PARSHVANATH CHARITABLE TRUST'S

A. P. SHAH INSTITUTE OF TECHNOLOGY

Department of Information Technology

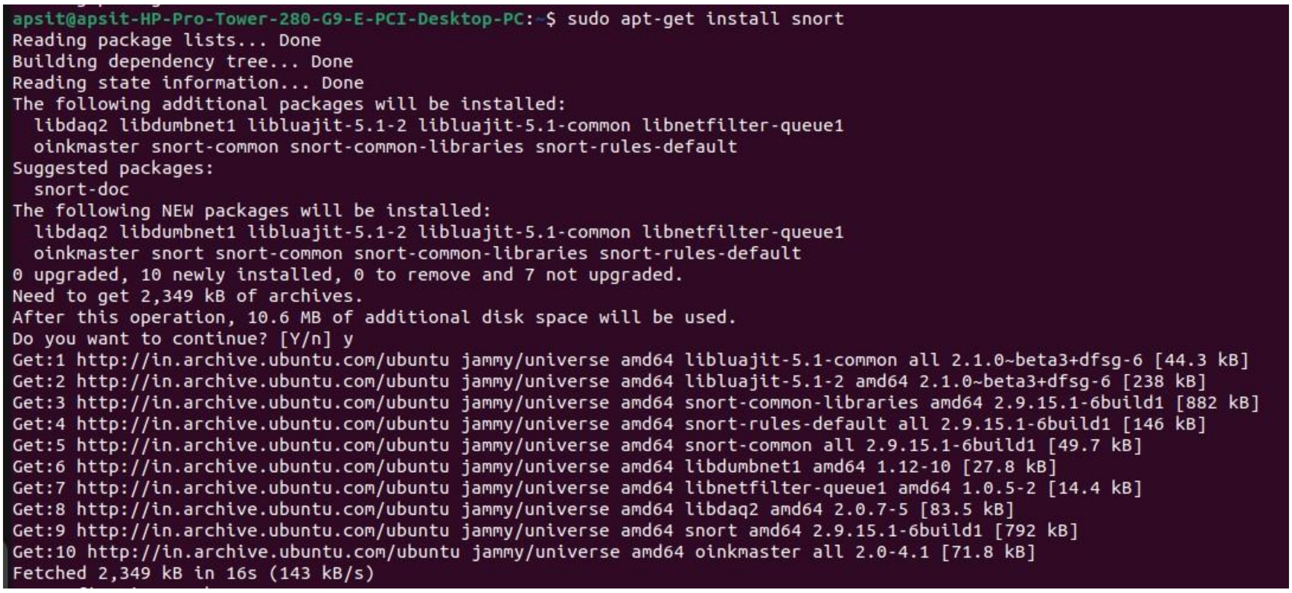
(NBA Accredited)

Semester: V
Academic Year: 2025-26
Class / Branch: TE IT
Subject: SECURITY LAB
Name of Instructor: Prof. Vishal Badgujar

Name of Student: Suyash Y Mane
Student ID: 24204008

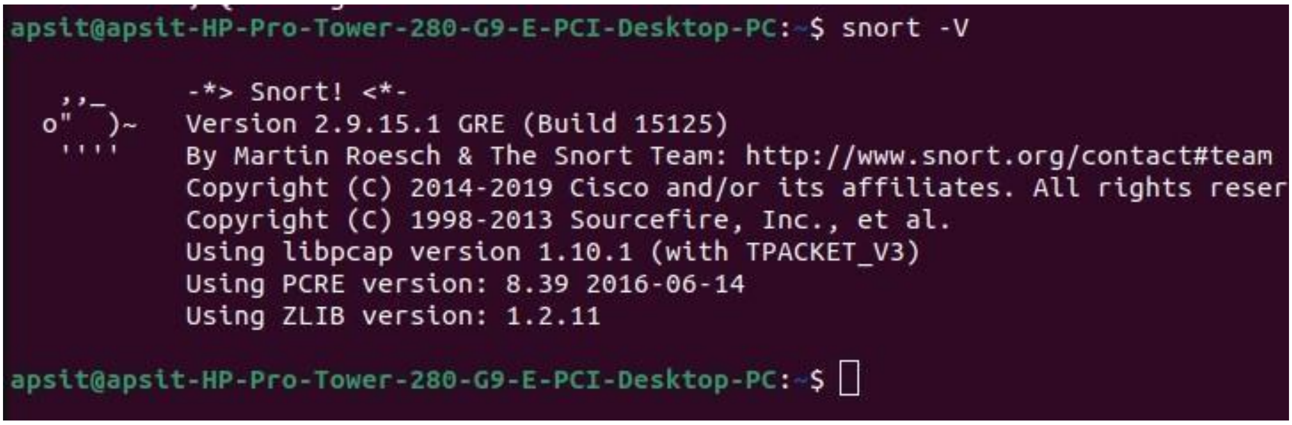
EXPERIMENT NO. 07

Aim: To study Intrusion Detection system SNORT and its log analysis.

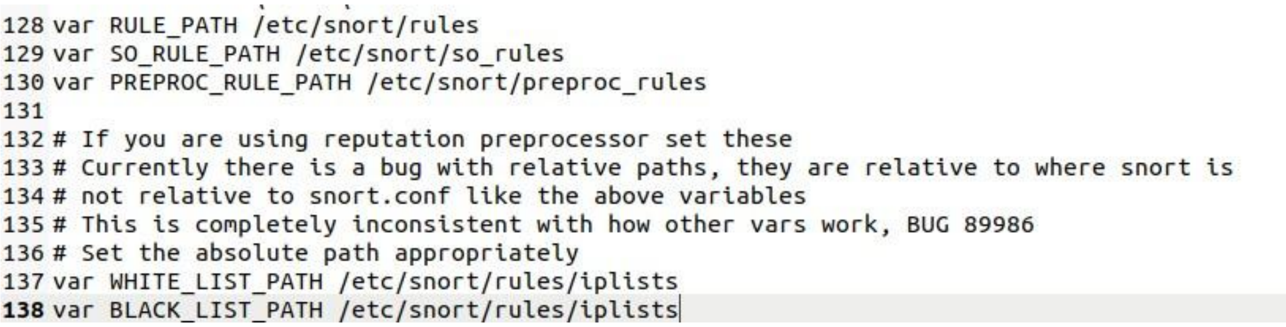


```
apsit@apsit-HP-Pro-Tower-280-G9-E-PCI-Desktop-PC:~$ sudo apt-get install snort
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  libdaq2 libdumbnet1 libluajit-5.1-2 libluajit-5.1-common libnetfilter-queue1
  oinkmaster snort-common snort-common-libraries snort-rules-default
Suggested packages:
  snort-doc
The following NEW packages will be installed:
  libdaq2 libdumbnet1 libluajit-5.1-2 libluajit-5.1-common libnetfilter-queue1
  oinkmaster snort snort-common snort-common-libraries snort-rules-default
0 upgraded, 10 newly installed, 0 to remove and 7 not upgraded.
Need to get 2,349 kB of archives.
After this operation, 10.6 MB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://in.archive.ubuntu.com/ubuntu jammy/universe amd64 libluajit-5.1-common all 2.1.0~beta3+dfsg-6 [44.3 kB]
Get:2 http://in.archive.ubuntu.com/ubuntu jammy/universe amd64 libluajit-5.1-2 amd64 2.1.0~beta3+dfsg-6 [238 kB]
Get:3 http://in.archive.ubuntu.com/ubuntu jammy/universe amd64 snort-common-libraries amd64 2.9.15.1-6build1 [882 kB]
Get:4 http://in.archive.ubuntu.com/ubuntu jammy/universe amd64 snort-rules-default all 2.9.15.1-6build1 [146 kB]
Get:5 http://in.archive.ubuntu.com/ubuntu jammy/universe amd64 snort-common all 2.9.15.1-6build1 [49.7 kB]
Get:6 http://in.archive.ubuntu.com/ubuntu jammy/universe amd64 libdumbnet1 amd64 1.12-10 [27.8 kB]
Get:7 http://in.archive.ubuntu.com/ubuntu jammy/universe amd64 libnetfilter-queue1 amd64 1.0.5-2 [14.4 kB]
Get:8 http://in.archive.ubuntu.com/ubuntu jammy/universe amd64 libdaq2 amd64 2.0.7-5 [83.5 kB]
Get:9 http://in.archive.ubuntu.com/ubuntu jammy/universe amd64 snort amd64 2.9.15.1-6build1 [792 kB]
Get:10 http://in.archive.ubuntu.com/ubuntu jammy/universe amd64 oinkmaster all 2.0-4.1 [71.8 kB]
Fetched 2,349 kB in 16s (143 kB/s)
```

