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

Flag	**Use**	**Example**
-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

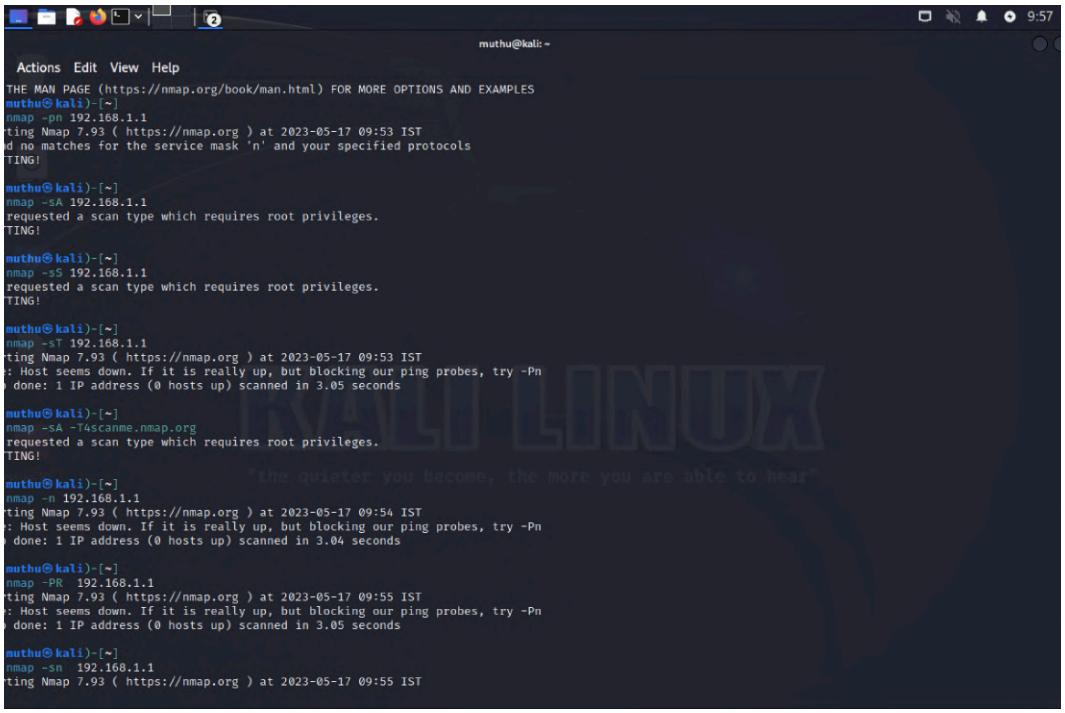
Flag	Use	Example
-sV	detect the version of services running	nmap -sV 192.168.1.1
-A	aggressive scan	nmap -A 192.168.1.1
-O	detect operating system of the target	nmap -O 192.168.1.1

Step 6:-

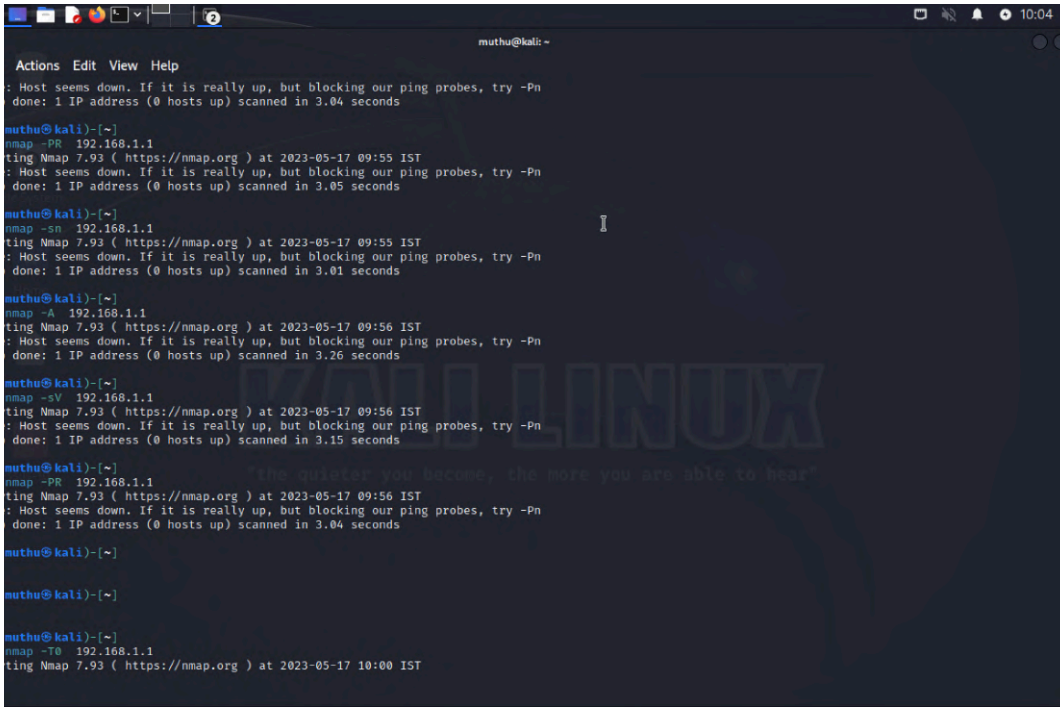
Timing and Performance

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:



Caption



Caption

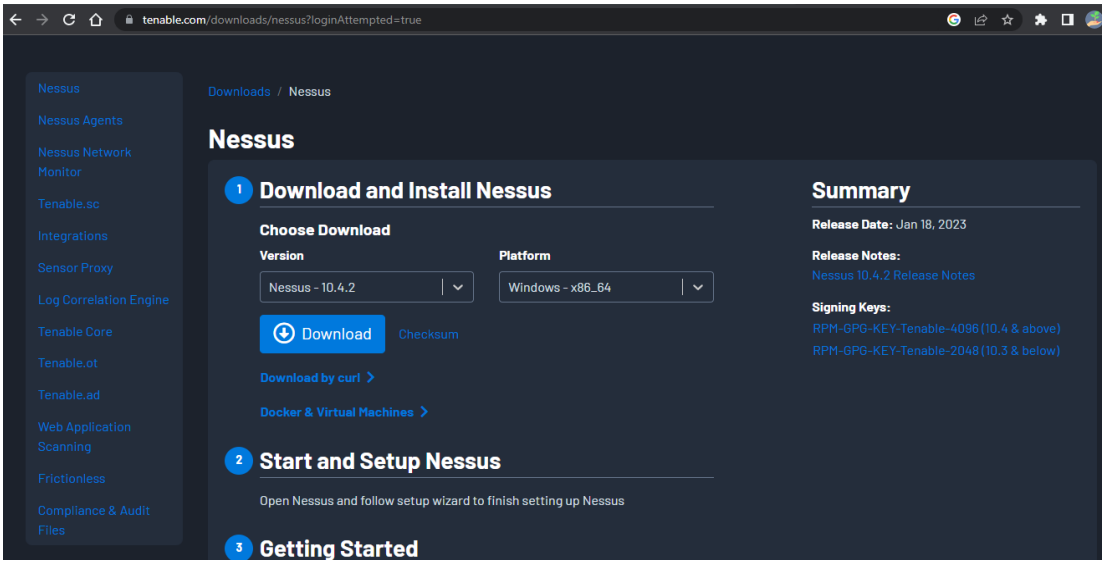
Result:

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

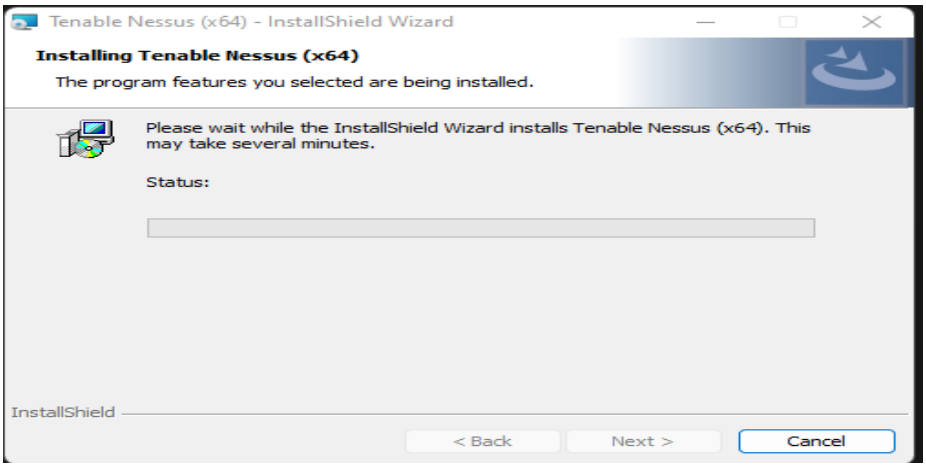
Exercise No 2: Vulnerability Access Scan Using Nessus

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

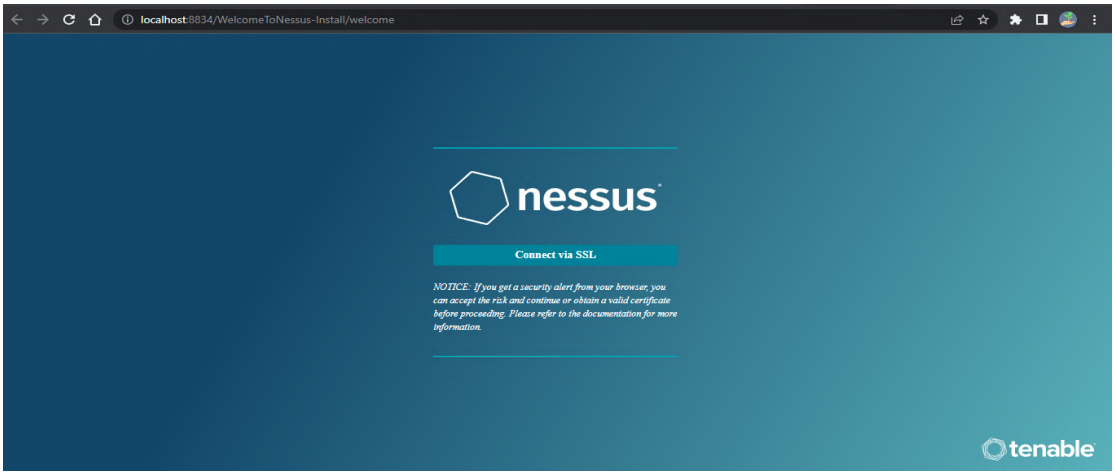
Step 1:- https://www.tenable.com/downloads/nessus?loginAttempted=true



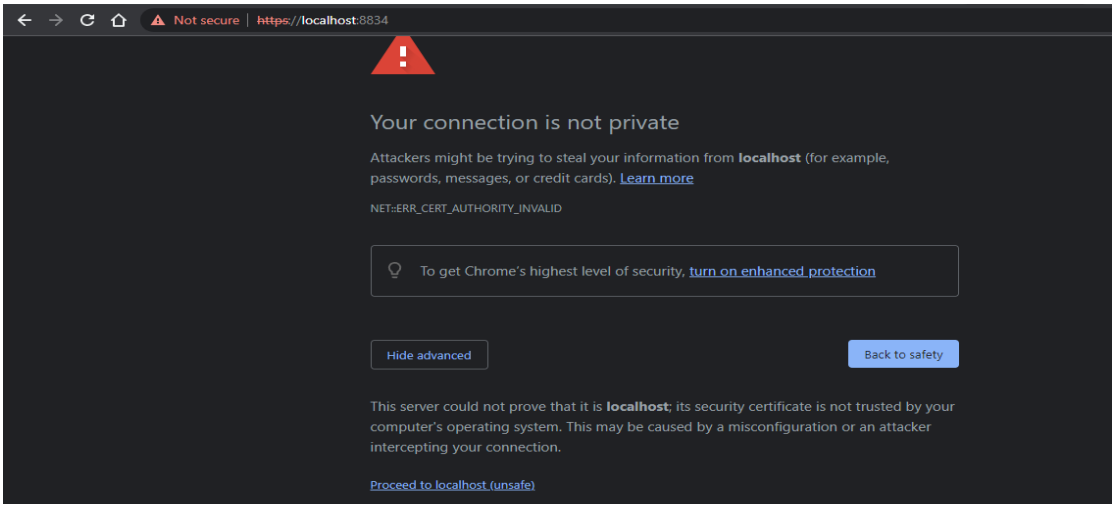
Step 2: Choose your OS and download , install



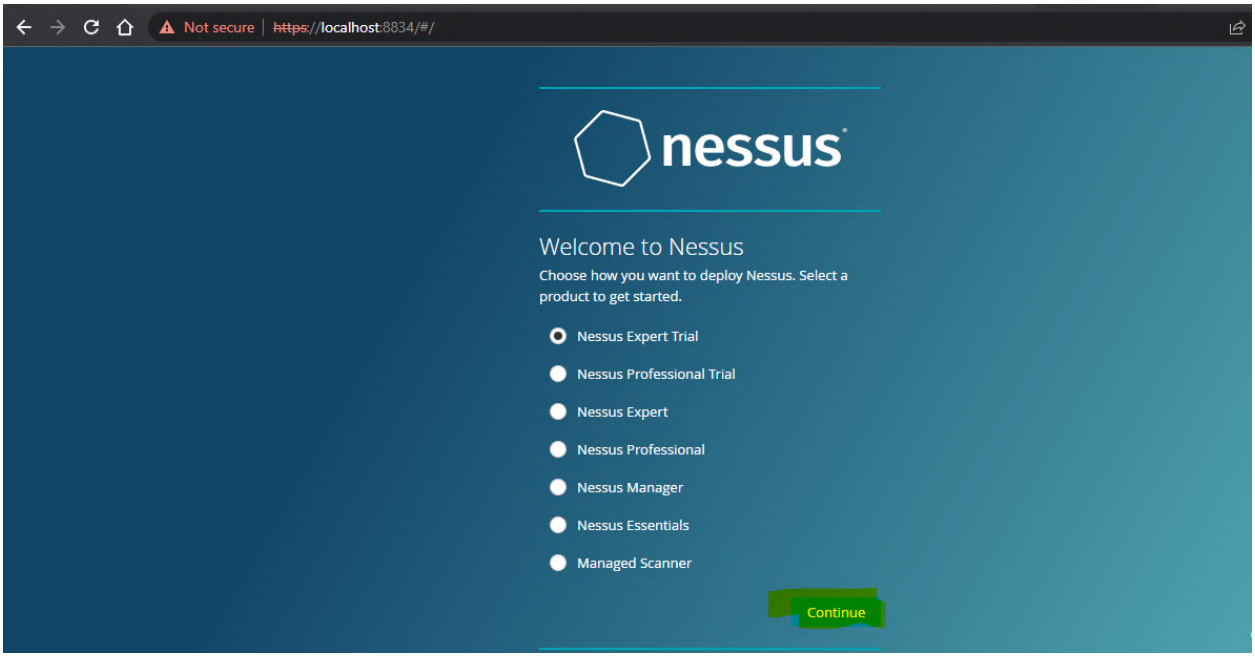
Step 3: Once installation is completed it will open in default browser



