SOC Level 1 Lab Report – TryHackMe

Name: Ashish Sawant

TryHackMe Username: ashish0301

Lab/Room: Pyramid of Pain

Date: April 12, 2025

# 🔍 Objective

Understand the concept of the 'Pyramid of Pain' in cybersecurity and how it applies to threat detection and incident response.

# 🛠️ Tools Used

• TryHackMe Lab Environment  
• Threat Intelligence Concepts  
• MITRE ATT&CK Framework

# 📌 Steps Taken

1. Explored the Pyramid of Pain and how each layer represents different levels of difficulty for adversaries.  
2. Analyzed indicators such as Hash Values, IP Addresses, and TTPs (Tactics, Techniques, and Procedures).  
3. Answered questions and challenges within the TryHackMe lab to reinforce threat intelligence knowledge.  
4. Mapped adversary behaviors using the MITRE ATT&CK framework.

# 🧠 MITRE ATT&CK Mapping

• T1110 – Brute Force (Technique Level)  
• T1059 – Command and Scripting Interpreter  
• TA0001 – Initial Access (Tactic Level)

# 📋 Observations & Findings

• The higher in the pyramid (e.g., TTPs), the harder it is for adversaries to change behavior.  
• Focusing on detecting TTPs instead of just indicators like IPs or hashes can significantly improve detection capabilities.

# ✅ Conclusion

The Pyramid of Pain offers a valuable perspective for SOC analysts. This lab helped reinforce the need to shift from indicator-based detection to behavior-based detection using MITRE ATT&CK.  
Continuous learning and practice with such frameworks will enhance threat-hunting skills and improve incident response strategies.