The Cyber Kill Chain

Authors:
Kevin Hjelmtveit

May, 2021

The Cyber Kill Chain

. ***Abstract*-With the rise of cyber-attack, there is always a way to improve security measures and techniques. A popular term frequently used within cyber-security is the term cyber kill chain, the term consists of series of events on how to counter cyber attacks and defend critical network infrastructures, it lays out seven steps in which measures can be taken and improved to stop an attack in each stage. The seven stages are Reconnaissance, Weaponize, Exploit, Delivery, Installation, Command, and Control, Act on Objectives, this paper will investigate each step to determine their purpose, countermeasures, weakness, and how an attacker can exploit and attack network security measures.**

***Keywords*-The Cyber Kill Chain, Weaponize, Exploit, Delivery, Installation, Command and Control, Act on Objectives, Network Security.**

, ,

Contents

1 INTRODUCTION

The number one thing the majority of people agree on is that private information should be kept safe and private from malicious actors. With the rise of the internet, attackers have found their play field by actively looking and take advantage of companies and people for not taking their security measurements seriously, this practice has led to companies losing billions and personal information is at the hand of the wrong people. The amount of stolen credentials and data has increased rapidly since the internet was born in the early 90's. nearly 500 million credentials were is stolen in 2018 [28]. Even businesses are not prepared, its reported that 75% of all businesses don't even have a formal cyber attack response plan where as 66% of businesses attacked by attackers were not confident they could recover [8]. Having good security practices and routines within the organization that can help detecting and preventing security risk is very important.

Intrusion detection is the process of detecting and identifying intrusion activities and managing responsive actions through a computer system or network while intrusion detection are automatic systems to perform intrusion detection techniques. For an intrusion detection system, there are many ways an intrusion can be detected. There a sensor within the system to ensure that rules are upheld. The sensors do collect data and also alert the system when something inordinate happens, this could happen to network packets, log files and system calls [25]. These alerts are then being analyzed by the system or an engineer to make sure that the alert does occur if it's a false positive. IDS systems are automated to perform detection using different detection techniques an example are honeypots. Honeypots are decoy systems that are designed to lure a potential attacker away from critical systems, it is designed to collect information about attacker's activity and diver an attacker from accessing the system.

Intrusion prevention systems are responsible for stopping malicious attempts. A firewall is an example of an intrusion prevention system, some firewalls are capable to perform both as an IDS and IPS. The firewall technology today has drastically improved with Next-Generation Firewalls (NGFW) that allows modification on advanced policy including blocking specific application a web site, for example blocking facebook-chat, but still, allow Facebook. These firewalls also come with great analysis tools and supports. Every information system in government or other organizations does have a form of firewall. A firewall can monitor network activity and apply security policies to allow or deny specific network traffic, or for a specific application by port number, etc. NGFW is able to do all of these but also work as a router by configuration doing VPN tunneling.

The kill cyber kill chain model is used in the industry to focus on where threats appear and how to avoid and protect against them. Intrusion detection system (IDS) end intrusion prevention systems (IPS) are heavily used in every industry and company to secure systems and infrastructure against an attacker.

The Lockheed Martin cyber kill chain is a framework[15] consisting of chain of events seen in figure 1 which a malicious actor perform to get your data, these chain of events is also being used by security professionals as away to stop the actors before the chain is completed, by interrupting the actors at any stage of the chain we can establish control of our systems and prevent loss of data.

, ,

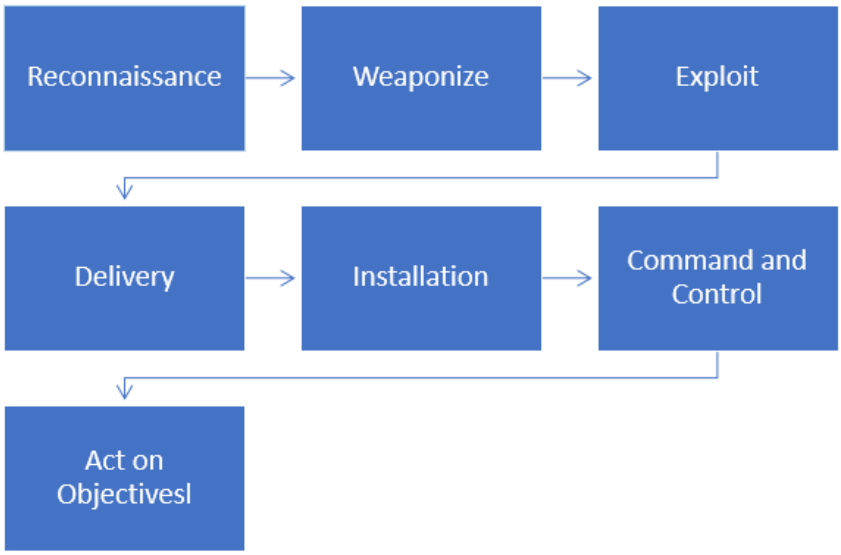

Fig. 1. The Cyber Kill Chain

2 RECONNAISSANCE

Reconnaissance has been an important part of warfare since the battles began. The ancient Roman army used surveillance techniques to gather intelligence about the enemy's defense [22]. The methods has maybe changed, but the primary goal of footprinting, meaning conducting reconnaissance against computer and information system is still the same. From a network security perspective, reconnaissance refers to a concept used for gathering intelligence about a system, company, or even people. In cybersecurity, reconnaissance involves activities carried out by a network operator to enhance network protection when external attacks occur on a network [6]. In other words, reconnaissance is highly applicable in network security and ethical hacking as a set of techniques and processes implemented to determine data and collect relevant information about a target system. In a cyber kill chain model, reconnaissance is the initial phase, as shown in figure 1.

