SNORT

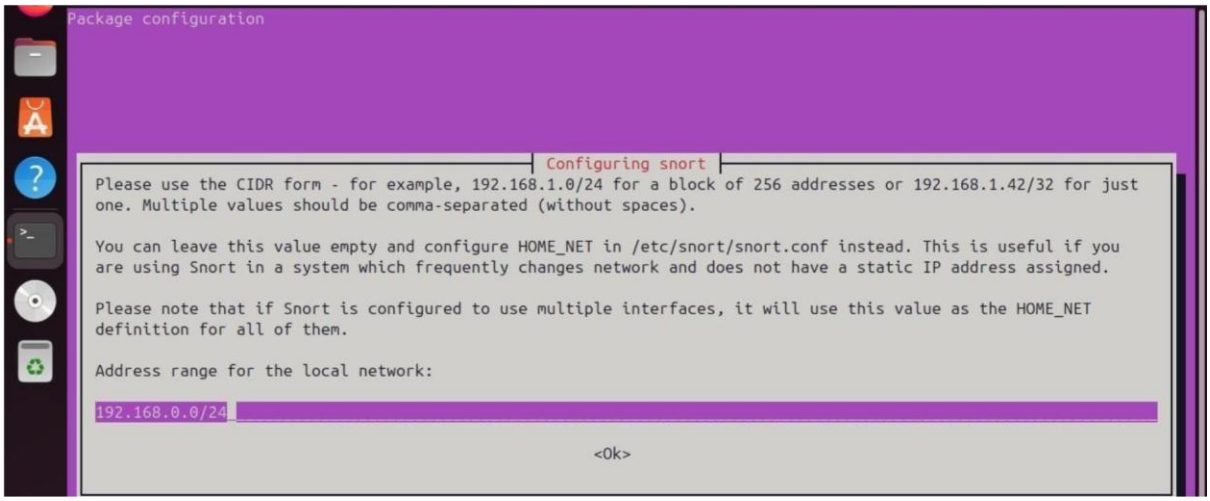
Snort is mainly known as a free tool that helps detect and prevent security issues on a computer network. It looks at the data moving through the network and checks for any unusual or suspicious activity. It uses a set of rules to analyze the data and spot any potential threats.

sudo apt-get install snort -y

```
[sudo] password for vboxuser:
root@workstation:/home/vboxuser# sudo apt-get install snort -y
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  libdaq2t64 libdumbnet1 libpcre3 net-tools oinkmaster snort-common snort-common-libraries snort-rules-default
Suggested packages:
  snort-doc
The following NEW packages will be installed:
  libdaq2t64 libdumbnet1 libpcre3 net-tools oinkmaster snort snort-common snort-common-libraries snort-rules-default
0 upgraded, 9 newly installed, 0 to remove and 18 not upgraded.
Need to get 2,529 kB of archives.
After this operation, 11.3 MB of additional disk space will be used.
Get:1 http://in.archive.ubuntu.com/ubuntu noble/universe amd64 libpcre3 amd64 2:8.39-15build1 [248 kB]
Get:2 http://in.archive.ubuntu.com/ubuntu noble/universe amd64 snort-common-libraries amd64 2.9.20-0+deb11u1ubuntu1 [899
 kB]
Get:3 http://in.archive.ubuntu.com/ubuntu noble/universe amd64 snort-rules-default all 2.9.20-0+deb11u1ubuntu1 [144 kB]
Get:4 http://in.archive.ubuntu.com/ubuntu noble/universe amd64 snort-common all 2.9.20-0+deb11u1ubuntu1 [47.7 kB]
Get:5 http://in.archive.ubuntu.com/ubuntu noble/main amd64 net-tools amd64 2.10-0.1ubuntu4 [204 kB]
Get:6 http://in.archive.ubuntu.com/ubuntu noble/universe amd64 libdumbnet1 amd64 1.17.0-1ubuntu2 [30.7 kB]
Get:7 http://in.archive.ubuntu.com/ubuntu noble/universe amd64 libdaq2t64 amd64 2.0.7-5.1build3 [92.9 kB]
Get:8 http://in.archive.ubuntu.com/ubuntu noble/universe amd64 snort amd64 2.9.20-0+deb11u1ubuntu1 [791 kB]
Get:9 http://in.archive.ubuntu.com/ubuntu noble/universe amd64 oinkmaster all 2.0-4.2 [71.9 kB]
Fetched 2,529 kB in 5s (530 kB/s)
Preconfiguring packages ...
Snort configuration: interface default not set, using 'enp0s3'
Selecting previously unselected package libpcre3:amd64.
(Reading database ... 205813 files and directories currently installed.)
Preparing to unpack .../0-libpcre3_2%3a8.39-15build1_amd64.deb ...
Unpacking libpcre3:amd64 (2:8.39-15build1) ...
Selecting previously unselected package snort-common-libraries.
```

Using sudo apt-get install snort -y is a straightforward way to install the Snort intrusion detection system on a Debian-based Linux distribution.

