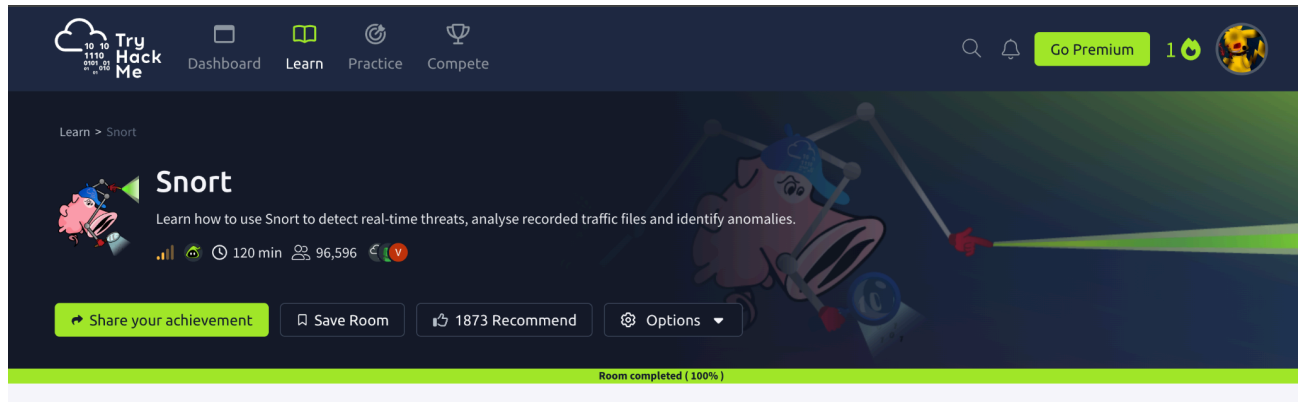


Configuration of Snort:

Prep for at home lab:

Before the completion of this at home lab, I completed a TryHackMe lab to gain more background knowledge about snort. A screenshot of the lab is shown below:



At home lab:

Updating my VM:

The commands I used to update my VM was:

```
sudo apt update
```

```
sudo apt upgrade -y
```

```
vansises@sv09:~$ sudo apt update
[sudo] password for vansises:
Hit:1 http://ports.ubuntu.com/ubuntu-ports jammy InRelease
Get:2 http://ports.ubuntu.com/ubuntu-ports jammy-updates InRelease [48.4 kB]
Get:3 http://ports.ubuntu.com/ubuntu-ports jammy-backports InRelease [62.6 kB]
Get:4 http://ports.ubuntu.com/ubuntu-ports jammy-security InRelease [62.6 kB]
50 packages can be upgraded. Run 'apt list --upgradable' to see them.
vansises@sv09:~$ sudo apt upgrade -y
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
Calculating upgrade... Done
The following NEW packages will be installed:
```

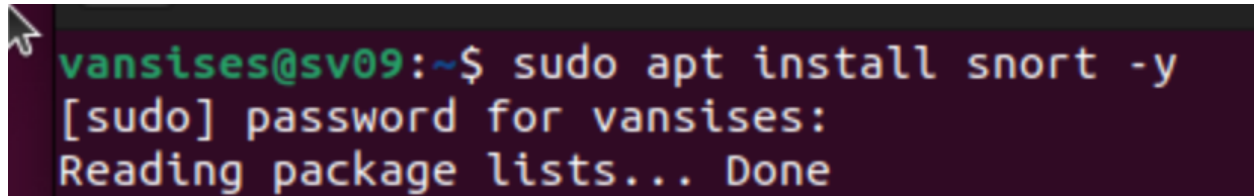
The purpose of this step is to:

- Be sure that everything on my VM is up to date and prepared to install Snort

Installing Snort onto my VM:

The command I used to install snort on my VM was:

```
sudo apt install snort -y
```



```
vansises@sv09:~$ sudo apt install snort -y
[sudo] password for vansises:
Reading package lists... Done
```

Before this the following command was needed to find specifics required to install Snort:
ip a

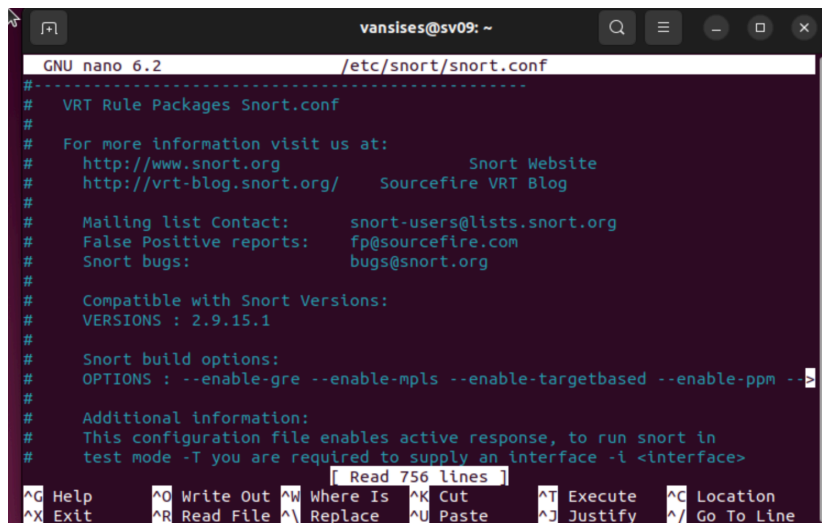
The purpose of this step is to:

- Be sure that everything on my VM is up to date and prepared to install Snort
- “ip a” is used to find your network interface and home network IP which are both required to install snort

Snort Configuration:

The command used to customize snort configuration was:

```
sudo nano /etc/snort/snort.conf
```



```
vansises@sv09: ~
GNU nano 6.2 /etc/snort/snort.conf
#-----
# VRT Rule Packages Snort.conf
#
# For more information visit us at:
#   http://www.snort.org           Snort Website
#   http://vrt-blog.snort.org/     Sourcefire VRT Blog
#
# Mailing list Contact:   snort-users@lists.snort.org
# False Positive reports: fp@sourcefire.com
# Snort bugs:             bugs@snort.org
#
# Compatible with Snort Versions:
# VERSIONS : 2.9.15.1
#
# Snort build options:
# OPTIONS : --enable-gre --enable-mpls --enable-targetbased --enable-ppm -->
#
# Additional information:
# This configuration file enables active response, to run snort in
# test mode -T you are required to supply an interface -i <interface>
[ Read 756 lines ]
^G Help      ^O Write Out ^W Where Is  ^K Cut       ^T Execute  ^C Location
^X Exit      ^R Read File ^I Replace   ^U Paste     ^D Justify  ^_ Go To Line
```

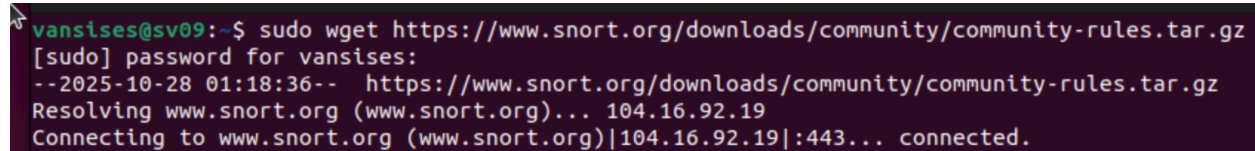
The purpose of this step is to:

- View and manage your snort configurations

Updating & Managing Snort Rules:

The following command was used to install snort's community ruleset:

`sudo wget https://www.snort.org/downloads/community/community-rules.tar.gz`



```
vansises@sv09:~$ sudo wget https://www.snort.org/downloads/community/community-rules.tar.gz
[sudo] password for vansises:
--2025-10-28 01:18:36-- https://www.snort.org/downloads/community/community-rules.tar.gz
Resolving www.snort.org (www.snort.org)... 104.16.92.19
Connecting to www.snort.org (www.snort.org)|104.16.92.19|:443... connected.
```

To add custom rules in snort the following command can be used:

`sudo nano /etc/snort/rules/local.rules`

The purpose of this step is to:

- Create a ruleset with capabilities of
 - Detecting threats
 - Monitoring traffic through your network
 - Alerting the user of suspicious activity
 - Preventing attacks

Important rule types and their functions:

Local.rules → Custom rules you create yourself

Icmp.rules → Rules detecting ICMP traffic (like pings)

Sql.rules → Detects SQL injection attempts

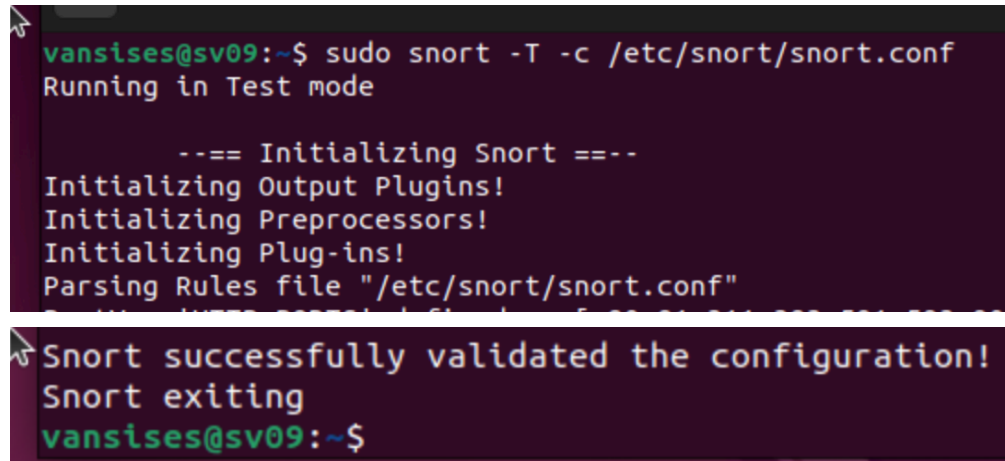
Dos.rules → Denial-of-Service attack signatures

