



REPORT OF SOCIAL ENGINEERING

MODULE 9

Aniket Sunil Pagare

Table of Contents

1. Introduction to Social Engineering

1.1 What is Social Engineering?

1.2 Importance and Impact

2. Types of Social Engineering

2.1 Phishing

3. Types of Phishing

3.1 Email Phishing

3.2 Spear Phishing

3.3 Whaling

3.4 Smishing

3.5 Vishing

3.6 Clone Phishing

4. Phishing Attacks Demonstrations

4.1 Performing a Phishing Attack Using SEToolkit

4.2 Performing a Phishing Attack Using a Gmail Account

4.3 Performing a Phishing Attack Using Zphisher

5. Extra Activities

5.1 Performing a Phishing Attack Using BlackEye Tool

5.2 Performing a Phishing Attack Using R3bu5 Tool

5.3 Performing a Phishing Attack Using CamPhish Tool

5.4 Generating a QR Code Using SEToolkit

5.5 Performing a Phishing Attack via QR Code Using SEToolkit

6. Phishing Detection Tools

6.1 Phishing Detection Using URLScan.io

6.2 Phishing Detection Using URLVoid.com

6.3 Phishing Detection Using CheckPhish.ai

SOCIAL ENGINEERING

Social engineering is a manipulation technique used by attackers to trick people into giving up confidential information or performing actions that compromise security. Instead of directly hacking systems, social engineering targets human psychology and behavior.

Human-Based Social Engineering Attack

A **human-based social engineering attack** is a method where attackers use direct human interaction and psychological manipulation to trick individuals into revealing confidential information or granting access to secure systems.

Computer-Based Social Engineering Attack

A **computer-based social engineering attack** uses digital means such as emails, websites, or software to deceive users and steal data, install malware, or gain unauthorized access.

Mobile-Based Social Engineering Attack

A **mobile-based social engineering attack** targets users through mobile devices using calls, text messages (SMS), or malicious apps to extract personal or financial information.

Common Types of Social Engineering:

1. **Phishing** – Sending fake emails or messages that look legitimate to trick users into revealing credentials or downloading malware.
2. **Spear Phishing** – Targeted phishing attacks customized for a specific person or organization.
3. **Vishing (Voice Phishing)** – Using phone calls to impersonate someone and extract information.

4. **Smishing (SMS Phishing)** – Similar to phishing but via text messages.
5. **Pretexting** – Creating a false scenario (pretext) to obtain information, e.g., pretending to be from IT support.
6. **Baiting** – Leaving infected USBs or links that lure users into compromising their system.
7. **Tailgating** – Following authorized personnel into restricted areas without proper authentication.

PHISHING

Phishing is a type of **cyber attack** where attackers try to trick individuals into revealing sensitive information such as usernames, passwords, credit card numbers, or other confidential data by pretending to be a trustworthy source.

Types of Phishing --

1. Email Phishing

- **Description:** The most common type. Attackers send fraudulent emails that appear to be from reputable sources (e.g., banks, government, or tech companies).
 - **Goal:** Steal credentials or deliver malware via links or attachments.
-

2. Spear Phishing

- **Description:** A targeted phishing attack aimed at a specific individual or organization.
 - **Goal:** Steal specific sensitive data by using personal information to appear trustworthy.
-

3. Whaling

- **Description:** A type of spear phishing that targets high-profile individuals (e.g., CEOs, CFOs).
 - **Goal:** Gain access to high-level company data or authorize fraudulent transactions.
-

4. Smishing (SMS Phishing)

- **Description:** Uses text messages instead of email.

- **Goal:** Trick users into clicking malicious links or calling fake customer service numbers.
-

5. Vishing (Voice Phishing)

- **Description:** Uses phone calls to impersonate legitimate institutions (e.g., banks, police).
 - **Goal:** Extract personal or financial information.
-

6. Pharming

- **Description:** Redirects users from legitimate websites to fake ones, usually via DNS poisoning or malware.
 - **Goal:** Harvest login credentials and personal data.
-

7. Angler Phishing

- **Description:** Conducted via social media platforms by impersonating customer service accounts.
 - **Goal:** Steal credentials or install malware through direct messages or fake links.
-

8. Clone Phishing

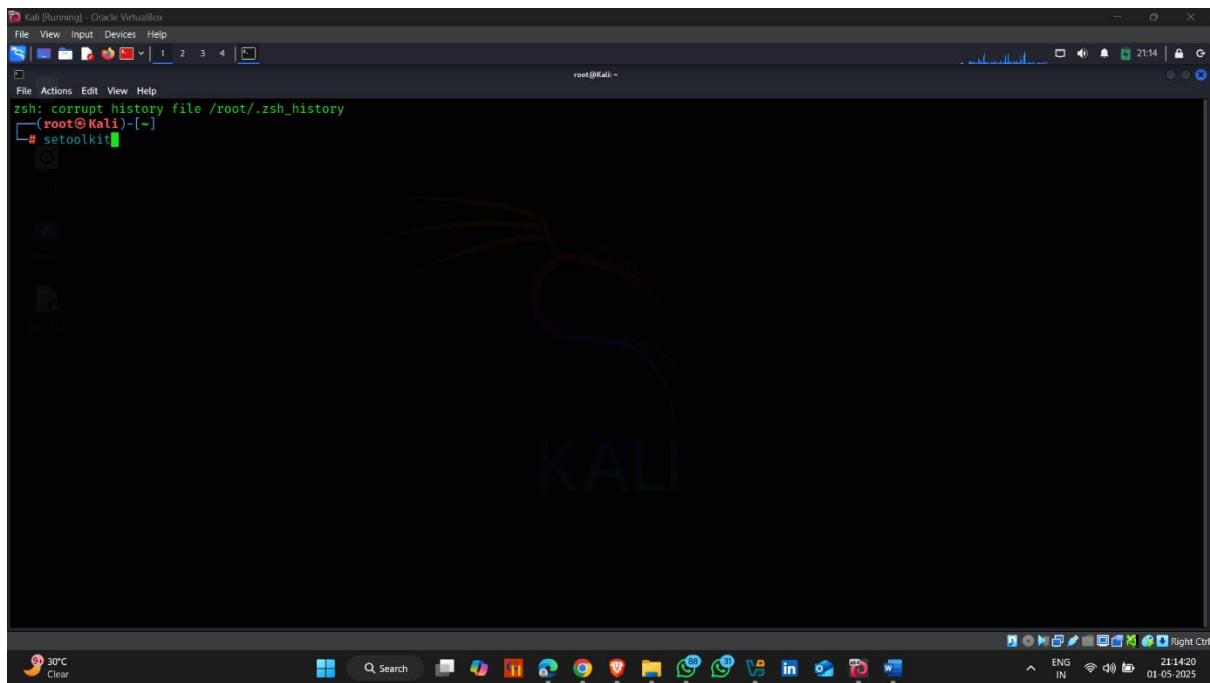
- **Description:** A legitimate email is cloned, and the attachment or link is replaced with a malicious one.
- **Goal:** Trick recipients who have already seen or trusted the original email.

1. Perform Phishing Attack Using SETOOLKIT

In **Kali Linux**, the **Social-Engineer Toolkit (SET)** is one of the most powerful tools for **phishing attacks**, specifically designed to simulate **real-world social engineering scenarios**. For phishing, SET helps you create **fake websites or emails** to trick users into entering their login credentials or executing malicious files.

How to use it :-

- Open kali linux terminal and type **setoolkit**



- It opens
- Now select 1 – **Social Engineering Attack**



```
Kali [Running] - Oracle VirtualBox
File View Input Devices Help
[ 1 2 3 4 ]
File Actions Edit View Help
root@Kali: ~
[—] 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!

Unable to check for new version of SET (is your network up?)

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
```

30°C Clear ENG IN 21:16 01-05-2025

- Now select 2 – Website attack Vector



```
Kali [Running] - Oracle VirtualBox
File View Input Devices Help
[ 1 2 3 4 ]
File Actions Edit View Help
root@Kali: ~
[—] 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) 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
```

30°C Clear ENG IN 21:16 01-05-2025

- Select 3 – Credential Harvesting Attack Method

```
Kali [Running] - Oracle VirtualBox
File View Input Devices Help
File | 1 2 3 4 | 
root@Kali: ~
File Actions Edit View Help

The Web Attack module is a unique way of utilizing multiple web-based attacks in order to compromise the intended victim.

The Java Applet Attack method will spoof a Java Certificate and deliver a Metasploit-based payload. Uses a customized java applet created by Thomas Werth to deliver the payload.

The Metasploit Browser Exploit method will utilize select Metasploit browser exploits through an iframe and deliver a Metasploit payload.

The Credential Harvester method will utilize web cloning of a web- site 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 whenever 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

30°C Clear ENG IN 21:53 01-05-2025
```

- Select 2 – Web Template

```
Kali [Running] - Oracle VirtualBox
File View Input Devices Help
File | 1 2 3 4 | 
root@Kali: ~
File Actions Edit View Help

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

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>1

30°C Clear ENG IN 21:07 01-05-2025
```

- Select Web template

```

Kali [Running] - Oracle VM VirtualBox
File View Input Devices Help
File Actions Edit View Help
root@Kali: ~
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 [192.168.182.192]: 

**** 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/setoolkit/set.config

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

1. Java Required
2. Google
3. Twitter

set:webattack> Select a template: 

```

- Now provide a ip address that you want to get response back

Note :- By default it select kali linux ip address

```

Kali [Running] - Oracle VM VirtualBox
File View Input Devices Help
File Actions Edit View Help
root@Kali: ~
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
[-] 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

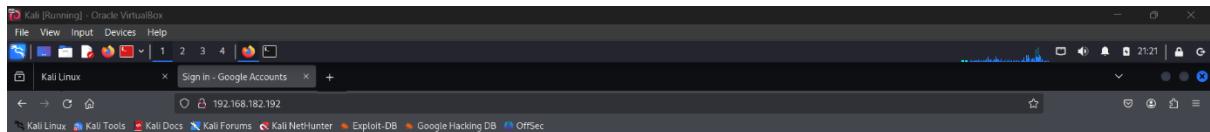
--- * IMPORTANT * READ THIS BEFORE ENTERING IN THE IP ADDRESS * IMPORTANT *

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 [192.168.182.192]: 
```

- Now open the browser on target machine and type kali linux ip address in url section
- Here , google login template occurred



Google

Sign in with your Google Account

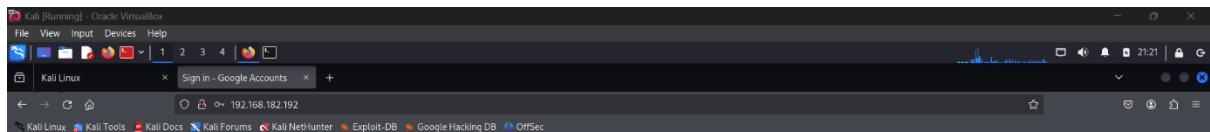
Sign in

Need help?

Create an account
One Google Account for everything Google
[Gmail](#) [Maps](#) [YouTube](#) [Play Store](#) [Photos](#)



- Provide a credentials



Google

Sign in with your Google Account

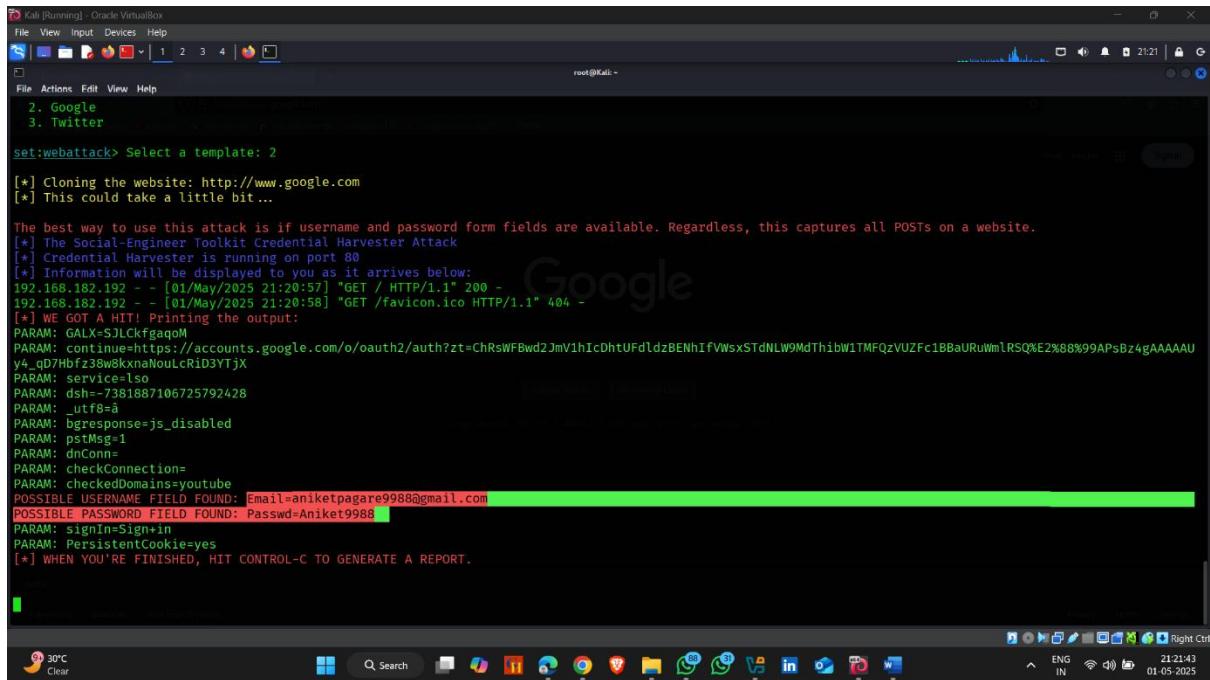
Sign in

Need help?

Create an account
One Google Account for everything Google
[Gmail](#) [Maps](#) [YouTube](#) [Play Store](#) [Photos](#)



- Now go to the kali linux terminal
- Here it got the creadentials



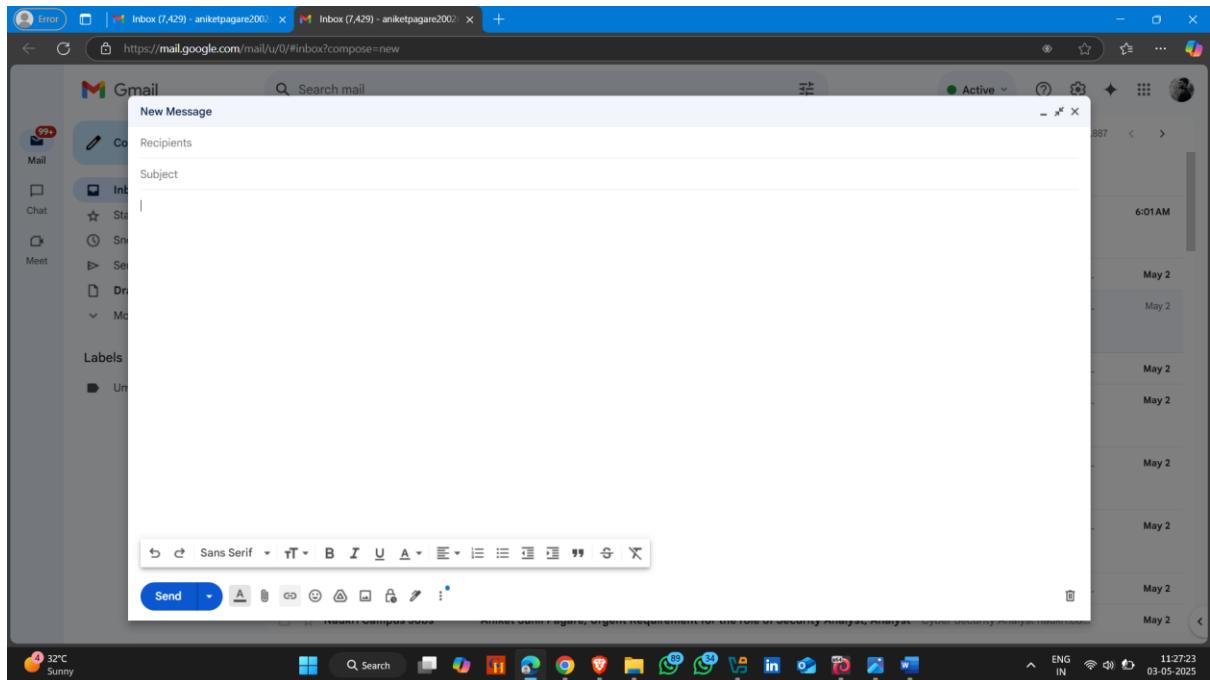
```
Kali [Running] - Oracle VirtualBox
File View Input Devices Help
File Actions Edit View Help
2. Google
3. Twitter
set:webatck> Select a template: 2
[*] Cloning the website: http://www.google.com
[*] This could take a little bit...
The best way to use this attack is if username and password form fields 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:
192.168.182.192 - - [01/May/2025 21:20:57] "GET / HTTP/1.1" 200 -
192.168.182.192 - - [01/May/2025 21:20:58] "GET /favicon.ico HTTP/1.1" 404 -
[*] WE GOT A HIT! Printing the output:
PARAM: GALX=SJLCKfgaqM
PARAM: continue=https://accounts.google.com/o/oauth2/auth?zt=ChRsWFBwd2JmV1hIcDhtUFdldzBENhIfVWsxSTDNLW9MdThibW1TMFQzVUZFc1BBaURuWmlRSQ%E2%88%99APsBz4gAAAAU
y_4q7HbfZ38w8kxxnaNouLCrId3YTjX
PARAM: service=lsos
PARAM: dsh=-7381887106725792428
PARAM: _utf8=â
PARAM: bgrresponse=js_disabled
PARAM: pstMsg=1
PARAM: dnConn=
PARAM: checkConnection=
PARAM: checkedDomains=youtube
POSSIBLE USERNAME FIELD FOUND: Email=aniketpagare9988@gmail.com
POSSIBLE PASSWORD FIELD FOUND: Passwd=Aniket9988
PARAM: signIn=Sign+in
PARAM: PersistentCookie=yes
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.
```

