LEARNING MADE EASY

7th Edition

Hacking

for dummies®

A Wiley Brand

Keep your network and information safe

Learn the latest vulnerability and penetration testing techniques

Defend against hackers and rogue insiders

Kevin Beaver, CISSP

Independent Information Security Consultant, Principle Logic, LLC

Hacking

7th Edition

by Kevin Beaver, CISSP

for dummies®
A Wiley Brand

Hacking For Dummies®, 7th Edition

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

Copyright © 2022 by John Wiley & Sons, Inc., Hoboken, New Jersey

Media and software compilation copyright © 2022 by John Wiley & Sons, Inc. All rights reserved.

Published simultaneously in Canada

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 the prior written permission of the Publisher. 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.

Trademarks: Wiley, For Dummies, the Dummies Man logo, Dummies.com, Making Everything Easier, and related trade dress are trademarks or registered trademarks of John Wiley & Sons, Inc. 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.

LIMIT OF LIABILITY/DISCLAIMER OF WARRANTY: WHILE THE PUBLISHER AND AUTHORS HAVE USED THEIR BEST EFFORTS IN PREPARING THIS WORK, THEY 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 ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. NO WARRANTY MAY BE CREATED OR EXTENDED BY SALES REPRESENTATIVES, WRITTEN SALES MATERIALS OR PROMOTIONAL STATEMENTS FOR THIS WORK. THE FACT THAT AN ORGANIZATION, WEBSITE, OR PRODUCT IS REFERRED TO IN THIS WORK AS A CITATION AND/OR POTENTIAL SOURCE OF FURTHER INFORMATION DOES NOT MEAN THAT THE PUBLISHER AND AUTHORS ENDORSE THE INFORMATION OR SERVICES THE ORGANIZATION, WEBSITE, OR PRODUCT MAY PROVIDE OR RECOMMENDATIONS IT MAY MAKE. THIS WORK IS SOLD WITH THE UNDERSTANDING THAT THE PUBLISHER IS NOT ENGAGED IN RENDERING PROFESSIONAL SERVICES. THE ADVICE AND STRATEGIES CONTAINED HEREIN MAY NOT BE SUITABLE FOR YOUR SITUATION. YOU SHOULD CONSULT WITH A SPECIALIST WHERE APPROPRIATE. FURTHER, READERS SHOULD BE AWARE THAT WEBSITES LISTED IN THIS WORK MAY HAVE CHANGED OR DISAPPEARED BETWEEN WHEN THIS WORK WAS WRITTEN AND WHEN IT IS READ. NEITHER THE PUBLISHER NOR AUTHORS SHALL BE LIABLE FOR ANY LOSS OF PROFIT OR ANY OTHER COMMERCIAL DAMAGES, INCLUDING BUT NOT LIMITED TO SPECIAL, INCIDENTAL, CONSEQUENTIAL, OR OTHER DAMAGES.

For general information on our other products and services, 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. For technical support, please visit https://hub.wiley.com/community/support/dummies.

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: 2022933150

ISBN 978-1-119-87219-1 (pbk); ISBN 978-1-119-87220-7 (ebk); ISBN 978-1-119-87221-4 (ebk)

Hacking For Dummies®

To view this book's Cheat Sheet, simply go to www.dummies.com and search for “Hacking For Dummies Cheat Sheet” in the Search box.

Table of Contents

- Cover
- Title Page
- Copyright
- Introduction
  - About This Book
  - Foolish Assumptions
  - Icons Used in This Book
  - Beyond the Book
  - Where to Go from Here
- Part 1: Building the Foundation for Security Testing
  - Chapter 1: Introduction to Vulnerability and Penetration Testing
    - Straightening Out the Terminology
    - Recognizing How Malicious Attackers Beget Ethical Hackers
    - Understanding the Need to Hack Your Own Systems
    - Understanding the Dangers Your Systems Face
    - Following the Security Assessment Principles

