"Informational gold."
—Bruce Schneier, CTO, Counterpane Internet Security, Inc.

HACKING EXPOSED

Second Edition

Network Security Secrets & Solutions

黑客曝光 第2版

世界畅销书

J. Scambray
S. McClure
G. Kurtz

McGraw-Hill Book Co
[illegible]图书出版公司

HACKING EXPOSED: NETWORK SECURITY SECRETS & SOLUTIONS SECOND EDITION

McGraw-Hill Book Co
世界图书出版公司

书　　名：Hacking Exposed 2nd ed.
作　　者：J. Scambray, S. Mchlure, G. Kurtz
中 译 名：黑客曝光　第 2 版
出 版 者：世界图书出版公司北京公司
印 刷 者：北京中西印刷厂
发　　行：世界图书出版公司北京公司 (北京朝内大街 137 号　100010)
开　　本：1/32　850×1168　印　张：23.125
出版年代：2001 年 4 月
书　　号：ISBN 7-5062-4975-8/TP・64
版权登记：图字 01-2000-3663
定　　价：108.00 元

Osborne/McGraw-Hill
2600 Tenth Street
Berkeley, California 94710
U.S.A.

For information on translations or book distributors outside the U.S.A., or to arrange bulk purchase discounts for sales promotions, premiums, or fund-raisers, please contact Osborne/McGraw-Hill at the above address.

Hacking Exposed: Network Security Secrets & Solutions

Attack icon (digital cannonball) courtesy of Foundstone, Inc.

1234567890 2CUS 2CUS 01987654321

ISBN 0-07-212748-1

Publisher
Brandon A. Nordin
Vice President & Associate Publisher
Scott Rogers
Senior Acquisitions Editor
Jane K. Brownlow
Senior Project Editor
LeeAnn Pickrell
Acquisitions Coordinator
Ross Doll
Technical Editors
Saumil Shah
Victor Robert "Bob" Garza
Eric Schultze
Martin W. Dolphin
Copy Editor
Jan Jue
Proofreader
John Gildersleeve
Indexer
Karin Arrigoni
Computer Designers
Roberta Steele
Melinda Moore Lytle
Illustrators
Michael Mueller
Lyssa Sieben-Wald
Series Design
Dick Schwartz
Peter F. Hancik
Cover Design
Dodie Shoemaker

IE ISBN 0-07-212127-0

To my parents and their parents, who set me on the path; to my wife, who continues to guide me along it; and to my children, who have taken it in miraculous new directions.

—Joel Scambray

To my wife and child, without whose love and support little else would matter; and to my parents for their continuing confidence in me.

—Stuart McClure

This book is dedicated to my loving wife, Anna. I could not have completed two editions of this book without her understanding, support, and continuous encouragement. I also would like to thank my entire family for their assistance in helping me "find the time" when deadlines seemed impossible.

—George Kurtz

To those who seek the truth, may they continue to search free from restraint and censorship.

—The Authors

About the Authors

Joel Scambray

Joel Scambray is a Principal of Foundstone Inc. (http://www.foundstone.com), where he provides information system security consulting services to clients ranging from members of the Fortune 50 to newly minted startups. He has field-tested knowledge of numerous security technologies and has designed and analyzed security architectures for a variety of applications and products. Mr. Scambray's regular publications include the monthly "Ask Us About...Security" (http://www.microsoft.com/technet/security/) for Microsoft's TechNet web site, and the weekly "Security Watch" column in *InfoWorld* magazine (http://www.infoworld.com/security), where he has additionally published over a dozen technology product analyses. He has held positions as a Manager for Ernst & Young LLP's eSecurity Solutions group, Senior Test Center Analyst for InfoWorld, and Director of IT for a major commercial real estate firm. Mr. Scambray is a Certified Information Systems Security Professional (CISSP) and Certified Checkpoint Security Engineer (CCSE).

Joel Scambray can be reached at joel@hackingexposed.com.

