Name : kunal jawale

Module 9 : Social Engineering

At its core, social engineering is not a cyber attack. Instead, social engineering is all about the psychology of persuasion: It targets the mind like your old school grifter or con man. The aim is to gain the trust of targets, so they lower their guard, and then encourage them into taking unsafe actions such as divulging personal information or clicking on web links or opening attachments that may be malicious.

Social engineering in cybersecurity refers to the manipulation of individuals through deception or persuasion to gain access to sensitive information or systems. It exploits human trust and vulnerabilities, often through tactics like impersonation, creating urgency, or dangling promises, to trick users into making mistakes or sharing confidential details.

Key Aspects of Social Engineering:

- **Psychological Manipulation:**

  Social engineering attacks rely on understanding and exploiting human psychology, such as trust, curiosity, and fear, to influence behavior.

- **Human Element:**

  Unlike technical vulnerabilities, social engineering attacks target individuals, making them a weak link in the security chain.

- **Diverse Attack Vectors:**

Name : kunal jawale

Social engineering can manifest in various forms, including phishing (emails), vishing (voice), and smishing (text messages), as well as physical attacks like tailgating.

- **Pretexting:**

  A common technique where attackers craft a believable story or scenario to gain trust and deceive the victim into revealing information.

- **Baiting:**

  Enticing users with a seemingly attractive offer or free item to lure them into clicking on malicious links or downloading harmful software.

- **Phishing:**

- One of the most prevalent forms, using emails or messages to impersonate legitimate sources and trick users into sharing sensitive information.

- **Spear Phishing:**

  A targeted form of phishing where attackers craft emails that specifically target individuals or organizations with customized information to increase their chance of success.

- **Watering Hole Attacks:**
  Attackers compromise websites that are frequented by a specific group of individuals, allowing them to intercept information from those who visit the website.

Examples of Social Engineering Attacks:

- A scammer might impersonate IT support, claiming there's a security issue and requesting login credentials to "resolve" it.
- An email might appear to be from a trusted source, like a bank, with a request to update account information through a malicious link.
- A phone call might claim to be from a prize winner, asking for personal information to claim the prize.
- A physical attack might involve tailgating (following someone into a secured area without proper authorization).

Protecting Against Social Engineering:

- **Cybersecurity Awareness Training:**

  Educating employees and users about social engineering tactics and how to recognize them is crucial.

- **Security Policies and Procedures:**

  Implementing clear policies and procedures regarding information sharing, password management, and security protocols can help prevent mistakes.

Name : kunal jawale

- **Email and Message Verification:**

  Being cautious about emails and messages from unknown or suspicious sources, and verifying their legitimacy before clicking on links or attachments.

- **Suspiciousness and Caution:**

  Encouraging users to be suspicious of requests for sensitive information, especially when they are unexpected or appear urgent.

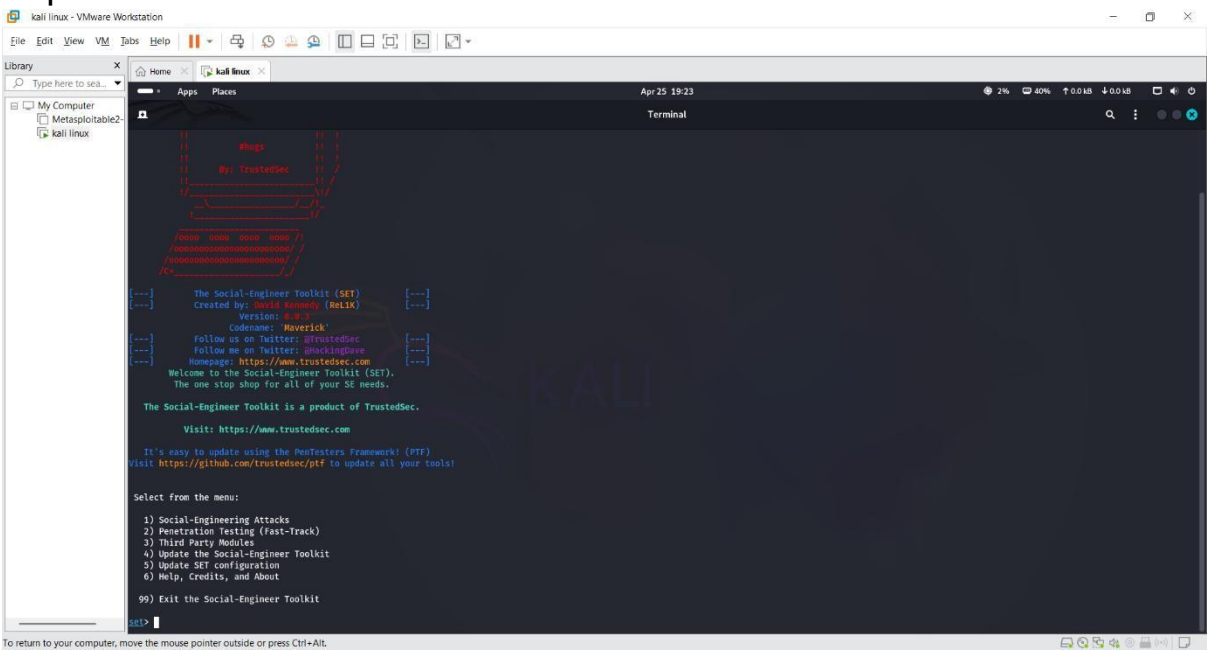
- **Multi-Factor Authentication:**

  Using multi-factor authentication can add an extra layer of security, requiring multiple forms of verification to access accounts.

- **Regular Security Audits:**
  Conducting regular security audits can help identify vulnerabilities and weaknesses in security protocols.

/ Here are some technique using setoolkit in kali linux generate a phishing attack .

Step 1 : open kali linux
Step 2 : go to exploitation tools
Step 3 : click on setoolkit

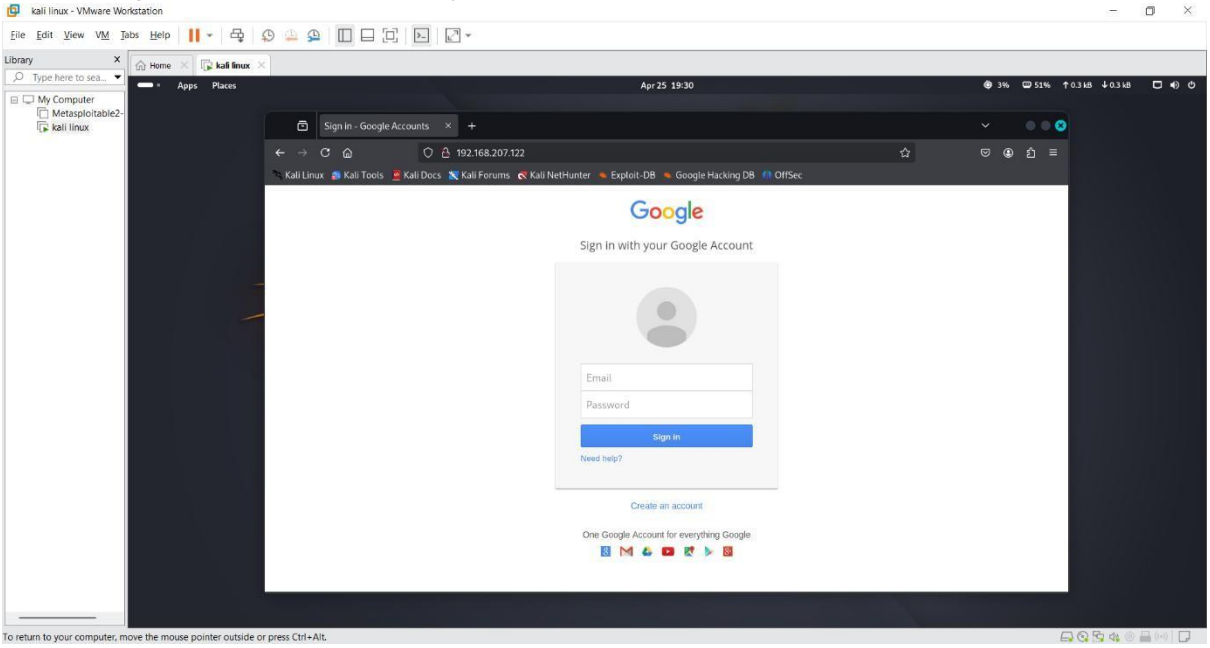


Step 4 : choose 1 social enginnering attack
Step 5 : go for 2 website attack vectors
Step 6 : go for 3 , credential harvester attack method
Step 7 : go for 1 , web tamplets

