Assignments:-4

Module:- NDC(SNORT_LINUX)

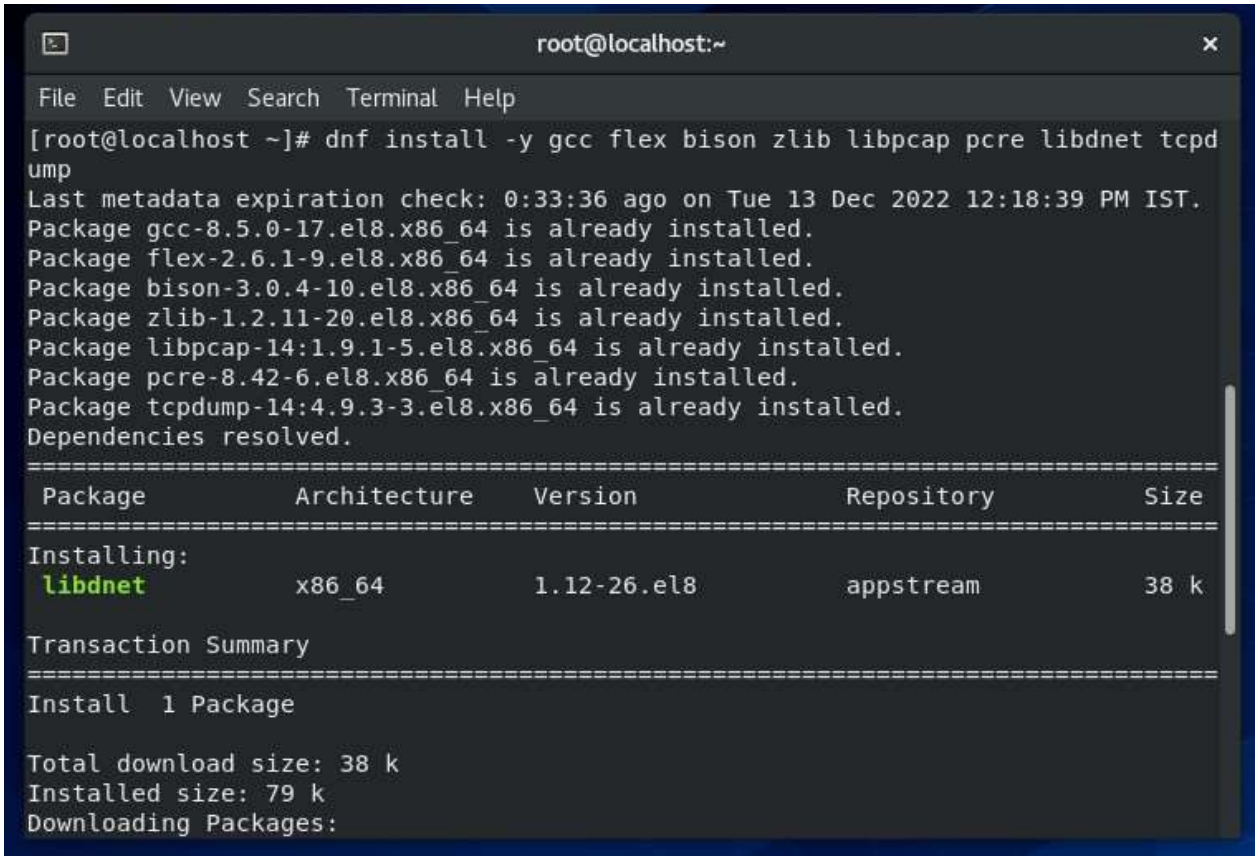
Name:- Prithviraj Nikam

Lab Assignment :-

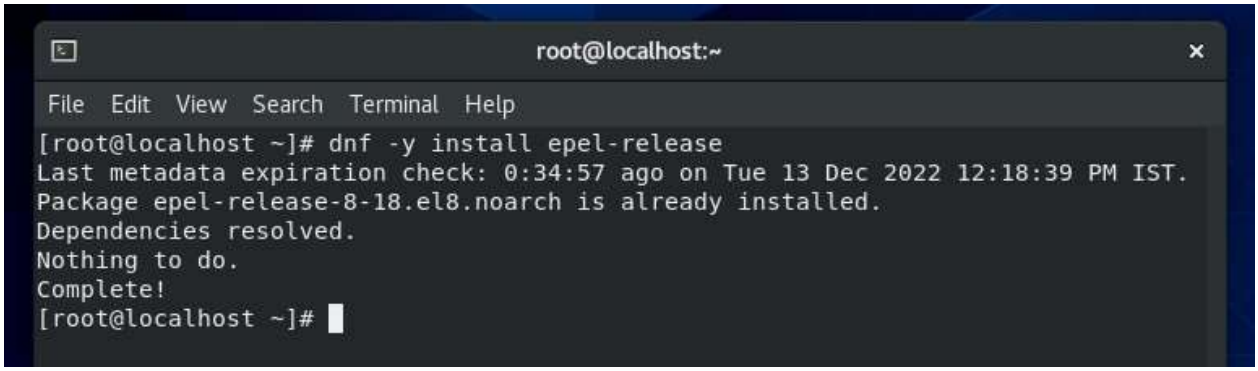
Install and configure SNORT-2.9.20 on following OS:

1. Linux CentOS-8

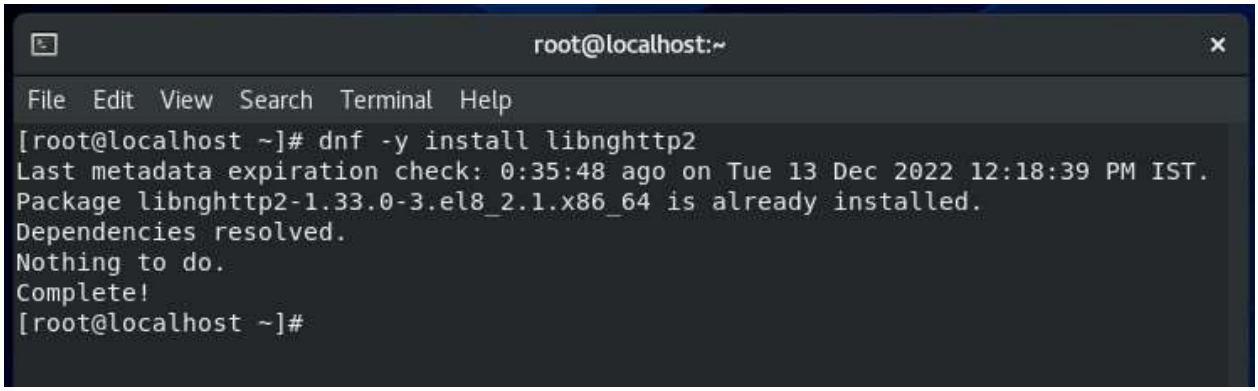
Step-1:- dnf install -y gcc flex bison zlib libpcap pcre libdnet tcpdump



