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>

```
#  6) Customize your rule set
#
##################################################
# Step #1: Set the network variables:
#
# You must change the following variables to reflect your local network.
The
# variable is currently setup for an RFC 1918 address space.
#
# You can specify it explicitly as:
var HOME_NET 10.10.10.105/24
#
# if Snort is built with IPv6 support enabled (--enable-ipv6), use:
#
# ipvar HOME_NET 10.1.1.0/24
#
# or use global variable $<interfacename>_ADDRESS which will be always
# initialized to IP address and netmask of the network interface which
you run
# snort at.  Under Windows, this must be specified as
```

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

```
root@divyang:~# /etc/init.d/snort restart
 * Starting Network Intrusion Detection System  snort                    [ OK ]
root@divyang:~#
```

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

```
root@divyang:~# snort -q -A console -i eth0 -c/etc/snort/snort.conf
ERROR: /etc/snort/rules/community-smtp.rules(13) => !any is not allowed
Fatal Error, Quitting..
root@divyang:~#
```

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.

```
root@divyang:~# nmap 10.10.10.105

Starting Nmap 6.01 ( http://nmap.org ) at 2015-10-08 20:50 IST
Nmap scan report for 10.10.10.105
Host is up (0.0035s latency).
All 1000 scanned ports on 10.10.10.105 are filtered
MAC Address: 18:AB:C0:03:18:03 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 21.62 seconds
```

The Following log generated in our system.

```
root@divyang:~# snort -q -A console -i eth0 -c/etc/snort/snort.conf
10/08-20:46:22.177822  [**] [1:100000160:2] COMMUNITY SIP TCP/IP message flooding directed to SIP pr
oxy [**] [Classification: Attempted Denial of Service] [Priority: 2] {UDP} 10.10.10.10:1900 -> 239.2
55.255.250:1900
10/08-20:47:18.303002  [**] [122:1:0] (portscan) TCP Portscan [**] [Priority: 3] {PROTO:255} 10.10.1
0.106 -> 10.10.10.102
10/08-20:47:19.713048  [**] [122:1:0] (portscan) TCP Portscan [**] [Priority: 3] {PROTO:255} 10.10.1
0.106 -> 10.10.10.105
10/08-20:47:21.451742  [**] [122:1:0] (portscan) TCP Portscan [**] [Priority: 3] {PROTO:255} 10.10.1
0.106 -> 10.10.10.109
10/08-20:47:21.835569  [**] [122:1:0] (portscan) TCP Portscan [**] [Priority: 3] {PROTO:255} 10.10.1
0.106 -> 10.10.10.110
10/08-20:47:23.919952  [**] [122:1:0] (portscan) TCP Portscan [**] [Priority: 3] {PROTO:255} 10.10.1
0.106 -> 10.10.10.108
10/08-20:47:26.150983  [**] [1:100000160:2] COMMUNITY SIP TCP/IP message flooding directed to SIP pr
oxy [**] [Classification: Attempted Denial of Service] [Priority: 2] {UDP} 10.10.10.10:1900 -> 239.2
55.255.250:1900
10/08-20:47:28.947023  [**] [122:1:0] (portscan) TCP Portscan [**] [Priority: 3] {PROTO:255} 10.10.1
0.106 -> 10.10.10.121
```

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

```
# $Id: local.rules,v 1.11 2004/07/23 20:15:44 bmc Exp $
# ----------------
# LOCAL RULES
# ----------------
# This file intentionally does not come with signatures.  Put your local
# additions here.

lert icmp any any -> any any (msg:"Some one Pinging...";sid:100000001)
alert tcp any any -> any any (content:"google.com";msg:"Google.com opned.";sid:100000002)
alert tcp any any -> any any (content:"gmail.com";msg:"gmail.com opned...";sid:100000003)
alert tcp any any -> any any (content:"gtu.ac.in";msg:"GTU opned...";sid:100000005)
alert tcp any any <> any 21 (content:"root";msg:"Some one trying to access ftp";sid:100000004)
```