Using the Vulnerability and Penetration Testing Process

Chapter 2: Cracking the Hacker Mindset

What You’re Up Against

Who Breaks into Computer Systems

Why They Do It

Planning and Performing Attacks

Maintaining Anonymity

Chapter 3: Developing Your Security Testing Plan

Establishing Your Goals

Determining Which Systems to Test

Creating Testing Standards

Selecting Security Assessment Tools

Chapter 4: Hacking Methodology

Setting the Stage for Testing

Seeing What Others See

Scanning Systems

Determining What’s Running on Open Ports

Assessing Vulnerabilities

Penetrating the System

Part 2: Putting Security Testing in Motion

Chapter 5: Information Gathering

Gathering Public Information

Mapping the Network

Chapter 6: Social Engineering

Introducing Social Engineering

Starting Your Social Engineering Tests

Knowing Why Attackers Use Social Engineering

Understanding the Implications

Performing Social Engineering Attacks

Social Engineering Countermeasures

Chapter 7: Physical Security

Identifying Basic Physical Security Vulnerabilities
Pinpointing Physical Vulnerabilities in Your Office
Chapter 8: Passwords
Understanding Password Vulnerabilities
Cracking Passwords
General Password Cracking Countermeasures
Securing Operating Systems
Part 3: Hacking Network Hosts
Chapter 9: Network Infrastructure Systems
Understanding Network Infrastructure Vulnerabilities
Choosing Tools
Scanning, Poking, and Prodding the Network
Detecting Common Router, Switch, and Firewall Weaknesses
Putting Up General Network Defenses
Chapter 10: Wireless Networks
Understanding the Implications of Wireless Network Vulnerabilities
Choosing Your Tools
Discovering Wireless Networks
Discovering Wireless Network Attacks and Taking Countermeasures
Chapter 11: Mobile Devices
Sizing Up Mobile Vulnerabilities
Cracking Laptop Passwords
Cracking Phones and Tablets
Part 4: Hacking Operating Systems
Chapter 12: Windows
Introducing Windows Vulnerabilities
Choosing Tools
Gathering Information About Your Windows Vulnerabilities
Detecting Null Sessions

Checking Share Permissions
Exploiting Missing Patches
Running Authenticated Scans

Chapter 13: Linux and macOS

Understanding Linux Vulnerabilities
Choosing Tools
Gathering Information About Your System Vulnerabilities
Finding Unneeded and Unsecured Services
Securing the .rhosts and hosts.equiv Files
Assessing the Security of NFS
Checking File Permissions
Finding Buffer Overflow Vulnerabilities
Checking Physical Security
Performing General Security Tests
Patching

Part 5: Hacking Applications

Chapter 14: Communication and Messaging Systems

Introducing Messaging System Vulnerabilities
Recognizing and Countering Email Attacks
Understanding VoIP

Chapter 15: Web Applications and Mobile Apps

Choosing Your Web Security Testing Tools
Seeking Out Web Vulnerabilities
Minimizing Web Security Risks
Uncovering Mobile App Flaws

Chapter 16: Databases and Storage Systems

Diving Into Databases
Following Best Practices for Minimizing Database Security Risks

Opening Up About Storage Systems

Following Best Practices for Minimizing Storage Security Risks

Part 6: Security Testing Aftermath

Chapter 17: Reporting Your Results

Pulling the Results Together

Prioritizing Vulnerabilities

Creating Reports

Chapter 18: Plugging Your Security Holes

Turning Your Reports into Action

Patching for Perfection

Hardening Your Systems

Assessing Your Security Infrastructure

Chapter 19: Managing Security Processes

Automating the Security Assessment Process

Monitoring Malicious Use

Outsourcing Security Assessments

Instilling a Security-Aware Mindset

Keeping Up with Other Security Efforts

Part 7: The Part of Tens

Chapter 20: Ten Tips for Getting Security Buy-In

Cultivate an Ally and a Sponsor

Don’t Be a FUDdy-Duddy

Demonstrate That the Organization Can’t Afford to Be Hacked

Outline the General Benefits of Security Testing

Show How Security Testing Specifically Helps the Organization

Get Involved in the Business

Establish Your Credibility

Speak on Management’s Level

Show Value in Your Efforts

Be Flexible and Adaptable

Chapter 21: Ten Reasons Hacking Is the Only Effective Way to Test

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

IT Governance and Compliance Are More Than High-Level Audits

Vulnerability and Penetration Testing Complements Audits and Security Evaluations