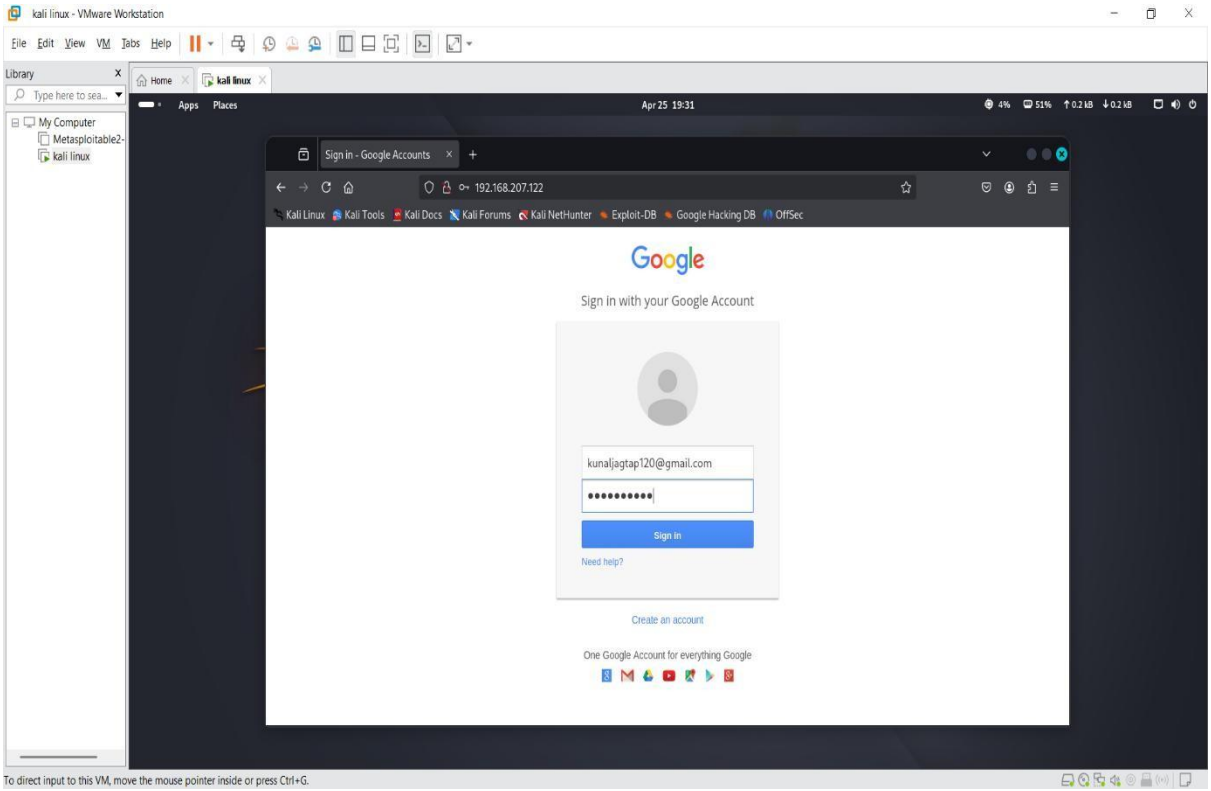
Name : kunal jawale

Step 8 : select 2 for google

Step 9 : go to browser and type linux IP

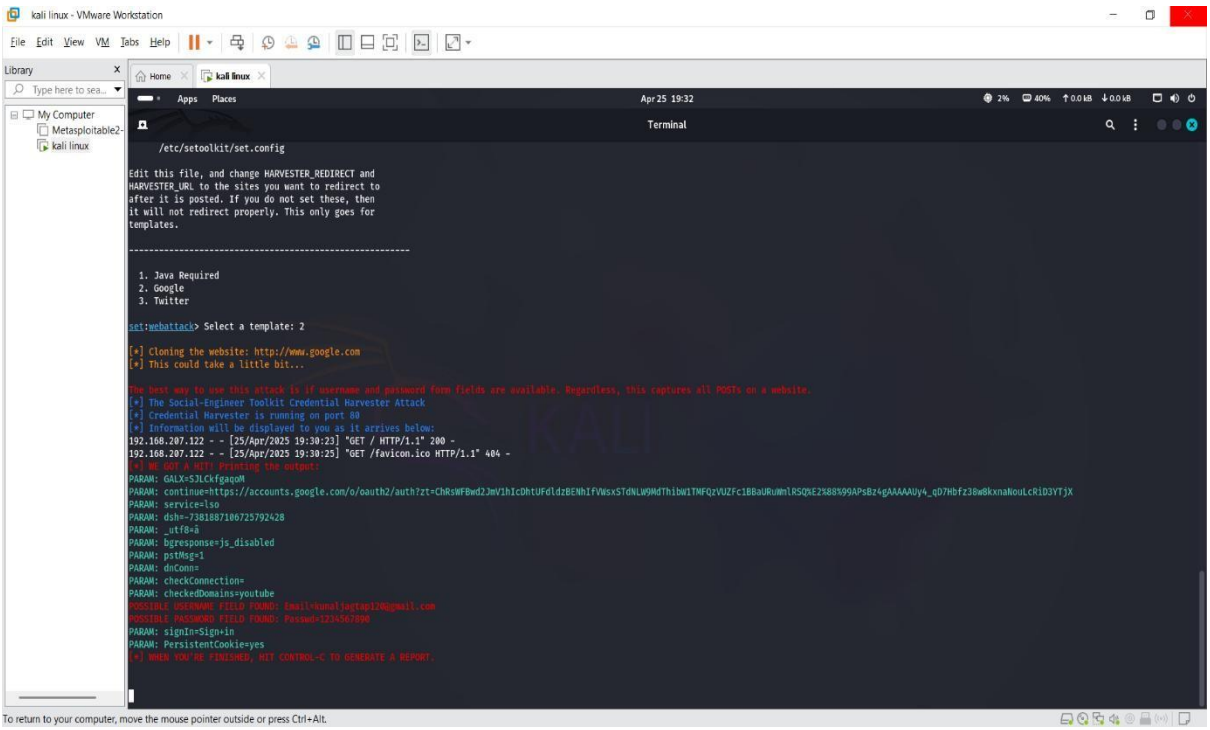


Step 10 : fill the information email and password



Step 11: open terminal and see the result phishing done successfully .

Name : kunal jawale



/ Here are some tools in kali linux for phishing and their information

O Zphisher :

Zphisher is a powerful open-source tool Phishing Tool. It became very popular nowadays and is used to do phishing attacks on Target. Zphisher is easier than Social Engineering Toolkit. It contains some templates generated by a tool called Zphisher and offers phishing templates webpages for 33 popular sites **such as Facebook, Instagram, Google, Snapchat, GitHub, Yahoo, Proton mail, Spotify, Netflix, LinkedIn, WordPress, Origin, Steam, Microsoft, etc**. It also provides an option to use a custom template if someone wants. This tool makes it easy to perform a phishing attack. Using this tool you can perform phishing in (wide area network). This tool can be used to get credentials such as **id, password.**

Name : kunal jawale

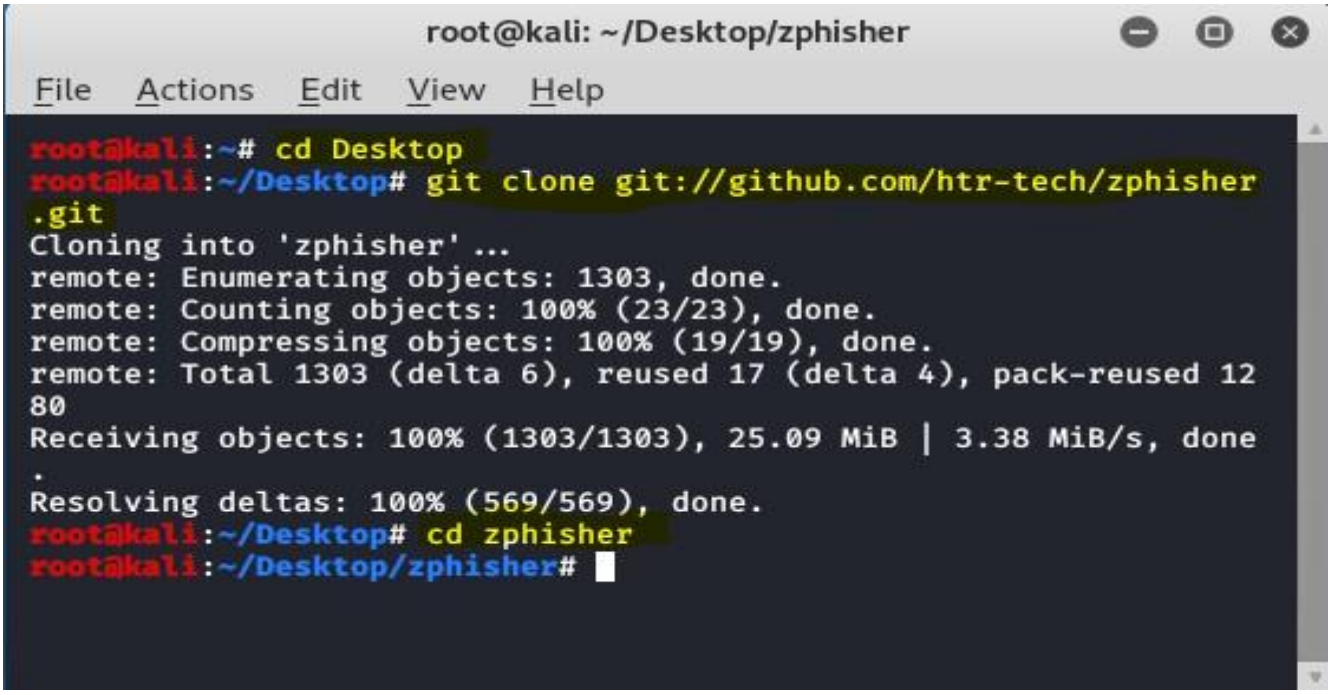
Uses and Features of Zphisher:

- Zphisher is open source tool.
- Zphisher is a tool of Kali Linux.
- Zphisher is used in Phishing attacks.
- Zphisher tool is a very simple and easy tool.
- Zphisher tool is a very simple and easy tool.
- Zphisher tool is a lightweight tool. It does not take extra space.
- Zphisher is written in bash language.
- Zphisher creates phishing pages for more than 33 websites.
- Zphisher creates phishing pages of popular sites such as Facebook, Instagram, Google, Snapchat, Github, Yahoo, Protonmail, Spotify, Netflix, LinkedIn, WordPress, Origin, Steam, Microsoft, etc

Step 1: To install the tool first go to the desktop directory and then install the tool using the following commands.