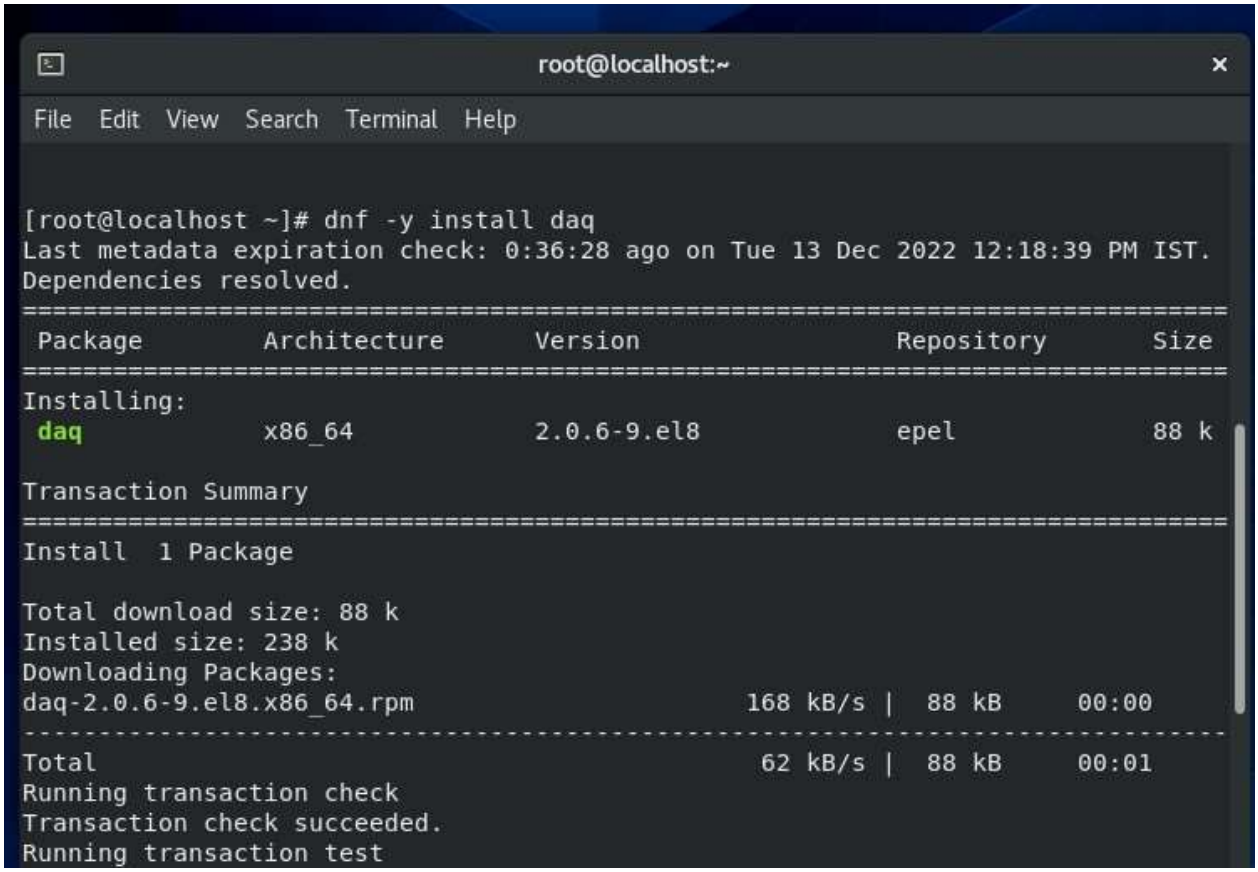
Step-2:- dnf install –y epel-release



Step-3:- dnf install -y libnghttp2

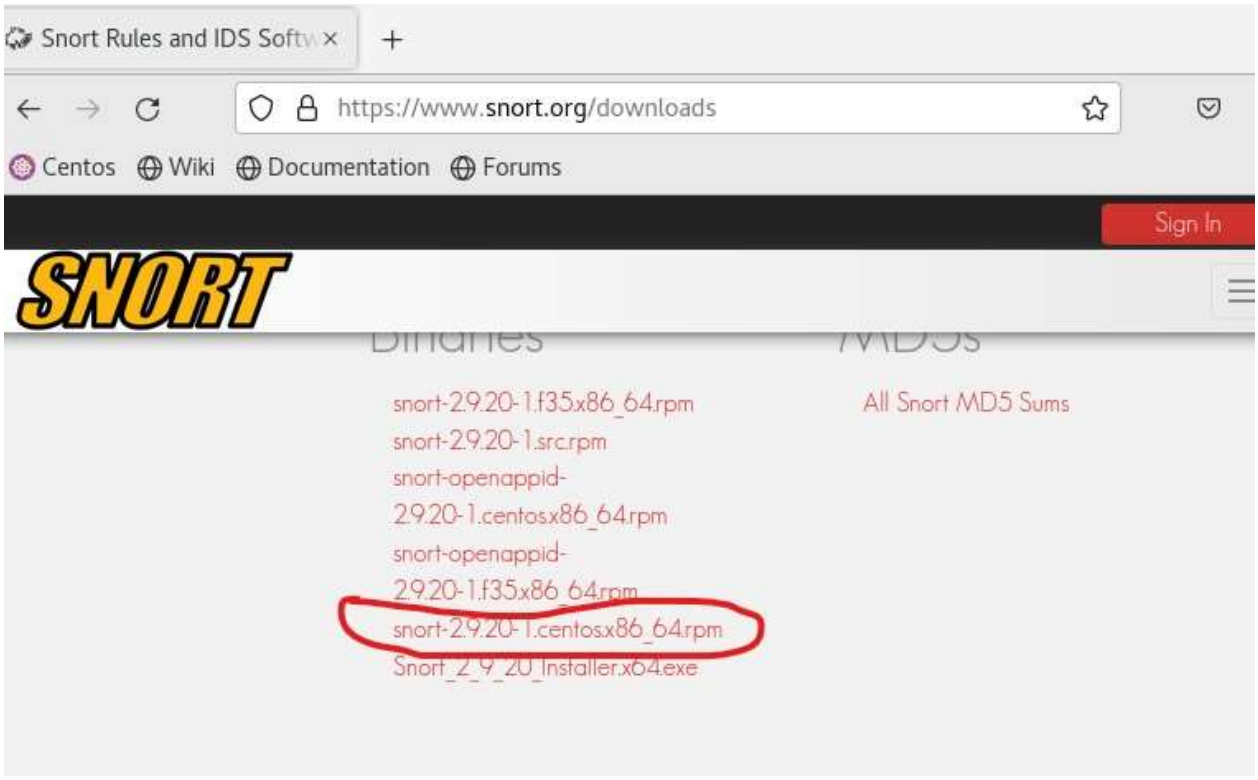


Step-4:- dnf install daq



Step-5:- dnf install

https://www.snort.org/downloads/snort/snort-2.9.20-1.centos.x86_64.rpm



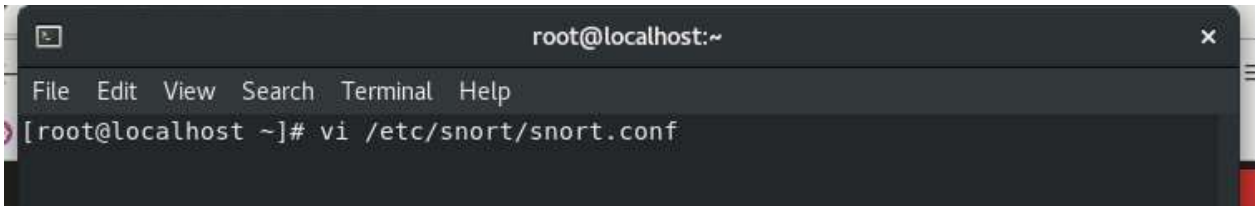

```
root@localhost:~
File  Edit  View  Search  Terminal  Help
[root@localhost ~]# dnf -y install https://www.snort.org/downloads/snort/snort-2
.9.20-1.centos.x86_64.rpm
Last metadata expiration check: 0:39:53 ago on Tue 13 Dec 2022 12:18:39 PM IST.
snort-2.9.20-1.centos.x86_64.rpm                349 kB/s | 4.6 MB     00:13
Dependencies resolved.
================================================================================
 Package              Arch        Version              Repository         Size
================================================================================
Installing:
 snort                x86_64      1:2.9.20-1           @commandline      4.6 M
Installing dependencies:
 compat-openssl10     x86_64      1:1.0.2o-4.el8       appstream         1.1 M
 libnsl               x86_64      2.28-220.el8         baseos            105 k

Transaction Summary
================================================================================
Install  3 Packages

Total size: 5.8 M
Total download size: 1.2 M
Installed size: 23 M
Downloading Packages:
(1/2): libnsl-2.28-220.el8.x86_64.rpm           335 kB/s | 105 kB     00:00
(2/2): compat-openssl10-1.0.2o-4.el8.x86_64.rpm 1.1 MB/s | 1.1 MB     00:00
```

