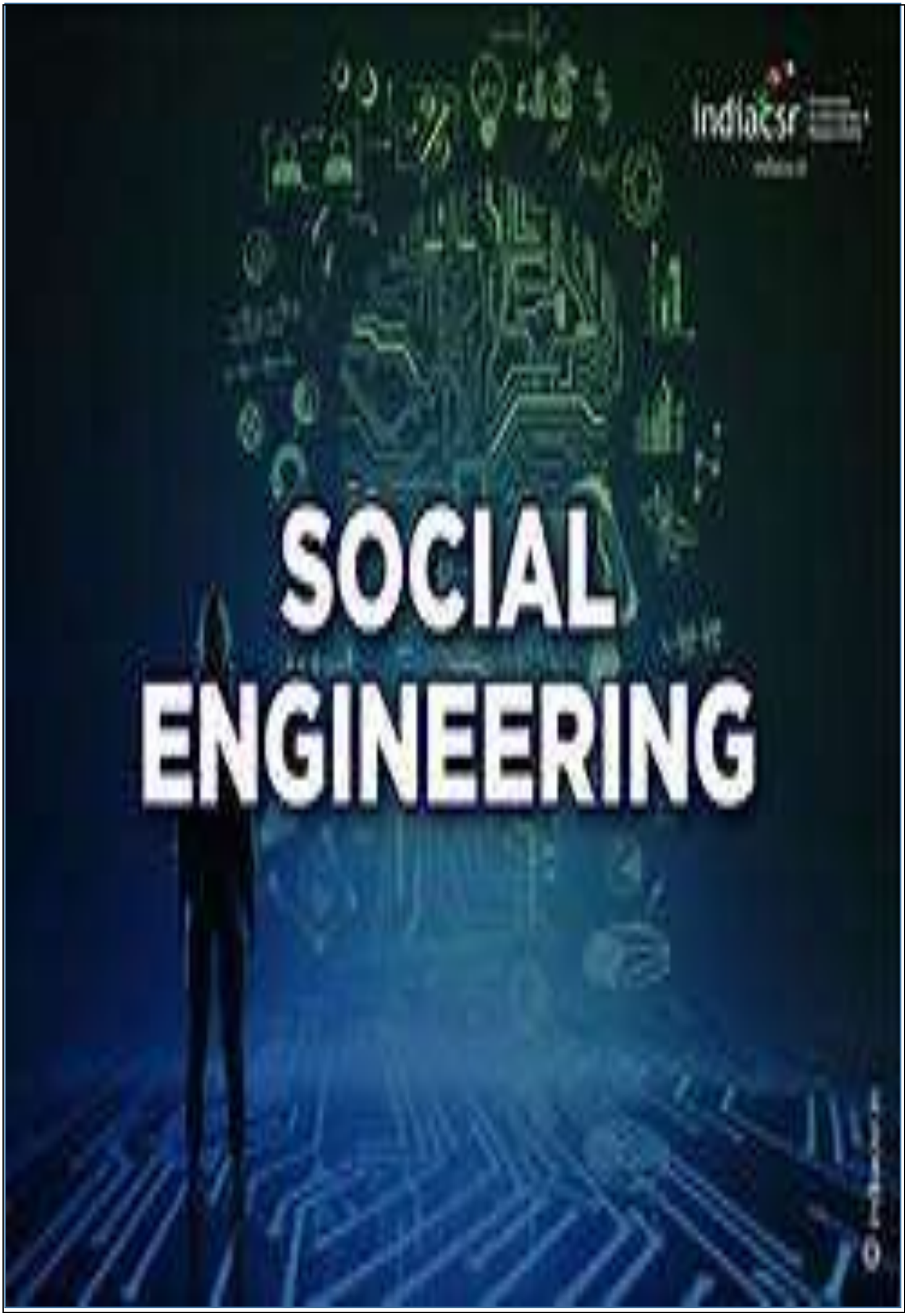

SOCIAL
ENGINEERING

Module 9 Social Engineering

What is Social Engineering

- **Why is it Dangerous?**
- **How It Works**

Types of social engineering attacks

1.Human base social engineering

2.Computer base social engineering

- **Common Computer-Based Social Engineering Techniques**
- **Phishing**
- **Spear Phishing**
- **Whaling**
- **Malware Baiting**
- **Fake Pop-Ups/Alerts**
- **Social Media Impersonation**
- **Clone Phishing**

- 🔍 **Key Characteristics**

3.Mobile base social engineering

4 Common Mobile-Based Social Engineering Techniques

Task1 Create the fishing page using Social Engineering

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

Task 3 using Zphisher Create Fishing Page

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

2 Extra Activity using website for fishing URL detections

Website: URL SACN.AI

3 Extra Activity using website for fishing URL detections

Website: URL VOID

4 Extra Activity using website for fishing URL detections

Website: checkphish.boster.ai

What is Social Engineering?

1. Social engineering is a manipulation technique.
2. It tricks people into revealing confidential information.
3. Unlike hacking computers, it targets **human psychology**.
4. It relies on **trust**, **urgency**, **fear**, or **curiosity**.

Why is it Dangerous?

5. It bypasses traditional cybersecurity measures.
6. Even strong passwords can't protect you from being tricked.
7. It's often the **first step** in larger cyberattacks.
8. Human error is a major security vulnerability.

How It Works:

Attackers study the target.

They gather public info from social media or th web.

Then they create a believable story or identity.

The goal is to **gain trust** or **create panic**.

Types of social engineering attacks

1 Human base

- Social engineering is the art of manipulating people.

- It focuses on human psychology, not just technology.
- Attackers exploit trust, fear, urgency, or curiosity.
- People are often the weakest link in security.

Let's explore the main types of human-based attacks.

2 Computer base

This refers to **manipulative attacks that occur using computers, networks, or digital systems** — rather than physical or in-person methods. Attackers use computers as the medium to deceive users and extract sensitive data.

🔍 Key Characteristics

- Uses **digital communication** (email, websites, social media, pop-ups)
- Exploits **human psychology** rather than technical vulnerabilities
- Often serves as the **first step** in larger cyberattacks (like installing malware or stealing data)

💻 Common Computer-Based Social Engineering Techniques

Method	Description
Phishing	Fraudulent emails or messages that appear legitimate, tricking users into clicking links or entering login info
Spear Phishing	Targeted phishing at a specific person or organization, often using personal details to increase credibility
Whaling	Phishing aimed at high-profile targets like executives (e.g., CEO fraud)
Malware Baiting	Offering fake software, games, or media downloads that install malware
Fake Pop-Ups/Alerts	Pop-up windows that warn about a fake virus and offer to "fix" it, leading to a scam
Social Media Impersonation	Creating fake accounts or messages on platforms to build trust and trick victims
Clone Phishing	Duplicating a real email, changing the links/attachments, and resending it as a trusted sender

3 Mobile-based social engineering

Mobile-based social engineering" refers to deceptive tactics used to manipulate individuals via mobile devices in order to extract sensitive information, gain access to systems, or perform unauthorized actions. These tactics often exploit human psychology rather than technical vulnerabilities.

Common Mobile-Based Social Engineering Techniques:

1. **Phishing via SMS (Smishing):**
    - Attackers send fraudulent SMS messages that appear to be from trusted sources (banks, delivery companies, etc.).
    - These messages may contain malicious links or request sensitive data like passwords or OTPs.
2. **Voice Phishing (Vishing):**
    - Scammers make phone calls pretending to be from legitimate institutions (like banks, tech support, or government agencies).
    - They try to convince the victim to reveal personal or financial information.
3. **Malicious Mobile Apps:**
    - Fake apps disguised as legitimate ones may request excessive permissions to access contacts, SMS, location, etc.
    - Some are used to harvest credentials or track user behavior.
4. **WhatsApp/Telegram/Signal Scams:**
    - Attackers may impersonate known contacts, request money, or share malicious links.
    - These platforms are often used to spread disinformation or fraudulent messages.
5. **QR Code Scams:**
    - Attackers trick users into scanning malicious QR codes, which can lead to phishing sites or trigger unwanted actions on the device.
6. **SIM Swap Attacks:**
    - Social engineering is used to convince a mobile carrier to transfer a victim's number to a new SIM controlled by the attacker.

    - This allows interception of calls, texts, and 2FA codes.
7. **Callback Scams:**
    - Users receive missed calls or messages urging them to call back premium-rate or scam numbers.
8. **Bluetooth or NFC Exploits:**
    - Some attackers use proximity-based methods to initiate unauthorized connections or data transfers.

How to Protect Against Mobile-Based Social Engineering:

- Be cautious with links in texts or messages.
- Avoid installing apps from unknown sources.
- Use multi-factor authentication (not solely SMS-based).
- Verify phone calls from institutions independently.
- Keep your mobile OS and apps updated.
- Use security software that can detect threats and phishing attempts.

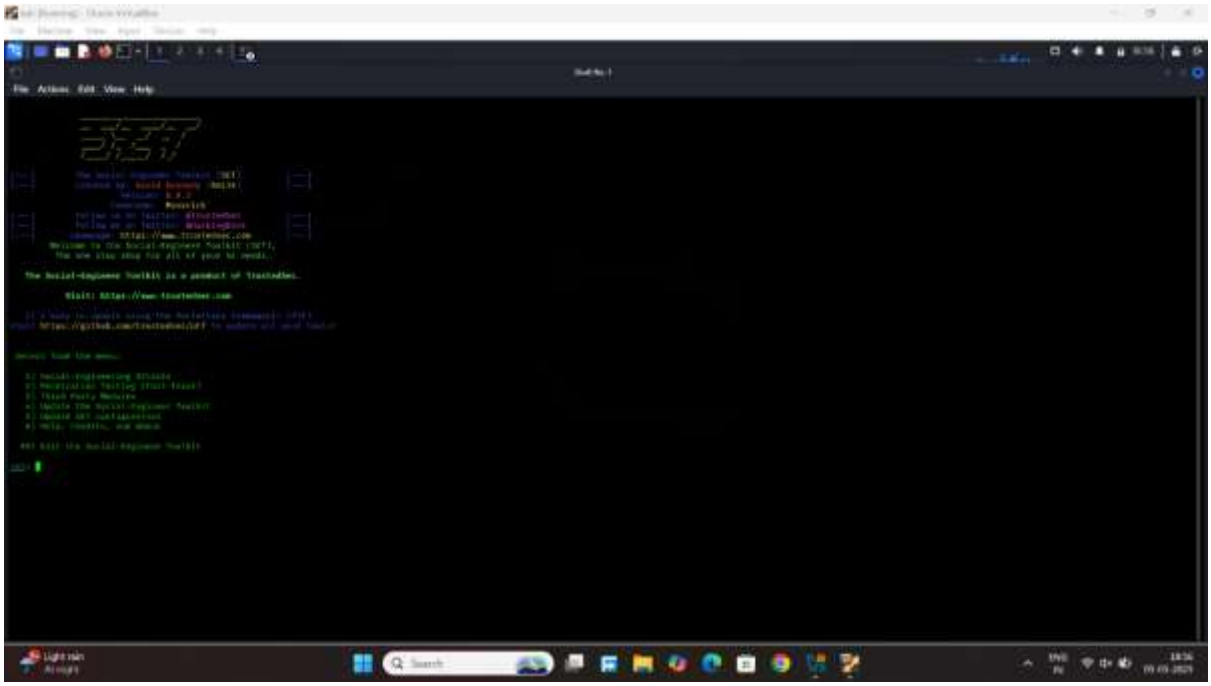
Would you like examples or case studies related to specific tactics?

