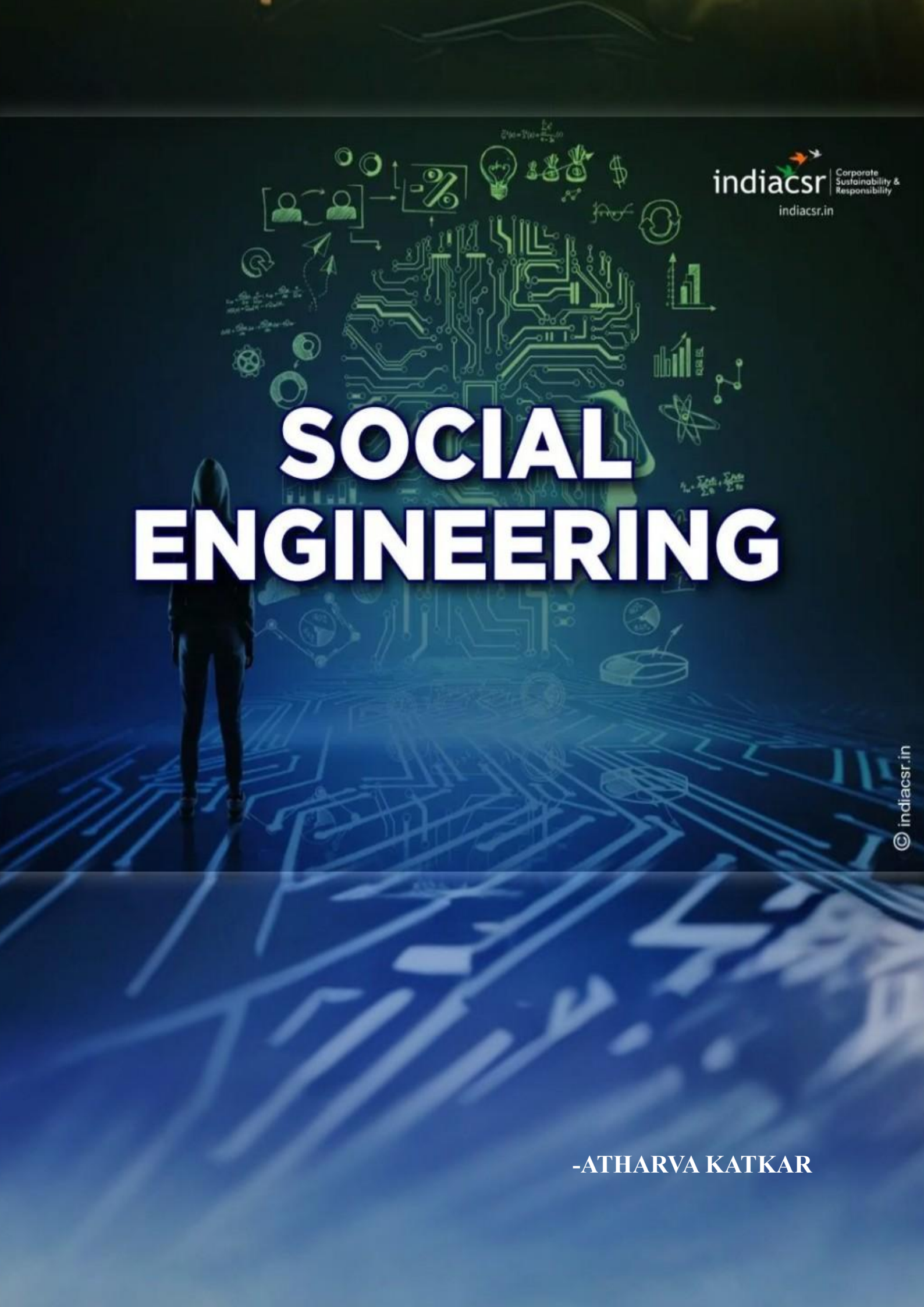

-ATHARVA KATKAR

TABLE OF CONTENTS

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

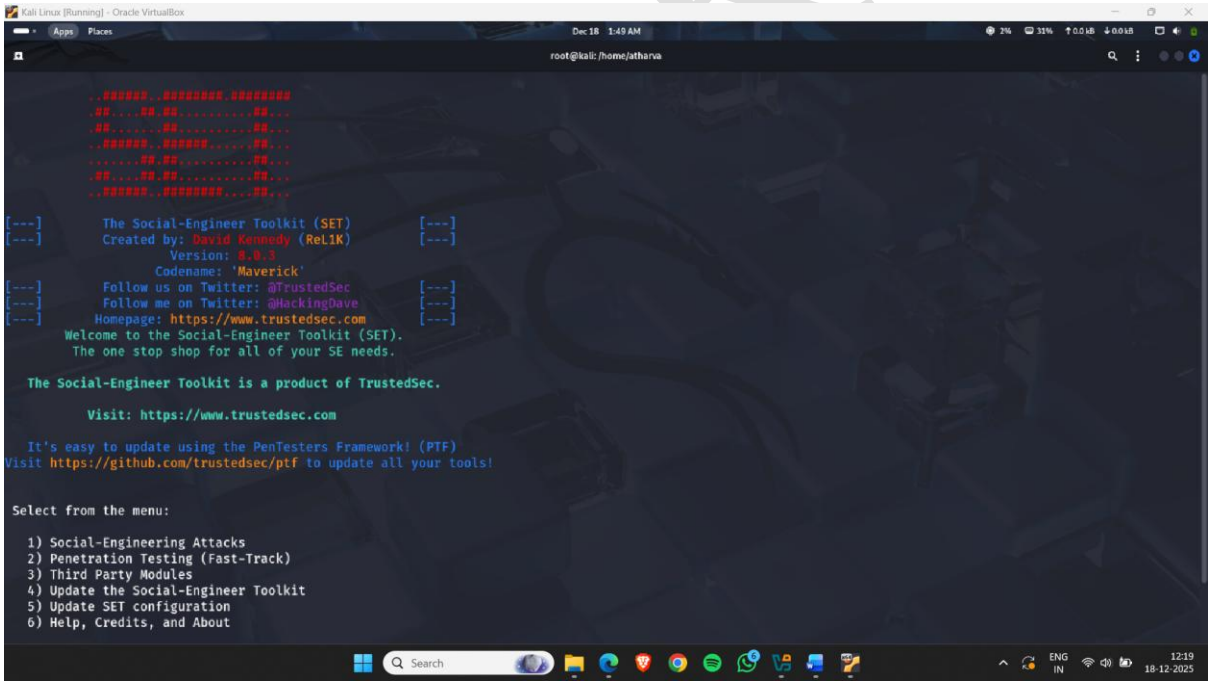

Figure 1

- Now select 2 – Website attack Vector

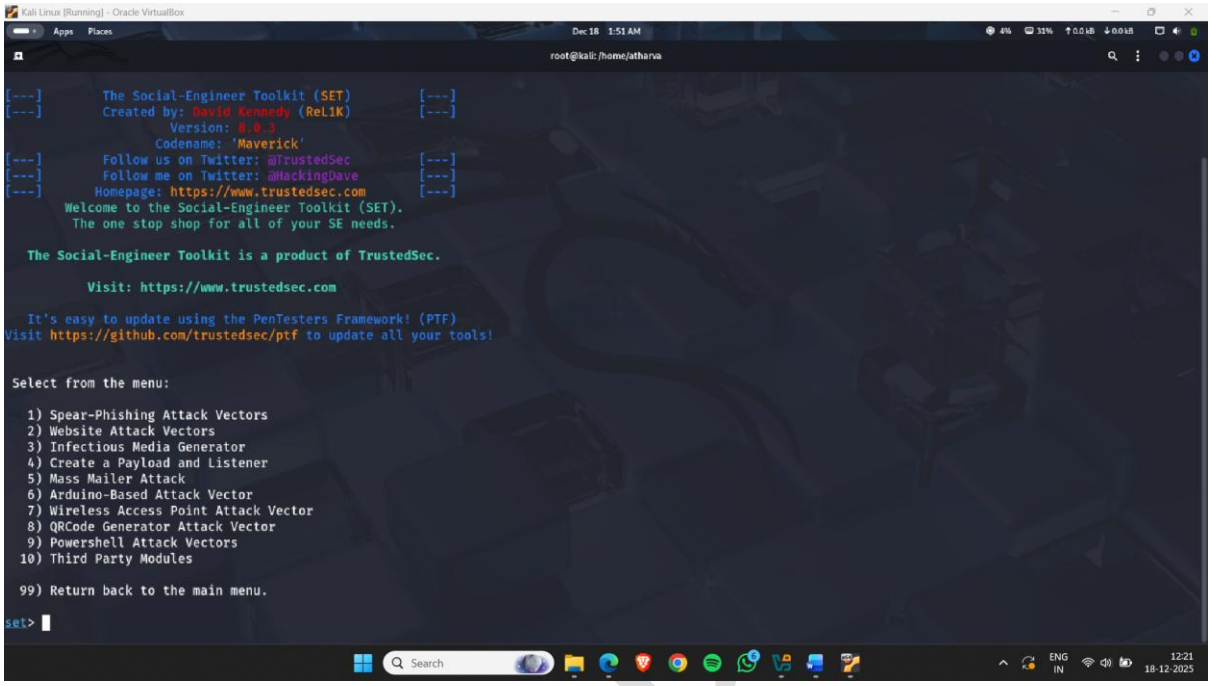

Figure 2

- Now select 3 – Credential Harvesting Attack Method

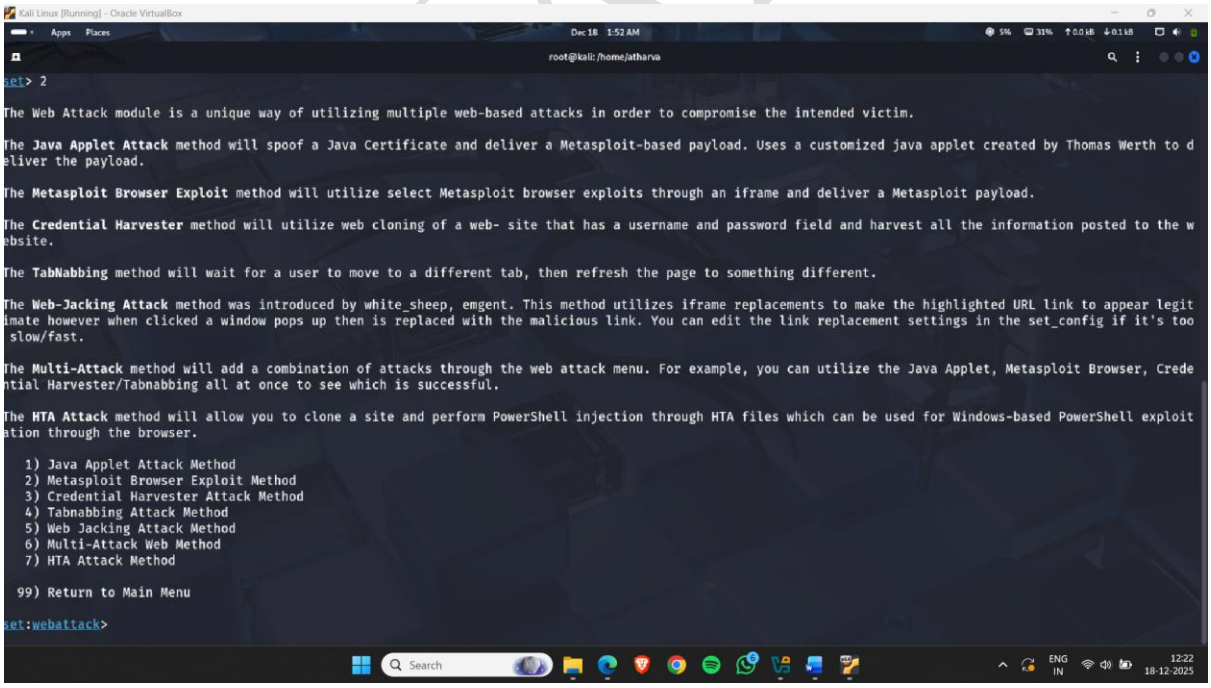

Figure 3

- Select 1 – Web Template

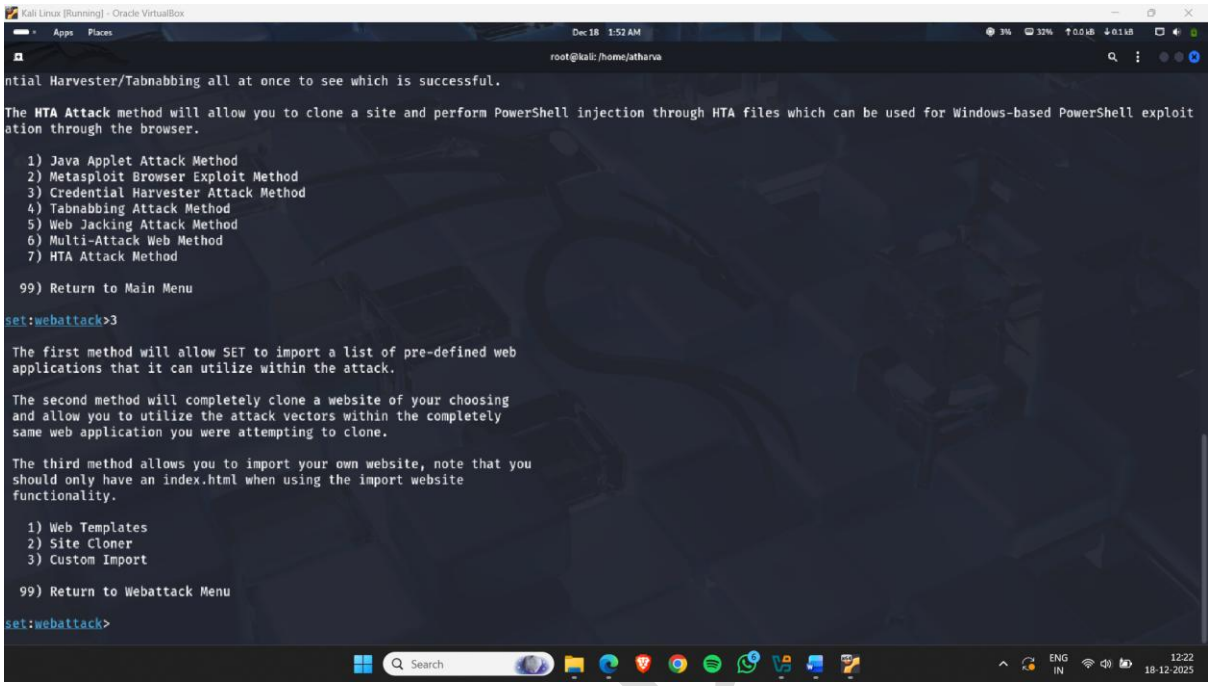

