Name - HARSHIL AMIT BUCH
Class - TY CSF-1
Roll Number - 14

Experiment No. 3

Title:

Conduct a phishing attack simulation to understand social engineering techniques.

Objective:

To understand how phishing attacks trick users by simulating fake login pages. This helps us study social engineering methods and learn how to detect such attacks.

Software/Tools Required:

- Kali Linux
- Terminal
- Zphisher

Theory:

Phishing is a type of cyber-attack where attackers create fake web pages to steal sensitive information like usernames and passwords. Zphisher automates phishing page creation for different platforms (Facebook, Gmail, etc.).

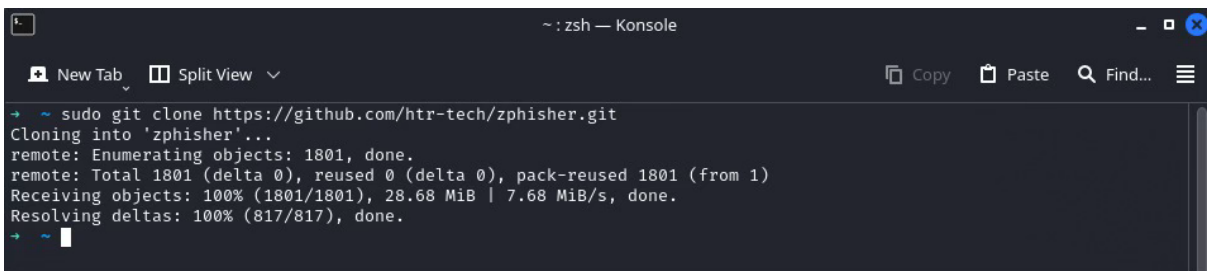
Installation Commands:

Tool: zphisher

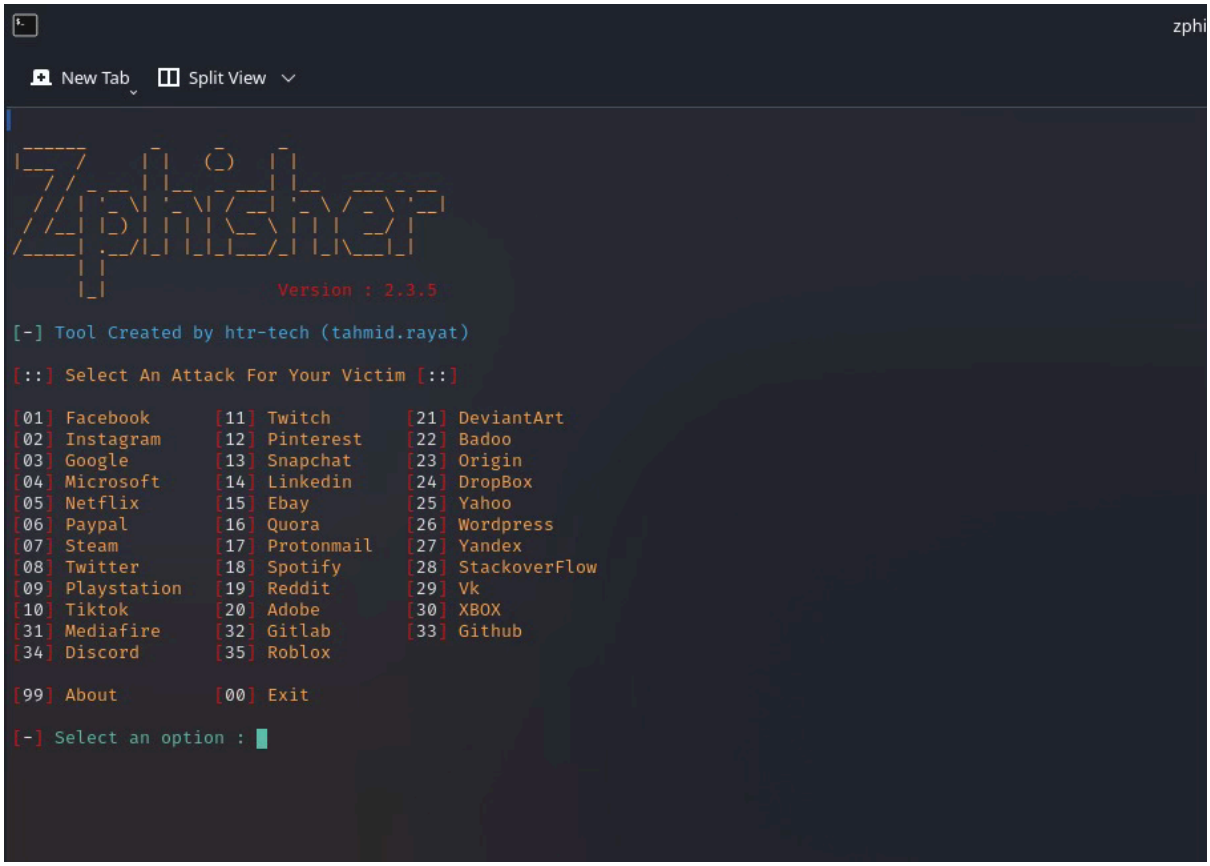
1. **Open Kali Linux Terminal Emulator**
2. **Commands:**

