Experiment 12

Study of Network security : Set up Snort and study the logs.

Roll No.	19
Name	Manav Jawrani
Class	D15-A
Subject	Security Lab
LO Mapped	LO6: Demonstrate the network security system using open source tools.

Aim: Study of Network security : Set up Snort and study the logs.

Introduction:

What is Snort?

Snort is an open source network intrusion detection system created Sourcefire founder and former CTO Martin Roesch. Cisco now develops and maintains Snort.

Snort is referred to as a packet sniffer that monitors network traffic, scrutinizing each packet closely to detect a dangerous payload or suspicious anomalies. Long a leader among enterprise intrusion prevention and detection tools, users can compile Snort on most Linux operating systems (OSes) or Unix. A version is also available for Windows.

How does Snort work?

Snort is based on library packet capture (libpcap). Libpcap is a tool that is widely used in Transmission Control Protocol/Internet Protocol address traffic sniffers, content searching and analyzers for packet logging, real-time traffic analysis, protocol analysis and content matching. Users can configure Snort as a sniffer, packet logger -- like TCPdump or Wireshark -- or network intrusion prevention methods.

Intrusion detection systems (IDS) vs. intrusion prevention systems (IPS)

Intrusion prevention system mode

As an open source network intrusion prevention system, Snort will monitor network traffic and compare it against a user-defined Snort rule set -- the file would be labeled snort.conf. This is Snort's most important function.

Snort applies rules to monitored traffic and issues alerts when it detects certain kinds of questionable activity on the network.

It can identify cybersecurity attack methods, including OS fingerprinting, denial of service, buffer overflow, common gateway interface attacks, stealth port scans and Server Message Block probes.

When Snort detects suspicious behavior, it acts as a firewall and sends a real-time alert to Syslog, to a separate alerts file or through a pop-up window.

Snort Modes:

Snort runs in three different modes:

1. Sniffer mode

2. Packet logger mode
3. Intrusion detection mode.

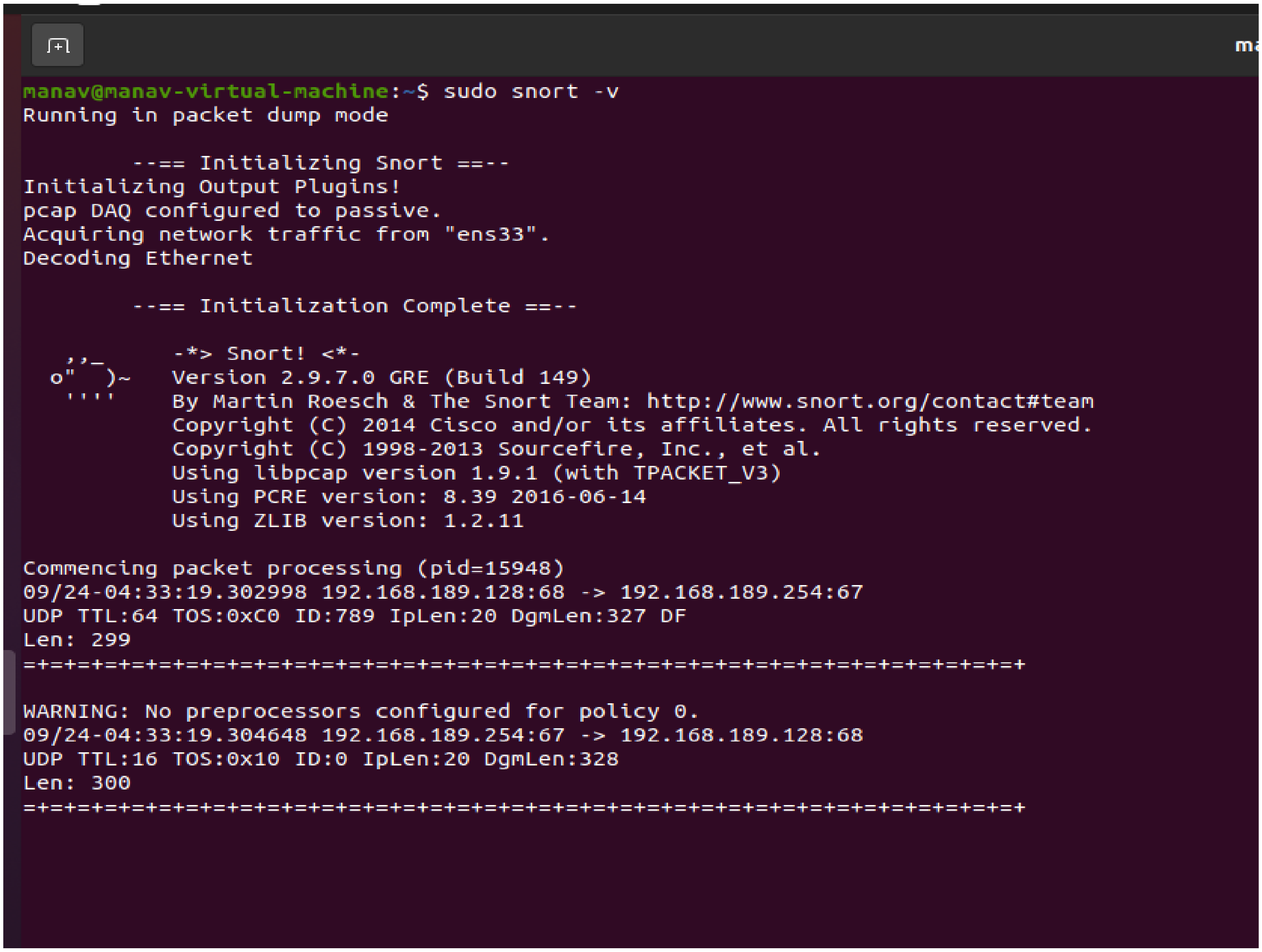
Packet logger and sniffer mode

If a subscriber configures Snort to operate as a sniffer, it will scan network packets and identify them. Snort can also log those packets to a disk file.

To use Snort as a packet sniffer, users set the host's network interface to promiscuous mode to monitor all network traffic on the local network interface. It then writes the monitored traffic to its console.

Installing snort on Ubuntu Machine:

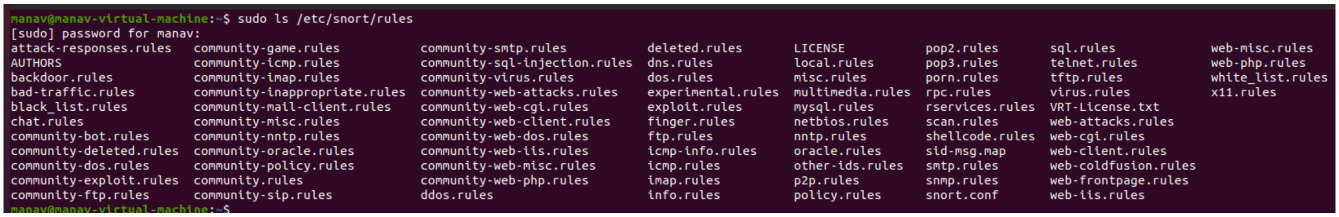
Use this website to install snort :
https://youtu.be/U6xMp-MIEfA
After successful installation you will see such a output:



```
manav@manav-virtual-machine:~$ sudo snort -v
Running in packet dump mode

        --== Initializing Snort ==--
Initializing Output Plugins!
pcap DAQ configured to passive.
Acquiring network traffic from "ens33".
Decoding Ethernet

        --== Initialization Complete ==--

   ,,_     -*> 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 1.9.1 (with TPACKET_V3)
           Using PCRE version: 8.39 2016-06-14
           Using ZLIB version: 1.2.11

Commencing packet processing (pid=15948)
09/24-04:33:19.302998 192.168.189.128:68 -> 192.168.189.254:67
UDP TTL:64 TOS:0xC0 ID:789 IpLen:20 DgmLen:327 DF
Len: 299
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

WARNING: No preprocessors configured for policy 0.
09/24-04:33:19.304648 192.168.189.254:67 -> 192.168.189.128:68
UDP TTL:16 TOS:0x10 ID:0 IpLen:20 DgmLen:328
Len: 300
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
```

Snort Rules:

Snort is a signature-based IDS, and it defines rules to detect the intrusions. All rules of Snort are stored under /etc/snort/rules directory. The screenshot below shows the files that contain rules of Snort.



