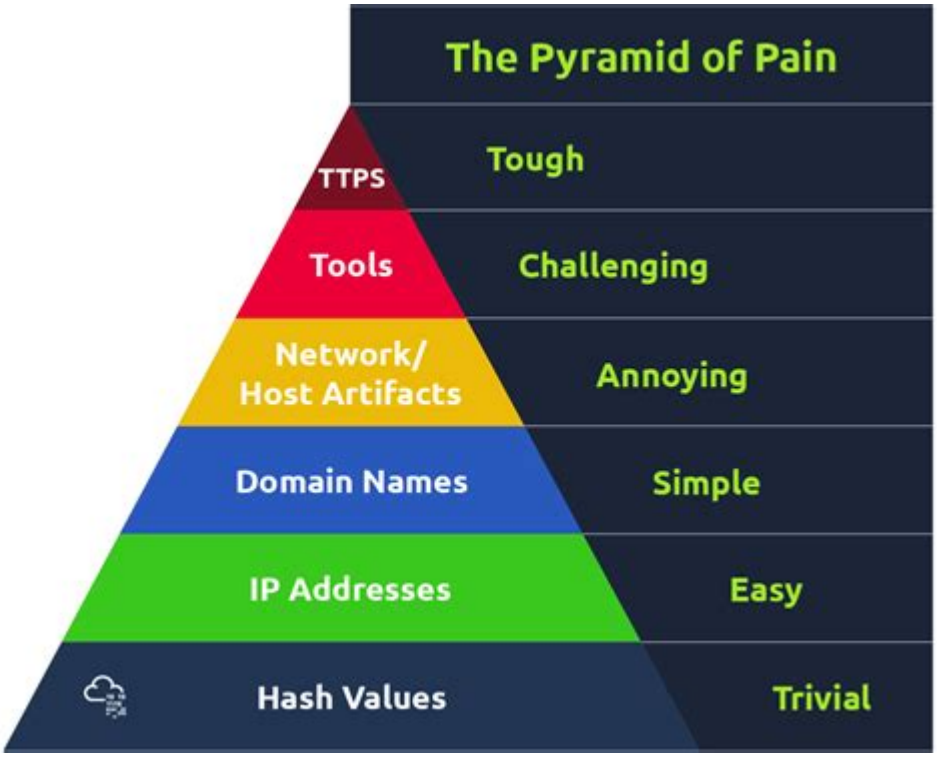
Pyramid Of Pain Tryhackme Walkthrough



Pyramid of Pain TryHackMe Walkthrough

The "Pyramid of Pain" is an essential concept in the field of cybersecurity, particularly within the context of threat hunting and incident response. It is a model that helps security professionals understand the varying levels of difficulty in detecting adversary tactics, techniques, and procedures (TTPs). The TryHackMe platform offers a hands-on learning experience centering around this concept, providing users with a structured walkthrough to enhance their skills in recognizing and mitigating threats. This article will guide you through the Pyramid of Pain as implemented in TryHackMe, detailing its components, the learning experience, and practical applications.

The Pyramid of Pain Explained

The Pyramid of Pain, conceptualized by David J. Bianco, visualizes the relationship between the difficulty of detecting certain indicators of compromise (IoCs) and the potential impact on an organization's security posture. It categorizes various types of IoCs into a pyramid structure:

1. Hash Values
2. IP Addresses
3. Domain Names
4. URLs

5. Tactics, Techniques, and Procedures (TTPs)

Each layer of the pyramid represents a different level of pain or challenge associated with detection and response. As you move up the pyramid, the IoCs become more abstract and harder to detect, making them more valuable for defenders to focus on.