

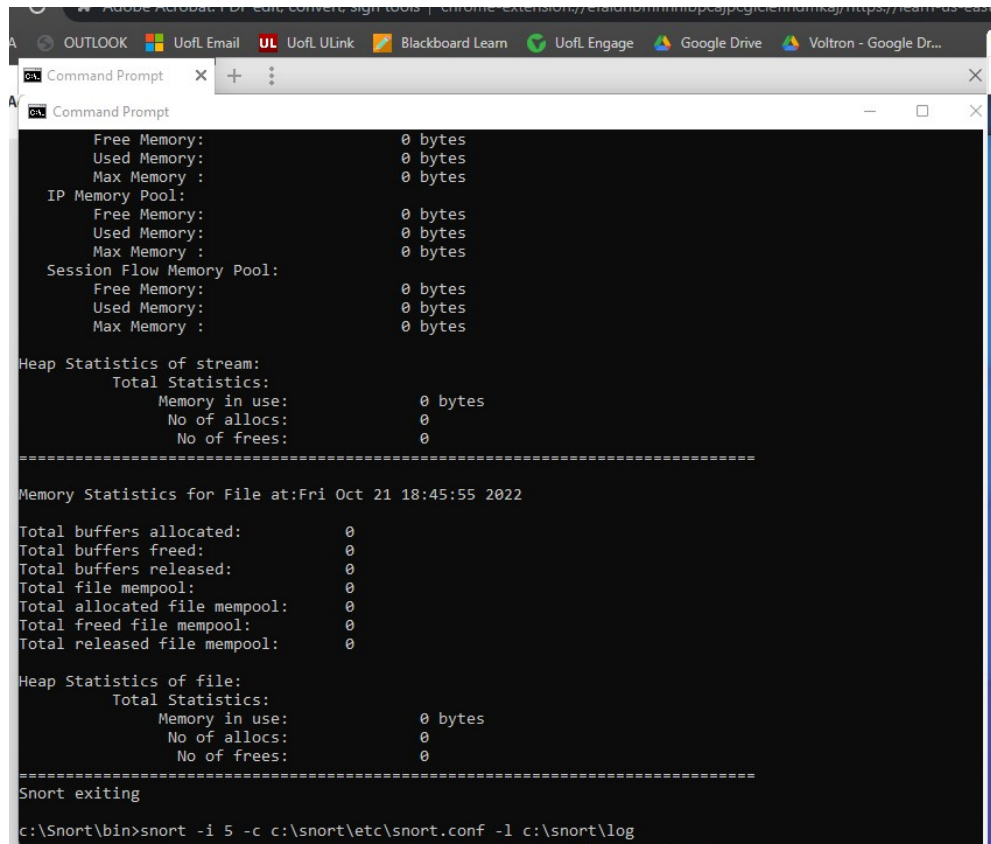
# Snort Lab

- This is a lab assignment, and worth 5 points.
- The due date is the same day midnight.

## 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.

\*\*\*\*I followed the directions of the video and attempted to do all the tasks in the snort tutorial. I have my snort rule below which uses Index 5 for my wireless LAN. I don't know if there is anything else that is needed for the lab so I took screenshots of my rule in the command prompt and a screenshot of the snort log with the ICMP messages.



```
Free Memory: 0 bytes
Used Memory: 0 bytes
Max Memory : 0 bytes
IP Memory Pool:
Free Memory: 0 bytes
Used Memory: 0 bytes
Max Memory : 0 bytes
Session Flow Memory Pool:
Free Memory: 0 bytes
Used Memory: 0 bytes
Max Memory : 0 bytes
Heap Statistics of stream:
Total Statistics:
Memory in use: 0 bytes
No of allocs: 0
No of frees: 0
=====
Memory Statistics for File at:Fri Oct 21 18:45:55 2022
Total buffers allocated: 0
Total buffers freed: 0
Total buffers released: 0
Total file mempool: 0
Total allocated file mempool: 0
Total freed file mempool: 0
Total released file mempool: 0
Heap Statistics of file:
Total Statistics:
Memory in use: 0 bytes
No of allocs: 0
No of frees: 0
=====
Snort exiting
c:\Snort\bin>snort -i 5 -c c:\snort\etc\snort.conf -l c:\snort\log
```

```
alertids - Notepad
File Edit View

[**] [1:1:0] Alert! ICMP [**]
[Priority: 0]
10/21-18:38:20.139557 fe80:0000:0000:0000:12d7:b0ff:fee8:8be2 -> 2603:6011:9e01:c3e2:08de:30e3:dfcf:3e30
IPv6-ICMP TTL:255 TOS:0x0 ID:0 Iplen:40 Dgmlen:72

[**] [1:1:0] Alert! ICMP [**]
[Priority: 0]
10/21-18:38:20.139592 2603:6011:9e01:c3e2:08de:30e3:dfcf:3e30 -> fe80:0000:0000:0000:12d7:b0ff:fee8:8be2
IPv6-ICMP TTL:255 TOS:0x0 ID:0 Iplen:40 Dgmlen:72

[**] [1:1:0] Alert! ICMP [**]
[Priority: 0]
10/21-18:38:23.700426 fe80:0000:0000:0000:61a1:496b:ca56:85b5 -> fe80:0000:0000:0000:12d7:b0ff:fee8:8be2
IPv6-ICMP TTL:255 TOS:0x0 ID:0 Iplen:40 Dgmlen:72

[**] [1:1:0] Alert! ICMP [**]
[Priority: 0]
10/21-18:38:23.701897 fe80:0000:0000:0000:12d7:b0ff:fee8:8be2 -> fe80:0000:0000:0000:61a1:496b:ca56:85b5
IPv6-ICMP TTL:255 TOS:0x0 ID:0 Iplen:40 Dgmlen:64

[**] [1:1:0] Alert! ICMP [**]
[Priority: 0]
10/21-18:38:28.709627 fe80:0000:0000:0000:12d7:b0ff:fee8:8be2 -> fe80:0000:0000:0000:61a1:496b:ca56:85b5
IPv6-ICMP TTL:255 TOS:0x0 ID:0 Iplen:40 Dgmlen:72

[**] [1:1:0] Alert! ICMP [**]
[Priority: 0]
10/21-18:38:28.709749 fe80:0000:0000:0000:61a1:496b:ca56:85b5 -> fe80:0000:0000:0000:12d7:b0ff:fee8:8be2
IPv6-ICMP TTL:255 TOS:0x0 ID:0 Iplen:40 Dgmlen:72

[**] [1:1:0] Alert! ICMP [**]
[Priority: 0]
10/21-18:38:41.691328 154.6.13.10 -> 192.168.1.203
ICMP TTL:53 TOS:0x0 ID:63486 Iplen:20 Dgmlen:60
Type:0 Code:0 ID:1 Seq:9571 ECHO REPLY

[**] [1:1:0] Alert! ICMP [**]
Ln 1, Col 1
100% Windows (CRLF) UTF-8
```