Cyberpaths

- Network Traffic & Denial of Service Lab -

Lab Goals

---

1. Getting used to work with GENI
2. Learn how to connect to your GENI nodes using PuTTY
3. Obtain an experiential perspective of a DDoS attack
4. Learn how to save network traffic logs in a pcap file to read with Wireshark
5. Use Wireshark to generate a graph from your network traffic logs

Prerequisites

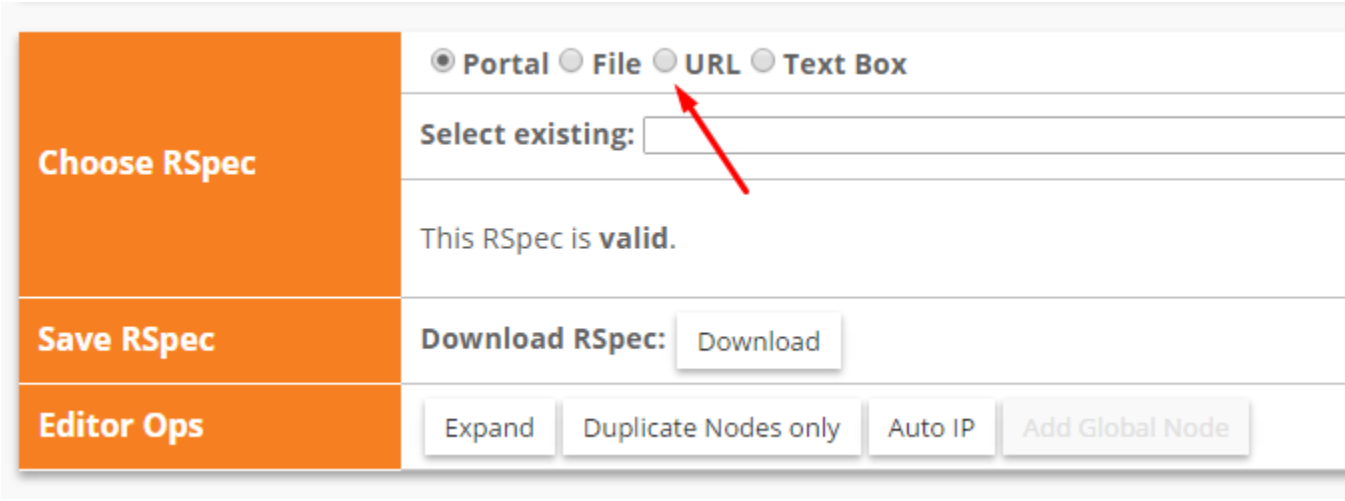
---

1. You will need basic command line knowledge to complete this lab. Codecademy has a great tutorial on this topic.
2. In this lab, you will implement a computer network attack, Denial of Service (DoS). This attack is designed to deprive services, such as web content, from legitimate users. From Wikipedia: "In computing, a denial-of-service attack is a cyber-attack where the perpetrator seeks to make a machine or network resource unavailable to its intended users by temporarily or indefinitely disrupting services of a host connected to the Internet." You can watch a video about this attack and read more about recent DDoS attacks using the Internet of Things interconnected devices.
3. To analyze the computer network traffic from this attack, we will use tool called Wireshark. Here is a quick video tutorial for this tool, or you can watch the video below, made by College of Charleston undergrad Thomas Setzler.
4. Iperf is a tool that is used through command line to generate computer network traffic that resembles regular usage of a computer network. You can read more about this tool here.
5. Hping3 is another computer networking tool that you will use. This tool, with the proper command line options, can generate a flood of computer network traffic that can overwhelm and take over networking resources. You can read more about this tool here.

