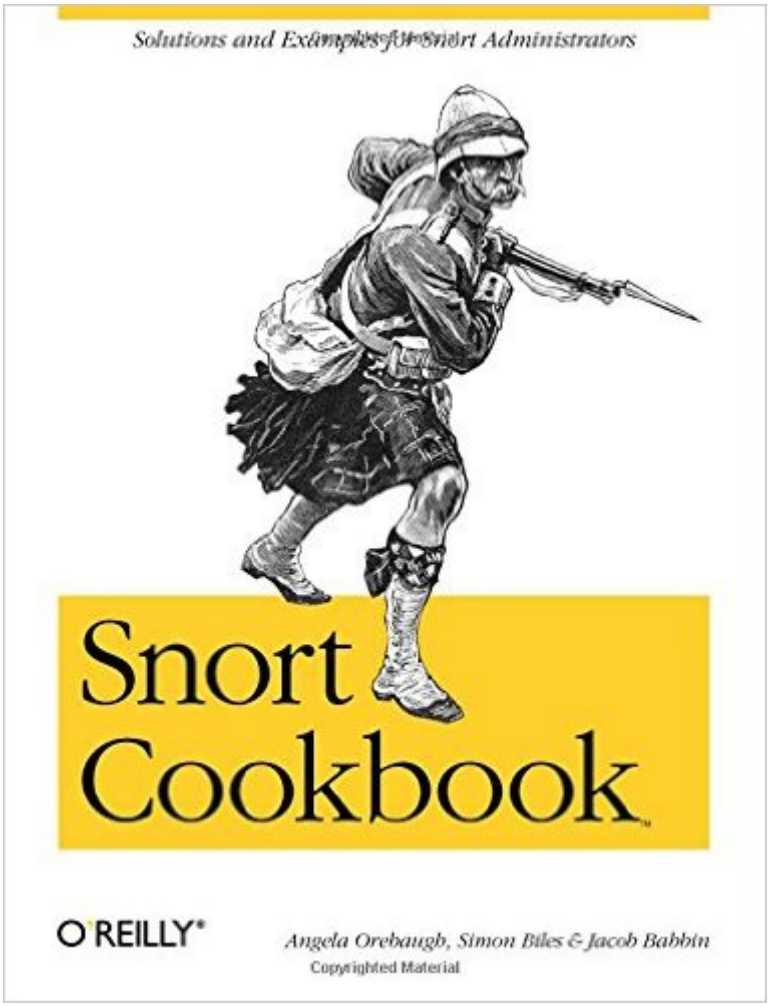
Snort Cookbook



Synopsis

If you are a network administrator, you're under a lot of pressure to ensure that mission-critical systems are completely safe from malicious code, buffer overflows, stealth port scans, Smb probes, Os fingerprinting attempts, Cgi attacks, and other network intruders. Designing a reliable way to detect intruders before they get in is an essential--but often overwhelming--challenge. Snort, the defacto open source standard of intrusion detection tools, is capable of performing real-time traffic analysis and packet logging on Ip network. It can perform protocol analysis, content searching, and matching. Snort can save countless headaches; the new Snort Cookbook will save countless hours of sifting through dubious online advice or wordy tutorials in order to leverage the full power of Snort.Each recipe in the popular and practical problem-solution-discussion O'Reilly cookbook format contains a clear and thorough description of the problem, a concise but complete discussion of a solution, and real-world examples that illustrate that solution. The Snort Cookbook covers important issues that sys admins and security pros will us everyday, such as:installationoptimizationloggingalertingrules and signaturesdetecting virusescountermeasuresdetecting common attacksadministrationhoneypotslog analysisBut the Snort Cookbook offers far more than quick cut-and-paste solutions to frustrating security issues. Those who learn best in the trenches--and don't have the hours to spare to pore over tutorials or troll online for best-practice snippets of advice--will find that the solutions offered in this ultimate Snort sourcebook not only solve immediate problems quickly, but also showcase the best tips and tricks they need to master be security gurus--and still have a life.

