

Licensed to:

Second Edition

# HANDS-ON ETHICAL HACKING AND NETWORK DEFENSE

Michael T. Simpson, Kent Backman, James Corley



PREPARING TOMORROW'S  
INFORMATION  
**SECURITY**  
PROFESSIONALS

***Hands-On Ethical Hacking  
and Network Defense,***  
**Second Edition**

**Michael T. Simpson, Kent Backman, and  
James E. Corley**

Vice President, Career and Professional  
Editorial: Dave Garza

Director of Learning Solutions: Matthew  
Kane

Executive Editor: Stephen Helba

Managing Editor: Marah Bellegarde

Product Manager: Natalie Pashoukos

Developmental Editor: Lisa M. Lord

Editorial Assistant: Meghan Orvis

Vice President, Career and Professional  
Marketing: Jennifer Ann Baker

Marketing Director: Deborah S. Yarnell

Senior Marketing Manager: Erin Coffin

Marketing Coordinator: Shanna Gibbs

Production Director: Carolyn Miller

Production Manager: Andrew Crouth

Senior Content Project Manager: Andrea  
Majot

Senior Art Director: Jack Pendleton

Manufacturing Buyer: Julio Esperas

Technical Editor: John Bosco

Quality Assurance: Green Pen Quality  
Assurance

Compositor: Pre-PressPMG

© 2011 Course Technology, Cengage Learning

ALL RIGHTS RESERVED. No part of this work covered by the copyright herein may be reproduced, transmitted, stored, or used in any form or by any means graphic, electronic, or mechanical, including but not limited to photocopying, recording, scanning, digitizing, taping, Web distribution, information networks, or information storage and retrieval systems, except as permitted under Section 107 or 108 of the 1976 United States Copyright Act, without the prior written permission of the publisher.

For product information and technology assistance, contact us at  
**Cengage Learning Customer & Sales Support, 1-800-354-9706**

For permission to use material from this text or product,  
submit all requests online at **cengage.com/permissions**.

Further permissions questions can be e-mailed to  
**permissionrequest@cengage.com**

Microsoft® is a registered trademark of Microsoft Corporation.

Novell® is a registered trademark of Novell, Inc.

Solaris® is a registered trademark of Sun Microsystems, Inc.

Mac OS X® is a registered trademark of Apple, Inc.

Library of Congress Control Number: 2010922642

ISBN-13: 978-1-4354-8609-6

ISBN-10: 1-4354-8609-9

**Course Technology**  
20 Channel Center Street  
Boston, MA 02210  
USA

Cengage Learning is a leading provider of customized learning solutions with office locations around the globe, including Singapore, the United Kingdom, Australia, Mexico, Brazil and Japan. Locate your local office at:  
**international.cengage.com/region**

Cengage Learning products are represented in Canada by Nelson Education, Ltd.

To learn more about Course Technology, visit **www.cengage.com/coursestechnology**

To learn more about Cengage Learning, visit **www.cengage.com**

Purchase any of our products at your local college store or at our preferred online store **www.cengagebrain.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  
2 3 4 5 12 11 10

# Ethical Hacking Overview

**After reading this chapter and completing the exercises, you will be able to:**

- Describe the role of an ethical hacker
- Describe what you can do legally as an ethical hacker
- Describe what you can't do as an ethical hacker



**The term “ethical hacker” might seem like an oxymoron—sort of like an ethical pickpocket or ethical embezzler.** In this chapter, you learn that ethical hackers are employed or contracted by a company to do what illegal hackers do: break in. Why? Companies need to know what, if any, parts of their security infrastructure are vulnerable to attack. To protect a company’s network, many security professionals recognize that knowing what tools the bad guys use and how they think enables them to better protect (harden) a network’s security.

Remember the old adage: You’re only as secure as your weakest link. The bad guys spend a lot of time and energy trying to find weak links. This book provides the tools you need to protect a network and shares some approaches an ethical hacker—also called a “security tester” or a “penetration tester”—might use to discover vulnerabilities in a network. It’s by no means a definitive book on ethical hacking. Rather, it gives you a good overview of a security tester’s role and includes activities to help you develop the skills you need to protect a network from attack. This book helps you understand how to protect a network when you discover the methods the bad guys (hackers) or the good guys (ethical hackers) use to break into a network. It also helps you select the most appropriate tools to make your job easier.

