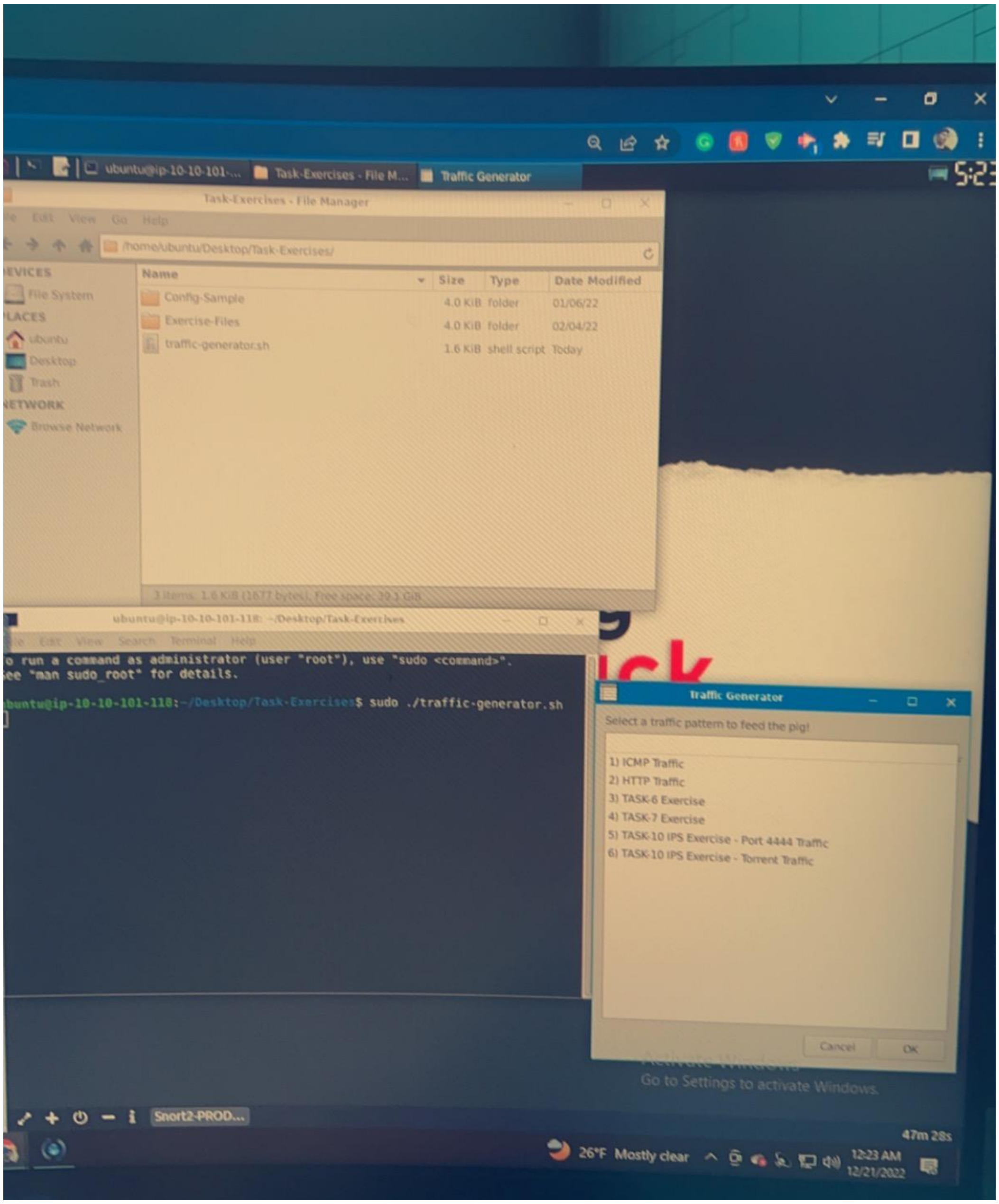
Mike Macancela Snort Lab



ubuntu@ip-10-10-101-...
Task-Exercises - File M...
Traffic Generator
Task-Exercises - File Manager
Edit View Go Help
/home/ubuntu/Desktop/Task-Exercises/
EVICES
File System
LACES
ubuntu
Desktop
Trash
ETWORK
Browse Network

Name	Size	Type	Date Modified
Config-Sample	4.0 KiB	folder	01/06/22
Exercise-Files	4.0 KiB	folder	02/04/22
traffic-generator.sh	1.6 KiB	shell script	Today

