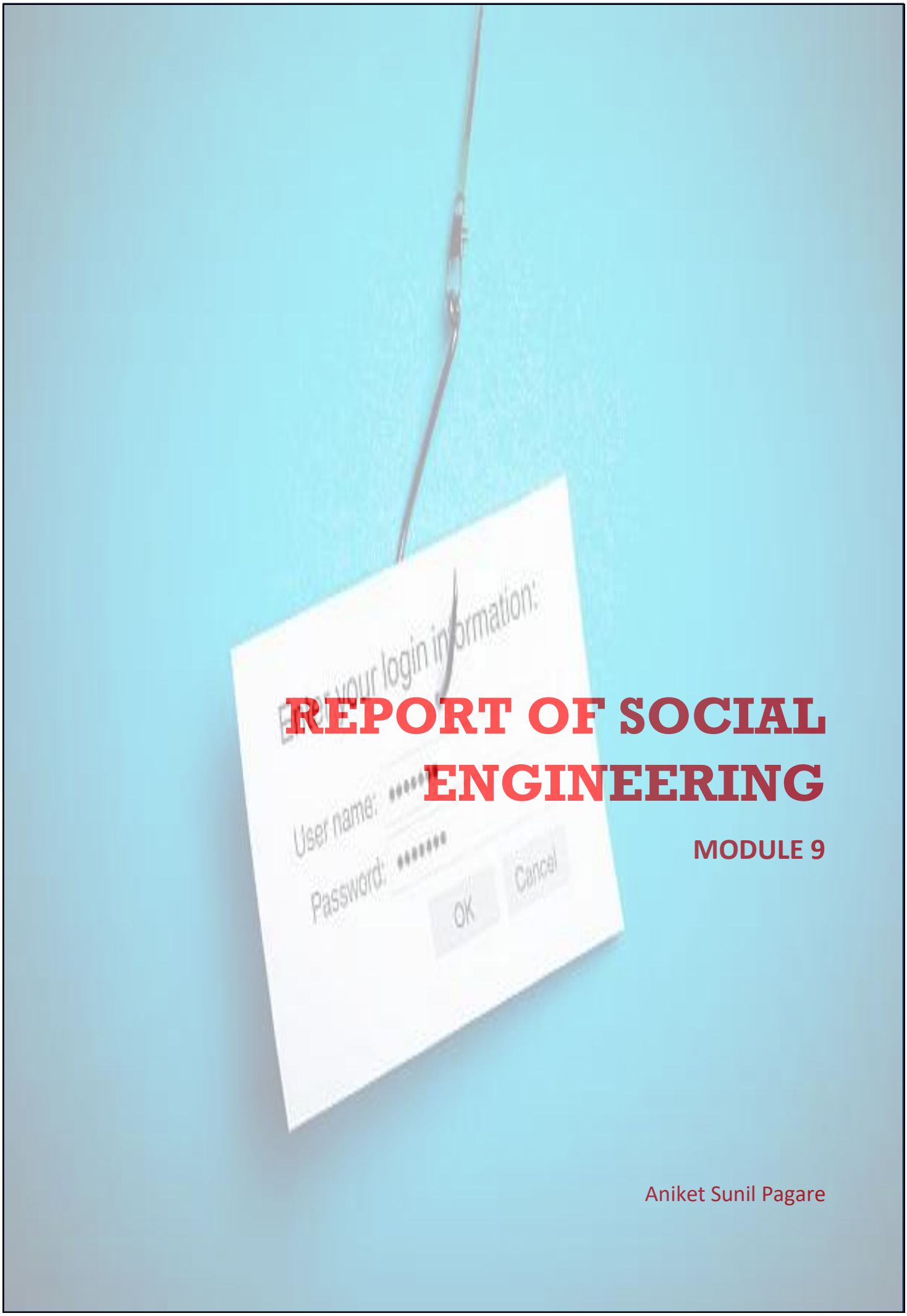


REPORT OF SOCIAL ENGINEERING

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

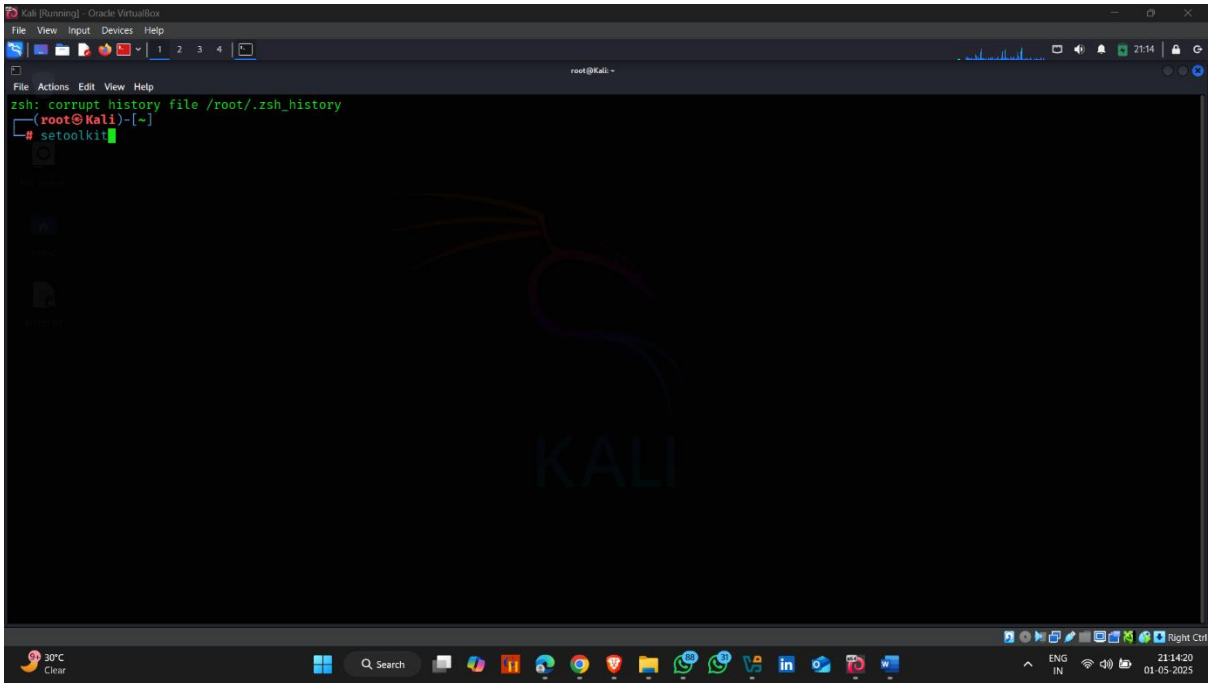
- **Description**: A legitimate email is cloned, and the attachment or link is replaced with a malicious one.
- **Goal**: Trick recipients who have already seen or trusted the original email.

1.Perform Phishing Attack Using SETOOLKIT

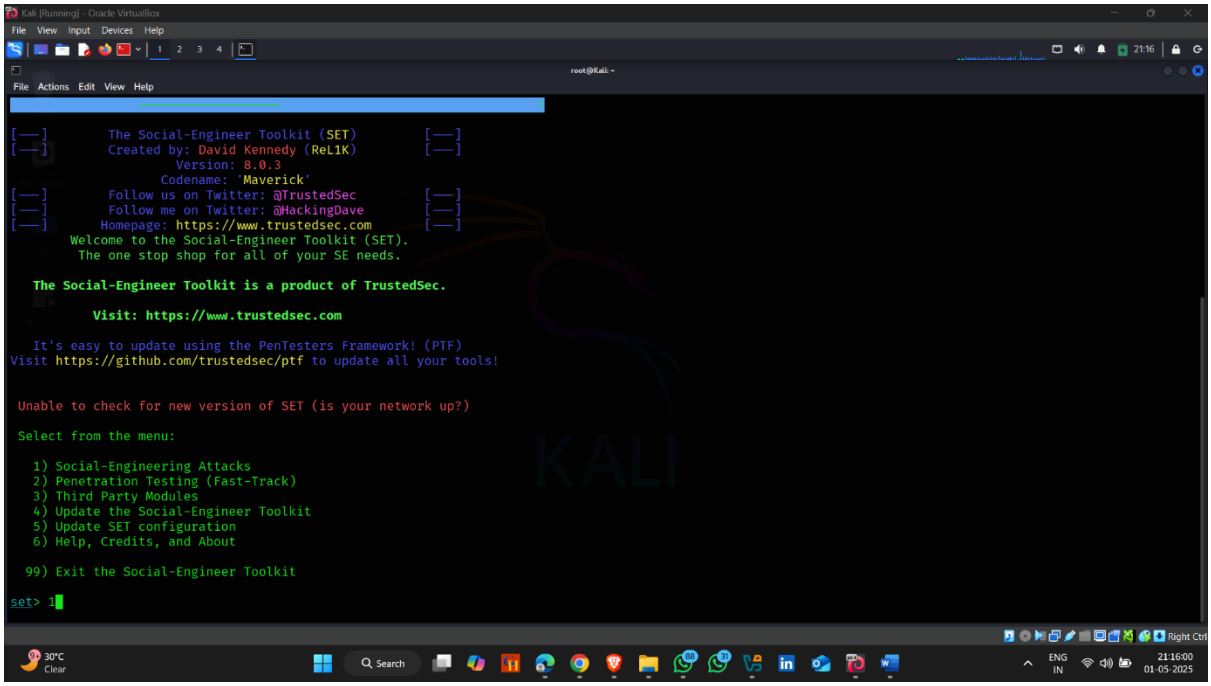
In **Kali Linux**, the **Social-Engineer Toolkit (SET)** is one of the most powerful tools for **phishing attacks**, specifically designed to simulate **real-world social engineering scenarios**. For phishing, SET helps you create **fake websites or emails** to trick users into entering their login credentials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

How to use it -:

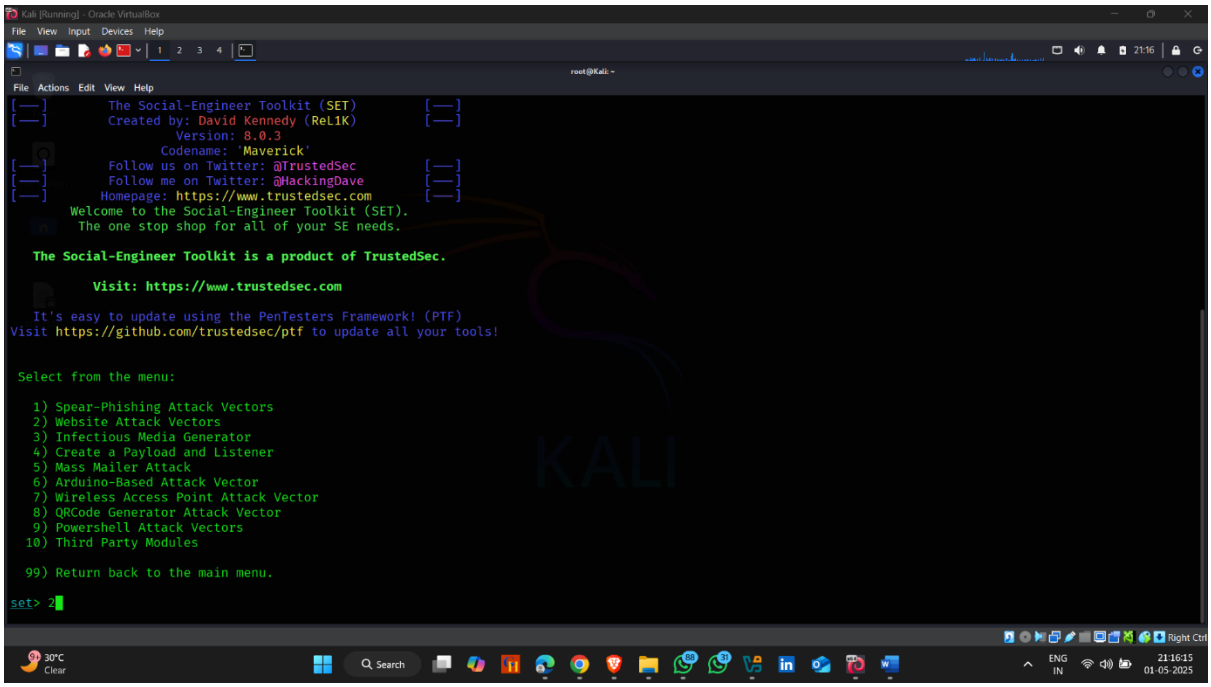
- Open kali linux terminal and type **setoolkit**



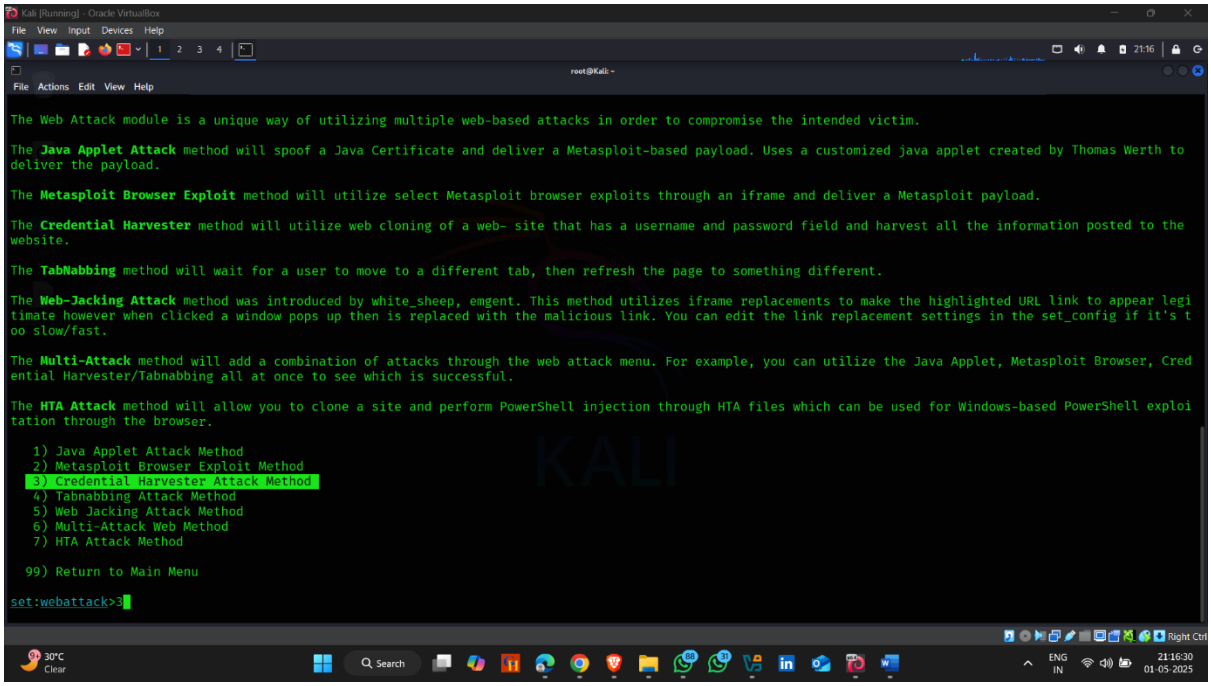
- It opens
- Now select 1 – **Social Engineering Attack**



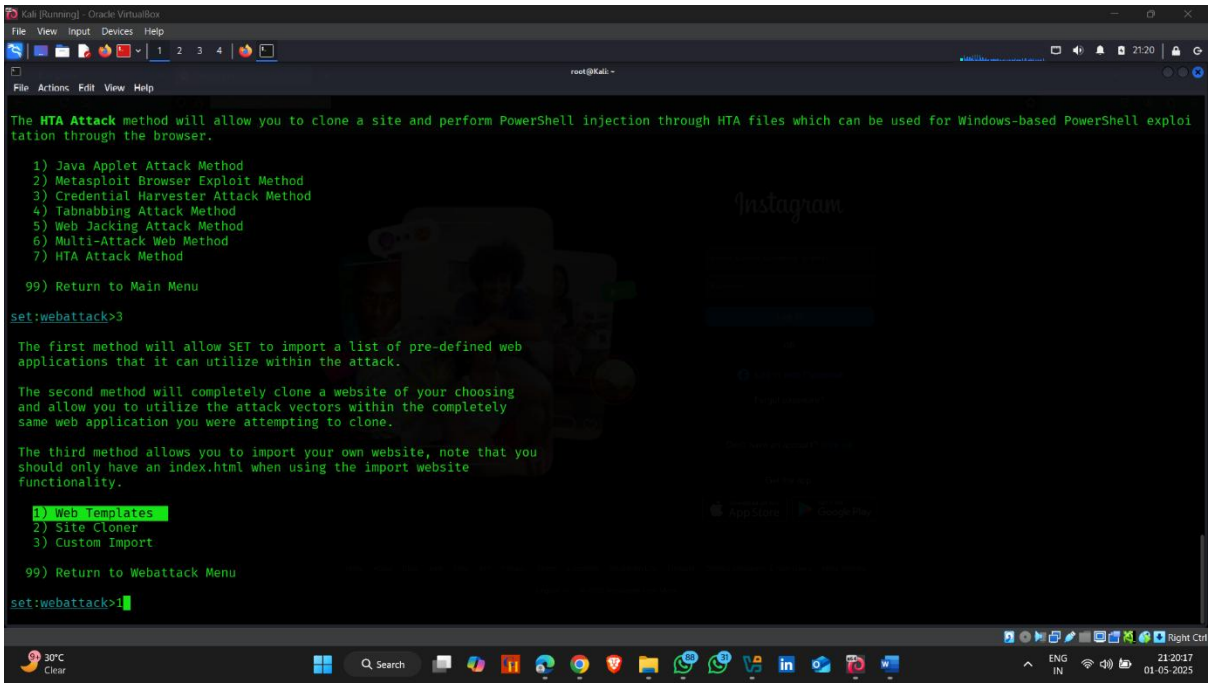
- Now select 2 – **Website attack Vector**



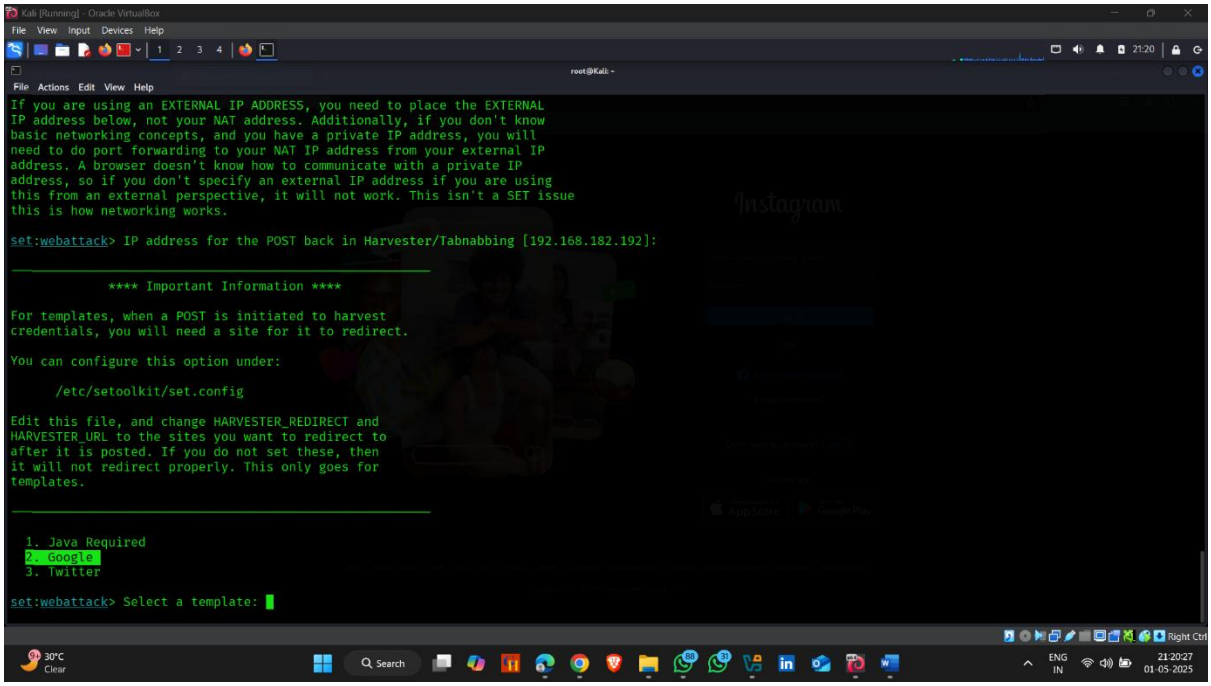
- Select 3 – Credential Harvesting Attack Method



- Select 2 – Web Template

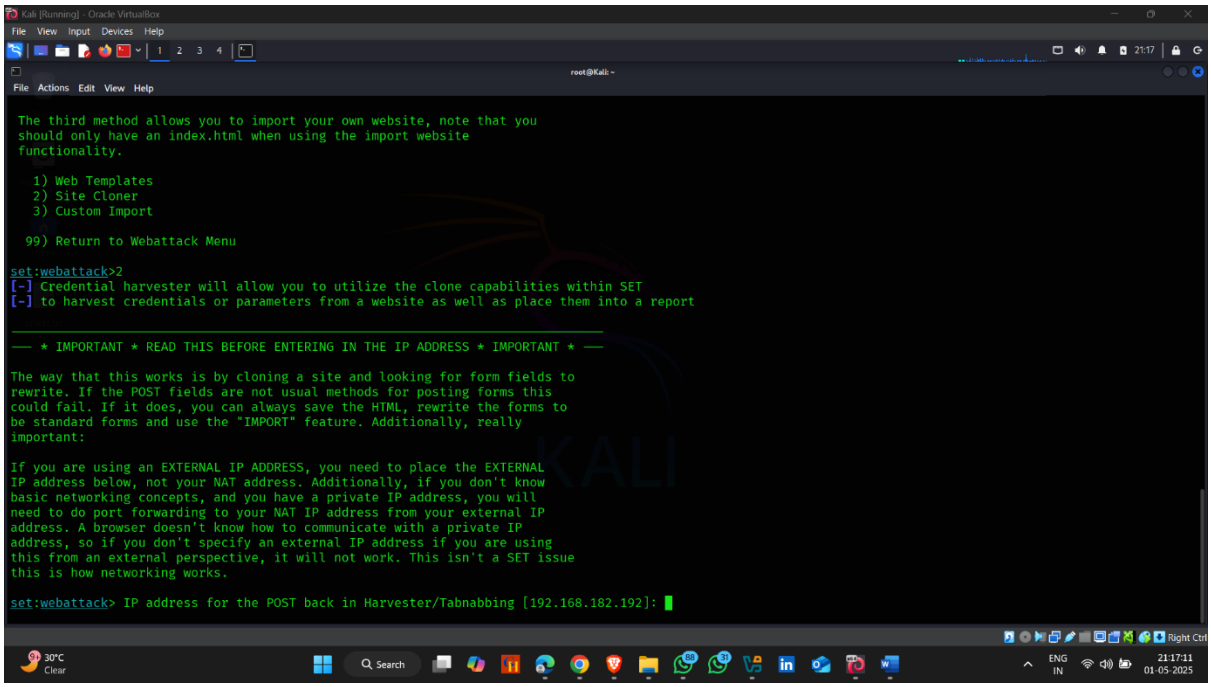


- Select Web template

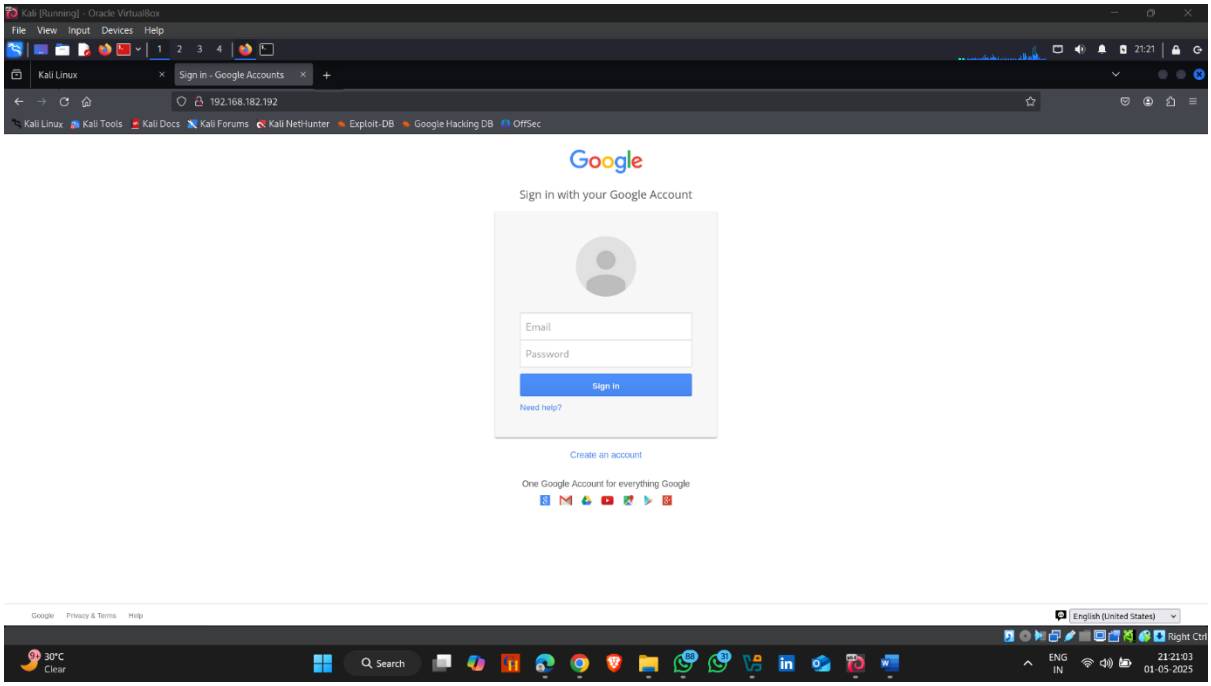


- Now provide a ip address that you want to get response back

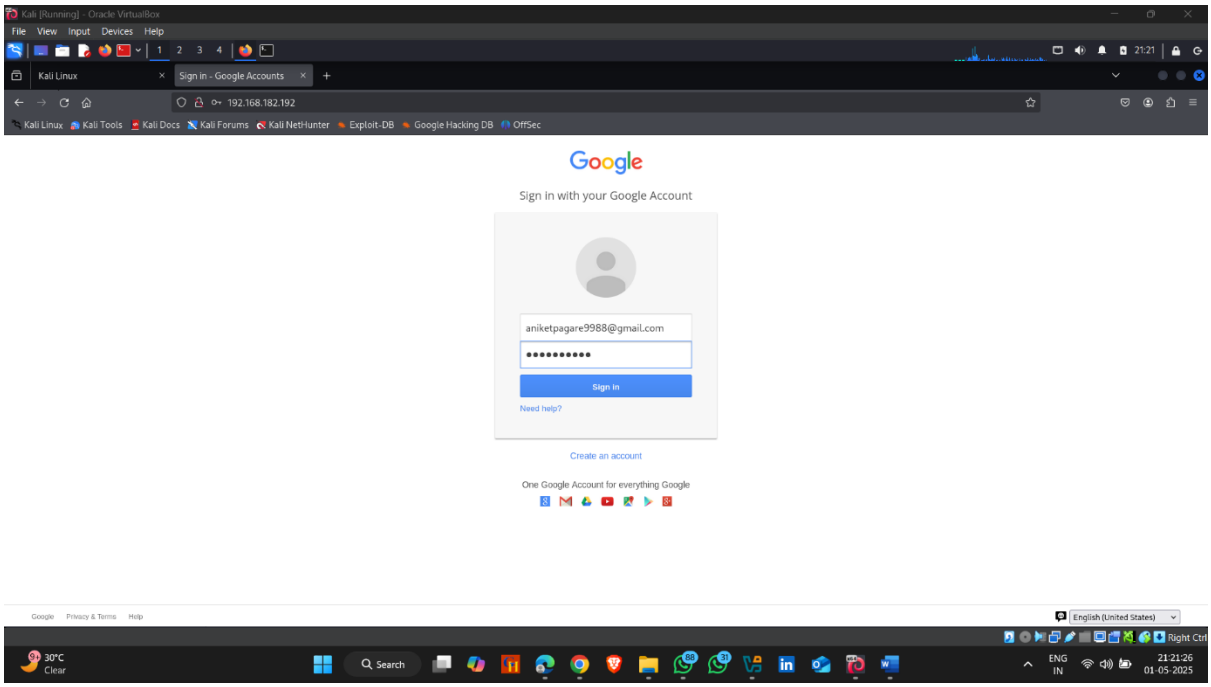
Note -: By default it select kali linux ip address



