BILLY GIBENDI
ADC-SOA01-24014
Microsoft ADC Cybersecurity Skilling Program

WEEK 5 ASSIGNMENT

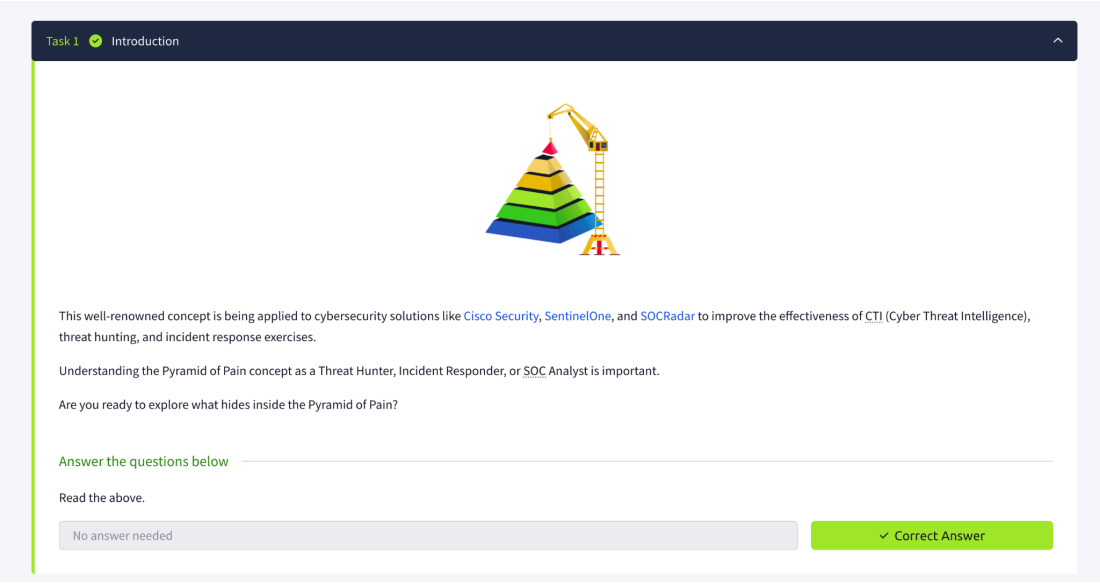
Pyramid Of Pain

Introduction

Understanding the intricacies of cyber threat intelligence is paramount to our success in the field. The "Pyramid of Pain" room on TryHackMe provides an invaluable framework for assessing the difficulty an adversary will face when attempting to alter their indicators of compromise (IOCs). Developed by David J. Bianco, the Pyramid of Pain categorizes different types of IOCs based on the level of pain they inflict on adversaries when changed. This structured approach helps cybersecurity professionals gauge the effectiveness of their defensive measures and refine their threat hunting strategies.

