

Assignments:-4

Module:- NDC(SNORT_LINUX)

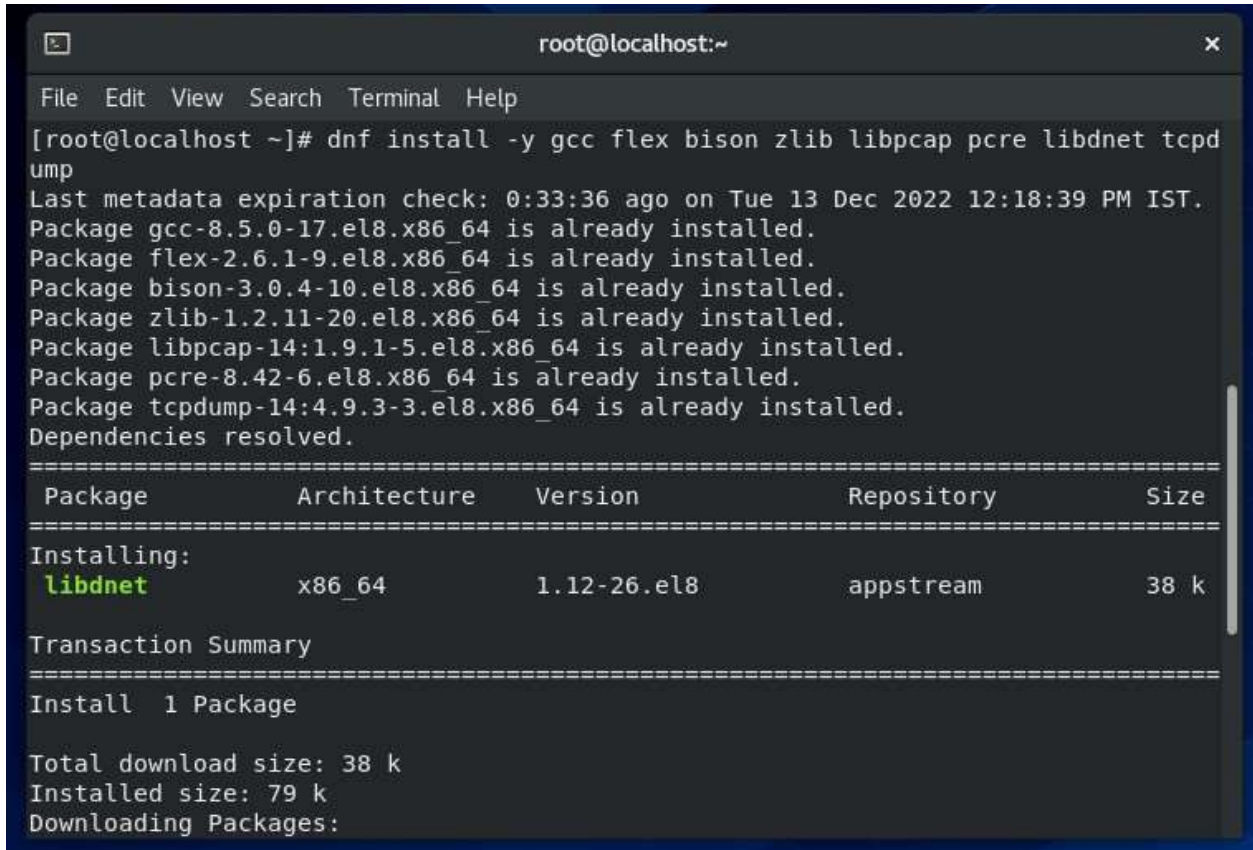
Name:- Prithviraj Nikam

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



```
root@localhost:~  
File Edit View Search Terminal Help  
[root@localhost ~]# dnf install -y gcc flex bison zlib libpcap pcre libdnet tcpdump  
Last metadata expiration check: 0:33:36 ago on Tue 13 Dec 2022 12:18:39 PM IST.  
Package gcc-8.5.0-17.el8.x86_64 is already installed.  
Package flex-2.6.1-9.el8.x86_64 is already installed.  
Package bison-3.0.4-10.el8.x86_64 is already installed.  
Package zlib-1.2.11-20.el8.x86_64 is already installed.  
Package libpcap-14:1.9.1-5.el8.x86_64 is already installed.  
Package pcre-8.42-6.el8.x86_64 is already installed.  
Package tcpdump-4:4.9.3-3.el8.x86_64 is already installed.  
Dependencies resolved.  
=====
```

Package	Architecture	Version	Repository	Size
libdnet	x86_64	1.12-26.el8	appstream	38 k

```
=====
```

