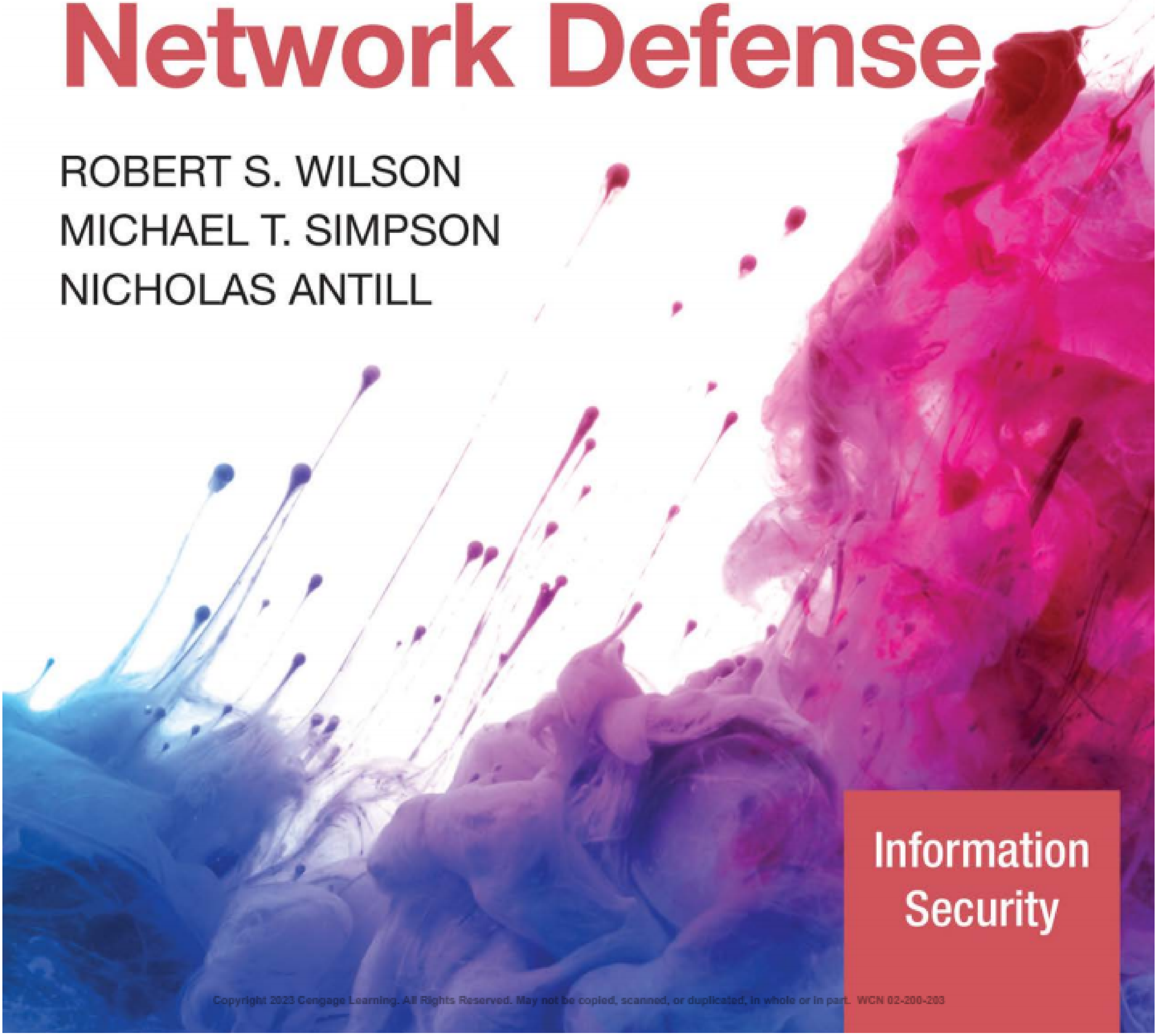
Cengage

Fourth Edition

Hands-On Ethical Hacking & Network Defense

ROBERT S. WILSON
MICHAEL T. SIMPSON
NICHOLAS ANTILL



Information Security

Fourth Edition

Hands-On Ethical Hacking and Network Defense

MICHAEL T. SIMPSON
NICHOLAS D. ANTILL
ROBERT S. WILSON

Cengage

Australia • Brazil • Canada • Mexico • Singapore • United Kingdom • United States

This is an electronic version of the print textbook. Due to electronic rights restrictions, some third party content may be suppressed. Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. The publisher reserves the right to remove content from this title at any time if subsequent rights restrictions require it. For valuable information on pricing, previous editions, changes to current editions, and alternate formats, please visit www.cengage.com/highered to search by ISBN#, author, title, or keyword for materials in your areas of interest.

Important Notice: Media content referenced within the product description or the product text may not be available in the eBook version.

Cengage

Hands-On Ethical Hacking and Network Defense, Fourth Edition

Michael T. Simpson, Nicholas D. Antill, and Robert S. Wilson

SVP, Higher Education Product Management: Erin Joyner

VP, Product Management, Learning Experiences: Thais Alencar

Product Director: Mark Santee

Product Manager: Natalie Onderdonk

Product Assistant: Ethan Wheel

Learning Designer: Natalie Onderdonk

Content Manager: Michele Stulga

Digital Delivery Quality Partner: Jim Vaughey

Technical Editor: Danielle Shaw

Developmental Editor: Lisa Ruffolo

VP, Product Marketing: Jason Sakos

Director, Product Marketing: Danaë April

Portfolio Marketing Manager: Mackenzie Paine

IP Analyst: Ann Hoffman

IP Project Manager: Ilakkiya Jayagopi, Lumina Datamatics

Production Service: Straive

Sr Designer: Erin Griffin

Cover Image Source: Rudchenko Liliia/Shutterstock.com

For product information and technology assistance, contact us at
Cengage Customer & Sales Support, 1-800-354-9706
or support.cengage.com.

For permission to use material from this text or product, submit all requests online at **www.copyright.com.**

Library of Congress Control Number: 2022930454

ISBN: 978-0-357-50975-3

Loose-leaf Edition:
ISBN: 978-0-357-50976-0

Cengage
200 Pier 4 Boulevard
Boston, MA 02210
USA

Cengage is a leading provider of customized learning solutions with employees residing in nearly 40 different countries and sales in more than 125 countries around the world. Find your local representative at **www.cengage.com**

To learn more about Cengage platforms and services, register or access your online learning solution, or purchase materials for your course, visit **www.cengage.com.**

Notice to the Reader

Publisher does not warrant or guarantee any of the products described herein or perform any independent analysis in connection with any of the product information contained herein. Publisher does not assume, and expressly disclaims, any obligation to obtain and include information other than that provided to it by the manufacturer. The reader is expressly warned to consider and adopt all safety precautions that might be indicated by the activities described herein and to avoid all potential hazards. By following the instructions contained herein, the reader willingly assumes all risks in connection with such instructions. The publisher makes no representations or warranties of any kind, including but not limited to, the warranties of fitness for particular purpose or merchantability, nor are any such representations implied with respect to the material set forth herein, and the publisher takes no responsibility with respect to such material. The publisher shall not be liable for any special, consequential, or exemplary damages resulting, in whole or part, from the readers' use of, or reliance upon, this material.

