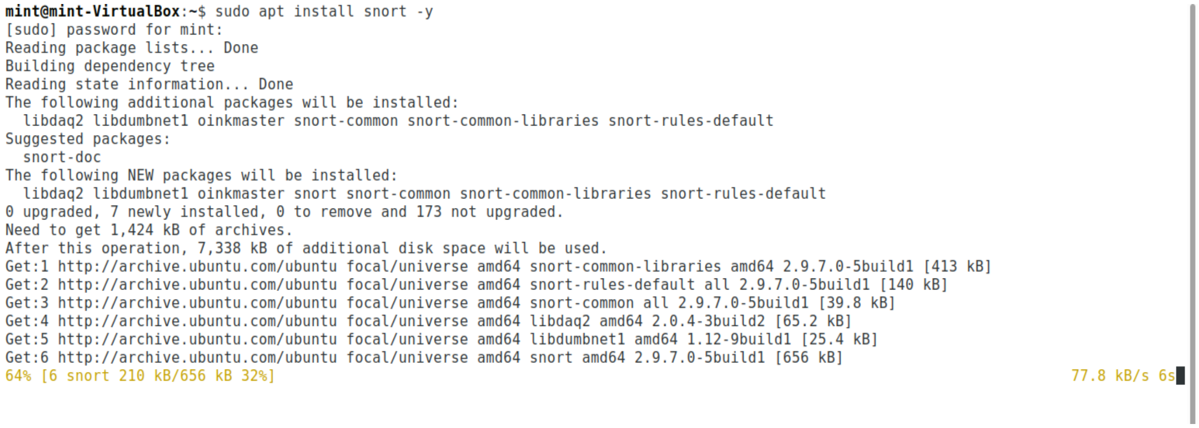
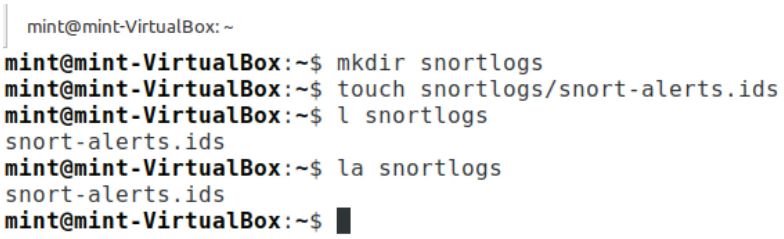
OUTPUT

Install snort package on the Linux virtual machine / Computer



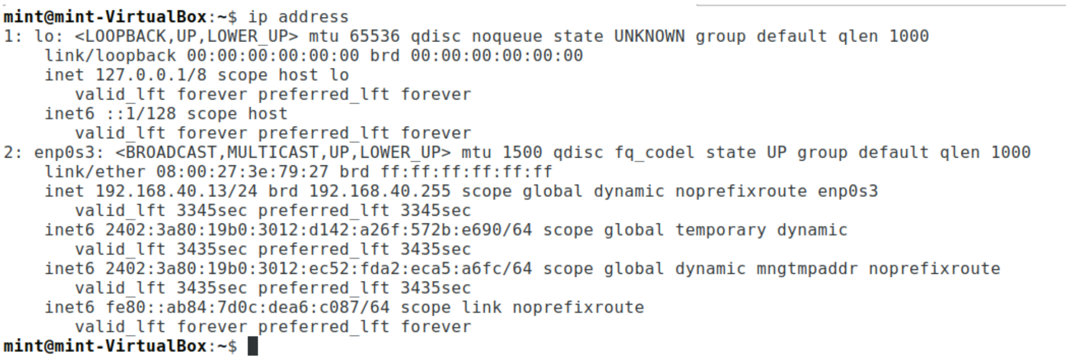
```
mint@mint-VirtualBox:~$ sudo apt install snort -y
[sudo] password for mint:
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  libdaq2 libdumbnet1 oinkmaster snort-common snort-common-libraries snort-rules-default
Suggested packages:
  snort-doc
The following NEW packages will be installed:
  libdaq2 libdumbnet1 oinkmaster snort snort-common snort-common-libraries snort-rules-default
0 upgraded, 7 newly installed, 0 to remove and 173 not upgraded.
Need to get 1,424 kB of archives.
After this operation, 7,338 kB of additional disk space will be used.
Get:1 http://archive.ubuntu.com/ubuntu focal/universe amd64 snort-common-libraries amd64 2.9.7.0-5build1 [413 kB]
Get:2 http://archive.ubuntu.com/ubuntu focal/universe amd64 snort-rules-default all 2.9.7.0-5build1 [140 kB]
Get:3 http://archive.ubuntu.com/ubuntu focal/universe amd64 snort-common all 2.9.7.0-5build1 [39.8 kB]
Get:4 http://archive.ubuntu.com/ubuntu focal/universe amd64 libdaq2 amd64 2.0.4-3build2 [65.2 kB]
Get:5 http://archive.ubuntu.com/ubuntu focal/universe amd64 libdumbnet1 amd64 1.12-9build1 [25.4 kB]
Get:6 http://archive.ubuntu.com/ubuntu focal/universe amd64 snort amd64 2.9.7.0-5build1 [656 kB]
64% [6 snort 210 kB/656 kB 32%]                                                                    77.8 kB/s 6s
```

