SETTING UP SNORT IN DMZ:

In this module, we setup the Snort in a workstation in DMZ which we had already configured in the previous modules.

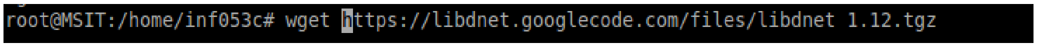
Steps involved in setting up Snort:

1. Install the pre-required dependencies for Snort.

   ```
   $ sudo apt-get install flex bison build-essential checkinstall libpcap-dev libnet1-dev libpcre3-dev libmysqlclient15-dev libnetfilter-queue-dev iptables-dev
   ```

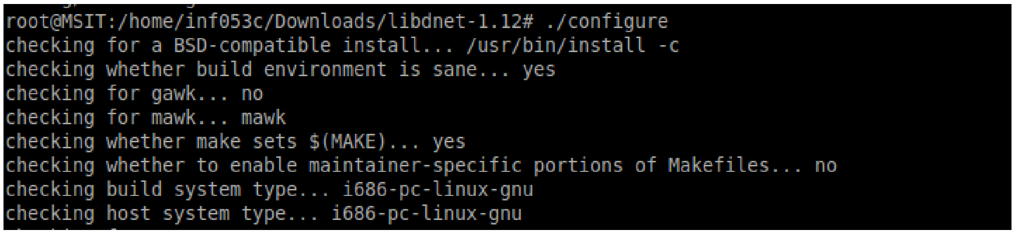
2. Build and install `libdnet` from its source code.

   a. Download `libdnet`.



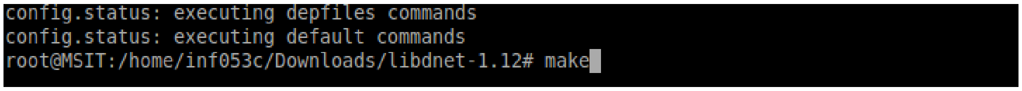
```
root@MSIT:/home/inf053c# wget https://libdnet.googlecode.com/files/libdnet 1.12.tgz
```

   b. Configure.



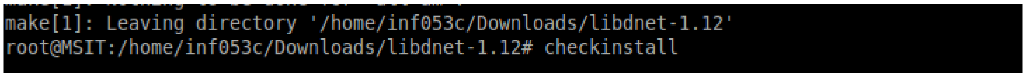
```
root@MSIT:/home/inf053c/Downloads/libdnet-1.12# ./configure
checking for a BSD-compatible install... /usr/bin/install -c
checking whether build environment is sane... yes
checking for gawk... no
checking for mawk... mawk
checking whether make sets $(MAKE)... yes
checking whether to enable maintainer-specific portions of Makefiles... no
checking build system type... i686-pc-linux-gnu
checking host system type... i686-pc-linux-gnu
```

   c. Make.

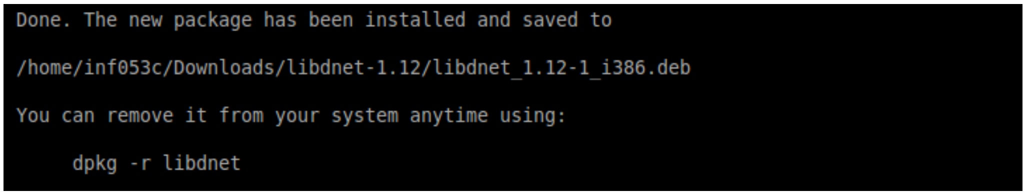


```
config.status: executing depfiles commands
config.status: executing default commands
root@MSIT:/home/inf053c/Downloads/libdnet-1.12# make
```

   d. Check Install

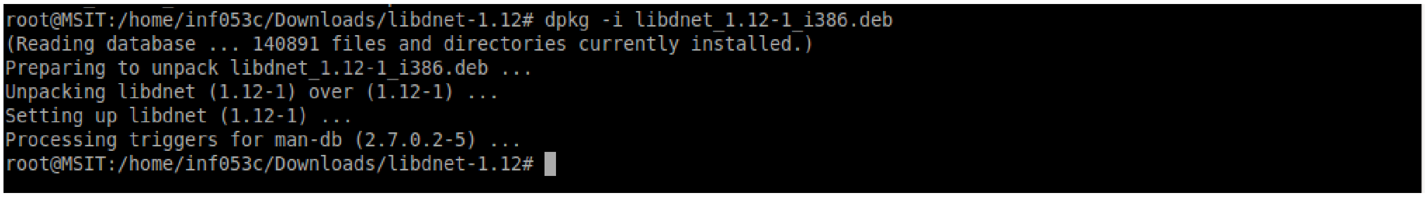


```
make[1]: Leaving directory '/home/inf053c/Downloads/libdnet-1.12'
root@MSIT:/home/inf053c/Downloads/libdnet-1.12# checkinstall
```



```
 Done. The new package has been installed and saved to

 /home/inf053c/Downloads/libdnet-1.12/libdnet_1.12-1_i386.deb

 You can remove it from your system anytime using:

      dpkg -r libdnet
```

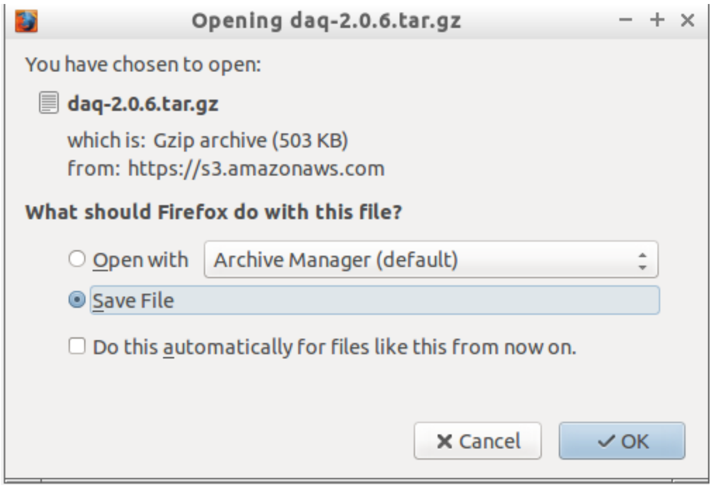
e. Install the `libdnet_1.12-1_i386.deb` package:



```
root@MSIT:/home/inf053c/Downloads/libdnet-1.12# dpkg -i libdnet_1.12-1_i386.deb
(Reading database ... 140891 files and directories currently installed.)
Preparing to unpack libdnet_1.12-1_i386.deb ...
Unpacking libdnet (1.12-1) over (1.12-1) ...
Setting up libdnet (1.12-1) ...
Processing triggers for man-db (2.7.0.2-5) ...
root@MSIT:/home/inf053c/Downloads/libdnet-1.12# 
```