3 items: 1.6 KiB (1677 bytes), Free space: 29.1 GiB

ubuntu@ip-10-10-101-118: ~/Desktop/Task-Exercises

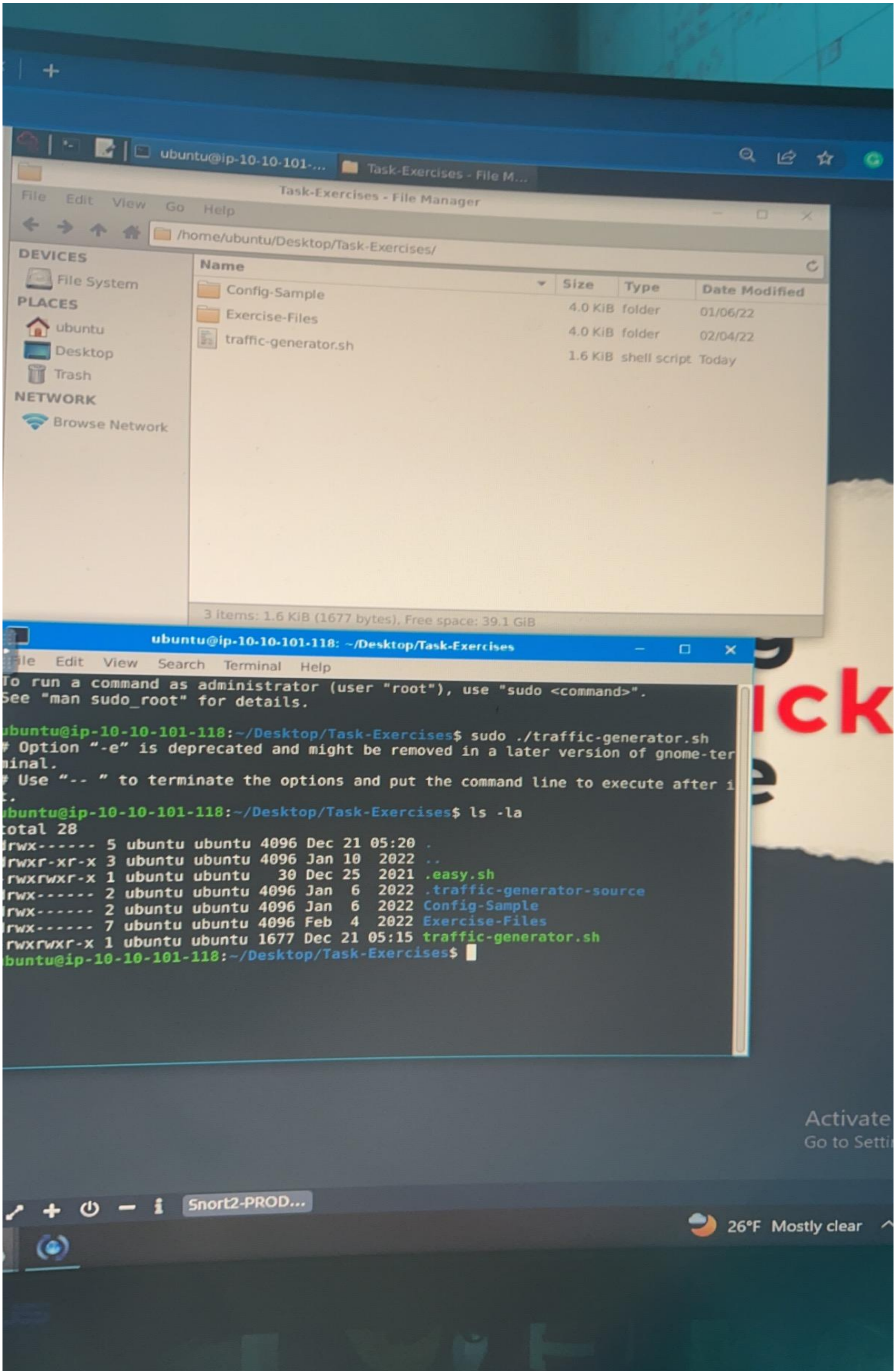
Edit View Search Terminal Help

```
o run a command as administrator (user "root"), use "sudo <command>".
ee "man sudo_root" for details.

buntu@ip-10-10-101-118:~/Desktop/Task-Exercises$ sudo ./traffic-generator.sh
```

Traffic Generator

Select a traffic pattern to feed the pig!

1) ICMP Traffic
2) HTTP Traffic
3) TASK-6 Exercise
4) TASK-7 Exercise
5) TASK-10 IPS Exercise - Port 4444 Traffic
6) TASK-10 IPS Exercise - Torrent Traffic



Task-Exercises - File Manager

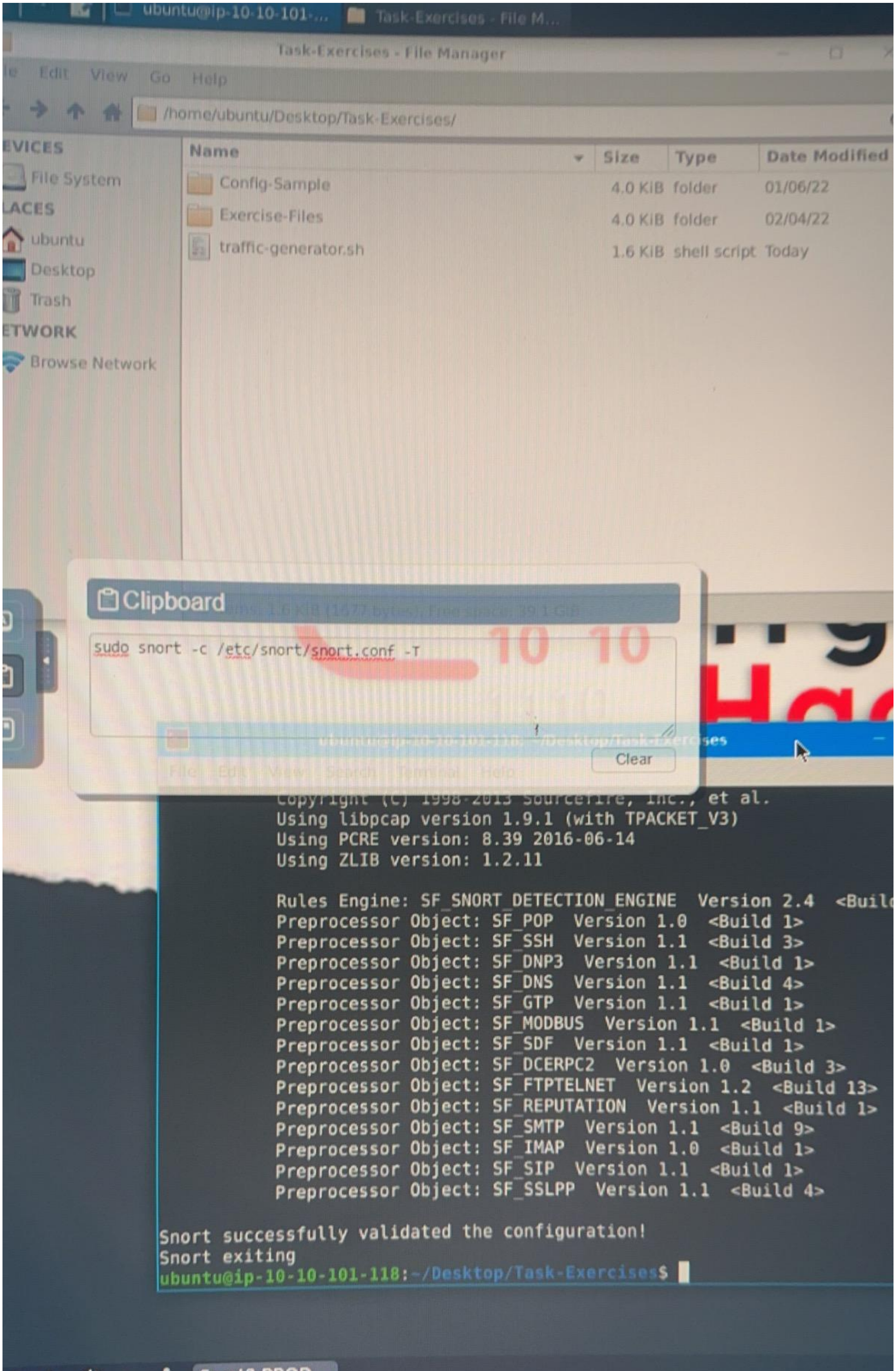
/home/ubuntu/Desktop/Task-Exercises/

Name	Size	Type	Date Modified
Config-Sample	4.0 KiB	folder	01/06/22
Exercise-Files	4.0 KiB	folder	02/04/22
traffic-generator.sh	1.6 KiB	shell script	Today

