Netsec Lab 3

by Vaughn Valle

Q1.1 Snort

Snort is an open-source, rule-based Network IDS/IPS

What is an IDS?

- IDS is a passive monitoring solution for detecting malicious activities
- If a signature is identified, an alert is created
    - Types
        - NIDS
            - monitor traffic flow on entire subnet
        - HIDS
            - monitor traffic flow from single endpoint

What is an IPS?

- IPS is an active protecting solution to terminate an event as soon as detection is performed
- If a signature is identified, the conn is terminated

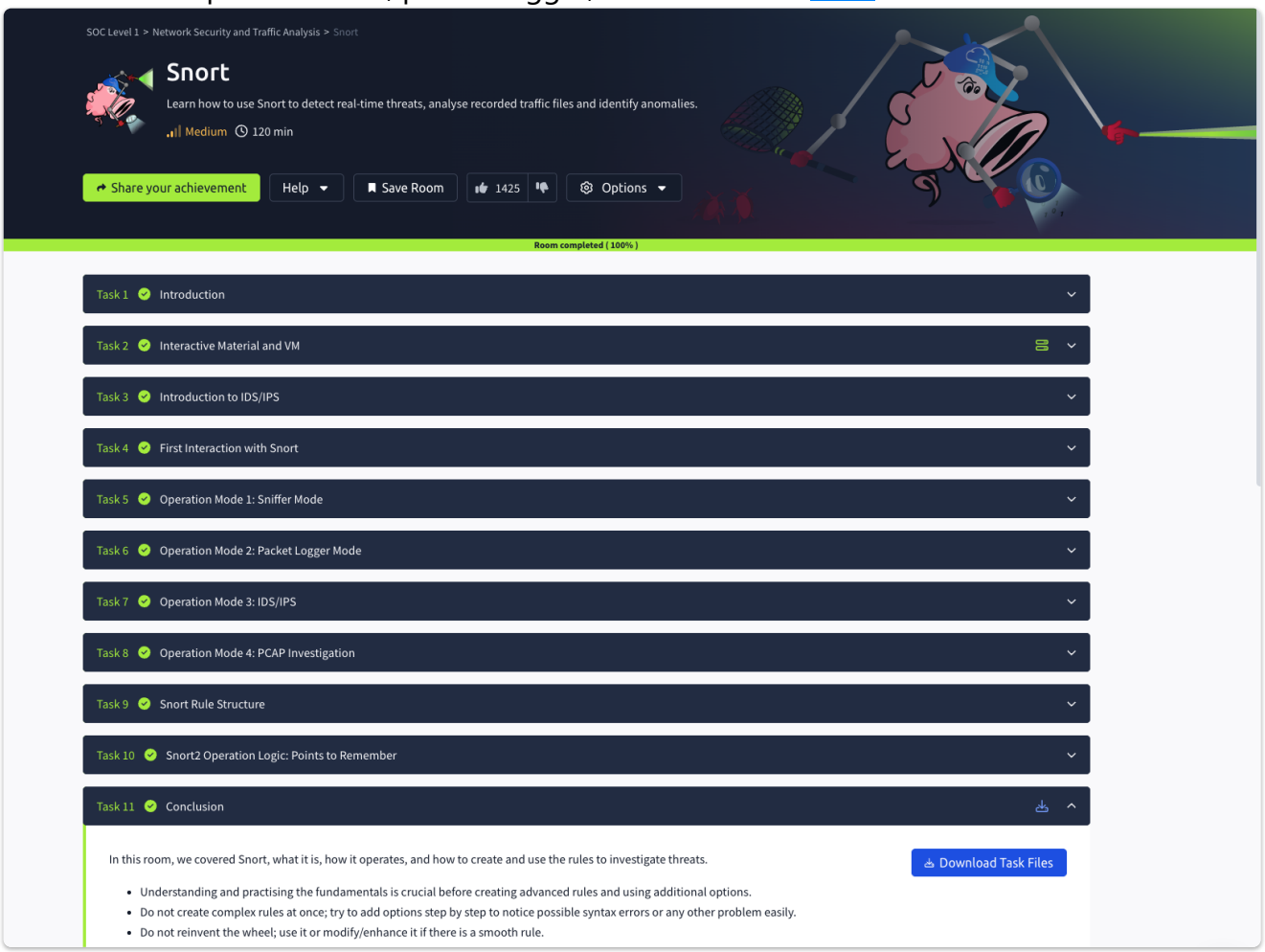
Types:
- NIPS
- protect traffic on entire subnet
- NBA
- similar to NIPS but requires a training period (baselining) to differentiate normal vs malicious, more efficient results
- WIPS
- protect wireless traffic
- HIPS
- protect traffic on an endpoint

Detection/Prevention Techniques

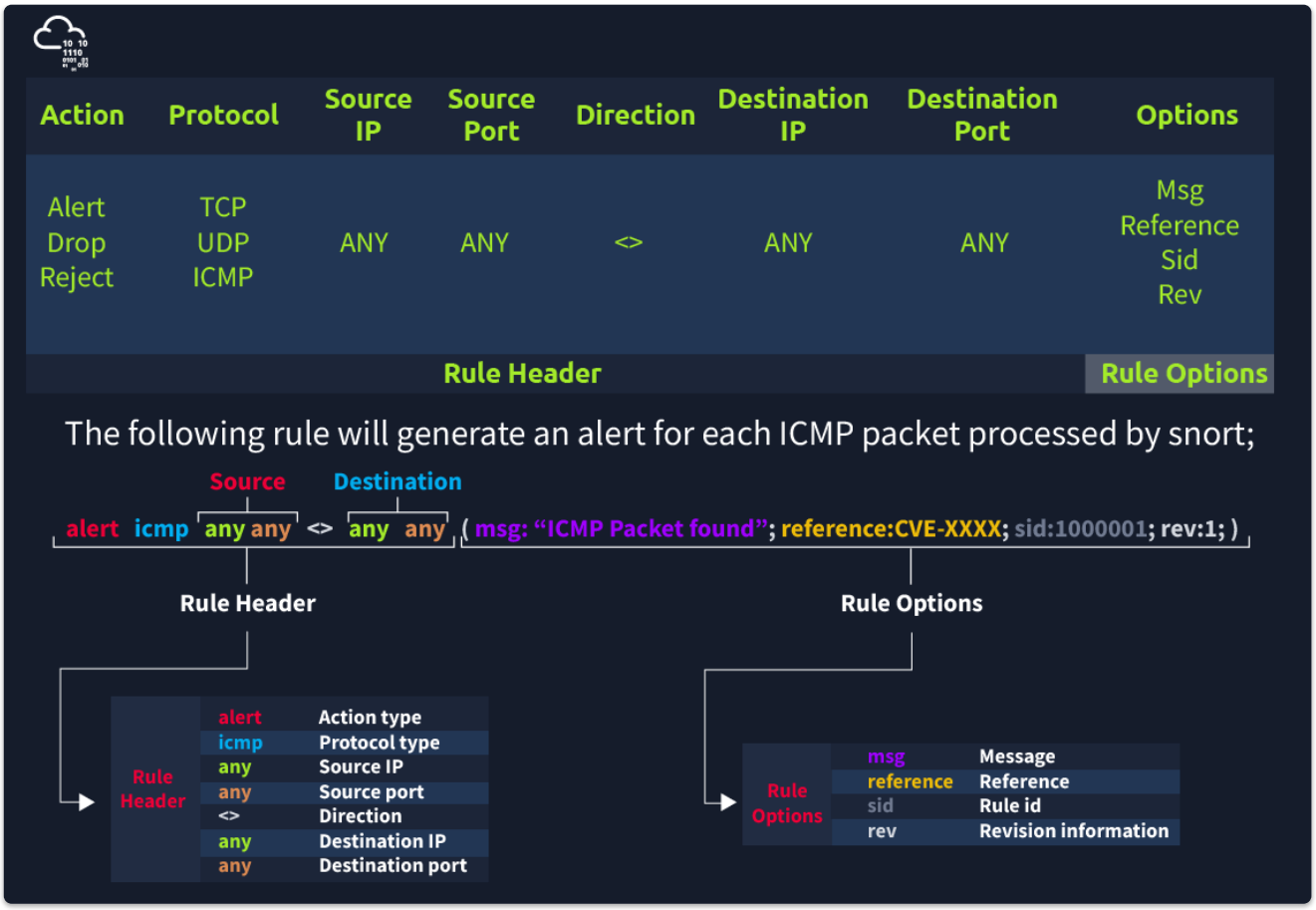
1. Signature-based
    1. identify specific patterns of known malicious behavior
2. Behaviour-based
    1. identify new threat with new patterns that pass signatures
3. Policy-based

