COMP 8006 Computer Systems Technology January 2016

Network Administration and Security Level 2

Assignment #1

Due Date: January 28, 2016 – 1300 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 outbound traffic to port 0.
- Create a set of **user-defined** chains that will implement **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 the firewall drops all inbound SYN packets, unless there is a rule that permits inbound traffic.
- 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 the firewall **script**.
- You are also required to demonstrate your working programs during the lab the day the assignment is due.
- Ensure that you clearly explain the testing procedures for your programs and provide test data as covered in lectures.
- Include a set of instructions on how to use your script. Essentially a small "HOW-TO".
- Submit a **zip** file containing all the code and documents as described below in the sharein folder for this course under "**Assignment #1**".
- Your report must follow the standard technical format.

Assignment #1 Evaluation

(1). Design Work & Documentation:	10
(2). Functionality:	25
(3). Testing	15
Total:	50