

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 QR 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

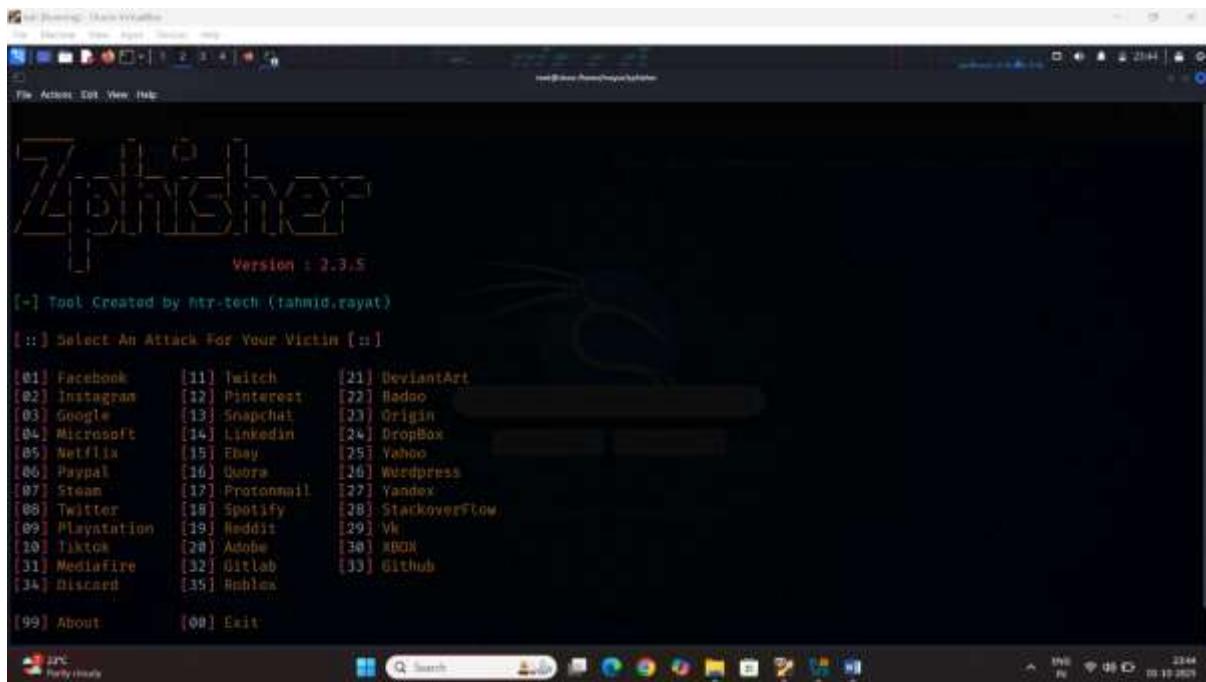
Step2 go to Zphisher



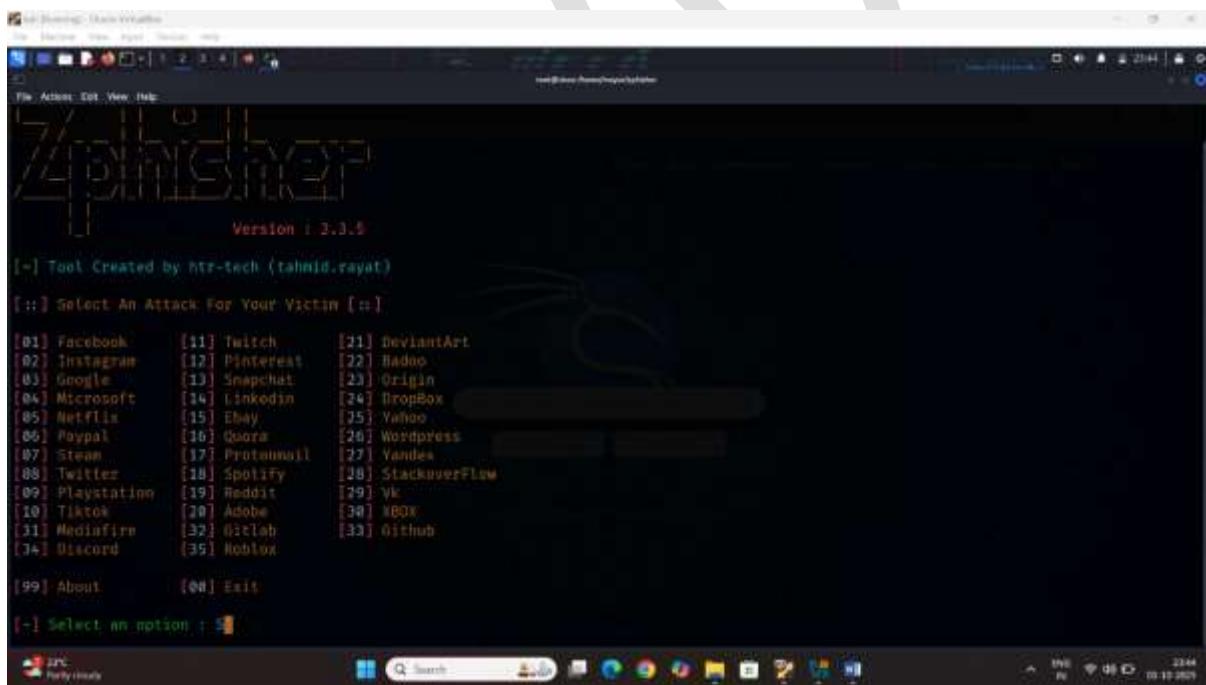
```
Mayur@Mayur-VirtualBox: ~
```

```
[Mayur@vbox ~]$ sudo su
[sudo] password for Mayur:
[Mayur@vbox ~]$ cd zphisher
[Mayur@vbox ~]$ ls
auth Dockerfile LICENSE make-deb.sh README.md run-docker.sh scripts zphisher.sh
[Mayur@vbox ~]$
```

The screenshot shows a terminal window titled "Mayur@Mayur-VirtualBox: ~". The user has root privileges. They have navigated to the directory "/home/mayur/zphisher" and listed its contents. The terminal is running on a Kali Linux host, as evidenced by the desktop environment icons in the taskbar.



Step3 select the 5 option



Step4 use 2 option

```
[!] Starting: Main Interface
File Actions Edit View Help
[!] ZEPHISHER 2.3.5
[01] Localhost [Auto Detects]
[02] CloudFlared [Auto Detects]
[03] LocalXpose [NEW! Max 15Min]
[-] Select a port forwarding service : 2
```

```
[!] Starting: Main Interface
File Actions Edit View Help
[!] ZEPHISHER 2.3.5
[01] Localhost [Auto Detects]
[02] CloudFlared [Auto Detects]
[03] LocalXpose [NEW! Max 15Min]
[-] Select a port forwarding service : 2
[?] Do You Want A Custom Port [y/N]: y
[+] Enter Your Custom 4-digit Port [1024-9999] : 5555
```

Step5 select the port option yes

Enter the port range 5555

Step6 enter the url Instagram.com

```
[+] Starting - User Watcher
File Edit View Insert Delete Help
File Actions Edit View Help
[+] Do you want to change Mask URL? [y/N] : y
[-] Enter your custom URL below (Example: https://get-free-followers.com)
=> https://

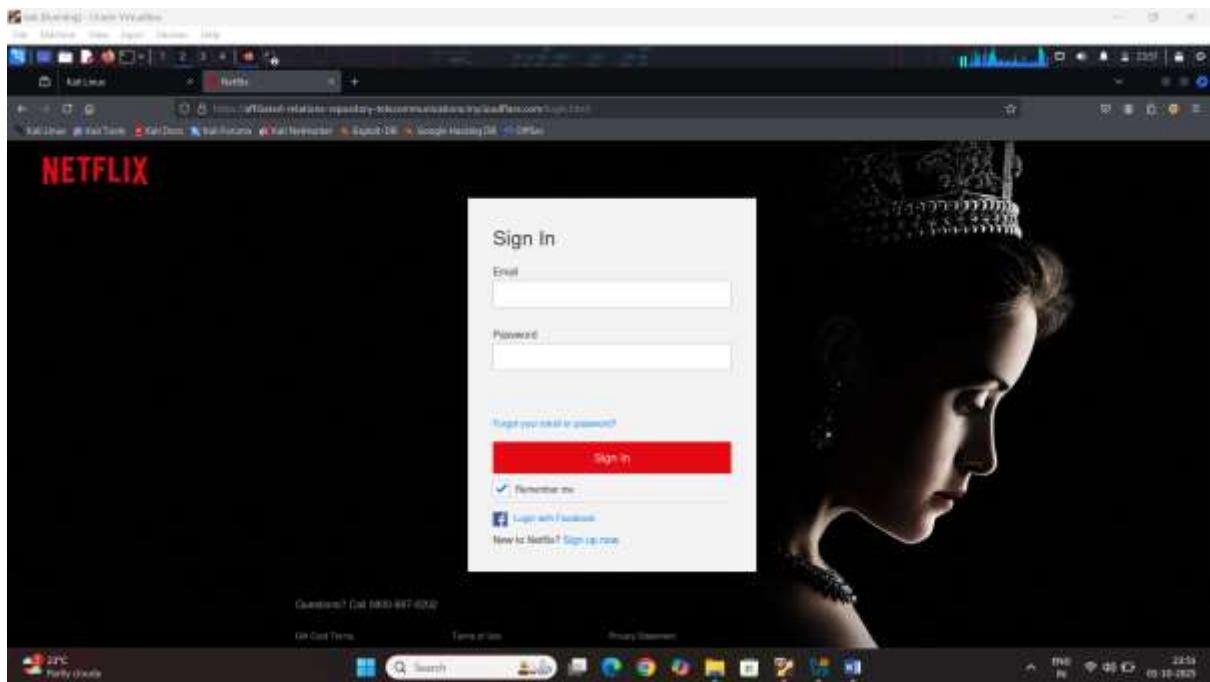
```

```
[+] Starting - User Watcher
File Edit View Insert Delete Help
File Actions Edit View Help
[+] URL 1 : https://affiliated-relations-repository-telecommunications.cloudflare.com
[+] URL 2 : https://
[+] URL 3 : https://instagram.com
[-] Waiting for Login Info, Ctrl + C to exit...[+]