2. Perform Phishing Attack Using Gmail Account

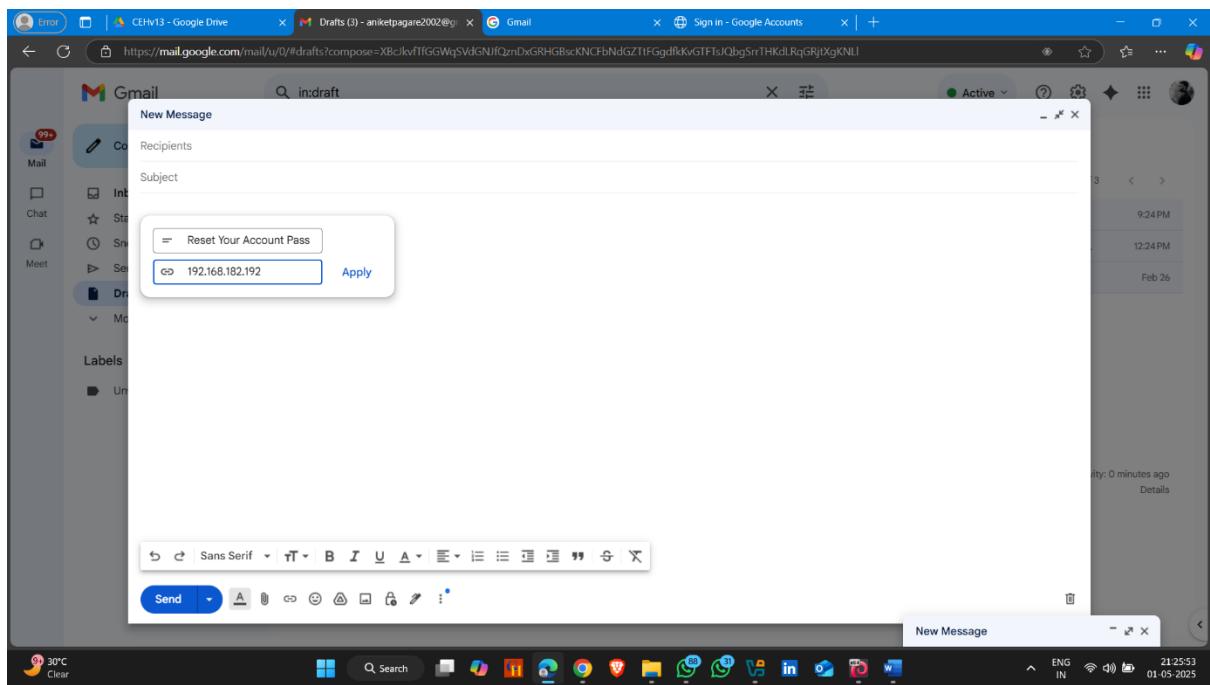
How to use it :-

- Firstly create a phishing link using kali linux
- Then open Your gmail account
- Now open the gmail account and **click on compose** and **create a hyperlink**

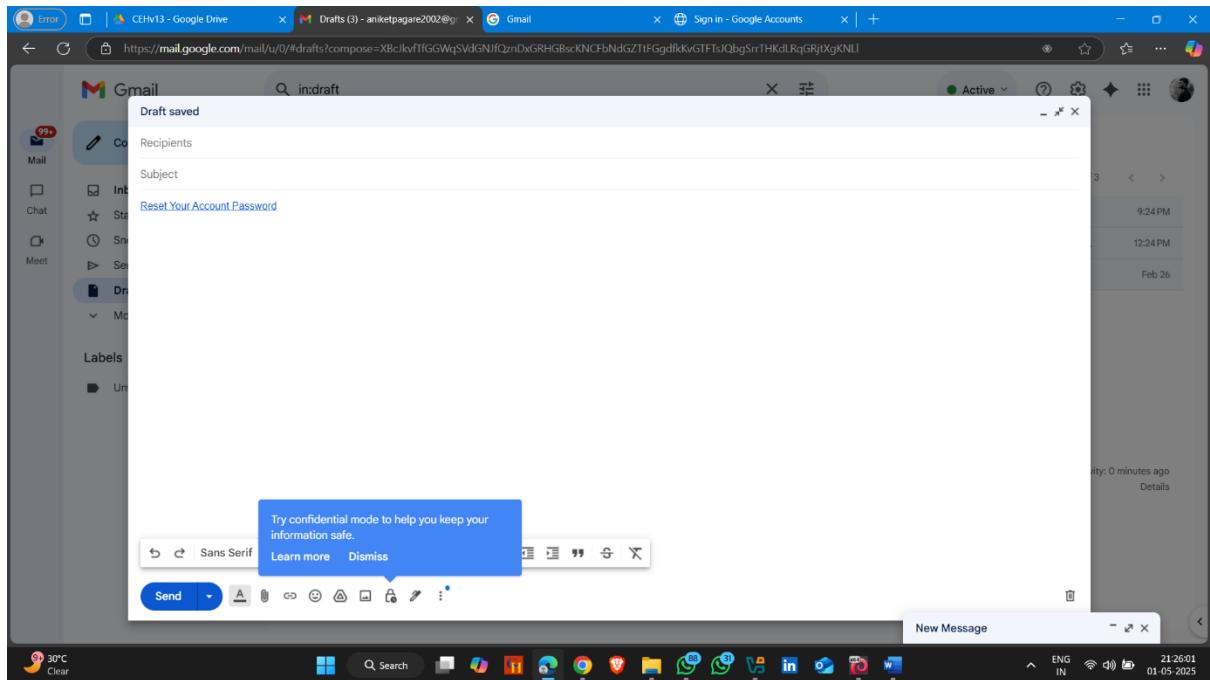
Note :- In Gmail, the hyperlink icon is typically found at the bottom of the composition window and looks like a few links in a chain.



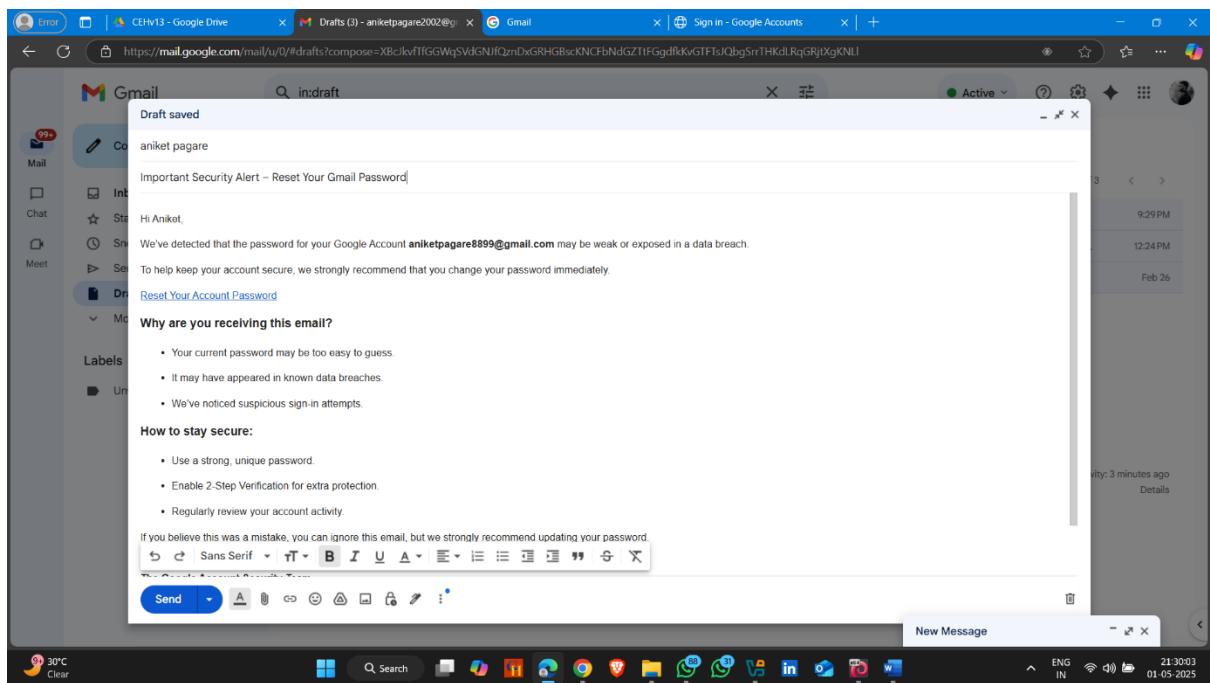
- First box – add message that display in main
- Second box – add attacker machine ip add and click on apply



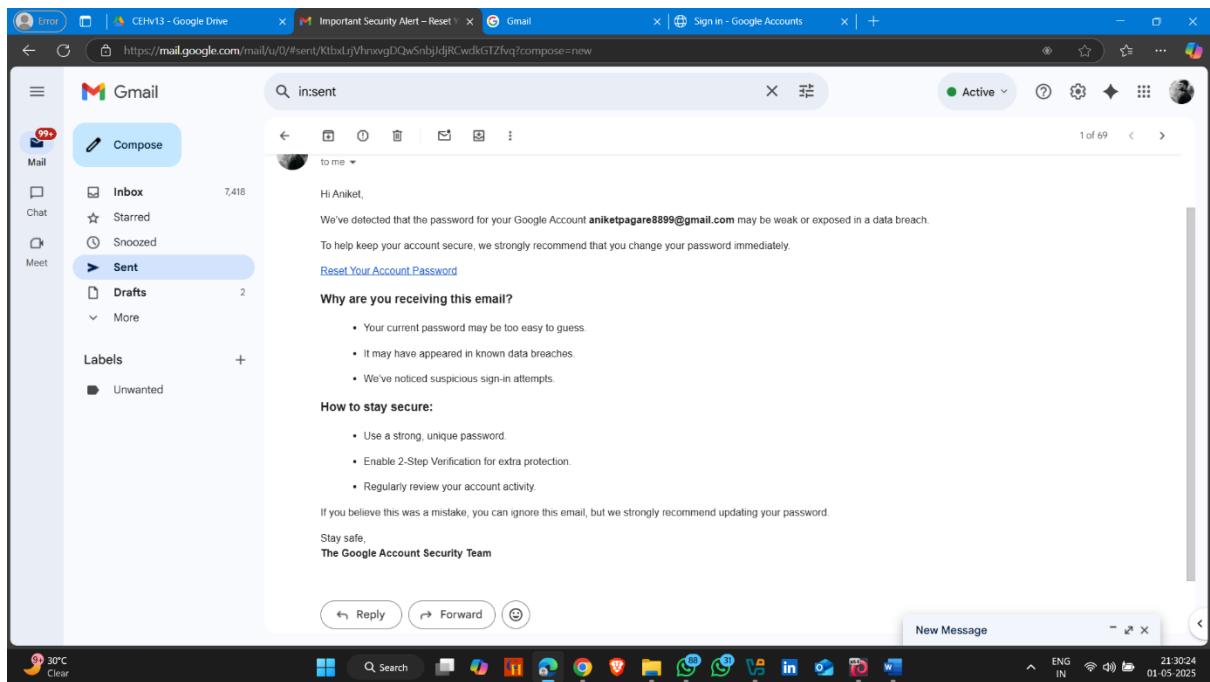
- **Hyperlink Generated**



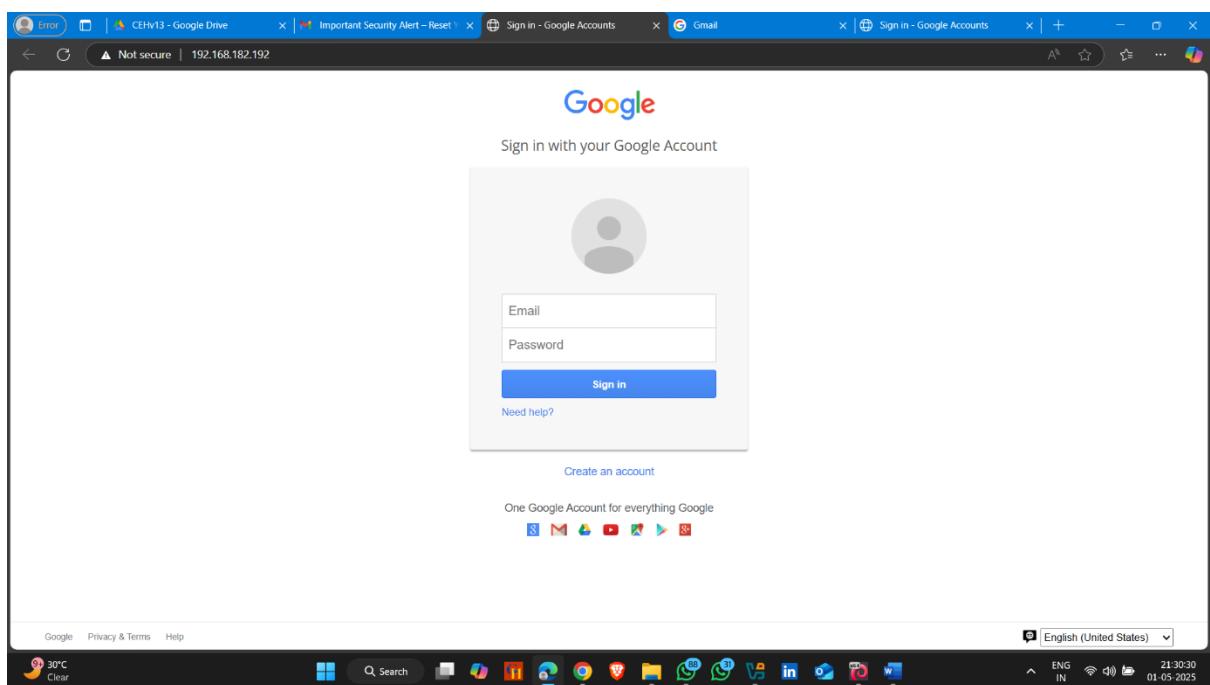
- Now add recipients and generate a mail using AI and it to the target



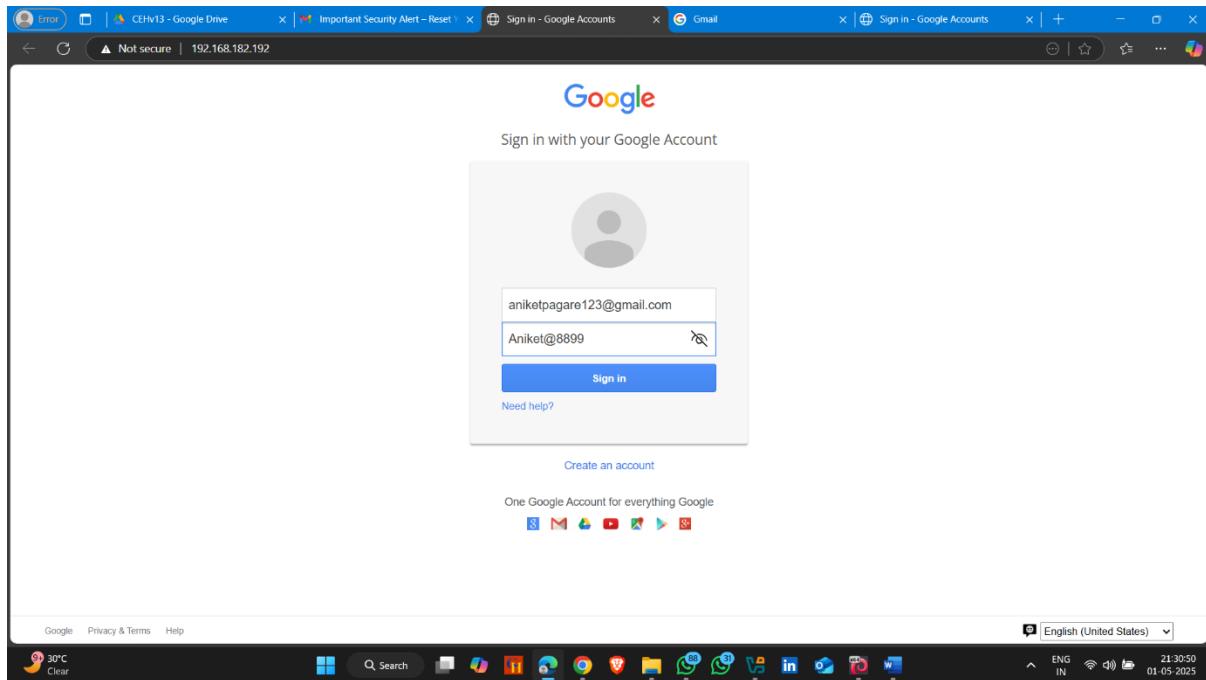
- Mail received**
- Click on link – Reset Your account password**



