Cyber Kill Chain

What is a Cyber Kill chain ?

The Cyber Kill Chain is a seven-step process that describes the different phases involved in a successful cyber attack. It was developed by Lockheed Martin in 2011 to help security professionals better understand and mitigate advanced persistent threats or APTs.

As you can see there are 7 steps or phases in the Cyber kill chain

- **Reconnaissance**: In this, The attacker gathers information about the target, such as network infrastructure, vulnerabilities, and potential entry points.
- **Weaponization**: The attacker couples a remote access payload with an exploit into a deliverable payload.
- **Delivery**: The weaponized payload is transmitted to the target, often through techniques like phishing, drive-by downloads, or exploiting web application vulnerabilities.
- **Exploitation**: The payload is triggered, exploiting a vulnerability to execute code on the target system.
- **Installation**: The attacker establishes a persistent presence on the compromised system by installing malware or backdoors.
- **Command and Control (C2)**: The attacker creates a communication channel to remotely control the compromised system.
- **Actions on Objectives**: The attacker carries out their intended malicious activities, such as data exfiltration, system disruption, or lateral movement within the network.

Lets understand this with an example. Suppose you have been given an assignment to hack into Apple and steal their latest iphone designs.

The first step, you will perform is to do some recon on the target. You will look for their employees, where there main office is, what software they use in the company, is their any vulnerability on their website, etc.

Let say you found a post on an employee's instagram with his work laptop. The picture shows an outdated Adobe Acrobat PDF Reader on his desktop which is vulnerable to a Remote Code Execution exploit.

Now in the next step - weaponization, you will use a malware or payload and add it with the Acrobat Reader exploit so that it can give you access on his system.

Next step is to deliver this to the target employee. For this, you will spoof their apple.com email address and attach a malicious PDF into the email and send it to the innocent employee who will thought that the PDF is his salary slip coming from the company's HR.

Once the victim clicks on the PDF. The exploit gets executed, giving us access on to his system and thus completing the step 4, that is exploitation.

Now, that we have access we don't want to loose it like if system reboots or something. So, we will add some backdoors on the system for persistence. This step is called installation.

Once we are done adding our backdoors on the target, we will establish a communication with our hacking Command and Control server from where we will give instructions to the target machine.

At last, in step 7 we will exfiltrate all the iphone designs to our server. Triggering FBI to roll out a arrest warrant in our name. Bingo!
