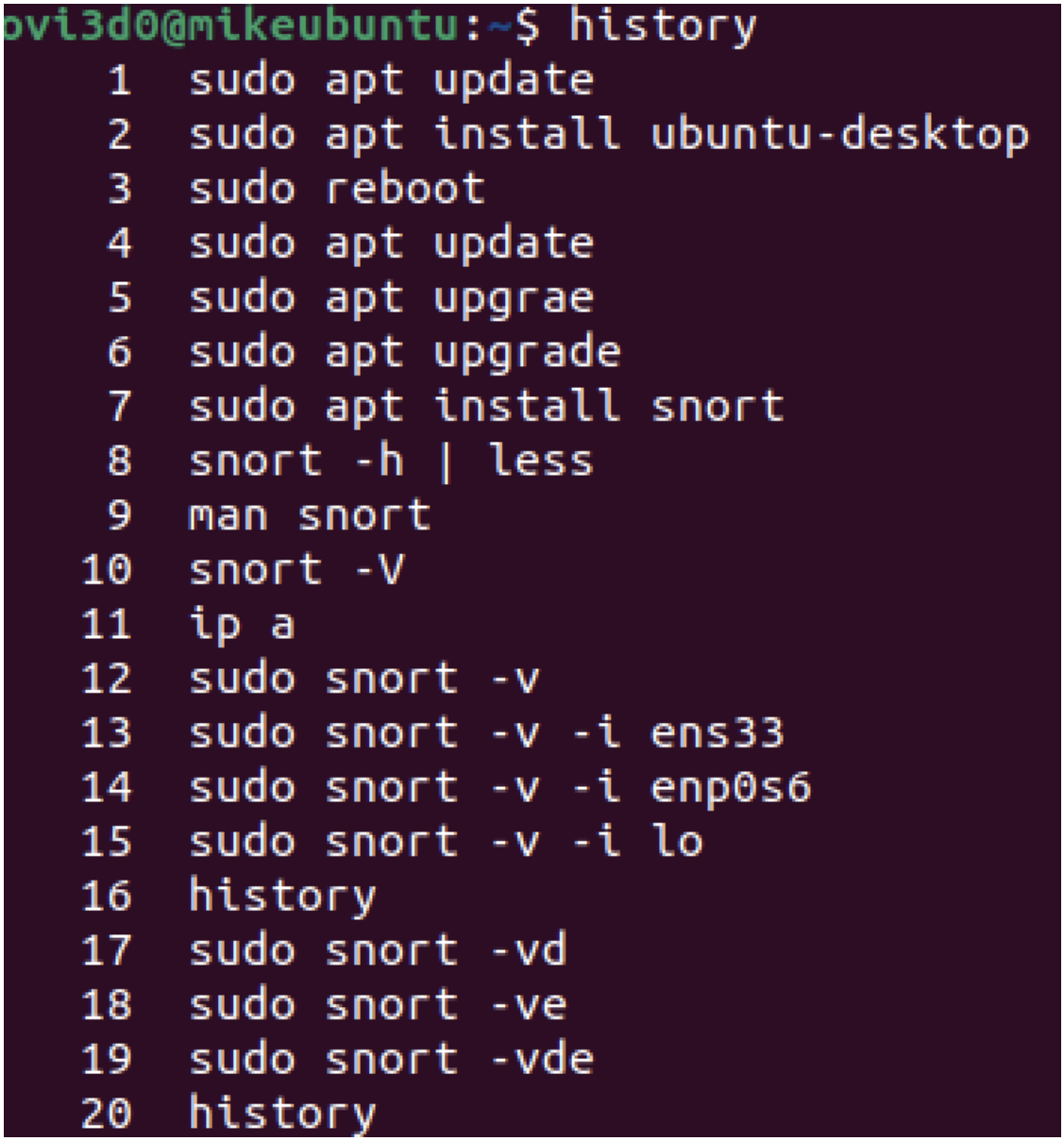
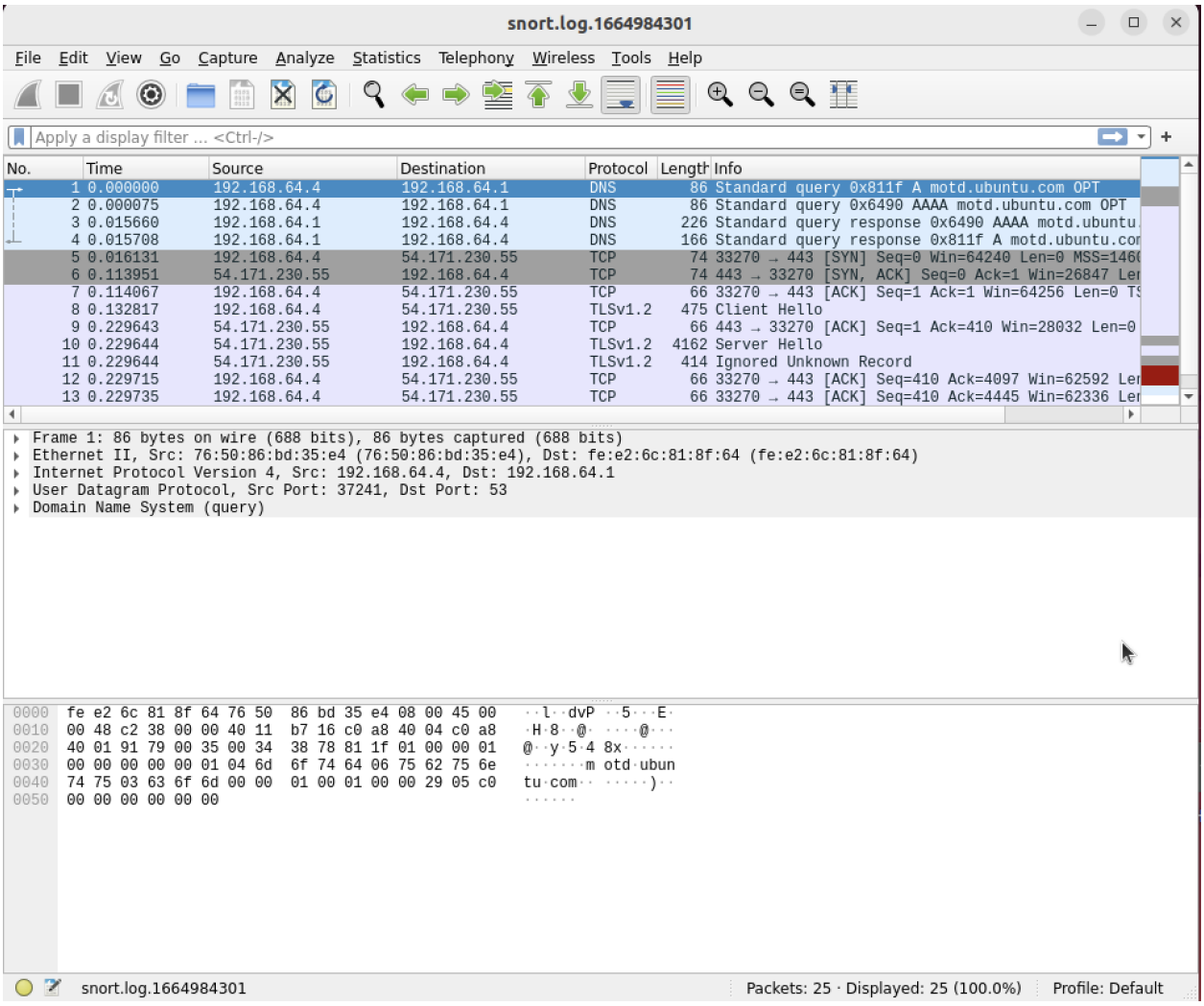
