Netfilter iptables on IPv4 & IPv6
1st Edition

Mostafa Moradian

February 18, 2010

Contents

Chapter 1

License

Chapter 2

Acknowledgments

I should thank my father and my mother and also all the teachers, professors and authors of all the books I've read who let me know that I know nothing. I also thank the Netfilter team, the OpenOffice.org team and all the people who made these nice operating system and softwares possible.

Chapter 3

I want to hear you

You are my reader and I value you as the best who knows. Don't hesitate to contact me. I really want to know what you think about my book and how you value or devalue it. I will help you with technical problems related to the topic of this book as much as I can; I will reply to every message. I'll take it for granted, but no man-made book on earth is immune to mistakes. Please include the name of the book in the topic of your message to get your answer faster.

Mostafa Moradian

Chapter 4

Getting started

The packet filtering has been with Linux kernel since version 1.1. It was first ported from BSD's ipfw and then enhanced in kernel 2.0 which by then controlled by ipfwadm tool. After then there was a rework which resulted the tool ipchains with many new features for kernel 2.2. The last attempt to rework has been done which then resulted iptables for kernel 2.4 and 2.6 that you are going to know about here.

For the sake of simplicity (or God), they made it modular, so that you can use whatever module you want or you write to control packet filtering by Linux kernel. Modularity is the key to success for iptables which lasted from mid-1999 till now. So there is no need to rework again and again to result a tool which lasts just some years.

There are many times you may use packet filtering, be it security, intrusion, hacking or whatever you call it, which disallows someone from accessing your data. Like it or not, your system is not secure and you should put all your efforts to protect your data if you want them and if they cost you more if they are lost or stolen. Undoubtedly, Linux packet filtering is powerful but no firewall on earth is really secure.

As of any other firewall application, iptables is used to:

- filter packets based on their header information
- pass traffic through (NAT / Masquerade / NAPT)
- modify packet headers

and many more which will be discussed in next chapters.

IPtables is just a tool that controls the Netfilter module which is loaded into Linux kernel by default in most distributions. Also it has the ability to load and

control existing and new modules to control new targets and new matches which are not built-in. The Netfilter is a module that is loaded into kernel for easier implementation of the features of iptables. The iptables' package contains these modules and other executables to manipulate rules and configurations. The IP Connection Tracker module is used to track connections passed through iptables and the sessions in which these connections relate to. There are also many details which will be discussed in following chapters.

This was really a quick introduction to iptables and I'm sure that I've said why I lessen the length of the book. I hope you more security than ever before.

4.1 Summary

Well, you learnt a bit about the history of the iptables. You also learnt how the iptables generally works. The IP connection tracker and the Netfilter are a part of iptables' package. So, you had a bird's eye view on them in order to be introduced later. The general features of iptables' package has also been explored.

Chapter 5

Introduction to TCP/IP Networking

5.1 The TCP/IP Protocol Architecture

Let's scratch some surface. The TCP/IP Protocol Architecture consists of four layers, shown in Figure 2-1.