- Here Fake gmail login page is open



- Enter Credentials and go to the kali linux



- Here , username and password are got it .

```
Kali [Running] - Oracle VirtualBox
File View Input Devices Help
File Actions Edit View Help
3. Twitter
set:webattack> Select a template: 2
[*] Cloning the website: http://www.google.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:
192.168.182.254 - - [01/May/2025 21:22:37] "GET / HTTP/1.1" 200 -
192.168.182.254 - - [01/May/2025 21:22:38] "GET /favicon.ico HTTP/1.1" 404 -
192.168.182.254 - - [01/May/2025 21:30:28] "GET / HTTP/1.1" 200 -
[*] WE GOT A HIT!! Printing the output:
PARAM: GALX=5JLCKfgaqqM
PARAM: continue=https://accounts.google.com/o/oauth2/auth?zt=ChRsWFbwd2JmV1hIcDhtUFdldzBENhIfVWsxSTDNLW9MdThibW1TMFQzVUZFc1BBaUrUwmlRSQ%E%88%9APsBz4gAAAAU
y4_qD7Hbfz38w8kxnaNouLC1D3YTjX
PARAM: service=also
PARAM: dsh=-7381887106725792428
PARAM: _utf8=â
PARAM: bgrresponse=js_disabled
PARAM: pstMsg=1
PARAM: dnConn=
PARAM: checkConnection=
PARAM: checkedDomains=youtube
POSSIBLE USERNAME FIELD FOUND: Email=aniketpagare123@gmail.com
POSSIBLE PASSWORD FIELD FOUND: Passwd=Aniket@8899
PARAM: signIn=Sign+in
PARAM: PersistentCookie=yes
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.

[  ] 30°C
Clear
File Search
Q Search
D M I C A Y N S L V W E P O U I B N K
ENG IN 21:31:07 01-05-2025
```

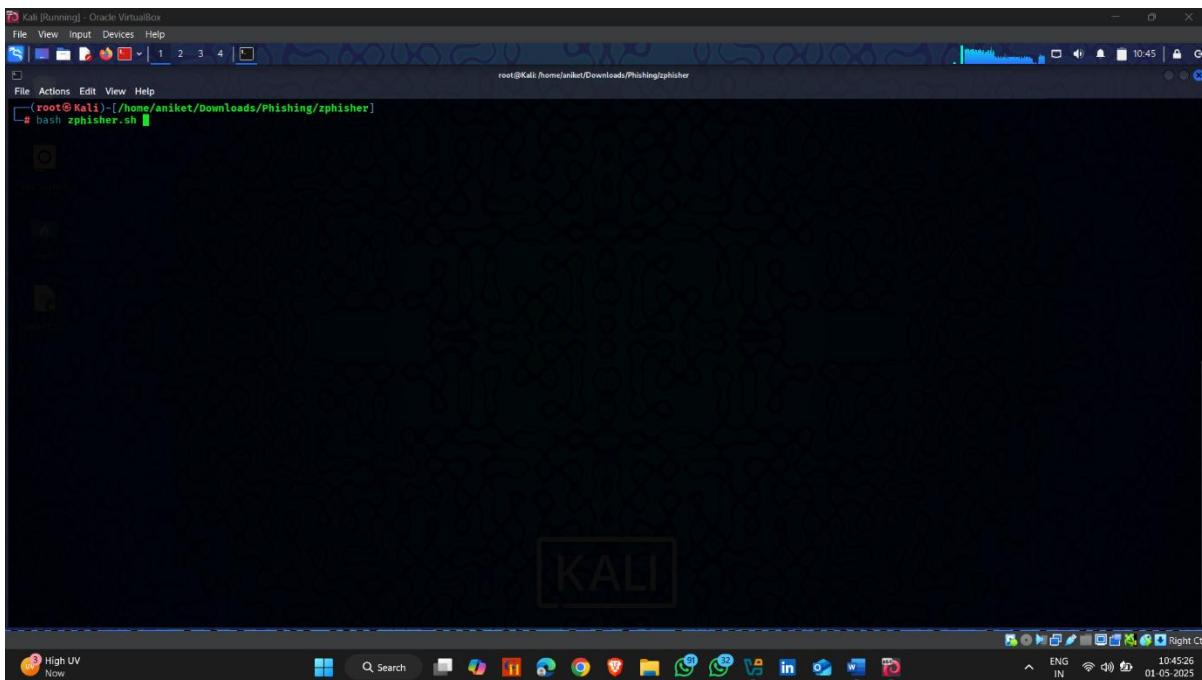
3. Perform Phishing Attack Using Zphisher

Zphisher is an open-source **phishing tool** used primarily for **educational and penetration testing purposes**. It automates the process of creating phishing pages for popular websites like Facebook, Instagram, Twitter, Google, and others, and delivers them via **social engineering techniques**.

Download Link :- <https://github.com/Tohidkhan6332/zphisher>

How to use It :-

- Open kali linux terminal and go to the zphisher directory
- And use command – **bash zphisher.sh**



- **Zphisher open**
- Now select the number that you want to create phishing page

```
ZPHISHER
Version : 2.3.5

[-] Tool Created by htr-tech (ahmid.rayat)

[::] Select An Attack For Your Victim [::]

[01] Facebook      [11] Twitch      [21] DeviantArt
[02] Instagram     [12] Pinterest   [22] Badou
[03] Twitter        [13] Snapchat    [23] Origin
[04] Microsoft      [14] LinkedIn    [24] Dropbox
[05] Netflix         [15] Ebay        [25] Yahoo
[06] Paypal          [16] Quora      [26] Wordpress
[07] Steam           [17] Protonmail [27] Yandex
[08] Twitter         [18] Spotify     [28] StackoverFlow
[09] Playstation    [19] Reddit      [29] Vk
[10] Tiktok          [20] Adobe      [30] XBOX
[31] Mediafire      [32] Gitlab     [33] Github
[34] Discord         [35] Roblox

[99] About          [00] Exit

[-] Select an option :
```

- Now select the **cloudflared server -2**

```
ZPHISHER
Version : 2.3.5

[01] Localhost
[02] Cloudflared [Auto Detects]
[03] LocalXpose  [NEW! Max 15Min]

[-] Select a port forwarding service :
```

- Zphisher started for generate the link

```
[+] Localhost
[+] Cloudflare [Auto Detects]
[+] LocalXpose [NEW! Max 15Min]

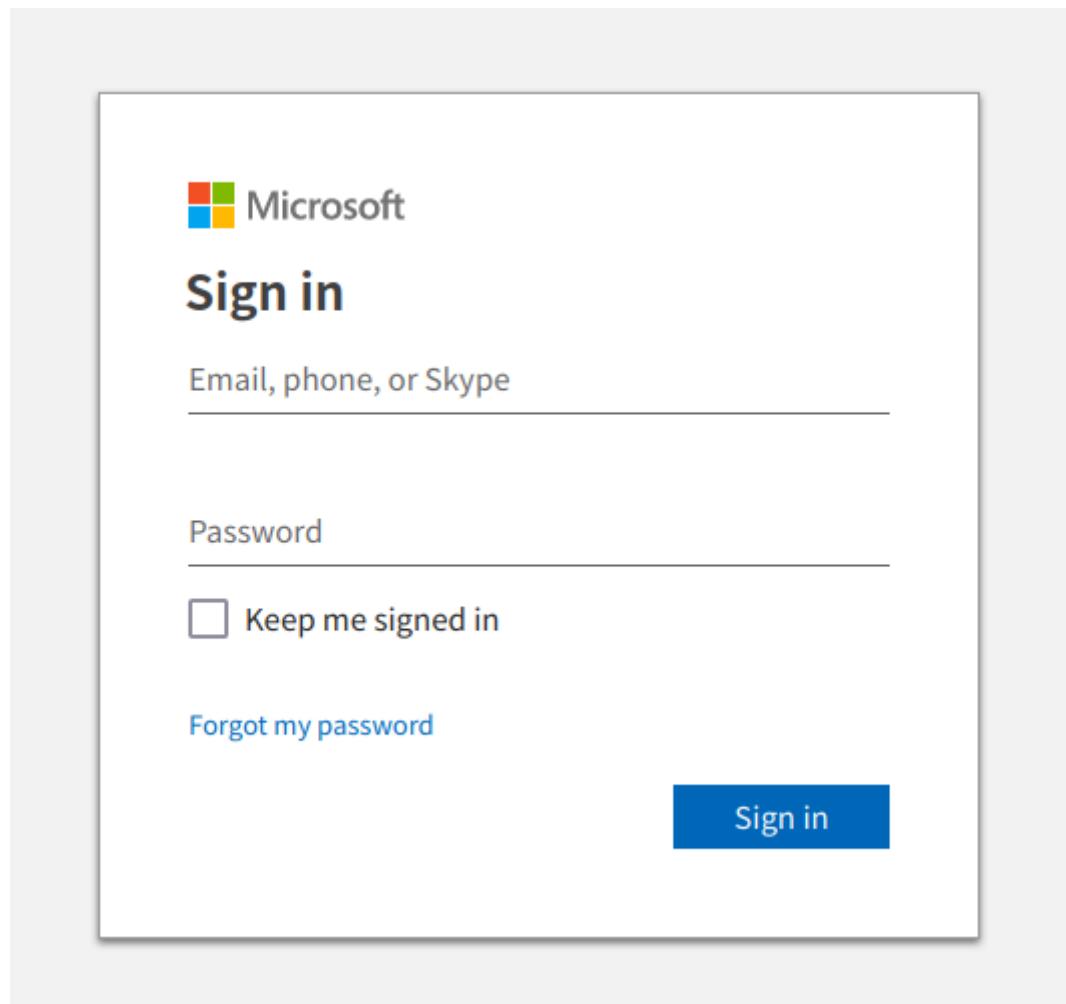
[-] Select a port forwarding service : 2
[?] Do You Want A Custom Port [y/N]: n
[-] Using Default Port 8080...
[-] Initializing... ( http://127.0.0.1:8080 )
[-] Setting up server...
[-] Starting PHP server...
[-] Launching Cloudflare ...
```

- Here , phishing link generated , now copy link and send it to the target

```
[+] AUTHOR : Mr Tohid
[+] FACEBOOK : TohidKhan6333
[+] GITHUB : TohidKhan6332

[+] URL 1 : https://collective-limitations-gloves-approve.trycloudflare.com
[+] URL 2 : https://
[+] URL 3 : https://get-500-usd-free-to-your-account@
[-] Waiting for Login Info, Ctrl + C to exit ...
```

- Now Provide Credentials



```
david@david-kali: ~
```

```
[z] URL 1 : https://profiles-azerbaijan-someone-disagree.cloudflare.com
[-] URL 2 : https://is.gd/PizE3f
[-] URL 3 : https://unlimited-onedrive-space-for-free@is.gd/PizE3f
[-] Waiting for Login Info, Ctrl + C to exit ...
[-] Victim IP Found !
[-] Victim's IP :
[-] Saved in : auth/ip.txt
[-] Login info Found !!
[-] Account : user1@example.com
[-] Password : 45Nople3@k90!
[-] Saved in : auth/usernames.dat
[-] Waiting for Next Login Info, Ctrl + C to exit.
```

EXTRA ACTIVITY

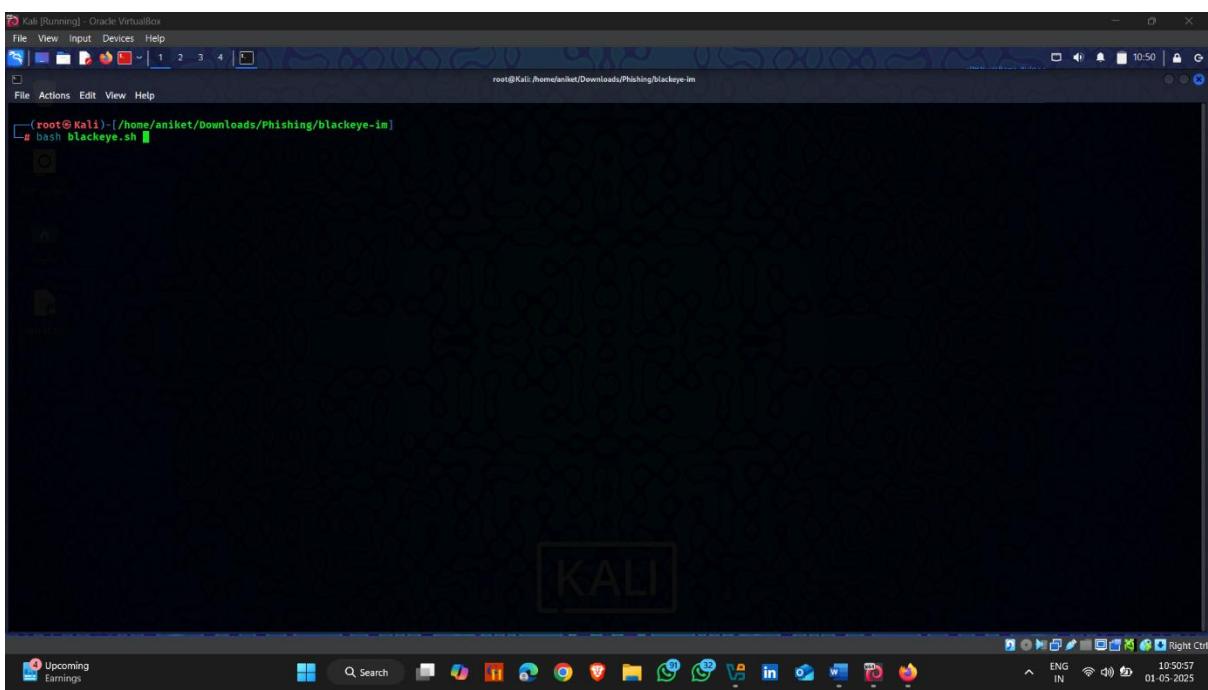
1. Perform Phishing Attack Using Blackeye Tool

Download Link :-

<https://github.com/thewickedkarma/blackeye-im>

How to use it :-

- Open Kali linux terminal and go to the blackeye directory
- Type command – **bash blackeye.sh**



- **Blackeye open**
- Now enter the number that you want to create a fake phishing page

```
[root@Kali :~/home/aniket/Downloads/Phishing/blackeye-im]
# bash blackeye.sh
[!] Disclaimer: Developers assume no liability and are not
responsible for any misuse or damage caused by Blackeye ...
only use for educational purposes!!

[!] Choose an option:[~]
[~] ~ 34
```

- Now select the tunneling method

```
[root@Kali :~/home/aniket/Downloads/Phishing/blackeye-im]
# bash blackeye.sh
[!] Disclaimer: Developers assume no liability and are not
responsible for any misuse or damage caused by Blackeye ...
only use for educational purposes!!

[!] Choose the tunneling method:[~]
[~] ~

[!] Choose an option:[~]
[~] ~ 34

1.Ngrok
2.Localtunnel

[!] Choose the tunneling method:[~]
[~] ~ 2
[*] Starting php server ...
[*] Starting localtunnel server ...

[!] Choose an option:[~]
[~] ~ 34
```

- Here link is generated
- Now copy link and send it to the target

```

Kali [Running] - Oracle VirtualBox
File View Input Devices Help
File Actions Edit View Help
root@Kali: /home/aniket/Downloads/Phishing/blackeye-in
# bash blackeye.sh
[Disclaimer: Developers assume no liability and are not
responsible for any misuse or damage caused by blackeye]
[only use for educational purposes!]

[ Choose an option: ]-[~]
[~] ~ 34

1.Ngrok
2.localetunnel

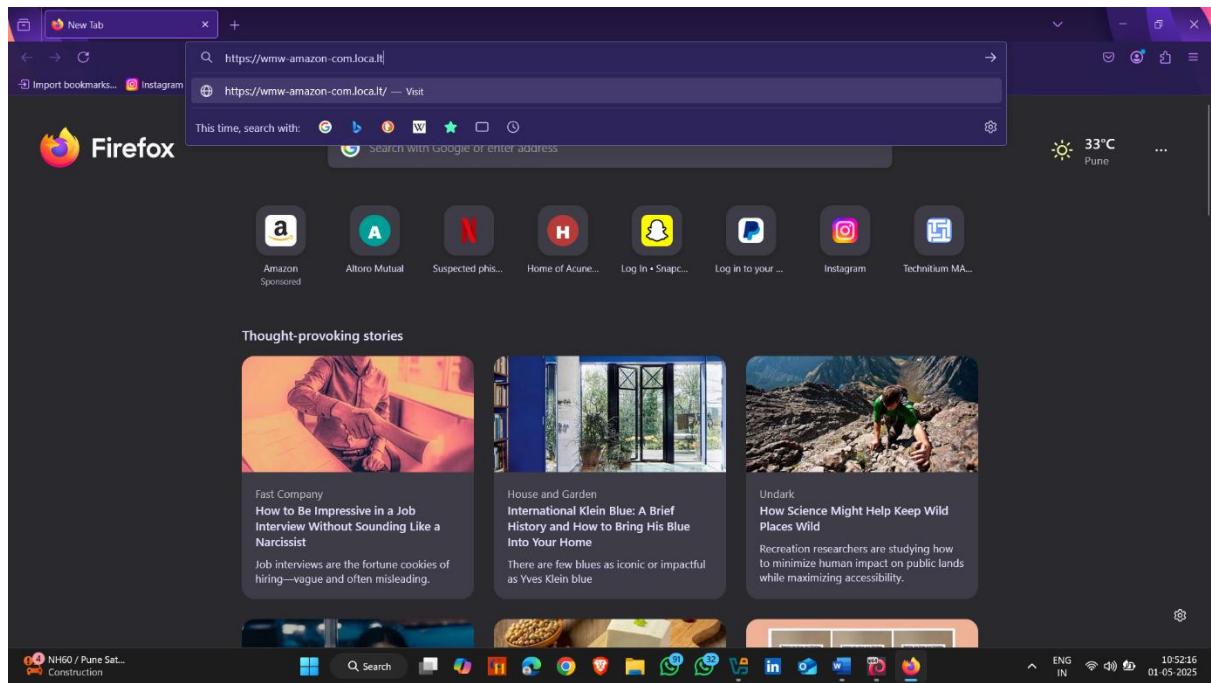
[ Choose the tunneling method: ]-[~]
[~] ~ 2
[~] Starting php server ...
[~] Starting localtunnel server ...
[~] Send this link to the Victim: https://www-amazon-com.loca.lt
[~] Use shortened link instead: https://tinyurl.com/yabxs27v

[*] Waiting victim open the link ...

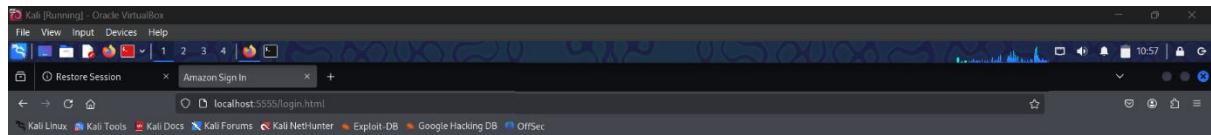
```

The terminal window is titled "Kali [Running] - Oracle VirtualBox". It shows the command "root@Kali: /home/aniket/Downloads/Phishing/blackeye-in" and the execution of "bash blackeye.sh". A disclaimer about liability is displayed. The script lists various social media and service targets with their corresponding index numbers. It then asks for a tunneling method, showing options 1 (Ngrok) and 2 (localetunnel). Finally, it provides a URL for the victim to access.

