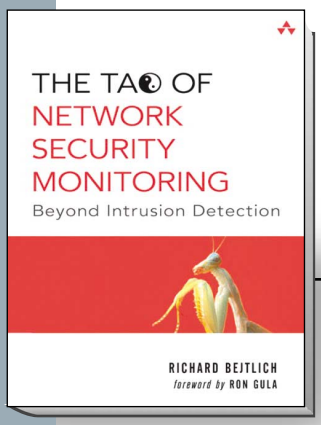
Quickly develop and apply the skills needed to detect, prevent, and respond to new and emerging computer security exploits.

COMING THIS JULY



RICHARD BEJTLICH
Foreword by Ron Gula

The Tao of Network Security Monitoring

Beyond Intrusion Detection

©2005, Paper, 832 pages,
0-321-24677-2, $49.99

Every network can be compromised. There are too many systems, offering too many services, running too many flawed applications. No amount of careful coding, patch management, or access control can keep out every attacker. If prevention eventually fails, how do you prepare for the intrusions that will eventually happen?

Network security monitoring (NSM) equips security staff to deal with the inevitable consequences of too few resources and too many responsibilities. NSM collects the data needed to generate better assessment, detection, and response processes--resulting in decreased impact from unauthorized activities.

In *The Tao of Network Security Monitoring*, Richard Bejtlich explores the products, people, and processes that implement the NSM model. By focusing on case studies and the application of open source tools, he helps you gain hands-on knowledge of how to better defend networks and how to mitigate damage from security incidents.

Inside, you will find in-depth information on the following areas.

- The NSM operational framework and deployment considerations.
- How to use a variety of open-source tools-including Sguil, Argus, and Ethereal-to mine network traffic for full content, session, statistical, and alert data.
- Best practices for conducting emergency NSM in an incident response scenario, evaluating monitoring vendors, and deploying an NSM architecture.
- Developing and applying knowledge of weapons, tactics, telecommunications, system administration, scripting, and programming for NSM.
- The best tools for generating arbitrary packets, exploiting flaws, manipulating traffic, and conducting reconnaissance.

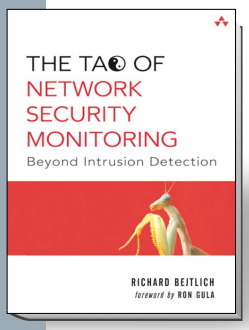
Whether you are new to network intrusion detection and incident response, or a computer-security veteran, this book will enable you to quickly develop and apply the skills needed to detect, prevent, and respond to new and emerging threats.

About the Author

RICHARD BEJTLICH
Former military intelligence officer Richard Bejtlich is a security engineer at ManTech International Corporation's Computer Forensics and Intrusion Analysis division. A recognized authority on computer security, he has extensive experience with network security monitoring, incident response, and digital forensics. Richard tests and writes documentation for Sguil, an open source GUI for the Snort intrusion detection engine. He also maintains the TaoSecurity Blog at taosecurity.blogspot.com.

Addison Wesley

Table of Contents



Preface
About the Author
Foreword
Acknowledgements
Legal Notice
Dedication

PART I: INTRODUCTION TO NSM

1. The Security Process
What is Security?
What is Risk?
A Risky Case Study
Security Principles: Characteristics of the Intruder
Security Principles: Defensible Networks
Conclusion

2. What is Network Security Monitoring?
Indications and Warning
Collection, Analysis, and Escalation
Detecting and Responding to Intrusions
Why Do IDS Deployments Often Fail?
Outsiders vs. Insiders: What is NSM's Focus?
Security Principles: Detection
Security Principles: Limitations
What NSM Is Not
Conclusion

3. Deployment Considerations
Threat Models and Monitoring Zones
Accessing Traffic in Each Zone
Wireless Monitoring
The Sensor
Sensor Management
Conclusion

PART II: NSM PRODUCTS

4. Reference Intrusion Model
CHM Plans
Ardala's Attack
Conclusion

5. Full Content Data
A Note on Software Versions
Libpcap
Tcpdump
Tethereal
Snort as Packet Logger
Ethereal
A Note on Commercial Full Content Collection Options
Conclusion

6. Additional Data Analysis
Editcap and Mergecap
Tcpslice
Tcpreplay
Tcpflow
Ngrep
Ipsumdump
Etherape
NetDude
POf
Conclusion

