Chapter 1

Introduction to Ethical Hacking

CEH EXAM OBJECTIVES COVERED IN THIS CHAPTER:

- ✓ **II. Analysis/Assessment**
  - C. Risk assessments
  - D. Technical assessment methods
- ✓ **III. Security**
  - L. Privacy/confidentiality (with regard to engagement)
- ✓ **V. Procedures/Methodology**
  - H. Security testing methodology
- ✓ **VII. Ethics**
  - A. Professional code of conduct
  - B. Appropriateness of hacking activities

Welcome to the beginning of your journey to becoming a Certified Ethical Hacker. In this book you will learn the tools, technologies, methods, and skills needed to earn the EC-Council's Certified Ethical Hacker v9 qualification. However, while this book will give you what you need to be prepared to successfully pass the exam, it will also strive to give you the additional knowledge and skills needed to be a successful penetration tester.

In this book, you will learn exactly what it takes to become an ethical hacker and the responsibilities and expectations that go with the title. You will experience the ethics and questions that go with the technology and the practices involved in this exciting field.

Ethical hackers, or penetration testers, have been around for a long time, but because of increases in cybercrime and regulations over the last decade, they have become more popular than in the past. The realization is that finding weaknesses and deficiencies in systems and addressing them proactively is less costly than dealing with the fallout that comes after the fact. In response, organizations have sought to create their own penetration testing teams internally as well as contract with outside experts when and if they are needed.

In this book you will encounter the two terms *penetration tester* and *ethical hacker*. Although both are correct and both are used in the IT and security industries, the former tends to be more popular than the latter. In most cases, you will run into the term *penetration tester* or its associated shorthand *pentester.*

Taking on the skillset associated with ethical hacking will quickly and effectively put you into the role of evaluating environments to identify, exploit, report, and recommend corrective actions to be taken in respect to threats and vulnerabilities. Note, however, that pentesters usually do not do corrective actions because that is something that the client must decide to perform or not, but in some cases the client may ask you do so.

Through a robust and effective combination of technological, administrative, and physical measures, these organizations have learned to address their given situation and head off major problems wherever and whenever possible. Technologies 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 countermeasures such as policies, procedures, and other rules have also been strengthened and implemented over the past decade. Physical measures include cable locks, device locks, alarm systems, and similar devices. Your new role as an ethical hacker will deal with all of these items, plus many more.

As an ethical hacker, you must know not only the environment you will be working in but also how to find weaknesses and address them as needed. But before we get to all of that, this chapter discusses the history of hacking and what it means to be an ethical hacker. We'll also look at the process of penetration testing and explore the importance of contracts.

Hacking: the Evolution

Hacker is one of the most misunderstood and overused terms in the security industry. Everyone from the nightly news to authors to Hollywood and the rest of the media uses the term frequently. Thanks to overuse of the term and the fact that it is almost constantly attached to activities that are shady or even criminal in nature, the general public looks at anyone with the label *hacker* as up to no good. Hackers are viewed as those operating in the shadows, antisocial and antiestablishment in many cases. Other members of the public have even come to embrace hackers as the new social activists thwarting politicians, governments, large corporations, and others. Newsworthy events by loosely organized groups such as Anonymous and Lizard Squad have contributed to the public perception of the hacker.

While many have taken different stances and have different opinions of whether hackers are good or bad, this book will not seek to pass judgment either way on many of those who engage in hacking. Groups such as Anonymous have both their supporters and detractors, for example; in this book we will mention this group but will use it to illustrate points, and that is all. We will leave the judgment of such groups up to you.

So, what is a hacker exactly and how did we get to the point where we are today? We can best address this question by looking into the past and seeing how things have evolved.

The Early Days of Hacking

The idea of hacking and hackers goes way back to the first technology enthusiasts who wanted to learn about new technology and were curious about how it worked. They were the same types of people who today are interested not only in acquiring all sorts of technology but also in learning how to customize and tweak it to do new things that the original designers never intended. In the early days (pre-1970), these hackers may have been found taking apart and learning about the inner workings of radios and early computers. As technology progressed, these individuals moved to more complex and advanced systems available at the time. Fast-forward to the 1970s, and the mainframes that were present on college campuses and corporate environments were the target of interest by new generations of hackers. Later, in the 1980s, the PC was the newest piece of technology, with

hackers moving to this environment. In fact, the 1980s saw hackers starting to engage in more mischievous and later malicious activities; adding to the situation was that fact that their attacks could now be used against many more systems because more people had access to PCs. In the 1990s, the Internet was made accessible to the public, and systems became interconnected; as a result, curiosity and mischief could easily spread beyond a small collection of systems and go worldwide. Since 2000, smartphones, tablets, Bluetooth, and other technologies have been added to the devices and technologies that hackers target. As you can see, as technology evolves, so do hackers' attacks in response to what's available at the time.

When the Internet became available to the public at large, hacking and hackers weren't too far behind. When the first generations of browsers became available in the early 1990s, attacks grew in the form of website defacements and other types of mischief. The first forays of hacking in cyberspace resulted in some humorous or interesting pranks, but later more aggressive attacks started to emerge. Incidents such as the hacking of movie and government websites were some of the first examples. Until the early 2000s, website defacing was so common that many incidents were no longer reported.

Making things easier for hackers is the fact that early network technologies such as the Internet were never designed with security as a goal. The goal was the sharing of information.

Current Developments

In the early 2000s, more malicious activity started to appear in the form of more advanced attacks. In the first few years of the new millennium, the aggressiveness of attacks increased, with many attacks criminally motivated. Malicious attacks that have occurred include the following (although there are many more):

- Denial-of-service attacks
- Manipulation of stock prices
- Identity theft
- Vandalism
- Credit card theft
- Piracy
- Theft of service

Among the many situations that have contributed to the increase in hacking and cybercrime are the amount of information being passed and the overall dependency on the Internet and digital devices. Over the last decade, the number of financial transactions online has increased, creating a tempting target for crooks. Also, the openness of modern devices such as smartphones and technologies such as Bluetooth has made hacking and stealing information more prevalent. Lastly, we can also point to the number of Internet-connected devices such as

tablets and other gadgets that individuals carry around in increasing numbers. Each of these devices has attracted the attention of criminals with the temptation of stealing never before heard of amounts of money, data, and other resources. As computer crime laws began to be passed, the bragging rights for hacking a website became less attractive. Prank activity seems to have slowed down, whereas real criminal activity has increased. With online commerce, skills started going to the highest bidder, with crime rings, organized crime, and nations with hostile interests using the Internet as an attack vector.

Remember that a good number of attacks that occur nowadays can be attributed to both crime and people pulling pranks. However, no matter what the underlying motivation of the attack, the end result is often the same: System owners are denied use of their assets, and the law is broken.

Hacking: Fun or Criminal Activity?

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

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. Due to an oversight in the design of the worm, it replicated extremely quickly, 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 for only a limited time).
- 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 deleted critical files on U.S. military networks, including information on weapons and other systems. He performed this action after compromising roughly 2000 computer systems inside the U.S. military's network.
- 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, Svechinskaya was named World's Sexiest Hacker at one point due to her stunning 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 also did not fit the stereotype of what a hacker looks like.
- In the mid-2000s, the Stuxnet virus was uncovered in Iran and was shown to be specifically designed to attack the systems involved in uranium production. What made the virus unique is the fact that it targeted only a very specific set of systems, and anything not meeting these requirements was ignored.
- Originating in 2003, 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.

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. Note that for every incident that is made public, only a small number of the individuals who carry them out are caught, and an even smaller number are prosecuted for cybercrime. In any case, hacking is indeed a crime, and anyone engaging in such activities can be prosecuted under laws that vary from location to location. The volume, frequency, and seriousness of attacks have only increased and will continue to do so as technology evolves.

Here are some generic examples of cybercrime:

- Stealing passwords and usernames, or using vulnerabilities in a system to gain access, falls under the category of theft of access and the stealing of services and resources that the party would not otherwise be given access to. In some cases stealing credentials but not using them is enough to constitute a cybercrime. In a few states even sharing usernames and passwords with a friend or family member is a crime.
- Network intrusions are a form of digital trespassing where a party goes someplace that they would not otherwise have access to. Access to any system or group of systems to which a party would not normally be given access is considered a violation of the network and therefore a cybercrime. In some cases the actual intrusions may not even involve hacking tools; the very act of logging into a guest account without permission may be sufficient to be considered an intrusion.
- Social engineering is both the simplest and the most complex form of hacking or exploiting a system by going after its weakest point, the human element. On the one hand, this is easy to attempt because the human being is many times the most accessible component of a system and the simplest to interact with. On the other hand, it can be extremely difficult to read both the spoken and unspoken cues to get information that may be useful to the attacker.

