

4 FREE BOOKLETS
YOUR SOLUTIONS MEMBERSHIP



Intrusion Prevention and Active Response

Deploying Network and Host IPS

- Automate Responses to Attempted Intrusions
- Master Buffer Overflow Prevention Technologies
- Avoid False Positives

Michael Rash
Angela Orebaugh
Graham Clark
Becky Pinkard
Jake Babbin

Foreword by Stephen Northcutt
Director of Training and Certification
The SANS Institute

Register for Free Membership to

s o l u t i o n s @ s y n g r e s s . c o m

Over the last few years, Syngress has published many best-selling and critically acclaimed books, including Tom Shinder's *Configuring ISA Server 2000*, Brian Caswell and Jay Beale's *Snort 2.1 Intrusion Detection*, and Angela Orebaugh and Gilbert Ramirez's *Ethereal Packet Sniffing*. One of the reasons for the success of these books has been our unique **solutions@syngress.com** program. Through this site, we've been able to provide readers a real time extension to the printed book.

As a registered owner of this book, you will qualify for free access to our members-only solutions@syngress.com program. Once you have registered, you will enjoy several benefits, including:

- Four downloadable e-booklets on topics related to the book. Each booklet is approximately 20-30 pages in Adobe PDF format. They have been selected by our editors from other best-selling Syngress books as providing topic coverage that is directly related to the coverage in this book.
- A comprehensive FAQ page that consolidates all of the key points of this book into an easy to search web page, providing you with the concise, easy to access data you need to perform your job.
- A "From the Author" Forum that allows the authors of this book to post timely updates links to related sites, or additional topic coverage that may have been requested by readers.

Just visit us at **www.syngress.com/solutions** and follow the simple registration process. You will need to have this book with you when you register.

Thank you for giving us the opportunity to serve your needs. And be sure to let us know if there is anything else we can do to make your job easier.

Intrusion Prevention and Active Response

Deploying Network and Host IPS

Michael Rash
Angela Orebaugh
Graham Clark
Becky Pinkard
Jake Babbin

Foreword by Stephen Northcutt
Director of Training and Certification
The SANS Institute

Syngress Publishing, Inc., the author(s), and any person or firm involved in the writing, editing, or production (collectively “Makers”) of this book (“the Work”) do not guarantee or warrant the results to be obtained from the Work.

There is no guarantee of any kind, expressed or implied, regarding the Work or its contents. The Work is sold AS IS and WITHOUT WARRANTY. You may have other legal rights, which vary from state to state.

In no event will Makers be liable to you for damages, including any loss of profits, lost savings, or other incidental or consequential damages arising out from the Work or its contents. Because some states do not allow the exclusion or limitation of liability for consequential or incidental damages, the above limitation may not apply to you.

You should always use reasonable care, including backup and other appropriate precautions, when working with computers, networks, data, and files.

Syngress Media®, Syngress®, “Career Advancement Through Skill Enhancement®,” “Ask the Author UPDATE®,” and “Hack Proofing®,” are registered trademarks of Syngress Publishing, Inc. “Syngress: The Definition of a Serious Security Library”™, “Mission Critical™,” and “The Only Way to Stop a Hacker is to Think Like One™” are trademarks of Syngress Publishing, Inc. Brands and product names mentioned in this book are trademarks or service marks of their respective companies.

KEY SERIAL NUMBER

001	HJIRTCV764
002	PO9873D5FG
003	829KM8NJH2
004	FG3298NJPP
005	CVPLQ6WQ23
006	VBP965T5T5
007	HJJJ863WD3E
008	2987GVTWMK
009	629MP5SDJT
010	IMWQ295T6T

PUBLISHED BY

Syngress Publishing, Inc.
800 Hingham Street
Rockland, MA 02370

Intrusion Prevention and Active Response: Deploying Network and Host IPS

Copyright © 2005 by Syngress Publishing, Inc. All rights reserved. Printed in the United States of America. Except as permitted under the Copyright Act of 1976, no part of this publication may be reproduced or distributed in any form or by any means, or stored in a database or retrieval system, without the prior written permission of the publisher, with the exception that the program listings may be entered, stored, and executed in a computer system, but they may not be reproduced for publication.