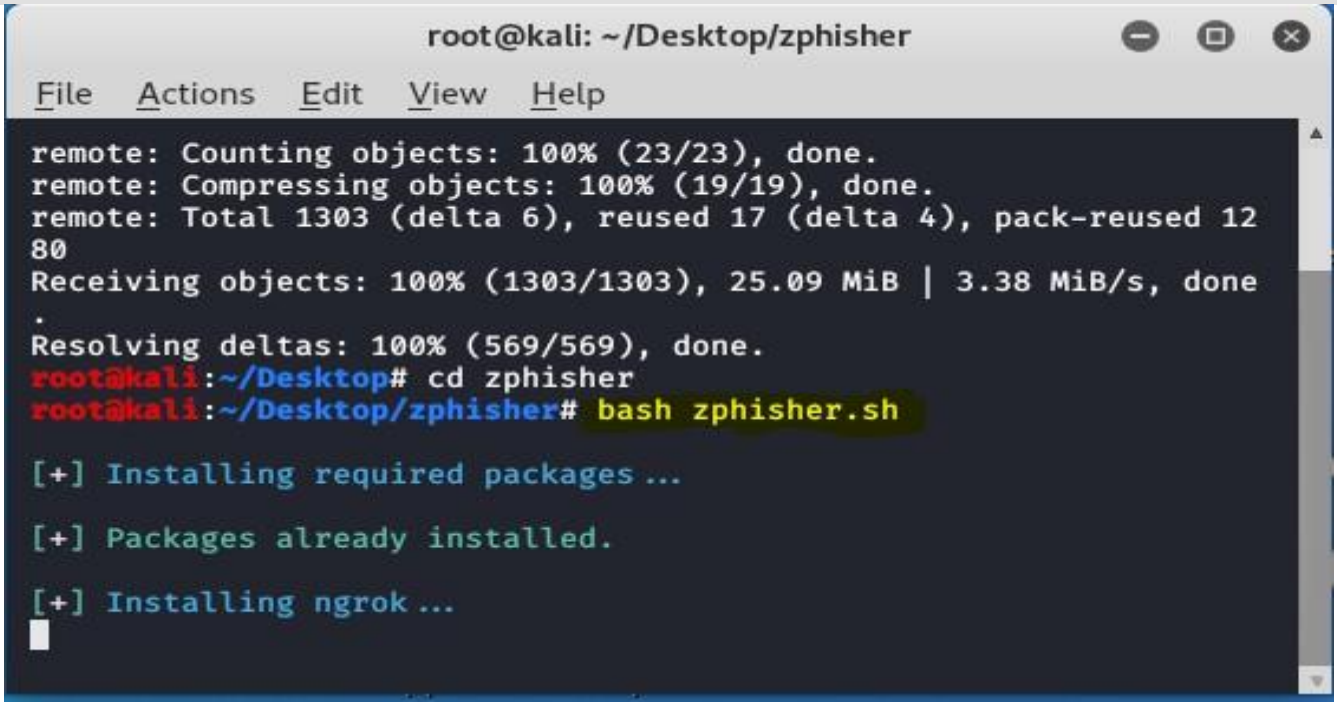
```
cd Desktop
git clone git://github.com/htr-tech/zphisher.git
cd zphisher
```

Name : kunal jawale



Step 2: Now you are in zphisher directory , use the following command to run the tool.

```
bash zphisher.sh
```

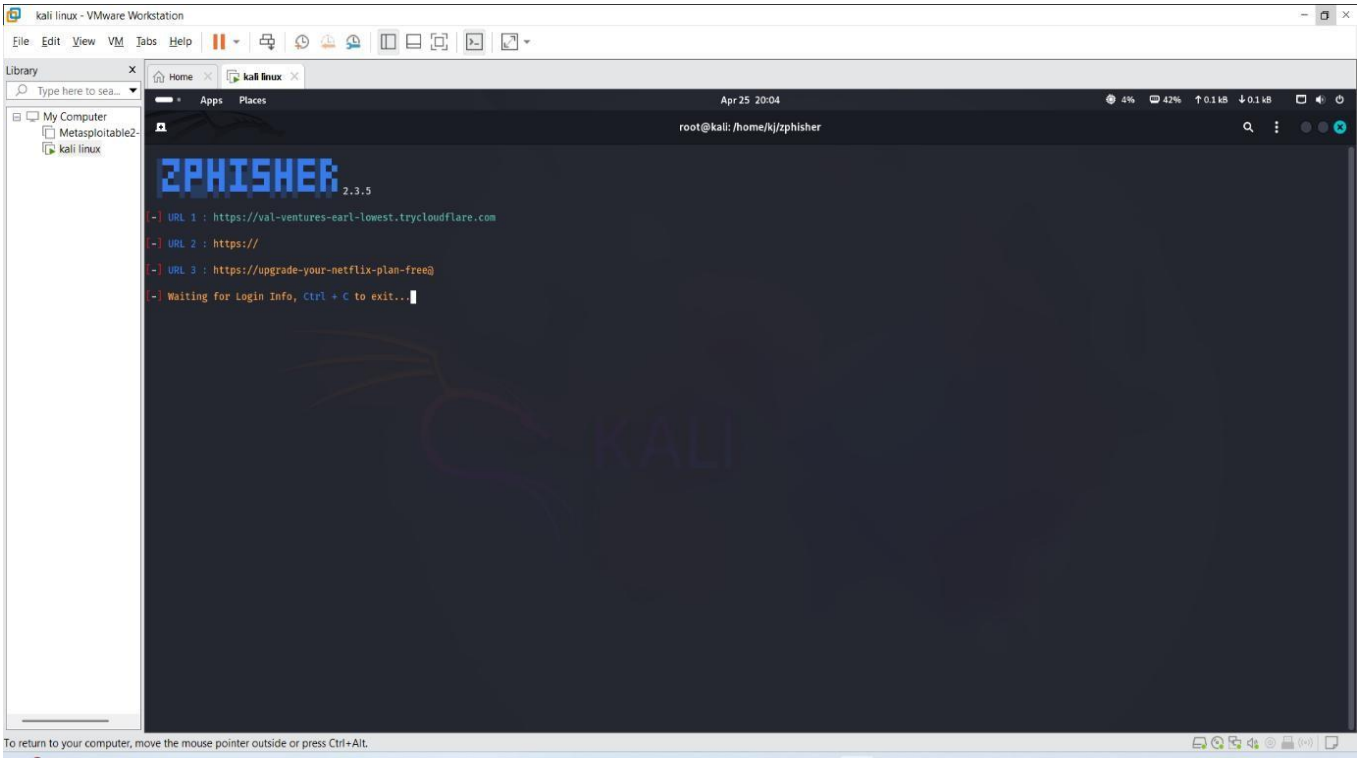


Step 3: The tool has started running successfully. Now you have to choose the options from the tool for which you have to make the phishing page.

Name : kunal jawale

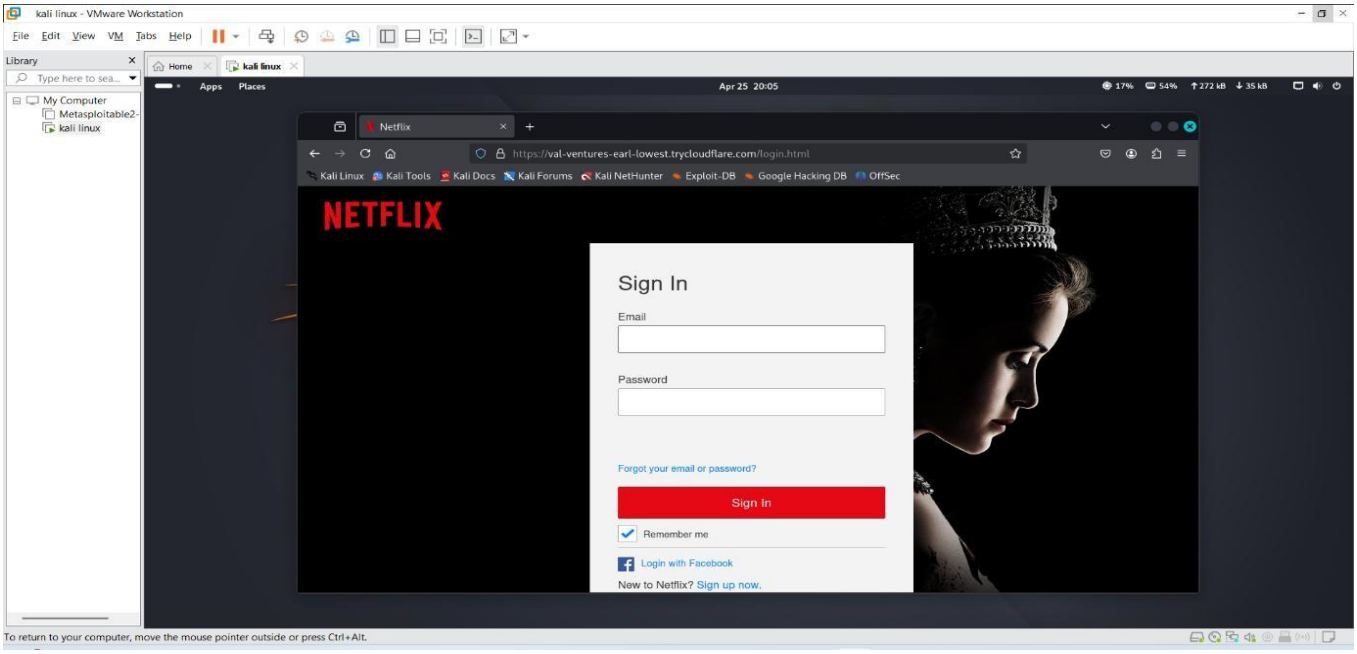
Step 4: From these options, you can choose the number for which you have to create a phishing page. Suppose you want to create a phishing page for netflix then choose option 5.

