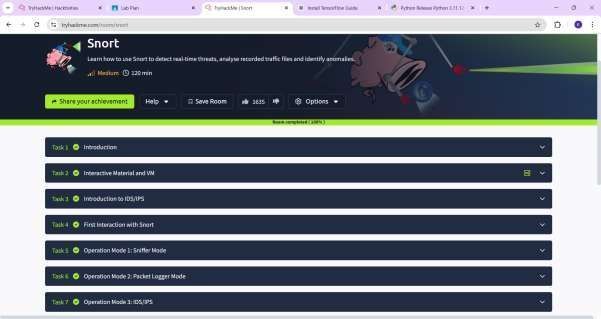
DETECTION OF REAL TIME THREATS,ANALYSE RECORDED 231901005

RECORDED TRAFFIC FILES AND IDENTIFY ANOMALIES

AIM:

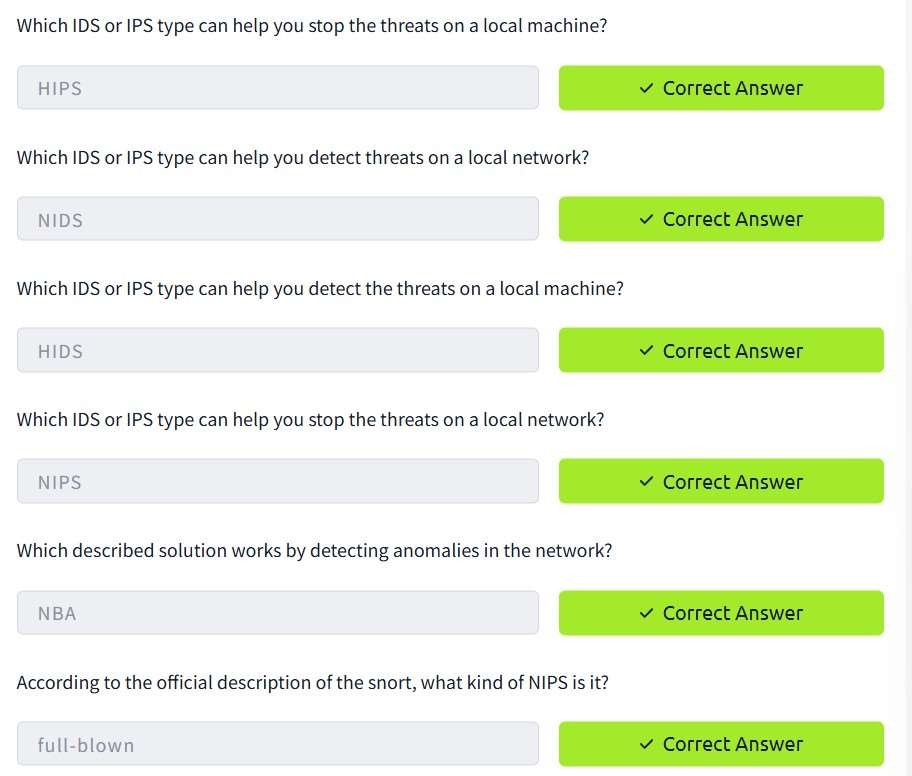
Learn how ton use snort to detect real time threats,analyse recorded traffic files and identify anomalies.



