

ATME COLLEGE OF ENGINEERING

13th KM Stone, Bannur Road, Mysore - 560 028



A T M E

College of Engineering

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

- CYBER SECURITY



LECTURE NOTES

COURSE: Hackers Technique, Tools and Incident Handling

COURSE CODE: BCY515C

SEMESTER: V

COURSE COORDINATOR: Ms. Darshini Y

(ACADEMIC YEAR 2026)

INSTITUTIONAL MISSION AND VISION

Objectives

- To provide quality education and groom top-notch professionals, entrepreneurs and leaders for different fields of engineering, technology and management.
- To open a Training-R & D-Design-Consultancy cell in each department, gradually introduce doctoral and postdoctoral programs, encourage basic & applied research in areas of social relevance, and develop the institute as a center of excellence.
- To develop academic, professional and financial alliances with the industry as well as the academia at national and transnational levels.
- To develop academic, professional and financial alliances with the industry as well as the academia at national and transnational levels.
- To cultivate strong community relationships and involve the students and the staff in local community service.
- To constantly enhance the value of the educational inputs with the participation of students, faculty, parents and industry.

Vision

Development of academically excellent, culturally vibrant, socially responsible and globally competent human resources.

Mission

- To keep pace with advancements in knowledge and make the students competitive and capable at the global level.
- To create an environment for the students to acquire the right physical, intellectual, emotional and moral foundations and shine as torch bearers of tomorrow's society.
- To strive to attain ever-higher benchmarks of educational excellence

MODULE 1

Chapter 1. Hacking: The Next Generation

THIS BOOK WILL COVER A WIDE RANGE of techniques and technologies that **hackers** can use to compromise a system in one way or another. Before you go further, it is important to first understand what hackers are and where they come from.

The first generation of hackers who emerged in the 1960s were individuals who would be called "geeks" or technology enthusiasts today. These early hackers would go on to create the foundation for technologies such as the ARPANET, which paved the way for the Internet. They also initiated many early software-development movements that led to what is known today as *open source*. Hacking was motivated by intellectual curiosity; causing damage or stealing information was "against the rules" for this small number of people.

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

Over the past two decades, the definition of what a hacker is has evolved dramatically from what was accepted in the 1980s and even the 1990s. Current hackers defy easy classification and require categorization into several groups to better match their respective goals. Here is a brief look at each of the groups to better understand what the information technology industry is dealing with:

- **Script kiddies**—These hackers occupy the lowest level of the hacker hierarchy. They typically possess very basic skills and rely upon existing tools that they can locate on the Internet. These hackers are the beginners and may or may not understand the impact of their actions in the larger scheme of things. It is important, however, not to underestimate the damage these individuals can cause; they can still do a great deal of harm.
- **White-hat hackers**—These individuals know how hacking works and the danger it poses, but use their skills for good. They adhere to an ethic of "do no harm." White-hat hackers are sometimes also referred to as **ethical hackers**, which is the name most widely known by the general public.
- **Gray-hat hackers**—Hackers in this class are "rehabilitated" hackers or those who once were on "the dark side," but are now reformed. For obvious reasons, not all people will trust a gray-hat hacker.
- **Black-hat hackers**—A black-hat hacker has, through actions or stated intent, indicated that his or her hacking is designed to break the law, disrupt systems or businesses, or generate an illegal financial return. Hackers in this class should be considered to be "up to no good," as the saying goes. They may have an agenda or no agenda at all. In most cases, black-hat hackers and outright criminal activity are not too far removed from one another.

MODULE 1

The purpose of this book is to teach you how to ensure the security of computers and networks by learning and understanding the mindset of individuals out to compromise those systems. To defend information technology assets, you need to understand the motivations, tools, and techniques that attackers commonly use.

Chapter 1 Topics

This chapter covers the following topics and concepts:

- What the profiles of hackers, crackers, and cybercriminals are
- What a look back at the history of computer hacking shows
- What ethical hacking and penetration testing are
- What common hacking methodologies are
- How to perform a penetration test
- What the roles of ethical standards and the law are

Chapter 1 Goals

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

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

Profiles of Hackers, Crackers, and Cybercriminals

In today's world, organizations have quickly learned that they can no longer afford to underestimate or ignore the threat attackers pose. Organizations of all sizes have learned to reduce threats through a combination of technological, administrative, and physical measures designed to address a specific range of problems. Technological measures include devices and techniques such as virtual private networks (VPNs), cryptographic protocols, intrusion detection systems (IDS), intrusion prevention systems (IPS), access control lists (ACLs), biometrics, smart cards, and other devices. Administrative controls include policies, procedures, and other rules. Physical measures include devices such as cable locks, device locks, alarm systems, and other similar devices. Keep in mind that each of these devices, even if expensive, can be cheaper and more effective than cleaning up the aftermath of an intrusion.

MODULE 1

FYI

People who break the law or break into systems without authorization are more correctly known as "**crackers**." The press does not usually make this distinction, because "hacker" has become such a universal term. However, there are many experienced hackers who never break the law, and who define hacking as producing an outcome the system designer never anticipated. In that respect, Albert Einstein can be considered to have "hacked" Newtonian physics. In the interest of simplicity, this book will use the term "hacker" to describe those who are either good or evil. No offense is intended to either group.

While discussing attacks and attackers, security professionals must be thorough in assessment and evaluation of the threat by also considering where it comes from. When evaluating the threats against an organization and possible sources of attack, always consider the fact that attackers can come from both outside and inside the organization. A single disgruntled employee can cause tremendous amounts of damage because he or she is an approved user of the system. In just about any given situation, the attacks originating from outside the firewall will greatly outnumber the attacks that originate from the inside. However, an insider may go unnoticed longer and also have some level of knowledge of how things work ahead of time, which can result in a more effective attack.

NOTE

Never underestimate the damage a determined individual can do to computer systems. For example, Michael Calce, commonly known as MafiaBoy, was an individual who in February 2000 launched a series of **denial of service (DoS)** attacks that were responsible for causing damages estimated upwards of \$1.2 billion.

NOTE

Both insiders and outsiders rely on exploits of some type. Remember that an **exploit** refers to a piece of software, a tool, or a technique that targets or takes advantage of a **vulnerability**—leading to privilege escalation, loss of integrity, or denial of service on a computer system.

Because the risk to any organization is very real, it is up to each organization to determine the controls that will be most effective in reducing or mitigating the threats it faces. When considering controls, you can examine something called the TAP principle of controls. TAP is an acronym for technical, administrative, and physical, the three types of controls you can use in risk mitigation. Here's a look at each type with a few examples:

- **Technical**—Technical controls take the form of software or hardware such as firewalls, proxies, **intrusion detection systems (IDS)**, **intrusion prevention systems (IPS)**, biometric **authentication**, permissions, auditing, and similar technologies.
- **Administrative**—Administrative controls take the form of policies and procedures. An example is a password policy that defines what makes a good password. In numerous cases, administrative controls may also fulfill legal requirements, such as policies that dictate

MODULE 1

privacy of customer information. Other examples of administrative policy include the rules governing the hiring and firing of employees.

- **Physical**—Physical controls are those that protect assets from traditional threats such as theft or vandalism. Mechanisms in this category include locks, cameras, guards, lighting, fences, gates, and other similar devices.