Customers and Partners Will Ask How Secure Your Systems Are

The Law of Averages Works Against Businesses

Security Assessments Improve Understanding of Business Threats

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

In-Depth Testing Brings Out the Worst in Your Systems

Combined Vulnerability and Penetration Testing Is What You Need

Proper Testing Can Uncover Overlooked Weaknesses

Chapter 22: Ten Deadly Mistakes

Not Getting Approval

Assuming That You Can Find All Vulnerabilities

Assuming That You Can Eliminate All Vulnerabilities

Performing Tests Only Once

Thinking That You Know It All

Running Your Tests Without Looking at Things from a Hacker’s Viewpoint

Not Testing the Right Systems

Not Using the Right Tools

Pounding Production Systems at the Wrong Time

Outsourcing Testing and Not Staying Involved

Appendix: Tools and Resources

Bluetooth

Certifications

Databases

Denial of Service (DoS) Protection
Exploits
Firewall Rulebase Analyzers
General Research and OSINT Tools
Hacker and Security Testing Publications
Internet of Things
Keyloggers
Laws and Regulations
Linux
Live Toolkits
Log Analysis
Messaging
Miscellaneous
Mobile
Networks
Password Cracking
Patch Management
Security Education and Learning Resources
Security Frameworks
Security Reports and Statistics
Social Engineering and Phishing
Source Code Analysis
Storage
User Awareness and Training
Voice over Internet Protocol
Vulnerability Databases
Websites and Applications
Windows
Wireless Networks

Index

About the Author

Advertisement Page

Connect with Dummies

End User License Agreement

List of Tables

Chapter 9

TABLE 9-1 Commonly Hacked Ports

Chapter 17

TABLE 17-1 Prioritizing Vulnerabilities

List of Illustrations

Chapter 4

FIGURE 4-1: Netcraft’s web server version utility.

Chapter 6

FIGURE 6-1: Using LUCY to start an email phishing campaign.

FIGURE 6-2: Sample email phishing template options in LUCY.

Chapter 8

FIGURE 8-1: Brute-force password-cracking options in Proactive Password Auditor...

FIGURE 8-2: Output from pwdump3.

FIGURE 8-3: Cracked password file hashes with John the Ripper.

FIGURE 8-4: Using Cain & Abel to capture passwords going across the network.

Chapter 9

FIGURE 9-1: Performing a ping sweep of an entire class C network with Nmap.

FIGURE 9-2: In-depth port-scanning options in NMapWin.

FIGURE 9-3: NetScanTools Pro OS Fingerprinting tool.

FIGURE 9-4: General SNMP information gathered by Getif.

FIGURE 9-5: Management interface user IDs gleaned via Getif’s SNMP browsing fun...

FIGURE 9-6: Information gathered about an email server via Telnet.

FIGURE 9-7: Connecting a network analyzer outside the firewall.

FIGURE 9-8: Omnipeek can help uncover someone running an illicit system, such a...

FIGURE 9-9: CommView’s interface for viewing network statistics

FIGURE 9-10: NetResident can track Internet use and ensure that security polici...

FIGURE 9-11: Selecting your victim hosts for ARP poisoning in Cain & Abel

FIGURE 9-12: ARP poisoning results in Cain & Abel

Chapter 10

FIGURE 10-1: Finding the MAC address of an AP by using arp.

FIGURE 10-2: Searching for your wireless APs by using the WiGLE database.

FIGURE 10-3: NetStumbler displays detailed data on APs.

