EX.NO:13 **NAME:KALAIYARASI.M**

DATE:17/4/25 **ROLLNO:231901503**

Snort

AIM:

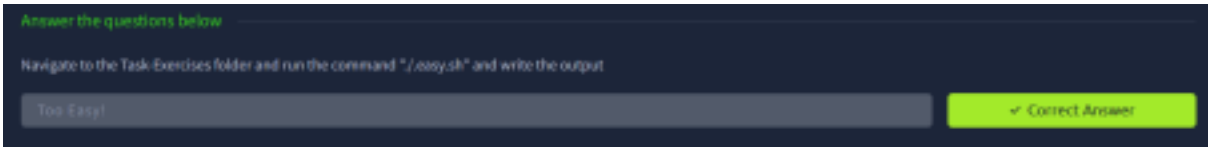
To learn how to use Snort to detect real-time threats, analyse recorded traffic files and identify anomalies.

PROCEDURE:

Complete the given task as per the instructions.

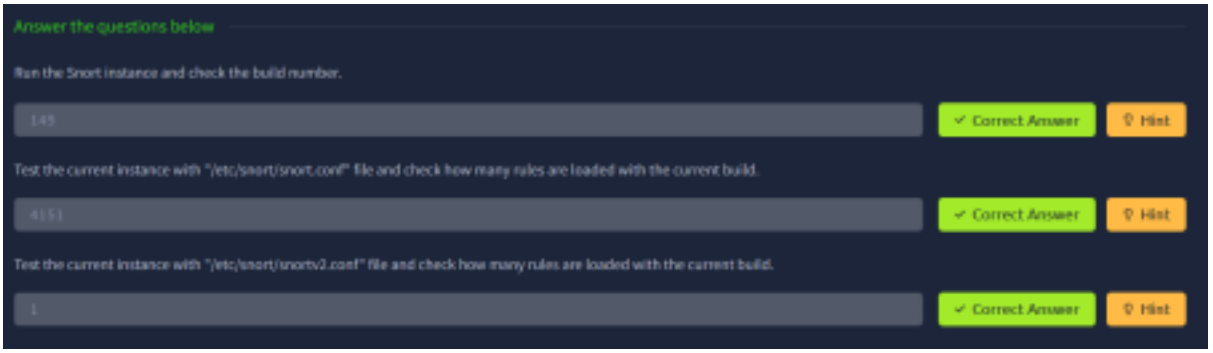
Task 1:Introduction