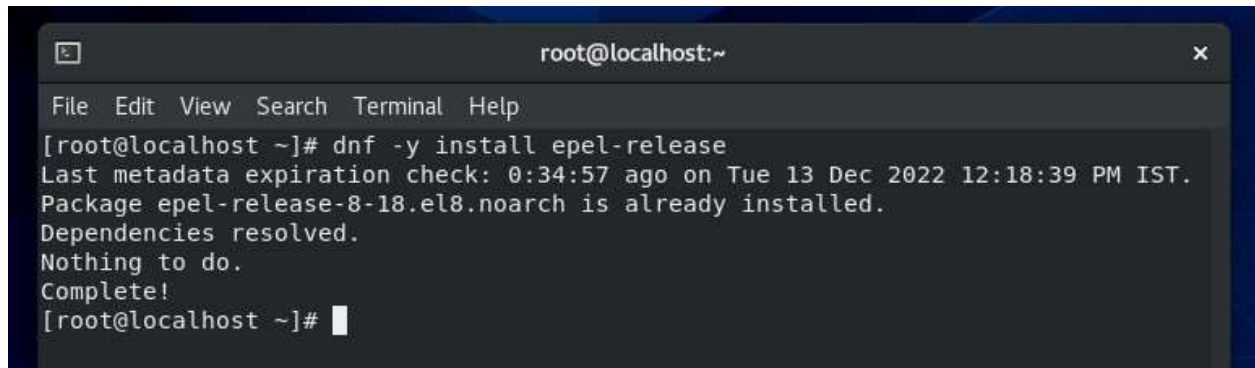
Transaction Summary

=====

Install 1 Package

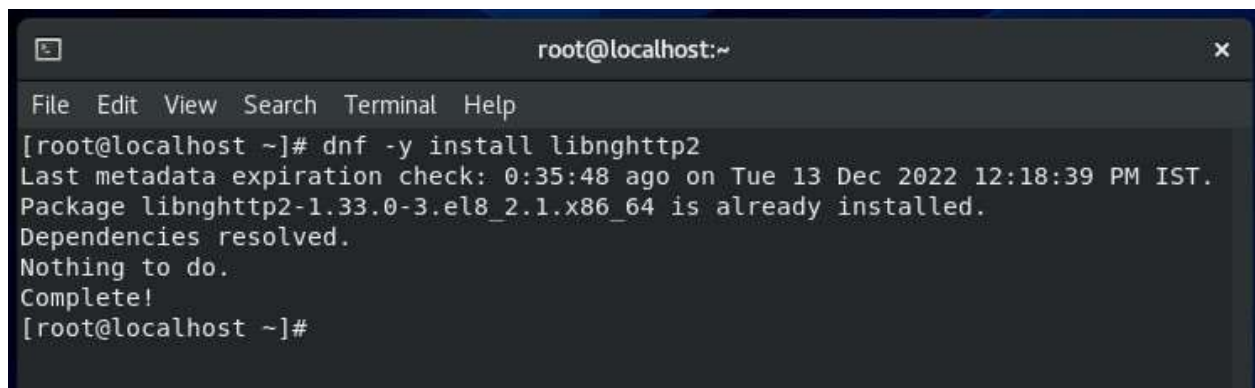
Total download size: 38 k
Installed size: 79 k
Downloading Packages:

Step-2:- dnf install -y epel-release

A terminal window titled 'root@localhost:~' with a menu bar (File, Edit, View, Search, Terminal, Help). The terminal shows the command 'dnf -y install epel-release' and its output: 'Last metadata expiration check: 0:34:57 ago on Tue 13 Dec 2022 12:18:39 PM IST. Package epel-release-8-18.el8.noarch is already installed. Dependencies resolved. Nothing to do. Complete! [root@localhost ~]#'.

```
root@localhost:~  
File Edit View Search Terminal Help  
[root@localhost ~]# dnf -y install epel-release  
Last metadata expiration check: 0:34:57 ago on Tue 13 Dec 2022 12:18:39 PM IST.  
Package epel-release-8-18.el8.noarch is already installed.  
Dependencies resolved.  
Nothing to do.  
Complete!  
[root@localhost ~]#
```

Step-3:- dnf install -y libnghttp2

A terminal window titled 'root@localhost:~' with a menu bar (File, Edit, View, Search, Terminal, Help). The terminal shows the command 'dnf -y install libnghttp2' and its output: 'Last metadata expiration check: 0:35:48 ago on Tue 13 Dec 2022 12:18:39 PM IST. Package libnghttp2-1.33.0-3.el8_2.1.x86_64 is already installed. Dependencies resolved. Nothing to do. Complete! [root@localhost ~]#'.

```
root@localhost:~  
File Edit View Search Terminal Help  
[root@localhost ~]# dnf -y install libnghttp2  
Last metadata expiration check: 0:35:48 ago on Tue 13 Dec 2022 12:18:39 PM IST.  
Package libnghttp2-1.33.0-3.el8_2.1.x86_64 is already installed.  
Dependencies resolved.  
Nothing to do.  
Complete!  
[root@localhost ~]#
```

Step-4:- dnf install daq

```
root@localhost:~  
File Edit View Search Terminal Help  
[root@localhost ~]# dnf -y install daq  
Last metadata expiration check: 0:36:28 ago on Tue 13 Dec 2022 12:18:39 PM IST.  
Dependencies resolved.  
=====
```

Package	Architecture	Version	Repository	Size
Installing:				
daq	x86_64	2.0.6-9.el8	epel	88 k

```
=====
```

Transaction Summary

=====

Install 1 Package

Total download size: 88 k
Installed size: 238 k
Downloading Packages:

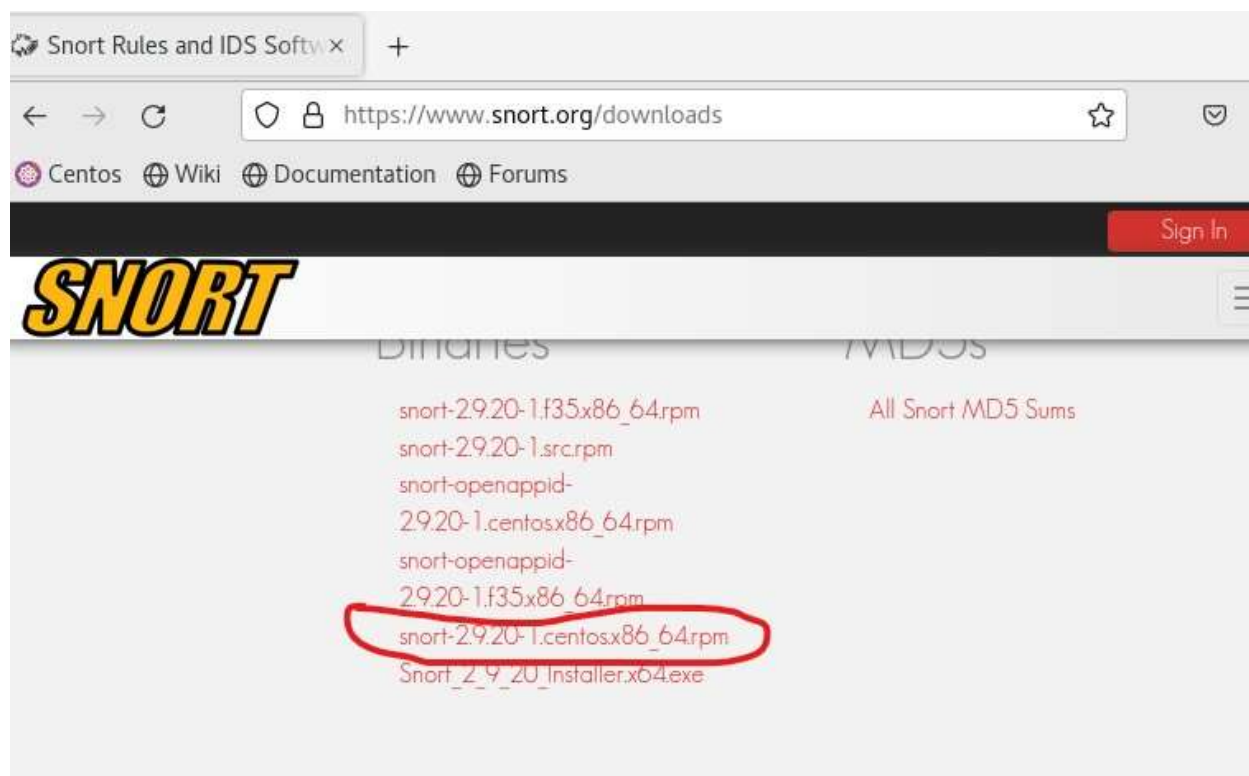
daq-2.0.6-9.el8.x86_64.rpm	168 kB/s 88 kB	00:00

Total	62 kB/s 88 kB	00:01

```
Running transaction check  
Transaction check succeeded.  
Running transaction test
```

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.  
=====
```

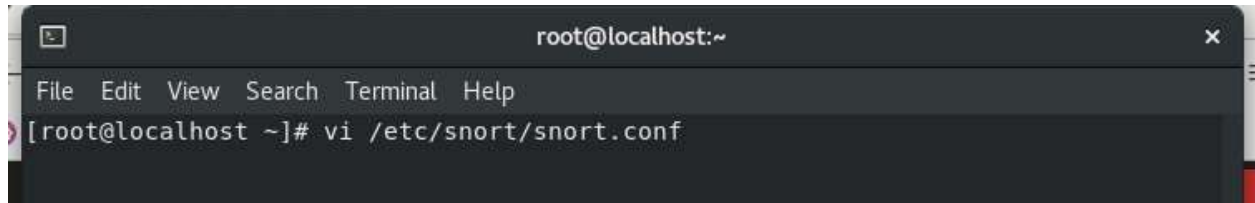
Package	Arch	Version	Repository	Size
Installing:				
snort	x86_64	1:2.9.20-1	@commandline	4.6 M
Installing dependencies:				
compat-openssl10	x86_64	1:1.0.2o-4.el8	appstream	1.1 M
libnsl	x86_64	2.28-220.el8	baseos	105 k

```
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	

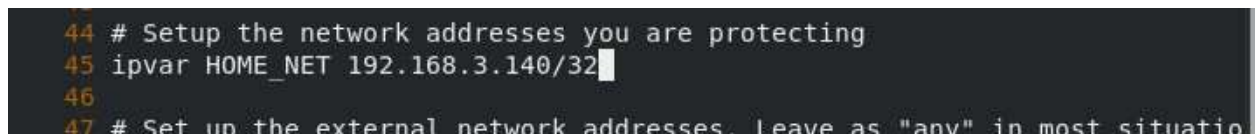
Step-6:-Configure SNORT

a. Vi /etc/snort/snort.conf

A screenshot of a terminal window titled 'root@localhost:~'. The window has a menu bar with 'File', 'Edit', 'View', 'Search', 'Terminal', and 'Help'. The command prompt shows '[root@localhost ~]# vi /etc/snort/snort.conf'.

b. On line number 45 –

ipvar HOME_NET 192.168.3.140/32

A screenshot of the snort.conf file in a terminal. Line 44 is '# Setup the network addresses you are protecting'. Line 45 is 'ipvar HOME_NET 192.168.3.140/32'. Line 46 is empty. Line 47 is '# Set up the external network addresses. Leave as "any" in most situations'.