The Hacker Mindset

Like many criminals, black-hat hackers do not consider their activities to be illegal or even morally wrong. Depending on whom you ask, you can get a wide range of responses from hackers on how they view their actions. It is also not unheard of for hackers or criminals to have a code of ethics that they hold sacred, but seem more than a little skewed to others. In defense of their actions, hackers have been known to cite all sorts of reasons, including the following:

- **The no-harm-was-done fallacy**—If one enters a system, even in an unauthorized manner, it is OK as long as nothing is stolen or damaged in the process.
- **The computer game fallacy**—If the computer or system did not take any action or have any mechanism to stop the attack, it must be OK.
- **The law-abiding citizen fallacy**—Writing a virus is not illegal, so it must be OK.
- **The shatterproof fallacy**—Computers cannot do any real harm. The worst that can happen is a deleted file or erased program.
- **The candy-from-a-baby fallacy**—If it is so easy to copy a program or download a song, how can it be illegal?
- **The hacker fallacy**—Information should be free. No one should have to pay for books or media. Everyone should have free access.

NOTE

Although it is true that the mere act of writing a computer virus is not illegal, releasing it into the "wild" is illegal.

NOTE

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

Another example of attempting to explain the ethics applied to hackers is known as the hacker ethic. This set of standards dates to Steven Levy in the 1960s. In the preface of his book, *Hackers: Heroes of the Computer Revolution*, Levy stated the following:

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

MODULE 1

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

Ethics are an important component in understanding what makes a hacker, but far from the only component. One must also consider motivation. Anyone who has watched a police drama or is a fan of detective stories knows that there are three things needed to commit a crime:

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

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

- **Monetary**—Attacks committed with the intention of reaping financial gains.
- **Status**—Attacks committed with the intention of gaining recognition and, by extension, increased credibility within a given group (for example, a hacking group).
- **Terrorism**—Attacks designed to scare, intimidate, or otherwise cause panic in the victim or target group.
- **Revenge or grudge**—Attacks conceived and carried out by individuals who are angry at an organization. Attacks of this nature are often launched by disgruntled employees or customers.
- **Hacktivism**—Attacks that are carried out to bring attention to a cause, group, or political ideology.
- **Fun**—Attacks that are launched with no specific goal in mind other than to just carry out an attack. These attacks can be indiscriminate in their execution.

No matter what the hackers' motivations are, any of them might result in the commission of a computer-based crime. For example, attackers may hack a game server to boost their stats in an online game against their friends, but they still have entered a server without authorization.

HACKTIVISM

A relatively new form of hacking is the idea of hacking in behalf of a cause. In the past, hacking was done for a range of different reasons that rarely included social expression. Over the past decade, however, there have been an increasing number of security incidents with roots in social or political activism. Examples include defacing Web sites of public officials, candidates, or agencies that an individual or group disagrees with, or performing DoS attacks against corporate Web sites.

A sampling of common attacks that fit the definition of computer crime include the following:

MODULE 1

- **Theft of access**—Stealing passwords, stealing usernames, and subverting access mechanisms to bypass normal authentication. In a number of situations, the very act of possessing stolen credentials such as passwords may be enough to bring formal charges.
- **Network intrusions**—Accessing a system of computers without authorization. Intrusions may not even involve hacking tools; the very act of logging into a guest account may be sufficient to be considered an intrusion.
- **Emanation eavesdropping**—Sniffing devices for intercepting radio frequency (RF) signals generated by computers or terminals. Years ago, the U.S. Department of Defense established a classified program codenamed TEMPEST that was designed to shield or suppress electronic emanations to protect sensitive and classified government information.
- **Social engineering**—Basically, telling lies to manipulate people into divulging information they otherwise would not provide. Information such as passwords, PINs (personal identification numbers), or other details can be used to attack computer-based systems. Although not necessarily a crime in every specific situation, social engineering methods such as pretexting (tricking an individual to reveal information under false pretenses) are often illegal.
- **Posting and/or transmitting illegal material**—Distributing pornography to minors is illegal in numerous jurisdictions, as is possessing or distributing child pornography.
- **Fraud**—Intentional deception designed to produce illegal financial gain or to damage another party.
- **Software piracy**—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.
- **Dumpster diving**—Gathering material that has been discarded or left in unsecured or unguarded receptacles. **Dumpster diving** often enables discarded data to be pieced together to reconstruct sensitive information.
- **Malicious code**—Software written with a deliberate purpose to cause damage, destruction, or disruption. Examples include viruses, worms, spyware, and **Trojan horses**.
- **Denial of service (DoS) and distributed denial of service (DDoS) attacks**—Overloading a system's resources so it cannot provide the required services. Both DoS and DDoS have the same effect, except that **distributed denial of service (DDoS)** is launched from large numbers of hosts that have been compromised and act after receiving a particular command.
- **IP address spoofing**—Substituting a forged IP address for a valid address in network traffic or a message to disguise the true location of the message or person. This attack method may also be used as a component of other larger attacks such as DoS or DDoS attacks.
- **Unauthorized destruction or alteration of information**—Modifying, destroying, or tampering with information without appropriate permission. This can involve manual or automated tools that have been developed for this purpose to change information at rest or in motion.
- **Embezzlement**—A form of financial fraud that involves theft or redirection of funds as a result of violating a position of trust.
- **Data-diddling**—The unauthorized modification of data used to forge or counterfeit information. Examples include changing performance review marks, adjusting expense account limits, or "tweaking" reports after the fact.

MODULE 1

- **Logic bomb**—A piece of code designed to cause harm, a **logic bomb** is intentionally inserted into a software system and will activate upon the occurrence of some predetermined data, time, or event.

A Look Back at the History of Computer Hacking

Typical early hackers were technology enthusiasts who were curious about the new technology of networks and computers and wanted to see just how far they could push its capabilities. In the decades since, hacking has changed quite a bit—getting more advanced and cleverer as the technology advanced. For example, in the 1970s, when mainframes were more common in corporate and university environments, hacking was mostly confined to those systems. The 1980s saw the emergence of personal computers (PCs), which meant every user had a copy of an operating system. As these systems were very similar, a hack that worked on one machine would work on nearly every other PC as well. Although the first Internet worm in November 1988 exploited a weakness in the UNIX `sendmail` command, worm and virus writers moved their attention to the world of PCs, where most infections occur today.

As hackers evolved so did their attacks as their skills and creativity increased. The first World Wide Web browser, Mosaic, was introduced in 1993. By 1995, hackers began defacing Web sites. Some of the earliest hacks were quite funny, if not somewhat offensive or vulgar. In August 1995, hackers hacked The MGM Web site for the movie "Hackers" suggesting readers attend the DEFCON hacker conference instead. A 1996 hack of the Department of Justice Web site replaced Attorney General Janet Reno's picture with that of Adolf Hitler. The next month, hackers defaced the CIA Web site, and later that year the Air Force Web site featured a link to Area 51, a secret government site in Nevada, long linked in the popular mind to UFOs. By May 2001, Web sites were being hacked at such a rate that the group that documented them gave up trying to keep track (see <http://attrition.org/mirror/attrition/>).

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

Numerous products emerged in the 1990s and early 2000s—antivirus, firewalls, intrusion detection systems, and remote access controls—each designed to counter an increasing number of new and diverse threats.

As technology, hackers, and countermeasures improved and evolved, so did the types of attacks and strategies that initially spawned them. As is true in the security field and the technology field as a whole, new developments move rapidly, and old defensive measures lose their effectiveness as time marches on. Attackers started introducing new threats in the form of worms, spam, spyware, adware, and rootkits. These attacks went beyond harassing and irritating the public; they

MODULE 1

also caused widespread disruptions by attacking the technologies that society increasingly depended on.

Hackers also started to realize that it was possible to use their skills to generate money in all sorts of interesting ways. For example, attackers 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 e-mail messages that advertise a product or service. Because sending out bulk e-mail costs mere pennies, it takes only a small number of purchasers to make a nice profit.

