SYNGRESS®




# 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

## solutions@syngress.com

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.

SYNGRESS®

# 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**

| 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


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

# 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, Modsecurity, 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 neccessary 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*

# Chapter 1

# 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