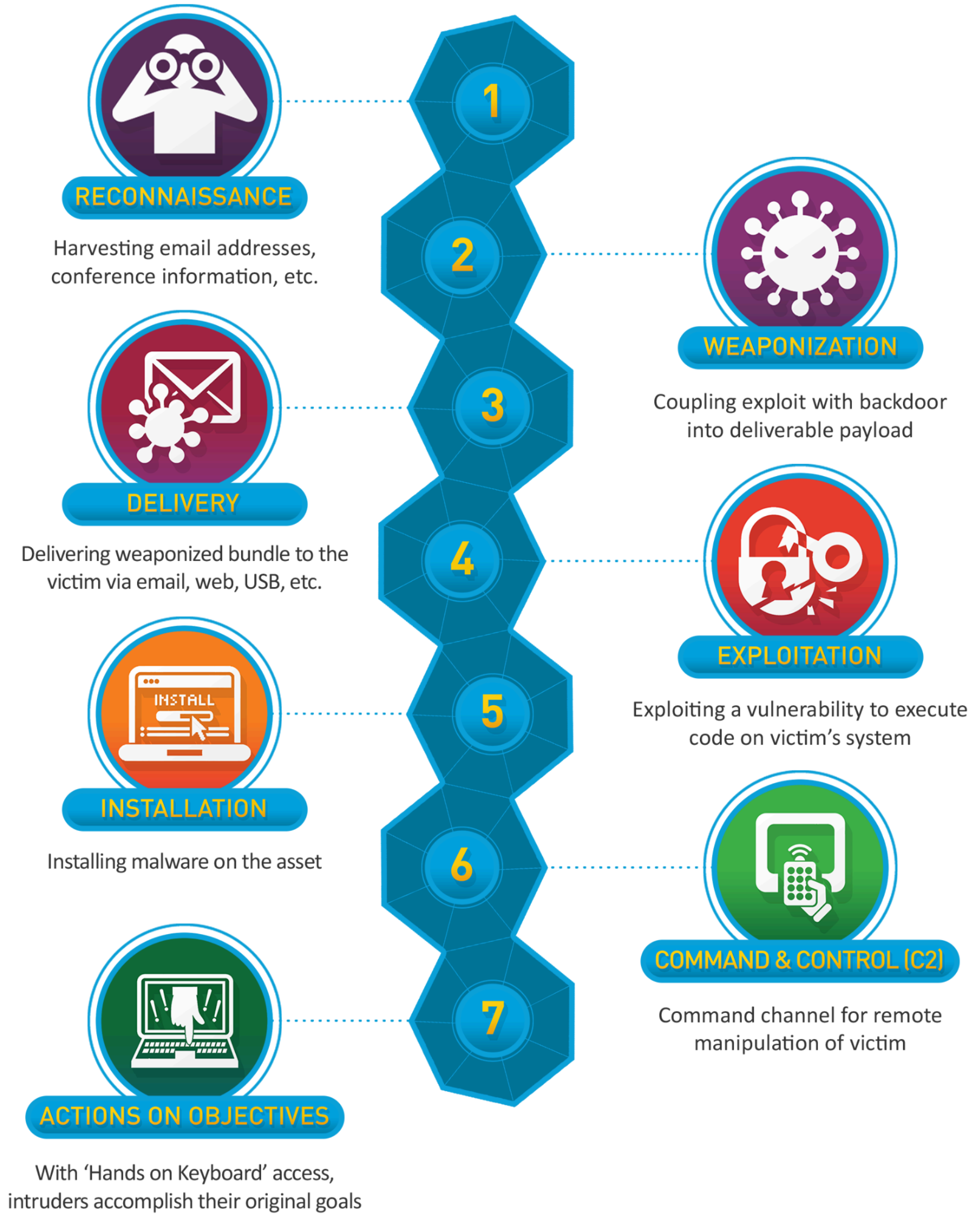
Cyber Kill Chain

Overview

This repository serves as a comprehensive resource for understanding and implementing the **Cyber Kill Chain** framework, a model developed by Lockheed Martin to identify and prevent cyber intrusions. The project showcases my learning journey in cybersecurity, focusing on analyzing and mitigating threats using the Cyber Kill Chain methodology.