Keep in mind that in the security field, there is an ongoing battle between attacker and defender to establish dominance. Attackers change their tactics in an effort to keep their attacks as fresh and effective as possible, while defenders improve and adapt their defenses to counter the attacks as well as anticipate and thwart new ones.

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

Security and technology professionals are on the front lines and as such must be aware of and deal with increasingly complex crimes. One of the biggest challenges security professionals face is staying current on the latest technologies, trends, and threats that appear in an ever-changing landscape. To be effective, security professionals must continually expand their understanding of many diverse but related areas such as ethical hacking, ethics, legal issues, cybercrime, forensic techniques, incident response, and other technologies.

Additionally, security professionals must strive to understand the reasons and motivations behind the hacker or criminal mindset. Understanding the motivations can, in some cases, yield valuable insight into why a given attack has been committed or may be committed.

FYI

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

MODULE 1

As stated earlier, hacking is by no means a new phenomenon; instead it has existed in one form or another since the 1960s. It is only for a portion of the time since then that hacking has been viewed as a crime and situation that must 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. According to Morris, his worm was designed to count the number of systems connected to the Internet. Due to a design flaw, the worm replicated quickly and indiscriminately, causing widespread slowdowns across the globe. Morris was eventually convicted under the 1986 Computer Fraud and Abuse Act and was sentenced to community service in lieu of any jail time. (Interestingly, his father, Robert Morris Sr., was the chief scientist of the National Security Agency at the time).
- In December 1999, David L. Smith created the Melissa virus, which was designed to e-mail itself to entries in a user's address book and later delete files on the infected system. Smith was convicted on charges of computer fraud and theft of services, and served 20 months in prison as well as being ordered to pay \$5,000 in fines and penalties for the damages he caused.
- In February 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 e-mail itself out to each. De Wit was ultimately sentenced to 150 hours of community service and 75 days in jail.
- In December 2004, Adam Botbyl and two friends conspired to steal credit card information from the Lowe's hardware chain. The three were charged with several counts of theft and fraud, but ultimately only Botbyl served any time.
- In September 2005, Cameron Lacroix (nickname "cam0") 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. Mr. Lacroix was charged with computer fraud and was sentenced to 11 months in a juvenile detention facility as a result of his actions.

NOTE

People have written worms and viruses over the years for any number of reasons. Some reasons for creating malicious code have included curiosity, monetary gain, ego, thrill seeking, desire for fame, and revenge; and in a handful of cases to impress, or get revenge against, a former lover.

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

Ethical Hacking and Penetration Testing

MODULE 1

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

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

NOTE

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

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

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

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

The Role of Ethical Hacking

An ethical hacker's role is to take the skills he or she has acquired and use that knowledge, together with an understanding of the hacker mindset, to simulate a hostile attacker. It often said that to

MODULE 1

properly and completely defend oneself against an aggressor, you must understand how that aggressor thinks, acts, and reacts. The idea is similar to military training exercises in which elite units are trained in the tactics of a hostile nation in order to give other units the ability to train and understand the enemy without risking lives.

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

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

NOTE

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

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

MODULE 1

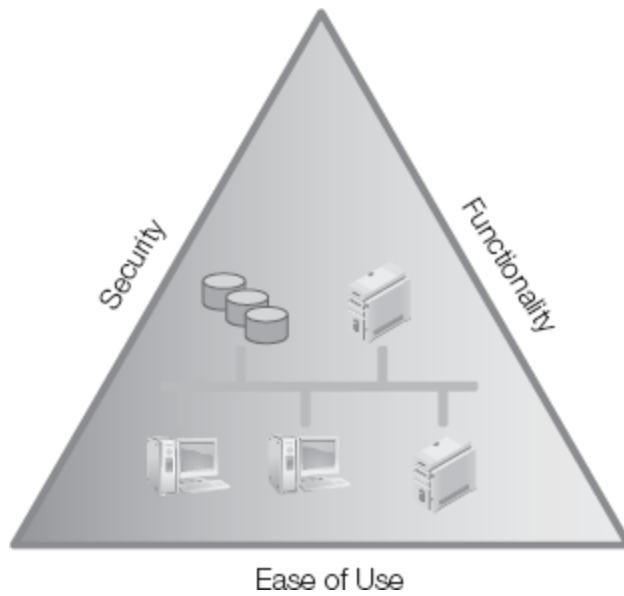


Figure 1-1. Usability versus security.

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

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

Some professionals refer to this as the A-I-C triad. Another way of looking at the balance is to observe the other side of the triad and how the balance is lost. The C-I-A triad is lost if any or all of the following occurs:

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

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

[Figure 1-2](#) shows the C-I-A triad.

MODULE 1

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

Common Hacking Methodologies

A hacking methodology refers to the step-by-step approach an aggressor uses to attack a target such as a computer network. There is no one specific step-by-step approach all hackers use. 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.

Hacking methodology generally includes the following steps ([Figure 1-3](#)):

- **Footprinting**—An attacker passively acquires information about the intended victim's systems. In this context, passive information gathering means that no active interaction occurs between the attacker and the victim (for example, conducting a whois query.)



MODULE 1

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

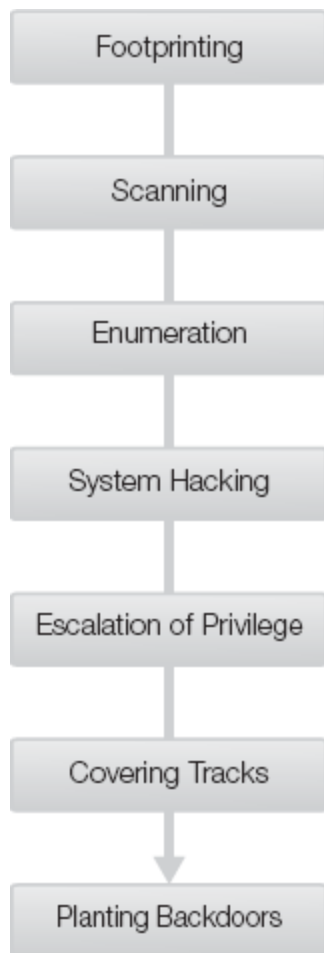


Figure 1-3. Hacking steps.

- **Scanning**—An attacker takes the information obtained during the footprinting phase and uses it to actively acquire more detailed information about a victim. For example, an attacker might conduct a ping sweep of all the victim's known IP addresses to see which machines respond.
- **Enumeration**—An attacker extracts more-detailed and useful information from a victim's system. Results of this step can include a list of usernames, groups, applications, banner settings, auditing information, and other similar information.
- **System hacking**—An attacker actively attacks a system using a method the attacker deems useful.
- **Escalation of privilege**—If this step is successful, an attacker obtains privileges on a given system higher than should be permissible. Under the right conditions, an attacker can use privilege escalation to move from a low-level account such as a guest account all the way up to administrator or system-level access.
- **Covering tracks**—In most cases, an attacker tries to avoid detection, and so will cover his or her tracks by purging information from the system to destroy evidence of a crime.

MODULE 1

- **Planting backdoors**—Depending on goals, an attacker may leave behind a backdoor on the system for later use. Backdoors can be used to regain access, as well as allow any number of different scenarios to take place, such as privilege escalations or remotely controlling a system.

Performing a Penetration Test

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

National Institute of Standards and Technology Publication 800-42 (NIST 800-42), *Guideline on Network Security Testing*, describes penetration testing as a four-step process, as shown in [Figure 1-4](#).

