"A fascinating tome of real-world security breach situations....The *Aesop's Fables* for the network security professional!"—David Goldsmith, *Regional Director, @stake, Inc.*

All challenges & solutions are **BRAND NEW!**

HACKER'S CHALLENGE 2

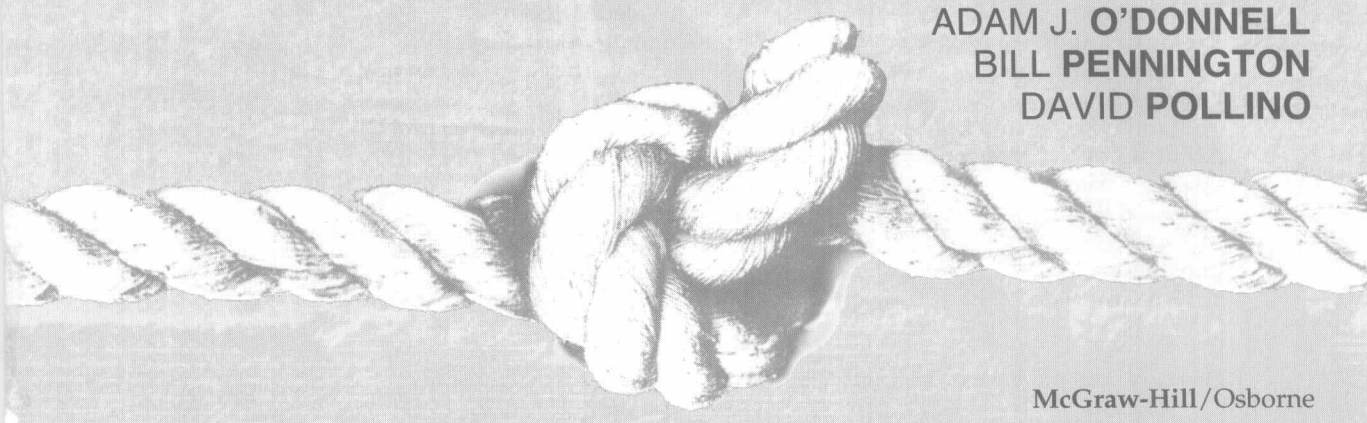
Test Your Network Security & Forensic Skills

Mike Schiffman, CISSP
Bill Pennington, CISSP
Adam J. O'Donnell
David Pollino

McGraw Hill OSBORNE

HACKER'S CHALLENGE 2: TEST YOUR NETWORK SECURITY & FORENSIC SKILLS

MIKE D. **SCHIFFMAN**
ADAM J. **O'DONNELL**
BILL **PENNINGTON**
DAVID **POLLINO**



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

The McGraw-Hill Companies

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

Hacker's Challenge 2: Test Your Network Security & Forensic Skills

4567890 FGR FGR 0198765

ISBN 0-07-222630-7

Publisher
Brandon A. Nordin
Vice President & Associate Publisher
Scott Rogers
Executive Editor
Jane K. Brownlow
Project Editors
Madhu Prasher and LeeAnn Pickrell
Acquisitions Coordinator
Tana Allen
Technical Editor
Tom Lee
Copy Editor
Lisa Theobald
Proofreader
Paul Tyler
Indexer
Valerie Robbins
Computer Designers
Lucie Ericksen and Jean Butterfield
Illustrators
Lyssa Wald, Michael Mueller, Melinda Lytle
Cover Series Design
Pattie Lee
Series Design
Dick Schwartz
Peter F. Hancik

This book was published with Corel Ventura™ Publisher.

Adam O'Donnell's material is based upon work supported under a National Science Foundation Graduate Research Fellowship.

Any opinions, findings, conclusions or recommendations expressed in this publication are those of the author and do not necessarily reflect the views of the National Science Foundation.

"*Hacker's Challenge* will definitely challenge even the most technically astute IT security pros with its 'ripped from the headlines' incident response scenarios. These based-on-real-life vignettes from a diverse field of experienced contributors make for page-turning drama, and the reams of authentic log data will test the analytical skills of anyone sharp enough to get to the bottom of these puzzling tableaus."

—**Joel Scambray,** Senior Director Security, MSN, Microsoft, and author of all three editions of the best-selling *Hacking Exposed* and *Hacking Exposed Windows 2000,* published by **McGraw-Hill**/Osborne

"*Hacker's Challenge* reads like a challenging mystery novel. It provides practical examples and a hands-on approach that is critical to learning how to investigate computer security incidents."

