

Lab 4: Generating, Capturing and Analyzing Network Scanner Traffic.

2.1 Starting a new instance of Zeek.

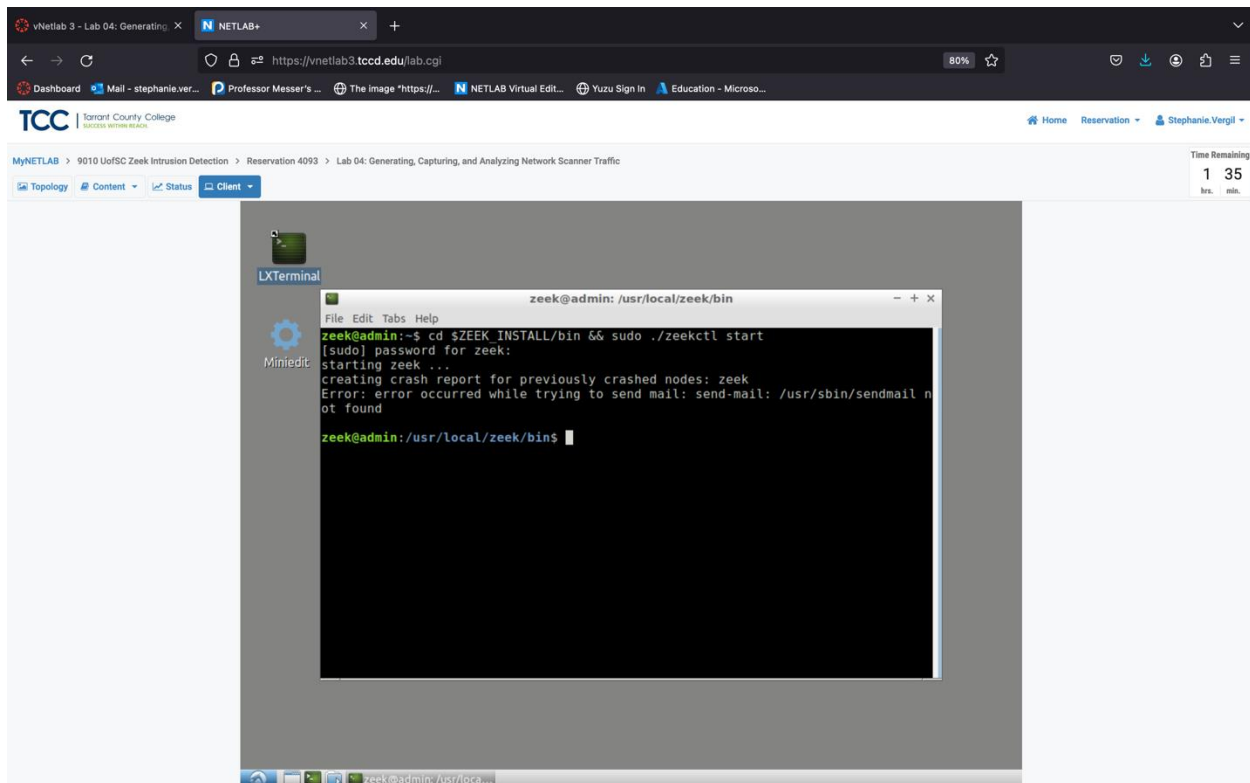
Step 1. Click on the client button to enter the client machine.

Step 2. Located in the desktop double click on the LXTerminal.

Step 3. To start Zeek enter the following command on the terminal:

```
cd $ZEEK_INSTALL/bin && sudo ./zeekctl start
```

The command enters Zeek's default installation directory and zeekctl tool to start a new instance. A new instance of zeek is now active.



2.2 Launching Mininet.

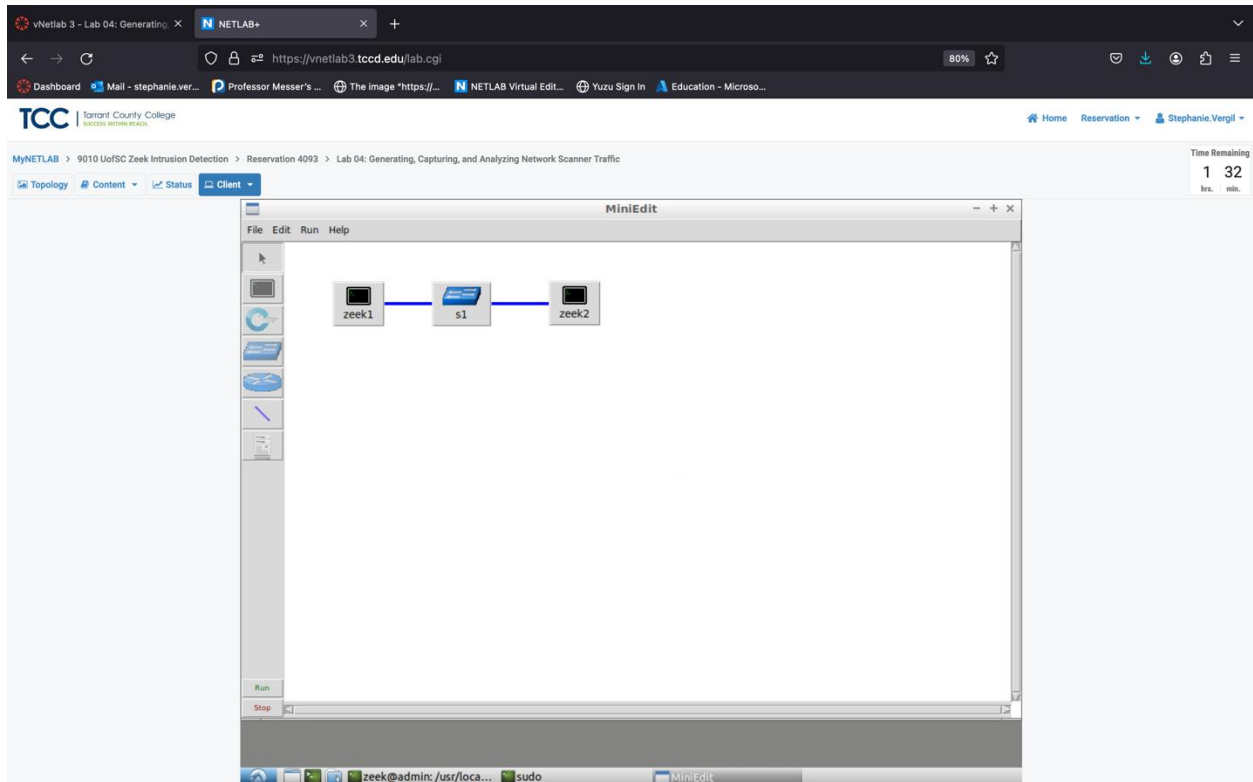
Stephanie Vergil

Step 1. Located on the client's desktop, double click on MiniEdit. When prompt enter the password and click enter to continue.