On line number 48 –

ipvar EXTERNAL_NET !\$HOME_NET

A screenshot of the snort.conf file in a terminal. Line 47 is '# Set up the external network addresses. Leave as "any" in most situations'. Line 48 is 'ipvar EXTERNAL_NET !\$HOME_NET'. Line 49 is empty.

On line number 105 and 106

var SO_RULE_PATH /etc/snort/so_rules

var PREPROC_RULE_PATH /etc/snort/preproc_rules

A screenshot of the snort.conf file in a terminal. Line 103 is '# such as: c:\snort\rules'. Line 104 is 'var RULE_PATH /etc/snort/rules'. Line 105 is 'var SO_RULE_PATH /etc/snort/so_rules'. Line 106 is 'var PREPROC_RULE_PATH /etc/snort/preproc_rules'. Line 107 is empty.

On line number 113 and 114

var WHITE_LIST_PATH /etc/snort/rules

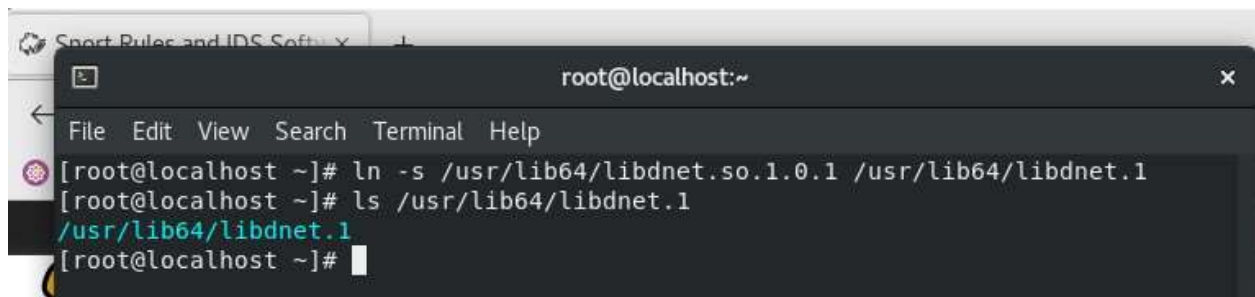
var BLACK_LIST_PATH /etc/snort/rules

```
111 # This is completely inconsistent with how other vars work, but 65500
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

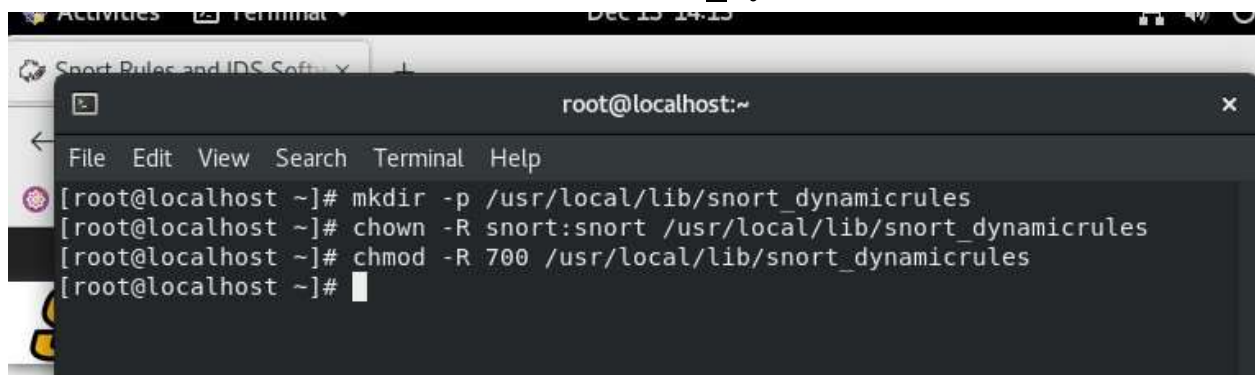
```
544
545 # site specific rules
546 include $RULE_PATH/local.rules
547
548 #####
```

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

A terminal window titled 'root@localhost:~' with a menu bar (File, Edit, View, Search, Terminal, Help). The terminal shows the following commands and output:

```
[root@localhost ~]# ln -s /usr/lib64/libdnet.so.1.0.1 /usr/lib64/libdnet.1
[root@localhost ~]# ls /usr/lib64/libdnet.1
/usr/lib64/libdnet.1
[root@localhost ~]#
```

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

A terminal window titled 'root@localhost:~' with a menu bar (File, Edit, View, Search, Terminal, Help). The terminal shows the following commands and output:

```
[root@localhost ~]# mkdir -p /usr/local/lib/snort_dynamicrules
[root@localhost ~]# chown -R snort:snort /usr/local/lib/snort_dynamicrules
[root@localhost ~]# chmod -R 700 /usr/local/lib/snort_dynamicrules
[root@localhost ~]#
```

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


```
root@localhost:~  
File Edit View Search Terminal Help  
[root@localhost ~]# touch /etc/snort/rules/white_list.rules  
[root@localhost ~]# touch /etc/snort/rules/black_list.rules  
[root@localhost ~]# touch /etc/snort/rules/local.rules  
[root@localhost ~]#
```

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

