

# 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](#)

SOC Level 1 > Network Security and Traffic Analysis > Snort

## Snort

Learn how to use Snort to detect real-time threats, analyse recorded traffic files and identify anomalies.

Medium 120 min

Share your achievement Help Save Room 1425 Options

Room completed (100%)

Task 1 Introduction

Task 2 Interactive Material and VM

Task 3 Introduction to IDS/IPS

Task 4 First Interaction with Snort

Task 5 Operation Mode 1: Sniffer Mode

Task 6 Operation Mode 2: Packet Logger Mode

Task 7 Operation Mode 3: IDS/IPS

Task 8 Operation Mode 4: PCAP Investigation

Task 9 Snort Rule Structure

Task 10 Snort2 Operation Logic: Points to Remember

Task 11 Conclusion

In this room, we covered Snort, what it is, how it operates, and how to create and use the rules to investigate threats.

Download Task Files

- Understanding and practising the fundamentals is crucial before creating advanced rules and using additional options.
- Do not create complex rules at once; try to add options step by step to notice possible syntax errors or any other problem easily.
- Do not reinvent the wheel; use it or modify/enhance it if there is a smooth rule.

## Snort Rule structure

10.10.1110  
00000000  
00000000

Action	Protocol	Source IP	Source Port	Direction	Destination IP	Destination Port	Options
Alert	TCP	ANY	ANY	<>	ANY	ANY	Msg
Drop	UDP						Reference
Reject	ICMP						Sid
							Rev

**Rule Header**
**Rule Options**

The following rule will generate an alert for each ICMP packet processed by snort;

```

alert icmp any any <> any any { msg: "ICMP Packet found"; reference: CVE-XXXX; sid: 1000001; rev: 1; }
  
```

**Rule Header**

alert	Action type
icmp	Protocol type
any	Source IP
any	Source port
<>	Direction
any	Destination IP
any	Destination port

**Rule Options**

msg	Message
reference	Reference
sid	Rule id
rev	Revision information

[Snort Usage](#)

## Q1.2 Snort Challenges

...

🔍

1

SOC Level 1 > Network Security and Traffic Analysis > Snort Challenge - The Basics

## Snort Challenge - The Basics

Put your snort skills into practice and write snort rules to analyse live capture network traffic.

Medium

🕒 90 min

🔄 Share your achievement

📖 Help ▾

🔖 Save Room

👍 528

🗨

⚙️ Options ▾

Room completed ( 100% )

Target Machine Information

Title	Target IP Address	Expires		
Snort Challenge 0 PROD-v1.4	10.10.244.147 📄	27min 36s	Add 1 hour	Terminate

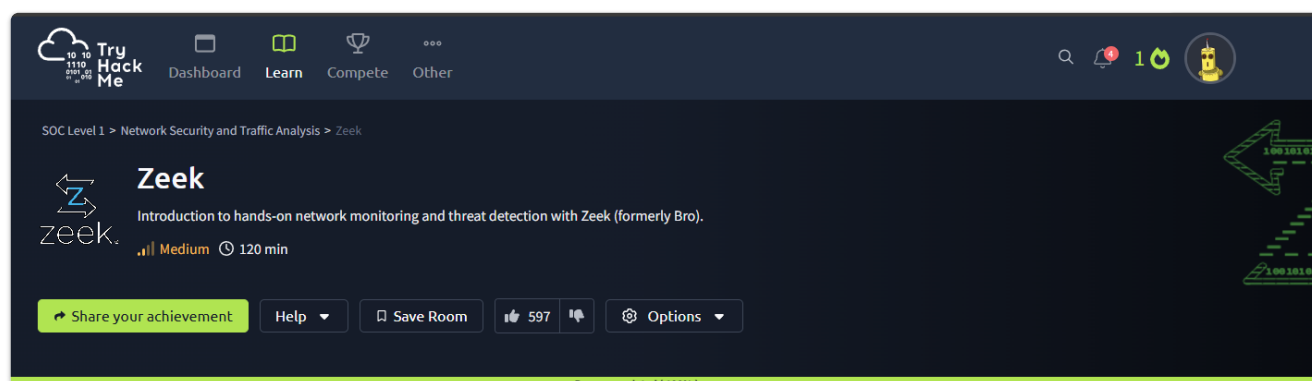
This lab was very fun as it doubled down on using snort to analyze real world traffic. At the end, I was able to use snort to analyze `pcap` files to investigate real world exploits and vulnerabilities

