Proceedings of the 2023 International Conference on Machine Learning and Automation
DOI: 10.54254/2755-2721/38/20230549

Navigating the Cyber Kill Chain: A modern approach to pentesting

Letao Zhao

Department of Computing, Hong Kong Polytechnic University, Hong Kong, China, 999077

Letao.zhao@polyu.edu.hk

Abstract. The Cyber Kill Chain is a strategic model that outlines the stages of a cyberattack, from initial reconnaissance to achieving the final objective. This framework is often mirrored in penetration testing (pentest), a legal and authorized simulated attack on a computer system performed to evaluate its security. By understanding the steps in the Cyber Kill Chain, penetration testers can mimic the strategies of malicious attackers, exploring vulnerabilities at each stage of the chain. This approach allows organizations to evaluate their defensive measures across the full spectrum of an attack, identifying weaknesses and enhancing their security protocols accordingly. In essence, the Cyber Kill Chain provides a roadmap for pen-testers to systematically evaluate an organization's cyber defences. The research method of this article involves a systematic analysis of the Cyber Kill Chain model, examining how penetration testers can employ this strategic framework to emulate the tactics of malicious attackers and identify methodology at each stage of the chain.

Keywords: cyber kill chain, pentesting methodologies, ethical hacking.

1. Introduction

In the rapidly evolving digital landscape, cybersecurity has become a paramount concern. The increasing sophistication of cyber threats necessitates robust and dynamic security measures. Central to these measures are ethical hacking and penetration testing. Ethical hacking, often performed by white-hat hackers, involves using hacking techniques to enhance security. These hackers are legally authorized and employ various tools to carry out their tasks, with phishing being a common technique [1]. Penetration testing, often seen as a component of ethical hacking, is a process that evaluates the security of a system. It involves assessing how well a system is protected against network security threats and how it responds to security countermeasures. This process is used to determine the system's susceptibility to network intrusion attacks, such as Denial of Service (DOS) [2]. The integration of ethical hacking and penetration testing forms a comprehensive approach to cybersecurity, providing a robust defence against ever-increasing cyber threats. The importance of penetration testing lies in its ability to identify and address vulnerabilities before they can be exploited by malicious actors. By simulating the tactics of potential attackers, penetration testers can uncover weaknesses and work to strengthen the system's defences. This proactive approach to cybersecurity is crucial in today's digital landscape, where threats are constantly evolving and becoming more sophisticated [3]. To better understand and counter these threats, the Cyber Kill Chain (CKC), alternatively known as the Intrusion

DOI: 10.54254/2755-2721/38/20230549

Kill Chain (IKC), serves as a valuable tool. This conceptual model, proposed by Hutchins and colleagues in 2011, delineates the stages of intrusion. The seven-phase model elucidates the steps that Advanced Persistent Threat (APT) actors undertake to accomplish their goals, providing a roadmap for penetration testers to anticipate and counter potential attacks [4].

2. Reconnaissance

The planning and reconnaissance phase is the initial step in the pen-testing process. This phase involves observing the target's regular operations to gather valuable information, such as the hardware and software in use, and communication patterns. This is often done by hackers who scan and probe networks before launching an attack to gather information about the target [5].

Passive reconnaissance, a non-intrusive form of gathering information, is a critical first step in the penetration testing process. It involves observing systems without directly interacting with them, thereby minimizing the risk of detection. The importance of penetration testing lies in its ability to identify and address vulnerabilities before they can be exploited by malicious actors. By simulating the tactics of potential attackers, penetration testers can uncover weaknesses and work to strengthen the system's defences. This proactive approach to cybersecurity is crucial in today's digital landscape, where threats are constantly evolving and becoming more sophisticated [6].

Active reconnaissance is a critical phase in hacking, where the hacker directly engages with the target's network to discover specific details such as individual hosts, IP addresses, and network services. This approach is sometimes referred to as "rattling the doorknobs." Unlike passive reconnaissance, where information is gathered covertly, active reconnaissance involves direct interaction with the target's system, leading to a higher risk of detection. It is a method that requires careful execution, as it can provide valuable insights into the target's security loopholes but also carries inherent risks [7]. Despite the development of sophisticated encryption methods and secure systems, the human element can often be the weakest link. This vulnerability can manifest in various ways, such as insiders revealing encryption codes, trusted members betraying secret societies, or the loss, theft, or sale of secure keys. Regardless of the complexity and ingenuity of security mechanisms, they can be easily compromised if the individuals using them are not cautious [8].

