

Snort

EX-NO:13

AIM:

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

PROCEDURE:

- 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 11 Conclusion

Task 1 Introduction :

Answer the questions below

Read the task above.

No answer needed

✓ Correct Answer

Task 2 Interactive Material and VM :

Answer the questions below

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 :

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.

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 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 -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?

✓ 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
```

✓ Correct Answer

🔍 Hint

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

✓ Correct Answer

🔍 Hint

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

✓ Correct Answer

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

✓ Correct Answer

🔍 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 -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?

✓ Correct Answer

🔍 Hint

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

✓ 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?

✓ Correct Answer

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

✓ Correct Answer

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

✓ Correct Answer

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

What is the number of the generated alerts?

✓ 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?

✓ Correct Answer

🔍 Hint

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

✓ 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?

✓ Correct Answer

Task 9 Snort Rule Structure :

Answer the questions below

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"

✓ 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?

✓ 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?

✓ 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

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

✓ Correct Answer

Task 10 Snort2 Operation Logic: Points to Remember :

Answer the questions below

Read the task above.

✓ Correct Answer

Task 11 Conclusion :

Answer the questions below

Read the task above.

✓ Correct Answer

EXP NO RESULT:

Thus the Snort is completed using tryhackme platform.