Task1 Create the fishing page using Social Engineering

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

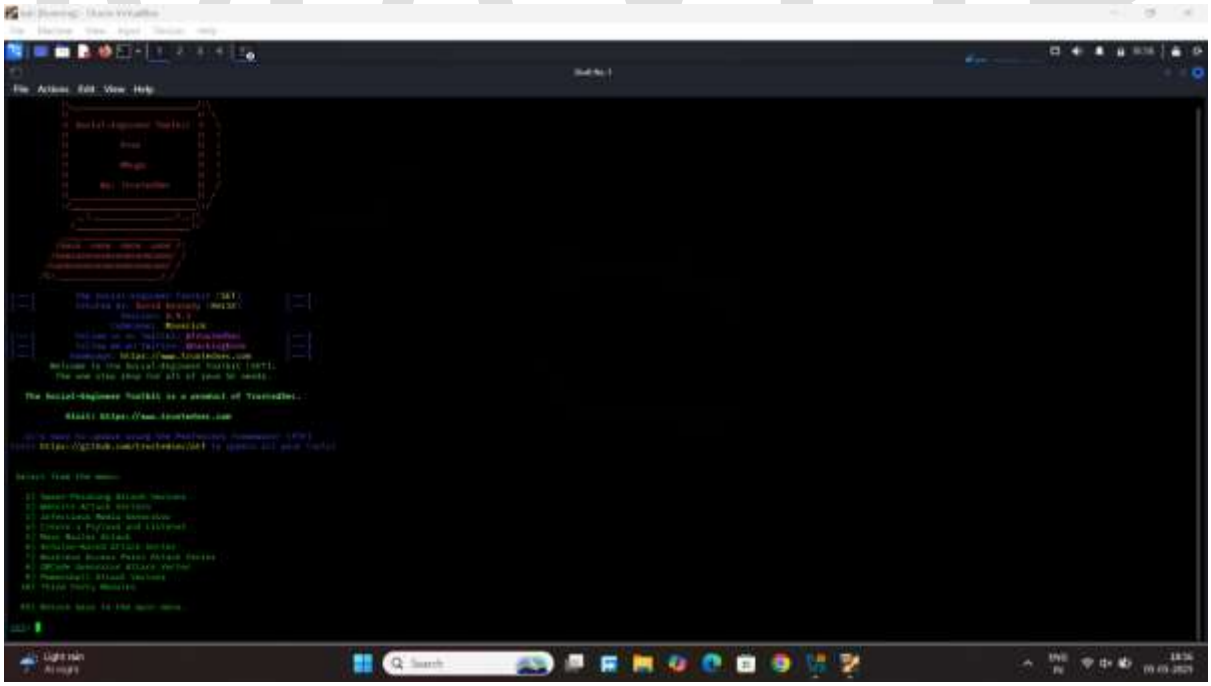
Step2: open the set tool kit choice the option