Figure 4

- Select 2 - Google

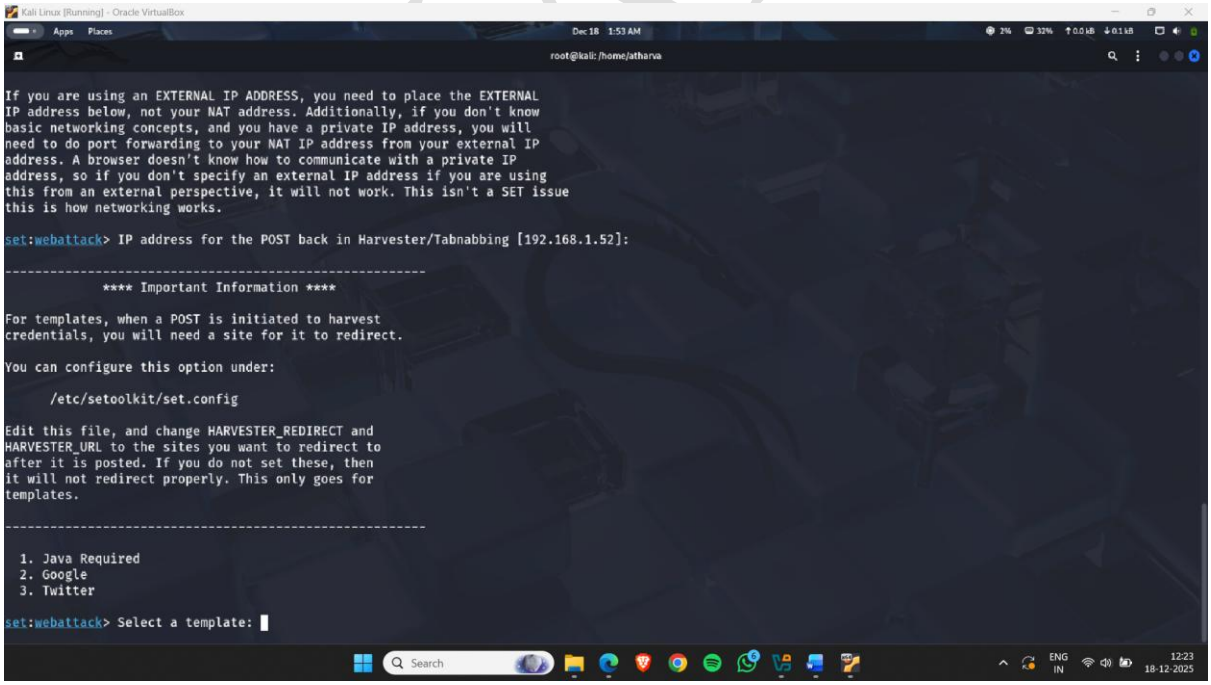

Figure 5

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

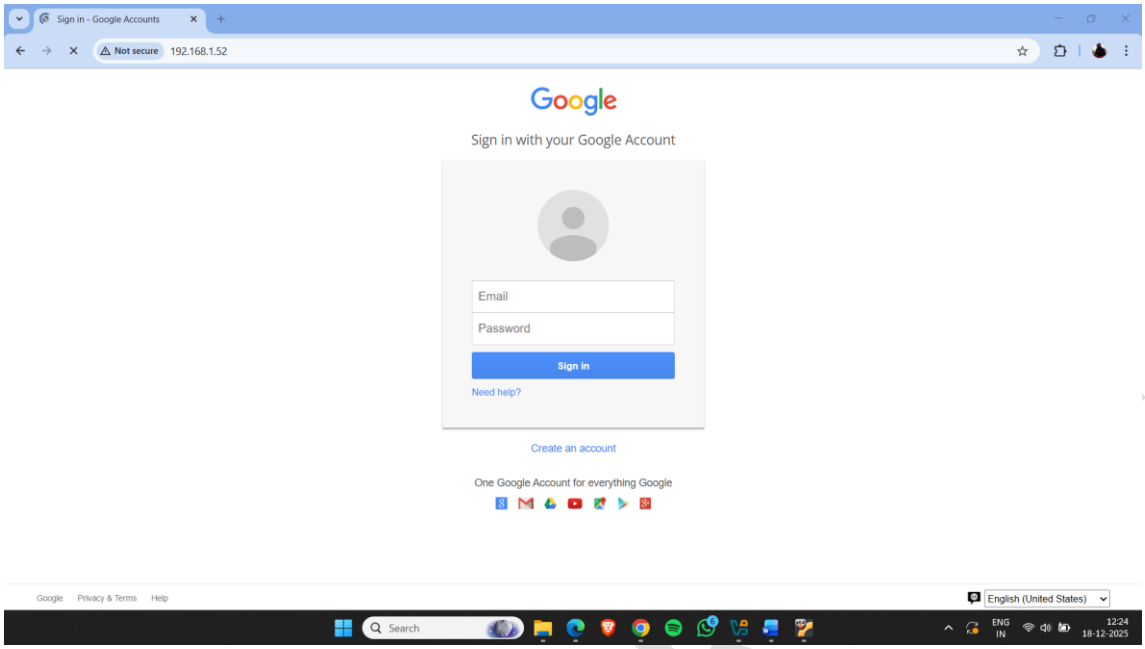

Figure 6

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

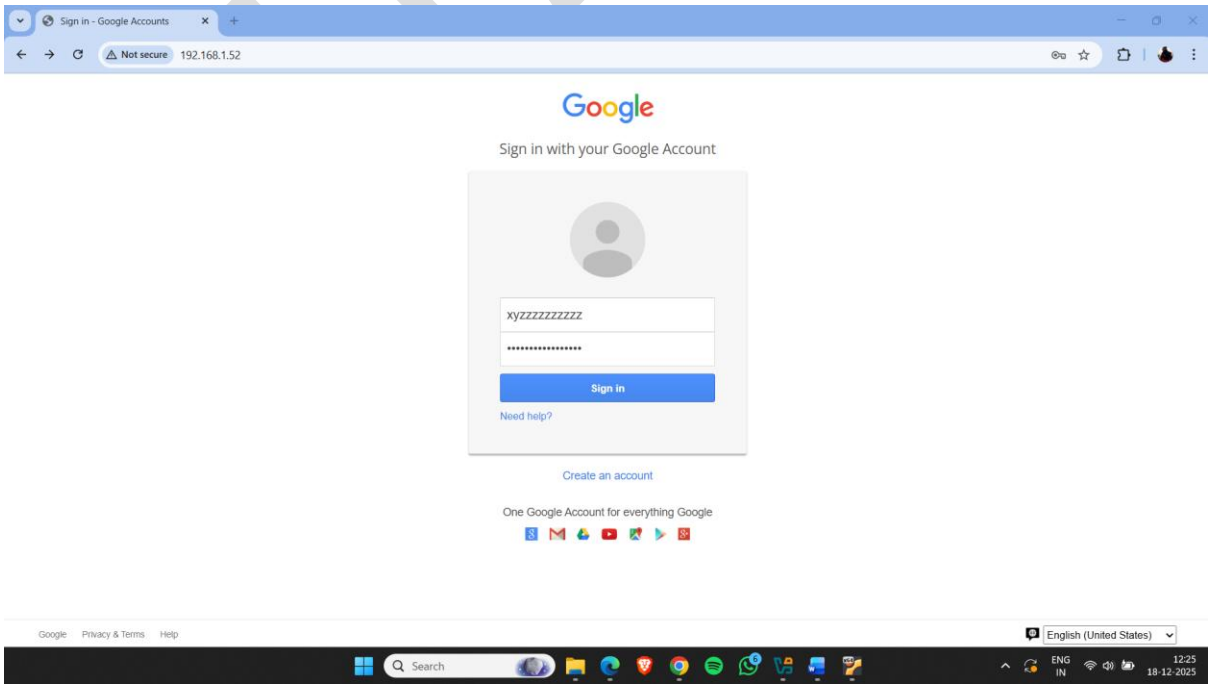

Figure 7

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

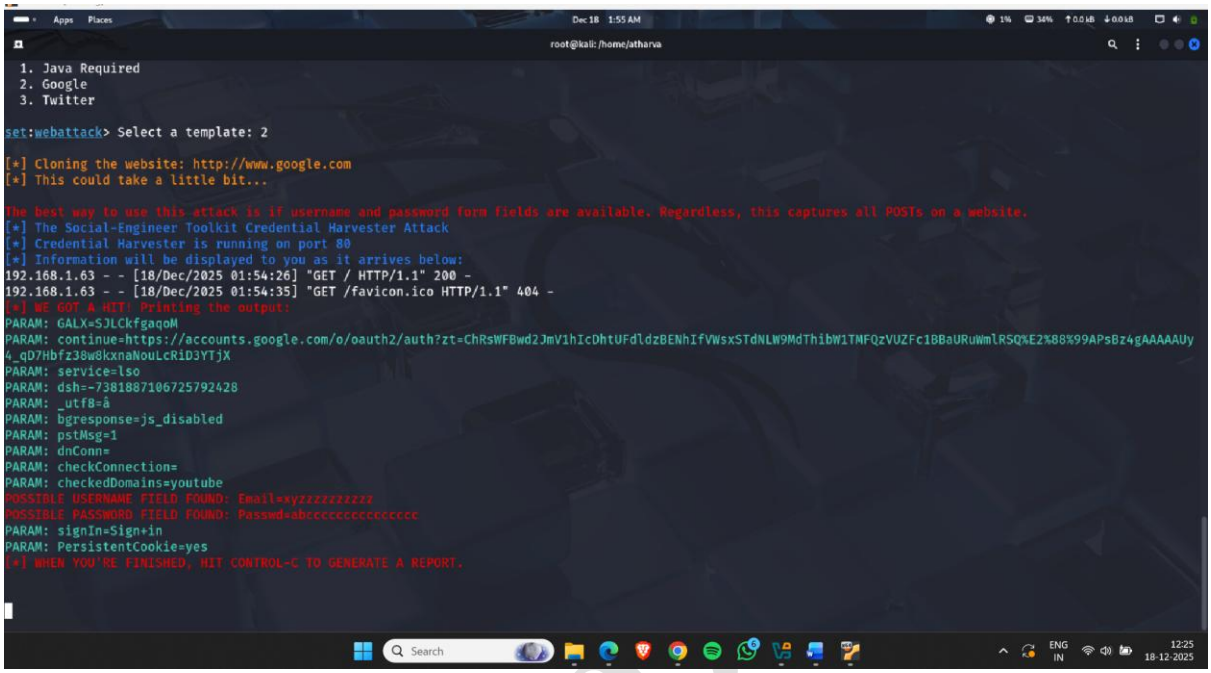

Figure 8

- Here we got the creadentials of google template.

