COMP 8006 Computer Systems Technology January 2014

Network Administration and Security Level 2

Assignment #2

Due: February 13, 2014 – 1330 hrs. Work in groups of two.

Objective: To design, implement and test a standalone Linux firewall and packet filter.

Assignment:

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

- Set the initial default policies.
- Get user specified parameters (see constraints) and create a set of rules that will implement the firewall requirements. Specifically the firewall will control:
    - Inbound/Outbound TCP packets on allowed ports.
    - Inbound/Outbound UDP packets on allowed ports.
    - Inbound/Outbound ICMP packets based on type numbers.
    - All packets that fall through to the default rule will be dropped.
    - Drop all packets destined for the firewall host from the outside.
    - Do not accept any packets with a source address from the outside matching your internal network.
    - You must ensure the you reject those connections that are coming the "wrong" way (i.e., inbound SYN packets to high ports).
    - Accept fragments.
    - Accept all TCP packets that belong to an existing connection (on allowed ports).
    - Drop all TCP packets with the SYN and FIN bit set.
    - Do not allow Telnet packets at all.
    - Block all external traffic directed to ports 32768 – 32775, 137 – 139, TCP ports 111 and 515.
    - For FTP and SSH services, set control connections to "Minimum Delay" and FTP data to "Maximum Throughput".
- Design a test procedure that will test all your firewall rules and print the results of the test to a file. Make sure that someone reading the file contents will know exactly which rule worked and which rule failed.
- The machines in the lab are equipped with two Ethernet cards. One of them is already configured and operational. You will have to enable and configure the other one for use as the gateway to your "internal" network.
- Your testbed will then have one machine operating as a firewall. It will have an "outside" connection (eth0) and it will forward datagrams to hosts on its internal hosts on the second NIC (eth1).

Constraints:

- The firewall/packet filter must be designed and implemented using **Netfilter**.
- Your firewall script must have two sections: a "User Configurable Section" and the "Implementation Section".
- The user configuration section will allow a user to set at least the following parameters:

    - Name and location of the utility you are using to implement the firewall.
    - Internal network address space and the network device.
    - Outside address space and the network device.
    - TCP services that will be allowed.
    - UDP services that will be allowed.
    - ICMP services that will be allowed.

- Only allow NEW and ESTABLISHED traffic to go through the firewall. In other words you are doing **stateful** filtering.

- You must ensure that you reject those connections that are coming the "wrong" way, meaning inbound connection requests (unless of course it is to a permitted service).
- Design test scripts to validate your firewall rules.
- You will be required to demonstrate your functional firewall in the lab on the day the assignment is due.

To Be Submitted (on disk):

- Hand in complete and well-documented design work and listings of your program.
- A formal and detailed test plan as well as the test results for each rule.
- Provide your test and firewall scripts and all supporting documentation on disk. Include a set of instructions on how to use your script. Essentially a small "HOW-TO".