Printed in the United States of America
Print Number: 01 Print Year: 2022

BRIEF CONTENTS

TABLE OF CONTENTS

MODULE 5

MODULE 6

MODULE 7

MODULE 8

MODULE 9

MODULE 10

MODULE 11

MODULE 12

MODULE 13

MODULE 14

APPENDIX A

APPENDIX B

INTRODUCTION

The need for security professionals who understand how attackers compromise networks is growing each day. You can't read the news without seeing an article on ransomware or personal information being stolen from unprotected databases. Since the first edition of *Hands-On Ethical Hacking and Network Defense* was published, the United States has created an organization with the sole purpose of countering cyber threats and attacks. Both public and private companies rely on skilled professionals to conduct test attacks on their networks as a way to discover vulnerabilities before attackers do. "Ethical hacker" is one term used to describe these professionals; others are "security tester" or "penetration tester."

This course isn't intended to provide comprehensive training in security testing or penetration testing. It does, however, introduce security testing to those who are new to the field. This course is intended for novices who have a thorough grounding in computer and networking basics but want to learn how to protect networks by using an attacker's knowledge to compromise network security. By understanding what tools and methods a hacker uses to break into a network, security testers can protect systems from these attacks.

The purpose of this course is to guide you toward becoming a skilled security tester. This profession requires creativity and critical thinking, which are sometimes difficult skills to learn in an academic environment. However, with an open mind and a willingness to learn, you can think outside the box and learn to ask more questions than this course or your instructor poses. Being able to dig past the surface to solve a problem takes patience and the willingness to admit that sometimes there's no simple answer.

Conducting a security test involves more than running exploits against a system and informing your client of existing vulnerabilities. Isn't it possible that you neglected to test for some areas that might be vulnerable to attacks? Haphazard approaches undermine the security profession and expose companies to theft. The goal of this course is to offer a more structured approach to conducting a security test and to introduce novices to professional certifications available in this growing field.

INTENDED AUDIENCE

Although people with a wide range of backgrounds can take this course, it's intended for those with a Security+ and Network+ certification or equivalent. A networking background is necessary so that you understand how computers operate in a networked environment and can work with a network administrator when needed. In addition, readers must know how to use a computer from the command line and how to use popular operating systems, such as Windows and Kali Linux.

This course can be used at any educational level, from technical high schools and community colleges to graduate students. Current professionals in the public and private sectors can also use this course.

NEW TO THIS EDITION

This fourth edition of *Hands-On Ethical Hacking and Network Defense* includes:

- Updated discussions and examples of new hacking tools
- Updated discussion of recent vulnerabilities and exploits
- Updated Internet of Things (IoT) security section and updated discussion of embedded devices
- Updated section regarding web application hacking, security, and web-hacking tools
- Additional in-depth review questions that require research and reporting on key security topics
- A new **Final Project** module where you create a penetration testing report by testing a lab of virtual machines for vulnerabilities using some of the tools and methodologies discussed in the course

MODULE DESCRIPTIONS

Following is a summary of the topics covered in each module of this course:

- **Module 1,** "Ethical Hacking Overview," defines what an ethical hacker can and can't do legally. This module also describes the roles of security and penetration testers and reviews certifications that are current at the time of publication.
- **Module 2,** "TCP/IP Concepts Review," describes the layers of the TCP/IP protocol stack and important ports and reviews IP addressing along with binary, octal, and hexadecimal numbering systems.
- **Module 3,** "Network and Computer Attacks," defines types of malicious software, explains methods for protecting against malware attacks, and discusses types of network attacks and physical security.
- **Module 4,** "Footprinting and Social Engineering," explores using web tools for footprinting and methods of gathering competitive intelligence. It also describes DNS zone transfers and social engineering methods.
- **Module 5,** "Port Scanning," explains the types of port scans and describes how to use port-scanning tools, how to conduct ping sweeps, and how to use shell scripting to automate security tasks.
- **Module 6,** "Enumeration," describes steps and tools for enumerating operating systems, such as Windows and UNIX/Linux.
- **Module 7,** "Programming for Security Professionals," gives you an overview of programming concepts as they relate to network and computer security.
- **Module 8,** "Desktop and Server OS Vulnerabilities," discusses vulnerabilities in Windows and Linux and explains best practices for hardening computers and servers running these operating systems.
- **Module 9,** "Embedded Operating Systems: The Hidden Threat," explains what embedded operating systems are and where they're used and describes known vulnerabilities and best practices for protecting embedded operating systems.
- **Module 10,** "Hacking Web Servers," explains web applications and their vulnerabilities and describes the tools used to attack web servers.
- **Module 11,** "Hacking Wireless Networks," gives you an overview of wireless technology and IEEE wireless standards. This module also covers wireless authentication, wardriving, and wireless hacking tools and countermeasures.
- **Module 12,** "Cryptography," summarizes the history and principles of cryptography, explains encryption algorithms and public key infrastructure components, and offers examples of different attacks on cryptosystems.
- **Module 13,** "Network Protection Systems," covers a variety of devices used to protect networks, such as routers, firewalls, and intrusion detection and prevention systems.
- **Module 14,** "Hands-On Ethical Hacking Final Project," guides you through the process of creating a penetration testing report document by using some of the tools and methodologies discussed in the course to test a lab of virtual machines for vulnerabilities.

- **Appendix A,** "Legal Resources," lists state laws affecting network security and provides applicable excerpts from the Computer Fraud and Abuse Act.
- **Appendix B,** "Resources," lists additional reference books and important URLs referenced throughout the modules.

FEATURES

To help you understand computer and network security, this course includes many features designed to enhance your learning experience:

- *Module objectives*—Each module begins with a detailed list of the concepts to master. This list gives you a quick reference to the module's contents and serves as a useful study aid.
- *Figures and tables*—Numerous screenshots show you how to use security tools, including command-line tools, and how to create programs. In addition, a variety of diagrams aid you in visualizing important concepts. Tables present information in an organized, easy-to-grasp manner.
- *Hands-on activities*—One of the best ways to reinforce learning about network security and security testing is to practice using the many tools security testers use. Hands-on activities are interspersed throughout each module to give you practice in applying what you have learned.
- *Notes*—Notes draw your attention to helpful material related to the subject being covered. In addition, notes with the title "Security Bytes" offer real-world examples related to security topics in each module.
- *Tips*—Tips offer extra information on resources and how to solve problems.
- *Caution*—Caution icons warn you about potential mistakes or problems and explain how to avoid them.
- *Module summary*—Each module ends with a summary of the concepts introduced in the module. These summaries are a helpful way to review the material covered in each module.
- *Key terms*—All terms in the module introduced with bold text are gathered together in the key terms list at the end of the module. This useful reference encourages a more thorough understanding of the module's key concepts. A full definition of each key term is provided in the Glossary.
- *Review questions*—The end-of-module assessment begins with review questions that reinforce the main concepts and techniques covered in each module. Answering these questions helps ensure that you have mastered important topics.
- *Case projects*—Each module closes with one or more case projects that help you evaluate and apply the material you have learned. To complete these projects, you must draw on real-world common sense as well as your knowledge of the technical topics covered to that point in the course. Your goal for each project is to come up with answers to problems similar to those you'll face as a working security tester. To help you with this goal, many case projects are based on a hypothetical company typical of companies hiring security consultants.