3. Download, build and Install DAQ (Data Acquisition Library).

   a. Download DAQ from Snort official website.



Opening daq-2.0.6.tar.gz

You have chosen to open:

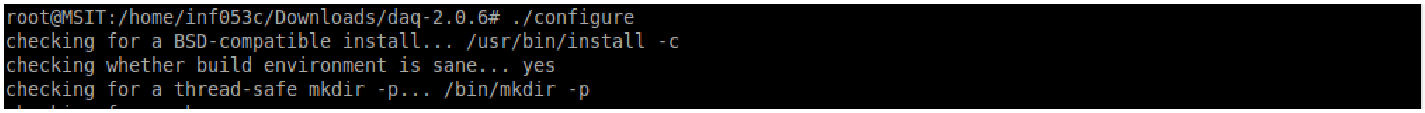
daq-2.0.6.tar.gz

which is: Gzip archive (503 KB)
from: https://s3.amazonaws.com

What should Firefox do with this file?

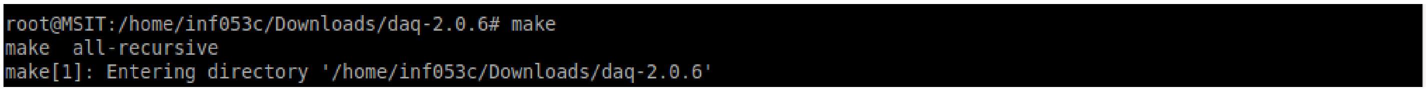
○ Open with Archive Manager (default)
● Save File
□ Do this automatically for files like this from now on.

   b. Extract it and configure.



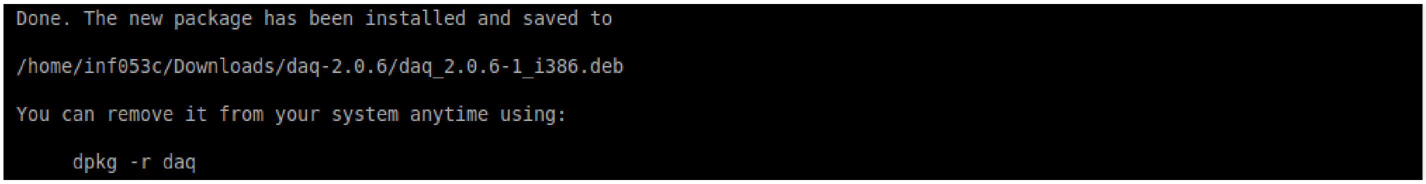
```
root@MSIT:/home/inf053c/Downloads/daq-2.0.6# ./configure
checking for a BSD-compatible install... /usr/bin/install -c
checking whether build environment is sane... yes
checking for a thread-safe mkdir -p... /bin/mkdir -p
```

   c. Make



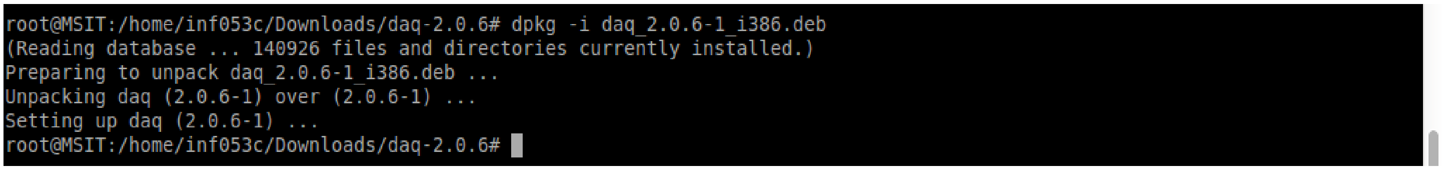
```
root@MSIT:/home/inf053c/Downloads/daq-2.0.6# make
make  all-recursive
make[1]: Entering directory '/home/inf053c/Downloads/daq-2.0.6'
```

   d. Check Install



```
 Done. The new package has been installed and saved to

 /home/inf053c/Downloads/daq-2.0.6/daq_2.0.6-1_i386.deb

 You can remove it from your system anytime using:

      dpkg -r daq
```

e. Install the `daq_2.0.6-1_i386.deb` package.

