

# Hardening Windows

## Second Edition



Jonathan Hassell

## **Hardening Windows, Second Edition**

**Copyright © 2006 by Jonathan Hassell**

All rights reserved. No part of this work may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, or by any information storage or retrieval system, without the prior written permission of the copyright owner and the publisher.

ISBN (pbk): 1-59059-539-4

Printed and bound in the United States of America 9 8 7 6 5 4 3 2 1

Trademarked names may appear in this book. Rather than use a trademark symbol with every occurrence of a trademarked name, we use the names only in an editorial fashion and to the benefit of the trademark owner, with no intention of infringement of the trademark.

Lead Editor: Jim Sumser

Technical Reviewer: Oris Orlando

Editorial Board: Steve Anglin, Dan Appleman, Ewan Buckingham, Gary Cornell, Tony Davis, Jason Gilmore, Jonathan Hassell, Chris Mills, Dominic Shakeshaft, Jim Sumser

Associate Publisher: Grace Wong

Project Manager: Kylie Johnston

Copy Edit Manager: Nicole LeClerc

Copy Editor: Liz Welch

Assistant Production Director: Kari Brooks-Copony

Production Editor: Katie Stence

Compositor: Pat Christenson

Proofreader: Elizabeth Berry

Indexer: Toma Mulligan

Interior Designer: Van Winkle Design Group

Cover Designer: Kurt Krames

Manufacturing Director: Tom Debolski

Distributed to the book trade worldwide by Springer-Verlag New York, Inc., 233 Spring Street, 6th Floor, New York, NY 10013. Phone 1-800-SPRINGER, fax 201-348-4505, e-mail [orders-ny@springer-sbm.com](mailto:orders-ny@springer-sbm.com), or visit <http://www.springeronline.com>.

For information on translations, please contact Apress directly at 2560 Ninth Street, Suite 219, Berkeley, CA 94710. Phone 510-549-5930, fax 510-549-5939, e-mail [info@apress.com](mailto:info@apress.com), or visit <http://www.apress.com>.

The information in this book is distributed on an “as is” basis, without warranty. Although every precaution has been taken in the preparation of this work, neither the author(s) nor Apress shall have any liability to any person or entity with respect to any loss or damage caused or alleged to be caused directly or indirectly by the information contained in this work.

The source code for this book is available to readers at <http://www.apress.com> in the Source Code section.

# Contents

About the Author .....	xi
About the Technical Reviewer .....	xiii
Acknowledgments .....	xv
Introduction .....	xvii

## ■ CHAPTER 1    **Some Words About Hardening** .....

1

What Is Security? .....	2
The Security Dilemma .....	3
Enemies of Security .....	4
What Windows Is Lacking .....	4
Some General Hardening Suggestions .....	5
Software Considerations .....	6
Hardware and Network Considerations .....	7
Checkpoints .....	9

## ■ CHAPTER 2    **Windows NT Security** .....

11

Windows NT System Policy Editor .....	11
Customizing and Applying Policies to Multiple Computers .....	12
Resolving Conflicts Between Multiple Policies .....	13
Recommended User Policy Settings .....	14
Extending Policies .....	19
Passwords .....	19
Password Policies .....	20
Password Cracking .....	21
Protecting User Accounts .....	22
Registry Procedures .....	22
Protecting the File System .....	23
Locking Down Local Directories .....	23
Search Paths .....	24
Guarding Against Internet Threats .....	25
Windows NT Port Filtering .....	25
Protecting Against Viruses .....	26

Assigning Rights to Users .....	27
Granting and Revoking User Rights .....	27
Remote Access Server Configuration .....	30
Selecting Appropriate Communications Protocols and Methods ..	30
Security Implications of Domains .....	31
Checkpoints .....	32
 <b>CHAPTER 3 Windows 2000 Security .....</b>	 35
System Updates .....	35
The “Slipstreaming” Process .....	36
Critical Updates and Security Hotfixes .....	37
Managing Critical Updates Across Multiple Computers .....	37
Security Templates .....	38
Creating a Custom Security Template .....	40
Recommended Security Policy Settings .....	41
User Accounts .....	42
Local Options .....	43
Other Security Considerations .....	46
Windows Component Selection and Installation .....	46
Tightening Running Services .....	47
Checkpoints .....	48
 <b>CHAPTER 4 Windows XP Security .....</b>	 49
Implementing the Built-In Windows XP Firewall .....	49
Profiles .....	50
Configuring Through Group Policy .....	51
The Internet Connection Firewall in XP Gold and Service Pack 1 .....	51
Disabling Unnecessary Services .....	53
Providing a Secure Configuration for Services .....	62
Microsoft Baseline Security Analyzer Patch Check and Security Tests .....	63
Installing Microsoft Baseline Security Analyzer .....	63
Penetration Tests .....	63
File System Security .....	64
Disable Automated Logins .....	65