```

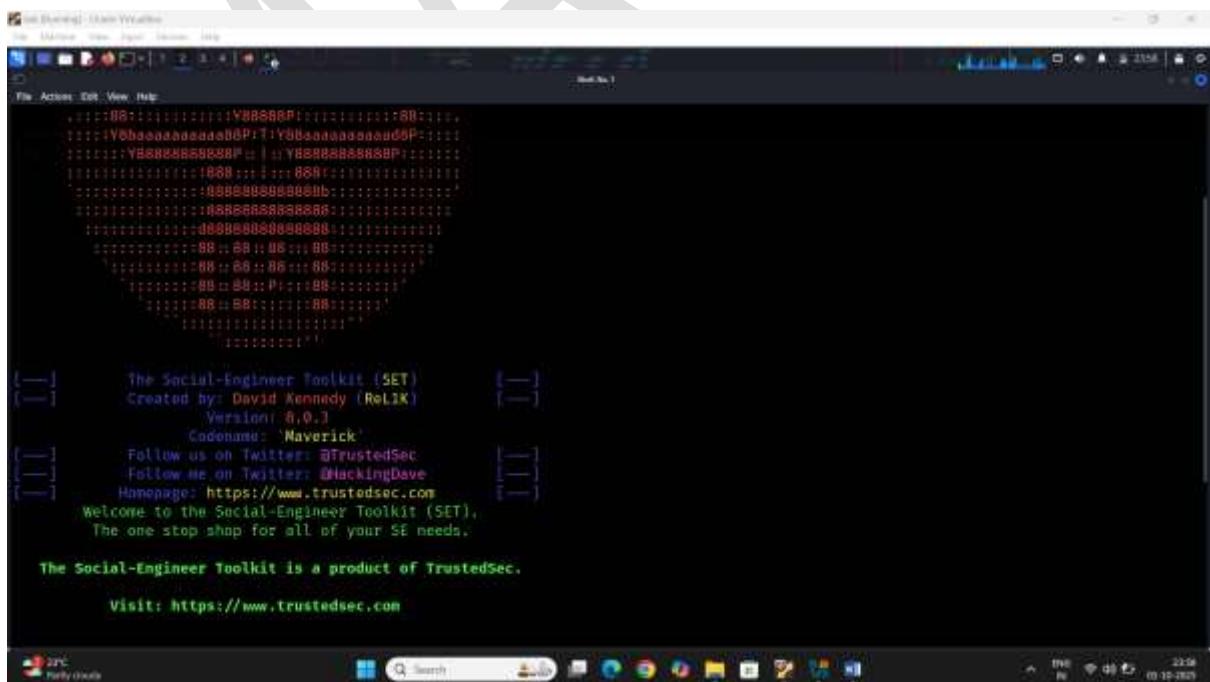
Step7 copy the 1st url and paste the chrome

Result:



Task 2 Create site cloner using Social Engineering tool

Step1 start the set tool kite



Step2 select the social engineering attack

```
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

```
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.

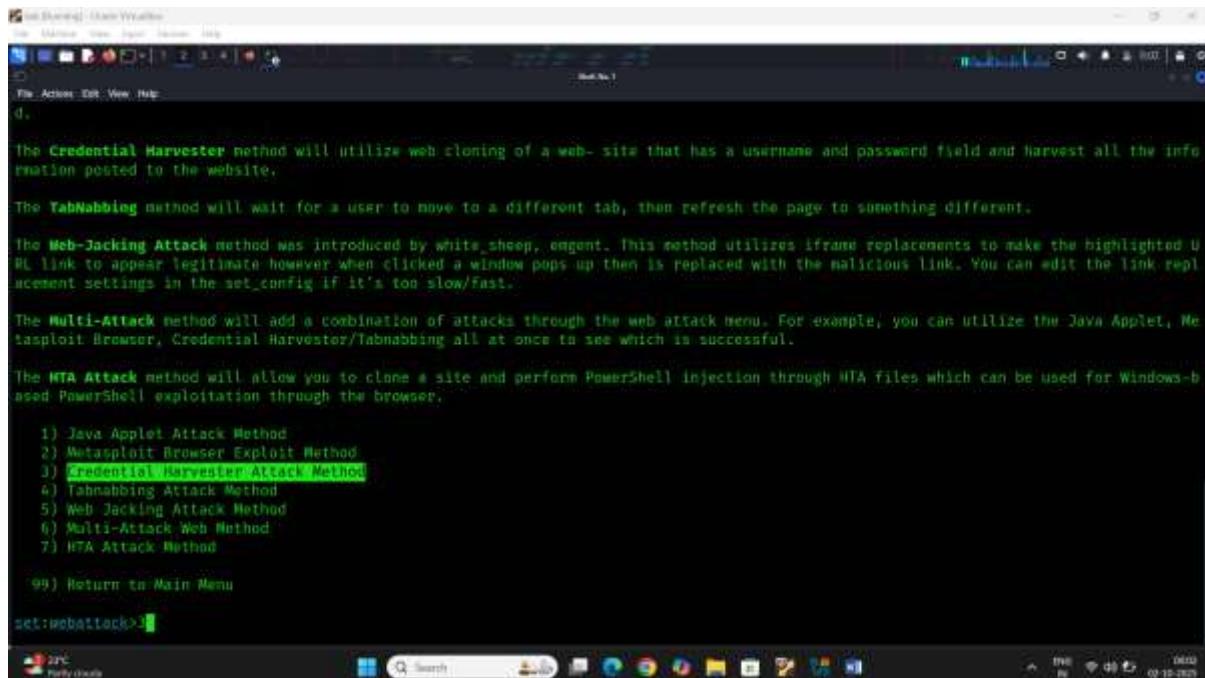
Visit: https://www.trustedsec.com

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

The Credential Harvester method will utilize web cloning of a website that has a username and password field and harvest all the information posted to the website.

The TabNabbing method will wait for a user to move to a different tab, then refresh the page to something different.

The Web-Jacking Attack method was introduced by white_sheep, emgent. This method utilizes iframe replacements 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.

