PART I

Hacker Techniques and Tools

CHAPTER 1

Hacking: The Next Generation

MANY OF TODAY'S NEWS STORIES RELATED to cybersecurity focus on attackers—what they do and the consequences of their actions. In this text, we will cover a wide range of techniques and technologies that attackers use to compromise a system. But before we dive into the details, it is important to first understand who these attackers are and why they do what they do.

During the early generations of digital computing (way back in the 1960s), learning about computing wasn't easy. In many cases, you had to build your own computer! A group of individuals emerged who were passionately interested in learning all they could about computers. They learned about hardware, software, and how to connect devices and communicate. Their often-imprecise methods of building and accessing devices earned them the moniker **hackers**. The first generation of hackers were individuals who are called "geeks," or technology enthusiasts, today. These early hackers went on to create the foundation for technologies such as the Advanced Research Projects Agency Network (ARPANET), which paved the way for the Internet. They also initiated many early software-development movements that led to what is known today as *open source*. Hacking was motivated by intellectual curiosity; causing damage or stealing information was "against the rules" for this small number of people.

In the 1980s, hackers started to gain more of the negative connotations by which the public now identifies them. Movies such as *WarGames* and media attention altered the image of a hacker from a technology enthusiast to a computer criminal. During this time, hackers engaged in activities such as theft of service by breaking into phone systems to make free phone calls. Books such as *The Cuckoo's Egg* and the emergence of magazines such as *Phrack* cast even more negative light on hackers. In many respects, the 1980s formed the basis for how a hacker is perceived today.

Chapter 1 Topics

This chapter covers the following topics and concepts:

- What the motives of different types of hackers are
- What a look at the history of computer hacking shows
- What ethical hacking and penetration testing are

- What common hacking methodologies are
- How to perform a penetration test
- What the roles of ethical standards and the law are

Chapter 1 Goals

When you complete this chapter, you will be able to:

- Distinguish the different motives of hackers and determine the basis of their attacks
- Describe the history of hacking
- Explain the evolution of hacking
- Explain why information systems and people are vulnerable to manipulation
- Differentiate between hacking, ethical hacking, penetration testing, and auditing
- Identify the motivations, skill sets, and primary attack tools used by hackers
- Compare the steps and phases of a hacking attack to those of a penetration test
- Explain the difference in risk between inside and outside threats and attacks
- Review the need for ethical hackers
- State the most important step in ethical hacking
- Identify important laws that relate to hacking

Profiles and Motives of Different Types of Hackers

Over the past three decades, the definition of what a hacker is has evolved quite a bit from what was accepted in the 1980s and even the 1990s. Current hackers defy easy classification and are best understood by looking at the motivations for their actions. Although there is no comprehensive list of the types of today's hackers, here is a general list of categories of their motivations (you'll learn more about each type of hacker in a later section in this chapter):

- **Good guys**—Information security (InfoSec) professionals who engage in hacking activities to uncover vulnerabilities in hopes of fixing them and making systems more secure.
- **Amateurs**—Entry-level hackers who do not possess their own advanced skills but rather use only scripts and software written by more experienced hackers.
- **Criminals**—Hackers who routinely use malicious software and devices to carry out illegal activities primarily for the purpose of financial gain.
- **Ideologues**—Hackers who carry out their activities to achieve ideological or political goals.

NOTE

Don't let the term "good guys" throw you. It doesn't actually imply that only one gender is a good fit for being an exceptional InfoSec professional. Some of the best InfoSec people with whom I have worked are not "guys."

Most of today's organizations have quickly learned that they can no longer afford to underestimate or ignore the threat attackers pose. Organizations of all sizes have learned to reduce threats through a combination of technical, administrative, and physical measures designed to address a specific range of problems. Technical measures include devices and techniques such as virtual private networks (VPNs), cryptographic protocols, **intrusion detection systems (IDSs)** or **intrusion prevention systems (IPSs)**, access control lists (ACLs), biometrics, smart cards, and other devices. Administrative controls include policies, procedures, and other rules. Physical measures include devices such as cable locks, device locks, alarm systems, and other similar devices. Although any of these devices or controls may be expensive, they will likely be cheaper and more effective than the cost and effort required to clean up after a successful attack.

FYI

People who break the law or break into systems without authorization are more correctly known as **crackers**. The media do not usually make this distinction because "hacker" has become such a universal term. However, there are many experienced hackers who never break the law and who define hacking as producing an outcome that the system's designers never intended or anticipated. In that respect, Albert Einstein can be considered to have "hacked" Newtonian physics. In the interest of simplicity, this book will use the term "hacker" to describe those who are either productive or destructive.

