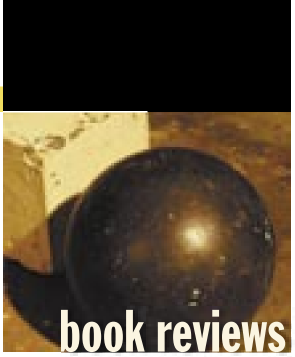
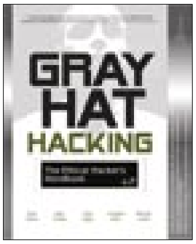


Gray Hat Hacking: The Ethical Hacker's Handbook

Shon Harris, Allen Harper, Chris Eagle,
Jonathan Ness, Michael Lester
McGraw-Hill Osborne Media, 2004, $49.99
ISBN: 0072257091



Few books are able to capture the reader's attention to the point where putting the book aside becomes an impossibility, while, paradoxically, the reader wishes it would never end and that there would be always be a page to read the next day. This is that kind of book.

Gray Hat Hacking combines a highly pedagogical approach with advanced knowledge of security vulnerability, discovery, and exploitation. The process of discovering and exploiting security vulnerabilities is a multiphased one: first, a series of laws must be considered and addressed, to avoid legal prosecution. Next, a network must be scanned, and potentially vulnerable machines detected. The final phase is exploitation, where vulnerable applications are injected with user-controlled data, and the underlying machine is "owned." These phases are common to both black hats and professional penetration testers, hired for assessment and testing purposes. The authors describe all of these phases in great detail.

The first part of the book reviews the most important laws that a professional penetration tester should know. The second part is highly technical, going from network scanning and fingerprinting to shellcode (machine code injected to detour the regular application) writing and vulnerability exploitation. The authors present both passive and active fingerprinting methods and illustrate their use with real network traces. Writing shellcode is a complex task, requiring a good knowledge of assembly programming and operating systems' innermost functions, as well as practical experience in application debugging.

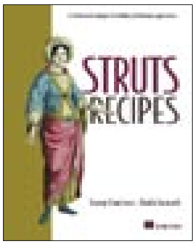
The book is self-contained and includes a brief introduction to most of the topics it covers. The novice reader, however, might have to look elsewhere for additional information.

In addition, *Gray Hat Hacking* covers the writing of exploits, addressing the essentials that you should know: buffer overflows for both Linux and Windows platforms, heap overflows, and format string overflows. I was very pleasantly surprised to discover that the authors also go into some detail about some lesser-known vulnerability detection methods, such as "fuzzing," reverse engineering, and commercial tools (including Core Impact and Canvas).

The authors have written an excellent, highly technical, and informative book. It sets a new standard for pedagogical quality and writing style, and I recommend it to any reader interested in learning how security penetration is done.—*Radu State*

Struts Recipes

George Franciscus, Danilo Gurovich
Manning Publications, 2004, $44.95
ISBN: 1932394249



This book addresses the real issues faced by developers building Web applications using the Struts open framework. Based on the famous MVC (model-view-controller) design pattern, this framework provides a clean separation of different roles in the development process. Most of the literature on Struts discusses the mechanics of the framework and other generic issues. This book is unique in that it addresses the real-life issues, scenarios, and challenges faced by developers, and it provides satisfactory solutions to most of these problems in the form of what the authors call "recipes."

The nine chapters cover major issues faced by developers. Chapters 1 through 3 cover Struts basics, such as forms and libraries; chapters 4 through 9 address validation, internationalization, security, and testing. Each chapter has a specific format, including sections covering the background, problem, recipe, and discussion. The authors also provide extensive code, which is helpful in understanding these recipes.

The authors have done a good job of compiling the most representative real-life scenarios and best practices in this practical book. They have successfully presented their content, with full meaning and purpose, in a reasonable number of pages. Long awaited by Struts practitioners, this is an excellent addition to the Struts literature. I strongly recommend it to the whole Struts user community.—*Sajjad Khan*

Reprinted from *Computing Reviews*, © 2005 ACM, http://www.reviews.com