

Name - HARSHIL AMIT BUCH
Class - TY CSF-1
Roll Number - 14

Experiment No. 3

Title:

Conduct a phishing attack simulation to understand social engineering techniques.

Objective:

To understand how phishing attacks trick users by simulating fake login pages. This helps us study social engineering methods and learn how to detect such attacks.

Software/Tools Required:

- Kali Linux
 - Terminal
 - Zphisher

Theory:

Phishing is a type of cyber-attack where attackers create fake web pages to steal sensitive information like usernames and passwords. Zphisher automates phishing page creation for different platforms (Facebook, Gmail, etc.).

Installation Commands:

Tool: zphisher

1. Open Kali Linux Terminal Emulator

2. Commands:

```
sudo git clone https://github.com/htr-tech/zphisher.git
```

Enter password and hit enter

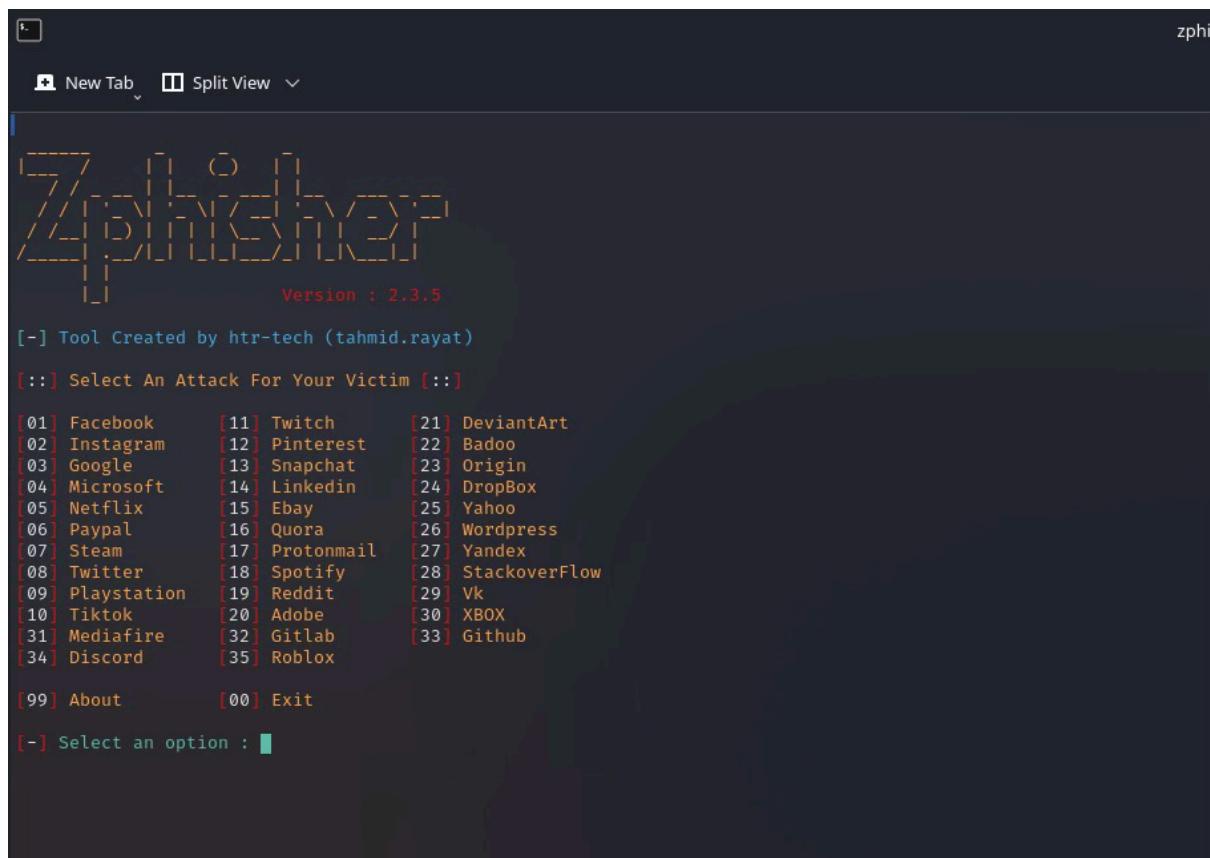
```
~:zsh — Konsole
New Tab Split View
Copy Paste Find...
→ ~ sudo git clone https://github.com/htr-tech/zphisher.git
Cloning into 'zphisher'...
remote: Enumerating objects: 1801, done.
remote: Total 1801 (delta 0), reused 0 (delta 0), pack-reused 1801 (from 1)
Receiving objects: 100% (1801/1801), 28.68 MiB | 7.68 MiB/s, done.
Resolving deltas: 100% (817/817), done.
→ ~
```