- Posting and/or transmitting illegal material has gotten to be a difficult problem to solve and deal with over the last decade. With the increased use of social media and other Internet-related services, illegal material can spread from one corner of the globe to another in a very short period of time.
- Fraud is the deception of another party or parties to elicit information or access typically for financial gain or to cause damage.
- Software piracy is the possession, duplication, or distribution of software in violation of a license agreement or the act of removing copy protection or other license-enforcing mechanisms. Again this has become a massive problem with the rise of file-sharing services and other mechanisms designed to ease sharing and distribution; in many cases the systems are used for distribution without the system owner's consent.
- Dumpster diving is the oldest and simplest way to gather material that has been discarded or left in unsecured or unguarded receptacles. Often, discarded data can be pieced together to reconstruct sensitive information.
- Malicious code refers to items such as viruses, worms, spyware, adware, rootkits, and other types of malware. This crime covers any type of software deliberately written to wreak havoc and destruction or disruption.
- Unauthorized destruction or alteration of information includes modifying, destroying, or tampering with information without permission.
- Embezzlement is a form of financial fraud that involves theft or redirection of funds as a result of violating a position of trust. The crime has been made much easier through the use of modern digital means.
- Data-diddling is the unauthorized modification of information to cover up activities.
- Denial-of-service (DoS) and distributed denial-of-service (DDoS) attacks are ways to overload a system's resources so it cannot provide the required services to legitimate users.
- Ransomware is a relatively newer class of malware that is designed to hunt down and encrypt files on a target system. Once such files are found, the code will encrypt the data and then tell the victim that they must pay a certain amount to get their data back.

The Evolution and Growth of Hacking

As you will see in this book, attacks and strategies have improved and evolved over the years in ways you may not be aware of. Attackers have constantly sought to up their game with new tactics and strategies to include various types of malware such as worms, spam, spyware, adware, and even rootkits. Although they have long known how to harass and irritate the public, in recent years they have caused ever bolder disruptions by preying on our connected lifestyle.

Hackers have also started to realize that it is possible to use their skills to generate money in many interesting ways. For example, attackers have used techniques to redirect

web browsers to specific pages that generate revenue for themselves. Another example is a spammer sending 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.

The field you are entering (or may already be working in as a security administrator or engineer) is one that changes rapidly. In this field attacker and defender are in an ongoing struggle to gain dominance. Because attackers have become highly flexible and adaptable, so must you be as an ethical hacker. Your ability to think outside the box will serve you well as you envision new strategies and potential attacks before they are used against you.

Whenever you encounter a new technology or new situation, always try to think of different ways the situation or technology can be used. Think, for example, how a device such as a tablet or smartphone can be used in ways different from what the designer or architect envisioned. Also keep an eye open for weaknesses or vulnerabilities that can be exploited. Train your mind to think outside the norm and think like someone who is trying to cause harm or get away with something. As an ethical hacker you will be expected to think along these lines but in a benevolent manner.

Making your life as a security manager even harder today is that attackers have adopted a new pack mentality that makes defensive measures and planning much harder. In the early days the attacking person was just that—one person. Nowadays groups such as Anonymous and LulzSec have shown us quite convincingly that attacking in numbers makes a difference even in the cyberworld. The collective or hive-like mentality has reaped huge benefits for attackers who are able to employ multiple methods in a short period of time to obtain impressive results. Such groups or packs are able to enhance their effectiveness by having a wide range of numbers, diversity, or complementary skill sets and also by the lack of any clear leadership structures. Also adding to the concern is that some groups can be linked to criminal or terrorist organizations.

In this book you will learn these methods and what is being used on the front lines to perpetrate increasingly complex and devastating attacks. You must be aware of how these attacks have evolved, how technology has played a part, and how the law is dealing with an ever more complicated landscape.

You will also learn more about the motivations of attackers and their mind-set. This is one of the challenges that you will have as an ethical hacker: understanding and empathizing with your attackers. Understanding the motivations can, in some cases, yield valuable insight into why a given attack has been committed or may be committed against an asset. For now you should keep in mind that an attacker needs three things to carry out a crime:

- 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, or the opening or weakness needed to carry out the threat at a given time

So, What Is an Ethical Hacker?

When you explore this book and the tools it has to offer, you are learning the skills of the hacker. But we can't leave it at that, because you need to be an *ethical hacker*, so let's explore what that means.

Ethical hackers are employed either through contracts or direct employment to test the security of an organization. They use the same skills and tactics as a hacker but with permission from the system owner to carry out their attack against the system. In addition, ethical hackers do not reveal the weaknesses of an evaluated system to anyone other than the system owner. Finally, ethical hackers work under contract for a company or client, and their contracts specify what is off-limits and what they are expected to do. Their role depends on the specific needs of a given organization. In fact, some organizations keep teams on staff specifically to engage in ethical hacking activities.

Types of Hackers

The following are categories of hackers:

Script Kiddies These hackers have limited or no training and know how to use only basic techniques or tools. Even then they may not 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 are typically characterized by having a code of ethics that says essentially they will cause no harm. This group is also known as ethical hackers or pentesters.

Gray-Hat Hackers These hackers straddle the line between good and bad and have decided to reform and become the good side. Once they are reformed, they still might not be fully trusted.

Black-Hat Hackers These hackers are the bad guys who operate on the opposite side of the law. They may or may not have an agenda. In most cases, black-hat hacking and outright criminal activity are not far removed from each other.

Suicide Hackers These hackers try to knock out a target to prove a point. They are not stealthy, because they are not worried about getting caught or doing prison time.

What Are Your Responsibilities?

One of the details you need to understand early and never forget is *permission*. As an ethical hacker you should never target a system or network that you do not own or have permission to test. If you do so, you are guilty of any number of crimes, which would be detrimental not only to your career but perhaps to your freedom as well. Before you test a target, you should have a contract in hand from the owner giving you permission to do so. Also remember that you should test only those things you have been contracted to test. If

the customer or client decides to add or remove items from the test, the contract must be altered to keep both parties out of legal trouble. Take special notice of the fact that ethical hackers operate with contracts in place between themselves and the target. Operating without permission is unethical; operating without a contract is downright stupid and illegal.

In addition, a contract must include verbiage that deals with the issue of confidentiality and privacy. It is possible that during a test you will encounter confidential information or develop an intimate knowledge of your client's network. As part of your contract you will need to address whom you will be allowed to discuss your findings with and whom you will not. Generally clients will want you to discuss your findings only with them and no one else.

According to the International Council of Electronic Commerce Consultants (EC-Council) you, as a CEH, must keep private any confidential information gained in your professional work (in particular as it pertains to client lists and client personal information). You cannot collect, give, sell, or transfer any personal information (such as name, email address, Social Security number, or other unique identifier) to a third party without your client's prior consent. Keep this in mind since a violation of this code could not only cause you to lose trust from a client but also land you in legal trouble.

Contracts are an important detail to get right; if you get them wrong it could easily mean legal problems later. The problem with contracts is that most people find the legalese nearly impossible to understand and the amount of preparation intimidating to say the least. I strongly recommend that you consider getting a lawyer experienced in the field to help you with contracts.

A contract is essential for another extremely important reason as well: proof. Without a contract you have no real proof that you have permission from the system owner to perform any tests.

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

Bad Guys and Good Guys, or Hackers and Ethical Hackers

The difference between an *ethical hacker* and a *hacker* is something that can easily get you into an argument. Just saying the word *hacker* in the wrong place can get you into an hours-long conversation of the history of hacking and how hackers are all good guys who mean nothing but the best for the world. Others will tell you that hackers are all evil and have nothing but bad intentions. In one case I was even told that hackers were originally model-train enthusiasts who happened to like computers.

