**Course Title:**
*Hands-On Network Security and System Administration Lab*

You can view this course introductory slides at https://alanshlam.github.io/lab/proposed_course_intro.pdf and find some demo videos of my lab work on my YouTube channel: https://youtu.be/x8QnnHYeG08 and https://youtu.be/b4hfGaglrys

## Course Description

This laboratory course delivers hands-on experience in system administration and network security through cloud-hosted lab environments. Students will develop practical skills in:

- Network debugging and traffic monitoring
- Vulnerability scanning, penetration testing, and intrusion detection using Wireshark, Nmap, Metasploit, Suricata, and the ELK/TIG stacks
- Secure service deployment with Nginx, Apache, two-factor authentication, and SSL/TLS certificates
- Analysis of real-world attack case studies and AI-assisted vulnerability assessment and forensic investigation

By integrating multiple monitoring and security tools, students learn to build and manage a cohesive security and monitoring environment. The course equips participants for roles in cybersecurity, IT administration, and security operations.

## Course Objectives

This lab course aims to:

1. Provide students with hands-on experience in system administration and network security using cloud-hosted lab environments.
2. Develop the ability to debug, monitor, and analyze networks using professional-grade tools.
3. Equip students with skills in vulnerability assessment, penetration testing, and intrusion detection.
4. Enable students to deploy and secure network services (web, 2FA, mail, DNS) in virtualized/cloud-hosted environments.
5. Introduce students to AI-assisted security analysis for vulnerability scanning and forensic investigation.
6. Foster the ability to integrate multiple security and monitoring tools into a cohesive infrastructure.
7. Prepare students for real-world cybersecurity operations by simulating incident handling, monitoring, and service deployment.

## Learning Outcomes

By the end of this lab course, students will be able to:

1. Perform network debugging and packet analysis using industry tools.
2. Configure and interpret results from system and network monitoring tools.
3. Conduct network reconnaissance and vulnerability scanning.
4. Execute penetration testing and analyze attack surfaces.
5. Deploy and manage intrusion detection and prevention systems (IDS/IPS).
6. Apply AI-assisted vulnerability and forensic analysis to real-world scenarios.

7. Configure virtual hosts, reverse proxies, 2FA, and SSL/TLS certificates for secure services.
8. Deploy and manage mail and DNS services.
9. Demonstrate Linux system administration skills for security and service operations.
10. Integrate multiple tools into a cohesive monitoring and security platform.

**Course Outline (Modules / Lab Topics)**

1. Foundations
   - Introduction to cloud-hosted lab environment
   - Linux system administration basics
   - Network management essentials (IP config, routing, services)
2. Network Debugging & Packet Analysis
   - Latency measurement with hping3
   - Path tracing with traceroute
   - Packet capture & analysis with tcpdump and Wireshark
3. Network & System Monitoring
   - SNMP monitoring
   - MRTG, ntopng for traffic visualization
   - Service and system monitoring with Nagios
   - TIG stack (Telegraf/InfluxDB/Grafana) for time-series monitoring
4. Mail and DNS Services
   - Setup Postfix (mail server) and Roundcube (webmail)
   - Setup Bind9 DNS server and explain DNS operation
5. Service Hosting & Web Security
   - Virtual host setup & reverse proxy with Nginx and Apache2
   - Implementing Two-Factor Authentication (2FA) for web access
   - SSL/TLS setup with Let’s Encrypt Certbot
   - Public Key Infrastructure (PKI) concepts and operation
6. Reconnaissance & Vulnerability Scanning
   - Network scanning with Nmap
   - Analyzing vulnerability scanning results
7. Security Testing & Intrusion Detection
   - Penetration testing with Metasploit
   - Intrusion detection and prevention with Suricata
   - Log analysis & visualization with ELK stack
   - Firewall basics and integration with IDS/IPS
8. AI-Powered Analysis
   - Real-word attack case studies
   - Using free LLM (via OpenRouter) for vulnerability scan analysis and network forensic recommendations
9. Final Integration Project
   - Students design and deploy a mini “security lab” combining:
     - Monitoring stack
     - IDS/IPS with logging and dashboards
     - Secure web services with SSL
     - Mail/DNS integration
     - AI-assisted vulnerability and forensic analysis

**Target Students**
Students who want to gain solid hands-on skills in system administration and network security using cloud-hosted environments, and explore AI-assisted tools in cybersecurity.