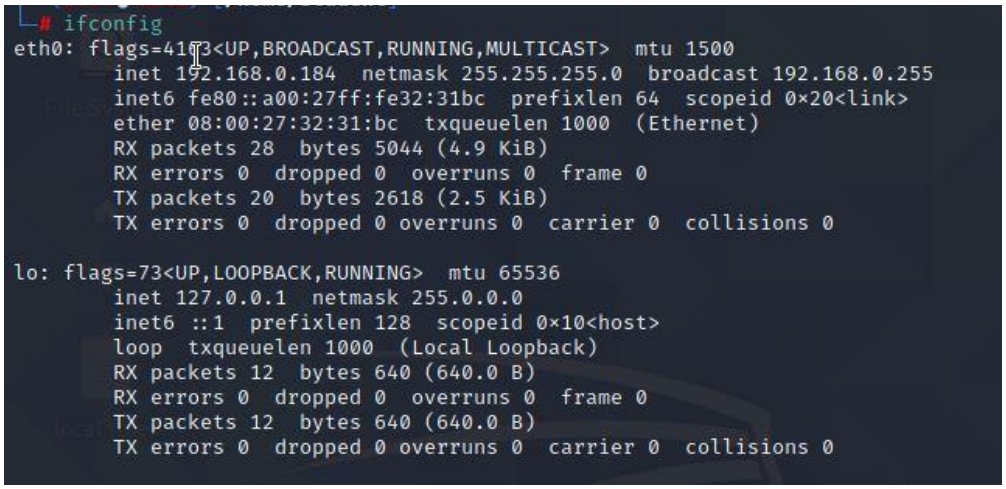
Xuan(James) Zhai

CS3339 Lab

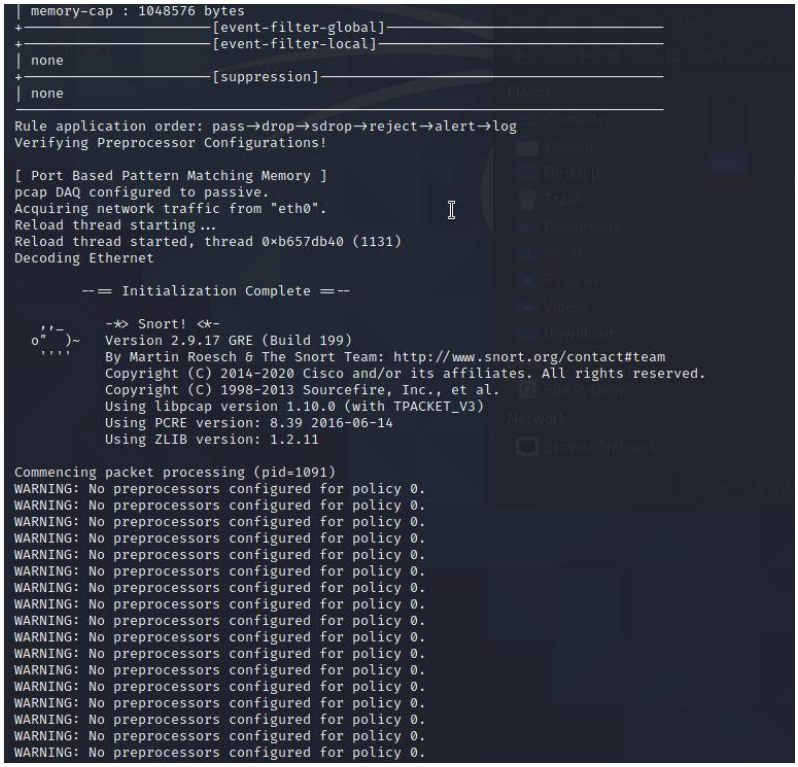
April 2nd, 2021

CS 3339 - Lab 6 - Lab Report

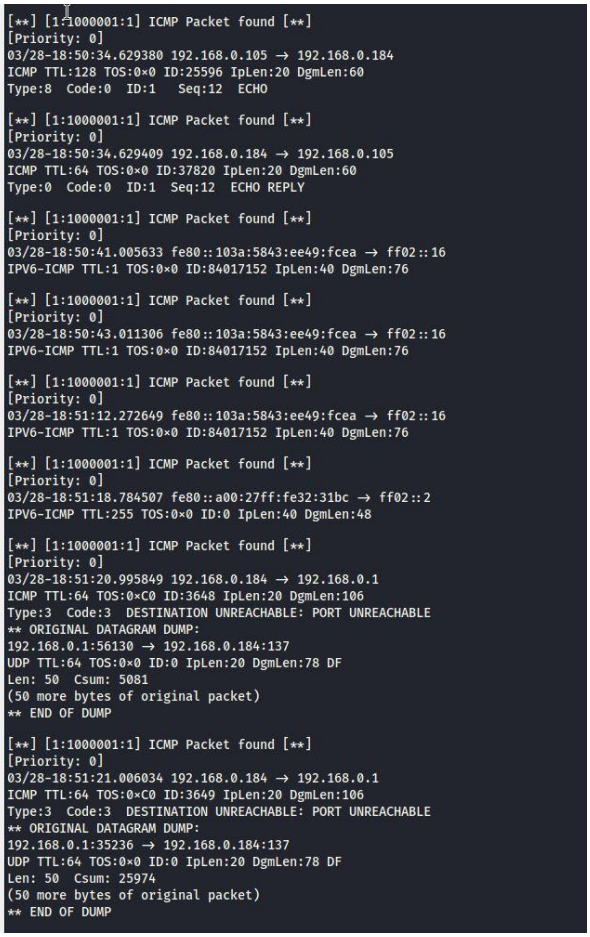
1: Use ifconfig to find the IP address.



