# Study Guide

## Cyber Kill Chain

Created By: Jeshrel V Cyril, Teaching Assistant

## **Module 1:** Introduction

- Course outline
- What is Lockheed Martin Cyber Kill Chain? Brief intro of the 7 stages of cyber kill chain
- Prerequisites for the course
    - Basic knowledge in cyber security
    - Basic knowledge in cyber attacks
    - In operation Kali Linux either in VM or physical
    - Good Internet connection
- Objective of the courses
    - Introduction to Lockheed Martin Cyber Kill Chain
    - Designing defense architecture in depth using cyber kill chain

## **Module 2:** The Cyber Kill Chain

*Skills Learned From This Lesson: knowledge on Lockheed Martin kill chain, Defense in Depth using cyber kill chain*

- What is cyber kill chain?
    - It's a structure for a successfully hacking into a victim. Many structures of cyber kill chain exist in this course, we will be only learning about Lockheed Martin Cyber kill chain.
- High level understanding of Lockheed Martin Cyber Kill Chain – Derived from military kill chain
- 7 Stages of Cyber Kill Chain
    - Reconnaissance - Attacker harvests information on the target before the actual attack starts.
    - Weaponization - Attacker couples exploit with backdoor into deliverable payloads

    - Delivery - Attacker sends the malicious payload to the victim by email, USB or other means, which represents one of many intrusion methods the attacker can use.
    - Exploitation - Exploiting a vulnerability to execute code on victim's system
    - Installation - Installing malware/software on the asset.
    - Command and control - Attacker creates a command and control channel in order to continue to operate his internal assets remotely.
    - Action on objectives - The attacker performs the steps to achieve his actual goals inside the victim's network.
- Steps of cyber kill chain in defense
    - Detect
    - Deny
    - Disrupt
    - Degrade
    - Deceive
    - Contain

## **Module 3:** Reconnaissance

Lesson 3.0: Reconnaissance

*Skills Learned From This Lesson: Methods of reconnaissance, Tools used for passive reconnaissance, harvesting information of victim from social media, Tools used for active reconnaissance*

- Types of reconnaissance
    - Active
    - Passive
- Passive Reconnaissance / Footprint
    - Looking into publicly available information of the internet exposed by victim
    - This method does not notify/alert the victim of the attacked trying to harvest their information.
    - More time should be spent on this
    - Some tools used for passive reconnaissance
        - Whois – Provides information on IP/website on their location, who it's registered to, name of the technical contact person and the contact number.

- Nslookup – Provides details on the country where it is hosted, server IP and more
- Censys – Information of host servers and open ports
- Shodan – Need an account to access information from Shodan.io. Provides information on used technologies and services, open ports
    - Pivoting into each of the available will result in proving more details of the victim.
- Social media – Employee on forums, Facebook, twitter, etc. provides information. These information helps attacker to send you targeted phishing emails. This helps us understand how the details provided by victim publicly can indirectly result in the type of technology or tools he or she expertise, which mostly would be the technology or tools they are working with in their respective organization.
- Dumpster Diving – Physically accessing the trash of the victim searching for documents/manuals which are not shredded or disposed in a secure way. If the documents/manual is not shredded attacker will have access to organization information, manual of prototype, email if, contact details and more
- More

- Active Reconnaissance / Footprint
    - Involves the use of tools and techniques that can aid you in gathering more information of the victim
    - This method notifies/alerts the victim
    - Few methods of technical active reconnaissance
        - Vulnerability scanning
        - Fingerprinting – nmap
        - Web application scanning
    - Tools used for active reconnaissance
        - Nmap
            - Nmap scans the victim system for open ports, the services used by the victim and the operating system used by the victim
            - Example – If we can find a VNC port open, in this case I will assume the victim has not secured the port. So, they

may have an insecure account or an open port which will help us exploit the victim
- Traceroute
- Masscan
- Data Miner
- More

