|  |  |  |  |
| --- | --- | --- | --- |
|  | 2/3/2016 |  | |
| |  |  | | --- | --- | |  |  | |  |  | |  |  | |  |  | | |  | |
| COMP8006 Assignment 2  *Standalone Linux Firewall* | | | |
|  | Rizwan Ahmed  Vishavpreet Singh  COMP6D | |  |

|  |  |  |
| --- | --- | --- |
|  |  |  |

Contents

[Introduction 2](#_Toc442299211)

[Listings 2](#_Toc442299212)

[Instructions 2](#_Toc442299213)

[Design 3](#_Toc442299214)

[Network Diagram 3](#_Toc442299215)

[Testing and Results 4](#_Toc442299216)

# Introduction

This is an implementation of a standalone Linux firewall that operates on one machine, which acts as a gateway, and forwards packets to another host on its internal network. The firewall, using user specified parameters, will implement the following rules:

* 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
* Drop any packets with a source address from the outside matching the host’s internal network
* Reject 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
* Drop all Telnet packets
* 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"

# Listings

# Instructions

To set up the firewall, first set the network interface names and IP addresses of the machine that will run the firewall and one of the internal hosts in the “hosts.sh” file.

Both machines, firewall and internal host, must have this script installed.

For the machine running the firewall, run the *hosts* script using “firewall” as the argument to set up the routing table and add MASQUERADE. As for the internal host, have the script run with “internal” as the argument to set up the host’s routing table.

To run the firewall: “sh firewall.sh”

To flush all rules and reset default policy to ACCEPT: “sh firewall.sh reset”

To run the test script: “sh testFirewall.sh”

# Design

## Network Diagram

F:\Users\Rizwan Ahmed\Dropbox\BTECH_WINTER_2016\COMP8006\diagram.png

# Testing and Results