CSEC 744 Network Security

Name : Shriram Karpoora Sundara Pandian Course

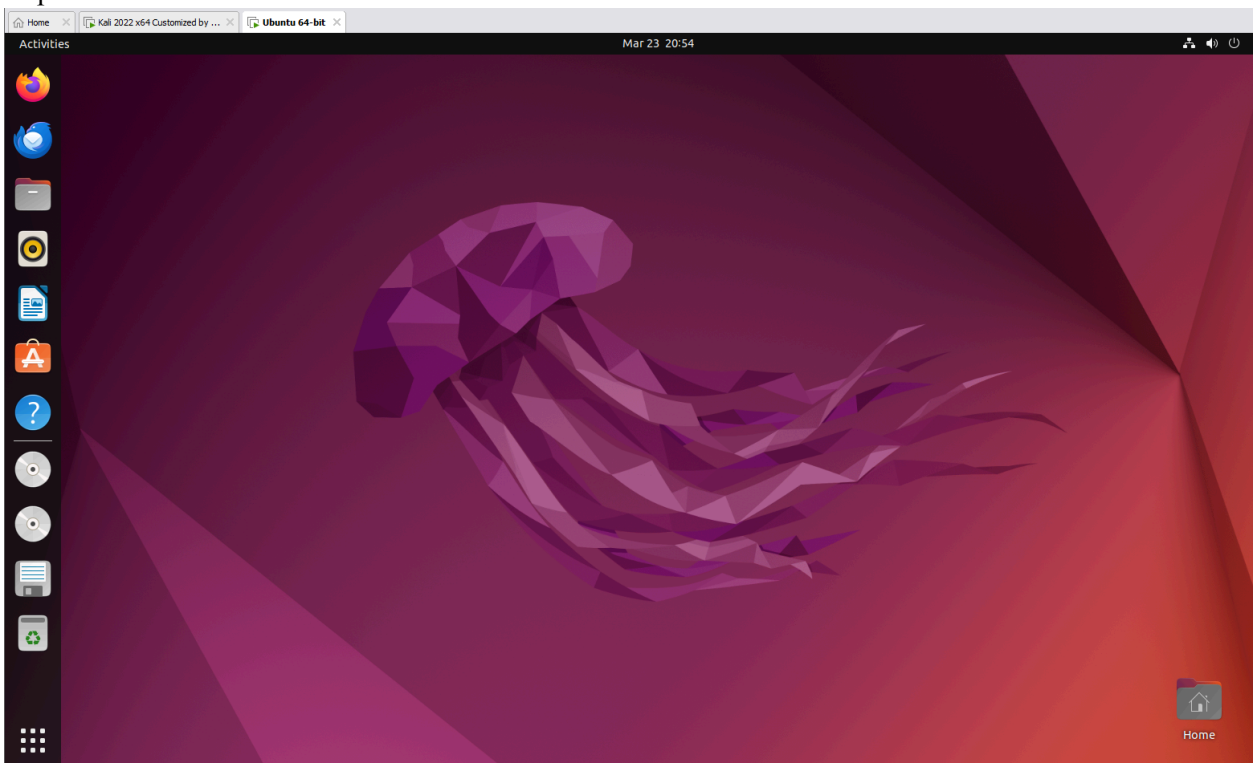
Title : Intrusion Detection Systems

Lab : 7

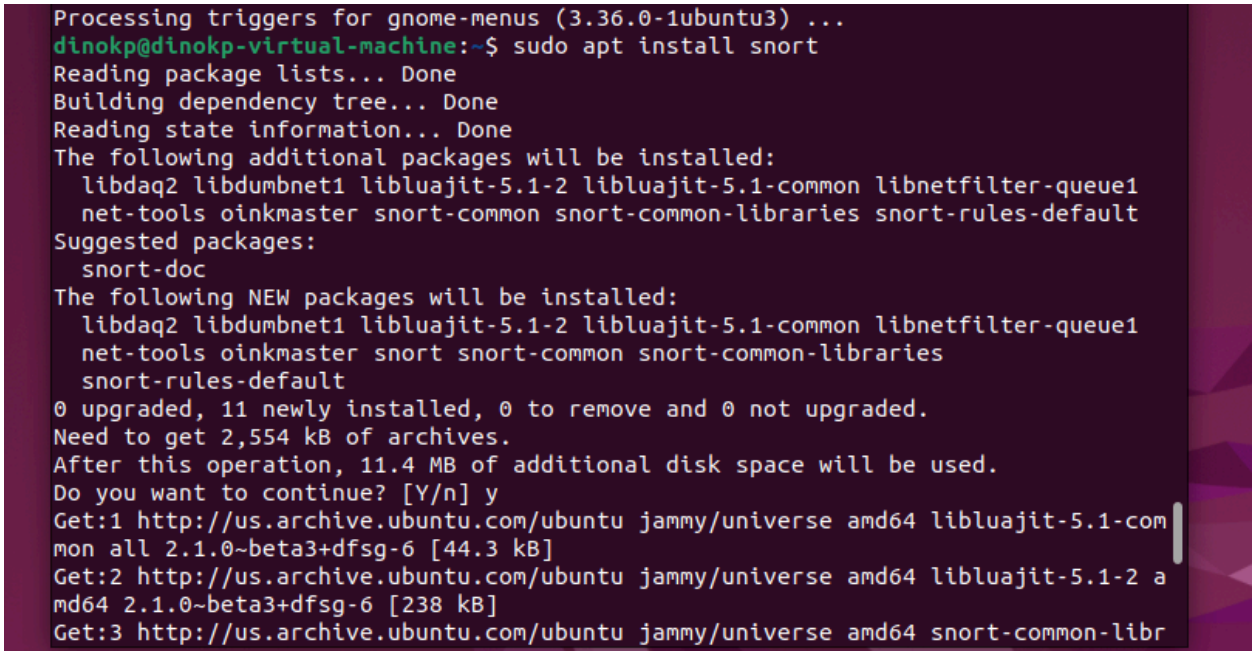
Chapter : 13 (SecurityPlus)

Exercise 13. 01 :

Step 1 :

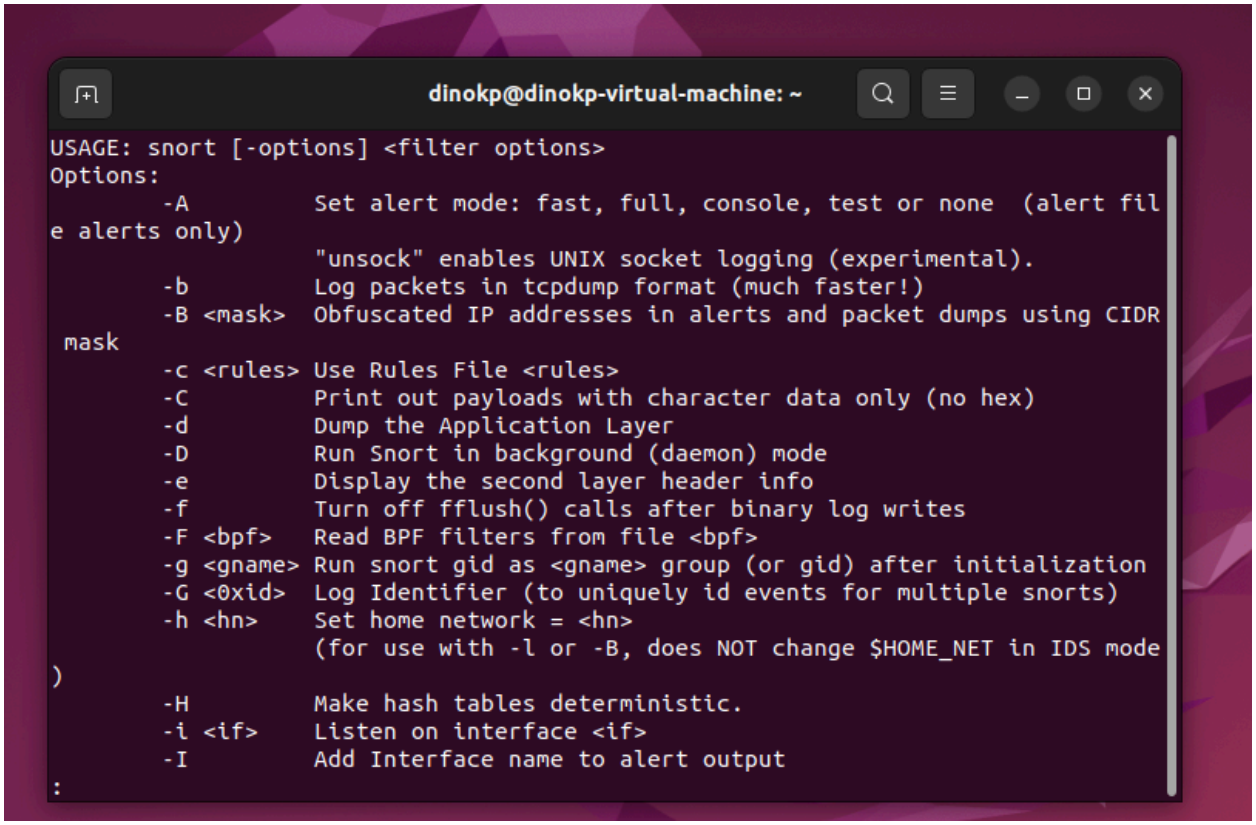


Step 2 :



Exercise 13. 02 :

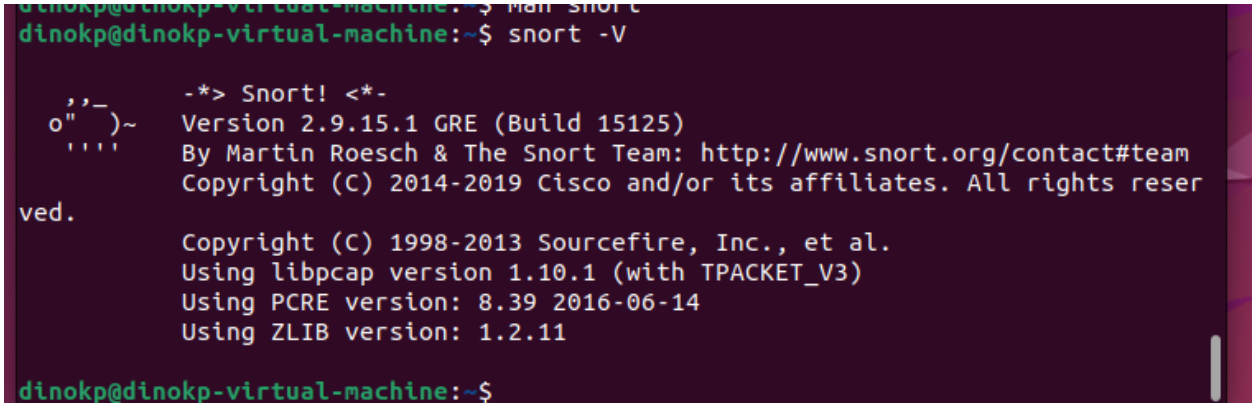
A.



B.


dinokp@dinokp-virtual-machine: ~
DESCRIPTION
Snort is an open source network intrusion detection 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. Snort uses a flexible rules language to describe traffic that it should collect or pass, as well as a detection engine that utilizes a modular plugin architecture. Snort also has a modular real-time alerting capability, incorporating alerting and logging plugins for syslog, a ASCII text files, UNIX sockets or XML.
Snort has three primary uses. It can be used as a straight packet sniffer like tcpdump(1), a packet logger (useful for network traffic debugging, etc), or as a full blown network intrusion detection system.
Snort logs packets in tcpdump(1) binary format or in Snort's decoded ASCII format to a hierarchy of logging directories that are named based on the IP address of the "foreign" host.
OPTIONS
-A alert-mode
Manual page snort(8) line 31 (press h for help or q to quit)

C.


dinokp@dinokp-virtual-machine:~$ snort -V
-*> Snort! <*-
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
dinokp@dinokp-virtual-machine:~$

Step 2 :

A.

```
dinokp@dinokp-virtual-machine:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group defaul
t 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: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP gro
up default qlen 1000
    link/ether 00:0c:29:bf:2a:83 brd ff:ff:ff:ff:ff:ff
    altname enp2s1
    inet 192.168.32.136/24 brd 192.168.32.255 scope global dynamic noprefixroute
 ens33
       valid_lft 1417sec preferred_lft 1417sec
    inet6 fe80::81ac:978b:40a8:b288/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
dinokp@dinokp-virtual-machine:~$
```

B.

```
Decoding Ethernet

        --== 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 reser
ved.
           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

Commencing packet processing (pid=18471)
WARNING: No preprocessors configured for policy 0.
03/23-21:14:38.902406 192.168.32.128:51590 -> 5.78.62.36:123
UDP TTL:64 TOS:0x10 ID:52548 IpLen:20 DgmLen:76 DF
Len: 48
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

WARNING: No preprocessors configured for policy 0.
03/23-21:14:38.984041 5.78.62.36:123 -> 192.168.32.128:51590
UDP TTL:128 TOS:0x0 ID:33371 IpLen:20 DgmLen:76
```

C.

```
03/23-21:19:06.558191 192.168.32.128 -> 192.168.32.136
ICMP TTL:64 TOS:0x0 ID:44424 IpLen:20 DgmLen:84 DF
Type:8  Code:0  ID:8420   Seq:7  ECHO
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

WARNING: No preprocessors configured for policy 0.
03/23-21:19:06.558233 192.168.32.136 -> 192.168.32.128
ICMP TTL:64 TOS:0x0 ID:22605 IpLen:20 DgmLen:84
Type:0  Code:0  ID:8420  Seq:7  ECHO REPLY
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

WARNING: No preprocessors configured for policy 0.
03/23-21:19:07.557912 192.168.32.128 -> 192.168.32.136
ICMP TTL:64 TOS:0x0 ID:44531 IpLen:20 DgmLen:84 DF
Type:8  Code:0  ID:8420   Seq:8  ECHO
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

WARNING: No preprocessors configured for policy 0.
03/23-21:19:07.557954 192.168.32.136 -> 192.168.32.128
ICMP TTL:64 TOS:0x0 ID:22615 IpLen:20 DgmLen:84
Type:0  Code:0  ID:8420  Seq:8  ECHO REPLY
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
```

