|  |  |  |  |
| --- | --- | --- | --- |
|  | 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)

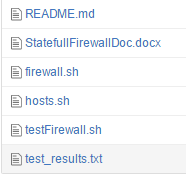
[Testing and Results 4](#_Toc442299216)

# 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



* Firewall.sh is the script to set up the firewall on the Firewall Machine
* Hosts.sh is the script to set up the routing on host and firewall machine
* testFirewall.sh is the testing script for the firewall
* test\_reults.txt is the file generated after running the testFirewall.sh script
* StatfullFirewallDoc.docx contains a detailed report of this assignment

# 

# 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”

To run host script on host machine: “sh hosts.sh internal”

To run host script on fireall machine: “sh hosts.sh firewall”

# 

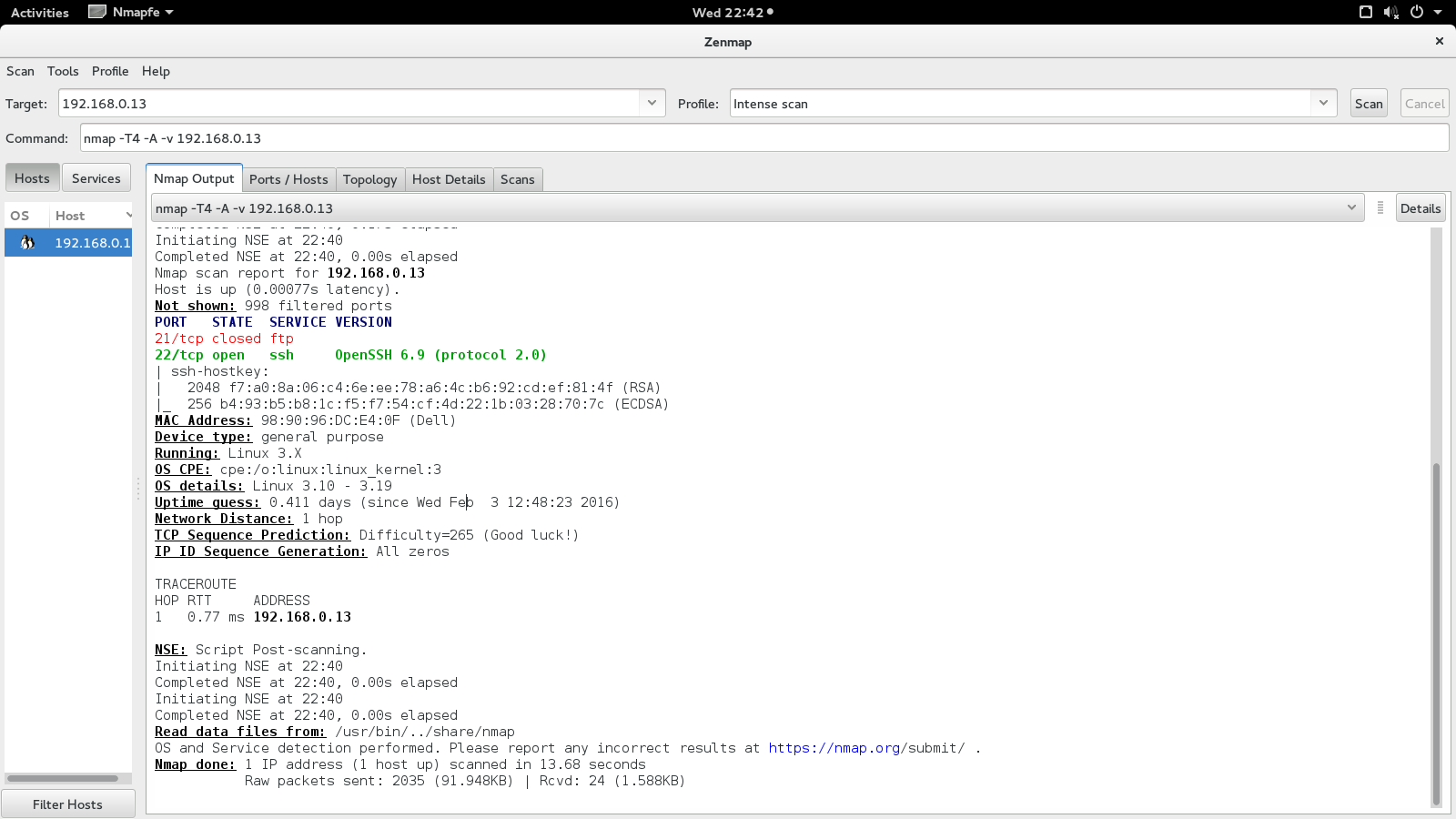
# Design

## Network Diagram

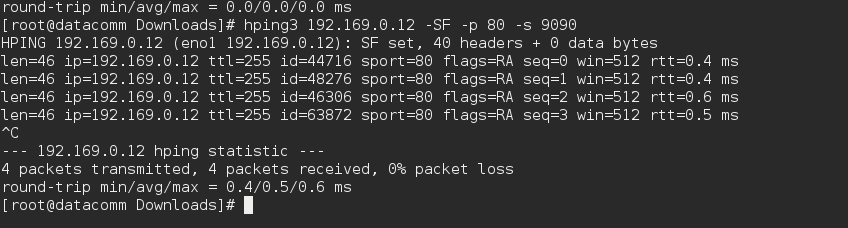
F:\Users\Rizwan Ahmed\Dropbox\BTECH_WINTER_2016\COMP8006\diagram.png

# Testing and Results

Test 1: NMMAPFE yielded the following results



Test 2: Hping for SYN FIN Packets



We ran the testing script included in the package, following are the results

Firewall test starting...

-------------------------

NMAP test

The open ports should be: 20,21,22,53,68,80,443

Starting Nmap 7.00 ( https://nmap.org ) at 2016-02-03 22:43 PST

Initiating ARP Ping Scan at 22:43

Scanning 192.168.0.13 [1 port]

Completed ARP Ping Scan at 22:43, 0.02s elapsed (1 total hosts)

Initiating Parallel DNS resolution of 1 host. at 22:43

Completed Parallel DNS resolution of 1 host. at 22:43, 6.50s elapsed

Initiating SYN Stealth Scan at 22:43

