CSE 232: Assignment 2

Due date: September 24, 2021

Read the following instructions carefully

- For all the observations and explanations create a single report.
- Attach screenshots in the report.
- Naming Convention: <Roll_No>-Assignment2.zip

Q1.[2+2+1] Run your client server socket program for 2 minutes, collect the packet trace using wireshark/tcpdump at the server side. Filter the packets that belong to the client server socket program. Analyze the packet capture, compute aggregate throughput for every 2 sec and plot it with time.

Q2. [2+2] Use your web browser to retrieve the http://info.cern.ch web page. While retrieving the web page, use wireshark/tshark/tcpdump at your machine to capture the communication between your machine and the web server. You may need to filter the required packets. Put the screenshot of HTTP request and response messages. Explain the following details for each captured packet.

- HTTP packet type
- For HTTP request packets
    - HTTP request type
    - User agent type
    - HTTP request packet's URL
    - Name and version of the web server
- For HTTP response packets
    - HTTP response code
    - HTTP response description

Q3. [1 +2]

a) Learn to use the ifconfig command, and figure out the IP address of your network interface. Put a screenshot.

b) Go to the webpage https://www.whatismyip.com and find out what IP is shown for your machine. Are they identical or different? Why?

Q4. [[1 +1] + 1]

a) Write and explain the command to test whether you can send a single packet with mtu 3000 to 'www.iiitd.ac.in'. If the test failed, what could be some of the reasons that it didn't work? (Assume client, server and all intermediate nodes are up).

b) Write the command to display all active tcp connections with pids

Q5. nslookup [[2+1] + [2 +1]]

a) Get an authoritative result in nslookup. Put a screenshot. Explain how you did it.

b) Find out time to live for any website on the local dns. Put a screenshot. Explain in words (with unit) that after how much time this entry would expire.

Q6. Run the command, *traceroute www.iiith.ac.in*

a) How many intermediate hosts do you see, what are the IP addresses, compute the average latency to each intermediate host. Put a screenshot. [2+2]

Note that some of the intermediate hosts might not be visible, their IP addresses will come as "", ignore those hosts for this assignment.***

b) Send 100 ping messages to iiith.ac.in, Determine the average latency. Put a screenshot.[2]

c) Add up the ping latency of all the intermediate hosts and compare with (b). Are they matching, explain?[1+1]

d) Take the maximum of ping latency amongst the intermediate hosts and compare with (b). Are they matching? Explain. [1+1]

e) Perform reverse DNS lookup of each intermediate host. List the host name and aliases (if any) for each intermediate host. [4]

Q7. [2+1] Make your ping command fail for 127.0.0.1 (with 100% packet loss). Explain how you do it. Put a screenshot that it failed.