D.

```
03/23-21:21:04.067782 127.0.0.1 -> 127.0.0.1
ICMP TTL:64 TOS:0x0 ID:55758 IpLen:20 DgmLen:84 DF
Type:8  Code:0  ID:1   Seq:5  ECHO
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

WARNING: No preprocessors configured for policy 0.
03/23-21:21:04.067799 127.0.0.1 -> 127.0.0.1
ICMP TTL:64 TOS:0x0 ID:55759 IpLen:20 DgmLen:84
Type:0  Code:0  ID:1  Seq:5  ECHO REPLY
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

WARNING: No preprocessors configured for policy 0.
03/23-21:21:05.091901 127.0.0.1 -> 127.0.0.1
ICMP TTL:64 TOS:0x0 ID:55860 IpLen:20 DgmLen:84 DF
Type:8  Code:0  ID:1   Seq:6  ECHO
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

WARNING: No preprocessors configured for policy 0.
03/23-21:21:05.091928 127.0.0.1 -> 127.0.0.1
ICMP TTL:64 TOS:0x0 ID:55861 IpLen:20 DgmLen:84
Type:0  Code:0  ID:1  Seq:6  ECHO REPLY
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
```

Step 3 :

A.

```
Len: 300
02 01 06 00 A9 72 25 52 00 01 00 00 C0 A8 20 80  .....r%R...... .
C0 A8 20 80 C0 A8 20 FE 00 00 00 00 00 0C 29 5B  .. ... .......)[
31 51 00 00 00 00 00 00 00 00 00 00 00 00 00 00  1Q..............
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 63 82 53 63  ............c.Sc
35 01 05 36 04 C0 A8 20 FE 33 04 00 00 07 08 01  5..6... .3......
04 FF FF FF 00 06 04 C0 A8 20 02 0F 0B 6C 6F 63  ......... ...loc
61 6C 64 6F 6D 61 69 6E 1C 04 C0 A8 20 FF 03 04  aldomain.... ...
C0 A8 20 02 FF 00 00 00 00 00 00 00              .. .........

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

WARNING: No preprocessors configured for policy 0.
WARNING: No preprocessors configured for policy 0.
```

B.


gmLen:202
Len: 174
WARNING: No preprocessors configured for policy 0.
03/23-21:24:54.473012 00:50:56:C0:00:08 -> 01:00:5E:7F:FF:FA type:0x800 len:0xD9
192.168.32.1:53020 -> 239.255.255.250:1900 UDP TTL:1 TOS:0x0 ID:36269 IpLen:20 D
gmLen:203
Len: 175
WARNING: No preprocessors configured for policy 0.
03/23-21:24:55.302684 00:50:56:C0:00:08 -> 01:00:5E:7F:FF:FA type:0x800 len:0xD8
192.168.32.1:53016 -> 239.255.255.250:1900 UDP TTL:1 TOS:0x0 ID:36270 IpLen:20 D
gmLen:202
Len: 174
WARNING: No preprocessors configured for policy 0.
03/23-21:24:55.472628 00:50:56:C0:00:08 -> 01:00:5E:7F:FF:FA type:0x800 len:0xD9
192.168.32.1:53020 -> 239.255.255.250:1900 UDP TTL:1 TOS:0x0 ID:36271 IpLen:20 D
gmLen:203
Len: 175
WARNING: No preprocessors configured for policy 0.
WARNING: No preprocessors configured for policy 0.

C.

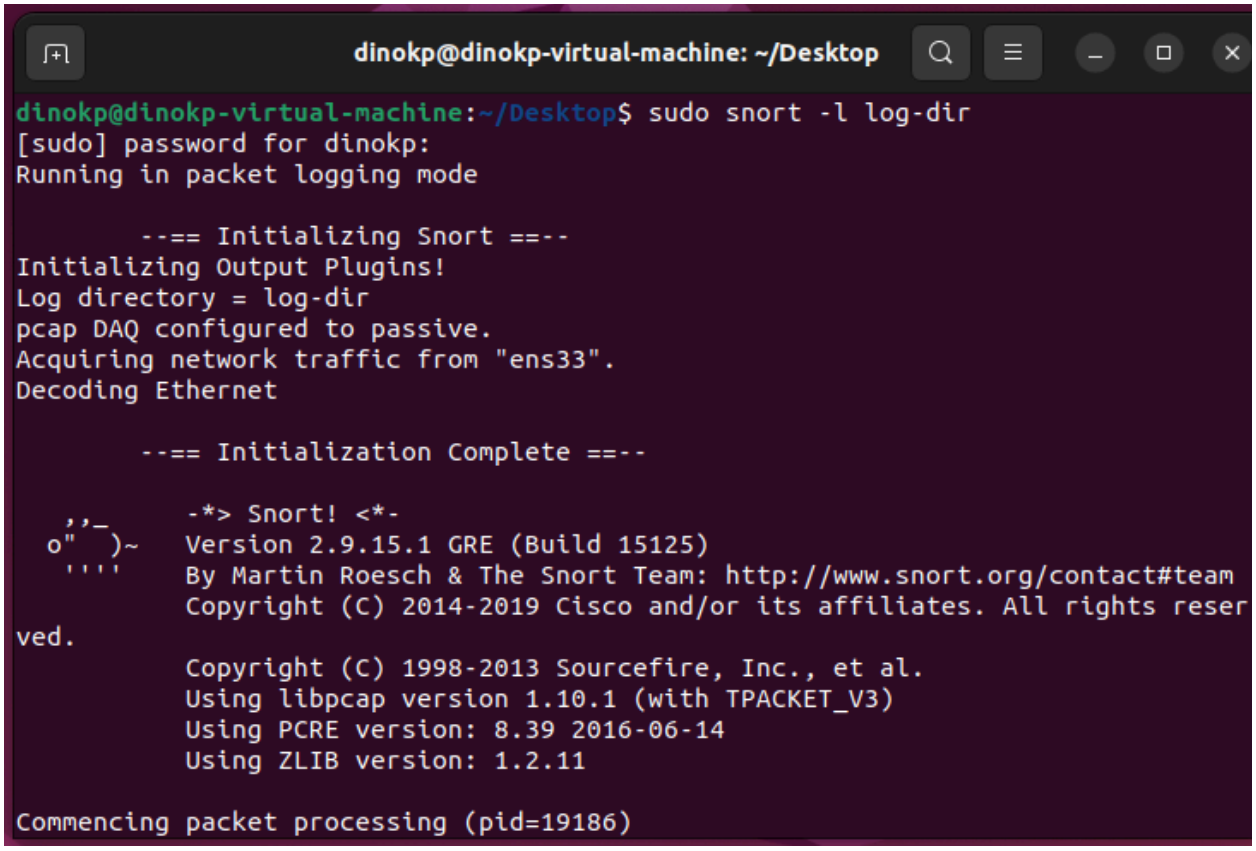

9F FB 00 00 00 01 00 00 00 00 00 06 64 69 6E .....din
6F 6B 70 00 00 FF 00 01 okp.....
WARNING: No preprocessors configured for policy 0.
03/23-21:26:04.809505 00:50:56:C0:00:08 -> 01:00:5E:00:00:16 type:0x800 len:0x3
192.168.32.1 -> 224.0.0.22 IGMP TTL:1 TOS:0x0 ID:49115 IpLen:24 DgmLen:40
IP Options (1) => RTRALT
22 00 F9 01 00 00 00 01 04 00 00 00 E0 00 00 FC "...
WARNING: No preprocessors configured for policy 0.
03/23-21:26:04.809511 00:50:56:C0:00:08 -> 33:33:00:00:00:16 type:0x86DD len:0x5
A
fe80::a586:436f:8c1a:c570 -> ff02::16 IPV6-ICMP TTL:1 TOS:0x0 ID:256 IpLen:40 Dg
mLen:76
00 00 00 01 04 00 00 00 FF 02 00 00 00 00 00 00 .....
00 00 00 00 00 01 00 03 .....

Exercise 13. 03 :

Step 1:
A.

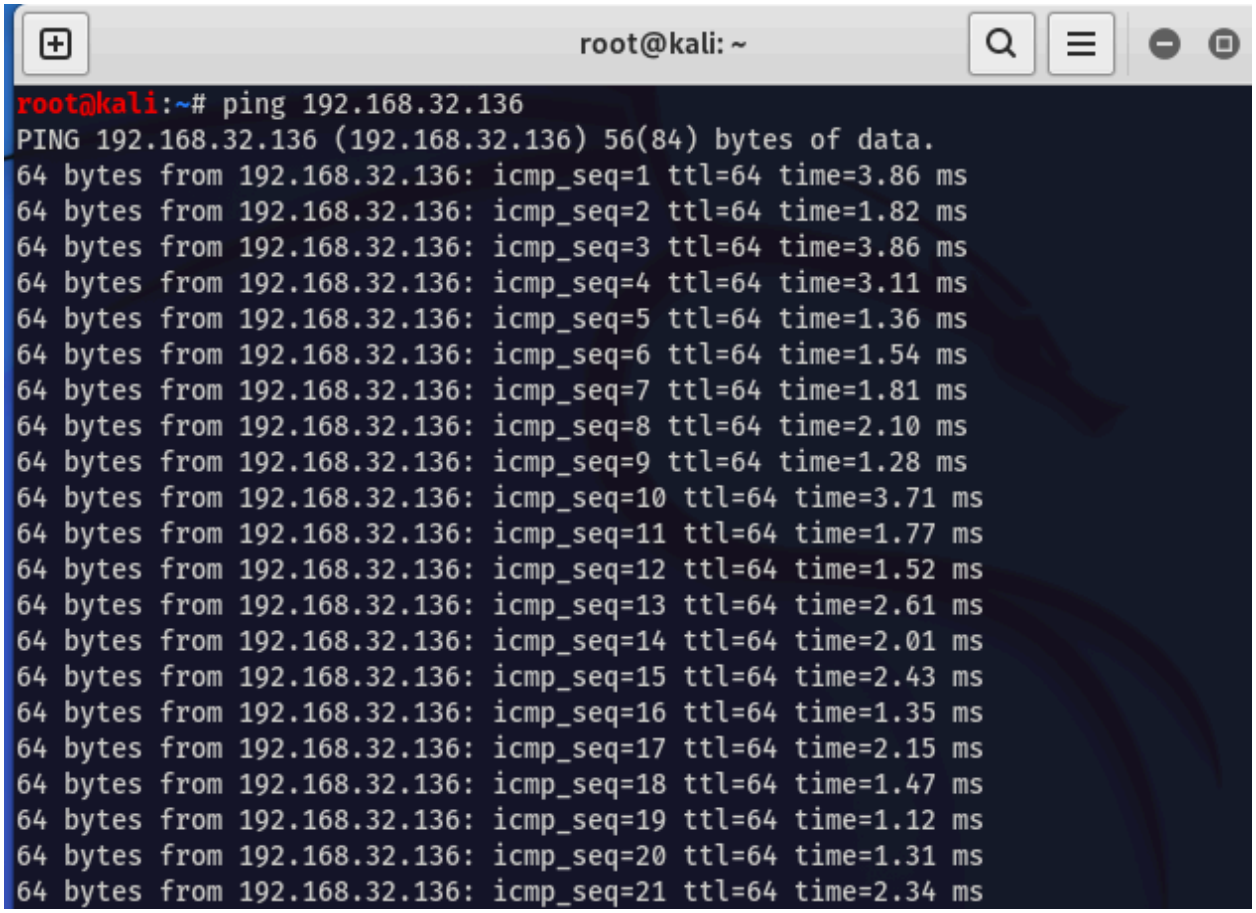
```
dinokp@dinokp-virtual-machine:~$ sudo snort -l .
Running in packet logging mode

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

        --== 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 rese
ved.
           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

Commencing packet processing (pid=18998)
```

We got the snort is opening and especially the logging directory is equal to .



Now i am trying to save the logs to log-dir in desktop and in next step i will ping with windows machine.

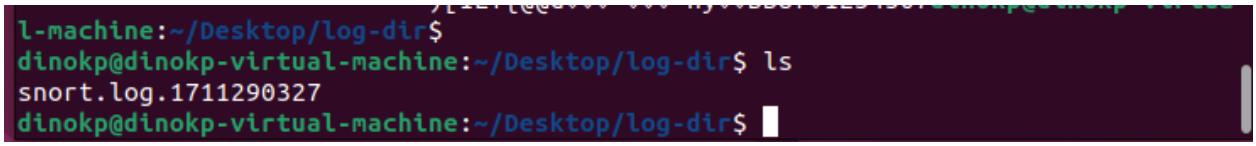
B. PInging Ubuntu :