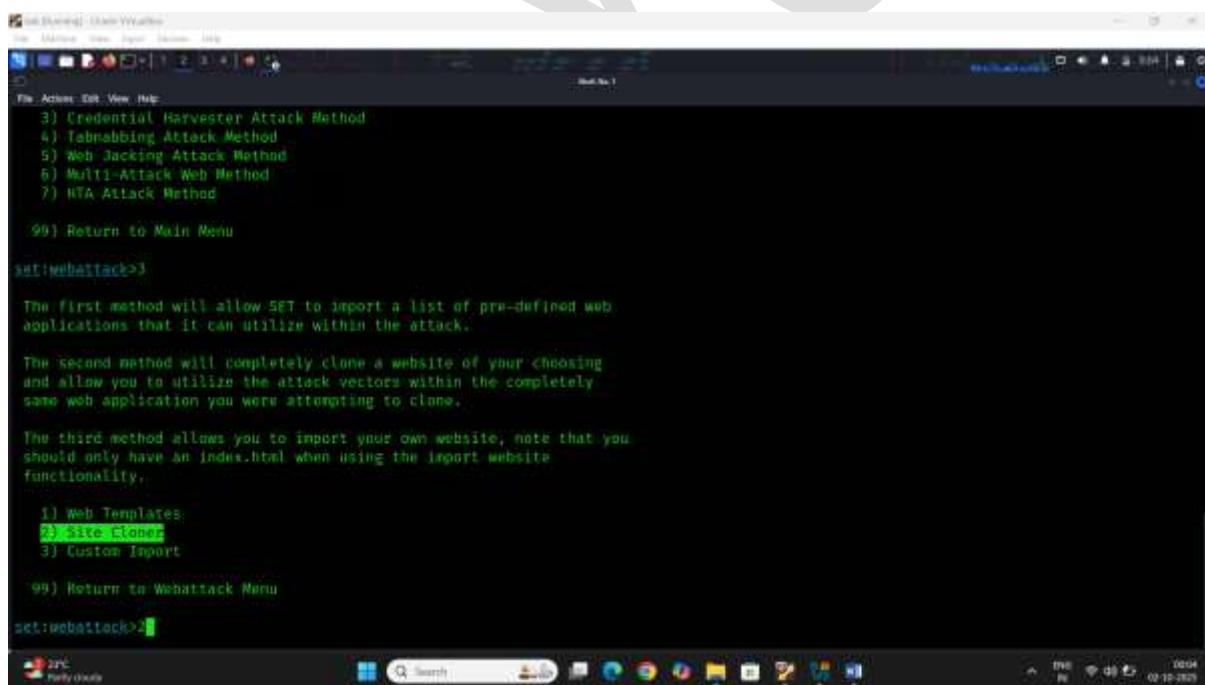
The Multi-Attack method will add a combination of attacks through the web attack menu. For example, you can utilize the Java Applet, Metasploit Browser, Credential Harvester/Tabnabbing all at once to see which is successful.

The HTA Attack method will allow you to clone a site and perform PowerShell injection through HTA files 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
```



```
set:webattack>3

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

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
```

Step5 select the option site cloner

Step6 type the klai linux url

```
set:Sharing - Share Webiste
File Edit View Help
File Actions Edit View Help
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 supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone: https://www.instagram.com/
```

```
set:Sharing - Share Webiste
File Edit View Help
File Actions Edit View Help
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: https://www.instagram.com/
```

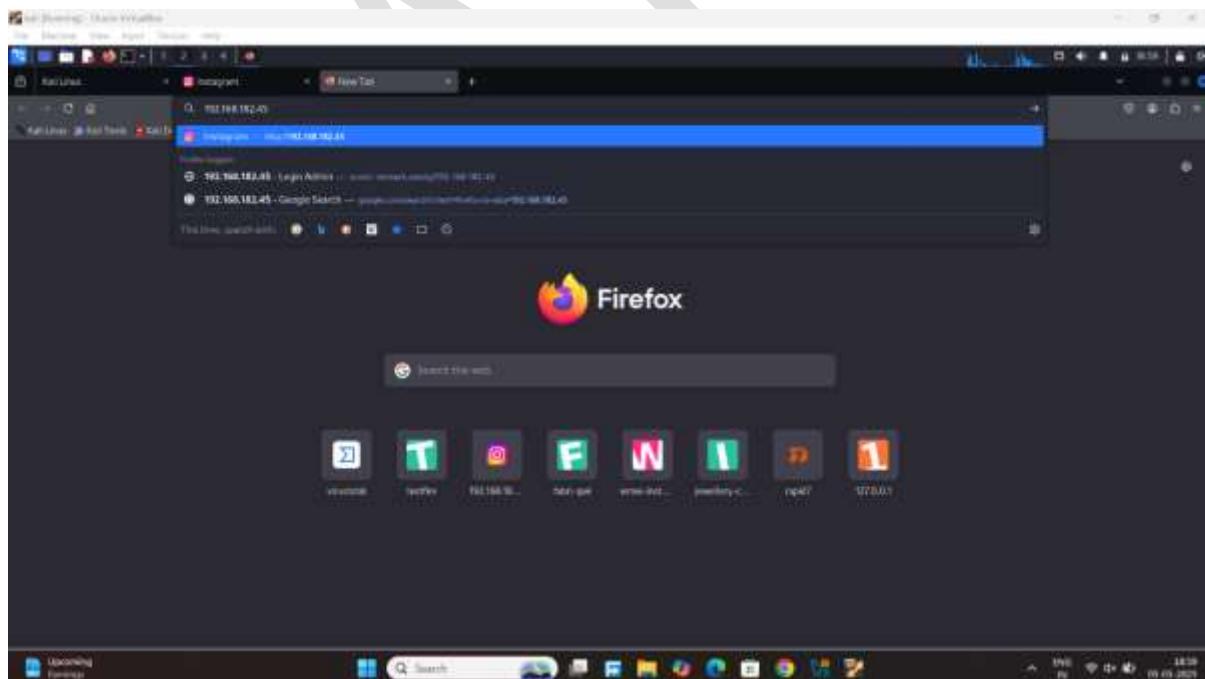
Step7 clone website Instagram.com

```
set: webkitattack> 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: webkitattack> Enter the url to clone: instagram.com

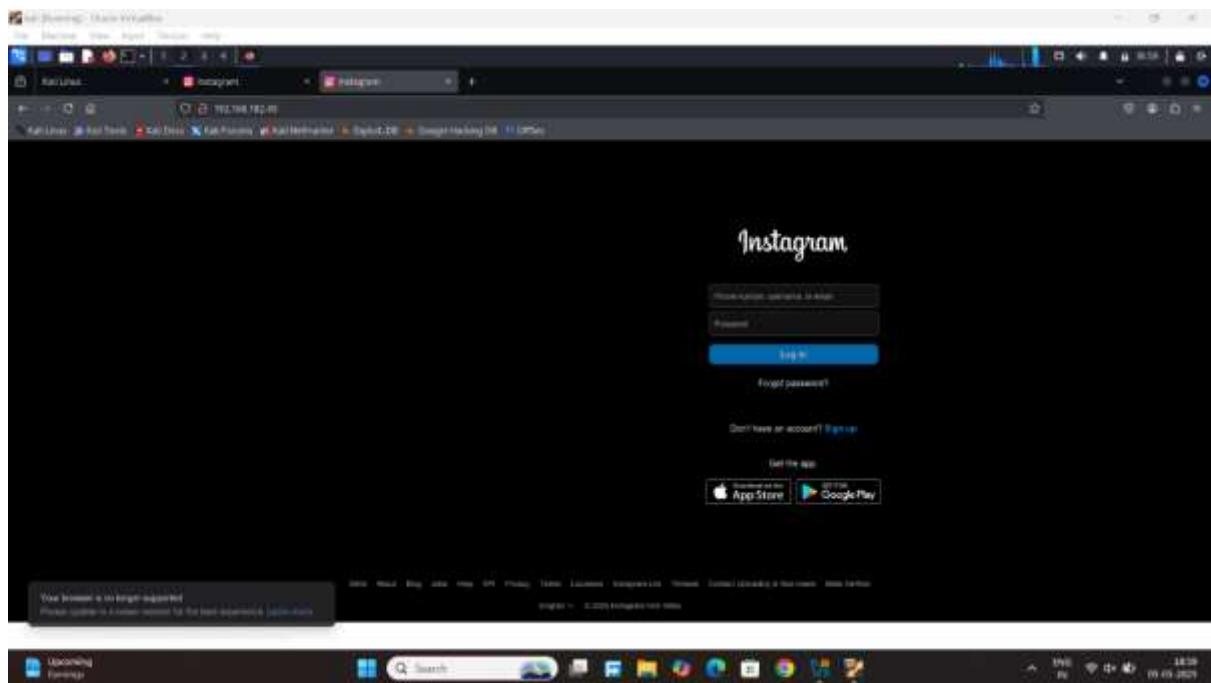
[*] Cloning the website: http://instagram.com
[*] This could take a little bit...
The best way to use this attack is if username and password form fields are available. Regardless, this captures all POSTs on a website.
[+] The Social-Engineer Toolkit Credential Harvester Attack
[+] Credential Harvester is running on port 88
[+] Information will be displayed to you as it arrives helmet