It is important to state that reconnaissance can be avoided. The most effective strategy for avoiding reconnaissance is early detection and prevention. For example, high fidelity enhances early detection of reconnaissance by alerting computer users on port and host scan if an intruder attempts an attack. Secondly, interception and redirection can be used to avoid reconnaissance by denying the attacker accurate access to information. We differ from two types of reconnaissance, active and passive.

2.1 Active

Active reconnaissance occurs when an attacker engages a targeted system to access unauthorized systems and networks based on collected data [30]. Therefore, the attacker targets the system by performing a port scan to evaluate all the open ports. During active reconnaissance, it is essential for users to directly interact with the computer system to obtain accurate and relevant information during active reconnaissance. In other words, active reconnaissance involves gathering system information to allow attackers to access or penetrate a computer system. Thus, system information collected by the attacker is used to make unauthorized access. However, it is also used for security

purposes by system analysts to scan or test potential vulnerabilities that may compromise the security of systems and networks.

Network map (nmap) is one of the most used tools for mapping a network and scanning ports. Nmap allows the user to see what hosts are on the network and which ports are available. It can scan a specific host or a network range too. Figure 2 below show a nmap scan with results. It will prompt back a result that shows the host IP and all open ports for that specific host. With this information, an attacker can try to fingerprint and look for vulnerabilities that might work on the host to gain access. The T4 flag used in figure 2, tells how fast the scanning should be seen in figure 3, the lower speed is used to avoid IDS/IPS system from noticing the scan. The port scanning itself is not an illegal act since a normal network connection is performing the same act by using the 3-way handshake. The only difference is that during a port scan we are not aiming to make the full 3-way handshake. Instead of an attacker sending a SYN-ACK back to the victim, it sends a RESET flag instead, interrupting the handshake.

```
nmap -T4 -A -p- 10.10.10.3

PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
|_ftp-anon: *Anonymous FTP login allowed (FTP code 230)
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 10.10.14.7
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      vsFTPd 2.3.4 - secure, fast, stable
|_End of status
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
|   1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|_  2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)
3632/tcp open  distccd     distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4))
```

Fig. 2. Nmap scan

, ,

2.2 Passive

This involves gaining information on targeted computers and networks. However, passive reconnaissance does not actively engage the systems [30]. During passive reconnaissance, information available on the web is used to gain access through direct steps of extracting relevant information on the target environment. Passive reconnaissance techniques are interesting since they cannot be detected. The only way to defend against passive reconnaissance is to be proactive. This can be done by requesting and analyzing all the information within the organization. Security analysts will perform passive and active reconnaissance on the company know as red and blue teaming. This helps security professionals to know which attacks work or what information is available on the internet.

2.3 Open Source Intelligence

Typically, Open Source Intelligence (OSINT) refers to the process or practice of gathering data and information from publicly published sources. Therefore, it allows users to gather and analyze publicly available information. This data is then used in decision making in various intelligence contexts. In other words, for a source to be classified as open-source intelligence, it must be publicly available, gathered and analyzed promptly to meet a specific intelligence need. Lastly, OSINT is used for different purposes, such as penetration testing, ethical hacking, and identifying external threats [23]. OSINT can be a complex task were little information found can lead to a spider web of information. OSINT framework seen in figure 3 which can be found as a static website can help gathering and provide information such as web links and various resources which can be used during a recon. This website show nodes with unique paths for collecting information for a certain subject, for instance when gather email addresses you can simply follow the path which will lead you to a node with resources and tools to assist you with email harvesting.

The most common reconnaissance tools are HTTrack-Website Copier, Google Directives, the Harvester, Maltego and Shodan.

- HTTrack-Website Copier: HTTrack-Website Copier is a tool used to download an offline copy of a website. It is used to minimize the time spent on a target website to evade monitoring.
- Google Directives: Google Directive is a reconnaissance tool that searches information using directives
- The Harvester: The Harvester is another reconnaissance tool that uses a python script developed by Martorella Christian. It is highly implemented during reconnaissance to create a systematic list of sub-domains and e-mail on the targeted systems and networks
- Maltego: Maltego is a commercial tool that lets you automatically collect and visualize open-source information in a graph. Maltego may help you collect information by scraping up data from all publicly available areas of the Internet. Maltego can find information by connecting related email connections, personal related information to these emails. Phone number correlation social media connected to personal information through online forums etc. It can also provide a timeline analysis of what happens in different orders and present it visually.

- Shodan: Shodan is a tool almost like Maltego, but Shodan lets you scan the entire internet for services such as telnet, ssh and so on. It will give you a result of which devices are connected to the Internet, where they are located, and who is using them.

3 WEAPONIZES

Weaponization is the second phase of the cyber kill chain. It takes advantage of the information found in the recon phase and for further investigation. The purpose of the weaponization phase is