You must understand that for us, hackers are separated by intentions. In our worldview hackers who intend to cause harm or who do not have permission for their activities are considered *black hats*, whereas those who do have permission and whose activities are benign are *white hats*. Calling one side *good* and the other *bad* may be controversial, but in this book we will adhere to these terms:

Black Hats They do not have permission or authorization for their activities; typically their actions fall outside the law.

White Hats They have permission to perform their tasks. White hats never share information about a client with anyone other than that client.

Gray Hats These hackers cross into both offensive and defensive actions at different times.

Another type of hacker is the *hacktivist*. *Hacktivism* is any action that an attacker uses to push or promote a political agenda. Targets of hacktivists have included government agencies and large corporations.

Code of Conduct and Ethics

As an ethical hacker you will need to make sure that you adhere to a code of conduct or ethics to ensure you remain trustworthy (and employed). In the case of the EC-Council's CEH credential you are expected to adhere to their Code of Ethics in your dealings lest you be decertified.

In order to make sure you fully understand what you will be expected to abide by when you become a CEH, I have provided the official EC-Council Code of Ethics here (with slight rewording for clarity). Read it and know it to make sure you are comfortable with everything expected of you as a CEH.

- Keep private and confidential information gained in your professional work (in particular as it pertains to client lists and client personal information). Not collect, give, sell, or transfer any personal information (such as name, email address, Social Security number, or other unique identifier) to a third party without client prior consent.
- Protect the intellectual property of others by relying on your own innovation and efforts, thus ensuring that all benefits vest with its originator.
- Disclose to appropriate persons or authorities potential dangers to any e-commerce clients, the Internet community, or the public that you reasonably believe to be associated with a particular set or type of electronic transactions or related software or hardware.
- Provide service in your areas of competence, being honest and forthright about any limitations of your experience and education. Ensure that you are qualified for any

project on which you work or propose to work by an appropriate combination of education, training, and experience.

- Never knowingly use software or a process that is obtained or retained either illegally or unethically.
- Not engage in deceptive financial practices such as bribery, double billing, or other improper financial practices.
- Use the property of a client or employer only in ways properly authorized and with the owner's knowledge and consent.
- Disclose to all concerned parties those conflicts of interest that cannot reasonably be avoided or escaped.
- Ensure good management for any project you lead, including effective procedures for promotion of quality and full disclosure of risk.
- Add to the knowledge of the e-commerce profession by constant study, share the lessons of your experience with fellow EC-Council members, and promote public awareness of benefits of electronic commerce.
- Conduct yourself in the most ethical and competent manner when soliciting professional service or seeking employment, thus meriting confidence in your knowledge and integrity.
- Ensure ethical conduct and professional care at all times on all professional assignments without prejudice.
- Not associate with malicious hackers nor engage in any malicious activities.
- Not purposefully compromise or cause to be compromised the client organization's systems in the course of your professional dealings.
- Ensure all penetration testing activities are authorized and within legal limits.
- Not take part in any black-hat activity or be associated with any black-hat community that serves to endanger networks.
- Not be part of any underground hacking community for purposes of preaching and expanding black-hat activities.
- Not make inappropriate reference to the certification or misleading use of certificates, marks, or logos in publications, catalogues, documents, or speeches.
- Not be in violation of any law of the land or have any previous conviction.

Ethical Hacking and Penetration Testing

Ethical hackers engage in sanctioned hacking—that is, hacking with permission from the system's owner. In the world of ethical hacking, most tend to use the term *pentester*, which is short for penetration tester. Pentesters do simply that: penetrate systems like a hacker but for benign purposes.

As an ethical hacker and future test candidate, you must become familiar with the lingo of the trade. Here are some of the terms you will encounter in pen testing:

Hack Value This term describes a target that may attract an above-average level of attention from an attacker. Presumably because this target is attractive, it has more value to an attacker because of what it may contain.

Target of Evaluation A target of evaluation (TOE) is a system or resource that is being evaluated for vulnerabilities. A TOE would be specified in a contract with the client.

Attack This is the act of targeting and actively engaging a TOE.

Exploit This is a clearly defined way to breach the security of a system.

Zero Day This describes a threat or vulnerability that is unknown to developers and has not been addressed. It is considered a serious problem in many cases.

Security This is a state of well-being in an environment where only actions that are defined are allowed.

Threat This is considered to be a potential violation of security.

Vulnerability This is a weakness in a system that can be attacked and used as an entry point into an environment.

Daisy Chaining This is the act of performing several hacking attacks in sequence with each building on or acting on the results of the previous action.

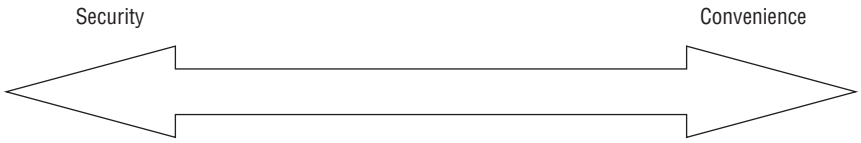
As an ethical hacker, you will be expected to take on the role and use the mind-set and skills of an attacker to simulate a malicious attack. The idea is that ethical hackers understand both sides, the good and the bad, and use this knowledge to help their clients. By understanding both sides of the equation, you will be better prepared to defend yourself successfully. Here are some things to remember about being an ethical hacker:

- You must have explicit permission in writing from the company being tested prior to starting any activity. Legally, the person or persons who must approve this activity or changes to the plan must be the owner of the company or their authorized representative. If the scope changes, you must update the contract to reflect those changes before performing the new tasks.
- You will use the same tactics and strategies as malicious attackers.
- You have the potential to cause the same harm that a malicious attack will cause and should always consider the effects of every action you carry out.
- You must have knowledge of the target and the weaknesses it possesses.
- You must have clearly defined rules of engagement prior to beginning your assigned job.
- You must never reveal any information pertaining to a client to anyone but the client.
- If the client asks you to stop a test, do so immediately.

- You must provide a report of your results and, if asked, a brief on any deficiencies found during a test.
- You may be asked to work with the client to fix any problems that you find. As I will discuss several times in this text, never accept a verbal agreement to expand test parameters. A verbal agreement has no record, and there is a chance of getting sued if something goes wrong and there's no record.

Under the right circumstances and with proper planning and goals in mind, you can provide a wealth of valuable information to your target organization. Working with your client, you should analyze your results thoroughly and determine which areas need attention and which need none at all. Your client will determine the perfect balance of security versus convenience. If the problems you uncover necessitate action, the next challenge is to ensure that existing usability is not adversely affected if security controls are modified or if new ones are put in place. Security and convenience often conflict: The more secure a system becomes, the less convenient it tends to be. Figure 1.1 illustrates this point.

FIGURE 1.1 Security versus convenience analysis



Although ethical hacking sometimes occurs without a formal set of rules of engagement, pen testing does require rules to be agreed on in advance in every case. If you choose to perform a pen test without having certain parameters determined ahead of time, it may be the end of your career if something profoundly bad occurs. For example, not having the rules established before 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 stopping the functioning of a company completely, which again could result in huge legal and other issues for you.

When a pen test is performed it typically takes one of three forms: white box, gray box, or black box. The three forms of testing are important to differentiate because you may be asked to perform any one of them at some point during your career, so let's take a moment to describe each:

Black Box A type of testing in which the pentester has little or no knowledge of the target. This situation is designed to closely emulate the situation an actual attacker would encounter because they would presumably have an extremely low level of knowledge of the target going in.

Gray Box A form of testing where the knowledge given to the testing party is limited. In this type of test, the tester acquires knowledge such as IP addresses, operating systems,

and the network environment, but that information is limited. This type of test would closely emulate the type of knowledge that someone on the inside might have; such a person would have some knowledge of a target but not always all of it.

White Box A form of testing in which the information given to the tester is complete. This means that the pentester is given all information about the target system. This type of test is typically done internally or by teams that perform internal audits of systems.

Another way to look at the different types of testing and how they stack up is shown in Table 1.1.

TABLE 1.1 Available types of pen tests

Type	Knowledge
White box	Full
Gray box	Limited
Black box	None

Do not forget the terms *black box, white box*, and *gray box* because you will be seeing them again both in this book and in the field. As you can see, the terms are not that difficult to understand, but you still should make an effort to commit them to memory.

In many cases, you will be performing what is known as an *IT audit*. This process is used to evaluate and confirm that the controls that protect an organization work as advertised. 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; the criteria for passing an audit may be out of date compared with what is currently happening in the industry.

