Title: Phishing offensive/defensive tool
Course: Application and Data Security
Semester: 3rd 2025
Group: Cyber-Phishing-Simulator-Defender

---
1. Attack Overview — Phishing Simulation

Our offensive team will develop a **phishing simulation tool** that safely mimics a real phishing campaign in a controlled lab environment. The simulator will:
- Generate and send simulated phishing emails to a local mail server or test inbox.
- Host a training landing page (via Flask) that looks like a login page.
- Log user clicks and credential entries (for demo only, no real data stored).
- Include strict lab-only safeguards:
  - Target whitelist (localhost or 10.x.x.x only)
  - Banner warnings (“For lab use only”)
  - No network propagation.

---
2. Defense Overview — Email Filter + Domain Detector + User Training
---
The defensive team will create a **multi-layer defense system** that includes:
- **Email filter:** Scans incoming messages for phishing indicators (keywords, links, sender mismatch).
- **Domain similarity detector:** Compares suspicious email domains (e.g., “gmai1.com”) against trusted ones using Levenshtein distance or fuzzy matching.
- **User training workflow:** Redirects caught users to an awareness page explaining phishing signs and safe practices.

---
3. Lab Target Description

- Environment: Two virtual machines (one attacker, one target)
- Attacker VM: Runs phishing simulator (Python + Flask)
- Target VM: Runs defense scripts and mail receiver
- Network: Closed lab network (no internet)
- Logs: Stored locally in `/logs/phishing_lab/`

Prepared by: Cyber-Phishing-Simulator-Defender Team
Date: October 2025