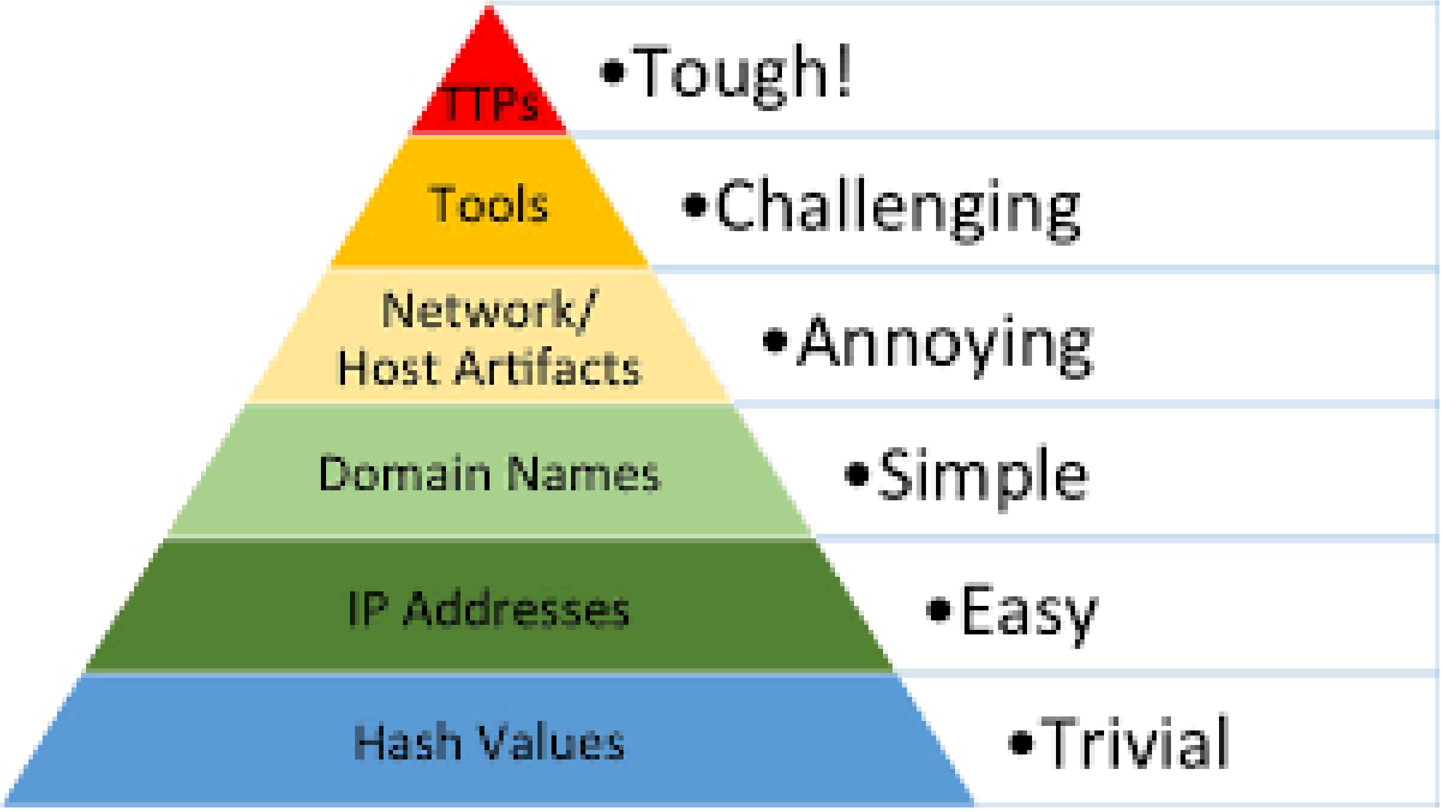
PYRAMID OF PAIN

Room Link : 🌐 Pyramid Of Pain

Description : The **Pyramid of Pain** is a conceptual model, developed by David J. Bianco, used in cybersecurity to classify and prioritize threat intelligence indicators. It illustrates that not all indicators are of equal value. The framework is structured as a pyramid with six levels, each representing a different type of indicator of compromise (IOC).

Task 1: Introduction



Task 2: Hash Values - Level 1

Concept:

A hash value is a numerical value of a fixed length that uniquely identifies data.

Types of hashing algorithms:

MD5- it uses 128 bit hash value and is not considered cryptographically secure.it is vulnerable against the hash collisions.

SHA-1 - it produces 160 bit hash value string and is vulnerable against bruteforce attacks.

SHA-2-Is considered secure and 256 bit hash value string is used.

so in the conext of the difficulty level, the attackers can easily change the hash value of the files.

Questions:

1. Analyse the report associated with the hash "b8ef959a9176aef07fdca8705254a163b50b49a17217a4ff0107487f59d4a35d" here. What is the filename of the sample?

Ans. Sales_Receipt 5606.xls

Task 3: Ip addresses-Level 2

Concept:

Ip addresses are used to recognize the devices on the network.Firewalls can be made available for banning or protecting the systems from malicious ips but the adversary can still change the ips and enter again.

The adversary can use fastflux to challenge the ip detections.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. The purpose of using the Fast Flux network is to make the communication between malware and its command and control server (C&C) challenging to be discovered by security professionals.

Questions:

1.Read the following report to answer this question. What is the **first IP address** the malicious process (**PID 1632**) attempts to communicate with?\

Ans.50.87.136.52

2.Read the following report to answer this question. What is the **first domain name** the malicious process ((PID 1632) attempts to communicate with?

Ans. craftingalegacy.com

Task 4: Domain names-Level 3

Concept:

Domain Names can be a little more of a pain for the attacker to change as they would most likely need to purchase the domain, register it and modify DNS records. Unfortunately for defenders, many DNS providers have loose standards and provide APIs to make it even easier for the attacker to change the domain.

Domain names can be spoofed with the puny code attacks.

"Punycode is a way of converting words that cannot be written in ASCII, into a Unicode ASCII encoding."

Internet Explorer, Google Chrome, Microsoft Edge, and Apple Safari are now pretty good at translating the obfuscated characters into the full Punycode domain name.

To detect malicious domains, proxy logs or web server logs can be used.

Attackers usually hide the malicious domains under URL shorteners. A URL Shortener is a tool that creates a short and unique URL that will redirect to the specific website specified during the initial step of setting up the URL Shortener link

The http requests,dns requests and the connections made by the domain can be viewed and analysed whethere the domain is malicious or not.

Questions:

1.Go to this report on app.any.run and provide the first **suspicious** domain request you are seeing, you will be using this report to answer the remaining questions of this task.

Ans.craftingalegacy.com

2.What term refers to an address used to access websites?

Ans. Domain Name

3.What type of attack uses Unicode characters in the domain name to imitate the a known domain?

Ans.Punycode attack

4.Provide the redirected website for the shortened URL using a preview: https://tinyurl.com/bw7t8p4u

Ans. 🌐 TryHackMe | Cyber Security Training

Task 5: host artifacts-Level 4

Concept:

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

So when some malicious process is executed the registry values and logs are changed and some malicious activities taking place can be easily visible and this makes the attacker frustrated.

Questions:

1.A process named **regidle.exe** makes a POST request to an IP address based in the United States (US) on **port 8080**. What is the IP address?

Ans.96.126.101.6

2.The actor drops a malicious executable (EXE). What is the name of this executable?

Ans.G_jugk.exe

3.Look at this report by Virustotal. How many vendors determine this host to be malicious?

Ans.9

Task 6: Network artifacts-level 4

Concept:

Network Artifacts also belong to the yellow zone in the Pyramid of Pain. This means if you can detect and respond to the threat, the attacker would need more time to go back and change his tactics or modify the tools, which gives you more time to respond and detect the upcoming threats or remediate the existing ones.
A network artifact can be a user-agent string, C2 information, or URI patterns followed by the HTTP POST requests.An attacker might use a User-Agent string that hasn't been observed in your environment before or seems out of the ordinary. The User-Agent is defined by RFC2616 as the request-header field that contains the information about the user agent originating the request.

Questions:

1.What browser uses the User-Agent string shown in the screenshot above?

Ans.Internet Explorer

2.How many POST requests are in the screenshot from the pcap file?

Ans.6

Task 7: Tools Level-5

Concept:

At this stage, we have levelled up our detection capabilities against the artifacts. The attacker would most likely give up trying to break into your network or go back and try to create a new tool that serves the same purpose. It will be a game over for the attackers as they would need to invest some money into building a new tool (if they are capable of doing so), find the tool that has the same potential, or even gets some training to learn how to be proficient in a certain tool.

Attackers would use the utilities to create malicious macro documents (maldocs) for spearphishing attempts, a backdoor that can be used to establish C2 (Command and Control Infrastructure), any custom .EXE, and .DLL files, payloads, or password crackers.

MalwareBazaar and Malshare are good resources to provide you with access to the samples, malicious feeds, and YARA results - these all can be very helpful when it comes to threat hunting and incident response.

For detection rules, SOC Prime Threat Detection Marketplace is a great platform, where security professionals share their detection rules for different kinds of threats including the latest CVE's that are being exploited in the wild by adversaries.

Fuzzy hashing is also a strong weapon against the attacker's tools. Fuzzy hashing helps you to perform similarity analysis - match two files with minor differences based on the fuzzy hash values. One of the examples of fuzzy hashing is the usage of SSDeep; on the SSDeep official website, you can also find the complete explanation for fuzzy hashing.

Questions:

1.Provide the method used to determine similarity between the files

Ans.Fuzzy hashing

2.Provide the alternative name for fuzzy hashes without the abbreviation

Ans.context triggered piecewise hashes

Task 8: Tactics,techniques and procedures -Level 6

Concept:

TTPs stands for Tactics, Techniques & Procedures. This includes the whole MITRE ATT&CK Matrix, which means all the steps taken by an adversary to achieve his goal, starting from phishing attempts to persistence and data exfiltration.

If you can detect and respond to the TTPs quickly, you leave the adversaries almost no chance to fight back. For, example if you could detect a Pass-the-Hash attack using Windows Event Log Monitoring and remediate it, you would be able to find the compromised host very quickly and stop the lateral movement inside your network

Questions:

1.Navigate to ATT&CK Matrix webpage. How many techniques fall under the Exfiltration category?

Ans.9

2.Chimera is a China-based hacking group that has been active since 2018. What is the name of the commercial, remote access tool they use for C2 beacons and data exfiltration?

Ans.Cobalt Strike