Printed in the United States of America

1 2 3 4 5 6 7 8 9 0

ISBN: 1-932266-47-X

Co-Founder, President: Chris Williams
Co-Founder, Vice President
of Marketing: Amorette Pedersen
Publisher: Andrew Williams
Acquisitions Editor: Jaime Quigley

Technical Editor: Michael Rash
Cover Designer: Michael Kavish
Page Layout and Art: Patricia Lupien
Copy Editor: Judy Eby
Indexer: Odessa&Cie

Distributed by O’Reilly Media, Inc. in the United States and Canada.

For information on rights and translations, contact Matt Pedersen, Director of Sales and Rights, at Syngress Publishing; email matt@syngress.com or fax to 781-681-3585.



Acknowledgments

Syngress would like to acknowledge the following people for their kindness and support in making this book possible.

Thank you to Stephen Northcutt for sharing his insights in the Foreword of this book.

Syngress books are now distributed in the United States and Canada by O'Reilly Media, Inc. The enthusiasm and work ethic at O'Reilly is incredible and we would like to thank everyone there for their time and efforts to bring Syngress books to market: Tim O'Reilly, Laura Baldwin, Mark Brokering, Mike Leonard, Donna Selenko, Bonnie Sheehan, Cindy Davis, Grant Kikkert, Opol Matsutaro, Steve Hazelwood, Mark Wilson, Rick Brown, Leslie Becker, Jill Lothrop, Tim Hinton, Kyle Hart, Sara Winge, C. J. Rayhill, Peter Pardo, Leslie Crandell, Valerie Dow, Regina Aggio, Pascal Honscher, Preston Paull, Susan Thompson, Bruce Stewart, Laura Schmier, Sue Willing, Mark Jacobsen, Betsy Waliszewski, Dawn Mann, Kathryn Barrett, John Chodacki, and Rob Bullington. And a hearty welcome to Aileen Berg—glad to be working with you.

The incredibly hard working team at Elsevier Science, including Jonathan Bunkell, Ian Seager, Duncan Enright, David Burton, Rosanna Ramacciotti, Robert Fairbrother, Miguel Sanchez, Klaus Beran, Emma Wyatt, Rosie Moss, Chris Hossack, Mark Hunt, and Krista Leppiko, for making certain that our vision remains worldwide in scope.

David Buckland, Marie Chieng, Lucy Chong, Leslie Lim, Audrey Gan, Pang Ai Hua, and Joseph Chan of STP Distributors for the enthusiasm with which they receive our books.

Kwon Sung June at Acorn Publishing for his support.

David Scott, Tricia Wilden, Marilla Burgess, Annette Scott, Andrew Swaffer, Stephen O'Donoghue, Bec Lowe, and Mark Langley of Woodslane for distributing our books throughout Australia, New Zealand, Papua New Guinea, Fiji Tonga, Solomon Islands, and the Cook Islands.

Winston Lim of Global Publishing for his help and support with distribution of Syngress books in the Philippines.



Lead Author/Technical Editor

Michael Rash works as a Security Research Engineer in Columbia, MD for Enterasys Networks, Inc. He is a frequent contributor to open source endeavors such as Bastille-Linux and the Netfilter Project, and has written security articles for publications such as *Sys Admin Magazine*, the *Linux Journal*, and *USENIX ;login:* magazine. Michael is the author of FwSnort and PSAD; two open source security tools designed to blur the boundaries between Netfilter firewalls and the Snort Intrusion Detection System. He is co-author of *Snort 2.1 Intrusion Detection* (Syngress Publishing, ISBN: 1931836043). He holds a master's degree in applied mathematics with a concentration in computer security from the University of Maryland, and resides in Maryland with his wife, Katie. More information about Michael and his open source projects can be found on his website: www.cipherdyne.org/



