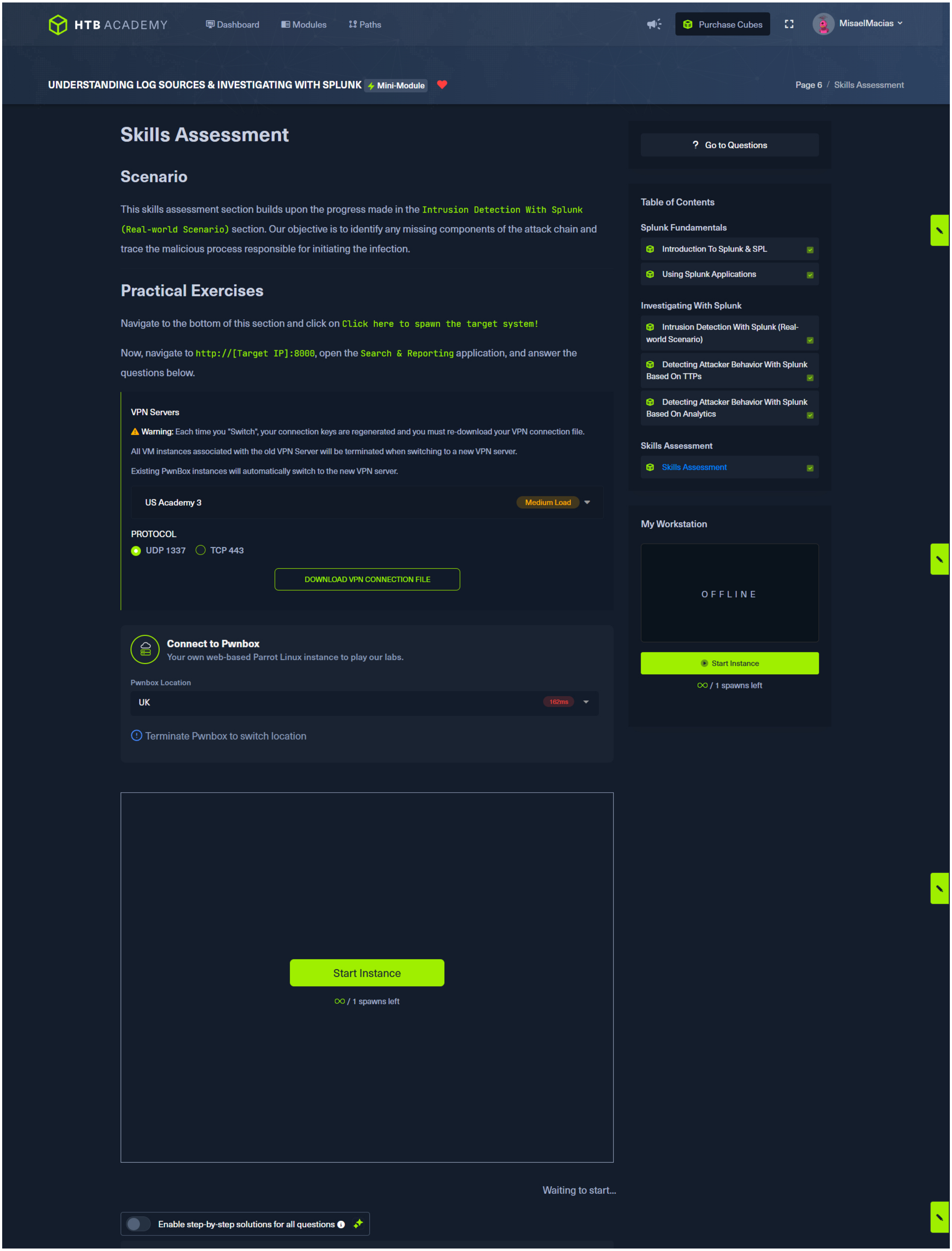


UNDERSTANDING LOG SOURCES & INVESTIGATING WITH SPLUNK Mini-Module

Skills Assessment

Scenario

This skills assessment section builds upon the progress made in the `Intrusion Detection With Splunk (Real-world Scenario)` section. Our objective is to identify any missing components of the attack chain and trace the malicious process responsible for initiating the infection.

