Name_____ _____/20 pts.

Name_____

CS 3CN3 and SE 4C03 Winter 2009

Lab Exercise 3

Instructor: William M. Farmer
Revised: 27 February 2009

Assigned:	27 February 2009
Lab report due for Lab Session 1:	3 March 2009
Lab report due for Lab Session 2:	6 March 2009

Do this lab exercise with your assigned group member.

1. Study the "man" pages for `tcpdump` and `netstat`.
2. Log into your host on the Little Internet.
3. Check that `ssh`, `tcpdump` and `netstat` are on your machine. If not, you will have to load the packages that contain them:
   (a) Switch to the root account.
   (b) Go to the `/mnt` directory and see if it is empty. If it is, execute
   ```
   mount -t auto -o ro /dev/scd0 /mnt
   ```
   (c) Go to `/mnt/Packages` and install the individual packages you need. Find the packages you need using `ls` and `grep`.
   (d) Execute
   `rpm -i --includedocs` *packagename*
   to load the packages.
4. Check that the routing table for your host is absolutely correct. Fix any problems you find by modifying your `route-script`.

_____/1 pt.

5. Use `traceroute`, `tracepath`, or `ping -R` to identify any problems with the Little Internet. Work with the other groups to fix them. Describe any unresolved problems here:

_____/1 pt.

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. Make a directory in one of the home directories of your group 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.

8. Execute

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

(in the background) to collect in `dump-files/frames-eth0` all the frames that are received at or sent from your host on the `eth0` interface. Keep collecting frames until you are done with this item. Use `traceroute`, `tracepath`, or `ping -R` to find the route from your home host to host X. Record the route you find here:

Stop the tcpdump process. (You should not let the tcpdump process run more than a couple minutes.)

_____/1 pt.

9. Execute

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

(in the background) to collect in `dump-files/frames-eth1` all the frames that are received at or sent from your host on the `eth1` interface. Keep collecting frames until you are done with this item. Use `traceroute`, `tracepath`, or `ping -R` to find the route from your home host to host X. Record the route you find here:

Stop the tcpdump process. (You should not let the tcpdump process run more than a couple minutes.)

_____/1 pt.

10. Do this part of the exercise after you are done with parts 8–9.

    (a) 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 pts.

    (c) How many ARP packets arrived at the `eth0` _____ and `eth1` _____ network interfaces? _____/2 pts.

    (d) How many ICMP packets arrived at the `eth0` _____ and `eth1` _____ interfaces? _____/2 pts.

    (e) How many UDP packets arrived at the `eth0` _____ and `eth1` _____ network interfaces? _____/2 pts.

    (f) How many TCP packets arrived at the `eth0` _____ and `eth1` _____ network interfaces? _____/2 pts.

11. 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:

_____/2 pts.

12. Log out of host X, go home, have dinner, and start reading *Treasure Island*.

For your group's lab report, hand in this sheet, your interface access findings, and a paper copy of each group 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 other group members 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.*