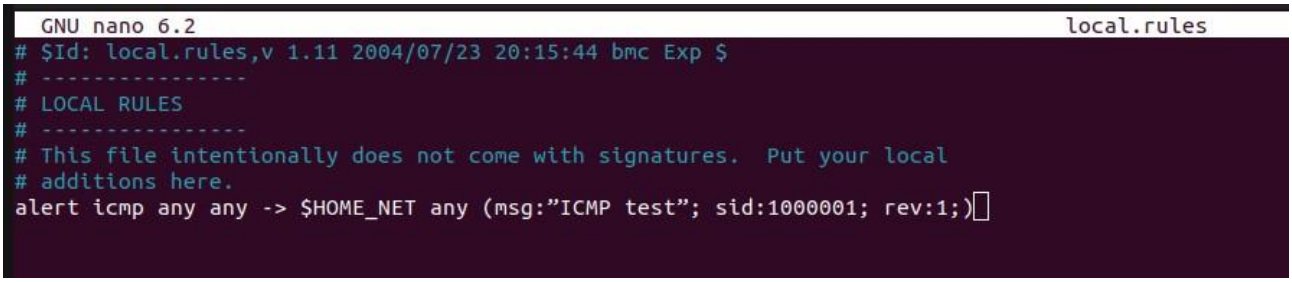
.



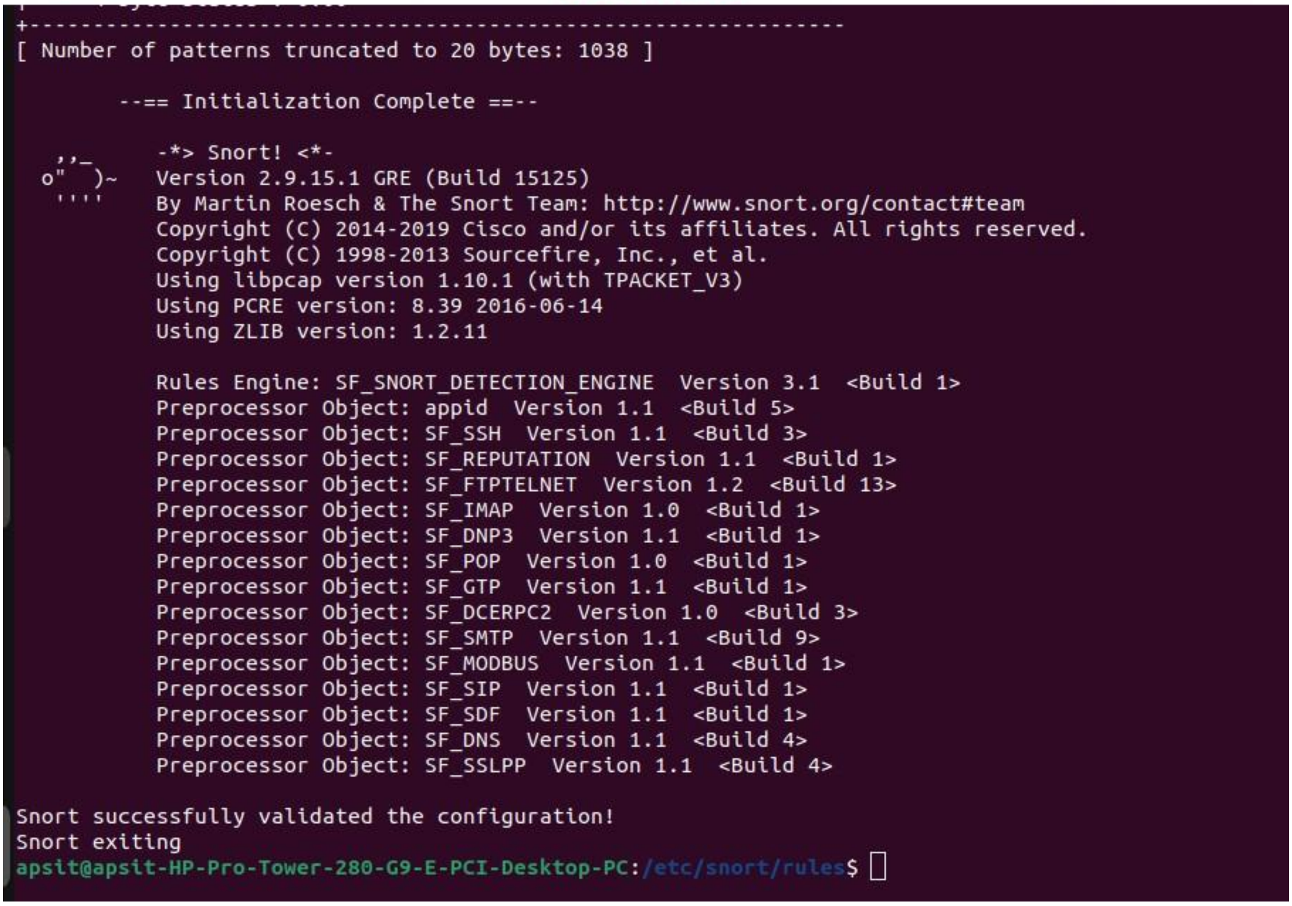
```
apsit@apsit-HP-Pro-Tower-280-G9-E-PCI-Desktop-PC:~$ snort -V

   ,,_     -*> Snort! <*-
  o"  )~   Version 2.9.15.1 GRE (Build 15125)
   ''''    By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
           Copyright (C) 2014-2019 Cisco and/or its affiliates. All rights reser
           Copyright (C) 1998-2013 Sourcefire, Inc., et al.
           Using libpcap version 1.10.1 (with TPACKET_V3)
           Using PCRE version: 8.39 2016-06-14
           Using ZLIB version: 1.2.11

apsit@apsit-HP-Pro-Tower-280-G9-E-PCI-Desktop-PC:~$ 
```