—**Kevin Mandia,** Director of Computer Forensics at Foundstone and author of *Incident Response: Investigating Computer Crime,* published by **McGraw-Hill**/Osborne

INTERNATIONAL CONTACT INFORMATION

AUSTRALIA
McGraw-Hill Book Company Australia Pty. Ltd.
TEL +61-2-9900-1800
FAX +61-2-9878-8881
http://www.mcgraw-hill.com.au
books-it_sydney@mcgraw-hill.com

CANADA
McGraw-Hill Ryerson Ltd.
TEL +905-430-5000
FAX +905-430-5020
http://www.mcgraw-hill.ca

GREECE, MIDDLE EAST, & AFRICA (Excluding South Africa)
McGraw-Hill Hellas
TEL +30-1-656-0990-3-4
FAX +30-1-654-5525

MEXICO (Also serving Latin America)
McGraw-Hill Interamericana Editores S.A. de C.V.
TEL +525-117-1583
FAX +525-117-1589
http://www.mcgraw-hill.com.mx
fernando_castellanos@mcgraw-hill.com

SINGAPORE (Serving Asia)
McGraw-Hill Book Company
TEL +65-863-1580
FAX +65-862-3354
http://www.mcgraw-hill.com.sg
mghasia@mcgraw-hill.com

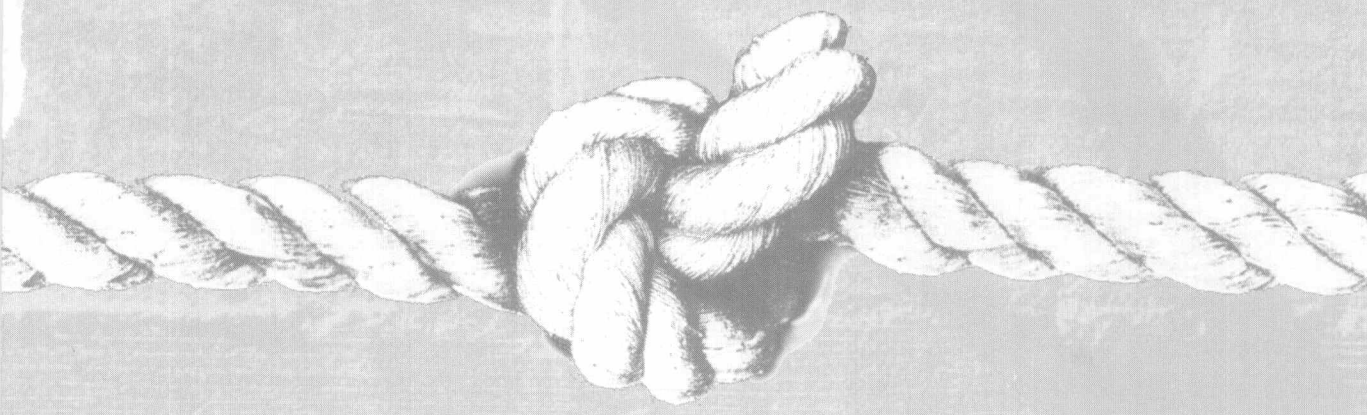
SOUTH AFRICA
McGraw-Hill South Africa
TEL +27-11-622-7512
FAX +27-11-622-9045
robyn_swanepoel@mcgraw-hill.com

SPAIN
McGraw-Hill/Interamericana de España, S.A.U.
TEL +34-91-180-3000
FAX +34-91-372-8513
http://www.mcgraw-hill.es
professional@mcgraw-hill.es

UNITED KINGDOM, NORTHERN, EASTERN, & CENTRAL EUROPE
McGraw-Hill Education Europe
TEL +44-1-628-502500
FAX +44-1-628-770224
http://www.mcgraw-hill.co.uk
computing_neurope@mcgraw-hill.com

ALL OTHER INQUIRIES Contact:
Osborne/McGraw-Hill
TEL +1-510-549-6600
FAX +1-510-883-7600
http://www.osborne.com
omg_international@mcgraw-hill.com

HACKER'S CHALLENGE 2: TEST YOUR NETWORK SECURITY & FORENSIC SKILLS



I would like to dedicate this book to my wonderfully eccentric and loving mother.
Thank you for everything.

—Mike Schiffman

To Sophy

—Adam O'Donnell

My effort on this book is dedicated to the two
greatest sources of inspiration in my life:
my wife, Michelle,
and my son,
Piero.

—David Pollino

To my wife, Dawn, who puts up with me day after day.
I love you.

—Bill Pennington

Technologies are morally neutral until we apply them.
It's only when we use them for good or for evil
that they become good or evil.