[10:16:20 03-05-2019]
```

Type the kali linux ip and send the target



Result: successful open the site

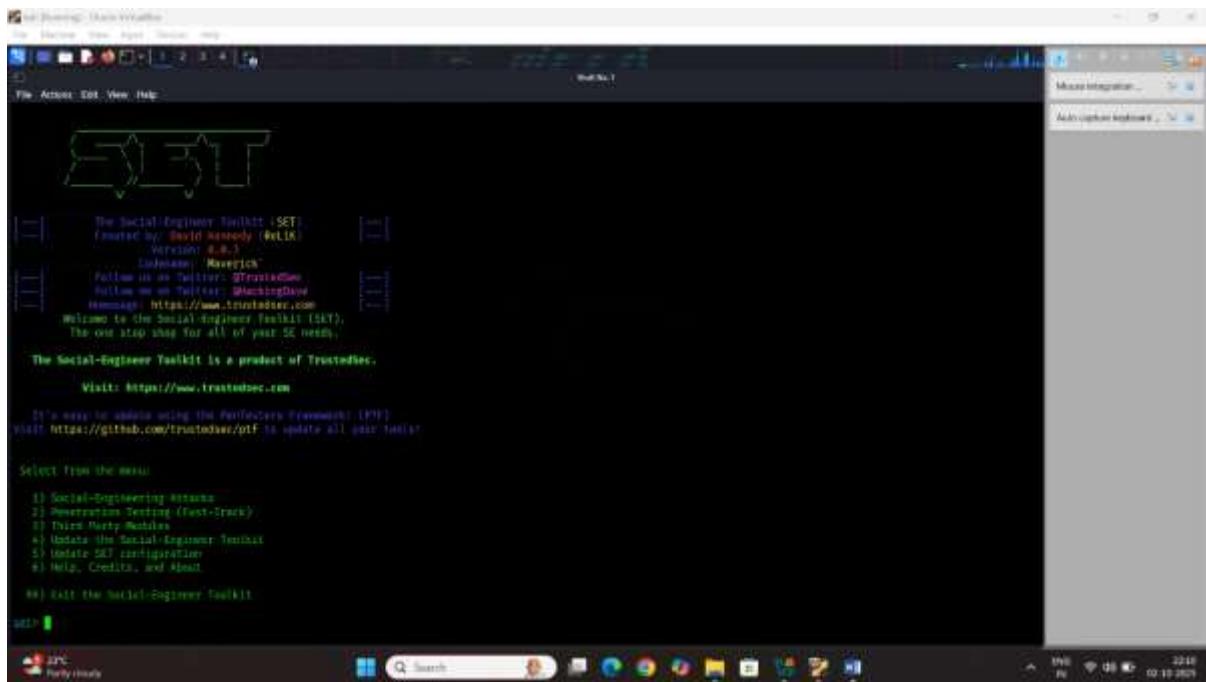


Task2: how to create fishing email and sent to the target using Social engineering tool

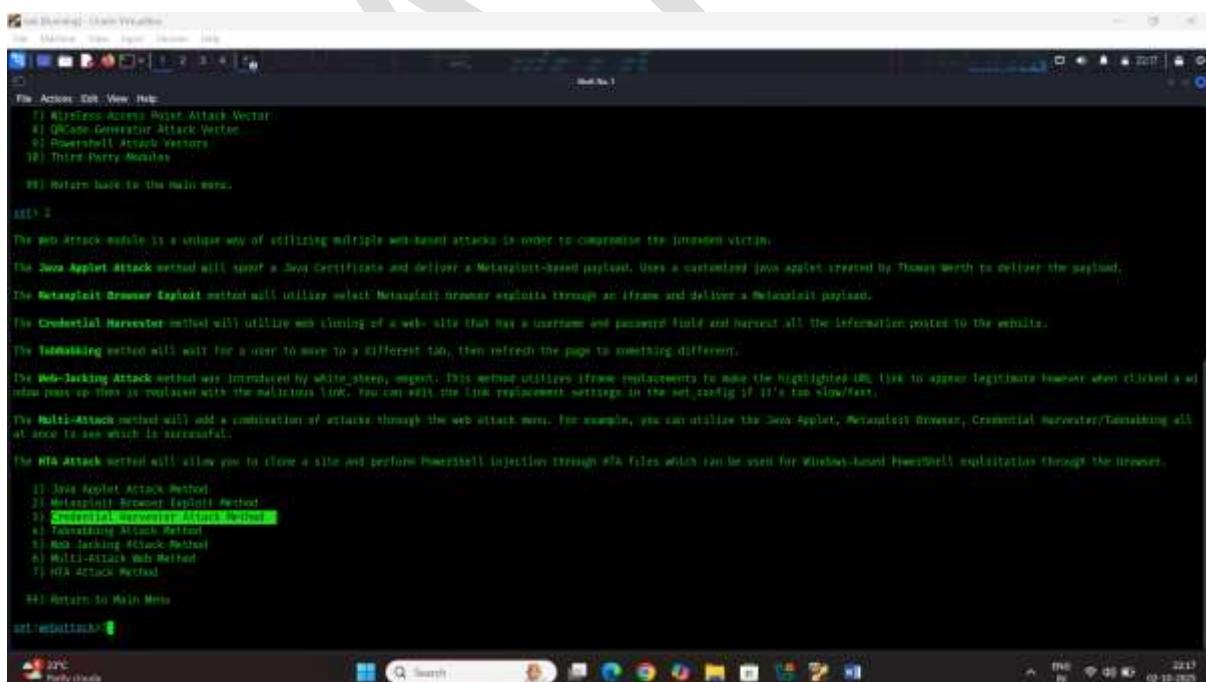
Step1: open the kali Linux terminal and Search the social engineering tool

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

```
msf3:1234567890 - msfvenom
```

The Actions: Edit View Help

The Web-Jacking Attack method was introduced by white_sheep, m0rgn3t. This method utilizes iframe replacements to make the highlighted URL look to appear legitimate however when clicked a evil follow page or item is replaced with the malicious item. You can edit the link replacement settings in the netzconfig if it's too slow/fast.

The Multi-Attack method will put a combination of attacks through the web attack menu. For example, you can utilize the Java Applet, Metasploit Listener, Credential Harvester/Tunneling all at once to see which is successful.

The HTA attack method will allow you to clone a site and perform PowerShell injection through HTA files which can be used for windows-based PowerShell exploitation through the browser.

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

8) Return to Main Menu

set webattack>1

The first method will allow SET to import a list of pre-defined web applications that it has utilized 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 Clone
3) Custom Import

4) Return to Webattack Menu

set webattack>1

Step5 select the option web templet

