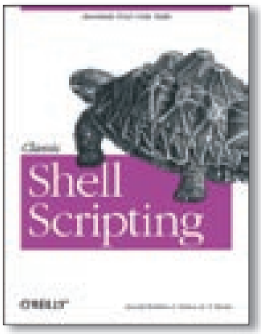
BOOK REVIEWS

BY JAMES MOHR

Classic Shell Scripting



When I came across *Classic Shell Scripting*, by Arnold Robbins and Nelson H.F. Beebe, my first reaction was "Oh, no! Not another book on shell programming." When I started reading it, my reaction was *still* that this was "just another book on shell programming." Still, something was different.

If you glance through the table of contents, you will find the same topics you'll find in other shell programming books. For example, there are chapters on text processing, pipes, flow control, file access, and so forth. Even with the addition of several chapters on "non-traditional" topics, like process management, portability, and secure shell scripts, this appears at first glance to be a YASPB (Yet Another Shell Programming Book).

Once you get into the meat of the book, though, things change dramatically. This book goes beyond the basics of writing shell scripts. It discusses not only how to write good scripts, but also covers how scripts (and the shells themselves) behave, as well as how they interact with other aspects of the system.

The book provides two appendices, one on writing manpages and one on files and file systems. Initially, these topics seems out of place, but they provide very useful information for script writers. If you want (or need to) provide documentation for your script in the form of a manpage, the first appendix will get you started. The second appendix covers the issue of files and file systems in terms of how they relate to shell scripts. Some of the information (like file permissions) may be "common knowledge," but I found this section to be a very useful resource.

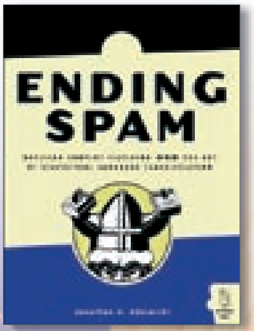
Discussing everything I like in this book would require a lot more space than I have. In essence, I can say that this books addresses all of those things that are missing from other books and more.

Arnold Robbins and Nelson H. F. Beebe
534 pages
O'Reilly Media, 0-596-00595-4
£ 24.95 UK, US$ 34.95, EUR 34.00

Ending Spam

Despite reducing incoming spam to less than 5% of what it was six months ago, I am still getting several dozen emails a day that I need to at least look at to make sure they are not something I want. As a result, I appreciate anything that helps me address this problem.

Unfortunately, *Ending Spam* does not give instructions on implementing specific solutions to the problem of spam. In fact, there is very little immediately applicable information. Although I would not necessarily call the information "theoretical," the book is limited to the methodology of fighting spam, as opposed to real techniques for how to configure any specific spam filter.



On the other hand, that's okay with me because I found the book not only enjoyable but actually captivating. It was easy to read, well-written, and full of interesting information. Instead of simply saying "this is how to filter spam," the author discusses different methodologies and addresses pros and cons of the various elements.

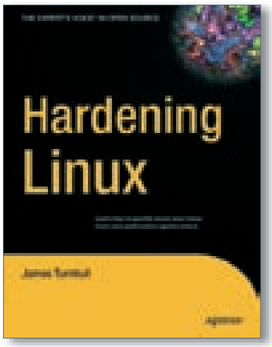
The book starts with a history of spam and goes into techniques of spam prevention, addressing the technical aspects of each topic, plus adding a look at the legal and ethical questions.

I enjoyed the chapter on "The Low-Down Dirty Tricks of Spammers," where the author describes a number of popular spamming methods. Other chapters include discussions of language classification, which is used to identify email based on its content, rather than on specific rules. This topic continues with a discussion of the process of "statistical filtering," whereby the email is given a "score." The higher the score, the greater the likelihood the message is spam. There is also a discussion of the steps spammers take to avoid detection.

The author also addresses a few administrative topics, such as data storage requirements in fighting spam, spam filtering in large environments, and methodologies for testing spam filters. If you are interested in strategies for fighting spam, this book is definitely worth a look.

Jonathan Zdziarski
287 pages
No Starch Press, 1-59327-052-6
£ 27.99 UK, US$ 39.95, EUR 36.50

Hardening Linux



The security of Linux systems is (or at least should be) a concern for every system administrator. There are so many books on the subject that it is hard to tell which to buy. Many books are rehashes of the same old stuff or are simply "theoretical," in that they fill you up will all sorts of information about security but never tell you what to do with it. That's where *Hardening Linux* comes in.

The book starts off with a chapter called "Hardening the Basics," which covers those areas that almost all administrators think about, such as user accounts, system services, kernel patches, and so forth. Subsequent chapters cover topics including firewalls, security of remote connections, file system security, system logging and monitoring, as well as three entire chapters on email. Considering that email is the most frequently used Internet service, and that email can cause a lot of harm if overlooked, I felt this emphasis was appropriate.

This is definitely a "hands-on" book. Each section describes programs to use and files to edit, but without overloading you with too much background information. What background information is provided is just enough to show why the topic is important before the author jumps into the nitty-gritty.

One thing I really enjoyed was that the author did not stick to just one Linux distribution. In places where commands or files are different, he makes explicit note of that fact and tells you where to look for more information. Obviously, not every distribution can be covered, but the major distributions Suse, RedHat, and Debian are represented.

Setting up a secure configuration is only the first step – you also need to test your system to ensure that the security is working. The author includes a chapter entitled "Using Tools for Security Testing." As the name implies, this chapter covers a range of tools you can employ to check the security of your system.

The only real problem with this book is not the author's fault. There are just too many things you need to address to make your system 100% secure. It would take dozens of books, and the threat, in most cases, isn't worth the effort. Instead, the author has chosen those areas that represent the greatest threats, addressing the problems that get your system to a high level of security much faster.

To say I was impressed with this book is to put things mildly. *Hardening Linux* is a must for any Linux system administrator.

James Turnbull
552 Pages
Apress, 1-59059-44-44
£ 30.99, US$ 44.95, EUR 40.90