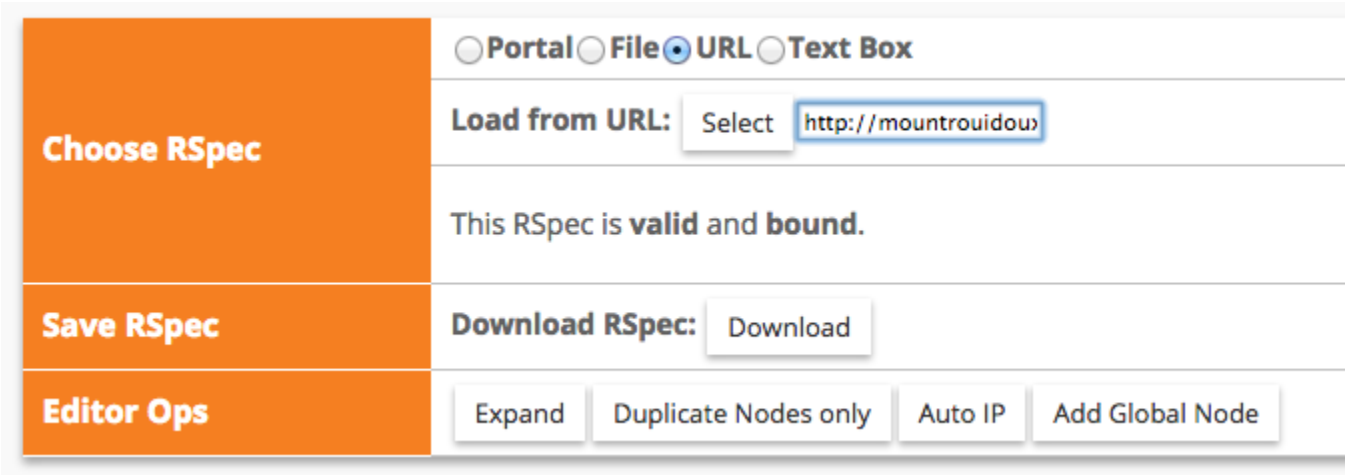
Setup

---

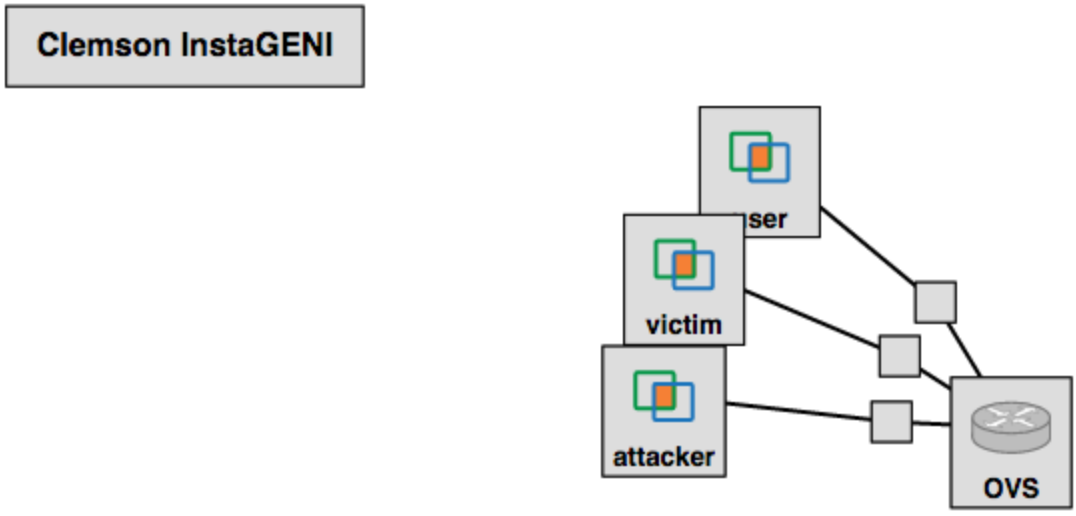
1. If your instructor has already provided you with a topology, you may move on to Part 1. Otherwise, complete the following instructions to set up your topology.
2. Create a new slice under the corresponding project
3. Click the "Add Resources" button located in the page of your newly created slice
4. Click the URL option



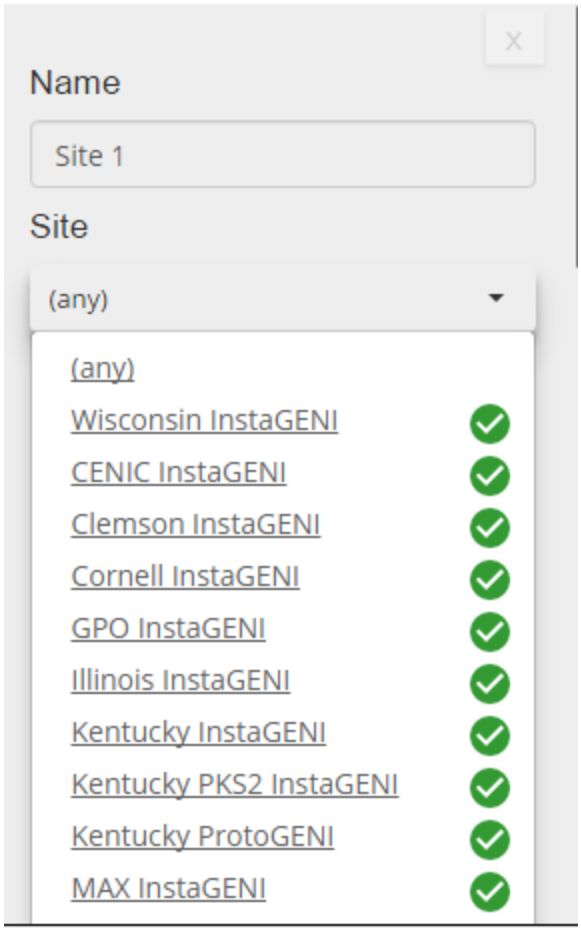
5. Paste on the input box the following link: **http://mountrouidoux.people.cofc.edu/CyberPaths/files/denialOfServiceLevel1.txt**
6. Then click on the "Select" button



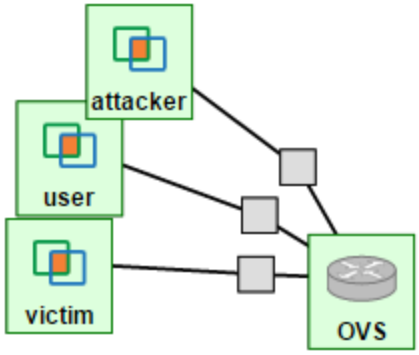
7. Your topology should now load and look like similar to this



8. Now click on "Clemson InstaGENI" and select one of aggregates on the left that is available and then reserve the resources



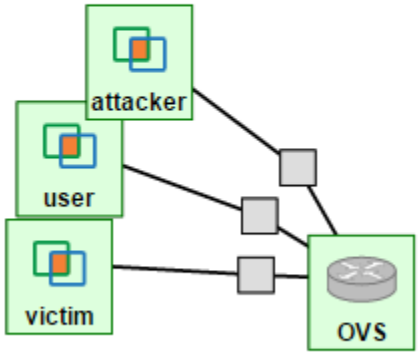
9. Then wait some time until all your resources are ready, you can check the status of these by going to the page of your slice. If the background color of a given node is grey, it means that such node is not available yet; if it is green, it means that it is ready. Just like so:



Part 1: Retrieving your computer network topology, describing it and understanding it.