Scanning 192.168.0.13 [1000 ports]

Discovered open port 22/tcp on 192.168.0.13

Completed SYN Stealth Scan at 22:43, 4.83s elapsed (1000 total ports)

Nmap scan report for 192.168.0.13

Host is up (0.00058s latency).

Not shown: 998 filtered ports

PORT STATE SERVICE

21/tcp closed ftp

22/tcp open ssh

MAC Address: 98:90:96:DC:E4:0F (Dell)

Read data files from: /usr/bin/../share/nmap

Nmap done: 1 IP address (1 host up) scanned in 11.44 seconds

Raw packets sent: 2001 (88.028KB) | Rcvd: 5 (192B)

-------------------------

-------------------------

TCP test

-----------------------------------------

Testing TCP packets allowed on port 20

Expected result: 0% packet loss

HPING 192.168.0.13 (eno1 192.168.0.13): S set, 40 headers + 0 data bytes

-----------------------------------------

Testing TCP packets allowed on port 21

Expected result: 0% packet loss

HPING 192.168.0.13 (eno1 192.168.0.13): S set, 40 headers + 0 data bytes

len=46 ip=192.168.0.13 ttl=62 DF id=44282 sport=21 flags=RA seq=0 win=0 rtt=0.9 ms

DUP! len=46 ip=192.168.0.13 ttl=62 DF id=44552 sport=21 flags=RA seq=0 win=0 rtt=1001.0 ms

DUP! len=46 ip=192.168.0.13 ttl=62 DF id=44769 sport=21 flags=RA seq=0 win=0 rtt=2001.0 ms

-----------------------------------------

Testing TCP packets allowed on port 22

Expected result: 0% packet loss

HPING 192.168.0.13 (eno1 192.168.0.13): S set, 40 headers + 0 data bytes

len=46 ip=192.168.0.13 ttl=62 DF id=0 sport=22 flags=SA seq=0 win=29200 rtt=1.0 ms

DUP! len=46 ip=192.168.0.13 ttl=62 DF id=0 sport=22 flags=SA seq=0 win=29200 rtt=1001.2 ms

DUP! len=46 ip=192.168.0.13 ttl=62 DF id=0 sport=22 flags=SA seq=0 win=29200 rtt=2001.3 ms

