Unified Kill Chain

## 📓 **Notes – Unified Kill Chain**

**Lab Name:** Unified Kill Chain

**Summary:**  
The **Unified Kill Chain (UKC)** is a modern attack lifecycle framework that merges elements of the **Lockheed Martin Cyber Kill Chain** and the **MITRE ATT&CK** framework. It expands the traditional kill chain into more detailed, real-world stages to better capture complex, multi-vector cyber attacks.

**Three Main Phases & 18 Stages:**

### **1. Initial Foothold (Preparation & Entry)**

1. Reconnaissance – Gathering intel on targets.
2. Weaponization – Creating malicious tools/payloads.
3. Delivery – Transmitting the payload to the target.
4. Social Engineering – Manipulating humans for access.
5. Exploitation – Using vulnerabilities to gain access.
6. Persistence – Establishing long-term access.

### **2. Network Propagation**

1. Privilege Escalation – Gaining higher access rights.
2. Defense Evasion – Avoiding detection (e.g., obfuscation, disabling defenses).
3. Credential Access – Stealing credentials.
4. Discovery – Mapping out the environment.
5. Lateral Movement – Spreading to other systems.

### **3. Action on Objectives**

1. Collection – Gathering targeted data.
2. Exfiltration – Transferring data out of the network.
3. Command & Control – Maintaining communication with C2 servers.
4. Impact – Disrupting, destroying, or encrypting systems (e.g., ransomware).
5. Objectives – Achieving attacker goals.
6. Obfuscation – Covering tracks.
7. Monetization – Turning access/data into financial gain.

**Practical Takeaway:**

* UKC is more comprehensive than the original Cyber Kill Chain.
* It aligns more closely with real-world attacker behavior and MITRE ATT&CK tactics.
* Helps SOC analysts map attacks more accurately during investigations.