Step 5: after this you link is generated

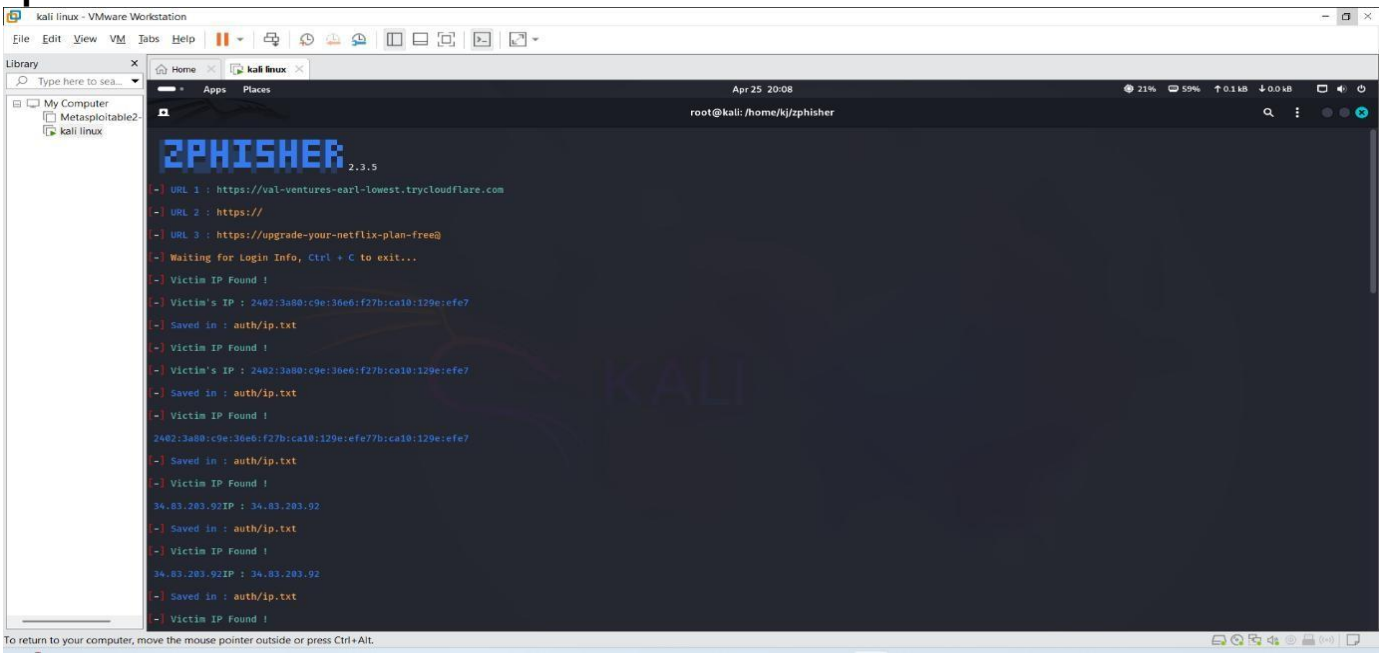


Step 6: open browser and see the interface of the link same like Netflix.

Name : kunal jawale



Step 7 : after anyone fill the information or click the link you got the ip and information about victim .



O Gophish :

Set Templates & Targets

Gophish makes it easy to create or import **pixel-perfect** phishing templates.

Our web UI includes a full HTML editor, making it easy to customize your templates right in your browser.

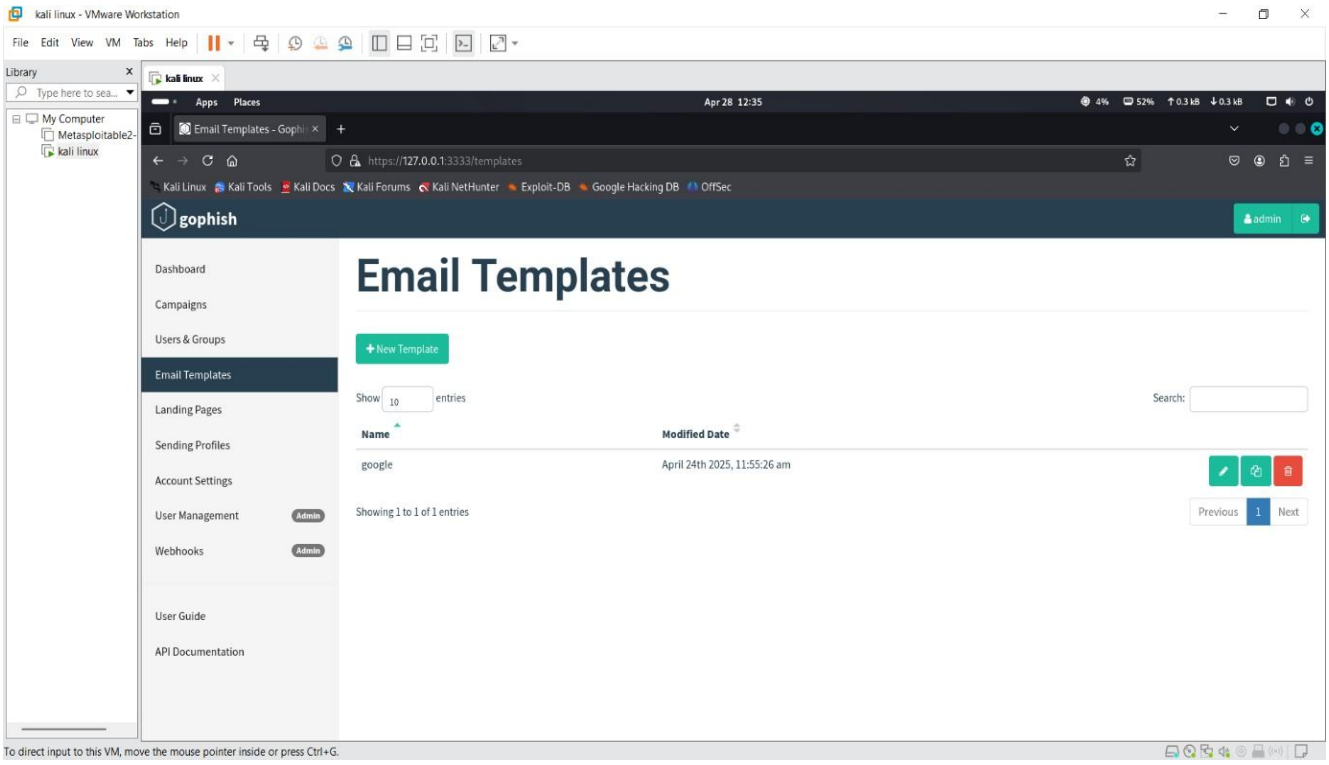
Name : kunal jawale

Launch the Campaign

Launch the campaign and phishing emails are sent in the background. You can also schedule campaigns to launch whenever you'd like.

Track Results

Detailed results are delivered in near real-time. Results can be exported for use in reports.

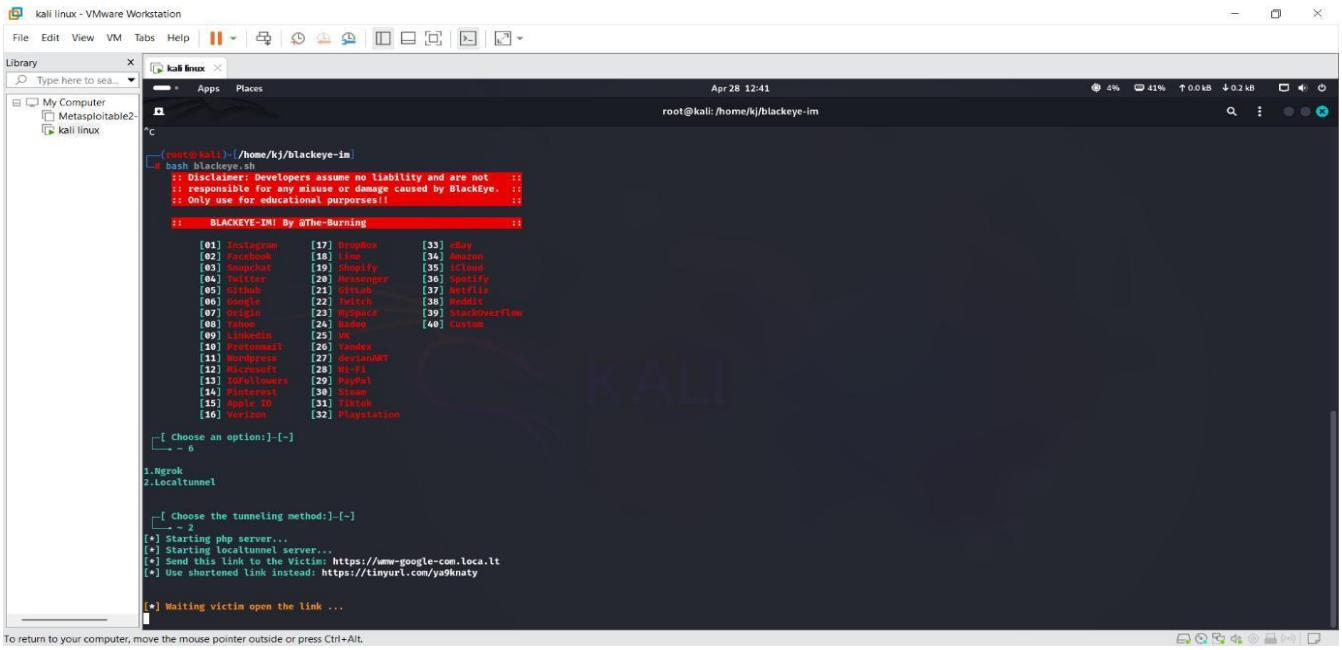


O Black eye :

Blackeye is a powerful open-source tool Phishing Tool. Blackeye is becoming very popular nowadays that is used to do phishing attacks on Target. Blackeye is an easy Social Engineering Toolkit. Blackeye contains some templates generated by another tool called Blackeye. This tool makes it easy to perform phishing attacks. There is a lot of creativity that they can put into making the email look as legitimate as possible. Blackeye offers phishing templates web pages for

Name : kunal jawale

33 popular sites such as Facebook, Instagram, Google, Snapchat, GitHub, Yahoo, Protonmail, Spotify, Netflix, Linkedin, WordPress, Origin, Steam, Microsoft, etc. Blackeye wants.