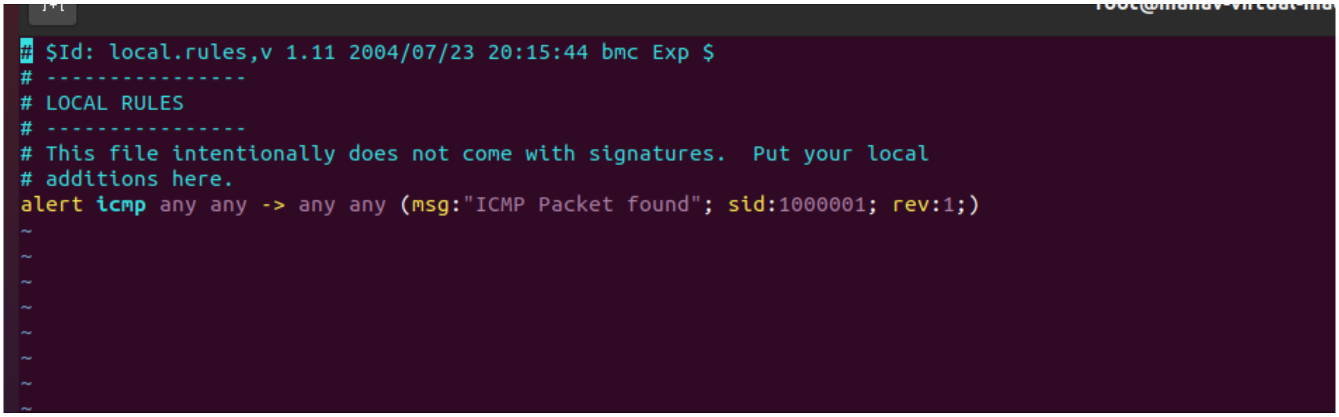
```
manav@manav-virtual-machine:~$ sudo ls /etc/snort/rules
[sudo] password for manav:
attack-responses.rules   community-game.rules           community-smtp.rules           deleted.rules       LICENSE           pop2.rules       sql.rules             web-misc.rules
AUTHORS                  community-icmp.rules           community-sql-injection.rules  dns.rules           local.rules       pop3.rules       telnet.rules          web-php.rules
backdoor.rules           community-imap.rules           community-virus.rules          dos.rules           misc.rules        porn.rules       tftp.rules            white_list.rules
bad-traffic.rules        community-inappropriate.rules  community-web-attacks.rules    experimental.rules  multimedia.rules  rpc.rules        virus.rules           x11.rules
black_list.rules         community-mail-client.rules    community-web-cgi.rules        exploit.rules       mysql.rules       rservices.rules  VRT-License.txt
chat.rules               community-misc.rules           community-web-client.rules     finger.rules        netbios.rules     scan.rules       web-attacks.rules
community-bot.rules      community-nntp.rules           community-web-dos.rules        ftp.rules           nntp.rules        shellcode.rules  web-cgi.rules
community-deleted.rules  community-oracle.rules         community-web-iis.rules        icmp-info.rules     oracle.rules      sid-msg.map      web-client.rules
community-dos.rules      community-policy.rules         community-web-misc.rules       icmp.rules          other-ids.rules   smtp.rules       web-coldfusion.rules
community-exploit.rules  community.rules                community-web-php.rules        imap.rules          p2p.rules         snmp.rules       web-frontpage.rules
community-ftp.rules      community-sip.rules            ddos.rules                     info.rules          policy.rules      snort.conf       web-iis.rules
manav@manav-virtual-machine:~$
```

Writing and Adding a Snort Rule:

Next, we are going to add a simple snort rule. You should add your own rules at /etc/snort/rules/local.rules. Add the following line into the local.rules file

alert icmp any any -> any any (msg:"ICMP Packet found"; sid:1000001; rev:1;)

Basically, this rule defines that an alert will be logged if an ICMP packet is found. The ICMP packet could be from any IP address and the rule ID is 1000001. Make sure to pick a SID greater than 1000000 for your own rules. The screenshot below shows the contents of the local.rules file after adding the rule.



```
# $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 -> any any (msg:"ICMP Packet found"; sid:1000001; rev:1;)
~
~
~
~
~
~
~
~
```

To make the rule become effective, you need to restart the snort service by typing the following command.

