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

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

Contents

[Introduction 2](#_Toc442295678)

[Listings 2](#_Toc442295679)

[Design 3](#_Toc442295680)

[Network Diagram 3](#_Toc442295681)

[Testing and Results 4](#_Toc442295682)

[Running the script 4](#_Toc442295683)

# 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

# Design

## Network Diagram

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

# Testing and Results

## Running the script

Using the reset argument in the firewall script:

