Cyber Kill chain

Task 1: Intro

The Cyber Kill Chain will help you understand and protect against ransomware attacks, security breaches as well as Advanced Persistent Threats (APTs). You can use the Cyber Kill Chain to assess your network and system security by identifying missing security controls and closing certain security gaps based on your company's infrastructure.

By understanding the Kill Chain as a SOC Analyst, Security Researcher, Threat Hunter, or Incident Responder, you will be able to recognize the intrusion attempts and understand the intruder's goals and objectives.

Task 2: Reconaissance

Reconnaissance is the research and planning phase of an attack against a system or victim. Adversaries use this phase to gather information about their target to inform their next steps. This information can include infrastructure details, employee data, business processes, and exposed technologies. Reconnaissance is often passive and undetected.

Poor recon typically leads to sloppy attacks, while well informed adversaries can create highly targeted, believable payloads that increase their chances of success.

A valuable piece of recon is **OSINT** (Open-Source Intelligence). With OSINT, adversaries gather insights about their target through publicly available information.

- **Passive Recon:** This involves having no direct interaction with the target. This may include WHOIS lookups, social media scraping, or reviewing breach data.
- **Active Recon:** This involves direct contact with the target with activities such as social engineering, port scanning, banner grabbing, or probing for open services.

Email harvesting is the process of obtaining email addresses from public, paid, or free services. An attacker can use email-address harvesting for a phishing attack (a type of social-engineering attack used to steal sensitive data, including login credentials and credit card numbers). The attacker will have a big arsenal of tools available for reconnaissance purposes. Here are some of them:

- theHarvester: other than gathering emails, this tool is also capable of gathering names, subdomains, IPs, and URLs using multiple public data sources.
- Hunter.io: this is an email hunting tool that will let you obtain contact information associated with the domain.
- OSINT Framework: OSINT Framework provides the collection of OSINT tools based on various categories.

Questions:

1.What is the name of the Intel Gathering Tool that is a web-based interface to the common tools and resources for open-source intelligence?

Ans.OSINT Framework

2.What is the definition for the email gathering process during the stage of reconnaissance?

Ans.email harvesting

Task 3: Weaponization

After a successful reconnaissance stage, "Megatron" would work on turning the raw information into actionable attack tools through crafting **malware** and **exploits** into a **payload**. Most attackers usually use automated tools to generate the malware or refer to the DarkWeb to purchase the malware. More sophisticated actors or nation-sponsored APT (Advanced Persistent Threat Groups) would write their custom malware to make the malware sample unique and evade detection on the target.

Malware is a program or software that is designed to damage, disrupt, or gain unauthorized access to a computer.

Exploits are programs or code that take advantage of the vulnerability or flaw in the application or system.

A **payload** is a malicious code that the attacker runs on the system.

Questions:

1.What is the term for automated scripts embedded in Microsoft Office documents that can be used to perform tasks or exploited by attackers for malicious purposes?

Ans. Macro

Task 4: Delivery

Delivery is when Megatron decides to choose the method for transmitting the payload or the malware onto the target environment. There are plenty of options to choose from:

- Phishing email: after conducting the reconnaissance and determining the targets for the attack, the malicious actor could craft a malicious email that would target either a specific person (spear phishing attack) or multiple people in the company. The email would contain a malicious link or email attachment that would result into a compromise.
- USB drops offer the attacker a physical delivery medium into public places like coffee shops, car parks, or on the street. An attacker might decide to conduct a sophisticated USB Drop Attack by printing the company's logo on the USB drives and mailing them to the company while pretending to be a customer sending the USB devices as a gift.
- Watering hole attacks are targeted and designed to aim at a specific group of people by compromising the website they are usually visiting, redirecting them to a malicious website of the attacker's choice or creation. Victims would unintentionally download malware or a malicious application to their computer, resulting in a drive-by download. An example can be a malicious pop-up asking to download a fake Browser extension.

Questions:

1.What do you call an attack targeting a specific group by infecting their frequently visited website?

