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.

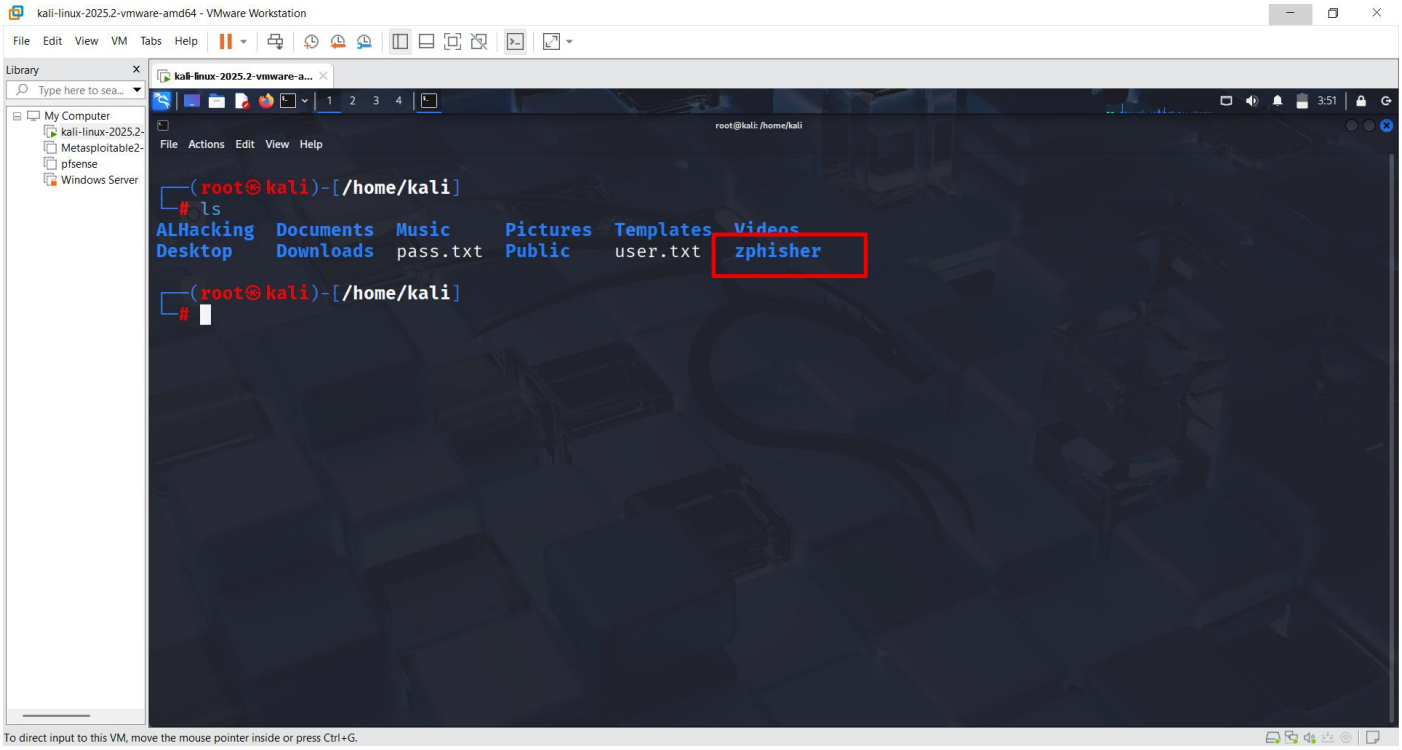
Zphisher Download Link: https://github.com/htr-tech/zphisher.git

Installation Steps:

