(ISC)²

HACKING THE HACKER

LEARN FROM THE EXPERTS WHO TAKE DOWN HACKERS

ROGER A. GRIMES

Foreword by Eric Knorr, editor-in-chief of *InfoWorld*

WILEY

Hacking the Hacker

Hacking the Hacker

Learn from the Experts Who Take Down Hackers

Roger A. Grimes

WILEY

Hacking the Hacker: Learn from the Experts Who Take Down Hackers

Published by
John Wiley & Sons, Inc.
10475 Crosspoint Boulevard
Indianapolis, IN 46256
www.wiley.com

Copyright © 2017 by John Wiley & Sons, Inc., Indianapolis, Indiana

Published simultaneously in Canada

ISBN: 978-1-119-39621-5
ISBN: 978-1-119-39623-9 (ebk)
ISBN: 978-1-119-39622-2 (ebk)

Manufactured in the United States of America

10 9 8 7 6 5 4 3 2 1

No part of this publication may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, scanning or otherwise, except as permitted under Sections 107 or 108 of the 1976 United States Copyright Act, without either the prior written permission of the Publisher, or authorization through payment of the appropriate per-copy fee to the Copyright Clearance Center, 222 Rosewood Drive, Danvers, MA 01923, (978) 750-8400, fax (978) 646-8600. Requests to the Publisher for permission should be addressed to the Permissions Department, John Wiley & Sons, Inc., 111 River Street, Hoboken, NJ 07030, (201) 748-6011, fax (201) 748-6008, or online at http://www.wiley.com/go/permissions.

Limit of Liability/Disclaimer of Warranty: The publisher and the author make no representations or warranties with respect to the accuracy or completeness of the contents of this work and specifically disclaim all warranties, including without limitation warranties of fitness for a particular purpose. No warranty may be created or extended by sales or promotional materials. The advice and strategies contained herein may not be suitable for every situation. This work is sold with the understanding that the publisher is not engaged in rendering legal, accounting, or other professional services. If professional assistance is required, the services of a competent professional person should be sought. Neither the publisher nor the author shall be liable for damages arising herefrom. The fact that an organization or Web site is referred to in this work as a citation and/or a potential source of further information does not mean that the author or the publisher endorses the information the organization or website may provide or recommendations it may make. Further, readers should be aware that Internet websites listed in this work may have changed or disappeared between when this work was written and when it is read.

For general information on our other products and services please contact our Customer Care Department within the United States at (877) 762-2974, outside the United States at (317) 572-3993 or fax (317) 572-4002.

Wiley publishes in a variety of print and electronic formats and by print-on-demand. Some material included with standard print versions of this book may not be included in e-books or in print-on-demand. If this book refers to media such as a CD or DVD that is not included in the version you purchased, you may download this material at http://booksupport.wiley.com. For more information about Wiley products, visit www.wiley.com.

Library of Congress Control Number: 2017934291

Trademarks: Wiley and the Wiley logo are trademarks or registered trademarks of John Wiley & Sons, Inc. and/or its affiliates, in the United States and other countries, and may not be used without written permission. All other trademarks are the property of their respective owners. John Wiley & Sons, Inc. is not associated with any product or vendor mentioned in this book.

I dedicate this book to my wife, Tricia. She is truly the woman behind the man in every sense of the saying.

(ISC)^{2}®

(ISC)^{2} books published by Wiley provide aspiring and experienced cybersecurity professionals with unique insights and advice for delivering on (ISC)^{2}'s vision of inspiring a safe and secure world.

(ISC)^{2} is an international nonprofit membership association focused on inspiring a safe and secure cyber world. Best known for the acclaimed Certified Information Systems Security Professional (CISSP) certification, (ISC)^{2} offers a portfolio of credentials that are part of a holistic, programmatic approach to security. (ISC)^{2}'s membership is made up of certified cyber, information, software and infrastructure security professionals who are making a difference and helping to advance the industry.

About the Author

Roger A. Grimes has been fighting malicious computer hackers for three decades (since 1987). He's earned dozens of computer security certifications (including CISSP, CISA, MCSE, CEH, and Security+), and he even passed the very tough Certified Public Accountants (CPA) exam, although it has nothing to do with computer security. He has created and updated computer security classes, been an instructor, and taught thousands of students how to hack or defend. Roger is a frequent presenter at national computer security conferences. He's been paid as a professional penetration tester to break into companies and their web sites, and it has never taken him more than three hours to do so. He's previously written or co-written eight books on computer security and nearly a thousand magazine articles. He's been the *InfoWorld* magazine computer security columnist (`http://www.infoworld.com/blog/security-adviser/`) since August 2005, and he's been working as a full-time computer security consultant for more than two decades. Roger currently advises companies, large and small, around the world on how to stop malicious hackers and malware. And in that time and those experiences, he's learned that most malevolent hackers aren't as smart as most people believe, and they are definitely not as smart as most of the defenders.