3. Weaponization

The 'Weaponization' phase in the Cyber Kill Chain is a complex stage that involves crafting malicious code to exploit specific weaknesses in a system. This phase is characterized by concealment, where techniques like encryption or disguising the code are used to bypass security measures. Tools such as backdoors bind shells, and reverse shells are employed to gain remote control over a system. In the context of penetration testing, the Metasploit framework is a vital component, offering an extensive database of exploits and tools to achieve the desired outcomes [9]. Backdoors, also known as 'trapdoors,' are secret ways of accessing a program or online service, sometimes intentionally built into the software for special access [10]. The understanding of these tools and techniques sets the groundwork for the actual attack, requiring both technical expertise and an understanding of human behavior. Reverse shells, for example, establish a connection from the victim machine back to the attacker, while bind shells attach a command prompt to a listening port on the exploited system [11].

4. Delivery

The "Delivery" phase marks a critical juncture in the Cyber Kill Chain, where the attacker transmits the weaponized payload to the intended target. This stage is multifaceted and can be executed through various channels, each with its unique challenges and considerations. From traditional email phishing techniques to more sophisticated methods like drive-by downloads and watering hole attacks, the delivery phase is all about finding the most effective way to reach the victim. Social engineering often plays a key role here, manipulating human behavior to facilitate the delivery of malicious content. The complexity of this phase is further heightened by the emergence of mobile and app-based attacks, as well as the use of Advanced Persistent Threats (APTs) that may involve highly targeted and coordinated

DOI: 10.54254/2755-2721/38/20230549

efforts. Understanding the intricacies of the delivery phase is essential for both attackers aiming to succeed and defenders working to thwart these attempts. It's a dynamic and evolving aspect of cybersecurity that reflects the ongoing cat-and-mouse game between cyber adversaries. Whether it's a massive phishing campaign or a carefully crafted targeted attack, the delivery phase sets the stage for the potential breach, making it a vital area of study and vigilance in the modern cybersecurity landscape.

5. Exploitation

In the Cyber Kill Chain model, the exploitation phase is pivotal, as it's where hackers capitalize on system vulnerabilities to deploy malicious code. Here, attackers exploit system weaknesses, often deploying specially crafted payloads to gain unauthorized access or privileges. A notable vulnerability in this context is SSRF (Server-Side Request Forgery). Luo [12] elucidates that SSRF vulnerabilities emerge when servers, driven by business requirements, fetch data from other services without adequately filtering and restricting the destination address of the access request. This laxity allows attackers to manipulate the server's request mechanism, granting them access to resources such as server files or even intranet assets protected by firewalls. Furthermore, SSRF vulnerabilities can be synergized with other vulnerabilities like RFI (Remote File Inclusion) and XXE (XML External Entity) to facilitate actions like automatic scanning, internal network infiltration, and local file reading. Another prevalent vulnerability is buffer overflow, which Lhee and Chapin [13] categorize as one of the most common security issues. These vulnerabilities can be weaponized to overwrite adjacent data, thereby altering the program's typical behavior. Such vulnerabilities predominantly stem from the C language's characteristics, where arrays are depicted as pointers, challenging compilers to detect potential overflows. Successful exploitation can pave the way for malware installation, solidifying the attacker's presence and ultimately achieving their objectives, such as data exfiltration or system disruption.

Toward the exploitation spectrum's tail end is the brute force attack method. Brute force attacks entail systematically trying all possible combinations to access a system or decrypt data. While they can be effective, they're often relegated to a lower priority in a hacker's methodology for two primary reasons: their time-consuming and resource-intensive nature makes them less efficient than exploiting known vulnerabilities, and the heightened risk of detection due to potential security alerts triggered by repeated failed attempts. Consequently, hackers often prioritize more discreet and efficient attack vectors before considering brute force.

6. Installation

In the 'Installation' stage of the Cyber Kill Chain, attackers meticulously strategize to establish a stronghold within a target system. Recognizing the layered privilege structure inherent in information systems, they exploit vulnerabilities to escalate their privileges, granting them unauthorized access to a broader spectrum of the system's functionalities. Such privilege escalation tactics are a cornerstone of their methodology, allowing them to deploy malicious tools or software and ensure sustained access and control over the compromised system.

However, as Yamauchi et al. [14] highlight, the cybersecurity landscape is evolving with the introduction of advanced defensive mechanisms like the Additional Kernel Observer (AKO). Designed specifically to counteract privilege escalation attacks that exploit operating system vulnerabilities, the AKO operates on the principle that a process privilege can only be altered by specific system calls. By vigilantly monitoring these privilege changes during system call processing, the AKO can swiftly detect and neutralize unauthorized privilege escalations. This presents a significant challenge for attackers, especially when AKO is implemented in systems like Linux x86, and 64-bit, where it has demonstrated its effectiveness in thwarting such attacks with minimal overhead.