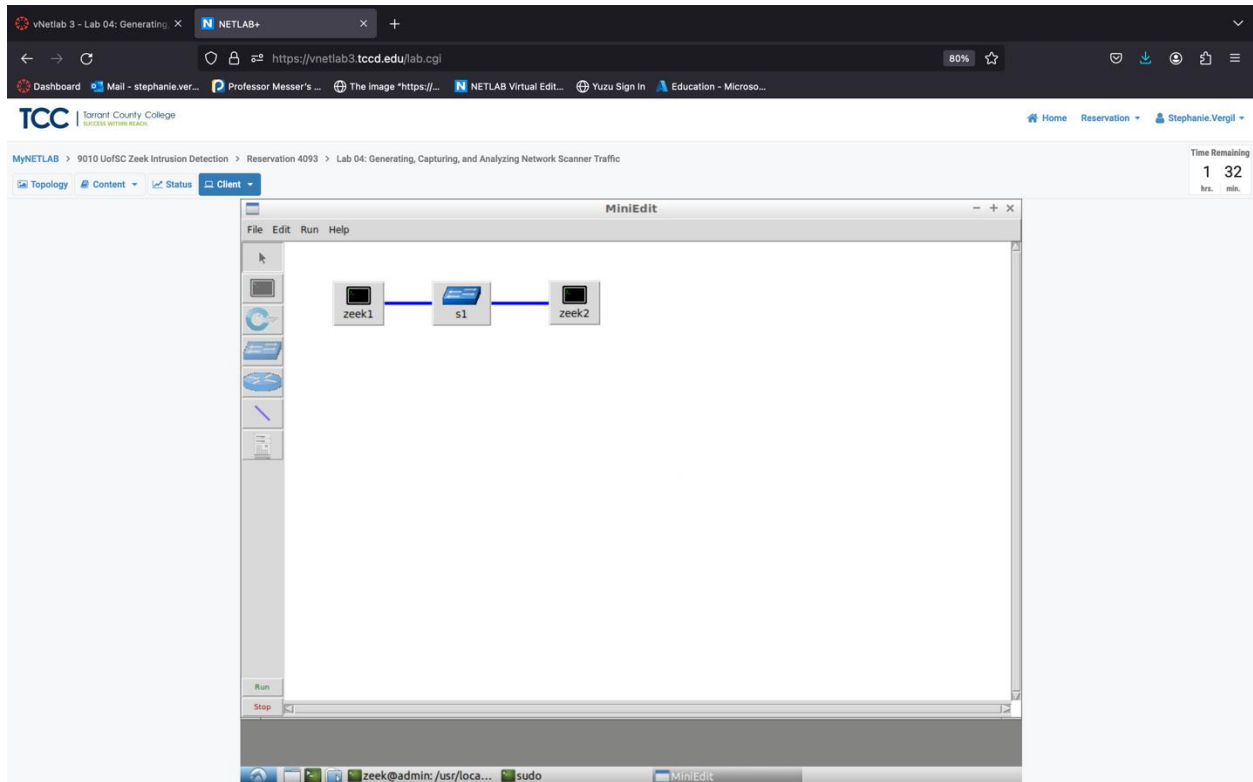
Step 2. Once the MiniEdit editor launches, load the correct topology by clicking the file tab and click on open.

Step 3. Navigate to the Zeek-Topologies directory by selecting the Zeek-Topologies and clicking on the open button.

Step 4. Select the Topology.mn file by double clicking.



Step 5. To begin running the virtual machines, click on the run button.

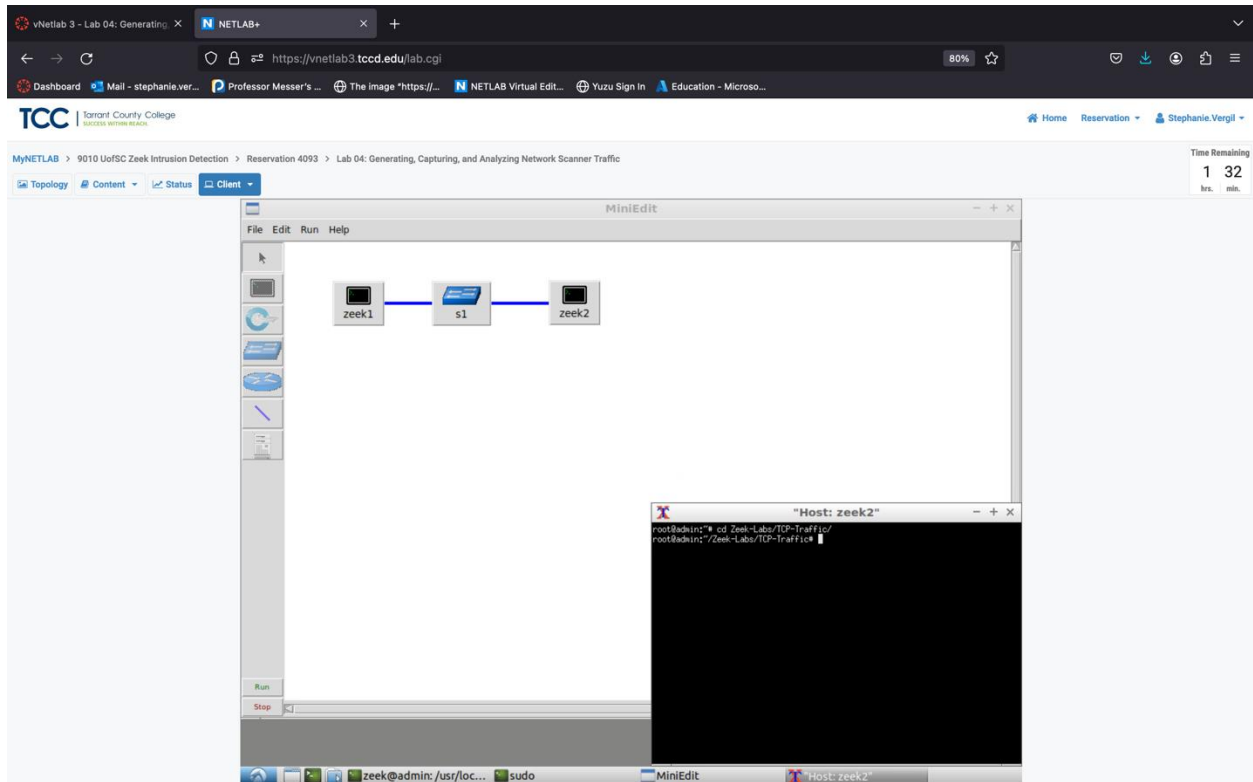


2.3 Setting up the zeek2 virtual machine for live network capture

Step 1. To Launch the zeek2 terminal hold the right mouse button on the zeek2 machine and click on the terminal button.

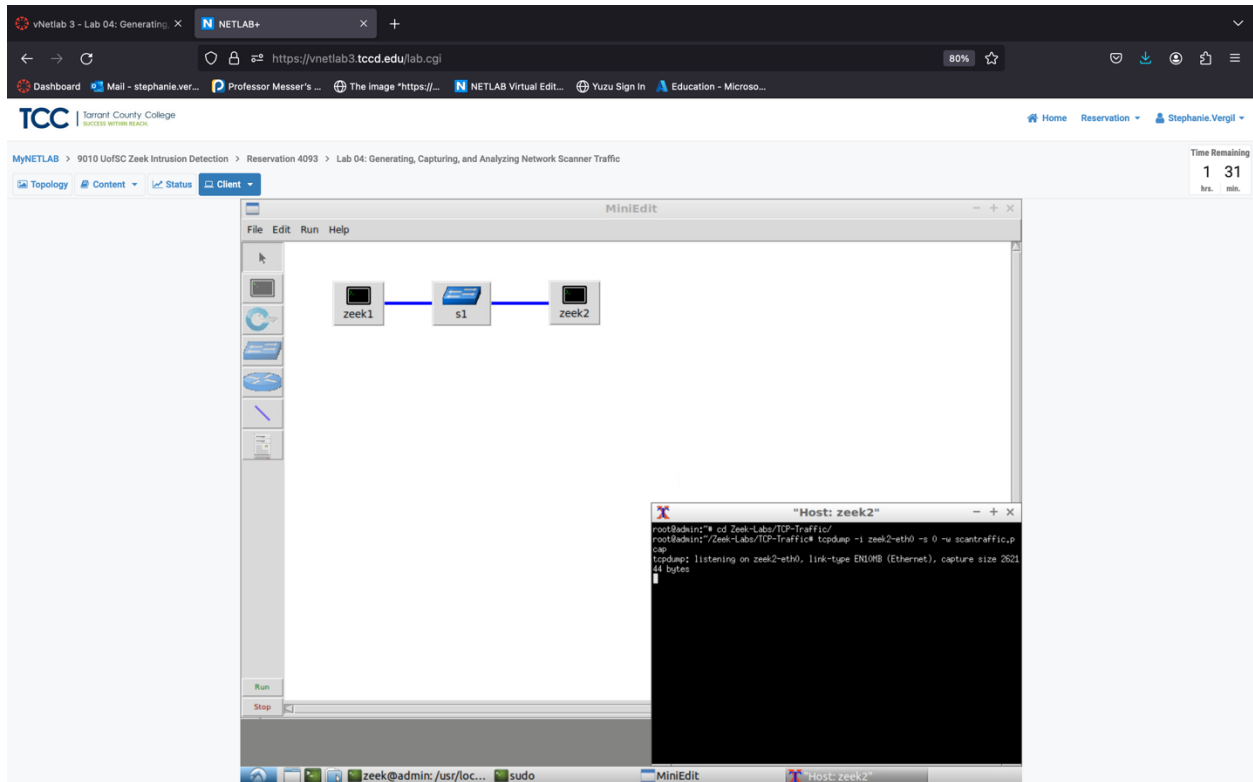
Step 2. From the zeek2 terminal enter the following command to navigate to the TCP-Traffic directory:

```
cd Zeek-Labs/TCP-Traffic/
```



