Final Year B. Tech., Sem VII 2022-23

Cryptography And Network Security

Lab PRN : 2019BTECS00036

Name : Nikhil Danapgol

Batch: B2

Assignment: 16

Title of assignment: Installation and Testing of Snort

Aim : To test and run snort

Theory:

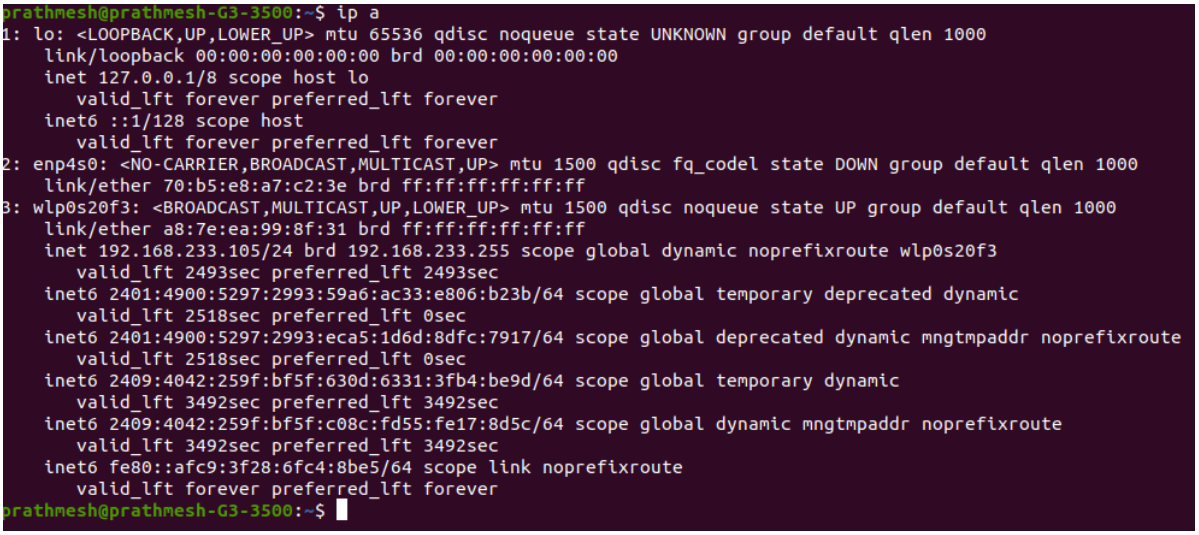
SNORT is a network based intrusion detection system which is written in C programming language. It was developed in 1998 by Martin Roesch. Now it is developed by Cisco. It is free open-source software. It can also be used as a packet sniffer to monitor the system in real time. The network admin can use it to watch all the incoming packets and find the ones which are dangerous to the system. It is based on library packet capture tool. The rules are fairly easy to create and implement and it can be deployed in any kind of operating system and any kind of network environment. The main reason of the popularity of this IDS over others is that it is a free-to-use software and also open source because of which any user can be able to use it as the way he wants.

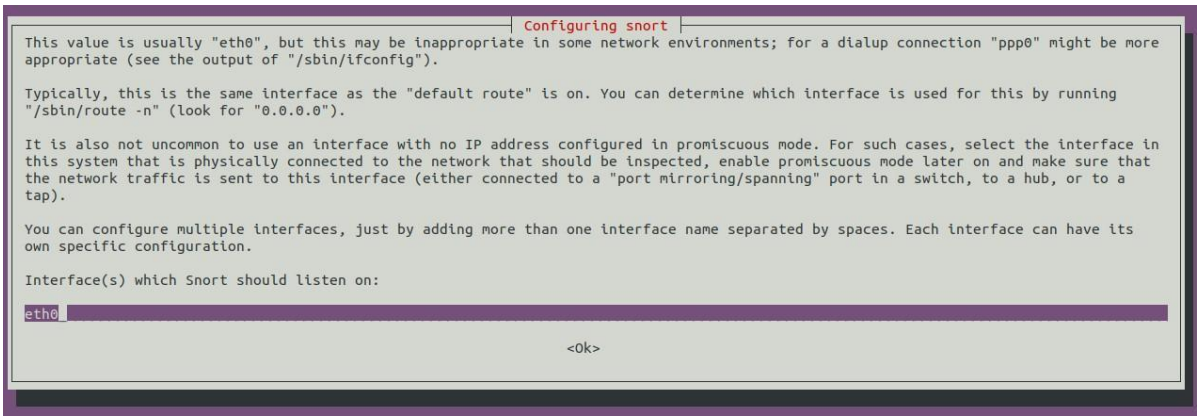
Features:

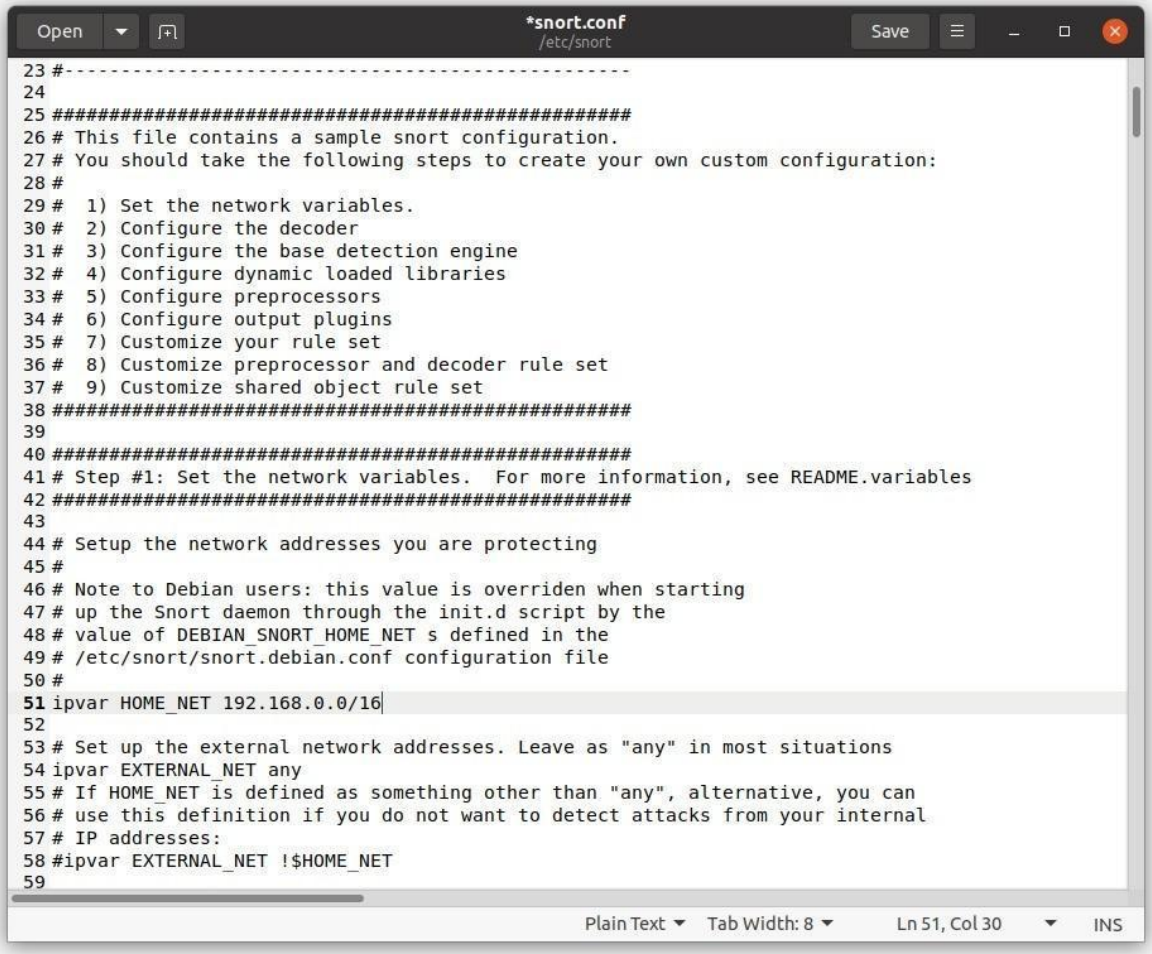
- **Real-time traffic monitor**
- **Packet logging**
- **Analysis of protocol**

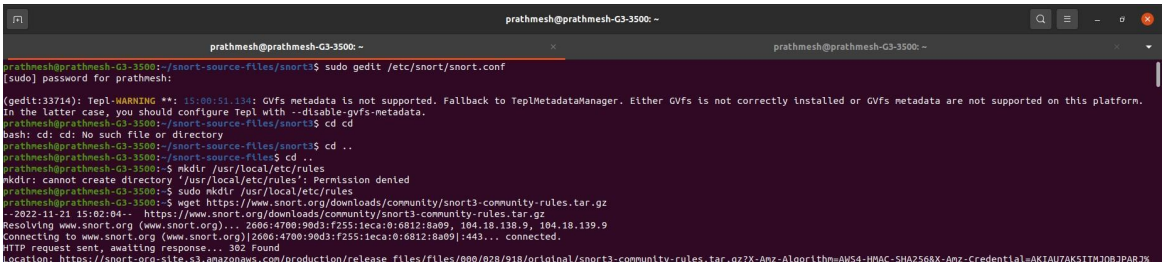
- **Content matching**
- **OS fingerprinting**
- **Can be installed in any network environment.**
- **Creates logs**
- **Open Source**
- **Rules are easy to implement**

