**Practical – 5**

**Aim:** BASIC configuration of Intrusion Detection System: Snort.

# What is Snort..?

* Snort: A Network Based Intrusion Detection System(IDS).
* It is an open source network-based intrusion detection system (NIDS). That can analyses the real-time traffic and can log packets on Internet Protocol (IP) networks. Snort can perform protocol analysis, content searching, and content matching. It also can be used to detect probes or attacks, including, but not limited to, operating system fingerprinting attempts, common gateway interface, buffer overflows, server message block probes, and stealth port scans.
* There are three modes in which snort can be configured:
  1. Sniffer
  2. Packet logger
  3. Network intrusion detection.
* In sniffer mode, It reads the network packets and display them on the console.
* In packet logger mode, the program will log packets to the disk.
* In intrusion detection mode, the program will monitor network traffic and analyze it against a rule set defined by the user.
* The program will then perform a specific action based on what has been identified.
* NSS Group, a European network security testing organization, tested Snort along with intrusion detection system (IDS) products from 15 major vendors including Cisco, Computer Associates, and Symantec. According to NSS, Snort, which was the sole open source freeware product tested, clearly out-performed the proprietary products.

**Snort Installation and BASIC configuration (LINUX)**

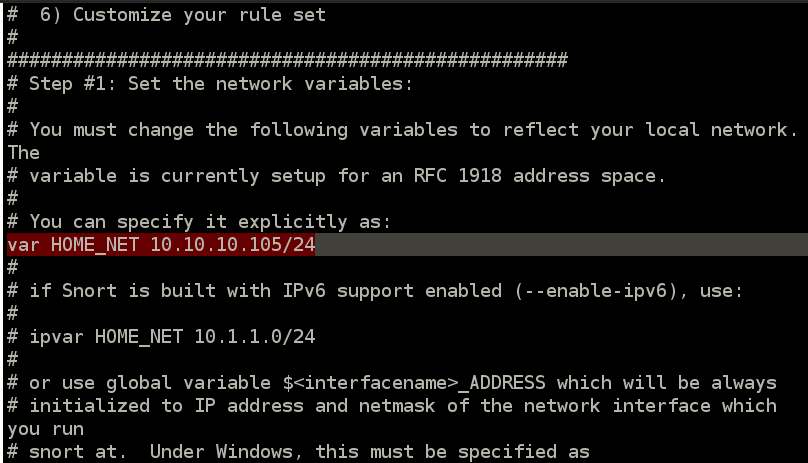
**Step 1:** The following command will download and install snort on our machine.

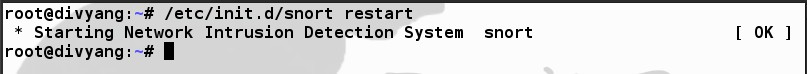
# sudo apt-get install snort

**Step 2:** Now edit the configuration file named snort.conf located in /etc/snort directory using vim or any other text editor and change

var HOME\_NET any to var HOME\_NET <target ip/nw add>

var EXTERNAL\_NET any to var EXTERNAL\_NET <attacker ip address>



**Step 3:** Save the file and restart snort service using /etc/init.d/snort restart command on terminal.

**Step 4:** Now open terninal and type the command below

snort -q -A console -i eth0 -c /etc/snort/snort.conf

Where:

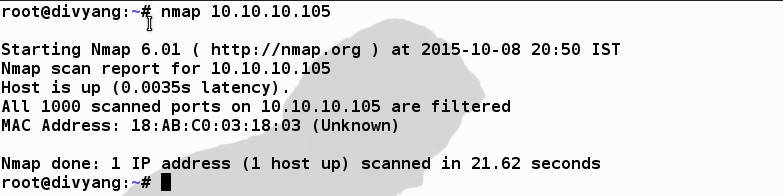
-q is for quiet:- not to show banner and status report