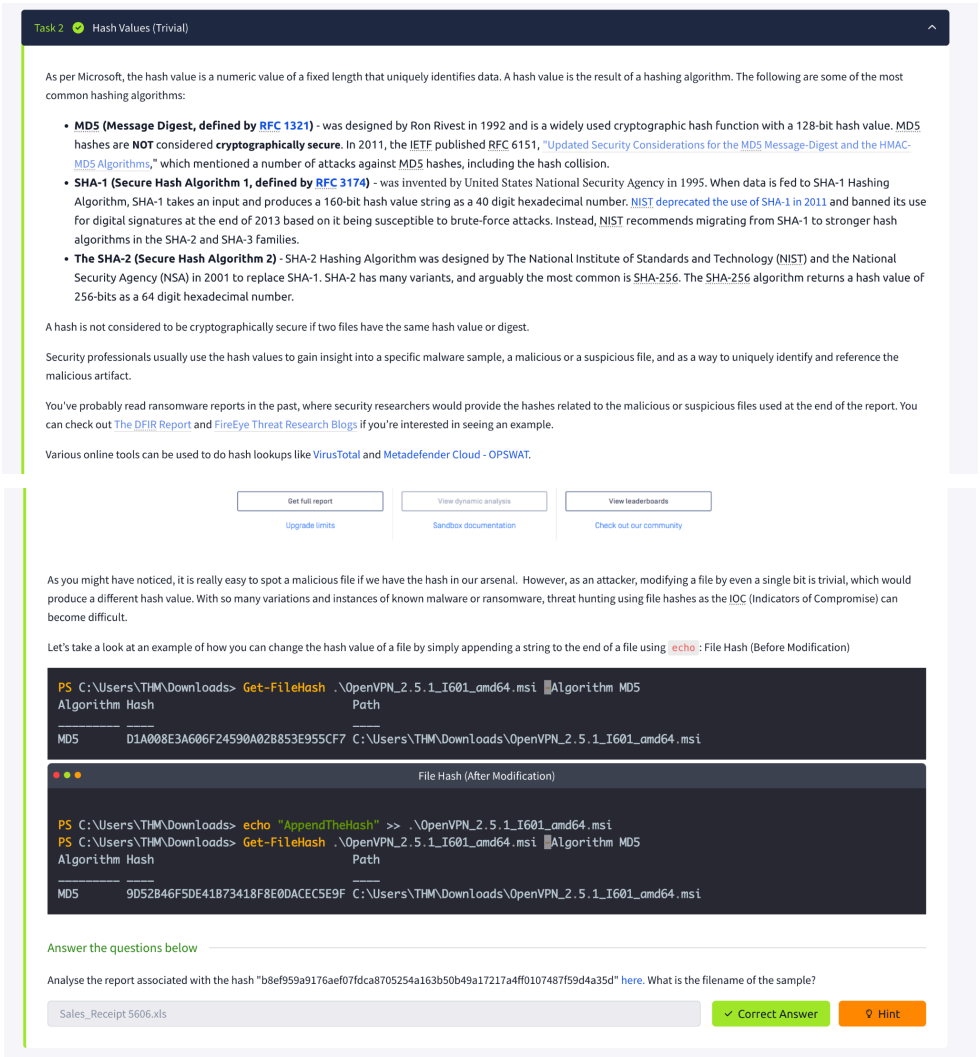
Task 1: Introduction

The introduction section sets the stage for the Pyramid of Pain by explaining its purpose and significance. It outlines how different types of indicators can impact an adversary's operations and highlights the importance of using this model to prioritize threat hunting and mitigation efforts. The Pyramid of Pain is divided into seven levels, each representing a different type of IOC, ranging from hash values to Tactics, Techniques, and Procedures (TTPs).



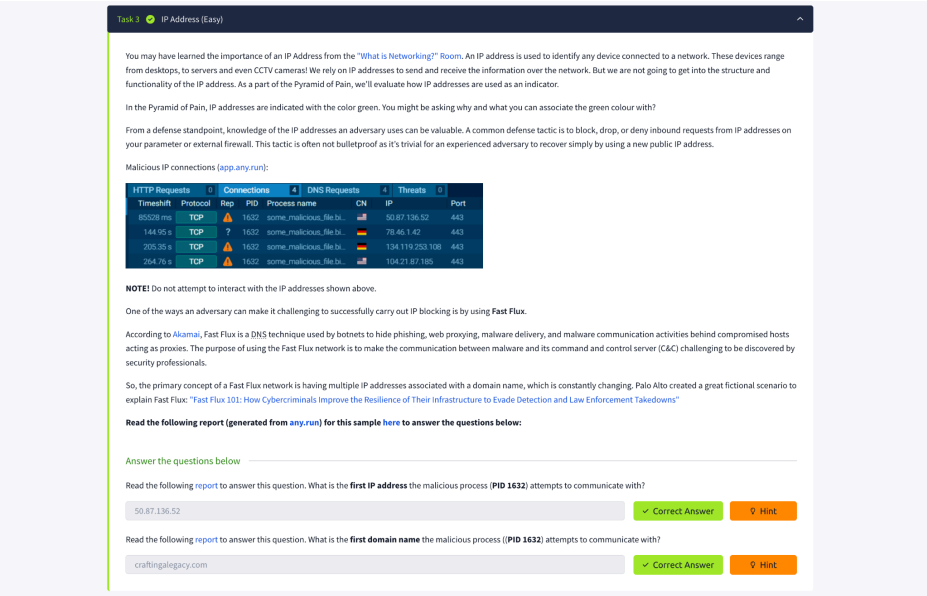
Task 2: Hash Values (Trivial)

