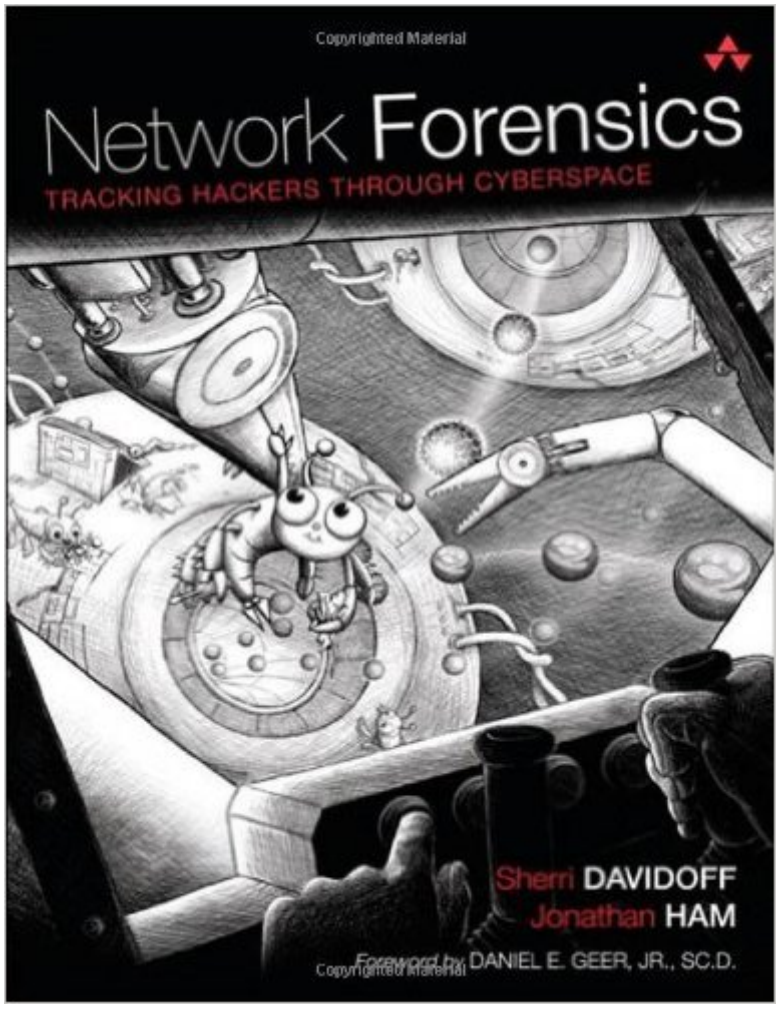
Network Forensics: Tracking Hackers Through Cyberspace



Synopsis

â œThis is a must-have work for anybody in information security, digital forensics, or involved with incident handling. As we move away from traditional disk-based analysis into the interconnectivity of the cloud, Sherri and Jonathan have created a framework and roadmap that will act as a seminal work in this developing field.â • â “ Dr. Craig S. Wright (GSE), Asia Pacific Director at Global Institute for Cyber Security + Research. Â â œItâ ™s like a symphony meeting an encyclopedia meeting a spy novel.â • â “Michael Ford, Corero Network Security Â On the Internet, every action leaves a markâ “in routers, firewalls, web proxies, and within network traffic itself. When a hacker breaks into a bank, or an insider smuggles secrets to a competitor, evidence of the crime is always left behind. Â Learn to recognize hackersâ ™ tracks and uncover network-based evidence in Network Forensics: Tracking Hackers through Cyberspace. Carve suspicious email attachments from packet captures. Use flow records to track an intruder as he pivots through the network. Analyze a real-world wireless encryption-cracking attack (and then crack the key yourself). Reconstruct a suspectâ ™s web surfing historyâ “and cached web pages, tooâ “from a web proxy. Uncover DNS-tunneled traffic. Dissect the Operation Aurora exploit, caught on the wire. Â Throughout the text, step-by-step case studies guide you through the analysis of network-based evidence. You can download the evidence files from the authorsâ ™ web site (lmgsecurity.com), and follow along to gain hands-on experience. Â Hackers leave footprints all across the Internet. Can you find their tracks and solve the case? Pick up Network Forensics and find out. Â

Book Information

Hardcover: 576 pages

Publisher: Prentice Hall; 1 edition (June 23, 2012)

Language: English

ISBN-10: 0132564718

ISBN-13: 978-0132564717

Product Dimensions: 7.1 x 1.4 x 9.2 inches

Shipping Weight: 2.3 pounds (View shipping rates and policies)

Average Customer Review: 4.4 out of 5 starsÂ Â See all reviewsÂ (28 customer reviews)

