

SOCIAL ENGINEERING:

Exploiting Human Trust

A Modern Threat Assessment



Access Actions		
Profile	Status	Notes
Facebook (John Doe's profile)	Transferred ownership to someone else	10 credit score loss
Foodbank (Lunch@workgroup)	Compromised	
Bank of America (John Doe's account)	Several losses	Recovering
Gmail (John Doe's account)	Info disclosed	Accessed
Retirement plan (John Doe's account)	John has no plan	Raid planned
Payroll Card (John Doe's account)	John has card	Data Exfiltrated
Instagram (John Doe's account)	John has bio	Data Collected
Facebook (John Doe's account)	Recent login	Data Enclosed

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

1. Social Engineering Concepts

- 1.1 Definition of Social Engineering
 - 1.2 Types of Social Engineering Attacks
 - 1.2.1 Human-Based Social Engineering Attack
 - 1.2.2 Computer-Based Social Engineering Attack
 - 1.2.3 Mobile-Based Social Engineering Attack
 - 1.3 Common Types of Social Engineering
-

2. Phishing

- 2.1 Definition of Phishing
 - 2.2 Types of Phishing
 - 2.2.1 Email Phishing
 - 2.2.2 Spear Phishing
 - 2.2.3 Whaling
 - 2.2.4 Smishing
 - 2.2.5 Vishing
 - 2.2.6 Pharming
 - 2.2.7 Angler Phishing
 - 2.2.8 Clone Phishing
-

3. Perform Social Engineering Using Various Techniques

- 3.1 Lab Scenario
-

4. Perform Phishing Attack Using SETOOLKIT

- 4.1 Objective of the Lab
 - 4.2 Tool Used
 - 4.3 Working of SETOOLKIT
-

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

MODULE – 9 SOCIAL ENGINEERING

- Now select 1 – Social Engineering Attack

```
kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help

Session Actions Edit View Help
root@kali:/home/sachet
[---]  The Social-Engineer Toolkit (SET)
[---]  Created By: David Kennedy (ReL1K)
[---]  codename: Maverick
[---]  Follow us on Twitter: @trustSec
[---]  Follow me on Twitter: @hackingDave
[---]  Home Page: https://www.trustedsec.com
[---]  Welcome to the Social-Engineer Toolkit (SET).
[---]  The one stop shop for all of your SE needs.

The Social-Engineer Toolkit is a product of TrustedSec.
Visit: https://www.trustedsec.com

It's easy to update using the PenTesters Framework! (PTF)
Visit https://github.com/trustedsec/ptf to update all your tools!

Unable to check for new version of SET (is your network up?)

Select from the menu:
1) Social-Engineering Attacks
2) Penetration Testing (Fast-Track)
3) Third Party Modules
4) Update the Social-Engineer Toolkit
5) Update SET configuration
6) Help, Credits, and About
99) Exit the Social-Engineer Toolkit

set> [ ]
```

MODULE – 9 SOCIAL ENGINEERING

- Now select 8 –

```
kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Session Actions Edit View Help
[---] The Social-Engineer Toolkit (SET)
[---] Created by: David Kennedy (ReL1K)
[---] Version: 8.0.4
[---] Contact: dkeith@pentestmonkey.net
[---] Follow us on Twitter: @TrustedSec
[---] Follow me on Twitter: @HackingDave
[---] Homepage: https://www.trustedsec.com
[---] Welcome to the Social-Engineer Toolkit (SET).
[---] The one stop shop for all of your SE needs.

The Social-Engineer Toolkit is a product of TrustedSec.

Visit: https://www.trustedsec.com

It's easy to update using the PenTesters Framework (PTF)
Visit https://github.com/trustedsec/ptf to update all your tools!

Unable to check for new version of SET (is your network up?)

Select from the menu:
1) Spear-Phishing Attack Vectors
2) Website Attack Vectors
3) Infectious Media Generator
4) Create a Payload and Listener
5) Java Applet
6) Arduino-Based Attack Vector
7) Wireless Access Point Attack Vector
8) QRCode Generator Attack Vector
9) PowerShell Attack Vectors
10) Third Party Modules

99) Return back to the main menu.

set> 8

QRCode Attack Vector will create a QRCode for you with whatever URL you want.

When you have the QRCode Generated, select an additional attack vector within SET and deploy the QRCode to your victim. For example, generate a QRCode of the SET Java Applet and send the QRCode via a mailer.

Enter the URL you want the QRCode to go to (99 to exit): instagram.com
```

Enter the URL you want the QRCode

```
kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Session Actions Edit View Help
[---] The Social-Engineer Toolkit (SET)
[---] Created by: David Kennedy (ReL1K)
[---] Version: 8.0.4
[---] Contact: dkeith@pentestmonkey.net
[---] Follow us on Twitter: @TrustedSec
[---] Follow me on Twitter: @HackingDave
[---] Homepage: https://www.trustedsec.com
[---] Welcome to the Social-Engineer Toolkit (SET).
[---] The one stop shop for all of your SE needs.

The Social-Engineer Toolkit is a product of TrustedSec.

Visit: https://www.trustedsec.com

It's easy to update using the PenTesters Framework (PTF)
Visit https://github.com/trustedsec/ptf to update all your tools!

Unable to check for new version of SET (is your network up?)

Select from the menu:
1) Spear-Phishing Attack Vectors
2) Website Attack Vectors
3) Infectious Media Generator
4) Create a Payload and Listener
5) Java Applet
6) Arduino-Based Attack Vector
7) Wireless Access Point Attack Vector
8) QRCode Generator Attack Vector
9) PowerShell Attack Vectors
10) Third Party Modules

99) Return back to the main menu.

set> 8

QRCode Attack Vector will create a QRCode for you with whatever URL you want.

When you have the QRCode Generated, select an additional attack vector within SET and deploy the QRCode to your victim. For example, generate a QRCode of the SET Java Applet and send the QRCode via a mailer.

Enter the URL you want the QRCode to go to (99 to exit): instagram.com
```