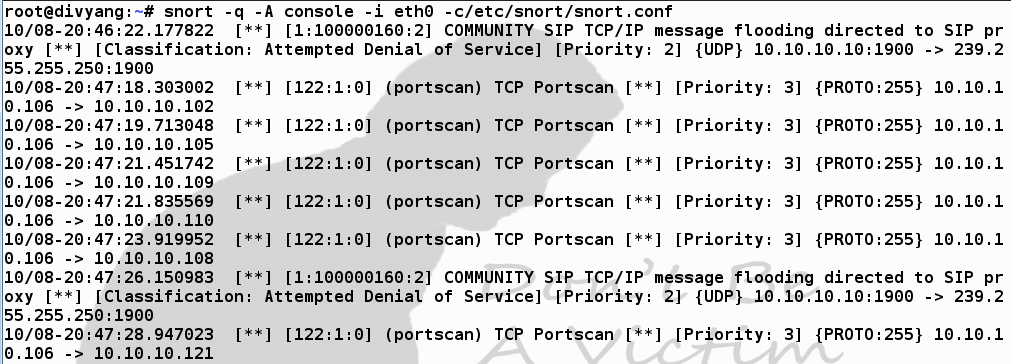
-A is to set alert mode in this case, it is console

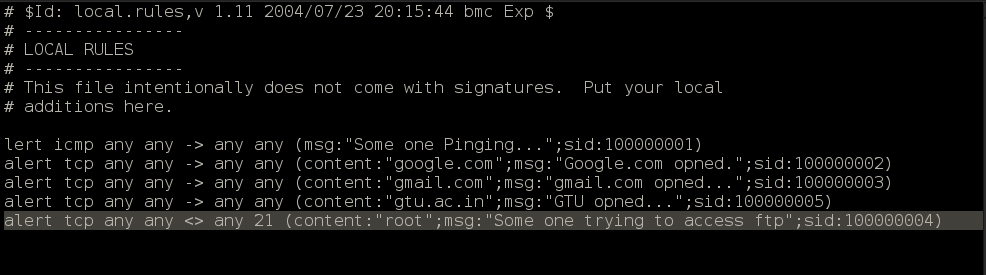
-i is to specify interface and

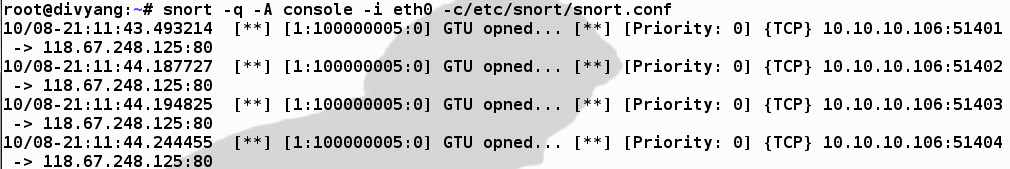
-c is to tell snort the location of configuration file

When we are trying to run the above command we found some errors as show in figure so we have to remove ! (exclamation mark) from the given line number.