Stuart McClure

Stuart McClure is President/CTO of Foundstone, Inc. (http://www.foundstone.com) and has over 10 years of IT and security experience. Mr. McClure specializes in security assessments, firewall reviews, e-commerce application testing, hosts reviews, PKI technologies, intrusion detection, and incident response. For over two years, Mr. McClure has co-authored a weekly column on security called "Security Watch" for *InfoWorld* magazine, a global security column addressing topical security issues, exploits, and vulnerabilities. Mr. McClure has spent the past four years with the both Big 5 security consulting and the *InfoWorld* Test Center where he tested dozens of network and security hardware and software products. Prior to *InfoWorld*, Mr. McClure spent over seven years managing and securing networks and systems ranging from Cisco, Novell, Solaris, AIX, AS/400, Window NT, and Linux in corporate, academic, and government landscapes.

Stuart McClure can be reached at stuart@hackingexposed.com.

George Kurtz

George Kurtz is CEO of Foundstone (http://www.foundstone.com), a cutting edge security consulting and training organization. Mr. Kurtz is an internationally recognized security expert and has performed hundreds of firewall, network, and e-commerce related security assessments throughout his security consulting career. Mr. Kurtz has significant experience with intrusion detection and firewall technologies, incident response procedures, and remote access solutions. He is regular speaker at many security conferences and has been quoted in a wide range of publications, including *The Wall Street Journal*, *InfoWorld*, *USA Today*, and the Associated Press. Mr. Kurtz is routinely called to comment on breaking security events and has been featured on various television stations, including CNN, CNBC, NBC, and ABC.

George Kurtz can be reached at george@hackingexposed.com.

About the Technical Reviewers

Saumil Shah

Saumil Shah provides information security consulting services to Foundstone clients, specializing in ethical hacking and security architecture. He holds a designation as a Certified Information Systems Security Professional (CISSP). Mr. Shah has over six years of experience with system administration, network architecture, integrating heterogeneous platforms and information security, and has performed numerous ethical hacking exercises for many significant companies in the IT arena. Prior to joining Foundstone, Mr. Shah was a senior consultant with Ernst & Young where he was responsible for their ethical hacking and security architecture solutions. Mr. Shah has also authored a book titled *The Anti-Virus Book*, published by Tata McGraw-Hill India, and he worked at the Indian Institute of Management, Ahmedabad, as a research assistant.

Saumil Shah can be reached at saumil.shah@foundstone.com.

Victor Robert "Bob" Garza

Bob Garza is a Senior IT Network Engineer for a large multinational corporation in the Silicon Valley. His primary areas of responsibility include operational support, network management, and security for a network with over 25 thousand hosts. He has over 20 years of experience in the computing industry and is author of several "For Dummies" books. Mr. Garza has also written reviews of networking and security products for *InfoWorld* and *Federal Computer Week* for the past nine years. Mr. Garza holds an M.S. in Telecommunications Management and a B.S. in Information Systems Management.

Eric Schultze

Eric Schultze has been involved with information technology and security for the past nine years, with a majority of his time focused on assessing and securing Microsoft technologies and platforms. He is a frequent speaker at security conferences including NetWorld Interop, Usenix, BlackHat, SANS, and MIS and is a faculty instructor for the Computer Security Institute. Mr. Schultze has also appeared on TV and in many publications including NBC, CNBC, *TIME*, *ComputerWorld*, and *The Standard*. Mr. Schultz's prior employers include Foundstone, Inc., SecurityFocus.com, Ernst & Young, Price Waterhouse, Bealls Inc., and Salomon Brothers. A contributing author to the first edition of *Hacking Exposed*, he is currently a Security Program Manager for a software development company.

Martin W. Dolphin

Martin Dolphin is Senior Manager of Security Technology Solutions in the New England Practice for Ernst & Young. Mr. Dolphin has more than 10 years of computer administration experience with more than 5 years of security experience specializing in Windows NT, Novell NetWare, and Internet security. Mr. Dolphin can also be found teaching the Extreme Hacking—Defending Your Site class.

FOREWORD

When a tree falls in the forest and no one is around to hear it, it certainly makes a sound. But if a computer network has a security vulnerability and no one knows about it, is it insecure? Only the most extreme Berkeleian idealist might argue against the former, but the latter is not nearly so obvious.

A network with a security vulnerability is insecure to those who know about the vulnerability. If no one knows about it—if it is literally a vulnerability that has not been discovered—then the network is secure. If one person knows about it, then the network is insecure to him but secure to everyone else. If the network equipment manufacturer knows about it...if security researchers know about it...if the hacking community knows about it—the insecurity of the network increases as news of the vulnerability gets out.