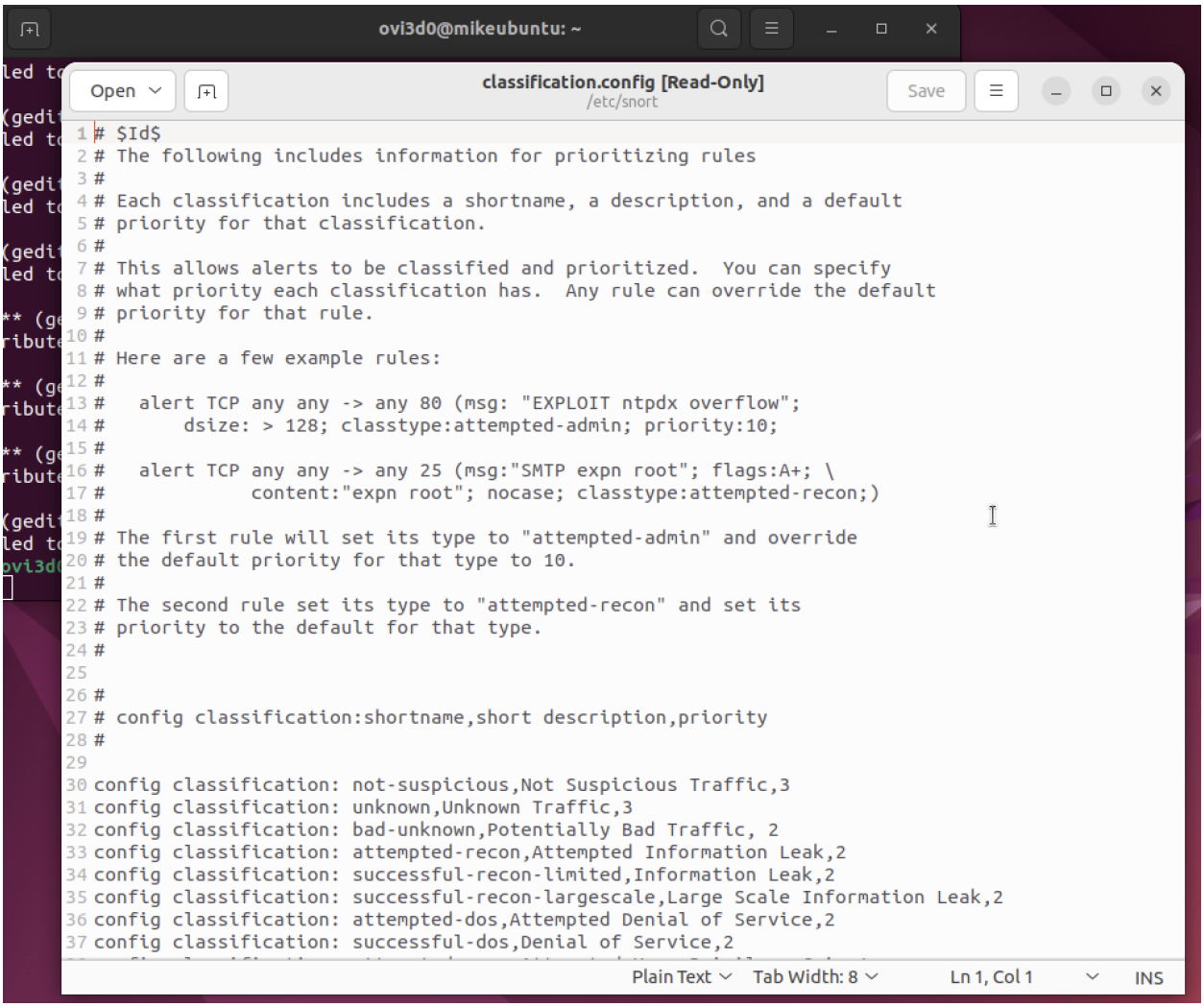
# Assignment 4 - Wireshark and Snort IDS

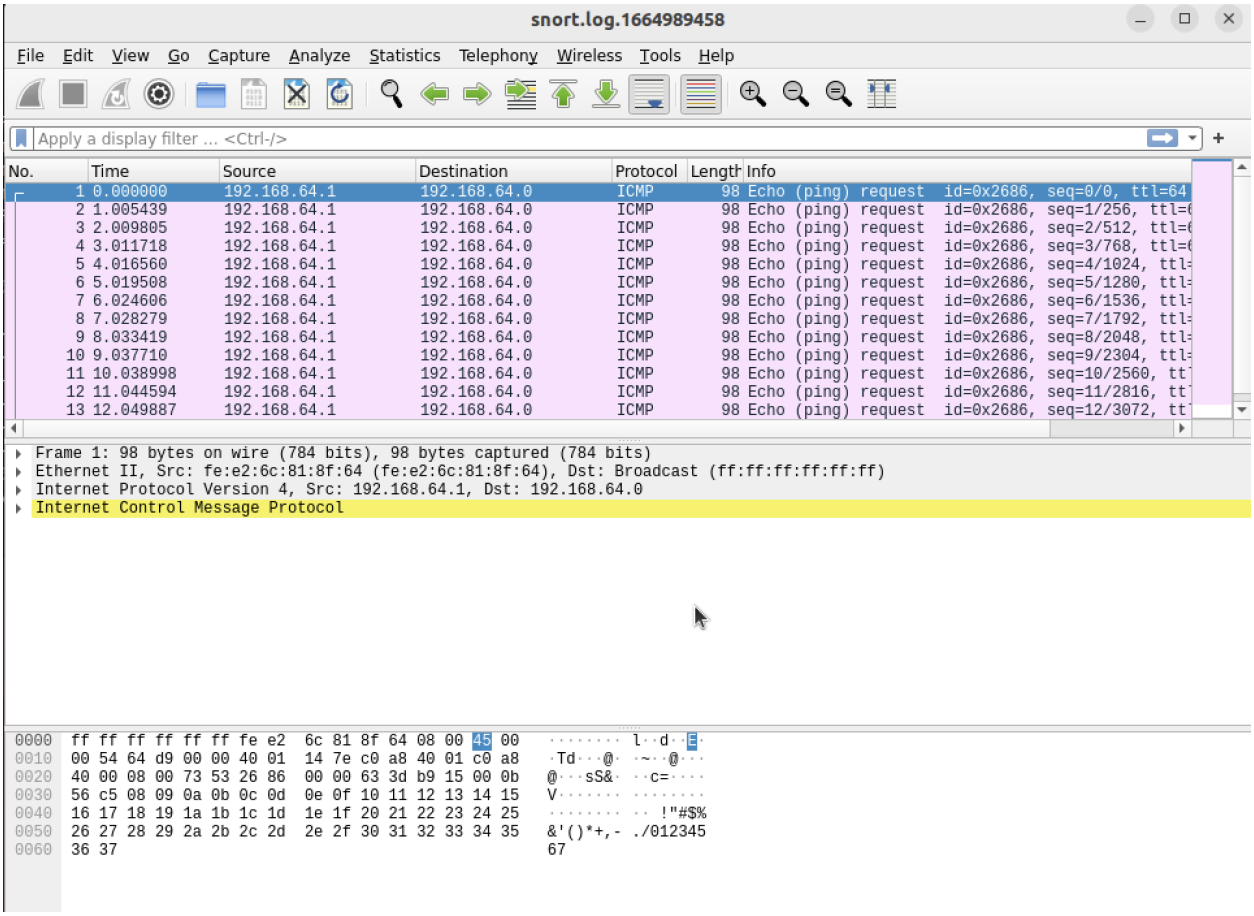