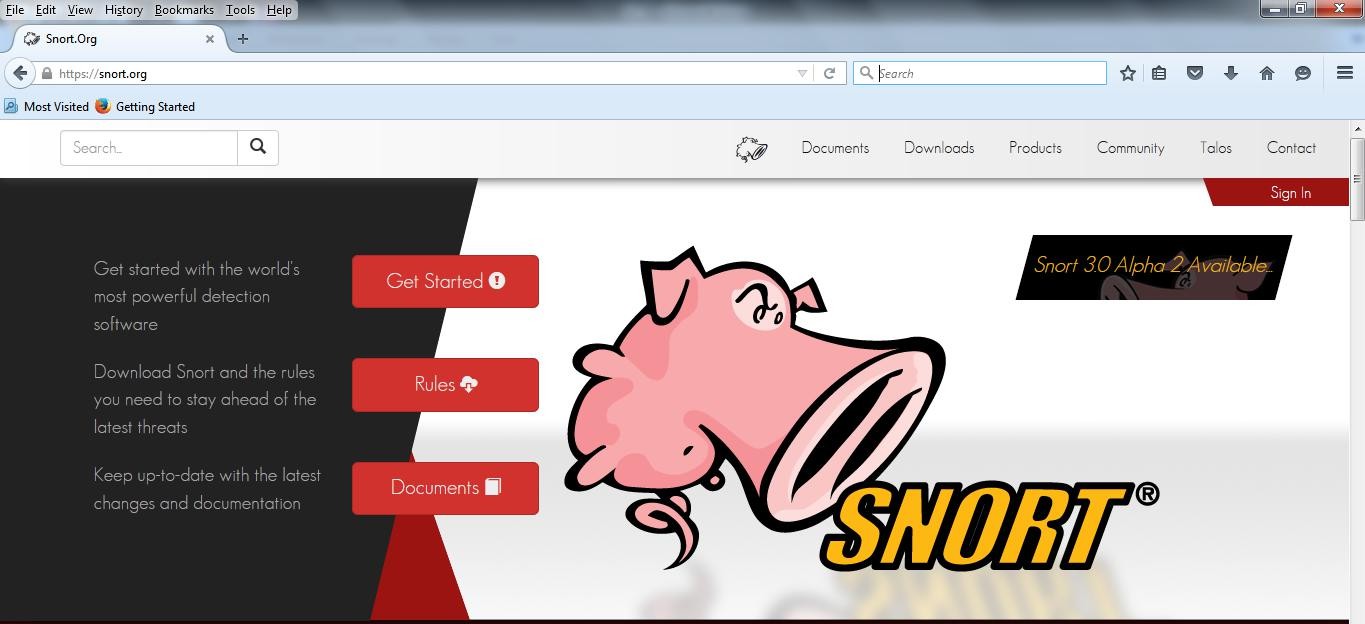
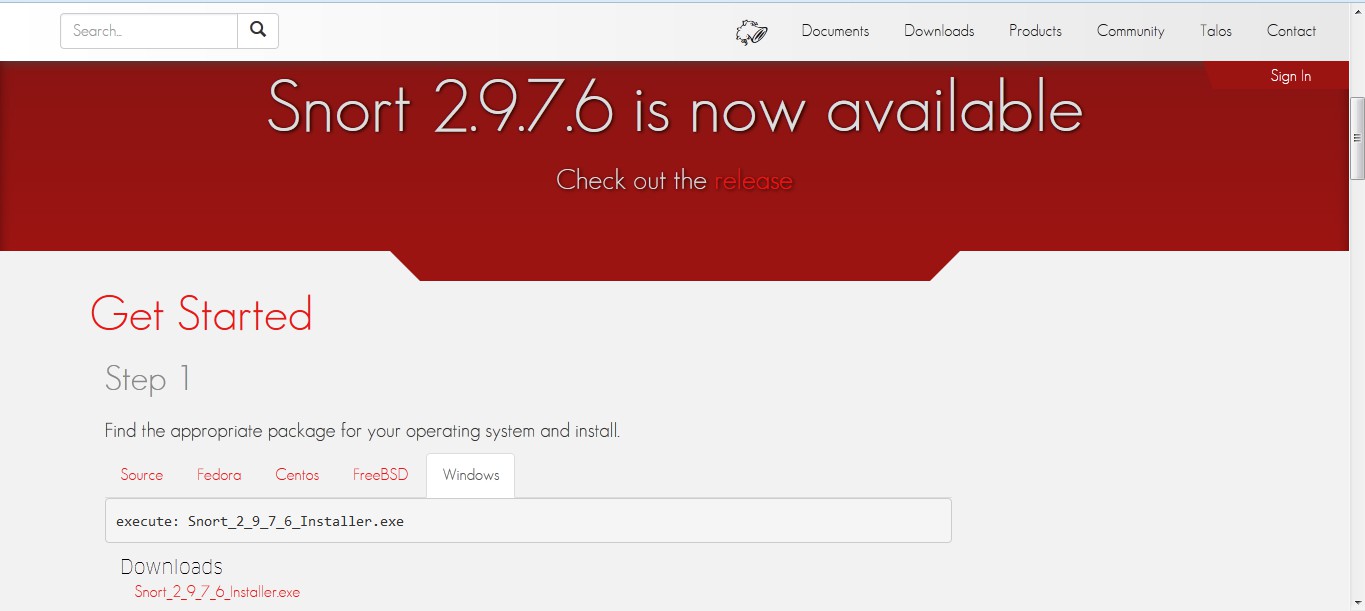
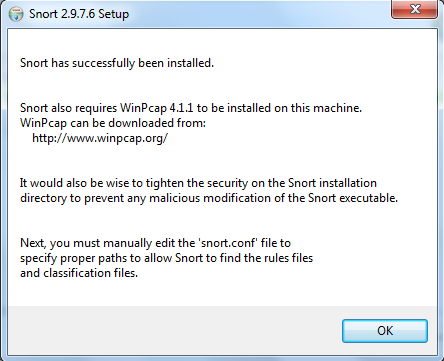
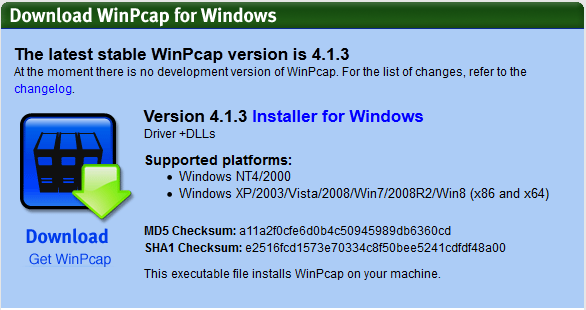
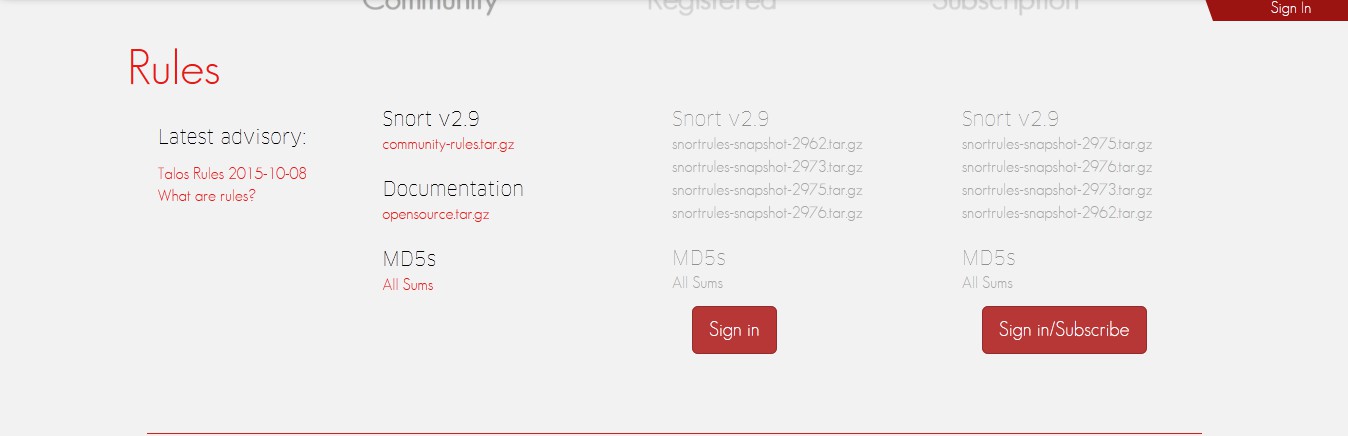
**Step 5:** After removing all error we can show the log which will be generated by the snort -q -A console -i eth0 -c /etc/snort/snort.conf command. From another machine someone try to do nmap scan.

