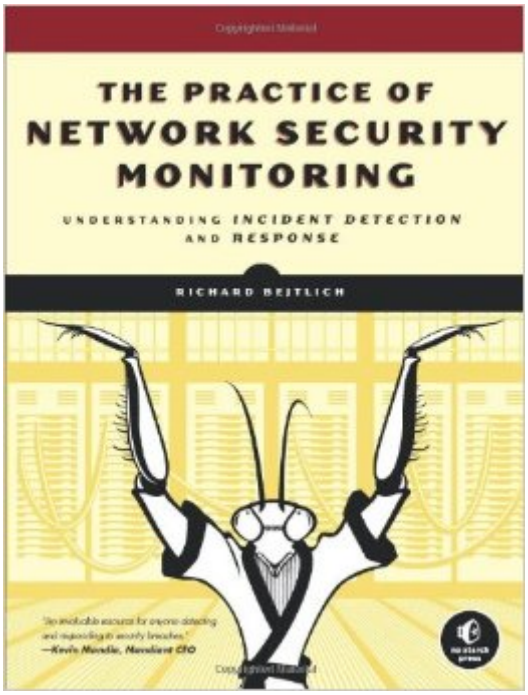
The Practice Of Network Security Monitoring: Understanding Incident Detection And Response



Synopsis

Network security is not simply about building impenetrable walls â ” determined attackers will eventually overcome traditional defenses. The most effective computer security strategies integrate network security monitoring (NSM): the collection and analysis of data to help you detect and respond to intrusions. In The Practice of Network Security Monitoring, Mandiant CSO Richard Bejtlich shows you how to use NSM to add a robust layer of protection around your networks â ” no prior experience required. To help you avoid costly and inflexible solutions, he teaches you how to deploy, build, and run an NSM operation using open source software and vendor-neutral tools. You'll learn how to: Determine where to deploy NSM platforms, and size them for the monitored networksDeploy stand-alone or distributed NSM installationsUse command line and graphical packet analysis tools, and NSM consolesInterpret network evidence from server-side and client-side intrusionsIntegrate threat intelligence into NSM software to identify sophisticated adversaries There's no foolproof way to keep attackers out of your network. But when they get in, you'll be prepared. The Practice of Network Security Monitoring will show you how to build a security net to detect, contain, and control them. Attacks are inevitable, but losing sensitive data shouldn't be.

Book Information

Paperback: 376 pages
Publisher: No Starch Press; 1 edition (August 5, 2013)
Language: English
ISBN-10: 1593275099
ISBN-13: 978-1593275099
Product Dimensions: 7 x 1.5 x 9.2 inches
Shipping Weight: 1.8 pounds (View shipping rates and policies)
Average Customer Review: 4.7 out of 5 starsÂ Â See all reviewsÂ (41 customer reviews)
Best Sellers Rank: #41,810 in Books (See Top 100 in Books) #9 inÂ Books > Computers & Technology > Networking & Cloud Computing > Network Administration > Disaster & Recovery #14 inÂ Books > Computers & Technology > Networking & Cloud Computing > Networks, Protocols & APIs > Networks #38 inÂ Books > Computers & Technology > Networking & Cloud Computing > Network Security

Customer Reviews

Most computer books are badly written. The information in the book is fine (usually, hopefully), but the actual craft of writing is poor. They read like computer programs. This isn't surprising, as most

computer books are written by computer professionals. By the time you’re good enough at a computing topic to write a book about it, your brain automatically arranged things in machine-friendly order. That’s human nature. The downside of this, however, is that most computing books lack the things that make books interesting to human beings. We readers grit our teeth and plow through them because we need the information.I’m pleased to say that Richard Bejtlich’s The Practice of Network Security Monitoring is not one of those books. The damn thing is actually readable. By normal people.That’s a vague assertion. How about a metric? Season 6 of Burn Notice just hit Netflix streaming. I watched a few episodes Saturday. They ended on a tense cliffhanger, but I finally had to go to bed. Sunday, I finished reading this book before seeing how Westin and company got out of their fix. (Okay, that’s not exactly a metric, but it’s a good sign.)Bejtlich graduated from Harvard and the Air Force Academy graduate. He led CIRT teams in the Air Force, built a security team at General Electric, and is now Chief Security Officer at Mandiant. He’s on television as an electronic security guru. And for the last decade-plus, he’s been beating the drum about intelligent attackers and the need for a holistic approach to security. When everybody else was going on about firewalls and antivirus and access controls and penetration testing, he wrote books like The Tao of Network Security Monitoring arguing that we need to think about network defense as an ongoing activity.

As we enter the murky age of Internet of Things (or "Internet of Insecure Things", "Internet of Evil Things", "Botnet of Things", take your pick) monitoring your home network has to become a common skill. Although by no means confined to application in home environments, The Practice of Network Security Monitoring does allow a modestly technically adept user to do just that. This book walks you through understanding the concepts, installing the needed software, configuring network monitoring components, and using some of the many free solutions for detecting unwanted or malicious traffic.For those who want to apply this work at home, allow me to make a few suggestions about corollary purchases you may need to make. I recommend dedicating a desktop or tower computer to the task of server. It doesn’t need an especially powerful CPU, but it should have a lot of RAM, at least 8 GB. Purchase your RAM with a view to exanding; using 8GB as an example, don’t buy 4 2GB sticks, but rather 2 4GB sticks. Later you could by 2 x 4GB or 2 x 8GB sticks to upgrade memory. You will also need at least 1 extra NIC (Network Interface Card), which will be in permanent ’listen only’ (aka "promiscuous") mode. You will be using the free Security Onion solution, running on the free Ubuntu 12.04 Linux, so you can skip buying a license for Windows if you purchase everything from scratch. Finally you will need at least one network device

that can duplicate traffic.

The Practice of Network Security Monitoring: Understanding Incident Detection and Response Crafting the InfoSec Playbook: Security Monitoring and Incident Response Master Plan Beyond Initial Response--2Nd Edition: Using The National Incident Management System Incident Command System Home Security: Top 10 Home Security Strategies to Protect Your House and Family Against Criminals and Break-ins (home security monitor, home security system diy, secure home network) Real Digital Forensics: Computer Security and Incident Response Extrusion Detection: Security Monitoring for Internal Intrusions Monitor Your Home Network: A How-To Guide to Monitoring a Small, Private Network Detection Estimation and Modulation Theory, Part I: Detection, Estimation, and Filtering Theory The Computer Incident Response Planning Handbook: Executable Plans for Protecting Information at Risk Incident Response & Computer Forensics, Third Edition Extending Simple Network Management Protocol (SNMP) Beyond Network Management: A MIB Architecture for Network-Centric Services Linux Firewalls: Attack Detection and Response Fetal Heart Monitoring: Principles and Practices (AWHONN, Fetal Heart Monitoring) Network Security Assessment: Know Your Network Host Response to Biomaterials: The Impact of Host Response on Biomaterial Selection Network Security: Private Communications in a Public World (Radia Perlman Series in Computer Networking and Security) CompTIA Security+ Guide to Network Security Fundamentals Nessus Network Auditing: Jay Beale Open Source Security Series (Jay Beale's Open Source Security) Controller Area Network Prototyping With Arduino: Creating CAN Monitoring, Diagnostics, and Simulation Applications Nagios: System and Network Monitoring