DAY 11 TASK 11 – Phishing Attack simulation and detection

Tools Used :

- GoPhish –open source phishing framework to create and manage phishing campaigns.
- MailHog – Local SMTP server used to capture phishing emails safely
- Linux (WSL)

Steps :

- Setup GoPhish
- Access admin via https://127.0.0.1.3333
- Setup Mailhog
- SMTP configuration and test email functionality to verify email delivery
- Create Email Template
- Crate a fake login page to capture credentials
- Create User Group
- Launch Campaign – fake landing page,created email template, mailhog smtp profile and test user group
- Attack Simulation
- Track and Monitor

Preventions:

- Secure awareness
- Verifying sender
- Avoid clicking unknown links
- Use MFA