	Hardening Default Accounts .....	65
	Use Runas for Administrative Work .....	66
	Disable Infrared Transfers .....	67
	Using Forensic Analysis Techniques .....	67
	Checkpoints .....	69
<b>CHAPTER 5</b>	<b>Windows Server 2003 Security .....</b>	<b>71</b>
	Enhancements to Security in Service Pack 1 .....	71
	The Security Configuration Wizard .....	72
	Installing the SCW .....	73
	Creating a Security Policy with the SCW .....	73
	The Rollback Feature .....	80
	SCW Best Practices .....	80
	Using SCW from the Command Line .....	81
	Checkpoints .....	82
<b>CHAPTER 6</b>	<b>Deploying Enterprise Security Policies .....</b>	<b>85</b>
	System Policies, Group Policies, and Interaction .....	85
	Mixing Policies and Operating Systems .....	87
	Security and the Group Policy Framework .....	89
	Organized Layout of Policies .....	90
	Policy Application Precedence .....	92
	Creating Security Configuration Files .....	92
	Default Domain Policy .....	94
	Default Domain Controller Security Policies .....	94
	Troubleshooting Group Policy .....	95
	Checkpoints .....	96
<b>CHAPTER 7</b>	<b>Patch Management .....</b>	<b>99</b>
	About Windows Server Update Services .....	99
	Comparing Windows Server Update Services to Systems Management Server .....	100
	Using Windows Server Update Services: On the Server Side ....	101
	Using WSUS: On the Client Side .....	114
	Checkpoints .....	117

<b>CHAPTER 8</b>	<b>Network Access Quarantine Control</b>	119
	How Network Access Quarantine Works	120
	A Step-by-Step Overview of Network Access Quarantine Control	120
	Deploying NAQC	122
	Creating Quarantined Resources	122
	Writing the Baseline Script	123
	Installing the Listening Components	125
	Creating a Quarantined Connection Profile	127
	Distributing the Profile to Remote Users	129
	Configuring the Quarantine Policy	130
	Checkpoints	135
<b>CHAPTER 9</b>	<b>Internet Information Services Security</b>	137
	Completely Disable IIS	138
	Keeping IIS Updated	138
	Using Windows Update	139
	Using Network-Based Hotfix Installation	139
	Securing Files, Folders, and Scripts	140
	The Microsoft Indexing Service	142
	TCP/IP Port Evaluation	144
	Administrative and Default Pages	145
	The Ins and Outs of Internet Services Application Programming Interface	146
	Looking at Apache as an Alternative	146
	Checkpoints	147
<b>CHAPTER 10</b>	<b>Exchange Server 2003 Security</b>	149
	Installation Security	149
	Security Policy Modifications	151
	For Exchange Server Machines	151
	For Domain Controller Machines	151
	Service Security	152
	Patch Management	153
	Protecting Against Address Spoofing	154
	Protecting Against Denial-of-Service Attacks	156

Restricting SMTP Access.....	158
Controlling Access .....	160
Checkpoints.....	161
<b>CHAPTER 11 Security Auditing and Event Logs .....</b>	<b>163</b>
For Windows 2000, XP, and Server 2003 .....	163
Recommended Items to Audit.....	165
Event Logs .....	165
The Event Viewer.....	166
For Windows NT 4.0.....	167
Recommended Items to Audit.....	168
The Event Log .....	169
Filtering Events .....	169
What Might Be Missing .....	170
Checkpoints.....	170
<b>APPENDIX Quick-Reference Checklists .....</b>	<b>173</b>
Chapter 1: Some Words About Hardening .....	173
Chapter 2: Windows NT Security .....	174
Chapter 3: Windows 2000 Security.....	176
Chapter 4: Windows XP Security .....	177
Chapter 5: Windows Server 2003 Security .....	178
Chapter 6: Deploying Enterprise Security Policies .....	179
Chapter 7: Patch Management.....	180
Chapter 8: Network Access Quarantine Control .....	180
Chapter 9: Internet Information Services Security .....	181
Chapter 10: Exchange Server 2003 Security.....	181
Chapter 11: Security Auditing and Event Logs .....	183
<b>INDEX .....</b>	<b>185</b>