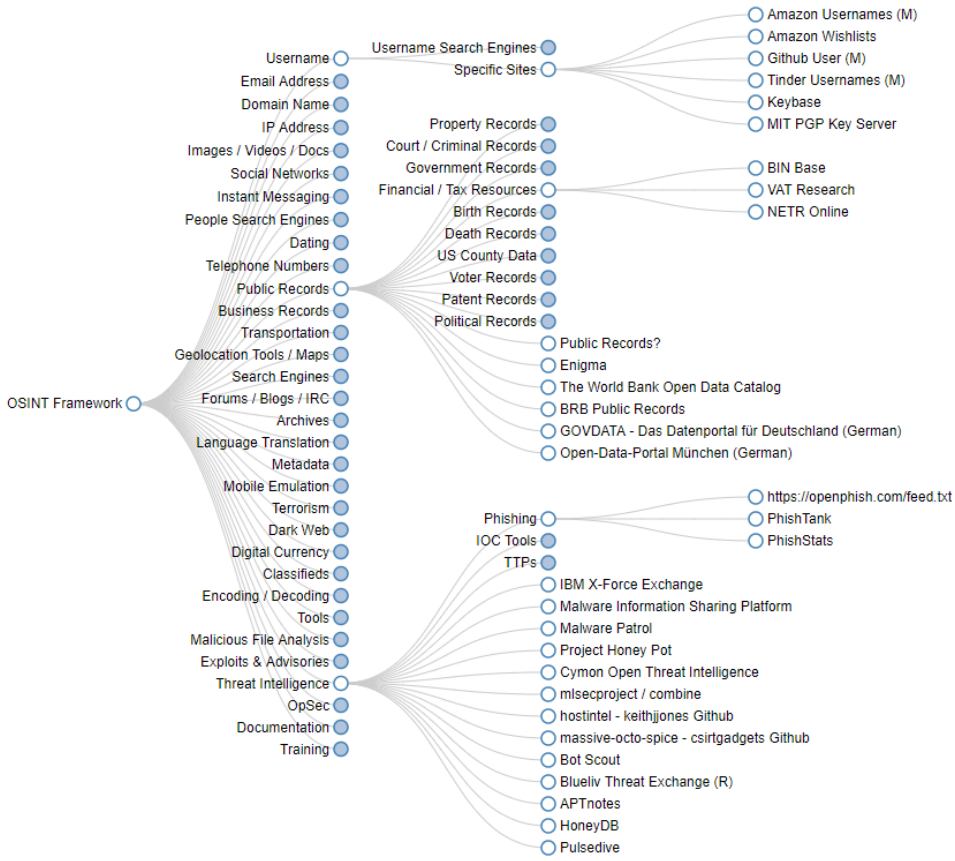

Fig. 3. OSINT Framework
[4]

to find a way "in" to the system, by taking advantage of the information found in the recon phase and then weaponize it in order access to the system. This is referred to as a backdoor, a backdoor can be almost anything a script that gives us persistent access to the system or even someone working for a company that has no clue that the email we sent was malicious, and by opening the email he invited us in. Phishing is the strategy explained above and is the most common way of getting hold of someone's information. Phishing is also used in social engineering attack were the attacker rely on trust when they want to steal data from an unsuspecting user [21]. In most cases, this attack occurs due to technological improvement and the improved means of accessing other people's data. An attacker using this mode of approach to exploit the victim's vulnerability tricks them into a trap where they are required to open an email or a text message that later allows the attacker to gain access to the data about the victim.

In real life, an attacker may create a bug that they send to the system of the users whom they plan to attack. These bugs collect information on the data of the target, the security system, and the preparedness of the users towards a specific attack. For this reason, installing a firewall assists one to block all the bugs, worms, and viruses sent by an unidentified attacker to collect personal

data. Limiting the number of users who can contact the system and the data storage unit for the organization is the other consideration essential for reducing the risk of attacks. This strategy reduces the risk of exposing critical data to attackers. When an intrusion occurs on the system, the effects can be devastating when the preparedness levels are relatively low [1]. Implementing an intrusion prevention system plays an essential role in reducing the risk of vulnerability and loss of critical data that the users may not wish to fall into an unwanted user's hands. One way that attackers can weaponize is by creating a malware weapon that they send to the target system to exploit their vulnerabilities. Therefore, an intrusion prevention program allows the users to prevent the cases of an attack and predict the next move that an attacker may use when exploiting the target. An access control list plays a vital role in data security since it reduces unauthorized users' rate of accessing the system.

The complexity of the risk is one of the assessments necessary for deciding concerning the right measure to consider in managing the cyber threat. The use of everyday vulnerability exposure is one of the most effective practices that allow insight into the significant vulnerabilities and exposure to specific threats. The National Institute of Standards and Technology (NIST) can also be applicable in managing cyber threats. It offers the guidelines that the private sector companies need to follow to prepare and identify significant cyber threats fully. This tool allows companies to create the right way to respond to cyber-attacks. A security policy also plays a vital role in avoiding cyber attacks. An effective security policy helps the users of a system select the right data security tool that may prevent the risk of attack. Weaponization may further make it challenging for the organization to undertake the practices that may help realize the firm's significant goals. Creating a security policy that focuses on the security details and potential vulnerabilities is an essential consideration that may create an effective way that puts it in a better position to prevent the occurrence of risks. Other security measures that can be taken to reduce the likelihood and impact of the weaponization stage:

- Awareness training to staff
- Have IDS/IPS in place to detect waponizers
- Collect logs and file incase of an attack

4 EXPLOIT

Cybercrimes are becoming common as criminals are continuously taking advantage of security vulnerabilities in computer systems. One of the he goals of cyber criminals' goals revolve around monetary gains, political motives, or simply prestige, hence posing significant threats to most organizations. Therefore, the best way to protect businesses from such threats is to understand the different vulnerabilities that might create risks to their network, then ensuring the weaknesses are secured before attackers can take advantage of the situation. However, before understanding the examples of computer vulnerabilities, it is essential to understand what vulnerability means in computer security.

A computer vulnerability refers to a system or network weakness that can cause damage when exploited or help attackers manipulate the system. However, it is not the same as a cyber threat, which involves outside elements. Computer vulnerabilities occur on network assets like particular applications, databases, or computers. Additionally, they are not caused by attackers' efforts or intentions, although criminals can leverage these patterns in their activities, causing some of them to use the definitions interchangeably. Hence, the exploitation of computer vulnerability is based on the attacker's motives and the vulnerability type. Some vulnerabilities can exist due to unexpected

interactions of fundamental flaws in particular programs, system components, or various software programs. Risks of a data breach can be reduced by understanding the common types of network vulnerabilities and implementing ways to address them.