Contributing Authors

Angela Orebaugh is a Senior Scientist in the Advanced Technology Research Center of Sytex, Inc. where she works with a specialized team to advance the state of the art in information systems security. She has over 10 years experience in information technology, with a focus on perimeter defense, secure network design, vulnerability discovery, penetration testing, and intrusion detection systems. She has a master's degree in computer science, and is currently pursuing her Ph.D. with a concentration in information security at George Mason University. Angela is the author of the Syngress best seller *Ethereal Packet Sniffing* (ISBN: 1-932266-82-8). She has also contributed to *Network Perimeter Security: The Definitive Guide to Firewalls, VPNs, Routers, and Network Intrusion Detection*, and

the *IT Ethics Handbook: Right and Wrong for IT Professionals* (Syngress, ISBN: 1-931836-14-0). Angela is a researcher, writer, and speaker for SANS Institute, where she has helped to develop and revise SANS course material and also serves as the Senior Coach for the SANS Local Mentor Program and SANS@Home. She holds several professional certifications including CISSP, GCIA, GCFW, GCIH, GSEC, and CCNA. More information on Angela's research and publications is located at www.securityknox.com.

Becky Pinkard (CCSA, CCNA, GCIA) has worked in the information technology industry for over 10 years. She is currently a senior security architect with a Fortune 50 company where she is delighted to work with security technology on a daily basis. Becky's main areas of interest are intrusion detection, pen testing, vulnerability assessments, risk management, and forensics. She is a SANS Certified Instructor and has taught for the SANS Institute since 2001. She participated on the Strategic Advisory Council for the Center for Internet Security where she edited the first draft of the CIS Windows NT benchmark. Becky holds a bachelor's degree from Texas A&M University and is a member of the North Texas chapter of InfraGard. She'd like to send out hacker-like greetz to her wonderful partner, awesome family, and incredible friends—*you are all loved beyond compare*.

Graham Clark is a Software Engineer working for Enterasys Networks, Inc. in Columbia, MD. Graham is a member of the Dragon team—a renowned and well-established network intrusion detection system where his main interests and responsibilities are host-based intrusion detection and prevention. He is the author of the web-server intrusion prevention capability that Dragon Host Sensor offers in its 7.0 release. Previously, Graham focused on abstract performance modeling of computers and networks, and holds a PhD in computer science from the University of Edinburgh, Scotland. He lives in Maryland with his wife, Leah.

Jake Babbin works as a contractor with a government agency filling the role of Intrusion Detection Team Lead. He has worked in both private industry as a security professional and in government space in a variety of IT security roles. He is a speaker at several IT security conferences and is a frequent assistant in SANS Security Essentials Bootcamp, Incident Handling and Forensics courses. Jake lives in Virginia.



Technical Reviewer

Anne Henmi is a System Administrator at the Center for Advanced Computational Research (CACR) at the California Institute of Technology. She is in charge of information security at CACR, which includes every aspect of information security including intrusion detection (running Snort, of course), network security, system security, internal IT auditing, and network security policy. Her specialties include Linux, Secure Shell, public key technologies, penetration testing, and network security architectures. Anne's background includes positions as a Principal Security Consultant at SSH Communications Security, and as an Information Security Analyst at VeriSign, Inc.

Contents

Chapter 1 Intrusion Prevention and Active Response . . .	1
Introduction	2
The Leap from Passive Detection to Active Countermeasures	4
Network Active Response	4
Network Intrusion Prevention	6
Network Countermeasures	7
Host Active Response	9
Host Intrusion Prevention	10
Host Countermeasures	11
Hybrid Countermeasures	12
Deployment Architectures	12
Network Architectures	13
Host Architectures	15
Applications of Intrusion Prevention	16
Worms and Automated Exploits	18
Well-defined Attacks	19
Vulnerable Software that Cannot be Patched or Upgraded	20
Checklist	21
Summary	22
Solutions Fast Track	23
Links to Sites	24
Frequently Asked Questions	26
Chapter 2 Packet Inspection for Intrusion Analysis . . .	29
Introduction	30
Defining Deep Packet Inspection	31
Current Packet Inspection Technologies	32
Packet Filters	32
Application Proxies	32