3. Once the installation is done,

`cd zphisher` → (Opens the tool's folder)

4. `bash zphisher.sh` → (Runs the tool to start phishing simulation)

5. Select Instagram option → (Choose Instagram phishing page)

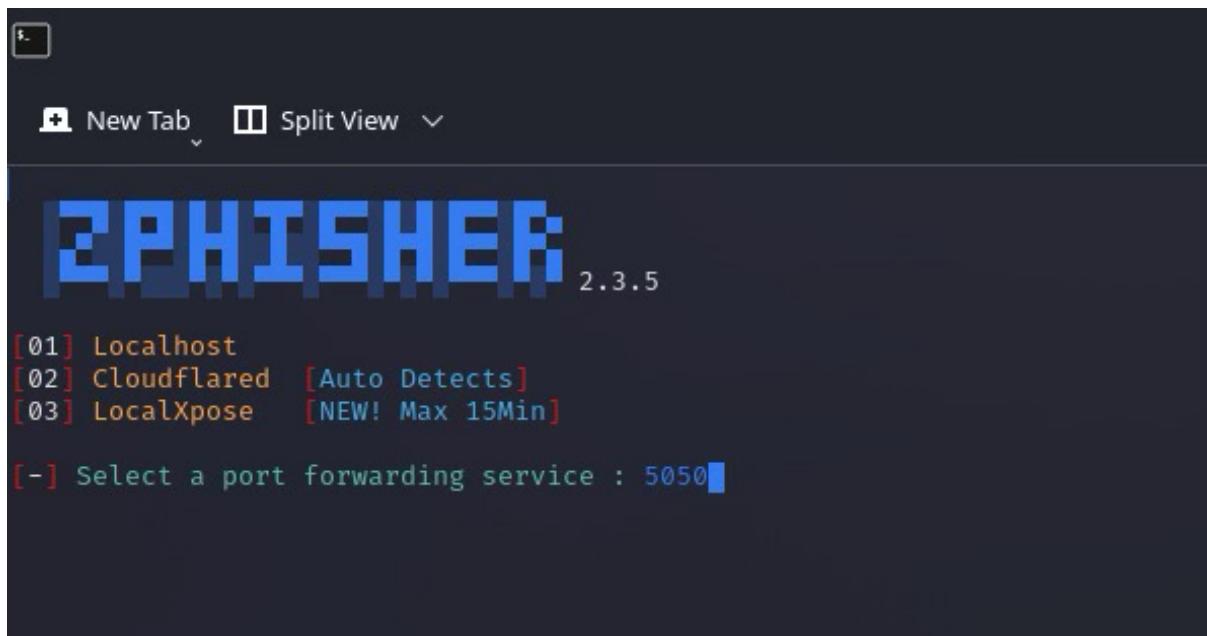


The screenshot shows a terminal window with a dark background. At the top, there are browser-like tabs labeled "New Tab" and "Split View". Below the tabs, there is a stylized logo composed of various symbols like brackets and arrows. To the right of the logo, the text "Version : 2.3.5" is displayed. The main menu is presented as a list of options:

- [--] 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

At the bottom of the menu, the text "[--] Select an option : █" is visible, indicating where user input is expected.

6. When asked for port, type: **5050** → (Host the phishing page on port **5050**) or any port you want



The screenshot shows a browser window with the ZEPHISHER interface at the top. The main content area displays the message: **[-] Successfully Hosted at : http://127.0.0.1:5050**. Below this, another message says: **[-] Waiting for Login Info Ctrl + C to exit**.

The browser's address bar shows the URL **127.0.0.1:5050/login.html**. The page content includes a heading **Free Instagram Followers Trial** and a subtext: "Get followers for an unlimited number of accounts that are free and authentic! There are several benefits for your Instagram account when you get followers from us. Increased brand recognition and visibility bring in more revenue." A yellow callout box contains the text: "News 1 January 2021: Get upto 1000 Followers fast and instantly. Feel free to try the free trial below."

The form section has fields for **Instagram Username** and **Instagram Password**, a **Submit** button, and a **Get Followers** link.

How to use our free insta followers trial?

iDigic offers you the chance to test our Instagram services – we are offering a FREE TRIAL for any number of accounts. Our followers trial package is 100% free the first time for every new account. We guarantee the safety of your account as we don't require your password.

Note: To conduct any phishing attack from zphisher tool two devices or tabs should be in same network.

Outcome:

After running Zphisher, we successfully simulated phishing pages and understood how attackers trick users into entering credentials. We also learned how easy it is to launch such attacks, highlighting the importance of awareness and preventive security measures.

Conclusion:

The experiment demonstrates how phishing works using Zphisher. It builds awareness about social engineering threats and emphasizes the need for user education, strong authentication, and vigilance against suspicious links.