

## Module 4 Social engineering Penetration testing

**Task1 Create Fishing Page using Zphisher**

**Task 2 Create site cloner using Social Engineering tool**

**Task3 how to create fishing email and sent to the target using Social engineering tool**

**1 Extra Activity Using Set tool kit  
Generate the fake Q AR code**

**2 Extra Activity using website for fishing URL detections**

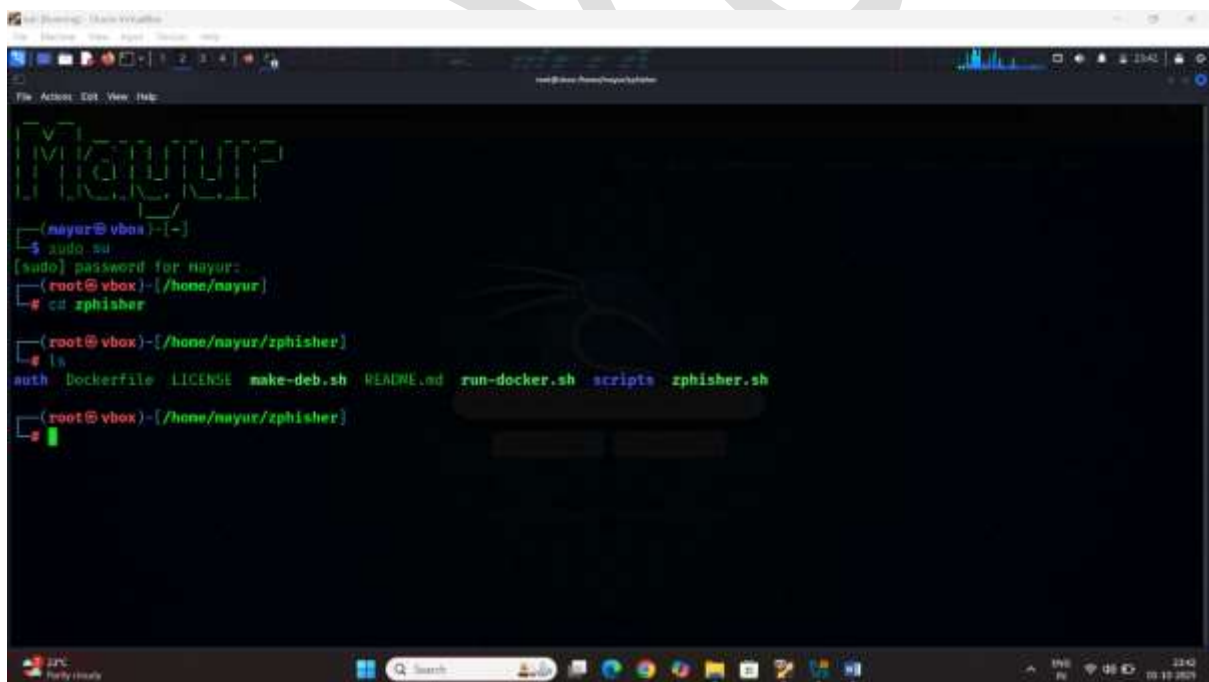
**3 Extra Activity using website for fishing URL detections**

**4 Extra Activity using website for fishing URL detections**

## Task1 Create Fishing Page using Zphisher

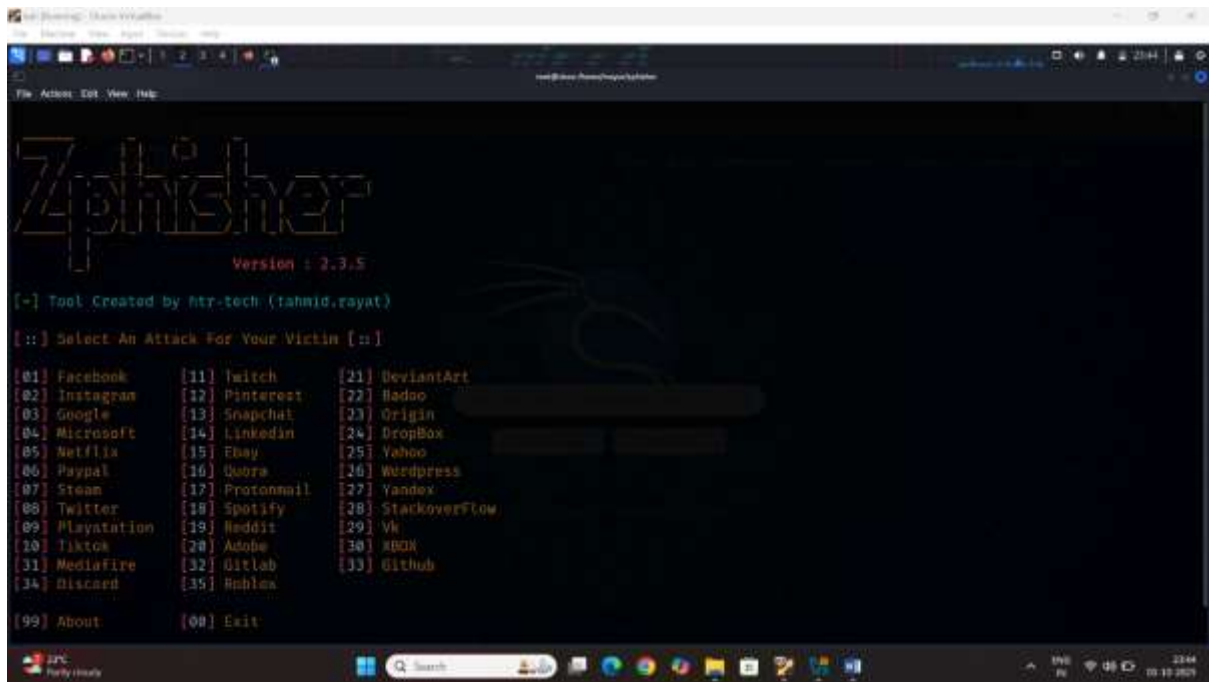
Step1 Start the kali linux machine

Step2 go to Zphisher



```
kali@kali:~/Desktop$ sudo su
[sudo] password for kali:
(kali@kali)~$ cd zphisher
(kali@kali)~/zphisher$ ls
auth Dockerfile LICENSE make-deb.sh README.md run-docker.sh scripts zphisher.sh
(kali@kali)~/zphisher$
```

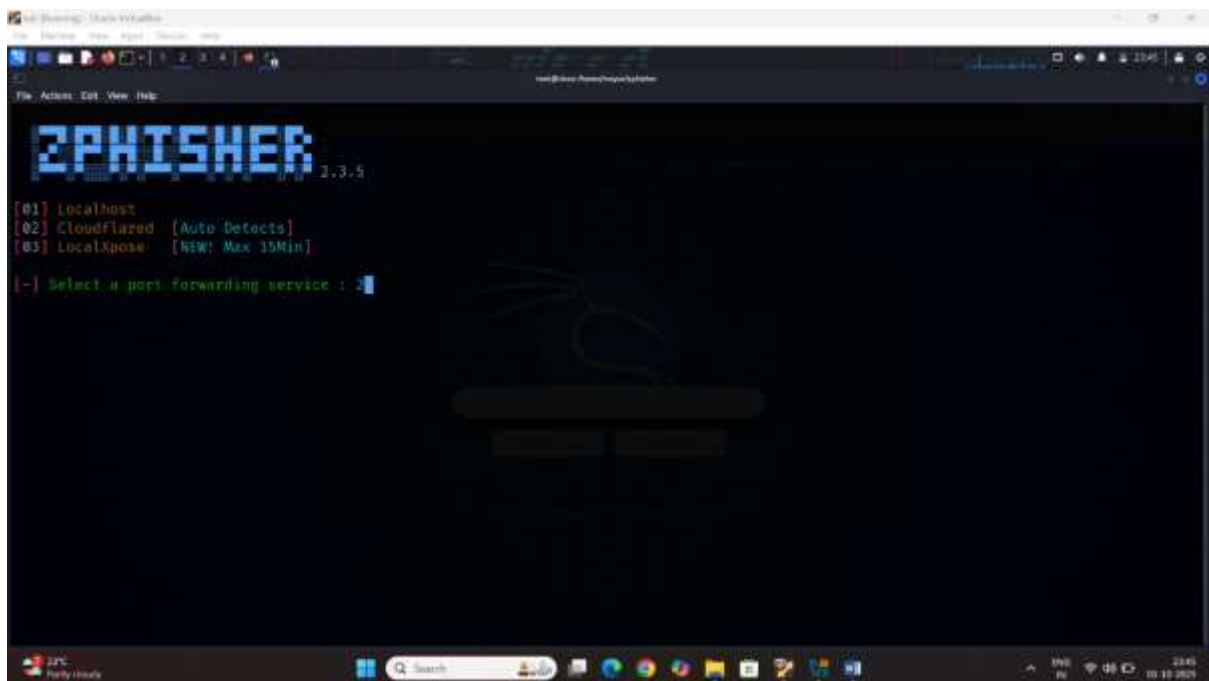
The screenshot shows a terminal window on a Kali Linux desktop environment. The user has successfully installed Zphisher by cloning the repository and navigating to the directory. The terminal output shows the user switching to root via 'sudo su', changing to the 'zphisher' directory, and listing the files which include 'auth', 'Dockerfile', 'LICENSE', 'make-deb.sh', 'README.md', 'run-docker.sh', 'scripts', and 'zphisher.sh'.



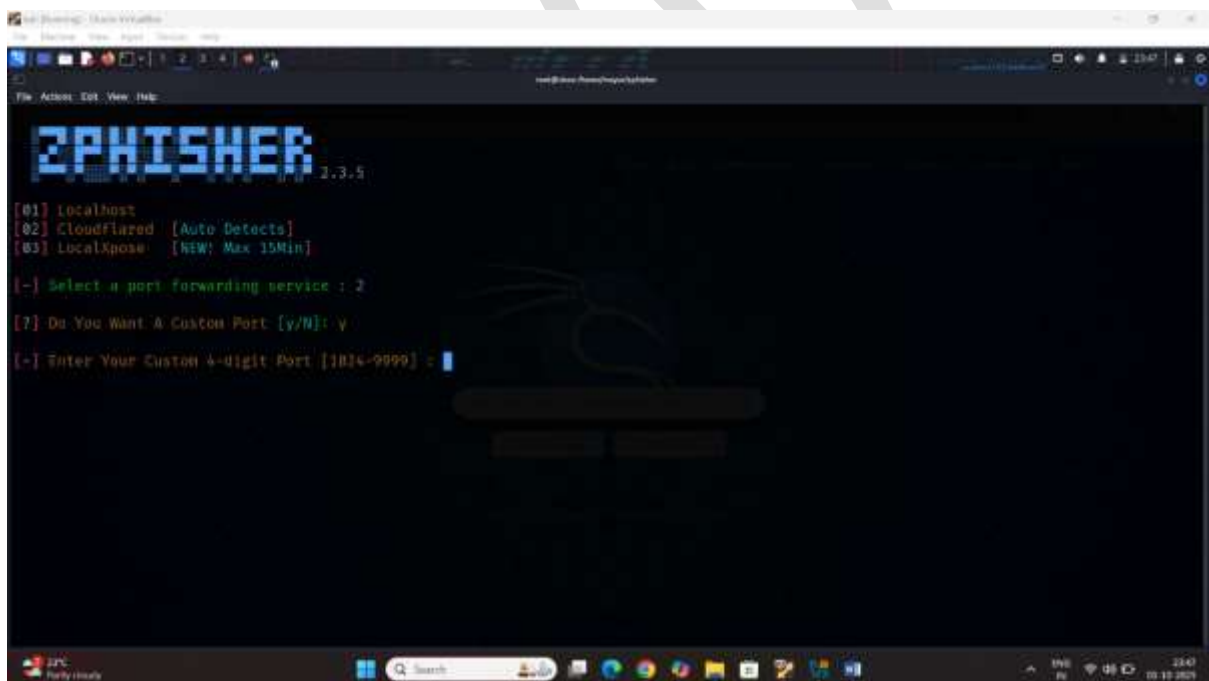
Step3 select the 5 option



Step4 use 2 option



```
2PHISHER 2.3.5
[01] localhost
[02] CloudFlared [Auto Detects]
[03] LocalXpose [NEW! Max 15Min]
[-] Select a port forwarding service : 2
```

