Name_____ _____/20 pts.

Name_____

SE 4C03 Winter 2006

Lab Exercise 3

Instructor: William M. Farmer

Revised: 28 February 2006

Assigned: 28 February 2006
Lab report due: 28 February 2006

Do this lab exercise with your partner.

1. Study the "man" pages for `tcpdump`, `traceroute`, and `netstat`.

2. Log into one of the ITB lab computers. Call this computer *your-home-host*.

3. Make a directory in either your home directory or your partner's home directory named `dump-files`. Ensure that all the files in this directory are accessible and readable by everyone. Write the path to this directory here:

   _____/2 pts.

4. Before doing any of the rest of this exercise, log into `cnode7` using `ssh` and execute

   ```
   tcpdump -w dump-files/frames -i e1000g0
   ```

   (in the background) to collect in `dump-files/frames` all the frames that are received at or sent from `cnode7`. Keep collecting frames until you are done with the parts 5–7 of the exercise.

   _____/2 pts.

5. Log into `cnode7` again using `ssh` and then start an `xterm`. Do not log out until after the exercise is completed.

6. Use `traceroute` to find the route from your-home-host to `cnode7`. Record the route you find here:

_____/4 pts.

7. Using `netstat`, determine what TCP connections are established between your-home-host and `cnode7`. Make a table that lists these connections with the TCP ports of the client and server processes here:

_____/4 pts.

8. Do this part of the exercise after you are done with parts 5–7.

   (a) Stop the tcpdump process and use `tcpdump -r` to put the header information of the frames in `dump-files/frames` into `dump-files/headers`. _____/2 pts.

   (b) How many frames _____ were received by or sent from your-home-host? _____/2 pts.

   (c) How many ARP messages _____ were received by or sent from your-home-host? _____/1 pt.

   (d) How many ICMP messages _____ were received by or sent from your-home-host? _____/1 pt.

   (e) How many UDP datagrams _____ were received by or sent from your-home-host? _____/1 pt.

   (f) How many TCP segments _____ were received by or sent from your-home-host? _____/1 pt.

For your team's lab report, hand in these three sheets. You must also turn in a paper copy of each team member's log book no later than the beginning of the lecture on March 2, 2006. If your log book is missing or incomplete, 4 points will be deducted from your mark. *You and your partner must hand the lab report in together before the end of the lab session. If you do not attend the lab session or leave the lab before handing in the lab report, you will receive a mark of 0 for the lab exercise.*

For your lab report, hand in the two sheets of this exercise, the required table, and a copy of your log book.