Defensive Security Intro - TryHackMe Lab Report

Name: Ashish Sawant

Email: aaashi0301@gmail.com

GitHub: https://github.com/aaashi03

LinkedIn: https://www.linkedin.com/in/ashish-sawant-a02412260/

TryHackMe Profile: https://tryhackme.com/p/ashish0301

Date: April 15, 2025

# 🧠 Lab Overview

The 'Defensive Security Intro' room on TryHackMe provides an overview of how organizations detect, respond to, and defend against cyber threats. It introduces defensive strategies, monitoring tools, and the Security Operations Center (SOC) role in protecting assets.

# 🎯 Objective

To understand core defensive security concepts and how they are used to monitor, detect, and respond to malicious activity in an organization.

# 📚 Key Topics Covered

- What is defensive security?

- Role and responsibilities of a SOC

- Introduction to monitoring and alerting

- Log analysis and incident response

- Tools used in defensive security: SIEM, firewalls, IDS/IPS

- Defense-in-depth strategy

# 🔐 Relevance to SOC Analyst Role

- Introduces the real-world tools and techniques used by SOC analysts

- Builds understanding of how alerts are generated and analyzed

- Shows the importance of accurate log correlation and response timing

# 🛠️ Hands-On Tasks Completed

- Reviewed common log sources and their use in detection

- Understood how SIEM systems help correlate and analyze logs

- Learned about alert triage and common false positive cases

# ✅ Conclusion

This lab strengthened my understanding of defensive cybersecurity and the SOC workflow. It is an essential step in my journey to becoming a SOC Level 1 Analyst, as it lays the foundation for threat detection and incident response.