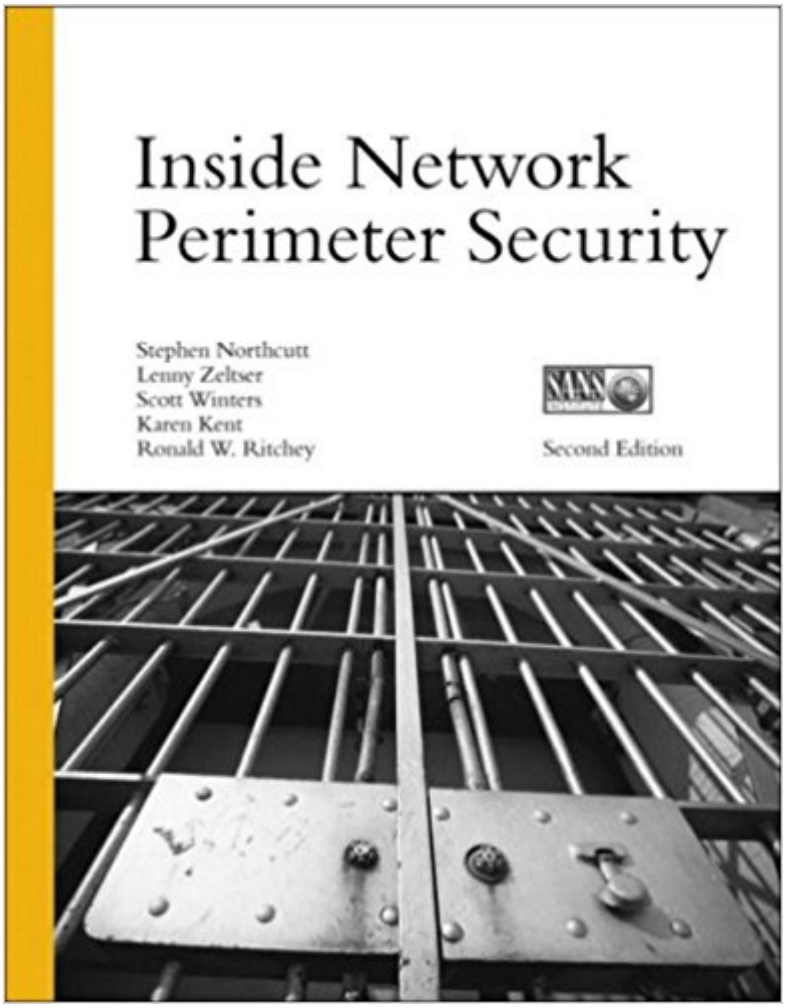
Inside Network Perimeter Security (2nd Edition)



Synopsis

Security professionals and administrators now have access to one of the most valuable resources for learning best practices for network perimeter security. Inside Network Perimeter Security, Second Edition is your guide to preventing network intrusions and defending against any intrusions that do manage to slip through your perimeter. This acclaimed resource has been updated to reflect changes in the security landscape, both in terms of vulnerabilities and defensive tools. Coverage also includes intrusion prevention systems and wireless security. You will work your way through fortifying the perimeter, designing a secure network, and maintaining and monitoring the security of the network. Additionally, discussion of tools such as firewalls, virtual private networks, routers and intrusion detection systems make Inside Network Perimeter Security, Second Edition a valuable resource for both security professionals and GIAC Certified Firewall Analyst certification exam candidates.

Book Information

Paperback: 768 pages

Publisher: Sams Publishing; 2 edition (March 14, 2005)

Language: English

ISBN-10: 0672327376

ISBN-13: 978-0672327377

Product Dimensions: 7 x 1.5 x 8.9 inches

Shipping Weight: 2.6 pounds (View shipping rates and policies)

Average Customer Review: 4.1 out of 5 stars 12 customer reviews

Best Sellers Rank: #166,921 in Books (See Top 100 in Books) #51 inÃ Â Books > Computers & Technology > Certification > CompTIA #110 inÃ Â Books > Computers & Technology > Networking & Cloud Computing > Networks, Protocols & APIs > Networks #190 inÃ Â Books > Computers & Technology > Networking & Cloud Computing > Network Security