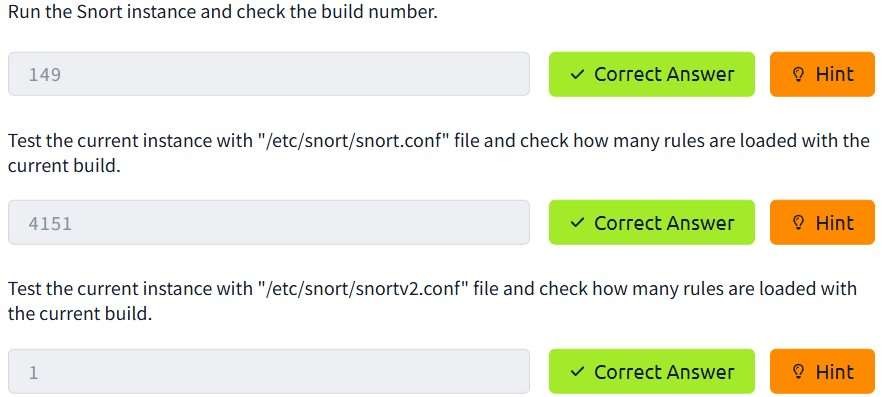
TASK 2 : INTERACTIVE MATERIAL AND VM



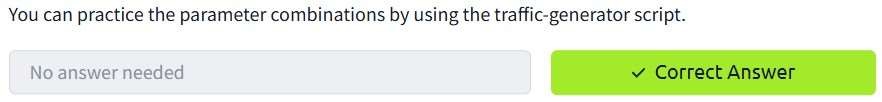
TASK 3 : INTRODUCTION TO IDS/IPS



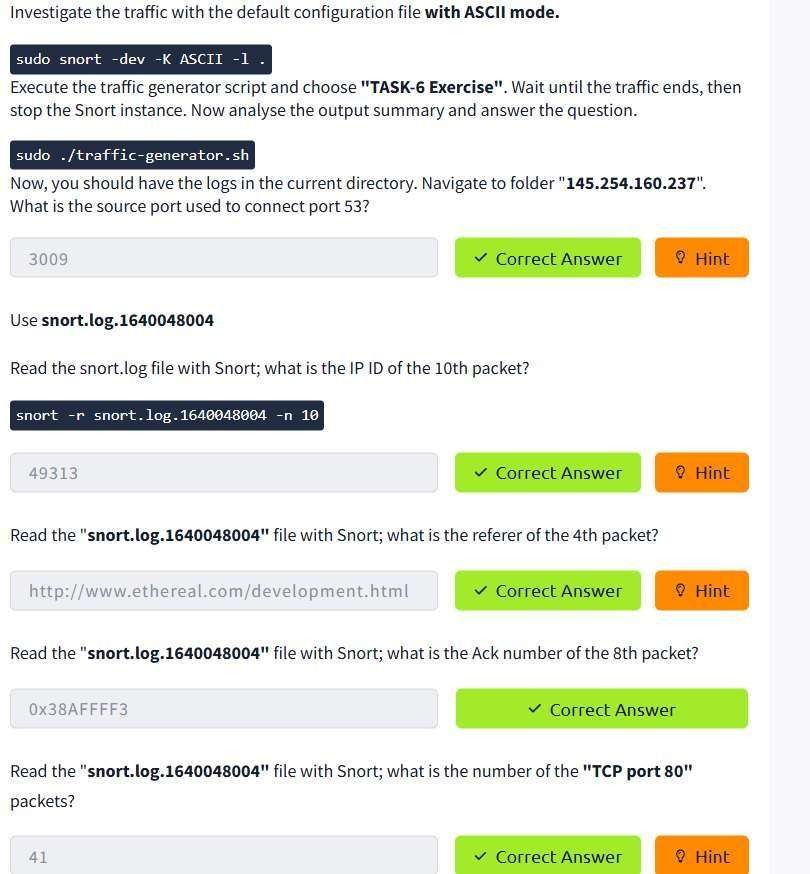
TASK 4 : FIRST INTERACTION WITH SNORT



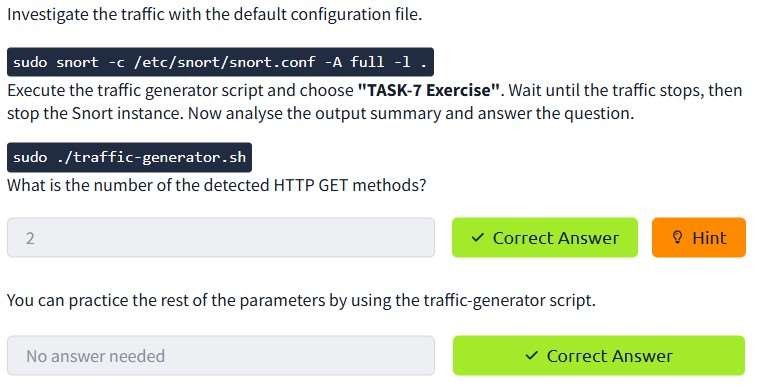
TASK 5 : OPERATON MODE 1 : SNIFFER MODE



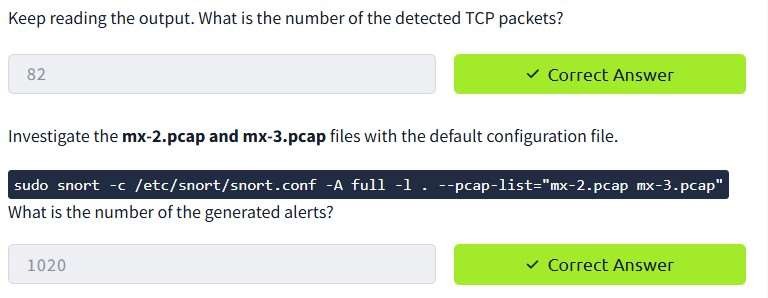
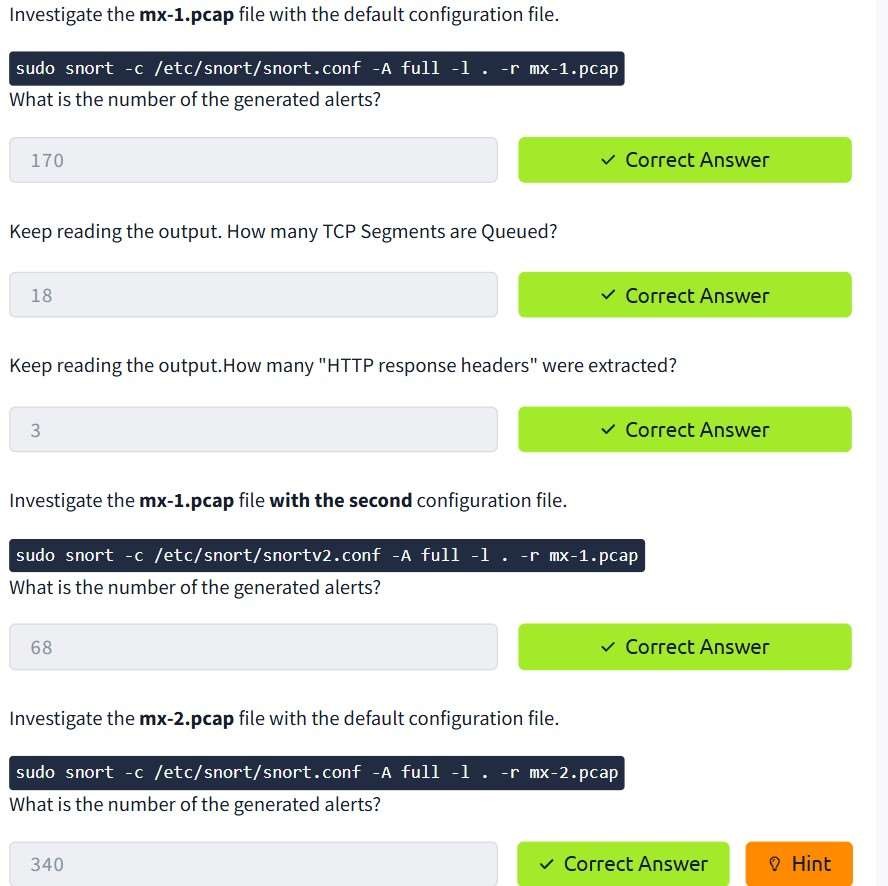