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

These questions include the following:

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

MODULE 1

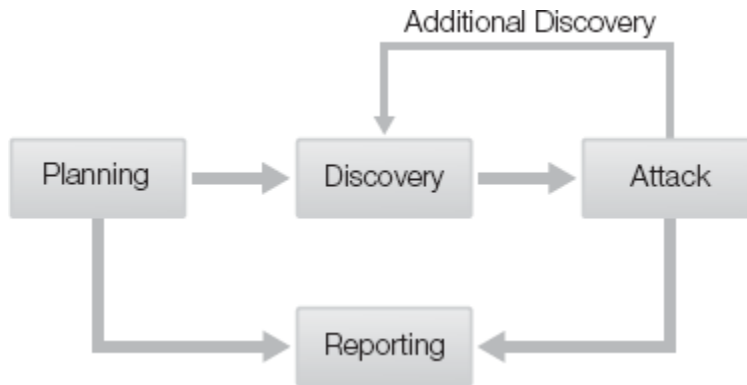


Figure 1-4. Ethical hacking steps.

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

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

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

- **Insider attack**—This is designed to simulate the actions that a disgruntled employee or other individuals who have authorized access to a system may undertake.
- **Outsider attack**—This is designed to closely match an outside aggressor's attack against an organization.
- **Stolen equipment attack**—This is designed to attack an organization's physical security. Actions of this type include breaking into server rooms, bypassing locks, and other similar activities.
- **Social engineering attack**—In this type of attack, the target is the human being, not the technology itself. If skillfully done, the attacker can obtain information or access that the attacker would not otherwise have. The attack exploits the inherent trust and habit in human nature.

Once the organization and the ethical hacker have discussed each test, determined its suitability, and evaluated its potential advantages and side effects, they can finalize the planning and contracts and perform the testing ([Figure 1-5](#)).

When performing a penetration test, the team should generally include members with different but complementary skills. When the rules of the test have been determined, the team is selected based on the intended tests it will perform and goals it will address. Expect a team to include diverse skill sets, including detailed knowledge of routers and routing protocols. Additional skills that prove useful are those that deal with the operation and configuration of firewalls and the operation of IDS and IPS systems. Team members should also share some skills, such as knowledge of networking, Transmission Control Protocol/Internet Protocol (TCP/IP), and similar technologies.

MODULE 1

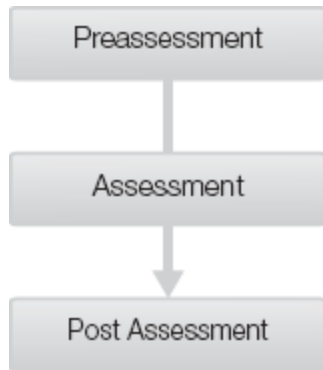


Figure 1-5. Ethical hacking test steps.

FYI

When employees are not provided information about a pending or an in-progress test, they are more likely to respond as if a real attack were occurring. This is an excellent way to check if training results in changed behavior. For example, if employees do not challenge strangers conducting a penetration test, they are unlikely to challenge a real intruder.

Another important aspect of the test is whether will have any knowledge that the test is being performed. In some cases, having employees unaware of the test will yield valuable insight into how they respond to incident(s). This allows for evaluation of current training.

Frameworks for the penetration test may include NIST 800-42 and 800-53, The Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE), or the Open Source Security Testing Methodology Manual (OSSTMM). The OSSTMM is very popular because it is an open source, peer-reviewed methodology for performing security tests and metrics.

NOTE

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

The Role of the Law and Ethical Standards

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

MODULE 1

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

- **Trust**—The client is placing trust in the ethical hacker to use the proper discretion when performing a test. If an ethical hacker breaks this trust, it can lead to the questioning of other details, such as the results of the test.
- **Legal implications**—Breaking a limit placed upon a test may be sufficient cause for a client to take legal action against the ethical hacker.

The following is a summary of laws, regulations, and directives that an ethical hacker 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 of 2000) addresses the issues of personal health care information privacy and health-plan portability in the United States.
- 1996 U.S. National Information Infrastructure Protection Act—enacted in October of 1996 as part of Public Law 104-294—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) is a corporate governance law that affects public corporations' financial reporting. Under SOX, corporations must certify the accuracy and integrity of their financial reporting and accounting.
- 2002 Federal Information Security Management Act (FISMA) requires every U.S. federal agency to create and implement an information security program to protect the information and information systems that agency uses. This act also requires agencies to conduct annual reviews of their information security program and submit results to the Office of Management and Budget (OMB).

MODULE 1**CHAPTER SUMMARY**

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

Conversely, regular hackers may not follow the same ethics and limitations of ethical hackers. Regular hackers may work without ethical limitations, and the results they can achieve are restricted only by the means, motives, and opportunities that are made available.

Finally, hacking that is not performed under contract is considered illegal and is treated as such. By its very nature, hacking activities can easily cross state and national borders into multiple legal jurisdictions.

KEY CONCEPTS AND TERMS

- Asset
- Authentication
- Black-box testing
- Cracker
- Denial of service (DoS)
- Distributed denial of service (DDoS)
- Dumpster diving
- Ethical hacker
- Exploit
- Hacker
- Intrusion detection system (IDS)
- Intrusion prevention system (IPS)
- Logic bomb
- Trojan horse
- Vulnerability
- White-box testing

CHAPTER 1 ASSESSMENT

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

MODULE 1

2. RFC 1087
3. OSSTMM
4. TCSEC
2. It is most important to obtain _____ before beginning a penetration test.
3. A security exposure in an operating system or application software component is called a _____.
4. The second step of the hacking process is _____.
5. When hackers talk about standards of behavior and moral issues of right and wrong, what are they referring to?
 1. Rules
 2. Standards
 3. Laws
 4. Ethics
6. Hackers may justify their actions based on which of the following:
 1. All information should be free
 2. Access to computers and their data should be unlimited
 3. Writing viruses, malware, or other code is not a crime
 4. Any of the above
7. This individual responsible for releasing what is considered to be the first Internet worm was:
 1. Kevin Mitnick
 2. Robert Morris, Jr.
 3. Adrian Lamo
 4. Kevin Poulsen
8. A hacker with computing skills and expertise to launch harmful attacks on computer networks and uses those skills illegally is best described as a(n):
 1. Disgruntled employee
 2. Ethical hacker
 3. White hat hacker
 4. Black hat hacker
9. If a penetration test team does not have anything more than a list of IP addresses of the organization's network, what type of test are the penetration testers conducting?
 1. Blind assessment
 2. White box
 3. Gray box
 4. Black box
10. How is the practice of tricking employees into revealing sensitive data about their computer system or infrastructure best described?
 1. Ethical hacking
 2. Dictionary attack
 3. Trojan horse
 4. Social engineering

Chapter 2

Chapter 2. Physical Security

WHEN DISCUSSING SECURITY it is easy to get caught up and immersed in the technology and the attacks associated with it. Take care not to forget areas such as physical security, however. The assets the security professional is charged with protecting are not just sitting "in a field" someplace. Each has facilities and other items surrounding it. Hackers know this fact, so they focus not only on trying to break and subvert technology. They also spend significant time looking for weaknesses in the facilities and the physical assets that make structures such as the network possible. If a hacker can gain physical access to a facility, it is more than possible for that attacker to inflict damage to the organization by accessing assets that are not properly protected. Some security experts say that if attackers can achieve physical access to a system it is under their control, and the battle is lost. Good physical security must be well thought out and considered. You must carefully consider devices such as computers, servers, notebooks, cell phones, BlackBerrys, and removable media and put in place countermeasures to protect them.

A basic example: Companies should position computer screens so that passersby cannot see sensitive data. They should also create a policy requiring users to secure their systems when they leave their computer for any reason.