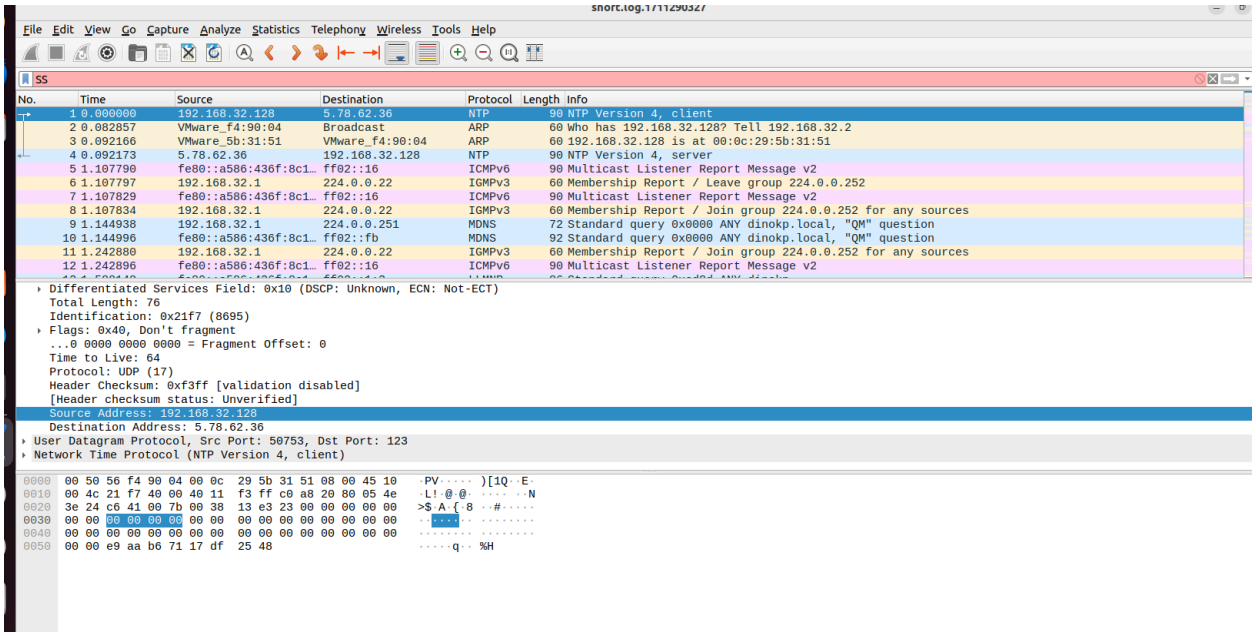

```
===============================================================================
Run time for packet processing was 107.542077 seconds
Snort processed 223 packets.
Snort ran for 0 days 0 hours 1 minutes 47 seconds
   Pkts/min:          223
   Pkts/sec:            2
===============================================================================
Memory usage summary:
  Total non-mmapped bytes (arena):       790528
  Bytes in mapped regions (hblkhd):      21590016
  Total allocated space (uordblks):      687184
  Total free space (fordblks):           103344
  Topmost releasable block (keepcost):   99936
===============================================================================
Packet I/O Totals:
   Received:          225
   Analyzed:          223 ( 99.111%)
    Dropped:            0 (  0.000%)
   Filtered:            0 (  0.000%)
Outstanding:            2 (  0.889%)
   Injected:            0
===============================================================================
```

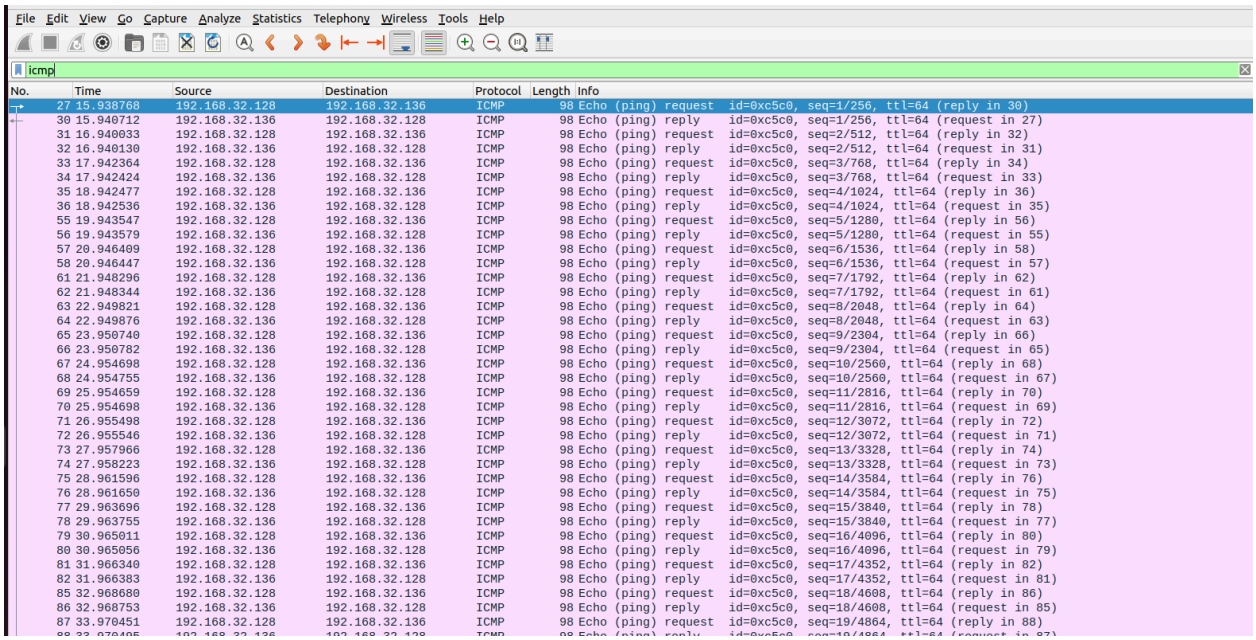
Step 2 :
A.

Snort log is successfully saved :



B.
We can see the source address of my kali machine.

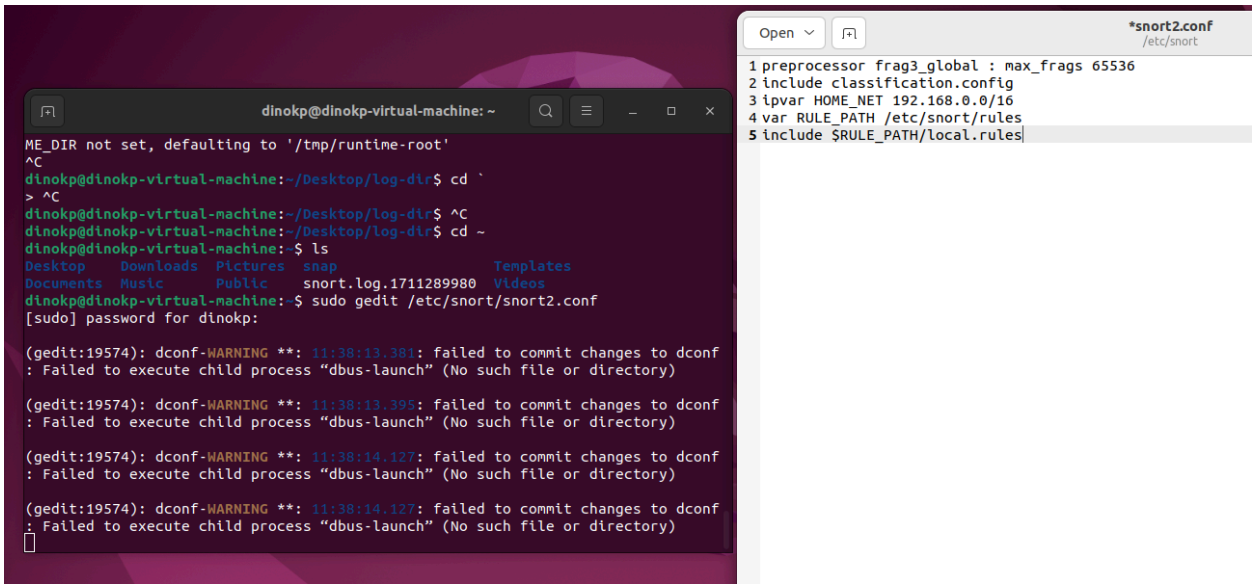




We can see the icmp request and replies above.

Exercise 13. 04 :

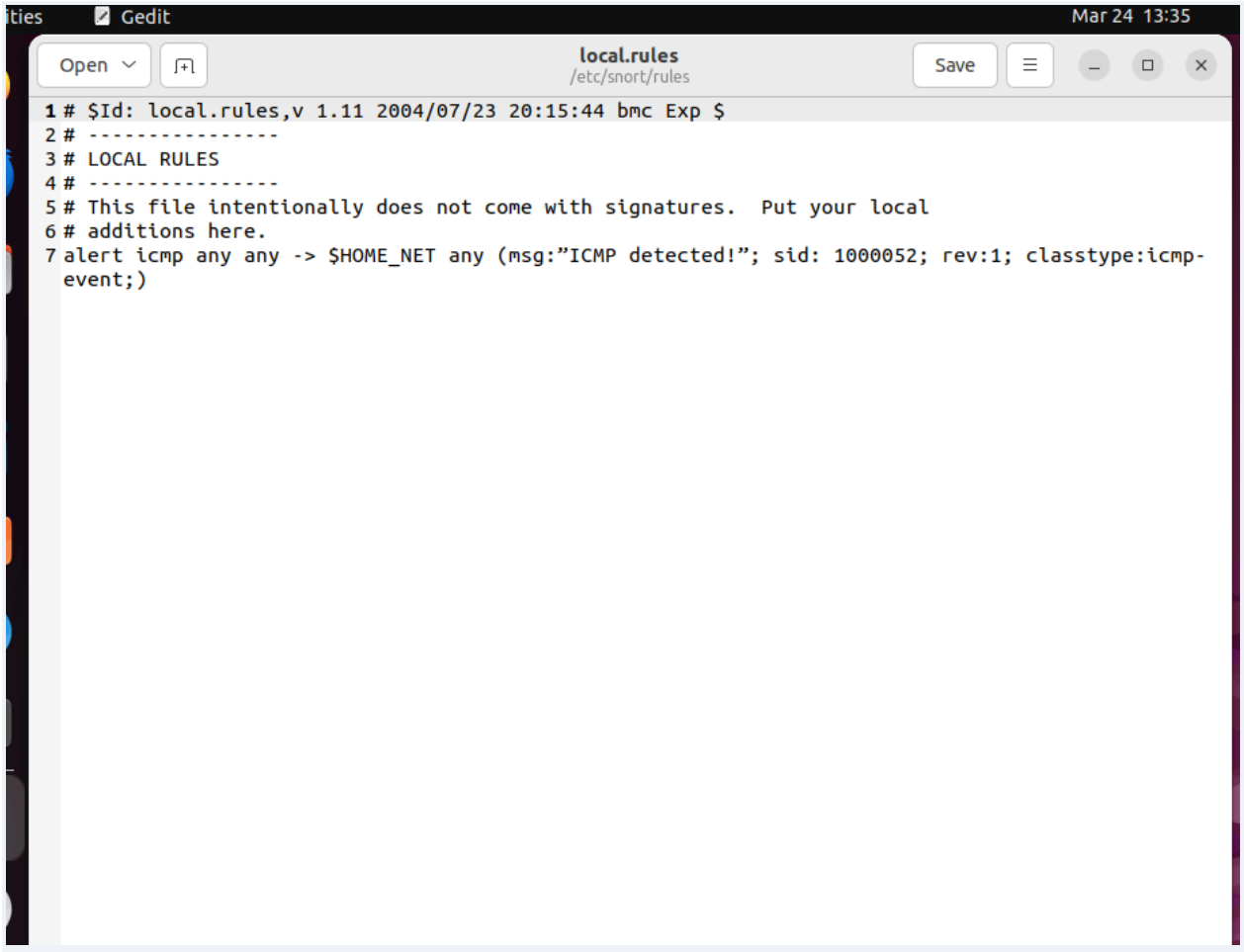
Step 1 :
A.

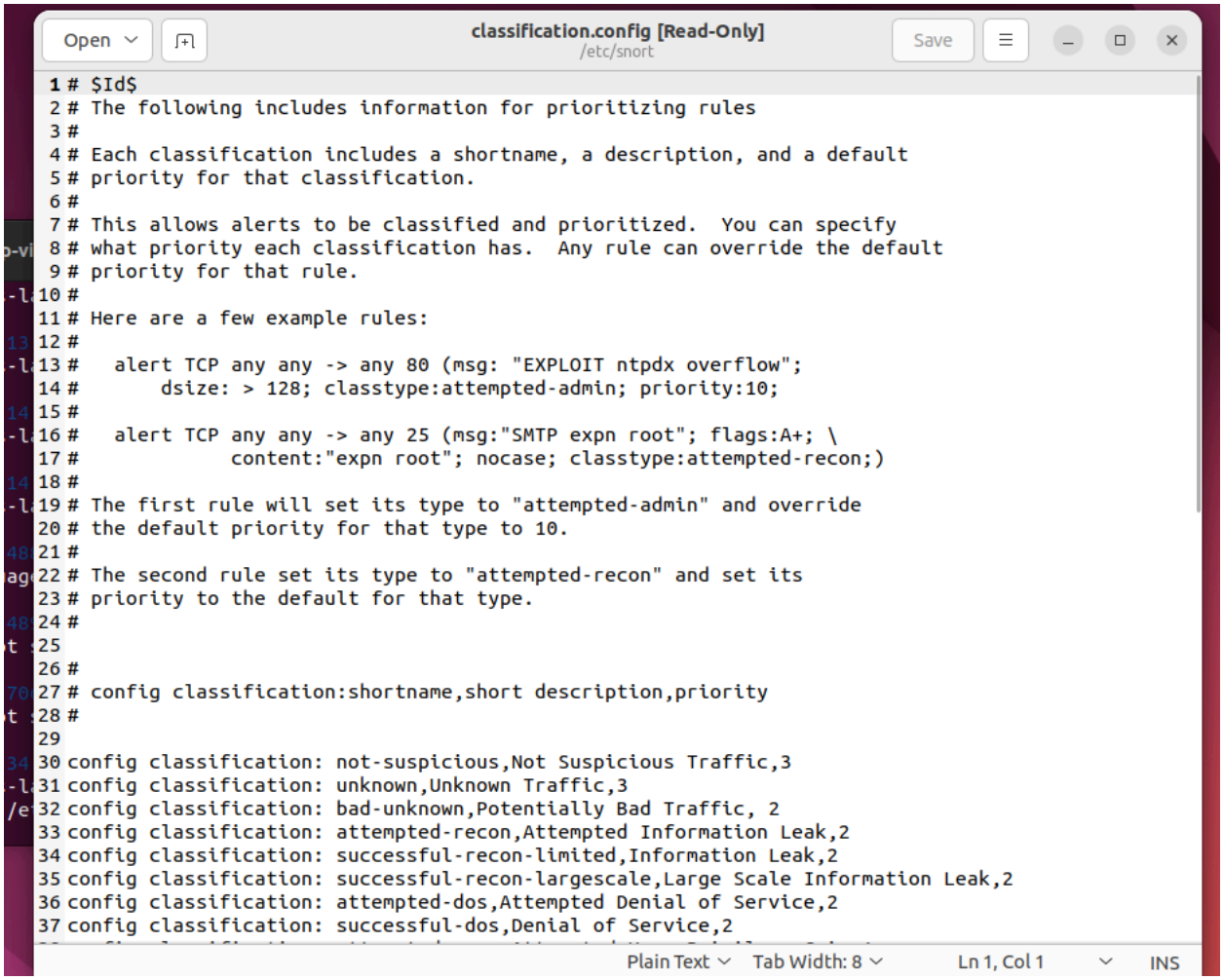


Geedit config file :

```
gedit /etc/snort/classification.config
```

B.


