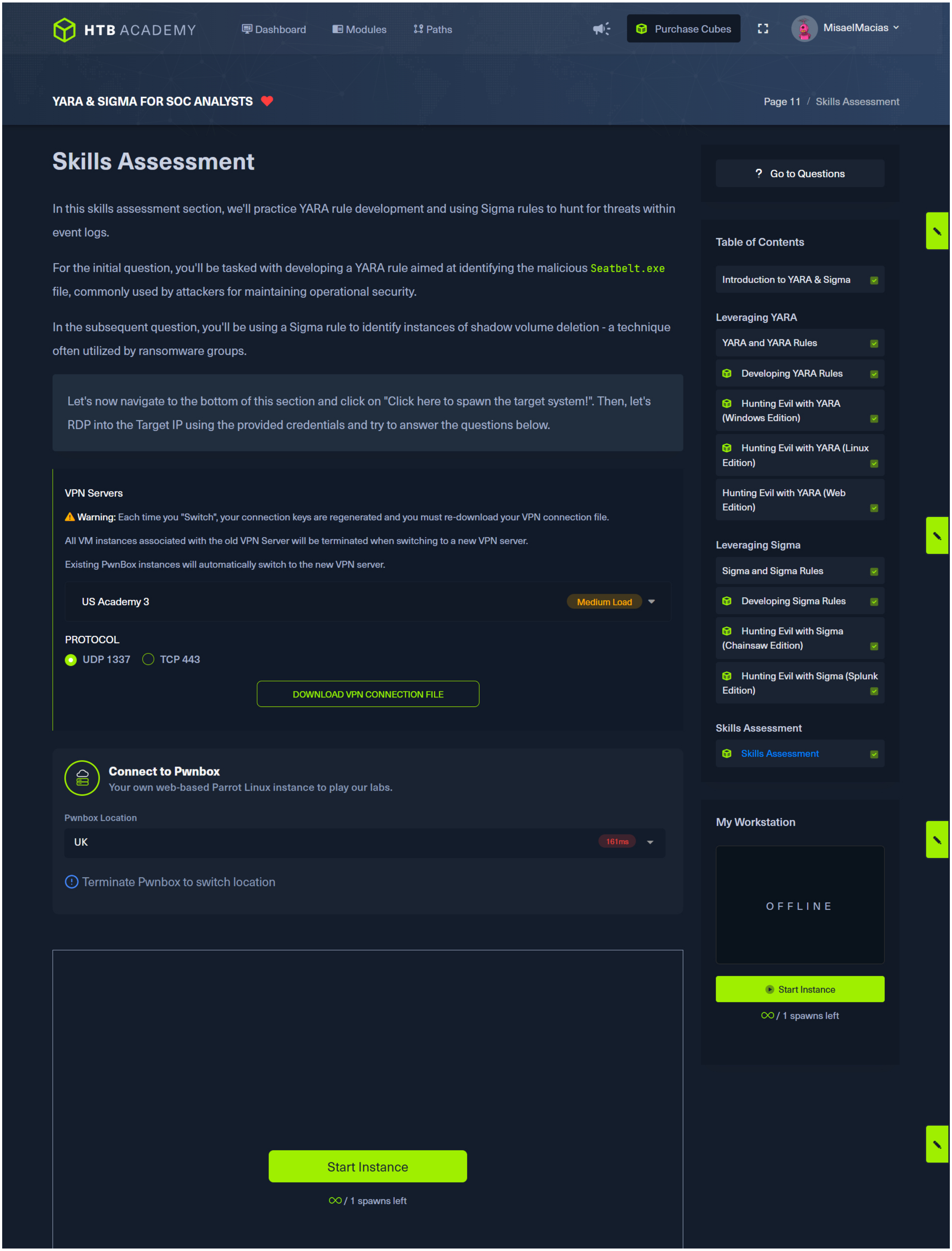


Skills Assessment

In this skills assessment section, we'll practice YARA rule development and using Sigma rules to hunt for threats within event logs.

For the initial question, you'll be tasked with developing a YARA rule aimed at identifying the malicious `Seatbelt.exe` file, commonly used by attackers for maintaining operational security.

In the subsequent question, you'll be using a Sigma rule to identify instances of shadow volume deletion - a technique often utilized by ransomware groups.

> Let's now navigate to the bottom of this section and click on "Click here to spawn the target system!". Then, let's RDP into the Target IP using the provided credentials and try to answer the questions below.