1. identify activities by comparing them with config and sys policies

Snort can be a packet sniffer, packet logger, or a full-blown NIPS

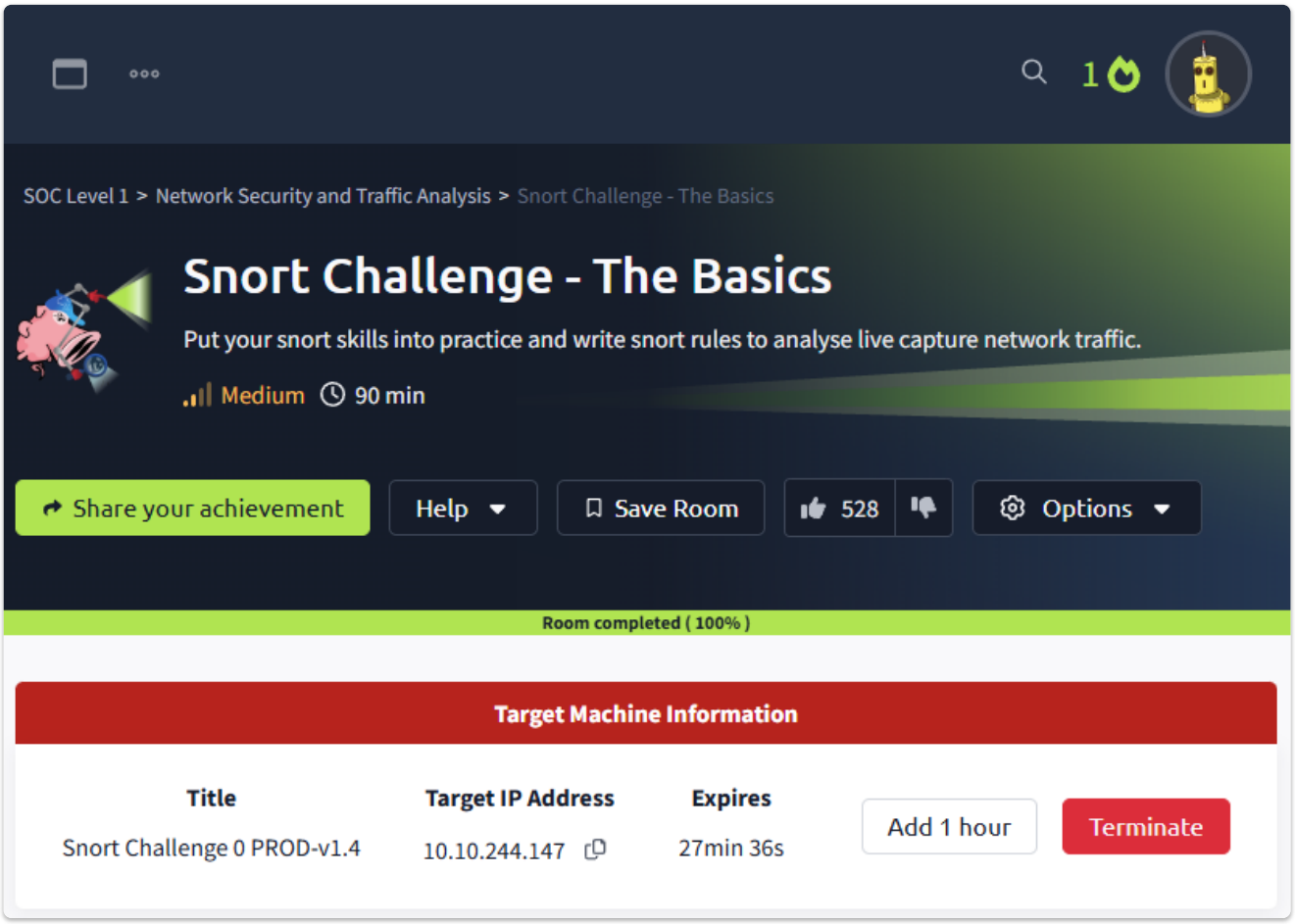


Snort Rule structure



[Snort Usage]