1 Social enginerring

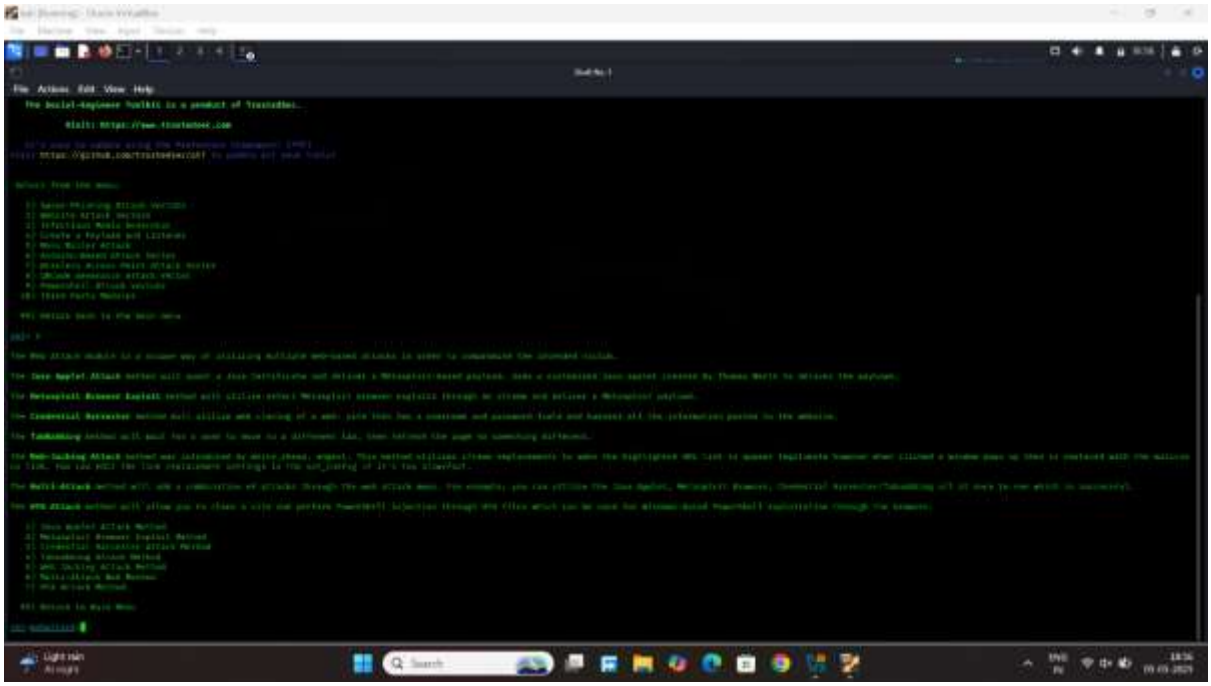


Step3: select the option

2 website attack vector

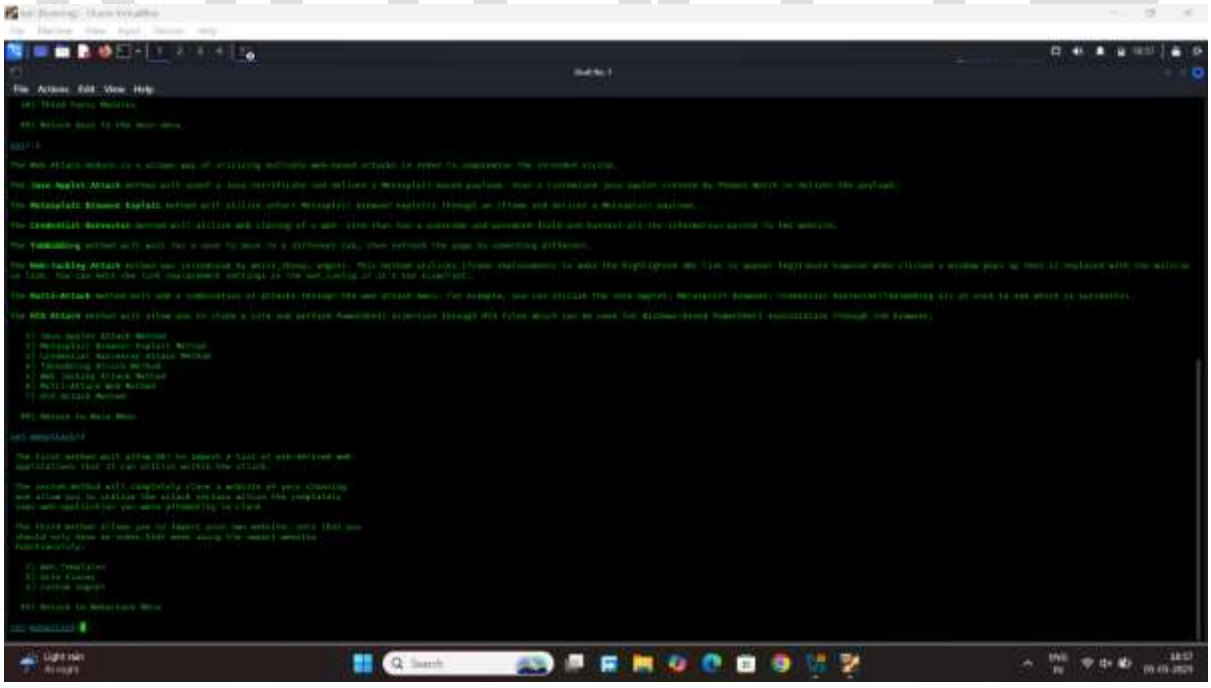


Step4: select the option credential harvester attack method



Step5: select the option

2 site cloner

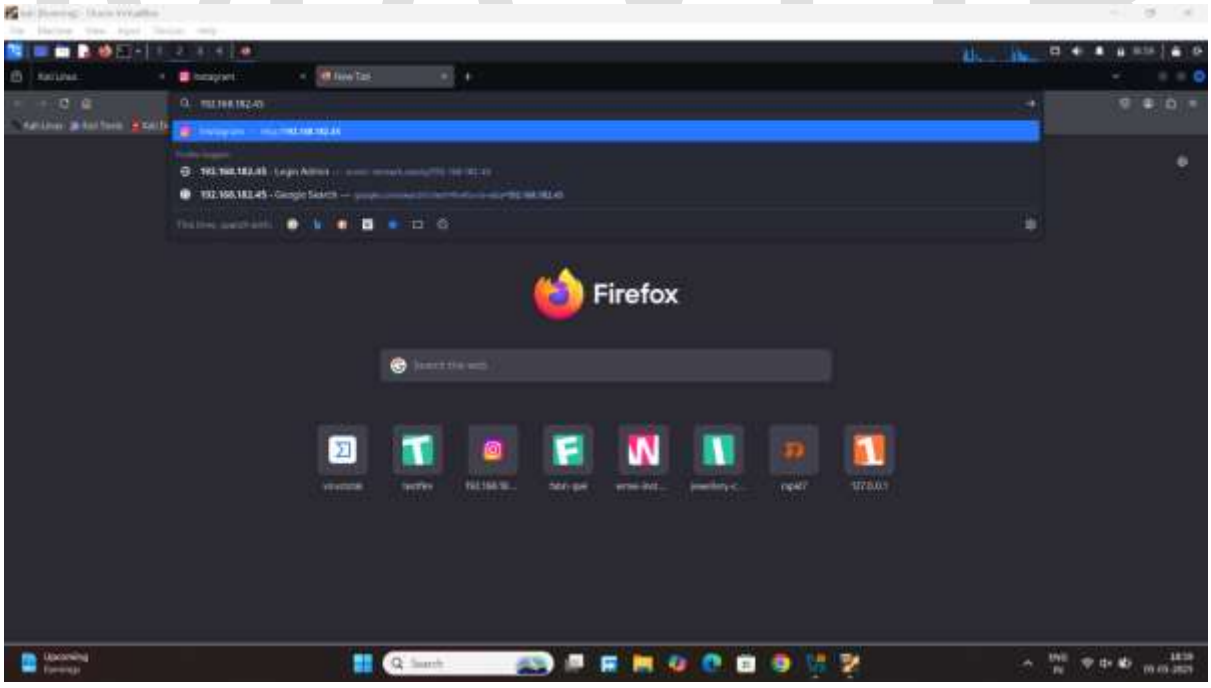


Step6: type the url

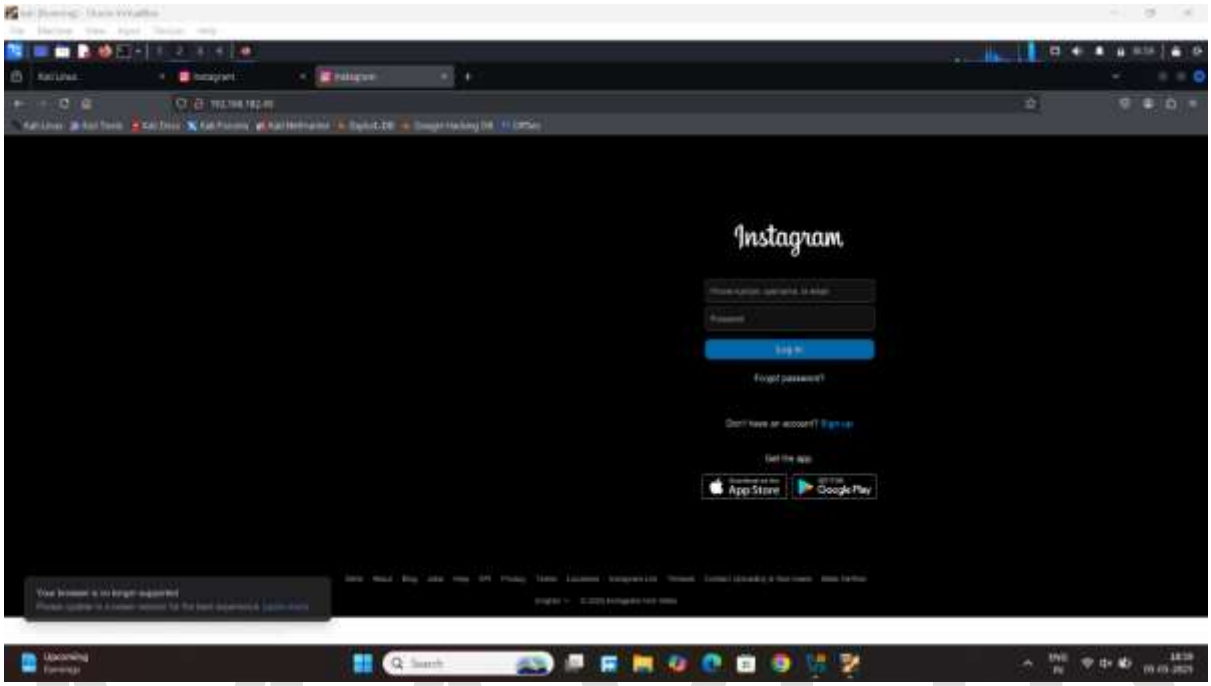
Example : https:// www.instagram.com

Step7: go to browser and type the kali linux ip

Example: 192.168.182.45



Result: successful open the site

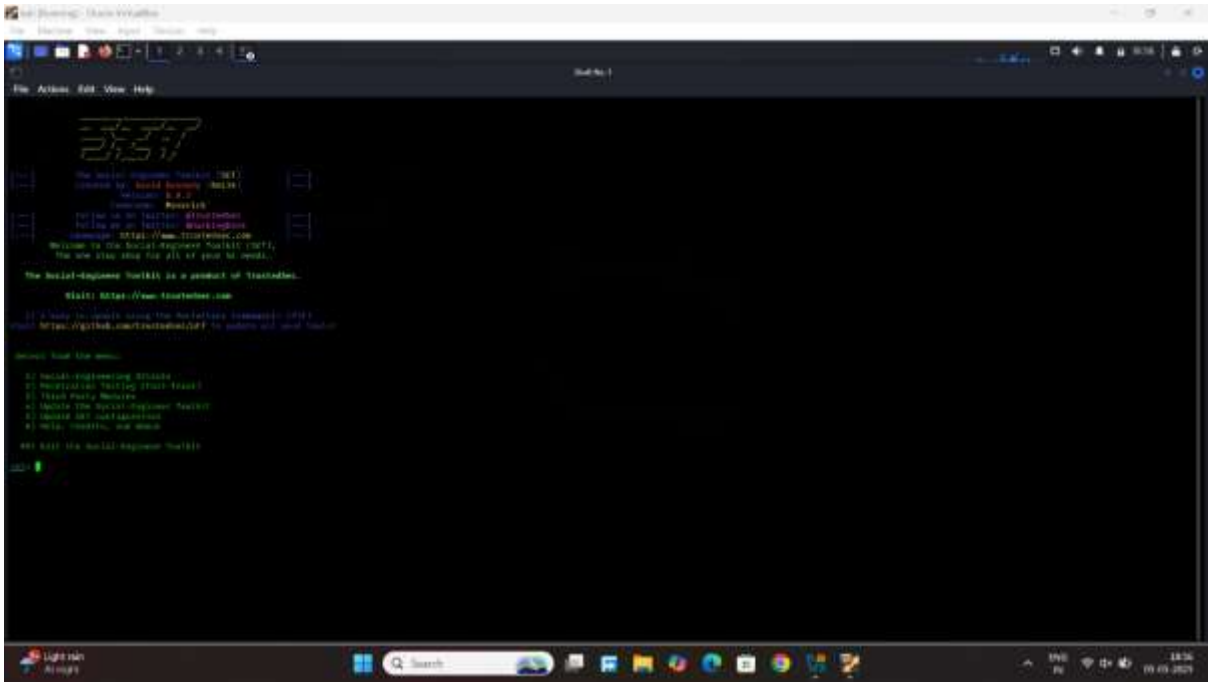


Task2: how to create fishing email and sent to the target using Social engineering tool

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

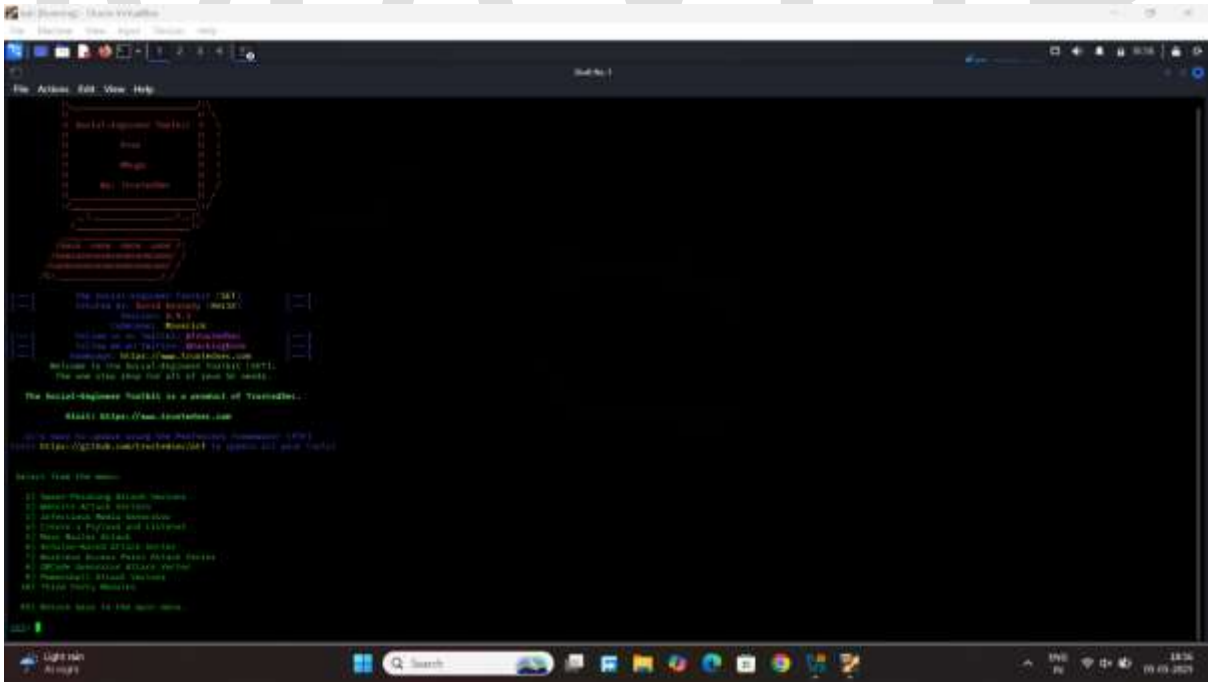
Step2: open the set tool kit choice the option