While discussing attacks and attackers, InfoSec professionals must be thorough when assessing and evaluating threats by also considering where they originate. When evaluating the threats against an organization and possible sources of attack, always consider the fact that attackers can come from both outside and inside the organization. A single disgruntled employee can cause tremendous damage because he or she is an approved user of the system. Although you will likely see many more external attacks, a malicious insider may go unnoticed longer and have some level of knowledge of how things work ahead of time, which can result in a more effective attack.

Controls

Each organization is responsible for protecting itself from risks by determining the controls that will be most effective in reducing or mitigating the threats it faces. One approach to developing a balanced and effective strategy to selecting security controls is the TAP principle. TAP is an acronym for technical, administrative, and physical, the three types of controls you can use to mitigate risk. Here's a look at each type, with a few examples:

- **Technical**—Technical controls take the form of software or hardware devices, such as firewalls, proxies, IDSs, IPSs, biometric **authentication**, permissions, auditing, and similar technologies.

NOTE

Never underestimate the damage a determined individual can do to computer systems. For example, the 2017 Cost of Cyber Crime Study by IBM and the Ponemon Institute found that breaches have cost the reporting large organizations a global annualized average of $11.7 million *each*. You can find this report at *www.accenture.com/us-en/insight-cost-of-cybercrime-2017*.

NOTE

Attacks depend on one or more weaknesses that exist in a system. Each weakness is referred to as a **vulnerability**. An **exploit** refers to a piece of software, a tool, or a technique that targets or takes advantage of a vulnerability—leading to privilege escalation, loss of integrity or confidentiality, or denial of service on a computer system or resource.

- **Administrative**—Administrative controls take the form of policies and procedures. An example is a password policy that defines what makes a good password. In numerous cases, administrative controls also fulfill legal requirements, such as policies that dictate privacy of customer information. Other examples of administrative policy include the rules governing actions taken when hiring and firing employees.
- **Physical**—Physical controls are those that protect assets from traditional threats such as theft or vandalism. Mechanisms in this category include doors, locks, cameras, security guards, lighting, fences, gates, and other similar devices.

The Hacker Mindset

Depending on whom you ask, you can get a wide range of responses from hackers on how they view their actions. In fact, many hackers, like other individuals who break rules or laws for various reasons, have their own codes of ethics that they hold sacred. In defense of their actions, hackers have been known to cite various justifications, including the following:

- **The notion of victimless crime**—Because humans are not the direct targets, there's nothing wrong with committing the crime. (Of course, this justification doesn't apply to attacks that actually do target individuals.)
- **The Robin Hood ideal**—Stealing software and other media from "rich" companies and delivering them to the "poor" consumers via methods such as BitTorrent is okay because the target companies have plenty of money.
- **National pride and patriotism**—Similar to the anti-establishment Robin Hood mentality, patriotic hackers may seek to upset the balance of national power, hacking to disrupt the due process of an adversary and/or bolster the opinion of their own country.
- **The educational value of hacking**—Essentially, it is okay to commit a crime as long as one is doing it to learn.
- **Curiosity**—Breaking into a network is okay as long as you don't steal or change anything.

NOTE

Although the mere act of writing malicious computer software, such as a virus or ransomware, is not illegal, releasing it into the "wild" *is* illegal.

Another example of attempting to explain the ethics applied to hackers is known as the hacker ethic. This set of standards dates back to Steven Levy in the 1980s. In the preface of his book *Hackers: Heroes of the Computer Revolution*, Levy states the following:

- Access to computers and anything that might teach you something about the way the world works should be unlimited and total.
- All information should be free.
- Authority should be mistrusted, and decentralization should be promoted.

NOTE

Although it is true that applications or data can be erased or modified, worse scenarios can happen under the right circumstances. For example, consider what could happen if someone broke into a system such as a 911 emergency service and then maliciously or accidentally took it down.

- Hackers should be judged by their hacking, not criteria such as degrees, age, race, gender, or position.
- You can create art and beauty on a computer.
- Computers can change your life for the better.

Motivation

Ethics are an important component in understanding hackers, but far from the only component. One must also consider motivation. Anyone who has watched one of the many television shows that focus on solving crimes knows that there are three things needed to commit a crime:

- **Means**—Does the attacker possess the ability to commit the crime in question?
- **Motive**—Does the attacker have a reason to commit the crime?
- **Opportunity**—Does the attacker have the necessary access and time to commit the crime?