Understanding what laws can affect you when performing your job as a security tester is important, especially if you use the testing methods outlined in this book. Also, understanding the importance of having a contractual agreement with a client before performing any aspects of a security test might help you avoid breaking the law.

---

## Introduction to Ethical Hacking

Companies sometimes hire **ethical hackers** to conduct penetration tests. In a **penetration test**, an ethical hacker attempts to break into a company’s network to find the weakest link in the network or a network system. In a **security test**, testers do more than attempt to break in; they also analyze a company’s security policy and procedures and report any vulnerabilities to management. Security testing, in other words, takes penetration testing to a higher level. As Peter Herzog states in the Open Source Security 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 issues are just some of the ones security testers must examine. In doing so, they alert companies to the 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 is to unplug the network cable. When you discover vulnerabilities (“holes”) in a network, you can spend time correcting them. This process might entail tasks such as updating an operating system (OS) or installing the vendor’s latest security patch.

If your job is a penetration tester, you simply report your findings to the company. Then 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. This book is 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 book, 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 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 system's 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 simply want to prove how vulnerable a system is by accessing the computer or network without destroying any data. For the purpose of this book, 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 that usage is followed in this book.

An ethical hacker is a person who performs most of the same activities a hacker does but with the owner or company's permission. This distinction is important and can mean the difference between being charged with a crime or 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 from knowledgeable programmers instead of creating the code themselves. Many experienced penetration testers can write computer programs or scripts in Perl (Practical Extraction and Report Language, although it's always referred to as "Perl") or the C language to carry out network attacks. (A script is a set of instructions that run in sequence to perform tasks on a computer system.)

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.

Penetration testers and security testers usually have a laptop computer configured with multiple OSs and hacking tools. The BackTrack DVD accompanying this book contains the Linux OS and many tools needed to conduct actual network attacks. This collection of tools for conducting vulnerability assessments and attacks is sometimes referred to as a “tiger box.” You can order tiger boxes on the Internet, but if you want to gain more experience, you can install multiple OSs and security tools on your own system. Learning how to install an OS isn’t covered in this book, but you can find books on this topic easily. The procedure for installing security tools varies, depending on the OS.



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

**Time Required:** 10 minutes

**Objective:** Examine the many 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 <http://jobsearch.monster.com>.
2. Click the **Search Jobs** text box, type **IT Security**, and then click the **Search** button.
3. Scroll to the bottom of the first page, and note the number of positions found. Select three to five positions and read the job description information.
4. When you’re finished, exit your Web browser.



### Security Bytes

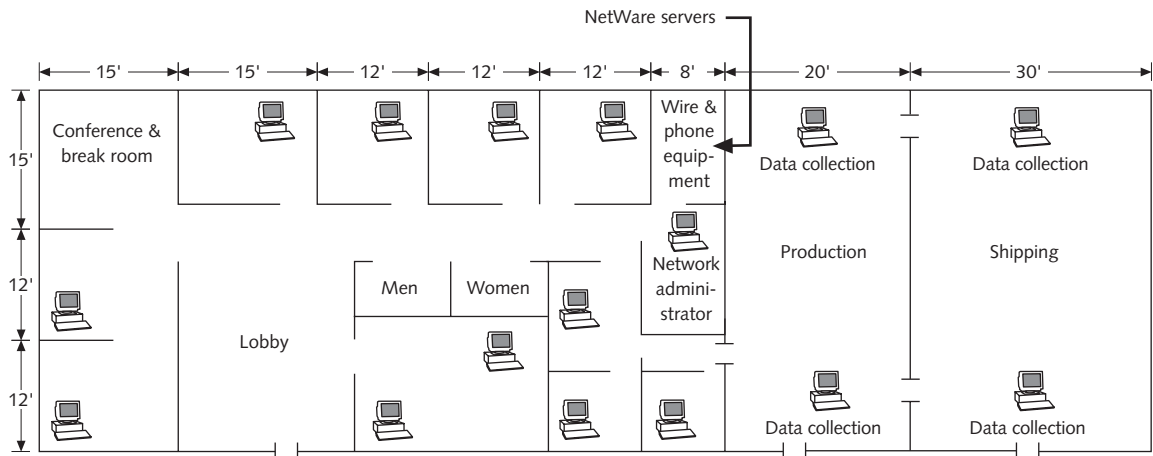
An April 2009 article in *USA Today*, “U.S. Looks to Hackers to Protect Cyber Networks,” revealed that the federal government is looking for hackers—not to prosecute them, but to pay them to secure the nation’s networks. Curiously, the term “ethical” didn’t precede the word “hacker.” One can only hope the hackers hired have moral and ethical values as well as hacking skills.

