nmap -sV 192.168.1.1
-A	aggressive scan	nmap -A 192.168.1.1
-O	detect operating system of the target	nmap -O 192.168.1.1

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

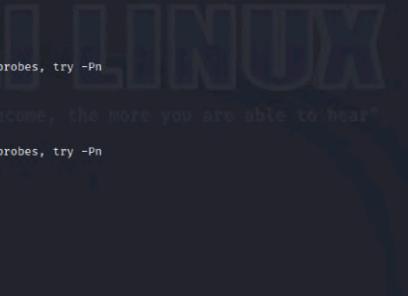
Output:



The screenshot shows a terminal window on a Kali Linux desktop environment. The terminal is running a series of Nmap commands against the IP address 192.168.1.1. The output for each command is as follows:

- nmap -pn 192.168.1.1**: Prints the version of Nmap (7.93) and the date (2023-05-17 09:53 IST). It also states that no matches were found for the service mask 'n' and your specified protocols.
- nmap -SA 192.168.1.1**: Prints the version of Nmap (7.93) and the date (2023-05-17 09:53 IST). It states that requested a scan type which requires root privileges.
- nmap -SS 192.168.1.1**: Prints the version of Nmap (7.93) and the date (2023-05-17 09:53 IST). It states that requested a scan type which requires root privileges.
- nmap -ST 192.168.1.1**: Prints the version of Nmap (7.93) and the date (2023-05-17 09:53 IST). It states that Host seems down. If it is really up, but blocking our ping probes, try -Pn.
- nmap -SA -T4scanne.rnmap.org**: Prints the version of Nmap (7.93) and the date (2023-05-17 09:54 IST). It states that requested a scan type which requires root privileges.
- nmap -n 192.168.1.1**: Prints the version of Nmap (7.93) and the date (2023-05-17 09:54 IST). It states that Host seems down. If it is really up, but blocking our ping probes, try -Pn.
- nmap -PR 192.168.1.1**: Prints the version of Nmap (7.93) and the date (2023-05-17 09:55 IST). It states that Host seems down. If it is really up, but blocking our ping probes, try -Pn.
- nmap -sn 192.168.1.1**: Prints the version of Nmap (7.93) and the date (2023-05-17 09:55 IST).

Caption



```
muthu@kali:~
```

```
Actions Edit View Help
```

```
: Host seems down. If it is really up, but blocking our ping probes, try -Pn
: done: 1 IP address (@ hosts up) scanned in 3.04 seconds
```

```
muthu@kali:[~]
```

```
nmap -PK 192.168.1.1
tinc Nmap 7.93 ( https://nmap.org ) at 2023-05-17 09:55 IST
: Host seems down. If it is really up, but blocking our ping probes, try -Pn
: done: 1 IP address (@ hosts up) scanned in 3.05 seconds
```

```
muthu@kali:[~]
```

```
nmap -Sn 192.168.1.1
tinc Nmap 7.93 ( https://nmap.org ) at 2023-05-17 09:55 IST
: Host seems down. If it is really up, but blocking our ping probes, try -Pn
: done: 1 IP address (@ hosts up) scanned in 3.01 seconds
```

```
muthu@kali:[~]
```

```
nmap -A 192.168.1.1
tinc Nmap 7.93 ( https://nmap.org ) at 2023-05-17 09:56 IST
: Host seems down. If it is really up, but blocking our ping probes, try -Pn
: done: 1 IP address (@ hosts up) scanned in 3.26 seconds
```

```
muthu@kali:[~]
```

```
nmap -SV 192.168.1.1
tinc Nmap 7.93 ( https://nmap.org ) at 2023-05-17 09:56 IST
: Host seems down. If it is really up, but blocking our ping probes, try -Pn
: done: 1 IP address (@ hosts up) scanned in 3.15 seconds
```

```
muthu@kali:[~]
```

```
"the quieter you become, the more you are able to hear"
nmap -PR 192.168.1.1
tinc Nmap 7.93 ( https://nmap.org ) at 2023-05-17 09:56 IST
: Host seems down. If it is really up, but blocking our ping probes, try -Pn
: done: 1 IP address (@ hosts up) scanned in 3.04 seconds
```

```
muthu@kali:[~]
```

```
nmap -TO 192.168.1.1
tinc Nmap 7.93 ( https://nmap.org ) at 2023-05-17 10:00 IST
```

Caption

Result:

Using the nmap tool in Karli linux all the port scanings are performed

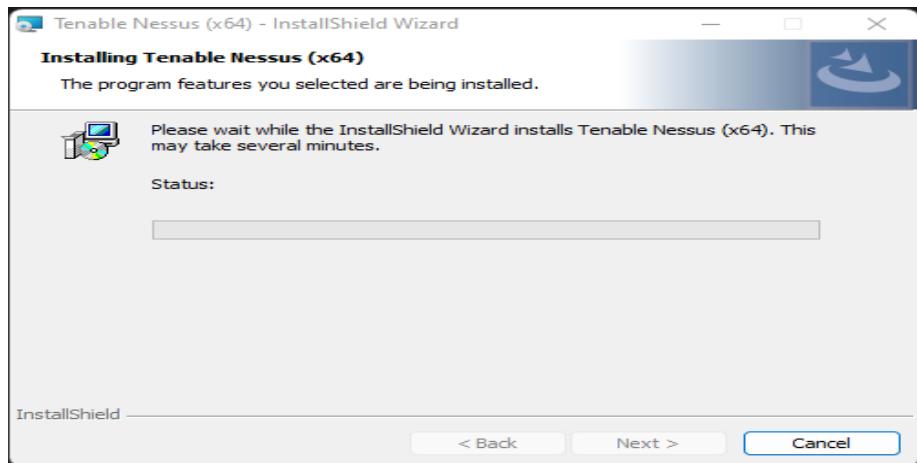
Exercise No 2: Vulnerability Access Scan Using Nessus

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

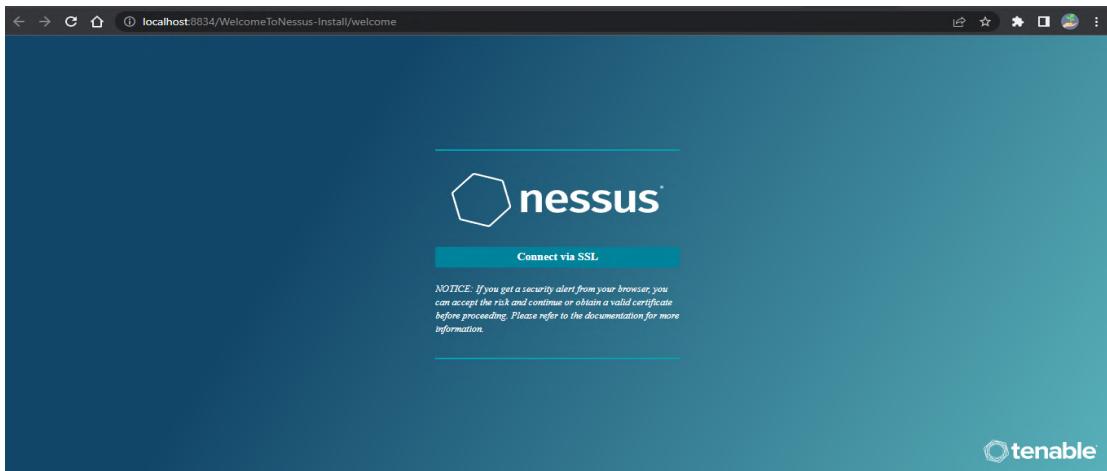
Step 1:- <https://www.tenable.com/downloads/nessus?loginAttempted=true>

The screenshot shows the Tenable.com website's download section for the Nessus tool. On the left, there's a sidebar with links to various Tenable products like Nessus, Nessus Agents, and Log Correlation Engine. The main content area is titled 'Nessus' and contains three numbered sections: 1. Download and Install Nessus, 2. Start and Setup Nessus, and 3. Getting Started. Under 'Download and Install Nessus', there are dropdown menus for 'Version' (set to 'Nessus - 10.4.2') and 'Platform' (set to 'Windows - x86_64'). A large blue 'Download' button is prominent. To the right, a 'Summary' box provides details: Release Date (Jan 18, 2023), Release Notes (Nessus 10.4.2 Release Notes), and Signing Keys (RPM-GPG-KEY-Tenable-4098 for 10.4 and above, and RPM-GPG-KEY-Tenable-2048 for 10.3 and below).