MINDTAP

MindTap for *Hands-On Ethical Hacking and Network Defense* is an online learning solution designed to help you master the skills needed in today's workforce. Research shows employers need critical thinkers, troubleshooters, and creative problem-solvers to stay relevant in our fast-paced, technology-driven world. MindTap helps you achieve this with assignments and activities that provide hands-on practice, real-life relevance, and mastery of difficult concepts. Students are guided through assignments that progress from basic knowledge and understanding to more challenging problems. MindTap activities and assignments are tied to learning objectives. MindTap features include the following:

- ***Live Virtual Machine labs*** allow you to practice, explore, and try different solutions in a safe sandbox environment. Each module provides you with an opportunity to complete an in-depth project hosted in a live virtual machine environment. You implement the skills and knowledge gained in the module through real design and configuration scenarios in a private cloud created with OpenStack.
- ***The Adaptive Test Prep (ATP)*** app is designed to help you quickly review and assess your understanding of key IT concepts. Test yourself multiple times to track your progress and improvement by filtering results by correct answers, by all questions answered, or only by incorrect answers to show where additional study help is needed.
- ***Security for Life*** assignments encourage you to stay current with what's happening in the IT field.
- ***Pre- and Post-Quizzes*** assess your understanding of key concepts at the beginning and end of the course.
- ***Reflection*** activities encourage classroom and online discussion of key issues covered in the modules.

Instructors, MindTap is designed around learning objectives and provides analytics and reporting so you can easily see where the class stands in terms of progress, engagement, and completion rates. Use the content and learning path as is or pick and choose how your materials will integrate with the learning path. You control what the students see and when they see it. Visit https://www.cengage.com/mindtap/ to learn more.

INSTRUCTOR RESOURCES

Instructors, please visit cengage.com and sign in to access instructor-specific resources, which include the instructor manual, solutions manual, PowerPoint presentations, and figure files.

- **Instructor manual.** The instructor manual that accompanies this course provides additional instructional material to assist in class preparation, including suggestions for classroom activities, discussion topics, and additional projects.
- **Solutions and Answer Guide.** Answers to the review questions, scenario-based practice questions, performance-based questions, case projects, and reflection activities are provided.
- **PowerPoint presentations.** This course comes with Microsoft PowerPoint slides for each module. These are included as a teaching aid for classroom presentation, to make available to students on the network for module review, or to be printed for classroom distribution. Instructors, please feel at liberty to add your own slides for additional topics you introduce to the class.
- **Figure files.** All of the figures in the course are reproduced on the Instructor Resource Site. Similar to the PowerPoint presentations, these are included as a teaching aid for classroom presentation, to make available to students for review, or to be printed for classroom distribution.

LAB REQUIREMENTS

The hands-on activities in this course help you apply what you have learned about conducting security or penetration tests. The following are the minimum system requirements for completing all activities:

- Computers that boot to Windows 10 or later.
- Access to the Internet, with each computer configured to receive IP configuration information from a router running DHCP
- Kali Linux for hands-on activities. This could be a live bootable version of Kali Linux on a USB, a Kali Linux Virtual Machine, or a computer with a full Kali Linux operating system installation.

Operating Systems and Hardware

The Windows activities in this course were designed for Windows 10 but should also run on Windows 11. Computers should meet the following minimum requirements:

- If you plan to run Kali Linux from a USB flash drive, you need a PC with BIOS that supports booting from a USB drive and an 8 GB USB flash drive with a minimum 15 MB/second read and write speed
- Video card with 512 MB video RAM
- 80 GB hard drive
- 1.5 GHz 32-bit or 64-bit processor
- 8 GB system RAM
- Wireless card for some optional wireless activities
- Mouse or another pointing device and a keyboard

Security-Testing Tools

This course includes hands-on activities that involve using many security tools. You can download these tools as freeware, shareware, or free home and educational versions. Because website addresses change frequently, use a search engine to find tools if the URL listed in an activity is no longer valid.

In addition, you use Microsoft Office Word (or other word-processing software) and need to have email software installed on your computer.

ABOUT THE AUTHORS

Michael T. Simpson is president/senior consultant of MTS Consulting, Inc., specializing in network security and network design. Mike's certifications include CEH, CISSP, Security+, OSSTMM Professional Security Tester (OPST), OSSTMM Professional Security Analyst (OPSA), MCSE, MCDBA, MCSD, MCT, and OCP. He has authored or co-authored eight books and has more than 30 years of industry experience, including 20 years with the Department of Defense (DoD), where he designed and configured computer networks and served as an Oracle database administrator, UNIX administrator, and information systems security officer (ISSO).

Nicholas D. Antill is a seasoned information security professional with over 10 years of specialized cybersecurity experience. Nicholas specializes in penetration testing, proactive security controls, and network defense. He holds many industry certifications, including the OSCP, GWAPT, GPEN, GCIH, CISA, CISSP, and GCFE. Nicholas currently manages the ethical hacking program at a large U.S. financial institution. He started his career at a small grocery chain in Pittsburgh, Pennsylvania, where he developed a fascination with network attack and defense techniques. He worked in support of both the U.S. Department of Justice and the U.S. Department of Defense before returning to the private sector.

Robert S. Wilson is the Cybersecurity Curriculum Coordinator and a cybersecurity instructor for Willis College (Canada's oldest career college). Rob created Willis College's Software Development and Cybersecurity Analyst (CSA) programs. Willis College's CSA program is currently being used by the Canadian military to train cyber operator recruits. Rob has a Computer Science degree from the University of Waterloo, holds numerous certifications from CompTIA, Microsoft, and Cisco, and has over 40 years of experience in the computing field. Rob has expertise in many areas including real-time programming and embedded systems development (having worked for a company that has software on Mars), database development and administration, network and domain administration, penetration testing, and cybersecurity.

ACKNOWLEDGMENTS

Creating the fourth edition of *Hands-On Ethical Hacking and Network Defense* was a group effort. I couldn't have completed my contributions without the invaluable assistance of the following people.

First, I would like to thank Sam Mozner, Senior National Account Manager from Cengage Canada. Who knew that a simple query to Sam about the availability of Cengage content would lead to me creating Cengage content? I wouldn't have had the opportunity to pen the fourth edition of this book if Sam hadn't suggested me as an author to his coworkers. Writing this book has been immensely exciting and satisfying. I look forward to the next book.

Second, I would like to thank all my students past and present. It's true that I gave a lot of myself in the classroom to guide you in your education and help you achieve your next career, but many of you have also given back to me. Those of you that I have kept in touch with and continued to mentor in your careers have provided me with invaluable insight into the real-world happenings in our field. Thank you for keeping me connected and current.

Next, I would like to thank the team from Cengage that worked with me and guided me throughout this edition of the book. Michele Stulga, Cengage Content Manager: Thank you, Michele, for guiding and coordinating this ship and keeping it on course, and for keeping me, the captain of the ship, aware of objects on the horizon. Lisa Ruffolo, my editor: Thank you, Lisa, for making me seem smarter. Your skill in the English language is unmatched and I hope you will be my editor on my next project so that I continue to seem smarter. Danielle Klahr, former Associate Product Manager and now Product Marketing Manager: Thank you, Danielle, for helping me learn the ways of Cengage authorship and for continuing to support me even after moving into your marketing position. Natalie Onderdonk, Learning Designer and now Product Manager: Natalie, I appreciate your expertise in designing learning content and how you passed that knowledge on to me. I look forward to your guidance as Product Manager for my next book.

Thank you to the copyeditors who used their observational skills to point out errors, omissions, and anomalies in each module before it was committed to print. I am very impressed with your abilities to find needles in haystacks.

Thank you to the many reviewers who read each module of the book and provided valuable feedback. Your suggestions greatly improved each module. Your time and efforts were truly appreciated.