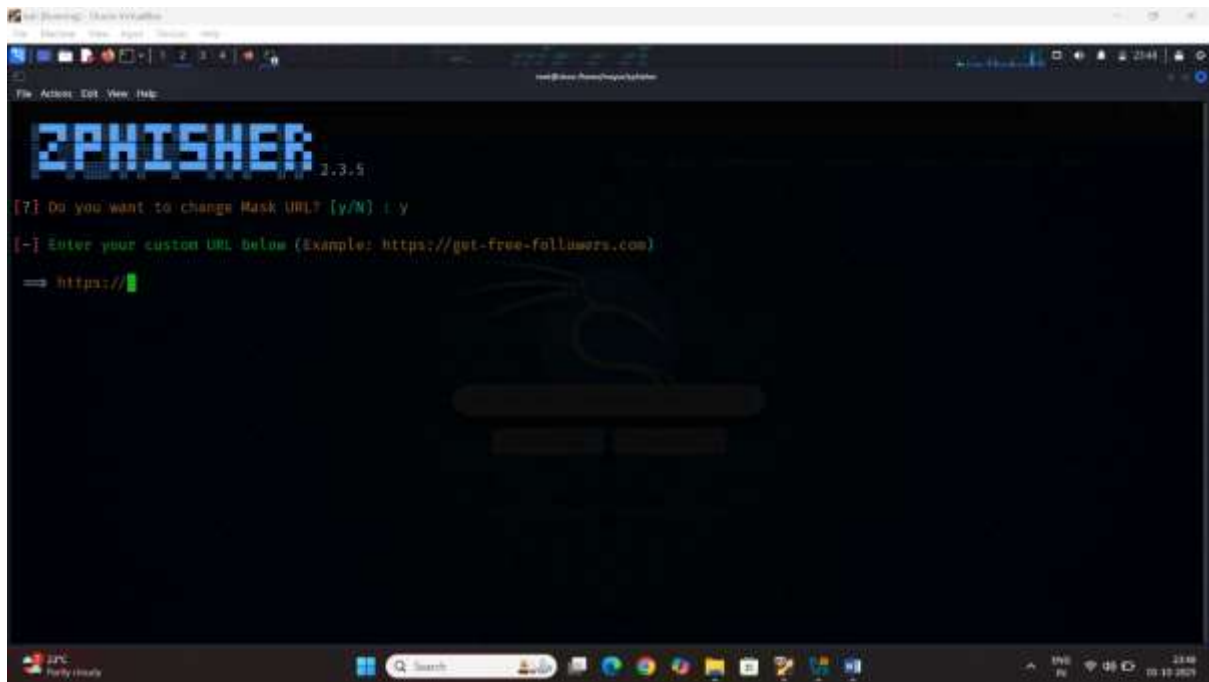


```
2PHISHER 2.3.5
[01] localhost
[02] CloudFlared [Auto Detects]
[03] LocalXpose [NEW! Max 15Min]
[-] Select a port forwarding service : 2
[7] Do You Want A Custom Port [y/N]: y
[-] Enter Your Custom 4-digit Port [1014-9999] :
```

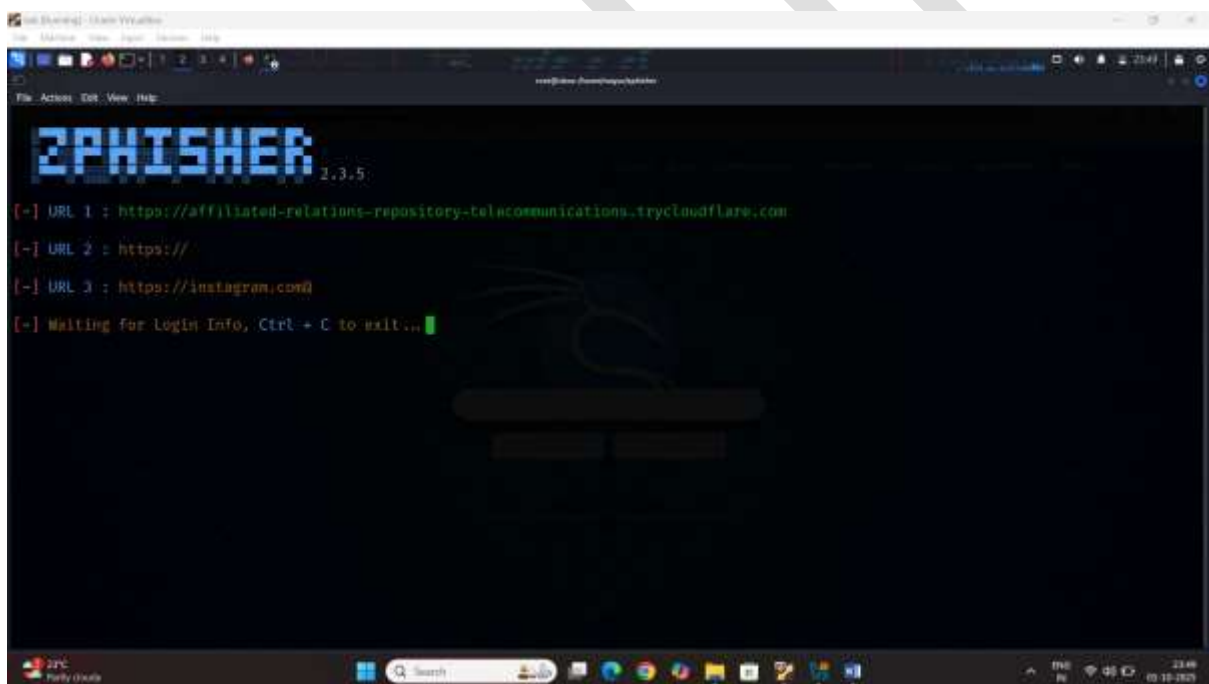
Step5 select the port option yes

Enter the port range 5555

Step6 enter the url Instagram.com

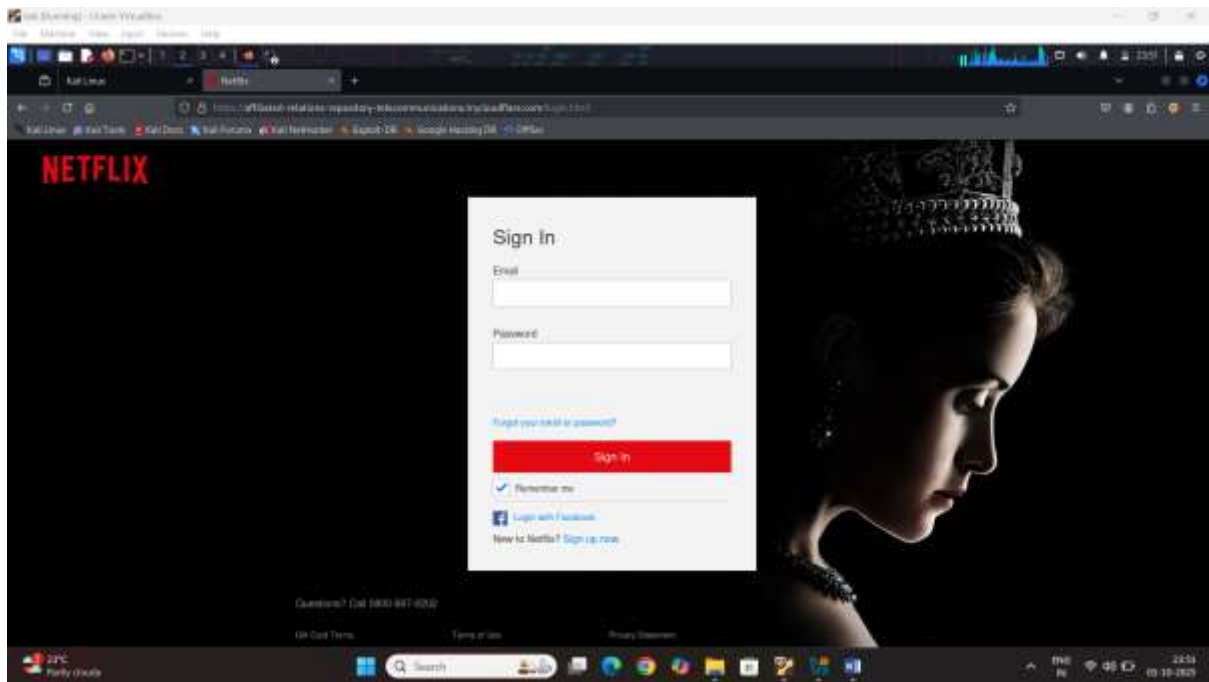


```
2PHISHER 2.3.5
[?] Do you want to change Mask URL? [y/N] : y
[-] Enter your custom URL below (Example: https://get-free-followers.com)
=> https://
```



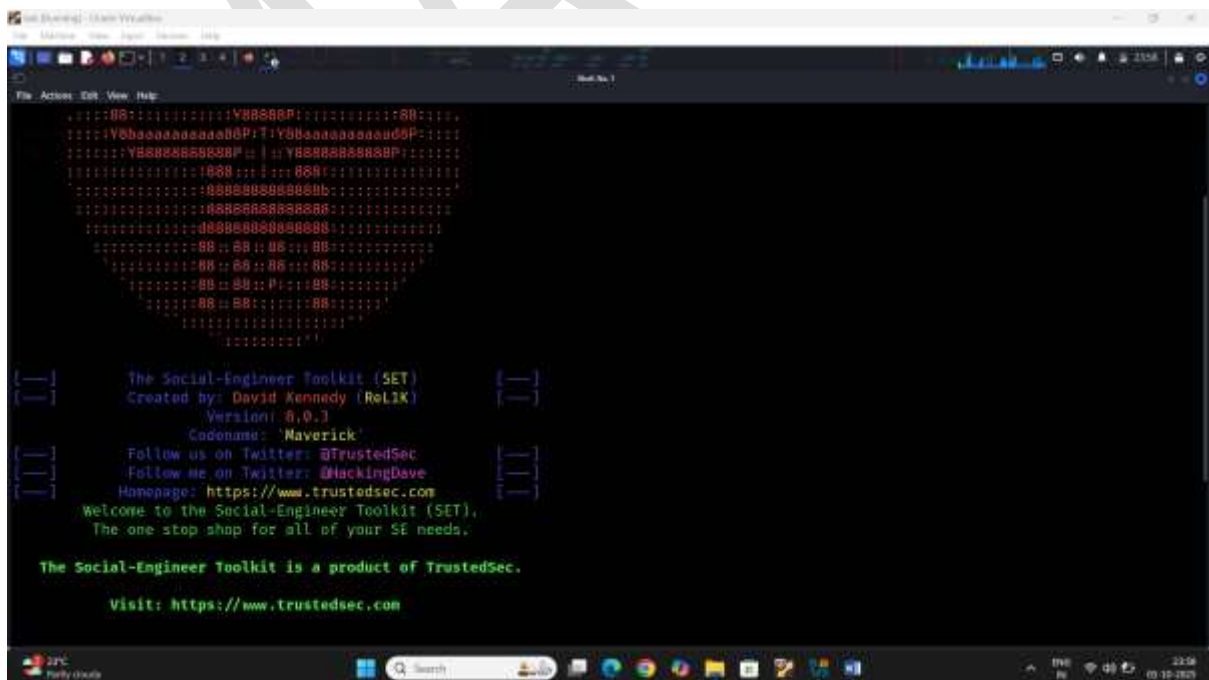
```
2PHISHER 2.3.5
[-] URL 1 : https://affiliated-relations-repository-telecommunications.trycloudflare.com
[-] URL 2 : https://
[-] URL 3 : https://instagram.com
[-] Waiting for Login Info, Ctrl + C to exit...
```

Step7 copy the 1<sup>st</sup> url and paste the chrome  
Result:

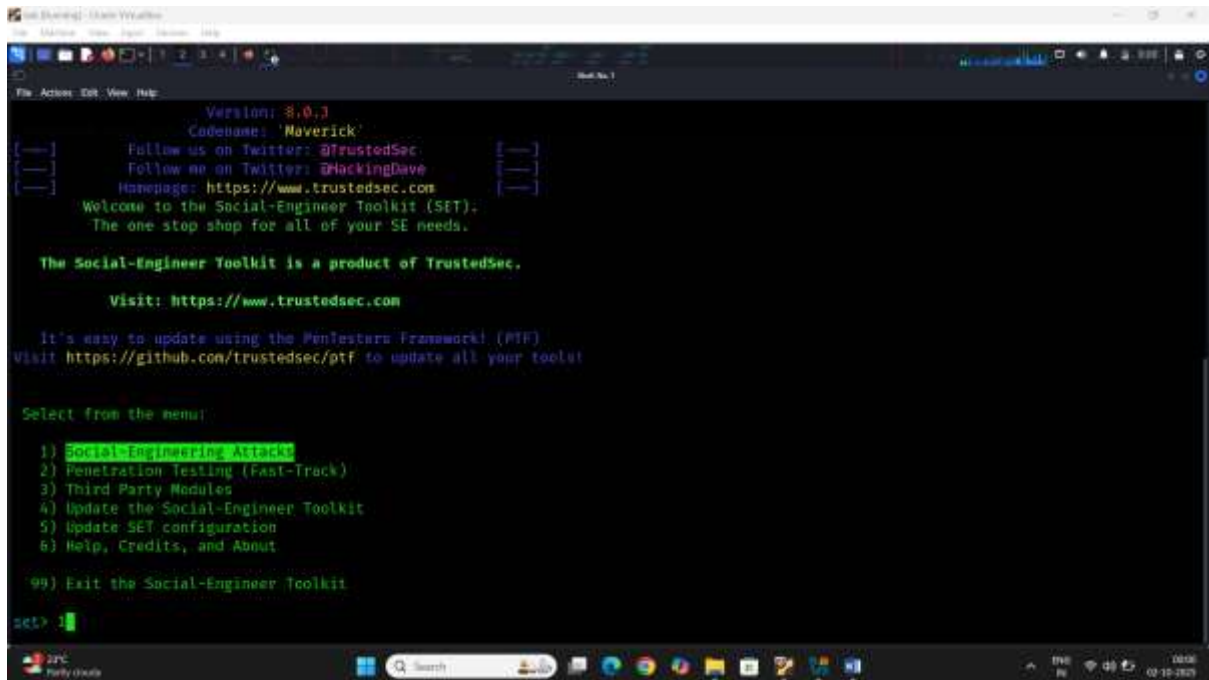


## Task 2 Create site cloner using Social Engineering tool

Step1 start the set tool kite



## Step2 select the social enegineering attack



The screenshot shows the main menu of the Social-Engineer Toolkit (SET) version 8.0.3. The interface is a terminal window with a dark background and green text. The menu options are listed as follows:

```
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!

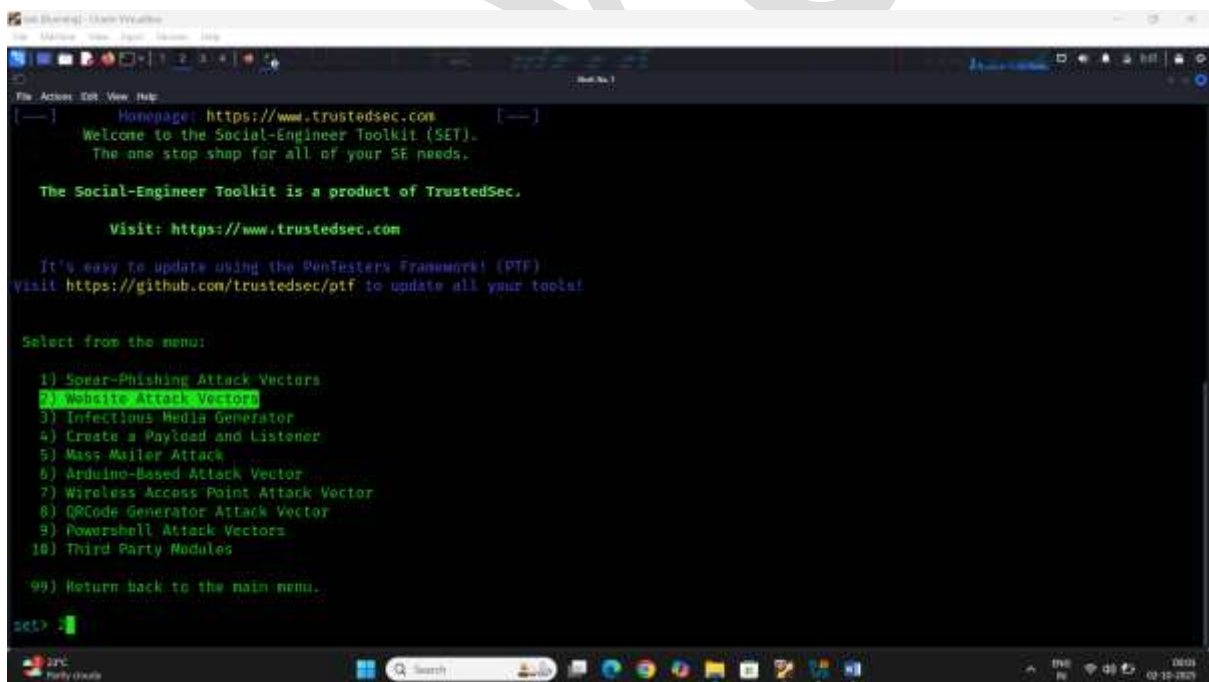
Select from the menu:

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

99) Exit the Social-Engineer Toolkit

set> 1
```

## step3 select the website attack vectors



The screenshot shows the 'Website Attack Vectors' menu within the Social-Engineer Toolkit (SET). The menu options are listed as follows:

```
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:

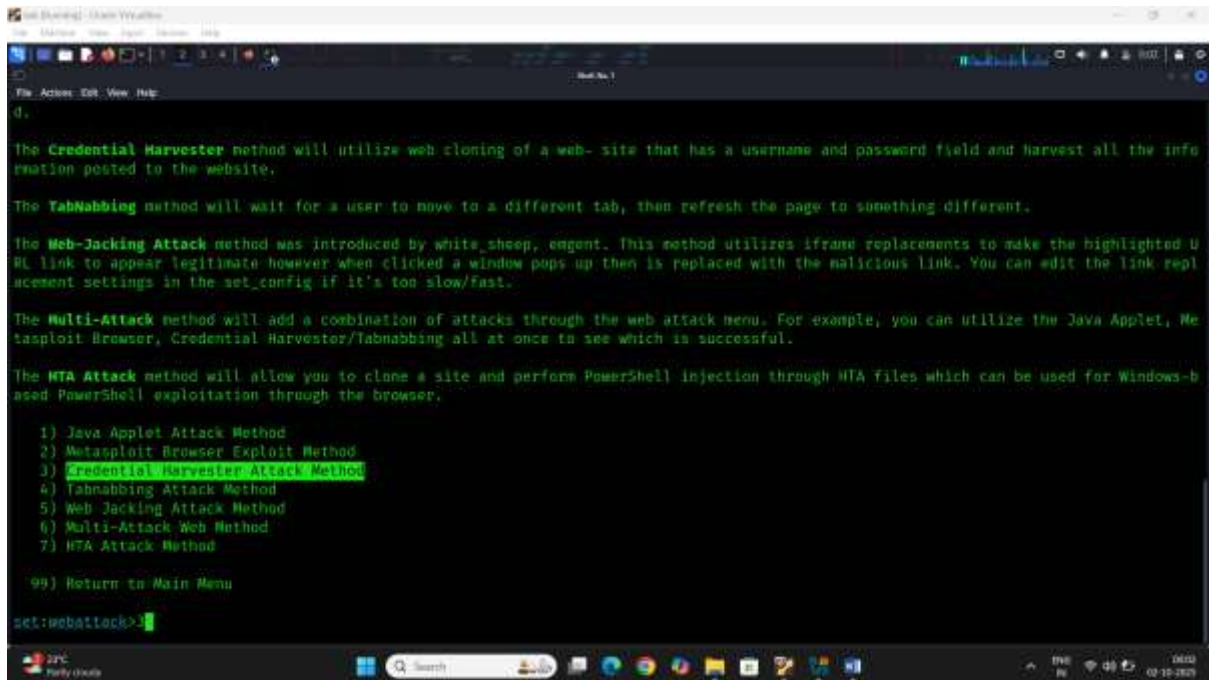
1) Spear-Phishing Attack Vectors
2) Website Attack Vectors
3) Infectious Media Generator
4) Create a Payload and Listener
5) Mass Mailer Attack
6) Arduino-Based Attack Vector
7) Wireless Access Point Attack Vector
8) QRCode Generator Attack Vector
9) Powershell Attack Vectors
10) Third Party Modules

99) Return back to the main menu.

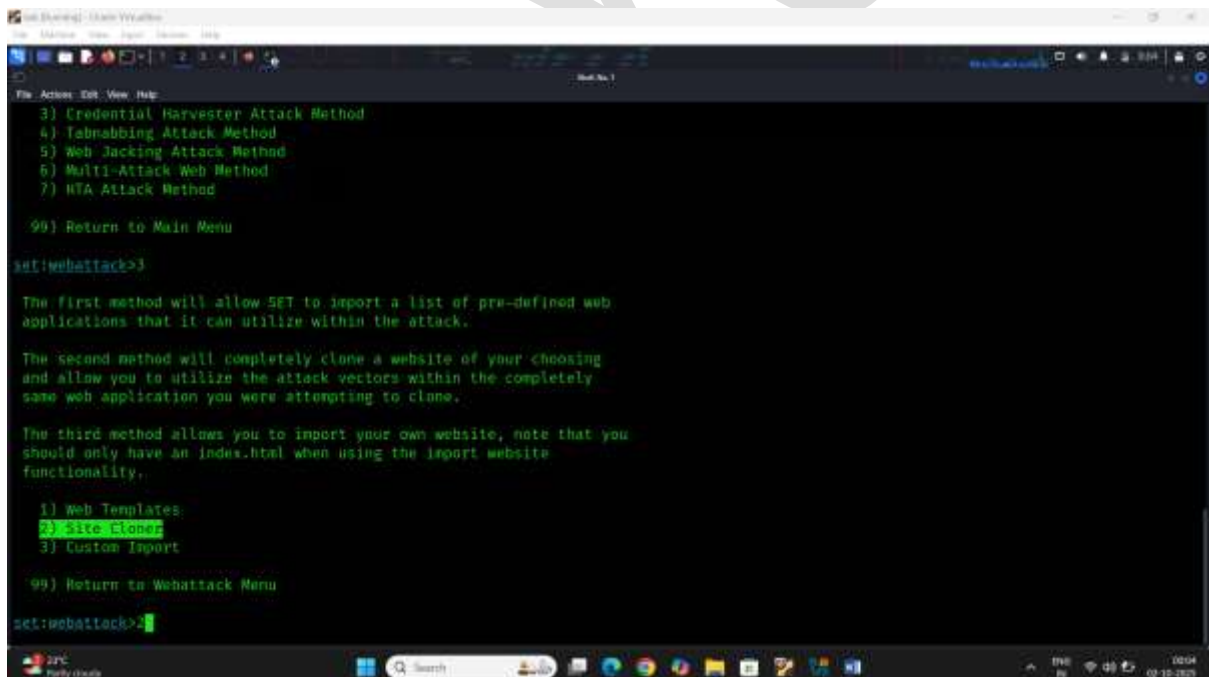
set> 2
```



## Step4 select the credential harvester attack method



```
set:webattack>3
```



```
set:webattack>2
```

## Step5 select the option site cloner

## Step6 type the klai linux url



```
set:webattack> 2) Site Cloner
3) Custom Import

99) Return to Webattack Menu

set:webattack>2
[-] Credential harvester will allow you to utilize the clone capabilities within SET
[-] 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 [10.76.163.45]: 10.76.163.45
```

```
set:webattack> 99) Return to Webattack Menu

set:webattack>2
[-] Credential harvester will allow you to utilize the clone capabilities within SET
[-] to harvest credentials or parameters from a website as well as place them into a report

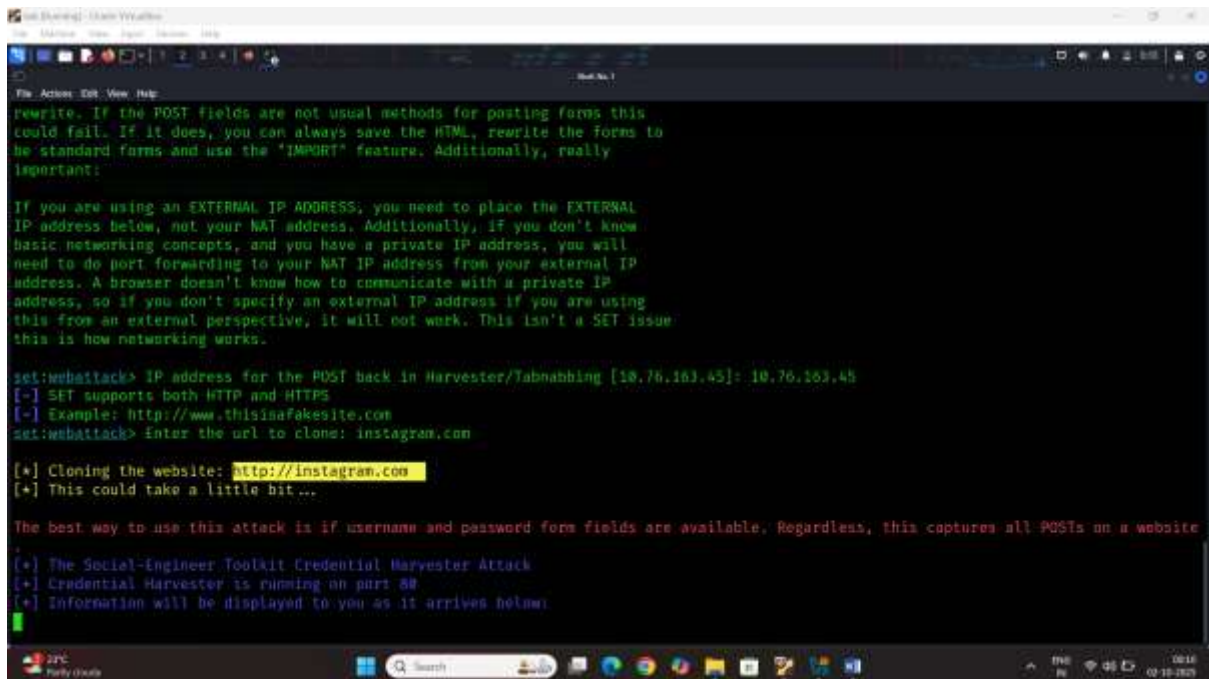
--- * IMPORTANT * READ THIS BEFORE ENTERING IN THE IP ADDRESS * IMPORTANT * ---

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 [10.76.163.45]: 10.76.163.45
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone: instagram.com
```