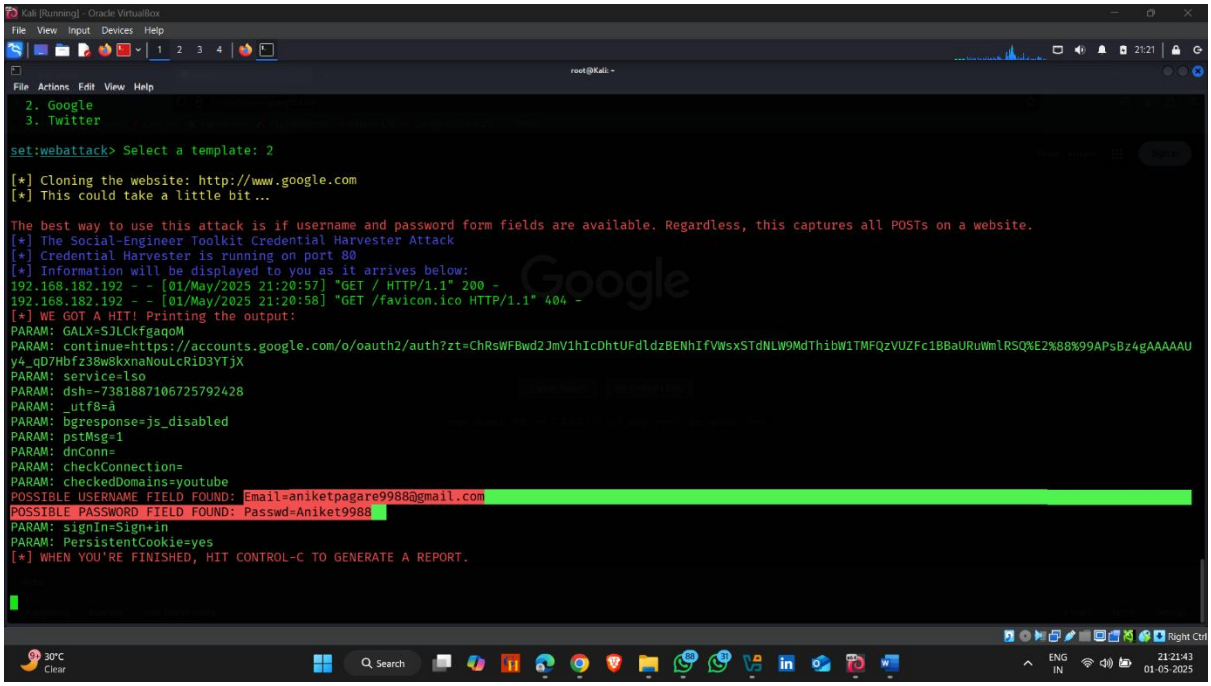
- Now open the browser on target machine and type kali linux ip address in url section
- Here , google login template occurred



- Provide a credentials



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

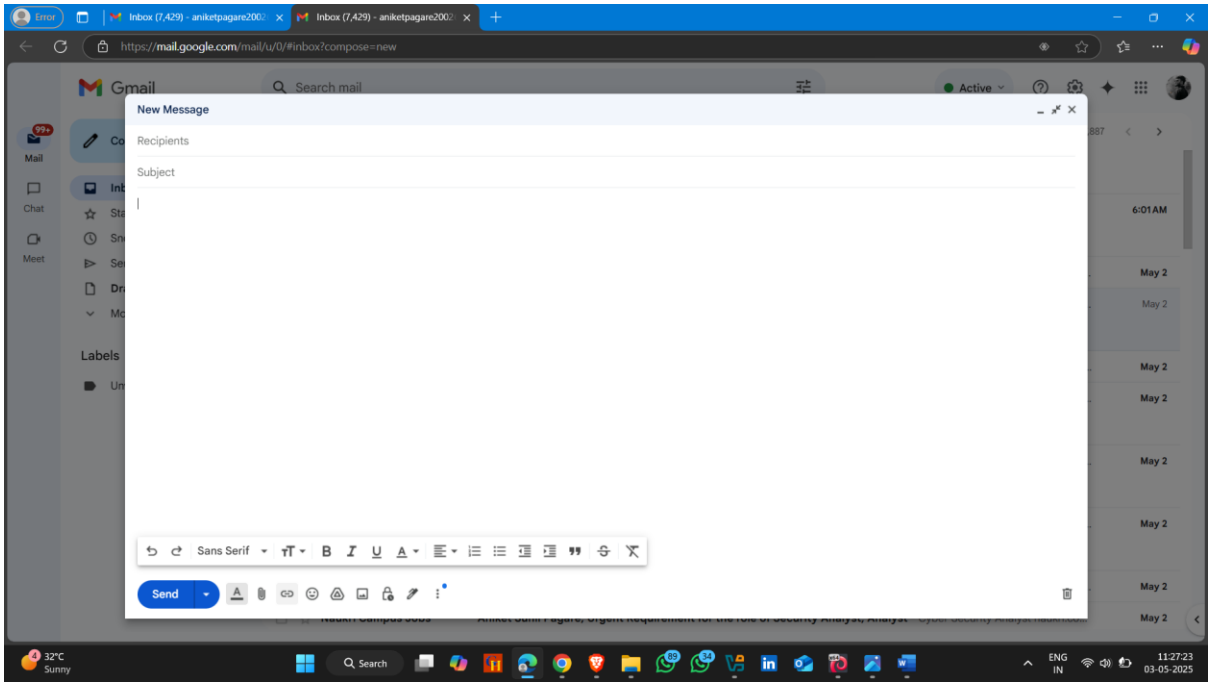


2.Perform Phishing Attack Using Gmail Account

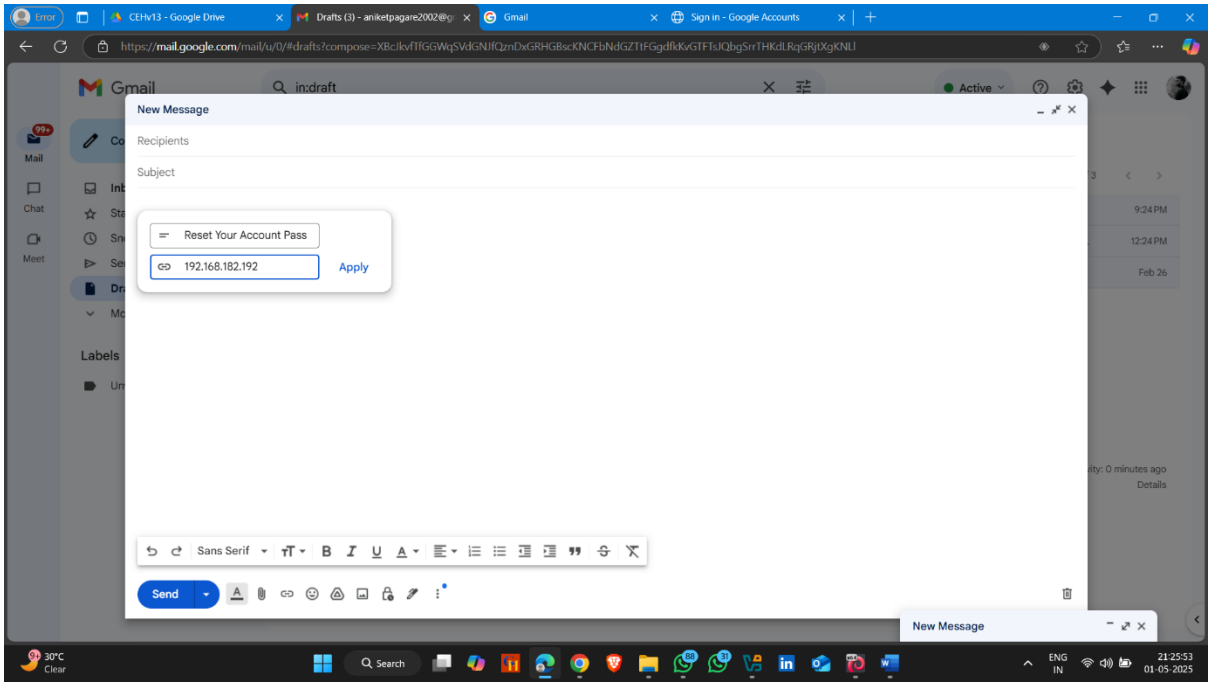
How to use it -:

- 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**

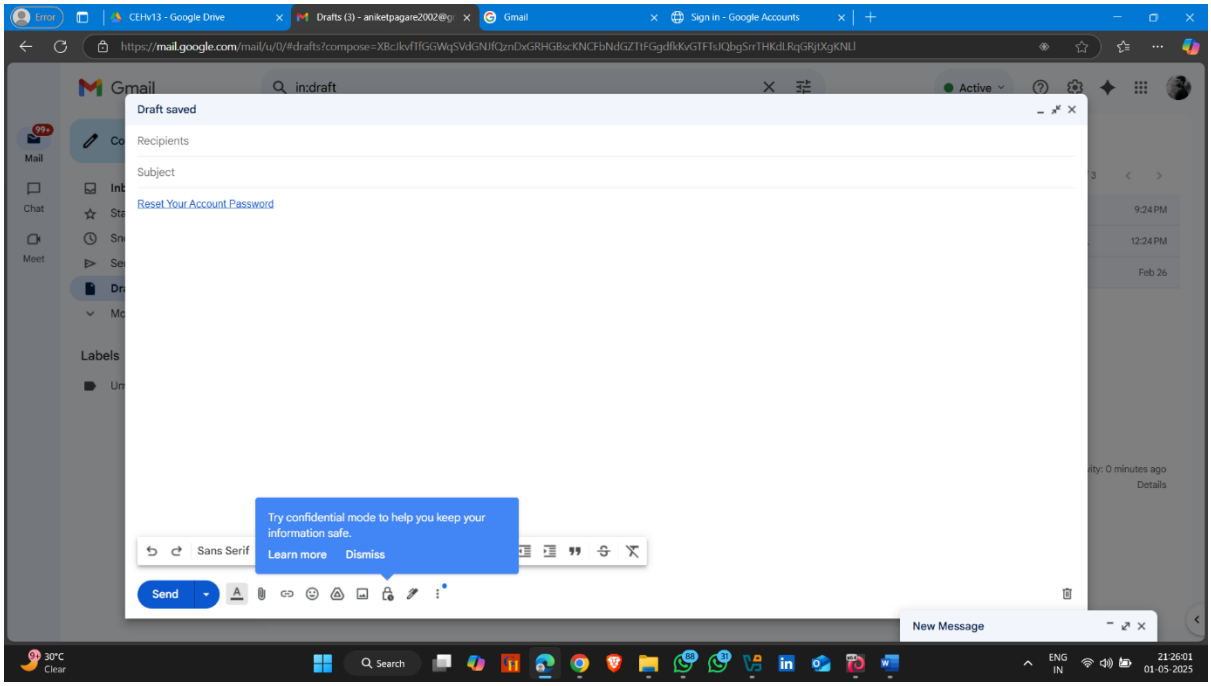
Note –: In Gmail, the hyperlink icon is typically found at the bottom of the composition window and looks like a few links in a chain.



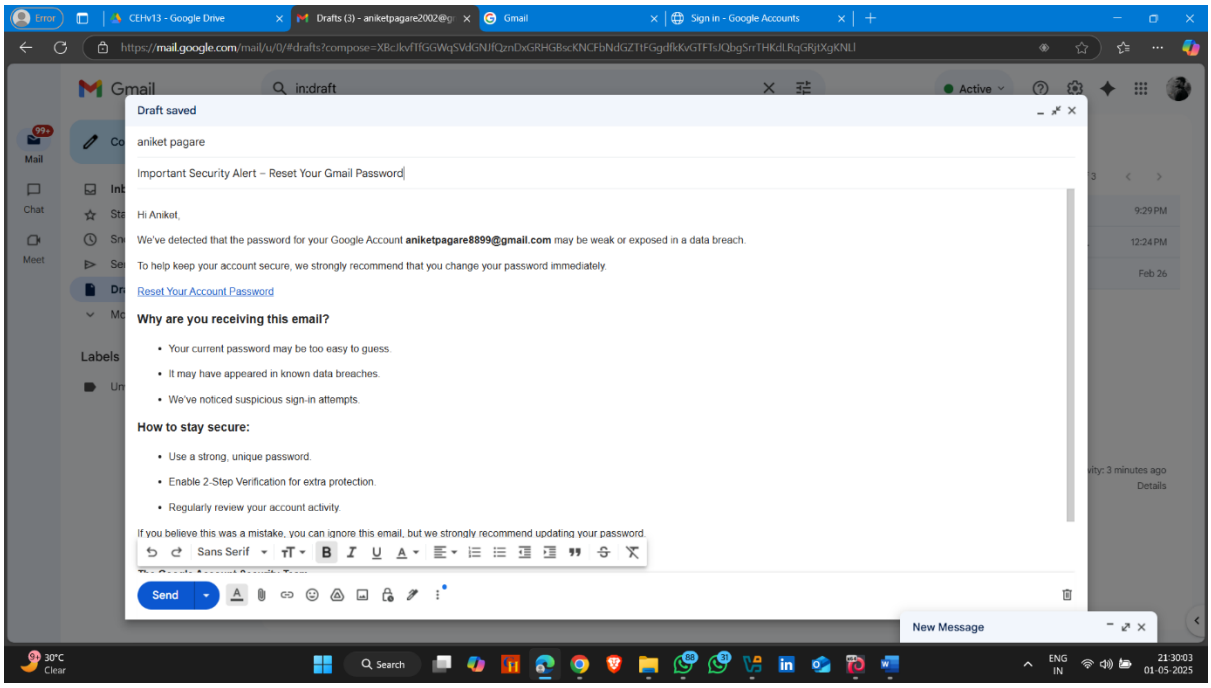
- First box – add message that display in main
- Second box – add attacker machine ip add and click on apply



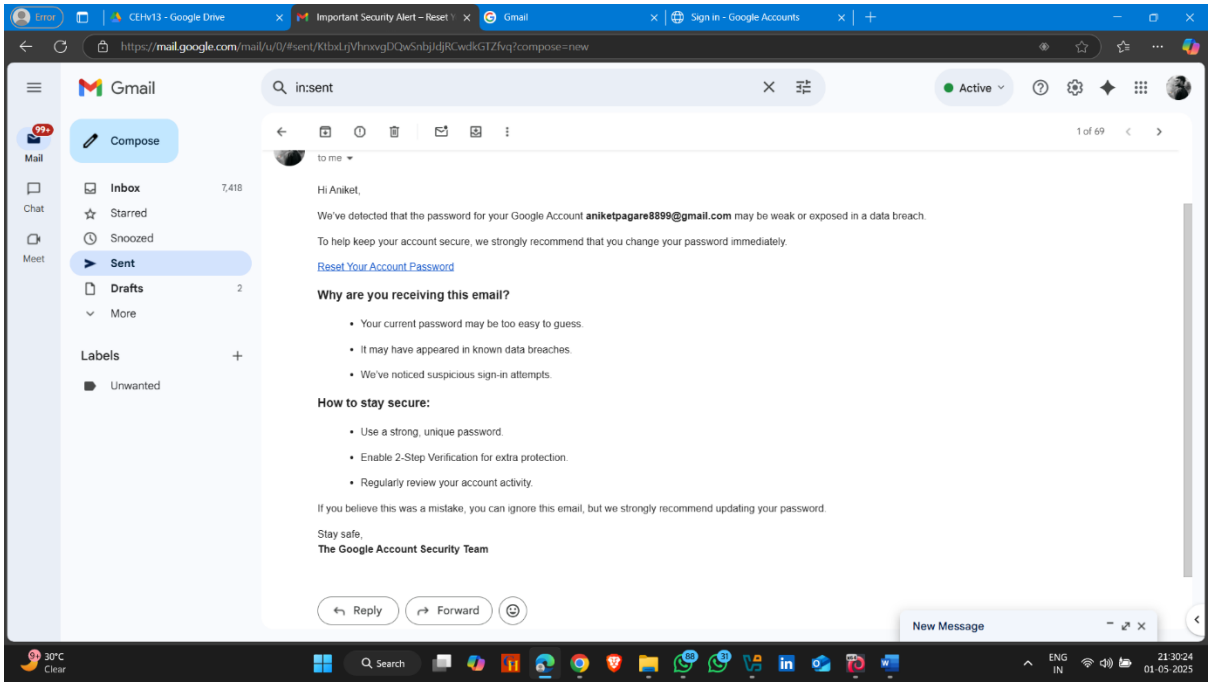
- **Hyperlink Generated**



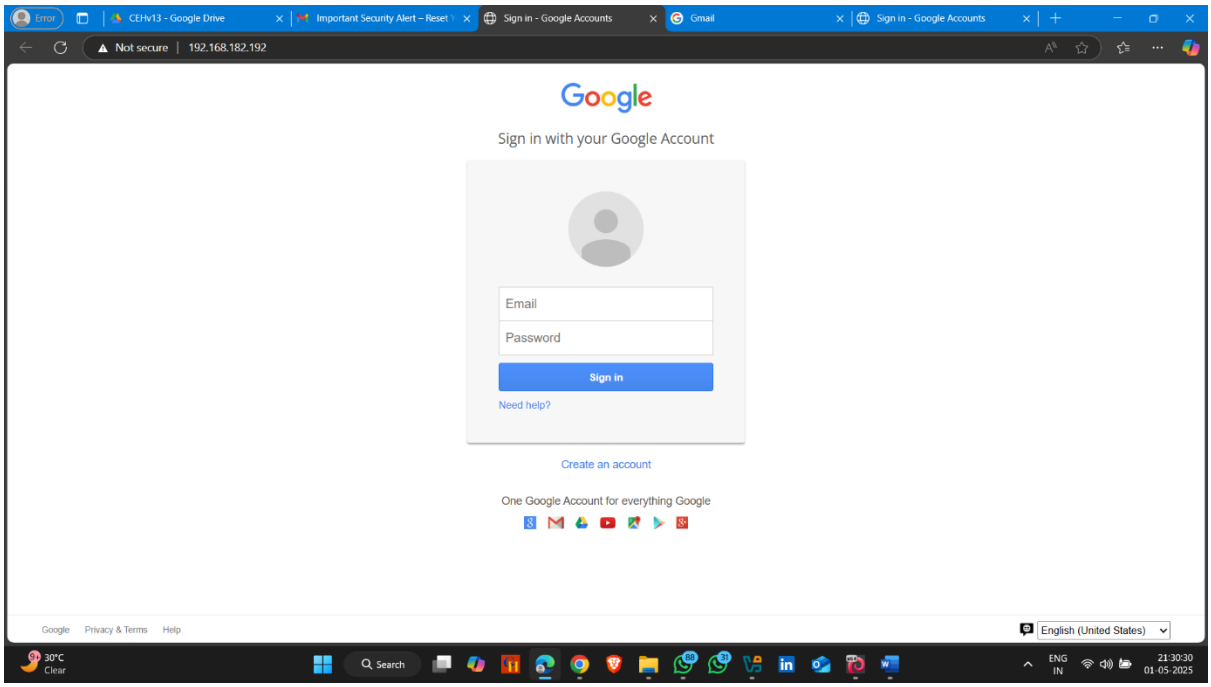
- Now add recipients and generate a mail using AI and it to the target



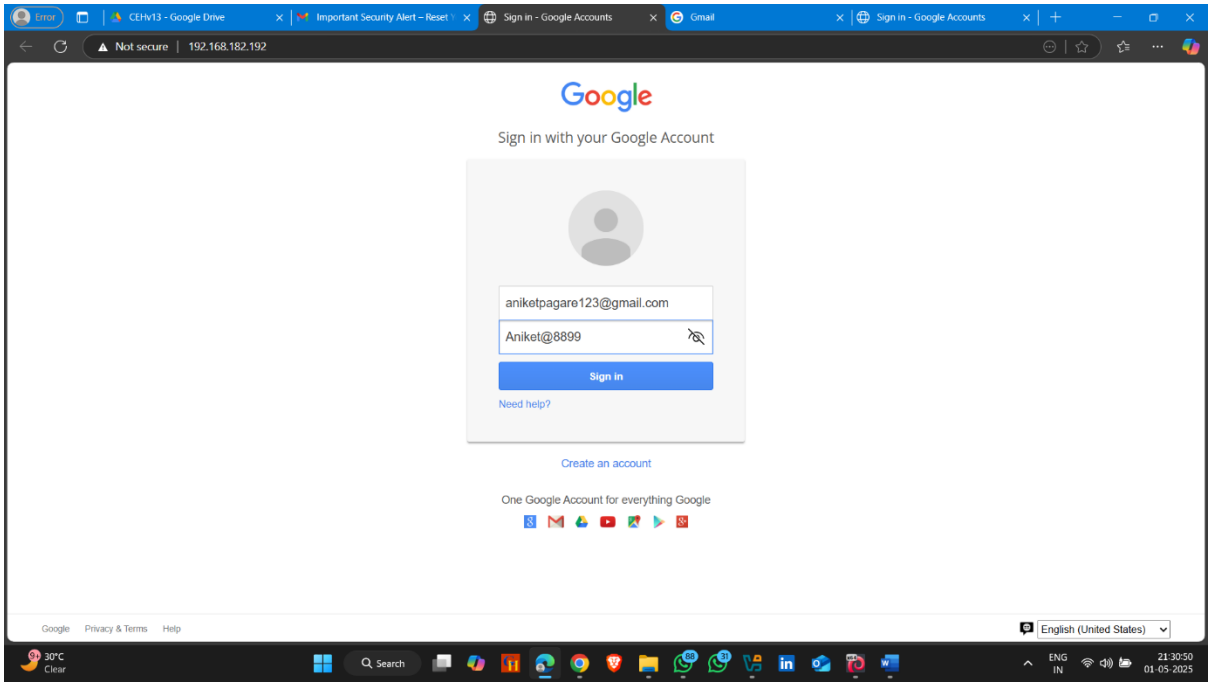
- **Mail received**
- Click on link – **Reset Your account password**



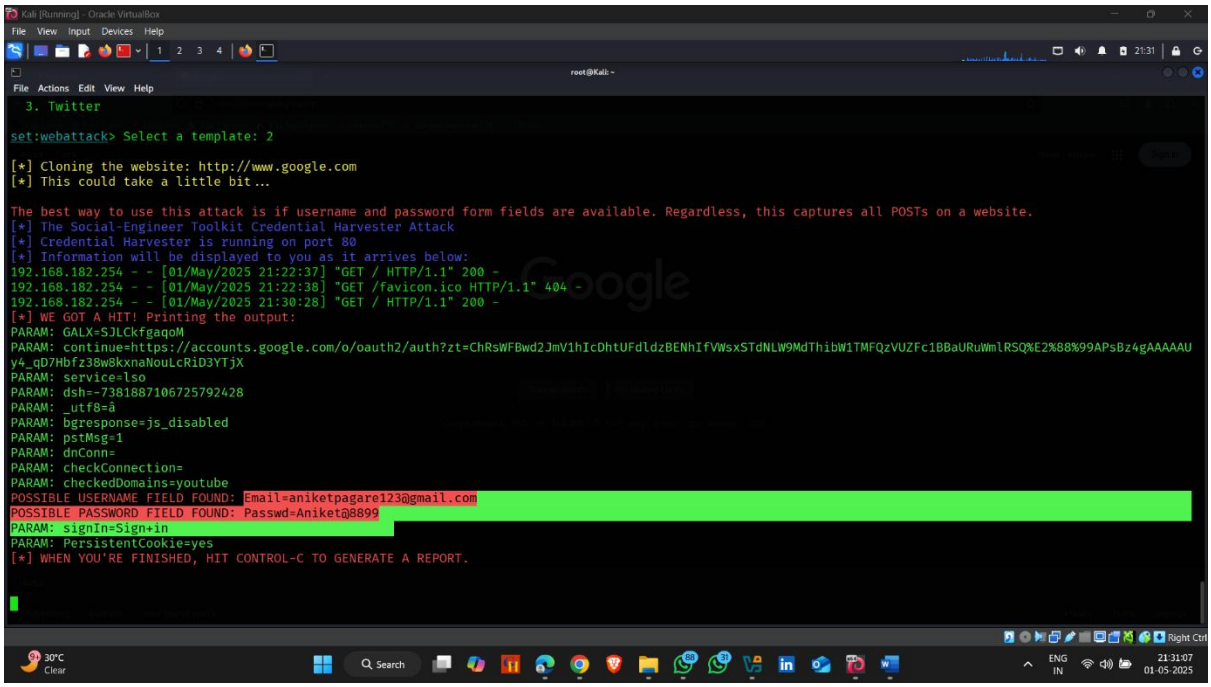
- Here Fake gmail login page is open



- Enter Credentials and go to the kali linux



- Here , username and password are got it .