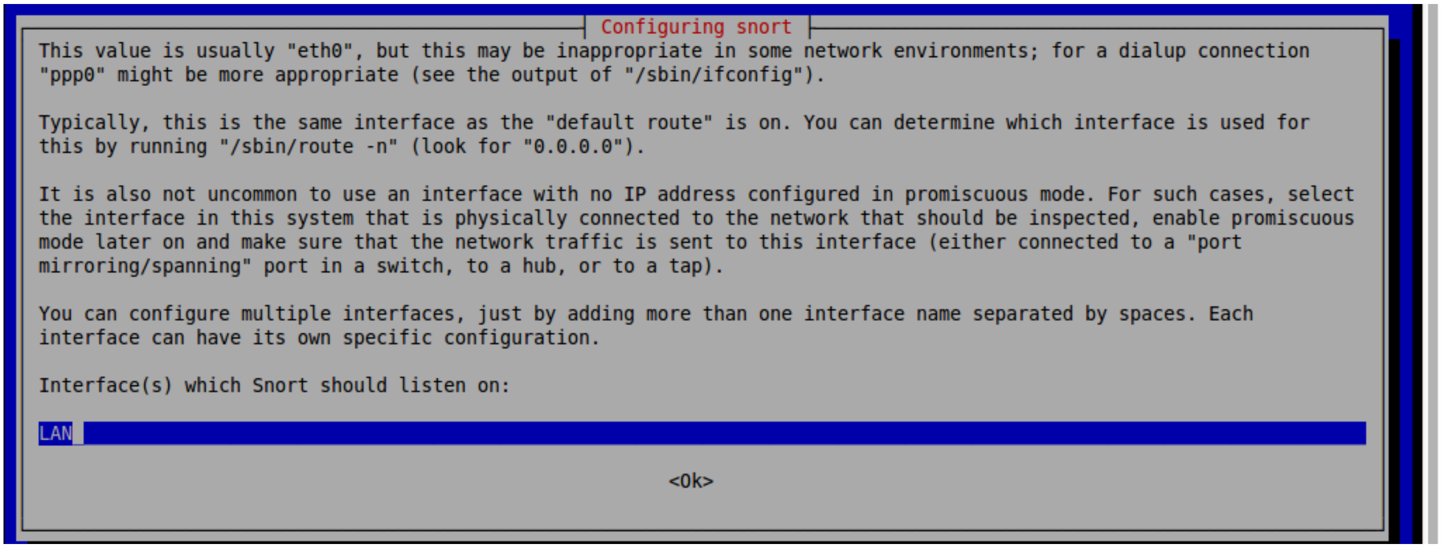


```
root@MSIT:/home/inf053c/Downloads/daq-2.0.6# dpkg -i daq_2.0.6-1_i386.deb
(Reading database ... 140926 files and directories currently installed.)
Preparing to unpack daq_2.0.6-1_i386.deb ...
Unpacking daq (2.0.6-1) over (2.0.6-1) ...
Setting up daq (2.0.6-1) ...
root@MSIT:/home/inf053c/Downloads/daq-2.0.6#
```

4. Install Snort.

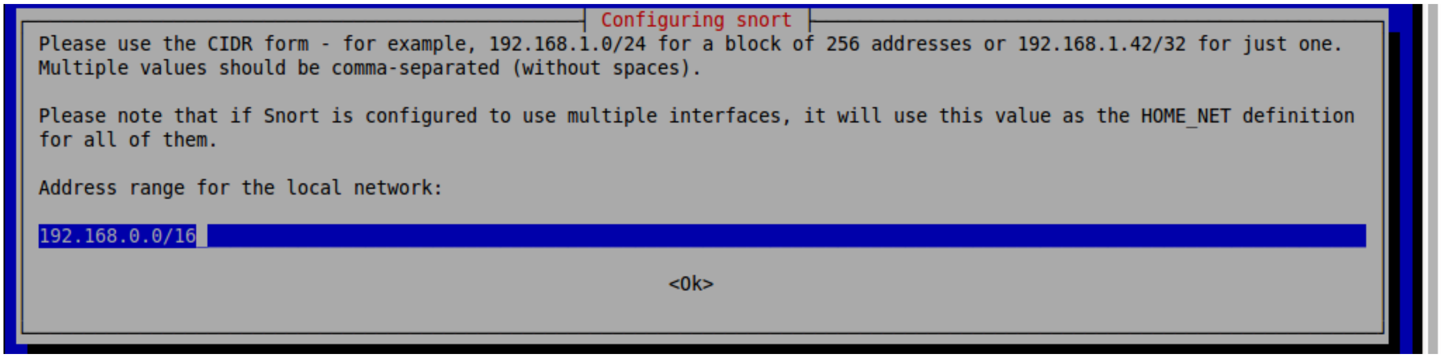
a. `$sudo apt-get install snort.`

b. Select the interface for Snort to listen



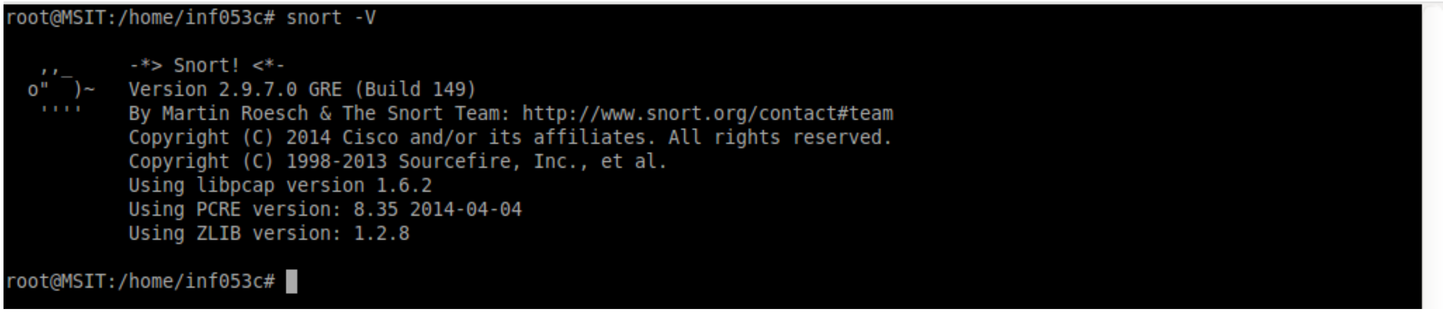
```
Configuring snort
This value is usually "eth0", but this may be inappropriate in some network environments; for a dialup connection
"ppp0" might be more appropriate (see the output of "/sbin/ifconfig").

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:

LAN

                                              <Ok>
```