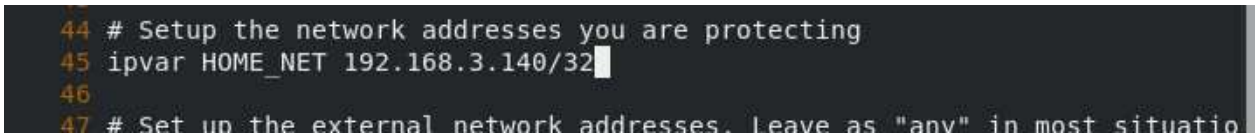
Step-6:-Configure SNORT

a. Vi /etc/snort/snort.conf



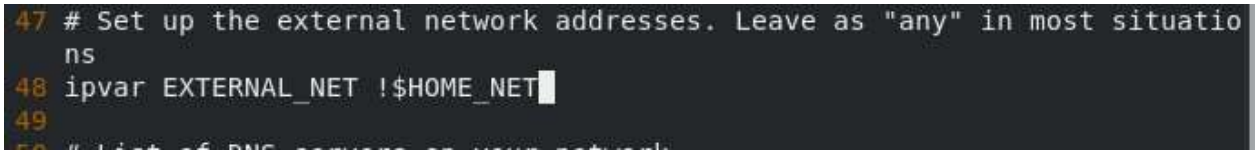
b. On line number 45 –

ipvar HOME_NET 192.168.3.140/32



On line number 48 –

ipvar EXTERNAL_NET !$HOME_NET



On line number 105 and 106

var SO_RULE_PATH /etc/snort/so_rules

var PREPROC_RULE_PATH /etc/snort/preproc_rules

On line number 113 and 114

var WHITE_LIST_PATH /etc/snort/rules

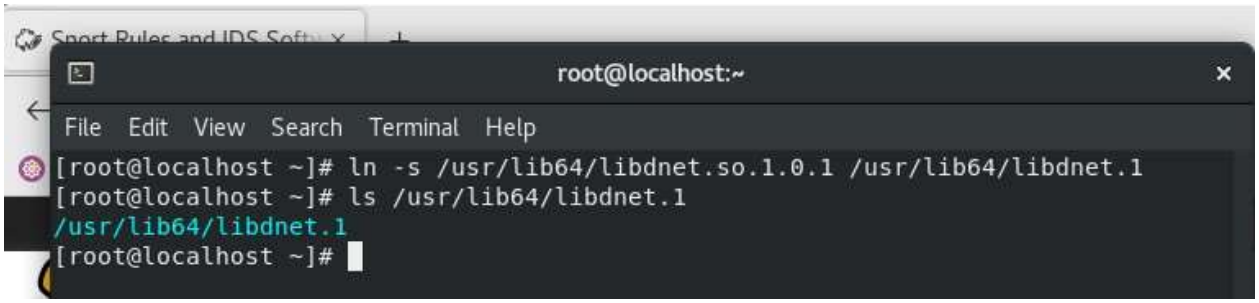
var BLACK_LIST_PATH /etc/snort/rules

```
112 # Set the absolute path appropriately
113 var WHITE_LIST_PATH /etc/snort/rules
114 var BLACK_LIST_PATH /etc/snort/rules
115
```

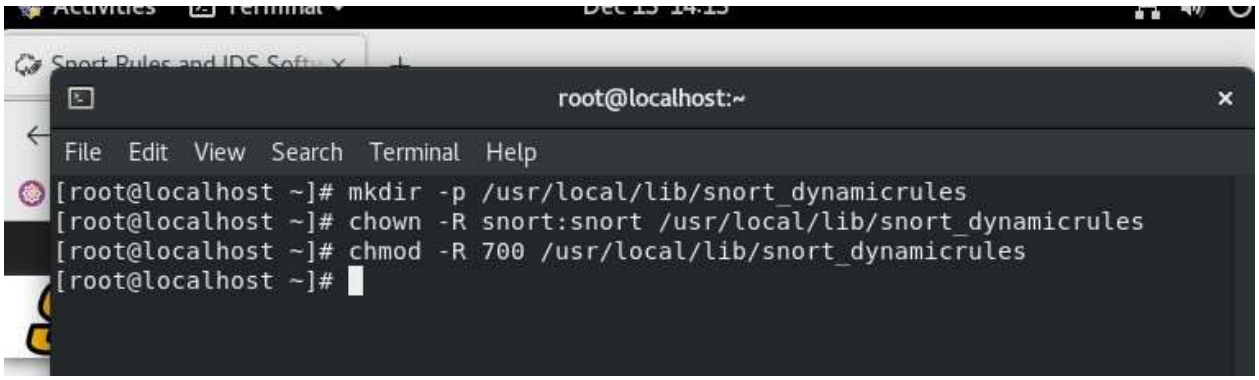
Delete rule files from 548 till ------X11

```
545 # site specific rules
546 include $RULE_PATH/local.rules
547
548 ##################################################
```

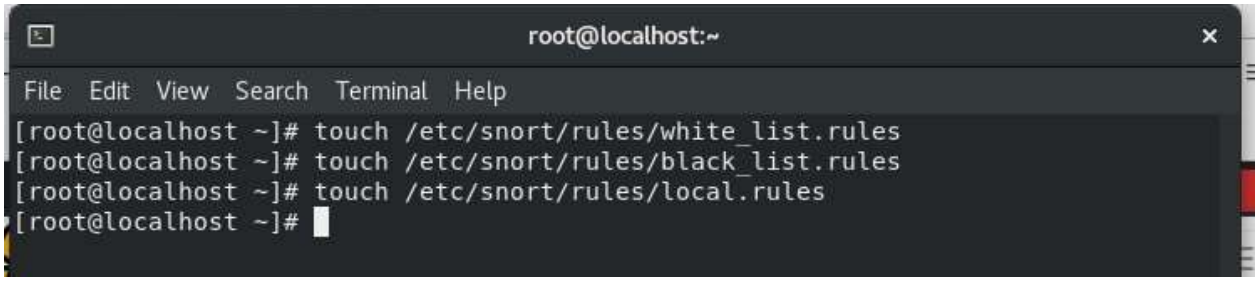
Step-7:- ln -s /usr/lib64/libdnet.so.1.0.1 /usr/lib64/libdnet.1