2: Start snort.



3: Catch ICMP alert.



```
[**] [1:1000001:1] ICMP Packet found [**]
[Priority: 0]
03/28-18:50:34.629380 192.168.0.105 → 192.168.0.184
ICMP TTL:128 TOS:0×0 ID:25596 IpLen:20 DgmLen:60
Type:8  Code:0  ID:1   Seq:12  ECHO

[**] [1:1000001:1] ICMP Packet found [**]
[Priority: 0]
03/28-18:50:34.629409 192.168.0.184 → 192.168.0.105
ICMP TTL:64 TOS:0×0 ID:37820 IpLen:20 DgmLen:60
Type:0  Code:0  ID:1  Seq:12  ECHO REPLY

[**] [1:1000001:1] ICMP Packet found [**]
[Priority: 0]
03/28-18:50:41.005633 fe80::103a:5843:ee49:fcea → ff02::16
IPV6-ICMP TTL:1 TOS:0×0 ID:84017152 IpLen:40 DgmLen:76

[**] [1:1000001:1] ICMP Packet found [**]
[Priority: 0]
03/28-18:50:43.011306 fe80::103a:5843:ee49:fcea → ff02::16
IPV6-ICMP TTL:1 TOS:0×0 ID:84017152 IpLen:40 DgmLen:76

[**] [1:1000001:1] ICMP Packet found [**]
[Priority: 0]
03/28-18:51:12.272649 fe80::103a:5843:ee49:fcea → ff02::16
IPV6-ICMP TTL:1 TOS:0×0 ID:84017152 IpLen:40 DgmLen:76

[**] [1:1000001:1] ICMP Packet found [**]
[Priority: 0]
03/28-18:51:18.784507 fe80::a00:27ff:fe32:31bc → ff02::2
IPV6-ICMP TTL:255 TOS:0×0 ID:0 IpLen:40 DgmLen:48

[**] [1:1000001:1] ICMP Packet found [**]
[Priority: 0]
03/28-18:51:20.995849 192.168.0.184 → 192.168.0.1
ICMP TTL:64 TOS:0×C0 ID:3648 IpLen:20 DgmLen:106
Type:3  Code:3  DESTINATION UNREACHABLE: PORT UNREACHABLE
** ORIGINAL DATAGRAM DUMP:
192.168.0.1:56130 → 192.168.0.184:137
UDP TTL:64 TOS:0×0 ID:0 IpLen:20 DgmLen:78 DF
Len: 50  Csum: 5081
(50 more bytes of original packet)
** END OF DUMP

[**] [1:1000001:1] ICMP Packet found [**]
[Priority: 0]
03/28-18:51:21.006034 192.168.0.184 → 192.168.0.1
ICMP TTL:64 TOS:0×C0 ID:3649 IpLen:20 DgmLen:106
Type:3  Code:3  DESTINATION UNREACHABLE: PORT UNREACHABLE
** ORIGINAL DATAGRAM DUMP:
192.168.0.1:35236 → 192.168.0.184:137
UDP TTL:64 TOS:0×0 ID:0 IpLen:20 DgmLen:78 DF
Len: 50  Csum: 25974
(50 more bytes of original packet)
** END OF DUMP
```

4: What is a zero-day attack?

Zero-day attack is a type of attack which the hacker exploits the vulnerability before software developers can find a fix. It’s called zero-day because the hacker exploits the vulnerability usually in the same day that the vulnerability is exposed and the updated patch is published.

5: Can Snort catch zero-day network attacks? If not,why not? If yes, how?

Snort itself may be hard to find the zero-day network attacks if the security staff does not know the vulnerability; if the staff does not know where the vulnerability is, it would be hard to set a trigger and can catch the attack. However, to mitigate the issue at the beginning, the security staff can use ML or other artificial intelligence technique to predict the vulnerability attack and monitor the protocol packet transfer wisely.

6: Add a new rule.

1) alert tcp any any -> any any (msg:"TCP Packet found";sid:1000002; rev:1;)
2) Instead of catching the ICMP packet, I've changed the rule to let it capture the TCP packet transfer. Then, I test the rule by accessing www.facebook.com, www.twitter.com and several websites.
3) The log data becomes: