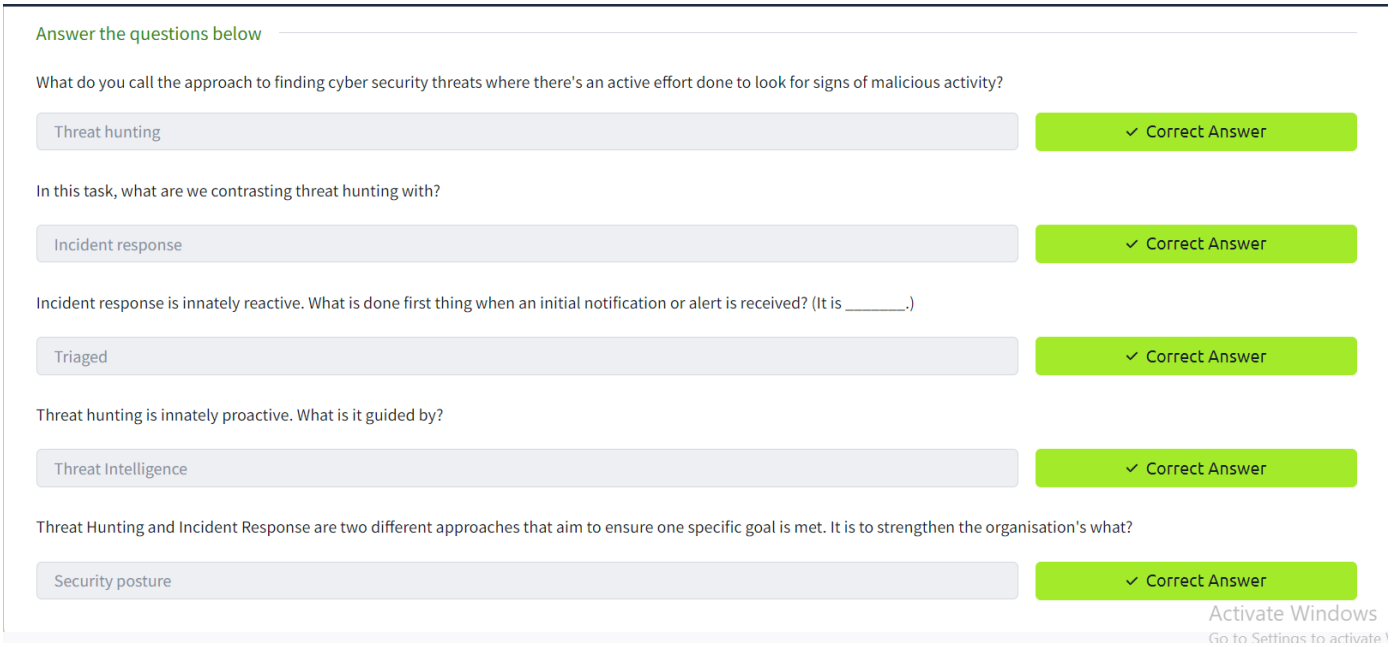
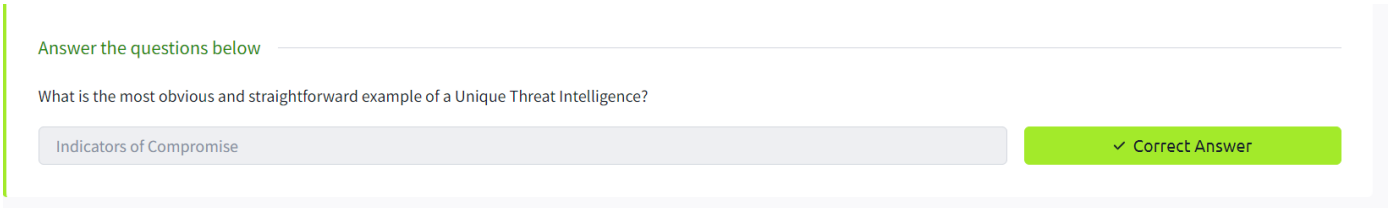
Check Point Attack, Threat and Vulnerability

Summarize and answer the questions for your attack, threat, and vulnerability checkpoint

https://tryhackme.com/r/room/introductiontothreathunting
https://tryhackme.com/r/room/threathuntingfoothold
https://tryhackme.com/r/room/threatemulationintro

QUESTION 1- INTRO TO THREAT HUNTING





Answer the questions below

Malwares are constantly being used in the toolkits of threat actors. What is the live malware repository that we touched upon above?

theZoo ✓ Correct Answer

Knowing what is normal in your environment and separating them from what's not is a skill all threat hunters should have.

