[PDF] The Tao Of Network Security Monitoring: Beyond Intrusion Detection

Richard Bejtlich - pdf download free book

Books Details:
Title: The Tao of Network Security M
Author: Richard Bejtlich
Released: 2004-07-22
Language:
Pages: 832
ISBN: 0321246772
ISBN13: 978-0321246776
ASIN: 0321246772

---

pdf, mobi, epub, azw, kindle

Description:

About the Author

Richard Bejtlich is founder of TaoSecurity, a company that helps clients detect, contain, and remediate intrusions using Network Security Monitoring (NSM) principles. He was formerly a principal consultant at Foundstone--performing incident response, emergency NSM, and security

research and training--and created NSM operations for ManTech International Corporation and Ball Aerospace & Technologies Corporation. For three years, Bejtlich defended U.S. information assets as a captain in the Air Force Computer Emergency Response Team (AFCERT). Formally trained as an intelligence officer, he is a graduate of Harvard University and of the U.S. Air Force Academy. He has authored or coauthored several security books, including *The Tao of Network Security Monitoring* (Addison-Wesley, 2004).

Welcome to *The Tao of Network Security Monitoring: Beyond Intrusion Detection*. The goal of this book is to help you better prepare your enterprise for the intrusions it will suffer. Notice the term "will." Once you accept that your organization will be compromised, you begin to look at your situation differently. If you've actually worked through an intrusion—a real compromise, not a simple Web page defacement—you'll realize the security principles and systems outlined here are both necessary and relevant.

This book is about *preparation* for compromise, but it's not a book about *preventing* compromise. Three words sum up my attitude toward stopping intruders: *prevention eventually fails*. Every single network can be compromised, either by an external attacker or by a rogue insider. Intruders exploit flawed software, misconfigured applications, and exposed services. For every corporate defender, there are thousands of attackers, enumerating millions of potential targets. While you might be able to prevent some intrusions by applying patches, managing configurations, and controlling access, you can't prevail forever. Believing only in prevention is like thinking you'll never experience an automobile accident. Of course you should drive defensively, but it makes sense to buy insurance and know how to deal with the consequences of a collision.

Once your security is breached, everyone will ask the same question: *now what?* Answering this question has cost companies hundreds of thousands of dollars in incident response and computer forensics fees. I hope this book will reduce the investigative workload of your computer security incident response team (CSIRT) by posturing your organization for incident response success. If you deploy the monitoring infrastructure advocated here, your CSIRT will be better equipped to scope the extent of an intrusion, assess its impact, and propose efficient, effective remediation steps. The intruder will spend less time stealing your secrets, damaging your reputation, and abusing your resources. If you're fortunate and collect the right information in a forensically sound manner, you might provide the evidence needed to put an intruder in jail.

Audience

This book is for security professionals of all skill levels and inclinations. The primary audience includes network security architects looking for ways to improve their understanding of their network security posture. My goal is to provide tools and techniques to increase visibility and comprehension of network traffic. If you feel let down by your network-based intrusion detection system (NIDS), this book is definitely for you. I explain why most NIDS deployments fail and how you can augment existing NIDS with open source tools.

Because this book focuses on open source tools, it is more likely to be accepted in smaller, less bureaucratic organizations that don't mandate the use of commercial software. Furthermore, large organizations with immense bandwidth usage might find some open source tools aren't built to

handle outrageous traffic loads. I'm not convinced the majority of Internet-enabled organizations are using connections larger than T-3 lines, however. While every tool and technique hasn't been stress-tested on high-bandwidth links, I'm confident the material in this book applies to a great majority of users and networks.

If you're a network security analyst, this book is also for you. I wrote this book as an analyst, for other analysts. This means I concentrate on interpreting traffic, not explaining how to install and configure every single tool from source code. For example, many books on "intrusion detection" describe the Transmission Control Protocol/Internet Protocol (TCP/IP) suite and how to set up the Snort open source IDS engine with the Analysis Console for Intrusion Databases (ACID) interface. These books seldom go further because they soon encounter inherent investigative limitations that restrict the usefulness of their tools. Since my analytical techniques do not rely on a single product, I can take network-based analysis to the next level. I also limit discussion of odd packet header features, since real intrusions do not hinge on the presence of a weird TCP flag being set. The tools and techniques in this book concentrate on giving analysts the information they need to assess intrusions and make decisions, not just identify mildly entertaining reconnaissance patterns.

This book strives to not repeat material found elsewhere. You will not read how to install Snort or run Nmap. I suggest you refer to the recommended reading list in the next section if you hunger for that knowledge. I introduce tools and techniques overlooked by most authors, like the material on protocol anomaly detection by Brian Hernacki, and explain how you can use them to your advantage.

