REPORT OF SOCIAL ENGINEERING

BY SACHCHITANAND YADAV

SOCIAL ENGINEERING
MODULE - 9

Learning Objectives -

- Explain Social Engineering Concepts
- Explain Various Human-based Social Engineering Techniques
- Explain Various Computer-based Social Engineering Techniques
- Explain Various Mobile-based Social Engineering Techniques
- Explain Social Engineering Countermeasures

TABLE OF CONTENTS

---

5. Perform Phishing Attack Using CamPhish Tool

5.1 Objective of the Experiment
5.2 Working of CamPhish

---

6. Perform Phishing Attack Using Zphisher

6.1 Objective
6.2 Working of Zphisher

---

7. Perform Phishing Attack Using ShellPhish

7.1 Objective of the Experiment
7.2 Tool Used
7.3 Conceptual Working of ShellPhish

---

8. Social Engineering Countermeasures

8.1 Security Awareness and Training
8.2 Password Policies
8.3 Physical Security Policies
8.4 Access Control and Privileges
8.5 Incident Response and Monitoring
8.6 Background Checks and Termination Process
8.7 Technical Defenses
8.8 Defense Strategy
8.9 Additional Countermeasures
8.10 Conclusion

---

9. Module Summary – Social Engineering

Social Engineering Concepts: -

SOCIAL ENGINEERING

Social engineering is the art of hacking the *mind* before the machine. No brute force. No zero-days. Just vibes, pressure, trust, fear—played like a cheap guitar. Attackers don't break systems first; they bend people.

At its core, social engineering exploits human psychology—curiosity, urgency, authority, and that dangerous instinct to be "helpful."

Types of Social Engineering Attacks

1. Human-Based Social Engineering Attack

This is face-to-face or voice-to-voice manipulation. Old as time. Con artists did this before computers even existed.

How it works:

- Direct interaction with the victim
- Attackers impersonate trusted figures (IT staff, security, colleagues)
- Psychological pressure does the heavy lifting

Goal:
Extract confidential information or gain physical/system access.

---

2. Computer-Based Social Engineering Attack

Here, the attacker hides behind a screen. Emails, fake websites, pop-ups—digital smoke and mirrors.

How it works:

- Fraudulent emails or websites
- Fake software updates or warnings
- Malicious links and attachments

Goal:
Steal credentials, install malware, or gain unauthorized access.

3. Mobile-Based Social Engineering Attack

Your phone? Yeah, that tiny rectangle of trust. Attackers love it.

How it works:

- Fake calls, SMS, or malicious mobile apps
- Impersonation of banks, delivery services, or government bodies

Goal:
Steal personal or financial data—fast and quiet.

Common Types of Social Engineering

1. **Phishing** – Fake emails or messages posing as legit sources. Classic. Still deadly.
2. **Spear Phishing** – Phishing with homework done. Personalized and precise.
3. **Vishing** – Voice calls that sound official and urgent.
4. **Smishing** – Phishing via SMS. Short text. Big damage.
5. **Pretexting** – Fake scenarios to extract info (hello, "IT Support").
6. **Baiting** – Infected USBs or links left as temptation. Curiosity killed the network.
7. **Tailgating** – Walking into restricted areas behind authorized people. No badge, just confidence.

PHISHING

Phishing is the poster child of social engineering. Simple, scalable, and still catching victims daily. If it looks urgent, sounds official, and asks for secrets—be suspicious.

Types of Phishing

1. Email Phishing

Description:
Mass emails pretending to be banks, companies, or institutions.

Goal:
Steal login credentials or deliver malware.

---

2. Spear Phishing

Description:
Targeted attacks using personal details to look trustworthy.

Goal:
Steal specific sensitive information.

---

3. Whaling

Description:
Spear phishing aimed at top executives—big fish, big payout.

Goal:
Access confidential company data or authorize fraud.

---

4. Smishing (SMS Phishing)

Description:
Malicious links or fake alerts via text messages.

Goal:
Trick users into clicking links or calling fake numbers.

---

5. Vishing (Voice Phishing)

Description:
Phone calls impersonating banks, police, or authorities.

Goal:
Extract personal or financial information.

---

6. Pharming

Description:
Redirects users from real websites to fake ones using DNS poisoning or malware.

Goal:
Harvest credentials silently.

---

7. Angler Phishing

Description:
Fake customer support accounts on social media.

Goal:
Steal credentials or push malware through DMs.

---

8. Clone Phishing

Description:
A trusted email is copied, but links or attachments are weaponized.

Goal:
Exploit existing trust to infect or steal data.

Perform Social Engineering Using Various Techniques

Social engineering techniques exploit human behavior to obtain sensitive information from individuals or organizations. These techniques are commonly used to commit fraud or enable further cyberattacks by bypassing technical security controls through psychological manipulation.

Lab Scenario

In the role of an **ethical hacker or penetration tester**, the objective is to assess an organization's security posture and employee awareness by simulating controlled social engineering attempts. The focus is on identifying human-level vulnerabilities rather than exploiting systems directly.

During a social engineering assessment, the tester attempts to induce users to disclose sensitive information such as:

- Credit card or banking details
- Telephone numbers
- Confidential organizational data
- System or network-related information

Perform Phishing Attack Using SETOOLKIT

The Social-Engineer Toolkit (SET) in Kali Linux is a penetration-testing framework designed to **simulate** real-world social engineering threats in **authorized lab environments**. Its purpose isn't crime—it's awareness, testing, and defense.

SET focuses on exploiting **human behavior**, not system vulnerabilities, helping security professionals understand how easily users can be manipulated.

Objective of the Lab

- To understand how phishing attacks are structured
- To analyze how attackers imitate trusted services
- To study the risks of credential harvesting
- To improve detection and prevention strategies

No ego. Just learning.

Tool Used

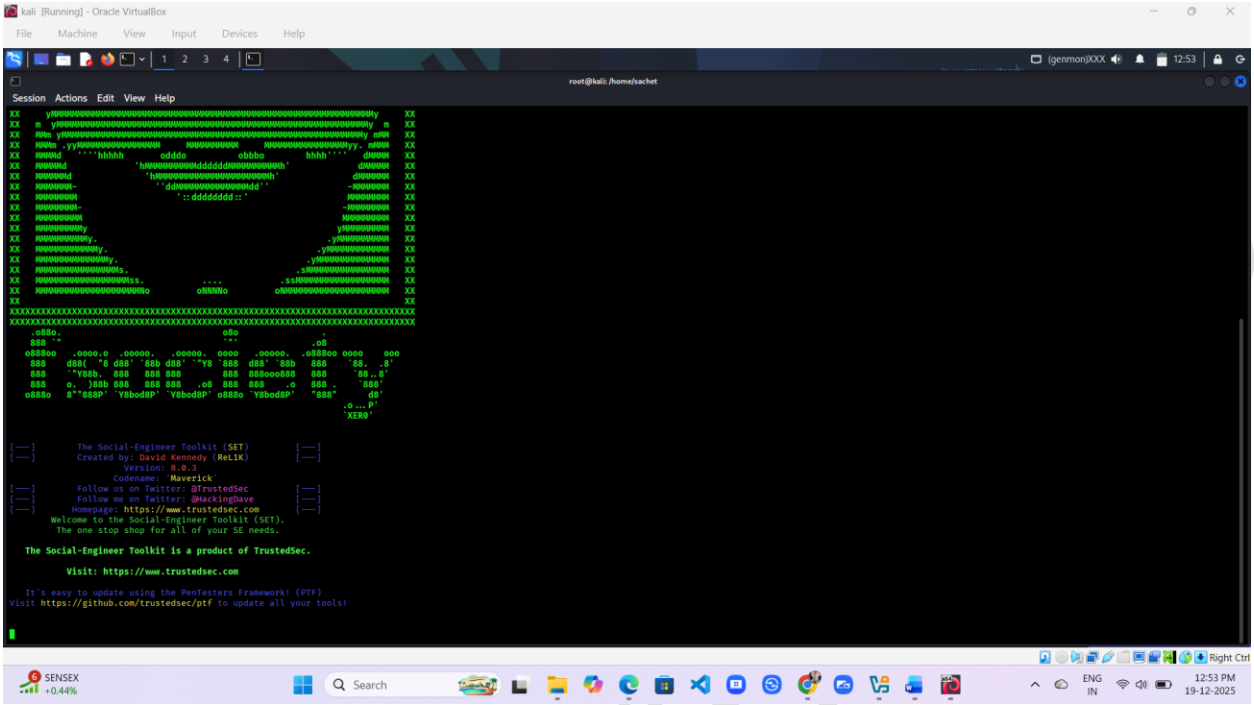
Social-Engineer Toolkit (SET)

- Pre-installed in Kali Linux
- Designed for controlled security testing
- Widely used in cybersecurity training and awareness programs

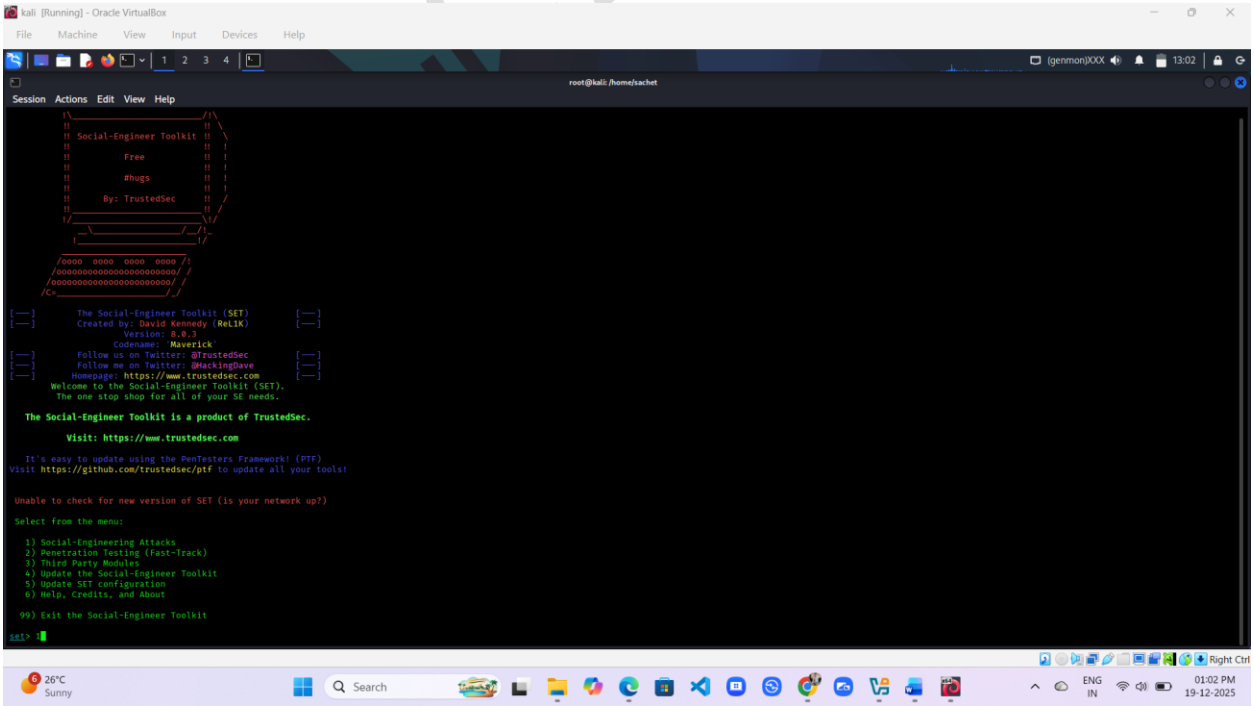
How to use it -:

• Open kali linux terminal and type setoolkit

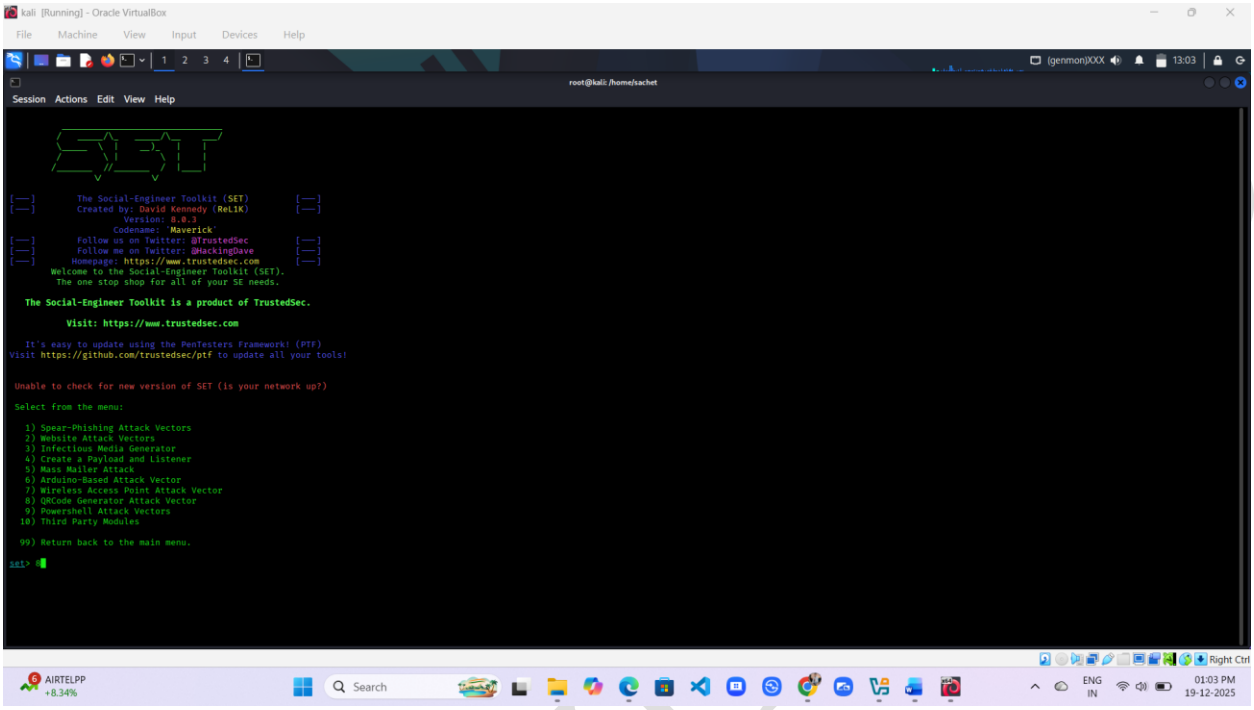
• It opens



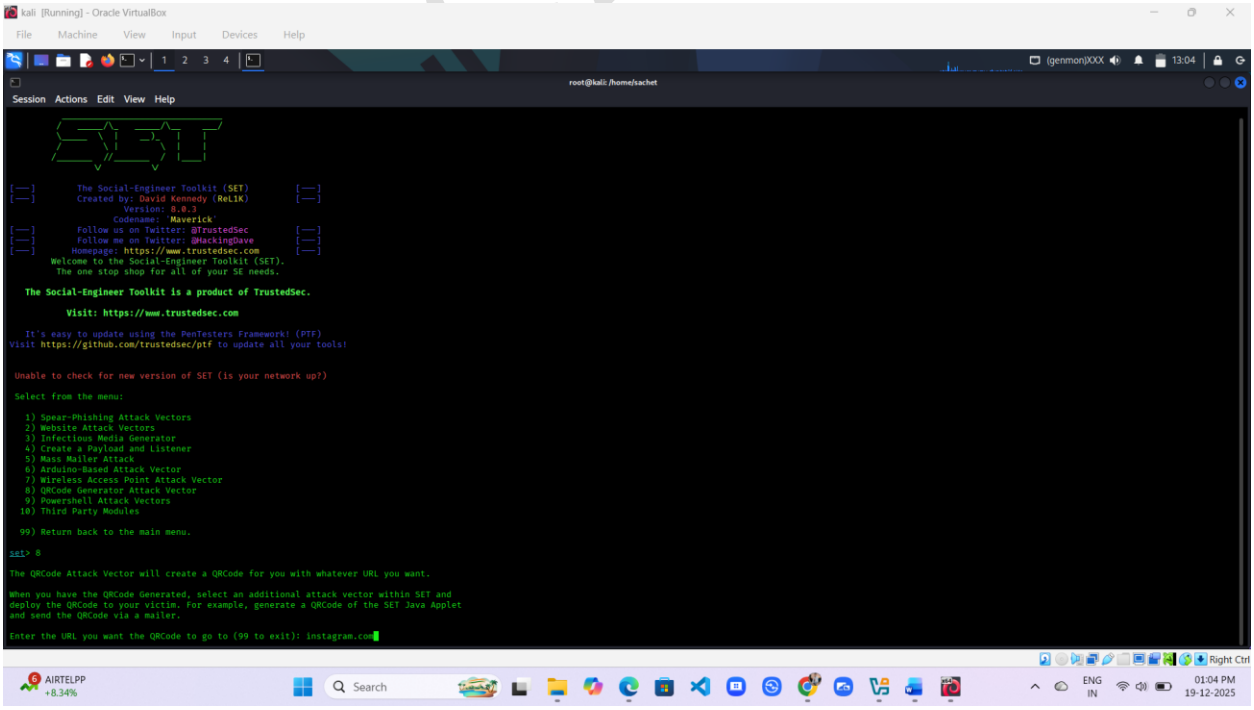
- Now select 1 – Social Engineering Attack