Hash values, such as MD5, SHA-1, or SHA-256, are at the base of the pyramid and are considered trivial for adversaries to change. These cryptographic hashes are unique to specific files or data, but modifying the file slightly will generate a new hash, rendering this type of IOC easily circumvented. Despite being trivial to change, hash values are still useful for quickly identifying known malicious files.



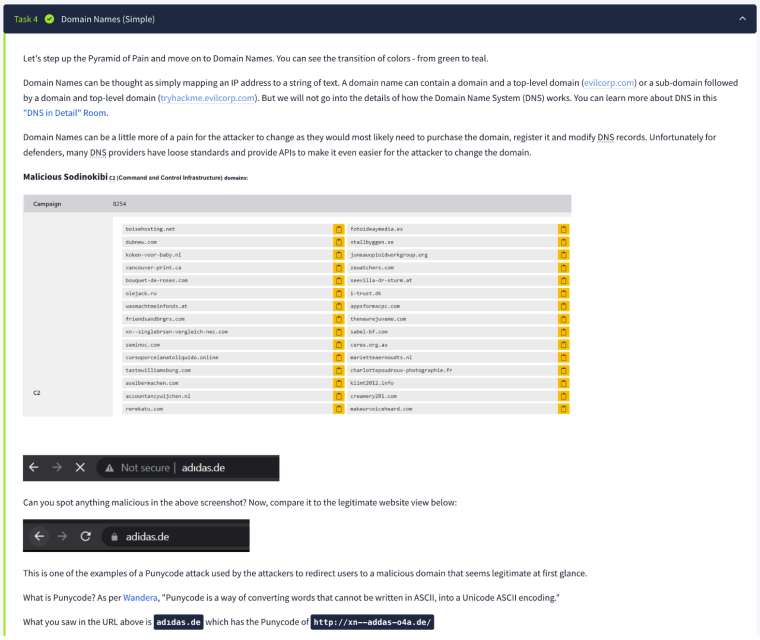
Task 3: IP Address (Easy)

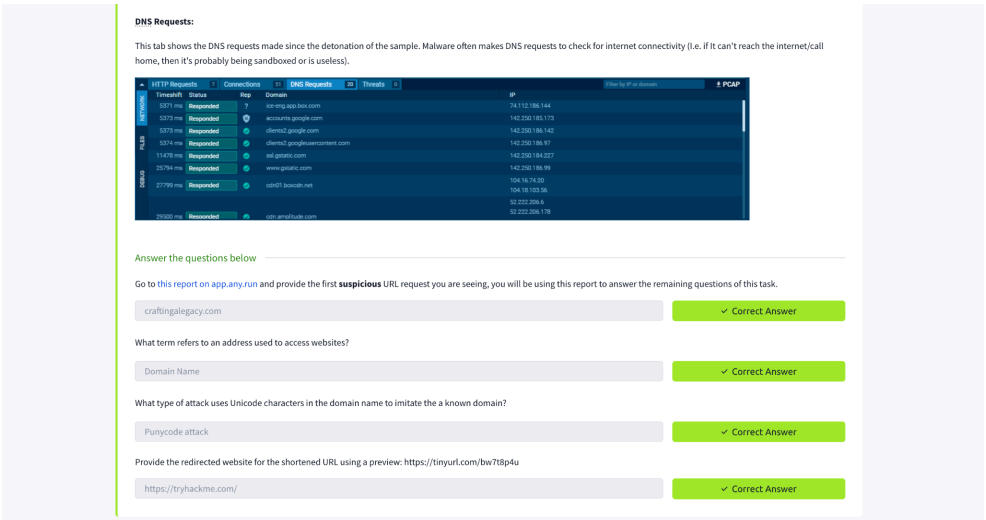
IP addresses are slightly more challenging for adversaries to change than hash values but are still relatively easy to alter. Attackers can switch to different IP addresses or use proxy services to mask their true origin. Monitoring and blocking malicious IP addresses can temporarily disrupt an attacker's activities, but this tactic alone is not sufficient for long-term protection.



