COMP232 Individual coursework

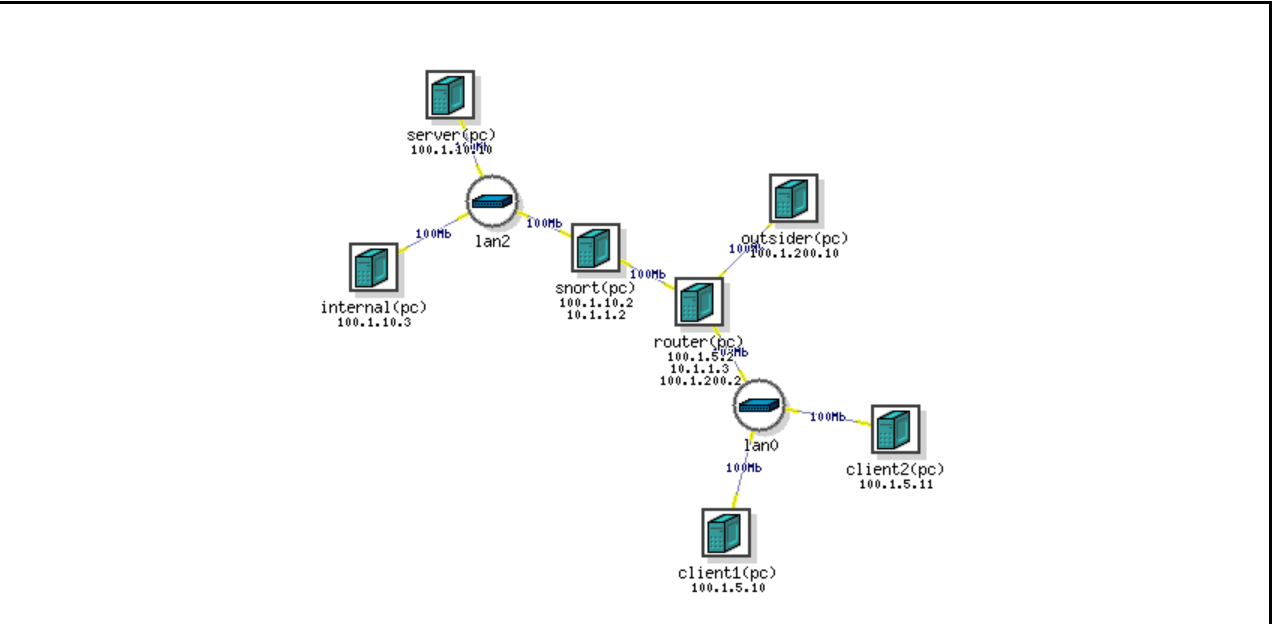
Assignment 3

Name: Yuyang.Wan

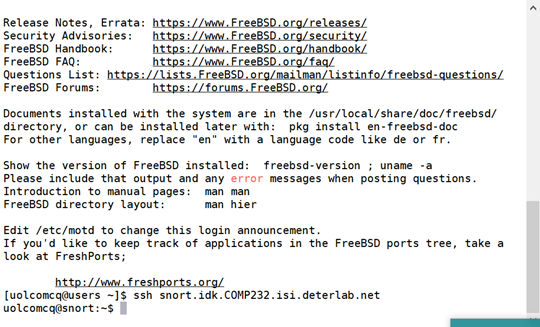
Student ID:20148429

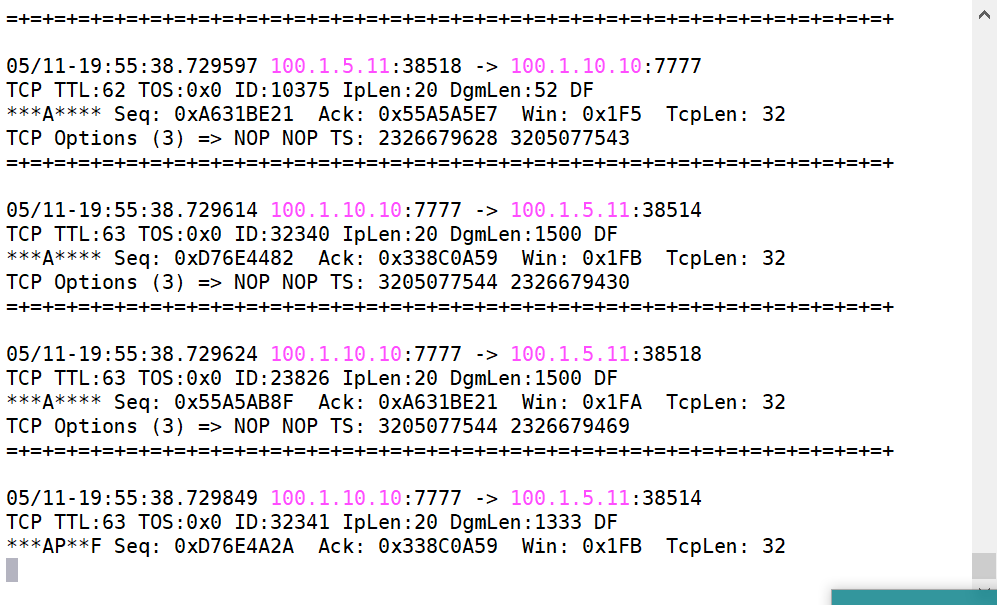
1. **Start Snort Without Rules**