Ans.Watering Hole attacks

Task 5: Exploitation

Concept:

> Exploitation is the moment the attacker's code executes on the target, taking advantage of a known vulnerability. In this phase, Megatron can opt to utilise a number of key techniques to gain access:

- Malicious macro execution: This may have been delivered through a phishing email, that would execute ransomware when the victim opens it.
- Zero-day exploits: These leverages on unknown and unpatched flaws in a system. These exploits leave no opportunity for detection at the beginning.
- Known CVEs: The attacker can choose to exploit unpatched public vulnerabilities found on the target environment.

> Questions:

1.What is the term for a cyber attack that exploits a software vulnerability that is unknown by software vendors?

Ans.Zero -day

Task-6 Installation

Concept

The backdoor is essential to maintain access to the system. it can be achieved through:

- Installing a **web shell** on the webserver. A web shell is a malicious script written in web development programming languages such as ASP, PHP, or JSP used by an attacker to maintain access to the compromised system. Because of the web shell simplicity and file formatting (.php, .asp, .aspx, .jsp, etc.) can be difficult to detect and might be classified as benign. You may check out this great article released by Microsoft on various web shell attacks.
- Installing a backdoor on the victim's machine. For example, the attacker can use Meterpreter to install a backdoor on the victim's machine. Meterpreter is a Metasploit Framework payload that gives an interactive shell from which an attacker can interact with the victim's machine remotely and execute the malicious code.
- Creating or modifying Windows services. This technique is known as T1543.003 on MITRE ATT&CK (MITRE ATT&CK® is a knowledge base of adversary tactics and techniques based on real-world scenarios). An attacker can create or modify the Windows services to execute the malicious scripts or payloads regularly as a part of the persistence. An attacker can use the tools like **ssc.exe** (sc.exe lets you Create, Start, Stop, Query, or Delete any Windows Service) and Reg to modify service configurations. The attacker can also **masquerade** the malicious payload by using a service name that is known to be related to the Operating System or legitimate software.
- Adding the entry to the "run keys" for the malicious payload in the Registry or the Startup Folder. By doing that, the payload will execute each time the user logs in to the computer. According to MITRE ATT&CK, there is a startup folder location for individual user accounts and a system-wide startup folder that will be checked no matter what user account logs in.

Questions:

1.What technique is used to modify file time attributes to hide new or changes to existing files?

Ans.Timestomping

2.What malicious script can be planted by an attacker on the web server to maintain access to the compromised system and enables the web server to be accessed remotely?

Ans.Web shell

Task 7- Command and control

Concept:

After getting persistence and executing the malware on the victim's machine, Megatron opens up the C2 (Command and Control) channel through the malware to remotely control and manipulate the victim. This term is also known as **C&C or C2 Beaconing** as a type of malicious communication between a C&C server and malware on the infected host. The infected host will consistently communicate with the C2 server; that is also where the beaconing term came from.

The most common C2 channels used by adversaries include:

- HTTP on port 80 and HTTPS on port 443, where this type of beaconing blends the malicious traffic with the legitimate traffic and can help the attacker evade firewalls.
- DNS (Domain Name Server), where the infected machine makes constant DNS requests to the DNS server that belongs to an attacker, this type of C2 communication is also known as DNS Tunnelling

Questions:

1.What is the C2 communication where the victim makes regular DNS requests to a DNS server and domain which belong to an attacker.

Ans.DNS Tunneling

Task 8: Actions on objectives

Concept:

After going through six phases of the attack, Megatron can finally achieve his goals, which means taking action on the original objectives. With hands-on keyboard access, the attacker can achieve the following:

- Collect the credentials from users.
- Perform privilege escalation (gaining elevated access like domain administrator access from a workstation by exploiting the misconfiguration).
- Internal reconnaissance (for example, an attacker gets to interact with internal software to find its vulnerabilities).
- Lateral movement through the company's environment.
- Collect and exfiltrate sensitive data.
- Deleting the backups and shadow copies. Shadow Copy is a Microsoft technology that can create backup copies, snapshots of computer files, or volumes.
- Overwrite or corrupt data.

Questions

1.What technology is included in Microsoft Windows that can create backup copies or snapshots of files or volumes on the computer, even when they are in use?

Ans.Shadow Copy