Or does it? The vulnerability exists, whether or not anyone knows about it. Publishing a vulnerability does not cause the network to be insecure. To claim that would be confusing knowledge about a thing with the thing itself. Publishing increases the likelihood that an attacker will use the vulnerability, but not the severity of the vulnerability. Publishing also increases the likelihood that people can defend against the vulnerability. Just as an attacker can't exploit a vulnerability he does not know about, a defender can't protect against a vulnerability he does not know about.

So if keeping vulnerabilities secret increases security, it does so in a fragile way. Keeping vulnerabilities secret only works as long as they remain secret—but everything about information works toward spreading information. Some people spread secrets accidentally; others spread them on purpose. Sometimes secrets are re-derived by someone else. And once a secret is out, it can never be put back.

Security that is based on publishing vulnerabilities is more robust. Yes, attackers learn about the vulnerabilities, but they would have learned about them anyway. More importantly, defenders can learn about them, product vendors can fix them, and sysadmins can defend against them. The more people who know about a vulnerability, the better chance it has of being fixed. By aligning yourself with the natural flow of information instead of trying to fight it, you end up with more security rather than less.

This is the philosophy behind the "full disclosure" security movement and has resulted in a more secure Internet over the years. Software vendors have a harder time denying the existence of vulnerabilities in the face of published research and demonstration code. Companies can't sweep problems under the rug when they're announced in the newspapers. The Internet is still horribly insecure, but it would be much worse if all these security vulnerabilities were kept hidden from the public.

But just because information is public doesn't automatically put it in the hands of the right people. That's where this book comes in. *Hacking Exposed* is the distilled essence of the full-disclosure movement. It's a comprehensive bible of security vulnerabilities: what they are, how they work, and what to do about them. After reading this, you will know more about your network and how to secure it than any other book I can think of. This book is informational gold.

Of course, information can be used for both good and bad, and some might use this book as a manual for attacking systems. That's both true and unfortunate, but the trade-off is worth it. There are already manuals for attacking systems: Web sites, chat rooms, point-and-click attacker tools. Those intent on attacking networks already have this information, albeit not as lucidly explained. It's the defenders who need to know how attackers operate, how attack tools work, and what security vulnerabilities are lurking in their systems.

The first edition of this book was a computer best seller: over 70,000 copies were sold in less than a year. The fact that the authors felt the need to update it so quickly speaks to how fast computer security moves these days. There really is so much new information out there that a second edition is necessary.

There's a Biblical quotation etched on a stone wall in the CIA's lobby: "And ye shall know the truth, and the truth shall make ye free." Knowledge is power, because it allows you to make informed decisions based on how the world really is...and not on how you may otherwise believe it is. This book gives you knowledge and the power that comes with it. Use both wisely.

Bruce Schneier, 1 July 2000
CTO, Counterpane Internet Security, Inc.
http://www.counterpane.com

Bruce Schneier is founder and CTO of Counterpane Internet Security, Inc. (http://www.counterpane.com), the premier Managed Security Monitoring company. He is a designer of Blowfish, Twofish, and Yarrow. His most recent book is *Secrets and Lies: Digital Security in a Networked World.*

ACKNOWLEDGMENTS

This book would not have occurred if not for the support, encouragement, input, and contributions of many entities. We hope we have covered them all here and apologize for any omissions, which are due to our oversight alone.

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, each of the authors deserves a pat on the back from the others. It would be an understatement to say that this was a group effort—thanks to each one in turn who supported the others through the many 3 A.M. sessions to make it happen.

We would like to thank all of our colleagues at Foundstone for providing so much help and guidance on many facets of this book. In particular, we acknowledge Stephan Barnes for his contributions to the discussion of PBX and voicemail system hacking in Chapter 9, and Eric Birkholz for his work with Case Study IV. Saumil Shah and Chris Prosise also deserve special thanks for late-night discussions of Internet client and server security, as does Jason Glassberg for his always amusing slant on the security world.

We would also like to thank Simple Nomad, Fyodor, and Lance Spitzner for their enormous help and expertise in reviewing several chapters of the book and for providing excellent feedback. Special thanks are due Fyodor for his guidance on the UNIX chapter and his affinity for writing stellar code.