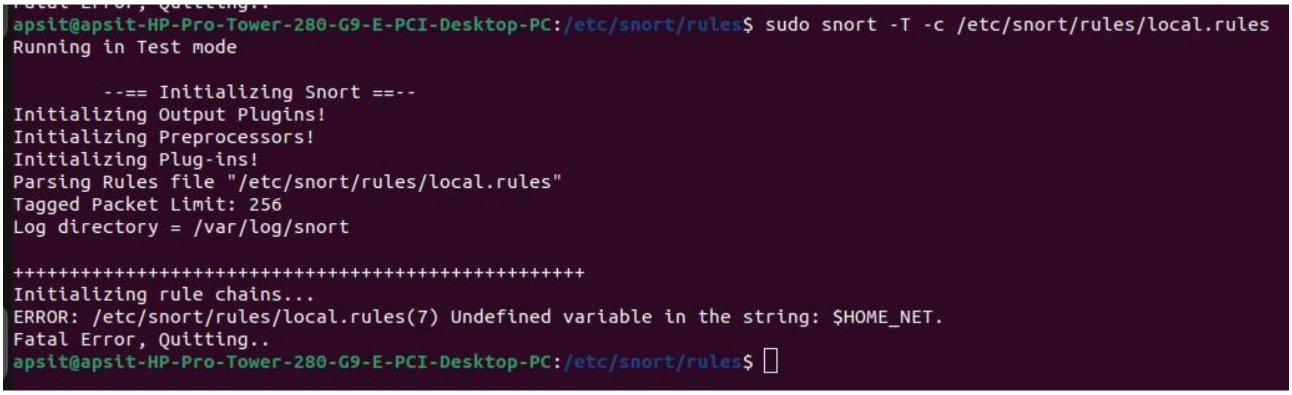
```
var RULE_PATH /etc/snort/rules
var SO_RULE_PATH /etc/snort/so_rules
var PREPROC_RULE_PATH /etc/snort/preproc_rules

# If you are using reputation preprocessor set these
# Currently there is a bug with relative paths, they are relative to where snort is
# not relative to snort.conf like the above variables
# This is completely inconsistent with how other vars work, BUG 89986
# Set the absolute path appropriately
var WHITE_LIST_PATH /etc/snort/rules/iplists
var BLACK_LIST_PATH /etc/snort/rules/iplists
```



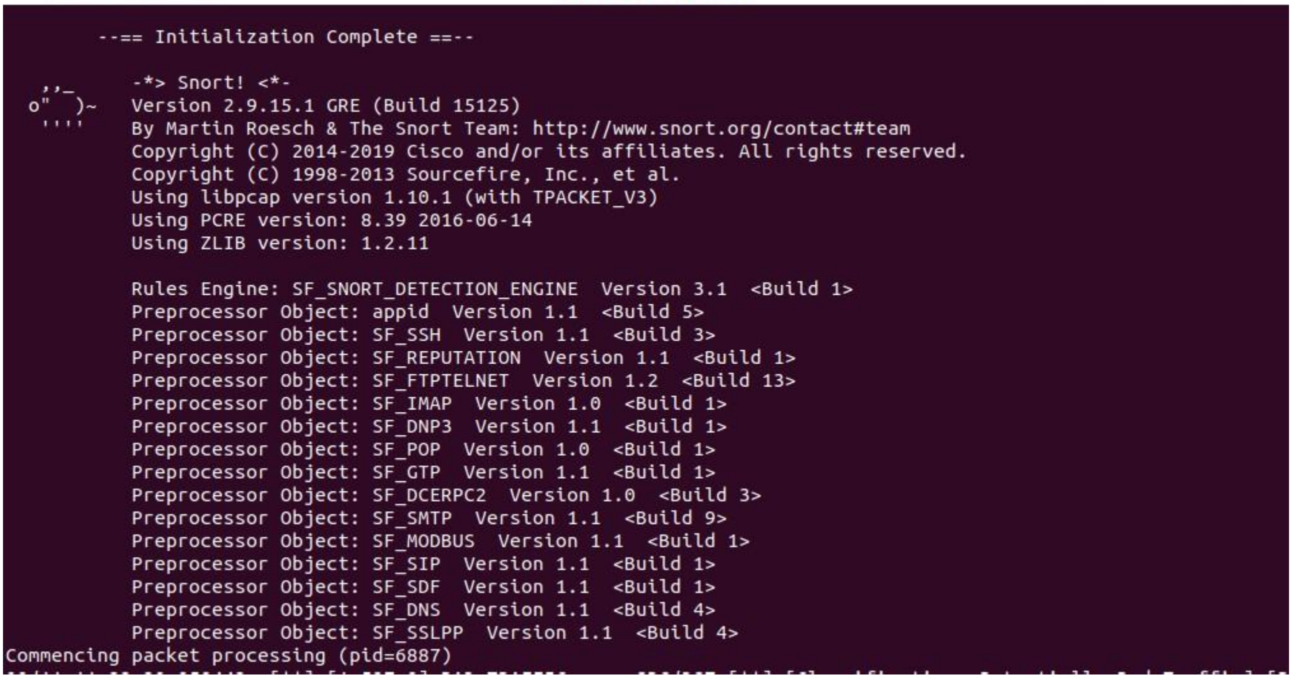
```
# $Id: local.rules,v 1.11 2004/07/23 20:15:44 bmc Exp $
# ----------------
# LOCAL RULES
# ----------------
# This file intentionally does not come with signatures.  Put your local
# additions here.
alert icmp any any -> $HOME_NET any (msg:”ICMP test”; sid:1000001; rev:1;)
```