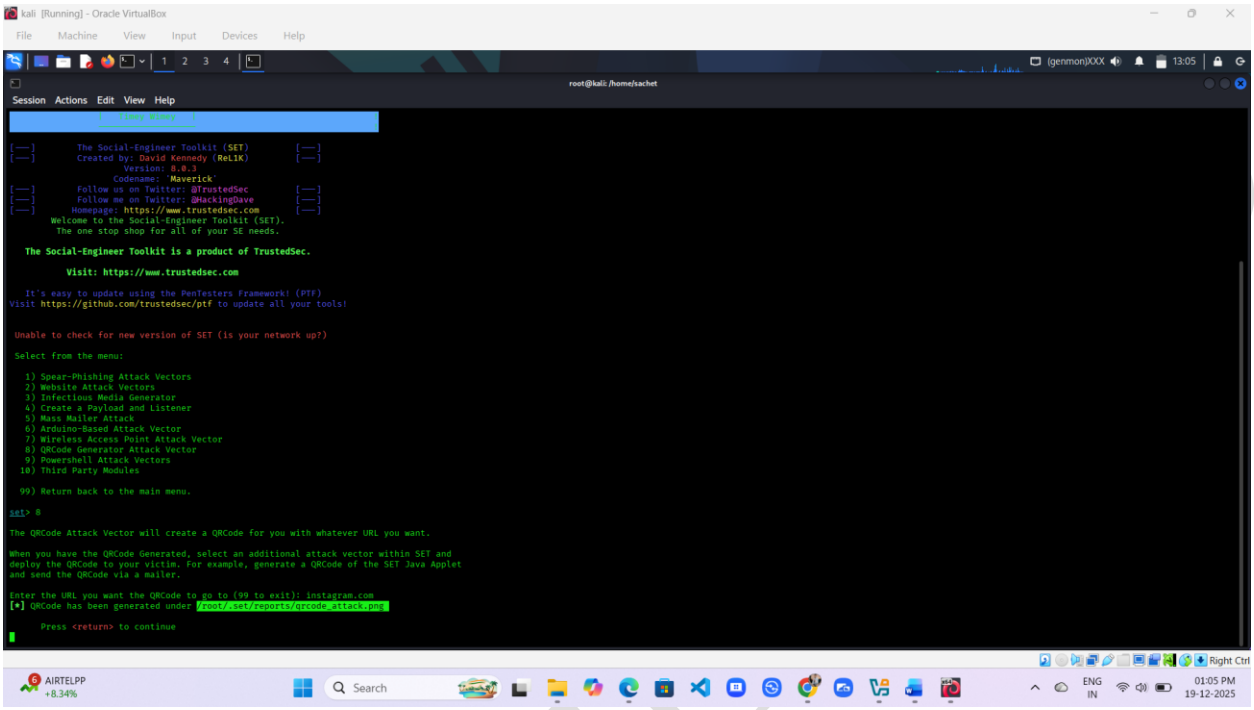
- Now select 8 –



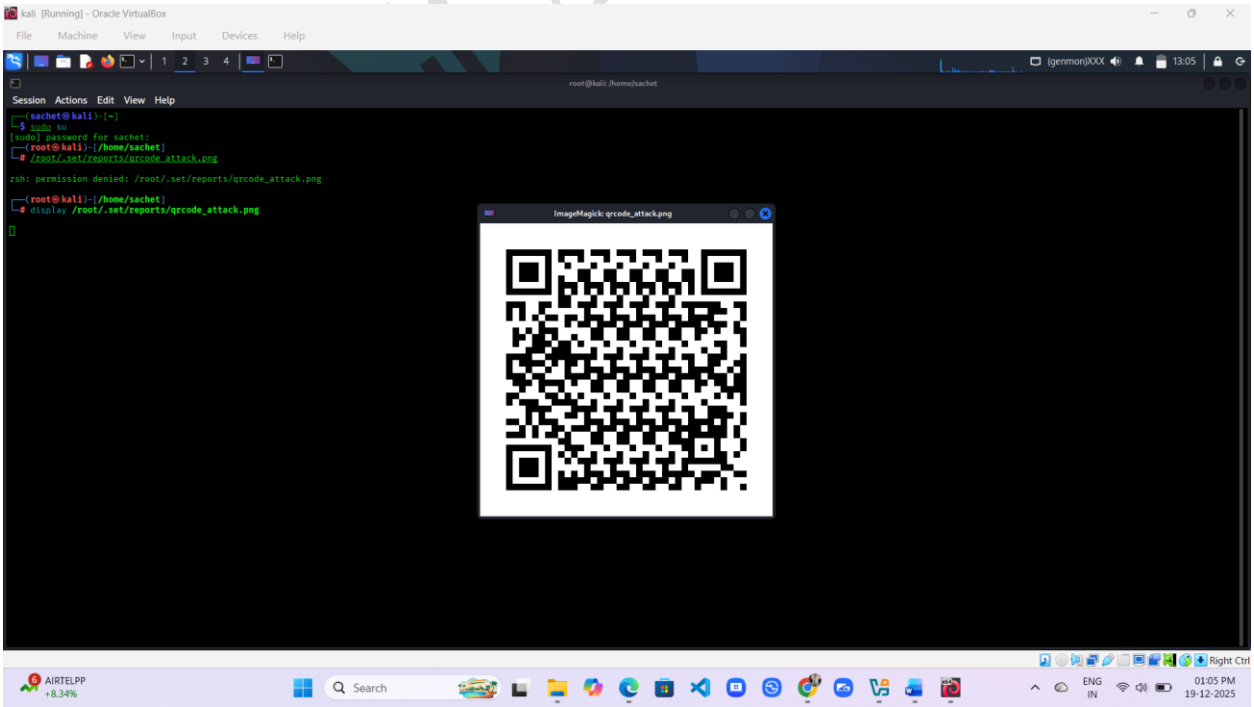
Enter the URL you want the QRCode



QRCode has been generated



Now display



Perform Phishing Attack Using CamPhish Tool

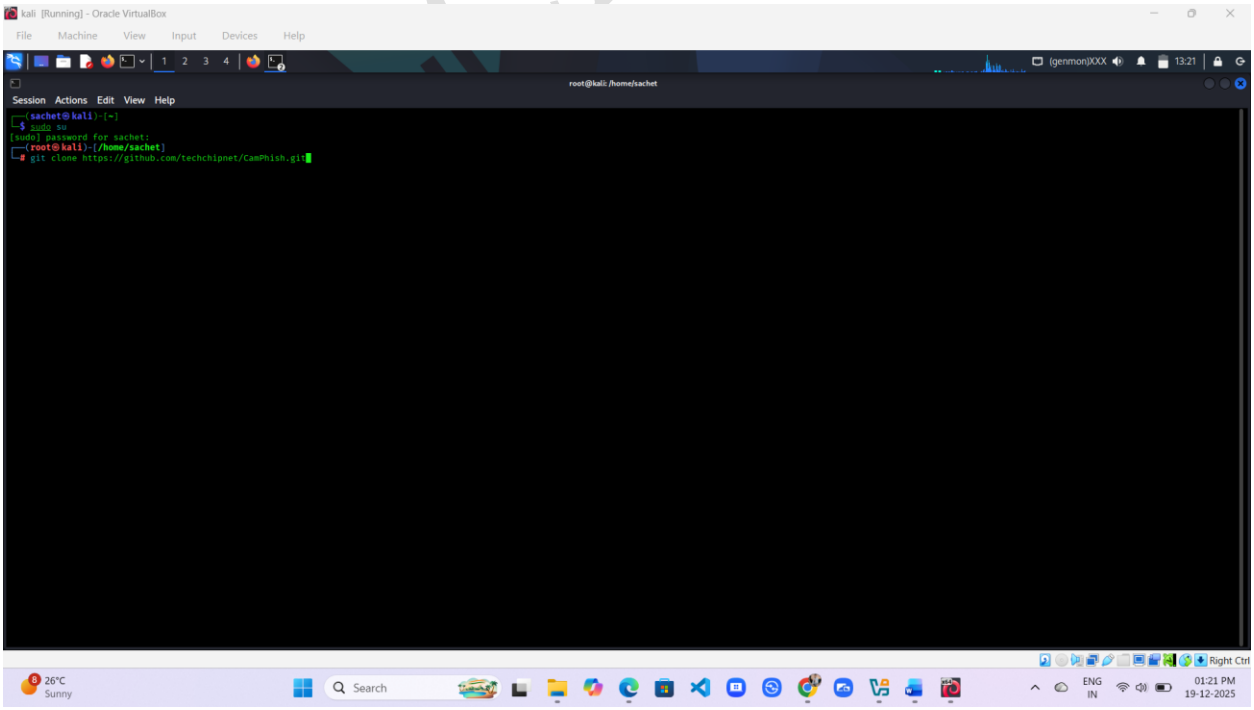
CamPhish is a social engineering–based phishing tool used in controlled environments to **demonstrate how attackers exploit curiosity and trust** to extract sensitive data. Instead of brute-force hacking, CamPhish relies on **deception**, proving once again that humans are the softest entry point.

Objective of the Experiment

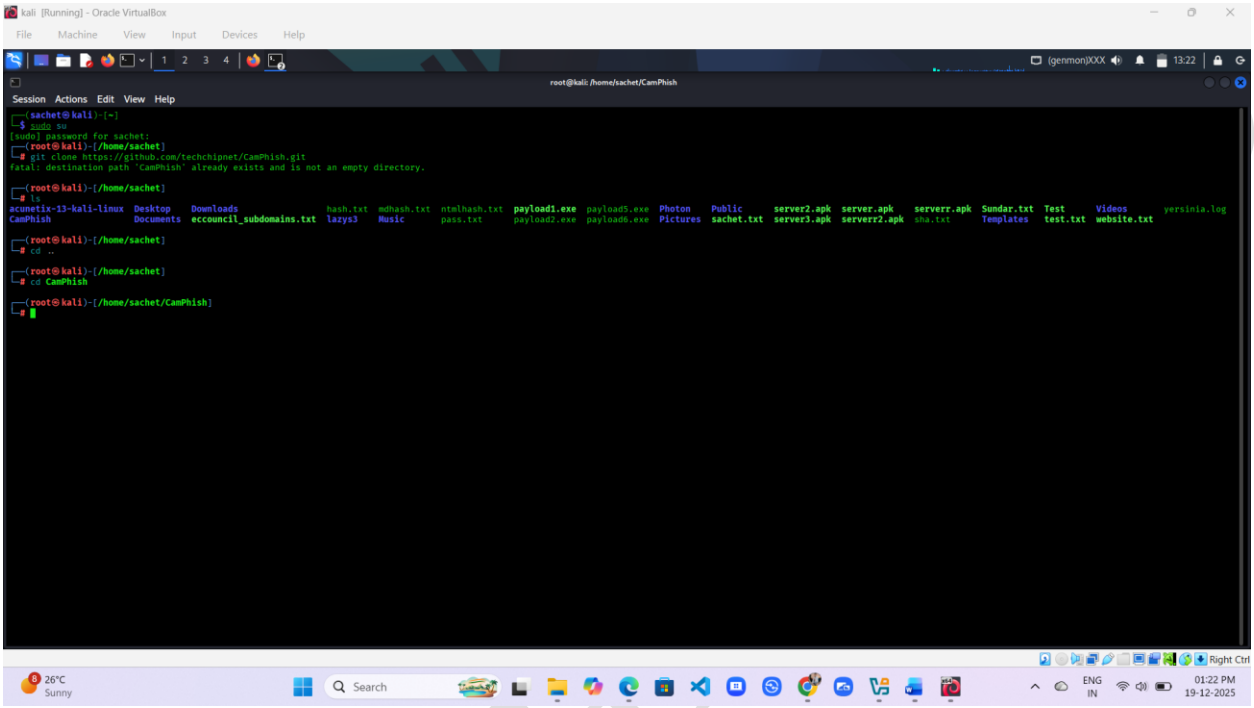
- To study camera-based phishing techniques
- To understand how fake web pages are used to deceive users
- To analyze risks related to unauthorized access to device hardware
- To emphasize the importance of user awareness and permissions

How to use it -:

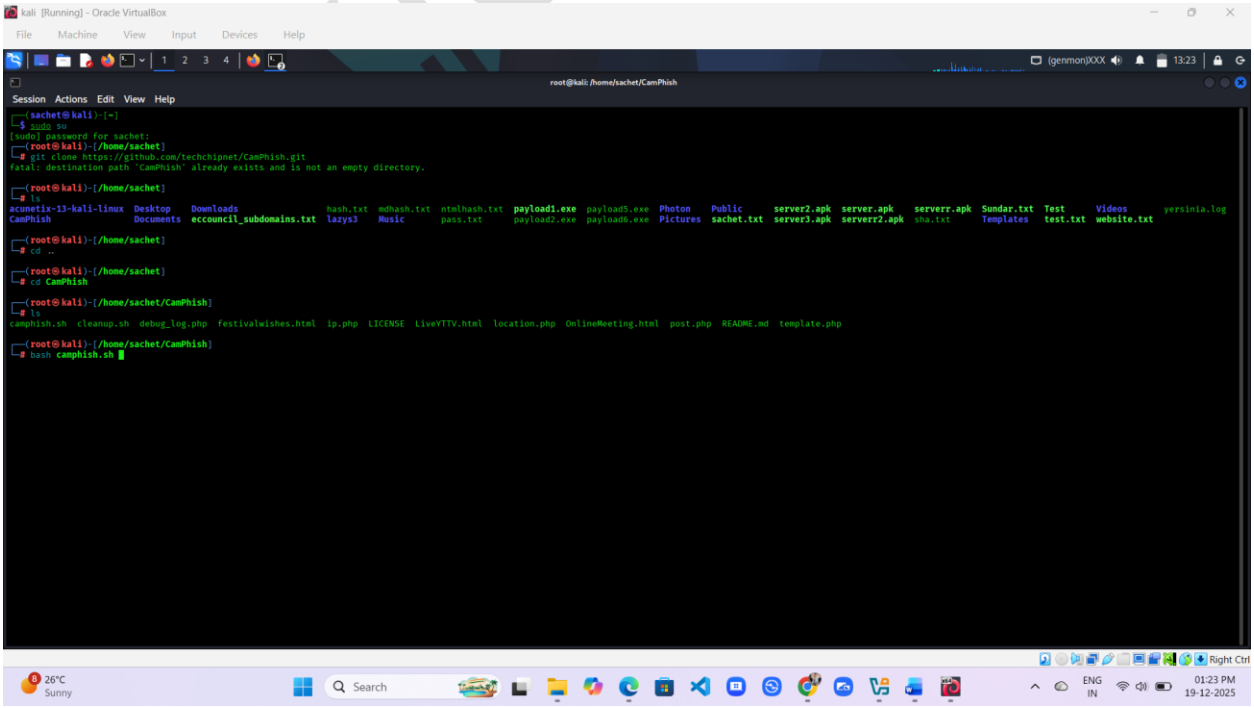
- Download from GitHub



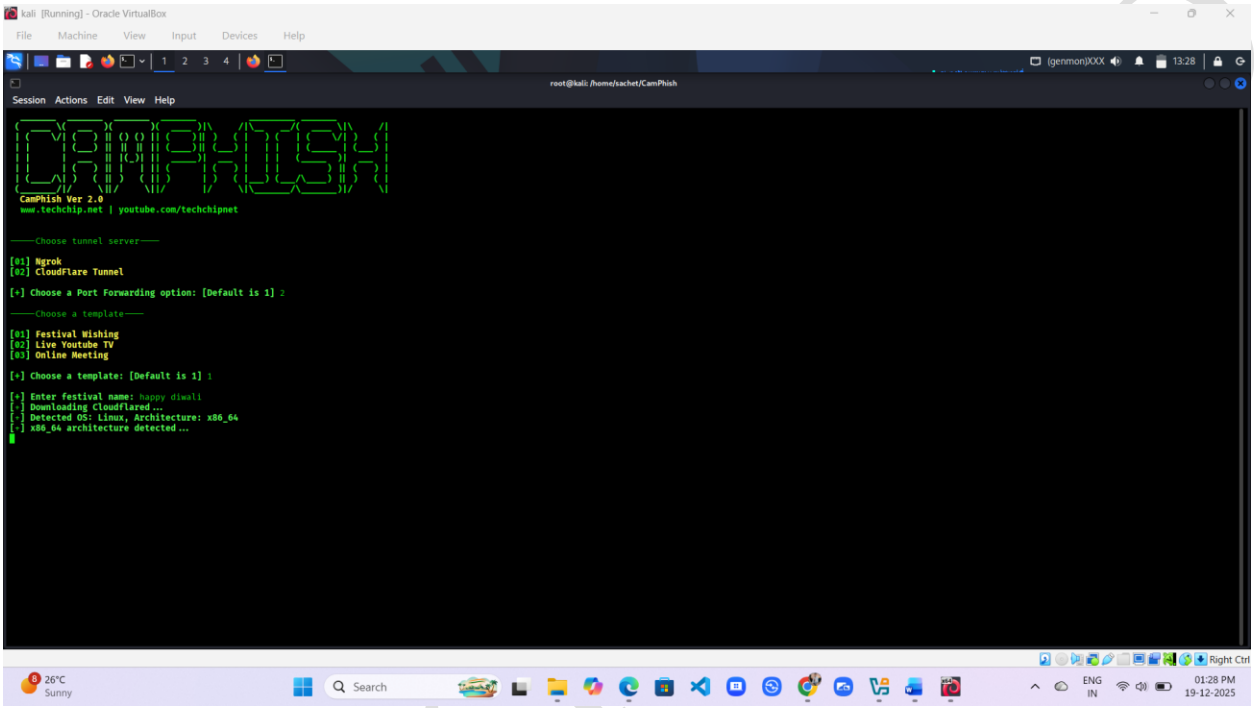
Open kali linux terminal go to the camphish directory



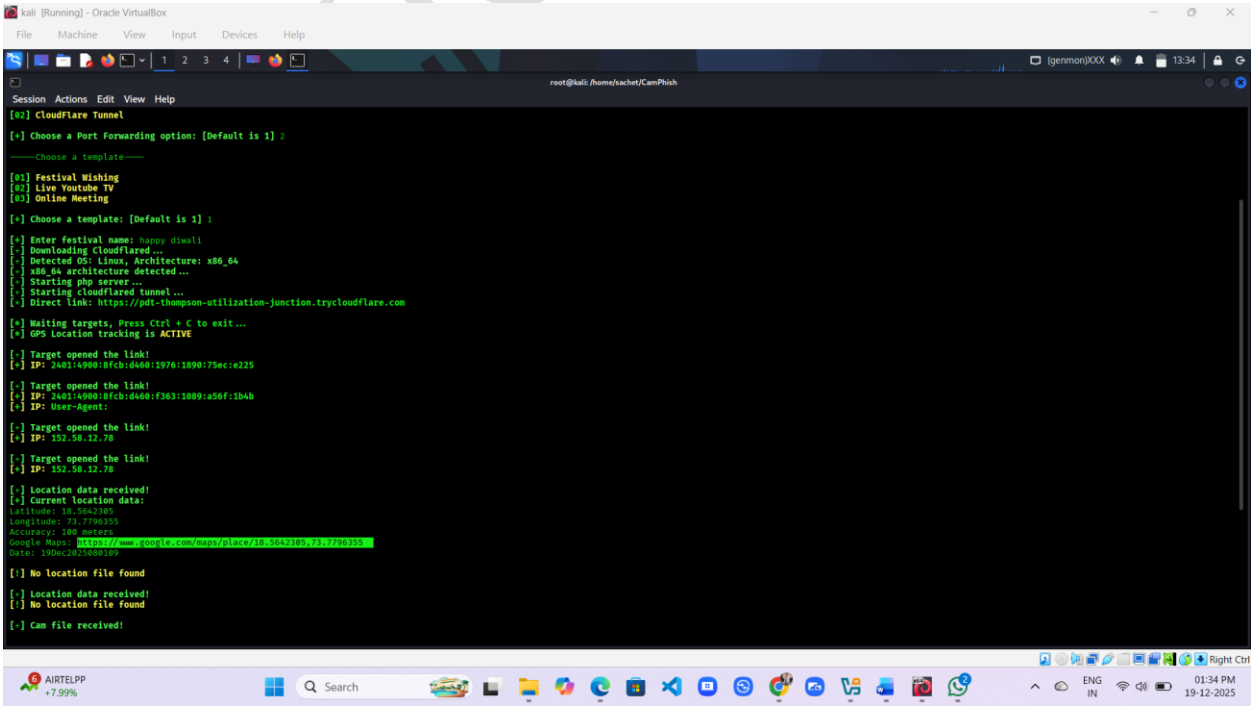
• Type command –bash camphish



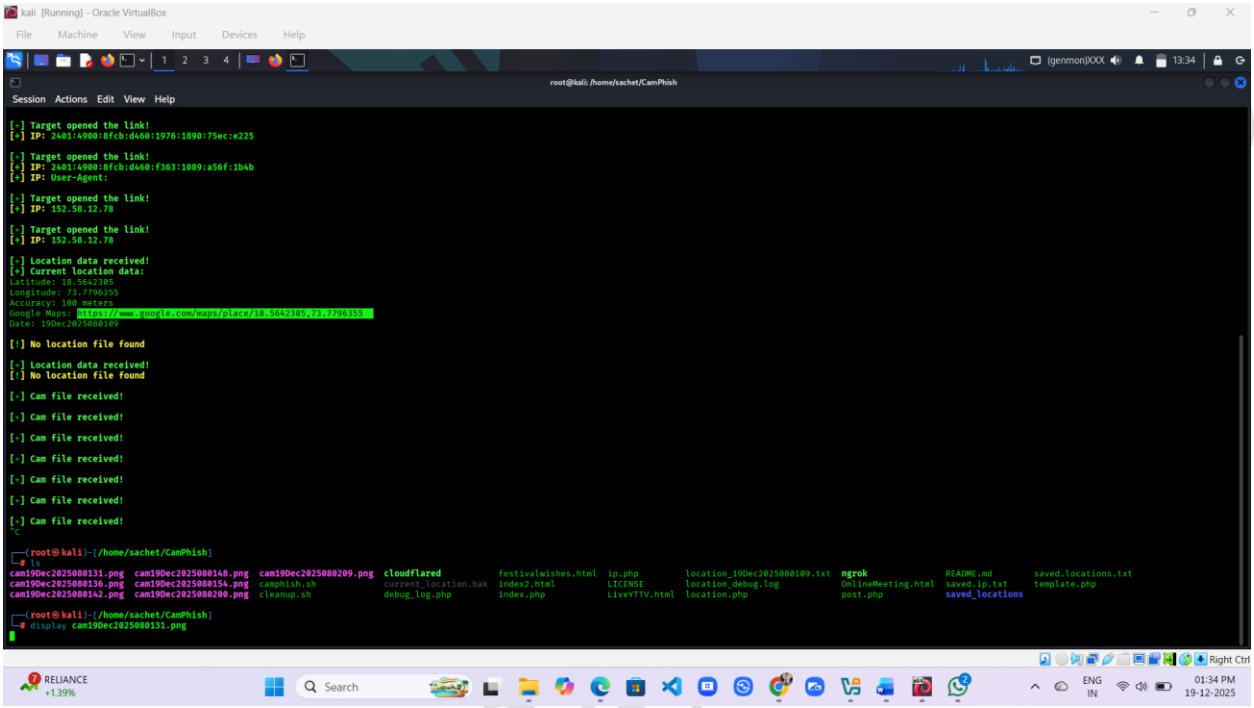
- Select Server – cloudflare tunnel
- Select 1
- Enter Message



