

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 1 ✓ Introduction



This well-renowned concept is being applied to cybersecurity solutions like [Cisco Security](#), [SentinelOne](#), and [SOCRadar](#) to improve the effectiveness of CTI (Cyber Threat Intelligence), threat hunting, and incident response exercises.

Understanding the Pyramid of Pain concept as a Threat Hunter, Incident Responder, or SOC Analyst is important.

Are you ready to explore what hides inside the Pyramid of Pain?

Answer the questions below

Read the above.

No answer needed ✓ Correct Answer

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 2 ● Hash Values (Trivial)

As per Microsoft, the hash value is a numeric value of a fixed length that uniquely identifies data. A hash value is the result of a hashing algorithm. The following are some of the most common hashing algorithms:

- **MD5 (Message Digest, defined by RFC 1321)** - was designed by Ron Rivest in 1992 and is a widely used cryptographic hash function with a 128-bit hash value. MD5 hashes are NOT considered cryptographically secure. In 2011, the IETF published RFC 6151, "Updated Security Considerations for the MD5 Message-Digest and the HMAC-MD5 Algorithms," which mentioned a number of attacks against MD5 hashes, including the hash collision.
- **SHA-1 (Secure Hash Algorithm 1, defined by RFC 3174)** - was invented by United States National Security Agency in 1995. When data is fed to SHA-1 Hashing Algorithm, SHA-1 takes an input and produces a 160-bit hash value string as a 40 digit hexadecimal number. NIST deprecated the use of SHA-1 in 2011 and banned its use for digital signatures at the end of 2013 based on it being susceptible to brute-force attacks. Instead, NIST recommends migrating from SHA-1 to stronger hash algorithms in the SHA-2 and SHA-3 families.
- **The SHA-2 (Secure Hash Algorithm 2)** - SHA-2 Hashing Algorithm was designed by The National Institute of Standards and Technology (NIST) and the National Security Agency (NSA) in 2001 to replace SHA-1. SHA-2 has many variants, and arguably the most common is SHA-256. The SHA-256 algorithm returns a hash value of 256-bits as a 64 digit hexadecimal number.

A hash is not considered to be cryptographically secure if two files have the same hash value or digest.

Security professionals usually use the hash values to gain insight into a specific malware sample, a malicious or a suspicious file, and as a way to uniquely identify and reference the malicious artifact.

You've probably read ransomware reports in the past, where security researchers would provide the hashes related to the malicious or suspicious files used at the end of the report. You can check out [The DFIR Report](#) and [FireEye Threat Research Blogs](#) if you're interested in seeing an example.

Various online tools can be used to do hash lookups like [VirusTotal](#) and [Metadefender Cloud - OPSWAT](#).

[Get full report](#) [View dynamic analysis](#) [View leaderboards](#)
[Upgrade limits](#) [Sandbox documentation](#) [Check out our community](#)

As you might have noticed, it is really easy to spot a malicious file if we have the hash in our arsenal. However, as an attacker, modifying a file by even a single bit is trivial, which would produce a different hash value. With so many variations and instances of known malware or ransomware, threat hunting using file hashes as the IOC (Indicators of Compromise) can become difficult.

Let's take a look at an example of how you can change the hash value of a file by simply appending a string to the end of a file using `echo : File Hash (Before Modification)`

```
PS C:\Users\THM\Downloads> Get-FileHash .\OpenVPN_2.5.1_I601_amd64.msi |Algorithm MD5
Algorithm Hash
Path
MD5      D1A008E3A606F24590A02B853E955CF7 C:\Users\THM\Downloads\OpenVPN_2.5.1_I601_amd64.msi
```

File Hash (After Modification)

```
PS C:\Users\THM\Downloads> echo "AppendTheHash" >> .\OpenVPN_2.5.1_I601_amd64.msi
PS C:\Users\THM\Downloads> Get-FileHash .\OpenVPN_2.5.1_I601_amd64.msi |Algorithm MD5
Algorithm Hash
Path
MD5      9D52B46F5DE41B73418F8E0DACEC5E9F C:\Users\THM\Downloads\OpenVPN_2.5.1_I601_amd64.msi
```

Answer the questions below

Analyse the report associated with the hash "b8ef959a9176aef07fdca8705254a163b50b49a17217a4ff0107487f59d4a35d" [here](#). What is the filename of the sample?

Sales_Receipt 5606.xls ✓ Correct Answer ? Hint

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 3 ● IP Address (Easy)

You may have learned the importance of an IP Address from the "What is Networking?" Room. An IP address is used to identify any device connected to a network. These devices range from desktops, to servers and even CCTV cameras! We rely on IP addresses to send and receive the information over the network. But we are not going to get into the structure and functionality of the IP Address. As a part of the Pyramid of Pain, we'll evaluate how IP addresses are used as an indicator.

