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!

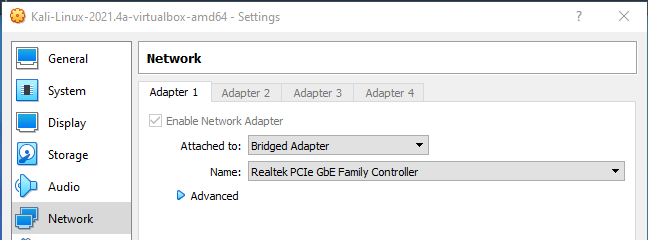
**Overview**

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.

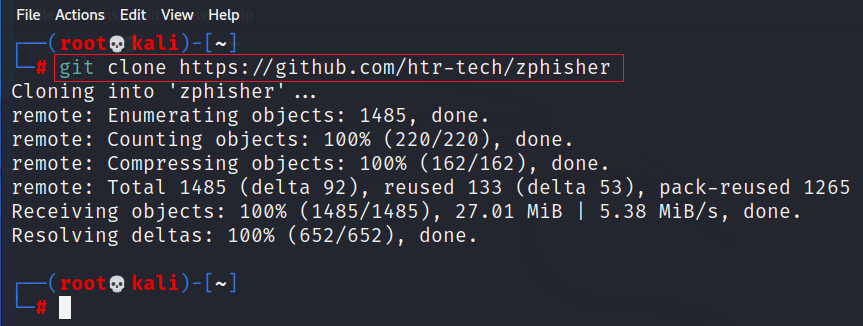


**Installing ZPhisher**

From your kali desktop, launch a new terminal.

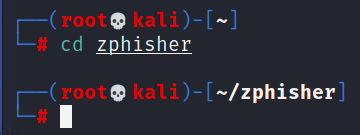
ZPhisher needs to be downloaded from its GitHub repository using the following command:

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



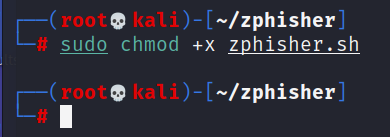
Once the install is complete, change the directory location to go inside the zphisher directory using the cd command:

cd zphisher



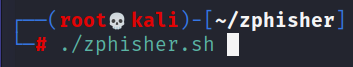
We need to give executable permission to the zphisher bash script by using the following command:

sudo chmod +x zphisher.sh

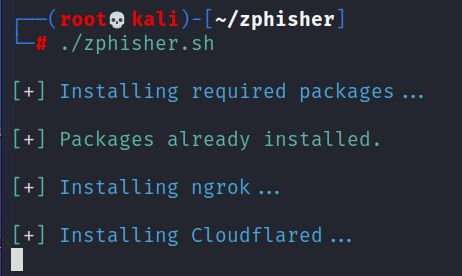


We are now ready to install zphisher. To launch the script, use the following command:

./zphisher.sh



ZPhisher completes its installation.



ZPhisher start page.

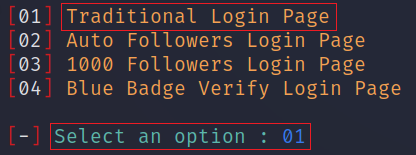


**Create an Instagram Phishing Page**

Choose Option 02. Press enter.



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

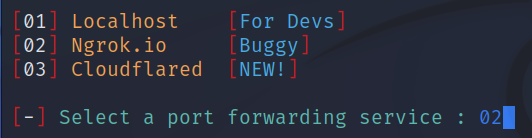


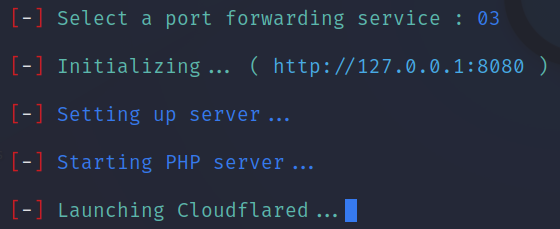
We next must choose our port forwarding option.

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

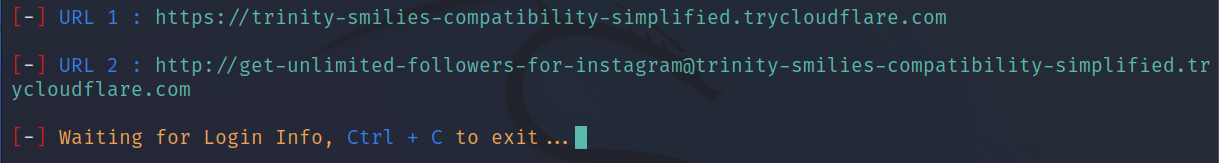
To deliver the "Traditional Login Page " via the Internet, we can choose a free port forwarding service such as ngrok or cloudflared. (These are all free port forwarding services. Note that some services may be down due to overloading. When that happens, choose an alternative.)