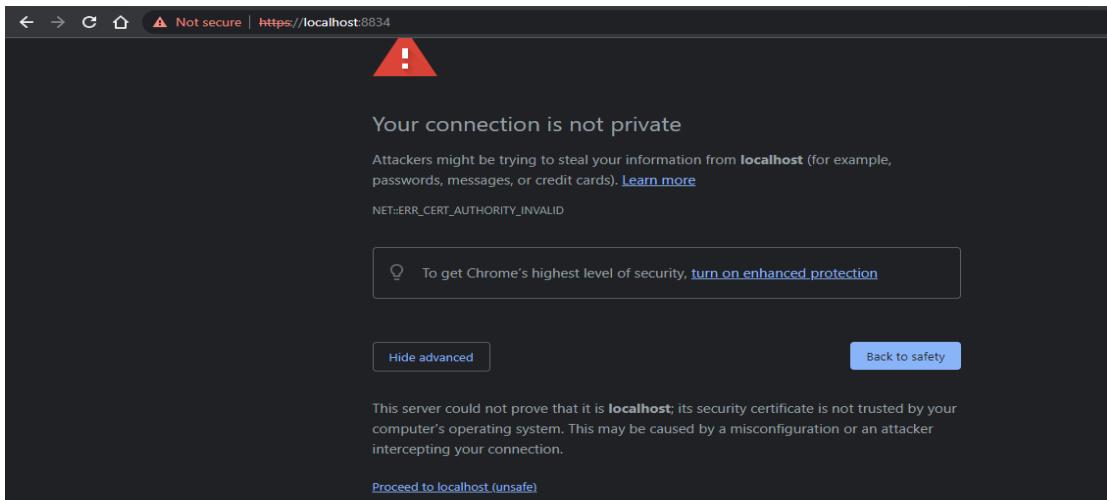
Step 2: Choose your OS and download , install



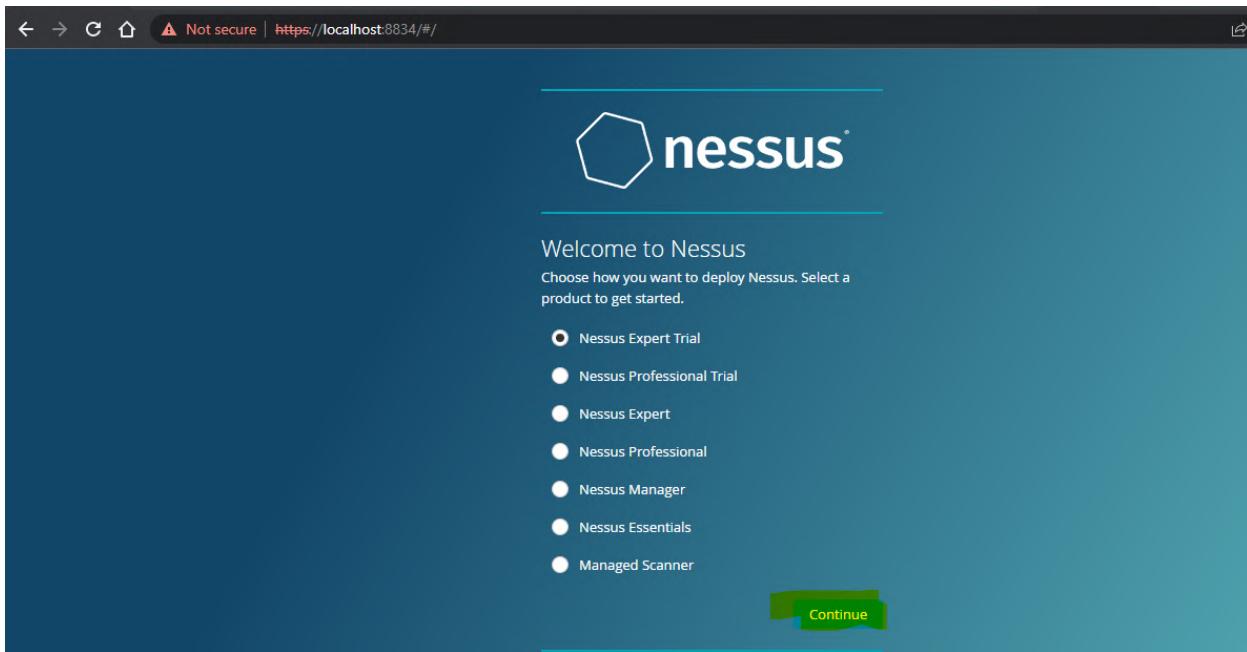
Step 3: Once installation is completed it will open in default browser



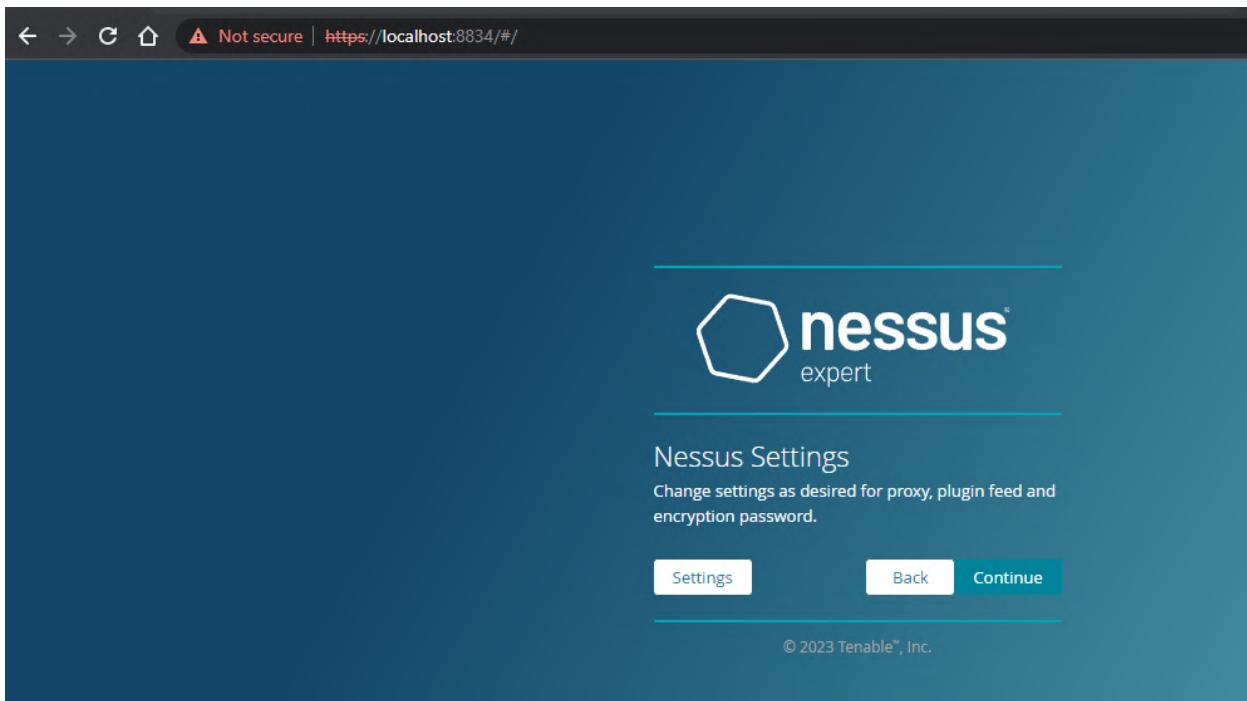
Step 5:- (click on the proceed to local host)