Step 3. Enter the following command to start live packet capture on interface zeek2-eth0 and save the output to a file named scantraffic.pcap :

```
tcpdump -i zeek2-eth0 -s 0 -w scantraffic.pcap
```



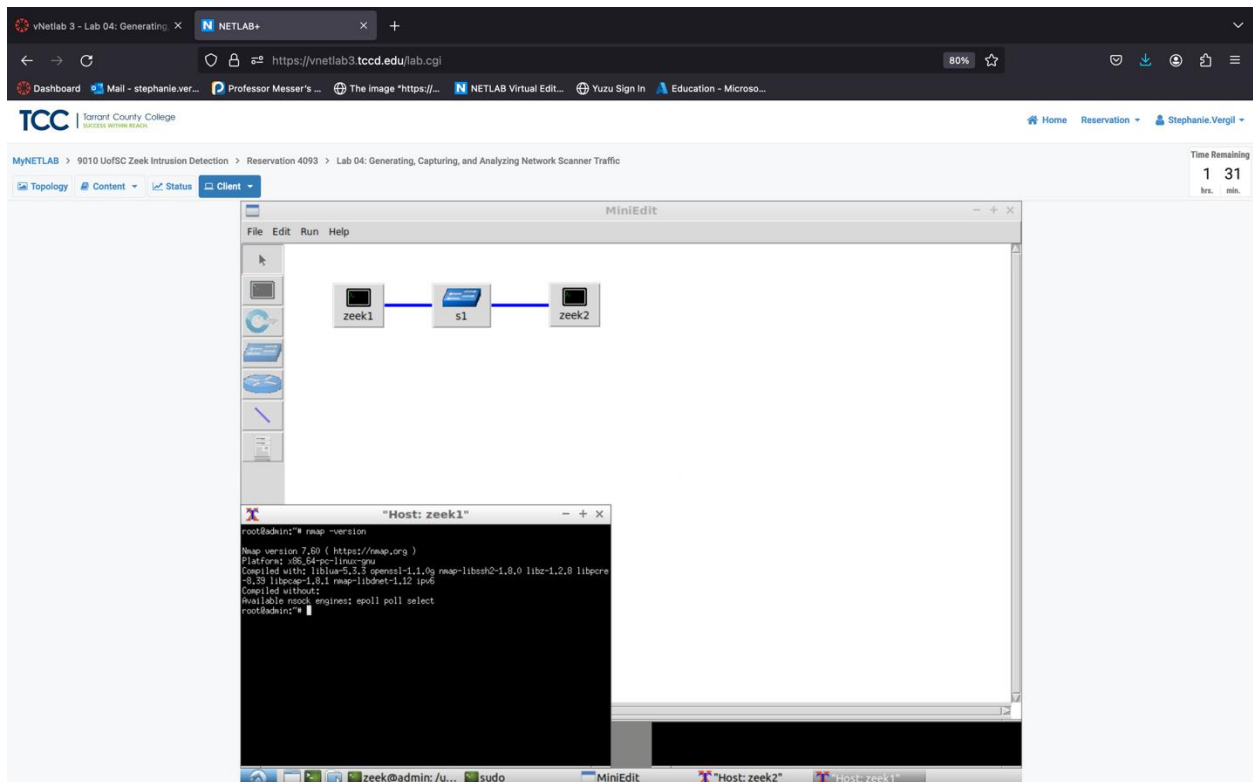
Now the zeek2 virtual machine is now ready to begin collecting live network traffic.

2.4 Using the zeek1 virtual machine for network scanning activities.

Step 1. Open the zeek1 terminal by right holding and selecting terminal.

Step 2. To verify that nmap is functioning properly by viewing the current installed version, enter the following command:

nmap -version



The screenshot shows that the currently installed version of nmap is 7.60.

2.4.2 TCP SYN scans.

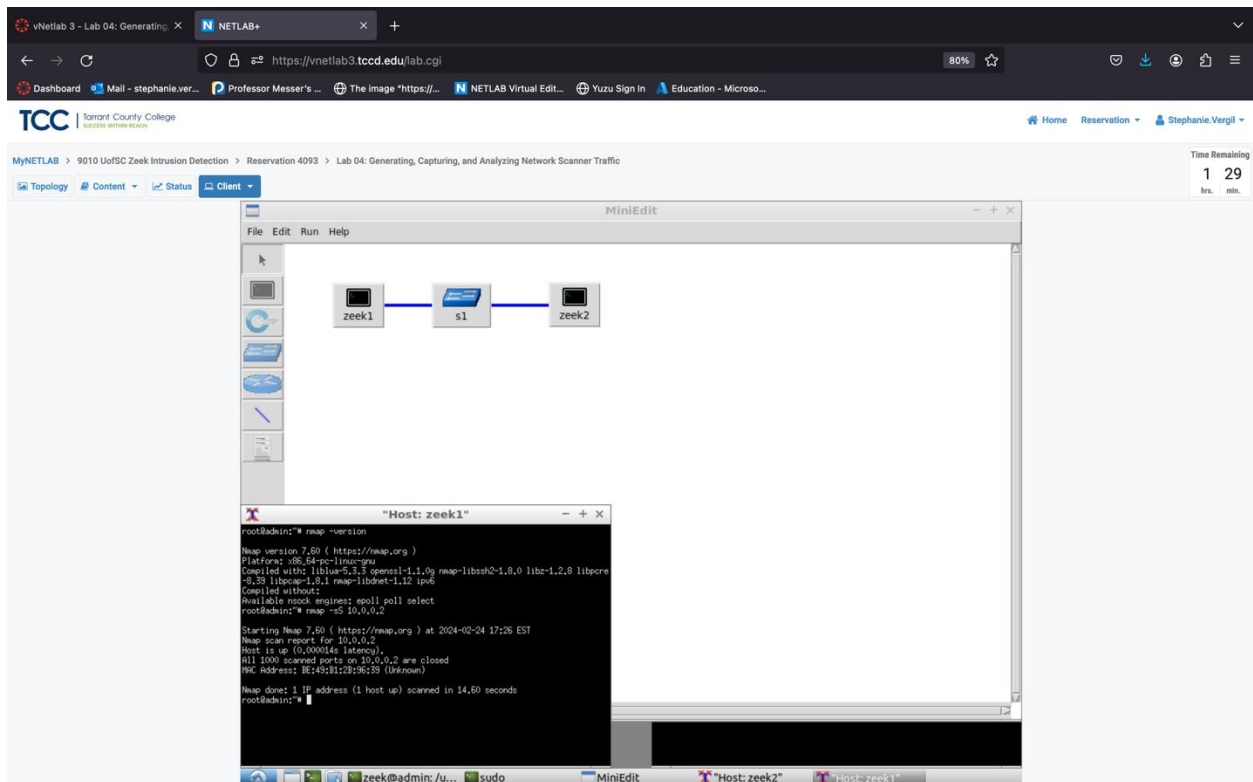
TCP SYN scans are frequently used to find vulnerabilities. In this type of scan, the scanning computer sends a special kind of request, called a SYN packet, to the target. When the target receives this request, it thinks a new connection is being requested and responds with a SYN/ACK packet if the port is open. The scanning computer can then confirm that the port is open and terminate the connection using a reset packet.

