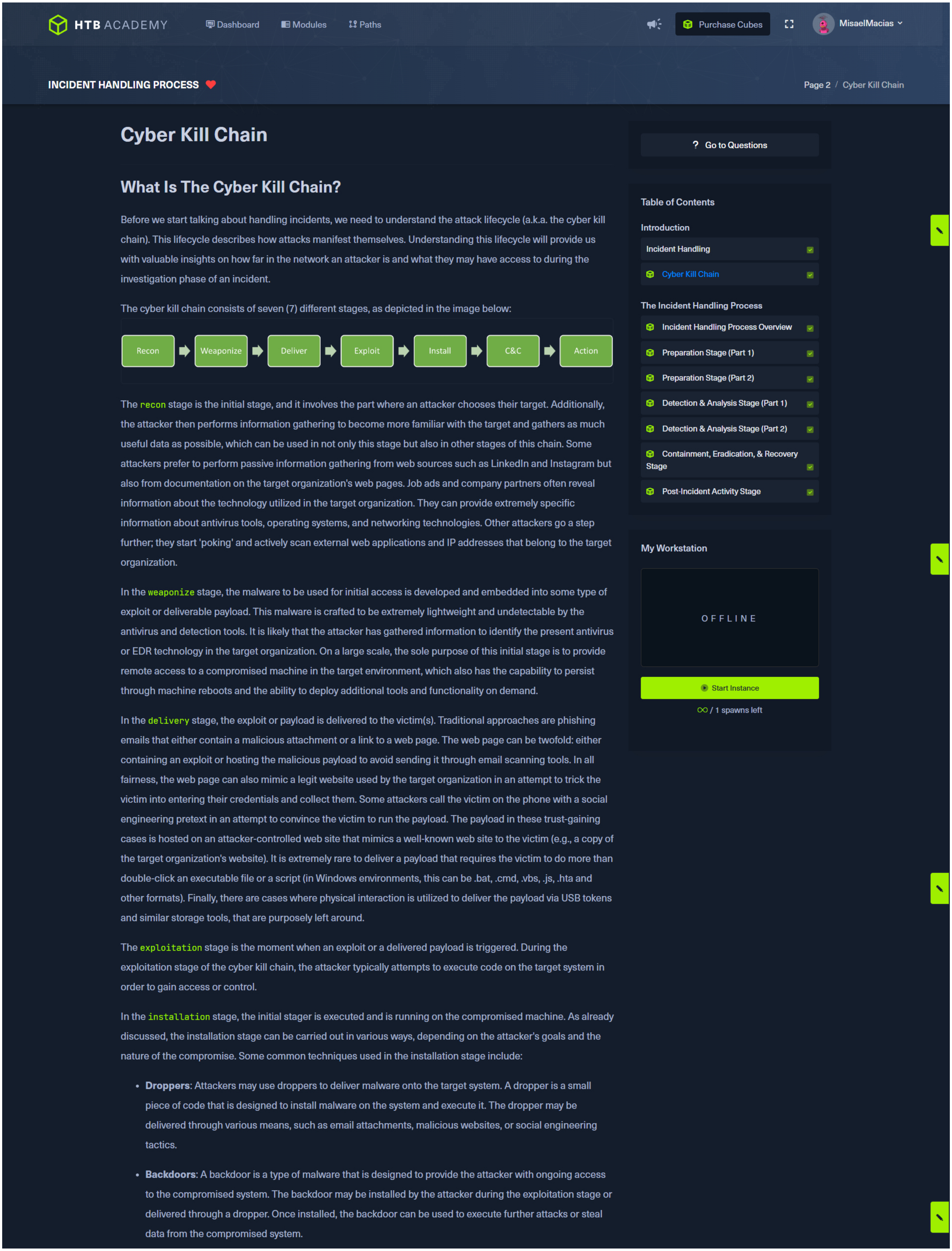


Cyber Kill Chain

What Is The Cyber Kill Chain?

Before we start talking about handling incidents, we need to understand the attack lifecycle (a.k.a. the cyber kill chain). This lifecycle describes how attacks manifest themselves. Understanding this lifecycle will provide us with valuable insights on how far in the network an attacker is and what they may have access to during the investigation phase of an incident.