Create a folder for logging the alerts as snort is a IDS logging is its core functionality.



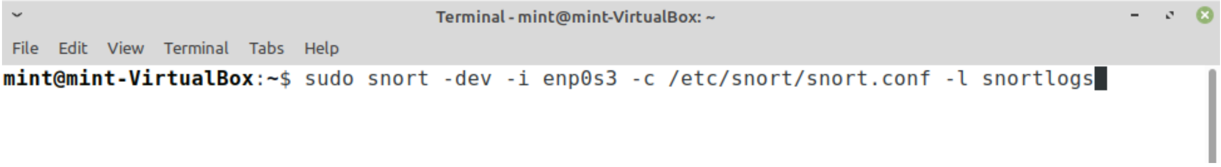
```
mint@mint-VirtualBox: ~
mint@mint-VirtualBox:~$ mkdir snortlogs
mint@mint-VirtualBox:~$ touch snortlogs/snort-alerts.ids
mint@mint-VirtualBox:~$ l snortlogs
snort-alerts.ids
mint@mint-VirtualBox:~$ la snortlogs
snort-alerts.ids
mint@mint-VirtualBox:~$
```

with “IP address” command check the interface for NIC added to machine (Virtual Machine).



```
mint@mint-VirtualBox:~$ ip address
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:3e:79:27 brd ff:ff:ff:ff:ff:ff
    inet 192.168.40.13/24 brd 192.168.40.255 scope global dynamic noprefixroute enp0s3
       valid_lft 3345sec preferred_lft 3345sec
    inet6 2402:3a80:19b0:3012:d142:a26f:572b:e690/64 scope global temporary dynamic
       valid_lft 3435sec preferred_lft 3435sec
    inet6 2402:3a80:19b0:3012:ec52:fda2:eca5:a6fc/64 scope global dynamic mngtmpaddr noprefixroute
       valid_lft 3435sec preferred_lft 3435sec
    inet6 fe80::ab84:7d0c:dea6:c087/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
mint@mint-VirtualBox:~$
```

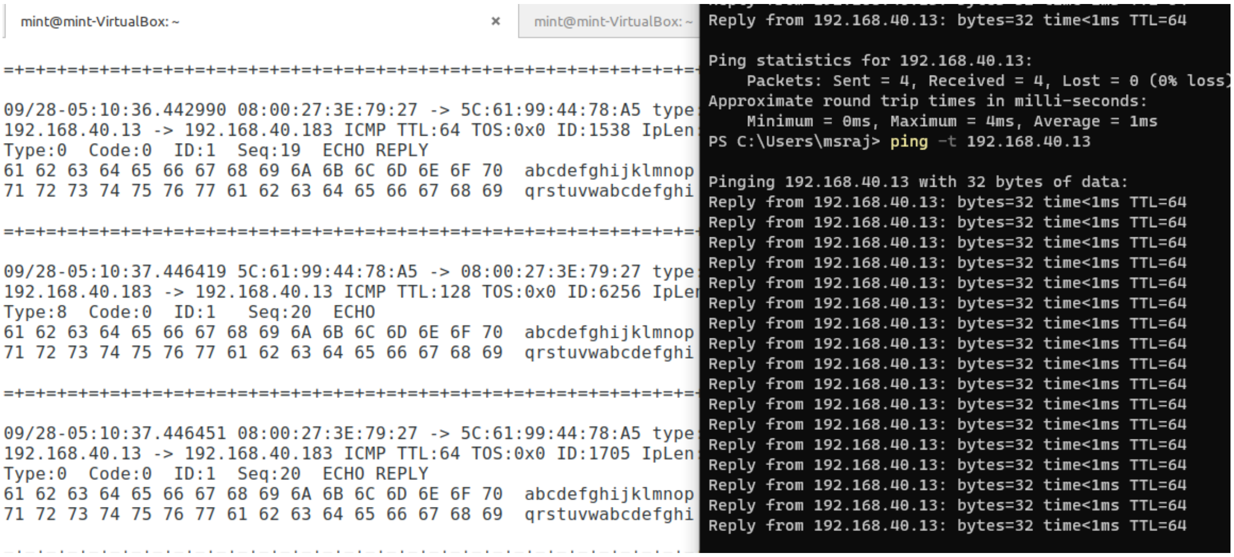
Start the snort Monitoring with the following command,