Exploit.rules → Known exploit signatures for various software

Testing Snort Configuration:

The command I used to test that snort was configured was:

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

A terminal window with a dark background and light green text. The prompt is 'vansises@sv09:~\$'. The command 'sudo snort -T -c /etc/snort/snort.conf' has been executed. The output shows 'Running in Test mode' followed by a series of initialization messages: '--== Initializing Snort ==--', 'Initializing Output Plugins!', 'Initializing Preprocessors!', 'Initializing Plug-ins!', and 'Parsing Rules file "/etc/snort/snort.conf"'. The final line of the screenshot shows 'Snort successfully validated the configuration!', 'Snort exiting', and the prompt 'vansises@sv09:~\$'.

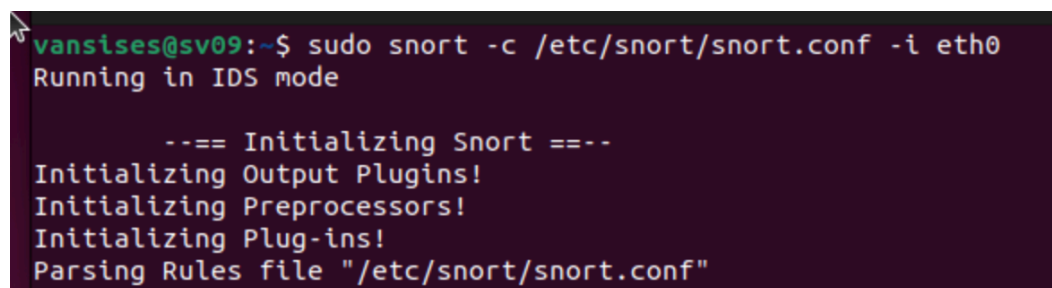
The purpose of this command is to:

- Be sure that snort was configured correctly
- Through confirmation from the system we know that snort is functioning properly

Running Snort in IDS Mode:

The command I used to run snort in IDS mode was:

```
sudo snort -c /etc/snort/snort.conf -i eth0
```

A terminal window with a dark background and light green text. The prompt is 'vansises@sv09:~\$'. The command 'sudo snort -c /etc/snort/snort.conf -i eth0' has been executed. The output shows 'Running in IDS mode' followed by a series of initialization messages: '--== Initializing Snort ==--', 'Initializing Output Plugins!', 'Initializing Preprocessors!', 'Initializing Plug-ins!', and 'Parsing Rules file "/etc/snort/snort.conf"'. The screenshot ends with the first line of the initialization messages.

The purpose of this command is to:

- Monitor traffic going through your network
- Logs any alerts of suspicious activity
- Runs until user forces exit with (ctrl + c)

Viewing Logs From Snort:

Snort logs are stored in the following directory:

/var/log/snort/

The items found here were:

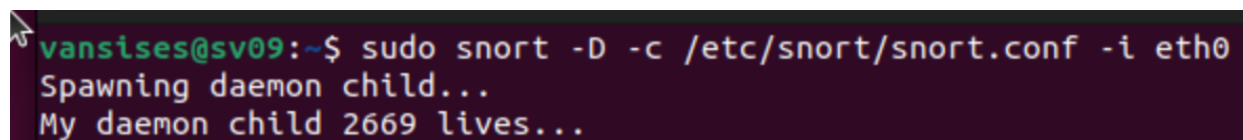
snort.alert.fast

This is the output file for any alerts that were made from oddities detected by snort. My file was empty due to no active alerts or threats being found.

Running Snort as a Daemon:

The command I used to run snort in the background as a Daemon was:

```
sudo snort -D -c /etc/snort/snort.conf -i eth0
```

A terminal window with a dark background. The prompt is 'vansises@sv09:~\$'. The command entered is 'sudo snort -D -c /etc/snort/snort.conf -i eth0'. The output shows 'Spawning daemon child...' and 'My daemon child 2669 lives...'.

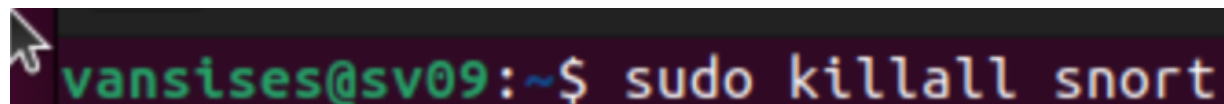
```
vansises@sv09:~$ sudo snort -D -c /etc/snort/snort.conf -i eth0
Spawning daemon child...
My daemon child 2669 lives...
```

The purpose of this command is to:

- Continuously monitor your specified network in the background

The command used to stop snort once it starts running is:

```
sudo killall snort
```

A terminal window with a dark background. The prompt is 'vansises@sv09:~\$'. The command entered is 'sudo killall snort'.

```
vansises@sv09:~$ sudo killall snort
```