Lab 13.1 Firewalling with iptables
IN618 Security

May 26, 2016

Introduction

A fundamental task in securing a networked host is the configure and run a firewall. In this lab we will see how to configure `iptables` to provide firewalling on Linux server.

Procedure

1. Obtain the ip address of a lab virtual machine from the lecturer. Ssh into it with our standard username/password.
2. Install apache2 and nmap with the commands

   ```
   sudo apt-get update
   sudo apt-get install apache2 nmap
   ```

   You may need to modify your `sources.list` file if it asks for an install CD.
3. Visit the web page on your server using your desktop's browser.
4. Perform an `nmap` scan of your own machine and note the results. You should find ports 80 and 22 open and all others closed.
5. Configure your `iptables` firewall following the tutorial at `https://www.digitalocean.com/community/tutorials/how-to-set-up-a-firewall-using-iptables-on-ubuntu-14-04`
6. Verify that you can access your VM using ssh and http.
7. Perform another nmap scan. What, if anything, has changed?
8. Now modify your firewall to block http traffic and verify that it worked.
9. Perform another nmap scan and note the results.