Chapter 4 Topics

This chapter covers the following topics and concepts:

- What basic equipment controls are
- What physical area controls are
- What facility controls consist of
- What personal safety controls are and how they work
- What physical access controls are and how they work
- How to avoid common threats to physical security
- What defense in depth is

Chapter 4 Goals

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

- Define the role of physical security
- Describe common physical controls
- List the purpose of fences
- Describe how bollards are used
- List advantages and disadvantages of guard dogs
- Explain basic types of locks
- Identify how lock picking works
- List the usage of closed-circuit TV (CCTV)
- Describe the concept of defense in depth
- Define physical intrusion detection

Chapter 2

- List ways to secure the physical environment
- Detail building design best practices
- Describe alarm systems

Basic Equipment Controls

Basic equipment controls are defensive measures placed on the front lines of security. These controls can be both an effective first line of defense as well as a visible deterrent to an attacker. Equipment controls represent one layer of defensive measures and as such coexist with technological and administrative controls.

Keep in mind that there are many different types of controls that regulate access to equipment, each of which is used to prevent unauthorized access in some way. Some basic equipment controls covered in this section include the following:

- Passwords
- Password screen savers and session controls
- Hard drive and mobile device encryption
- Fax machines and public branch exchanges (PBX)

Hard Drive and Mobile Device Encryption

When discussing basic equipment controls another important area you should consider is the security of portable devices and hard drives. In today's world there is an ever-increasing number of portable devices such as hard drives as well as laptops, tablet PCs, and similar types of systems. Mobile devices have made working remotely easier, but at the same time the devices have introduced problems with the inevitable loss or theft of the device and the data it carries. Hard drives with sensitive data represent a real risk for the organization if they are lost, stolen, or misplaced. Consider a report from <http://www.searchsecurity.com> that cited a 2009 case in which Health Net Inc. reported the loss of patient data as the result of a data security breach that led to the loss of data affecting 1.5 million customers. In this case, the breach took place when an external hard drive that contained a mixture of medical data, Social Security numbers, and other personally identifiable information was lost.

FYI

Health Net Inc. is not the only company to report the loss of data as a result of stolen drives or systems. In 2006, the Department of Veterans Affairs (VA) lost the data of 26.5 million patients as the result of a lost laptop. While there was no evidence that the information had been accessed, the incident did result in a \$20 million settlement. In 2008, the Registered Traveler program in the United States was briefly blocked from taking new applicants after a laptop containing the personal information of 33,000 people was lost. The laptop did resurface a week later and did not appear tampered with, but the incident triggered a review of how devices were handled within the program.

Chapter 2

The solution to such problems is the application of encryption. Encryption can be applied on the file, folder, or an entire hard disk and provide a strong level of protection. Applying encryption to an entire disk is known as full disk encryption or full volume encryption. Full drive encryption, which is a technique that can be implemented in hardware or software, encrypts all the data on a selected volume or disk as selected by the owners of the system. With the widespread availability of full disk encryption, a security professional should evaluate the viability of drive encryption for mobile devices as a solution to theft, loss, and the unauthorized access to data. Software programs such as Pretty Good Privacy (PGP), TrueCrypt, and BitLocker can be used to lock files and folders. Microsoft offers data encryption programs such as BitLocker and Encrypted File System (EFS) as part of the operating system in Windows Vista and Windows 2000.

DRIVE ENCRYPTION: YES OR NO?

Drive encryption offers tremendous benefits and should be considered whenever mobile devices are in use. However, it is important to remember that drive encryption isn't always the best solution or even useful in every case. As the old saying goes, "You don't get something for nothing" because the cost of using the technology is a bit of processor power. While mobile systems are ideal candidates for full drive encryption, fixed systems that are already in secure areas may not be good candidates for full drive encryption.

BE AFRAID OF THUMB DRIVES

Are you curious about how an attacker can so easily steal data or walk out with sensitive information? It can take nothing more than a thumb drive to do so. If the attacker has malware such as a keylogger, password ripper, or data stealing program loaded on the thumb drive, it could be that just inserting it into a computer could launch a devastating attack. This technique is commonly used during security assessment.

Learn more about this technique at <http://www.securityfocus.com/news/11397>.

While discussing mobile devices, don't forget the multitude of mobile storage options. Companies used to be concerned about individuals carrying off sensitive information on floppies. In today's world, however, things have changed due largely to the availability and storage capacities available on new devices. Today, companies have to seriously consider the problems posed by mobile storage. Observe the situation in most workplaces; it is easy to see a sea of iPods, universal serial bus (USB) thumb drives, portable hard drives, cell phones with cameras, and even CD/DVD blanks and burners. Each of these devices has the potential to move massive amounts of information out of an organization quickly and quietly. Think for a moment about today's most common mobile storage device: the USB flash drive. These devices can carry upwards of 64GB of data in a package that is smaller than a pack of gum. Also consider the fact that USB flash drives are common in an ever-increasing number of forms, from watches to Swiss army knives to pens, making them more difficult to detect. A December 2009 report from <http://www.military.com> describes a recent hacking attack that occurred when a South Korean officer failed to remove a USB thumb drive when the system switched from a restricted-access intranet to the Internet. Attackers were able to access top secret information.

Chapter 2

The examples cited here, as well as countless others, illustrate that even an item as seemingly harmless as a thumb drive can become dangerous when connected to a system that is part of a network. Under the right conditions, a thumb drive can be loaded with malicious code and inserted into a computer. Because many systems have features such as auto run enabled, the applications run automatically. Just the sheer number of these portable devices (and their small size) raises the concern of network administrators and security professionals alike. As a security professional, one of your bigger challenges is dealing with devices such as thumb drives. While the devices are a definite security risk, they are universally recognized as convenient. The security professional will be required to discuss the security versus convenience issue with management to enlighten all involved of risks inherent in the system and any possible countermeasure. Whatever the decision might be in an organization, there is a need to establish some policies to enforce management's decision. This policy should address all types of media controls, how they are used, and what devices such media can be connected to.

Organizations should consider the implementation, or appropriate media controls, that dictate how floppy disks, CDs, DVDs, hard drives, portable storage, paper documents, and other forms of media are handled. Controls should dictate how sensitive media will be controlled, handled, and destroyed in an approved manner. Most important, the organization will need to make a decision about what employees can bring into the company and install on a computer. Included in this discussion will be portable drives, CD burners, cameras, and other devices. Management also needs to dictate how each of these approved forms of storage can be handled. Finally, a decision on how media is to be disposed of must be determined.

Media can be disposed of in many acceptable ways, each depending on the type of data it was used to store and the type of media it happens to be. Paper documents can be shredded, CDs can be destroyed, and magnetic media can be degaussed. Hard drives should be sanitized. (Sanitization is the process of clearing all identified content so no data remnants can be recovered.) When sanitization is performed, none of the original information is easily recovered. Some of the methods used for sanitization are as follows:

- **Drive wiping**—Overwriting all information on the drive. As an example, DoD.5200.28-STD (7) specifies overwriting the drive with a special digital pattern through seven passes. Drive wiping allows the drive to be reused.
- **Zeroization**—A process usually associated with cryptographic processes. The term was originally used with mechanical cryptographic devices. These devices would be reset to 0 to prevent anyone from recovering the key. In the electronic realm, zeroization involves overwriting the data with zeros. Zeroization is defined as a standard in ANSI X9.17.

NOTE

In certain situations organizations have taken the step of melting down hard drives instead of wiping them. The perception here is that this process makes it impossible to recover the contents of the drive; however, when done correctly, wiping a drive is extremely effective at preventing recovery of data.

Chapter 2

- **Degaussing**—Permanently destroys the contents of the hard drive or magnetic media. Degaussing works by means of a powerful magnet that uses its field strength to penetrate the media and reverse the polarity of the magnetic particles on the tape or hard disk platters. After media has been degaussed, it cannot be reused. The only method more secure than degaussing is physical destruction.