1 Social engineering

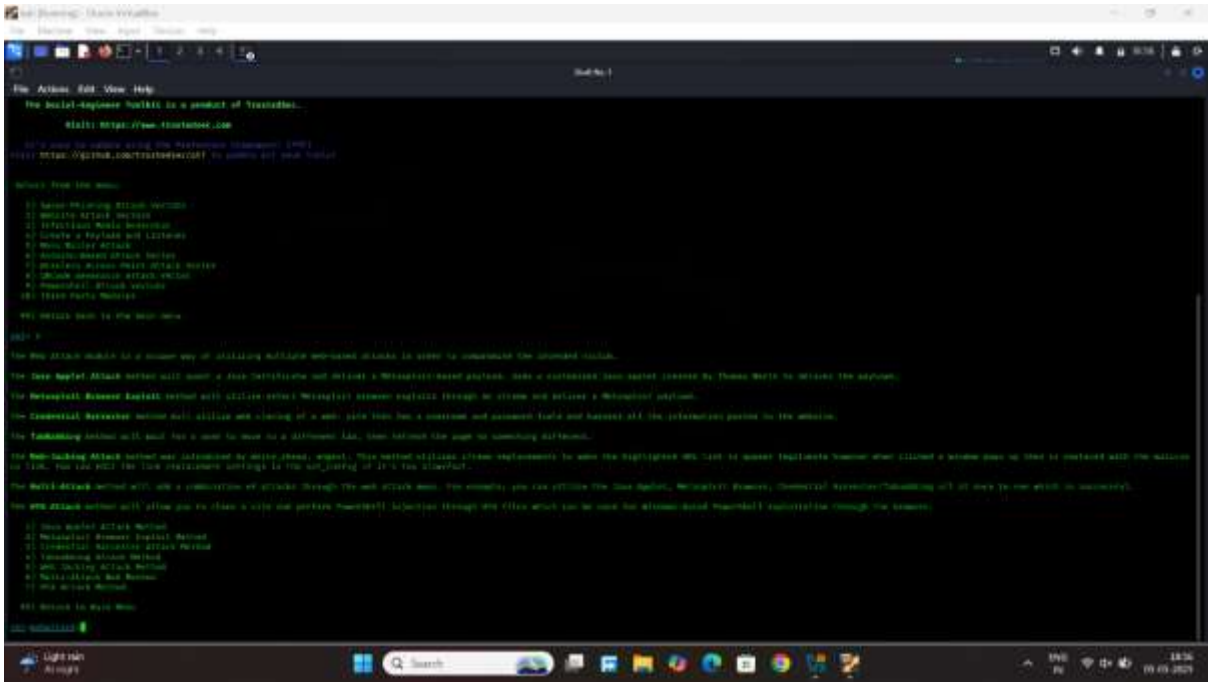


Step3: select the option

2 website attack vector

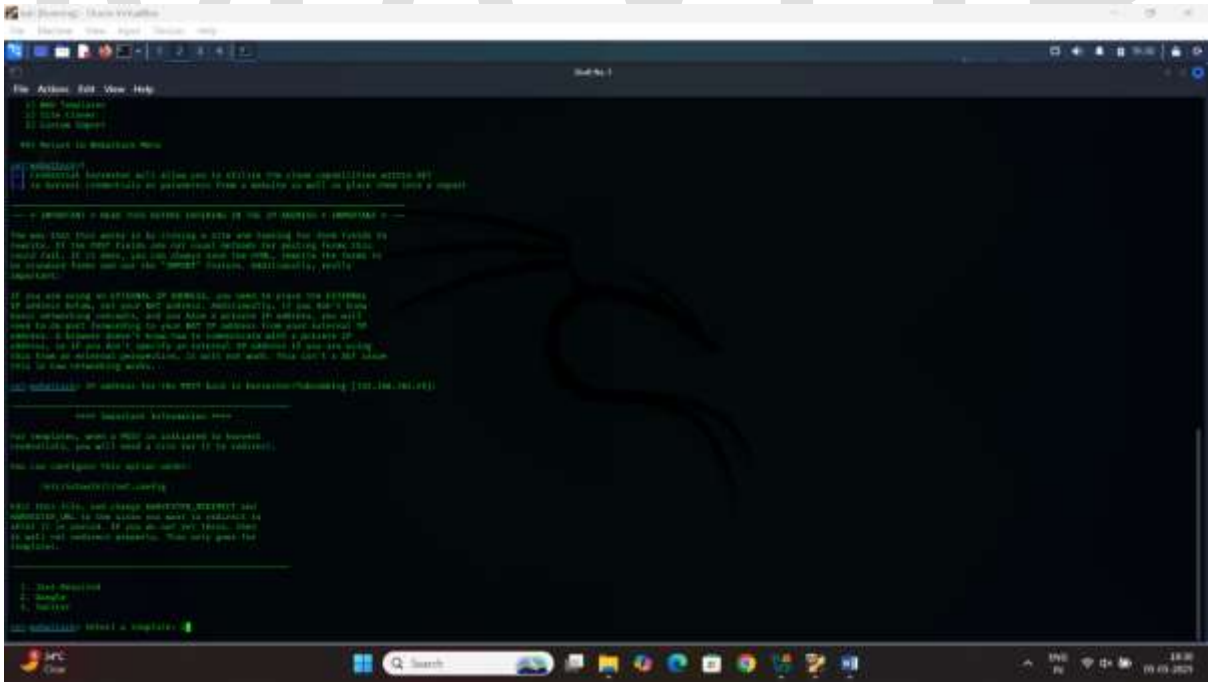


Step4: select the option credential harvester attack method



Step5: select the option

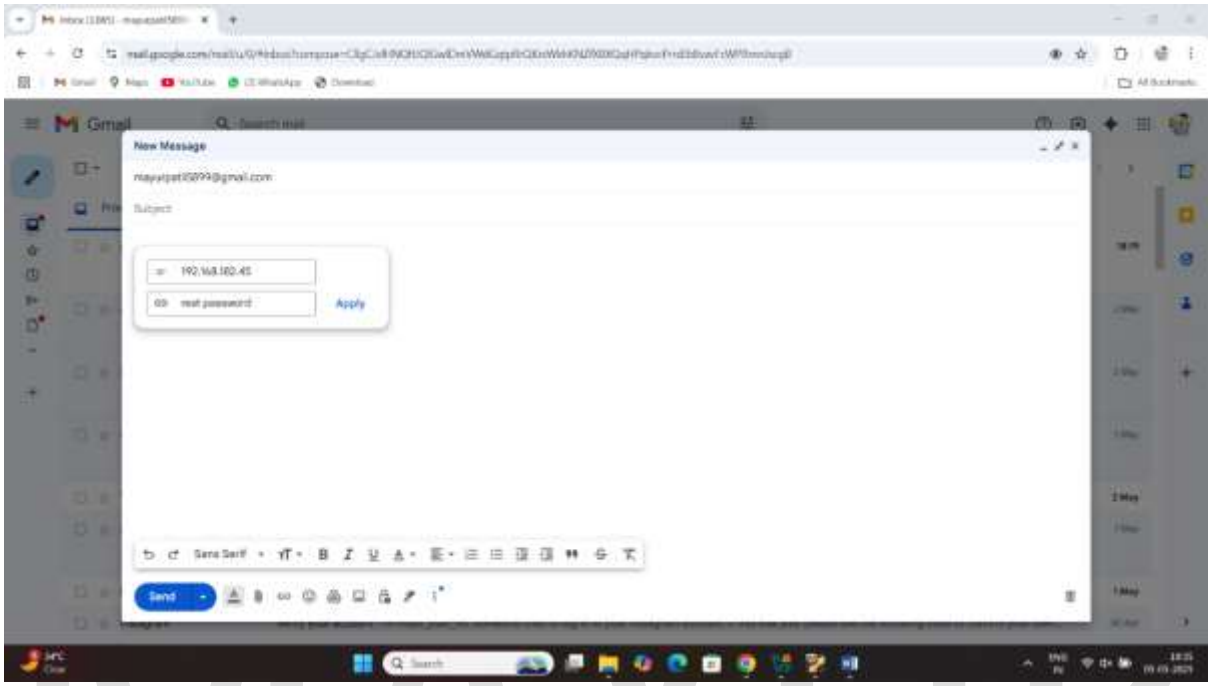
1 web cloner



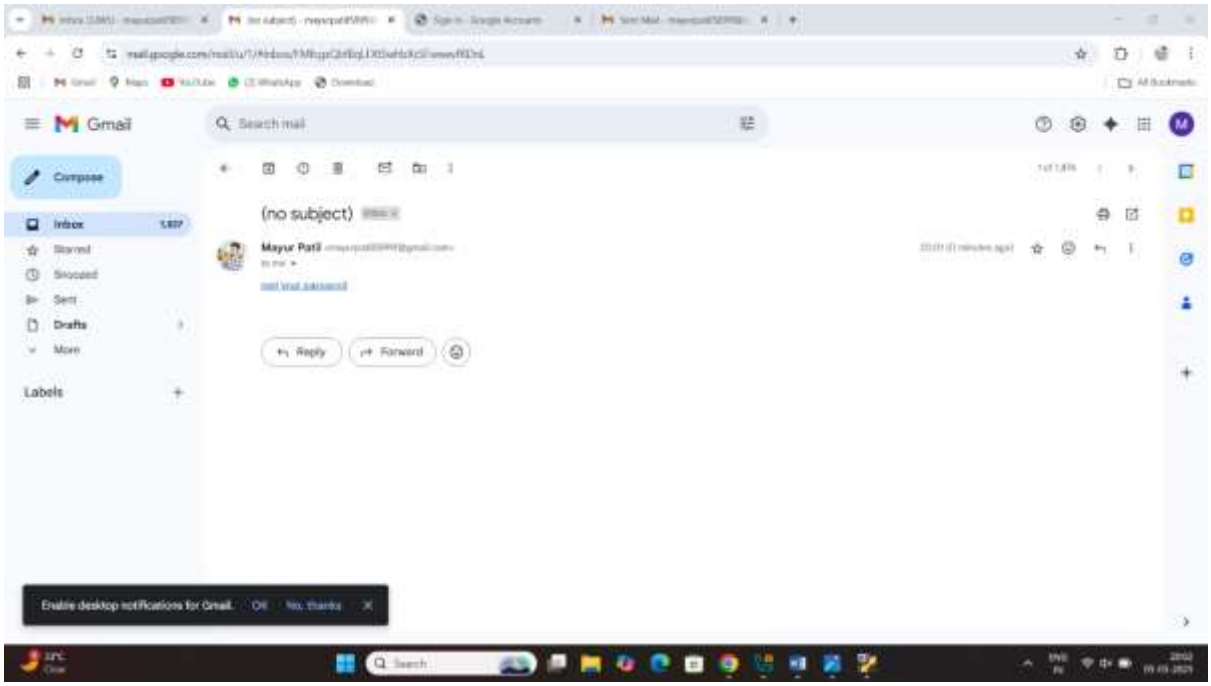
Step6: Select the google option

Step7: go to email Write the email for fishing email

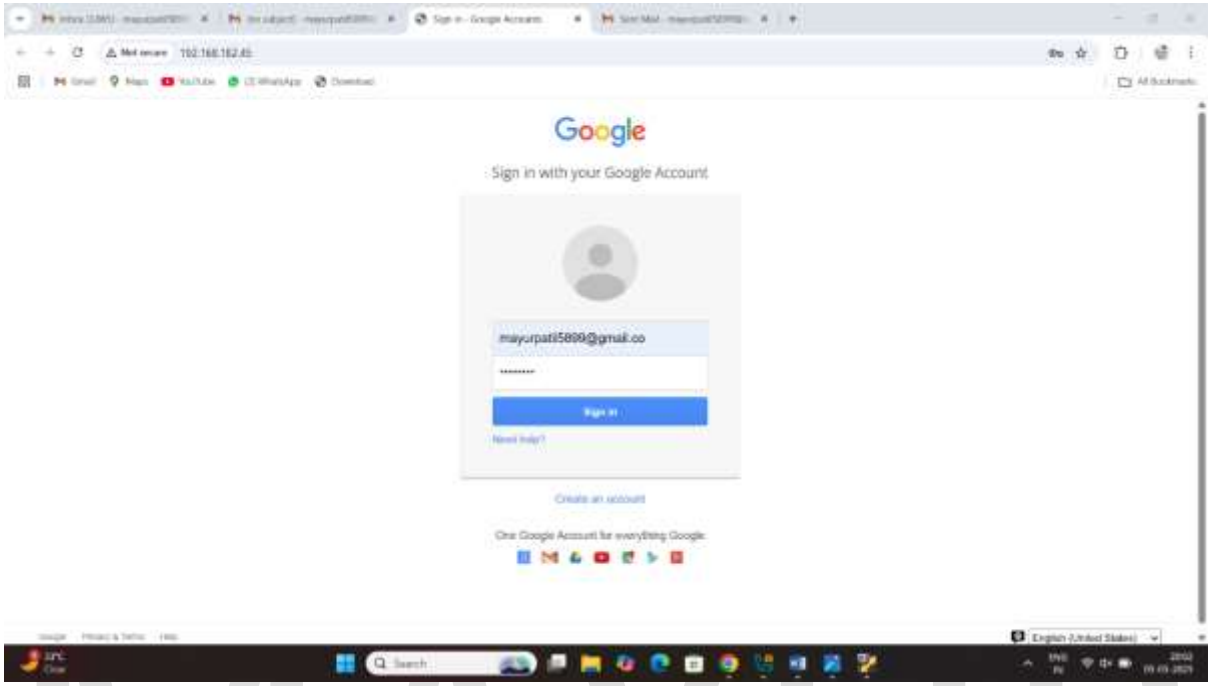
Step8: open the email create the fishing email click on insert link type the kali linux ip



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

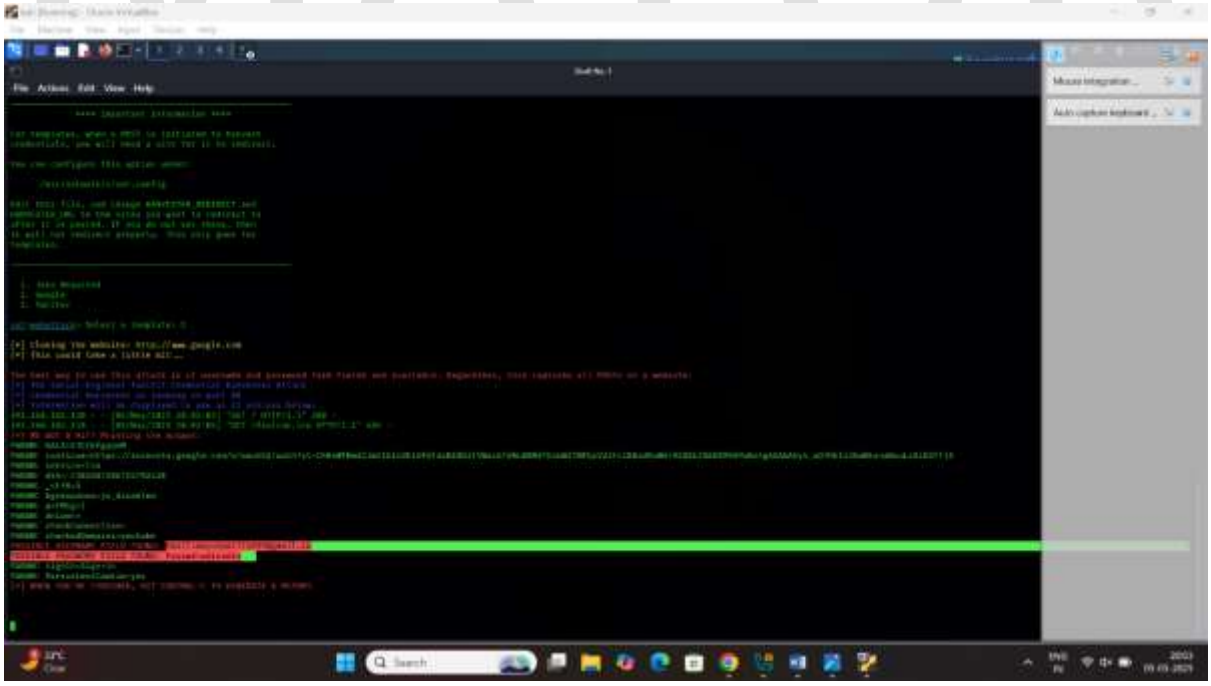


Open the target link and login gmail id



Click on sign

Result:



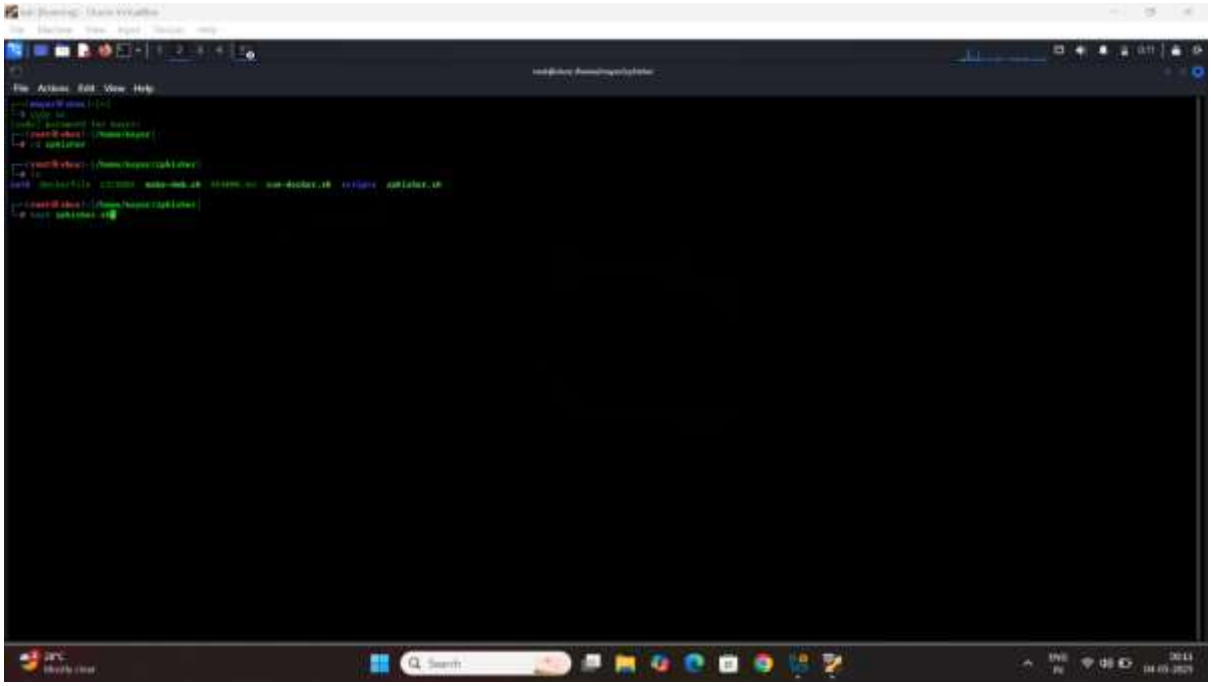
Task 3 using Zphisher Create Fishing Page