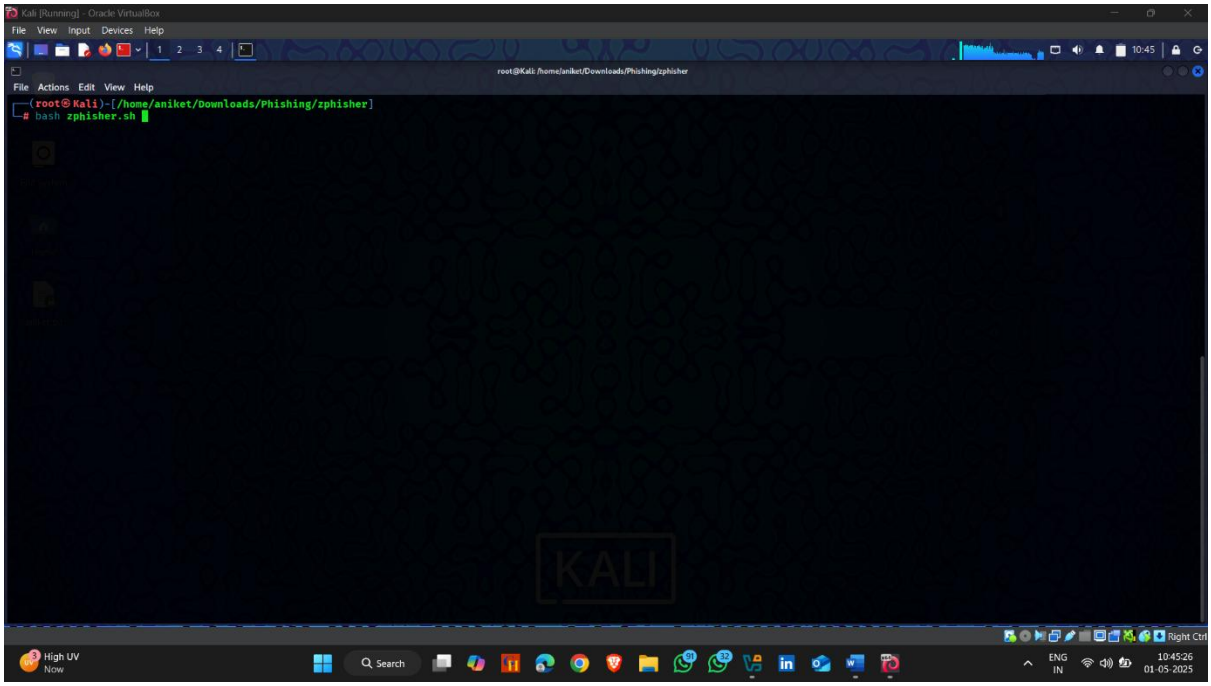
3.Perform Phishing Attack Using Zphisher

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**.

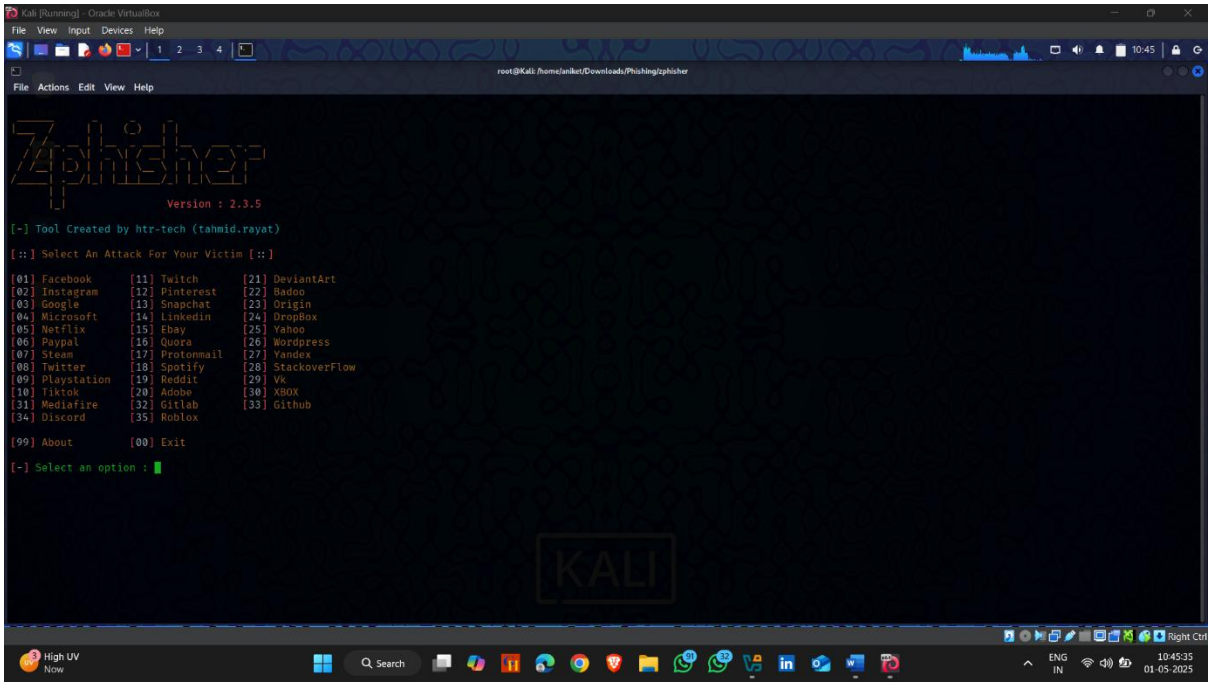
Download Link -: https://github.com/Tohidkhan6332/zphisher

How to use It -:

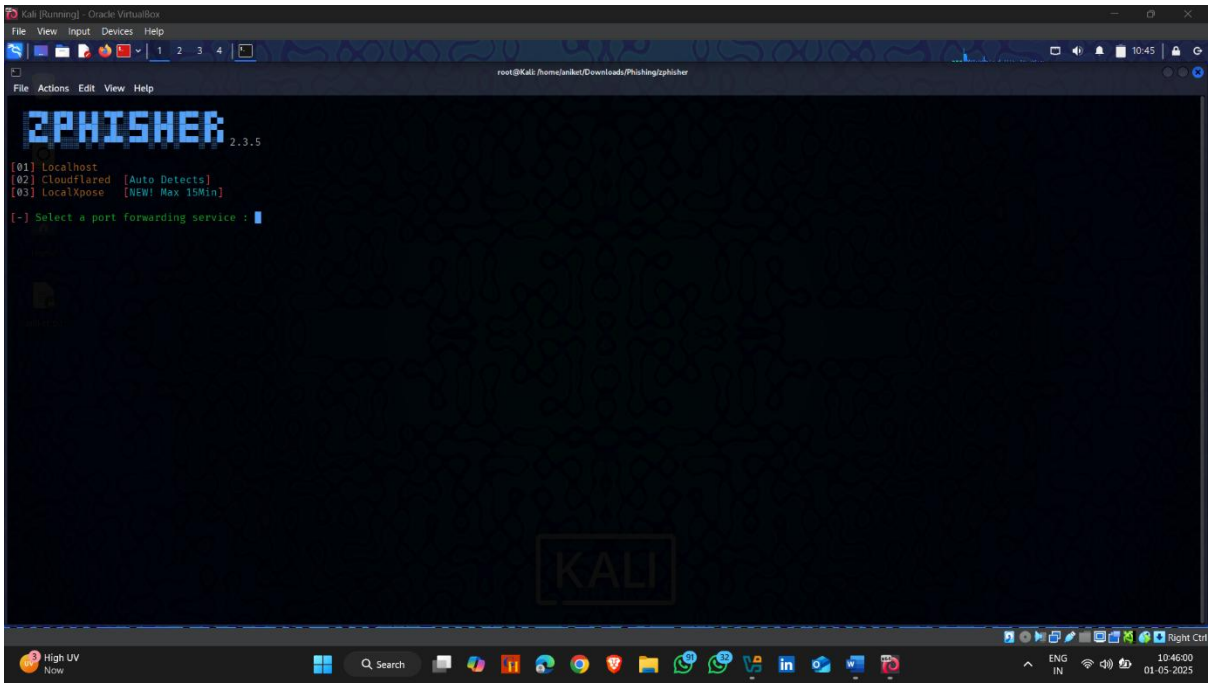
- Open kali linux terminal and go to the zphisher directory
- And use command – **bash zphisher.sh**



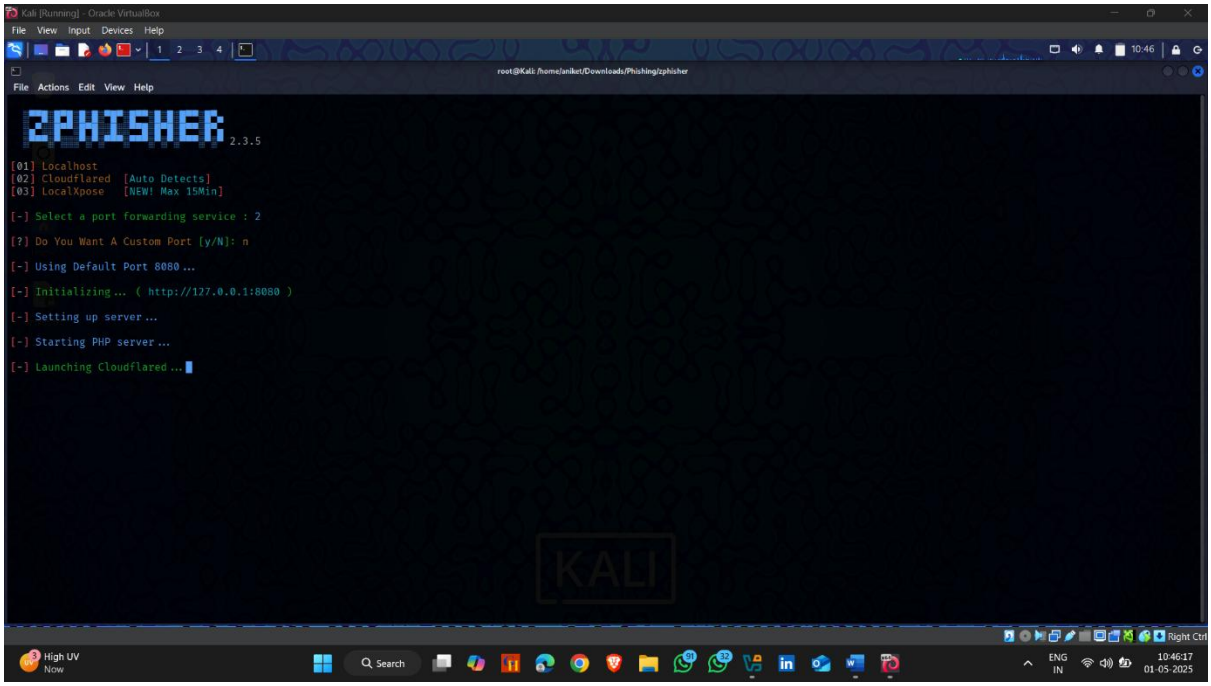
- **Zphisher open**
- Now select the number that you want to create phishing page



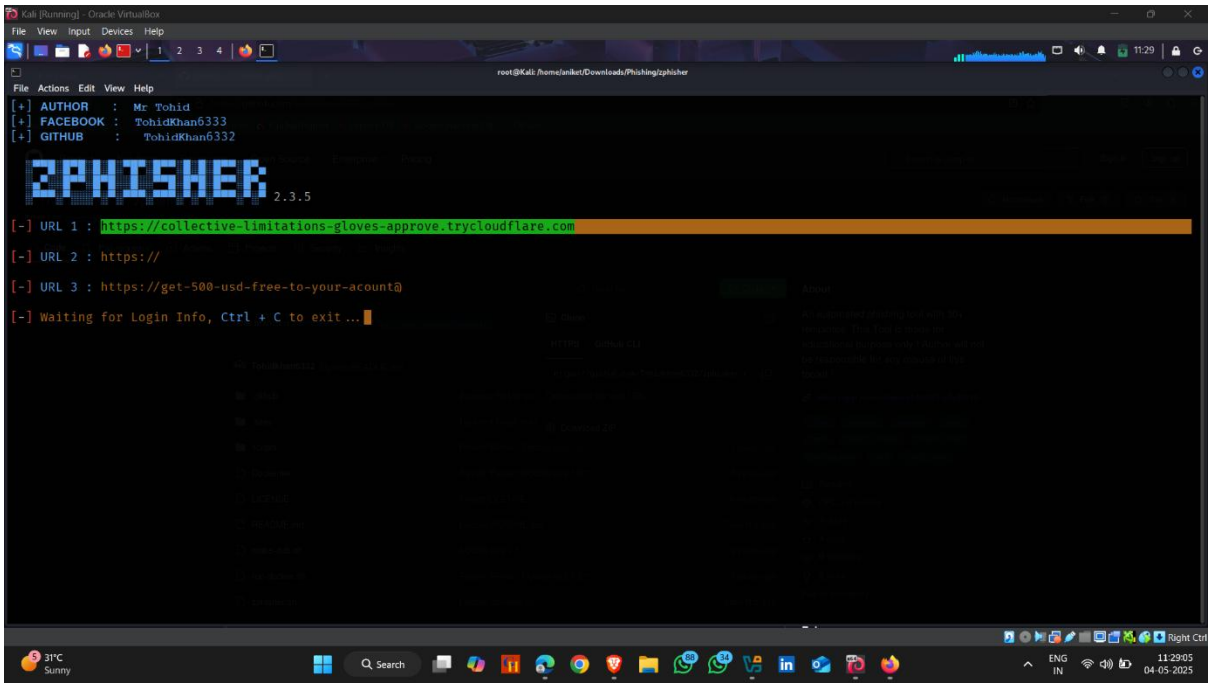
- Now select the **cloudflared server -2**



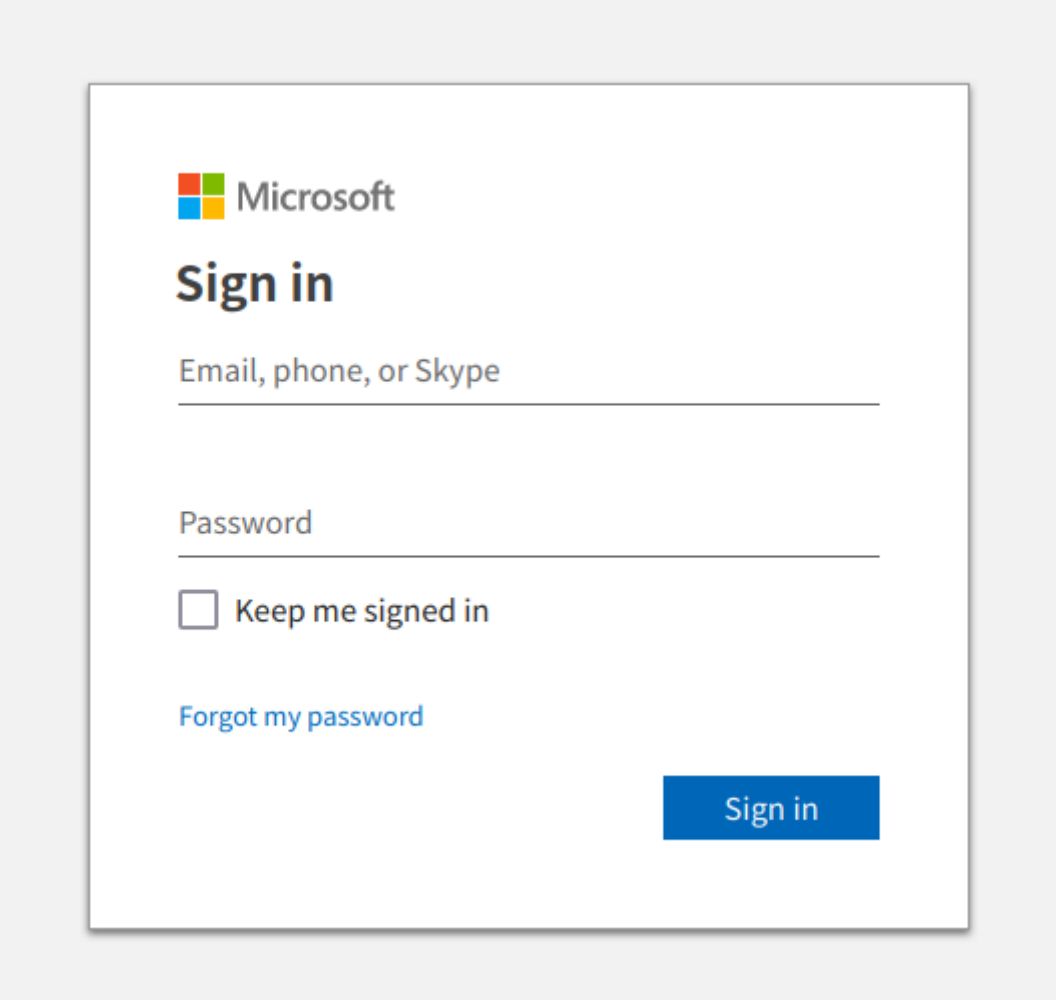
- Zphisher started for generate the link

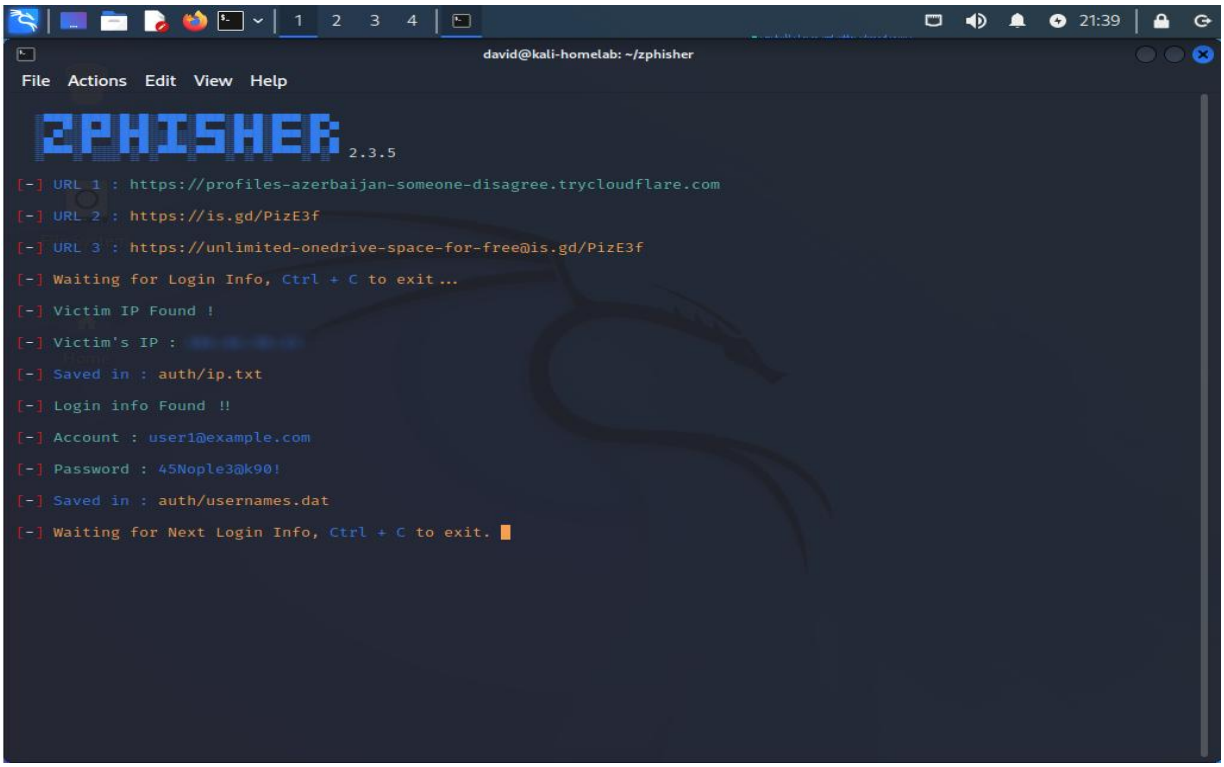


- Here , phishing link generated , now copy link and send it to the target



- Now Provide Credentials


Microsoft
Sign in
Email, phone, or Skype
Password
Keep me signed in
Forgot my password
Sign in


1 2 3 4
21:39
david@kali-homelab: ~/zphisher
File Actions Edit View Help
ZPHISHER 2.3.5
[-] URL 1 : https://profiles-azerbaijan-someone-disagree.trycloudflare.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.

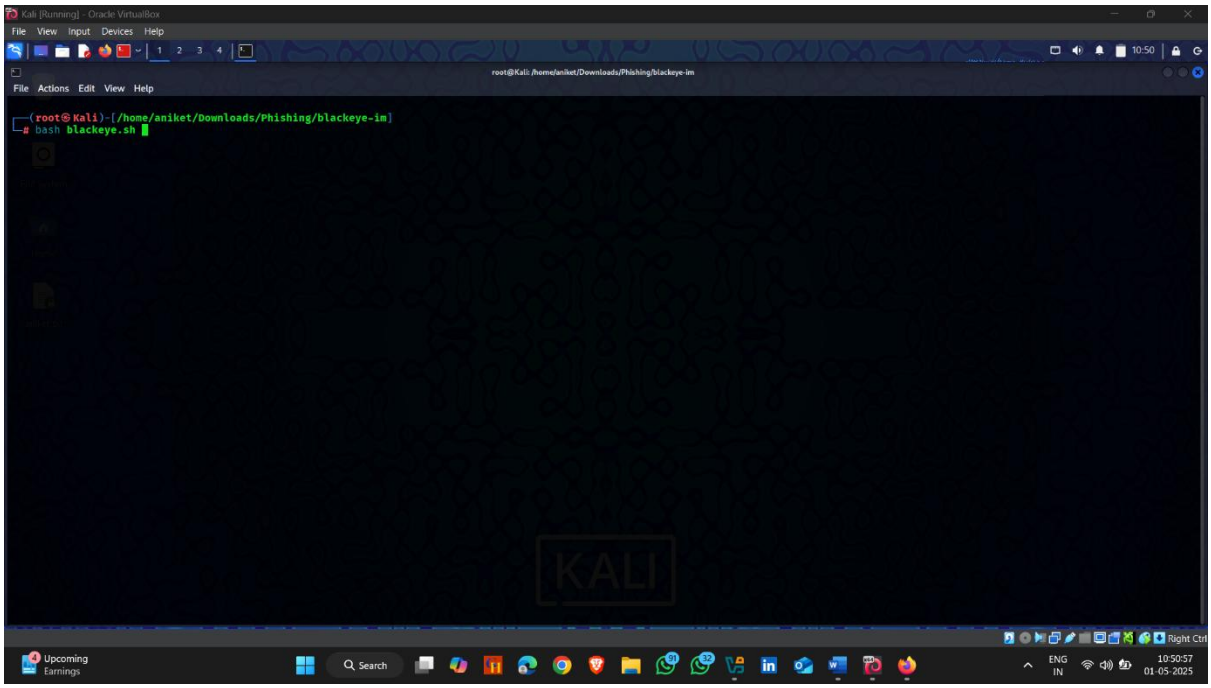
EXTRA ACTIVITY

1.Perform Phishing Attack Using Blackeye Tool

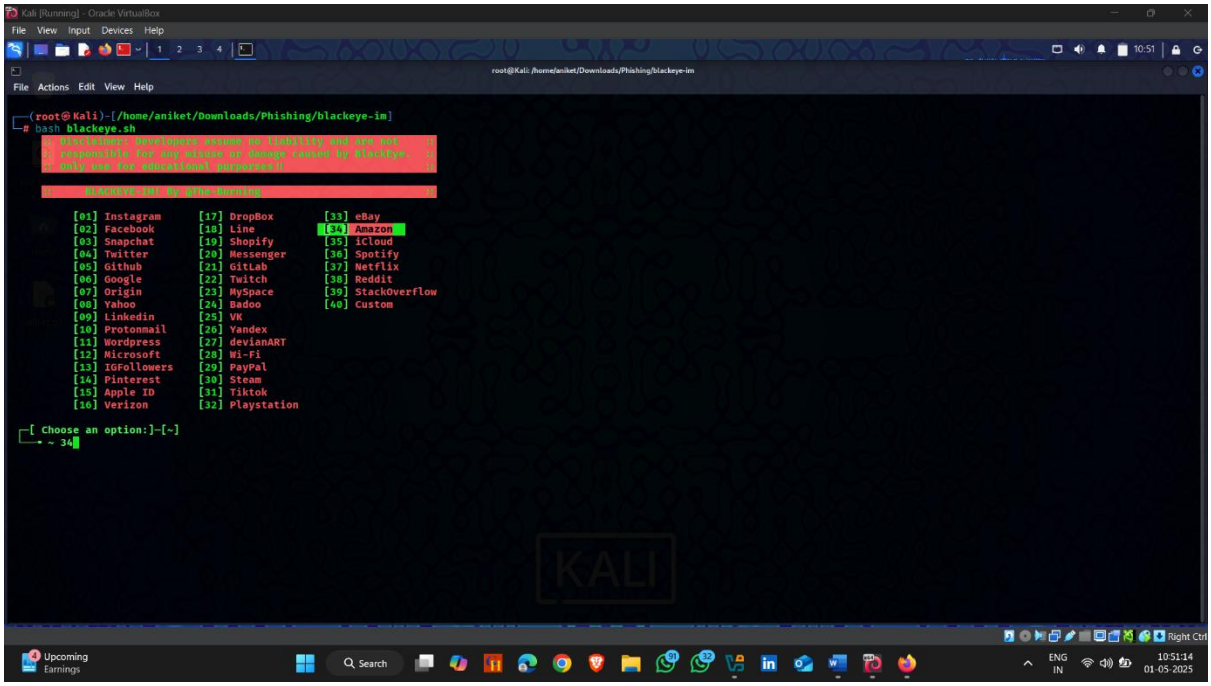
Download Link -:
https://github.com/thewickedkarma/blackeye-im

How to use it -:

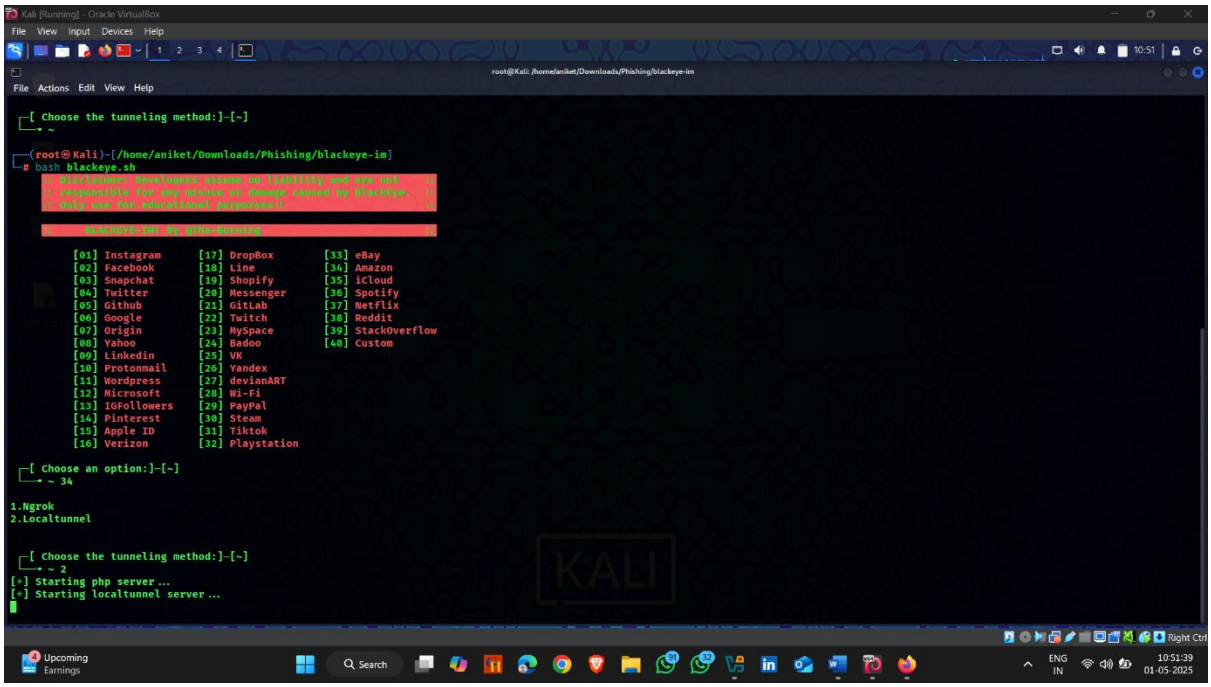
- Open Kali linux terminal and go to the blackeye directory
- Type command – **bash blackeye.sh**



