Making Everything Easier!™

4th Edition

Hacking

FOR DUMMIES®

Learn to:

- Defend against the latest Windows® 8 and Linux® hacks
- Develop an effective ethical hacking plan
- Protect web applications, databases, laptops, and smartphones
- Use the latest testing tools and techniques

Kevin Beaver, CISSP

Independent Information Security Consultant

Hacking FOR DUMMIES®

4TH EDITION

by Kevin Beaver, CISSP

John Wiley & Sons, Inc.

Hacking For Dummies®, 4th Edition

Published by
John Wiley & Sons, Inc.
111 River Street
Hoboken, NJ 07030-5774
www.wiley.com

Published by John Wiley & Sons, Inc., Hoboken, New Jersey

Published simultaneously in Canada

Library of Congress Control Number: 2012955723

ISBN 978-1-11838093-2 (pbk); ISBN 978-1-118-38094-9 (ebk); ISBN 978-1-118-38095-6 (ebk); ISBN 978-1-118-38096-3 (ebk)

Manufactured in the United States of America

10 9 8 7 6 5 4 3 2 1

About the Author

Kevin Beaver is an independent information security consultant, expert witness, professional speaker, and author with Atlanta-based Principle Logic, LLC. He has two and a half decades of experience and specializes in performing information security assessments for corporations, security product vendors, independent software developers, universities, government agencies, and nonprofit organizations. Before starting his information security consulting practice in 2001, Kevin served in various information technology and security roles for several healthcare, e-commerce, financial, and educational institutions.

Kevin has appeared on CNN television as an information security expert and has been quoted in *The Wall Street Journal*, *Entrepreneur*, *Fortune Small Business*, *Women's Health*, and *Inc.* magazine's technology site IncTechnology.com. Kevin's work has also been referenced by the PCI Council in their Data Security Standard Wireless Guidelines. Kevin has been a top-rated speaker, giving hundreds of presentations and panel discussions for IT and security seminars, conferences, and webcasts over the past decade.

Kevin has authored/coauthored 10 information security books, including *Hacking Wireless Networks For Dummies*, *Implementation Strategies for Fulfilling and Maintaining IT Compliance* (Realtimepublihers.com), and *The Practical Guide to HIPAA Privacy and Security Compliance* (Auerbach). Kevin has written more than 30 whitepapers and 600 articles and is a regular contributor to SearchCompliance.com, SearchEnterpriseDesktop.com, and Security Technology Executive magazine. Kevin is the creator and producer of the Security On Wheels audiobooks, which provide security learning for IT professionals on the go (`securityonwheels.com`), and the Security On Wheels blog (`securityonwheels.com/blog`). He also covers information security and related matters on Twitter (`@kevinbeaver`) and YouTube (`PrincipleLogic`). Kevin earned his bachelor's degree in Computer Engineering Technology from Southern College of Technology and his master's degree in Management of Technology from Georgia Tech. He has obtained his CISSP certification in 2001 and also holds MCSE, Master CNE, and IT Project+ certifications.

Kevin can be reached through his website, `www.principlelogic.com`, and

you can connect to him via LinkedIn at www.linkedin.com/in/kevinbeaver.

Dedication

This one’s for my country, the United States of America. You’re under attack and have been dealt another blow — kicked while you were down. I know without a doubt I wouldn’t be where I’m at both personally and professionally without the opportunities your Founding Fathers and brave soldiers fighting for freedom have afforded me. I’m going to continue to fight, along with my fellow independent thinkers, to preserve America in the spirit of which it was intended. We shall prevail.

Author's Acknowledgments

First, I want to thank Amy, Garrett, and Mary Lin for being here for me yet again and putting up with my intermittent crankiness while working on this edition. I love you all 100 percent!

I'd also like to thank Melody Layne, my original acquisitions editor at Wiley, for contacting me long ago with this book idea and providing me this great opportunity. I'd also like to thank my current acquisitions editor, Amy Fandrei, for continuing this project and presenting me the opportunity to shape this book into something I'm very proud of.

I'd like to thank my project editor, Becky Huehls. You've been extraordinarily patient and a real gem to work with! I hope I have a chance to work with you again. I'd also like to thank Virginia Sanders, my copy editor, for helping me keep my focus and really fine-tuning the wording. Also, many thanks to my technical editor, business colleague, friend, and coauthor of *Hacking Wireless Networks For Dummies*, Peter T. Davis. Again, I'm honored to be working with you and very much appreciate your valuable feedback and additions. Your keen eye has kept me in check, yet again.

Much gratitude to Robert Abela with Acunetix; HD Moore, Jill McInnis, and Chris Kirsch with Rapid7; Vladimir Katalov and Olga Koksharova with Elcomsoft; Charlene Sciberras with GFI Software; Maty Siman and Asaph Schulman with Checkmarx; Dmitry Sumin with Passware; Brian Miller with HP's Application Security Center; Kirk Thomas with Northwest Performance Software; David Vest with Mythicsoft; Justin Warren and Dan Kuykendall with NT Objectives; Michael Berg with TamoSoft; Terry Ingoldsby with Amenaza Technologies; Oleg Fedorov with Oxygen Software Company; Todd Feinman and Chris Arold with Identity Finder for responding to all my requests. Thanks to Dave Coe for your help in keeping me current on the latest security tools and hacks. Much gratitude to all the others I forgot to mention as well!

Mega thanks to Queensrÿche, Rush, Incubus, Black Country Communion, and Dream Theater for your energizing sounds and inspirational words. Your music truly helped me stayed motivated during the long hours spent getting this new edition out!

Serious thanks to Neal Boortz for going against the grain and educating me

Serious thanks to Neal Boortz for going against the grain and educating me about what's happening in our country and the world we live in. You have kept me motivated as an entrepreneur, small business owner, and libertarian for a couple of decades. You speak the truth and I'm saddened that you're retiring. Enjoy it though; you've earned it!

Thanks to Brian Tracy, John Maxwell, and the late Richard Carlson for your immeasurable insight and guidance on what it takes to be a better person. Each of your contributions have helped me in so many ways that I couldn't possibly pay you back.

Finally, I want to send out a sincere thanks and humble appreciation to my clients for hiring me, a "no-name-brand" consultant, and keeping me around for the long term. I wouldn't be here without your willingness to break out of the "must hire big company" mindset and your continued support. Thank you very much.

Publisher's Acknowledgments

We're proud of this book; please send us your comments at http://dummies.custhelp.com. For other comments, please contact our Customer Care Department within the U.S. at 877-762-2974, outside the U.S. at 317-572-3993, or fax 317-572-4002.

Some of the people who helped bring this book to market include the following:

Acquisitions and Editorial

Sr. Project Editor: Rebecca Huehls

Acquisitions Editor: Amy Fandrei

Copy Editor: Virginia Sanders

Technical Editor: Peter T. Davis

Sr. Editorial Manager: Leah Michael

Editorial Assistant: Annie Sullivan

Sr. Editorial Assistant: Cherie Case

Cover Photo: © Nicolas Loran *iStockphoto (computer image); © rionm* iStockphoto (background image)

Cartoons: Rich Tennant (www.the5thwave.com)

Composition Services

Project Coordinator: Sheree Montgomery

Layout and Graphics: Jennifer Creasey

Proofreaders: Cynthia Fields, Jessica Kramer

Indexer: Potomac Indexing, LLC

Publishing and Editorial for Technology Dummies

Richard Swadley, Vice President and Executive Group Publisher

Andy Cummings, Vice President and Publisher

Mary Bednarek, Executive Acquisitions Director

Mary C. Corder, Editorial Director

Publishing for Consumer Dummies

Kathleen Nebenhaus, Vice President and Executive Publisher

Composition Services

Debbie Stailey, Director of Composition Services

Hacking For Dummies®, 4th Edition

Visit www.dummies.com/cheatsheet/hacking to view this book's cheat sheet.

Table of Contents

Part II: Putting Ethical Hacking in Motion

Chapter 5: Social Engineering

Chapter 6: Physical Security

Chapter 7: Passwords

Introduction

Welcome to *Hacking For Dummies*, 4th Edition. This book outlines — in plain English — computer hacker tricks and techniques that you can use to assess the security of your information systems, find the security vulnerabilities that matter, and fix the weaknesses before criminal hackers and malicious users take advantage of them. This hacking is the professional, aboveboard, and legal type of security testing — which I call *ethical hacking* throughout the book.

Computer and network security is a complex subject and an ever-moving target. You must stay on top of it to ensure that your information is protected from the bad guys. That's where the tools and techniques outlined in this book can help.

You can implement all the security technologies and other best practices possible, and your information systems might be secure — as far as you know. However, until you understand how malicious attackers think, apply that knowledge, and use the right tools to assess your systems from their point of view, you can't get a true sense of how secure your information really is.

Ethical hacking — which encompasses formal and methodical *penetration testing*, *white hat hacking*, and *vulnerability testing* — is necessary to find security flaws and to help validate that your information systems are truly secure on an ongoing basis. This book provides you with the knowledge to implement an ethical hacking program successfully, perform ethical hacking tests, and put the proper countermeasures in place to keep external hackers and malicious users in check.

Who Should Read This Book?

Disclaimer: If you choose to use the information in this book to hack or break into computer systems maliciously and without authorization, you're on your own. Neither I (the author) nor anyone else associated

with this book shall be liable or responsible for any unethical or criminal choices that you might make and execute using the methodologies and tools that I describe. This book is intended solely for IT and information security professionals to test information security — either on your own systems or on a client's systems — in an authorized fashion.

Okay, now that that's out of the way, it's time for the good stuff! This book is for you if you're a network administrator, information security manager, security consultant, security auditor, compliance manager, or interested in finding out more about legally and ethically testing computer systems and IT operations to make things more secure.

As the ethical hacker performing well-intended information security assessments, you can detect and point out security holes that might otherwise be overlooked. If you're performing these tests on your systems, the information you uncover in your tests can help you win over management and prove that information security really is a business issue to be taken seriously. Likewise, if you're performing these tests for your clients, you can help find security holes that can be plugged before the bad guys have a chance to exploit them.

The information in this book helps you stay on top of the security game and enjoy the fame and glory of helping your organization and clients prevent bad things from happening to their information.

About This Book

Hacking For Dummies, 4th Edition, is a reference guide on hacking your systems to improve security and help minimize business risks. The ethical hacking techniques are based on written and unwritten rules of computer system penetration testing, vulnerability testing, and information security best practices. This book covers everything from establishing your hacking plan to testing your systems to plugging the holes and managing an ongoing ethical hacking program. Realistically, for many networks, operating systems, and applications, thousands of possible hacks exist. I cover the major ones on various platforms and systems. Whether you need to assess security vulnerabilities on a small home office network, a medium-sized corporate network, or across large enterprise systems, *Hacking For Dummies*, 4th Edition, provides the information you need.

How to Use This Book

This book includes the following features:

- Various technical and nontechnical hack attacks and their detailed methodologies
- Information security testing case studies from well-known information security experts
- Specific countermeasures to protect against hack attacks

Before you start hacking your systems, familiarize yourself with the information in Part I so you're prepared for the tasks at hand. The adage "if you fail to plan, you plan to fail" rings true for the ethical hacking process. You must get permission and have a solid game plan in place if you're going to be successful.

This material is not intended to be used for unethical or illegal hacking purposes to propel you from script kiddie to megahacker. Rather, it is designed to provide you with the knowledge you need to hack your own or your clients' systems — ethically and legally — to enhance the security of the information involved.

What You Don't Need to Read

Depending on your computer and network configurations, you may be able to skip chapters. For example, if you aren't running Linux or wireless networks, you can skip those chapters. Just be careful. You may think you're not running certain systems, but they could very well be on your network somewhere.

Foolish Assumptions

I make a few assumptions about you, the aspiring information security professional:

- You're familiar with basic computer-, network-, and information-security–related concepts and terms.

- You have a basic understanding of what hackers and malicious users do.
- You have access to a computer and a network on which to use these techniques.
- You have access to the Internet to obtain the various tools used in the ethical hacking process.
- You have permission to perform the hacking techniques described in this book.

How This Book Is Organized

This book is organized into seven modular parts, so you can jump around from one part to another as needed. Each chapter provides practical methodologies and practices you can use as part of your ethical hacking efforts, including checklists and references to specific tools you can use, as well as resources on the Internet.

Part I: Building the Foundation for Ethical Hacking

This part covers the fundamental aspects of ethical hacking. It starts with an overview of the value of ethical hacking and what you should and shouldn't do during the process. You get inside the malicious mindset and discover how to plan your ethical hacking efforts. This part covers the steps involved in the ethical hacking process, including how to choose the proper tools.

Part II: Putting Ethical Hacking in Motion

This part gets you rolling with the ethical hacking process. It covers several well-known and widely used hack attacks, including social engineering and cracking passwords, to get your feet wet. This part covers the human and physical elements of security, which tend to be the weakest links in any information security program. After you plunge into these topics, you'll know the tips and tricks required to perform common general hack attacks against your systems, as well as specific countermeasures to keep your information systems secure.

Part III: Hacking Network Hosts

Starting with the larger network in mind, this part covers methods to test your systems for various well-known network infrastructure vulnerabilities. From weaknesses in the TCP/IP protocol suite to wireless network insecurities, you find out how networks are compromised by using specific methods of flawed network communications, along with various countermeasures that you can implement to avoid becoming a victim. I then delve down into mobile devices and show how phones, tablets, and the like can be exploited. This part also includes case studies on some of the network hack attacks that are presented.

Part IV: Hacking Operating Systems

Practically all operating systems have well-known vulnerabilities that hackers often exploit. This part jumps into hacking the widely used operating systems: Windows and Linux. The hacking methods include scanning your operating systems for vulnerabilities and enumerating the specific hosts to gain detailed information. This part also includes information on exploiting well-known vulnerabilities in these operating systems, taking over operating systems remotely, and specific countermeasures that you can implement to make your operating systems more secure. This part includes case studies on operating system hack attacks.

Part V: Hacking Applications

Application security is gaining more visibility in the information security arena these days. An increasing number of attacks — which are often able to bypass firewalls, intrusion detection systems, and antivirus software — are aimed directly at various applications. This part discusses hacking specific business applications, including coverage of e-mail systems, Voice over Internet Protocol (VoIP), web applications, databases, and storage systems, along with practical countermeasures that you can put in place to make your systems more secure.

Part VI: Ethical Hacking Aftermath

After you perform your ethical hack attacks, what do you do with the information you gather? Shelve it? Show it off? How do you move forward? This part answers these questions and more. From developing reports for upper management to remediating the security flaws that you discover to establishing procedures for your ongoing ethical hacking efforts, this part brings the ethical hacking process full circle. This information not only ensures that your effort and time are well spent, but also is evidence that information security is an essential element for success in any business that depends on computers and information technology.

Part VII: The Part of Tens

This part contains tips to help ensure the success of your ethical hacking program. You find out how to get upper management to buy into your ethical hacking program so you can get going and start protecting your systems. This part also includes the top ten ethical hacking mistakes you absolutely must avoid.

This part also includes an Appendix that provides a one-stop reference listing of ethical hacking tools and resources. You can find all the links in the Appendix on the *Hacking For Dummies* online Cheat Sheet at www.dummies.com/cheatsheet/hacking.

Icons Used in This Book

This icon points out information that is worth committing to memory.

This icon points out information that could have a negative impact on your ethical hacking efforts — so please read it!

This icon refers to advice that can help highlight or clarify an important point.

This icon points out technical information that is interesting but not vital to your understanding of the topic being discussed.

Where to Go from Here

The more you know about how external hackers and rogue insiders work and how your systems should be tested, the better you're able to secure your

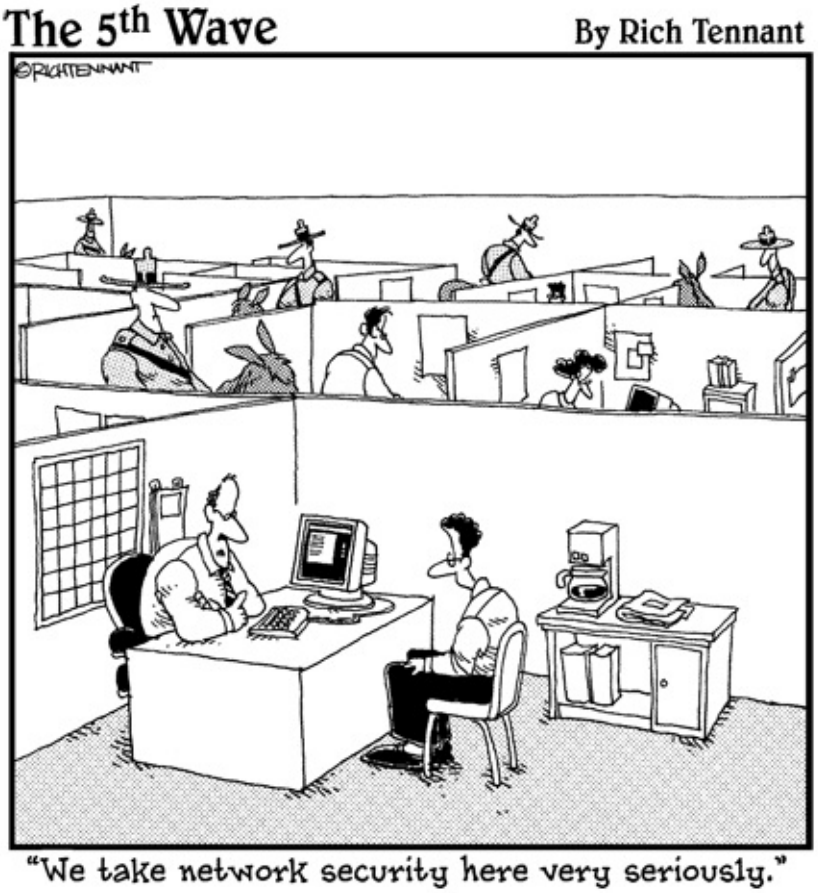
computer systems. This book provides the foundation that you need to develop and maintain a successful ethical hacking program in order to minimize business risks.

Keep in mind that the high-level concepts of ethical hacking won't change as often as the specific information security vulnerabilities you protect against. Ethical hacking will always remain both an art and a science in a field that's ever-changing. You must keep up with the latest hardware and software technologies, along with the various vulnerabilities that come about month after month and year after year. When I do have important updates to this book, you can find them at www.dummies.com/go/hackingfdupdates.

You won't find a single *best* way to hack your systems, so tweak this information to your heart's content. Happy (ethical) hacking!

Part I

Building the Foundation for Ethical Hacking



In this part . . .

Your mission — should you choose to accept it — is to find the holes in your network before the bad guys do. This mission will be fun, educational, and most likely entertaining. It will certainly be an eye-opening experience. The cool part is that you can emerge as the hero, knowing that your organization

will be better protected against malicious hackers and insider attacks and less likely to experience a breach and have its name smeared across the headlines.

If you’re new to ethical hacking, this is the place to begin. The chapters in this part get you started with information on what to do and how to do it when you’re hacking your own systems. Oh, and you find out what not to do as well. This information will guide you through building the foundation for your ethical hacking program. This foundation will keep you on the right path and off any one-way dead-end streets. This mission is indeed possible — you just have to get your ducks in a row first.

Chapter 19

Ten Tips for Getting Upper Management Buy-In

Dozens of key steps exist for obtaining the buy-in and sponsorship that you need to support your ethical hacking efforts. In this chapter, I describe the ones that I find are the most effective.

Cultivate an Ally and a Sponsor

Selling ethical hacking and information security to management isn't something you want to tackle alone. Get an ally — preferably your direct manager or someone at that level or higher in the organization. Choose someone who understands the value of ethical hacking as well as information security in general. Although this person might not be able to speak for you directly, she can be seen as an unbiased third-party sponsor and can give you more credibility.

Don't Be a FUDdy Duddy

Sherlock Holmes said, "It is a capital mistake to theorize before one has data." To make a good case for information security and the need for ethical hacking, support your case with relevant data. However, don't blow stuff out of proportion for the sake of stirring up fear, uncertainty, and doubt (FUD). Managers worth their salt can see right through that. Focus on educating management with practical advice. Rational fears proportional to the threat are fine. Just don't take the Chicken Little route, claiming that the sky is falling with everything all the time.

Demonstrate How the Organization Can't Afford to Be Hacked

Can't Afford to Be Hacked

Show how dependent the organization is on its information systems. Create *what-if* scenarios — sort of a business impact assessment — to show what can happen, how the organization's reputation can be damaged, and how long the organization can go without using the network, computers, and data. Ask upper-level managers what they would do without their computer systems and IT personnel — or what they'd do if sensitive business or client information was compromised. Show real-world anecdotal evidence of hacker attacks, including malware, physical security, and social engineering issues, but be positive about it. Don't approach management negatively with FUD. Rather, keep them informed on serious security happenings. To help management relate, find stories regarding similar businesses or industries. (A good resource is the Privacy Rights Clearinghouse listing, Chronology of Data Breaches, at www.privacyrights.org/data-breach.) Clip magazine and newspaper articles as well. Let the facts speak for themselves.

Google is a great tool to find practically everything you need regarding information security breaches.

Show management that the organization *does* have what a hacker wants. A common misconception among those ignorant about information security threats and vulnerabilities is that their organization or network is not really at risk. Be sure to point out the potential costs from damage caused by hacking:

- Missed opportunity costs
- Exposure of intellectual property
- Liability issues
- Legal costs and judgments
- Compliance-related fines
- Lost productivity
- Clean-up time and incident response costs
- Replacement costs for lost, exposed, or damaged information or systems
- Costs of fixing a tarnished reputation

Outline the General Benefits of Ethical Hacking

In addition to the potential costs listed in the preceding section, talk about how proactive testing can help find security vulnerabilities in information systems that normally might be overlooked. Tell management that information security testing in the context of ethical hacking is a way of thinking like the bad guys so that you can protect yourself from the bad guys — the "know your enemy" mindset from Sun Tzu's *The Art of War*.

Show How Ethical Hacking Specifically Helps the Organization

Document benefits that support the overall business goals:

- **Demonstrate how security can be inexpensive and can save the organization money in the long run.**
  - Security is much easier and cheaper to build up front than to add on later.
  - Security doesn't have to be inconvenient and can enable productivity if it's done properly.
- **Discuss how new products or services can be offered for a competitive advantage if secure information systems are in place.**
  - State and federal privacy and security regulations are met.
  - Business partner and customer requirements are satisfied.
  - Managers and the company come across as business worthy.
  - Ethical hacking and the appropriate remediation process show that the organization is protecting sensitive customer and business information.
- **Outline the compliance benefits of in-depth security testing.**

Get Involved in the Business

Understand the business — how it operates, who the key players are, and

what politics are involved:

- **Go to meetings to see and be seen.** This can help prove that you're concerned about the business.
- **Be a person of value who's interested in contributing to the business.**
- **Know your opposition.** Again, use the "know your enemy" mentality — if you understand the people you're dealing with, along with their potential objections, buy-in is *much* easier to get.

Establish Your Credibility

Focus on these three characteristics:

- **Be positive about the organization and prove that you really mean business.** Your attitude is critical.
- **Empathize with managers and show them that you understand the business side and what they're up against.**
- **To create any positive business relationship, you must be trustworthy.** Build that trust over time, and selling security will be *much* easier.

Speak on Management's Level

As cool as it sounds, no one is really that impressed with techie talk. Talk in terms of the business. This key element of obtaining buy-in is actually part of establishing your credibility, but deserves to be listed by itself.

I've seen countless IT and security professionals lose upper-level managers as soon as they start speaking. A megabyte here; stateful inspection there; packets, packets everywhere! Bad idea. Relate security issues to everyday business processes and job functions. Period.

Show Value in Your Efforts

Here's where the rubber meets the road. If you can demonstrate that what you're doing offers business value on an ongoing basis, you can maintain a

good pace and not have to constantly plead to keep your ethical hacking program going. Keep these points in mind:

- **Document your involvement in IT and information security, and create ongoing reports for management regarding the state of security in the organization.** Give management examples of how the organization's systems will be secured from attacks.
- **Outline tangible results as a proof of concept.** Show sample vulnerability assessment reports you've run on your systems or from the security tool vendors.
- **Treat doubts, concerns, and objections by upper management as requests for more information.** Find the answers and go back armed and ready to prove your ethical-hacking worthiness.

Be Flexible and Adaptable

Prepare yourself for skepticism and rejection at first. It happens a lot, especially from upper-level managers such as CFOs and CEOs, who are often completely disconnected from IT and security in the organization. A middle management structure that lives to create complexity is a party to the problem as well.

Don't get defensive. Security is a long-term process, not a short-term product or single assessment. Start small — use a limited amount of resources, such as budget, tools, and time, and then build the program over time.

Studies have found that new ideas presented casually and without pressure are considered and have a higher rate of acceptance than ideas that are forced on people under a deadline. Just as with a spouse or colleagues at work, if you focus on and fine tune your approach — at least as much as you focus on the content of what you're going to say — you can often get people on your side, and in return, get a lot more accomplished.

Chapter 20

Ten Reasons Hacking Is the Only Effective Way to Test

Ethical hacking is not just for fun or show. For numerous business reasons, ethical hacking is the only effective way to find the security vulnerabilities that matter in your organization.

The Bad Guys Think Bad Thoughts, Use Good Tools, and Develop New Methods

If you're going to keep up with external attackers and malicious insiders, you have to stay current on the latest attack methods and tools that they're using. I cover some of the latest tricks, techniques, and tools in Chapter 10 (mobile) and Chapter 14 (websites and applications).

IT Governance and Compliance Are More Than High-Level Checklist Audits

With all the government laws and industry regulations in place, your business likely doesn't have a choice in the security matter. The problem is that being compliant with these laws and regulations doesn't automatically mean you're secure. PCI DSS comes to mind. You have to take off the checklist audit blinders. Using ethical hacking tools and techniques enables you to dig deeper into your business's true vulnerabilities.

Ethical Hacking Complements Audits and Security Evaluations

No doubt, someone in your organization understands higher-level security audits better than this ethical hacking stuff. However, if you can sell that person on ethical hacking and integrate it into existing security initiatives (such as internal audits and compliance spot checks), the auditing process can go much deeper and improve your outcomes. Everyone wins.

Clients and Partners Will Ask, "How Secure Are Your Systems?"

Many businesses now require in-depth security assessments of their business partners. The same goes for certain clients. The bigger companies might want to know how secure their information is on your network. The only way to definitively know where things stand is to use the methods and tools I cover in this book.

The Law of Averages Works against Businesses

Information systems are becoming more complex by the day. Literally. It's just a matter of time before these complexities work against you and in the bad guys' favor. A criminal hacker needs to find only one flaw to be successful in his efforts. Security professionals have to find them all. If you're going to stay informed and ensure that your critical business systems and the sensitive information they process and store stay secure, you have to look at things with a malicious mindset.

Ethical Hacking Improves Understanding of Business Threats

You can say passwords are weak or patches are missing, but actually

exploiting such flaws and showing the outcome are quite different matters. There's no better way to prove there's a problem and motivate management to do something about it than by showing the outcomes of ethical hacking.

If a Breach Occurs, You Have Something to Fall Back On

In the event a malicious insider or external attacker still breaches your security, your business is sued, or your business falls out of compliance with laws or regulations, the management team can at least demonstrate that it was performing due diligence to uncover security risks on a periodic and consistent basis. A related area that can be problematic is knowing about a problem and not fixing it. The last thing you need is a lawyer and his expert witness pointing out how your business was lax in the area of information security testing or follow-through.

Ethical Hacking Brings Out the Worst in Your Systems

Someone walking around with a checklist can find security "best practices" you're missing, but he isn't going to find most of the in-depth security flaws that ethical hacking is going to uncover. You know, the ones that can get you into the worst trouble. Ethical hacking brings out the warts and all.

Ethical Hacking Combines the Best of Penetration Testing and Vulnerability Assessments

Penetration testing is rarely enough to find everything in your systems because the scope of traditional penetration testing is simply too limited. The same goes for vulnerability assessments that mostly involve security scans. Ethical hacking combines the best of both and gets you the most bang for your buck.

Ethical Hacking Can Uncover Weaknesses That Might Go Overlooked for Years

Ethical hacking not only uncovers technical, physical, and human weaknesses, but it can also reveal problems with IT and security operations, such as patch management, change management, and lack of awareness, which may not be found otherwise.

Appendix

Tools and Resources

To stay up-to-date with the latest and greatest ethical hacking tools and resources, you need to know where to turn. This appendix contains my favorite security sites, tools, resources, and more that you can benefit from in your ongoing ethical hacking program.

This book's online Cheat Sheet contains links to all the online tools and resources listed in this appendix. Check it out at www.dummies.com/cheatsheet/hacking.

Advanced Malware

Bit9 Parity Suite — https://www.bit9.com/products

Damballa Failsafe — www.damballa.com/solutions/damballa_failsafe.php

Sourcefire — www.sourcefire.com/security-technologies/network-security/next-generation-intrusion-prevention-system

Bluetooth

Blooover — http://trifinite.org/trifinite_stuff_blooover.html

Bluejacking Forums and Community site — www.bluejackq.com/bluejacking-forums.shtml

BlueScanner — http://sourceforge.net/projects/bluescanner

Bluesnarfer — www.alighieri.org/tools/bluesnarfer.tar.gz

BlueSniper rifle — www.tomsguide.com/us/how-to-bluesniper-pt1,review-408.html

BTScanner for XP — www.pentest.co.uk/src/btscanner_1_0_0.zip

Car Whisperer — http://trifinite.org/trifinite_stuff_carwhisperer.html

Smurf — www.gatefold.co.uk/smurf

Certifications

Certified Ethical Hacker — www.eccouncil.org/CEH.htm

Certified Information Security Manager — www.isaca.org

Certified Information Systems Security Professional — www.isc2.org/cissp/default.aspx

Certified Wireless Security Professional — www.cwnp.com/certifications/cwsp/

CompTIA Security+ — http://certification.comptia.org/getCertified/certifications/secu

SANS GIAC — www.giac.org

Databases

Advanced Access Password Recovery — www.elcomsoft.com/acpr.html

Advanced SQL Password Recovery — www.elcomsoft.com/asqlpr.html

AppDetectivePro — www.appsecinc.com/products/appdetective

Elcomsoft Distributed Password Recovery — www.elcomsoft.com/edpr.html

Idera — www.idera.com

Microsoft SQL Server Management Studio Express — www.microsoft.com/en-us/download/details.aspx?id=7593

Nexpose — www.rapid7.com/vulnerability-scanner.jsp

Pete Finnigan's listing of Oracle scanning tools — www.petefinnigan.com/tools.htm

QualysGuard — www.qualys.com

SQLPing3 — www.sqlsecurity.com/downloads

Exploits

Metasploit — www.metasploit.com

Offensive Security's Exploit Database — www.exploit-db.com

Pwnie Express http://pwnieexpress.com

General Research Tools

AFRINIC — www.afrinic.net

APNIC — www.apnic.net

ARIN — http://whois.arin.net/ui

Bing — www.bing.com

DNSstuff — www.dnsstuff.com

DNS Tools — www.dnstools.com

The File Extension Source — http://filext.com

Google — www.google.com

Google advanced operators — www.googleguide.com/advanced_operators.html

Government domains — www.dotgov.gov/portal/web/dotgov/whois

Hoover's business information — www.hoovers.com

LACNIC — www.lacnic.net

Netcraft's *What's that site running?* — http://news.netcraft.com

RIPE Network Coordination Centre — https://apps.db.ripe.net/search/query.html

Switchboard.com — www.switchboard.com

theHarvester — http://code.google.com/p/theharvester

United States Patent and Trademark Office — www.uspto.gov

US Search.com — www.ussearch.com

U.S. Securities and Exchange Commission — www.sec.gov/edgar.shtml

Wotsit's Format — www.wotsit.org

Whois — www.whois.net

WhatIsMyIP — www.whatismyip.com

Yahoo! Finance — http://finance.yahoo.com

ZabaSearch — www.zabasearch.com

Hacker Stuff

2600 The Hacker Quarterly — www.2600.com

Computer Underground Digest — http://cu-digest.org

Hacker T-shirts, equipment, and other trinkets — www.thinkgeek.com

Hackin9 — http://hakin9.org

Honeypots: Tracking Hackers — www.tracking-hackers.com

The Jargon File — www.jargon.8hz.com

Phrack — www.phrack.org

Keyloggers

Invisible KeyLogger Stealth — www.amecisco.com/iks.htm

KeyGhost — www.keyghost.com

SpectorSoft — www.spectorsoft.com

Laws and Regulations

Computer Fraud and Abuse Act — www.fas.org/sgp/crs/misc/RS20830.pdf

Gramm-Leach-Bliley Act (GLBA) Safeguards Rule — www.ftc.gov/os/2002/05/67fr36585.pdf

Health Information Technology for Economic and Clinical Health (HITECH) Act — http://en.wikipedia.org/wiki/Health_Information_Technology_for_Ec

Health Insurance Portability and Accountability Act (HIPAA) Security Rule — www.hhs.gov/ocr/privacy/hipaa/understanding/srsummary.html

Payment Card Industry Data Security Standard (PCI DSS) — www.pcisecuritystandards.org/security_standards/index.php

Sarbanes-Oxley Act — www.sec.gov/about/laws.shtml#sox2002

United States state breach notification laws — www.ncsl.org/programs/lis/cip/priv/breachlaws.htm

Linux

BackTrack Linux — www.backtrack-linux.org

freshmeat.net — http://freecode.com

GFI LanGuard — www.gfi.com/networksecurity-vulnerability-scanner

Linux Security Auditing Tool (LSAT) — http://usat.sourceforge.net

Nexpose — www.rapid7.com/vulnerability-scanner.jsp

QualysGuard — www.qualys.com

SourceForge — http://sourceforge.net

THC-Amap — www.thc.org/thc-amap

Tiger — www.nongnu.org/tiger

Live Toolkits

BackTrack Linux — www.backtrack-linux.org

Comprehensive listing of live bootable Linux toolkits — www.livecdlist.com/

Knoppix — http://knoppix.net

Network Security Toolkit — www.networksecuritytoolkit.org

Security Tools Distribution — http://s-t-d.org

Log Analysis

ArcSight Logger — www.hpenterprisesecurity.com/products/hp-arcsight-security-intelligence/hp-arcsight-logger/

GFI EventsManager — www.gfi.com/eventsmanager

Messaging

Abuse.net SMTP relay checker — www.abuse.net/relay.html

Brutus — www.hoobie.net/brutus

Cain & Abel — www.oxid.it/cain.html

DNSstuff relay checker — www.dnsstuff.com

EICAR Anti-Virus test file — www.eicar.org/anti_virus_test_file.htm

GFI e-mail security test — www.gfi.com/pages/email-security.asp

mailsnarf — www.monkey.org/~dugsong/dsniff

smtpscan — www.freshports.org/security/smtpscan

Miscellaneous

3M Privacy Filters — www.shop3m.com/3m-privacy-filters.html

7-Zip — www.7-zip.org

WinZip — www.winzip.com

Mobile

BitLocker whitepapers www.principlelogic.com/bitlocker.html

Checkmarx CxDeveloper — www.checkmarx.com

Elcomsoft Forensic Disk Decryptor — www.elcomsoft.com/efdd.html

Elcomsoft's Phone Password Breaker — www.elcomsoft.com/eppb.html

Elcomsoft System Recovery — www.elcomsoft.com/esr.html

iOS Forensic Toolkit — http://ios.elcomsoft.com

Ophcrack — http://ophcrack.sourceforge.net

Oxygen Forensic Suite — www.oxygen-forensic.com

Passware Kit Forensic — www.lostpassword.com/kit-forensic.htm

Veracode — www.veracode.com

Networks

Arpwatch — http://linux.maruhn.com/sec/arpwatch.html

Blast — www.mcafee.com/us/downloads/free-tools/blast.aspx

Cain & Abel — www.oxid.it/cain.html

CommView — www.tamos.com/products/commview

dsniff — www.monkey.org/~dugsong/dsniff

Essential NetTools — www.tamos.com/products/nettools

Ettercap — http://ettercap.sourceforge.net

Fortinet — www.fortinet.com

Getif — www.wtcs.org/snmp4tpc/getif.htm

GFI LanGuard — www.gfi.com/networksecurity-vulnerability-scanner

GNU MAC Changer — www.alobbs.com/macchanger

IETF RFCs — www.rfc-editor.org/rfcxx00.html

IKECrack — http://ikecrack.sourceforge.net

MAC address vendor lookup — http://standards.ieee.org/develop/regauth/oui/public.html

Nessus vulnerability scanner — www.tenable.com/products/nessus

Netcat — http://netcat.sourceforge.net

netfilter/iptables — www.netfilter.org

NetResident — www.tamos.com/products/netresident

NetScanTools Pro — www.netscantools.com

Nexpose — www.rapid7.com/vulnerability-scanner.jsp

Nmap port scanner — http://nmap.org

NMapWin — http://sourceforge.net/projects/nmapwin

OmniPeek — www.wildpackets.com/products/omnipeek_network_analyzer

Port number listing — www.iana.org/assignments/port-numbers

Port number lookup — www.cotse.com/cgi-bin/port.cgi

PortSentry — http://sourceforge.net/projects/sentrytools

PromiscDetect — http://ntsecurity.nu/toolbox/promiscdetect

QualysGuard vulnerability scanner — www.qualys.com

SMAC MAC address changer — www.klcconsulting.net/smac

SNARE — www.intersectalliance.com/projects/Snare

sniffdet — http://sniffdet.sourceforge.net

SNMPUTIL — www.wtcs.org/snmp4tpc/FILES/Tools/SNMPUTIL/SNMPUTIL.zip

SonicWALL — www.sonicwall.com

Sourcefire — www.sourcefire.com/security-technologies/networksecurity/next-generation-intrusion-prevention-system

TCP Wrappers — http://protect.iu.edu/cybersecurity/tcp-wrappers

Traffic IQ Professional — www.idappcom.com

UDPFlood — www.mcafee.com/us/downloads/free-tools/udpflood.aspx

WhatIsMyIP — www.whatismyip.com

Wireshark — www.wireshark.org

Password Cracking

Advanced Archive Password Recovery — www.elcomsoft.com/archpr.html

BIOS passwords — http://labmice.techtarget.com/articles/BIOS_hack.htm

BitLocker security whitepapers — www.principlelogic.com/bitlocker.html

Brutus — www.hoobie.net/brutus

Cain & Abel — www.oxid.it/cain.html

Crack — ftp://coast.cs.purdue.edu/pub/tools/unix/pwdutils/crack

Default vendor passwords — www.cirt.net/passwords

Dictionary files and word lists

- ftp://ftp.cerias.purdue.edu/pub/dict
- http://packetstormsecurity.org/Crackers/wordlists/
- www.outpost9.com/files/WordLists.html

eBlaster and Spector Pro — www.spectorsoft.com

Elcomsoft Distributed Password Recovery — www.elcomsoft.com/edpr.html

Elcomsoft Forensic Disk Decryptor — www.elcomsoft.com/efdd.html

Elcomsoft System Recovery — www.elcomsoft.com/esr.html

Invisible KeyLogger Stealth — www.amecisco.com/iks.htm

John the Ripper — www.openwall.com/john

KeyGhost — www.keyghost.com

LastPass — http://lastpass.com

ophcrack — http://ophcrack.sourceforge.net

Oxygen Forensic Suite — www.oxygen-forensic.com

Pandora — www.nmrc.org/project/pandora

Passware Kit Forensic — www.lostpassword.com/kit-forensic.htm

Password Safe — http://passwordsafe.sourceforge.net

Proactive Password Auditor — www.elcomsoft.com/ppa.html

Proactive System Password Recovery — www.elcomsoft.com/pspr.html

pwdump3 — www.openwall.com/passwords/microsoft-windows-nt-2000-xp-2003-vista-7#pwdump

NetBIOS Auditing Tool — www.securityfocus.com/tools/543

NIST Guide to Enterprise Password Management — http://csrc.nist.gov/publications/drafts/800-118/draft-sp800-118.pdf

NTAccess — www.mirider.com/ntaccess.html

RainbowCrack — http://project-rainbowcrack.com

Rainbow tables — http://rainbowtables.shmoo.com

SQLPing3 — www.sqlsecurity.com/downloads

THC-Hydra — www.thc.org/thc-hydra

WinHex — www.winhex.com

Patch Management

Debian Linux Security Alerts — www.debian.org/security

Ecora Patch Manager — www.ecora.com/ecora/products/patchmanager.asp

GFI LanGuard — http://www.gfi.com/networksecurity-vulnerability-scanner

Kaseya Patch Management — www.kaseya.com/features/patchmanagement.aspx

Lumension Patch and Remediation — www.lumension.com/vulnerability-management/patchmanagement-software.aspx

Microsoft TechNet Security Center — http://technet.microsoft.com/en-us/security/default.aspx

Red Hat Linux Security Alerts — http://updates.redhat.com

Slackware Linux Security Advisories — www.slackware.com/security

SUSE Linux Security Alerts — http://en.opensuse.org/System_Updates

VMware vCenter Protect — www.vmware.com/products/datacenter-virtualization/vcenter-protect/overview.html

Windows Server Update Services from Microsoft — http://technet.microsoft.com/en-us/windowsserver/bb332157.aspx

Security Education and Learning Resources

Kevin Beaver's information security articles, whitepapers, webcasts, podcasts, and screencasts — www.principlelogic.com/resources.html

Kevin Beaver's *Security On Wheels* information security audio programs — http://securityonwheels.com

Kevin Beaver's *Security On Wheels* blog — http://securityonwheels.com/blog

Kevin Beaver's Twitter page — https://twitter.com/kevinbeaver

Security Methods and Models

Open Source Security Testing Methodology Manual — www.isecom.org/research/osstmm.html

OWASP — www.owasp.org

Secur*IT*ree — www.amenaza.com

The Open Group's Risk Taxonomy — www.opengroup.org

Social Engineering

Simple Phishing Toolkit — www.sptoolkit.com

Source Code Analysis

Checkmarx — www.checkmarx.com

Veracode — www.veracode.com

Storage

Effective File Search — www.sowsoft.com/search.htm

FileLocator Pro — www.mythicsoft.com

GFI LanGuard — www.gfi.com/networksecurity-vulnerability-scanner

GrabiQNs — www.isecpartners.com/SecuringStorage/GrabiQNs.zip

Identity Finder — www.identityfinder.com

System Hardening

Bastille Linux Hardening Program — http://bastille-linux.sourceforge.net

Center for Internet Security Benchmarks — www.cisecurity.org

Deep Freeze Enterprise — www.faronics.com/products/deep-freeze/enterprise

Fortres 101 — www.fortresgrand.com

Imperva — www.imperva.com/products/database-firewall.html

Linux Administrator's Security Guide — www.seifried.org/lasg

Microsoft Security Compliance Manager — http://technet.microsoft.com/en-us/library/cc677002.aspx

Pyn Logic — www.pynlogic.com

SecureIIS — www.eeye.com/products/secureiis-web-server-security

ServerDefender — www.port80software.com/products/serverdefender

TrueCrypt — www.truecrypt.org

Symantec PGP — www.symantec.com/products-solutions/families/?fid=encryption

WinMagic — www.winmagic.com

User Awareness and Training

Awareity MOAT — www.awareity.com

Dogwood Management Partners Security Posters — www.securityposters.net

Greenidea Visible Statement — www.greenidea.com

Interpact, Inc. Awareness Resources — www.thesecurityawarenesscompany.com

Managing an Information Security and Privacy Awareness and Training Program by Rebecca Herold (Auerbach) — www.amazon.com/Managing-Information-SecurityAwareness-Training/dp/0849329639

Peter Davis & Associates training services — www.pdaconsulting.com/services.htm

Security Awareness, Inc. — www.securityawareness.com

Voice over IP

Cain & Abel — www.oxid.it/cain.html

CommView — www.tamos.com/products/commview

Listing of various VoIP tools — www.voipsa.org/Resources/tools.php

NIST's SP800-58 document — http://csrc.nist.gov/publications/nistpubs/800-58/SP800-58-final.pdf

OmniPeek — www.wildpackets.com/products/distributed_network_analysis/omnipee

PROTOS — www.ee.oulu.fi/research/ouspg/Protos

sipsak — http://sipsak.org

SiVuS — www.voip-security.net/index.php/component/jdownloads/view.download/30/299

vomit — http://vomit.xtdnet.nl

VoIP Hopper — http://voiphopper.sourceforge.net

Vulnerability Databases

Common Vulnerabilities and Exposures — http://cve.mitre.org

CWE/SANS Top 25 Most Dangerous Programming Errors — www.sans.org/top25-software-errors/

National Vulnerability Database — http://nvd.nist.gov

Privacy Rights Clearinghouse's *A Chronology of Data Breaches* — www.privacyrights.org/data-breach

SANS Top 20 Internet Security Problems, Threats, and Risks — www.sans.org/top20

US-CERT Vulnerability Notes Database — www.kb.cert.org/vuls

Wireless Vulnerabilities and Exploits — www.wve.org

Websites and Applications

Acunetix Web Vulnerability Scanner — www.acunetix.com

Brutus — www.hoobie.net/brutus/index.html

Checkmarx CxDeveloper — www.checkmarx.com

Defaced websites — http://zone-h.org/archive

HTTrack Website Copier — www.httrack.com

Firefox Web Developer — http://chrispederick.com/work/web-developer

Foundstone's Hacme Tools — www.mcafee.com/us/downloads/free-tools/index.aspx

Google Hack Honeypot — http://ghh.sourceforge.net

Google Hacking Database — http://johnny.ihackstuff.com/ghdb

NTOSpider — www.ntobjectives.com

Paros Proxy — www.parosproxy.org

Port 80 Software's ServerMask — www.port80software.com/products/servermask

SiteDigger — www.mcafee.com/us/downloads/free-tools/sitedigger.aspx

SQL Inject Me — https://addons.mozilla.org/en-us/firefox/addon/sql-inject-me

SQL Power Injector — www.sqlpowerinjector.com

SWFScan — http://bit.ly/ShyhVz

THC-Hydra — www.thc.org/thc-hydra

Veracode — www.veracode.com

WebInspect — www.hpenterprisesecurity.com/products/hp-fortify-software-security-center/hp-webinspect

WebGoat — www.owasp.org/index.php/Category:OWASP_WebGoat_Project

WSDigger — www.mcafee.com/us/downloads/free-tools/wsdigger.aspx

WSFuzzer —
www.owasp.org/index.php/Category:OWASP_WSFuzzer_Project

Windows

BitLocker security whitepapers — www.principlelogic.com/bitlocker.html

DumpSec — www.systemtools.com/somarsoft/?somarsoft.com

GFI LanGuard — www.gfi.com/networksecurity-vulnerability-scanner

Microsoft Baseline Security Analyzer — www.microsoft.com/technet/security/tools/mbsahome.mspx

Network Users — www.optimumx.com/download/netusers.zip

Nexpose — www.rapid7.com/vulnerability-scanner.jsp

QualysGuard — www.qualys.com

Sysinternals — http://technet.microsoft.com/en-us/sysinternals/default.aspx

Winfo — www.ntsecurity.nu/toolbox/winfo

Wireless Networks

Aircrack-ng — http://aircrack-ng.org

AirMagnet WiFi Analyzer — www.airmagnet.com/products/wifi_analyzer

Asleap — http://sourceforge.net/projects/asleap

CommView for Wi-Fi — www.tamos.com/products/commwifi

Digital Hotspotter — www.canarywireless.com

Elcomsoft Wireless Security Auditor — www.elcomsoft.com/ewsa.html

Homebrew WiFi antenna — www.turnpoint.net/wireless/has.html

KisMAC — http://trac.kismac-ng.org

Kismet — www.kismetwireless.net

NetStumbler — www.netstumbler.com

OmniPeek — www.wildpackets.com/products/omnipeek_network_analyzer

Reaver — http://code.google.com/p/reaver-wps

Reaver Pro — http://hakshop.myshopify.com/products/reaver-pro

SeattleWireless Hardware Comparison page — www.seattlewireless.net/index.cgi/HardwareComparison

Super Cantenna — www.cantenna.com

Wellenreiter — http://sourceforge.net/projects/wellenreiter

WEPCrack — http://wepcrack.sourceforge.net

WiGLE database of wireless networks — www.wigle.net

WiFinder — www.boingo.com/boingo-apps/boingo-wifinder/pc/

WinAirsnort — http://winairsnort.free.fr