Lab 9.1 Introduction to Nmap
IN715 Networks Three

September 23, 2014

Introduction

In today's class we saw how to use lists, macros, and tables to manage firewall rules. In this lab we will get some experience working with PF firewall rules.

Carry out this lab on your `router2` system.

1 Macros and lists

1. One good use for macros is to identify your network interfaces, since "em0" and "em1" are not very descriptive. Create two macros, `$inside_if` and `$outside_if` for your network interfaces and use those macros in your rules.

2. Create a list with your OpenBSD server and your Windows server addresses. Use that list in rules that allow DNS and DHCP requests to pass from your inside network to the outer network. Use the macro `$servers` for that list.

3. Create a rule set that lets hosts on your inner network send packets out to any destinations using ssh, http, https, and irc (on their standard ports). Use a list so you only need to write one rule.

2 Tables

1. Create persistent, constant tables that refer to

- your outer network;
- your inner network;
- your outer network, *except the router interfaces*

Use the tables wherever they are appropriate in your rules.

2. Create a dynamic table called `<spammers>` and populate it from a text file called `/etc/spammers`. Put the following addresses in it (one per line).

```
76.121.0.0/16
123.231.12.3
201.11.44.128/25
```

Write a firwall rule blocking any traffic to port 25 coming from these addresses. Use `pfctl` to view the list once it is active.

Use `pfctl` to add the address `91.114.17.190` to the table.

Use `pfctl` to remove `123.231.12.3` from the table. View the updated table to verify that your changes have taken effect.