Step 1 Finish set up of new experiment

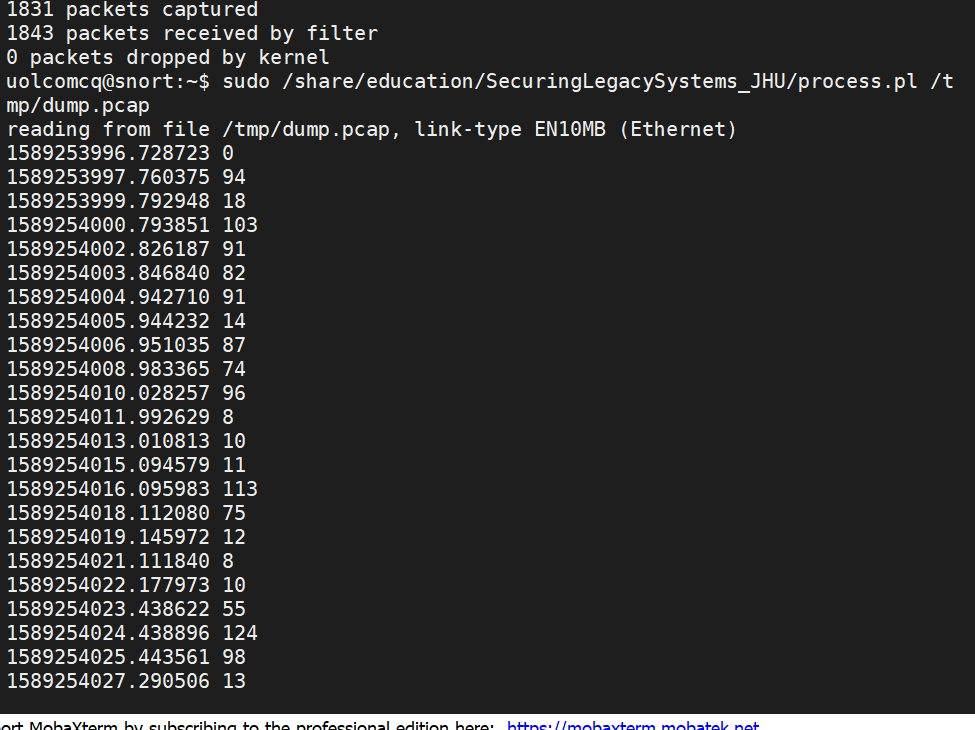


Step 2 Activate remote server Linux server and open an SSH client on your computer to connect to users.deterlab.net. Start snort.