Best Sellers Rank: #178,458 in Books (See Top 100 in Books) #107 inÂ Books > Computers & Technology > Security & Encryption > Privacy & Online Safety #114 inÂ Books > Law > Criminal Law > Forensic Science #132 inÂ Books > Computers & Technology > Networking & Cloud Computing > Network Security

Customer Reviews

With a title like Network Forensics: Tracking Hackers through Cyberspace, the book at first sounds like a cheesy novel. But by page 25, you will quickly see this is the real thing. By the time you hit the last page, you will have read the collective wisdom of two of the smartest minds in the space.Author's Jonathan Ham and Sherri Davidoff are both SANS Institute instructors, and bring significant real-world experience to every chapter. Martin McKeay has an interview (albeit dated) with the authors on his web site here about their SANS course on network forensics.In 12 densely written chapters at just over 500 pages, the book covers nearly every aspect within network and digital forensics.While the book Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet provides a comprehensive overview of the topic; Network Forensics: Tracking Hackers through Cyberspace focuses at the packet level.Part 2, which is about a third of the book, is spent on traffic analysis, with all-embracing coverage of concepts and topics such as statistical flow analysis, wireless traffic capture and analysis, NIDS detection and analysis, packet logging and more.Readers should be very comfortable with Wireshark packet capture output, which the book extensively references. Those not quite comfortable with packet capture analysis will likely find this book way over their head.Part 3 focuses on network devices and logging for all types of network devices. Detailed logging aspects for switches, routers and firewalls are dealt with.The last 2 chapters deal with advanced topics such as network tunneling and malware forensics.

Any book, child story or technical manual that has a forward written by Dr. Daniel Geer is going to be amazing. Not that I recommend Dr. Geer start writing childrenâ ™s literature, itâ ™s just he is an incredible mind for his time. That was the first thing that caught my attention about the book. I am quite excited about the book because it isnâ ™t your typical forensic book. This masterpiece goes well beyond anything Iâ ™ve read in a long time.Warning: Network Forensics is not for entry level readers or even intermediate. This is hardcore PhD level material.I was surprised that the book cover says â œTracking Hackers Through Cyberspace.â • First off, there isnâ ™t anything wrong with being a hacker. There is something wrong with conducting criminal activity and those are two completely different things. If the book would have posted â œTracking Criminals Through Cyberspaceâ •, I might have only cringed a little bit. My second gripe is about the word â œCyber.â • Come on folks, it is â œdigitalâ • not â œcyber.â • Iâ ™m sure the authors didnâ ™t do this; it was probably the editorâ ™s fault. They have to sell books with sexy names so I donâ ™t directly blame the writers.The entire book is an in-depth technical manual and how-to guide for network forensics. The difference between regular digital forensics and network forensics is that evidence is much

harder to locate and more volatile across a network than data storage devices. Husband and wife team Sherri and Jonathan dive deep, deep into hidden corners of switches and hubs to show you where evidence resides. The text is clearly written and done so in a straight forward manner. The content is tough though. Donâ ™t expect an easy read.You will need a sharp mind to completely understand the importance of this material, as itâ ™s presented.

Network Forensics: Tracking Hackers through Cyberspace Extending Simple Network Management Protocol (SNMP) Beyond Network Management: A MIB Architecture for Network-Centric Services The Basics of Digital Forensics: The Primer for Getting Started in Digital Forensics Computer Forensics: Investigating Network Intrusions and Cyber Crime (EC-Council Press) Monitor Your Home Network: A How-To Guide to Monitoring a Small, Private Network How To Set Up a Home Network With Windows 7: Your Step-By-Step Guide To Setting Up a Home Network With Windows 7 Home Network Handbook: Learn how to set up your home network Network Security Assessment: Know Your Network Network Programmability and Automation: Skills for the Next-Generation Network Engineer Effective TCP/IP Programming: 44 Tips to Improve Your Network Programs: 44 Tips to Improve Your Network Programs Wireless Network Administration A Beginner's Guide (Network Pro Library) Descubra los secretos del network marketing: Redes de Mercadeo y Network marketing (Spanish Edition) Hackers & Painters: Big Ideas from the Computer Age Hackers and Painters: Big Ideas from the Computer Age The Ultimate Guide to WordPress Security: Secure and protect your WordPress website form hackers and protect your data, get up to date security updates Black Hat Python: Python Programming for Hackers and Pentesters Violent Python: A Cookbook for Hackers, Forensic Analysts, Penetration Testers and Security Engineers Bayesian Methods for Hackers: Probabilistic Programming and Bayesian Inference (Addison-Wesley Data & Analytics) Hackers vs. Security Pros: A Security Manager's Playbook (The CTO Playbook 1) Design for Hackers: Reverse Engineering Beauty