Credits

Project Editor
Kelly Talbot

Production Editor
Barath Kumar Rajasekaran

Copy Editor
Kelly Talbot

Production Manager
Kathleen Wisor

Manager of Content Development & Assembly
Mary Beth Wakefield

Marketing Manager
Carrie Sherrill

Professional Technology & Strategy Director
Barry Pruett

Business Manager
Amy Knies

Executive Editor
Jim Minatel

Project Coordinator, Cover
Brent Savage

Proofreader
Nancy Bell

Indexer
Johnna VanHoose Dinse

Cover Designer
Wiley

Cover Image
©CTRd/Getty Images

Acknowledgments

I would like to thank Jim Minatel for greenlighting this book, which has been living in my head for 10 years, and Kelly Talbot for being the best book editor I've had in over 15 years of book writing. Kelly is great at fixing the problems while not changing the voice. I want to thank Microsoft, my employer for over 10 years, for being the best company I've worked for and pushing us to recognize the strength that diversity brings to the table. I want to thank Bruce Schneier for his unofficial mentoring of me and everyone else in the industry. Kudos to Brian Krebs for his great investigative reporting and pulling back the curtain on the big business that cybercrime has become. Thanks to Ross Greenberg, Bill Cheswick, and other early authors who wrote so interestingly about computer security that I decided to make a career of it as well. Lastly, I wouldn't be who I am today without my twin brother, Richard Grimes, the better writer of the family, encouraging me to write over 20 years ago. To everyone in our industry, thanks for your help on the behalf of all of us.

Contents at a glance

Foreword xxxi

Introduction xxxiii

1 What Type of Hacker Are You? 1

2 How Hackers Hack 9

3 Profile: Bruce Schneier 23

4 Social Engineering 27

5 Profile: Kevin Mitnick 33

6 Software Vulnerabilities 39

7 Profile: Michael Howard 45

8 Profile: Gary McGraw 51

9 Malware 55

10 Profile: Susan Bradley 61

11 Profile: Mark Russinovich 65

12 Cryptography 69

13 Profile: Martin Hellman 75

14 Intrusion Detection/APTs 81

15 Profile: Dr. Dorothy E. Denning 87

16 Profile: Michael Dubinsky 91

17 Firewalls 95

18 Profile: William Cheswick. 101

19 Honeypots 107

20 Profile: Lance Spitzner 111

21 Password Hacking 115

22 Profile: Dr. Cormac Herley 123

23 Wireless Hacking 127

24 Profile: Thomas d'Otreppe de Bouvette 133

25 Penetration Testing 137

26 Profile: Aaron Higbee. 147

27 Profile: Benild Joseph 151

28 DDoS Attacks 155

29 Profile: Brian Krebs 161

30 Secure OS 165

31 Profile: Joanna Rutkowska 171

32 Profile: Aaron Margosis 175

33 Network Attacks 181

34 Profile: Laura Chappell. 185

35 IoT Hacking. 189

36 Profile: Dr. Charlie Miller 193

37 Policy and Strategy 201
38 Profile: Jing de Jong-Chen 205
39 Threat Modeling 211
40 Profile: Adam Shostack 217
41 Computer Security Education 221
42 Profile: Stephen Northcutt. 227
43 Privacy 231
44 Profile: Eva Galperin 235
45 Patching 239
46 Profile: Window Snyder 245
47 Writing as a Career 249
48 Profile: Fahmida Y. Rashid 259
49 Guide for Parents with Young Hackers 263
50 Hacker Code of Ethics 271
Index 275

Contents

Foreword xxxi

Introduction xxxiii

1 What Type of Hacker Are You? 1

Most Hackers Aren't Geniuses 2

Defenders Are Hackers Plus 3

Hackers Are Special 3

Hackers Are Persistent 4

Hacker Hats 4

2 How Hackers Hack 9

The Secret to Hacking 10

The Hacking Methodology 11

Hacking Is Boringly Successful 20

Automated Malware as a Hacking Tool 20

Hacking Ethically 21

3 Profile: Bruce Schneier 23

For More Information on Bruce Schneier 26

4 Social Engineering 27

Social Engineering Methods 27

Phishing 27

Trojan Horse Execution 28

Over the Phone 28

Purchase Scams 28

In-Person 29

Carrot or Stick 29

Social Engineering Defenses . . . 30
Education . . . 30
Be Careful of Installing Software from Third-Party Websites . . . 30
EV Digital Certificates . . . 31
Get Rid of Passwords . . . 31
Anti–Social Engineering Technologies . . . 31

