

Lab 5

Snort Intrusion Detection System

```
chrisjoy@chris-macbook ~  
$ snort -vde
```

```

    ---== Initializing Snort ===
    Initializing Output Plugins!
    pcap DAQ configured to passive.
    Acquiring network traffic from "en0".
    Decoding Ethernet

    ---== Initialization Complete ===

```

```
Commencing packet processing (pid=27036)
WARNING: No preprocessors configured for policy 0.
04/10-13:13:21.641552 A4:83:E7:2D:DD:AA -> 68:FF:7B:A4:9A:69 type:0x800 len:0x41
192.168.1.8:61274 -> 216.58.200.110:443 UDP TTL:64 TOS:0x0 ID:34856 IpLen:20 DgmLen:51
Len: 23
40 61 44 AC 1F 29 58 4E AC 83 5A 01 5A F2 09 F7  @aD..)XN..Z.Z...
E7 14 17 DD B2 33 86 .....3.
```

```
WARNING: No preprocessors configured for policy 0.
04/10-13:13:21.662503 68:FF:7B:A4:9A:69 -> A4:83:E7:2D:DD:AA type:0x800 len:0x3F
216.58.200.110:443 -> 192.168.1.8:61274 UDP TTL:60 TOS:0x0 ID:0 IpLen:20 DgmLen:49 DF
Len: 21
40 FE 06 51 A2 2B AD BF 53 2A 2B 3D 86 E4 B3 1D  @..Q.+..S*+=....
0F FA CD 71 45      ...gE
```

```
WARNING: No preprocessors configured for policy 0.
04/10-13:13:21.769509 68:FF:7B:A4:9A:69 -> 33:33:00:00:00:01 type:0x86DD len:0x56
fe80::6aff:7bff:fea4:9a69 -> ff02::1 IPV6-ICMP TTL:255 TOS:0x0 ID:0 IpLen:40 DgmLen:72
40 C0 00 00 00 00 00 00 00 00 00 00 00 05 01 00 00 @.....
00 00 05 DC 01 01 68 FF 7B A4 9A 69 .....h.{.i
```

```

WARNING: No preprocessors configured for policy 0.
04/10-13:13:22.079516 68:FF:7B:A4:9A:69 -> A4:83:E7:2D:DD:AA type:0x800 len:0x181
162.159.130.234:443 -> 192.168.1.8:59643 TCP TTL:59 TOS:0x0 ID:51223 IpLen:20 DgmLen:371 DF
***AP*** Seq: 0xA72CAF80 Ack: 0x39A3369C Win: 0x46 TcpLen: 20
17 03 03 01 46 5E 72 6A EF 86 8C B0 35 C1 BD 86 ....F^rj....5...
AB CE D0 47 25 CC C9 B4 43 D9 BA 1E 40 1D 90 7E ...G%...C...@..~
97 16 2D C0 E4 AA 57 B6 F3 AB 33 37 F8 15 00 A7 ..-...W...37....
A9 23 AF 58 48 24 2B 6F 1C CE 6B 55 69 68 A0 3D .#.XHS+o...kUih.=
7A 26 21 D8 3E A9 CF 13 9D A9 2F F4 16 C3 98 79 z&!.>...../.....y
93 CF E5 1C D6 A1 C2 CA 1D CC CB 2D 46 4A 48 0E .....-FJH.
0D 28 6E 24 F2 7E 3A 58 5A 6D FF 90 81 62 AE 04 .(n$.~:XZm...b..
BA 56 39 65 A5 10 60 EB 90 12 B0 EF FC 83 81 22 .V9e...`....."
BE A2 CA EE 5F 63 AE 3C CA D5 5A E2 3F D8 6E 76 ...._c.<..Z.?.nv
1A 7C B4 B6 8A 57 37 3F 48 A3 9E F8 0F E2 02 2A .|...W7?H.....*
E7 6D A2 E7 52 1E 2E 55 5D 4A 1F 45 28 F7 60 FD .m..R..U]J.E(.
DA 1B 73 83 55 29 CA ED BC 03 C4 DF CC 84 E7 87 ..s.U).....
66 22 7B 10 56 F7 CC 81 83 9A 96 4E 34 D0 54 AB f"{.V.....N4.T.
5F 30 D8 28 22 09 5A 7C 01 8F FB 99 FC B5 7B 73 _0.(".Z|.....{s
DF FE EC 42 42 4E 48 48 60 6F 3E 15 CD C6 21 D1 A3 ...BNHH'o>....!..
D0 6F EC 0E 0D 49 83 D0 0F 19 76 DF E1 28 C8 EC .o...I...v..{..