Focusing on the second point—motive—helps better understand why an attacker might engage in hacking activities. The early "pioneers" of hacking engaged in those activities almost exclusively out of curiosity. Today's hackers can have any number of motives, many of which are similar to the motives for committing traditional crimes:

- **Beneficial contribution**—Hackers with this motive are not criminals. White-hat hackers, also called ethical hackers, are InfoSec professionals who engage in hacking activities to help make their organization's systems more secure. They try to attack their systems like attackers would to uncover vulnerabilities that can be mitigated before malicious attacks can succeed. The two main differences between ethical hackers and unethical hackers is that ethical hackers have permission to carry out their activities, and they do so to make their organizations more secure.
- **Status/validation**—New hackers nearly always learn the ropes by running prepackaged scripts and programs written by more experienced hackers. These tools require very little sophistication and make it easy for inexperienced hackers to cause damage. These new hackers with limited original skills are generally referred to as script kiddies. As these hackers gain more skills, they often modify existing exploits and eventually write their own malicious software. Many of today's hackers start out to make a name for themselves. Each successful attack gives them more status and elevates their reputation in the eyes of established hackers. For many hackers, this recognition is all they really want—at least at first.
- **Monetary gain**—Most of today's malicious attacks are specifically targeted to either generate revenue for the attacker or deny revenue to the target. Attacks can provide access to financial resources or to valuable data that can be resold, deny resources or processes that generate revenue, or deny access to resources that can be held for ransom. In any case, money is at the heart of the motivation for this type of hacker, which can include malicious insiders, individual criminals, organized crime organizations, or cybermercenaries.
- **Ideology**—Hackers in this last category of motivations use technology to achieve ideological goals. Hackers who use malicious software to carry out activist attacks have given rise to the label of hacktivists. But hacktivists aren't the only actors in this category. Nationalists and nation-state actors are also motivated by ideology. Their attacks are carried out

Hacktivism

A relatively new form of hacking is the idea of hacking on behalf of a cause. In the past, hacking was done for a range of different reasons that rarely included social expression. Over the past decade, however, there have been an increasing number of security incidents with roots in social or political activism. Examples include defacing websites of public officials, candidates, or agencies that an individual or group disagrees with or performing denial of service (DoS) attacks against corporate websites. With the rise of social media and microblogging, hacktivism can also manifest as simply spreading rumors and false stories. Hacktivists generally focus on attacks that cause widespread disruption as opposed to financial gain.

to promote a particular agenda. Actors who operate in this area are often those with the most advanced skills and greatest financial backing. For this reason, these types of hackers tend to be the most sophisticated and dangerous, resulting in grave, global consequences.

A Look at the History of Computer Hacking

Typical early hackers were curious about the new technology of networks and computers and wanted to see just how far they could push their capabilities. Hacking has changed quite a bit since then. For example, in the 1970s, before the widespread availability of the personal computer, hacking was mostly confined to mainframes that were common in corporate and university environments. When personal computers (PCs) became widely available in the 1980s, every user had a copy of an operating system. Hackers soon realized that a hack that worked on one PC would work on nearly every other PC as well. Although the first Internet worm in November 1988 exploited a weakness in the UNIX `sendmail` command, worm and virus writers moved their attention to the world of PCs, where most infections occur today.

As hackers' skills and creativity evolved, so did their attacks. The first web browser, Mosaic, was introduced in 1993. By 1995, hackers were defacing websites. Some of the earliest hacks were quite funny, if not somewhat offensive or vulgar. By May 2001, websites were hacked at such a rate that the group that documented them gave up trying to keep track (see *http://attrition.org/mirror/attrition/*).

By the turn of the century, hacks started to progress from pranks to malicious activity. DoS attacks took out companies' Internet access, affecting stock prices and causing financial damage. As websites began to process more credit card transactions, their back-end databases became prime targets for attacks. As computer crime laws came into being, the bragging rights for hacking a website became less attractive—sure, a hacker could show off to friends, but that didn't produce a financial return. With online commerce, skills started going to the highest bidder, with crime rings, organized crime, and nations with hostile interests utilizing the Internet as an attack route.

Numerous products emerged in the 1990s and early 2000s—antivirus, firewalls, IDSs, and remote access controls—each designed to counter an increasing number of new and diverse threats. As technology, hackers, and countermeasures improved and evolved, so did

the types of attacks and strategies that initially spawned them. Attackers started introducing new threats in the form of worms, spam, spyware, adware, and rootkits. These attacks went beyond harassing and irritating the public; they also caused widespread disruptions by attacking the technologies that society increasingly depended on.

Hackers also started to realize that it was possible to use their skills to generate money in all sorts of interesting ways. For example, attackers used techniques to redirect web browsers to specific pages that generate revenue for themselves. Spammers send out thousands upon thousands of email messages that advertise a product or service. Because sending out bulk email costs mere pennies, it takes only a small number of purchasers to make a nice profit.