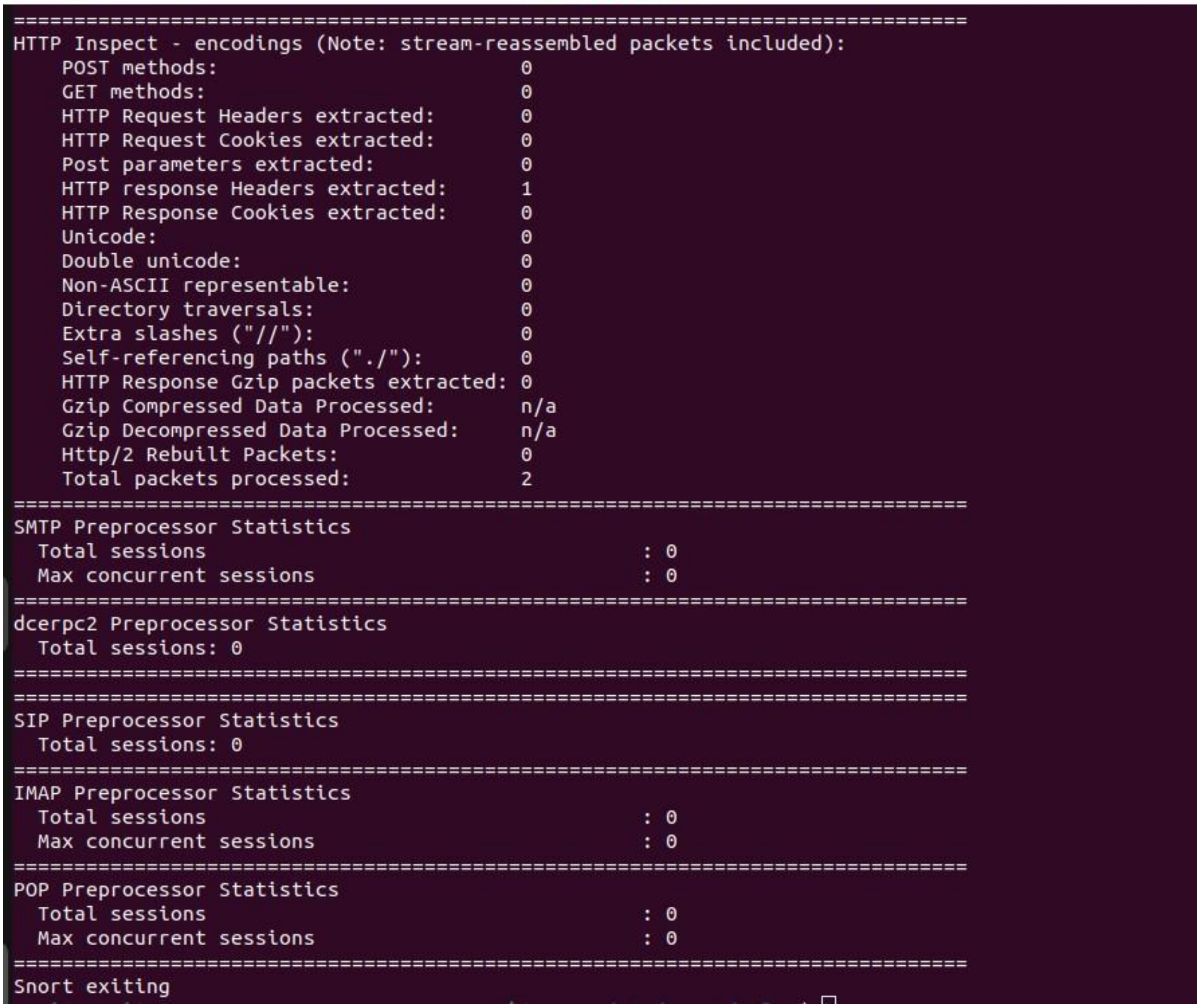
```
+----------------------------------------------------------------
[ Number of patterns truncated to 20 bytes: 1038 ]

        --== Initialization Complete ==--

   ,,_     -*> Snort! <*-
  o"  )~   Version 2.9.15.1 GRE (Build 15125)
   ''''    By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
           Copyright (C) 2014-2019 Cisco and/or its affiliates. All rights reserved.
           Copyright (C) 1998-2013 Sourcefire, Inc., et al.
           Using libpcap version 1.10.1 (with TPACKET_V3)
           Using PCRE version: 8.39 2016-06-14
           Using ZLIB version: 1.2.11

           Rules Engine: SF_SNORT_DETECTION_ENGINE  Version 3.1  <Build 1>
           Preprocessor Object: appid  Version 1.1  <Build 5>
           Preprocessor Object: SF_SSH  Version 1.1  <Build 3>
           Preprocessor Object: SF_REPUTATION  Version 1.1  <Build 1>
           Preprocessor Object: SF_FTPTELNET  Version 1.2  <Build 13>
           Preprocessor Object: SF_IMAP  Version 1.0  <Build 1>
           Preprocessor Object: SF_DNP3  Version 1.1  <Build 1>
           Preprocessor Object: SF_POP  Version 1.0  <Build 1>
           Preprocessor Object: SF_GTP  Version 1.1  <Build 1>
           Preprocessor Object: SF_DCERPC2  Version 1.0  <Build 3>
           Preprocessor Object: SF_SMTP  Version 1.1  <Build 9>
           Preprocessor Object: SF_MODBUS  Version 1.1  <Build 1>
           Preprocessor Object: SF_SIP  Version 1.1  <Build 1>
           Preprocessor Object: SF_SDF  Version 1.1  <Build 1>
           Preprocessor Object: SF_DNS  Version 1.1  <Build 4>
           Preprocessor Object: SF_SSLPP  Version 1.1  <Build 4>

Snort successfully validated the configuration!
Snort exiting
apsit@apsit-HP-Pro-Tower-280-G9-E-PCI-Desktop-PC:/etc/snort/rules$ 
```



```
Fatal Error, Quitting..
apsit@apsit-HP-Pro-Tower-280-G9-E-PCI-Desktop-PC:/etc/snort/rules$ sudo snort -T -c /etc/snort/rules/local.rules
Running in Test mode

        --== Initializing Snort ==--
Initializing Output Plugins!
Initializing Preprocessors!
Initializing Plug-ins!
Parsing Rules file "/etc/snort/rules/local.rules"
Tagged Packet Limit: 256
Log directory = /var/log/snort

++++++++++++++++++++++++++++++++++++++++++++++++++++
Initializing rule chains...
ERROR: /etc/snort/rules/local.rules(7) Undefined variable in the string: $HOME_NET.
Fatal Error, Quitting..
apsit@apsit-HP-Pro-Tower-280-G9-E-PCI-Desktop-PC:/etc/snort/rules$ 
```