In the Pyramid of Pain, IP addresses are indicated with the color green. You might be asking why and what you can associate the green colour with?

From a defense standpoint, knowledge of the IP addresses an adversary uses can be valuable. A common defense tactic is to block, drop, or deny inbound requests from IP addresses on your perimeter or external firewall. This tactic is often not bulletproof as it's trivial for an experienced adversary to recover simply by using a new public IP address.

Malicious IP connections ([app.any.run](#)):

HTTP Requests	Connections	DNS Requests	Threats
8500 ms	1	1	1
144.95.160.7	TCP	1607	some_malicious_file.txt
144.95.7.160	TCP	7	some_malicious_file.txt
205.35.160.205	TCP	1607	some_malicious_file.txt
204.76.160.204	TCP	1607	some_malicious_file.txt

NOTE! Do not attempt to interact with the IP addresses shown above.

One of the ways an adversary can make it challenging to successfully carry out IP blocking is by using **Fast Flux**.

According to Akamai, 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.

So, the primary concept of a Fast Flux network is having multiple IP addresses associated with a domain name, which is constantly changing. Palo Alto created a fictional scenario to explain Fast Flux: "[Fast Flux 101: How Cybercriminals Improve the Resilience of Their Infrastructure to Evasion Detection and Law Enforcement Takedowns](#)"

Read the following report ([generated from any.run](#)) for this sample [here](#) to answer the questions below:

Answer the questions below

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

50.87.136.52 Correct Answer Hint

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

craftingalegacy.com Correct Answer Hint

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 4 ● Domain Names (Simple)

Let's step up the Pyramid of Pain and move on to Domain Names. You can see the transition of colors - from green to teal.

Domain Names can be thought as simply mapping an IP address to a string of text. A domain name can contain a domain and a top-level domain ([evilcorp.com](#)) or a sub-domain followed by a domain and top-level domain ([tryhackme.evilcorp.com](#)). But we will not go into the details of how the Domain Name System (DNS) works. You can learn more about DNS in this "[DNS in Detail](#)" Room.

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.

Malicious Sodinokibi (Command and Control Infrastructure) domains:

Campaign	ID	
C2	b01shosting.net	fordidawaymedia.es
	dubnew.com	stallingen.se
	kakon-vor-baby.nl	janeauwpublishergroup.org
	vancouver-print.ca	zweathers.com
	boisquet-de-rooses.com	seville-dr-store.at
	olxjek.ru	l-trust.dk
	seasacasteinfors.at	mpfprawaco.com
	franklingr.org	republiq.com
	an-singleraten-vergleich-noc.com	rebel.or.com
	seminic.com	carres.org.ar
	corporationrelaxationlondononline	mariteteamroute.nl
	taxstellenlinienberatung.online	charlotteprodrus-photographe.fr
	ausberatungen.com	kliset2011.info
	accountancygijnen.nl	cranny201.com
	revkata.com	makuracosmear.com

← → ▲ Not secure | [adidas.de](#)

Can you spot anything malicious in the above screenshot? Now, compare it to the legitimate website view below:

← → C ⓘ adidas.de

This is one of the examples of a Punycode attack used by the attackers to redirect users to a malicious domain that seems legitimate at first glance.

What is Punycode? As per [Wandera](#), "Punycode is a way of converting words that cannot be written in ASCII, into a Unicode ASCII encoding."

What you saw in the URL above is [adidas.de](#) which has the Punycode of <http://xn--addas-04a.de/>

DNS Requests:

This tab shows the DNS requests made since the detonation of the sample. Malware often makes DNS requests to check for internet connectivity (i.e. if it can't reach the internet/call home, then it's probably being sandboxed or is useless).

Answer the questions below

Go to this report on [app.any.run](#) and provide the first **suspicious** URL request you are seeing, you will be using this report to answer the remaining questions of this task.

✓ Correct Answer

What term refers to an address used to access websites?

✓ Correct Answer

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

✓ Correct Answer

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

✓ Correct Answer

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.

