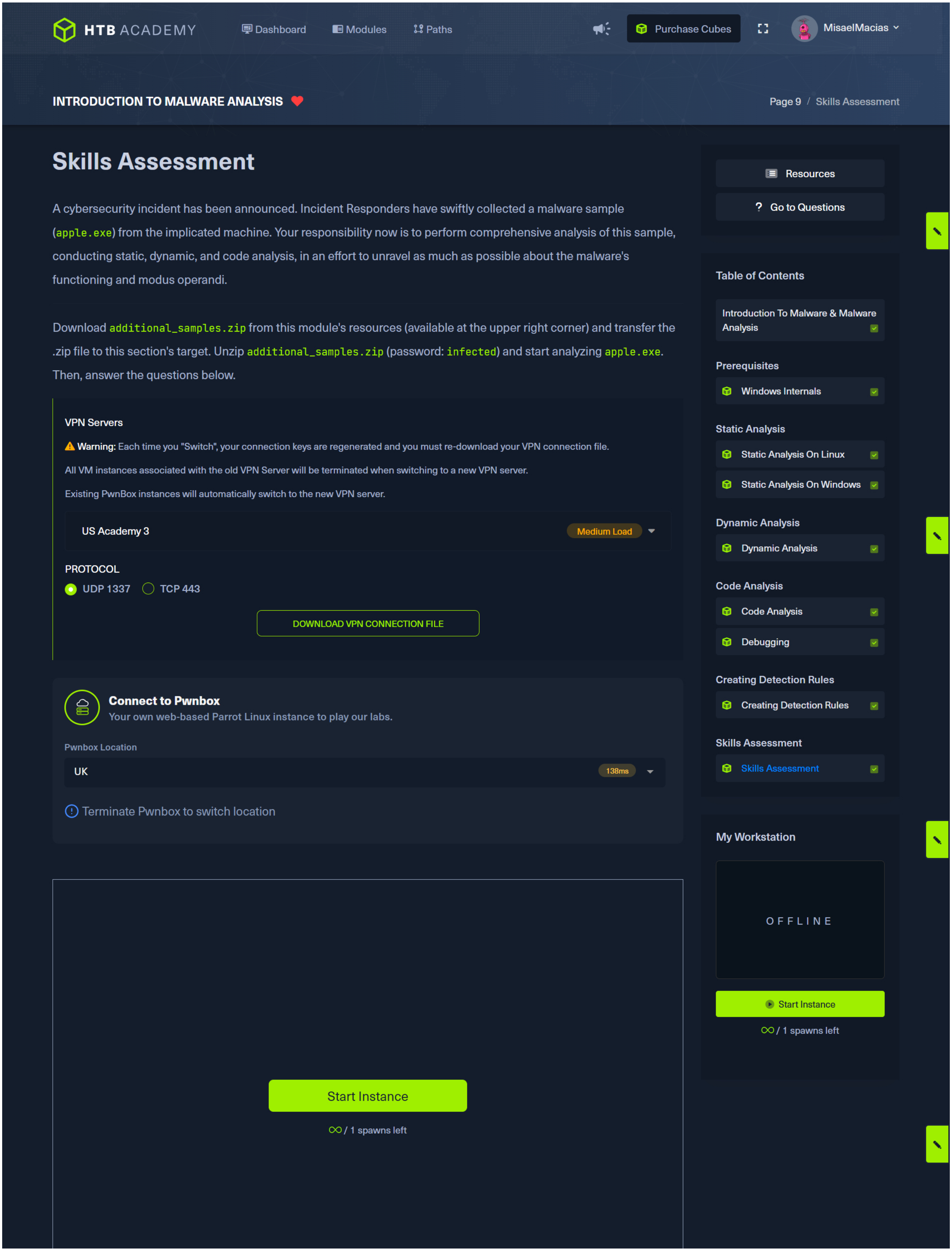


Skills Assessment

A cybersecurity incident has been announced. Incident Responders have swiftly collected a malware sample (`apple.exe`) from the implicated machine. Your responsibility now is to perform comprehensive analysis of this sample, conducting static, dynamic, and code analysis, in an effort to unravel as much as possible about the malware's functioning and modus operandi.

Download `additional_samples.zip` from this module's resources (available at the upper right corner) and transfer the .zip file to this section's target. Unzip `additional_samples.zip` (password: `infected`) and start analyzing `apple.exe`. Then, 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 — 138ms