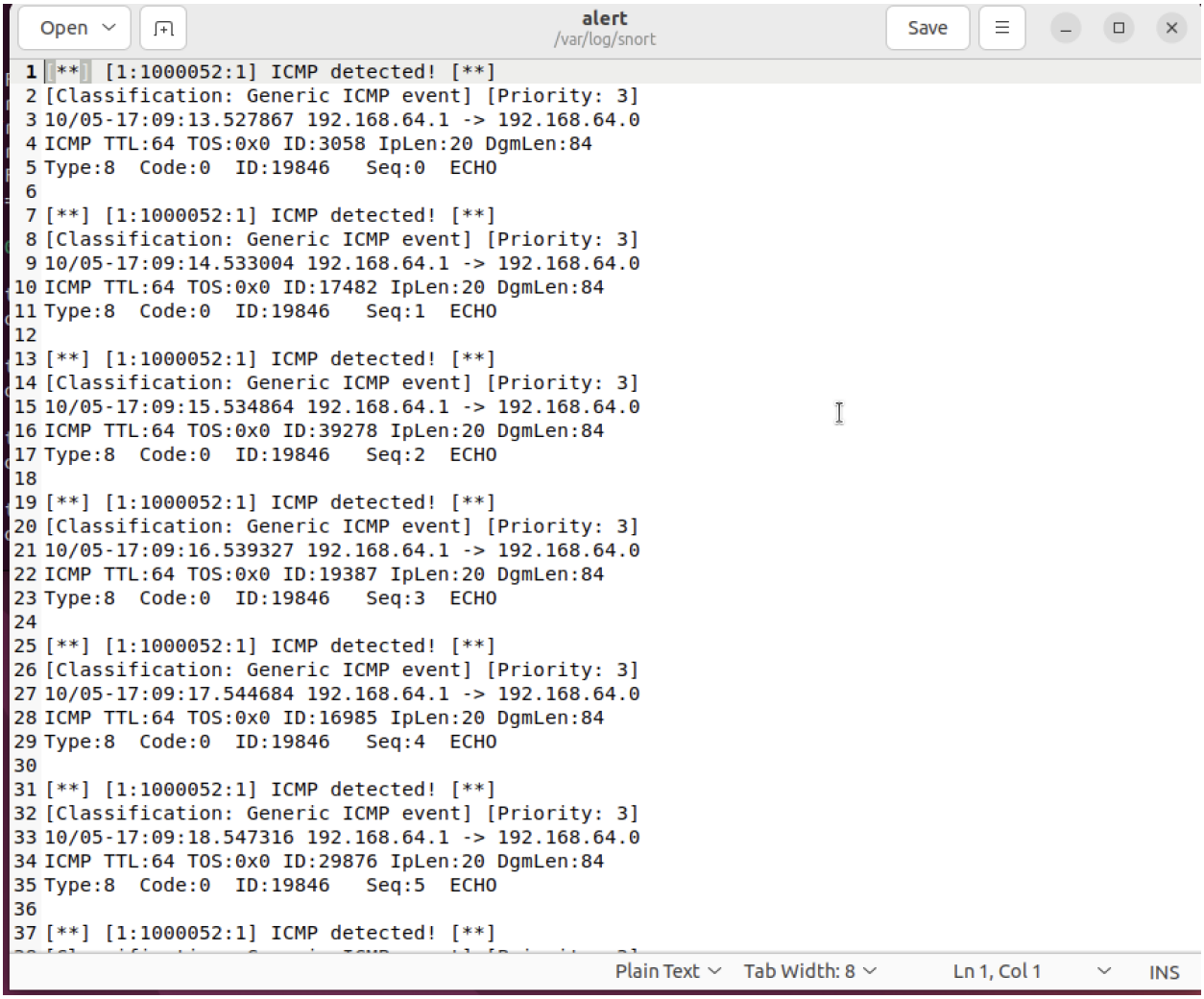
```
26  sudo snort -l .
27  ls