The files modified/dropped by the malicious actor:

2728 WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\VBE\MSForms.exe MD5: CC11BFD14D6ECC83477B69FF06C6C6S7	SHA256: A4E8F5821887CA26449C3D9B027CE31BE0E720300035C5DC7D34A9AEF01A6DA file
2728 WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\~S0_100120_CDW-102220.doc MD5: 2E7A044236F2D505669BC791888BD069	SHA256: BF007001BACFB6ABF371B0B2797B7D13B741879E1E5B76FB016A934318410A9 file
3828 Powershell.exe	C:\Users\admin\AppData\Local\photowiz\regidle.exe MD5: 92F58C4E2F524EC53E8E10D914D96CCB	SHA256: 4A9E32BC5348265C43945ADAFA140B98864329BD05878BC13671FA916F423710 executable
1640 G_jugk.exe	C:\Users\admin\AppData\Local\photowiz\regidle.exe MD5: 92F58C4E2F524EC53E8E10D914D96CCB	SHA256: 4A9E32BC5348265C43945ADAFA140B98864329BD05878BC13671FA916F423710 executable

Answer the questions below

A security vendor has analysed the malicious sample for us. Review the report [here](#) to answer the following questions.

No answer needed ✓ Correct Answer

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?

96.126.101.6 ✓ Correct Answer Hint

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

G_jugk.exe ✓ Correct Answer Hint

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

9 ✓ Correct Answer Hint

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 6 ● Network Artifacts (Annoying)

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.

Network artifacts can be detected in Wireshark PCAPs (file that contains the packet data of a network) by using a network protocol analyzer such as [TShark](#) or exploring iIDS (Intrusion Detection System) logging from a source such as [Snort](#).

HTTP POST requests containing suspicious strings:

```
192.168.100.160 258.187.133.160 938 HTTP POST /regidle/?2086/ HTTP/1.1
192.168.100.160 78.24.213.147 938 HTTP POST /?/098871P9pcCrjLVW96oeyz5R3477/bad0A9b9b0f298/ HTTP/1.1
192.168.100.160 110.145.77.103 888 HTTP POST /?/098871P9pcCrjLVW96oeyz5R3477/bad0A9b9b0f298/ HTTP/1.1
```

Let's use TShark to filter out the User-Agent strings by using the following command: `tshark -Y http.request -T fields -e http.host -e http.user_agent -r analysis_file.pcap`

```
$ tshark -Y http.request -T fields -e http.user_agent -r analysis.pcap
--(at tshark)~/Desktop$
```

Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/7.0; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0; .NET4.0E)
Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/7.0; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0; .NET4.0E)
Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/7.0; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0; .NET4.0E)
Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/7.0; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0; .NET4.0E)
Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/7.0; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0; .NET4.0E)
Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/7.0; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0; .NET4.0E)
Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/7.0; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0; .NET4.0E)
Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/7.0; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0; .NET4.0E)
Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/7.0; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0; .NET4.0E)
Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/7.0; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0; .NET4.0E)
Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/7.0; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0; .NET4.0E)
Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/7.0; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0; .NET4.0E)
Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/7.0; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0; .NET4.0E)
These are the most common User-Agent strings found for the Emotet Downloader Trojan

If you can detect the custom User-Agent strings that the attacker is using, you might be able to block them, creating more obstacles and making their attempt to compromise the network more annoying.

Detection System) logging from a source such as Snort.

HTTP POST requests containing suspicious strings:

```

192.168.100.140 194.127.133.160 936 HTTP POST /#eliz/wQ8Ue/ HTTP/1.1
192.168.100.140 90.19.10.72 936 HTTP POST /#eliz/wQ8Ue/ HTTP/1.1
192.168.100.140 106.49.13 936 HTTP POST /#eliz/wQ8Ue/ HTTP/1.1
192.168.100.140 78.24.219.147 904 HTTP POST /#eliz/qQmPml1lEoLs0/Phan/2d2aaRQ14r-600M/ HTTP/1.1
192.168.100.140 109.16.107.73 886 HTTP POST /#eliz/t51ivw/9uNQq1g/xdqBq1abnHvD79jCjCj/ HTTP/1.1
192.168.100.140 150.163.77.193 886 HTTP POST /#eliz/qQmPml1lEoLs0/Phan/2d2aaRQ14r-600M/ HTTP/1.1

```

Let's use Tshark to filter out the User-Agent strings by using the following command: `tshark -Y http.request -T fields -e http.host -e http.user_agent -r analysis_file.pcap`

These are the most common User-Agent strings found for the Emotet Downloader Trojan

If you can detect the custom User-Agent strings that the attacker is using, you might be able to block them, creating more obstacles and making their attempt to compromise the network more annoying.

Answer the questions below

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

Internet Explorer Correct Answer Hint

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

6 Correct Answer

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 7 ✔ Tools (Challenging)

Congratulations! We have made it to the challenging part for the adversaries!

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.

