CSE 232: Assignment 1

Due date: September 23, 2022

Read the following instructions carefully

- For all the observations and explanations create a single report.
- Attach screenshots in the report.
- Naming Convention: <Roll_No>-Assignment1.zip

Q1. [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?

Q2. 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.

Q3. Run the command, *traceroute google.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 google.in, Determine the average latency. Put a screenshot.[2]

c) Send 100 ping messages to columbia.edu, Determine the average latency. Put a screenshot.[2]

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

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

f) Traceroute columbia.edu. Compare the number of hops between google.in and columbia.edu (between the traceroute result of google.in and columbia.edu). Can you explain the reason for the latency difference between google.in and columbia.edu? [1+1]

Q4. [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.

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

- For HTTP request packets
    - HTTP request type
    - User agent type
    - HTTP request packet's URL
- For HTTP response packets
    - HTTP response code
    - HTTP response description
    - Name and version of the web server
- How many web objects get downloaded? Were they over the same TCP connection or different connections?
- From this tell if it is HTTP persistent or non-persistent?

Q6. [1+1] Note: perform this test after Q5

a) Write the command to display all active tcp connections with pids
b) Determine the state of the TCP connection(s) to this server http://info.cern.ch