3 items: 1.6 KiB (1677 bytes), Free space: 39.1 GiB

ubuntu@ip-10-10-101-118: ~/Desktop/Task-Exercises

```
o run a command as administrator (user "root"), use "sudo <command>".
ee "man sudo_root" for details.

ubuntu@ip-10-10-101-118:~/Desktop/Task-Exercises$ sudo ./traffic-generator.sh
 Option "-e" is deprecated and might be removed in a later version of gnome-ter
inal.
 Use "-- " to terminate the options and put the command line to execute after i
.
buntu@ip-10-10-101-118:~/Desktop/Task-Exercises$ ls -la
otal 28
rwx------ 5 ubuntu ubuntu 4096 Dec 21 05:20 .
rwxr-xr-x 3 ubuntu ubuntu 4096 Jan 10  2022 ..
rwxrwxr-x 1 ubuntu ubuntu   30 Dec 25  2021 .easy.sh
rwx------ 2 ubuntu ubuntu 4096 Jan  6  2022 .traffic-generator-source
rwx------ 2 ubuntu ubuntu 4096 Jan  6  2022 Config-Sample
rwx------ 7 ubuntu ubuntu 4096 Feb  4  2022 Exercise-Files
rwxrwxr-x 1 ubuntu ubuntu 1677 Dec 21 05:15 traffic-generator.sh
buntu@ip-10-10-101-118:~/Desktop/Task-Exercises$ 
```


ubuntu@ip-10-10-101-...
Task-Exercises - File M...
Task-Exercises - File Manager
le Edit View Go Help
EVICES
File System
LACES
ubuntu
Desktop
Trash
ETWORK
Browse Network
Clipboard
Clear
ubuntu@ip-10-10-101-118: ~/Desktop/Task-Exercises
File Edit View Search Terminal Help

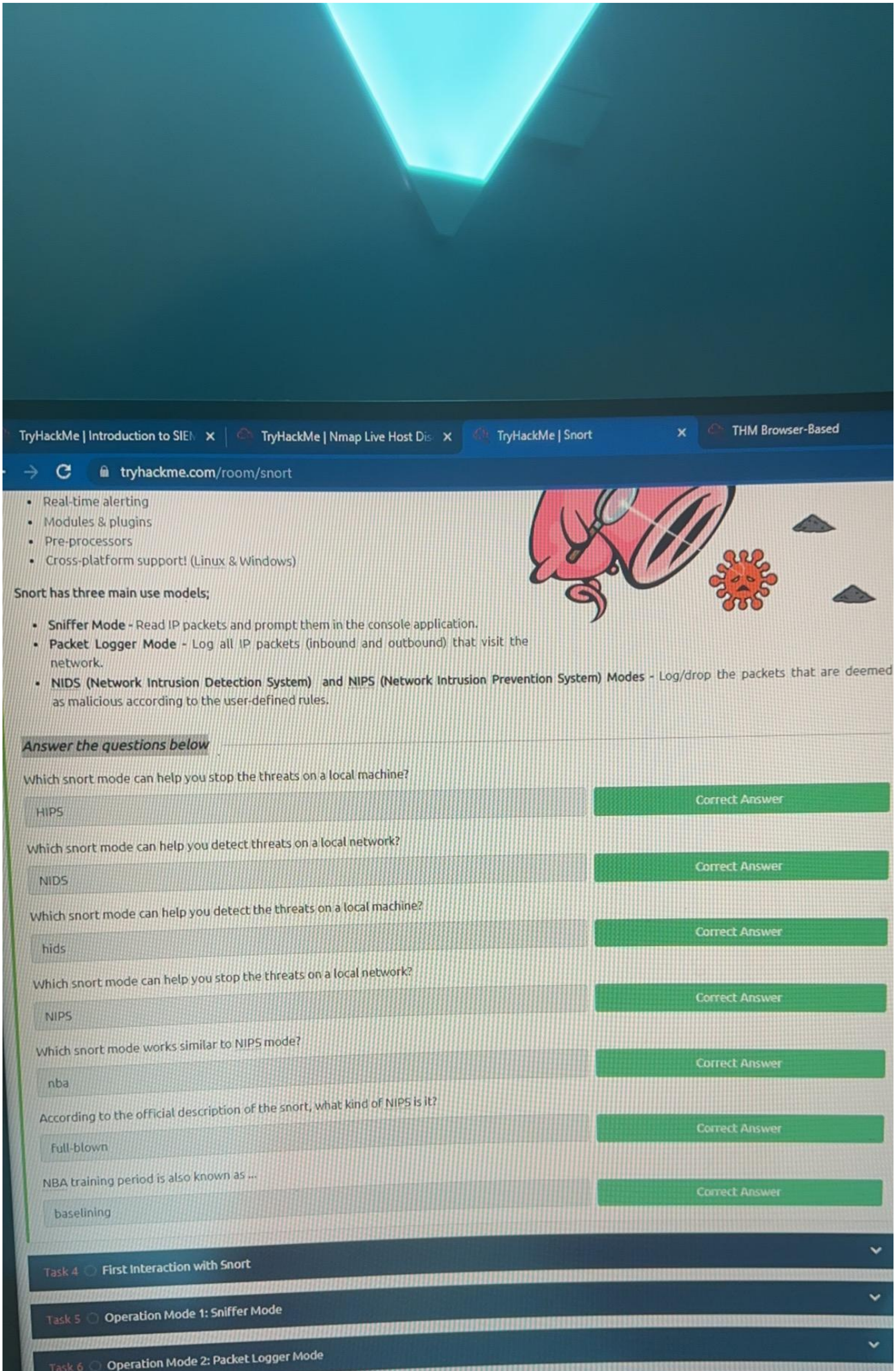
/home/ubuntu/Desktop/Task-Exercises/

Name	Size	Type	Date Modified
Config-Sample	4.0 KiB	folder	01/06/22
Exercise-Files	4.0 KiB	folder	02/04/22
traffic-generator.sh	1.6 KiB	shell script	Today