1
RECONNAISSANCE
Harvesting email addresses, conference information, etc.
2
WEAPONIZATION
Coupling exploit with backdoor into deliverable payload
3
DELIVERY
Delivering weaponized bundle to the victim via email, web, USB, etc.
4
EXPLOITATION
Exploiting a vulnerability to execute code on victim's system
5
INSTALL
INSTALLATION
Installing malware on the asset
6
COMMAND & CONTROL (C2)
Command channel for remote manipulation of victim
7
ACTIONS ON OBJECTIVES
With 'Hands on Keyboard' access, intruders accomplish their original goals

What is the Cyber Kill Chain?

The Cyber Kill Chain is a structured model that outlines the stages of a cyber attack, from initial reconnaissance to achieving the attacker's objective. By understanding these stages, defenders can identify, disrupt, and mitigate threats effectively. Below is a brief overview of each phase, including an example and a mitigation strategy:

1. Reconnaissance

- **Description**: In Reconnaissance, a malicious actor identifies a target and explores a vulnerability and weakness in the network and gathers information about the target. Information such as network infrastructure, emails addresses, ip address, user id, physical location, operating system details or vulnerabilities, often through open-source intelligence (OSINT), social engineering and actively scanning the target.

There are two types of Reconnaissance :-

a) **Passive Reconnaissance** – It means gathering information without actually making contact with the target. It is stealthy and can collect information about DNS records, WHOIS records, user information, etc.Examples are crawling and scraping websites, social engineering and google dorking.

b) **Active Reconnaissance** – It means gathering information about the target system by actively scanning the target. It is noisy and less stealthy and can reveal information about the open ports, OS, running services, and other network infrastructure. Examples are scanning networks using the Nmap tool.

- **Mitigation Strategy**:
  i. Implement employee training on social media privacy settings and limit publicly available information about the organization.
  ii. WHOIS record should not reveal any names and addresses. Many registrars offer a privacy service, usually for an added cost.
  iii. Monitor and analyse network traffic to detect vulnerability and network port scanning.
  iv. Checking service logs.

2. Weaponization

- **Description**: During the Weaponization phase, the attacker creates an attack vector or payload, such as remote access malware, ransomware, virus or worm that can exploit a known vulnerability often combining it with a delivery mechanism like a document or script. They can also set up a backdoor so that they can continue to access the system even if their initial point is closed.

- **Example**:
    1. Attackers might use one of the available exploit kits. An exploit kit is an automated platform containing various exploits for various vulnerabilities. These platforms make it easy for attackers to package the exploit code within a payload, such as an executable file or specific documents.
    2. Attackers usually rely on creating Microsoft Office documents with malicious macros. If macros are enabled, a macro executes a saved set of instructions when the document is opened.
    3. The attacker may create a harmful attachment for a phishing email, host it on a website, or store it on a USB memory device. The attacker must, however, prepare how to send the payload to the vulnerable service in the following phase if they wish to target a service that is vulnerable.
- **Mitigation Strategy**:
    1. Employee or user training on how to check legitimate emails.
    2. Users should check if the email is suspicious and report it to the security team.
    3. Disable unnecessary features and uninstall unnecessary software and remove unnecessary browser plugins.
    4. Disabling macros in office documents and enforcing Windows Group Policies.

3. Delivery

- **Description**: The weaponized payload is transmitted to the target, commonly via phishing emails, malicious attachments, compromised websites, or USB drives.
- **Example**:
    1. Phishing emails
    2. Spear phishing emails
    3. Malicious web link
    4. File sharing platform
    5. Malvertising
    6. Smishing
    7. Social Engineering
    8. Physical means of Delivery
- **Mitigation Strategy**:
    1. User training in cyber security awareness
    2. Safe browsing practises
    3. Email and web filtering
    4. Use Web Application Firewall (WAF)
    5. Network monitoring and patch management

4. Exploitation

- **Description**: The payload exploits a vulnerability in the target's system, such as unpatched software or misconfigurations, to gain unauthorized access. The most straightforward approach is targeting a password-based authentication system. If the password is a default or weak password, it is easy for the attacker to discover.
- **Example**:
    i. An attacker exploits a zero-day vulnerability in a web server to gain initial access.
    ii. There are many other vulnerabilities that could be exploited, ranging from SQL injection to buffer overflow.
    iii. Depending on the specific vulnerability, this can create an easy entry even for someone without login credentials.
- **Mitigation Strategy**:
    i. Use intrusion detection systems (IDS) and Intrusion Prevention System (IPS) to monitor and flag suspicious activity that may indicate exploitation attempts and block suspicious traffic.
    ii. To strengthen password-based authentication, multi-factor authentication (MFA) should be mandated and password requirements should be strictly enforced.
    iii. To eliminate known vulnerabilities, patch management for clients and servers is essential. Moreover, vulnerability scanning is required to find any unpatched vulnerabilities.
    iv. Use of Web Application Firewall (WAF).