The Following log generated in our system.

We can also add our own rule in the **local.rules (** /etc/snort/rules/local.rules ) file as shown in snapshot.

After applying rules and running snort -q -A console -i eth0 -c /etc/snort/snort.conf command we found log as below.

# Snort Installation and BASIC configuration (Windows)

* First of all, we need snort.exe setup file for windows and a tool known as winpcap.
* Goto: snort.org
* Scroll Down the page and we found windows option as shown in image from there we have to download file (Snort\_2\_9\_7\_6\_Installer.exe).
* Now run Snort\_2\_9\_7\_6\_Installer.exe file and follow the instruction and install it into the windows machine.
* After completion of setup we found following screen.
* According to previous dialog we have also require WinPcap 4.1.1/4.1.3 to be installed.
* If wire shark and similar kind of tools is already available then no need to install WinPcap otherwise we have to open [http://www.winpcap.org/.](http://www.winpcap.org/) and click on installer on windows, save it and install.
* We have to download the rules from snort.org
* Community is freely available and but for the registered rules signup is required.
* Extract all the rules (in rules folder) in c:\snort\rules and preprpc\_rules(folder) in to c:\snort\preproc\_rules
* (same rules is available in preproc\_rules but we have to replace the files. And also same for the etc (folder) rules.

**Steps:** Go to c:\snort\etc and right click on snort file -> open with notepad++ (here you need to change something in configuration) Follow the steps.

**Step1:** go to step1 (line 41): Set the network variables

# Setup the network addresses you are protecting

1. Set the your own pc ip address like ipvar HOME\_NET 10.10.13.51/8

# Set up the external network addresses. Leave as "any" in most situations Instead of any you have to change as ipvar EXTERNAL\_NET !$HOME\_NET ! – consider as NOT

1. Set the path according to rules folder available in your computer (line 104 to 110)

var RULE\_PATH c:\Snort\rules (Change here)

Put # before the # var SO\_RULE\_PATH ../so\_rules

var PREPROC\_RULE\_PATH c:\Snort\preproc\_rules (Change here)

1. # If you are using reputation preprocessor set these var WHITE\_LIST\_PATH c:\Snort\rules (Change here) var BLACK\_LIST\_PATH c:\Snort\rules (Change here) **Step2:** **go to**
2. **step 2: Configure the decoder**

Remove # in line 182 and write path

config logdir: c:\Snort\log

## Step 3: go to Step #4: Configure dynamic loaded libraries.

This line

dynamicpreprocessor directory usr/local/lib/snort\_dynamicpreprocessor/ Replace with following line

dynamicpreprocessor directory c:\Snort\lib\snort\_dynamicpreprocessor This line

dynamicengine usr/local/lib/snort\_dynamicengine/libsf\_engine.so Replace with following line

dynamicengine c:\Snort\lib\snort\_dynamicengine\sf\_engine.dll Place # before this line dynamicdetection directory

/usr/local/lib/snort\_dynamicrules

# dynamicdetection directory /usr/local/lib/snort\_dynamicrules

**Step 4**: Step 5: configure Processors

For following lines we have to put # for the disable preprocessor normalize\_ip4

preprocessor normalize\_tcp: block, rsv, pad, urp, req\_urg, req\_pay, req\_urp, ips, ecn stream

preprocessor normalize\_icmp4 preprocessor normalize\_ip6 preprocessor normalize\_icmp6 As

