Phases of Cyber Operation

Ryan Coon

CYB-610

Professor Ian Standefer

March 19, 2025

**Target Identification** – This is the initial phase that involves defining the target of the operation. The target could be an organization, a particular system, or even an individual. The overall goal in the target identification stage is to gather preliminary intelligence about the target, including its structure, key personnel, and potential vulnerabilities(Simpson, 2023). In turn the attacker can use this information to tailor the subsequent phases to the target’s specific content. An example would be that an attacker may target a financial institution for financial gain, while a nation-state actor may target a government agency for espionage.

**Reconnaissance** – This phase involves extensive research to gather as much information about the target as possible. This includes open-source intelligence (OSINT), where publicly available information is collected via online, social media, and other sources(Team, 2023). Techniques such as social engineering might also come into play to gather information from unsuspecting individuals. Another crucial tool is network scanning, which is used to identify open ports, running services, and any potential entry points into the target’s network. The key objective is to identify any vulnerabilities that can be exploited later on in the operation.

**Gaining Access** – In this phase, the focus is exploiting the vulnerabilities that were discovered during the reconnaissance phase to gain unauthorized access into the target’s system. Techniques in this phase include phishing, where malicious emails or fictitious websites are used to trick users into revealing sensitive information or even into downloading malware(Richardson, 2025). Another common methos is exploiting the software’s vulnerabilities, such as unpatched flaws in the software’s applications. Stolen credentials obtained through phishing or other means can also be used to gain access. The goal in this phase is to establish an initial foothold within the targets environment to allow further action from the attacker.

**Hiding Presence** – Once access is gained, it is crucial for the attacker to hide their presence in order to maintain control over the compromised systems without being detected. This would involve the attacker to delete logs, modify system files, and employ other stealthy techniques to cover their tracks(Phases of a Cyber Attack, n.d.). Rootkits, which are programs designed to hide malicious activities from system administrators, are often used in this step. The objective in this phase is to ensure that any actions that are taken do not alert the target to the breach, allowing the attacker to operate undetected for an extended period of time.

**Establishing persistence** – This phase involves implementing the methods in order to maintain access to the target’s systems even if the initial access points are discovered and closed. Techniques used include installing backdoors or hidden programs that allow the attacker to regain access without the need to exploit vulnerabilities again(NSIT, n.d.). Another way attackers can establish persistence is to create new user accounts with elevated privileges. The goal of this phase is to ensure that the attacker can continue to regain access after system reboots, updates, or changes in the targets security posture, therefore maintaining a continuous presence within the target environment.

**Execution** – This is the phase in which the attacker executes their primary objectives, which can range from system disruption, data exfiltration, or espionage. The specific goals depend on the attacker’s initial intent of the operation(Lockheed Martin, 2024). An example would be that a ransomware attacker might encrypt sensitive data and demand payment for its release, while a nation-state actor might steal the intellectual property or disrupt critical infrastructure. The objective of this phase is to achieve the desired outcome all the while minimizing the risk of detection.

**Assessment** – After the execution of the operation, it is essential to assess the effectiveness of the attack. This would involve analyzing whether the objectives were met and what systems or data was compromised. The attacker may also gather insights from the operation to improve upon future tactics and strategies. The objective of this phase is to learn from the operation and adapt future attacks to be more effective.

References:

Lockheed Martin. (2024). *Cyber Kill Chain*. Lockheed Martin. https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

*NIST Cybersecurity Framework: Five Essential Phases*. (n.d.). Sopa.tulane.edu. https://sopa.tulane.edu/blog/NIST-cybersecurity-framework

Richardson, A. (2025). *Recognizing the seven stages of a cyber-attack*. DNV. https://www.dnv.com/cyber/insights/articles/recognizing-the-seven-stages-of-a-cyber-attack/

*SI110: Phases of a Cyber-attack / Cyber-recon*. (n.d.). Www.usna.edu. https://www.usna.edu/Users/cs/wcbrown/courses/si110AY13S/lec/l32/lec.html

Simpson, M. T., & Antill, N. (2017). *Hands-on ethical hacking and network defense*. Cengage Learning.

Team, T. G. (2023, February 21). *Cyber Security: Understanding the 5 Phases of Intrusion*. Graylog. https://graylog.org/post/cyber-security-understanding-the-5-phases-of-intrusion/