MODULE – 9 SOCIAL ENGINEERING

QRCode has been generated

```
kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Session Actions Edit View Help
[...]
root@kali:~/home/sachet
[...]
The Social-Engineer Toolkit (SET)
Created By: David Kennedy (ReL1K)
[...]
codename: 'Maverick'
[...]
Follow us on Twitter: @TrustedSec
[...]
Follow us on Facebook: @TrustedSec
[...]
Home Page: https://www.trustedsec.com
Welcome to the Social-Engineer Toolkit (SET).
The one stop shop for all of your SE needs.

The Social-Engineer Toolkit is a product of TrustedSec.
Visit: https://www.trustedsec.com

It's easy to update using the PenTesters Framework! (PTF)
Visit https://github.com/trustedsec/ptf to update all your tools!

Unable to check for new version of SET (is your network up?)

Select from the menu:

1) Spear-Phishing Attack Vectors
2) Website Attack Vectors
3) Infection Media Generator
4) TCP & Port Listener and Listener
5) Mass Mailer Attack
6) Arduino-Based Attack Vector
7) Wireless Access Point Attack Vector
8) Network Sniffer Attack Vector
9) Powershell Attack Vectors
10) Third Party Modules

99) Return back to the main menu.

set> 8

The QRCode Attack Vector will create a QRCode for you whatever URL you want.

When you have the QRCode Generated, select an additional attack vector within SET and
double click on the QRCode. For example, generate a QRCode of the SET Java Applet
and send the QRCode via a maller.

Enter the URL you want the QRCode to go to (99 to exit): instagram.com
[*] QRCode has been generated under /root/.set/reports/qrcode.attack.png

Press <return> to continue

[...]
AIRTELPP +8.34% Search
[...]
10:05 PM 19-12-2025
```

Now display

A screenshot of a Kali Linux desktop environment. The terminal window shows a root shell session where a QR code has been generated and displayed. The command used was 'display /root/.set/reports/qrcode_attack.png'. The QR code is centered in a white window titled 'ImageMagick: qrcode_attack.png'. The desktop taskbar at the bottom includes icons for File Explorer, File Manager, Terminal, and a camera. The system tray shows battery level (8.34%), signal strength, and system status. The system clock indicates it's 01:05 PM on 19-12-2025.

Perform Phishing Attack Using CamPhish Tool

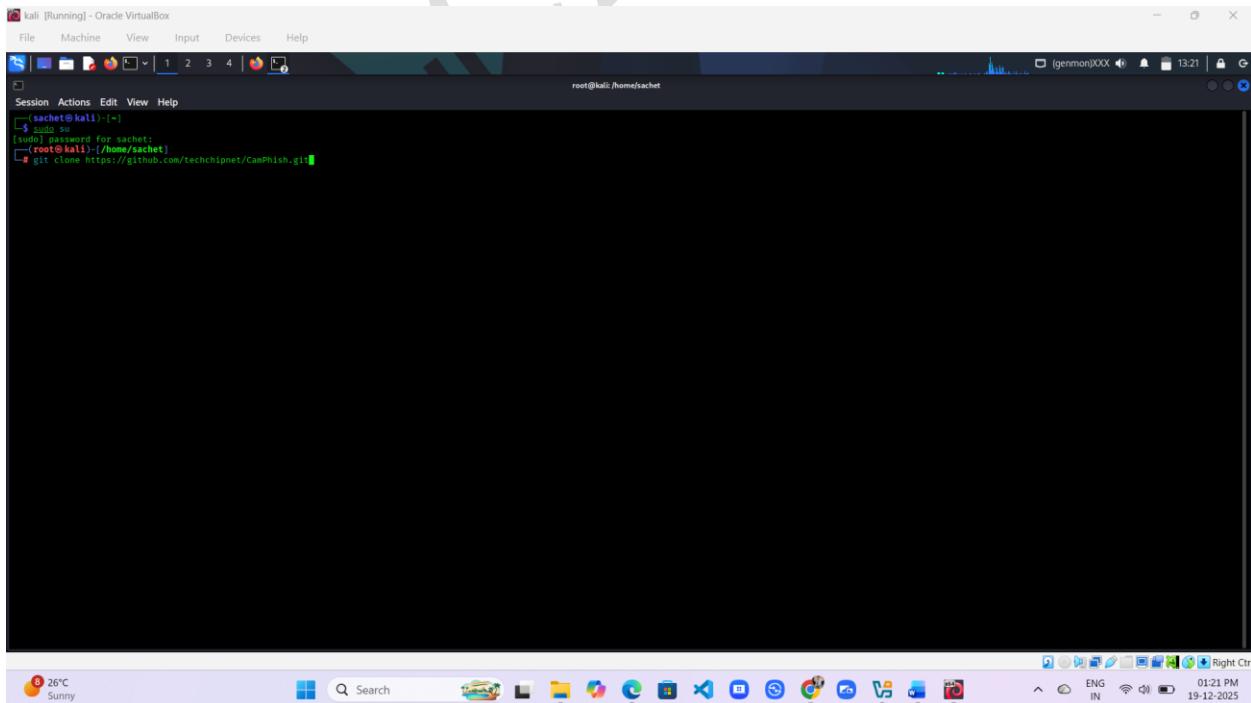
CamPhish is a social engineering-based phishing tool used in controlled environments to demonstrate how attackers exploit curiosity and trust to extract sensitive data. Instead of brute-force hacking, CamPhish relies on deception, proving once again that humans are the softest entry point.

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



```
kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Session Actions Edit View Help
root@sachet:kali:~#
$ sudo su
[sudo] password for sachet:
(root@kali:~# /home/sachet]
# git clone https://github.com/techchipnet/CamPhish.git
```

MODULE – 9 SOCIAL ENGINEERING

Open kali linux terminal go to the camphish directory

```
kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Session Actions Edit View Help
[sachet@kali:~]
$ sudo su
[sudo] password for sachet:
(root@kali:~/home/sachet)
# git clone https://github.com/techchipnet/CamPhish.git
fatal: destination path 'CamPhish' already exists and is not an empty directory.
[root@kali:~/home/sachet]
# ls
acunetix-13-kali-linux Desktop Downloads hash.txt mdhash.txt ntlmhash.txt payload1.exe payload5.exe Photon Public server2.apk server.apk serverr.apk Sundar.txt Test Videos yersinia.log
CamPhish Documents ecountil_subdomains.txt lazy3 Music pass.txt payload2.exe payload4.exe Pictures sachet.txt server3.apk server22.apk sha1.txt Templates test.txt website.txt
[root@kali:~/home/sachet]
# cd ..
[root@kali:~/]
# cd CamPhish
[root@kali:~/home/sachet/CamPhish]
# ls
```

- Type command –bash camphish

```
kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Session Actions Edit View Help
[sachet@kali:~]
$ sudo su
[sudo] password for sachet:
(root@kali:~/home/sachet)
# git clone https://github.com/techchipnet/CamPhish.git
fatal: destination path 'CamPhish' already exists and is not an empty directory.
[root@kali:~/home/sachet]
# ls
acunetix-13-kali-linux Desktop Downloads hash.txt mdhash.txt ntlmhash.txt payload1.exe payload5.exe Photon Public server2.apk server.apk serverr.apk Sundar.txt Test Videos yersinia.log
CamPhish Documents ecountil_subdomains.txt lazy3 Music pass.txt payload2.exe payload4.exe Pictures sachet.txt server3.apk server22.apk sha1.txt Templates test.txt website.txt
[root@kali:~/home/sachet]
# cd ..
[root@kali:~/]
# cd CamPhish
[root@kali:~/home/sachet/CamPhish]
# ls
camphish.sh cleanup.sh debug_log.php FestivalWishes.html ip.php LICENSE LiveYTtv.html location.php OnlineMeeting.html post.php README.md template.php
[root@kali:~/home/sachet/CamPhish]
# bash camphish.sh
```