```
root@localhost:~  
File Edit View Search Terminal Help  
[root@localhost ~]# snort -T -i enp0s3 -c /etc/snort/snort.conf  
Running in Test 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 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 34443:34444 41080 50002  
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 14  
14 1741 1830 2301 2381 2809 3037 3128 3702 4343 4848 5250 6988 7000:7001 7144:71  
45 7510 7777 7779 8000 8008 8014 8028 8080 8085 8088 8090 8118 8123 8180:8181 82  
43 8280 8300 8800 8888 8899 9000 9060 9080 9090:9091 9443 9999 11371 34443:34444  
41080 50002 55555 ]
```

Step-11:- go to local.rules

#vi /etc/snort/rules/local.rules

```
root@localhost:~  
File Edit View Search Terminal Help  
[root@localhost ~]# vi /etc/snort/rules/local.rules
```

```
root@localhost:~  
File Edit View Search Terminal Help  
alert icmp any any -> $HOME_NET any (msg:"ICMP"; sid:10000001; rev:001;)  
~  
~
```

Step-12:- run the console

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

```
root@localhost:~  
File Edit View Search Terminal Help  
[root@localhost ~]# vi /etc/snort/rules/local.rules  
[root@localhost ~]# snort -A console -i enp0s3 -c /etc/snort/snort.conf  
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 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 34443:34444 41080 50002  
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 14  
14 1741 1830 2301 2381 2809 3037 3128 3702 4343 4848 5250 6988 7000:7001 7144:71  
45 7510 7777 7779 8000 8008 8014 8028 8080 8085 8088 8090 8118 8123 8180:8181 82  
43 8280 8300 8800 8888 8899 9000 9060 9080 9090:9091 9443 9999 11371 34443:34444  
41080 50002 55555 ]
```

**Step-13:- Go to Windows Command Prompt and
ping 192.168.3.140**


```
CA: Command Prompt
Microsoft Windows [Version 10.0.19044.2251]
(c) Microsoft Corporation. All rights reserved.

C:\Users\CDAC>ping 192.168.3.140

Pinging 192.168.3.140 with 32 bytes of data:
Reply from 192.168.3.140: bytes=32 time<1ms TTL=64
Reply from 192.168.3.140: bytes=32 time<1ms TTL=64
Reply from 192.168.3.140: bytes=32 time<1ms TTL=64
Reply from 192.168.3.140: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.3.140:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\CDAC>
```

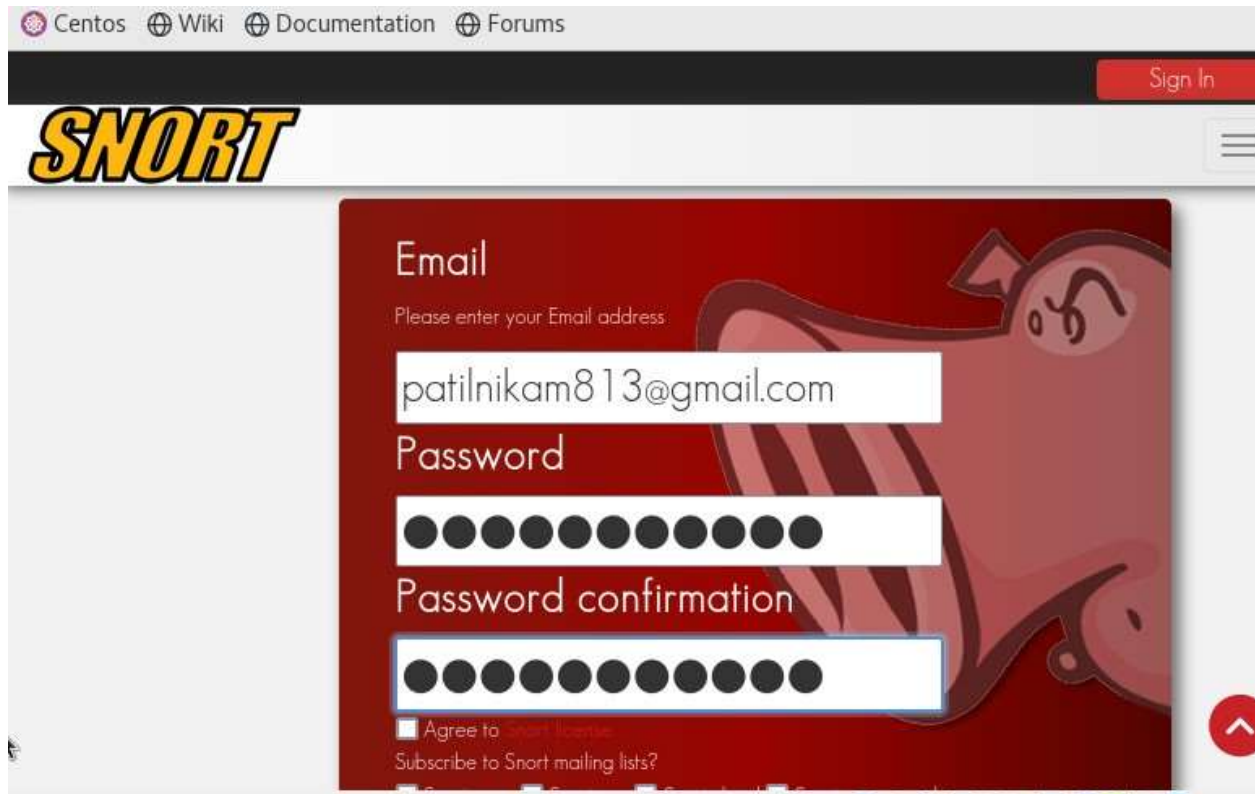
Step-14:-Go to CentOS and check the output

