Editors: Martin R. Stytz, mstytz@att.net
Shari Lawrence Pfleeger, pfleeger@rand.org
Chuck Pfleeger, c.pfleeger@computer.org

BookReviews

A Framework to Consider

Roy Iversen
Xacta Corporation

Reviewed in this issue:

James S. Tiller, *The Ethical Hack: A Framework for Business Value Penetration Testing*, Auerbach Publications, 2003, ISBN 0-8493-1609-X, 322 pages, US$69.95.

Although the military has used ethical hacking—also known as penetration testing (testing your own computer infrastructure for vulnerabilities)—to test its computer systems for decades, only in recent years has the method become mainstream. In *The Ethical Hack: A Framework for Business Value Penetration Testing*, James Tiller details a framework you can use to plan, coordinate, execute, and analyze an ethical hack, and describes the steps you should follow when you've finished the testing.

Now that the topic of computer security has become so popular, numerous books about security testing have emerged. Traditionally, those focusing on ethical hacking have been both technical and specific, explaining how you'd attack a Web server, exploit software, operate network scanners, or find wireless access points. This approach, although valid, is doomed to rapidly become outdated because products, versions, vulnerabilities, and attack tools change frequently.

This book differentiates itself by presenting a structured approach to testing an organization's security. Tiller steps back and discusses all facets of a successful test. He first explains ethical hacking, hackers and the threats they pose, as well as security models and programs. After defining the framework, he devotes the rest of the book to more deeply exploring its eight steps: planning, operations, reconnaissance, enumeration, analysis, exploitation, deliverable, and integration. Each chapter discusses common challenges, such as "Who should be informed of the tests?" and "How much testing is enough?" The author also explores other interesting issues, such as what legal documents should be in place before testing can commence. The framework lets readers customize each test, ensuring that their organization or client will get the greatest value from it.

Tiller's writing style makes the book easy to follow, and he uses plenty of real-world examples. Having worked in the industry for a while, I've seen many examples of how *not* to conduct an ethical hack; Tiller describes common pitfalls and presents examples of penetration tests that have little or no real value for the organization being tested. Only the final chapter, "Integrating the Results," was a bit lacking, as it only touched on topics such as setting up a CERT and performing architecture reviews. However, given that this book focuses primarily on penetration testing rather than preventative measures, the section is adequate because it directs the reader to other important areas beyond its core topic.

The Ethical Hack: A Framework for Business Value Penetration Testing isn't too technical, nor should it be. The ideal reader is a CSO or CIO, a manager in charge of an IT system, or a project lead for penetration testing. Additionally, ethical hackers and some developers who read this book will better understand what their clients will expect or what their products will need to stand up to. The book isn't meant to replace technical reference books, such as the *Hacking Exposed* series (McGraw-Hill); rather, it complements them. Although it's not devoid of technical terms, readers without a deep technical understanding of networks shouldn't have any problem understanding it, as Tiller defines any technical terms used. And while security vulnerabilities constantly change, the framework that Tiller describes will remain valid because security's fundamental aspects will change slowly. □

__Roy Iversen__ is a certified information systems security professional (CISSP) and a senior security analyst for Xacta Corporation, an information security management and solution provider. He wrote his master's thesis on the quantification of penetration testing results. He received his master's degree in computer and information science from the Norwegian University of Science and Technology. Iversen is a member of the High Technology Crime Investigation Association and the Project Management Institute. Contact him at security@iversen.tv.