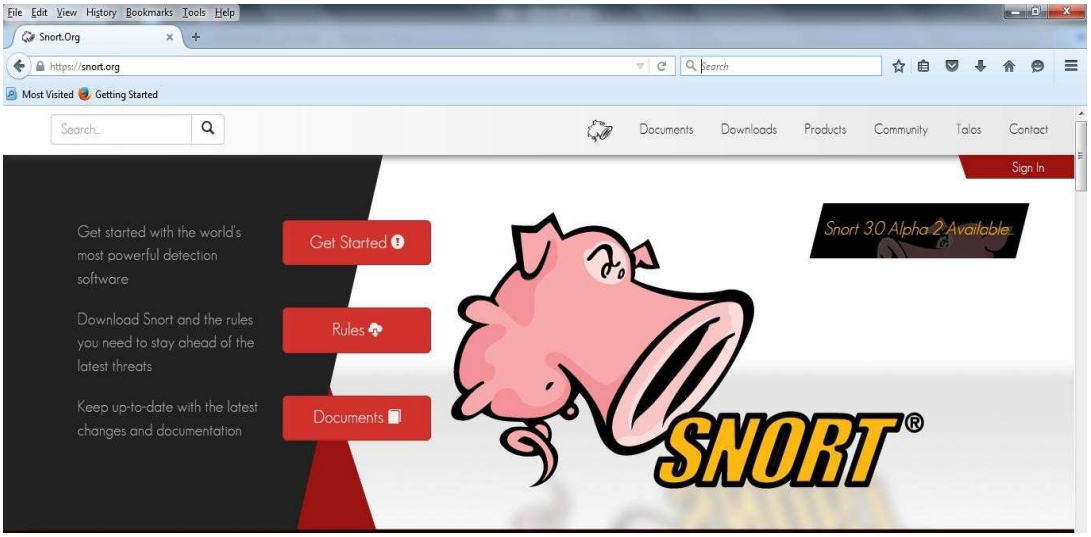
After applying rules and running snort -q -A console -i eth0 -c /etc/snort/snort.conf command we found log as below.

```
root@divyang:~# snort -q -A console -i eth0 -c/etc/snort/snort.conf
10/08-21:11:43.493214  [**] [1:100000005:0] GTU opned... [**] [Priority: 0] {TCP} 10.10.10.106:51401
 -> 118.67.248.125:80
10/08-21:11:44.187727  [**] [1:100000005:0] GTU opned... [**] [Priority: 0] {TCP} 10.10.10.106:51402
 -> 118.67.248.125:80
10/08-21:11:44.194825  [**] [1:100000005:0] GTU opned... [**] [Priority: 0] {TCP} 10.10.10.106:51403
 -> 118.67.248.125:80
10/08-21:11:44.244455  [**] [1:100000005:0] GTU opned... [**] [Priority: 0] {TCP} 10.10.10.106:51404
 -> 118.67.248.125:80
```

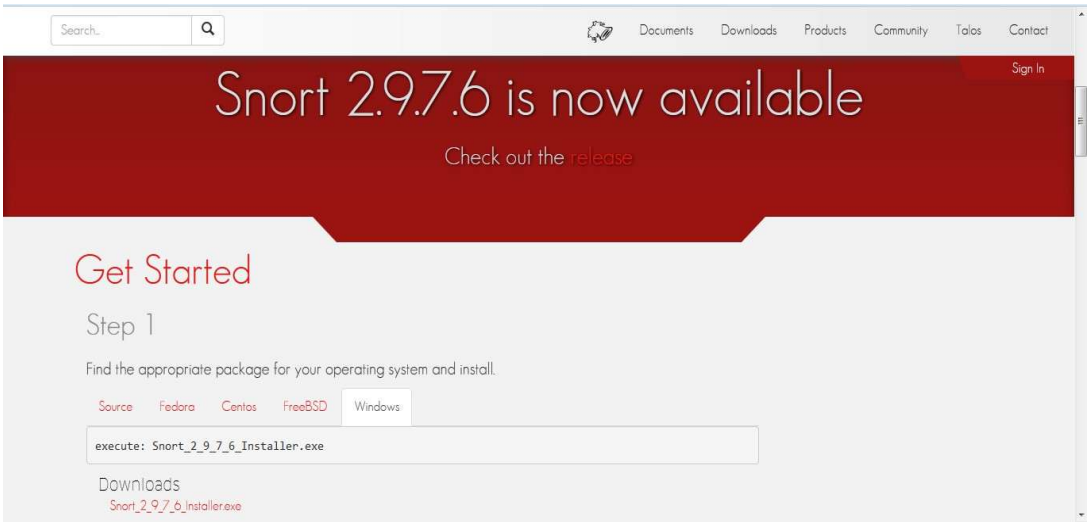
```
root@divyang:~# snort -q -A console -i eth0 -c/etc/snort/snort.conf
10/08-21:12:25.691189  [**] [1:100000005:0] GTU opned... [**] [Priority: 0] {TCP} 10.10.10.106:51401
 -> 118.67.248.125:80
10/08-21:12:49.372432  [**] [1:100000003:0] gmail.com opned... [**] [Priority: 0] {TCP} 10.10.10.106
:51415 -> 173.194.36.117:443
10/08-21:12:49.396362  [**] [1:100000002:0] Google.com opned. [**] [Priority: 0] {TCP} 10.10.10.106:
51416 -> 173.194.36.118:443
10/08-21:12:49.430223  [**] [1:100000002:0] Google.com opned. [**] [Priority: 0] {TCP} 173.194.36.11
8:443 -> 10.10.10.106:51416
```

