

"The most demystifying source of information since Toto exposed the Wizard. *Hacking Exposed Windows Server 2003* eliminates the mystique and levels the playing field by revealing the science behind the curtain." —Greg Wood, General Manager, Information Security, Microsoft Corporation

HACKING Windows® Server 2003 EXPOSED

Windows Security Secrets & Solutions

Joel Scambray
Stuart McClure

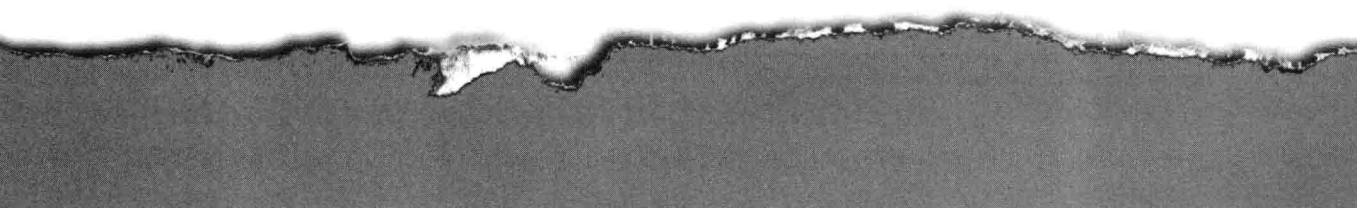
From the best-selling
authors of
Hacking Exposed



HACKING EXPOSED WINDOWS[®] SERVER 2003

JOEL SCAMBRAY
STUART McCLURE

McGraw-Hill/Osborne
New York Chicago San Francisco
Lisbon London Madrid Mexico City Milan
New Delhi San Juan Seoul Singapore Sydney Toronto



McGraw-Hill/Osborne
2100 Powell Street, 10th Floor
Emeryville, California 94608
U.S.A.

To arrange bulk purchase discounts for sales promotions, premiums, or fund-raisers, please contact **McGraw-Hill/Osborne** at the above address. For information on translations or book distributors outside the U.S.A., please see the International Contact Information page immediately following the index of this book.

Hacking Exposed Windows® Server 2003

Copyright © 2003 by Joel Scambray. 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 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.

234567890 FGR FGR 01987654

ISBN 0-07-223061-4

Publisher

Brandon A. Nordin

Vice President & Associate Publisher

Scott Rogers

Executive Acquisitions Editor

Jane K. Brownlow

Project Editor

Julie M. Smith

Acquisitions Coordinator

Athena Honore

Technical Editors

John Bock

Michael O'Dea

Copy Editor

Lisa Theobald

Proofreader

Susie Elkind

Indexer

Valerie Perry

Composition

Jean Butterfield

Lucie Ericksen

Illustrators

Kathleen Fay Edwards

Melinda Moore Lytle

Michael Mueller

Series Design

Dick Schwartz

Peter F. Hancik

Cover Series Design

Dodie Shoemaker

This book was published with Corel Ventura™ Publisher.

Information has been obtained by **McGraw-Hill/Osborne** from sources believed to be reliable. However, because of the possibility of human or mechanical error by our sources, **McGraw-Hill/Osborne**, or others, **McGraw-Hill/Osborne** does not guarantee the accuracy, adequacy, or completeness of any information and is not responsible for any errors or omissions or the results obtained from the use of such information.



HACKING EXPOSED WINDOWS® SERVER 2003

“Because attackers can strike at will and defenders must be constantly vigilant, protecting systems from malicious attack involves understanding how the bad guys operate. You cannot secure your systems unless you know what you’re up against and *Hacking Exposed Windows Server 2003* is an invaluable resource highlighting how attackers will attempt to assail your systems.”

—**Michael Howard**, Senior Program Manager,
Secure Windows Initiative, Microsoft

“If you want to be able to defend your systems, an understanding of the tools and techniques your attackers will use against you is essential. Frequent penetration testing of your own networks will give you the best insight into your actual security posture, and go far beyond what any security assessment tool or intrusion detection system can provide. *Hacking Exposed Windows Server 2003* levels the playing field, and gives you access to the same information as professional consultants.”