-----------------------------------------

Testing TCP packets allowed on port 53

Expected result: 0% packet loss

HPING 192.168.0.13 (eno1 192.168.0.13): S set, 40 headers + 0 data bytes

-----------------------------------------

Testing TCP packets allowed on port 68

Expected result: 0% packet loss

HPING 192.168.0.13 (eno1 192.168.0.13): S set, 40 headers + 0 data bytes

-----------------------------------------

Testing TCP packets allowed on port 80

Expected result: 0% packet loss

HPING 192.168.0.13 (eno1 192.168.0.13): S set, 40 headers + 0 data bytes

-----------------------------------------

Testing TCP packets allowed on port 443

Expected result: 0% packet loss

HPING 192.168.0.13 (eno1 192.168.0.13): S set, 40 headers + 0 data bytes

---------------------------------------\n

---------------------------------------

UDP test

-----------------------------------------

Testing UDP packets allowed on port 20

Expected result: 0% packet loss

HPING 192.168.0.13 (eno1 192.168.0.13): NO FLAGS are set, 40 headers + 0 data bytes

-----------------------------------------

Testing UDP packets allowed on port 21

Expected result: 0% packet loss

HPING 192.168.0.13 (eno1 192.168.0.13): NO FLAGS are set, 40 headers + 0 data bytes

-----------------------------------------

Testing UDP packets allowed on port 22

Expected result: 0% packet loss

HPING 192.168.0.13 (eno1 192.168.0.13): NO FLAGS are set, 40 headers + 0 data bytes

-----------------------------------------

Testing UDP packets allowed on port 53

Expected result: 0% packet loss

HPING 192.168.0.13 (eno1 192.168.0.13): NO FLAGS are set, 40 headers + 0 data bytes

-----------------------------------------

Testing UDP packets allowed on port 68

Expected result: 0% packet loss

HPING 192.168.0.13 (eno1 192.168.0.13): NO FLAGS are set, 40 headers + 0 data bytes

---------------------------------------\n

---------------------------------------

ICMP test

-----------------------------------------

Testing ICMP packet type 0

Expected result: 0% packet loss

HPING 192.168.0.13 (eno1 192.168.0.13): icmp mode set, 28 headers + 0 data bytes

-----------------------------------------

Testing ICMP packet type 3

Expected result: 0% packet loss

HPING 192.168.0.13 (eno1 192.168.0.13): icmp mode set, 28 headers + 0 data bytes

-----------------------------------------

Testing ICMP packet type 8

Expected result: 0% packet loss

HPING 192.168.0.13 (eno1 192.168.0.13): icmp mode set, 28 headers + 0 data bytes

---------------------------------------\n

---------------------------------------

Fragment test

Expected result: 0% packet loss

HPING 192.168.0.13 (eno1 192.168.0.13): NO FLAGS are set, 40 headers + 0 data bytes

---------------------------------------

Testing SYN packets on high port

Expected result: 100% packet loss

HPING 192.168.0.13 (eno1 192.168.0.13): S set, 40 headers + 0 data bytes

---------------------------------------

Telnet test

Expected result: 100% packet loss

HPING 192.168.0.13 (eno1 192.168.0.13): NO FLAGS are set, 40 headers + 0 data bytes

---------------------------------------

---------------------------------------

Blocked ports 32768-32775 test

Expected result: 100% packet loss

HPING 192.168.0.13 (eno1 192.168.0.13): S set, 40 headers + 0 data bytes

HPING 192.168.0.13 (eno1 192.168.0.13): udp mode set, 28 headers + 0 data bytes

---------------------------------------

Blocked ports 137-139

Expected result: 100% packet loss

HPING 192.168.0.13 (eno1 192.168.0.13): NO FLAGS are set, 40 headers + 0 data bytes

HPING 192.168.0.13 (eno1 192.168.0.13): udp mode set, 28 headers + 0 data bytes

---------------------------------------

Blocked TCP port 111 and 515 test

Expected result: 100% packet loss

HPING 192.168.0.13 (eno1 192.168.0.13): S set, 40 headers + 0 data bytes

HPING 192.168.0.13 (eno1 192.168.0.13): S set, 40 headers + 0 data bytes

---------------------------------------

Firewall test complete