Q1.2 Snort Challenges



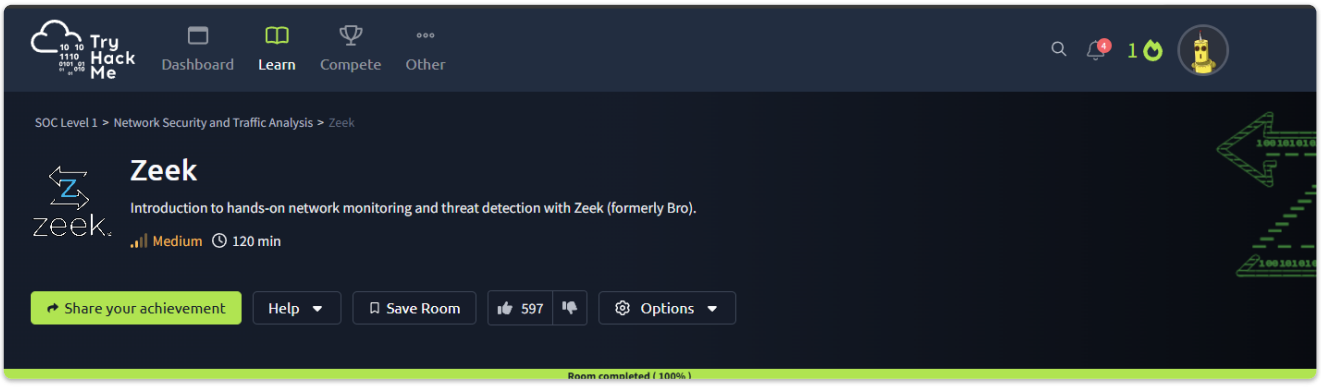
This lab was very fun as it doubled down on using snort to analyze real world traffic. At the end, I was able to use snort to analyze `pcap` files to investigate real world exploits and vulnerabilities

Q3 ZeekBro

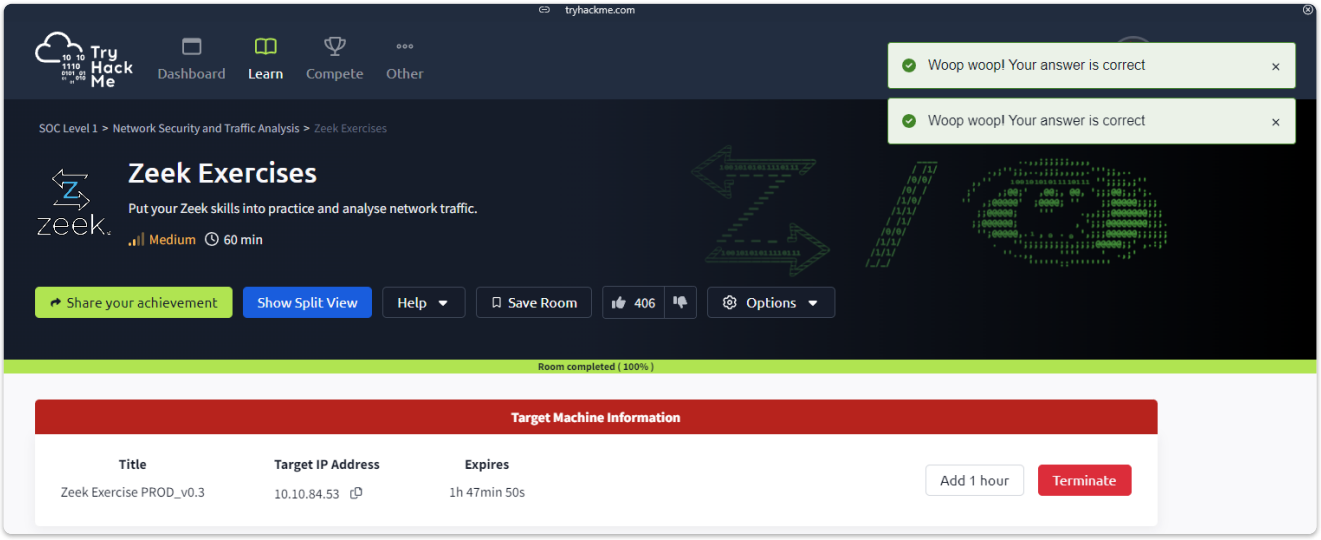
Zeek

Zeek is a passive open-source traffic analyzer and is mainly used as a network security monitor (NSM)

