# **Snort**

#### **EX-NO:13**

# AIM:

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

#### PROCEDURE:

- 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

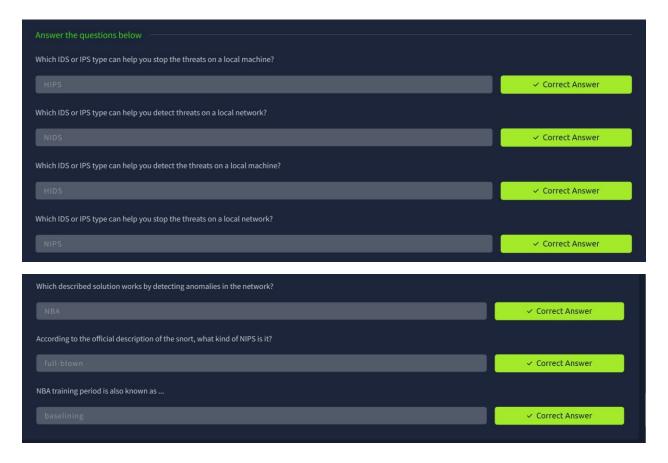
# Task 1 Introduction:



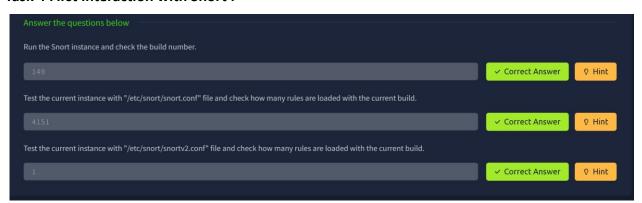
# Task 2 Interactive Material and VM:



Task 3 Introduction to IDS/IPS:



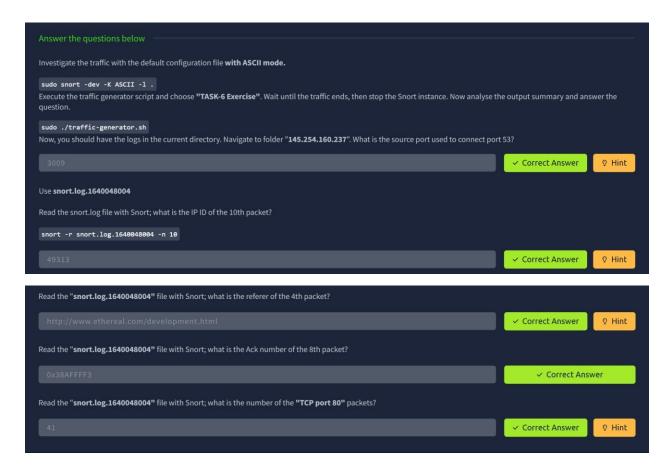
#### Task 4 First Interaction with Snort:



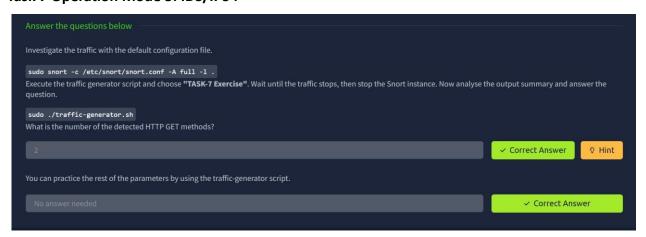
Task 5 Operation Mode 1: Sniffer Mode:



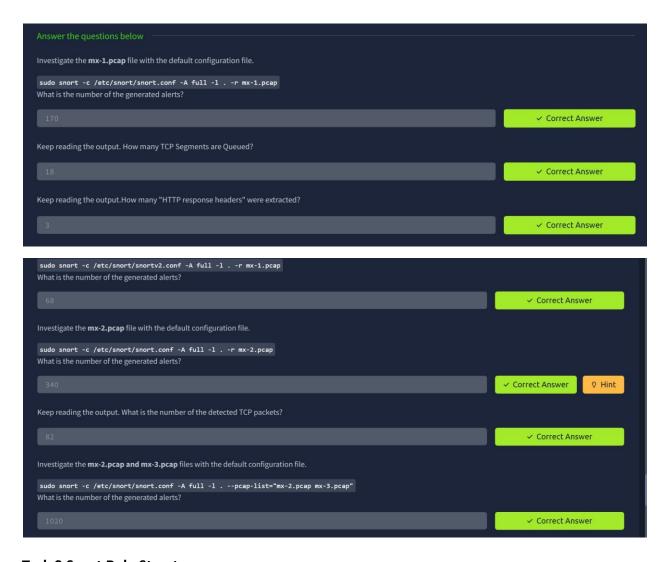
Task 6 Operation Mode 2: Packet Logger Mode:



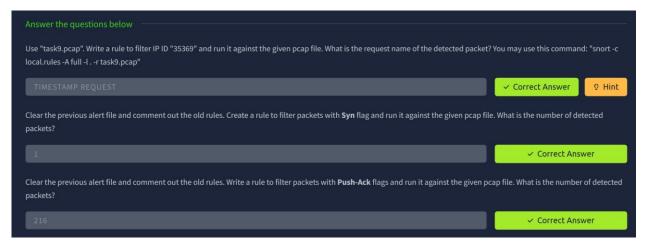
# Task 7 Operation Mode 3: IDS/IPS:

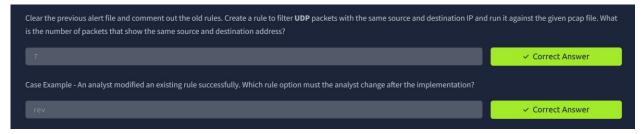


Task 8 Operation Mode 4: PCAP Investigation:



# Task 9 Snort Rule Structure:





# Task 10 Snort2 Operation Logic: Points to Remember:



# Task 11 Conclusion:



# **RESULT:**

Thus the Snort is completed using tryhackme platform.