28  sudo wireshark snort.log.1664984301
29  sudo apt-get install wireshark
30  ls
31  clear
32  ls
33  sudo wireshark snort.log.1664983301
34  history
```

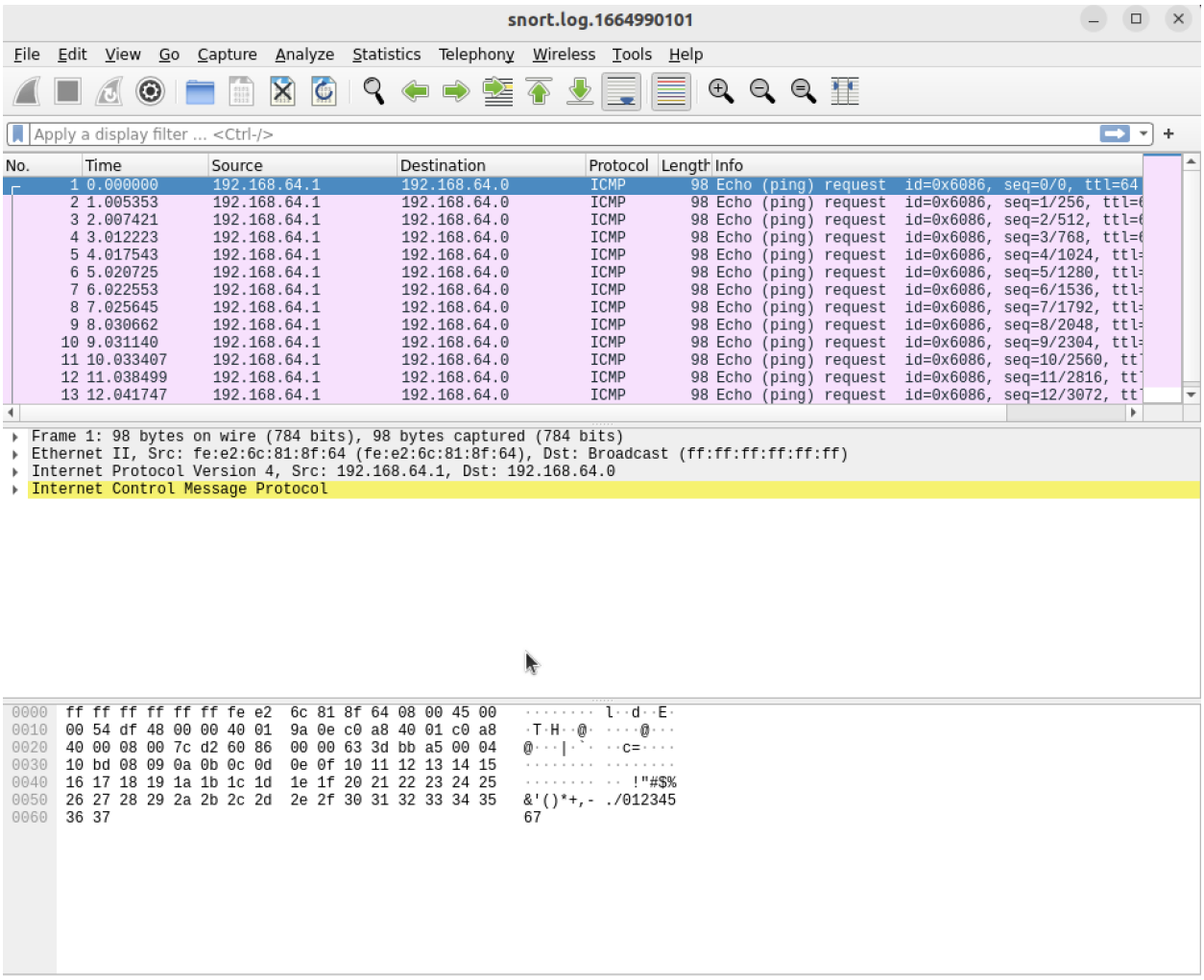