## 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) or give the tester a floor plan detailing the location of computer systems and the OSs running on these systems (see Figure 1-1).



**Figure 1-1** A sample floor plan

*Courtesy Course Technology/Cengage Learning*

This background information makes the penetration tester's job a little easier than it is with 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 book. This model also helps management see whether the company's security personnel can detect an attack.

The **gray box model** is a hybrid of the white and black box models. In this model, the company gives the tester only partial information. For example, the tester might get information about which OSs are used but not get any network diagrams.



### Security Bytes

Hospitals often check the intake procedures medical staff perform by using interns and nurses as "potential patients." In one psychiatric hospital, intake staff was told in advance that some potential patients would be doctors or nurses. Surprisingly, the number of patients admitted that month was unusually low, even though none of the patients were interns or nurses. In the same vein, if a company knows that it's being monitored to assess the security of its systems, employees might behave more vigilantly and adhere to existing procedures. Many companies don't want this false sense of security; they want to see how personnel operate without forewarning that someone might attempt to attack their network.

## Certification Programs for Network Security Personnel

As most IT professionals are aware, professional certification is available in just about every area of network security. The following sections cover several applicable certifications. Whether you're a security professional, computer programmer, database administrator, or wide area network (WAN) specialist, professional organizations offer enough certifications and exams to keep you busy for the rest of your career. The following sections cover the most popular IT security certifications and describe some exam requirements briefly. You

should have already earned, at minimum, CompTIA Security+ certification or have equivalent knowledge, which assumes networking competence at the CompTIA Network+ level of knowledge, a prerequisite for the Security+ certification. For more details, visit the CompTIA Web site ([www.comptia.org](http://www.comptia.org)).

**Certified Ethical Hacker** The International Council of Electronic Commerce Consultants (EC-Council) has developed a certification designation called **Certified Ethical Hacker (CEH)**. Currently, the multiple-choice CEH exam is based on 22 domains (subject areas) the tester must be familiar with. Knowledge requirements change periodically, so if you're interested in taking this exam, visit EC-Council's Web site ([www.eccouncil.org](http://www.eccouncil.org)) for the most up-to-date information. The 22 domains tested for the CEH exam are as follows:

- Ethics and legal issues
- Footprinting
- Scanning
- Enumeration
- System hacking
- Trojans and backdoors
- Sniffers
- Denial of service
- Social engineering
- Session hijacking
- Hacking Web servers
- Web application vulnerabilities
- Web-based password-cracking techniques
- Structured Query Language (SQL) injection
- Hacking wireless networks
- Viruses and worms
- Physical security
- Hacking Linux
- Intrusion detection systems (IDSs), firewalls, and honeypots
- 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. (You learn more about SQL injections in Chapter 10.) 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. Reading this book and working through the activities and case projects will help you gain this knowledge.

**Open Source Security Testing Methodology Manual (OSSTMM) Professional Security Tester** The OSSTMM Professional Security Tester (OPST) certification is designated by the **Institute for Security and Open Methodologies (ISECOM)**, a non-profit 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. This manual is one of the most widely used security testing methodologies to date and is available on the DVD accompanying this book. You'll use many of its methodologies throughout this book. Because the manual is updated periodically, you should check the ISECOM site ([www.isecom.org](http://www.isecom.org)) 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 not only answer multiple-choice questions, but also conduct security testing on an attack network successfully. This practical-application portion of the exam ensures that testers can apply their knowledge to a real-world setting. For more information on this certification, visit [www.isecom.org](http://www.isecom.org).

**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 (ISC<sup>2</sup>). 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. ISC<sup>2</sup> requires exam takers to have five years' experience before taking the five-hour exam, so don't rush into it until you've been in the industry a while. The exam covers questions from the following 10 domains:

- Access control systems and methodology
- Telecommunications and network security
- Security management practices
- Application and systems development security
- Cryptography
- Security architecture and models



- Operations security
- Business continuity planning and disaster recovery planning
- Laws, investigations, and ethics
- Physical security

For more information on this certification, visit [www.isc2.org](http://www.isc2.org).

**SANS Institute** The SysAdmin, Audit, Network, Security (SANS) Institute offers training and IT security certifications through **Global Information Assurance Certification (GIAC)**. It also disseminates research documents on computer and network security worldwide at no cost. One of the most popular SANS Institute documents is the Top 20 list, which details 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. For more information on security certification exams, visit [www.sans.org](http://www.sans.org) or [www.giac.org](http://www.giac.org).

