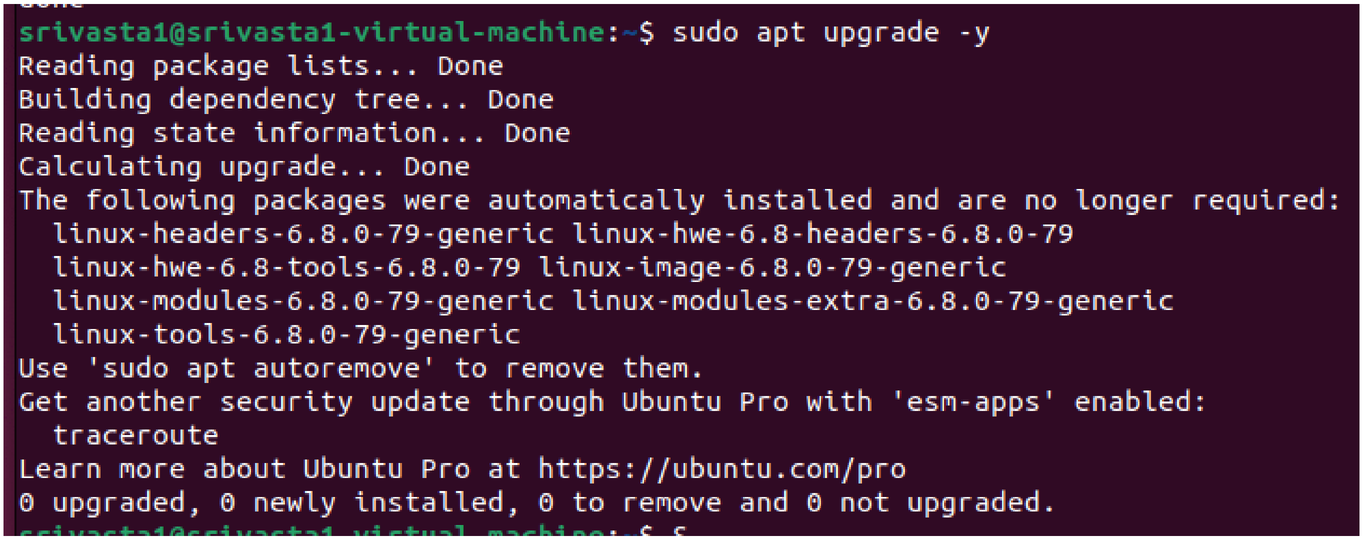
Network Security with Snort

In this assignment, I’m installing and configuring Snort on my Ubuntu Virtual Machine. This is just a starting point for how I can use Snort, so I’m excited to explore and experiment with the configuration files!

Step 1: Update the System

I want to ensure my system is up to date before installing Snort, so I run these commands:

```
sudo apt update
sudo apt upgrade -y
```



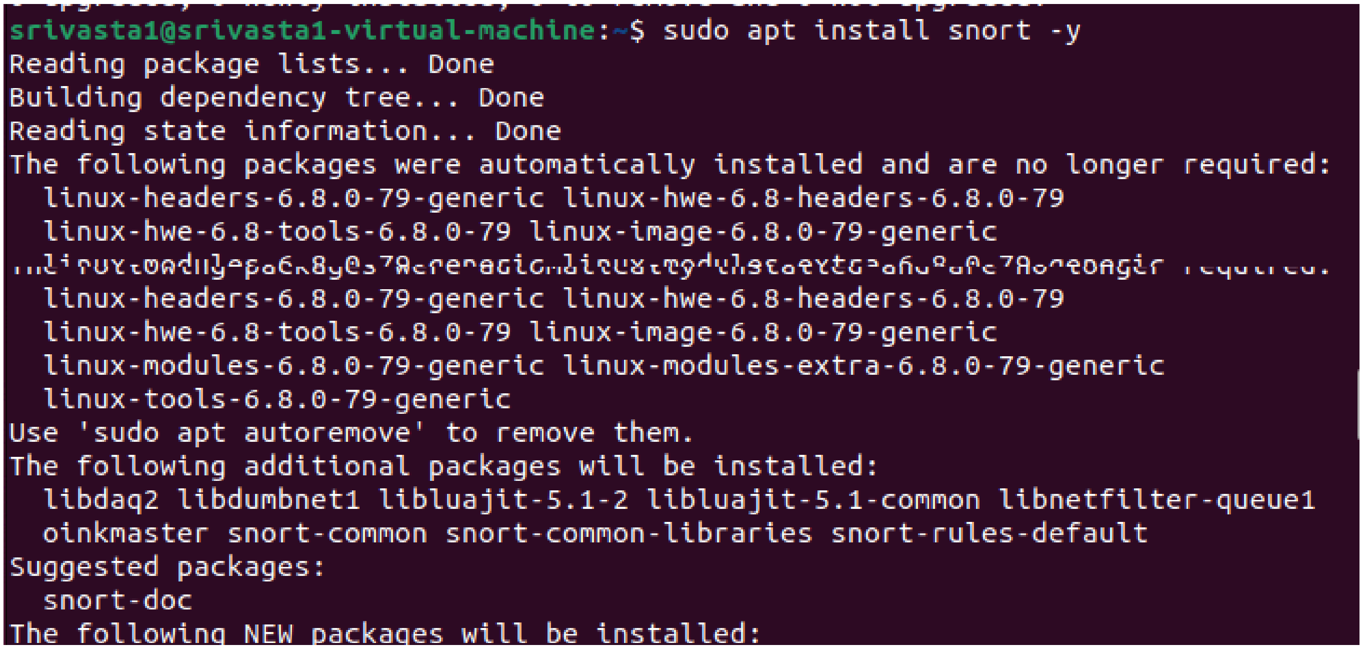
```
done
srivasta1@srivasta1-virtual-machine:~$ sudo apt upgrade -y
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
Calculating upgrade... Done
The following packages were automatically installed and are no longer required:
  linux-headers-6.8.0-79-generic linux-hwe-6.8-headers-6.8.0-79
  linux-hwe-6.8-tools-6.8.0-79 linux-image-6.8.0-79-generic
  linux-modules-6.8.0-79-generic linux-modules-extra-6.8.0-79-generic
  linux-tools-6.8.0-79-generic
Use 'sudo apt autoremove' to remove them.
Get another security update through Ubuntu Pro with 'esm-apps' enabled:
  traceroute
Learn more about Ubuntu Pro at https://ubuntu.com/pro
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
srivasta1@srivasta1-virtual-machine:~$
```

image_2025-10-27_18-32-36.png

Step 2: Install Snort

I’m installing Snort directly using apt with this command:

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



```
srivasta1@srivasta1-virtual-machine:~$ sudo apt install snort -y
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages were automatically installed and are no longer required:
  linux-headers-6.8.0-79-generic linux-hwe-6.8-headers-6.8.0-79
  linux-hwe-6.8-tools-6.8.0-79 linux-image-6.8.0-79-generic
[illegible]
  linux-headers-6.8.0-79-generic linux-hwe-6.8-headers-6.8.0-79
  linux-hwe-6.8-tools-6.8.0-79 linux-image-6.8.0-79-generic
  linux-modules-6.8.0-79-generic linux-modules-extra-6.8.0-79-generic
  linux-tools-6.8.0-79-generic
Use 'sudo apt autoremove' to remove them.
The following additional packages will be installed:
  libdaq2 libdumbnet1 libluajit-5.1-2 libluajit-5.1-common libnetfilter-queue1
  oinkmaster snort-common snort-common-libraries snort-rules-default
Suggested packages:
  snort-doc
The following NEW packages will be installed:
```

image_2025-10-27_18-33-24.png

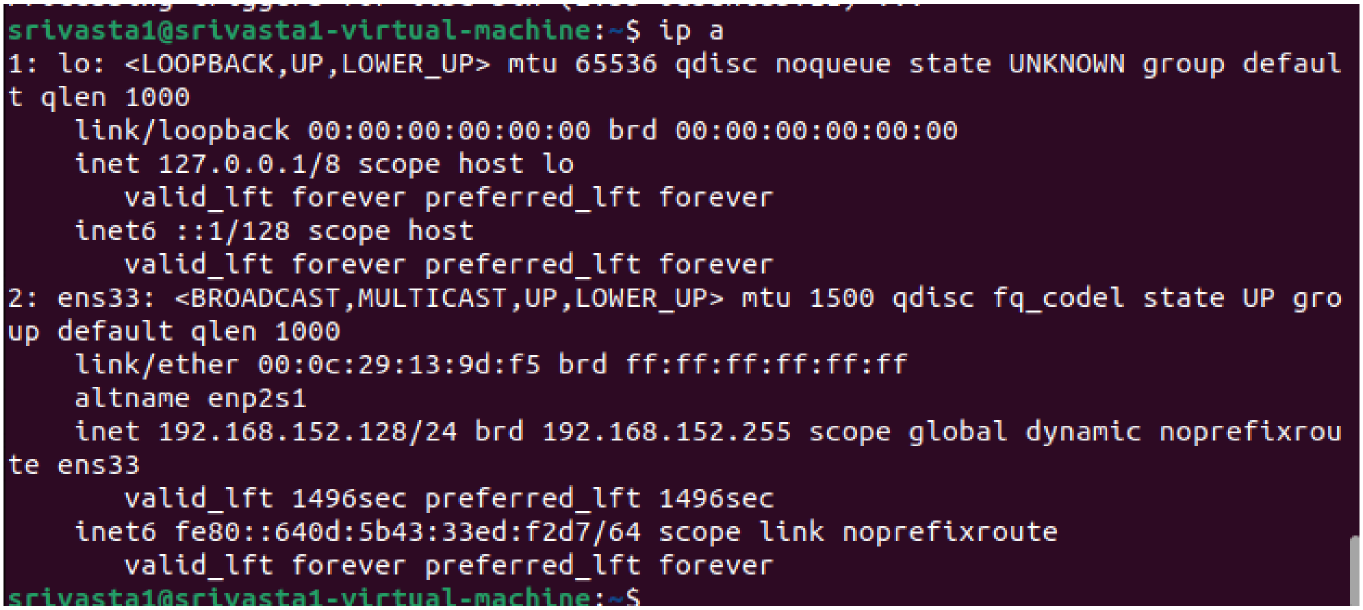
During the installation, I'm prompted to enter the network interface and the HOME_NET IP range that Snort will monitor. I need to decide on:

1. **Network Interface:** I'll enter the interface I want Snort to monitor (e.g., `eth0`, `enX0`, `ens33`, etc.).
2. **HOME_NET:** I'll define my home network (e.g., `192.168.1.0/24` for a private network or `any` to monitor all networks).

After installation, I notice Snort is installed to `/etc/snort/` with the default configuration and rules.