"...name": 1.6 KiB (1677 bytes), Free space: 39.1 GiB

```
sudo snort -c /etc/snort/snort.conf -T
```

```
           Copyright (C) 1998-2013 Sourcefire, Inc., et al.
           Using libpcap version 1.9.1 (with TPACKET_V3)
           Using PCRE version: 8.39 2016-06-14
           Using ZLIB version: 1.2.11

           Rules Engine: SF_SNORT_DETECTION_ENGINE  Version 2.4  <Buil
           Preprocessor Object: SF_POP  Version 1.0  <Build 1>
           Preprocessor Object: SF_SSH  Version 1.1  <Build 3>
           Preprocessor Object: SF_DNP3  Version 1.1  <Build 1>
           Preprocessor Object: SF_DNS  Version 1.1  <Build 4>
           Preprocessor Object: SF_GTP  Version 1.1  <Build 1>
           Preprocessor Object: SF_MODBUS  Version 1.1  <Build 1>
           Preprocessor Object: SF_SDF  Version 1.1  <Build 1>
           Preprocessor Object: SF_DCERPC2  Version 1.0  <Build 3>
           Preprocessor Object: SF_FTPTELNET  Version 1.2  <Build 13>
           Preprocessor Object: SF_REPUTATION  Version 1.1  <Build 1>
           Preprocessor Object: SF_SMTP  Version 1.1  <Build 9>
           Preprocessor Object: SF_IMAP  Version 1.0  <Build 1>
           Preprocessor Object: SF_SIP  Version 1.1  <Build 1>
           Preprocessor Object: SF_SSLPP  Version 1.1  <Build 4>

Snort successfully validated the configuration!
Snort exiting
ubuntu@ip-10-10-101-118:~/Desktop/Task-Exercises$
```


TryHackMe | Introduction to SIEM ×
TryHackMe | Nmap Live Host Dis ×
TryHackMe | Snort ×
THM Browser-Based
tryhackme.com/room/snort

- Real-time alerting
- Modules & plugins
- Pre-processors
- Cross-platform support! (Linux & Windows)

Snort has three main use models;

- **Sniffer Mode** - Read IP packets and prompt them in the console application.
- **Packet Logger Mode** - Log all IP packets (inbound and outbound) that visit the network.
- **NIDS (Network Intrusion Detection System) and NIPS (Network Intrusion Prevention System) Modes** - Log/drop the packets that are deemed as malicious according to the user-defined rules.

Answer the questions below

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

HIPS

Correct Answer

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

NIDS

Correct Answer

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

hids

Correct Answer

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

NIPS

Correct Answer

Which snort mode works similar to NIPS mode?

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 ...