**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 its weight in gold. The argument that a certification is just a piece of paper can be countered by saying “So is a hundred dollar bill, but it’s nice to have in your wallet!” 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 book, 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 there are laws governing what you can or can’t 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.

Again, visit Web sites 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 wireless networking because the technology wasn’t widely available, but now the exam covers wireless technology.



## Activity 1-2: Examining the Top 20 List

**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.

**TIP**

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

1. Start your Web browser, and go to **www.sans.org**.
2. Under Free Resources, click the **Top 20 Security Vulnerabilities** link. (Because Web sites change as rapidly as the price of gas, you might have to search to locate this link.)
3. Read the contents of the SANS Top 20 list. (Note that this document changes often to reflect the many new exploits created daily.) The list is organized into several categories, including server-side and client-side vulnerabilities.
4. Click a few links to investigate some vulnerabilities. For each one, scroll down to the section "How to Determine If You Are at Risk," and read the information. Then scroll down and read the section "How to Protect against ...," noting possible remedies for correcting the vulnerability. Does the remedy use a third-party tool or one that can be downloaded from Microsoft?
5. Go back to the Top 20 list, and in the section on server-side vulnerabilities, click the **Unix and Mac OS Services** link.
6. Scroll down and note the operating systems listed in the "Affected OSs" section. Then read the information in "How to Determine If You Are Vulnerable." Scroll down and read the section "How to Protect Against These Vulnerabilities," noting possible remedies for correcting the vulnerability. Do vendors offer software patches or any step-by-step directions for IT professionals?
7. 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 getting 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.

## Laws of the Land

As with lockpicking tools, having some hacking tools on your computer might be illegal. You should contact local law enforcement agencies and ask about the laws for your state or country before installing hacking tools on your computer. 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, and a quick drive over the George Washington Bridge brings you to the laws of 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 just a small fraction of the cases prosecuted in the past few years; in these cases, many people have been sentenced to prison for "hacking," the term used by the Department of Justice. Most attacks involved more than just scanning a business, but this information shows that the government is getting more serious about punishment for cybercrimes. Some of the most infamous cases are hacks carried out by college students, such as the eBay hack of 1999. As you read Table 1-1, note that some hackers used software to crack passwords of logon 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.



Table 1-1 An overview of recent hacking cases

State and year	Description
California, 2006	Jeanson James Ancheta, 21, of Downey, California, was sentenced to 57 months in federal prison and 3 years of supervised release by the U.S. District Court of Los Angeles for conspiring to violate the Computer Fraud Abuse Act and the CAN-SPAM Act, causing damage to federal government computers used in national defense, and accessing protected computers without authorization to commit fraud.
California, 2008	Jon Paul Oson, a former IT network engineer and technical services manager for San Diego’s Council of Community Health Clinics, was sentenced to 63 months in prison on federal hacking charges. He was convicted of intentionally damaging protected computers by disabling the backup database of patient information and deleting data and software on several servers.
California, 2008	Ukrainian Maksym Yastremskiy, 25, was among 11 people charged with hacking T.J. Maxx’s network in 2007. He’s believed to be responsible for losses up to tens of millions of dollars worldwide and involved in the theft of 45 million identities. He was charged with trafficking in unauthorized access devices, identity theft, and money laundering and sentenced to 30 years in prison. T.J. Maxx’s parent company has paid millions in compensation to affected banks and customers.
California, 2009	Mario Azar, 28, an IT consultant for Pacific Energy Resources (PER), was indicted on federal charges of damaging the company’s computer systems after it declined to offer him permanent employment. He was charged with unauthorized impairment of a protected computer, which carries a maximum penalty of 10 years in federal prison. Azar accessed PER computer systems illegally and caused thousands of dollars of damage to data.
Minnesota, 2009	Zachary Wiley Mann was sentenced to 60 months in federal prison on one count of wire fraud and one count of aggravated identity theft. Mann obtained credit card account information from thousands of victims by hacking into a Web-based order processing server and used the stolen credit card numbers to add value to gift cards he purchased for small dollar amounts at restaurants.
California, 2009	Concluding the first prosecution of its kind in the nation, John Schiefer, an information security consultant known to be associated with the “botnet underground,” was sentenced to 48 months in federal prison for using his botnets to steal identities by extracting victims’ information from their computers and wiretapping their communications.
Pennsylvania, 2009	University of Pennsylvania student Ryan Goldstein, 22, was sentenced to 3 months in prison and 5 years of probation for a hacking scheme that crashed an engineering school server. He helped a New Zealand hacker launch a 50,000-computer attack against online chat networks by using a botnet. With this attack, Goldstein was able to access the university’s server illegally, which was used by more than 4000 students, faculty, and staff.