ities
Gedit
Mar 24 13:35
Open
local.rules
/etc/snort/rules
Save
1 # $Id: local.rules,v 1.11 2004/07/23 20:15:44 bmc Exp $
2 # ----------------
3 # LOCAL RULES
4 # ----------------
5 # This file intentionally does not come with signatures. Put your local
6 # additions here.
7 alert icmp any any -> $HOME_NET any (msg:”ICMP detected!”; sid: 1000052; rev:1; classtype:icmp-
event;)


Open
classification.config [Read-Only]
/etc/snort
Save
Id
The following includes information for prioritizing rules
#
Each classification includes a shortname, a description, and a default
priority for that classification.
#
This allows alerts to be classified and prioritized. You can specify
what priority each classification has. Any rule can override the default
priority for that rule.
#
Here are a few example rules:
#
alert TCP any any -> any 80 (msg: "EXPLOIT ntpdx overflow";
dsize: > 128; classtype:attempted-admin; priority:10;
#
alert TCP any any -> any 25 (msg:"SMTP expn root"; flags:A+; \
content:"expn root"; nocase; classtype:attempted-recon;)
#
The first rule will set its type to "attempted-admin" and override
the default priority for that type to 10.
#
The second rule set its type to "attempted-recon" and set its
priority to the default for that type.
#
#
#
config classification:shortname,short description,priority
#
config classification: not-suspicious,Not Suspicious Traffic,3
config classification: unknown,Unknown Traffic,3
config classification: bad-unknown,Potentially Bad Traffic, 2
config classification: attempted-recon,Attempted Information Leak,2
config classification: successful-recon-limited,Information Leak,2
config classification: successful-recon-largescale,Large Scale Information Leak,2
config classification: attempted-dos,Attempted Denial of Service,2
config classification: successful-dos,Denial of Service,2
Plain Text
Tab Width: 8
Ln 1, Col 1
INS

C.

```
dinokp@dinokp-virtual-machine:~$ sudo snort -A console -A fast -c /etc/snort/sno
rt2.conf -i ens33
Running in IDS mode

        --== Initializing Snort ==--
Initializing Output Plugins!
Initializing Preprocessors!
Initializing Plug-ins!
Parsing Rules file "/etc/snort/snort2.conf"
Tagged Packet Limit: 256
Log directory = /var/log/snort
Frag3 global config:
    Max frags: 65536
    Fragment memory cap: 4194304 bytes

++++++++++++++++++++++++++++++++++++++++++++++++++
Initializing rule chains...
1 Snort rules read
    1 detection rules
    0 decoder rules
    0 preprocessor rules
1 Option Chains linked into 1 Chain Headers
++++++++++++++++++++++++++++++++++++++++++++++++++
```

D.

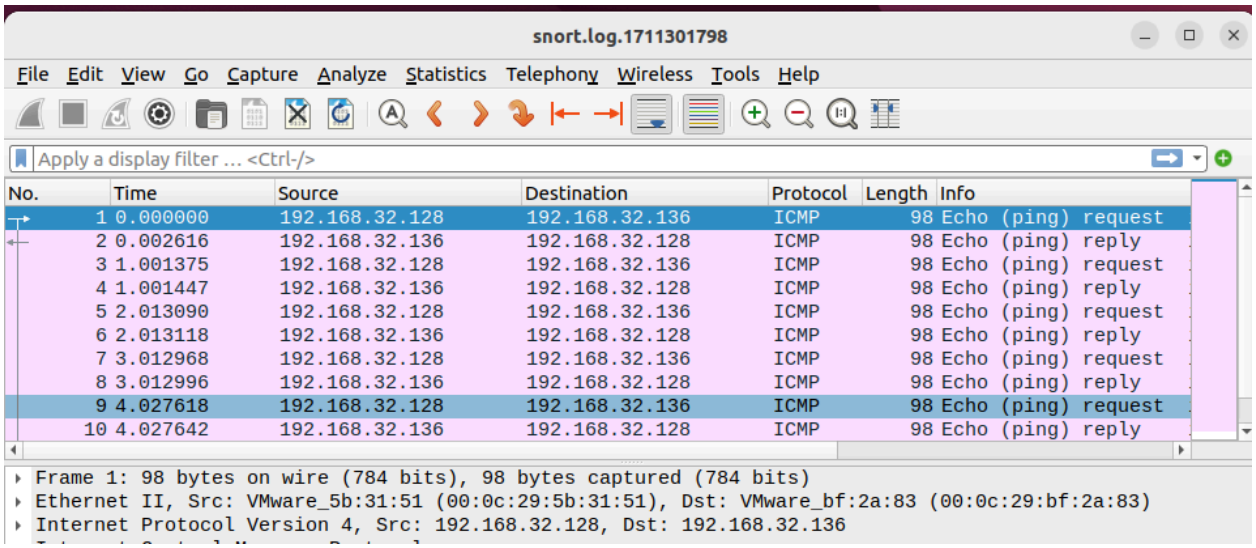
```
dinokp@dinokp-virtual-machine: ~
 Generic ICMP event] [Priority: 3] {ICMP} 192.168.32.128 -> 192.168.32.136
03/24-13:37:46.014768  [**] [1:1000052:1] "ICMP detected!" [**] [Classification:
 Generic ICMP event] [Priority: 3] {ICMP} 192.168.32.136 -> 192.168.32.128
03/24-13:37:47.038636  [**] [1:1000052:1] "ICMP detected!" [**] [Classification:
 Generic ICMP event] [Priority: 3] {ICMP} 192.168.32.128 -> 192.168.32.136
03/24-13:37:47.038677  [**] [1:1000052:1] "ICMP detected!" [**] [Classification:
 Generic ICMP event] [Priority: 3] {ICMP} 192.168.32.136 -> 192.168.32.128
03/24-13:37:48.062749  [**] [1:1000052:1] "ICMP detected!" [**] [Classification:
 Generic ICMP event] [Priority: 3] {ICMP} 192.168.32.128 -> 192.168.32.136
03/24-13:37:48.062776  [**] [1:1000052:1] "ICMP detected!" [**] [Classification:
 Generic ICMP event] [Priority: 3] {ICMP} 192.168.32.136 -> 192.168.32.128
03/24-13:37:49.086645  [**] [1:1000052:1] "ICMP detected!" [**] [Classification:
 Generic ICMP event] [Priority: 3] {ICMP} 192.168.32.128 -> 192.168.32.136
03/24-13:37:49.086668  [**] [1:1000052:1] "ICMP detected!" [**] [Classification:
 Generic ICMP event] [Priority: 3] {ICMP} 192.168.32.136 -> 192.168.32.128
03/24-13:37:50.110567  [**] [1:1000052:1] "ICMP detected!" [**] [Classification:
 Generic ICMP event] [Priority: 3] {ICMP} 192.168.32.128 -> 192.168.32.136
03/24-13:37:50.110591  [**] [1:1000052:1] "ICMP detected!" [**] [Classification:
 Generic ICMP event] [Priority: 3] {ICMP} 192.168.32.136 -> 192.168.32.128
03/24-13:37:51.134805  [**] [1:1000052:1] "ICMP detected!" [**] [Classification:
 Generic ICMP event] [Priority: 3] {ICMP} 192.168.32.128 -> 192.168.32.136
03/24-13:37:51.134833  [**] [1:1000052:1] "ICMP detected!" [**] [Classification:
 Generic ICMP event] [Priority: 3] {ICMP} 192.168.32.136 -> 192.168.32.128
```

```
Packet I/O Totals:
   Received:           80
   Analyzed:           79 ( 98.750%)
    Dropped:            0 (  0.000%)
   Filtered:            0 (  0.000%)
Outstanding:            1 (  1.250%)
   Injected:            0
```

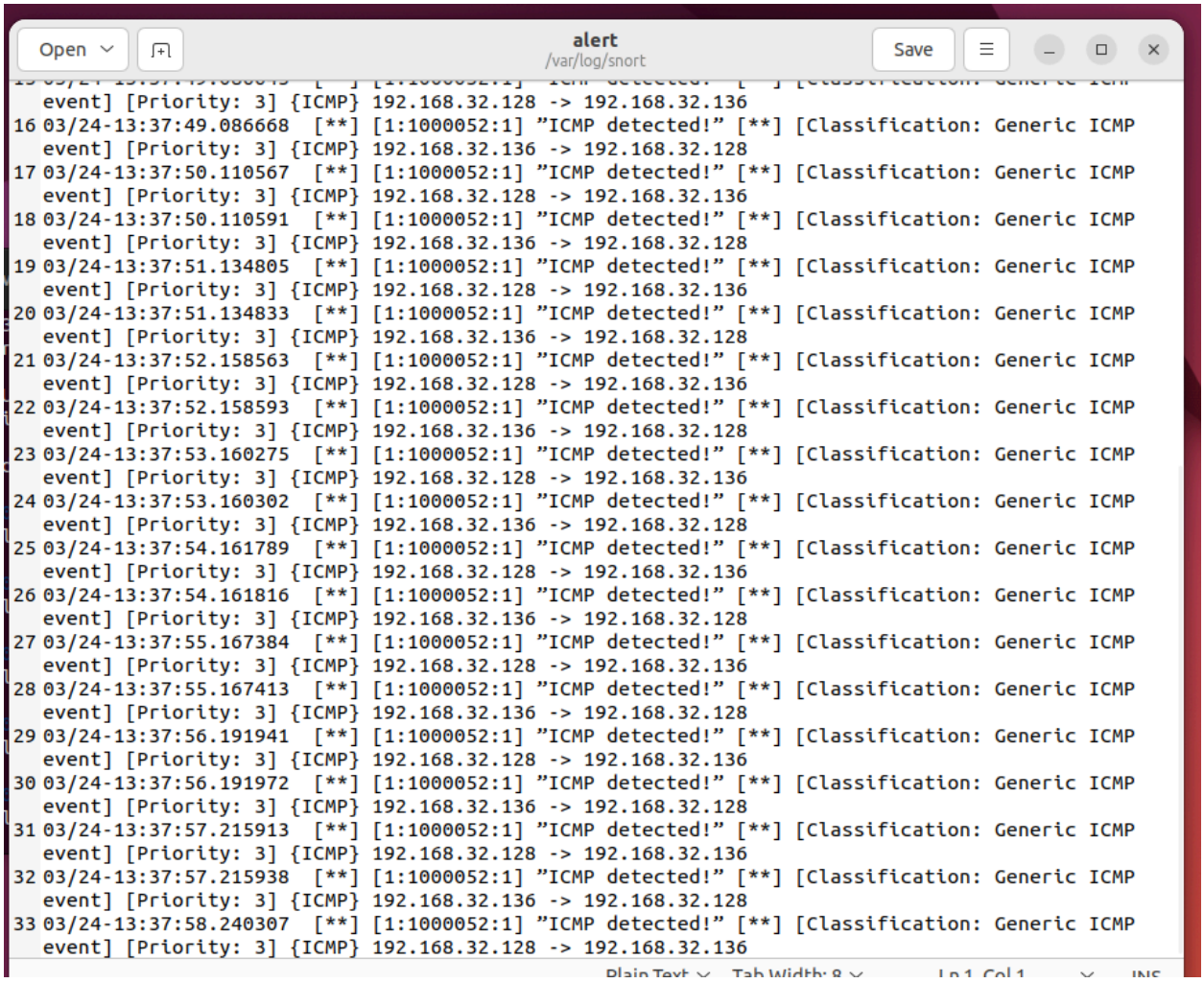
E.

```
Snort exiting
dinokp@dinokp-virtual-machine:~$ sudo ls -l /var/log/snort
total 588
-rw-r--r-- 1 root  adm    5247 Mar 24 13:37 alert
-rw-r----- 1 snort adm   53820 Mar 24 13:38 snort.alert
-rw-r--r-- 1 root  adm  168611 Mar 24 13:38 snort.alert.fast
-rw-r----- 1 snort adm  345028 Mar 24 13:38 snort.log
-rw------- 1 root  adm    3786 Mar 24 13:37 snort.log.1711301798
dinokp@dinokp-virtual-machine:~$
```

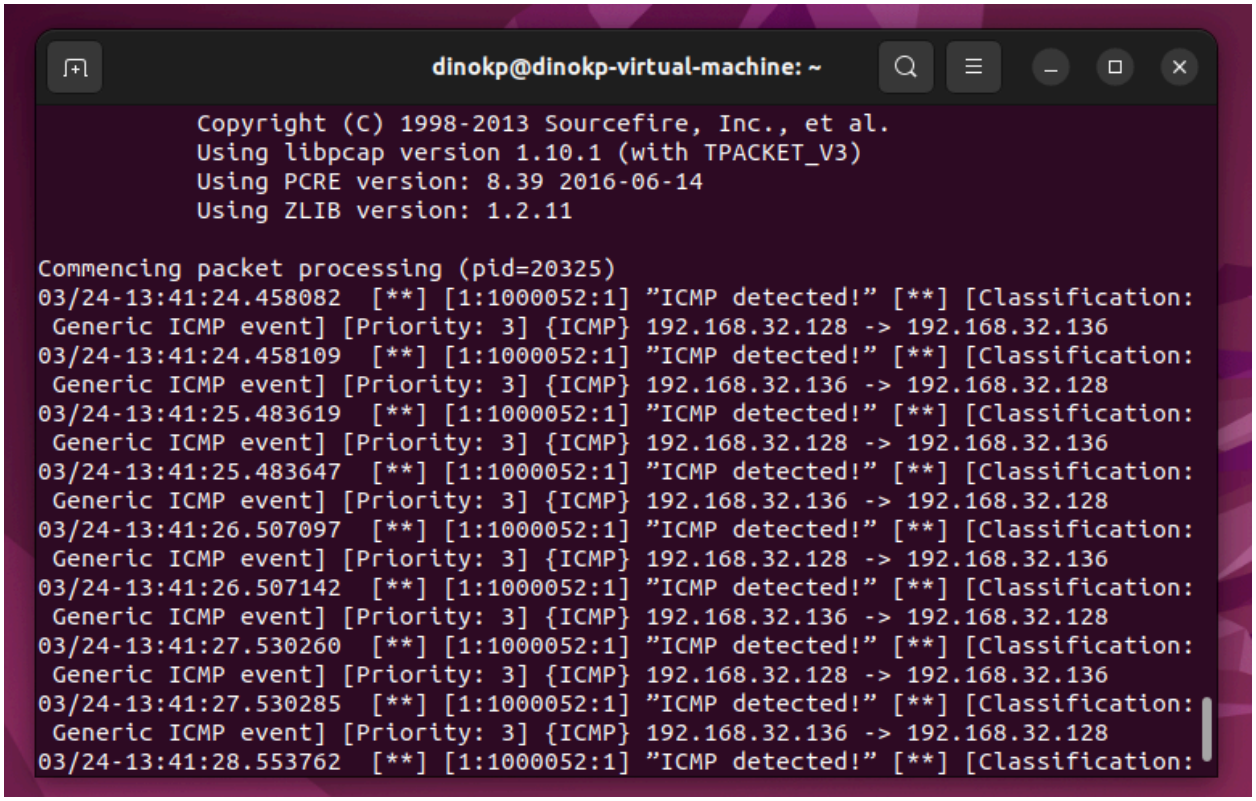
F.