Step1:open the kali linux terminal download the zphisher for github

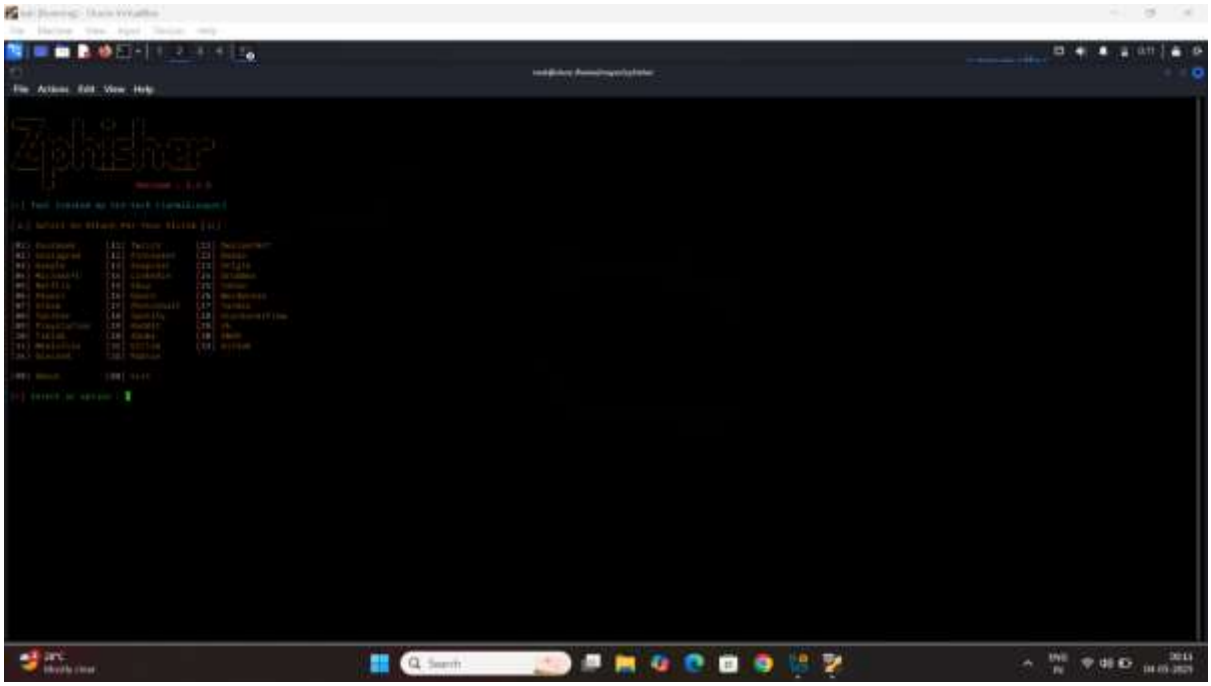
Command: cd zphisher /for this command are use go to file directory

Step2: open zphisher execute permission

Command: bash zpshier.sh

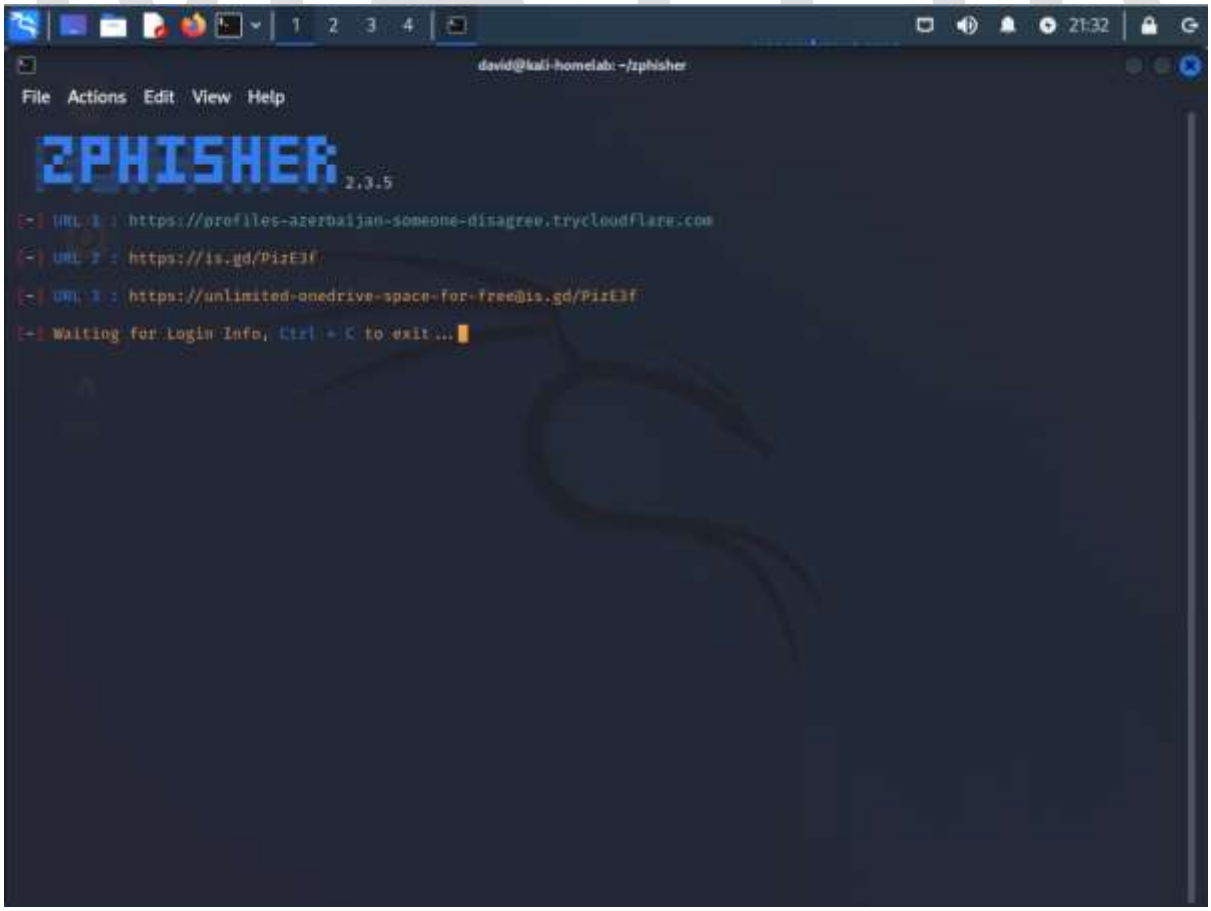


Step3: Select the one option for phishing page create



Step4: Select the 1 option /for Instagram phishing page create

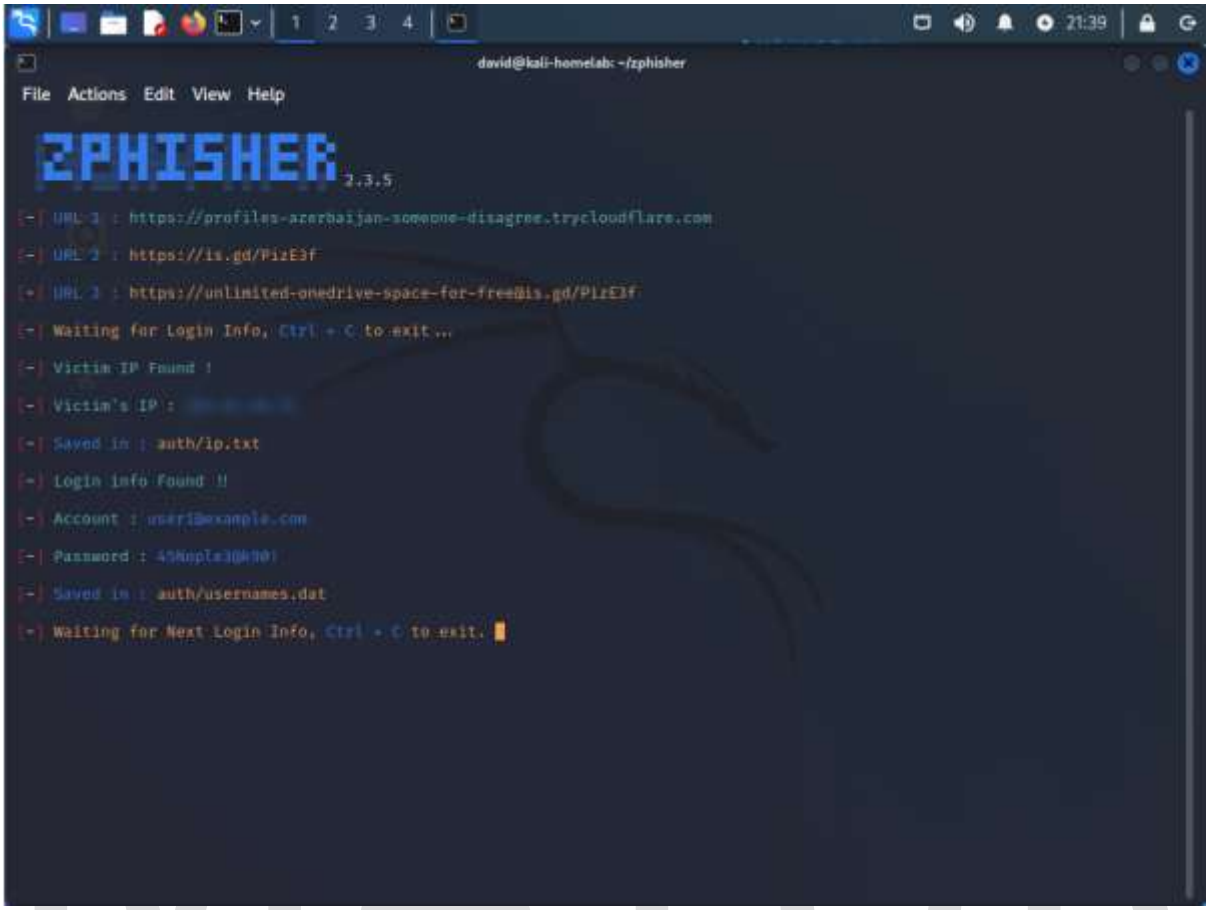
Step5: Atomatic the generate link



Step6: send the target fishing link

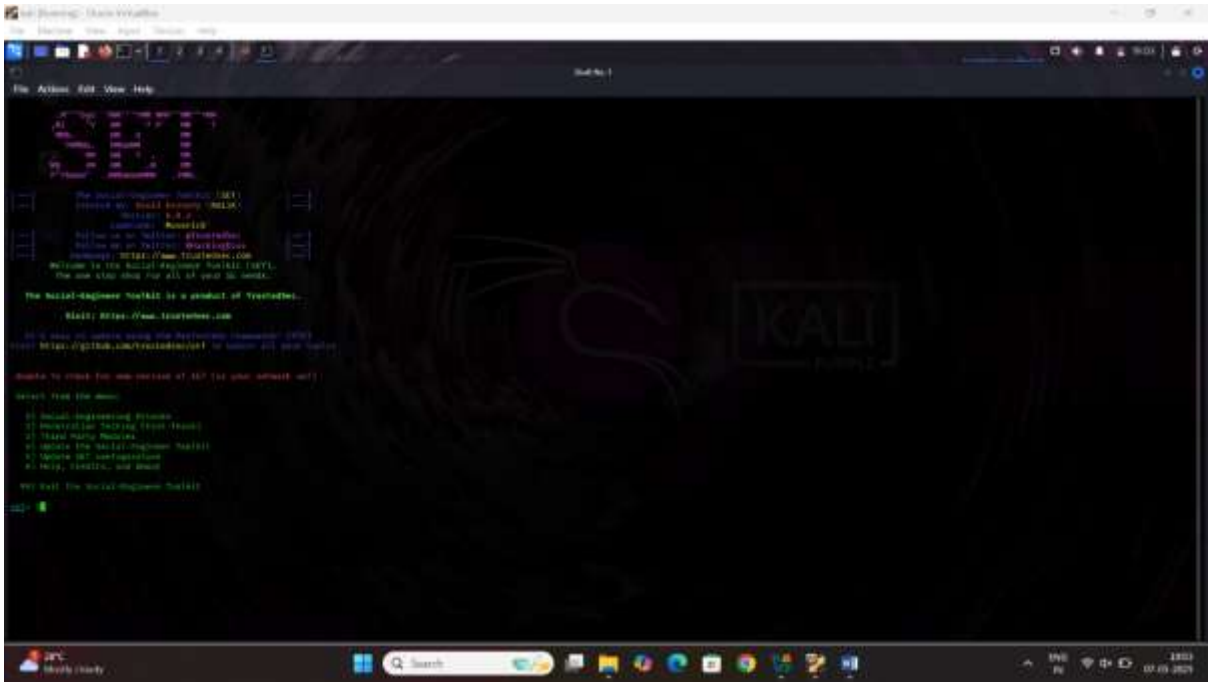
Step7: login the fishing link use id password hack the account

Result:

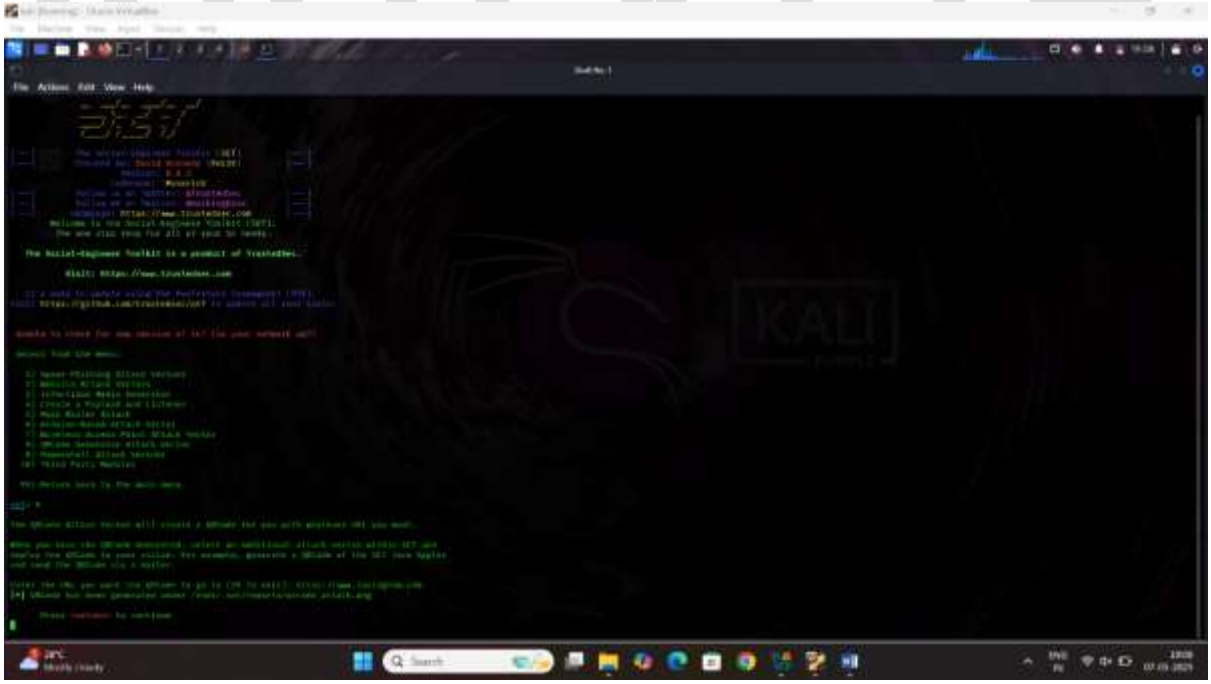


Extra Activity Using Set tool kit Generate the fake Q AR code

Step1: go to kali linux open the set tool kit



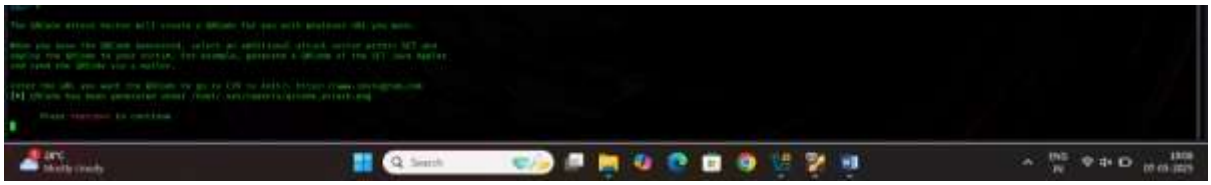
Step2: select the 1 options social engineering



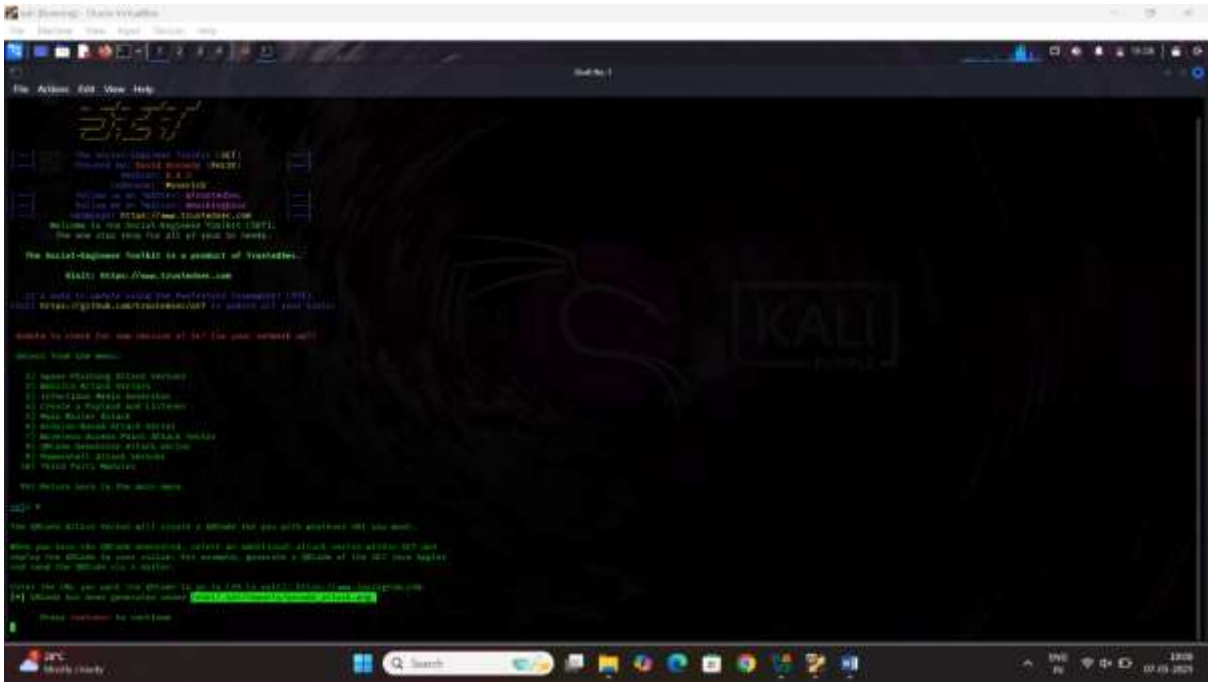
Step3: select the 8 option QR code Genretor attack vector

Step4: type the URL

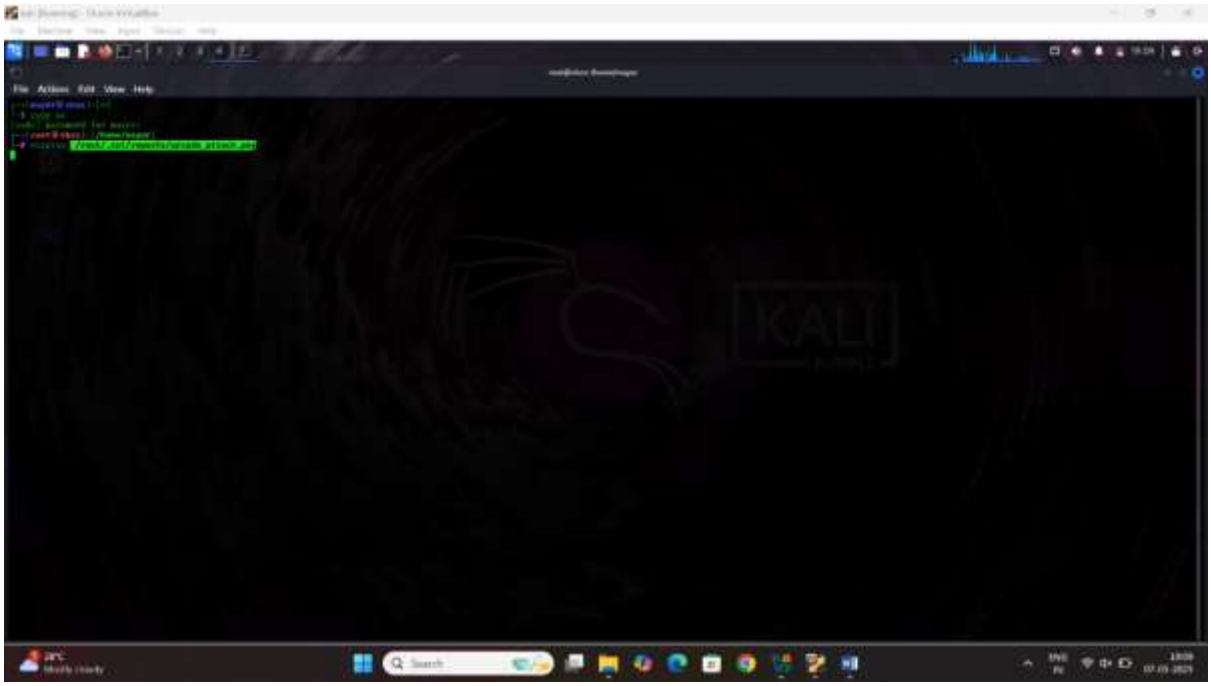
Example: https://instagram.com



Step5: copy the link as root



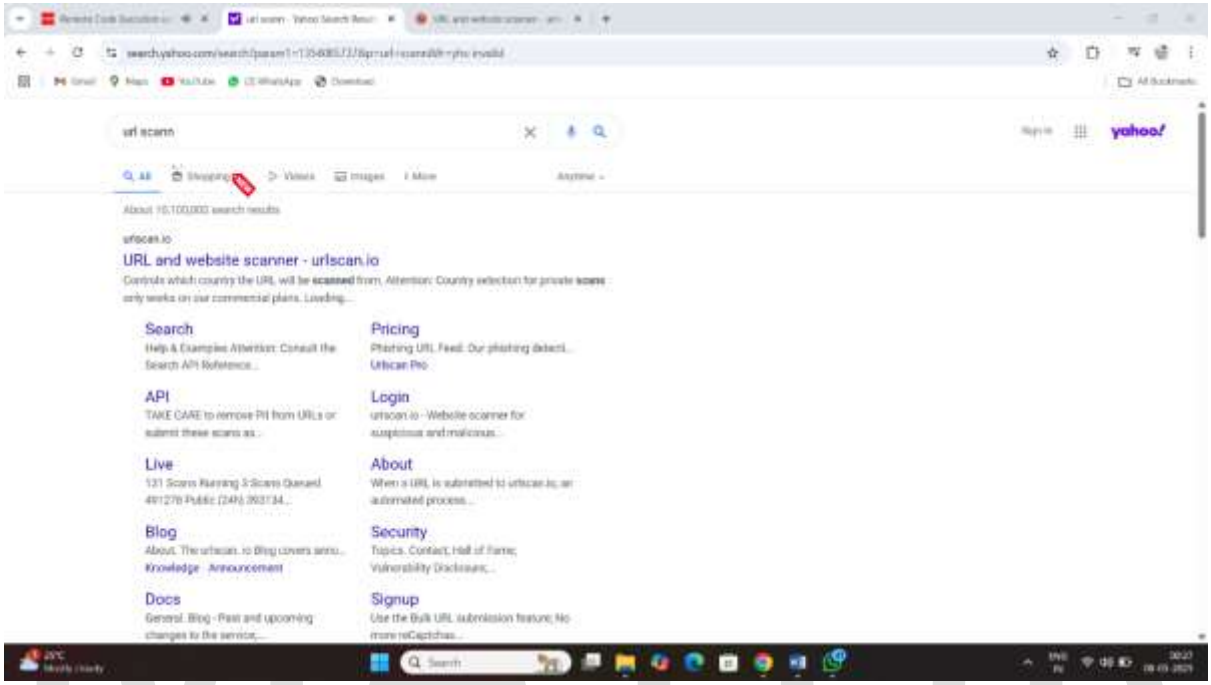
Step6: open the kali linux terminal copy the root link past it terminal