Computer security vulnerabilities come in different kinds depending on the criteria like how the vulnerability can be used, what caused it, or where it exists. The most common vulnerabilities include; network, operating system, human, and process vulnerabilities. Network vulnerabilities involve issues around the network's software or hardware, which may expose it to outsiders' interference. Some examples include firewalls that are poorly configured and Wi-Fi access points that are insecure. Moreover, operating system vulnerabilities occur in specific operating systems that attackers can exploit to gain access and cause damage. A good example is evasion superuser accounts present in hidden programs or OS installs. Human vulnerabilities are the weakest connections in most architectures of cyber-security. Sensitive or personal information can easily be exposed by user errors. Also, it can disrupt systems or create available access points for cyber-criminals. Lastly, process vulnerabilities involve weaknesses that can be molded by specific process controls. A good example is using weak passwords, which can easily be hacked, giving attackers a chance to invade a computer system. Also, this may fall under human vulnerability.

, ,

The Open Web Application Security Project (OWASP) release every year the top 10 web application vulnerabilities faced by companies and organizations, this list is specific for web applications.

OWASP top 10

1. Injection
2. Broken Authentication
3. Sensitive Data Exposure
4. XML External Entities (XXE)
5. Broken Access Control
6. Security Misconfigurations
7. Cross-Site Scripting (XSS)
8. Insecure Deserialization
9. Using Components with Known Vulnerabilities
10. Insufficient Logging and Monitoring

Fig. 4. OWASP Top 10
[19]

On the top of the list we see [19]:

- 1. Injection , this include SQL, NoSQL, OS, and LDAP injection.
- 2. Broken Authentication this allows attackers to compromise passwords, keys, or session tokens, or to exploit.
- 3. Sensitive Data Exposure includes sensitive data, such as financial, healthcare, and PII. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes.

After disclosing the extent of vulnerabilities, they must be prioritized and assets by security teams to help reduce risks effectively and avoid misusing limited resources. A lot of research indicates that using traditional methods to reduce the risk for most companies has been insufficient. Hence, the industry should advance and start offering resources and data-driven equipment to security teams to promote effective remedies. Tenable collected vulnerability data is combined with threat and third-party data to analyze the vulnerabilities that can be highly exploited in the near future. While remedies to exploit vulnerabilities are still lacking, most of them undergo remediation for more than a year all over the global population. Remedy practices can be improved through threat intelligence and data-driven prioritization, as well as closing the avenue attacks of both Operational Technology (OT) and IT infrastructure. Overall, organizations should have better priority methods that involve components such as asset criticality and threat intelligence.

An exploitation technique used by an attacker with a very powerful, advanced but rare attack is Border Gateway Protocol (BGP) hijack. A successful BGP hijack will result in rerouting internet traffic through the attacker's network. To do this, the attacker needs to access an edge router to modify BGP and Autonomous System Number (ASN) information. The internet consists of several Autonomous Systems (AS) which are interconnected. BGP inter-AS routing mechanism that allows reachability information to be exchanged. The BGP nodes called peers are exchanging routing information among each other. The peer is informed about routes from different neighbors This information ends up in the routing table of a BGP router.

To defend against BGP hijacking attacks, defenders should first do simple network troubleshooting and contact ISP. The combination of RPKI and Prefix Filtering can still significantly lower the amount of BGP hijacking incidents

5 DELIVERY

Attackers have different techniques to access computer servers, to either disrupt normal operations or access sensitive information. To ensure an attack is delivered, methods such as phishing, Trojans, botnets, and Cross-Site Request Forgery (XSRF) are used. Phishing attacks are the most common attacks, phishing can occur in emails as seen in figure 5 where the attacker is masquerading the email address to be someone of importance or someone trustworthy. The key purpose is tricking email users, making them believe the message sent is vital [9]. Such applications send bizarre messages to emails to help access delicate information like security codes and bank passwords. When using Trojans, users are tricked through social engineering techniques to load and implement Trojans in their computer systems. For example, Trojans can resemble banking links like URL zones, but only calculates user accounts, hence giving chances for cyber-attacks.

Fig. 5. Apple Phishing email

Moreover, Botnets have been identified as significant threats, and researchers in security have identified some social media platforms due to their capacity to control and command channels for some botnets. Examples of these channels involve P2P file applications and IRC. This results to accounts shutting down some of the applications, hence giving botnets prospective threats and access to social platforms and organizations [10]. Lastly, the XSRF uses tricks to attack web browsers, which later execute illegal data or information in account forums managed by most users. When such attacks happen, it is easier for other users to share the data or image, hence increasing the chances of the attack. It is not enough to infect a user with malware by opening a phishing email. Typically, users must click the malicious links to ensure they access the websites and thus

deliver the malware. There are several ways malware can be masqueraded such as Windows macros, exploit kits, and fireless malware.

Windows macros refer to codes entrenched in a program to mechanize repetitive responsibilities. Hiding these malicious macros in programs can help launch attacks. Also, exploit kits are software systems on web servers to identify software weaknesses and exploit the discovered defects. They are easy to use since they are sold with already existing vulnerabilities. Lastly, fireless malware operates through legitimate programs like PowerShell to conduct malicious actions. PowerShell decodes malicious decoded and encoded script reaches out to Control and Command (CC) servers without including any file to the local hard drives. Among the three methods of delivering malware, using exploit kits is the easiest [20]. It resembles picking a lock, which makes it easier for attackers to access data or services. The kits already have installed vulnerabilities,hence making it easy to execute and upload malicious codes. Since they are easy to use, most cyber-criminals prefer them to other methods.

There is also a way to deliver malware physically, a classic example is to upload malware to a USB drives and go scatter the USB all over the potential targeted area, hoping an employee will pick one up and plug it into their computer inside the company's network. Another example of physical delivery is to dress up as a repairman and get access inside the server room and plug the device in the computer.

