COMP2190 – Semester 1 2024/2025

Assignment 0

Assigned: Sep. 16, 2024
Due: Sep. 23, 2024

This assignment will involve you exploring the tools that are available to users for exploring what is occurring on a network. You can probably complete the exercises from within a Linux distribution running on a virtualization manager, e.g., VirtualBox. However, I have not tested this configuration. Note, that while Windows 10 and 11 now have support for a bash shell, some of the networking functionality in that shell is still broken, thus you may not be able to complete the exercises under Windows. Include a printout of your commands. After running each command also run the date command before taking the screenshot. This will be proof that you actually ran the command in question. Make friends with the *man* pages. In this homework you will look at the following tools:

Problems

1. ifconfig [3]
    a. What is ifconfig used for? No more than two succinct sentences will do.
    b. Use ifconfig to show your IP address.
2. traceroute [4]
    a. What is traceroute used for?
    b. Perform a traceroute to scanme.nmap.org. Compute the number of hops, and the mean and standard deviation of the response times. By default, traceroute only gives you 3 readings, but I suggest you collect 6 readings to compute more meaningful results. Include a printout of your readings.
3. ping [7]
    a. What is ping used for?
    b. Use ping to obtain the mean and standard deviation of the delay between your machine and scanme.nmap.org. Use 10 readings to get meaningful results. Include a printout of your readings.
    c. Use ping to determine the largest packet size between your host and scanme.nmap.org. Try packet sizes of 528 and 1492 bytes.
4. netstat [7]
    a. What is netstat used for? One sentence will do.
    b. Use netstat to show all the IPv4 TCP connections on your machine. Include a printout. How do these correspond to the applications that you have running on your machine? Are there more connections than applications? If so, what is the theoretical maximum number of connections between your host and another host?
    c. Use netstat to show your host's routing table. Include a printout. Can you identify your host's default route from the output? If your computer has a packet destined for a

destination address that it cannot recognize what will your computer do with that packet?

5. whois [3]
    a. What is whois used for?
    b. Suppose that I get a lot of spam from Outlook.com users. I would like to complain to Microsoft. Use whois to determine the administrative contact for outlook.com.
6. dig [9]
    a. What is dig used for?
    b. What is the IP address of xray.uwimona.edu?
    c. Suppose that the outlook.com sysadmin replies to my complaint about Outlook spam. What mailserver will they use? Assume the response is coming from the e-mail address that you found using whois, and that the sysadmin is using the default mailserver. If there is more than one possible answer to this question, just give one.
    d. Use dig to demonstrate the difference between recursive and iterative DNS queries by looking up ns1.mona.uwi.edu.
7. arp [4]
    a. What is arp used for? One sentence will suffice.
    b. Print out the current arp table on your computer. Next, get the IP address of a device that is on the same local area network as yours (You can do this by finding the IP address of a classmate who is on MonaConnect at the same time as you). Ping this device a few times. Next, print out your arp table again. What do you notice?
8. nmap [3]
    a. What is nmap used for?
    b. Run nmap against scanme.nmap.org and include a printout of your results.
9. md5sum [5]
    a. What is md5sum used for?
    b. Check the md5 message digest against the signature posted on VLE. [To do this you will need to download both the signature and this file to the same directory. Save this file as Lab0.pdf.] What does the result of the check indicate to you?
10. Measure the “speed” of Internet connections [7]
    a. Use http://www.speedtest.net/ to measure the upload and download speeds from your home somewhere between 8 and 4:30 PM on a weekday, i.e., Monday to Friday. In your answer include what kind of service you are using—cable modem, DSL, mobile data—and the day and time of the measurement.
    b. Use http://www.speedtest.net/ to measure the upload and download speeds from your home sometime between 6 PM and 10 PM or at any time during the weekend. In your answer include what kind of service you are using—cable modem, DSL, mobile data—and the day and time of the measurement.
    c. Explain the differences between the results from parts a) & b).

Acknowledgement

Questions 1–6 in this homework are based on problems originally developed by Dr. Tristan Henderson for COSC78 at Dartmouth College. Question 10 is based on a problem developed by Prof. Victor Frost for EECS563 at the University of Kansas.

Posted: 2024-09-07