Linux Firewall Specification

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

Due: April 14 – 0930 hrs. Work in groups of two.

Assignment:

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

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

- Set the initial default policies to **DROP**.
- 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 user-specified ports.
    - Inbound/Outbound UDP packets on user-specified ports.
    - Inbound/Outbound ICMP packets based on type numbers.
    - Do not accept any packets with a source address from the outside matching your internal network.
    - Accept all TCP packets that belong to an existing connection (on allowed ports). These packets have the ACK bit set.
    - Drop all TCP packets with the SYN and FIN bit set.
    - Do not allow Telnet or FTP packets at all.
- The firewall machine in the lab is equipped with two Ethernet cards. You will have to enable and configure both. One NIC will connect to the external router/network and the other will be used as the gateway to the internal lab LAN.
- 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).
- Since the LAN is private, your firewall must use NAT to allow internal machines to access the Internet.

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.
    - Internal IP addresses to which specific port/service traffic will be forwarded.

- Remember to allow DNS and DHCP traffic through so that your machine can function properly.
- Only allow NEW and ESTABLISHED traffic to go through the firewall. In other words you are doing **stateful** filtering.
- The implementation section will contain all the ***iptables*** commands.
- Design test scripts to validate your firewall rules.
- You will be required to demonstrate your firewall in action on the day the assignment is due.

To Be Submitted:

- Hand in complete and well-documented design work and printed listings of your program.

- Provide your test and firewall scripts and all supporting documentation on a disk. Include a set of instructions on how to use your script. Essentially a small "HOW-TO".