c. Select the address range



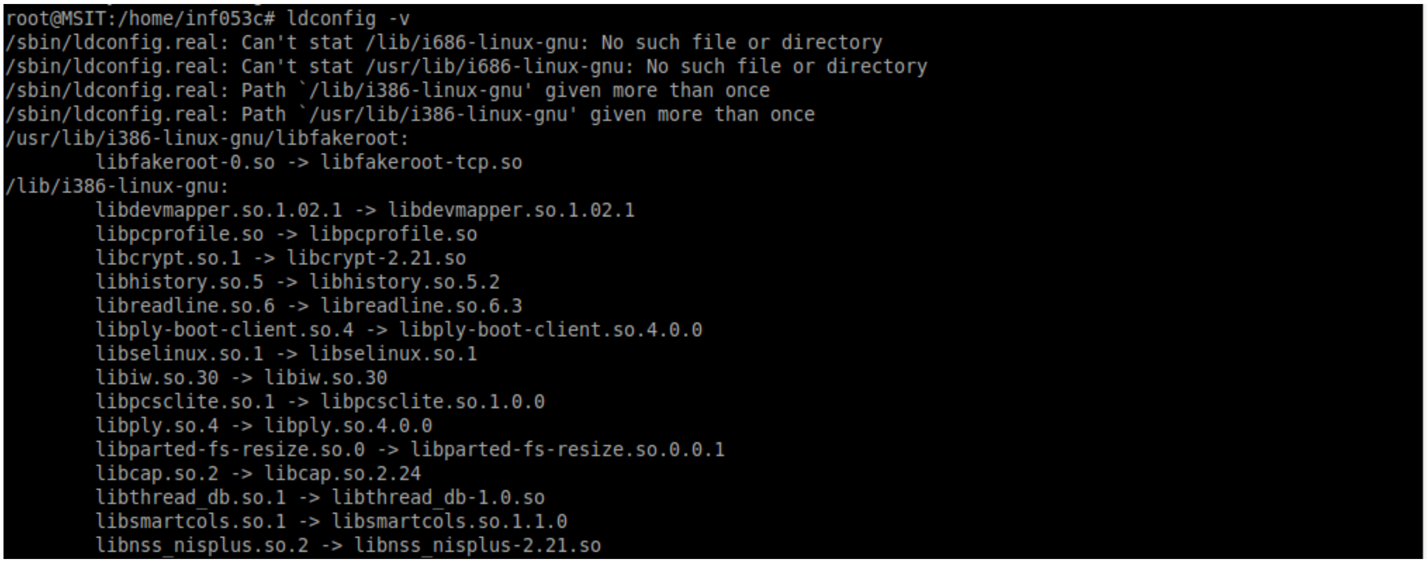
```
Configuring snort
Please use the CIDR form - for example, 192.168.1.0/24 for a block of 256 addresses or 192.168.1.42/32 for just one.
Multiple values should be comma-separated (without spaces).

Please note that if Snort is configured to use multiple interfaces, it will use this value as the HOME_NET definition
for all of them.

Address range for the local network:

192.168.0.0/16

                                              <Ok>
```

d. Verify that snort is installed properly.



```
root@MSIT:/home/inf053c# snort -V

   ,,_     -*> Snort! <*-
  o"  )~   Version 2.9.7.0 GRE (Build 149)
   ''''    By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
           Copyright (C) 2014 Cisco and/or its affiliates. All rights reserved.
           Copyright (C) 1998-2013 Sourcefire, Inc., et al.
           Using libpcap version 1.6.2
           Using PCRE version: 8.35 2014-04-04
           Using ZLIB version: 1.2.8

root@MSIT:/home/inf053c# 
```

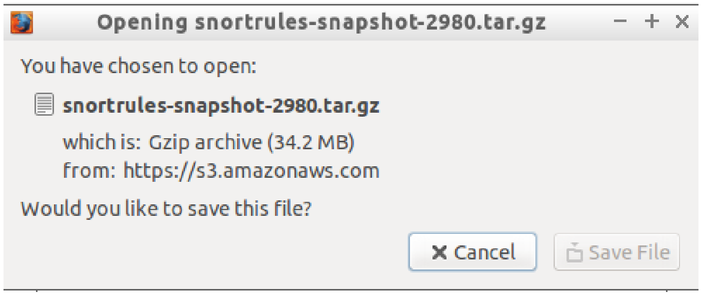
5. Run the `ldconfig` command, so that dynamic linker runtime bindings for `libdnet` and `DAQ` libraries are properly set up.



```
root@MSIT:/home/inf053c# ldconfig -v
/sbin/ldconfig.real: Can't stat /lib/i686-linux-gnu: No such file or directory
/sbin/ldconfig.real: Can't stat /usr/lib/i686-linux-gnu: No such file or directory
/sbin/ldconfig.real: Path `/lib/i386-linux-gnu' given more than once
/sbin/ldconfig.real: Path `/usr/lib/i386-linux-gnu' given more than once
/usr/lib/i386-linux-gnu/libfakeroot:
        libfakeroot-0.so -> libfakeroot-tcp.so
/lib/i386-linux-gnu:
        libdevmapper.so.1.02.1 -> libdevmapper.so.1.02.1
        libpcprofile.so -> libpcprofile.so
        libcrypt.so.1 -> libcrypt-2.21.so
        libhistory.so.5 -> libhistory.so.5.2
        libreadline.so.6 -> libreadline.so.6.3
        libply-boot-client.so.4 -> libply-boot-client.so.4.0.0
        libselinux.so.1 -> libselinux.so.1
        libiw.so.30 -> libiw.so.30
        libpcsclite.so.1 -> libpcsclite.so.1.0.0
        libply.so.4 -> libply.so.4.0.0
        libparted-fs-resize.so.0 -> libparted-fs-resize.so.0.0.1
        libcap.so.2 -> libcap.so.2.24
        libthread_db.so.1 -> libthread_db-1.0.so
        libsmartcols.so.1 -> libsmartcols.so.1.1.0
        libnss_nisplus.so.2 -> libnss_nisplus-2.21.so
```

6. Configure the Snort Rules.

a. Download Snort rules by signing in.



