Skills Assessment - Suricata

Suricata Rule Development Exercise: Detecting WMI Execution (Through WMIExec)

PCAP source: https://github.com/elcabezzonn/Pcaps

Attack description and possible detection points: https://labs.withsecure.com/publications/attack-detection-fundamentals-discovery-and-lateral-movement-lab-5

`Windows Management Instrumentation (WMI)` is a powerful feature in the Windows operating system that allows for management tasks, such as the execution of code or management of devices, both locally and remotely. As you might expect, this can be a very enticing tool for attackers who are seeking to execute malicious activities remotely.

To detect WMI execution (through `wmiexec`) over the network, we need to focus on the `SMB (Server Message Block)` and `DCOM (Distributed Component Object Model)` protocols, which are the primary means by which remote WMI execution is accomplished.

One method an attacker might use is to create a `Win32_Process` via the WMI service. In this instance, the attacker would create an instance of `Win32_ProcessStartup`, set its properties to control the environment of the new process, then call the `Create` method to start a new process such as `cmd.exe` or `powershell.exe`.

Review the previously referenced resource that discusses the network traces resulting from WMI execution, and then proceed to address the following question.

VPN Servers

⚠ **Warning:** Each time you "Switch", your connection keys are regenerated and you must re-download your VPN connection file.

All VM instances associated with the old VPN Server will be terminated when switching to a new VPN server.

Existing PwnBox instances will automatically switch to the new VPN server.

US Academy 3 — Medium Load

PROTOCOL

UDP 1337 TCP 443

DOWNLOAD VPN CONNECTION FILE

Connect to Pwnbox

Your own web-based Parrot Linux instance to play our labs.

Pwnbox Location

UK — 160ms

Terminate Pwnbox to switch location

? Go to Questions

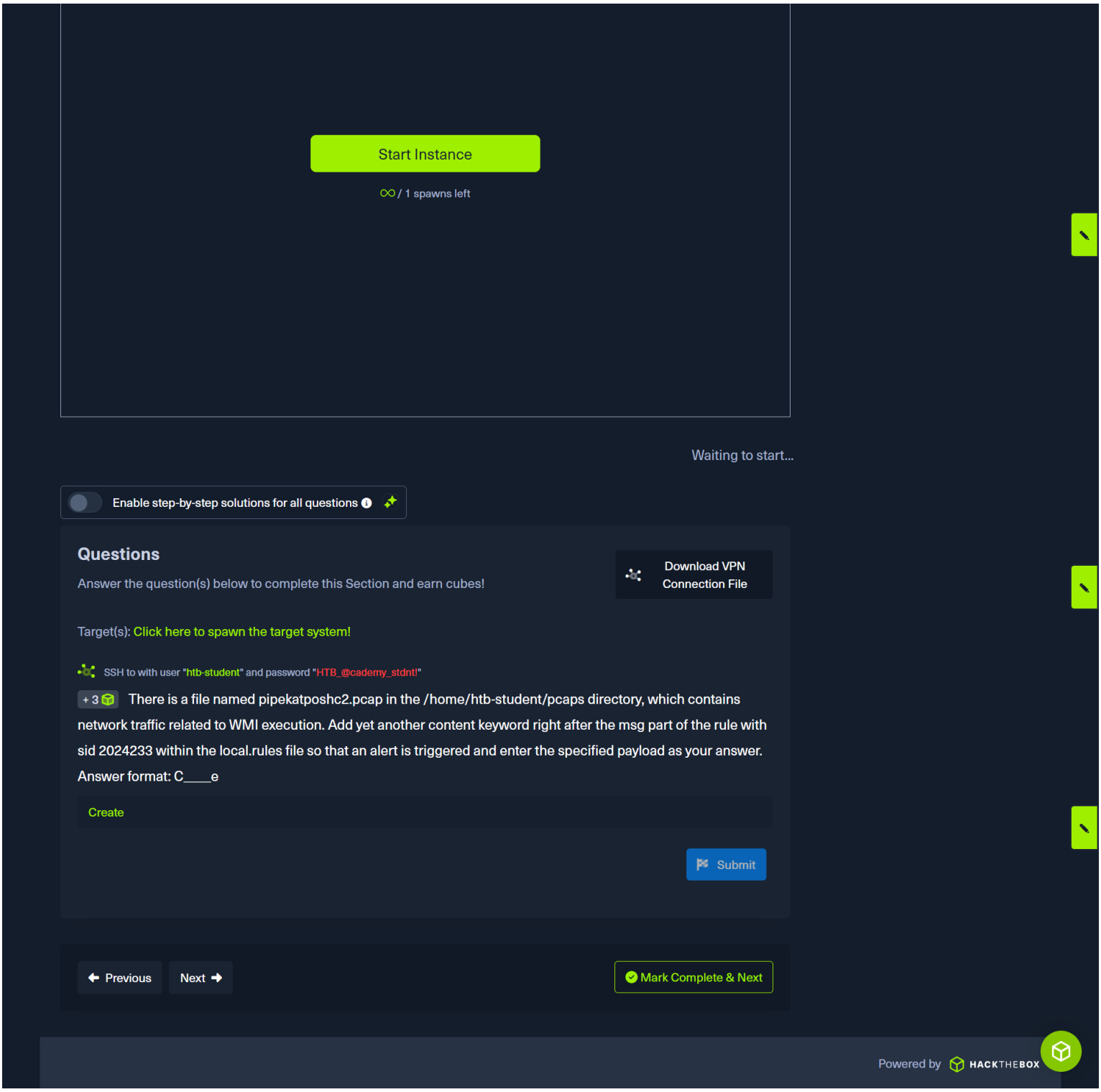
Table of Contents

My Workstation

OFFLINE

Start Instance

∞ / 1 spawns left


Start Instance
∞ / 1 spawns left
Waiting to start...
Enable step-by-step solutions for all questions
Questions
Answer the question(s) below to complete this Section and earn cubes!
Download VPN Connection File
Target(s): Click here to spawn the target system!
SSH to with user "htb-student" and password "HTB_@cademy_stdnt!"
+ 3
There is a file named pipekatposhc2.pcap in the /home/htb-student/pcaps directory, which contains network traffic related to WMI execution. Add yet another content keyword right after the msg part of the rule with sid 2024233 within the local.rules file so that an alert is triggered and enter the specified payload as your answer. Answer format: C____e
Create
Submit
Previous
Next
Mark Complete & Next
Powered by HACKTHEBOX