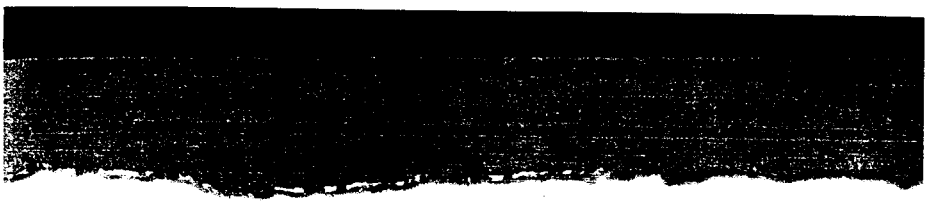
Thanks go also to Bruce Schneier for providing guidance on a diversity of security topics in the book and for his outstanding comments in the Foreword.

One again, 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, Mike Schiffman, Simple Nomad, and Georgi Guninski, but especially to Hobbit for writing one of our favorites—netcat—and providing his guidance on port redirection.

We must also nod to The Microsoft Product Security Team, who helped clarify many topics discussed in Chapters 4, 5, 6, and 16 during phone and email conversations over the last year.

Big thanks must also go to the tireless Osborne/McGraw-Hill editors and production team who worked on the book, including Jane Brownlow, Tara Davis, Ross Doll, and LeeAnn Pickrell.

And finally, a tremendous "Thank You" to all of the readers of the first edition, whose continuing support has driven the topics covered in *Hacking Exposed* from whispered conversations into the light of mainstream consumption.



INTRODUCTION

INTERNET SECURITY—DEATH BY A THOUSAND CUTS

In the year since the first edition of *Hacking Exposed* was published, it has become almost trite to utter the phrase "information systems are the lifeblood of modern society." Electronic pulses of ones and zeroes sustain our very existence now, nurturing an almost biological dependence upon instantaneous online commerce, coursing like blood through the vessels of our popular culture and our collective consciousness.

We are sad to report, however, that these vessels are bleeding from a thousand cuts sustained on the digital battlefield that is the Internet today. What saddens us more is that the millions who participate daily in the bounty of the network are not aware of these multiplying wounds:

- **The number of information system vulnerabilities reported to the venerable Bugtraq database has roughly quadrupled** since the start of 1998, from around 20 to nearly 80 in some months of 2000 (http:// www.securityfocus.com/vdb/stats.html).
- The Common Vulnerabilities and Exposures (CVE) Editorial Board, comprised of representatives from over 20 security-related organizations including security software vendors and academic institutions, **published over 1,000 mature, well-understood vulnerabilities to the CVE list in 1999** (http://cve.mitre.org).

- The Computer Security Institute and the FBI's joint survey of 643 computer security practitioners in U.S. corporations, government agencies, financial institutions, medical institutions, and universities found that **90 percent of survey respondents detected cyber attacks in the last year, with 273 organizations reporting $265,589,940 in financial losses** (http://www.gocsi.com, "2000 Computer Crime and Security Survey").

And this is just what has been reported. As experienced security practitioners who are immersed in the field each day, we can confidently say that the problem is much worse than everything you've heard or read.

Clearly, our newfound community is at risk of slowly bleeding to death from this multitude of injuries. How can we protect ourselves from this onslaught of diverse and sophisticated attacks that continues to mount?

The Solution: More Information

You are holding the answers in your hand. We have painstakingly tracked the pulse of the battle over the last year to bring you this latest report from the front lines. We are here to say that the fighting is fierce, but the war appears winnable. In this book, we lay out the methods of the enemy, and in every instance provide field-tested strategies for protecting your own portion of the digital landscape. Can you really afford to put off learning this information for much longer?

We think our esteemed colleague Bruce Schneier said it best in the Foreword to the Second Edition (which you may have just read). He said it so well that we're going to repeat some of his thoughts here:

> "*Hacking Exposed* is the distilled essence of the full-disclosure movement. It's a comprehensive bible of security vulnerabilities: what they are, how they work, and what to do about them. After reading this, you will know more about your network and how to secure it than any other book I can think of. This book is informational gold."