FIGURE 10-4: A LanGuard scan of a live AP.

FIGURE 10-5: Using airodump to capture WEP initialization vectors.

FIGURE 10-6: Using aircrack to crack WEP.

FIGURE 10-7: Using ElcomSoft Wireless Security Auditor to crack WPA PSKs.

FIGURE 10-8: Using Omnipeek to view encrypted wireless traffic.

FIGURE 10-9: ElcomSoft Wireless Security Auditor’s numerous password cracking o...

FIGURE 10-10: The Reaver Pro startup window.

FIGURE 10-11: Using Reaver Pro to determine that Wi-Fi Protected Setup is enabl...

FIGURE 10-12: NetStumbler showing potentially unauthorized APs.

FIGURE 10-13: You can configure Omnipeek to detect APs that don’t broadcast the...

FIGURE 10-14: CommView for WiFi showing several unauthorized ad-hoc clients.

FIGURE 10-15: Finding an accessible AP via NetStumbler.

FIGURE 10-16: Looking for the MAC address of a wireless client on the network b...

FIGURE 10-17: SMAC showing a spoofed MAC address.

Chapter 11

FIGURE 11-1: ElcomSoft System Recovery is great for cracking and resetting Wind...

FIGURE 11-2: Loading password hashes from a remote SAM database in ophcrack.

FIGURE 11-3: Usernames and hashes extracted via ophcrack.

FIGURE 11-4: Loading the required hash tables in ophcrack.

FIGURE 11-5: iOS Forensic Toolkit's main page.

FIGURE 11-6: Select the appropriate iOS device from the list.

FIGURE 11-7: iOS Forensic Toolkit Ramdisk loading successfully.

FIGURE 11-8: Cracking a four-digit PIN on an iPhone.

Chapter 12

FIGURE 12-1: Port-scanning a Windows 11 system with NetScanTools Pro.

FIGURE 12-2: Gathering SMB versions with NetScanTools SMB Scanner.

FIGURE 12-3: Using Nmap to determine the Windows version.

FIGURE 12-4: Using nbtstat to gather information on a Windows 11 system.

FIGURE 12-5: Using LanGuard to scan your network for Windows shares.

FIGURE 12-6: Mapping a null session to a vulnerable Windows system.

FIGURE 12-7: net view displays drive shares on a remote Windows host.

FIGURE 12-8: Default local security-policy settings in Windows 7 that restrict ...

FIGURE 12-9: SoftPerfect Network Scanner's Share Finder profile seeks out Windo...

FIGURE 12-10: Exploitable vulnerability found by Nexpose.

FIGURE 12-11: The main Metasploit console.

FIGURE 12-12: Metasploit options to obtain a remote command prompt on the targe...

FIGURE 12-13: Remote command prompt on target system obtained by exploiting a m...

FIGURE 12-14: Metasploit Pro's graphical interface provides broad security test...

FIGURE 12-15: Starting the exploit process in Metasploit Pro is as simple as im...

FIGURE 12-16: Testing login credentials before running an authenticated scan wi...

Chapter 13

FIGURE 13-1: Port scanning a Linux host with NetScanTools Pro.

FIGURE 13-2: Using Nexpose to discover vulnerabilities in macOS.

FIGURE 13-3: Using the Test Credentials feature as part of the Nexpose scan con...

FIGURE 13-4: Using Nmap to determine the OS kernel version of a Linux server.

FIGURE 13-5: Using NetScanTools Pro to determine that Slackware Linux is likely...

FIGURE 13-6: Using Nmap to check application versions.

FIGURE 13-7: Viewing the PIDs for running daemons by using ps -aux.

FIGURE 13-8: The rexec file showing the disable option.

FIGURE 13-9: /etc/inittab showing the line that allows a Ctrl+Alt+Delete shutdo...

FIGURE 13-10: Running the Tiger security-auditing tool.

FIGURE 13-11: Partial output of the Tiger tool.

Chapter 14

FIGURE 14-1: Limiting the number of resources that handle inbound messages.