## Step7 clone website Instagram.com



```
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.

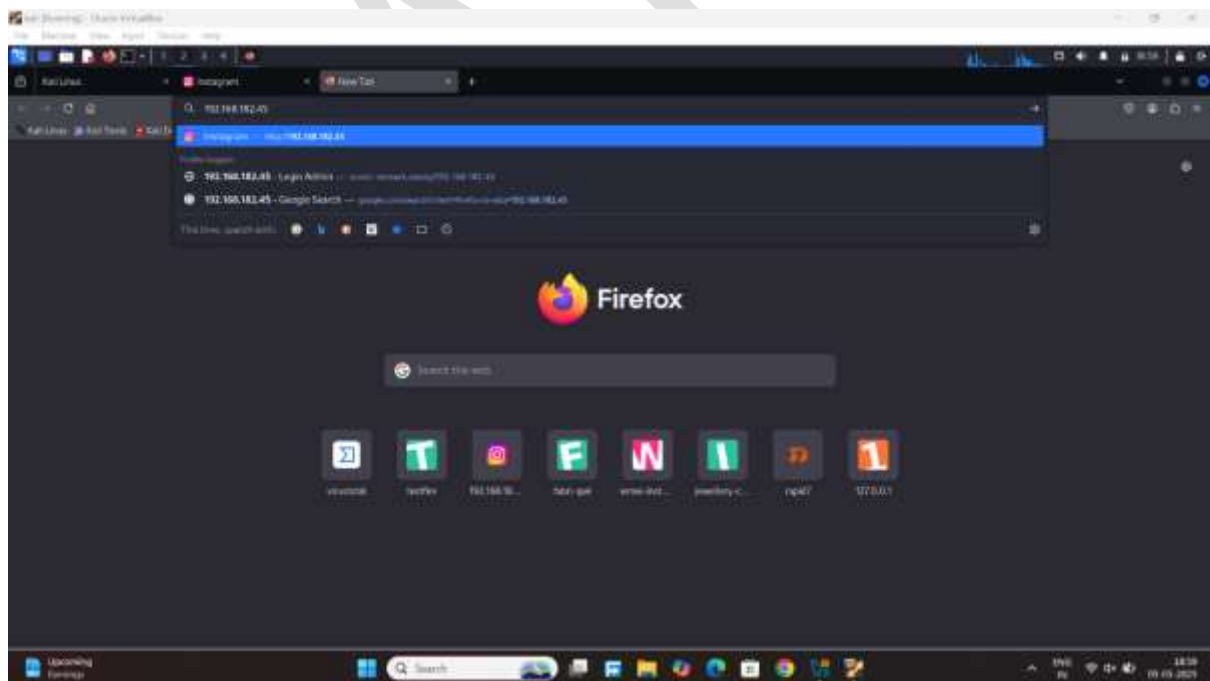
set:webattack> IP address for the POST back in Harvester/Tabnabbing [10.76.163.45]: 10.76.163.45
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone: instagram.com

[*] Cloning the website: http://instagram.com
[*] This could take a little bit...

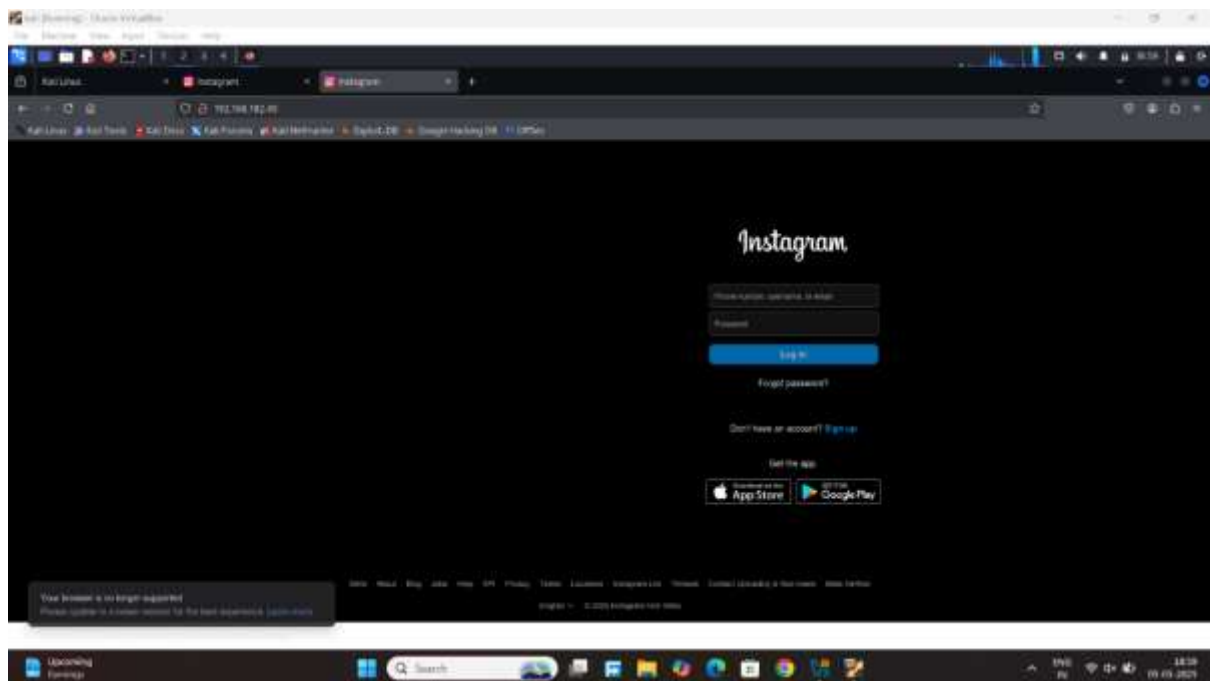
The best way to use this attack is if username and password form fields are available. Regardless, this captures all POSTs on a website

[*] The Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:
```

Type the kali linux ip and send the target



**Result:** successful open the site

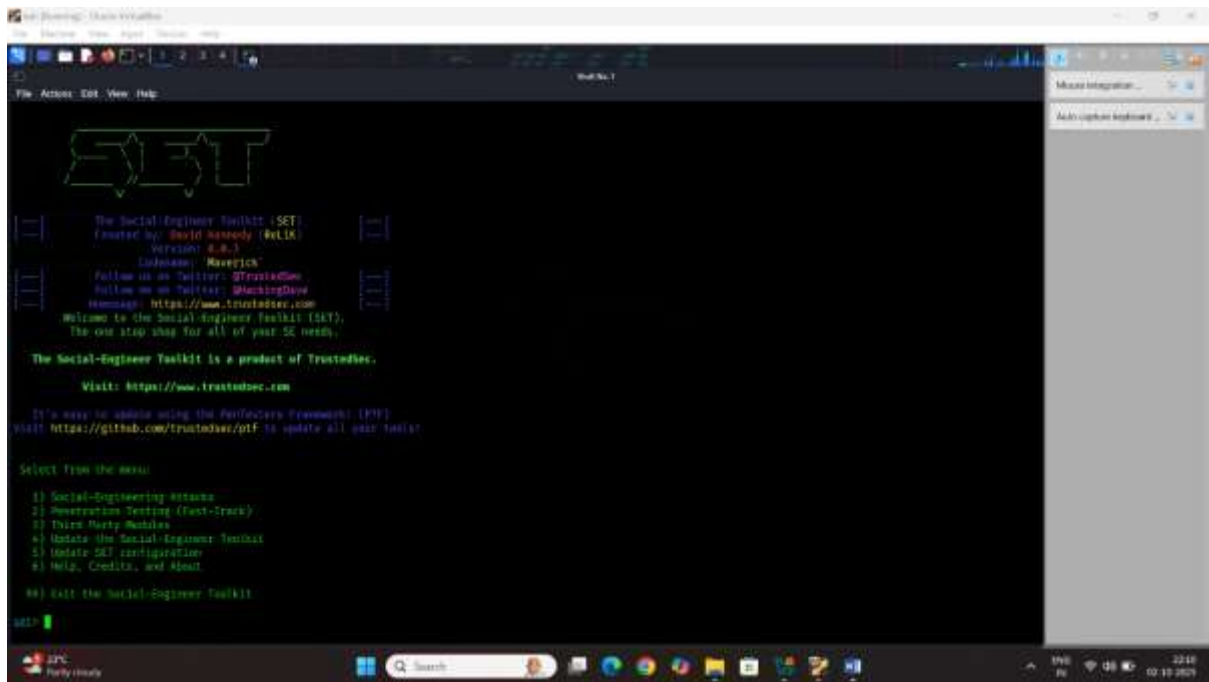


**Task2: how to create fishing email and sent to the target using Social engineering tool**

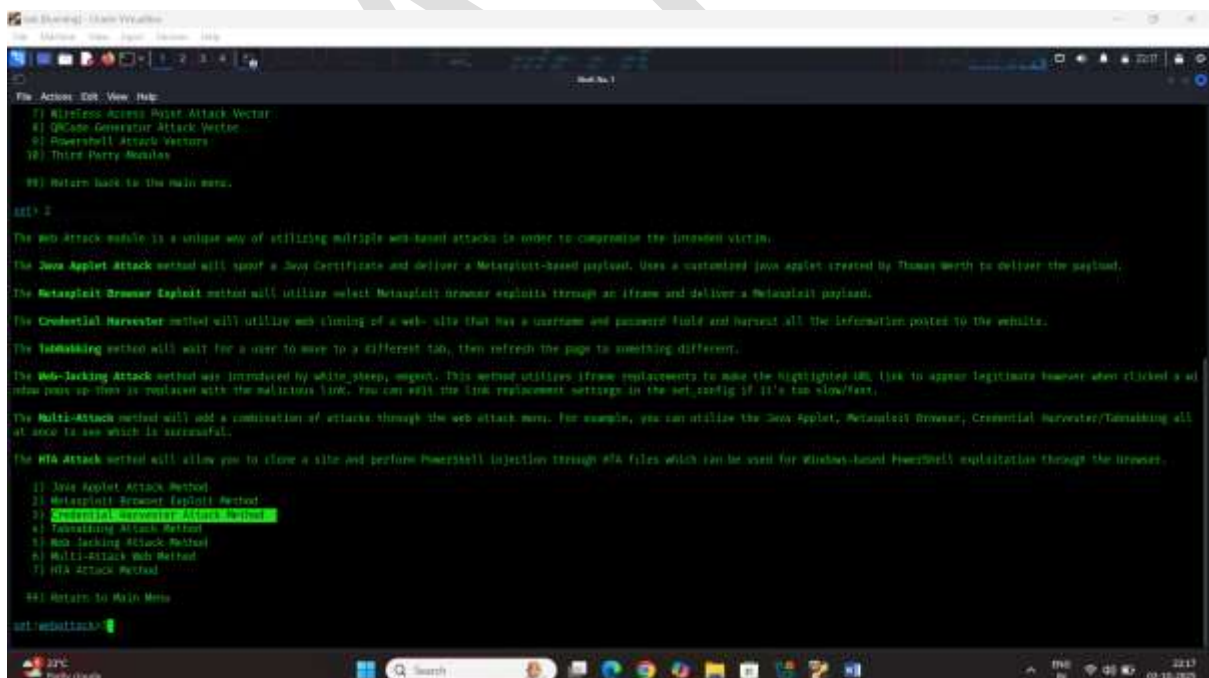
Step1: open the kali Linux terminal and Search the social engineering tool

