

## EXERCISE 13

### Detection of real-time threats, analyse recorded traffic files and identify anomalies

**Aim:** To learn how to use Snort for real-time threat detection, traffic analysis, and anomaly identification using both live and recorded network data.

The screenshot displays the Snort exercise interface. At the top, the Snort logo is shown with the text "Learn how to use Snort to detect real-time threats, analyse recorded traffic files and identify anomalies." Below this, a progress bar indicates "Room completed (100%)". A list of tasks follows, each marked with a green checkmark and a dropdown arrow:

- 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

Below the task list, three question prompts are shown, each with a text input field, a "Correct Answer" button, and a "Hint" button:

1. Navigate to the Task-Exercises folder and run the command `"/.easy.sh"` and write the output.  
Input: Too Easy! Correct Answer

2. Run the Snort instance and check the build number.  
Input: 149 Correct Answer Hint

3. Test the current instance with `"/etc/snort/snort.conf"` file and check how many rules are loaded with the current build.  
Input: 4151 Correct Answer Hint

4. Test the current instance with `"/etc/snort/snortv2.conf"` file and check how many rules are loaded with the current build.  
Input: 1 Correct Answer Hint

What is the number of the detected HTTP GET methods?

2

✓ Correct Answer

🔍 Hint

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

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

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

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

**Result:** Successfully configured Snort to detect live threats, analyzed pcap traffic files, and identified suspicious patterns and anomalies in network behavior.