—**David LeBlanc**, Security Architect, Microsoft

“This book not only gives information that allows you to proactively secure hosts on your network before an attack, but provides the foundation needed to actively analyze and defend it once it does get attacked.”

—**Dave Dittrich**, University Computing Services, University of Washington



To the MSN Security team, for a year that I will never forget—thank you.

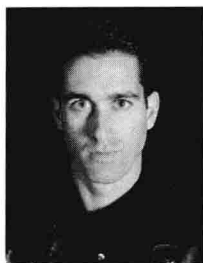
—Joel Scambray

For my wife and family. Without their love and support, little could be done.

—Stuart McClure

ABOUT THE AUTHORS

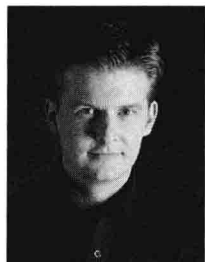
Joel Scambray



Joel is the Senior Director of MSN Security for Microsoft Corporation, where he faces daily the full brunt of the Internet's most notorious denizens, from spammers to Slammer. He is most widely recognized as co-author of *Hacking Exposed: Network Security Secrets & Solutions*, the international best-selling Internet security book that reached its Fourth Edition in February 2003. He is also lead author of *Hacking Exposed Web Applications*. Joel's writing draws primarily on his many years as an IT security consultant for clients ranging from members of the Fortune 50 to newly minted startups. He has spoken widely on information security to organizations including CERT, The Computer Security Institute (CSI), ISSA, ISACA, SANS, private corporations, and government agencies, including the FBI and the RCMP. Before joining Microsoft in August 2002, Joel helped launch security services startup Foundstone Inc. to a highly regarded position in the industry, and he previously held positions as a Manager for Ernst & Young, security columnist for Microsoft TechNet, Editor at Large for InfoWorld Magazine, and Director of IT for a major commercial real estate firm. Joel's academic background includes advanced degrees from the University of California at Davis and Los Angeles (UCLA), and he is a Certified Information Systems Security Professional (CISSP).

—Joel Scambray can be reached at joel@winhackingexposed.com.

Stuart McClure



Stuart McClure is president and chief technology officer of Foundstone, a leading global information security software, services and education provider employing one of the world's largest teams of network security experts. Foundstone empowers large enterprises, including US government agencies and Global 500 customers in the financial, technical and other industries including insurance, critical infrastructure, legal and manufacturing markets, to continuously and measurably manage and mitigate risk to protect the most important digital assets and their customers' private information from critical threats. Foundstone saves each customer millions in revenue and hundreds of man-hours annually in attack investigation and employee downtime that would have otherwise been lost to hackers, viruses, worms and other attacks.

Widely recognized for his extensive and in-depth knowledge of security products, Stuart is considered one of the industry's leading authorities in information security today. A well-published and acclaimed security visionary, Stuart brings over 14 years of technology and executive leadership to Foundstone with profound technical, operational,

and financial experience. Stuart leads both the product vision and strategy for Foundstone, as well as operational responsibilities for all technology development, support, and implementation. Since he assumed this leadership position, Stuart has helped grow annual revenues more than 100% every year since the company's inception in 1999.

In 1999, he took the lead in authoring *Hacking Exposed: Network Security Secrets and Solutions*. This book has been translated into 19 languages, and ranked the #4 computer book sold—positioning it as one of the best-selling security and computer books in history. Stuart has also co-authored *Hacking Exposed: Windows 2000* by McGraw-Hill/Osborne and *Web Hacking: Attacks and Defense* by Addison-Wesley.

Prior to Foundstone, Stuart held a variety of leadership positions in security and IT management, with Ernst & Young's National Security Profiling Team, two years as an industry analyst with InfoWorld's Test Center, five years as Director of IT with both state and local California government, two years as owner of an IT consultancy, and two years in IT with University of Colorado, Boulder.