Is Port Scanning Legal?

Some states consider port scanning (covered in Chapter 5) 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. In some cases, a company has filed criminal charges against hackers for scanning its system, but judges ruled that no damage was done to the network, 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 book. Even if you're found innocent in your state, the legal costs could be damaging to your business or personal finances. Therefore, researching your state laws before using what you learn in this book is essential, even if you're using the tools for the benefit of others, not criminal activity. As of this writing, you can check the Web site [www.ncsl.org/programs/lis/CIP/hacklaw.htm](http://www.ncsl.org/programs/lis/CIP/hacklaw.htm) 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](http://www.ncsl.org) and do a search.) Spending time at this site is certainly preferable to spending time in court or prison.

You should also read your ISP contract, specifically the section usually called "Acceptable Use Policy." Most people just glance over and accept the terms of their contract. Figure 1-2 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 1-2** An example of an acceptable use policy

*Courtesy Course Technology/Cengage Learning*

Another ISP responded to an e-mail 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 being on the other side of the connection. For example, a bot can be created that welcomes 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.

Table A-2 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 keeping up with your state laws before trying penetration-testing tools is important. In Activity 1-3, you research the laws of your state or country, using Table A-2 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 hacking a network or computer system 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 have an impact on the security testers they employ. Write a one-page memo to Bob Lynch, director of security and operations, listing any 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 the 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 getting more specific about cybercrimes and intellectual property issues. In fact, the government now has a new branch of computer crime called computer hacking and intellectual property (CHIP).

Table 1-2 Federal computer crime laws

Federal law	Description
The Computer Fraud and Abuse Act. 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.
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.

(Continued)

Table 1-2 Federal computer crime laws (continued)

Federal law	Description
U.S. Patriot Act Sec. 217. Interception of Computer Trespasser Communications	This law amended Chapter 119 of Title 18, U.S. Code.
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.



Security Bytes

Even though you might think you’re following the requirements set forth by the client who hired you to perform a security test, don’t assume that management will be happy with your results. One tester was reprimanded by a manager who was upset that security testing revealed all the logon names and passwords. The manager believed that the tester shouldn’t know this information and considered stopping the security testing.



Activity 1-4: Examining Federal Computer Crime Laws

Time Required: 15 minutes

Objective: Increase your understanding of U.S. federal laws related to computer crime.

Description: For this activity, use Internet search engines to gather information on U.S. Code, Title 18, Sec. 1030, which covers fraud and related activity in connection with computers. Write a summary explaining how this law can affect ethical hackers and security testers.

What You Cannot Do Legally

After reviewing the state and federal laws on computer crime, you can see that accessing a computer without permission, destroying data, and copying information without the owner’s permission are illegal. It doesn’t take a law degree to understand that certain actions are

illegal, such as installing viruses on a computer network that deny users access to network resources. As a security tester, you must be careful that your actions don't prevent the client's employees from doing their jobs. If you run a program that uses network resources to the extent that a user is denied access to them, you have violated federal law. For example, denial-of-service (DoS) attacks, covered in Chapter 3, should not be initiated on your client's networks.

## Get It in Writing

As discussed earlier, you can cause a DoS attack inadvertently by running certain hacking programs on a client's network. This possibility is what makes your job difficult, especially if you're conducting security tests as an independent contractor hired by a company instead of being an employee of a large security company that has a legal team to draw up a contract with the client. Employees of a security company are protected under the company's contract with the client.

For the purposes of this discussion, assume you're an independent contractor who needs a little guidance in creating a written contract. Some contractors don't believe in written contracts, thinking they undermine their relationships with clients. The old handshake and verbal agreement work for many computer consultants, but consulting an attorney is always wise. Some think it's a matter of trust, and others argue that a written contract is just good business. Consultants who haven't received payment from the client usually vote yes on the contract question. Similarly, users often aren't convinced of the importance of backing up important documents until their computers crash. Don't be like them and wait until you're in court to wish you had something in writing.