An ethical hacker tries to preserve what is known as the CIA triad: confidentiality, integrity, and availability. The following list describes these core concepts. Keep these concepts in mind when performing the tasks and responsibilities of a pentester:

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

Integrity Deals with keeping information in a format that is true and correct to its original purposes, meaning that the data that the receiver accesses is the data the creator intended them to have.

Availability The final and possibly one of the most important items that you can perform, availability deals with keeping information and resources available to those who need to use it. Information or resources, no matter how safe and sound, are useful only if they are available when called upon.

CIA is possibly the most important set of goals to preserve when you are assessing and planning security for a system. An aggressor will attempt to break or disrupt these goals when targeting a system. As an ethical hacker your job is to find, assess, and remedy these issues whenever they are discovered to prevent an aggressor from doing harm.

Another way of looking at this balance is to observe the other side of the triad and how the balance is lost. Any of the following break the CIA triad:

- Disclosure is the inadvertent, accidental, or malicious revealing or allowing access of information or resources to an outside party. If you are not authorized to have access to an object, you should never have access to it.
- Alteration is the counter to integrity; it deals with the unauthorized modification of information. This modification can be caused by corruption, accidental access that leads to modification, or modifications that are malicious in nature.
- Disruption (also known as loss) means that authorized access to information or resources has been lost. Information is useless if it is not there when it is needed. Although information or other resources can never be 100 percent available, some organizations spend the time and money to ensure 99.999 percent uptime for critical systems, which averages about six minutes of downtime per year.

Think of these last three points as the *anti-CIA triad* or the inverse of the CIA triad. The CIA triad deals with preserving information and resources, whereas the anti-CIA triad deals with violating those points. You can also think of the anti-CIA triad as dealing with the aggressor's perspective rather than the defender's.

An ethical hacker will be entrusted with ensuring that the CIA triad is preserved at all times and threats are dealt with in the most appropriate manner available (as required by the organization's own goals, legal requirements, and other needs). For example, consider what could happen if an investment firm or defense contractor suffered a disclosure incident at the hands of a malicious party. The results would be catastrophic with lawsuits from customers and investigation by law enforcement if that information was personal in nature (such as health or financial).

It is also important to consider two supporting elements to the CIA triad, which are non-repudiation and authentication.

Non-repudiation Non-repudiation is the concept that once an action is carried out by a party it cannot be denied by that party. For example, by using techniques such as digital

signatures it is possible to definitively say who sent a message without any possibility of denial that they were the originator of the message.

Authenticity Authenticity is the ability to state that an object such as a piece of data or message came from a legitimate and identifiable source. This is an important property for an item to have because it states that the source of an action is valid and known. Because the sender has signed their digital signature with their private key, the subsequent verification of the signature using their public key proves the sender's identity and thus authenticates the sender and the origin of the message.

In this book you will encounter legal issues several times. You are responsible for checking the details of what laws apply to you, and you will need to get a lawyer to do that. You should be conscious of the law at all times and recognize when you may be crossing into a legal area that you need advice on.

Hacking Methodologies

A hacking methodology refers to the step-by-step approach used by an aggressor to attack a target such as a computer network. There is no specific step-by-step approach used by all hackers. As can be expected when a group operates outside the rules as hackers do, rules do not apply the same way. A major difference between a hacker and an ethical hacker is the code of ethics to which each subscribes.

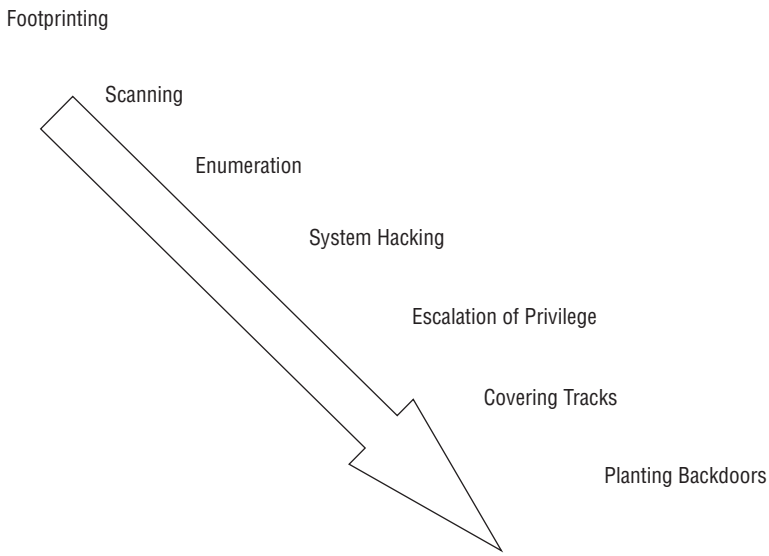
The following steps, illustrated in Figure 1.2, typically make up the hacking process:

- *Footprinting* means that you are using primarily passive methods of gaining information from a target prior to performing the later active methods. Typically, you keep interaction with your target to a minimum to avoid detection, thus alerting the target that something is coming in their direction. A myriad of methods are available to perform this task, such as Whois queries, Google searches, job board searches, and discussion groups. We will examine this topic in Chapter 4, "Footprinting."
- *Scanning* is the phase in which you take the information gleaned from the footprinting phase and use it to target your attack much more precisely (see Chapter 5, "Scanning"). The idea here is to act on the information from the prior phase, not to blunder around without purpose and set off alarms. Scanning means performing tasks like ping sweeps, port scans, and observations of facilities. One of the tools you will use is Nmap, which is very useful for this purpose.
- *Enumeration* is the next phase (see Chapter 6, "Enumeration"), where you extract much more detailed information about what you uncovered in the scanning phase to determine its usefulness. Think of the information gathered in the previous phase as walking down a hallway and rattling the doorknobs, taking note of which ones turn and which ones do not. Just because a door is unlocked doesn't mean anything of use

is behind it. In this phase you are looking behind the door to see if there is anything of value behind it. Results of this step can include a list of usernames, groups, applications, banner settings, and auditing information.

- *System hacking* (Chapter 7, "System Hacking") follows enumeration. You can now plan and execute an attack based on the information you uncovered. You could, for example, start choosing user accounts to attack based on the ones uncovered in the enumeration phase. You could also start crafting an attack based on service information uncovered by retrieving banners from applications or services.
- *Escalation of privilege* is the hacking phase, where you can start to obtain privileges that are granted to higher privileged accounts than you broke into originally. Depending on your skills, it might be possible to move from a low-level account such as a guest account all the way up to administrator or system-level access.
- *Covering tracks* is the phase when you attempt to remove evidence of your presence in a system. You purge log files and destroy other evidence that might give away the valuable clues needed for the system owner to determine an attack occurred. Think of it this way: If someone were to pick a lock to get into your house versus throwing a brick through the window, the clues are much less obvious in the former than the latter. In the latter case you would look for what the visitor took immediately, and in the former case you might notice the break-in much later, after the trail had gone cold.
- *Planting of backdoors* means to leave something behind that would enable you to come back later if you wanted. Items such as special accounts or Trojan horses come to mind.

FIGURE 1.2 The hacking process



Both ethical hackers and hackers follow similar processes as the one outlined here though in less or stricter ways. Hackers are able to write their own rules and use the process however they want without concern or reasons except those that make sense to themselves. Ethical hackers follow the same type of process as seen here with little modification, but they have added something that hackers do not have: Ethical hackers not only will have *permission* prior to starting the first phase but will also be *generating a report* that they will present at the end of the process. The ethical hacker will be expected to keep detailed notes about what is procured at each phase for later generation of that report.

When you decide to carry out this process, seek your client's guidance and ask the following questions along with any others that you think are relevant. During this phase, your goal is to clearly determine why a pen test and its associated tasks are necessary.

- Why did the client request a pen test?
- What is the function or mission of the organization to be tested?
- What will be the constraints or rules of engagement for the test?
- What data and services will be included as part of the test?
- 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?
- Will insiders be notified?
- Will the test be performed as black or white box?
- What conditions will determine the success of the test?
- Who will be the emergency contacts?

Pen testing can take several forms. You must decide, along with your client, which tests are appropriate and will yield the desired results. Tests that can be part of a pen test may include the following:

- An insider attack is intended to mimic the actions that may be undertaken by internal employees or parties who have authorized access to a system.
- An outsider attack is intended to mimic those actions and attacks that would be undertaken by an outside party.

