CHAPTER 1

Introduction to Penetration Testing

So, you have decided to become a penetration tester (commonly known as a *pentester*). Not sure where to start? This book helps you learn what it means to become a penetration tester and the responsibilities you will be assuming both technically and ethically when you take on this role. You will build the skills necessary to be successful in the world of penetration and hands-on security.

Specifically, you will encounter many hacking methods that are currently being used on the front lines. You will also encounter techniques that you can use during your pen test to gain information or establish a foothold from which to launch more advanced attacks.

In addition, understanding the motivations of hackers can aid you in understanding the scope of an attack or perhaps even aid in discovering details of the attack. In fact, you need to empathize with hackers in order to establish why they may be carrying out an attack and then use that experience to test a client's network.

In this chapter, you'll learn to:

- **Define what penetration testing is and what a pentester does**
- **Learn why you want to preserve confidentiality, integrity, and availability**
- **Appreciate the history of hacking and penetration testing**

Defining Penetration Testing

Being a pentester has become more important in today's world as organizations have had to take a more serious look at their security posture and how to improve it. Several high-profile incidents such as the ones involving retail giant Target and entertainment juggernaut Sony have drawn attention to the need for better trained and more skilled security professionals

who understand the weaknesses in systems and how to locate them. Through a program that combines technological, administrative, and physical measures, many organizations have learned to fend off their vulnerabilities.

- Technology controls such as virtual private networks (VPNs), cryptographic protocols, intrusion detection systems (IDSs), intrusion prevention systems (IPSs), access control lists (ACLs), biometrics, smart cards, and other devices have helped security.
- Administrative controls such as policies, procedures, and other rules have also been strengthened and implemented over the past decade.
- Physical controls include devices such as cable locks, device locks, alarm systems, and other similar devices.

As a pentester, you must be prepared to test environments that include any or all of the technologies listed here as well as an almost endless number of other types. So, what is a penetration tester anyway?

Defining What a Penetration Tester Does

A penetration tester, or pentester, is employed by an organization either as an internal employee or as an external entity such as a contractor hired on a per-job or per-project basis. In either case, pentesters conduct a penetration test, meaning they survey, assess, and test the security of a given organization by using the same techniques, tactics, and tools that a malicious hacker would use. The main differences between a malicious hacker and a pentester are intent and the permission that they get, both legal and otherwise, from the owner of the system that will be evaluated. Additionally, pentesters are never to reveal the results of a test to anyone except those designated by the client. As a safeguard for both parties, a nondisclosure agreement (NDA) is usually signed by both the hiring firm and the pentester. This protects company property and allows the pentester access to internal resources. Finally, the pentester works under contract for a company, and the contract specifies what is off-limits and what the pentester is expected to deliver at the end of the test. All of the contractual details depend on the specific needs of a given organization.

Some other commonly encountered terms for pentester are penetration tester, ethical hacker, and white-hat hacker. All three terms are correct and describe the same type of individual (though some may debate these apparent similarities in some cases). Typically the most commonly used name is pentester.

EC-Council uses ethical hacker when referencing its own credential, the Certified Ethical Hacker.

In some situations, what constitutes a hacker is a topic ripe for argument. I have had many interesting conversations over the years addressing the question of whether the term hacker is good or bad. Many hackers are simply bad news all-around and have no useful function, and that's how hackers are usually portrayed in movies, TV, books, and other media. However, hackers have evolved, and the term can no longer be applied to just those who engage in criminal actions. In fact, many hackers have shown that while they have the skill to commit crimes and wreak havoc, they are more interested in engaging with clients and others to improve security or perform research.

To be safe, a professional who does not want to cause confusion should avoid the term hacker so as to head off any fears clients may have. The term pentester is preferred.

Recognizing Your Opponents

In the real world, you can categorize hackers to differentiate their skills and intent.

Script Kiddies These hackers have limited or no training and know how to use basic tools or techniques. They may not even understand any or all of what they are doing.

White-Hat Hackers These hackers think like the attacking party but work for the good guys. They typically are characterized by having what is commonly considered to be a code of ethics that says they will cause no harm. This group is also known as pentesters.

Gray-Hat Hackers These hackers straddle the line between the good and bad sides and have decided to reform and become the good side. Once they are reformed, they may not be fully trusted, however. Additionally, in the modern era of security these types of individuals also find and exploit vulnerabilities and provide their results to the vendor either for free or for some form of payment.