7. Session Data
Forms of Session Data
Cisco NetFlow
Fprobe
Ng_netflow
Flow-tools
SFlow and Sflow Toolkit
Argus
Tcptrace
Conclusion

8. Statistical Data
What is Statstical Data?
Cisco Accounting
Ipcad
Ifstat
Bmon
Trafshow
Ttt
Tcpdstat
MRTG
Ntop
Conclusion

9. Alert Data: Bro and Prelude
Bro
Prelude
Conclusion

10. Alert Data: NSM Using Sguil
Why Sguil?
So What is Sguil?
The Basic Sguil Interface
Sguil's Answer to "Now What?"
Decision-Making with Sguil
Sguil vs. the Reference Intrusion Model
Conclusion

PART III: NSM PROCESSES

11. Best Practices
Assessment
Protection
Detection
Response
Conclusion

12. Case Studies for Managers
Introduction to Hawke Helicopter Supplies
Case Study 1: Emergency Network Security Monitoring
Case Study 2: Evaluating Managed Security Monitoring Providers
Case Study 3: Deploying an In-House NSM Solution
Conclusion

PART IV: NSM PEOPLE

13. Analyst Training Program
Weapons and Tactics
Telecommunications
System Administration
Scripting and Programming
Management and Policy
Training In Action
Periodicals and Web Sites
Case Study: Staying Current with Tools
Conclusion

14. Discovering DNS
Normal Port 53 Traffic
Suspicious Port 53 Traffic
Malicious Port 53 Traffic
Conclusion

15. The Power of Session Data
The Session Scenario
Session Data from the Wireless Segment
Session Data from the DMZ Segment
Session Data from the VLANs
Session Data from the External Segment
Conclusion

16. Packet Monkey Heaven
Truncated TCP Options
SCAN FIN
Chained Covert Channels
Conclusion

PART V: THE INTRUDER VS. NSM OPERATIONS

17. Tools to Attack NSM Operations
Packit
IP Sorcery
Fragroute
LFT
Xprobe2
Cisco IOS Denial of Service
Solaris Sadmind Exploitation Attempt
Microsoft RPC Exploitation
Conclusion

18. Tactics to Attack NSM Operations
Promote Anonymity
Evade Detection
Appear Normal
Degrade Or Deny Collection
Self-Inflicted Problems
Conclusion

Epilogue: The Future of NSM
Remote Packet Capture and Centralized Analysis
Integration with Vulnerability Analysis Products
Traffic Modeling and Anomaly Detection
NSM Beyond the Gateway
Conclusion

APPENDICES

A. Protocol Headers
Ethernet Frames
Address Resolution Protocol
Internet Protocol
Internet Control Message Protocol
Transmission Control Protocol
User Datagram Protocol

B. NSM Intellectual History
Foundation
Sensor Architecture
Packet Analysis
Flow-Based Monitoring
Alert-Centric Intrusion Detection
Complimentary Technologies
Researcher Home Pages
Network Security Monitoring History First-Hand

C. Protocol Anomaly Detection

Index

Addison Wesley

ORDERING INFORMATION:

SINGLE COPY SALES:
Visa, Master Card, American Express, Checks, or Money Orders only —
Tel: 515-284-6761
Fax: 515-284-2607
Toll-Free: 800-811-0912

GOVERNMENT AGENCIES:
Kathryn Bass
GS-14F-8023A
703-404-9194
www.pearsongovernmentsales.com

COLLEGE PROFESSORS:
Desk or Review Copies —
exam@aw.com

CORPORATE ACCOUNTS:
Quantity, Bulk Orders totalling 10 or more books. Purchase orders only — No credit cards.
Fax: 317-428-3343
Toll-Free: 800-382-3419

INTERNATIONAL ORDERING INFORMATION:

CANADA:
cdn.ordr@pearsoned.com

UK/EMEA:
Europe, Middle East, South Africa
de-order@pearson.com

BENELUX:
amsterdam@pearsoned-ema.com

AUSTRALIA:
trade@pearsoned.com.au

SOUTH ASIA:
asia@pearsoned.com.sg

NORTH ASIA:
misip@pearsoned.com.hk

OTHER REGIONS:
tim.galligan@pearsoned.com