- Stateful Packet Filtering33
- New Packet Inspection Methods35
 - Protocol Standards Compliance36
 - Protocol Anomaly Detection37
 - Detecting Malicious Data39
 - Application Control40
 - Signature Matching40
- Attack, Detection, and Prevention Examples42
 - Binary Code in HTTP headers42
 - HTTP or HTTPS Tunneling43
 - URL Directory Traversal44
 - Excessive HTTP URL and Header Length46
 - Cross-site Scripting47
 - SQL Injection48
 - Malicious URLs50
 - Signature Matching on Payload Content51
 - Inspect File Transfers55
 - Inspect Mail Attachments56
 - Decrypt Connections for Inspection58
 - Inline Network-based Anti-virus and Worm Detection59
- Calculating Packet Sizes60
- Evolution of the Perimeter62
- Next Generation Security Devices63
- Summary65
- Solutions Fast Track66
- Links to Sites70
- Frequently Asked Questions71
- Chapter 3 False Positives and Real Damage73**
 - Introduction74
 - The Last Word on Port Scan Responses76
 - Minimizing the Network Discovery Footprint78
 - Restricting Scan Ports to Possessed Exploits.81
 - Extending Scan Time Delays.83
 - Cloaking the Source Address85
 - Nmap Idle Scanning.89
 - Application Layer Attack Spoofing91

False Positives: A Viewpoint Derived from Bayesian Statistics	95
Checklist	98
Summary	99
Solutions Fast Track	100
Links to Sites	101
Mailing Lists	101
Frequently Asked Questions	102
Chapter 4 Four Layers of IPS Actions	105
Introduction	106
Kerio Personal Firewall DOS	107
Description of Attack	107
Application Layer	111
Transport Layer	113
Network Layer	114
Data Link Layer	116
Witty Attack	117
Description of Attack	117
Application Layer	119
Transport Layer	119
Network Layer	121
Data Link Layer	121
SSH1 CRC32 Compensation Attack	122
Description of Attack	122
Application Layer	124
Transport Layer	124
Network Layer	125
Data Link Layer	125
Checklist	126
Summary	127
Solutions Fast Track	128
Links to Sites	129
Mailing Lists	130
Frequently Asked Questions	131

Chapter 5 Network Inline Data Modification	133
Introduction	134
Application Layer Data Modification and Protocol Breakage	136
Snort_inline	138
Installation	139
Operation	142
Netfilter Data Replacement Patch	146
Installation	147
Netfilter String Match Operation	152
ASCII String Matching and Data Replacement	156
Binary Data Matching and Replacement	162
Application-Layer Byte Replacement	166
DNS Exploit: x86 Linux Overflow	170
Microsoft Frontpage Server Extensions Attack	174
Metasploit LSASS Exploit	179
Checklist	184
Summary	185
Solutions Fast Track	186
Links to Sites	188
Mailing Lists	189
Frequently Asked Questions	190
Chapter 6 Protecting Your Host Through the Operating System	193
Introduction	194
Motivating IPS on the Host	194
What Isn't a Host IPS?	195
What is a Host IPS?	196
Process and Memory Management	197
Segmentation	199
Pagination	201
Process Address Space	203
The Bad Joke Server	203
Using the Stack	210
Buffer Overflow Protection	214
What is a Buffer Overflow?	214

Compromising the Bad Joke Server Using Metasploit . . .	215
Software Solutions for Protecting the Stack	223
Extending the Compiler	223
Reimplementing Unsafe Library Functions	229
Stack Randomization	229
Using the Processor Architecture	231
Making the Stack Non-Executable	231
Finer-Grained Non-Executable Memory	235
PaX	237
Running a Hardened OS	242
Adamantix	242
Hardened Gentoo	242
Preventing Damage After an Exploit is Delivered	245
Access Control	245
SELinux – Mandatory Access Control Implemented	246
Checklist	250
Summary	251
Solutions Fast Track	252
Links to Sites	254
Frequently Asked Questions	255
Chapter 7 IPS at the Application Layer	257
Introduction	258
Motivating Application-level IPS	259
Attacking a Web Server	260
SQL Injection	260
Cross-site Scripting (XSS)	261
Form Field Manipulation	262
Positioning an Application-level IPS	264
Disadvantages of a Remote IPS	264
Pros and Cons of a Local IPS	271
Processing Application-layer Data	272
Testing Your Web Server with Nikto	273
Deploying Application-level IPS	278
ModSecurity	278
IIS Lockdown	283
SecureIIS	285

