## DETECTING WINDOWS ATTACKS WITH SPLUNK



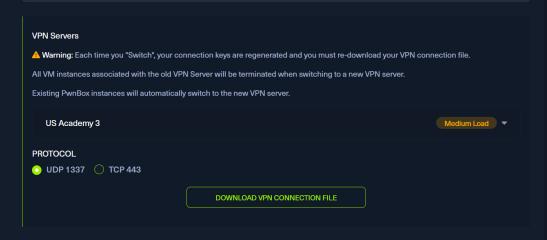
Page 23 / Skills Assessment

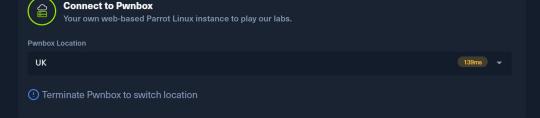
## **Skills Assessment**

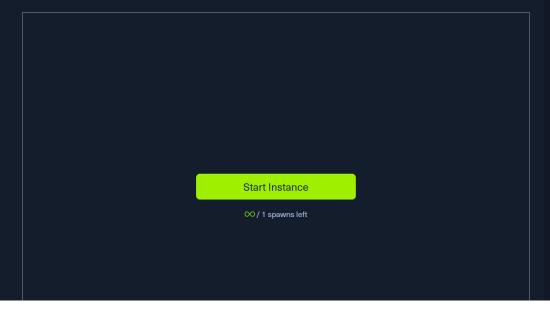
This module's skills assessment involves identifying malicious activity using Splunk and Zeek logs.

In many instances, the solution can be discovered by simply viewing the events in each index, as the number of events is limited. However, please take the time to refine your Splunk searches to achieve a better understanding.

Let's now navigate to the bottom of this section and click on "Click here to spawn the target system!". Then, access the Splunk interface at https://[Target IP]:8000 and launch the Search & Reporting Splunk application to answer the questions below.









**69** Detecting Golden Tickets Detecting Cobalt Strike's

Detecting Zerologon

Detecting Exfiltration (HTTP) 
■

Detecting Exfiltration (DNS)

Detecting Ransomware

Skills Assessment

**PSExec** 