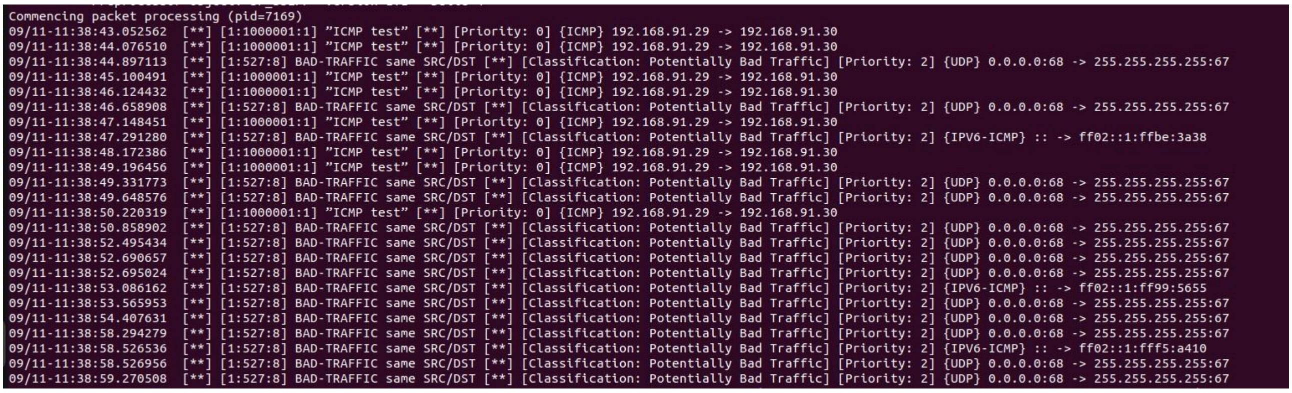


```
        --== Initialization Complete ==--

   ,,_     -*> Snort! <*-
  o"  )~   Version 2.9.15.1 GRE (Build 15125)
   ''''    By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
           Copyright (C) 2014-2019 Cisco and/or its affiliates. All rights reserved.
           Copyright (C) 1998-2013 Sourcefire, Inc., et al.
           Using libpcap version 1.10.1 (with TPACKET_V3)
           Using PCRE version: 8.39 2016-06-14
           Using ZLIB version: 1.2.11

           Rules Engine: SF_SNORT_DETECTION_ENGINE  Version 3.1  <Build 1>
           Preprocessor Object: appid  Version 1.1  <Build 5>
           Preprocessor Object: SF_SSH  Version 1.1  <Build 3>
           Preprocessor Object: SF_REPUTATION  Version 1.1  <Build 1>
           Preprocessor Object: SF_FTPTELNET  Version 1.2  <Build 13>
           Preprocessor Object: SF_IMAP  Version 1.0  <Build 1>
           Preprocessor Object: SF_DNP3  Version 1.1  <Build 1>
           Preprocessor Object: SF_POP  Version 1.0  <Build 1>
           Preprocessor Object: SF_GTP  Version 1.1  <Build 1>
           Preprocessor Object: SF_DCERPC2  Version 1.0  <Build 3>
           Preprocessor Object: SF_SMTP  Version 1.1  <Build 9>
           Preprocessor Object: SF_MODBUS  Version 1.1  <Build 1>
           Preprocessor Object: SF_SIP  Version 1.1  <Build 1>
           Preprocessor Object: SF_SDF  Version 1.1  <Build 1>
           Preprocessor Object: SF_DNS  Version 1.1  <Build 4>
           Preprocessor Object: SF_SSLPP  Version 1.1  <Build 4>
Commencing packet processing (pid=6887)
```



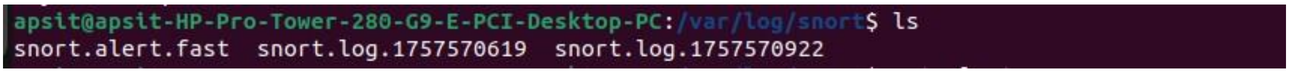
```
================================================================================
HTTP Inspect - encodings (Note: stream-reassembled packets included):
    POST methods:                         0
    GET methods:                          0
    HTTP Request Headers extracted:       0
    HTTP Request Cookies extracted:       0
    Post parameters extracted:            0
    HTTP response Headers extracted:      1
    HTTP Response Cookies extracted:      0
    Unicode:                              0
    Double unicode:                       0
    Non-ASCII representable:              0
    Directory traversals:                 0
    Extra slashes ("//"):                 0
    Self-referencing paths ("./"):        0
    HTTP Response Gzip packets extracted: 0
    Gzip Compressed Data Processed:       n/a
    Gzip Decompressed Data Processed:     n/a
    Http/2 Rebuilt Packets:               0
    Total packets processed:              2
================================================================================
SMTP Preprocessor Statistics
  Total sessions                                    : 0
  Max concurrent sessions                           : 0
================================================================================
dcerpc2 Preprocessor Statistics
  Total sessions: 0
================================================================================
================================================================================
SIP Preprocessor Statistics
  Total sessions: 0
================================================================================
IMAP Preprocessor Statistics
  Total sessions                                    : 0
  Max concurrent sessions                           : 0
================================================================================
POP Preprocessor Statistics
  Total sessions                                    : 0
  Max concurrent sessions                           : 0
================================================================================
Snort exiting
```

