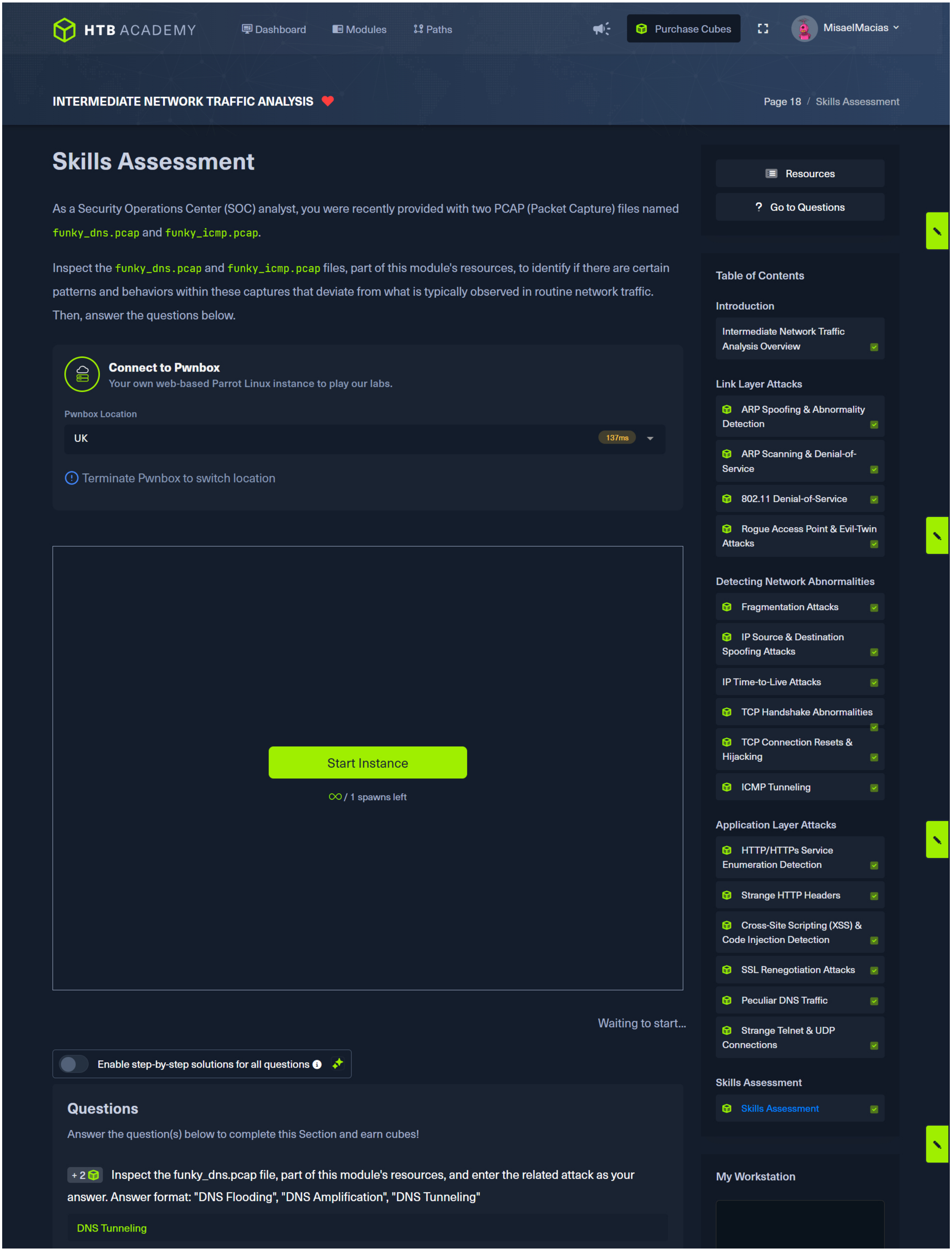

HTB ACADEMY
Dashboard
Modules
Paths
Purchase Cubes
MisaelMacias
INTERMEDIATE NETWORK TRAFFIC ANALYSIS
Page 18 / Skills Assessment

Skills Assessment

As a Security Operations Center (SOC) analyst, you were recently provided with two PCAP (Packet Capture) files named `funky_dns.pcap` and `funky_icmp.pcap`.

