

CS470

Computer Security

Laboratory Project Due Date:

Packet Capture

The objective of this project is to understand the methods of packet capturing over a network using an open source packet capture program such as Wireshark or Snort. Network packet capturing is used by both legitimate users and illegitimate (hackers) users of the system to gather system activity information. You are required to capture raw packets that are moved in and out of the network interface card on a system and to perform a thorough analysis of the packets.

Your mission is to capture packets, using Wireshark, at some specified time interval, to save the captured packet information in a file, to analyze the packets, and to answer activity-related questions to the best of your ability. Your final report should consist of a description of all the steps that you have taken and the tools that you have used to successfully complete the mission. In addition, you need to include, in your report, a detailed answer to each of the following questions.

- 1) Describe the main fields in a typical output of a Wireshark capture.
- 2) What is (are) the service(s) used by the client in connecting to your system?
- 3) What is (are) the password(s) used by the client?
- 4) What is the client's IP address and MAC address?
- 5) What is (are) the tool(s) used by the client in scanning your system?
- 6) What are the five scanning methods that were used by the client system?
- 7) What are the ports found open in your system?
- 8) What operating system is used by the client system?