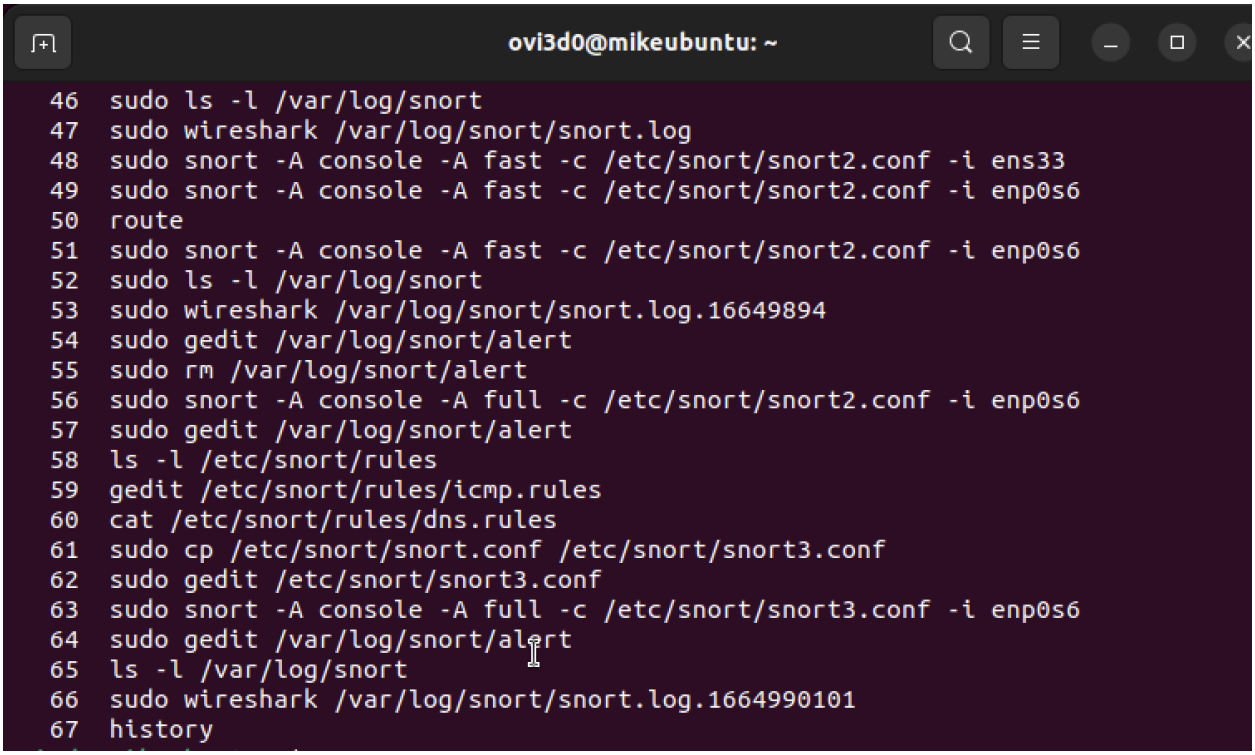

ovi3d0@mikeubuntu: ~
Open
classification.config [Read-Only]
