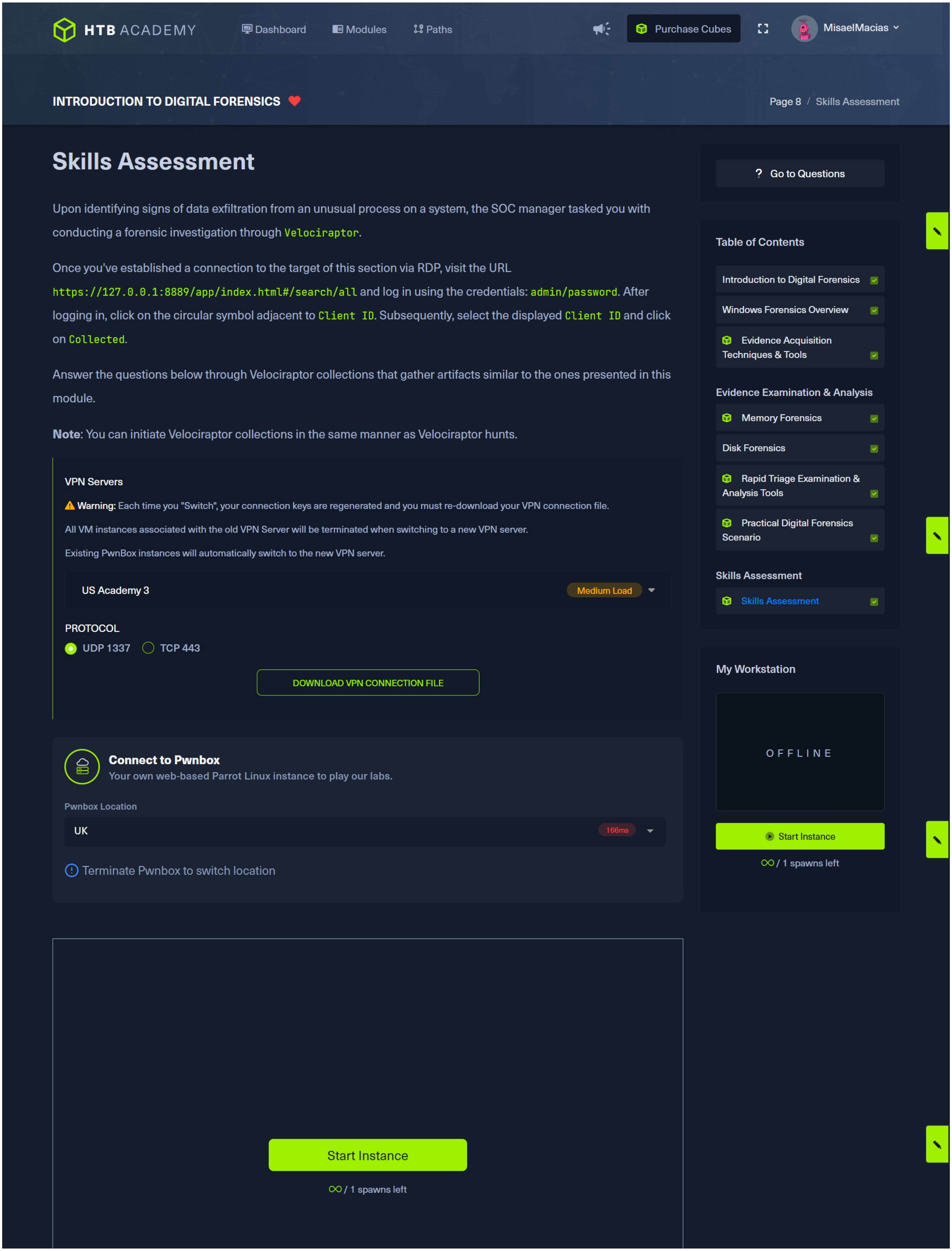


INTRODUCTION TO DIGITAL FORENSICS

Page 8 / Skills Assessment

Skills Assessment

Upon identifying signs of data exfiltration from an unusual process on a system, the SOC manager tasked you with conducting a forensic investigation through `Velociraptor`.

Once you've established a connection to the target of this section via RDP, visit the URL `https://127.0.0.1:8889/app/index.html#/search/all` and log in using the credentials: `admin/password`. After logging in, click on the circular symbol adjacent to `Client ID`. Subsequently, select the displayed `Client ID` and click on `Collected`.

Answer the questions below through Velociraptor collections that gather artifacts similar to the ones presented in this module.

Note: You can initiate Velociraptor collections in the same manner as Velociraptor hunts.