## Q3 ZeekBro

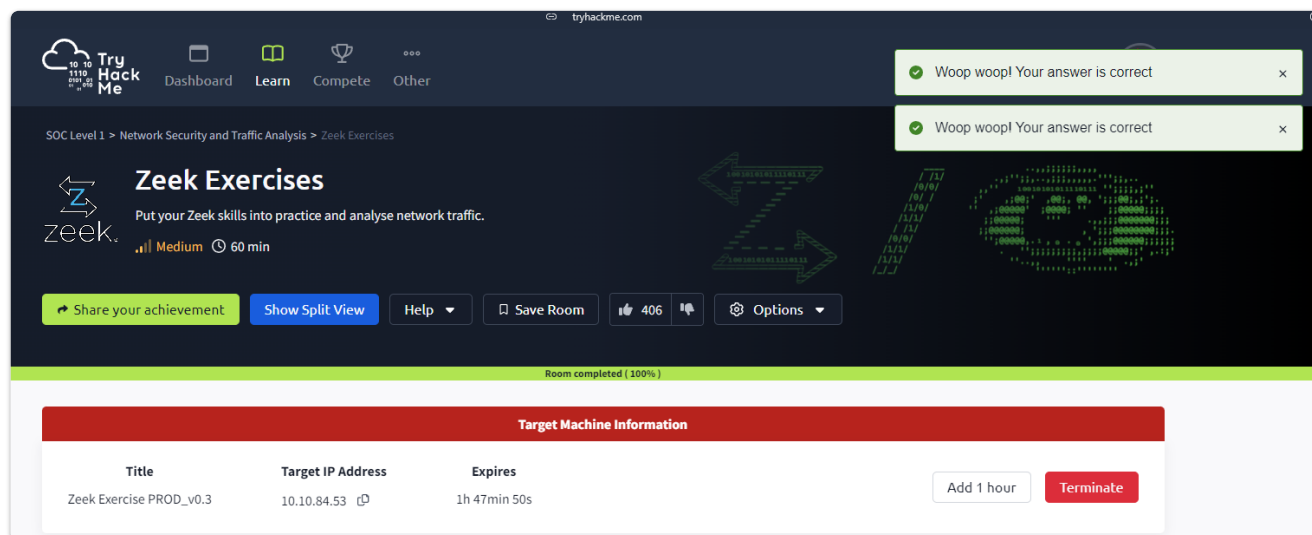
### Zeek

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

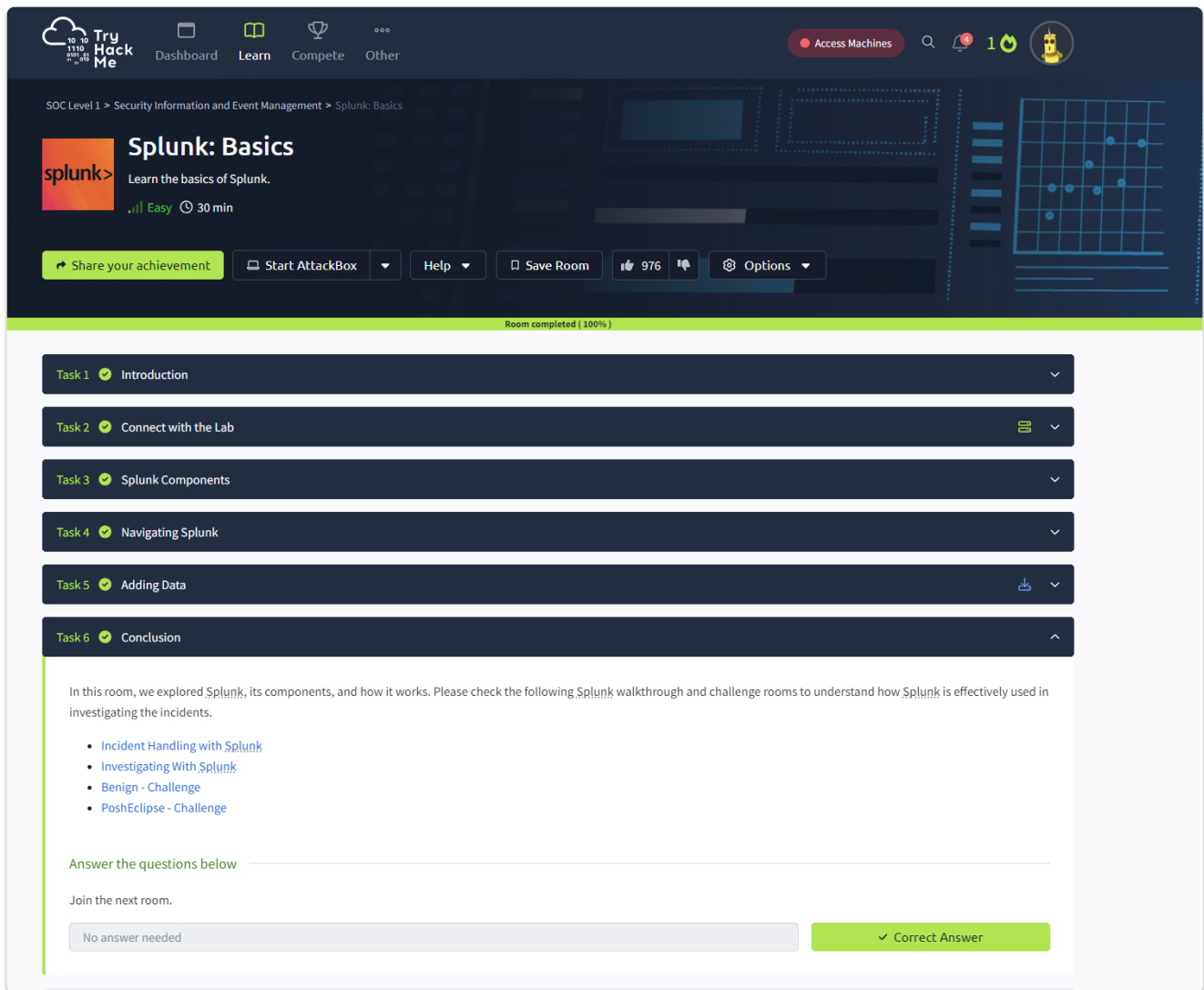
### Zeek vs Snort



## 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

The screenshot shows the TryHackMe interface for the 'Splunk: Dashboards and Reports' room. The top navigation bar includes 'Dashboard', 'Learn', 'Compete', and 'Other' tabs, along with an 'Access Machines' button and a search icon. The room title 'Splunk: Dashboards and Reports' is prominently displayed, followed by the subtitle 'Creating Dashboards and Reports in Splunk.' and a difficulty level of 'Easy' with a 90-minute timer. A green progress bar indicates 'Room completed (100%)'. Below this, a red header section titled 'Target Machine Information' contains a table with the following data:

Title	Target IP Address	Expires	
Splunk_Dashboard	10.10.23.58	1h 55min 3s	<div><span>?</span> <span>Add 1 hour</span> <span>Terminate</span></div>

## Q4.2 Splunk Data Manipulation

Learn > Splunk: Data Manipulation

## Splunk: Data Manipulation

Learn how to parse and manipulate data in Splunk.

Medium 150 min

Share your achievement Start AttackBox Badge Help Save Room 134 Options

Room completed ( 100% )

- Task 1 Introduction
- Task 2 Scenario and Lab Instructions
- Task 3 Splunk Data Processing: Overview
- Task 4 Exploring Splunk Configuration files
- Task 5 Creating a Simple Splunk App
- Task 6 Event Boundaries - Understanding the problem
- Task 7 Parsing Mult-line Events
- Task 8 Masking Sensitive Data
- Task 9 Extracting Custom Fields
- Task 10 Recap and Conclusion

This room covered how to configure Splunk to parse and manipulate data according to the situation or requirement. As a SOC Analyst, it's important to know how

## 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.