

“Practical Intrusion Analysis provides a solid fundamental overview of the art and science of intrusion analysis.”

—**Nate Miller**, Cofounder, Stratum Security



PRACTICAL INTRUSION ANALYSIS

Prevention and Detection for
the Twenty-First Century



RYAN TROST

www.it-ebooks.info

Practical Intrusion Analysis

This page intentionally left blank

Practical Intrusion Analysis

**PREVENTION AND DETECTION
FOR THE TWENTY-FIRST CENTURY**

Ryan Trost

◆◆ Addison-Wesley

Upper Saddle River, NJ • Boston • Indianapolis • San Francisco
New York • Toronto • Montreal • London • Munich • Paris • Madrid
Capetown • Sydney • Tokyo • Singapore • Mexico City

Many of the designations used by manufacturers and sellers to distinguish their products are claimed as trademarks. Where those designations appear in this book, and the publisher was aware of a trademark claim, the designations have been printed with initial capital letters or in all capitals.

The author and publisher have taken care in the preparation of this book, but make no expressed or implied warranty of any kind and assume no responsibility for errors or omissions. No liability is assumed for incidental or consequential damages in connection with or arising out of the use of the information or programs contained herein.

The publisher offers excellent discounts on this book when ordered in quantity for bulk purchases or special sales, which may include electronic versions and/or custom covers and content particular to your business, training goals, marketing focus, and branding interests. For more information, please contact:

U.S. Corporate and Government Sales
(800) 382-3419
corpsales@pearsontechgroup.com

For sales outside the United States please contact:

International Sales
international@pearson.com

Visit us on the Web: informit.com/aw

Library of Congress Cataloging-in-Publication Data:

Trost, Ryan.

Practical intrusion analysis : prevention and detection for the twenty-first century / Ryan Trost.

p. cm.

Includes index.

ISBN-13: 978-0-321-59180-7 (pbk. : alk. paper)

ISBN-10: 0-321-59180-1

1. Computer networks--Security measures. 2. Computer networks--Monitoring. 3. Computer security.
4. Computers--Access control. I. Title.

TK5105.59.T76 2009

005.8--dc22

2009019158

Copyright © 2010 Pearson Education, Inc.

All rights reserved. Printed in the United States of America. This publication is protected by copyright, and permission must be obtained from the publisher prior to any prohibited reproduction, storage in a retrieval system, or transmission in any form or by any means, electronic, mechanical, photocopying, recording, or likewise. For information regarding permissions, write to:

Pearson Education, Inc
Rights and Contracts Department
501 Boylston Street, Suite 900
Boston, MA 02116
Fax (617) 671-3447

ISBN-13: 978-0-321-59180-7

ISBN-10: 0-321-59180-1

Text printed in the United States on recycled paper at R.R. Donnelley in Crawfordsville, Indiana.

First printing July 2009

Editor-in-Chief

Karen Gettman

Acquisitions Editor

Jessica Goldstein

Senior Development Editor

Chris Zahn

Managing Editor

Kristy Hart

Project Editor

Jovana San Nicolas-Shirley

Copy Editor

Sheri Cain

Indexer

Erika Millen

Proofreader

Debbie Williams

Publishing Coordinator

Romny French

Cover Designer

Chuti Prasertsith

Compositor

Jake McFarland

To my loving wife, Kasey, who is pregnant with our first beautiful child.

To my supportive families: To my parents, sister, and brother, who have supported me, motivated me and somehow sustained my endless IT ramblings. And to my wife's family, the Arbacas clan, who have only had to endure my InfoSec rambling for a couple years and still invite me to dinner.

I very much appreciate all the help and support!

This page intentionally left blank

Contents

	Preface	xv
Chapter 1	Network Overview	1
	Key Terms and Concepts	2
	Brief History of the Internet	2
	Layered Protocols	3
	TCP/IP Protocol Suite	10
	Internet Protocol	14
	Addressing	21
	IP Addresses	22
	IPv6	27
	Summary	29
Chapter 2	Infrastructure Monitoring	31
	Network-Analysis Tools	32
	Packet Sniffing	35
	Accessing Packets on the Network	40
	SPANs (Port Mirroring)	40
	Network Taps	43
	To Tap or to SPAN	48
	Defense-in-Depth	50
	Summary	51

Chapter 3	Intrusion Detection Systems	53
	IDS Groundwork	54
	From the Wire Up	55
	DoS Attacks	55
	IP Fragmentation	57
	TCP Stream Issues	58
	Target-Based Reassembly	59
	Two Detection Philosophies: Signature and Anomaly Based	60
	Snort: Signature-Based IDS	61
	Two Signature Writing Techniques	67
	Bro: An Anomaly-Based IDS	74
	Similarities Between the Systems	82
	Summary	85
Chapter 4	Lifecycle of a Vulnerability	87
	A Vulnerability Is Born	87
	FlashGet Vulnerability	88
	Collecting a Sample Packet Capture	90
	Packet Analysis and Signature-Writing	95
	Signature Tuning	100
	Detection Tuning	100
	Performance Tuning	101
	Advanced Examples	104
	CitectSCADA ODBC Server Buffer Overflow: Metasploit	104
	FastStone Image Viewer Bitmap Parsing	109
	LibspF2 DNS TXT Record Size Mismatch	114
	Summary	117
Chapter 5	Proactive Intrusion Prevention and Response via Attack Graphs	119
	Topological Vulnerability Analysis (TVA)	121
	Overview of Approach	121
	Illustrative Example	122
	Limitations	125
	Attack Modeling and Simulation	126
	Network Attack Modeling	126
	Attack Simulation	130
	Optimal Network Protection	134
	Vulnerability Mitigation	135
	Attack Graph Visualization	137
	Security Metrics	139

	Intrusion Detection and Response	141
	Intrusion Detection Guidance	141
	Attack Prediction and Response	144
	Summary	147
	Acknowledgments	147
	Endnotes	148
Chapter 6	Network Flows and Anomaly Detection	151
	IP Data Flows	152
	NetFlow Operational Theory	153
	A Matter of Duplex	155
	Cisco IOS NetFlow and Flexible NetFlow	156
	sFlow: More Data, But Less Frequency	159
	Internet Protocol Flow Information Export (IPFIX)	161
	It's a Virtual World	162
	Endless Streams of Data	164
	Behavioral Analysis and Anomaly Detection	167
	Compare and Contrast	172
	IDS and NetFlow	172
	Signature Updates	173
	IDS System Resources	174
	Syslog and NetFlow	178
	Technology Matrix	180
	Summary	182
	Endnotes	183
Chapter 7	Web Application Firewalls	185
	Web Threat Overview	186
	Why a WAF?	189
	WAF Protection Models	191
	Positive Security Model	191
	Negative Security Model	192
	Virtual Patching Model	193
	Output Detection Model/Content Scrubbing	194
	WAF Policy Models	195
	Learning	195
	Vulnerability Assessment Feedback	195
	Manual Entry	195
