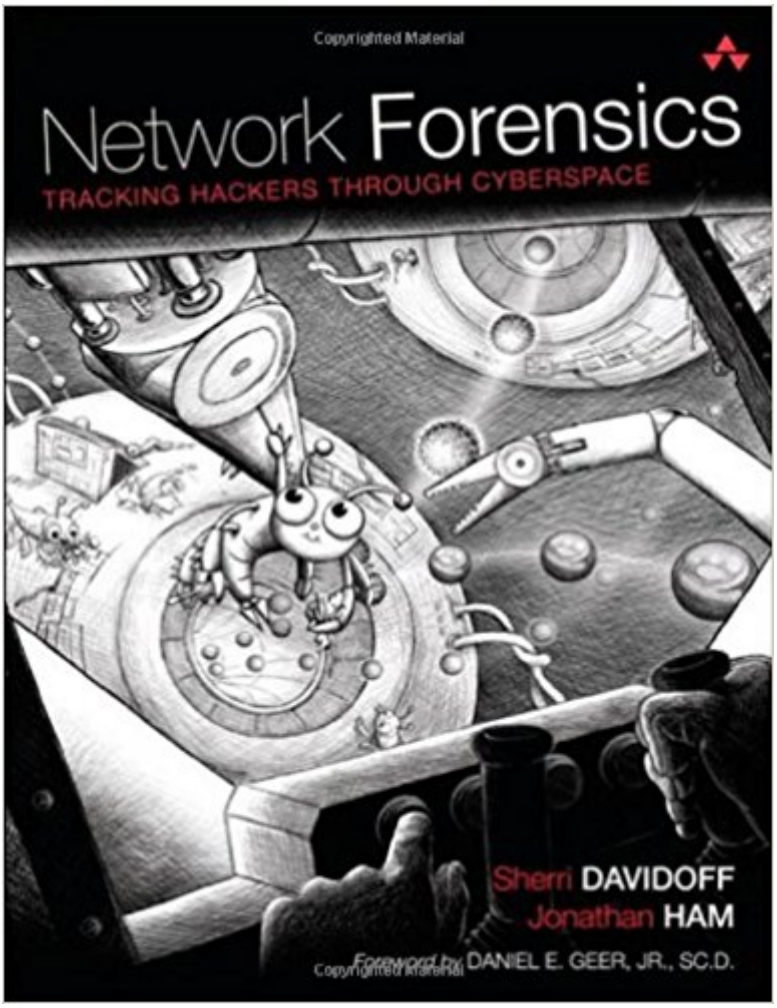
Network Forensics: Tracking Hackers Through Cyberspace



Synopsis

Ã¢â ¬Å“This 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.Ã¢â ¬Â• Ã¢â ¬â œ Dr. Craig S. Wright (GSE), Asia Pacific Director at Global Institute for Cyber Security + Research. Ã Â Ã¢â ¬Å“ItÃ¢â ¬â„¢s like a symphony meeting an encyclopedia meeting a spy novel.Ã¢â ¬Â• Ã¢â ¬â œMichael Ford, Corero Network Security Ã Â On the Internet, every action leaves a markÃ¢â ¬â œin 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. Ã Â Learn to recognize hackersÃ¢â ¬â„¢ 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 suspectÃ¢â ¬â„¢s web surfing historyÃ¢â ¬â œand cached web pages, tooÃ¢â ¬â œfrom a web proxy. Uncover DNS-tunneled traffic. Dissect the Operation Aurora exploit, caught on the wire. Ã 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 authorsÃ¢â ¬â„¢ web site (lmgsecurity.com), and follow along to gain hands-on experience. Ã Â Hackers leave footprints all across the Internet. Can you find their tracks and solve the case? Pick up Network Forensics and find out. Ã 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: 4.1 out of 5 stars 34 customer reviews

Best Sellers Rank: #167,266 in Books (See Top 100 in Books) #97 inÃ Â Books > Computers & Technology > Security & Encryption > Privacy & Online Safety #148 inÃ Â Books > Computers & Technology > Internet & Social Media > Hacking #148 inÃ Â Books > Law > Criminal Law >

Forensic Science

Customer Reviews

Sherri Davidoff is a founder of LMG Security, an information security consulting and research firm. Her specialties include network penetration testing, digital forensics, social engineering testing, and web application assessments. She holds her S.B. in Computer Science and Electrical Engineering from MIT. Ã Â Jonathan Ham has been commissioned to teach NCIS investigators how to use Snort, performed packet analysis from a facility more than two thousand feet underground, taught intrusion analysis to the NSA, and chartered and trained the CIRT for one of the largest U.S. civilian federal agencies. He is a founder of LMG Security. His favorite field is ip[6:2].

This book should be considered required reading for anyone interested or involved in network forensics or InfoSec un general. The case studies are especially interesting to perform and a great way to hone your knowledge and skills in this area.Probably best for an individual with a strong background in networking theory, design and implementation as well as at least a basic knowledge of packet capture and analysis tools, (tcpdump, Wireshark, etc).

Outstanding book on network forensics. The authors take us through a variety of scenarios with lots of great explanations and details about how to achieve the goals. They provide pcaps on their website so it is possible to work through the exercises myself. Excellent learning tool! I will look for more books on this topic from them.

I used this book in a grad school network forensics course and I was very impressed.

Excellent material. well done. Get this with the Blue Team Handbook, and you’ve got a winner.

This is a must have, the way the book is setup to work a case is great.

There’s lot’s of material on "computer forensics" but until now this book there’s been absolutely nothing on "network forensics".This is the "Bible" if networks are important to your company’s security or you need to know how to find the top talent in the field.Not overly technical (some things may be better kept secret) but it will certainly have you thinking about things you may not have known were hidden within your networks. Should be on every networking professional’s bookshelf!

Good but dated material.

This seems to be a decent book. I wish the author covered more on advanced topics, like Ch 16. I have to admit I was disappointed to see things like, "this is a switch" and "this is what a router does." If you don’t know what a router is, you should probably be starting with a different book. While I can understand why authors include this type of information, to sell more books, I appreciate authors that can target their books to a specific and not as general audience. Just my .02.

Network Forensics: Tracking Hackers through Cyberspace 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) The Basics of Digital Forensics: The Primer for Getting Started in Digital Forensics Network Marketing For Introverts: Guide To Success For The Shy Network Marketer (network marketing, multi level marketing, mlm, direct sales) Soul Music: Tracking the Spiritual Roots of Pop from Plato to Motown (Tracking Pop) Computer Forensics: Investigating Network Intrusions and Cybercrime (CHFI), 2nd Edition 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) How to Follow Up With Your Network Marketing Prospects: Turn Not Now Into Right Now! (MLM & Network Marketing Book 4) CompTIA Network+ Study Guide: Exam N10-006 (Comptia Network + Study Guide Authorized Courseware) Wireshark Network Analysis (Second Edition): The Official Wireshark Certified Network Analyst Study Guide Network Programmability and Automation: Skills for the Next-Generation Network Engineer The Cuckoo’s Egg: Tracking a Spy Through the Maze of Computer Espionage The Healing Protocol Journal: A Journal For Tracking Your Progress Through An Elimination Diet, Including AIP, GAPS, SCD, low FODMAPS and more Cyberspace Law: Cases and Materials (Aspen Casebook) Capoeira: The Jogo de Angola from Luanda to Cyberspace The Darkening Web: The War for Cyberspace