LAB Manual

PART A

(PART A : TO BE REFFERED BY STUDENTS)

**Experiment No.01**

**A.1 Aim:**

To Study of Cyber Kill Chain Framework for any Critical Infrastructure Cyber Attack

**A.2 Prerequisite:**

Fundamentals of cyber-attack, types of attack, Cyber Kill Chain Framework, Critical Infrastructure.

**A.3 Outcome:**

**After successful completion of this experiment students will be able to** 1. Study the different types of attack focused on Critical Infrastructure

2. Study and able to investigate the attack tactics.

**A.4 Theory:**

The **Cyber Kill Chain** offers a comprehensive framework as a part of the **Intelligence Driven Defense model**.

**What is the Cyber Kill Chain?**

The term “**kill chain**” was first used as a military concept that defines the structure of an attack that covers:

* The identification of the target
* The force dispatch towards the target
* The decision and order to attack the target
* The destruction of the target

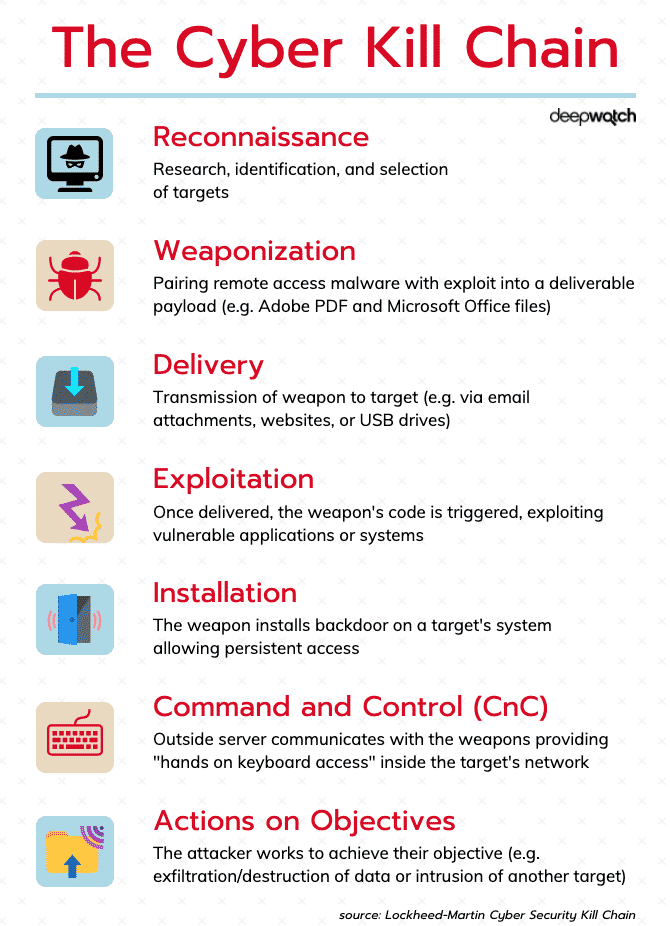
The idea of interrupting the opponent’s kill chain activity is often employed as a defence. Inspired by the whole kill chain concept, Lockheed Martin (an aerospace, security, arms, defence and advanced technologies company based in the United States of America) created the Cyber Kill Chain. It is a **cybersecurity framework** that offers a method to deal with the intrusions on a computer network.

Since it first emerged, the Cyber Kill Chain has evolved significantly in order to anticipate and recognize **insider threats** much better, detect various other attack techniques like advanced ransomware and **social engineering.**

The Cyber Kill Chain consists of seven steps that aim to offer a better attack visibility while supporting the cyberattack / cybersecurity analyst to get a better understanding of the adversary’s tactics, procedures and techniques. The **seven steps of the Cyber Kill Chain** illustrates the different phases of a **cyberattack** starting from reconnaissance, reaching to the exfiltration.

## What are the 7 steps of the Cyber Kill Chain?

The Cyber Kill Chain consists of 7 steps: Reconnaissance, weaponization, delivery, exploitation, installation, command and control, and finally, actions on objectives. Below you can find detailed information on each.



***Figure 1. Cyber Kill Chain Framework***

**1. Reconnaissance:** In this step, the attacker / intruder chooses their target. Then they conduct an in-depth research on this target to identify its vulnerabilities that can be exp+-9loited.

**2. Weaponization:** In this step, the intruder creates a **malware weapon** like a virus, worm or such in order to exploit the vulnerabilities of the target. Depending on the target and the purpose of the attacker, this malware can exploit new, **undetected vulnerabilities** (also known as the **zero-day exploits**) or it can focus on a combination of different vulnerabilities.

**3. Delivery:** This step involves transmitting the weapon to the target. The intruder / attacker can employ different methods like USB drives, e-mail attachments and websites for this purpose.

**4. Exploitation:** In this step, the malware starts the action. The program code of the malware is triggered to exploit the target’s vulnerability/vulnerabilities.

**5. Installation:** In this step, the malware installs an access point for the intruder / attacker. This access point is also known as the backdoor.

**6. Command and Control:** The malware gives the intruder / attacker access in the network/system.

**7. Actions on Objective:** Once the attacker / intruder gains persistent access, they finally take action to fullfil their purpose, such as **encryption** for ransom, **data exfiltration** or even **data destruction**.

PART B

(PART B : TO BE COMPLETED BY STUDENTS)

***(Students must submit the soft copy as per following segments within two hours of the practical. The soft copy must be uploaded on the Blackboard or emailed to the concerned lab in charge faculties at the end of the practical in case the there is no Black board access available)***

|  |  |
| --- | --- |
| Roll. No. | Name: |
| Class | Batch: |
| Date of Experiment: | Date of Submission: |
| Grade: | |

**B.1Aim**

**B.2 History of an Attack**

**B.3 Affected Areas/Impact**

**B.4 Observations and learning: Comparing with Cyber Kill Chain Framework**

***(Students are expected to comment on the output obtained with clear observations and learning for each task/ sub part assigned)***

**B.5 Conclusion**

*(****Students must write the conclusion as per the attainment of individual outcome listed above and learning/observation noted in section B.4)***

**B.6 Reference**

**B.5 Questions:**

1. Give presentation of your study experiment. Time limit is 10 minutes