Terminal - mint@mint-VirtualBox: ~
File Edit View Terminal Tabs Help

```
mint@mint-VirtualBox:~$ sudo snort -dev -i enp0s3 -c /etc/snort/snort.conf -l snortlogs
```

(FLOODING - METHOD 1 USING PING COMMAND)

Open another machine that is connected to virtual machine and open command line and try pinging the virtual machine with snort running,



```
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=

09/28-05:10:36.442990 08:00:27:3E:79:27 -> 5C:61:99:44:78:A5 type
192.168.40.13 -> 192.168.40.183 ICMP TTL:64 TOS:0x0 ID:1538 IpLen
Type:0  Code:0  ID:1   Seq:19  ECHO REPLY
61 62 63 64 65 66 67 68 69 6A 6B 6C 6D 6E 6F 70  abcdefghijklmnop
71 72 73 74 75 76 77 61 62 63 64 65 66 67 68 69  qrstuvwabcdefghi

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=

09/28-05:10:37.446419 5C:61:99:44:78:A5 -> 08:00:27:3E:79:27 type
192.168.40.183 -> 192.168.40.13 ICMP TTL:128 TOS:0x0 ID:6256 IpLen
Type:8  Code:0  ID:1   Seq:20  ECHO
61 62 63 64 65 66 67 68 69 6A 6B 6C 6D 6E 6F 70  abcdefghijklmnop
71 72 73 74 75 76 77 61 62 63 64 65 66 67 68 69  qrstuvwabcdefghi

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=

09/28-05:10:37.446451 08:00:27:3E:79:27 -> 5C:61:99:44:78:A5 type
192.168.40.13 -> 192.168.40.183 ICMP TTL:64 TOS:0x0 ID:1705 IpLen
Type:0  Code:0  ID:1   Seq:20  ECHO REPLY
61 62 63 64 65 66 67 68 69 6A 6B 6C 6D 6E 6F 70  abcdefghijklmnop
71 72 73 74 75 76 77 61 62 63 64 65 66 67 68 69  qrstuvwabcdefghi
```

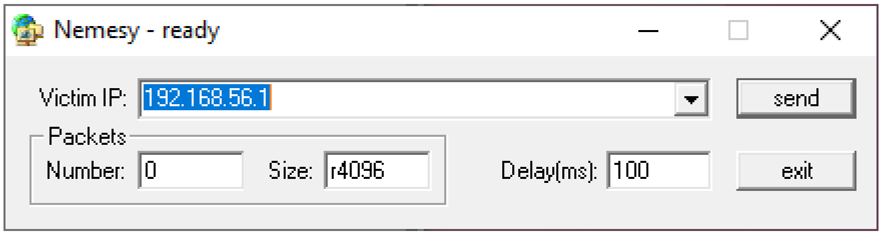
```
Reply from 192.168.40.13: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.40.13:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss)
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 4ms, Average = 1ms
PS C:\Users\msraj> ping -t 192.168.40.13

Pinging 192.168.40.13 with 32 bytes of data:
Reply from 192.168.40.13: bytes=32 time<1ms TTL=64
Reply from 192.168.40.13: bytes=32 time<1ms TTL=64
Reply from 192.168.40.13: bytes=32 time<1ms TTL=64
Reply from 192.168.40.13: bytes=32 time<1ms TTL=64
Reply from 192.168.40.13: bytes=32 time<1ms TTL=64
Reply from 192.168.40.13: bytes=32 time<1ms TTL=64
Reply from 192.168.40.13: bytes=32 time<1ms TTL=64
Reply from 192.168.40.13: bytes=32 time<1ms TTL=64
Reply from 192.168.40.13: bytes=32 time<1ms TTL=64
Reply from 192.168.40.13: bytes=32 time<1ms TTL=64
Reply from 192.168.40.13: bytes=32 time<1ms TTL=64
Reply from 192.168.40.13: bytes=32 time<1ms TTL=64
Reply from 192.168.40.13: bytes=32 time<1ms TTL=64
Reply from 192.168.40.13: bytes=32 time<1ms TTL=64
Reply from 192.168.40.13: bytes=32 time<1ms TTL=64
Reply from 192.168.40.13: bytes=32 time<1ms TTL=64
Reply from 192.168.40.13: bytes=32 time<1ms TTL=64
```

(FLOODING – METHOD 2 USING NEMESY TOOL)

Download and run Nemesy Tool, → open Nemesy → Enter Ip address to Attack → Click “Send” Button.