Over the past few years, the hacking community has adopted a new team ethic or work style. In the past, it was normal for a "lone wolf" type to engage in hacking activities. Over the past few years, a new pattern of a collective or group effort has emerged. Attackers found that working together can provide greater results than one individual carrying out an attack. Such teams increase their effectiveness not only by sheer numbers, diversity, or complementary skills but also by adding clear leadership structures. Also of concern is the trend in which groups of hackers receive financing from nefarious or resourceful sources, such as criminal organizations, terrorists, or even foreign governments. The proliferation of and increasing dependence on technology has proved it to be an irresistible target for criminals.

FYI

In the 1960s, Intel scientist Gordon Moore noted that the density of transistors was doubling every 18 to 24 months. Because computing power is directly related to transistor density, the statement "computing power doubles every 18 months" became known as Moore's Law. Cybersecurity author and expert G. Mark Hardy has offered a corollary for security professionals, known as G. Mark's Law: "Half of what you know about security will be obsolete in 18 months." Successful security professionals commit to lifelong learning.

As stated earlier, hacking is by no means a new phenomenon; it has existed in one form or another since the 1960s. It is only for a portion of the time since then that hacking has been viewed as a crime and a situation that must be addressed.

Although the media commonly cover successful cybersecurity attacks, 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 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 increased and will continue to do so as technology and techniques evolve.

Ethical Hacking and Penetration Testing

As an InfoSec professional, two of the terms you will encounter early on are **ethical hacker** and **penetration testing**. Today's InfoSec community includes different schools of thought on

NOTE

Engaging in any hacking activity without the explicit permission of the owner of the target you are attacking is a crime whether or not you get caught. And the only way to prove that you have explicit permission is to get it in writing—before you start! InfoSec professionals often call this written permission their "get out of jail free card."

NOTE

Anyone wishing to become an ethical hacker has many options that were unavailable before. Many commercial organizations and academic institutions offer classes that prepare students for a variety of related certifications. The most popular certification organizations that offer hacking-related certifications include the EC-Council (*www.eccouncil.org/*), SANS Institute (*www.giac.org/*), and Offensive Security (*www.offensive-security.com/*). A quick Internet search will return more certifications, but these will give you a start toward becoming an experienced white-hat hacker. Always remember that the main characteristic that separates black hats (hackers who attempt to attack systems) from white hats (security professionals who use hacking skills to protect systems) is compliance with the law.

the precise definition of each term. It's important to separate and clarify these two terms to understand each one and how they fit into the big picture.

From everything discussed so far, you might think that hacking is not something you can engage in legally or for any positive or helpful 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 an InfoSec 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 (should be written) of the asset owner*.

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, identifying, 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 attacker initiated one or more attacks.

Penetration tests are also commonly used as part of a larger effort to evaluate the overall effectiveness of the information technology (IT) system controls that safeguard the organization. Penetration testing is often confused with vulnerability assessments. However, the two have quite different goals. The primary goal of a penetration test is to determine whether a specific resource can be compromised. If the testers find a single weak access point, they will exploit that weakness. On the other hand, a vulnerability assessment is a survey of a system to identify as many vulnerabilities as possible. While penetration testing may accompany a vulnerability assessment, the two activities are different.

Another common activity to help enhance the security of an environment is an IT security audit. An IT security audit is usually conducted against some standard or checklist that covers security protocols, software development, administrative policies, and IT governance. The audit determines whether the organization's deployed controls align with the security policy. It also often evaluates the security policy for alignment with best practices, regulations, and legislation. However, passing an IT audit does not mean that the system is completely secure because 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 is 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 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, strategies, and tools as malicious hackers.
- It can harm a system if you don't exercise proper care. (And sometimes even when you do.)
- It requires detailed advance knowledge of the actual techniques a malicious hacker will use.
- It requires that rules of engagement or guidelines be established prior to any 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 to be addressed. 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 processes to continue. However, a client may choose not to act for a variety of reasons. In some cases, problems uncovered may be considered minor or low risk and left as is. Alternatively, some problems have such a minimal effect that protecting the environment is costlier than any minor loss. 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 smart cards to biometrics, it becomes more secure—but at the same time, users may have to take longer to authenticate, which may cause increasing frustration.

NOTE

Ethical hackers can be employed to test a specific aspect of a group of systems or even the security of a whole organization's environment. In fact, a new range of opportunities exist for people who like to find software bugs. These specialists are called bug bounty hunters and are compensated by software development organizations for the bugs they find *before* their customers find them. The scope of the activities depends on the specific goals of a given organization. In fact, some organizations keep people on staff specifically to engage in ethical hacking activities as an ongoing effort to support secure environments. Other organizations choose to outsource these tasks to organizations that provide threat intelligence services.

