**CIS 2640 – Lab 17**

**Capturing Network Traffic**

| **Your Name:** | Liliane Owens |
| --- | --- |
| **Date:** | 3/19/23 |

**Instructions**: Complete the tasks described in this worksheet. Read the instructions carefully and submit evidence of your completed tasks (a screen shot is your evidence). Answer the questions below in the space provided.

* **Showing Evidence of Completion:** Your evidence of completion is a screen shot, as described in each exercise. Use the tool of your choice to take a screen shot of the required content. ***Screen shots should be pasted at the end of this document.***
* **Answering Questions:** Your answers should be written in carefully edited college-level English, using complete sentences.

| **Lab – Capturing Network Traffic** | |
| --- | --- |
| **Instructions and Evidence of Completion** | **Answer a Question** |
| At the end of this document (not within this table) paste screen captures that show the following:   1. Using Wireshark to view the netcapture1.pcap file 2. Output from the urlsnarf command with spoofed MAC addresses 3. The Wireshark capture showing ftp credentials displayed in cleartext.   You should include three screen shots that show both the command and the output of the command.  ***Be sure your screen shot(s) include any command executed and the resulting output in clear / cropped screenshots.*** | Question(s): Answer each of the questions below; use the space to the right of each question for your answer. Make sure your answers are clear and complete. |
| ***Questions*** | ***Answers*** |
| 1. Explain why a network interface that has promiscuous mode turned off would prevent a sniffer running on the host from capturing all network traffic. | The network interface that has promiscuous mode turned off would prevent the sniffer capturing the whole network traffic because the promiscuous mode in a network allows the network to intercept all messages that comes through the network and read them all to the network. So, if there would be a sniffer in the network then it would be very easily to read all messages that goes through the network. To prevent it when we turn off this mode then the network would still receive all the messages, but it would not read the message to the network to determine if the message belongs to that network address or not. As if we turn off the mode , all the packages that will be intercepted would be first checked or determined if the network address attached to the packet is similar to the network it arrived or not and if and only if it matches then the network can read it otherwise not. So, it prevents the sniffer to read all the data packets intercepted by the network as is done by promiscuous mode. |
| 1. Does a network interface on a sniffer machine require an IP address? | Sniffer doesn’t require Internet Protocol (IP) address because it is hidden to other computers and sniffer wants to intercept message from the computer without any interference by other computers. |
| 1. In what mode does a sniffer’s network interface operate? | Promiscuous mode. |
| 1. How do you determine available switches (options) for tcpdump? | The command tcpdump used to display available switches. |
| 1. What command would you issue to display all of the network interfaces in Linux? | ifconfig . |
| 1. Do FTP usernames and passwords appear in clear text? | Yes, they do appear in clear text because FTP does not encrypt its data and control connections. |
| 1. How do you choose the interface to capture on within Wireshark? | You can select an interface in the welcome screen, then select Capture-> Start or click the top menu option Capture -> Interfaces. |
| 1. How do you filter for a certain protocol within the Wireshark program? | Go to filter bar on top, there is a box you can type, for example tcp. |
| 1. What command would you use to open the Wireshark program from the terminal in Linux? | Simply type wireshark into the root@bt bar. |

Put Screenshots here:

1. Using Wireshark to view the netcapture1.pcap file

![Graphical user interface, text, application

Description automatically generated]()

1. Output from the urlsnarf command with spoofed MAC addresses

![Text

Description automatically generated]()

1. The Wireshark capture showing ftp credentials displayed in cleartext.