To find my network interface, I run this command:

```
ip a
```

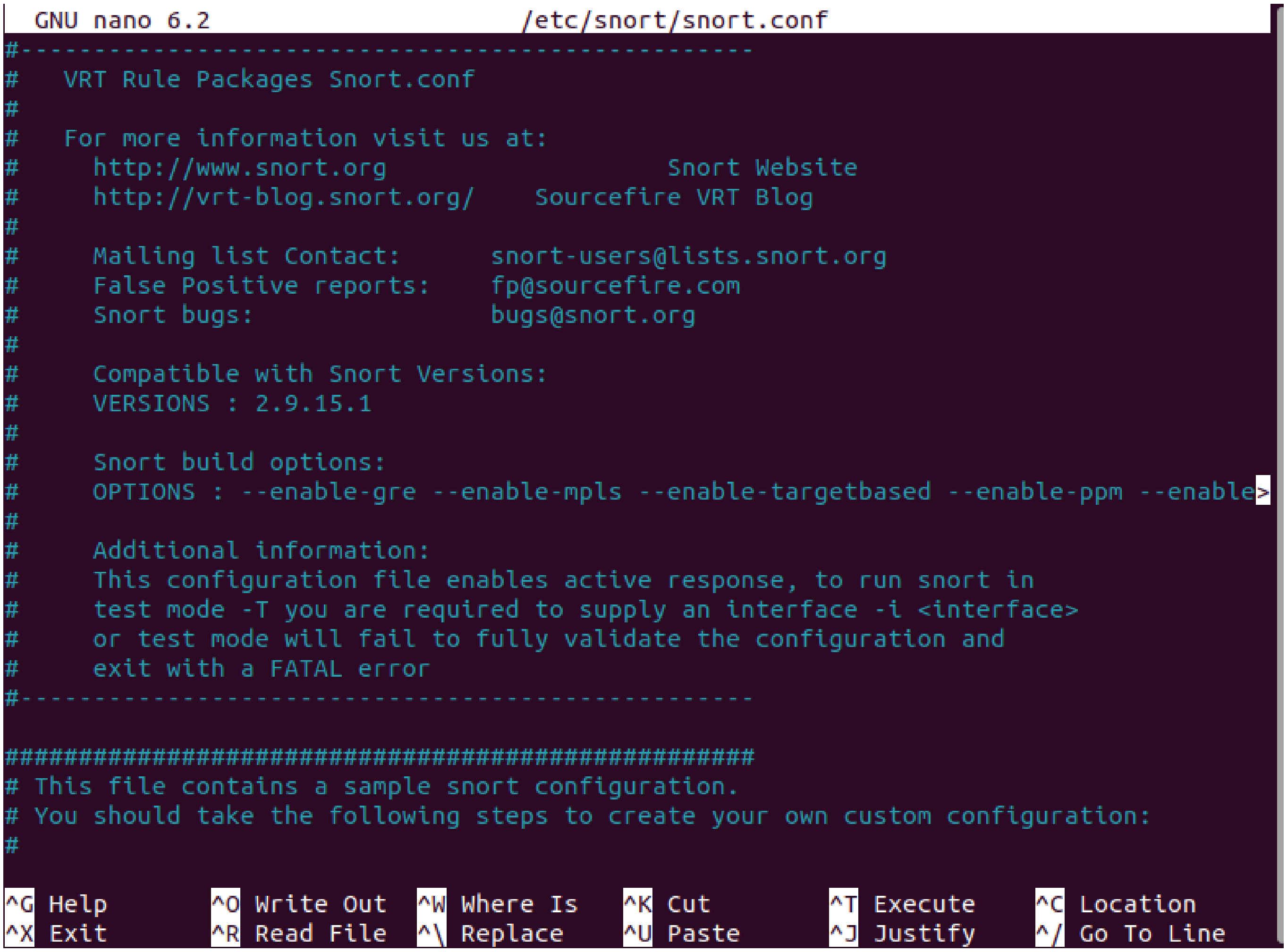


```
srivasta1@srivasta1-virtual-machine:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group defaul
t qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP gro
up default qlen 1000
    link/ether 00:0c:29:13:9d:f5 brd ff:ff:ff:ff:ff:ff
    altname enp2s1
    inet 192.168.152.128/24 brd 192.168.152.255 scope global dynamic noprefixrou
te ens33
       valid_lft 1496sec preferred_lft 1496sec
    inet6 fe80::640d:5b43:33ed:f2d7/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
srivasta1@srivasta1-virtual-machine:~$
```

image_2025-10-27_18-33-45-1.png

Step 3: Configure Snort

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



```
  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 --enable>
#
#     Additional information:
#     This configuration file enables active response, to run snort in
#     test mode -T you are required to supply an interface -i <interface>
#     or test mode will fail to fully validate the configuration and
#     exit with a FATAL error
#--------------------------------------------------

###################################################
# This file contains a sample snort configuration.
# You should take the following steps to create your own custom configuration:
#
^G Help         ^O Write Out    ^W Where Is     ^K Cut          ^T Execute      ^C Location
^X Exit         ^R Read File    ^\ Replace      ^U Paste        ^J Justify      ^/ Go To Line
```

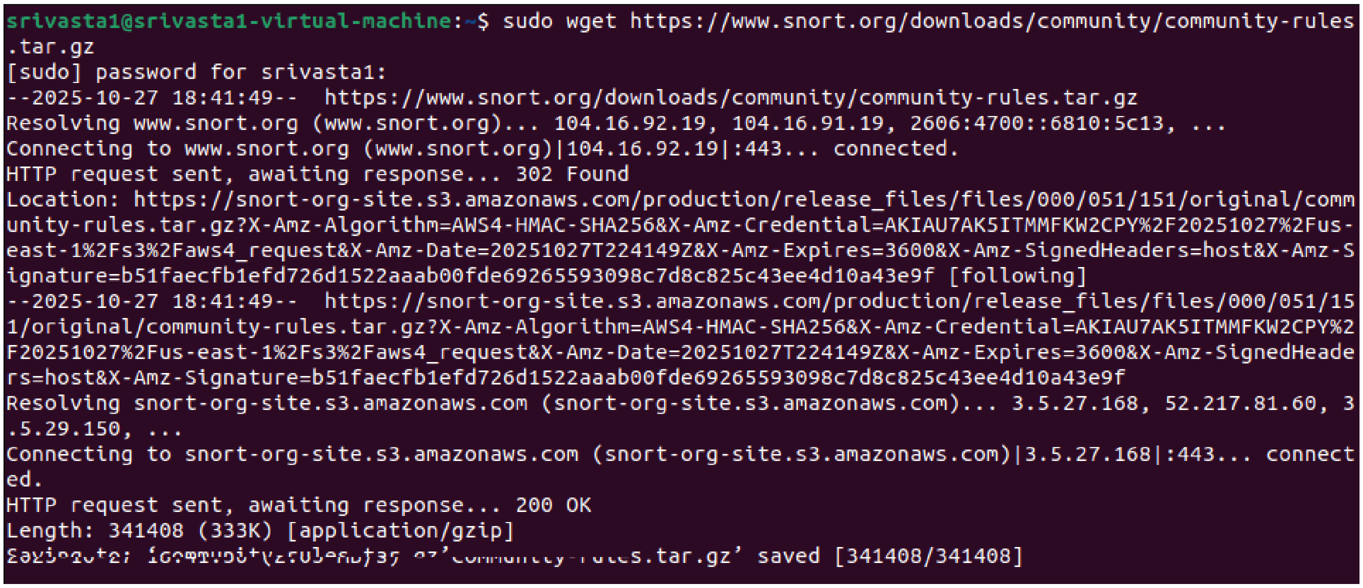
image_2025-10-27_18-35-17.png

Step 4: Update and Manage Snort Rules

By default, Snort comes with community rules, but I can download and add additional rules for better threat detection.

