Cyber Kill Chain

## 📓 **Notes – Cyber Kill Chain**

**Lab Name:** Cyber Kill Chain

**Summary:**  
The Cyber Kill Chain is a framework developed by Lockheed Martin to describe the stages of a cyber attack, from reconnaissance to achieving the attacker’s goal. It helps SOC analysts identify and stop threats earlier in the chain to reduce damage.

**Stages of the Cyber Kill Chain:**

1. **Reconnaissance** – Attacker gathers information about the target (e.g., open ports, public data, employee info).
2. **Weaponization** – Creating a malicious payload (e.g., malware, exploit code) based on gathered intel.
3. **Delivery** – Sending the payload to the victim (e.g., phishing email, malicious USB, drive-by download).
4. **Exploitation** – Triggering the vulnerability to execute malicious code.
5. **Installation** – Installing malware or persistence mechanisms.
6. **Command & Control (C2)** – Establishing a communication channel to the attacker’s server.
7. **Actions on Objectives** – Carrying out the attacker’s main goal (e.g., data theft, ransomware deployment, sabotage).

**Practical Takeaway:**

* Detecting and stopping an attacker **earlier** in the chain (e.g., at Recon or Delivery) greatly reduces the damage.
* SOC analysts can map indicators and alerts to the relevant stage of the kill chain.

**Tools/Commands:**

* None — conceptual learning.

