HACKING EXPOSED™ WINDOWS®: WINDOWS SECURITY SECRETS & SOLUTIONS

THIRD EDITION

JOEL SCAMBRAY
STUART McCLURE

McGraw Hill

New York Chicago San Francisco
Lisbon London Madrid Mexico City Milan
New Delhi San Juan Seoul Singapore Sydney Toronto

ABOUT THE AUTHORS

Joel Scambray

Joel Scambray is Chief Strategy Officer for Leviathan Security Group, an information security consultancy located in Seattle and Denver. As a member of Leviathan's board and executive management team, Joel guides the evolution and execution of Leviathan's business and technical strategy.

Prior to Leviathan, Joel was a senior director at Microsoft Corporation, where he led Microsoft's online services security efforts for three years before joining the Windows platform and services division to focus on security technology architecture. Before joining Microsoft, Joel co-founded security software and services startup Foundstone, Inc. and helped lead it to acquisition by McAfee for $86M. 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 is widely recognized as co-author of the original *Hacking Exposed: Network Security Secrets & Solutions,* the international best-selling computer security book that reached its Fifth Edition in April 2005. He is also lead author of the *Hacking Exposed: Windows* and *Hacking Exposed: Web Applications* series.

Joel's writing draws primarily on his experiences in security technology development, IT operations security, and consulting. He has worked with organizations ranging in size from the world's largest enterprises to small startups. He has spoken widely on information security at forums including Black Hat, I-4, and The Asia Europe Meeting (ASEM), as well as organizations including CERT, The Computer Security Institute (CSI), ISSA, ISACA, SANS, private corporations, and government agencies such as the Korean Information Security Agency (KISA), the FBI, and the RCMP.

Joel holds a BS from the University of California at Davis, an MA from UCLA, and he is a Certified Information Systems Security Professional (CISSP).

Stuart McClure

Stuart McClure is an independent computer security consultant in the Southern California area. Prior to returning to running his own consultancy, Stuart was SVP of Global Threats and Research for McAfee where he led an elite global security threats team fighting the most vicious cyber attacks ever seen. McAfee purchased Foundstone (a leading global enterprise risk management company) in 2004, of which Stuart was founder, president, and chief technology officer. Foundstone empowered large enterprises, including U.S. government agencies and Global 500 customers, to continuously and measurably manage and mitigate risk to protect their most important digital assets and customers' private information from critical threats.

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 brought over 20 years of technology and executive leadership to Foundstone with profound technical, operational, and financial experience.

In 1999, he published the first of many books on computer hacking and security. His first book, *Hacking Exposed: Network Security Secrets & Solutions,* has been translated into over 20 languages and was ranked the #4 computer book ever 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 many leadership positions in security and IT management, including positions within Ernst & Young's National Security Profiling Team, the InfoWorld Test Center, state and local California government, IT consultancy, and with the University of Colorado, Boulder, where Stuart holds a bachelor's degree in psychology and philosophy, with an emphasis in computer science applications. He has also earned numerous certifications including ISC2's CISSP, Novell's CNE, and Check Point's CCSE.

ABOUT THE CONTRIBUTING AUTHORS

Chip Andrews (CISSP, MCDBA) is the head of Research and Development for Special Ops Security. Chip is the founder of the SQLSecurity.com website, which focuses on Microsoft SQL Server security topics and issues. He has over 16 years of secure software development experience, helping customers design, develop, deploy, and maintain reliable and secure software. Chip has been a primary and contributing author to several books, including *SQL Server Security* and *Hacking Exposed: Windows Server 2003.* He has also authored articles focusing on SQL Server security and software development issues for magazines such as *Microsoft Certified Professional Magazine*, *SQL Server Magazine*, and *Dr. Dobb's Journal*. He is a prominent speaker at security conferences such as the Black Hat Briefings.

Blake Frantz has over ten years of professional experience in information security with a broad background ranging from software security research to enterprise policy development. He is currently a principal consultant for Leviathan Security Group where he specializes in penetration testing and source code reviews. Prior to Leviathan, Blake was a security engineer within Washington Mutual's Infrastructure Security and Security Assurance teams where he was responsible for leading vulnerability assessments of critical financial systems.

