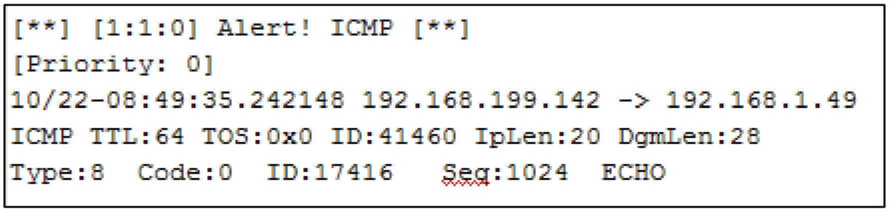
# Snort Lab

- This is an assignment, and worth 2 points.
- The due date is the same day midnight. It will be graded as pass/fail (2 or 0 points).

**Task 1.**

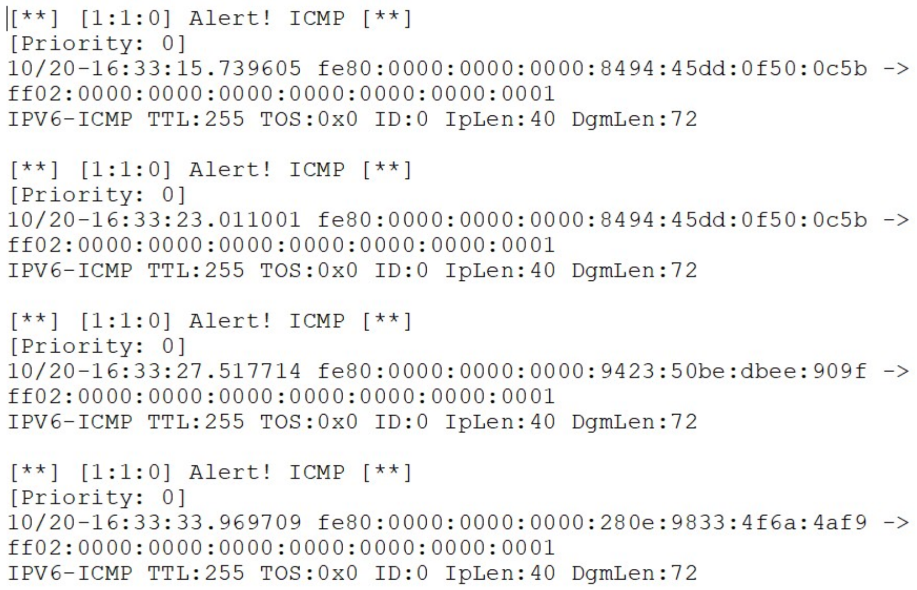
- Create a Snort rule that captures ICMP Echo Request from Kali and shows alerts with the message “Alert! ICMP”. (The *icode* and *itype* options are not necessary.)
- Send five (5) ICMP Echo Request messages from the Kali.

- Display your Snort rule.
- Go to **c:\snort\log** and find the **alert.ids** file. Open it with a text editor. Provide a screenshot for the five alerts you have captured.



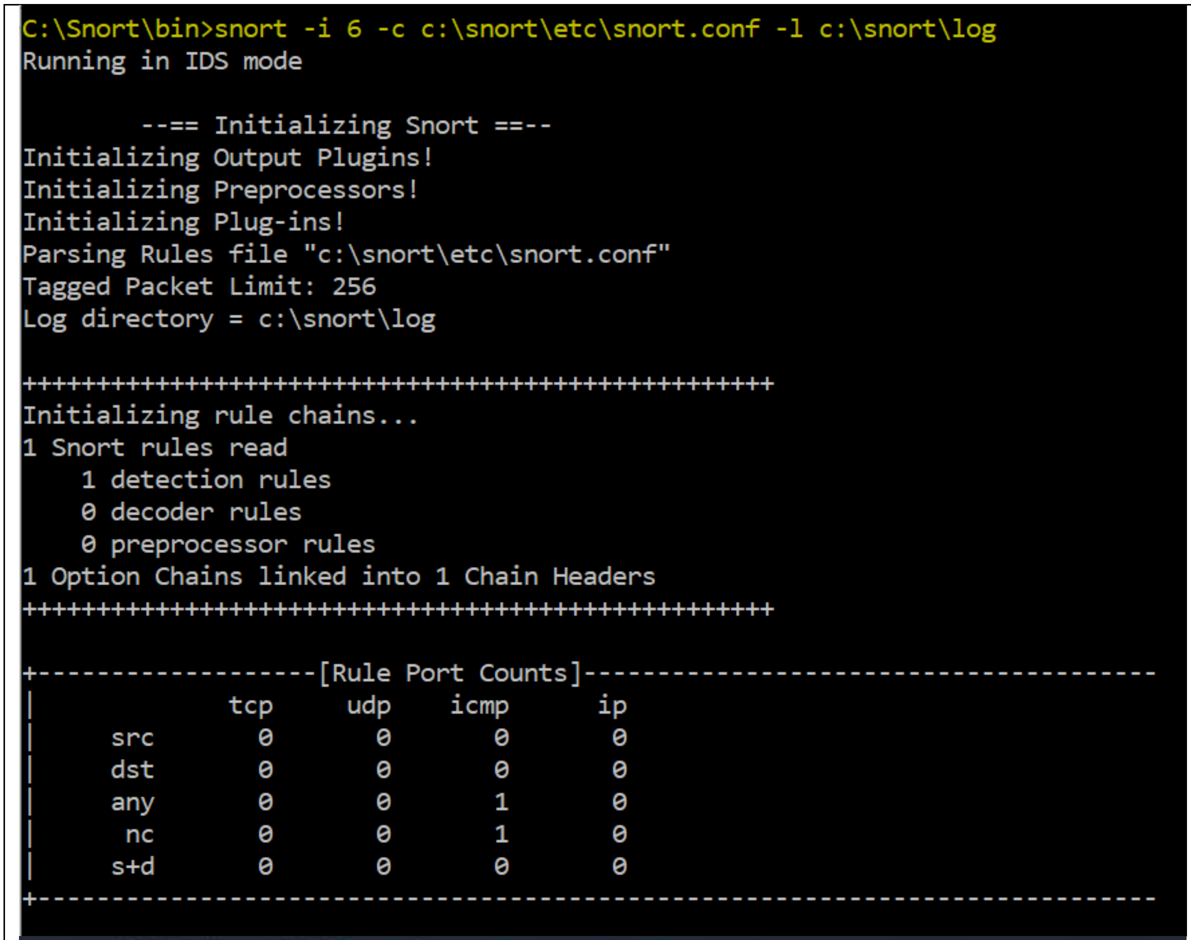
```
[**] [1:1:0] Alert! ICMP [**]
[Priority: 0]
10/22-08:49:35.242148 192.168.199.142 -> 192.168.1.49
ICMP TTL:64 TOS:0x0 ID:41460 IpLen:20 DgmLen:28
Type:8  Code:0  ID:17416   Seq:1024  ECHO
```

