SE 4C03 Winter 2005
Lab Exercise 3
Instructor: Kartik Sivaramakrishnan
Revised: 21st February 2005

Assigned: 21-FEB-2005
Lab report due: 11-MAR-2005

Do this lab with your assigned team members.

1. You will work with ssh in this lab exercise. In order that others can ssh into your machine, please put the following command /etc/init.d/ipchains stop in your rc.local files.

2. Consult the man pages for tcpdump, netstat, and traceroute.

3. 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 the rest of the exercise, use tcpdump -w in the background to collect in dump-files/dlink-frames all the frame 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 of the exercise.

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.

5. 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 logout until you are done with the remainder of the exercise.
6. Using `netstat`, determine what TCP connections are established on your remote server. Make a table that lists these connections with the TCP port of the client and server processes.

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.

8. Do this part after you have done with parts 2-7.

   (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-headers` respectively.

   (b) How many frames arrived at the D-Link and 3Com network interfaces?.

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

   (d) How many ICMP packets arrived at the D-Link and 3Com network interfaces?.

   (e) How many TCP packets arrived at the D-Link and 3Com network interfaces?.

For your team’s lab report, hand the two sheets of this lab exercise, the two required tables, your answers to part 8, and finally a copy of each member’s log book.