## **Module 3:** Reconnaissance

Lesson 3.1: Reconnaissance - Part 1

*Skills Learned From This Lesson: Social media usage to prevent reconnaissance, harvesting information of victim from social media, Tools used for passive reconnaissance*

- Social Media
  - What information does forum, Facebook, twitter and others provide attackers?
  - One of the most vulnerable links in an organization is the human aspect
  - Forum - Administrators usually help or post queries faced by them on public forum's they also update their profile on the tools and technology they have working knowledge and proficiency on. By doing so we are in-directly provided data to the attacker on the tools/technology used by the organization the victim works for. This way we can search for known vulnerabilities for the tool/technology on exploit-db to exploit the victim.
  - Facebook/twitter/others – Attacker gain knowledge of victim's like and dislikes and other personal information this helps attackers to send targeted phishing emails to the victim based on the reconnaissance.

## **Module 3:** Reconnaissance

Lesson 3.2: Reconnaissance - Part 2

*Skills Learned From This Lesson: What to look in an active scan, nmap usage and how to read its output, Tools used to find details from a web application*

- Active Reconnaissance / Footprint
  - Technical:
    - Vulnerability scanning

- Most popular way to find the vulnerabilities of operating system, applications and web applications
- If we find a vulnerability, we can exploit the vulnerability by following cyber kill chain

■ Fingerprinting – nmap
- Nmap scans the victim system for open ports, the services used by the victim and the operating system used by the victim
  - How does nmap detect operating system of a remote system? nmap sends a series of TCP and UDP packets to the remote host and examines practically every bit in the responses. After performing dozens of tests such as TCP ISN sampling, TCP options support and ordering, IP ID sampling, and the initial window size check, nmap compares the results to its nmap-os-db database of more than 2,600 known OS fingerprints and prints out the OS details if there is a match. Each fingerprint includes a freeform textual description of the OS, and a classification which provides the vendor name.
- Example – If we are able to find a VNC port open, in this case I will assume the victim has not secured the port. So

■ Web application scanning
- By using spider/web crawler we can find out all the links, services and dependencies available.
- Web Application is the most exploited
- Tools used for web application scanning
  - Burpsuite
  - Zed Attack Proxy
  - W3af
  - HTTrack
  - Octoparse
  - more

○ Non-Technical – Attacker interacts physically or in-directly(email) with victim or victims close circle and then masking the email like it was sent from there close circle to gain access

■ Physical interaction

- Social Media
    - Employee on forums, Facebook, twitter, etc. provides information. These information helps attacker to send you targeted phishing emails. This helps us understand how the details provided by victim public ally can indirectly result in the type of technology or tools he or she expertise, which mostly would be the technology or tools they are working with in their respective organization.

## **Module 4:** Weaponization

Lesson 4.0: Weaponization

*Skills Learned From This Lesson: Tools used to deliver payload, How to deliver a payload, How to turn an .exe into .rc, reverse_tcp.*

- This step and the following rely heavily on the efforts and the results obtained from reconnaissance. If we do not have any information of the victim, we would not be able to perform a targeted attack on the victim which is result is more success than a wild hunt which would end as the rate at which attack started in most cases.
- Metasploit is used to pick an exploit and in payload delivery
- Metasploit is one of the main tools used by the penetration tester (red team)
- We are in this case study using metasploit to deliver the payload using reverse_tcp
    - Articles to know more on reverse shell
    - How-to-use-a-reverse-shell-in-Metasploit
    - metasploit-tips-reverse-https-payload
    - Meterpreter HTTP/HTTPS Communication
- In this case study we have successfully delivered a .exe to the victim but in real world scenario these would be detected by the antivirus or other security tools deployed in the victim network
- To mask this we are going to use “unicorn”. Unicorn will mask the executable as a .rc and .txt which after being delivered to the victim using metasploit can delivered successfully without detection.
- Weaponization is a passive phase.
- In this stage we do not interact with the victim.