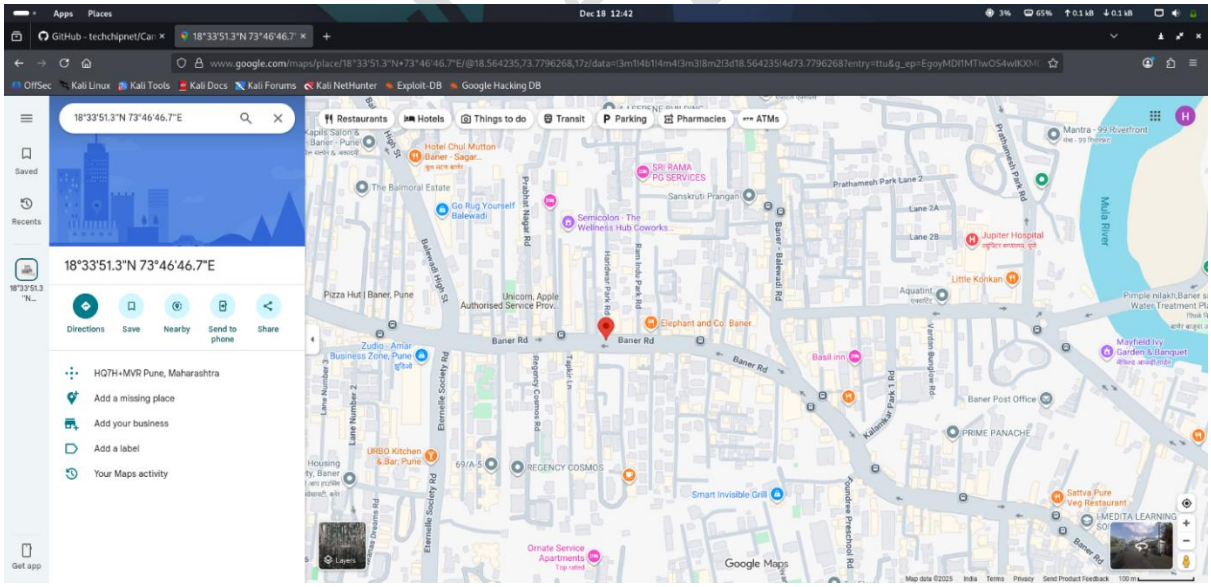

Figure 9

2) QRCode Generator

Select 8 – QRCode generator Attack Vector

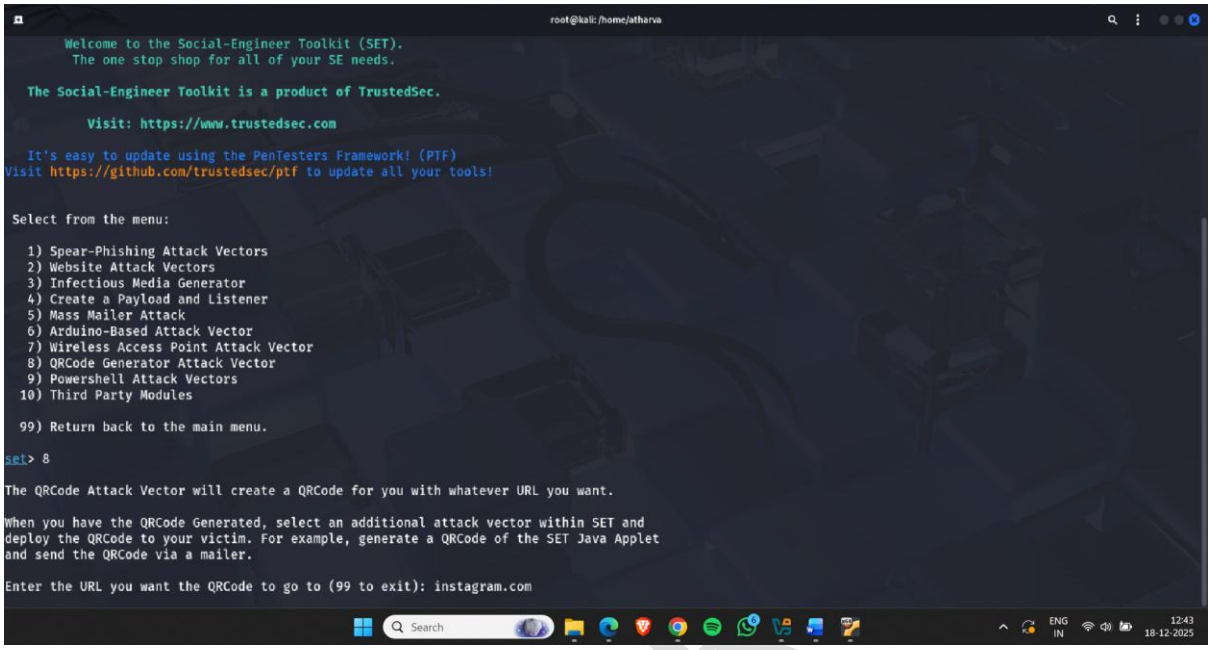

Figure 10

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

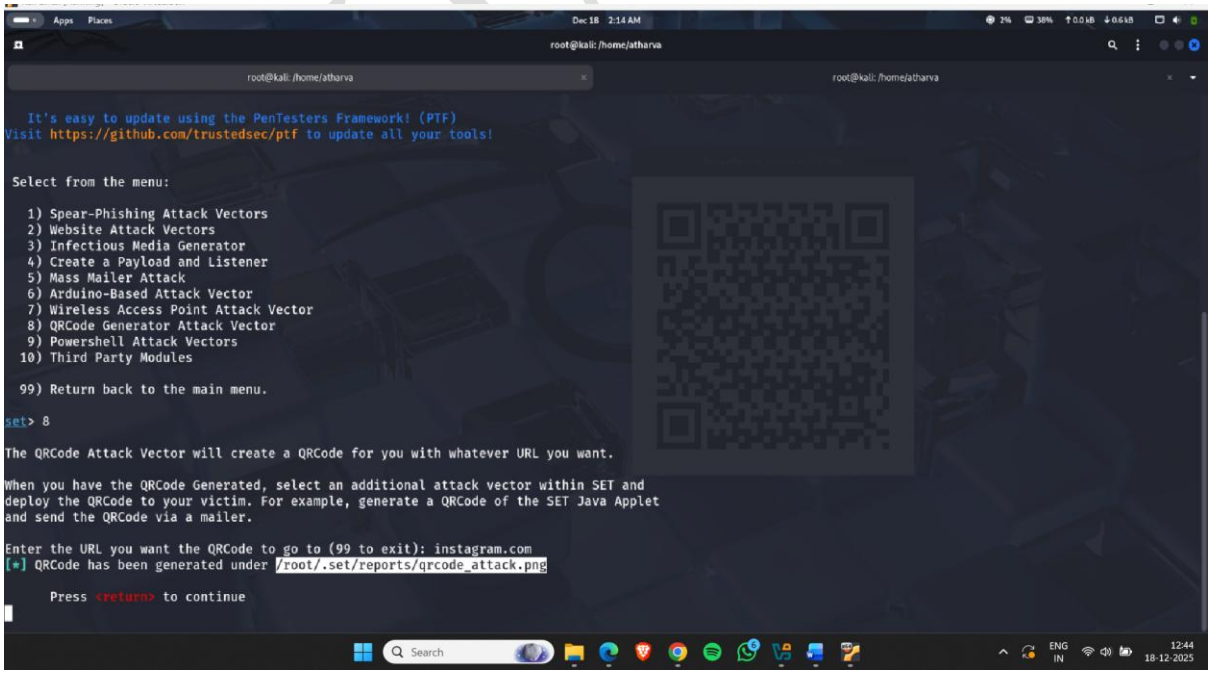

Figure 11

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

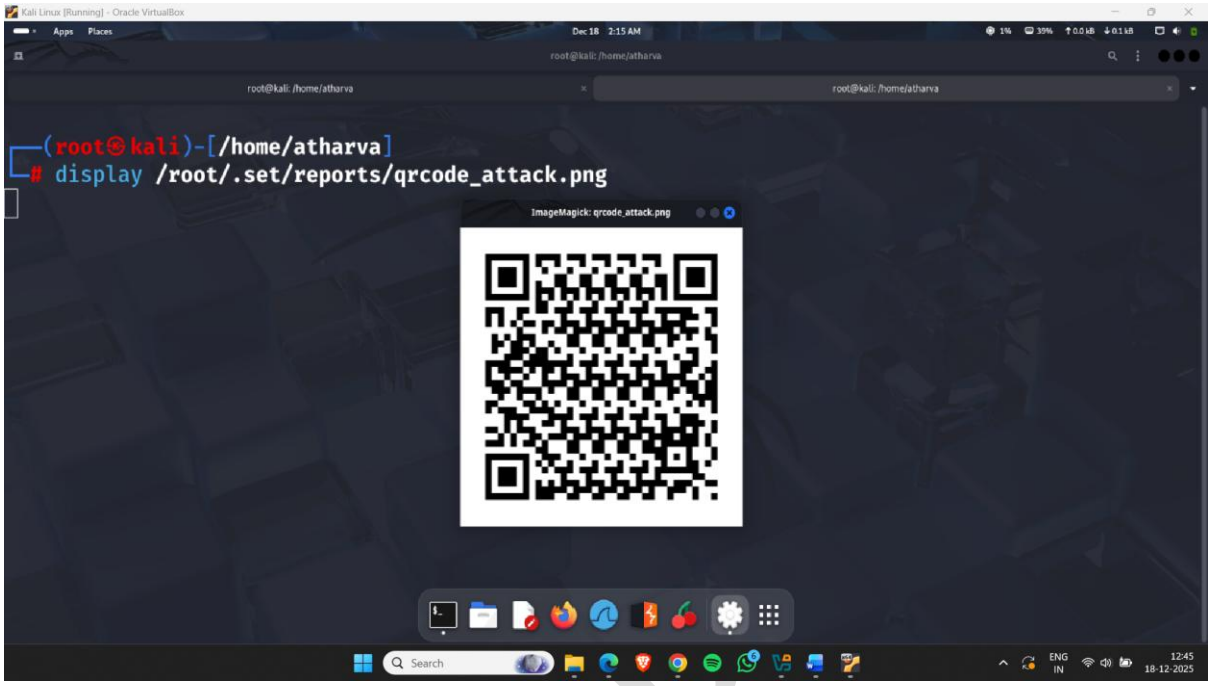

Figure 12

- Scan the QR Code it will open the link.