During installation it will asked for ip address enter 192.168.0.0/24

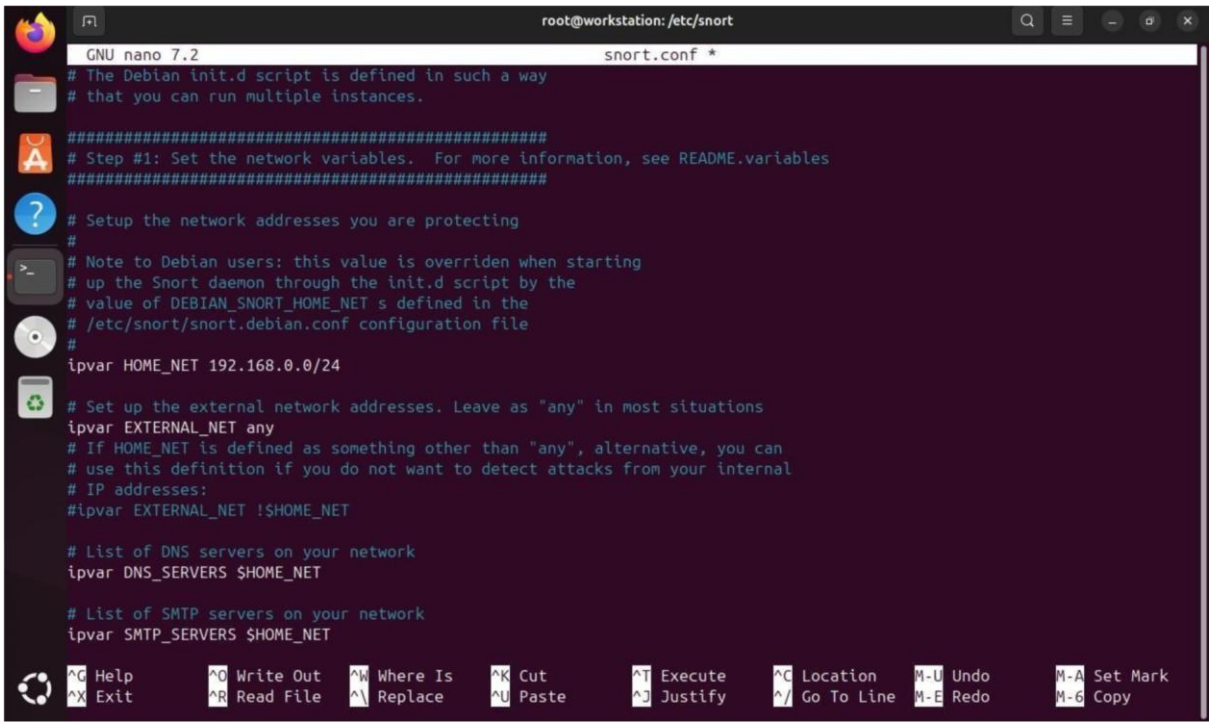


snort –version to check whether it installed properly

or not

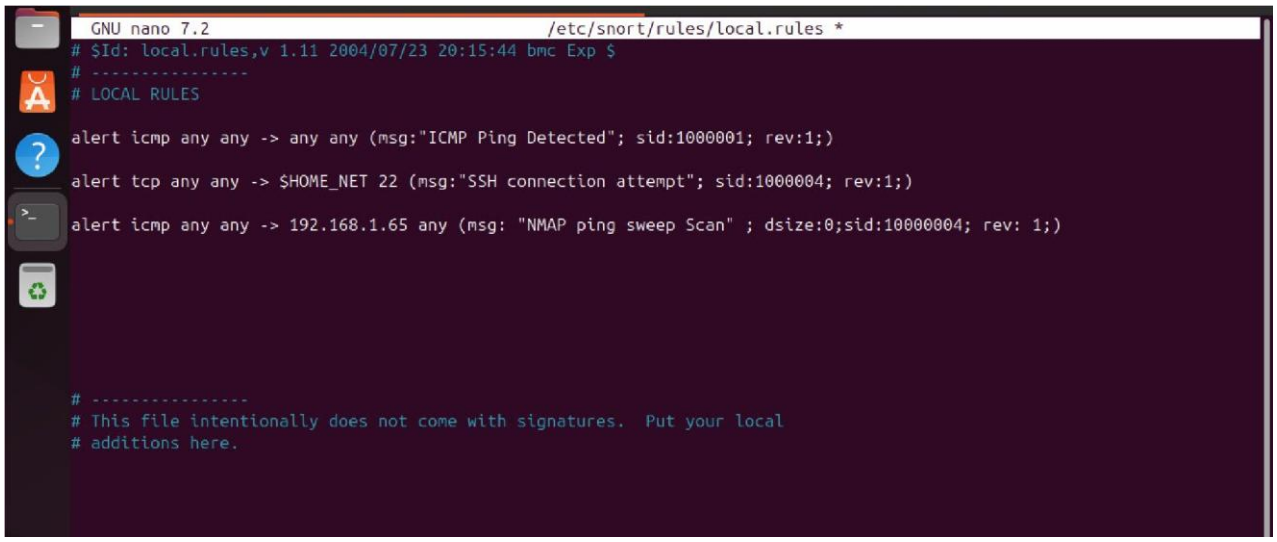
The command **snort --version** is used to check the version of the Snort software installed on your system.

nano /etc/snort/snort.conf



Find ipvar and enter 192.168.0.0/24

Nano /etc/snort/rules/local.rules



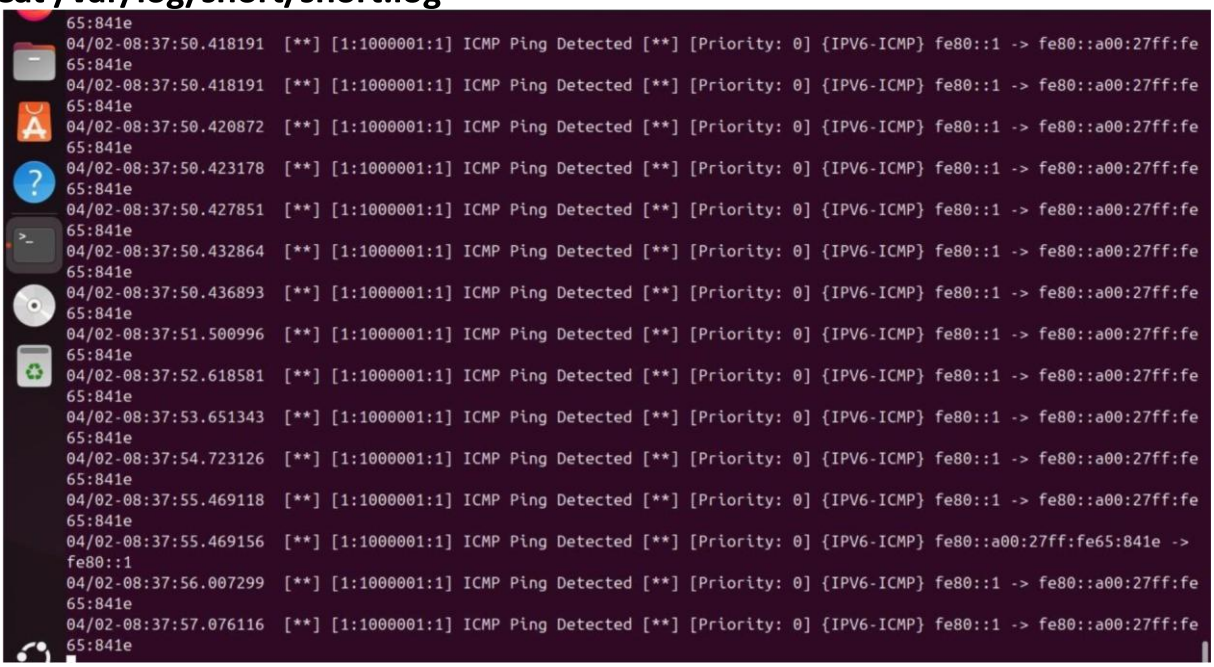
Enter the rules as per given in image

Rule 1: In simple terms, this Snort rule will trigger an alert whenever it detects an ICMP packet (like a ping), no matter where it's coming from or going to. The alert will show the message "ICMP Ping Detected," and the rule has an ID number (SID) of 1000001 with a version number of 1. This helps keep track of network activity and can spot potential scanning or probing attempts on the network.