---

1. Log into the GENI Portal using your login credentials. Go to "Home", "Slices", and click on the slice that corresponds to your lab. Describe the names of the machines that you see in the topology and how they are connected.
2. Based on the names on each machine that is in your topology, describe what you think each machine will do. (You will need to make an educated guess.)



3. The OVS in your topology is going to play the role of a network switch. Describe in your own words what you think a network switch is and how it works

Part 2: SSHing/Logging into your nodes.

---

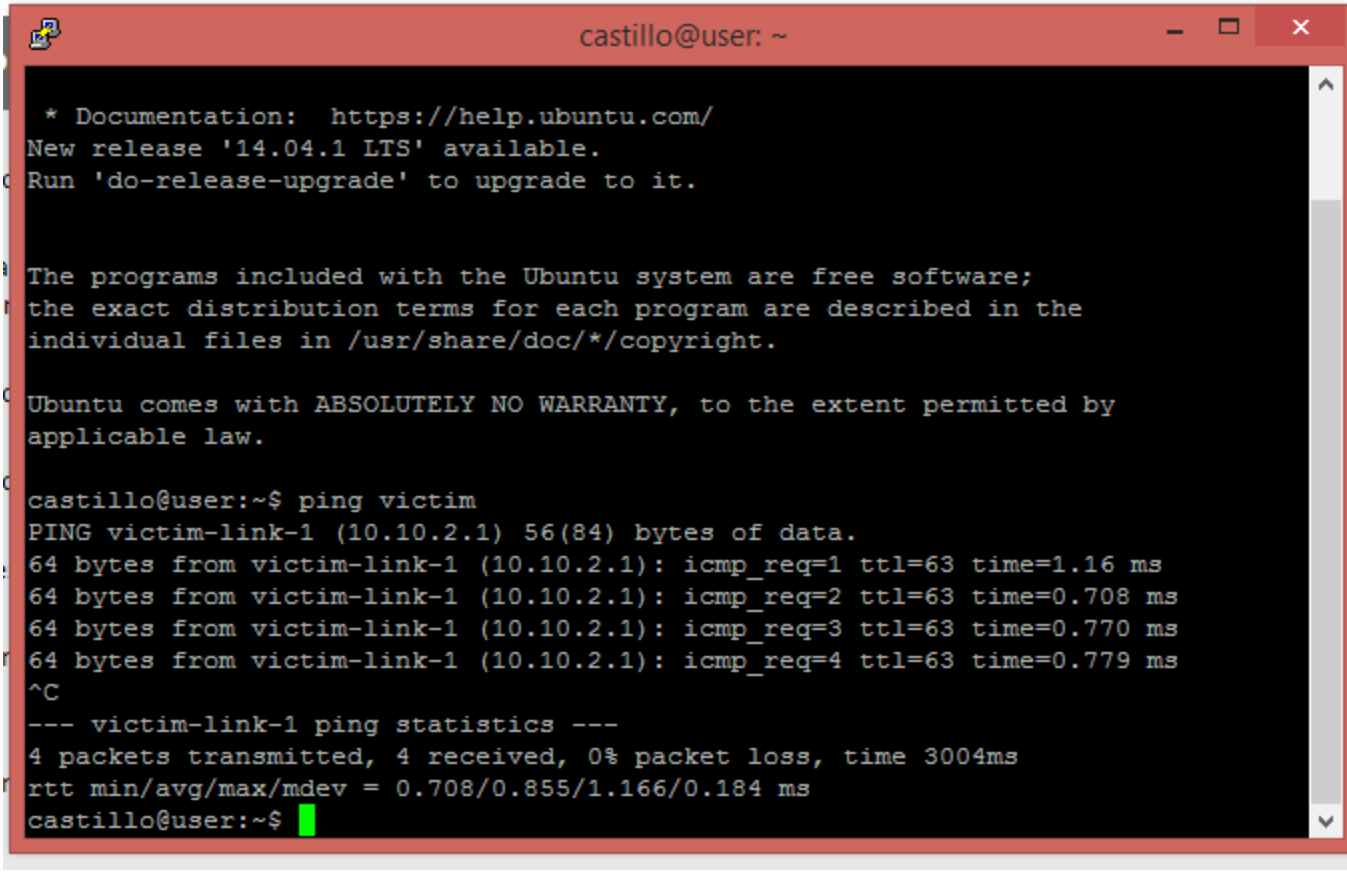
1. SSH stands for Secure Shell. SSH is a UNIX-based command interface and protocol for securely getting access to a remote computer. It is widely used by network administrators to control web servers and other kinds of servers remotely.
2. What is a network protocol and why do we need a protocol like SSH? (You may search for the answer but remember to include sources.)
3. Take a look at your topology. You should see four machines. These machines include "user", "victim", "attacker" and "OVS".

    - **"user"** machine: acts as a regular user on a network; like a user that browses the internet.
    - **"victim"** machine: acts as a victim of a Denial of Service (DoS) attack.
    - **"attacker"** machine: acts as a malicious user and creates and sends DoS attack to the victim.
4. On the GENI Portal, click on the machine in your topology called "user". You will need to open an SSH connection to this user node If you do not know how to do this, follow the "HelloGENI" tutorial for Windows users or Mac users.
5. Repeat the process and open ssh connection with all the nodes in your topology.

