# book reviews

RIK FARROW

*rik@spirit.com*

## GOOGLE HACKS, 2ND EDITION

*Tara Calishain and Rael Dornfest*

O'Reilly, 2005, 0-596-00857-0, 443 pp.

When the first edition of *Google Hacks* came out, I ignored it. Sure, I thought I would learn something from the book, but Google seemed pretty easy to use as is. Then I heard Johnny Long (http://johnny.ihackstuff.com) talking about penetration testing using Google. Long opened my eyes to a lot of Google potential that I had been missing, and now I wanted to learn more.

This is not a review about Google Hacking for Penetration Testers. That book hasn't arrived yet (but I did ask for a copy). What showed up first was the second edition of *Google Hacks*, which seemed like a good place to start learning more about Google. And it is.

The first 28 pages cover the "basics" of Google, including useful special syntax such as site:, inurl:, and define:. Did you know you can include number ranges in your searches? Some of this information is so easy and useful, searching will never be the same.

But what are the other 415 pages for? The hacks in this book often require some programming, as hacks should. Unlike some recent O'Reilly books, this one is mostly for UNIX users, and it is useful to have not only Perl but also Python and PHP installed. If you want to try all the hacks, you will also need Java and .Net. And, yes, there are one or two hacks that will work only on Windows, and other things that work only if you have a Web server that can run scripts.

Why bother programming when you can just use the interfaces Google provides you? You can use Advanced Search or choose a date range for your search. Or you can instruct the Google search engine to include only pages indexed within a certain time period—but you must use Julian dates if you want to do so. A bit of Perl programming makes using Julian dates trivial to do.

Many hacks are pretty fanciful, such as a grid search, a popularity contest, Google mindshare, or finding a recipe to match the ingredients you have in your refrigerator. But there is lots of useful stuff, including an entire chapter about using the Google API, Gmail, how Google PageRank works, and adding Google searches to your own Web sites. If you are interested in improving the accuracy of your searches, or just want to have fun with Google, this book is a bargain.

## KNOPPIX HACKS

*Kyle Rankin*

O'Reilly, 2005, 0-596-00787-6, 314 pp. + CD.

Ever wanted to turn someone on to Linux but shied away from having to take responsibility for supporting the installation? Instead of taking the plunge, just hand someone a copy of Knoppix on a CD (knoppix.net), and—as long as they have an i386-based system that can boot from the CD-ROM—they can experience Linux without installing it. Note that there are versions of Knoppix for some other architectures as well.

*Knoppix Hacks* is not for the casual explorer but for someone who wants to understand how to get the most out of Knoppix, because Knoppix is a lot more than a demo CD. I have been using Knoppix to teach my hands-on Linux security class for a year now. I customize my version of Knoppix by removing some packages and adding class exercises. When I first started doing this, I had to piece together the methods for working with Knoppix. This book provides details about creating your own custom Knoppix distribution in the final group of hacks. Wish I had had this a year ago.

Knoppix out-of-the-box is a fine toolbox. You can use it to replace lost passwords (including on Windows systems, with a downloaded utility), replace or fix boot loaders, repartition a system, and even recover a master boot block (as long as you don't use extended partitions). Knoppix can be a terminal server, DNS server, DHCP server, NFS server, Samba server, or Web server. Knoppix can also be used to rescue unbootable Windows systems through a registry edit or recovery of a CAB file.

*Knoppix Hacks* provides the information you need to make the most out of Knoppix. Without it, you would be hard pressed to discover all you can do with Knoppix. The book comes with an older version of a Knoppix CD (3.4), but even so, think of it as the perfect gift for a talented sysadmin, whether she works with UNIX or Windows.

## FORENSIC DISCOVERY

*Dan Farmer and Wietse Venema*

Addison-Wesley, 2004, 0-201-63497-X, 217 pp.

*Forensic Discovery* is a book you must have if you are seriously interested in computer security. Farmer and Venema take you on a journey that covers just about anything that might remain in a computer as a result of an intrusion or other activity. Unlike other forensics books, the focus is not on finding evidence that can stand up in court. Instead, the authors

explore uncovering all the bits and pieces that might still be around months or years after an incident.

Farmer and Venema carefully lay the foundation for their methods of discovery. They explain booting, kernel initialization, system startup, file system details, process details, and examining malware in safety. They also dig deep into file systems, uncovering information about deleted files and information cached by journaling file systems. They offer thorough explanations that make it much easier to understand those normally ignored structures that underlie all modern file systems, yet are critical in forensics. Ever wonder just how long deleted data stays on UNIX systems? The authors explore persistence of data on disk and in memory through experiments, using real systems with different activity profiles to determine just how long data, or signs of intrusion, can remain in a system. The authors also discuss why uncovered data may only poorly represent the past, either because of normal system activity or active attempts at deception by miscreants.

While this book uses some of the tools developed as part of the Coroner's Toolkit, it is not a book about those tools. Rather, it is a serious exploration of how modern operating systems work in practice, what types of information get stored, how this information is stored, and techniques for retrieving and making sense of that data. The writing flows smoothly and clearly, with occasional geek humor, making this book easy to read and very accessible.

Even if you do not focus on security, you might want to read this little book just so you can have a better understanding of the systems you use and manage daily. The authors focus mainly on Solaris, Linux, and the BSDs. While Windows gets mentioned in passing, this is not a book for MSCEs. I highly recommend *Forensic Discovery* and am very glad it has finally been published.