- A stolen equipment attack is a type of attack where an aggressor steals a piece of equipment and uses it to gain access or extracts the information desired from the equipment itself.
- A social engineering attack is a form of attack where the pentester targets the users of a system seeking to extract the needed information. The attack exploits the trust inherent in human nature.

Once you discuss each test, determine the suitability of each, and evaluate the potential advantages and side effects, you can finalize the planning and contracts and begin testing.

When you are undertaking an actual test against a system or environment you must be prepared to think as a malicious party would in the same conditions. Remember that as a pentester you must understand the tools and techniques and use them the same way a bad guy would; however, you temper that with the mindset that you are doing this to help the client and only with their permission would you carry out a test. Be prepared for problems to arise and roadblocks to emerge during the test; you'll have to deal with them each accordingly much like a malicious party would when attacking a target. The idea is to understand how an attack can or would happen, what an attacker would encounter, and how to defeat it. You must understand both sides, the good and the bad, and use this knowledge to help the clients and customers.

Penetration testing does require rules to be agreed upon in advance in every case. If a penetration tester chooses to perform a penetration test without having certain parameters determined ahead of time, it may be the end of that tester's career if something profoundly bad occurs. 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 stopping the functioning of a company completely, which again could result in huge legal and other issues for the tester.

With these goals in mind and a good plan, a penetration tester should be on track to extract valuable information from the target. Whatever vulnerabilities, weaknesses, or other problems you find during your test should be fully documented and ranked in order of seriousness or importance. Once this is complete, the tester should be prepared to present a detailed report of their findings to the client. Presentation of the report may be the last task the tester has, or there may be additional steps. Expect any one of the following outcomes to occur upon completion of the testing phase:

- Presentation of the report to the client—This is just what it states; the report is generated and handed over to the client, and if they need any further explanations or discussion they will request it. If no explanation is needed, then the testing and reporting process is complete and the job is finished.
- Presentation plus recommendations—If the client requests it, the tester will explain the results of the test and then propose recommendations to fix the problems discovered. The client may not ultimately use all or any of the recommendations, but they will request them to see what needs to be done.
- Presentation plus recommendation with remediation—In this particular outcome the test is completed and the review and recommendations are made. What differentiates

this outcome from the others is that the client asks the tester to get involved at some level with actually implementing fixes.

Ultimately the client will determine what the next steps are and if this actually involves the testing party or not. The client will decide what the perfect balance of security versus convenience is in their environment and if the recommended fixes will maintain their desired balance. In other words, the client should not look at the results and immediately start thinking that they must fix every problem because doing so may impair the usefulness of the system. If the problems uncovered necessitate action, the next challenge is to ensure that if security controls are modified or if new ones are put in place, existing usability is not adversely affected.

Your role as a penetration tester is to provide your expertise to the client and try to answer their questions. Be proactive and attempt to address questions that they may have ahead of time, and always be available to answer questions after the fact should they have questions later on about your report.

Vulnerability Research and Tools

An important part of your toolkit as an ethical hacker will be the information gathered from vulnerability research. This process involves searching for and uncovering vulnerabilities in a system and determining their nature. In addition, the research seeks to classify each vulnerability as high, medium, or low. You or other security personnel can use this research to keep up to date on the latest weaknesses involving software, hardware, and environments.

The benefit of having this information is that an administrator or other personnel could use this information to position defenses. The information may also show where to place new resources or be used to plan monitoring.

Vulnerability research is not the same as ethical hacking in that it passively uncovers security issues, whereas the process of ethical hacking actively looks for the vulnerabilities. However, vulnerability scanning may be utilized as part of a test but not by itself.

What Is Incident Response?

As a penetration tester your job is to provide information that will reduce the chance of a security breach or incident to the lowest possible level, but does a regular user have no responsibility? Absolutely not; users have an important role to play as well. So as a well-prepared individual, you must plan how you will react when a security incident occurs or follow the plans the company or client provides to you. Planning ahead or knowing plans others have made will be beneficial because it will give you the edge when determining what to do after an incident and how to do it. Proper security incident response will determine if an incident is dealt with swiftly and completely or if it gets worse and out of control.

One of the first things to keep in mind when thinking about incident response is the fact that you may very well be dealing with something that falls under the banner of crime and as such will require that you take special care. Responding to an incident of computer

crime can be particularly challenging and should be left to professionals because the evidence that needs to be collected is intangible and can prevent a case from being prosecuted if you damage it.

Before going too far, however, it is worth defining what is inferred by the term *computer crime*. Computer crime is defined as any criminal act during which a computer or computing device is used in the commission of a crime. The goal of computer crime can be anything that negatively impacts in some way, shape, or form the operations of a company, individual, or government. By its very nature computer crime does not discriminate against activities that are initiated via the Internet or launched internally against a private network.

Incident Response Policies

The next detail that is important when considering incident response is incident response policy (IRP). The IRP defines the course of action that a company or organization will take in the time following a security incident. An IRP specifies many details, but the following are usually always included:

- Who will determine when and if a security incident has occurred
- Which individuals and/or departments are to be notified
- The means through which they will be notified
- Who will be responsible for responding to the incident
- Appropriate response guidelines
- What you as a system administrator will be responsible for doing in the event of an incident

So who will be involved in the incident response process? This depends on the organization, assets involved, and the overall severity of the situation. Several departments within an organization can work together such as human resources, public relations, information technology, corporate security, and others. The idea is to get the appropriate personnel and departments involved in order to properly deal with the situation at hand. The personnel involved can also determine which information can be released and to whom. For example, employees may not be privy to all the details of a security incident and may be informed only on a need-to-know basis.

Typically you will not be included in the development of this policy, but you will be included as someone who must follow it when the time comes and an incident has been declared by the person in charge.

Phases of an Incident and Response

There exist a number of phases in the incident response process; each incident will traverse these phases as the incident occurs, evolves, and moves to its final resolution. While an end user will not be truly aware of each of the phases of incident response, having some idea of the big picture may help you understand what you are doing and why you are being asked to do it. Each phase has distinct actions that take place within it, which you will learn more about as you move on, but for now let's take a high-level look at the incident response

process itself. Table 1.2 covers what is generally accepted by the National Institute of Standards and Technology (NIST) and others as the phases of incident response.

TABLE 1.2 The phases of incident response

Phase	Description
Response	It is important to early on establish just what has actually occurred. Is the incident an actual security incident or is it something else? The incident response team will be the ones responsible for making this determination as well as making the determination or discovery as to what was impacted.
Triage	The next step after the determination that a security incident has occurred is to determine how seriously the incident has impacted critical systems. Remember, not all systems or services will be affected the same way, and so some will require more attention than others. Also remember that some systems are more mission critical than others and will require more attention as well. In a computer crime security incident scenario, once the incident response team has evaluated the situation and determined the extent of the incidents, a triage approach will be implemented and the situation will be responded to according to criticality. If multiple events have occurred, the most serious event will be addressed first and remaining events will be investigated based on risk level.
Investigation	Once the response team discovers the cause of the problem, the investigative process can start. The investigation is designed to methodically collect evidence without destroying or altering it in any way. This process can be performed by internal personnel or by an external team where appropriate. The key point in either case is that the team involved in the investigative process understands how to collect the evidence properly because the end result of the process may be to take this collected information to court. So who may investigate a security incident may vary depending on the extent and type of security breach. In some cases internal teams or consultants may be all that's needed to investigate and analyze a crime scene; however, in some cases that may not be enough. It is possible under certain conditions to get local law enforcement involved in the investigation of a crime. This option will vary depending on the skills that the local law enforcement have. Some police departments are adept at dealing with computer crime, but this is not always the case. Investigations should never be taken lightly, and once local law enforcement is involved other issues arise. Police departments may not be able to respond in a timely fashion because corporate security problems are not part of the police mission and therefore are low priority.