```

Task 2 - Run a command in snort to capture only ICMP packets. (For testing, you may have to use ping to generate some ICMP packets if your network is not busy)

```

chrisjoy@chris-macbook ~/tmp
$ sudo snort -c snort.rules -l log -i en1

Running in packet dump mode

--== Initializing Snort ==--
Initializing Output Plugins!
pcap DAQ configured to passive.
Acquiring network traffic from "en0".
Decoding Ethernet

--== Initialization Complete ==--

,,-
o" )~
'''
-*> Snort! <*-
Version 2.9.12 GRE (Build 325)
By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
Copyright (C) 2014-2018 Cisco and/or its affiliates. All rights reserved.
Copyright (C) 1998-2013 Sourcefire, Inc., et al.
Using libpcap version 1.9.1
Using PCRE version: 8.44 2020-02-12
Using ZLIB version: 1.2.11

Commencing packet processing (pid=27747)
WARNING: No preprocessors configured for policy 0.
WARNING: No preprocessors configured for policy 0.
04/10-13:38:03.650393 192.168.1.8 -> 216.58.200.110
ICMP TTL:64 TOS:0x0 ID:49112 IpLen:20 DgmLen:84
Type:8 Code:0 ID:20332 Seq:20 ECHO
=====
WARNING: No preprocessors configured for policy 0.
04/10-13:38:03.668265 216.58.200.110 -> 192.168.1.8
ICMP TTL:57 TOS:0x0 ID:0 IpLen:20 DgmLen:84
Type:0 Code:0 ID:20332 Seq:20 ECHO REPLY
=====

```

Task 3 - Execute: `snort -c /etc/snort/snort.conf -l /var/log/snort -K ascii -i eth0`, Examine the alert file in the `/var/log/snort` folder. Did you find alerts generated by your rule?

Yes, found the alert file containing all the logs in /var/log/snort/alert. As shown below:

```

[~] cat log/alert
[**] [1:1000002:0] IP Packet detected [**]
[Priority: 0]
04/10-13:41:19.166480 111.221.29.254:443 -> 192.168.1.8:60055
TCP TTL:110 TOS:0x0 ID:1770 IpLen:20 DgmLen:1480 DF
***** Seq: 0x2BC97E96 Ack: 0xC5747020 Win: 0x402 TcpLen: 32
TCP Options (3) => NOP NOP TS: 3559006666 1807623379

[**] [1:1000002:0] IP Packet detected [**]
[Priority: 0]
04/10-13:41:19.166932 111.221.29.254:443 -> 192.168.1.8:60055
TCP TTL:110 TOS:0x0 ID:1771 IpLen:20 DgmLen:1480 DF
***** Seq: 0x2BC9842A Ack: 0xC5747020 Win: 0x402 TcpLen: 32
TCP Options (3) => NOP NOP TS: 3559006666 1807623379


[**] [1:1000002:0] IP Packet detected [**]
[Priority: 0]
04/10-13:41:19.167018 192.168.1.8:60055 -> 111.221.29.254:443
TCP TTL:64 TOS:0x0 ID:0 IpLen:20 DgmLen:52 DF
***** Seq: 0xC5747020 Ack: 0x2BC989BE Win: 0x7E9 TcpLen: 32
TCP Options (3) => NOP NOP TS: 1807623508 3559006666

[**] [1:1000002:0] IP Packet detected [**]
[Priority: 0]
04/10-13:41:19.167590 111.221.29.254:443 -> 192.168.1.8:60055
TCP TTL:110 TOS:0x0 ID:1772 IpLen:20 DgmLen:1221 DF
***** Seq: 0x2BC989BE Ack: 0xC5747020 Win: 0x402 TcpLen: 32
TCP Options (3) => NOP NOP TS: 3559006666 1807623379

[**] [1:1000002:0] IP Packet detected [**]
[Priority: 0]
04/10-13:41:19.167689 192.168.1.8:60055 -> 111.221.29.254:443
TCP TTL:64 TOS:0x0 ID:0 IpLen:20 DgmLen:52 DF
***** Seq: 0xC5747020 Ack: 0x2BC989BE Win: 0x7E9 TcpLen: 32
TCP Options (3) => NOP NOP TS: 1807623508 3559006666