Black-Hat Hackers These hackers are the bad guys who operate on the wrong side of the law. They may have an agenda or no agenda at all. In most cases, black-hat hackers and outright criminal activity are not too far removed from one another.

Cyberterrorists Cyberterrorists are a new form of attacker that tries to knock out a target without regard to being stealthy. The attacker essentially is not worried about getting caught or doing prison time to prove a point.

Preserving Confidentiality, Integrity, and Availability

Any organization that is security minded is trying to maintain the CIA triad—or the core principles of confidentiality, integrity, and availability. The following list describes the core concepts. You should keep these concepts in mind when performing the tasks and responsibilities of a pentester.

Confidentiality This refers to the safeguarding of information, keeping it away from those not otherwise authorized to possess it. Examples of controls that preserve confidentiality are permissions and encryption.

Integrity This deals with keeping information in a format that retains its original purposes, meaning that the data the receiver opens is the same the creator intended.

Availability This deals with keeping information and resources available to those who need to use it. Simply put, information or resources, no matter how safe, are not useful unless they are ready and available when called upon.

CIA is one of the most important if not the most important set of goals to preserve when assessing and planning security for a system. An aggressor will attempt to break or disrupt these goals when targeting a system. Figure 1.1 illustrates the "balance" of the CIA triad.

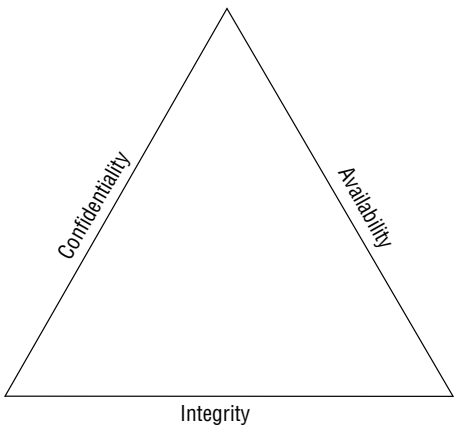

FIGURE 1.1 The CIA triad

Why is the CIA triad so important? Well, consider what could result if an investment firm or defense contractor suffered a disclosure incident at the

hands of a malicious party. The results would be catastrophic, not to mention it could put either organization at serious risk of civil and criminal actions. As a pentester, you will be working toward finding holes in the client's environment that would disrupt the CIA triad and how it functions. Another way of looking at this is through the use of something I call the anti-CIA triad (Figure 1.2).

Improper Disclosure This is the inadvertent, accidental, or malicious revealing or accessing of information or resources to an outside party. Simply put, if you are not someone who is supposed to have access to an object, you should never have access to it.

Unauthorized Alteration This is the counter to integrity as it deals with the unauthorized or other forms of modifying information. This modification can be corruption, accidental access, or malicious in nature.

Disruption (aka Loss) This means that access to information or resources has been lost when it otherwise should not have. Essentially, information is useless if it is not there when it is needed. While information or other resources can never be 100 percent available, some organizations spend the time and money to get 99.999 percent uptime, which averages about six minutes of downtime per year.

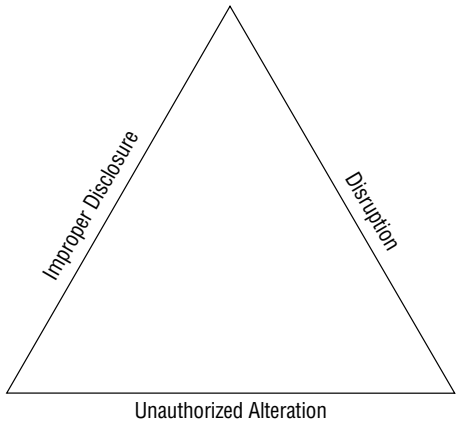

FIGURE 1.2 The anti-CIA triad

Appreciating the Evolution of Hacking

The role of the pentester tends to be one of the more misunderstood positions in the IT security industry. To understand the role of this individual, let's first look back at the evolution of the hacker from which the pentester evolved.

The term hacker is an old one that can trace its origin back about 50 years to technology enthusiasts of the 1960s. These individuals were not like the hackers of today; they were simply those who were curious and passionate about new technologies and spent time exploring the inner workings and limitations of early systems. In the early days, these hackers would seek out systems and try to push the envelope by making the systems do new things or finding undocumented or unknown things that the technology of the day could do. While the technology has become more advanced, the mind-set of these early hackers has lived on.

