Stephanie Vergil

ZEEK INSTRUSION DETECTION SERIES

Lab 5: Generating, Capturing and Analyzing DoS and DDoS-centric Network Traffic

2.1 Starting a new instance of Zeek.

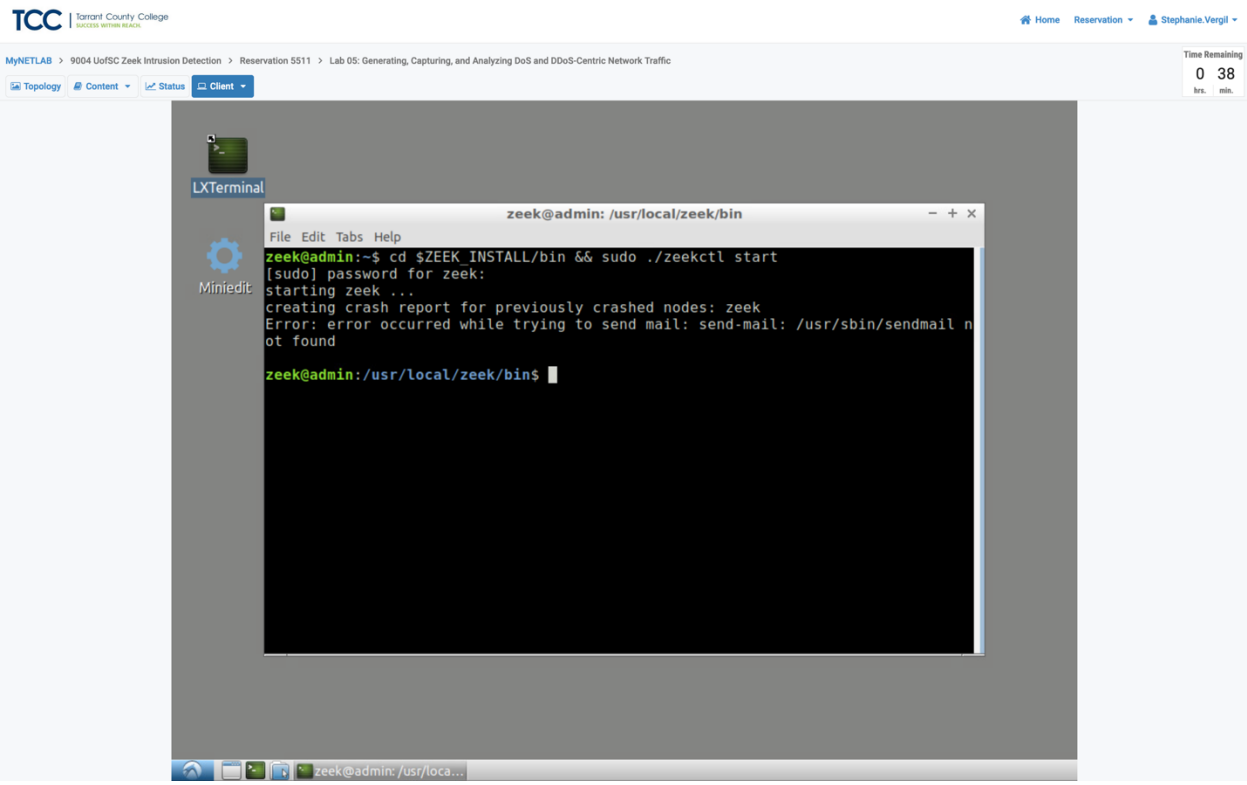
Step 1. Click on the client button to enter the client machine.

Step2. Once the client machine is open located on the desktop click on the LXTerminal to launch.

Step 3. To start Zeek enter the following command:

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

enter password when prompt.



2.2 Launching Mininet

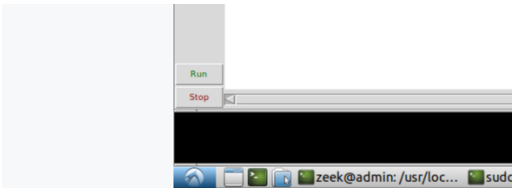
Step 1. Launch MiniEdit from the client's desktop, enter password when prompt.

Step 2. Once MiniEdit launches click on file and the click on open to load the correct topology.

Step 3. Navigate to the Zeek-Topologies directory, double click the Zeek-Topologies Icon.

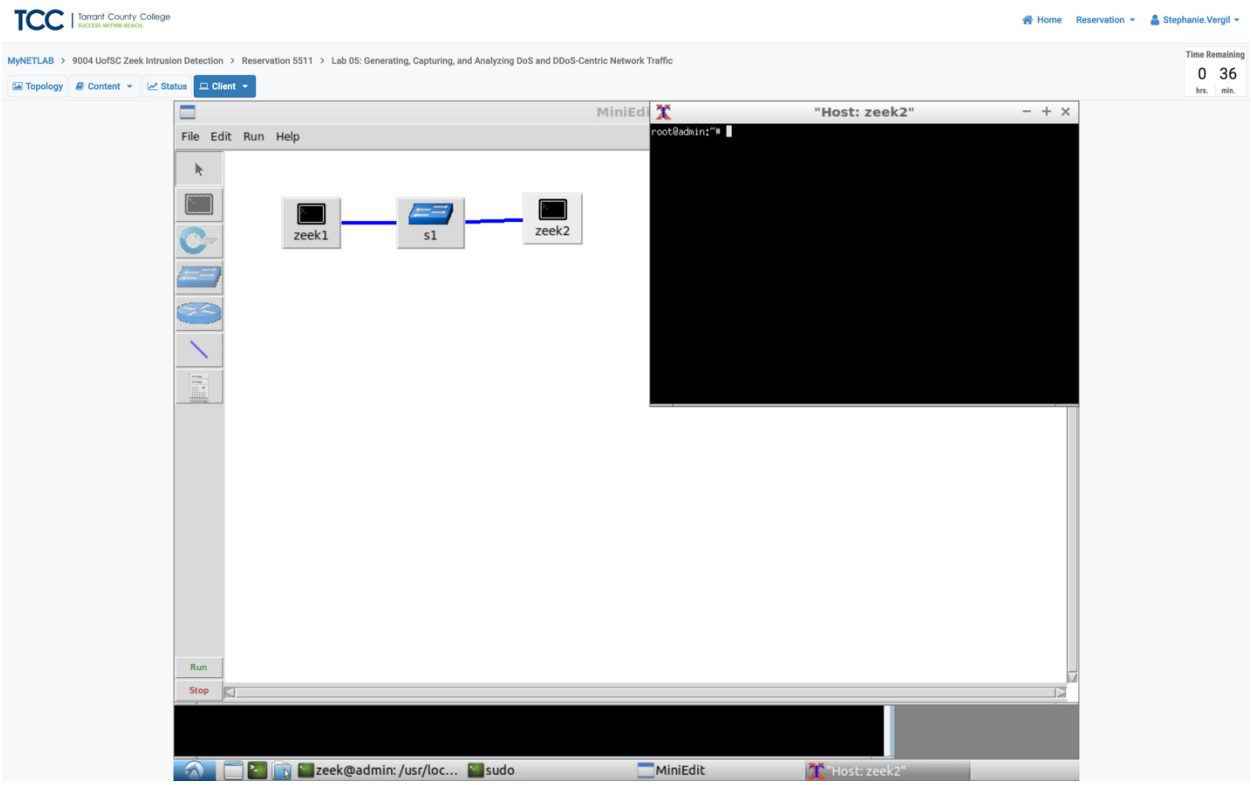
Step 4. Once it is open select the topology.mn and click on the open button.

Step 5. To start running the VM's on the bottom left select the run button.



2.3 Setting up the zeek2 machine for live network capture.

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



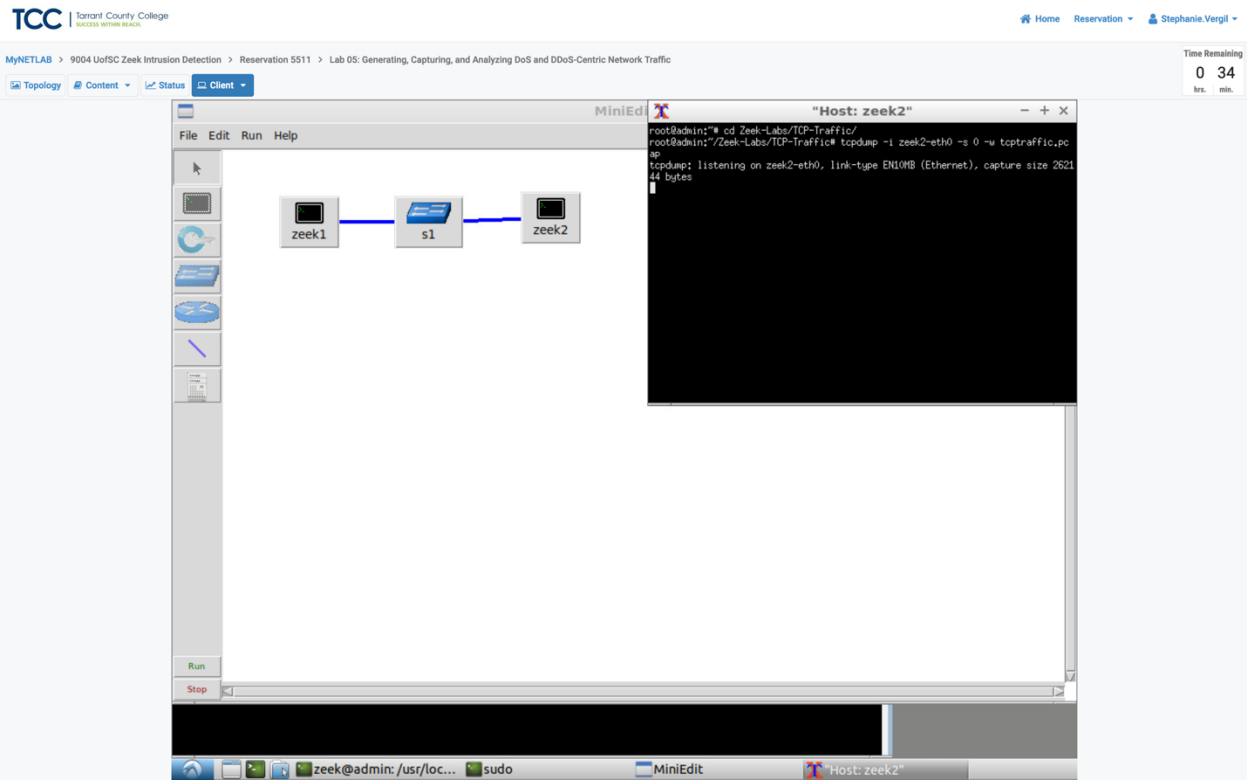
Step 2. Enter the following command to navigate to the TCP-Traffic directory from the zeek2 terminal:

cd Zeek-Labs/TCP-Traffic/

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

tcpdump -i zeek2-eth0 -s 0 -w tcptraffic.pcap

Now the zeek2 virtual machine is now ready to start collecting live network traffic. To continue I will use the zeek1 machine to generate scan-based network traffic.



2.4 Launching LOIC

Step 1. Open the zeek1 terminal.

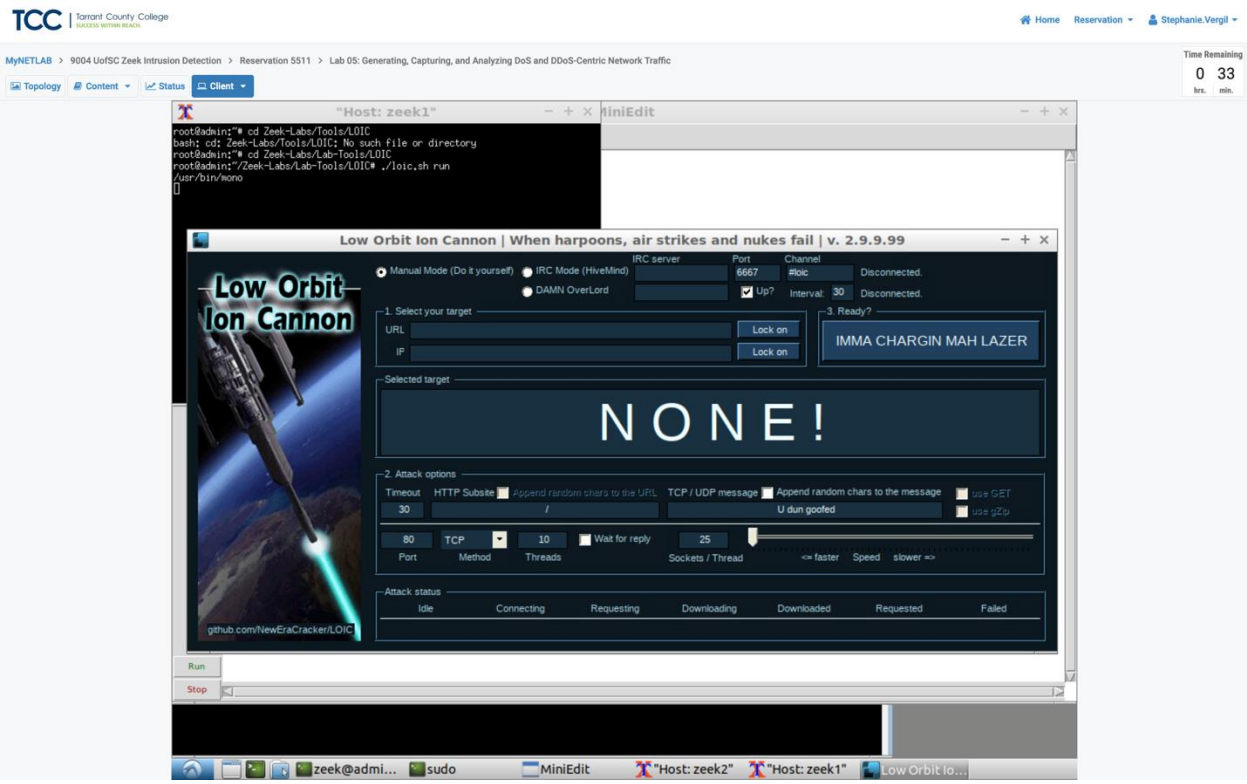
Step 2. To navigate to the Zeek-Labs/Lab-Tools/LOIC directory enter the following command:

cd Zeek-Labs/Lab-Tools/LOIC

Step 3. To execute the loic.sh shell script enter the following command in the terminal:

./loic.sh run

Step 4. View the LOIC GUI. Scale the GUI if necessary.



The LOIC interface comprises several key features:

Target IP Address (Red Box): Input field for specifying the destination IP address. Clicking the "Lock on" button selects the IP as the target destination.

Target Port (Green Box): Allows for the adjustment of the target port, which varies depending on the chosen method for launching the Denial of Service (DoS) attack.

Target Method (Yellow Box): Provides options for selecting the protocol to be used in the DoS attack.

Number of Threads (Blue Box): Indicates the quantity of resources allocated by LOIC on the host machine for the attack.

Number of Sockets per Thread (Purple Box): Determines the speed of the DoS attack; increasing this number exponentially boosts the attack speed but demands more resources.

Packet Payload (Brown Box): Defines the content carried by each packet as payload.

Start Button (Orange Box): Initiates the attack after customizing the desired parameters.

2.5 Using the zeek1 virtual machine to launch a TCP-based DoS attack.

Step 1: Customize the DoS attack by entering the following values in their correct boxes.

IP: 10.0.0.2

Port: 80

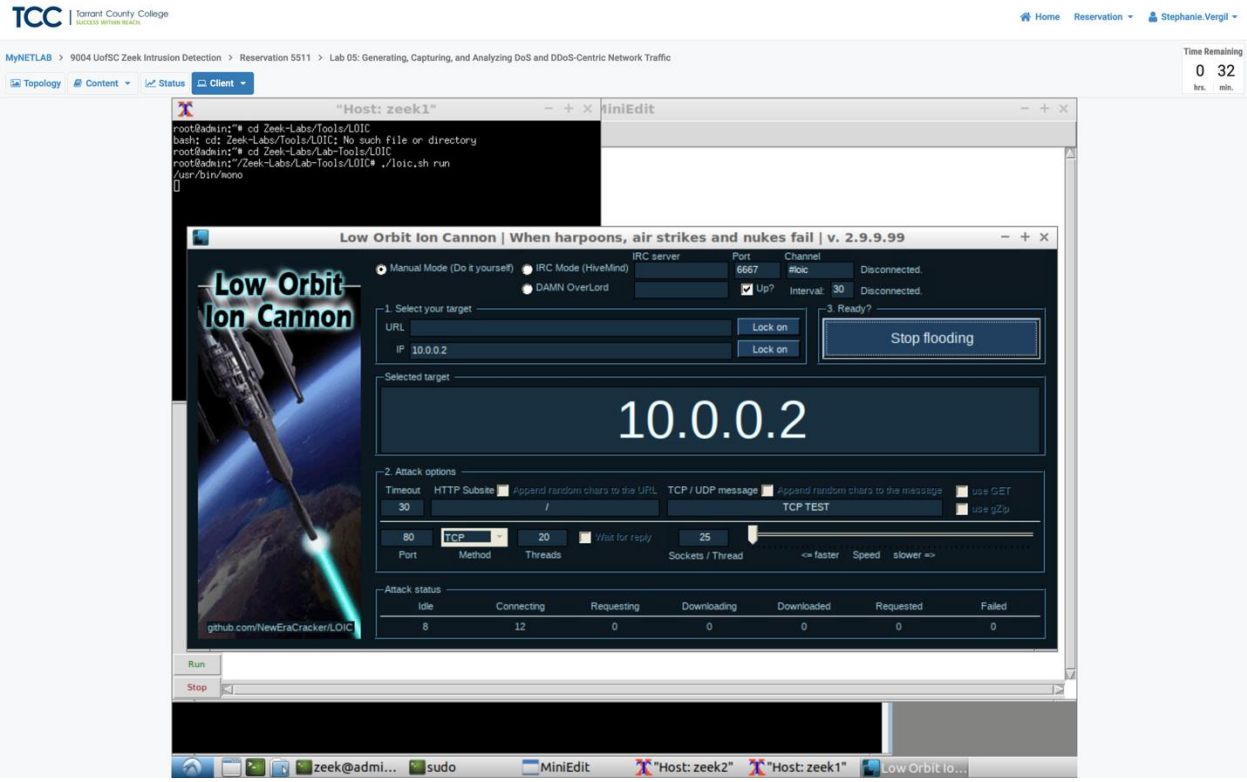
Method: TCP

Threads: 20

Sockets: 25

Payload: TCP TEST

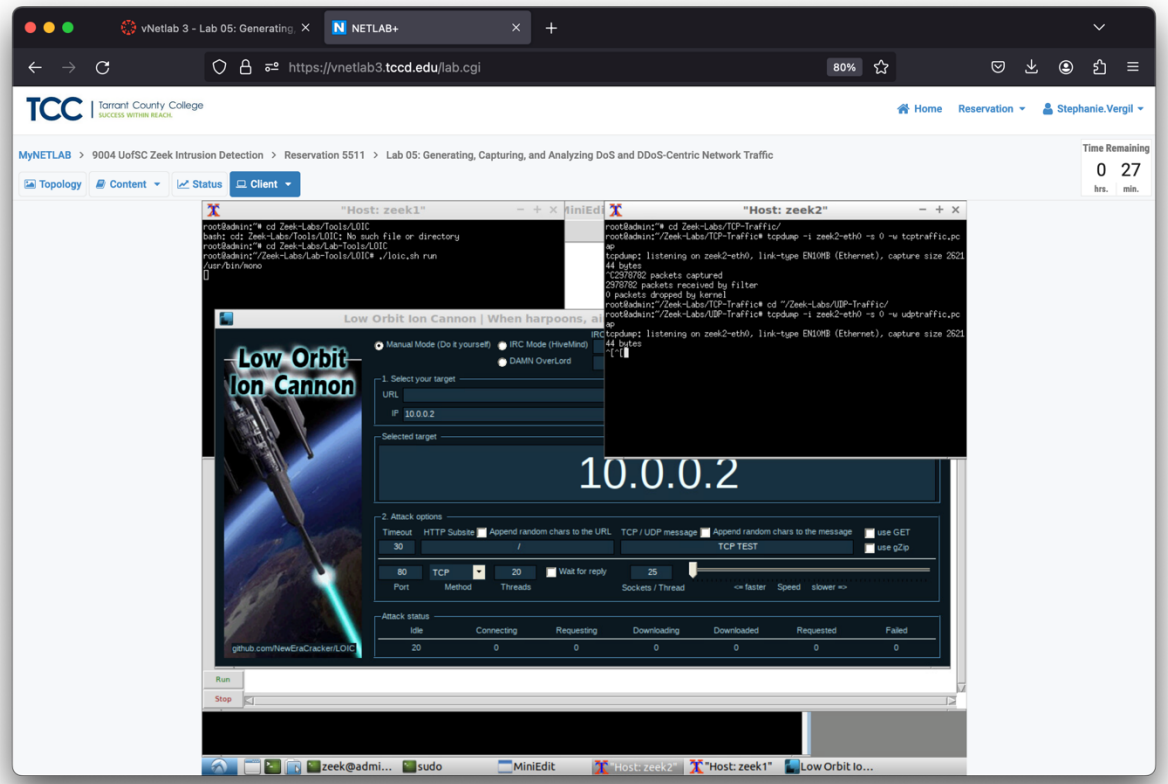
Step 2. Click the Lock on button to save the current configurations. Click the Start (IMMA CHARGIN MAH LAZER) button to begin the DoS attack. Wait around 10 seconds and click. the Stop button to stop the DoS attack.



Step 3. open the zeek2 Terminal using the navigation bar at the bottom of the screen.

Step 4. Use Ctrl+c to stop live traffic capture. The Statistics of the capture session will be displayed with network packets being stored in the new tcptraffic.pcap file.

2978782 packets were generated and collected. DoS attacks create a lot of network traffic, which is shown by the large number of packets. This is much more than what we see during regular scan events, where only a few packets are generated.



2.6 Using the zeek1 virtual machine to launch a UDP-based DoS attack

Step 1. Using the zeek2 virtual machine, enter to following command to navigate to the lab workspace directory:

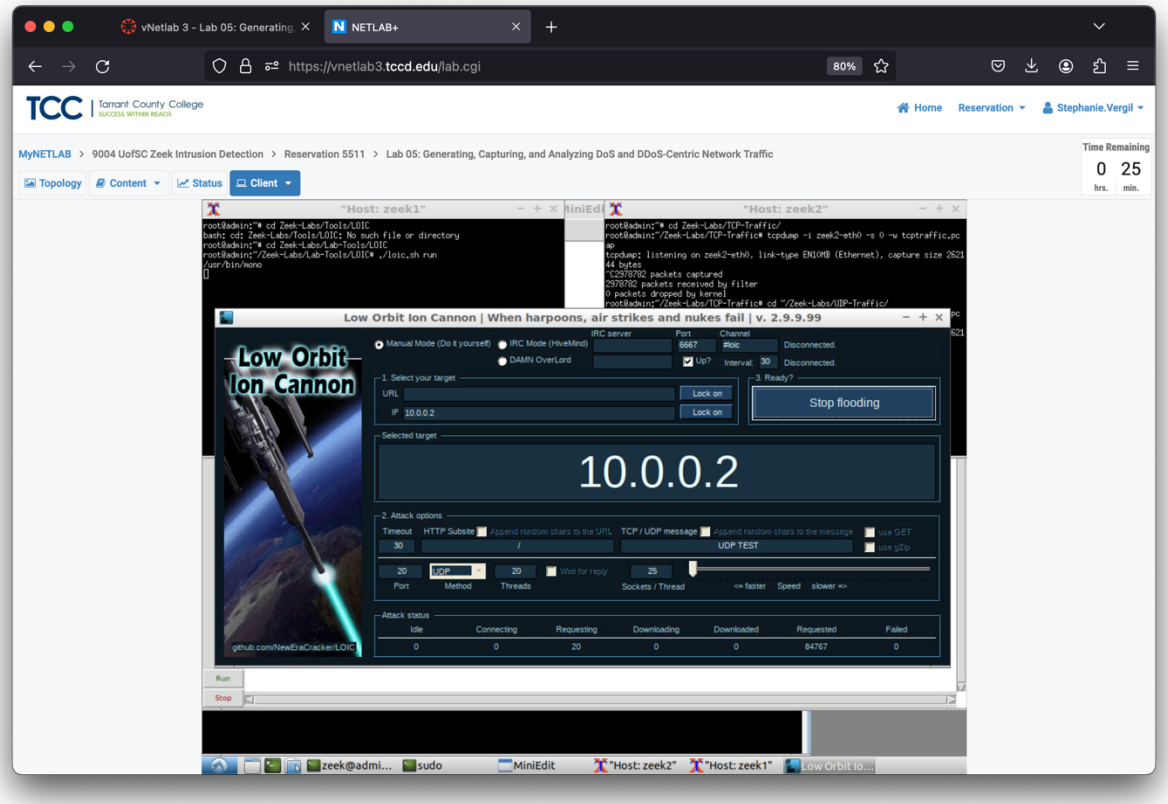
cd ~/Zeek-Labs/UDP-Traffic/

Step 2. To start live packet capture on interface zeek2-eth0 and save the output to a file

named udptraffic.pcap enter the following command:

tcpdump -i zeek2-eth0 -s 0 -w udptraffic.pcap

Step 3. open the LOIC GUI using the navigation bar.



Step 4. Customize the DoS attack by entering the following values in their respective boxes.

IP: 10.0.0.2

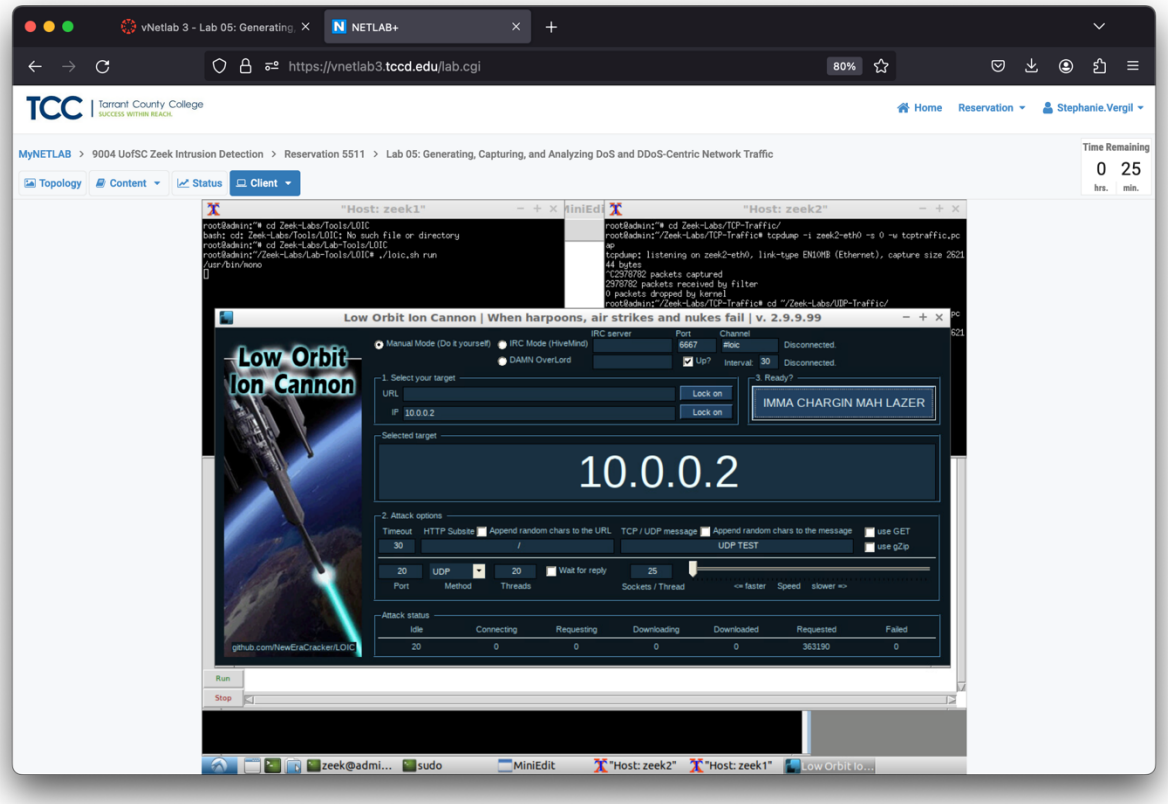
Port: 20

Method: UDP

Threads: 20

Sockets: 25

Payload: UDP TEST (Must be changed before updating Method feature)

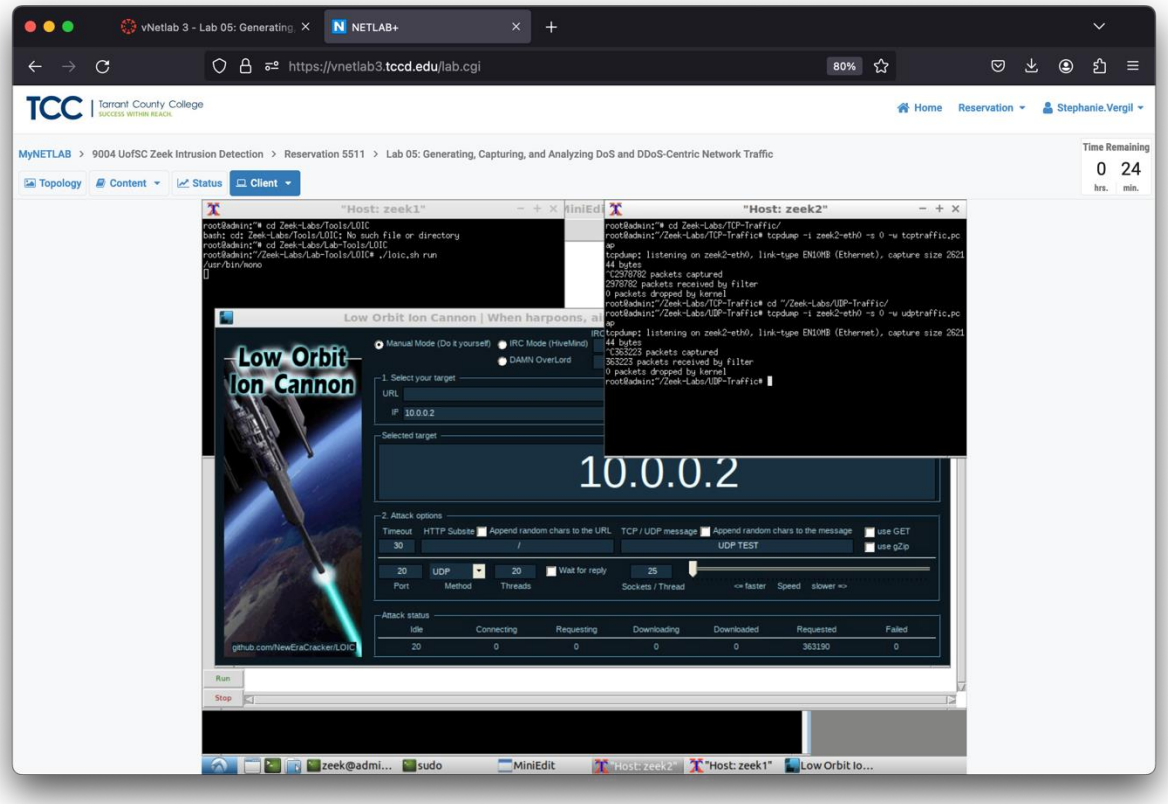


Step 5. Click the Lock on button to save the current configurations. Click the Start (IMMA CHARGIN MAH LAZER) button to begin the DoS attack. Wait around 10 seconds and click. the Stop button to stop the DoS attack.

Step 6. Open the zeek2 terminal.

Step 7. Use Ctrl+c to stop live traffic capture. The Statistics of the capture session will be displayed with network packets being stored in the new tcptraffic.pcap file. 363223 packets were generated and collected.

Although the UDP-based DoS attack didn't produce as much network traffic as the TCP-based one, it still generated substantial traffic from a single machine. When expanded to a large-scale attack, DoS attacks can be highly damaging.



Step 8. To end the current Mininet session, click on the Stop button.

3.1 Analyzing TCP-based traffic.

After completing both a TCP-based and UDP-based DoS attack successfully, we can analyze the collected network traffic using Zeek and the zeek-cut utility commands to view the captured traffic.

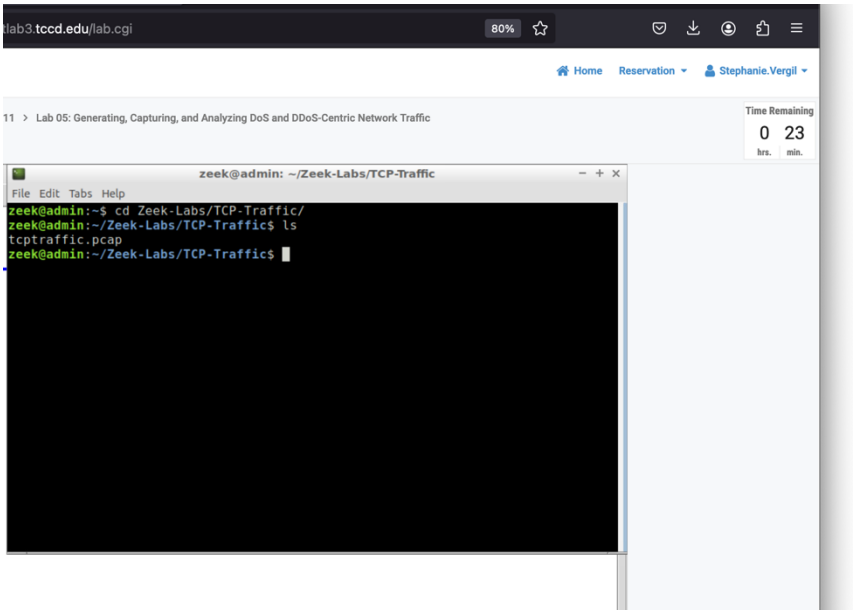
Step 1. Launch LXTerminal located on the client's machine desktop

Step 2. To navigate to the TCP-Traffic directory to find the tcptraffic.pcap file enter the following command:

cd Zeek-Labs/TCP-Traffic/

Step 3. Enter the following command to view the file contents of the TCP-Traffic directory to ensure that the tcptraffic.pcap file was successfully saved:

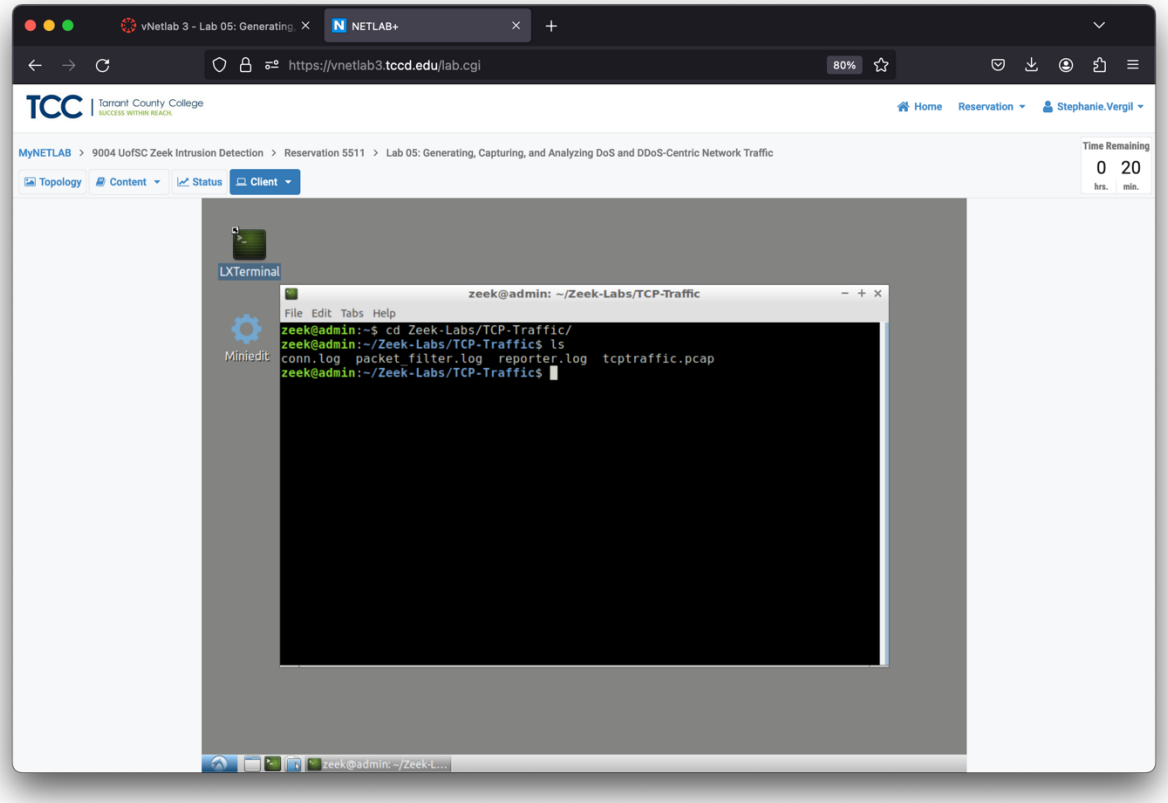
ls



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

zeek –C -r tcptraffic.pcap

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

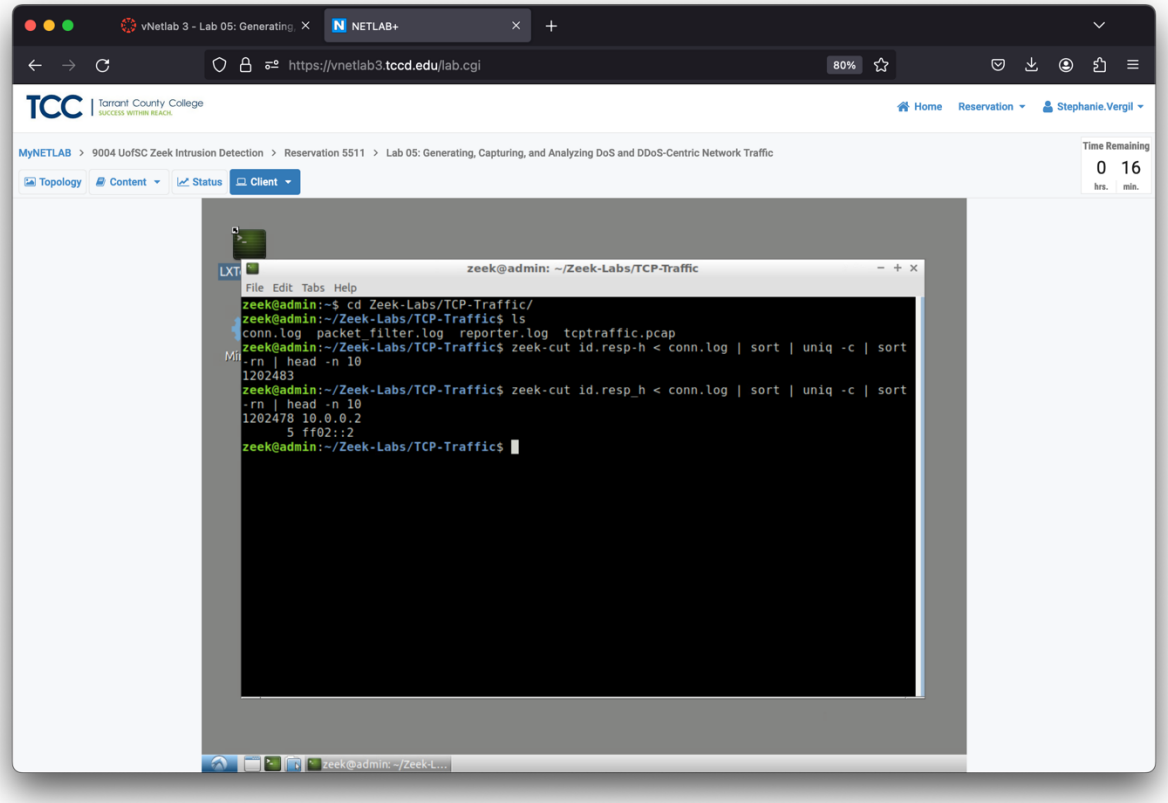


3.1.1 TCP Example Query 1

Example 1: Show the source IP addresses that generated the most network traffic, organized in descending order using the following command:

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

The zeek2 VM received 1202478 TCP packets. Commands like this help find vulnerable hosts in networks, aiding threat mitigation.

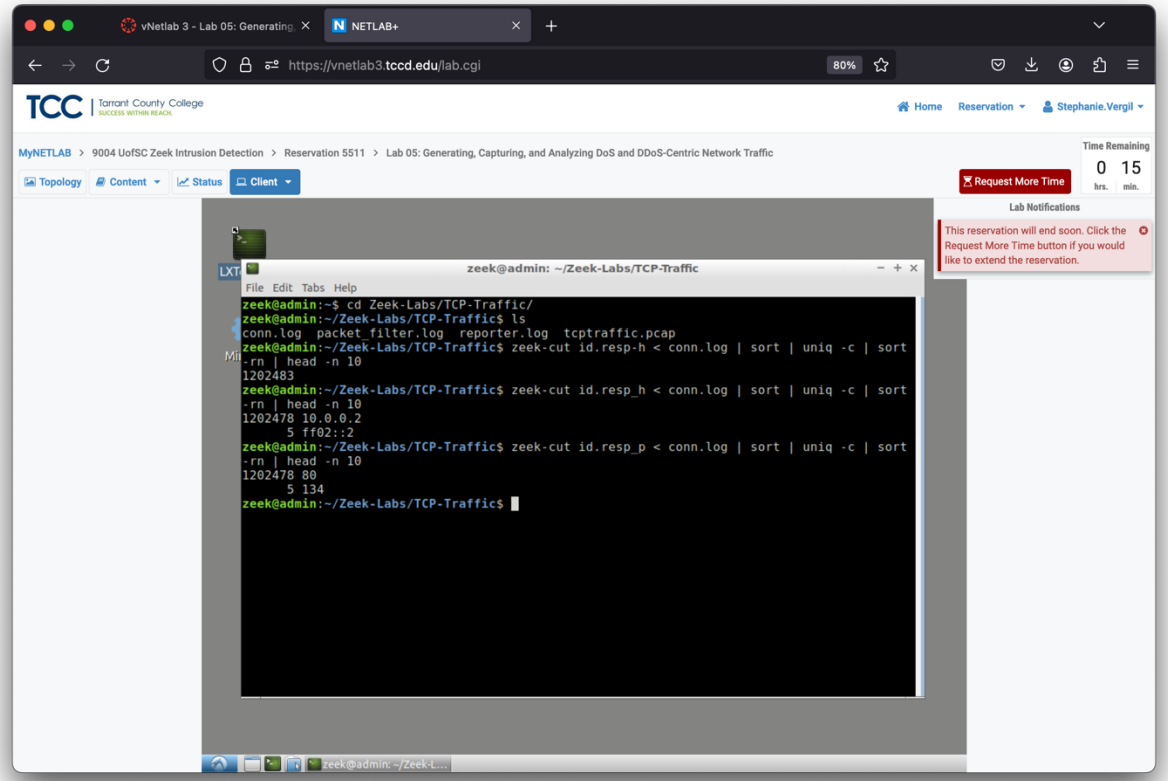


3.1.2 TCP Example Query 2

Example 1: Show the destination ports that received the most traffic, organized in descending order. Use the following command:

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

We observed 1202478 packets received by the zeek2 VM on port 80, the specified target for zeek1. Although LOIC (Low Orbit Ion Cannon) attempts connections, revealing additional ports, like port 134 it's evident our designated port is the primary target in the DoS attack.



3.2 Analyzing UDP-based traffic

Step 1. To navigate to the UDP-Traffic directory to find the udptraffic.pcap file enter the following command:

cd ~/Zeek-Labs/UDP-Traffic/

Step 2. Enter the following command to view the file contents of the TCP-Traffic directory to ensure that the udptraffic.pcap file was successfully saved:

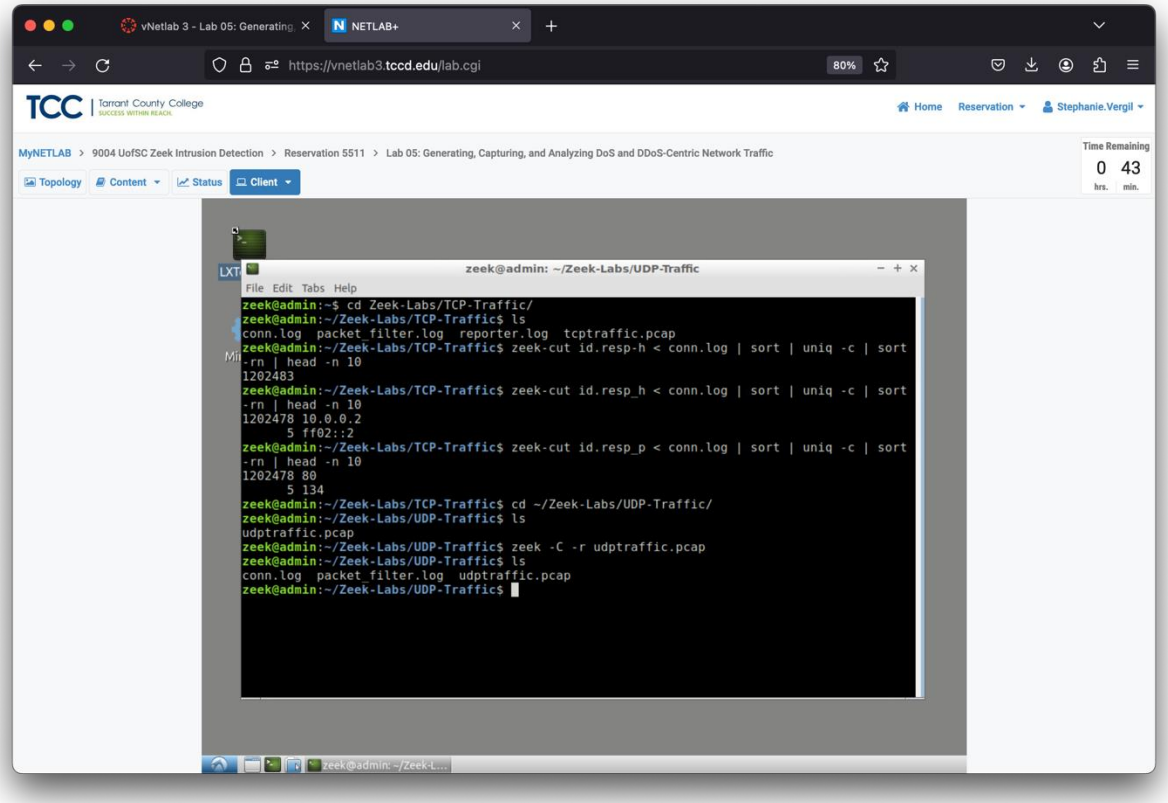
ls

Step 3. Enter the following Zeek command to process the packet capture file:

zeek –C -r udptraffic.pcap

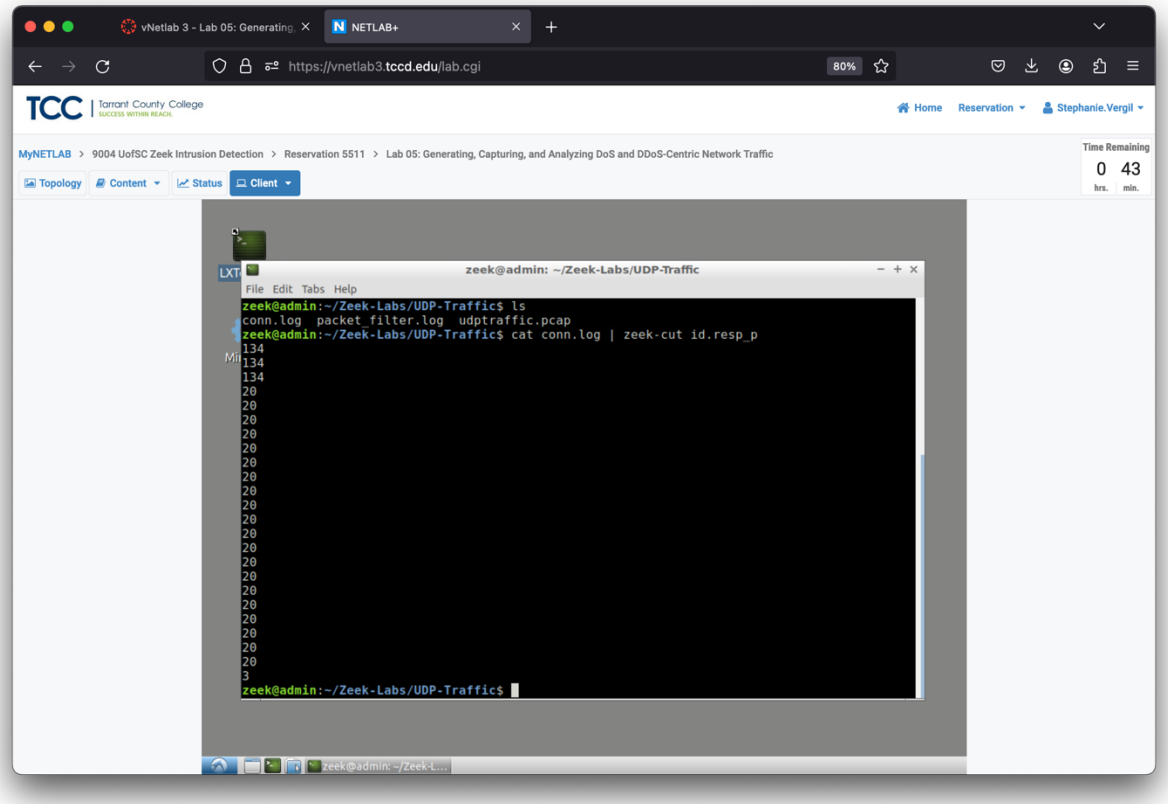
Step 4. To List the generated Zeek log files enter the following command:

ls



Step 5. To show the list of ports that received network traffic enter the following command: cat conn.log | zeek-cut id.resp_p

Despite collecting a large number of packets, only a few were registered by Zeek's event-based engine. Although we targeted port 20 in our DoS attack, the identified packet count is lower than anticipated. This drop is mainly because many UDP packets are being dropped, likely due to firewalls. While UDP packets might be traced on the interface, they may not reach the intended destination. Additionally, Zeek's default settings are geared towards TCP traffic and lack comprehensive UDP handling, requiring additional scripts and policies.

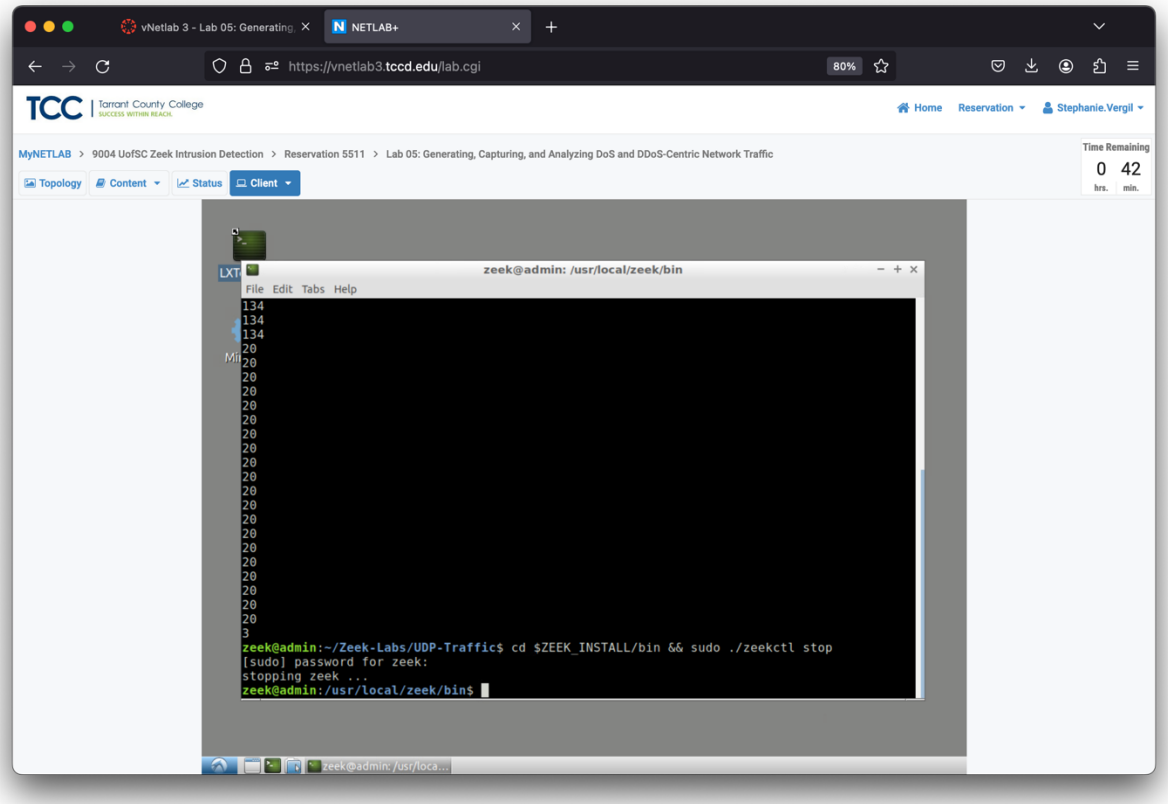


3.3 Closing the current instance of Zeek

it's essential to terminate the current Zeek instance properly. Execute the following command in the terminal:

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

If prompted, enter the password.


vNetlab 3 - Lab 05: Generating
NETLAB+
https://vnetlab3.tccd.edu/lab.cgi
80%
TCC
Tarrant County College
Home
Reservation
Stephanie.Vergil
MyNETLAB > 9004 UofSC Zeek Intrusion Detection > Reservation 5511 > Lab 05: Generating, Capturing, and Analyzing DoS and DDoS-Centric Network Traffic
Time Remaining
0 hrs. 42 min.
Topology
Content
Status
Client
zeek@admin: /usr/local/zeek/bin
File Edit Tabs Help
134
134
134
20
20
20
20
20
20
20
20
20
20
20
20
20
20
20
20
20
20
20
3
zeek@admin:~/Zeek-Labs/UDP-Traffic$ cd $ZEEK_INSTALL/bin && sudo ./zeekctl stop
[sudo] password for zeek:
stopping zeek ...
zeek@admin:/usr/local/zeek/bin$