What example of Threat Intelligence blends well with environmental noise?

Attack Residues ✓ Correct Answer

Threat actors are quite creative in finding vulnerabilities and misconfigurations.

What should the organisation be extra vigilant in monitoring for announcements of?

Zero-day vulnerabilities ✓ Correct Answer

Characterisation of the subject of the hunt into specific and actionable identifiers is imperative for the hunt's success.

How is it done most effectively?

Attack Signatures and IOCs ✓ Correct Answer

Answer the questions below

Which tactic has the most techniques highlighted?

Discovery ✓ Correct Answer

Which technique does the three threats have in common?

Exploitation of Remote Services ✓ Correct Answer

What technique does WannaCry and Conficker have in common?

Inhibit System Recovery ✓ Correct Answer

What's the score of techniques that Stuxnet and Conficker have in common?

6 ✓ Correct Answer

Answer the questions below

What is the primary goal of Threat Hunting?

Minimise a threat actor's dwell time ✓ Correct Answer

Feedback is important to keep the organisation secure.

Upon profiling threats through our Threat Hunting efforts, what should these profiles be translated to?

Detection mechanisms ✓ Correct Answer

Congratulations!

You've completed the room! Share this with your friends:

Twitter Facebook Linkedin

Leave feedback

QUESTION 2- THREAT HUNTING: FOOTHOLD

Answer the questions below

Use the Discover tab on the left sidebar (via the hamburger button) to answer the question.

What is the attacker's successful authentication timestamp on the Jumphost server? (Format: Nov 1, 2018 @ 13:45:00.000)

Jul 3, 2023 @ 14:14:09.000 ✓ Correct Answer Hint

What is the name of the PHP file accessed by the attacker via the cat command after gaining successful code execution on web01?

config.php ✓ Correct Answer

What is the name of the unusual process executed within the timeframe of update.lnk execution on WKSTN-2?

powershell.exe ✓ Correct Answer Hint

Answer the questions below

Tracing back the cmd and PowerShell child processes spawned by installer.exe, what is the first command executed via cmd?

whoami /priv ✓ Correct Answer Hint

Using the process ID of the PowerShell process spawned by mshta.exe, what is the destination IP of the network connections made by this process?

167.71.198.43 ✓ Correct Answer Hint

Following the cmd.exe process spawned by Python, what is the command-line value of the net.exe process?

net users ✓ Correct Answer

Answer the questions below

What is the PID of the cmd.exe process that executed "powershell Set-MpPreference -DisableRealtimeMonitoring $true"?