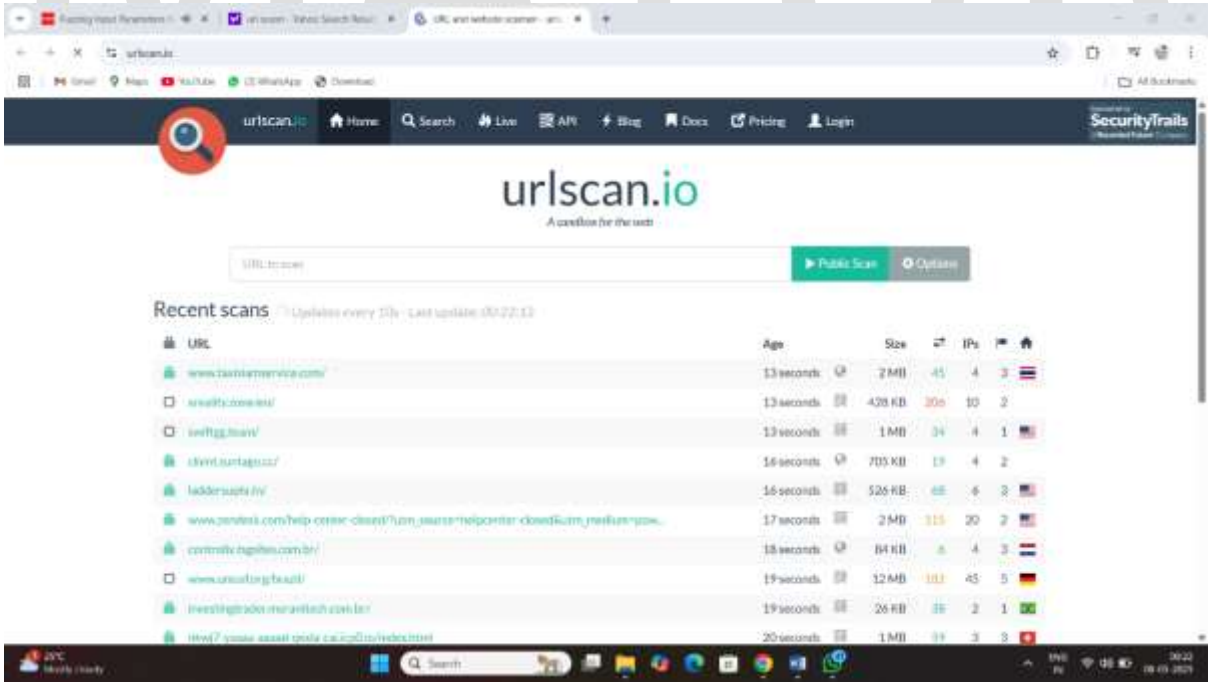


Result:

2 Extra Activity using website for fishing URL detections

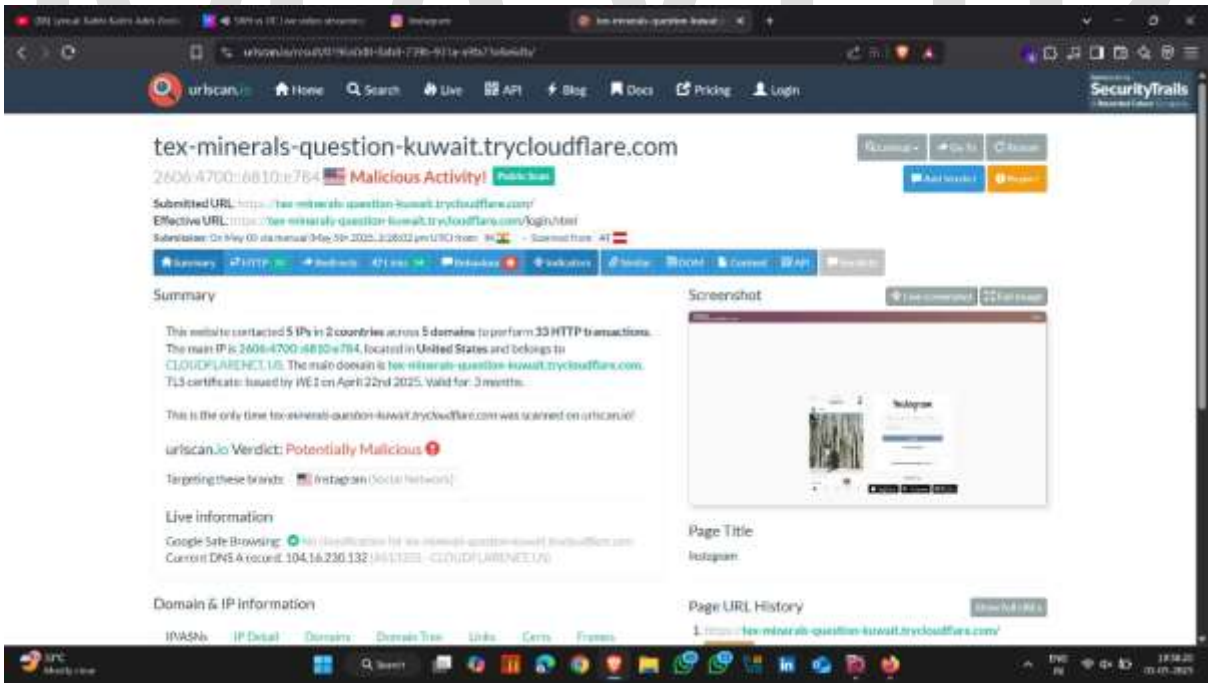
1 web site name: urlscan.io





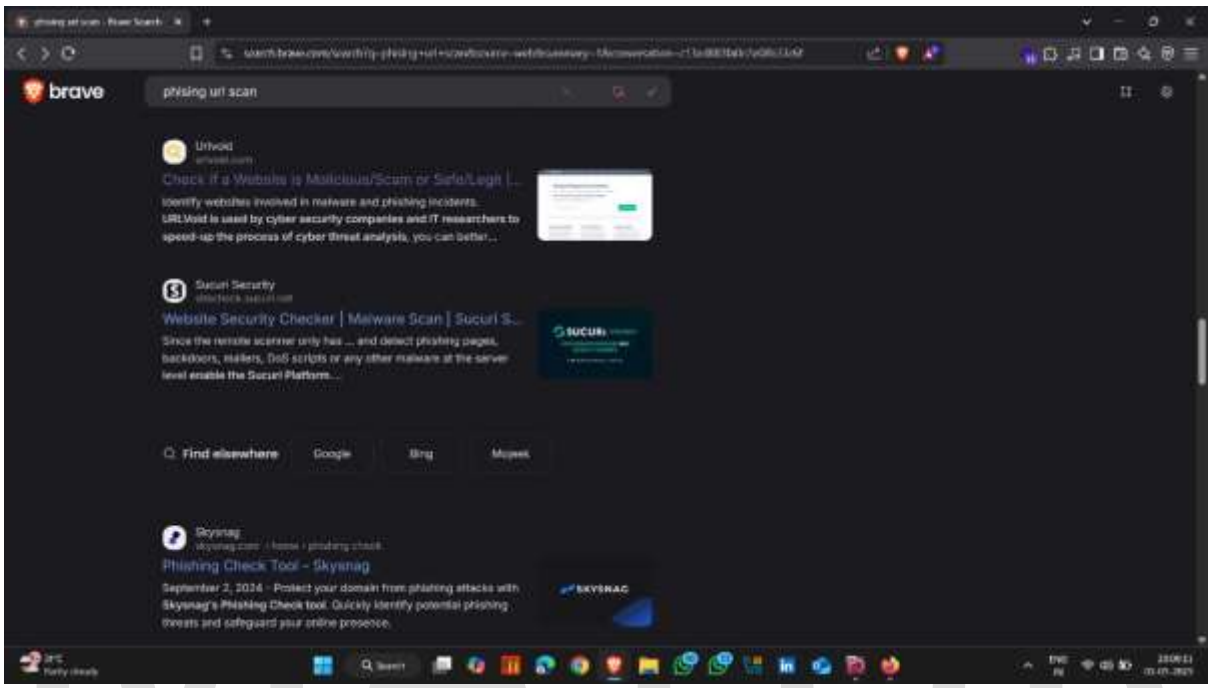

urlscan.io
Home
Search
Live
API
Blog
Docs
Pricing
Login
SecurityTrails
urlscan.io
A sandbox for the web
Public Scan
Options
Recent scans
URL
Age
Size
IPs

Result:

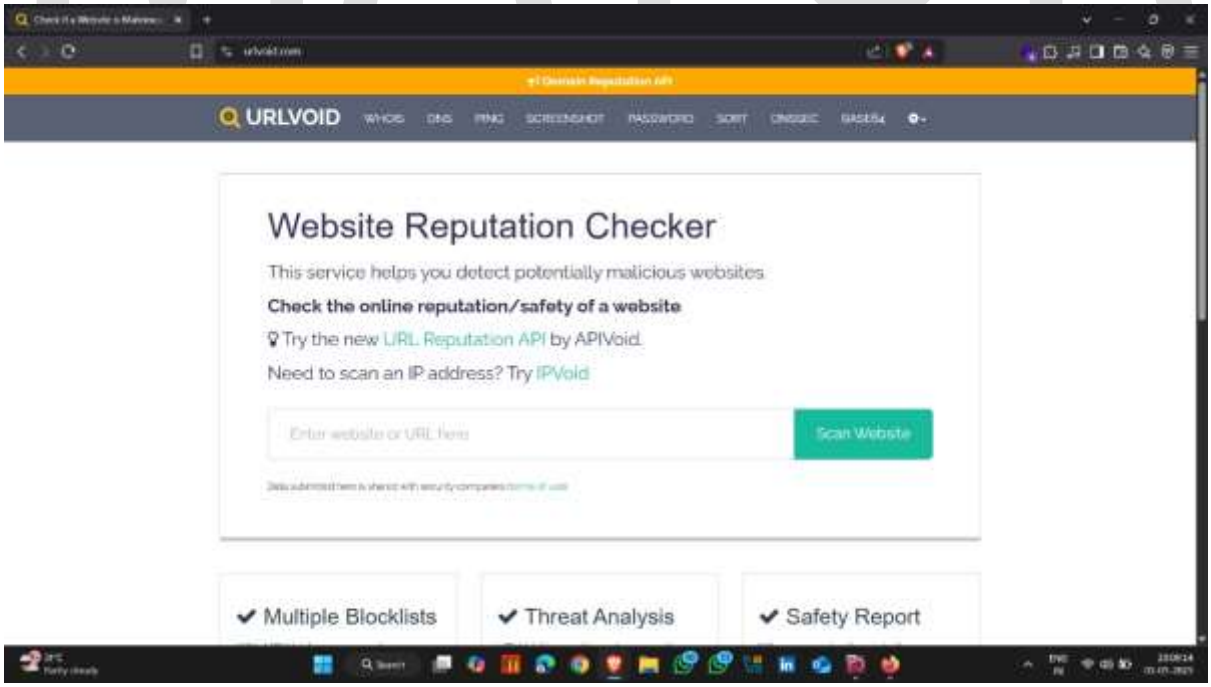

urlscan.io
Home
Search
Live
API
Blog
Docs
Pricing
Login
SecurityTrails
tex-minerals-question-kuwait.trycloudflare.com
Malicious Activity!
Summary
Screenshot
urlscan.io Verdict: Potentially Malicious
Live information
Page Title
Domain & IP information
Page URL History

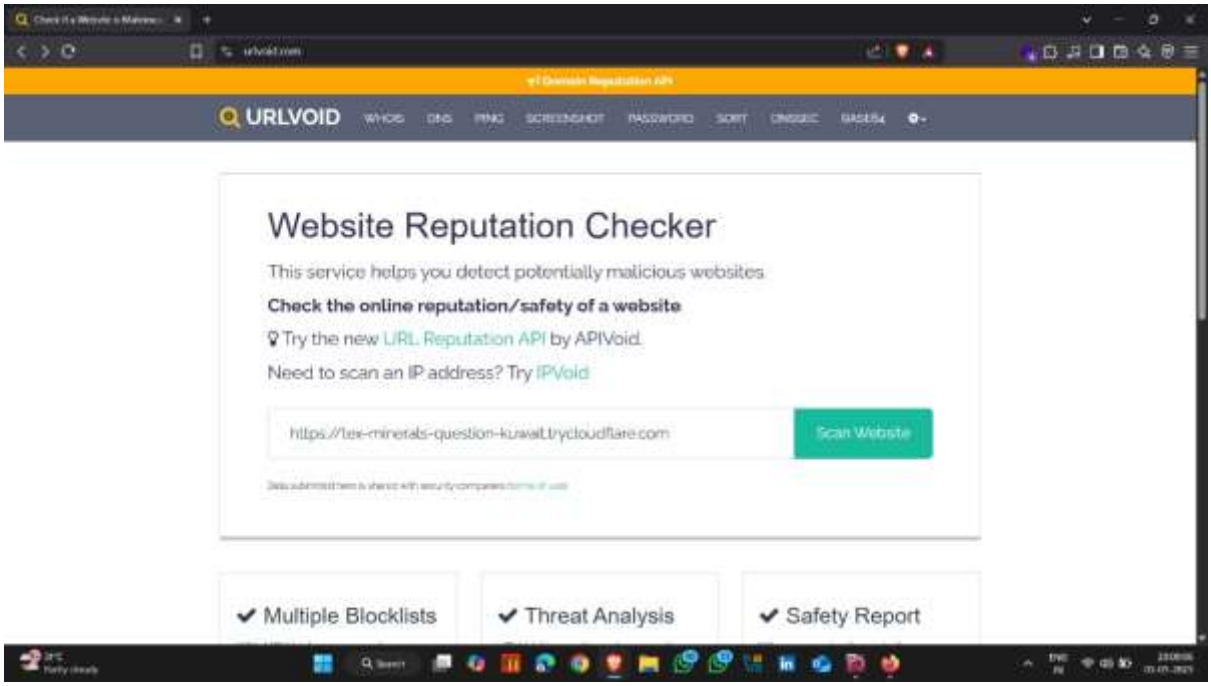
3 Extra Activity using website for fishing URL detections

