Research The Cyber Kill Chain Model and The MITRE Matrix

Background of study.

The Cyber Kill Chain is a process that is used in many cyber attacks. It starts with reconnaissance, where the attacker gathers information about the target. This is followed by weaponization, where the attacker prepares the attack tool or payload. The next step is delivery, where the attack is delivered to the target. The final stage is exploitation, where the attacker takes advantage of a vulnerability to gain access to the target's systems.This process can be used to target individuals, organizations, or governments.

The Mitre ATT&CK Framework is used to help organizations understand the various techniques adversaries use to attack their systems. The framework provides a common language and structure for discussing attacks, and can be used to help identify potential gaps in an organization's defenses.

The Cyber Kill Chain Model Attack Techniques

1. Reconnaissance

- **Definition**: Reconnaissance refers to the gathering of information on a target, such as identifying potential entry points, services, and vulnerabilities, before launching an attack. This is typically performed by scanning networks, researching the company, and obtaining any publicly available data.
- **Purpose**: To map out the target environment and gain as much information as possible before moving to later attack phases. It helps adversaries determine the best approach for an attack.
- **How it is Employed**: Attackers use tools to collect data like open ports, domain names, IP addresses, and public records to create a detailed picture of the network.

Penetration Testing Tools:

- **Nmap**: Used for network discovery and port scanning.
- **Shodan**: An internet-connected device search engine.
- **Recon-ng**: A full-featured web reconnaissance framework written in Python.

Example of Custom Tools:

- **Maltego**: While also used by pentesters, attackers may develop their own information-gathering tools or scripts tailored to the specific environment they are attacking.

2. Weaponization

- **Definition**: Weaponization involves creating a payload that will exploit a vulnerability and deliver it to the target. This could be malware embedded into a document or a crafted email with malicious links.
- **Purpose**: To develop a tool or code that exploits the vulnerabilities found during reconnaissance and creates a delivery mechanism.
- **Employment**: Commonly, attackers will combine malicious code with a delivery vehicle like an email or exploit kits in websites.

Penetration Testing Tools:

- **Metasploit Framework**: For developing and testing exploits.
- **SET (Social Engineer Toolkit)**: Used to create spear-phishing attacks or payloads.
- **Veil-Evasion**: A tool for evading antivirus detection.

Example of Custom Tools:

- **Empire**: A post-exploitation framework that attackers customize for covert operations.

3. Delivery

- **Definition**: Delivery is the transmission of the weapon to the intended target. This could be via email attachments, websites, or even removable media.
- **Purpose**: To successfully transmit the weaponized code to the victim's environment.
- **Employment**: Attackers may use phishing emails, waterhole attacks, or exploit kits embedded in websites to deliver the malicious payload.

Penetration Testing Tools:

- **Phishing Framework**: Tools like Gophish for simulating phishing campaigns.
- **Social Engineering Toolkit (SET)**: Again, for spear-phishing.
- **BeEF (Browser Exploitation Framework)**: Targets web browsers.

Example of Custom Tools:

- **Spearfish**: Custom phishing toolkits that adversaries can tailor to specific organizations and targets.

4. Exploitation

- **Definition**: Exploitation is the act of exploiting a vulnerability in the target system to gain unauthorized access. The attacker executes their malicious code to gain control over a system.
- **Purpose**: To gain control of the target system by triggering the exploit and achieving initial access.
- **Employment**: Exploits can be zero-day vulnerabilities or known exploits that have not been patched on the target system.

Penetration Testing Tools:

- **Metasploit**: Popular for testing exploits and payload delivery.
- **Exploit-DB**: A database of known exploits that pentesters can use.
- **Core Impact**: A professional-grade penetration testing tool.

Example of Custom Tools:

- **RIG Exploit Kit**: Custom exploit kits used by attackers to exploit vulnerabilities in outdated software.

5. Installation

- **Definition**: Installation occurs when the attacker successfully installs malware or another malicious tool on the victim's system.
- **Purpose**: To establish a foothold and ensure continuous access to the system by installing backdoors or rootkits.
- **Employment**: This could involve installing ransomware, spyware, or other tools that allow the attacker to maintain control.

Penetration Testing Tools:

- **Meterpreter**: A post-exploitation tool within Metasploit.
- **Cobalt Strike**: A legitimate penetration testing tool that can be used for persistence and payload delivery.
- **Empire**: Often used for persistent access.

Example of Custom Tools:

- **PlugX**: A common backdoor used by attackers to maintain access to a compromised system.

6. Command and Control (C2)

- **Definition**: Command and Control refers to the method used by attackers to remotely control infected devices. It's how they send commands and retrieve data from compromised systems.
- **Purpose**: To maintain control over compromised systems and execute further actions.
- **Employment**: Attackers may use HTTP, HTTPS, or DNS for covert communication between compromised systems and their command servers.

Penetration Testing Tools:

- **Cobalt Strike**: Often used to simulate command and control for Red Teams.
- **Metasploit**: Can be used for basic C2 setups.
- **Merlin**: A cross-platform C2 framework.