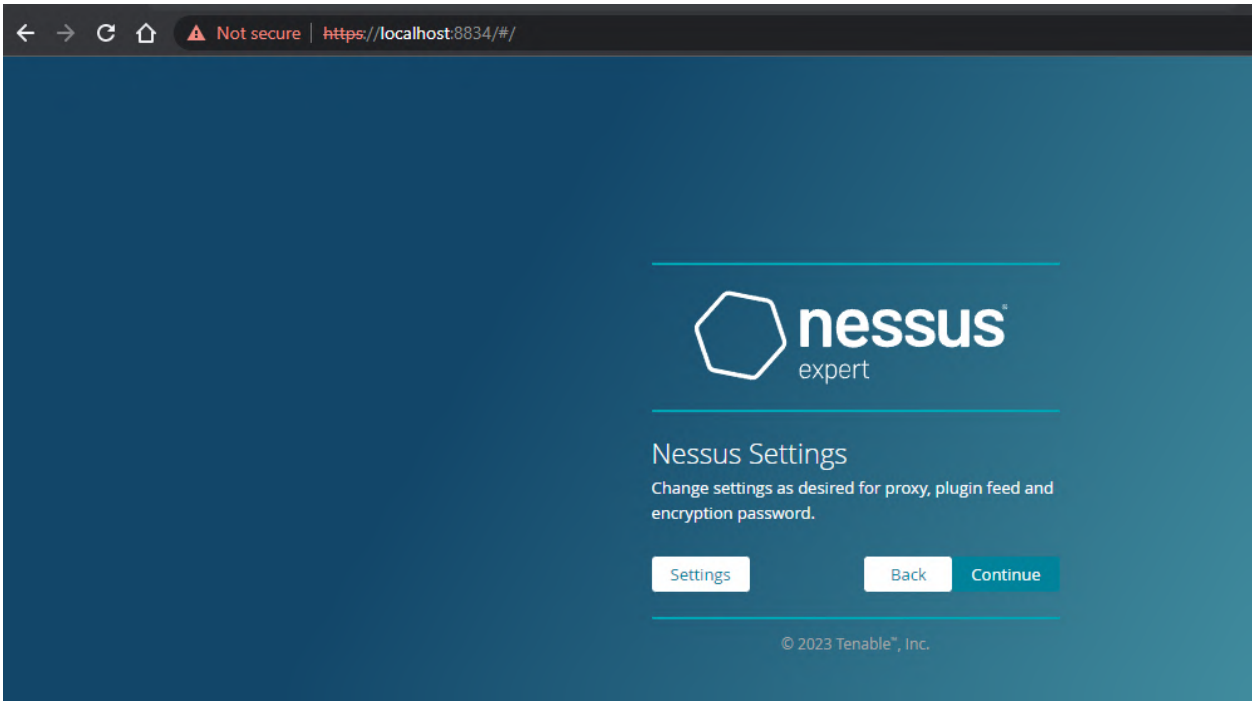
Step 5:- (click on the proceed to local host)



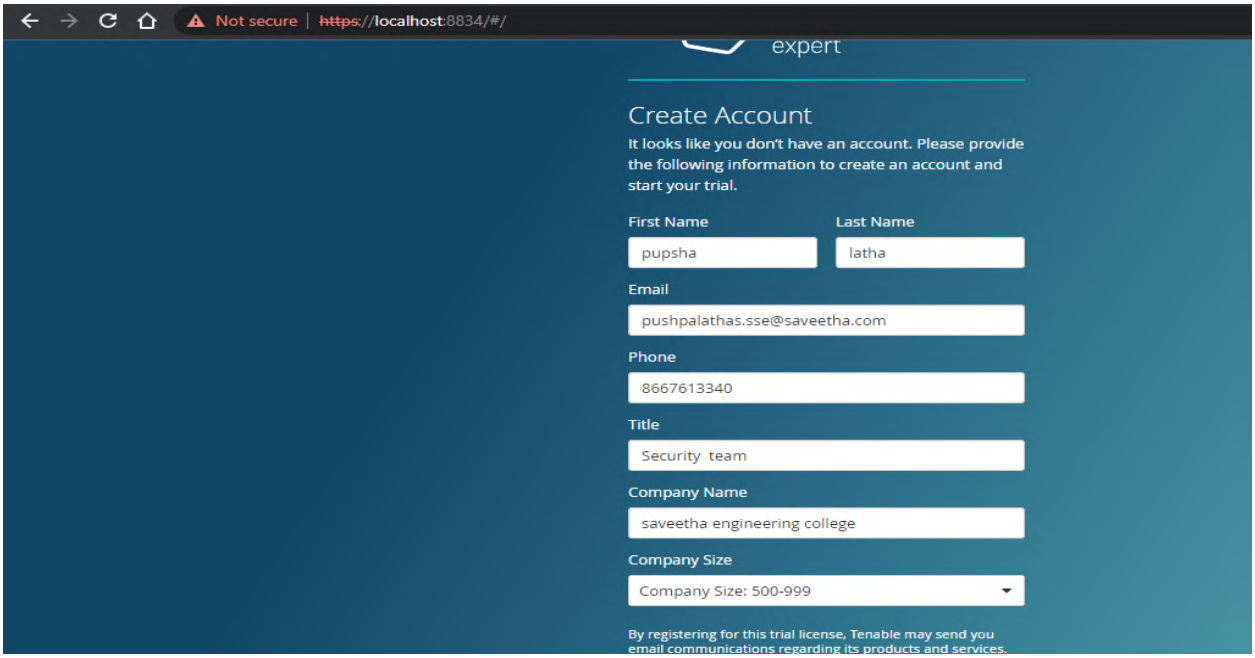
Step 6:- Please choose the Nessus Expert



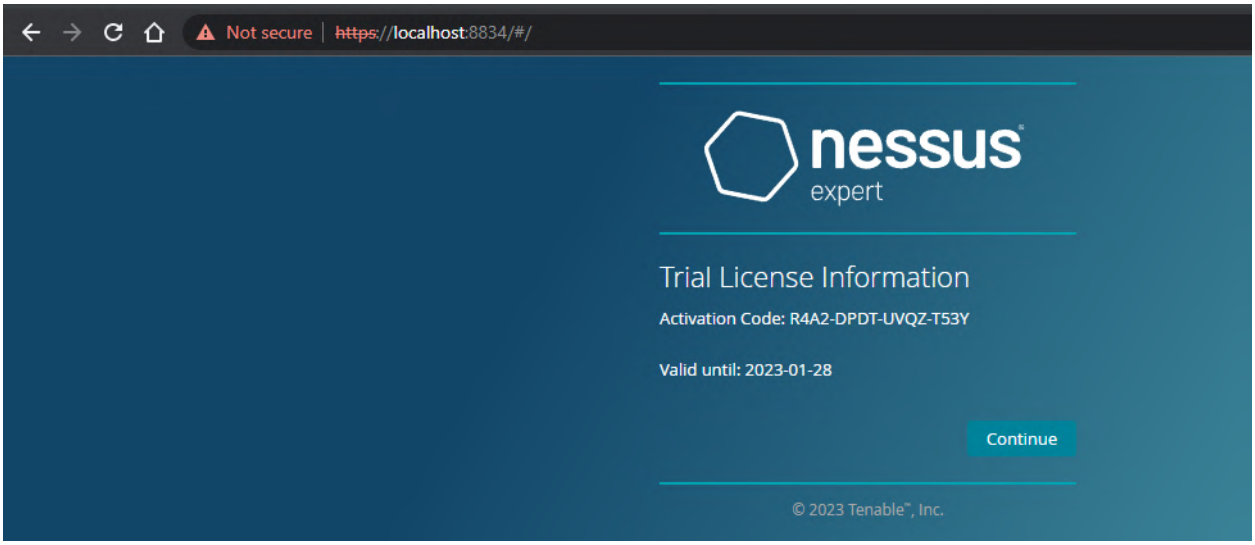
Step 7: Click on continue



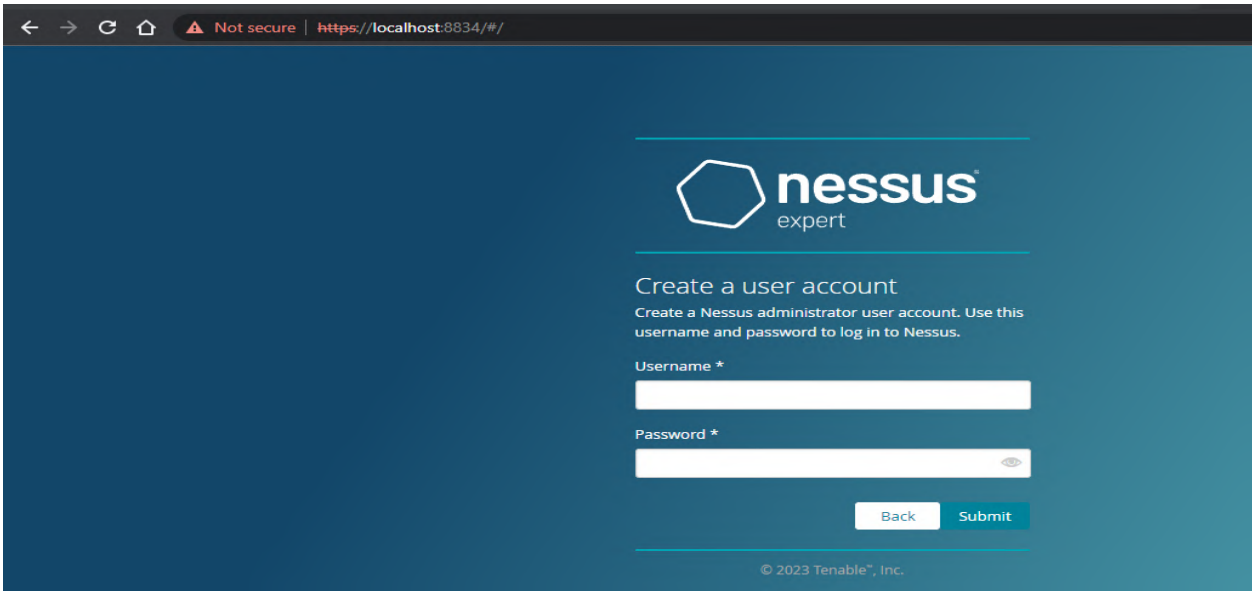
Step 8:- Register with your organizational email id



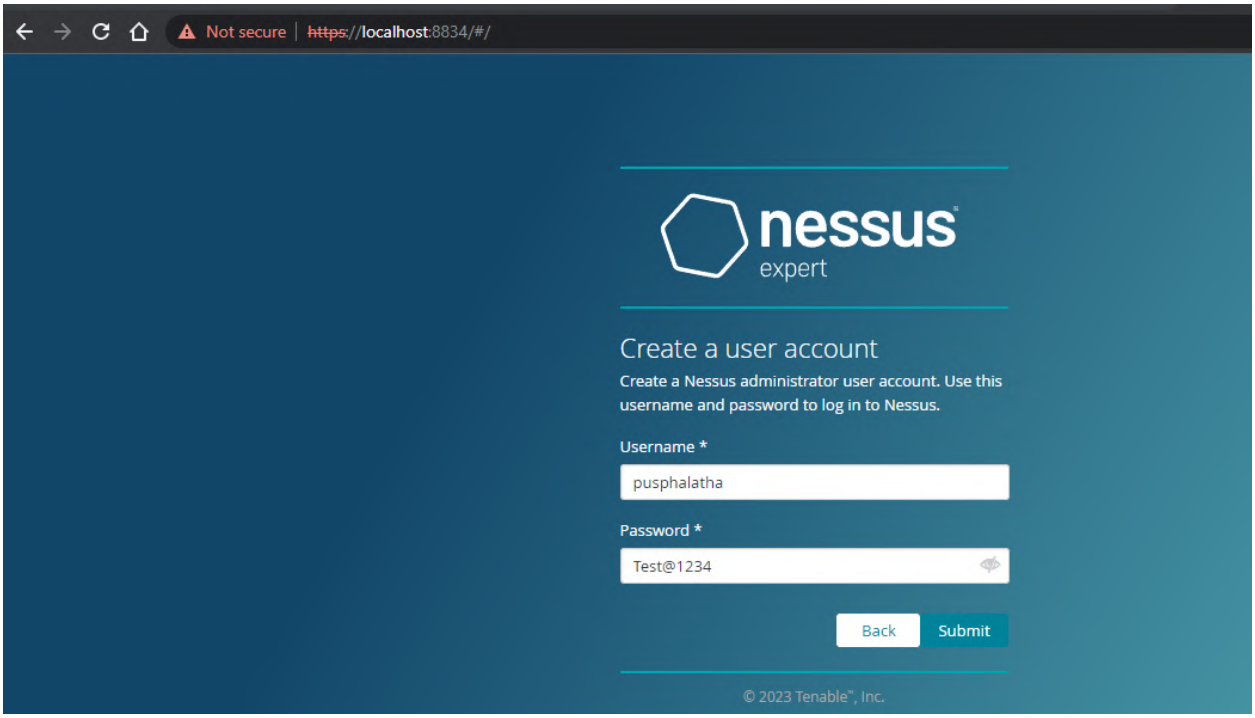
Step 9:- please note down the activation key



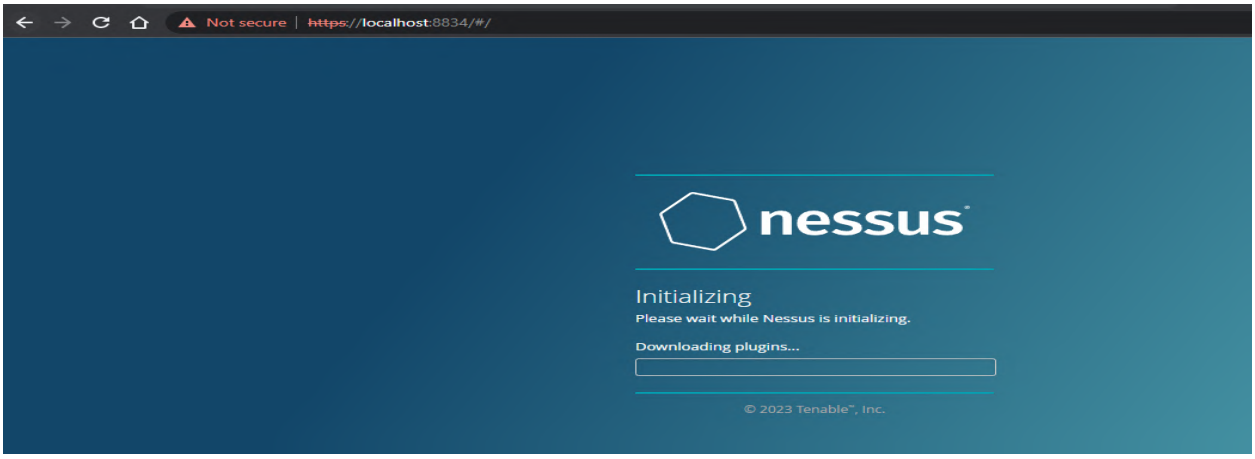
Step 10:- set up your username & password



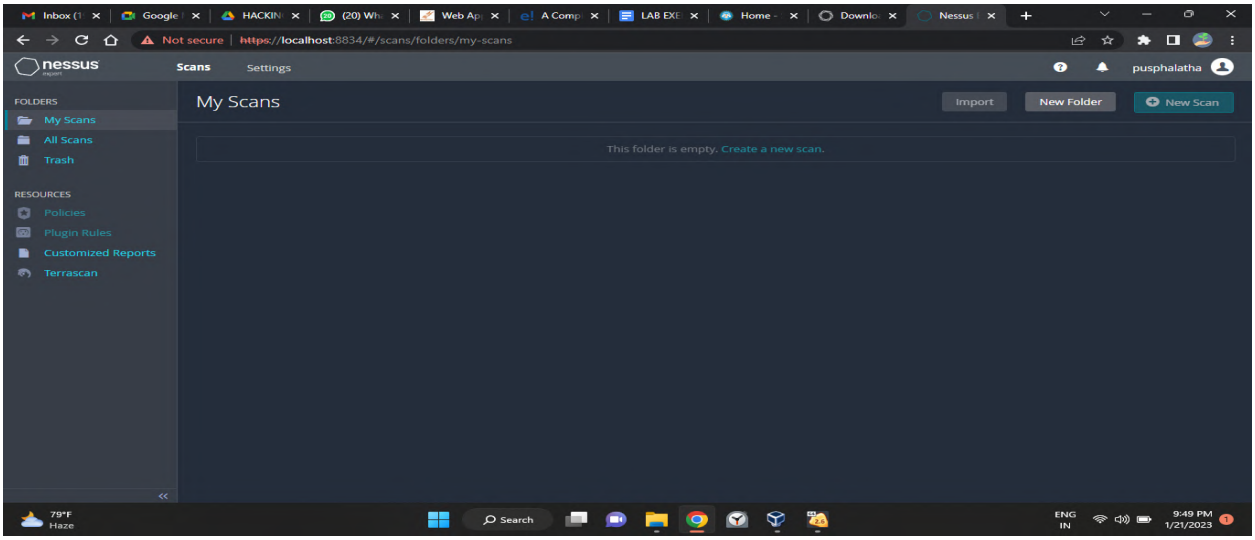
Step 11:-Type username and password



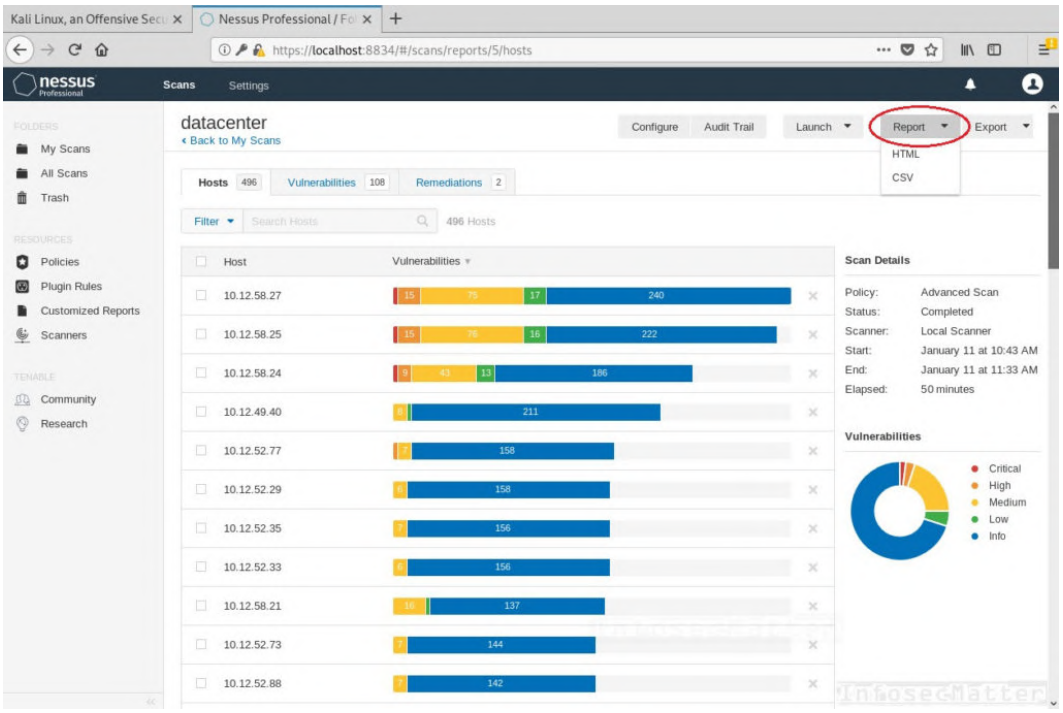
Step 12:- Please wait until download is completed



