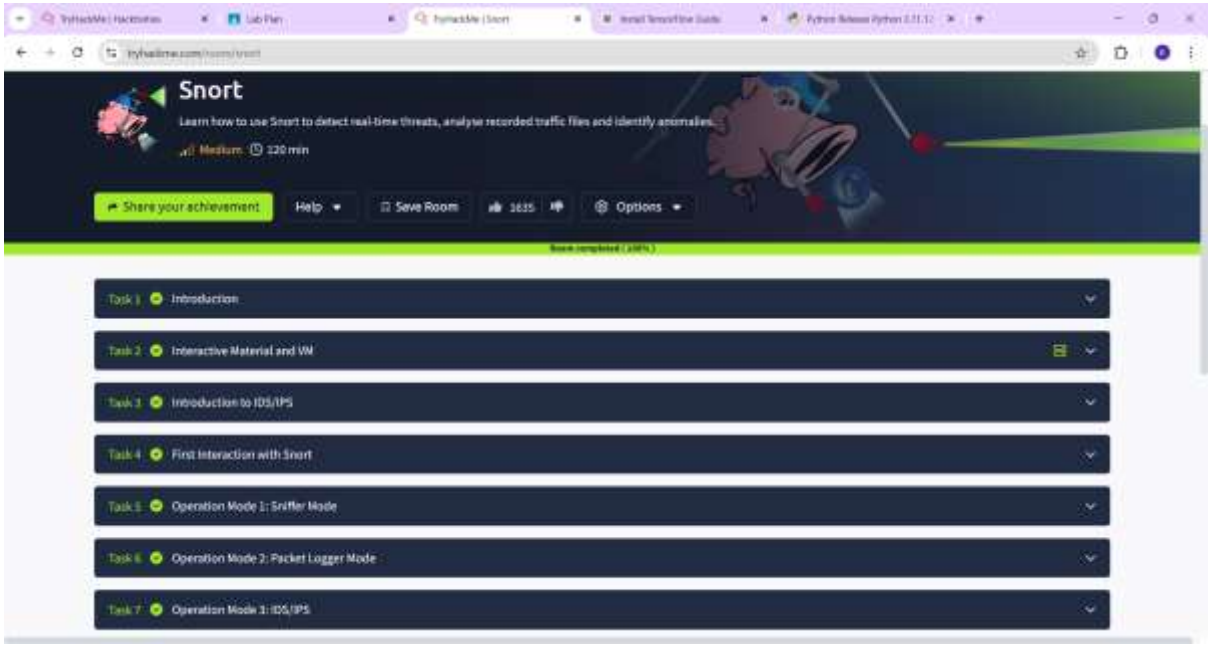
EX NO : 13 DETECTION OF REAL TIME THREATS,ANALYSE RECORDED

DATE : 16.04.202 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

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

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

Run the Snort instance and check the build number.

149 ✓ Correct Answer Hint

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

4151 ✓ Correct Answer Hint

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

1 ✓ Correct Answer Hint

TASK 5 : OPERATON MODE 1 : SNIFFER MODE

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

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

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

Execute the traffic generator script and choose **"TASK-6 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?

3009 ✓ Correct Answer Hint

Use **snort.log.1640048004**

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

```
snort -r snort.log.1640048004 -n 10
```

49313 ✓ Correct Answer Hint

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

http://www.ethereal.com/development.html ✓ Correct Answer Hint

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

0x38AFFFF3 ✓ Correct Answer

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

41 ✓ Correct Answer Hint

TASK 7 OPERATION MODE 3 : IDS/IPS

Investigate the traffic with the default configuration file.

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

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 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

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?

340 ✓ 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?

1020 ✓ Correct Answer

TASK 9 SNORT RULE STRUCTURE

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 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?

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?

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 : POINT TO REMEMBER

CONCLUSION:

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