William Gibson

ABOUT THE AUTHORS

Mike D. Schiffman is a Director of Security Architecture with @stake, the world's leading digital security consultancy. @stake applies industry expertise and pioneering research to design and build secure business solutions. Previous to @stake, Schiffman was the Director of Research and Development at Guardent, Inc., where he was responsible for the integration of R&D into other business units inside the company, including delivery, forensics, and managed security services. Prior to joining Guardent, Schiffman held senior positions at Internet Security Systems and Cambridge Technology Partners.

Schiffman's primary areas of expertise are research and development, consulting, and writing. He is the original co-author of the well-known network security tool *firewalk*, as well as author of the ubiquitously used, low-level packet shaping library *libnet*. Schiffman has led security consulting engagements for Fortune 500 companies in many vertical markets, including critical infrastructure, financial, automotive, manufacturing, and software. As a sought-after speaker, he has presented to industry professionals as well as government agencies including the NSA, CIA, DOD, FBI, NASA, AFWIC, SAIC, and Army intelligence.

Schiffman has authored several books on computer security, including *Building Open Source Network Security Tools* (Wiley & Sons), a how-to book on building network security tools; as well as the *Hacker's Challenge* book series (McGraw-Hill/Osborne), a line of books on computer security forensics and incident response. He co-authored and contributed to several other books, including *Hacking Exposed* (McGraw-Hill/Osborne) and *Hack Proofing Your Network: Internet Tradecraft* (Syngress Media, Inc.). He has written for numerous technical journals and authored many white papers on topics ranging from UNIX kernel enhancements to network protocol deficiencies.

Adam J. O'Donnell is an NSF Graduate Research Fellow pursuing a Ph.D. in Electrical Engineering at Drexel University, having graduated *summa cum laude* from Drexel with a Bachelor of Science in Electrical Engineering. Adam currently spends his time performing academic research and authoring, as well as consulting for the information security industry. His current research interests are in networking, computer security, and distributed systems. Adam has optimized RF Amplifier subsystems at Lucent Technologies, where he was awarded a patent for his work, and he has held a research position at Guardent, Inc. He is a contributing author of the original *Hacker's Challenge*.

Bill Pennington, CISSP, is currently employed at WhiteHatSec, the premier provider of web application security services. Bill has six years of professional experience in information security, and twelve in information technology. He is familiar with Linux, Solaris, Windows, and OpenBSD, and he is a Certified Information Security Systems Practitioner (CISSP), Certified Cisco Network Administrator (CCNA), Certified Internet Security Specialist (CISS), and Microsoft Certified Product Specialist, Windows NT 4.0. He has broad experience in computer forensics, web application security, network architecture, installing and maintaining VPNs, Cisco Pix firewalls, IDS, and monitoring systems. Bill is a frequent speaker at security industry events and a contributing author of the original *Hacker's Challenge*.

David Pollino leads @stake's Wireless Center of Excellence focusing on wireless technologies such as WLAN, WAP, Bluetooth, and GPRS. His extensive networking experience includes working for a tier 1 Internet Service Provider as well as architecting and deploying secure networks for Fortune 500 companies. David is a published author in security books and magazines. He contributed to the first *Hacker's Challenge* book and is the co-author of *RSA Press: Wireless Security.*

ABOUT THE TECHNICAL REVIEWER

Tom Lee (MCSE) is the IT Manager at Foundstone. He is currently tasked with keeping the systems at Foundstone operational and safe from intruders and—even more challenging—from the employees. Tom has 10 years of experience in systems and network administration, and he has secured a variety of systems ranging from Novell and Windows NT/2000 to Solaris, Linux, and BSD. Before joining Foundstone, Tom worked as an IT Manager at the University of California, Riverside. Tom is a contributing author of *Windows XP Professional Security*, published by McGraw-Hill/Osborne. Tom also was the technical reviewer of the first edition of *Hacker's Challenge*, and he has technically edited *Hacking Exposed*, Third Edition, as well as *Hacking Linux Exposed*, Second Edition.

ACKNOWLEDGMENTS

Initially I'd like to thank the entire Osborne team for putting up with us with our very hectic careers and lives to finally get this book out the door. I am convinced that we gave Executive Editor Jane Brownlow many gray hairs over this book! In any event, as my esteemed co-authors know, it is truly a difficult thing to balance a full-time career with writing a book (let alone writing three in a row). Throw in life's unpredictability and the wheels can definitely start coming off. I would like to thank Adam, Dave, and Bill for their hard work in the face of the aforementioned. Great work, guys.

