Parshvanath Charitable Trust's

A. P. SHAH INSTITUTE OF TECHNOLOGY

(Approved by AICTE New Delhi & Govt. of Maharashtra, Affiliated to University of Mumbai)
(Religious Jain Minority)

Department of Information Technology

Semester: V
Academic Year: 2022-23
Class / Branch: TE IT
Subject: Security Lab (SL)
Name of Instructor: Prof. Apeksha Mohite

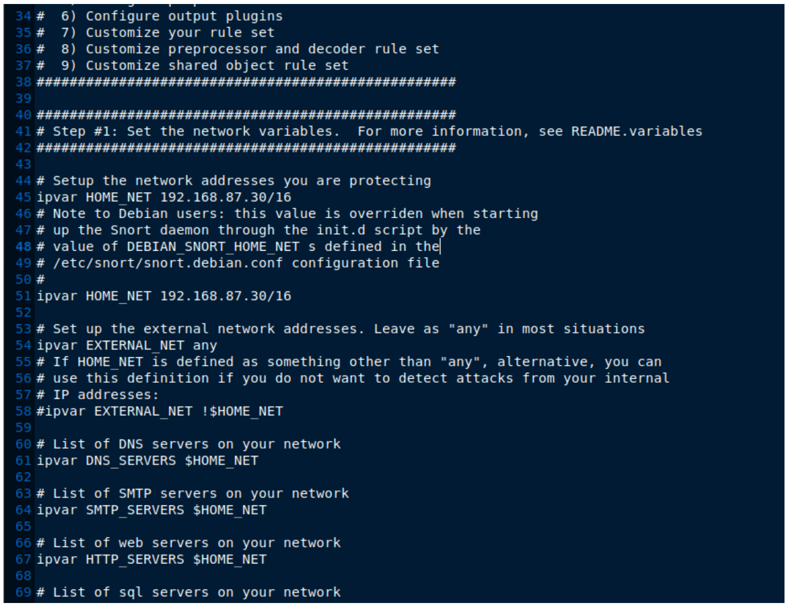
Name of Student: Vishal Bangar
Student ID: 20104084

EXPERIMENT NO. 06

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

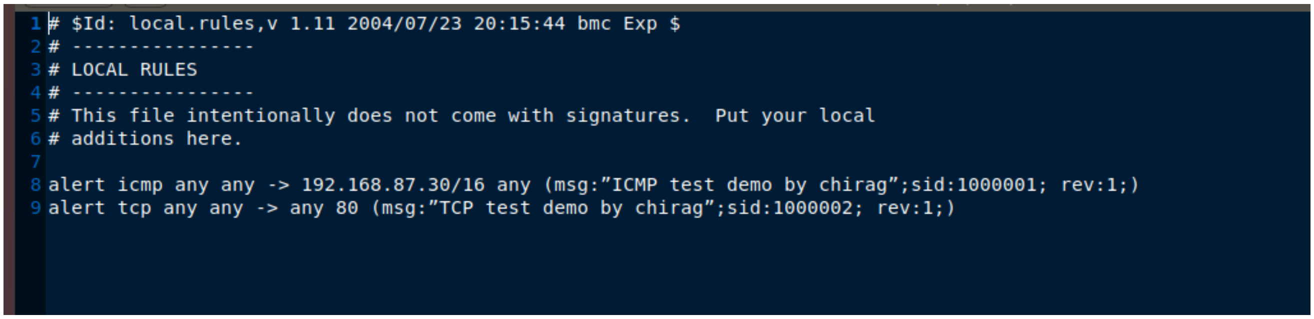
Output:

1) snort.conf



```
#  6) Configure output plugins
#  7) Customize your rule set
#  8) Customize preprocessor and decoder rule set
#  9) Customize shared object rule set
###################################################

###################################################
# Step #1: Set the network variables.  For more information, see README.variables
###################################################

# Setup the network addresses you are protecting
ipvar HOME_NET 192.168.87.30/16
# Note to Debian users: this value is overriden when starting
# up the Snort daemon through the init.d script by the
# value of DEBIAN_SNORT_HOME_NET s defined in the
# /etc/snort/snort.debian.conf configuration file
#
ipvar HOME_NET 192.168.87.30/16

# 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

# List of DNS servers on your network
ipvar DNS_SERVERS $HOME_NET

# List of SMTP servers on your network
ipvar SMTP_SERVERS $HOME_NET

# List of web servers on your network
ipvar HTTP_SERVERS $HOME_NET

# List of sql servers on your network
```

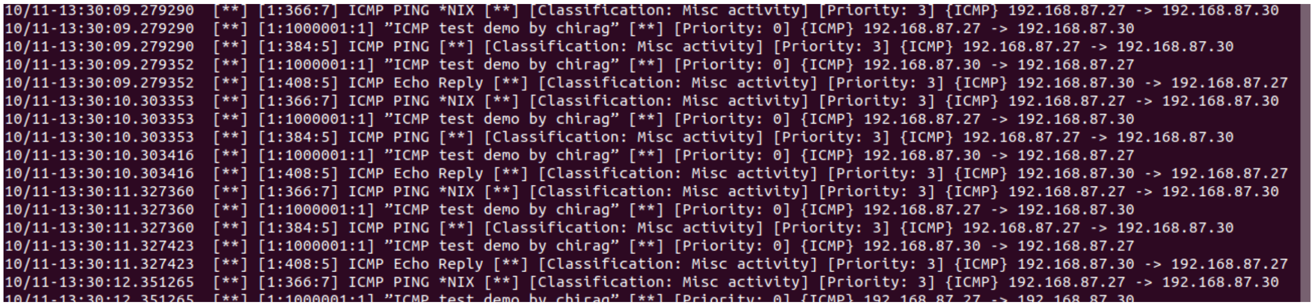
2) local.rules



```
# $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 -> 192.168.87.30/16 any (msg:”ICMP test demo by chirag”;sid:1000001; rev:1;)
alert tcp any any -> any 80 (msg:”TCP test demo by chirag”;sid:1000002; rev:1;)
```