Step 13: Select My Scans



OUTPUT



Caption

RESULT : SUCCESSFULLY SCANED THE PORTS

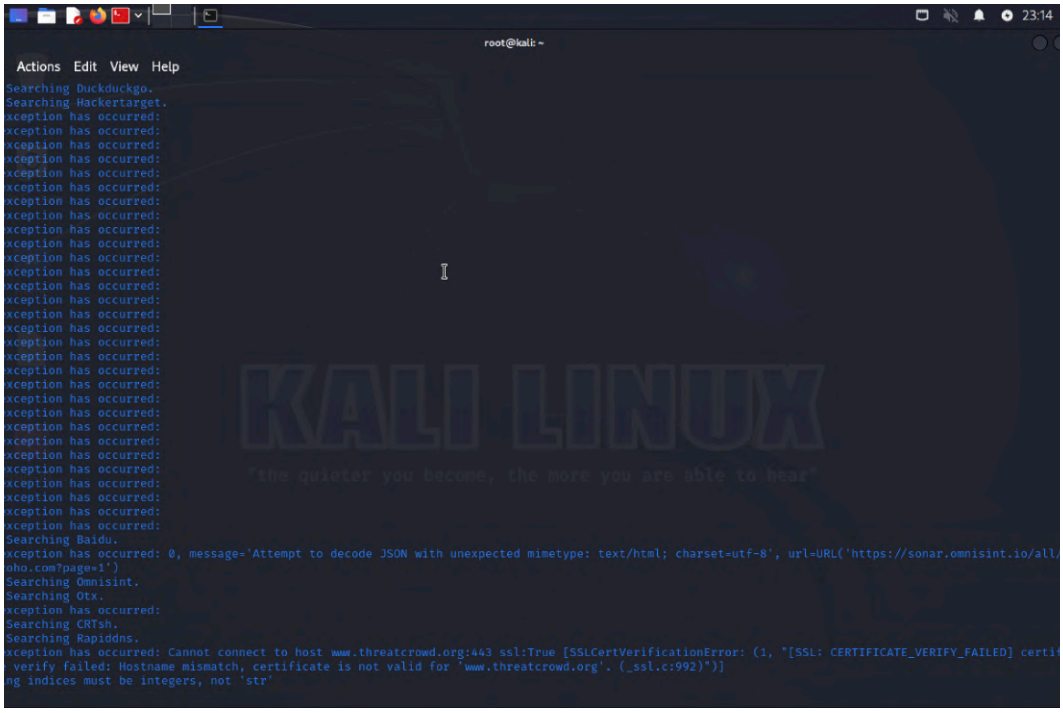
Exercise No 3: Information gathering using theHarvester

Aim: To demonstrate information gathering using theHarvester
Procedure:

STEP 1: Open Terminal in the kali linux

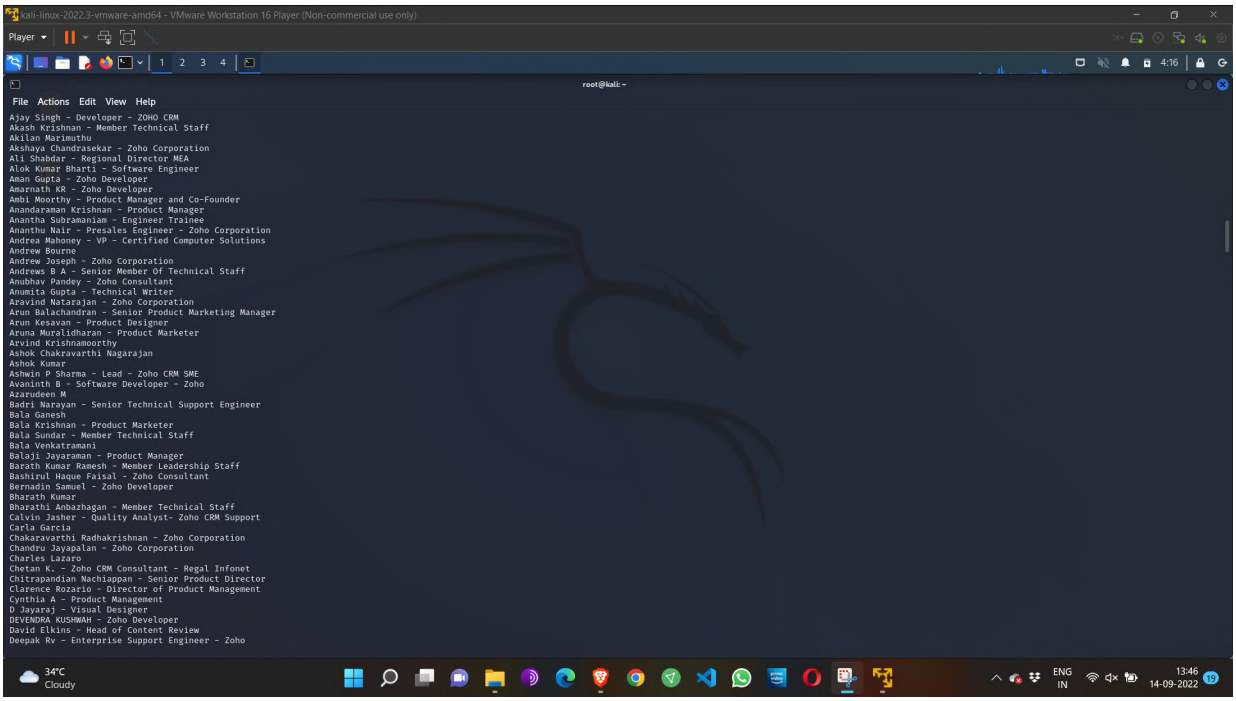
```
-d [url] will be the remote site from which you wants to fetch


-l will limit the search for specified number.


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

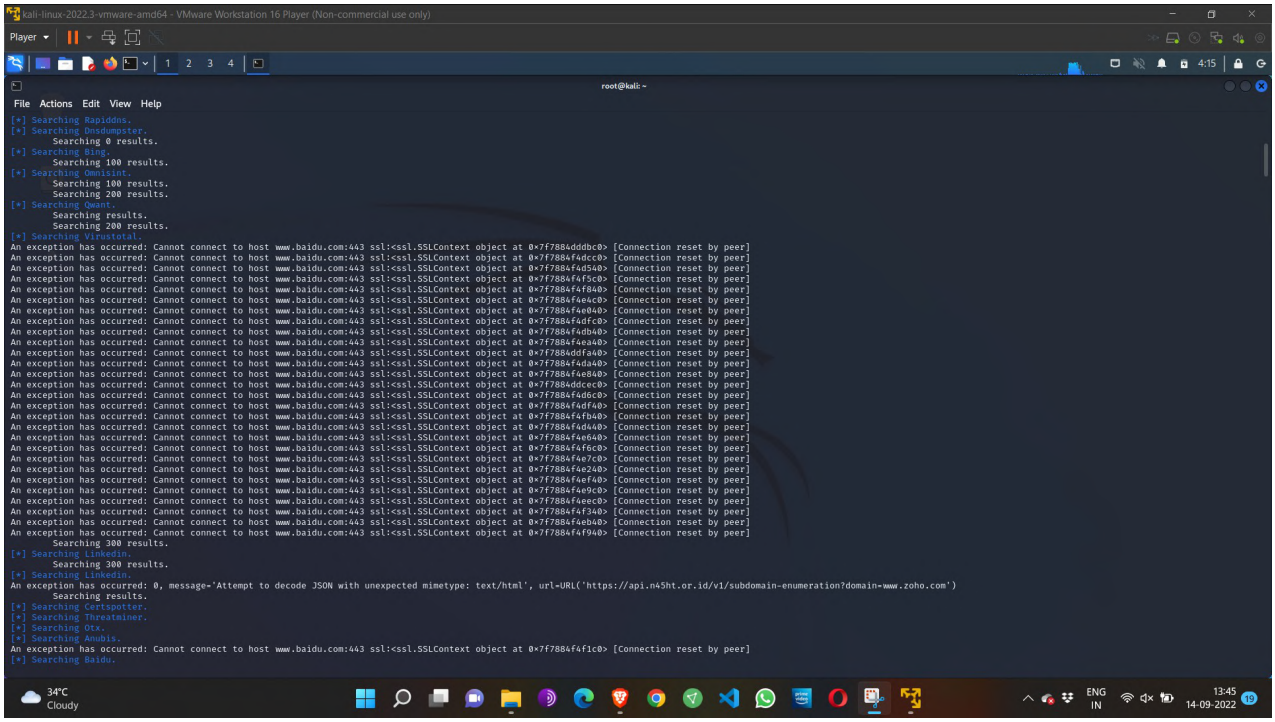
STEP 2: Run the following command
Command: theHarvester -d www.zoho.com -l 300 -b all

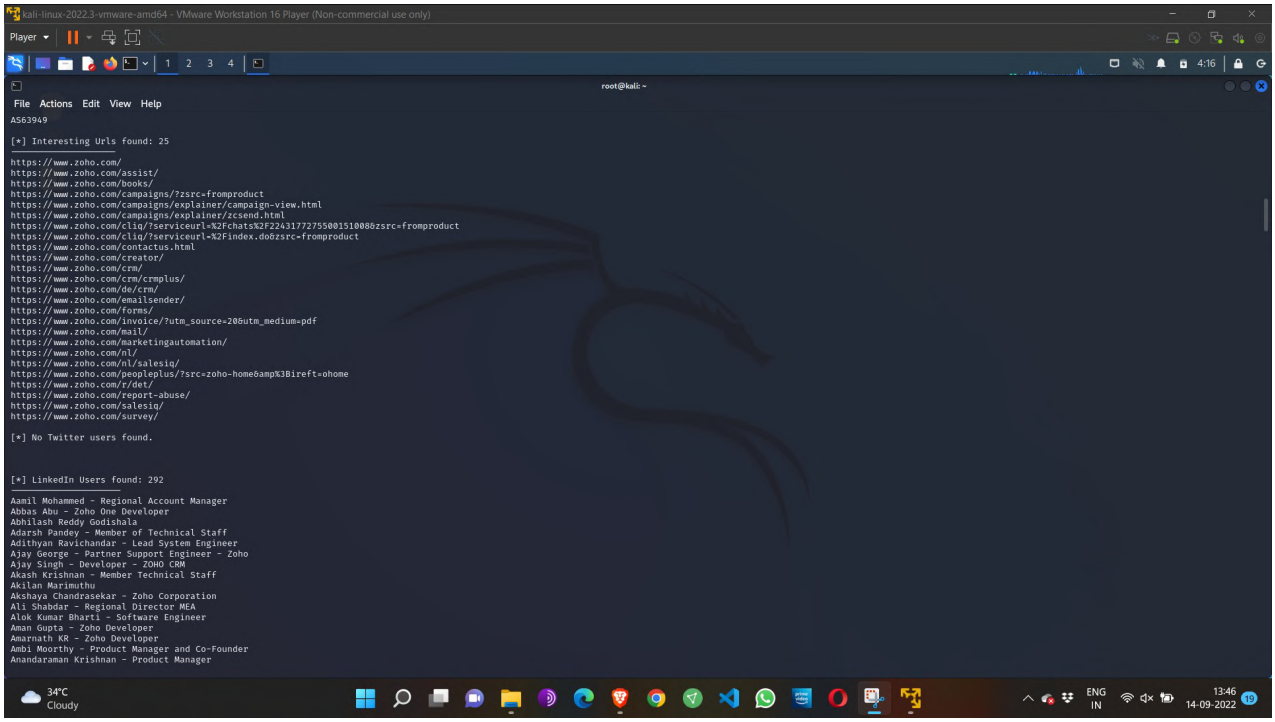


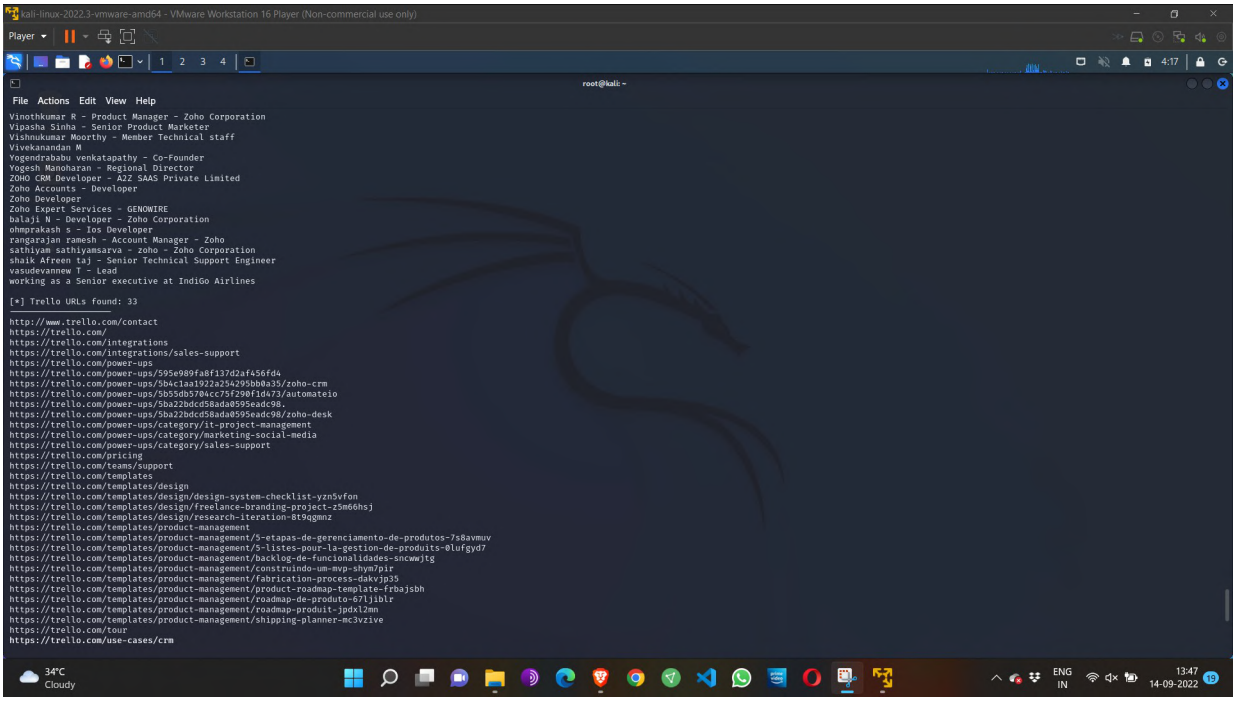
Caption

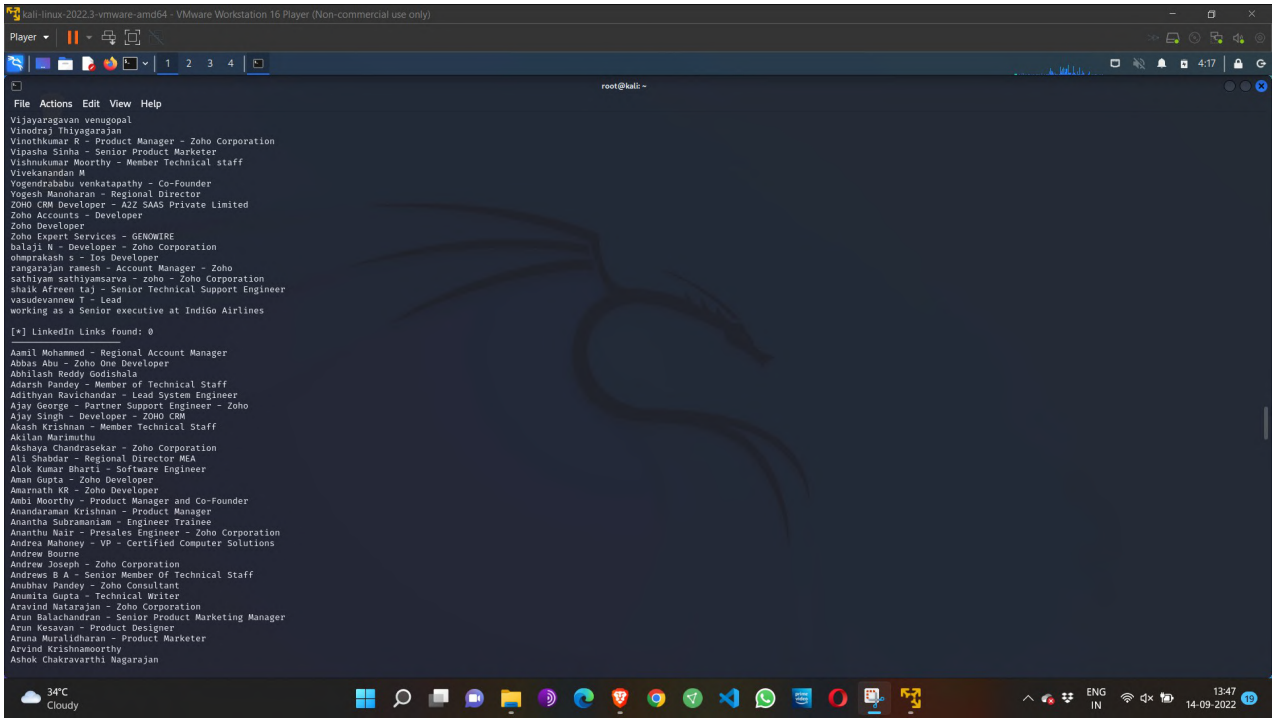
Caption

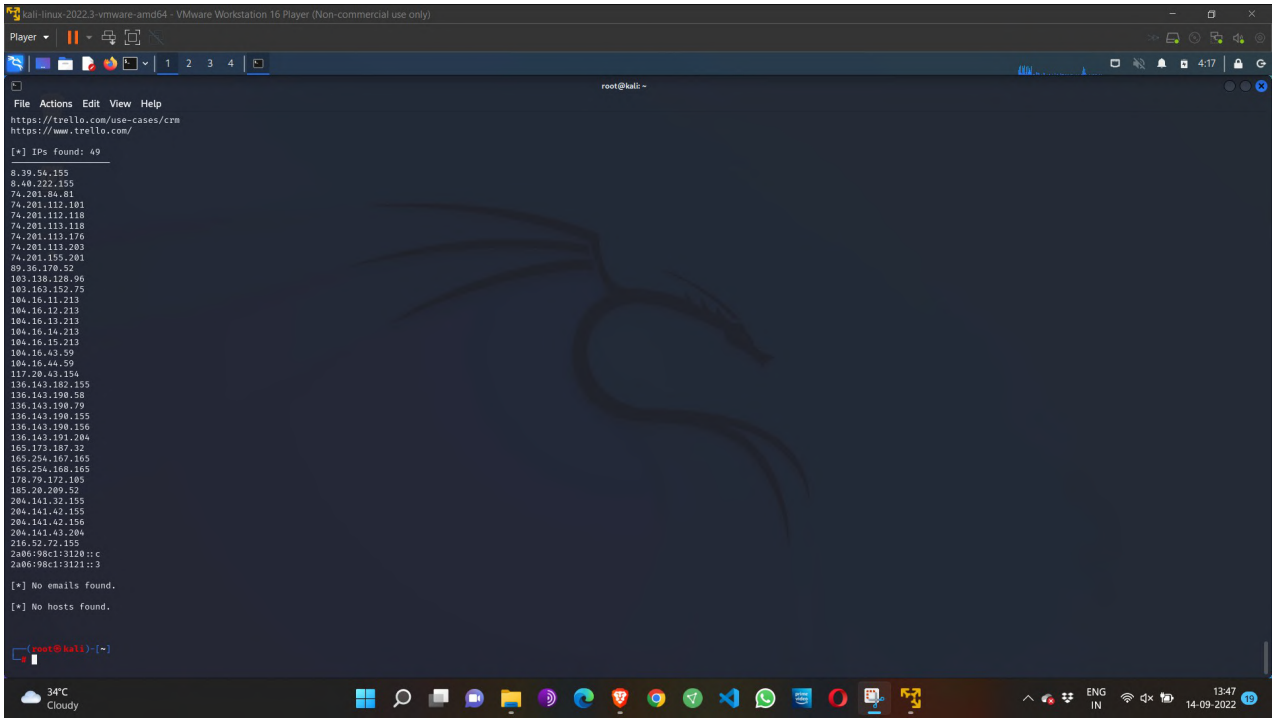

kali-linux-2022.3-vmware-amd64 - VMware Workstation 16 Player (Non-commercial use only)
Player
root@kali: ~
File Actions Edit View Help
Ajay Singh - Developer - ZOHO CRM
Akash Krishnan - Member Technical Staff
Akilan Marimuthu
Akshaya Chandrasekar - Zoho Corporation
Ali Shabdar - Regional Director MEA
Alok Kumar Bharti - Software Engineer
Aman Gupta - Zoho Developer
Amarnath KR - Zoho Developer
Ambi Moorthy - Product Manager and Co-Founder
Anandaraman Krishnan - Product Manager
Anantha Subramaniam - Engineer Trainee
Ananthu Nair - Presales Engineer - Zoho Corporation
Andrea Mahoney - VP - Certified Computer Solutions
Andrew Bourne
Andrew Joseph - Zoho Corporation
Andrews B A - Senior Member Of Technical Staff
Anubhav Pandey - Zoho Consultant
Anumita Gupta - Technical Writer
Aravind Natarajan - Zoho Corporation
Arun Balachandran - Senior Product Marketing Manager
Arun Kesavan - Product Designer
Aruna Muralidharan - Product Marketer
Arvind Krishnamoorthy
Ashok Chakravarthi Nagarajan
Ashok Kumar
Ashwin P Sharma - Lead - Zoho CRM SME
Avanith B - Software Developer - Zoho
Azarudeen M
Badri Narayan - Senior Technical Support Engineer
Bala Ganesh
Bala Krishnan - Product Marketer
Bala Sundar - Member Technical Staff
Bala Venkatramani
Balaji Jayaraman - Product Manager
Barath Kumar Ramesh - Member Leadership Staff
Bashirul Haque Faisal - Zoho Consultant
Bernadin Samuel - Zoho Developer
Bharath Kumar
Bharathi Anbazhagan - Member Technical Staff
Calvin Jasher - Quality Analyst- Zoho CRM Support
Carla Garcia
Chakaravarthi Radhakrishnan - Zoho Corporation
Chandru Jayapalan - Zoho Corporation
Charles Lazaro
Chetan K. - Zoho CRM Consultant - Regal Infonet
Chitrapandian Nachiappan - Senior Product Director
Clarence Rozario - Director of Product Management
Cynthia A - Product Management
D Jayaraj - Visual Designer
DEVENDRA KUSHWAH - 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
root@kali: ~
File Actions Edit View Help
[*] Searching Rapiddns.
[*] Searching Dnsdumpster.
Searching 0 results.
[*] Searching Bing.
Searching 100 results.
[*] Searching Omnisint.
Searching 100 results.
Searching 200 results.
[*] Searching Qwant.
Searching results.
Searching 200 results.
[*] Searching Virustotal.
An exception has occurred: Cannot connect to host www.baidu.com:443 ssl:<ssl.SSLContext object at 0×7f7884dddbc0> [Connection reset by peer]
An exception has occurred: Cannot connect to host www.baidu.com:443 ssl:<ssl.SSLContext object at 0×7f7884f4dcc0> [Connection reset by peer]
An exception has occurred: Cannot connect to host www.baidu.com:443 ssl:<ssl.SSLContext object at 0×7f7884f4d540> [Connection reset by peer]
An exception has occurred: Cannot connect to host www.baidu.com:443 ssl:<ssl.SSLContext object at 0×7f7884f4f5c0> [Connection reset by peer]
An exception has occurred: Cannot connect to host www.baidu.com:443 ssl:<ssl.SSLContext object at 0×7f7884f4f840> [Connection reset by peer]
An exception has occurred: Cannot connect to host www.baidu.com:443 ssl:<ssl.SSLContext object at 0×7f7884f4e4c0> [Connection reset by peer]
An exception has occurred: Cannot connect to host www.baidu.com:443 ssl:<ssl.SSLContext object at 0×7f7884f4e940> [Connection reset by peer]
An exception has occurred: Cannot connect to host www.baidu.com:443 ssl:<ssl.SSLContext object at 0×7f7884f4dfc0> [Connection reset by peer]