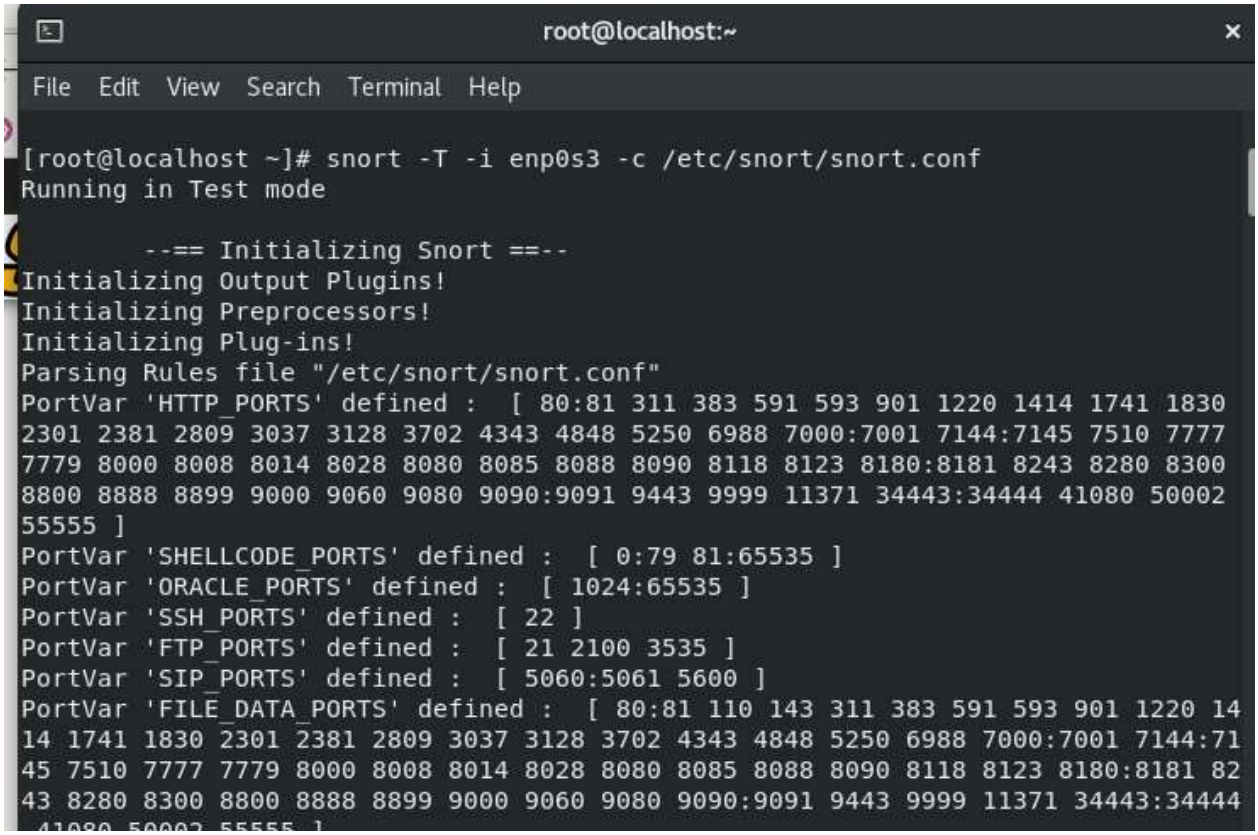
Step-8:- mkdir -p /usr/local/lib/snort_dynamicrules
chown -R snort:snort /usr/local/lib/snort_dynamicrules
chmod -R 700 /usr/local/lib/snort_dynamicrules



Step-9:- touch /etc/snort/rules/white_list.rules
touch /etc/snort/rules/black_list.rules
touch /etc/snort/rules/local.rules

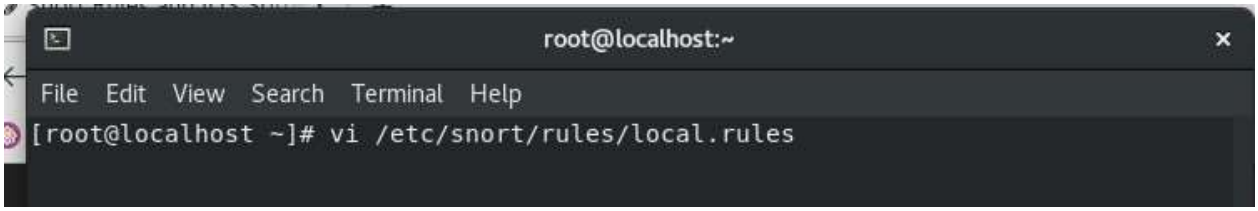


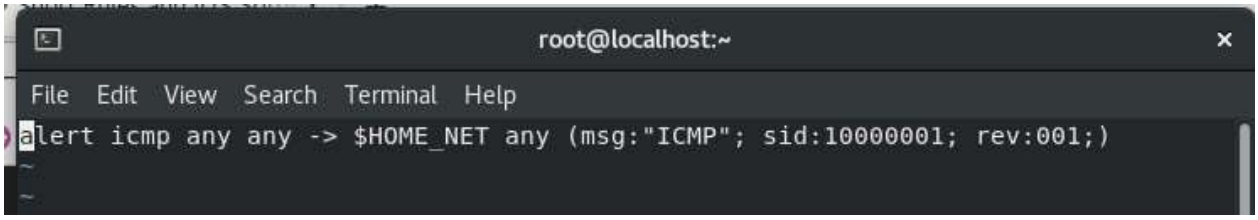
Step-10:- snort -T -i enp0s3 -c /etc/snort/snort.conf