Customer Reviews

Security professionals and administrators now have access to one of the most valuable resources for learning best practices for network perimeter security. "Inside Network Perimeter Security, Second Edition" is your guide to preventing network intrusions and defending against any intrusions that do manage to slip through your perimeter. This acclaimed resource has been updated to reflect changes in the security landscape, both in terms of vulnerabilities and defensive tools. Coverage also includes intrusion prevention systems and wireless security. You will work your way through

fortifying the perimeter, designing a secure network, and maintaining and monitoring the security of the network. Additionally, discussion of tools such as firewalls, virtual private networks, routers and intrusion detection systems make "Inside Network Perimeter Security, Second Edition" a valuable resource for both security professionals and GIAC Certified Firewall Analyst certification exam candidates.

Stephen Northcutt is a graduate of Mary Washington College. Before entering the field of computer security, he worked as a Navy helicopter search and rescue crewman, whitewater raft guide, chef, martial arts instructor, cartographer, and network designer. Stephen is author/coauthor of Incident Handling Step-by-Step, Intrusion Signatures and Analysis, Inside Network Perimeter Security, 2nd Edition, IT Ethics Handbook, SANS Security Essentials, SANS Security Leadership Essentials, and Network Intrusion Detection, 3rd Edition. He was the original author of the Shadow Intrusion Detection System before accepting the position of Chief for Information Warfare at the Ballistic Missile Defense Organization. Stephen currently serves as Director of the SANS Institute. Lenny Zeltser's work in information security draws upon experience in system administration, software architecture, and business administration. Lenny has directed security efforts for several organizations, co-founded a software company, and consulted for a major financial institution. He is a senior instructor at the SANS Institute, having written and taught a course on reverse-engineering malware. Lenny is also a coauthor of books such as SANS Security Essentials and Malware: Fighting Malicious Code. He holds a number of professional certifications, including CISSP and GSE, and is an incident handler at SANS Internet Storm Center. Lenny has earned a bachelor of science in engineering degree from the University of Pennsylvania and a master in business administration degree from MIT. More information about Lenny's projects and interests is available at http://www.zeltser.com. Scott Winters has been working in all aspects of networking and computer security for over 14 years. He has been an Instructor, Network Engineer, and Systems Administrator and is currently employed as a Senior Consultant for Unisys at the Commonwealth of Pennsylvania Enterprise Server Farm. He has SANS GIAC Firewalls and Incident Handling certifications, as well as MCSE, CNE, Cisco CCNP, CCDP, and other industry certifications. Other accomplishments include authoring and editing of SANS GIAC Training and Certification course content, as well as exam content. He was a primary author of the first edition of Inside Network Perimeter Security and a contributing author for SANS Security Essentials with CISSP CBK. He has also been involved in the SANS GIAC Mentoring program and has served on the SANS GCFW Advisory Board. Karen Kent is an Associate with Booz Allen Hamilton, where she

provides guidance to Federal agencies on a broad range of information assurance concerns, including incident handling, intrusion detection, VPNs, log monitoring, and host security. Karen has earned a bachelor's degree in computer science from the University of Wisconsin-Parkside and a master's degree in computer science from the University of Idaho. She holds the CISSP certification and four SANS GIAC certifications. Karen has contributed to several books, including Intrusion Signatures and Analysis, published numerous articles on security, and coauthored several publications for the National Institute of Standards and Technology (NIST), including NIST Special Publication 800-61: Computer Security Incident Handling Guide. Ronald W. Ritchey has an active interest in secure network design and network intrusion techniques. He gets to exercise this interest regularly by conducting penetration testing efforts for Booz Allen Hamilton, where he has had the opportunity to learn firsthand the real-world impact of network vulnerabilities. He is also an active researcher in the field with peer-reviewed publications in the area of automated network security analysis. Ronald has authored courses on computer security that have been taught across the country, and he periodically teaches graduate-level courses on computer security. Ronald holds a masters degree in computer science from George Mason University and is currently pursuing his Ph.D. in information technology at their School of Information Technology and Engineering. His doctoral research involves automating network security analysis. About the Technical Editors Todd Chapman has 10+ years of experience delivering IT services as varied as systems management, security, networking, clustering, Perl programming, and corporate development and training. Currently, Todd is a consultant for gedas USA, Inc., in Auburn Hills, Michigan, where he provides security consulting services for Volkswagen/Audi of America. For the last three years Todd has been an active member of the SANS GCFW advisory board and has written SANS certification exam questions in a number of disciplines. Todd's certifications include Red Hat Certified Engineer (RHCE), Microsoft Certified Systems Engineer (MCSE), GIAC Certified Firewall Analyst (GCFW), GIAC Certified Intrusion Analyst (GCIA), and GIAC Systems and Network Auditor (GSNA). Anton Chuvakin, Ph.D., GCIA, GCIH, is a Security Strategist with netForensics, a security information management company, where he is involved with designing the product, researching potential new security features, and advancing the security roadmap. His areas of infosec expertise include intrusion detection, UNIX security, forensics, honeypots, and more. He is the author of the book Security Warrior (O'Reilly, January 2004) and a contributor to "Know Your Enemy II" by the Honeynet Project (AWL, June 2004) and "Information Security Management Handbook" (CRC, April 2004). In his spare time he maintains his security portal http://www.info-secure.org website. Dan Goldberg recently created MADJiC Consulting, Inc., to provide network design and architecture

reviews, intrusion detection and response, and vulnerability assessments in Central Virginia. He also works on research and writing projects for the SANS Institute and as technical director for Global Information Assurance Certification (GIAC). When not occupied by these activities, you may find him riding a mountain bike in the Blue Ridge Mountains. John Spangler is a freelance Network Systems Engineer. Having over 10 years of experience, he has worked on everything from small office systems to large enterprise and ISP networks. John has worked as a technical editor for Cisco certification manuals.

Great book that helps refresh the knowledge as well as bridge the knowledge gap. There are some areas that might be slightly outdated but the principles are still sound.

This book has lots of good security insights, definately an intermediate level book 300-400 level. It arrived well packaged and covers the topics I hoped it would without being a "cert" book, like the awful cisco books.

This book isn’t bad, but it’s a textbook so it can be a bit boring. I needed it for class and I did read through it. Good book but not very interesting.

Needed it for class. This book uses Cisco syntax. It’s a decent reference, although it’s easier to find information on an internet search. This book is not organized that well and has poorly named titles making it hard to search the index for specific information.

This book arrived in the time stated in good condition and was ready to use . The seller did a very good job of as I truly needed this book this week it help answer a lot of questions.

The binding of the book is terrible. The book itself is very informative.

This review is for the 2nd edition of this book."Inside Network Perimeter Security" (INPS) by Northcutt, Zeltser, Winters, Kent, and Ritchey suitably covers the broad topic of securing a network’s edge. The book is based, on part, from various SANS Institute training material (Northcutt is the CEO of the SANS Institute). Most of the items documented in INPS are honed from years of discussions in classes (and is mentioned an `excellent supplementary resource" for the GIAC Certified Firewall Analyst (GCFW)).The book first focuses on perimeter fundamentals - including

dedicating about 100 pages to the three main types of firewalls (Packet, Stateful & Proxy). The second section discusses how to fortify other areas of the perimeter - by implementing hardened routers and hosts, VPNs, IDSs, and IPS. The third section discusses designing a secure perimeter from the ground up (consider it best practices). This includes a much-needed chapter on wireless security. The last section is how to monitor and maintain the perimeter.It is hard to characterize who this book should be aimed at. While configurations examples are given for many different platforms and OSs, the configs cannot be considered complete. I feel this book would serve network admins well as a starting point and as introduction to concepts that they might not be familiar with.Some items I like from Inside Network Perimeter Security:-Chapter 6 gives a great discussion on Cisco routers. What really impresses me is, since the documentation is from someone besides CiscoPress, you get an idea of other ways to harden Cisco routers (see the telnet trick on page 142). The first appendix also gives a great collection of different ACLs (consider it an update of the NSA's list). I have over 50 CiscoPress books, and information found in these 2 chapters I have not seen documented in any CiscoPress book.-Chapter 21 provides a `quick' list of tools to use to help troubleshoot and isolate an issue. While there are some great books that are wholly dedicated to showing the ins-and-outs of different tools, sometimes you can't see the trees through the forest. Within just a few short pages, INPS is able to suggest a plethora of different tools to use based upon the issue.The book mentions that it's goal "...is to create a practical guide for designing, deploying, and maintaining a real-world network security perimeter." I believe they have done just that!I give this book 5 pings out of 5:!!!!!

