Task1:

Correct Answer: No answer needed.

Task2:

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

Task3:

1. Which snort mode can help you stop the threats on a local machine?

Correct Answer: HIPS

1. Which snort mode can help you detect threats on a local network?

Correct Answer: NIDS

1. Which snort mode can help you detect the threats on a local machine?

Correct Answer: HIDS

1. Which snort mode can help you stop the threats on a local network?

Correct Answer:NIPS

1. Which snort mode works similar to NIPS mode?

Correct Answer:NBA

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

Correct Answer:Full-blown

1. NBA training period is also known as ...

Correct Answer: baselining

Task4:

1. Run the Snort instance and check the build number.

Correct Answer: 149

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

Correct Answer: 4151

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

Ans:1

Task5:

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

Correct Answer: No answer needed.

Task6

1. 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: 3009

1. 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: 49313

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

Correct Answer: http://www.ethereal.com/developent.html

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

Correct Answer: 0x38AFFFF3

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

Correct Answer: 41

Task7:

1. 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: 2

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

Correct Answer: No answer needed

Task8:

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

1. What is the number of the generated alerts?

Correct Answer: 170

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

Correct Answer:18

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

Correct Answer:3

1. 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?

Correct Answer:68

1. 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: 340

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

Correct Answer:82

1. 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:1020

Task9:

Use **"task9.pcap".**

1. 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? snort -c local.rules -A full -l . -r task9.pcap

Correct Answer: timestamp request

1. 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:1

1. Clear the previous log and alarm files and deactivate/comment out the old rule.

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: 216

1. Clear the previous log and alarm files and deactivate/comment out the old rule.

Create a rule to filter **packets with the same source and destination IP**and run it against the given pcap file. What is the number of detected packets?

Correct Answer:10

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

Correct Answer: rev

Task10:

Correct Answer: No answer needed.

Task11:

Correct Answer: No answer needed.