An exception has occurred: Cannot connect to host www.baidu.com:443 ssl:<ssl.SSLContext object at 0×7f7884f4db40> [Connection reset by peer]
An exception has occurred: Cannot connect to host www.baidu.com:443 ssl:<ssl.SSLContext object at 0×7f7884f4eaa0> [Connection reset by peer]
An exception has occurred: Cannot connect to host www.baidu.com:443 ssl:<ssl.SSLContext object at 0×7f7884ddfa40> [Connection reset by peer]
An exception has occurred: Cannot connect to host www.baidu.com:443 ssl:<ssl.SSLContext object at 0×7f7884f4da40> [Connection reset by peer]
An exception has occurred: Cannot connect to host www.baidu.com:443 ssl:<ssl.SSLContext object at 0×7f7884f4e840> [Connection reset by peer]
An exception has occurred: Cannot connect to host www.baidu.com:443 ssl:<ssl.SSLContext object at 0×7f7884ddcec0> [Connection reset by peer]
An exception has occurred: Cannot connect to host www.baidu.com:443 ssl:<ssl.SSLContext object at 0×7f7884f4d6c0> [Connection reset by peer]
An exception has occurred: Cannot connect to host www.baidu.com:443 ssl:<ssl.SSLContext object at 0×7f7884f4df40> [Connection reset by peer]
An exception has occurred: Cannot connect to host www.baidu.com:443 ssl:<ssl.SSLContext object at 0×7f7884f4fb40> [Connection reset by peer]
An exception has occurred: Cannot connect to host www.baidu.com:443 ssl:<ssl.SSLContext object at 0×7f7884f4d440> [Connection reset by peer]
An exception has occurred: Cannot connect to host www.baidu.com:443 ssl:<ssl.SSLContext object at 0×7f7884f4e640> [Connection reset by peer]
An exception has occurred: Cannot connect to host www.baidu.com:443 ssl:<ssl.SSLContext object at 0×7f7884f4f6c0> [Connection reset by peer]
An exception has occurred: Cannot connect to host www.baidu.com:443 ssl:<ssl.SSLContext object at 0×7f7884f4e7c0> [Connection reset by peer]
An exception has occurred: Cannot connect to host www.baidu.com:443 ssl:<ssl.SSLContext object at 0×7f7884f4e240> [Connection reset by peer]
An exception has occurred: Cannot connect to host www.baidu.com:443 ssl:<ssl.SSLContext object at 0×7f7884f4ef40> [Connection reset by peer]
An exception has occurred: Cannot connect to host www.baidu.com:443 ssl:<ssl.SSLContext object at 0×7f7884f4e9c0> [Connection reset by peer]
An exception has occurred: Cannot connect to host www.baidu.com:443 ssl:<ssl.SSLContext object at 0×7f7884f4eec0> [Connection reset by peer]
An exception has occurred: Cannot connect to host www.baidu.com:443 ssl:<ssl.SSLContext object at 0×7f7884f4f340> [Connection reset by peer]
An exception has occurred: Cannot connect to host www.baidu.com:443 ssl:<ssl.SSLContext object at 0×7f7884f4eba0> [Connection reset by peer]
An exception has occurred: Cannot connect to host www.baidu.com:443 ssl:<ssl.SSLContext object at 0×7f7884f4f940> [Connection reset by peer]
Searching 300 results.
[*] Searching Linkedin.
Searching 300 results.
[*] Searching Linkedin.
An exception has occurred: 0, message='Attempt to decode JSON with unexpected mimetype: text/html', url=URL('https://api.n45ht.or.id/v1/subdomain-enumeration?domain=www.zoho.com')
Searching results.
[*] Searching Certspotter.
[*] Searching Threatminer.
[*] Searching Otx.
[*] Searching Anubis.
An exception has occurred: Cannot connect to host www.baidu.com:443 ssl:<ssl.SSLContext object at 0×7f7884f4f1c0> [Connection reset by peer]
[*] Searching Baidu.
34°C
Cloudy
ENG
IN
13:45
14-09-2022


kali-linux-2022.3-vmware-amd64 - VMware Workstation 16 Player (Non-commercial use only)
Player
root@kali: ~
File Actions Edit View Help
AS63949
[*] Interesting Urls found: 25
https://www.zoho.com/
https://www.zoho.com/assist/
https://www.zoho.com/books/
https://www.zoho.com/campaigns/?zsrc=fromproduct
https://www.zoho.com/campaigns/explainer/campaign-view.html
https://www.zoho.com/campaigns/explainer/zcsend.html
https://www.zoho.com/cliq/?serviceurl=%2Fchats%2F224317727550015108&zsrc=fromproduct
https://www.zoho.com/cliq/?serviceurl=%2Findex.do&zsrc=fromproduct
https://www.zoho.com/contactus.html
https://www.zoho.com/creator/
https://www.zoho.com/crm/
https://www.zoho.com/crm/crmplus/
https://www.zoho.com/de/crm/
https://www.zoho.com/emailsender/
https://www.zoho.com/forms/
https://www.zoho.com/invoice/?utm_source=20&utm_medium=pdf
https://www.zoho.com/mail/
https://www.zoho.com/marketingautomation/
https://www.zoho.com/nl/
https://www.zoho.com/nl/salesiq/
https://www.zoho.com/peopleplus/?src=zoho-home&amp%3Bireft=ohome
https://www.zoho.com/r/det/
https://www.zoho.com/report-abuse/
https://www.zoho.com/salesiq/
https://www.zoho.com/survey/
[*] No Twitter users found.
[*] LinkedIn Users found: 292
Aamil Mohammed - Regional Account Manager
Abbas Abu - Zoho One Developer
Abhilash Reddy Godishala
Adarsh Pandey - Member of Technical Staff
Adithyan Ravichandar - Lead System Engineer
Ajay George - Partner Support Engineer - Zoho
Ajay Singh - Developer - ZOHO CRM
Akash Krishnan - Member Technical Staff
Akilan Marimuthu
Akshaya Chandrasekar - Zoho Corporation
Ali Shabdar - Regional Director MEA
Alok Kumar Bharti - Software Engineer
Aman Gupta - Zoho Developer
Amarnath KR - Zoho Developer
Ambi Moorthy - Product Manager and Co-Founder
Anandaraman Krishnan - Product Manager
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
root@kali: ~
File Actions Edit View Help
Vinothkumar R - Product Manager - Zoho Corporation
Vipasha Sinha - Senior Product Marketer
Vishnukumar Moorthy - Member Technical staff
Vivekanandan M
Yogendrababu venkatapathy - Co-Founder
Yogesh Manoharan - Regional Director
ZOHO CRM Developer - A2Z SAAS Private Limited
Zoho Accounts - Developer
Zoho Developer
Zoho Expert Services - GENOWIRE
balaji N - Developer - Zoho Corporation
ohmprakash s - Ios Developer
rangarajan ramesh - Account Manager - Zoho
sathiyam sathiyamsarva - zoho - Zoho Corporation
shaik Afreen taj - 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/595e989fa8f137d2af456fd4
https://trello.com/power-ups/5b4c1aa1922a254295bb0a35/zoho-crm
https://trello.com/power-ups/5b55db5704cc75f290f1da73/automateio
https://trello.com/power-ups/5ba22bdcd58ada0595eadc98,
https://trello.com/power-ups/5ba22bdcd58ada0595eadc98/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-yzn5vfon
https://trello.com/templates/design/freelance-branding-project-25m66hsj
https://trello.com/templates/design/research-iteration-8t9qgmnz
https://trello.com/templates/product-management
https://trello.com/templates/product-management/5-etapas-de-gerenciamento-de-produtos-7s8avmuv
https://trello.com/templates/product-management/5-listes-pour-la-gestion-de-produits-0lufgyd7
https://trello.com/templates/product-management/backlog-de-funcionalidades-sncwwjtg
https://trello.com/templates/product-management/construindo-um-mvp-shym7pir
https://trello.com/templates/product-management/fabrication-process-dakvjp35
https://trello.com/templates/product-management/product-roadmap-template-frbajsbh
https://trello.com/templates/product-management/roadmap-de-produto-67ljiblr
https://trello.com/templates/product-management/roadmap-produit-jpdxl2mn
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
root@kali: ~
File Actions Edit View Help
Vijayaragavan venugopal
Vinodraj Thiyagarajan
Vinothkumar R - Product Manager - Zoho Corporation
Vipasha Sinha - Senior Product Marketer
Vishnukumar Moorthy - Member Technical staff
Vivekanandan M
Yogendrababu venkatapathy - Co-Founder
Yogesh Manoharan - Regional Director
ZOHO CRM Developer - A2Z SAAS Private Limited
Zoho Accounts - Developer
Zoho Developer
Zoho Expert Services - GENOWIRE
balaji N - Developer - Zoho Corporation
ohmprakash s - Ios Developer
rangarajan ramesh - Account Manager - Zoho
sathiyam sathiyamsarva - zoho - Zoho Corporation
shaik Afreen taj - 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 Godishala
Adarsh Pandey - Member of Technical Staff
Adithyan Ravichandar - Lead System Engineer
Ajay George - Partner Support Engineer - Zoho
Ajay Singh - Developer - ZOHO CRM
Akash Krishnan - Member Technical Staff
Akilan Marimuthu