5 Profile: Kevin Mitnick . . . 33
For More Information on Kevin Mitnick . . . 37

6 Software Vulnerabilities . . . 39
Number of Software Vulnerabilities . . . 39
Why Are Software Vulnerabilities Still a Big Problem? . . . 40
Defenses Against Software Vulnerabilities . . . 41
Security Development Lifecycle . . . 41
More Secure Programming Languages . . . 42
Code and Program Analysis . . . 42
More Secure Operating Systems . . . 42
Third-Party Protections and Vendor Add-Ons . . . 42
Perfect Software Won’t Cure All Ills . . . 43

7 Profile: Michael Howard . . . 45
For More Information on Michael Howard . . . 49

8 Profile: Gary McGraw . . . 51
For More Information on Gary McGraw . . . 54

9 Malware . . . 55
Malware Types . . . 55
Number of Malware Programs . . . 56
Mostly Criminal in Origin . . . 57
Defenses Against Malware . . . 58
Fully Patched Software . . . 58
Training . . . 58

Anti-Malware Software 58

Application Control Programs 59

Security Boundaries 59

Intrusion Detection 59

10 Profile: Susan Bradley 61

For More Information on Susan Bradley 63

11 Profile: Mark Russinovich 65

For More on Mark Russinovich 68

12 Cryptography 69

What Is Cryptography? 69

Why Can’t Attackers Just Guess All the Possible Keys? 70

Symmetric Versus Asymmetric Keys 70

Popular Cryptography 70

Hashes 71

Cryptographic Uses 72

Cryptographic Attacks 72

Math Attacks 72

Known Ciphertext/Plaintext 73

Side Channel Attacks 73

Insecure Implementations 73

13 Profile: Martin Hellman 75

For More Information on Martin Hellman 79

14 Intrusion Detection/APTs 81

Traits of a Good Security Event Message 82

Advanced Persistent Threats (APTs) 82

Types of Intrusion Detection 83

Behavior-Based 83

Signature-Based 84

Intrusion Detection Tools and Services 84

Intrusion Detection/Prevention Systems. 84

Event Log Management Systems 85

Detecting Advanced Persistent Threats (APTs) 85

15 Profile: Dr. Dorothy E. Denning 87

For More Information on Dr. Dorothy E. Denning 90

16 Profile: Michael Dubinsky 91

For More Information on Michael Dubinsky 93

17 Firewalls 95

What Is a Firewall? 95

The Early History of Firewalls 95

Firewall Rules 97

Where Are Firewalls? 97

Advanced Firewalls. 98

What Firewalls Protect Against 98

18 Profile: William Cheswick. 101

For More Information on William Cheswick 105

19 Honeypots 107

What Is a Honeypot? 107

Interaction 108

Why Use a Honeypot? 108

Catching My Own Russian Spy 109

Honeypot Resources to Explore 110

20 Profile: Lance Spitzner 111

For More Information on Lance Spitzner 114

21 Password Hacking 115

Authentication Components 115

Passwords 116

Authentication Databases 116
Password Hashes 116
Authentication Challenges 116
Authentication Factors 117
Hacking Passwords 117
Password Guessing 117
Phishing 118
Keylogging 118
Hash Cracking 118
Credential Reuse 119
Hacking Password Reset Portals 119
Password Defenses 119
Complexity and Length 120
Frequent Changes with No Repeating 120
Not Sharing Passwords Between Systems 120
Account Lockout 121
Strong Password Hashes 121
Don’t Use Passwords 121
Credential Theft Defenses 121
Reset Portal Defenses 122

22 Profile: Dr. Cormac Herley 123
For More Information on Dr. Cormac Herley 126

23 Wireless Hacking 127
The Wireless World 127
Types of Wireless Hacking 127
Attacking the Access Point 128
Denial of Service 128
Guessing a Wireless Channel Password 128
Session Hijacking 128
Stealing Information 129
Physically Locating a User 129

Some Wireless Hacking Tools 129
Aircrack-Ng 130
Kismet 130
Fern Wi-Fi Hacker 130
Firesheep 130
Wireless Hacking Defenses 130
Frequency Hopping 130
Predefined Client Identification 131
Strong Protocols 131
Long Passwords 131
Patching Access Points 131
Electromagnetic Shielding 131