# preprocessor normalize\_ip4

# preprocessor normalize\_tcp: block, rsv, pad, urp, req\_urg, req\_pay, req\_urp, ips, ecn stream

# preprocessor normalize\_icmp4 # preprocessor normalize\_ip6

# preprocessor normalize\_icmp6

Remove # from the following line (line number 413)

preprocessor sfportscan: proto { all } memcap { 10000000 } sense\_level { low }

In reputation preprocessor preprocessor reputation: \ memcap 500, \

priority whitelist, \ nested\_ip inner, \

Change following lines to

whitelist $WHITE\_LIST\_PATH\white.\_list.list, \ blacklist $BLACK\_LIST\_PATH\black\_list.list As

whitelist $WHITE\_LIST\_PATH/white\_list.rules, \ blacklist $BLACK\_LIST\_PATH/black\_list.rules

## Step 5 : Step #7: Customize your rule set # site specific rules From the following rules lines we have to replace / with the \

**(applicable 541 to 648)**

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 #include $RULE\_PATH\file-executable.rules #include $RULE\_PATH\file-flash.rules #include $RULE\_PATH\file-identify.rules #include $RULE\_PATH\file-image.rules #include $RULE\_PATH\file-java.rules #include $RULE\_PATH\file-multimedia.rules #include $RULE\_PATH\file-office.rules #include $RULE\_PATH\file-other.rules #include $RULE\_PATH\file-pdf.rules #include $RULE\_PATH\finger.rules

#include $RULE\_PATH\ftp.rules #include $RULE\_PATH\icmp-info.rules #include $RULE\_PATH\icmp.rules #include $RULE\_PATH\imap.rules

#include $RULE\_PATH\indicator-compromise.rules #include $RULE\_PATH\indicator-obfuscation.rules #include $RULE\_PATH\indicator-scan.rules #include $RULE\_PATH\indicator-shellcode.rules #include $RULE\_PATH\info.rules

#include $RULE\_PATH\malware-backdoor.rules #include $RULE\_PATH\malware-cnc.rules #include $RULE\_PATH\malware-other.rules #include $RULE\_PATH\malware-tools.rules #include $RULE\_PATH\misc.rules

#include $RULE\_PATH\multimedia.rules #include $RULE\_PATH\mysql.rules #include $RULE\_PATH\netbios.rules #include $RULE\_PATH\nntp.rules #include $RULE\_PATH\oracle.rules #include $RULE\_PATH\os-linux.rules #include $RULE\_PATH\os-mobile.rules #include $RULE\_PATH\os-other.rules #include $RULE\_PATH\os-solaris.rules

#include $RULE\_PATH\os-windows.rules #include $RULE\_PATH\other-ids.rules #include $RULE\_PATH\p2p.rules

#include $RULE\_PATH\phishing-spam.rules #include $RULE\_PATH\policy-multimedia.rules #include $RULE\_PATH\policy-other.rules #include $RULE\_PATH\policy.rules

#include $RULE\_PATH\policy-social.rules #include $RULE\_PATH\policy-spam.rules #include $RULE\_PATH\pop2.rules #include $RULE\_PATH\pop3.rules #include $RULE\_PATH\protocol-dns.rules

#include $RULE\_PATH\protocol-finger.rules #include $RULE\_PATH\protocol-ftp.rules #include $RULE\_PATH\protocol-icmp.rules #include $RULE\_PATH\protocol-imap.rules #include $RULE\_PATH\protocol-nntp.rules #include $RULE\_PATH\protocol-other.rules #include $RULE\_PATH\protocol-pop.rules #include $RULE\_PATH\protocol-rpc.rules #include $RULE\_PATH\protocol-scada.rules #include $RULE\_PATH\protocol-services.rules #include $RULE\_PATH\protocol-snmp.rules include $RULE\_PATH\protocol-telnet.rules #include $RULE\_PATH\protocol-tftp.rules #include $RULE\_PATH\protocol-voip.rules #include $RULE\_PATH\pua-adware.rules #include $RULE\_PATH\pua-other.rules #include $RULE\_PATH\pua-p2p.rules #include $RULE\_PATH\pua-toolbars.rules include $RULE\_PATH\rpc.rules