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

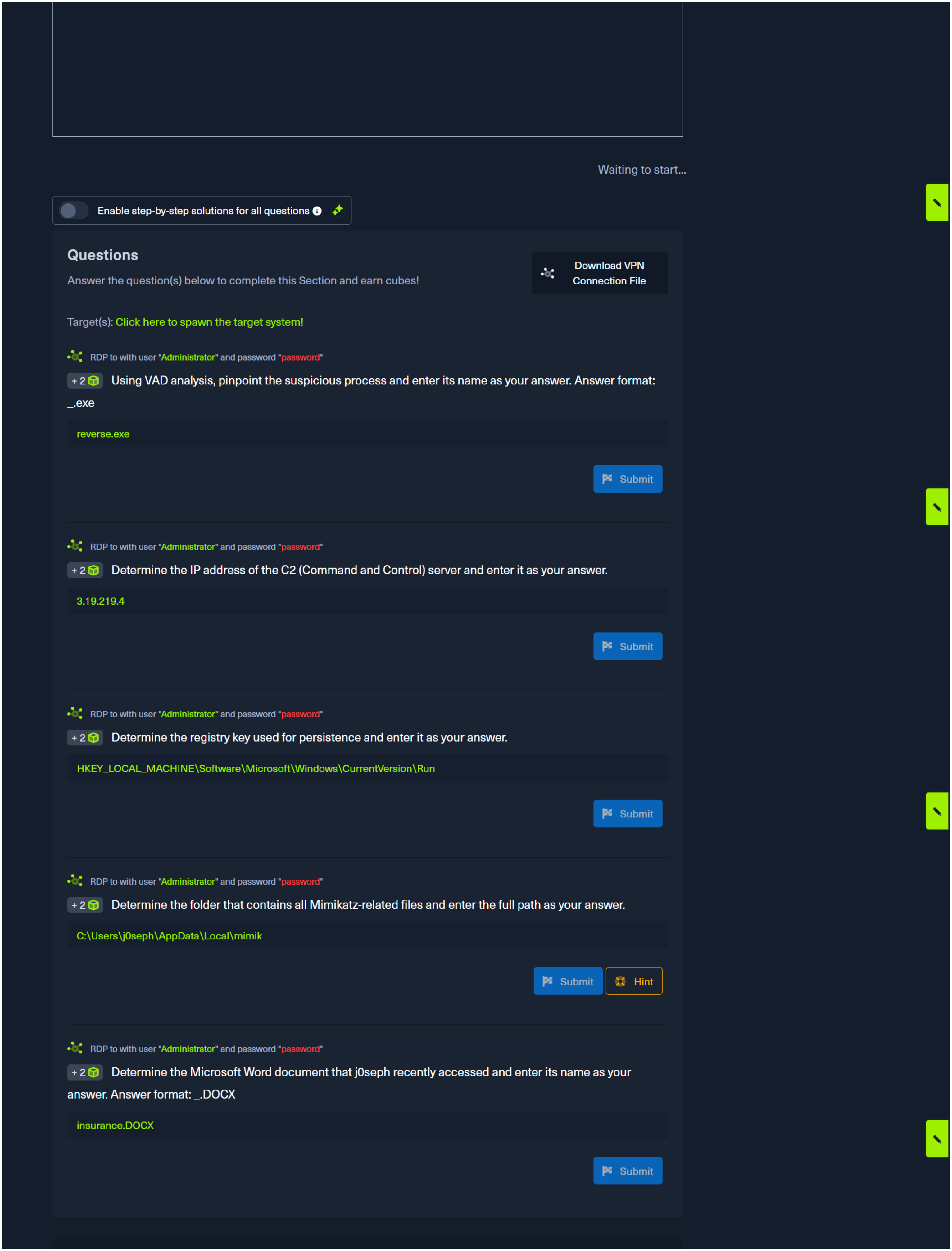
UK — 166ms

Terminate Pwnbox to switch location

Table of Contents

My Workstation

OFFLINE



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 "Administrator" and password "password"

+2 Using VAD analysis, pinpoint the suspicious process and enter its name as your answer. Answer format: _.exe

reverse.exe

Submit

RDP to with user "Administrator" and password "password"

+2 Determine the IP address of the C2 (Command and Control) server and enter it as your answer.

3.19.219.4

Submit

RDP to with user "Administrator" and password "password"

+2 Determine the registry key used for persistence and enter it as your answer.

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run

Submit

RDP to with user "Administrator" and password "password"

+2 Determine the folder that contains all Mimikatz-related files and enter the full path as your answer.

C:\Users\j0seph\AppData\Local\mimik

Submit Hint

RDP to with user "Administrator" and password "password"

+2 Determine the Microsoft Word document that j0seph recently accessed and enter its name as your answer. Answer format: _.DOCX

insurance.DOCX

Submit

Previous
Finish
Powered by HACKTHEBOX