- Paste link in the url section



- Fake amazon login page open



amazon seller central

Sign in

Email (phone or mobile account)

Password [Forgot your password?](#)

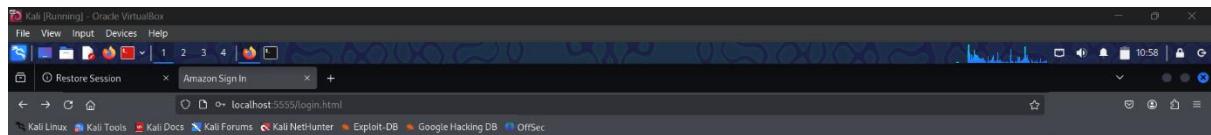
Keep me signed in. [Details](#)

[Register now](#)

Help
© 1996-2018, Amazon.com, Inc. or its affiliates.



- **Provide Credentials and sign in**



amazon seller central

Sign in

Email (phone or mobile account)
ankitapagare123@gmail.com

Password [Forgot your password?](#)

Keep me signed in. [Details](#)

[Register now](#)

Help
© 1996-2018, Amazon.com, Inc. or its affiliates.



- **Now open kali linux teminal**

- **Username and password are captured**

```

root@Kali: /home/aniket/Downloads/Phishing/r3bu5
File View Input Devices Help
File Actions Edit View Help
└── ~ 2
[*] Starting php server ...
[*] Starting localtunnel server ...
[*] Send this link to the Victim: https://www-amazon-com.loca.lt
[*] Use shortened link instead: https://tinyurl.com/yabxxszv

[*] Waiting victim open the link ...

[*] IP Found!
blackeye.sh: line 308: jq: command not found
blackeye.sh: line 309: jq: command not found
blackeye.sh: line 310: jq: command not found
blackeye.sh: line 311: jq: command not found
blackeye.sh: line 312: jq: command not found
blackeye.sh: line 313: jq: command not found
blackeye.sh: line 314: jq: command not found
blackeye.sh: line 315: jq: command not found
blackeye.sh: line 316: jq: command not found
blackeye.sh: line 317: jq: command not found
[*] IPv6: 127.0.0.1
[*] User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
[*] Country:
[*] Region:
[*] City:
[*] Postal:
[*] Location:
[*] ISP:
[*] Timezone:
[*] Saved: amazon/saved.ip.txt
[*] Waiting credentials ...
[*] Credentials Found!
[*] Account: amilvepazare123@gmail.com
[*] Password: 112233445566
[*] Saved: sites/amazon/saved.usernames.txt
[root@Kali:~/home/aniket/Downloads/Phishing/r3bu5]
#
```

2. Perform Phishing Attack Using r3bu5 Tool

How to use it :-

- Open kali linux Terminal and go to the r3bu5 Directory
- And type command – **bash r3bu5.sh** and enter

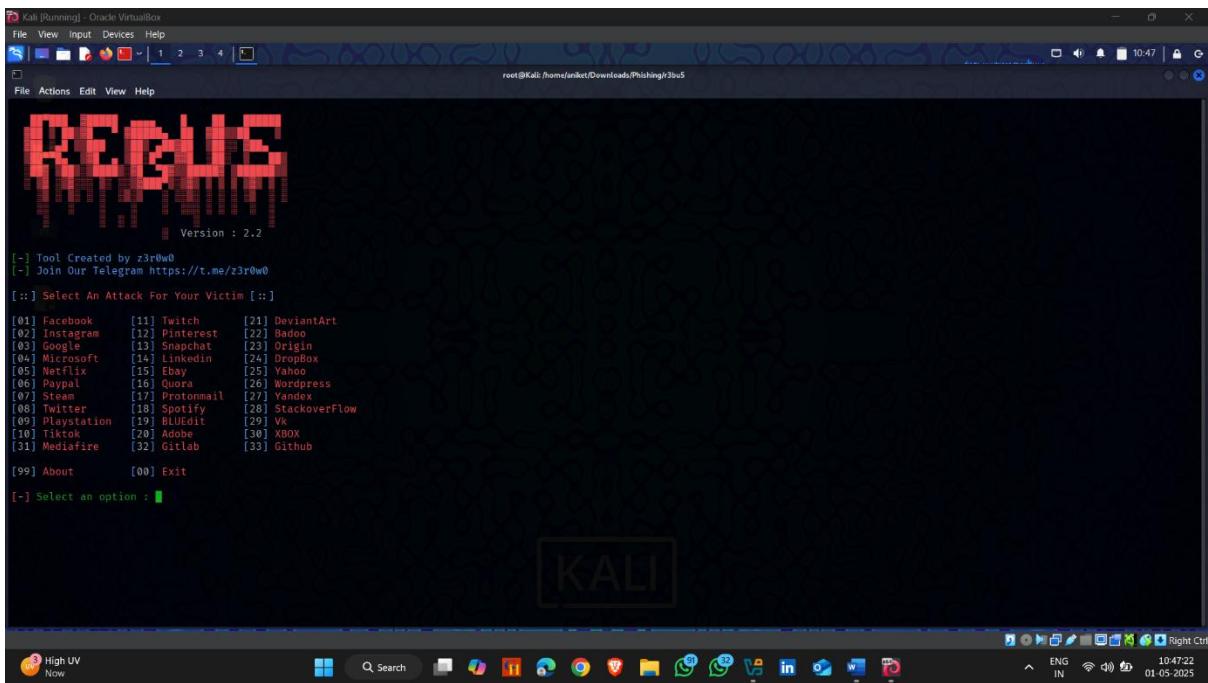
```

root@Kali: /home/aniket/Downloads/Phishing/r3bu5
File View Input Devices Help
File Actions Edit View Help
File Actions Edit View Help
└── ~ 2
[*] Starting php server ...
[*] Starting localtunnel server ...
[*] Send this link to the Victim: https://www-amazon-com.loca.lt
[*] Use shortened link instead: https://tinyurl.com/yabxxszv

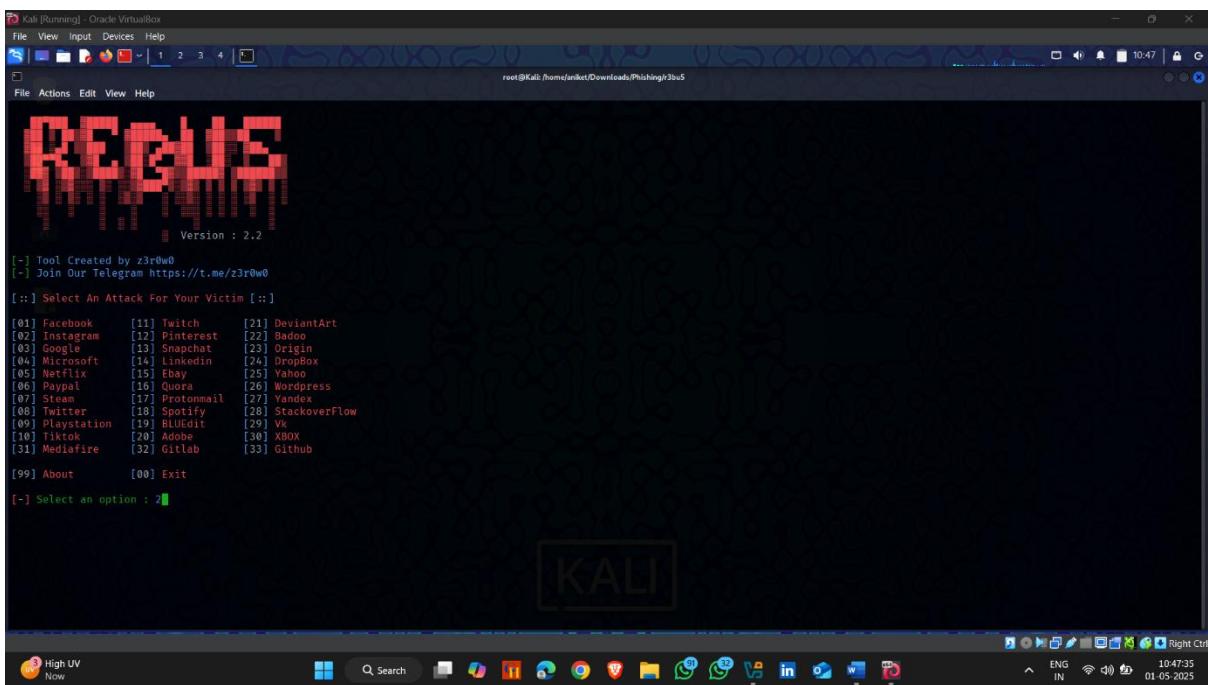
[*] Waiting victim open the link ...

[*] IP Found!
blackeye.sh: line 308: jq: command not found
blackeye.sh: line 309: jq: command not found
blackeye.sh: line 310: jq: command not found
blackeye.sh: line 311: jq: command not found
blackeye.sh: line 312: jq: command not found
blackeye.sh: line 313: jq: command not found
blackeye.sh: line 314: jq: command not found
blackeye.sh: line 315: jq: command not found
blackeye.sh: line 316: jq: command not found
blackeye.sh: line 317: jq: command not found
[*] IPv6: 127.0.0.1
[*] User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
[*] Country:
[*] Region:
[*] City:
[*] Postal:
[*] Location:
[*] ISP:
[*] Timezone:
[*] Saved: amazon/saved.ip.txt
[*] Waiting credentials ...
[*] Credentials Found!
[*] Account: amilvepazare123@gmail.com
[*] Password: 112233445566
[*] Saved: sites/amazon/saved.usernames.txt
[root@Kali:~/home/aniket/Downloads/Phishing/r3bu5]
#
```

- R3bu5 start



- now select the number for create a phishing site



- Now select the option for what kind of login page you want

```
R3BUS - 2.2
Version : 2.2

[-] Tool Created by z3r0w0
[-] Join Our Telegram https://t.me/z3r0w0

[::] Select An Attack For Your Victim [::]

[01] Facebook      [11] Twitch      [21] DeviantArt
[02] Instagram     [12] Pinterest   [22] Badoo
[03] Google         [13] Snapchat    [23] Origin
[04] Microsoft     [14] LinkedIn    [24] DropBox
[05] Netflix        [15] Ebay        [25] Yahoo
[06] Paypal         [16] Quora       [26] Wordpress
[07] Steam          [17] Protonmail [27] Yandex
[08] Twitter        [18] Spotify     [28] StackoverFlow
[09] Playstation    [19] BLUEdit    [29] Vk
[10] Tiktok         [20] Adobe      [30] XBOX
[31] Mediafire     [32] Gitleb     [33] Github

[99] About          [00] Exit

[-] Select an option : 2

[01] Traditional Login Page
[02] Auto Followers Login Page
[03] 1000 Followers Login Page
[04] Blue Badge Verify Login Page

[-] Select an option : 1
```

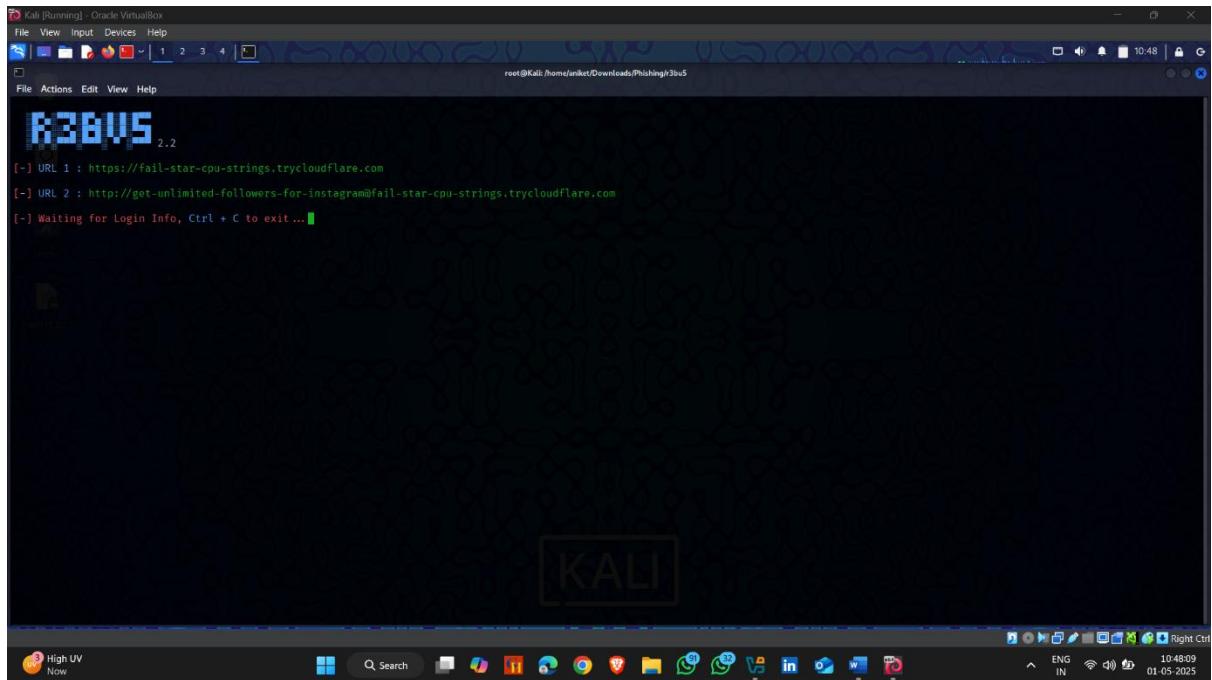
- Select the server

```
R3BUS - 2.2

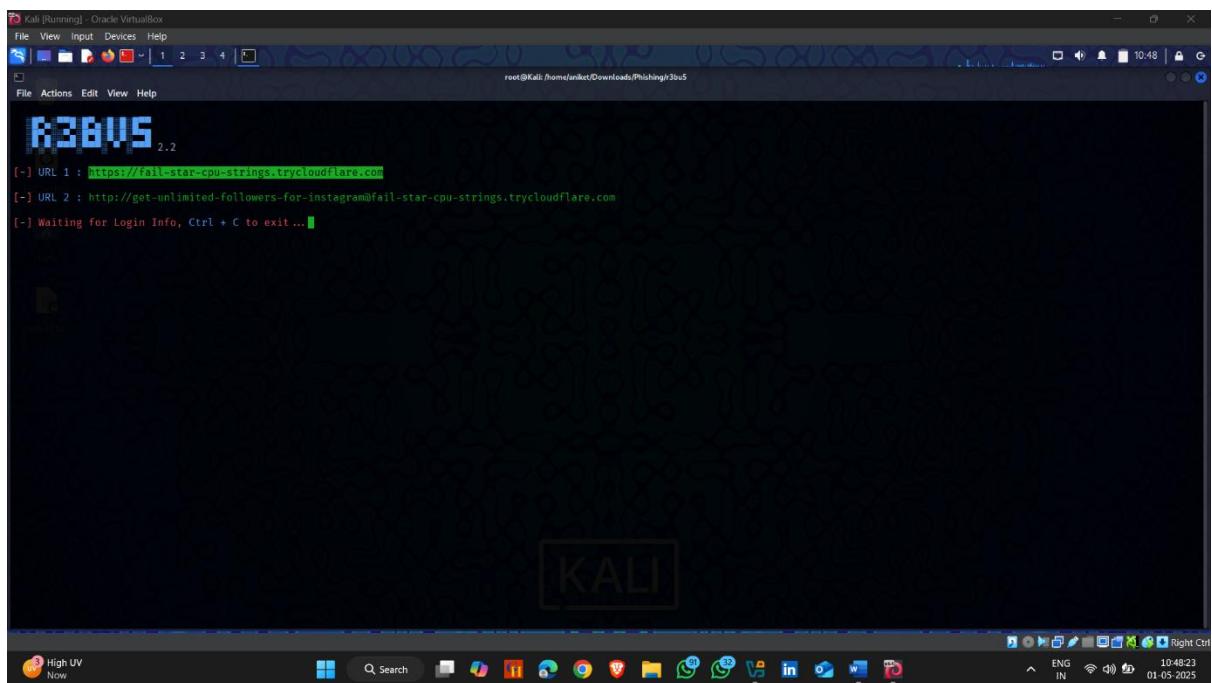
[01] Localhost      [For Devs]
[02] Ngrok.io       [Buggy]
[03] Cloudflared    [New!]

[-] Select a port forwarding service : 3
```