/etc/snort
Save
# $Id$
# The following includes information for prioritizing rules
#
# Each classification includes a shortname, a description, and a default
# priority for that classification.
#
# This allows alerts to be classified and prioritized.  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

```
ic ICMP event] [Priority: 3] {ICMP} 192.168.64.1 -> 192.168.64.0
10/05-17:04:24.768887  [**] [1:1000052:1] ICMP detected! [**] [Classification: Gener
ic ICMP event] [Priority: 3] {ICMP} 192.168.64.1 -> 192.168.64.0
10/05-17:04:25.773729  [**] [1:1000052:1] ICMP detected! [**] [Classification: Gener
ic ICMP event] [Priority: 3] {ICMP} 192.168.64.1 -> 192.168.64.0
10/05-17:04:26.776677  [**] [1:1000052:1] ICMP detected! [**] [Classification: Gener
ic ICMP event] [Priority: 3] {ICMP} 192.168.64.1 -> 192.168.64.0
10/05-17:04:27.781775  [**] [1:1000052:1] ICMP detected! [**] [Classification: Gener
ic ICMP event] [Priority: 3] {ICMP} 192.168.64.1 -> 192.168.64.0
10/05-17:04:28.785448  [**] [1:1000052:1] ICMP detected! [**] [Classification: Gener
ic ICMP event] [Priority: 3] {ICMP} 192.168.64.1 -> 192.168.64.0
10/05-17:04:29.790588  [**] [1:1000052:1] ICMP detected! [**] [Classification: Gener
ic ICMP event] [Priority: 3] {ICMP} 192.168.64.1 -> 192.168.64.0
10/05-17:04:30.794879  [**] [1:1000052:1] ICMP detected! [**] [Classification: Gener
ic ICMP event] [Priority: 3] {ICMP} 192.168.64.1 -> 192.168.64.0
10/05-17:04:31.796167  [**] [1:1000052:1] ICMP detected! [**] [Classification: Gener
ic ICMP event] [Priority: 3] {ICMP} 192.168.64.1 -> 192.168.64.0
10/05-17:04:32.801763  [**] [1:1000052:1] ICMP detected! [**] [Classification: Gener
ic ICMP event] [Priority: 3] {ICMP} 192.168.64.1 -> 192.168.64.0
10/05-17:04:33.807056  [**] [1:1000052:1] ICMP detected! [**] [Classification: Gener
ic ICMP event] [Priority: 3] {ICMP} 192.168.64.1 -> 192.168.64.0
10/05-17:04:34.809694  [**] [1:1000052:1] ICMP detected! [**] [Classification: Gener
ic ICMP event] [Priority: 3] {ICMP} 192.168.64.1 -> 192.168.64.0
```




Open
alert
/var/log/snort
Save
1 [**] [1:1000052:1] ICMP detected! [**]
2 [Classification: Generic ICMP event] [Priority: 3]
3 10/05-17:09:13.527867 192.168.64.1 -> 192.168.64.0
4 ICMP TTL:64 TOS:0x0 ID:3058 IpLen:20 DgmLen:84
5 Type:8 Code:0 ID:19846 Seq:0 ECHO
6
7 [**] [1:1000052:1] ICMP detected! [**]
8 [Classification: Generic ICMP event] [Priority: 3]
9 10/05-17:09:14.533004 192.168.64.1 -> 192.168.64.0
10 ICMP TTL:64 TOS:0x0 ID:17482 IpLen:20 DgmLen:84
11 Type:8 Code:0 ID:19846 Seq:1 ECHO
12
13 [**] [1:1000052:1] ICMP detected! [**]
14 [Classification: Generic ICMP event] [Priority: 3]
15 10/05-17:09:15.534864 192.168.64.1 -> 192.168.64.0
16 ICMP TTL:64 TOS:0x0 ID:39278 IpLen:20 DgmLen:84
17 Type:8 Code:0 ID:19846 Seq:2 ECHO
18
19 [**] [1:1000052:1] ICMP detected! [**]
20 [Classification: Generic ICMP event] [Priority: 3]
21 10/05-17:09:16.539327 192.168.64.1 -> 192.168.64.0
22 ICMP TTL:64 TOS:0x0 ID:19387 IpLen:20 DgmLen:84
23 Type:8 Code:0 ID:19846 Seq:3 ECHO
24
25 [**] [1:1000052:1] ICMP detected! [**]
26 [Classification: Generic ICMP event] [Priority: 3]
27 10/05-17:09:17.544684 192.168.64.1 -> 192.168.64.0
28 ICMP TTL:64 TOS:0x0 ID:16985 IpLen:20 DgmLen:84