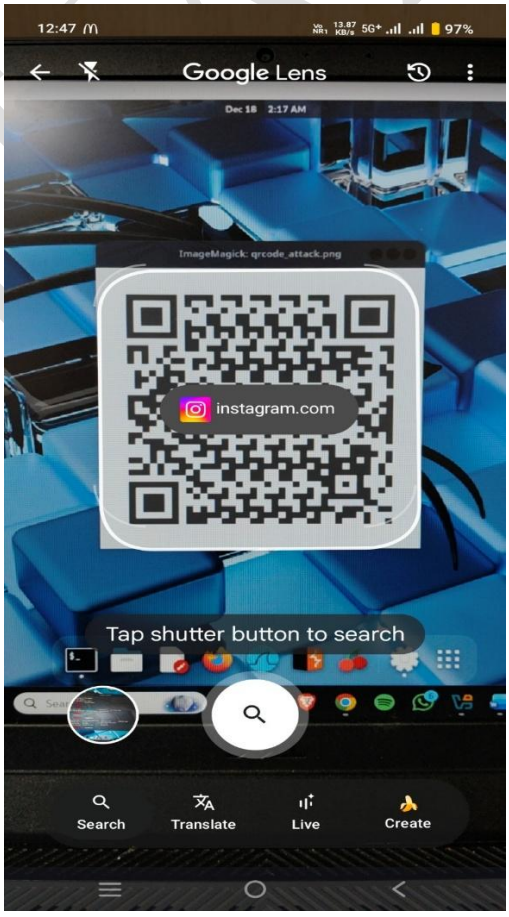

Figure 13

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

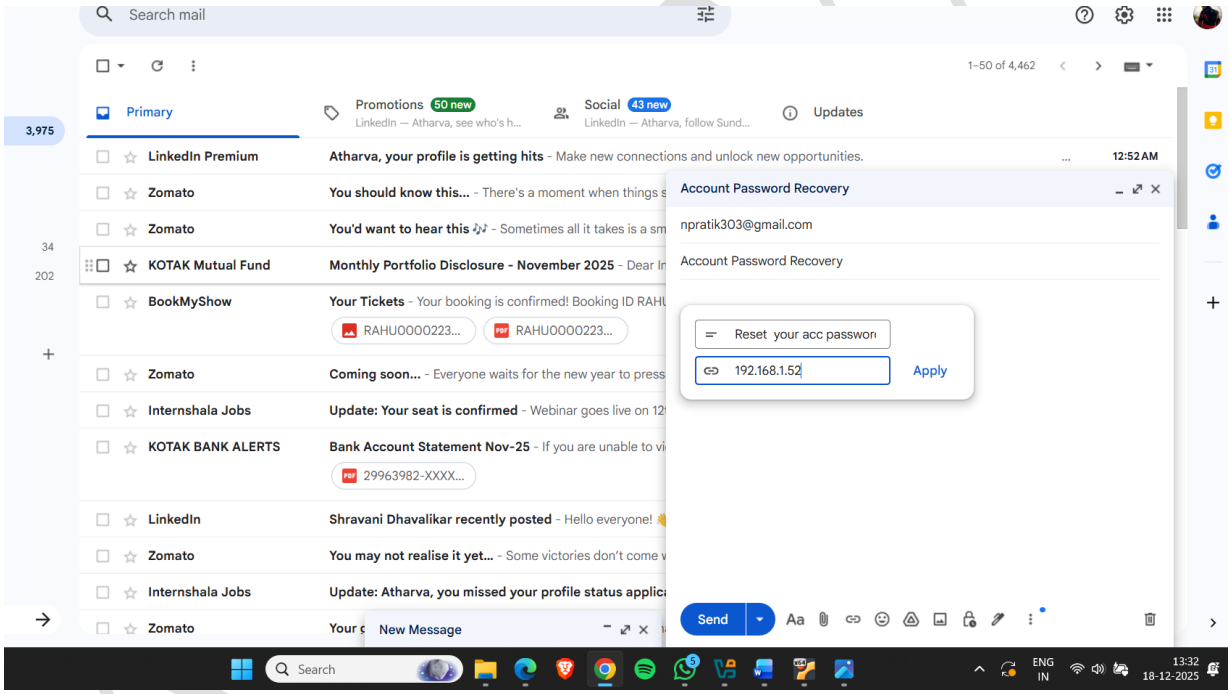

Figure 14

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

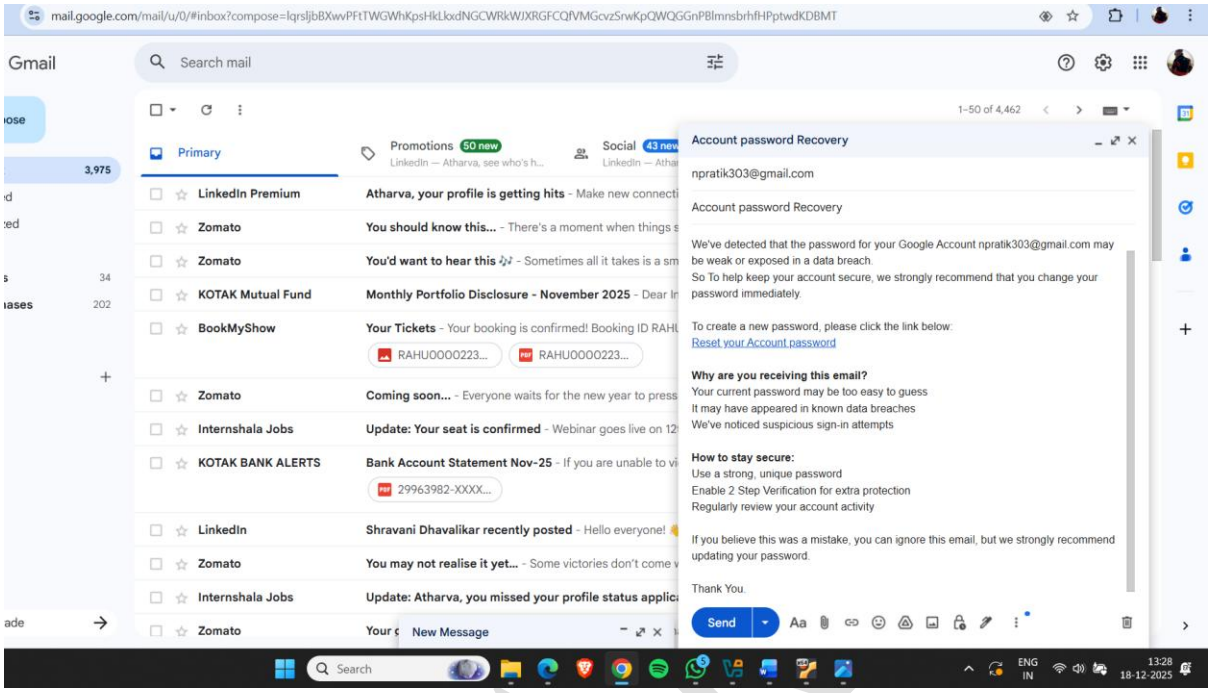

Figure 15

- 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.