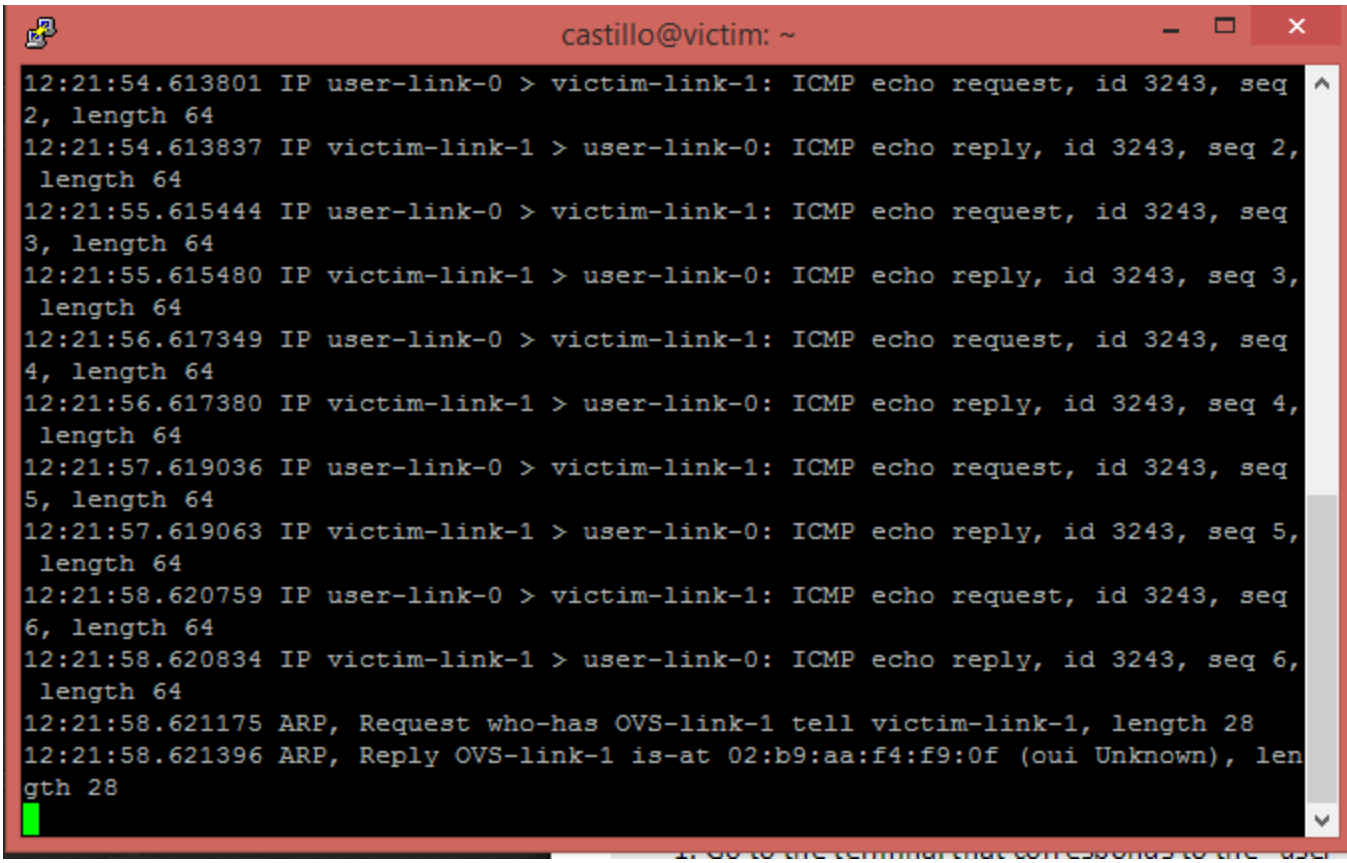
Part 3: Running your first experiment.

---

1. Go to the terminal that corresponds to the "user" machine. Type: ping victim and hit enter on your keyboard.



2. Press both the Ctrl key and C key together. This will cancel the ping command as we do not want this to run forever. Copy three lines that were printed on the terminal after you pressed enter.
3. Go to the terminal that corresponds to the "victim" machine. Type: `sudo tcpdump -i eth1` and hit enter on your keyboard.
4. Go to the terminal that corresponds to the "user" machine. Type: `ping victim` and hit enter on your keyboard.
5. After a few seconds, press both the Ctrl key and C key together on both terminals.