Despite these advancements, attackers continue to refine their techniques. They often employ a systematic approach, analysing log messages to identify patterns and outliers indicative of potential privilege escalation avenues. Through this meticulous analysis, they aim to exploit any overlooked vulnerabilities, further deepening their infiltration and compromising the system's security [15].

DOI: 10.54254/2755-2721/38/20230549

7. Command & control (C2)

The C2 stage is a testament to the attacker's progression within the Cyber Kill Chain. No longer merely an external threat, they are now deeply embedded within the system, manipulating it as a puppeteer would a marionette. Given the significance of this stage, it's unsurprising that attackers employ a myriad of sophisticated techniques to ensure their C2 communications remain discreet, robust, and elusive.

The rise of the Internet of Things (IoT) has expanded the potential target pool, intensifying the threat of botnets. These compromised networks can execute a vast array of malicious activities under the direction of the C2 server, which remains shrouded, concealing the true identity of the botmaster.

To bolster their stealth capabilities, attackers have adopted advanced obfuscation techniques. One such method is Tor domain-fronting, which uses the Tor network's encrypted multi-hop communication to disguise C2 traffic. By employing pluggable transport protocols, such as Meek, Tor traffic is transformed, appearing as benign TLS traffic and blending seamlessly with legitimate requests to cloud servers [16].

Further complicating detection efforts is the use of domain generation algorithms (DGAs) by certain botnets. DGAs algorithmically produce a plethora of domain names, serving as potential communication points with their C2 servers. This dynamic generation makes it challenging for defenders to predict and block these domains. DGA-based botnets, in particular, are adept at camouflaging their server queries within regular domain name system (DNS) traffic, making traditional DNS security measures, which often rely on blacklists, less effective [17].

Recognizing the limitations of conventional detection methods, researchers like Suryotrisongko and Musashi have explored innovative solutions. Their study introduces a hybrid quantum-classical deep learning model tailored for DGA-based botnet detection. By integrating quantum computations with classical deep learning algorithms, they've enhanced the model's capability to detect these elusive threats.

8. Actions on objectives

In the realm of cybersecurity, the "actions on objective" stage of the Cyber Kill Chain (CKC) represents the culmination of a cyber attacker's efforts. After successfully navigating the preceding stages, attackers reach their endgame, where they exploit the vulnerabilities, they've identified to achieve their ultimate goals. One of the most prominent manifestations of this stage is the deployment of ransomware attacks. Originating in 1989 with Joseph L. Popp's creation, ransomware has evolved to become a formidable threat. Modern ransomware either encrypts the victim's data, rendering it inaccessible until a ransom is paid or locks out users from their devices entirely. Another recent and increasingly prevalent threat is crypto-jacking. Emerging in 2017, this attack involves unauthorized crypto miners exploiting a user's computing resources to mine cryptocurrency. The insidious nature of crypto-jacking lies in its ability to operate covertly, often without the victim's knowledge. As cyber threats continue to evolve, understanding and addressing the "actions on objective" stage becomes paramount in the fight against cyber adversaries.

9. Future trends

The rapid progression of Artificial Intelligence (AI) has ushered in a new era of cybersecurity. Historically, the Cyber Kill Chain model served as a benchmark for understanding cyber threats. However, with the advent of AI, the landscape of cyber threats and defences has evolved significantly. AI-based technologies, initially developed for cyber defence, are now being weaponized for offensive purposes, ranging from tampering with medical images to influencing the safety of autonomous vehicles. The weaponization of AI, especially in cyberspace, presents new challenges. For instance, the Microsoft bot "Tay" showcased the potential dangers when AI is fed malicious data. As AI continues to integrate into various sectors, including military operations, the need for robust pen-testing methodologies becomes paramount. Future challenges in pen-testing will revolve around ensuring that AI systems are resilient against adversarial attacks, while opportunities lie in harnessing AI's capabilities to enhance cybersecurity measures. As the cyber realm expands, the reliance on AI for efficient system management and security will only grow, emphasizing the importance of continuous research and adaptation in the

DOI: 10.54254/2755-2721/38/20230549

face of evolving threats. The sophistication of cyberattacks, especially those driven by AI, poses significant risks to organizations and infrastructures. AI-driven cyberattacks have the potential to be faster, more unpredictable, and more sophisticated than even the most advanced cybersecurity teams can counter. As AI becomes a more potent tool in the hands of malicious actors, there is an urgent need for inventive solutions to safeguard cyberspace from these emerging threats.