•



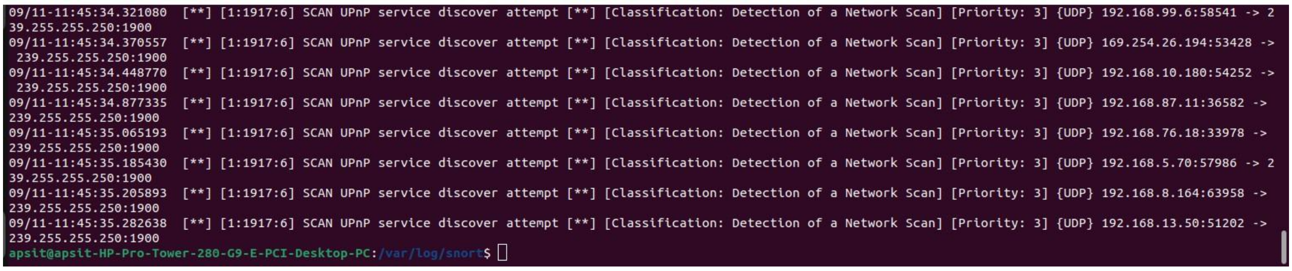
```
Commencing packet processing (pid=7169)
09/11-11:38:43.052562  [**] [1:1000001:1] ”ICMP test” [**] [Priority: 0] {ICMP} 192.168.91.29 -> 192.168.91.30
09/11-11:38:44.076510  [**] [1:1000001:1] ”ICMP test” [**] [Priority: 0] {ICMP} 192.168.91.29 -> 192.168.91.30
09/11-11:38:44.897113  [**] [1:527:8] BAD-TRAFFIC same SRC/DST [**] [Classification: Potentially Bad Traffic] [Priority: 2] {UDP} 0.0.0.0:68 -> 255.255.255.255:67
09/11-11:38:45.100491  [**] [1:1000001:1] ”ICMP test” [**] [Priority: 0] {ICMP} 192.168.91.29 -> 192.168.91.30
09/11-11:38:46.124432  [**] [1:1000001:1] ”ICMP test” [**] [Priority: 0] {ICMP} 192.168.91.29 -> 192.168.91.30
09/11-11:38:46.658908  [**] [1:527:8] BAD-TRAFFIC same SRC/DST [**] [Classification: Potentially Bad Traffic] [Priority: 2] {UDP} 0.0.0.0:68 -> 255.255.255.255:67
09/11-11:38:47.148451  [**] [1:1000001:1] ”ICMP test” [**] [Priority: 0] {ICMP} 192.168.91.29 -> 192.168.91.30
09/11-11:38:47.291280  [**] [1:527:8] BAD-TRAFFIC same SRC/DST [**] [Classification: Potentially Bad Traffic] [Priority: 2] {IPV6-ICMP} :: -> ff02::1:ffbe:3a38
09/11-11:38:48.172386  [**] [1:1000001:1] ”ICMP test” [**] [Priority: 0] {ICMP} 192.168.91.29 -> 192.168.91.30
09/11-11:38:49.196456  [**] [1:1000001:1] ”ICMP test” [**] [Priority: 0] {ICMP} 192.168.91.29 -> 192.168.91.30
09/11-11:38:49.331773  [**] [1:527:8] BAD-TRAFFIC same SRC/DST [**] [Classification: Potentially Bad Traffic] [Priority: 2] {UDP} 0.0.0.0:68 -> 255.255.255.255:67
09/11-11:38:49.648576  [**] [1:527:8] BAD-TRAFFIC same SRC/DST [**] [Classification: Potentially Bad Traffic] [Priority: 2] {UDP} 0.0.0.0:68 -> 255.255.255.255:67
09/11-11:38:50.220319  [**] [1:1000001:1] ”ICMP test” [**] [Priority: 0] {ICMP} 192.168.91.29 -> 192.168.91.30
09/11-11:38:50.858902  [**] [1:527:8] BAD-TRAFFIC same SRC/DST [**] [Classification: Potentially Bad Traffic] [Priority: 2] {UDP} 0.0.0.0:68 -> 255.255.255.255:67
09/11-11:38:52.495434  [**] [1:527:8] BAD-TRAFFIC same SRC/DST [**] [Classification: Potentially Bad Traffic] [Priority: 2] {UDP} 0.0.0.0:68 -> 255.255.255.255:67
09/11-11:38:52.690657  [**] [1:527:8] BAD-TRAFFIC same SRC/DST [**] [Classification: Potentially Bad Traffic] [Priority: 2] {UDP} 0.0.0.0:68 -> 255.255.255.255:67
09/11-11:38:52.695024  [**] [1:527:8] BAD-TRAFFIC same SRC/DST [**] [Classification: Potentially Bad Traffic] [Priority: 2] {UDP} 0.0.0.0:68 -> 255.255.255.255:67
09/11-11:38:53.086162  [**] [1:527:8] BAD-TRAFFIC same SRC/DST [**] [Classification: Potentially Bad Traffic] [Priority: 2] {IPV6-ICMP} :: -> ff02::1:ff99:5655
09/11-11:38:53.565953  [**] [1:527:8] BAD-TRAFFIC same SRC/DST [**] [Classification: Potentially Bad Traffic] [Priority: 2] {UDP} 0.0.0.0:68 -> 255.255.255.255:67
09/11-11:38:54.407631  [**] [1:527:8] BAD-TRAFFIC same SRC/DST [**] [Classification: Potentially Bad Traffic] [Priority: 2] {UDP} 0.0.0.0:68 -> 255.255.255.255:67
09/11-11:38:58.294279  [**] [1:527:8] BAD-TRAFFIC same SRC/DST [**] [Classification: Potentially Bad Traffic] [Priority: 2] {UDP} 0.0.0.0:68 -> 255.255.255.255:67
09/11-11:38:58.526536  [**] [1:527:8] BAD-TRAFFIC same SRC/DST [**] [Classification: Potentially Bad Traffic] [Priority: 2] {IPV6-ICMP} :: -> ff02::1:fff5:a410
09/11-11:38:58.526956  [**] [1:527:8] BAD-TRAFFIC same SRC/DST [**] [Classification: Potentially Bad Traffic] [Priority: 2] {UDP} 0.0.0.0:68 -> 255.255.255.255:67
09/11-11:38:59.270508  [**] [1:527:8] BAD-TRAFFIC same SRC/DST [**] [Classification: Potentially Bad Traffic] [Priority: 2] {UDP} 0.0.0.0:68 -> 255.255.255.255:67
```

•



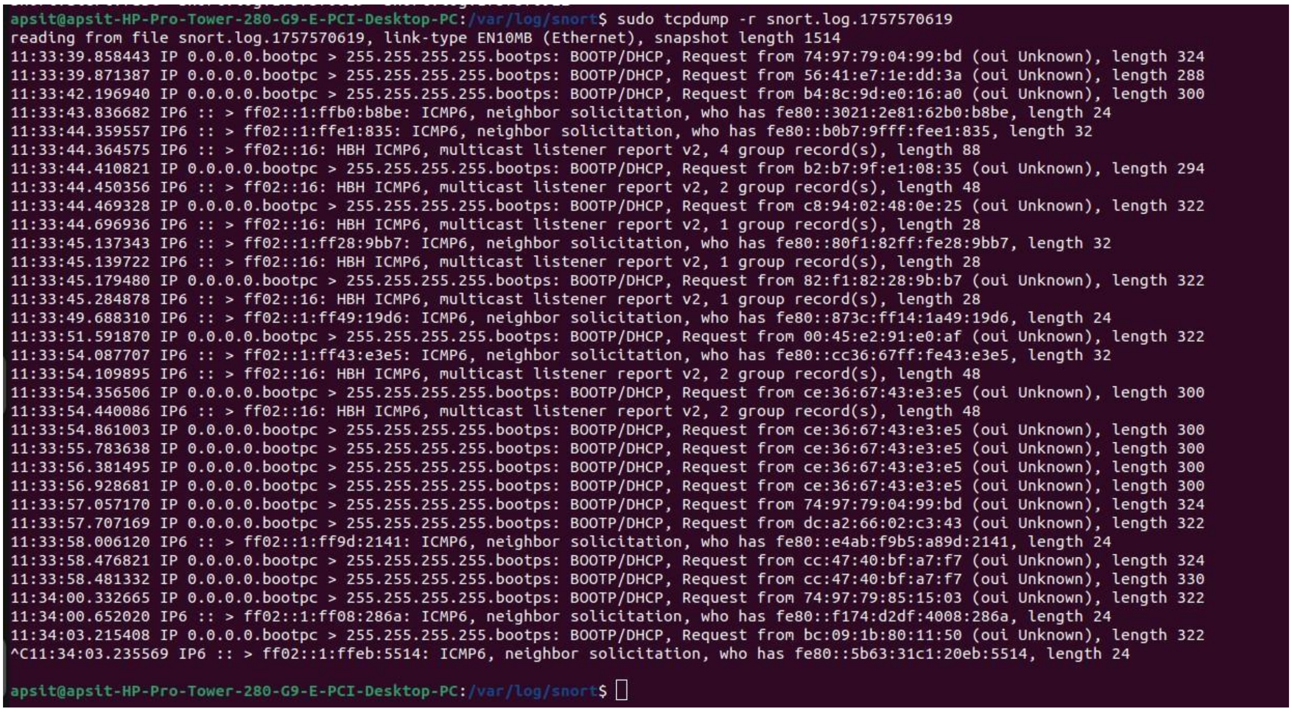
```
apsit@apsit-HP-Pro-Tower-280-G9-E-PCI-Desktop-PC:/var/log/snort$ ls
snort.alert.fast   snort.log.1757570619   snort.log.1757570922
```