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

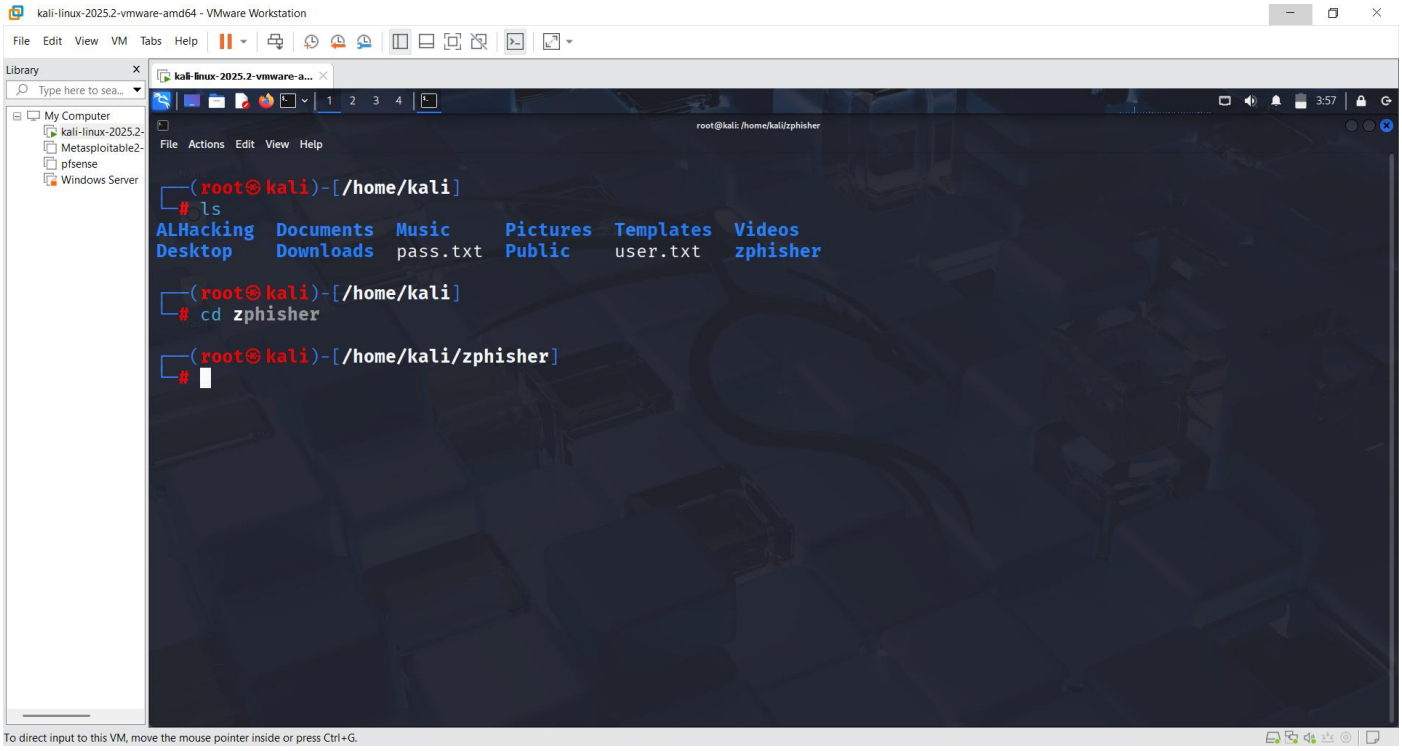
git clone https://github.com/htr-tech/zphisher.git