Fax Machines and Public Branch Exchanges

While fax machines are nowhere near as popular as they were in the 1990s, they still remain an area of concern for the security professional. Digital fax machines have been in use since the 1970s and continue to be used. When fax machines were originally designed, it was not with security in mind, so information in faxes is transmitted completely unprotected. Fax transmissions can potentially be intercepted, sniffed, and decoded by the clever and astute attacker. Additionally, once at the destination, faxes typically sit in a tray waiting for the owner to retrieve them, which sometimes takes a long time. Faxes are vulnerable at this point because anyone can retrieve the fax and review its contents. Another issue is that cheap fax machines use ribbons; therefore, anyone with access to the trash can retrieve the ribbon and use it as a virtual carbon copy of the original document.

NOTE

An attacker picking up a fax meant for another individual from a tray can easily go unnoticed. Consider that the recipient of a fax often tells someone to resend instead of asking any questions about where the original fax may have gone.

NOTE

While PBX systems are typically reserved for large companies and not just anyone can get access, it is not difficult to gain information. A quick Google search for a specific PBX system will, after some investigation, yield information on how to configure and administer a PBX system. With this information in hand, an attacker can hack into a PBX system and perform all sorts of actions that may go unnoticed.

When performing a security assessment for an organization it is important to take note of any fax machines present, what they are used for, and any policies that dictate the use of such devices. Worth noting is the fact that most organizations that have fax numbers may not have a physical fax, having replaced the devices with fax servers instead, which are not as obvious to spot. These devices can send faxes as well as receive faxes and route them to a user's e-mail. While it may be argued that this is better than a fax machine, it is not enough to secure the transmission of confidential information by fax. As an additional and more robust level of security, activity logs and exception reports should be collected to monitor for potential security problems.

In today's world, more companies are reliant on a technology known as private branch exchange (PBX) for intraoffice phone communication. These devices make attractive targets for an attacker, and if misconfigured have the capability to be hacked; under the right conditions, it is possible that

Chapter 2

an attacker can make anonymous and free phone calls. To secure this portion of the communication infrastructure, default passwords need to be changed, and remote maintenance must be restricted. These systems are not usually run by security professionals and may not be as secure as the network infrastructure. Individuals that target such devices are known as phreakers.

Voice over IP (VoIP)

A rapidly growing technology, Voice over IP (VoIP) is more than likely something you will have to address in your security planning. VoIP allows the placing of telephone calls over computer networks and the Internet. VoIP has the ability to transmit voice signals as data packets over the network in real-time and provide the same level of service as you would expect with traditional phone service.

Because voice is transmitted over the network as data packets much like any other data, it is susceptible to most of the attacks that affect regular data transmission. Attacks such as packet sniffing and capture can easily capture phone calls transmitted over the network; in fact, due to the sheer volume of calls that may be placed at any one time, a single attack can intercept and affect numerous calls.

Physical Area Controls

When looking at the overall security stance of an organization, you have numerous controls to use, each for a different reason. In the physical world, the first controls that someone wishing to cause harm is likely to encounter are those that line the perimeter of an organization. This perimeter is much like the moat or walls around a castle, designed to provide both a deterrent and a formidable obstacle in the event of an attack. When assessing an organization, pay attention to those structures and controls that extend in and around an organization's assets or facilities. Every control or structure observed should provide protection either to delay or deter an attack, with the ultimate goal of stopping unauthorized access. While it is possible that, in some cases, a determined attacker will make every effort to bypass the countermeasures in the first layer, additional layers working with and supporting the perimeter defenses should provide valuable detection and deterrent functions. During the construction of new facilities, the security professional should get involved early to give advice on what measures can be implemented. It is more than likely, however, that the security professional will arrive on scene long after construction of facilities has been completed. In these cases, a thorough site survey should be conducted with the goal of assessing the current protection offered. If tasked with performing a site survey, do not overlook the fact that natural geographic features can and do provide protection as well as the potential to hide individuals with malicious intent from detection. When surveying an existing facility, consider items such as natural boundaries at the location and fences or walls around the site. Common physical area controls placed at the perimeter of the facility can include many types of physical barriers that will physically and psychologically deter:

- Fences
- Perimeter intrusion detection systems (PIDS)
- Gates

Chapter 2

- Bollards
- Warning signs and notices
- Trees and foliage

Fences

Fences are one of the physical boundaries that provide the most visible and imposing deterrent. Depending on the construction, placement, and type of fence in place, it may deter only the casual intruder or a more determined individual. As fences change in construction, height, and even color, they also can provide a psychological deterrent. For example, consider an eight-foot iron fence with thick bars painted flat black; such a barrier can definitely represent a psychological deterrent. Ideally, a fence should put limit an intruder's access to a facility as well as provide a psychological barrier.

WALLS IN HISTORY

Almost everyone has heard about the Great Wall of China, built to keep out the Mongols. Two other examples from history of walls that served as effective barriers are the Berlin Wall and Hadrian's Wall. The Berlin Wall was put in place to stop the exodus of people from East Germany to the West. Until it was torn down in 1989, the physical and psychological deterrent of this barrier was obvious to anyone who looked upon the structure. In its final form, the Berlin Wall was a miles-long concrete and steel barrier line that was supplemented with land mines, dogs, guards, antitank barriers, and other mechanisms designed to strike fear into people and prevent escape attempts. Of course, the Berlin Wall did not prevent the occasional escape attempt (100 to 200 people died trying to make their way into the West over the wall).

Hadrian's Wall was put in place by the Roman Emperor Hadrian to stop invaders and mark the edge of his territory. Hadrian's Wall was an impressive engineering marvel, stretching across a large swath of northern Britain, designed to keep out the "barbarians" and serve as a physical manifestation of the edge of the empire. Ultimately, as the empire decayed and fell into ruin, the wall went unmanned, but not before serving its purpose for some time.

Depending on the company or organization involved, the goal of erecting a fence may vary from stopping casual intruders to providing a formidable barrier to entry. Fences work well at preventing unauthorized individuals from gaining access to specific areas, but also force individuals that have or want access to move to specific chokepoints to enter the facility. When determining the type of fence to use, it is important to get an idea of what the organization may need to satisfy the goals of the security plan. To get a better idea, review [Table 4-1](#), which contains a sampling of fence types and the construction and design of each. Fences should be eight feet long or greater to deter determined intruders.

Table 4-1. Fence types.

Chapter 2

TYPE	SECURITY	MESH	GAUGE
A	Extreme High Security	$\frac{3}{8}$ inch	11 gauge
B	Very High Security	1 inch	9 gauge
C	High Security	1 inch	11 gauge
D	Greater Security	2 inch	6 gauge
E	Normal Fencing	2 inch	9 gauge

In situations where security is even more of a concern, and just the placement of a fence may not be enough, it is possible to layer other protective systems. For example, a perimeter intrusion and detection assessment system (PIDA) can be used. This special fencing system works as an intrusion detection system (IDS) in that it has sensors which can detect intruders. While these systems are expensive, they offer an enhanced level of protection over standard fences. In addition to cost, the downside of these systems is that it is possible that they may produce false positives due to environmental factors such as a stray deer, high winds, or other natural events.