Hacker has a double meaning within the technology industry in that it has been known to describe both software programmers and those who break into computers and networks uninvited. The former meaning tends to be the more positive of the two, with the latter being the more negative connotation. The news media adds to the confusion by using the term liberally whenever a computer or other piece of technology is involved. Essentially the news media, movies, and TV consider anyone who alters technology or has a high level of knowledge to be a hacker.

When we take a look back at these early technology enthusiasts, we find that they seem to fit a common profile, a curiosity about new technology and an eagerness to learn new things. The original hackers had their curiosity piqued by the mainframes that were available at the time in locations such as college and university campuses as well as some businesses. As time moved on, the PC drew their attention as it was a new, shiny piece of technology to be explored, dissected, and used. The early PC, in fact, allowed many more individuals to take on the mantle of technology enthusiast and hacker than would have been possible a few short years earlier. When the 1990s rolled around, the Internet offered up an irresistible lure for hackers who could spread their activities far and wide with greater ease than ever before. Now, post-2016, we have many more possibilities than were possible at any point in time previously. The explosion of technologies such as Wi-Fi, Bluetooth, tablets, smartphones, and much more has only added to the confusion and amount of devices that can be hacked and attacked. As technology evolved, so did the hackers, with their attacks the result of increasing skill sets and creativity.

Attacks also have become easier as manufacturers of consumer products are not focused on security as much as they are focused on features. When it comes down to it, often a manufacturer shipping a new product such as a tablet, PC, or other item is focused on its functionality and not on whether the device is secure. Although this attitude may have been changed somewhat over the past handful of years, with some vendors securing their

products more than they have in the past, don't be fooled—many are still vulnerable by default.

The Role of the Internet

Hackers became more prolific and more dangerous not too long after the availability of the Internet to the general public. At first many of the attacks that were carried out on the Internet were of the mischievous type such as the defacing of web pages or similar types of activity. Although initially, many of these first types of attacks on the Internet may have been pranks or mischievous in nature, later attacks became much more malicious.

In fact, attacks that have been perpetrated since the year 2000 have become increasingly more sophisticated and aggressive as well as more publicized. One example from August 2014 is the massive data breach against Apple's iCloud, which was responsible for the public disclosure of hundreds of celebrity pictures in various intimate moments. Unfortunately, Apple's terms and conditions for customers using iCloud cannot hold Apple accountable for data breaches and other issues. This breach has so far resulted in lawsuits by many of those who had their pictures stolen as well as a lot of negative publicity for Apple. The photos that were stolen as a result of this breach can be found all over the Internet and have spread like wildfire much to the chagrin of those in the photos.

Another example of the harm malicious hackers have caused is the Target data breach in September 2014. This breach was responsible for the disclosure of an estimated 56 million credit card accounts. This single breach took place less than a year after the much publicized Target data breach, which itself was responsible for 40 million customer accounts being compromised.

A final example comes from information provided by the U.S. government in March 2016. It was revealed that the 18-month period ending in March 2015 had a reported 316 cybersecurity incidents of varying levels of seriousness against the Obamacare website. This website is used by millions of Americans to search for and acquire healthcare and is used in all but 12 states and Washington, DC. While the extensive analysis of the incidents did not reveal any personal information such as Social Security numbers or home addresses, it did show that the site is possibly considered a valid target for stealing this information. Somewhat disconcerting is the fact that there are thought to be numerous other serious issues such as unpatched systems and poorly integrated systems.

All of these attacks are examples of the types of malicious attacks that are occurring and how the general public is victimized in such attacks.

Many factors have contributed to the increase in hacking and cybercrime, with the amount of data available on the Internet and the spread of new

technology and gadgets two of the leading causes. Since the year 2000, more and more portable devices have appeared on the market with increasing amounts of power and functionality. Devices such as smartphones, tablets, wearable computing, and similar items have become very open and networkable, allowing for the easy sharing of information. Additionally, I could also point to the number of Internet-connected devices such as smartphones, tablets, and other gadgets that individuals carry around in increasing numbers. Each of these examples has attracted attention of criminals, many of whom have the intention of stealing money, data, and other resources.