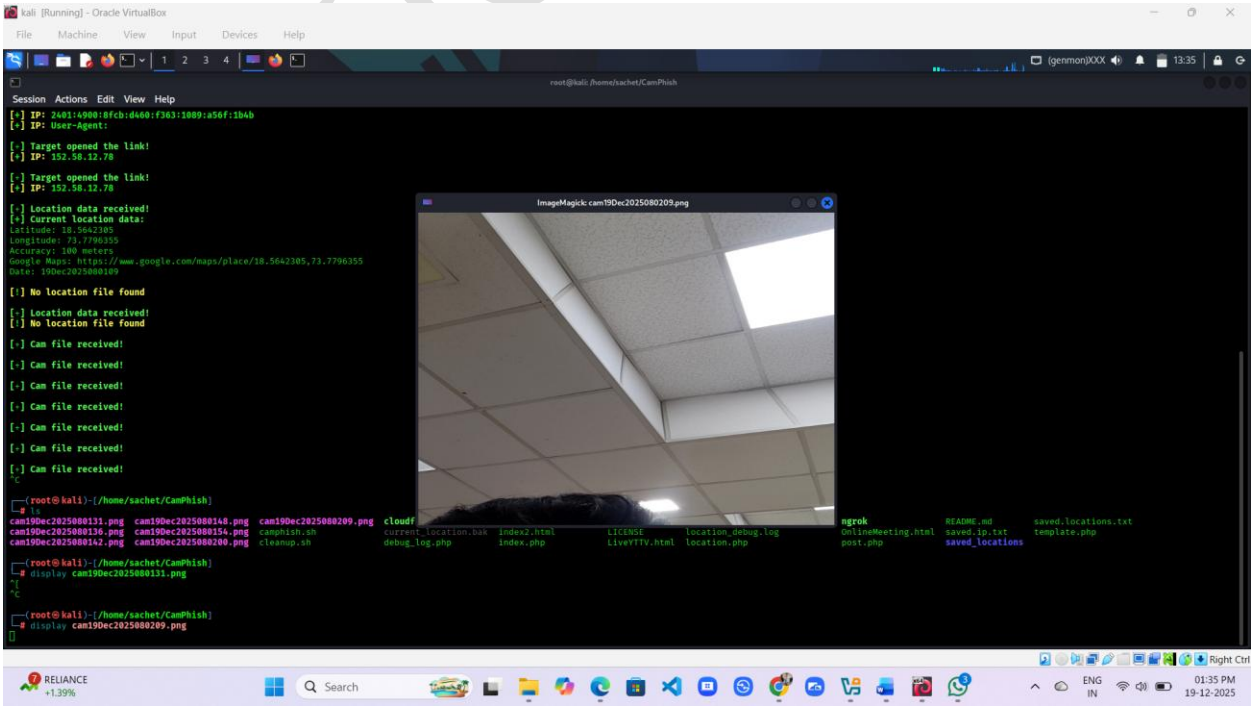
- Link Generated



• Paste link on Browser



• Here It capture the photos and Location



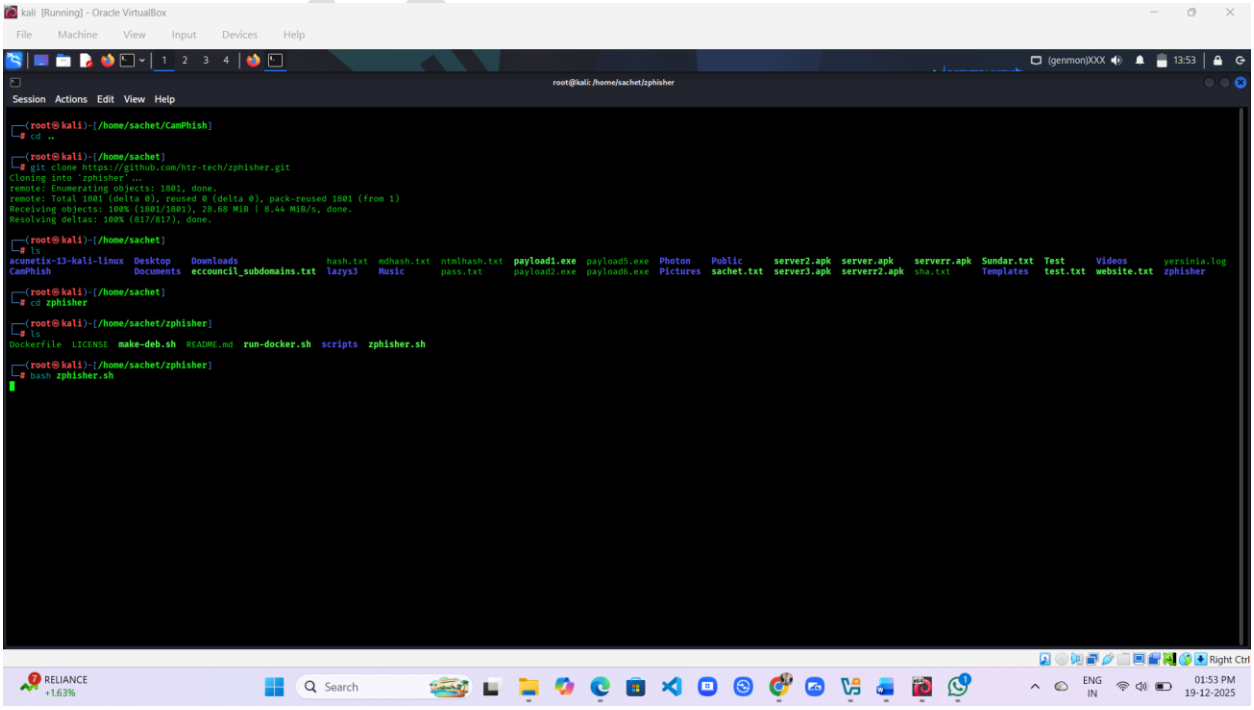
Perform Phishing Attack Using Zphisher

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.

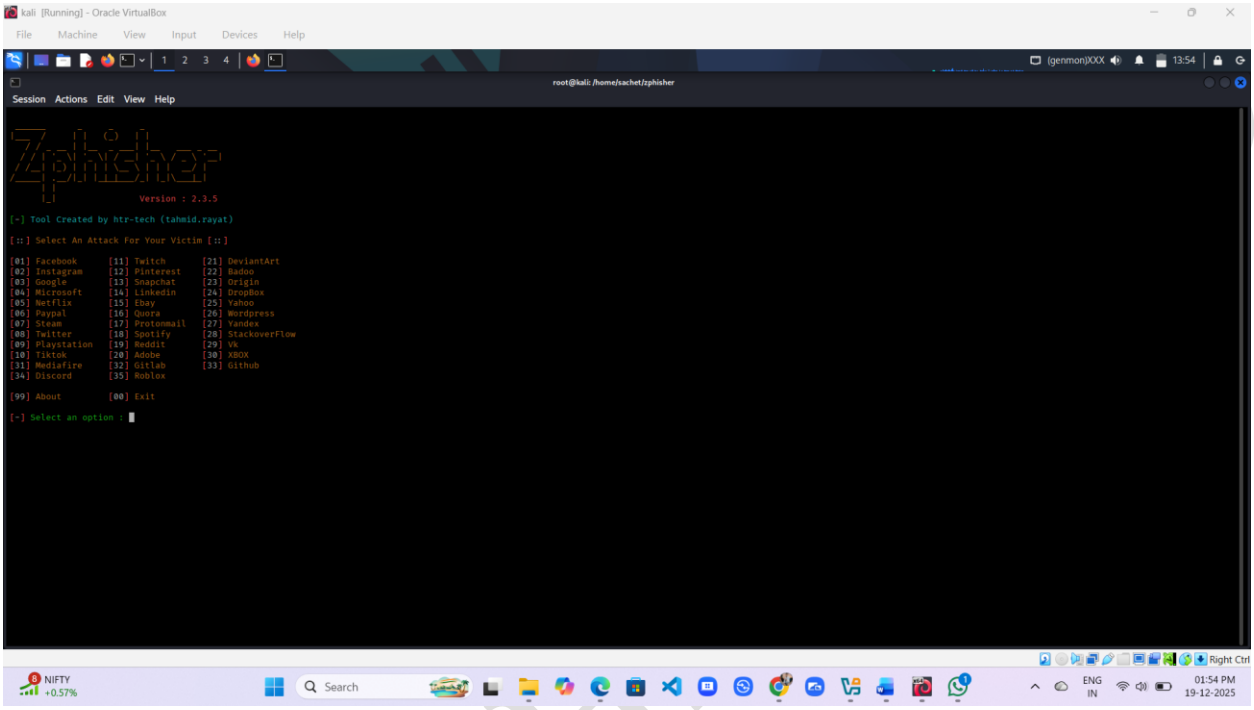
Download Link -: https://github.com/Tohidkhan6332/zphisher

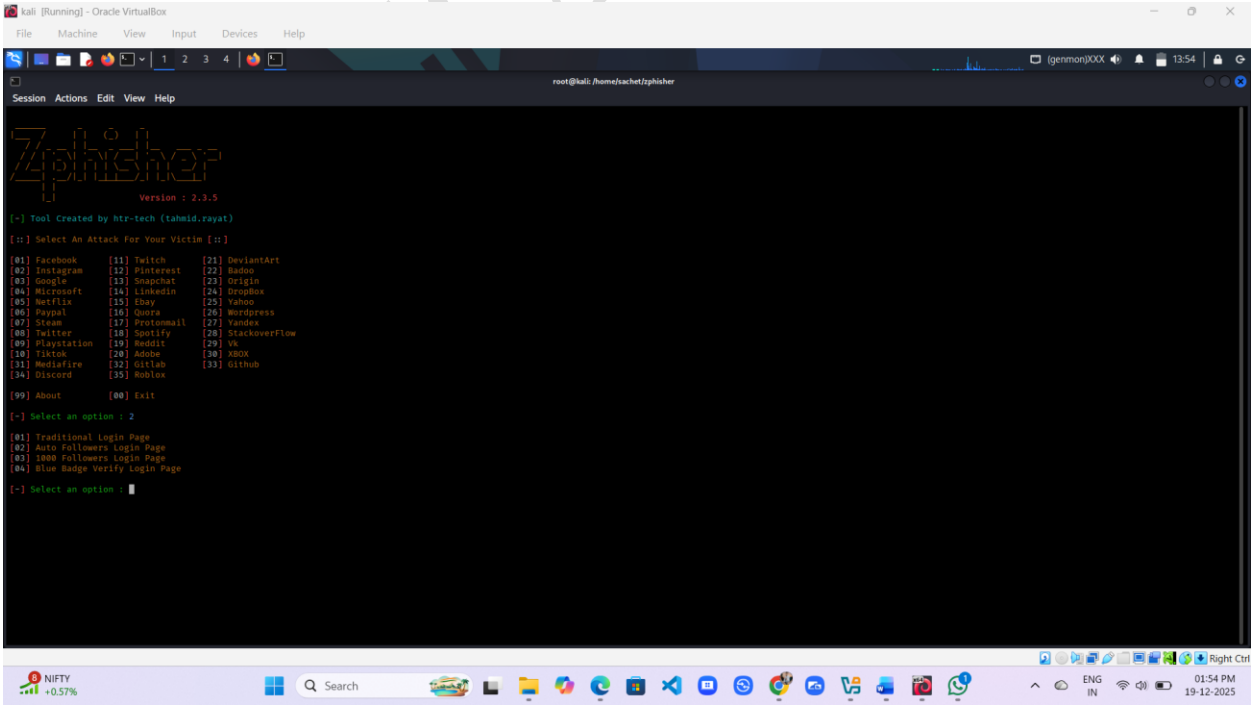
How to use It -:

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

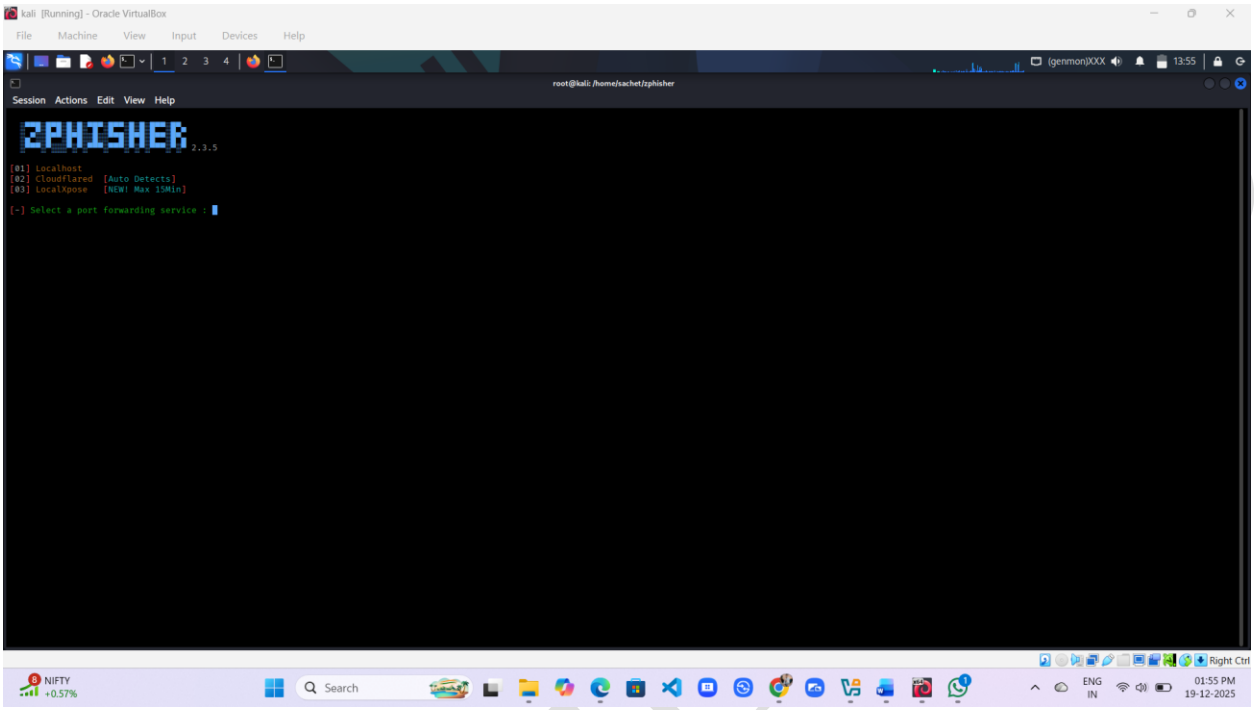


- Zphisher open
- Now select the number that you want to create phishing page

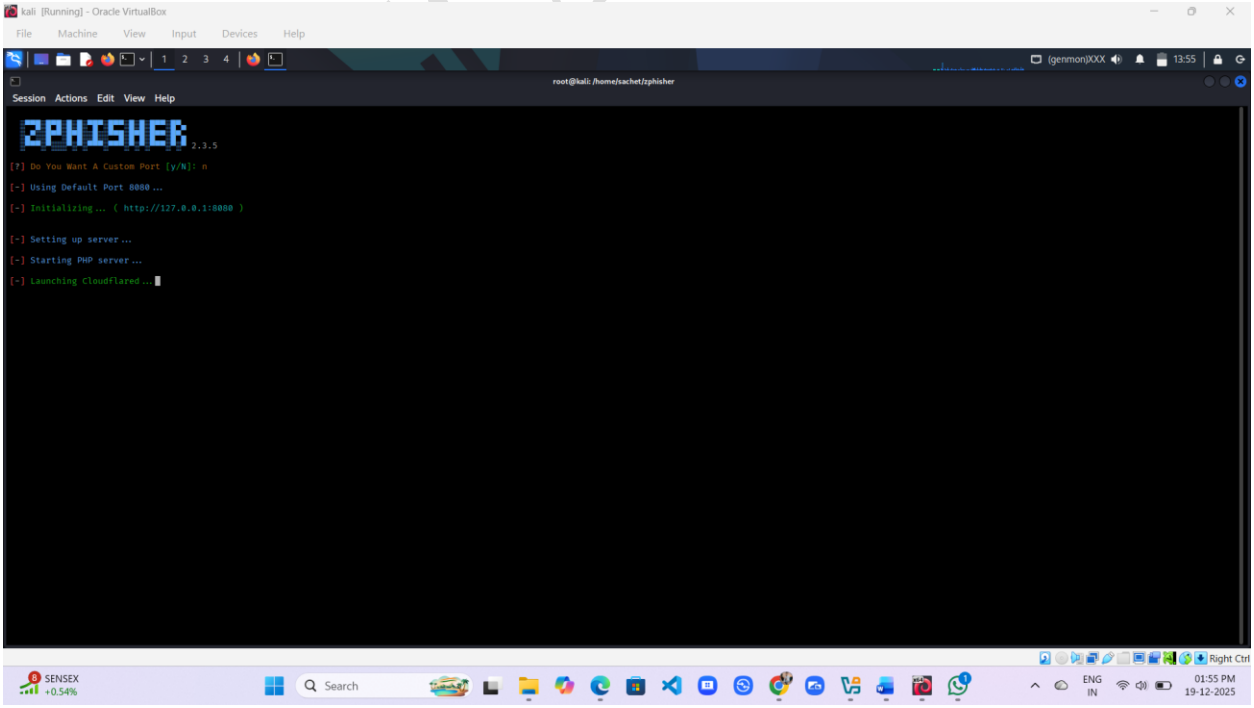




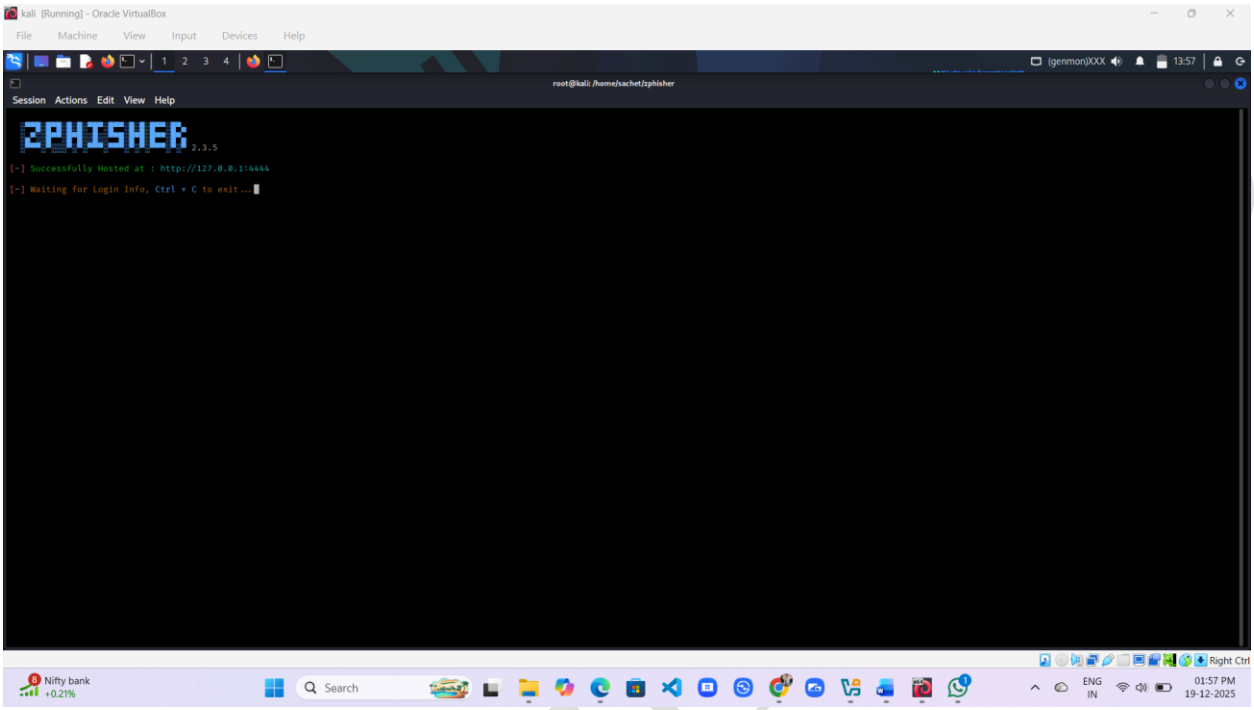
• Now select the cloudflared server -2



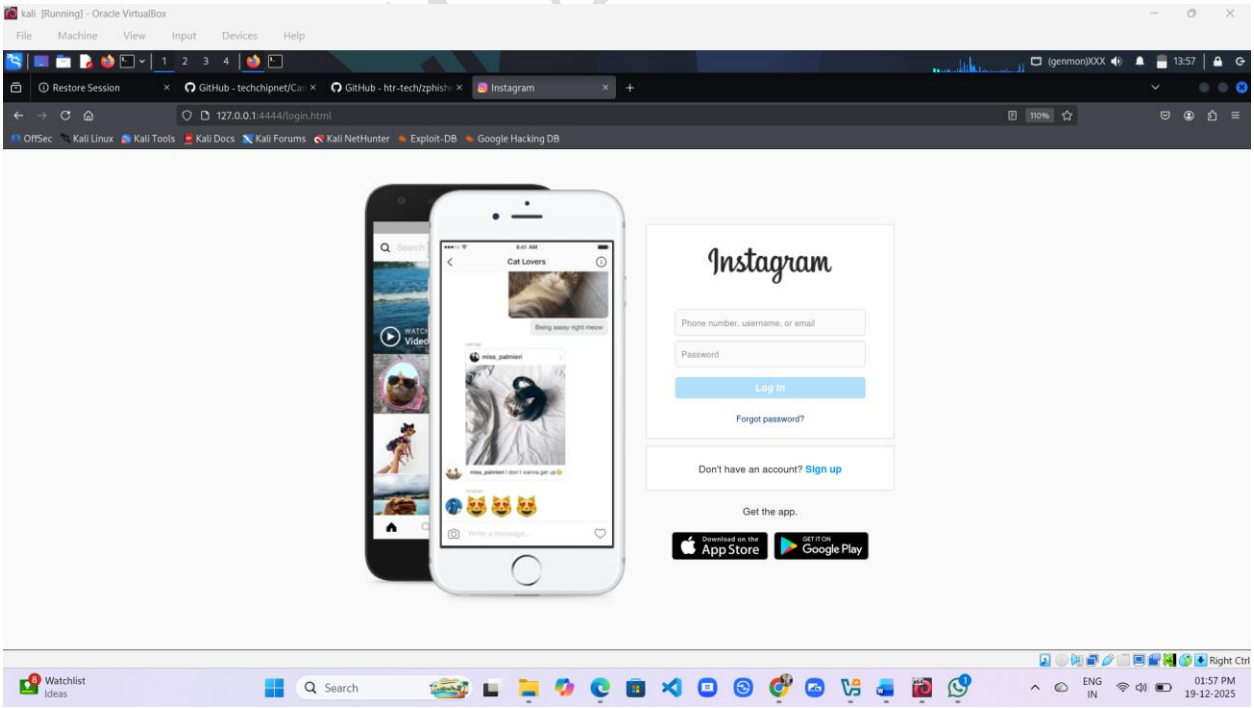
• Zphisher started for generate the link



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



• Now Provide Credentials



Perform Phishing Attack Using ShellPhish

ShellPhish is a social engineering–based phishing framework used in **authorized lab environments** to demonstrate how attackers imitate popular platforms to steal sensitive information. It doesn't "hack" systems—it **asks nicely and lies confidently**.

Classic move. Works way too often.

Objective of the Experiment

- To understand website-based phishing techniques
- To analyze how fake login pages mimic real services
- To study user behavior and trust exploitation
- To emphasize awareness and prevention of phishing attacks

Learning the enemy's mindset, not joining their team.

Tool Used

ShellPhish

- Linux-based phishing simulation framework
- Uses cloned login pages of popular websites