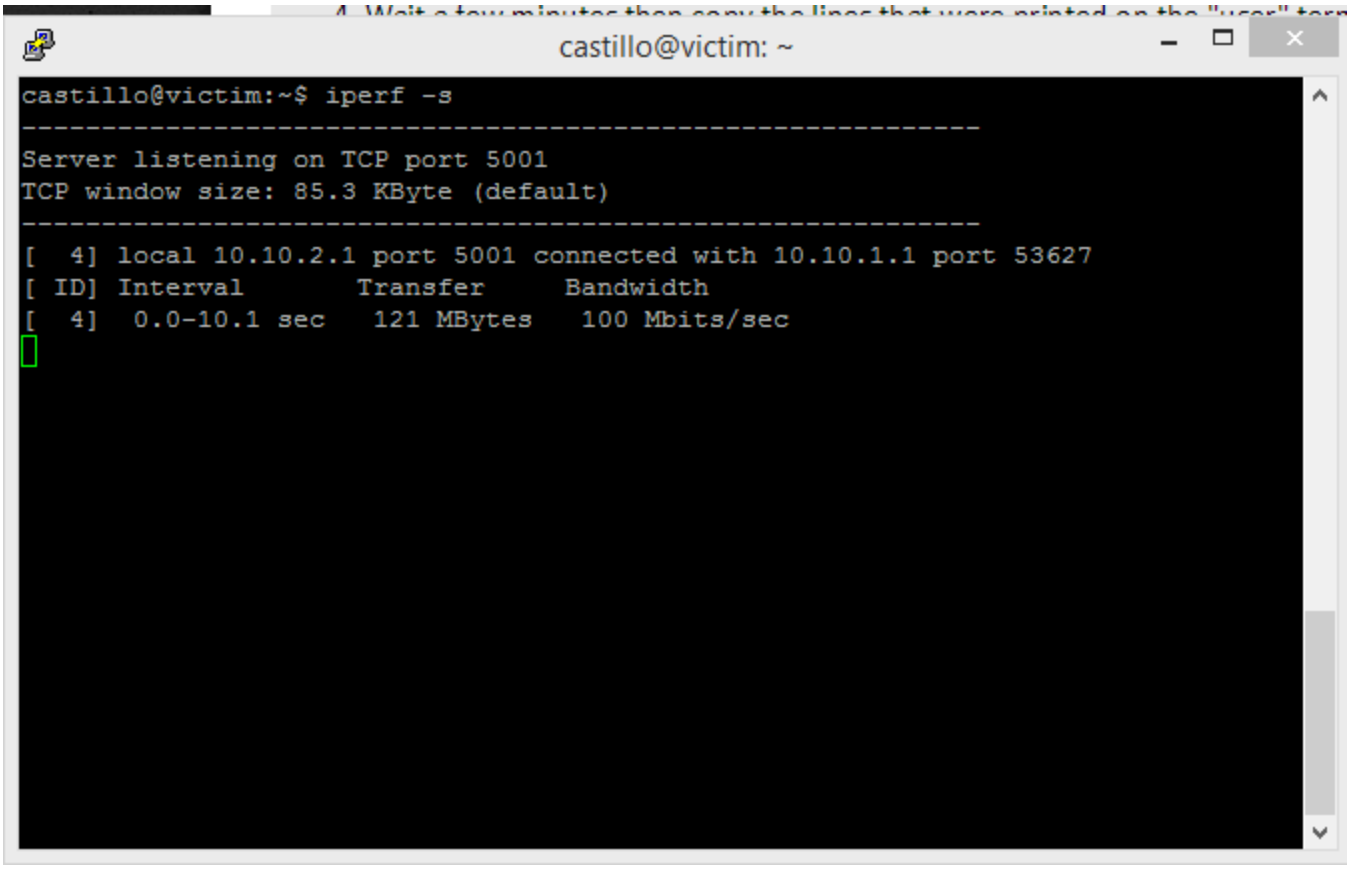


6. Take a look at the terminal that corresponds to the "victim" machine. Copy the lines that were printed on the "victim" terminal. Do you think these lines have any relation to the command entered on the "user" machine terminal?
7. Take a look at the terminal that corresponds to the "user" machine. Copy the lines that were printed on the "user" terminal. What time units are used in the ping statistics?
8. What is RTT? (You may search the abbreviation but include sources.)
9. Do the ping statistics from 7 indicate a fast or slow network? (You may search network speeds for comparison but include sources.)
10. ***The ping command is a query, or a question, to another computer on a network. In this case the question is sent from the "user" machine to the "victim" machine to determine whether there is a connection.***

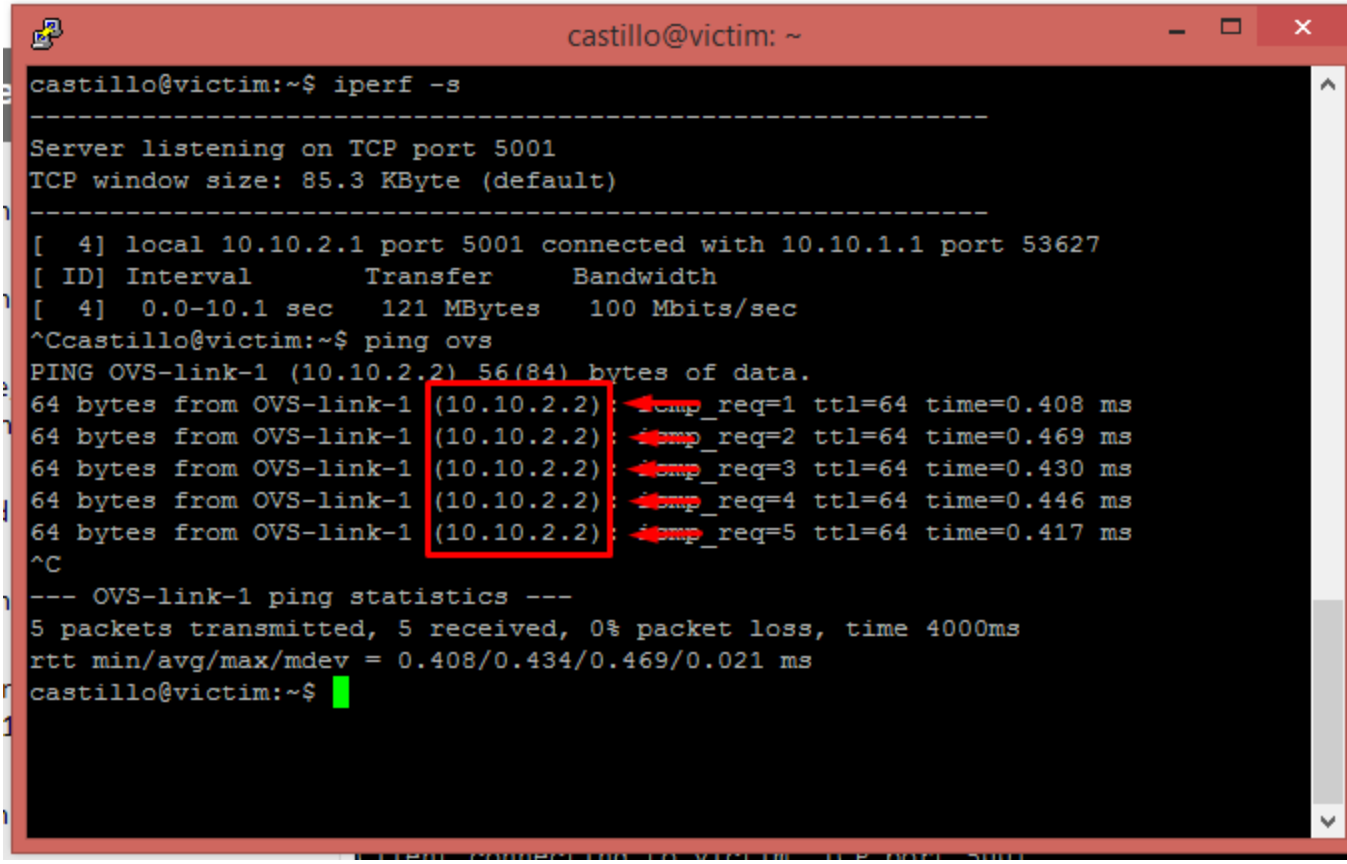
Part 4: Running an attack, observing user traffic, collecting and analyzing data.