Stuart holds a bachelor's degree in psychology and philosophy, with an emphasis in computer science applications from the University of Colorado, Boulder. He later earned numerous certifications including ISC2's CISSP, Novell's CNE, and Check Point's CCSE.

About the Contributing Author

Chip Andrews

Chip Andrews is a software security professional with over 12 years of software development experience and maintainer of the SQLSecurity.com website. He is a contributing author to several books including *SQL Server Security* (McGraw-Hill/Osborne, 2003) and others. Chip has also authored several articles for magazines such as *Microsoft Certified Professional* and *SQL Server Magazine* focusing on SQL security and software development issues. He has also been known to speak at security conferences concerning Microsoft SQL Server security issues and secure application design. When not working or consulting, he is boating and pretending that the computer was never invented.

About the Technical Reviewers

John Bock

As an R&D engineer at Foundstone, John Bock, CISSP, specializes in network assessment technologies and wireless security. John is responsible for designing new assessment features in the Foundstone Enterprise Risk Solutions product line. John has a strong background in network security both as a consultant and lead for an enterprise security team. Before joining Foundstone he performed penetration testing and security assessments,

and he spoke about wireless security as a consultant for Internet Security Systems (ISS). Prior to ISS he was a network security analyst at marchFIRST, where he was responsible for maintaining security on a 7000-user global network. John has also been a contributing author to *Hacking Exposed* (McGraw-Hill/Osborne) and *Special Ops: Host and Network Security for Microsoft, UNIX, and Oracle* *Special Ops: Internal Network Security* (Syngress, 2003).

Michael O'Dea

Michael O'Dea is Project Manager of Product Services for security firm Foundstone, Inc. Michael has been immersed in information technology for over 10 years, working with technologies such as enterprise data encryption, virus defense, firewalls, and proxy service solutions on a variety of UNIX and Windows platforms. Currently, Michael develops custom integration solutions for the Foundstone Enterprise vulnerability management product line. Prior to joining Foundstone, Michael worked as a senior analyst supporting Internet security for Disney Worldwide Services, Inc., the data services arm of the Walt Disney Company; and as a consultant for Network Associates, Inc., Michael has contributed to multiple security publications, including *Hacking Exposed: Fourth Edition* and *Special Ops: Internal Network Security*.

FOREWORD

Working with the precision of a neurosurgeon, the computational capability of a nuclear physicist and the tenacity of a rookie detective on his first stakeout, hackers dissect complex technologies in their quest to discover and exploit a microscopic network or computer gaffe.

This is a common perception IT professionals attribute to hackers and unless you arm yourself with the same knowledge as cyber-criminals, these statements might as well be true. Don't be intimidated by the mystique surrounding "hackers". Knowing how attackers think and the tools they use is the first step in mounting an effective defense.

These aren't new concepts, albeit perhaps uniquely applied. 2000 years ago, SunTzu detailed a basis for war in which he almost scientifically decomposes battle into many rational decisions. Most appropriate:

"know thy enemy and know thyself; in a hundred battles you will never be in peril. When you are ignorant of the enemy but know yourself, your chances of winning or losing are equal. If ignorant both of your enemy and of yourself, you are certain in every battle to be in peril."

The Art of War
Sun Tzu

The only barrier to an effective defense is knowledge. Whether you are a security hobbyist, an IT professional or experienced security practitioner, understanding the basic tools and methods are critical to establishing an effective defensive posture.

Computer hacking is no longer predicated on computer literacy and intelligence. Tool automation has effectively eliminated most, if not all intellectual barriers while the proliferation of high-speed access has dramatically improved the capabilities of the masses. The “art” of hacking detailed in the media through the eyes of infamous social-engineers turned consultants, no longer exists. Hacking today is a science. It is a series of tool enhanced processes methodically executed by criminals. In many cases, hacking has regressed to a state of cut and paste plagiarism.

