Pyramid Of Pain

## 📓 **Notes – Pyramid of Pain**

**Lab Name:** Pyramid of Pain

**Summary:**  
The Pyramid of Pain is a cybersecurity model that ranks types of threat indicators by how difficult they are for an attacker to change. The higher you go, the more it disrupts their operations if detected. It’s used to guide defensive focus toward high-value indicators like TTPs instead of easily changeable ones like hashes.

**Key Points Learned:**

* **Hash Values:** Easy for attackers to change by re-compiling malware.
* **IP Addresses:** Simple to rotate via VPNs, proxies, or new infrastructure.
* **Domain Names:** Harder than IPs but still changeable; can register new ones.
* **Network/Host Artifacts:** Require code changes or reconfiguration (file paths, registry keys, services).
* **Tools:** Changing or rebuilding tools requires more effort and time.
* **TTPs (Tactics, Techniques, and Procedures):** The hardest for attackers to change — these represent their behavior patterns and strategy.

**Practical Takeaway:**

* Focus detection efforts on **TTPs and Tools** for longer-lasting defense.
* Lower-level indicators like hashes and IPs are still useful but can be evaded quickly.

**Tools/Commands:**

* None — theoretical concept.