TABLE 1.2 The phases of incident response *(continued)*

Phase	Description
Containment	It is necessary early on in the process of incident response to contain and control the crime scene as much as possible. When considering a crime scene it is important that no alterations or tampering of any sort occur to avoid damaging of evidence. This means that the crime scene should not be tampered with in any way including disconnecting any devices, wires, or peripherals or even shutting down the system. It is important to let trained professionals do their job at the crime scene.
Analysis and tracking	Evidence that has been gathered is useless unless it is examined and dissected to determine what has occurred. At this point the company will either be involving external professionals to examine the evidence or employing its own internal teams. These teams will be responsible for determining what evidence is relevant to the investigation and what is not. Additionally the team must maintain the chain of custody, which means that evidence must be accounted for and under positive control of the team at all times.
Recovery	During the recovery phase it is assumed that all relevant evidence has been collected and the crime scene has been cleaned. At this point the crime scene investigation has been completed and the effected systems can be restored and returned to service. This process will include restoring and rebuilding operating systems with their applications and data from backups or drive images.
Repair	In the event that a system has experienced substantial damage in the course of an attack, it becomes necessary to repair the system. The recovery process is designed to deal with rebuilding a system after evidence has been collected, but it does not account for potential damage done that may need to be repaired. Also, the collection of evidence may have required the removal of components to preserve the evidence, and those components will need to be replaced.
Debriefing and feedback	When the situation is under control, you will need to debrief and obtain feedback from all involved. The incident happened for a reason; presumably at this point you have determined what this reason is, at least in some part. The goal of this phase is to determine what the company did right, what it did wrong, and how to improve. Additionally, depending on the crime it may be necessary to start the process of informing clients and other agencies and regulatory bodies of the breach. This last point may be the most important one because failure to inform the appropriate regulatory bodies can mean you or your company is guilty of a crime.

It is important to note that the actual phases described here may vary wildly between organizations because they fine-tune the incident response process to their own needs. You may work in an industry that is heavily regulated and that has its own requirements that dictate a unique incident response process.

Incident Response Team

As organizations grow in size and importance it is likely that they will build or already have a group known as an incident response team. These teams will comprise individuals who have the training and experience to properly collect and preserve evidence of a crime and the associated components of the response process. You may, depending on your experience and background, be asked to participate in these teams in the event an incident occurs. Of course, you will know ahead of time and be prepared so you are ready when and if the call ever comes. As part of the incident response team, you must be both properly trained and have the requisite experience to respond to and investigate any security incident.

One of the components of incident response is the first individuals to respond when an incident is reported. In the broadest sense this can be the individuals appropriate for the security incident, including the following:

- IT personnel
- Human resources
- Public relations
- Local law enforcement
- Security officers
- Chief security officer

The goal of security response is to have a team in place that is well versed and aware of how to deal with security incidents. These members will know what to do and have been drilled on how to do it in the event an incident occurs. You may be asked, if you are not a member of the team, to contact certain individuals if a security incident occurs and determine what information to provide these first responders in order for them to do their job properly.

Incident Response Plans

Once a security incident has been recognized and declared, it is vital that the team have a plan to follow. This plan will include all the steps and details required to investigate the crime as necessary.

Some of the elements required to investigate a security crime are the following:

- If an IRP exists and is relevant, follow the process outlined in this plan.
- If an IRP does not currently exist, is out of data, or is irrelevant, then designate a lead examiner for the process so there is a coordinated response.
- Examine and evaluate the nature of the events that occurred and, as much as possible, determine the damage that has been incurred by the systems, services, and other items involved.

- Document and identify all involved components of the incident as completely as possible.
- Undertake a complete analysis to determine the different risk priorities for all systems, services, and other processes involved.
- Evaluate the need for outside expertise or consultants.
- Determine if local law enforcement involvement is needed.
- Determine how to contain the crime scene, including hardware, software, and other artifacts present.
- Decide how to collect the required evidence at the crime scene with special provisions for electronic evidence, hardware, and other items.
- Set up a procedure for interviewing personnel who may have additional knowledge or other information to share that would be beneficial to investigating the crime scene.
- Put in place a reporting mechanism for the crime and determine who should receive the report, such as regulatory bodies.

Business Continuity Plan

At some point you may be asked to follow a business continuity plan (BCP). This policy defines how the organization will maintain what is acceptable as normal day-to-day business in the event of a security incident or other event disruptive to the business. This plan will be called into play in the event that a disaster or severely disruptive event occurs and causes the business to become unavailable. If a company provides services to customers or clients and the business becomes unavailable, the company loses both money and the faith of its customers—something that no business wants to experience. The importance of the BCP cannot be understated because it is necessary in ensuring that the business continues to perform and can continue to operate on a limited basis through a disaster. A BCP is designed to ensure that vital systems, services, and documents that support the business remain available to alert key stakeholders and recover assets even when the bulk of critical systems are down.

Next to a BCP, and closely intertwined with it, is a disaster recovery plan (DRP). This document outlines a policy that defines how personnel and assets will be safeguarded in the event of a disaster and how those assets will be restored and brought back to an operating state once the disaster passes. The DRP typically will include a list of responsible individuals who will be involved in the recovery process, an inventory of vital hardware and software, steps to respond to and address the outage, and how to rebuild affected systems.

Supporting Business Continuity and Disaster Recovery

Several techniques can be used to keep the organization running and diminish the impact of a disaster when it occurs. Some of these techniques are discussed in this section. While some or all of these techniques may be out of your control, they are provided here for you to understand what IT will do to keep services available for you and clients.

Fault tolerance is a valuable tool in the company arsenal because it provides the ability to weather potential failures while providing some measure of service. While this service may not be optimal, it should be enough to maintain some business operations even if not at the normal level of performance. Fault-tolerant mechanisms include service and infrastructure duplication designed to handle a component failure when it occurs.

Another mechanism commonly used by companies is high-availability architecture. This is simply a gauge of how well the system is providing its services, specifically how available the system actually is. Ideally a system should be available 100 percent of the time, but in practice this is usually not possible and over long periods of time unlikely. High availability simply states, as a percentage, how available a system is, so the closer a system's availability is to 100 percent, the less time it spends offline. High availability can be attained by having redundant systems and reliable backup systems. When implemented properly, it means that the services you rely on to do your job and provide service to clients are available and ready to use for the greatest possible amount of time.

A document that is commonly mentioned when discussing high availability and fault tolerance is a service-level agreement (SLA). This document spells out the obligations of the service provider to you, the client. Specifically, an SLA is a legal contract that lays out what the service provider will provide, at what performance level, and steps that will be taken in the event of an outage. For an idea of what an SLA looks like, you can look at the contract you signed with your cell phone provider. Cell phone providers use this document to describe what they will provide and what you can expect should an outage occur. This document can include specific performance and availability levels that are expected and the associated penalties for not meeting these levels. Additionally it will spell out the parties responsible and the extent of their responsibilities in the event of a disaster, such as who will take care of the problems related to the disaster.

Alternate sites are another technique used in the event of a system failure or disaster. The idea is to have another location to conduct business operations from in the event of a disaster. Under ideal conditions all operations will be moved to an alternate site if the primary or normal site is no longer able to provide services.

Not all alternate sites are created equal, however. There are three types of sites that an organization can use:

- **Cold site**—This is the most basic type of alternate site and the least expensive to operate. A cold site, by normal definition, does not include backed-up copies of data or configuration data from the primary location. It also does not have any sort of hardware set up and in place. The lack of these essentials makes the cold site the cheapest option but also contributes to greater outage times because this infrastructure will need to be built and the data restored prior to going back online.
- **Warm site**—This is the middle-of-the-road option, offering a balance between expense and outage time. A warm site typically has some if not all of the hardware in place, with other items such as power and Internet connectivity already established though not to the degree that the primary site has in place. This type of site also has some backups on hand, though they may be out of date by several days or even weeks.

- **Hot site**—This is the top option as far as capabilities go, offering little to no downtime and the greatest expense. This type of site typically has a high degree of synchronization with the primary site up to the point of completely duplicating the primary site. The setup requires a high degree of complexity in the form of complex network links and other systems and services designed to keep the sites in sync. This level of complexity adds to the expense of the site but also has the advantage of substantially reduced (or eliminated) downtime.

Before an alternate site can work, however, the company must have a data backup, and this backup must be kept secure because it contains information about the company, its clients, and its infrastructure. Backups should be stored safely and securely, with copies kept both onsite and offsite to give optimal protection. In addition, backups should always be stored on separate media and ideally in a locked location offsite. Most of the time, these backups are encrypted for further protection of unauthorized disclosure if stolen. Other safeguards should be taken to protect the backups from environmental concerns such as fire, floods, and earthquakes, to name a few.