FIGURE 14-2: An SMTP banner showing server-version information.

FIGURE 14-3: An SMTP banner that disguises the version information.

FIGURE 14-4: smtpscan gathers version info even when the SMTP banner is disguis...

FIGURE 14-5: Using VRFY to verify that an email address exists.

FIGURE 14-6: Using EXPN to verify that a mailing list exists.

FIGURE 14-7: Using EmailVerify to verify an email address.

FIGURE 14-8: Using smtp-user-enum to glean email addresses.

FIGURE 14-9: Using NetScanTools Pro SMTP Server Tests to check for an open emai...

FIGURE 14-10: Critical information revealed in email headers.

FIGURE 14-11: Using the EICAR test string to test antimalware software.

FIGURE 14-12: A WebInspect scan of a VoIP network adapter showing several weakn...

FIGURE 14-13: Using Cain & Abel to capture, record, and play back VoIP conversa...

FIGURE 14-14: Connecting to a VoIP phone’s web interface using the default pass...

Chapter 15

FIGURE 15-1: Using HTTrack to crawl a website.

FIGURE 15-2: Using Firefox Web Developer to reset form-field lengths.

FIGURE 15-3: Using WebInspect to find and manipulate hidden fields.

FIGURE 15-4: Netsparker discovered SQL injection vulnerabilities.

FIGURE 15-5: Script code reflected to the browser.

FIGURE 15-6: Using Acunetix Web Vulnerability Scanner to find cross-site script...

FIGURE 15-7: The URL returns an error when an invalid user ID is entered.

FIGURE 15-8: The URL returns a different error when an invalid password is ente...

FIGURE 15-9: The Brutus tool tests for weak web logins.

FIGURE 15-10: A network camera’s login credentials embedded directly in its HTM...

Chapter 16

FIGURE 16-1: SQLPing3 can find SQL Server systems and check for missing sa acco...

FIGURE 16-2: Using Cain & Abel to crack Oracle password hashes.

FIGURE 16-3: Using SoftPerfect Network Scanner to search for network shares.

FIGURE 16-4: Using FileLocator Pro to search for sensitive text on unprotected ...

Introduction

Welcome to *Hacking For Dummies,* 7th Edition. This book outlines — in plain English — computer hacking tricks and techniques that you can use to assess the security of your information systems, find the vulnerabilities that matter, and fix the weaknesses before criminal hackers and malicious insiders take advantage of them. This hacking is the professional, aboveboard, and legal type of security testing — which I refer to as *vulnerability and penetration testing* or *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 and their exploits, including the growing challenges associated with ransomware. The techniques and tools outlined in this book can help.

You could implement all the security technologies and other best practices possible, and your network environment might be secure — *as far as you know*. But unless and until you understand how malicious attackers think, apply that knowledge, and use the right tools to assess your systems from their point of view, it's practically impossible to have a true sense of how secure your systems and information really are.

Ethical hacking (or, more simply, security assessments), which encompasses formal and methodical vulnerability and penetration testing, is necessary to find security flaws and to validate that your information systems are truly secure on an ongoing basis.

Given the COVID-19 situation, ensuring security is especially critical today. With so many people working

from home and outside the traditional enterprise network security controls, hacking and related breaches are off the charts. It's clear that businesses are having to adapt to new ways of working. IT and security professionals are also grappling with the associated emerging technologies, and that's only further complicating security. It's a tricky place to be and not an enviable position. Still, it represents an opportunity for learning and improving, so it's not all bad.

This book will help you successfully navigate the craziness of the world as it relates to IT and security. I'll also help you implement a proper vulnerability and penetration testing program, perform the right security checks, and put the necessary countermeasures in place to keep external hackers and malicious users in check.

About This Book

Hacking For Dummies is a reference guide for hacking your systems to improve security and minimize business risks. The security testing techniques are based on written and unwritten rules of computer system vulnerability and penetration testing and information security best practices. This book covers everything from establishing your testing plan to assessing your systems to plugging the holes and managing an ongoing security testing program.