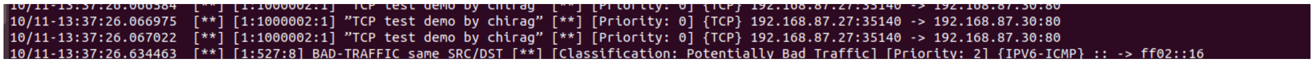
3) Alert

a) icmp



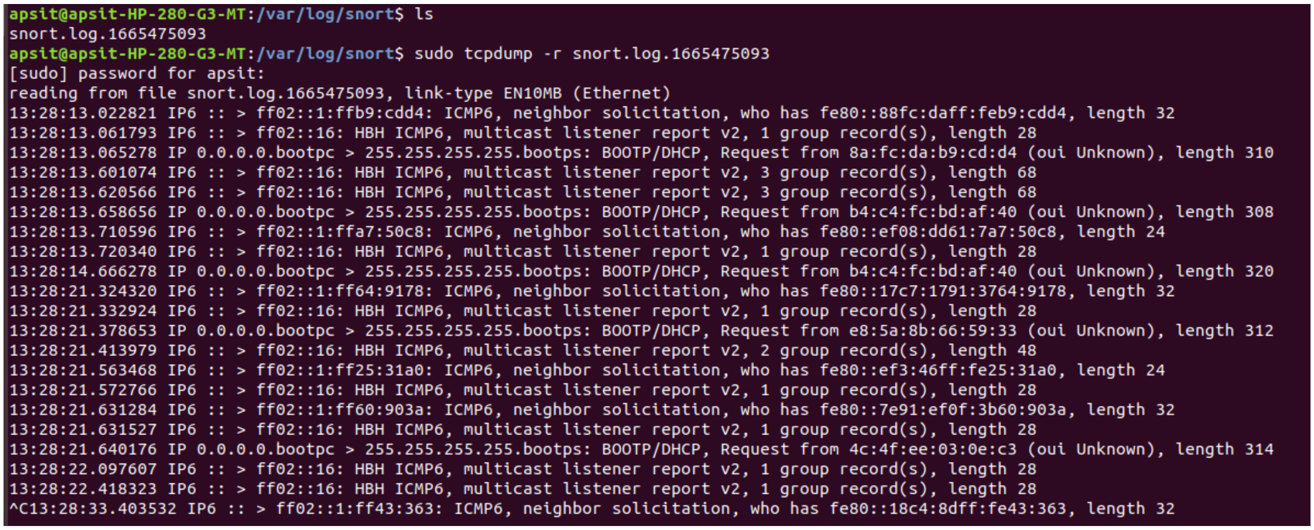
```
10/11-13:30:09.279290  [**] [1:366:7] ICMP PING *NIX [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.87.27 -> 192.168.87.30
10/11-13:30:09.279290  [**] [1:1000001:1] ”ICMP test demo by chirag” [**] [Priority: 0] {ICMP} 192.168.87.27 -> 192.168.87.30
10/11-13:30:09.279290  [**] [1:384:5] ICMP PING [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.87.27 -> 192.168.87.30
10/11-13:30:09.279352  [**] [1:1000001:1] ”ICMP test demo by chirag” [**] [Priority: 0] {ICMP} 192.168.87.30 -> 192.168.87.27
10/11-13:30:09.279352  [**] [1:408:5] ICMP Echo Reply [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.87.30 -> 192.168.87.27
10/11-13:30:10.303353  [**] [1:366:7] ICMP PING *NIX [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.87.27 -> 192.168.87.30
10/11-13:30:10.303353  [**] [1:1000001:1] ”ICMP test demo by chirag” [**] [Priority: 0] {ICMP} 192.168.87.27 -> 192.168.87.30
10/11-13:30:10.303353  [**] [1:384:5] ICMP PING [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.87.27 -> 192.168.87.30
10/11-13:30:10.303416  [**] [1:1000001:1] ”ICMP test demo by chirag” [**] [Priority: 0] {ICMP} 192.168.87.30 -> 192.168.87.27
10/11-13:30:10.303416  [**] [1:408:5] ICMP Echo Reply [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.87.30 -> 192.168.87.27
10/11-13:30:11.327360  [**] [1:366:7] ICMP PING *NIX [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.87.27 -> 192.168.87.30
10/11-13:30:11.327360  [**] [1:1000001:1] ”ICMP test demo by chirag” [**] [Priority: 0] {ICMP} 192.168.87.27 -> 192.168.87.30
10/11-13:30:11.327360  [**] [1:384:5] ICMP PING [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.87.27 -> 192.168.87.30
10/11-13:30:11.327423  [**] [1:1000001:1] ”ICMP test demo by chirag” [**] [Priority: 0] {ICMP} 192.168.87.30 -> 192.168.87.27
10/11-13:30:11.327423  [**] [1:408:5] ICMP Echo Reply [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.87.30 -> 192.168.87.27
10/11-13:30:12.351265  [**] [1:366:7] ICMP PING *NIX [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.87.27 -> 192.168.87.30
10/11-13:30:12.351265  [**] [1:1000001:1] ”ICMP test demo by chirag” [**] [Priority: 0] {ICMP} 192.168.87.27 -> 192.168.87.30
```

b) tcp



```
10/11-13:37:26.066384  [**] [1:1000002:1] ”TCP test demo by chirag” [**] [Priority: 0] {TCP} 192.168.87.27:35140 -> 192.168.87.30:80
10/11-13:37:26.066975  [**] [1:1000002:1] ”TCP test demo by chirag” [**] [Priority: 0] {TCP} 192.168.87.27:35140 -> 192.168.87.30:80
10/11-13:37:26.067022  [**] [1:1000002:1] ”TCP test demo by chirag” [**] [Priority: 0] {TCP} 192.168.87.27:35140 -> 192.168.87.30:80
10/11-13:37:26.634463  [**] [1:527:8] BAD-TRAFFIC same SRC/DST [**] [Classification: Potentially Bad Traffic] [Priority: 2] {IPV6-ICMP} :: -> ff02::16
```