You have chosen to open:

snortrules-snapshot-2980.tar.gz

which is: Gzip archive (34.2 MB)

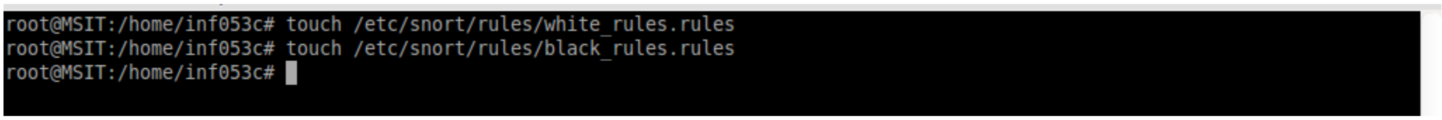
from: https://s3.amazonaws.com

Would you like to save this file?

b. Unpack the Snort rules to `/etc/snort`

```
$ sudo tar xvfz snortrules-snapshot-2980.tar.gz -C /etc/snort
```

c. Create white_list.rules file and a black_list.rules

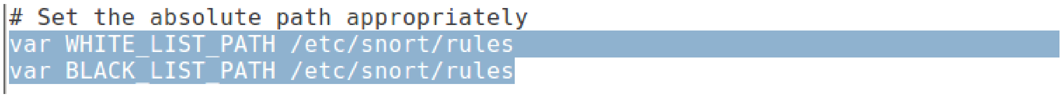


```
root@MSIT:/home/inf053c# touch /etc/snort/rules/white_rules.rules
root@MSIT:/home/inf053c# touch /etc/snort/rules/black_rules.rules
root@MSIT:/home/inf053c# 
```

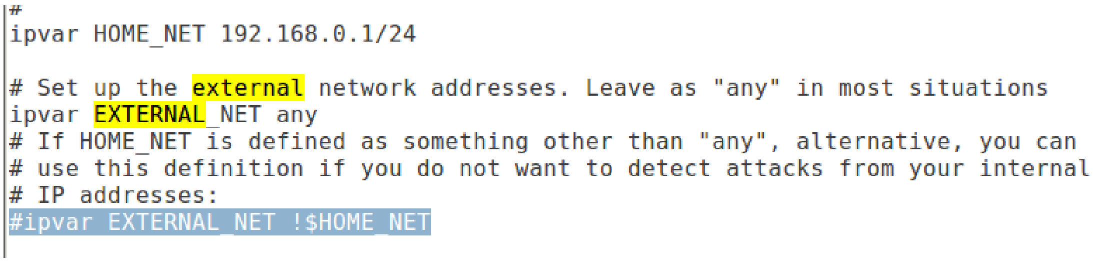
d. Change ownership of `/etc/snort/`:

```
$ sudo chown -R snort:snort /etc/snort/*
```

e. Edit the default Snort configuration file `/etc/snort/snort.conf`



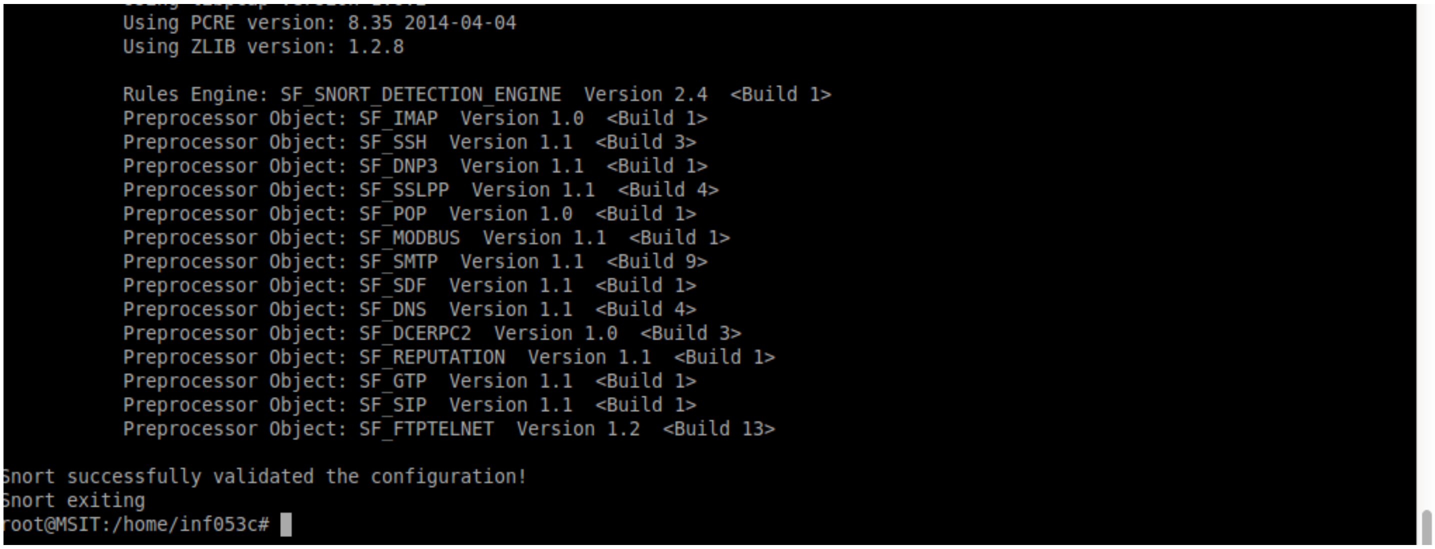
```
# Set the absolute path appropriately
var WHITE_LIST_PATH /etc/snort/rules
var BLACK_LIST_PATH /etc/snort/rules
```



```
#
ipvar HOME_NET 192.168.0.1/24

# 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
```

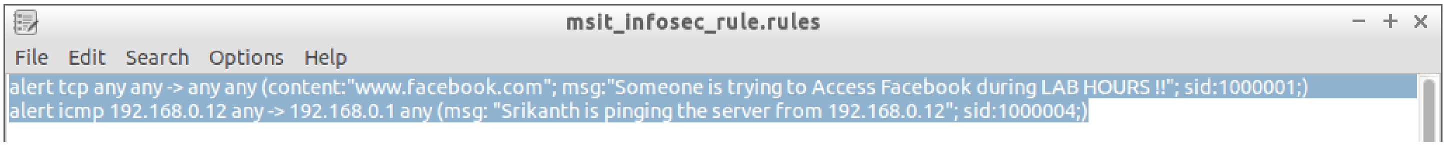
f. Test our Snort configuration by running it in self-test mode.