Realistically, for most networks, operating systems, and applications, thousands of possible vulnerabilities exist. I don't cover them all, but I do cover the big ones on various platforms and systems that I believe contribute to most security problems in business today. I cover basic Pareto principle (80/20 rule) stuff, with the goal of helping you find the 20 percent of the issues that create 80 percent of your security risks. Whether you need to

assess security vulnerabilities on a small home-office network, a medium-size corporate network, or across a large enterprise, *Hacking For Dummies* provides the information you need.

This book includes the following features:

- Various technical and nontechnical tests and their detailed methodologies
- Specific countermeasures to protect against hacking and breaches

Before you start testing your systems, familiarize yourself with the information in Part 1 so that you're prepared for the tasks at hand. The adage "If you fail to plan, you plan to fail" rings true for the security assessment process. You must have a solid game plan in place if you're going to be successful.

Foolish Assumptions

Disclaimer: This book is intended solely for information technology (IT) and information security professionals to test the security of their (or their clients') systems in an authorized fashion. 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.

Okay, now that that's out of the way, let's get to the good stuff! This book is for you if you're a network administrator, IT or information security manager, security consultant, security auditor, compliance

manager, or otherwise interested in finding out more about evaluating computer systems, software, and IT operations for security flaws and, of course, making long-term improvements.

I also make a few assumptions about you, the aspiring information technology (IT) or security professional:

- You're familiar with basic computer, network, and information security concepts and terms.
- You have access to a computer and a network on which to use these techniques and tools.
- You have the go-ahead from your employer or your client to perform the hacking techniques described in this book.

Icons Used in This Book

Throughout this book, you'll see the following icons in the margins.

REMEMBER This icon points out information that's worth committing to memory.

WARNING This icon points out information that could have a negative effect on your vulnerability and penetration testing efforts — so please read it!

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

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

Beyond the Book

First off, be sure to check out the Cheat Sheet associated with this book. You can access the Cheat Sheet by visiting dummies.com and searching for *Hacking For Dummies*. The Cheat Sheet is a great way to get you pointed in the right direction or get you back on track with your security testing program if needed.

Also, be sure to check out my website www.principlelogic.com, especially the Resources page.

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 and network systems. This book provides the foundation you need to develop and maintain a successful security assessment and vulnerability management program to minimize business risks.

Depending on your computer and network configurations, you may be able to skip certain 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, waiting to be exploited.

Keep in mind that the high-level concepts of security testing won't change as often as the specific vulnerabilities you protect against. Vulnerability and penetration testing 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 day after day and month after month. The good news is the vulnerabilities are often very predictable and, therefore, easy to discover and resolve.

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

Part 1

Building the Foundation for Security Testing

IN THIS PART ...

Discover the basics of vulnerability and penetration testing.

Get a look inside a hacker’s head to understand why and how they do what they do.

Develop a security testing plan.

Understand the methodology for finding the most (and best) vulnerabilities.

Chapter 1

Introduction to Vulnerability and Penetration Testing

IN THIS CHAPTER

- **» Understanding hackers' and malicious users' objectives**
- **» Examining how the security testing process came about**
- **» Recognizing what endangers your computer systems**
- **» Starting to use the process for security testing**

This book is about testing your computers and networks for security vulnerabilities and plugging the holes you find before the bad guys get a chance to exploit them.

Straightening Out the Terminology

Everyone has heard of hackers and malicious users. Many people have even suffered the consequences of their criminal actions. Who are these people, and why do you need to know about them? The next few sections give you the lowdown on these attackers.

REMEMBER In this book, I use the following terminology:

- **Hackers** (or *external attackers)* try to compromise computers, sensitive information, and even entire networks for ill-gotten gains — usually from the outside — as unauthorized users. Hackers go for almost any system they think they can compromise. Some prefer prestigious, well-protected systems, but hacking into anyone's system increases an attacker's status in hacker circles.
- **Malicious users** (*external* or *internal attackers, often called black-hat hackers)* try to compromise computers and sensitive information from the outside (such as customers or business partners) or the inside as authorized and trusted users. Malicious users go for systems that they believe they can compromise for ill-gotten gains or revenge, because they may have access or knowledge of a system that gives them a leg up.