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

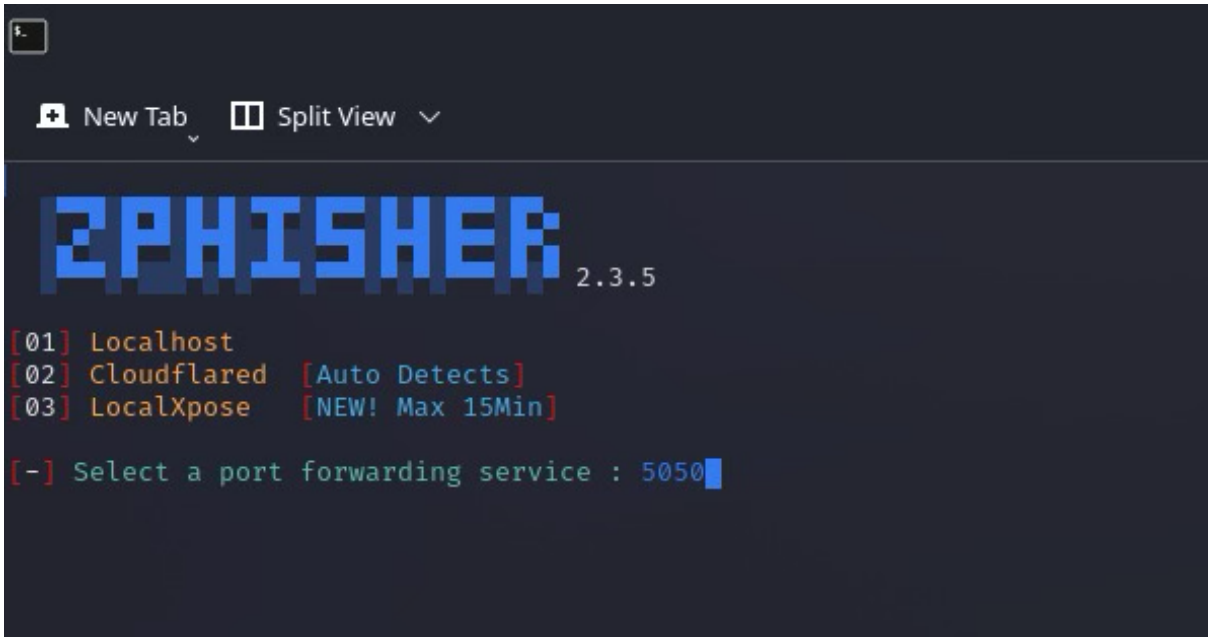
   Enter password and hit enter

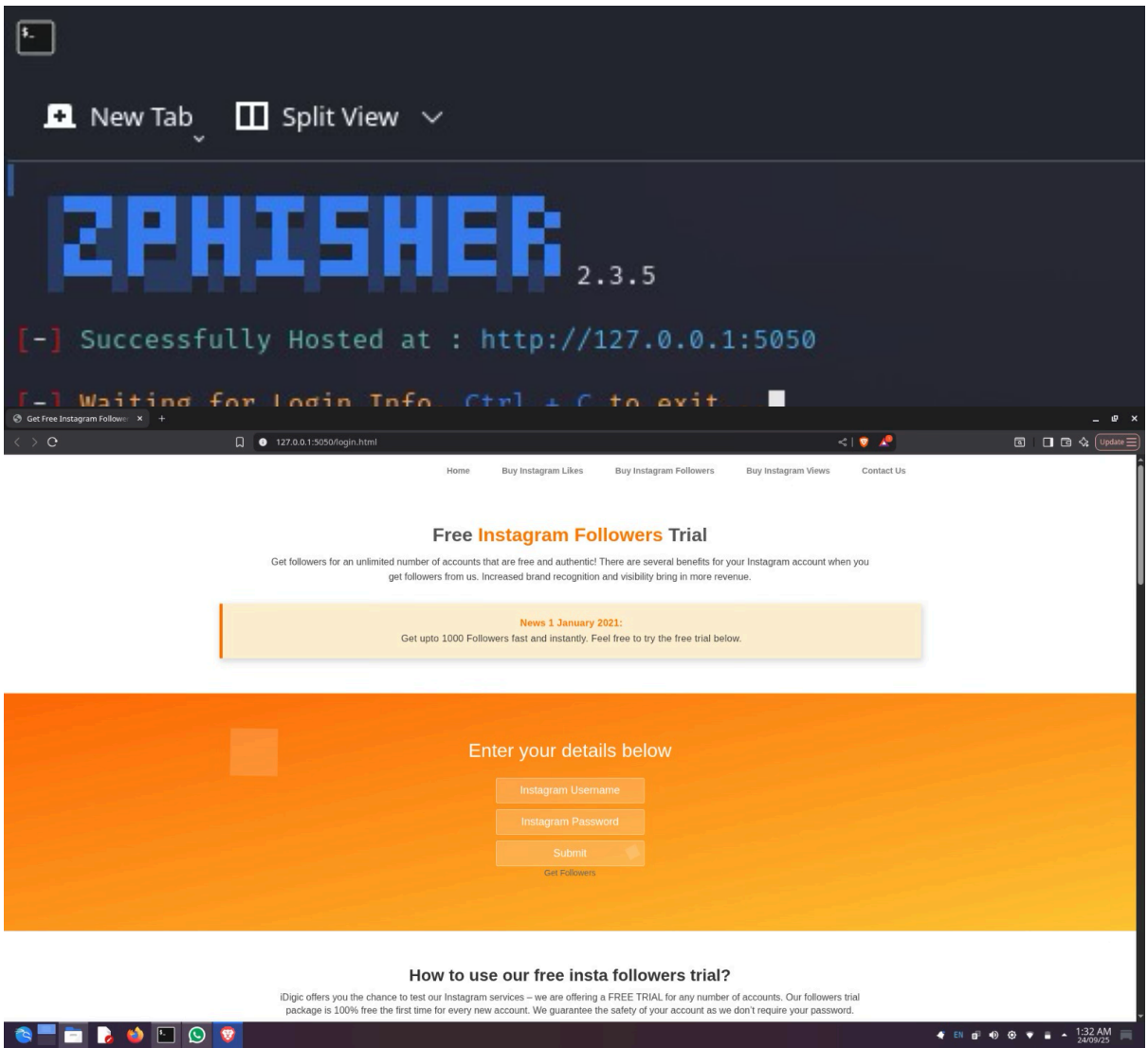


3. **Once the installation is done,**
   cd zphisher → (Opens the tool's folder)
4. bash zphisher.sh → **(Runs the tool to start phishing simulation)**
5. Select Instagram option → **(Choose Instagram phishing page)**



6. **When asked for port, type: 5050 → (Host the phishing page on port 5050) or any port you want**





Note: To conduct any phishing attack from zphisher tool two devices or tabs should be in same network.

Outcome:

After running Zphisher, we successfully simulated phishing pages and understood how attackers trick users into entering credentials. We also learned how easy it is to launch such attacks, highlighting the importance of awareness and preventive security measures.

Conclusion:

The experiment demonstrates how phishing works using Zphisher. It builds awareness about social engineering threats and emphasizes the need for user education, strong authentication, and vigilance against suspicious links.