4) tcpdump snort log



```
apsit@apsit-HP-280-G3-MT:/var/log/snort$ ls
snort.log.1665475093
apsit@apsit-HP-280-G3-MT:/var/log/snort$ sudo tcpdump -r snort.log.1665475093
[sudo] password for apsit:
reading from file snort.log.1665475093, link-type EN10MB (Ethernet)
13:28:13.022821 IP6 :: > ff02::1:ffb9:cdd4: ICMP6, neighbor solicitation, who has fe80::88fc:daff:feb9:cdd4, length 32
13:28:13.061793 IP6 :: > ff02::16: HBH ICMP6, multicast listener report v2, 1 group record(s), length 28
13:28:13.065278 IP 0.0.0.0.bootpc > 255.255.255.255.bootps: BOOTP/DHCP, Request from 8a:fc:da:b9:cd:d4 (oui Unknown), length 310
13:28:13.601074 IP6 :: > ff02::16: HBH ICMP6, multicast listener report v2, 3 group record(s), length 68
13:28:13.620566 IP6 :: > ff02::16: HBH ICMP6, multicast listener report v2, 3 group record(s), length 68
13:28:13.658656 IP 0.0.0.0.bootpc > 255.255.255.255.bootps: BOOTP/DHCP, Request from b4:c4:fc:bd:af:40 (oui Unknown), length 308
13:28:13.710596 IP6 :: > ff02::1:ffa7:50c8: ICMP6, neighbor solicitation, who has fe80::ef08:dd61:7a7:50c8, length 24
13:28:13.720340 IP6 :: > ff02::16: HBH ICMP6, multicast listener report v2, 1 group record(s), length 28
13:28:14.666278 IP 0.0.0.0.bootpc > 255.255.255.255.bootps: BOOTP/DHCP, Request from b4:c4:fc:bd:af:40 (oui Unknown), length 320
13:28:21.324320 IP6 :: > ff02::1:ff64:9178: ICMP6, neighbor solicitation, who has fe80::17c7:1791:3764:9178, length 32
13:28:21.332924 IP6 :: > ff02::16: HBH ICMP6, multicast listener report v2, 1 group record(s), length 28
13:28:21.378653 IP 0.0.0.0.bootpc > 255.255.255.255.bootps: BOOTP/DHCP, Request from e8:5a:8b:66:59:33 (oui Unknown), length 312
13:28:21.413979 IP6 :: > ff02::16: HBH ICMP6, multicast listener report v2, 2 group record(s), length 48
13:28:21.563468 IP6 :: > ff02::1:ff25:31a0: ICMP6, neighbor solicitation, who has fe80::ef3:46ff:fe25:31a0, length 24
13:28:21.572766 IP6 :: > ff02::16: HBH ICMP6, multicast listener report v2, 1 group record(s), length 28
13:28:21.631284 IP6 :: > ff02::1:ff60:903a: ICMP6, neighbor solicitation, who has fe80::7e91:ef0f:3b60:903a, length 32
13:28:21.631527 IP6 :: > ff02::16: HBH ICMP6, multicast listener report v2, 1 group record(s), length 28
13:28:21.640176 IP 0.0.0.0.bootpc > 255.255.255.255.bootps: BOOTP/DHCP, Request from 4c:4f:ee:03:0e:c3 (oui Unknown), length 314
13:28:22.097607 IP6 :: > ff02::16: HBH ICMP6, multicast listener report v2, 1 group record(s), length 28
13:28:22.418323 IP6 :: > ff02::16: HBH ICMP6, multicast listener report v2, 1 group record(s), length 28
^C13:28:33.403532 IP6 :: > ff02::1:ff43:363: ICMP6, neighbor solicitation, who has fe80::18c4:8dff:fe43:363, length 32
```