```
Preprocessor Object: SF_IMAP Version 1.0 <Build 1>
Preprocessor Object: SF_GTP Version 1.1 <Build 1>
Preprocessor Object: SF_SSH Version 1.1 <Build 3>
Preprocessor Object: SF_FTPTELNET Version 1.2 <Build 13>
Preprocessor Object: SF_DNS Version 1.1 <Build 4>
Preprocessor Object: SF_DNP3 Version 1.1 <Build 1>
Preprocessor Object: SF_DCERPC2 Version 1.0 <Build 3>
Commencing packet processing (pid=1067890)
12/13-14:30:28.264834  [**] [1:10000001:1] ICMP [**] [Priority: 0] {ICMP} 192.16
8.3.131 -> 192.168.3.140
12/13-14:30:29.267901  [**] [1:10000001:1] ICMP [**] [Priority: 0] {ICMP} 192.16
8.3.131 -> 192.168.3.140
12/13-14:30:30.271880  [**] [1:10000001:1] ICMP [**] [Priority: 0] {ICMP} 192.16
8.3.131 -> 192.168.3.140
12/13-14:30:31.276751  [**] [1:10000001:1] ICMP [**] [Priority: 0] {ICMP} 192.16
8.3.131 -> 192.168.3.140
```

Step-15:- Go to Snort official website

<https://www.snort.org/>

And sign in

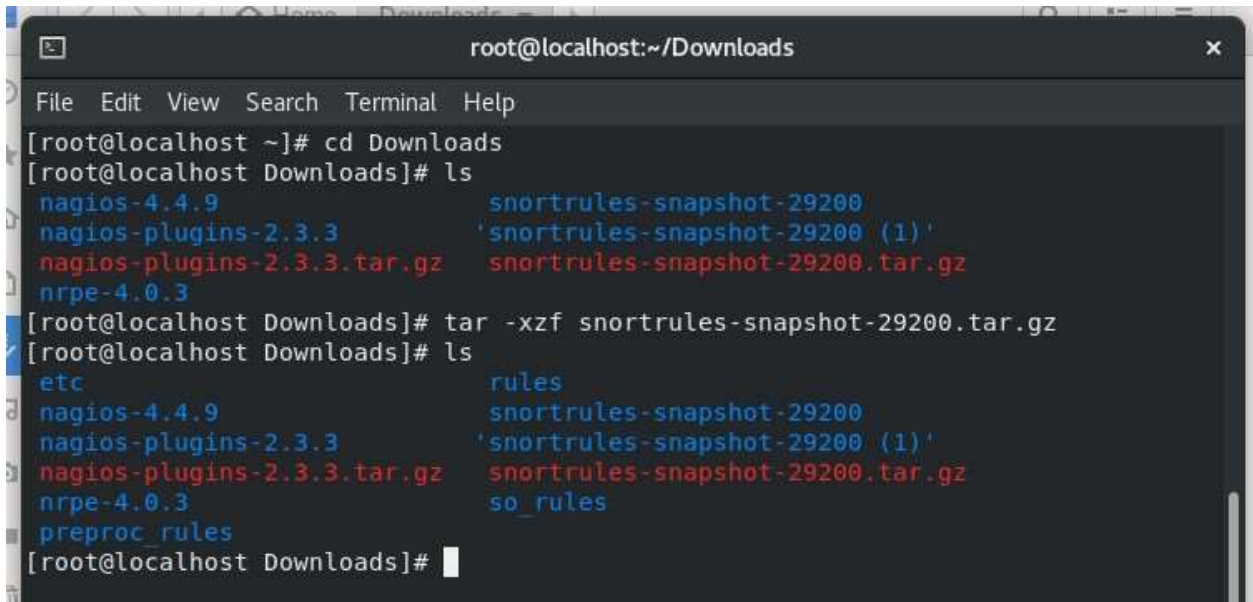


Step-16:-Downloads the

<https://www.snort.org/downloads/registered/snortrules-snapshot-29200.tar.gz>

Extract the file

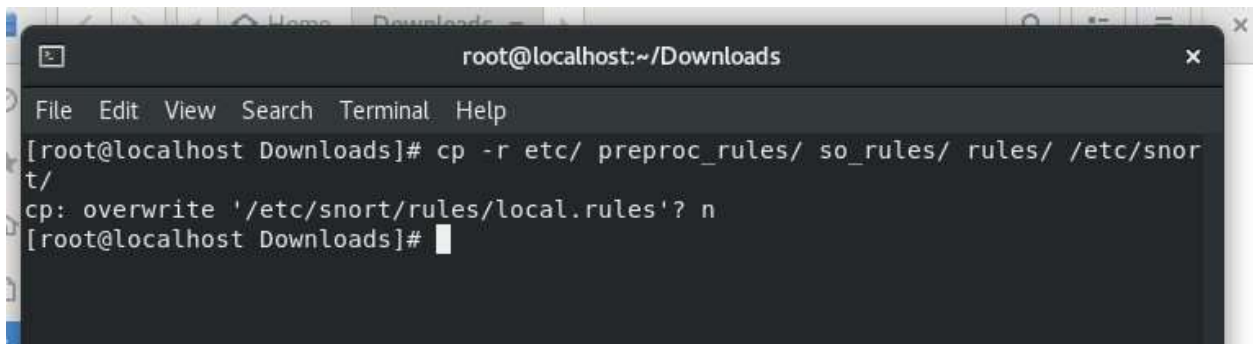
#tar -xzf File_name.tar.gz



