Lab 1 Wireshark

Description: In this lab, you will use the Wireshark application to analyze captured network traffic. Specifically, your goal is to find any usernames and passwords.

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 Wireshark and click on the Wireshark lab by CyberScore.

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: You should see the Ubuntu desktop.

Step 6: Launch a Terminal window by clicking the black-colored icon on the left-side menu.

Step 7: Enter this command at the prompt and press Enter.

sudo wireshark

Step 8: You will be prompted for a password. Enter this password and press Enter.

student

Step 9: Next, you may see a “Lua: Error during loading” error message. Just click the OK button to close the pop-up.

Step 10: The Wireshark application should launch.

Step 11: Click **Capture** at the top of the screen, then **Options** .

Note: You can also just hold down Ctrl and then press the K button on your keyboard to launch the window.

Step 12: A new pop-up box will open

Step 13: Check the box to the left of the **eth0** interface option in the top box.

Step 14: Make sure the “ **Use promiscuous mode on all interfaces** ” checkbox is marked.

Step 15: Make sure the Capture Filter box is empty.

Step 16: Under the “Display Options” at the bottom-right, make sure all of the boxes are checked (they should be by default).

Step 17: Under the “Name Resolution” at the bottom-right of the window, uncheck all of the boxes.

Step 18: Next, click the Start button.

Step 19: We will now open a new Terminal window.

Step 20: Right-click on the Terminal icon and select the New Terminal option.

Step 21: Next, we are going to generate some traffic for Wireshark to capture.

Step 22: In the new Terminal window, type the following at the prompt and press Enter.

```
ping 10.0.10.12
```

Step 23: You will now see traffic being captured by the Wireshark application.

Step 24: Let the capture run for 10-20 seconds and then press Ctrl+C on your keyboard to stop the ping command.

Step 25: Type the following command at the prompt and press Enter.

```
wget 10.0.10.12
```

Note: This command allows us to interact with HTTP servers. On the server, there is a program listening for traffic on port 444. We will use the netcat utility to start interaction with that port.

Step 26: Type this at the Terminal prompt and press Enter.

```
nc 10.0.10.12 444
```

Step 27: In the Terminal window, type cat and press Enter.

Step 28: Next, type dog and press Enter.

Step 29: Next, type bird and press Enter.

Step 30: In Wireshark, you should see the packets containing data being highlighted.

Step 31: Right-click on the packet and select " **Follow TCP Stream** "

Question 1: Do you see the words you typed in?

____

Step 32: Click the close button to close the “Follow TCP Stream” window.

Step 33: Click back in the Terminal window and press Ctrl+C to stop netcat.

Step 34: Next, stop the traffic capture in Wireshark by clicking the red-colored square button at the top of the application.

Step 35: Next, click on a TCP packet that has an ACK flag showing.

Question 2: What is the source and destination IP address for the packet you have chosen?

____

Step 36: Next, we will open a packet capture file and analyze it.

Step 37: Click **File** at the top-left of the Wireshark application, then click **Open** .

Step 38: Click the “ **Continue without Saving** ” option in the pop-up message.

Step 39: Next, click Desktop at the pop-up box that opens.

Step 40: Double-click on the **captures** folder

Step 41: Double-click on the **capture2.pcap** file

Step 42: Select **Go** at the top of the screen and then choose **Go to Packet** .

Note: We’re looking for packet 2286.

Step 43: Type **2286** in the pop-up box and then click the “ **Jump to** ” button.

Question 3: What is the source IP address for the packet?

____

Question 4: What is the source port number?

____

Question 5: What is the destination IP address for the packet?

____

Question 6: What is the destination port number?

____

Step 44: Next, right-click on the 2286 packet and select the “Follow TCP Stream” option.

Question 7: What information do you see?

____