```
msf3:1234567890 - msfvenom
```

The Actions: Edit View Help

Setting fail. If it fails, you can always save the WTM, enable the form to be standard form 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 have static numbering controls, 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>1 IP address for the POST back in Harvesting? [192.168.1.10]: 192.168.1.10

**** Important Information ****

For templates, when a POST is initiated to Harvest credentials, you will need a site for it to redirect.

You can configure this option under:

/etc/metasploit/conf/config

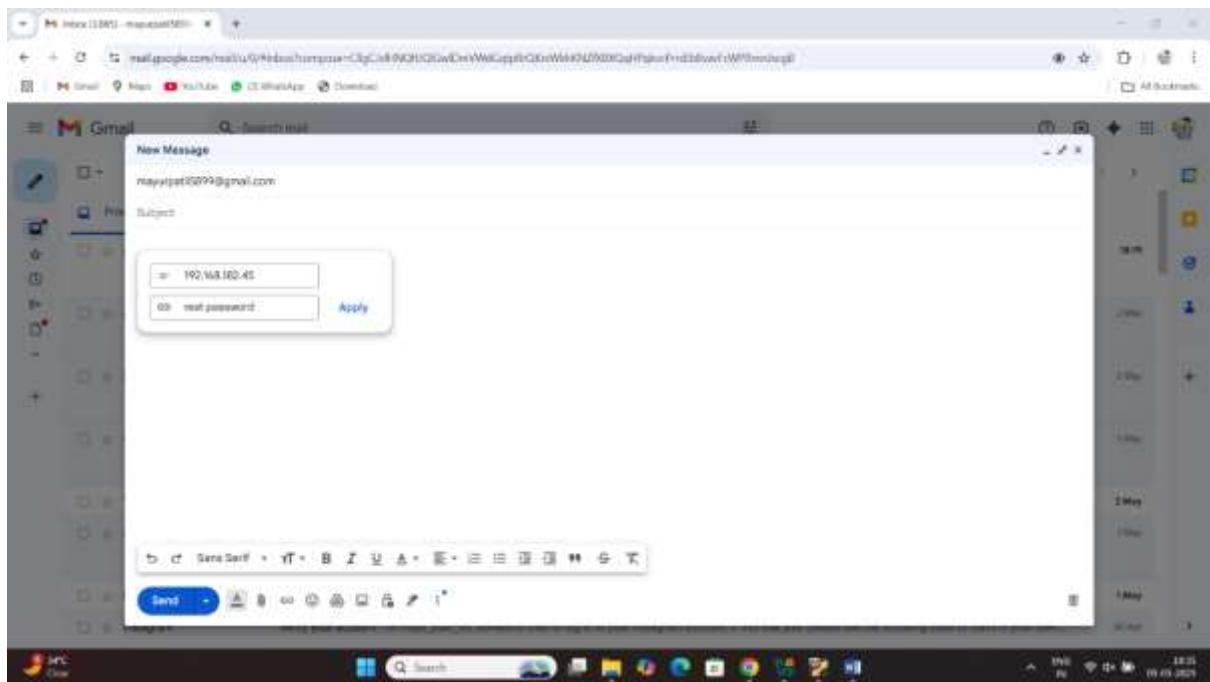
Edit this file, and change HARVESTER_REDIRECT and HARVESTED_URL to the sites you want to redirect to after it is posted. If you do not set these, they will not redirect properly. This only goes for templates.

1. Java Applet
2. Google
3. Twitter

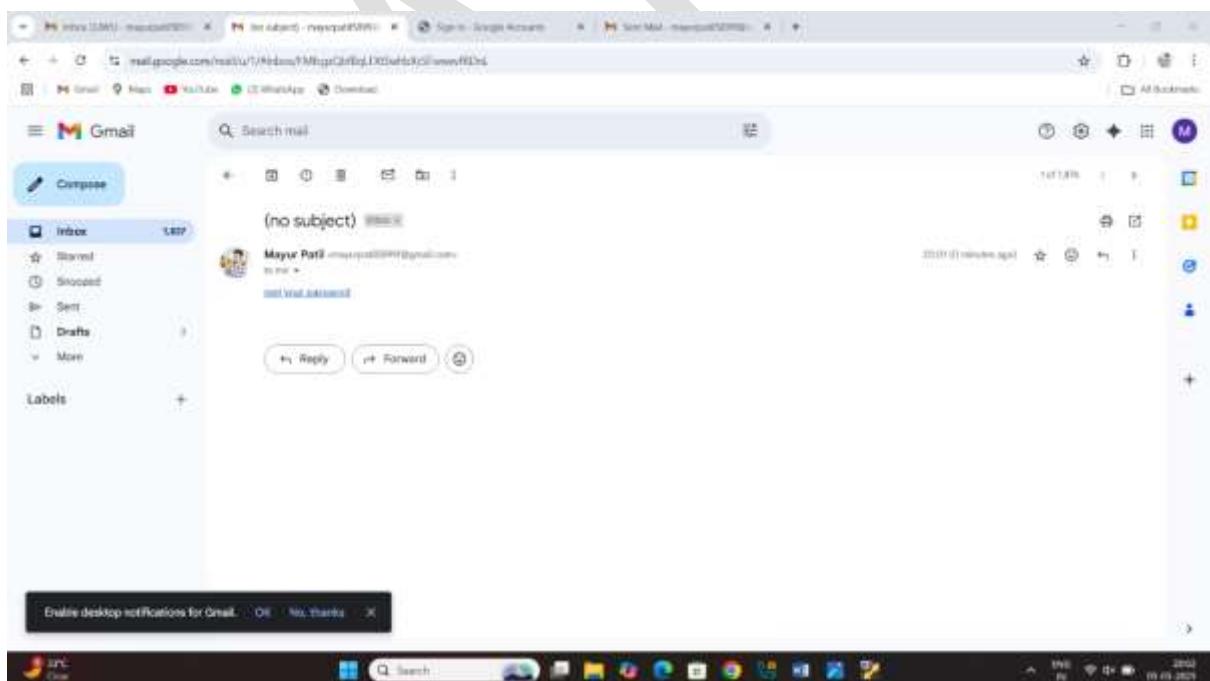
set webattack Select a template: 1

Step6 select the option google

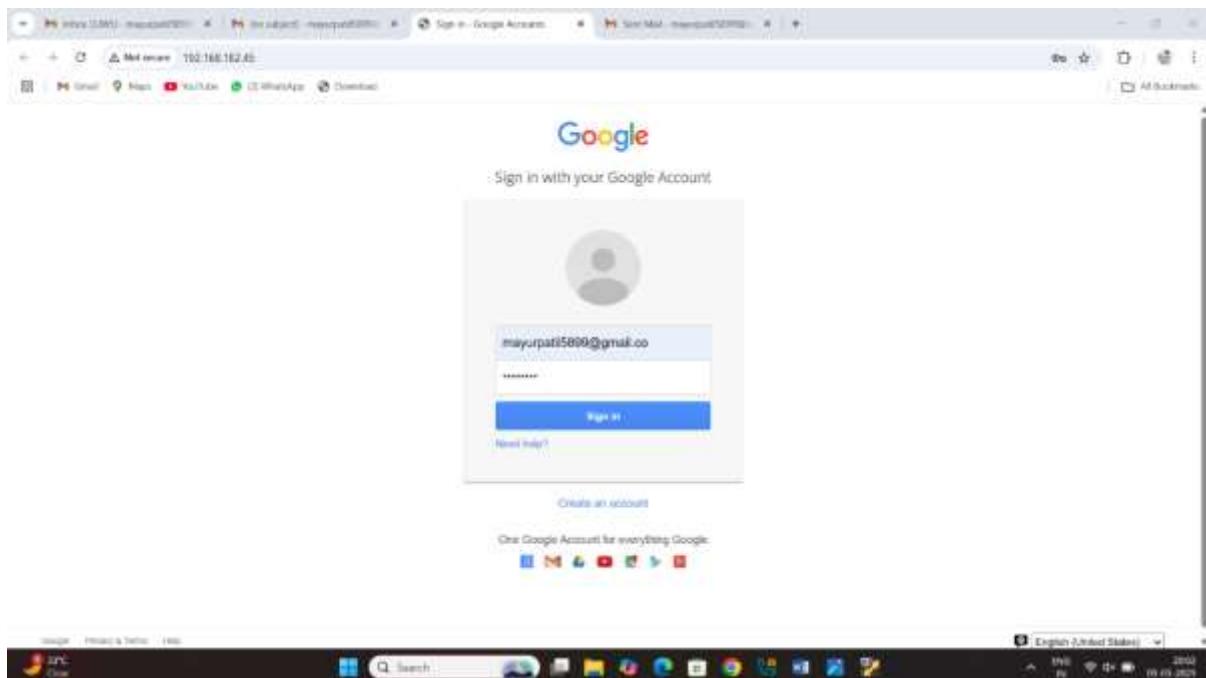
Step8: open the email create the fishing email click on insert link type the kali linux ip



Send it email the target my target email is
mayurpatil5899@gmail.com

