Name________________________________ _____/20 pts.

SE 4C03 Winter 2002

Lab Exercise 3

Instructor: William M. Farmer

Revised: 5 March 2002

Assigned: 05 March 2002
Lab report due: 22 March 2002

Do this lab exercise by yourself.

1. Create an account on your host named `intruder` with the password `intruder`. _____/1 pt.

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

3. Make a directory in your personal account's home directory named `dump-files`. Before doing any of the rest of this exercise, use `tcpdump -w` (in the background) to collect in `dump-files/dlink-frames` all the frames that arrive at the D-Link network interface of your host and in `dump-files/3com-frames` all the frames that arrive at the 3Com network interface of your host. Keep collecting frames until you are done with parts 4–7 the exercise. _____/2 pts.

4. The Little Internet has six class C networks: 192.168.2.0, 192.168.3.0, 192.168.4.0, 192.168.5.0, 192.168.6.0, and 192.168.7.0. For each class network N, choose a network interface with an IP address in N. _____/1 pt.

5. For each interface chosen above, log in into the intruder account on the host with the interface using `ssh` and then start an xterm. Do not log out until you are done with the exercise. _____/1 pt.

6. Using `netstat`, determine what TCP connections are established on your host. Make a table that lists these connections with the TCP ports of the client and server processes. _____/3 pts.

7. Use `traceroute` to determine the route packets take from your host to the six interfaces chosen above. Put the routes you find into a table. Mark the routes that do not satisfy the Little Internet Routing Specification. _____/6 pts.

8. Do this part of the exercise after you are done with parts 4–7.

   (a) Stop the tcpdump processes and use `tcpdump -r` to put the header information of the frames in `dump-files/dlink-frames` and `dump-files/3com-frames` into `dump-files/dlink-headers` and `dump-files/3com-headers`, respectively. _____/1 pt.

   (b) How many frames arrived at the D-Link __________ and 3Com __________ network interfaces? _____/1 pt.

   (c) How many ARP packets arrived at the D-Link __________ and 3Com __________ network interfaces? _____/1 pt.

   (d) How many ICMP packets arrived at the D-Link __________ and 3Com __________ interfaces? _____/1 pt.

   (e) How many UDP packets arrived at the D-Link __________ and 3Com __________ network interfaces? _____/1 pt.

   (f) How many TCP packets arrived at the D-Link __________ and 3Com __________ network interfaces? _____/1 pt.

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