Security Summary Report

Overview

This document summarizes the key security operations and risk management activities performed as part of the Cybersecurity Manager Home Lab.

Key Accomplishments

- Implemented a SIEM solution (Splunk) for centralized log monitoring.

- Conducted vulnerability scans using OpenVAS and Nmap.

- Managed and remediate findings based on CVSS prioritization.

- Automated alert triaging using Python scripts.

- Performed incident response simulation and documentation.

Tools Used

- Splunk: Event monitoring and correlation.

- OpenVAS & Nmap: Vulnerability and network scanning.

- Cisco Firewall: Access control and network segmentation.

- Microsoft AD: User authentication and policy enforcement.

- Linux (Ubuntu): Web and server management.

Compliance Reference

Aligned with security best practices based on **NIST CSF** and **ISO 27001** standards.

Future Improvements

- Integrate Threat Intelligence feeds predictive detection.

- Expand automation scripts for faster response.

- Perform regular phishing awareness and user training.