5. Installation

- **Description**: The installation phase ensures persistent access to the exploited system. Malware or backdoors are installed to establish persistent access, this allows the attacker to revisit the compromised system at a later time without having to go through the exploitation process again.
- **Example**:
    i. A remote access trojan (RAT) is installed on a compromised device to allow persistent access.
    ii. Creating scheduled tasks in MS windows and cronjobs in linux.
    iii. Attackers take advantage of system builtin functions such as tools and binaries also known as living-off-the-land binaries (LOLBins).
    iv. Deploying web shells and running it on HTTPS will ensure they can log in to their target system while camouflaging their activity within HTTPS traffic.
- **Mitigation Strategy**:

    i. Deploy endpoint detection and response (EDR) tools to detect and remove unauthorized software installations.
    ii. Regular system audit and comparison against a secure baseline are necessary to identify unauthorised changes.
    iii. Implement application allowlisting to prevent the installation of unauthorised software.

6. Command and Control (C2)

- **Description**:The Command and Control (C2) phase aims to establish this covert communication channel for use in the next phase. In this phase, the attacker sets up the C2 communication channel between the compromised systems and their own infrastructure enabling remote control and data exfiltration.
- **Example**: C2 infrastructure uses several tactics for resilient, covert communication:
    i. Common Protocols: Utilizes HTTP, HTTPS, DNS, or SMTP to blend with legitimate traffic.
    ii. Encrypted Channels: Employs HTTPS to evade network monitoring tools.
    iii. DNS Tunneling: Encodes data in DNS requests to bypass security solutions and firewalls.
    iv. Social Media & Cloud Services: Uses platforms like X direct messages or cloud services (e.g., Dropbox, Google Docs) for command delivery or data exfiltration.
    v. Domain Generation Algorithms (DGAs): Generates thousands of domain names, registering only a small fraction. Malware iterates through the list to find active domains, switching if one is blocked.
    vi. Fast Flux: Associates numerous IP addresses with a single domain, swapping them frequently. Compromised devices act as proxies, and malware switches IPs if one is blocked.
- **Mitigation Strategy**:
    i. Network Monitoring: Use firewalls, IDS, and IPS to identify unusual traffic patterns, high volumes, or connections to known malicious IPs.
    ii. DNS Monitoring: Analyze DNS queries for long or suspicious requests and high request volumes to detect C2 tunneling.
    iii. Web Traffic Monitoring: Monitor HTTP/HTTPS traffic and use content filtering to block suspicious URLs.
    iv. Encryption Inspection: Decrypt and inspect HTTPS traffic to uncover hidden C2 communication.
    v. Honeypots: Deploy honeypots to detect, analyze, and monitor C2 communication attempts and attacker behavior.

7. Actions on Objectives

- **Description**: Attackers execute their ultimate goal, such as stealing data, disrupting operations, deploying ransomware, or causing other damage.
- **Example**:
  1. An organization may be the target of attacks for a number of reasons. There are some blaring attacks. For instance, if the attacker's sole goal is to cause harm, they can start a destructive attack by deleting or modifying data in order to interfere with regular system functions.
  2. Cybercriminals often seek quick financial profits through ransomware attacks.
  3. In covert operations like industrial or political espionage, attackers prioritize stealing sensitive data, a process known as data exfiltration.
  4. To gain access to additional systems on a target network, attackers employ lateral movement, discreetly compromising other systems.
- **Mitigation Strategy**:
  1. Implement data loss prevention (DLP) solutions to monitor and prevent unauthorized data transfers.
  2. Establishing a reliable backup and recovery plan is indispensable to mitigate ransomware and other destructive attacks.
  3. To reduce an attacker's impact, organizations should implement network segmentation and strict access controls. Segmentation isolates critical systems, preventing lateral movement if one segment is breached. Access controls and the least privilege principle restrict access to sensitive systems and data.

Objectives

- Demonstrate a deep understanding of the Cyber Kill Chain framework.
- Offer actionable mitigation strategies for cybersecurity professionals.
- Serve as a learning resource for others interested in cybersecurity.

Why This Project?

This project reflects my commitment to advancing my cybersecurity knowledge and sharing it with the community. By studying the Cyber Kill Chain, I've gained insights into attacker methodologies and defensive strategies, which I've documented here for others to learn from.

"Understanding the Cyber Kill Chain empowers defenders to stay one step ahead of attackers."