Task 2:Interactive Material and VM



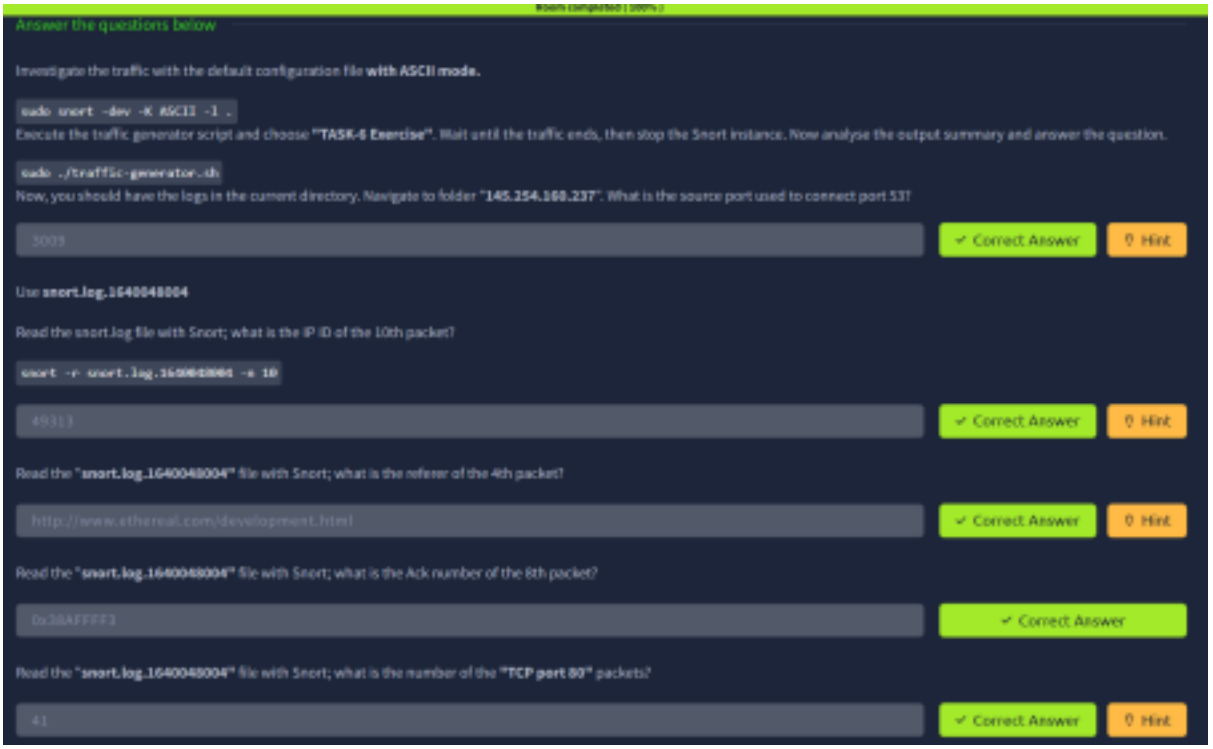
Task 3:Introduction to IDS/IPS

Task 4:First Interaction with Snort



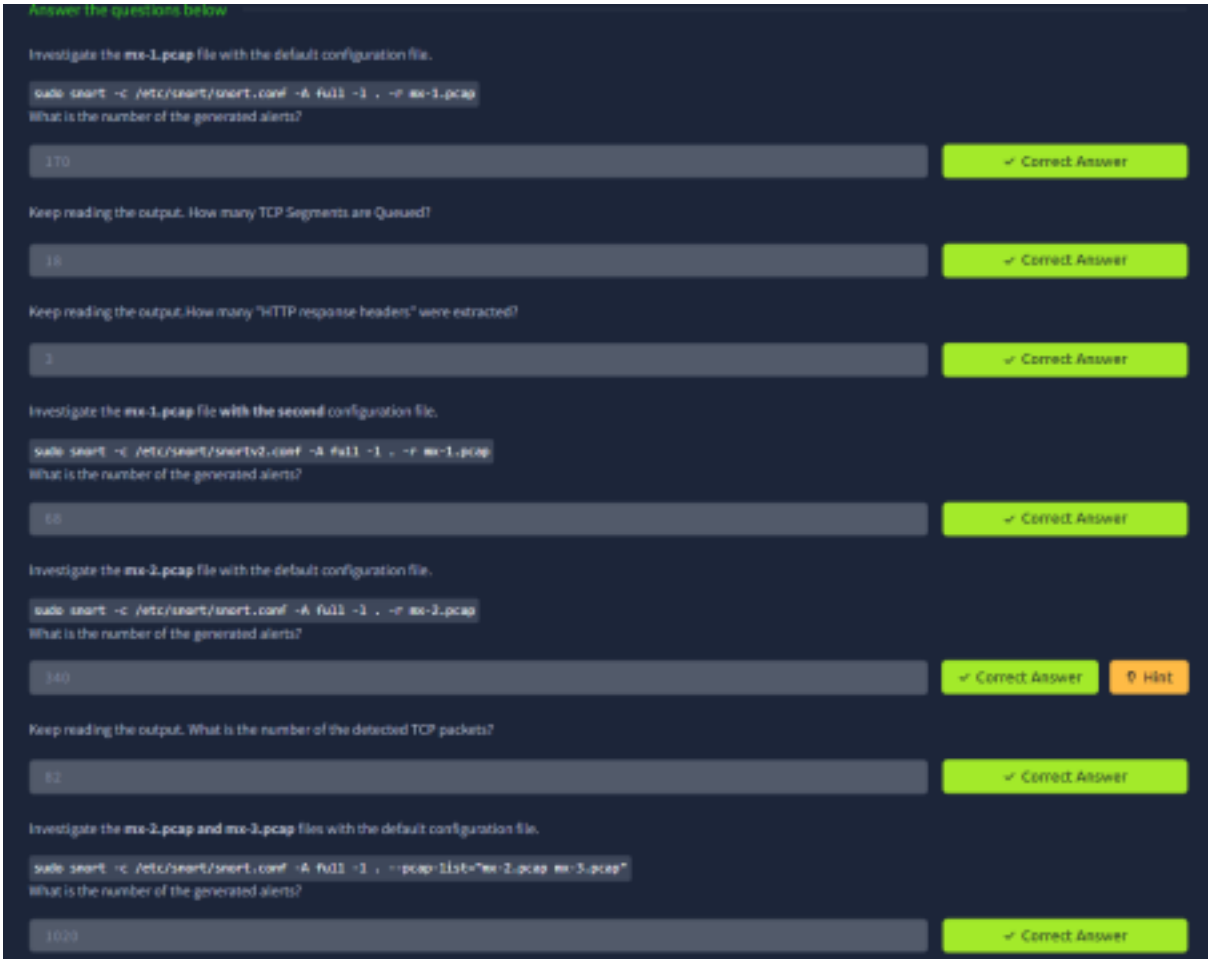
Task 5:Operation Mode 1: Sniffer Mode

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 11Conclusion

RESULT:

Thus, the experiment is completed successfully in try hack me platform.