MODULE – 9 SOCIAL ENGINEERING

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

- Link Generated

MODULE – 9 SOCIAL ENGINEERING

- Paste link on Browser

- Here It capture the photos and Location

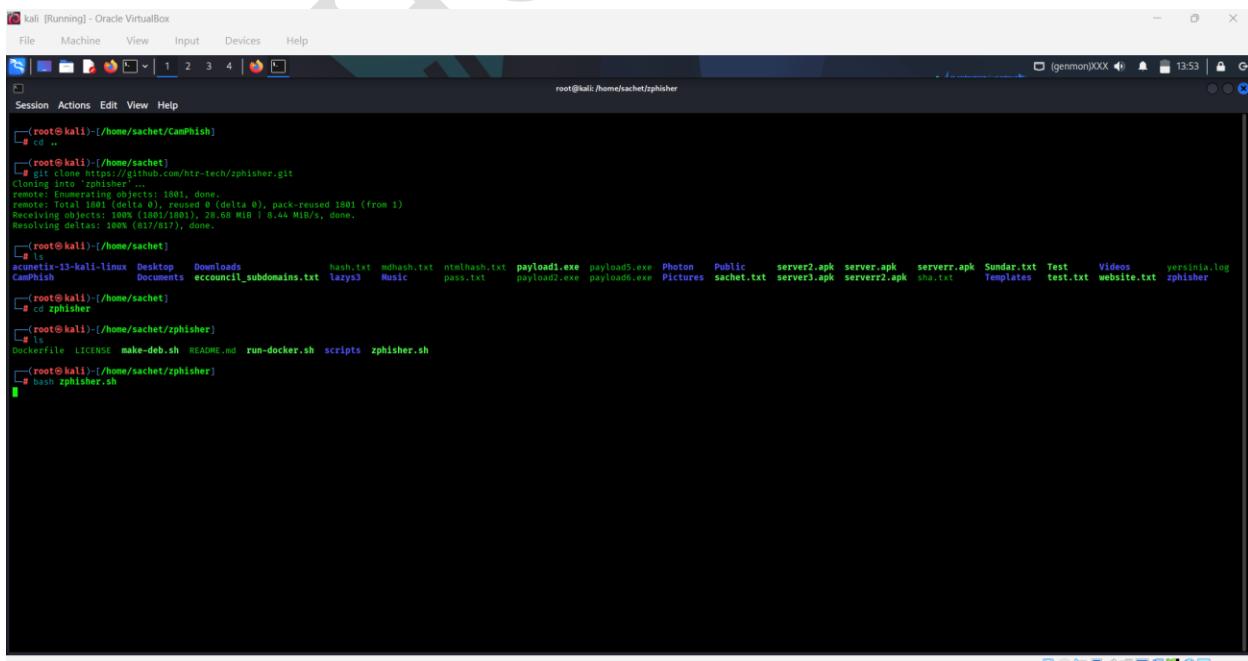
Perform Phishing Attack Using Zphisher

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



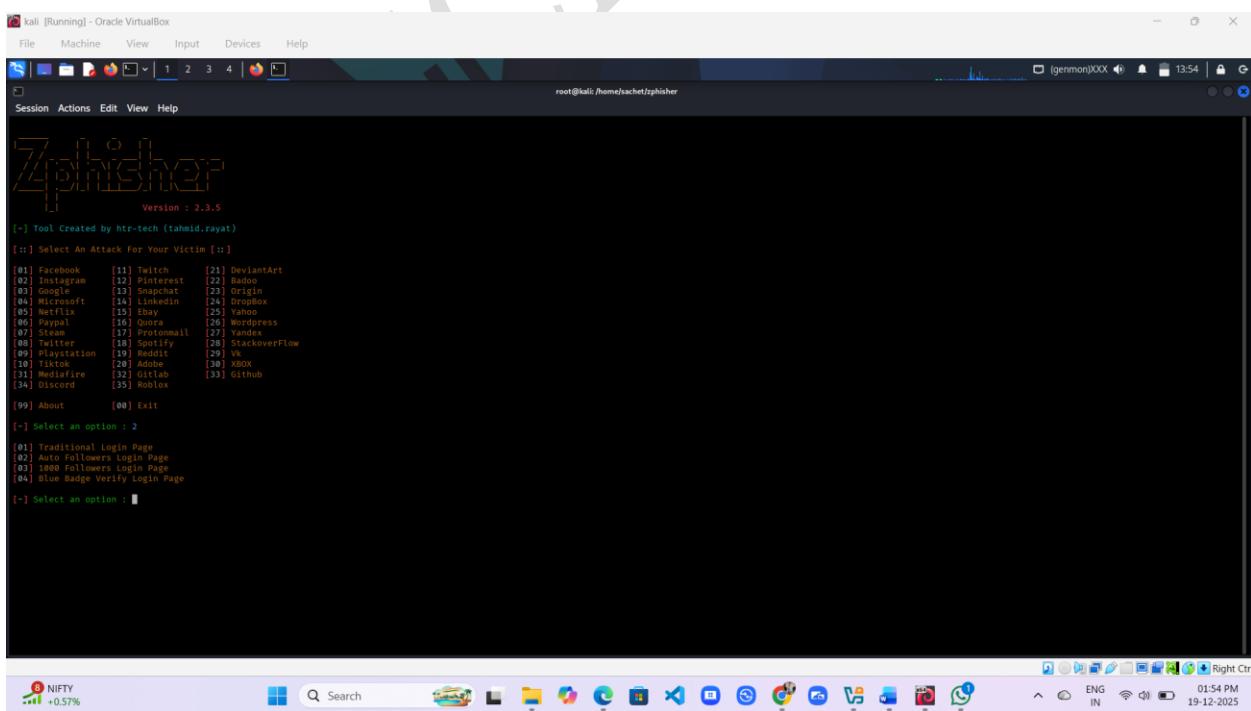
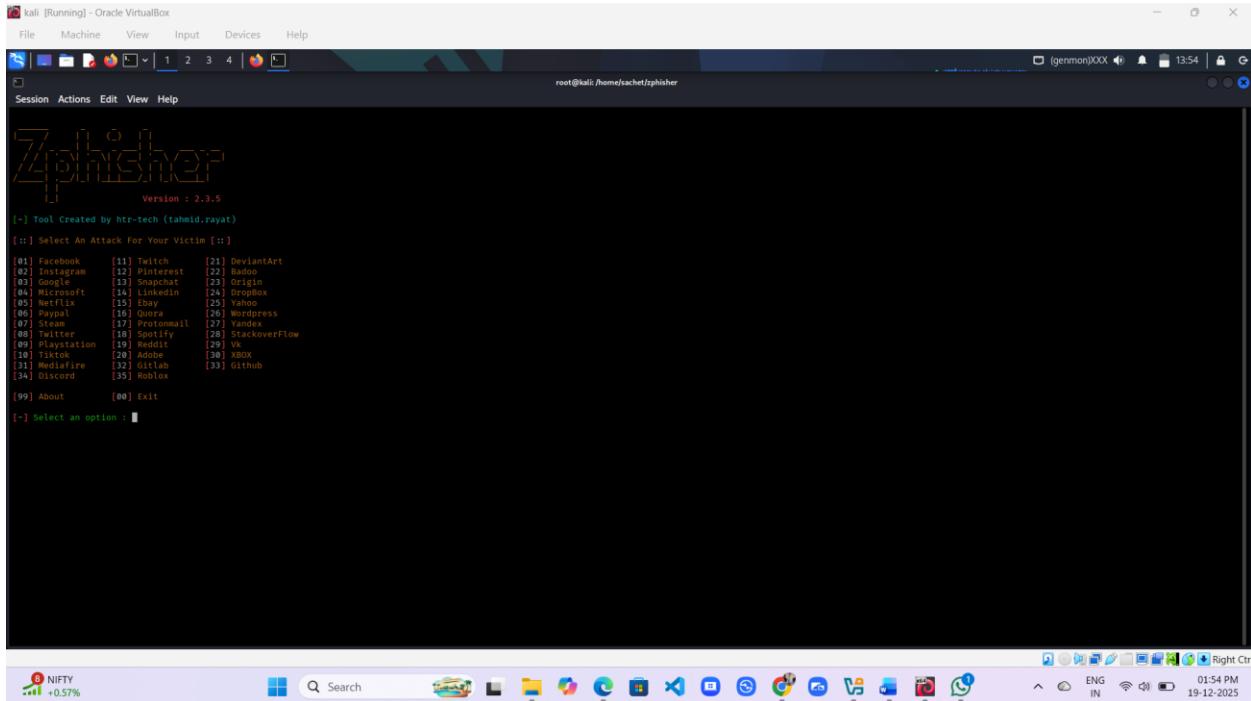
```

kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Session Actions Edit View Help
root@kali:~/home/sachet/zphisher
[root@kali:~/home/sachet] # cd ..
[root@kali:~/home/sachet] # git clone https://github.com/httr-tech/zphisher.git
Cloning into 'zphisher'...
remote: Enumerating objects: 1801, done.
remote: Total 1801 (delta 0), reused 0 (delta 0), pack-reused 1801 (from 1)
Receiving objects: 100% (1801/1801), 28.68 MiB | 8.44 MiB/s, done.
Resolving deltas: 100% (817/817), done.
[root@kali:~/home/sachet] # ls
Desktop Documents eccouncil_subdomains.txt hash.txt mdhash.txt htmlhash.txt payload1.exe payload0.exe Photon Public server3.apk server.apk serverr.apk server2.apk Sundar.txt Test Videos website.txt zphisher
[root@kali:~/home/sachet] # cd zphisher
[root@kali:~/home/sachet/zphisher] # ls
Dockerfile LICENSE make-deb.sh README.md run-docker.sh scripts zphisher.sh
[root@kali:~/home/sachet/zphisher] # bash zphisher.sh