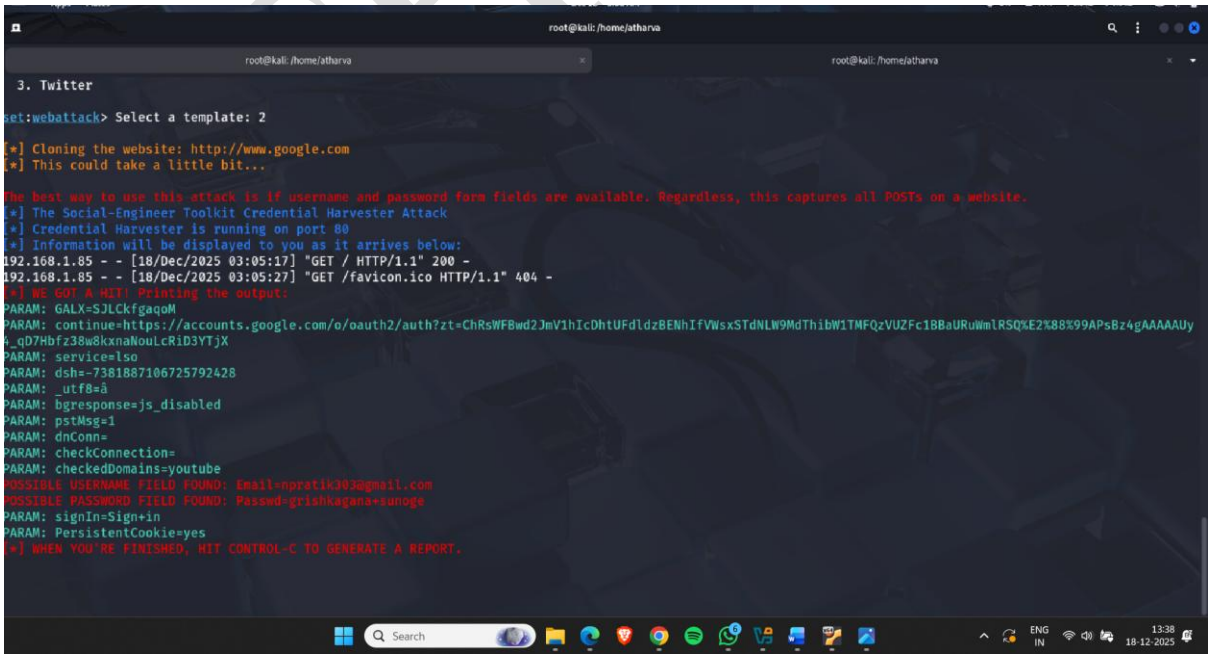

Figure 16

- 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

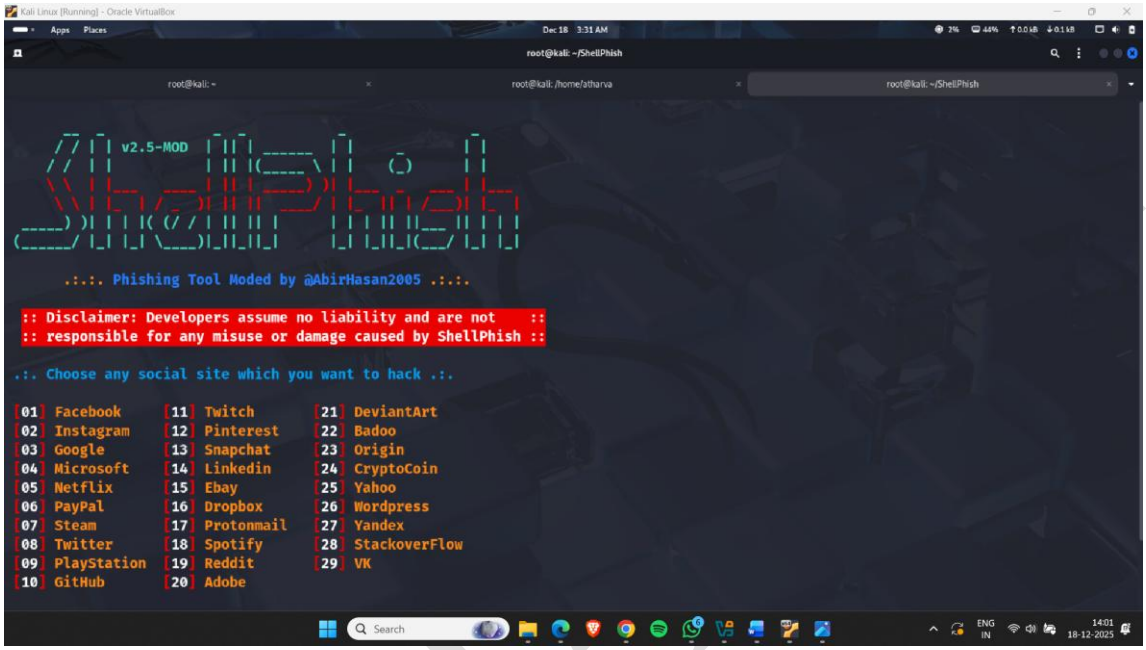

Figure 17

- Now select 1 – Localhost

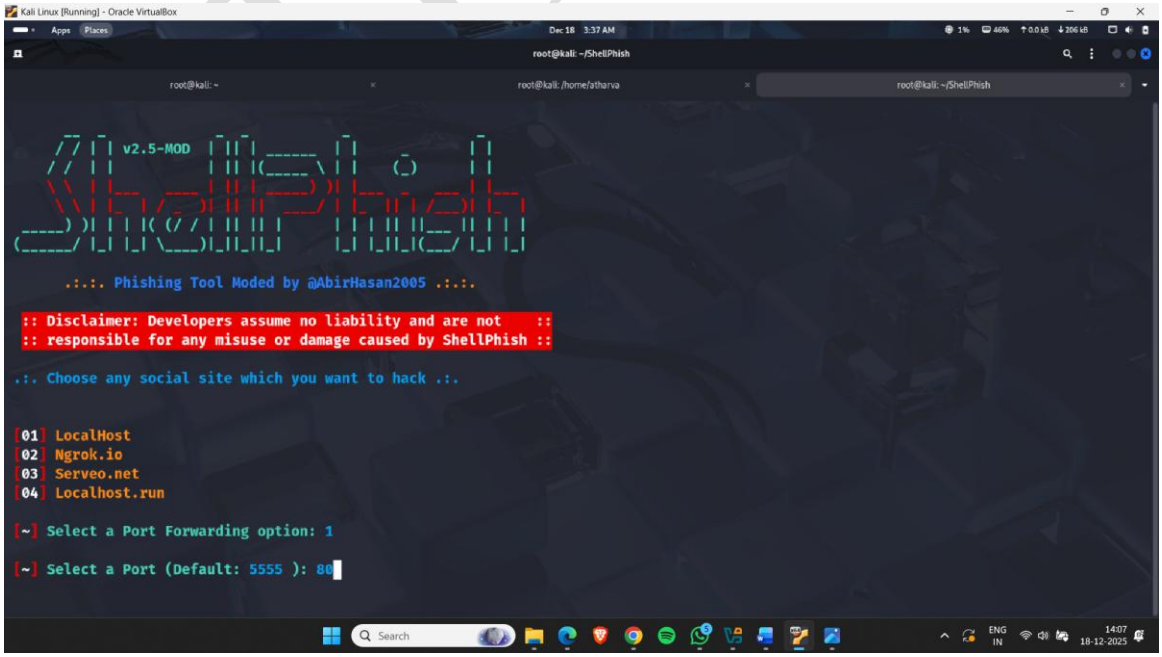

Figure 18

- Link will be generated

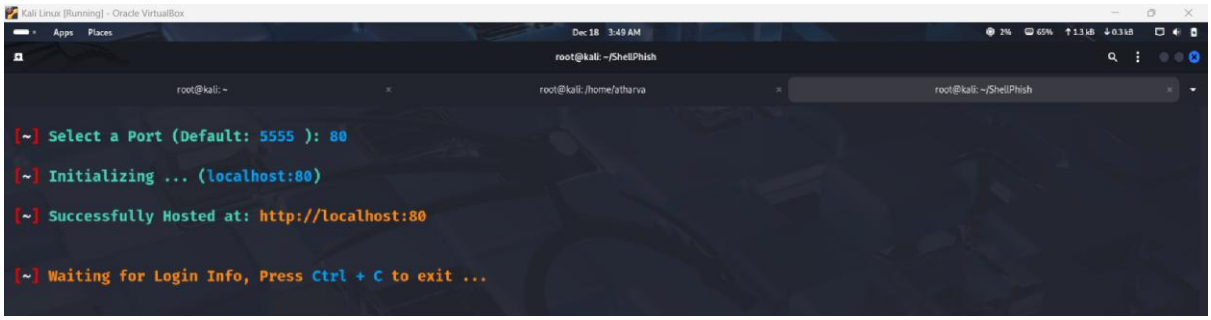

Figure 19

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