Ethical Hackers and the C-I-A Triad

Ethical hackers are tasked with evaluating the overall state of the foundational tenets of InfoSec, commonly depicted as the C-I-A triad, which represents information confidentiality, integrity, and availability. **FIGURE 1-2** shows the C-I-A triad.

- **Confidentiality**—Ensuring that only authorized subjects can access protected data
- **Integrity**—Ensuring that only authorized subjects can modify protected data
- **Availability**—Ensuring that information and the resources that manage information are available on demand to authorized subjects

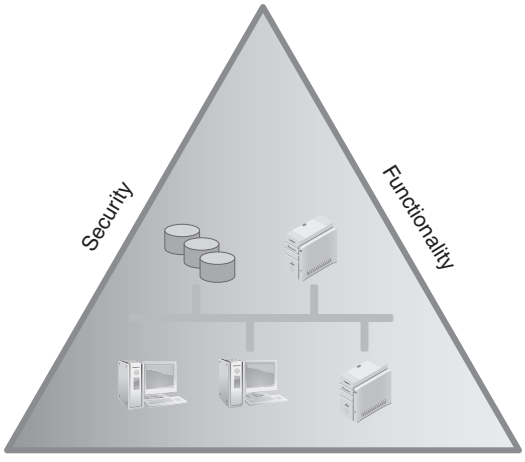

FIGURE 1-1
Usability versus security.

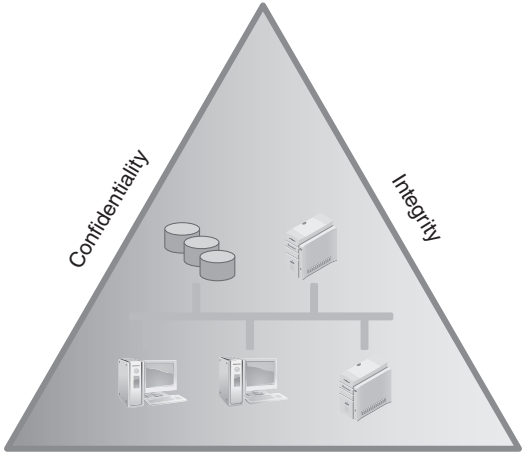

FIGURE 1-2
The C-I-A triad.

Another way you can view the C-I-A triad is to consider the inverse of each security property. You can call this the anti–C-I-A triad, which shows the threats to each part of C-I-A. An ethical hacker must strive to maintain the integrity of C-I-A and not let any of the elements of the anti-triad occur:

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

Part of ethical hacking is identifying assets, risks, vulnerabilities, and threats. From an InfoSec perspective, not all assets are created equal and do not have equal value for an organization. By definition, assets possess some value to a given organization. Asset owners evaluate each asset to determine how important it is relative to other assets and to the company as a whole. Next, the ethical hacker identifies potential threats and determines the capability of each threat to cause harm to the assets in question. Once assets and potential threats are identified, the ethical hacker thoroughly and objectively evaluates and documents each asset's vulnerabilities in order to understand potential weaknesses. Note that a vulnerability exists only if a particular threat can adversely affect an asset if exploited. Finally, the ethical hacker performs a risk determination for each asset individually and overall to determine the probability that a security incident could occur, given the threats and vulnerabilities in question. In a sense, risk is comparable to an individual's pain threshold—different individuals can tolerate different levels of pain. Risk is the same—each organization has its own tolerance of risk even if the threats and vulnerabilities are the same.

Common Hacking Methodologies

A hacking methodology refers to the step-by-step approach an attacker uses to attack a target. There is no one specific step-by-step approach that all hackers use. A major difference between a malicious hacker and an ethical hacker is the code of ethics to which each subscribes.

Hacking methodology generally includes the following steps (**FIGURE 1-3**):

1. **Reconnaissance**—An attacker passively acquires information about the intended victim and/or the intended victim's systems. The purpose of reconnaissance is to identify one or more potential entry points into a target environment. This phase includes both passive information gathering, in which no active interaction occurs between the attacker and the victim (for example, conducting a Whois query), and potential exploratory contact with the victim (as in phishing emails).
2. **Scanning**—An attacker takes the information obtained during the reconnaissance phase and uses it to actively acquire more detailed information about a victim. For example, an attacker might conduct a ping sweep of all the victim's known Internet Protocol (IP) addresses (i.e., all IP addresses the attacker can associate with the intended victim) to see which machines respond. The scanning phase then proceeds with efforts to extract more detailed information from the discovered systems that appear interesting. Most activities at this point are focused on identifying weaknesses in target systems. Results of this phase can include lists of users, groups, applications, configuration settings, known vulnerabilities, and other similar information.
3. **Infiltration and escalation**—Using information acquired in the previous phase, the attacker will attempt to exploit one or more identified vulnerabilities. Most activities in this phase have the goal of gaining access to a resource and then escalating access privileges to allow the attacker to move freely around a system or environment. Once sufficiently elevated privilege is obtained, the attacker can carry out the most damaging phases of the attack.