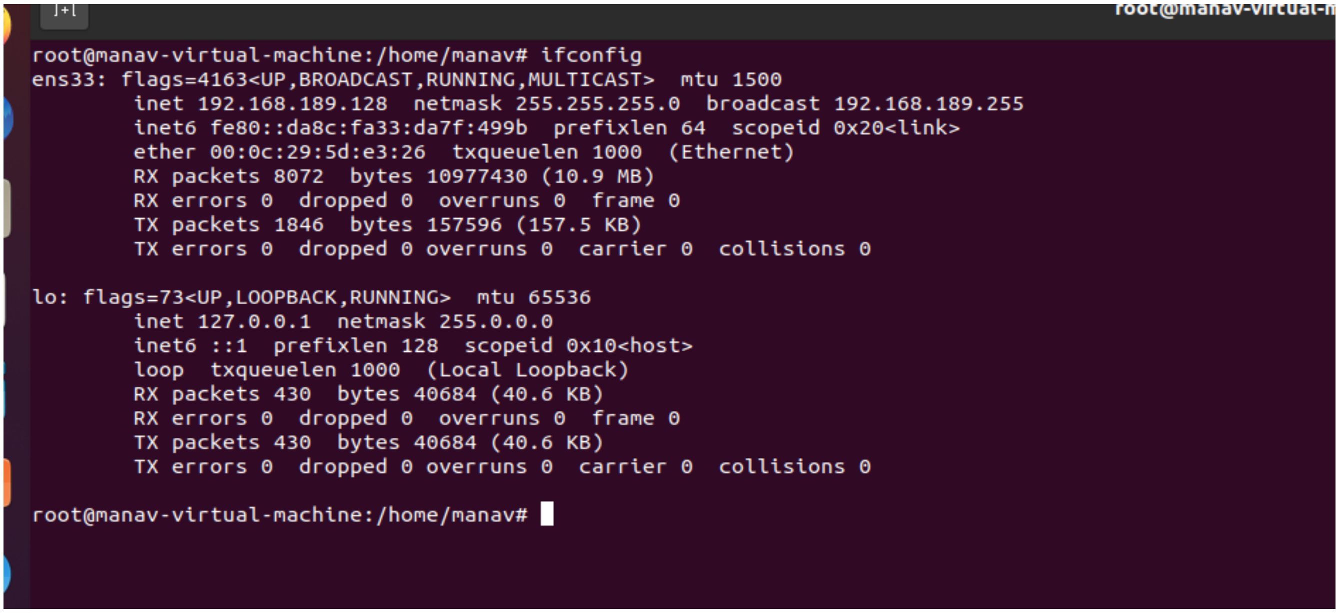
$ service snort restart

Triggering an Alert for the New Rule:

To trigger an alert for the new rule, you only need to send an ICMP message to the VM image wheresnort runs. First, you need to find the IP address of the VM by typing the following command.

$ ifconfig

For instance, the screenshot shows the execution result on my VM image, and the IP address is 192.168.189.128



```
root@manav-virtual-machine:/home/manav# ifconfig
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.189.128  netmask 255.255.255.0  broadcast 192.168.189.255
        inet6 fe80::da8c:fa33:da7f:499b  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:5d:e3:26  txqueuelen 1000  (Ethernet)
        RX packets 8072  bytes 10977430 (10.9 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 1846  bytes 157596 (157.5 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 430  bytes 40684 (40.6 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 430  bytes 40684 (40.6 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

root@manav-virtual-machine:/home/manav# 
```

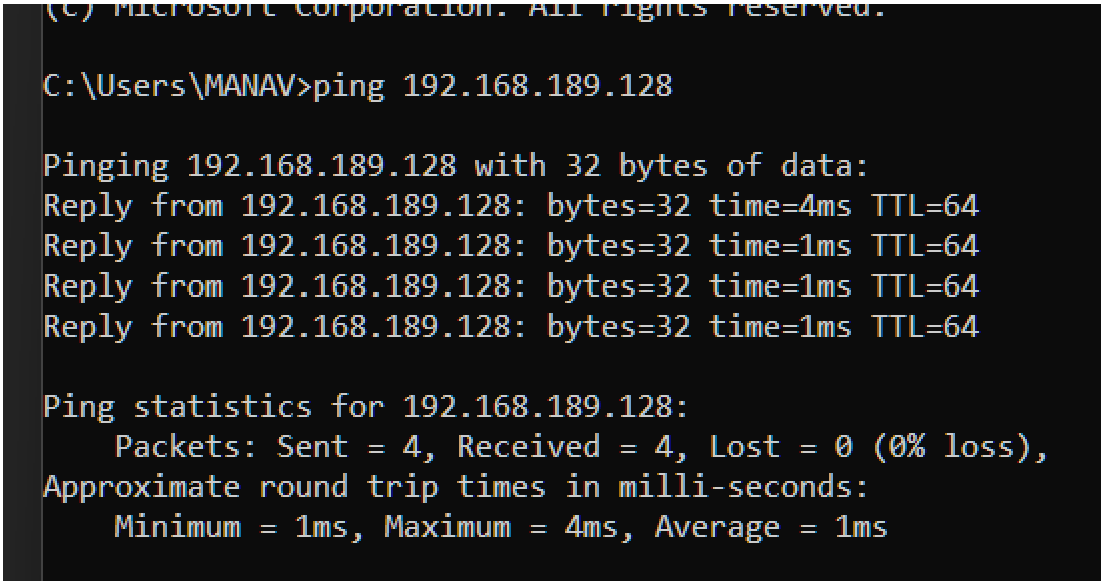
Next, you can open a terminal in your host. If you host is a Windows OS, you can use one of the following two ways to open a terminal