—Mike Schiffman

I would like to first thank Jon Hoult and Pete Moffe for beta testing early drafts of my chapters. Readers of the chapters should be thankful of their input; without it, the work would be far more cryptic. My parents, Joseph and Monica O'Donnell, are also responsible for this book by providing the Aquarius, the Commodore C64, the Apples, and the numerous IBM clones, all of which taught me a little something more about the digital world. My graduate advisor, Dr. Harish Sethu, deserves thanks for his advice through the course of this project. Finally, I would like to mention Sophy Ting, for without all her love and support, I would not have been able to crank this out.

—Adam O'Donnell

I would like to thank all those who have enriched my knowledge over the years—most notably, Mike Schiffman, Doug Barbin, Gabe Wachman, Dede Summerly, Jason Recla, Jason Luster, Jeremiah Grossman, Dennis Groves, Lex Arquette, and countless others. To my parents for always supporting me, even when it looked like I had no idea what I was doing.

—Bill Pennington

I would like to give special thanks to the friends and family who have been extremely important in my life. My very supportive family members are Paul and Paula Pollino Sr., Farrah Pollino, Paul and Cheryl Pollino Jr., Gilbert and Deanna Ribét, Shelah Ryan, and Lois Spencer. My lifelong friends who put up with my eccentricities are Mat Hughey, Aaron and Angie Keaton, David and Tina Kim, Andrew and Jenny Mehren, Jay and Lalenya Mehren, Eric and Rebekah Rafanan, and Joanna Tandaguen.

—David Pollino

INTRODUCTION

For the introduction of *Hacker's Challenge* during the summer of 2001, we queried cnn.com to see what security headlines were making news. We found consistent reports of widespread misuse of all sorts of systems by all sorts of people. Well, guess what? It's now winter 2002, and things haven't gotten any better:

- ▼ Report gives U.S. computer security an F
- ■ U.S. cracks case of military network hacker
- ■ British national indicted in military hacking case
- ■ Attack on heart of Internet fails to bring it down
- ■ China computers face virus epidemic
- ■ Hackers say holes exposed retail data
- ■ Bugbear virus attacks computer security
- ■ U.S. computer systems vulnerable to attack?
- ▲ Hack attack–how you might be a target

The bottom line is that the world is not a safe place (neither physically nor electronically). Fear not, gentle reader! *Hacker's Challenge 2: Test Your Network Security & Forensic Skills* is here

to confront you with 19 new real-world vignettes covering contemporary topics such as the following:

- ▼ Man in the Middle Attacks
- ■ New Wireless Attacks
- ■ Layer 2 Attacks
- ■ Security Policy Enforcement
- ▲ Shady Employees

For those of you who didn't read the first book, you might be wondering just what is *Hacker's Challenge 2*? As the Internet grows in size and constituency, so do the number of computer-security incidents. One thing the news doesn't inform us is *how* these incidents take place. What led up to the incident? What enabled it? What provoked it? What could have prevented it? How can the damage be mitigated? And most of all, *how* did it happen? If any of this interests you, this book is for you.

Hacker's Challenge 2 brings you fact-based, computer-security war stories from the same core team who brought you the first book. Taking the same successful formula from the first book, it pulls you, the reader, inside the story. As each story unfolds, you are presented with information about the incident and are asked to solve the case.

People who are responsible for networks and network security across many different industries can read about actual penetrations of similar companies. They can use the information in this book to learn the kinds of scenarios they need to worry about and the *modi operandi* of some attackers. This book is also a lot of fun to read.

For those of you who did read the first book, you'll definitely want to read this second book as well, because this is not a revision of what you already read, but a brand-new book written from scratch with all new challenges and solutions!

ORGANIZATION

Hacker's Challenge is divided into two parts. Part I contains all of the case studies, or *Challenges*. Included in each Challenge is a detailed description of the case with all of the evidence and forensic information (log files, network maps, and so on) necessary for the reader to determine exactly what occurred. For the sake of brevity, in many of the chapters, vast portions of the evidence have been removed, leaving the reader almost exclusively with pertinent information (as opposed to just pages and pages of data to wade through). At the end of each case study, a few specific questions guide the reader toward a correct forensic analysis.

Part II of the book contains all of the *Solutions* to the Challenges set forth in Part I. In this section, the case study is thoroughly examined, with all of the evidential information completely explained, along with the questions answered. Additionally, sections on mitigation and prevention offer even more information.

TO PROTECT THE INNOCENT...