The black eye is same framework like a zphisher .

Fonephreak :-

"Fonephreak" refers to the practice of exploiting telephone networks and automated systems, typically to gain free long-distance calls or access other services. This involves using specific tones, codes, and techniques to manipulate the phone network's infrastructure and bypass security measures.

Elaboration:

- **Historical Context:**

Phone phreaking has roots in the 1950s and gained popularity in the 1970s when hackers discovered how to make free long-distance calls by mimicking the tones used by the telephone system.

- **Techniques:**

Phreakers have used various techniques, including:

- **Blue Boxes:** Devices that generate tones to mimic the signals used by the phone network to route calls.

- **Red Boxes:** Similar to blue boxes but also create tones that simulate a payment to make calls from pay phones.
- **Social Engineering:** Exploiting human interaction to gain access to information or systems.
- **Dumpster Diving:** Retrieving discarded technical documents from telephone companies.
- **Modern Relevance:**

With the rise of VoIP networks, phone phreaking has adapted to exploit these systems as well.

- **Purpose:**

The primary purpose of phone phreaking has historically been to obtain free long-distance calls or to access services like conference calling and voicemail.

/ here are some websites for phishing detection

O Netcraft extension :-

Netcraft uses its various tools and platform, including browser extensions and a global cybercrime detection platform, to identify and block phishing attacks. These tools analyze websites, emails, and mobile messages for signs of phishing, providing real-time protection and helping users report suspicious activity.

How Netcraft combats phishing:

- **Browser extensions:**

Netcraft offers browser extensions (for Chrome, Firefox, Edge, and Opera) that provide real-time protection against phishing sites, fake shops, and malicious scripts. These extensions can detect and block phishing URLs, warn users about suspicious sites, and allow users to report them to Netcraft.

- **Mobile apps:**

Netcraft's mobile apps for Android and iOS provide similar protection, blocking phishing URLs in web browsers and SMS messages, and alerting users to potential threats.

- **Email protection:**

Name : kunal jawale

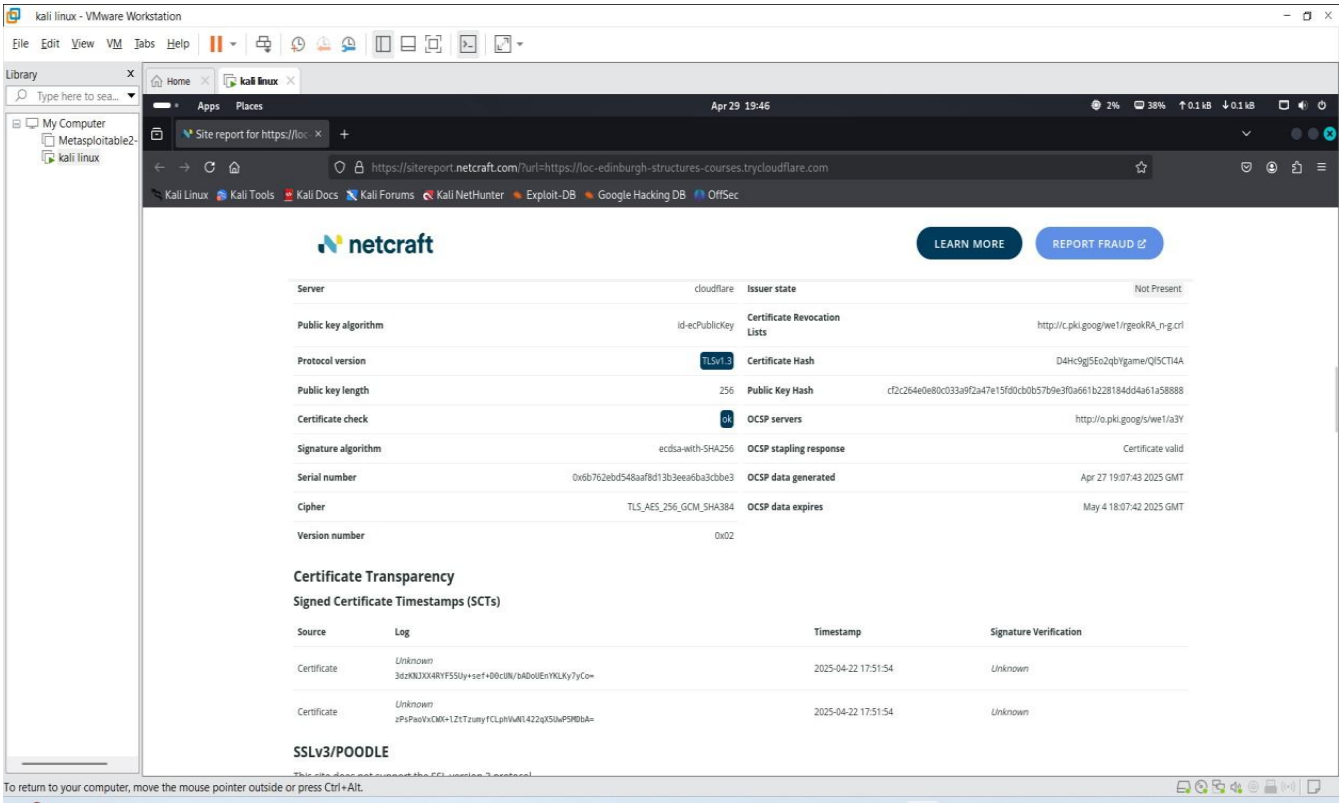
Netcraft's email protection features, such as the Netcraft Mail Reporter, allow users to report suspicious emails, analyze them for malicious content, and help protect others from phishing attempts.

- **Cybercrime detection platform:**

  Netcraft's platform utilizes automation, AI, and machine learning to detect and disrupt various cybercrime attacks, including phishing, fraud, and scams, 24/7.

- **Takedown services:**
  Netcraft analyzes and validates phishing attacks and dispatches takedown notices to relevant authorities, working to quickly remove malicious websites and disrupt attack infrastructure.

In essence, Netcraft uses a combination of technology, community reporting, and rapid takedown services to combat phishing and other cyber threats



O Phishtank :-

PhishTank is a free, community-driven service that helps identify and combat phishing attempts. It allows users to submit, verify, and share data about suspected phishing websites, offering an information clearinghouse to help safeguard internet users from fraud and malicious activity. Essentially, it's a tool for sharing and verifying information about phishing scams.

Here's a more detailed breakdown of how PhishTank is used:

Name : kunal jawale

- **Submission and Verification:**

  Users can report suspected phishing URLs to PhishTank, and the community can then verify those reports.

- **Information Sharing:**

  PhishTank compiles and shares this data with other organizations and users, helping them identify and avoid phishing websites.

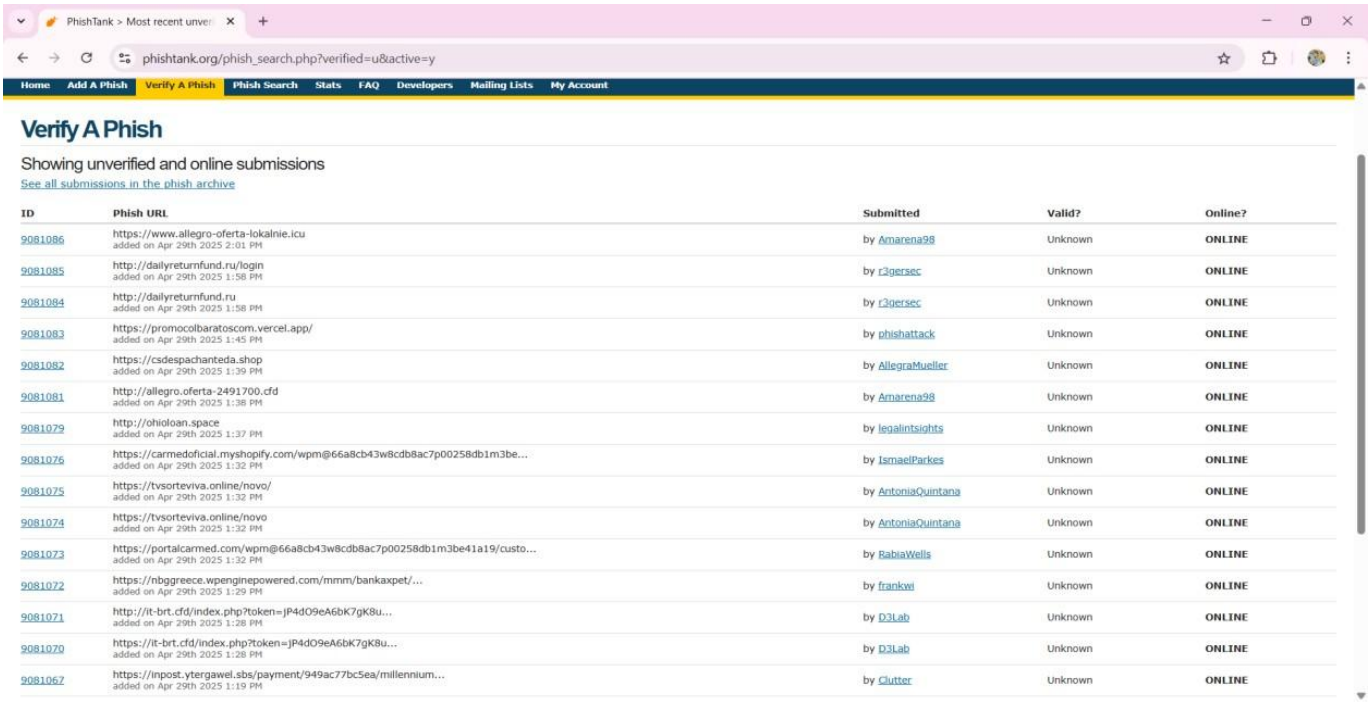
- **Combating Online Fraud:**

  By exposing phishing attempts, PhishTank helps protect users from having their personal information stolen or being manipulated by malicious actors.