Snort Installation and BASIC configuration (Windows)

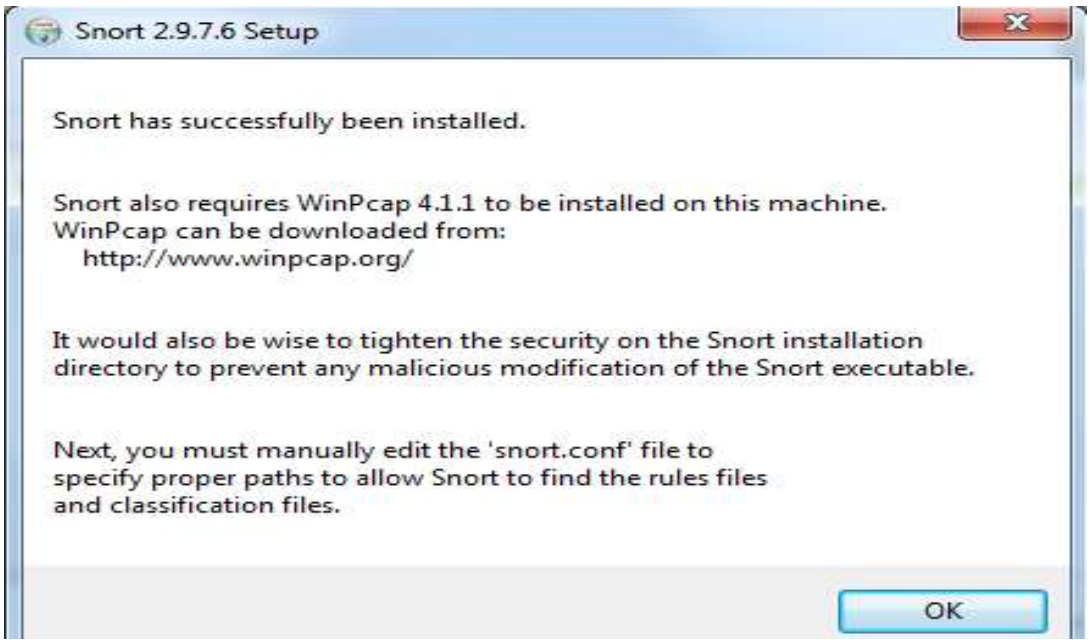
- First of all, we need snort.exe setup file for windows and a tool known as winpcap.
- Goto: snort.org



- 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).

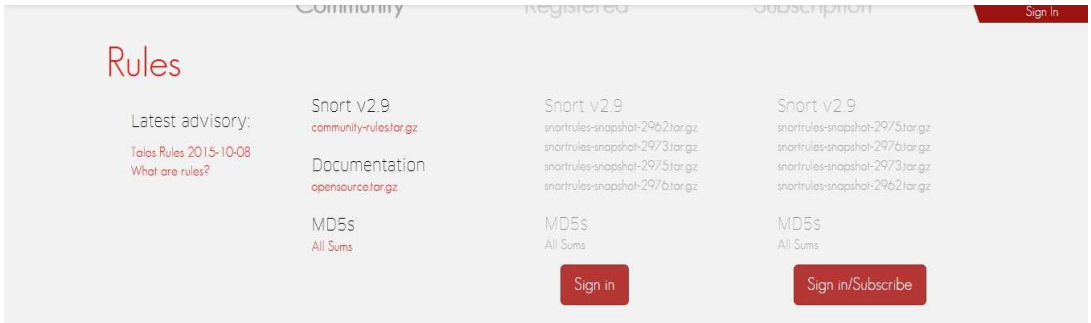


- Now run Snort_2_9_7_6_Installer.exe file and follow the instruction and install it into the windows machine.
- After completion of setup we found following screen.



- 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/. 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
2) 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)