Step-11:- go to local.rules

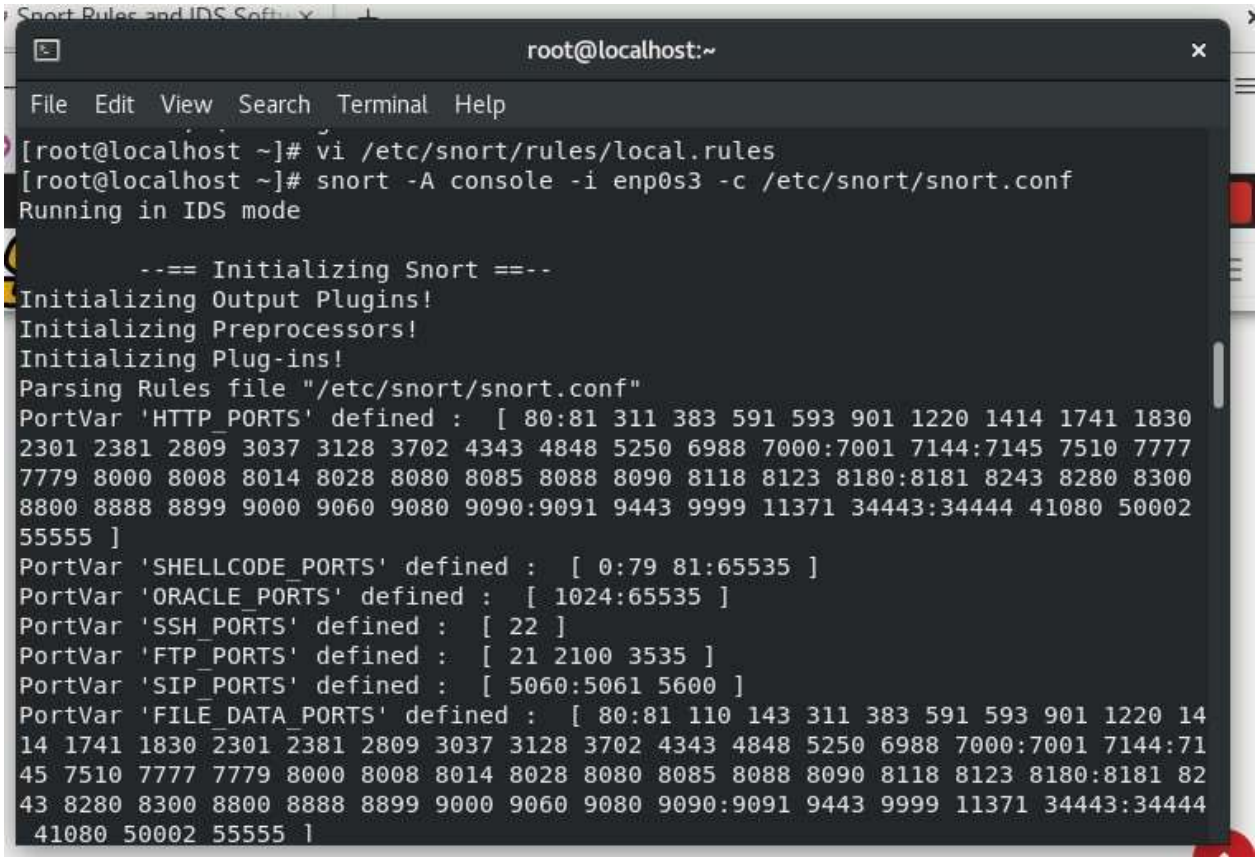
#vi /etc/snort/rules/locals.rules





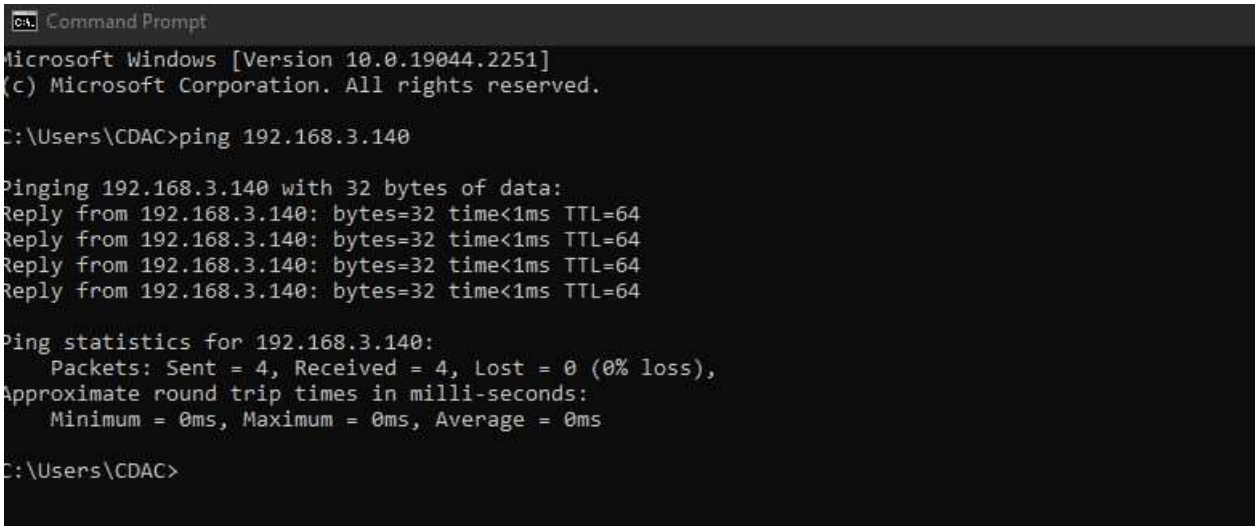
Step-12:- run the console

#snort -A console -i enp0s3 -c /etc/snort/snort.conf

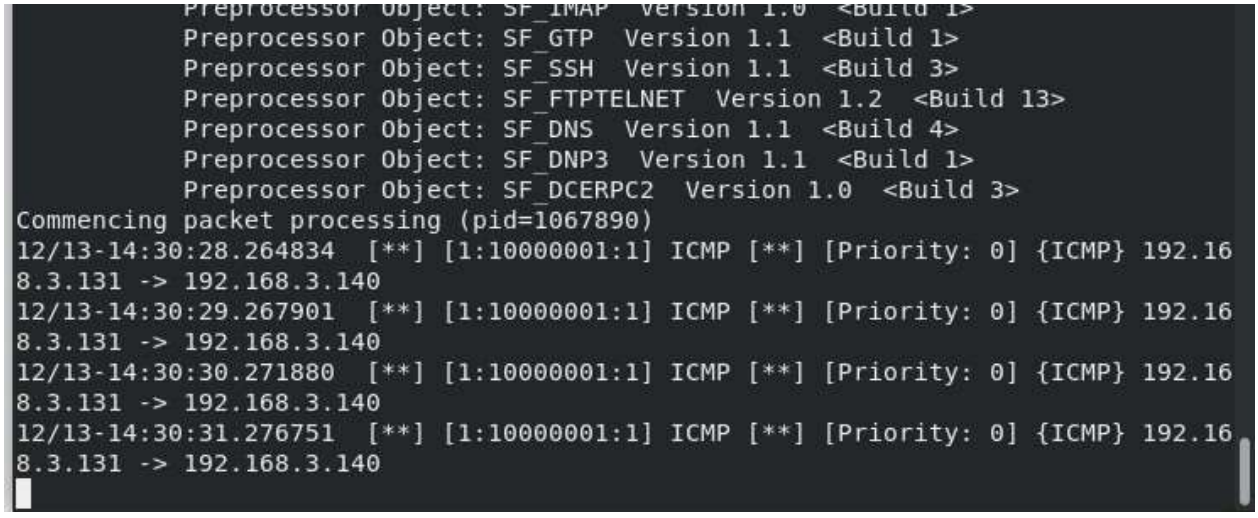


Step-13:- Go to Windows Command Prompt and

ping 192.168.3.140



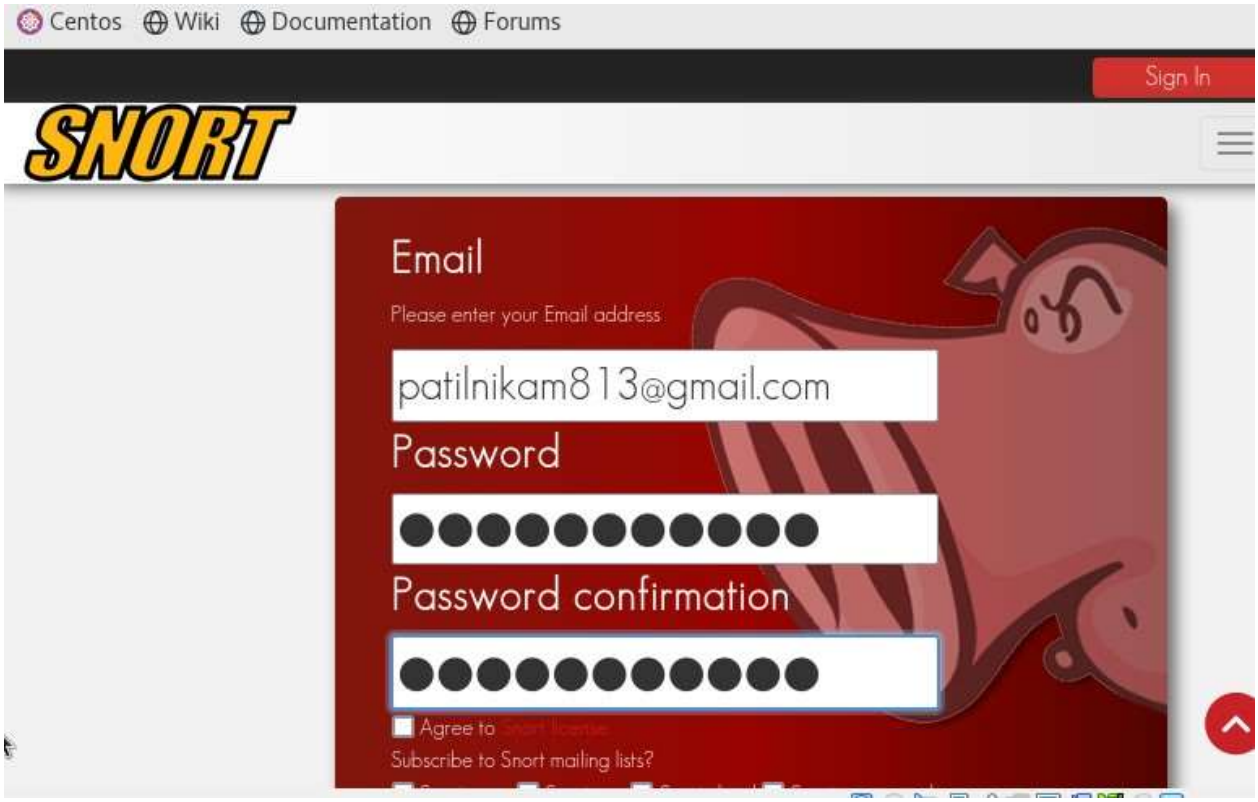
Step-14:-Go to CentOS and check the output