Recovering Systems

Secure recovery requires a number of items to be in place; primary among these is the requirement to have an administrator designated to guide the recovery process. This administrator may come to you as a trained employee to carry out the recovery process. They may ask you to follow specific steps that you will have been trained in and indicate what needs to be restored. As is the case with any backup and recovery process, you will need to review the steps and relevance of the process and update the process where necessary or at least consult with experts on what to do.

Planning for Disaster and Recovery

In order to properly plan for disaster recovery you will need to know where you stand, specifically where the company stands. You need to completely assess the state of preparedness of the organization and understand what you need to do to be properly prepared.

In order to properly plan for disaster recovery, you should observe the following guidelines and best practices:

- Once your organization has established a BCP it is important for this plan to undergo regular testing and review. Consider conducting simulations and drills designed to evaluate the efficacy of the plan.
- If the company has not recently tested the DRP, make it a point to do so. Much like BCPs, consider the use of drills and other similar types of simulations to evaluate how well the DRP functions.
- Always consider and evaluate the proper redundancy measures for all critical resources. Look for adequate protection for systems such as servers, routers, and other devices in the event they are needed for emergency use.
- Check with all critical service providers to ensure that they've taken adequate precautions to guarantee that the services provided will be available.

- Check for the existence or the ability to obtain spare hardware wherever necessary. Ensure that the devices are not only appropriate for use but also can be obtained quickly in an emergency.
- Evaluate any existing SLAs currently in place so that you know what constitutes acceptable downtime.
- Establish mechanisms for communication that do not require the company resources, which may be unavailable. Such communication channels should also take into account that power may be unavailable.
- Ensure that the organization's designated hot site can be brought online immediately.
- Identify and document any and all points of failure, as well as any up-to-date redundancy measures that have been put in place to safeguard these points.
- Ensure that the company's redundant storage is secure.

Once the incident response process has been defined, at a high level at this point, you can turn your attention to the collection of evidence from a crime scene. While you may be involved in this process, it is possible that you will require special teams or external consultants for this task.

In many cases companies will have specially trained professionals on staff or externally contracted to respond to security incidents and collect evidence. It is important for you to know which it is or at the very least who to contact in the event an incident happens.

Evidence-Collection Techniques

Proper collection of evidence is essential as stated previously and is something that is best left to professionals. In addition, when a crime has been suspected it becomes mandatory to have trained professionals involved in the process. If this is not you, then you should not disturb the crime scene; rather you should contact a manager or someone in charge for guidance on how to proceed. The process here is really one of forensics—the methodical and defensible process of collecting information from a crime scene. This process is best left to those professionals trained to do so because novices can inadvertently damage evidence in such a way that makes the investigation impossible or indefensible in court. Trained personnel will know how to avoid these blunders and properly collect everything relevant.

Evidence Types

Evidence is the key to proving a case, and not all evidence is created equal and should not be treated as such. Collecting the wrong evidence or treating evidence incorrectly can have an untold impact on your company's case, which should not be underestimated.

Table 1.3 lists some of the different types of evidence that can be collected and what makes each unique.

TABLE 1.3 Types of evidence

Evidence	Description
Best	The best evidence is category evidence that is admissible by requirement in any court of law. The existence of best evidence eliminates your ability to use any copies of the same evidence in court.
Secondary	Secondary evidence is a copy of the original evidence. This could be items such as backups and drive images. This type of evidence may not always be admissible in a court of law and is not admissible if best evidence of the item exists.
Direct	Direct evidence is received as the result of testimony or interview of an individual. This individual could have obtained their evidence as a result of observation. Evidence in this category can be used to prove a case based on its existence.
Conclusive	Conclusive evidence includes that which is above dispute. Conclusive evidence is considered so strong that it directly overrides all other evidence types by its existence.
Opinion	Opinion evidence is derived from an individual's gut feelings. Opinion evidence is divided into the following types: Expert–Any evidence that is based on known facts, experience, and an expert's knowledge. Non-expert–Any evidence that is derived from fact alone and comes from a non-expert in the field.
Corroborative	Corroborative evidence is obtained from multiple sources and is supportive in nature. This type of evidence cannot stand on its own and is used to bolster the strength of other evidence.
Circumstantial	Circumstantial evidence can be obtained from multiple sources, but unlike corroborative evidence it is only able to indirectly infer a crime.

Chain of Custody

When collecting evidence the chain of custody must be maintained at all times. The chain of custody documents the whereabouts of the evidence from the point of collection to the time it is presented in court and then when it is returned to its owner or destroyed. The chain is essential because any break in the chain or question about the status of evidence at

any point can result in a case being thrown out. A chain of custody needs to include every detail about the evidence, from how it was collected up to how it was processed.

A chain of custody can be thought of as enforcing or maintaining six key points. These points will ensure that you focus on how information is handled at every step:

- What evidence has been collected?
- How was the evidence obtained?
- When was the evidence collected?
- Who has handled the evidence?
- What reason did each person have for handling the evidence?
- Where has the evidence traveled and where was this evidence ultimately stored?

Also remember if you are involved to keep the chain of custody information up to date at all times. Every time any evidence is handled by an investigator, you must update the record to reflect this. You may be asked at some point to sign off on where evidence was or that it was collected from you; this would be an example of where you would fit in regard to the chain of custody. This information should explain every detail such as what the evidence actually consists of, where it originated, and where it was delivered to. It is important that no gaps exist at any point.

For added legal protection, evidence can be validated through the use of hashing to prove that it has not been altered. Ideally the evidence you collected at the crime scene is the same evidence you present in court.

Remember, a verifiable or non-verifiable chain of custody can win or lose a case.

Rules of Evidence

All evidence, no matter the type, may not be admissible in court. Evidence cannot be presented in court unless certain rules are followed, and you should review those rules ahead of time. The five rules of evidence presented here are general guidelines and are not consistent across jurisdictions:

- Reliable—The evidence presented is consistent and leads to a common conclusion.
- Preserved—Chain of custody comes into play and the records help identify and prove the preservation of the evidence in question.
- Relevant—The evidence directly relates to the case being tried.
- Properly identified—Records can provide proper proof of preservation and identification of the evidence.
- Legally permissible—The evidence is deemed by the judge to fit the rules of evidence for the court and case at hand.

Recovering from a Security Incident

When a security incident happens, and it will happen, the company should have a plan to restore business operations as quickly and effectively as possible. This may require you and possibly your team to correctly assess the damage, complete the investigation, and then

initiate the recovery process. From the time of the initial security incident onward, the organization presumably has been operating at some reduced capacity, and so you need to recover the systems and environment as quickly as possible to restore normal business operations. Other key requirements are the need to generate a report on what happened and the ability to communicate with appropriate team members.

Reporting a Security Incident

Once an incident has been responded to and a team has gotten involved to assess the damage and start the cleanup, the required parties will need to be informed. These parties will be responsible for getting the ball rolling whether it is legal action, an investigative process, or other requirements as necessary.

When considering how to report a security incident the following guidelines are worth keeping in mind and can prove helpful at the time of crisis:

- Adhere to known best practices and guidelines that have been previously established. These best practices and guidelines will describe how to best assess the damage and implement loss control as necessary.
- Wherever feasible refer to previously established guidelines as documented and described in the company IRP. The IRP should include guidelines on how to create a report and who to report to. Furthermore, the IRP should define the formats and guidelines for putting the report together in order to ensure that the information is actually usable by its intended audience.
- Consider the situations where it is necessary to report the incident to local law enforcement in addition to the company officials.
- Consider the situations and conditions about when and if the security incident must be reported to regulatory bodies as required by law.
- In situations where security incidents are reported outside the organization, note this in the company incident report.

During the preparation of a security incident report include all the relevant information to detail and describe the incident. The following items should be included at a minimum:

- A timeline of the events of the security incident that includes any and all actions taken during the process.
- A risk assessment that includes extensive details of the state of the system before and after the security incident occurred.
- A detailed list of any and all who took part in the discovery, assessment, and final resolution (if this has occurred) of the security incident. It is important to include every person who took part in this process regardless of how important or unimportant their role may be perceived.
- Detailed listing of the motivations for the decisions that were made during the process. Document these actions in a format that states what each action was and what factors led to the decision to take the designated action.