In fact, a job description for the mass-market, average computer hacker might look like the following:

Job Title: Computer Hacker

The ideal candidate must have at least 3 months of computer experience. The candidate should be experienced in both the “cut” and “paste”, although we are willing to train. In addition, the ideal candidate must be able to count to at least 1. Counting from 0 to 15 is preferred. Working knowledge of letters “A” through “F” recommended. The right candidate will possess a Pentium III and have access to a discreet, high-speed internet connection.

Obviously the tongue-in-cheek job description overstates the simplicity with which these modern day miscreants operate. The point is, as computer owner, system administrator or network operator you don’t have to be smarter than every computer hacker, just recognize you’re smarter than most. Hackers don’t want you to read this book. *Hacking Exposed* unravels the mystery by opening the curtain.

The fact remains, the incidence of computer borne attacks will continue to grow in number, complexity and severity. And while there are minimal defenses against the motivated professional criminal, there are some basic steps to limit your exposure. Most importantly is arming yourself with the same basic knowledge as your attacker. Without a common understanding of the tools and methods used by our collective enemy, defending against the next generation of attack is futile. The least we can do is make it challenging.

Greg Wood
General Manager, Information Security
Microsoft Corporation

ACKNOWLEDGMENTS

First and foremost, many special thanks to all our families for once again supporting us through still more months of demanding research and writing. Their understanding and support was crucial to us completing this book. We hope that we can make up for the time we spent away from them to complete this project.

Secondly, we would like to thank all of our colleagues for providing contributions to this book. In particular, we acknowledge Chip Andrews, whose Chapter 11 is simply stellar, as always, and Greg Wood, whose Foreword and general insights into the practical application of security in the enterprise continue to be invaluable. Thanks also to Michael Howard and Dave Dittrich who generously provided quotations after reviewing drafts of the manuscript.

We'd also like to acknowledge the many people who provided so much help and guidance on many facets of this book, including the entire virtual security gang at Microsoft and the team at Foundstone. Special thanks to John Bock and Mike O'Dea for keeping us technically on track.

As always, we bow profoundly to all of the individuals that wrote the innumerable tools and proof-of-concept code that we document in this book, including Todd Sabin, Tim Mullen, Rain Forest Puppy, Mike Schiffman, Simple Nomad, Georgi Gunninski, Sir Dystic, Dildog, Weld Pond, Roelof Temmingh, Maceo, NSFfocus, eEye, Petter Nordahl-Hagen, and all of the people who continue to contribute anonymously to the collective codebase of security each day.

Thanks also to the contributors to the first edition, David Wong, Erik Birkholz, Clinton Mugge, and technical editor Eric Schultze, whose presence is still felt in the foundations of this book.

Big thanks must also go to the tireless McGraw-Hill/Osborne editors and production team who worked on the book, including our indefatigable acquisitions editor Jane Brownlow, editorial assistant Athena Honore who kept things on track, and especially project editor Julie Smith and her army of assiduous copy editors.

And finally, a tremendous “Thank You” to all of the readers of the first edition of this book, and all the books of the *Hacking Exposed* series, whose continuing support makes all of the hard work worthwhile.



INTRODUCTION

WINDOWS SECURITY: FACT OR FICTION?

If you are to believe the United States government, Microsoft Corporation controls a monopoly share of the computer operating system market, and possibly many other related software markets as well (web browsers, office productivity software, and so on). And despite continued jeers from its adversaries in the media and the marketplace, Microsoft manages to hold on to this “monopoly” year after year, flying in the face of a lengthening history of flash-in-the-pan information technology startups ground under by the merciless onslaught of change and the growing fickleness of the digital consumer. Love ‘em, hate ‘em, or both, Microsoft continues to produce some of the most broadly popular software products on the planet today.

And yet, in parallel with this continued popularity, most media outlets and many security authorities still continue to portray Microsoft’s software as fatally flawed from a security perspective. If Bill Gates’ products are so insecure, why do they seem to remain so popular?

