

Assignment 4 - Wireshark and Snort IDS

```
ovi3d0@mikeubuntu:~$ history
 1  sudo apt update
 2  sudo apt install ubuntu-desktop
 3  sudo reboot
 4  sudo apt update
 5  sudo apt upgrae
 6  sudo apt upgrade
 7  sudo apt install snort
 8  snort -h | less
 9  man snort
10  snort -V
11  ip a
12  sudo snort -v
13  sudo snort -v -i ens33
14  sudo snort -v -i enp0s6
15  sudo snort -v -i lo
16  history
17  sudo snort -vd
18  sudo snort -ve
19  sudo snort -vde
20  history
```

```

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

```

snort.log.1664984301

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	192.168.64.4	192.168.64.1	DNS	86	Standard query 0x811f A motd.ubuntu.com OPT
2	0.000075	192.168.64.4	192.168.64.1	DNS	86	Standard query response 0x6490 AAAA motd.ubuntu.com OPT
3	0.015660	192.168.64.1	192.168.64.4	DNS	226	Standard query response 0x6490 AAAA motd.ubuntu.com OPT
4	0.015708	192.168.64.1	192.168.64.4	DNS	166	Standard query response 0x811f A motd.ubuntu.com OPT
5	0.016131	192.168.64.4	54.171.230.55	TCP	74	33270 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460
6	0.113951	54.171.230.55	192.168.64.4	TCP	74	443 → 33270 [SYN, ACK] Seq=0 Ack=1 Win=26847 Len=0
7	0.114067	192.168.64.4	54.171.230.55	TCP	66	33270 → 443 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TS=0
8	0.132817	192.168.64.4	54.171.230.55	TLSv1.2	475	Client Hello
9	0.229643	54.171.230.55	192.168.64.4	TCP	66	443 → 33270 [ACK] Seq=1 Ack=410 Win=28032 Len=0
10	0.229644	54.171.230.55	192.168.64.4	TLSv1.2	4162	Server Hello
11	0.229644	54.171.230.55	192.168.64.4	TLSv1.2	414	Ignored Unknown Record
12	0.229715	192.168.64.4	54.171.230.55	TCP	66	33270 → 443 [ACK] Seq=410 Ack=4097 Win=62592 Len=0
13	0.229735	192.168.64.4	54.171.230.55	TCP	66	33270 → 443 [ACK] Seq=410 Ack=4445 Win=62336 Len=0

Frame 1: 86 bytes on wire (688 bits), 86 bytes captured (688 bits) on interface 0

Ethernet II, Src: 76:50:86:bd:35:e4 (76:50:86:bd:35:e4), Dst: fe:e2:6c:81:8f:64 (fe:e2:6c:81:8f:64)

Internet Protocol Version 4, Src: 192.168.64.4, Dst: 192.168.64.1

User Datagram Protocol, Src Port: 37241, Dst Port: 53

Domain Name System (query)

0000 fe e2 6c 81 8f 64 76 50 86 bd 35 e4 08 00 45 00 ..l..dvP..5..E..

0010 00 48 c2 38 00 00 40 11 b7 16 c0 a8 00 04 c0 a8 .H.8..@...@...

0020 40 01 91 79 00 35 00 34 38 78 81 1f 01 00 00 01 @..y.5.4.8x.....

0030 00 00 00 00 00 01 04 6d 6f 74 64 06 75 62 75 6em otd-ubun

0040 74 75 03 63 6f 6d 00 00 01 00 01 00 00 29 05 c0 tu-com.. ..)

0050 00 00 00 00 00 00

snort.log.1664984301 Packets: 25 · Displayed: 25 (100.0%) Profile: Default

```
1 # $Id$
2 # The following includes information for prioritizing rules
3 #
4 # Each classification includes a shortname, a description, and a default
5 # priority for that classification.
6 #
7 # This allows alerts to be classified and prioritized. You can specify
8 # what priority each classification has. Any rule can override the default
9 # priority for that rule.
10 #
11 # Here are a few example rules:
12 #
13 # alert TCP any any -> any 80 (msg: "EXPLOIT ntpdx overflow";
14 #   dsize: > 128; classtype:attempted-admin; priority:10;
15 #
16 # alert TCP any any -> any 25 (msg:"SMTP expn root"; flags:A+; \
17 #   content:"expn root"; nocase; classtype:attempted-recon;)
18 #
19 # The first rule will set its type to "attempted-admin" and override
20 # the default priority for that type to 10.
21 #
22 # The second rule set its type to "attempted-recon" and set its
23 # priority to the default for that type.
24 #
25
26 #
27 # config classification:shortname,short description,priority
28 #
29
30 config classification: not-suspicious,Not Suspicious Traffic,3
31 config classification: unknown,Unknown Traffic,3
32 config classification: bad-unknown,Potentially Bad Traffic, 2
33 config classification: attempted-recon,Attempted Information Leak,2
34 config classification: successful-recon-limited,Information Leak,2
35 config classification: successful-recon-largescale,Large Scale Information Leak,2
36 config classification: attempted-dos,Attempted Denial of Service,2
37 config classification: successful-dos,Denial of Service,2
```

```

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