Step2: open the set tool kit choice the option

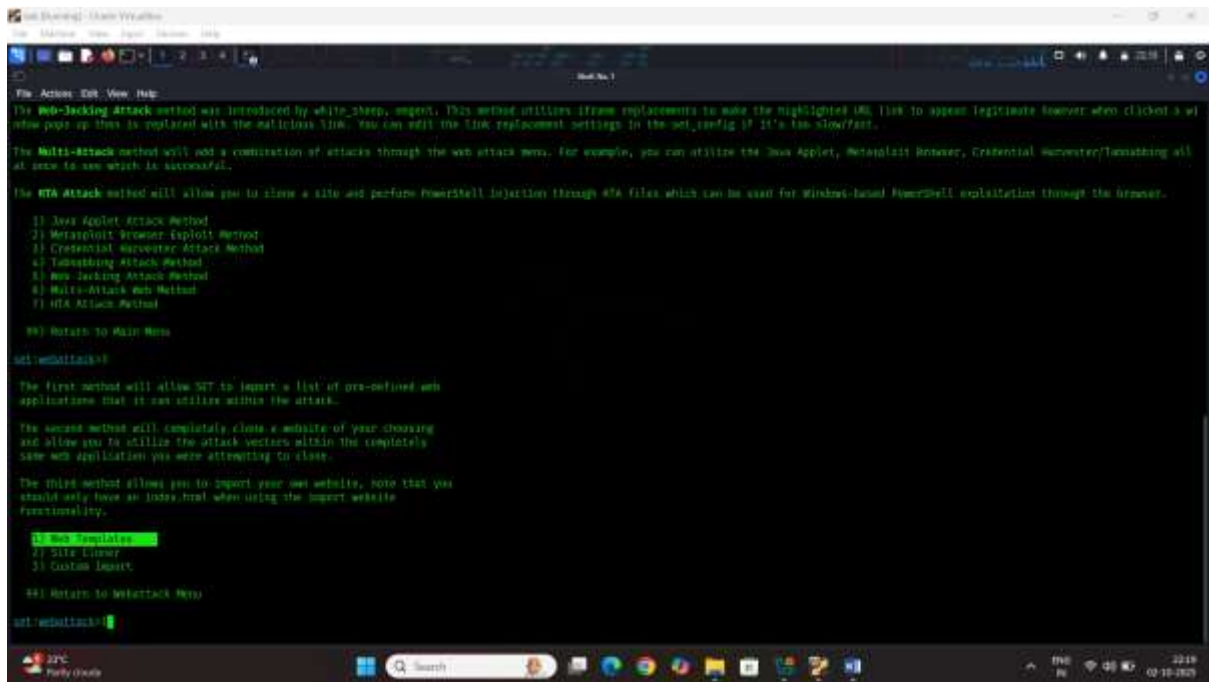
1 Social engineering



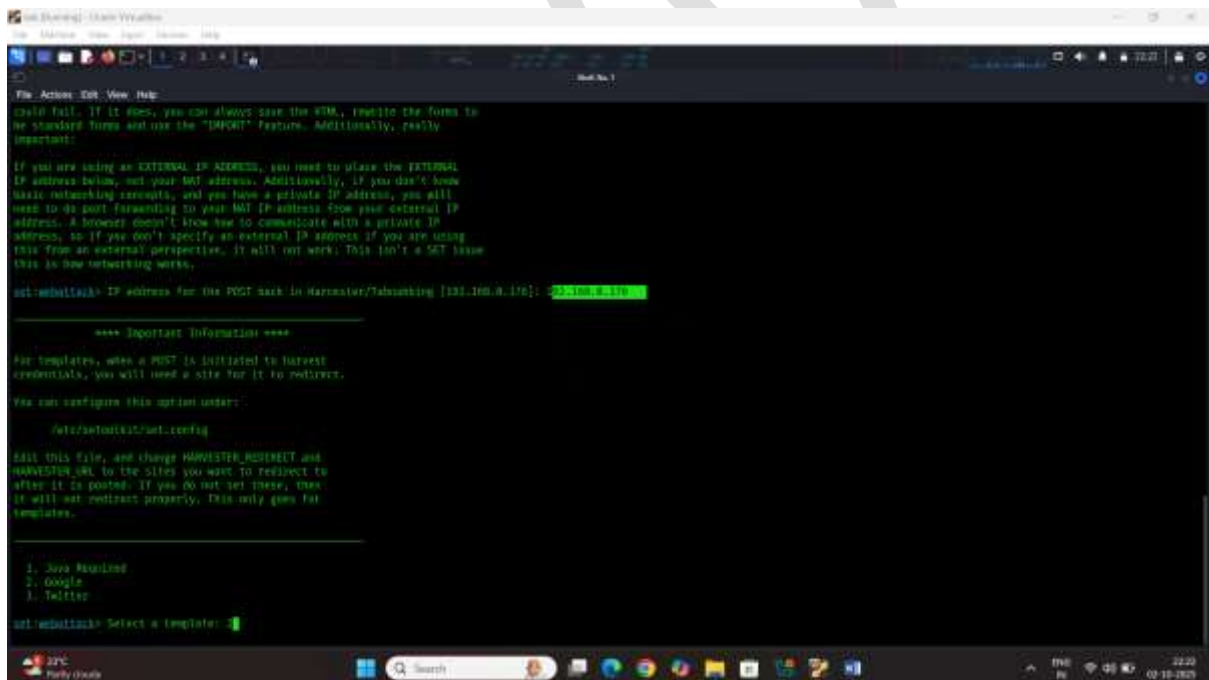
Step3 select the option  
credential harvester attack method



Step4 select the option web template



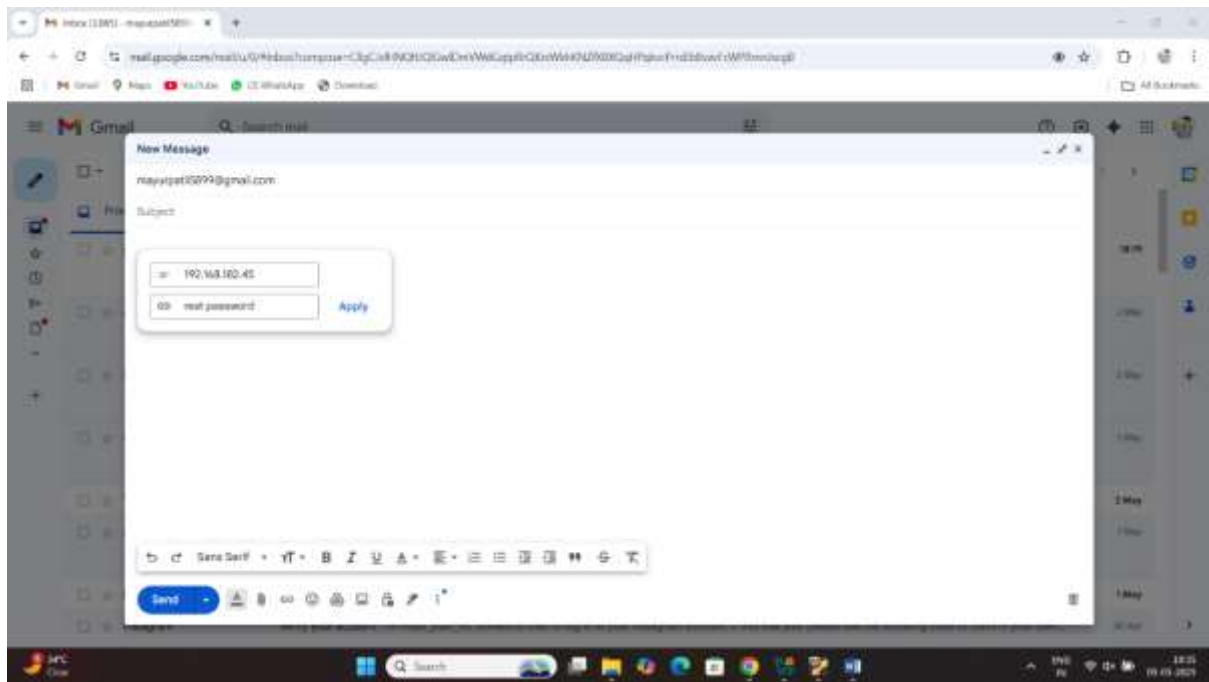
Step5 select the option web templet



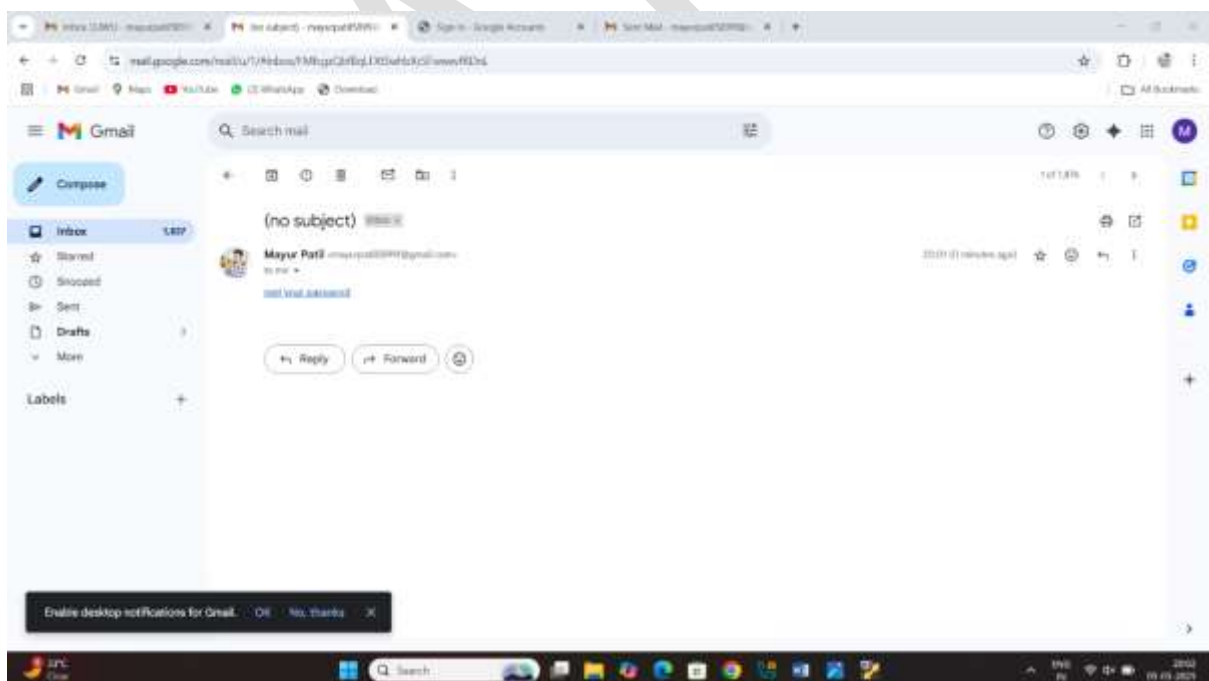
Step6 select the option google

Step8: open the email create the fishing email click on insert link type the kali linux ip