-

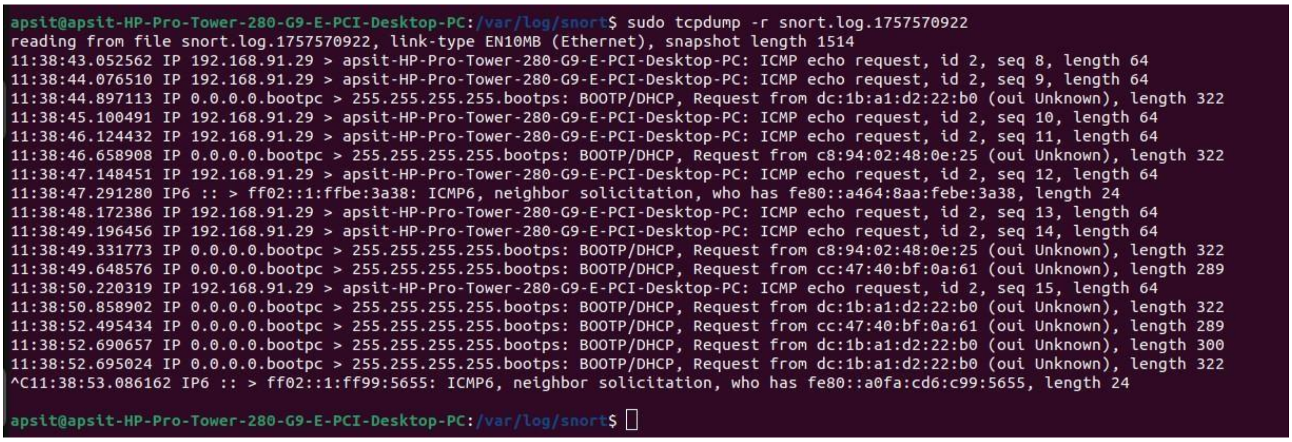


```
09/11-11:45:34.321080  [**] [1:1917:6] SCAN UPnP service discover attempt [**] [Classification: Detection of a Network Scan] [Priority: 3] {UDP} 192.168.99.6:58541 -> 2
39.255.255.250:1900
09/11-11:45:34.370557  [**] [1:1917:6] SCAN UPnP service discover attempt [**] [Classification: Detection of a Network Scan] [Priority: 3] {UDP} 169.254.26.194:53428 ->
 239.255.255.250:1900
09/11-11:45:34.448770  [**] [1:1917:6] SCAN UPnP service discover attempt [**] [Classification: Detection of a Network Scan] [Priority: 3] {UDP} 192.168.10.180:54252 ->
 239.255.255.250:1900
09/11-11:45:34.877335  [**] [1:1917:6] SCAN UPnP service discover attempt [**] [Classification: Detection of a Network Scan] [Priority: 3] {UDP} 192.168.87.11:36582 ->
239.255.255.250:1900
09/11-11:45:35.065193  [**] [1:1917:6] SCAN UPnP service discover attempt [**] [Classification: Detection of a Network Scan] [Priority: 3] {UDP} 192.168.76.18:33978 ->
239.255.255.250:1900
09/11-11:45:35.185430  [**] [1:1917:6] SCAN UPnP service discover attempt [**] [Classification: Detection of a Network Scan] [Priority: 3] {UDP} 192.168.5.70:57986 -> 2
39.255.255.250:1900
09/11-11:45:35.205893  [**] [1:1917:6] SCAN UPnP service discover attempt [**] [Classification: Detection of a Network Scan] [Priority: 3] {UDP} 192.168.8.164:63958 ->
239.255.255.250:1900
09/11-11:45:35.282638  [**] [1:1917:6] SCAN UPnP service discover attempt [**] [Classification: Detection of a Network Scan] [Priority: 3] {UDP} 192.168.13.50:51202 ->
239.255.255.250:1900
apsit@apsit-HP-Pro-Tower-280-G9-E-PCI-Desktop-PC:/var/log/snort$ 
```

-



```
apsit@apsit-HP-Pro-Tower-280-G9-E-PCI-Desktop-PC:/var/log/snort$ sudo tcpdump -r snort.log.1757570619
reading from file snort.log.1757570619, link-type EN10MB (Ethernet), snapshot length 1514
11:33:39.858443 IP 0.0.0.0.bootpc > 255.255.255.255.bootps: BOOTP/DHCP, Request from 74:97:79:04:99:bd (oui Unknown), length 324
11:33:39.871387 IP 0.0.0.0.bootpc > 255.255.255.255.bootps: BOOTP/DHCP, Request from 56:41:e7:1e:dd:3a (oui Unknown), length 288
11:33:42.196940 IP 0.0.0.0.bootpc > 255.255.255.255.bootps: BOOTP/DHCP, Request from b4:8c:9d:e0:16:a0 (oui Unknown), length 300
11:33:43.836682 IP6 :: > ff02::1:ffb0:b8be: ICMP6, neighbor solicitation, who has fe80::3021:2e81:62b0:b8be, length 24
11:33:44.359557 IP6 :: > ff02::1:ffe1:835: ICMP6, neighbor solicitation, who has fe80::b0b7:9fff:fee1:835, length 32
11:33:44.364575 IP6 :: > ff02::16: HBH ICMP6, multicast listener report v2, 4 group record(s), length 88
11:33:44.410821 IP 0.0.0.0.bootpc > 255.255.255.255.bootps: BOOTP/DHCP, Request from b2:b7:9f:e1:08:35 (oui Unknown), length 294
11:33:44.450356 IP6 :: > ff02::16: HBH ICMP6, multicast listener report v2, 2 group record(s), length 48
11:33:44.469328 IP 0.0.0.0.bootpc > 255.255.255.255.bootps: BOOTP/DHCP, Request from c8:94:02:48:0e:25 (oui Unknown), length 322
11:33:44.696936 IP6 :: > ff02::16: HBH ICMP6, multicast listener report v2, 1 group record(s), length 28
11:33:45.137343 IP6 :: > ff02::1:ff28:9bb7: ICMP6, neighbor solicitation, who has fe80::80f1:82ff:fe28:9bb7, length 32
11:33:45.139722 IP6 :: > ff02::16: HBH ICMP6, multicast listener report v2, 1 group record(s), length 28
11:33:45.179480 IP 0.0.0.0.bootpc > 255.255.255.255.bootps: BOOTP/DHCP, Request from 82:f1:82:28:9b:b7 (oui Unknown), length 322
11:33:45.284878 IP6 :: > ff02::16: HBH ICMP6, multicast listener report v2, 1 group record(s), length 28
11:33:49.688310 IP6 :: > ff02::1:ff49:19d6: ICMP6, neighbor solicitation, who has fe80::873c:ff14:1a49:19d6, length 24
11:33:51.591870 IP 0.0.0.0.bootpc > 255.255.255.255.bootps: BOOTP/DHCP, Request from 00:45:e2:91:e0:af (oui Unknown), length 322
11:33:54.087707 IP6 :: > ff02::1:ff43:e3e5: ICMP6, neighbor solicitation, who has fe80::cc36:67ff:fe43:e3e5, length 32
11:33:54.109895 IP6 :: > ff02::16: HBH ICMP6, multicast listener report v2, 2 group record(s), length 48
11:33:54.356506 IP 0.0.0.0.bootpc > 255.255.255.255.bootps: BOOTP/DHCP, Request from ce:36:67:43:e3:e5 (oui Unknown), length 300
11:33:54.440086 IP6 :: > ff02::16: HBH ICMP6, multicast listener report v2, 2 group record(s), length 48
11:33:54.861003 IP 0.0.0.0.bootpc > 255.255.255.255.bootps: BOOTP/DHCP, Request from ce:36:67:43:e3:e5 (oui Unknown), length 300
11:33:55.783638 IP 0.0.0.0.bootpc > 255.255.255.255.bootps: BOOTP/DHCP, Request from ce:36:67:43:e3:e5 (oui Unknown), length 300
