**ZPhisher - A phishing tool**

**What is social engineering?**

Social engineering is a manipulative strategy employed by cybercriminals to deceive individuals into divulging confidential information or granting unauthorized access to systems, often by exploiting human psychology. This method relies on tricking people rather than hacking systems directly, using techniques such as phishing, pretexting, baiting, and quid pro quo. By gaining the trust of the target, social engineers can extract sensitive data or access restricted areas without raising suspicion.

To illustrate how such attacks are executed, we will be using the Zphisher tool in this article.

**What is Zphisher?**

Zphisher is an advanced phishing tool that is widely used for educational and ethical hacking purposes to demonstrate how phishing attacks can be conducted and to test the resilience of systems against such attacks. Developed as an open-source tool, Zphisher facilitates the creation of phishing websites by replicating legitimate web pages to deceive users into providing sensitive information, such as login credentials, personal identification numbers (PINs), or financial information.

Key features of Zphisher include:

* **User-Friendly Interface**: Zphisher provides a direct command-line interface that assists users in setting up the process, simplifying the deployment of phishing attacks.
* **Multiple Phishing Templates**: The tool comes with a variety of templates for different websites and services, allowing users to choose the most appropriate one for their target.
* **Port Forwarding**: Zphisher supports port forwarding via tools like Ngrok and Serveo, which makes it possible to host phishing pages on the internet without requiring advanced network configuration.
* **Custom URL Generation**: Users can generate custom URLs to make the phishing pages appear more legitimate and increase the chances of success.
* **Real-Time Data Capture**: The tool captures the entered credentials in real-time and displays them to the attacker, allowing for immediate access to the stolen information.

**Practical steps to perform phishing attack using zphisher**

1. Install the zphisher by writing this command in the kali terminal

**git clone --depth=1** [**https://github.com/htr-tech/zphisher.git**](https://github.com/htr-tech/zphisher.git)

****

1. Open the zphisher folder and execute the zphisher.sh file in the kali terminal.

**bash zphisher.sh**

****

1. After opening this tool, we will select the website that we want to impersonate. So in this we will select the 14th option as we want to create a fake **LinkedIn** website.



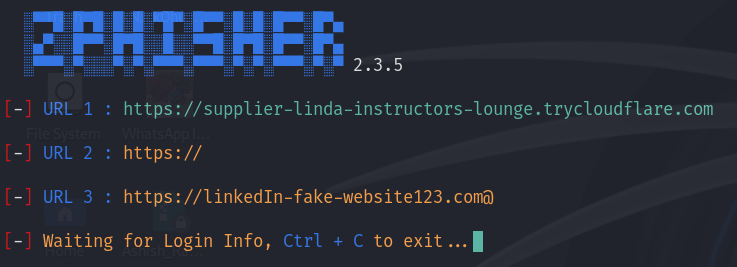
1. We will select the 2nd option as our choice for port forwarding service.



1. After this we can change the url and mask it with our own custom URL.

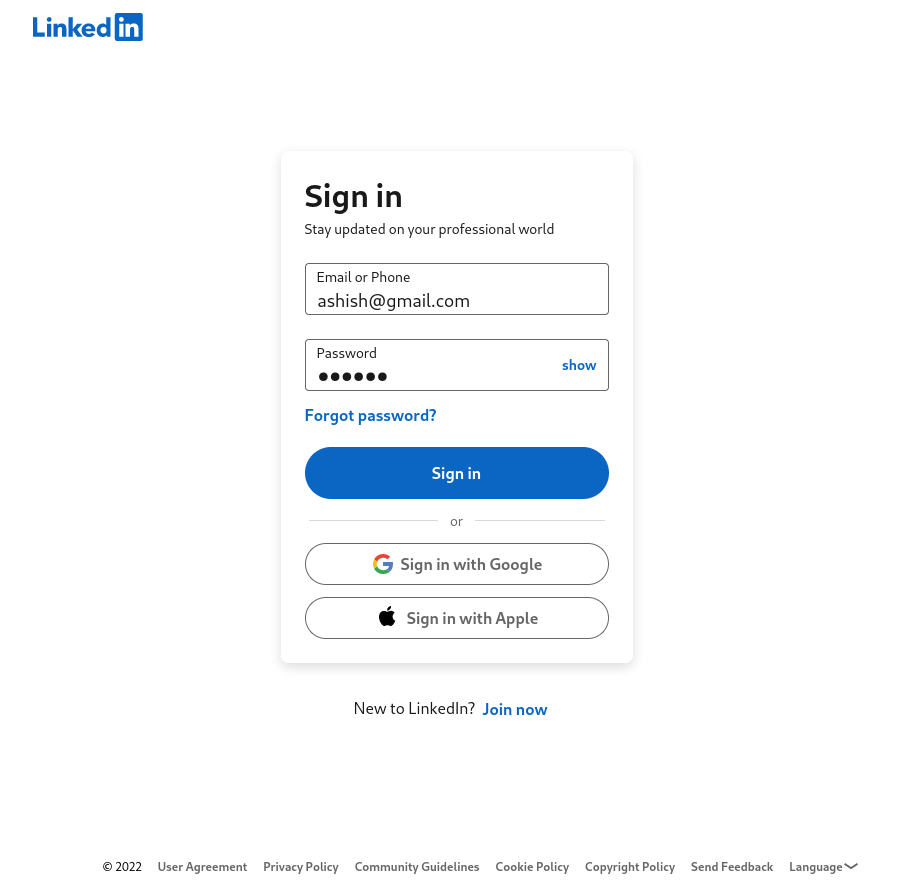


1. Open up any of the **URL links** shown in the zphisher.

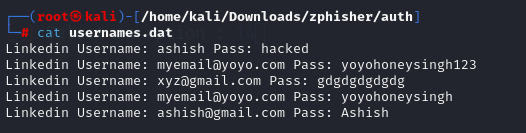


1. We have successfully created the LinkedIn fake website. If a victim clicks on the link and opens it in the browser. He/She will see the exact copy of the LinkedIn login page.

Now, if the victim writes his/her **email**(ashish@gmail.com) and **password**(ashish) thinking he/she is logging into the real website.



1. **Congratulations** we have successfully collected the credentials of the victim. In the zphisher directory, open the **auth** folder. Open **username.dat**. You will find all the email and passwords of those victims which tried to login their linkedIn account using our website.



Zphisher is a powerful phishing tool that aids in demonstrating and understanding the mechanics of phishing attacks by replicating legitimate websites to deceive users into providing sensitive information. While it is a valuable resource for educational and ethical hacking purposes, it must be used responsibly and legally to avoid severe consequences. Understanding and mitigating the risks posed by tools like Zphisher is crucial in strengthening cybersecurity defenses.