CS393 - Network Security - Lab Assignment 4
Network Defense – Part I
Firewalls
Due April 2

Summary:
In the last few labs you have learnt how to discover the layout of a network, find hosts and servers, and discover vulnerable services running on them. In this lab you will learn how to defend your network, against attacks, using a packet filtering firewall and in the next lab you’ll learns how to detect an attack using an intrusion detection system.

A Packet Filtering Firewall is one of the basic protection mechanisms placed on a network. Firewalls could be installed and configured in several ways, depending upon the level of protection needed for the network behind it. In this assignment, you will explore how to configure a firewall. As usual, you will be using Linux as our base operating system, and use ipchains to make it act as a firewall.

Prerequisites:
Read about ipchains from the following links:
- [http://www.flounder.net/ipchains/ipchains-howto.html](http://www.flounder.net/ipchains/ipchains-howto.html)

A firewall configuration tool can be found at:

Estimated time to finish this lab:
Based on the amount of time it took for us to create this lab, we estimate that it will take at least 10 hours for you to finish this lab.

Lab Work:
All labs, from this Lab onwards, will be completed as group. Your group will be assigned to a small network to do all the labs following this lab. Below is the layout of your small network:
You will use your network to do the following:

**Part A:**

Configure the protected server to meet the following requirements:

- **Rules for outgoing traffic:**
  - Your local machine should be able to communicate with the external world without any restrictions.

- **Rules for incoming traffic:**
  - All incoming connection requests should be rejected, with the following exception:
    - Your machine should respond to Ping from network 10.0.0.0 (netmask: 255.255.255.0)
    - Your machine should accept any incoming SSH, HTTP, FTP requests from Network 10.0.0.0 (netmask: 255.255.0.0)
    - Your machine should accept any incoming telnet connections from the machine 10.0.0.100 and 10.0.0.110.

**Part B:**

Configure the firewall to meet the following requirements:

- **Rules for outgoing traffic from protected server:**
  - Only SSH, DNS, and ICMP traffic should be allowed from 10.11.x.2 to go out
  - All other traffic should be blocked

- **Rule for incoming traffic to protected server:**
  - All incoming SSH, http, SMTP, Ping, and anonymous ftp should be permitted
  - All other incoming traffic should be blocked

**What to Hand in:**

- Two page summary on how `ipchains` works. Your summary should also include the difference between input/output, forward chains and how `ipchains` uses them.
- Your firewall configuration file for each part, with comments for each rule in the file. **If you use the firewall configuration tool then clearly indicate where you made changes to the configuration produced by the tool and why?**