3) # 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**

4) **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

```
C:\Snort\bin>snort -r ..\log\snort.log.1444356202
Running in packet dump mode

        --== Initializing Snort ==--
Initializing Output Plugins!
pcap DAQ configured to read-file.
The DAQ version does not support reload.
Acquiring network traffic from "..\log\snort.log.1444356202".

        --== Initialization Complete ==--

           -*> Snort! <*-
  o"  )~   Version 2.9.7.5-WIN32 GRE (Build 262)
   ''''    By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
           Copyright (C) 2014-2015 Cisco and/or its affiliates. All rights reser
ved.
           Copyright (C) 1998-2013 Sourcefire, Inc., et al.
           Using PCRE version: 8.10 2010-06-25
           Using ZLIB version: 1.2.3

Commencing packet processing (pid=3576)
WARNING: No preprocessors configured for policy 0.
10/09-07:33:29.918059 10.10.10.106:50722 -> 10.10.10.10:80
TCP TTL:128 TOS:0x0 ID:27072 IpLen:20 DgmLen:40 DF
***A**** Seq: 0x3BEC18B0  Ack: 0x2AE1  Win: 0xFA70  TcpLen: 20
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

WARNING: No preprocessors configured for policy 0.
10/09-07:33:29.717461 10.10.10.10:80 -> 10.10.10.106:50722
TCP TTL:64 TOS:0x0 ID:21780 IpLen:20 DgmLen:328 DF
***AP*** Seq: 0x29C1  Ack: 0x3BEC18B0  Win: 0x1770  TcpLen: 20
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

WARNING: No preprocessors configured for policy 0.
10/09-07:34:29.916134 10.10.10.106:50724 -> 10.10.10.10:80
TCP TTL:128 TOS:0x0 ID:27100 IpLen:20 DgmLen:40 DF
***A**** Seq: 0x4A1741E  Ack: 0x4251  Win: 0xFA70  TcpLen: 20
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

WARNING: No preprocessors configured for policy 0.
10/09-07:34:29.714855 10.10.10.10:80 -> 10.10.10.106:50724
TCP TTL:64 TOS:0x0 ID:22116 IpLen:20 DgmLen:328 DF
***AP*** Seq: 0x4131  Ack: 0x4A1741E  Win: 0x1770  TcpLen: 20
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

WARNING: No preprocessors configured for policy 0.
10/09-07:35:18.636079 10.10.10.106:50726 -> 10.10.10.10:80
TCP TTL:128 TOS:0x0 ID:27122 IpLen:20 DgmLen:40 DF
***A**** Seq: 0xE88F6C57  Ack: 0x5559  Win: 0xFA70  TcpLen: 20
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

WARNING: No preprocessors configured for policy 0.
10/09-07:35:18.435150 10.10.10.10:80 -> 10.10.10.106:50726
TCP TTL:64 TOS:0x0 ID:22393 IpLen:20 DgmLen:328 DF
***AP*** Seq: 0x5439  Ack: 0xE88F6C57  Win: 0x1770  TcpLen: 20
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
```

```
===============================================================================
Run time for packet processing was 0.57000 seconds
Snort processed 15 packets.
Snort ran for 0 days 0 hours 0 minutes 0 seconds
   Pkts/sec:           15
===============================================================================
Packet I/O Totals:
   Received:           15
   Analyzed:           15 (100.000%)
    Dropped:            0 (  0.000%)
   Filtered:            0 (  0.000%)
Outstanding:            0 (  0.000%)
   Injected:            0
===============================================================================
Breakdown by protocol (includes rebuilt packets):
        Eth:           15 (100.000%)
       VLAN:            0 (  0.000%)
        IP4:           15 (100.000%)
       Frag:            0 (  0.000%)
       ICMP:            0 (  0.000%)
        UDP:            0 (  0.000%)
        TCP:           12 ( 80.000%)
        IP6:            0 (  0.000%)
    IP6 Ext:            0 (  0.000%)
   IP6 Opts:            0 (  0.000%)
      Frag6:            0 (  0.000%)
      ICMP6:            0 (  0.000%)
       UDP6:            0 (  0.000%)
       TCP6:            0 (  0.000%)
     Teredo:            0 (  0.000%)
    ICMP-IP:            0 (  0.000%)
      EAPOL:            0 (  0.000%)
    IP4/IP4:            0 (  0.000%)
    IP4/IP6:            0 (  0.000%)
    IP6/IP4:            0 (  0.000%)
    IP6/IP6:            0 (  0.000%)
        GRE:            0 (  0.000%)
    GRE Eth:            0 (  0.000%)
   GRE VLAN:            0 (  0.000%)
    GRE IP4:            0 (  0.000%)
    GRE IP6:            0 (  0.000%)
GRE IP6 Ext:            0 (  0.000%)
   GRE PPTP:            0 (  0.000%)
    GRE ARP:            0 (  0.000%)
    GRE IPX:            0 (  0.000%)
   GRE Loop:            0 (  0.000%)
       MPLS:            0 (  0.000%)
        ARP:            0 (  0.000%)
        IPX:            0 (  0.000%)
   Eth Loop:            0 (  0.000%)
   Eth Disc:            0 (  0.000%)
   IP4 Disc:            0 (  0.000%)
   IP6 Disc:            0 (  0.000%)
   TCP Disc:            0 (  0.000%)
   UDP Disc:            0 (  0.000%)
  ICMP Disc:            0 (  0.000%)
All Discard:            0 (  0.000%)
```