Task 4: Domain Names (Simple)

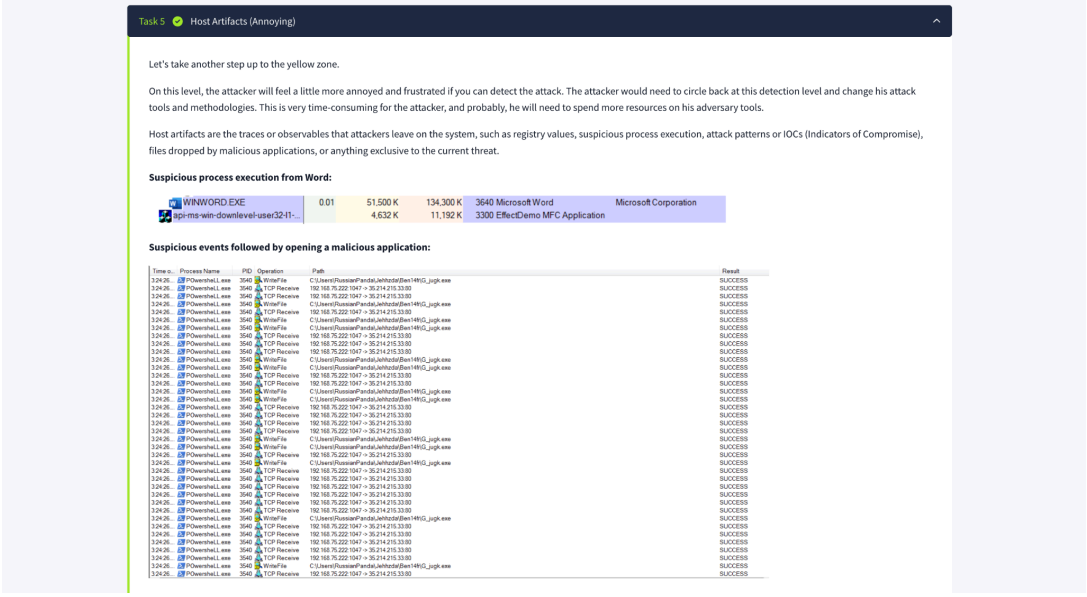
Domain names are used by adversaries to host malicious websites or control servers for command and control (C2) purposes. Changing domain names requires more effort than altering hash values or IP addresses but is still considered simple for determined attackers. Blocking malicious domains can interrupt phishing campaigns and other attacks, but adversaries can quickly register new domains to resume their activities.