Akshaya Chandrasekar - Zoho Corporation
Ali Shabdar - Regional Director MEA
Alok Kumar Bharti - Software Engineer
Aman Gupta - Zoho Developer
Amarnath KR - Zoho Developer
Ambi Moorthy - Product Manager and Co-Founder
Anandaraman Krishnan - Product Manager
Anantha Subramaniam - Engineer Trainee
Ananthu Nair - Presales Engineer - Zoho Corporation
Andrea Mahoney - VP - Certified Computer Solutions
Andrew Bourne
Andrew Joseph - Zoho Corporation
Andrews B A - Senior Member Of Technical Staff
Anubhav Pandey - Zoho Consultant
Anumita Gupta - Technical Writer
Aravind Natarajan - Zoho Corporation
Arun Balachandran - Senior Product Marketing Manager
Arun Kesavan - Product Designer
Aruna Muralidharan - Product Marketer
Arvind Krishnamoorthy
Ashok Chakravarthi Nagarajan
34°C
Cloudy
ENG
IN
13:47
14-09-2022



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 .

REULTS :

successfully demonstrated information gathering using theHarvester

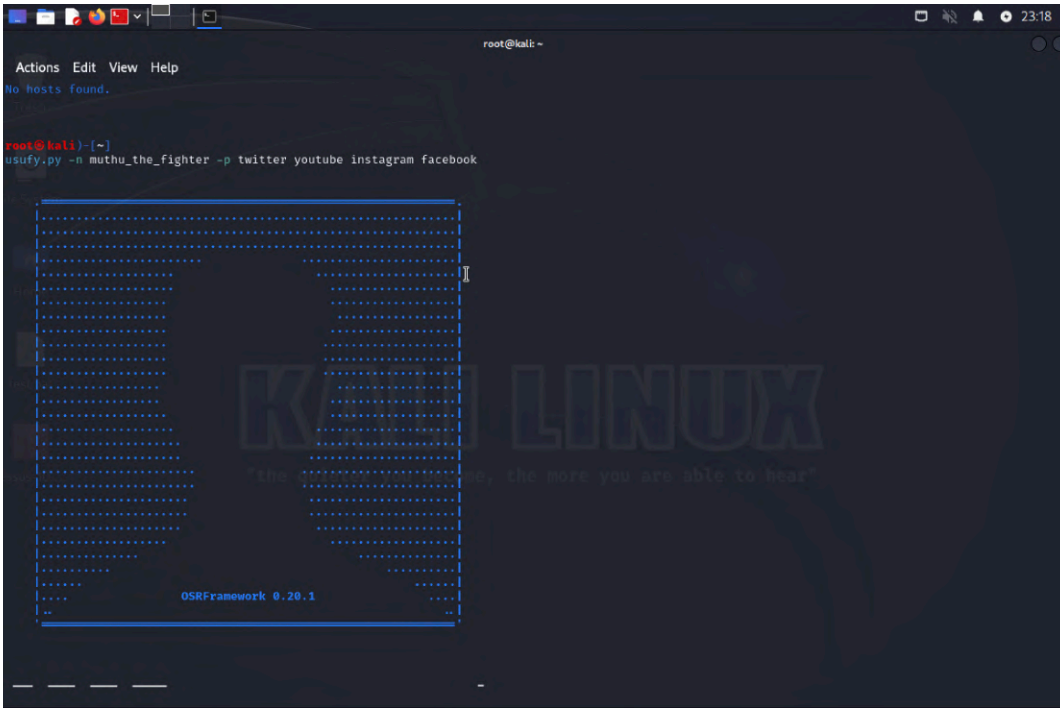
Exercise No 4 - Open Source Intelligence Gathering Using OSRFramework

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

Step 1: Log into kali linux machine
Step 2: Launch a command line terminal by clicking on terminal icon from taskbar
Step 3: Usufy.py checks for the existence of a profile for given user details in different platforms

Command:

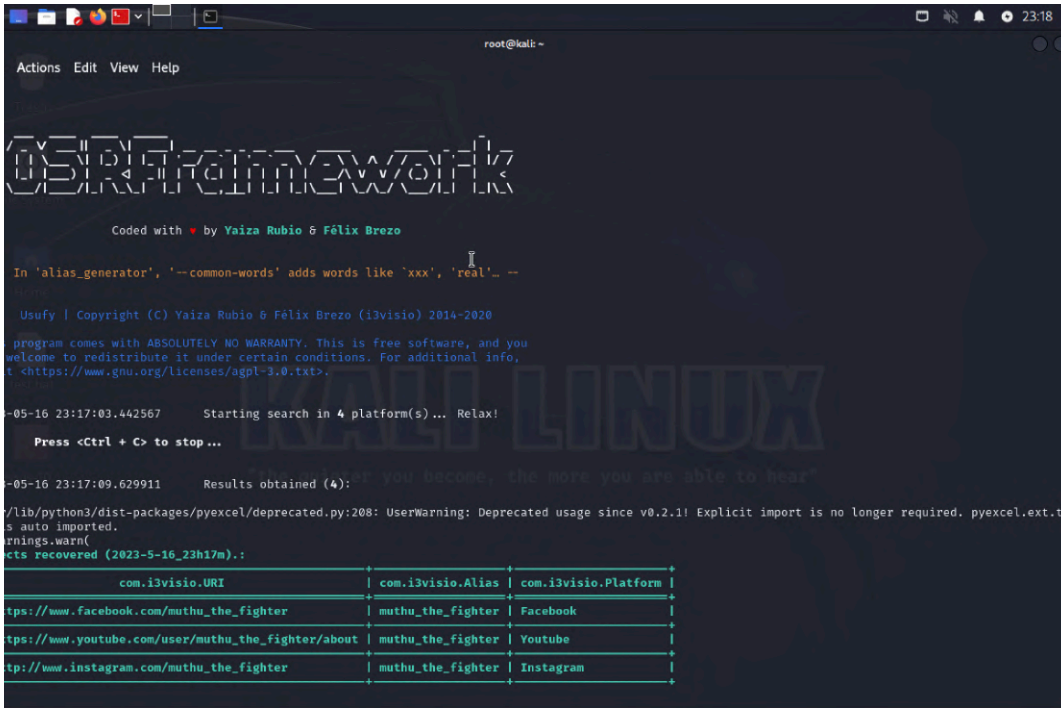
Usufy.py -n <Target username or profile name> -p twitterfacebook youtube



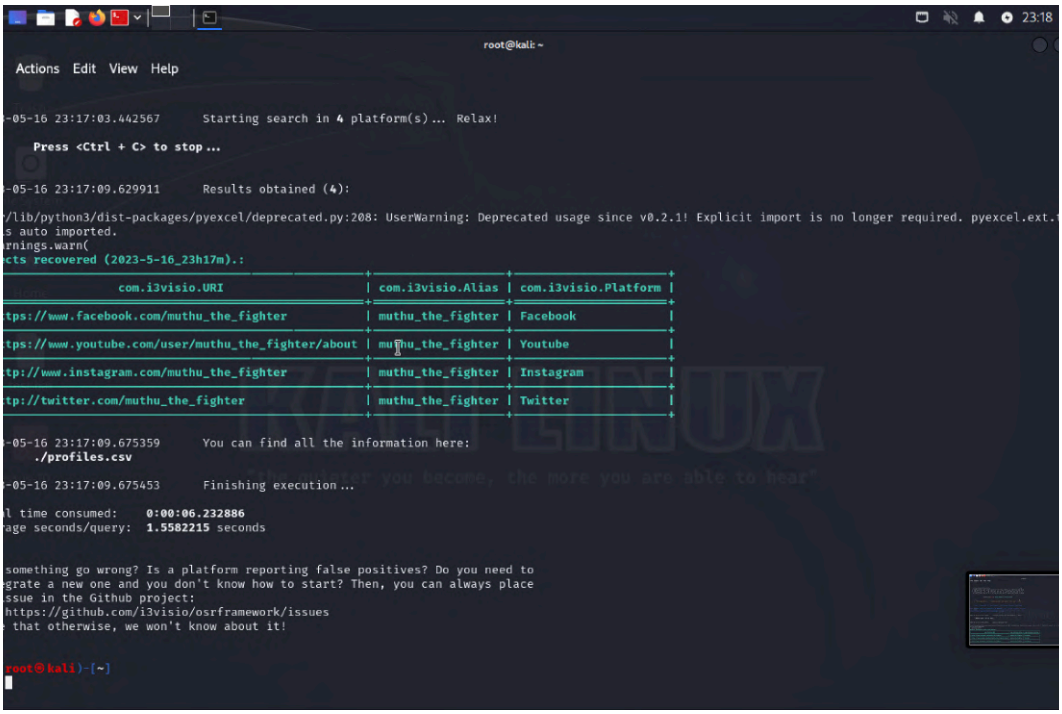
Caption

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

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



Caption



Caption

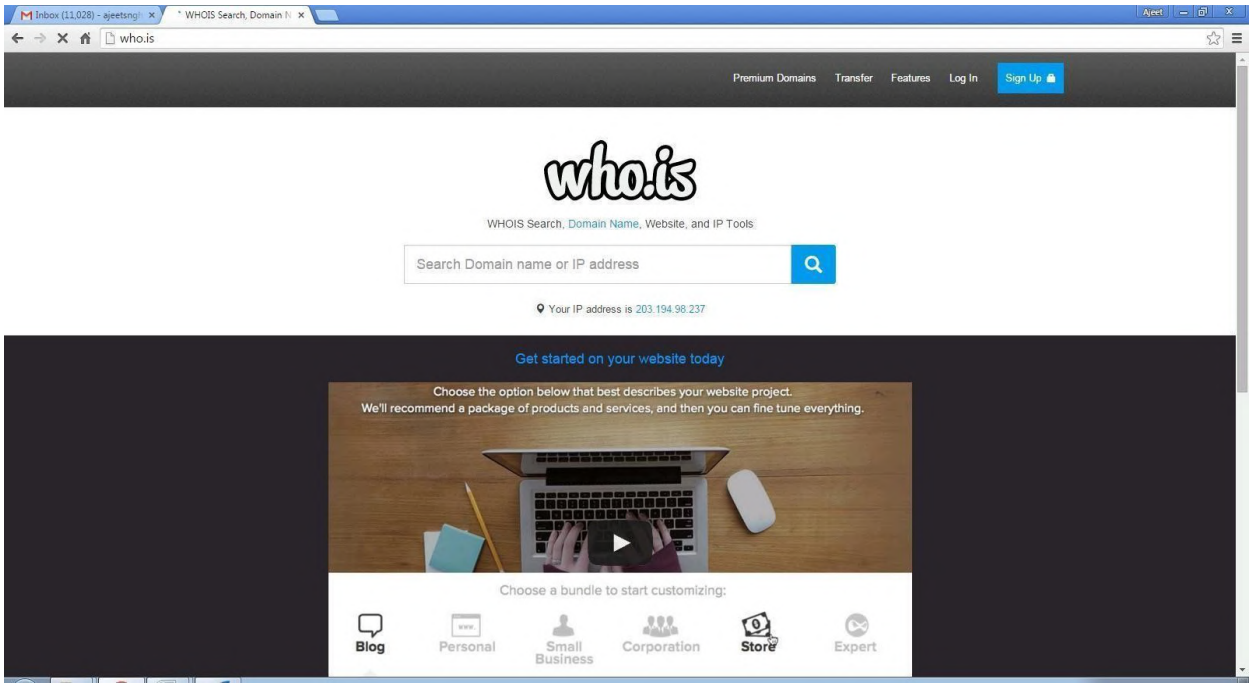
RESULT:

SUCCESFULLY Checked for the Existence of a Profile for given user details in differentplatforms

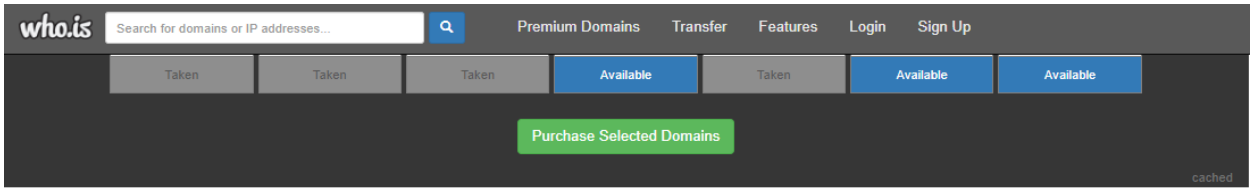
Exercise NO 5: Use Google and Whois for Reconnaisasance.

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



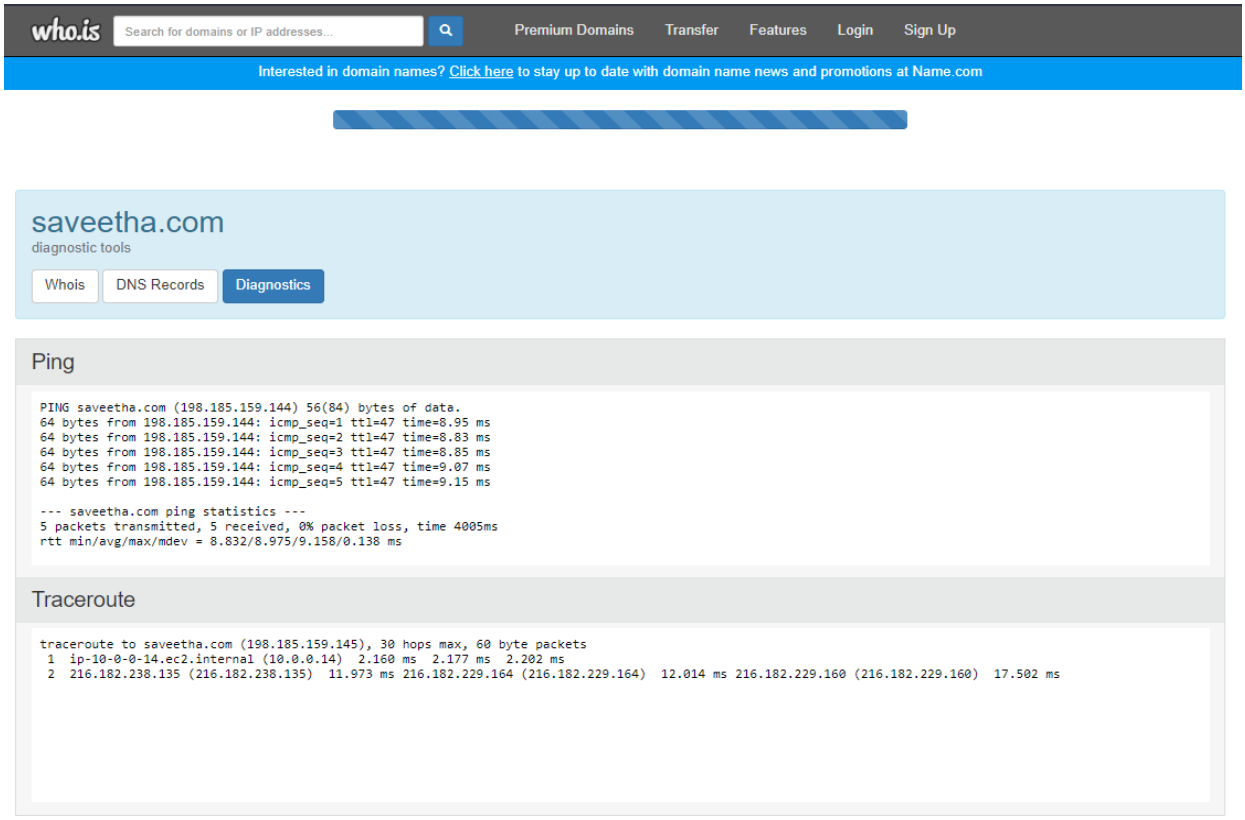
saveetha.com

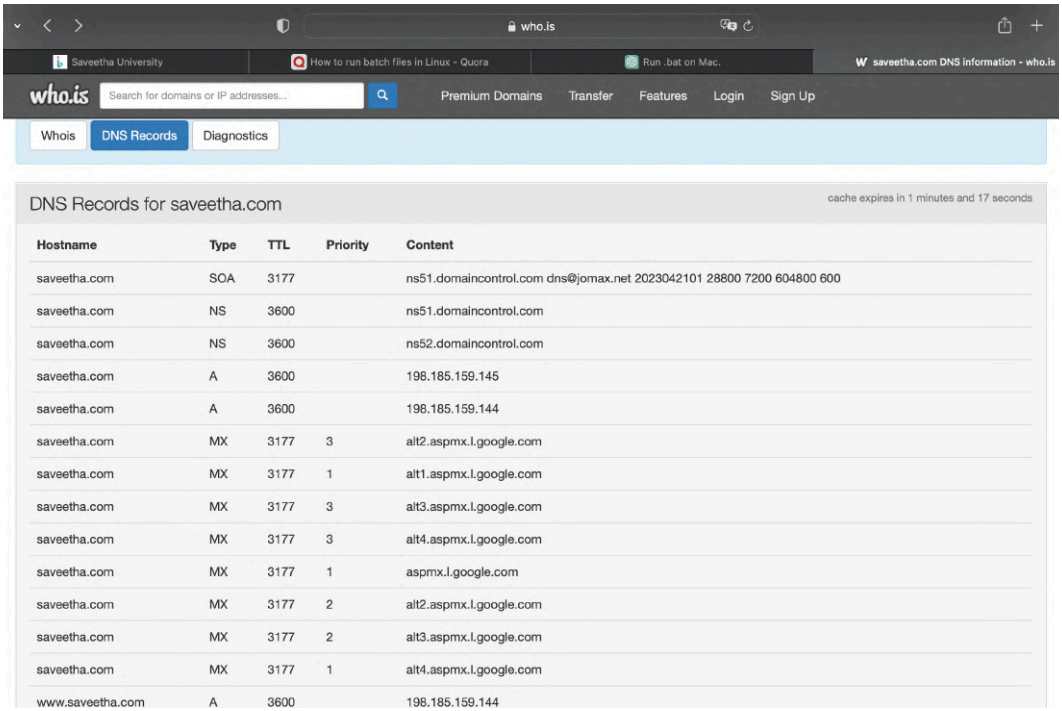
DNS information

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





Hostname	Type	TTL	Priority	Content
saveetha.com	SOA	3177		ns51.domaincontrol.com dns@jomax.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

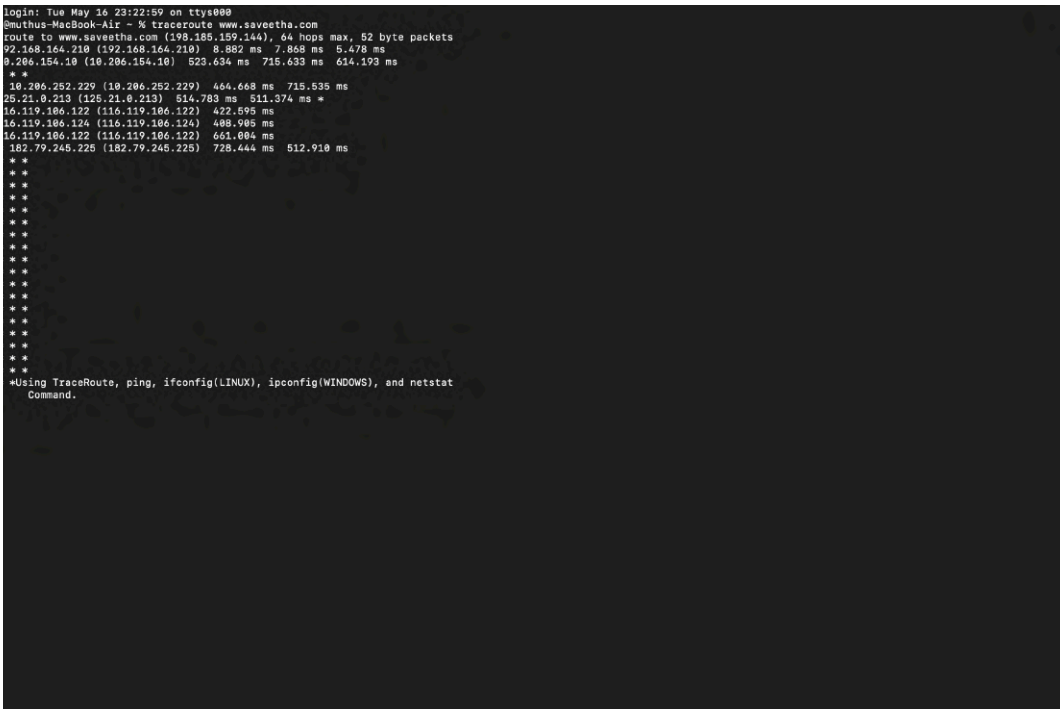
RESULT:

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.

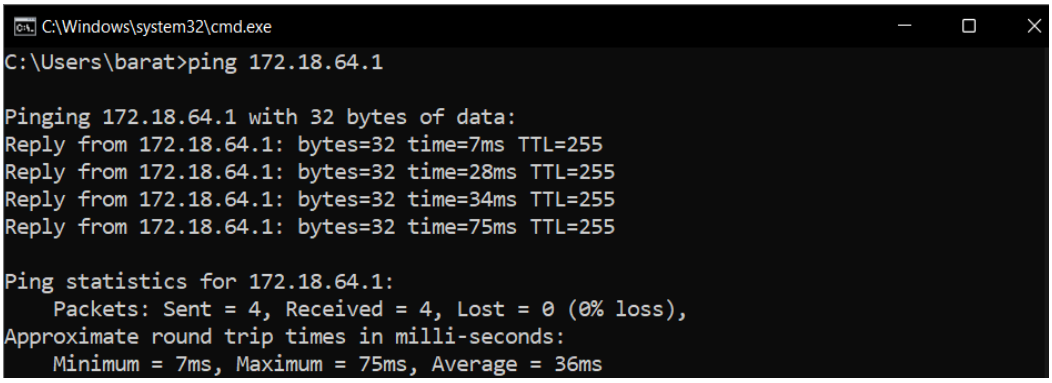
Procedure:



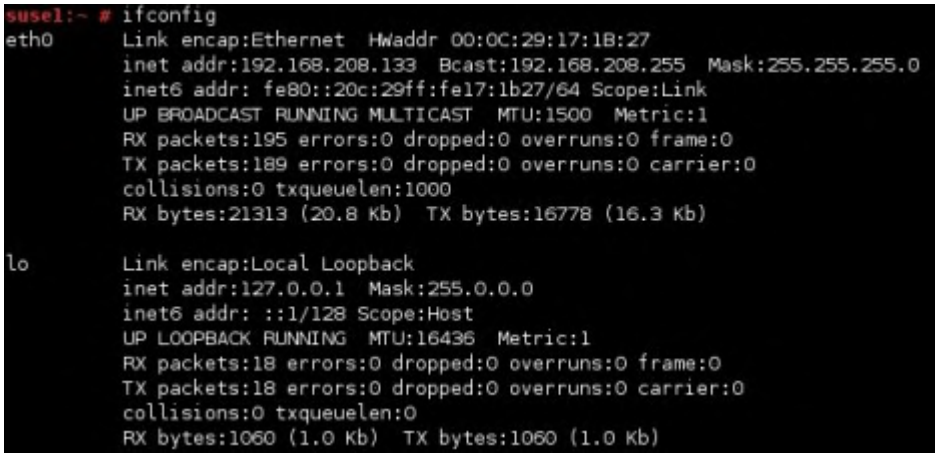
Caption

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

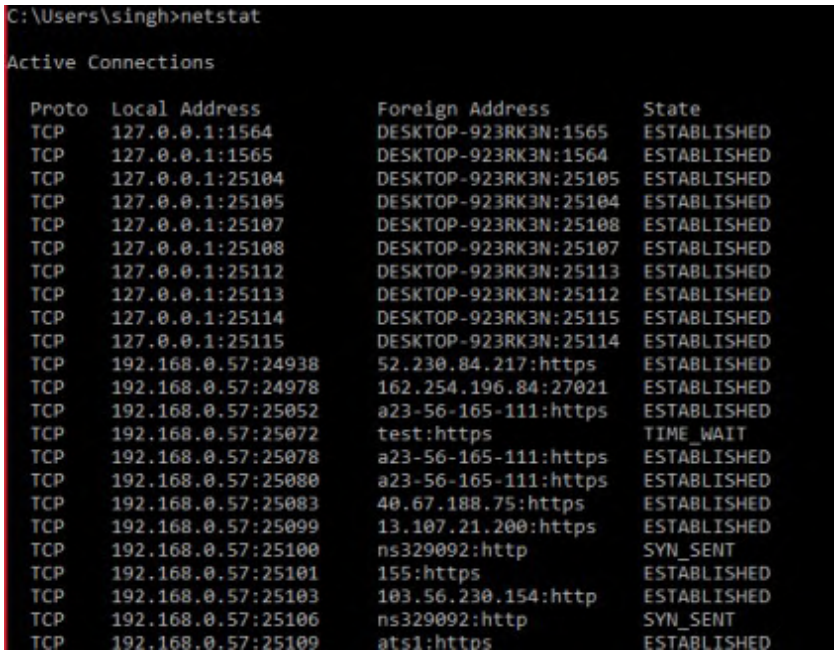
Step 2: Type ping command and type IP Address press “Enter”



Step 3: Type ifconfig command



Step 4: Type netstat command



RESULT:

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

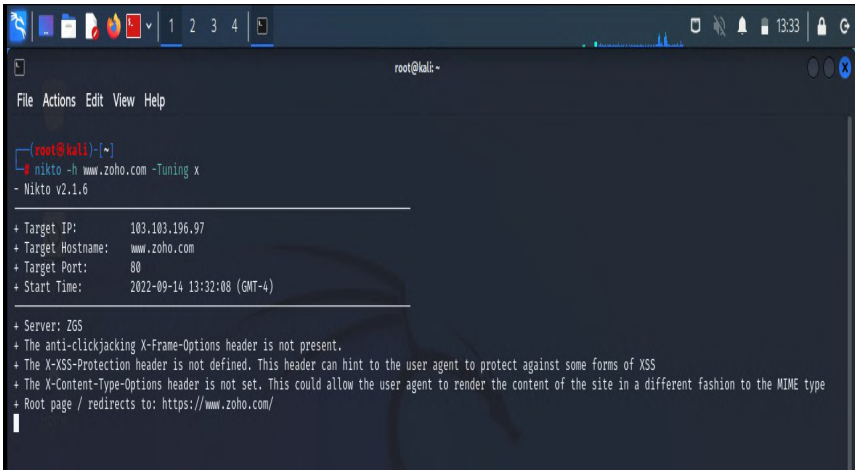
Exercise No 7:VULNERABILITY ANALYSIS - CGI Scanning with Nikto

Aim:To perform vulnerability Analysis using CGI Scanning with Nikto

Procedure:

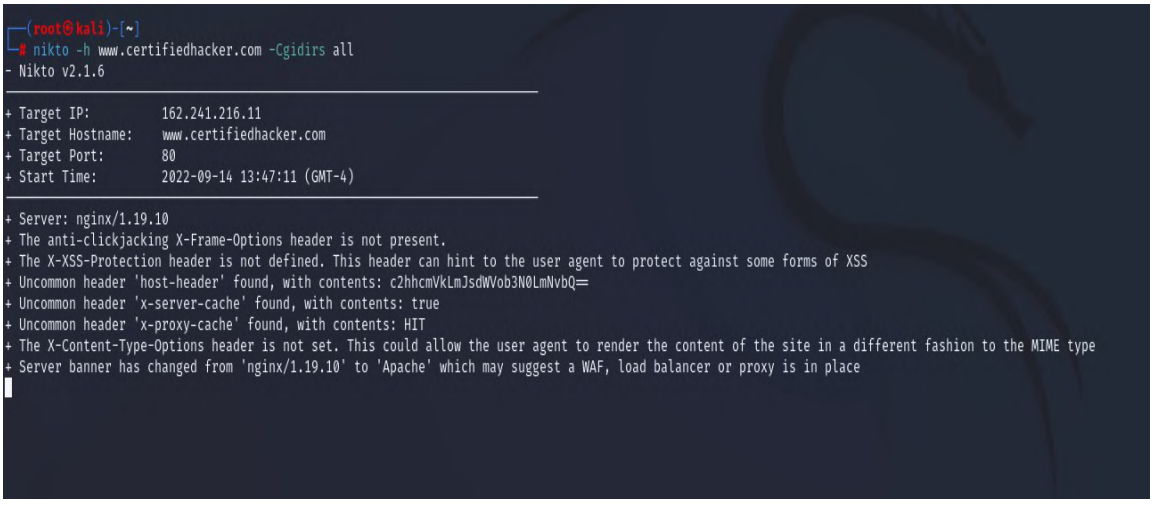
Step 1: open a terminal window and type nikto –H and press enter

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



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



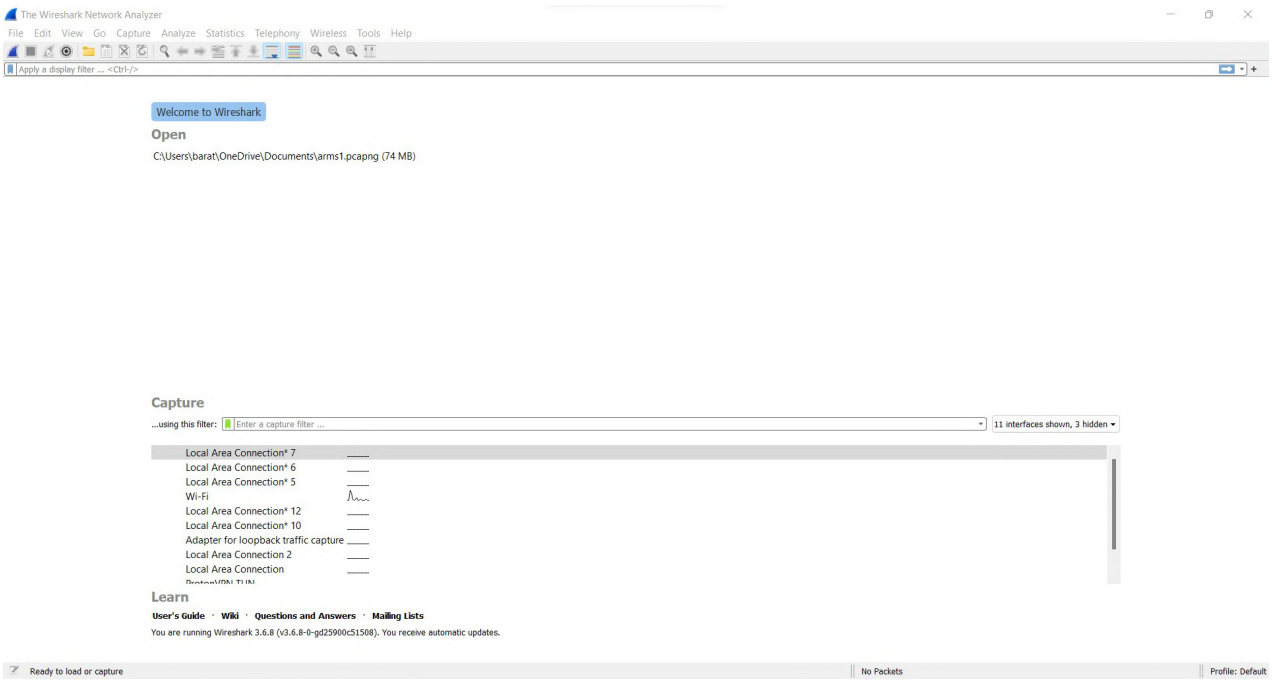
Step 5. Nikto will scan the webserver as it looks vulnerable CGI directories. It scans the webserverand list out the directories

EXCERSISE 8: WireShark sniffer

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

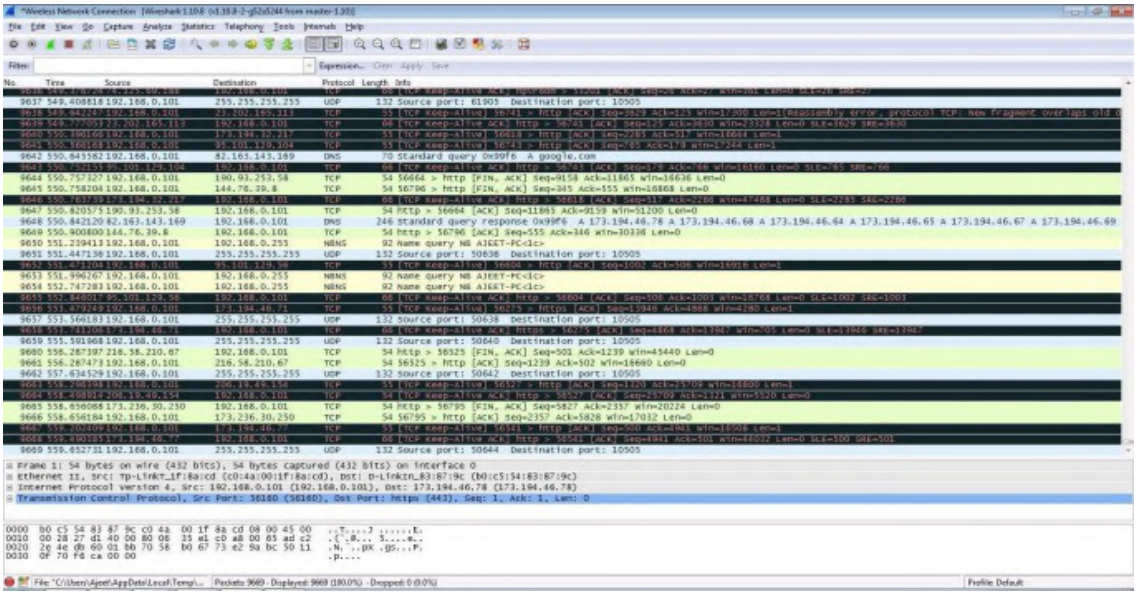
Procedure:

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



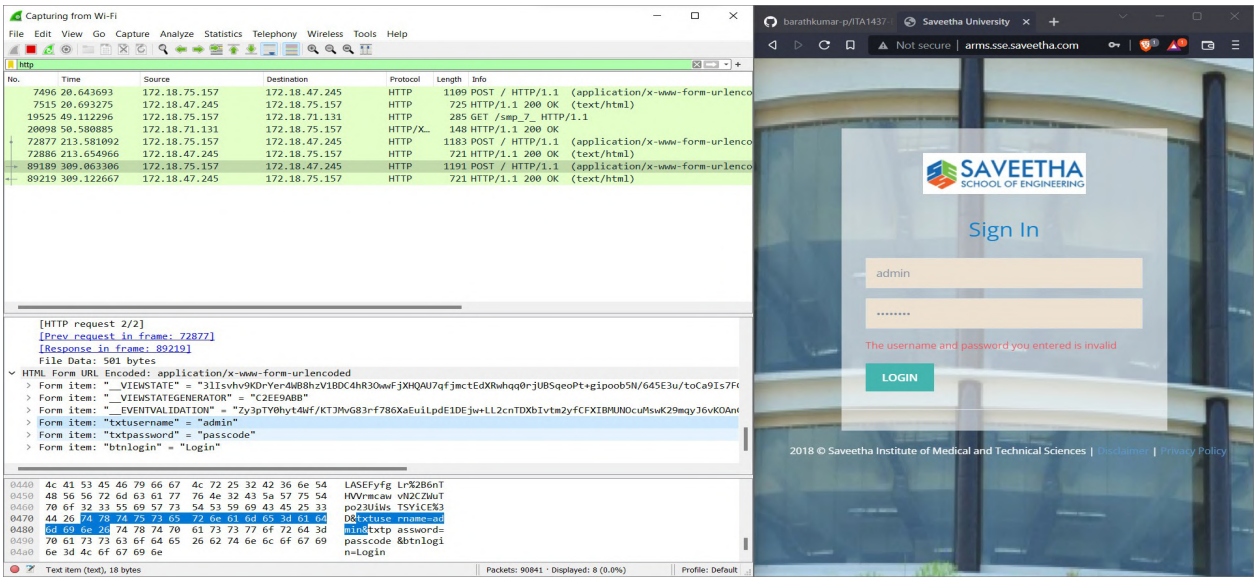
Step 4: Open a website in a new window and enter the user id and password. Register ifneeded.

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.

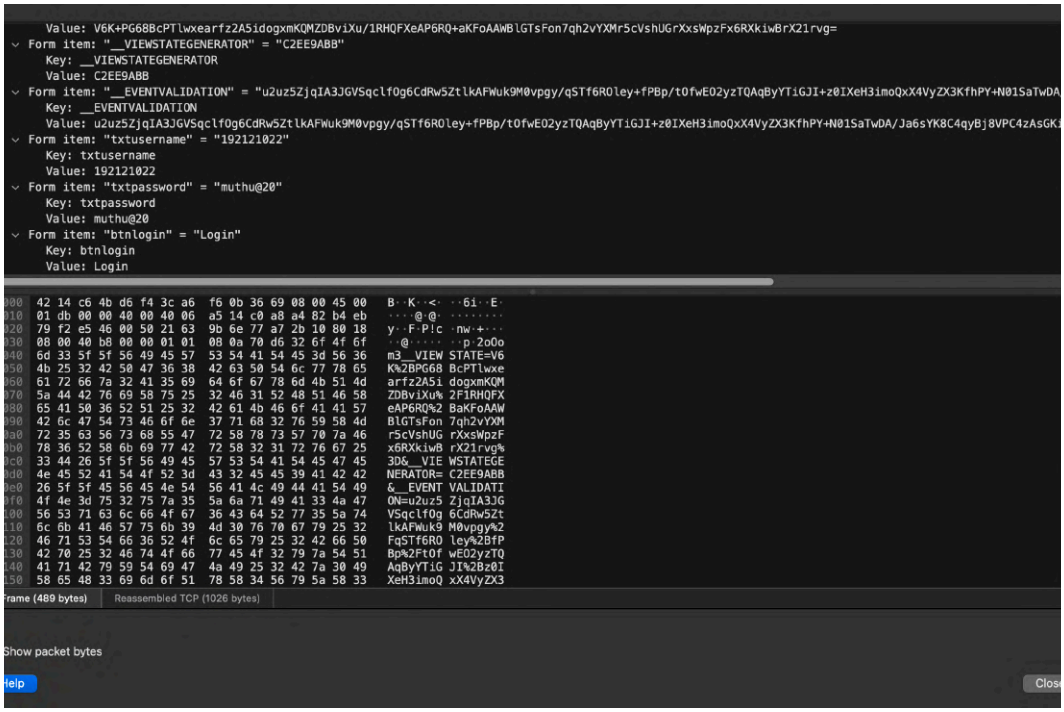
Step 9: Now stop the tool to stop recording



Step 10: Find the post methods for username and passwords

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

OUTPUT