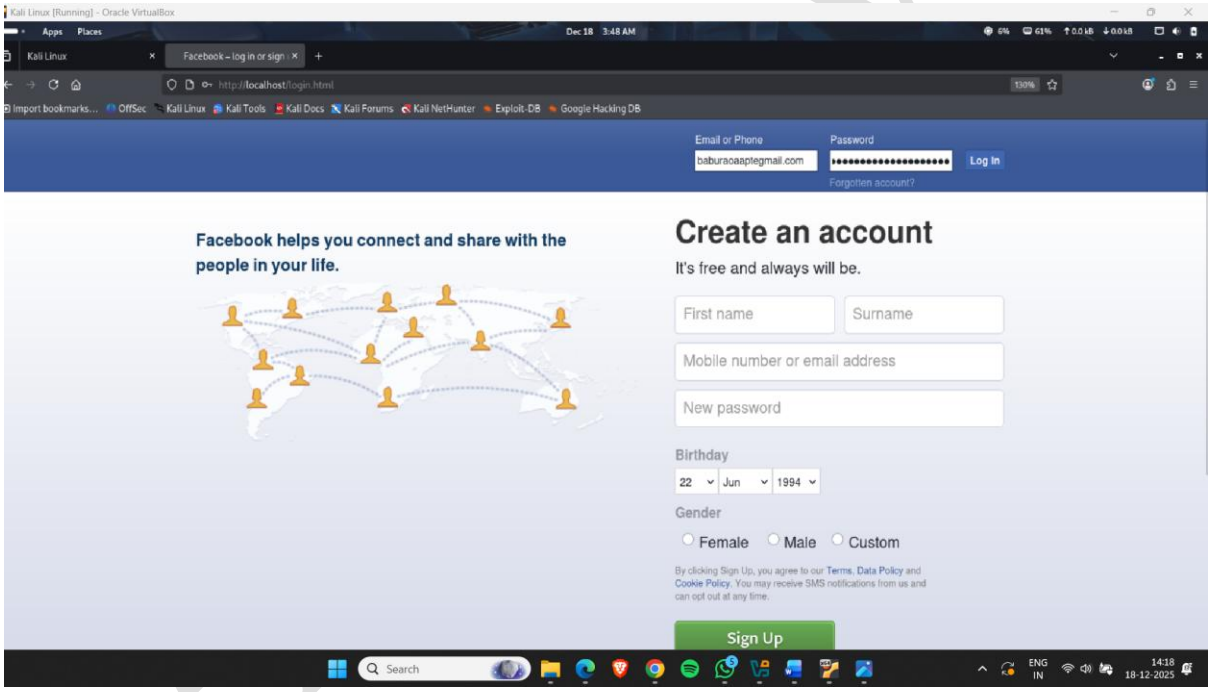

Figure 20

- You’ll get target’s credentials

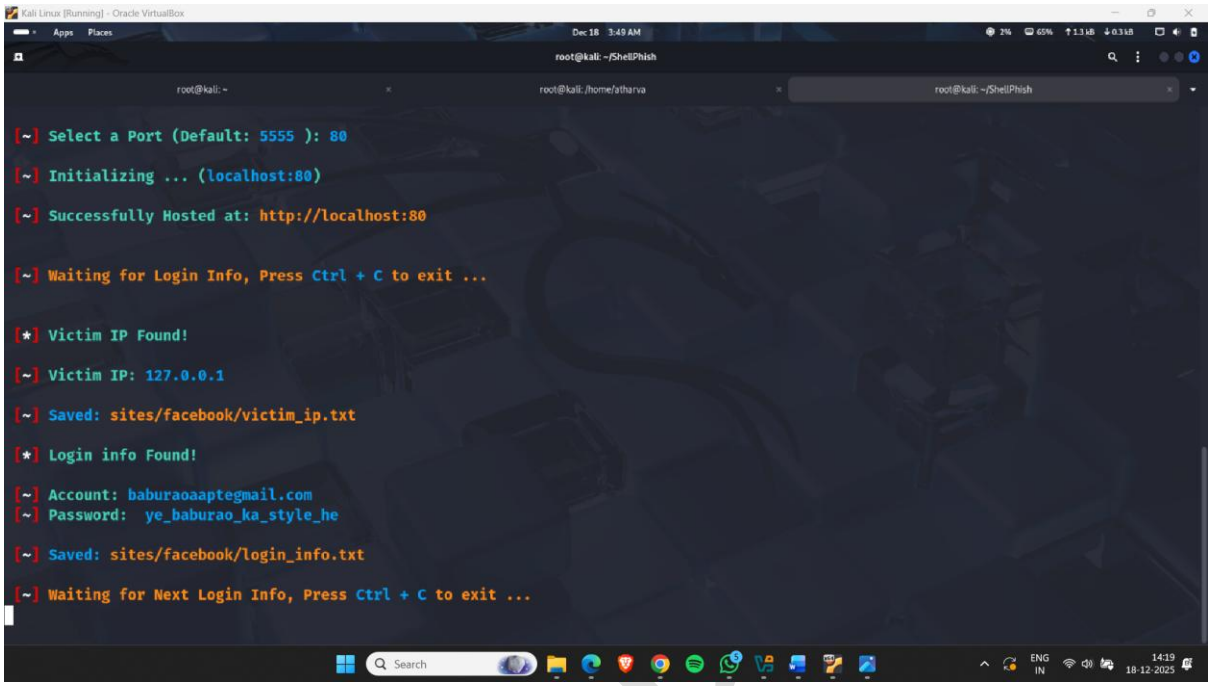

Figure 21

Perform Phishing Attack Using CamPhish

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

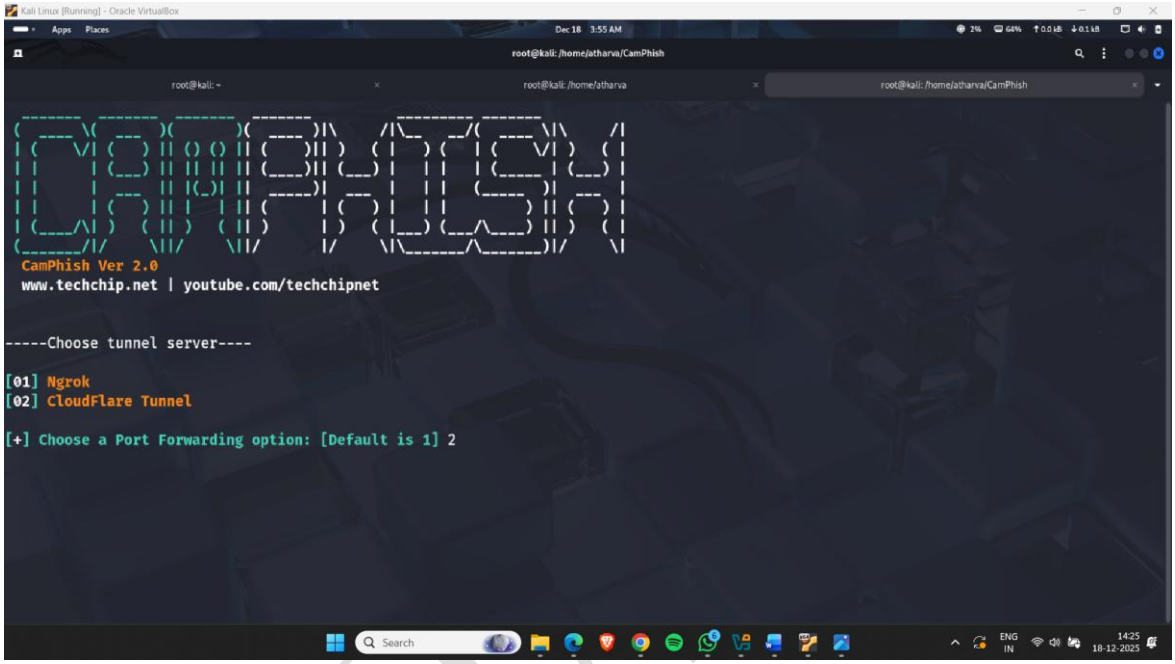

Figure 22

- Select Server – cloudflare tunnel

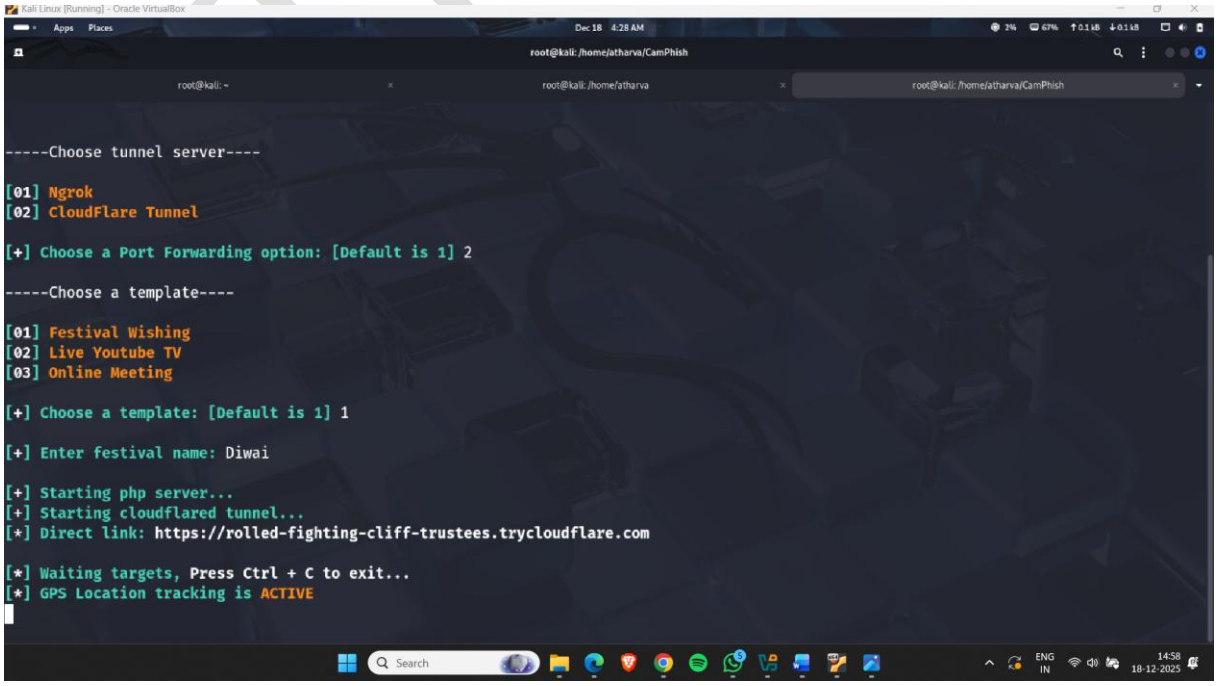

Figure 23

