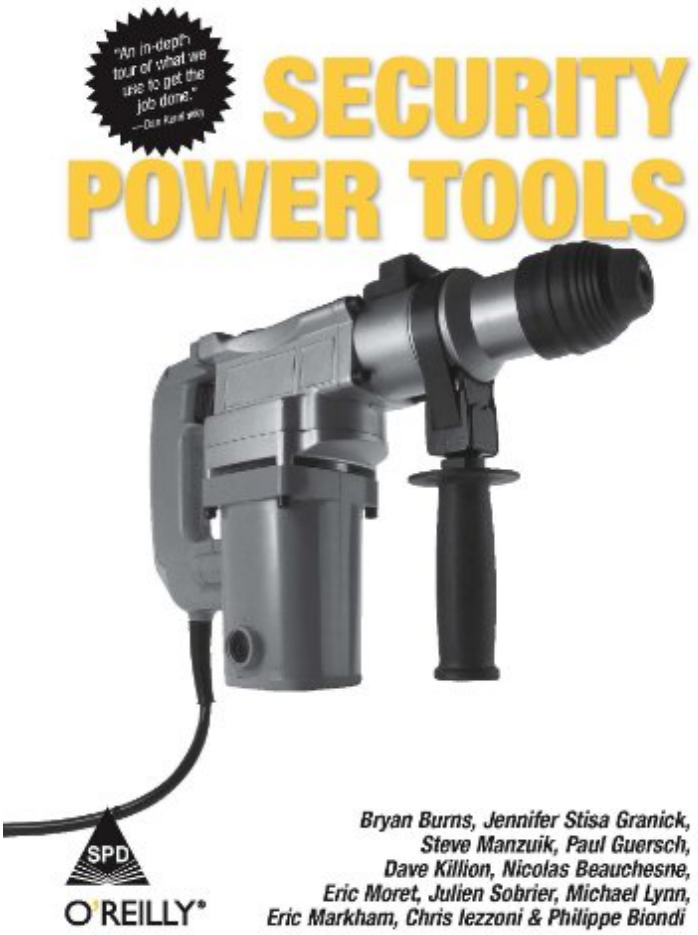
Security Power Tools

Dave Killion, Nicolas Beauchesne Bryan Burns
*ebooks | Download PDF | *ePub | DOC | audiobook*



2007-01-01Original language:English .0 x .0 x .0l, .0 #File Name: 8184043759 | File size: 64.Mb

Dave Killion, Nicolas Beauchesne Bryan Burns : Security Power Tools before purchasing it in order to gage whether or not it would be worth my time, and all praised Security Power Tools:

1 of 1 people found the following review helpful. A solid resource for those interested in learning available toolsBy Gift Card RecipientI am very pleased with this purchase. The explanations and how-to directions are helping me get up to speed on a variety of powerful tools to assess security of a given environment. I recommend this book to others interested in finding out how secure their networked environments really are.7 of 8 people found the following review helpful. More than a mere collection of tools...By R. S. Shyaam SundharI guess there is a misconception in the field of pentesting that everything is about tools. People started considering pentesting as mere collection of tools. This books is not about that. This book does not only help with knowing the various tools, it helps you to understand them, to tune them according to your need or your customer's need. The real skill is not to write a tool of your own when you already have the same tool out there. The real skill in this field is to take an existing tool and modify it based on your need.21 of 22 people found the following review helpful. Everyone will find at least one chapter to likeBy Richard

BejtlichI 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. For example, Ch 9 (Exploitation Framework Applications) covers CORE IMPACT and Immunity CANVAS. Ch 3 (Vulnerability Scanning) describes WebInspect. Ch 17 (Device Security Testing) describes Traffic IQ Pro. Other commercial tools are mentioned in SPT but these were covered with more than a cursory overview.The major problems I had with SPT involved indications of old material and lack of originality. Ch 20 (Host Monitoring) doesn't include any URLs for the tools it mentions. Tool versions are incredibly out-of-date, with references to 2006 or even 2005, despite versions from early 2007 (pre-publication) being available. (Examples: Afick 2.10-1, 17 May 07; Samhain 2.3.4, 1 May 07; Tripware Open Source 2.4.1.2, 18 Apr 07). Ch 19 (Network Monitoring) mentions ACID as a Snort console; BASE replaced ACID in Sep 04! The script to download and update Snort rules uses snortrules.tar.gz, which also (besides not working now) dates it to late 2004. Ch 22 says @Stake's WebProxy is a great tool, but it's been unavailable for several years. Ch 23 mentions SoftIce, but it was discontinued in Apr 06. (Unfortunately the same chapter neglects covering PaiMei "since it will probably change" -- although the Web page lists 22 May 07 as the last update.) Ch 2 (Network Scanning) lists PortSentry, but that tool hasn't been supported since '03 and is now replaced by Mike Rash's Psad. Ch 13 spends a lot of time talking about IPFW as a BSD firewall, even though Pf has been the preferred tool for several years. Ch 5 (Wireless Reconnaissance) seems to ignore that AirPcap is a viable solution for wireless sniffing on Windows. Ch 21 (Forensics) offered absolutely nothing new or advanced.Overall, you will probably find something to really like about SPT. I would take a much different approach in the future. Trying to coordinate so many authors probably resulted in some authors finishing their sections in late '05 or early '06. They waited until the remainder finished so the book could be published in Aug 07. I am not convinced another mammoth book is needed -- maybe smaller books on focused topics would be worthwhile. I would also not bother to cover tools addressed elsewhere --especially in other O'Reilly books.