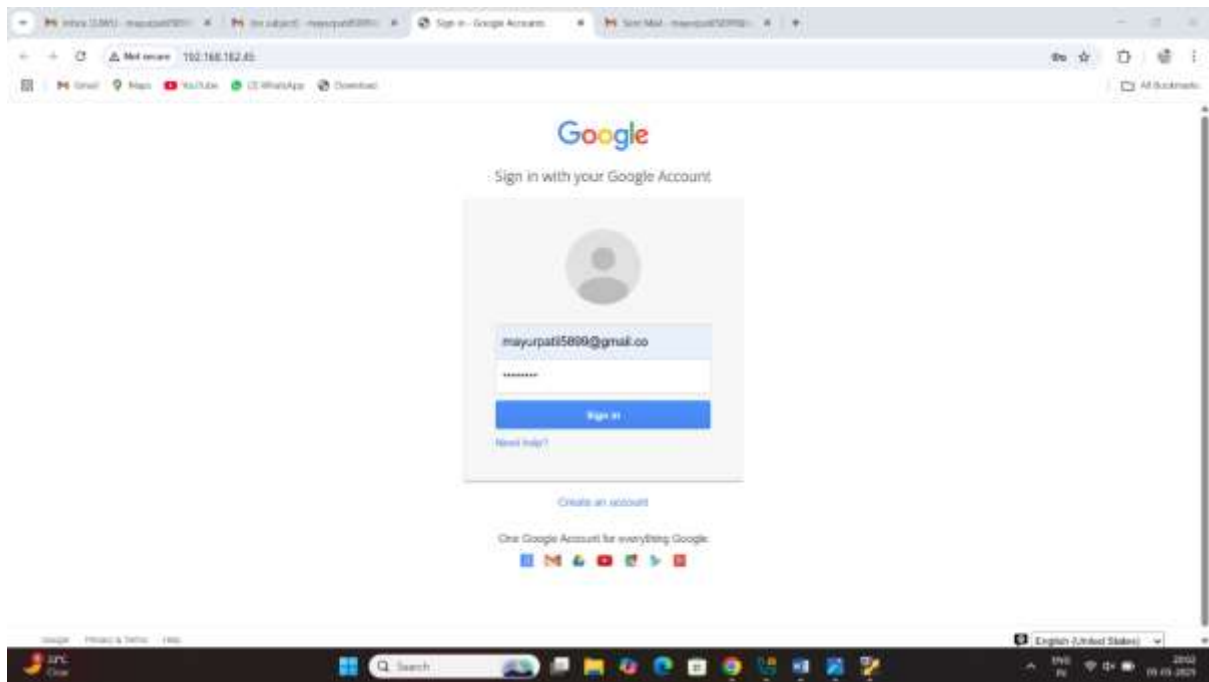




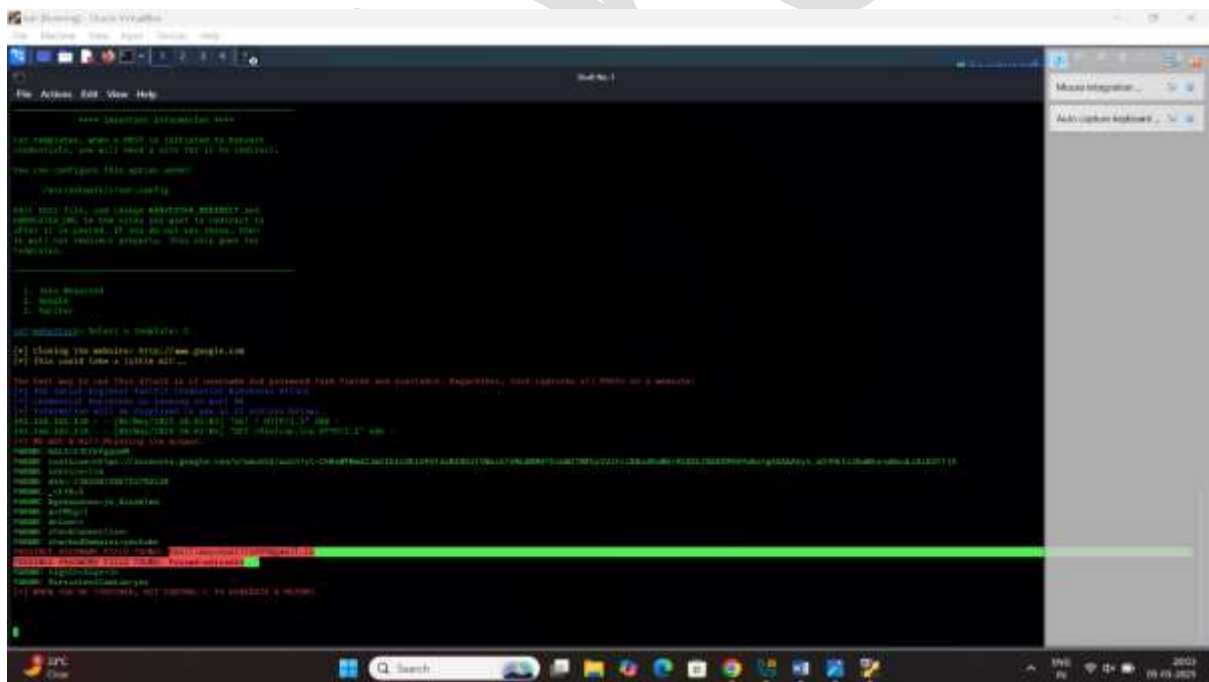
Send it email the target my target email is [mayurpatil5899@gmail.com](mailto:mayurpatil5899@gmail.com)



Open the target link and login gmail id



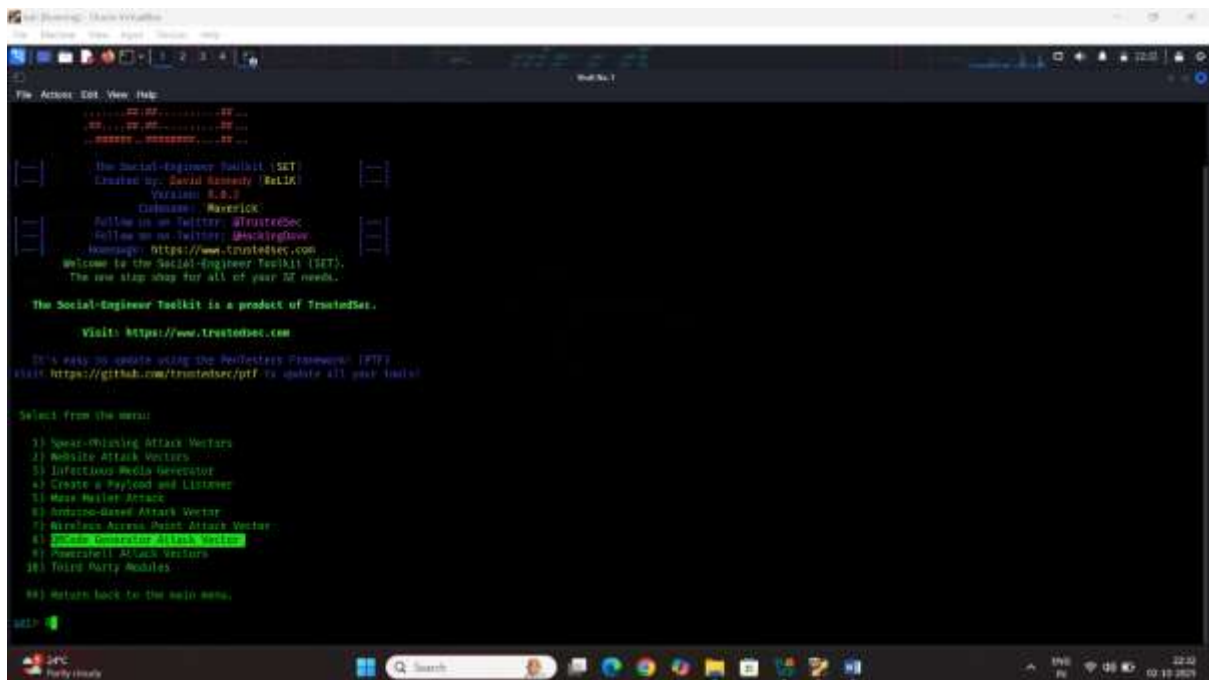
Click on sign  
Result:



**Extra Activity Using Set tool kit Generate the fake Q AR code**



Step1: go to kali linux open the set tool kit



```

The Social-Engineer Toolkit (SET)
Created by: David Kennedy (ReL1K)
Version: 5.0.5
Username: Maverick
Follow us on Twitter: @TrustedSec
Follow us 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 RedFolks Framework (RFF)
Visit https://github.com/trustedsec/rff to update all your tools!

Select from the menu:

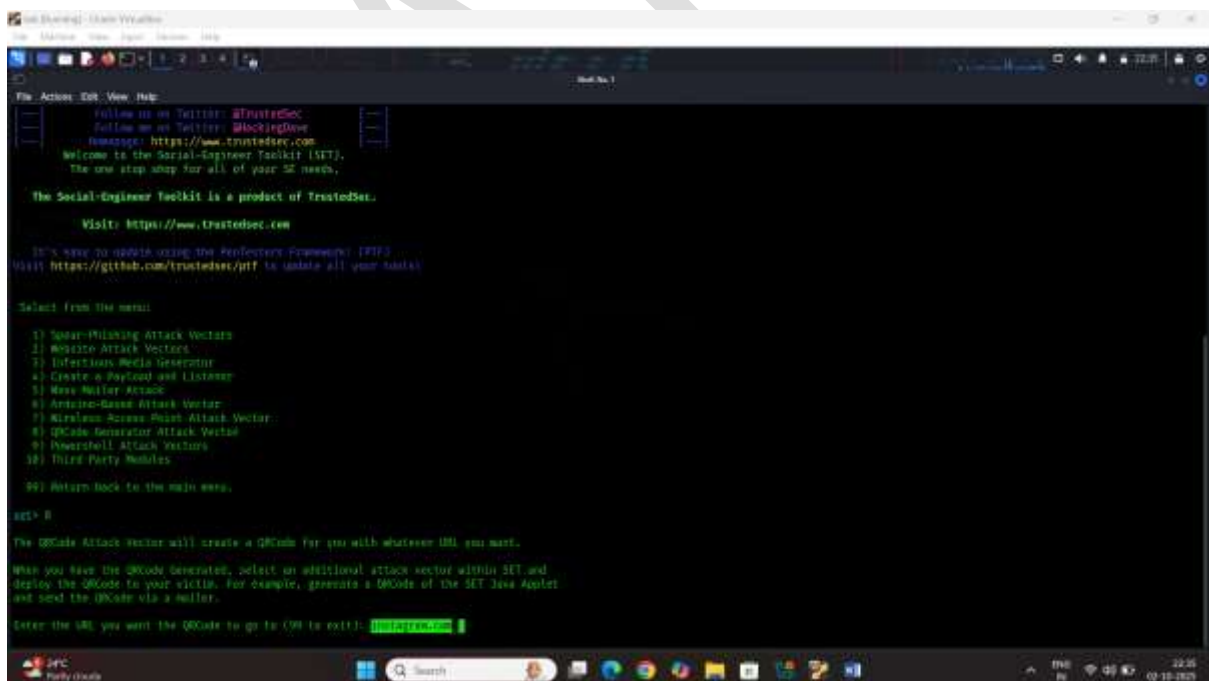
1) Spear-Phishing Attack Vectors
2) Website Attack Vectors
3) Infectious Media Generator
4) Create a Payload and Listener
5) Mass Mailer Attack
6) Android-based Attack Vector
7) Wireless Access Point Attack Vector
8) QRCode Generator Attack Vector
9) Powershell Attack Vectors
10) Third Party Modules

99) Return back to the main menu.

set> 
```

Step4: type the URL

Example: <https://instagram.com>



```

The Social-Engineer Toolkit (SET)
Created by: David Kennedy (ReL1K)
Version: 5.0.5
Username: Maverick
Follow us on Twitter: @TrustedSec
Follow us 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 RedFolks Framework (RFF)
Visit https://github.com/trustedsec/rff 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) Android-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> 8

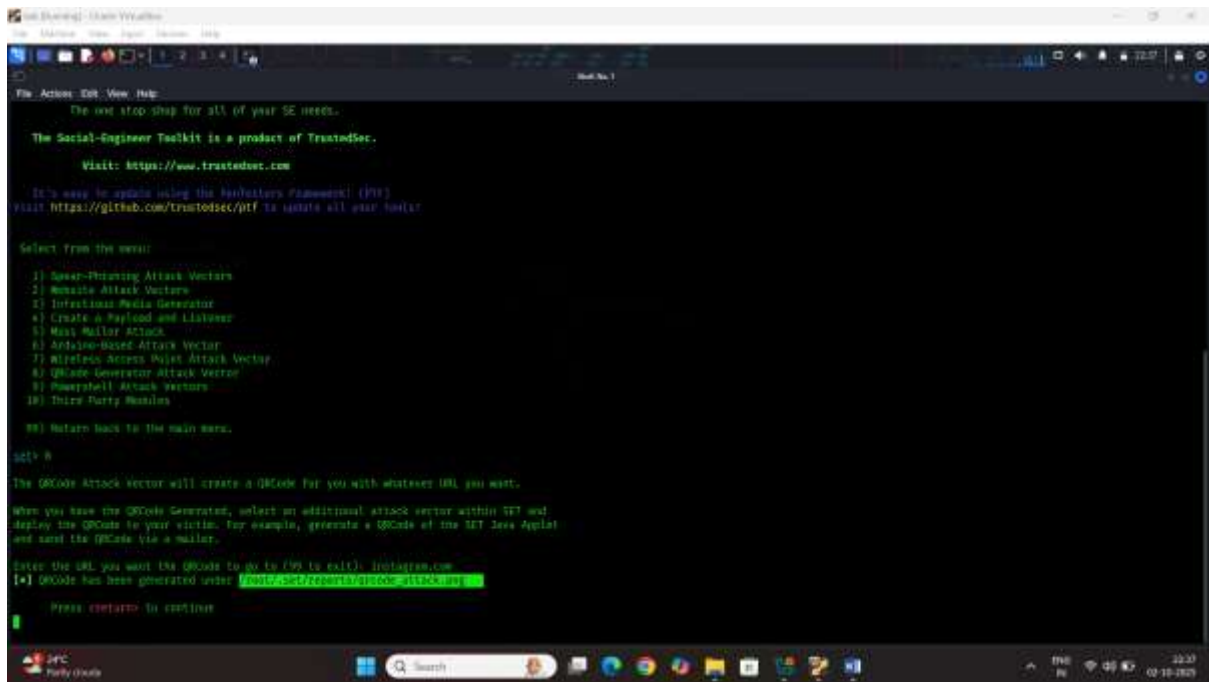
The QRCode Attack Vector will create a QRcode for you with whatever URL you want.

When you have the QRcode generated, select an additional attack vector within SET and
deploy the QRcode to your victim. For example, generate a QRcode of the SET Java Applet
and send the QRcode via a mailer.

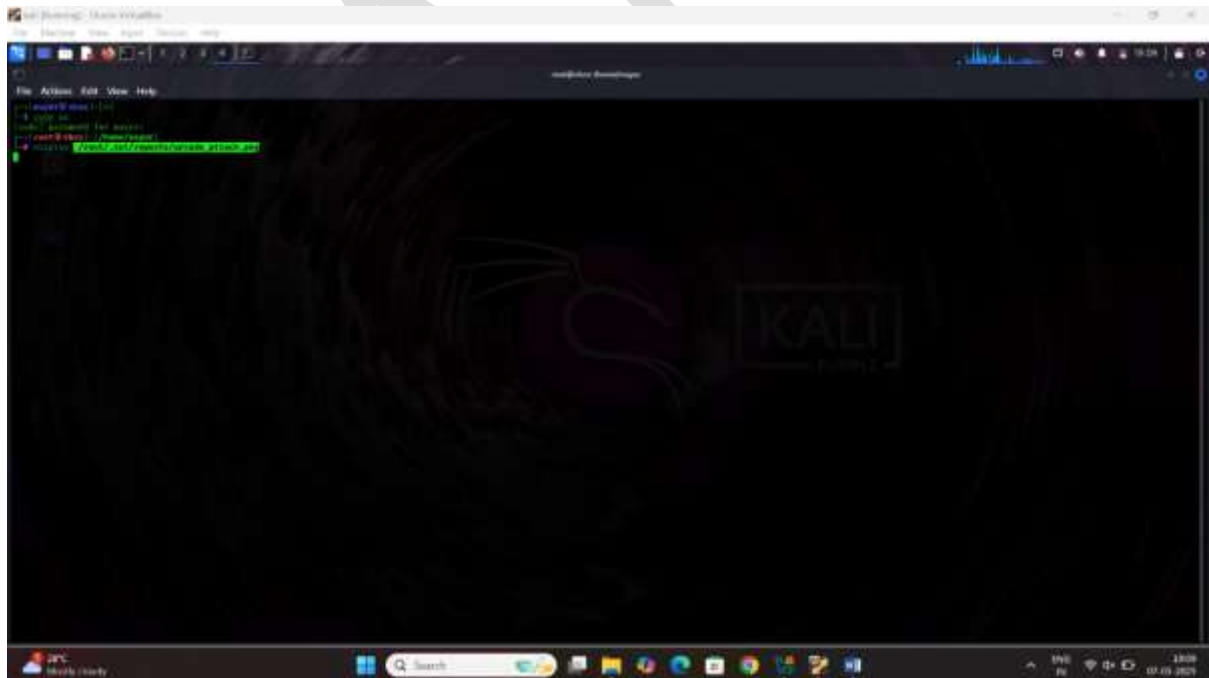
Enter the URL you want the QRcode to go to (99 to exit): https://instagram.com

