BOOK REVIEWS

BY JAMES MOHR

Internet Forensics

Internet Forensics has a lot of very useful information about hidden clues regarding Internet attacks, phishing attempts, and many other unpleasant "events." It is well written and easy to understand, and it gives you the background necessary to start investigating on your own. I definitely recommend it, however, it was still a disappointment.

I was already familiar with most of the topics discussed in the book, so I didn't actually learn very much new material. Sometimes that happens with books covering the basics of a given topic, so this is not a disappointment in and of itself. What disappointed me was the fact that the book *stopped* with the basics. I found myself often reading a section with growing excitement, only to text to cut too short and too soon.

I also felt that the book spent too much time on irrelevant topics, such as dissecting Microsoft Word and PDF files.

Although Word and PDF files *can* be found on the Internet, and you *can* use "forensic" techniques and procedures to extract otherwise hidden information, I felt that talking about this topic was out of place, particularly at the depth the author discussed this subject. (The discussion took up about 10% of the book.) I felt the limited number of pages provided should would have been better spent going into more depth about other topics.

If you have been running your own Internet server for a while, it very likely that you have already needed the information in this book. If you have had to do the research on your own to figure out how to analyze web logs, email headers, and so forth, you might not get much out of this book. However, if you are just starting out or have simply ac-

cepted the fact your server is going to be a victim of various assaults, you will definitely get something out of this.
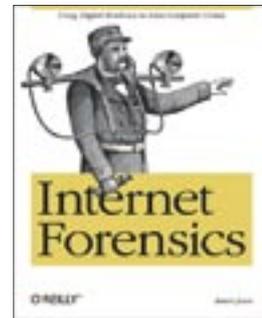
I really don't want to come across completely negative about this book. In fact, I actually recommend it highly. With all that said, I wish that O'Reilly would come out with a second edition – not to simply update the material, but to **expand** it. This could be a truly great book if the author would simply take the material one step further.

Robert Jones
223 pages
**O'Reilly Media, Inc.,**
0-596-10006-X
£ 28.50, US$ 39.95, EUR 36.90

Spring Into Linux

If you were to "spring" into a pool as shallow as this book in the manner depicted on the cover, you would most definitely break your neck.

If you get this book, you will probably learn *about* Linux, but don't expect to "learn Linux," even though the marketing departments says, no other books covers this amount of material.

Despite my distaste for certain misleading marketing decisions, this is overall a good book. The author has an enjoyable writing style, the examples are easy to follow, and you do actually learn a fair bit about the topics. For a user who has very little Linux experience, then this can be very useful.
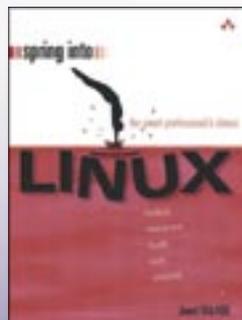
One of the key aspects I really liked was that the material was broken in to fairly small bite-sized chunks. Each issue is covered in one or two pages and you shouldn't have a problem doing what is expected after reading it. Although, this meant that some background information was skipped, I felt it was actually a benefit for those people who are trying to get to the point where they can work with Linux instead of trying to pass a Linux certification.

While I might have personally chosen different topics to cover, I think the author made a good choice of what to include. The book starts with a refreshingly brief introduction to

Linux, GNU, and open source, and it moves quickly to installing the system. Here the author went through the installation process for each of the distributions she discusses. The book then progresses logically from basic interaction with the system through using many of the more common applications.

Despite what the cover says, reading this book is **not** the "fastest route to true Linux mastery." However, *Spring Into Linux* is a great way of getting yourself to a place where you can work effectively with Linux.

Janet Valade
336 pages
Addison-Wesley,
0-13-185354-6
£ 21.99, US$ 29.99, EUR 27.90

Time Management for System Administrators

On the one hand, the subject of this book is almost trivially obvious. On the other hand, it is a stroke of genius. Personally, I often think that being simply disorganized would be an *improvement*, so I have read a couple of books on time management and tried several different methods. I *might* be tempted to say that if you are already using some methodology to manage your time, you might not get much out of this book. However, I was using a methodology I got from a different book and decided this one is for me.

Although what I was doing before is neither bad nor ineffective, the methodology was developed by someone other than a system administrator. Admittedly, the environment the author describes does not match mine 100% (and probably does not match yours completely, either). There are a few aspects of my job where I had to extrapolate what he said, but there were also a number of places where I could take pride in the fact that I was already doing it "right."

It was refreshing to see that, like me, the author still uses an "old-fashioned" time management system consisting of paper and pens. Although we have a groupware tool at work, I am more comfortable with a notebook. The nice thing is that the methodology dis-cussed is essentially independent of whether you have a PDA or pen and paper.

One enjoyable aspect is that your get the feeling that the author it actually talking to you and not simply spouting off his philosophy. There are several places were he *insists* you stop reading to carry out the task he is discussing. Each chapter ends with a bullet-list summary, covering the points discussed making for an quick and easy review.

The book goes beyond simply using a time management tool to keep track of appointments and ToDos. The last part of the book covers a number of different ways to implement the technology you administer to simplify that administration. Although this covered about a quarter of the book, my only wish is that the author could have expanded that particular topic – something for the next edition, I guess.

Bless you, Tom!

Thomas A. Limoncella
200 pages
O'Reilly Media, Inc.,
0-596-00783-3
£ 17.50, US$ 24.95,
EUR 28.90

THE AUTHOR

James Mohr is responsible for the monitoring of several datacenters for a business solutions provider in Coburg, Germany. In addition to running the Linux Tutorial website *http://www.linux-tutorial.info,* James is the author of several books and dozens of articles on a wide range of topics.