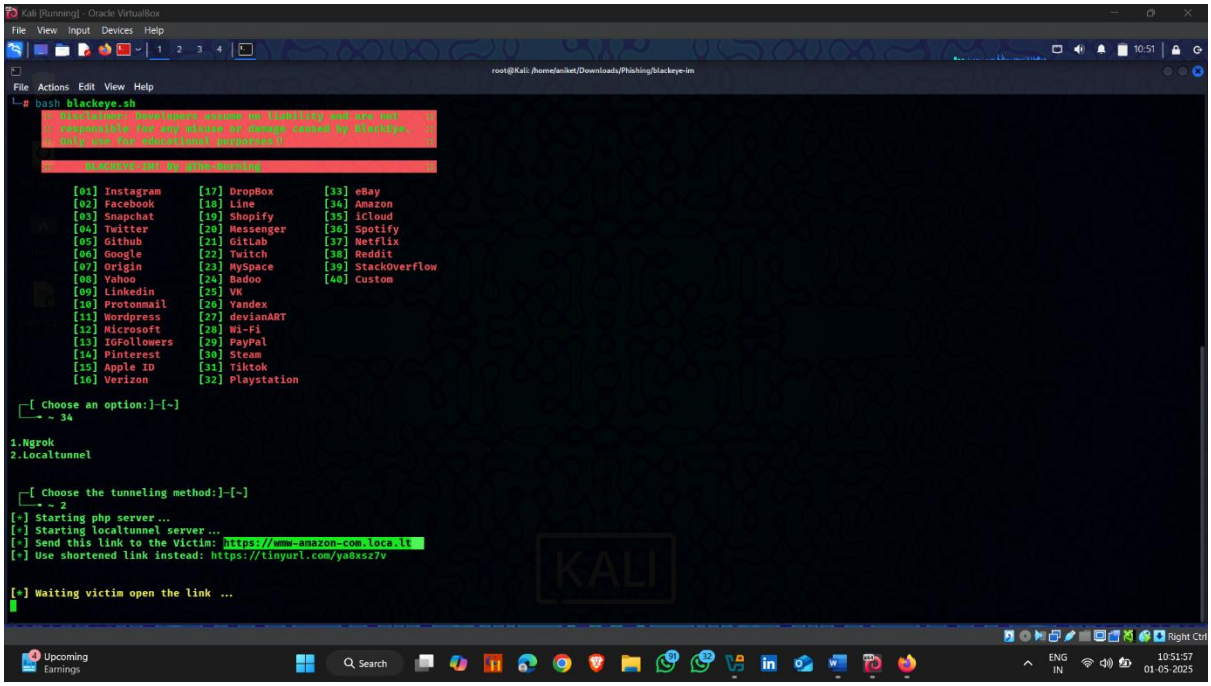
- **Blackeye open**
- Now enter the number that you want to create a fake phishing page



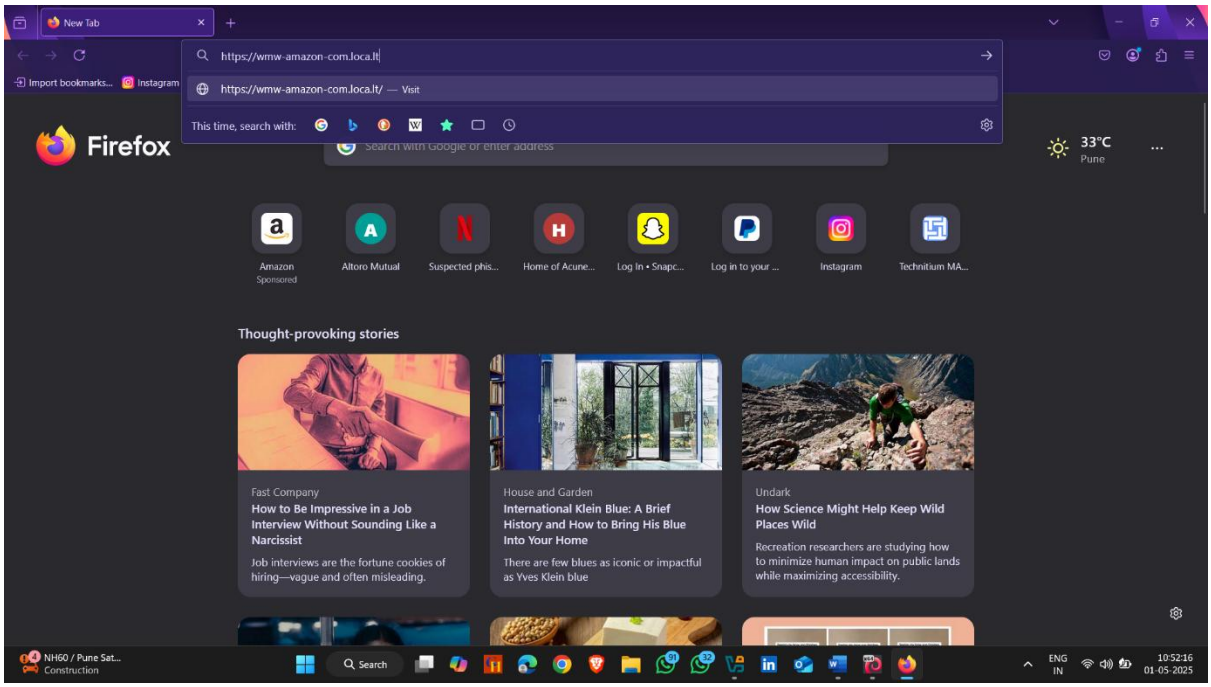
- Now select the tunneling method



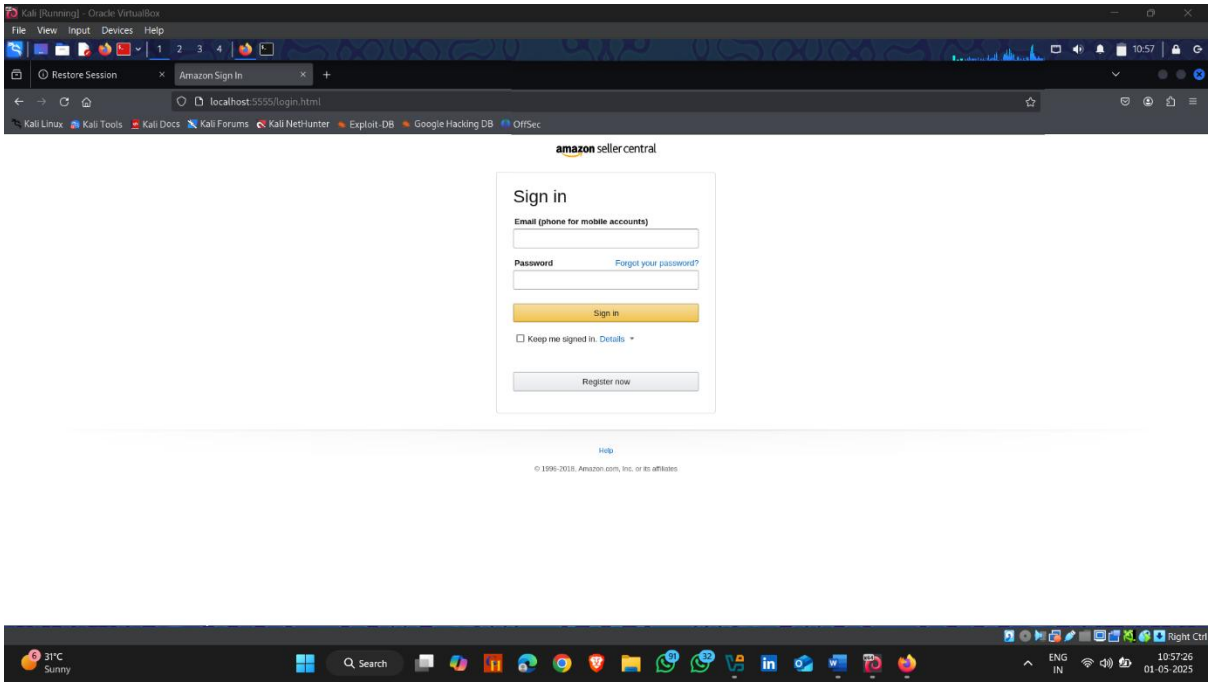
- Here link is generated
- Now copy link and send it to the target



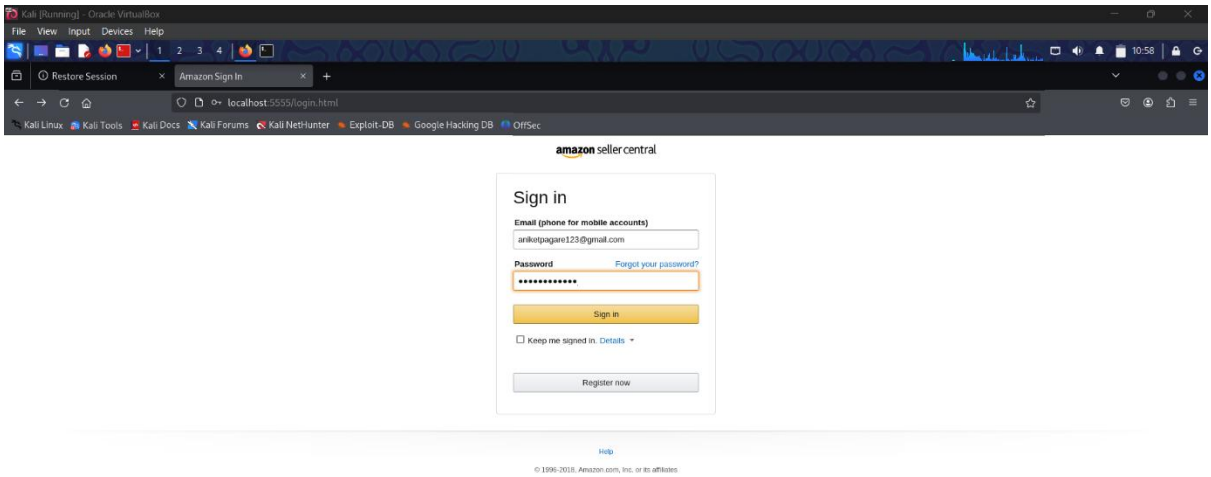
- Paste link in the url section



- Fake amazon login page open

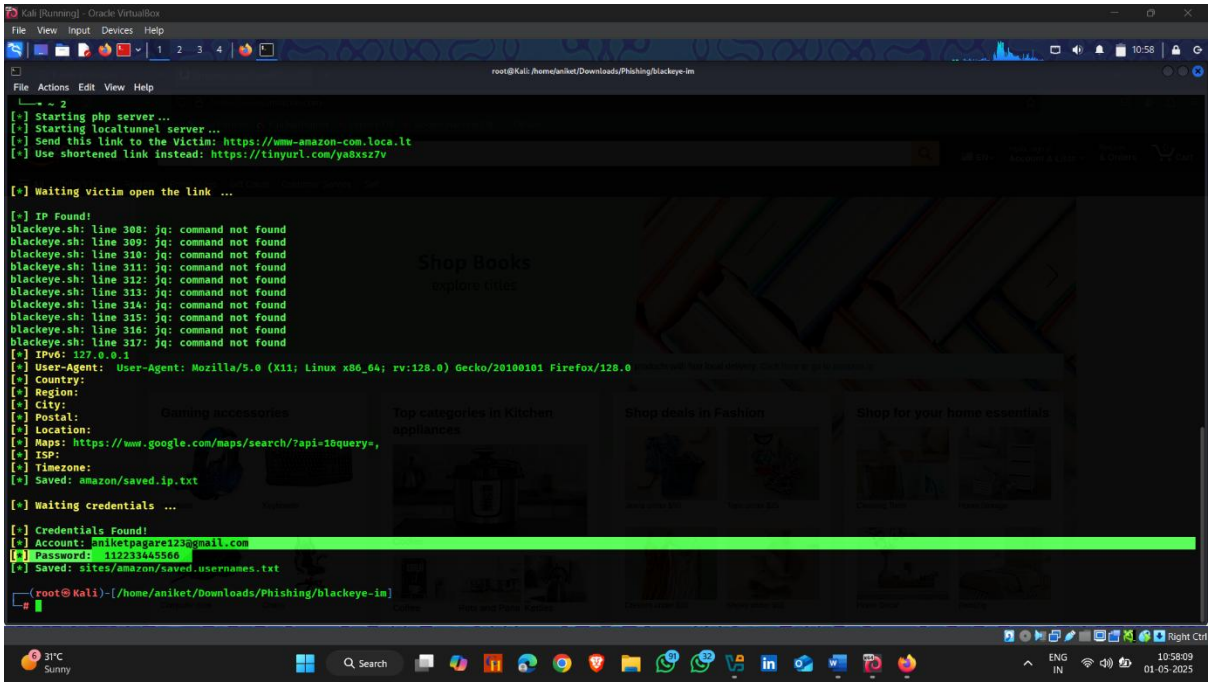


- Provide Credentials and sign in



- Now open kali linux teminal

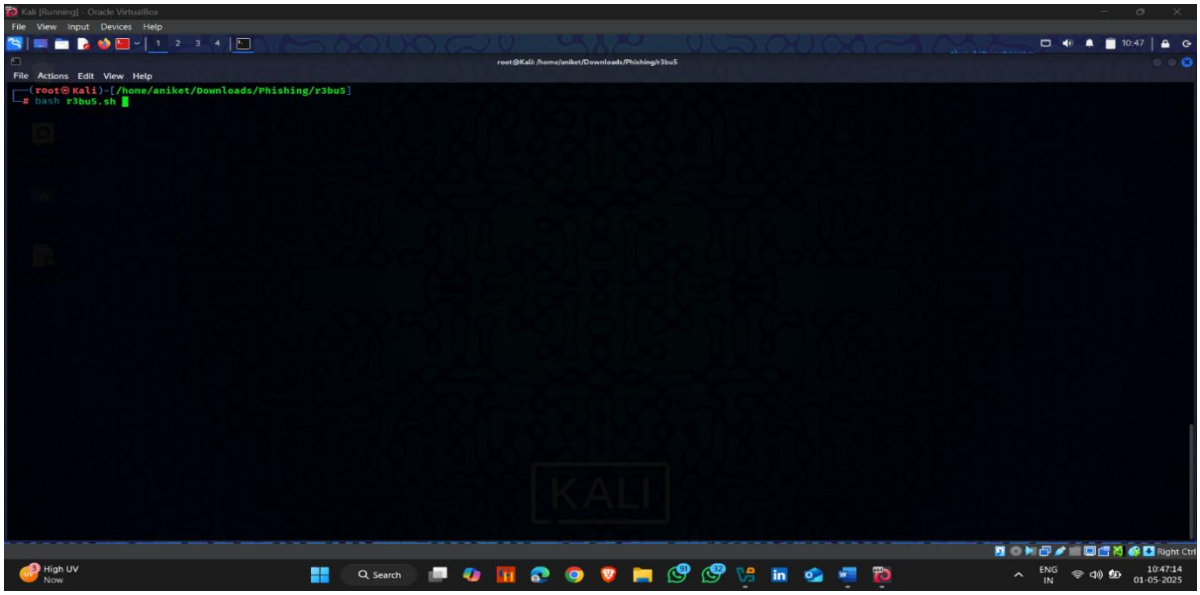
- **Username and password are captured**



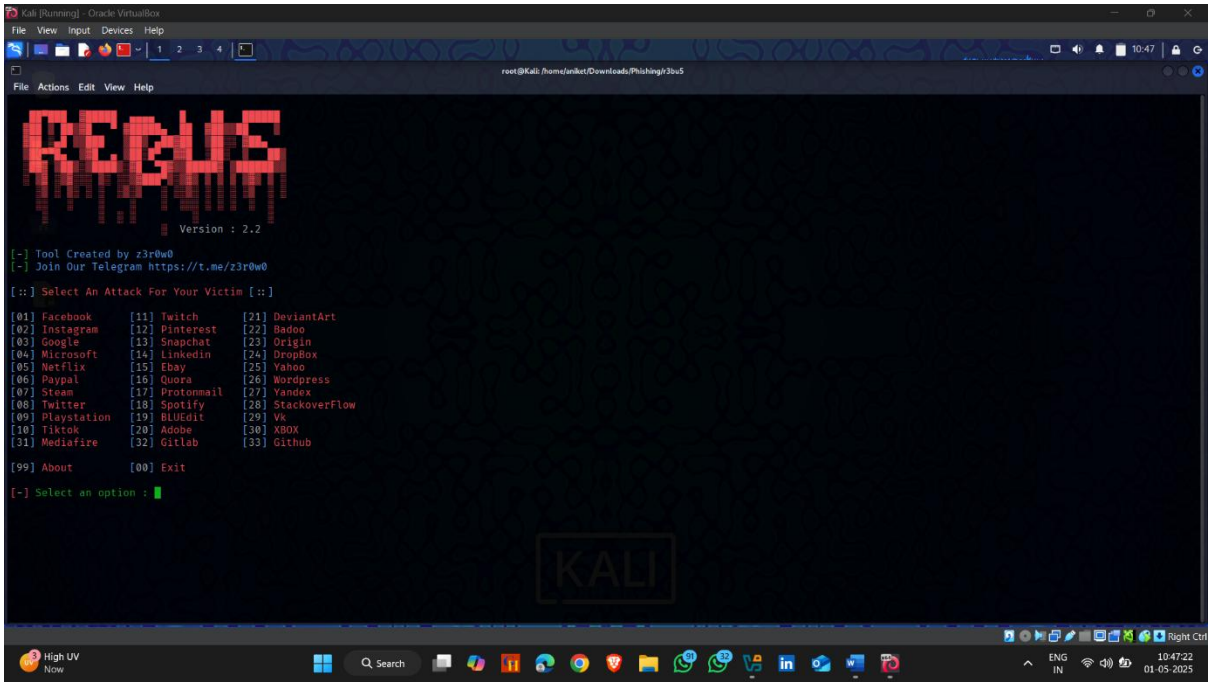
2.Perform Phishing Attack Using r3bu5 Tool

How to use it -:

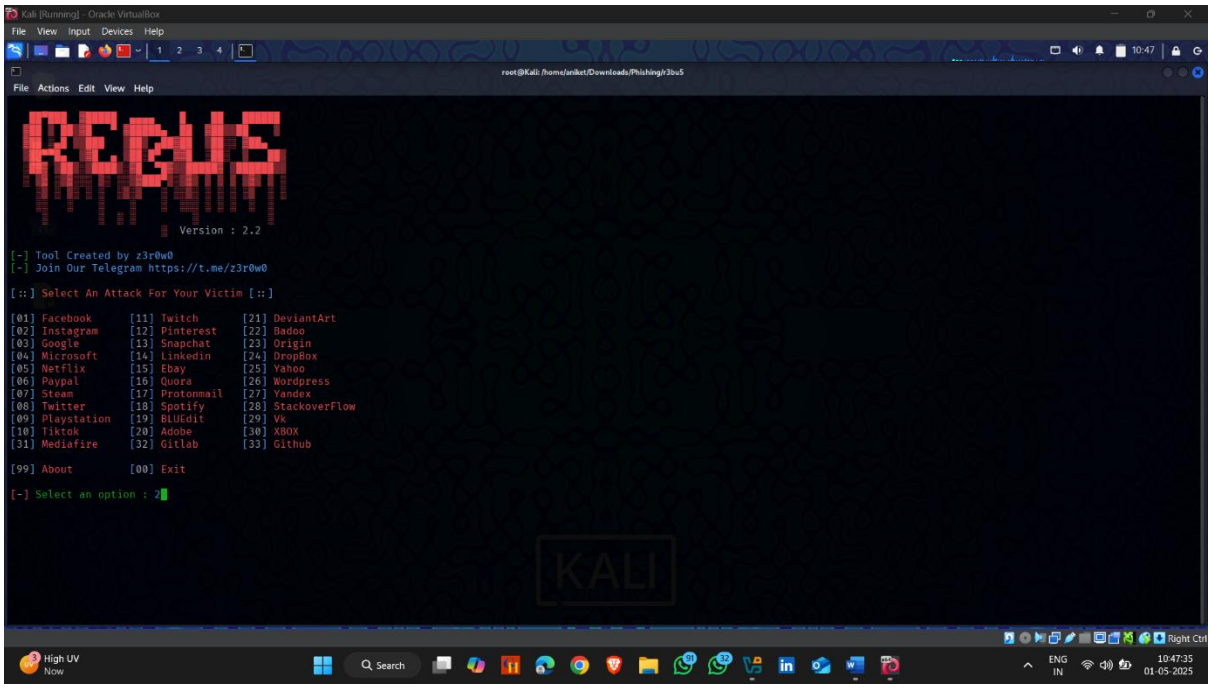
- Open kali linux Terminal and go to the r3bu5 Directory
- And type command – **bash r3bu5.sh** and enter



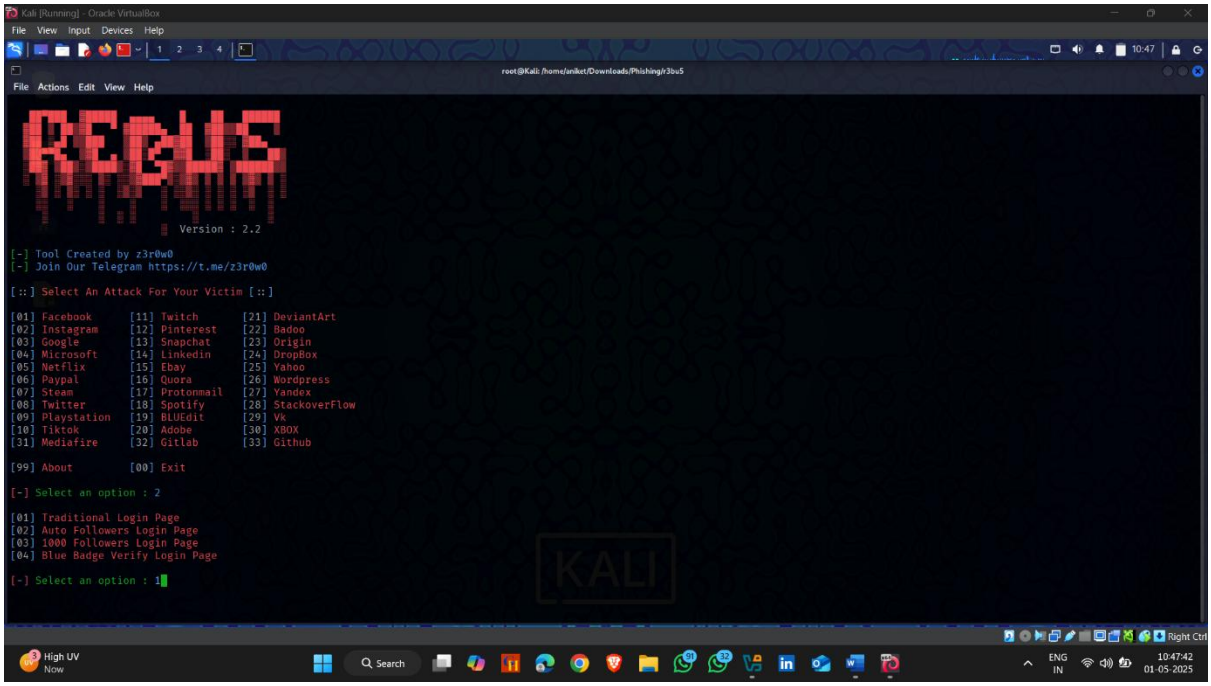
- R3bu5 start



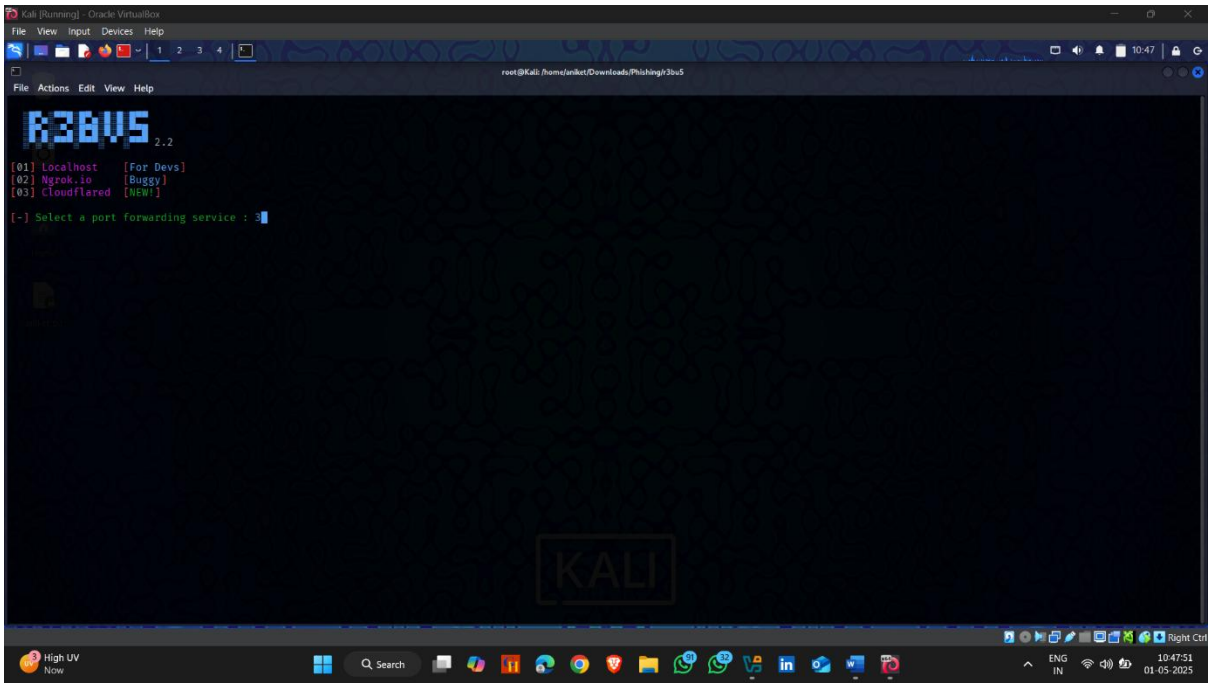
- now select the number for create a phishing site