Step 6:- Please choose the Nessus Expert



Step 7: Click on continue



Step 8:- Register with your organizational email id

Not secure | https://localhost:8834/#/

expert

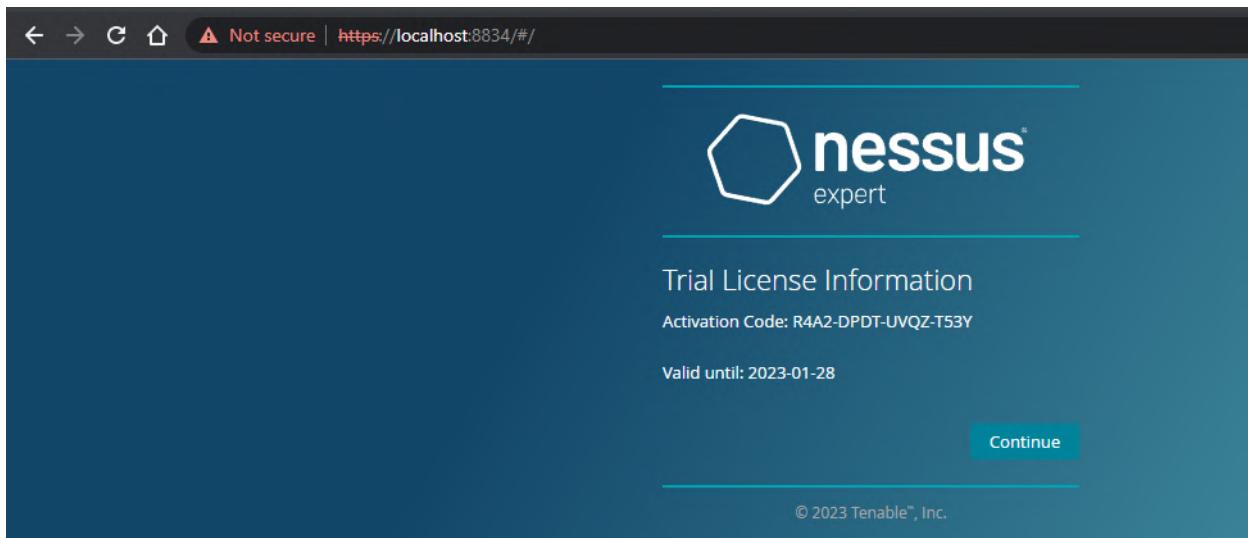
Create Account

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

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

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

Step 9:- please note down the activation key



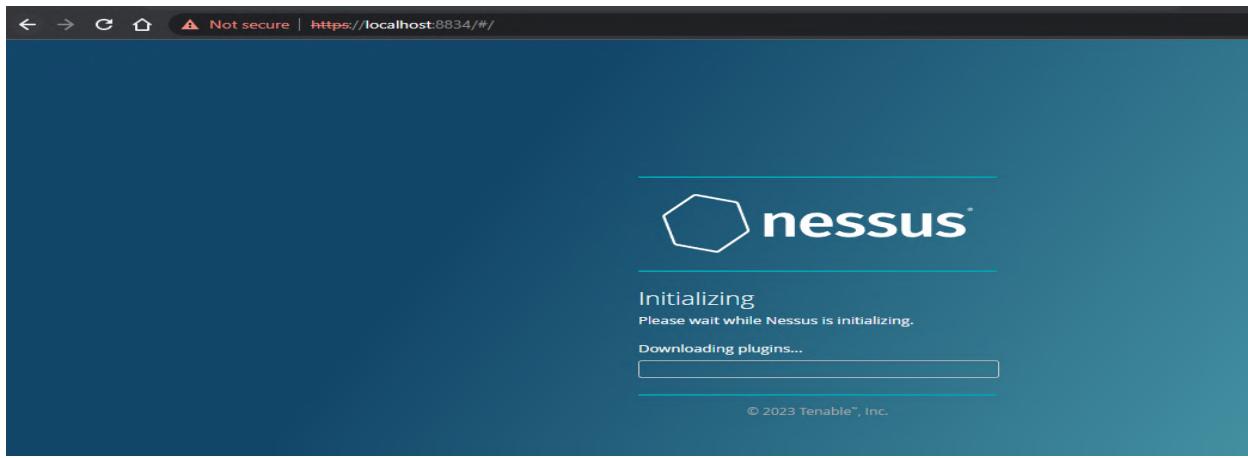
Step 10:- set up your username & password

The screenshot shows a web browser window with the URL <https://localhost:8834/#/>. The page title is "Create a user account". The Nessus logo, consisting of a hexagon icon and the word "nessus" in lowercase, is displayed above the form. The subtext "expert" is visible below the logo. The form fields are labeled "Username *" and "Password *". Below the password field is an "Eye" icon for password visibility. At the bottom right are "Back" and "Submit" buttons. A copyright notice at the bottom reads "© 2023 Tenable™, Inc."

Step 11:-Type username and password

The screenshot shows the same "Create a user account" page as the previous one, but with the fields populated. The "Username *" field contains "pusphalatha" and the "Password *" field contains "Test@1234". The rest of the page layout, including the logo, subtext, and buttons, remains the same.

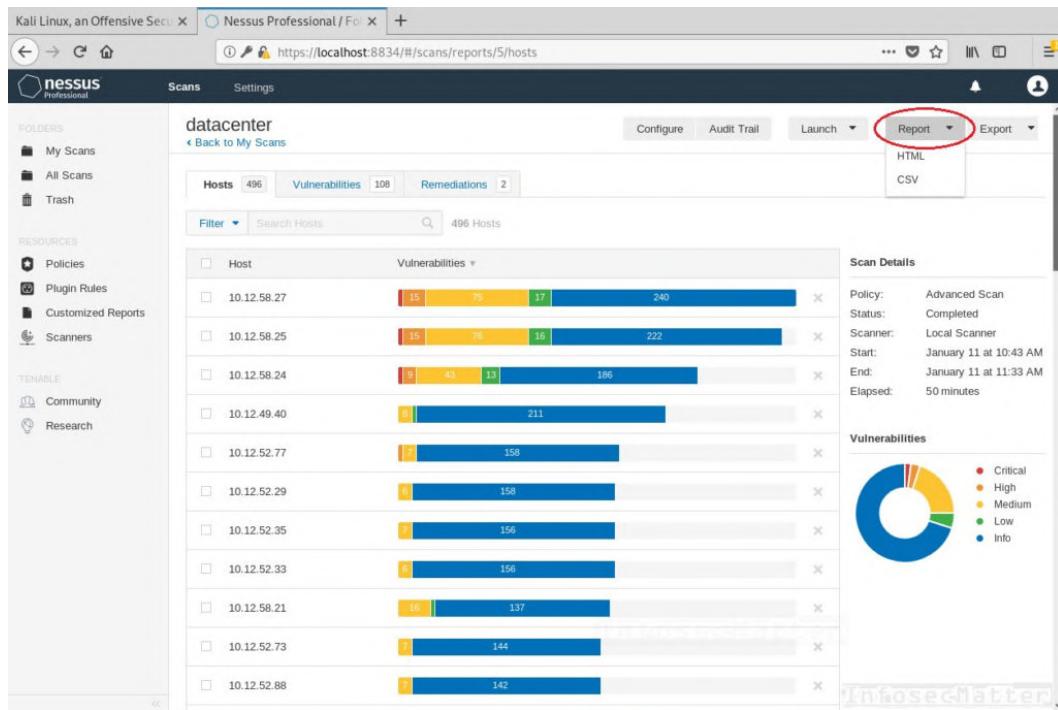
Step 12:- Please wait until download is completed



Step 13: Select My Scans

A screenshot of the Nessus web interface. The top navigation bar shows multiple tabs open, including "Inbox", "Google", "HACKIN", "Web Ap...", "A Comp...", "LAB EXE", "Home", and "Nessus". The main menu on the left includes "Scans" and "Settings". The "Scans" section has a sidebar with "FOLDERS" (My Scans, All Scans, Trash), "RESOURCES" (Policies, Plugin Rules, Customized Reports, Terrascan), and a weather widget (79°F Haze). The main content area is titled "My Scans" and displays the message "This folder is empty. [Create a new scan.](#)". There are buttons for "Import", "New Folder", and "New Scan". The bottom of the screen shows a taskbar with various icons and a system tray with the date and time (9:49 PM 1/21/2023).

OUTPUT



Caption

RESULT : SUCCESSFULLY SCANED THE PORTS

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.
```

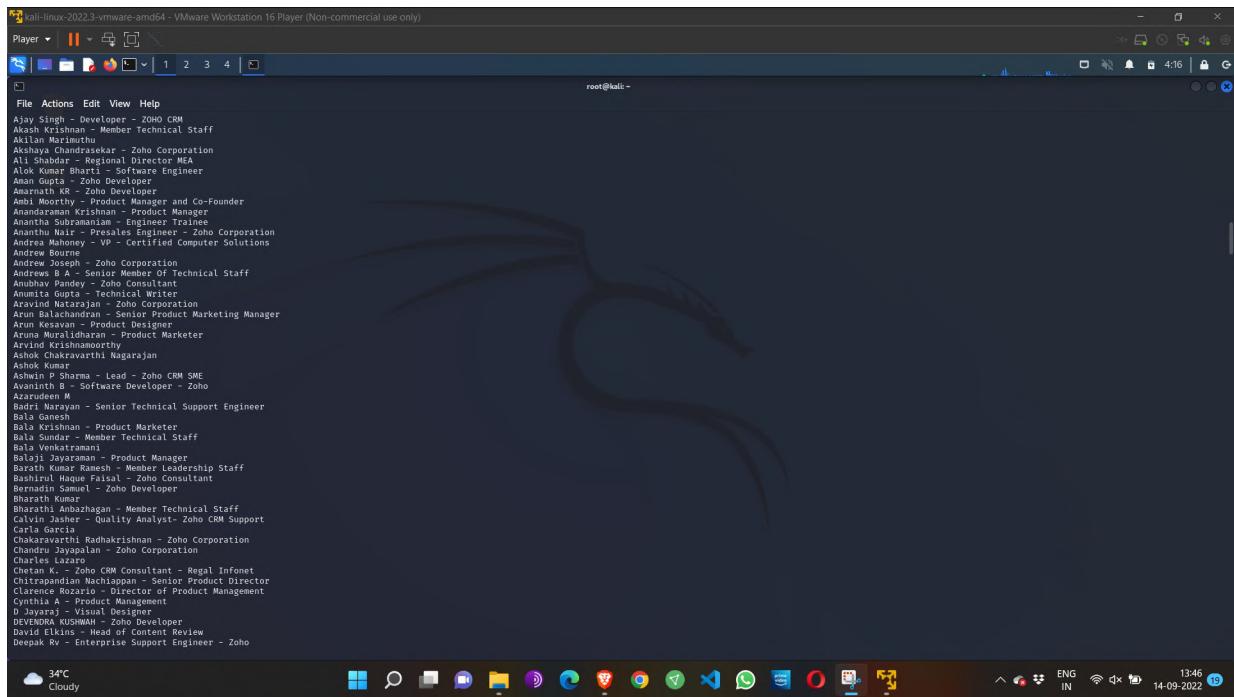
```
-b is used to specify search engine name.
```

STEP 2: Run the following command

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

Caption