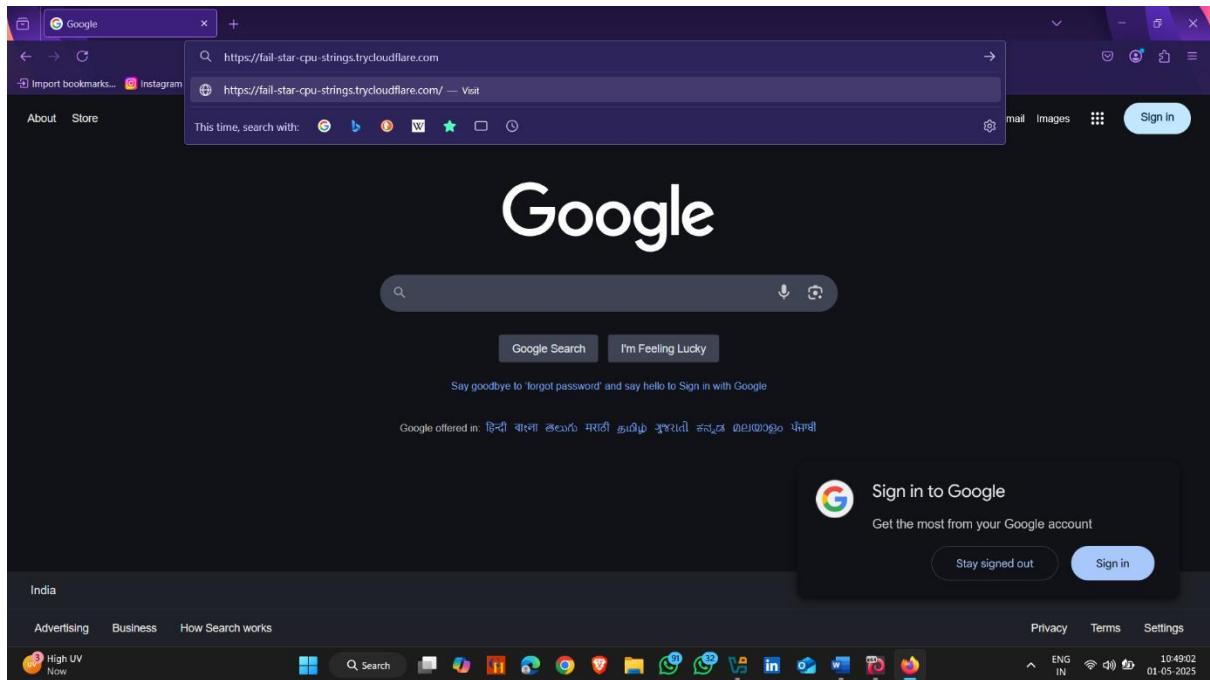
- Link is Generated



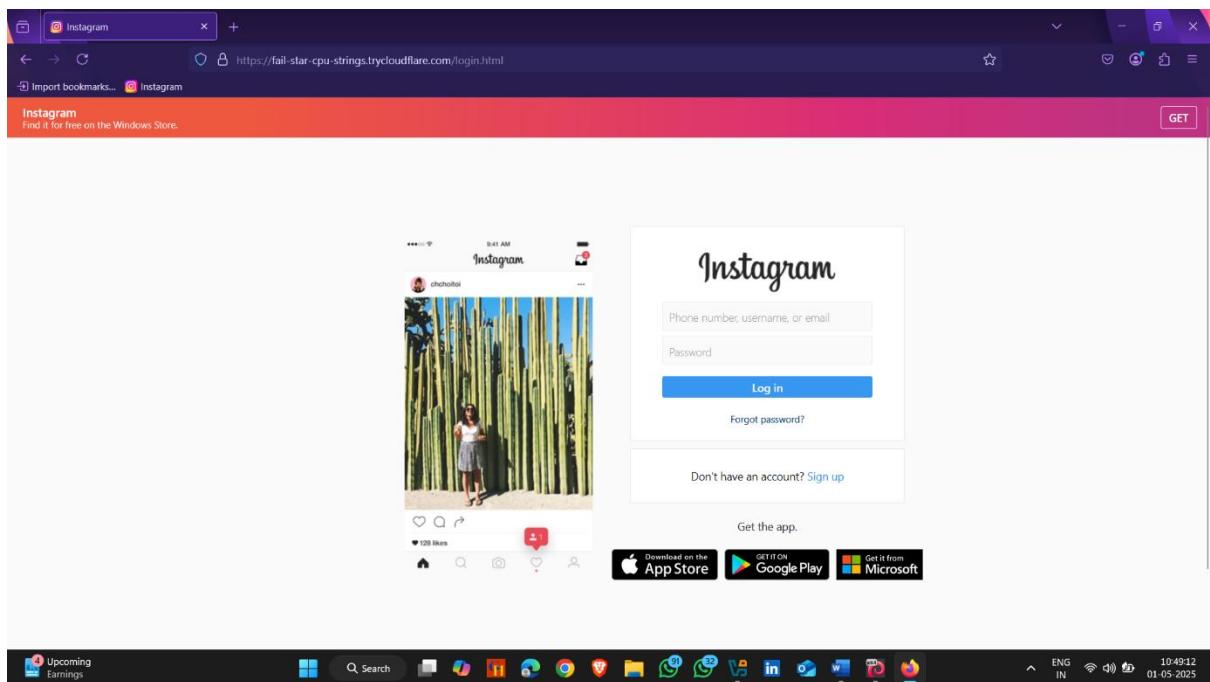
- Copy first url and send it to the target



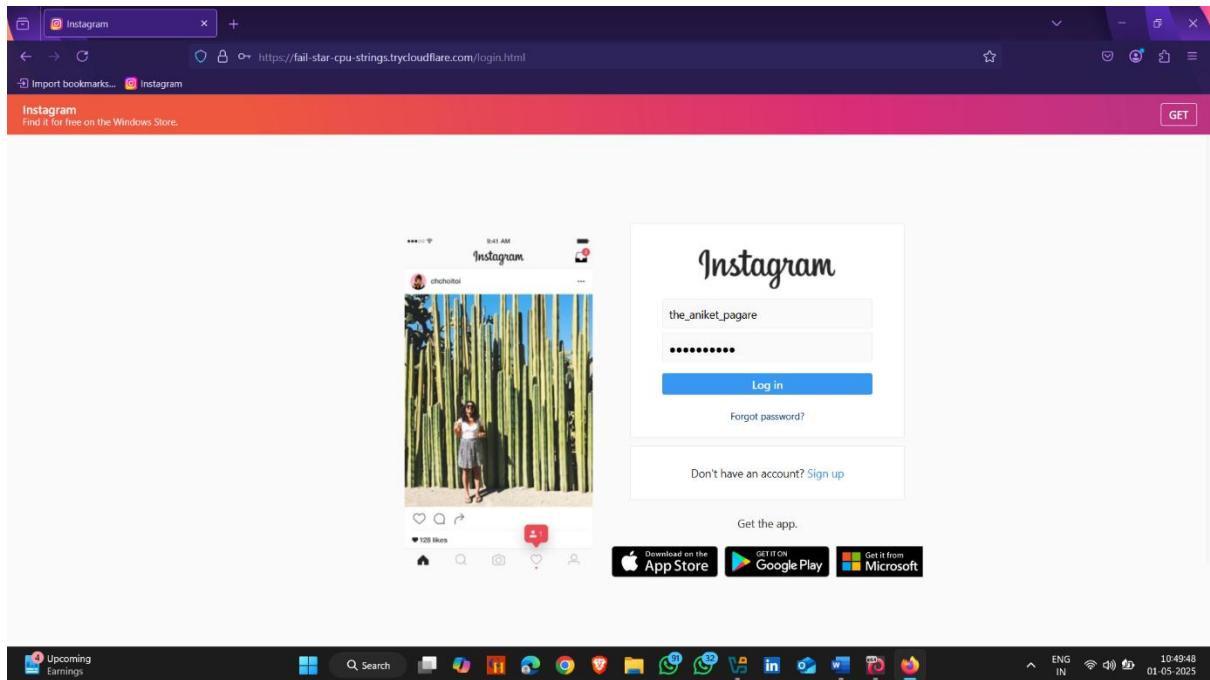
- Paste it on url section and enter



- Phishing page generate successfully



- Enter username and password



- Open kali linux and see can it capture the username and password

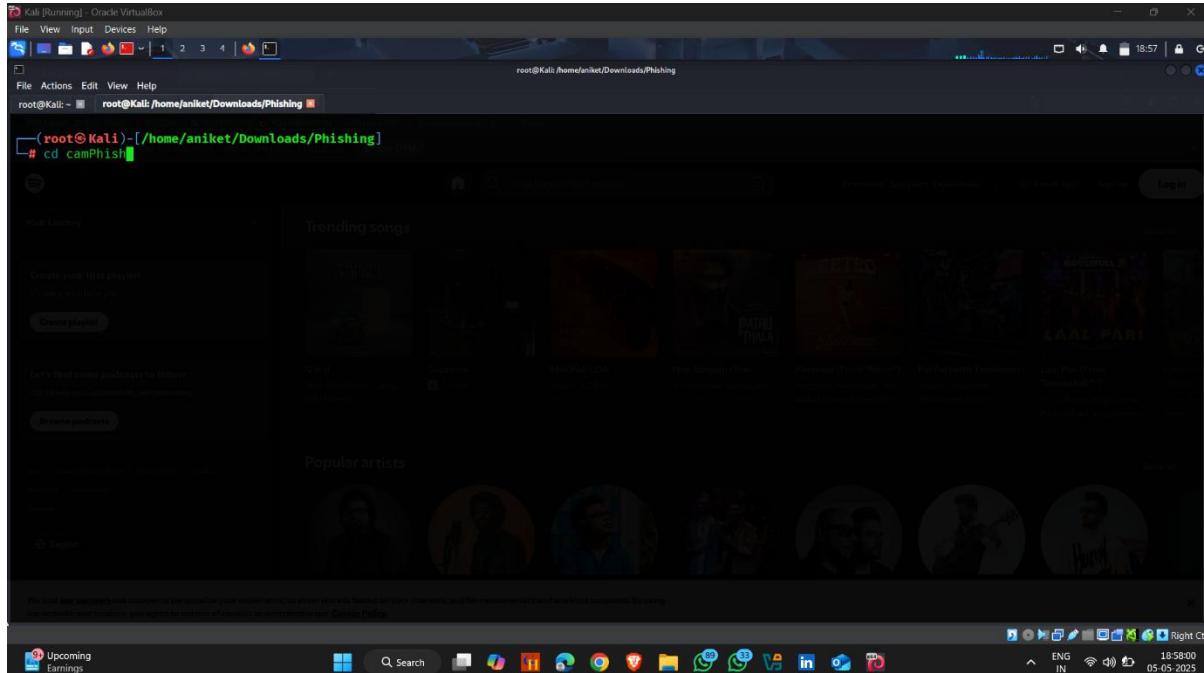
- Username and password are captured

```
Kali [Running] - Oracle VirtualBox
File View Input Devices Help
File Actions Edit View Help
152.58.32.16
152.58.32.16
[-] Saved in : ip.txt
[-] Victim IP Found !
[-] Victim's IP : 152.58.32.16
152.58.32.16
152.58.32.16
152.58.32.16
[-] Saved in : ip.txt
[-] Victim IP Found !
[-] Victim's IP : 34.83.203.92
[-] Saved in : ip.txt
[-] Victim IP Found !
[-] Victim's IP : 34.83.203.92
[-] Saved in : ip.txt
[-] Victim IP Found !
[-] Victim's IP : 34.83.203.92
[-] Saved in : ip.txt
[-] Login info Found !!
[-] Account : the_aniket_pagare
[+] Password : Aniket234
[-] Saved in : usernames.dat
[-] Waiting for Next Login Info, Ctrl + C to exit. ■
KALI
File View Input Devices Help
File Actions Edit View Help
152.58.32.16
152.58.32.16
[-] Saved in : ip.txt
[-] Victim IP Found !
[-] Victim's IP : 152.58.32.16
152.58.32.16
152.58.32.16
152.58.32.16
[-] Saved in : ip.txt
[-] Victim IP Found !
[-] Victim's IP : 34.83.203.92
[-] Saved in : ip.txt
[-] Victim IP Found !
[-] Victim's IP : 34.83.203.92
[-] Saved in : ip.txt
[-] Login info Found !!
[-] Account : the_aniket_pagare
[+] Password : Aniket234
[-] Saved in : usernames.dat
[-] Waiting for Next Login Info, Ctrl + C to exit. ■
KALI
```

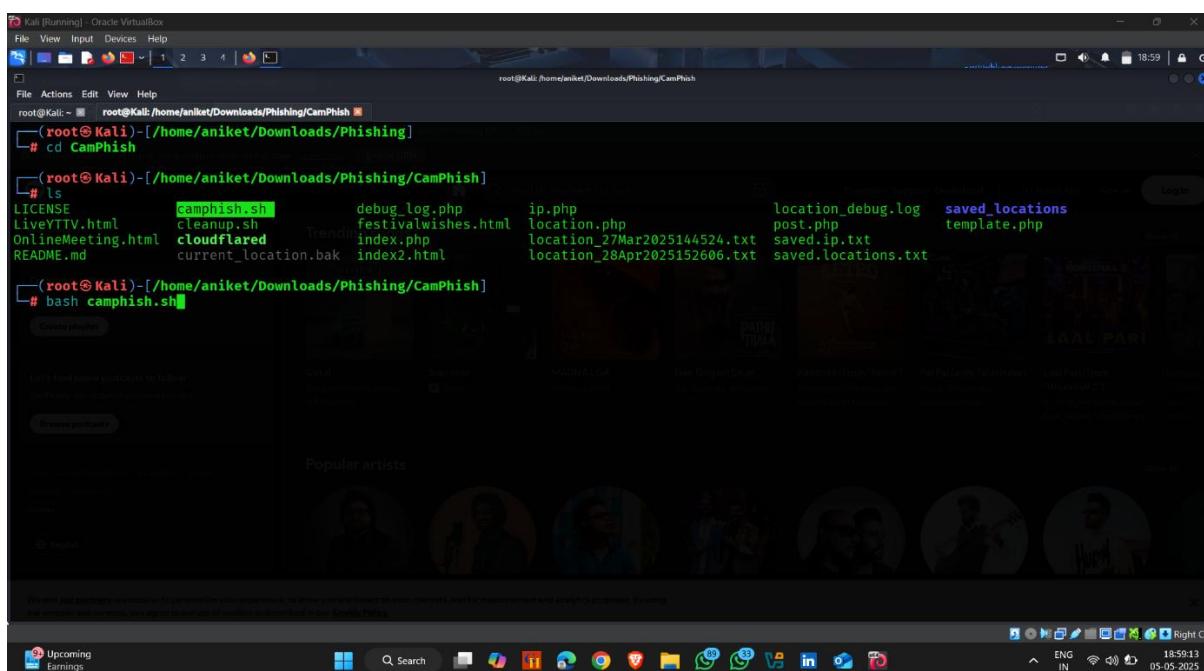
3. Perform Phishing Attack Using CamPhish Tool

How to use it :-

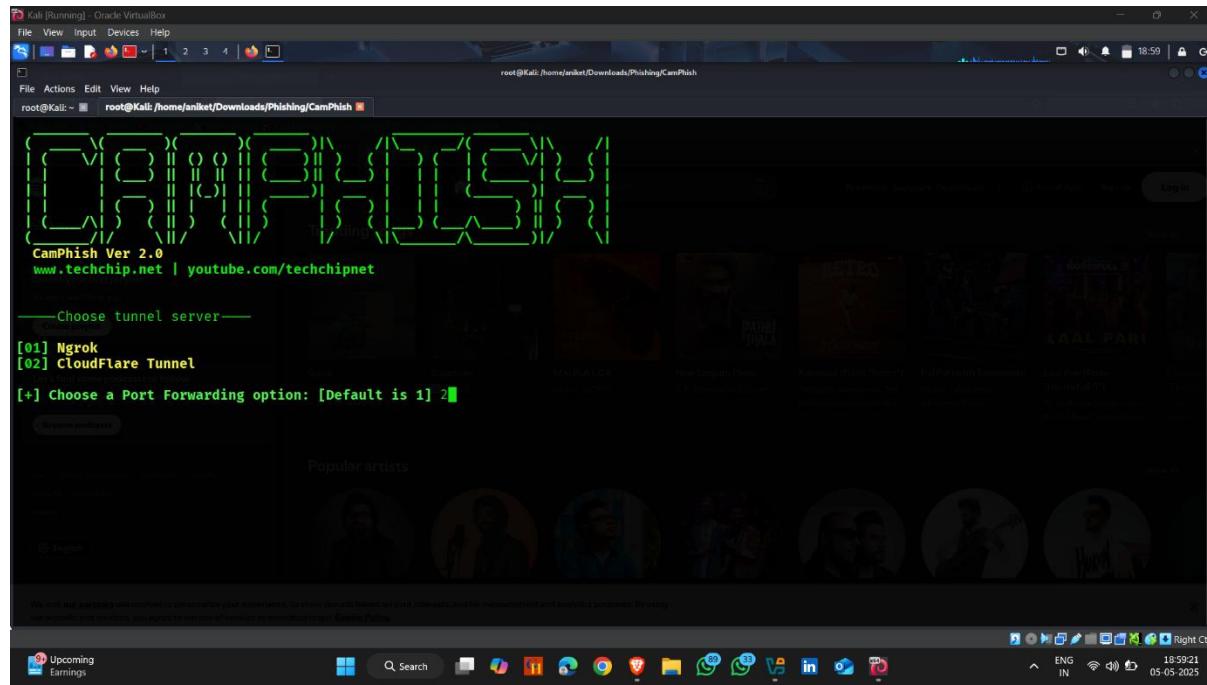
- Open kali linux terminal go to the camphish directory