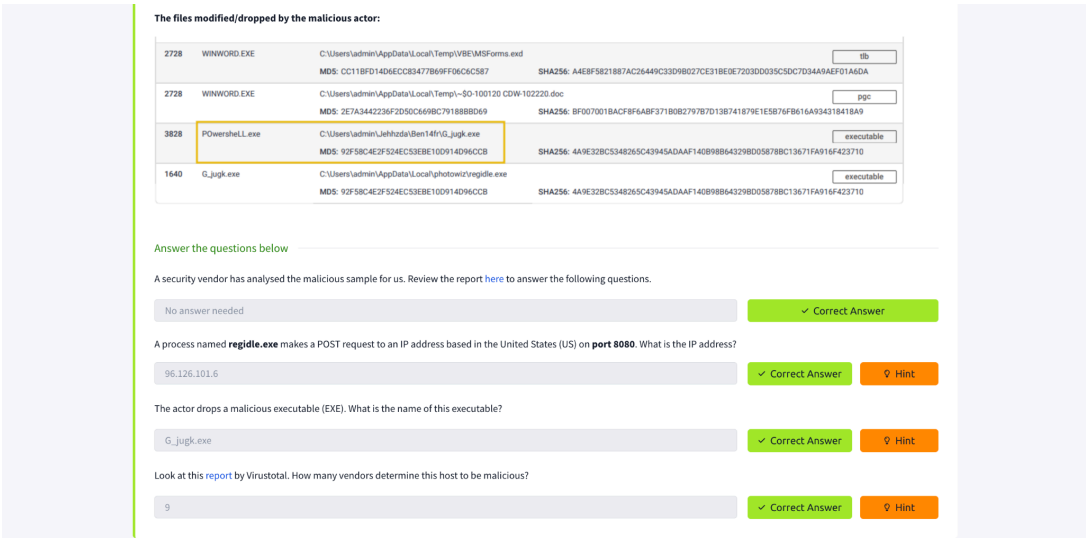




Task 5: Host Artifacts (Annoying)

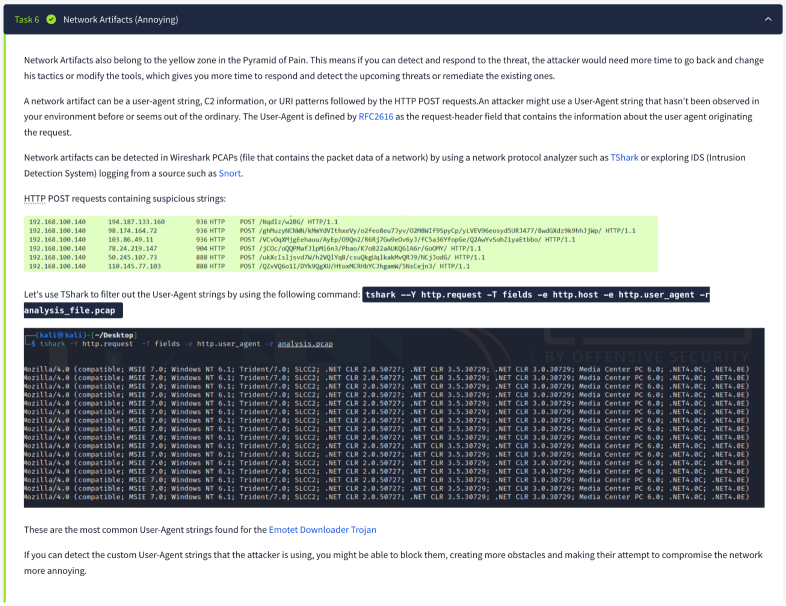
Host artifacts include traces left on compromised systems, such as registry keys, file names, or specific configurations. These artifacts are more difficult for adversaries to change because they are deeply embedded within the system. Detecting and responding to host artifacts can significantly hinder an attacker's ability to maintain persistence and move laterally within a network.