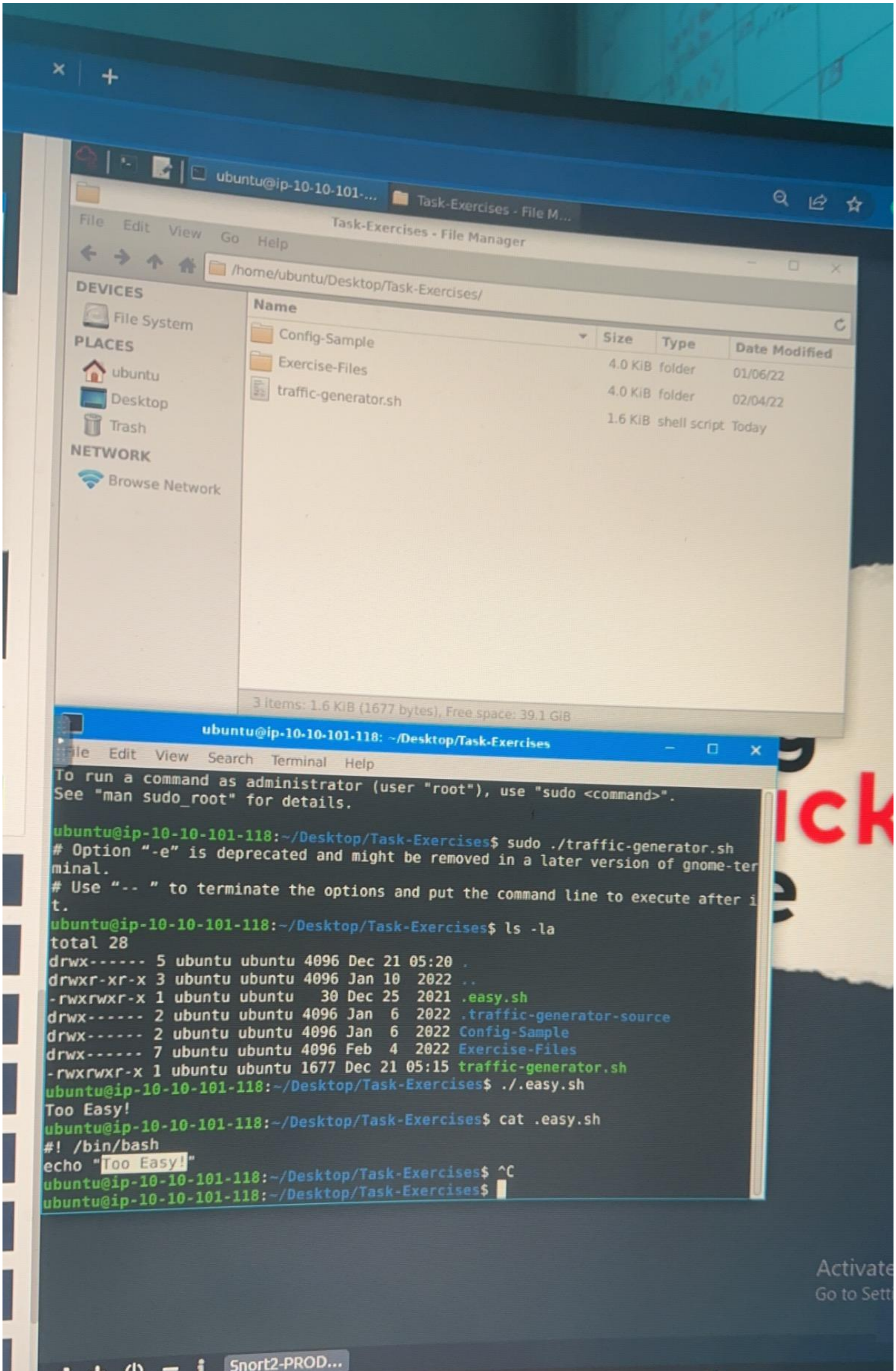
baselining

Correct Answer

Task 4 ○ First Interaction with Snort

Task 5 ○ Operation Mode 1: Sniffer Mode

Task 6 ○ Operation Mode 2: Packet Logger Mode

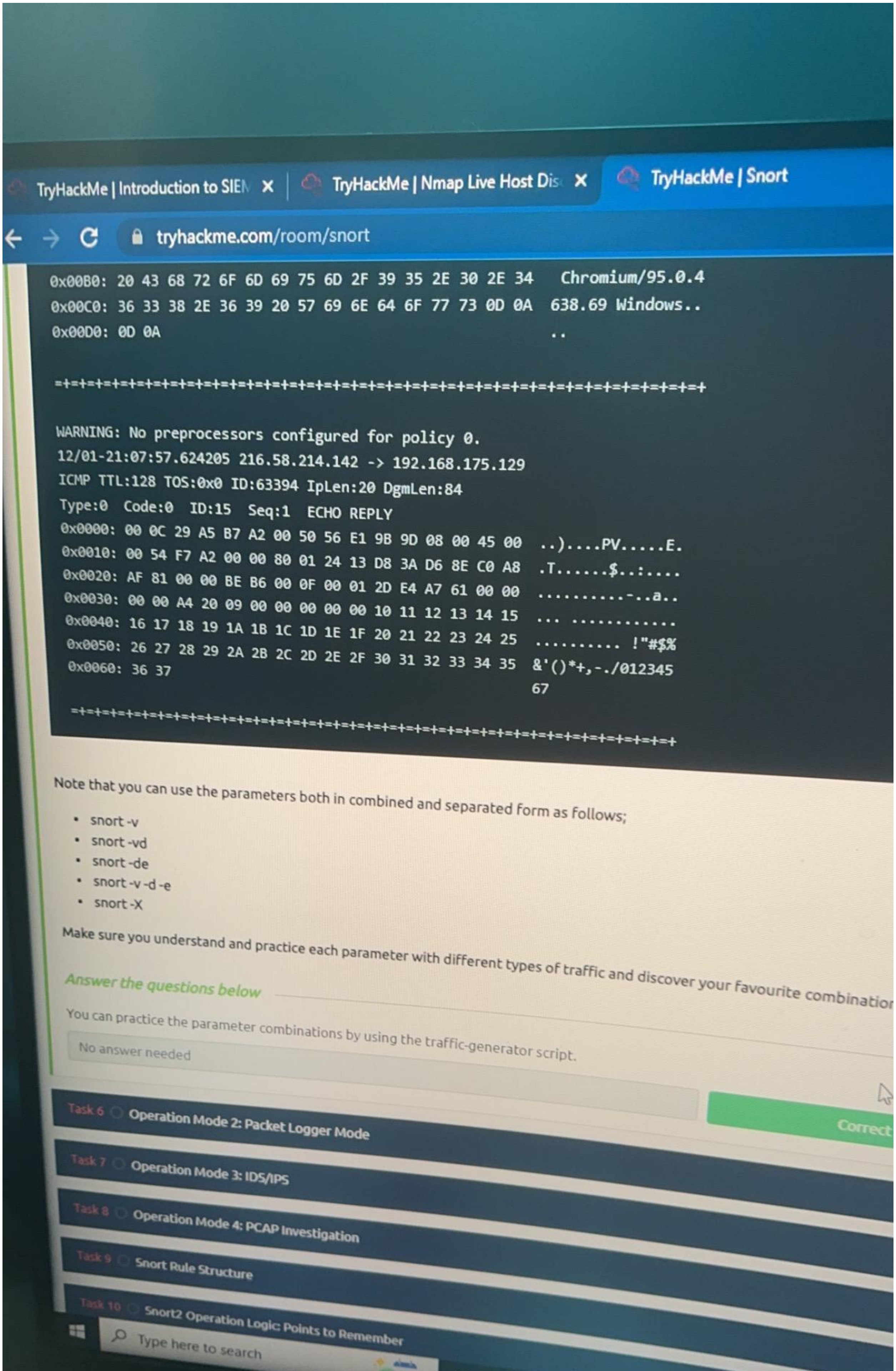


/home/ubuntu/Desktop/Task-Exercises/

Name	Size	Type	Date Modified
Config-Sample	4.0 KiB	folder	01/06/22
Exercise-Files	4.0 KiB	folder	02/04/22
traffic-generator.sh	1.6 KiB	shell script	Today

3 items: 1.6 KiB (1677 bytes), Free space: 39.1 GiB

```
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

ubuntu@ip-10-10-101-118:~/Desktop/Task-Exercises$ sudo ./traffic-generator.sh
# Option “-e” is deprecated and might be removed in a later version of gnome-ter
minal.
# Use “-- ” to terminate the options and put the command line to execute after i
t.
ubuntu@ip-10-10-101-118:~/Desktop/Task-Exercises$ ls -la
total 28
drwx------ 5 ubuntu ubuntu 4096 Dec 21 05:20 .
drwxr-xr-x 3 ubuntu ubuntu 4096 Jan 10  2022 ..
-rwxrwxr-x 1 ubuntu ubuntu   30 Dec 25  2021 .easy.sh
drwx------ 2 ubuntu ubuntu 4096 Jan  6  2022 .traffic-generator-source
drwx------ 2 ubuntu ubuntu 4096 Jan  6  2022 Config-Sample
drwx------ 7 ubuntu ubuntu 4096 Feb  4  2022 Exercise-Files
-rwxrwxr-x 1 ubuntu ubuntu 1677 Dec 21 05:15 traffic-generator.sh
ubuntu@ip-10-10-101-118:~/Desktop/Task-Exercises$ ./.easy.sh
Too Easy!
ubuntu@ip-10-10-101-118:~/Desktop/Task-Exercises$ cat .easy.sh
#! /bin/bash
echo "Too Easy!"
ubuntu@ip-10-10-101-118:~/Desktop/Task-Exercises$ ^C
ubuntu@ip-10-10-101-118:~/Desktop/Task-Exercises$ 
ubuntu@ip-10-10-101-118:~/Desktop/Task-Exercises$ 
```