G.


Open
alert
/var/log/snort
Save
event] [Priority: 3] {ICMP} 192.168.32.128 -> 192.168.32.136
16 03/24-13:37:49.086668 [**] [1:1000052:1] "ICMP detected!" [**] [Classification: Generic ICMP
event] [Priority: 3] {ICMP} 192.168.32.136 -> 192.168.32.128
17 03/24-13:37:50.110567 [**] [1:1000052:1] "ICMP detected!" [**] [Classification: Generic ICMP
event] [Priority: 3] {ICMP} 192.168.32.128 -> 192.168.32.136
18 03/24-13:37:50.110591 [**] [1:1000052:1] "ICMP detected!" [**] [Classification: Generic ICMP
event] [Priority: 3] {ICMP} 192.168.32.136 -> 192.168.32.128
19 03/24-13:37:51.134805 [**] [1:1000052:1] "ICMP detected!" [**] [Classification: Generic ICMP
event] [Priority: 3] {ICMP} 192.168.32.128 -> 192.168.32.136
20 03/24-13:37:51.134833 [**] [1:1000052:1] "ICMP detected!" [**] [Classification: Generic ICMP
event] [Priority: 3] {ICMP} 192.168.32.136 -> 192.168.32.128
21 03/24-13:37:52.158563 [**] [1:1000052:1] "ICMP detected!" [**] [Classification: Generic ICMP
event] [Priority: 3] {ICMP} 192.168.32.128 -> 192.168.32.136
22 03/24-13:37:52.158593 [**] [1:1000052:1] "ICMP detected!" [**] [Classification: Generic ICMP
event] [Priority: 3] {ICMP} 192.168.32.136 -> 192.168.32.128
23 03/24-13:37:53.160275 [**] [1:1000052:1] "ICMP detected!" [**] [Classification: Generic ICMP
event] [Priority: 3] {ICMP} 192.168.32.128 -> 192.168.32.136
24 03/24-13:37:53.160302 [**] [1:1000052:1] "ICMP detected!" [**] [Classification: Generic ICMP
event] [Priority: 3] {ICMP} 192.168.32.136 -> 192.168.32.128
25 03/24-13:37:54.161789 [**] [1:1000052:1] "ICMP detected!" [**] [Classification: Generic ICMP
event] [Priority: 3] {ICMP} 192.168.32.128 -> 192.168.32.136
26 03/24-13:37:54.161816 [**] [1:1000052:1] "ICMP detected!" [**] [Classification: Generic ICMP
event] [Priority: 3] {ICMP} 192.168.32.136 -> 192.168.32.128
27 03/24-13:37:55.167384 [**] [1:1000052:1] "ICMP detected!" [**] [Classification: Generic ICMP
event] [Priority: 3] {ICMP} 192.168.32.128 -> 192.168.32.136
28 03/24-13:37:55.167413 [**] [1:1000052:1] "ICMP detected!" [**] [Classification: Generic ICMP
event] [Priority: 3] {ICMP} 192.168.32.136 -> 192.168.32.128
29 03/24-13:37:56.191941 [**] [1:1000052:1] "ICMP detected!" [**] [Classification: Generic ICMP
event] [Priority: 3] {ICMP} 192.168.32.128 -> 192.168.32.136
30 03/24-13:37:56.191972 [**] [1:1000052:1] "ICMP detected!" [**] [Classification: Generic ICMP
event] [Priority: 3] {ICMP} 192.168.32.136 -> 192.168.32.128
31 03/24-13:37:57.215913 [**] [1:1000052:1] "ICMP detected!" [**] [Classification: Generic ICMP
event] [Priority: 3] {ICMP} 192.168.32.128 -> 192.168.32.136
32 03/24-13:37:57.215938 [**] [1:1000052:1] "ICMP detected!" [**] [Classification: Generic ICMP
event] [Priority: 3] {ICMP} 192.168.32.136 -> 192.168.32.128
33 03/24-13:37:58.240307 [**] [1:1000052:1] "ICMP detected!" [**] [Classification: Generic ICMP
event] [Priority: 3] {ICMP} 192.168.32.128 -> 192.168.32.136

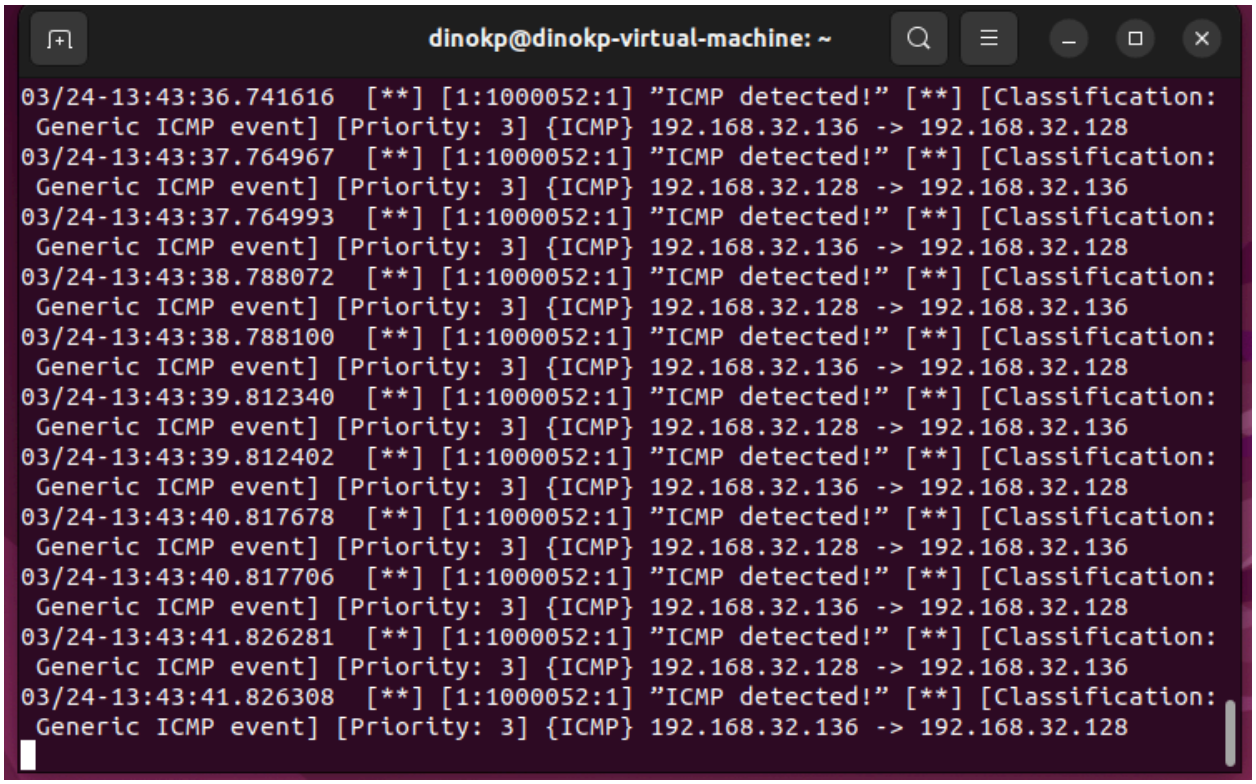
H.


dinokp@dinokp-virtual-machine: ~
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
Commencing packet processing (pid=20325)
03/24-13:41:24.458082 [**] [1:1000052:1] "ICMP detected!" [**] [Classification: Generic ICMP event] [Priority: 3] {ICMP} 192.168.32.128 -> 192.168.32.136
03/24-13:41:24.458109 [**] [1:1000052:1] "ICMP detected!" [**] [Classification: Generic ICMP event] [Priority: 3] {ICMP} 192.168.32.136 -> 192.168.32.128
03/24-13:41:25.483619 [**] [1:1000052:1] "ICMP detected!" [**] [Classification: Generic ICMP event] [Priority: 3] {ICMP} 192.168.32.128 -> 192.168.32.136
03/24-13:41:25.483647 [**] [1:1000052:1] "ICMP detected!" [**] [Classification: Generic ICMP event] [Priority: 3] {ICMP} 192.168.32.136 -> 192.168.32.128
03/24-13:41:26.507097 [**] [1:1000052:1] "ICMP detected!" [**] [Classification: Generic ICMP event] [Priority: 3] {ICMP} 192.168.32.128 -> 192.168.32.136
03/24-13:41:26.507142 [**] [1:1000052:1] "ICMP detected!" [**] [Classification: Generic ICMP event] [Priority: 3] {ICMP} 192.168.32.136 -> 192.168.32.128
03/24-13:41:27.530260 [**] [1:1000052:1] "ICMP detected!" [**] [Classification: Generic ICMP event] [Priority: 3] {ICMP} 192.168.32.128 -> 192.168.32.136
03/24-13:41:27.530285 [**] [1:1000052:1] "ICMP detected!" [**] [Classification: Generic ICMP event] [Priority: 3] {ICMP} 192.168.32.136 -> 192.168.32.128
03/24-13:41:28.553762 [**] [1:1000052:1] "ICMP detected!" [**] [Classification:

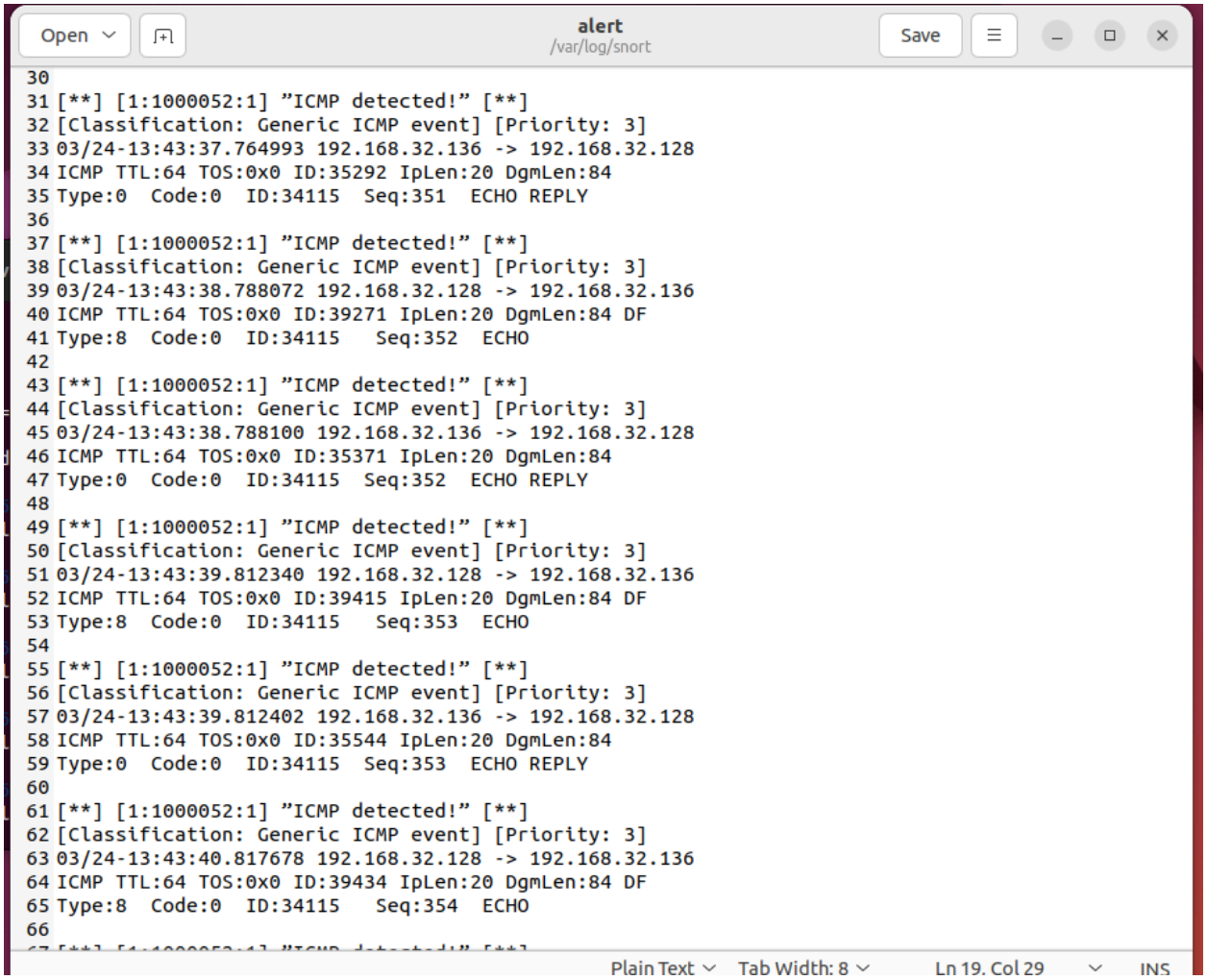
I.