- **Used by Various Entities:**

  PhishTank's data is used by companies like Opera, WOT, Yahoo! Mail, McAfee, and others in their security systems to identify and block phishing attempts.

- **Website and API:**
  PhishTank provides both a website and a web service (API) for accessing and utilizing the phishing data.



Camphish :

CamPhish is a social engineering tool used to generate fake camera login pages and remotely access a device's camera by tricking users into granting permission via

phishing. It's popular among cybersecurity students for **demonstration and educational** purposes. Here's a detailed explanation:

🔍 What is CamPhish?

CamPhish is a **camera phishing tool** that hosts a fake website using tools like **Ngrok** or **Serveo**. When the victim opens the URL, the page requests access to their device's camera. If the victim accepts, CamPhish captures and sends images back to the attacker's terminal.

⚙️ How Does CamPhish Work?

1. **Creates a phishing page** – usually mimicking platforms like YouTube or Facebook.
2. **Hosts it online** using tunnels (Ngrok, Serveo).
3. **Sends the link to the victim** via social media, email, etc.
4. **Victim clicks and allows camera access** (thinking it's legitimate).
5. **Captured images are sent** to the attacker's terminal in real time.

🛠️ Features of CamPhish

- Easy to use in Linux (especially Kali Linux, Parrot OS)
- Multiple phishing templates (e.g., YouTube, Google)
- Real-time webcam image capture
- Public URL tunneling via Ngrok/Serveo
- Lightweight and command-line-based

⚠️ Important Notice:

CamPhish is for educational and ethical hacking purposes only.
Using it without a user's **informed consent** is illegal and violates privacy laws (e.g., IT Act in India, GDPR in Europe).

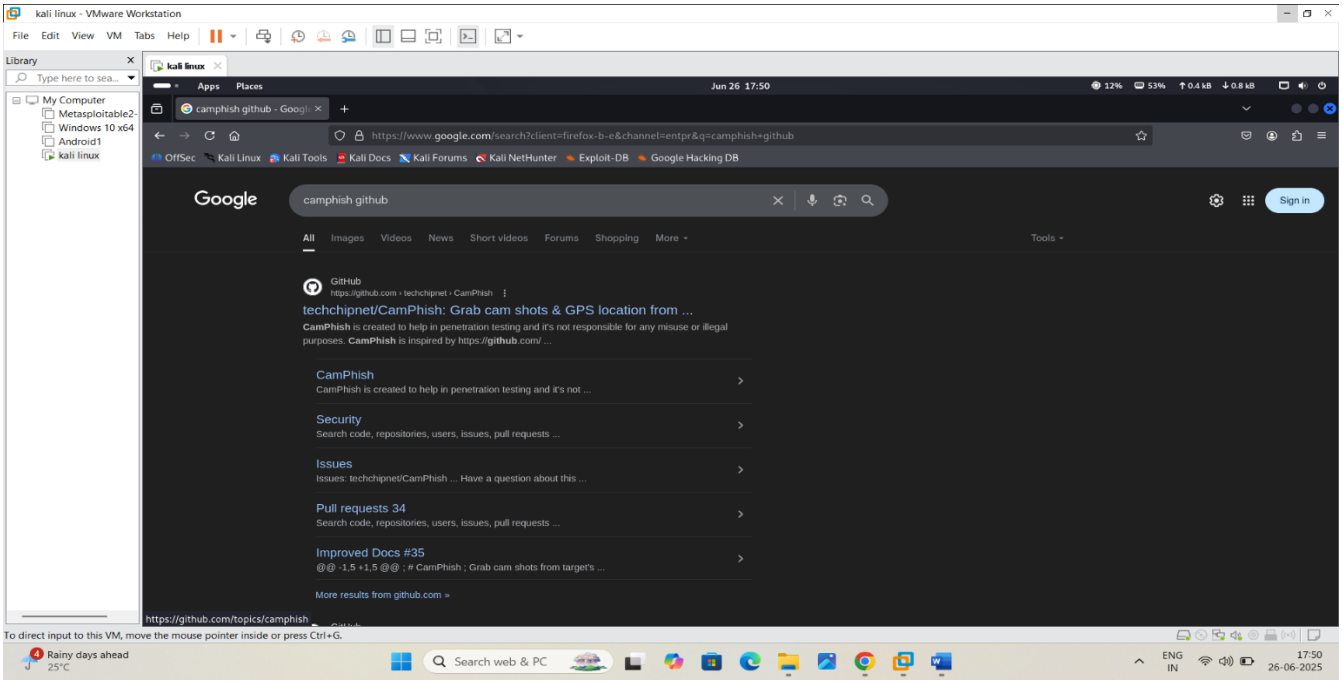
✅ Educational Use Cases

Name : kunal jawale

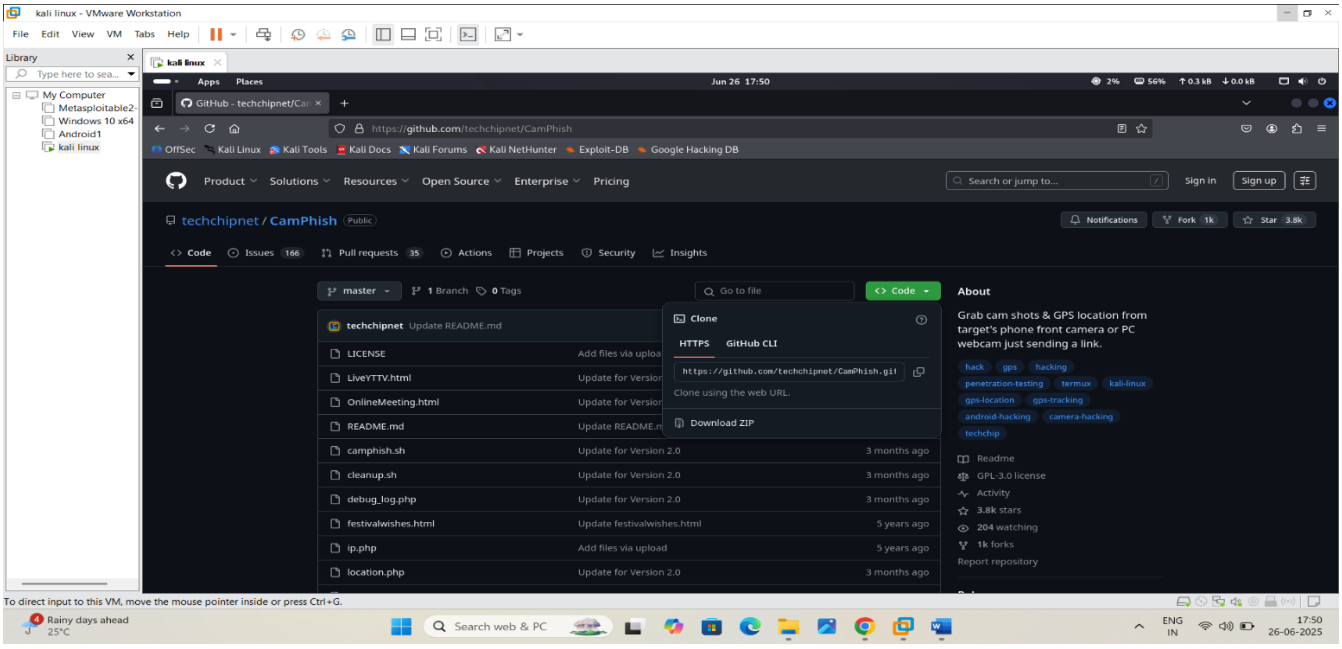
- Demonstrating **phishing techniques** in cybersecurity workshops
- Learning about **social engineering tactics**
- Practicing **ethical hacking** in controlled environments (labs, CTFs)