Gates

Fences are an effective barrier, but they must work in concert with other security measures and structures. A gate is a chokepoint or a point where all traffic must enter or exit the facility. All gates are not created equal, however, and if you select the incorrect one, you won't get proper security. In fact, choosing the incorrect gate can even detract from an otherwise effective security measure. A correctly chosen gate provides an effective deterrent and a barrier that will slow down an intruder, whereas an incorrectly chosen barrier may not deter anyone but the casual intruder. UL Standard number 325 describes gate requirements. Gates are divided into the following four classifications:

- **Residential or Class 1**—These are ornamental in design and offer little protection from intrusion.
- **Commercial or Class 2**—These are of somewhat heavier construction and fall in the range of three to four feet in height.
- **Industrial or Class 3**—These are in the range of six to seven feet in height and are of heavier construction, including chain link construction.
- **Restricted Access or Class 4**—These meet or exceed a height of eight feet and are of heavier construction—iron bars or concrete and similar materials. Gates in this category can include enhanced protective measures including barbed wire.

Chapter 2

WANT TO KNOW MORE?

For more detailed information on site security consider the many resources available on this topic. One is RFC 2196_Site Security Handbook. This document provides practical guidance to administrators seeking to secure critical assets. You can read more at: <http://www.faqs.org/rfcs/rfc2196.html#ixzz0iPiLB2vn>.

FYI

Bollards may not always be as visible as a steel post or concrete barrier. In some situations the bollards are cleverly hidden using landscaping or subtle design cues. For example, some locations (for example, malls or shopping centers) will place large concrete planters with trees or some other form of plants or decorations in front of entry points vulnerable to vehicle attacks. Another example is a retailer like Target, which often uses large concrete balls painted red in front of the main doors. While most customers may think of these as decorations or a representation of the Target logo, they are actually a form of bollard. Typically, bollards are hidden to be less imposing to customers, but still serve the designated function.

Bollards

Bollards are devices that can take many forms, but the goal is the same: prevent entry into designated areas by motor vehicle traffic. To get an idea of a location where bollards would be ideal and how they function, consider an electronics superstore such as Best Buy. In this case, lots of valuable merchandise is present and someone could very easily back a truck through the front doors after hours, load up on merchandise, and drive away quickly before law enforcement arrives. In the same situation, the placement of heavy steel posts or concrete barriers would stop a motor vehicle from even reaching the doors. Many companies use bollards to prevent vehicles from going into areas in which they are not permitted. Bollards, which can be concrete or steel, block vehicular traffic or protect areas where pedestrians may be entering or leaving buildings. While fences act as a first line of defense, bollards are a close second as they can deter individuals from ramming a facility with a motor vehicle.

Bollards can come in many shapes, sizes, and types. Some are permanent, while others pop up as needed to block a speeding car from ramming a building or ram-raiding. Ram-raiding is a type of smash and grab burglary in which a heavy vehicle is driven through the windows or doors of a closed shop, usually one selling electronics or jewelry, to quickly rob it.

Facility Controls

In addition to bollards, other security controls offer protection, and each has to be evaluated to ensure that security requirements are being met. These security controls, or facility controls, come in the form of doors, windows, and any other entry points into a facility. The weakest point of a structure is generally the first to be attacked. This means doors, windows, roof access, fire escapes, delivery access, and even chimneys are targets for attackers. In fact, anyone who has watched

Chapter 2

programs such as *COPS* or other types of reality shows based on law enforcement long enough has probably seen a handful of "dumb" criminals who got stuck trying to get into a chimney. This should serve as a reminder that you need strong facility controls and that you must provide only the minimum amount of access required and restrict no authorized individuals from secure areas. Some of the ways to achieve these goals is by examining and assessing the following:

- Doors, mantraps, and turnstiles
- Walls, ceilings, and floors
- Windows
- Guards and dogs
- Construction

Doors, Mantraps, and Turnstiles

Except for the majority of exterior doors, most doors are not designed or placed with security in mind. While doors in a home environment that are not designed with security as a goal are fine, the same cannot be said for those in a business environment. Business environments should always consider solid core doors as the primary option for doors unless otherwise specified. The advantages between solid and hollow are obvious when you consider just how easily hollow core doors can be defeated. Consider that an attacker with a good pair of boots on can kick through a hollow core door quite easily. A door designed for security will be very solid and durable and have hardened hardware. While the tendency for businesses to cut costs wherever possible is a known fact, it should be discouraged when purchasing doors by selecting the type of door only after security needs have been assessed. Low-cost doors are easy to breach, kick in, smash, or compromise. A solid core door should always be used for the protection of a server room or other critical assets. Doors also need to have a fire rating assigned to them, which is another item to be considered before installing. Doors come in many configurations, including the following:

- Industrial doors
- Vehicle access doors
- Bulletproof doors
- Vault doors

NOTE

While the importance of selecting the correct door is not something to be overlooked by the security professional, also understand that proper evaluation may require the services of a specialist. Because an information security professional doesn't usually have a background in construction or carpentry, it is important to consult with a specialist who better understands the issues involved.

Is just having a well-selected door the end of the problem? Absolutely not; you must consider the frame that the door is attached to. A good door connected to a poorly designed or constructed frame can be the Achilles heel of an otherwise good security mechanism. During a security review, it is also important to examine not only the doors in place but also the hardware used to attach the

Chapter 2

door to the frame and the frame itself. Consider the fact that something as simple as installing the hinges incorrectly to a door and frame can make them easy for a potential intruder with a screwdriver to bypass. Critical areas secured with doors should be hinged to the inside. This type of design makes it much harder for a criminal to gain access. This means that hinges and strike plates must be secure. Some doors are hinged on the outside and are designed to open out. Exterior doors are a good example of this. While the hinges are protected, the open-out feature of the door provides an invaluable safeguard against people getting trapped in a building in the event of a fire or other emergency. These doors are more expensive because they are harder to install and remove. Common places to observe these types of doors are shopping malls and other public facilities, specifically the exit doors. In some cases, exit doors are even equipped with a panic bar that can help when large crowds rush the door and need to leave quickly.

Companies should also be concerned about the flow of traffic into the facility. This is the type of situation where a device known as a mantrap can prove helpful. A mantrap is a structure that replaces a normal single door with a phone booth-sized object with a door on each side. When an individual enters the mantrap there is only enough space for one person at a time, and only one door can be opened at a time. The structure's design allows individuals to be screened via a camera or code to ensure that every individual is supposed to be entering and (in some cases) exiting the area. While mantraps are designed to regulate the flow of traffic in and out of an area, they specifically stop piggybacking, which is the practice of one individual actually opening the door to let several enter.

Another type of physical control device in common usage is the **turnstile**, which is commonly used at sporting events, subways, and amusement parks. Turnstiles can be used to slow the flow of traffic into areas or even ensure that individuals are properly screened and authenticated prior to entering an area.

Walls, Ceilings, and Floors

Working in concert with doors are the walls that the doors or mantraps are embedded into. A reinforced wall can keep a determined attacker from entering an area through any point other than the defined doors. On the other hand, a poorly constructed wall may present no obstacle at all and allow an intruder to kick through. Construction of walls should take into consideration several factors in addition to security, such as the capability to slow the spread of fires. Walls should run from the slab to the roof. Consider one of the more common mistakes that can be a detriment to security: the false wall. These are walls that run from the floor up to the ceiling, but the ceiling isn't real; it's but a drop ceiling that has a good amount of space between it and the roof. An attacker needs only a table, a chair, or a friend for a foothold to push up the ceiling tile and climb over. If asked to perform a physical security assessment of a data center or other type of high value physical asset, check to see that the wall runs past the drop ceiling. Also tap on the wall gently and check to see whether it is hollow or of a solid construction.

For ceilings, the weight-bearing load and fire ratings must be considered. For dropped ceilings, the walls should extend above the ceiling, especially in sensitive areas. Any ceiling-mounted air ducts should be small enough to prevent an intruder from crawling through them. The slab of the

Chapter 2

facility needs to have the proper weight load, fire rating, and drains. When dealing with raised floors, you will want to make sure the flooring is grounded and nonconducting. In areas with raised floors, the walls should extend below the false floor.