Step-15:- Go to Snort official website

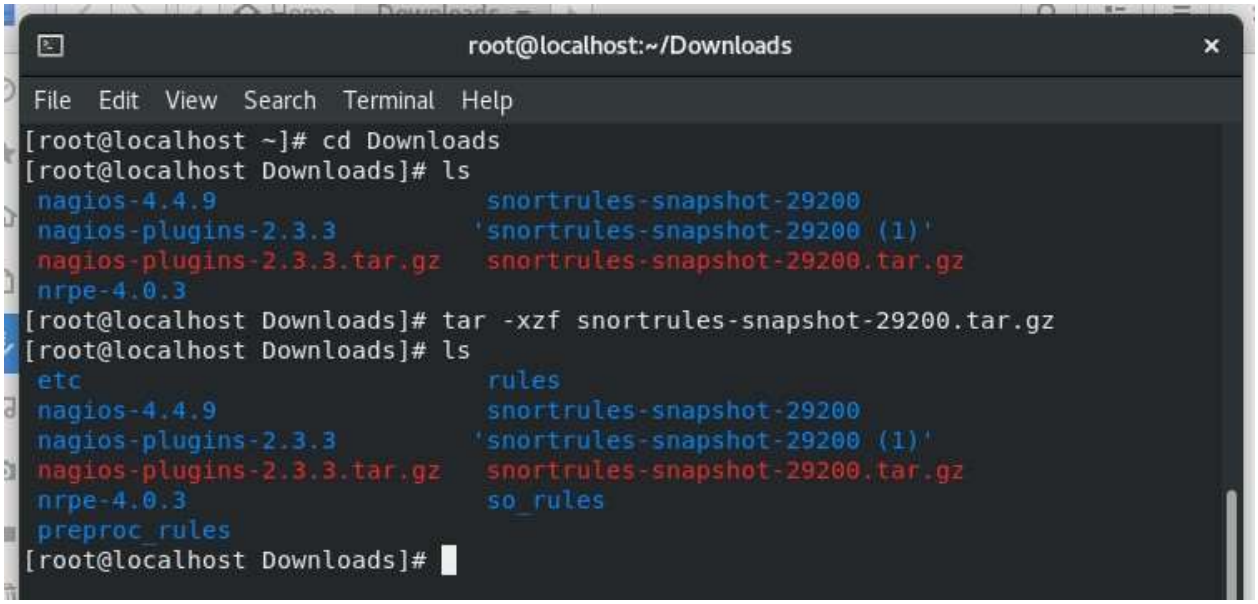
https://www.snort.org/

And sign in



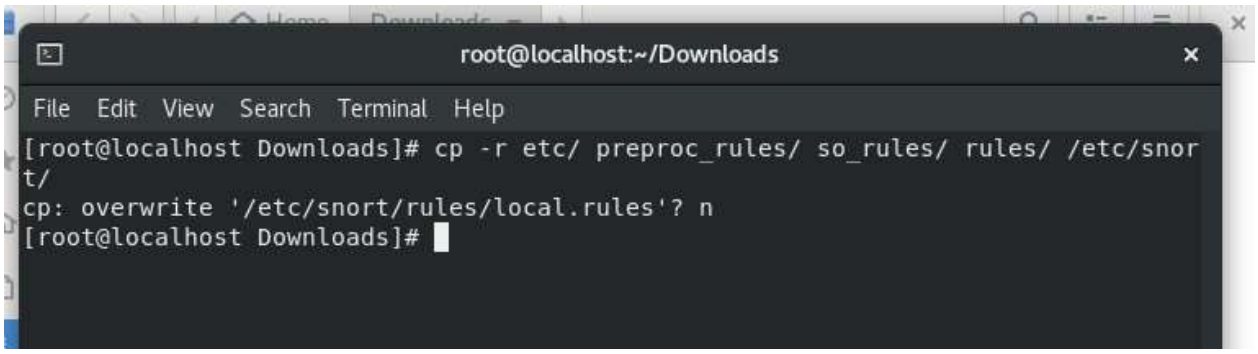
Step-16:-Downloads the
https://www.snort.org/downloads/registered/snortrules-snapshot-29200.tar.gz

Extract the file
#tar -xzf File_name.tar.gz



Step-17:- Copy the files

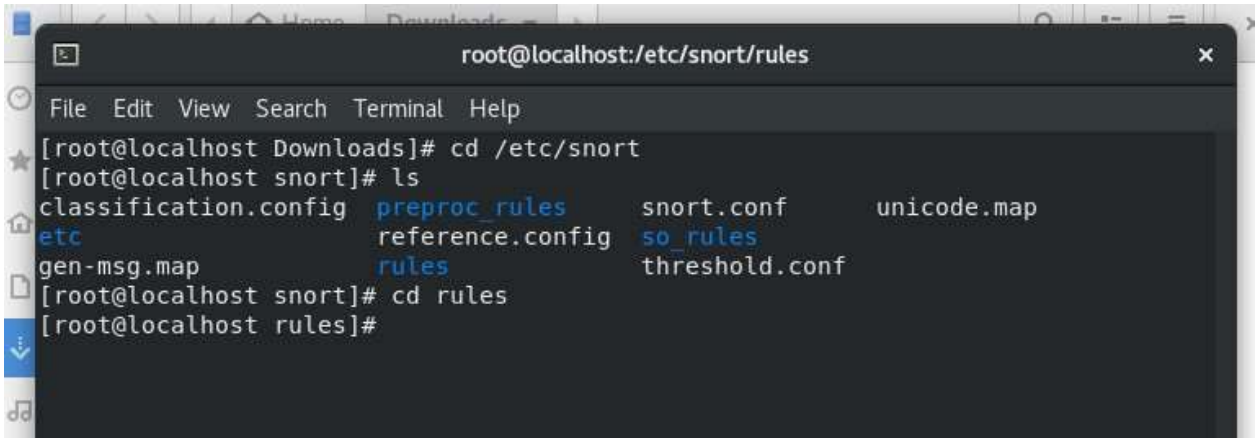
 # cp -r etc/ preproc_rules/ so_rules/ rules/ /etc/snort/

