A Project Report on

***Physhing using Zphisher***

### Network Protocols and Security(23EC2210A)

Submitted by

#### of Section 7

Under the guidance of

**Shaik Asif**

**Group Members:**

M V Karthikeya – 2320030081

G Sai Chetan Kumar - 2320030045

P Samith - 2320090067

**Introduction:**

Phishing attacks have become a significant threat in the cybersecurity landscape, leveraging deception to trick individuals into divulging sensitive information. These attacks exploit human psychology and weaknesses in digital security systems. To better understand and combat these threats, our project focuses on simulating phishing attacks using Kali Linux and Zphisher.

Kali Linux, known for its extensive suite of security tools, provides a robust environment for testing and analysis. Zphisher is a specialized phishing tool that automates the creation of phishing pages, making it an ideal choice for this simulation. Our goal was to explore the practical application of Zphisher in generating phishing attacks and to assess its effectiveness in capturing user credentials.

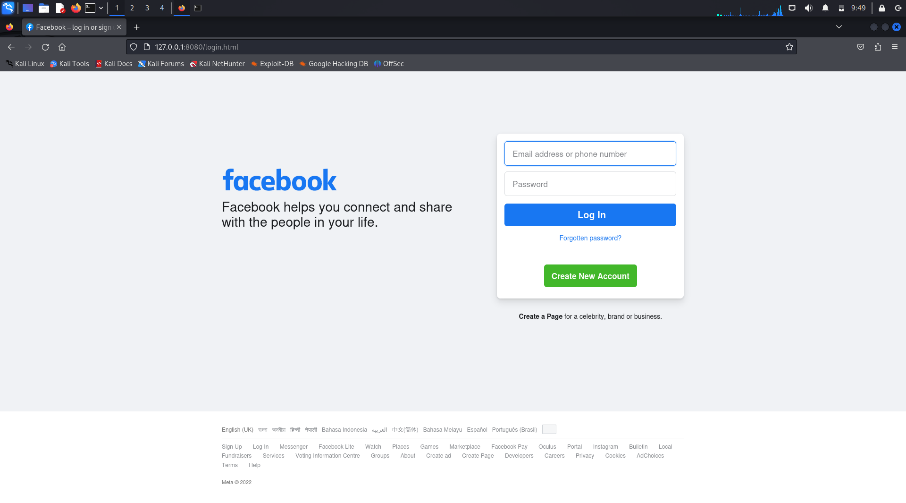
**Description:**

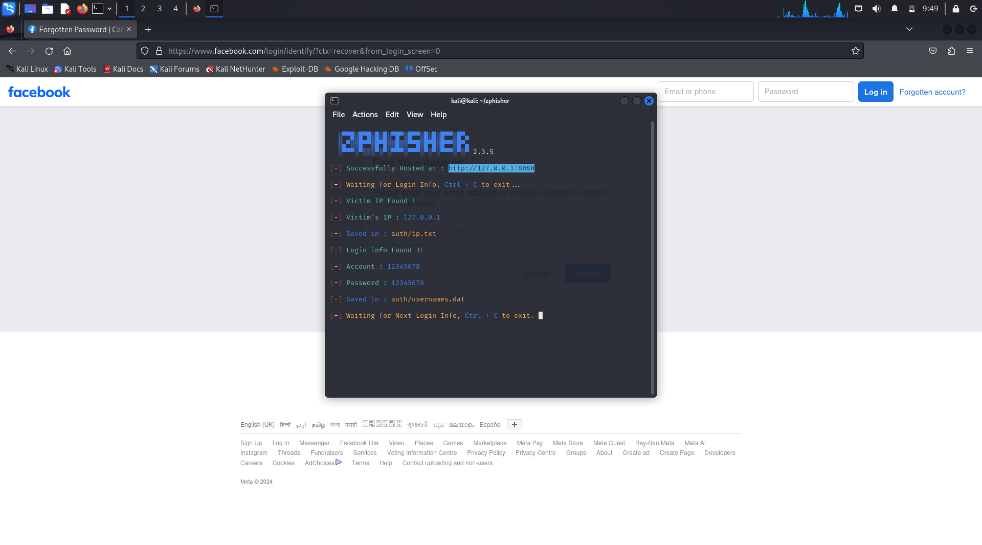
The project was conducted in a controlled lab environment to ensure ethical considerations and data protection. We started by setting up Kali Linux, configuring it for penetration testing, and installing Zphisher. The tool was used to generate phishing pages that mimic popular online services, including social media platforms and email providers. We selected various templates and customized them to enhance realism. The simulation involved deploying these phishing pages and tracking user interactions to evaluate the success rate of each phishing attempt.

Metrics such as the number of captured credentials and user engagement rates were collected to assess the effectiveness of the phishing pages. We also monitored network traffic to analyze how users interacted with the phishing sites. The project included an in-depth analysis of the phishing pages' design and the techniques used to make them convincing.

**OUTPUT:**







**Conclusion:**

The project successfully demonstrated the efficacy of Zphisher in creating realistic phishing scenarios. The tool allowed us to effectively simulate phishing attacks, highlighting the vulnerabilities that users might face when interacting with deceptive websites.

Through this simulation, we observed significant engagement with the phishing pages, underscoring the need for robust security training and awareness. The outcomes emphasized the importance of implementing advanced security measures and educating users about recognizing and avoiding phishing threats.