Cyber Kill Chain - 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 'Cyber Kill Chain' room on TryHackMe focuses on understanding the seven stages of the kill chain model. It helps SOC Analysts detect, analyze, and respond to threats more effectively by identifying which stage of an attack is occurring.

# 🎯 Objective

To understand each phase of the Cyber Kill Chain, identify indicators of compromise at each step, and learn how defenders can detect and disrupt attacks at various stages.

# 🔗 Cyber Kill Chain Stages

- \*\*1. Reconnaissance\*\*: Identifying targets and gathering information.

- \*\*2. Weaponization\*\*: Creating a malicious payload.

- \*\*3. Delivery\*\*: Sending the payload to the target (e.g., via phishing).

- \*\*4. Exploitation\*\*: Executing malicious code on the target system.

- \*\*5. Installation\*\*: Installing backdoors or malware.

- \*\*6. Command & Control (C2)\*\*: Establishing communication with the attacker.

- \*\*7. Actions on Objectives\*\*: Exfiltration or data destruction.

# 📌 Key Takeaways

- Each stage can be monitored using different log sources and SIEM tools.

- Early detection (Reconnaissance, Delivery) can stop an attack before serious damage.

- MITRE ATT&CK mappings help correlate attack techniques to the kill chain.

# 📊 Logs & Indicators Observed

- Suspicious IP scanning attempts in the Reconnaissance phase.

- Use of exploit kits observed during the Exploitation phase.

- Outbound C2 traffic over non-standard ports.

# 🛡️ SOC Analyst Response Actions

- Set up alerts for known IOC patterns.

- Monitor for unusual login behaviors and outbound traffic.

- Correlate across multiple log sources (firewall, endpoint, IDS).