```

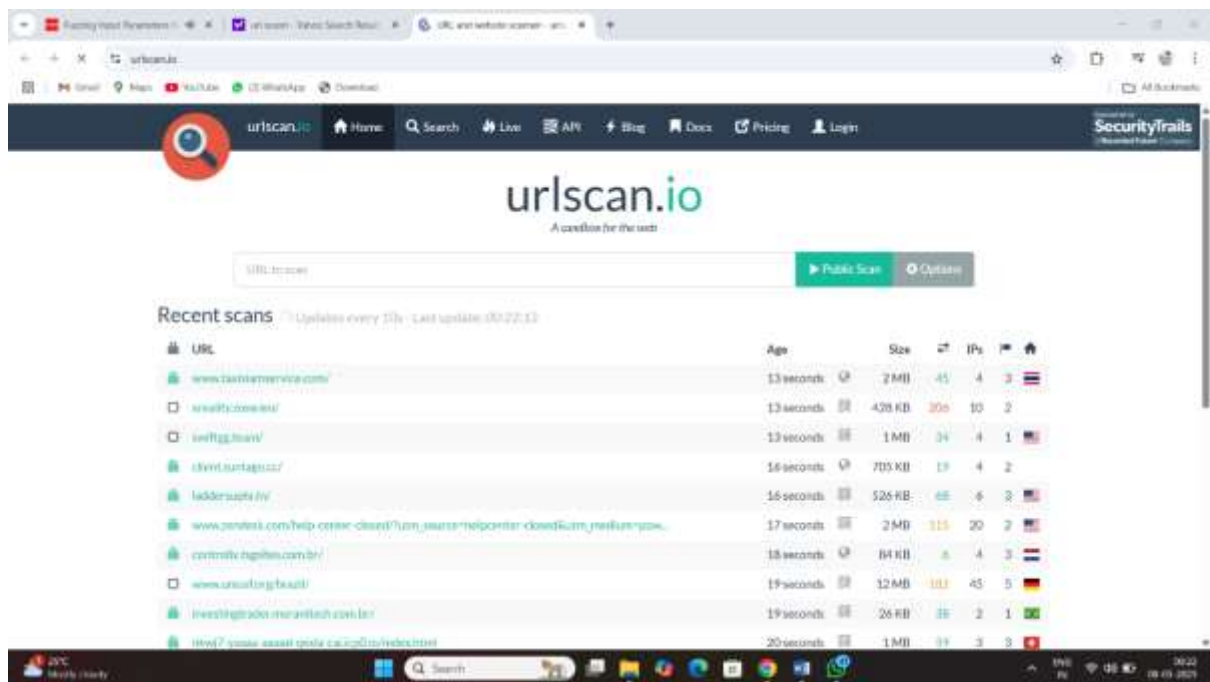
Step5 copy the root option



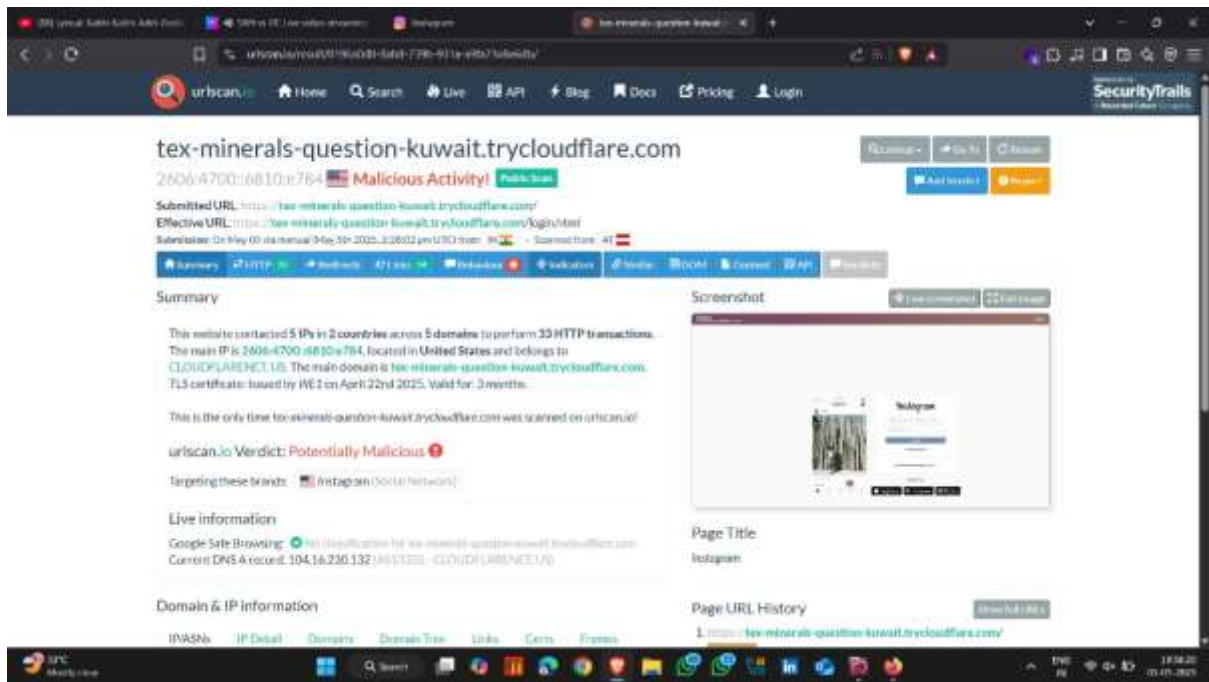
**Step6:** open the kali linux terminal copy the root link past it terminal





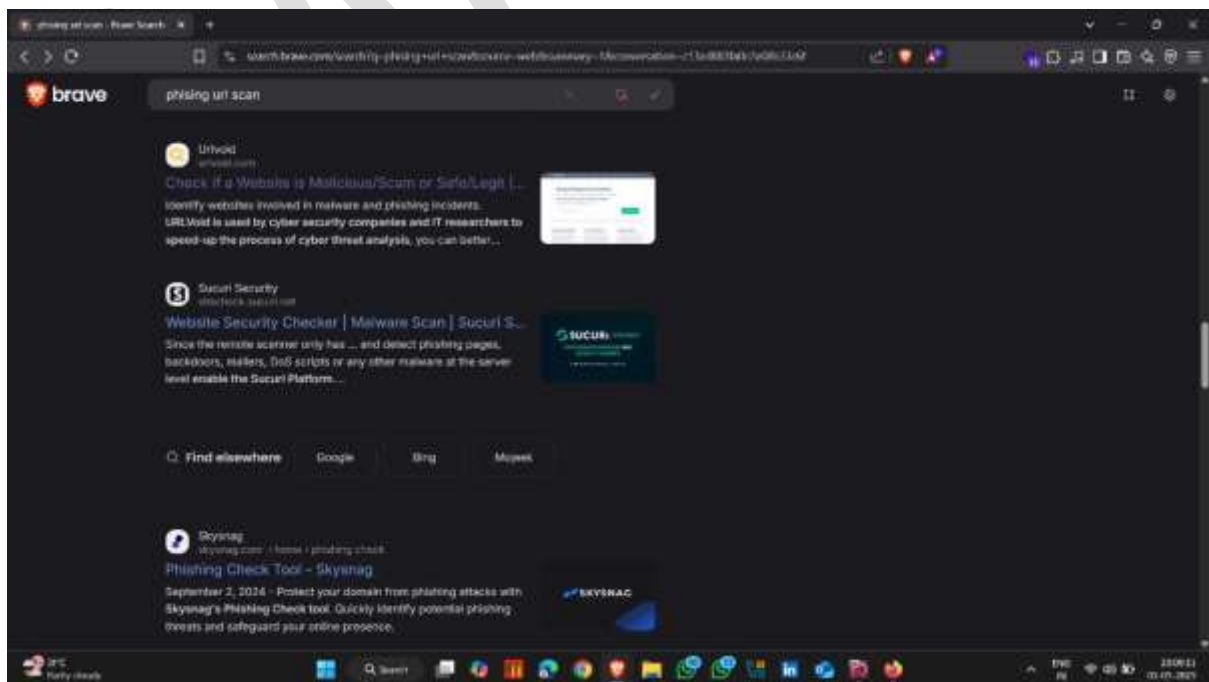


Result:

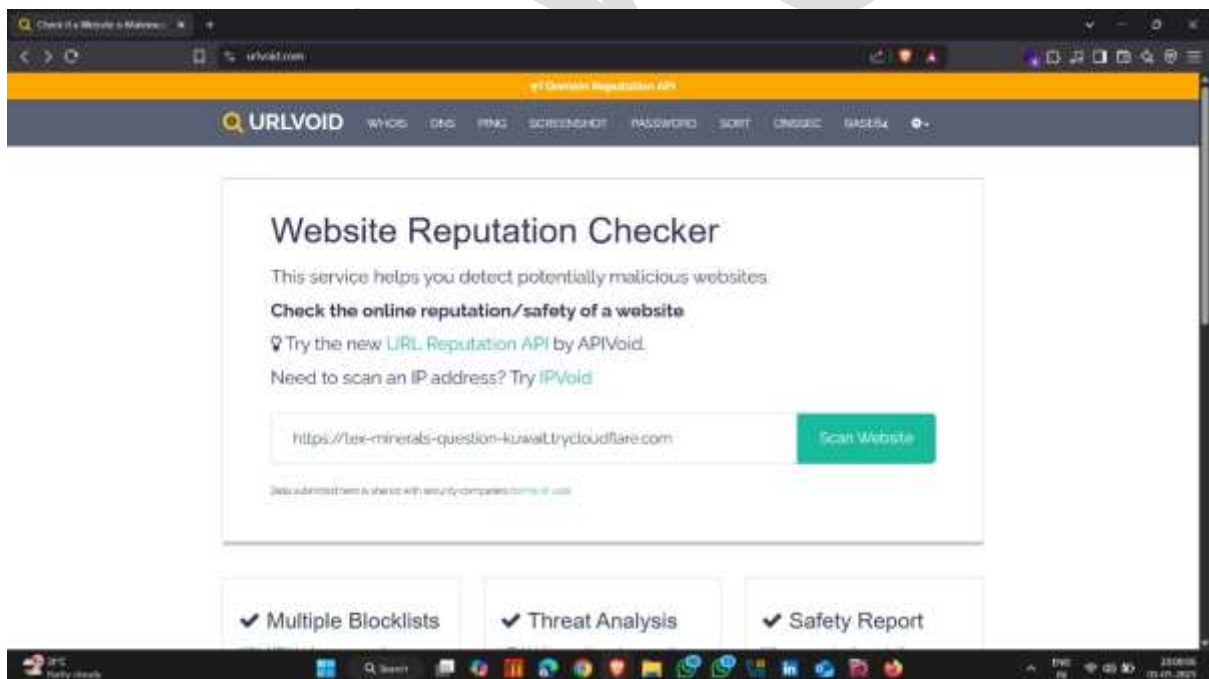
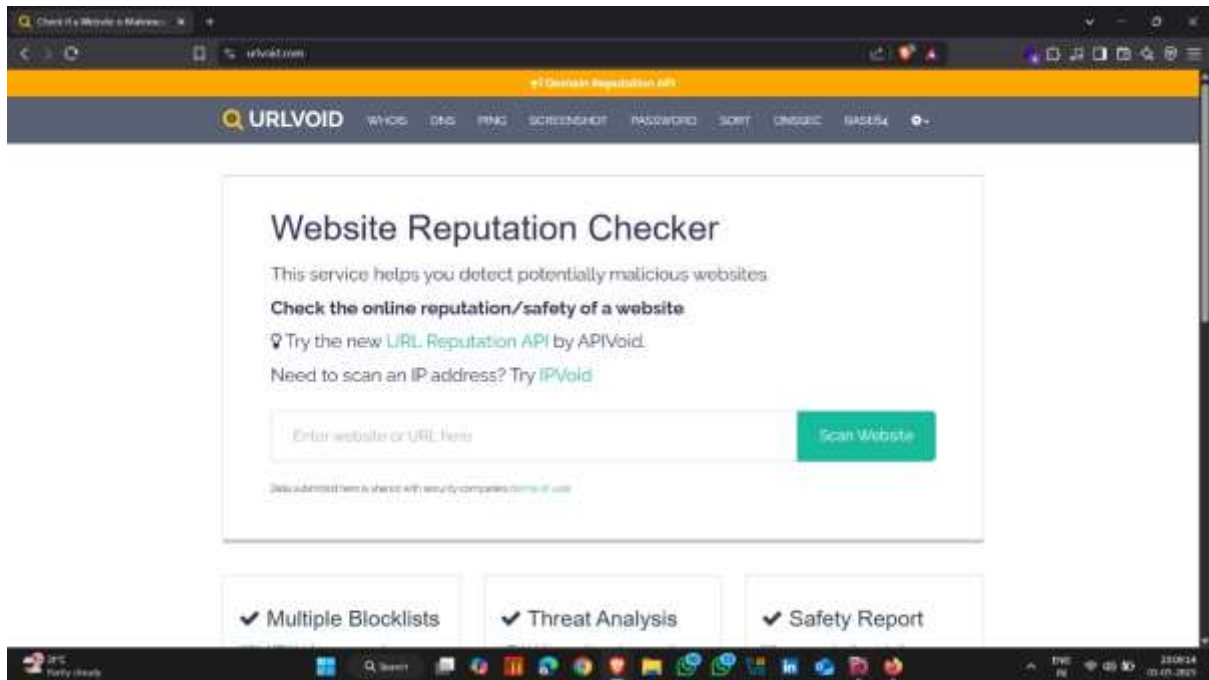


