Ethical Phishing Simulation Platform – Internship Report

**1. Introduction**

In today’s digital landscape, cybersecurity awareness is vital for every organization. This project centres on developing a controlled phishing simulation platform designed to safely replicate real-world phishing attacks. Its purpose is to test users, provide hands-on training, and raise awareness about recognizing and responding to social engineering threats.

**2. Abstract**

The Ethical Phishing Simulation Platform is a web-based tool designed to simulate phishing attacks for training and awareness. Built around a Flask web server, it hosts realistic fake login pages, uses Postfix to send simulated phishing emails, and tracks user interactions in a SQLite database. After each campaign, the platform offers educational feedback and analytics dashboards to boost user awareness and assess organizational risk.

**3. Tools Used**

* **Flask** – A lightweight Python web framework used to build and run the simulation server.
* **HTML/CSS** – For designing email templates and creating realistic web pages.
* **SQLite** – A simple, file-based database for logging user interactions securely.
* **Postfix** – An SMTP mail server that delivers the simulated phishing emails.
* **Social Engineering Toolkit (SET)** – A powerful tool for crafting and managing phishing simulations.
* **Kali Linux** – The host operating system, chosen for its robust security testing capabilities.

**4. Steps Involved in Building the Project**

1. **Environment Setup**
   * Created a virtual environment using venv
   * Installed Flask and created project structure (app.py, /templates, /static)
2. **Phishing Web Pages**
   * Designed fake login page (index.html)
   * Created form capture endpoint (submit.html)
   * Redirects to awareness page (educate.html)
   * Developed dashboard.html for viewing captured data
3. **Database**
   * Used SQLite (phishing.db) to log events: user\_id, action type, timestamp
4. **Mail Server Configuration**
   * Installed and configured Postfix on Kali Linux
   * SET used to craft and send HTML email with phishing link
5. **Phishing Simulation Execution**
   * Crafted realistic email content with SET
   * Sent emails using Postfix (127.0.0.1) to test addresses
   * Tracked form submissions and time of click
6. **Result Tracking**
   * Queried logs using SQLite to review interaction data
   * Educated users post-submission with tips and links

**5. Conclusion**

The phishing simulation platform demonstrates how attackers exploit human vulnerabilities. This ethical tool helps organizations evaluate employee awareness and strengthen their defense through education. It successfully integrates real-world simulation with safe lab practices using open-source tools.