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



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

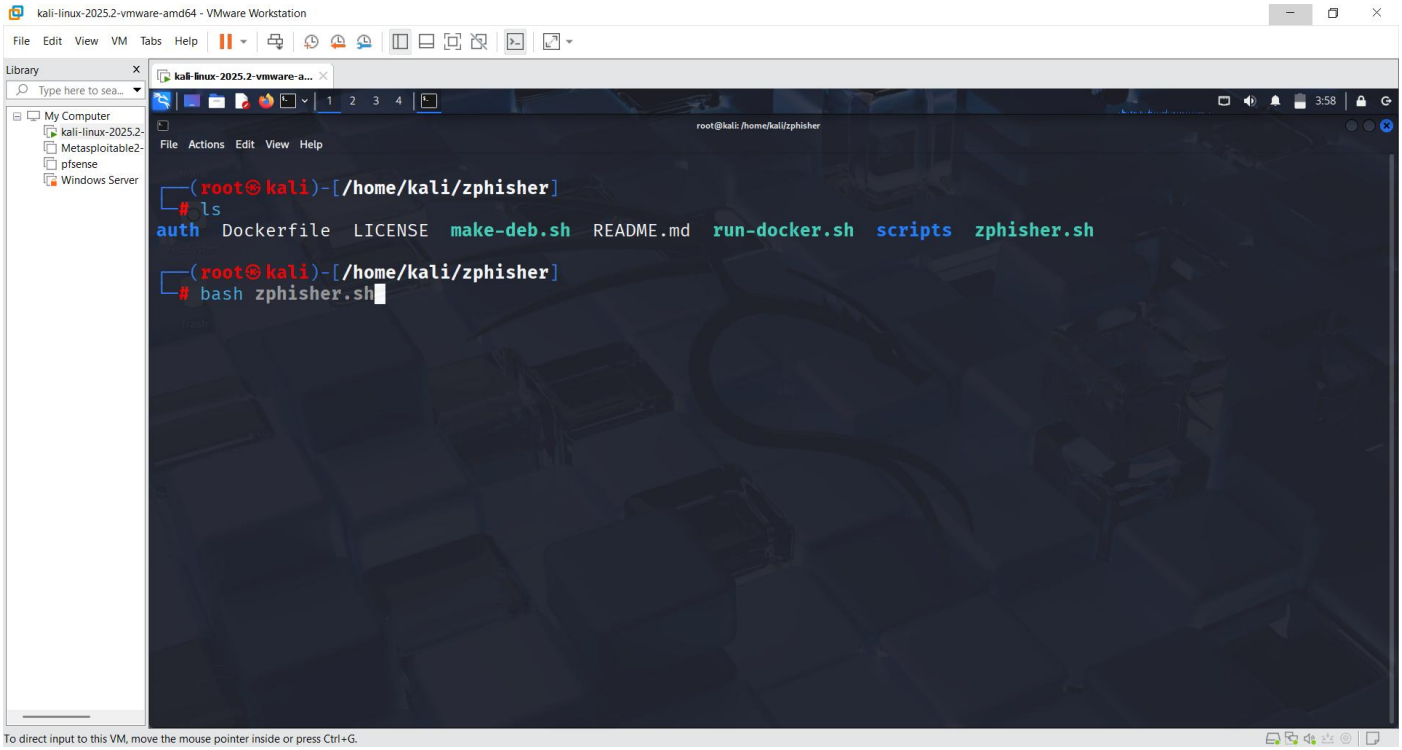
cd zphisher



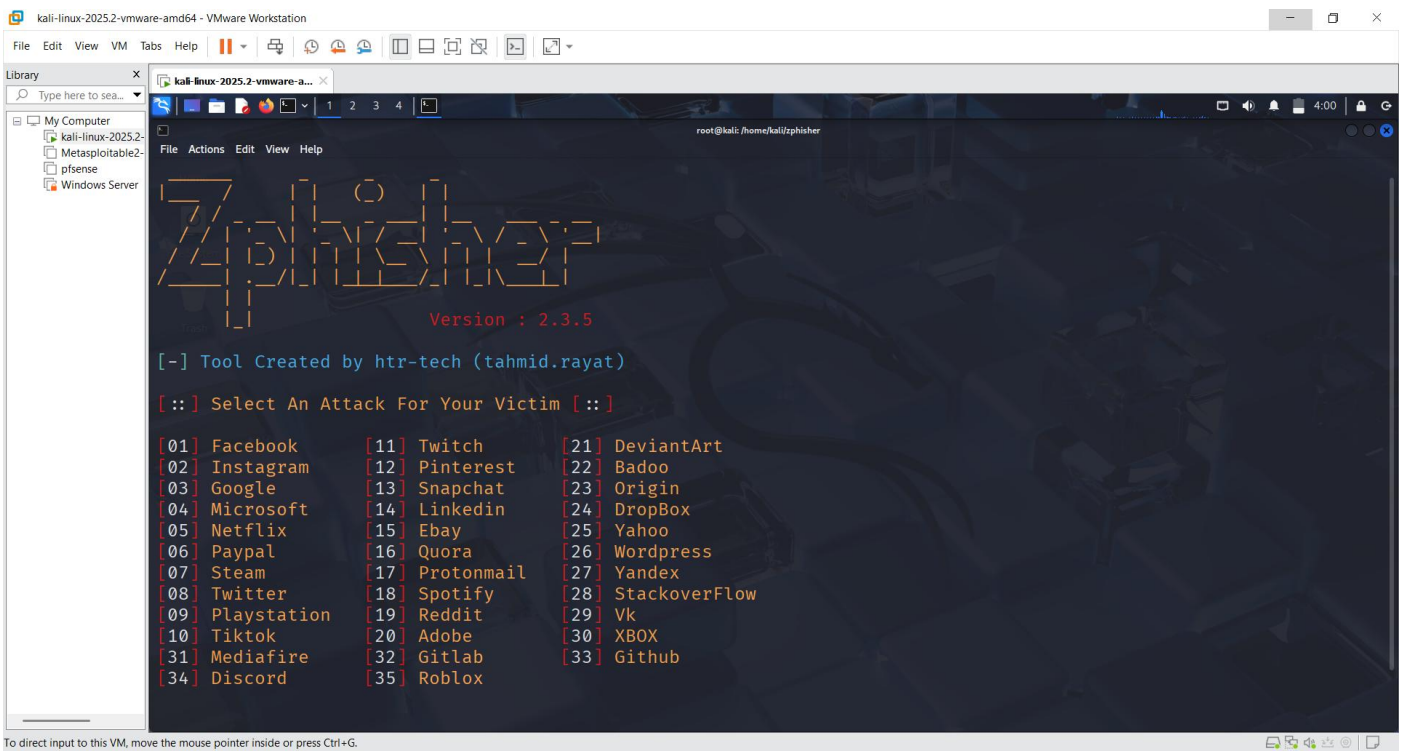
Reported By: - Lakshman Kumar Das

