Ethical Email Phishing Simulation Using Gophish

Introduction

The Email Phishing Simulation Project was conducted as a cybersecurity training exercise using Gophish. It aimed to test employee awareness by ethically simulating phishing attacks in a safe environment.

Abstract

This project focused on designing and launching a controlled phishing campaign to educate users about the dangers of phishing emails. It allowed real-time tracking of user interactions such as email opens, link clicks, and credential submissions.

Tools Used

- Gophish (Open-source phishing framework)
- Gmail SMTP Server (smtp.gmail.com:587)
- Ngrok (to expose local landing page)
- HTML Templates (index.html, login.html)
- CSV (for importing user targets)

Steps Involved in Building the Project

1. Installed and launched Gophish locally.
2. Created sending profiles using Gmail SMTP with app password.
3. Designed phishing email using index.html.
4. Cloned login page using login.html and enabled data capture.
5. Imported target users via CSV.
6. Created and launched the campaign with Ngrok public URL.
7. Monitored real-time results (email open, link click, data entry).

Conclusion

The simulation provided insights into user behavior when exposed to phishing emails. It helped identify weak points and served as a strong awareness tool. Gophish proved effective in conducting ethical phishing simulations for educational purposes.