If you want additional information, you can consult books on working as an independent contractor, such as *The Computer Consultant's Guide* (Janet Ruhl, 1997, ISBN 0471176494) and *Getting Started in Computer Consulting* (Peter Meyer, 1999, ISBN 0471348139). The Internet can also be a helpful resource for finding free contract templates that can be modified to fit your business situation. The modifications you make might create more problems than having no contract at all, however, so having an attorney read your contract before it's signed is a good investment of your time and money.

Are you concerned? Good. Most textbooks or courses on ethical hacking gloss over this topic, yet it's the most important part of the profession. If your client gives you a contract drawn up by the company's legal department, consulting a lawyer can save you time and money. Attempting to understand a contract written by attorneys representing the company's best interests warrants an attorney on your side looking out for your best interests. The complexity of law is too much for most laypeople to understand. Keeping up with computer technology is difficult enough. Both fields are changing constantly, but law is even more complex, as it changes from state to state.

Figure B-1 in Appendix B shows an example of a contract you might want to use, with modifications, after joining the Independent Computer Consultants Association (ICCA). Read through the legal language in this figure, and then do Activity 1-5.





## Activity 1-5: Understanding a Consulting Contract

**Time Required:** 30 minutes

**Objective:** Increase your understanding of a consulting contract.

**Description:** For this activity, review the sample contract shown in Appendix B. This contract can't be used unless you're a member of the ICCA, but it's an excellent example of how a contract might be worded. After reading the contract, write a one-page summary discussing the areas you would modify or add to. Include areas important for a penetration tester that are missing, if any.



### Security Bytes

Because the job of an ethical hacker is fairly new, the laws are changing constantly. Even though a company has hired you to test its network for vulnerabilities, be careful that you aren't breaking any laws in your state or country. If you're worried that one of your tests might slow down the network because of excessive bandwidth use, that concern should signal a red flag. The company might consider suing you for lost time or monies caused by this delay.

## Ethical Hacking in a Nutshell

After reading all the dos and don'ts, you might have decided to go into a different profession. Before switching careers, however, take a look at the skills a security tester needs to help determine whether you have what it takes to do this job:

- *Knowledge of network and computer technology*—As a security tester, you must have a good understanding of networking concepts. You should spend time learning and reviewing TCP/IP and routing concepts and be able to read network diagrams. If you don't have experience working with networks, it's important that you start now. Being a security tester is impossible without a high level of expertise in this area. You should also have a good understanding of computer technologies and OSs. Read as much as you can on OSs in use today, paying particular attention to \*nix (UNIX and Linux) systems and Windows OSs because most security testing is done on these popular systems.
- *Ability to communicate with management and IT personnel*—Security testers need to be good listeners and must be able to communicate verbally and in writing with members of management and IT personnel. Explaining your findings to CEOs might be difficult, especially if they don't have a technical background. Your reports should be clear and succinct and offer constructive feedback and recommendations.
- *An understanding of the laws that apply to your location*—As a security tester, you must be aware of what you can and can't do legally. Gathering this information can be difficult when working with global companies, as laws can vary widely in other countries.
- *Ability to apply the necessary tools to perform your tasks*—Security testers must have a good understanding of tools for conducting security tests. More important, you must be able to think outside the box by discovering, creating, or modifying tools when current tools don't meet your needs.





### Security Bytes

If being liked by others is important to you, you might want to consider a different profession than security testing. If you're good at your job, many IT employees resent you discovering vulnerabilities in their systems. In fact, it's one of the only professions in which the better you do your job, the more enemies you make!



---

## Chapter Summary

- Many companies hire ethical hackers to perform penetration tests. The purpose of a penetration test is to discover vulnerabilities in a network. A security test is typically performed by a team of people with varied skills, sometimes referred to as a red team, and goes further to recommend solutions for addressing vulnerabilities.
- Penetration tests are usually conducted by using one of three models: white box model, black box model, and gray box model. The model the tester uses is based on the amount of information the client is willing to supply. In some tests, the client doesn't want the tester to have access to any of the company's information. In other words, the client is saying "Find out what you can about my company without my help."
- Security testers can earn certifications from multiple sources. The most popular certifications are CEH, CISSP, and OPST. Each certification requires taking an exam and covers different areas the tester must master. Because test requirements change periodically, visit the certification company's Web site to verify exam requirements.
- As a security tester or penetration tester, you must be aware of what you're legally allowed or not allowed to do. Contacting your local law enforcement agency is a good place to start before beginning any security testing.
- Your ISP might have an acceptable use policy in the contract you signed. It could limit your ability to use many of the tools available to security testers. Running scripts or programs not authorized by the ISP can result in termination of services.
- State and federal laws pertaining to computer crime should be understood before conducting a security test. Federal laws are applicable for all states, whereas state laws can vary. Being aware of the laws that apply is imperative.
- Get it in writing. As an independent contractor, having the client sign a written contract allowing you to conduct penetration testing before you begin is critical. You should also have an attorney read the contract, especially if you or the company representative made any modifications.
- You need to understand the tools available to conduct security tests. Learning how to use them should be a focused and methodical process.