Step 1. Using the following command to conduct a TCP SYN scan.

```
nmap -sS 10.0.0.2
```

the -sS option is used to indicate a TCP SYN scan.

Once the scan finishes, nmap generates a report detailing various aspects such as when the scan began, the number of ports scanned, the overall duration, and more. In this case, the TCP SYN scan took 14.60 seconds to complete, and none of the scanned ports were found to be open.



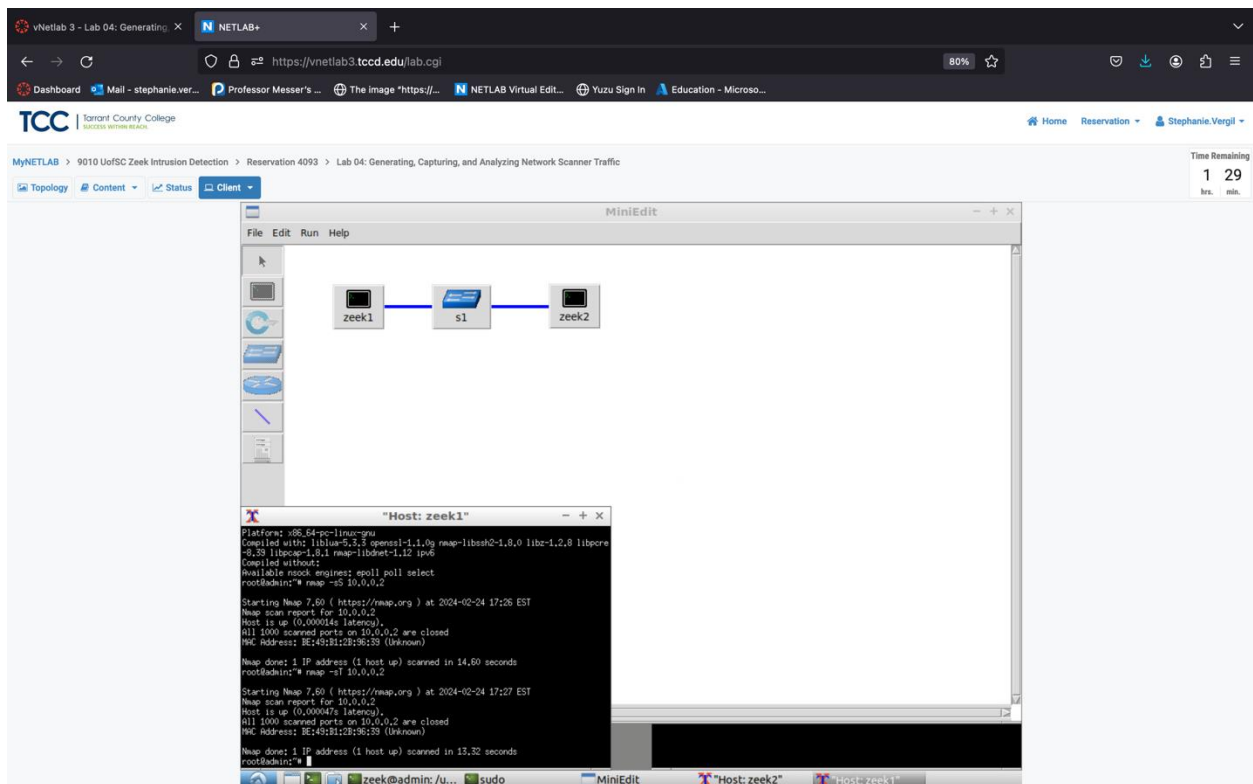
2.4.3 TCP connect scans.

TCP Connect scans offer another method compared to TCP SYN scans. Instead of initiating a TCP handshake, the scanning system tries to directly establish a connection with the target. If the connection is successful, it indicates that the port is open.

Step 1. Enter the following command to conduct a TCP connect scan:

```
nmap -sT 10.0.0.2
```

The -sT option is used to indicate a TCP connect scan.



The report in the above figure shows that the scan was completed in 13.32 seconds and none of the scanned ports were open.

2.4.4 TCP NULL scans.

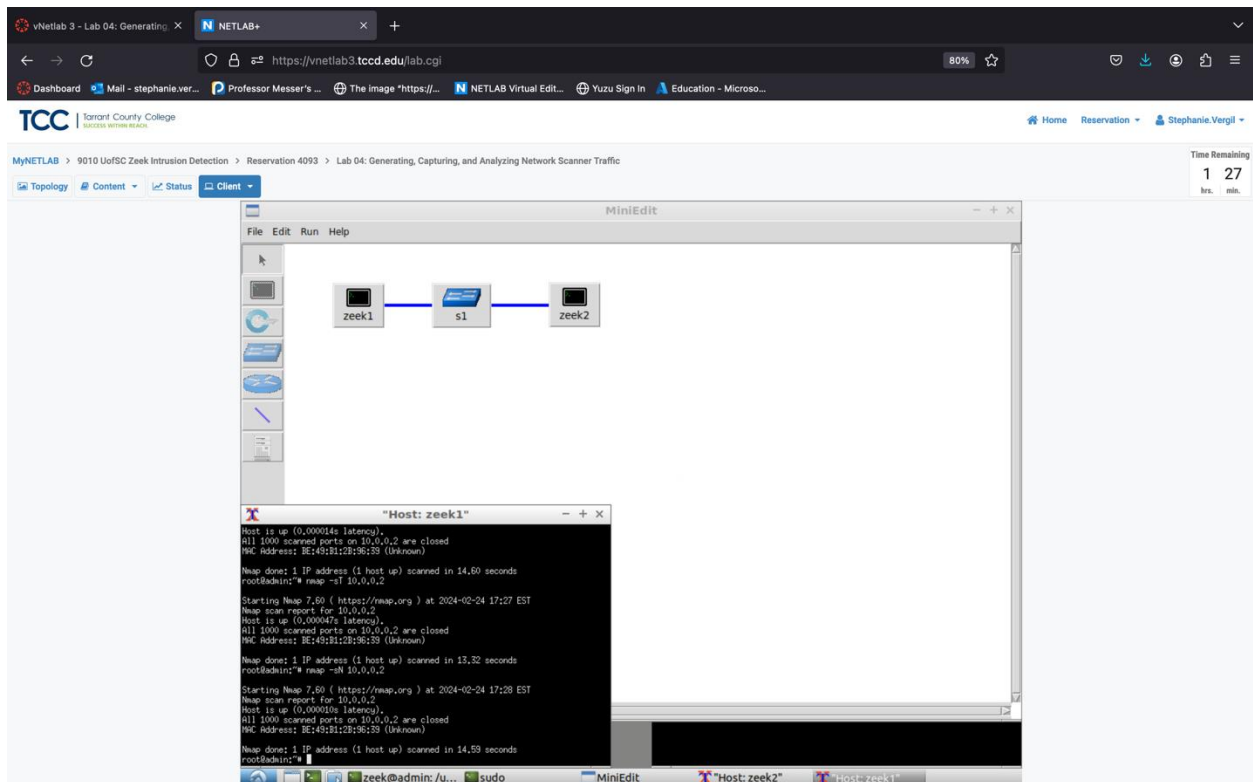
TCP NULL scans are a type of TCP (Transmission Control Protocol) scanning method. Normally, TCP packets contain flags that firewalls may use to filter traffic. TCP NULL scans try to avoid detection by sending packets without any flags in their headers. By setting the sequence number to 0, these packets can slip through firewalls undetected.

Step 1. Enter the following command to conduct a TCP NULL scan:

```
nmap -sN 10.0.0.2
```

The -sN option is used to indicate a TCP NULL scan.