A Trojan dropped the suspicious "Stealer.exe" in the Temp folder:

The execution of the suspicious binary:

payload.exe	1356	12.09 MB	WBV-31...RussianPanda
Stealer.exe	2928	11.63 MB	WBV-31...RussianPanda Galactus

Antivirus signatures, detection rules, and YARA rules can be great weapons for you to use against attackers at this stage.

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.

Example of SSDeep from VirusTotal:

	Detection	Details	Relations	Behavior	Community
Basic Properties					
MDS	949ff82aa4ff44539bc8426ed3ea5d				
SHA-1	36f9ca0b3ae9ecfcfc1fcfa5a72293535365c2b				
SHA-256	B2c2701e919195c573865894c70437712e056b1c7c4b99				
MD5	0200909a7919195c573865894c70437712e056b1c7c4b99				
Filepath	4ef1f610a4a5f7bf1f75644c07979f4f48fb1fcadfc1415690e0e6d4644ce4				
AuthenticodeHash	4ef1f610a4a5f7bf1f75644c07979f4f48fb1fcadfc1415690e0e6d4644ce4				
Imphash	d788447a47c5c9b4a554437171951				
Rich PE header hash	f4d4bc091910707093c24644e4ef483				
SSDeep	4144c9c90d1c7099b1b1d9d2e...vvaWPE4XePbaeTCNzXGvPogLcIWNUHvqJPhQ7Cnb				
TLSH	1f1844c2f29d760083d0f09431c7c3f9473cf123215a586a447979f9307e0a7e7839e				
File type	Win32 EXE				
Imports	PE executable for MS Windows (GUI) Intel 80386 32-bit				
TnID	Win32 Executable MS Visual C++ (generic) (48.4%)				
TnID	Win32 Executable (generic) (16.4%)				
TnID	Win32 Dynamic Link Library (generic) (10.2%)				
TnID	Win32 Non executable (generic) (7.8%)				
TnID	Win32 Executable (generic) (7%)				
File size	249.00 KB (254976 bytes)				

Answer the questions below

Provide the method used to determine similarity between the files

Fuzzy Hashing ✓ Correct Answer

Provide the alternative name for fuzzy hashes without the abbreviation

context triggered piecewise hashes ✓ Correct Answer ? Hint

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 8 ✓ TTPs (Tough)

It is not over yet. But good news, we made it to the final stage or the apex of the Pyramid of Pain!

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. At this point, the attacker would have two options:

1. Go back, do more research and training, reconfigure their custom tools
2. Give up and find another target

Option 2 definitely sounds less time and resource-consuming.

Answer the questions below

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

9 ✓ Correct Answer

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?

Cobalt Strike ✓ Correct Answer ? Hint

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.

The screenshot shows a task interface titled "Task 9 Practical: The Pyramid of Pain". It includes instructions to deploy a static site and place prompts into a pyramid of pain, with a "View Site" button. A text area for answers is present, along with a "Correct Answer" button.

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.

The screenshot shows a task interface titled "Task 10 Conclusion". It provides information about the concept of the Pyramid of Pain and suggests picking an APT group for research. It also quotes David Blanco and includes a "Correct Answer" button.

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.

Shared Link

Links to my shared progress can be accessed [here](#)

The screenshot shows the TryHackMe platform interface for the 'Pyramid Of Pain' room. At the top, there's a navigation bar with icons for Dashboard, Learn (highlighted), Compete, and Other. On the right, there are buttons for Access Machines, Go Premium, and a user profile icon. Below the navigation is a breadcrumb trail: SOC Level 1 > Cyber Defence Frameworks > Pyramid Of Pain. The main title is 'Pyramid Of Pain' with a small icon. A descriptive text block says: 'Learn what is the Pyramid of Pain and how to utilize this model to determine the level of difficulty it will cause for an adversary to change the indicators associated with them, and their campaign.' It indicates the difficulty is 'Easy' and the duration is '30 min'. Below this are standard room controls: Start AttackBox, Help, Save Room, a like counter (3318), and Options. A progress bar at the bottom shows 'Room completed | 100%'. The main content area lists ten tasks in a vertical stack, each with a green checkmark and a difficulty rating: Task 1 (Introduction - Trivial), Task 2 (Hash Values - Trivial), Task 3 (IP Address - Easy), Task 4 (Domain Names - Simple), Task 5 (Host Artifacts - Annoying), Task 6 (Network Artifacts - Annoying), Task 7 (Tools - Challenging), Task 8 (TTPs - Tough), Task 9 (Practical: The Pyramid of Pain), and Task 10 (Conclusion). Each task has a dropdown arrow to its right.