

SOCIAL ENGINEERING

TABLE OF CONTENTS

1) Social Engineering

- 1.1 Introduction to Social Engineering
- 1.2 Human-Based Social Engineering Attack
- 1.3 Computer-Based Social Engineering Attack
- 1.4 Mobile-Based Social Engineering Attack
- 1.5 Impact of Social Engineering
- 1.6 Common Types of Social Engineering
- 1.7 Prevention and Protection Techniques

2) Phishing

- 2.1 Introduction to Phishing
- 2.2 Types of Phishing Attacks
- 2.3 Perform Phishing Attack Using Social Engineering Toolkit
- 2.4 Perform Phishing Attack Using Gmail Account
- 2.5 Perform Phishing Attack Using ShellPhish Tool
- 2.6 Perform Phishing Attack Using CamPhish Tool
- 2.7 Perform Phishing Attack Using r3bu5 Tool
- 2.8 Phishing Detection Using CheckPhish Website

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.

Impact of Social Engineering

- Data breaches
- Financial loss
- Identity theft
- Malware and ransomware infections
- Reputation damage

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.

Prevention & Protection

- Security awareness training
- Verify emails, links, and callers
- Do not share OTPs or passwords
- Use multi-factor authentication (MFA)
- Report suspicious activity
- Strong email filtering

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.

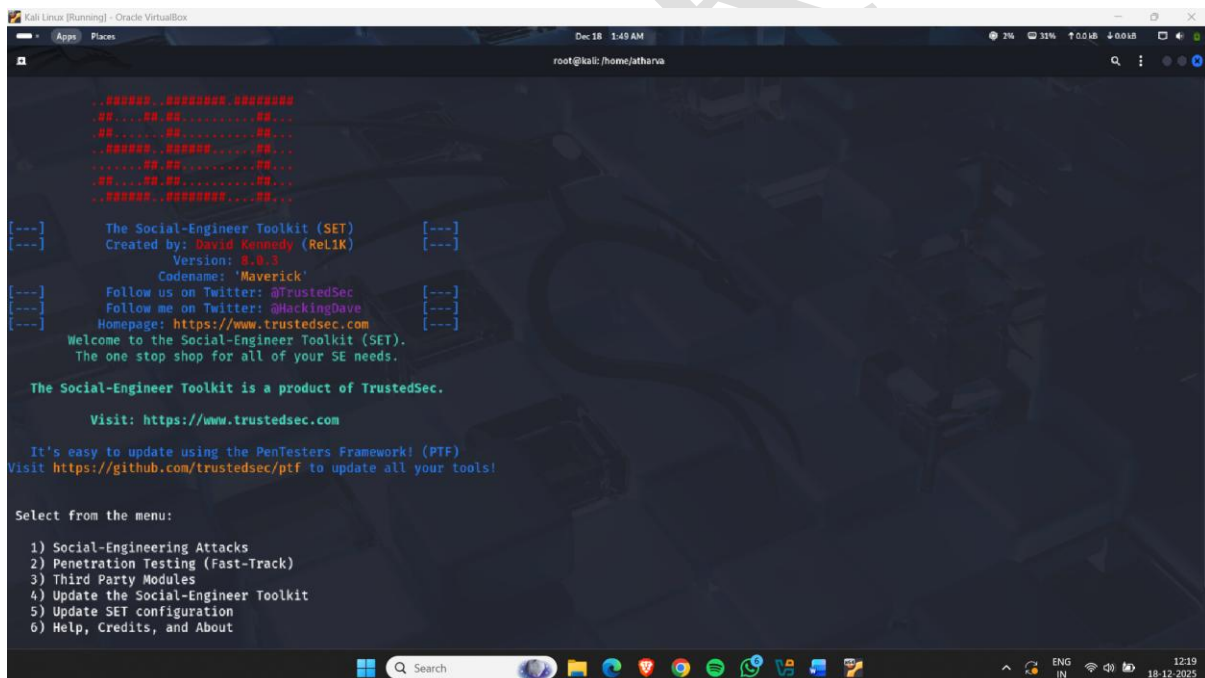
Perform Phishing Attack Using SETOOLKIT

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.

1) Website attack vector

How to use it -:

- Open kali linux terminal and type setoolkit
- Now select 1 – Social Engineering Attack



```
root@kali: /home/atharia

..#####..#####..#####..
..#####..#####..#####..
..#####..#####..#####..
..#####..#####..#####..
..#####..#####..#####..
..#####..#####..#####..
..#####..#####..#####..
..#####..#####..#####..
..#####..#####..#####..
..#####..#####..#####..

[---] The Social-Engineer Toolkit (SET) [---]
[---] Created by: David Kennedy (Rel1K) [---]
[---] Version: 8.0.3 [---]
[---] Codename: 'Maverick' [---]
[---] Follow us on Twitter: @TrustedSec [---]
[---] Follow me on Twitter: @HackingDave [---]
[---] Homepage: https://www.trustedsec.com [---]
Welcome to the Social-Engineer Toolkit (SET).
The one stop shop for all of your SE needs.

The Social-Engineer Toolkit is a product of TrustedSec.

Visit: https://www.trustedsec.com

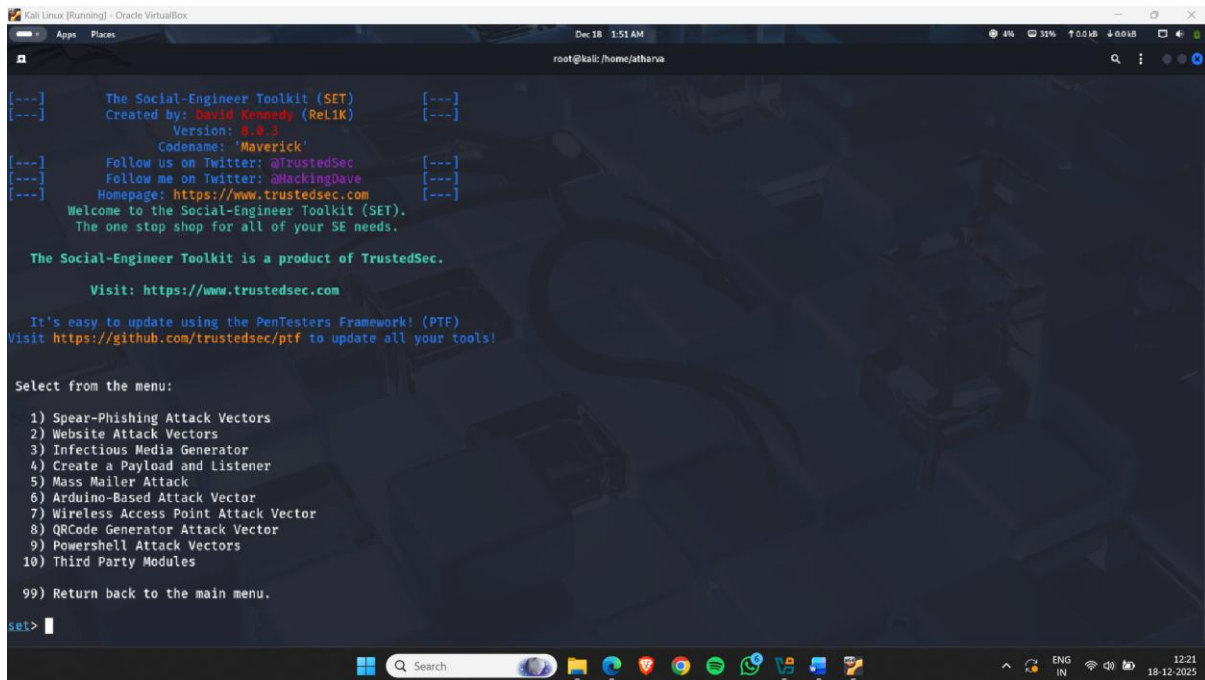
It's easy to update using the PenTesters Framework! (PTF)
Visit https://github.com/trustedsec/ptf to update all your tools!

Select from the menu:

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

Figure 1

- Now select 2 – Website attack Vector



```

[---] 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

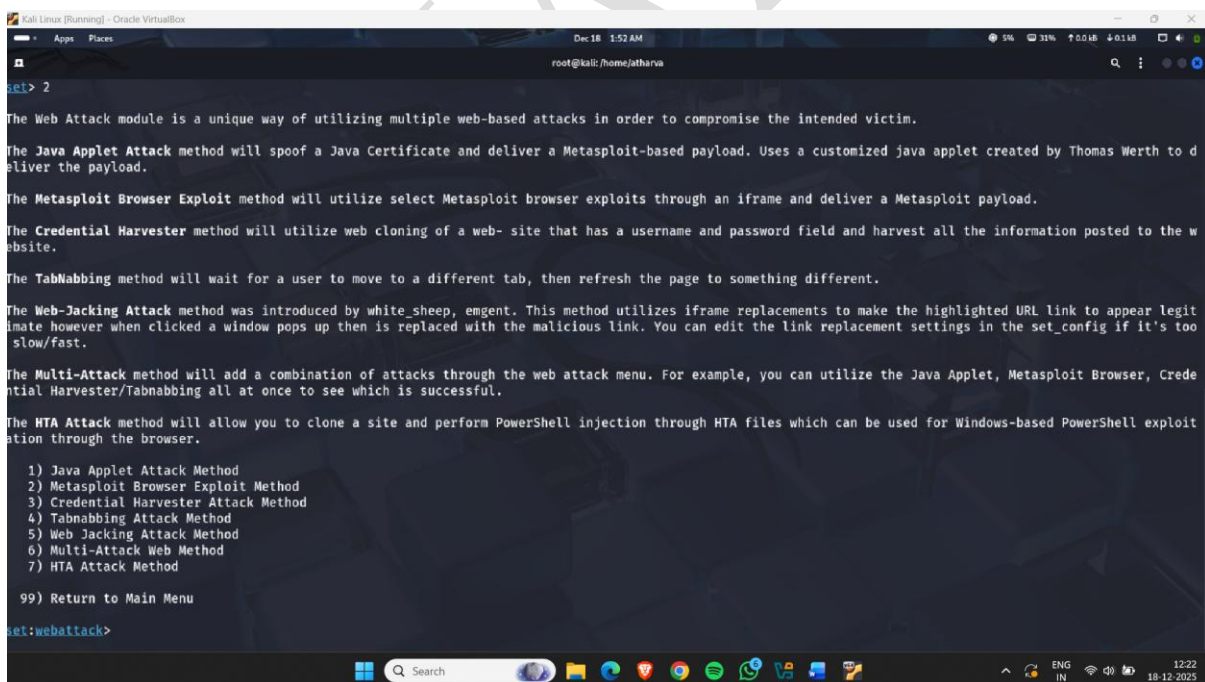
99) Return back to the main menu.