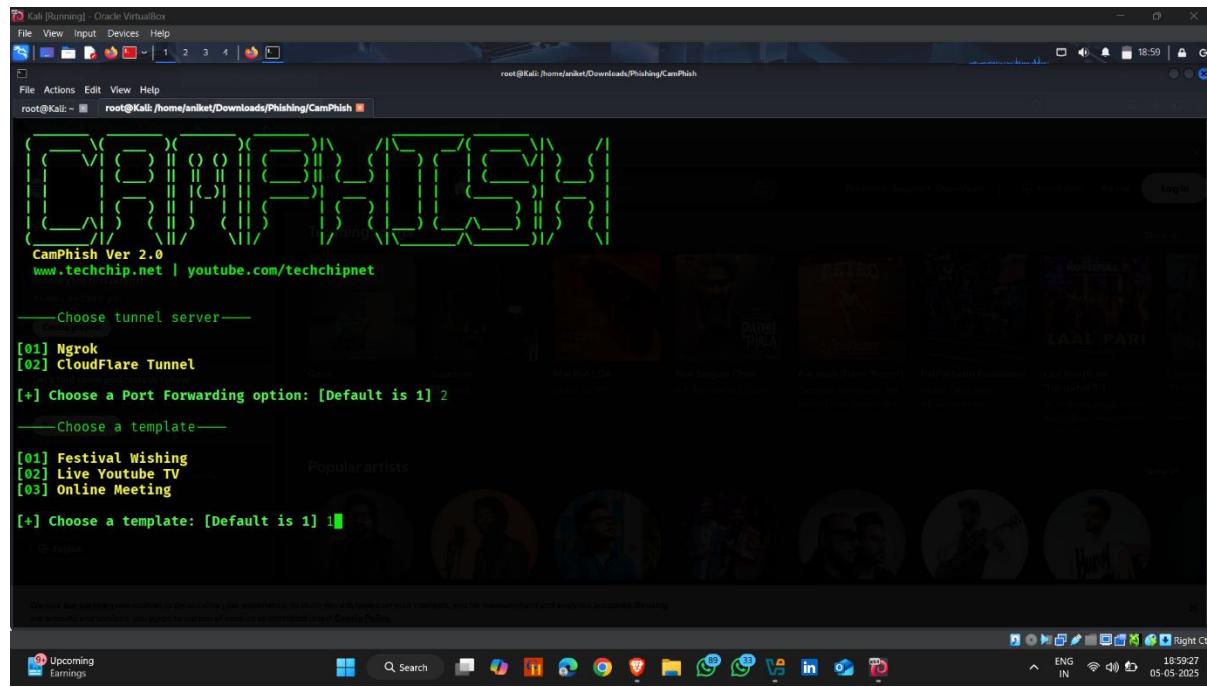
- Type command **-bash camphish**



- Select Server – cloudflare tunnel



- Select 1



- Enter Message

```
Kali [Running] - Oracle VirtualBox
File View Input Devices Help
File Actions Edit View Help
root@Kali: ~ root@Kali:/home/aniket/Downloads/Phishing/CamPhish
CamPhish Ver 2.0
www.techchip.net | youtube.com/techchipnet

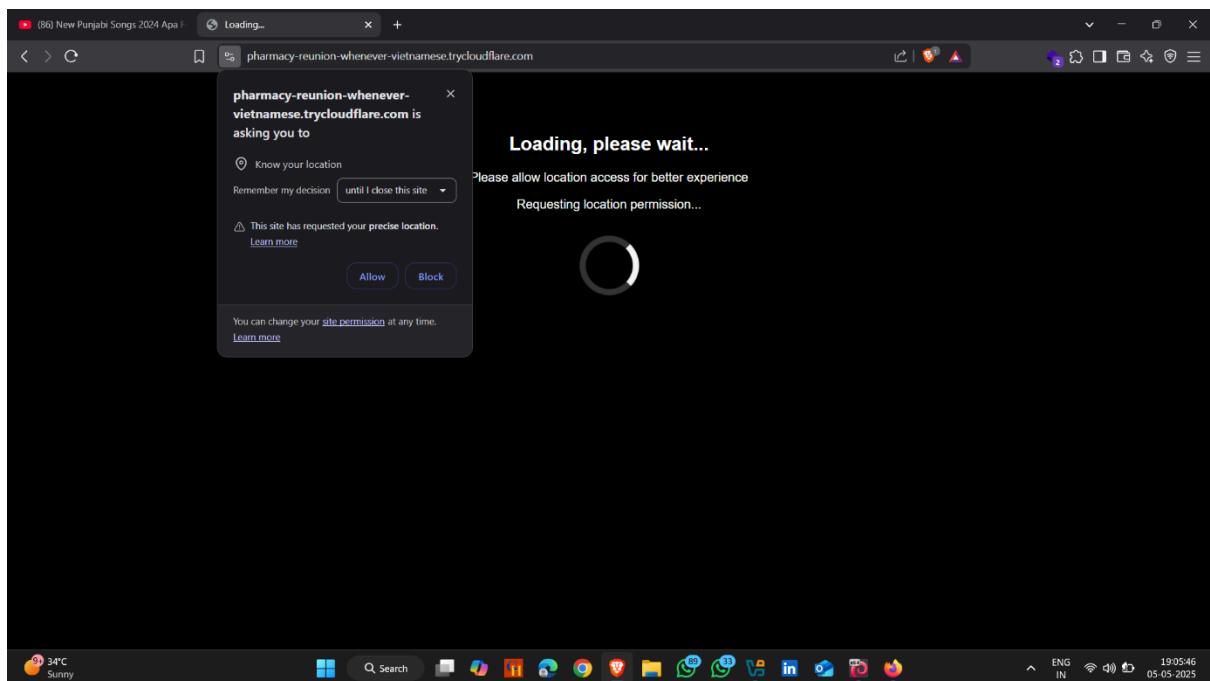
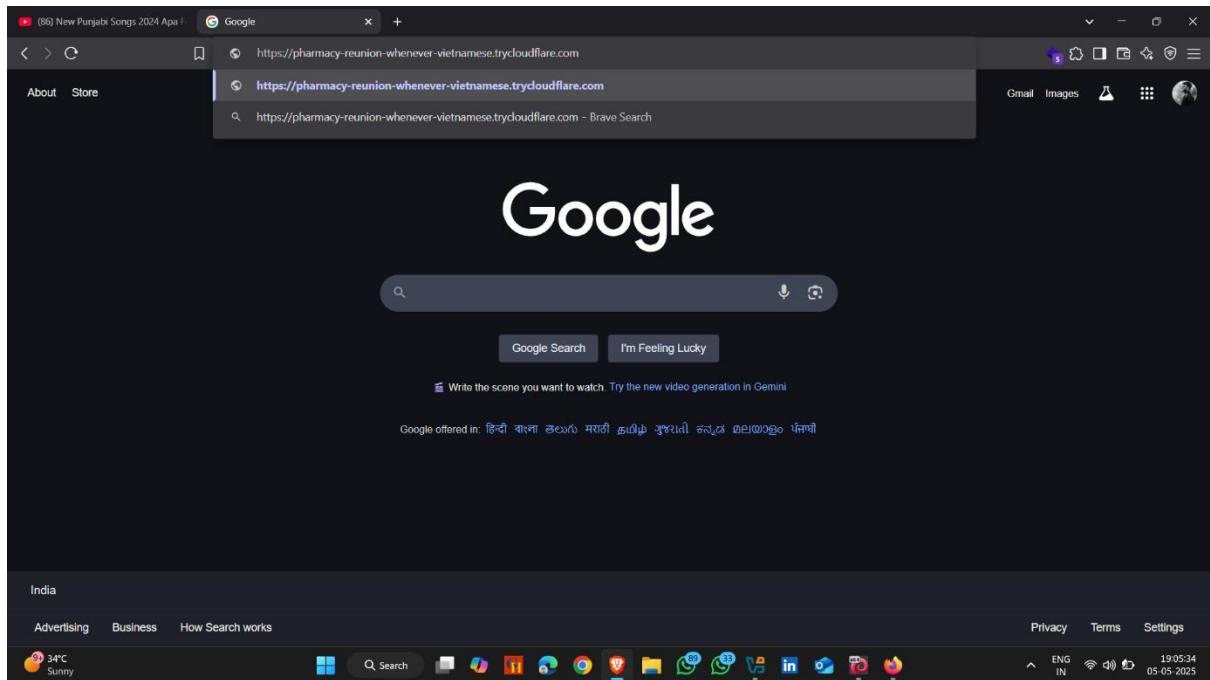
Choose tunnel server—
[01] Ngrok
[02] CloudFlare Tunnel
[+] Choose a Port Forwarding option: [Default is 1] 2
Choose a template—
[01] Festival Wishing
[02] Live Youtube TV
[03] Online Meeting
[+] Choose a template: [Default is 1] 1
[+] Enter festival name: Happy Diwali

Upcoming Earnings
ENG IN 18:59:50 05-05-2025
```

- Link Generated

```
Kali [Running] - Oracle VirtualBox
File View Input Devices Help
File Actions Edit View Help
root@Kali: ~ root@Kali:/home/aniket/Downloads/Phishing/CamPhish
CamPhish Ver 2.0
www.techchip.net | youtube.com/techchipnet
Trending songs
Choose tunnel server—
[01] Ngrok
[02] CloudFlare Tunnel
[+] Choose a Port Forwarding option: [Default is 1] 2
Choose a template—
[01] Festival Wishing
[02] Live Youtube TV
[03] Online Meeting
[+] Choose a template: [Default is 1] 1
[+] Enter festival name: Happy Diwali
[+] Starting php server ...
[+] Starting cloudflared tunnel...
[*] Direct link: https://panama-boring-elected-do.trycloudflare.com
[*] Waiting targets, Press Ctrl + C to exit...
[*] GPS Location tracking is ACTIVE
Upcoming Earnings
ENG IN 19:00:11 05-05-2025
```

- Paste link on Browser



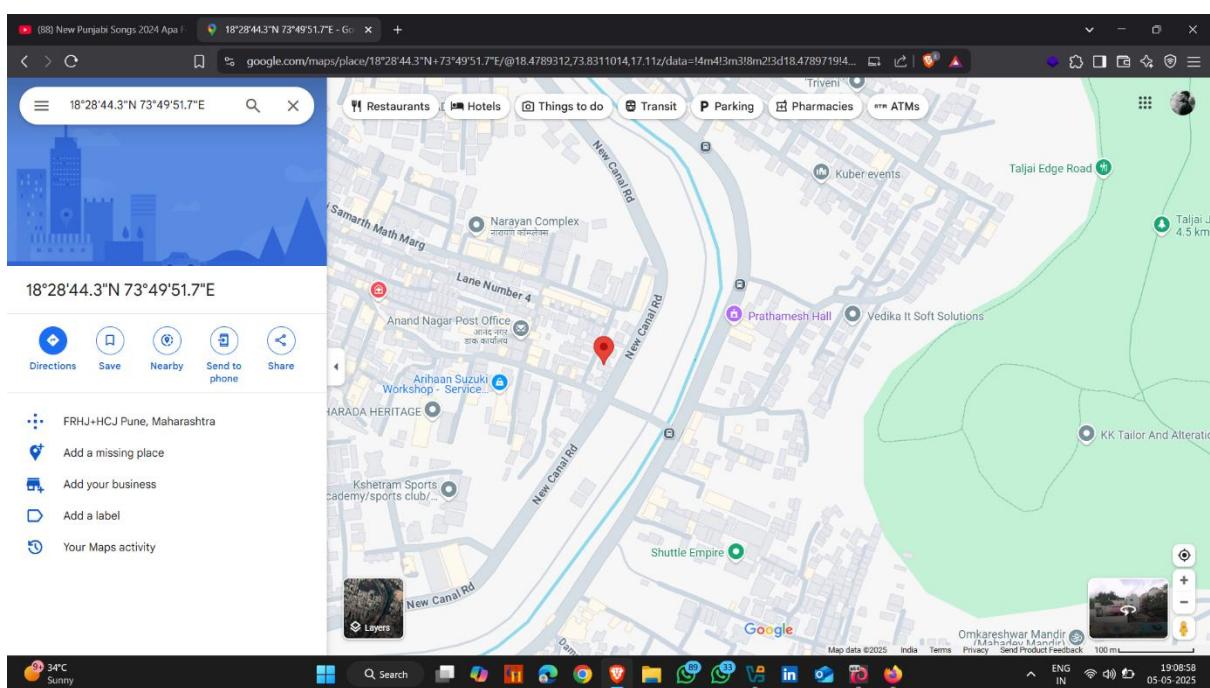
- **Here It capture the photos and Location**

Kali [Running] - Oracle VirtualBox

File View Input Devices Help

File Actions Edit View Help

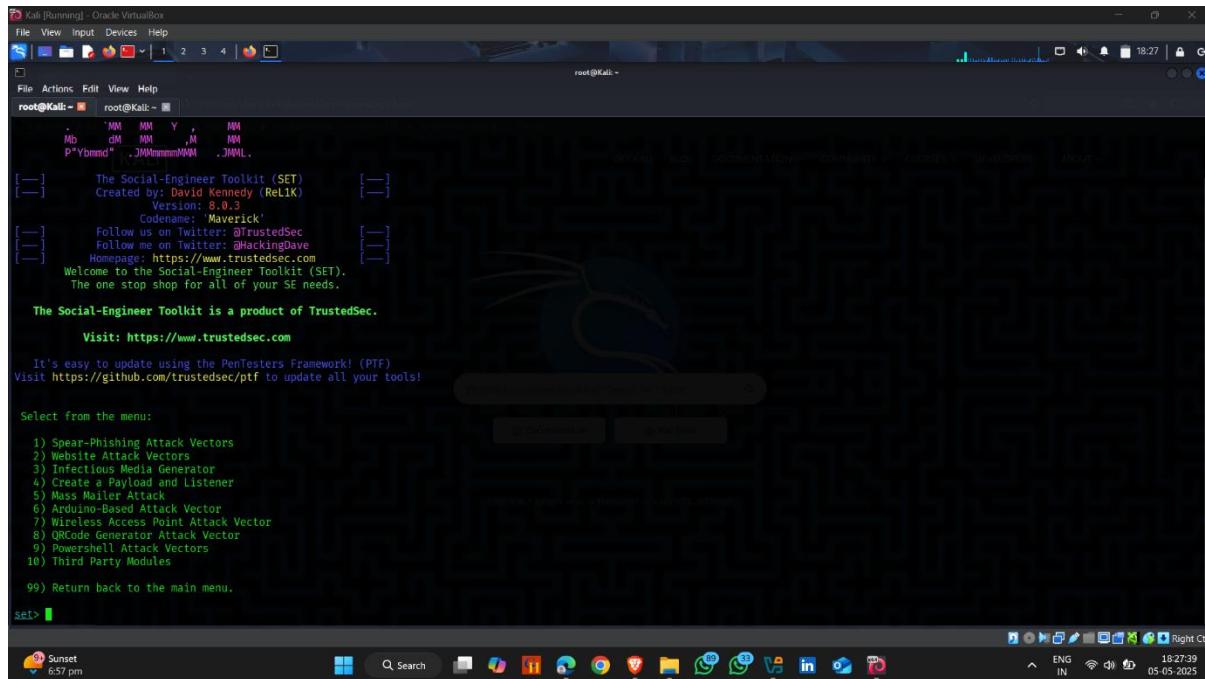
```
[root@Kali ~]# ls
LICENSE           cam05May2025133543.png  cam05May2025133549.png  cloudflared   index.php    location_05May2025133527.txt  post.php    template.php
LiveYTVC.html    cam05May2025133544.png  cam05May2025133550.png  current_location.bak  index2.html  location_27Mar202514524.txt  saved.ip.txt
OnlineMeeting.html cam05May2025133546.png  camphish.sh    debug_log.php  ip.php      location_28Apr2025152606.txt  saved.locations.txt
README.md        cam05May2025133547.png  cleanup.sh    festivalwishes.html  location.php  location_debug.log  saved_locations.txt
[root@Kali ~]
```



