

**EX.NO:13**

**NAME:KALAIYARASI.M**

**DATE:17/4/25**

**ROLLNO:231901503**

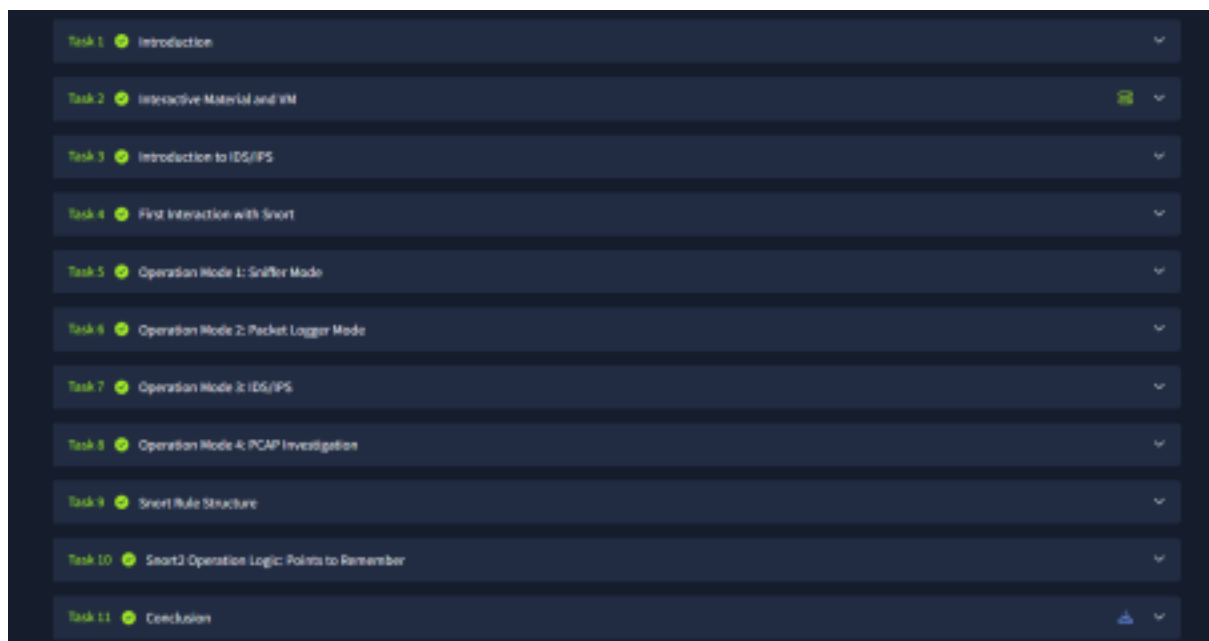
## **Snort**

AIM:

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

PROCEDURE:

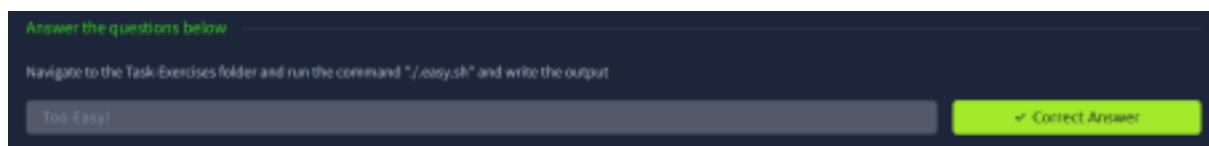
Complete the given task as per the instructions.



Task 1:Introduction



Task 2:Interactive Material and VM



Task 3:Introduction to IDS/IPS

Answer the questions below

Which IDS or IPS type can help you stop the threats on a local machine?

HIPS ✓ Correct Answer

Which IDS or IPS type can help you detect threats on a local network?

NIDS ✓ Correct Answer

Which IDS or IPS type can help you detect the threats on a local machine?

HIDS ✓ Correct Answer

Which IDS or IPS type can help you stop the threats on a local network?

NIPS ✓ Correct Answer

Which described solution works by detecting anomalies in the network?

NBA ✓ Correct Answer

According to the official description of the snort, what kind of NIPS is it?

full-blown ✓ Correct Answer

NBA training period is also known as ...

baselining ✓ Correct Answer

#### Task 4:First Interaction with Snort

Answer the questions below

Run the Snort instance and check the build number.