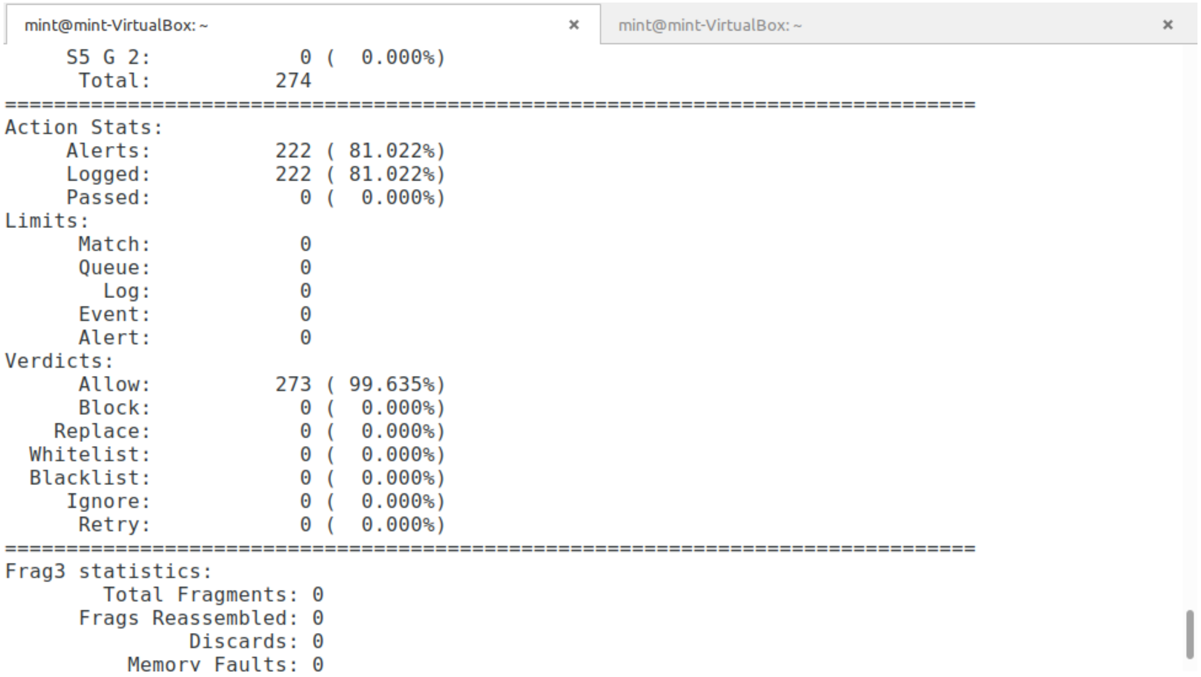
Victim IP: 192.168.56.1

Packets
Number: 0
Size: r4096

Delay(ms): 100

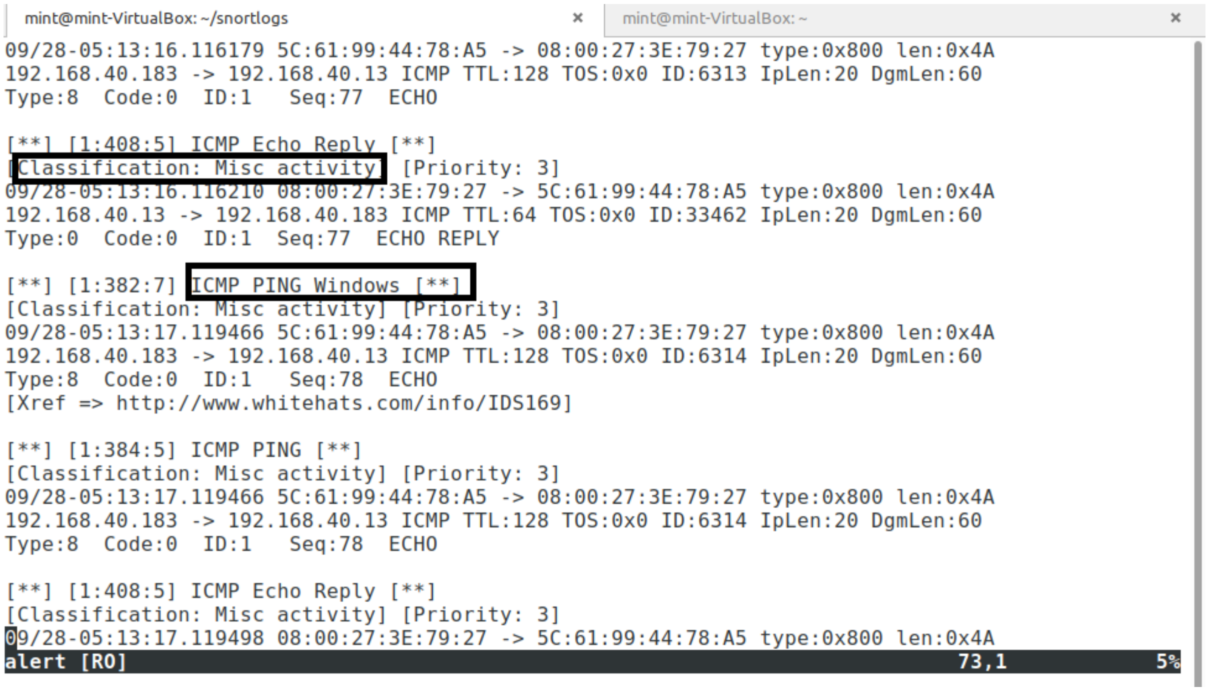
Regardless of the tools used both methods results in alerts, thus logged by snort IDS.

Stop the snort IDS and it gives a brief summary



```
     S5 G 2:            0 (  0.000%)
      Total:          274
===============================================================================
Action Stats:
     Alerts:          222 ( 81.022%)
     Logged:          222 ( 81.022%)
     Passed:            0 (  0.000%)
Limits:
      Match:            0
      Queue:            0
        Log:            0
      Event:            0
      Alert:            0
Verdicts:
      Allow:          273 ( 99.635%)
      Block:            0 (  0.000%)
    Replace:            0 (  0.000%)
  Whitelist:            0 (  0.000%)
  Blacklist:            0 (  0.000%)
     Ignore:            0 (  0.000%)
      Retry:            0 (  0.000%)
===============================================================================
Frag3 statistics:
        Total Fragments: 0
      Frags Reassembled: 0
               Discards: 0
          Memory Faults: 0
```

Now check the previously created “snortlogs” folder and check for alerts / alerts.ids file



```
