

Your name \_\_\_\_\_/20 pts.

Your account \_\_\_\_\_

## SE 4C03 Winter 2003

### Lab Exercise 3

Instructor: William M. Farmer

Revised: 14 February 2003

Assigned: 14 February 2003

Lab report due: 07 March 2003

Do this lab exercise by yourself.

1. Study the “man” pages for `tcpdump`, `netstat`, and `traceroute`.
2. Make a directory in your personal account’s home directory named `dump-files`. Ensure that all the files in this directory are readable by the `instructor` account. 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 3–6 of the exercise.  
\_\_\_\_\_/4 pts.
3. 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  $N$ .
4. For each interface chosen above, log 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.
5. 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.  
\_\_\_\_\_/4 pts.

6. Use **tracert** 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.
7. Do this part of the exercise after you are done with parts 3–6.
  - (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.