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

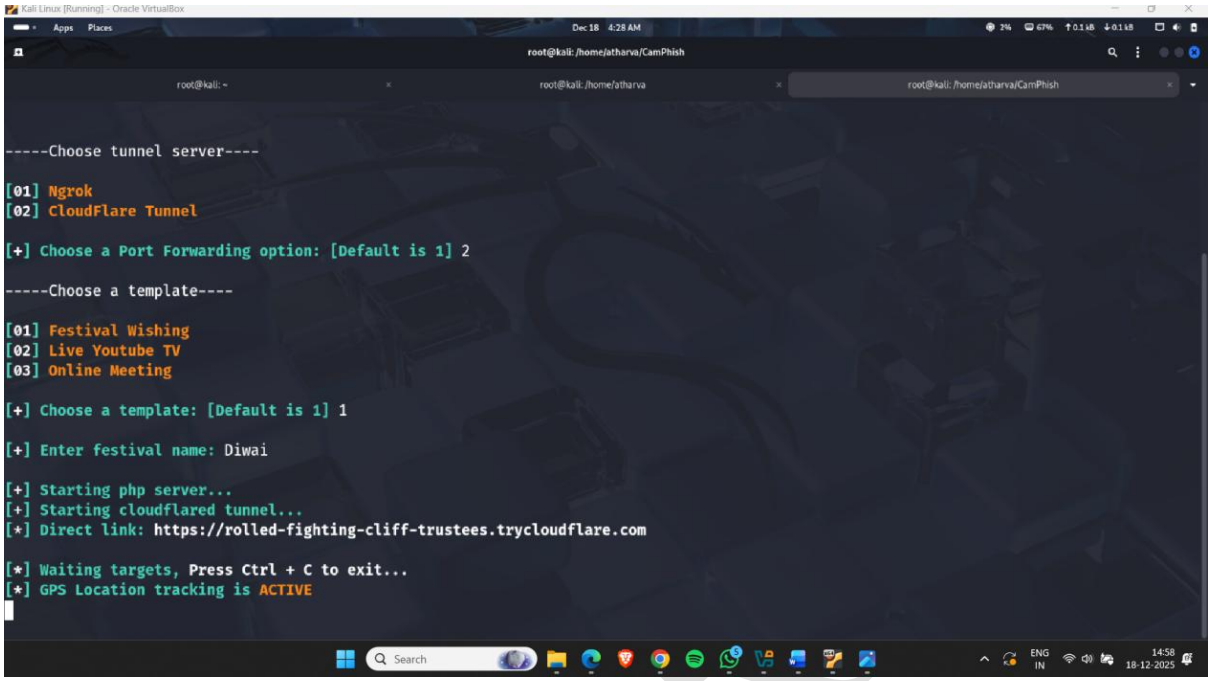

Figure 24

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

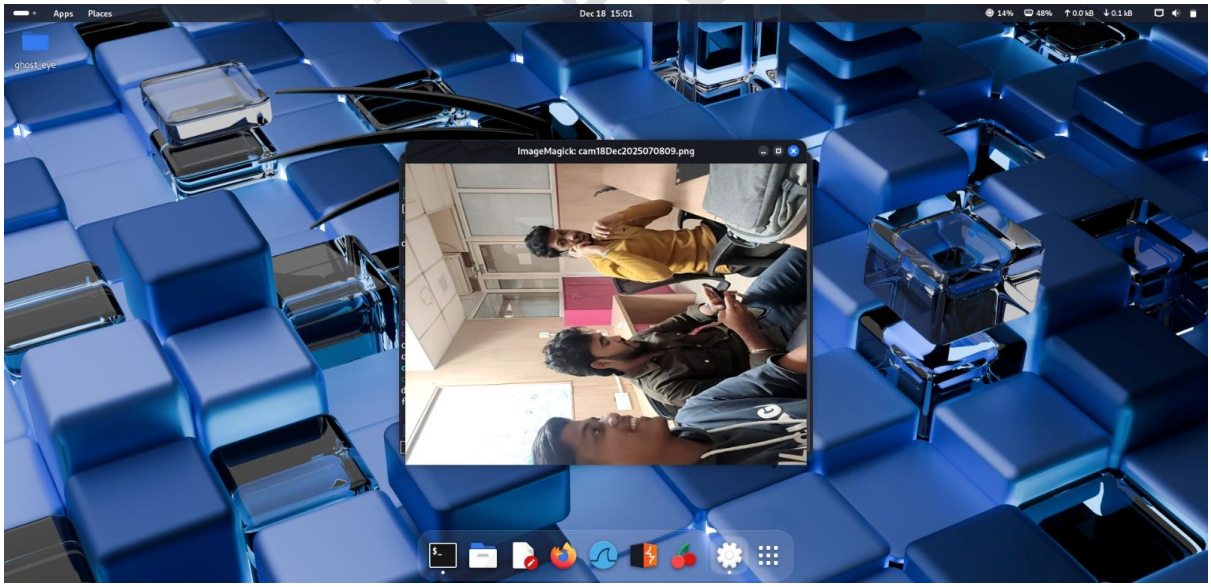

Figure 25

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

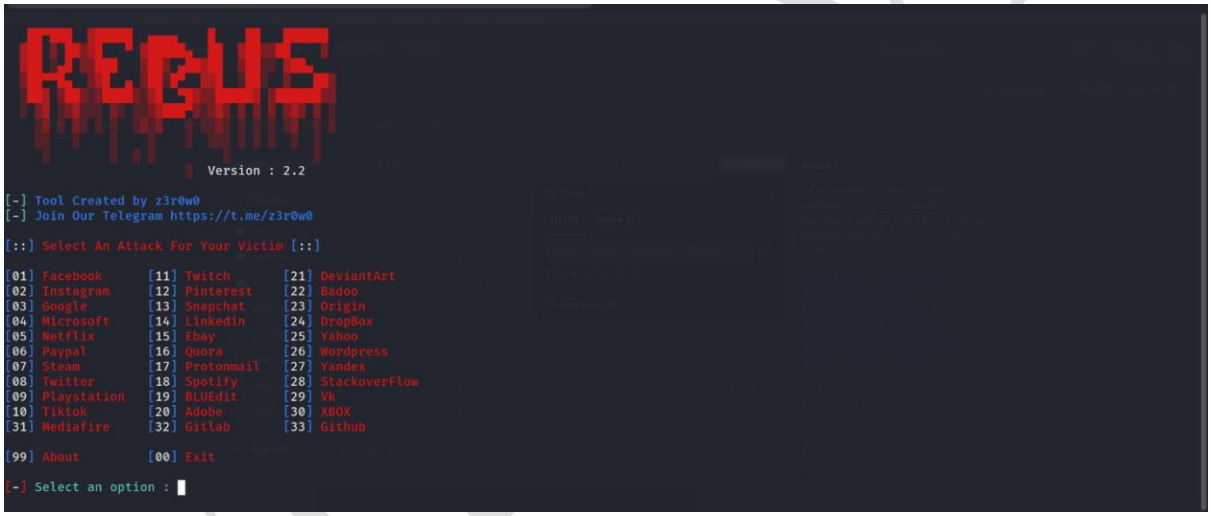

Figure 26

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

Figure 27