The Windows Security Gap

The answer is really quite simple. Microsoft's products are designed for maximum ease-of-use, which drives their rampant popularity. What many fail to grasp is that security is a zero-sum game: the easier it is to use something, the more time and effort must go into securing it. Think of security as a continuum between the polar extremes of 100% security on one side and 100% usability on the other, where 100% security equals 0% usability, and 100% usability equates to 0% security.

The best example of this trade-off is Microsoft's flagship Web server, Internet Information Server (IIS). It comes pre-installed and fully configured on Windows Server 2003, and anyone with a halfway decent understanding of Web technologies can have an entire Web site up and running within minutes on IIS.

Unfortunately, if it is deployed on the Internet as-is, this Web server will be compromised and completely pillaged within days by opportunistic intruders armed with an arsenal of the latest hacker attacks against IIS, or it will be ravaged by one of the many IIS worms that continue to circulate on networks public and private.

NOTE

To its credit, Microsoft turned off IIS in the default Windows Server 2003 deployment. The product's tagline, "Do more with less," indicates that the continuum between 100% usability and 100% security is beginning to dawn on the folks in Redmond (grin).

Nevertheless, if you elect to deploy IIS because of its "usability" advantages (rapid development and deployment, easy GUI management, and so on), and we're betting you might because nearly 24% of the servers on the Internet made the same choice (that's #2 in the Netcraft.com September 2003 survey), then you are going to have to learn how to secure it. Since IIS version 4, Microsoft has published various checklists and tools to help make IIS secure from attack, but they don't ship with Windows and many never implement even the simplest elements to protect themselves.

Hacking Exposed Windows Server 2003 came about largely because of this tremendous gap between Microsoft's out-of-the-box configurations and what it takes to run their software—securely—in the real world.

Closing the Gap with *Hacking Exposed*

We show you how to eliminate this gap with the two-pronged approach adapted from the original *Hacking Exposed*, now in its fourth edition.

First, we catalog the greatest threats your Windows deployment will face and explain how they work in excruciating detail. How do we know these are the greatest threats? Because we are hired by the world's largest companies to break into their Windows-based networks, servers, products, and services, and we use them on a daily basis to do our jobs. And we've been doing it for over three years, researching the most recently publicized hacks, developing our own tools and techniques, and combining them into what we think is the most effective methodology for penetrating Windows security in existence.

Once we have your attention by showing you the damage that can be done, we tell you how to prevent each and every attack. Running Windows Server 2003 without understanding the information in this book is roughly equivalent to driving a car without seatbelts—down a slippery road, over a monstrous chasm, with no brakes, and the throttle jammed on full.

Embracing and Extending *Hacking Exposed*

For all of its similarities, *Hacking Exposed Windows Server 2003* is also distinct from the original title in several key ways. Obviously, it is focused on one platform, as opposed to the multi-disciplinary approach of *Hacking Exposed*. While *Hacking Exposed* surveys the Windows security landscape, this book peels back further layers to explore the byte-level workings of Windows security attacks and countermeasures, revealing insights that will turn the heads of even seasoned Windows system administrators. It is this in-depth analysis that sets it apart from the original title, where the burdens of exploring many other computing platforms necessitate superficial treatment of some topic areas.

NOTE

Throughout this book, we use the phrase “NT Family” to refer to all systems based on Microsoft’s “New Technology” (NT) platform, including Windows NT 3.x–4.x, Windows Server 2003, Windows XP, and Windows Server 2003. Where necessary, we will differentiate between desktop and server versions. In contrast, we will refer to the Microsoft DOS/Windows 1.x/3.x/9x/Me lineage as the “DOS Family.”

You will find no aspect of NT Family security treated superficially in this book. Not only does it embrace all of the great information and features of the original *Hacking Exposed*, it extends it in significant ways. Here, you will find all of the secret knowledge necessary to close the NT Family security gap for good, from the basic architecture of the system to the undocumented Registry keys that tighten it down.