## **Module 5:** Delivery

Lesson 5.0: Reconnaissance

*Skills Learned From This Lesson: Payload delivery methods, How to deliver payload via USB*

- Transmission of payload/attack to the intended victim
- An attacker can send a payload using anonymous logins, escalated privileges, open port, social media or physical interaction.
- Extremely popular way to deliver a payload is by phishing email or distributing the infected USB drives at a local coffee shop/cafe or dropping them at car parking lots or leaving them at the front desk.
    - Ways to create a bad USB to deliver payload
    - Make Your Own Bad USB
    - How I made a programmable hacking USB device to infiltrate PCs?
- Main purpose of this phase is to find creative and effective ways to deliver a payload.

## **Module 6:** Exploitation and Installation

Lesson 6.0: Exploitation and Installation

*Skills Learned From This Lesson: How to send an exploit, How to install a payload, Ways to install a payload on the victim, what is exploitation*

- This phase is where we use the exploit on the system/network/other methods
- We are targeting the weakest link in an organization security posture – humans.
- This method out of all must be the most creative part for attacked as an attacker has to come up with a way to compel the victim to download/install the delivered payload by masking it actual intent.
- Another method is by collecting user credentials from a phishing email and then using those details to install the payload for command and control

## **Module 7:** Command and Conquer

Lesson 7.0: Command and Conquer

*Skills Learned From This Lesson: Communication ways to C&C, Twitter to communicate to C&C, C&C vs malware*

- Once a system's compromised and/or infected, the system has to call home to a Command and Control (C&C) system for the attacker to gain control and have connectivity.
- The challenge with C&C is to communicate without detection.
- Methods of C&C
    - RAT – Remote access tool
    - IRC chat relay
        - Both RAT and IRC are commonly used methods are easily detectable
        - If the victim has a SOC or a good security posture they will be able to detect both.
    - Twitter account
        - Twitter traffic in a network is not determined as a malicious traffic, attackers can post a command which is most cases is not detectable and even if detected they are ignored.
        - Attacked communicates to the payload/malware using twitter commands successfully
            - Command and control server in social media (Twitter, Instagram, Youtube + Telegram)
- When we have delivered a payload and started C&C we have verify if it is a system or a honeypot
    - A honeypot is a network-attached system set up as a decoy to lure attackers and to detect, deflect or study hacking attempts in order to gain unauthorized access to information systems. The function of a honeypot is to represent itself on the internet as a potential target for attackers
- We can now use metasploit to take a screenshot of the system.
- In this case we can see that the screenshot show that this is a laptop and a window PC
- In some cases, a C&C is not required if the attacker is in need of a specific data, the attacker can write a malware to collect the data based on the parameters of the program and let it communicate all the details one time to the attacker

- The downside is the attacker's ability is limited to the malware and if the data is not present in the specified locations the attacker does not get access to the data.
- By having connectivity to the victim, we can pivot deeper and exploit the system and the network to the fullest.

## **Module 8:** Action of Objective

Lesson 8.0: Action of Objective

*Skills Learned From This Lesson: What is Action of objective, How to cover your tracks*

- Attacker establishes access to the organization, they can then execute actions to achieve their objectives.
- It may include payment history, login credentials, account information, financial or military information.
- In our use case as per the screenshot the exploited system has no antivirus and is a laptop in most cases will have more local data stored.
- Using C&C we can
    - Extract data from the laptop
    - Kill process of the system
    - Clear windows event to delete the attacker's presence on the system
        - How to Cover Your Tracks & Leave No Trace Behind on the Target System
    - And more.