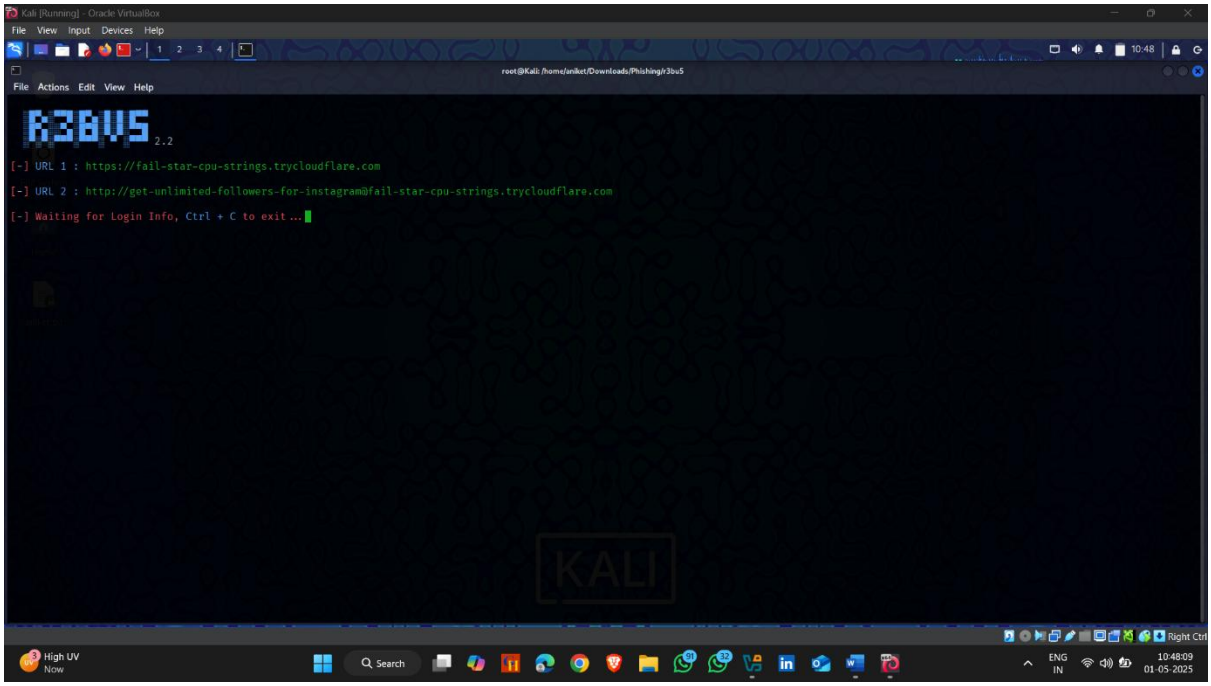
- Now select the option for what kind of login page you want



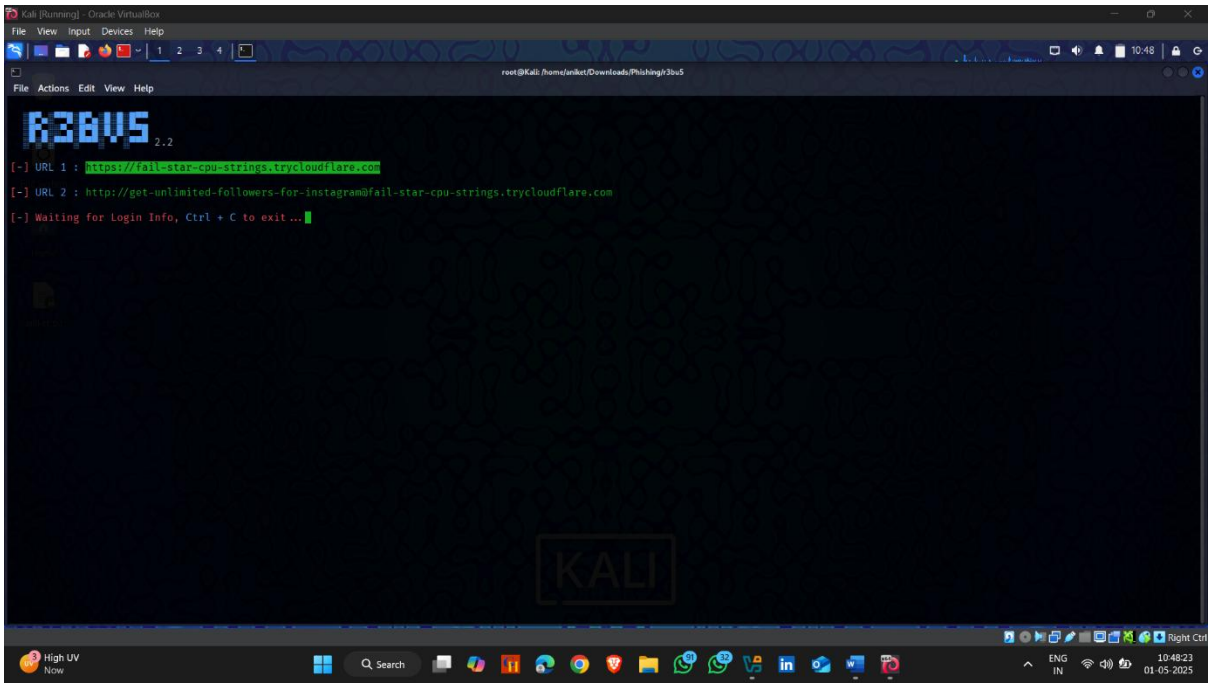
- Select the server



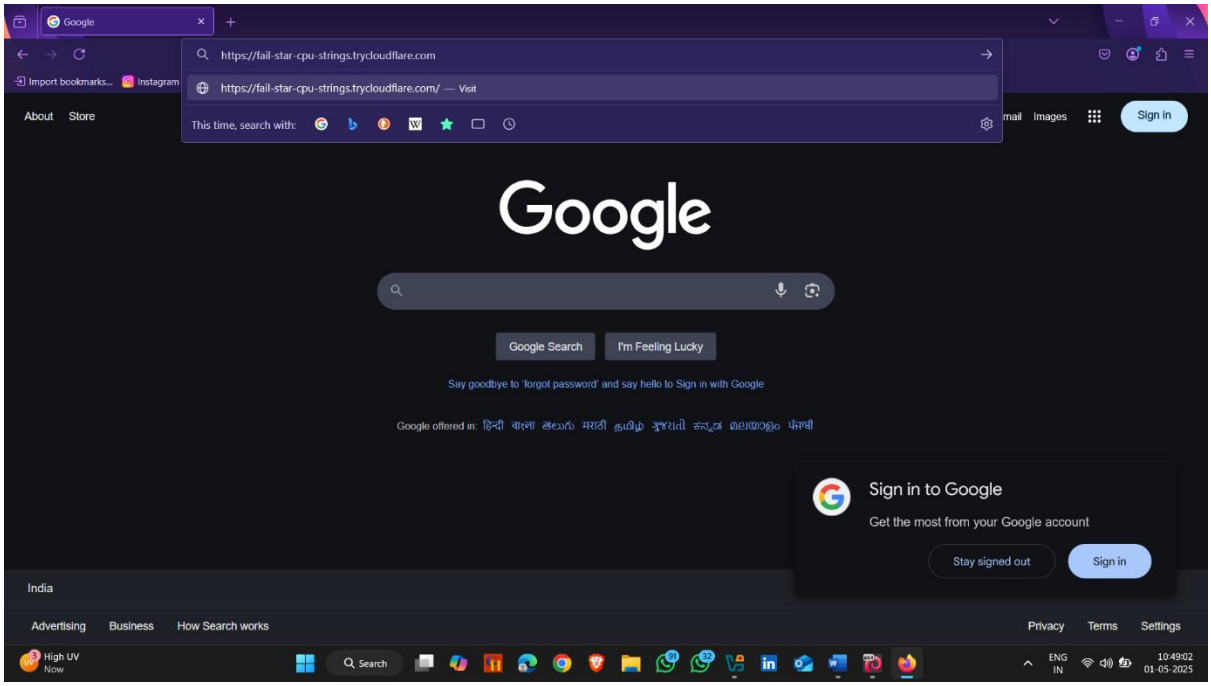
- Link is Generated



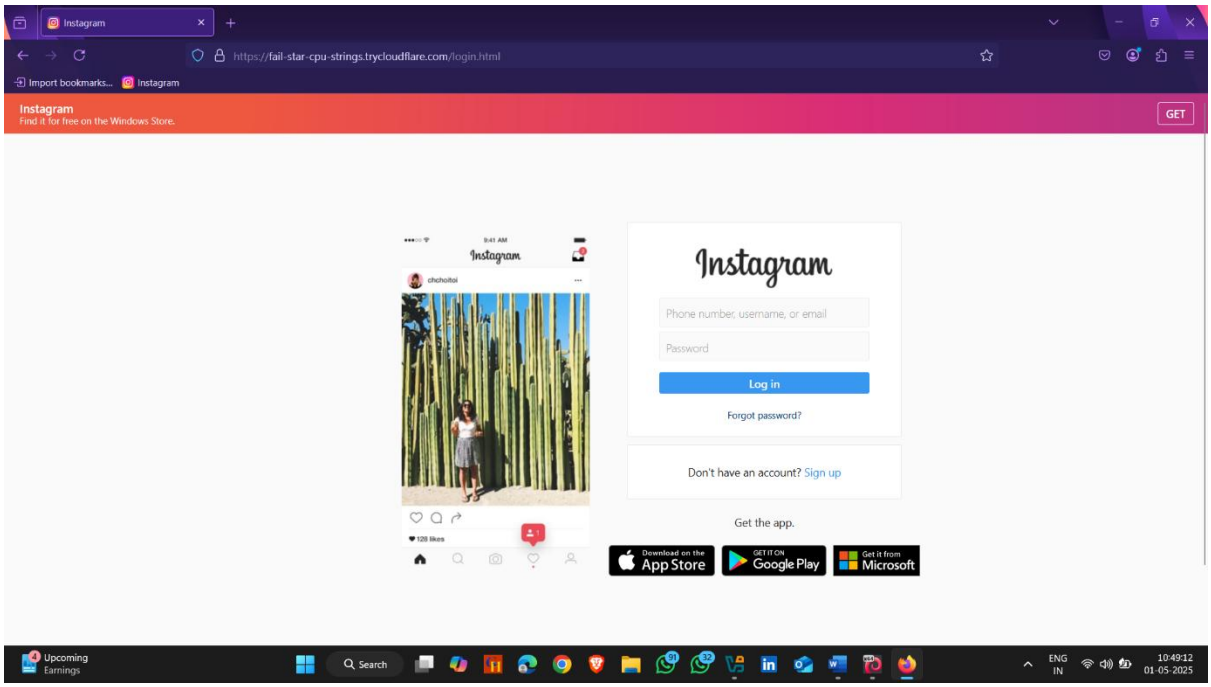
- Copy first url and send it to the target



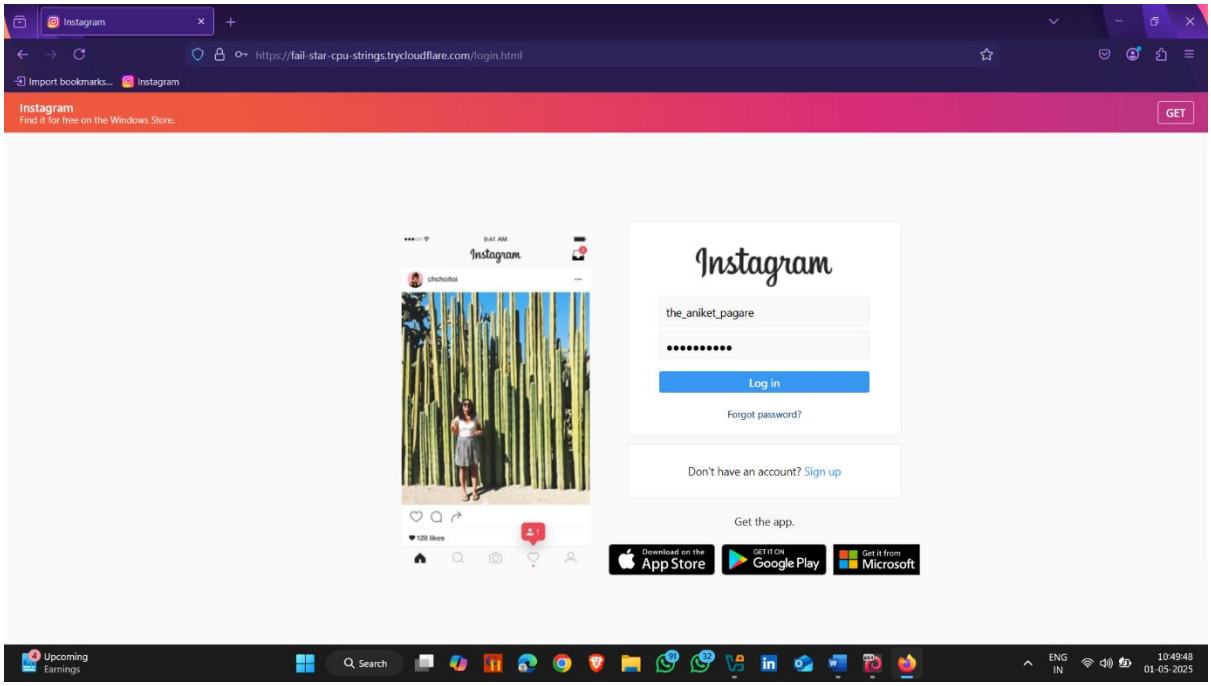
- Paste it on url section and enter



- Phishing page generate successfully

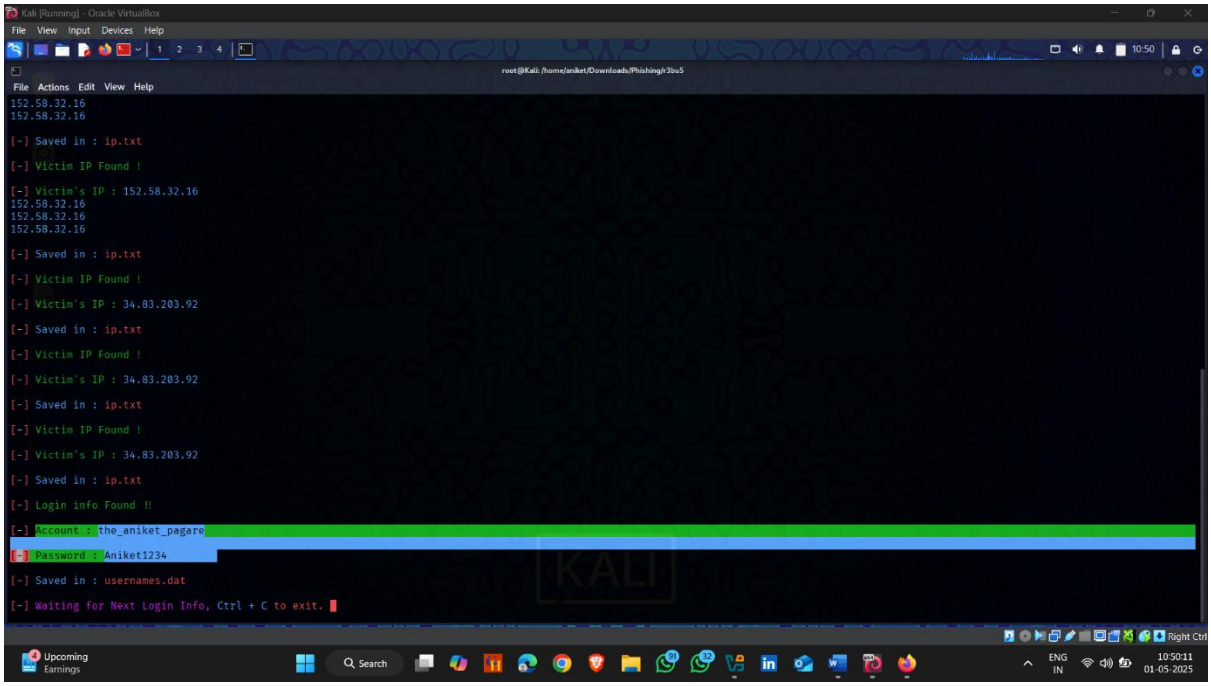


- Enter username and password



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

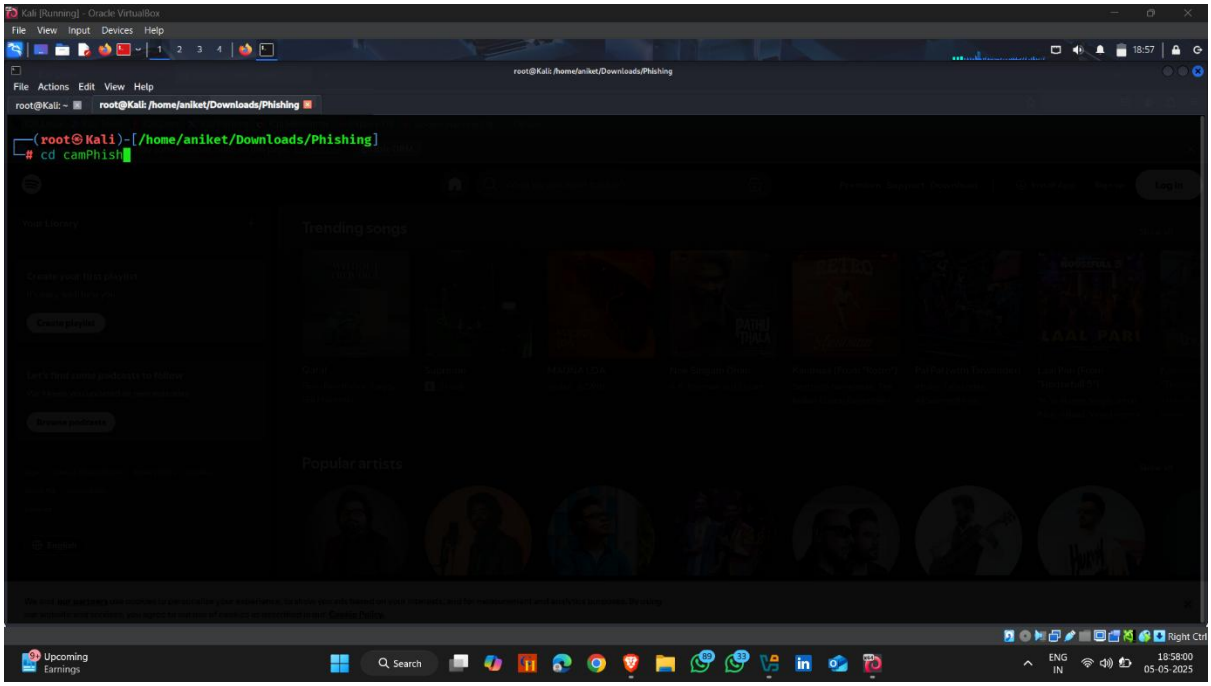
- Username and password are captured



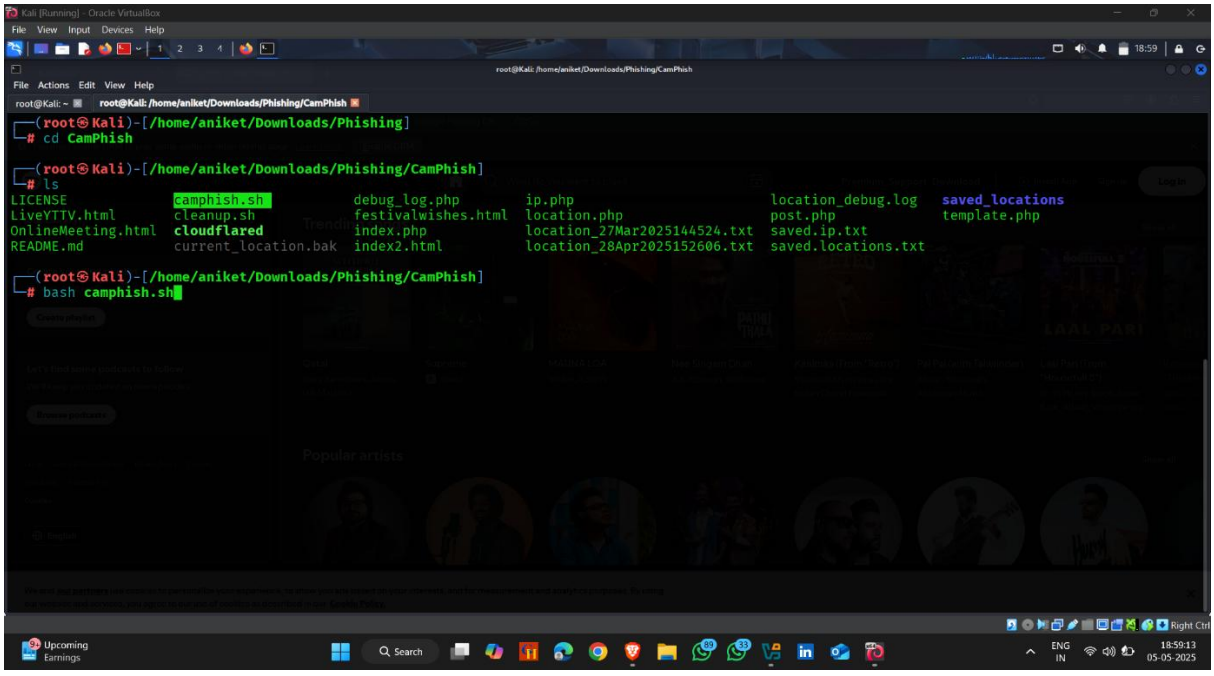
3.Perform Phishing Attack Using CamPhish Tool

How to use it -:

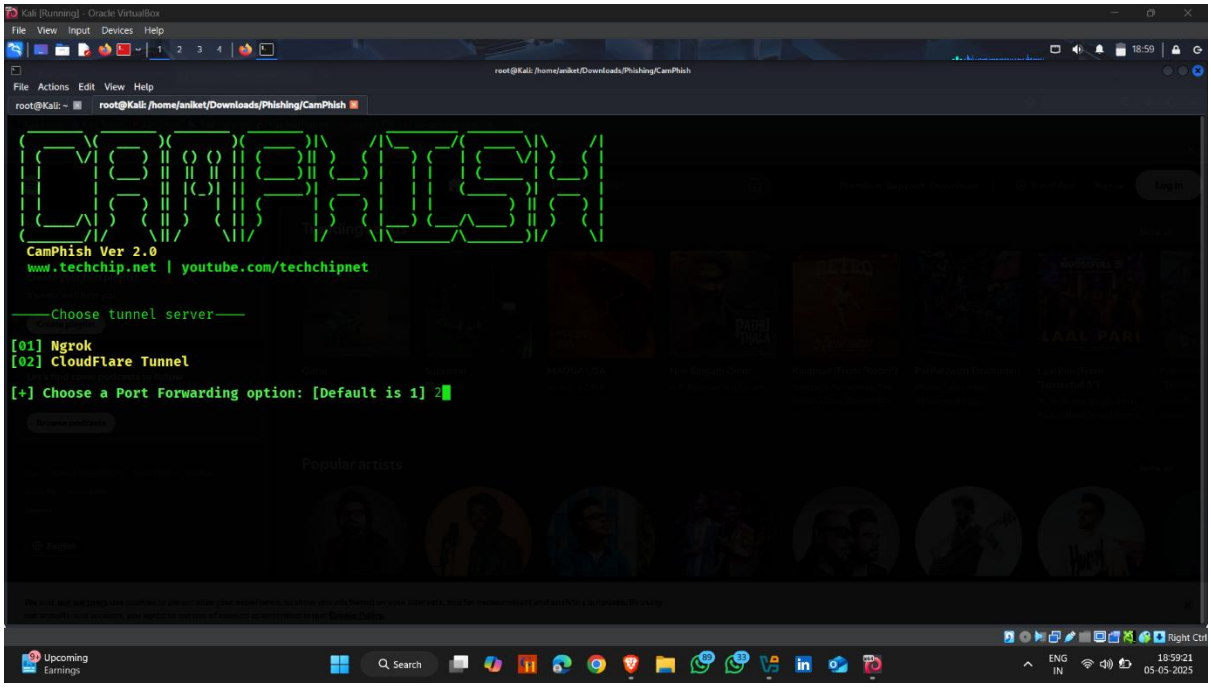
- Open kali linux terminal go to the camphish directory