```

snort.log.1664989458

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=0x2686, seq=0/0, ttl=64
2	1.005439	192.168.64.1	192.168.64.0	ICMP	98	Echo (ping) request id=0x2686, seq=1/256, ttl=64
3	2.009805	192.168.64.1	192.168.64.0	ICMP	98	Echo (ping) request id=0x2686, seq=2/512, ttl=64
4	3.011718	192.168.64.1	192.168.64.0	ICMP	98	Echo (ping) request id=0x2686, seq=3/768, ttl=64
5	4.016560	192.168.64.1	192.168.64.0	ICMP	98	Echo (ping) request id=0x2686, seq=4/1024, ttl=64
6	5.019508	192.168.64.1	192.168.64.0	ICMP	98	Echo (ping) request id=0x2686, seq=5/1280, ttl=64
7	6.024606	192.168.64.1	192.168.64.0	ICMP	98	Echo (ping) request id=0x2686, seq=6/1536, ttl=64
8	7.028279	192.168.64.1	192.168.64.0	ICMP	98	Echo (ping) request id=0x2686, seq=7/1792, ttl=64
9	8.033419	192.168.64.1	192.168.64.0	ICMP	98	Echo (ping) request id=0x2686, seq=8/2048, ttl=64
10	9.037710	192.168.64.1	192.168.64.0	ICMP	98	Echo (ping) request id=0x2686, seq=9/2304, ttl=64
11	10.038998	192.168.64.1	192.168.64.0	ICMP	98	Echo (ping) request id=0x2686, seq=10/2560, ttl=64
12	11.044594	192.168.64.1	192.168.64.0	ICMP	98	Echo (ping) request id=0x2686, seq=11/2816, ttl=64
13	12.049887	192.168.64.1	192.168.64.0	ICMP	98	Echo (ping) request id=0x2686, seq=12/3072, ttl=64

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 e2 6c 81 8f 64 08 00 45 00  .....l..d..E
0010  00 54 64 d9 00 00 40 01 14 7e c0 a8 40 01 c0 a8  .Td...@...@...
0020  40 00 08 00 73 53 26 86 00 00 63 3d b9 15 00 0b  @...sS&...c=...
0030  56 c5 08 09 0a 0b 0c 0d 0e 0f 10 11 12 13 14 15  V.....
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  &'()*+,-./012345
0060  36 37                                     67

```

```
Open [v] [f] 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! [**]
```

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=64
3	2.007421	192.168.64.1	192.168.64.0	ICMP	98	Echo (ping) request id=0x6086, seq=2/512, ttl=64
4	3.012223	192.168.64.1	192.168.64.0	ICMP	98	Echo (ping) request id=0x6086, seq=3/768, ttl=64
5	4.017543	192.168.64.1	192.168.64.0	ICMP	98	Echo (ping) request id=0x6086, seq=4/1024, ttl=64
6	5.020725	192.168.64.1	192.168.64.0	ICMP	98	Echo (ping) request id=0x6086, seq=5/1280, ttl=64
7	6.022553	192.168.64.1	192.168.64.0	ICMP	98	Echo (ping) request id=0x6086, seq=6/1536, ttl=64
8	7.025645	192.168.64.1	192.168.64.0	ICMP	98	Echo (ping) request id=0x6086, seq=7/1792, ttl=64
9	8.030662	192.168.64.1	192.168.64.0	ICMP	98	Echo (ping) request id=0x6086, seq=8/2048, ttl=64
10	9.031140	192.168.64.1	192.168.64.0	ICMP	98	Echo (ping) request id=0x6086, seq=9/2304, ttl=64
11	10.033407	192.168.64.1	192.168.64.0	ICMP	98	Echo (ping) request id=0x6086, seq=10/2560, ttl=64
12	11.038499	192.168.64.1	192.168.64.0	ICMP	98	Echo (ping) request id=0x6086, seq=11/2816, ttl=64
13	12.041747	192.168.64.1	192.168.64.0	ICMP	98	Echo (ping) request id=0x6086, seq=12/3072, ttl=64

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  .....l..d..E.
0010  00 54 df 48 00 00 40 01  9a 0e c0 a8 40 01 c0 a8  .T.H..@...@...
0020  40 00 08 00 7c d2 60 86  00 00 63 3d bb a5 00 04  @...|...c=...
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  .....&'()*+,-./012345
0050  26 27 28 29 2a 2b 2c 2d  2e 2f 30 31 32 33 34 35  .....
0060  36 37                                     67
  
```

```
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
```