Cybersecurity Portfolio - Kaleb Moffat

Technology plays a critical role in today's world, and securing digital assets is more important than ever. As an **entry-level cybersecurity and IT professional**, I am eager to apply my technical skills and problem-solving abilities to protect systems and mitigate security risks. The following portfolio showcases my skills, certifications, and projects while demonstrating my commitment to continuous learning.

With a passion for cybersecurity and IT, I am ready to bring my knowledge, adaptability, and problem-solving skills to an organization that values security and innovation. My goal is to **contribute to strengthening IT infrastructure, defending against cyber threats, and supporting overall system reliability.**

Technical Skills

Through my studies to obtain a **Google Cybersecurity Professional Certificate**, I have gained a strong foundation in cybersecurity and IT principles, completing the following courses:

- **Foundations of Cybersecurity** – Understanding key security concepts and best practices.
- **Manage Security Risks** – Identifying and mitigating security vulnerabilities.
- **Networks and Network Security** – Securing network infrastructure and defending against cyber threats.
- **Linux and SQL** – Using essential tools for system administration and data management.
- **Assets, Threats, and Vulnerabilities** – Assessing risks to maintain secure environments.
- **Detection and Response** – Monitoring systems and responding to security incidents.
- **Automate Cybersecurity Tasks with Python** – Using automation to enhance security operations.
- **Security Incidents and AI** – Gaining practical insights in security incident escalation and the use of AI in cybersecurity.

Project Experience

Security Audit

- Conducted security audit by reviewing company documents and scenarios.
- Analyzed security frameworks.

Network Attack Analysis

- Identified and assessed Denial-of-Service (DoS) attacks.

Network Layer Communication Analysis

- Monitored and interpreted IP addresses, access timestamps, and port connections for security evaluation.

OS Hardening

- Established a secure sandbox environment for testing and security analysis.
- Used TCP dump for network traffic inspection.

Network Hardening

- Configured firewall rules and conducted routine firewall maintenance.
- Implemented multi-factor authentication and developed secure password policies.

NIST Cybersecurity Framework (CSF) Implementation

- Applied NIST CSF principles to enhance organizational cybersecurity posture.

Linux File Permissions Management

- Configured and modified Linux file permissions for department-specific access control.

SQL Queries for Log Analysis

- Executed SQL queries to extract and review security logs for system monitoring.

Vulnerability Assessment

- Conducted vulnerability assessments and established risk grading criteria.

Incident Handling and Reporting

- Documented security incidents and compiled incident journal.

Automating File Updates with Python

- Used Python scripts to update files.
- Implemented algorithms to remove unauthorized IP addresses and maintain an updated access list.

Cybersecurity Training Platforms

- HackTheBox
- TryHackMe

Certifications

- Google Cybersecurity Professional Certificate (Completed)
- CompTIA Security+ (In Progress)