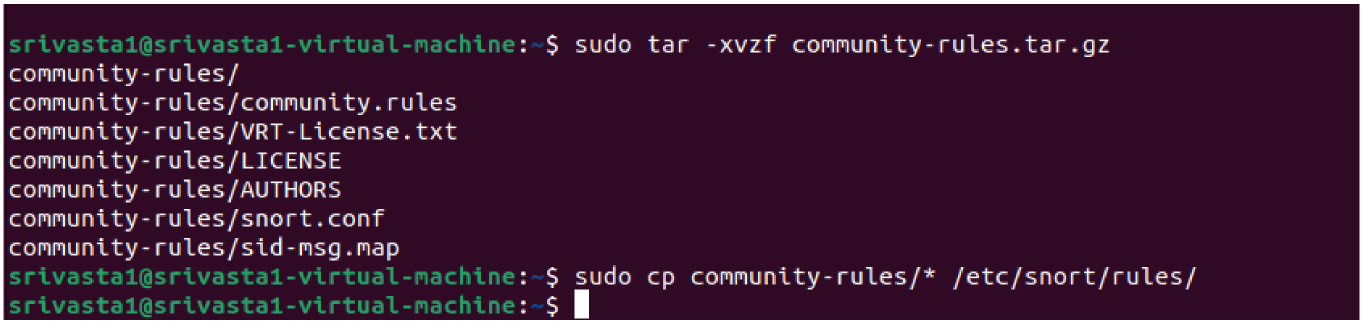
If I need to, I download community rules with:

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



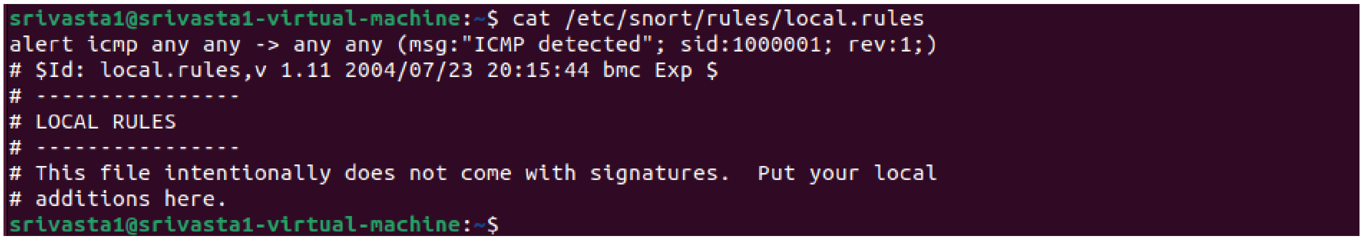
```
srivasta1@srivasta1-virtual-machine:~$ sudo wget https://www.snort.org/downloads/community/community-rules
.tar.gz
[sudo] password for srivasta1:
--2025-10-27 18:41:49--  https://www.snort.org/downloads/community/community-rules.tar.gz
Resolving www.snort.org (www.snort.org)... 104.16.92.19, 104.16.91.19, 2606:4700::6810:5c13, ...
Connecting to www.snort.org (www.snort.org)|104.16.92.19|:443... connected.
HTTP request sent, awaiting response... 302 Found
Location: https://snort-org-site.s3.amazonaws.com/production/release_files/files/000/051/151/original/comm
unity-rules.tar.gz?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=AKIAU7AK5ITMMFKW2CPY%2F20251027%2Fus-
east-1%2Fs3%2Faws4_request&X-Amz-Date=20251027T224149Z&X-Amz-Expires=3600&X-Amz-SignedHeaders=host&X-Amz-S
ignature=b51faecfb1efd726d1522aaab00fde69265593098c7d8c825c43ee4d10a43e9f [following]
--2025-10-27 18:41:49--  https://snort-org-site.s3.amazonaws.com/production/release_files/files/000/051/15
1/original/community-rules.tar.gz?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=AKIAU7AK5ITMMFKW2CPY%2
F20251027%2Fus-east-1%2Fs3%2Faws4_request&X-Amz-Date=20251027T224149Z&X-Amz-Expires=3600&X-Amz-SignedHeade
rs=host&X-Amz-Signature=b51faecfb1efd726d1522aaab00fde69265593098c7d8c825c43ee4d10a43e9f
Resolving snort-org-site.s3.amazonaws.com (snort-org-site.s3.amazonaws.com)... 3.5.27.168, 52.217.81.60, 3
.5.29.150, ...
Connecting to snort-org-site.s3.amazonaws.com (snort-org-site.s3.amazonaws.com)|3.5.27.168|:443... connect
ed.
HTTP request sent, awaiting response... 200 OK
Length: 341408 (333K) [application/gzip]
[illegible]’community-rules.tar.gz’ saved [341408/341408]
```

image_2025-10-27_18-41-44.png



```
srivasta1@srivasta1-virtual-machine:~$ sudo tar -xvzf community-rules.tar.gz
community-rules/
community-rules/community.rules
community-rules/VRT-License.txt
community-rules/LICENSE
community-rules/AUTHORS
community-rules/snort.conf
community-rules/sid-msg.map
srivasta1@srivasta1-virtual-machine:~$ sudo cp community-rules/* /etc/snort/rules/
srivasta1@srivasta1-virtual-machine:~$ 
```

image_2025-10-27_18-43-22.png

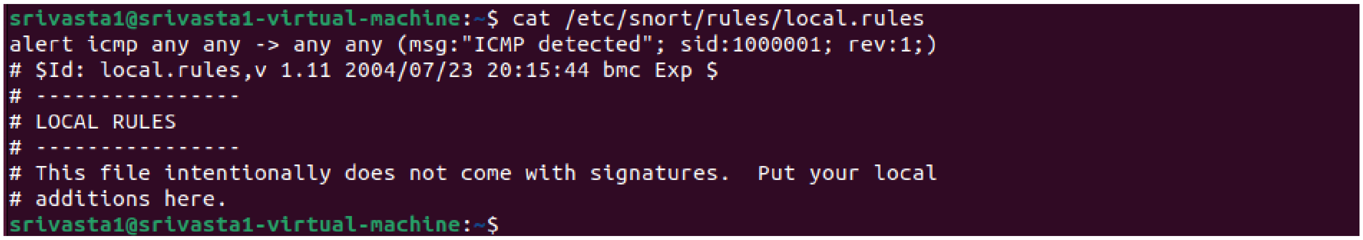


```
srivasta1@srivasta1-virtual-machine:~$ cat /etc/snort/rules/local.rules
alert icmp any any -> any any (msg:"ICMP detected"; sid:1000001; rev:1;)
# $Id: local.rules,v 1.11 2004/07/23 20:15:44 bmc Exp $
# ----------------
# LOCAL RULES
# ----------------
# This file intentionally does not come with signatures.  Put your local
# additions here.
srivasta1@srivasta1-virtual-machine:~$
```

image_2025-10-27_18-53-13.png

If I want to add my own rules, I manually edit the local rule file:

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

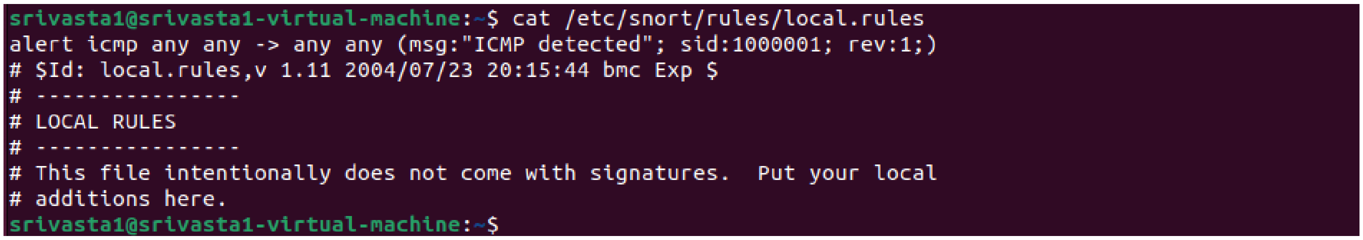


```
srivasta1@srivasta1-virtual-machine:~$ cat /etc/snort/rules/local.rules
alert icmp any any -> any any (msg:"ICMP detected"; sid:1000001; rev:1;)
# $Id: local.rules,v 1.11 2004/07/23 20:15:44 bmc Exp $
# ----------------
# LOCAL RULES
# ----------------
# This file intentionally does not come with signatures.  Put your local
# additions here.
srivasta1@srivasta1-virtual-machine:~$
```

image_2025-10-27_18-53-13.png

Then, I add custom rules if needed. For example, I use:

```
alert icmp any any -> any any (msg:"ICMP detected"; sid:1000001; rev:1;)
```



```
srivasta1@srivasta1-virtual-machine:~$ cat /etc/snort/rules/local.rules
alert icmp any any -> any any (msg:"ICMP detected"; sid:1000001; rev:1;)
# $Id: local.rules,v 1.11 2004/07/23 20:15:44 bmc Exp $
# ----------------
# LOCAL RULES
# ----------------
# This file intentionally does not come with signatures.  Put your local
# additions here.
srivasta1@srivasta1-virtual-machine:~$
```

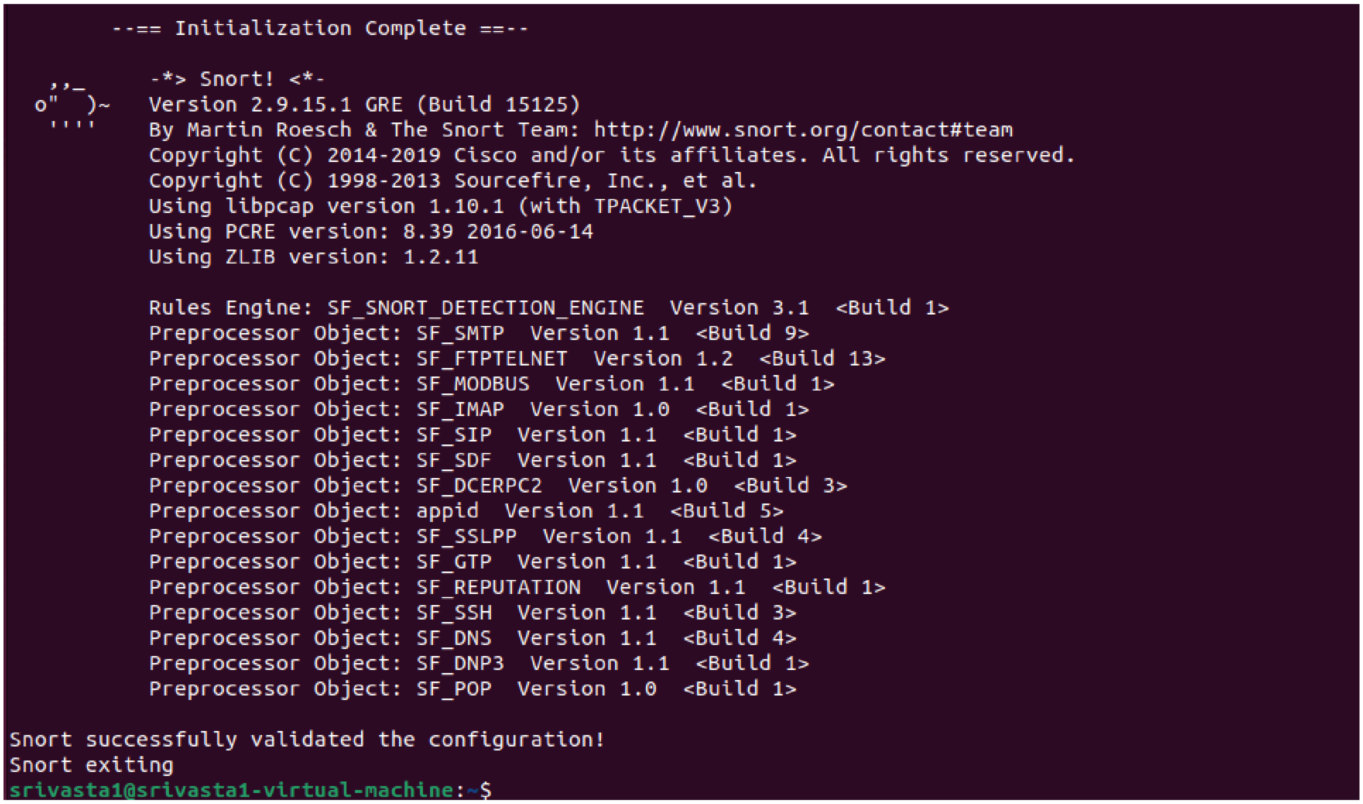
image_2025-10-27_18-53-13.png

I check out the various rule files in the `rules` directory. Which rules stick out to me? The `malware.rules` file stood out to me because it contains rules to detect malware-related traffic, which feels critical for security. What is the purpose of rules in general? Rules define patterns in network traffic to identify threats like intrusions or malware, triggering alerts to help me monitor and secure my network.