🚀 Example: How to Use CamPhish

1. Go to kali browser and search camphish github

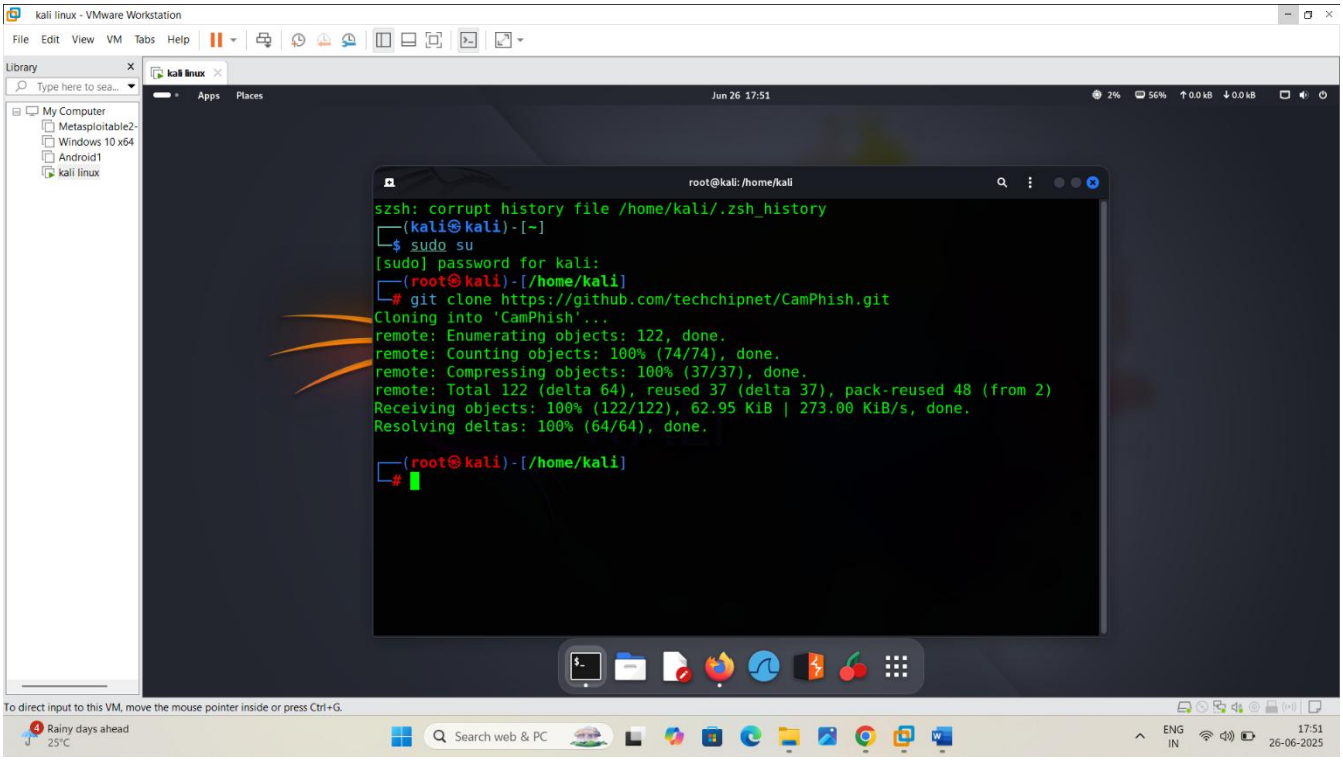


2. Select first link and copy the code

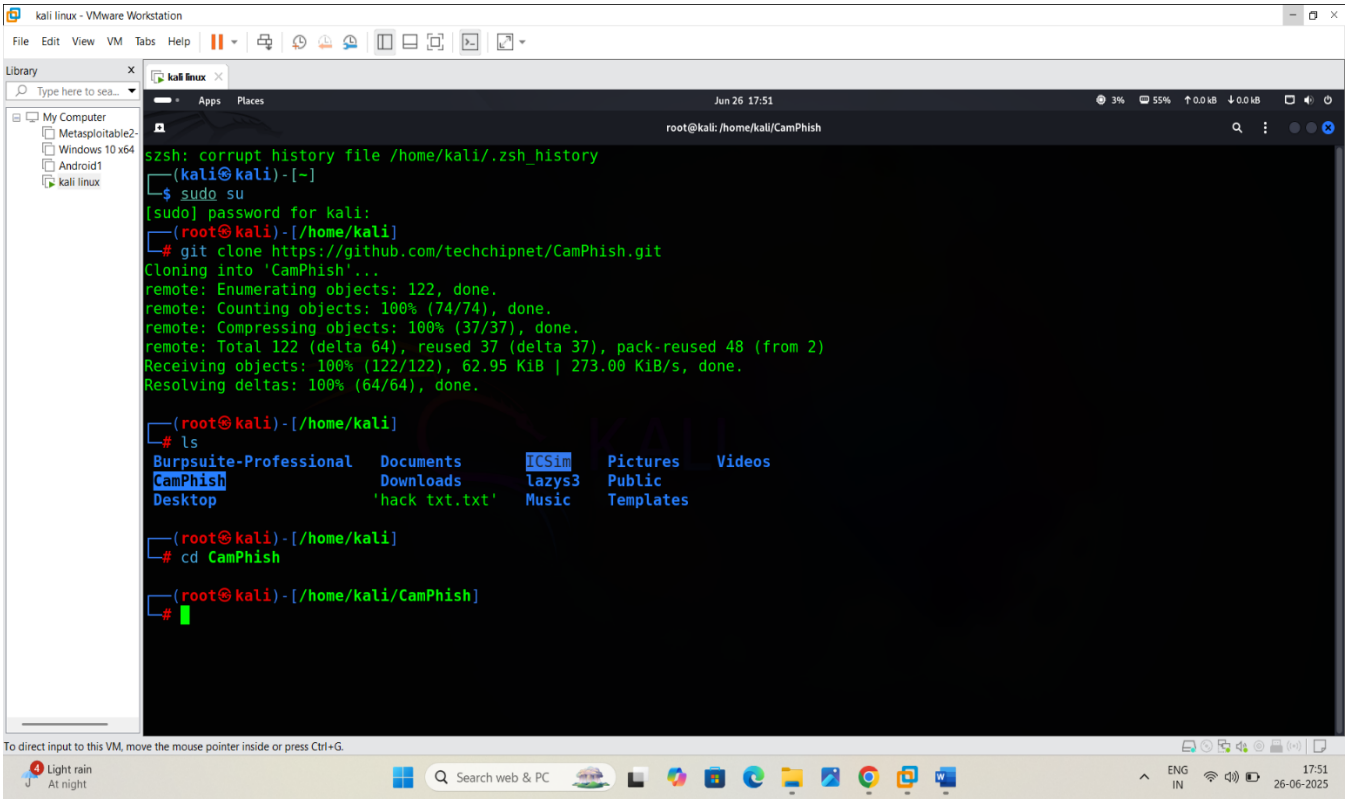


Name : kunal jawale

3. Go to terminal and type
   # git clone and paste the copy code to install the camphish

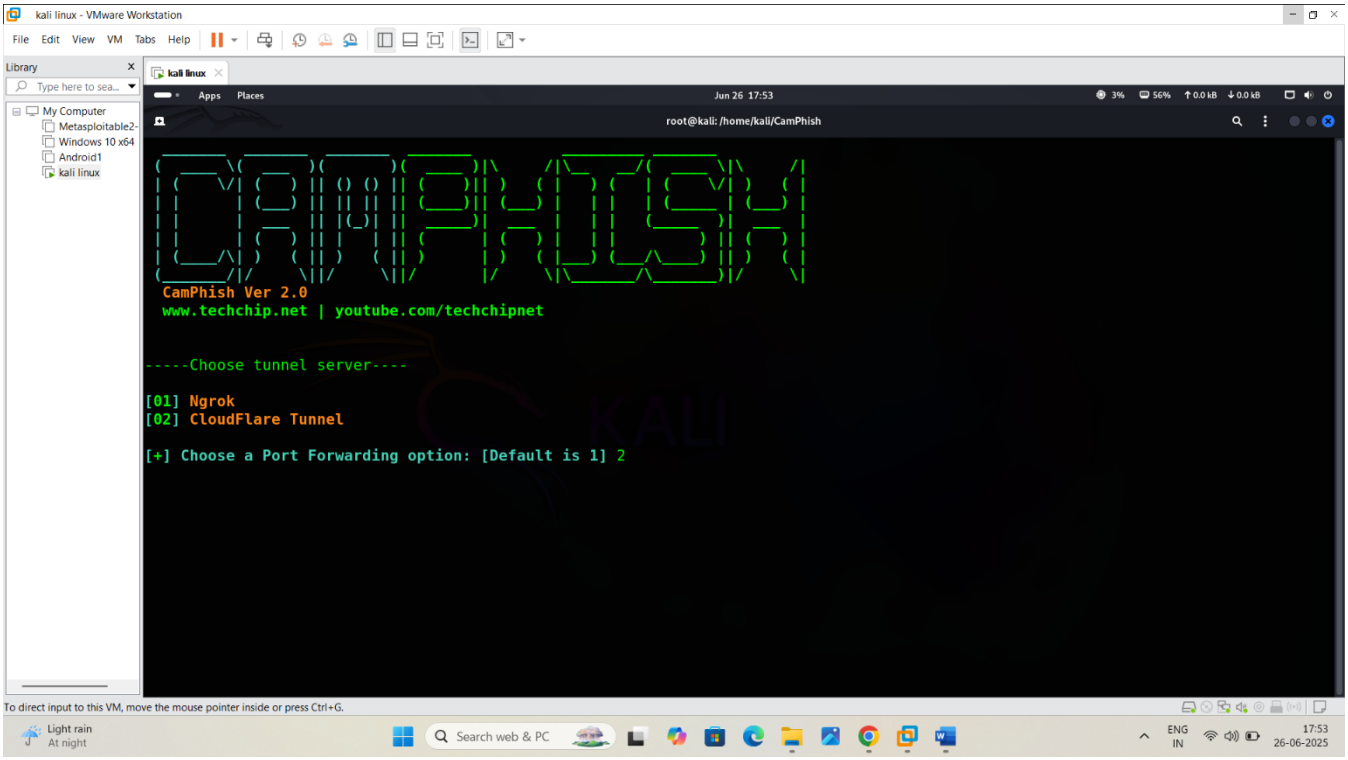


4. Do ls command and go to camphish directory using
   # cd camphish

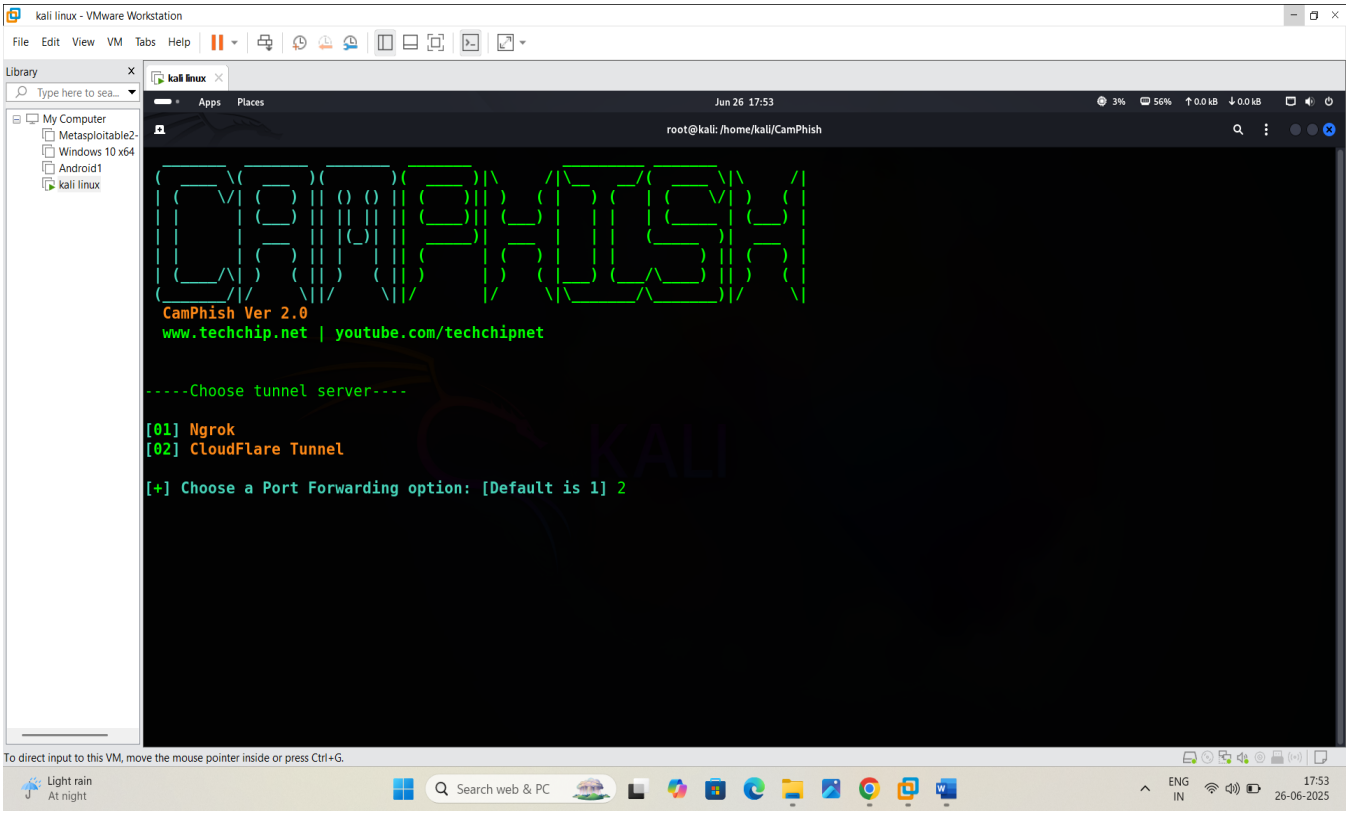