ⓘ Terminate Pwnbox to switch location

Start Instance

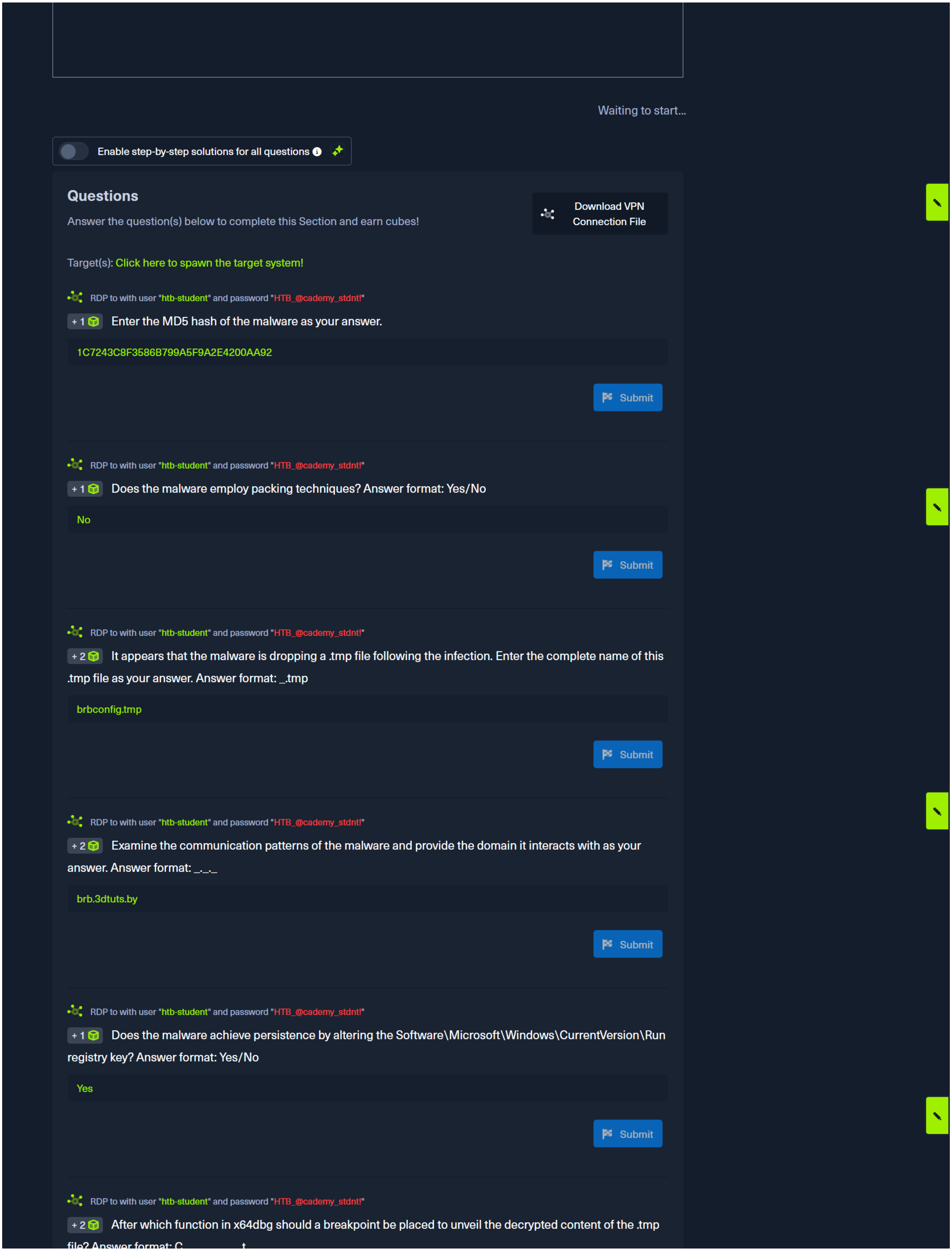
∞ / 1 spawns left

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!

Target(s): Click here to spawn the target system!

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

+ 1 Enter the MD5 hash of the malware as your answer.

1C7243C8F3586B799A5F9A2E4200AA92

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

+ 1 Does the malware employ packing techniques? Answer format: Yes/No

No

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

+ 2 It appears that the malware is dropping a .tmp file following the infection. Enter the complete name of this .tmp file as your answer. Answer format: _.tmp

brbconfig.tmp

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

+ 2 Examine the communication patterns of the malware and provide the domain it interacts with as your answer. Answer format: _._._

brb.3dtuts.by

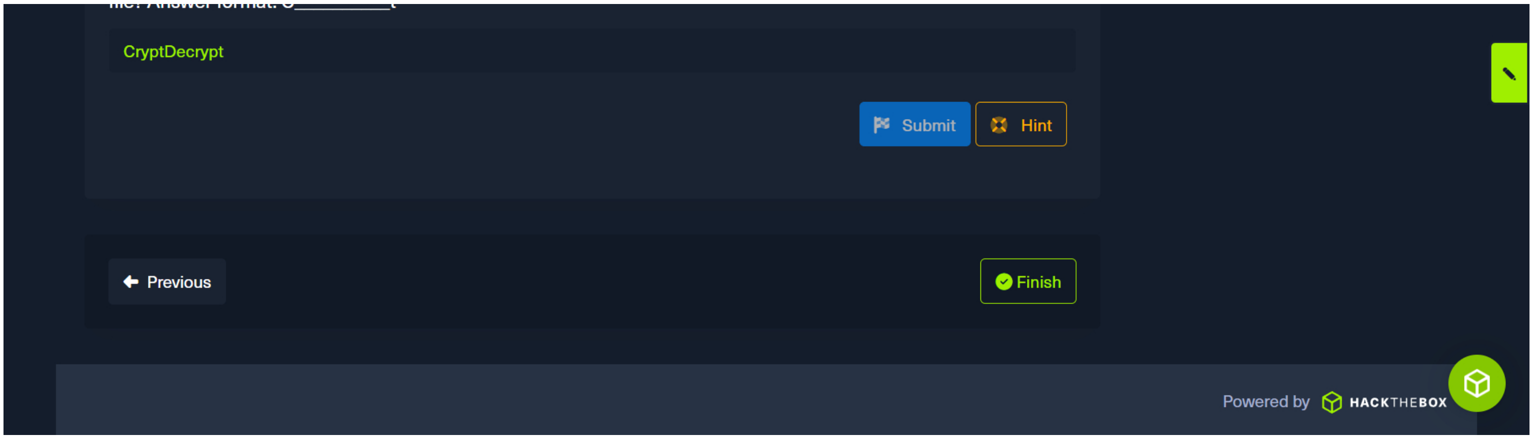
RDP to with user "htb-student" and password "HTB_@cademy_stdnt!"

+ 1 Does the malware achieve persistence by altering the Software\Microsoft\Windows\CurrentVersion\Run registry key? Answer format: Yes/No

Yes

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

+ 2 After which function in x64dbg should a breakpoint be placed to unveil the decrypted content of the .tmp file? Answer format: C t



file? Answer format: C_________t

CryptDecrypt