The previous examples represent some of the higher-profile incidents that have occurred, but for every news item or story that makes it into the public consciousness, many more never do. For every hacking incident that is made public, only a small portion of perpetrators are caught, and an even smaller number ever get prosecuted for cybercrime. In any case, hacking is indeed a crime, and those engaging in such activities can be prosecuted under any number of laws. The volume, frequency, and seriousness of attacks have only increased and will continue to do so as technology evolves even more.

Ethical Hacking and Penetration Testing

As a security professional, two of the terms you will encounter early on are *ethical hacker* and *penetration testing*. Today's security community includes different schools of thought on what constitutes each. It's important to separate and clarify these two terms to understand each and where they fit into the big picture.

Engaging in any hacking activity without the explicit permission of the owner of the target you are attacking is a crime, whether you get caught or not. From everything discussed so far, you might think that hacking is not something you can engage in legally or for any benign reason whatsoever, but this is far from the truth. It is possible to engage in hacking for good reasons (for example, when a network owner contracts with a security professional to hack systems to uncover vulnerabilities that should be addressed). Notice the important phrases "network owner contracts" and "explicit permission": *Ethical hackers engage in their activities only with the permission of the asset owner.*

> **NOTE**
> In today's environment, those wishing to become ethical hackers have many options that were unavailable before. They can pursue certification classes and participate in boot camps as part of a diverse development course to hone their skills. Always remember that the main characteristic that separates black hats from white hats is compliance with the law.

Once ethical hackers have the necessary permissions and contracts in place, they can engage in penetration testing, which is the structured and methodical means of investigating, uncovering, attacking, and reporting on a target system's strengths and vulnerabilities. Under the right circumstances, penetration testing can provide a wealth of information that the system owner can use to adjust defenses.

Penetration testing can take the form of black-box or white-box testing, depending on what is being evaluated and what the organization's goals are. **Black-box testing** is most often used when an organization wants to closely simulate how an attacker views a system, so no knowledge of the system is provided to the testing team. In **white-box testing**, advanced knowledge is provided to the testing team. In either case, an attack is simulated to determine what would happen to an organization if an actual attack had occurred.

Penetration tests are also commonly used as part of a larger effort commonly known as an IT audit, which evaluates the overall effectiveness of the IT systems controls that safeguard the organization. An IT audit is usually conducted against some standard or checklist that covers security protocols, software development, administrative policies, and IT governance. However, passing an IT audit does not mean that the system is completely secure, as audit checklists often trail new attack methods by months or years.

The Role of Ethical Hacking

An ethical hacker's role is to take the skills he or she has acquired and use that knowledge, together with an understanding of the hacker mindset, to simulate a hostile attacker. It often said that to properly and completely defend oneself against an aggressor, you must understand how that aggressor thinks, acts, and reacts. The idea is similar to military training exercises in which elite units are trained in the tactics of a hostile nation in order to give other units the ability to train and understand the enemy without risking lives.

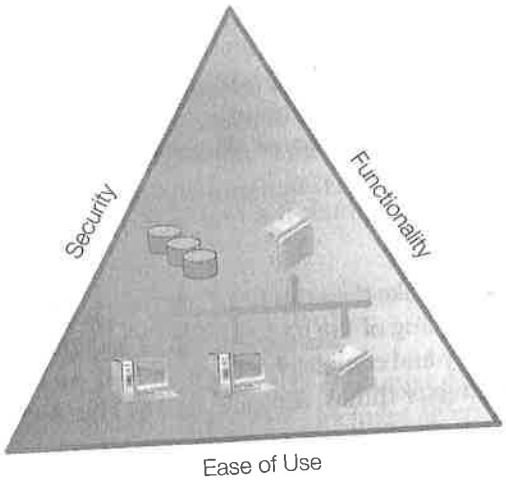
Here a few key points about ethical hacking that are important to the process:

- It requires the explicit permission of the "victim" before any activity can take place.
- Participants use the same tactics and strategies as regular hackers.
- It can harm a system if you don't exercise proper care.
- It requires detailed advance knowledge of the actual techniques a regular hacker will use.
- It requires that rules of engagement or guidelines be established prior to any testing.

> **NOTE**
> Ethical hackers can be employed to test a specific feature of a group of systems, or even the security of a whole organization. It depends on the specific needs of a given organization. In fact, some organizations keep people on staff specifically to engage in ethical hacking activities.

Under the right circumstances and with proper planning and goals, ethical hacking or penetration testing can provide a wealth of valuable information to the target organization ("client") about security issues that need addressing. The client should take these results, prioritize them, and take appropriate action to improve security. Effective security must still allow the system to provide the functionality and features needed for business to continue. However, a client may choose not to take action for a variety of reasons. In some cases, problems uncovered may be considered minor or low risk and left as is. If the problems uncovered require action, the challenge is to ensure that if security controls are modified or new ones put in place, existing usability is not decreased. Security and convenience are often in conflict with one another—the more secure a system becomes, the less convenient it tends to be (Figure 1-1). A great example of this concept is to look at authentication mechanisms. As a system moves from passwords to smartcards to biometrics, it becomes more secure—but at the same time users may have to take longer to authenticate, which may cause some disgruntlement.

FIGURE 1-1
Usability versus security.



From the theoretical side, ethical hackers are tasked with evaluating the overall state of something known as the C-I-A triad, which represents one of the core principles of security: to preserve confidentiality, integrity, and availability.

- **Confidentiality**—Safeguarding information or services against disclosure to unauthorized parties
- **Integrity**—Ensuring that information is in its intended format or state; in other words, ensuring that data is not altered
- **Availability**—Ensuring that information or a service can be accessed or used whenever requested

Another way you can view the C-I-A triad is to turn it on its head. You can call this the anti–C-I-A triad, which shows the threats to each part of C-I-A. What an ethical hacker must do is strive to maintain the integrity of C-I-A and not let any of the elements of the anti-triad take hold:

- **Disclosure**—Information is accessed in some manner by an unauthorized party.
- **Alteration**—Information is maliciously or accidentally modified in some manner.
- **Disruption**—Information and/or services are not accessible or usable when called upon.

An ethical hacker is tasked with ensuring that the C-I-A triad is preserved and threats are dealt with adequately (as required by the organization's own rules). For example, consider what could result if a health care organization lost control of (or could not provide access to) sensitive information about patients. Such situations typically result in civil and criminal actions.

Figure 1-2 shows the C-I-A triad.