Rule 2: This Snort rule will trigger an alert if a TCP packet tries to connect to an SSH service (port 22) on any device within your network. The alert will show the message "SSH Connection Attempt," and the rule has an ID number (SID) of 1000001 with a version number of 1. This helps you keep an eye on any unauthorized or suspicious SSH connection attempts to your network.

Rulee 3: This Snort rule will trigger an alert if a TCP packet matches a specific target IP and port, and contains a pattern that suggests an Nmap scan is happening. The alert will display the message "NMAP scan detected!" and has an ID number (SID) of 1000001 with a version number of 1. It is marked as a highpriority warning. This helps you detect possible scanning or checking activities on your network.

Cat /var/log/snort/snort.log



```
65:841e
04/02-08:37:50.418191  [**] [1:1000001:1] ICMP Ping Detected [**] [Priority: 0] {IPV6-ICMP} fe80::1 -> fe80::a00:27ff:fe
65:841e
04/02-08:37:50.418191  [**] [1:1000001:1] ICMP Ping Detected [**] [Priority: 0] {IPV6-ICMP} fe80::1 -> fe80::a00:27ff:fe
65:841e
04/02-08:37:50.420872  [**] [1:1000001:1] ICMP Ping Detected [**] [Priority: 0] {IPV6-ICMP} fe80::1 -> fe80::a00:27ff:fe
65:841e
04/02-08:37:50.423178  [**] [1:1000001:1] ICMP Ping Detected [**] [Priority: 0] {IPV6-ICMP} fe80::1 -> fe80::a00:27ff:fe
65:841e
04/02-08:37:50.427851  [**] [1:1000001:1] ICMP Ping Detected [**] [Priority: 0] {IPV6-ICMP} fe80::1 -> fe80::a00:27ff:fe
65:841e
04/02-08:37:50.432864  [**] [1:1000001:1] ICMP Ping Detected [**] [Priority: 0] {IPV6-ICMP} fe80::1 -> fe80::a00:27ff:fe
65:841e
04/02-08:37:50.436893  [**] [1:1000001:1] ICMP Ping Detected [**] [Priority: 0] {IPV6-ICMP} fe80::1 -> fe80::a00:27ff:fe
65:841e
04/02-08:37:51.500996  [**] [1:1000001:1] ICMP Ping Detected [**] [Priority: 0] {IPV6-ICMP} fe80::1 -> fe80::a00:27ff:fe
65:841e
04/02-08:37:52.618581  [**] [1:1000001:1] ICMP Ping Detected [**] [Priority: 0] {IPV6-ICMP} fe80::1 -> fe80::a00:27ff:fe
65:841e
04/02-08:37:53.651343  [**] [1:1000001:1] ICMP Ping Detected [**] [Priority: 0] {IPV6-ICMP} fe80::1 -> fe80::a00:27ff:fe
65:841e
04/02-08:37:54.723126  [**] [1:1000001:1] ICMP Ping Detected [**] [Priority: 0] {IPV6-ICMP} fe80::1 -> fe80::a00:27ff:fe
65:841e
04/02-08:37:55.469118  [**] [1:1000001:1] ICMP Ping Detected [**] [Priority: 0] {IPV6-ICMP} fe80::1 -> fe80::a00:27ff:fe
65:841e
04/02-08:37:55.469156  [**] [1:1000001:1] ICMP Ping Detected [**] [Priority: 0] {IPV6-ICMP} fe80::a00:27ff:fe65:841e ->
fe80::1
04/02-08:37:56.007299  [**] [1:1000001:1] ICMP Ping Detected [**] [Priority: 0] {IPV6-ICMP} fe80::1 -> fe80::a00:27ff:fe
65:841e
04/02-08:37:57.076116  [**] [1:1000001:1] ICMP Ping Detected [**] [Priority: 0] {IPV6-ICMP} fe80::1 -> fe80::a00:27ff:fe
65:841e
```