Ethical Phishing Simulation Platform

INTRODUCTION

Phishing constitutes a significant threat to cybersecurity, and fostering user awareness remains one of the most effective countermeasures. This project showcases an Ethical Phishing Simulation Platform developed using Python and Flask, augmented by a bespoke email dispatch script and an authentic-looking login interface. By leveraging Ngrok, the local Flask server is securely exposed to external devices, thereby emulating real-world phishing scenarios for educational and training purposes.

SYNOPSIS

This project is designed to raise awareness about phishing threats by safely demonstrating how attackers can lure users into revealing sensitive information. It uses Flask for the backend, a custom HTML/CSS login page for realistic simulation, and an SMTP-based Python script (send_email.py) to send phishing-like emails. Ngrok securely exposes the local server for remote access, and captured data is stored safely in a log file for educational analysis only — no real credentials are compromised, as clearly stated in the email. The primary goal is to educate users and promote best practices for identifying and avoiding phishing scams.

TOOLS USED

- **Programming Language:** Python
- **Framework:** Flask
- **Email Sending:** Python smtplib with Gmail SMTP server
- **Frontend:** HTML, CSS (for realistic design)

- **Server Exposure:** Ngrok tunnel to test on different devices
- **Logging:** Text file (logs.txt) for storing entered credentials (simulation only)

PROCEDURE

1. Created an HTML page with custom CSS to closely replicate a real login interface.
2. Developed a Flask application (app.py) in Python to serve the fake login page and capture user-entered credentials.
3. Used Ngrok to generate a public URL, making the local Flask server accessible from other devices.
4. Implemented the send_email.py script to send phishing simulation emails containing the Ngrok link to test participants.
5. Collected submitted credentials in log files for analysis and awareness demonstration.
6. Tested the entire setup on multiple devices to ensure proper functionality and realistic simulation.

CONCLUSION

This project effectively illustrates the mechanisms behind phishing attacks and underscores how effortlessly unsuspecting users can be misled by a deceptively authentic login page. It emphasizes the critical importance of scrutinizing email links and exercising vigilance while navigating online platforms. Furthermore, this simulation can be enhanced by integrating user-specific training modules, real-time monitoring dashboards, and automated reporting systems, thereby making it a robust awareness and training solution for large-scale organizational deployment.

Submitted by: SATVIK BHAGAT

Internship: Elevate labs