There are various ways to protect from these methods. For instance, avoid downloading attachments from unknown sources or clicking on suspicious links. Consequently, this can help prevent phishing, which tricks people into opening emails or clicking links that may prompt them to enter their personal information or infect their computer with malware. Also, an individual can update their software regularly to prevent attackers from accessing their information through outdated systems or vulnerabilities. For a company to avoid these methods, installing a firewall is the most appropriate strategy. Firewalls block unauthorized access either to or from private computer networks, hence preventing malicious attacks. Also, in anti-virus software cases, firewalls give extra malware barriers, thus lowering the chances of cyber-attacks.

6 INSTALLATION

Installation is the 5th step of the cyber kill chain. The purpose is to install the malicious content that has been delivered to the targeted system, this is a critical step that attackers apply to manipulate the system. Here, attackers are interested in the access gain to ensure that they manipulate the given system [17]. As a result, they will establish their tools and malicious software in form of viruses, Trojan horses, DoS, and malware within a system and later on be used to gain a foothold on the system. For the attacker to install the malicious tools onto the computing system, they create a backdoor process. The purpose is to control the system through Installation, this is established by creating a backdoor to maintain a high level of persistence on the targeted system to achieve the objectives, this will make sure that the attacker always has a way back on to the system. The backdoor server runs on the victim machine listening on the network and accepting connections from the attacker, the client runs on the attacker machine and it is used to connect to the backdoor to control it.

With remote Installation, the attacker will have to use online-based methods, including sending malicious emails and web content that tracks the installation process hidden in other prompts. The physical installation will come with the application of the USB devices or on hardware. Hardware

backdoors are backdoors where code has been implemented inside hardware or firmware of computer chips [2]. The intent is to undermine security in smartcards and other cryptoprocessors, but has also been found in cars. [27].

Detection of the malware issues is possible using various systems and mechanisms. Understanding the attack system will be essential to create a defensive mechanism. In the detection process, the scenarios are tested and will identify vulnerabilities. Hence, the IT department ensures that they close the loopholes within the system. Several tools are applicable to detect malicious attacks quickly and include antivirus, firewall, IDS, IPS, log analyzers, SIEM systems, traffic analyzers, and proper training to the employee [26].

To ensure that systems are secure, the security personnel must be aware of the loopholes and security vulnerabilities they face. Hence, the security personnel must apply a similar model to identify the vulnerabilities associated with the systems [12]. Here, there is a need to understand how the tack comes. The security personnel may consider preventing the attacks from happening. In this case, the access control lists, firewalls, anti-viruses, the IPS, penetration tests, and custom configurations. Ultimately, this allows them to lower any form of a successful attack on a system. Finding malware is promoted by the anti-malware programs that will not only detect but also identify it.

6.1 Post-Exploit

This is also called post-exploitation, where an initial foothold has been gained and the attacker can perform activities to help them understand and map out where they landed and can move laterally inside the system. Some the most common post-exploitation activities an attacker will perform to gain a foothold are:

- Privilege Escalation
- Lateral Movement
- Credential theft

Privilege escalation is the process of exploiting operating system or software security to exploit bugs, design flaws or mis-configuration, for the attacker to access protected resources. Privilege escalation results in the attacker gaining unauthorized access to these resources which the attack is not supposed to have.

It is important to differentiate privilege given to a user account and privilege gained by an attacker, one with authorized and other unauthorized. Authorized users are granted access tokens by the Local Security Authority (LSA). These access token describe the security context of a process or thread. Every authorization decision for securable resources taken access token into account

Attackers are known for searching for stored credentials in their attempt to escalate their privileges and move laterally. Unattended installations can leave behind files that contain credentials of privileged local accounts. Security training for employees can help avoid this by not saving passwords on the computer but use a password manager. Attackers will attempt to obtain credentials to gain access to other systems in the network

Passwords are the first and, most of the time, the only line of defense of the system, services, and accounts against unauthorized access. To protect users and applications, operating systems have to store passwords securely. Passwords are usually stored inside files or databases. If they were stored

in clear text, attackers would just have to open the password file or database to steal them.

Getting control over the credentials of an account means getting full control over the account and its privileges on a system Because of this, computer systems store a password by encrypting it, to make it harder for attackers the password is stored using a one-way encryption algorithm. There is no way to know the password starting from its encrypted form. Cryptographic hashing functions are also used to transform password from clear-text to encrypted form.

An attacker would have to try to guess the password, this can be done using a brute force attack. Brute force attack algorithm work by guessing the password, starting with one letter after the other.

Brute force attack cycle through every possible input combination, starting from a single character and escalates to n-characters long. By doing this we are sure that we will find the correct password, but it will take some time depending on password length and password strength. The biggest weakness of brute force attack is its time constraint, if the password we try to guess is complex and contains a combination of number, upper and lower case letters, special characters, and symbols it could take days or even years.

7 COMMAND AND CONTROL

The 6th phase of the cyber kill chain is the Command and Control phase, the purpose of this phase is to establish command and control (C&C) of the system. Before planning an attack on a particular target, the attacker evaluates the situation, to make sure that content is within the scope and the possibility of succeeding. This phase is done when the attacker has put in place their management and communication APT code onto the target network [5]. The attacker takes control of a system that he already compromised and later extracted the desired data on the target network. The command and control get executed using various techniques known by the attacker and mostly run undetected. The above occurs in the following ways; first, the attacker focuses on a specific computerized machine usually connected to systems inside the organization. The attacker gets to exploit the system by installing programs, commanding malicious applications on the target machines, or taking advantage of the plugins vulnerability on various browsers installed in the victim's computer [24] and send remote hidden instructions to compromised computers.

