Name: Ram Haygrev S Roll no: 231901039

EX NO: 13 DETECTION OF REAL TIME THREATS, ANALYSE RECORDED TRAFFIC FILES AND IDENTIFY ANOMALIES

DATE: 16.04.2025

AIM:

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

TASK 2: INTERACTIVE MATERIAL AND VM

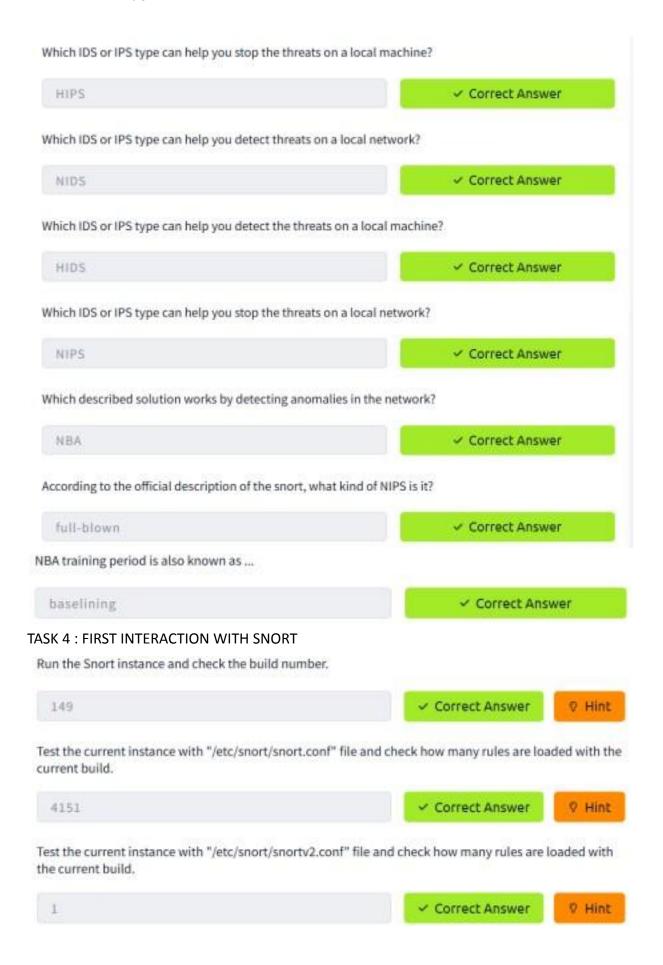
Navigate to the Task-Exercises folder and run the command "./.easy.sh" and write the output

Too Easy!

Correct Answer

TASK 3: INTRODUCTION TO IDS/IPS

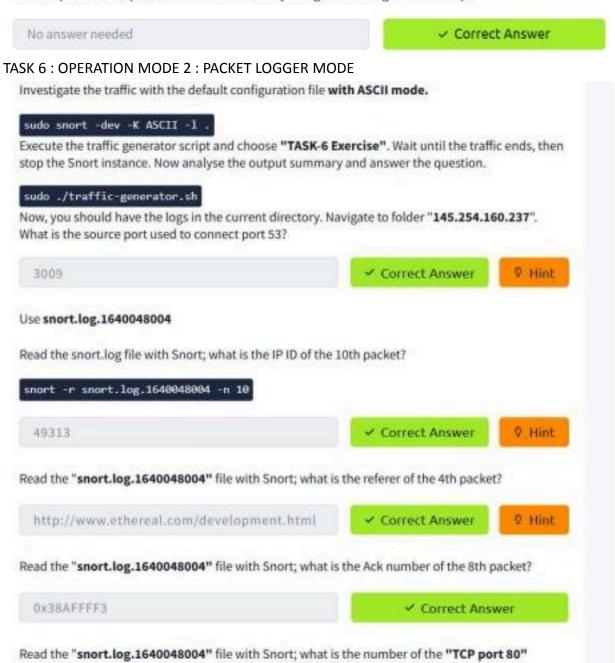
Name : Ram Haygrev S Roll no: 231901039



Name: Ram Haygrev S Roll no: 231901039

TASK 5: OPERATON MODE 1: SNIFFER MODE

You can practice the parameter combinations by using the traffic-generator script.



Correct Answer

Q Hint

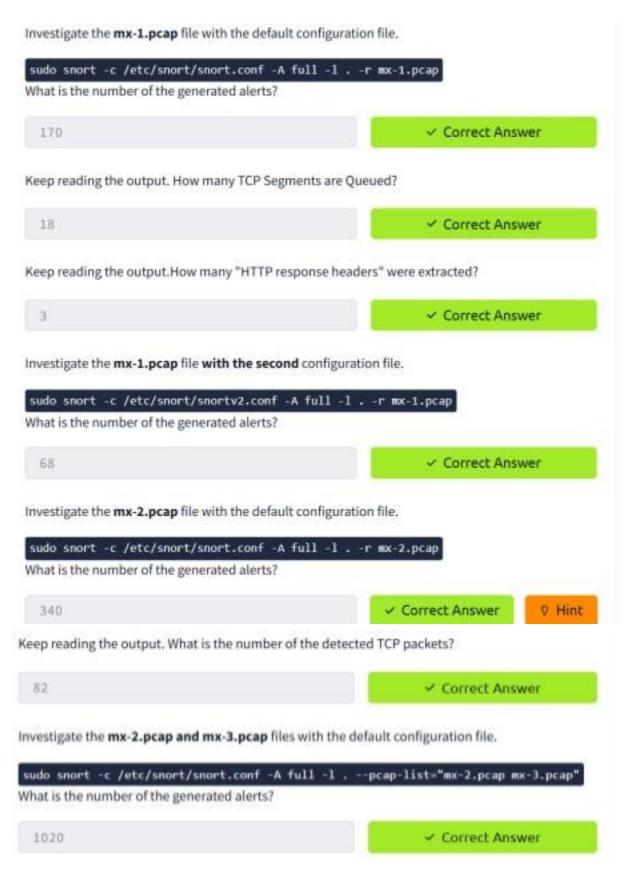
TASK 7 OPERATION MODE 3: IDS/IPS

packets?

41

TASK 8: OPERATION MODE 4: PCAP INVESTIGATION

Name : Ram Haygrev S Roll no: 231901039



TASK 9 SNORT RULE STRUCTURE

Name: Ram Haygrev S Roll no: 231901039

Use "task9.pcap". Write a rule to filter IP ID "35369" and run it against the given pcap file. What is the request name of the detected packet? You may use this command: "snort -c local.rules -A full -l . -r task9.pcap" TIMESTAMP REQUEST ✓ Correct Answer 0 Hint Clear the previous alert file and comment out the old rules. Create a rule to filter packets with Syn flag and run it against the given pcap file. What is the number of detected packets? Correct Answer Clear the previous alert file and comment out the old rules. Write a rule to filter packets with Push-Ack flags and run it against the given pcap file. What is the number of detected packets? 216 Correct Answer Clear the previous alert file and comment out the old rules. Create a rule to filter UDP packets with the same source and destination IP and run it against the given pcap file. What is the number of packets that show the same source and destination address?

Correct Answer

Correct Answer

TASK 10 SNORT2 OPERATION LOGIC: POINT TO REMEMBER

analyst change after the implementation?

Result:

rev

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

Case Example - An analyst modified an existing rule successfully. Which rule option must the