10. Conclusion

The Cyber Kill Chain, a strategic model delineating the stages of a cyberattack, has emerged as an invaluable tool in the realm of cybersecurity. By understanding and mirroring this model, penetration testers can simulate the tactics of malicious actors, systematically uncovering vulnerabilities at each stage of an attack. This comprehensive approach to cybersecurity, encompassing ethical hacking and penetration testing, offers a robust defence against the multifaceted threats of the digital age. From the initial reconnaissance phase to the final actions on objectives, each stage presents unique challenges and opportunities for both attackers and defenders. The rise of AI and machine learning further complicates this landscape, introducing new dimensions of threats and defences. As cyber threats continue to evolve, especially with the weaponization of AI, the importance of understanding the Cyber Kill Chain and employing rigorous pen-testing methodologies cannot be overstated. In this ever-shifting battleground, continuous research, adaptation, and vigilance are paramount. Only by staying ahead of the curve can organizations hope to safeguard their digital assets and ensure a secure future in an increasingly interconnected world.

References

[1] Patil, S., Jangra, A., Bhale, M., Raina, A., & Kulkarni, P. (2017). Ethical Hacking: The Need for Cyber Security. In IEEE International Conference on Power, Control, Signals and Instrumentation Engineering (ICPCSI-2017). IEEE.

[2] Vats, P., Mandot, M., & Gosain, A. (2020). A Comprehensive Literature Review of Penetration Testing & Its Applications. 2020 8th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO).

[3] Bishop, M. (2023). Penetration Testing. In 2023 IEEE Symposium on Security and Privacy (SP). IEEE.

[4] Garba, F. A., Junaidu, S. B., Ahmad, B. I., & Tekanyi, A. M. S. (2023). Proposed Framework for Effective Detection and Prediction of Advanced Persistent Threats Based on the Cyber Kill Chain. Scientific and Practical Cyber Security Journal (SPCSJ), 3(3), 1-11.

[5] Sanghvi, H. P., & Dahiya, M. S. (2013). Cyber Reconnaissance: An Alarm Before Cyber Attack. International Journal of Computer Applications, 63(6), 1-4.

[6] Barrett, N. (2003). Penetration testing and social engineering: hacking the weakest link. Information Security Technical Report, 8(4), 56-64.

[7] International Journal of Computer Science Trends and Technology (IJCST). (2014). Study Of Ethical Hacking. Volume (Issue), page range.

[8] Y. Kolli, T. K. Mohd and A. Y. Javaid, "Remote Desktop Backdoor Implementation with Reverse TCP Payload using Open Source Tools for Instructional Use," 2018 IEEE 9th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON), Vancouver, BC, Canada, 2018, pp. 444-450, doi: 10.1109/IEMCON.2018.8614801.

[9] Information Security Technical Report. (2001). Backdoors and Trojan Horses. Information Security Technical Report, Vol. 6, No. 4, pp. 1-31.

[10] Luo, H. (2019). SSRF vulnerability Attack and Prevention based on PHP. 2019 International Conference on Communications, Information System and Computer Engineering (CISCE). DOI 10.1109/CISCE.2019.00109

[11] Lhee, K.-S., & Chapin, S. J. (2003). Buffer overflow and format string overflow vulnerabilities. Software—Practice and Experience, 33, 423-460.

DOI: 10.54254/2755-2721/38/20230549

[12] F. Jaafar, G. Nicolescu and C. Richard, "A Systematic Approach for Privilege Escalation Prevention," 2016 IEEE International Conference on Software Quality, Reliability and Security Companion (QRS-C), Vienna, Austria, 2016, pp. 101-108, doi: 10.1109/QRS-C.2016.17.

[13] T. Yamauchi, Y. Akao, R. Yoshitani, Y. Nakamura and M. Hashimoto, "Additional Kernel Observer to Prevent Privilege Escalation Attacks by Focusing on System Call Privilege Changes," 2018 IEEE Conference on Dependable and Secure Computing (DSC), Kaohsiung, Taiwan, 2018, pp. 1-8, doi: 10.1109/DESEC.2018.8625137.

[14] Suryotrisongko, H., & Musashi, Y. (2022). Evaluating hybrid quantum-classical deep learning for cybersecurity botnet DGA detection. Procedia Computer Science, 197, 223-229.

[15] Z. Li, M. Wang, X. Wang, J. Shi, K. Zou and M. Su, "Identification Domain Fronting Traffic for Revealing Obfuscated C2 Communications," 2021 IEEE Sixth International Conference on Data Science in Cyberspace (DSC), Shenzhen, China, 2021, pp. 91-98, doi: 10.1109/DSC53577.2021.00020.

[16] Yamin, M. M., Ullah, M., Ullah, H., & Katt, B. (2021). Weaponized AI for cyber attacks. Journal of Information Security and Applications, 57, 102722.

[17] Guembe, B., Azeta, A., Misra, S., Osamor, V. C., Fernandez-Sanz, L., & Pospelova, V. (2022). The Emerging Threat of Ai-driven Cyber Attacks: A Review. Applied Artificial Intelligence, 36(1), 2037254.