```
kali-linux-2022.3-vmware-and64 - VMware Workstation 16 Player (Non-commercial use only)
Player | II | 1 2 3 4 | X
File Actions Edit View Help
Ajay Singh - Developer - Zoho CRM
Akash Krishnamoorthy - Member Technical Staff
Akshay Chaudhary - Member Technical Staff
Akshaya Chandrasekar - Zoho Corporation
Alis Shabdar - Regional Director MEA
Alka Kumar Bharti - Software Engineer
Anan Venkata - Zoho Developer
Anuradha KR - Zoho Developer
Anubhav - Product Manager and Co-Founder
Anubhav - Zoho Project Manager
Anushtha Subramanian - Engineer Trainee
Anushtha Nair - Presales Engineer - Zoho Corporation
Andrew Mahoney - VP - Certified Computer Solutions
Andrew Baskaran
Andrew Joseph - Zoho Corporation
Andrews B A - Senior Member Of Technical Staff
Anil Kumar Pandey - Zoho Corporation
Anusita Srinivas - Technical Writer
Aravind Natarajan - Zoho Corporation
Arun Balachandran - Senior Product Marketing Manager
Aruna Venkateswaran - Designer
Aruna Muralidharan - Product Marketer
Arvind Krishnamoorthy
Ashok Chakravarthy Nagarajan
Ashok Kumar
Ashwin P Sharma - Lead - Zoho CRM SME
Avaninth B - Software Developer - Zoho
Avaziradeen M
Badrinath - Senior Technical Support Engineer
Bala Ganesh
Bala Krishnan - Product Marketer
Balaji Venkatesan - Member Technical Staff
Balaji Venkatramani
Balaji Jayaraman - Product Manager
Barath Kumar Ramesh - Member Leadership Staff
Barath Kumar Ramesh - Financial Analyst & Consultant
Bernardin Samuel - Zoho Developer
Bharath Kumar
Bharathi Subrahmanyam - Member Technical Staff
Carla Jashra - Quality Analyst- Zoho CRM Support
Carla Garcia
Chakaravarthi Radhakrishnan - Zoho Corporation
Chandru Venkatesan - Zoho Corporation
Charles Lazar
Chetan K. - Zoho CRM Consultant - Regal Infonet
Chittrapandian Nachimuthu - Senior Product Director
Cleber Souza - Director of Product Management
Cynthia A - Product Management
D Jayaraj - Visual Designer
DEVENKUMAR KUSUMAH - Zoho Developer
David Elkins - Head of Content Review
Deepak RV - Enterprise Support Engineer - Zoho
root@kali: ~
```



kali-linux-2022.3-vmware-amd64 - VMware Workstation 16 Player (Non-commercial use only)

Player | || v [] X

File Actions Edit View Help

A563949

[*] Interesting URLs found: 25

<http://www.zoho.com/>

<http://www.zoho.com/assist/>

<http://www.zoho.com/books/>

<http://www.zoho.com/campaigns/?src=fromproduct>

<http://www.zoho.com/campaigns/explainerv/campaignr-view.html>

<http://www.zoho.com/cliq/?serviceurl=%2Fchats%2F24317725500151008&src=fromproduct>

<http://www.zoho.com/cliq/?serviceurl=%2Findex.2d0zsrc=fromproduct>

<http://www.zoho.com/creatus.html>

<http://www.zoho.com/crm/>

<http://www.zoho.com/crmplus/>

<http://www.zoho.com/crmplus/>

<http://www.zoho.com/emailsender/>

<http://www.zoho.com/forms/>

http://www.zoho.com/invoice/?utm_source=20sum_medium-pdf

<http://www.zoho.com/marketingautomation/>

<http://www.zoho.com/ml/>

<http://www.zoho.com/ml/salesid/>

<http://www.zoho.com/rdevs/?src=zoho-home&%3Bref=zohome>

<http://www.zoho.com/report-abuse/>

<http://www.zoho.com/salesid/>

<http://www.zoho.com/survey/>

[*] No Twitter users found.

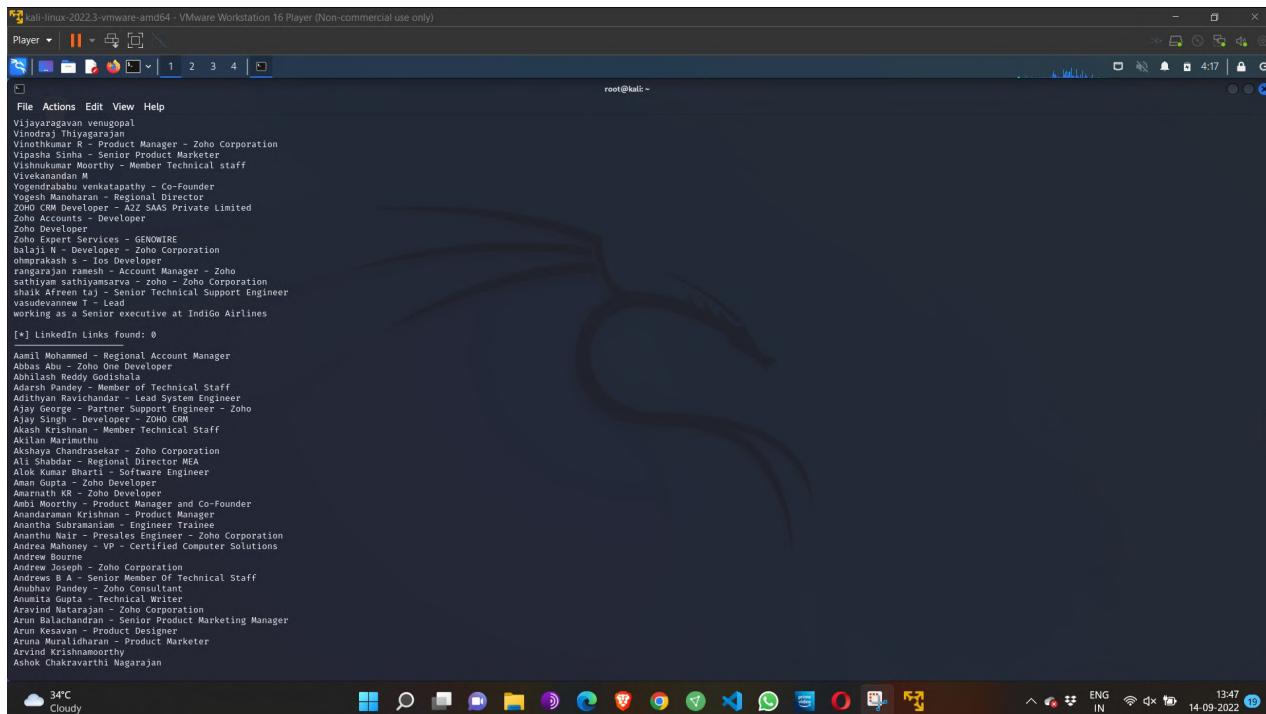
[*] LinkedIn Users found: 292

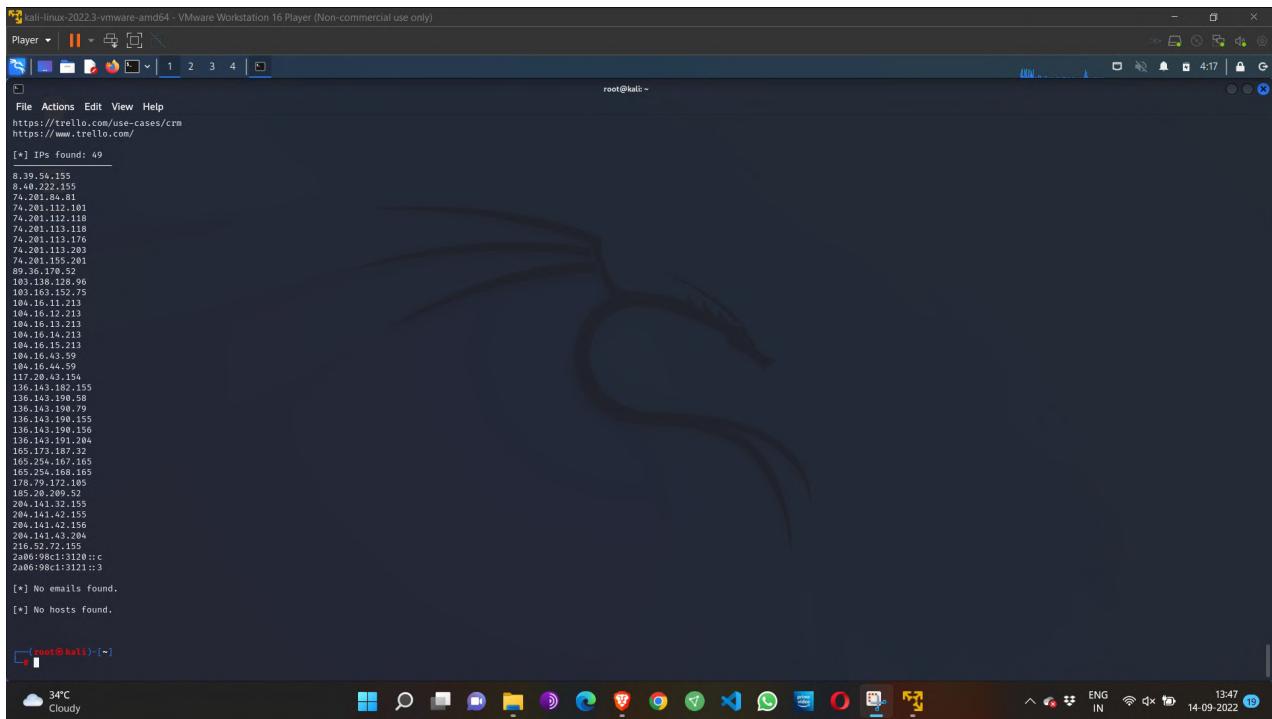
Asmil Mohammed - Regional Account Manager
Abbas Abu - Zoho One Developer
Abhilash Reddy Godishala
Adarsh Pandey - Member Technical Staff
Akash Ravindra - Lead System Engineer
Ajay George - Partner Support Engineer - Zoho
Ajay Singh - Developer - ZOHO CRM
Akash Krishnamoorthy - Member Technical Staff
Ali Shabdar - Regional Director MEA
Akshaya Chandrasekar - Zoho Corporation
Ali Shabdar - Regional Director MEA
Alok Kumar Bharat - Software Engineer
Anandaraman Krishnan - Zoho Developer
Amaranath KR - Zoho Developer
Ambi Moorthy - Product Manager and Co-Founder
Anandaraman Krishnan - Product Manager

Cloudy 34°C ENG IN 13:46 14-09-2022