set>

```

Figure 2

- Now select 3 – Credential Harvesting Attack Method



```

set> 2

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 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

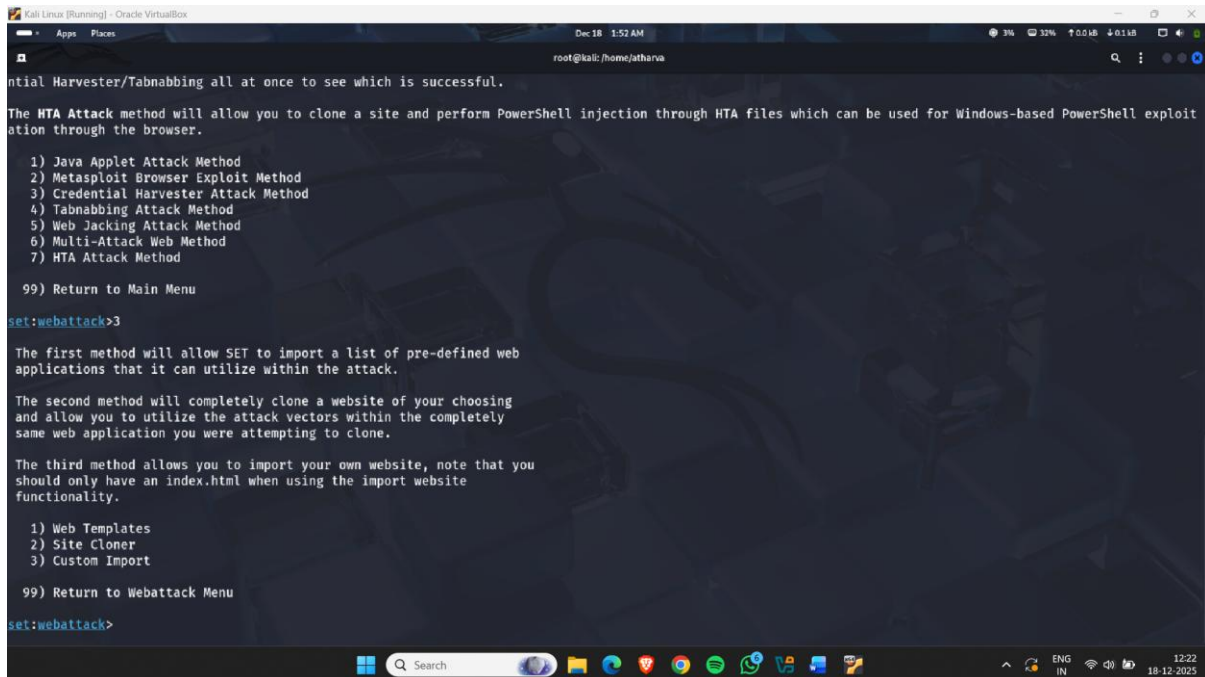
99) Return to Main Menu

set:webattack>

```

Figure 3

- Select 1 – Web Template



```
Kali Linux [Running] - Oracle VM VirtualBox
Dec 18 1:52 AM
root@kali: /home/atharva

ntial 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

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.

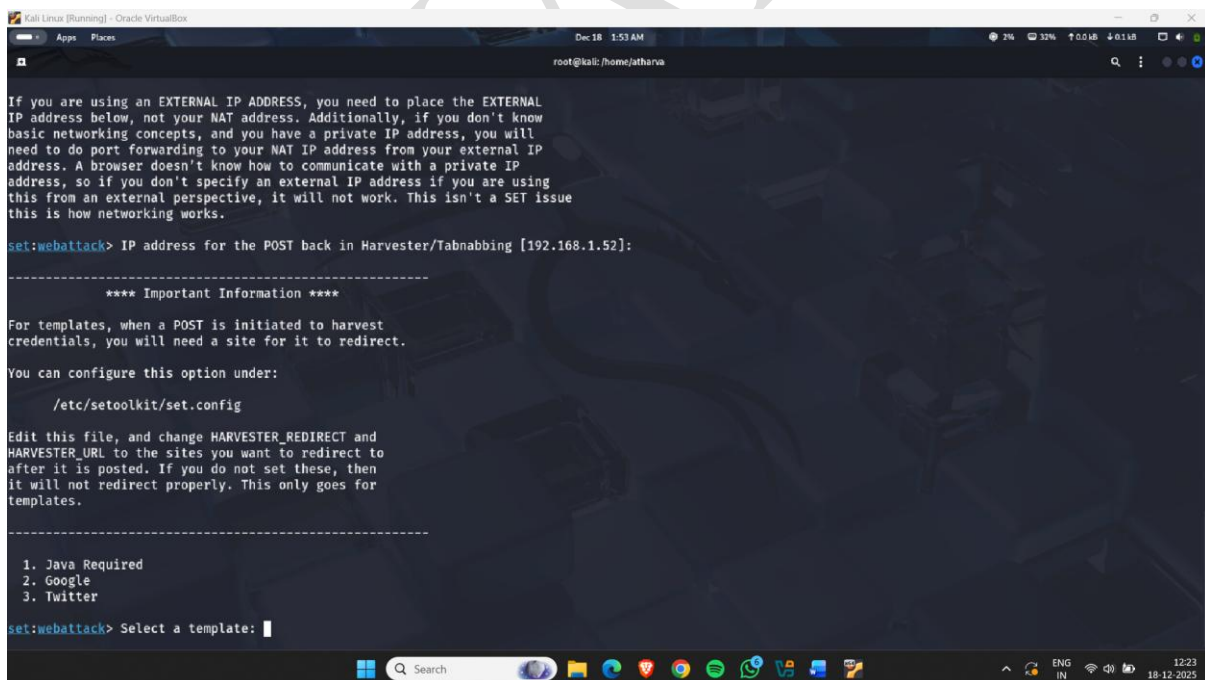
1) Web Templates
2) Site Cloner
3) Custom Import

99) Return to Webattack Menu

set:webattack>
```

Figure 4

- Select 2 - Google



```
Kali Linux [Running] - Oracle VM VirtualBox
Dec 18 1:53 AM
root@kali: /home/atharva

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 [192.168.1.52]:

-----
**** 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: |
```

Figure 5

- Now provide a ip address that you want to get response back
Note -: By default it select kali linux ip address.

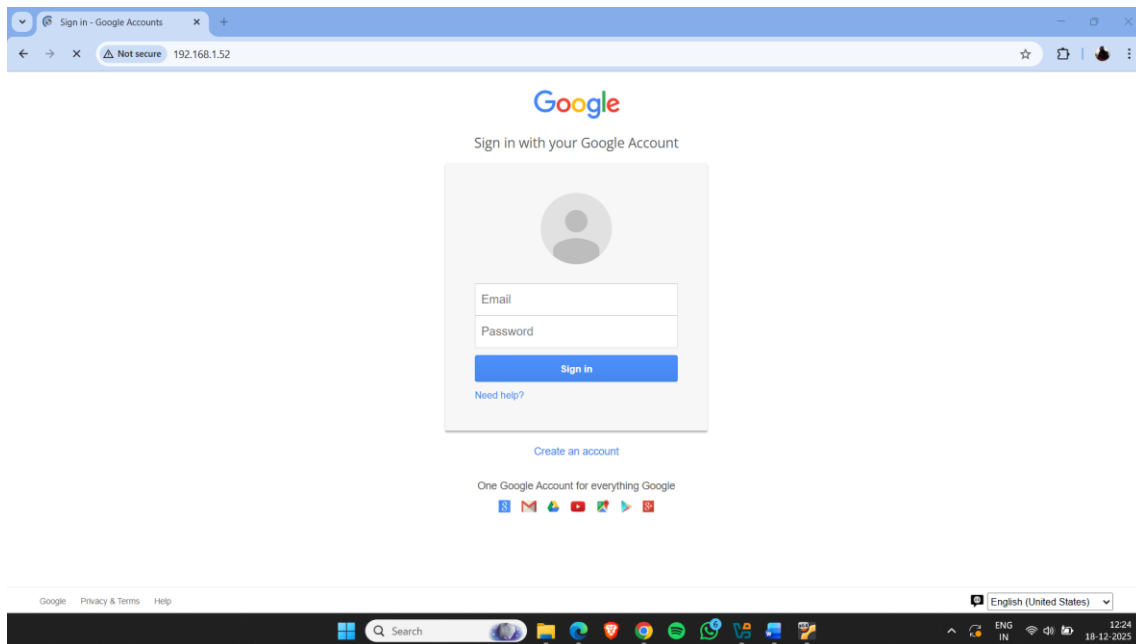


Figure 6

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

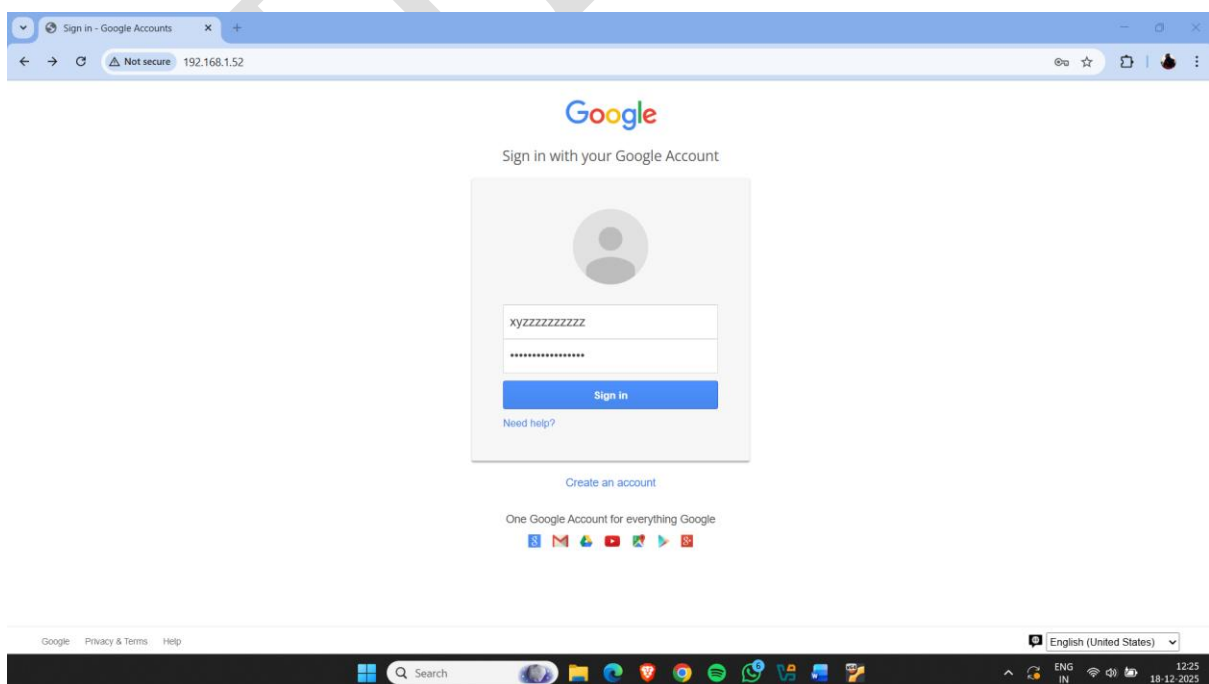


Figure 7

- Now go to the kali linux terminal & you'll get the credentials.