TASK 6 : OPERATION MODE 2 : PACKET LOGGER MODE



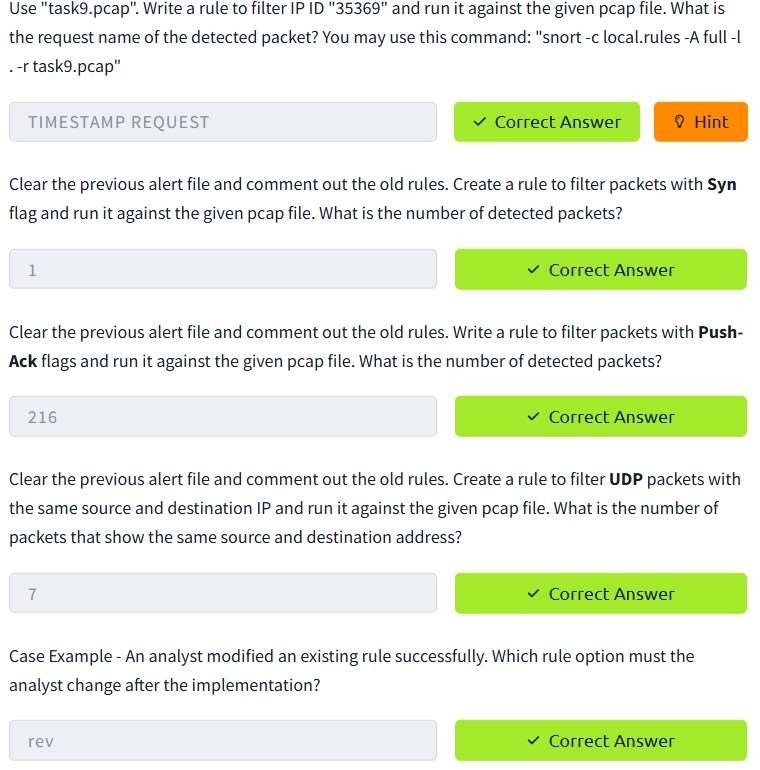
TASK 7 OPERATION MODE 3 : IDS/IPS



TASK 8 : OPERATION MODE 4 : PCAP INVESTIGATION



TASK 9 SNORT RULE STRUCTURE



TASK 10 SNORT2 OPERATION LOGIC : POINT TO REMEMBER

CONCLUSION:

Detection of real time threrats,analyse recorded traffic files and identify anomalies task is successfully completed.