---

## Key Terms

**black box model** A model for penetration testing in which management doesn't divulge to IT security personnel that testing will be conducted or give the testing team a description of the network topology. In other words, testers are on their own.

**Certified Ethical Hacker (CEH)** A certification designated by the EC-Council.

**Certified Information Systems Security Professional (CISSP)** Non-vendor-specific certification issued by the International Information Systems Security Certification Consortium, Inc. (ISC<sup>2</sup>).

**crackers** Hackers who break into systems with the intent of doing harm or destroying data.

**ethical hackers** Users who attempt to break into a computer system or network with the owner's permission.

**Global Information Assurance Certification (GIAC)** An organization founded by the SANS Institute in 1999 to validate the skills of security professionals. GIAC certifications encompass many areas of expertise in the security field.

**gray box model** A hybrid of the black box and white box models for penetration testing. In other words, the company might give a tester some information about which OSs are running but not provide any network topology information (diagrams of routers, switches, intrusion detection systems, firewalls, and so forth).

**hacker** A user who attempts to break into a computer system or network without authorization from the owner.

**Institute for Security and Open Methodologies (ISECOM)** A nonprofit organization that provides training and certification programs for security professionals.

**Open Source Security Testing Methodology Manual (OSSTMM)** This security manual developed by Peter Herzog has become one of the most widely used security-testing methodologies to date.

**OSSTMM Professional Security Tester (OPST)** An ISECOM-designated certification for penetration and security testers. *See also* Institute for Security and Open Methodologies (ISECOM).

**packet monkeys** A derogatory term for unskilled crackers or hackers who steal program code and use it to hack into network systems instead of creating the programs themselves.

**penetration test** In this test, a security professional performs an attack on a network with permission from the owner to discover vulnerabilities; penetration testers are also called ethical hackers.

**red team** A group of penetration testers who work together to break into a network.

**script kiddies** Similar to packet monkeys, a term for unskilled hackers or crackers who use scripts or programs written by others to penetrate networks.

**security test** In this test, security professionals do more than attempt to break into a network; they also analyze security policies and procedures, report vulnerabilities to management, and recommend solutions.

**SysAdmin, Audit, Network, Security (SANS) Institute** Founded in 1989, this organization conducts training worldwide and offers multiple certifications through GIAC in many aspects of computer security and forensics.


**white box model** A model for penetration testing in which testers can speak with company staff and are given a full description of the network topology and technology.



## Review Questions

1. The U.S. Department of Justice defines a hacker as which of the following?
  - a. A person who accesses a computer or network without the owner's permission
  - b. A penetration tester
  - c. A person who uses telephone services without payment
  - d. A person who accesses a computer or network system with the owner's permission
2. A penetration tester is which of the following?
  - a. A person who accesses a computer or network without permission from the owner
  - b. A person who uses telephone services without payment
  - c. A security professional who's hired to hack into a network to discover vulnerabilities
  - d. A hacker who accesses a system without permission but does not delete or destroy files
3. Some experienced hackers refer to inexperienced hackers who copy or use prewritten scripts or programs as which of the following? (Choose all that apply.)
  - a. Script monkeys
  - b. Packet kiddies
  - c. Packet monkeys
  - d. Script kiddies
4. What three models do penetration or security testers use to conduct tests?
5. A team composed of people with varied skills who attempt to penetrate a network is referred to as which of the following?
  - a. Green team
  - b. Blue team
  - c. Black team
  - d. Red team
6. How can you find out which computer crime laws are applicable in your state?
  - a. Contact your local law enforcement agencies.
  - b. Contact your ISP provider.
  - c. Contact your local computer store vendor.
  - d. Call 911.
7. What portion of your ISP contract might affect your ability to conduct a penetration test over the Internet?
  - a. Scanning policy
  - b. Port access policy
  - c. Acceptable use policy
  - d. Warrant policy