```

root@kali: /home/atharva
1. Java Required
2. Google
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:
192.168.1.63 - - [18/Dec/2025 01:54:26] "GET / HTTP/1.1" 200 -
192.168.1.63 - - [18/Dec/2025 01:54:35] "GET /favicon.ico HTTP/1.1" 404 -
[*] WE GOT A HIT! Printing the output:
PARAM: GALX=SJLckfgaqoM
PARAM: continue=https://accounts.google.com/o/oauth2/auth?z=CtRwSFBwd2JmV1hIcDhtUfdldzBENhIfVwsxStdNLW9MdhThbW1TMFQzVUZFc1BBaURuWmLR5QkE2%88%99APsBz4gAAAAAUy
4_qD7Hbfz3Bw8kxnaNouLcRiD3YTjX
PARAM: service=lso
PARAM: dsh=-7381887106725792428
PARAM: _utf8=a
PARAM: bgresponse=js_disabled
PARAM: pstMsg=1
PARAM: dnConn=
PARAM: checkConnection=
PARAM: checkedDomains=youtube
POSSIBLE USERNAME FIELD FOUND: Email=xyzxxxxxxxxx
POSSIBLE PASSWORD FIELD FOUND: Passwd=abcccccccccccccc
PARAM: signIn=Sign+in
PARAM: PersistentCookie=yes
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.

```

Figure 8

- Here we got the credentials of google template.

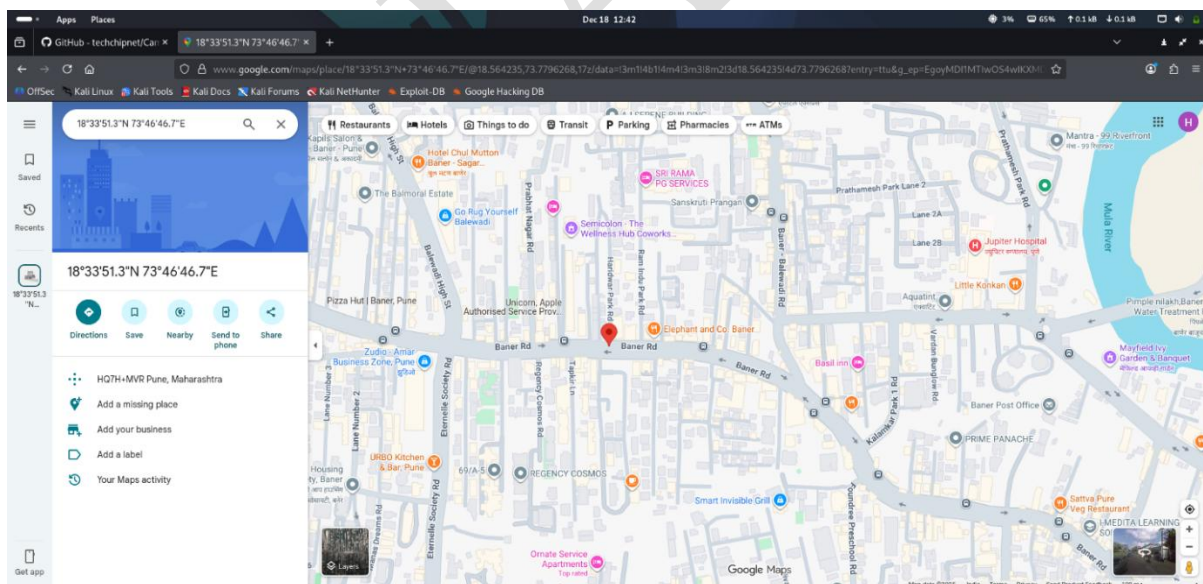


Figure 9

2) QRCode Generator

Select 8 – QRCode generator Attack Vector

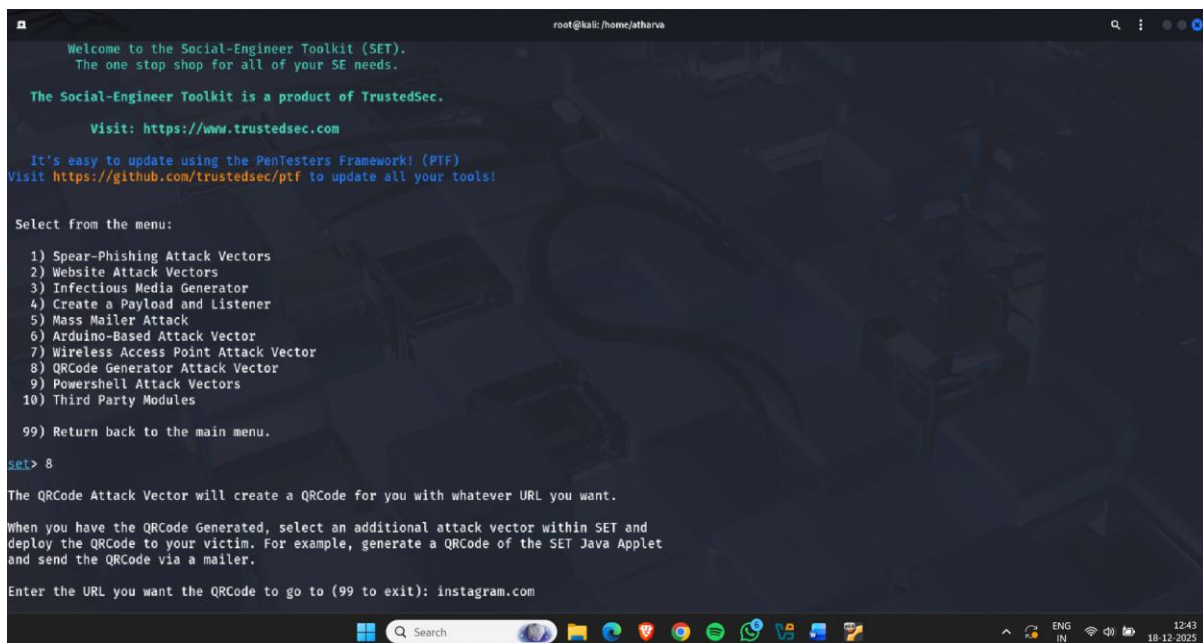


Figure 10

- Enter the URL you want
- You'll get a path of the qr code



Figure 11