The cyber kill chain consists of seven (7) different stages, as depicted in the image below:

Recon ➡ Weaponize ➡ Deliver ➡ Exploit ➡ Install ➡ C&C ➡ Action

The `recon` stage is the initial stage, and it involves the part where an attacker chooses their target. Additionally, the attacker then performs information gathering to become more familiar with the target and gathers as much useful data as possible, which can be used in not only this stage but also in other stages of this chain. Some attackers prefer to perform passive information gathering from web sources such as LinkedIn and Instagram but also from documentation on the target organization's web pages. Job ads and company partners often reveal information about the technology utilized in the target organization. They can provide extremely specific information about antivirus tools, operating systems, and networking technologies. Other attackers go a step further; they start 'poking' and actively scan external web applications and IP addresses that belong to the target organization.

In the `weaponize` stage, the malware to be used for initial access is developed and embedded into some type of exploit or deliverable payload. This malware is crafted to be extremely lightweight and undetectable by the antivirus and detection tools. It is likely that the attacker has gathered information to identify the present antivirus or EDR technology in the target organization. On a large scale, the sole purpose of this initial stage is to provide remote access to a compromised machine in the target environment, which also has the capability to persist through machine reboots and the ability to deploy additional tools and functionality on demand.

In the `delivery` stage, the exploit or payload is delivered to the victim(s). Traditional approaches are phishing emails that either contain a malicious attachment or a link to a web page. The web page can be twofold: either containing an exploit or hosting the malicious payload to avoid sending it through email scanning tools. In all fairness, the web page can also mimic a legit website used by the target organization in an attempt to trick the victim into entering their credentials and collect them. Some attackers call the victim on the phone with a social engineering pretext in an attempt to convince the victim to run the payload. The payload in these trust-gaining cases is hosted on an attacker-controlled web site that mimics a well-known web site to the victim (e.g., a copy of the target organization's website). It is extremely rare to deliver a payload that requires the victim to do more than double-click an executable file or a script (in Windows environments, this can be .bat, .cmd, .vbs, .js, .hta and other formats). Finally, there are cases where physical interaction is utilized to deliver the payload via USB tokens and similar storage tools, that are purposely left around.

The `exploitation` stage is the moment when an exploit or a delivered payload is triggered. During the exploitation stage of the cyber kill chain, the attacker typically attempts to execute code on the target system in order to gain access or control.

In the `installation` stage, the initial stager is executed and is running on the compromised machine. As already discussed, the installation stage can be carried out in various ways, depending on the attacker's goals and the nature of the compromise. Some common techniques used in the installation stage include:

- **Droppers**: Attackers may use droppers to deliver malware onto the target system. A dropper is a small piece of code that is designed to install malware on the system and execute it. The dropper may be delivered through various means, such as email attachments, malicious websites, or social engineering tactics.
- **Backdoors**: A backdoor is a type of malware that is designed to provide the attacker with ongoing access to the compromised system. The backdoor may be installed by the attacker during the exploitation stage or delivered through a dropper. Once installed, the backdoor can be used to execute further attacks or steal data from the compromised system.

