Name_____ _____/20 pts.

Name_____

SE 4C03 Winter 2007

Lab Exercise 3

Instructor: William M. Farmer

Revised: 1 March 2007

Assigned: 2 March 2007
Lab report due: 2 March 2007

Do this lab exercise with your partner.

1. Log into your host on the Little Internet.
2. Check that the routing table for your host is absolutely correct. Fix any problems you find by modifying your `route-script`.
3. Study the "man" pages for `tcpdump`, `traceroute`, and `netstat`.
4. 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.

5. Before doing any of the rest of this exercise, execute both

```
tcpdump -w dump-files/frames-eth0 -i eth0 &
tcpdump -w dump-files/frames-eth1 -i eth1 &
```

(in the background) to collect in `dump-files/frames-eth0` and `dump-files/frames-eth1` all the frames that are received at or sent from your host on the `eth0` and `eth1` interfaces, respectively. Keep collecting frames until you are done with the parts 5–7 of the exercise. _____/2 pts.

6. Using `ssh` log into the `intruder` account on another host (called it X) on the Little Internet that is at least three hops away from your host and then start a `top` process. Do not log out until after the exercise is completed.

7. Use `traceroute` to find the route from your-home-host to host X. Since the Little Internet does not have a DNS service running, you need to invoke `traceroute` with the option that uses IP addresses instead domain names. Record the route you find here:

_____/4 pts.

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

   (a) Stop the tcpdump processes and use `tcpdump -r` to put the header information of the frames in `dump-files/frames-eth0` and `dump-files/frames-eth1` into `dump-files/headers-eth0` and `dump-files/headers-eth1`, respectively. _____/2 pts.

   (b) How many frames arrived at the `eth0` _____ and `eth1` _____ network interfaces? _____/2 pt.

   (c) How many ARP packets arrived at the `eth0` _____ and `eth1` _____ network interfaces? _____/1 pt.

   (d) How many ICMP packets arrived at the `eth0` _____ and `eth1` _____ interfaces? _____/1 pt.

(e) How many UDP packets arrived at the `eth0` _____ and `eth1` _____ network interfaces? _____/1 pt.

(f) How many TCP packets arrived at the `eth0` _____ and `eth1` _____ network interfaces? _____/1 pt.

9. 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 here:

_____/4 pts.

10. Log out of host X.

For your team's lab report, hand in the sheets of this exercise and a paper copy of each team member's log book (if it is more convenient, you may hand this in at the beginning of the next lecture). 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.*