- Designed for cybersecurity awareness and training

Simple tool. Dangerous results—when users stop thinking.

Conceptual Working of ShellPhish

High-level view only. No buttons, no recipes:

1. **Website Cloning Concept**
   ShellPhish replicates the appearance of legitimate websites to create convincing fake login pages.
2. **Social Engineering Phase**
   Victims are lured via trust, urgency, or curiosity—because humans are predictable under pressure.

3. **Credential Capture (Simulation)**
   When users enter login details, the tool demonstrates how credentials can be exposed in a phishing scenario.
4. **Awareness Outcome**
   The goal is to show how easily trust can be abused when verification is skipped.

Why ShellPhish Works

- Familiar website designs lower suspicion
- Users rush instead of verifying URLs
- Visual trust beats logical caution
- Repetition makes scams feel “normal”

How to use It -:

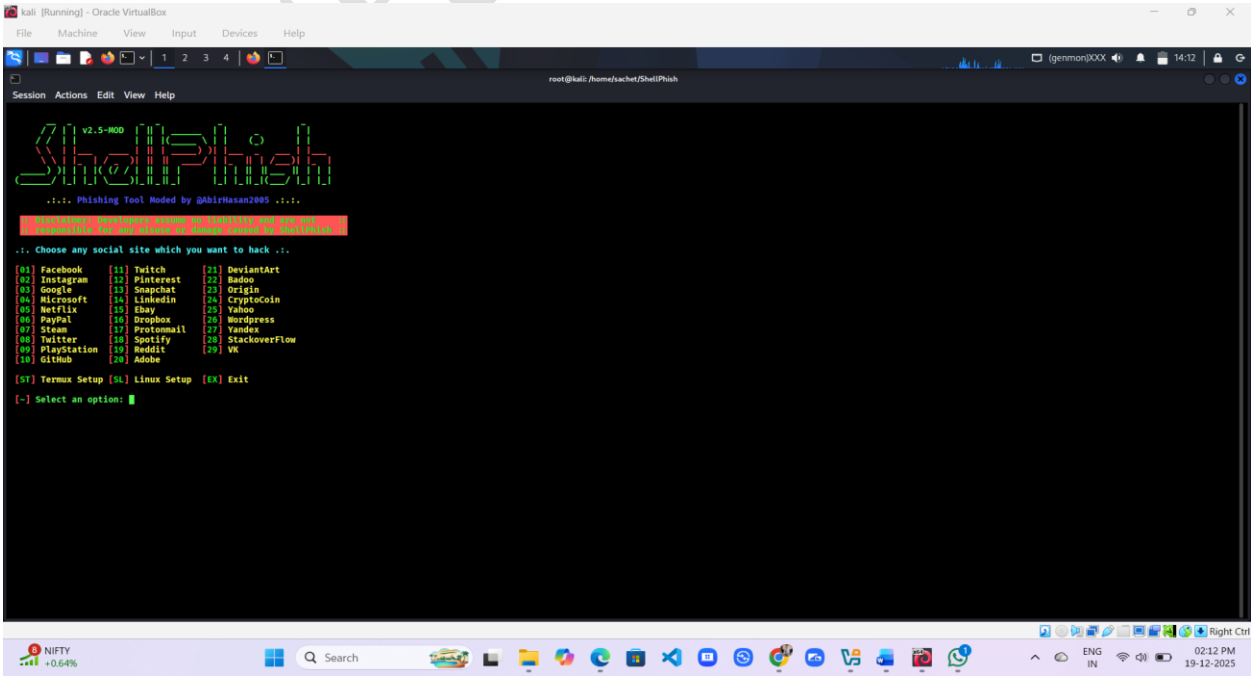
• Download from GitHub

• Open kali linux terminal and go to the ShellPhish directory

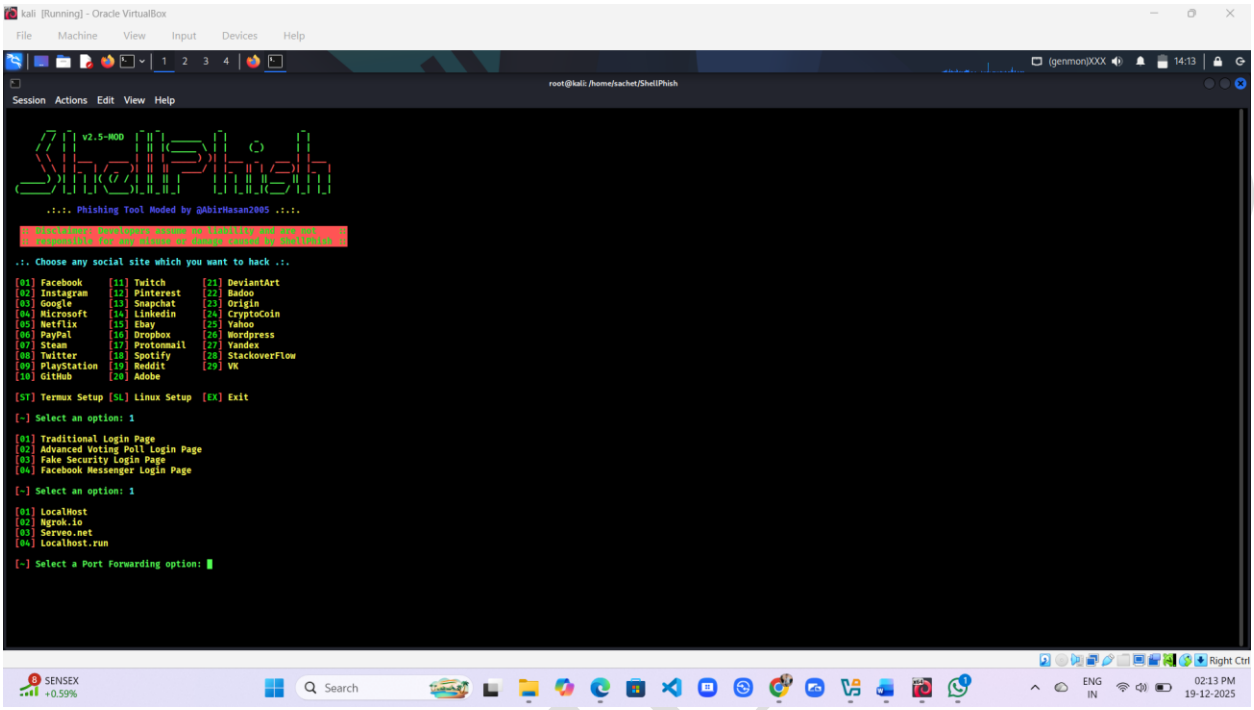
• And use command – bash ShellPhish.sh

• Zphisher open

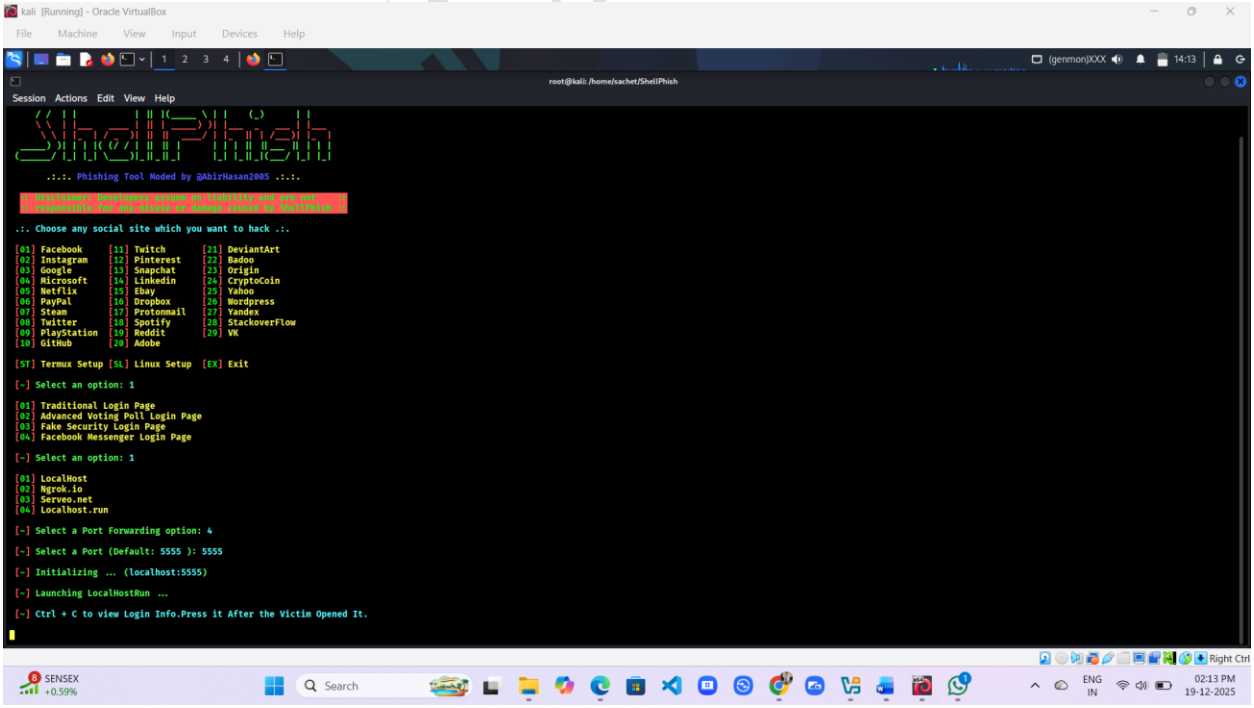
• Now select the number that you want to create phishing page