Thank you to reviewers Shawn Brown, Elizabethtown Community and Technical College; Jenelle Davis, Colorado Christian University; Mike Saylor, Collin College; and Ping Wang, Robert Morris University.

And finally, thank you to the previous authors upon whose shoulders I stood to complete this fourth edition, Michael T. Simpson and Nicholas D. Antill. Thank you, gentlemen, for going before me and blazing the trail.

DEDICATION

This book is dedicated to my grandson, Harrison Begrande. Some of my fondest memories are of Harrison and me sitting in the shower of the lawn sprinkler on hot summer days, playing with cars, Legos, and action figures. If I could freeze a moment in time and live in it forever, I would choose one of those moments. In my lifetime the growth of technology has been astounding. I wonder what new technological marvels will be created in Harry's lifetime?

KALI LINUX

Kali Linux is used throughout this course for many of the hands-on activities. To run Kali Linux, you have the following options:

- Install Kali Linux as a virtual machine with free virtualization software, such as VMware Server or VirtualBox. The advantage of using a virtual machine is that it enables you to run Kali and Windows at the same time.
- Install Kali Linux on a USB flash drive with at least 8 GB storage capacity. With this method, you can move your personalized Linux system and run it on any system. You can also save files and reports on this drive.

- Install Kali Linux in a dual-boot arrangement with Windows. Dual-boot installations can vary depending on the hardware and require some complex steps if BitLocker or other disk encryption is used. Dual-boot installation isn't explained in this course, but you can find plenty of information online.
- Install Kali Linux directly on computer hardware as the only operating system. If you do this, make sure not to overwrite any existing operating system.

CREATING A BOOTABLE USB FLASH DRIVE

To install Kali Linux on a USB flash drive, you need a drive with a capacity of at least 8 GB. Note that the speed of some flash drives isn't adequate for running a live Linux OS. Performance improvements can be substantial if you use a flash drive with faster read and write speeds. For the best results, a flash drive with a minimum of 15 MB/second read and write speed is recommended. You can check websites, such as https://usb.userbenchmark.com, for performance benchmarks to help you choose a suitable drive within your budget.

After you find the proper flash drive, you'll find up-to-date USB installation instructions on the Kali Linux website (https://www.kali.org/docs/usb/). The website provides installation instructions for those using Windows, Linux, or macOS. These instructions walk you through downloading Kali Linux to booting into Kali Linux for the first time. You must make sure your Kali Linux software is up to date, so run the `apt-get update` and `apt-get upgrade` commands, which check the Kali Linux repositories for updates.

INSTALLING NEW SOFTWARE

Because Kali is a Debian-based Linux distribution, thousands of free programs are available that you can download and install with just a few commands. These programs, which are specific to an OS version, are stored on Internet archives called repositories. To install new software, you can use the command `apt-get install` *`packagename`* (replacing *`packagename`* with the name of the software package you want to install). If you don't know the software package name, use a search engine to look it up.

COMMUNITY SUPPORT FOR KALI LINUX

To find the most recent Kali Linux updates and online forums for help in solving problems, visit www.kali.org. This website is a good place to start if you want to learn more about Kali Linux.

Testing Methodology Manual, "[Security testing] relies on a combination of creativeness, expansion [of] knowledge bases of best practices, legal issues, and client industry regulations as well as known threats and the breadth of the target organization's security presence (or point of risk)."

These are only some of the issues security testers must examine. In doing so, they alert companies to areas that need to be monitored or secured. As a security tester, you can't make a network impenetrable. The only way to do that with certainty is to unplug the network cable. When you discover vulnerabilities ("holes") in a network, you can correct them. This process might entail tasks such as updating an operating system (OS), eliminating unnecessary applications or services, or installing a vendor's latest security patch.

If your job is a penetration tester, you simply report your findings to the company. It's up to the company to make the final decision on how to use the information you have supplied. However, as a security tester, you might also be required to offer solutions for securing or protecting the network. The modules in this course are written with the assumption that you're working toward becoming a network security professional in charge of protecting a corporate network, so the emphasis is on using a security tester's skills to secure or protect a network.

In this course, you learn how to find vulnerabilities in a network and correct them. A security tester's job is to document all vulnerabilities and alert management and information technology (IT) staff of areas that need special attention.

The Role of Security and Penetration Testers

A **hacker** accesses a computer system or network without the authorization of the systems owner. By doing so, a hacker is breaking the law and can go to prison. Those who break into systems to steal or destroy data are often referred to as **crackers**; hackers might only want to prove how vulnerable a system is by accessing the computer or network without destroying any data. For the purpose of this course, no distinction is made between the terms "hackers" and "crackers." The U.S. Department of Justice labels all illegal access to computer or network systems as "hacking," and this course follows that usage.

An ethical hacker is a person who performs most of the same activities a hacker does but with the permission of the owner or company. This distinction is important and can mean the difference between being charged with a crime and not being charged. Ethical hackers are usually contracted to perform penetration tests or security tests. Companies realize that intruders might attempt to access their network resources and are willing to pay for someone to discover these vulnerabilities first. Companies would rather pay a "good hacker" to discover problems in their current network configuration than have a "bad hacker" discover these vulnerabilities. Bad hackers spend many hours scanning systems over the Internet, looking for openings or vulnerable systems.

Some hackers are skillful computer experts, but others are younger, inexperienced people who experienced hackers refer to as **script kiddies** or **packet monkeys**. These derogatory terms refer to people who copy code or use tools created by knowledgeable programmers without understanding how they work. Many experienced penetration testers can write programs or scripts in Python, Ruby, Perl, or C to carry out attacks. (A script is a set of instructions that runs in sequence to perform tasks on a computer system.) You have a chance to write a script in one of these languages in a later module.

A person who hacks computer systems for political or social reasons is called a **hacktivist**. For several years, the hacktivist group known as Anonymous wreaked havoc on federal government computer systems as well as those in the private sector. The group once threatened to release the names of Ku Klux Klan (KKK) members after hacking the organization's Twitter account. This type of hacking is called "hacktivism."

Nation-states are now engaging in cyber hacking attacks with greater frequency and sophistication. The infamous SolarWinds supply chain attack that compromised government agencies and even cybersecurity companies was a nation-state cyber attack perpetrated by Russia.

An Internet search on IT job recruiter sites for "penetration tester" produces hundreds of job announcements, many from Fortune 500 companies looking for experienced applicants. A typical ad might include the following requirements:

- Perform vulnerability, attack, and penetration assessments in Internet, intranet, and wireless environments.
- Perform discovery and scanning for open ports and services.
- Apply appropriate exploits to gain access and expand access as necessary.
- Participate in activities involving application penetration testing and application source code review.
- Interact with the client as required throughout the engagement.
- Produce reports documenting discoveries during the engagement.
- Debrief with the client at the conclusion of each engagement.

- Participate in research and provide recommendations for continuous improvement.
- Participate in knowledge sharing.
- Demonstrate a good understanding of current country, state, and city cyber laws.

Penetration testers and security testers usually have a laptop computer configured with multiple OSs and hacking tools. This course uses Windows, Kali Linux, and other Linux tools needed to conduct actual network and web application attacks. Learning how to install an OS isn't covered in this book, but you can find resources on this topic easily. The most recent versions of Kali Linux can be found at www.kali.org. The procedure for installing security tools varies, depending on the tool and the OS.

Activity 1-1: Determining the Corporate Need for IT Security Professionals

Time Required: 10 minutes

Objective: Examine corporations looking to employ IT security professionals.