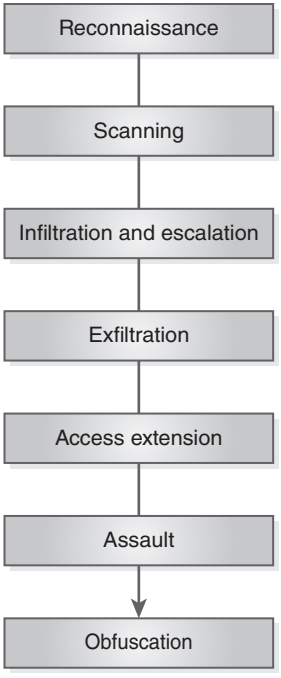

FIGURE 1-3
Hacking steps.

4. **Exfiltration**—Once the attacker attains elevated or even unrestricted access to an environment, he or she can access protected resources and data. Access can be to quietly extract data, modify or delete sensitive files, or obtain configuration information. The actions taken during this phase depend on the attacker's goals for the attack.
5. **Access extension**—Most attackers want the ability to return to a victim's system at some point in the future. Many attacks are iterative and rely on multiple actions. To make it easy to re-access a victim's systems, most attackers install additional exploits during this phase. An attacker may install a rootkit or other tools to provide easier silent access for future visits. Once these new exploits are in place, the attacker can get back into systems with elevated privileges with very little effort.
6. **Assault**—This phase is not present in all attacks. If the goal of an attack is to exfiltrate confidential data, an attacker will likely skip any overt destructive actions. Although exfiltration can occur silently, assault leaves no question that an attack is in progress. The assault phase is the place in an attack where the most damage occurs. An attacker could remove or modify critical configuration files to alter the way in which a computer or device operates. Likewise, the attacker could change data or programs to alter the way physical devices are directed to operate as well. In short, the assault phase is where the attacker who really wants to cause damage operates.
7. **Obfuscation**—This is also an optional, although common, phase. Some attackers want the whole world to know they struck and caused damage. However, many other attackers want to quietly do their work and hopefully get away without alerting anyone to their activities. For attackers who want to be clandestine, this last phase is one in which they cover their tracks. With elevated privileges, attackers can often modify log files and other

artifacts of their activities or install additional malware to erase any traces of their presences. This makes it difficult to track attackers and subsequently stop them from launching further attacks.

Performing a Penetration Test

A penetration test is an integral part of ethical hacking. Although ethical hacking sometimes occurs without formal rules of engagement, penetration testing does require rules to be agreed upon in advance. If an ethical hacker chooses to perform a penetration test without having certain parameters determined ahead of time, a wide range of unpleasant outcomes can ensue. For example, not having the rules established prior to engaging in a test could result in criminal or civil charges, depending on the injured party and the attack involved. It is also entirely possible that without clearly defined rules, an attack may result in shutting down systems or services and completely stopping a company's operations.

National Institute of Standards and Technology Publication 800-115 (NIST 800-115), *Technical Guide to Information Security Testing and Assessment*, describes penetration testing as a four-step process, as shown in **FIGURE 1-4**.

When the organization decides to carry out a penetration test, the ethical hacker should pose certain questions to establish goals. During this phase, the aim should be to clearly determine why a penetration test and its associated tasks are necessary. These questions include the following:

- Why is a penetration test deemed necessary?
- What is the function or mission of the organization to be tested?
- What are the limits or rules of engagement for the test?
- What data and services will the test include?
- Who is the data owner?
- What results are expected at the conclusion of the test?
- What will be done with the results when presented?
- What is the budget?
- What are the expected costs?
- What resources will be made available?
- What actions will be allowed as part of the test?
- When will the tests be performed?

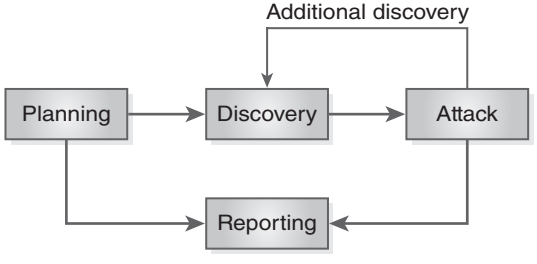

FIGURE 1-4
Ethical hacking steps.

- Will insiders be notified?
- Will the test be performed as black or white box?
- What conditions will determine the test's success?
- Who are the emergency contacts?

Penetration testing can take several forms. The ethical hacker must decide, along with the client, which tests are appropriate and will yield the results the client seeks.