```

This rule is bad as it doesn't convey any information and just indicates that snort is working, alerting when an IP packet has been detected (which is pretty much the majority of packets flowing through the NIC).

```
Users > chrisjoy > tmp >  snort.rules
1  alert icmp any any -> 192.168.0.1 any (msg: "ICMP Packet found";)
```

Task 5 - Explain what the following rule is doing? `alert tcp !192.168.1.0/24 any -> 192.168.1.0/24 !:1024`


This rule basically states to alert when TCP packets not from source 192.168.1.0/24 on any port being send to the source 192.168.1.0/24 on port 1024. In essence, it seems like a rule to filter out packets that are going from the current host to the router on port 1024, which is a reserved port (perhaps used to detect an intrusion).

```
Users > chrisjoy > tmp >  snort.rules
1 alert tcp any any -> any 80 (msg:"HTTP GET Request"; \
2 flow:to_server,established; content:"GET"; nocase; http_method; \
3 detection_filter:track by_src, count 30, seconds 30; metadata: service http;)
4 |
```

```
chrisjoy@chris-macbook ~/tmp
$ sudo snort -c snort.rules -l log -i en1
```


Task 8 - Write a rule that detects a telnet session initiation. Once this session is detected, the rule should log the next 10 packets of this session. Note: You need to telnet to any free telnet server (such as telehack.com) to check whether your rule is working or not.

Rule:

```
Users > chrisjoy > tmp >  snort.rules
1 alert tcp any any -> any 23 (msg:"Telnet Request"; threshold:type limit, track \
2 by_src, count 10, seconds 60; sid: 1234213;)
```

Connecting to telnet server:

```
chrisjoy@chris-macbook ~/tmp
$ telnet telehack.com
Trying 64.13.139.230...
Connected to telehack.com.
Escape character is '^]'.

Connected to TELEHACK port 35

It is 10:52 pm on Thursday, April 9, 2020 in Mountain View, California, USA.
There are 51 local users. There are 26638 hosts on the network.
```

```
Type HELP for a detailed command list.
Type NEWUSER to create an account.
```

May the command line live forever.

Command, one of the following:

2048	?	a2	ac	advent	basic
bf	c8	cal	calc	ching	clear
clock	cowsay	date	ddate	echo	eliza
factor	figlet	finger	fnord	geopip	help
hosts	ipaddr	joke	login	mac	md5
morse	newuser	notes	octopus	phoon	pig
ping	primes	privacy	qr	rain	rand
rfc	rig	roll	rot13	sleep	starwars
traceroute	units	uptime	usenet	users	uumap
uupath	uuplot	weather	when	zc	zork
zrun					

[.?

Snort command/logs:

```
chrisjoy@chris-macbook ~/tmp
$ sudo snort -c snort.rules -l log -i en1

chrisjoy@chris-macbook ~/tmp
$ cat log/alert
[**] [1:1234213:0] Telnet Request [**]
[Priority: 0]
04/10-15:52:32.485107 A4:83:E7:2D:DD:AA -> 68:FF:7B:A4:9A:69 type:0x800 len:0x4E
192.168.1.8:60923 -> 64.13.139.230:23 TCP TTL:64 TOS:0x10 ID:0 IpLen:20 DgmLen:64 DF
*****S* Seq: 0x6799F852 Ack: 0x0 Win: 0xFFFF TcpLen: 44
TCP Options (8) => MSS: 1460 NOP WS: 6 NOP NOP TS: 1815449822 0 SackOK EOL

[**] [1:1234213:0] Telnet Request [**]
[Priority: 0]
04/10-15:52:32.659968 A4:83:E7:2D:DD:AA -> 68:FF:7B:A4:9A:69 type:0x800 len:0x42
192.168.1.8:60923 -> 64.13.139.230:23 TCP TTL:64 TOS:0x10 ID:0 IpLen:20 DgmLen:52 DF
***A*** Seq: 0x6799F853 Ack: 0xED5B5A14 Win: 0x804 TcpLen: 32
TCP Options (3) => NOP NOP TS: 1815449996 763412725

[**] [1:1234213:0] Telnet Request [**]
[Priority: 0]
04/10-15:52:32.660474 A4:83:E7:2D:DD:AA -> 68:FF:7B:A4:9A:69 type:0x800 len:0x5D
192.168.1.8:60923 -> 64.13.139.230:23 TCP TTL:64 TOS:0x10 ID:0 IpLen:20 DgmLen:79 DF
***AP*** Seq: 0x6799F853 Ack: 0xED5B5A14 Win: 0x804 TcpLen: 32
TCP Options (3) => NOP NOP TS: 1815449996 763412725
```

```
[**] [1:1234213:0] Telnet Request [**]
[Priority: 0]
04/10-15:52:32.849583 A4:83:E7:2D:DD:AA -> 68:FF:7B:A4:9A:69 type:0x800 len:0x42
192.168.1.8:60923 -> 64.13.139.230:23 TCP TTL:64 TOS:0x10 ID:0 IpLen:20 DgmLen:52 DF
***A**** Seq: 0x6799F86E Ack: 0xED5B5A17 Win: 0x804 TcpLen: 32
TCP Options (3) => NOP NOP TS: 1815450184 763412894

[**] [1:1234213:0] Telnet Request [**]
[Priority: 0]
04/10-15:52:33.017842 A4:83:E7:2D:DD:AA -> 68:FF:7B:A4:9A:69 type:0x800 len:0x42
192.168.1.8:60923 -> 64.13.139.230:23 TCP TTL:64 TOS:0x10 ID:0 IpLen:20 DgmLen:52 DF
***A**** Seq: 0x6799F86E Ack: 0xED5B5A41 Win: 0x804 TcpLen: 32
TCP Options (3) => NOP NOP TS: 1815450351 763413085

[**] [1:1234213:0] Telnet Request [**]
[Priority: 0]
04/10-15:52:33.018123 A4:83:E7:2D:DD:AA -> 68:FF:7B:A4:9A:69 type:0x800 len:0x4E
192.168.1.8:60923 -> 64.13.139.230:23 TCP TTL:64 TOS:0x10 ID:0 IpLen:20 DgmLen:64 DF
***AP*** Seq: 0x6799F86E Ack: 0xED5B5A41 Win: 0x804 TcpLen: 32
TCP Options (3) => NOP NOP TS: 1815450351 763413085

[**] [1:1234213:0] Telnet Request [**]
[Priority: 0]
04/10-15:52:33.185409 A4:83:E7:2D:DD:AA -> 68:FF:7B:A4:9A:69 type:0x800 len:0x42
192.168.1.8:60923 -> 64.13.139.230:23 TCP TTL:64 TOS:0x10 ID:0 IpLen:20 DgmLen:52 DF
***A**** Seq: 0x6799F87A Ack: 0xED5B5E79 Win: 0x7F3 TcpLen: 32
TCP Options (3) => NOP NOP TS: 1815450518 763413251

[**] [1:1234213:0] Telnet Request [**]
[Priority: 0]
04/10-15:52:33.223611 A4:83:E7:2D:DD:AA -> 68:FF:7B:A4:9A:69 type:0x800 len:0x56
192.168.1.8:60923 -> 64.13.139.230:23 TCP TTL:64 TOS:0x10 ID:0 IpLen:20 DgmLen:72 DF
***AP*** Seq: 0x6799F87A Ack: 0xED5B5E79 Win: 0x800 TcpLen: 32
TCP Options (3) => NOP NOP TS: 1815450556 763413291

[**] [1:1234213:0] Telnet Request [**]
[Priority: 0]
04/10-15:52:35.582242 A4:83:E7:2D:DD:AA -> 68:FF:7B:A4:9A:69 type:0x800 len:0x43
192.168.1.8:60923 -> 64.13.139.230:23 TCP TTL:64 TOS:0x10 ID:0 IpLen:20 DgmLen:53 DF
***AP*** Seq: 0x6799F88E Ack: 0xED5B5E79 Win: 0x800 TcpLen: 32
TCP Options (3) => NOP NOP TS: 1815452912 763413458
```