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

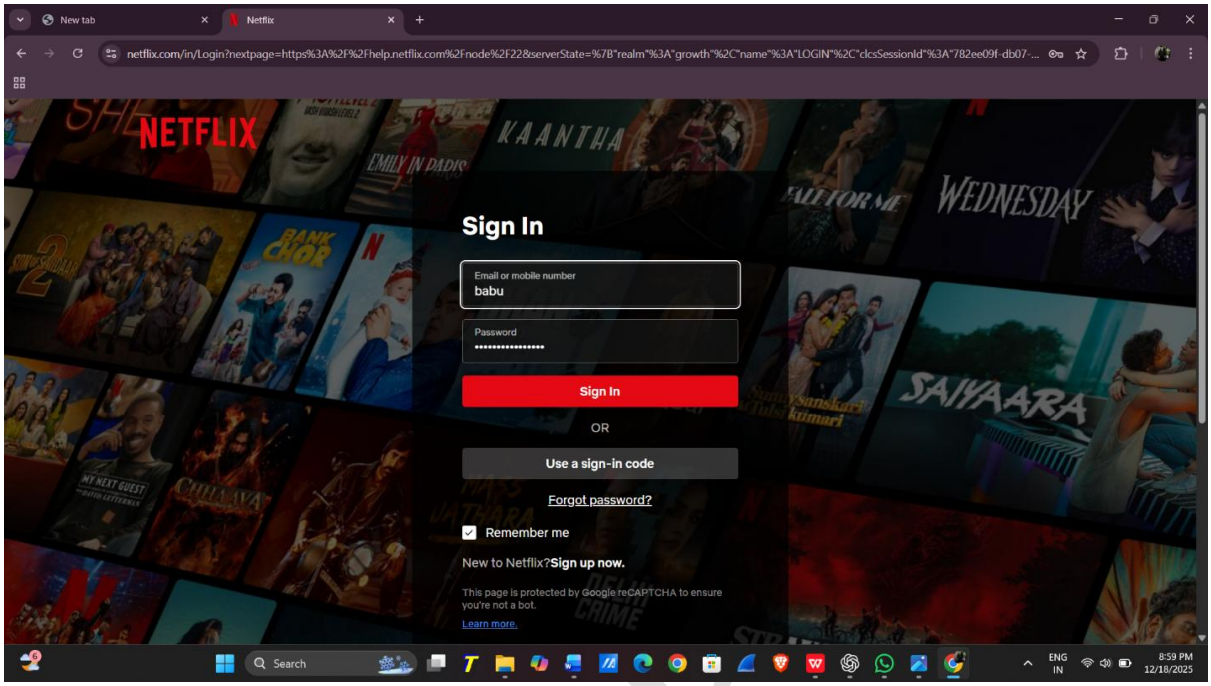

Figure 28

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

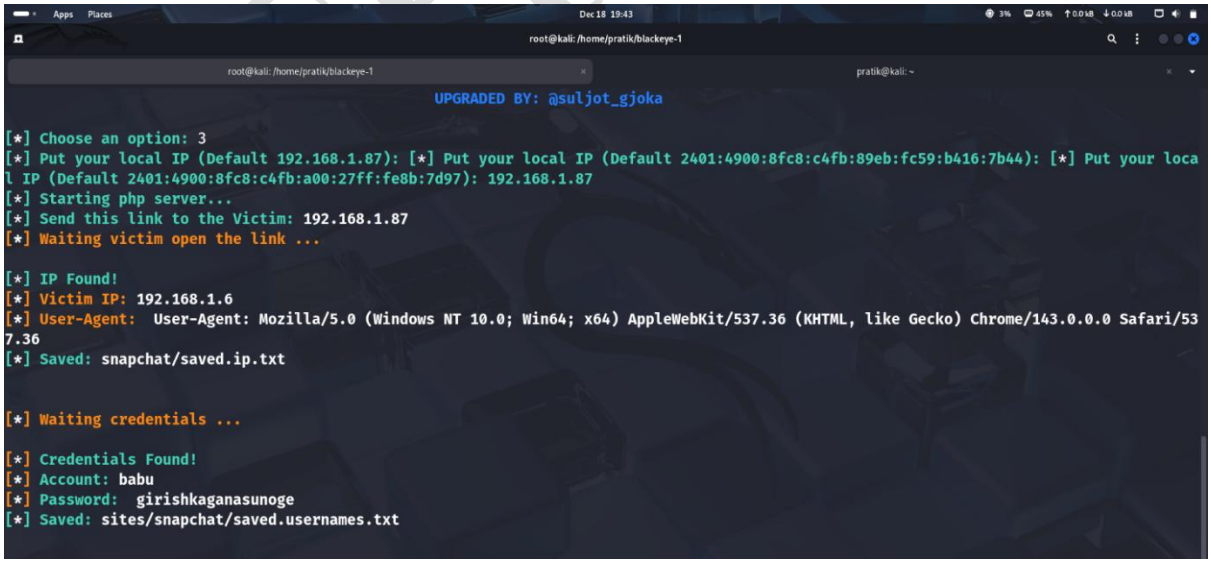

Figure 29

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

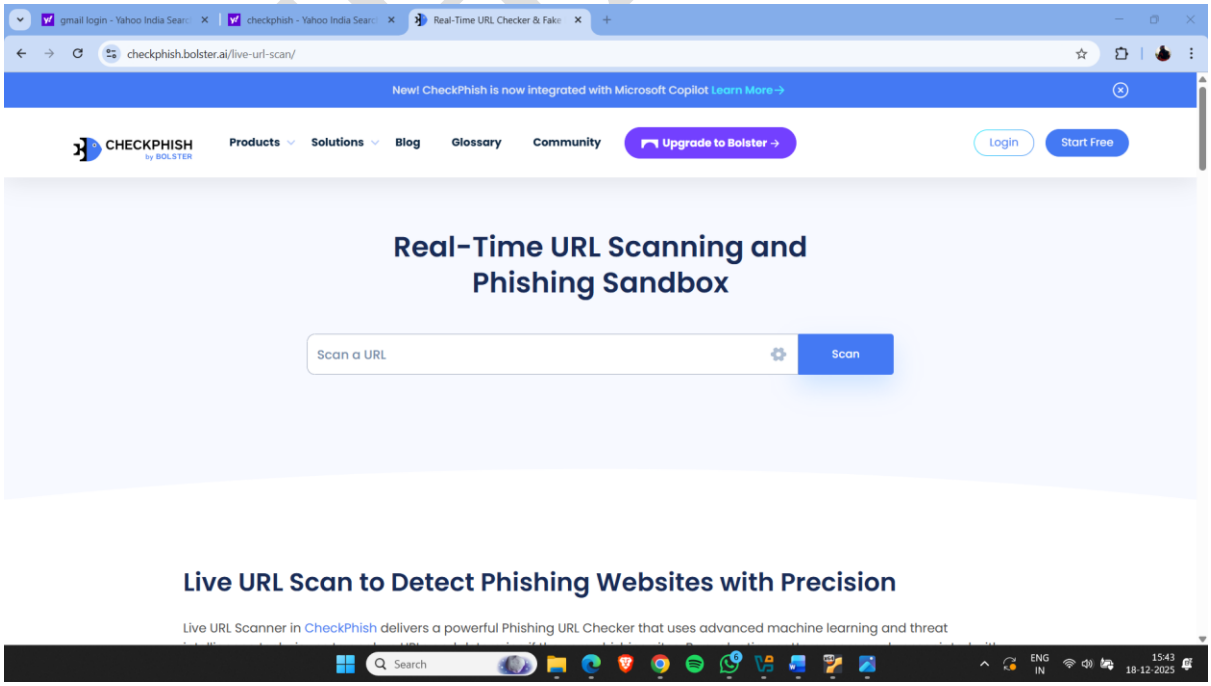

Figure 30

- Phishing Detected

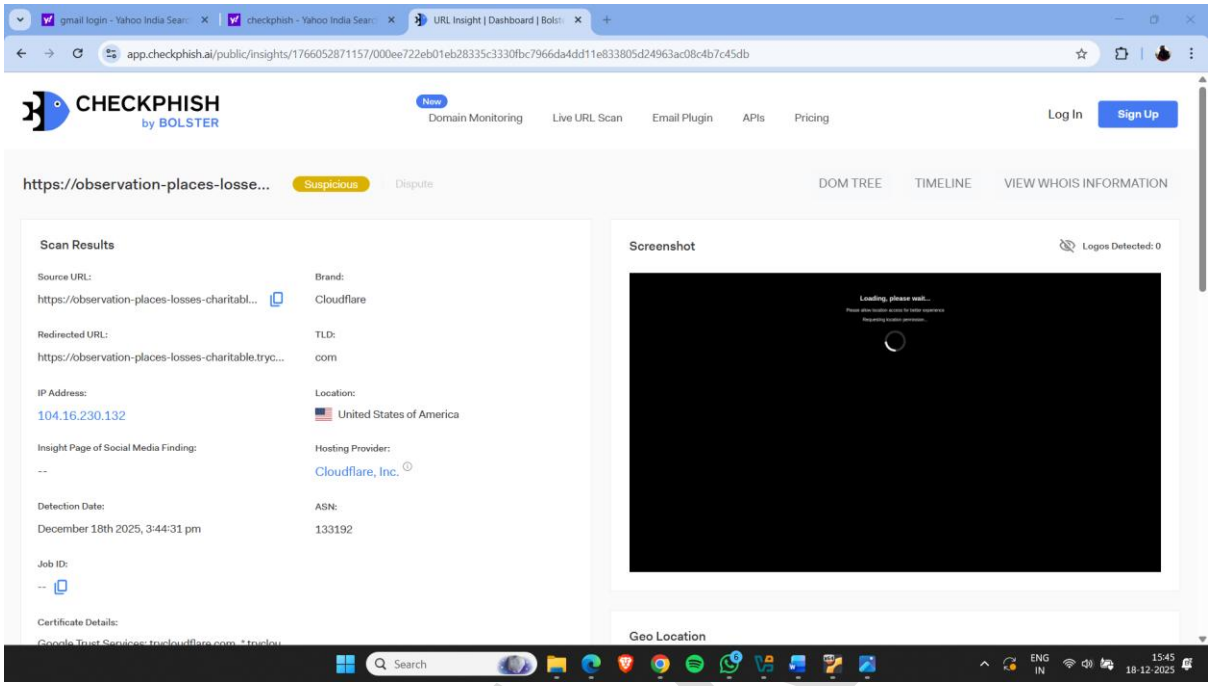

Figure 31