Example of Custom Tools:

- **Zeus**: A well-known banking Trojan that also serves as a C2 tool to exfiltrate information.

7. Actions on Objectives

- **Definition**: Actions on Objectives refer to the end goals of the attacker, whether it's data exfiltration, system destruction, or another form of sabotage.
- **Purpose**: To achieve the attacker's ultimate goal, such as stealing sensitive data or disrupting operations.
- **Employment**: The attacker may now exfiltrate data, encrypt files, or alter system configurations based on their objectives.

Penetration Testing Tools:

- **Exfiltration Tools**: **rclone**, used to exfiltrate data to cloud services.
- **Cobalt Strike**: Used to simulate data theft or system sabotage.
- **PowerShell Empire**: For stealthy post-exploitation and data exfiltration.

Example of Custom Tools:

- **DarkComet RAT**: Custom remote access tools used to exfiltrate data or destroy systems.

The MITRE Matrix Model Attack Techniques

1. Initial Access

- **Definition**: Initial Access refers to techniques that adversaries use to gain a foothold within a network or system. This is often the first step in an attack.
- **Purpose**: To obtain access to the target's systems.
- **Employment**: Attackers use phishing, exploiting vulnerabilities, or leveraging weak credentials to gain access.

Penetration Testing Tools:

- **Social Engineer Toolkit (SET)**: For creating spear-phishing campaigns.
- **Metasploit**: To test for vulnerabilities in systems.
- **Gophish**: For phishing simulations.

Example of Custom Tools:

- **Phishing Kits**: Custom kits like **RoyalRoad** or **Phishing Frenzy** used to deliver malware via phishing.

2. Execution

- **Definition**: Execution refers to techniques where adversaries execute malicious code on a local or remote system.
- **Purpose**: To run malicious code and initiate the attack within the target's system.
- **Employment**: Attackers may use scripting languages, infected documents, or exploit software vulnerabilities to execute code.

Penetration Testing Tools:

- **Metasploit**: Used to execute payloads on the target system.
- **Cobalt Strike**: For advanced red teaming and executing scripts on remote systems.
- **PowerShell**: Widely used in pentesting for script execution.

Example of Custom Tools:

- **PowerShell Empire**: A custom tool used by attackers to execute code through PowerShell.

3. Persistence

- **Definition**: Persistence techniques are used by attackers to maintain access to a compromised system through reboots or network disruptions.
- **Purpose**: To ensure long-term control over the compromised system.
- **Employment**: Attackers install backdoors, create scheduled tasks, or modify boot settings to re-establish access after interruptions.

Penetration Testing Tools:

- **Cobalt Strike**: Provides persistence mechanisms like remote services.
- **Empire**: For maintaining access through backdoors.
- **Metasploit**: Offers various persistence methods such as modifying startup scripts.

Example of Custom Tools:

- **PlugX**: A custom backdoor often used to persistently access targeted systems.

4. Privilege Escalation

- **Definition**: Privilege Escalation refers to techniques attackers use to gain elevated access, such as admin or root privileges, on a compromised system.
- **Purpose**: To increase control over the system and access restricted areas.
- **Employment**: Exploiting software vulnerabilities, credential dumping, or leveraging misconfigured permissions to escalate privileges.

Penetration Testing Tools:

- **Metasploit**: Commonly used for testing privilege escalation exploits.
- **Privilege Escalation Awesome Scripts Suite (PEASS-ng)**: A collection of tools to identify privilege escalation vectors.
- **BeRoot**: A privilege escalation project.

Example of Custom Tools:

- **Dirty COW**: A custom privilege escalation exploit used to gain root access on Linux systems.

5. Defense Evasion

- **Definition**: Defense Evasion involves techniques used to avoid detection by security tools like antivirus software, firewalls, or intrusion detection systems (IDS).
- **Purpose**: To operate within the system without being detected.
- **Employment**: Attackers may obfuscate files, disable security features, or manipulate timestamps to evade detection.

Penetration Testing Tools:

- **Veil-Evasion**: Used to create payloads that bypass antivirus detection.
- **Mimikatz**: Often used to evade detection while dumping credentials.
- **Obfuscator.IO**: A tool for obfuscating JavaScript code.

Example of Custom Tools:

- **FinFisher**: A custom tool used to evade detection by leveraging sophisticated obfuscation techniques.

6. Credential Access

- **Definition**: Credential Access techniques are used to steal usernames, passwords, tokens, or other authentication data.
- **Purpose**: To gain unauthorized access to systems by obtaining valid credentials.
- **Employment**: Attackers use techniques like keylogging, credential dumping, and brute-forcing to steal or guess passwords.

Penetration Testing Tools:

- **Mimikatz**: The go-to tool for credential dumping.
- **Hashcat**: A powerful password-cracking tool.
- **John the Ripper**: Another password-cracking tool widely used in pentesting.

Example of Custom Tools:

- **Custom Keyloggers**: Attackers may create tailored keylogging software to capture sensitive information.

7. Discovery

- **Definition**: Discovery techniques involve finding information about the network, systems, and other devices within the environment to map out further attack paths.