1 web site name: URLvoid

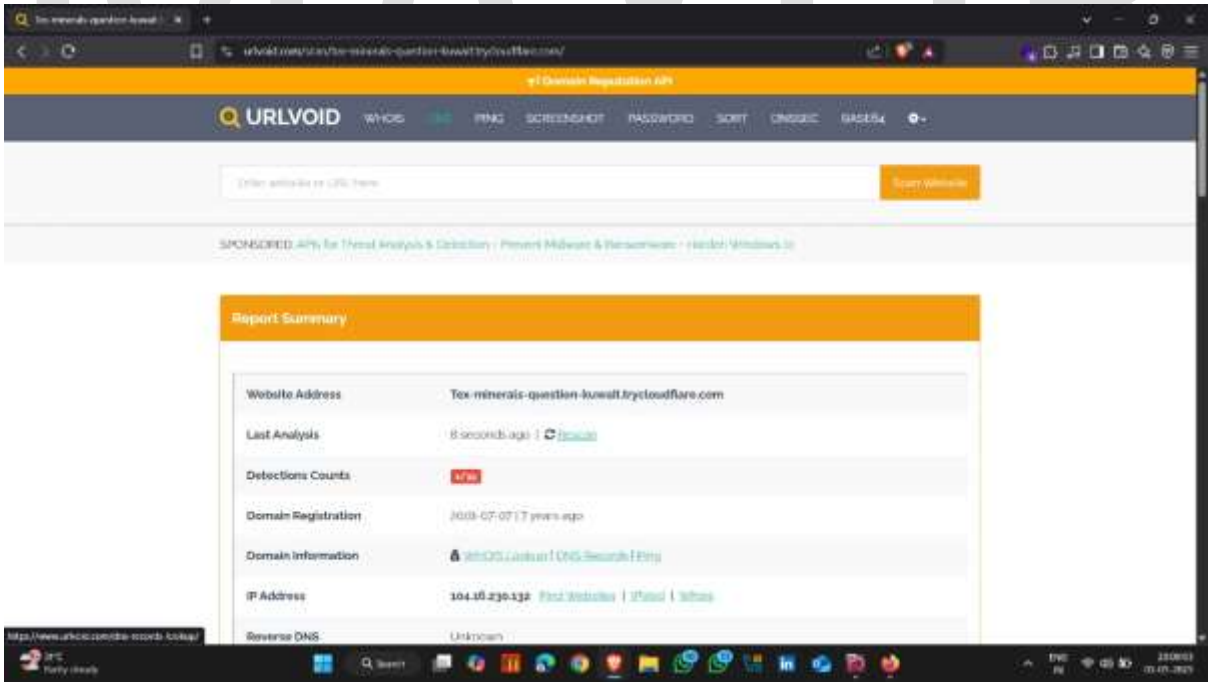


Open the web site

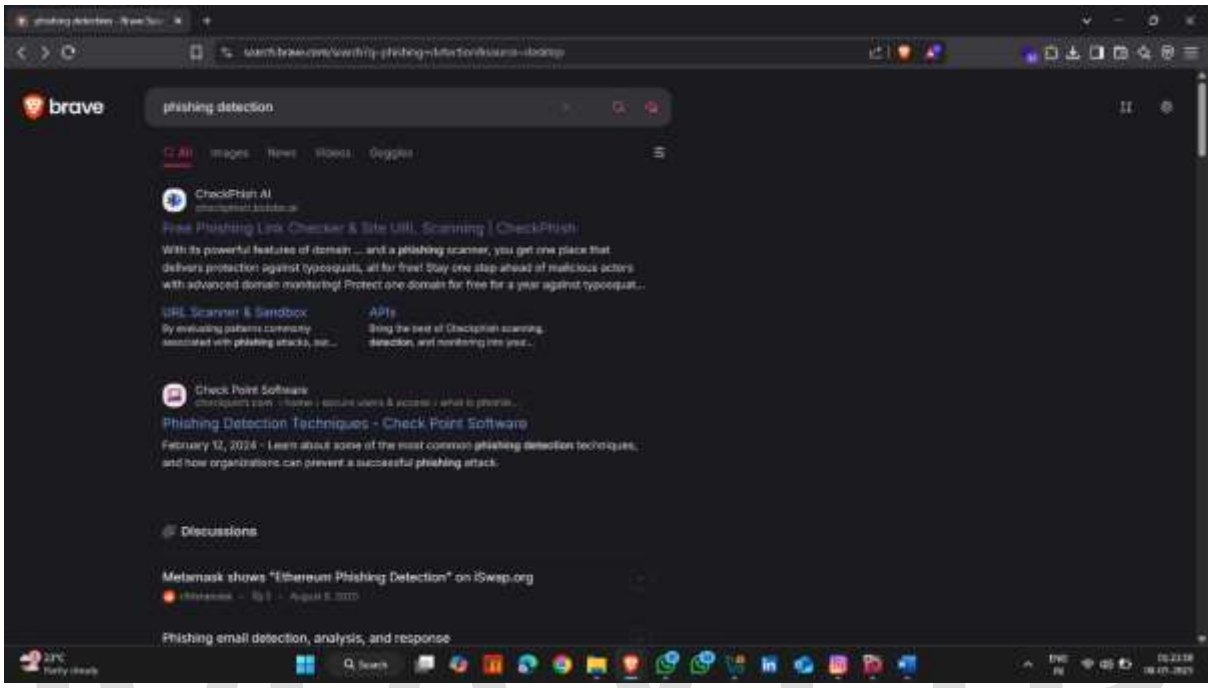


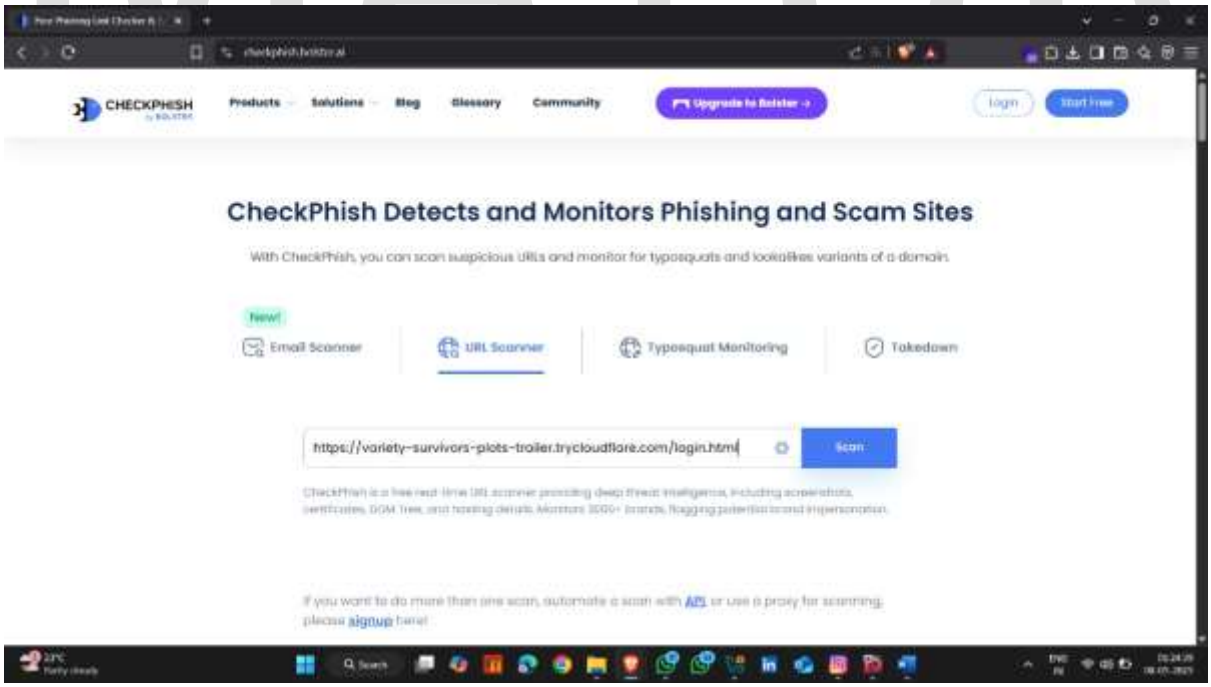

URLVOID
Website Reputation Checker
This service helps you detect potentially malicious websites
Check the online reputation/safety of a website
Try the new URL Reputation API by APIVoid
Need to scan an IP address? Try IPVoid
https://tex-minerals-question-kuwait.trycloudflare.com
Scan Website
✔ Multiple Blocklists
✔ Threat Analysis
✔ Safety Report

Result :

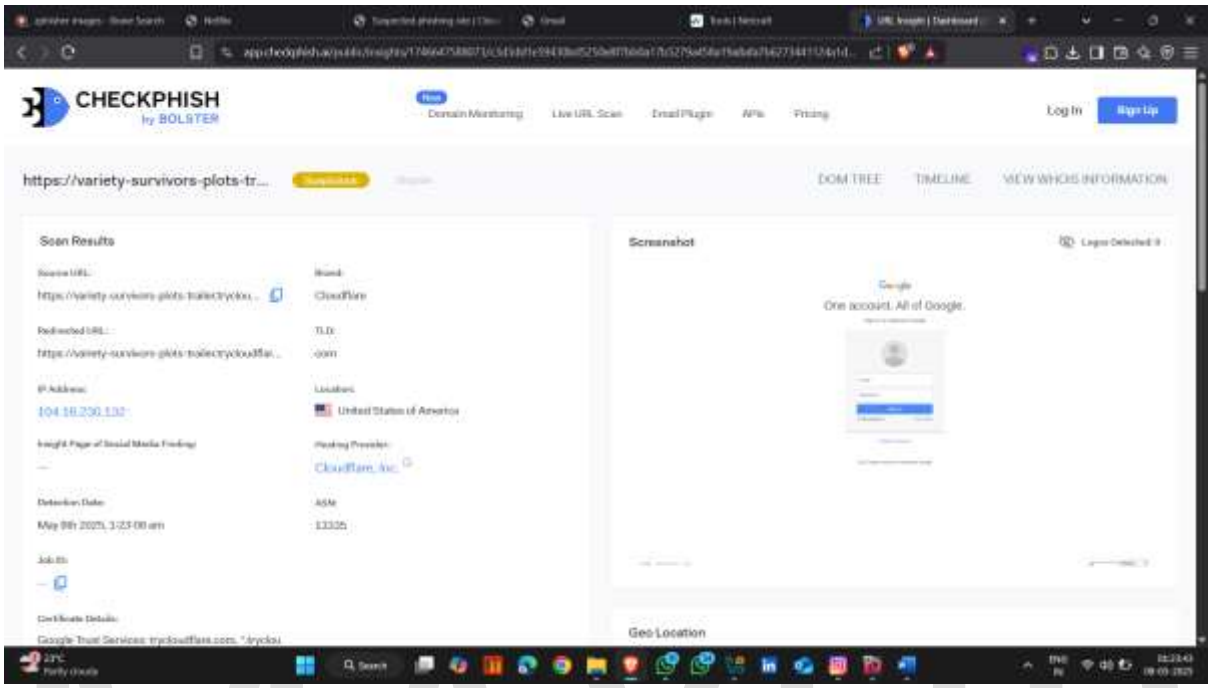

URLVOID
Report Summary
Website Address
tex-minerals-question-kuwait.trycloudflare.com
Last Analysis
Detections Counts
Domain Registration
Domain Information
IP Address
104.16.230.132
Reverse DNS

4 Extra Activity using website for fishing URL detections





Result:



How to Detected Phishing link

Detecting a phishing link involves analyzing both technical indicators and contextual clues. Here's how you can spot a phishing link:

🔍 1. Inspect the URL Carefully

- **Check the domain:** Look for misspelled names (e.g., `g00gle.com` instead of `google.com`).
- **Avoid shortened URLs:** Attackers use URL shorteners to hide malicious domains.

- **Look for extra words or characters:** Legit domains rarely have strange subdomains (e.g., `login.security-update.paypal.com.fakewebsite.com`).

□ 2. Hover Before You Click

- Hover over the link to **preview the actual destination** (in the browser status bar) before clicking.

🛑 3. Look for HTTPS — But Don't Rely on It

- A **valid HTTPS** connection (padlock icon) is necessary but **not sufficient**. Phishing sites can have SSL certificates too.

🛠️ 4. Use Online Link Scanners

- Tools like:
  - Google Safe Browsing
  - VirusTotal
  - PhishTank

🛍️ 5. Analyze the Email or Message Context

- Be wary of:
  - **Urgent language** ("Your account will be locked!")
  - **Unsolicited attachments or links**

- **Generic greetings** (“Dear user”)