## **Module 9:** Defense in depth using the kill chain

Lesson 9.0: Action of Objective

*Skills Learned From This Lesson: How to plan a defense architecture, Defense action matrix*

- Cyber kill chain can not only be used for attack but also for designing an architecture to prevent an attacker from exploiting an organization.
- To design an architecture based on cyber kill chain involves 6 steps
    - Detect – In this step is to detect any and all reconnaissance activity on the organization

- Deny – In this step we are trying to deny all reconnaissance activity on the organization
- Disrupt – In this step we are trying to stop/change the reconnaissance activity on the organization
- Degrade – In this step we are trying to counter attack or reduce the impact of the attack on the organization
- Deceive – In this method blue team(defense) can get creative by sending fake or false information to the attacker during “Action of Objective” phase of the cyber kill chain.
- Contain – This step relies on the segregation in our network to contain or destroy the attacker’s activity in the network.

- To get all the above steps right in were the Defense Action Matrix comes in place. The defense can check and validate their placement of devices or device rules/policies against the attackers to build an effective architecture using this framework.

| Phase | Detect | Deny | Disrupt | Degrade | Deceive | Destroy |
|---|---|---|---|---|---|---|
| **Reconnaissance** | Web analytics | Firewall ACL | | | | |
| **Weaponization** | NIDS | NIPS | | | | |
| **Delivery** | Vigilant user | Proxy filter | In-line AV | Queuing | | |
| **Exploitation** | HIDS | Patch | DEP | | | |
| **Installation** | HIDS | “chroot” jail | AV | | | |
| **C2** | NIDS | Firewall ACL | NIPS | Tarpit | DNS redirect | |
| **Actions on Objectives** | Audit log | | | Quality of Service | Honeypot | |

Example:

- Detect <> Reconnaissance
    - We would need two technologies to detect passive and active reconnaissance
    - Passive Reconnaissance can be detected by Web Analytics which would find details of company published online.
    - One method to detect active reconnaissance is by using a NIDS either in Passive or Inline mode to detect any footprinting/reconnaissance activity on the organization.
- Detect <> Weaponization
    - Firewall rules / NIDS policies can be used to detect any footprinting/reconnaissance activity on the organization. Firewall rules can be set to detect a certain type of traffic and every good firewall rule will have a default deny/stop all traffic as the last rule in the rule set to prevent anyone from accessing the network apart from the authorized rule. NIDS policies can be configured in the same way to analyze packets
    - Information Sharing – Within an organization it is must to have the employee's educated about all basic security ethics. With one of the key rules as not to share sensitive information online, sensitive information can be of client details, work details, technology used within the organization, tools/devices used within the organization, etc.
- Detect <> Reporting
    - Every organization should have an internal way to report abnormal email/activity within the network/organization. This would include the organization educating the employees to report any suspicious/malicious email in their inbox. This would also include with employee informing/alerting the organization if they have found information leaked online that can harm/damage the organization in any way.
- By using this blueprint, we can measure the effectiveness the device/policies deployed and plan for future investment as per the organization needs for better security.

## **Module 10:** Conclusion

Lesson 10.0: Conclusion

*Skills Learned From This Lesson: Solution for flaws in cyber kill chain, Unified kill chain*

- Like every tool or policy, we have certain downsides/criticisms for cyber kill chain, and they are
- Passive Steps:
    - Criticism – It is hard to detect passive steps of reconnaissance and weaponization.
    - Possible solution – It is to add for devices or policies based on Defense Action Matrix to prevent all possible loopholes
- Insider Threat
    - Criticism – Model is not suitable for insider threats, which is partial true
    - Possible solution - If the right policies and devices are in place as per Defense Action Matrix even insider threat can be identified.
    - Example Policy:
        - Is to limit all users with administrative privileges so that they won't be able to install any software.
        - To monitor all important/sensitive folder/files are read, modify and write action to prevent even from administrator & users from misusing the information.
        - By using DLP within the network we can identify if a sensitive information is being sent outside the organization.
- Planning an architecture based on the cyber kill chain will help identify and eliminate and lot of attacks.
- Unifies Kill Chain is an extension to Lockheed Martin's kill chain and MITRE's ATT&CK framework.
- This model is a flow of 18 phases with 3 main steps with each step having a cycle that an attacker will go through to achieve the objective