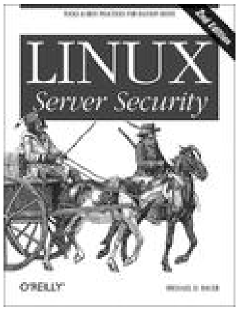
Linux Server Security *by Michael D Bauer*

Martin C Brown



While developed and supported with the best of intentions, Linux is still based on a wide range of different applications and systems working together. From the free software perspective this is its power; many people working together to produce a top quality operating system.

From a security stand point it can also be a curse. Although with full access to the source code you know exactly what different components are doing, the disparate nature of the applications can mean that securing all of the applications and services in Linux is significantly more difficult. For example, securing a web server may involve configuring Apache, transport layer security tools and OpenLDAP. Knowing how to correctly configure each of these units for security, rather than straightforward operation, can be difficult at worst and time consuming at best.

Michael D Bauer addresses this problem in Linux Server Security (O'Reilly), a concise, and yet somehow extensive, guide to configuring your Linux server for security. The book covers everything from network security and firewalling through to specific applications, such as web serving, or email.

> Knowing how to correctly configure each of these units for security, rather than straightforward operation, can be difficult at worst and time consuming at best

The contents

Linux Server Security is organized into what I can only describe as a spiral—it starts by examining the outer layers of your Linux installation and moves further inwards towards protocol and application level security, such as sendmail, OpenLDAP and file sharing.

We start off with a simple look at the mechanics of security with threat modelling and risk management. These are vital steps to take if you are going to secure the rest of your systems. Without knowing the potential for security problems in your systems, how are you going to secure them?

On the way through the rest of the book we go through layer upon layer of security, through DMZs and perimeter networks, iptables and firewalls, remote administration (SSH), transport level security (through OpenSSL and Stunnel) and finally onto the protocol and application techniques such as Email, web servers, databases and file sharing. The book then wraps up with a look at logging and intrusion detection techniques.

Throughout, the book contains full information on the various theoretical and technical details of the steps required. The major difference from some guides is that the book is a practical guide to the steps required to reach the security goals; it is not a book based on pure theory.

It is also very succinct; the book instructs you on how to reach security goals in specific areas, and is therefore a more practical guide to what needs to be done, rather than concentrating on possibilities and theories.

Who's this book for?

I'd be tempted to say that everybody using Linux should read the book, but the realities are that much of the content really applies only to administrators. If you are in this group though, this book should be required reading, regardless of what servers or services you are managing.

Getting your security right at all levels is tricky and this book covers many different aspects. You can use the book in two ways; either use it as a step by step guide to configure and lock down your server or servers, if that's what you wanted. You can also use it as a dip-in guide to securing specific elements of your server.

What I found most useful—as an administrator of Linux—was the ability to use individual chapters of the guide to cover the practical details of exactly what I needed. The theoretical information is useful, and while many of us know the principles well, we just need the mental reminders for specific utilities, command line options and configuration options that enable us to do exactly what we need.

It's also worth mentioning that although the book is Linux focused, many of the principles and much of the content of the book would be just as valid to any Unix-based administrator

Pros

The best aspect of the book is its scope. It covers the whole gamut from simple network security through firewalls down to protocol and application specific systems. I liked, for example, the specific chapters on securing DNS, email, database and web services, along with the more traditional file systems and other systems common in books of this type.

The last two chapters also helped to fill in another commonly ignored area—monitoring and detecting security issues. Setting up the security is often relatively simple compared to actually tracking and detecting unwanted activity. These two chapters do an excellent job of wrapping up the content of the book.

Cons

The focus on security means that some of the simpler steps are skipped. For example, in the OpenLDAP chapter there is all the information you need to set the system up for security, and for securing LDAP transactions using Transport Layer Security, but you are expected to get OpenLDAP up and running by yourself first. This is not a major complaint, this isn't, afterall, a beginners book, but OpenLDAP is not the easiest of systems to get working, and as a major component of many security installations it would have been nice to have a bit more detail on the process.

In short

Title	Linux Server Security
Author	Michael D Bauer
Publisher	O'Reilly
ISBN	0596006705
Year	2005
Pages	522
CD included	No
Mark	9

The major difference between this book and some other guides is that this book is a practical guide to the steps required to reach the security goals; it is not a book based on pure theory

Copyright information