  Malicious attackers are, generally speaking, both hackers and malicious users. For the sake of simplicity, I refer to both as *hackers* and specify *hacker* or *malicious user* only when I need to differentiate and drill down further into their unique tools, techniques, and ways of thinking.
- **Ethical hackers** (or *good guys),* often referred to as white-hat hackers or penetration testers, hack systems to discover vulnerabilities to protect against unauthorized access, abuse, and misuse. Information security researchers, consultants, and internal staff fall into this category.

Hacker

Hacker has two meanings:

- Traditionally, hackers like to tinker with software or electronic systems. Hackers enjoy exploring and learning how computer systems operate. They love discovering new ways to work — both mechanically and electronically.
- Over the years, *hacker* has taken on a new meaning: someone who maliciously breaks into systems for personal gain. Technically, these criminals are *crackers* (criminal hackers). These "crackers" break into — or crack — systems with malicious intent. They seek fame, intellectual property, profit, or even revenge. They modify, delete, and steal critical information, and they spread ransomware and take entire networks offline, often bringing large corporations and government agencies to their knees.

  

  WARNING Don't get me started on how pop culture and the media have hijacked the word *hack*, from *life hacking* to so-called election meddling. Marketers, politicians, and media strategists know that the average person doesn't understand the term *hacking,* so many of them use it however they desire to achieve their goals. Don't be distracted.

The good-guy *(white-hat)* hackers don't like being lumped in the same category as the bad-guy *(black-hat)* hackers. (In case you're curious, the *white hat* and *black hat* come from old Western TV shows in which the good guys wore white cowboy hats and the bad guys wore black cowboy hats.) *Gray-hat* hackers are a bit of both.

Whatever the case, the word *hacker* often has a negative connotation.

Many malicious hackers claim that they don't cause damage but help others for the greater good of society. Yeah, whatever. Malicious hackers are electronic miscreants and deserve the consequences of their actions.

Be careful not to confuse criminal hackers with security researchers. Researchers not only hack aboveboard and develop the amazing tools that we get to use in our work, but they also (usually) take responsible steps to disclose their findings and publish their code. Unfortunately, there is a war going on against legitimate information security research, and the tools and techniques are often questioned by government agencies. Some people are even forced to remove these tools from their websites.

Malicious user

A malicious user — meaning a rogue employee, contractor, intern, or other user who abuses their trusted privileges — is a common term in security circles and in headlines about information breaches. The issue isn't necessarily users hacking internal systems but users who abuse the computer access privileges they've been given. Users ferret through critical database systems to glean sensitive information, email confidential client information to the competition or elsewhere to the cloud to save for later, or delete sensitive files from servers that they probably didn't need to have access to in the first place.

Sometimes, an innocent (or ignorant) insider whose intent isn't malicious still causes security problems by moving, deleting, or corrupting sensitive information. Even an innocent fat finger on the keyboard can have

dire consequences in the business world. Think about all the ransomware infections affecting businesses around the world. All it takes is one click by a careless user for your entire network to be affected.

Malicious users are often the worst enemies of IT and information security professionals because they know exactly where to go to get the goods and don’t need to be computer-savvy to compromise sensitive information. These users have the access they need, and management trusts them — often without question.

Recognizing How Malicious Attackers Beget Ethical Hackers

You need protection from hacker shenanigans. Along the lines of what my father taught me about being smarter than the machine you’re working on, you have to become as savvy as the guys who are trying to attack your systems. A true IT or security professional possesses the skills, mindset, and tools of a hacker but is trustworthy. They perform hacks as security tests against systems based on how hackers think and work and make tireless efforts to protect the organizations’ network and information assets.