8. If you run a program in New York City that uses network resources to the extent that a user is denied access to them, what type of law have you violated?
  - a. City
  - b. State
  - c. Local
  - d. Federal
9. Which federal law prohibits unauthorized access of classified information?
  - a. Computer Fraud and Abuse Act, Title 18
  - b. Electronic Communication Privacy Act
  - c. Stored Wire and Electronic Communications and Transactional Records Act
  - d. Fifth Amendment
10. Which federal law prohibits intercepting any communication, regardless of how it was transmitted?
  - a. Computer Fraud and Abuse Act, Title 18
  - b. Electronic Communication Privacy Act
  - c. Stored Wire and Electronic Communications and Transactional Records Act
  - d. Fourth Amendment
11. Which federal law amended Chapter 119 of Title 18, U.S. Code?
  - a. Computer Fraud and Abuse Act, Title 18
  - b. Electronic Communication Privacy Act
  - c. Stored Wire and Electronic Communications and Transactional Records Act
  - d. U.S. Patriot Act, Sec. 217: Interception of Computer Trespasser Communications
12. To determine whether scanning is illegal in your area, you should do which of the following?
  - a. Refer to U.S. code.
  - b. Refer to the U.S. Patriot Act.
  - c. Refer to state laws.
  - d. Contact your ISP.
13. What organization offers the Certified Ethical Hacker (CEH) certification exam?
  - a. International Information Systems Security Certification Consortium (ISC<sup>2</sup>)
  - b. EC-Council
  - c. SANS Institute
  - d. GIAC

- 
14. What organization designates a person as a CISSP?
    - a. International Information Systems Security Certification Consortium (ISC<sup>2</sup>)
    - b. EC-Council
    - c. SANS Institute
    - d. GIAC
  15. What organization designates a person as an OPST?
    - a. International Information Systems Security Certification Consortium (ISC<sup>2</sup>)
    - b. EC-Council
    - c. SANS Institute
    - d. ISECOM
  16. As a security tester, what should you do before installing hacking software on your computer?
    - a. Check with local law enforcement agencies.
    - b. Contact your hardware vendor.
    - c. Contact the software vendor.
    - d. Contact your ISP.
  17. Before using hacking software over the Internet, you should contact which of the following? (Choose all that apply.)
    - a. Your ISP
    - b. Your vendor
    - c. Local law enforcement authorities to check for compliance
    - d. The FBI
  18. Which organization issues the Top 20 list of current network vulnerabilities?
    - a. SANS Institute
    - b. ISECOM
    - c. EC-Council
    - d. OPST
  19. A written contract isn't necessary when a friend recommends a client. True or False?
  20. A security tester should possess which of the following attributes? (Choose all that apply.)
    - a. Good listening skills
    - b. Knowledge of networking and computer technology
    - c. Good verbal and written communication skills
    - d. An interest in securing networks and computer systems



---

## Case Projects



### Case Project 1-1: Determining Legal Requirements for Penetration Testing

Alexander Rocco Corporation, a large real estate management company in Maui, Hawaii, has contracted your computer consulting company to perform a penetration test on its computer network. The company owns property that houses a five-star hotel, golf courses, tennis courts, and restaurants. Claudia Mae, the vice president, is your only contact at the company. To avoid undermining the tests you're conducting, you won't be introduced to any IT staff or employees. Claudia wants to determine what you can find out about the company's network infrastructure, network topology, and any discovered vulnerabilities, without any assistance from her or company personnel.

Based on this information, write a report outlining the steps you should take before beginning penetration tests of the Alexander Rocco Corporation. Research the laws applying to the state where the company is located, and be sure to reference any federal laws that might apply to what you have been asked to do.

### Case Project 1-2: Understanding the Rules of Engagement for Security Testers

You're a new security tester for Security Consulting Company (SCC). Before you go out on your first assignment, Shelley Canon, the vice president of SCC, wants you to read the rules of engagement section of the OSSTMM to make sure you don't violate any company policies.

Write a memo to Shelley Canon summarizing the OSSTMM's rules of engagement section (available on this book's DVD). The memo should describe the purpose of the rules of engagement and include answers to the following questions:

- When is releasing the names of past clients permissible?
- If you aren't able to penetrate a client's network, is offering your services free of charge permissible?
- When is conducting denial-of-service attacks on a client's network permissible?