```

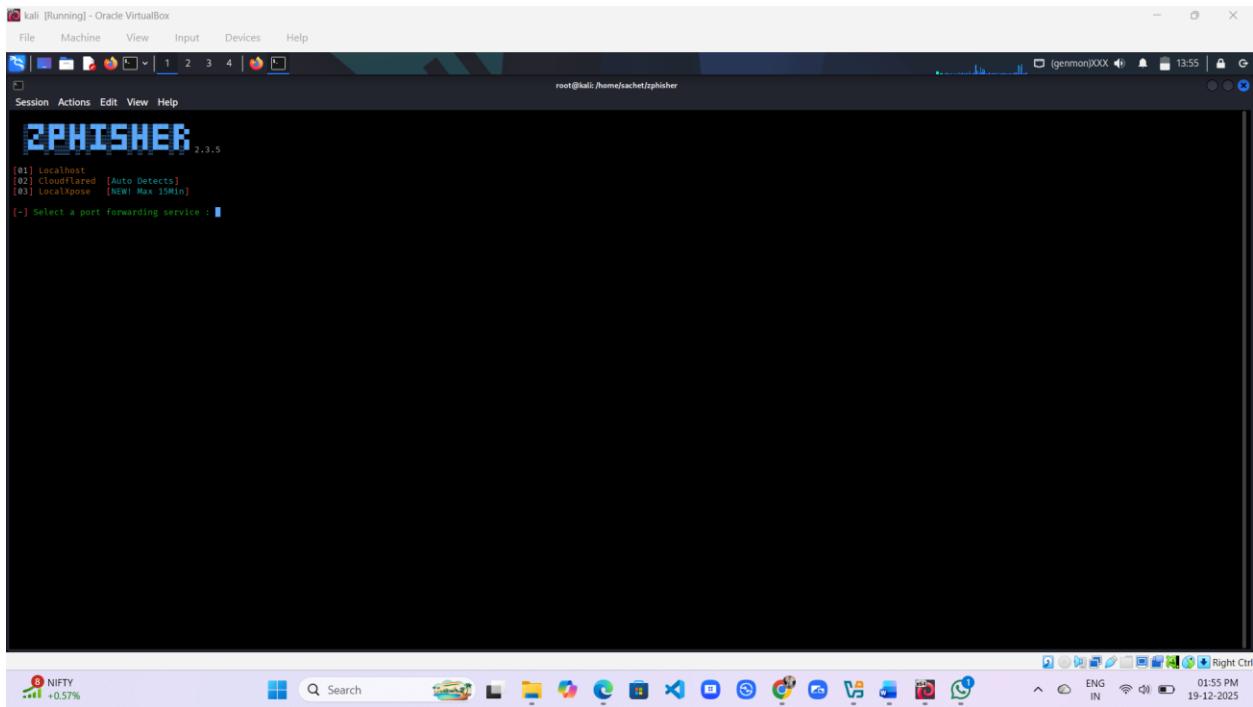
MODULE – 9 SOCIAL ENGINEERING

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

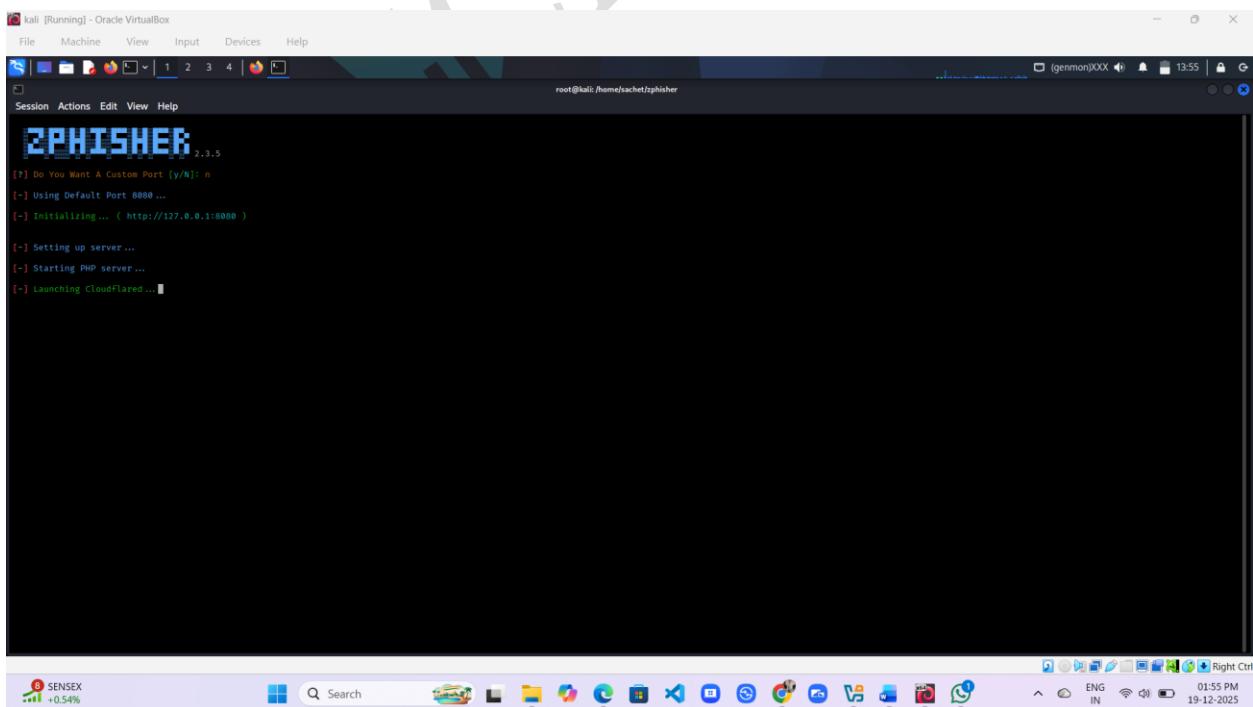


MODULE – 9 SOCIAL ENGINEERING

- Now select the cloudflared server -2

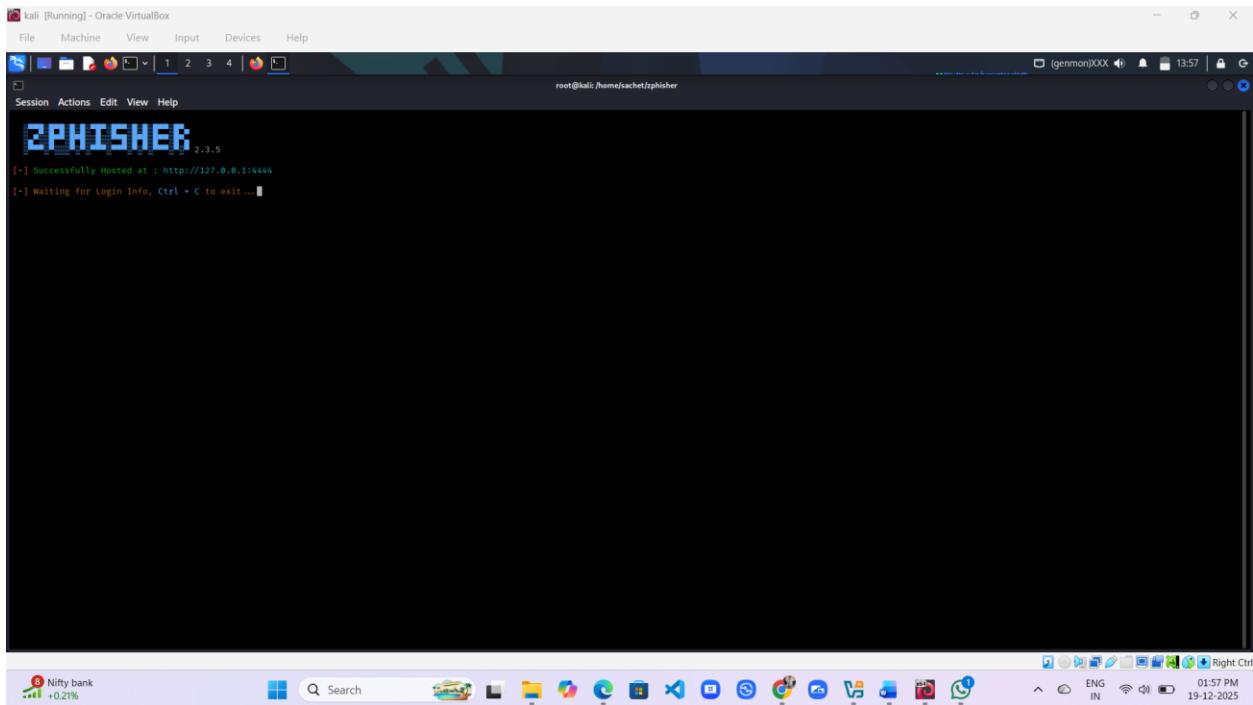


- Zphisher started for generate the link

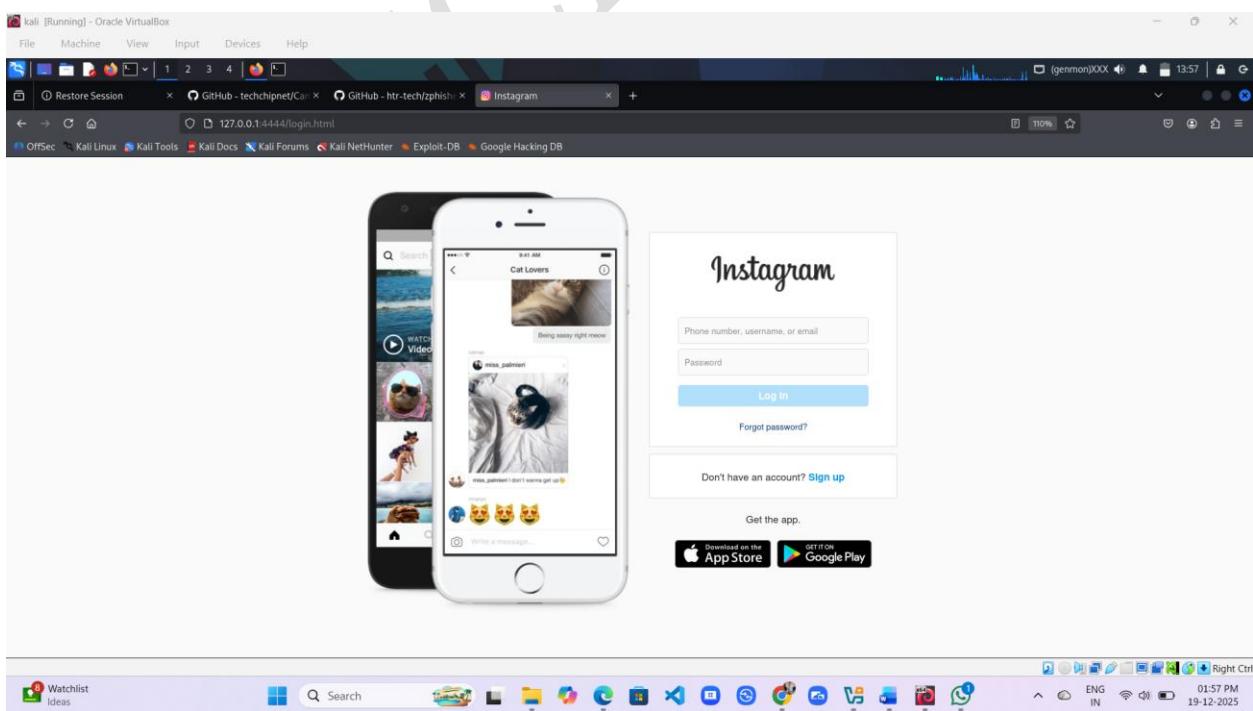


MODULE – 9 SOCIAL ENGINEERING

- 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 :-:

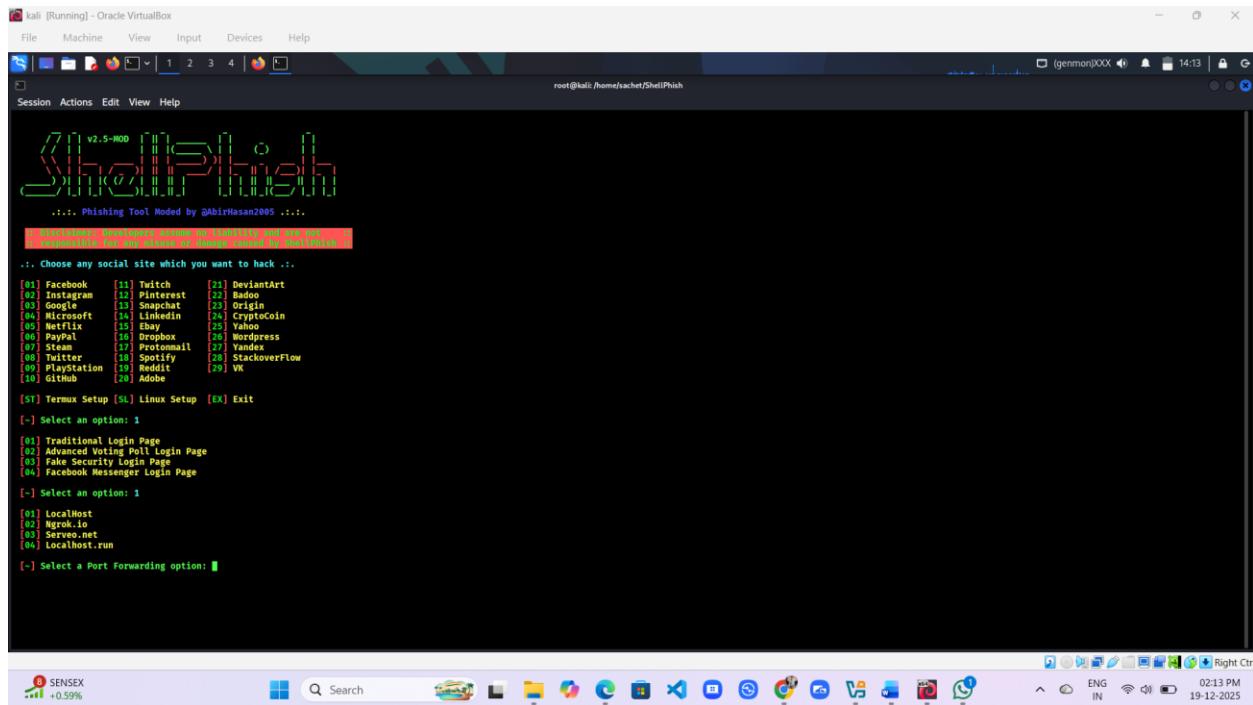
- Download from GitHub
- Open kali linux terminal and go to the ShellPhish directory
- And use command – bash ShellPhish.sh
- Zphisher open
- Now select the number that you want to create phishing page

```
v2.5-M0
[1] Facebook [11] Twitch [21] DeviantArt
[2] Instagram [12] Pinterest [22] Badoo
[3] Google [13] Snapchat [23] Origin
[4] Twitter [14] LinkedIn [24] Robinhood
[5] LinkedIn [15] Ebay [25] Yahoo
[6] Netflix [16] Dropbox [26] Wordpress
[7] Amazon [17] Gmail [27] LinkedIn
[8] PayPal [18] Spotify [28] StackoverFlow
[9] Playstation [19] Reddit [29] VK
[10] GitHub [20] Adobe

[ST] Termux Setup [SL] Linux Setup [EX] Exit
[-] Select an option: 1
```