Book Information

Paperback: 400 pages

Publisher: O'Reilly Media; 1 edition (April 8, 2005)

Language: English

ISBN-10: 0596007914

ISBN-13: 978-0596007911

Product Dimensions: 7 x 0.7 x 9.2 inches

Shipping Weight: 15.5 ounces (View shipping rates and policies)

Average Customer Review: 4.0 out of 5 starsÂ Â See all reviewsÂ (5 customer reviews)

Best Sellers Rank: #696,759 in Books (See Top 100 in Books) #73 inÂ Books > Computers & Technology > Networking & Cloud Computing > Network Administration > Email Administration #131 inÂ Books > Computers & Technology > Hardware & DIY > Internet & Networking #148

inÂ Books > Computers & Technology > Networking & Cloud Computing > Intranets & Extranets

Customer Reviews

I read the Snort Cookbook because I am always trying to learn more about Snort. I've read almost every book on the open source intrusion detection system, so I hoped the Snort Cookbook might offer advice not found elsewhere. Unfortunately, whatever good material appears in the book is overshadowed by outdated or outright bad advice. The best Snort book is still Syngress' Snort 2.1, so I recommend reading that title.The Snort Cookbook starts poorly with ch 1, which at 50 pages is the book's largest. After repeating installation instructions covered in online resources, the book turns to dubious packet collection recommendations. Item 1.10 suggests creating a listen-only Ethernet cable but never mentions disabling ARP traffic with ifconfig's -arp option. Item 1.11 describes how to build a homebrew tap but doesn't address signal regeneration problems that could result in traffic loss.Item 1.12 gives terrible advice: "If your Snort machine has only one network interface, using the passive tap, run both lines to a small hub. Then from another port of the hub, run a cable to your IDS. This will combine and maybe even buffer the traffic for the IDS and give a full duplex connection." Wrong -- this is a nice way to never see traffic when full-duplex packets from the two transmit lines collide in the hub.Item 1.14 says "Snort itself is incapable of sniffing a wireless network," but it ignores the fact that while Snort doesn't understand 802.11 traffic, the sensor can join a wireless network and interpret what it sees. Item 1.15 demonstrates more ignorance of hardware issues by saying "Linux-compatible gigabit Ethernet cards are available with up to six ports.

Christmas in the Country Cookbook (Seasonal Cookbook Collection) Halloween Cookbook: The Worlds Most Spooktacular Halloween Cookbook You Now Want! Autumn in a Jiffy Cookbook: All Your Favorite Flavors of Fall in Over 200 Fast-Fix, Family-Friendly Recipes. (Seasonal Cookbook Collection) Southern Cooking: Southern Cooking Cookbook - Southern Cooking Recipes - Southern Cooking Cookbooks - Southern Cooking for Thanksgiving - Southern Cooking Recipes - Southern Cooking Cookbook Recipes The Ragu Bolognese Cookbook: The Secret Recipe and More ... The Best Cookbook Ever Mediterranean Slow Cooker Cookbook: A Mediterranean Cookbook with 101 Easy Slow Cooker Recipes Pressure Cooker Cookbook: 370 Quick, Easy, and Healthy Pressure Cooker Recipes for Amazingly Tasty and Nourishing Meals (Pressure Cooker, Electric Pressure Cooker Cookbook) Canning And Preserving Cookbook: 100+ Mouth-Watering Recipes of Canned Food: (Canning and Preserving Cookbook, Best Canning Recipes) (Home Canning Recipes, Pressure Canning Recipes) Rice Cooker Recipes - A Low Carb Cookbook - Low Sugar & 1001% Refined Sugar Free - Gluten Free & Diabetic Friendly (Rice Rice Baby - Rice Cooker Cookbook) (Volume 2) The Ultimate Rice Cooker Cookbook: The Best Rice Cooker Recipes Cookbook You Will Find; Over 25 Mouthwatering Rice Cooker Recipes You Will Love! The Unofficial Downton Abbey Cookbook, Revised Edition: From Lady Mary’s Crab Canapes to Daisy’s Mousse au Chocolat--More Than 150 Recipes from Upstairs and Downstairs (Unofficial Cookbook)