Linux Fundamentals Part 1 & Part 2 - TryHackMe Lab Report

Name: Ashish Sawant

Email: aaashi0301@gmail.com

GitHub: https://github.com/aaashi03

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

Date: April 13, 2025

# 🧠 Lab Overview

These labs are part of TryHackMe’s beginner-friendly path designed to teach foundational Linux skills. Both Part 1 and Part 2 cover essential concepts and commands needed for navigating and operating in a Linux environment – a core skill for any SOC Analyst.

# 🎯 Objective

To develop hands-on knowledge of the Linux file system, permissions, navigation commands, user management, and scripting basics – all of which are crucial for incident response and threat hunting in SOC environments.

# 📚 Key Topics Covered

- Linux command-line navigation (pwd, ls, cd, etc.)

- File operations (cat, touch, mkdir, cp, mv, rm)

- Understanding file permissions (chmod, chown)

- Users and groups management

- Linux process management (ps, top, kill)

- Searching and filtering (grep, find, locate)

- Bash scripting basics

# 🔐 Relevance to SOC Analyst Role

- Linux is a common OS in production systems and servers.

- Many logs, alerts, and incidents happen on Linux-based systems.

- Comfort with shell commands helps in investigating compromised machines and logs efficiently.

# 🛠️ Hands-On Tasks Completed

- Navigated through different directories and files using CLI

- Practiced permission management using chmod and chown

- Used ps and grep to monitor processes and services

- Wrote simple bash scripts to automate basic tasks

# ✅ Conclusion

These labs provided a solid introduction to Linux, reinforcing skills critical for any cybersecurity career. The ability to handle Linux systems directly helps SOC analysts in real-world investigations and defensive operations.