• Now select the Traditional Login Page

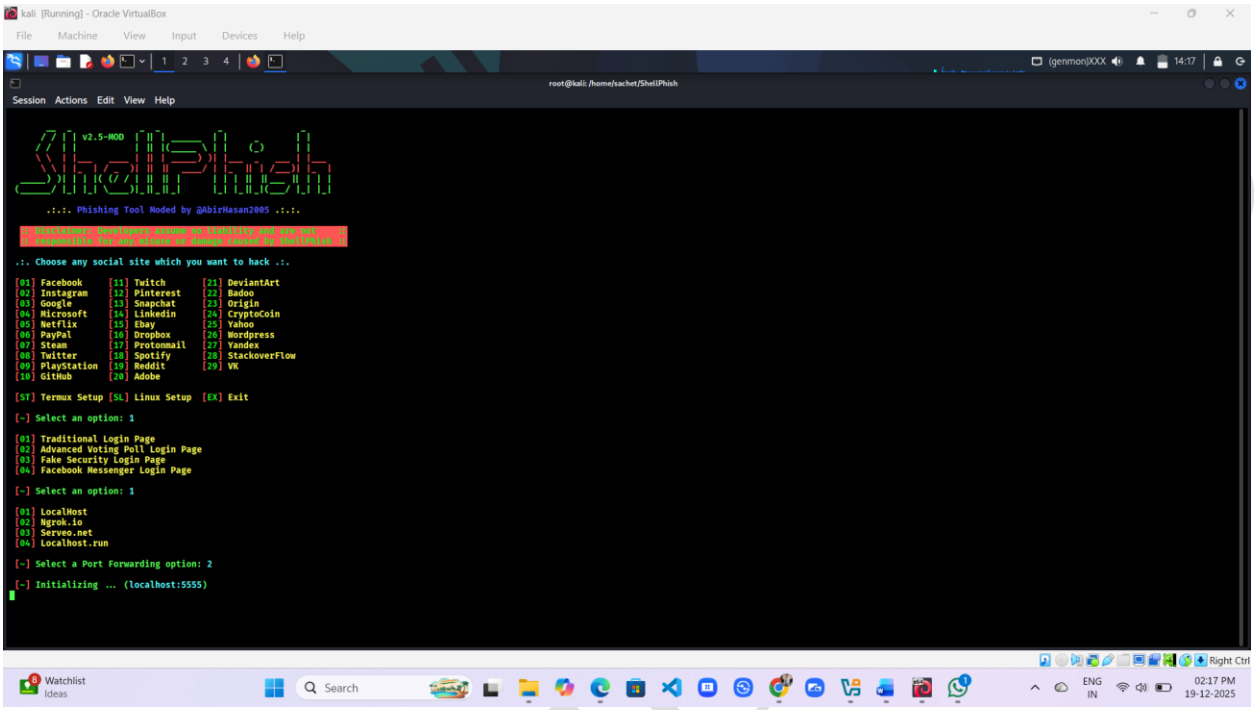


• Now select the Ngrok.io



• Here link is generated

• Now copy link and send it to the target

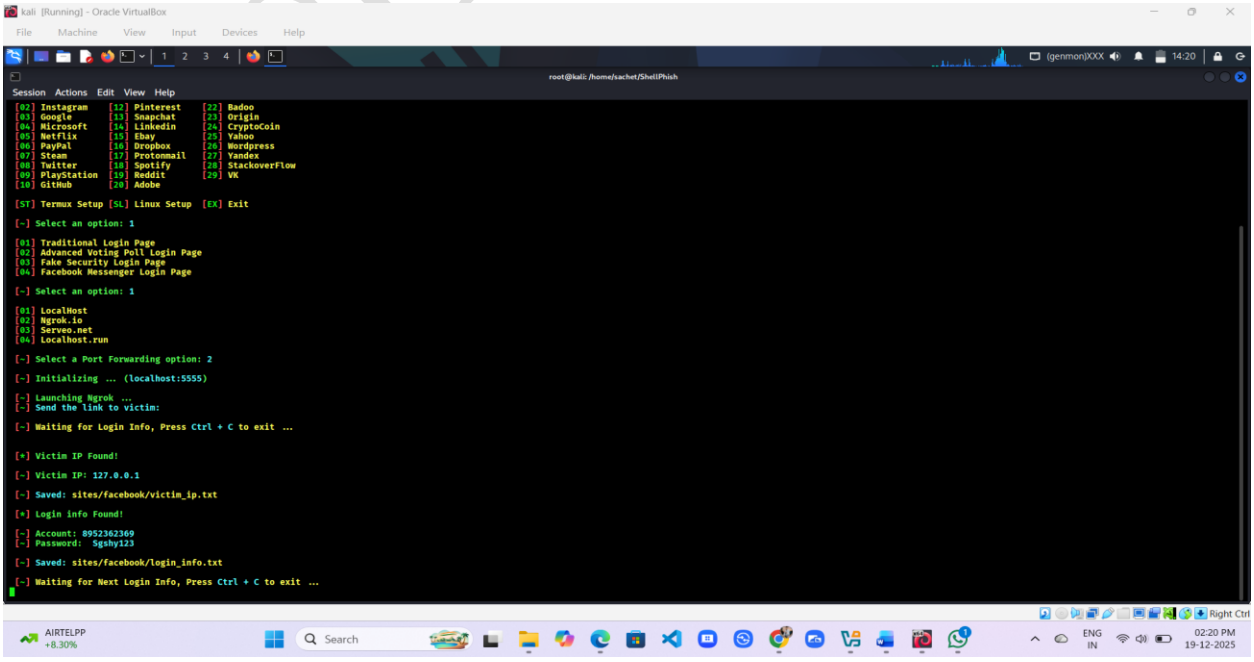


• Paste link in the url section

• Fake amazon login page open

• Now open kali linux teminal

• Username and password are captured



Social Engineering Countermeasures

Social Engineering

Social engineering attacks exploit human trust, not technical flaws. To defend against them, organizations must combine **policies, awareness, physical security, and technical controls**. Writing policies isn't enough—they must be taught, practiced, and enforced.

---

1. Security Awareness & Training

- Train employees on social engineering tactics
- Conduct regular awareness programs and mock drills
- Ensure users acknowledge and understand security policies

Truth bomb: an untrained user is an attacker's favorite tool.

---

2. Password Policies

- Enforce strong, complex passwords
- Change passwords periodically
- Avoid guessable passwords
- Lock accounts after multiple failed attempts
- Maintain confidentiality of passwords

Old rule, still gold: passwords are secrets, not suggestions.

---

3. Physical Security Policies

- Issue employee ID cards
- Escort visitors at all times
- Restrict access to sensitive areas
- Secure physical documents
- Deploy security personnel

If someone can walk in freely, your firewall is just decoration.

---

4. Access Control & Privileges

- Grant access on a need-to-know basis
- Restrict system resources to authorized users
- Regularly review and revoke unused privileges

Less access = less damage.

---

5. Incident Response & Monitoring

- Ensure quick incident response
- Scrutinize suspicious requests or information
- Report and analyze security incidents promptly

Speed matters. Silence kills.

---

6. Background Checks & Termination Process

- Conduct employee background verification
- Immediately revoke access after employee termination

Insiders aren't always innocent. Facts > feelings.

---

7. Technical Defenses

- Use anti-virus and anti-phishing tools
- Implement two-factor authentication (2FA)
- Keep software and systems regularly updated
- Adopt proper change management procedures

Tech supports people—but doesn't replace thinking.

---

8. Defense Strategy

- Run social engineering awareness campaigns
- Perform gap analysis to identify weaknesses
- Apply remediation strategies to fix gaps

Security isn't a one-time setup. It's maintenance—like discipline.

Core Idea

Good policies fail when:

- Employees aren't trained
- Rules aren't reinforced
- Accountability is missing

After training, users should *acknowledge* they understand the policies. Old-school? Yes. Effective? Also yes.

The main objective here is to:

- Raise **user awareness**
- Strengthen **internal network controls**
- Enforce **secure policies, plans, and processes**

Additional Countermeasures (Continued)

1. Training individuals on security policies
2. Implementing proper access privileges
3. Ensuring quick incident response
4. Restricting resources to authorized users
5. Scrutinizing information before sharing
6. Conducting background checks and proper termination procedures
7. Using anti-virus and anti-phishing tools
8. Implementing two-factor authentication
9. Adopting documented change management
10. Keeping software regularly updated

Conclusion

Social engineering works because humans rush, trust, and assume. Countermeasures work when people **pause, verify, and question**.

Module Summary – Social Engineering

This module walks through the anatomy of social engineering—how attackers don't smash systems, they **sweet-talk humans**. It breaks down the **core concepts** and the **phases of social engineering attacks**, showing how manipulation unfolds step by step.

You covered:

- **Social engineering concepts** and why they work
- **Human-based techniques** (face-to-face, voice, trust abuse)
- **Computer-based techniques** (emails, fake sites, digital bait)
- **Mobile-based techniques** (SMS, calls, apps—small screen, big risk)
- **Impersonation using AI** and fake identities on social networking sites
- **Identity theft** and the many forms it takes
- **Warning signs** of social engineering and phishing attacks
- **Countermeasures** used to defend organizations against these attacks

THANK YOU