HOW THIS BOOK IS ORGANIZED

This book is the sum of parts, parts which are described below from largest organizational level to smallest.

Parts

This book is divided into five parts:

I: Foundations

Security basics and an exploration of the features of the NT Family security architecture from the hacker’s perspective.

II: Profiling

Casing the establishment in preparation for the big heist.

III: Conquest

Breaking and entering via the traditional point of ingress, Windows file sharing services (SMB), exploitation of common Windows vulnerabilities, followed by escalating privilege, expanding influence, pillaging, and covering tracks.

IV: Exploiting Vulnerable Services & Clients

Attacking the NT Family through common features, including IIS, SQL, Terminal Services, Internet Explorer and Outlook/Outlook Express, physical attacks that thwart the Encrypting File System, and Denial of Service.

V: Playing Defense

The latest, greatest Windows Server 2003 security features, tips, tricks, and a look ahead at the next generation of Windows security, codenamed Longhorn.

CHAPTERS: THE *HACKING EXPOSED* METHODOLOGY

Chapters make up each part, and the chapters in this book follow a definite plan of attack. That plan is the methodology of the malicious hacker, adapted from *Hacking Exposed*:

- ▼ Footprint
- Scan
- Enumerate
- Penetrate
- Escalate
- Get interactive
- Pillage
- Expand influence
- ▲ Cleanup

This structure forms the backbone of this book, for without a methodology, this would be nothing but a heap of information without context or meaning. It is the map by which we will chart our progress throughout the book, so it will be printed at the start of each chapter.

Beginning with Part IV, we will expand this outline somewhat to encompass several additional approaches to penetrating Windows Server 2003 security (step four in the above methodology):

- ▼ Applications
- Services: IIS, SQL, TS

- CIFS/SMB
- Internet clients
- Physical Attacks
- ▲ Denial of Service

Modularity, Organization, and Accessibility

Clearly, this book could be read from start to finish to achieve a soup-to-nuts portrayal of Windows Server 2003 penetration testing. However, like *Hacking Exposed*, we have attempted to make each section of each chapter stand on its own, so the book can be digested in modular chunks, suitable to the frantic schedules of our target audience.

Moreover, we have strictly adhered to the clear, readable, and concise writing style that readers overwhelmingly responded to in *Hacking Exposed*. We know you're busy, and you need the straight dirt without a lot of doubletalk and needless jargon. As a reader of *Hacking Exposed* once commented, "Reads like fiction, scares like hell!"

We think you will be just as satisfied reading from beginning to end as you would piece by piece, but it's built to withstand either treatment.

Chapter Summaries and References and Further Reading

In an effort to improve the organization of this book, we have included the standard features from the previous edition at the end of each chapter: a "Summary" and "References and Further Reading" section.

The "Summary" is exactly what it sounds like, a brief synopsis of the major concepts covered in the chapter, with an emphasis on countermeasures. We would expect that if you read the "Summary" from each chapter, you would know how to harden a Windows Server 2003 system to just about any form of attack.

"References and Further Reading" includes hyperlinks, ISBN numbers, and any other bit of information necessary to locate each and every item references in the chapter, including Microsoft Security Bulletins, Service Packs, Hotfixes, Knowledge Base Articles, third-party advisories, commercial and freeware tools, Windows Server 2003 hacking incidents in the news, and general background reading that amplifies or expands on the information presented in the chapter. You will thus find few hyperlinks within the body text of the chapters themselves—if you need to find something, turn to the end of the chapter, and it will be there. We hope this consolidation of external references into one container improves your overall enjoyment of the book.

Appendix A: The Windows Server 2003 Hardening Checklist

We took all of the great countermeasures discussed throughout this book, boiled them down to their bare essences, sequenced them appropriately for building a system from scratch, and stuck them all under one roof in Appendix A. Yes, there are a lot of Windows Server 2003 security checklists out there, but we think ours is the most real-world, down-to earth, yet rock-hard set of recommendations you will find anywhere.