Description: Many companies are eager to employ or contract security testers for their corporate networks. In this activity, you search the Internet for job postings, using the keywords "IT Security," and read some job descriptions to determine the IT skills (as well as any non-IT skills) most companies want an applicant to possess.

1. Start your web browser, and go to **indeed.com**.
2. In the What search box, type **IT Security**. In the Where search box, enter the name of a major city near you, and then press **Enter**.
3. Note the number of jobs. Select three to five job postings, and read the job description in each posting.
4. When you're finished, exit your web browser.

SECURITY BYTES

The urgent cybersecurity needs of organizations has created a labor shortage for qualified security professionals. In response, a company called Synack developed a "crowdsourced" model to provide ethical hacking services. Synack created a software platform that offers automated ways for companies to discover security flaws; then it turns those vulnerabilities over to penetration testers—basically, ethical hackers who use their skills for good. These ethical hackers are freelancers hired online on a job-by-job basis. If you choose to become an ethical hacker, you will find many employment opportunities and enjoy long-term job security.[1]

Penetration-Testing Methodologies

Ethical hackers who perform penetration tests use one of these models:

- White box model
- Black box model
- Gray box model

In the **white box model**, the tester is told what network topology and technology the company is using and is given permission to interview IT personnel and company employees. For example, the company might print a network diagram showing all the company's routers, switches, firewalls, and intrusion detection systems (IDSs; see Figure 1-1) or give the tester a floor plan detailing the location of computer systems and the OSs running on these systems (see Figure 1-2).

This background information makes the penetration tester's job easier than it is with using the black box model. In the **black box model**, management doesn't divulge to staff that penetration testing is being conducted, nor does it give the tester any diagrams or describe what technologies the company is using. This model puts the burden on the tester to find this information by using techniques you learn throughout this course. This model also helps management see whether the company's security personnel can detect an attack.

- Participate in research and provide recommendations for continuous improvement.
- Participate in knowledge sharing.
- Demonstrate a good understanding of current country, state, and city cyber laws.

Penetration testers and security testers usually have a laptop computer configured with multiple OSs and hacking tools. This course uses Windows, Kali Linux, and other Linux tools needed to conduct actual network and web application attacks. Learning how to install an OS isn't covered in this book, but you can find resources on this topic easily. The most recent versions of Kali Linux can be found at www.kali.org. The procedure for installing security tools varies, depending on the tool and the OS.

Activity 1-1: Determining the Corporate Need for IT Security Professionals

Time Required: 10 minutes

Objective: Examine corporations looking to employ IT security professionals.

Description: Many companies are eager to employ or contract security testers for their corporate networks. In this activity, you search the Internet for job postings, using the keywords "IT Security," and read some job descriptions to determine the IT skills (as well as any non-IT skills) most companies want an applicant to possess.

1. Start your web browser, and go to **indeed.com**.
2. In the What search box, type **IT Security**. In the Where search box, enter the name of a major city near you, and then press **Enter**.
3. Note the number of jobs. Select three to five job postings, and read the job description in each posting.
4. When you're finished, exit your web browser.

SECURITY BYTES

The urgent cybersecurity needs of organizations has created a labor shortage for qualified security professionals. In response, a company called Synack developed a "crowdsourced" model to provide ethical hacking services. Synack created a software platform that offers automated ways for companies to discover security flaws; then it turns those vulnerabilities over to penetration testers—basically, ethical hackers who use their skills for good. These ethical hackers are freelancers hired online on a job-by-job basis. If you choose to become an ethical hacker, you will find many employment opportunities and enjoy long-term job security.[1]

Penetration-Testing Methodologies

Ethical hackers who perform penetration tests use one of these models:

- White box model
- Black box model
- Gray box model

In the **white box model**, the tester is told what network topology and technology the company is using and is given permission to interview IT personnel and company employees. For example, the company might print a network diagram showing all the company's routers, switches, firewalls, and intrusion detection systems (IDSs; see Figure 1-1) or give the tester a floor plan detailing the location of computer systems and the OSs running on these systems (see Figure 1-2).

This background information makes the penetration tester's job easier than it is with using the black box model. In the **black box model**, management doesn't divulge to staff that penetration testing is being conducted, nor does it give the tester any diagrams or describe what technologies the company is using. This model puts the burden on the tester to find this information by using techniques you learn throughout this course. This model also helps management see whether the company's security personnel can detect an attack.

- Participate in research and provide recommendations for continuous improvement.
- Participate in knowledge sharing.
- Demonstrate a good understanding of current country, state, and city cyber laws.

Penetration testers and security testers usually have a laptop computer configured with multiple OSs and hacking tools. This course uses Windows, Kali Linux, and other Linux tools needed to conduct actual network and web application attacks. Learning how to install an OS isn't covered in this book, but you can find resources on this topic easily. The most recent versions of Kali Linux can be found at www.kali.org. The procedure for installing security tools varies, depending on the tool and the OS.

Activity 1-1: Determining the Corporate Need for IT Security Professionals

Time Required: 10 minutes

Objective: Examine corporations looking to employ IT security professionals.

Description: Many companies are eager to employ or contract security testers for their corporate networks. In this activity, you search the Internet for job postings, using the keywords "IT Security," and read some job descriptions to determine the IT skills (as well as any non-IT skills) most companies want an applicant to possess.

1. Start your web browser, and go to **indeed.com**.
2. In the What search box, type **IT Security**. In the Where search box, enter the name of a major city near you, and then press **Enter**.
3. Note the number of jobs. Select three to five job postings, and read the job description in each posting.
4. When you're finished, exit your web browser.

SECURITY BYTES

The urgent cybersecurity needs of organizations has created a labor shortage for qualified security professionals. In response, a company called Synack developed a "crowdsourced" model to provide ethical hacking services. Synack created a software platform that offers automated ways for companies to discover security flaws; then it turns those vulnerabilities over to penetration testers—basically, ethical hackers who use their skills for good. These ethical hackers are freelancers hired online on a job-by-job basis. If you choose to become an ethical hacker, you will find many employment opportunities and enjoy long-term job security.[1]

Penetration-Testing Methodologies

Ethical hackers who perform penetration tests use one of these models:

- White box model
- Black box model
- Gray box model

In the **white box model**, the tester is told what network topology and technology the company is using and is given permission to interview IT personnel and company employees. For example, the company might print a network diagram showing all the company's routers, switches, firewalls, and intrusion detection systems (IDSs; see Figure 1-1) or give the tester a floor plan detailing the location of computer systems and the OSs running on these systems (see Figure 1-2).

This background information makes the penetration tester's job easier than it is with using the black box model. In the **black box model**, management doesn't divulge to staff that penetration testing is being conducted, nor does it give the tester any diagrams or describe what technologies the company is using. This model puts the burden on the tester to find this information by using techniques you learn throughout this course. This model also helps management see whether the company's security personnel can detect an attack.

- Buffer overflows
- Cryptography
- Penetration-testing methodologies

As you can see, you must be familiar with a vast amount of information to pass this exam. Although you do need a general knowledge of these 22 domains for the exam, in the workplace, you'll most likely be placed on a team that conducts penetration tests. This team, called a **red team** in the industry, is composed of people with varied skills who perform the tests. For example, a red team might include a programming expert who can perform SQL injections or other programming vulnerability testing. The team might also include a network expert who's familiar with port vulnerabilities and IDS, router, or firewall vulnerabilities. It's unlikely that one person will perform all tests. However, passing the exam requires general knowledge of all the domains listed.