When a connection is established and the attacker succeeds in compromising the targeted network. The victim's computer recognizes the attacker's machines, and through the established connection, it sends signals where further commands get executed. The attacker can download and install software that will offer further support for the next attack through these commands. After this, it means that the attacker has already gained full access to the organization's computers. Therefore, he can save and run codes that are malicious on the organization's server. The codes make it easy to maneuver through the organization network, therefore, compromising all the organization's information. After the complete information has gotten compromised, the attacker can create a botnet which is a network created on a compromised system. The creation of a botnet means the attacker has full access to the organization's information. From there, he can do as he pleases with the information without being detected by a network security system.

Once the attacker has a connection, they may try as much as possible to stay undetected, and this is done by; evading signatures. Some system relies on antivirus that detects any malicious code. The attacker opts to attack the system with weak anti-viruses and avoids dynamic analysis systems

to avoid being detected. A system with this kind of analysis detects any malware immediately. The attacker accesses the system and terminates it immediately.

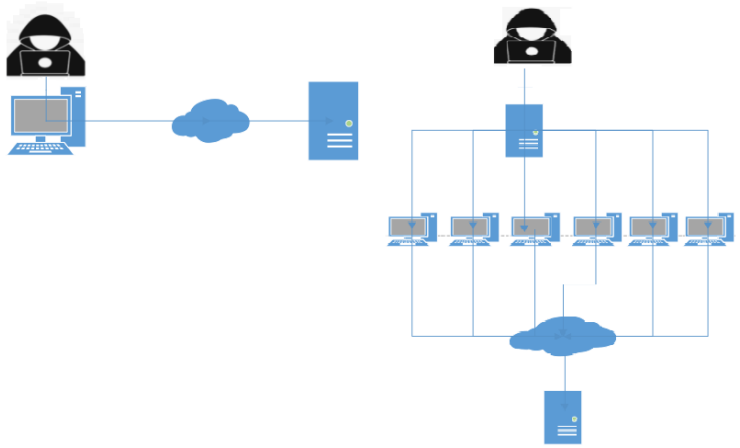

Fig. 6. DoS and DDoS Attack Strategies

The most common attack done by an attacker as DoS and DDOs attacks, these attacks rely on having a foothold into the victim's system and make them not able to reach their critical systems. This is done by resource exhaustion, meaning send and spread a huge amount of traffic to one target making it deny service which makes it unavailable. This can potentially shut the whole system down and all services that are dependent on it. Both DoS and DDoS attack use a command and control approach.

The major difference between DoS and DDoS attacks is that DDoS is using multiple computers to flood the servers making it inaccessible, this is done through a command and control server that sends out a request to the server. Figure 6 illustrates an attacker using a Command and control to control multiple computers called a botnet to attack a server.

The attack strategies in DoS and DDoS have a lot of similarities. The strategies can be divided into four phases. The primary components in the attack strategies are the attacker, master (handlers), agents, and the victims [16][11][3].

- First we have the victim, which is the host we are targeting for our attack.
- Second, we need agents, These are agent programs that actually conduct the attack on the victim. Attack agents are usually installed on host computers. To deploy agents we have to exploit our victim to find security holes to install our attack codes.
- Third, we have the master. This is controlled by the attacker. Its task is to coordinate the attack. This is also referred to as a command & control server, files and documents can be sent back to this server
- Lastly, we have the real attacker, this is the attacker using the control master. The attacker can hide behind the control master program.

With all of the components in place, the attacker can be his strategy. To perform a DDoS attack the strategies is simple, we divide it into three simple steps [3][11].

- Step 1. The real attacker will send his attack code as an execute message to the control master program
- Step 2. The control master will receive the message and deliver the command to his agents
- Step 3. The agent's machines will perform the attack on the victim host.

The use of honeypot has been on the rise in various organizations since it acts like a decoy or a bait whereby the attacker follows it without knowledge of being led to a trap [7]. Though it contains the valuable information the attackers require, it is still an effective method of dealing with cyber-attacks based on how legitimate it appears in attackers' eyes. Organizations can use other tools such as installing strong and updated antiviruses in their system that will help detect any malware. The other approaches to use are to train the employees on the dangers of opening an anonymous link and use a Virtual Private Network that creates a safe connection between the user and the internet.

8 ACT ON OBJECTIVES

When exploring new areas, there is an objective or goal that drives one to do so. The objective may or may not be of good intention, and therefore a particular motive is created to enhance the willingness and ability to perform the task. In the recent decade, many devices connect to the internet, thereby giving attackers a wide field to perform their task. The majority go unnoticed based on how best they are familiar with information technology. To find the objectives on how to deal with cyber-attacks, the reasoning has to appear similar to that of the attacker. The attackers base their objectives and motivation on the surrounding or from personal reasoning. Some of these reasons are founded behind aims and objectives such as; identity theft. attackers focus on people's credit cards by generating identical credit cards with the same social security information. Once the information is obtained, the attacker can steal the victim's identity and access their financial records and accounts, leaving them bankrupt. Second, through espionage.

This instance is where the attackers gain access to the organization's information and later use the precious information for their gain. The secrets extracted from this invasion traded to either competitors or people interested in the detailed data [13]. The attacker can also trick the management into buying back the information, whereby such threats leave the seniority with no option other than to comply. Thirdly, to gain complete control. The attacker's theme is to feel that excitement of being on top of things, and therefore they take complete control of the system with motivates such as espionage or activities such as sabotage. Such malicious act proves that they have the will and power even to explore complex hacks. They are also hacking for fun. The majority of attackers perform the hacks as an enjoyable test, just like in gaming. The above tests their knowledge and skills in their area of specialization. The accomplishment of tasks can act as a motivational factor towards their perfections. The other way that it occurs is through disruption by hacktivists. The theme of hacktivism is to strengthen political movements by exposing government secrets such as corruption, and illegal dealings carried out by the government either directly or indirectly [14]. They appear as the voice of the democrats, and this motivates them to continue with their set missions.