The report in the below figure shows that the scan was completed in 14.59 seconds



2.4.5 TCP XMAS scans.

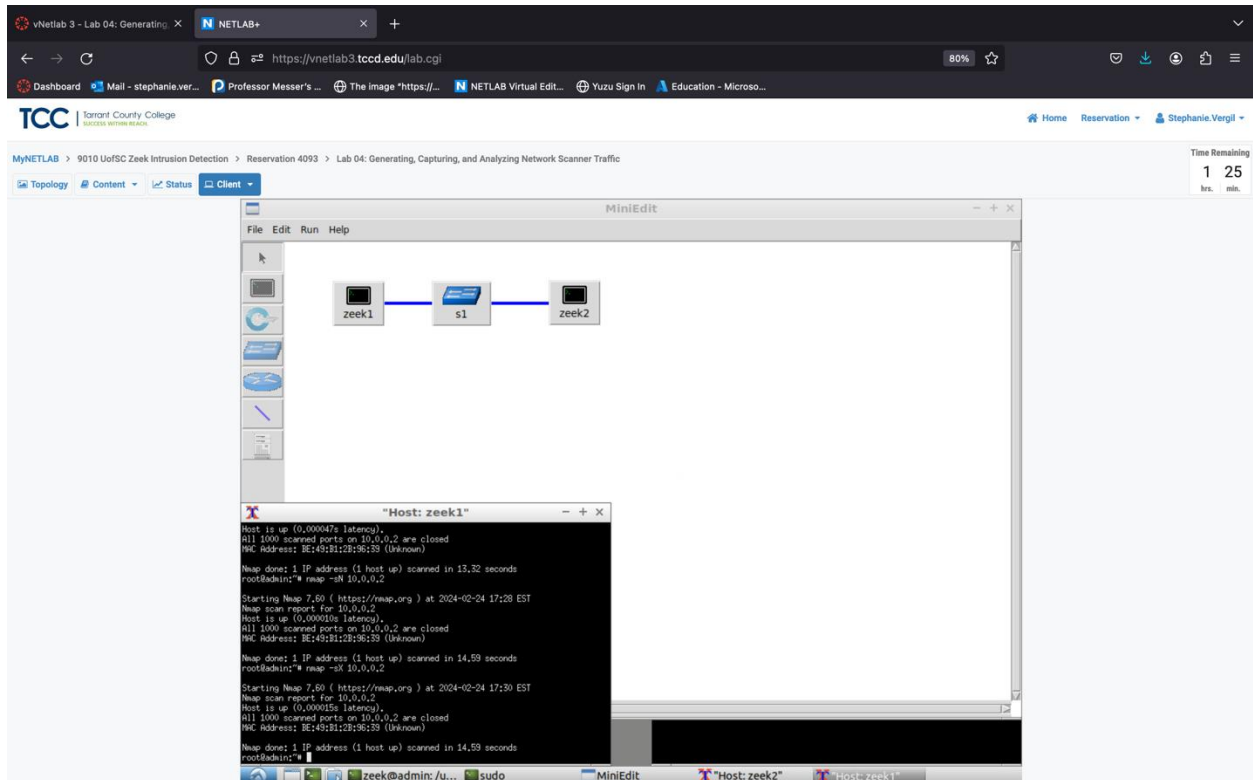
TCP Xmas scans, or Christmas tree scans, are a type of port scanning technique used to probe target systems for open ports. The name "Christmas tree scan" comes from the way the TCP packet's flags light up like a Christmas tree due to the combination of flags set in the TCP header. In a TCP Xmas scan, the scanning tool sets the PSH (Push), URG (Urgent), and FIN (Finish) flags in the TCP header of the packet sent to the target port. This combination of flags is unusual and not typically seen in normal network traffic. By sending packets with these flags set, the scanner aims to probe the target system's response to these non-standard packets.

Step 1. Enter the following command to conduct a TCP XMAS scan:

```
nmap -sX 10.0.0.2
```

The -sX option is used to indicate a TCP XMAS scan.

On the below figure it shows that the scan was completed in 14.59 seconds and none of the scanned ports were opened or vulnerable.



2.4.6 Terminating live network capture.

Step 1. Open the zeek2 terminal.

Step 2. Press the ctrl+c key combination to stop the live traffic capture. The statistics of the capture session will display. In my case 8030 packets were recorded by the interface, which were then captured and stored in the new scantraffic.pcap file.

Stephanie Vergil

vNetlab 3 - Lab 04: Generating > NETLAB+ > +

Dashboard Mail - stephanie.ver... Professor Messer's... The Image "https://... NETLAB Virtual Edit... Yuzu Sign In Education - Microso...

TCC | Toronto County College

MyNETLAB > 9010 UofSC Zeek Intrusion Detection > Reservation 4093 > Lab 04: Generating, Capturing, and Analyzing Network Scanner Traffic

Time Remaining 1 hrs. 25 min.

Topology Content Status Client

MiniEdit

File Edit Run Help

zeek1 s1 zeek2

"Host: zeek1"

```
Host is up (0.00047s latency).
All 1000 scanned ports on 10.0.0.2 are closed
MAC Address: BE:49:81:23:96:39 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 13.32 seconds
root@admin:~# nmap -sT 10.0.0.2

Starting Nmap 7.60 ( https://nmap.org ) at 2024-02-24 17:28 EST
Nmap scan report for 10.0.0.2
Host is up (0.000010s latency).
All 1000 scanned ports on 10.0.0.2 are closed
MAC Address: BE:49:81:23:96:39 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 14.59 seconds
root@admin:~# nmap -sX 10.0.0.2

Starting Nmap 7.60 ( https://nmap.org ) at 2024-02-24 17:30 EST
Nmap scan report for 10.0.0.2
Host is up (0.000055s latency).
All 1000 scanned ports on 10.0.0.2 are closed
MAC Address: BE:49:81:23:96:39 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 14.59 seconds
root@admin:~#
```

"Host: zeek2"

```
root@admin:~# cd /zeek-labs/zeek-traffic/
root@admin:~# cd /zeek-labs/zeek-traffic/
root@admin:~# tcpdump -i zeek2-eth0 -s 0 -w scantraffic.pcap
tcpdump: listening on zeek2-eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
12030 packets captured
0/30 packets received by filter
0 packets dropped by kernel
root@admin:~#
```

zeek@admin: /u... sudo MiniEdit Host: zeek2 Host: zeek1

Step 3. Stop the current Mininet session by clicking 'STOP'.

vNetlab 3 - Lab 04: Generating > NETLAB+ > +

Dashboard Mail - stephanie.ver... Professor Messer's... The Image "https://... NETLAB Virtual Edit... Yuzu Sign In Education - Microso...

TCC | Toronto County College

MyNETLAB > 9010 UofSC Zeek Intrusion Detection > Reservation 4093 > Lab 04: Generating, Capturing, and Analyzing Network Scanner Traffic

Time Remaining 1 hrs. 25 min.

Topology Content Status Client

MiniEdit

File Edit Run Help

zeek1 s1 zeek2

Run

Stop

zeek@admin: /usr/loca... sudo MiniEdit

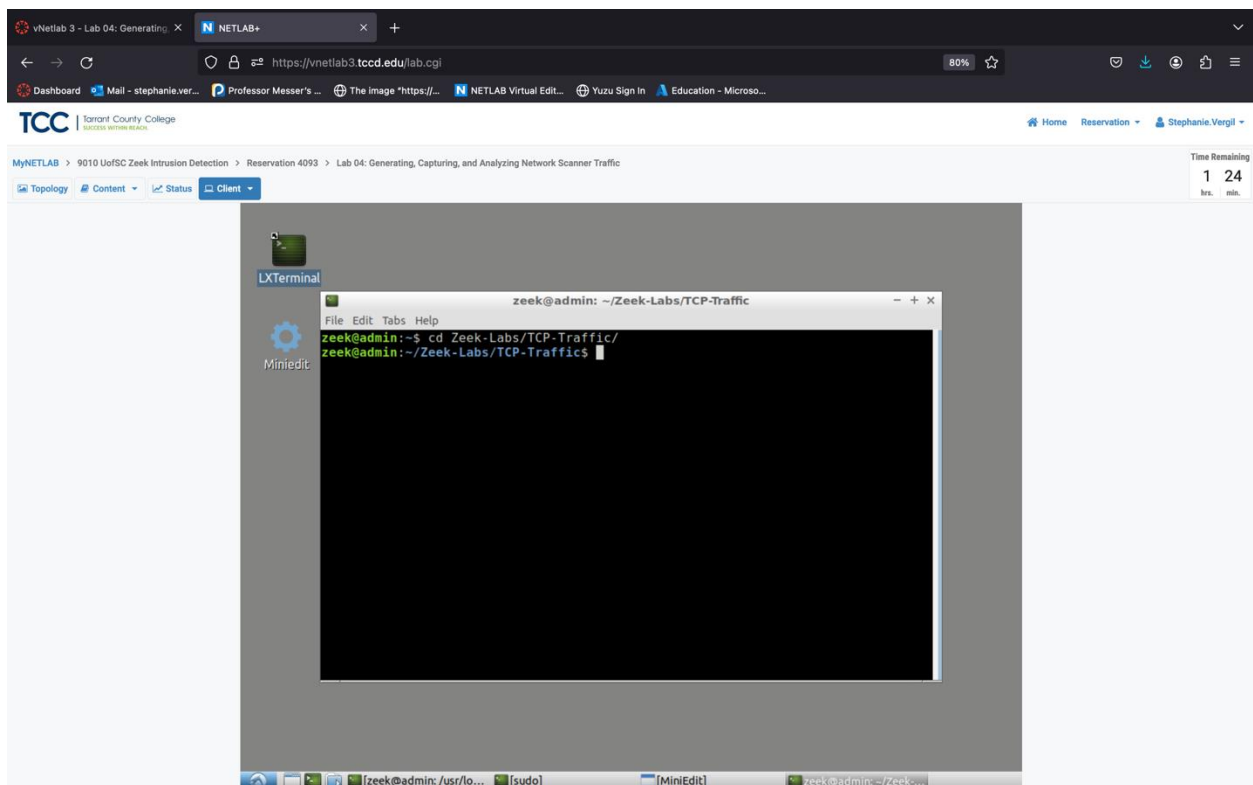
3 Analyzing collected network traffic.

After completing several TCP-based scans, we now have the network traffic stored in the scanpackets.pcap file. In this part, we'll examine the captured network data using Zeek.

Step 1. Launch the LXTerminal

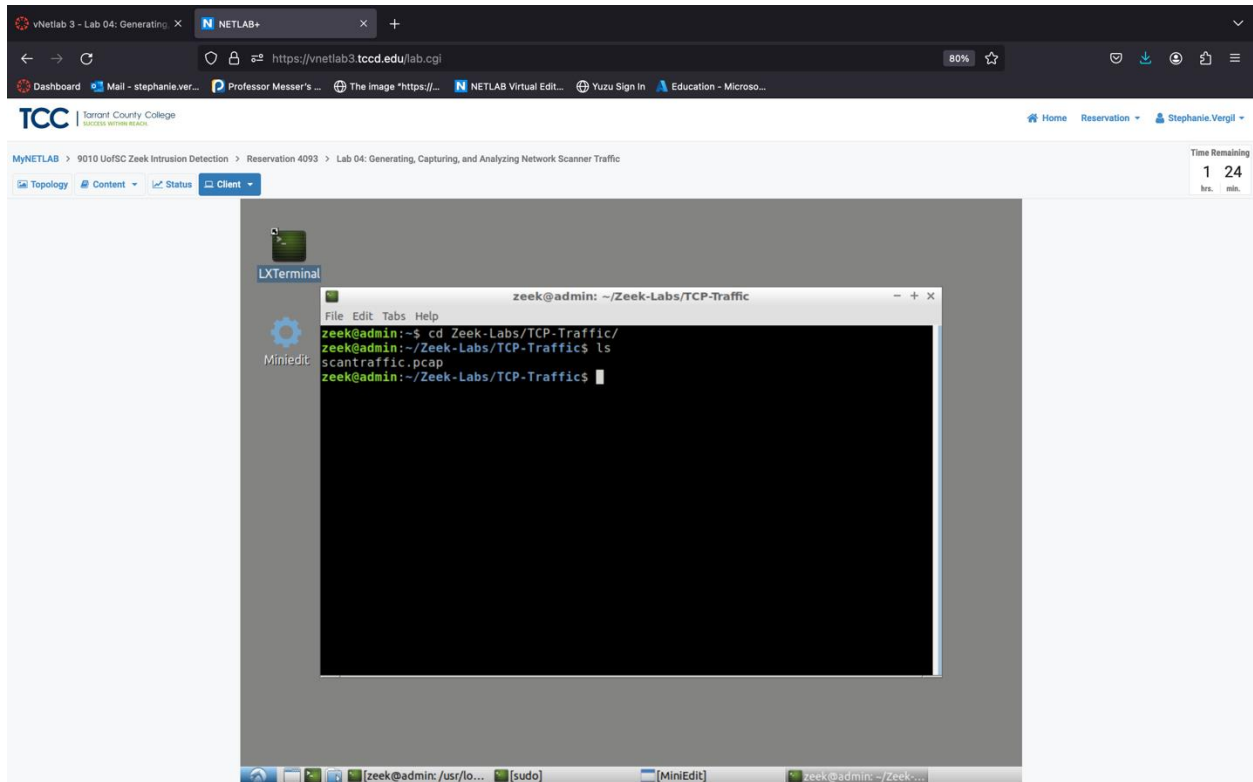
Step 2. Enter the following command to navigate to the TCP-Traffic directory to find the scantraffic.pcap file:

```
cd Zeek-Labs/TCP-Traffic/
```



Step 3. To view the file contents of the TCP-Traffic directory to make sure that the scantraffic.pcap file was successfully saved enter the following command:

```
ls
```



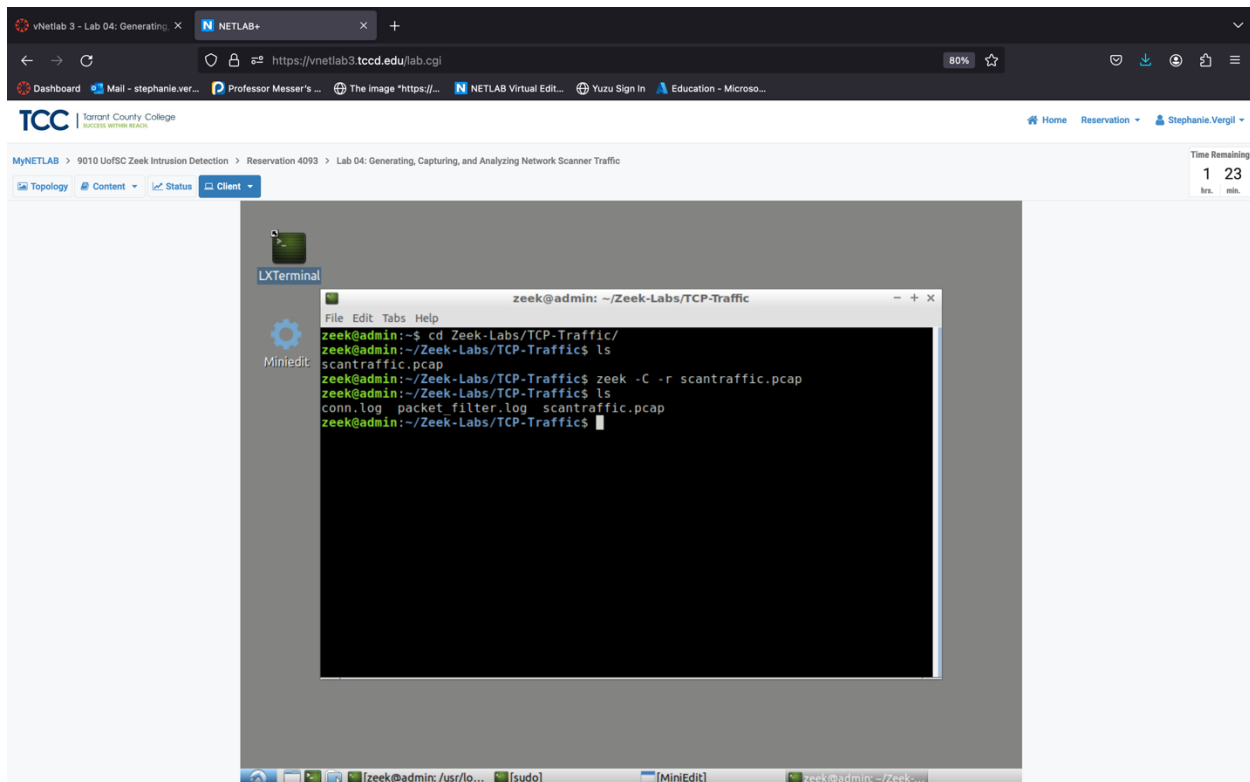
Step 4. Enter the following zeek command to process the packet capture file.

```
zeek -C -r scantraffic.pcap
```

Step 5. To list the generated Zeek log files enter the following command:

```
ls
```

Zeek will process the scantraffic.pcap file and generate resulting log files based off of the default Zeek configurations.



Now that the log files generated, we can now use the zeek-cut utility for further analysis.

3.1 Example Query 1

Example 1: Show the source IP addresses that generated the most traffic organized in descending order.

Step 1. Enter the following command:

```
zeek-cut id.orig_h < conn.log | sort | uniq -c | sort -rn | head -n 10
```

The command breakdown is as follows:

`zeek-cut id.orig_h < conn.log`: This selects the `id.orig_h` column from the `conn.log` file using the `zeek-cut` tool.

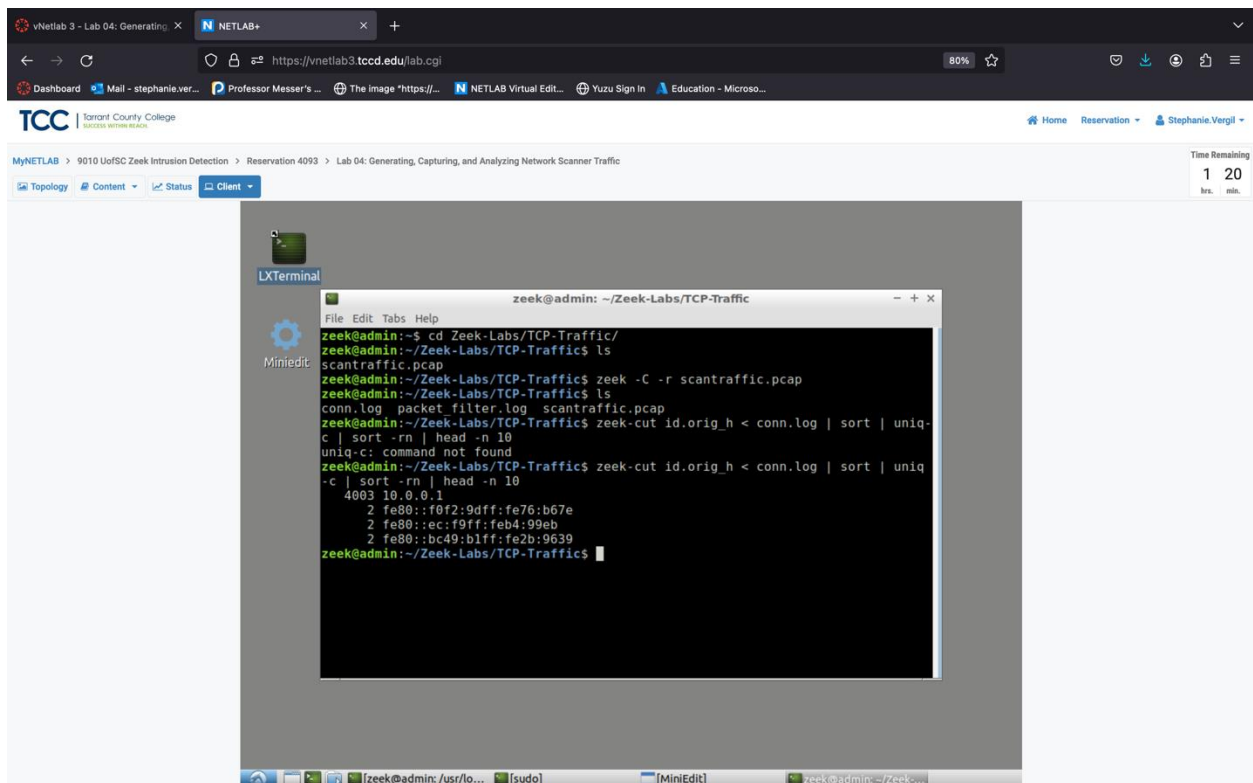
`| sort`: It sorts the rows in alphabetical order.

`| uniq -c`: This removes duplicate rows while displaying unique instances and their counts.

`| sort -rn`: It sorts the rows in reverse numerical order.

| head -n 10: Finally, it displays the top 10 values using the head command.

In conclusion this command extracts a specific column from a log file, sorts the data alphabetically, removes duplicates while counting occurrences, sorts the unique instances by count in descending order, and displays the top 10 results.



On the above image we can see that majority of the packets were received from zeek1 machine denoted by the Ip address 10.0.0.1

3.2 Example Query 2

Example 2: Show the 10 destination ports that received the most network traffic, organized in descending order.

Step 1. Enter the following command.

```
zeek-cut id.resp_p < conn.log | sort | uniq -c | sort -rn | head -n 10
```

This command breakdown is as follows:

zeek-cut id.orig_h < conn.log: Selects the id.orig_h column from the conn.log file.

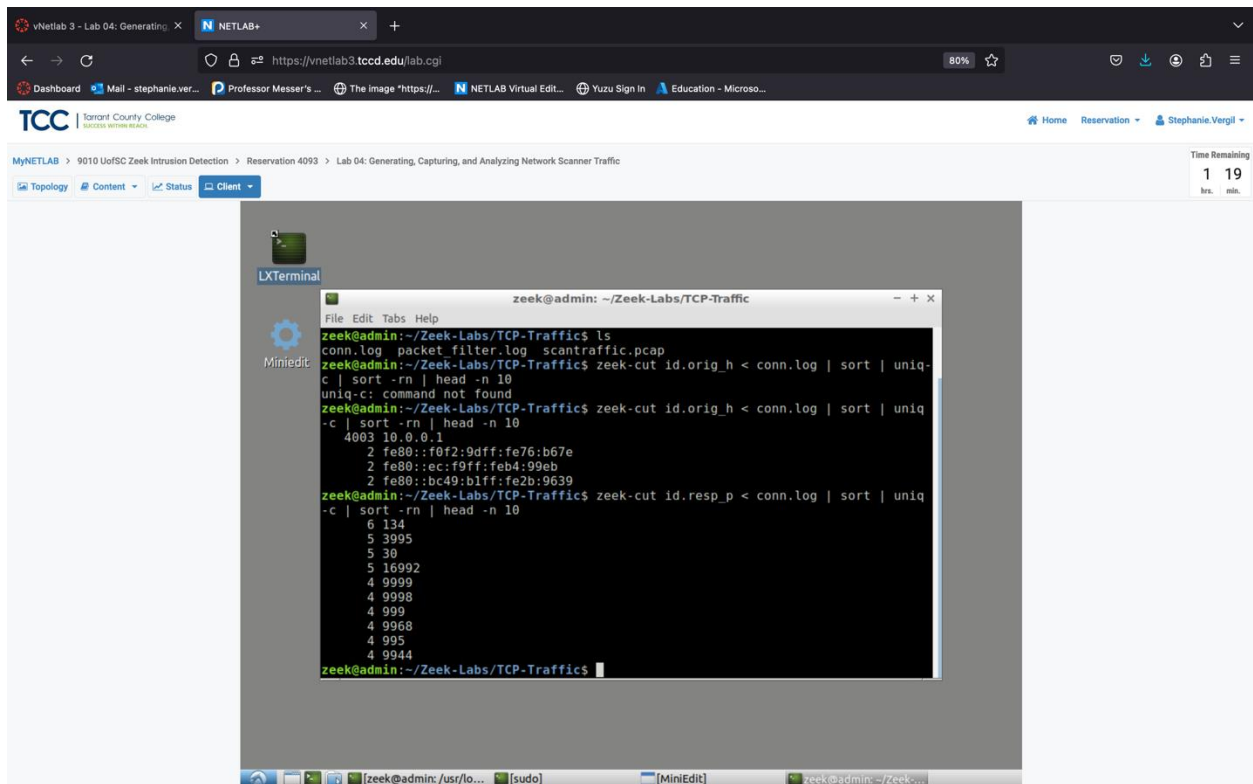
| sort: Arranges the rows in alphabetical order.

| uniq -c: Removes duplicate rows while showing unique instances and their counts.

| sort -rn: Sorts the rows in reverse numerical order.

| head -n 10: Displays the top 10 values using the head command.

In summary, this command sequence extracts the originating IP addresses from a connection log file, sorts them alphabetically, counts how many times each IP address appears, sorts them by count in descending order, and then displays the top 10 IP addresses with the highest counts. The left column shows the count of duplicate entries, while the corresponding destination ports are displayed in the right column. Since there were more than 10 unique destination ports found, only the top 10 are shown. It's important to note that the specific destination ports observed can vary depending on the scanning configurations used by nmap.



The screenshot shows a virtual machine environment with a web browser at the top displaying the TCC (Toront County College) MyNETLAB page. Below the browser, a terminal window titled 'zeek@admin: ~/Zeek-Labs/TCP-Traffic' is open. The terminal shows the following commands and output:

```
zeek@admin:~/Zeek-Labs/TCP-Traffic$ ls
conn.log packet_filter.log scantraffic.pcap
zeek@admin:~/Zeek-Labs/TCP-Traffic$ zeek-cut id.orig_h < conn.log | sort | uniq -c | sort -rn | head -n 10
uniq-c: command not found
zeek@admin:~/Zeek-Labs/TCP-Traffic$ zeek-cut id.orig_h < conn.log | sort | uniq -c | sort -rn | head -n 10
4003 10.0.0.1
  2 fe80::f0f2:9dff:fe76:b67e
  2 fe80::ec:f9ff:feb4:99eb
  2 fe80::bc49:b1ff:fe2b:9639
zeek@admin:~/Zeek-Labs/TCP-Traffic$ zeek-cut id.resp_p < conn.log | sort | uniq -c | sort -rn | head -n 10
  6 134
  5 3995
  5 39
  5 16992
  4 9990
  4 9998
  4 999
  4 9968
  4 995
  4 9944
zeek@admin:~/Zeek-Labs/TCP-Traffic$
```

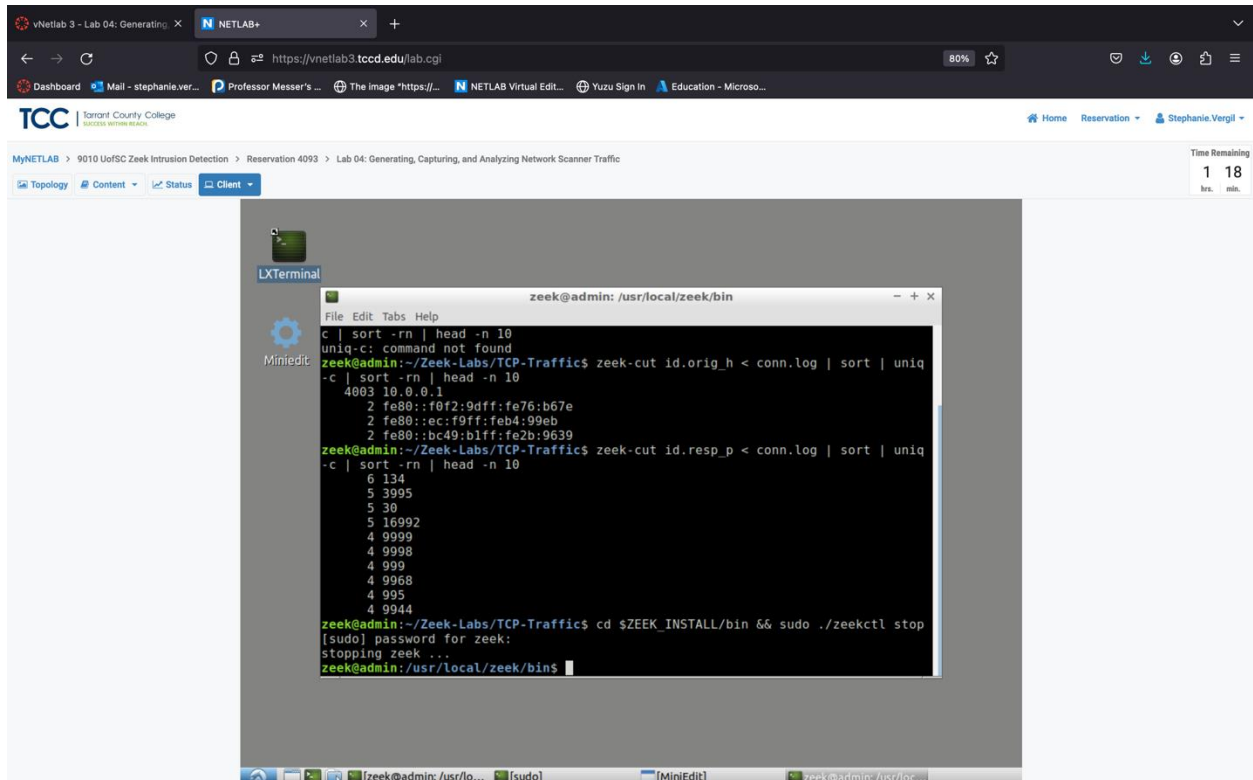
3.3 Closing the current instance of Zeek

It's essential to properly terminate the active instance of Zeek. Shutting down your computer while Zeek is still running can lead to improper shutdowns, potentially causing errors in future instances.

Step 1. Enter the following command to stop zeek:

```
cd $ZEEK_INSTALL/bin && sudo ./zeekctl stop.
```

Enter password when prompt.



The screenshot shows a web browser window with the URL <https://vnetlab3.tccd.edu/lab.cgi>. The page displays the TCC (Tarrant County College) logo and navigation links. A terminal window titled "LXTerminal" is open, showing the following commands and output:

```
zeek@admin: /usr/local/zeek/bin
c | sort -rn | head -n 10
uniq-c: command not found
zeek@admin:~/Zeek-Labs/TCP-Traffic$ zeek-cut id.orig_h < conn.log | sort | uniq
-c | sort -rn | head -n 10
4003 10.0.0.1
2 fe80::f0f2:9dff:fe76:b67e
2 fe80::ec:f9ff:feb4:99eb
2 fe80::bc49:blff:fe2b:9639
zeek@admin:~/Zeek-Labs/TCP-Traffic$ zeek-cut id.resp_p < conn.log | sort | uniq
-c | sort -rn | head -n 10
6 134
5 3995
5 30
5 16992
4 9999
4 9998
4 999
4 9968
4 995
4 9944
zeek@admin:~/Zeek-Labs/TCP-Traffic$ cd $ZEEK_INSTALL/bin && sudo ./zeekctl stop
[sudo] password for zeek:
stopping zeek ...
zeek@admin: /usr/local/zeek/bin$
```

In this lab we covered the process of generating scan traffic and enabling live traffic capture using Zeek. Once the data is collected, trace files can be analyzed to investigate empirical data concerning the current state of a network and its devices.