Chapter 1

Introduction to Ethical Hacking

In This Chapter

- Understanding hacker objectives
- Outlining the differences between ethical hackers and malicious hackers
- Examining how the ethical hacking process has come about
- Understanding the dangers that your computer systems face
- Starting the ethical hacking process

This book is about hacking ethically — the science of testing your computers and network for security vulnerabilities and plugging the holes you find before the bad guys get a chance to exploit them.

Although ethical is an often overused and misunderstood word, the Merriam-Webster dictionary defines ethical perfectly for the context of this book and the professional security testing techniques that I cover — that is, conforming to accepted professional standards of conduct. IT practitioners are obligated to perform all the tests covered in this book aboveboard and only after permission has been obtained by the owner(s) of the systems — hence the disclaimer in the introduction.

How Hackers Beget Ethical Hackers

We’ve all heard of hackers. Many of us have even suffered the consequences of hacker actions. So who are these hackers? Why is it important to know about them? The next few sections give you the lowdown on hackers.

Defining hacker

Hacker is a word that has two meanings:

- Traditionally, a hacker is someone who likes to tinker with software or electronic systems. Hackers enjoy exploring and learning how computer systems operate. They love discovering new ways to work electronically.
Recently, *hacker* has taken on a new meaning — someone who maliciously breaks into systems for personal gain. Technically, these criminals are *crackers* (criminal hackers). Crackers break into (crack) systems with malicious intent. They are out for personal gain: fame, profit, and even revenge. They modify, delete, and steal critical information, often making other people miserable.

The good-guy (*white-hat*) hackers don’t like being in the same category as the bad-guy (*black-hat*) hackers. (These terms come from Western movies where the good guys wore white cowboy hats and the bad guys wore black cowboy hats.) Whatever the case, most people give *hacker* a negative connotation.

Many malicious hackers claim that they don’t cause damage but instead are altruistically helping others. Yeah, right. Many malicious hackers are electronic thieves.

In this book, I use the following terminology:

- **Hackers (or bad guys)** try to compromise computers.
- **Ethical hackers (or good guys)** protect computers against illicit entry.

Hackers go for almost any system they think they can compromise. Some prefer prestigious, well-protected systems, but hacking into anyone’s system increases their status in hacker circles.

**Ethical Hacking 101**

You need protection from hacker shenanigans. An *ethical hacker* possesses the skills, mindset, and tools of a hacker but is also trustworthy. Ethical hackers perform the hacks as security tests for their systems.

If you perform ethical hacking tests for customers or simply want to add another certification to your credentials, you may want to consider the ethical hacker certification Certified Ethical Hacker, which is sponsored by EC-Council. See [www.eccouncil.org/CEH.htm](http://www.eccouncil.org/CEH.htm) for more information.

Ethical hacking — also known as *penetration testing* or *white-hat hacking* — involves the same tools, tricks, and techniques that hackers use, but with one major difference: Ethical hacking is legal. Ethical hacking is performed with the target’s permission. The intent of ethical hacking is to discover vulnerabilities from a hacker’s viewpoint so systems can be better secured. It’s part of an overall information risk management program that allows for ongoing security improvements. Ethical hacking can also ensure that vendors’ claims about the security of their products are legitimate.
To hack your own systems like the bad guys, you must think like they think. It’s absolutely critical to know your enemy; see Chapter 2 for details.

**Understanding the Need to Hack Your Own Systems**

*To catch a thief, think like a thief.* That’s the basis for ethical hacking.

The law of averages works against security. With the increased numbers and expanding knowledge of hackers combined with the growing number of system vulnerabilities and other unknowns, the time will come when all computer systems are hacked or compromised in some way. Protecting your systems from the bad guys — and not just the generic vulnerabilities that everyone knows about — is absolutely critical. When you know hacker tricks, you can see how vulnerable your systems are.

Hacking preys on weak security practices and undisclosed vulnerabilities. Firewalls, encryption, and virtual private networks (VPNs) can create a false feeling of safety. These security systems often focus on high-level vulnerabilities, such as viruses and traffic through a firewall, without affecting how hackers work. Attacking your own systems to discover vulnerabilities is a step to making them more secure. This is the only proven method of greatly hardening your systems from attack. If you don’t identify weaknesses, it’s a matter of time before the vulnerabilities are exploited.

As hackers expand their knowledge, so should you. You must think like them to protect your systems from them. You, as the ethical hacker, must know activities hackers carry out and how to stop their efforts. You should know what to look for and how to use that information to thwart hackers’ efforts.

*Tip*

You don’t have to protect your systems from everything. You can’t. The only protection against everything is to unplug your computer systems and lock them away so no one can touch them — not even you. That’s not the best approach to information security. What’s important is to protect your systems from known vulnerabilities and common hacker attacks.

It’s impossible to buttress all possible vulnerabilities on all your systems. You can’t plan for all possible attacks — especially the ones that are currently unknown. However, the more combinations you try — the more you test whole systems instead of individual units — the better your chances of discovering vulnerabilities that affect everything as a whole.

Don’t take ethical hacking too far, though. It makes little sense to harden your systems from unlikely attacks. For instance, if you don’t have a lot of foot traffic
End of ebook preview
Download the full PDF tutorial from the link below:

Click Here