- Now open a new terminal and paste the path, you'll get QR

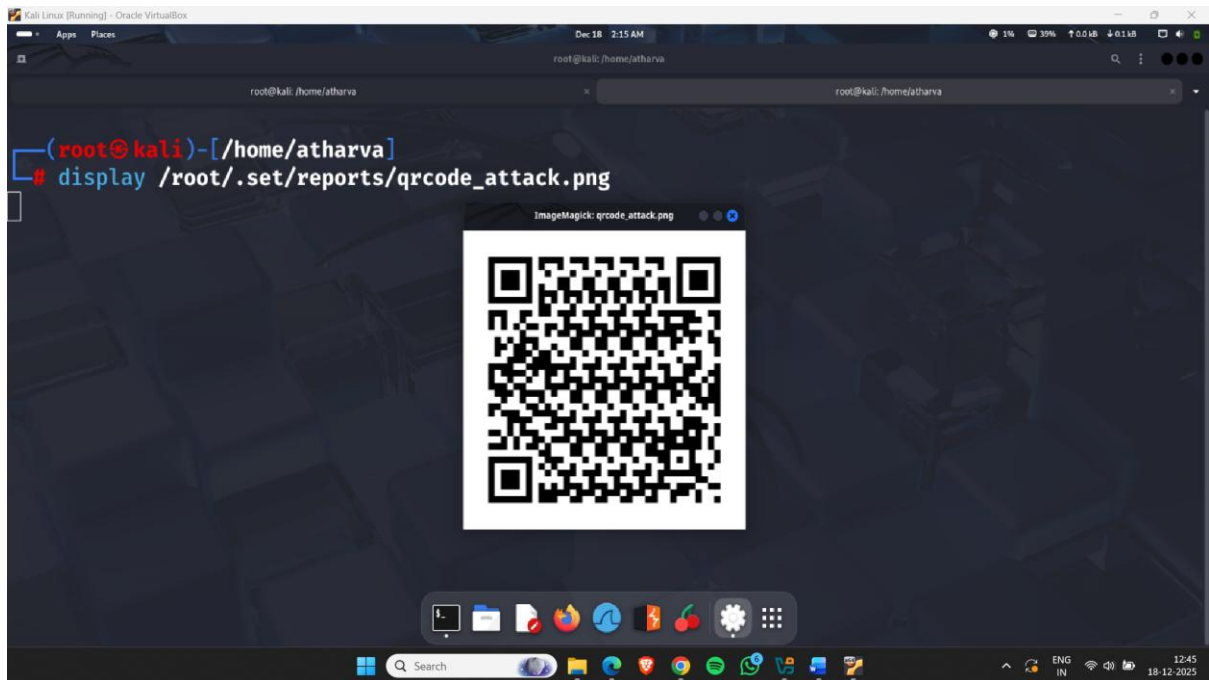


Figure 12

- Scan the QR Code it will open the link.

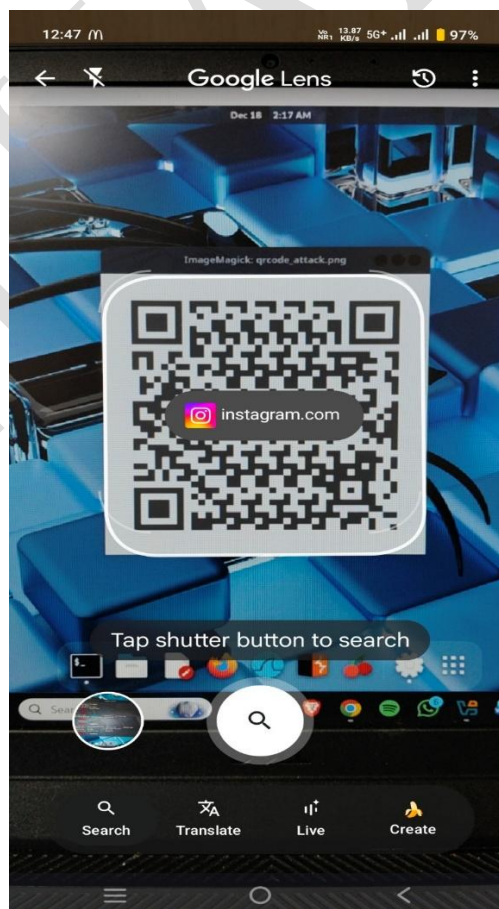


Figure 13

Perform Phishing Attack Using Gmail Account

How to use it -:

- Firstly create a phishing link using kali linux (eg:setoolkit)
- Then open Your gmail account
Note: Create a fake mail id for security purpose.
- Now open the gmail account and click on compose and create a hyperlink

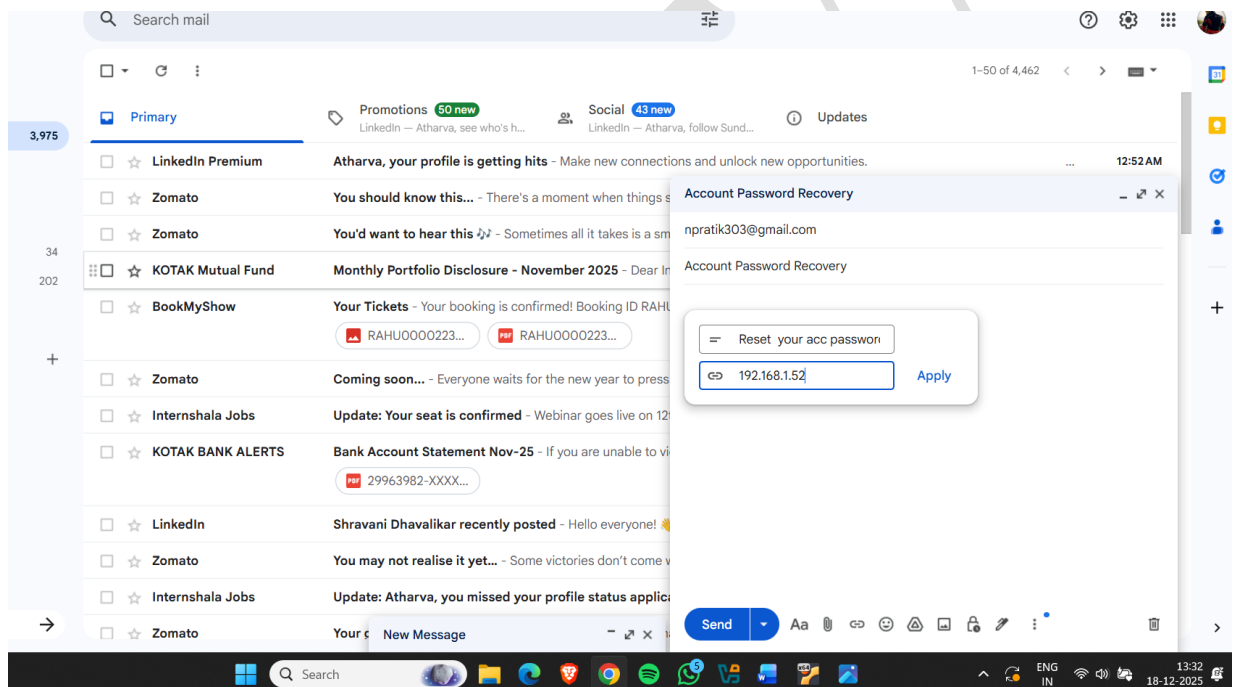


Figure 14

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

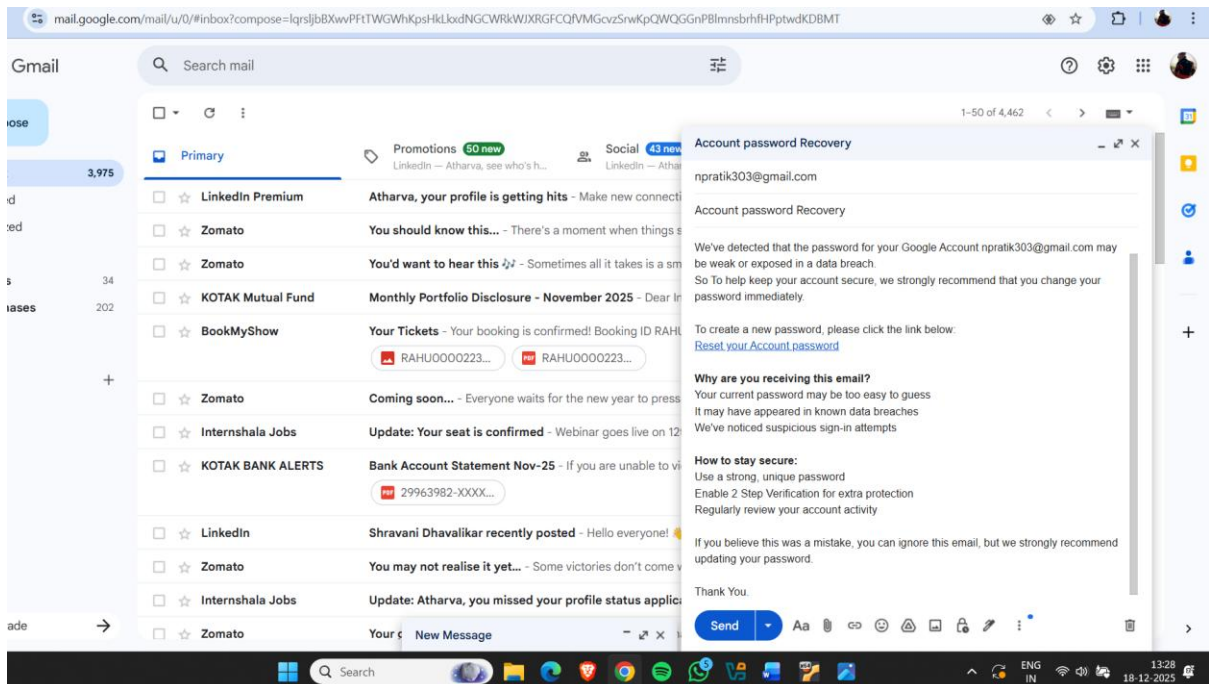


Figure 15

- When the target will open the link an fake gmail login page will open.
- If, the target will try to login with the credentials you'll get it.

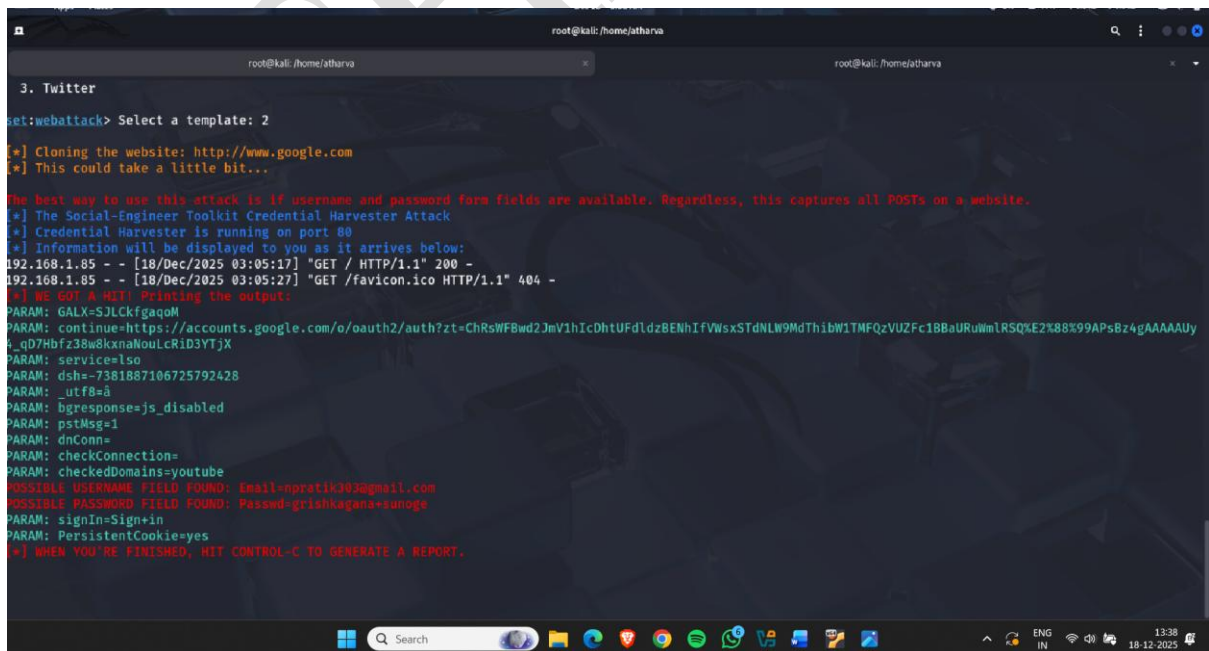


Figure 16

- Here, you have got the login credentials of the target.

Perform Phishing Attack Using ShellPhish

- Open kali linux terminal and go in shellphish directory
- Now select 1 – Facebook

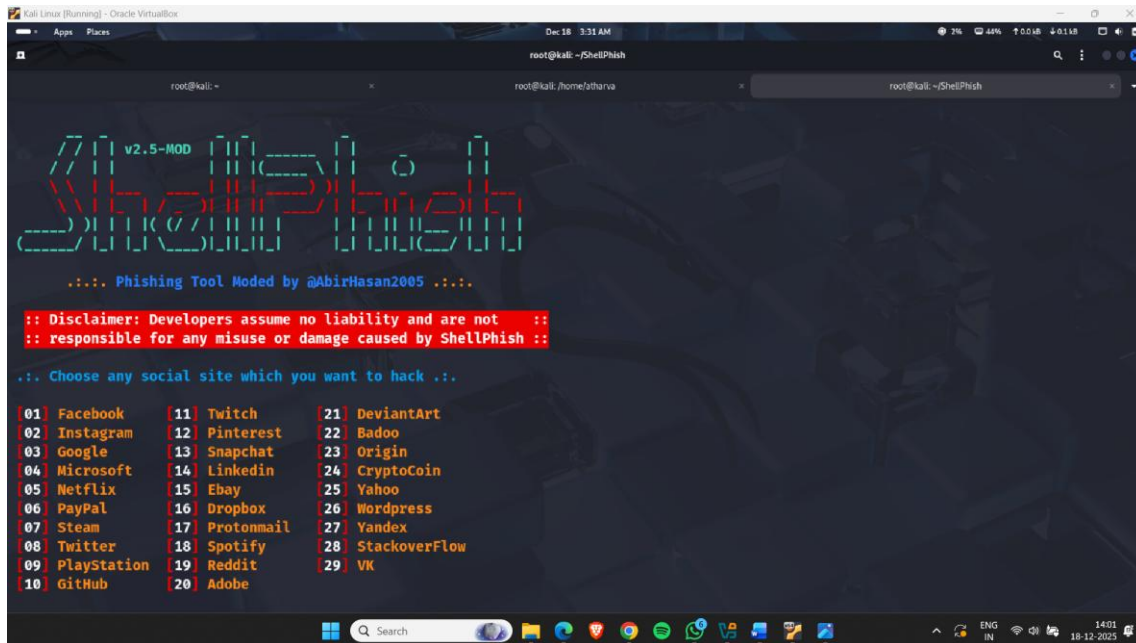


Figure 17

- Now select 1 – Localhost

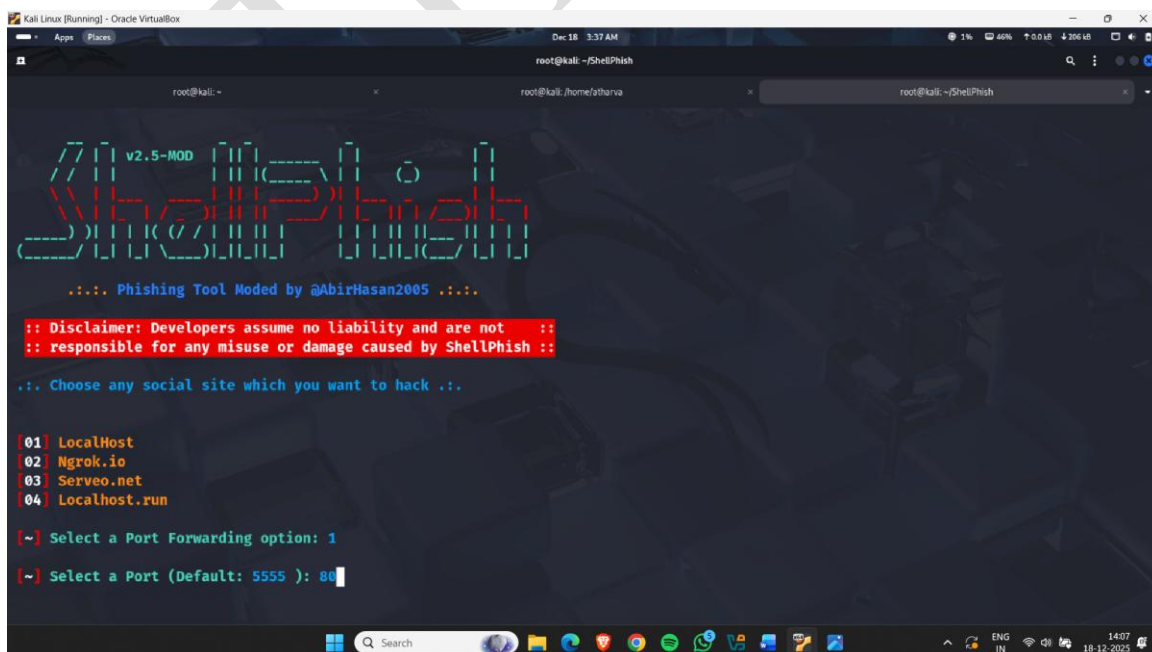
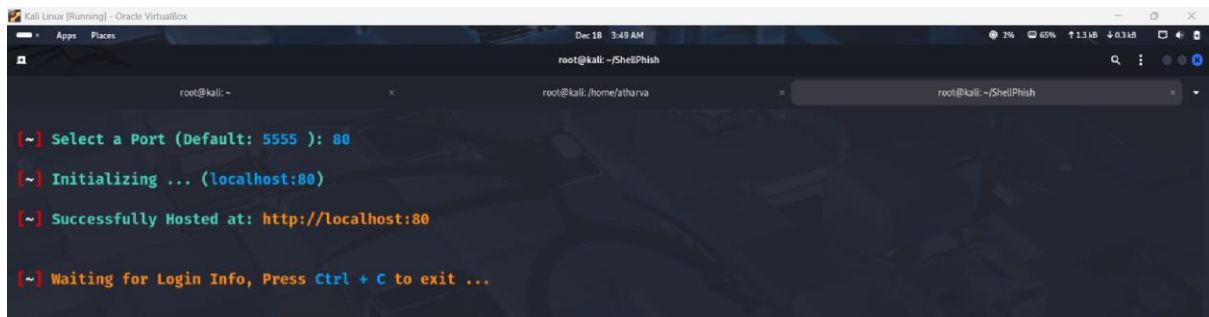


Figure 18

- Link will be generated