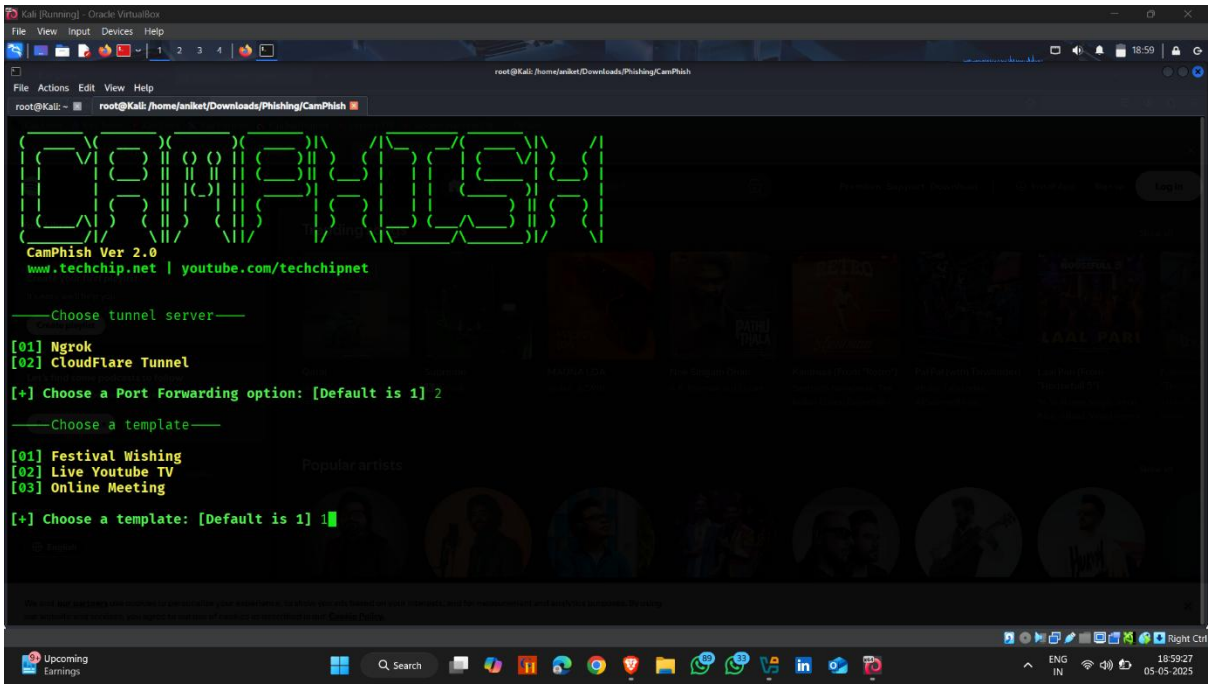
- Type command –**bash camphish**



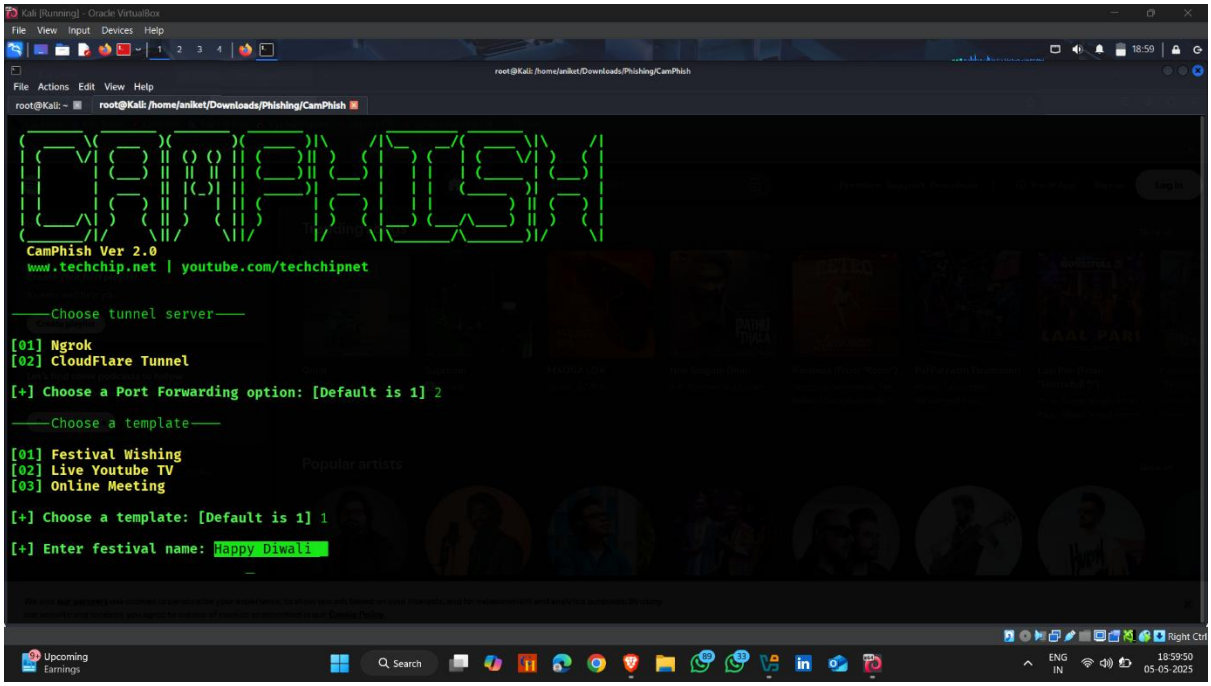
- Select Server – cloudflare tunnel



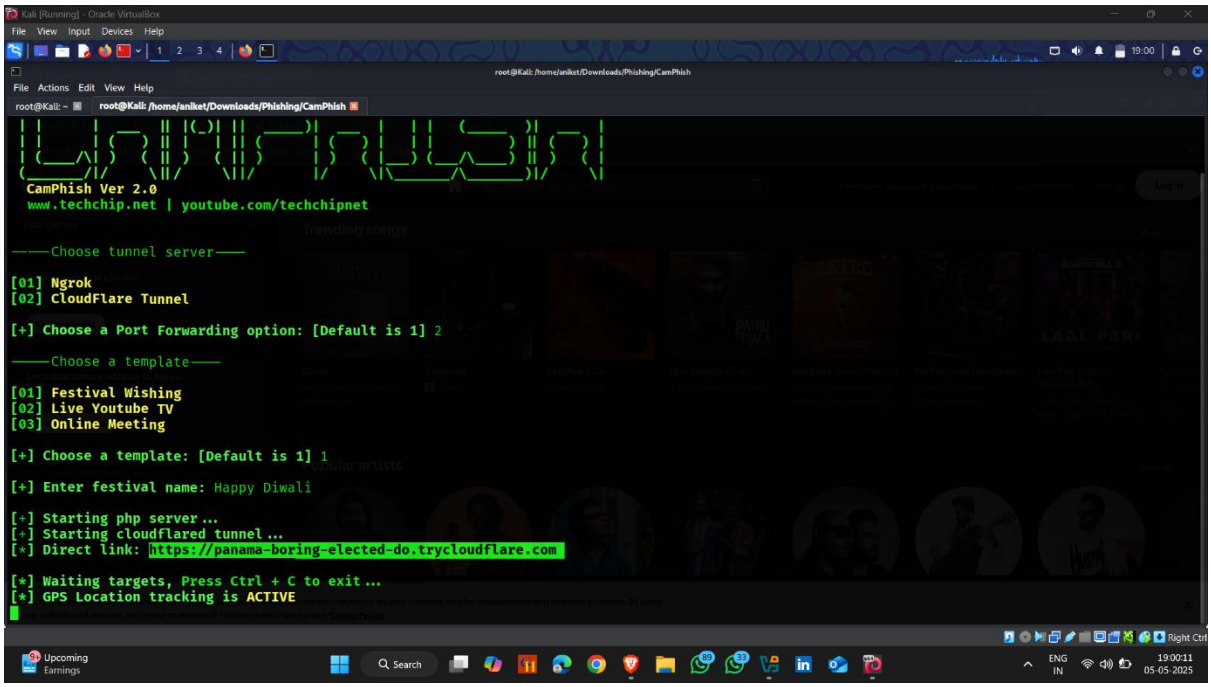
- Select 1



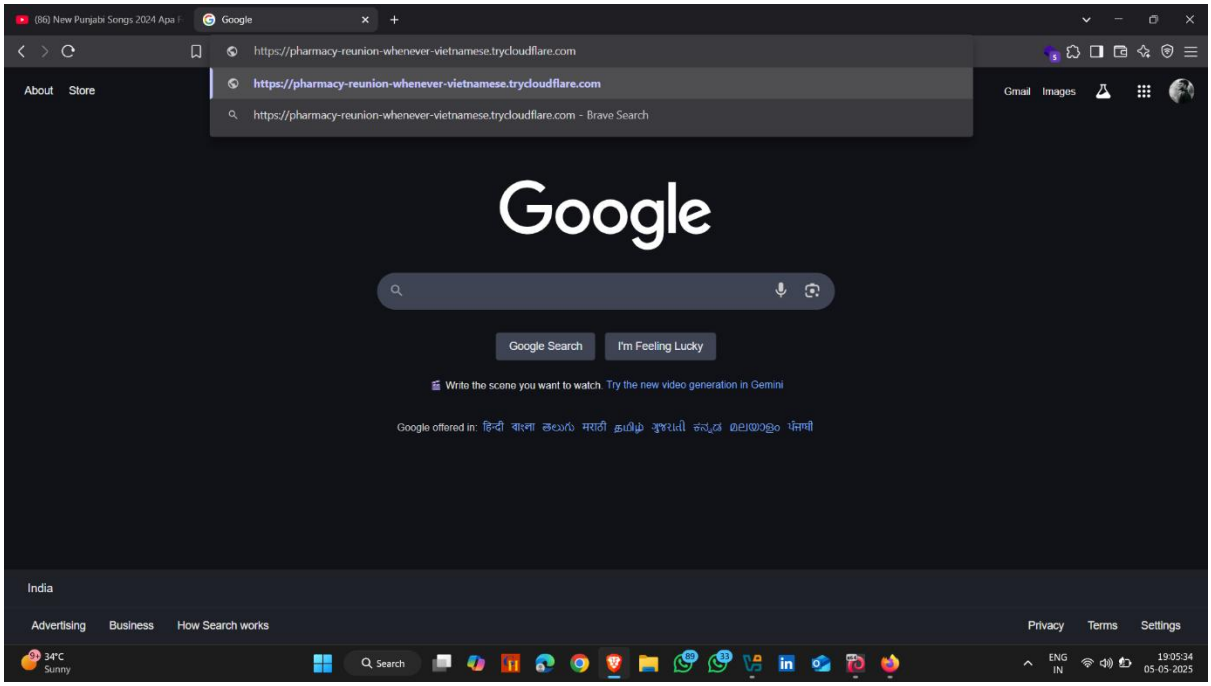
- **Enter Message**

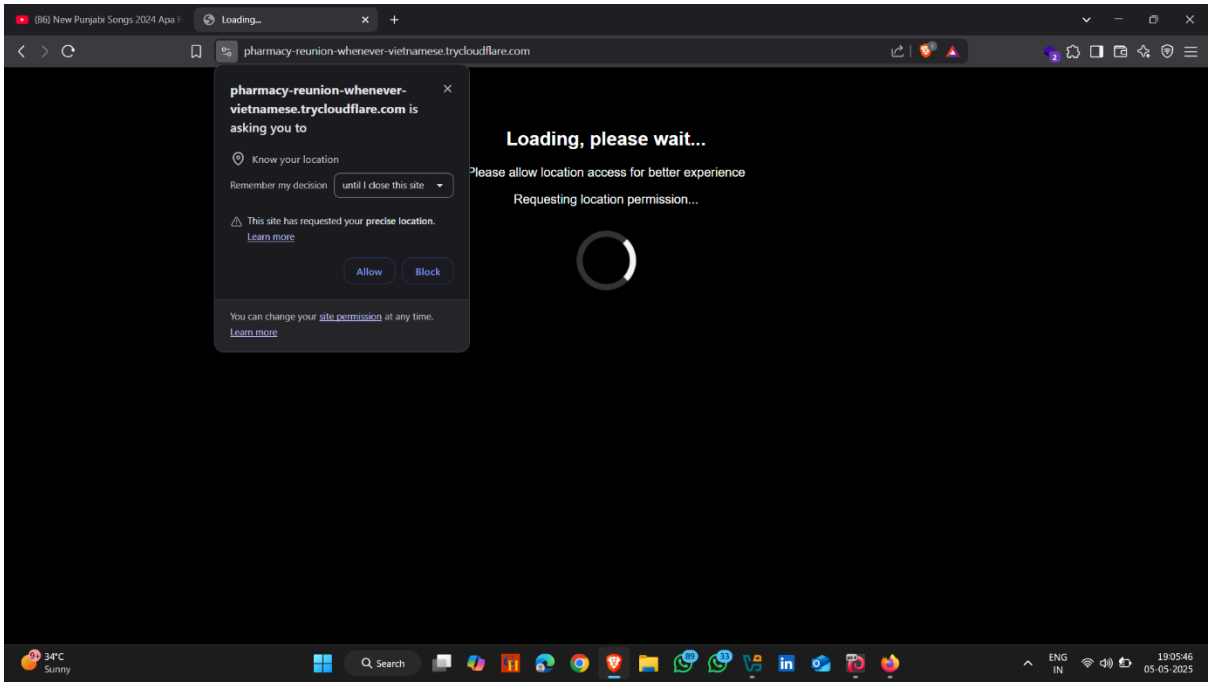


- Link Generated

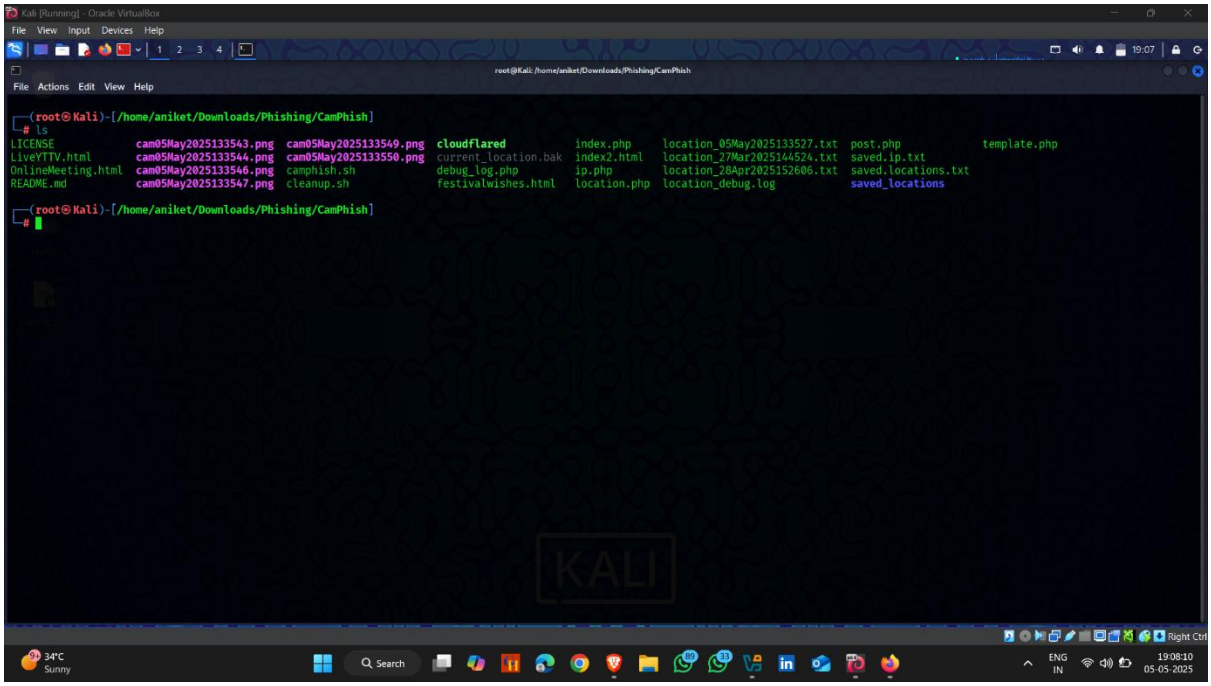


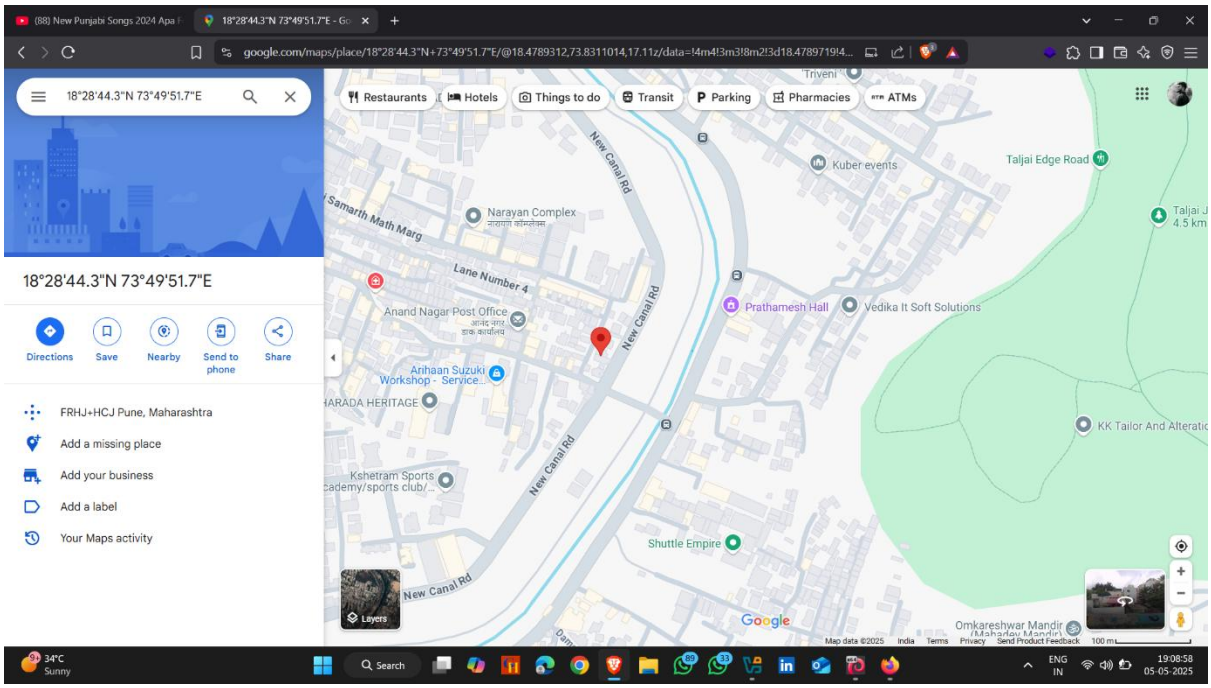
- Paste link on Browser





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

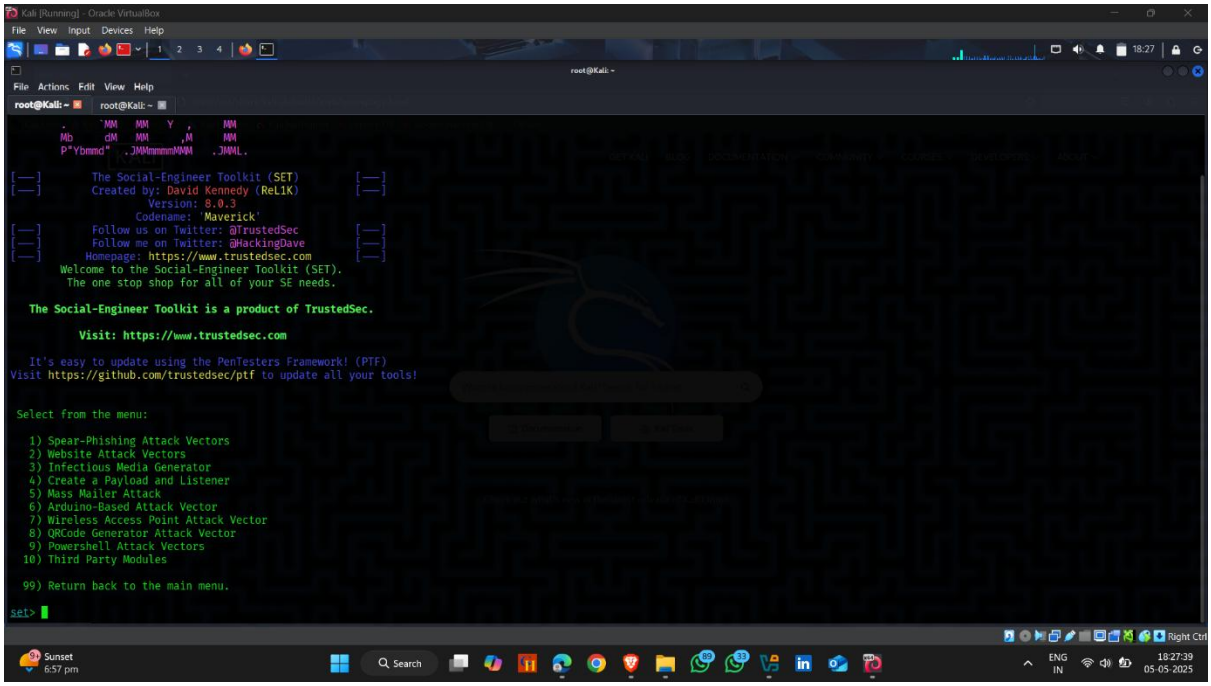

Kali [Running] - Oracle VirtualBox
File View Input Devices Help
File Actions Edit View Help
(root㉿Kali)-[/home/aniket/Downloads/Phishing/CamPhish]
ls
LICENSE cam05May2025133543.png cam05May2025133549.png cloudflared index.php location_05May2025133527.txt post.php template.php
LiveYTTV.html cam05May2025133544.png cam05May2025133550.png current_location.bak index2.html location_27Mar2025144524.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
(root㉿Kali)-[/home/aniket/Downloads/Phishing/CamPhish]
#
KALI
34°C Sunny
Search
ENG IN
19:08:10 05-05-2025


18°28'44.3"N 73°49'51.7"E
Directions
Save
Nearby
Send to phone
Share
FRHJ+HCJ Pune, Maharashtra
Add a missing place
Add your business
Add a label
Your Maps activity
Restaurants
Hotels
Things to do
Transit
Parking
Pharmacies
ATMs
Kuber events
Taljai Edge Road
Narayan Complex
Lane Number 4
Anand Nagar Post Office
Prathamesh Hall
Vedika It Soft Solutions
Arihaan Suzuki Workshop - Service...
KK Tailor And Alteratio
Shuttle Empire
New Canal Rd
Layers
Google
34°C Sunny
Search
ENG IN
19:08:58 05-05-2025

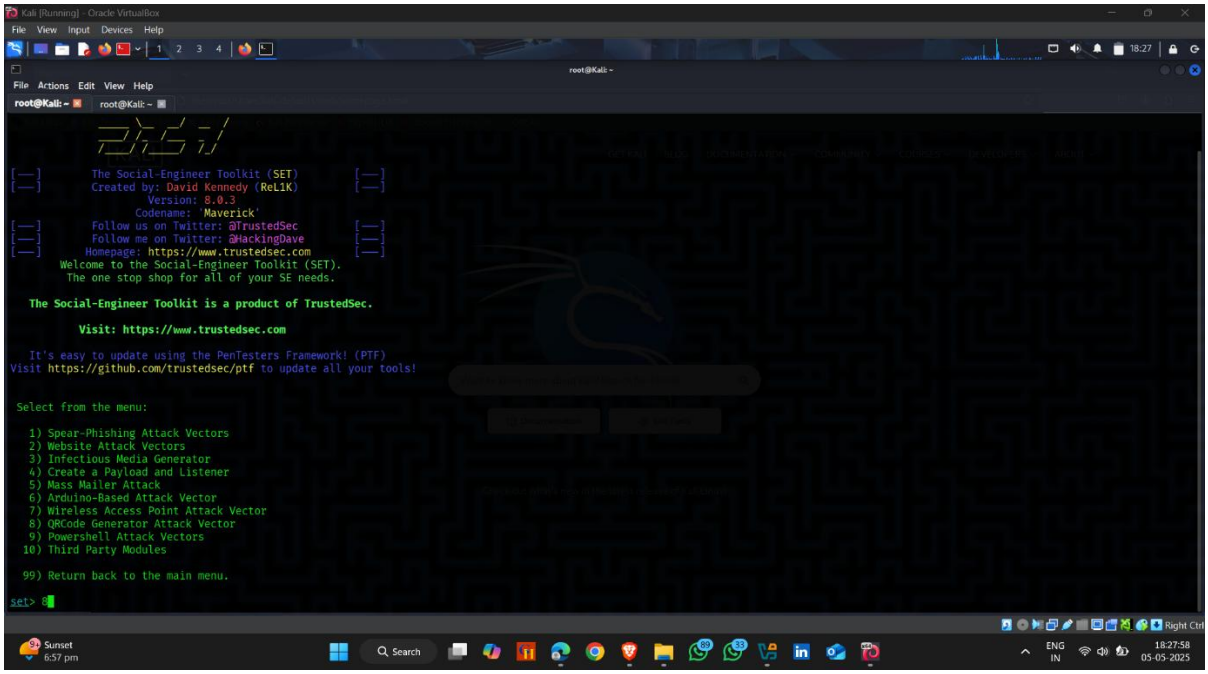
4.Perform QRCODE Generate Using SETOOLKIT

How to do it -:

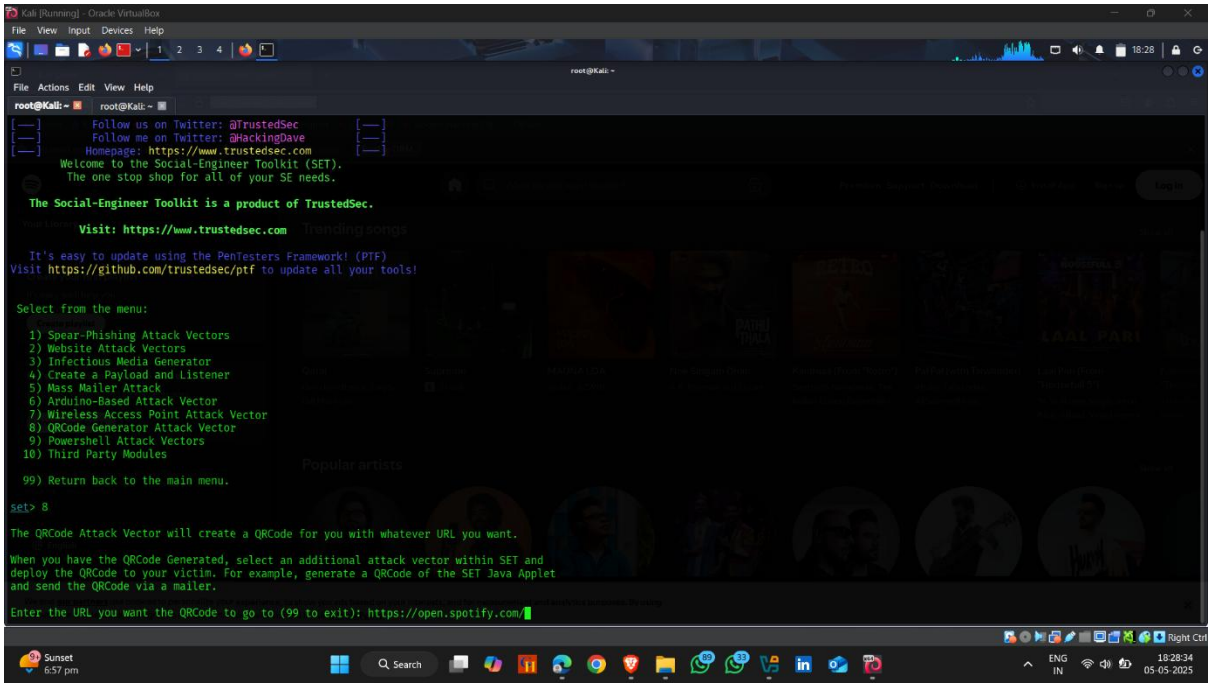
- Open kali linux terminal and type **setoolkit**



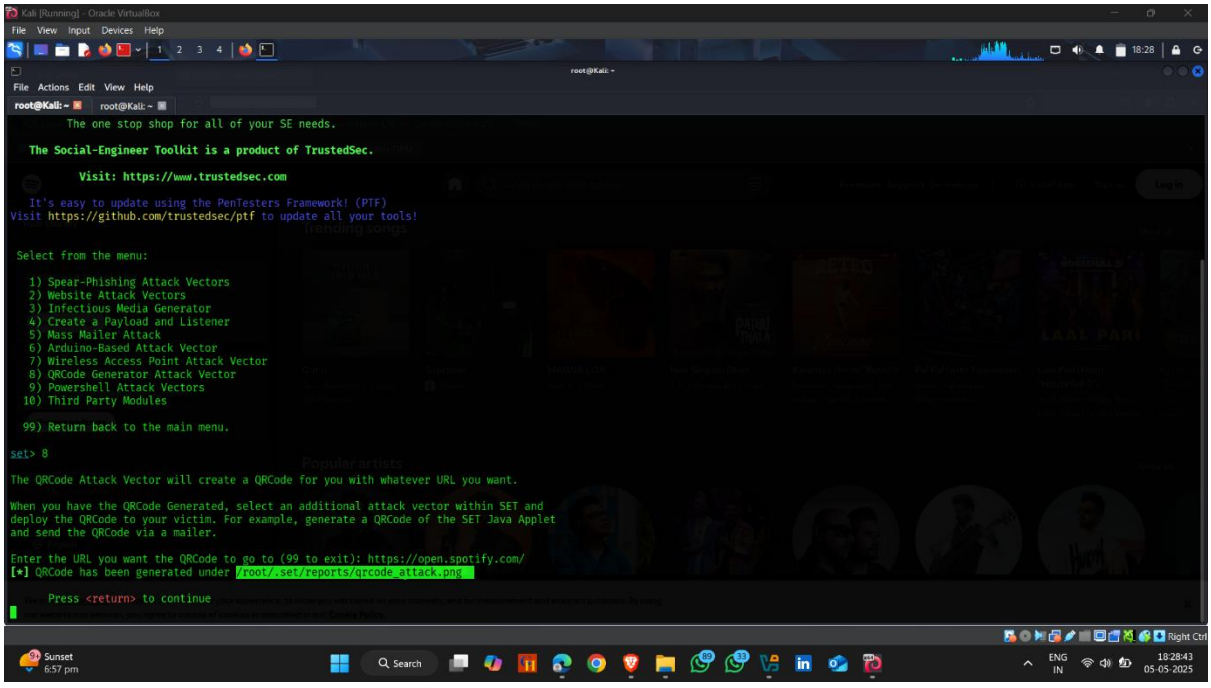
- And Select option **8 - QRcode Generator Attack Vector**