MODULE – 9 SOCIAL ENGINEERING

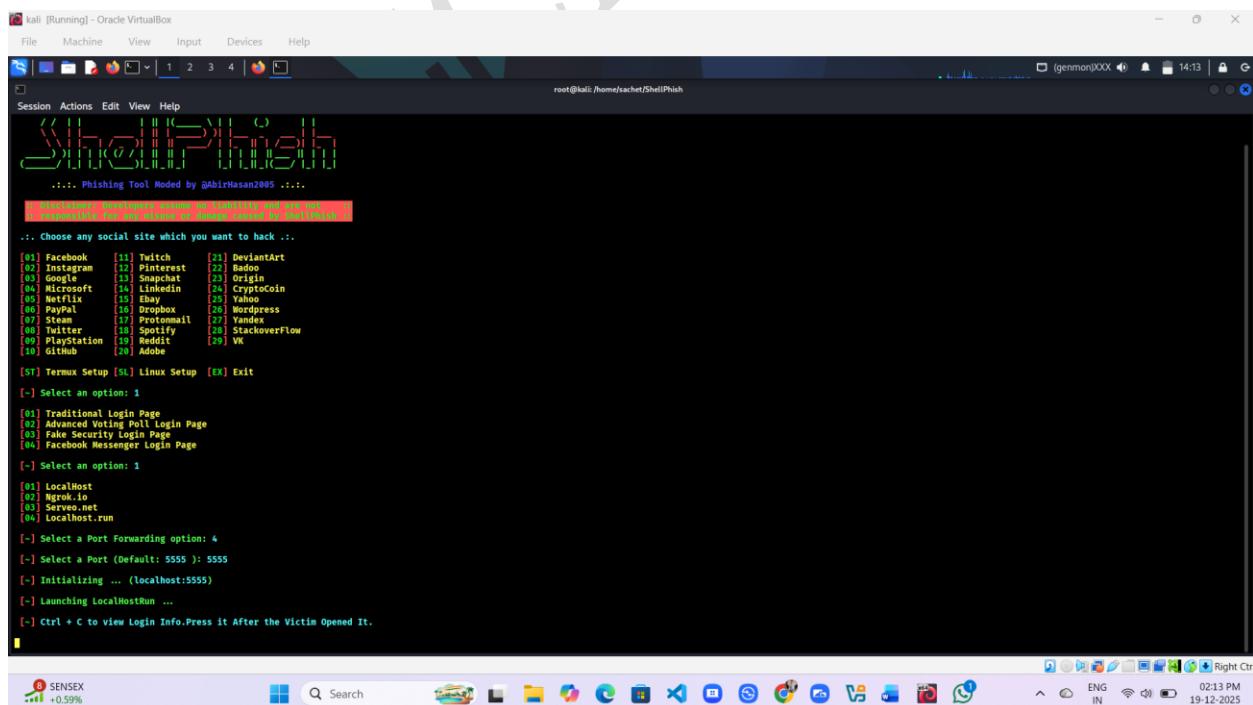
- Now select the Traditional Login Page



```
v2.5-MOD
... Phishing Tool Moded by @AbirHasan2005 ...
[+] Disclaimer: Developers assume no liability and are not ...
[+] responsible for any misuse or damage caused by this tool ...
... Choose any social site which you want to hack ...
[01] Facebook [01] Twitch [21] DeviantArt
[02] Instagram [02] Pinterest [22] Badoo
[03] LinkedIn [03] Snapchat [23] Origin
[04] Microsoft [04] LinkedIn [24] CryptoCoin
[05] Netflix [05] Ebay [25] Yahoo
[06] PayPal [06] Dropbox [26] Wordpress
[07] Steam [07] Protomall [27] Yandex
[08] Twitter [08] Spotify [28] StackoverFlow
[09] Playstation [09] Reddit [29] VK
[10] Github [20] Adobe

[S1] Termux Setup [S2] Linux Setup [EX] Exit
[-] Select an option: 1
[01] Traditional Login Page
[02] Advanced Voting Poll Login Page
[03] Fake Security Login Page
[04] Facebook Messenger Login Page
[-] Select an option: 1
[01] LocalHost
[02] Ngrok.io
[03] Serveo.net
[04] Localhost.run
[-] Select a Port Forwarding option: 1
```

- Now select the Ngrok.io



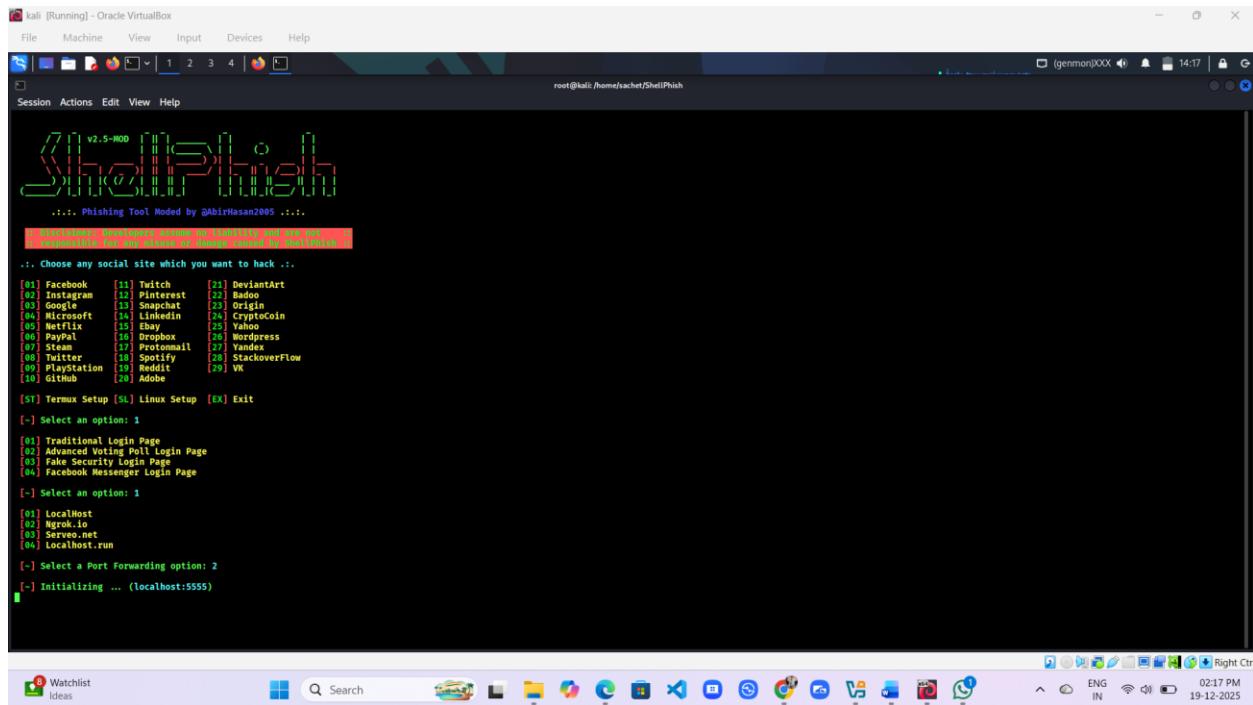
```
v2.5-MOD
... Phishing Tool Moded by @AbirHasan2005 ...
[+] Disclaimer: Developers assume no liability and are not ...
[+] responsible for any misuse or damage caused by this tool ...
... Choose any social site which you want to hack ...
[01] Facebook [01] Twitch [21] DeviantArt
[02] Instagram [02] Pinterest [22] Badoo
[03] LinkedIn [03] Snapchat [23] Origin
[04] Microsoft [04] LinkedIn [24] CryptoCoin
[05] Netflix [05] Ebay [25] Yahoo
[06] PayPal [06] Dropbox [26] Wordpress
[07] Steam [07] Protomall [27] Yandex
[08] Twitter [08] Spotify [28] StackoverFlow
[09] Playstation [09] Reddit [29] VK
[10] Github [20] Adobe

[S1] Termux Setup [S2] Linux Setup [EX] Exit
[-] Select an option: 1
[01] Traditional Login Page
[02] Advanced Voting Poll Login Page
[03] Fake Security Login Page
[04] Facebook Messenger Login Page
[-] Select an option: 1
[01] LocalHost
[02] Ngrok.io
[03] Serveo.net
[04] Localhost.run
[-] Select a Port Forwarding option: 4
[-] Select a Port (Default: 5555 ): 5555
[-] Initializing ... (localhost:5555)
[-] Launching LocalHostRun ...
[-] Ctrl + C to view Login Info.Press it After the Victim Opened It.
```

