Lab 3 Applying Filters to TCPDump and Wireshark

Description: In this lab, you will practice applying filters to TCPDump and Wireshark for packet analysis.

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

Part 1: TCPDump

Step 1: Log into the Cybrary website

Step 2: In the search box, search for " **Applying Filters to TCPDump and Wireshark** "

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 will then be taken to the Ubuntu Linux desktop.

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

Step 7: Next, type the following command in the Terminal and press Enter.

cd /home/student/Desktop/captures

Step 8: Next, we are going to read one of the captured files.

Step 9: Type the following command at the prompt and press Enter.

tcpdump -n -xx tcp -r "Lab 2.2.3-3.pcap" | less

Question 1: What port numbers do you see in the output?

_____

Question 2: What IP addresses are listed?

_____

Step 10: Next, press the **q** on your keyboard to back out of the file.

Step 11: Next, we will filter the information in the file to only include HTTP information.

Step 12: Type the following command at the prompt and press Enter.

tcpdump -n -xx tcp port 80 -r "Lab 2.2.3-3.pcap" | less

Question 3: What port numbers do you see in the output now?

_____

Question 4: What Web server IP address do you see?

_____

Step 13: Next, press the **q** on your keyboard to back out of the file.

Step 14: We're going to now just look at the packet capture for the Web server address.

Step 15: Type this command at the prompt and press Enter.

tcpdump -n -xx host 172.16.20.24 and tcp port 80 -r "Lab 2.2.3-3.pcap" | less

Question 5: Do you just see inbound traffic?

_____

Part 2: Wireshark

Step 1: Click on the blue-colored Wireshark icon on the left menu.

Step 2: Once Wireshark launches, click File, then Open

Step 3: A new window will open.

Step 4: Click Desktop on the left-side

Step 5: Double-click the captures folder

Step 6: Click on the **Lab 2.2.3-3.pcap** file and then click the Open button

Step 7: Expand the view

Step 8: In the Filter box at the top, type the following command and then either press the Enter key or click the Apply button.

ip.dst_host contains "172.16" and http

Question 1: Has the protocol column changed with the filter?

_____

Question 2: Do any of the IP addresses listed look familiar to you?

_____

Step 9: Next, we're going to export an HTML object.

Step 10: Select File, then Export Objects, then HTTP

Step 11: A new window will open.

Step 12: Click on packet number **50** , then click the Save As button

Step 13: Name the file **http_object_one** and save it to the Desktop

Step 14: Minimize the Wireshark window

Step 15: Double-click the http_object_one file to review the contents.

Step 16: Next, close the file and click back on the Wireshark icon.

Step 17: Click the Clear button at the top of the Wireshark window to clear the filter.

Step 18: Next, type **ftp** in the Filter box and click Apply.

Step 19: Right-click on packet **28** .

Step 20: Select Follow TCP Stream

Question 3: What information do you see?

_____

Step 21: Click Save As and name the file **ftp_traffic.txt** , navigate to the Desktop, and click the Save button

Step 22: Click the Close button

Step 23: Next, click the Clear button at the top to clear out the filter.

Step 24: Type **telnet** in the Filter box and select Apply

Step 25: Scroll down until you find packet 880

Step 26: Right-click on packet **880** and select Follow TCP Stream

Question 4: Do you see any password information?

_____

Step 27: Next, click the Save As button

Step 28: Name the file telnet_traffic.txt and save it to the Desktop

Step 29: Click the Close button

Step 30: Click the Clear button at the top to clear the telnet filter.

Step 31: Let's take a look at traffic that is not related to TCP

Step 32: In the Filter box, type the following and select the Apply option.

!tcp

Question 5: What protocols do you see?

_____