COMP 8006 Assignment 2 Design Doc

Alex Zielinski

02/15/2018

Table of Contents

How it Works

There are two scripts within the folder called ***src*** (which can be found in the project folders top directory). The first script is called ***firewall.sh*** which contains the script that configures the firewall and/or internal host machine. The second script is called ***clean.sh*** which flush's all chains, deletes all user defined chains and sets the default policies to ACCEPT.

The firewall implements the following rules:

- Set default policies to DROP
- ACCEPT inbound/outbound SSH traffic (port 22)
- ACCEPT inbound/outbound WWW traffic (HTTP port 80 and HTTPS port 443)
- ACCEPT inbound/outbound DNS traffic (port 53)
- ACCEPT inbound/outbound ICMP traffic on allowed ports
- ACCEPT fragments
- ACCEPT TCP packets that belong to existing connection on allowed ports
- ACCEPT inbound/outbound DHCP traffic (port 67 and 68)
- DROP packets destined for firewall from outside
- DROP packets from outside with source address matching internal network
- DROP connections coming the wrong way (inbound SYN to high ports)
- DROP all TELNET traffic
- DROP external traffic directed to ports 32768-32775
- DROP external traffic directed to ports 137-139
- DROP external traffic directed to TCP port 111
- DROP external traffic directed to TCP port 515

There is also a user defined section starting on line 4. These variables allow the user to customize and change TCP/UDP/ICMP ports, external and internal interfaces, the firewall and internal IP as well as the utility name and location of the firewall. For example, in order to allow TCP traffic on a series of ports, one would need to modify the **TCP_PORTS** variable found at the top of the script as follows:

TCP_PORTS="80,443,53,22,21".

The firewall will be making use of both of its network cards. The external network card (eno1) will be used to communicate with the outside. The internal card (enp3s2) will be bound to an internal IP that is user specified and will be used to communicate with the internal host machine. The internal host machine will disable its external network card (eno1) as to prohibit direct communication with the outside. The internal host will make use of its internal card (enp3s2) as a means to communicate with the outside. This way the firewall machine and the internal machine will be connected by a cross-over cable via their internal network cards and the internal machine will have to go through the firewall in order to achieve communication with the outside.

User Guide

As mentioned earlier there are two scripts located in the ***src*** directory. These two scripts are called ***firewall.sh*** and ***cleanup.sh***. The firewall script configures the firewall (as well as the internal host machine) based on the rules mentioned in the ***How it Works*** section of this document. In order to run the firewall script, the user must navigate to the project's ***src*** folder via terminal and enter the following command with arguments:

./firewall.sh firewall

This will do two things. First, the script will configure the firewall machines network cards as well as routing options. It will enable the internal network card (enp3s2) bound with an internal IP (192.168.10.1) so that the firewall can receive and forward packets from/to the internal host machine. Secondly, the script will set the firewall rules.

In order to configure the internal host machine, the firewall script must be run (on a separate machine from the firewall machine) containing the argument **client** as such:

./firewall.sh client

This will disable the machines external card (eno1) so that it cannot communicate with the outside directly and will enable the internal network card (enp3s2) with a bound internal IP (192.168.10.2). This way the internal host can communicate with the outside via the firewall by sending and receiving packets that go through the firewall using the internal network card (that is connected with a cross-over cable).

The cleanup script is used to reset the firewall configurations. It flushes all chains, deletes all user defined chains and sets the default chain policies to ACCEPT. In order to run the cleanup script, the user must navigate to the project's ***src*** folder via terminal and enter the following command:

./clean.sh

There are 2 test scripts that can be found in the ***test*** folder. There is a test for inbound and outbound traffic. To run these tests simply run the shell script via terminal as follows:

./inbound_test.sh

./outbound_test.sh

The scripts will output the results of the tests into a file called ***inbound_test_results*** and ***outbound_test_results***.

Project folder directory listings

/src

|------ clean.sh

|------ firewall.sh

/test

|------ inbound_test.sh

|------ outbound_test.sh

Design Doc

Testing Doc

Finite State Machines