Many of the attacks that have taken place over the last decade have been perpetrated not by the curious hackers of the past but rather by other groups. The groups that have entered the picture include those who are politically motivated, activist groups, and criminals. While there are still plenty of cases of cyberattacks being carried out by the curious or by pranksters, the attacks that tend to get reported and have the greatest impact are these more maliciously motivated ones.

The Hacker Hall of Fame (or Shame)

Many hackers and criminals have chosen to stay hidden behind aliases or in many cases they have never gotten caught, but that doesn't mean there haven't been some noticeable faces and incidents. Here's a look at some famous hacks over time:

- In 1988, Cornell University student Robert T. Morris, Jr. created what is considered to be the first Internet worm. Because of an oversight in the design of the worm, it replicated extremely quickly and indiscriminately, resulting in widespread slowdowns affecting the whole Internet.
- In 1994, Kevin Lee Poulsen, going by the name Dark Dante, took over the telephone lines of the entire Los Angeles–based radio station KIIS-FM to ensure he would be the 102nd caller in order to win a Porsche 944 S2. Poulsen has the notable distinction of being the first to be banned from using the Internet after his release from prison (though the ban was only for a limited time). As a footnote to Poulsen's story, Poulsen is now an editor at Wired magazine.
- In 1999, David L. Smith created the Melissa virus, which was designed to email itself to entries in a user's address book and later delete files on the infected system.

- In 2001, Jan de Wit authored the Anna Kournikova virus, which was designed to read all the entries of a user's Outlook address book and email itself to each.
- In 2002, Gary McKinnon connected to and deleted critical files on U.S. military networks, including information on weapons and other systems.
- In 2004, Adam Botbyl, together with two friends, conspired to steal credit card information from the Lowe's hardware chain.
- In 2005, Cameron Lacroix hacked into the phone of celebrity Paris Hilton and also participated in an attack against the site LexisNexis, an online public record aggregator, ultimately exposing thousands of personal records.
- In 2009, Kristina Vladimirovna Svechinskaya, a young Russian hacker, got involved in several plots to defraud some of the largest banks in the United States and Great Britain. She used a Trojan horse to attack and open thousands of bank accounts in the Bank of America, through which she was able to skim around $3 billion in total. In an interesting footnote to this story, Ms. Svechinskaya was named World's Sexiest Hacker at one point due to her good looks. I mention this point to illustrate the fact that the image of a hacker living in a basement, being socially awkward, or being really nerdy looking is gone. In this case, the hacker in question was not only very skilled and dangerous, but she also did not fit the stereotype of what a hacker looks like.
- In 2010 through the current day, the hacking group Anonymous has attacked multiple targets, including local government networks, news agencies, and others. The group is still active and has committed several other high-profile attacks up to the current day. Attacks in recent history have included the targeting of individuals such as Donald Trump and his presidential campaign of 2016.

While many attacks and the hackers that perpetrate them make the news in some way shape or form, many don't. In fact, many high-value, complicated, and dangerous attacks occur on a regular basis and are never reported or, even worse, are never detected. Of the attacks that are detected, only a small number of hackers ever even see the inside of a courtroom much less a prison cell. Caught or not, however, hacking is still a crime and can be prosecuted under an ever-developing body of laws.

Recognizing How Hacking Is Categorized Under the Law

Over the past two decades crimes associated with hacking have evolved tremendously, but these are some broad categories of cybercrime:

Identity Theft This is the stealing of information that would allow someone to assume the identity of another party for illegal purposes. Typically this type of activity is done for financial gains such as opening credit card or bank accounts or in extreme cases to commit other crimes such as obtaining rental properties or other services.

Theft of Service Examples are the use of phone, Internet, or similar items without expressed or implied permission. Examples of crimes or acts that fall under this category would be acts such as stealing passwords and exploiting vulnerabilities in a system. Interestingly enough, in some situations just the theft of items such as passwords is enough to have committed a crime of this sort. In some states, sharing an account on services such as Netflix with friends and family members can be considered theft of service and can be prosecuted.

Network Intrusions or Unauthorized Access This is one of the oldest and more common types of attacks. It is not unheard of for this type of attack to lead into other attacks such as identity theft, theft of service, or any one of a countless other possibilities. In theory, any access to a network that one has not been granted access to is enough to be considered a network intrusion; this would include using a Wi-Fi network or even logging into a guest account without permission.