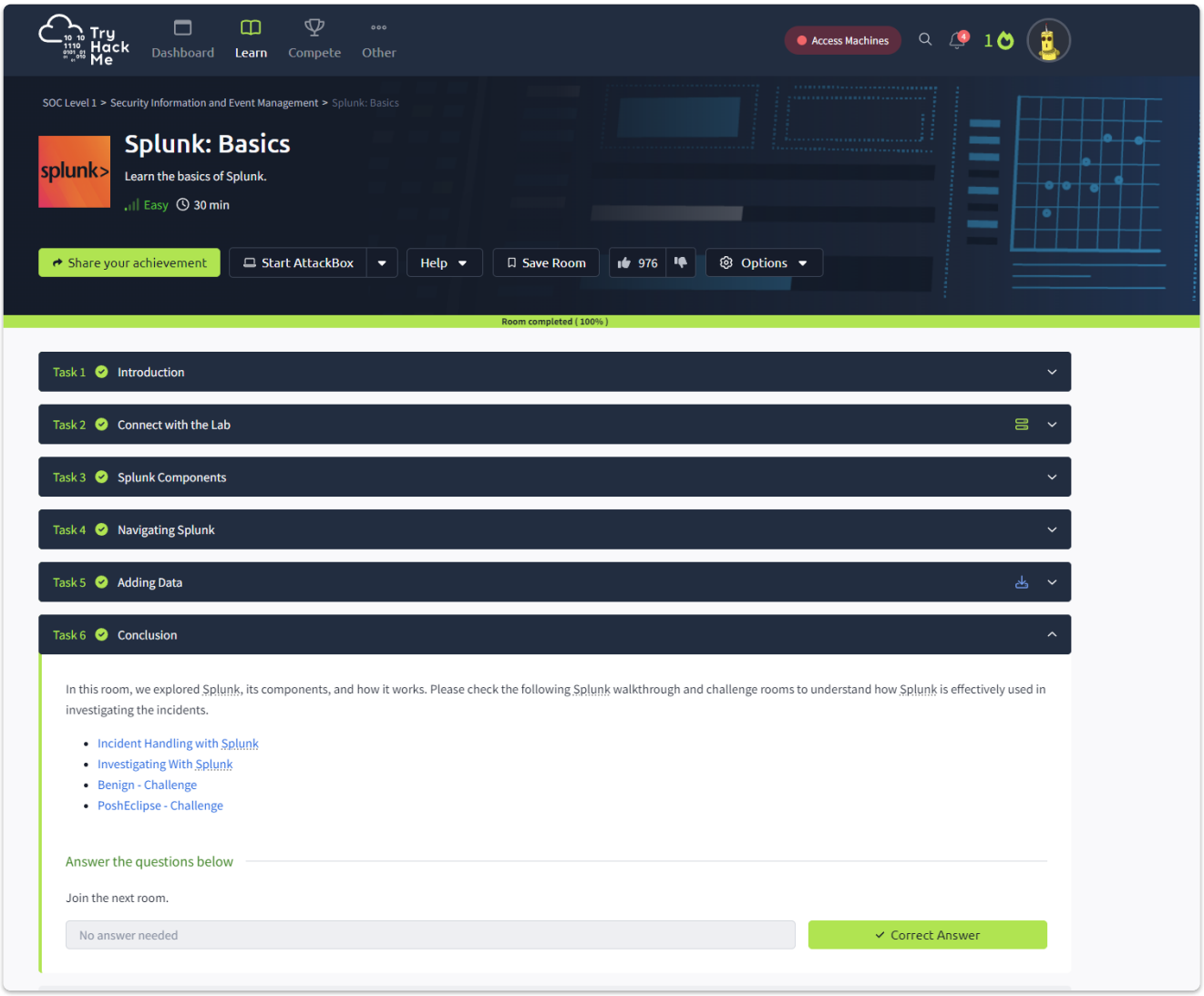
Zeek vs Snort



Q3.2 Zeekbro Exercises



Q4 Splunk



Splunk is one of the leading SIEM solutions in the market that provides the ability to collect, analyze and correlate the network and machine logs in real-time.