Checklist	.288
Summary	.289
Solutions Fast Track	.290
Frequently Asked Questions	.292
Chapter 8 Deploying Open Source IPS Solutions	.295
Introduction	.296
Attack Simulations	.299
Web Server WWWBoard passwd.txt Access	.301
NFS Mountd Exploit	.305
Snort Flexible Response Plugin	.307
SnortSam	.309
Snortsam in Action	.312
WWWBoard passwd.txt Access Attack	.313
NFS mountd Overflow Attack	.320
Fwsnort	.323
WWWBoard passwd.txt Access Attack (Revisited)	.326
NFS mountd Overflow Attack (Revisited)	.331
Snort Inline	.336
Architecture	.337
Web Server Attack	.338
NFS mountd Overflow Attack	.341
Modsecurity	.344
LIDS	.348
Grsecurity and PaX	.351
Portsentry and PSAD	.352
Summary	.358
Solutions Fast Track	.359
Links to Sites	.362
Frequently Asked Questions	.363

Chapter 9 IPS Evasion Techniques (Network)	367
Introduction	368
How to Cause Problems with an IPS Platform	370
Malformed packets...oh my!	370
Snort	372
Spoofed traffic... I Blocked My Business with My IPS!	376
Bandwidth Concerns...This Thing is Inline, Right?!	377
Mitigation Strategies	378
How'd That SSH Connection Get Out Our Firewall?	379
Border Routers and Defense in Depth	380
Network Design Constraints	382
Summary	385
Solutions Fast Track	386
Frequently Asked Questions	388

Foreword

Within a year of the infamous “Intrusion Detection is Dead” report by Gartner, we started seeing intrusion prevention system (IPS) products actually working in the real world. Security professionals will be approaching management for funding in the next year or two to procure intrusion prevention devices, especially intelligent switches such as the 3Com (TippingPoint), as well as host-based intrusion prevention solutions like Cisco Security Agent, Platform Logic, Ozone or CrossTec. Both managers and security technologists face a pressing need to get up-to-speed, and fast, on the commercial and open source intrusion prevention solutions.

What you’ll find in the chapters to follow is the first book-length work that specifically concentrates on the concept, implementation, and implications of intrusion prevention and active response. The term IPS has been thrown around with reckless abandon by the security community. Here, the author team works to establish a common understanding and terminology, and compare the approaches to intrusion prevention.

This book provides a survey of various intrusion prevention and active response technologies for both networks (data link through application layer) and individual hosts (kernel enforced system call interception, buffer overflow prevention, and application shims). Readers are strongly encouraged to read the cautionary chapter devoted to discussing the implications of false positives, which carry much more damaging consequences for an IPS than for an IDS (which is strictly passive). The ability of a network or system to temporarily reconfigure itself in response to an “event” generated by some underlying intrusion detection capability (on which IPS’s are fundamentally built) can wreak havoc unless used for very limited and well-defined events. The authors

emphasize the need to treat intrusion prevention as one tool in the toolbox and not as a magic technology that will save your organization from any threat.

Other important topics include various open source tools that offer intrusion prevention and/or active response capabilities, including Snort_inline, Mod-security, LIDS, FWSnort, SnortSam, Bro, and more. There is a chapter devoted exclusively to the concept of modifying application layer data by an inline device, as implemented by the *replace* keyword in Snort_inline, and also in a custom patch that has been developed for the Netfilter string match extension.

There are also a few examples of Metasploit; one example even includes a custom exploit written for a custom server to assist in illustrating the effectiveness of various host-level buffer overflow prevention technologies.

This book will provide you with the opportunity to grasp the necessary material on the various intrusion prevention and active response capabilities to make informed decisions about which (if any) are applicable to your networks and hosts.

It will leave you with a healthy respect for the limitations of detecting intrusions in the first place, and why deploying an IPS can be risky. It can also help you avoid fundamental architectural errors, such as placing a chokehold style IPS in front of your firewall, or forgetting the importance of validating latency before signing your check. An IPS that is properly configured and tested can provide an awesome capability in some cases, such as a protection mechanism for legacy systems that simply cannot be patched, but are Internet facing.

—Stephen Northcutt
Director of Training and Certification
The SANS Institute
December 2004

Intrusion Prevention and Active Response

Solutions in this Chapter:

- The Leap from Passive Detection to Active Countermeasures
 - Deployment Architectures
 - Applications of Intrusion Prevention
-
- ☑ Summary
 - ☑ Solutions Fast Track
 - ☑ Frequently Asked Questions