```
root@localhost:~/Downloads
File Edit View Search Terminal Help
[root@localhost ~]# cd Downloads
[root@localhost Downloads]# ls
nagios-4.4.9          snortrules-snapshot-29200
nagios-plugins-2.3.3  'snortrules-snapshot-29200 (1)'
nagios-plugins-2.3.3.tar.gz  snortrules-snapshot-29200.tar.gz
nrpe-4.0.3
[root@localhost Downloads]# tar -xzf snortrules-snapshot-29200.tar.gz
[root@localhost Downloads]# ls
etc          rules
nagios-4.4.9  snortrules-snapshot-29200
nagios-plugins-2.3.3  'snortrules-snapshot-29200 (1)'
nagios-plugins-2.3.3.tar.gz  snortrules-snapshot-29200.tar.gz
nrpe-4.0.3      so_rules
preproc_rules
[root@localhost Downloads]#
```

Step-17:- Copy the files

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



```
root@localhost:~/Downloads
File Edit View Search Terminal Help
[root@localhost Downloads]# cp -r etc/ preproc_rules/ so_rules/ rules/ /etc/snort/
cp: overwrite '/etc/snort/rules/local.rules'? n
[root@localhost Downloads]#
```

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]#
```

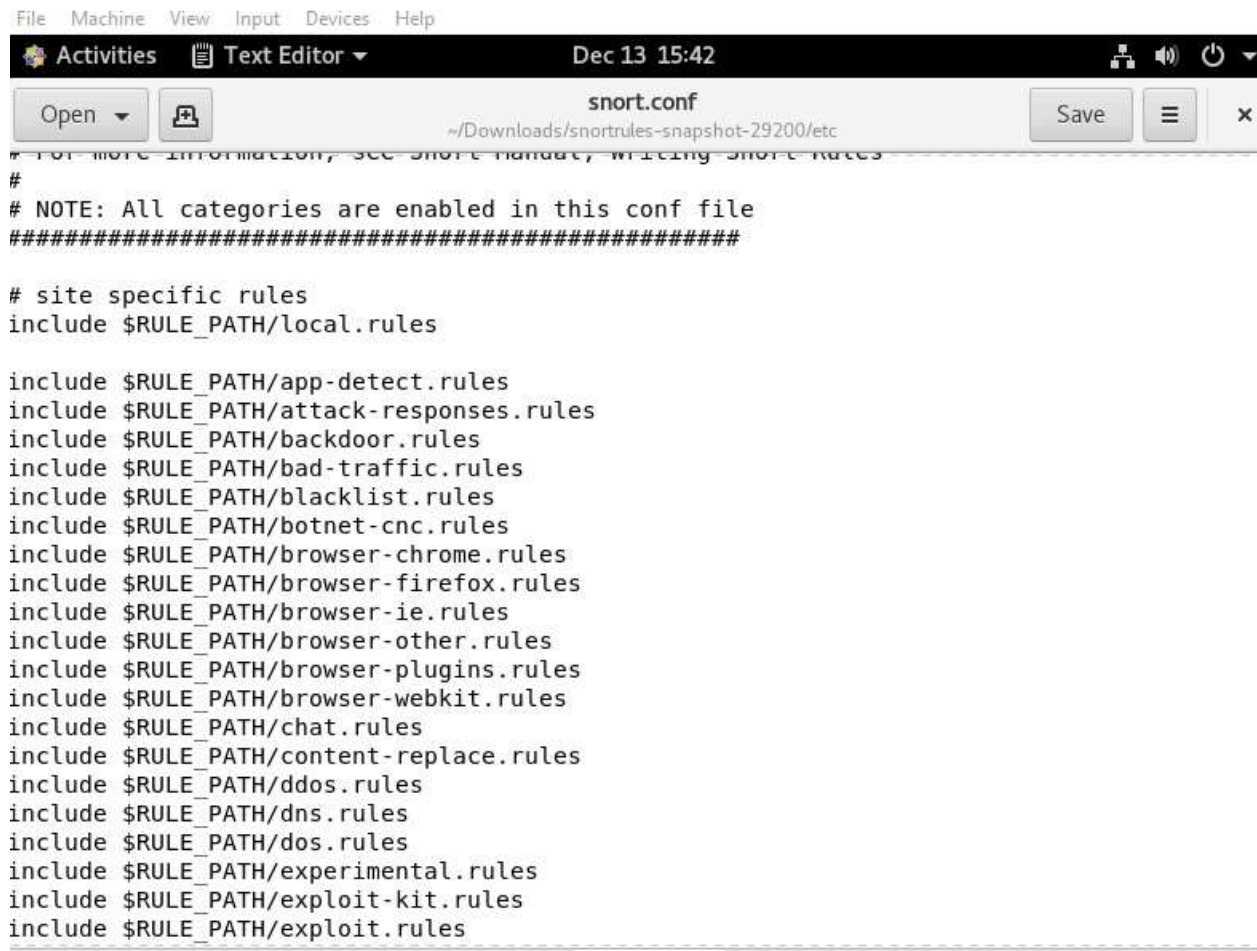
```
root@localhost:/etc/snort/rules
File Edit View Search Terminal Help
gen-msg.map           rules          threshold.conf
[root@localhost snort]# cd rules
[root@localhost rules]# ls
app-detect.rules      local.rules    pua-adware.rules
attack-responses.rules  malware-backdoor.rules  pua-other.rules
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

A screenshot of a Linux desktop environment. At the top, there is a menu bar with 'File', 'Machine', 'View', 'Input', 'Devices', and 'Help'. Below it is a panel with 'Activities', 'Text Editor', and a clock showing 'Dec 13 15:42'. The main window is a text editor titled 'snort.conf' with a path bar showing '~/.Downloads/snortrules-snapshot-29200/etc'. The editor contains the following text:

```
# For more information, see snort manual, writing snort rules
#
# NOTE: All categories are enabled in this conf file
#####

# site specific rules
include $RULE_PATH/local.rules

include $RULE_PATH/app-detect.rules
include $RULE_PATH/attack-responses.rules
include $RULE_PATH/backdoor.rules
include $RULE_PATH/bad-traffic.rules
include $RULE_PATH/blacklist.rules
include $RULE_PATH/botnet-cnc.rules
include $RULE_PATH/browser-chrome.rules
include $RULE_PATH/browser-firefox.rules
include $RULE_PATH/browser-ie.rules
include $RULE_PATH/browser-other.rules
include $RULE_PATH/browser-plugins.rules
include $RULE_PATH/browser-webkit.rules
include $RULE_PATH/chat.rules
include $RULE_PATH/content-replace.rules
include $RULE_PATH/ddos.rules
include $RULE_PATH/dns.rules
include $RULE_PATH/dos.rules
include $RULE_PATH/experimental.rules
include $RULE_PATH/exploit-kit.rules
include $RULE_PATH/exploit.rules
```

Step-20:-

#vi /etc/snort/snort.conf

And add the all rule line 548 to till —X11


```
root@localhost:~# cat /etc/snort/rules
536
537
538 #####
539 # Step #7: Customize your rule set
540 # For more information, see Snort Manual, Writing Snort Rules
541 #
542 # NOTE: All categories are enabled in this conf file
543 #####
544
545 # site specific rules
546 include $RULE_PATH/local.rules
547
548 include $RULE_PATH/app-detect.rules
549 include $RULE_PATH/attack-responses.rules
550 include $RULE_PATH/backdoor.rules
551 include $RULE_PATH/bad-traffic.rules
552 include $RULE_PATH/blacklist.rules
553 include $RULE_PATH/botnet-cnc.rules
554 include $RULE_PATH/browser-chrome.rules
555 include $RULE_PATH/browser-firefox.rules
556 include $RULE_PATH/browser-ie.rules
557 include $RULE_PATH/browser-other.rules
558 include $RULE_PATH/browser-plugins.rules
-- INSERT --
```

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

```
C:\> Command Prompt
Microsoft Windows [Version 10.0.19044.2251]
(c) Microsoft Corporation. All rights reserved.

C:\Users\CDAC>ping 192.168.3.140

Pinging 192.168.3.140 with 32 bytes of data:
Reply from 192.168.3.140: bytes=32 time<1ms TTL=64
Reply from 192.168.3.140: bytes=32 time<1ms TTL=64
Reply from 192.168.3.140: bytes=32 time<1ms TTL=64
Reply from 192.168.3.140: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.3.140:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\CDAC>
```

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

```
inc Preprocessor Object: SF_NGHTTP Version 1.1 <Build 1>
inc Preprocessor Object: SF_IMAP Version 1.0 <Build 1>
inc Preprocessor Object: SF_GTP Version 1.1 <Build 1>
inc Preprocessor Object: SF_SSH Version 1.1 <Build 3>
inc Preprocessor Object: SF_FTPTELNET Version 1.2 <Build 13>
inc Preprocessor Object: SF_DNS Version 1.1 <Build 4>
Preprocessor Object: SF_DNP3 Version 1.1 <Build 1>
Preprocessor Object: SF_DCERPC2 Version 1.0 <Build 3>
###
# S Commencing packet processing (pid=1117377)
# F 12/13-15:41:41.227932  [**] [1:10000001:1] ICMP [**] [Priority: 0] {ICMP} 192.16
8.3.131 -> 192.168.3.140
###
# d 12/13-15:41:42.231641  [**] [1:10000001:1] ICMP [**] [Priority: 0] {ICMP} 192.16
8.3.131 -> 192.168.3.140
# i 12/13-15:41:43.236711  [**] [1:10000001:1] ICMP [**] [Priority: 0] {ICMP} 192.16
8.3.131 -> 192.168.3.140
# i 12/13-15:41:44.240241  [**] [1:10000001:1] ICMP [**] [Priority: 0] {ICMP} 192.16
8.3.131 -> 192.168.3.140
###
# Step #9: Customize your Shared Object Snort Rules
```