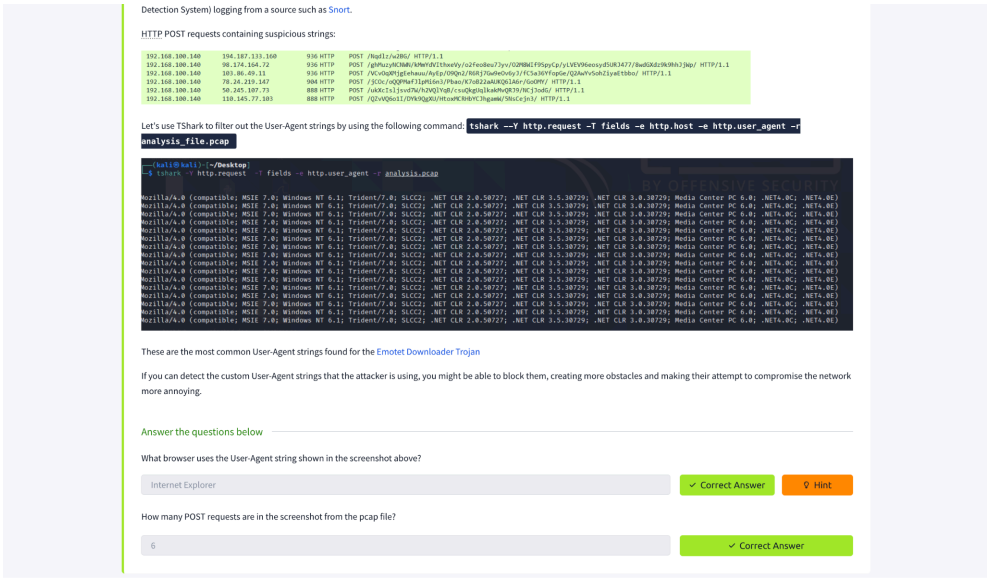




Task 6: Network Artifacts (Annoying)

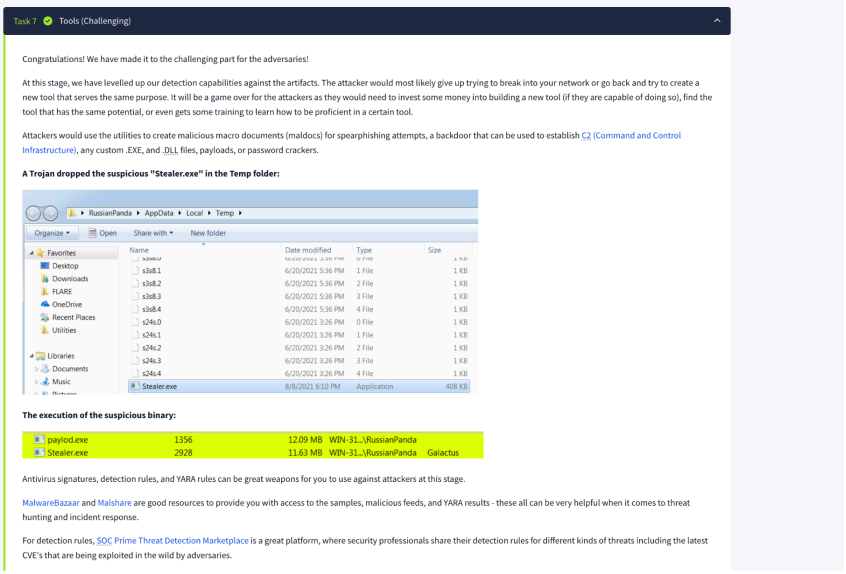
Network artifacts refer to patterns in network traffic that can indicate malicious activity, such as specific protocols, unusual data flows, or anomalous behavior. Changing network artifacts is annoying for adversaries because it often requires altering their tools or techniques. Effective monitoring of network traffic can help detect and prevent ongoing attacks, making it more difficult for attackers to operate undetected.

