Statement and Confirmation of Own Work



***A signed copy of this form must be submitted with every assignment.***

***If the statement is missing your work may not be marked.***

**Student Declaration**

I confirm the following details:

|  |  |
| --- | --- |
| **Student Name:** | Johnson Kenisha Corera |
| **Student ID Number:** | c23020001@cicra.edu.lk |
| **Qualification:** | Bachelor in Cyber Security |
| **Unit:** | SIT325 Advanced Network Security |
| **Centre:** | CICRA Campus |
| **Word Count:** | 383 |
| I have read and understood both *Deakin* *Academic Misconduct Policy* and the *Referencing and Bibliographies* document. To the best of my knowledge my work has been accurately referenced and all sources cited correctly.  I confirm that I have not exceeded the stipulated word limit by more than 10%.  I confirm that this is my own work and that I have not colluded or plagiarized any part of it. | |
| **Candidate Signature:** |  |
| **Date:** | 01/02/2025 |

**Task 6.2C**

**Table of Content**

[Part A](#PartA)…………………………………………………………………………………………04

[Installation Jpert](#Jpert)……………………………………………………………………………...06

[Installation (LOIC)](#LOIC)…………………………………………………………………………...09

[DDoS Attack](#Attack)………………………………………………………………………………….11

**Table of Figures**

[Figure 01](#figure1)……………………………………………………………………………………04

[Figure 02](#figure2)……………………………………………………………………………………04

[Figure 03](#figure3)……………………………………………………………………………………04

[Figure 04](#figure4)……………………………………………………………………………………05

[Figure 05](#figure5)……………………………………………………………………………………06

[Figure 06](#figure6)……………………………………………………………………………………07

[Figure 07](#figure7)……………………………………………………………………………………07

[Figure 08](#figure8)……………………………………………………………………………………08

[Figure 09](#figure9)……………………………………………………………………………………09

[Figure 10](#figure10)……………………………………………………………………………………09

[Figure 11](#figure11)……………………………………………………………………………………10

[Figure 12](#figure12)……………………………………………………………………………………11

[Figure 13](#figure13)……………………………………………………………………………………11

[Figure 14](#figure14)……………………………………………………………………………………12

[Figure 15](#figure15)……………………………………………………………………………………12

[Figure 16](#figure16)……………………………………………………………………………………13

[Figure 17](#figure17)……………………………………………………………………………………14

[Figure 18](#figure18)……………………………………………………………………………………14

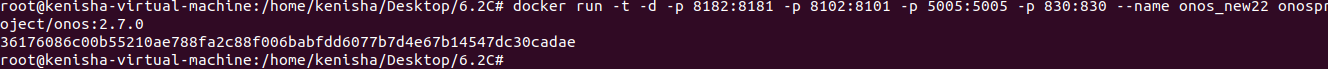
[Figure 19](#figure19)……………………………………………………………………………………15

[Figure 20](#figure20)……………………………………………………………………………………15

[Figure 21](#figure21)……………………………………………………………………………………16

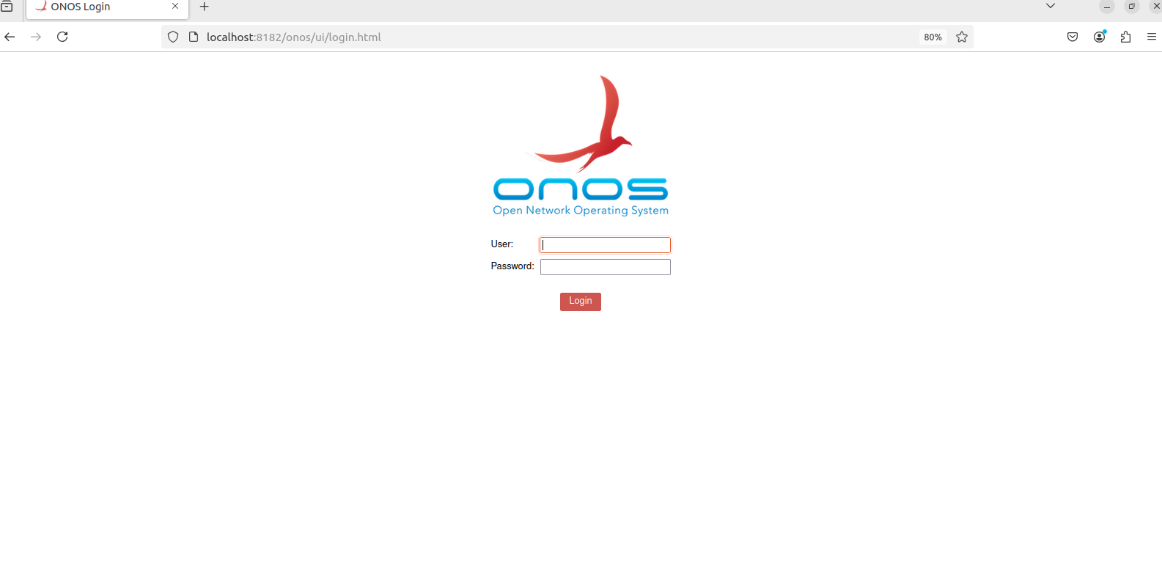
**Part A**

* I was able to successfully run onos in the Docker container first.

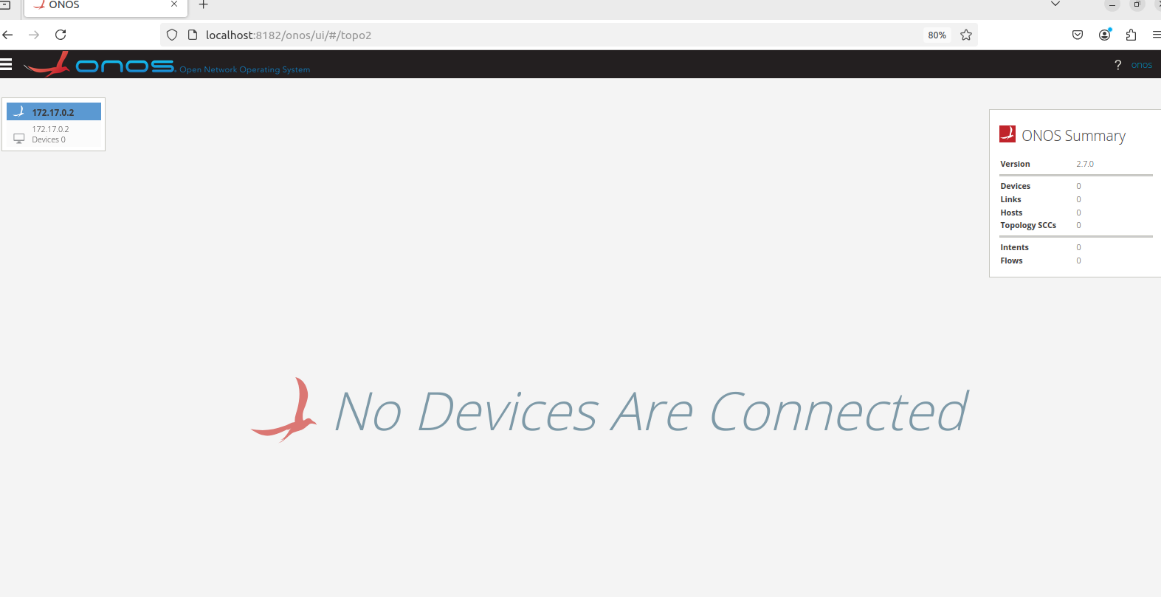


*Figure 01: Using Docker to operate onos*

* I used the browser to log into the Onos after that.



*Figure 02: Accessing Onos*

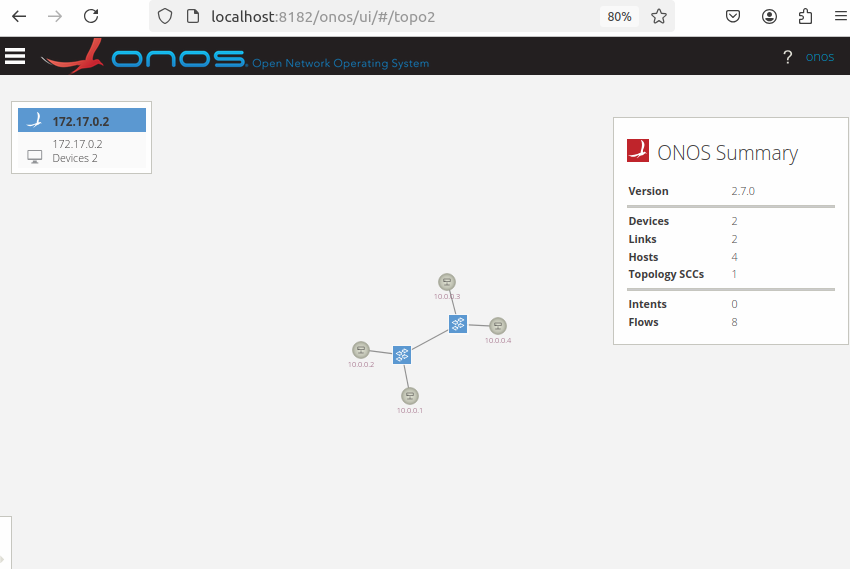
**

*Figure 03: The main page of Onos*

**

*Figure 04:* Mininet operating successfully

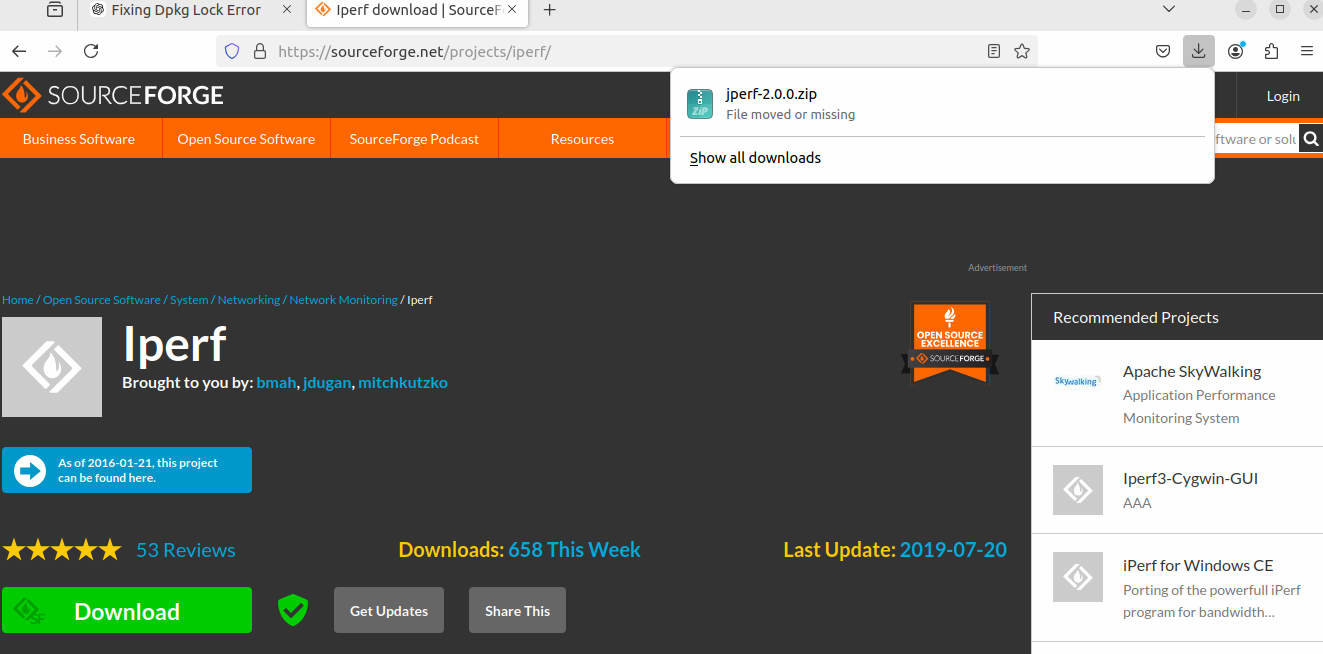
* After testing mininet execution I performed connectivity tests through the ping command.



*Figure 05: linked network topology*

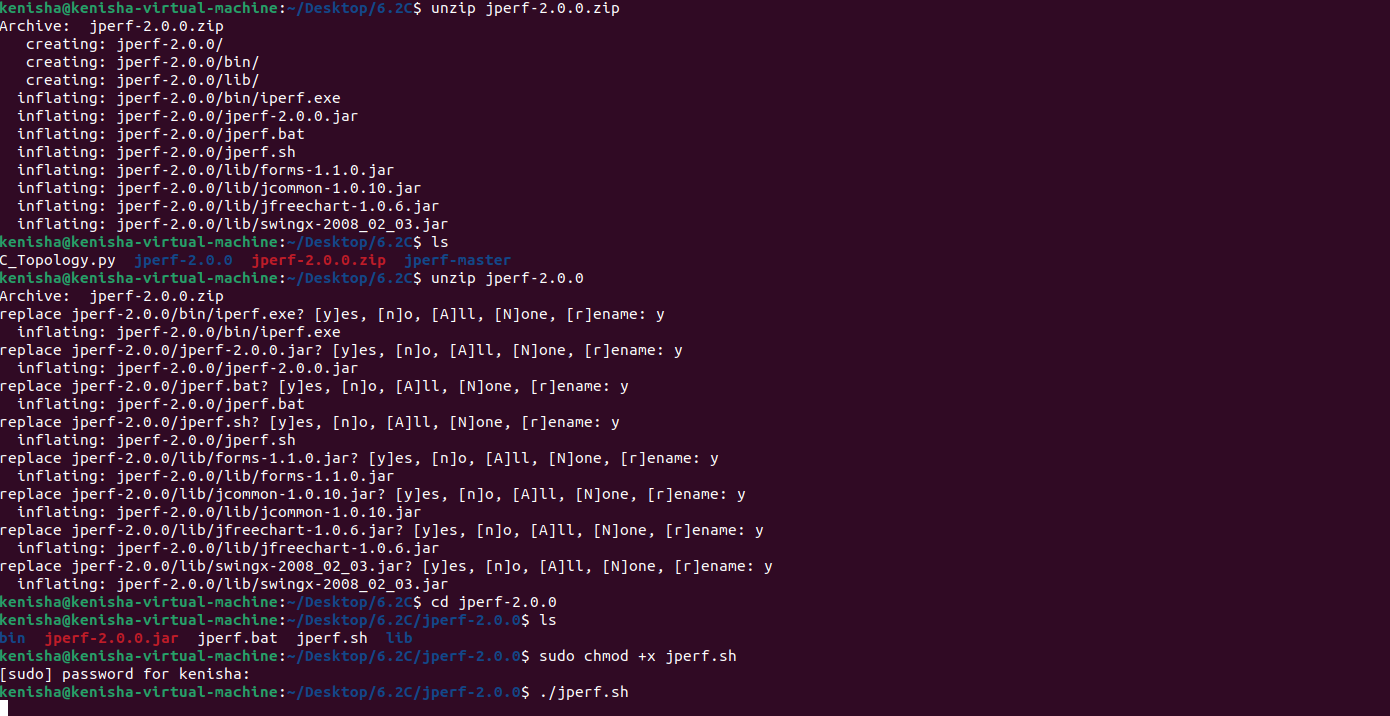
* I used the pingall command to build network connections between my hosts and the onos devices.

**Installation Jpert**



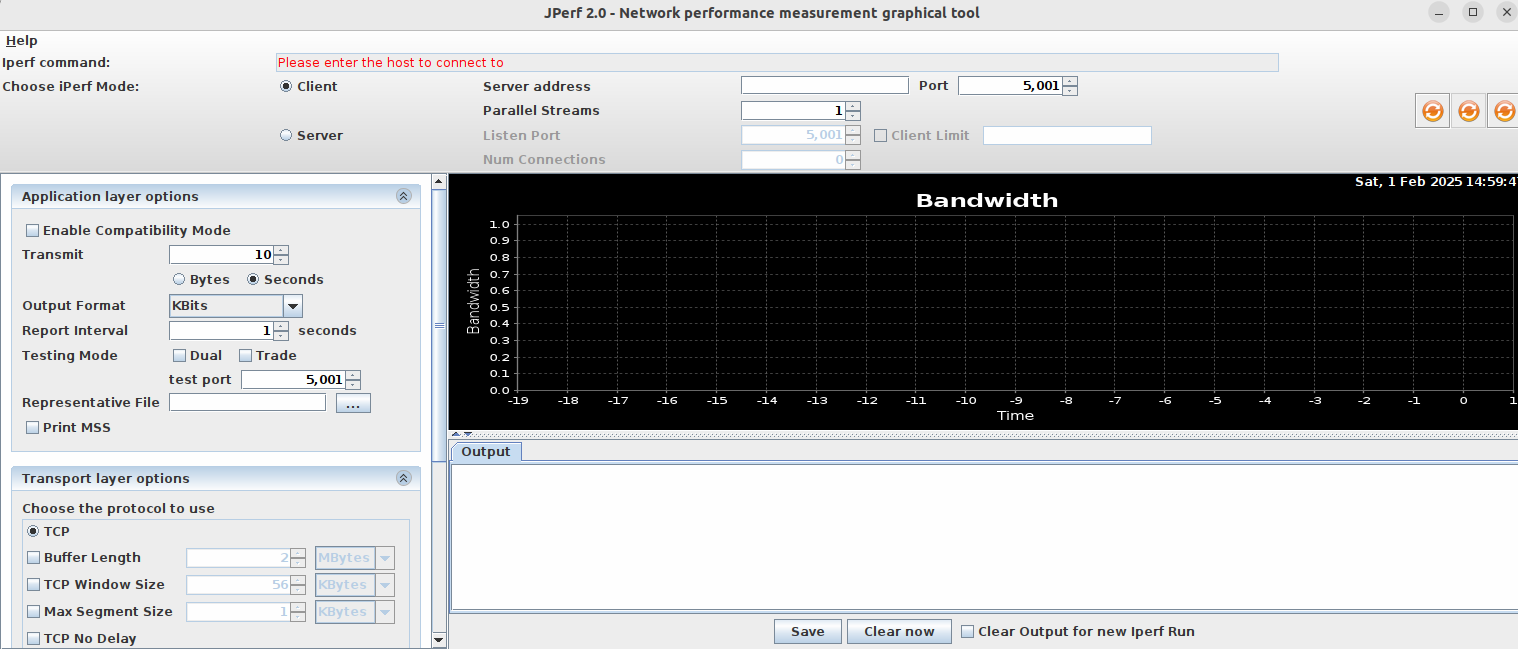
*Figure 06: JPerf installation via SourceForge*

* Setting up JPERF and releasing the files.



*Figure 07: launching the program after unzipping it*

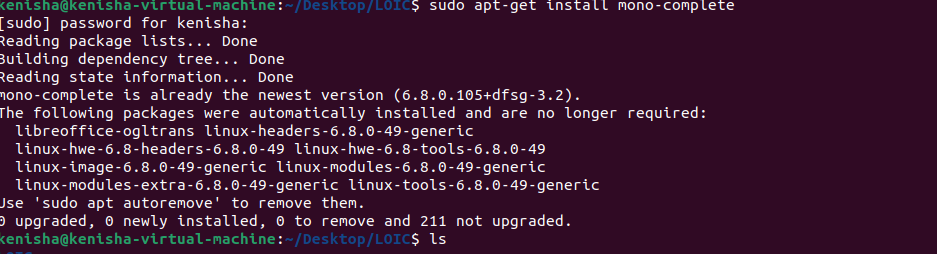
* Executive process launch of the JPerf utility succeeded once I ran the program.



*Figure 08: Jperf had a successful launch.*

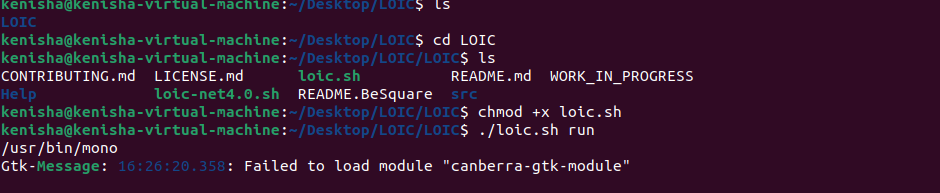
**Installation (LOIC) Low Orbit Ion Cannon**

* Through the LOIC application I am currently conducting a DDoS attack.

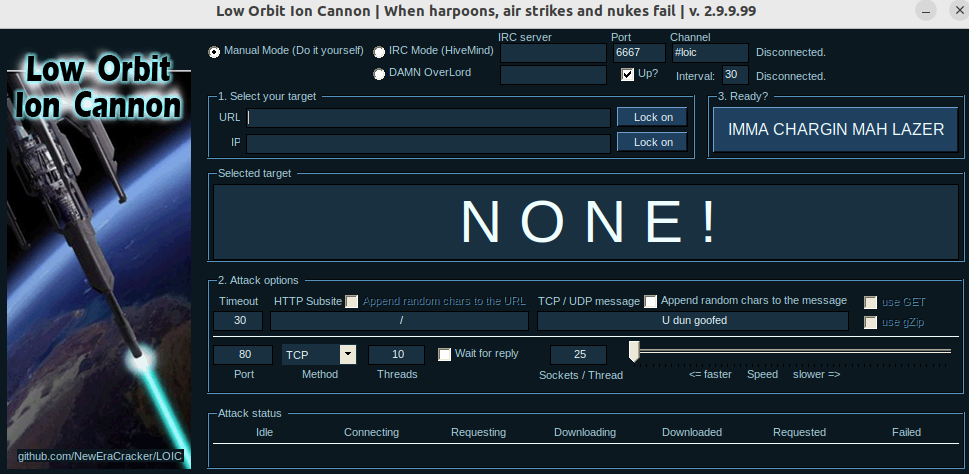


*Figure 09: Setting up LOIC*

* The tool extraction process took place immediately following installation.



*Figure 10: conducted with success LOIC.*

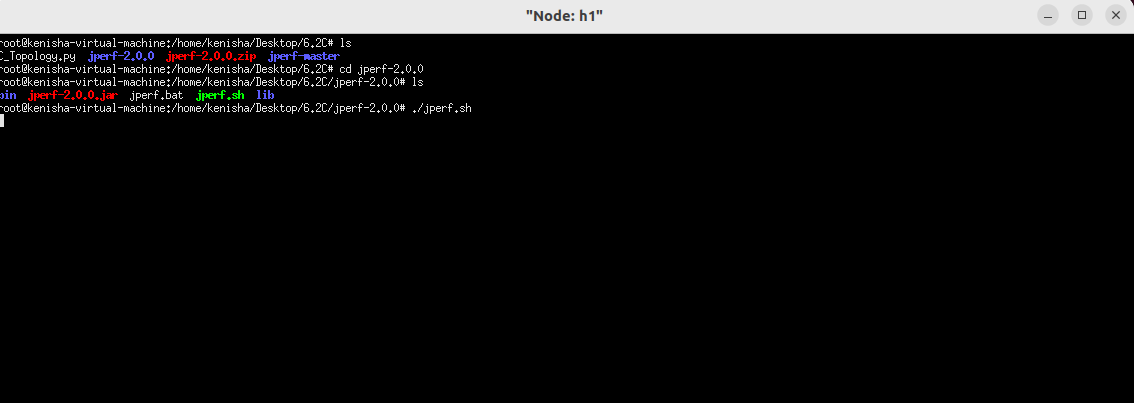
**

*Figure 11: operating LOIC*

* I managed to acquire the LOIC GUI interface successfully*.*

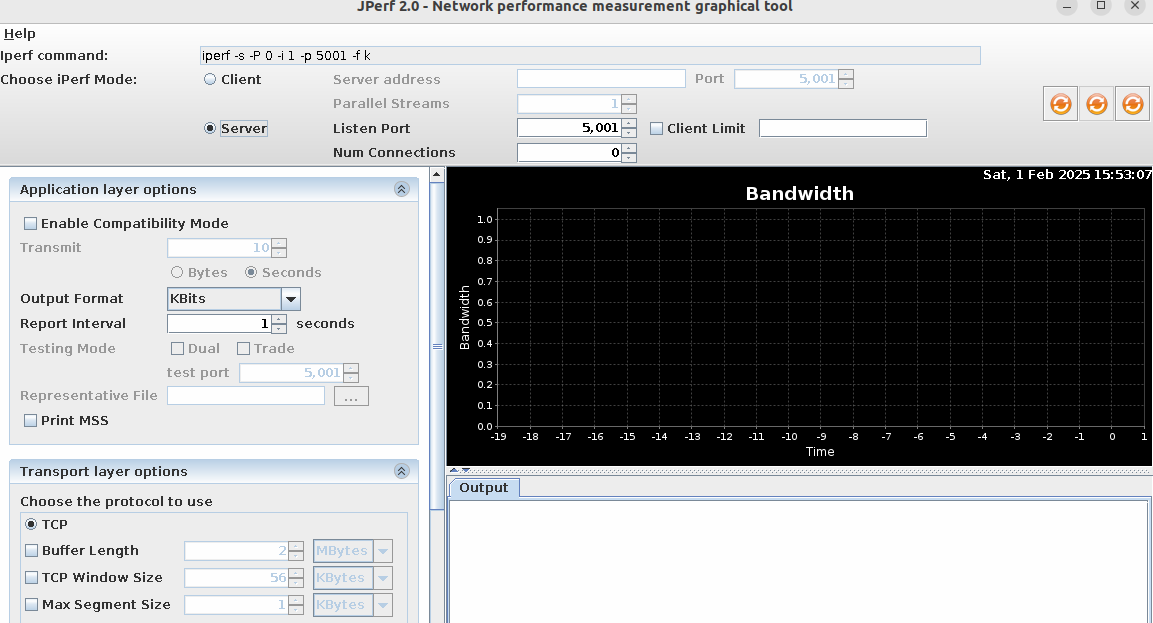
**DDoS Attack**

* The experimental setup consisted of H1 functioning as the host machine with H2 running as the client system supported by H3 running the LOIC program.



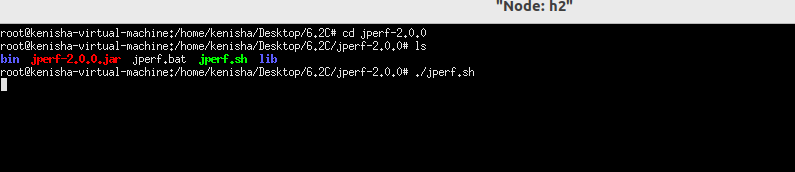
*Figure 12: Using H1 as the operating system*

* JPerf functionality on H1 required suitable parameter settings to become an operational server. The system required setup of a listening port along with other necessary consumption parameters. The server currently operated in a state where it could receive client data. The client believed these configurations delivered precise performance measurement results. Figure 1 displays how the H1 needs to be configured to serve as a server system.

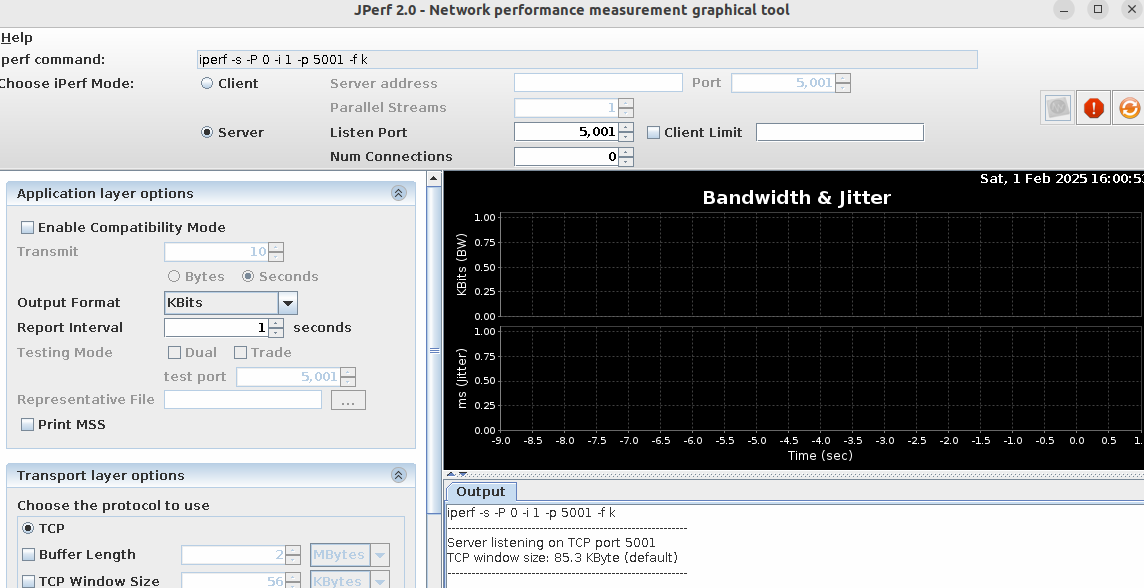


*Figure 13: H1 JPerf*

* I provided JPerf all necessary server information including the IP address and test parameters to allow it operate as a client on h2. The client had the willingness to share performance measurement data with the server on h1. Precise data transfer and measurement required these setup configurations. The host H2 could start testing.

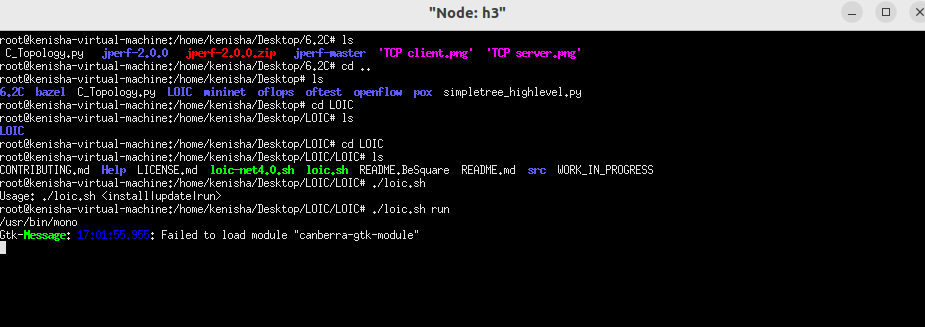


*Figure 14: utilizing H2 as a client*



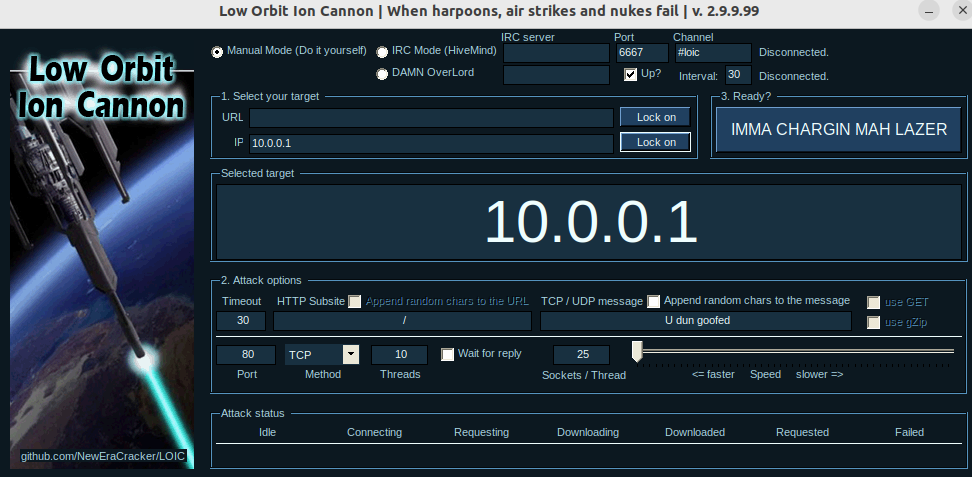
*Figure 15: Using H2 as a client, Jperf*

* The client computer is on H2.
* The H3 will serve as my trigger to start the DDoS attack.



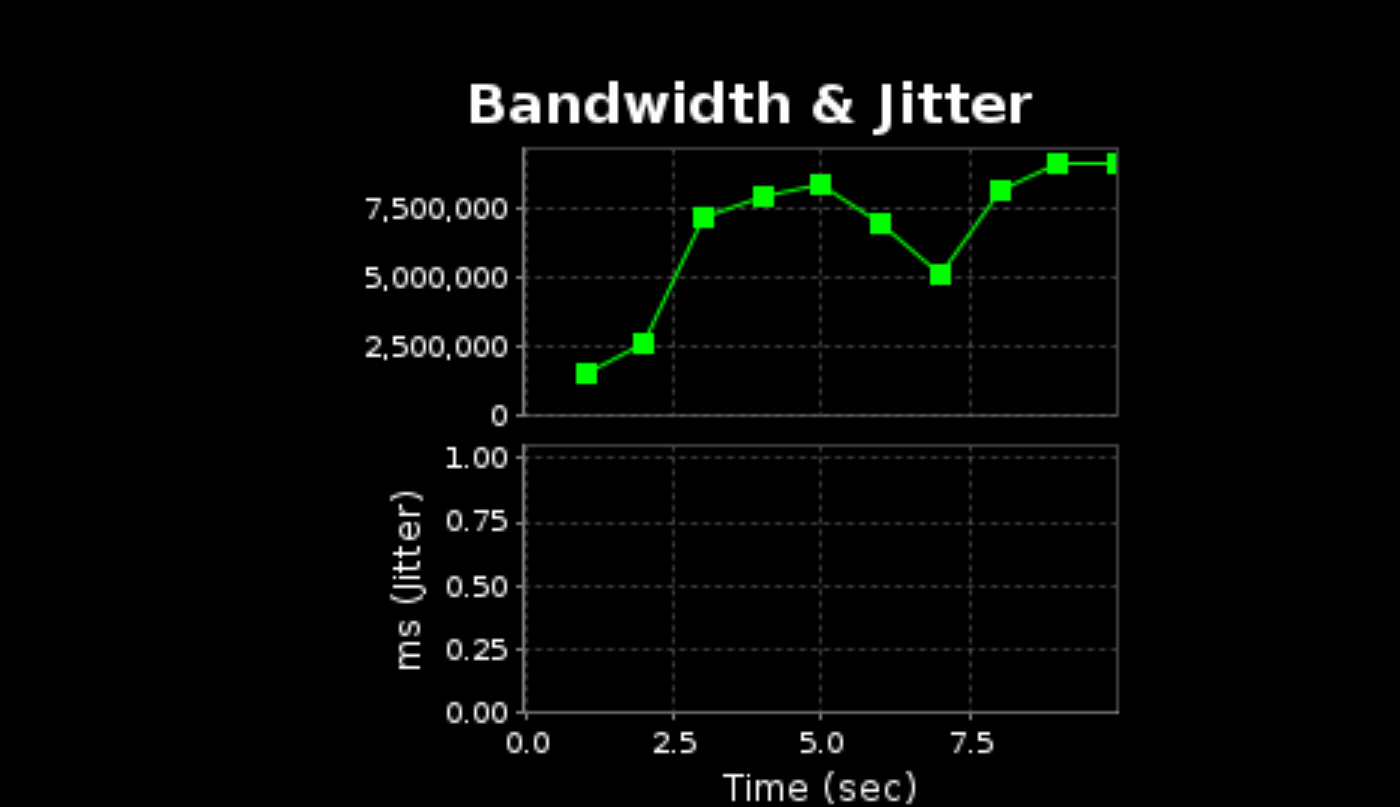
*Figure 16: H3 operating as LOIC*

* Server targeting becomes an essential step when working with the LOIC tool from H3.

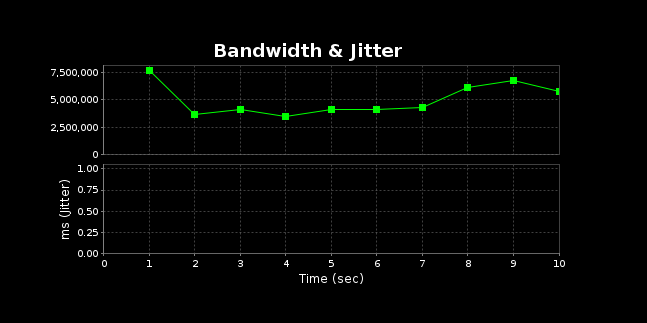


*Figure 17: LOIC began to run.*

* During H3 I deployed the attack before implementing the LOIC protocol. Users must construct an H2 client application which connects to a server system to initiate the monitoring process.



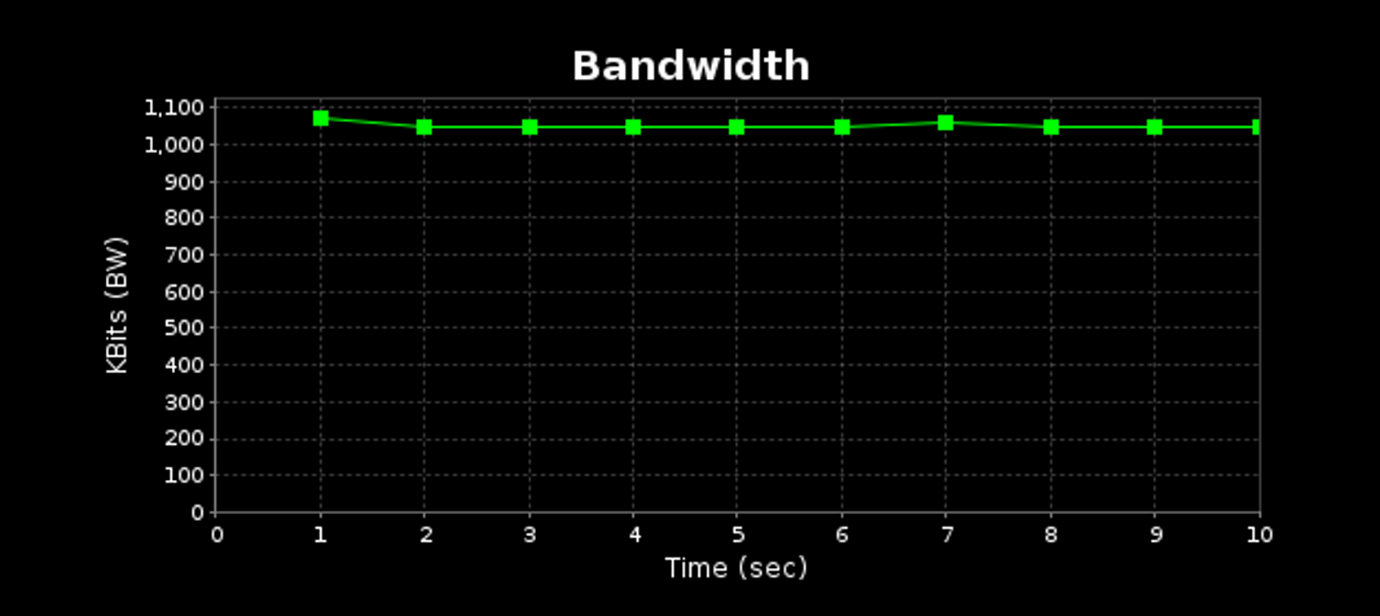
*Figure 18: Without DDoS, TCP*



*Figure 19: DDoS and TCP*



*Figure 20: Without DDoS, UDP*



*Figure 21: UDP with DDoS*