#include $RULE\_PATH\rservices.rules #include $RULE\_PATH\scada.rules #include $RULE\_PATH\scan.rules

include $RULE\_PATH\server-apache.rules include $RULE\_PATH\server-iis.rules #include $RULE\_PATH\server-mail.rules #include $RULE\_PATH\server-mssql.rules #include $RULE\_PATH\server-mysql.rules

#include $RULE\_PATH\server-oracle.rules #include $RULE\_PATH\server-other.rules #include $RULE\_PATH\server-samba.rules #include $RULE\_PATH\server-webapp.rules #include $RULE\_PATH\shellcode.rules #include $RULE\_PATH\smtp.rules

#include $RULE\_PATH\snmp.rules

#include $RULE\_PATH\specific-threats.rules #include $RULE\_PATH\spyware-put.rules #include $RULE\_PATH\sql.rules

#include $RULE\_PATH\telnet.rules #include $RULE\_PATH\tftp.rules #include $RULE\_PATH\virus.rules #include $RULE\_PATH\voip.rules #include $RULE\_PATH\web-activex.rules #include $RULE\_PATH\web-attacks.rules #include $RULE\_PATH\web-cgi.rules #include $RULE\_PATH\web-client.rules

#include $RULE\_PATH\web-coldfusion.rules #include $RULE\_PATH\web-frontpage.rules #include $RULE\_PATH\web-iis.rules #include $RULE\_PATH\web-misc.rules #include $RULE\_PATH\web-php.rules #include $RULE\_PATH\x11.rules

# Step 6:

Step #8: Customize your preprocessor and decoder alerts # decoder and preprocessor event rules

Remove # from the following lines

include $PREPROC\_RULE\_PATH\preprocessor.rules include $PREPROC\_RULE\_PATH\decoder.rules include $PREPROC\_RULE\_PATH\sensitive-data.rules

**Step 7:**

Finally Save the configuration File (Snort.conf)

**Step 8:**

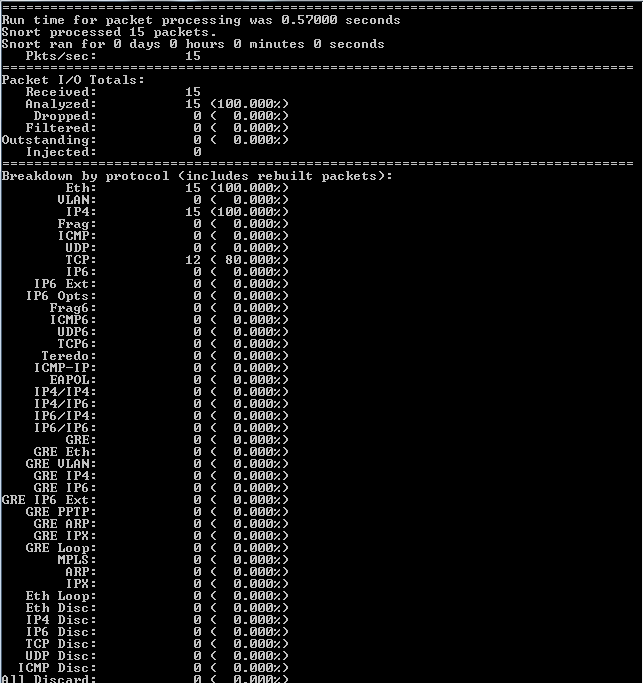
Create file **white\_list.rules** and **black\_list.rules** in **C:\Snort\rules** folder.

**Step 9:**

To start snort in IDS mode, run following command: **snort -c c:\snort\etc\snort.conf -l c:\snort\log -i 2 Step 10:**

Above command will generate log file that will not be readable without using a tool. To read it use following command:

C:\Snort\Bin\> **snort -r ..\log\log-filename**

after Applying above command we found following Output