COMP 8006 Computer Systems Technology January 2010

Network Administration and Security Level 2

Assignment #1

DUE: January 28, 2010 – 1330 hrs. This is an individual assignment.

OBJECTIVE: To implement and test a simple personal Linux firewall.

ASSIGNMENT:

Design a firewall for Linux that will implement the following rules:

- Set the default policies to **DROP**.
- Create a set of rules that will:
    - Permit inbound/outbound **ssh** packets.
    - Permit inbound/outbound **www** packets.
    - Drop inbound traffic to port 80 (http) from source ports less than 1024.
    - Drop all incoming packets from reserved port 0 as well as inbound traffic to port 0.
- Create a set of **user-defined** chains that will implementing **accounting rules** to keep track of www, ssh traffic, versus the rest of the traffic on your system.

CONSTRAINTS:

- Use **Netfilter** for your firewall implementation.
- You must ensure the you reject those connections that are coming the "wrong" way (i.e., inbound SYN packets).
- You will be required to demonstrate your firewall in action on the day the assignment is due.
- Remember to allow DNS and DHCP traffic through so that your machine can function properly.

TO BE SUBMITTED:

- Hand in complete and well-documented design work and listings of your program.
- Clearly document your testing procedures. Provide printed copies of your test results.
- Provide your shell script on a disk. Include a set of instructions on how to use your script. Essentially a small "HOW-TO".
- You will be required to demonstrate your functional firewall in the lab on the day the assignment is due.