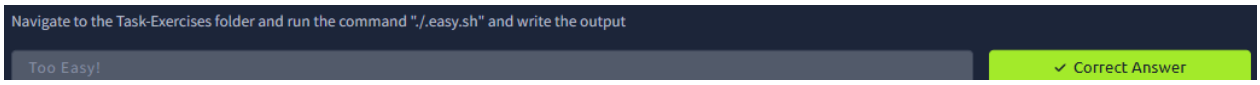
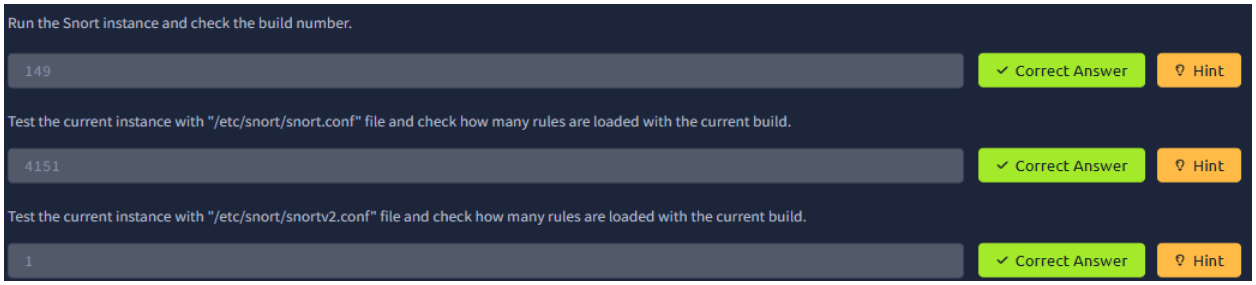
DHARSHNA U **231901008**

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.





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?

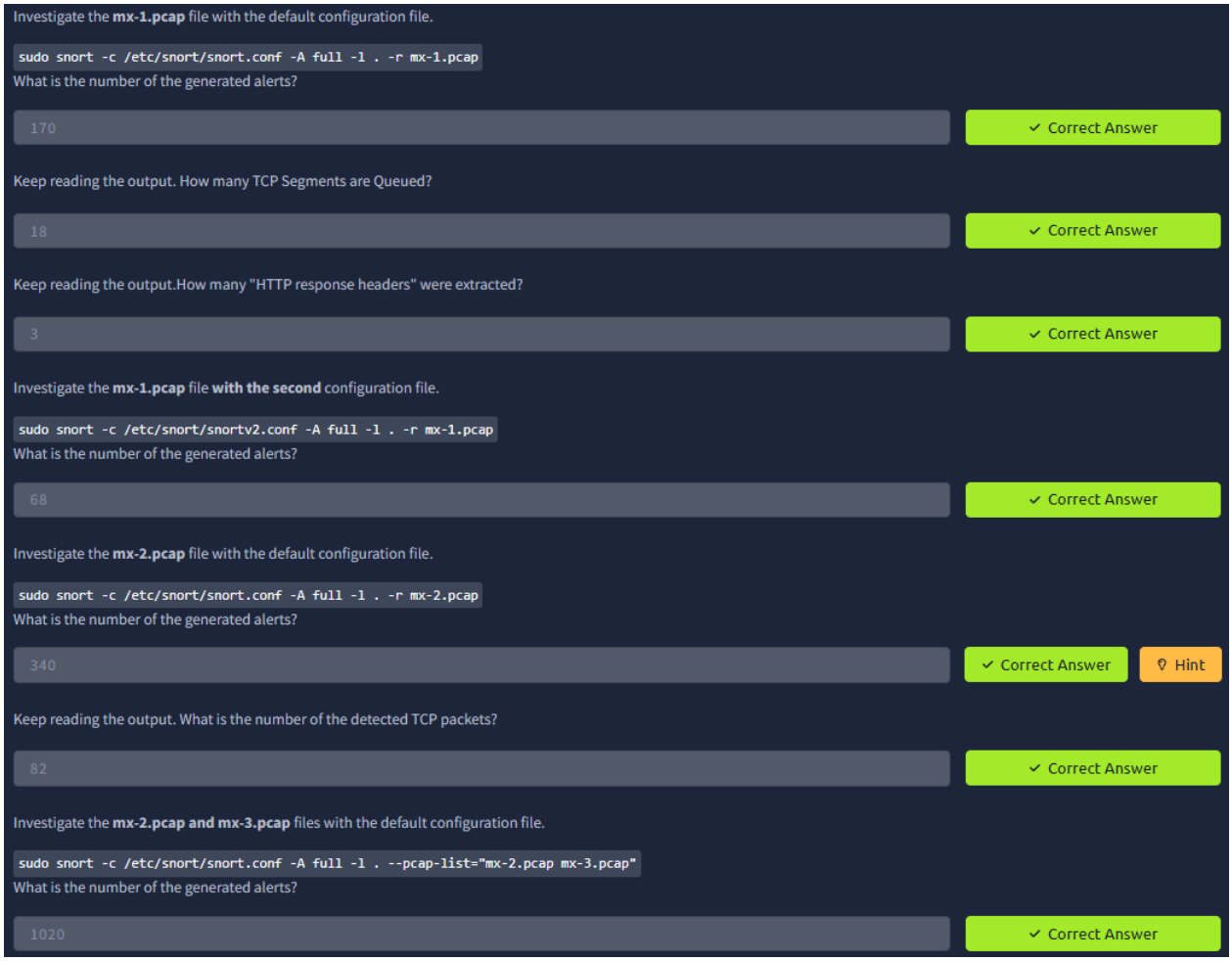
http://www.ethereal.com/development.html ✓ Correct Answer Hint

