JAY BEALE'S OPEN SOURCE SECURITY SERIES

SYNGRESS®

4 FREE BOOKLETS
YOUR SOLUTIONS MEMBERSHIP

SYNGRESS
4 FREE
E-BOOKLETS
PUBLISHING

Snort®
IDS and IPS Toolkit

Featuring Jay Beale and Members of the Snort Team from Sourcefire®

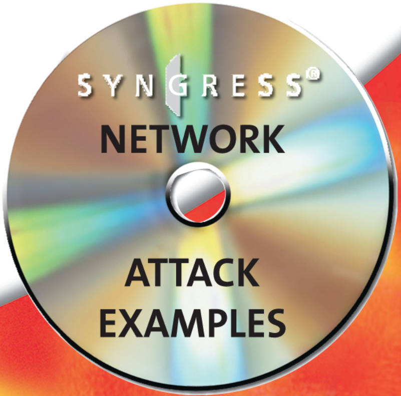
Andrew R. Baker
Joel Esler

SOURCEfire®
Security for the real world.

Foreword by Stephen Northcutt,
President, The SANS Technology Institute

Toby Kohlenberg Technical Editor

Raven Alder • Dr. Everett F. (Skip) Carter, Jr • James C. Foster • Matt Jonkman • Raffael Marty • Eric Seagren



Jay Beale's Open Source Security Series

SYNGRESS®

Snort®

IDS and IPS Toolkit

SOURCEfire®
Security for the real world.

Featuring Jay Beale
and Members of the Snort Team

Andrew R. Baker
Joel Esler

Foreword by Stephen Northcutt,
President, The SANS Technology Institute

Toby Kohlenberg Technical Editor

Raven Alder • Dr. Everett F. (Skip) Carter, Jr •
James C. Foster • Matt Jonkman •
Raffael Marty • Eric Seagren

KEY	**SERIAL NUMBER**
001	HJIRTCV764
002	PO9873D5FG
003	829KM8NJH2
004	854HLM329D
005	CVPLQ6WQ23
006	VBP965T5T5
007	HJJJ863WD3E
008	2987GVTWMK
009	629MP5SDJT
010	IMWQ295T6T

PUBLISHED BY
Syngress Publishing, Inc.
Elsevier, Inc.
30 Corporate Dr.
Burlington, MA 01803

Snort Intrusion Detection and Prevention Toolkit

1 2 3 4 5 6 7 8 9 0
ISBN-10: 1-59749-099-7
ISBN-13: 978-1-59749-099-3

Publisher: Andrew Williams
Acquisitions Editor: Erin Heffernan
Technical Editor: Toby Kohlenburg
Cover Designer: Michael Kavish

Page Layout and Art: Patricia Lupien
Copy Editor: Audrey Doyle
Indexer: Julie Kawabata

For information on rights, translations, and bulk sales, contact Matt Pedersen, Commercial Sales Director, at Syngress Publishing; email m.pedersen@elsevier.com or call 781-359-2450.

Acknowledgments

A special thanks to Marty Roesch and the rest of the Snort developers for all their efforts to maintain Snort: Erek Adams, Andrew R. Baker, Brian Caswell, Roman D., Chris Green, Jed Haile, Jeremy Hewlett, Jeff Nathan, Marc Norton, Chris Reid, Daniel Roelker, Marty Roesch, Dragos Ruiu, JP Vossen. Daniel Wittenberg, and Fyodor Yarochkin.

Thank you to Mike Guiterman, Michele Perry, and Joseph Boyle at Sourcefire for making this book possible.

Technical Editor

Toby Kohlenberg is a Senior Information Security Specialist for Intel Corporation. He does penetration testing, incident response, malware analysis, architecture design and review, intrusion analysis, and various other things that paranoid geeks are likely to spend time dealing with. In the last two years he has been responsible for developing security architectures for world-wide deployments of IDS technologies, secure WLANs, Windows 2000/Active Directory, as well as implementing and training a security operations center. He is also a handler for the Internet Storm Center, which provides plenty of opportunity to practice his analysis skills. He holds the CISSP, GCFW, GCIH, and GCIA certifications. He currently resides in Oregon with his wife and daughters, where he enjoys the 9 months of the year that it rains much more than the 3 months where it's too hot.

Contributing Authors

Raven Alder is a Senior Security Engineer for IOActive, a consulting firm specializing in network security design and implementation. She specializes in scalable enterprise-level security, with an emphasis on defense in depth. She designs large-scale firewall and IDS systems, and then performs vulnerability assessments and penetration tests to make sure they are performing optimally. In her copious spare time, she teaches network security for LinuxChix.org and checks cryptographic vulnerabilities for the Open Source Vulnerability Database. Raven lives in Seattle, WA. Raven was a contributor to *Nessus Network Auditing* (Syngress Publishing, ISBN: 1931836086).

Raven Alder is the author of Chapters 1 and 2.

Andrew R. Baker is the Product Maintenance Manager for Sourcefire, Inc. His work experience includes the development and use of intrusion detection systems, security event correlation, as well as the use of vulnerability scanning software, network intrusion analysis, and network infrastructure management. Andrew has been involved in the Snort project since 2000. He is the primary developer for Barnyard, which he started working on in 2001 to address performance problems with the existing output plugins.

Andrew has instructed and developed material for the SANS Institute, which is known for providing information security training and GIAC certifications. He has an MBA from the R.H. Smith School of Business at the University of Maryland and a Bachelors of Science in Computer Science from the University of Alabama at Birmingham.

Andrew R. Baker is the author of Chapters 5 and 13.

Dr. Everett F. (Skip) Carter, Jr. is President of Taygeta Network Security Services (a division of Taygeta Scientific Inc.). Taygeta Scientific Inc. provides contract and consulting services in the areas of scientific computing, smart instrumentation, and specialized data analysis. Taygeta Network Security Services provides security services for real-time firewall and IDS management and monitoring, passive network traffic analysis audits, external security reviews, forensics, and incident investigation.

Skip holds a Ph.D. and an M.S. in Applied Physics from Harvard University. In addition he holds two Bachelor of Science degrees (Physics and Geophysics) from the Massachusetts Institute of Technology. Skip is a member of the American Society for Industrial Security (ASIS). He was contributing author of Syngress Publishing's book, *Hack Proofing XML* (ISBN: 1931836507). He has authored several articles for *Dr. Dobbs Journal* and *Computer Language* as well as numerous scientific papers and is a former columnist for *Forth Dimensions* magazine. Skip resides in Monterey, CA, with his wife, Trace, and his son, Rhett.

Dr. Everett F. (Skip) Carter, Jr. is the author of Chapter 12.