Experienced attackers keep their ethical cover behind the systems by maintaining a digital footprint hidden in the system. To avoid being detected, they tend to get rid of any evidence that one can trace back. This issue is done by; clearing logs of all events. The attacker uses the Metasploit to exploit the network he has created, leading to clearing all events logs. The attacker

can also install a program that will clear any log on the Windows machine after each access as per his commands—further erasing all the command history. The system can detect malware access, and in the event of tracking this malware, the attacker has no time to clear all the event logs. Therefore he is only left with no option other than to shred the command history by deleting all the information in the bash shell through resetting its huge size back to zero—the other use of Internet Control Message Protocol (ICMP). Attackers use the echo from ICMP connections and enclose them with Transmission Control Protocol (TCP) payloads that transfer data. The enclosure prevents the devices used in network security from detecting the attacker's tracks. Reversing the HyperText Transfer Protocol (HTTP) shells. The attackers use the reserved shell to the confidence that it will return commands [18]. The use of reverse command makes it easier and impossible for the firewall to detect any malware, leading to non-detection of attackers' tracks giving safe passage in and out of the system anytime the attacker wants to.

9 SUMMARY

In this paper we looked into how the cyber kill chain is used to prevent and stop cyber-attacks. The job of security professionals is to stop an attack early as possible, but an attack can be disrupted and prevented by being stopped at any point of the chain.

First, the attacker will identify, select and profile the target corporation, individual, or other entity. The focus is set to attack the machines and other computer resources associated with the target. The 2nd phase will come with the weaponization process. Here, the attacker will couple a Trojan horse remotely to exploit a targeted resource or system. As a result, the attacker is promoted to make their cyber weaponization process effective.

The 3rd phase is set on the delivery of the weapon applied to the target. An attacker will find a way to have the attacking tool enter a system through penetration on loopholes left. This transmission and its success are vital goals of the attacker that will enable them to do their malicious intent. Phase 4 includes the exploitation process, where the attacker will trigger a payload on the targeted system. This happens first as the attacker will seek to move to the next step of Installation. Through Installation, the process entirely happens a backdoor to maintain a high level of persistence in the target to achieve the set attacker's objectives. The next step involves a command and control process where the attacker's controller server will communicate with the target systems. Hence, this empowers them to manipulate it. Finally, the attacker will have reasonable control of the resource leading to action that targets to attain the main objective of the attack. Some of the objectives can include network spreading, data theft, eavesdropping on sensitive information, and system disruption [29].
With remote Installation, the attacker will have to use online-based methods, including sending malicious emails and web content that tracks the installation process hidden in other prompts. The physical installation will come with the application of the USB devices.

, ,

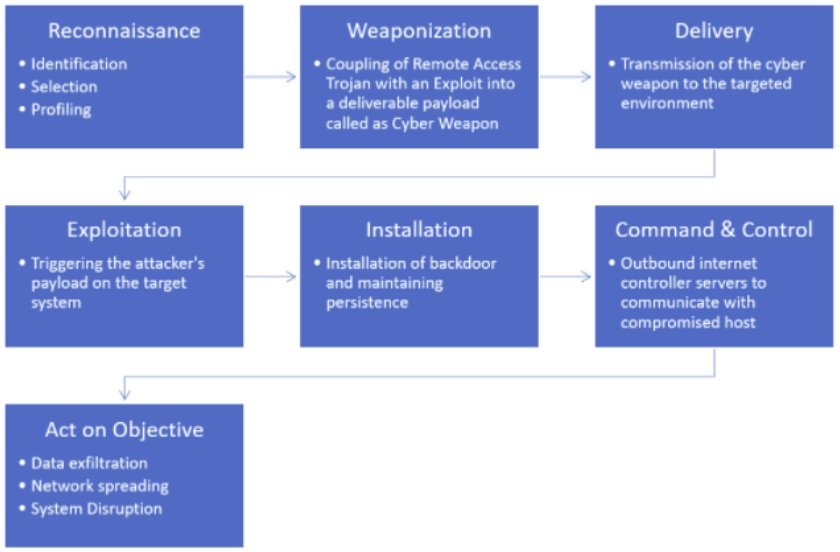

Fig. 7. The Cyber Kill Chain

10 CONCLUSION AND FUTURE SCOPE

The cyber kill chain is widely used within network and cyber-security, it is used as a practice. The kill chain is an effective way to stop a cyber attack at any stage, the chains are crucial steps for and should be secured. The cyber kill chain revolutionized the entire cyber-security industry for dealing with modern attacks, but most companies face threats within the organization. The cyber kill chain does not consider insider threats. If an attacker has access to privileged accounts, then they can move to other systems. They will gain access to more important accounts. Thus, they can steal more important data.

The cyber kill chain does have a flaw, it assumes a traditional perimeter defense, including firewall as the main impediment to intruders. The kill chain does not consider other attack vectors that do not operate by the traditional workflow. Today's threats are more sophisticated and versatile than the traditional model is not sufficient anymore. With more sophisticated attacks adversaries could skip some of these phases and only 2 phases are necessary for an attacker to infiltrate a system, step 1 and step 7. The kill chain is still valuable and are used as a framework in today's security systems and helps to prioritize threats and where to focus time on.

The paper gave an in-depth overview of each step within the cyber kill chain, a possible future scope of the paper is to go more in-depth, and research algorithms used for detection and prevention of threats, and also find techniques related to Machine learning which is a hot topic nowadays. Machine learning could be used with detection and prevention to learn about new threats and automatically prevent them.