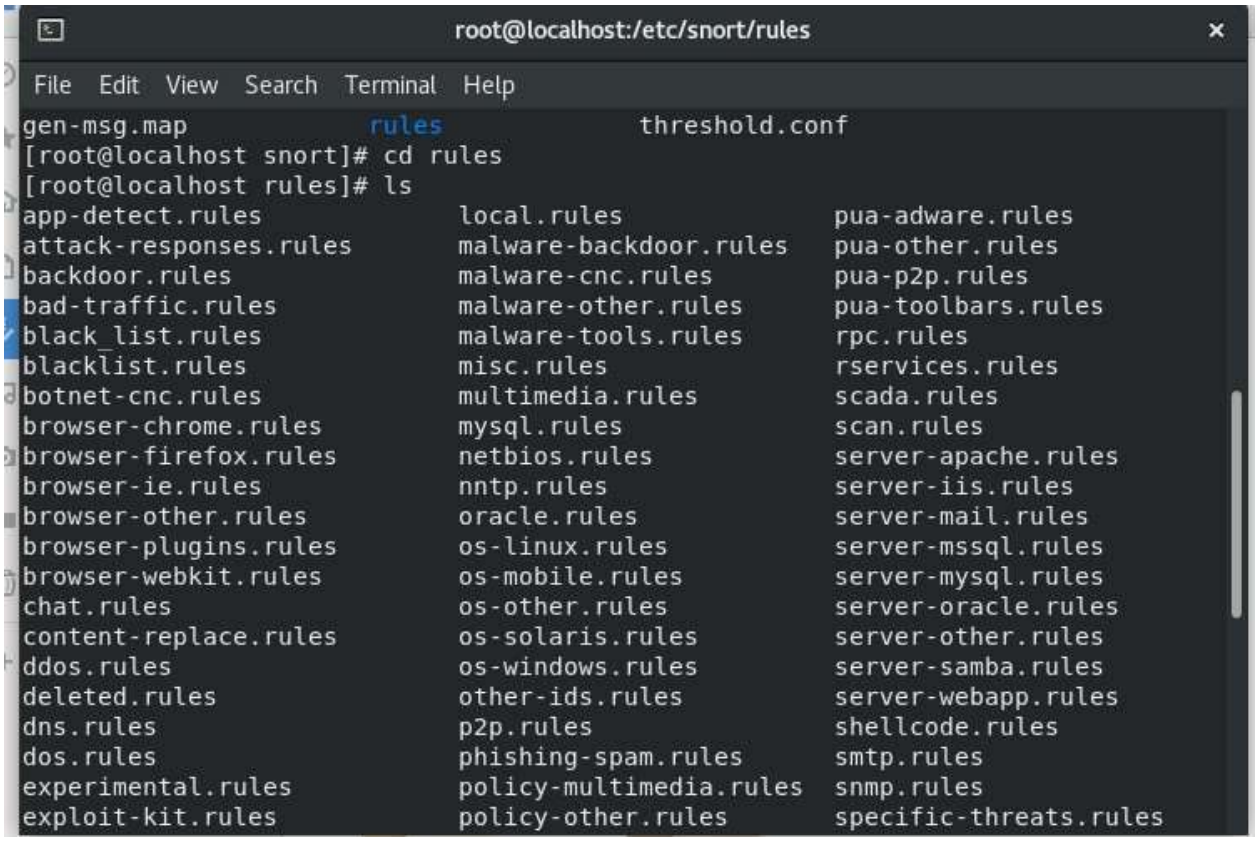


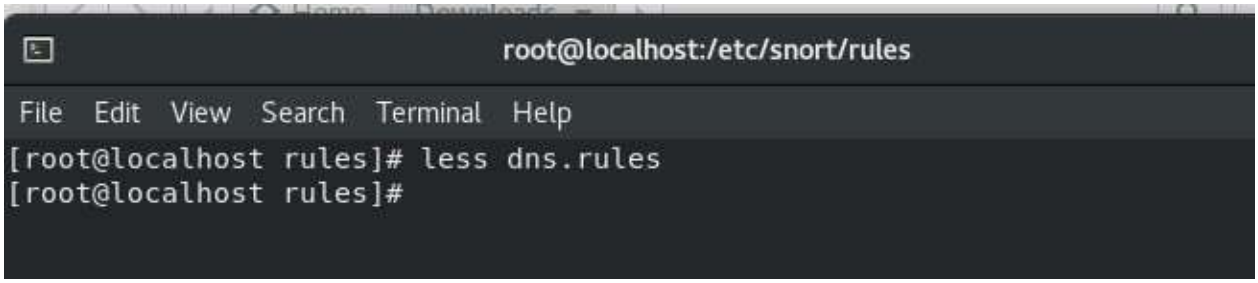
Step-18:- # cd /etc/snort

#ls

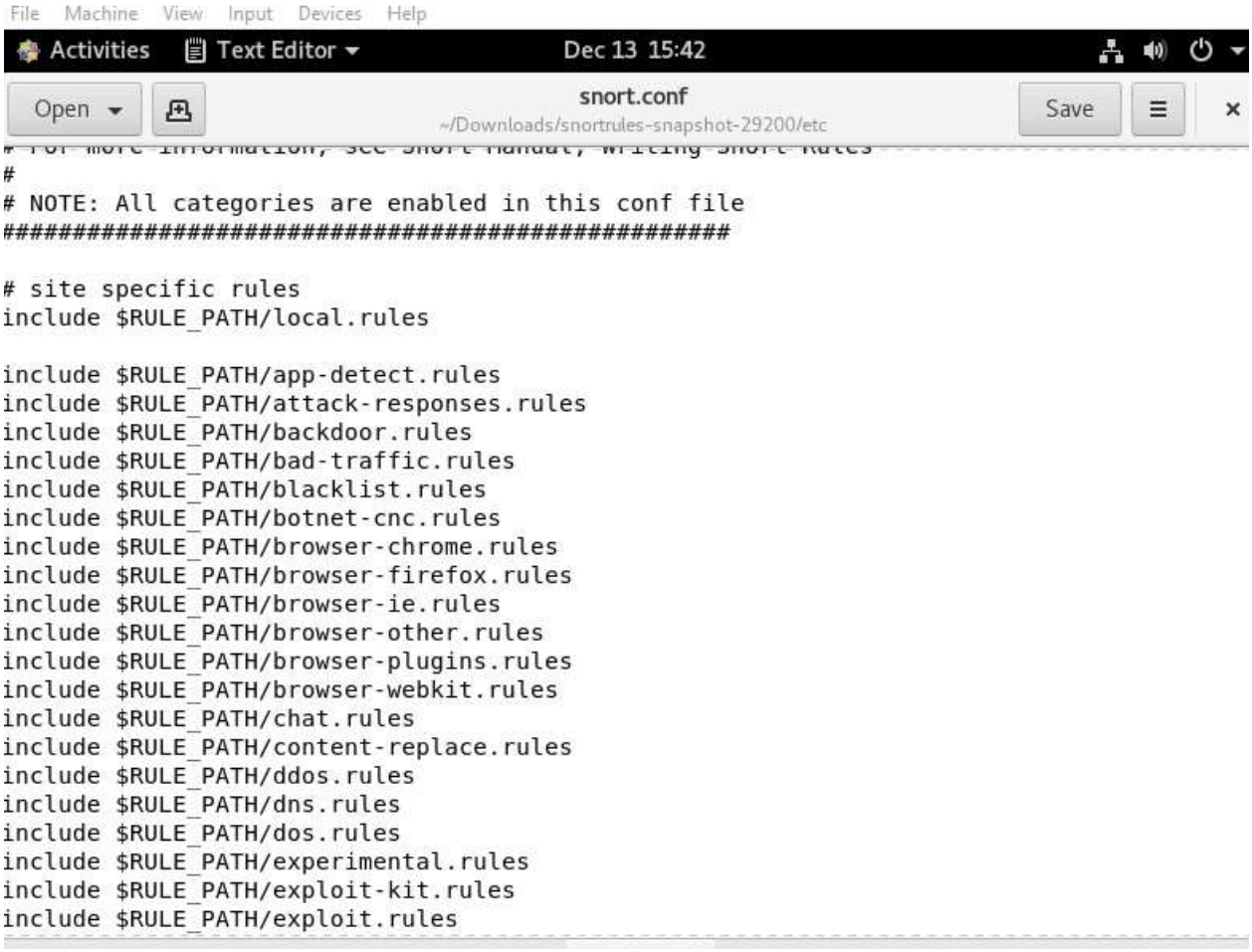
#cd rules


root@localhost:/etc/snort/rules
File Edit View Search Terminal Help
[root@localhost Downloads]# cd /etc/snort
[root@localhost snort]# ls
classification.config preproc_rules snort.conf unicode.map
etc reference.config so_rules
gen-msg.map rules threshold.conf
[root@localhost snort]# cd rules
[root@localhost rules]#