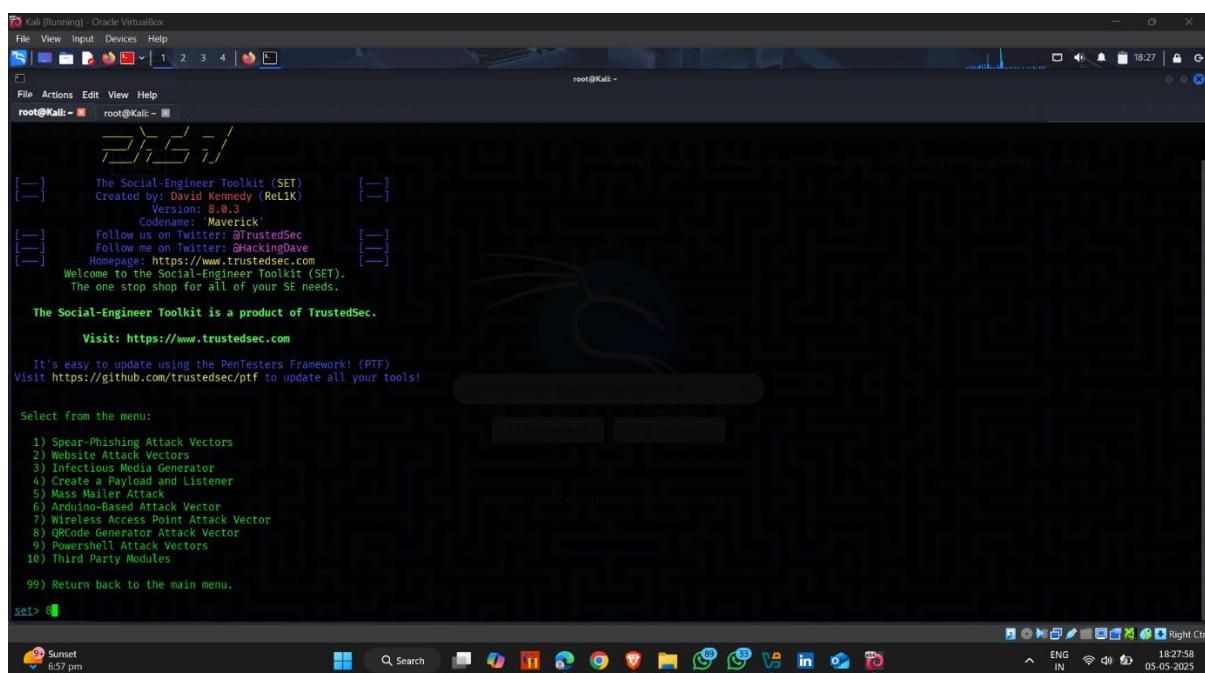
4. Perform QRCode Generate Using SETOOLKIT

How to do it :-

- Open kali linux terminal and type **setoolkit**



- And Select option 8 - QRcode Generator Attack Vector



- Now paste url that you want to generate a qrcode

```

root@Kali:~# Follow us on Twitter: @TrustedSec
root@Kali:~# Follow me on Twitter: @HackingDave
root@Kali:~# Homepage: https://www.trustedsec.com
root@Kali:~# Welcome to the Social-Engineer Toolkit (SET).
root@Kali:~# The one stop shop for all of your SE needs.

The Social-Engineer Toolkit is a product of TrustedSec.
Visit: https://www.trustedsec.com Trending songs

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> 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 maller.

Enter the URL you want the QRCode to go to (99 to exit): https://open.spotify.com/

```

- Here , qrcode generated successfully and copy it and paste it on another terminal

```

root@Kali:~# The one stop shop for all of your SE needs.

The Social-Engineer Toolkit is a product of TrustedSec.
Visit: https://www.trustedsec.com Trending songs

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> 8
The QRCode Attack Vector will create a QRCode for you with whatever URL you want.

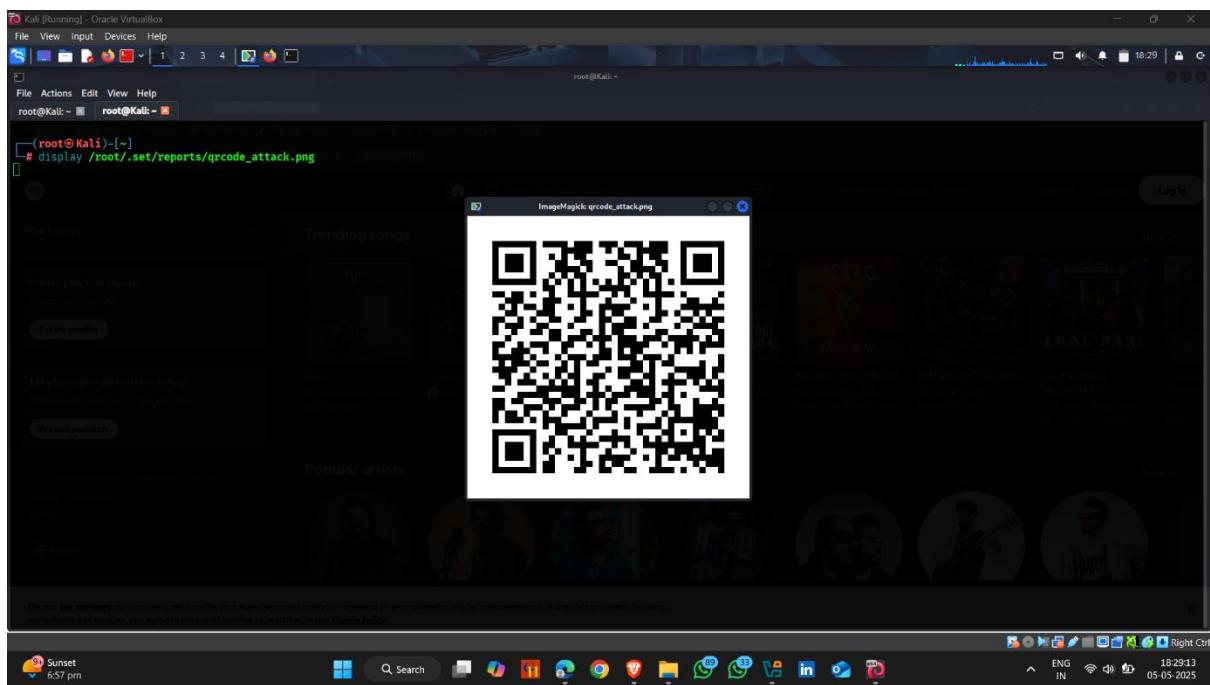
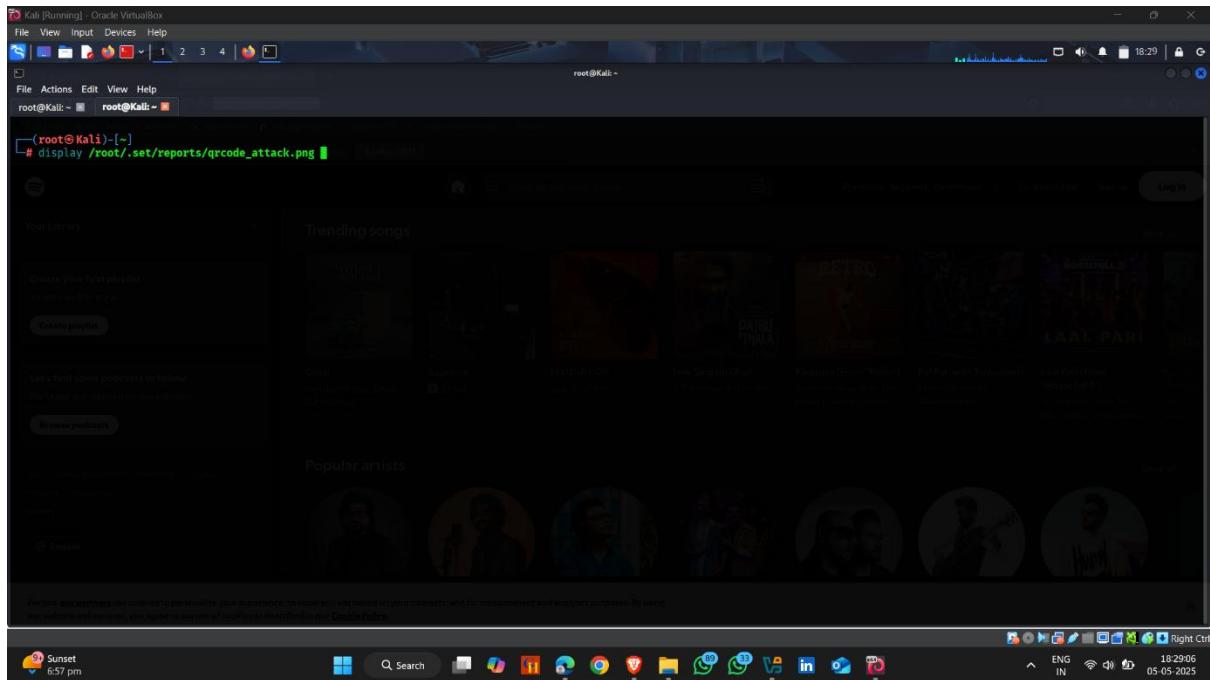
When you have the QRCode Generated, select an additional attack vector within SET and
deploy the QRCode to your victim. For example, generate a QRCode of the SET Java Applet
and send the QRCode via a maller.

Enter the URL you want the QRCode to go to (99 to exit): https://open.spotify.com/
[*] QRCode has been generated under /root/.set/reports/qrcode.attack.png

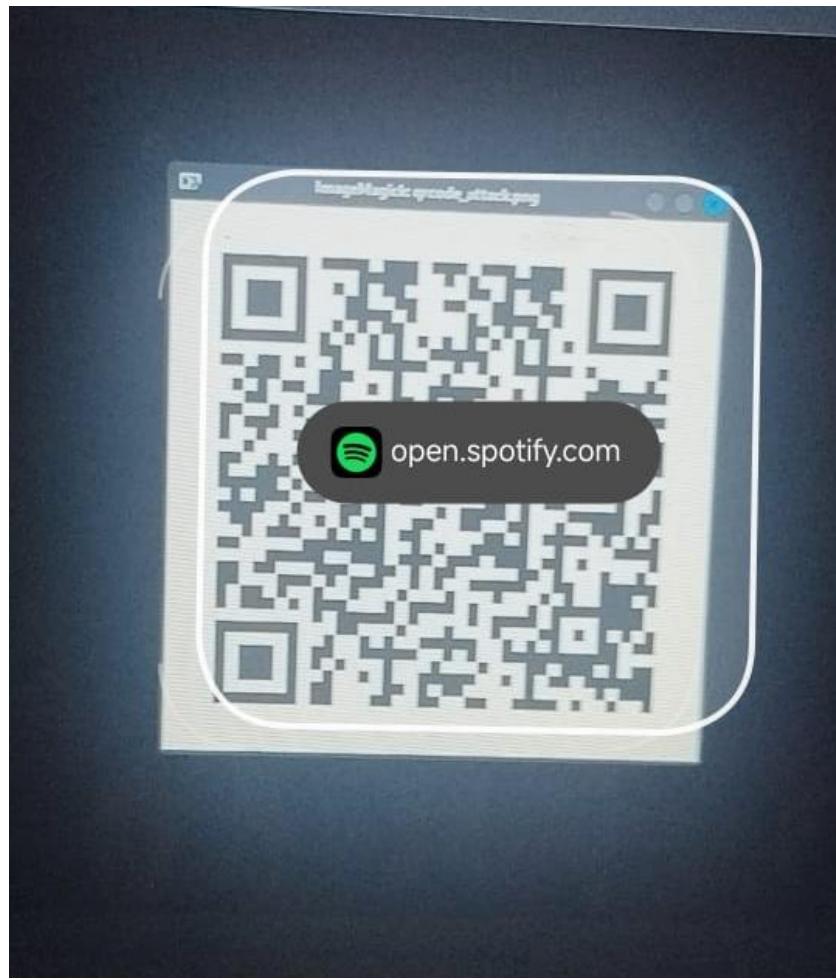
Press <return> to continue

```

- Now open New terminal
- And used command – display and paste qrcode



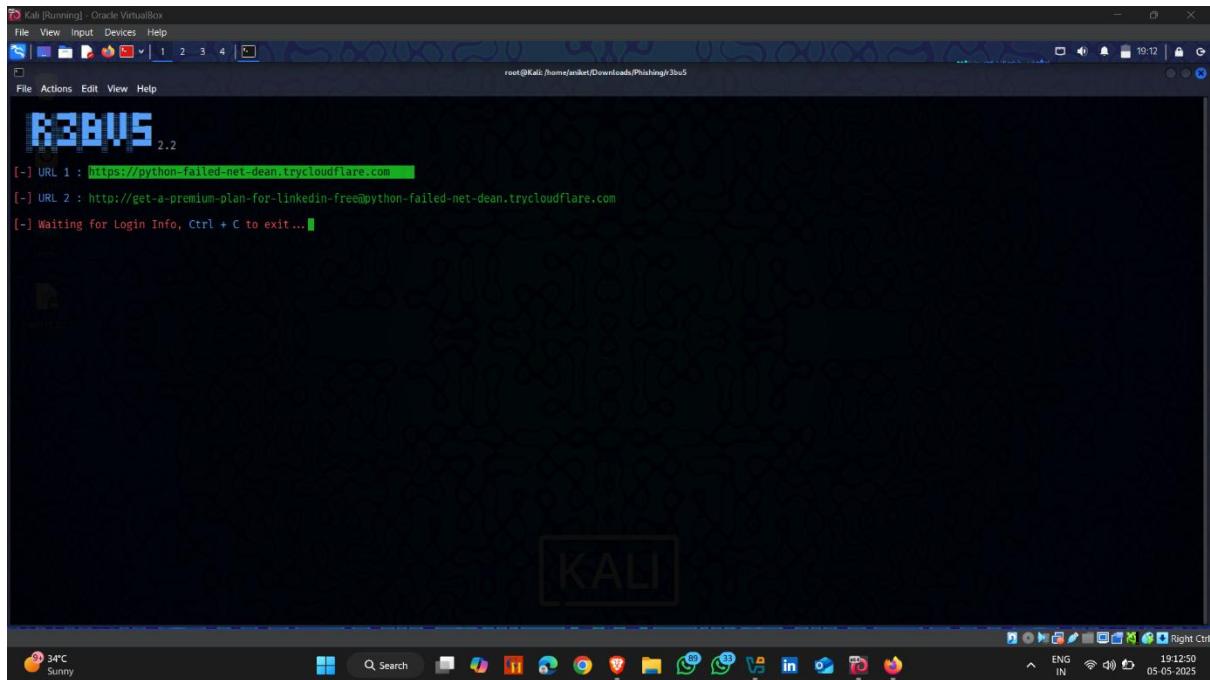
- Here spotify qrcode generated



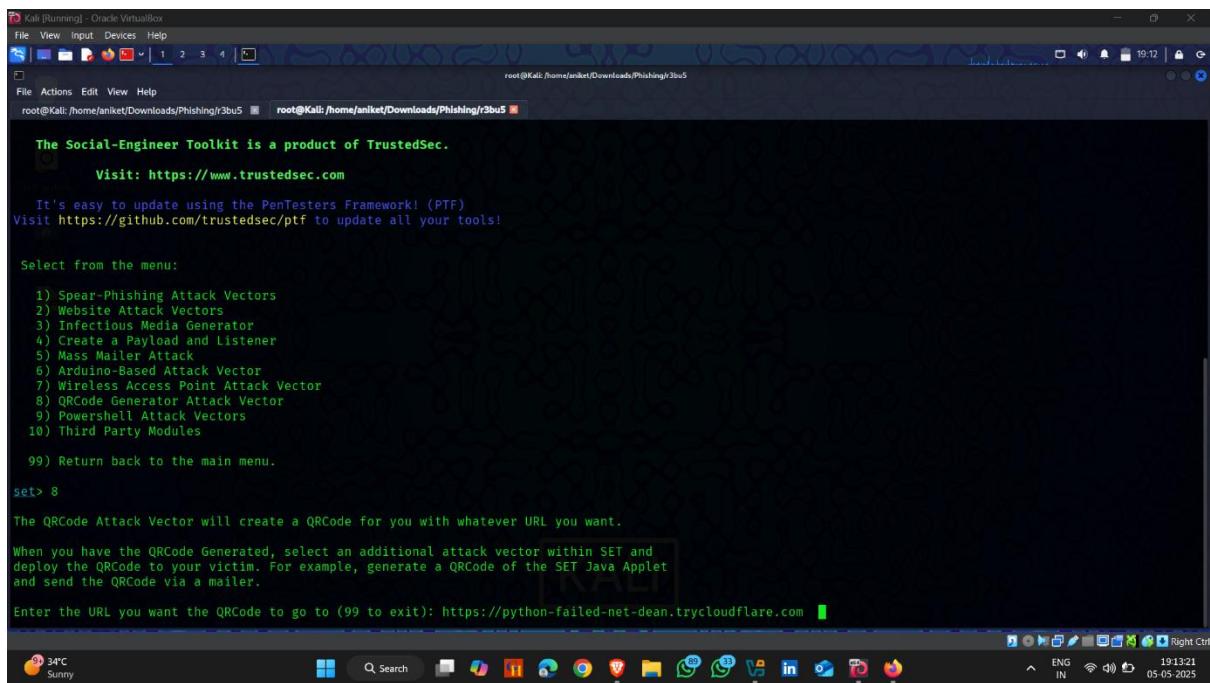
5. Perform Phishing QRCode Generate Using SETOOLKIT

How to use it :-

- Open kali linux terminal and generate a phishing link
- Phishing link generated