## 3 Extra Activity using website for fishing URL detections

1 web site name: URLvoid

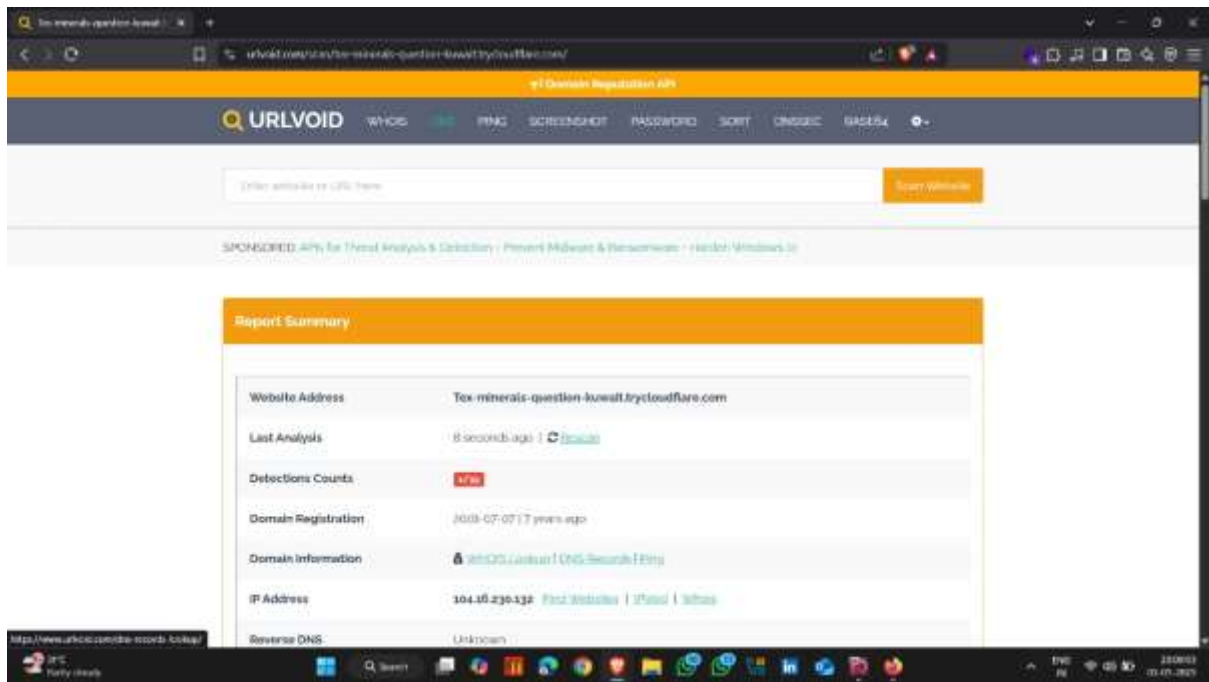


Open the web site

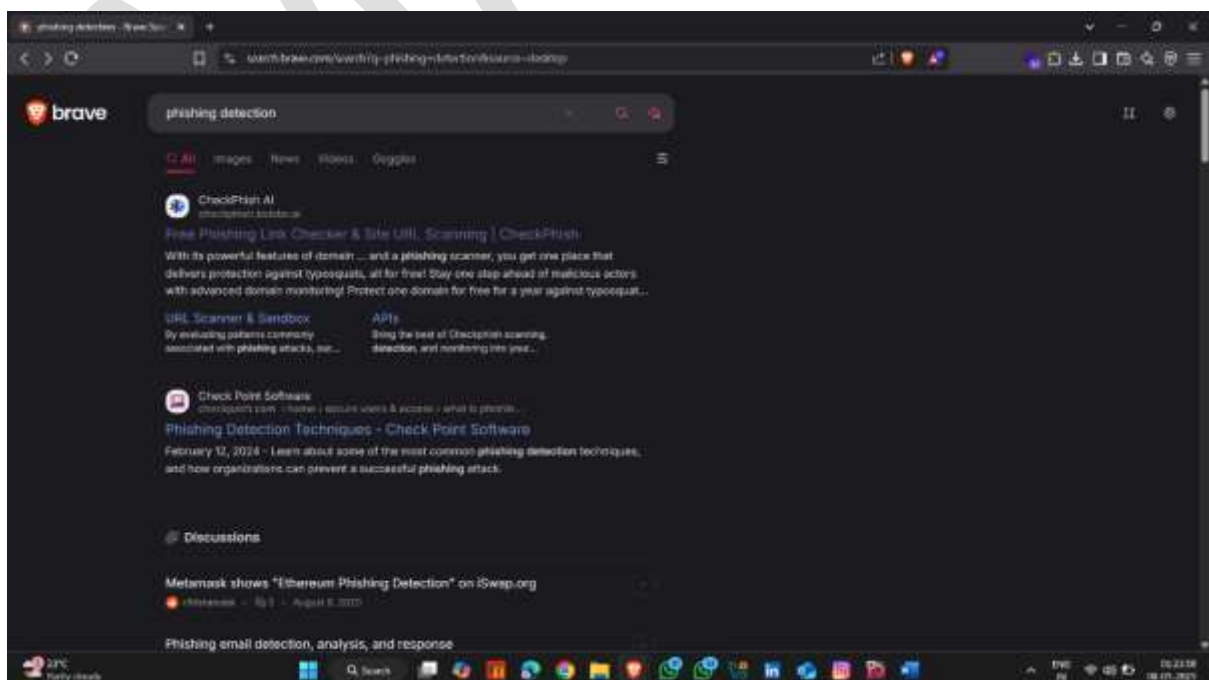


Result :

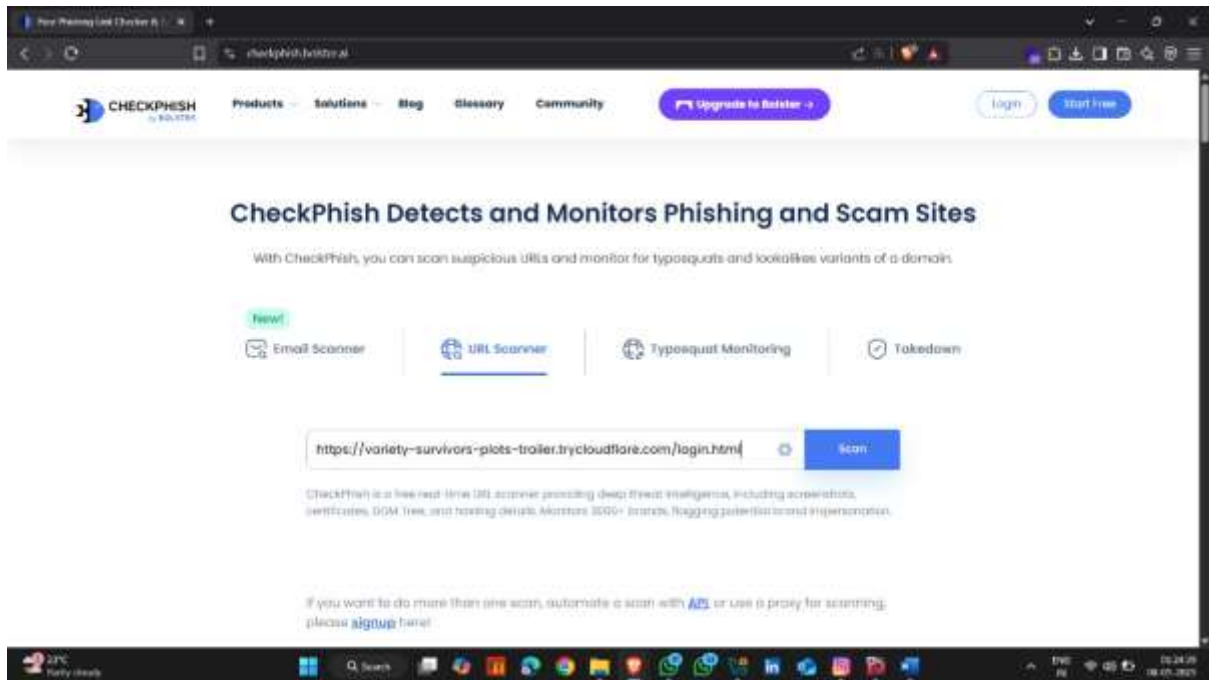




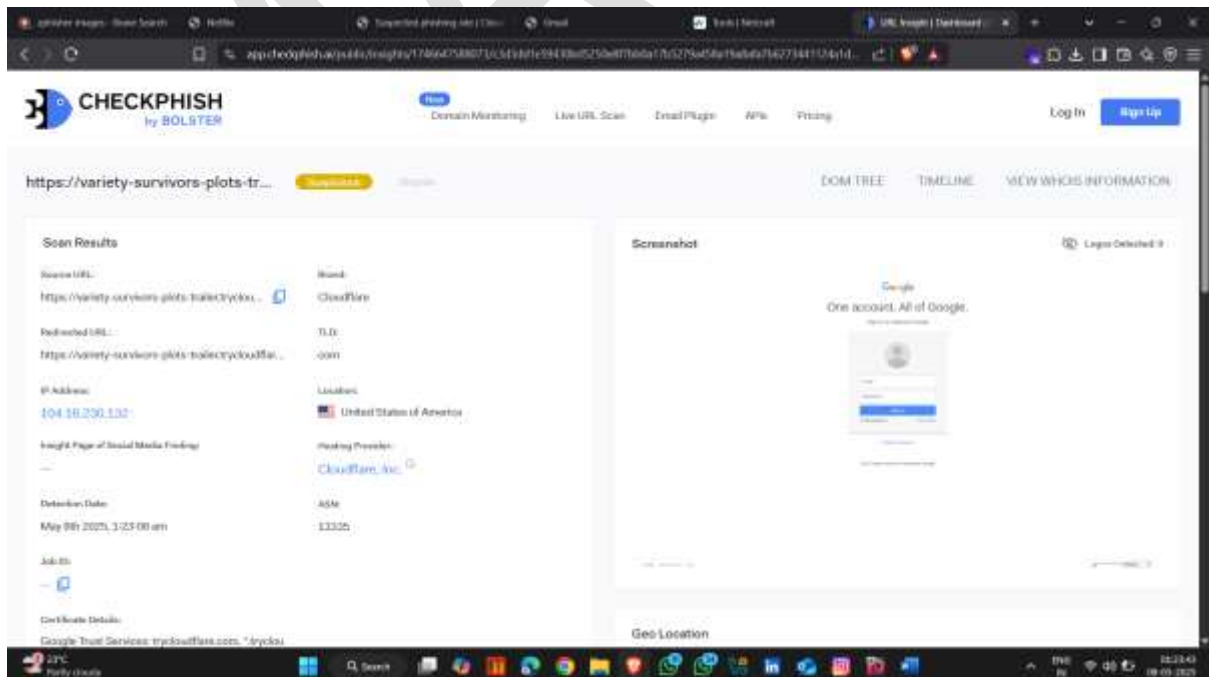
## 4 Extra Activity using website for fishing URL detections







## Result:



MAYUR