Step 5: Test Snort Configuration

After configuring, I test that Snort is working properly by running a configuration test:

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



```
        --== Initialization Complete ==--

   ,,_     -*> Snort! <*-
  o"  )~   Version 2.9.15.1 GRE (Build 15125)
   ''''    By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
           Copyright (C) 2014-2019 Cisco and/or its affiliates. All rights reserved.
           Copyright (C) 1998-2013 Sourcefire, Inc., et al.
           Using libpcap version 1.10.1 (with TPACKET_V3)
           Using PCRE version: 8.39 2016-06-14
           Using ZLIB version: 1.2.11

           Rules Engine: SF_SNORT_DETECTION_ENGINE  Version 3.1  <Build 1>
           Preprocessor Object: SF_SMTP  Version 1.1  <Build 9>
           Preprocessor Object: SF_FTPTELNET  Version 1.2  <Build 13>
           Preprocessor Object: SF_MODBUS  Version 1.1  <Build 1>
           Preprocessor Object: SF_IMAP  Version 1.0  <Build 1>
           Preprocessor Object: SF_SIP  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: appid  Version 1.1  <Build 5>
           Preprocessor Object: SF_SSLPP  Version 1.1  <Build 4>
           Preprocessor Object: SF_GTP  Version 1.1  <Build 1>
           Preprocessor Object: SF_REPUTATION  Version 1.1  <Build 1>
           Preprocessor Object: SF_SSH  Version 1.1  <Build 3>
           Preprocessor Object: SF_DNS  Version 1.1  <Build 4>
           Preprocessor Object: SF_DNP3  Version 1.1  <Build 1>
           Preprocessor Object: SF_POP  Version 1.0  <Build 1>

Snort successfully validated the configuration!
Snort exiting
srivasta1@srivasta1-virtual-machine:~$
```

image_2025-10-27_18-53-59.png

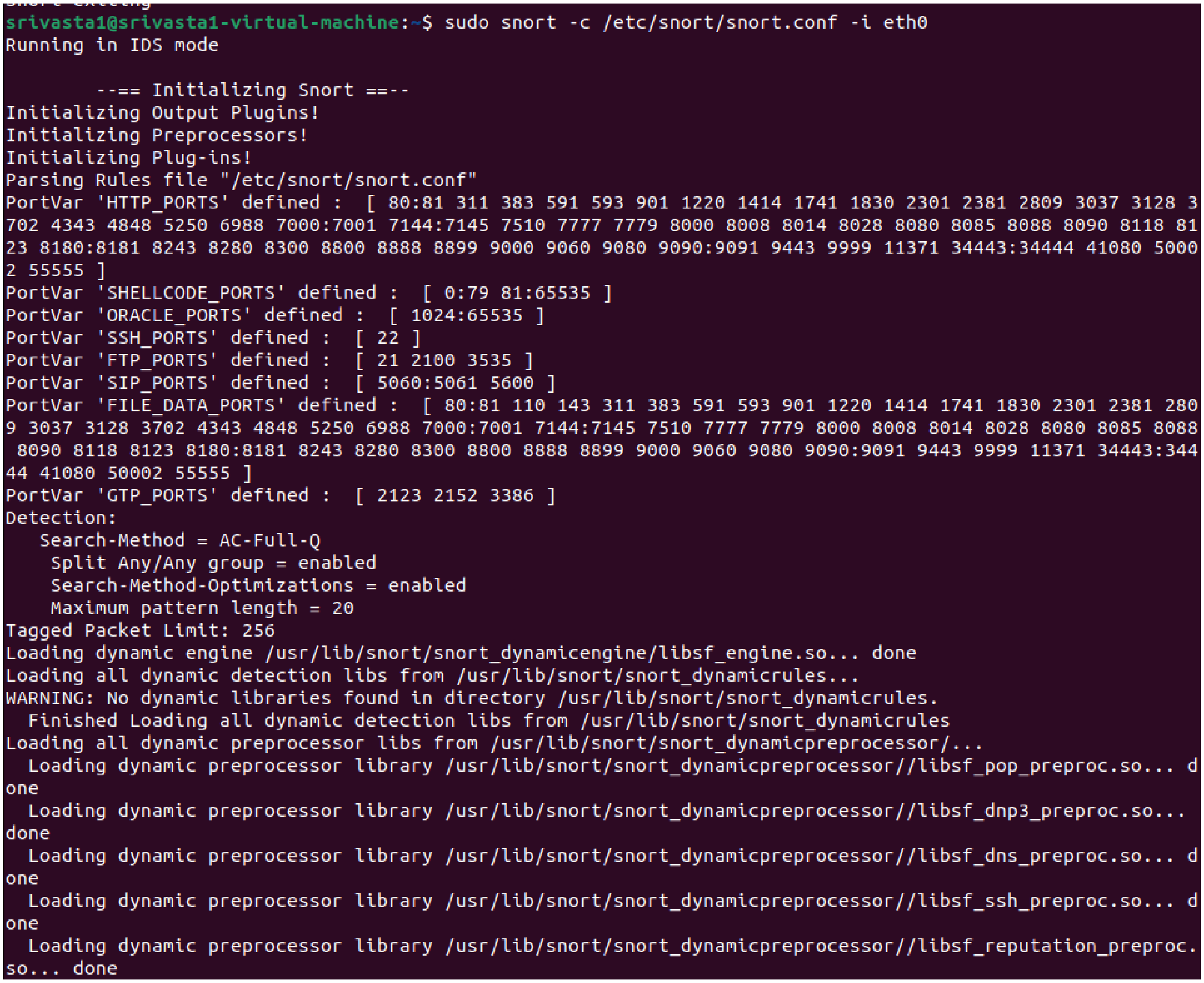
If the configuration is correct, I see a message like:

Snort successfully validated the configuration! (As visible in the screenshot above)

Step 6: Running Snort in IDS Mode

Now that Snort is installed and configured, I run it in IDS mode to monitor traffic. I specify the interface to monitor (e.g., `eth0`, `enX0`, etc.) with:

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



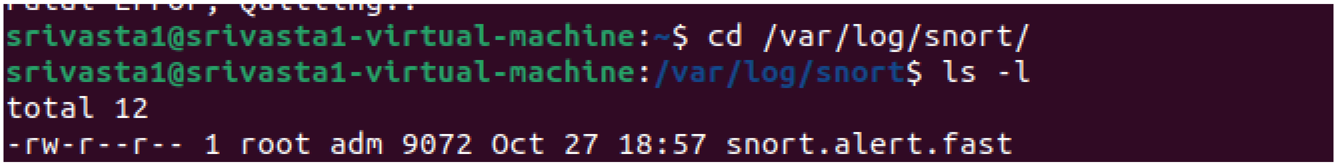
```
Snort exiting
srivasta1@srivasta1-virtual-machine:~$ sudo snort -c /etc/snort/snort.conf -i eth0
Running in IDS mode

        --== Initializing Snort ==--
Initializing Output Plugins!
Initializing Preprocessors!
Initializing Plug-ins!
Parsing Rules file "/etc/snort/snort.conf"
PortVar 'HTTP_PORTS' defined :  [ 80:81 311 383 591 593 901 1220 1414 1741 1830 2301 2381 2809 3037 3128 3
702 4343 4848 5250 6988 7000:7001 7144:7145 7510 7777 7779 8000 8008 8014 8028 8080 8085 8088 8090 8118 81
23 8180:8181 8243 8280 8300 8800 8888 8899 9000 9060 9080 9090:9091 9443 9999 11371 34443:34444 41080 5000
2 55555 ]
PortVar 'SHELLCODE_PORTS' defined :  [ 0:79 81:65535 ]
PortVar 'ORACLE_PORTS' defined :  [ 1024:65535 ]
PortVar 'SSH_PORTS' defined :  [ 22 ]
PortVar 'FTP_PORTS' defined :  [ 21 2100 3535 ]
PortVar 'SIP_PORTS' defined :  [ 5060:5061 5600 ]
PortVar 'FILE_DATA_PORTS' defined :  [ 80:81 110 143 311 383 591 593 901 1220 1414 1741 1830 2301 2381 280
9 3037 3128 3702 4343 4848 5250 6988 7000:7001 7144:7145 7510 7777 7779 8000 8008 8014 8028 8080 8085 8088
 8090 8118 8123 8180:8181 8243 8280 8300 8800 8888 8899 9000 9060 9080 9090:9091 9443 9999 11371 34443:344
44 41080 50002 55555 ]
PortVar 'GTP_PORTS' defined :  [ 2123 2152 3386 ]
Detection:
   Search-Method = AC-Full-Q
    Split Any/Any group = enabled
    Search-Method-Optimizations = enabled
    Maximum pattern length = 20
Tagged Packet Limit: 256
Loading dynamic engine /usr/lib/snort/snort_dynamicengine/libsf_engine.so... done
Loading all dynamic detection libs from /usr/lib/snort/snort_dynamicrules...
WARNING: No dynamic libraries found in directory /usr/lib/snort/snort_dynamicrules.
  Finished Loading all dynamic detection libs from /usr/lib/snort/snort_dynamicrules
Loading all dynamic preprocessor libs from /usr/lib/snort/snort_dynamicpreprocessor/...
  Loading dynamic preprocessor library /usr/lib/snort/snort_dynamicpreprocessor//libsf_pop_preproc.so... d
one
  Loading dynamic preprocessor library /usr/lib/snort/snort_dynamicpreprocessor//libsf_dnp3_preproc.so...
done
  Loading dynamic preprocessor library /usr/lib/snort/snort_dynamicpreprocessor//libsf_dns_preproc.so... d
one
  Loading dynamic preprocessor library /usr/lib/snort/snort_dynamicpreprocessor//libsf_ssh_preproc.so... d
one
  Loading dynamic preprocessor library /usr/lib/snort/snort_dynamicpreprocessor//libsf_reputation_preproc.
so... done
```

image_2025-10-27_18-55-21.png

Snort now monitors my network traffic and logs alerts. To exit, I hit `ctrl+c`.