24 Profile: Thomas d'Otreppe de Bouvette 133
For More Information on Thomas d'Otreppe de Bouvette 135

25 Penetration Testing 137
My Penetration Testing Highlights 137
Hacked Every Cable Box in the Country. 137
Simultaneously Hacked a Major Television Network and Pornography 138
Hacked a Major Credit Card Company. 138
Created a Camera Virus 139
How to Be a Pen Tester. 139
Hacker Methodology 139
Get Documented Permission First 140
Get a Signed Contract 140
Reporting 140
Certifications 141
Be Ethical. 145
Minimize Potential Operational Interruption 145

26 Profile: Aaron Higbee. 147
For More Information on Aaron Higbee 149

27 Profile: Benild Joseph 151

For More Information on Benild Joseph 153

28 DDoS Attacks 155

Types of DDoS Attacks 155

Denial of Service 155

Direct Attacks 156

Reflection Attacks 156

Amplification 156

Every Layer in the OSI Model 157

Escalating Attacks 157

Upstream and Downsteam Attacks 157

DDoS Tools and Providers. 158

Tools 158

DDoS as a Service 158

DDoS Defenses. 159

Training 159

Stress Testing 159

Appropriate Network Configuration 159

Engineer Out Potential Weak Points 159

Anti-DDoS Services 160

29 Profile: Brian Krebs 161

For More Information on Brian Krebs 164

30 Secure OS 165

How to Secure an Operating System 166

Secure-Built OS 166

Secure Guidelines 168

Secure Configuration Tools 169

Security Consortiums 169

Trusted Computing Group 169

FIDO Alliance 169

31 Profile: Joanna Rutkowska 171

For More Information on Joanna Rutkowska 173

32 Profile: Aaron Margosis 175

For More Information on Aaron Margosis 179

33 Network Attacks 181

Types of Network Attacks 181

Eavesdropping 182

Man-in-the-Middle Attacks 182

Distributed Denial-of-Service Attacks 183

Network Attack Defenses 183

Domain Isolation 183

Virtual Private Networks 183

Use Secure Protocols and Applications 183

Network Intrusion Detection 184

Anti-DDoS Defenses. 184

Visit Secure Web Sites and Use Secure Services 184

34 Profile: Laura Chappell. 185

For More Information on Laura Chappell 188

35 IoT Hacking 189

How Do Hackers Hack IoT? 189

IoT Defenses 190

36 Profile: Dr. Charlie Miller 193

For More Information on Dr. Charlie Miller 198

37 Policy and Strategy 201

Standards 201

Policies 202

Procedures 203

Frameworks 203

Regulatory Laws 203

Global Concerns 203

Systems Support 204

38 Profile: Jing de Jong-Chen 205

For More Information on Jing de Jong-Chen 209

39 Threat Modeling 211

Why Threat Model? 211

Threat Modeling Models 212

Threat Actors 213

Nation-States 213

Industrial Hackers 213

Financial Crime 213

Hacktivists 214

Gamers 214

Insider Threats 214

Ordinary, Solitary Hackers or Hacker Groups 214

40 Profile: Adam Shostack 217

For More Information on
Adam Shostack 220

41 Computer Security Education 221

Computer Security Training Topics 222

End-User/Security Awareness Training 222

General IT Security Training 222

Incident Response 222

OS and Application-Specific Training 223

Technical Skills 223

Certifications 223

Training Methods 224

Online Training 224

Break into My Website 224

Schools and Training Centers 224

Boot Camps 225

Corporate Training 225

Books 225

42 Profile: Stephen Northcutt 227

For More Information on Stephen Northcutt 230

43 Privacy 231

Privacy Organizations 232

Privacy-Protecting Applications 233

44 Profile: Eva Galperin 235

For More Information on Eva Galperin 237

45 Patching 239

Patching Facts 240

Most Exploits Are Caused by Old Vulnerabilities That Patches Exist For 240

Most Exploits Are Caused by a Few Unpatched Programs 240

The Most Unpatched Program Isn't Always the Most Exploited Program 241

You Need to Patch Hardware Too 241

Common Patching Problems 241

Detecting Missing Patching Isn't Accurate 241

You Can't Always Patch 242

Some Percentage of Patching Always Fails 242

Patching Will Cause Operational Issues 242

A Patch Is a Globally Broadcasted Exploit Announcement 243

46 Profile: Window Snyder 245

For More Information on Window Snyder 248