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



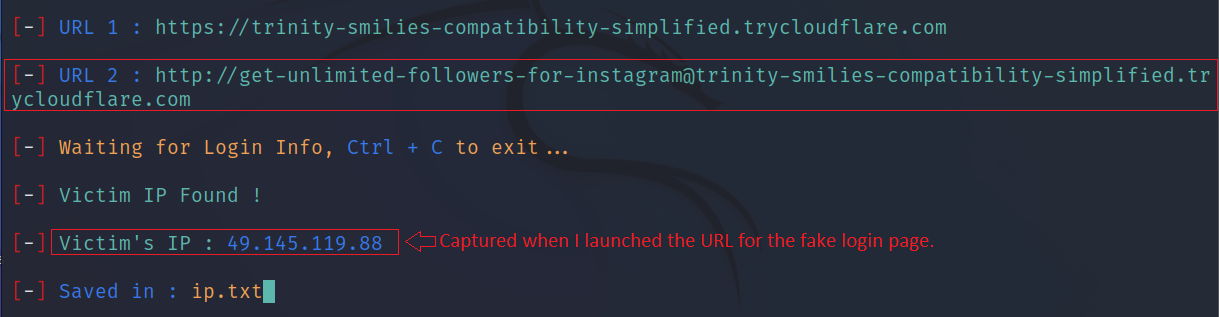


Here are our URLs.

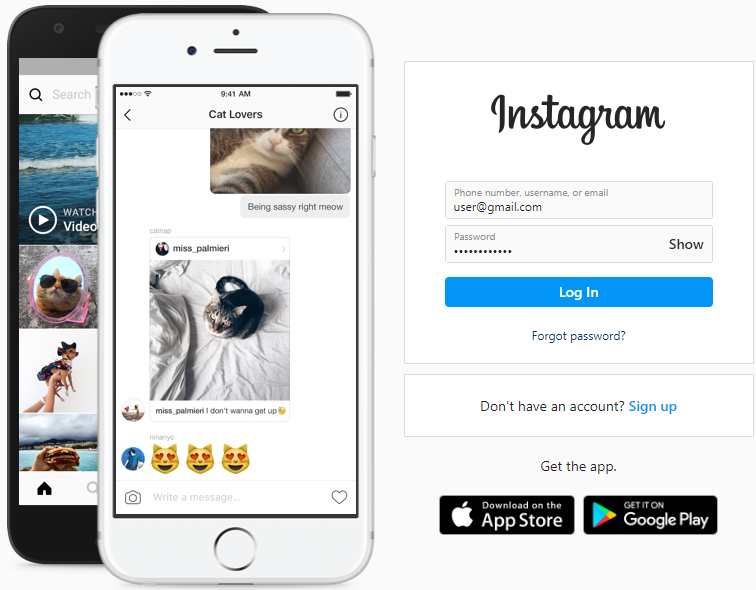


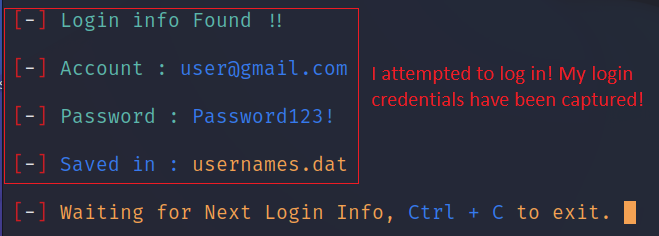
From your localhost machine or any machine with Internet access, open a browser and copy and paste your URL 2 into the address bar.

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.

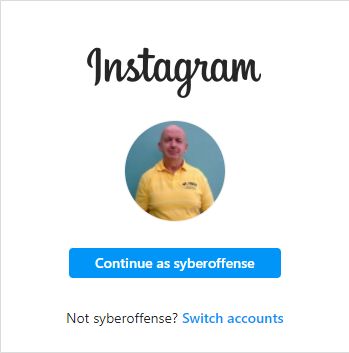


When the victim attempts to log in to their Instagram account, their credentials are captured and sent back to the attack machine.

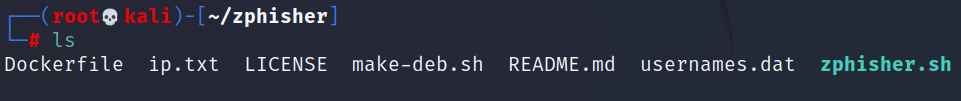




My attempt failed, but I was redirected to an actual Instagram page where my machine was recognized. Very convincing!

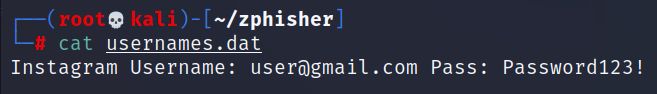


Back at your Kali terminal, Ctrl + C to exit. At the terminal. Type ls to see that files are present in the zphisher home folder.



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

cat usernames.dat.



**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!