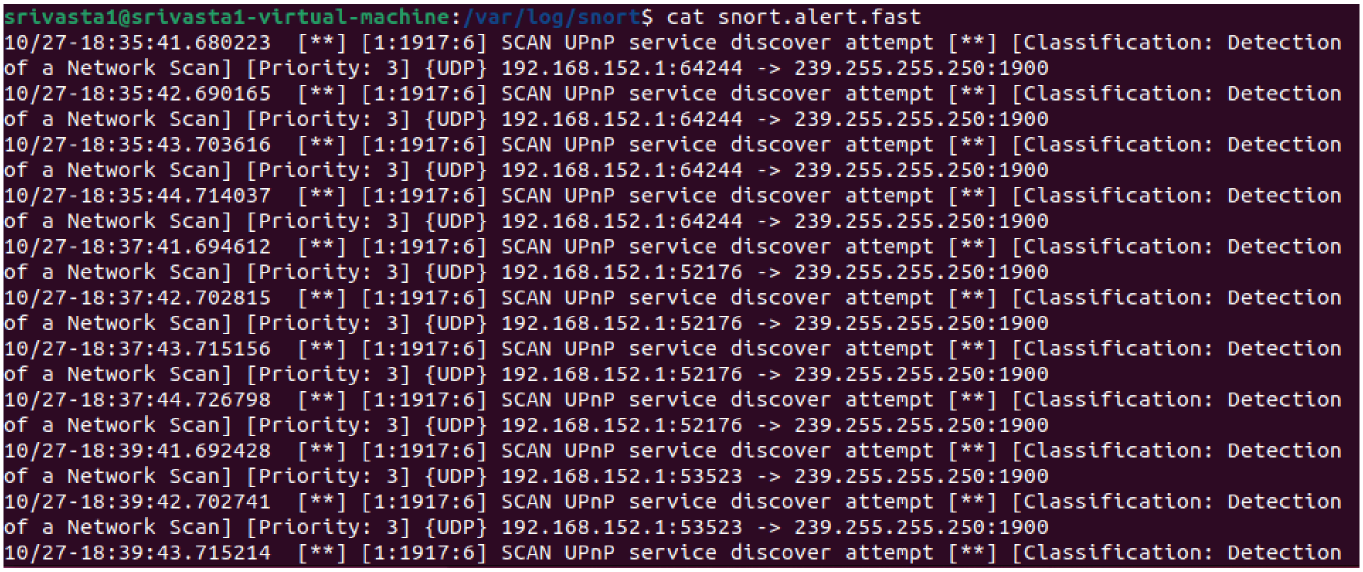
Step 7: Viewing Snort Logs

Snort logs alerts in the `/var/log/snort/` directory. I go to this directory. I found a file named `snort.alert.fast` in the `/var/log/snort/` directory. It's empty because I haven't generated enough network traffic (like ICMP pings) to trigger my rule, or Snort might need more time running as a daemon to log events. It's likely empty due to insufficient traffic or recent daemon startup.



```
Fatal Error, Quitting!!
srivasta1@srivasta1-virtual-machine:~$ cd /var/log/snort/
srivasta1@srivasta1-virtual-machine:/var/log/snort$ ls -l
total 12
-rw-r--r-- 1 root adm 9072 Oct 27 18:57 snort.alert.fast
```

image_2025-10-27_18-59-13.png



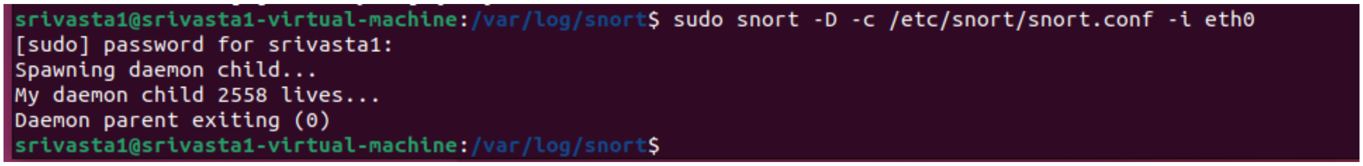
```
srivasta1@srivasta1-virtual-machine:/var/log/snort$ cat snort.alert.fast
10/27-18:35:41.680223  [**] [1:1917:6] SCAN UPnP service discover attempt [**] [Classification: Detection
of a Network Scan] [Priority: 3] {UDP} 192.168.152.1:64244 -> 239.255.255.250:1900
10/27-18:35:42.690165  [**] [1:1917:6] SCAN UPnP service discover attempt [**] [Classification: Detection
of a Network Scan] [Priority: 3] {UDP} 192.168.152.1:64244 -> 239.255.255.250:1900
10/27-18:35:43.703616  [**] [1:1917:6] SCAN UPnP service discover attempt [**] [Classification: Detection
of a Network Scan] [Priority: 3] {UDP} 192.168.152.1:64244 -> 239.255.255.250:1900
10/27-18:35:44.714037  [**] [1:1917:6] SCAN UPnP service discover attempt [**] [Classification: Detection
of a Network Scan] [Priority: 3] {UDP} 192.168.152.1:64244 -> 239.255.255.250:1900
10/27-18:37:41.694612  [**] [1:1917:6] SCAN UPnP service discover attempt [**] [Classification: Detection
of a Network Scan] [Priority: 3] {UDP} 192.168.152.1:52176 -> 239.255.255.250:1900
10/27-18:37:42.702815  [**] [1:1917:6] SCAN UPnP service discover attempt [**] [Classification: Detection
of a Network Scan] [Priority: 3] {UDP} 192.168.152.1:52176 -> 239.255.255.250:1900
10/27-18:37:43.715156  [**] [1:1917:6] SCAN UPnP service discover attempt [**] [Classification: Detection
of a Network Scan] [Priority: 3] {UDP} 192.168.152.1:52176 -> 239.255.255.250:1900
10/27-18:37:44.726798  [**] [1:1917:6] SCAN UPnP service discover attempt [**] [Classification: Detection
of a Network Scan] [Priority: 3] {UDP} 192.168.152.1:52176 -> 239.255.255.250:1900
10/27-18:39:41.692428  [**] [1:1917:6] SCAN UPnP service discover attempt [**] [Classification: Detection
of a Network Scan] [Priority: 3] {UDP} 192.168.152.1:53523 -> 239.255.255.250:1900
10/27-18:39:42.702741  [**] [1:1917:6] SCAN UPnP service discover attempt [**] [Classification: Detection
of a Network Scan] [Priority: 3] {UDP} 192.168.152.1:53523 -> 239.255.255.250:1900
10/27-18:39:43.715214  [**] [1:1917:6] SCAN UPnP service discover attempt [**] [Classification: Detection
```

image_2025-10-27_18-59-27.png

Step 8: Running Snort as a Daemon

To run Snort in the background as a daemon, I use the following. I specify the interface to monitor (e.g., `eth0`, `enX0`, etc.):

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



```
srivasta1@srivasta1-virtual-machine:/var/log/snort$ sudo snort -D -c /etc/snort/snort.conf -i eth0
[sudo] password for srivasta1:
Spawning daemon child...
My daemon child 2558 lives...
Daemon parent exiting (0)
srivasta1@srivasta1-virtual-machine:/var/log/snort$
```

College Work/Fall 25/NS (Network Security)/Assignment 6/image-3.png

This keeps Snort running in the background, continuously monitoring my specified network interface.

To see the different processes running in my system, I use the command `top`. If I wait a few seconds, I should see Snort running.
If I want to stop the Snort process from running, I can use the command

```
    sudo kill -9 [PID]
And from my earlier results I can see that the PID is 2558. Thus the command becomes

    sudo kill -9 2558
```

~~~
```
~~~