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



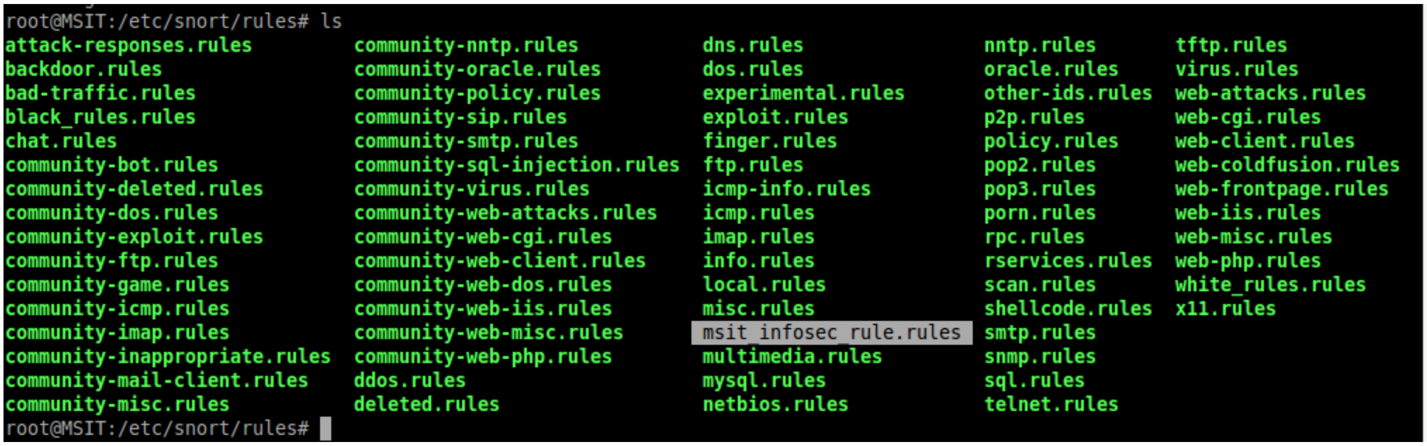
```
           Using PCRE version: 8.35 2014-04-04
           Using ZLIB version: 1.2.8

           Rules Engine: SF_SNORT_DETECTION_ENGINE  Version 2.4  <Build 1>
           Preprocessor Object: SF_IMAP  Version 1.0  <Build 1>
           Preprocessor Object: SF_SSH  Version 1.1  <Build 3>
           Preprocessor Object: SF_DNP3  Version 1.1  <Build 1>
           Preprocessor Object: SF_SSLPP  Version 1.1  <Build 4>
           Preprocessor Object: SF_POP  Version 1.0  <Build 1>
           Preprocessor Object: SF_MODBUS  Version 1.1  <Build 1>
           Preprocessor Object: SF_SMTP  Version 1.1  <Build 9>
           Preprocessor Object: SF_SDF  Version 1.1  <Build 1>
           Preprocessor Object: SF_DNS  Version 1.1  <Build 4>
           Preprocessor Object: SF_DCERPC2  Version 1.0  <Build 3>
           Preprocessor Object: SF_REPUTATION  Version 1.1  <Build 1>
           Preprocessor Object: SF_GTP  Version 1.1  <Build 1>
           Preprocessor Object: SF_SIP  Version 1.1  <Build 1>
           Preprocessor Object: SF_FTPTELNET  Version 1.2  <Build 13>

Snort successfully validated the configuration!
Snort exiting
root@MSIT:/home/inf053c# 
```

7. Create Custom Snort Rules.
   a. Create a custom rule file `/etc/snort/rules/msit_is_rule.rules`.



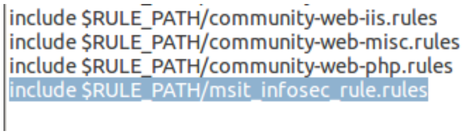
```
alert tcp any any -> any any (content:"www.facebook.com"; msg:"Someone is trying to Access Facebook during LAB HOURS !!"; sid:1000001;)
alert icmp 192.168.0.12 any -> 192.168.0.1 any (msg: "Srikanth is pinging the server from 192.168.0.12"; sid:1000004;)
```

   b. Verify that the rule has been created.



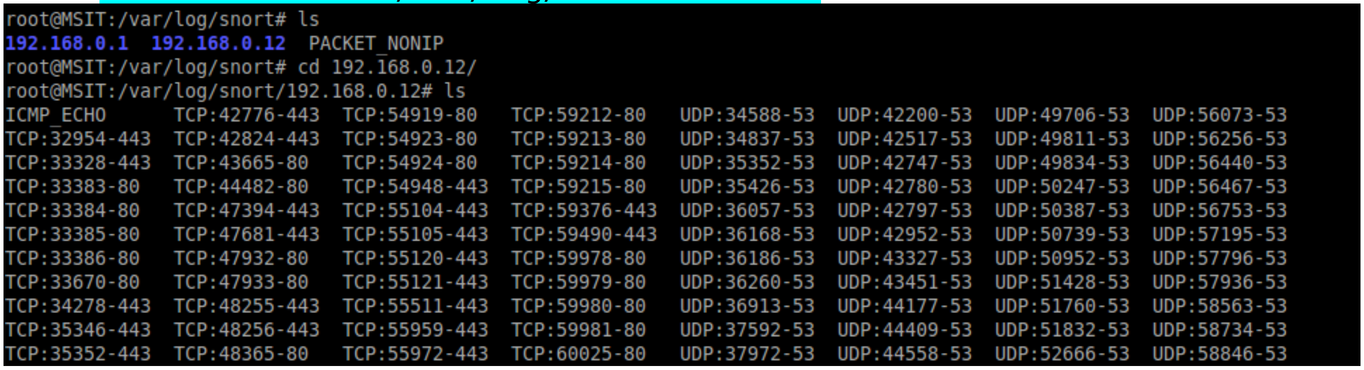
```
root@MSIT:/etc/snort/rules# ls
attack-responses.rules         community-nntp.rules           dns.rules                nntp.rules       tftp.rules
backdoor.rules                 community-oracle.rules         dos.rules                oracle.rules     virus.rules
bad-traffic.rules              community-policy.rules         experimental.rules       other-ids.rules  web-attacks.rules
black_rules.rules              community-sip.rules            exploit.rules            p2p.rules        web-cgi.rules
chat.rules                     community-smtp.rules           finger.rules             policy.rules     web-client.rules
community-bot.rules            community-sql-injection.rules  ftp.rules                pop2.rules       web-coldfusion.rules
community-deleted.rules        community-virus.rules          icmp-info.rules          pop3.rules       web-frontpage.rules
community-dos.rules            community-web-attacks.rules    icmp.rules               porn.rules       web-iis.rules
community-exploit.rules        community-web-cgi.rules        imap.rules               rpc.rules        web-misc.rules
community-ftp.rules            community-web-client.rules     info.rules               rservices.rules  web-php.rules
community-game.rules           community-web-dos.rules        local.rules              scan.rules       white_rules.rules
community-icmp.rules           community-web-iis.rules        misc.rules               shellcode.rules  x11.rules
community-imap.rules           community-web-misc.rules       msit_infosec_rule.rules  smtp.rules
community-inappropriate.rules  community-web-php.rules        multimedia.rules         snmp.rules
community-mail-client.rules    ddos.rules                     mysql.rules              sql.rules
community-misc.rules           deleted.rules                  netbios.rules            telnet.rules
root@MSIT:/etc/snort/rules#
```

   c. Edit the `/etc/snort/snort.conf` file to make sure that the created rule (`msit_is_rule.rules`) is included in it.



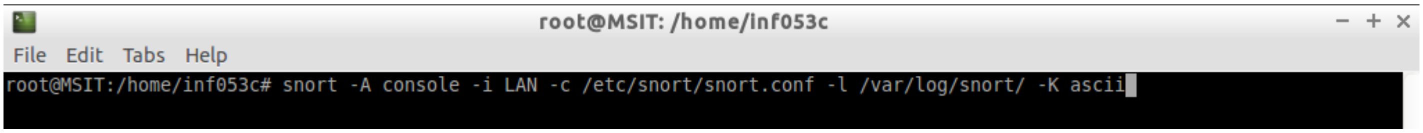
```
include $RULE_PATH/community-web-iis.rules
include $RULE_PATH/community-web-misc.rules
include $RULE_PATH/community-web-php.rules
include $RULE_PATH/msit_infosec_rule.rules
```

8. Run Snort.
   a. Result of running Snort in Packet Logger Mode:
      `$ snort -vde -l /var/log/snort -K ascii`



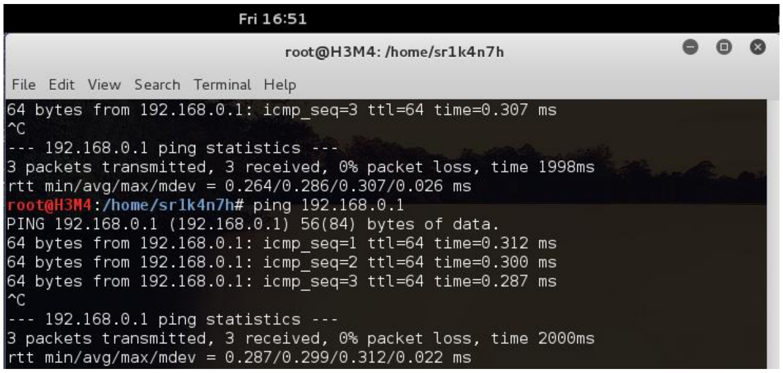
```
root@MSIT:/var/log/snort# ls
192.168.0.1  192.168.0.12  PACKET_NONIP
root@MSIT:/var/log/snort# cd 192.168.0.12/
root@MSIT:/var/log/snort/192.168.0.12# ls
ICMP_ECHO      TCP:42776-443  TCP:54919-80   TCP:59212-80   UDP:34588-53  UDP:42200-53  UDP:49706-53  UDP:56073-53
TCP:32954-443  TCP:42824-443  TCP:54923-80   TCP:59213-80   UDP:34837-53  UDP:42517-53  UDP:49811-53  UDP:56256-53
TCP:33328-443  TCP:43665-80   TCP:54924-80   TCP:59214-80   UDP:35352-53  UDP:42747-53  UDP:49834-53  UDP:56440-53
TCP:33383-80   TCP:44482-80   TCP:54948-443  TCP:59215-80   UDP:35426-53  UDP:42780-53  UDP:50247-53  UDP:56467-53
TCP:33384-80   TCP:47394-443  TCP:55104-443  TCP:59376-443  UDP:36057-53  UDP:42797-53  UDP:50387-53  UDP:56753-53
TCP:33385-80   TCP:47681-443  TCP:55105-443  TCP:59490-443  UDP:36168-53  UDP:42952-53  UDP:50739-53  UDP:57195-53
TCP:33386-80   TCP:47932-80   TCP:55120-443  TCP:59978-80   UDP:36186-53  UDP:43327-53  UDP:50952-53  UDP:57796-53
TCP:33670-80   TCP:47933-80   TCP:55121-443  TCP:59979-80   UDP:36260-53  UDP:43451-53  UDP:51428-53  UDP:57936-53
TCP:34278-443  TCP:48255-443  TCP:55511-443  TCP:59980-80   UDP:36913-53  UDP:44177-53  UDP:51760-53  UDP:58563-53
TCP:35346-443  TCP:48256-443  TCP:55959-443  TCP:59981-80   UDP:37592-53  UDP:44409-53  UDP:51832-53  UDP:58734-53
TCP:35352-443  TCP:48365-80   TCP:55972-443  TCP:60025-80   UDP:37972-53  UDP:44558-53  UDP:52666-53  UDP:58846-53
```

b. Result of running Snort with the configuration file.



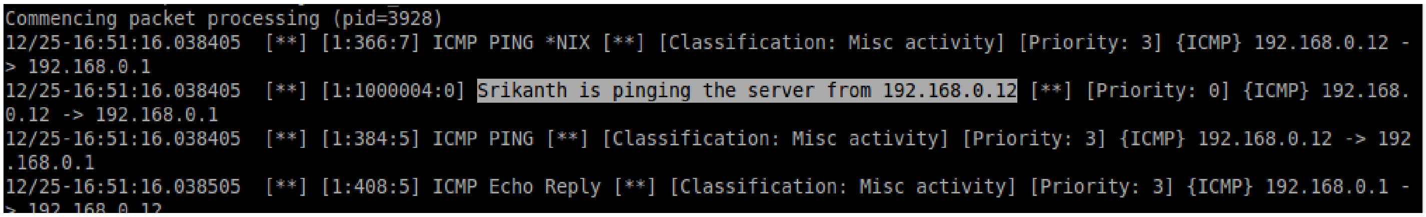
```
root@MSIT:/home/inf053c# snort -A console -i LAN -c /etc/snort/snort.conf -l /var/log/snort/ -K ascii
```

Action #1: Ping from 192.168.0.12. Time Stamp: 25-Dec-2015 16:51:16.038405


Fri 16:51
root@H3M4: /home/sr1k4n7h
File Edit View Search Terminal Help

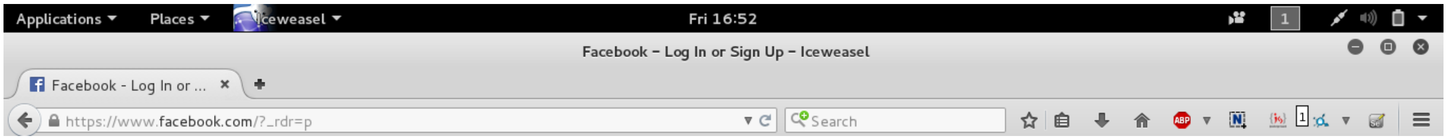
```
64 bytes from 192.168.0.1: icmp_seq=3 ttl=64 time=0.307 ms
^C
--- 192.168.0.1 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 1998ms
rtt min/avg/max/mdev = 0.264/0.286/0.307/0.026 ms
root@H3M4:/home/sr1k4n7h# ping 192.168.0.1
PING 192.168.0.1 (192.168.0.1) 56(84) bytes of data.
64 bytes from 192.168.0.1: icmp_seq=1 ttl=64 time=0.312 ms
64 bytes from 192.168.0.1: icmp_seq=2 ttl=64 time=0.300 ms
64 bytes from 192.168.0.1: icmp_seq=3 ttl=64 time=0.287 ms
^C
--- 192.168.0.1 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2000ms
rtt min/avg/max/mdev = 0.287/0.299/0.312/0.022 ms
```

Result: Alert Message on Snort Console.

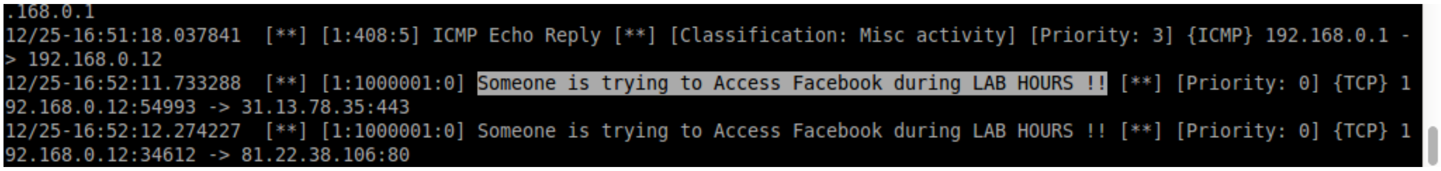


```
Commencing packet processing (pid=3928)
12/25-16:51:16.038405  [**] [1:366:7] ICMP PING *NIX [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.0.12 -
> 192.168.0.1
12/25-16:51:16.038405  [**] [1:1000004:0] Srikanth is pinging the server from 192.168.0.12 [**] [Priority: 0] {ICMP} 192.168.
0.12 -> 192.168.0.1
12/25-16:51:16.038405  [**] [1:384:5] ICMP PING [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.0.12 -> 192
.168.0.1
12/25-16:51:16.038505  [**] [1:408:5] ICMP Echo Reply [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.0.1 -
> 192.168.0.12
```

Action #2: Accessing Facebook. Time Stamp: 25-Dec-2015 16:52:11.733288


Applications
Places
Iceweasel
Fri 16:52
1
Facebook – Log In or Sign Up – Iceweasel
Facebook - Log In or ...
https://www.facebook.com/?_rdr=p
Search
ABP

Result: Alert Message on Snort Console.



```
.168.0.1
12/25-16:51:18.037841  [**] [1:408:5] ICMP Echo Reply [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.0.1 -
> 192.168.0.12
12/25-16:52:11.733288  [**] [1:1000001:0] Someone is trying to Access Facebook during LAB HOURS !! [**] [Priority: 0] {TCP} 1
92.168.0.12:54993 -> 31.13.78.35:443
12/25-16:52:12.274227  [**] [1:1000001:0] Someone is trying to Access Facebook during LAB HOURS !! [**] [Priority: 0] {TCP} 1
92.168.0.12:34612 -> 81.22.38.106:80
```