**Dr. Im, I tried indexes 1-10 and only 6 displayed anything in the log files. I only received 4 alerts back even though the kali command has 5. I’m unsure why, but I’ve attached screenshots to show you that I’ve configured the file and run the commands correctly.**

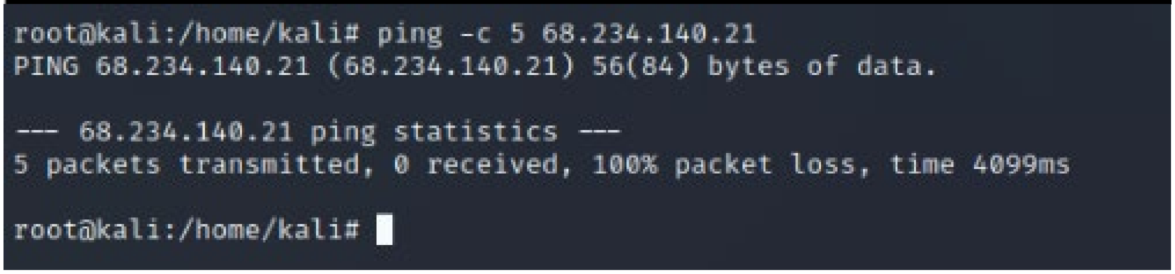


```
[**] [1:1:0] Alert! ICMP [**]
[Priority: 0]
10/20-16:33:15.739605 fe80:0000:0000:0000:8494:45dd:0f50:0c5b ->
ff02:0000:0000:0000:0000:0000:0000:0001
IPV6-ICMP TTL:255 TOS:0x0 ID:0 IpLen:40 DgmLen:72

[**] [1:1:0] Alert! ICMP [**]
[Priority: 0]
10/20-16:33:23.011001 fe80:0000:0000:0000:8494:45dd:0f50:0c5b ->
ff02:0000:0000:0000:0000:0000:0000:0001
IPV6-ICMP TTL:255 TOS:0x0 ID:0 IpLen:40 DgmLen:72

[**] [1:1:0] Alert! ICMP [**]
[Priority: 0]
10/20-16:33:27.517714 fe80:0000:0000:0000:9423:50be:dbee:909f ->
ff02:0000:0000:0000:0000:0000:0000:0001
IPV6-ICMP TTL:255 TOS:0x0 ID:0 IpLen:40 DgmLen:72

[**] [1:1:0] Alert! ICMP [**]
[Priority: 0]
10/20-16:33:33.969709 fe80:0000:0000:0000:280e:9833:4f6a:4af9 ->
ff02:0000:0000:0000:0000:0000:0000:0001
IPV6-ICMP TTL:255 TOS:0x0 ID:0 IpLen:40 DgmLen:72
```

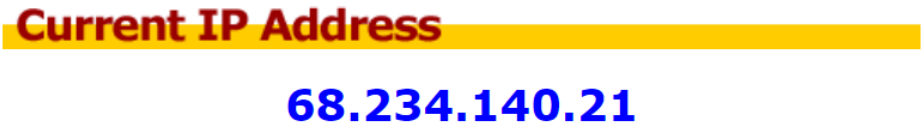
**More below** ⬇



```
C:\Snort\bin>snort -i 6 -c c:\snort\etc\snort.conf -l c:\snort\log
Running in IDS mode

        --== Initializing Snort ==--
Initializing Output Plugins!
Initializing Preprocessors!
Initializing Plug-ins!
Parsing Rules file "c:\snort\etc\snort.conf"
Tagged Packet Limit: 256
Log directory = c:\snort\log

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

+-------------------[Rule Port Counts]---------------------------------------
|             tcp     udp    icmp      ip
|     src       0       0       0       0
|     dst       0       0       0       0
|     any       0       0       1       0
|      nc       0       0       1       0
|     s+d       0       0       0       0
+----------------------------------------------------------------------------
```



```
root@kali:/home/kali# ping -c 5 68.234.140.21
PING 68.234.140.21 (68.234.140.21) 56(84) bytes of data.

--- 68.234.140.21 ping statistics ---
5 packets transmitted, 0 received, 100% packet loss, time 4099ms

root@kali:/home/kali# 
```



Current IP Address

68.234.140.21

```
# Simple ICMP test
var HOME_NET any
var EXTERNAL_NET any
alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"Alert!
ICMP";sid:1;)
```