```
fati-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
Aishwarya D'Souza - Member Technical staff
Vivekanandan W
Yogendrababu venkatapatty - Co-Founder
Yogesh Manoharan - Regional Director
Zoho - Founder - A2Z SaaS Private Limited
Zoho Accounts - Dev
Zoho Developer
Zoho Expert Services - GENWIRE
Zoho Global Services - Zoho Corporation
omprakash s - Ios Developer
ompragaran ramesh - Account Manager - Zoho
sanket saliyasareva - zoho - Zoho Corporation
shukt Afridi - Zoho Technical Support Engineer
vasudevanem T - Lead
working as a Senior executive at Indigo Airlines
[*] Trellio URLs found: 33
http://www.trellio.com/contact
https://trellio.com/integrations
https://trellio.com/integrations/sales-support
https://trellio.com/power-ups
https://trellio.com/power-ups/595e990fa8f37372a4f456fd4
https://trellio.com/power-ups/5bc1aa1922a254299bb0a3/zoho-crm
https://trellio.com/power-ups/5b53db70cc75f299f1d473/automateio
https://trellio.com/power-ups/5b53db70cc75f299f1d473/automateio
https://trellio.com/power-ups/5b53db70cc75f299f1d473/automateio
https://trellio.com/power-ups/Category/it-project-management
https://trellio.com/power-ups/Category/marketing-social-media
https://trellio.com/power-ups/Category/sales-support
https://trellio.com/pricing
https://trellio.com/teams/support
https://trellio.com/templates
https://trellio.com/templates/design
https://trellio.com/templates/design/design-system-checklist-yzn5vfon
https://trellio.com/templates/design/free-lance-branding-project-z5w66hs]
https://trellio.com/templates/design/research-iteration-8tqggnmz
https://trellio.com/templates/design/research-iteration-8tqggnmz
https://trellio.com/templates/product-management/5-etapas-de-gerenciamento-de-produtos-7s8avmuv
https://trellio.com/templates/product-management/5-listes-pour-la-gestion-de-produits-0lufgyd7
https://trellio.com/templates/product-management/5-listes-pour-la-gestion-de-produits-0lufgyd7
https://trellio.com/templates/product-management/5-listes-pour-la-gestion-de-produits-0lufgyd7
https://trellio.com/templates/product-management/contraindu-un-mvp-shy7plr
https://trellio.com/templates/product-management/fabrication-process-dakvjp35
https://trellio.com/templates/product-management/product-roadmap-template-frbqjsbh
https://trellio.com/templates/product-management/roadmap-de-produits-0lufgyd7
https://trellio.com/templates/product-management/roadmap-de-produits-0lufgyd7
https://trellio.com/templates/product-management/shipping-planner-mc3vzive
https://trellio.com/tour
https://trellio.com/use-cases/crm

43°C Cloudy ENG IN 13:47
```





```
kali-linux-2022.3-vmware-amd64 - VMware Workstation 16 Player (Non-commercial use only)
Player | || v [ ] X
[ ] 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
74.201.111.101
74.201.112.118
74.201.113.118
74.201.113.176
74.201.113.193
74.201.155.201
89.36.170.52
103.138.128.96
134.12.12.75
104.16.11.213
104.16.12.213
104.16.13.213
104.16.14.213
104.16.15.213
104.16.43.59
104.16.44.59
11.11.11.155
136.143.182.155
136.143.190.58
136.143.190.79
136.143.193.155
136.143.198.156
136.143.191.204
165.173.187.32
165.173.187.155
165.254.168.165
178.79.172.185
185.20.209.50
204.141.42.155
204.141.42.156
204.141.43.284
23.23.23.155
2406:98c1:3120::c
2406:98c1:3121::3
[*] No emails found.
[*] No hosts found.

[root@kali ~]
[ ] 34°C Cloudy
```

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 .

RESULTS :

successfully demonstrated information gathering 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:

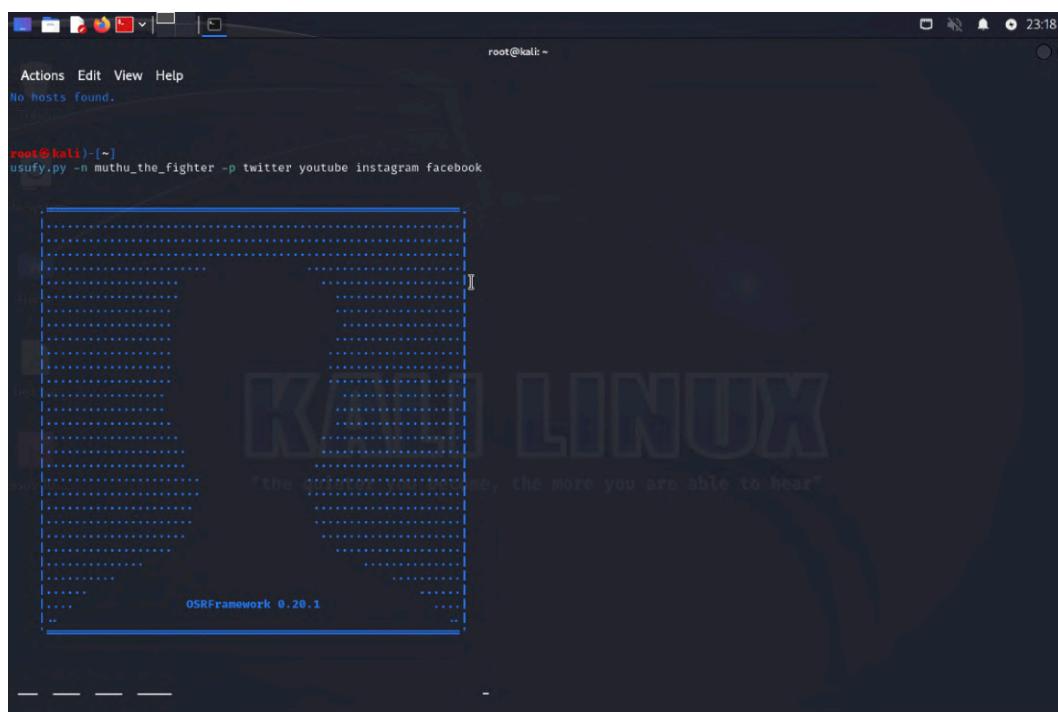
Step 1: Log into kali linux machine

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
```



The screenshot shows a terminal window on a Kali Linux desktop environment. The terminal title is 'root@kali: ~'. The command entered is 'usufy.py -n muthu_the_fighter -p twitter youtube instagram facebook'. The output shows a large, faint watermark of the word 'LINUX' in the background, with the text 'the more you see, the more you are able to hear'. At the bottom of the terminal window, it says 'OSRFramework 0.20.1'.

Caption

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

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

In 'alias_generator', '--common-words' adds words like 'xxx', 'real'... -- 

Usufy | Copyright (c) Yaiza Rubio & Félix Brezo (i3visio) 2014-2020

This program comes with ABSOLUTELY NO WARRANTY. This is free software, and you
welcome to redistribute it under certain conditions. For additional info,
visit <https://www.gnu.org/licenses/agpl-3.0.txt>.

--05-16 23:17:03.442567      Starting search in 4 platform(s)... Relax!
Press <Ctrl + C> to stop ...

--05-16 23:17:09.629911      Results obtained (4):

/lib/python3/dist-packages/pyexcel/deprecated.py:208: UserWarning: Deprecated usage since v0.2.1! Explicit import is no longer required. pyexcel.ext.xls auto imported.
warnings.warn(
cts recovered (2023-5-16_23h17m)::

    com.i3visio.URI           | com.i3visio.Alias | com.i3visio.Platform |
    tps://www.facebook.com/muthu_the_fighter | muthu_the_fighter | Facebook |
    tps://www.youtube.com/user/muthu_the_fighter/about | muthu_the_fighter | Youtube |
    tp://www.instagram.com/muthu_the_fighter | muthu_the_fighter | Instagram |
```

Caption

```
--05-16 23:17:03.442567      Starting search in 4 platform(s)... Relax!
Press <Ctrl + C> to stop ...

--05-16 23:17:09.629911      Results obtained (4):

/lib/python3/dist-packages/pyexcel/deprecated.py:208: UserWarning: Deprecated usage since v0.2.1! Explicit import is no longer required. pyexcel.ext.xls auto imported.
warnings.warn(
cts recovered (2023-5-16_23h17m)::

    com.i3visio.URI           | com.i3visio.Alias | com.i3visio.Platform |
    tps://www.facebook.com/muthu_the_fighter | muthu_the_fighter | Facebook |
    tps://www.youtube.com/user/muthu_the_fighter/about | muthu_the_fighter | Youtube |
    tp://www.instagram.com/muthu_the_fighter | muthu_the_fighter | Instagram |
    tp://twitter.com/muthu_the_fighter | muthu_the_fighter | Twitter |

--05-16 23:17:09.675359      You can find all the information here: ./profiles.csv
--05-16 23:17:09.675453      Finishing execution ...