- **Purpose**: To understand the environment and identify other potential targets or weak points.
- **Employment**: Attackers use various tools to list processes, users, network shares, and services.

Penetration Testing Tools:

- **Nmap**: A tool for network discovery and port scanning.
- **BloodHound**: Used for Active Directory mapping and privilege escalation paths.
- **PowerView**: A tool for discovering information about Windows environments.

Example of Custom Tools:

- **Custom Recon Scripts**: Attackers may develop their own reconnaissance tools to automate the discovery process.

8. Lateral Movement

- **Definition**: Lateral Movement techniques allow attackers to move across systems within a network, often by compromising multiple machines.
- **Purpose**: To gain access to more sensitive data or higher-privilege systems.
- **Employment**: Attackers may use remote services like Remote Desktop Protocol (RDP) or Windows Admin Shares to move laterally across the network.

Penetration Testing Tools:

- **PsExec**: For executing commands on remote systems.
- **Impacket**: A collection of Python classes for working with network protocols.
- **CrackMapExec**: Used to move laterally by executing code across multiple machines in a network.

Example of Custom Tools:

- **EternalBlue**: A well-known custom exploit used to move laterally across systems by exploiting SMB vulnerabilities.

9. Collection

- **Definition**: Collection involves gathering data from target systems, such as sensitive files, credentials, or logs, in preparation for exfiltration.
- **Purpose**: To obtain the information of interest that the attacker wants to steal or use.

- **Employment**: Attackers may use keyloggers, screenshot tools, or search the file system for valuable data.

Penetration Testing Tools:

- **Wireshark**: For capturing and analyzing network traffic.
- **PowerShell Empire**: Can be used to collect information stealthily from compromised systems.
- **Metasploit**: Also used to collect sensitive data from compromised systems.

Example of Custom Tools:

- **DarkComet RAT**: A remote access tool that can be customized to collect sensitive data from compromised machines.

10. Command and Control (C2)

- **Definition**: Command and Control is the method attackers use to maintain communication with compromised systems to execute further actions or exfiltrate data.
- **Purpose**: To send commands and receive responses from infected systems.
- **Employment**: Attackers may use protocols like HTTP, HTTPS, DNS, or custom protocols to communicate with compromised machines.

Penetration Testing Tools:

- **Cobalt Strike**: Provides command and control capabilities for red teams.
- **Merlin**: A post-exploitation C2 framework.
- **Metasploit**: Can also be used for basic command and control.

Example of Custom Tools:

- **Zeus**: A well-known custom tool used for banking Trojans with command and control capabilities.

11. Exfiltration

- **Definition**: Exfiltration refers to the techniques used by attackers to steal data from compromised systems and transfer it to their own servers.
- **Purpose**: To obtain and extract the data of interest.
- **Employment**: Attackers may use encrypted communication, hide data in images, or use cloud services for exfiltration.

Penetration Testing Tools:

- **Rclone**: Used to exfiltrate data to cloud services like Google Drive.
- **Exfiltrator**: A tool that mimics data exfiltration over common protocols.
- **Metasploit**: Can be used for exfiltrating data through custom payloads.

Example of Custom Tools:

- **Hidden Tear**: A custom ransomware that encrypts files and exfiltrated data.

12. Impact

- **Definition**: Impact techniques aim to disrupt or destroy the target's systems or data, whether through encryption, wiping, or other means.
- **Purpose**: To destroy, disrupt, or alter the target's systems or data for financial gain or sabotage.
- **Employment**: Attackers may deploy ransomware, wipe files, or alter data to cause damage.

Penetration Testing Tools:

- **Cobalt Strike**: Can be used to simulate attacks that would disrupt systems.
- **Metasploit**: Can be used to demonstrate the impact of destructive attacks.
- **Shiva**: A tool for simulating ransomware attacks.

Example of Custom Tools:

- **WannaCry**: A well-known ransomware that encrypts files and causes significant impact.

References

Hutchins, E. M., Cloppert, M. J., & Amin, R. M. (2011). *Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains*. Proceedings of the 6th Annual International Conference on Information Warfare and Security, Seattle, USA. Lockheed Martin Corporation. https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/Gaining-the-Advantage_Cyber-Kill-Chain.pdf

MITRE Corporation. (2018). *MITRE ATT&CK: Design and philosophy*. MITRE Corporation. https://attack.mitre.org/docs/ATTACK_Design_and_Philosophy_March_2020.pdf

Offensive Security. (n.d.). *Metasploit unleashed: A comprehensive guide to the Metasploit framework*. Offensive Security. https://www.offensive-security.com/metasploit-unleashed/

Strom, B. E., Applebaum, A., Miller, D. P., Nickels, K. C., Pennington, A., & Thomas, C. B. (2018). *MITRE ATT&CK: Design and philosophy*. MITRE Corporation. https://www.mitre.org/publications/technical-papers/mitre-attack-design-and-philosophy

Strategic Cyber LLC. (2023). *Cobalt Strike user guide*. Strategic Cyber LLC. https://www.cobaltstrike.com/help

Delpy, B. (n.d.). *Mimikatz*. GitHub. https://github.com/gentilkiwi/mimikatz