**Intro to the Cyber Kill Chain**

The cyber kill chain (CKC) is a classic cybersecurity model developed by the computer security incident response (CSIRT) team at Lockheed Martin.

The kill chain model describes an attack by an external attacker attempting to gain access to data or assets inside the security perimeter. Each stage is related to a certain type of activity in a cyber-attack, regardless of whether it’s an internal or external attack.

These are the seven stages of the cyber Kill chain.

1. Reconnaissance

In the reconnaissance phase, cyber attackers are concerned with research, identification, and selection of targets. This is often achieved by crawling the Internet for conference attendees, email addresses, social media relationships, or information on target systems.

2. Weaponization

The weaponization stage is the preparation and staging phase of a cyberattack. The attacker has still not interacted with its intended victim. Instead, they are creating their attack.

This typically means coupling malicious software, like a remote access trojan (RAT), with an exploit by means of an automated tool called a weaponizer.

For example, an attacker may create an infected Microsoft Office document that is intended to be delivered via phishing emails.

3. Delivery

Delivery is the third phase of the cyber kill chain and refers to the attack vectors used to deliver malicious payloads. Such vectors include email attachments, malicious websites, and USB media.

4. Exploitation

After the payload has been delivered to the victim, the exploitation triggers the intruders' code. Most often this will target an application or operating system vulnerability, but it could also simply exploit the victim or leverage an operating system feature that auto-executes code.

5. Installation

The installation phase implies the attacker has an active exploit running on the target system. In this situation, they may look for additional vulnerabilities or use privilege escalation to gain additional access to the system to install a backdoor or remote access trojan that allows for persistence within the environment. They may also employ some form of obfuscation to conceal their presence and mask activity to avoid detection and thwart an investigation. This can include wiping files and metadata, overwriting data with false timestamps and misleading information, or modifying critical information so it looks as though access was never granted.

6. Command and control (C2) Typically compromised hosts communicate to an outside server to establish a command & control channel. Once the connection is established, the intruders have hands on the keyboard access to the target environment.

7. Actions on objectives Now after progressing through the six previous phases of the intrusion kill chain, intruders can take actions to achieve their original objectives. This is typically a violation of either confidentiality, integrity, or availability or a combination of the three. Alternatively, the attackers may only desire access to the initial victim in order to compromise additional systems and use lateral movement to gain access to new systems deeper in the network.

Project Submission Steps

1. Benefits of the Cyber Kill Chain Model For this assignment, write a 1-2 paragraph response to the following question.

How does the cyber kill chain model benefit cybersecurity professionals, especially as it pertains to the prevention of attacks and the response to attacks?

* The Cyber Kill Chain system, created by Lockheed Martin, is a component of the Intelligence Driven defence strategy for identifying and stopping cyber-attack activity.

Cyber kill Chain covers all phases of a potential assault and suggests different security measures to identify, reject, disrupt, degrade, trick, and contain attacks at every level. Analysing each stage of an attack can assist the cyber security analysts to prevent it.