Total time consumed: 0:00:06.232886
Average seconds/query: 1.5582215 seconds

something go wrong? Is a platform reporting false positives? Do you need to
upgrade 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
so that otherwise, we won't know about it!

root@Kali:[~]
```

Caption

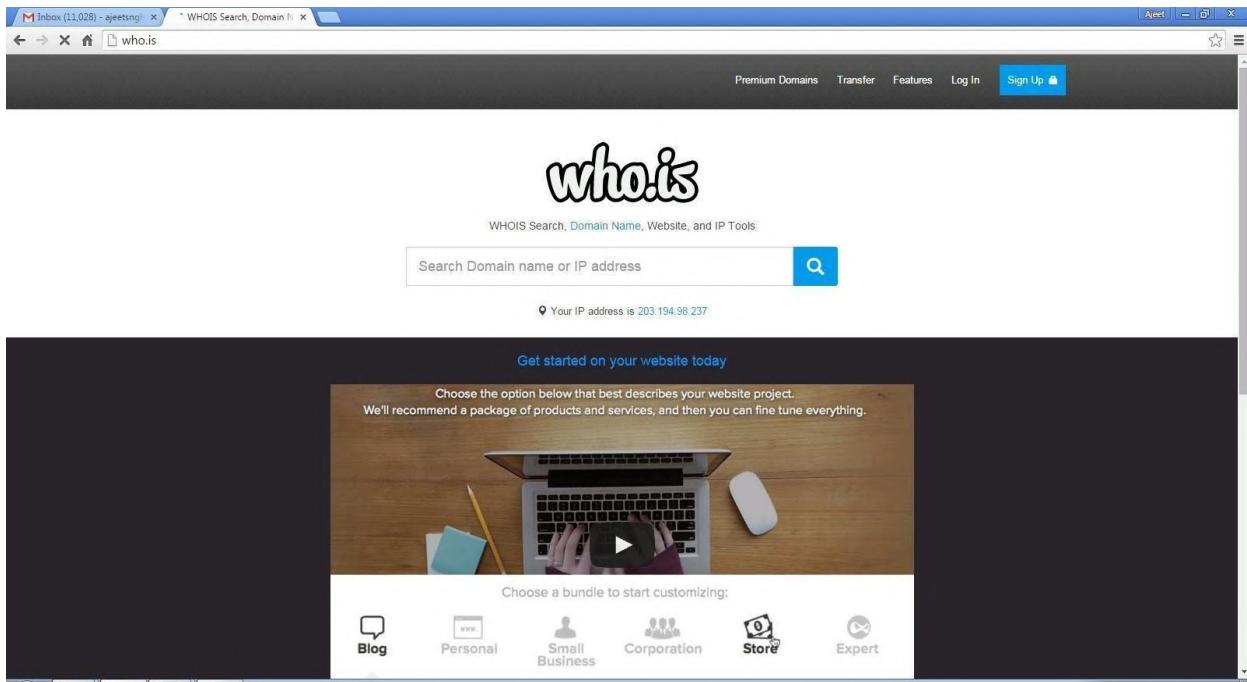
RESULT:

SUCCESSFULLY Checked for the Existence of a Profile for given user details in different platforms

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
```

Saveetha University [How to run batch files in Linux - Quora](#) Run .bat on Mac. [saveetha.com DNS information - who.is](#)

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

Premium Domains Transfer Features Login Sign Up

DNS Records for saveetha.com

cache expires in 1 minutes and 17 seconds

Hostname	Type	TTL	Priority	Content
saveetha.com	SOA	3177		ns51.domaincontrol.com dns@jormax.net 2023042101 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	3177	3	alt2.aspmx.l.google.com
saveetha.com	MX	3177	1	alt1.aspmx.l.google.com
saveetha.com	MX	3177	3	alt3.aspmx.l.google.com
saveetha.com	MX	3177	3	alt4.aspmx.l.google.com
saveetha.com	MX	3177	1	aspmx.l.google.com
saveetha.com	MX	3177	2	alt2.aspmx.l.google.com
saveetha.com	MX	3177	2	alt3.aspmx.l.google.com
saveetha.com	MX	3177	1	alt4.aspmx.l.google.com
www.saveetha.com	A	3600		198.185.159.144

Caption

RESULT:

SUCCSFULLY gathered all the informations using whois.com

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

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

Procedure:

```
Login: Tue May 16 23:22:59 on ttys000
$ netstat -an | grep www.saveetha.com
route to www.saveetha.com (198.185.159.144). 64 hops max. 52 byte packets
92.168.164.210 (192.168.164.210) 8.882 ms 7.868 ms 5.478 ms
8.286.154.10 (10.286.154.10) 523.633 ms 715.633 ms 614.193 ms
 *
 * *
 * *
 * *
 * *
 * *
 * *
 * *
 * *
 * *
 * *
 * *
 * *
 * *
 * Using TraceRoute, ping, ifconfig(LINUX), ipconfig(WINDOWS), and netstat
 Command.
```

Caption

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

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

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

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

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

Step 3: Type ifconfig command

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

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

Step 4: Type netstat command

```
C:\Users\singh>netstat
Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    127.0.0.1:1564        DESKTOP-923RK3N:1565  ESTABLISHED
  TCP    127.0.0.1:1565        DESKTOP-923RK3N:1564  ESTABLISHED
  TCP    127.0.0.1:25104       DESKTOP-923RK3N:25105  ESTABLISHED
  TCP    127.0.0.1:25105       DESKTOP-923RK3N:25104  ESTABLISHED
  TCP    127.0.0.1:25107       DESKTOP-923RK3N:25108  ESTABLISHED
  TCP    127.0.0.1:25108       DESKTOP-923RK3N:25107  ESTABLISHED
  TCP    127.0.0.1:25112       DESKTOP-923RK3N:25113  ESTABLISHED
  TCP    127.0.0.1:25113       DESKTOP-923RK3N:25112  ESTABLISHED
  TCP    127.0.0.1:25114       DESKTOP-923RK3N:25115  ESTABLISHED
  TCP    127.0.0.1:25115       DESKTOP-923RK3N:25114  ESTABLISHED
  TCP    192.168.0.57:24938     52.230.84.217:https  ESTABLISHED
  TCP    192.168.0.57:24978     162.254.196.84:27021  ESTABLISHED
  TCP    192.168.0.57:25052     a23-56-165-111:https  ESTABLISHED
  TCP    192.168.0.57:25072     test:https            TIME_WAIT
  TCP    192.168.0.57:25078     a23-56-165-111:https  ESTABLISHED
  TCP    192.168.0.57:25080     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
```

RESULT:

Using TraceRoute, ping, ifconfig(LINUX), ipconfig(WINDOWS), and netstat Command. We found a output

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



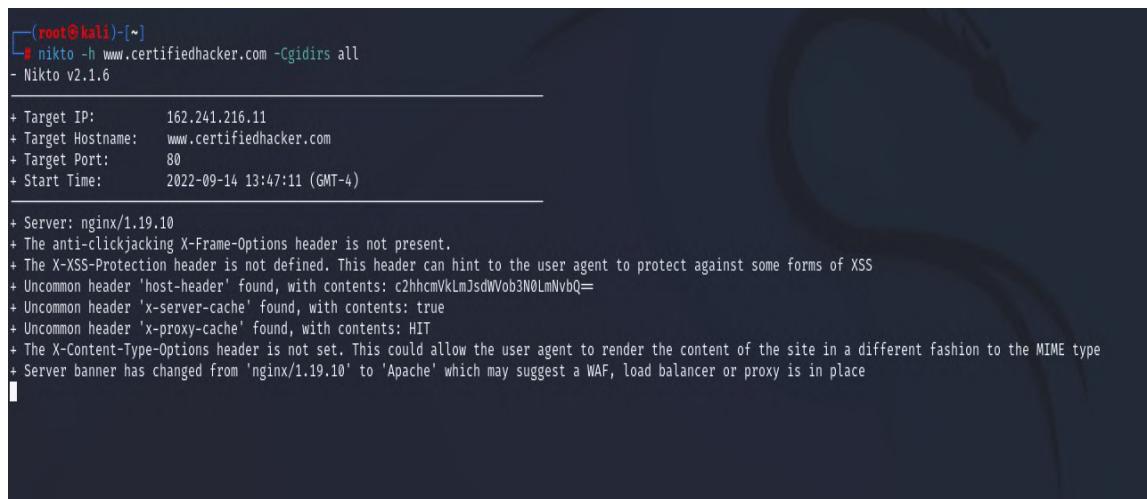
```
(root㉿kali)-[~]
# nikto -h www.zoho.com -Tuning x
- Nikto v2.1.6

+ 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: ZS5
+ 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: c2hhcmVlLmJsdWVob3N0LmNvbQ==
+ 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
```