TryHackMe | Introduction to SIEM ×
TryHackMe | Nmap Live Host Dis ×
TryHackMe | Snort
tryhackme.com/room/snort

```
0x00B0: 20 43 68 72 6F 6D 69 75 6D 2F 39 35 2E 30 2E 34   Chromium/95.0.4
0x00C0: 36 33 38 2E 36 39 20 57 69 6E 64 6F 77 73 0D 0A  638.69 Windows..
0x00D0: 0D 0A                                            ..

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

WARNING: No preprocessors configured for policy 0.
12/01-21:07:57.624205 216.58.214.142 -> 192.168.175.129
ICMP TTL:128 TOS:0x0 ID:63394 IpLen:20 DgmLen:84
Type:0  Code:0  ID:15   Seq:1  ECHO REPLY
0x0000: 00 0C 29 A5 B7 A2 00 50 56 E1 9B 9D 08 00 45 00  ..)....PV.....E.
0x0010: 00 54 F7 A2 00 00 80 01 24 13 D8 3A D6 8E C0 A8  .T......$..:....
0x0020: AF 81 00 00 BE B6 00 0F 00 01 2D E4 A7 61 00 00  ..........-..a..
0x0030: 00 00 A4 20 09 00 00 00 00 00 10 11 12 13 14 15  ... ............
0x0040: 16 17 18 19 1A 1B 1C 1D 1E 1F 20 21 22 23 24 25  .......... !"#$%
0x0050: 26 27 28 29 2A 2B 2C 2D 2E 2F 30 31 32 33 34 35  &'()*+,-./012345
0x0060: 36 37                                            67

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
```

Note that you can use the parameters both in combined and separated form as follows;

- snort -v
- snort -vd
- snort -de
- snort -v -d -e
- snort -X

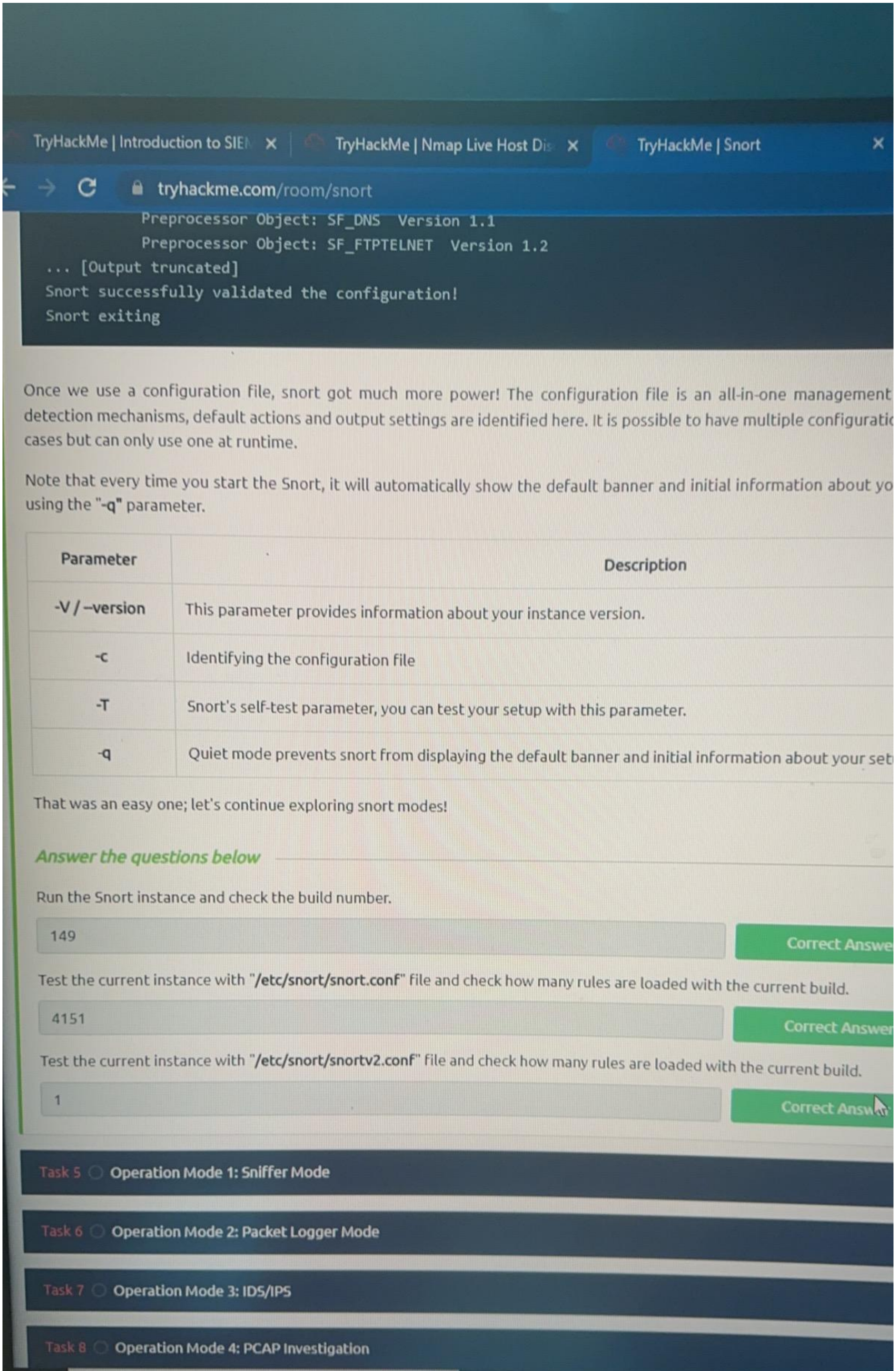
Make sure you understand and practice each parameter with different types of traffic and discover your favourite combinatior

Answer the questions below

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

No answer needed

Correct
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
Type here to search


TryHackMe | Introduction to SIE
TryHackMe | Nmap Live Host Dis
TryHackMe | Snort
tryhackme.com/room/snort

```
        Preprocessor Object: SF_DNS  Version 1.1
        Preprocessor Object: SF_FTPTELNET  Version 1.2
... [Output truncated]
Snort successfully validated the configuration!
Snort exiting
```

Once we use a configuration file, snort got much more power! The configuration file is an all-in-one management detection mechanisms, default actions and output settings are identified here. It is possible to have multiple configuratic cases but can only use one at runtime.

Note that every time you start the Snort, it will automatically show the default banner and initial information about yo using the "**-q**" parameter.

Parameter	Description
-V / –version	This parameter provides information about your instance version.
-c	Identifying the configuration file
-T	Snort's self-test parameter, you can test your setup with this parameter.
-q	Quiet mode prevents snort from displaying the default banner and initial information about your set

That was an easy one; let's continue exploring snort modes!

Answer the questions below

Run the Snort instance and check the build number.