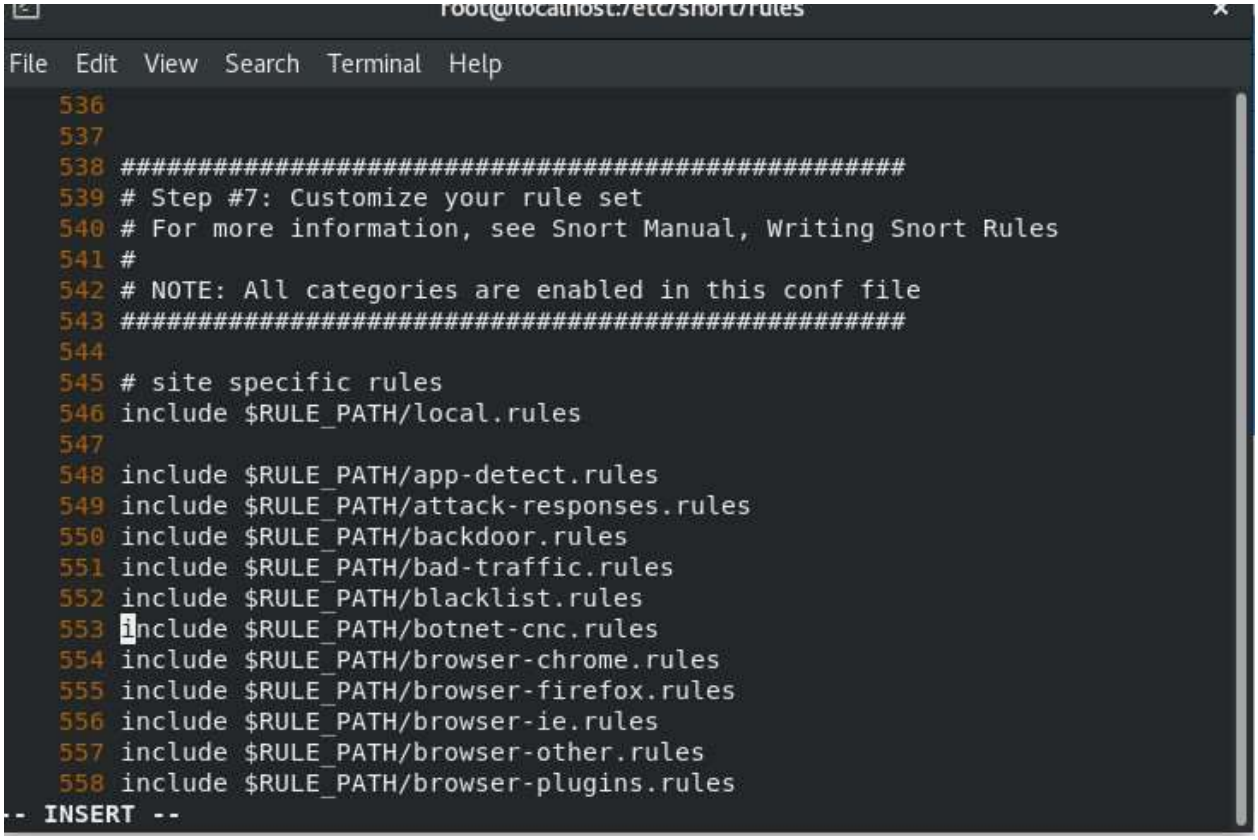

root@localhost:/etc/snort/rules
File Edit View Search Terminal Help
gen-msg.map rules threshold.conf
[root@localhost snort]# cd rules
[root@localhost rules]# ls
app-detect.rules local.rules pua-adware.rules
attack-responses.rules malware-backdoor.rules pua-other.rules
backdoor.rules malware-cnc.rules pua-p2p.rules
bad-traffic.rules malware-other.rules pua-toolbars.rules
black_list.rules malware-tools.rules rpc.rules
blacklist.rules misc.rules rservices.rules
botnet-cnc.rules multimedia.rules scada.rules
browser-chrome.rules mysql.rules scan.rules
browser-firefox.rules netbios.rules server-apache.rules
browser-ie.rules nntp.rules server-iis.rules
browser-other.rules oracle.rules server-mail.rules
browser-plugins.rules os-linux.rules server-mssql.rules
browser-webkit.rules os-mobile.rules server-mysql.rules
chat.rules os-other.rules server-oracle.rules
content-replace.rules os-solaris.rules server-other.rules
ddos.rules os-windows.rules server-samba.rules
deleted.rules other-ids.rules server-webapp.rules
dns.rules p2p.rules shellcode.rules
dos.rules phishing-spam.rules smtp.rules
experimental.rules policy-multimedia.rules snmp.rules
exploit-kit.rules policy-other.rules specific-threats.rules


root@localhost:/etc/snort/rules
File Edit View Search Terminal Help
[root@localhost rules]# less dns.rules
[root@localhost rules]#

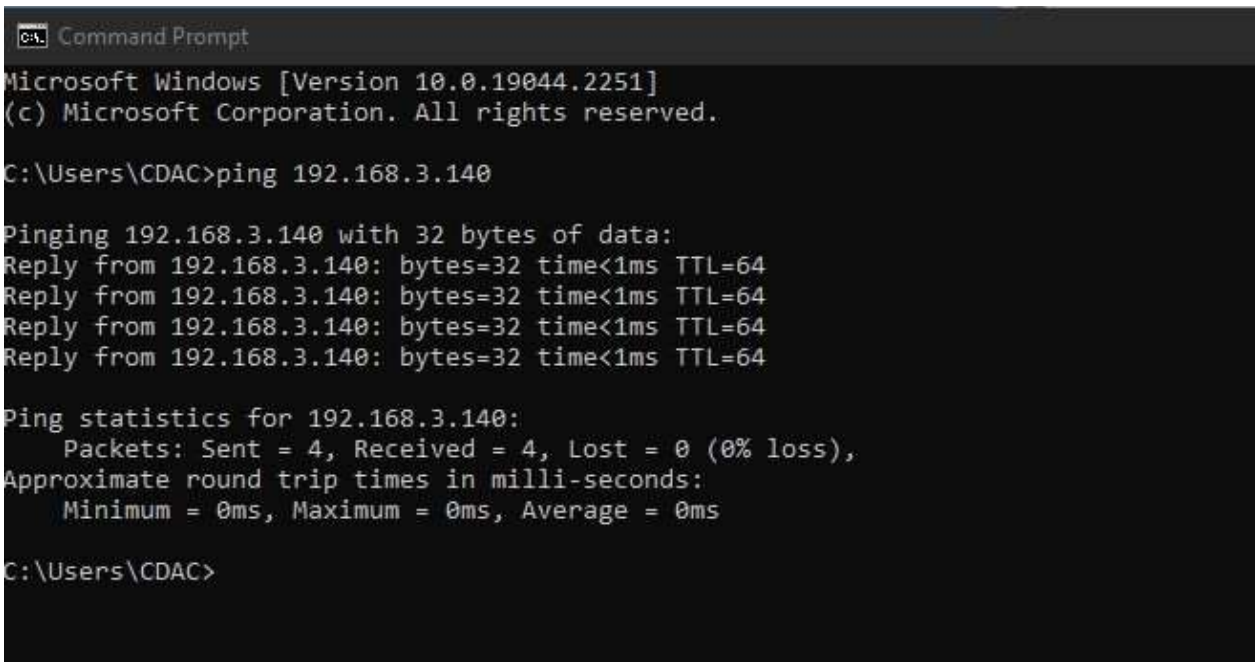
Step-19:- go to directory
home/downloads/snortrules-snapshot-2.9.200/etc/snort.conf
Copy the rules line 548 to till —X11



Step-20:-
#vi /etc/snort/snort.conf
And add the all rule line 548 to till —X11



Step-21:- Go to Windows Command Prompt and Ping 192.168.3.140



Step-22:- Now Go to CentOS and check the output