100,000 Readers Already Know

But don't take our word for it. Or Bruce's. Here's what some of the **over 100,000** readers of the first edition had to say:

> "I reviewed the book *Hacking Exposed* about 6 months ago and found it to be incredible. A copy of it was given to every attendee (over 300) at the [large U.S. military] conference that I attended last March..." *—President of a computer-based training company*

"I have to recommend this book as a total and absolute MUST for anyone running a commercial Win NT operation...it's written in a clear, understandable, fun style, and they give plenty of examples and resources where tools and other solutions are available. If you only buy _one_ computer book this quarter, THIS SHOULD BE THE ONE." —*Stu Sjouwerman, President, Sunbelt Software; Editor, NTools E-News (600,000+ subscribers); Author of Amazon.com Top 10 Bestseller* Windows NT Power Toolkit *and the* **Windows 2000 System Administrator's Black Book**

"Just when you think you know a topic, you read a book like this. I thought I knew NT and UNIX, how wrong I was! This book really opened my eyes to the loopholes and possibilities for security breaches in systems I thought I had secured..." —*a reader from Ireland*

"I build encrypted data networks for the U.S. government. This book contains MUCH more information than I expected. It fluently covers the methods used before and during a network attack. *Hacking Exposed* impressed me so much that I have put it into my personal collection and recommended it to more than a dozen colleagues. Excellent work gentlemen!" —*a reader from the United States*

"Reads like fiction, scares like hell! This book is *the* how-to manual of network security. Each vulnerability is succinctly summarized along with explicit instructions for exploiting it and the appropriate countermeasures. The overview of tools and utilities is also probably the best ever published. If you haven't read it yet, do so immediately because a lot of other people *are*." —*a reader from Michigan*

"...the book's 'it takes a thief to catch a thief' approach does the trick. I recommend that every CIO in the world read this book. Or else." —*a reader from Boston, Massachusetts*

"One the best books on computer security on the market....If you have anything at all to do with securing a computer this book is a must read." —*Hacker News Network, www.hackernews.com*

An International Best-Seller

These are just a few of the many accolades we've received via email and in person over the last year. We wish we could print them all here, but we'll let the following facts sum up the overwhelmingly positive reader sentiment that's flooded our inboxes:

- Many colleges and universities, including the U.S. Air Force and the University of Texas, have developed entire curricula around the contents of *Hacking Exposed*, using it as a textbook.
- It has been translated into over a dozen languages, including German, Mandarin Chinese, Spanish, French, Russian, and Portuguese, among others. It continues to be an international best-seller.

- *Hacking Exposed* has consistently ranked in the top 200 on Amazon.com during the first year of its publication, reaching as high as No. 10 in only six months, a truly phenomenal performance for a "niche" technical topic.
- It has been consistently ranked the No. 1 technical or computer security book on numerous booklists, web sites, newsletters, and more, including Amazon, Borders, Barnes & Noble, as well as the No. 5 spot amongst General Computer Books on the *Publisher's Weekly* Bestseller List in May 2000, and in the June 26, 2000, *News & Observer* "Goings On—Best Selling Computer Books."
- ▲ *Hacking Exposed* was the No. 1 selling book when we first launched it at Networld+Interop in fall 1999.

What's New in the Second Edition

Of course, we're not perfect. The world of Internet security moves even faster than the digital economy, and many brand-new tools and techniques have surfaced since the publication of our first edition. We have expended prodigious effort to capture what's important in this new edition, while at the same time making all of the improvements readers suggested over the last year.

Over 220 Pages of New Content

Here's an overview of the terrific changes we've made:

1. An entirely new chapter, entitled **"Hacking the Internet User,"** covering insidious threats to web browsers, email software, active content, and all manner of Internet client attacks, including the vicious new **Outlook email date field buffer overflow and ILOVEYOU worms.**
2. **A huge new chapter on Windows 2000 attacks and countermeasures.**
3. Significantly **updated e-commerce hacking methodologies** in Chapter 15.
4. Coverage of all the new **Distributed Denial of Service (DDoS)** tools and tricks that almost broke down the Internet in February 2000 (Trinoo, TFN2K, Stacheldraht).
5. Coverage of **new back doors and forensic techniques,** including defenses against Win9*x* back doors like Sub7.
6. New network discovery tools and techniques, including an updated section on **Windows-based scanning tools,** an explanation of **how to carry out eavesdropping attacks on switched networks using ARP redirection,** and an in-depth analysis of **RIP spoofing attacks.**
7. **New updated case studies** at the beginning of each section, covering recent security attacks of note.