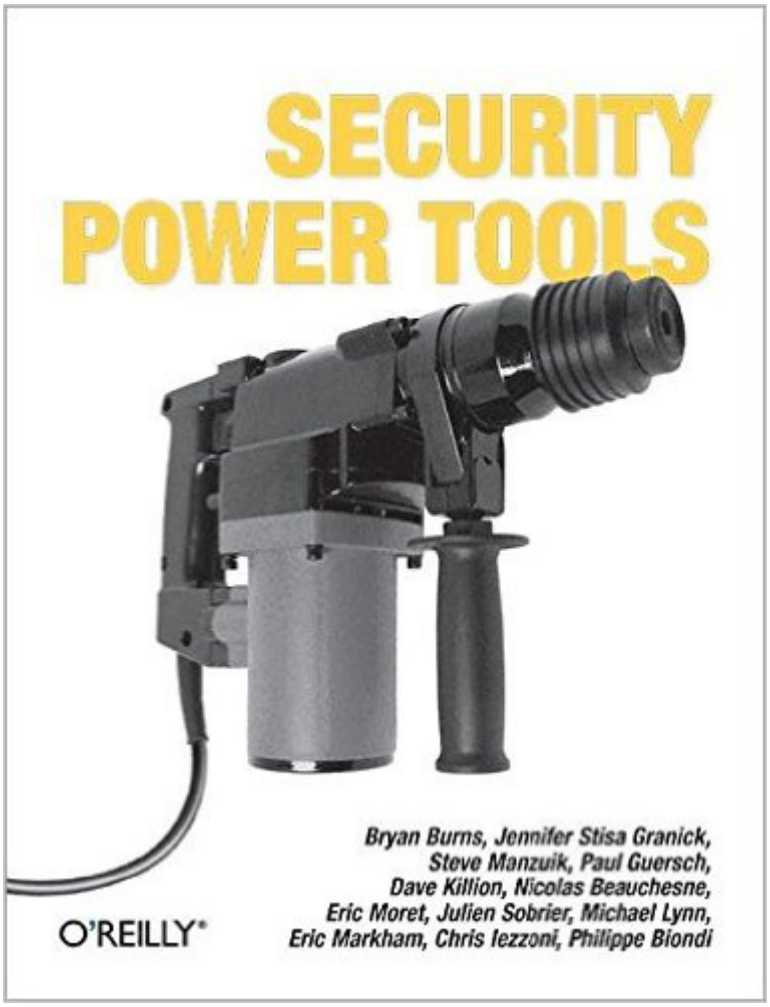
Security Power Tools



Synopsis

What if you could sit down with some of the most talented security engineers in the world and ask any network security question you wanted? Security Power Tools lets you do exactly that! Members of Juniper Networks' Security Engineering team and a few guest experts reveal how to use, tweak, and push the most popular network security applications, utilities, and tools available using Windows, Linux, Mac OS X, and Unix platforms.Designed to be browsed, Security Power Tools offers you multiple approaches to network security via 23 cross-referenced chapters that review the best security tools on the planet for both black hat techniques and white hat defense tactics. It's a must-have reference for network administrators, engineers and consultants with tips, tricks, and how-to advice for an assortment of freeware and commercial tools, ranging from intermediate level command-line operations to advanced programming of self-hiding exploits.Security Power Tools details best practices for:Reconnaissance -- including tools for network scanning such as nmap; vulnerability scanning tools for Windows and Linux; LAN reconnaissance; tools to help with wireless reconnaissance; and custom packet generationPenetration -- such as the Metasploit framework for automated penetration of remote computers; tools to find wireless networks; exploitation framework applications; and tricks and tools to manipulate shellcodesControl -- including the configuration of several tools for use as backdoors; and a review of known rootkits for Windows and LinuxDefense -- including host-based firewalls; host hardening for Windows and Linux networks; communication security with ssh; email security and anti-malware; and device security testingMonitoring -- such as tools to capture, and analyze packets; network monitoring with Honeyd and snort; and host monitoring of production servers for file changesDiscovery -- including The Forensic Toolkit, SysInternals and other popular forensic tools; application fuzzer and fuzzing techniques; and the art of binary reverse engineering using tools like Interactive Disassembler and OllydbgA practical and timely network security ethics chapter written by a Stanford University professor of law completes the suite of topics and makes this book a goldmine of security information. Save yourself a ton of headaches and be prepared for any network security dilemma with Security Power Tools.