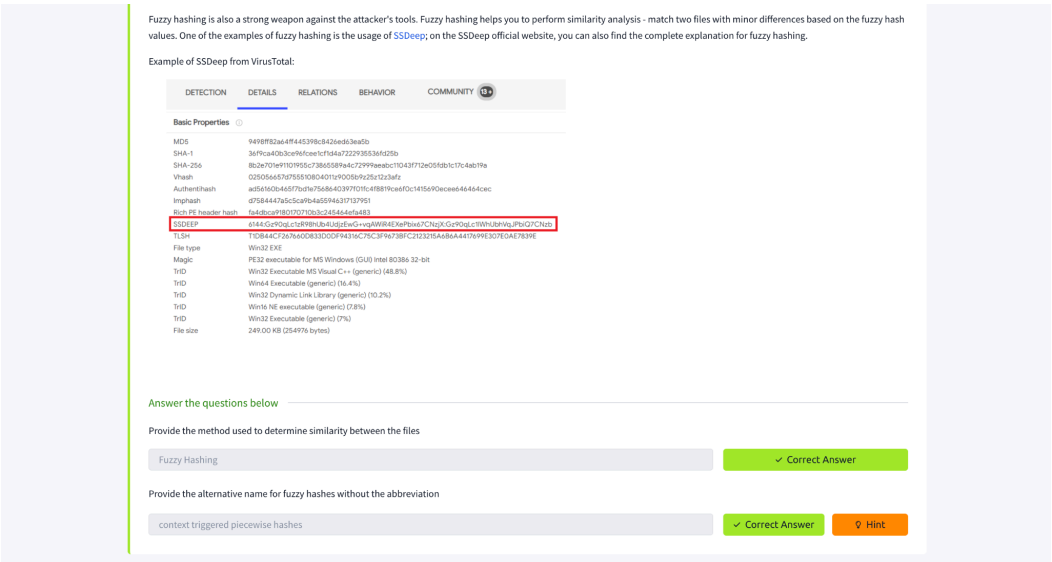




Task 7: Tools (Challenging)

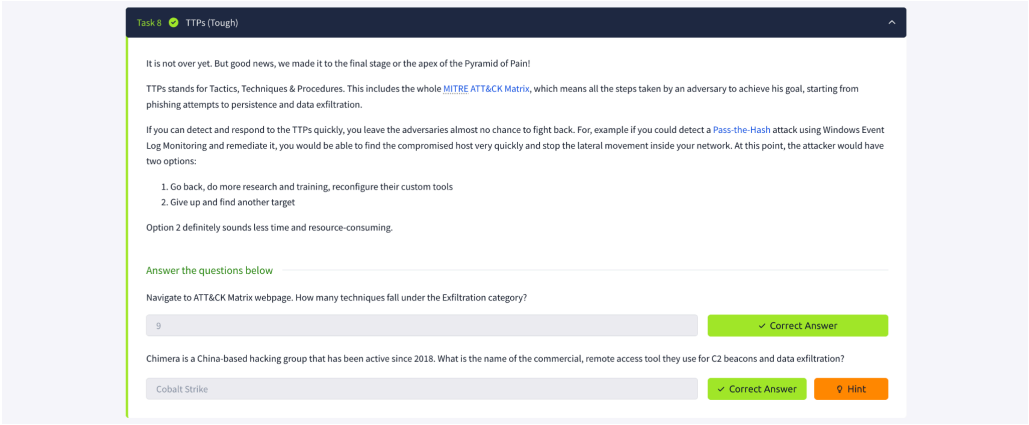
Tools include the software and scripts used by attackers to conduct their operations. These can range from publicly available hacking tools to custom malware. Forcing adversaries to change their tools is challenging because it requires them to find, develop, or modify software, which can be time-consuming and costly. Identifying and neutralizing these tools can disrupt an attacker's capabilities and delay their progress.





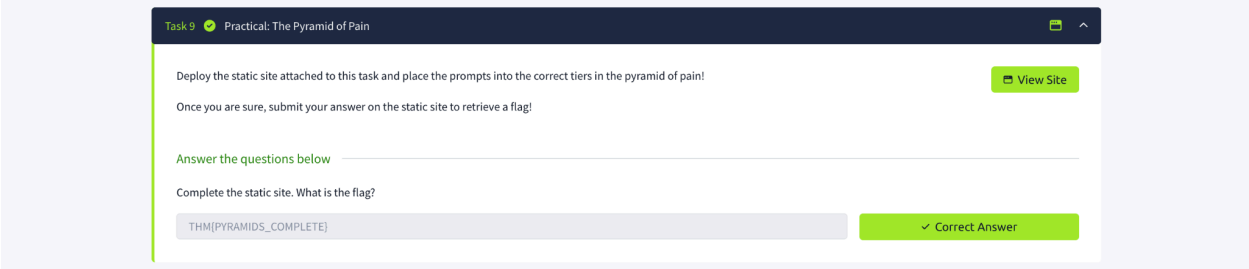
Task 8: TTPs (Tough)