- Recommendation as to what could be done to prevent a repeat of the incident and what could be done to reduce any damage that may result.
- Two sections in the report to ensure that it is usable by all parties. First, prepare a long-format report that includes specific details and actions that occurred during the security incident. Second, include an executive-level summary that provides a high-level, short-format description of what occurred.

Ethics and the Law

As an ethical hacker, you need to be aware of the law and how it affects what you do. Ignorance or lack of understanding of the law not only is a bad idea but can quickly put you out of business—or even in prison. In fact, under some situations the crime may be serious enough to get you prosecuted in several jurisdictions in different states, counties, or even countries due to the highly distributed nature of the Internet. Of course, prosecution of a crime can also be difficult considering the web of various legal systems in play. A mix of common, military, and civil law exists, requiring knowledge of a given legal system to be successful in any move toward prosecution.

As an ethical hacker you must also obey the Code of Ethics as defined by the EC-Council. One thing to remember though about ethics is that while you can get in legal trouble for violating a law, breaking a code of ethics won't get you in legal trouble but could lead to other actions such as getting decertified.

Depending on when and where your testing takes place, it is even possible for you to break religious laws. Although you may never encounter this problem, it is something that you should be aware of—you never know what type of laws you may break.

Always ensure that you exercise the utmost care and concern to ensure that you observe proper safety and avoid legal issues. When your client has determined their goals along with your input, together you must put the contract in place. Remember the following points when developing a contract and establishing guidelines:

Trust The client is placing trust in you to use proper discretion when performing a penetration test. If you break this trust, it can lead to the questioning of other details such as the results of the test.

Legal Implications Breaking a limit placed on a test may be sufficient cause for your client to take legal action against you.

The following is a summary of laws, regulations, and directives that you should have a basic knowledge of:

- 1973—U.S. Code of Fair Information Practices governs the maintenance and storage of personal information by data systems such as health and credit bureaus.

- 1974—U.S. Privacy Act governs the handling of personal information by the U.S. government.
- 1984—U.S. Medical Computer Crime Act addresses illegally accessing or altering medication data.
- 1986 (amended in 1996)—U.S. 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—U.S. Electronic Communications Privacy Act prohibits eavesdropping or the interception of message contents without distinguishing between private or public systems.
- 1994—U.S. Communications Assistance for Law Enforcement Act requires all communications carriers to make wiretaps possible.
- 1996—U.S. Kennedy-Kassebaum Health Insurance and Portability Accountability Act (HIPAA) (with additional requirements added in December 2000) addresses the issues of personal healthcare information privacy and health plan portability in the United States.
- 1996—U.S. National Information Infrastructure Protection Act was enacted in October 1996 as part of Public Law 104-294; it amended the Computer Fraud and Abuse Act, which is codified in 18 U.S.C. § 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 or SarBox) is a law pertaining to accountability for public companies relating to financial information.
- 2002—Federal Information Security Management Act (FISMA) is a law designed to protect the security of information stored or managed by government systems at the federal level.

Summary

When becoming an ethical hacker, you must develop a rich and diverse skill set and mindset. Through a robust and effective combination of technological, administrative, and physical measures, organizations have learned to address their given situation and head off major problems through detection and testing. Technology 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 has helped security become much stronger but still has not eliminated the need for vigilance.

Administrative countermeasures such as policies, procedures, and other rules have also been strengthened and implemented over the past decade. Physical measures include devices such as cable locks, device locks, alarm systems, and other similar devices. Your new role as an ethical hacker will deal with all of these items, plus many more.

As an ethical hacker you must know not only the environment you will be working in but also how to find weaknesses and address them as needed. You will also need to understand the laws and ethics involved and know the client's expectations. Understand the value of getting the proper contracts in place and not deviating from them.

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. Breaking out of the scope of a contract can expose you to legal problems and become a career-ending blunder.

Exam Essentials

Know the purpose of an ethical hacker. Ethical hackers perform their duties against a target system *only* with the explicit permission of the system owner. To do so without permission is a violation of ethics and the law in some cases.

Know the difference between black, white, and gray box tests. Know the differences in the types of tests you can offer to your client and the advantages of each. Not all tests are the same nor will they yield the same results. Make sure you know what your client's expectations are so you can choose the most appropriate form.

Understand your targets. Be sure you know what the client is looking to gain from a pen test early in the process. The client must be able to provide some guidance as to what they are trying to accomplish as a result of your services.

Understand the Code of Ethics. Be sure you know what is required as acceptable behavior when you become a CEH. Violations of the ethical code could easily get you decertified by the EC-Council if serious enough and reported.

Know your opponents. Understand the differences between the various types of hackers. You should know what makes a gray-hat hacker different from a black-hat hacker, as well as the differences between all types.

Know your tools and terms. The CEH exam is drenched with terms and tool names that can eliminate even the most skilled test takers if they don't know what the question is even talking about. Familiarize yourself with all the key terms, and be able to recognize the names of the different tools on the exam.

Review Questions

1. If you have been contracted to perform an attack against a target system, you are what type of hacker?
   - **A.** White hat
   - **B.** Gray hat
   - **C.** Black hat
   - **D.** Red hat
2. Which of the following describes an attacker who goes after a target to draw attention to a cause?
   - **A.** Terrorist
   - **B.** Criminal
   - **C.** Hacktivist
   - **D.** Script kiddie
3. What level of knowledge about hacking does a script kiddie have?
   - **A.** Low
   - **B.** Average
   - **C.** High
   - **D.** Advanced
4. Which of the following does an ethical hacker require to start evaluating a system?
   - **A.** Training
   - **B.** Permission
   - **C.** Planning
   - **D.** Nothing
5. A white-box test means the tester has which of the following?
   - **A.** No knowledge
   - **B.** Some knowledge
   - **C.** Complete knowledge
   - **D.** Permission
6. Which of the following describes a hacker who attacks without regard for being caught or punished?
   - **A.** Hacktivist
   - **B.** Terrorist
   - **C.** Criminal
   - **D.** Suicide hacker

7. What is a code of ethics?
   - **A.** A law for expected behavior
   - **B.** A description of expected behavior
   - **C.** A corporate policy
   - **D.** A standard for civil conduct

8. The group Anonymous is an example of what?
   - **A.** Terrorists
   - **B.** Script kiddies
   - **C.** Hacktivists
   - **D.** Grayware

9. Companies may require a penetration test for which of the following reasons?
   - **A.** Legal reasons
   - **B.** Regulatory reasons
   - **C.** To perform an audit
   - **D.** To monitor network performance

10. What should a pentester do prior to initiating a new penetration test?
    - **A.** Plan
    - **B.** Study the environment
    - **C.** Get permission
    - **D.** Study the code of ethics

11. Which of the following best describes what a hacktivist does?
    - **A.** Defaces websites
    - **B.** Performs social engineering
    - **C.** Hacks for political reasons
    - **D.** Hacks with basic skills

12. Which of the following best describes what a suicide hacker does?
    - **A.** Hacks with permission
    - **B.** Hacks without stealth
    - **C.** Hacks without permission
    - **D.** Hacks with stealth

13. Which type of hacker may use their skills for both benign and malicious goals at different times?
    - **A.** White hat
    - **B.** Gray hat
    - **C.** Black hat
    - **D.** Suicide hacker

14. What separates a suicide hacker from other attackers?

A. A disregard for the law

B. A desire to be helpful

C. The intent to reform

D. A lack of fear of being caught

15. Which of the following would most likely engage in the pursuit of vulnerability research?

A. White hat

B. Gray hat

C. Black hat

D. Suicide hacker

16. Vulnerability research deals with which of the following?

A. Actively uncovering vulnerabilities

B. Passively uncovering vulnerabilities

C. Testing theories

D. Applying security guidance

17. How is black-box testing performed?

A. With no knowledge

B. With full knowledge

C. With partial knowledge

D. By a black hat

18. A contract is important because it does what?

A. Gives permission

B. Gives test parameters

C. Gives proof

D. Gives a mission

19. What does TOE stand for?

A. Target of evaluation

B. Time of evaluation

C. Type of evaluation

D. Term of evaluation

20. Which of the following best describes a vulnerability?

A. A worm

B. A virus

C. A weakness

D. A rootkit