# Contents

This page is purposely empty.

## Disclaimer

This was developed and organized with the help of Claude.ai.
By referencing the write-up that I made after completing a course, Claude.ai is used to extract information and create questions alongside their answers.

If anyone reading this document finds any mistakes or inconsistencies in the questions and answers, please let me know at mikhailamzarkamaruddin@gmail.com.

If you're using this document for the purpose of studying, I recommend reading the write-up that it is based upon first to gain more insights and context. Since this document is developed with the help of Claude.ai. It might miss some important context and details from the original write-up, the write-ups may include images as well that Claude.ai could not read.

For more write-ups or documentation check out my repo at:
https://github.com/MikhailAmzar/reports

## Questions & answers: Cyber Defense Framework (30)

**What is the Pyramid of Pain?**
The Pyramid of Pain is a conceptual framework that illustrates the varying levels of difficulty and cost an adversary would encounter to evade detection and continue their attack, in the context of cybersecurity defenses.

**What is the purpose of the Pyramid of Pain framework?**
The purpose of the Pyramid of Pain framework is to enable security experts, predominantly blue teamers, to channel their resources on elements inducing the most pain to adversaries to alter.

**Why are hash values considered trivial in the Pyramid of Pain?**
Hash values are considered trivial in the Pyramid of Pain because even a single bit change in a malicious file will change the end hash value, making it easy for an attacker to evade detection based on file hashes.

**What is an IP address?**
An IP address is a logical address used to identify devices on a network.

**Why are IP addresses considered "easy" in the Pyramid of Pain?**
IP addresses are considered "easy" in the Pyramid of Pain because it is trivial for an experienced adversary to recover simply by using a new public IP address.

**What is Fast Flux, and how can it make IP blocking challenging?**
Fast Flux is a DNS technique used by botnets to hide phishing, web proxying, malware delivery, and malware communication activities behind compromised hosts acting as proxies. It can make IP blocking challenging by constantly changing the IP addresses associated with a domain.

**Why are domain names considered "simple" in the Pyramid of Pain?**
Domain names are considered "simple" in the Pyramid of Pain because, while more difficult for an attacker to change than an IP address, many DNS providers have loose standards and provide APIs to make it easier for the attacker to change the domain.

**What are some methods attackers can use to manipulate the display of domain/URLs?**
Some methods attackers can use to manipulate the display of domain/URLs include Punycode (converting characters into another) and hiding malicious URLs using URL shortener services.

**What are host artifacts?**
Host artifacts are the traces or observables that attackers leave on the system, such as registry values, suspicious process execution, attack patterns or IOCs (Indicators of Compromise), files dropped by malicious applications, or anything exclusive to the current threat.

**Why are host artifacts considered "annoying" in the Pyramid of Pain?**
Host artifacts are considered "annoying" in the Pyramid of Pain because the attacker would need to circle back at this detection level and change their attack tools and methodologies, which is very time-consuming and resource-intensive.

**What are some examples of network artifacts?**
Examples of network artifacts include user-agent strings, C2 information, URI patterns, and HTTP POST requests.

**Why are tools considered "challenging" in the Pyramid of Pain?**
Tools are considered "challenging" in the Pyramid of Pain because, at this stage, the attacker would most likely give up trying to break into the network or go back and try to create a new tool, which would require significant investment and effort.

**What are some examples of tools that attackers might use?**
Examples of tools that attackers might use include malicious macro documents (maldocs) for spearphishing attempts, backdoors to establish Command and Control (C2) infrastructure, custom .EXE and .DLL files, payloads, or password crackers.

**Why are TTPs (Tactics, Techniques, Procedures) considered "tough" in the Pyramid of Pain?**
TTPs (Tactics, Techniques, Procedures) are considered "tough" in the Pyramid of Pain because if you can detect a specific attack and know the techniques, it should be easy to remediate swiftly, forcing the attacker to either give up or invest significant time and resources to change their approach.

**What is the purpose of the Cyber Kill Chain framework?**
The purpose of the Cyber Kill Chain framework is to enable the identification and prevention of network intrusions by understanding the steps adversaries need to take to achieve their goals.

**What is the reconnaissance phase in the Cyber Kill Chain?**
The reconnaissance phase in the Cyber Kill Chain is the planning phase where the attacker discovers and collects information on the system and the victim.

**What is the weaponization phase in the Cyber Kill Chain?**
The weaponization phase in the Cyber Kill Chain is where the attacker creates their malicious payload, sets up their C2 techniques, etc.

**What is the delivery phase in the Cyber Kill Chain?**
The delivery phase in the Cyber Kill Chain is where the attacker decides the method for transmitting their payload, such as phishing emails, malicious USB distribution, watering hole attacks, or drive-by attacks.

**What is the exploitation phase in the Cyber Kill Chain?**
The exploitation phase in the Cyber Kill Chain is where the attacker carries out their exploit, either by the victim triggering it (e.g., opening a malicious attachment or link) or exploiting vulnerabilities in software, hardware, or human factors.

**What is the installation phase in the Cyber Kill Chain?**
The installation phase in the Cyber Kill Chain is where the attacker might install something on the compromised system to maintain persistence, such as a web shell, backdoor, or modifying Windows services.

**What is the Command & Control (C2) phase in the Cyber Kill Chain?**
The Command & Control (C2) phase in the Cyber Kill Chain is where the attacker opens up their C2 channel to remotely control and manipulate the victim, often using common channels like HTTP/HTTPS, DNS, or infected machines making DNS requests.

**What is the exfiltration (Actions on Objectives) phase in the Cyber Kill Chain?**
The exfiltration (Actions on Objectives) phase in the Cyber Kill Chain is where the attacker acts on their ultimate objective, such as collecting credentials, performing privilege escalation, lateral movement, exfiltrating sensitive data, deleting backups, or corrupting data.

**What is the purpose of the Unified Kill Chain framework?**
The purpose of the Unified Kill Chain framework is to provide a detailed understanding of the steps an attacker takes during an intrusion, from initial reconnaissance to achieving their objectives, to enable defenders to implement appropriate security measures.

**What are the three main phases of the Unified Kill Chain?**
The three main phases of the Unified Kill Chain are Phase In (Initial Foothold), Phase Through (Network Propagation), and Phase Out (Action on Objectives).

**What is the main focus of the "Phase In" stage in the Unified Kill Chain?**
The main focus of the "Phase In" stage in the Unified Kill Chain is for an attacker to gain access to a system or networked environment and establish persistence.

**What is the main focus of the "Phase Through" stage in the Unified Kill Chain?**
The main focus of the "Phase Through" stage in the Unified Kill Chain is for the attacker to gain additional access and privileges to systems and data to fulfill their goals, setting up a base for pivoting and gathering information about the internal network.

**What is the main focus of the "Phase Out" stage in the Unified Kill Chain?**
The main focus of the "Phase Out" stage in the Unified Kill Chain is for the attacker to gain access to critical assets and fulfill their attack goals, typically related to compromising the confidentiality, integrity, and availability (CIA) triad.

**What is the purpose of the Diamond Model of Intrusion Analysis?**
The purpose of the Diamond Model of Intrusion Analysis is to help identify the elements of an intrusion, including the adversary, victim, capabilities, and infrastructure involved.

**What is the MITRE ATT&CK framework?**
The MITRE ATT&CK framework is a globally accessible knowledge base of adversary tactics and techniques based on real-world observations.

**What is the purpose of the MITRE Engage framework?**
The purpose of the MITRE Engage framework is to provide a framework for planning and discussing adversary engagement operations that empower organizations to engage their adversaries and achieve their cybersecurity goals through cyber denial and cyber deception strategies.