Robert Hensing, a nine-year veteran of Microsoft, is a software security engineer on the Microsoft Secure Windows Initiative team. Robert works closely with the Microsoft Security Response Center with a focus on identifying mitigations and workarounds for product vulnerabilities that can be documented in advisories and bulletins to help protect Microsoft's customers. Prior to joining the Secure Windows Initiative team, Robert was a senior member of the Product Support Services Security team where he helped customers with incident response–related investigations.

The Toolcrypt Group (www.toolcrypt.org) is an internationally recognized association of professional security consultants who have contracted widely throughout Europe and the U.S. Their work has helped improve security at government agencies, multinationals, financial institutions, nuclear power plants, and service providers of all sizes in many different countries. They have been invited speakers at numerous conferences and industry forums, including Microsoft BlueHat and T2 Finland. Toolcrypt's ongoing research and tool development continues to help responsible security professionals to improve network and computer security globally.

Dave Wong manages the Ernst & Young Advanced Security Center in New York where he runs a team of dedicated attack and penetration testing professionals. Dave has over ten years of experience in attack and penetration testing and has managed and performed hundreds of assessments for financial services, government, and Fortune 500 clients. Prior to joining Ernst & Young, he gained a wide array of information security experience and previously held positions at Lucent's Bell Laboratories, Foundstone, and Morgan Stanley. Dave has taught a number of secure coding and hacking courses for public and corporate clients. He has taught courses at the Black Hat Security Conferences in the U.S. and Asia and has spoken at OWASP meetings. Dave is also a Certified Information Systems Security Professional (CISSP).

ABOUT THE TECHNICAL REVIEWERS

Aaron Turner is Cybersecurity Strategist for the Idaho National Laboratory (INL). In this role, he applies his experience in information security to collaborate with control systems experts, industry engineers, and homeland security/law enforcement officials to develop solutions to the cyber threats that critical infrastructure is currently facing. Before joining INL, he worked in several of Microsoft's security divisions for seven years—including as a senior security strategist within the Security Technology Unit as well as the Security Readiness Manager for Microsoft Sales, Marketing, and Services Group where he led the development of Microsoft's information security curriculum for over 22,000 of Microsoft's field staff. Prior to focusing on Microsoft's global security readiness challenge, he managed Microsoft Services' response to enterprises' needs during the aftermath of the Blaster worm. He has been an information security practitioner since 1994, designing security solutions and responding to incidents in more than 20 countries around the world.

Lee Yan (CISSP, PhD) is a security escalation engineer on the Microsoft PSS Security Team, which provides worldwide security response, security products, and technology support to Microsoft customers. He has been with Microsoft for more than ten years. Prior to joining the security team about five years ago, he was an escalation engineer in developer support for Visual Studio. He authors some of the incident response and rootkit detection tools for his team. He holds a PhD in Fisheries from the University of Washington and discovered that he enjoyed working with computers by accident.

CONTENTS

Foreword xvii
Acknowledgments xix
Introduction xxi

▼ 1 Information Security Basics 1
A Framework for Operational Security 2
Plan 3
Prevent 8
Detect 8
Respond 9
Rinse and Repeat 9
Basic Security Principles 10
Summary 13
References and Further Reading 14

▼ 2 The Windows Security Architecture from the Hacker's Perspective 15
Overview 16
Attacking the Kernel 17
Attacking User Mode 18
Access Control Overview 19
Security Principals 19
SIDs 20
Users 22
Groups 25
Computers (Machine Accounts) 28
User Rights 30
Putting It All Together: Access Control 31
The Token 32
Network Authentication 36
The SAM and Active Directory 39
Forests, Trees, and Domains 41
Scope: Local, Global, and Universal 42
Trusts 43
Administrative Boundaries: Forest or Domain? 43

Auditing 46
    Cryptography 47
    The .NET Framework 48
Summary 50
References and Further Reading 51

▼ 3 Footprinting and Scanning 53
Footprinting 54
Scanning 60
A Final Word on Footprinting and Scanning 69
Summary 70
References and Further Reading 70

▼ 4 Enumeration 73
Prelude: Reviewing Scan Results 74
    NetBIOS Names vs. IP Addresses 74
NetBIOS Name Service Enumeration 77
RPC Enumeration 82
SMB Enumeration 84
Windows DNS Enumeration 101
SNMP Enumeration 103
Active Directory Enumeration 107
All-in-One Enumeration Tools 111
Summary 112
References and Further Reading 113