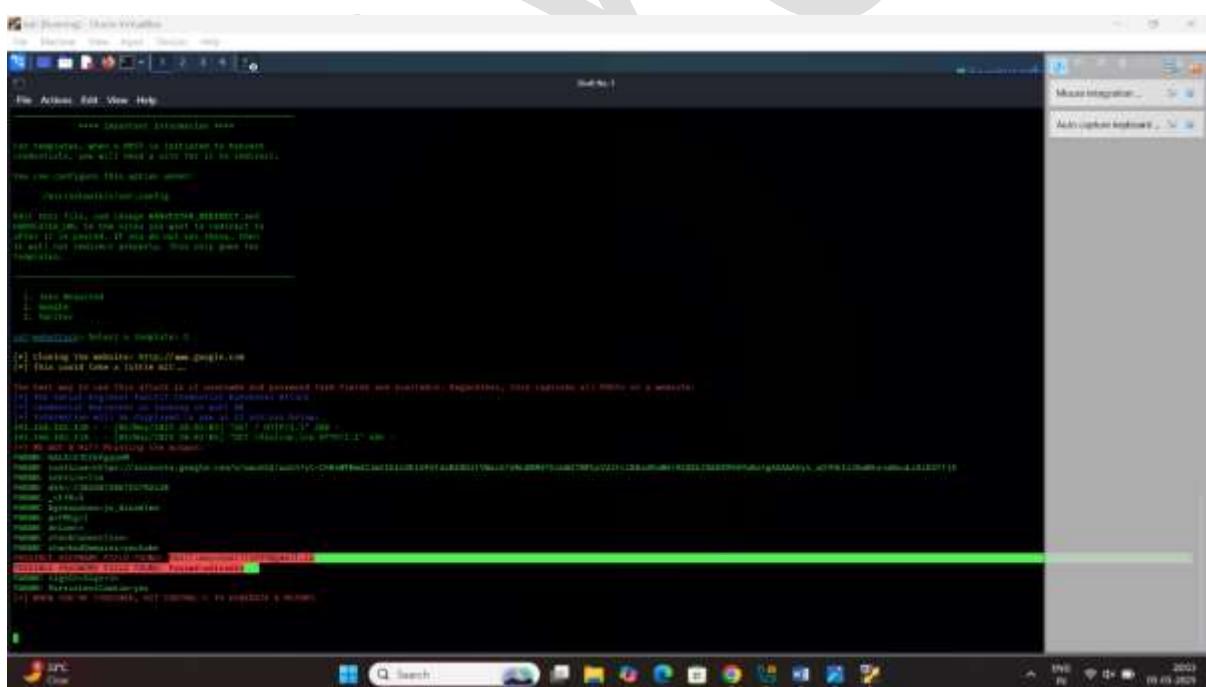


Open the target link and login gmail id



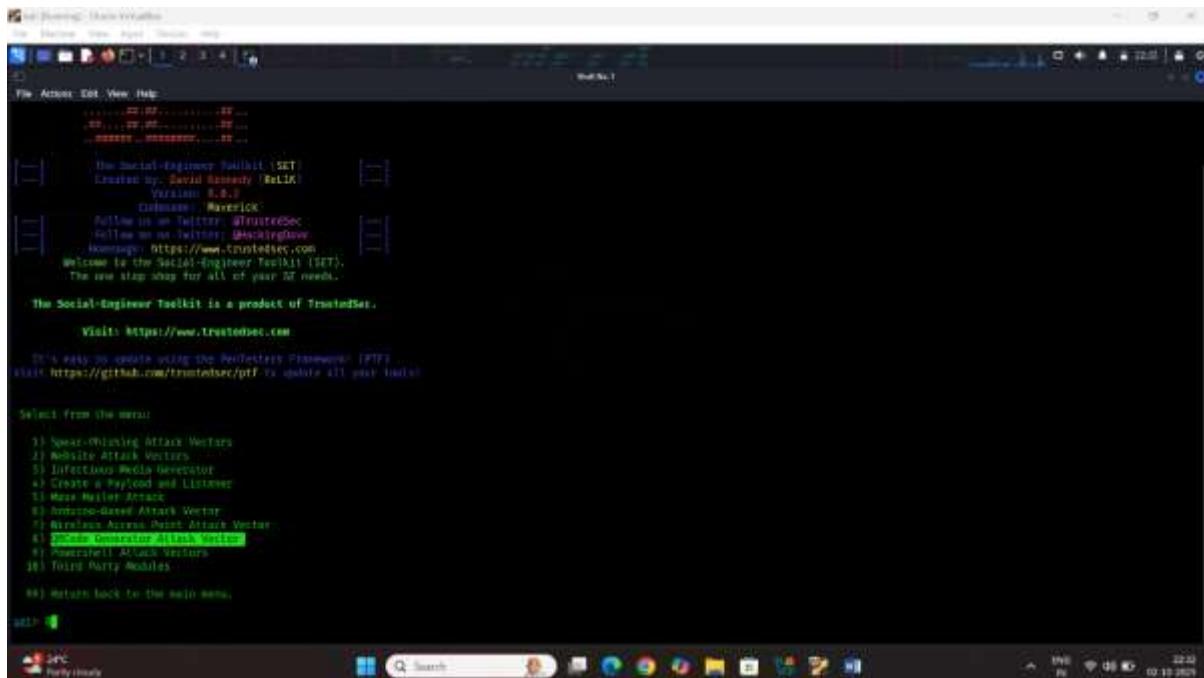
Click on sign

Result:



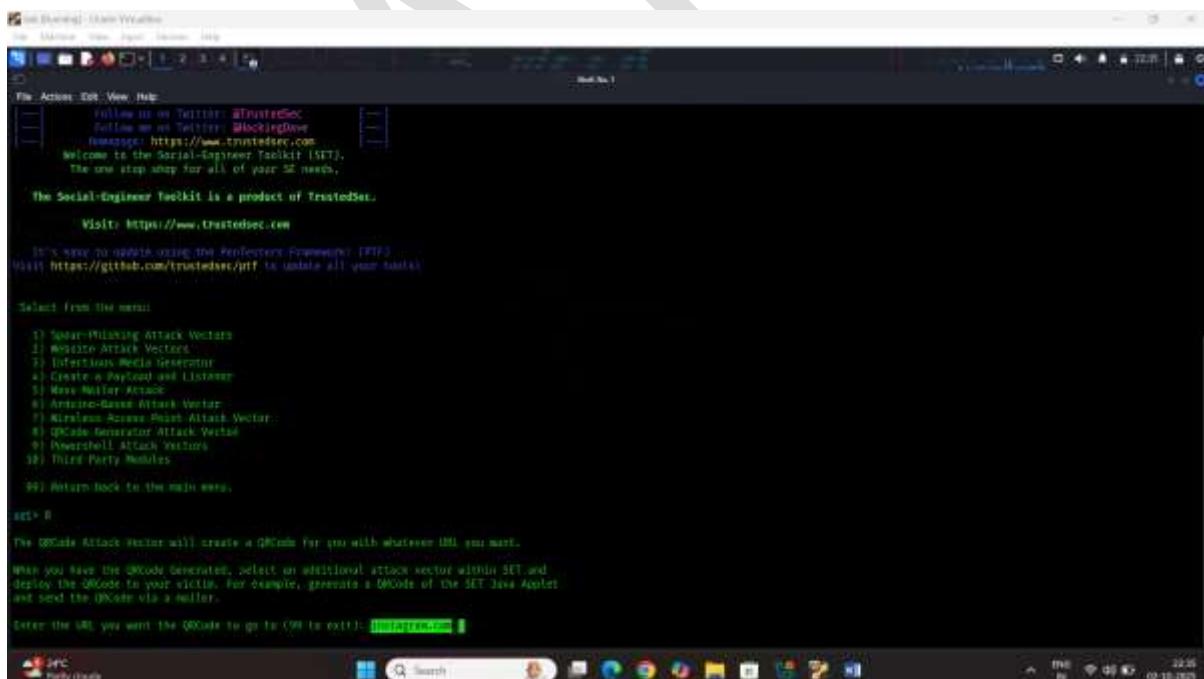
Extra Activity Using Set tool kit Generate the fake Q AR code

Step1: go to kali linux open the set tool kit

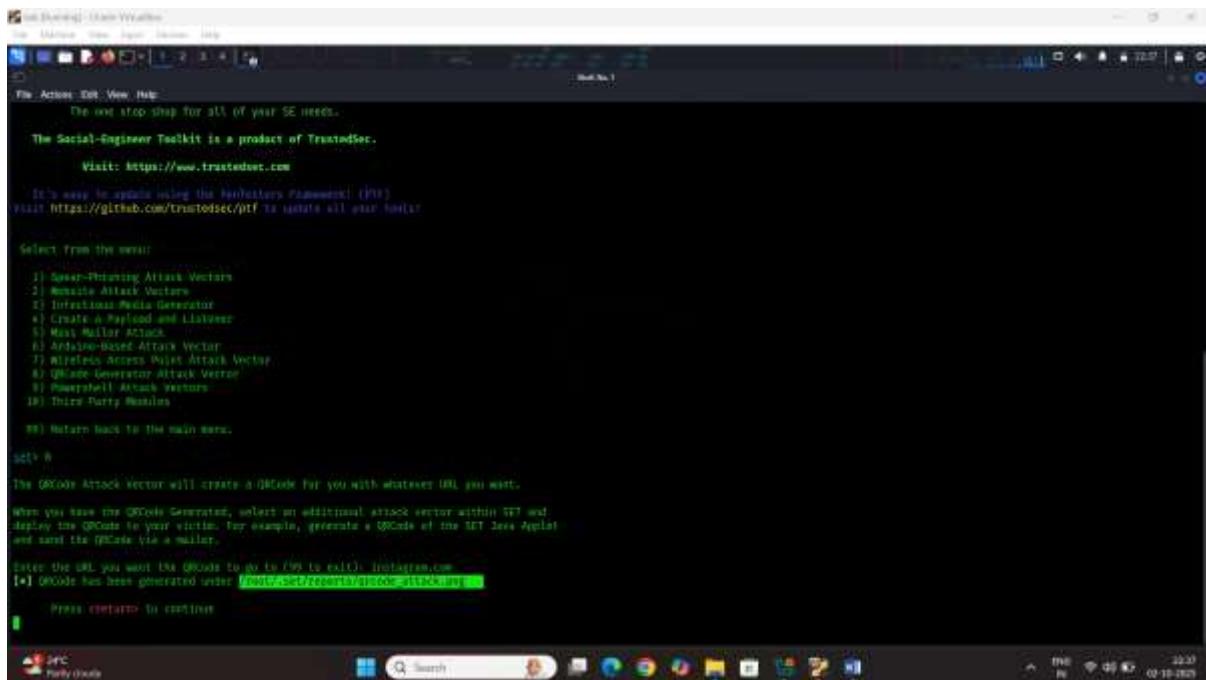


Step4: type the URL

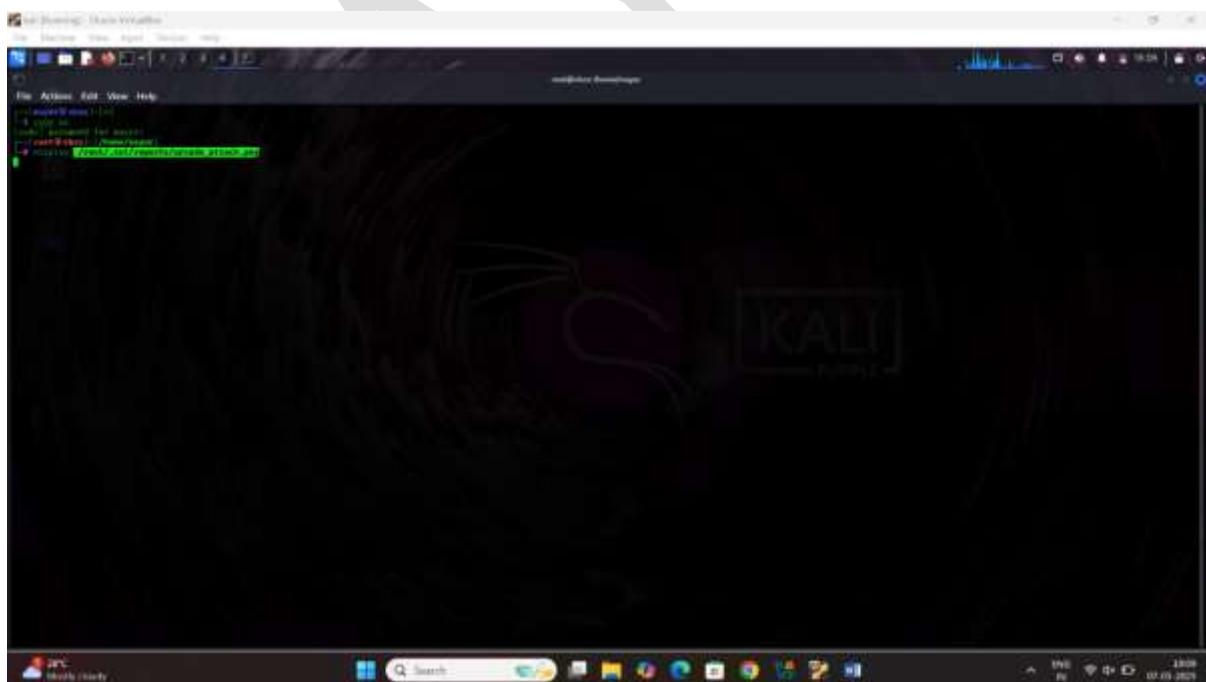
Example: <https://instagram.com>



Step5 copy the root option



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





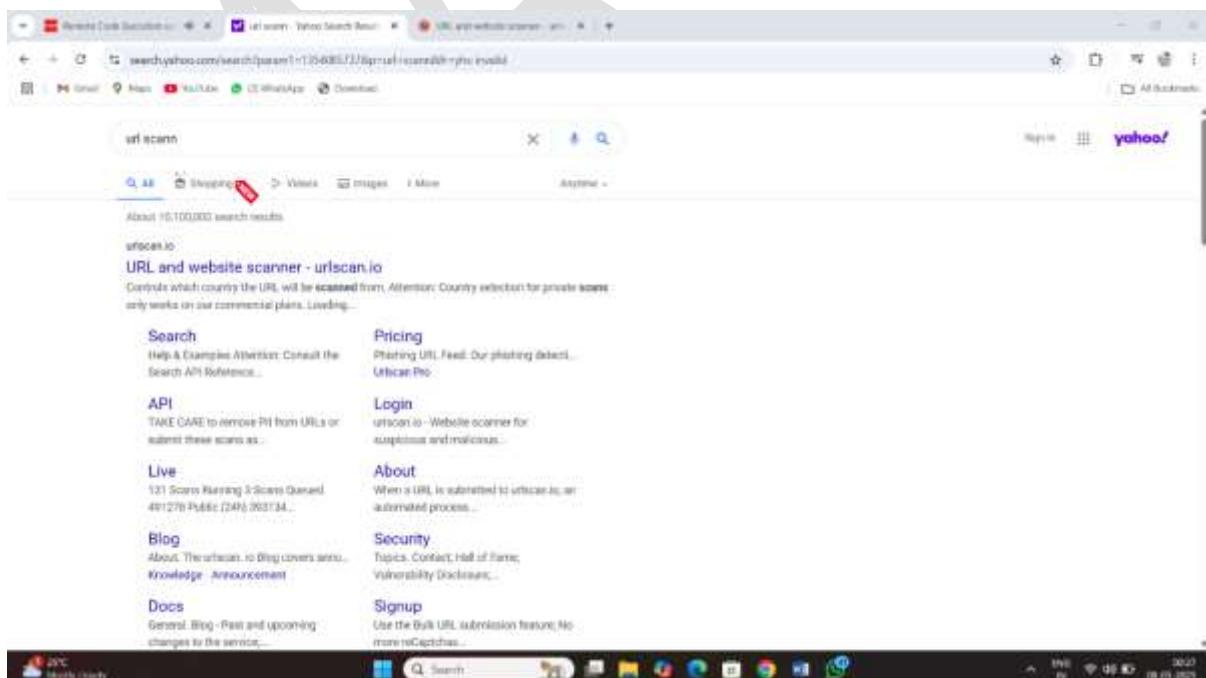
```