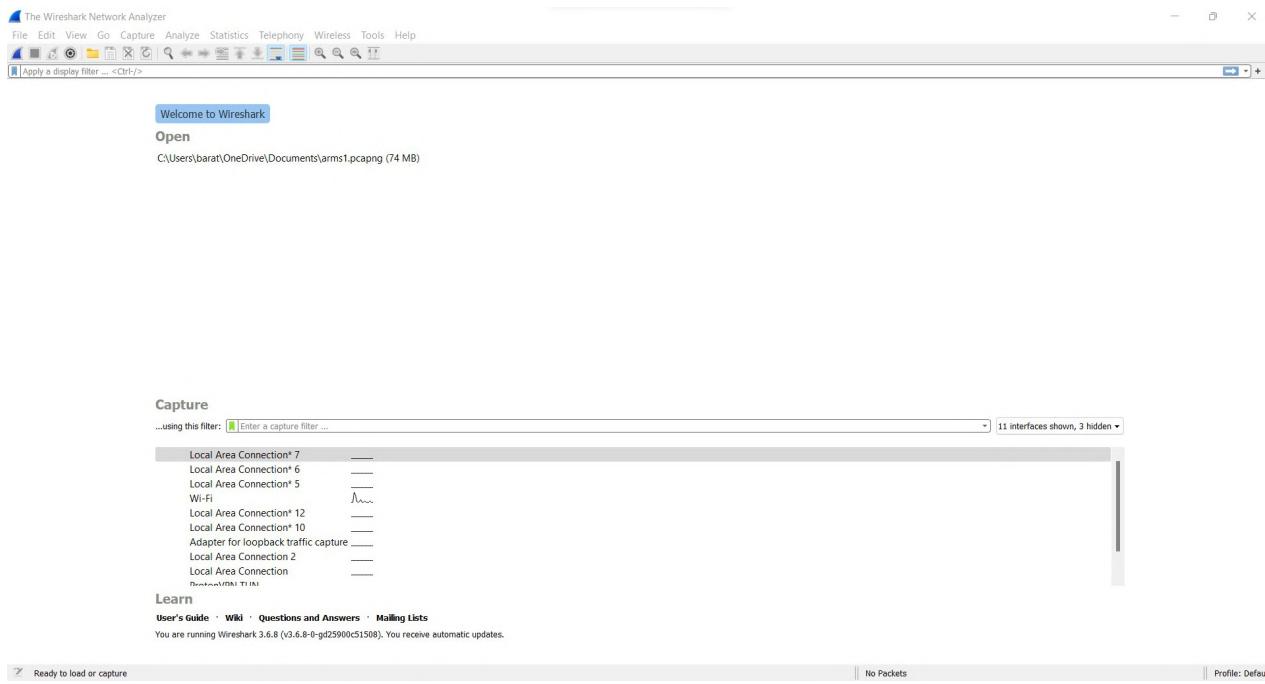
Step 5. Nikto will scan the webserver as it looks vulnerable CGI directories. It scans the webserver and list out the directories

EXCERSISE 8: WireShark sniffer

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

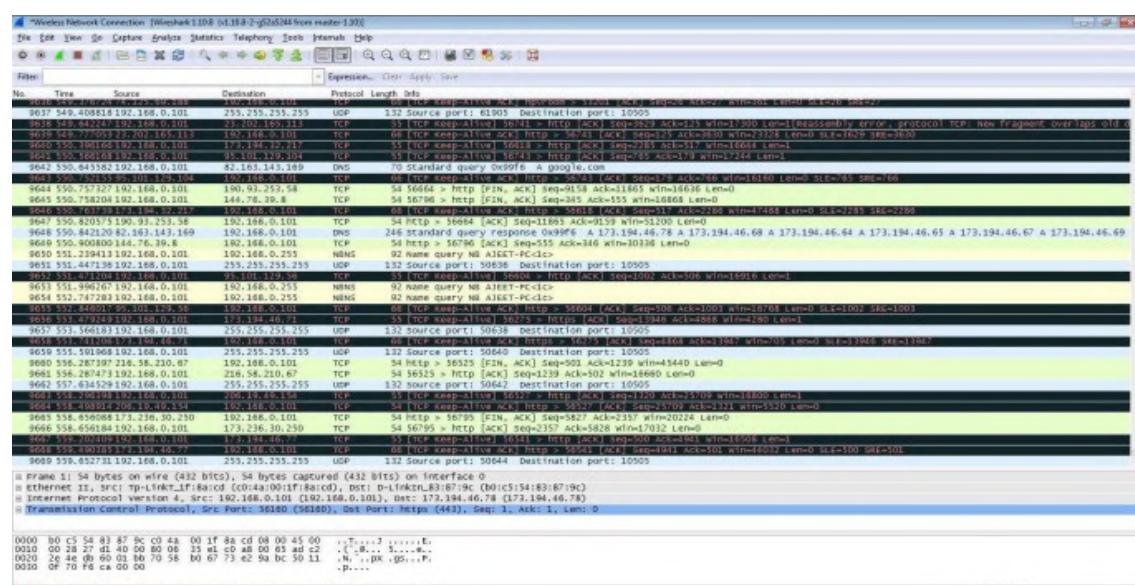
Procedure:

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



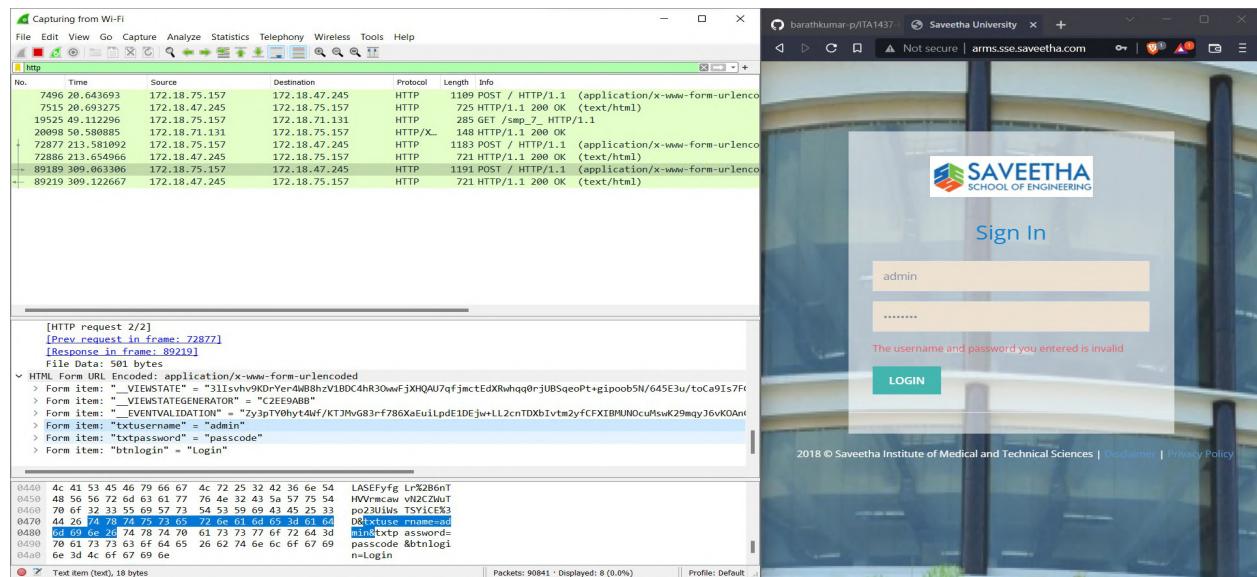
Step 4: Open a website in a new window and enter the user id and password. Register ifneeded.

Step 5: Enter the credentials and then sign inStep

6: The wireshark tool will keep recording the packets.

Step 7: Select filter as http to make the search easier and click on apply.

Step 9: Now stop the tool to stop recording



Step 10: Find the post methods for username and password

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

OUTPUT

```
Value: V6K+PG68BcPTlwearffzzA5idogxmIQMZDbv1Xu/1RHFxFxeAPGRq+aKFoAAWB LGTsFon7qh2vYXMr5cvshUGrXsWpzFx6RxkiwBrX21rvg=
Form item: "__VIEWSTATEGENERATOR" = "C2EE9ABB"
Key: __VIEWSTATEGENERATOR
Value: C2EE9ABB
Form item: "__EVENTVALIDATION" = "uuz25ZjqiA3JGVsqclf0g6cdRw5t1kAFWuk9M0vpgy/qStf6R0ley+fPBp/t0fwE02yztQaqByYtiGJI+z0IXeH3imoQxX4VyxZ3KfhPY+N01SaTwDA
Key: __EVENTVALIDATION
Value: uuz25ZjqiA3JGVsqclf0g6cdRw5t1kAFWuk9M0vpgy/qStf6R0ley+fPBp/t0fwE02yztQaqByYtiGJI+z0IXeH3imoQxX4VyxZ3KfhPY+N01SaTwDA/Ja6sYK8C4qyBj8VPC4zAsGK
Form item: "txtusername" = "192121022"
Key: txtusername
Value: 192121022
Form item: "txtpassword" = "muthu@20"
Key: txtpassword
Value: muthu@20
Form item: "btnlogin" = "Login"
Key: btnlogin
Value: Login

Frame (489 bytes) | Reassembled TCP (1026 bytes)|
```

Caption

RESULT :

BY using Wireshark password has been detected successfully

EX.NO: 10

DATE: BATCH FILE EXECUTION

AIM:

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

To create a Windows batch 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.