Practical Exercises

Navigate to the bottom of this section and click on `Click here to spawn the target system!`

Now, navigate to `http://[Target IP]:8000`, open the `Search & Reporting` application, and 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

Connect to Pwnbox

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

Pwnbox Location

UK — 162ms

Terminate Pwnbox to switch location

Enable step-by-step solutions for all questions

Table of Contents

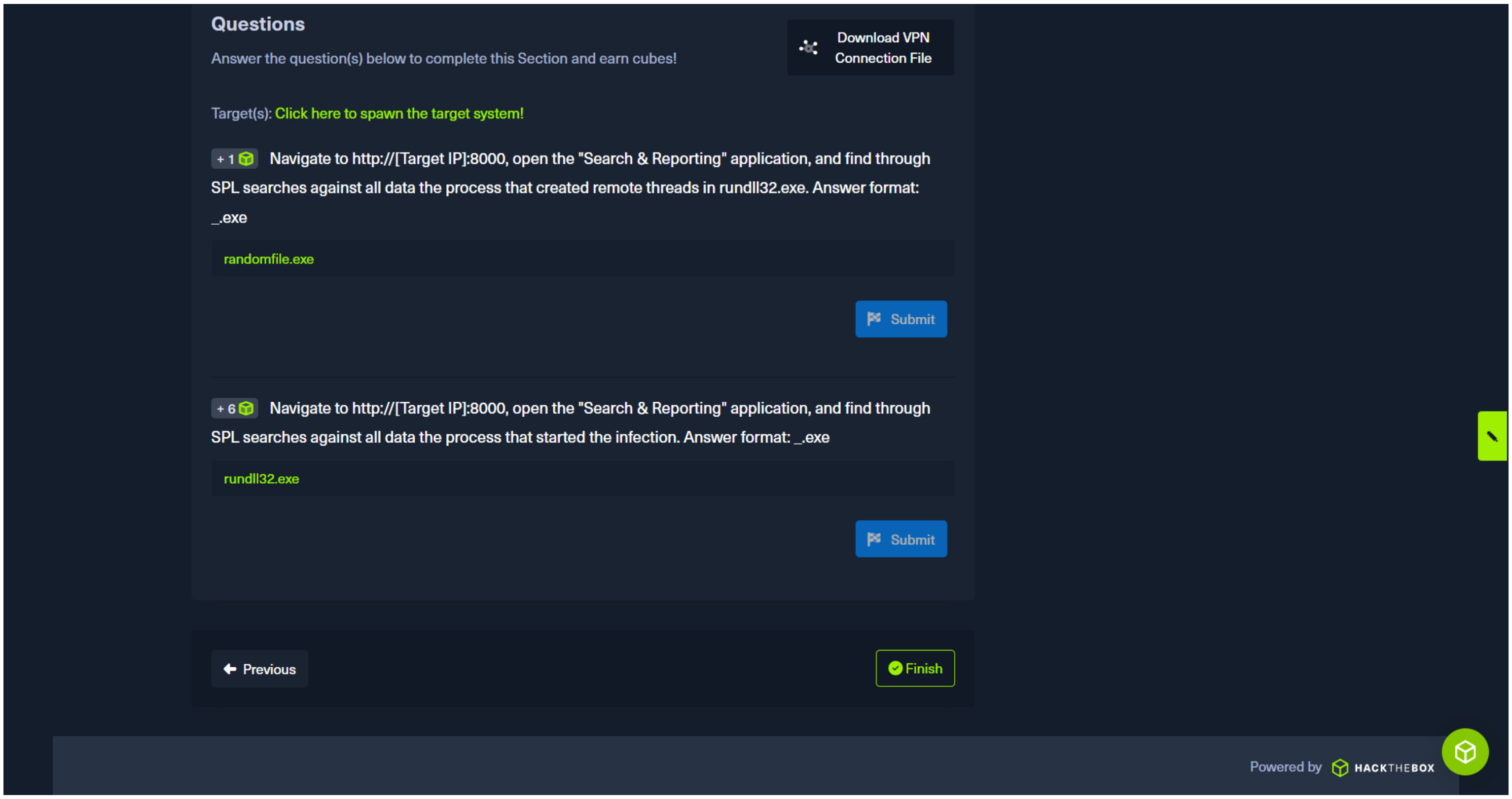
Splunk Fundamentals

Investigating With Splunk

Skills Assessment

My Workstation

OFFLINE



Questions

Answer the question(s) below to complete this Section and earn cubes!

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

+ 1 Navigate to http://[Target IP]:8000, open the "Search & Reporting" application, and find through SPL searches against all data the process that created remote threads in rundll32.exe. Answer format: _.exe

randomfile.exe

+ 6 Navigate to http://[Target IP]:8000, open the "Search & Reporting" application, and find through SPL searches against all data the process that started the infection. Answer format: _.exe

rundll32.exe