```

root@kali: ~
[~] Select a Port (Default: 5555 ): 80
[~] Initializing ... (localhost:80)
[~] Successfully Hosted at: http://localhost:80
[~] Waiting for Login Info, Press Ctrl + C to exit ...
  
```

Figure 19

- Copy the link generated and open it on target machine & type credentials & press on login.

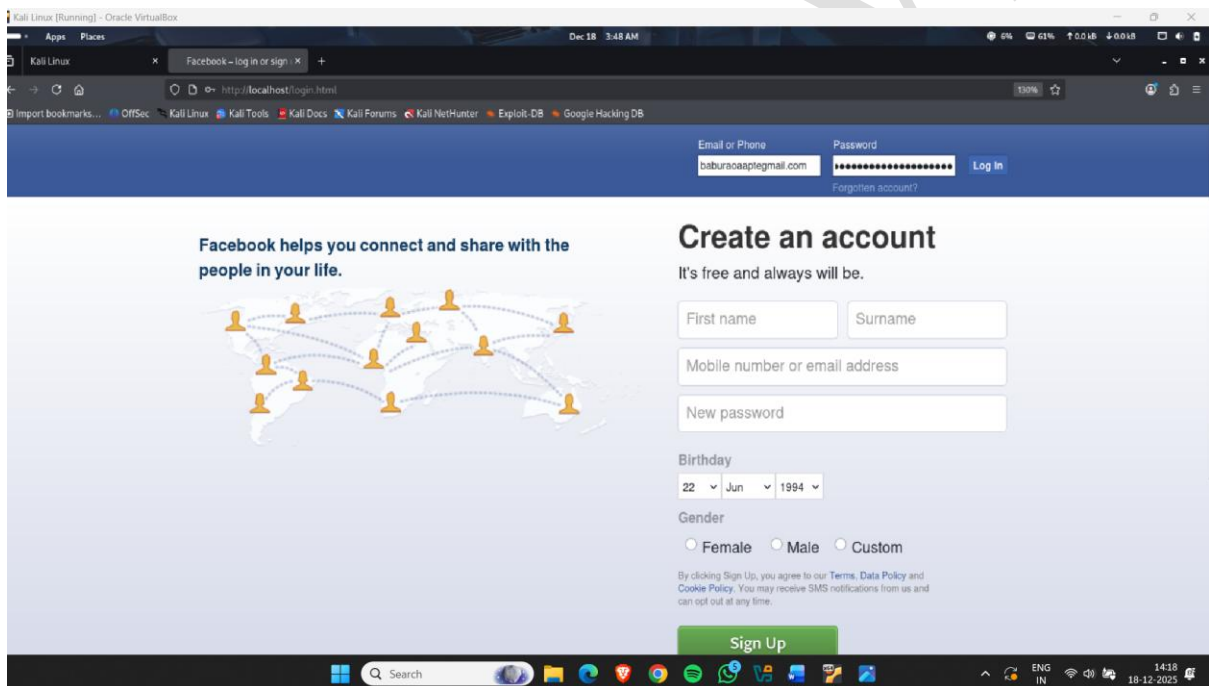
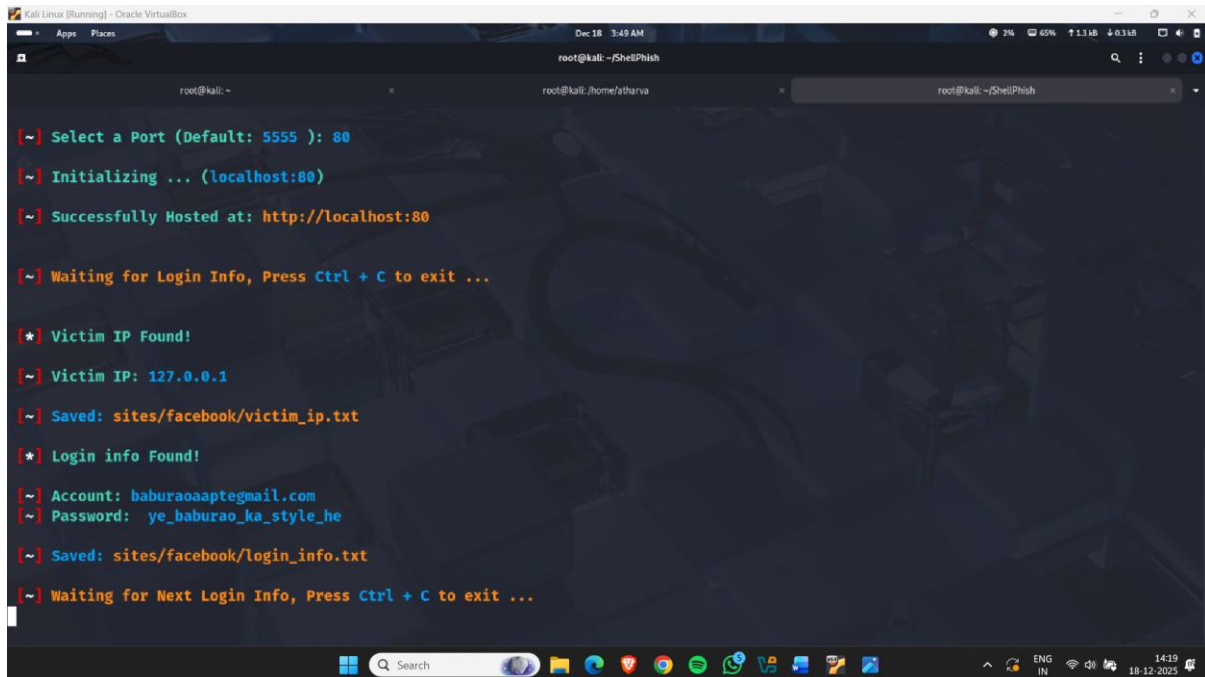


Figure 20

- You'll get target's credentials