11:33:56.381495 IP 0.0.0.0.bootpc > 255.255.255.255.bootps: BOOTP/DHCP, Request from ce:36:67:43:e3:e5 (oui Unknown), length 300
11:33:56.928681 IP 0.0.0.0.bootpc > 255.255.255.255.bootps: BOOTP/DHCP, Request from ce:36:67:43:e3:e5 (oui Unknown), length 300
11:33:57.057170 IP 0.0.0.0.bootpc > 255.255.255.255.bootps: BOOTP/DHCP, Request from 74:97:79:04:99:bd (oui Unknown), length 324
11:33:57.707169 IP 0.0.0.0.bootpc > 255.255.255.255.bootps: BOOTP/DHCP, Request from dc:a2:66:02:c3:43 (oui Unknown), length 322
11:33:58.006120 IP6 :: > ff02::1:ff9d:2141: ICMP6, neighbor solicitation, who has fe80::e4ab:f9b5:a89d:2141, length 24
11:33:58.476821 IP 0.0.0.0.bootpc > 255.255.255.255.bootps: BOOTP/DHCP, Request from cc:47:40:bf:a7:f7 (oui Unknown), length 324
11:33:58.481332 IP 0.0.0.0.bootpc > 255.255.255.255.bootps: BOOTP/DHCP, Request from cc:47:40:bf:a7:f7 (oui Unknown), length 330
11:34:00.332665 IP 0.0.0.0.bootpc > 255.255.255.255.bootps: BOOTP/DHCP, Request from 74:97:79:85:15:03 (oui Unknown), length 322
11:34:00.652020 IP6 :: > ff02::1:ff08:286a: ICMP6, neighbor solicitation, who has fe80::f174:d2df:4008:286a, length 24
11:34:03.215408 IP 0.0.0.0.bootpc > 255.255.255.255.bootps: BOOTP/DHCP, Request from bc:09:1b:80:11:50 (oui Unknown), length 322
^C11:34:03.235569 IP6 :: > ff02::1:ffeb:5514: ICMP6, neighbor solicitation, who has fe80::5b63:31c1:20eb:5514, length 24

apsit@apsit-HP-Pro-Tower-280-G9-E-PCI-Desktop-PC:/var/log/snort$ 
```



```
apsit@apsit-HP-Pro-Tower-280-G9-E-PCI-Desktop-PC:/var/log/snort$ sudo tcpdump -r snort.log.1757570922
reading from file snort.log.1757570922, link-type EN10MB (Ethernet), snapshot length 1514
11:38:43.052562 IP 192.168.91.29 > apsit-HP-Pro-Tower-280-G9-E-PCI-Desktop-PC: ICMP echo request, id 2, seq 8, length 64
11:38:44.076510 IP 192.168.91.29 > apsit-HP-Pro-Tower-280-G9-E-PCI-Desktop-PC: ICMP echo request, id 2, seq 9, length 64
11:38:44.897113 IP 0.0.0.0.bootpc > 255.255.255.255.bootps: BOOTP/DHCP, Request from dc:1b:a1:d2:22:b0 (oui Unknown), length 322
11:38:45.100491 IP 192.168.91.29 > apsit-HP-Pro-Tower-280-G9-E-PCI-Desktop-PC: ICMP echo request, id 2, seq 10, length 64
11:38:46.124432 IP 192.168.91.29 > apsit-HP-Pro-Tower-280-G9-E-PCI-Desktop-PC: ICMP echo request, id 2, seq 11, length 64
11:38:46.658908 IP 0.0.0.0.bootpc > 255.255.255.255.bootps: BOOTP/DHCP, Request from c8:94:02:48:0e:25 (oui Unknown), length 322
11:38:47.148451 IP 192.168.91.29 > apsit-HP-Pro-Tower-280-G9-E-PCI-Desktop-PC: ICMP echo request, id 2, seq 12, length 64
11:38:47.291280 IP6 :: > ff02::1:ffbe:3a38: ICMP6, neighbor solicitation, who has fe80::a464:8aa:febe:3a38, length 24
11:38:48.172386 IP 192.168.91.29 > apsit-HP-Pro-Tower-280-G9-E-PCI-Desktop-PC: ICMP echo request, id 2, seq 13, length 64
11:38:49.196456 IP 192.168.91.29 > apsit-HP-Pro-Tower-280-G9-E-PCI-Desktop-PC: ICMP echo request, id 2, seq 14, length 64
11:38:49.331773 IP 0.0.0.0.bootpc > 255.255.255.255.bootps: BOOTP/DHCP, Request from c8:94:02:48:0e:25 (oui Unknown), length 322
11:38:49.648576 IP 0.0.0.0.bootpc > 255.255.255.255.bootps: BOOTP/DHCP, Request from cc:47:40:bf:0a:61 (oui Unknown), length 289
11:38:50.220319 IP 192.168.91.29 > apsit-HP-Pro-Tower-280-G9-E-PCI-Desktop-PC: ICMP echo request, id 2, seq 15, length 64
11:38:50.858902 IP 0.0.0.0.bootpc > 255.255.255.255.bootps: BOOTP/DHCP, Request from dc:1b:a1:d2:22:b0 (oui Unknown), length 322
11:38:52.495434 IP 0.0.0.0.bootpc > 255.255.255.255.bootps: BOOTP/DHCP, Request from cc:47:40:bf:0a:61 (oui Unknown), length 289
11:38:52.690657 IP 0.0.0.0.bootpc > 255.255.255.255.bootps: BOOTP/DHCP, Request from dc:1b:a1:d2:22:b0 (oui Unknown), length 300
11:38:52.695024 IP 0.0.0.0.bootpc > 255.255.255.255.bootps: BOOTP/DHCP, Request from dc:1b:a1:d2:22:b0 (oui Unknown), length 322
^C11:38:53.086162 IP6 :: > ff02::1:ff99:5655: ICMP6, neighbor solicitation, who has fe80::a0fa:cd6:c99:5655, length 24

apsit@apsit-HP-Pro-Tower-280-G9-E-PCI-Desktop-PC:/var/log/snort$
```

Conclusion:

Hence we have successfully studied Snort which is network intrusion prevention system, capable of performing real-time traffic analysis and packet logging on IP networks. It can perform protocol analysis, content searching/matching, and can be used to detect a variety of attacks and probes, such as buffer overflows, stealth port scans, CGI attacks, SMB probes, OS fingerprinting attempts, and much more. Also we have done analysis of log generated by snort.