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

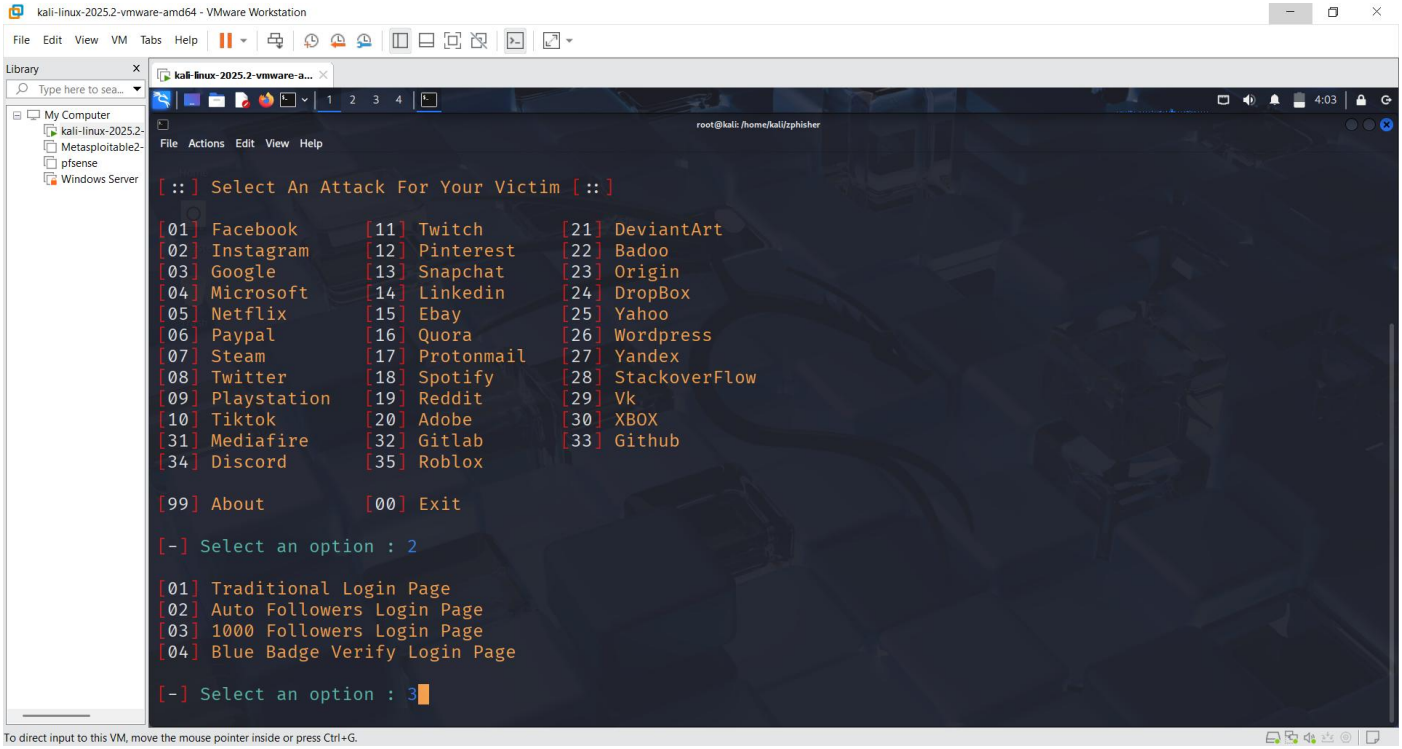
bash zphisher.sh



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



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.