Open Source Security Testing Methodology Manual Professional Security Tester

The **OSSTMM Professional Security Tester (OPST)** certification is designated by the **Institute for Security and Open Methodologies** (**ISECOM**; www.isecom.org), a nonprofit organization that provides security training and certification programs for security professionals. The OPST certification uses the **Open Source Security Testing Methodology Manual (OSSTMM)**, written by Peter Herzog, as its standardized methodology. You'll use many of its methodologies throughout this course. Because the manual is updated periodically, you should check the ISECOM site regularly to download the most current version.

The exam covers some of the following topics:

- *Professional*—Rules of engagement (defining your conduct as a security tester)
- *Enumeration*—Internet packet types, denial-of-service testing
- *Assessments*—Network surveying, controls, competitive intelligence scouting
- *Application*—Password cracking, containment measures
- *Verification*—Problem solving, security testing

The exam requires testers to answer multiple-choice questions and successfully conduct security testing on an attack network. This practical-application portion of the exam ensures that testers can apply their knowledge to a real-world setting.

Certified Information Systems Security Professional

The **Certified Information Systems Security Professional (CISSP)** certification for security professionals is issued by the International Information Systems Security Certification Consortium (ISC²; www.isc2.org). Even though the CISSP certification isn't geared toward the technical IT professional, it has become one of the standards for many security professionals. The exam doesn't require testers to have technical knowledge in IT; it tests security-related managerial skills. CISSPs are usually more concerned with policies and procedures than the actual tools for conducting security tests or penetration tests, so they don't need the skills of a technical IT professional. ISC² requires exam takers to have five years of experience before taking the five-hour exam, so don't rush into this certification until you've been in the industry a while. The exam covers questions from the following 10 domains:

- Security and risk management
- Asset security (protecting security of assets)
- Security engineering (engineering and management of security)
- Communication and network security (designing and protecting network security)
- Identity and access management (controlling access and managing identity)
- Security assessment and testing (designing, performing, and analyzing security testing)
- Security operations (foundational concepts, investigations, incident management, and disaster recovery)
- Software development security (understanding, applying, and enforcing software security)

SANS Institute

The **SysAdmin, Audit, Network, Security (SANS) Institute** (www.sans.org) offers training and IT security certifications through **Global Information Assurance Certification** (**GIAC**, www.giac.org). Two related certifications in ethical hacking are the GIAC Certified Penetration Tester (GPEN) and the GIAC Certified Web Application Tester (GWAPT).

In addition to its well-respected certification, SANS offers its training courses through an accredited university, SANS Technology Institute. Alongside its training and degree programs, SANS disseminates research documents on computer and network security worldwide at no cost. One of its most popular documents is the Top 25 Software Errors list, which describes the most common network exploits and suggests ways of correcting vulnerabilities. This list offers a wealth of information for penetration testers or security professionals, and you examine it in Activity 1-2.

Which Certification Is Best?

Deciding which certification exam to take can be difficult. Both penetration testers and security testers need technical skills to perform their duties effectively. They must also have a good understanding of networks and the role of management in an organization, skills in writing and verbal communication, and a desire to continue learning. Any certification, if it encourages you to read and study more, is worth working toward. Being certified gives you a hiring advantage over someone who is not. If you have certifications in the area an employer is looking for, your resume will often go to the top of the prospects pile. The danger of certification exams is that some participants simply memorize terminology and don't have a good grasp of the subject matter or complex concepts, much like students who have managed to pass a final exam by cramming but then forget most of the information after taking the test. Use the time you spend studying for a certification exam wisely, discovering areas in which you might need improvement instead of memorizing answers to questions.

By learning the material in this course, you can acquire the skills you need to become a competent IT security professional and pass exams covering ethical hacking, penetration-testing methods, and network topologies and technologies. Regardless of the exam you take, however, the most critical point to remember is that laws govern what you can or cannot do as an ethical hacker, a security tester, or a penetration tester. Following the laws and behaving ethically are more important than passing an exam.

Be sure to visit websites for the organizations conducting certification testing because exam requirements change as rapidly as technology does. For example, several years ago, the CISSP exam had no questions on the Internet of Things (IoT), but now the exam covers this topic.

NOTE

Be aware that websites change often. You might have to dig around to find the information you're looking for. Think of this activity as practice for being a skilled security tester.

Activity 1-2: Examining the Top 25 Most Dangerous Software Flaws

Time Required: 15 minutes

Objective: Examine the SANS list of the most common network exploits.

Description: As fast as IT security professionals attempt to correct network vulnerabilities, someone creates new exploits, and network security professionals must keep up to date on these exploits. In this activity, you examine some current exploits used to attack networks. Don't worry—you won't have to memorize your findings. This activity simply gives you an introduction to the world of network security.

1. Start your web browser, and go to **www.sans.org**.
2. Under Resources, click the **Top 25 Programming Errors** link. (Because websites change frequently, you might have to search to find this link.)
3. Read the contents of the Top 25 list. (This document changes often to reflect the many new exploits created daily.) The Top 25 list is also known as the Top 25 Most Dangerous Software Errors. Links in the list explain the scoring system and framework used to rank these errors.
4. Investigate the first few flaws by clicking the **CWE-#** link. For each flaw, note the description, applicable platform, and consequences.
5. When you're finished, exit your web browser.

WHAT YOU CAN DO LEGALLY

Because laws involving computer technology change as rapidly as technology itself, you must keep abreast of what's happening in your area of the world. What's legal in Des Moines might not be legal in Indianapolis, for example. Finding out what's legal in your state or country can be just as difficult as performing penetration tests, however. Many state officials aren't aware of the legalities surrounding computer technology. This confusion also makes it difficult to prosecute wrongdoers in computer crimes. The average citizen on a jury doesn't want to send a person to jail for doing something the state prosecutor hasn't clearly defined as illegal.

As a security tester, you must be aware of what you're allowed to do and what you should not or cannot do. For example, some security testers know how to pick a deadbolt lock, so a locked door wouldn't deter them from gaining physical access to a server. However, testers must be knowledgeable about the laws for possessing lockpicks before venturing out to a corporate site with tools in hand. In fact, laws vary from state to state and country to country. In some states, the mere possession of lockpicking tools constitutes a crime, whereas other states allow possession as long as a crime hasn't been committed. In one state, you might be charged with a misdemeanor for possessing these tools; in another state, you might be charged with a felony.

TIP The Open Organisation of Lockpickers (TOOOL) is worth a look if you are considering adding this skill to your arsenal. Their website, https://toool.us/laws.html, makes it easy for you to check the laws in each state before your pack your suitcase with your lockpicking tools.

Laws of the Land

As with lockpicking tools, having hacking tools on your computer or mobile device might be illegal. You could contact local law enforcement agencies or research online about the laws for your state or country before installing hacking tools on your devices. You can see how complex this issue gets as you travel from state to state or country to country. New York City might have one law for installing hacking tools, and a quick drive over the George Washington Bridge brings you to a different law in New Jersey. Table A-1, in Appendix A, compares Vermont's computer crime statutes to New York's to demonstrate the variety of verbiage the legal community uses.

Laws are written to protect society, but often the written words are open to interpretation, which is why courts and judges are necessary. In Hawaii, for example, the state must prove that the person charged with committing a crime on a computer had the "intent to commit a crime." So just scanning a network isn't a crime in Hawaii. Also, the state has the even more difficult task of having to prove that the computer used in committing a crime had been used by only one person—the one alleged to have committed the crime. If the person charged with the crime claims that more than one person had access to the computer used to gather evidence of wrongdoing, the state can't use that computer as evidence.