---

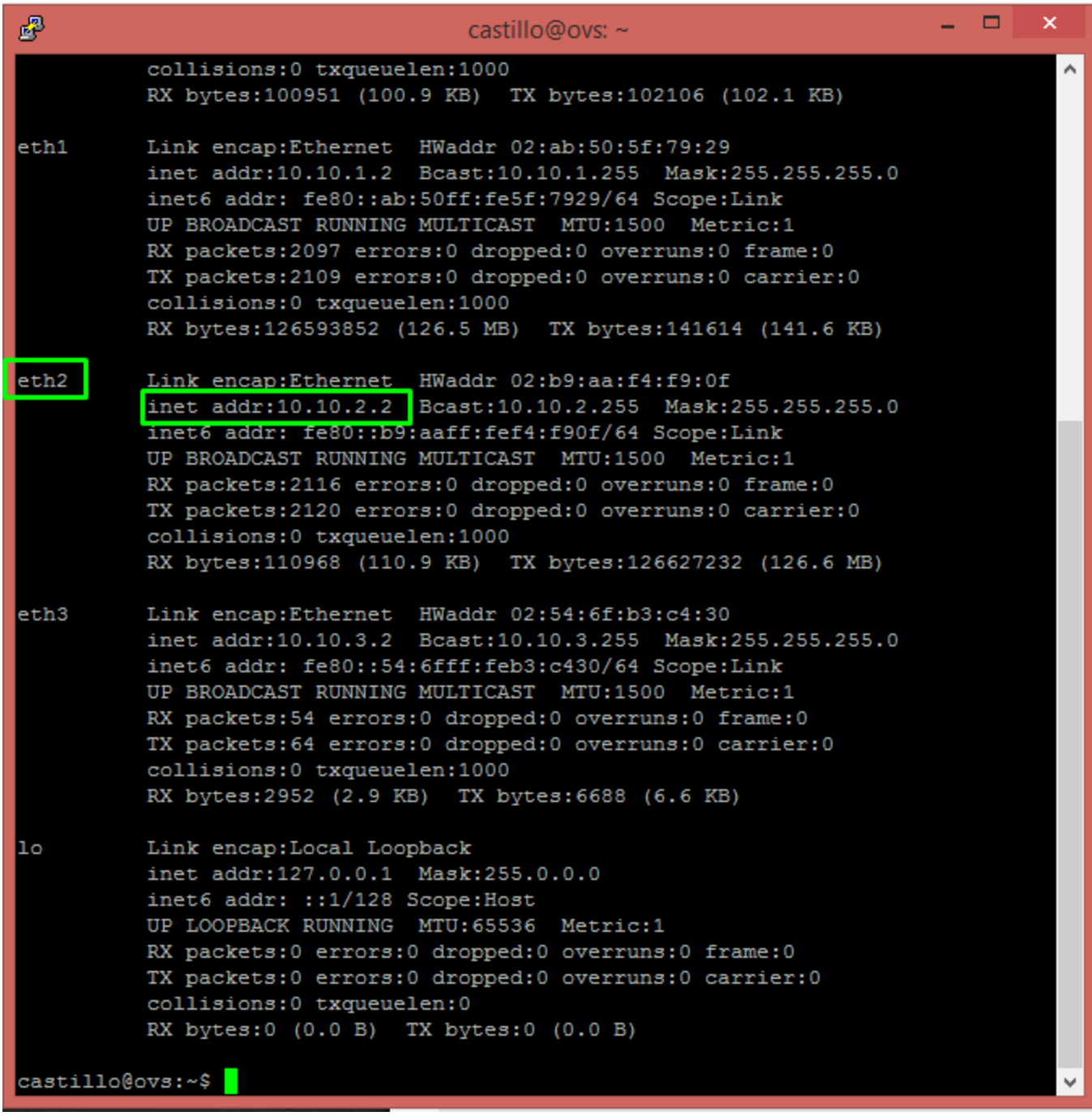
1. Go to the terminal that corresponds to the "victim" machine. Type: `iperf -s` and hit enter on your keyboard.
2. Go to the terminal that corresponds to the "user" machine. Type: `iperf -c victim` and hit enter on your keyboard.