[1] 11:29:45.128 [root@kali:~]# ./qrcode_attack.py
[*] QR code generated at /root/reports/qrcode_attack.png
[*] QR code generated at /root/reports/qrcode_attack.jpg

```

2 Extra Activity using website for fishing URL detections

1 web site name: urlscan.io



The screenshot shows the homepage of urlscan.io. The URL in the address bar is "search.yahoo.com/search?&sq=123-0000122&p=1&o=1&t=0&u=https://www.urlscan.io/&v=1". The page displays search results for the query "url scan". It includes sections for "Search", "API", "Live", "Blog", "Docs", "About", "Security", and "Signup". The "About" section notes that the service is a "URL and website scanner - urlscan.io". The "Security" section states that "When a URL is submitted to urlscan.io, an automated process...".

The screenshot shows the urlscan.io homepage with the URL `urlscan.io` in the address bar. The page features a search bar and navigation links for Home, Search, Live, API, Blog, Docs, Pricing, and Login. A banner for SecurityTrails is visible. The main content area displays a table of recent scans with columns for Age, Size, RTT, IPs, and a flag icon. The table lists various URLs with their corresponding details.

Age	Size	RTT	IPs	Flag
13 seconds	3 MB	41	4	GB
13 seconds	428 KB	306	10	2
13 seconds	1 MB	34	4	US
16 seconds	705 KB	19	4	2
16 seconds	526 KB	66	6	US
17 seconds	2 MB	115	20	2
18 seconds	84 KB	6	4	GB
19 seconds	12 MB	103	45	DE
19 seconds	26 KB	35	2	GB
20 seconds	1 MB	39	3	GB

The screenshot shows the urlscan.io homepage with the URL `https://new-minerlate-question-kuwait.trycloudflare.com` in the address bar. The page displays the same interface as the first screenshot, including the search bar and navigation links. The main content area shows a table of recent scans with the specified URL at the top. The table includes columns for Age, Size, RTT, IPs, and a flag icon.

Age	Size	RTT	IPs	Flag
16 seconds	3 MB	36	3	GB
18 seconds	223 KB	32	1	2
20 seconds	920 KB	230	7	DE
20 seconds	70 KB	10	4	2
20 seconds	571 KB	31	7	2
21 seconds	53 KB	5	2	2
22 seconds	289 KB	8	4	2
23 seconds	2 MB	33	5	2
23 seconds	415 KB	13	6	2
23 seconds	796 KB	30	4	2

Result:

The screenshot shows the urbscan.io interface. At the top, it displays the URL `tex-minerals-question-kuwait.trycloudflare.com` and identifies it as "Malicious Activity". Below this, there's a summary of the analysis, mentioning 2606:4700:6810:e784:: Malicious Activity!, and a screenshot of the website itself.

Summary:
This analysis contacted 5 IPs in 2 countries across 5 domains to perform 33 HTTP transactions. The main IP is 2606:4700:6810:e784, located in United States and belongs to CLOUDFLARENET.US. The main domain is `tex-minerals-question-kuwait.trycloudflare.com`. TLS certificate issued by IWE1 on April 22nd 2025. Valid for 3 months.

This is the only time `tex-minerals-question-kuwait.trycloudflare.com` was scanned on urbscan.io.

urbscan.io Verdict: Potentially Malicious ⓘ

Targeting these brands: Instagram (Social Network)

Live Information:
Google Safe Browsing: [Malicious](#) (`tex-minerals-question-kuwait.trycloudflare.com`)
Current DNS A record: 104.16.230.132 (Cloudflare)

Domain & IP Information:

IPASNs IP Details Domains Domains Tree Links Certs Friends

Screenshot: A small preview of the website showing a login form for "Instagram".

Page Title: Instagram

Page URL History: [View history](#)

3 Extra Activity using website for fishing URL detections

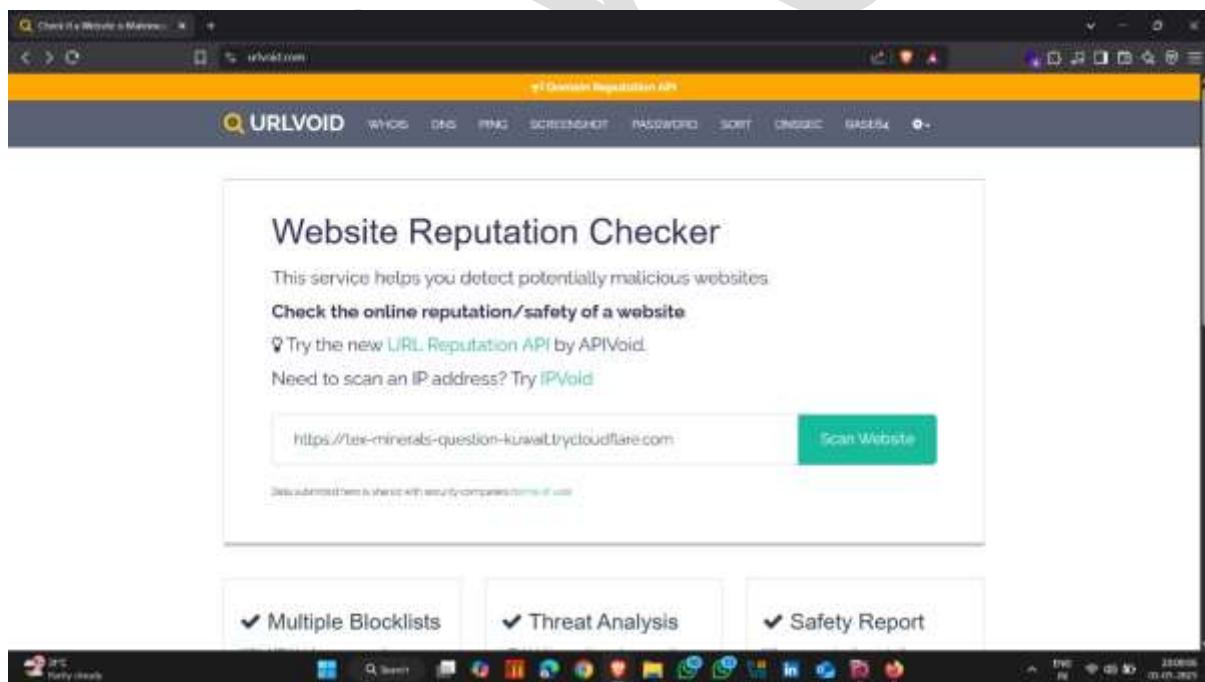
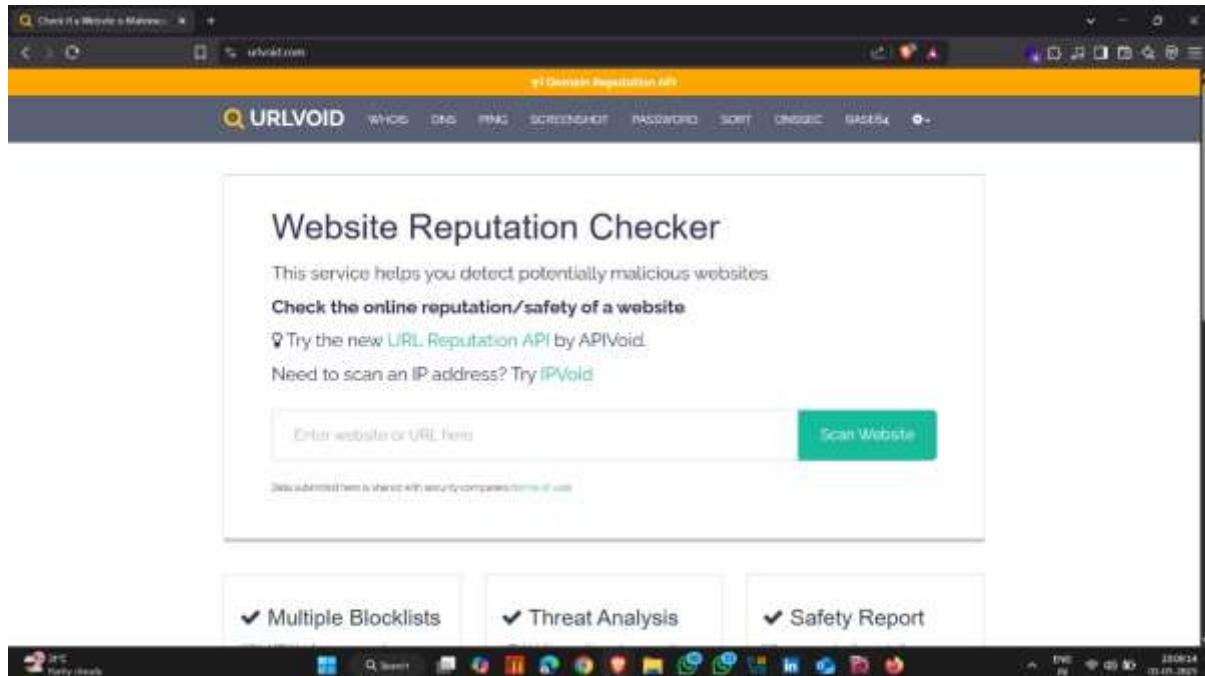
1 web site name: URLvoid

The screenshot shows the URLvoid website. The search bar indicates a query for "phishing url scan". The results page displays several cards:

- Check if a Website is Malicious/Scam or Safe/Legit**: A card from URIT.MAIL showing a warning about identifying websites involved in malware and phishing incidents. It mentions that URIT.MAIL is used by cyber security companies and IT researchers to speed up the process of cyber threat analysis.
- Sucuri Security**: A card from Sucuri Security showing a link to the Website Security Checker and Malware Scan.
- Phishing Check Tool - Skynag**: A card from Skynag showing a link to the Phishing Check Tool, which protects domains from phishing attacks.

At the bottom, there are links to "Find elsewhere", "Google", "Bing", and "Majestic".

Open the web site



Result :

The screenshot shows a web browser window with the URL <https://www.urlvoid.com/analyze/Tex-minerals-question-kuwait.cloudflare.com>. The page title is "Report Summary". Key details from the report include:

- Website Address: Tex-minerals-question-kuwait.cloudflare.com
- Last Analysis: 8 seconds ago | [View Details](#)
- Detections Counts: 1/10
- Domain Registration: 2023-07-07 | 7 years ago
- Domain Information: [DNS](#) | [CNAME](#) | [NS](#) | [MX](#) | [TXT](#)
- IP Address: 304.88.230.132 | [Find Websites](#) | [Whois](#) | [Details](#)
- Reverse DNS: Unknown

4 Extra Activity using website for fishing URL detections

The screenshot shows a search results page for "phishing detection" on the Brave browser. The results include:

- CheckPhish AI**: A service that checks for phishing links and scans sites for vulnerabilities.
- URL Scanner & Sandbox**: A tool for evaluating potential cybersecurity threats by sandboxing URLs and analyzing them for malicious activity.
- Check Point Software**: A company that provides security solutions, including a blog post titled "Phishing Detection Techniques - Check Point Software".
- Discussions**: A section where users can discuss topics related to phishing detection.

CheckPhish Detects and Monitors Phishing and Scam Sites

With CheckPhish, you can scan suspicious URLs and monitor for typosquats and lookalikes variants of a domain.

New! Email Scanner URL Scanner Typequat Monitoring Takedown

https://variety-survivors-plots-trailer.cloudflare.com/login.html Scan!

CheckPhish is a free next-level URL scanner providing deep threat intelligence, including screenshots, certificates, DOM Tree, and hosting details. Monitors 300M+ domains. Relying on machine learning and automation.

If you want to do more than one scan, automate a scan with API or use a proxy for scanning. Please sign up here!

Result:

https://variety-survivors-plots-tr...

Scan Results

Source URL: https://variety-survivors-plots-trail...

Redirected URL: https://variety-survivors-plots-trail...

IP Address: 104.16.230.132

Detection Date: May 8th 2020, 3:23:00 am

Job ID: 13326

Geo-Location: Google Trust Services (trycloudflare.com) * (yields)

Screenshot

DOM TREE TIMELINE VIEW WHOIS INFORMATION

Log In Sign Up

Google One account. All of Google.

MAYUR