```
[~] Select a Port (Default: 5555 ): 80
[~] Initializing ... (localhost:80)
[~] Successfully Hosted at: http://localhost:80
[~] Waiting for Login Info, Press Ctrl + C to exit ...
[*] Victim IP Found!
[~] Victim IP: 127.0.0.1
[~] Saved: sites/facebook/victim_ip.txt
[*] Login info Found!
[~] Account: baburaoaaptegmail.com
[~] Password: ye_baburao_ka_style_he
[~] Saved: sites/facebook/login_info.txt
[~] Waiting for Next Login Info, Press Ctrl + C to exit ...
```

Figure 21

Perform Phishing Attack Using CamPhish

- Open kali linux terminal go to the camphish directory & type command –bash camphish.

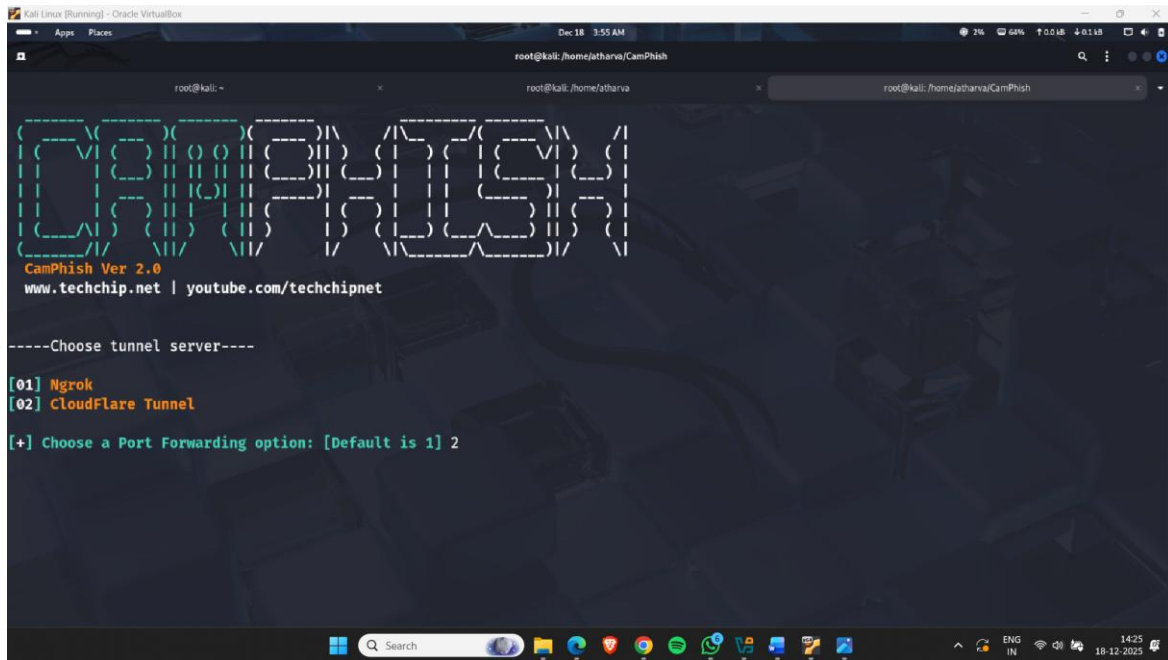


Figure 22

- Select Server – cloudflare tunnel

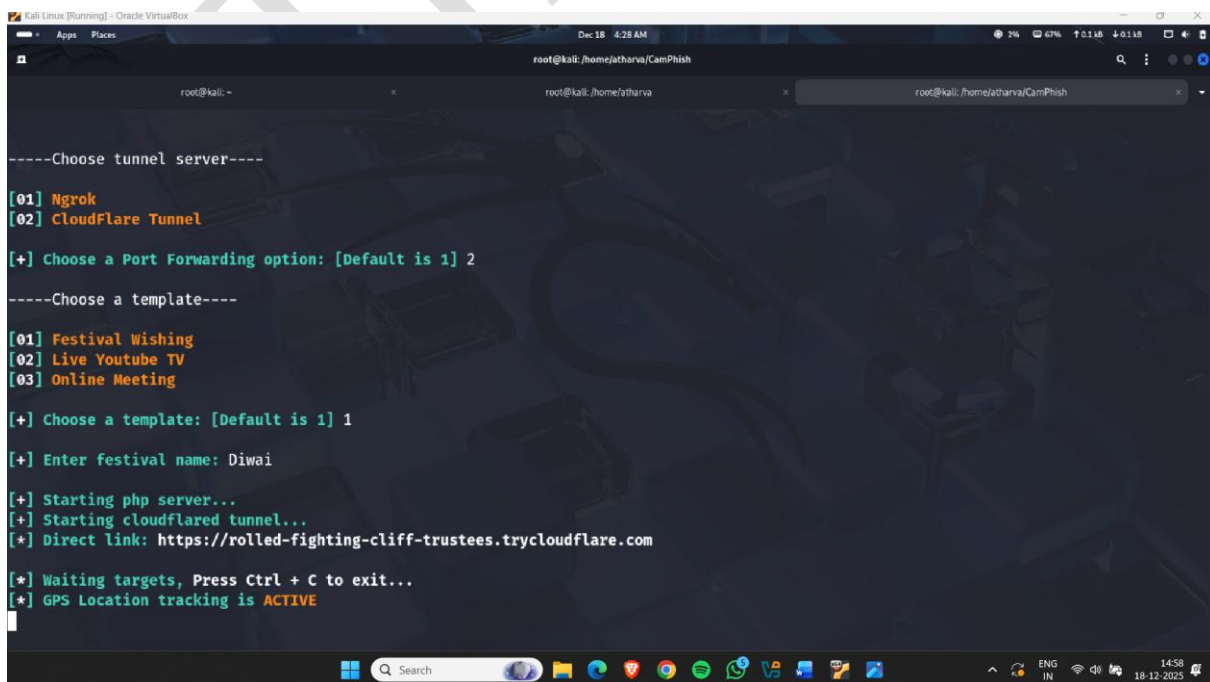


Figure 23

- Select 1- Festival wishing & type festivals name
- a link will be generated, copy the link & send it to victim.

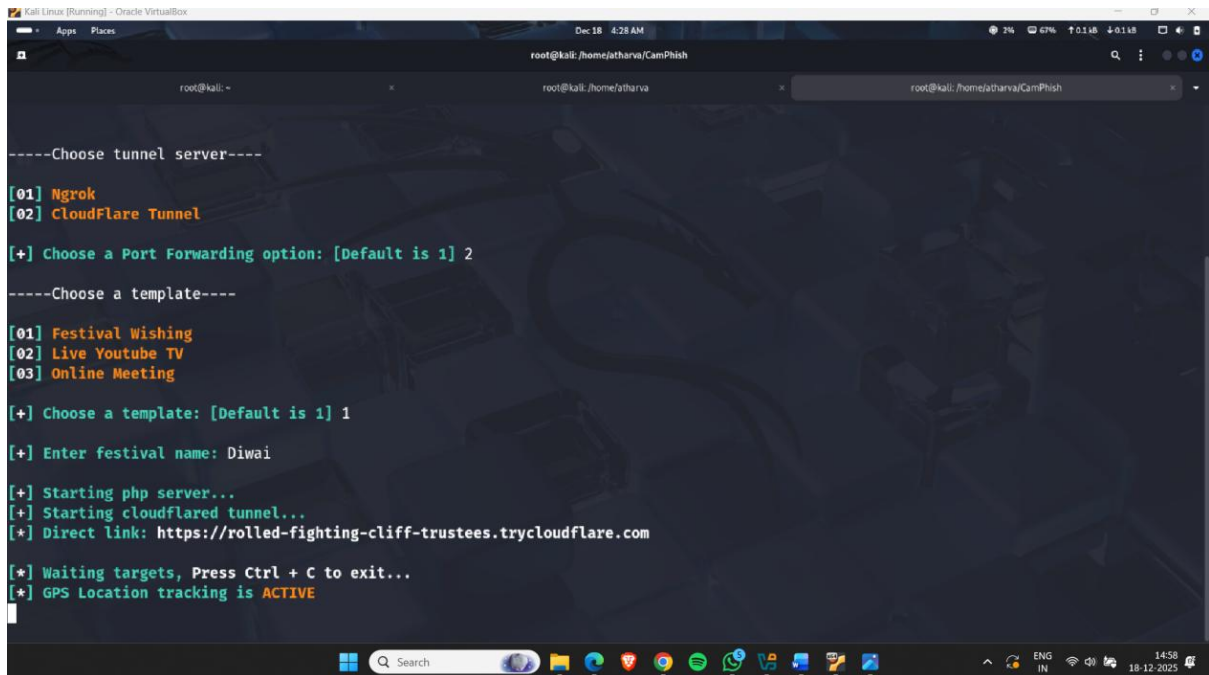


Figure 24

- Here It capture the photos and Location of the victim.



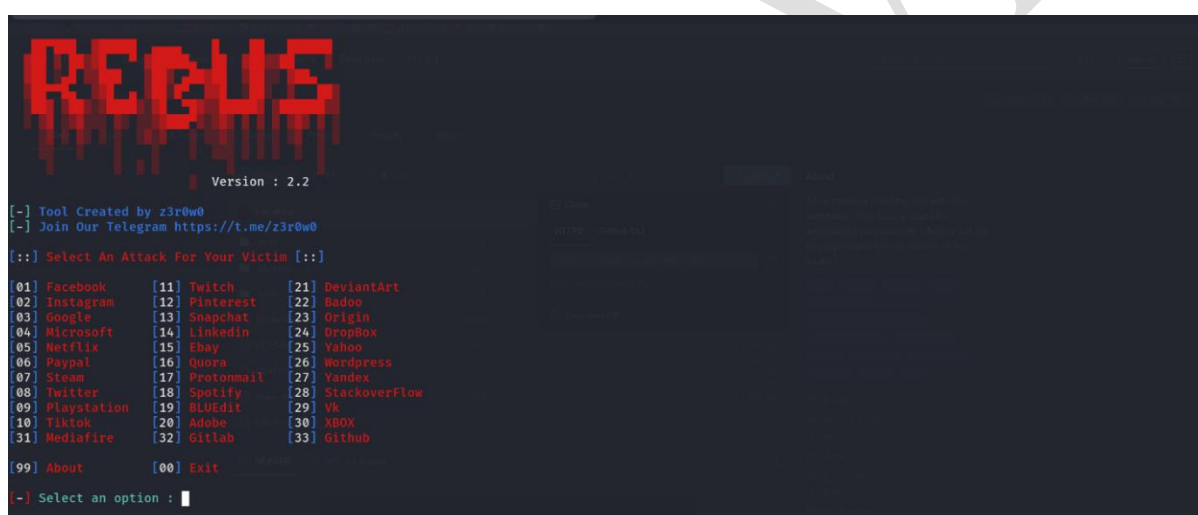
Figure 25

Perform Phishing Attack Using r3bu5 Tool

r3bu5 is a social-engineering based phishing tool used to demonstrate how attackers can trick users into revealing login credentials, emphasizing the importance of cyber security awareness and safe browsing practices.

How to use it -:

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



```

  R3BU5
  Version : 2.2

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

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

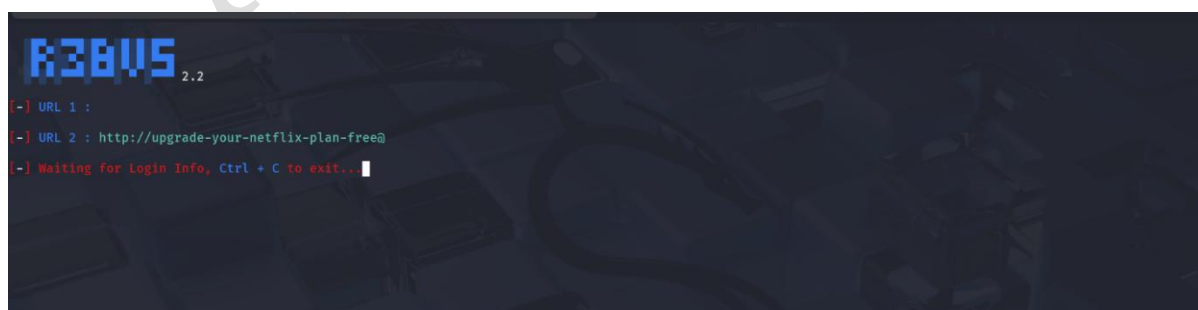
01] Facebook      [11] Twitch          [21] DeviantArt
02] Instagram     [12] Pinterest       [22] Badoo
03] Google        [13] Snapchat        [23] Origin
04] Microsoft     [14] LinkedIn        [24] DropBox
05] Netflix       [15] Ebay            [25] Yahoo
06] Paypal        [16] Quora           [26] 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] Gitlab          [33] Github

99] About        [00] Exit

[-] Select an option : 
```

Figure 26

- Now ,select any option and create phishing site of given listed platforms.
- Now select the option for what kind of login page you want.