Open
alert
/var/log/snort
Save
[Classification: Generic ICMP event] [Priority: 3]
03/24-13:41:28.553789 192.168.32.136 -> 192.168.32.128
ICMP TTL:64 TOS:0x0 ID:18800 IpLen:20 DgmLen:84
Type:0 Code:0 ID:34115 Seq:224 ECHO REPLY
[**] [1:1000052:1] "ICMP detected!" [**]
[Classification: Generic ICMP event] [Priority: 3]
03/24-13:41:29.577378 192.168.32.128 -> 192.168.32.136
ICMP TTL:64 TOS:0x0 ID:22609 IpLen:20 DgmLen:84 DF
Type:8 Code:0 ID:34115 Seq:225 ECHO
[**] [1:1000052:1] "ICMP detected!" [**]
[Classification: Generic ICMP event] [Priority: 3]
03/24-13:41:29.577404 192.168.32.136 -> 192.168.32.128
ICMP TTL:64 TOS:0x0 ID:18958 IpLen:20 DgmLen:84
Type:0 Code:0 ID:34115 Seq:225 ECHO REPLY
[**] [1:1000052:1] "ICMP detected!" [**]
[Classification: Generic ICMP event] [Priority: 3]
03/24-13:41:30.601004 192.168.32.128 -> 192.168.32.136
ICMP TTL:64 TOS:0x0 ID:22763 IpLen:20 DgmLen:84 DF
Type:8 Code:0 ID:34115 Seq:226 ECHO
[**] [1:1000052:1] "ICMP detected!" [**]
[Classification: Generic ICMP event] [Priority: 3]
03/24-13:41:30.601032 192.168.32.136 -> 192.168.32.128
ICMP TTL:64 TOS:0x0 ID:19197 IpLen:20 DgmLen:84
Type:0 Code:0 ID:34115 Seq:226 ECHO REPLY
[**] [1:1000052:1] "ICMP detected!" [**]
[Classification: Generic ICMP event] [Priority: 3]
03/24-13:41:31.624255 192.168.32.128 -> 192.168.32.136
ICMP TTL:64 TOS:0x0 ID:22908 IpLen:20 DgmLen:84 DF
Type:8 Code:0 ID:34115 Seq:227 ECHO
[**] [1:1000052:1] "ICMP detected!" [**]
[Classification: Generic ICMP event] [Priority: 3]

J.


dinokp@dinokp-virtual-machine: ~
03/24-13:43:36.741616 [**] [1:1000052:1] "ICMP detected!" [**] [Classification: Generic ICMP event] [Priority: 3] {ICMP} 192.168.32.136 -> 192.168.32.128
03/24-13:43:37.764967 [**] [1:1000052:1] "ICMP detected!" [**] [Classification: Generic ICMP event] [Priority: 3] {ICMP} 192.168.32.128 -> 192.168.32.136
03/24-13:43:37.764993 [**] [1:1000052:1] "ICMP detected!" [**] [Classification: Generic ICMP event] [Priority: 3] {ICMP} 192.168.32.136 -> 192.168.32.128
03/24-13:43:38.788072 [**] [1:1000052:1] "ICMP detected!" [**] [Classification: Generic ICMP event] [Priority: 3] {ICMP} 192.168.32.128 -> 192.168.32.136
03/24-13:43:38.788100 [**] [1:1000052:1] "ICMP detected!" [**] [Classification: Generic ICMP event] [Priority: 3] {ICMP} 192.168.32.136 -> 192.168.32.128
03/24-13:43:39.812340 [**] [1:1000052:1] "ICMP detected!" [**] [Classification: Generic ICMP event] [Priority: 3] {ICMP} 192.168.32.128 -> 192.168.32.136
03/24-13:43:39.812402 [**] [1:1000052:1] "ICMP detected!" [**] [Classification: Generic ICMP event] [Priority: 3] {ICMP} 192.168.32.136 -> 192.168.32.128
03/24-13:43:40.817678 [**] [1:1000052:1] "ICMP detected!" [**] [Classification: Generic ICMP event] [Priority: 3] {ICMP} 192.168.32.128 -> 192.168.32.136
03/24-13:43:40.817706 [**] [1:1000052:1] "ICMP detected!" [**] [Classification: Generic ICMP event] [Priority: 3] {ICMP} 192.168.32.136 -> 192.168.32.128
03/24-13:43:41.826281 [**] [1:1000052:1] "ICMP detected!" [**] [Classification: Generic ICMP event] [Priority: 3] {ICMP} 192.168.32.128 -> 192.168.32.136
03/24-13:43:41.826308 [**] [1:1000052:1] "ICMP detected!" [**] [Classification: Generic ICMP event] [Priority: 3] {ICMP} 192.168.32.136 -> 192.168.32.128

K.

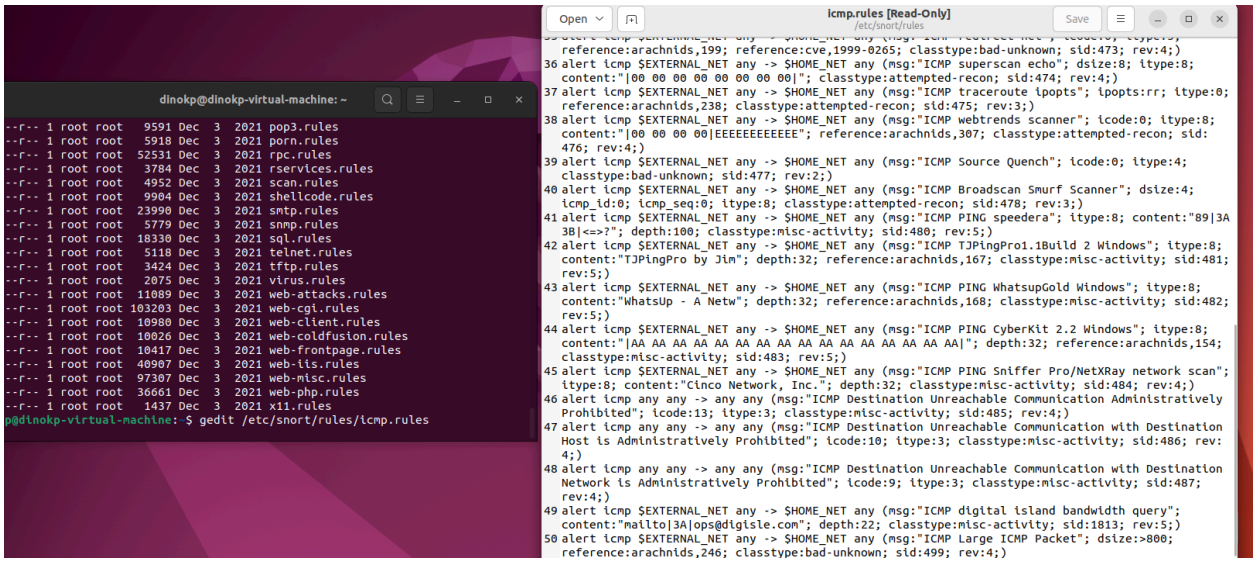

Open
alert
/var/log/snort
Save
30
31 [**] [1:1000052:1] "ICMP detected!" [**]
32 [Classification: Generic ICMP event] [Priority: 3]
33 03/24-13:43:37.764993 192.168.32.136 -> 192.168.32.128
34 ICMP TTL:64 TOS:0x0 ID:35292 IpLen:20 DgmLen:84
35 Type:0 Code:0 ID:34115 Seq:351 ECHO REPLY
36
37 [**] [1:1000052:1] "ICMP detected!" [**]
38 [Classification: Generic ICMP event] [Priority: 3]
39 03/24-13:43:38.788072 192.168.32.128 -> 192.168.32.136
40 ICMP TTL:64 TOS:0x0 ID:39271 IpLen:20 DgmLen:84 DF
41 Type:8 Code:0 ID:34115 Seq:352 ECHO
42
43 [**] [1:1000052:1] "ICMP detected!" [**]
44 [Classification: Generic ICMP event] [Priority: 3]
45 03/24-13:43:38.788100 192.168.32.136 -> 192.168.32.128
46 ICMP TTL:64 TOS:0x0 ID:35371 IpLen:20 DgmLen:84
47 Type:0 Code:0 ID:34115 Seq:352 ECHO REPLY
48
49 [**] [1:1000052:1] "ICMP detected!" [**]
50 [Classification: Generic ICMP event] [Priority: 3]
51 03/24-13:43:39.812340 192.168.32.128 -> 192.168.32.136
52 ICMP TTL:64 TOS:0x0 ID:39415 IpLen:20 DgmLen:84 DF
53 Type:8 Code:0 ID:34115 Seq:353 ECHO
54
55 [**] [1:1000052:1] "ICMP detected!" [**]
56 [Classification: Generic ICMP event] [Priority: 3]
57 03/24-13:43:39.812402 192.168.32.136 -> 192.168.32.128
58 ICMP TTL:64 TOS:0x0 ID:35544 IpLen:20 DgmLen:84
59 Type:0 Code:0 ID:34115 Seq:353 ECHO REPLY
60
61 [**] [1:1000052:1] "ICMP detected!" [**]
62 [Classification: Generic ICMP event] [Priority: 3]
63 03/24-13:43:40.817678 192.168.32.128 -> 192.168.32.136
64 ICMP TTL:64 TOS:0x0 ID:39434 IpLen:20 DgmLen:84 DF
65 Type:8 Code:0 ID:34115 Seq:354 ECHO
66
Plain Text
Tab Width: 8
Ln 19, Col 29
INS

Step 2 :

A.

```
dinokp@dinokp-virtual-machine:~$ ls -l /etc/snort/rules
total 1600
-rw-r--r-- 1 root root   5520 Dec  3  2021 attack-responses.rules
-rw-r--r-- 1 root root  17898 Dec  3  2021 backdoor.rules
-rw-r--r-- 1 root root   3862 Dec  3  2021 bad-traffic.rules
-rw-r--r-- 1 root root   7994 Dec  3  2021 chat.rules
-rw-r--r-- 1 root root  12759 Dec  3  2021 community-bot.rules
-rw-r--r-- 1 root root   1223 Dec  3  2021 community-deleted.rules
-rw-r--r-- 1 root root   2042 Dec  3  2021 community-dos.rules
-rw-r--r-- 1 root root   2176 Dec  3  2021 community-exploit.rules
-rw-r--r-- 1 root root    249 Dec  3  2021 community-ftp.rules
-rw-r--r-- 1 root root   1376 Dec  3  2021 community-game.rules
-rw-r--r-- 1 root root    689 Dec  3  2021 community-icmp.rules
-rw-r--r-- 1 root root   2777 Dec  3  2021 community-imap.rules
-rw-r--r-- 1 root root    948 Dec  3  2021 community-inappropriate.rules
-rw-r--r-- 1 root root    257 Dec  3  2021 community-mail-client.rules
-rw-r--r-- 1 root root   7837 Dec  3  2021 community-misc.rules
-rw-r--r-- 1 root root    621 Dec  3  2021 community-nntp.rules
-rw-r--r-- 1 root root    775 Dec  3  2021 community-oracle.rules
-rw-r--r-- 1 root root   1621 Dec  3  2021 community-policy.rules
-rw-r--r-- 1 root root   3551 Dec  3  2021 community-sip.rules
-rw-r--r-- 1 root root   2722 Dec  3  2021 community-smtp.rules
```

B.



C. Which five categories are the most interesting?

The most interesting categories, I felt are follows :

- Backdoor.rules : As steganography and phishing emails are growing I found it as interesting and useful one.
- Attack_responses rules : It is very important to manage the attack and manage it, so this is the main one.
- Dns.rules : It is mandatory for any company
- DDOS rules : Especially for financial services this is very impotant and interesting one i felt.
- Finally ICMP rules : This is great one, while someone tries to ping our server, having this is very important likewise

D. Which five individual rules are the most interesting?

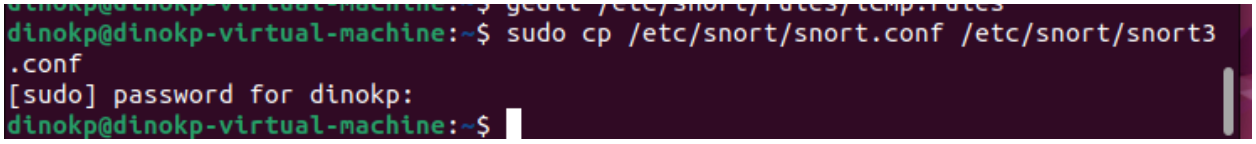
- alert icmp any any -> any any (msg:"ICMP Destination Unreachable Communication with Destination Host is Administratively Prohibited"; icode:10; itype:3; classtype:misc-activity; sid:486; rev:4;)
- alert tcp $EXTERNAL_NET any -> $HOME_NET 53 (msg:"DNS TCP inverse query"; flow:to_server,established; byte_test:1,<,16,2; byte_test:1,&,8,2; reference:bugtraq,2302; reference:cve,2001-0010; classtype:attempted-recon; sid:2922; rev:1;)
- alert tcp $EXTERNAL_NET any -> $TELNET_SERVERS 23 (msg:"BACKDOOR MISC Linux rootkit attempt"; flow:to_server,established; content:"wh00t!"; classtype:attempted-admin; sid:213; rev:4;)
- alert tcp $HOME_NET any -> $EXTERNAL_NET 25 (msg:"VIRUS OUTBOUND bad file attachment"; flow:to_server,established; content:"Content-Disposition|3A|"; nocase; pcre:"/filename\s*=\s*.*?\.(?=[abcdehijlmnoprsvwx])(a(d[ep]|s[dfx])|c([ho]m|li|md|pp)|d(iz|ll|ot)|e(m[fl]|xe)|h(lp|sq|ta)|jse?|m(d[abew]|s[ip])|p(p[st]|if|[lm]|ot)|r(eg|tf)|s(cr

|[hy]s|wf)|v(b[es]?|cf|xd)|w(m[dfsz]|p[dmsz]|s[cfh])|xl[tw]|bat|ini|lnk|nws|ocx)[\x27\x22\n\r\s]/iR"; classtype:suspicious-filename-detect; sid:721; rev:8;)