Name : kunal jawale

5. Do again ls and write the command
   # bash camphish.sh for open camphish

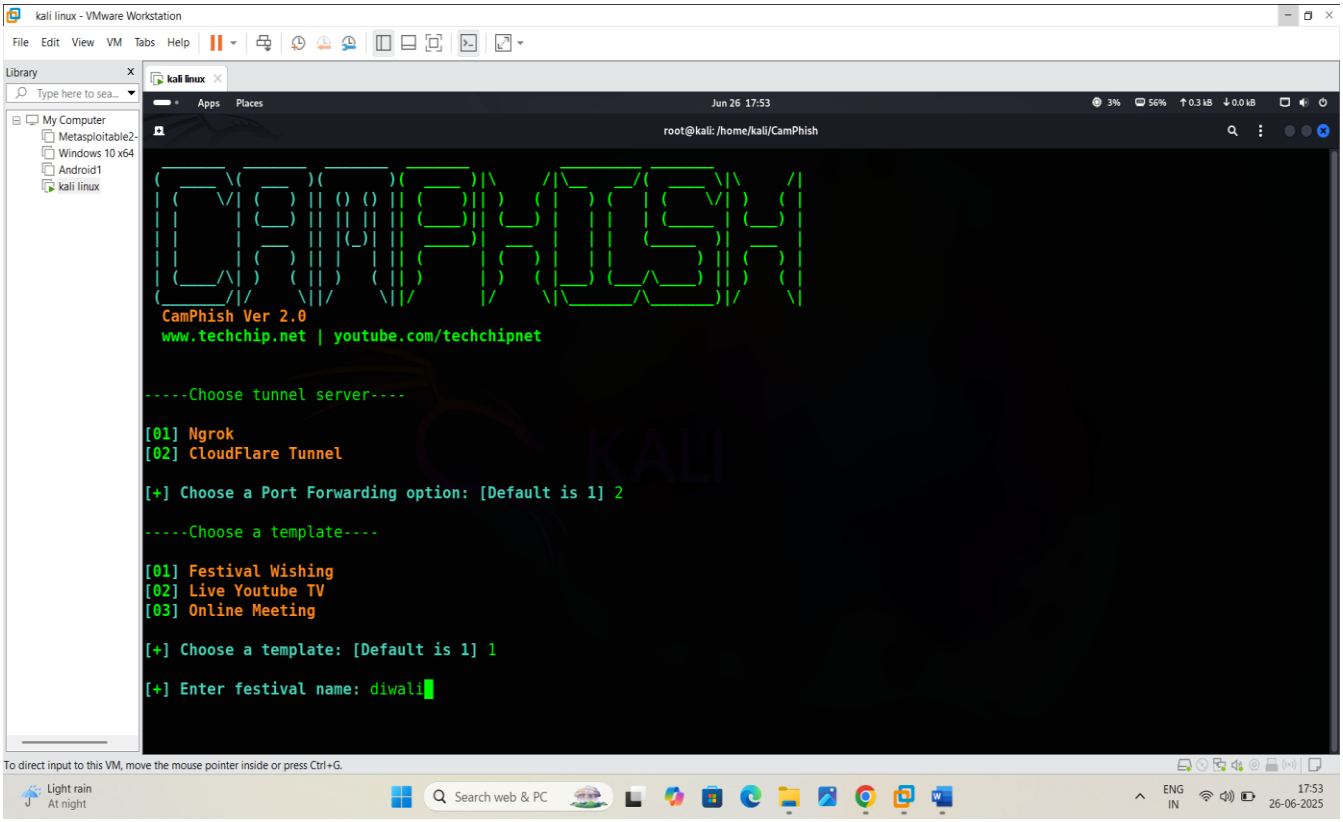


6. Select 2nd option

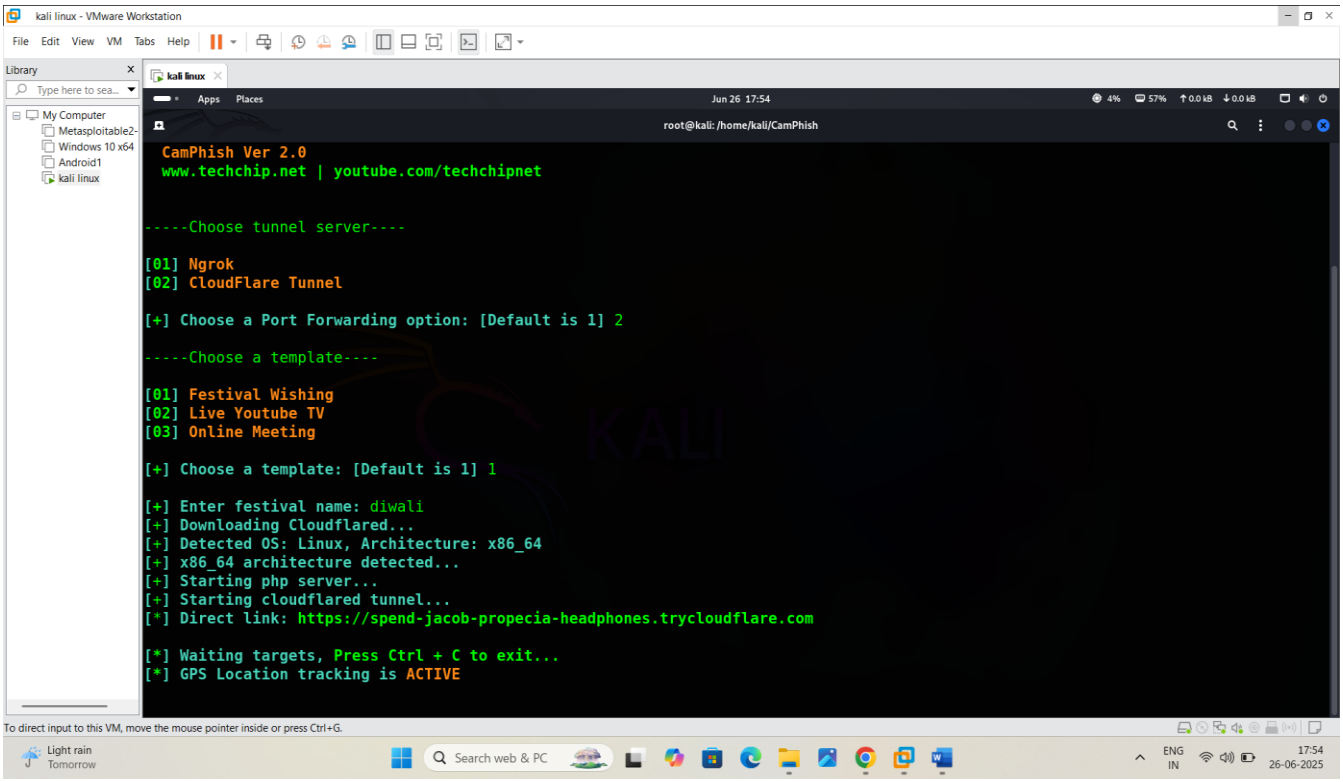


Name : kunal jawale

7. Choose tamplet 1 and give festival name like Diwali



8. After this generate a link like this :



Name : kunal jawale

Share this link with anyone then you got the camera access and location of the target person.