Posting and/or Transmitting Illegal Material This has gotten to be a difficult problem to solve and deal with over the last decade. Material that is considered illegal to distribute includes copyrighted materials, pirated software, and child pornography, to name a few. The accessibility of technologies such as encryption, file sharing services, and ways to keep oneself anonymous has made these activities hard to stop.

Fraud This is the deception of another party or parties to illicit information or access typically for financial gain or to cause damage.

Embezzlement This is one form of financial fraud that involves theft or redirection of funds as a result of violating a position of trust. The task has been made easier through the use of modern technology.

Dumpster Diving This is the oldest and simplest way to get and gather material that has been discarded or left in unsecured or unguarded receptacles. Often, discarded data can be pieced together to reconstruct sensitive information. While going through trash itself is not illegal, going through trash on private property is and could be prosecuted under trespassing laws as well as other portions of the law.

Writing Malicious Code This refers to items such as viruses, worms, spyware, adware, rootkits, and other types of malware. Essentially this crime covers a type of software deliberately written to wreak havoc and destruction or disruption.

Unauthorized Destruction or Alteration of Information This covers the modifying, destroying, or tampering with information without appropriate permission.

Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS) Attacks These are both ways to overload a system's resources so it cannot provide the required services to legitimate users. While the goals are the same, the terms DoS and DDoS actually describe two different forms of the attack. DoS attacks are small scale, one-on-one attacks, whereas DDoS attacks are much larger in scale, with thousands of systems attacking a target.

Cyberstalking This is a relatively new crime on this list. The attacker in this type of crime uses online resources and other means to gather information about an individual and uses this to track the person and, in some cases, try to meet these individuals in real life. While some states, such as California, have put laws in place against stalking, which also cover crimes of the cyber variety, they are far from being universal. In many cases, when the stalker crosses state lines during the commission of their crime, it becomes a question of which state or jurisdiction can prosecute.

Cyberbullying This is much like cyberstalking except in this activity individuals use technologies such as social media and other techniques to harass a victim. While this type of crime may not seem like a big deal, it has been known to cause some individuals to commit suicide as a result of being bullied.

Cyberterrorism This, unfortunately, is a reality in today's world as hostile parties have realized that conventional warfare does not give them the same power as waging a battle in cyberspace. It is worth nothing that a perpetrator conducting terrorism through cyberspace runs the very real risk that they can and will be expedited to the targeted country.

To help understand the nature of cybercrime, it is first important to understand the three core forces that must be present for a crime, any crime, to be committed. These three items are:

- Means or the ability to carry out their goals or aims, which in essence means that they have the skills and abilities needed to complete the job
- Motive or the reason to be pursuing the given goal
- Opportunity, the opening or weakness needed to carry out the threat at a given time

As we will explore in this book, many of these attack types started very simply but rapidly moved to more and more advanced forms. Attackers have quickly upgraded their methods as well as included more advanced strategies, making their attacks much more effective than in the past. While they already knew how to harass and irritate the public, they also caused ever bolder disruptions of today's world by preying on our "connected" lifestyle.

Attacks mentioned here will only increase as newer technologies such as smartphones and social networking integrate even more into our daily lives. The large volumes of information gathered, tracked, and processed by these devices and technologies are staggering. It is estimated by some sources that information on location, app usage, web browsing, and other data is collected on most individuals every three minutes. With this amount of information being collected, it is easy to envision scenarios where abuse could occur.

What has been behind a lot of the attacks in the past decade or more is greed. Hackers have realized that their skills are now more than curiosity and are something that could be used for monetary gain. One of the common examples is the malware that has appeared over this time period. Not only can malware infect a system, but in many cases it has been used to generate revenue for their creators. For example, malware can redirect a user's browser to a specific site with the purpose of making the user click or view ads.

Now You Know

Now you know that a penetration tester is someone who surveys, assesses, and tests the security of a given organization by using the same techniques a malicious hacker would use. You know your "opponents" are script kiddies, white-hat hackers, gray-hat hackers, black-hat hackers, and cyberterrorists. You also know that you will be trying to disrupt your client's confidentiality, integrity, and availability.

In addition, you learned to appreciate the evolution of hacking and penetration testing, including the role of the Internet and famous hacks in history.

The Essentials and Beyond

1. What are the three types of controls that a company can use to defend against hackers?
2. What is the main difference between a hacker and a pentester?
3. What are some other names for a pentester?
4. What does the CIA triad represent when referring to information security?
5. Name some of the crimes categorized as cybercrime.