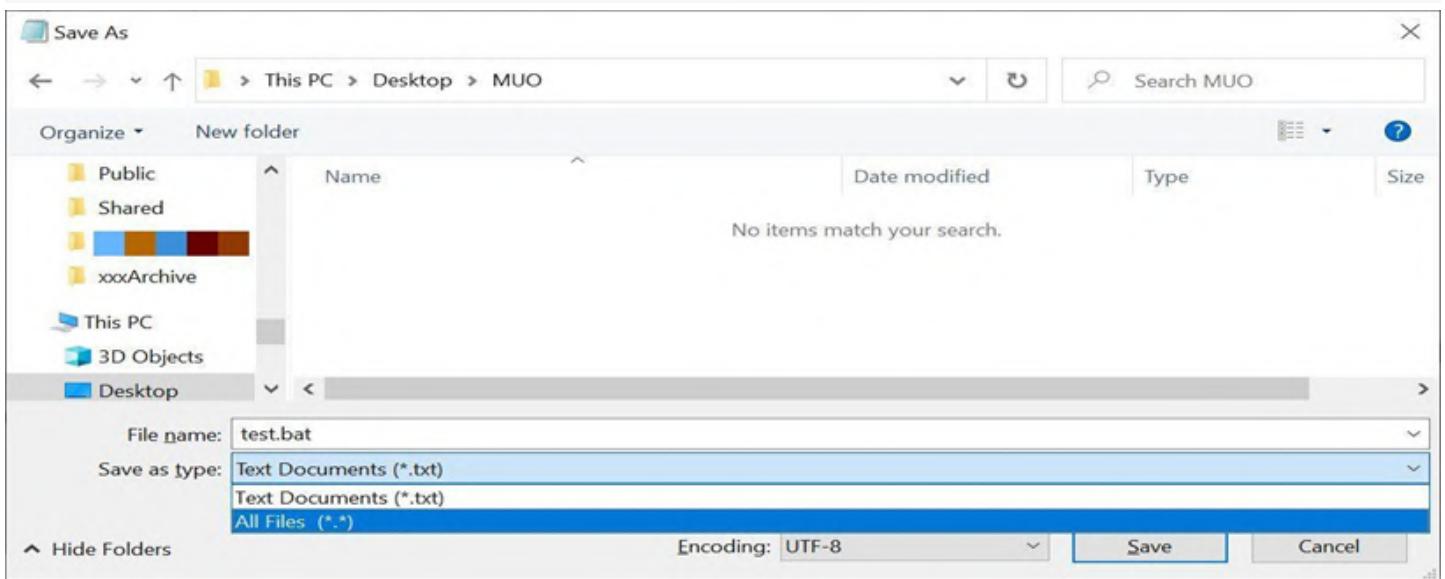
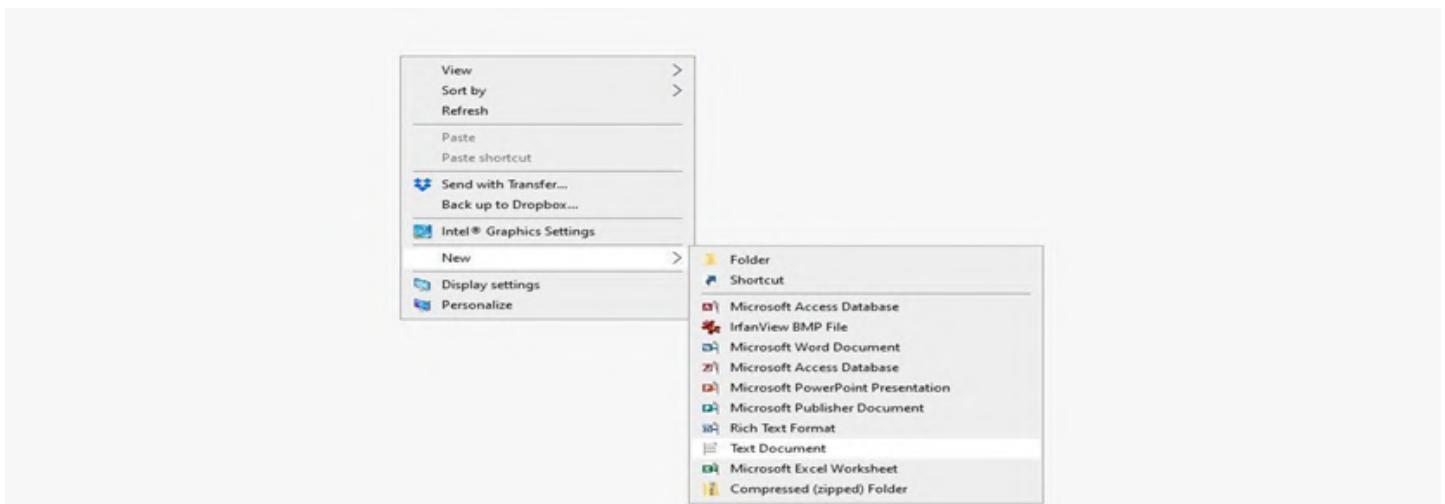
OUTPUT:

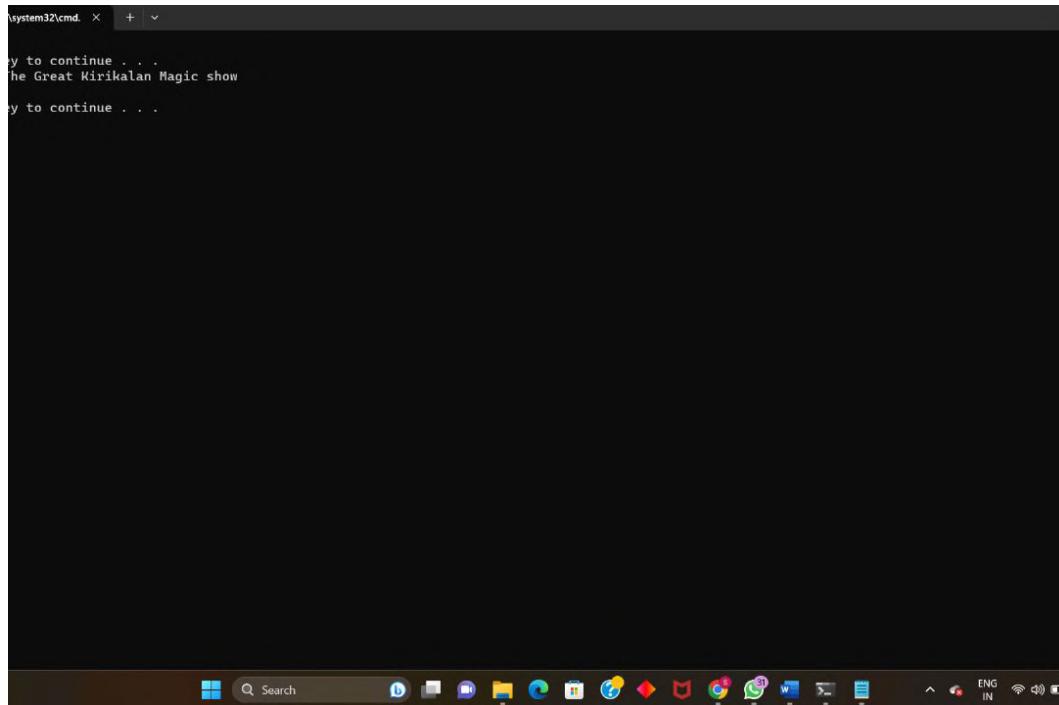
The image shows two windows demonstrating the execution of a batch script. The top window is a Notepad application titled 'test.bat - Notepad'. It contains the following script:

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

The bottom window is a command-line interface (CMD) window. It displays the output of the script:

```
This is your first batch script.
Welcome to batch scripting.
Press any key to continue . . .
```





Caption

RESULT:

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

Ex. No.10 – 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 <username> -p <password> -U <ipaddress> 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 <ipaddress> -a

kali-linux-2022.3-vmware-amd64 - VMware Workstation 16 Player (Non-commercial use only)

Player | [] [] [] [] [] [] []

File Actions Edit View Help

[root@kali)-~]

[#] enum4linux -a 172.20.10.5

Starting enum4linux v0.9.1 (http://labs.portcullis.co.uk/application/enum4linux/) on Wed Sep 14 03:48:35 2022

(Target Information)

Target 172.20.10.5
RID Range 500-558,1000-1050
Username ''
Password ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none

(Enumerating Workgroup/Domain on 172.20.10.5)

[E] Can't find workgroup/domain

(Nbtstat Information for 172.20.10.5)

Looking up status of 172.20.10.5
No reply from 172.20.10.5

(Session Check on 172.20.10.5)

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

(Getting domain SID for 172.20.10.5)

do_cmd: Could not initialise lsarpc. Error was NT_STATUS_ACCESS_DENIED

[+] Can't determine if host is part of domain or part of a workgroup

(OS information on 172.20.10.5)

[E] Can't get OS info with smbclient

[+] Got OS info for 172.20.10.5 from srvinfo:
do_cmd: Could not initialise svrsvc. Error was NT_STATUS_ACCESS_DENIED

(Users on 172.20.10.5)

33°C
Partly sunny

3:56 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

root@kali: ~
[+] Attempting to map shares on 172.20.10.5
[!] 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.)

[+] Failed to get password policy with rpcclient

[+] 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 | X
File Actions Edit View Help
root@kali: ~

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

[E] Failed to get password policy with rpcclient

( Groups on 172.20.10.5 )

[*] Getting builtin groups:
[*] Getting builtin group memberships:
[*] Getting local groups:
[*] Getting local group memberships:
[*] Getting domain groups:
[*] Getting domain group memberships:
( Users on 172.20.10.5 via RID cycling (RIDs: 500-550,1000-1050) )

[E] Couldn't get SID: NT_STATUS_ACCESS_DENIED. RID cycling not possible.

( Getting printer info for 172.20.10.5 )
do_cmd: Could not initialise spoolss. Error was NT_STATUS_ACCESS_DENIED

enum4linux complete on Wed Sep 14 03:48:58 2022

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

RESULT:

sucessfully Enumerated information from windows and Samba Host Using Enum4linux