What do these laws have to do with a network security professional using penetration-testing tools? Laws for having hacking tools that allow you to view a company's network infrastructure aren't as clearly defined as laws for possession of lockpicking tools because laws haven't been able to keep up with the speed of technological advances. In some states, running a program that gives an attacker an overview and a detailed description of a company's network infrastructure isn't seen as a threat.

As another example of how laws can vary, is taking photos of a bank's exterior and interior legal? Security personnel at a bank in Hawaii say you would be asked to stop taking photos and leave the premises. An FBI spokesperson put it in simple terms: You can be asked to stop taking photos if you're on private property. Taking photos across the street from the bank with a zoom lens is legal, but if you use the photos to commit a crime in the future, an attorney would tell you the charges against you might be more serious. Because of the fear of terrorism, in certain parts of the United States and many parts of Europe, taking photos of bridges, train stations, and other public areas is illegal.

The point of mentioning all these laws and regulations is to make sure you're aware of the dangers of being a security tester or a student learning hacking techniques. Table 1-1 lists a small fraction of the cases prosecuted in the past few years; in these cases, many people have been sentenced to prison for hacking. Most attacks involved more than scanning a business, but the cases show that the government is serious about punishment for cybercrimes.

Table 1-1 Overview of recent hacking cases

State and year	Description
Kansas, 2021	A resident of Ellsworth County, Kansas, was charged with one count of tampering with a public water system and one count of reckless damage to a protected computer during unauthorized access. The indictment alleged that a former employee knowingly accessed the Ellsworth County Rural Water District's protected computer system without authorization. During this unauthorized access, the accused allegedly performed activities that shut down the processes at the facility, which affected cleaning and disinfecting procedures, with the intention of harming the public drinking water system. If found guilty, the accused faces up to 25 years in prison and a fine of up to $500,000 for illegally accessing the protected computer and tampering with the water system.
California, 2021	A former employee of an IT consulting firm accessed the server of a company in Carlsbad, California, and deleted more than 1,200 of the company's 1,500 Microsoft user accounts. The employee was apparently retaliating for being fired. The attack affected most of the Carlsbad company's employees so that they could not access email or other network services, effectively shutting down the company for days and causing continuous IT problems for three months. The former contractor was sentenced in federal court to two years in prison and ordered to pay the company more than $560,000.
Nevada, 2021	A Russian national offered $1 million to an employee of Tesla's electric battery plant in Nevada in a scheme to have the insider introduce malicious software into the company's computer network. The malware attack was designed to extract data from the company's network and then demand a ransom for its return. The ransomware case is considered unusual because it involves face-to-face bribery rather than anonymous hacking via the Internet. Such an attack typically carries a penalty of up to five years in prison and a $250,000 fine.
Atlanta, 2021	A Cypriot national hacked into major websites as a teenager and threatened that he would release stolen user information unless the websites paid a ransom. The hacker identified vulnerable websites, including those for sports news and online games, and then stole personally identifiable information from user and customer databases. He became the first Cypriot national extradited from Cyprus to the United States, and paid nearly $600,000 in restitution to his victims. In addition, he has been sentenced to federal prison for at least three years.
New Jersey, 2021	While employed at a data analytics and risk assessment firm based in New Jersey, a resident of Moorefield, Nebraska, obtained confidential information that belonged to the firm—including names, passwords, email addresses, and telephone numbers of clients—and then attempted to sell the information. Nearly two years after his arrest, the hacker was sentenced to three years of supervised release and ordered to pay restitution of more than $290,000.
Florida, 2021	A Florida high school conducted online voting to select a homecoming queen but found out that an assistant principal in the school district manipulated the vote electronically. She accessed a network database storing confidential student information—including grades, medical history, and credentials—and then used the credentials to cast ballots in favor of her daughter. The pair were arrested and charged with fraudulently accessing confidential student information. The daughter was expelled from the high school, and her mother was suspended from her job as they awaited sentencing.

Some of the most infamous cases are hacks carried out by students, such as the recent attack on Miami-Dade schools. Many hackers use software to crack passwords of online accounts. This act, performed by many security professionals when given permission to do so by a network's owner, is a federal offense when done without permission and can add substantial prison time to a hacker's sentence.

SECURITY BYTES

HackerOne is a security platform that connects hackers with organizations needing security vulnerability assessments.[2] The hackers are ethical hackers who use their devious skills for good. HackerOne pays the ethical hackers a so-called bug bounty according to the criticality of the bugs they find. A handful of HackerOne hackers have become millionaires as a result of the bug bounty payments.

Is Port Scanning Legal?

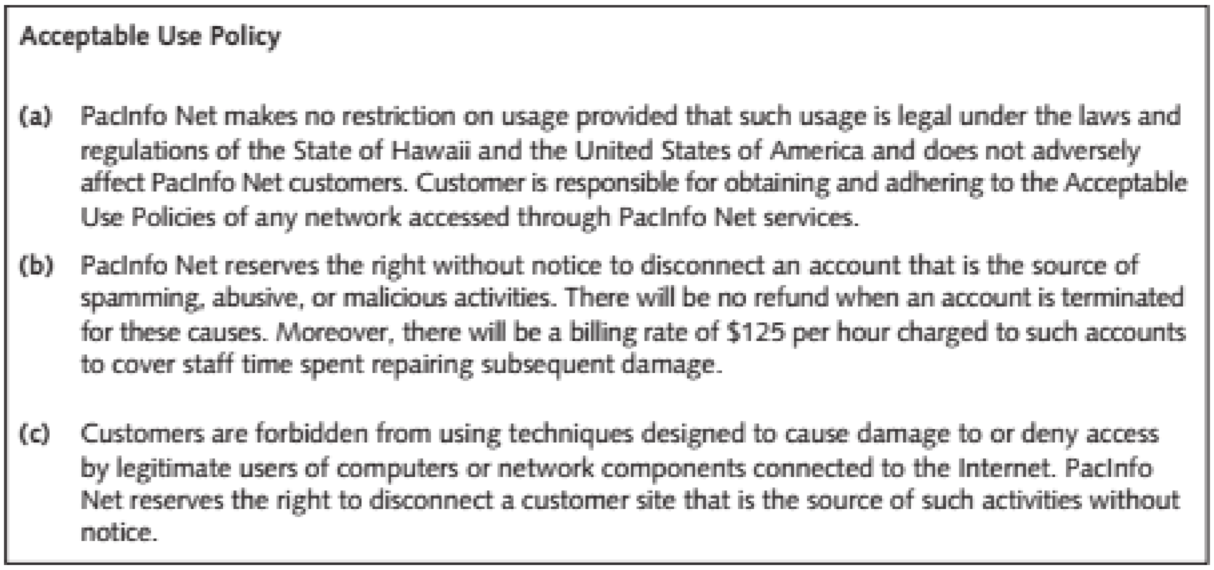
Port scanning is a common activity in penetration testing. Testers use port scanning to detect computing devices on a network and itemize the services they offer. For example, if a scan detects that a computer at the IP address 192.168.1.100 has port 443 open for connections, the machine is probably a web server and could later be targeted for web server penetration tests.