```

  R3BU5 2.2

[-] URL 1 :
[-] URL 2 : http://upgrade-your-netflix-plan-free@
[-] Waiting for login Info, Ctrl + C to exit... 
```

Figure 27

- Now copy url and paste it on target's browser.

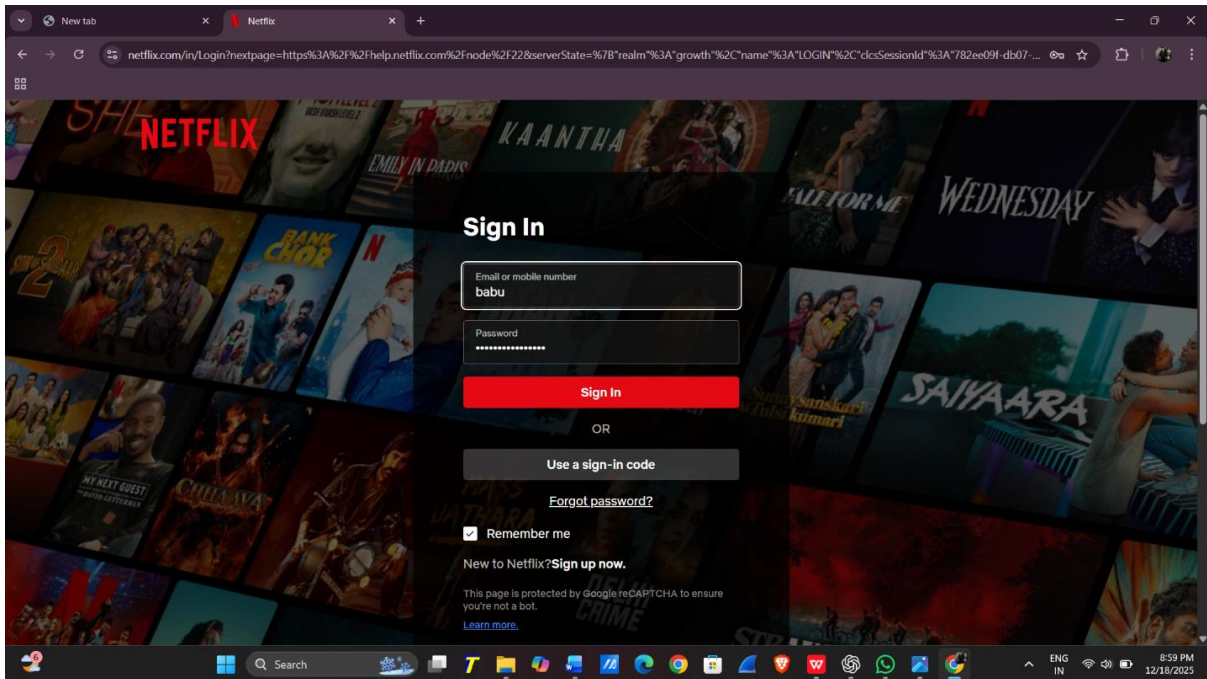


Figure 28

- Open kali ,Here we got username and passwords of phishing site
- We created Netflix clone site and here we have captured username & password.

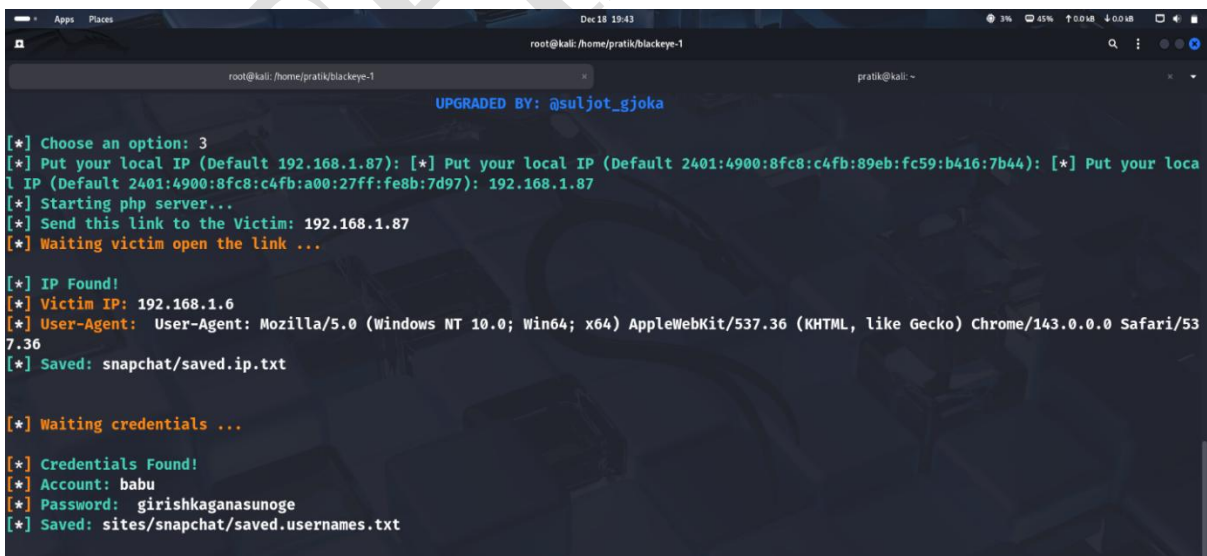


Figure 29

Perform Phishing Detection Using Checkphish Website

CheckPhish is an AI-powered anti-phishing platform that analyzes URLs, domains, and webpages to detect:

- Phishing attacks
- Brand impersonation
- Fake login pages
- Scam and fraudulent websites

It is widely used by SOC teams, security analysts, and ethical hackers

How to use it -:

- Open Browser and search Phishing detection
- Click on checkphish website
- Paste Phishing Url
- Click on scan

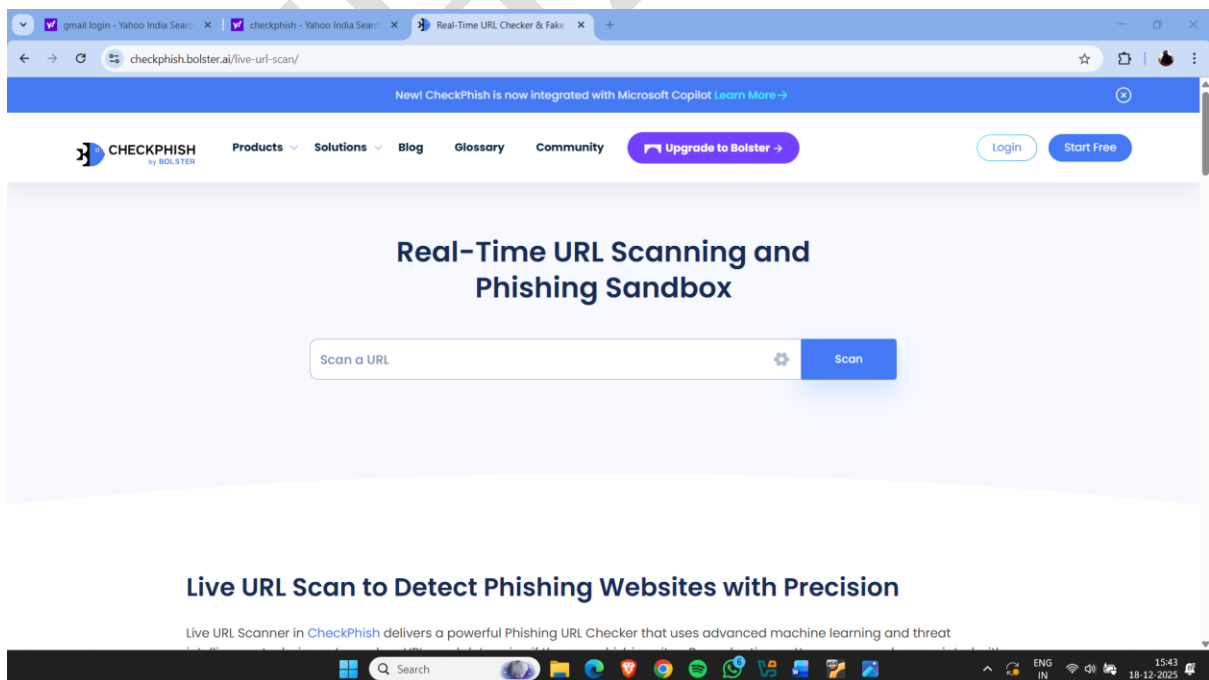


Figure 30

- Phishing Detected

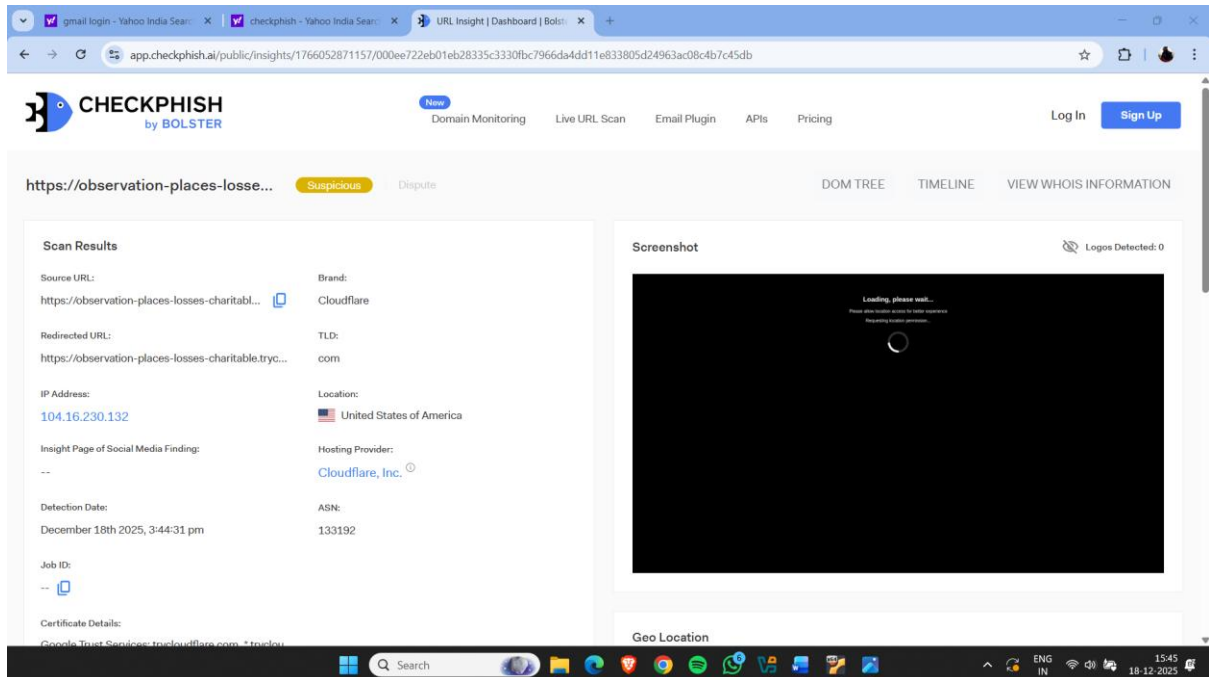


Figure 31