Book Information

Paperback: 860 pages
Publisher: O'Reilly Media; 1 edition (September 6, 2007)
Language: English
ISBN-10: 0596009631
ISBN-13: 978-0596009632

Product Dimensions: 7 x 1.9 x 9.2 inches

Shipping Weight: 3 pounds (View shipping rates and policies)

Average Customer Review: 4.4 out of 5 starsÂ Â See all reviewsÂ (13 customer reviews)

Best Sellers Rank: #746,859 in Books (See Top 100 in Books) #181 inÂ Books > Computers & Technology > Certification > CompTIA #449 inÂ Books > Computers & Technology > Security & Encryption > Privacy & Online Safety #661 inÂ Books > Computers & Technology > Networking & Cloud Computing > Network Security

Customer Reviews

I am probably the first reviewer to have read the vast majority of Security Power Tools (SPT). I do not think the other reviewers are familiar with similar books like Anti-Hacker Toolkit, first published in 2002 and most recently updated in a third edition (AHT3E) in Feb 2006. (I doubt the SPT authors read or even were aware of AHT3E.) SPT has enough original material that I expect at least some of it will appeal to many readers, justifying four stars. On the other hand, a good portion of the material (reviewed previously as "the most up-to-date tools") offers nothing new and in some cases is several years old.I'll begin with my favorite sections. SPT started very strongly with Jennifer Grannick's chapter on law as it pertains to security issues. She is an excellent writer and I would like to see her create her own book on the same subject. I liked Philippe Biondi's work in Ch 6 (Custom Packet Generation) although his coverage of Scapy (while great) is not for the beginner. (Just try as many examples as you can -- Scapy is cool.) Ch 7 (Metasploit) provided a great discussion of Metasploit 3; I learned quite a bit. I was pleasantly surprised by Ch 15 (Securing Communications). It was very practical. I should mention that some of the chapters appeared to be good, but they were outside my expertise and beyond my skill level. These included Ch 10 (Custom Exploitation), Ch 22 (Application Fuzzing) and Ch 23 (Binary Reverse Engineering). I was initially inclined to skip the section on BO2k in Ch 11 (Backdoors), but I didn't know the tool had been updated in Mar 07 and could be considered "viable" in the age of botnets.Readers may also like SPT because it mixes coverage of open source and commercial tools.

Security Power Tools (SPT) is O'Reilly Publishing's sister manual to their popular Unix Power Tools [â ‖]. It is written as a primer to various security tools, organized within seven sections, covering Legal and Ethics, Reconnaissance, Penetration, Control, Defense, Monitoring, and Discovery. While the target audience of SPT is security professionals, the book weighs in at just over 800 pages and probably has something for everyone working in a technical facet of IT.Having said that, I really

enjoyed reading this book. I read it nearly cover-to-cover, and while I was at least familiar with most of the material in the book, I was still able to find gems of knowledge, even in tools that I work with on a daily basis. Expect to read about some tools that you may already know about, like Nmap, Nessus, and The Metasploit Framework, but keep reading for a heap of other useful applications that you may not be familiar with.One of the strengths of the book is the varying backgrounds of its contributing authors; just as the book covers a diverse tool set, the expertise of the authors is also diverse. The book was written collaboratively by twelve individuals, made up primarily of Juniper Networks' J-Security team [â ‖]. Despite an opportunity for vendor-bias towards Juniper products, the book remained vendor-neutral. The majority of the book focuses on open-source and free-ware applications, although there is commercial software covered as well. In fact, Chapter 9 - Exploitation Framework Applications covers Canvas [â ‖] and Core Impact [â ‖] exclusively; both commercial applications.One of the chapters that makes this book unique is the chapter on Law and Ethics, written by Jennifer Stisa Granick.

Sp/Cluster Writing Security Tools and Exploits Unix Shell Programming Tools with CDROM (Unix Tools) Cancer Survivorship Coping Tools - We'll Get you Through This: Tools for Cancer's Emotional Pain From a Melanoma and Breast Cancer Survivor