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.

_____ _____ _____

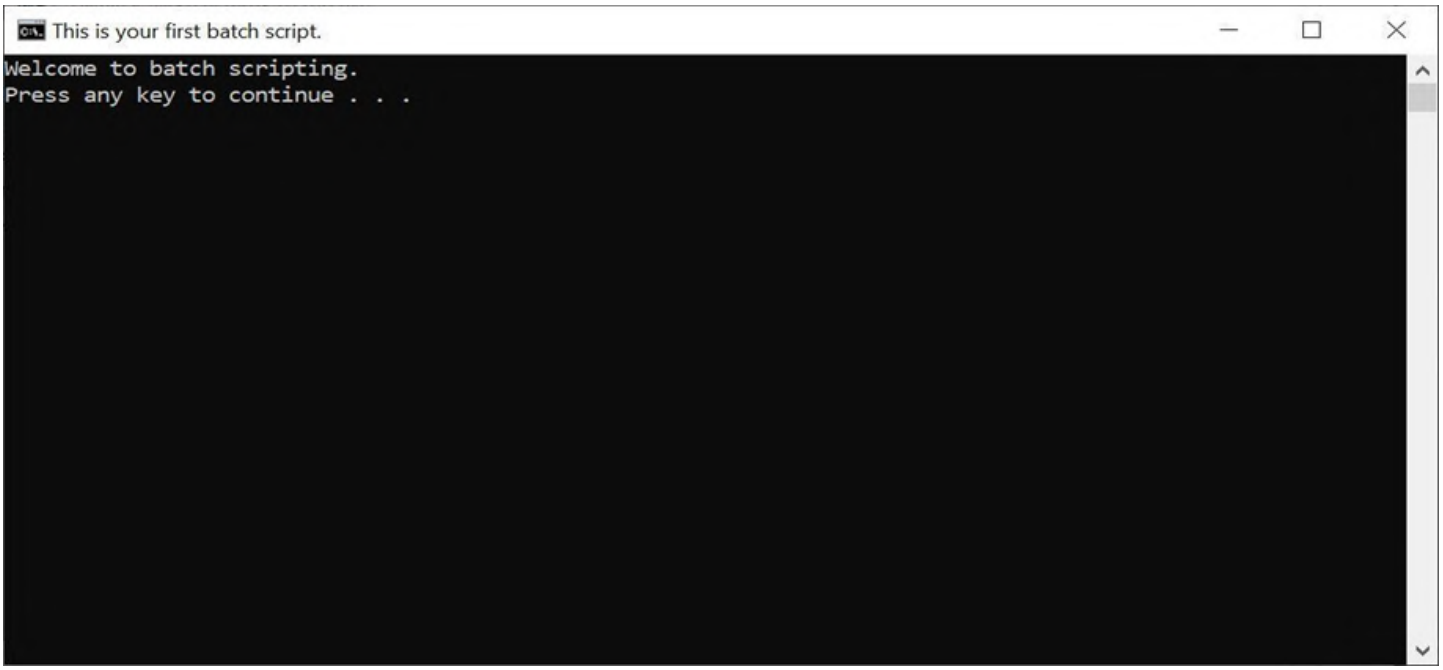
The above script echoes back the text "Welcome to batch scripting!" Save your file by heading to **File > Save As**, and then name your file what you'd like. End your

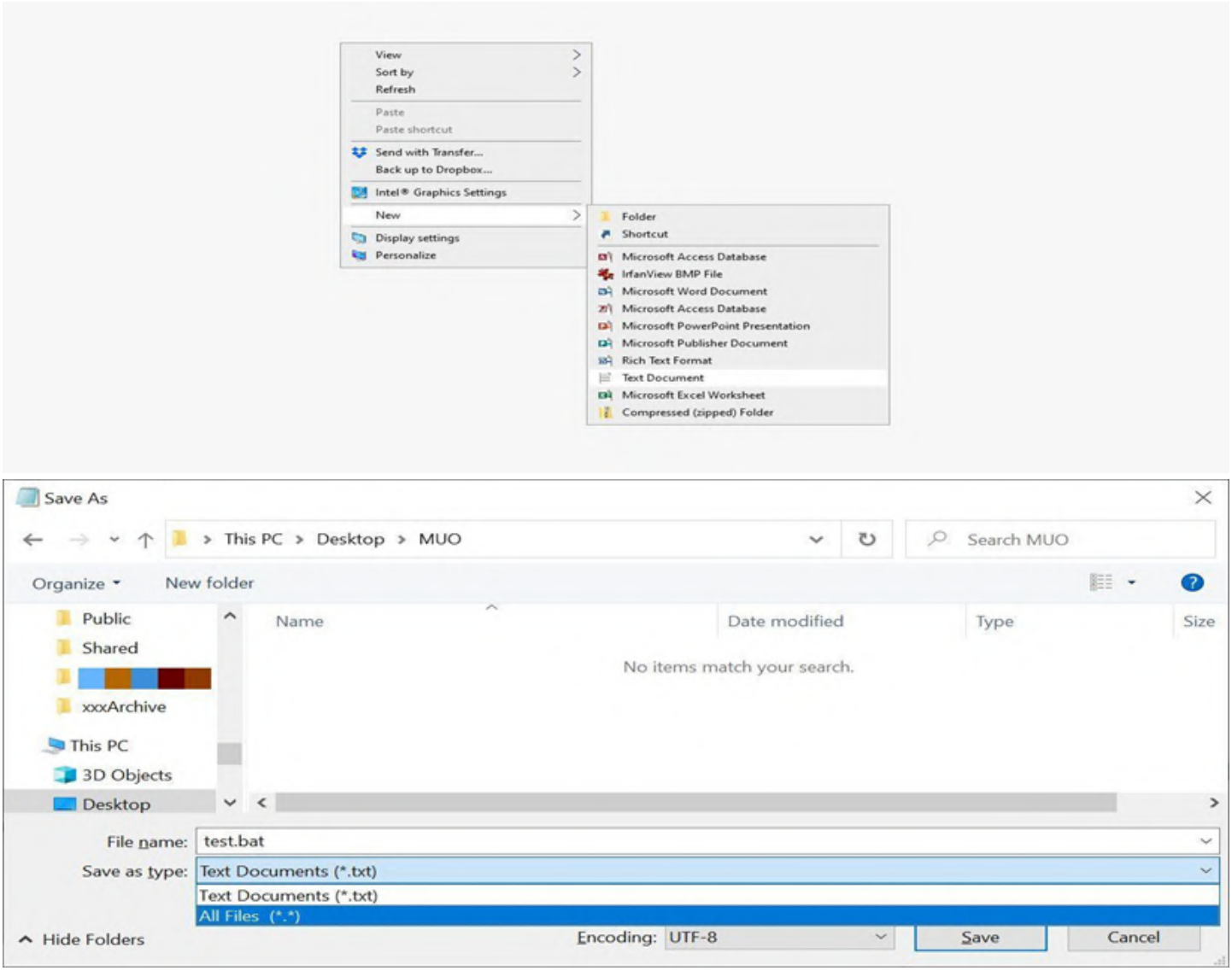
file name with the added **BAT** extension, for example **test.bat**, and click **OK**. This will finalize the batch process. Now, double-click on your newly created batch file to activate it.

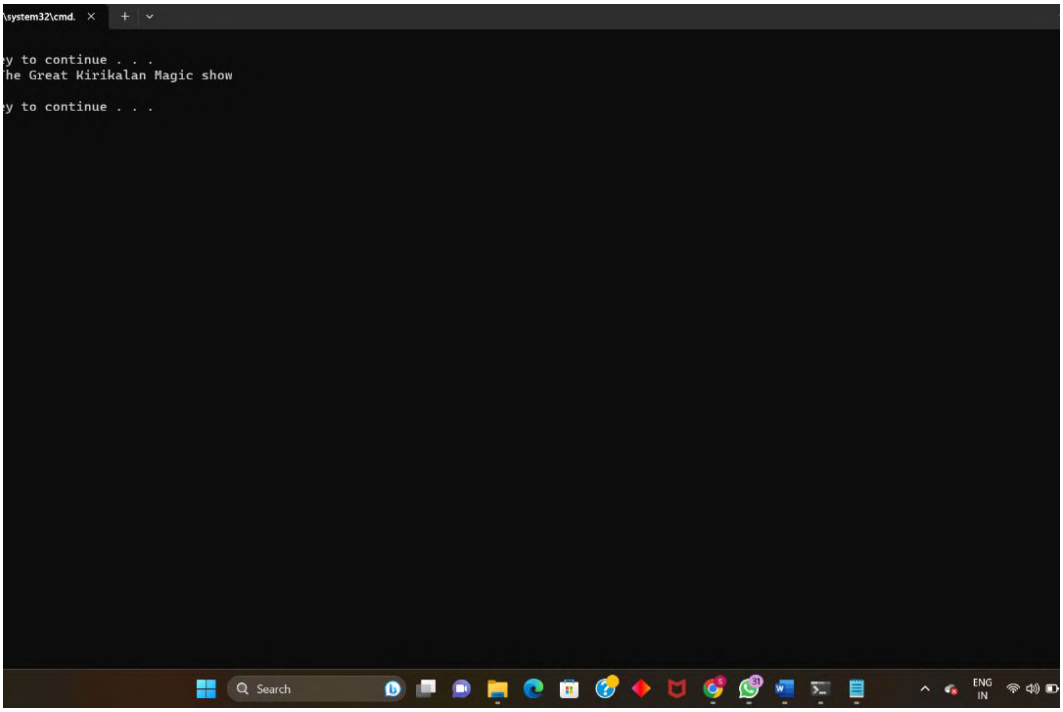
2.To RUN as BAT File

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:




View
Sort by
Refresh
Paste
Paste shortcut
Send with Transfer...
Back up to Dropbox...
Intel® Graphics Settings
New
Display settings
Personalize
Folder
Shortcut
Microsoft Access Database
IrfanView BMP File
Microsoft Word Document
Microsoft Access Database
Microsoft PowerPoint Presentation
Microsoft Publisher Document
Rich Text Format
Text Document
Microsoft Excel Worksheet
Compressed (zipped) Folder
Save As
This PC > Desktop > MUO
Search MUO
Organize
New folder
Public
Shared
xxxArchive
This PC
3D Objects
Desktop
Name
Date modified
Type
Size
No items match your search.
File name: test.bat
Save as type: Text Documents (*.txt)
Text Documents (*.txt)
All Files (*.*)
Hide Folders
Encoding: UTF-8
Save
Cancel



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

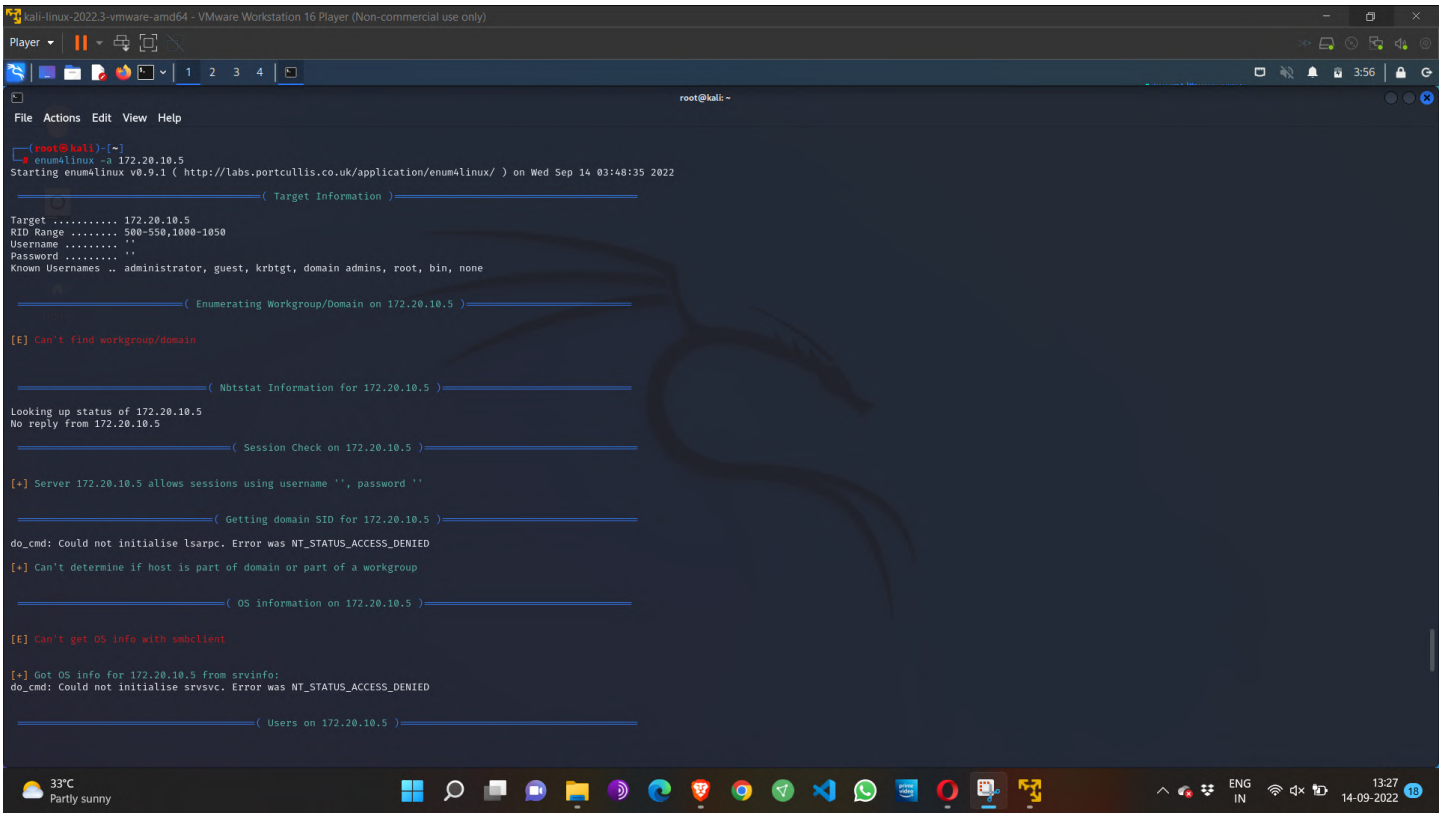
Requirements:

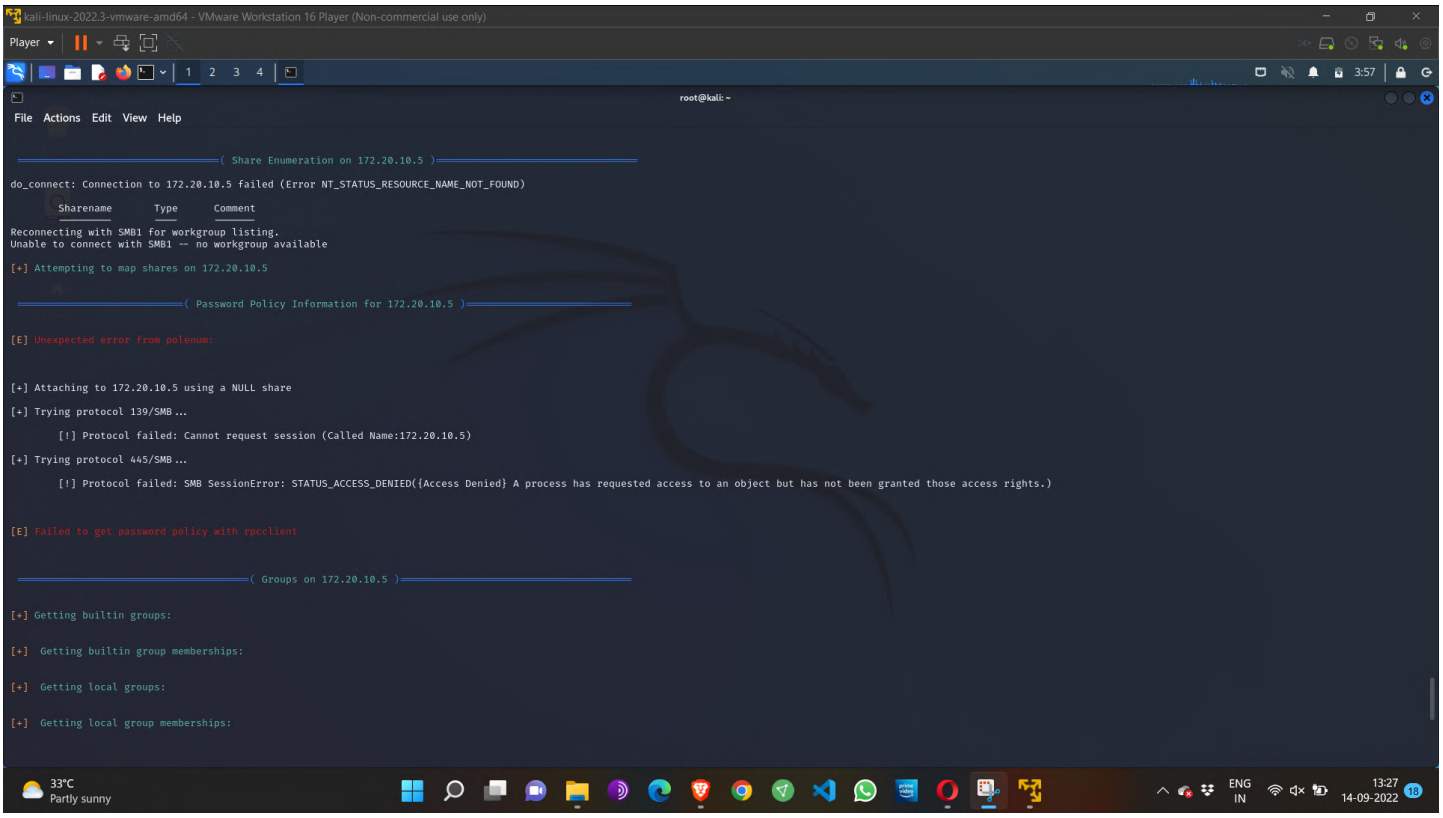
● Kali linux running as an attacker machine ● Windows 7 running as virtual machine
● Admin privileges

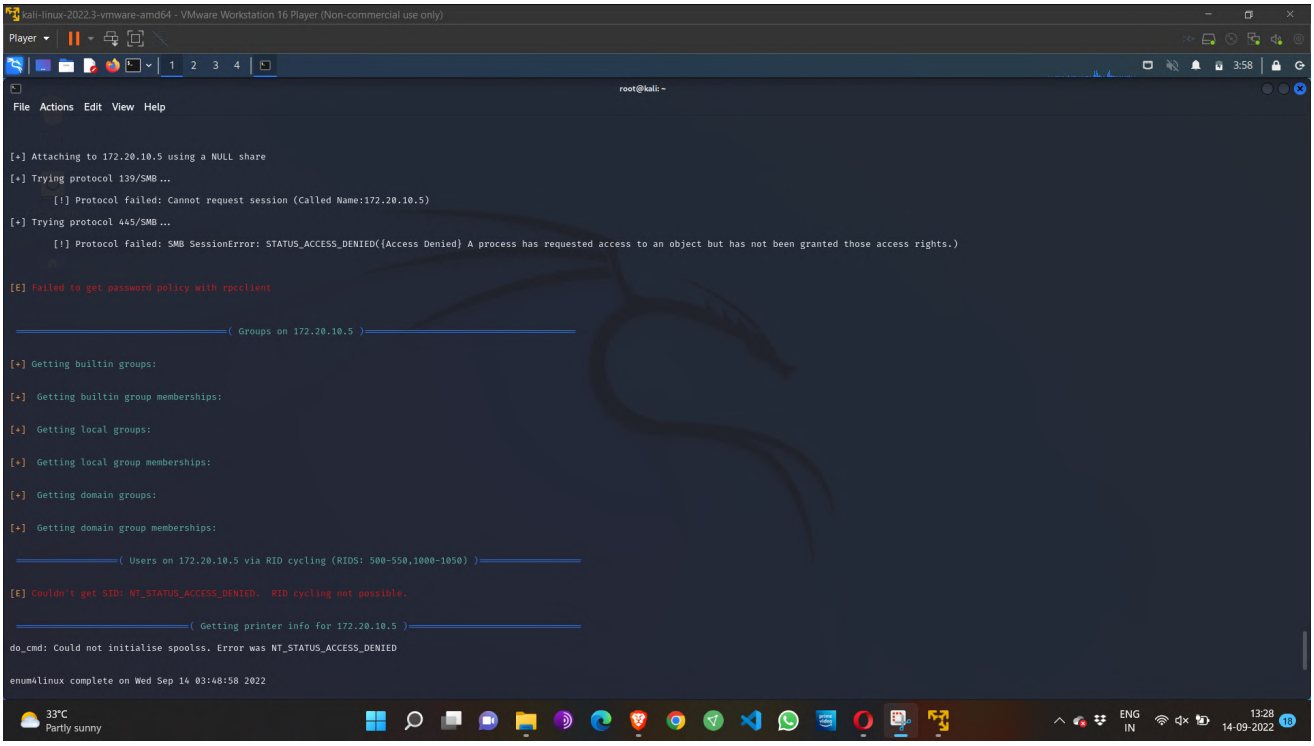
Procedure:

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
root@kali: ~
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 500-550,1000-1050
Username ..... ''
Password ..... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none
(Enumerating Workgroup/Domain on 172.20.10.5)
[E] Can't find workgroup/domain
(Nbtstat Information for 172.20.10.5)
Looking up status of 172.20.10.5
No reply from 172.20.10.5
(Session Check on 172.20.10.5)
[+] Server 172.20.10.5 allows sessions using username '', password ''
(Getting domain SID for 172.20.10.5)
do_cmd: Could not initialise lsarpc. Error was NT_STATUS_ACCESS_DENIED
[+] Can't determine if host is part of domain or part of a workgroup
(OS information on 172.20.10.5)
[E] Can't get OS info with smbclient
[+] Got OS info for 172.20.10.5 from srvinfo:
do_cmd: Could not initialise srvsvc. Error was NT_STATUS_ACCESS_DENIED
(Users on 172.20.10.5)
33°C
Partly sunny
ENG
IN
13:27
14-09-2022


kali-linux-2022.3-vmware-amd64 - VMware Workstation 16 Player (Non-commercial use only)
Player
root@kali: ~
File Actions Edit View Help
(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
ENG
IN
13:27
14-09-2022


kali-linux-2022.3-vmware-amd64 - VMware Workstation 16 Player (Non-commercial use only)
Player
root@kali: ~
File Actions Edit View Help
[+] Attaching to 172.20.10.5 using a NULL share
[+] Trying protocol 139/SMB ...
[!] Protocol failed: Cannot request session (Called Name:172.20.10.5)
[+] Trying protocol 445/SMB ...
[!] Protocol failed: SMB SessionError: STATUS_ACCESS_DENIED({Access Denied} A process has requested access to an object but has not been granted those access rights.)
[E] Failed to get password policy with rpcclient
(Groups on 172.20.10.5)
[+] Getting builtin groups:
[+] Getting builtin group memberships:
[+] Getting local groups:
[+] Getting local group memberships:
[+] Getting domain groups:
[+] Getting domain group memberships:
(Users on 172.20.10.5 via RID cycling (RIDS: 500-550,1000-1050))
[E] Couldn't get SID: NT_STATUS_ACCESS_DENIED. RID cycling not possible.
(Getting printer info for 172.20.10.5)
do_cmd: Could not initialise spoolss. Error was NT_STATUS_ACCESS_DENIED
enum4linux complete on Wed Sep 14 03:48:58 2022
33°C
Partly sunny
ENG
IN
13:28
14-09-2022

RESULT:

sucessfully Enumerated information from windows and Samba Host Using Enum4linux