Name________________________________ _____/20 pts.

SE 4C03 Winter 2001

Lab Exercise 4

Instructor: William M. Farmer

Revised: 27 February 2001

Assigned: 28 February 2001
Lab report due: 14 March 2001

Do this lab exercise by yourself except for part B.1.

A. Learn how to use IPTraf, a tool for monitoring packet traffic on network interfaces. (You should have already loaded the rpm for IPTraf.)

1. Look over the manual for IPTraf at

   `/usr/doc/iptraf-2.3.1/manual.html`.

2. Start up IPTraf, turn on logging, and then run the "IP traffic monitor" function with the "all interfaces" option set. Use some network services and watch what packets are generated.

3. Run for at least one hour the IPTrac "detailed interface statistics" function with the "eth0" option set, and then for at least another hour run the function with the "eth1" option set. Put a copy of the

   `/var/log/iptraf/iface_stats_detailed.log`

   file in you home directory. Using the information logged in this file, fill in the following tables:

Interface	eth0	Elapsed time:				
Number of Packets	IP	TCP	UDP	ICMP	Other IP	nonIP

Interface	eth1	Elapsed time:				
Number of Packets	IP	TCP	UDP	ICMP	Other IP	nonIP

_____/ 4 pts.

B. Configure the Secure Shell network service for public key authentication. (You should have already loaded the rpm for IPTraf.)

1. Suppose your account name is a and your host name is x. Modify the `sshd` configuration file at `/etc/ssh2/sshd2_config` on x so that only public key authentication is allowed (and not password authentication). Restart the `sshd` server program located at `/usr/sbin/sshd` as a root process on x. _____/4 pts.

2. Ask one of the other teams in the class to give you an account named a on their host . (Do not use the `intruder` account for this purpose.) Suppose the name of this host is y.

3. Use the `ssh-keygen` command to create a public key pair for your account on x (and an `.ssh2` directory). You will have to enter a passphrase which will be used for public key authentication. Rename the private and public key files to something convenient, say id_a_x and id_a_x.pub. Do the same on y.

4. Copy the public key file id_a_x.pub to the `.ssh2` directory on y. Copy the public key file id_a_y.pub to the `.ssh2` directory on x.

5. Create a file named `identification` in the `.ssh2` directory on x and put the line

   IdKey id_a_x

   in it. Do the same on y.

6. Create a file named `authorization` in the `.ssh2` directory on x and put the lines

   Key id_a_x.pub
   Key id_a_y.pub

   in it. Do the same on y.

7. Make the `identification` and `authorization` files on x and y readable and writeable by owner only. _____/ 2 pts.

8. Test the set up by executing

   ssh -v x

   on x. The `-v` option for "verbose" will show each step of the process of creating an Secure Shell communication channel from your computer to itself. After the communication channel is established, try starting an X Windows client like `xterm` or `netscape`. _____/ 4 pts.

9. Test the set up by executing

   `ssh -v` x

   on y. After the communication channel is established, try starting an X Windows client like `xterm` or `netscape`. _____/ 3 pts.

10. Test the set up by executing

    `ssh -v` y

    on x. After the communication channel is established, try starting an X Windows client like `xterm` or `netscape`. _____/ 3 pts.

11. Demonstrate your set up of Secure Shell to the TA.

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