3. Iperf is software that tests the performance of a machine; how fast it serves network requests. The "victim" machine is running a server and the "user" machine is running a client with requests to the server on the "victim" machine.
4. Wait a few minutes then copy the lines that were printed on the "user" terminal.
5. Go to the terminal that corresponds to the "victim" machine and press both the Ctrl key and C key together.
6. Type: `ping ovs` and hit enter on your keyboard. Note the numbers and periods inside the parenthesis. There should be 4 numbers separated by 3 periods. For example, inside the parenthesis for me contains "10.10.2.2".

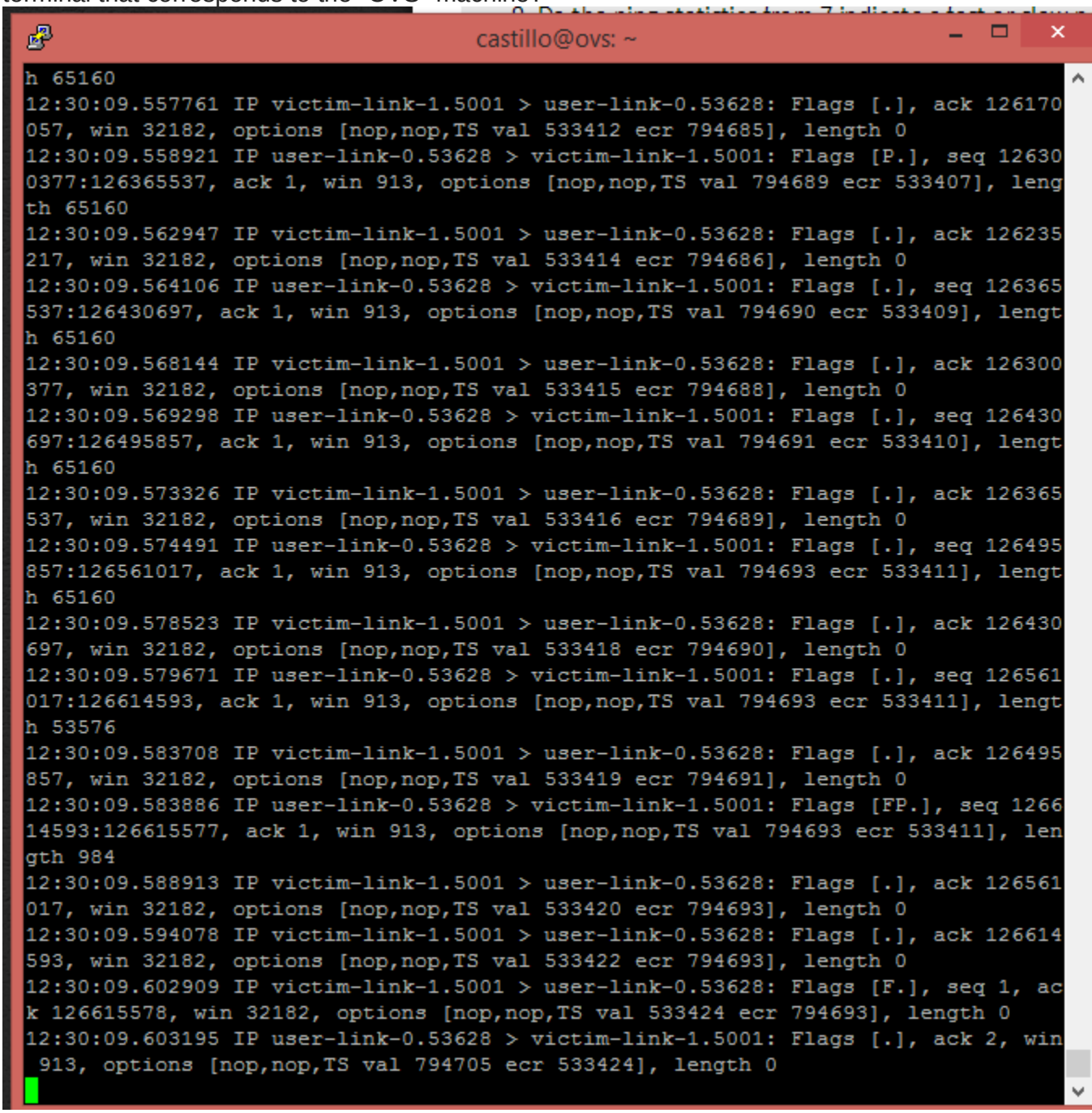


7. Go to the terminal that corresponds to the "OVS" machine. Type: `ifconfig` and hit enter.
8. Find the corresponding numbers from above in step 5 and remember the specific "eth" it is paired with. For example, after running ifconfig, I am looking for 10.10.2.2 and I see that it is located beside "eth2". The "eth" you see on your screen that corresponds to your specific number is what you will type. For example, I would use eth2. I would type: `sudo tcpdump -i eth2 -vv` and hit enter.