29 Type:8 Code:0 ID:19846 Seq:4 ECHO
30
31 [**] [1:1000052:1] ICMP detected! [**]
32 [Classification: Generic ICMP event] [Priority: 3]
33 10/05-17:09:18.547316 192.168.64.1 -> 192.168.64.0
34 ICMP TTL:64 TOS:0x0 ID:29876 IpLen:20 DgmLen:84
35 Type:8 Code:0 ID:19846 Seq:5 ECHO
36
37 [**] [1:1000052:1] ICMP detected! [**]
Plain Text
Tab Width: 8
Ln 1, Col 1
INS


snort.log.1664990101
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
1 0.000000 192.168.64.1 192.168.64.0 ICMP 98 Echo (ping) request id=0x6086, seq=0/0, ttl=64
2 1.005353 192.168.64.1 192.168.64.0 ICMP 98 Echo (ping) request id=0x6086, seq=1/256, ttl=6
3 2.007421 192.168.64.1 192.168.64.0 ICMP 98 Echo (ping) request id=0x6086, seq=2/512, ttl=6
4 3.012223 192.168.64.1 192.168.64.0 ICMP 98 Echo (ping) request id=0x6086, seq=3/768, ttl=6
5 4.017543 192.168.64.1 192.168.64.0 ICMP 98 Echo (ping) request id=0x6086, seq=4/1024, ttl=
6 5.020725 192.168.64.1 192.168.64.0 ICMP 98 Echo (ping) request id=0x6086, seq=5/1280, ttl=
7 6.022553 192.168.64.1 192.168.64.0 ICMP 98 Echo (ping) request id=0x6086, seq=6/1536, ttl=
8 7.025645 192.168.64.1 192.168.64.0 ICMP 98 Echo (ping) request id=0x6086, seq=7/1792, ttl=
9 8.030662 192.168.64.1 192.168.64.0 ICMP 98 Echo (ping) request id=0x6086, seq=8/2048, ttl=
10 9.031140 192.168.64.1 192.168.64.0 ICMP 98 Echo (ping) request id=0x6086, seq=9/2304, ttl=
11 10.033407 192.168.64.1 192.168.64.0 ICMP 98 Echo (ping) request id=0x6086, seq=10/2560, tt
12 11.038499 192.168.64.1 192.168.64.0 ICMP 98 Echo (ping) request id=0x6086, seq=11/2816, tt
13 12.041747 192.168.64.1 192.168.64.0 ICMP 98 Echo (ping) request id=0x6086, seq=12/3072, tt
Frame 1: 98 bytes on wire (784 bits), 98 bytes captured (784 bits)
Ethernet II, Src: fe:e2:6c:81:8f:64 (fe:e2:6c:81:8f:64), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Internet Protocol Version 4, Src: 192.168.64.1, Dst: 192.168.64.0
Internet Control Message Protocol
0000 ff ff ff ff ff ff fe e2 6c 81 8f 64 08 00 45 00
0010 00 54 df 48 00 00 40 01 9a 0e c0 a8 40 01 c0 a8
0020 40 00 08 00 7c d2 60 86 00 00 63 3d bb a5 00 04
0030 10 bd 08 09 0a 0b 0c 0d 0e 0f 10 11 12 13 14 15
0040 16 17 18 19 1a 1b 1c 1d 1e 1f 20 21 22 23 24 25
0050 26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 32 33 34 35
0060 36 37


ovi3d0@mikeubuntu: ~
46 sudo ls -l /var/log/snort
47 sudo wireshark /var/log/snort/snort.log
48 sudo snort -A console -A fast -c /etc/snort/snort2.conf -i ens33
49 sudo snort -A console -A fast -c /etc/snort/snort2.conf -i enp0s6
50 route
51 sudo snort -A console -A fast -c /etc/snort/snort2.conf -i enp0s6
52 sudo ls -l /var/log/snort
53 sudo wireshark /var/log/snort/snort.log.16649894
54 sudo gedit /var/log/snort/alert
55 sudo rm /var/log/snort/alert
56 sudo snort -A console -A full -c /etc/snort/snort2.conf -i enp0s6
57 sudo gedit /var/log/snort/alert
58 ls -l /etc/snort/rules
59 gedit /etc/snort/rules/icmp.rules
60 cat /etc/snort/rules/dns.rules
61 sudo cp /etc/snort/snort.conf /etc/snort/snort3.conf
62 sudo gedit /etc/snort/snort3.conf
63 sudo snort -A console -A full -c /etc/snort/snort3.conf -i enp0s6
64 sudo gedit /var/log/snort/alert
65 ls -l /var/log/snort
66 sudo wireshark /var/log/snort/snort.log.1664990101
67 history