▼ 5 Hacking Windows-Specific Services 115
Guessing Passwords 117
    Close Existing SMB Sessions to Target 117
    Review Enumeration Results 118
    Avoid Account Lockout 119
    The Importance of Administrator and Service Accounts 121
Eavesdropping on Windows Authentication 137
Subverting Windows Authentication 148
Exploiting Windows-Specific Services 156
Summary 161
References and Further Reading 162

▼ 6 Discovering and Exploiting Windows Vulnerabilities 165
Security Vulnerabilities 166
Finding Security Vulnerabilities 166
    Prep Work 167
    Exploiting ANI 181
Summary 184
References and Further Reading 184

▼ 7 Post-Exploit Pillaging 185
Transferring Attacker's Toolkit for Further Domination 186
Remote Interactive Control 191
Password Extraction 201
Introduction to Application Credential Usage and the DPAPI 205
Password Cracking 210
Cracking LM Hashes 210
Cracking NT Hashes 214
Rinse and Repeat 220
Summary 220
References and Further Reading 221

▼ 8 Achieving Stealth and Maintaining Presence 225
The Rise of the Rootkit 226
Windows Rootkits 227
The Changing Threat Environment 229
Achieving Stealth: Modern Techniques 235
Windows Internals 235
DKOM 240
Shadow Walker 245
Antivirus Software vs. Rootkits 246
Windows Vista vs. Rootkits 247
Kernel Patch Protection (KPP): Patchguard 247
UAC: You're About to Get 0wn3d, Cancel or Allow? 248
Secure Startup 250
Other Security Enhancements 251
Summary of Vista vs. Rootkits 251
Rootkit Detection Tools and Techniques 252
Rise of the Rootkit Detection Tool 252
Cross-View-Based Rootkit Detection 253
Ad Hoc Rootkit Detection Techniques 254
The Future of Rootkits 262
Are Rootkits Really Even Necessary? 262
Summary 268
References and Further Reading 269

▼ 9 Hacking SQL Server 273
Case Study: Penetration of a SQL Server 274
SQL Server Security Concepts 277
Network Libraries 277
Security Modes 278
Logins 278
Users 279
Roles 279

Logging 279
SQL Server 2005 Changes 280
Hacking SQL Server 281
SQL Server Information Gathering 282
SQL Server Hacking Tools and Techniques 286
Critical Defensive Strategies 306
Additional SQL Server Security Best Practices 309
Summary 315
References and Further Reading 316

▼ 10 Hacking Microsoft Client Apps 317
Exploits 319
Trickery 327
General Countermeasures 334
IE Security Zones 335
Low-privilege Browsing 339
Summary 340
References and Further Reading 340

▼ 11 Physical Attacks 345
Offline Attacks 346
Implications for EFS 349
Online Attacks 354
Device/Media/Wireless Attacks 359
Summary 363
References and Further Reading 364

▼ 12 Windows Security Features and Tools 367
BitLocker Drive Encryption 368
BitLocker Configurations 369
BitLocker with TPM 370
Windows Integrity Control 372
Managing Integrity Levels 374
User Account Control 375
Tokens and Processes 375
UnAdmin 375
Windows Service Hardening 377
Service Resource Isolation 377
Least Privilege Services 380
Service Refactoring 385
Restricted Network Access 386
Session 0 Isolation 386
Your Compiler Can Save You 387
An Overview of Overflows 387
GS Cookies 388

SafeSEH 392
Stack Changes 397
Address Space Layout Randomization 398
Windows Resource Protection 399
Summary 402
References and Further Reading 402

▼ A Windows Security Checklist 405
Caveat Emptor: Roles and Responsibilities 406
Preinstallation Considerations 406
Basic Windows Hardening 407
Non-Template Recommendations 407
Security Templates Recommendations 409
Windows Firewall and IPSec 411
Group Policy 412
Miscellaneous Configurations 412
Web Application Security Considerations 413
SQL Server Security Considerations 414
Terminal Server Security Considerations 416
Denial of Service Considerations 417
Internet Client Security 418
Audit Yourself! 420

▼ B About the Companion Website 421

Index 423