- Here link is generated

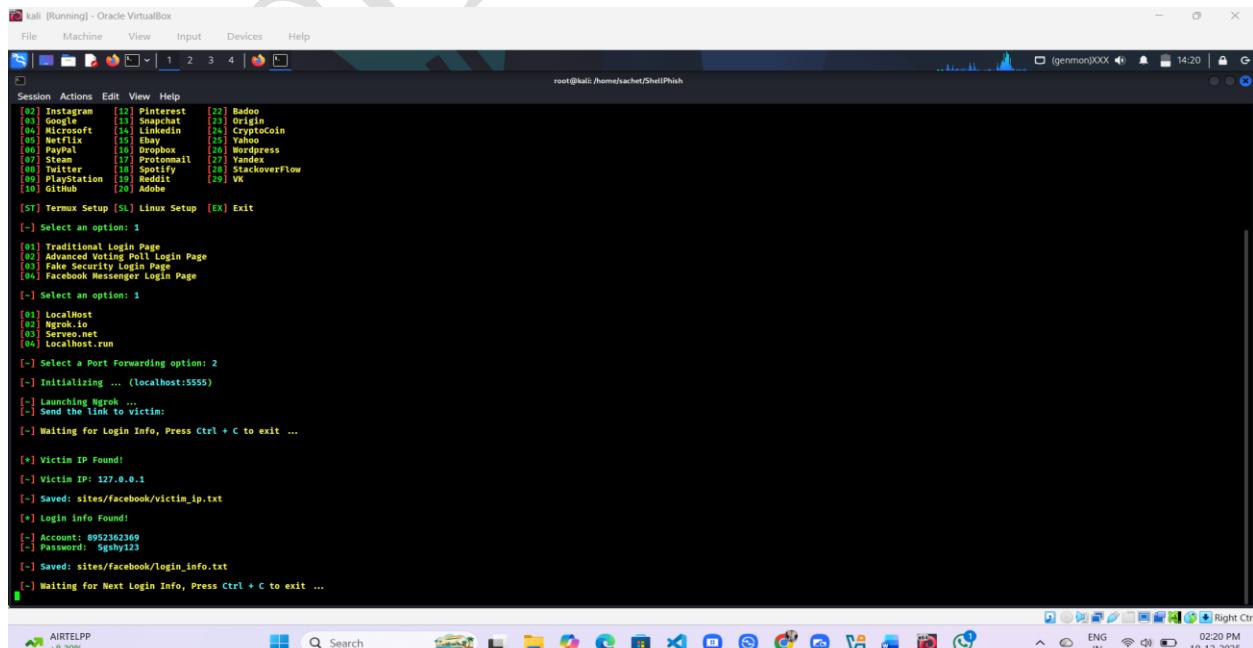
MODULE – 9 SOCIAL ENGINEERING

- Now copy link and send it to the target



```
v2.5-MOD
... Phishing Tool Modded by @AbirHasan2005 ...
[+] Disclaimer: Developers assume no liability and are not ...
[+] responsible for any misuse or damage caused by this tool ...
... Choose any social site which you want to hack ...
[01] Facebook [01] Twitch [22] DeviantArt
[02] Instagram [02] Pinterest [23] Badoo
[03] Google [03] Snapchat [24] Origin
[04] Microsoft [04] LinkedIn [25] CryptoCoin
[05] Netflix [05] Shein [26] Wordpress
[06] PayPal [06] Dropbox [27] Yandex
[07] Steam [07] Protonmail [28] StackOverflow
[08] Twitter [08] Spotify [29] VK
[09] PlayStation [09] Reddit [30] Adobe
[10] GitHub
[ST] Termux Setup [SL] Linux Setup [EX] Exit
[-] Select an option: 1
[01] Traditional Login Page
[02] Advanced Voting Poll Login Page
[03] Fake Security Login Page
[04] Facebook Messenger Login Page
[-] Select an option: 1
[01] LocalHost
[02] Ngrok.io
[03] Servo.net
[04] Localhost.run
[-] Select a Port Forwarding option: 2
[-] Initializing ... (localhost:5555)
```

- Paste link in the url section
- Fake amazon login page open
- Now open kali linux teminal
- Username and password are captured



```
v2.5-MOD
... Phishing Tool Modded by @AbirHasan2005 ...
[+] Disclaimer: Developers assume no liability and are not ...
[+] responsible for any misuse or damage caused by this tool ...
... Choose any social site which you want to hack ...
[02] Instagram [02] Pinterest [22] Badoo
[03] Google [03] Snapchat [23] Origin
[04] Microsoft [04] LinkedIn [24] CryptoCoin
[05] Netflix [05] Shein [25] Wordpress
[06] PayPal [06] Dropbox [26] Yandex
[07] Steam [07] Protonmail [27] StackOverflow
[08] Twitter [08] Spotify [28] VK
[09] PlayStation [09] Reddit [29] Adobe
[10] GitHub
[ST] Termux Setup [SL] Linux Setup [EX] Exit
[-] Select an option: 1
[01] Traditional Login Page
[02] Advanced Voting Poll Login Page
[03] Fake Security Login Page
[04] Facebook Messenger Login Page
[-] Select an option: 1
[01] LocalHost
[02] Ngrok.io
[03] Servo.net
[04] Localhost.run
[-] Select a Port Forwarding option: 2
[-] Initializing ... (localhost:5555)
[-] Launching Ngrok ...
[-] Send the link to victim:
[-] Waiting for Login Info, Press Ctrl + C to exit ...
[+] Victim IP Found!
[-] Victim IP: 127.0.0.1
[-] Saved: sites/facebook/victim_ip.txt
[+] Login info Found!
[-] Account: 8952362369
[-] Password: 0gmy113
[-] Saved: sites/facebook/login_info.txt
[-] Waiting for Next Login Info, Press Ctrl + C to exit ...
```

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

SACHCHITANAND