1. Press "Win-R" type "cmd" and press "Enter" to open a Command Prompt session using just your keyboard.

2. Click the "Start | Program Files | Accessories | Command Prompt" to open a Command Prompt session using just your mouse.

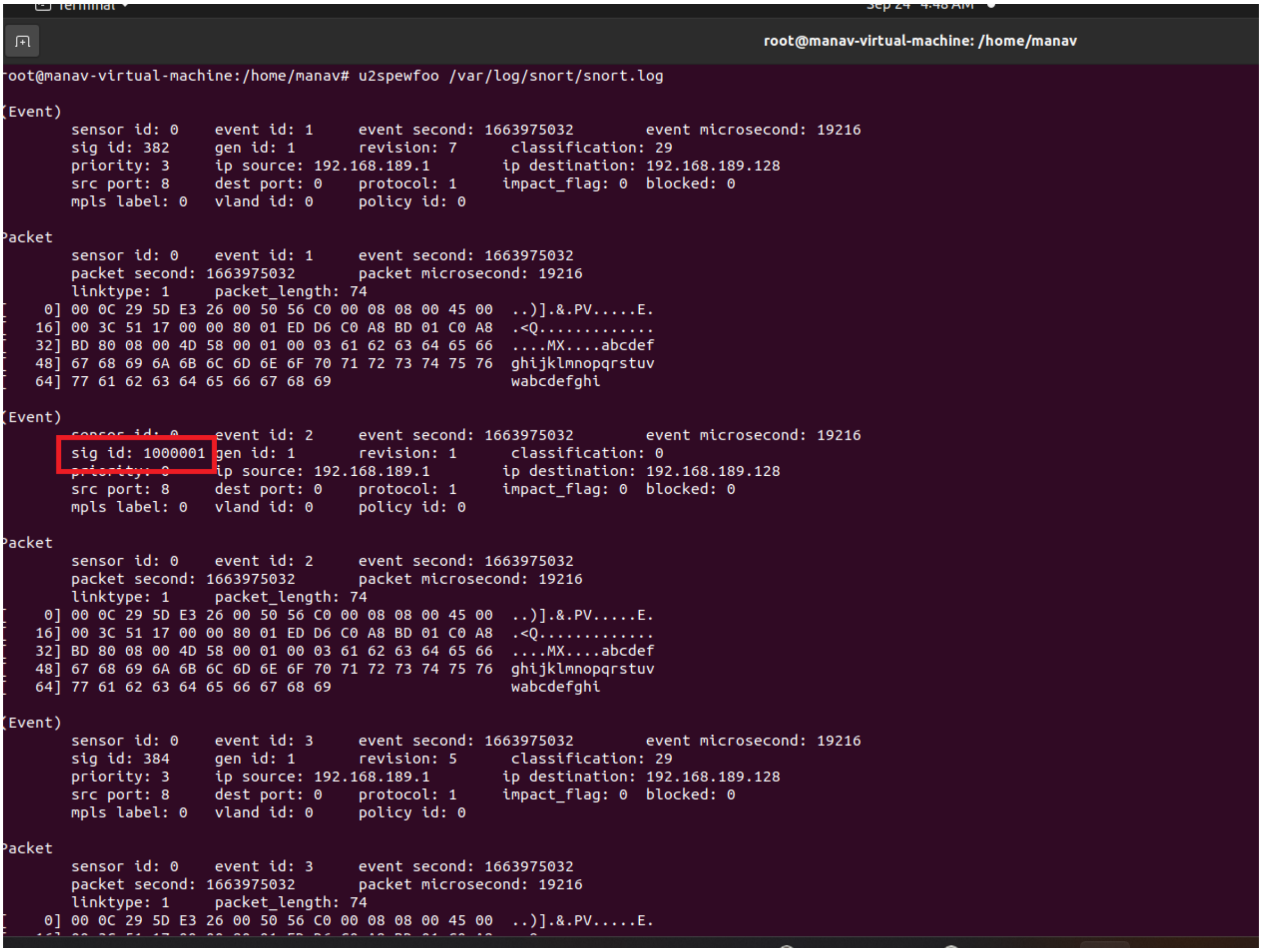
After you have a terminal, you can just type the following command to send ping messages to the VM.