The authors provide a nicely detailed explanation of current network defenses and practises. Each major topic in this field is well covered. Firewalls and packet filtering are clearly done. The preferred choice of example router is from Cisco. But the principles are obviously applicable to devices from any competing vendor.The book also recommends egress filtering; which is not often discussed in other texts. It helps guard against your net being used to send out malware. This helps the overall environment of the Internet. Moreover, there is also a tangible benefit to you. By doing egress checks, you can detect if one of your machines has been subverted. Which is always good to know.VPNs are given an entire chapter, due to their importance. The book also goes beyond talking about Intrusion Detection Systems to discuss Intrusion Prevention Systems. More proactive.To some sysadmins, the most important chapter might be that on wireless networks. As these have grown hugely, so too have the attacks against them. You can learn how to bolt down your wireless network.

Inside Network Perimeter Security (2nd Edition) Network Marketing: Go Pro in Network Marketing, Build Your Team, Serve Others and Create the Life of Your Dreams - Network Marketing Secrets Revealed, ... Books, Scam Free Network Marketing Book 1) Social Security & Medicare Facts 2016: Social Security Coverage, Maximization Strategies for Social Security Benefits, Medicare/Medicaid, Social Security Taxes, Retirement & Disability, Ser Network Marketing For Introverts: Guide To Success For The Shy Network Marketer (network marketing, multi level marketing, mlm, direct sales) CompTIA Security+ Guide to Network Security Fundamentals (with CertBlaster Printed Access Card) Access Control, Security, and Trust: A Logical Approach (Chapman & Hall/CRC Cryptography and Network Security Series) Handbook of Financial Cryptography and Security (Chapman & Hall/CRC Cryptography and Network Security Series) Security+ Guide to Network Security Fundamentals Human Systems Integration to Enhance Maritime Domain Awareness for Port/Harbour Security: Volume 28 NATO Science for Peace and Security Series - D: ... D: Information and Communication Security) Security Camera For Home: Learn Everything About Wireless Security Camera System, Security Camera Installation and More Nuclear Safeguards, Security and Nonproliferation: Achieving Security with Technology and Policy (Butterworth-Heinemann Homeland Security) Fundamentals Of Information Systems Security (Information Systems Security & Assurance) - Standalone book (Jones & Bartlett Learning Information Systems Security & Assurance) Network Security: Private Communication in a Public World (2nd Edition) Wireshark Network Analysis (Second Edition): The Official Wireshark Certified Network Analyst Study Guide The Three U.S.-Mexico Border Wars: Drugs, Immigration, and Homeland Security, 2nd Edition (Praeger Security International) How to get every Network Diagram question right on the PMPÃ Â® Exam:: 50+ PMPÃ Â® Exam Prep Sample Questions and Solutions on Network Diagrams (PMPÃ Â® Exam Prep Simplified) (Volume 3) How to get every Network Diagram question right on the PMPÃ Â® Exam:: 50+ PMPÃ Â® Exam Prep Sample Questions and Solutions on Network Diagrams (PMPÃ Â® Exam Prep Simplified Book 3) Rock Your Network Marketing Business: How to Become a Network Marketing Rock Star The Miracle Morning for Network Marketers 90-Day Action Planner (The Miracle Morning for Network Marketing) (Volume 2) The Four Color Personalities For MLM: The Secret Language For Network Marketing (MLM & Network Marketing Book 2)

Privacy

FAQ & Help