Tactics, Techniques, and Procedures (TTPs) represent the highest level of the Pyramid of Pain and are the most challenging for adversaries to change. TTPs encompass the overall strategies and methodologies used by attackers, including how they conduct reconnaissance, exploit vulnerabilities, and maintain persistence. Altering TTPs often requires a complete overhaul of their approach, making it extremely difficult and resource-intensive for adversaries.



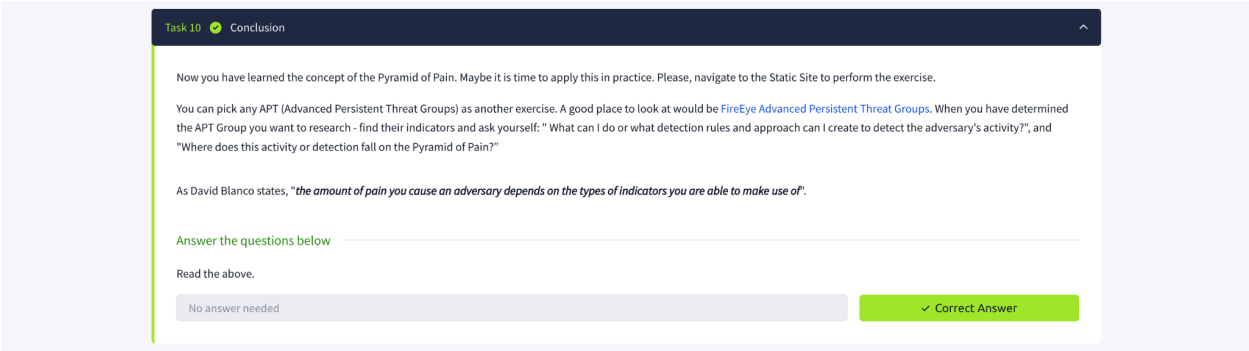
Task 9: Practical: The Pyramid of Pain

In the practical section, learners apply the concepts of the Pyramid of Pain to real-world scenarios. This hands-on approach reinforces understanding by allowing participants to analyze various IOCs and determine the level of difficulty an adversary would face in altering them. This exercise helps solidify the theoretical knowledge gained throughout the room and demonstrates the practical application of the Pyramid of Pain model.



Task 10: Conclusion

The conclusion reinforces the importance of understanding the Pyramid of Pain and applying it in cybersecurity defenses. It encourages trainees to use the model to evaluate and enhance their detection and response strategies, ultimately making it more difficult for adversaries to achieve their objectives.



Conclusion

In conclusion, the "Pyramid of Pain" room on TryHackMe offers an invaluable framework for understanding the complexity and effectiveness of various indicators of compromise in cybersecurity defense. By progressing through each task, trainees gain a comprehensive understanding of how different levels of indicators impact adversary behavior and the difficulty associated with changing those indicators.

Utilizing the Pyramid of Pain model enables cybersecurity professionals to prioritize their defensive efforts effectively. By focusing on indicators that impose the greatest challenge for adversaries to alter, defenders can significantly disrupt adversary operations and enhance their overall security posture.

As part of the Microsoft ADC Cybersecurity Skilling Program, mastering these concepts is essential for developing robust defensive strategies and becoming proficient in thwarting sophisticated cyber threats. Understanding and applying the Pyramid of Pain empowers trainees to cause substantial pain to adversaries, thereby increasing the security and resilience of their organizations.sophisticated cyber threats.

Shared Link

Links to my shared progress can be accessed here