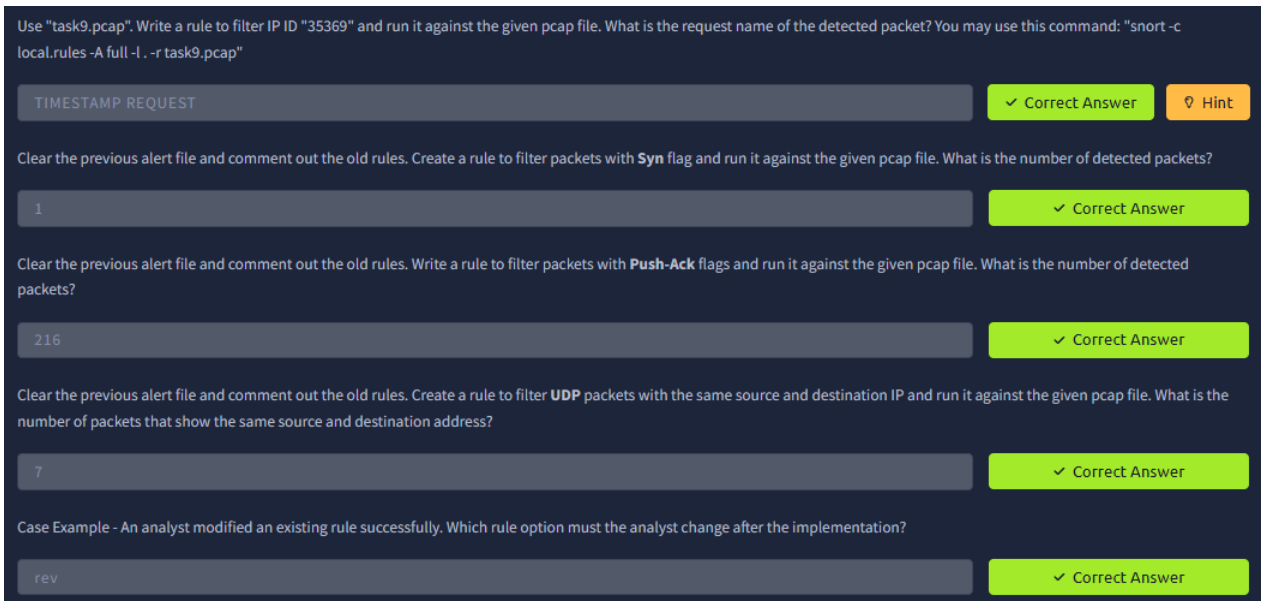
Read the "**snort.log.1640048004**" file with Snort; what is the Ack number of the 8th packet?

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





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