CHAPTER 6

Networking and Firewalls

By Dennis Matotek

So far we’ve shown you some of the basic features of Linux, but one of the most critical is networking. It is via networking that your host talks to other hosts and your applications communicate with your users and the world. In this chapter, we’ll describe how to set up your host’s networking and then how to protect that network from attackers using a firewall.

Note A firewall is a series of rules that control access to your host through the network.

We’ll teach you about how to configure your network cards or interfaces and how to give them IP addresses. You’ll learn how to connect to other networks and how to troubleshoot your connections.

We’ll also be looking at a software application called Netfilter that is a firewall common to all Linux distributions. You will learn how to manage a firewall and how to write firewall rules. To do this, we’ll introduce you to Netfilter’s management interface, iptables. Finally, we will also show you how you can use TCP Wrappers to secure daemons running on your host.

Once we’ve introduced the basics of network configuration, we’ll also show you how to configure an example network that might suit your environment. By the end of this chapter, you should have the skills to be able to configure a suitable network for your environment.

Throughout this chapter, we’ll be using networking terminology. We don’t expect you to be a networking expert, but we have assumed you do have some basic knowledge. If you don’t feel that you know enough, we recommend you check out these sites and tutorials:

- http://www.w3schools.com/tcip/default.asp
- http://compnetworking.about.com/od/workingwithipaddresses/1/blip.htm

Note iptables is used to protect your network services. You’ll learn more about how to run network services like DNS and DHCP on your host in Chapter 9.
Introduction to Networks and Networking

Networks are made of both hardware and software. They vary in complexity depending on their size and the level of interconnectedness they require. In a small business you will probably have a simple network. You may have a web server and mail server, and you will probably have a file/print server (sometimes all these servers are actually one host). Undoubtedly, you will have a connection to the Internet, and you will probably want to share that connection with others in your organization.

The nature of your business and the work you do will heavily dictate how you choose to set up your network. A business that is starting out often has only one main server that pretty much does all the functions the business requires. It could be a DHCP, DNS, file, mail, and web server all rolled into one. Those familiar with Microsoft products would regard this as similar to a product like Windows Small Business Server. But as that business grows, it will probably begin to move some of these combined functions to its own hosts. Very few larger businesses would trust their entire company IT infrastructure to an individual host that has so many roles. This single point of failure should be avoided where possible, but a small business rarely has the luxury of having a host for each service it wishes to provide.

**Caution** If your business does have single points of failure, like many services on one host, backup and recovery become critical. Losing your data could be a disaster for your business, so you should always have backups and the ability to recover your hosts and data. See Chapter 13 for details of how to implement a backup and recovery strategy for your organization.

Then there are the interconnecting pieces of hardware you may require. If you are connecting users in your office to a single network, you will need cables, patch panels switches, and potentially a wireless access point that can create a wireless network.

**Caution** Wireless networks are a useful and cheap way to spread your network. They don’t require expensive cabling and switches, and your staff can be a bit more mobile in the office. They present some challenges, however. Wireless networks can allow attackers to connect and sniff your network if inappropriately secured, and they don’t perform as well as wired networks (those with physical cables). For example, it is still much faster to transfer large amounts of data over wired connections rather than over wireless connections. If you’re considering a wireless network for your business, we recommend you read the information at http://en.wikipedia.org/wiki/Wireless_security, http://www.practicallynetworked.com/support/wireless_secure.htm, and http://www.us-cert.gov/reading_room/Wireless-Security.pdf.

We’re going to start by explaining how to configure networking on a single host and introduce you to the tools and commands you’ll need to configure a broader network.

In order to show you how to configure a network, we’re going to use an example network that we’ve created. You can see this example network in Figure 6-1.