Splunk has three main components, namely Forwarder, Indexer, and Search Head. These components are explained below:

Forwarder

Splunk Forwarder is a lightweight agent installed on the endpoint intended to be monitored, and its main task is to collect the data and send it to the Splunk instance

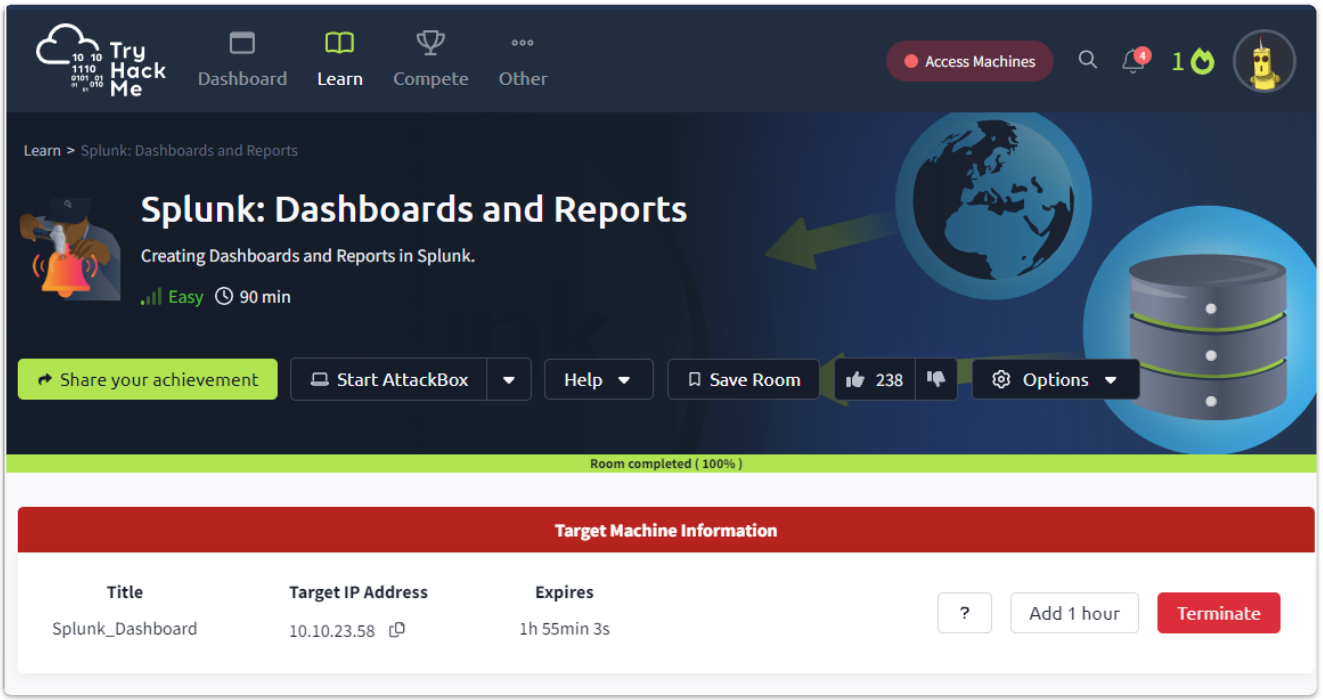
Indexer

Splunk Indexer plays the main role in processing the data it receives from forwarders. It takes the data, normalizes it into field-value pairs, determines the datatype of the data, and stores them as events. Processed data is easy to search and analyze.

