Hacking the Hacker
Hacking the Hacker

Learn from the Experts Who Take Down Hackers

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

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Foreword</td>
<td>xxxi</td>
</tr>
<tr>
<td>Introduction</td>
<td>xxxiii</td>
</tr>
<tr>
<td>1 What Type of Hacker Are You?</td>
<td>1</td>
</tr>
<tr>
<td>2 How Hackers Hack</td>
<td>9</td>
</tr>
<tr>
<td>3 Profile: Bruce Schneier</td>
<td>23</td>
</tr>
<tr>
<td>4 Social Engineering</td>
<td>27</td>
</tr>
<tr>
<td>5 Profile: Kevin Mitnick</td>
<td>33</td>
</tr>
<tr>
<td>6 Software Vulnerabilities</td>
<td>39</td>
</tr>
<tr>
<td>7 Profile: Michael Howard</td>
<td>45</td>
</tr>
<tr>
<td>8 Profile: Gary McGraw</td>
<td>51</td>
</tr>
<tr>
<td>9 Malware</td>
<td>55</td>
</tr>
<tr>
<td>10 Profile: Susan Bradley</td>
<td>61</td>
</tr>
<tr>
<td>11 Profile: Mark Russinovich</td>
<td>65</td>
</tr>
<tr>
<td>12 Cryptography</td>
<td>69</td>
</tr>
<tr>
<td>13 Profile: Martin Hellman</td>
<td>75</td>
</tr>
<tr>
<td>14 Intrusion Detection/APTs</td>
<td>81</td>
</tr>
<tr>
<td>15 Profile: Dr. Dorothy E. Denning</td>
<td>87</td>
</tr>
<tr>
<td>16 Profile: Michael Dubinsky</td>
<td>91</td>
</tr>
<tr>
<td>Chapter</td>
<td>Title</td>
</tr>
<tr>
<td>---------</td>
<td>--------------------------------------------</td>
</tr>
<tr>
<td>17</td>
<td>Firewalls</td>
</tr>
<tr>
<td>18</td>
<td>Profile: William Cheswick</td>
</tr>
<tr>
<td>19</td>
<td>Honeypots</td>
</tr>
<tr>
<td>20</td>
<td>Profile: Lance Spitzner</td>
</tr>
<tr>
<td>21</td>
<td>Password Hacking</td>
</tr>
<tr>
<td>22</td>
<td>Profile: Dr. Cormac Herley</td>
</tr>
<tr>
<td>23</td>
<td>Wireless Hacking</td>
</tr>
<tr>
<td>24</td>
<td>Profile: Thomas d’Otreppe de Bouvette</td>
</tr>
<tr>
<td>25</td>
<td>Penetration Testing</td>
</tr>
<tr>
<td>26</td>
<td>Profile: Aaron Higbee</td>
</tr>
<tr>
<td>27</td>
<td>Profile: Benild Joseph</td>
</tr>
<tr>
<td>28</td>
<td>DDoS Attacks</td>
</tr>
<tr>
<td>29</td>
<td>Profile: Brian Krebs</td>
</tr>
<tr>
<td>30</td>
<td>Secure OS</td>
</tr>
<tr>
<td>31</td>
<td>Profile: Joanna Rutkowska</td>
</tr>
<tr>
<td>32</td>
<td>Profile: Aaron Margosis</td>
</tr>
<tr>
<td>33</td>
<td>Network Attacks</td>
</tr>
<tr>
<td>34</td>
<td>Profile: Laura Chappell</td>
</tr>
<tr>
<td>35</td>
<td>IoT Hacking</td>
</tr>
<tr>
<td>36</td>
<td>Profile: Dr. Charlie Miller</td>
</tr>
</tbody>
</table>
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
Contents

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
Contents

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
<table>
<thead>
<tr>
<th>24</th>
<th>Profile: Thomas d’Otreppe de Bouvette</th>
<th>133</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>For More Information on Thomas d’Otreppe de Bouvette</td>
<td>135</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>26</th>
<th>Profile: Aaron Higbee</th>
<th>147</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>For More Information on Aaron Higbee</td>
<td>149</td>
</tr>
</tbody>
</table>
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
<table>
<thead>
<tr>
<th>Page</th>
<th>Section</th>
</tr>
</thead>
<tbody>
<tr>
<td>38</td>
<td>Profile: Jing de Jong-Chen</td>
</tr>
<tr>
<td></td>
<td>For More Information on Jing de Jong-Chen</td>
</tr>
<tr>
<td>39</td>
<td>Threat Modeling</td>
</tr>
<tr>
<td></td>
<td>Why Threat Model?</td>
</tr>
<tr>
<td></td>
<td>Threat Modeling Models</td>
</tr>
<tr>
<td></td>
<td>Threat Actors</td>
</tr>
<tr>
<td></td>
<td>Nation-States</td>
</tr>
<tr>
<td></td>
<td>Industrial Hackers</td>
</tr>
<tr>
<td></td>
<td>Financial Crime</td>
</tr>
<tr>
<td></td>
<td>Hacktivists</td>
</tr>
<tr>
<td></td>
<td>Gamers</td>
</tr>
<tr>
<td></td>
<td>Insider Threats</td>
</tr>
<tr>
<td></td>
<td>Ordinary, Solitary Hackers or Hacker Groups</td>
</tr>
<tr>
<td>40</td>
<td>Profile: Adam Shostack</td>
</tr>
<tr>
<td></td>
<td>For More Information on Adam Shostack</td>
</tr>
<tr>
<td>41</td>
<td>Computer Security Education</td>
</tr>
<tr>
<td></td>
<td>Computer Security Training Topics</td>
</tr>
<tr>
<td></td>
<td>End-User/Security Awareness Training</td>
</tr>
<tr>
<td></td>
<td>General IT Security Training</td>
</tr>
<tr>
<td></td>
<td>Incident Response</td>
</tr>
<tr>
<td></td>
<td>OS and Application-Specific Training</td>
</tr>
<tr>
<td></td>
<td>Technical Skills</td>
</tr>
<tr>
<td></td>
<td>Certifications</td>
</tr>
<tr>
<td></td>
<td>Training Methods</td>
</tr>
<tr>
<td></td>
<td>Online Training</td>
</tr>
</tbody>
</table>
Contents

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