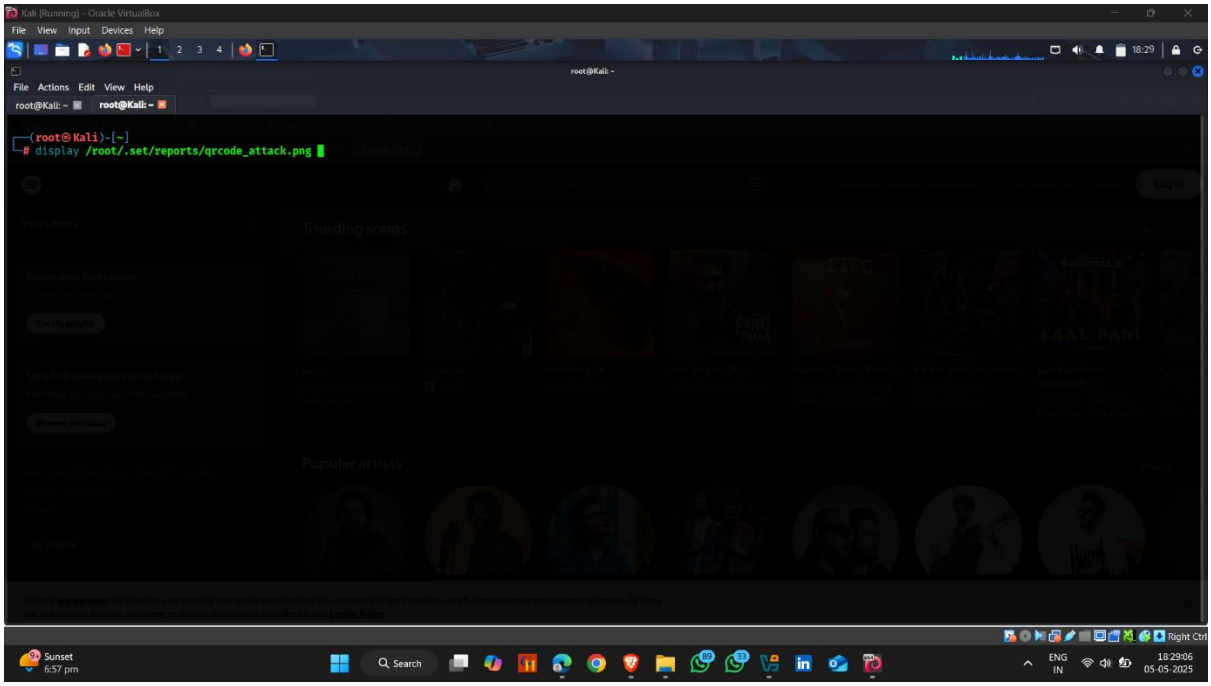
- Now paste url that you want to generate a qrcode

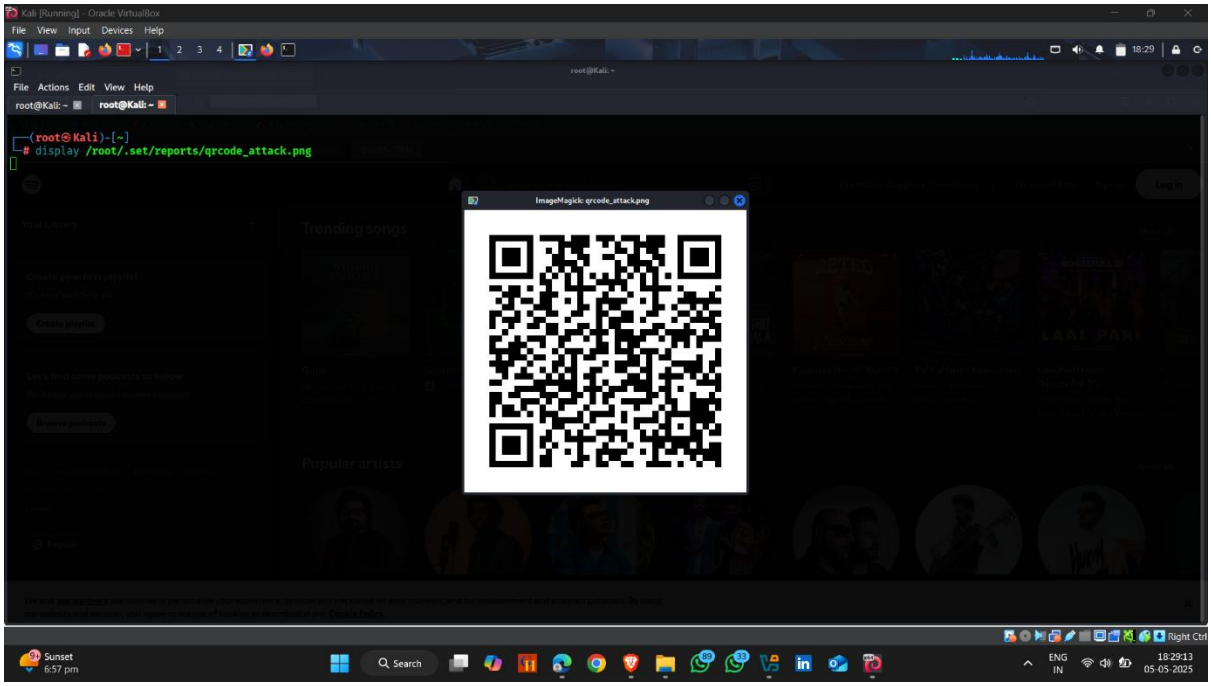


- Here , qrcode generated successfully and copy it and paste it on another terminal



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





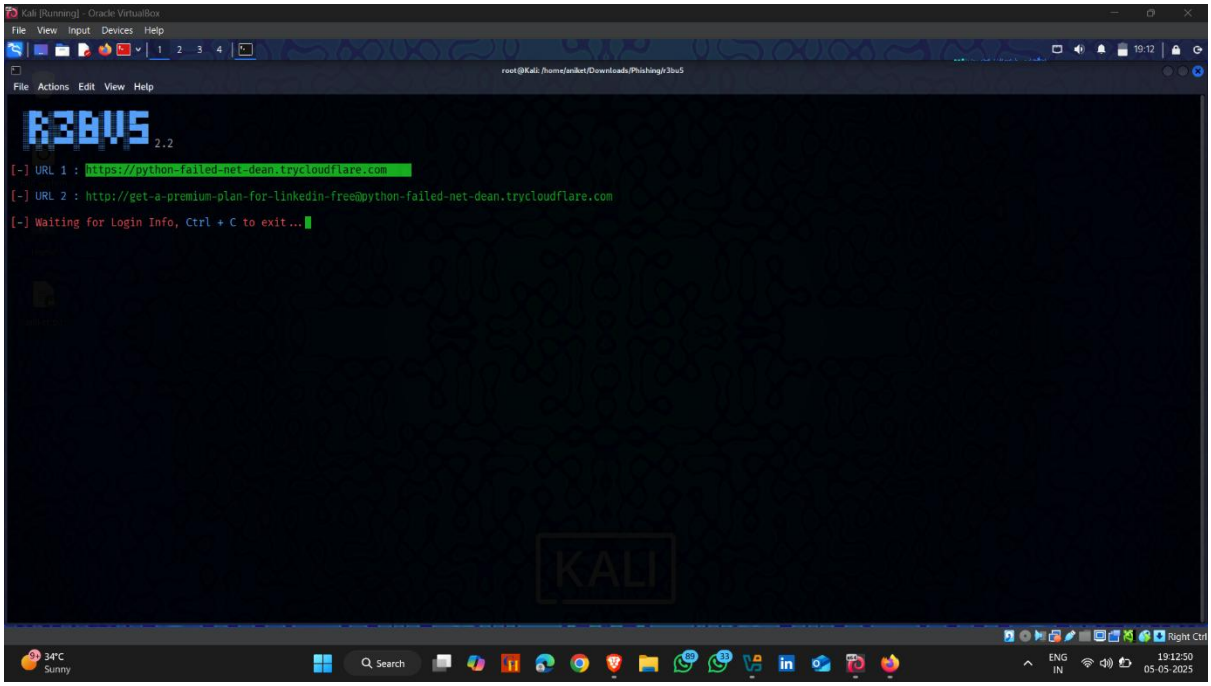
- Here spotify qrcode generated

5.Perform Phishing QRCODE Generate Using SETOOLKIT

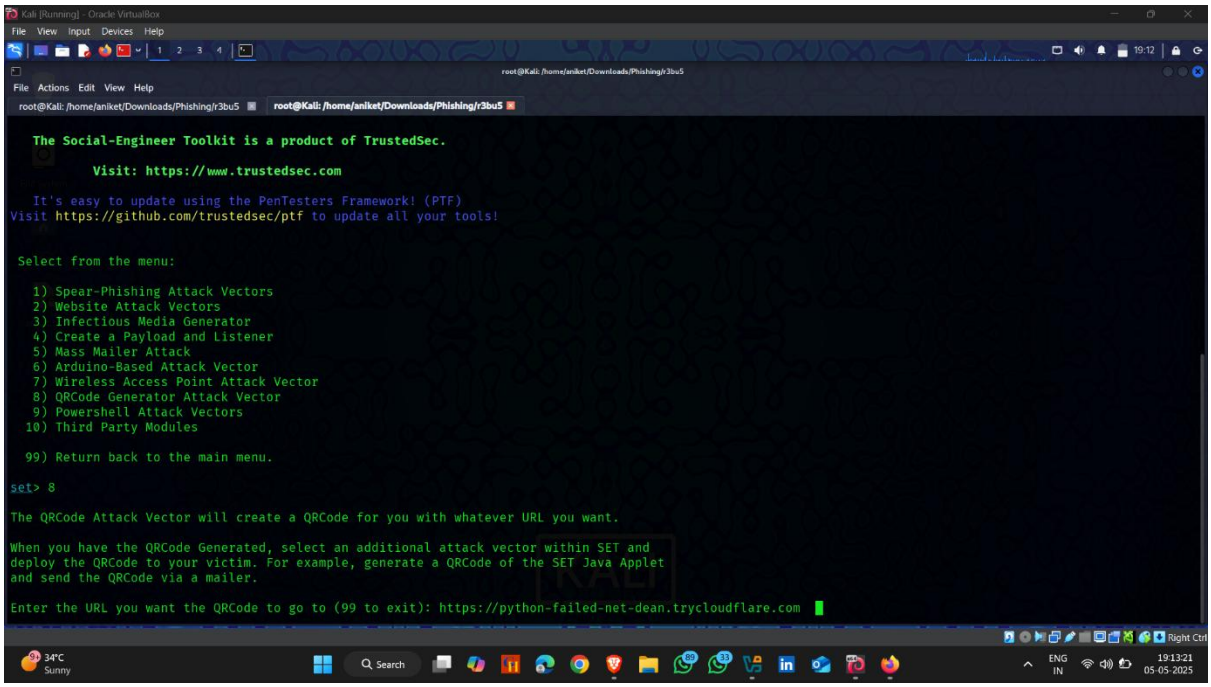
How to use it -:

- Open kali linux terminal and generate a phishing link

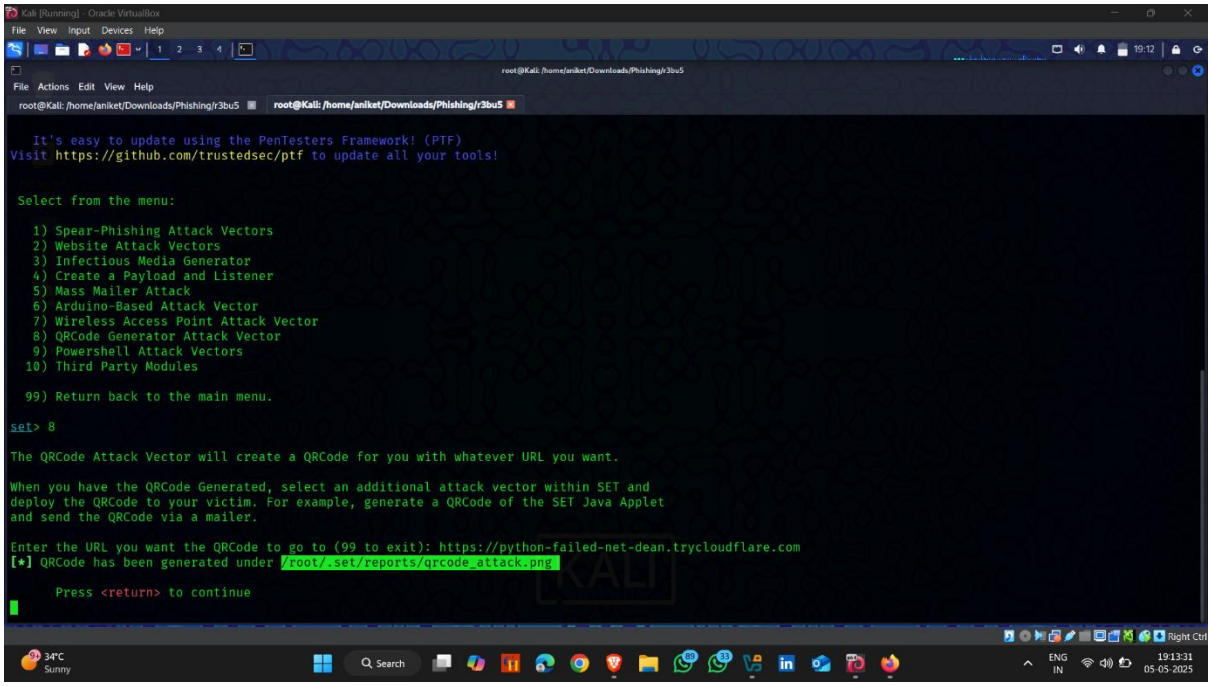
- Phishing link generated



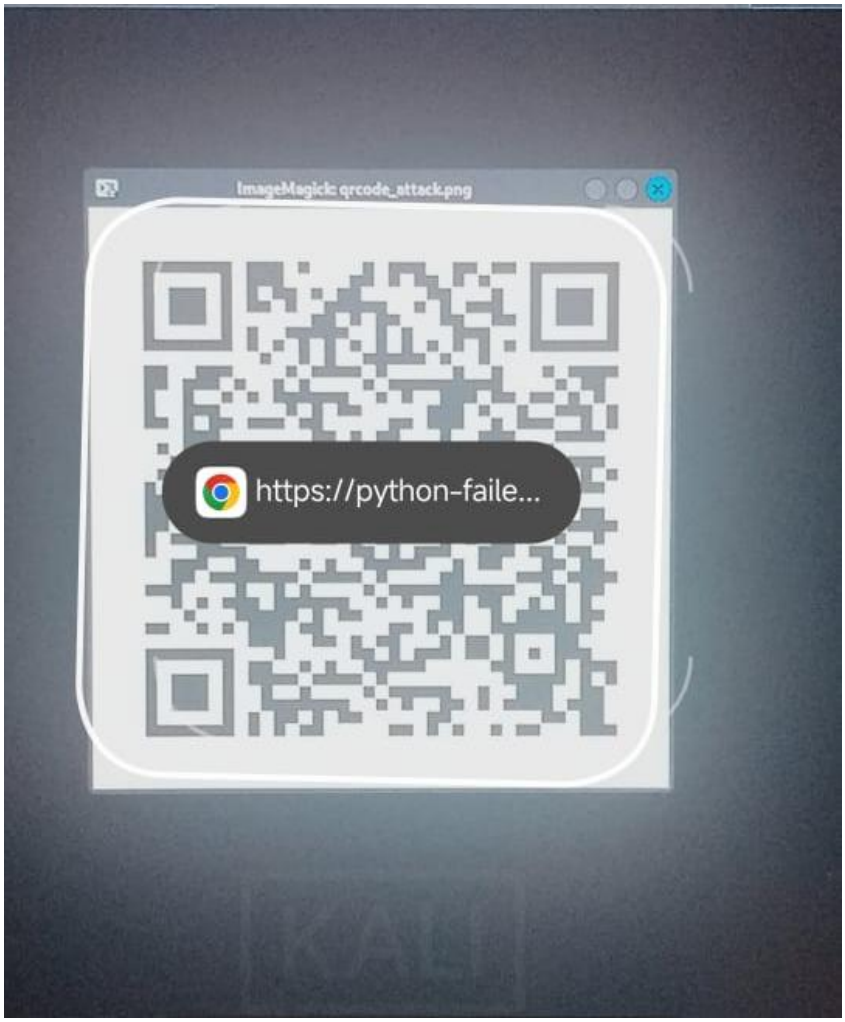
- Now open SETOOLKIT , select qrcode generator option and paste phishing link



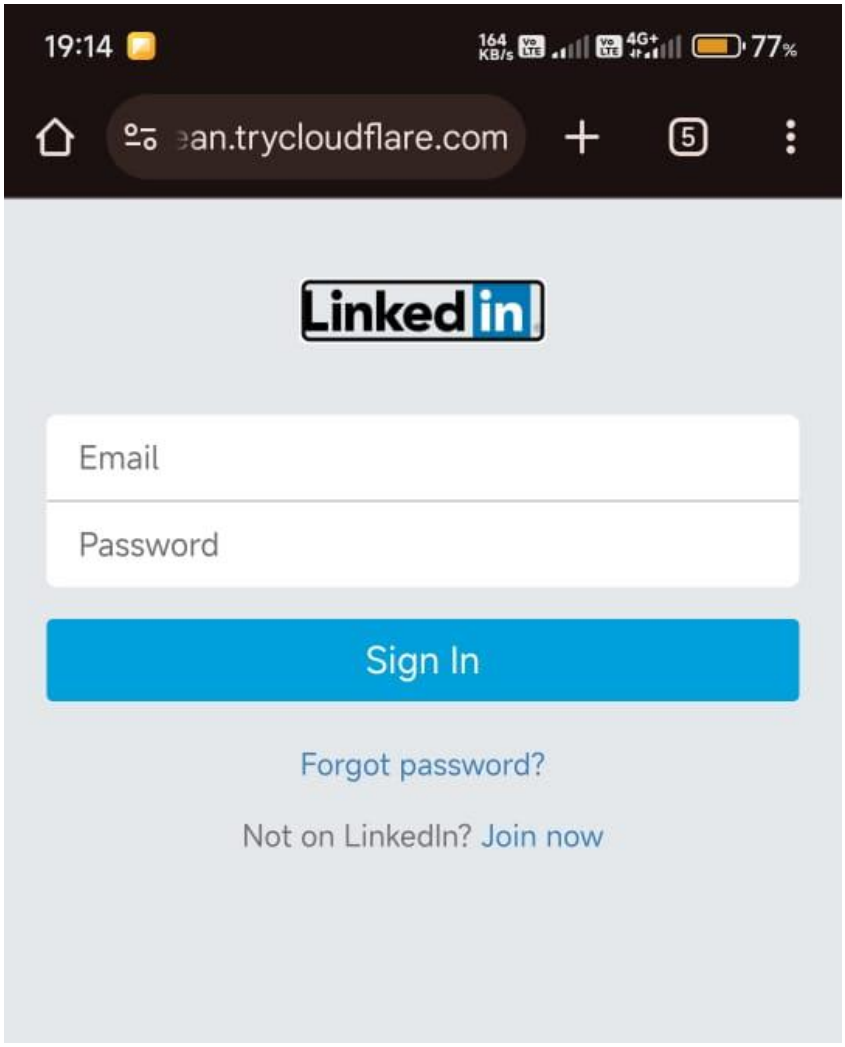
- Qrcode generated successfully



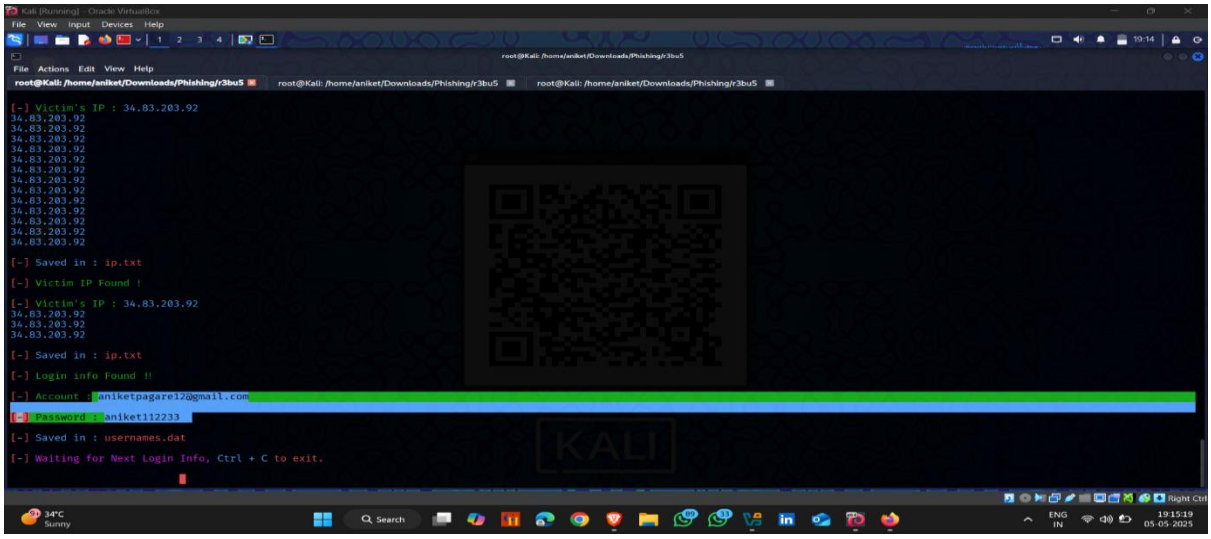
- Phishing QRcode 👇



- Type credentials



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

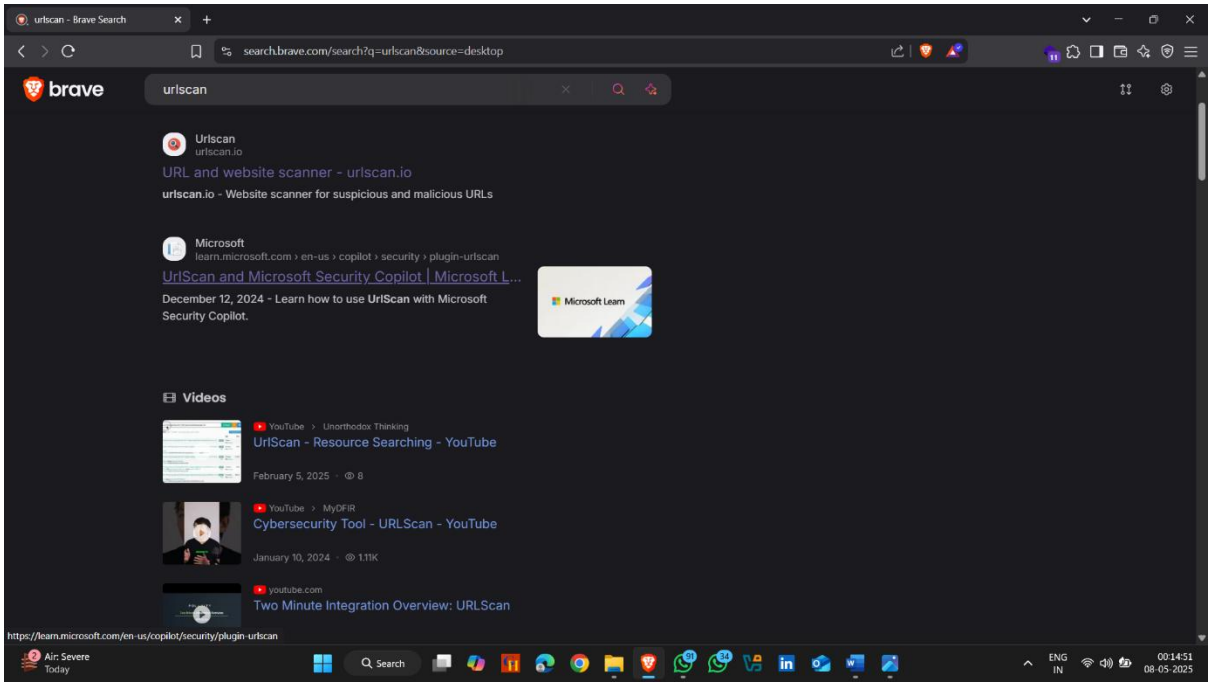


PHISHING DETECTION TOOLS

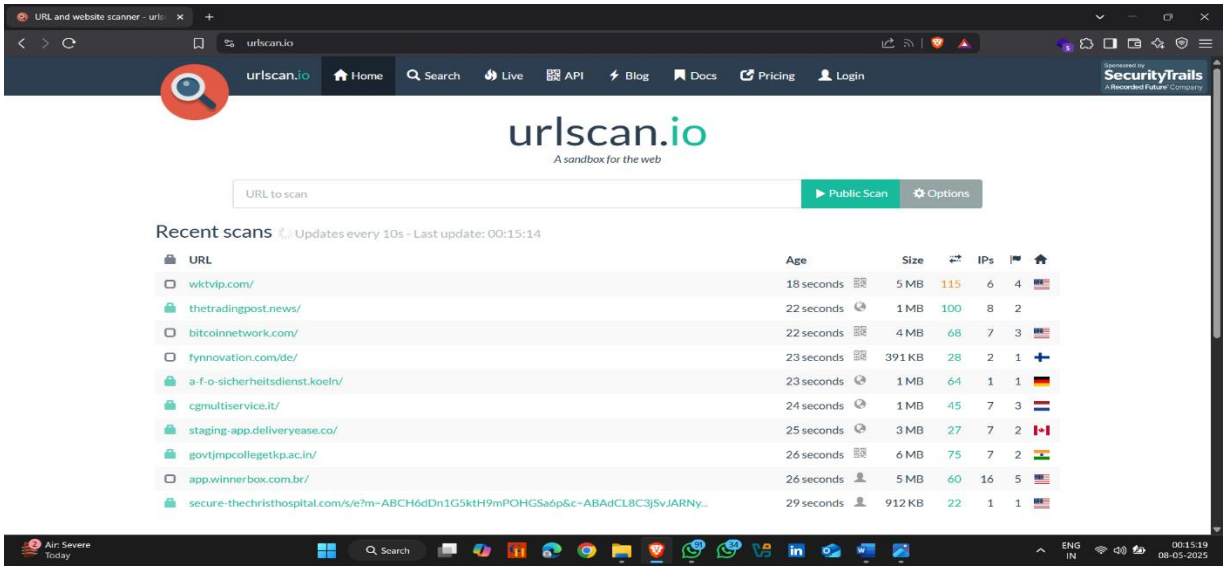
1.Perform Phishing Detection Using URLScan Website

How to use it -:

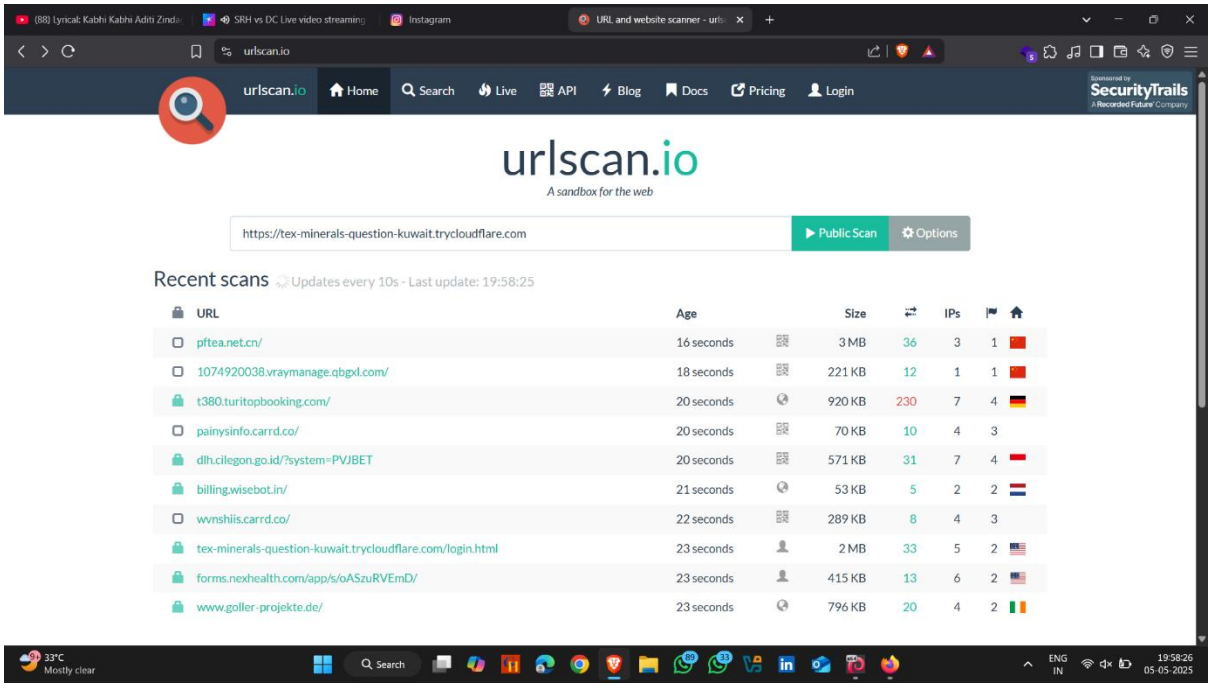
- Click on urlscan.io website



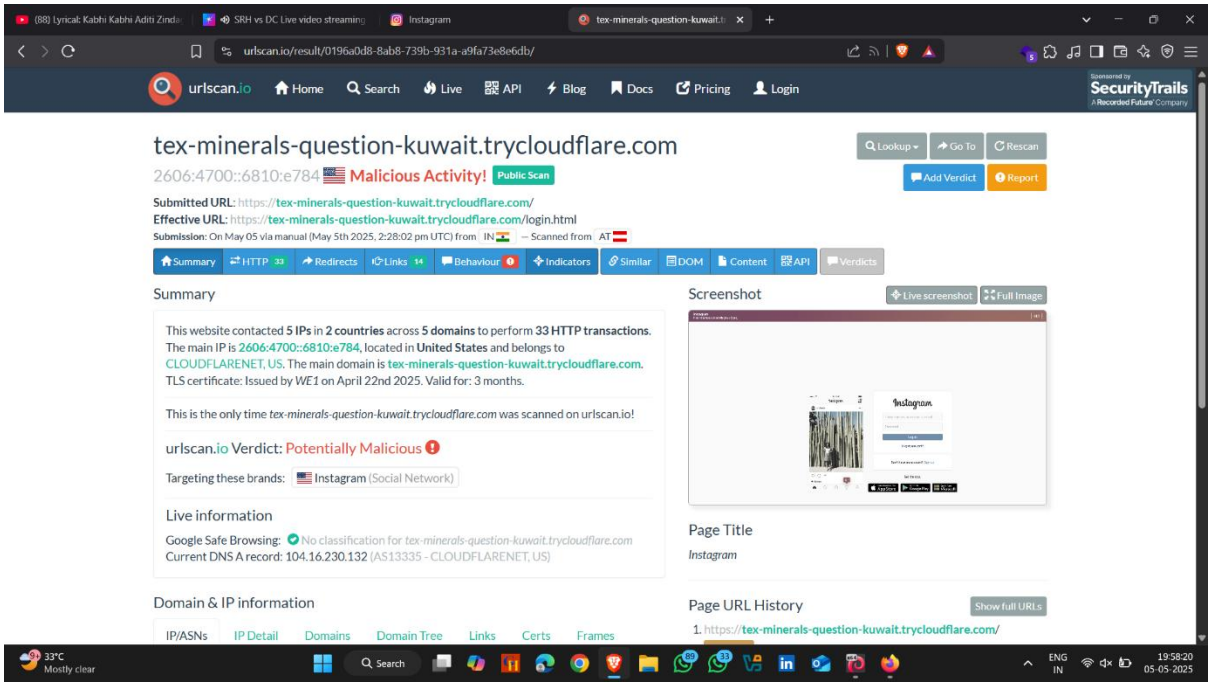
- Paste Phishing Link



- Click on **Public Scan**



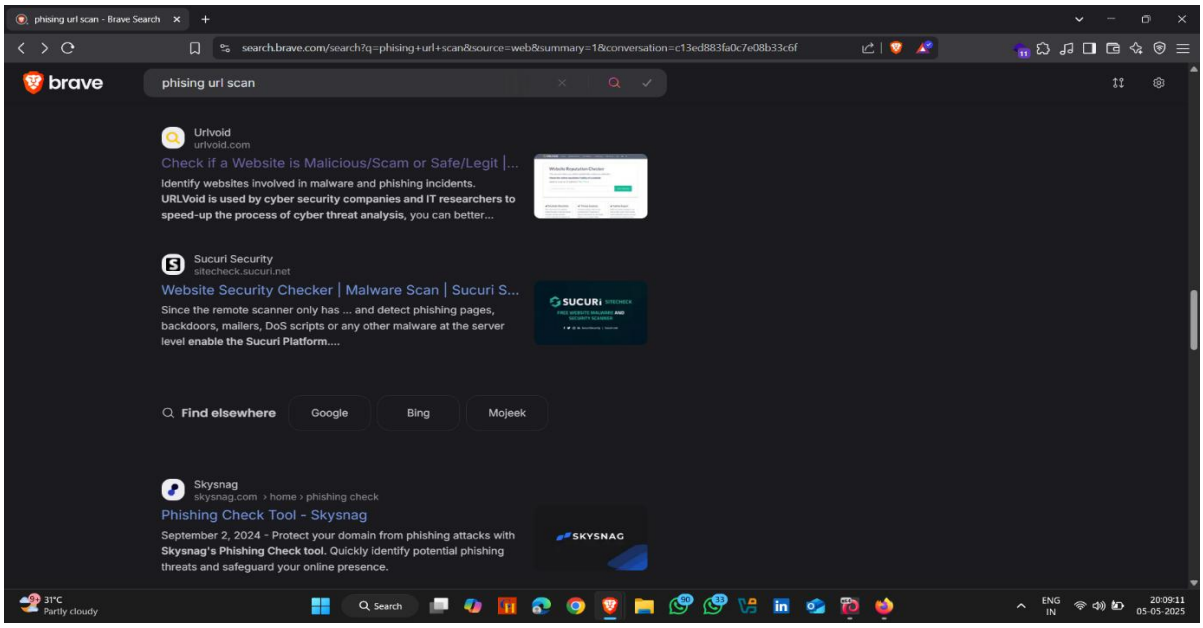
- **Phishing Detected** 👇



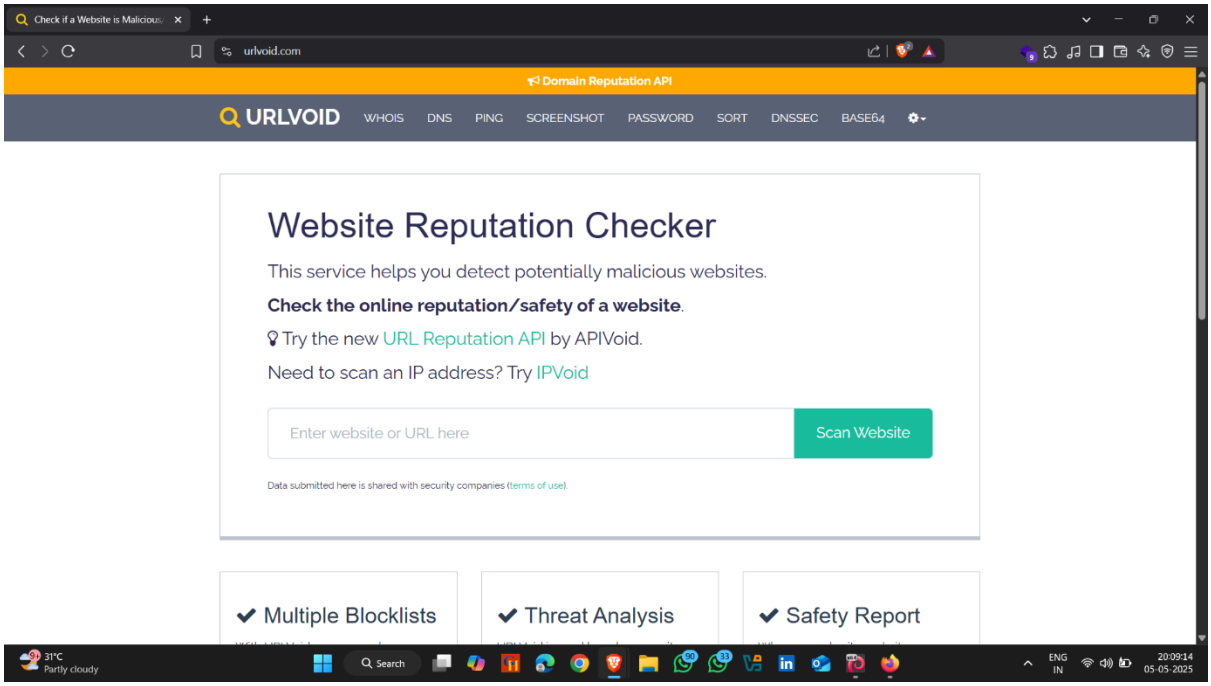
2.Perform Phishing Detection Using UrlVoid Website

How to use it -:

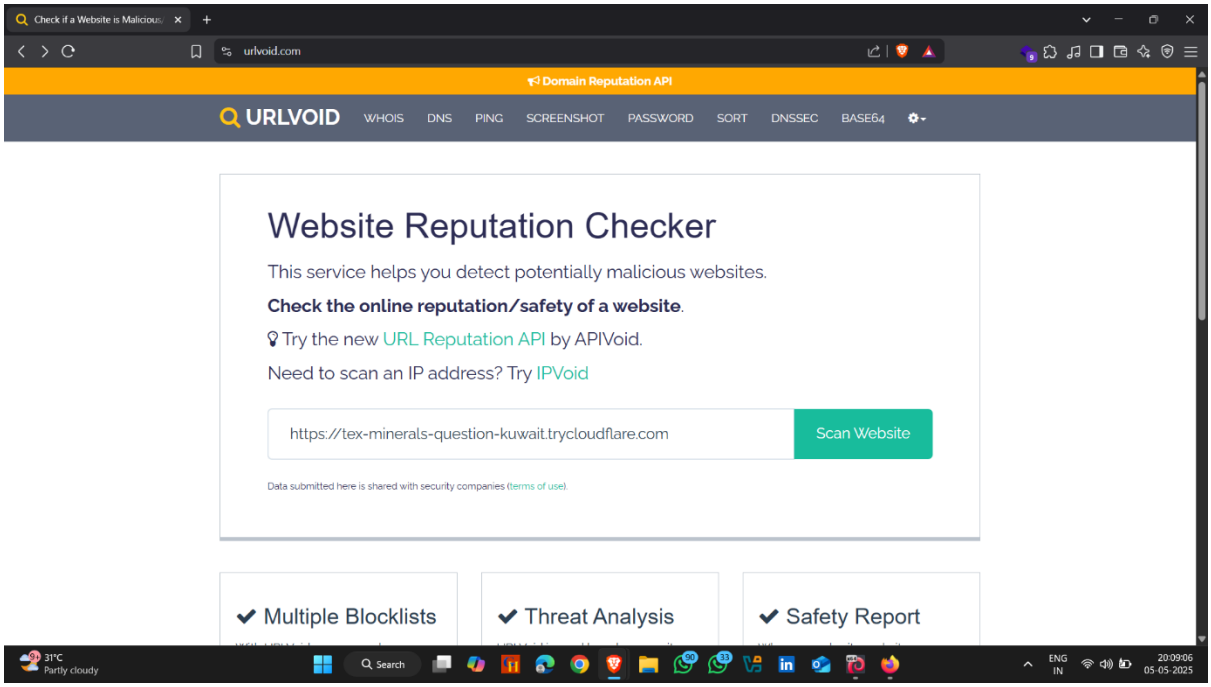
- Open Browser And Search Phishing Url scan Click on Urlvoid Website



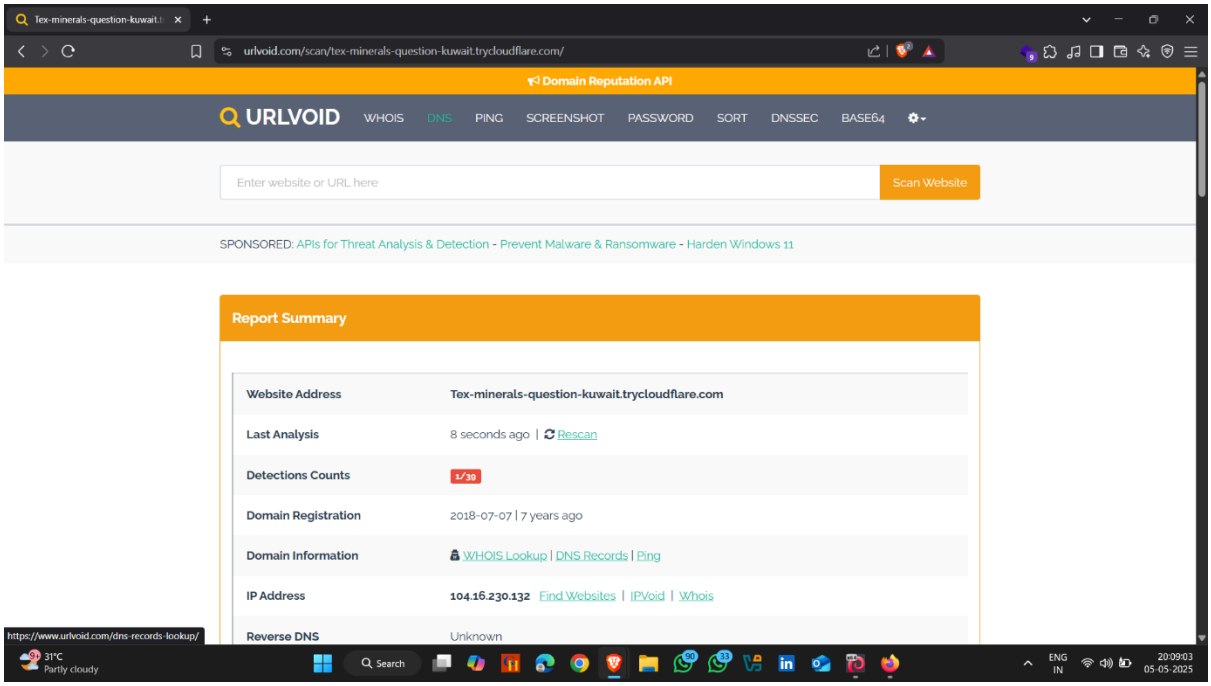
- Paste phishing website



- Click on Scan Website



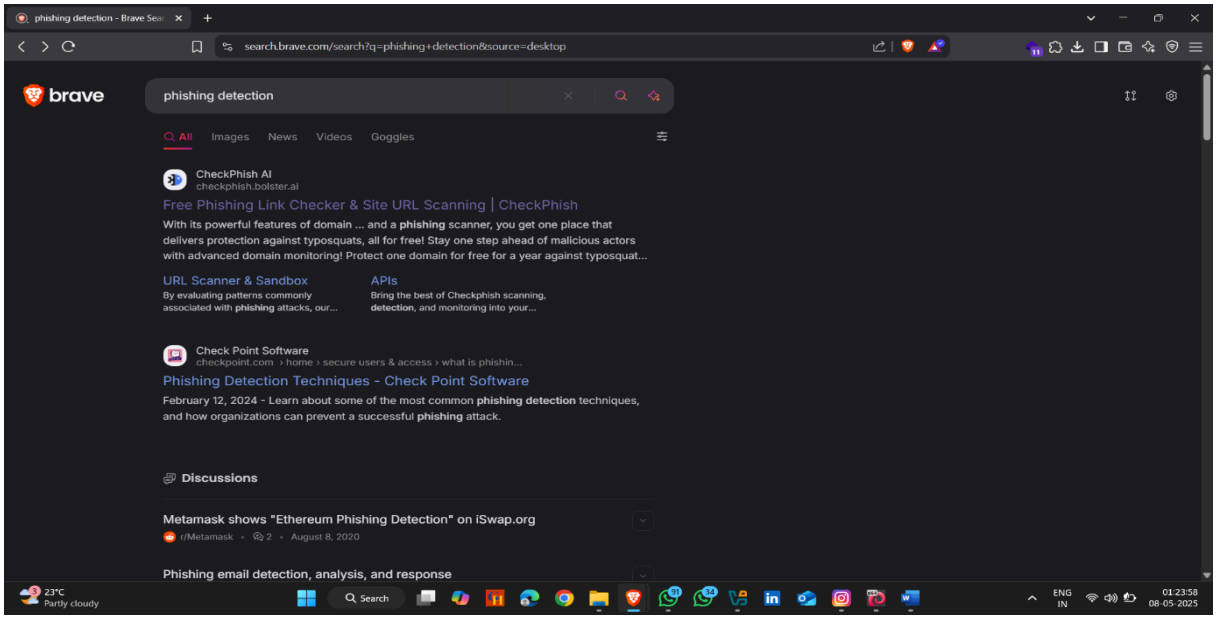
- Phishing Detected 👇



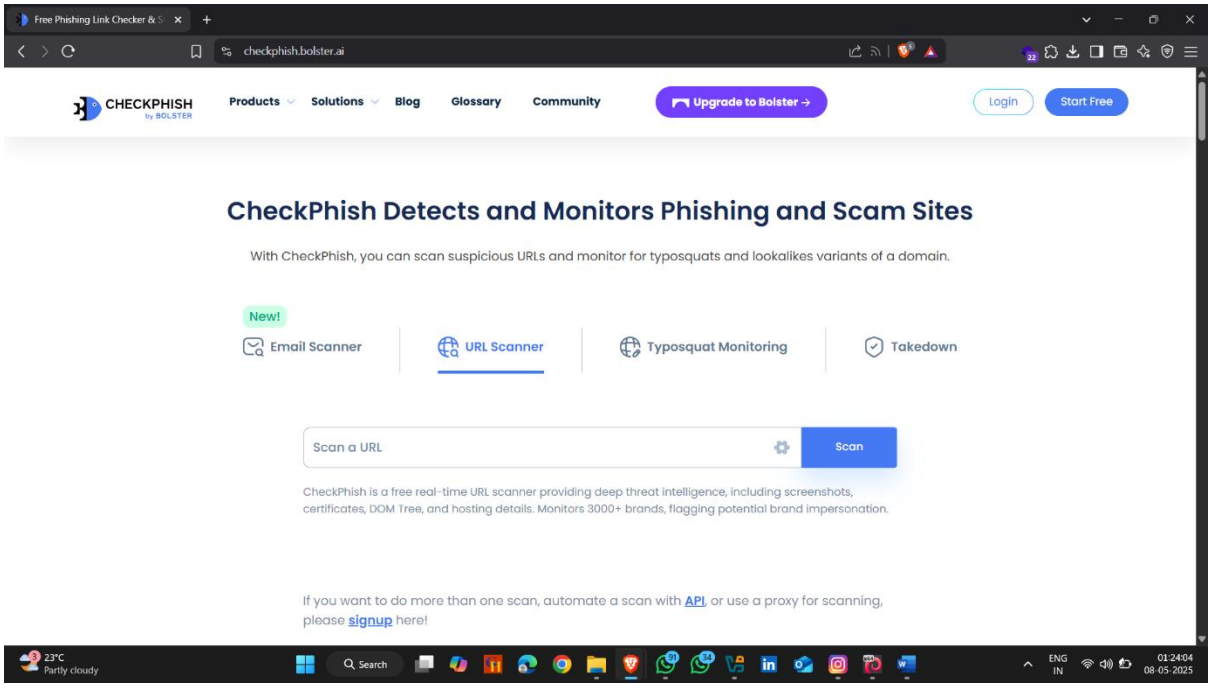
3.Perform Phishing Detection Using Checkphish Website

How to use it -:

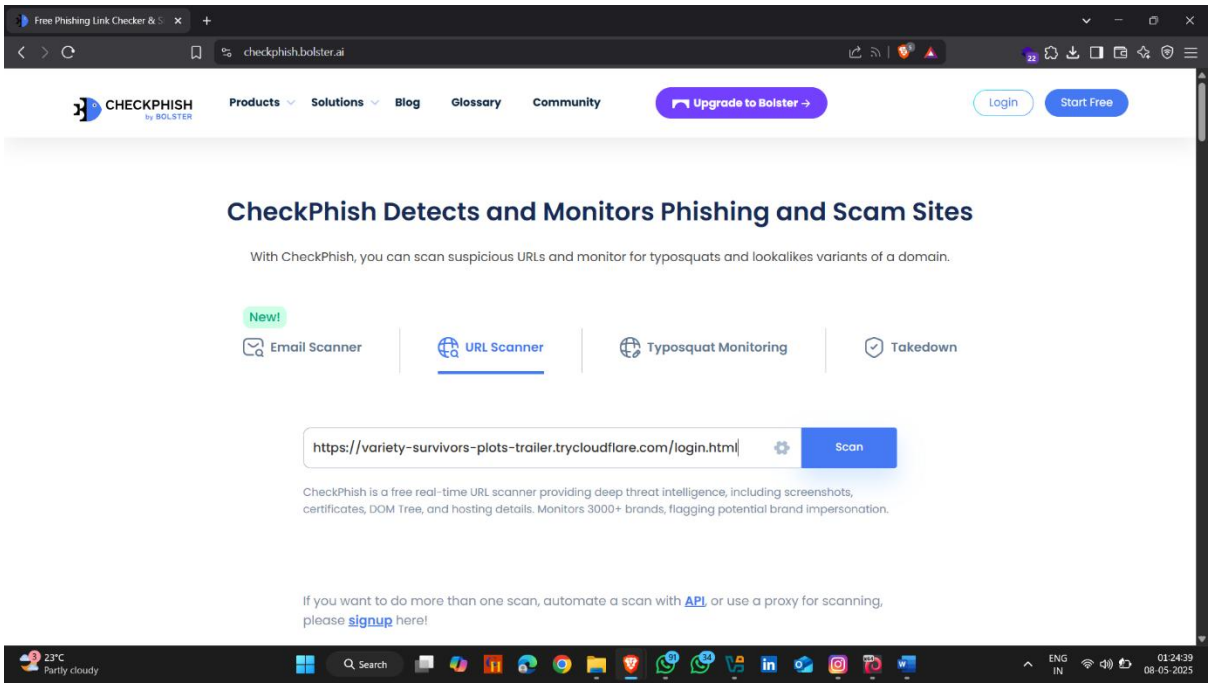
- Open Browser and search Phishing detection
- Click on checkphish website



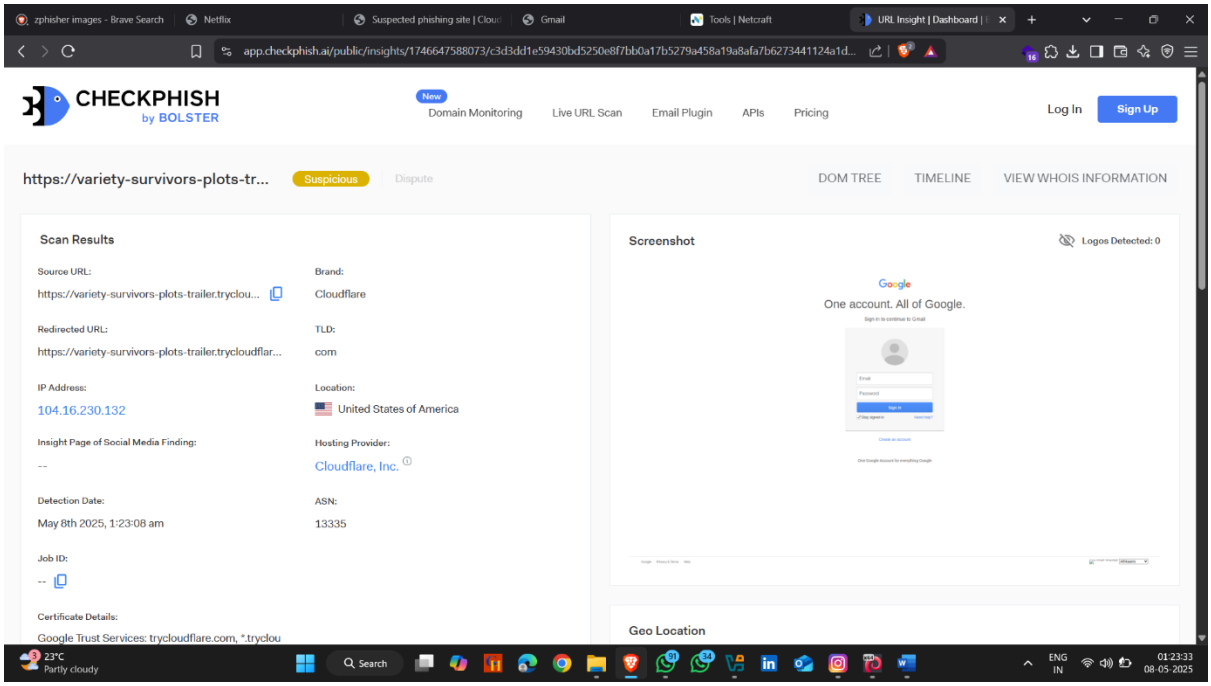
- Paste Phishing Url



- Click on Scan



- Phishing Detected 👇


zphisher images - Brave Search
Netflix
Suspected phishing site | Cloud
Gmail
Tools | Netcraft
URL Insight | Dashboard |
app.checkphish.ai/public/insights/1746647588073/c3d3dd1e59430bd5250e8f7bb0a17b5279a458a19a8afa7b6273441124a1d...
CHECKPHISH
by BOLSTER
New
Domain Monitoring
Live URL Scan
Email Plugin
APIs
Pricing
Log In
Sign Up
https://variety-survivors-plots-tr...
Suspicious
Dispute
DOM TREE
TIMELINE
VIEW WHOIS INFORMATION
Scan Results
Source URL:
https://variety-survivors-plots-trailer.tryclou...
Brand:
Cloudflare
Redirected URL:
https://variety-survivors-plots-trailer.trycloudflar...
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, *.tryclou
Screenshot
Logos Detected: 0
Google
One account. All of Google.
Geo Location
23°C
Partly cloudy
Search
ENG
IN
01:23:33
08-05-2025

THANK YOU