Inspect the `funky_dns.pcap` and `funky_icmp.pcap` files, part of this module's resources, to identify if there are certain patterns and behaviors within these captures that deviate from what is typically observed in routine network traffic. Then, answer the questions below.

Connect to Pwnbox

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

Pwnbox Location

UK 137ms

Terminate Pwnbox to switch location

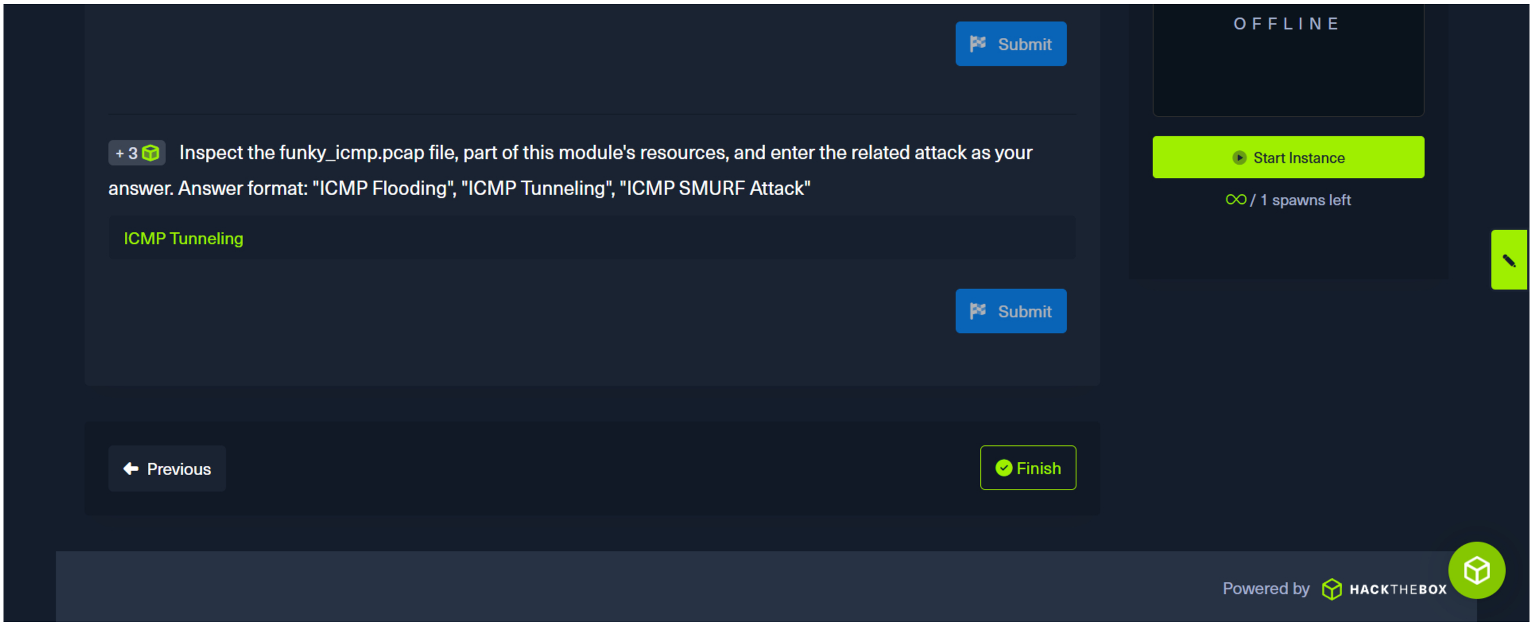
Questions

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

+ 2 Inspect the funky_dns.pcap file, part of this module's resources, and enter the related attack as your answer. Answer format: "DNS Flooding", "DNS Amplification", "DNS Tunneling"

DNS Tunneling

My Workstation



+3 Inspect the funky_icmp.pcap file, part of this module's resources, and enter the related attack as your answer. Answer format: "ICMP Flooding", "ICMP Tunneling", "ICMP SMURF Attack"

ICMP Tunneling