Comp 4985 - Lab #2

Packet analysis using *tcpdump*

Due Date: March 25, 2009.

Work in groups of **two**.

Objective: To analyze traffic using **tcpdump** filters.

Your Mission:

You are required to install and set up **Telnet** services on your server. Design a tcpdump filter that will capture Telnet traffic from your partner's machine only.

Constraints:

- Run tcpdump on the same server as Telnet and capture the session to a separate text file.
- Also run tcpdump on the client machine and also capture that session to a text file.
- Identify key packets such as connection establishment and the packets carrying username/password information.
- Your filter must exclude **all** traffic **except** Telnet traffic to and from your and your partner's machines.

Requirements:

1. Demonstrate your testbed in the lab.