Some states consider port scanning as noninvasive or nondestructive in nature and deem it legal. This isn't always the case, however, so you must be prudent before you start using penetration-testing tools. Some companies have filed criminal charges against hackers for scanning their systems, but judges ruled that no damage was done to the networks, so the charges were dismissed. It's just a matter of time before a business will claim that its network is also private property, and it should have the right to say that scanning is not allowed.

Because the federal government currently doesn't see these infringements as a violation of the U.S. Constitution, each state is allowed to address these issues separately. However, a company could bring up similar charges against you if you decide to practice using the tools you learn in this course. Even if you're found innocent in your state, the legal costs could be damaging to your business or personal finances. Therefore, you must research your state laws before using what you learn, even if you're using the tools for the benefit of others, not criminal activity. As of this writing, you can check www.ncsl.org/research/telecommunications-and-information-technology/computer-hacking-and-unauthorized-access-laws.aspx for each state's laws on unauthorized access and hacking. (If this URL doesn't work, go to the home page at www.ncsl.org and do a search.) Spending time at this site is certainly preferable to spending time in court or prison.

TIP When traveling outside the United States, be aware of the cyber laws of the country you're visiting. For example, driving a car equipped with an antenna designed to identify wireless access points is a crime in Germany.

You should also read your ISP contract, specifically the section titled "Acceptable Use Policy" or something similar. Most people glance at and accept the terms of their contract. Figure 1-3 is an excerpt from an actual ISP contract. Notice that section (c) might create some problems if you run scanning software that slows down network access or prevents users from accessing network components.



Acceptable Use Policy

(a) PacInfo Net makes no restriction on usage provided that such usage is legal under the laws and regulations of the State of Hawaii and the United States of America and does not adversely affect PacInfo Net customers. Customer is responsible for obtaining and adhering to the Acceptable Use Policies of any network accessed through PacInfo Net services.

(b) PacInfo Net reserves the right without notice to disconnect an account that is the source of spamming, abusive, or malicious activities. There will be no refund when an account is terminated for these causes. Moreover, there will be a billing rate of $125 per hour charged to such accounts to cover staff time spent repairing subsequent damage.

(c) Customers are forbidden from using techniques designed to cause damage to or deny access by legitimate users of computers or network components connected to the Internet. PacInfo Net reserves the right to disconnect a customer site that is the source of such activities without notice.

Figure 1-3 Sample acceptable use policy

Another ISP responded to an email about the use of scanning software with the following message:

> *Any use of the Service that disturbs the normal use of the system by HOL or by other HOL customers or consumes excessive amounts of memory or CPU cycles for long periods of time may result in termination pursuant to Section 1 of this Agreement. Users are strictly prohibited from any activity*

> *that compromises the security of HOL's facilities. Users may not run IRC "bots" or any other scripts or programs not provided by HOL.*
>
> *Regards,*
> *Customer Support*
> *Hawaii Online*

The statement prohibiting the use of Internet Relay Chat (IRC) bots or any other scripts or programs not provided by the ISP might be the most important for penetration testers. An IRC bot is a program that sends automatic responses to users, giving the appearance of a person on the other side of a connection. For example, a bot can welcome new users joining a chat session, even though a person isn't actually present to welcome them. Even if you have no intentions of creating a bot, the "any other scripts or programs" clause should still raise an eyebrow.

Another consideration when performing port scans is whether your computer is connected to your business network by a virtual private network (VPN). Many people work from home using a VPN to connect to their work network. If you run a port scanner while your VPN is connected, you may end up scanning work computers, which could be problematic.

Table A-1 in Appendix A shows which legal statutes to look at before you begin your journey. The statutes listed in the table might have changed since the writing of this book, so keep up with your state laws before trying penetration-testing tools. In Activity 1-3, you research the laws of your state or country, using Table A-1 as a guide.

Activity 1-3: Identifying Computer Statutes in Your State or Country

Time Required: 30 minutes

Objective: Learn what laws might prohibit you from conducting a network penetration test in your state or country.

Description: For this activity, you use Internet search engines to gather information on computer crime in your state or country (or a location selected by your instructor). You have been hired by ExecuTech, a security consulting company, to gather information on any new statutes or laws that might affect the security testers it employs. Write a one-page memo to Liang Choi, director of security and operations, listing applicable statutes or laws and offering recommendations to management. For example, you might note in your memo that conducting a denial-of-service attack on a company's network is illegal because your state's penal code prohibits this type of attack unless authorized by the owner.

Federal Laws

You should also be aware of applicable federal laws when conducting your first security test (see Table 1-2). Federal computer crime laws are becoming more specific about cybercrimes and intellectual property issues. In fact, the government has a branch of computer crime called computer hacking and intellectual property (CHIP).

Table 1-2 Federal computer crime laws

Federal law	Description
The No Electronic Theft Act (P.L. 105–147)	Extends the reach of criminal copyright law to specifically include electronic means as one method for committing the crime (17U S. C. § 501 (a) (1)). The act also expands the scope of the criminal conduct covered under this crime, allowing for prosecutions without showing that the distributor of the copyrighted material profited from the activity.
The Economic Espionage Act (EEA)	The EEA offers trade secret protection to both businesses and the government. The significance of information to society, and the problems that are attached to protecting this information, make the EEA an important step in how the law can provide protection from computer crime.

(continues)

Table 1-2 Federal computer crime laws *(continued)*

Federal law	Description
The Computer Fraud and Abuse Act (CFAA). Title 18, Crimes and Criminal Procedure. Part I: Crimes, Chapter 47, Fraud and False Statements, Sec. 1030: Fraud and related activity in connection with computers	This law makes it a federal crime to access classified information or financial information without authorization.
The Identity Theft and Assumption Deterrence Act (ITADA) [18 U.S.C. Section 1028(a)(7)]	This act criminalizes identity theft and allows courts to assess the losses suffered by individual consumers. While the CFAA covers certain aspects of identity theft, the ITADA addresses restitution and relief for the victims.
Electronic Communication Privacy Act. Title 18, Crimes and Criminal Procedure. Part I: Crimes, Chapter 119, Wire and Electronic Communications Interception and Interception of Oral Communications, Sec. 2510: Definitions and Sec. 2511: Interception and disclosure of wire, oral, or electronic communications prohibited	These laws make it illegal to intercept any communication, regardless of how it was transmitted.
U.S. PATRIOT Act, Sec. 217. Interception of Computer Trespasser Communications	This act largely seeks to amend previous privacy and surveillance laws and fund government surveillance programs. It also specifies ways for the government to monitor individuals and allows victims of cybercrimes to monitor the activity of trespassers on their systems.
Homeland Security Act of 2002, H.R. 5710, Sec. 225: Cyber Security Enhancement Act of 2002	This amendment to the Homeland Security Act of 2002 specifies sentencing guidelines for certain types of computer crimes.
The Computer Fraud and Abuse Act. Title 18, Crimes and Criminal Procedure, Sec. 1029: Fraud and related activity in connection with access devices	This law makes it a federal offense to manufacture, program, use, or possess any device or software that can be used for unauthorized use of telecommunications services.
Stored Wire and Electronic Communications and Transactional Records Act. Title 18, Crimes and Criminal Procedure. Part I: Crimes, Chapter 121, Stored Wire and Electronic Communications and Transactional Records Act, Sec. 2701: Unlawful access to stored communications (a) Offense. Except as provided in subsection of this section whoever (1) intentionally accesses without authorization a facility through which an electronic communication service is provided; or (2) intentionally exceeds an authorization to access that facility; Sec. 2702: Disclosure of contents	This law defines unauthorized access to computers that store classified information.