149

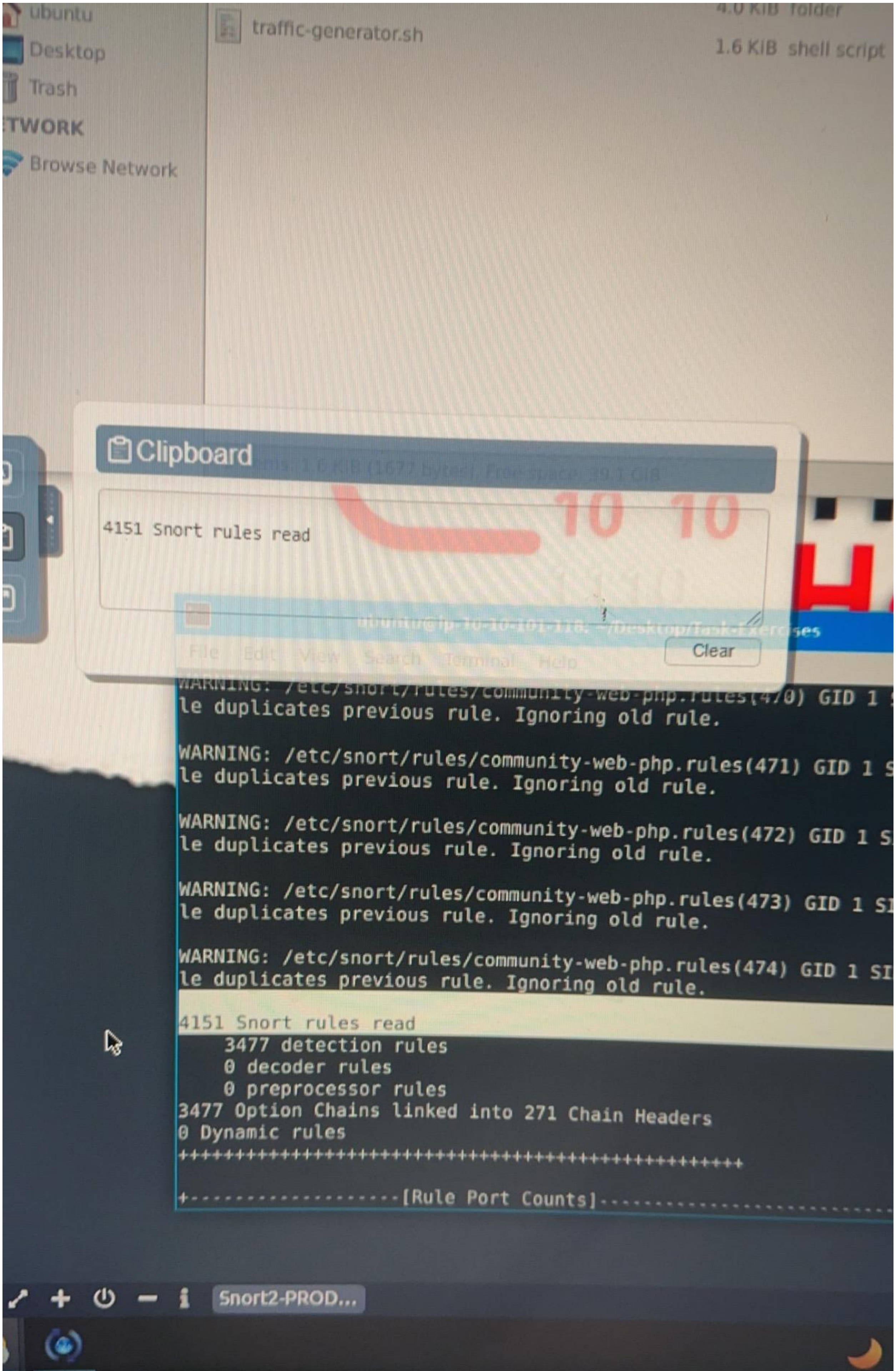
Test the current instance with "**/etc/snort/snort.conf**" file and check how many rules are loaded with the current build.