1.43 ✓ Correct Answer [Hist](#)

Test the current instance with "/etc/snort/snort.conf" file and check how many rules are loaded with the current build.

4151 ✓ Correct Answer [Hist](#)

Test the current instance with "/etc/snort/snortv2.conf" file and check how many rules are loaded with the current build.

1 ✓ Correct Answer [Hist](#)

#### Task 5:Operation Mode 1: Sniffer Mode

Answer the questions below

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

No answer needed ✓ Correct Answer

#### Task 6:Operation Mode 2: Packet Logger Mode

Answer the questions below

Investigate the traffic with the default configuration file with ASCII mode.

```
sudo snort -dev -K ASCII -i .
```

Execute the traffic generator script and choose "TASK-8 Exercise". Wait until the traffic ends, then stop the Snort instance. Now analyse the output summary and answer the question.

```
sudo ./traffic-generator.sh
```

Now, you should have the logs in the current directory. Navigate to folder "145.254.160.237". What is the source port used to connect port 53?

3003

✓ Correct Answer 0 Hint

Use smart.log.1640048004

Read the smart.log file with Snort; what is the IP ID of the 10th packet?

```
snort -r smart.log.1640048004 -s 10
```

49313

✓ Correct Answer 0 Hint

Read the "smart.log.1640048004" file with Snort; what is the referer of the 4th packet?

http://www.ethereal.com/development.html

✓ Correct Answer 0 Hint

Read the "smart.log.1640048004" file with Snort; what is the Ack number of the 8th packet?

6c38affff3

✓ Correct Answer

Read the "smart.log.1640048004" file with Snort; what is the number of the "TCP port 80" packets?

41

✓ Correct Answer 0 Hint

## Task 7: Operation Mode 3: IDS/IPS

Answer the questions below

Investigate the traffic with the default configuration file.

```
sudo snort -c /etc/snort/snort.conf -A full -i .
```

Execute the traffic generator script and choose "TASK-7 Exercise". Wait until the traffic stops, then stop the Snort instance. Now analyse the output summary and answer the question.

```
sudo ./traffic-generator.sh
```

What is the number of the detected HTTP GET methods?

2

✓ Correct Answer 0 Hint

You can practice the rest of the parameters by using the traffic generator script.

No answer needed

✓ Correct Answer

## Task 8: Operation Mode 4: PCAP Investigation

Answer the questions below

Investigate the `mx-1.pcap` file with the default configuration file.

```
sudo snort -c /etc/snort/snort.conf -A full -l . -r mx-1.pcap
```

What is the number of the generated alerts?

170 ✓ Correct Answer

Keep reading the output. How many TCP Segments are Queued?

18 ✓ Correct Answer

Keep reading the output. How many "HTTP response headers" were extracted?

3 ✓ Correct Answer

Investigate the `mx-1.pcap` file with the second configuration file.

```
sudo snort -c /etc/snort/snortv2.conf -A full -l . -r mx-1.pcap
```

What is the number of the generated alerts?

68 ✓ Correct Answer

Investigate the `mx-2.pcap` file with the default configuration file.

```
sudo snort -c /etc/snort/snort.conf -A full -l . -r mx-2.pcap
```

What is the number of the generated alerts?

140 ✓ Correct Answer Hint

Keep reading the output. What is the number of the detected TCP packets?

82 ✓ Correct Answer

Investigate the `mx-2.pcap` and `mx-3.pcap` files with the default configuration file.

```
sudo snort -c /etc/snort/snort.conf -A full -l . --pcap-list="mx-2.pcap mx-3.pcap"
```

What is the number of the generated alerts?

1029 ✓ Correct Answer

## Task 9:Snort Rule Structure

Answer the questions below

Use "task8.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 localRules -A full -l . -r task8.pcap"

TIME STAMP REQUEST ✓ Correct Answer 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?

1 ✓ 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?

236 ✓ 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?

7 ✓ Correct Answer

Case Example - An analyst modified an existing rule successfully. Which rule option must the analyst change after the implementation?

REV ✓ Correct Answer

## Task 10:Snort2 Operation Logic: Points to Remember

Answer the questions below

Read the task above.

No answer needed

✔ Correct Answer

## Task 11 Conclusion

Answer the questions below

Read the task above.

No answer needed

✔ Correct Answer

RESULT:

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