- Now open SETOOLKIT , select qrcode generator option and paste phishing link



- Qrcode generated successfully

```
Kali [Running] - Oracle VirtualBox
File View Input Devices Help
File Actions Edit View Help
root@Kali: /home/aniket/Downloads/Phishing/r3bu5  root@Kali: /home/aniket/Downloads/Phishing/r3bu5

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> 8

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

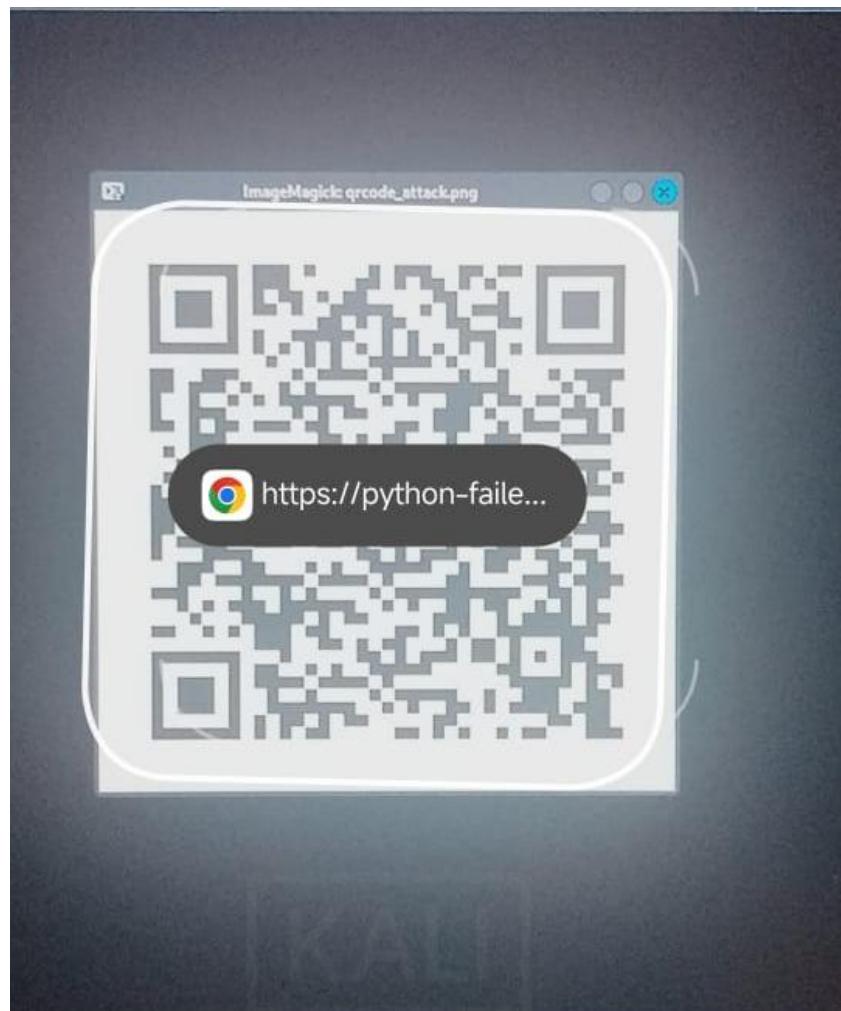
When you have the QRCode Generated, select an additional attack vector within SET and
deploy the QRCode to your victim. For example, generate a QRCode of the SET Java Applet
and send the QRCode via a mailer.

Enter the URL you want the QRCode to go to (99 to exit): https://python-failed-net-dean.trycloudflare.com
[*] QRCode has been generated under /root/.set/reports/qrcode_attack.png

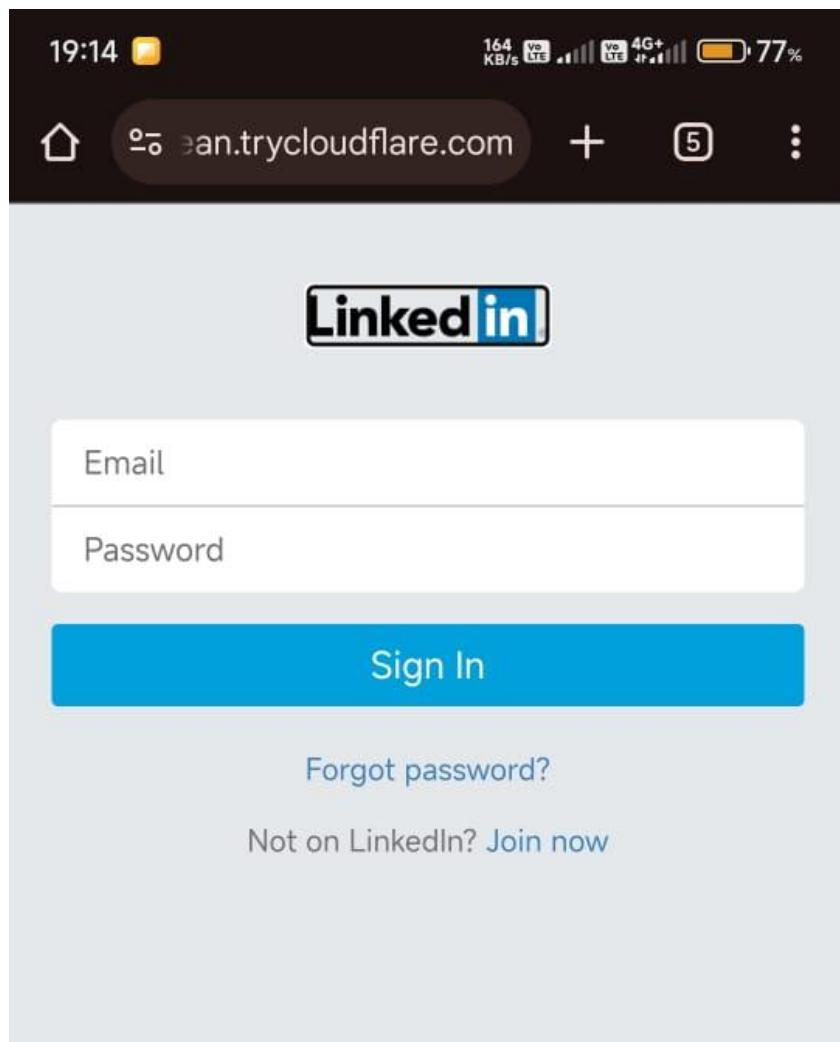
Press <return> to continue

34°C
Sunny
Q Search ENG IN 19:13:31 05-05-2025
```

- Phishing QRcode 🤲



- Type credentials



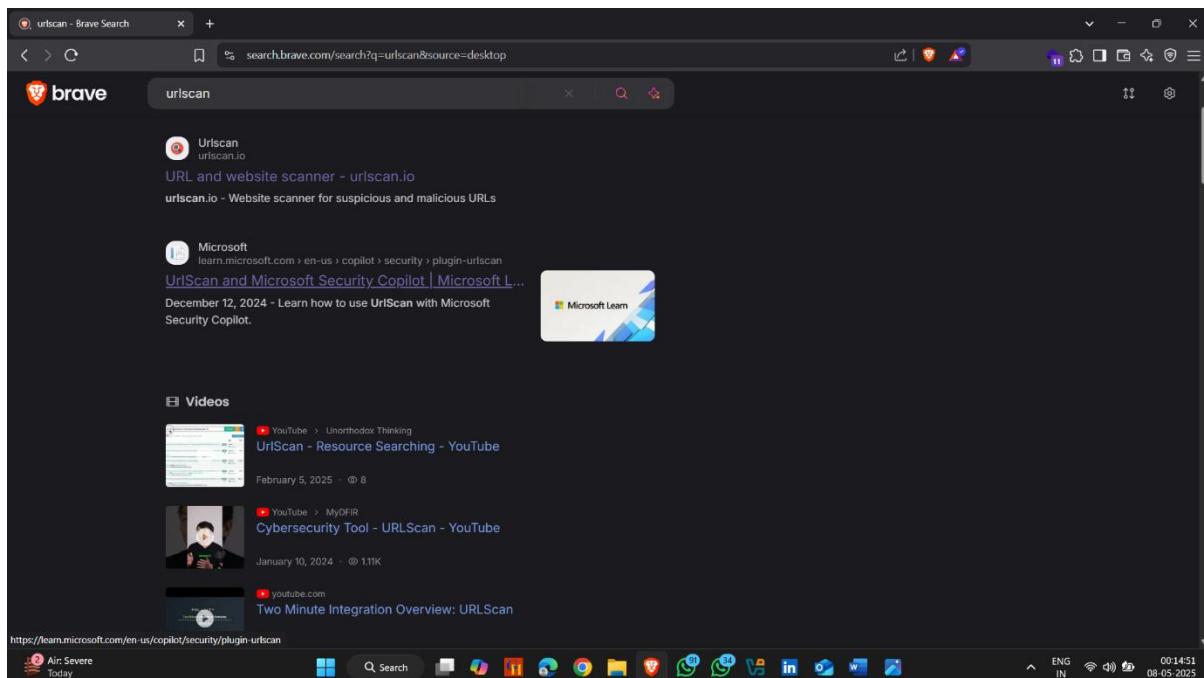
- Now go back to the phishing terminal and you see the credentials

PHISHING DETECTION TOOLS

1. Perform Phishing Detection Using URLScan Website

How to use it :-

- Click on urlscan.io website



- Paste Phishing Link

The screenshot shows the urlscan.io homepage. At the top, there's a navigation bar with links for Home, Search, Live, API, Blog, Docs, Pricing, and Login. A banner for SecurityTrails is visible. Below the header, the urlscan.io logo and tagline 'A sandbox for the web' are displayed. A search bar labeled 'URL to scan' has 'https://www.google.com' typed into it. To the right of the search bar are two buttons: '▶ Public Scan' and '⚙ Options'. Underneath the search bar, a section titled 'Recent scans' shows a list of URLs with their respective details: Age, Size, IPs, and a small icon. The list includes various websites like wktvip.com, thetradingpost.news, bitcoinnetwork.com, and fynnovation.com. The interface is clean with a dark header and light body.

- Click on Public Scan

This screenshot shows the urlscan.io interface after a public scan was initiated. The search bar now contains 'https://tex-minerals-question-kuwait.trycloudflare.com'. The '▶ Public Scan' button is highlighted in green. The 'Recent scans' section has been updated to show results for the new URL. The table includes columns for Age, Size, IPs, and a flag icon. The results show a single entry with an age of 16 seconds, a size of 3 MB, and 3 IPs from China. The URL itself is flagged with a red warning icon. The rest of the page remains consistent with the first screenshot, featuring the same header, footer, and sidebar.

- Phishing Detected

(88) Lyrical: Kabhi Kabhi Aditi Zindgi

SRH vs DC Live video streaming

Instagram

tex-minerals-question-kuwait.t...

urscan.io/result/0196a0d8-8ab8-739b-931a-a9fa73e8e6db/

Home Search Live API Blog Docs Pricing Login

Sponsored by SecurityTrails A Recorded Future Company

tex-minerals-question-kuwait.trycloudflare.com

2606:4700::6810:e784 Malicious Activity! Public Scan

Submitted URL: <https://tex-minerals-question-kuwait.trycloudflare.com/>

Effective URL: <https://tex-minerals-question-kuwait.trycloudflare.com/login.html>

Submission: On May 05 via manual (May 5th 2025, 2:28:02 pm UTC) from IN - Scanned from AT

Summary HTTP Redirects Links Behaviour Indicators Similar DOM Content API Verdicts

Summary

This website 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 WE1 on April 22nd 2025. Valid for: 3 months.

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

urscan.io Verdict: Potentially Malicious !

Targeting these brands: Instagram (Social Network)

Live information

Google Safe Browsing: No classification for tex-minerals-question-kuwait.trycloudflare.com

Current DNS A record: 104.16.230.132 AS13335 - CLOUDFLARENET, US

Domain & IP information

IP/ASNs IP Detail Domains Domain Tree Links Certs Frames

Page Title

Instagram

Page URL History Show full URLs

1 <https://tex-minerals-question-kuwait.trycloudflare.com/>

89 33°C Mostly clear ENG IN 19:58:20 05-05-2025

2. Perform Phishing Detection Using UrlVoid Website

How to use it :-

- Open Browser And Search Phishing Url scan Click on Urlvoid Website

phising url scan - Brave Search

search.brave.com/search?q=phising+url+scan&source=web&summary=1&conversation=c13ed883fa0c07e08b3c6f

brave

phising url scan

Urvoid
urvoid.com

Check if a Website is Malicious/Scam or Safe/Legit |...
Identify websites involved in malware and phishing incidents.
URLVoid is used by cyber security companies and IT researchers to speed-up the process of cyber threat analysis, you can better...

Sucuri Security
sitecheck.sucuri.net

Website Security Checker | Malware Scan | Sucuri S...
Since the remote scanner only has ... and detect phishing pages, backdoors, mailers, DoS scripts or any other malware at the server level enable the Sucuri Platform....

Find elsewhere Google Bing Mojeek

Skysnag
skysnag.com > home > phishing check

Phishing Check Tool - Skysnag
September 2, 2024 - Protect your domain from phishing attacks with Skysnag's Phishing Check tool. Quickly identify potential phishing threats and safeguard your online presence.

31°C Partly cloudy

Search

ENG IN

20:09:11 05-05-2025

- Paste phishing website

The screenshot shows the URLVoid homepage with the title "Website Reputation Checker". Below it, a sub-section titled "Check the online reputation/safety of a website." includes a link to "Try the new URL Reputation API by APIVoid". A note says "Need to scan an IP address? Try IPVoid". There is a search bar with the placeholder "Enter website or URL here" and a green "Scan Website" button. Below the search bar is a small note: "Data submitted here is shared with security companies (terms of use)". At the bottom of the main content area are three boxes: "Multiple Blocklists" (with a checkmark), "Threat Analysis" (with a checkmark), and "Safety Report" (with a checkmark). The browser's status bar at the bottom shows the date as 05.05.2025.

- Click on Scan Website

This screenshot is identical to the one above, except the "Scan Website" button is now greyed out, indicating the process is ongoing or completed. The rest of the interface, including the search bar, the note about sharing data, and the three analysis boxes at the bottom, remains the same.

- Phishing Detected 🤡

The screenshot shows a web browser window for URLVOID. The address bar displays 'urvoid.com/scan/tex-minerals-question-kuwait.trycloudflare.com/'. The main interface has a dark header with tabs for WHOIS, DNS, PING, SCREENSHOT, PASSWORD, SORT, DNSSEC, and BASE64. Below the header is a search bar with placeholder text 'Enter website or URL here' and a yellow 'Scan Website' button. A banner at the bottom of the page reads 'SPONSORED: APIs for Threat Analysis & Detection - Prevent Malware & Ransomware - Harden Windows 11'. The central content area is titled 'Report Summary' and contains a table with the following data:

| Website Address | Tex-minerals-question-kuwait.trycloudflare.com |
|---------------------|---|
| Last Analysis | 8 seconds ago Rescan |
| Detections Counts | 1/39 |
| Domain Registration | 2018-07-07 7 years ago |
| Domain Information | WHOIS Lookup DNS Records Ping |
| IP Address | 104.15.230.132 Find Websites IPVoid Whois |
| Reverse DNS | Unknown |

At the bottom of the browser window, there is a toolbar with various icons and a status bar showing 'https://www.urvoid.com/dns-records-lookup/' and weather information '31°C Partly cloudy'.

3. Perform Phishing Detection Using Checkphish Website

How to use it :-

- Open Browser and search Phishing detection
- Click on checkphish website

The screenshot shows a Brave browser search results page for 'phishing detection'. The search bar at the top contains 'search.brave.com/search?q=phishing+detection&source=desktop'. The results include a link to 'CheckPhish AI' from 'checkphish.bolster.ai', which is described as a 'Free Phishing Link Checker & Site URL Scanning | CheckPhish'. Below this, there are sections for 'URL Scanner & Sandbox' and 'APIs'. Further down, there is a link to 'Check Point Software' and a section for 'Discussions' with a post about Metamask showing Ethereum Phishing Detection on iSwap.org. The browser's toolbar and status bar are visible at the bottom.

- Paste Phishing Url

The screenshot shows the homepage of the CheckPhish website. At the top, there is a navigation bar with links for Products, Solutions, Blog, Glossary, Community, Upgrade to Bolster, Login, and Start Free. Below the navigation bar, the title "CheckPhish Detects and Monitors Phishing and Scam Sites" is displayed. A sub-header below it states, "With CheckPhish, you can scan suspicious URLs and monitor for typosquats and lookalikes variants of a domain." There are four main tabs: Email Scanner (New!), URL Scanner (selected), Typosquat Monitoring, and Takedown. A search bar labeled "Scan a URL" contains the placeholder "https://variety-survivors-plots-trailer.cloudflare.com/login.htm". A blue "Scan" button is to the right of the search bar. Below the search bar, a descriptive text block explains the service's capabilities. At the bottom of the page, there is a footer with weather information (23°C, Partly cloudy), system icons, and a timestamp (01:24:04 08-05-2025).

- Click on Scan

This screenshot is identical to the one above, showing the CheckPhish homepage with the URL "https://variety-survivors-plots-trailer.cloudflare.com/login.htm" entered into the "Scan a URL" field. The "Scan" button is visible to the right of the search bar.

- Phishing Detected 🤞

Suspicious

DOM TREE TIMELINE VIEW WHOIS INFORMATION

Scan Results

Source URL: https://variety-survivors-plots-tr... Brand: Cloudflare

Redirected URL: https://variety-survivors-plots-trailer.trycloudflare.com TLD: com

IP Address: 104.16.230.132 Location: United States of America

Insight Page of Social Media Finding: -- Hosting Provider: Cloudflare, Inc.

Detection Date: May 8th 2025, 1:23:08 am ASN: 13335

Job ID: --

Certificate Details: Google Trust Services: trycloudflare.com, *trycloudflare.com

Screenshot

Logos Detected: 0

One account. All of Google.

Sign in to continue to Gmail

Google

Sign in or Create Account

Log In Sign Up

Geo Location

23°C Partly cloudy

Search

Cloudflare, Inc.

01:23:33 08-05-2025

THANK YOU