$ ping 192.168.189.128



```
(c) Microsoft Corporation. All rights reserved.

C:\Users\MANAV>ping 192.168.189.128

Pinging 192.168.189.128 with 32 bytes of data:
Reply from 192.168.189.128: bytes=32 time=4ms TTL=64
Reply from 192.168.189.128: bytes=32 time=1ms TTL=64
Reply from 192.168.189.128: bytes=32 time=1ms TTL=64
Reply from 192.168.189.128: bytes=32 time=1ms TTL=64

Ping statistics for 192.168.189.128:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 4ms, Average = 1ms
```

After you send the ping messages, the alerts should be triggered and you can find the log messages in /var/log/snort/snort.log. However, the snort.log file will be binary format. You need to use a tool, called u2spewfoo, to read it. The screenshot below shows the result of reading the snort alerts.



```
root@manav-virtual-machine:/home/manav# u2spewfoo /var/log/snort/snort.log

(Event)
        sensor id: 0    event id: 1     event second: 1663975032        event microsecond: 19216
        sig id: 382     gen id: 1       revision: 7      classification: 29
        priority: 3     ip source: 192.168.189.1        ip destination: 192.168.189.128
        src port: 8     dest port: 0    protocol: 1     impact_flag: 0  blocked: 0
        mpls label: 0   vland id: 0     policy id: 0

Packet
        sensor id: 0    event id: 1     event second: 1663975032
        packet second: 1663975032       packet microsecond: 19216
        linktype: 1     packet_length: 74
[    0] 00 0C 29 5D E3 26 00 50 56 C0 00 08 08 00 45 00  ..)].&.PV.....E.
[   16] 00 3C 51 17 00 00 80 01 ED D6 C0 A8 BD 01 C0 A8  .<Q.............
[   32] BD 80 08 00 4D 58 00 01 00 03 61 62 63 64 65 66  ....MX....abcdef
[   48] 67 68 69 6A 6B 6C 6D 6E 6F 70 71 72 73 74 75 76  ghijklmnopqrstuv
[   64] 77 61 62 63 64 65 66 67 68 69                    wabcdefghi

(Event)
        sensor id: 0    event id: 2     event second: 1663975032        event microsecond: 19216
        sig id: 1000001 gen id: 1       revision: 1      classification: 0
        priority: 0     ip source: 192.168.189.1        ip destination: 192.168.189.128
        src port: 8     dest port: 0    protocol: 1     impact_flag: 0  blocked: 0
        mpls label: 0   vland id: 0     policy id: 0

Packet
        sensor id: 0    event id: 2     event second: 1663975032
        packet second: 1663975032       packet microsecond: 19216
        linktype: 1     packet_length: 74
[    0] 00 0C 29 5D E3 26 00 50 56 C0 00 08 08 00 45 00  ..)].&.PV.....E.
[   16] 00 3C 51 17 00 00 80 01 ED D6 C0 A8 BD 01 C0 A8  .<Q.............
[   32] BD 80 08 00 4D 58 00 01 00 03 61 62 63 64 65 66  ....MX....abcdef
[   48] 67 68 69 6A 6B 6C 6D 6E 6F 70 71 72 73 74 75 76  ghijklmnopqrstuv
[   64] 77 61 62 63 64 65 66 67 68 69                    wabcdefghi

(Event)
        sensor id: 0    event id: 3     event second: 1663975032        event microsecond: 19216
        sig id: 384     gen id: 1       revision: 5      classification: 29
        priority: 3     ip source: 192.168.189.1        ip destination: 192.168.189.128
        src port: 8     dest port: 0    protocol: 1     impact_flag: 0  blocked: 0
        mpls label: 0   vland id: 0     policy id: 0

Packet
        sensor id: 0    event id: 3     event second: 1663975032
        packet second: 1663975032       packet microsecond: 19216
        linktype: 1     packet_length: 74
[    0] 00 0C 29 5D E3 26 00 50 56 C0 00 08 08 00 45 00  ..)].&.PV.....E.
```

You can see that the SID is 1000001, and the alerts are generated by the ICMP messages.

Conclusion:

Thus, we have successfully set up snort and studied the logs in a network security.