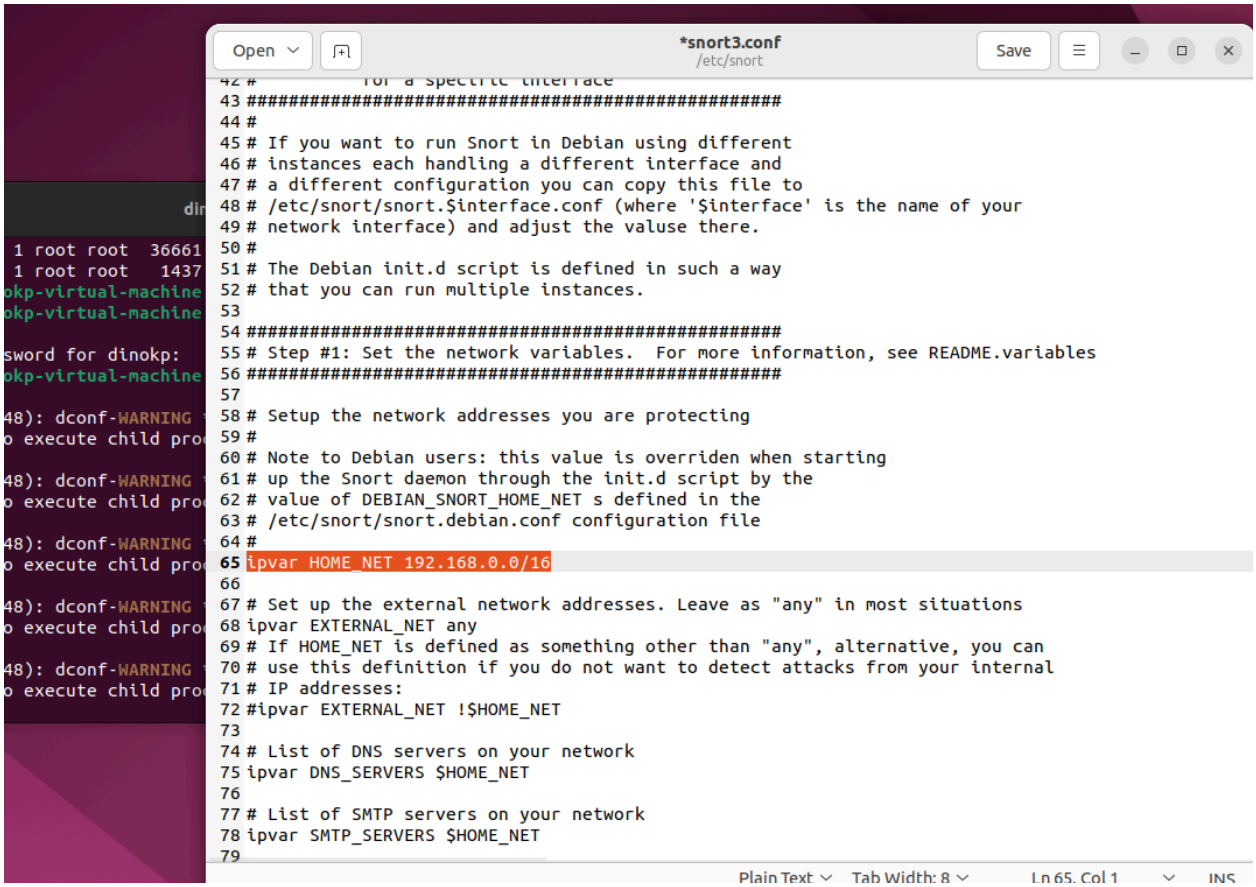
- alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"DDOS Stacheldraht client spoofworks"; icmp_id:1000; itype:0; content:"spoofworks"; reference:arachnids,192; classtype:attempted-dos; sid:227; rev:6;)

These five rules from different categories I feel are interesting because they are very important rules for those particular categories, depending on them.

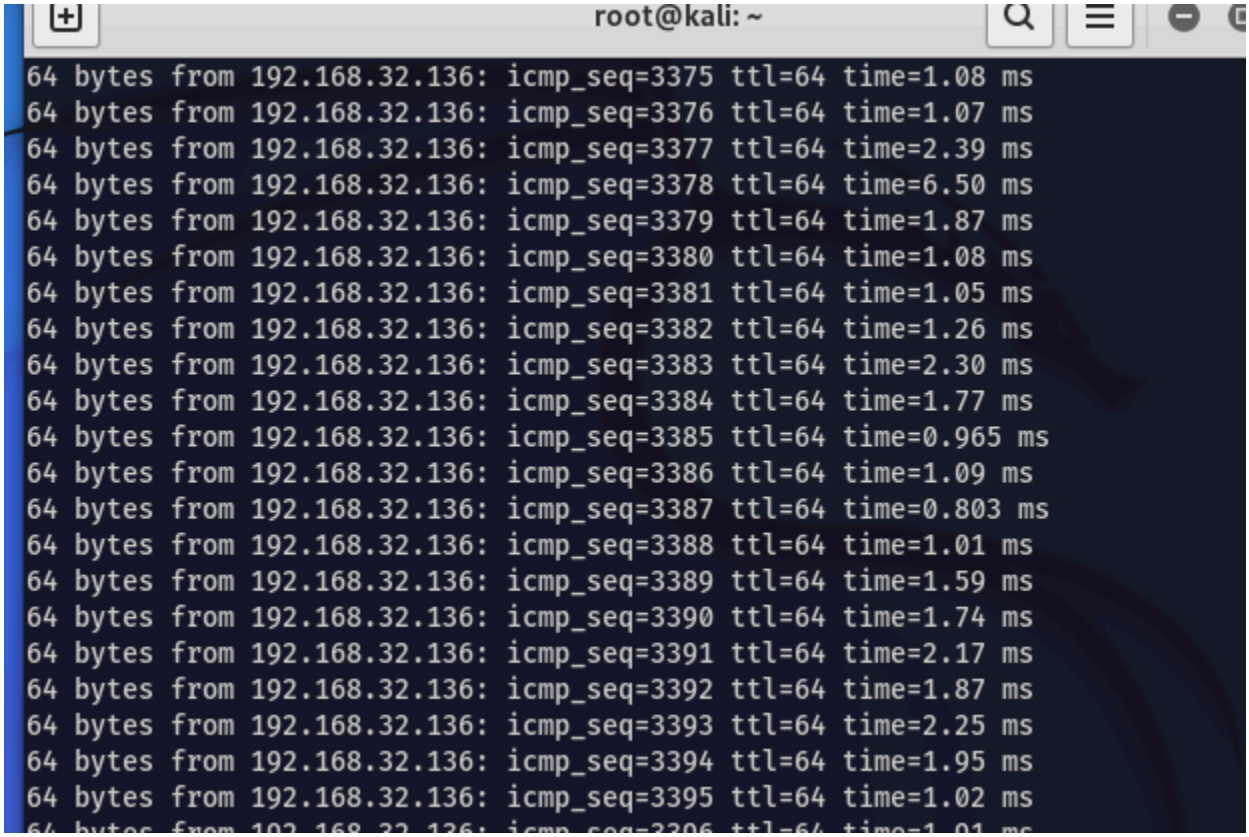
Step 3 :
A.

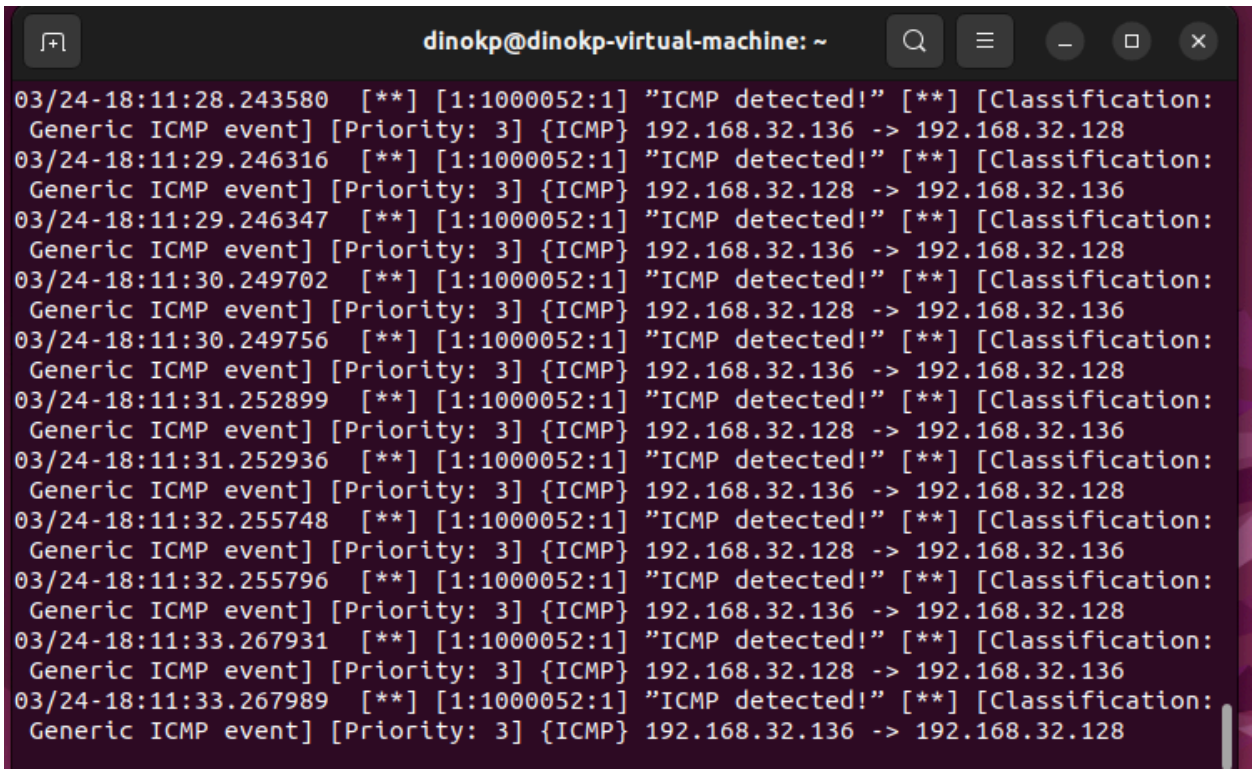


B

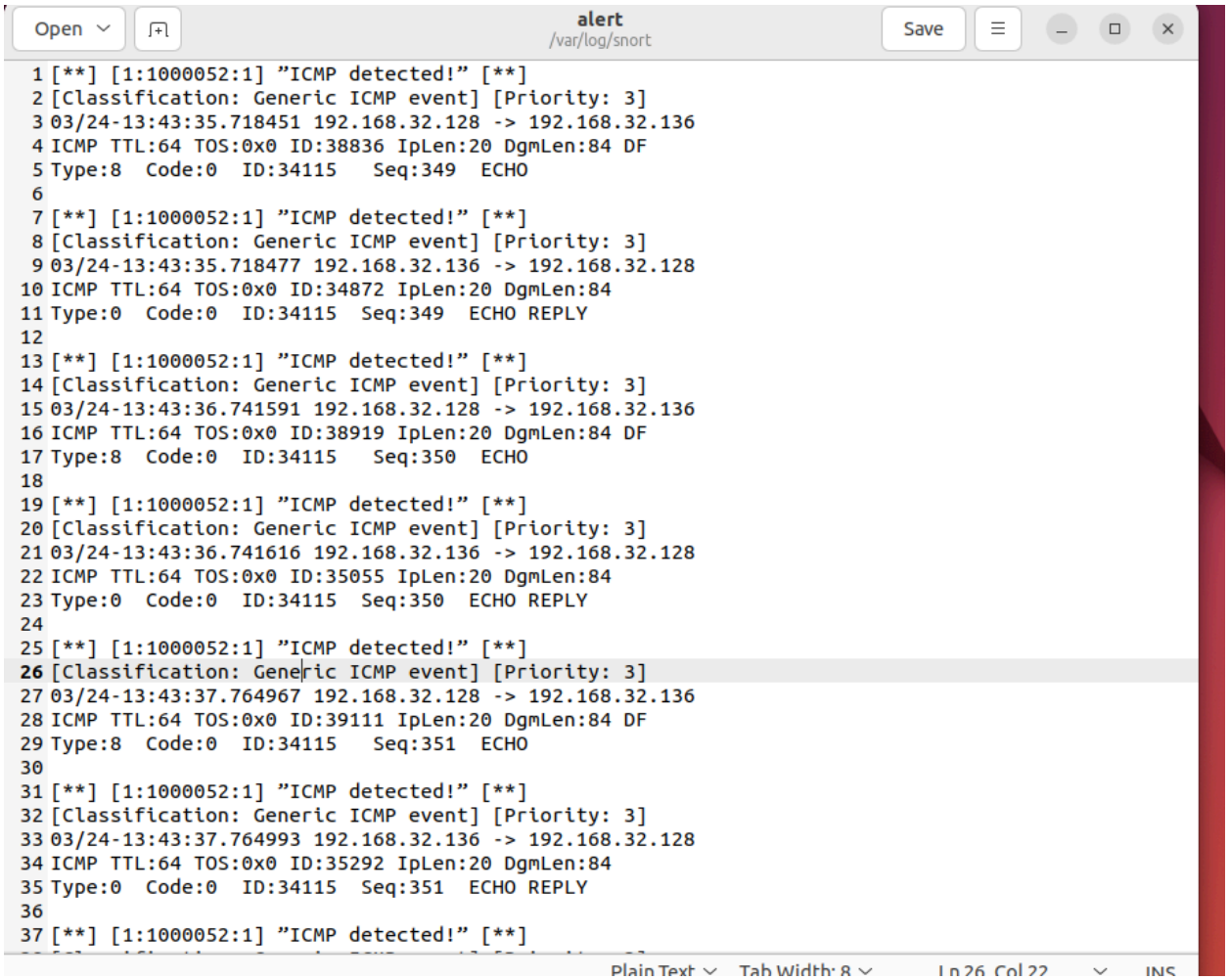

Open
*snort3.conf
/etc/snort
Save
##
If you want to run Snort in Debian using different
instances each handling a different interface and
a different configuration you can copy this file to
/etc/snort/snort.$interface.conf (where '$interface' is the name of your
network interface) and adjust the valuse there.
The Debian init.d script is defined in such a way
that you can run multiple instances.
##
Step #1: Set the network variables. For more information, see README.variables
##
Setup the network addresses you are protecting
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 192.168.0.0/16
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
Plain Text
Tab Width: 8
Ln 65, Col 1
INS

C.