9. Complete step 1 - 2 for a few seconds. What do you observe on the "OVS" machine? Where does this traffic come from?
10. Go to the terminal that corresponds to the "attacker" machine. Type: `sudo apt-get update` and hit enter on your keyboard. This command updates all the repositories in your machine and prepares it to install another tool. Then typle `sudo apt-get install hping3` and hit enter on your keyboard. This command installs the tool "hping3". Finally, type: `sudo hping3 -S --flood victim` and hit enter on your keyboard. After a few seconds, press both the Ctrl key and C key together. What is happening in the

terminal that corresponds to the "OVS" machine?



11. Does the traffic generated from the "attacker" machine look like it goes through at a faster pace than the traffic that you generated in task 3?
    - The first part of the commands above, "sudo", makes you a root user. You are now the privileged user that is allowed to run anything you want on the machine.
    - The "tcpdump" command, calls a program that monitors the network traffic that is entering the “victim” machine. The ending part of the "tcpdump" command is the network interface that is being monitored.
    - The "hping3" command was used to run a flooding attack towards the "victim" machine. This attack is called a Denial of Service (DoS) attack and is designed to bring the network down by sending it useless traffic.

Part 5: Collecting Data from GENI machines.

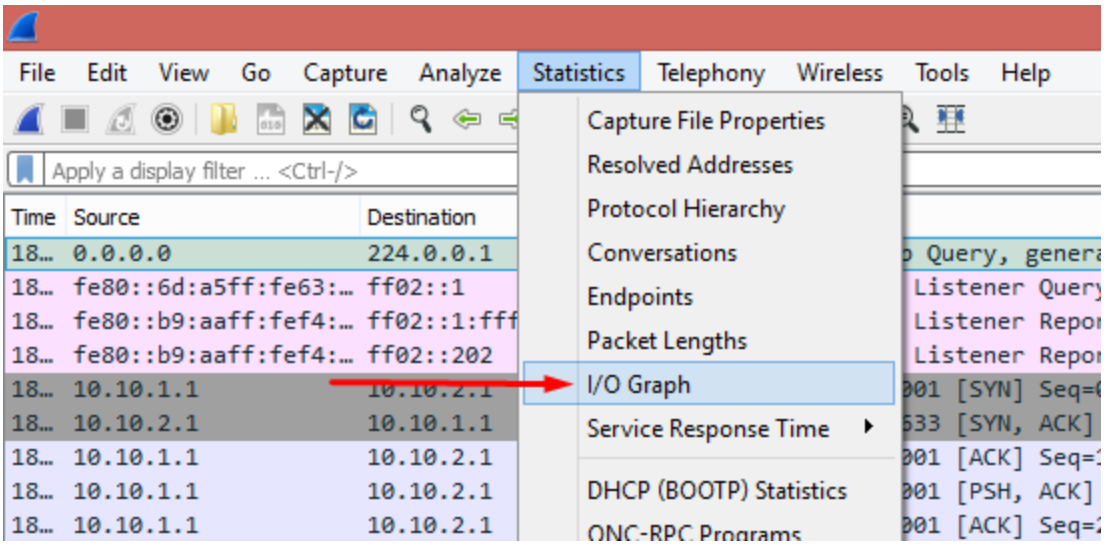
---

1. We will now collect normal traffic and DoS traffic data and compare them. First, go to the terminal that corresponds to the "OVS" machine and press both the Ctrl key and C key together. Now in the "OVS" machine terminal, Type: `sudo tcpdump -i eth1 -s0 -w capture1.pcap` (where eth1 corresponds to the same "eth" you used in Task 4, Step 8) and hit enter on your keyboard. This command takes the tcpdump monitored traffic and writes it in a file called capture1.pcap.
2. Go to the terminal that corresponds to the "victim" machine and press both the Ctrl key and C key together. Now in the "victim" machine terminal, Type: `iperf -s` and hit enter on your keyboard. When you use `iperf -s` you are running an iperf server. Next you will run and iperf client on the “user” machine and generate some regular traffic
3. Go to the terminal that corresponds to the "user" machine. Type: `iperf -c victim` and hit enter on your keyboard.
4. Go to the terminal that corresponds to the "attacker" machine. Type: `sudo hping3 -S --flood victim` and hit enter on your keyboard. After 10 seconds, press both the Ctrl key and C key together on all your terminal windows.
5. Now we will analyze the information gathered after generating an attack.
    - If you are a windows user, drag and drop the capture file from your "OVS" machine to your computer using WinSCP. You can find instructions on how to install and use WinSCP in the embedded link.
    - If you are a Mac or Linux user, you may use sftp to transfer your files. Open a terminal on your local machine (Mac or Linux). You can find instructions on how to install and use SFTP in the embedded link.

Part 6: Analyzing the data.

---

1. Use Wireshark to view the statistics of your capture file. Write all the traffic statistics here.



2. Describe the I/O graph that is generated by your capture file. This is the graph of the traffic you ran in the previous task. Do you see at which time you started the flooding attack? Why is it very distinctive? Copy the graph.
3. Did the attack end at some point? What do you think happened at this point? (Refer back to Wireshark Installation & Usage Guide from Lab 0 if you need instruction on how to view the statistics and I/O graph of your capture file.)

Part 7: Repeatable experiments.

---

1. Repeat the experiments from task 3 at least four more times. You will need to change the name of the capture everytime (capture1.pcap, capture2.pcap, capture3.pcap, capture4.pcap, capture5.pcap).
2. Take the statistics of packet size and bandwidth from Wireshark from each pcap file and put these in an Excel spreadsheet. Calculate the average and standard deviation of this data and plot the data. Describe your observations of this data.