Lab 4 TCPDump

Description: In this lab, you will review the man page of TCPDump and perform a packet capture.

Requirement: You will need access to the Cybrary lab environment to complete this lab.

Step 1: Log into the Cybrary website

Step 2: In the search box, search for " **TCPDump** "

Step 3: Click the Launch button

Note: You may receive a message that the lab needs to be launched in a separate window. If you receive this message, please click the "Launch Item" button to launch the lab. It may take 1-2 minutes to launch the lab.

Step 4: You will then see a pop-up box. Select the Next button, then Ok to close the pop-up box.

Step 5: Next, open a Terminal window by click the black-colored box on the left-side menu.

Step 6: At the Terminal prompt, type the following and press Enter.

cd /home/student/Desktop/captures

Step 7: Next, let's look at the manual for TCPDump.

Step 8: Type the following command and press Enter.

man tcpdump

Step 9: Look through the different options available.

Step 10: Press the **q** button on your keyboard to go back to the Terminal prompt.

Step 11: Next, type the following command at the prompt and press Enter. This will show the interfaces available.

sudo tcpdump -D –list-interfaces

Step 12: You will be prompted for a password. Enter the word **student** and press Enter.

Question 1: What interfaces are listed?

_____

Step 13: Next, type the following command and press Enter.

sudo tcpdump -i eth0

Step 14: This will start TCPDump in the Terminal window.

Step 15: Open a new Terminal window by right-clicking on the black-colored box on the left-side menu.

Step 16: In the new Terminal window, type the following and press Enter.

ping 10.0.10.11

Question 2: Do you see the IP address now in the original Terminal window?

_____

Step 17: Press Ctrl+C to stop the ping command for 10.0.10.11

Step 18: Next, type this command and press Enter.

ping 10.0.10.12

Step 19: Next, press Ctrl+C in the newer Terminal window to stop the ping scan.

Step 20: Press Ctrl+C in the original Terminal window to stop TCPDump.

Question 3: How many packets were captured?

_____