Windows Fundamentals Part 1, 2 & 3 - 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

The Windows Fundamentals series (Part 1, 2, and 3) from TryHackMe is designed to provide foundational knowledge of the Windows operating system. These labs cover core concepts such as the Windows file system, registry, task manager, services, networking tools, and PowerShell. Understanding these is crucial for any SOC Analyst involved in threat detection and investigation.

# 🎯 Objective

To gain practical experience with the Windows OS environment, including navigating system tools, interpreting logs, and managing services, all of which are essential for detecting and responding to threats on Windows-based systems.

# 📚 Key Topics Covered

- Windows file system and navigation (Explorer, CLI tools)

- Task Manager and process monitoring

- Understanding the Windows Registry and regedit

- Services (services.msc), and common startup programs

- Networking tools like ipconfig, netstat, and nslookup

- PowerShell basics and automation

- Event Viewer logs and system diagnostics

# 🔐 Relevance to SOC Analyst Role

- Windows is the most widely targeted OS in enterprise environments.

- Log sources from Windows Event Viewer are crucial for incident detection.

- Many real-world attacks (malware, privilege escalation, persistence) target Windows environments.

# 🛠️ Hands-On Tasks Completed

- Navigated Windows system files and directories using CLI and GUI.

- Used Task Manager and services.msc to inspect running processes.

- Explored the Windows Registry and understood its role in system configuration.

- Executed PowerShell commands for system control and automation.

- Investigated Event Viewer logs to trace potential attack patterns.

# ✅ Conclusion

The Windows Fundamentals series built strong foundational knowledge for understanding Windows internals and system behavior. These skills will support my ability to identify and analyze threats during real SOC operations.