09/28-05:13:16.116179 5C:61:99:44:78:A5 -> 08:00:27:3E:79:27 type:0x800 len:0x4A
192.168.40.183 -> 192.168.40.13 ICMP TTL:128 TOS:0x0 ID:6313 IpLen:20 DgmLen:60
Type:8  Code:0  ID:1   Seq:77  ECHO

[**] [1:408:5] ICMP Echo Reply [**]
[Classification: Misc activity] [Priority: 3]
09/28-05:13:16.116210 08:00:27:3E:79:27 -> 5C:61:99:44:78:A5 type:0x800 len:0x4A
192.168.40.13 -> 192.168.40.183 ICMP TTL:64 TOS:0x0 ID:33462 IpLen:20 DgmLen:60
Type:0  Code:0  ID:1  Seq:77  ECHO REPLY

[**] [1:382:7] ICMP PING Windows [**]
[Classification: Misc activity] [Priority: 3]
09/28-05:13:17.119466 5C:61:99:44:78:A5 -> 08:00:27:3E:79:27 type:0x800 len:0x4A
192.168.40.183 -> 192.168.40.13 ICMP TTL:128 TOS:0x0 ID:6314 IpLen:20 DgmLen:60
Type:8  Code:0  ID:1   Seq:78  ECHO
[Xref => http://www.whitehats.com/info/IDS169]

[**] [1:384:5] ICMP PING [**]
[Classification: Misc activity] [Priority: 3]
09/28-05:13:17.119466 5C:61:99:44:78:A5 -> 08:00:27:3E:79:27 type:0x800 len:0x4A
192.168.40.183 -> 192.168.40.13 ICMP TTL:128 TOS:0x0 ID:6314 IpLen:20 DgmLen:60
Type:8  Code:0  ID:1   Seq:78  ECHO

[**] [1:408:5] ICMP Echo Reply [**]
[Classification: Misc activity] [Priority: 3]
09/28-05:13:17.119498 08:00:27:3E:79:27 -> 5C:61:99:44:78:A5 type:0x800 len:0x4A
alert [RO]                                                              73,1           5%
```