REFERENCES

[1] Hussain Aldawood and Geoffrey Skinner. 2019. Reviewing cyber security social engineering training and awareness programs—Pitfalls and ongoing issues. *Future Internet* 11, 3 (2019), 73.

[2] Sebastian Anthony. 2020. Rakshasa: The hardware backdoor that China could embed in every computer. https://www.extremetech.com/computing/133773-rakshasa-the-hardware-backdoor-that-china-could-embed-in-every-computer

[3] Meghna Chhabra, Brij Gupta, and Ammar Almomani. 2013. A novel solution to handle DDOS attack in MANET. (2013).

[4] Miguel Sampaio da Veiga. 2019. OSINT Framework. https://medium.com/hacker-toolbelt/osint-framework-13eca3040a88

[5] Darren Deathy. 2018. The Cyber Kill Chain Explained. https://www.forbes.com/sites/forbestechcouncil/2018/10/05/the-cyber-kill-chain-explained/

[6] Tony Degonia. 2020. Cyber Kill Chain model and framework explained. https://cybersecurity.att.com/blogs/security-essentials/the-internal-cyber-kill-chain-model

[7] Wenjun Fan, Zhihui Du, David Fernández, and Víctor A Villagrá. 2017. Enabling an anatomic view to investigate honeypot systems: A survey. *IEEE Systems Journal* 12, 4 (2017), 3906–3919.

[8] Nick Galov. 2021. 40 Worrisome Hacking Statistics that Concern Us All in 2020. https://hostingtribunal.com/blog/hacking-statistics/

[9] Faisal Ali Garba. 2019. The anatomy of a cyber attack: dissecting the cyber kill chain (ckc). *Scientific and Practical Cyber Security Journal* 3, 1 (2019).

[10] Lucy Hamilton. 2014. Gaining The Advantage. *GeoInformatics* 17, 1 (2014), 14.

[11] Kevin Hjelmtveit. 2020. Overview of DoS and DDoS Attacks. *IMT4113 Introduction to Cyber and Information Security Technology* (2020).

[12] Eric M Hutchins, Michael J Cloppert, Rohan M Amin, et al. 2011. Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains. *Leading Issues in Information Warfare & Security Research* 1, 1 (2011), 80.

[13] Emilio Iasiello. 2016. China's Three Warfares strategy mitigates fallout from cyber espionage activities. *Journal of Strategic Security* 9, 2 (2016), 45–69.

[14] Vasileios Karagiannopoulos and Vasileios Karagiannopoulos. 2018. *Living with hacktivism*. Springer.

[15] lockheed martin. [n.d.]. the Cyber Kill Chain. https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

[16] Tasnuva Mahjabin, Yang Xiao, Guang Sun, and Wangdong Jiang. 2007. A survey of distributed denial-of-service attack, prevention, and mitigation techniques. *International Journal of Distributed Sensor Networks* 13, 12 (Jan. 2007), 1550147717741463. https://doi.org/10.1145/1188913.1188915

[17] Lockheed Martin. 2015. Gaining the advantage: applying cyber kill chain methodology to network defense. *Lockheed Martin Corporation* (2015).

[18] John Narayan, Sandeep K Shukla, and T Charles Clancy. 2015. A survey of automatic protocol reverse engineering tools. *ACM Computing Surveys (CSUR)* 48, 3 (2015), 1–26.

[19] OWASP. 2020. OWASP Top Ten. https://owasp.org/www-project-top-ten/

[20] Ian Perera, Jena Hwang, Kevin Bayas, Bonnie Dorr, and Yorick Wilks. 2018. Cyberattack prediction through public text analysis and mini-theories. In *2018 IEEE International Conference on Big Data (Big Data)*. IEEE, 3001–3010.

[21] Fatima Salahdine and Naima Kaabouch. 2019. Social engineering attacks: a survey. *Future Internet* 11, 4 (2019), 89.

[22] Omar Santos and Ron Taylor. 2018. *CompTIA PenTest+ PT0-001 Cert Guide*. Pearson IT Certification.

[23] Mujahid Shah, Sheeraz Ahmed, Khalid Saeed, Muhammad Junaid, Hamayun Khan, et al. 2019. Penetration testing active reconnaissance phase–optimized port scanning with nmap tool. In *2019 2nd International Conference on Computing, Mathematics and Engineering Technologies (iCoMET)*. IEEE, 1–6.

[24] shivays abharwal. 2020. Cyber Security – Attacking through Command and Control. https://www.geeksforgeeks.org/cyber-security-attacking-through-command-and-control/

[25] William Stallings, Lawrie Brown, Michael D Bauer, and Arup Kumar Bhattacharjee. 2012. *Computer security: principles and practice*. Pearson Education Upper Saddle River, NJ, USA.

[26] Ireneusz Tarnowski. 2017. How to use cyber kill chain model to build cybersecurity? *European Journal of Higher Education IT* (2017).

[27] Adam Waksman and Simha Sethumadhavan. 2010. Tamper evident microprocessors. In *2010 IEEE Symposium on Security and Privacy*. IEEE, 173–188.

[28] Herb Weisbaum. 2019. You've been breached: Hackers stole nearly half a billion personal records in 2018. https://www.nbcnews.com/business/consumer/you-ve-been-breached-hackers-stole-nearly-half-billion-personal-n966496

[29] Tarun Yadav and Arvind Mallari Rao. 2015. Technical aspects of cyber kill chain. In *International Symposium on Security in Computing and Communication*. Springer, 438–452.

[30] Siti Nur Hidayah Zulkiffli, Md Nabil Ahmad Zawawi, and Fiza Abdul Rahim. 2020. Passive and Active Reconnaissance: A Social Engineering Case Study. In *2020 8th International Conference on Information Technology and Multimedia (ICIMU)*. IEEE, 138–143.