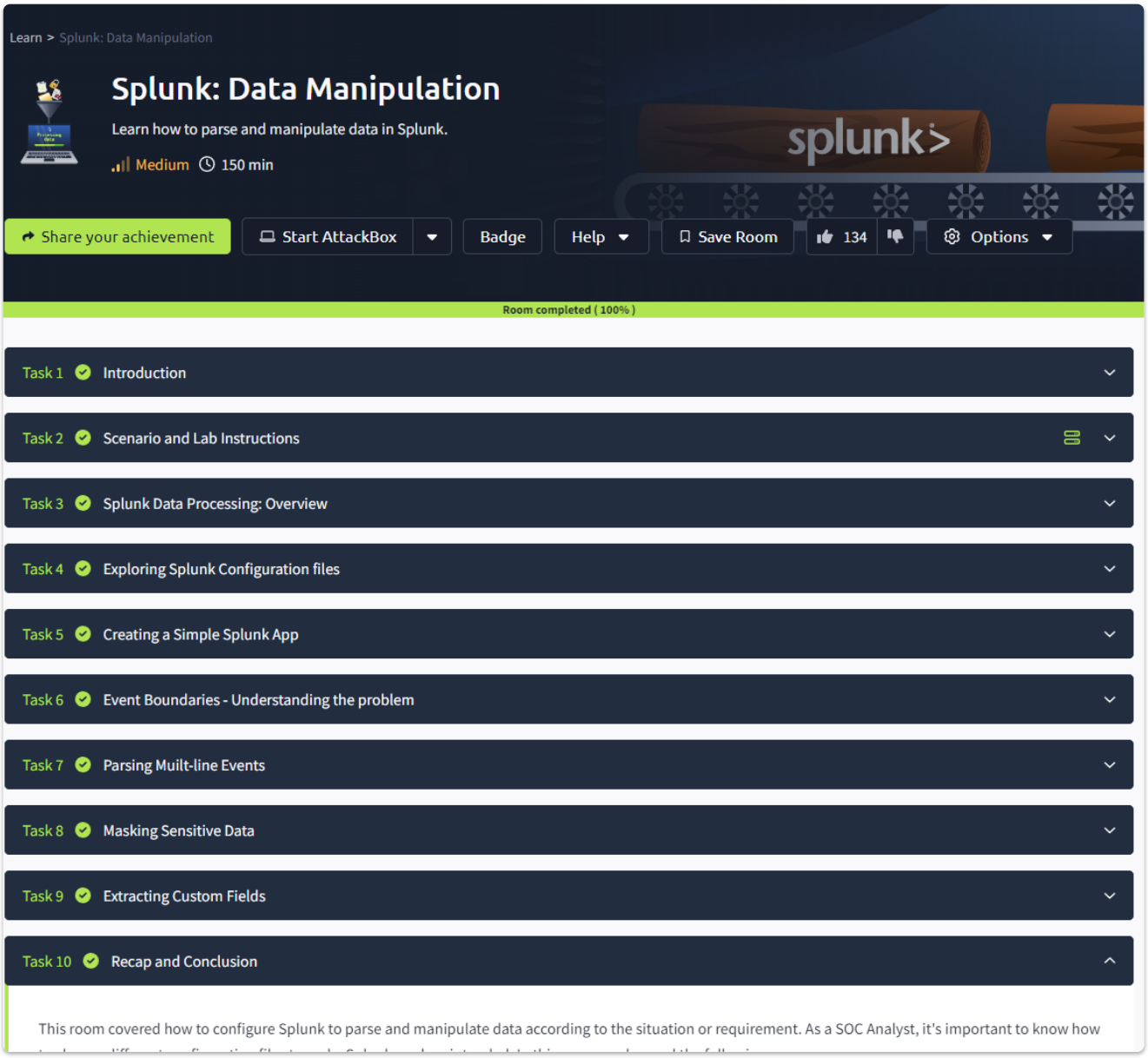
Search Head

Splunk Search Head is the place within the Search & Reporting App where users can search the indexed logs as shown below. When the user searches for a term or uses a Search language known as Splunk Search Processing Language, the request is sent to the indexer and the relevant events are returned in the form of field-value pairs.

Q4.1 Splunk Dashboard and Reports



Q4.2 Splunk Data Manipulation



Q5 Lab Write-up

I recently completed the labs to learn more about tools like Snort, Zeek, and Splunk: how they are set up and used for network analysis. The labs provided hands-on experience with these tools and helped me understand how they can be used for network intrusion detection and log analysis.

Challenges Encountered

- Snort: Configuring Snort rules to accurately detect malicious traffic while minimizing false positives was a challenge especially with the plethora of rules and combinations
- Zeek: Understanding the Zeek scripting language and writing scripts to analyze network traffic was hard to remember for me
- Splunk: The dashboard was intuitive but at first, learning the Splunk search language and creating dashboards to visualize log data had a learning curve

Key Learnings

- Network Intrusion Detection:
  - Snort is a powerful tool for detecting malicious network traffic since it can be a packet sniffer, packet logger, and even a full blown network IPS
  - Snort is very rule-based heavy
  - Zeek on the other hand is a passive open-source traffic analyzer used as an NSM
  - Zeek is a flexible tool that allows for more complex analysis of network traffic using scripts instead of Snort Rules
- Log Analysis:
  - Splunk is a powerful tool for collecting, analyzing, and visualizing log data.
  - Log analysis can be used to identify security threats, troubleshoot issues, and comply with regulations on networks we manage.