To protect the anonymity of the profiled organizations, many details in each story had to be changed or removed. Care was taken to preserve the integrity of each case study, so no information was lost in the process. The changed information includes some of the following:

- ▼ Company names
- ■ Employee names
- ■ IP addresses
- ■ Dates
- ■ Web defacement details (to change the message and remove profanity or other unsuitable content)
- ▲ Nonessential story details

VULNERABILITY INFORMATION

Throughout the book, wherever possible, we will make reference to external resources that contain additional information about specific profiled vulnerabilities (look for the "Additional Resources" section at the end of some of the Solutions). Also, the organizations MITRE and SecurityFocus both contain slightly different vulnerability databases that are useful general resources.

MITRE (http://cve.mitre.org) is a not-for-profit national technology resource that provides systems engineering, research and development, and information technology support to the government. Common Vulnerabilities and Exposures (CVE) is a list or dictionary that provides common names for publicly known information security vulnerabilities and exposures. Using a common name makes it easier to share data across separate databases and tools that until now were not easily integrated. This makes CVE the key to information sharing.

SecurityFocus (http://www.securityfocus.com) is the leading provider of security information services for business. The company manages the industry's largest and most active security community and operates the security industry's leading portal, which serves a community of more than a quarter of a million unique users per month. SecurityFocus's vulnerability database is the most comprehensive collection of published computer security vulnerabilities anywhere.

COMPLEXITY TAXONOMY

There are three ratings, found in a table at the beginning of each Challenge, that describe the overall complexity of each chapter. These ratings cover the incident from both the attacker's and the security practitioner's sides of the fence.

Attack Complexity

The attack complexity addresses the level of technical ability on the attacker's part. This class profiles the overall sophistication of the attacker. Often we'll see that the more complex and secure an environment, the more complex the attacker had to be to compromise it (of course, this isn't always the case...).

- ▼ **Low/Easy** Attacks at this level are generally of script-kiddie caliber. The attacker did little more than run an attack script, compile some easy-to-find code, or employ a publicly known attack method, and he showed little or no innovative behavior. This is the lowest hanging fruit.
- ■ **Moderate/Medium** The attacker used a publicly known attack method, but she extended the attack and innovated something beyond the boilerplate. This might involve address forgery or slight modifications of attack behaviors beyond the norm.
- ■ **Hard** The attacker was very clever and reasonably skilled. The exploit may or may not have been public, and the attacker probably writes his own code.
- ▲ **High** Attacks of this caliber generally show domain expertise. The attacker was extremely skilled, employing either nonpublic exploits or cutting-edge technology. The attacker was also forced to innovate a great deal, and, if applicable, she may have covered her tracks well and left a covert method of reentry. The attacker probably wouldn't have been caught except by a veteran security administrator or by fluke.

Prevention and Mitigation Complexity

The prevention complexity is the level of complexity that *would have been* required on the organization's part to prevent the incident from happening. The mitigation complexity is the level of complexity required to lessen the impact of the damage of the incident across the organization's infrastructure. They are very similar, and both can be defined by the same taxonomy:

- ▼ **Low/Easy** Preventing or mitigating the problem could be as simple as a single software patch or update, or a rule addition to a firewall. These changes are generally simple and do not involve a great deal of effort to invoke.
- ■ **Moderate/Medium** Remediation could involve a complex software patch or update, possibly in addition to policy changes on a firewall. Reinstallation of an infected machine and/or small infrastructure changes may also be necessary.
- ▲ **Hard/High** A complex patch or an update or series of updates to many machines, in addition to major infrastructure changes, are required. This level may also include vulnerabilities that are extremely difficult to completely prevent or mitigate altogether.

CONVENTIONS USED IN THIS BOOK

To get the most out of *Hacker's Challenge*, it may help you to know how this book is designed. Here's a quick overview.

In the body of each chapter you will find log files, network maps, file listings, command outputs, code, and various other bits of forensic evidence. This information is reprinted as closely as possible to the original, but you should take into account that printing restrictions and confidentiality required some changes.

This book is broken up into two sections. In Part I, Challenges 1 through 19 present the details of a real-life incident. Each Challenge begins with a summary table that lists the industry of the victimized company and complexity ratings for attack, prevention, and mitigation.

QUESTIONS

At the end of each Challenge, you will find a list of questions that will direct your search for the details of the incident and guide you toward the overall solution. Feel free to make notes in this section or throughout the text as you solve the Challenge.

ANSWERS

In Part II of this book, you'll find the corresponding Solutions 1 through 19. The Solution explains the details of how the incident was actually solved, as well as the answers to the questions presented in the first part of the book.

PREVENTION

The Solution contains a "Prevention" section, where you will find suggestions for how to stop an attack before it starts (useful for companies that find themselves in situations similar to the unfortunate organizations profiled in the book).

MITIGATION

The Solution also contains a "Mitigation" section, where you will learn what the victimized company did to pick up the pieces after the attack.

Good luck!