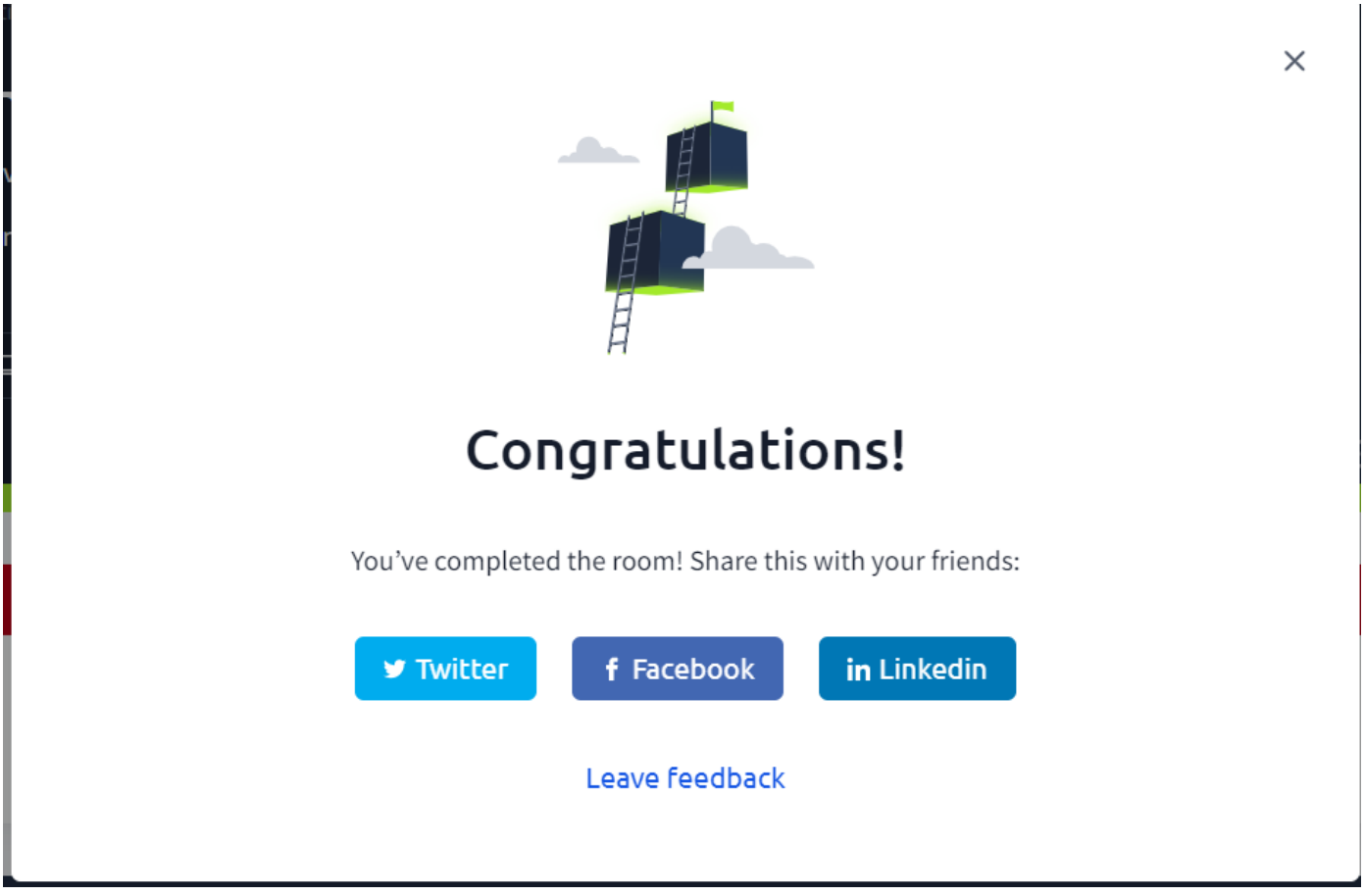
428 ✓ Correct Answer

What is the PowerShell command-line argument used to clear the event logs of WKSTN-1?

Clear-EventLog -LogName Security ✓ Correct Answer

What is the process PID of chrome.exe's target for process injection?

4240 ✓ Correct Answer Hint



**QUESTION 3- INTRO TO THREAT EMULATION

Answer the questions below

What can be defined as an intelligence-driven impersonation of real-world attacks?

Threat Emulation ✓ Correct Answer

What is the exercise of representing adversary functions through predefined and automated attack patterns?

Threat simulation ✓ Correct Answer

**

Answer the questions below

Under TIBER-EU, under which phase would Engagement and Scoping fall?

Preparation ✓ Correct Answer

What is the library that provides technical emulation tests based on TTPs?

Atomic Red Team ✓ Correct Answer

Answer the questions below

The emulation plan component determining which activities are to be conducted is known as the?

Scope ✓ Correct Answer

What is flag one obtained after completing the exercise?

THM{C4RB0N_$P1D3R_1$_F1N7} ✓ Correct Answer

What is flag two obtained after completing the exercise?

THM{3$P1ON4G3_F0R_R34P3R} ✓ Correct Answer

Answer the questions below

Click the **View Site** button at the top of the task to launch the static site. What is flag three obtained after completing the exercise?

THM{D3F3NC3_1N_3MUL4T10N} ✓ Correct Answer

What is flag four obtained after completing the exercise?

THM{S3CUR3_4LL_W3B_4553T5} ✓ Correct Answer

Congratulations!

You've completed the room! Share this with your friends:

Twitter Facebook Linkedin

Leave feedback