Step 3 Run tcpdump to capture the data



Full data

1589253996.728723 0

1589253997.760375 94

1589253999.792948 18

1589254000.793851 103

1589254002.826187 91

1589254003.846840 82

1589254004.942710 91

1589254005.944232 14

1589254006.951035 87

1589254008.983365 74

1589254010.028257 96

1589254011.992629 8

1589254013.010813 10

1589254015.094579 11

1589254016.095983 113

1589254018.112080 75

1589254019.145972 12

1589254021.111840 8

1589254022.177973 10

1589254023.438622 55

1589254024.438896 124

1589254025.443561 98

1589254027.290506 13

1589254028.292415 14

1589254030.308750 6

1589254031.363143 99

1589254033.392982 91

1589254034.395913 99

1589254036.454933 5

1589254037.465602 14

1589254038.481757 6

1589254039.525910 2

1589254040.527091 113

1589254042.560141 74

1589254043.574817 15

1589254043.617514 6

**Questions:**

1. What happens to the traffic to client1 when Snort is not running?

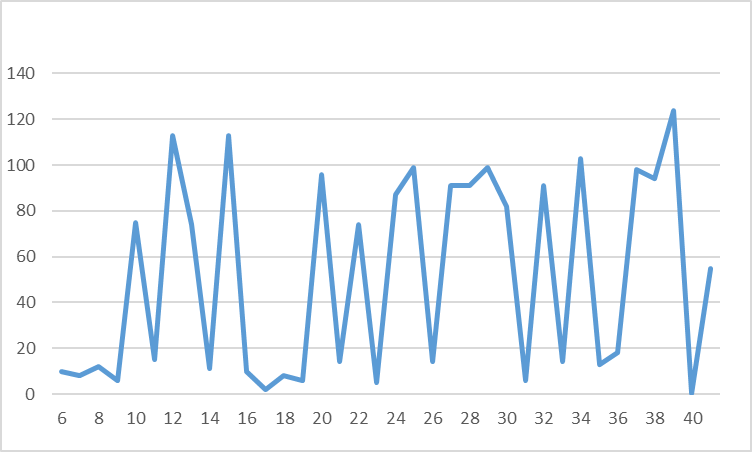
Traffic to client1 rises rapidly when snort is not running.

1. Is this a good thing?

No, it can block the access to client1. Technically this can be developed into dos attack.

1. Based on Snort's output what can you say about the application? What port does it connect to?

Snort can detect abnormal traffic to the client and restraints it. It is connected to the incoming port.

1. Please attach a graph of the traffic over time to your answers
2. What does the "-Q" option do in Snort?

-Q stand for Enable inline mode operation. In inline mode Snort creates a bridge between two network segments, and is responsible for passing traffic between the segments. It can inspect the traffic it passes, as well as drop suspicious traffic.

1. What does the "--daq nfq" option do in Snort?

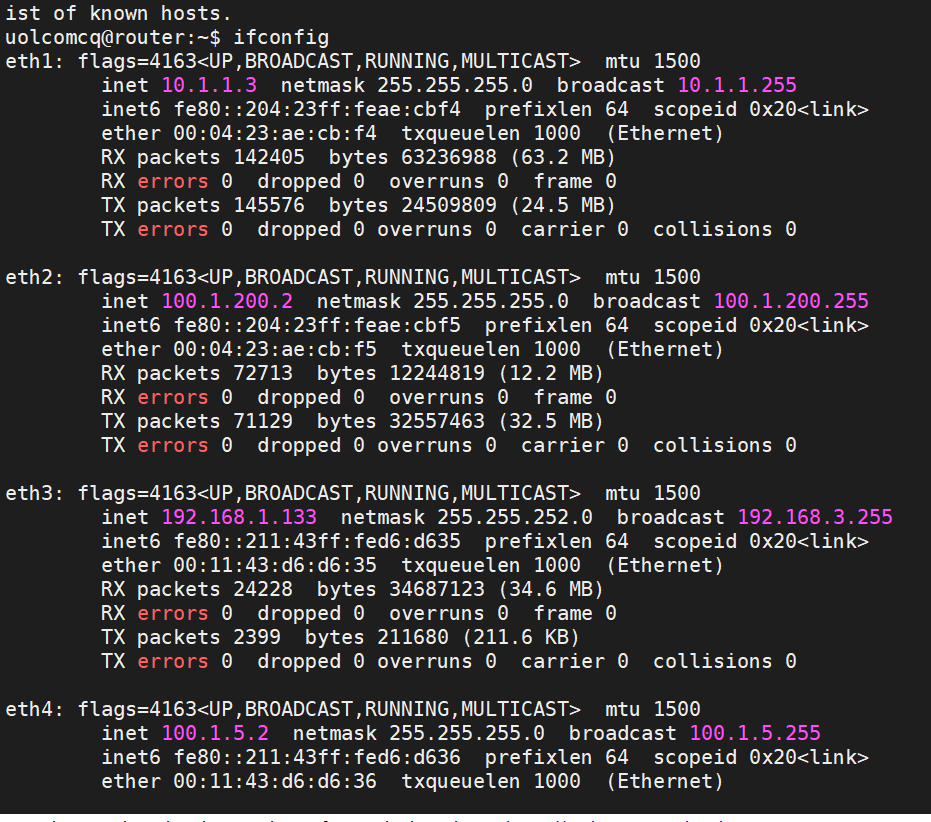
--daq nfq means inline on Linux using netfilter. It provides three main functionalities including Packet filtering to Accepts or drops packets, NAT to Changes the source or destination IP address of network packets, Packet Mangling to Modifies packets for Quality of Service.

1. **Analyze Network Traffic**

Step1 Connect to router



Step2 Capture the data



**Questions:**

1. The request that the client sends the server is broken into four parts. What are these parts and what order does they appear in? How are these parts seperated in the request?
2. Is this is a secure way for the client to send requests to the server? Explain your answer.

I think it is a save way for client to send requests to server.

1. Can you recover one of the files sent by the server to a client? If so attach the file, a pcap the relevant packets and indicate which client this was sent to.