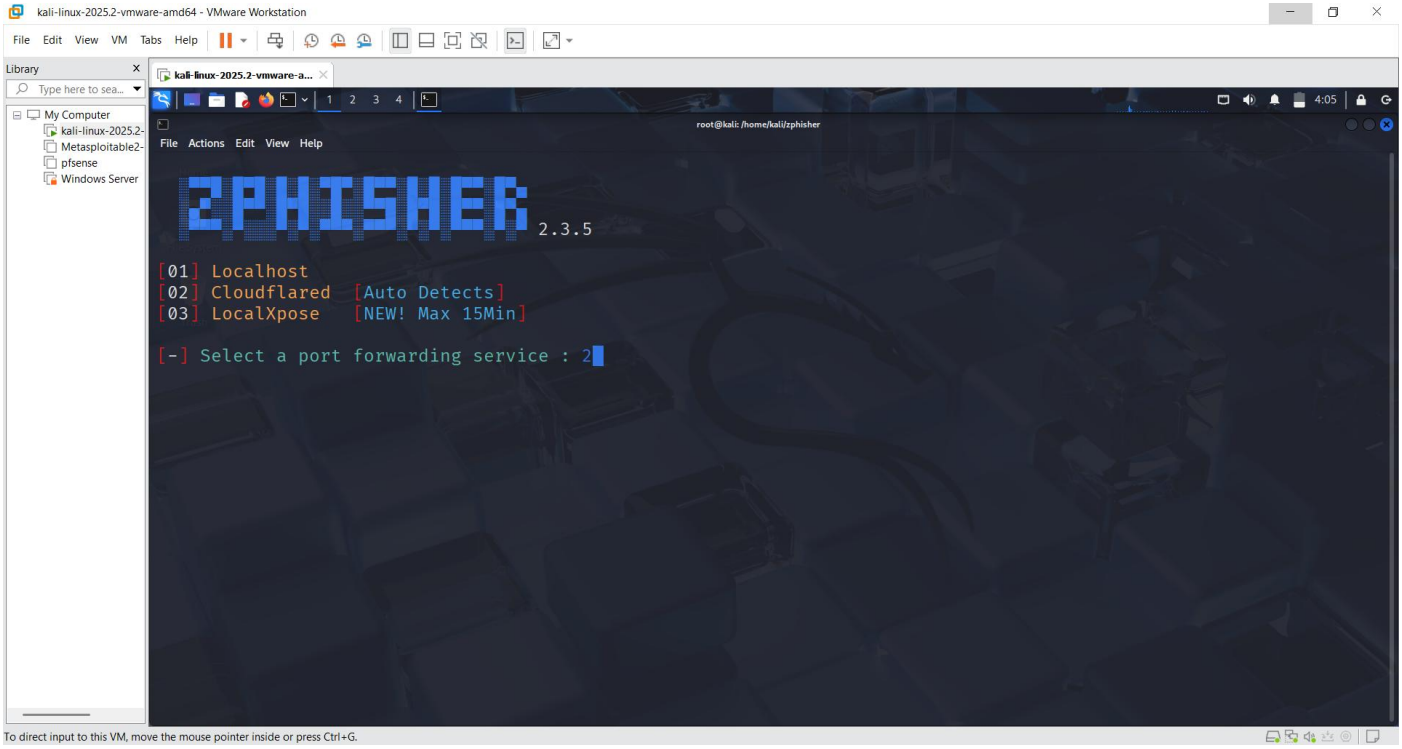


You will see an interface with different options. Choose one — for example, I selected option 2.

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

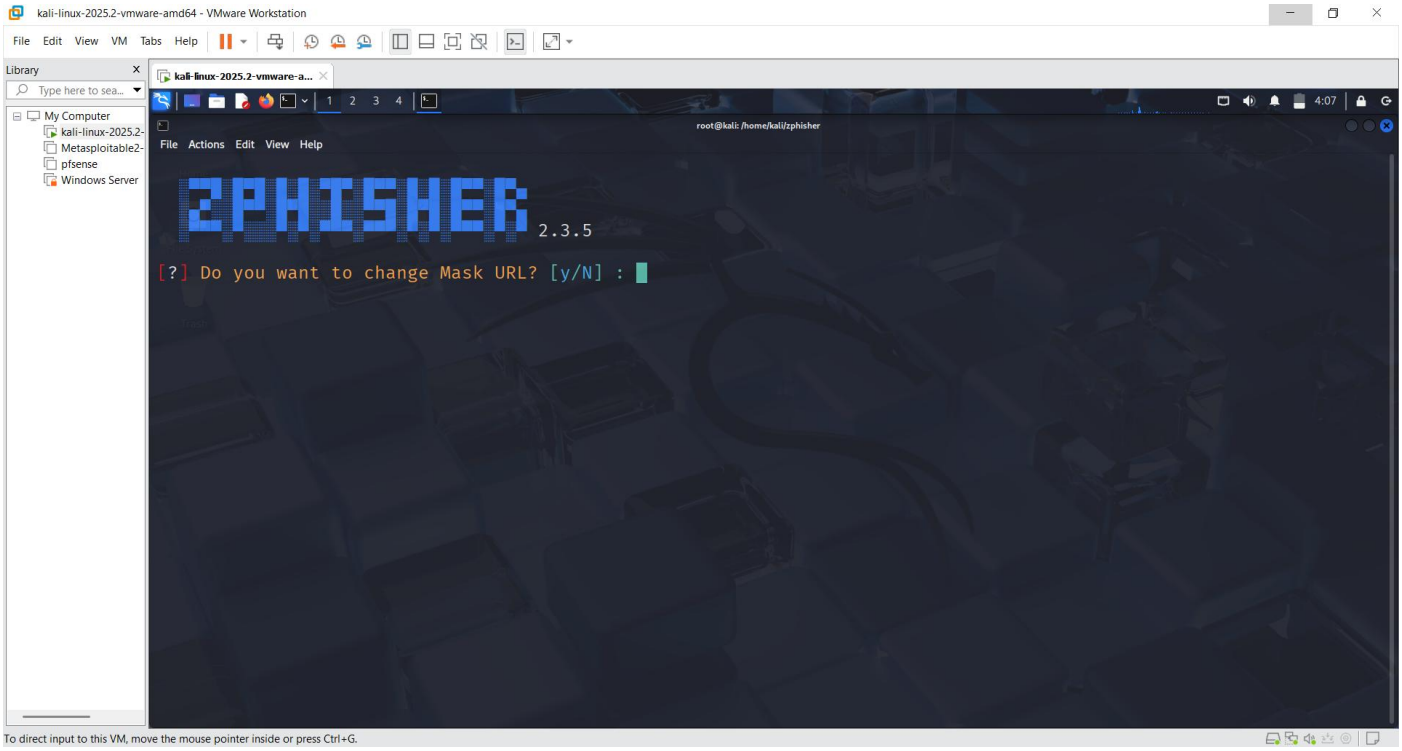
Cloudflared: Creates a public link that anyone can open — no router setup needed.

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

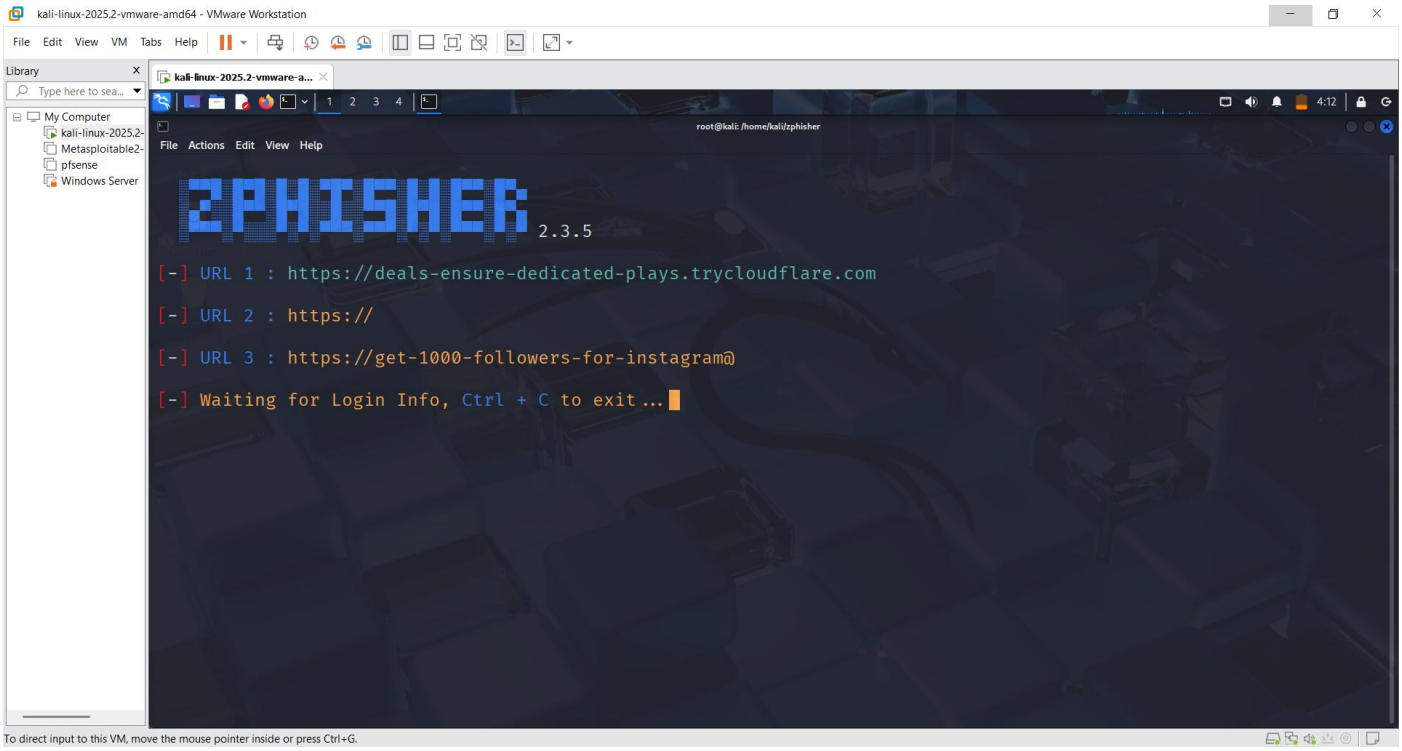


Reported By: - Lakshman Kumar Das

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



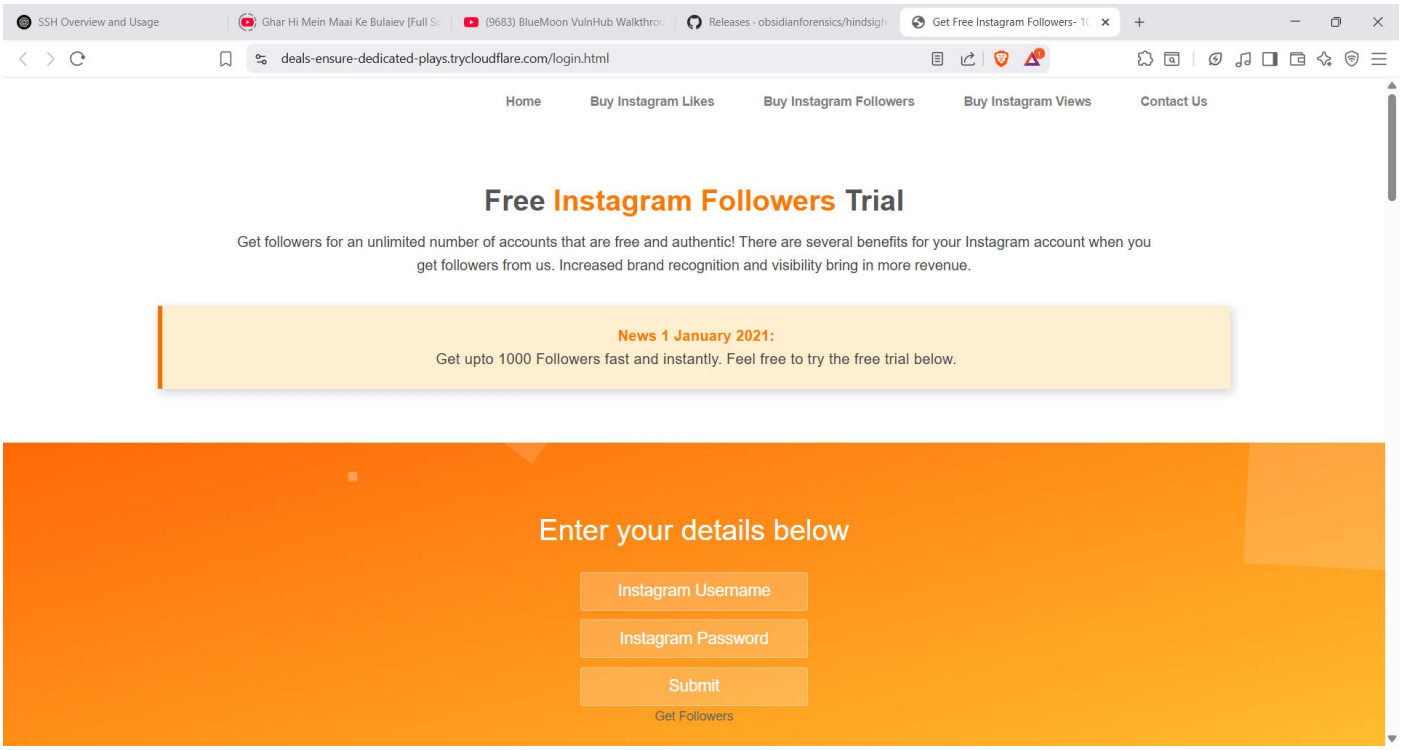
Here, you can see that the phishing links have been generated.



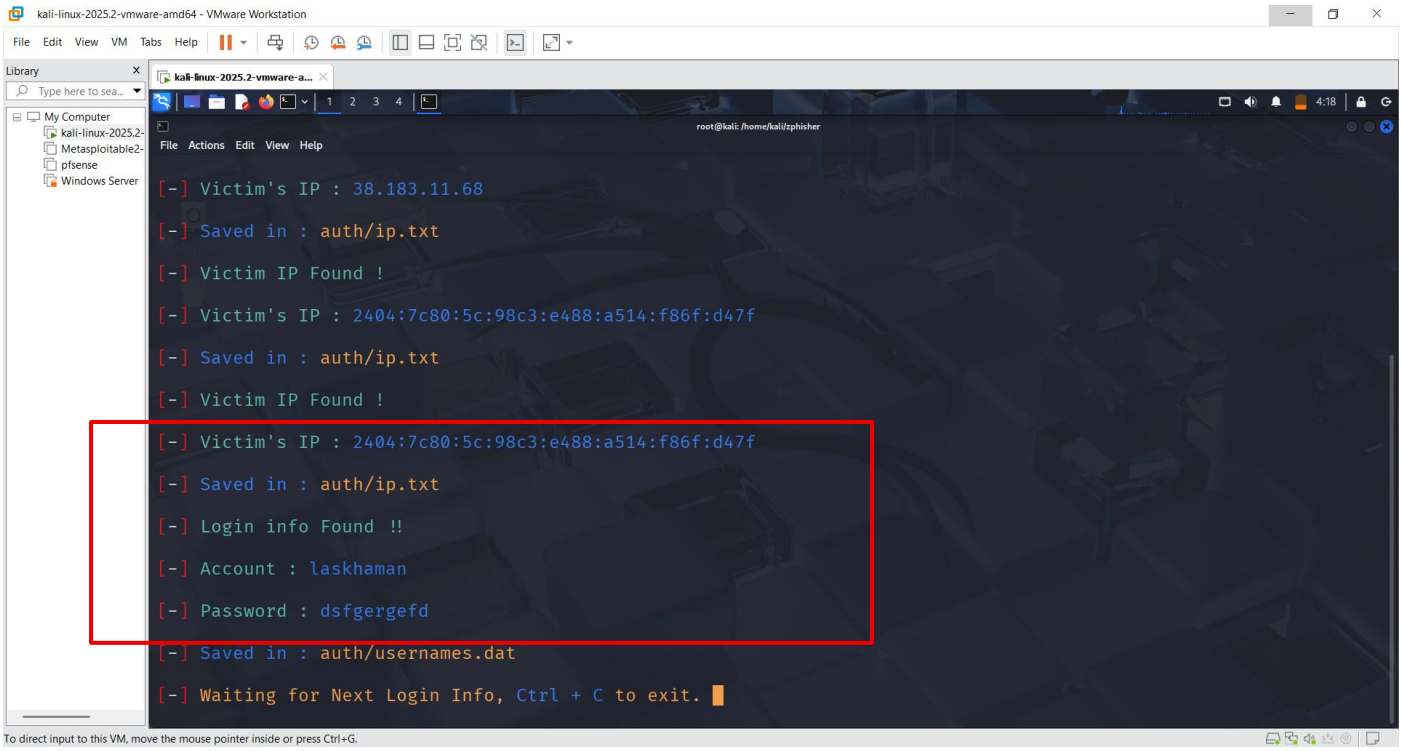
Copy the generated phishing link and send it through WhatsApp, social media, or other platforms.

