Project Topic: Research The Cyber Kill Chain Model And The MITRE Matrix

Exercise: Create a google document that comprehensively covers attack techniques defined by the cyber kill chain model and the MITRE Matrix.

Specification:
For each of the attack techniques listed, provide the following information:
A concise definition for the technique, explaining its purpose and how it is typically employed by adversaries.
A list of penetration testing tools that can be utilized to test the technique.
Example of custom software tools used by attackers for the technique from the MITRE website (https://attack.mitre.org/software/).

Attack Techniques
Reconnaissance
Weaponization
Delivery
Exploitation
Installation
Command and Control (C2)
Action on Objectives
Resource Development
Initial Access
Execution
Persistence
Privilege Escalation
Defense Evasion
Credential Access
Discovery
Lateral Movement
Collection
Exfiltration
Impact.

Name of Student : Mboro Miracle Joseph
Course : Cyber security Analysis

Project Approach

What is Cyber KillChain

Cyber Kill Chain is the process or steps a malicious attacker takes in other to successfully hack a system or network.
like every Operations the Doctors perform, they carry out necessary or basic steps just as Test, Scan, More Test .

The total process hackers take to carry out each attack is called a Cyber KillChain.

In movies it looks pretty and fast like Flash in DC Cartoons, but that's not true, It takes time and processes.

Steps in Cyber killchain.

What is Reconninassance ?

1. Reconnaissance : The first stage of the Cyber Kill Chain is "Reconnaissance." This stage involves the attacker gathering information about the target, such as identifying potential vulnerabilities, key personnel, network configurations, and putting security measures in place.
Hackers identify a vulnerable target and explore how to exploit it

● It purpose? : The major purpose of this stage is simple getting to know who your target is, his weakness ' Vulnerabilities ' and aspects you can implement Threats and your target becomes at Risk .

●. A list of penetration testing tools that can be utilized to test the technique.

• Port Scanning: This involves scanning the targets network to identify open ports and services.
•Vulnerability scanning: This involves using automated tools to scan the target’s systems for known vulnerabilities. •Enumeration involves gathering information about the target’s users, groups, and shares.

●. Example of custom software tools used by attackers for the technique ?
•Pen tester
•Red teamer,
•Adversary.

2. What is Weaponization?

Weaponization Stage : This is the process or stage where an attacker develops new malwares or payload to carry out an attack on its target.
● Purpose : The purpose of this stage is to gain access to its targeted individuals/ companies system or informations.
●This could involve creating believable spear phishing e-mails that look like e-mails that the target could potentially receive from a known vendor or other business contact.

☆ A list of penetration testing tools that can be utilized to test the technique.
• Nmap
• OpenVas
• Dmitry

What is Delivery in Cyber KillChain

3. **Delivery** : Like it implies to deliver an item to someone, now in Cyber Security the attacker is delivering malicious malwares to his target. Before this stage the attacker has researched and gained informations " Reconnaissance " about his target and created malicious malwares using different codes and tools " Weaponization", Now his sending it via different ways to his target

● Purpose?
The aim is to gain unauthorised access to this target system, Delivering his malwares is to simply to make his aim achievable.

●. Penetration testing tools :
• Email phishing

• Infected Attachments
• Decompromised Websites.

●. Software tools used by attackers for the Delivering Malwares.
• IM-Flooder
• Flooder
• Email-Flooder

What is Exploitation in Cyber killchain

4. **Exploitation** :
Exploitation means taking advantage of vulnerabilities identified during reconnaissance to execute the malicious payload delivered in the previous stage.
Vulnerability means weakness/ flaw, Exploitation means making those flaws and weakness to an advance to attack his target. The Vulnerabilities were discovered during the attackers Reconnaissance stage.
•Attackers have already scoped out vulnerabilities and now they actively exploit them to insert malicious code or to hijack legitimate processes.

●Penetration Testing For Exploitation are
•Brute force attacks.
•Buffer overflow attacks.
•SQL injection attacks.

● Example of custom software tools used by attackers for Exploitation technique
• sqlmap
• SILENTTRINITY
• Squirrelwaffle

What is Installation in Cyber killchain

5. **INSTALLATION** :
Installation like it implies is setting up a software/ Application in any device. This time its a malicious malware sent from an Attacker.
●His aim in installing his malwares is to get access but at this point his just setting up his Malwares in his targets network, system or Device remotely.
● Example of custom software tools used by attackers in Installation phase
• SDBbo

6. **Command and Control C^2 :**
Command and Control is a stage where y the attacker has successfully installed his malwares in the system " Targets System, Device or Network " and his gaining full command and control of that system. At this point he can fully access the clients System remotely .

- His aim is fully gaining access to C^2 his targets system, He can steal more informations or delivery his aim purpose of his attack.

- Example of custom software tools used by attackers in C^2 technique

- Sakula
- Rclone
- Rifdoor

7. **Action on Objectives :**
Action on Objectives stage simply means the main motive, plan or reason of carry out an attack, it will either be ransomware, spyware or to steal sensitive informations for his targets.

What is Resource Development in Cyber KillChain

8. **Resource Development** : Resource developmeResource development consists of techniques the attacker uses to create, purchase, or compromise resources to aid in targeting.

What is Initial Access in Cyber KillChain

9. **Initial Access**: It defines as acquiring access to the victim's systems. Gaining more access to the 🎯 targets system and devices not just his network

What is Execution in Cyber KillChain

10. **Execution**: It means executing malicious code on the compromised network or systems. Malwares and codes will be planted the targets network and Systems.

What is Persistence in Cyber KillChain

11. **Persistence**: Appropriately sustaining access to that system, Creating more grands to stay hidden and longer.

What is Defense Evasion in Cyber KillChain

12. **Defense Evasion** : defense evasion as a way for malicious actors to evade detection during an attack. Hackers use this technique to bypass security tools and mechanisms to gain a stronger foothold in enterprise cloud environments.
This stage they create an escape route to avoid getting known or traced.

What is Credential Access in Cyber KillChain

13. **Credential Access** :
refers to the phase within the cyber attack lifecycle where an attacker obtains unauthorized access to a system's credentials. Credential dumping occurs when a threat actor steals your credentials, such as your password, to perform various malicious activities, including ransomware. It is often confused with credential stuffing, a type of cyber attack that “stuffs” stolen credentials into multiple websites.

What is Discovery in Cyber KillChain

14. **Discovery** :
Not all informations are known during the Reconnaissance stage, But this stage he Discovers more flaws, weakness or personal informations about his Targets. This stage is carried out inside the targets system, network or device because the malicious actor is currently inside the targets system.

What is Lateral Movement in Cyber KillChain

15. **Lateral Movement** : lateral movement is the process by which attackers spread from an entry point to the rest of the network
lateral movement stage, attackers connect to additional systems and attempt to find the organization's most valuable assets. Attackers move laterally from one system to another to gain access to privileged accounts, sensitive data, or critical assets.

What is Collection in Cyber KillChain

16. **Collection** :
This stage involves the malicious actor extracting informations he got from lateral movement,

What is Exfiltration in Cyber KillChain

17. **Exfiltration** :
At the exfiltration stage, an advanced attacker finally hits home, getting their hands on the organization's most sensitive data. Attackers will find a mechanism — typically some sort of protocol tunneling — to copy the data outside the organization.

What is Impact in Cyber KillChain

18. **Impact** :
The cyber kill chain's purpose is to bolster an organization's defenses against advanced persistent threats (APTs), also known as sophisticated cyberattackers