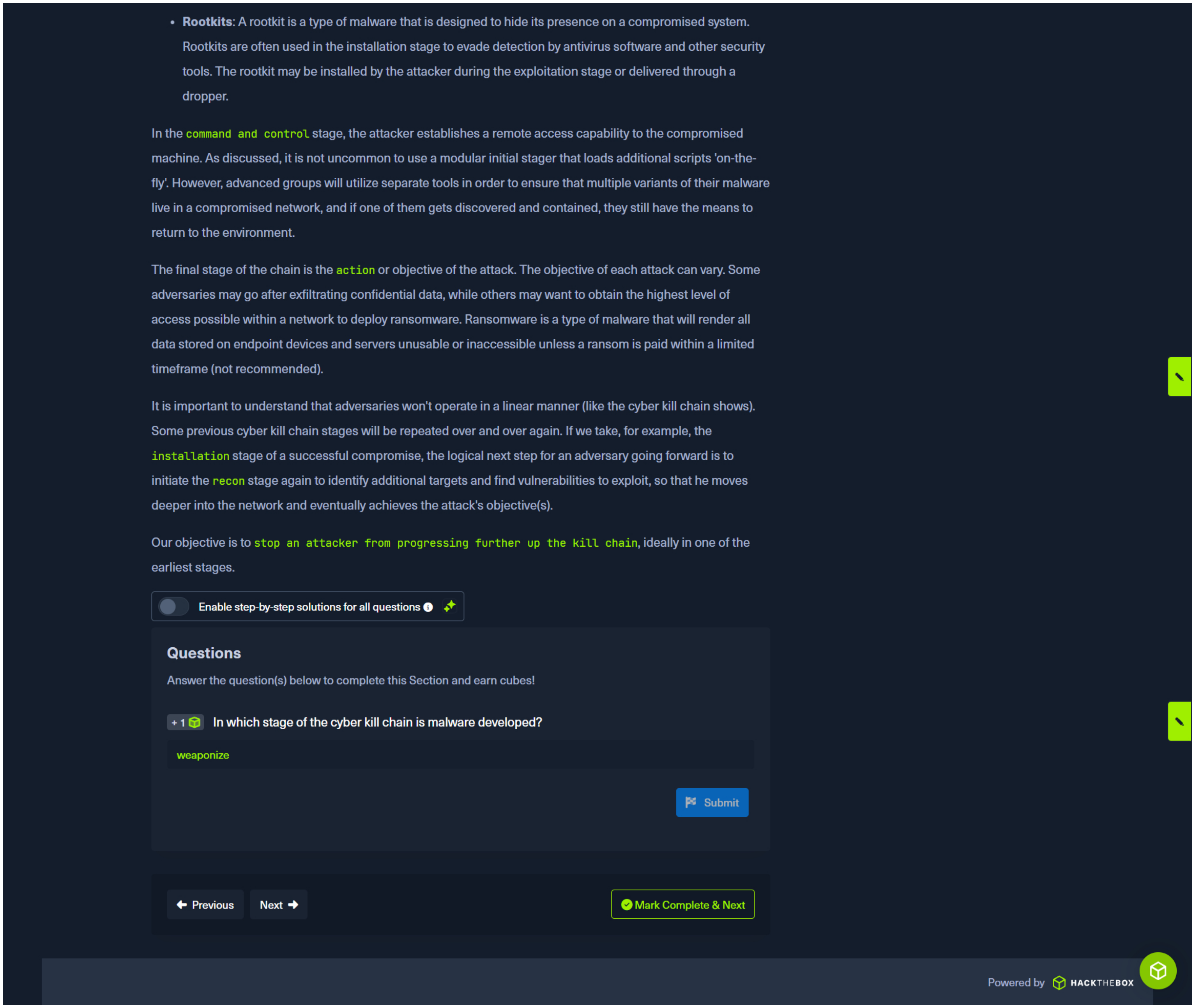
Table of Contents

Introduction

The Incident Handling Process

My Workstation

OFFLINE



- **Rootkits**: A rootkit is a type of malware that is designed to hide its presence on a compromised system. Rootkits are often used in the installation stage to evade detection by antivirus software and other security tools. The rootkit may be installed by the attacker during the exploitation stage or delivered through a dropper.

In the `command and control` stage, the attacker establishes a remote access capability to the compromised machine. As discussed, it is not uncommon to use a modular initial stager that loads additional scripts 'on-the-fly'. However, advanced groups will utilize separate tools in order to ensure that multiple variants of their malware live in a compromised network, and if one of them gets discovered and contained, they still have the means to return to the environment.

The final stage of the chain is the `action` or objective of the attack. The objective of each attack can vary. Some adversaries may go after exfiltrating confidential data, while others may want to obtain the highest level of access possible within a network to deploy ransomware. Ransomware is a type of malware that will render all data stored on endpoint devices and servers unusable or inaccessible unless a ransom is paid within a limited timeframe (not recommended).

It is important to understand that adversaries won't operate in a linear manner (like the cyber kill chain shows). Some previous cyber kill chain stages will be repeated over and over again. If we take, for example, the `installation` stage of a successful compromise, the logical next step for an adversary going forward is to initiate the `recon` stage again to identify additional targets and find vulnerabilities to exploit, so that he moves deeper into the network and eventually achieves the attack's objective(s).

Our objective is to `stop an attacker from progressing further up the kill chain`, ideally in one of the earliest stages.

Questions

Answer the question(s) below to complete this Section and earn cubes!

+1 In which stage of the cyber kill chain is malware developed?

weaponize