Tests that can be part of a penetration test include the following:

- **Technical attack**—Designed to simulate an attack against technology from either the inside or the outside, depending on the goals and intentions of the client.
- **Administrative attack**—Designed to find loopholes or shortcomings in how tasks and operational processes are performed.
- **Physical attack**—Includes anything that targets physical equipment and facilities with actions such as theft, breaking and entering, or similar actions. Can also include actions against people, such as social engineering–related threats.

After the organization and the ethical hacker have discussed each test, determined its suitability, and evaluated its potential advantages and side effects, they can finalize the planning and contracts and perform the testing (**FIGURE 1-5**).

NOTE

There are many software packages available to pen testers, as they are known, that can ease the process of gathering vital information from the target and organizing attack activities. A simple Internet search for "penetration testing software" will provide a good starting point for researching available tools.

When performing a penetration test, the team should generally include members with different but complementary skills from the business and technical domains. When the rules of the test have been determined, the team is selected based on the intended tests it will perform and goals it will address. Expect a team to include diverse skill sets, including detailed knowledge of routers and routing protocols, organizational policies, and even legal requirements. Technical team members should also share some skills, such as knowledge of networking, Transmission Control Protocol/Internet Protocol (TCP/IP), and similar technologies.

Another important aspect of the test is whether personnel will have any knowledge that the test is being performed. In some cases, having personnel unaware of the test will yield valuable insight into how they respond to incidents. This helps the organization evaluate the effectiveness of their security awareness training.

As penetration testing becomes more prevalent, several methodologies and frameworks are available to help formalize organizational efforts. The following list includes

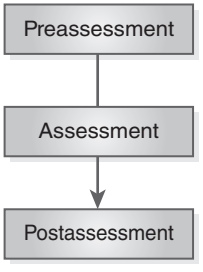

FIGURE 1-5
Ethical hacking test steps.

FYI

Do you want your penetration test to be realistic? When an organization's personnel are not provided with information about a pending or an in-progress test, they are more likely to respond as if a real attack were occurring. This is an excellent way to check whether training results in changed behavior. For example, if employees do not challenge strangers conducting a penetration test, they are unlikely to challenge a real intruder.

some of the more popular currently available resources for developing penetration testing procedures:

- NIST SP 800-115, "Technical Guide to Information Security Testing and Assessment" (http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-115.pdf)
- NIST SP 800-53A Revision 4, "Assessing Security and Privacy Controls in Federal Information Systems and Organizations" (http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53Ar4.pdf)
- "Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process" (www.cert.org/resilience/products-services/octave/)
- *Open Source Security Testing Methodology Manual* (OSSTMM) (www.isecom.org/research/)
- Penetration Testing Execution Standard (PTES) Technical Guidelines (www.pentest-standard.org/index.php/PTES_Technical_Guidelines)

The Role of the Law and Ethical Standards

When an ethical hacker engages in any hacking-related activity, it is essential that he or she know all applicable laws or seek assistance to determine what the laws may be. Never forget that because of the nature of the Internet and computer crime, it is entirely possible for any given crime to stretch over multiple local and international jurisdictions, potentially frustrating any attempts to prosecute it. Additionally, prosecution can be stymied by the legal systems of different countries in which a mix of religious, military, criminal, and civil laws exist. Successful prosecution requires knowledge of the legal systems in multiple jurisdictions.

NOTE

NIST Special Publication (SP) 800-53A, Revision 4, *Assessing Security and Privacy Controls in Federal Information Systems and Organizations*, specifically requires penetration testing and that ethical hackers exploit vulnerabilities and demonstrate the effectiveness of in-place security and privacy controls.

Ethical hackers should exercise proper care not to violate the rules of engagement because doing so can have serious repercussions. Once a client has determined what the goals and limitations of a test will be and contracted with the ethical hacker, the ethical hacker must carefully adhere to the stated scope. Remember two very important points when considering exceeding scope or violating stated guidelines:

- **Trust**—The client is placing trust in the ethical hacker to use the proper discretion when performing tests. If an ethical hacker breaks this trust, it can degrade trust in other project aspects, such as the reported results of tests.

- **Legal implications**—Violating limits defined by the permitted scope of testing may be sufficient cause for a client to take legal action against the ethical hacker. In fact, if violating test scope results in damages, the client may be compelled to take legal action.

An ethical hacker should have a basic knowledge of the current laws, regulations, and directives that affect penetration testing activities. Although these requirements change with time, here is a basic list of the most common set of requirements you may encounter (Note that this list includes requirements from only the United States. There are many more laws, regulations, and directives from other countries. Make sure you are aware of the requirements in effect for your jurisdiction.):

- 1973 US Code of Fair Information Practices governs the maintenance and storage of personal information by data systems, such as health and credit bureaus.
- 1974 US Privacy Act governs the handling of personal information by the US government.
- 1984 US Medical Computer Crime Act addresses illegally accessing or altering medication data.
- 1986 (amended in 1996) US Computer Fraud and Abuse Act includes issues such as altering, damaging, or destroying information in a federal computer and trafficking in computer passwords if it affects interstate or foreign commerce or permits unauthorized access to government computers.
- 1986 US Electronic Communications Privacy Act prohibits eavesdropping or the interception of message contents without distinguishing between private and public systems.
- 1994 US Communications Assistance for Law Enforcement Act requires all communications carriers to make wiretaps possible.
- 1996 US Kennedy-Kassebaum Health Insurance and Portability Accountability Act (HIPAA) (with additional requirements added in December 2000) addresses the issues of personal health care information privacy and health plan portability in the United States.
- 1996 US National Information Infrastructure Protection Act (enacted in October 1996 as part of Public Law 104-294) amended the Computer Fraud and Abuse Act, which is codified in 18 USC § 1030. This act addresses the protection of the confidentiality, integrity, and availability of data and systems. This act is intended to encourage other countries to adopt a similar framework, thus creating a more uniform approach to addressing computer crime in the existing global information infrastructure.
- 2002 Sarbanes-Oxley Act (SOX) is a corporate governance law that affects public corporations' financial reporting. Under SOX, corporations must certify the accuracy and integrity of their financial reporting and accounting.
- 2002 Federal Information Security Management Act (FISMA) requires every US federal agency to create and implement an InfoSec program to protect the information and information systems that agency uses. This act also requires agencies to conduct annual reviews of their InfoSec program and submit results to the Office of Management and Budget (OMB).
- 2014 Federal Information Security Modernization Act (FISMA 2014) updates requirements placed by FISMA 2002, particularly surrounding the Department of Homeland Security authority. This act amends OMB oversight over InfoSec practices and seeks to reduce "inefficient and wasteful reporting" to the OMB.

CHAPTER SUMMARY

This chapter addressed ethical hacking and its value to the InfoSec professional. Ethical hackers are individuals who possess skills comparable to regular hackers, but ethical hackers engage in their activities only with permission and in efforts that contribute to the requesting organization's overall security. Ethical hackers attempt to use the same skills, mindset, and motivation as a hacker to simulate an attack by an actual hacker while at the same time allowing for the test to be more closely controlled and monitored. Ethical hackers are professionals who work within the confines of a set of rules of engagement that are never exceeded, lest they find themselves facing potential legal action.

Conversely, regular hackers may not follow the same ethics and limitations of ethical hackers. Regular hackers may work without ethical limitations, and the results they can achieve are restricted only by the means, motives, and opportunities that are made available. Finally, hacking that is not performed under contract is considered illegal and is treated as such. By its very nature, hacking activities can easily cross state and national borders into multiple legal jurisdictions.

KEY CONCEPTS AND TERMS

Asset
Authentication
Black-box testing
Cracker
Ethical hacker
Exploit
Hacker
Intrusion detection systems (IDSs)
Intrusion prevention systems (IPSs)
Penetration testing
Vulnerability
White-box testing

CHAPTER 1 ASSESSMENT

1. Which of the following represents a valid ethical hacking test methodology?

A. HIPAA
B. RFC 1087
C. OSSTMM
D. TCSEC

2. It is most important to obtain _____ before beginning a penetration test.

3. A security exposure in an operating system or application software component is called a _____.

4. The second step of the hacking process is _____.

5. When hackers talk about standards of behavior and moral issues of right and wrong, what are they referring to?

A. Rules
B. Standards
C. Laws
D. Ethics

6. Hackers may justify their actions based on which of the following:
   A. All information should be free.
   B. Access to computers and their data should be unlimited.
   C. Writing viruses, malware, or other code is not a crime.
   D. Any of the above.

7. The individual responsible for releasing what is considered the first Internet worm was:
   A. Kevin Mitnick
   B. Robert T. Morris, Jr.
   C. Adrian Lamo
   D. Kevin Poulsen

8. A hacker with computing skills and expertise to launch harmful attacks on computer networks and who uses those skills illegally is best described as a(n):
   A. Disgruntled employee
   B. Ethical hacker
   C. White-hat hacker
   D. Black-hat hacker

9. If a penetration test team does not have anything more than a list of IP addresses of the organization's network, what type of test are the penetration testers conducting?
   A. Blind assessment
   B. White box
   C. Gray box
   D. Black box

10. How is the practice of tricking employees into revealing sensitive data about their computer system or infrastructure best described?
   A. Ethical hacking
   B. Dictionary attack
   C. Hacktivism
   D. Social engineering