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.

Reported By: - Lakshman Kumar Das

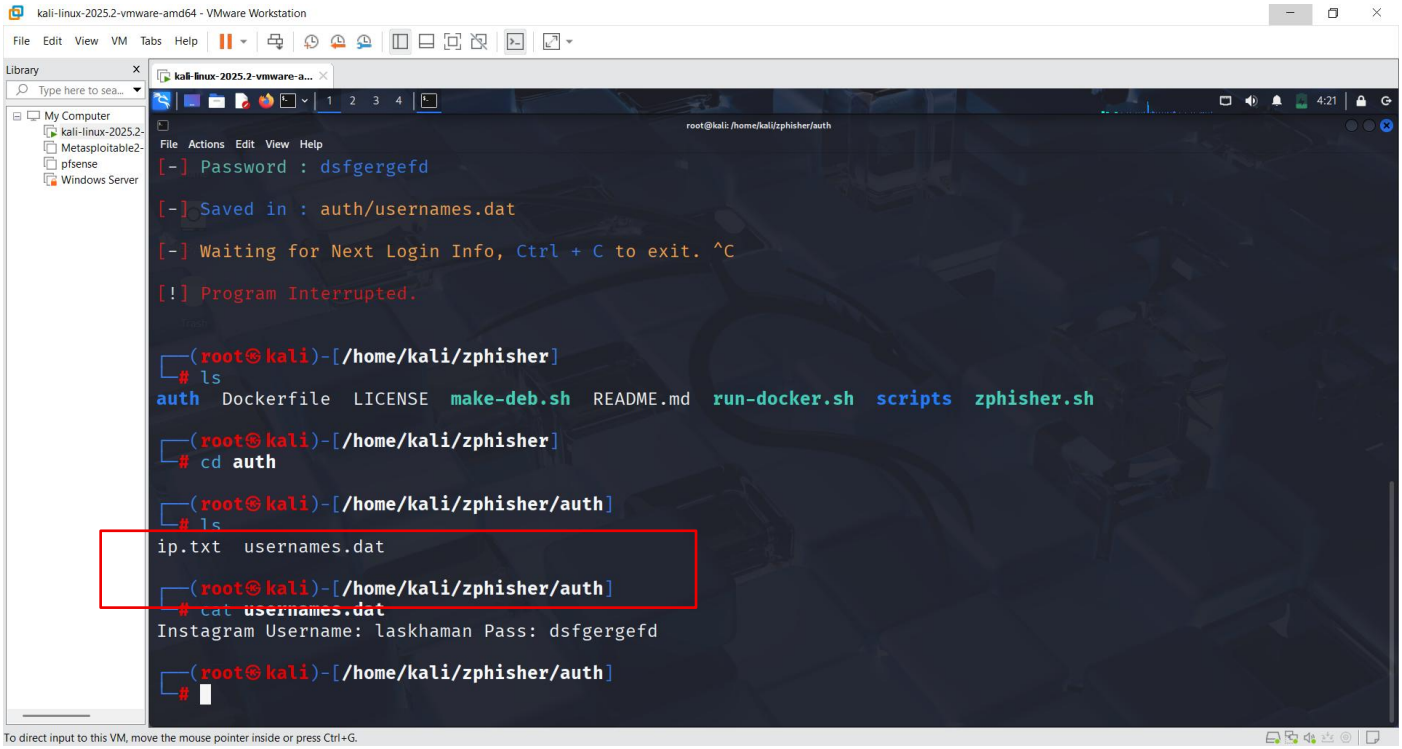


You can clearly see the victim's IP address along with their Instagram username and password displayed in your terminal.



Reported By: - Lakshman Kumar Das

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



Reported By: - Lakshman Kumar Das