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 161ms ▾

ⓘ Terminate Pwnbox to switch location

Start Instance

∞ / 1 spawns left

? Go to Questions

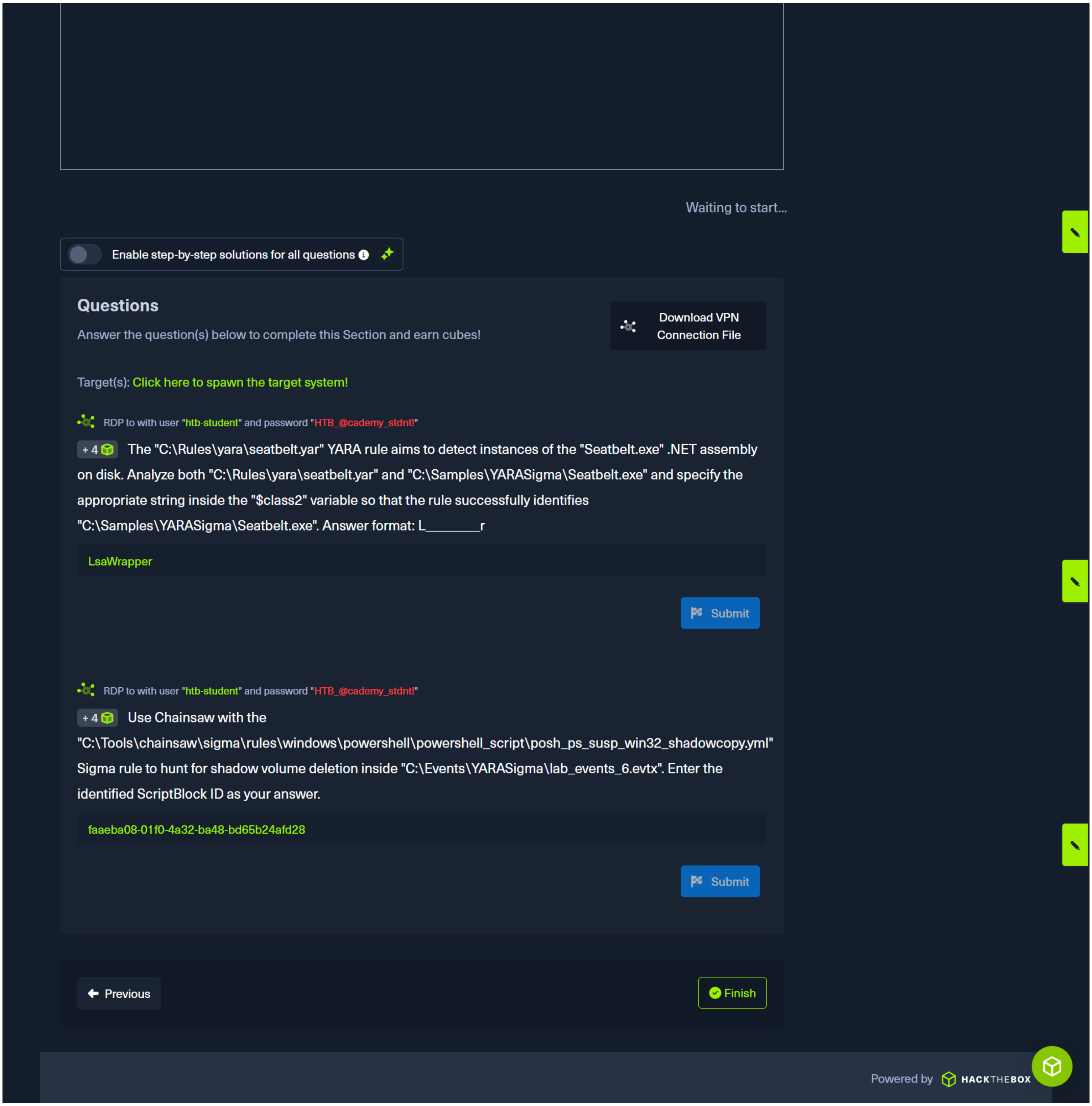
Table of Contents

My Workstation

OFFLINE

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!

RDP to with user "htb-student" and password "HTB_@cademy_stdnt!"

+ 4 The "C:\Rules\yara\seatbelt.yar" YARA rule aims to detect instances of the "Seatbelt.exe" .NET assembly on disk. Analyze both "C:\Rules\yara\seatbelt.yar" and "C:\Samples\YARASigma\Seatbelt.exe" and specify the appropriate string inside the "$class2" variable so that the rule successfully identifies "C:\Samples\YARASigma\Seatbelt.exe". Answer format: L_______r

LsaWrapper

Submit

RDP to with user "htb-student" and password "HTB_@cademy_stdnt!"

+ 4 Use Chainsaw with the "C:\Tools\chainsaw\sigma\rules\windows\powershell\powershell_script\posh_ps_susp_win32_shadowcopy.yml" Sigma rule to hunt for shadow volume deletion inside "C:\Events\YARASigma\lab_events_6.evtx". Enter the identified ScriptBlock ID as your answer.

faaeba08-01f0-4a32-ba48-bd65b24afd28

Submit