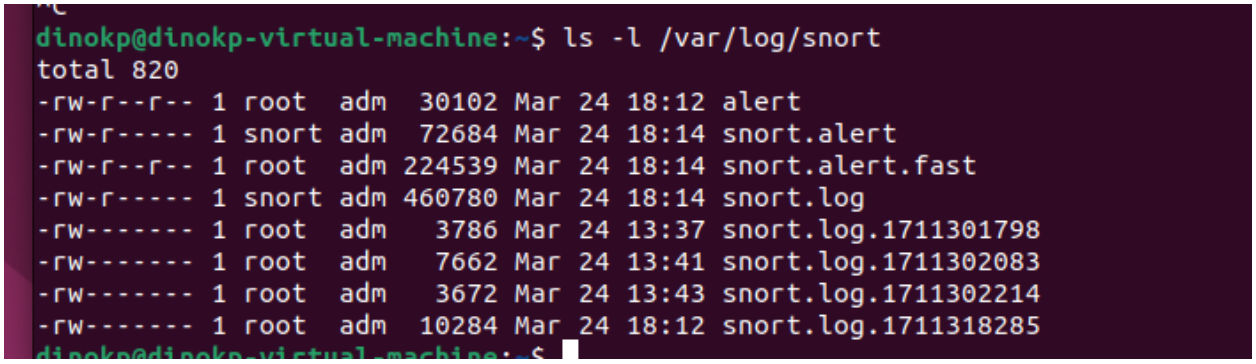

root@kali: ~
64 bytes from 192.168.32.136: icmp_seq=3375 ttl=64 time=1.08 ms
64 bytes from 192.168.32.136: icmp_seq=3376 ttl=64 time=1.07 ms
64 bytes from 192.168.32.136: icmp_seq=3377 ttl=64 time=2.39 ms
64 bytes from 192.168.32.136: icmp_seq=3378 ttl=64 time=6.50 ms
64 bytes from 192.168.32.136: icmp_seq=3379 ttl=64 time=1.87 ms
64 bytes from 192.168.32.136: icmp_seq=3380 ttl=64 time=1.08 ms
64 bytes from 192.168.32.136: icmp_seq=3381 ttl=64 time=1.05 ms
64 bytes from 192.168.32.136: icmp_seq=3382 ttl=64 time=1.26 ms
64 bytes from 192.168.32.136: icmp_seq=3383 ttl=64 time=2.30 ms
64 bytes from 192.168.32.136: icmp_seq=3384 ttl=64 time=1.77 ms
64 bytes from 192.168.32.136: icmp_seq=3385 ttl=64 time=0.965 ms
64 bytes from 192.168.32.136: icmp_seq=3386 ttl=64 time=1.09 ms
64 bytes from 192.168.32.136: icmp_seq=3387 ttl=64 time=0.803 ms
64 bytes from 192.168.32.136: icmp_seq=3388 ttl=64 time=1.01 ms
64 bytes from 192.168.32.136: icmp_seq=3389 ttl=64 time=1.59 ms
64 bytes from 192.168.32.136: icmp_seq=3390 ttl=64 time=1.74 ms
64 bytes from 192.168.32.136: icmp_seq=3391 ttl=64 time=2.17 ms
64 bytes from 192.168.32.136: icmp_seq=3392 ttl=64 time=1.87 ms
64 bytes from 192.168.32.136: icmp_seq=3393 ttl=64 time=2.25 ms
64 bytes from 192.168.32.136: icmp_seq=3394 ttl=64 time=1.95 ms
64 bytes from 192.168.32.136: icmp_seq=3395 ttl=64 time=1.02 ms

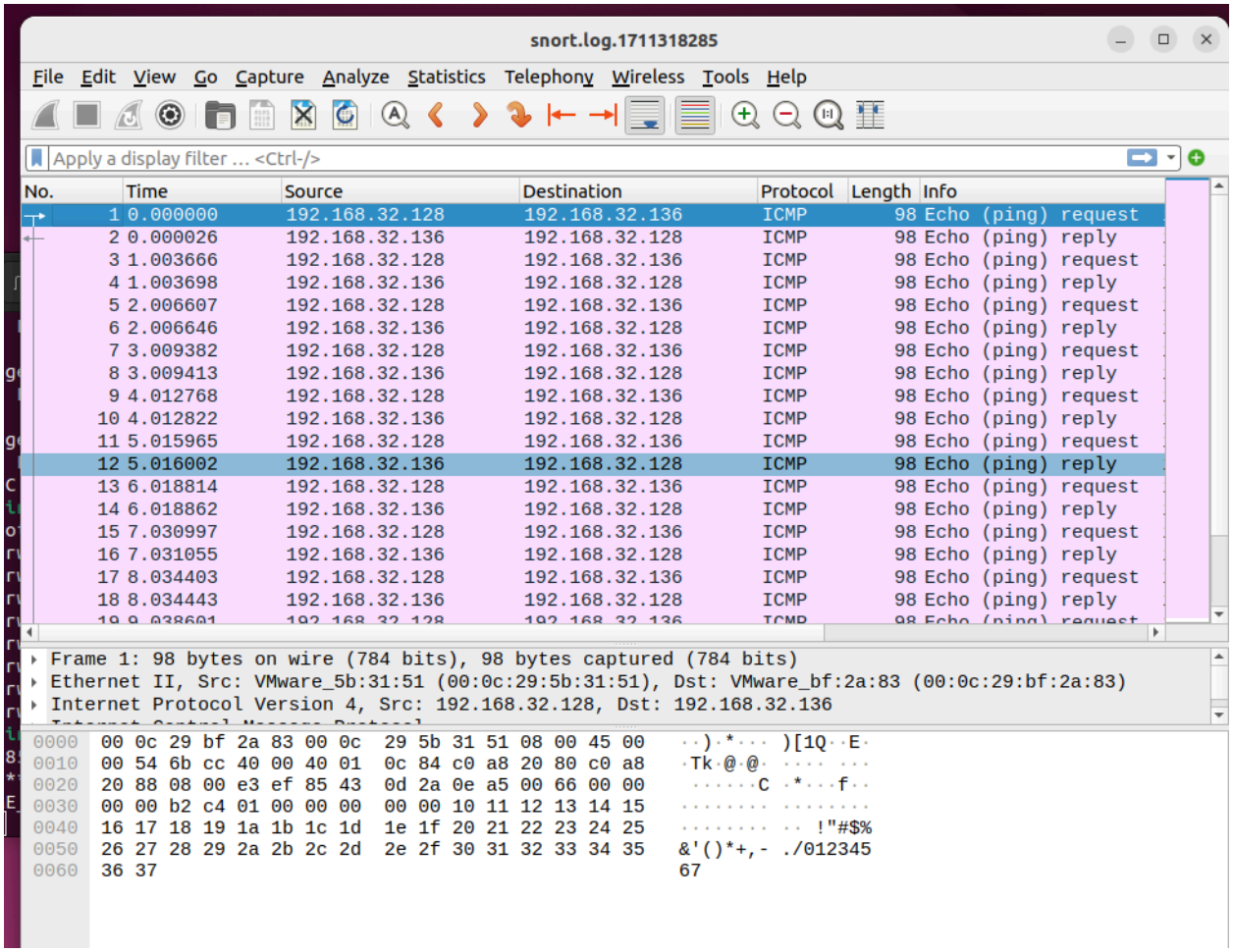

dinokp@dinokp-virtual-machine: ~
03/24-18:11:28.243580 [**] [1:1000052:1] "ICMP detected!" [**] [Classification: Generic ICMP event] [Priority: 3] {ICMP} 192.168.32.136 -> 192.168.32.128
03/24-18:11:29.246316 [**] [1:1000052:1] "ICMP detected!" [**] [Classification: Generic ICMP event] [Priority: 3] {ICMP} 192.168.32.128 -> 192.168.32.136
03/24-18:11:29.246347 [**] [1:1000052:1] "ICMP detected!" [**] [Classification: Generic ICMP event] [Priority: 3] {ICMP} 192.168.32.136 -> 192.168.32.128
03/24-18:11:30.249702 [**] [1:1000052:1] "ICMP detected!" [**] [Classification: Generic ICMP event] [Priority: 3] {ICMP} 192.168.32.128 -> 192.168.32.136
03/24-18:11:30.249756 [**] [1:1000052:1] "ICMP detected!" [**] [Classification: Generic ICMP event] [Priority: 3] {ICMP} 192.168.32.136 -> 192.168.32.128
03/24-18:11:31.252899 [**] [1:1000052:1] "ICMP detected!" [**] [Classification: Generic ICMP event] [Priority: 3] {ICMP} 192.168.32.128 -> 192.168.32.136
03/24-18:11:31.252936 [**] [1:1000052:1] "ICMP detected!" [**] [Classification: Generic ICMP event] [Priority: 3] {ICMP} 192.168.32.136 -> 192.168.32.128
03/24-18:11:32.255748 [**] [1:1000052:1] "ICMP detected!" [**] [Classification: Generic ICMP event] [Priority: 3] {ICMP} 192.168.32.128 -> 192.168.32.136
03/24-18:11:32.255796 [**] [1:1000052:1] "ICMP detected!" [**] [Classification: Generic ICMP event] [Priority: 3] {ICMP} 192.168.32.136 -> 192.168.32.128
03/24-18:11:33.267931 [**] [1:1000052:1] "ICMP detected!" [**] [Classification: Generic ICMP event] [Priority: 3] {ICMP} 192.168.32.128 -> 192.168.32.136
03/24-18:11:33.267989 [**] [1:1000052:1] "ICMP detected!" [**] [Classification: Generic ICMP event] [Priority: 3] {ICMP} 192.168.32.136 -> 192.168.32.128

D.


Open
alert
/var/log/snort
Save
1 [**] [1:1000052:1] "ICMP detected!" [**]
2 [Classification: Generic ICMP event] [Priority: 3]
3 03/24-13:43:35.718451 192.168.32.128 -> 192.168.32.136
4 ICMP TTL:64 TOS:0x0 ID:38836 IpLen:20 DgmLen:84 DF
5 Type:8 Code:0 ID:34115 Seq:349 ECHO
6
7 [**] [1:1000052:1] "ICMP detected!" [**]
8 [Classification: Generic ICMP event] [Priority: 3]
9 03/24-13:43:35.718477 192.168.32.136 -> 192.168.32.128
10 ICMP TTL:64 TOS:0x0 ID:34872 IpLen:20 DgmLen:84
11 Type:0 Code:0 ID:34115 Seq:349 ECHO REPLY
12
13 [**] [1:1000052:1] "ICMP detected!" [**]
14 [Classification: Generic ICMP event] [Priority: 3]
15 03/24-13:43:36.741591 192.168.32.128 -> 192.168.32.136
16 ICMP TTL:64 TOS:0x0 ID:38919 IpLen:20 DgmLen:84 DF
17 Type:8 Code:0 ID:34115 Seq:350 ECHO
18
19 [**] [1:1000052:1] "ICMP detected!" [**]
20 [Classification: Generic ICMP event] [Priority: 3]
21 03/24-13:43:36.741616 192.168.32.136 -> 192.168.32.128
22 ICMP TTL:64 TOS:0x0 ID:35055 IpLen:20 DgmLen:84
23 Type:0 Code:0 ID:34115 Seq:350 ECHO REPLY
24
25 [**] [1:1000052:1] "ICMP detected!" [**]
26 [Classification: Generic ICMP event] [Priority: 3]
27 03/24-13:43:37.764967 192.168.32.128 -> 192.168.32.136
28 ICMP TTL:64 TOS:0x0 ID:39111 IpLen:20 DgmLen:84 DF
29 Type:8 Code:0 ID:34115 Seq:351 ECHO
30
31 [**] [1:1000052:1] "ICMP detected!" [**]
32 [Classification: Generic ICMP event] [Priority: 3]
33 03/24-13:43:37.764993 192.168.32.136 -> 192.168.32.128
34 ICMP TTL:64 TOS:0x0 ID:35292 IpLen:20 DgmLen:84
35 Type:0 Code:0 ID:34115 Seq:351 ECHO REPLY
36
37 [**] [1:1000052:1] "ICMP detected!" [**]
Plain Text
Tab Width: 8
Ln 26, Col 22
INS

E.


dinokp@dinokp-virtual-machine:~$ ls -l /var/log/snort
total 820
-rw-r--r-- 1 root adm 30102 Mar 24 18:12 alert
-rw-r----- 1 snort adm 72684 Mar 24 18:14 snort.alert
-rw-r--r-- 1 root adm 224539 Mar 24 18:14 snort.alert.fast
-rw-r----- 1 snort adm 460780 Mar 24 18:14 snort.log
-rw------- 1 root adm 3786 Mar 24 13:37 snort.log.1711301798
-rw------- 1 root adm 7662 Mar 24 13:41 snort.log.1711302083
-rw------- 1 root adm 3672 Mar 24 13:43 snort.log.1711302214
-rw------- 1 root adm 10284 Mar 24 18:12 snort.log.1711318285



Lab Analysis :

1. Three modes include Sniffer mode, which simply shows the packets from the stream, next is Packet Logger mode, which will save the logs of the packets. Finally Network Intrusion Detection mode, which helps to analyze the network packets and traffic.
2. Most often used mode is obviously the NIDS mode, which is used to monitor the network and stop the malicious network based on the rules configured. This NIDS from snort will be combined with security infrastruture of the companies to give better protection, like working along with SIEM tools, firewalls, Network Monitoring tools etc. In this mode we can write our custom rule to prevent the traffic for safeguarding the network.
3. Categories of rules snort use :
    - Web based attacks : Rules that will be used to prevent url attacks and hex modification on urls and browser attacks
    - Malware : Has some signature of the malwares to find it and stop their activity.

- DDOS : To prevent ddos attacks, this rule can identify and monitors the network the activity of the DDOS attacks and multiple request from lot of different variation to find the pattern.

KEY TERM QUIZ

1. Rules
2. Configuration
3. Log