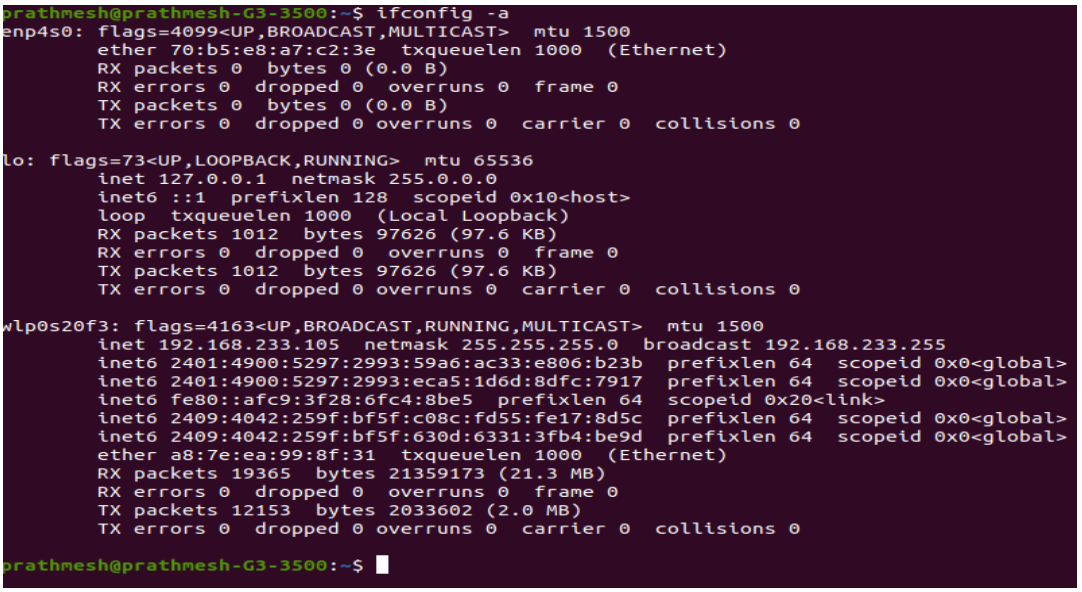
Installation of snort:



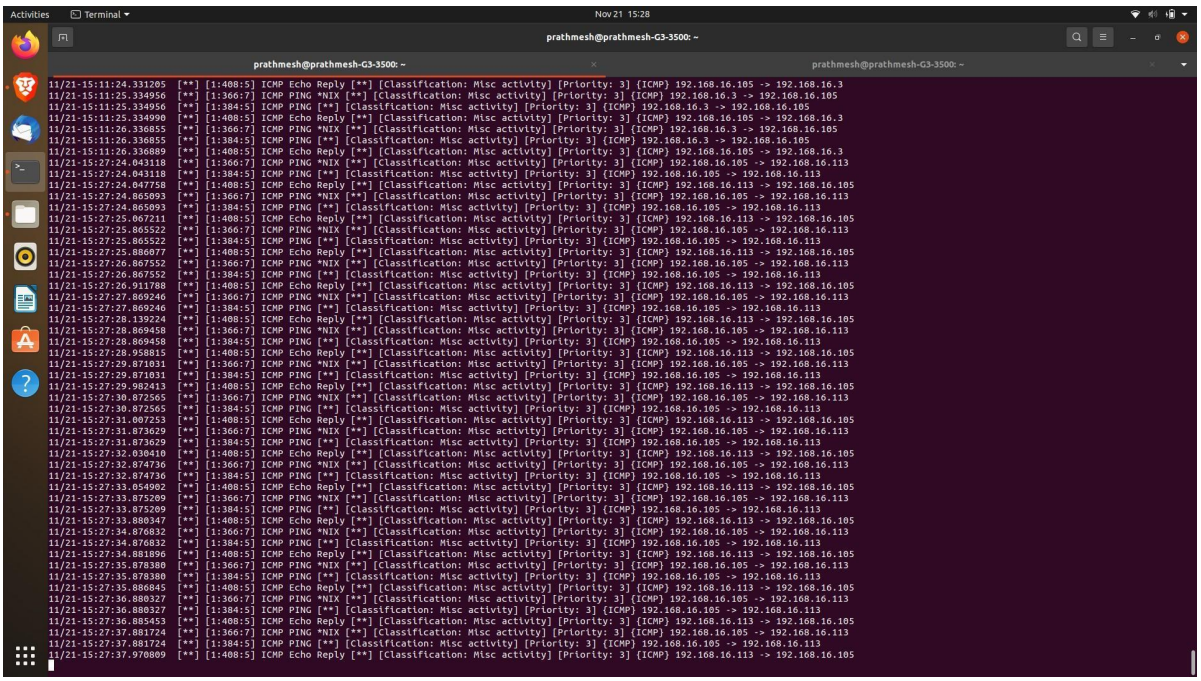

Configuring snort
This value is usually "eth0", but this may be inappropriate in some network environments; for a dialup connection "ppp0" might be more appropriate (see the output of "/sbin/ifconfig").
Typically, this is the same interface as the "default route" is on. You can determine which interface is used for this by running "/sbin/route -n" (look for "0.0.0.0").
It is also not uncommon to use an interface with no IP address configured in promiscuous mode. For such cases, select the interface in this system that is physically connected to the network that should be inspected, enable promiscuous mode later on and make sure that the network traffic is sent to this interface (either connected to a "port mirroring/spanning" port in a switch, to a hub, or to a tap).
You can configure multiple interfaces, just by adding more than one interface name separated by spaces. Each interface can have its own specific configuration.
Interface(s) which Snort should listen on:
eth0
<Ok>


Open
*snort.conf
/etc/snort
Save
#--
##
This file contains a sample snort configuration.
You should take the following steps to create your own custom configuration:
#
1) Set the network variables.
2) Configure the decoder
3) Configure the base detection engine
4) Configure dynamic loaded libraries
5) Configure preprocessors
6) Configure output plugins
7) Customize your rule set
8) Customize preprocessor and decoder rule set
9) Customize shared object rule set
##
##
Step #1: Set the network variables. For more information, see README.variables
##
Setup the network addresses you are protecting
#
Note to Debian users: this value is overriden when starting
up the Snort daemon through the init.d script by the
value of DEBIAN_SNORT_HOME_NET s defined in the
/etc/snort/snort.debian.conf configuration file
#
ipvar HOME_NET 192.168.0.0/16
Set up the external network addresses. Leave as "any" in most situations
ipvar EXTERNAL_NET any
If HOME_NET is defined as something other than "any", alternative, you can
use this definition if you do not want to detect attacks from your internal
IP addresses:
#ipvar EXTERNAL_NET !$HOME_NET
Plain Text
Tab Width: 8
Ln 51, Col 30
INS


prathmesh@prathmesh-G3-3500: ~
prathmesh@prathmesh-G3-3500:~/snort-source-files/snort3$ sudo gedit /etc/snort/snort.conf
[sudo] password for prathmesh:
(gedit:33714): Tepl-WARNING **: 15:00:51.134: GVfs metadata is not supported. Fallback to TeplMetadataManager. Either GVfs is not correctly installed or GVfs metadata are not supported on this platform. In the latter case, you should configure Tepl with --disable-gvfs-metadata.
prathmesh@prathmesh-G3-3500:~/snort-source-files/snort3$ cd cd
bash: cd: cd: No such file or directory
prathmesh@prathmesh-G3-3500:~/snort-source-files/snort3$ cd ..
prathmesh@prathmesh-G3-3500:~/snort-source-files$ cd ..
prathmesh@prathmesh-G3-3500:~$ mkdir /usr/local/etc/rules
mkdir: cannot create directory '/usr/local/etc/rules': Permission denied
prathmesh@prathmesh-G3-3500:~$ sudo mkdir /usr/local/etc/rules
prathmesh@prathmesh-G3-3500:~$ wget https://www.snort.org/downloads/community/snort3-community-rules.tar.gz
--2022-11-21 15:02:04-- https://www.snort.org/downloads/community/snort3-community-rules.tar.gz
Resolving www.snort.org (www.snort.org)... 2606:4700:90d3:f255:1eca:0:6812:8a09, 104.18.138.9, 104.18.139.9
Connecting to www.snort.org (www.snort.org)|2606:4700:90d3:f255:1eca:0:6812:8a09|:443... connected.
HTTP request sent, awaiting response... 302 Found



Testing of snort: Ip 192.168.16.3 is trying to ping the host 192.168.16.105 and it get detected on snort



Conclusion:

Performed the experiment successfully. Snort is installed and tested succesfully.