Technical managers will appreciate sections on best practices, training, and personnel issues. All the technology in the world is worthless if the staff manning it doesn't understand their roles, responsibilities, and escalation procedures. Managers will also develop an intuition for the sorts of information a monitoring process or product should provide. Many vendors sell services and products named with combinations of the terms "network," "security," and "monitoring." This book creates a specific definition for *network security monitoring* (NSM), built on a historical and operational foundation.

Prerequisites

I've tried to avoid duplicating material presented elsewhere, so I hope readers lacking prerequisite knowledge take to heart the following reading suggestions. I highly recommend reading the following three books prior to this one. If you've got the necessary background, consider these titles as references.

- *Internet Site Security*, by Erik Schetina, Ken Green, and Jacob Carlson (Boston, MA: Addison-Wesley, 2002). This is an excellent "security 101" book. If you need to start from the ground floor, this book is a great beginning.

- *Counter Hack: A Step-by-Step Guide to Computer Attacks and Effective Defenses*, by Ed Skoudis (Upper Saddle River, NJ: Prentice Hall PTR, 2001). *Counter Hack* offers the best single-chapter introductions to TCP/IP, Microsoft Windows, UNIX, and security issues available.

- *Hacking Exposed: Network Security Secrets and Solutions*, 4th ed., by Stuart McClure, Joel Scambray, and George Kurtz (New York: McGraw-Hill, 2003). *Hacking Exposed* explores the capabilities and intentions of digital threats. By knowing how to compromise computers, you'll understand the sorts of attacks network security monitoring practitioners will encounter.

If you need an introduction to intrusion detection theory, I recommend the following book:

- *Intrusion Detection*, by Rebecca Gurley Bace (Indianapolis, IN: New Riders, 2000). While not strictly needed to understand the concepts in this book, *Intrusion Detection* provides the history and mental lineage of IDS technology. As *The Tao of Network Security Monitoring* focuses on network-based tactics, you can turn to *Intrusion Detection* for insight on host-based detection or the merits of signature- or anomaly-based IDS.

It helps to have a good understanding of TCP/IP beyond that presented in the aforementioned titles. The following are a few of my favorite books on TCP/IP.

- *Internet Core Protocols: The Definitive Guide*, by Eric A. Hall (Cambridge, MA: O'Reilly, 2000). Many people consider Richard Stevens' *TCP/IP Illustrated Volume 1: The Protocols* (Reading, MA: Addison-Wesley, 1994) to be the best explanation of TCP/IP. I think Eric Hall's more recent book is better suited for modern network traffic analysts.

- *Network Analysis and Troubleshooting*, by J. Scott Haugdahl (Boston, MA: Addison-Wesley, 2000). Troubleshooting books tend to offer the more interesting explanations of protocols in action. Scott Haugdahl works his way up the seven layers of the Open Systems Interconnect (OSI) model, using packet traces and case studies.

- *Troubleshooting Campus Networks: Practical Analysis of Cisco and LAN Protocols*, by Priscilla Oppenheimer and Joseph Bardwell (Indianapolis, IN: Wiley, 2002). This title is considerably broader in scope than Scott Haugdahl's work, with coverage of virtual local area networks (VLANs), routing protocols, and wide area network (WAN) protocols like Asynchronous Transfer Mode (ATM).

One other book deserves mention, but I request you forgive a small amount of self-promotion. *The Tao of Network Security Monitoring* is primarily about detecting incidents through network-based means. In some senses it is also an incident response book. Effective incident response, however, reaches far beyond network-based evidence. To learn more about host-based data, such as file systems and memory dumps, I recommend *Real Digital Forensics* (Boston, MA: Addison-Wesley, 2005). I wrote the network monitoring sections of the book, and coauthors Keith Jones and Curtis Rose did the host- and memory-level forensics. If you'd like to see the big picture for incident response, read *Real Digital Forensics*.

A Note on Operating Systems

All of the tools I discuss in this book run on the FreeBSD (http://www.freebsd.org) operating system. FreeBSD is a UNIX-like, open source environment well suited for building network security monitoring platforms. If you're familiar with Linux or any other Berkeley Software Distribution (OpenBSD or NetBSD), you'll have no trouble with FreeBSD. I strongly recommend running NSM tools on UNIX-like platforms like the BSDs and Linux.

You might consider trying a live CD-ROM FreeBSD distribution prio…

- Title: The Tao of Network Security Monitoring: Beyond Intrusion Detection

- Author: Richard Bejtlich
- Released: 2004-07-22
- Language:
- Pages: 832
- ISBN: 0321246772
- ISBN13: 978-0321246776
- ASIN: 0321246772