4151

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

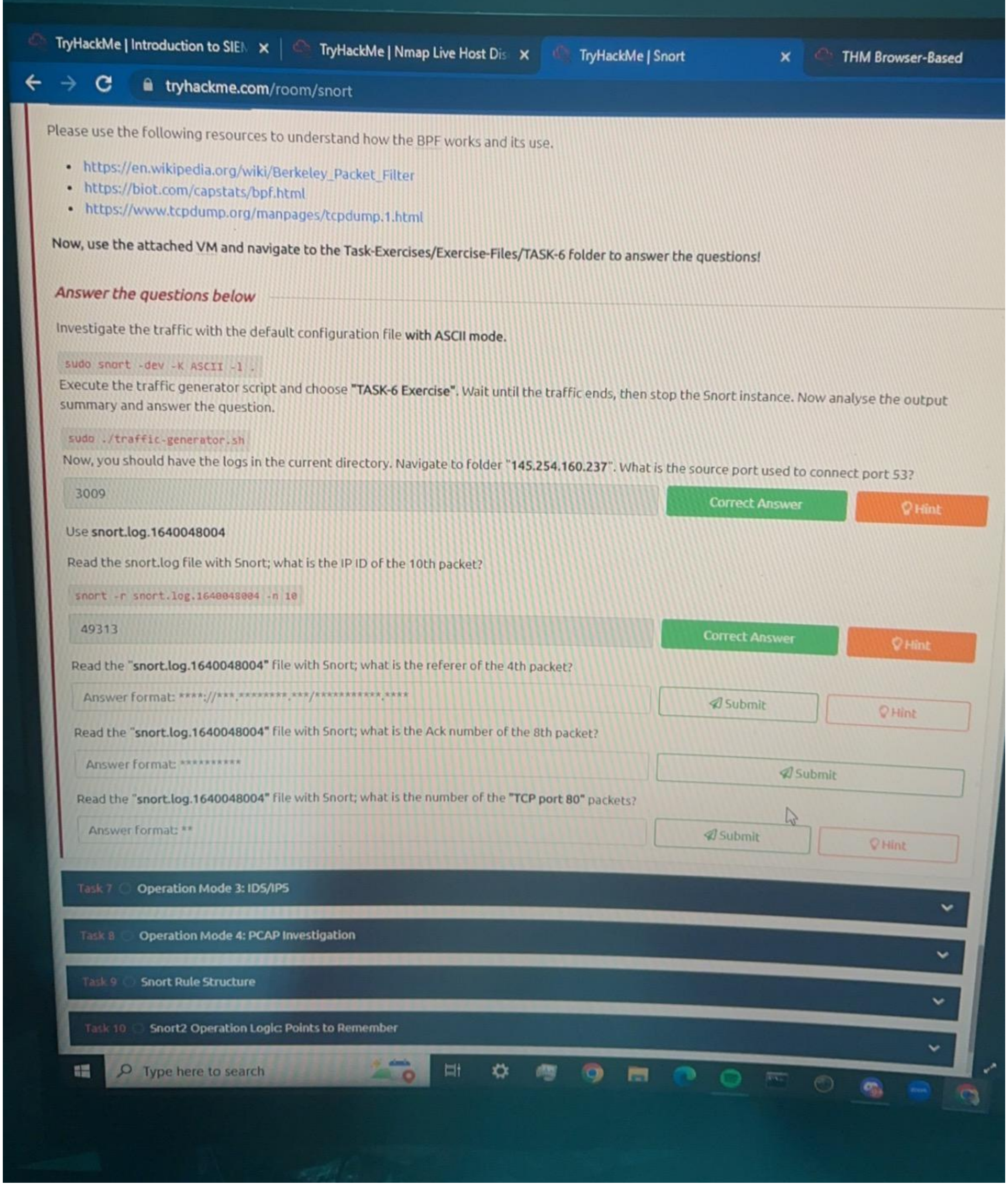
1

Correct Answ
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



```
4151 Snort rules read
```

```
WARNING: /etc/snort/rules/community-web-php.rules(470) GID 1 S
le duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(471) GID 1 S
le duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(472) GID 1 S
le duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(473) GID 1 SI
le duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(474) GID 1 SI
le duplicates previous rule. Ignoring old rule.

4151 Snort rules read
    3477 detection rules
    0 decoder rules
    0 preprocessor rules
3477 Option Chains linked into 271 Chain Headers
0 Dynamic rules
+++++++++++++++++++++++++++++++++++++++++++++++++++

+-------------------[Rule Port Counts]--------------------------
```



TryHackMe | Introduction to SIEM
TryHackMe | Nmap Live Host Dis
TryHackMe | Snort
THM Browser-Based
tryhackme.com/room/snort

Please use the following resources to understand how the BPF works and its use.

- https://en.wikipedia.org/wiki/Berkeley_Packet_Filter
- https://biot.com/capstats/bpf.html
- https://www.tcpdump.org/manpages/tcpdump.1.html

Now, use the attached VM and navigate to the Task-Exercises/Exercise-Files/TASK-6 folder to answer the questions!

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?

3009

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

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

Answer format: ****://***.********.***/***********.****

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

Answer format: **********

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

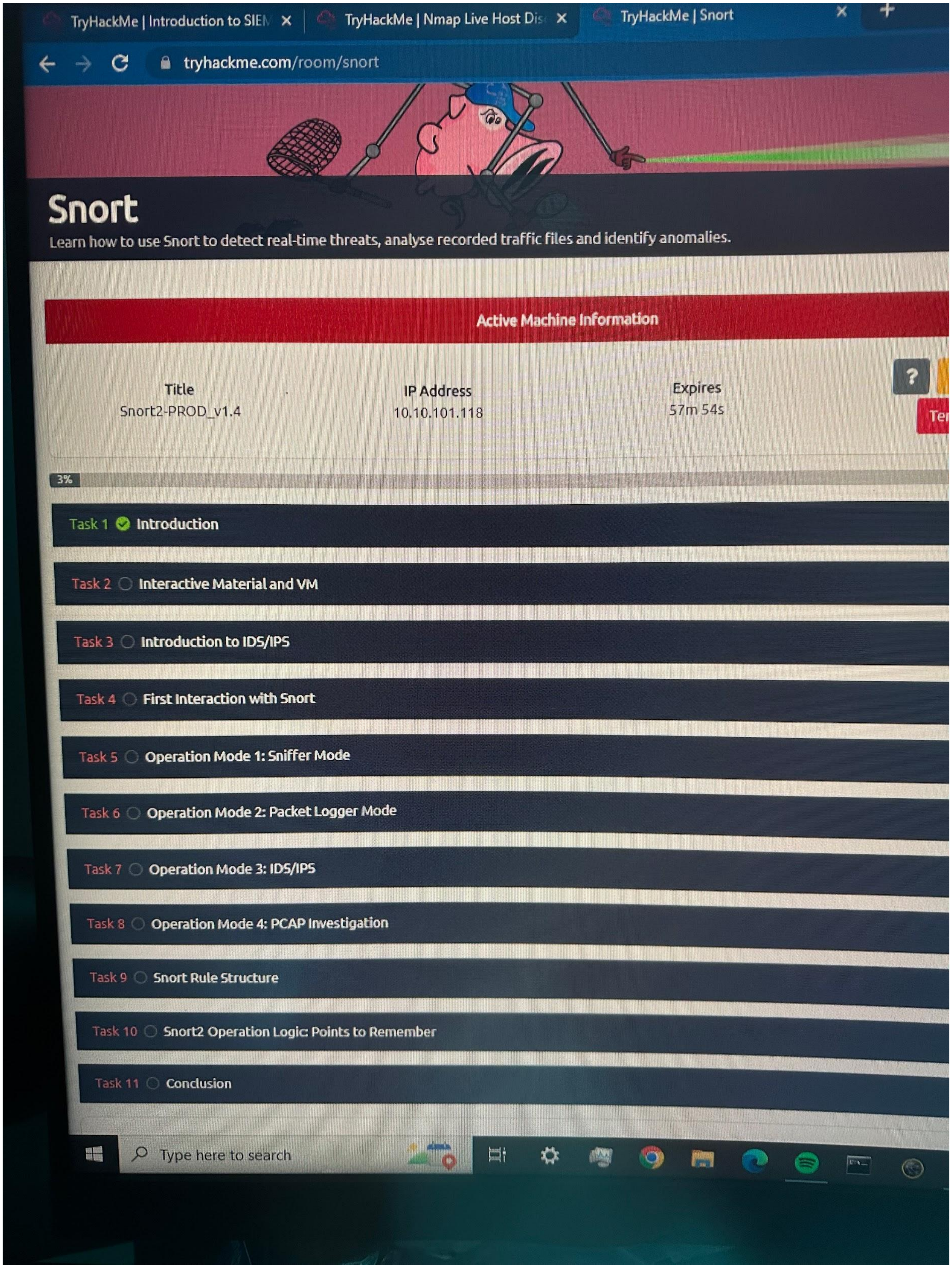
Answer format: **

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



TryHackMe | Introduction to SIEM ×   TryHackMe | Nmap Live Host Dis ×   TryHackMe | Snort ×   +

tryhackme.com/room/snort

Snort

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

Active Machine Information

Title	IP Address	Expires
Snort2-PROD_v1.4	10.10.101.118	57m 54s

- 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