NOTE

A common decorative feature is the glass block wall commonly seen in locations such as doctors' offices or lobbies. While such structures and designs do look attractive, they can very easily be seen through and a kick of a boot can get through most designs.

Windows

Windows serve several purposes in any building or workplace: "opening up" the office to let more light in and giving the inhabitants a look at the world outside. But what about the security aspect? While windows let people enjoy the view, security can never be overlooked. Depending on the placement and use of windows, anything from tinted to shatterproof windows may be required to ensure that security is preserved. It is also important to consider that in some situations the windows may need to be enhanced through the use of sensors or alarms. Window types include the following:

- **Standard**—The lowest level of protection. It's cheap, but easily shattered and destroyed.
- **Polycarbonate acrylic**—Much stronger than standard glass, this type of plastic offers superior protection.
- **Wire reinforced**—Adds shatterproof protection and makes it harder for an intruder to break and access.
- **Laminated**—Similar to what is used in an automobile. By adding a laminate between layers of glass, the strength of the glass is increased and shatter potential is decreased.
- **Solar film**—Provides a moderate level of security and decreases shatter potential.
- **Security film**—Used to increase the strength of the glass in case of breakage or explosion.

Guards and Dogs

For areas where proper doors, fences, gates, and other structures cannot offer the required security, other options include guards or dogs. Guards can serve several functions just by being present; guards can be very real deterrents in addition to introducing the "human element" of security—they have the ability to make decisions and think through situations. While computerized systems can provide vital security on the physical side, such systems have not reached the level where the human element can be replaced. Guards add discernment to onsite security.

Of course, as the old saying goes, "You don't get something for nothing" and guards are no exception to this old rule. Guards need to be screened before hiring, background checks and criminal background need to be performed, and, if needed, security clearances must be obtained. Interestingly enough, however, increased technology has in part driven the need for security guards. More and more businesses have closed-circuit television (CCTV), premise control

Chapter 2

equipment, intrusion detection systems, and other computerized surveillance devices. Guards can monitor such systems. They can fill dual roles, and monitor, greet, and escort visitors, too.

Guards cost money. However, if a company does not have the money for a guard, there are other options. Dogs have been used for centuries for perimeter security. Breeds such as German shepherds guard facilities and critical assets. While it is true that dogs are loyal, obedient, and steadfast, they are not perfect and might possibly bite or harm the wrong person because they do not have the level of discernment that human beings possess. Because of these factors, dogs are usually restricted to exterior premise control and should be used with caution.

Construction

Construction of a facility has as much to do with the environment in which the facility is to be located as does the security it will be responsible for maintaining. As an example, a facility built in Tulsa, Oklahoma, has much different requirements from one built in Anchorage, Alaska. One is concerned with tornadoes; the other with snowstorms. The security professional is expected in most cases to provide input on the design or construction of a new facility or the functionality of a preexisting facility that the company is considering. When this situation arises consider the following factors:

- What are the unique physical security concerns of the organization's operations?
- Do redundancy measures exist (such as backup power or coverage by multiple telecom providers)?
- Is the location particularly vulnerable to riots or terrorism?
- Are there any specific natural/environmental concerns for the specific region in which construction is being considered?
- Is the proposed construction close to military bases, train tracks, hazardous chemical production areas, or other hazards?
- Is the construction planned in high crime neighborhoods?
- How close is the proposed construction to emergency services such as the hospital, fire department, and police station?

Personal Safety Controls

The bulk of what has been discussed up to this point has focused on the protection of assets such as computers, facilities and data; however, the human factor has been overlooked. Any security plan must address the protection and security of all assets, and this absolutely includes both silicon-based assets and carbon-based ones. There is a wide assortment of technologies specifically designed to protect not only people but also the organization itself, including the following:

- Lighting
- Alarms
- CCTV

Chapter 2

Lighting

Lighting is perhaps one of the lowest-cost security controls that can be implemented by an organization. Lighting can provide a welcome addition to locations such as parking garages and building perimeters. Consider the fact that when properly placed, lighting can eliminate shadows and the spots that cameras or guards can't monitor, as well as reduce the places in which an intruder can hide. Effective lighting means the system is designed to put the light where it is needed and in the proper wattage as appropriate. Lights are designed for specific types of applications. Some of the more common types of lights include these:

- **Continuous**—Fixed lights arranged to flood an area with overlapping cones of light (most common)
- **Standby**—Randomly turned on to create an impression of activity
- **Movable**—Manually operated movable searchlights; used as needed to augment continuous or standby lighting
- **Emergency**—Can duplicate any or all of the previous lights; depends on an alternative power source

Two issues that occur with lighting are overlighting and glare. Too much light, or overly bright lights, can bleed over to the adjacent owner's property and be a source of complaints. Too much light can also lead to a false sense of security because a company may feel that because all areas are lit, intrusion is unlikely. Additionally, when lighting is chosen incorrectly, it is possible to introduce high levels of glare. Glare can make it tough for those tasked with monitoring an area to observe all the activities that may be occurring. When placing lighting, avoid any placement that directs the lighting toward the facility and instead direct the lights toward fences, gates, or other areas of concern such as access points. Also consider the problems associated with glare when guards are present; for example, if guards are tasked with checking IDs at a checkpoint into a facility, ensure that the lights are not directed toward the guards. This offers good glare protection to the security force and guards.

Alarms and Intrusion Detection

Alarms and physical intrusion detection systems can also increase physical security. Alarms typically are used to provide an alert mechanism if a potential break-in or fire has been detected. Alarms can have a combination of audible and visual indicators that allow people to see and hear the alarm and react to the alert. Alarms are of no use if no one can hear or see the alert and respond accordingly. More advanced alarm systems even include the ability to contact fire or police services if the alarm is activated after business hours, for example. Of course, a drawback is the simple fact that if an alarm system is tied to the police or fire department, false alarms could result in being assessed fines.

Additional options that can enhance physical intrusion detection are motion, audio, infrared wave pattern, and capacitance detection systems. Of these systems, infrared detection tends to be one of the most common, but like any system, these have both pros and cons. Infrared systems are expensive and they may be larger than other comparable devices, but at the same time the systems

Chapter 2

can detect activity outside the normal visual range. Another popular form of intrusion detection systems are those devices sensitive to changes in weight, and such systems may be useful when used with mantraps because they can detect changes in weight that may signal a thief.

If asked to provide guidance to an organization on what type of IDS to consider implementing, always take the situation into account. What is important to avoid is placing a too complex or inappropriate IDS for the given situation. For example, systems that detect weight changes may not be as important or may even be completely unnecessary in situations where theft is not a concern. Also keep in mind that IDSs are not foolproof and are not an excuse for avoiding using common sense or other security controls. Any guidance on what type of IDS to implement should also mention that human involvement is essential.

Closed-Circuit TV (CCTV)

Another mechanism that can be used to protect people and potentially deter crime is CCTV. CCTV usually works in conjunction with guards or other monitoring mechanisms to extend their capacity. When dealing with surveillance devices, you must understand factors such as focal length, lens types, depth of field, and illumination requirements. As an example, the requirement of a camera that will be placed outside in an area of varying light is much different from one placed inside in a fixed lighting environment. Also, there is the issue of focal length, which defines the camera's effectiveness in viewing objects from a horizontal and vertical view. Short focal lengths provide wider angle views while longer focal lengths provide more narrow views.

NOTE

Modern CCTV systems can provide additional features such as the ability to alert the monitoring agency or organization in the form of e-mail or other similar methods. These systems can be said to be smart in that they can even be configured in some instances to send these alerts only during certain hours.

When considering placement of CCTV, keep in mind areas such as perimeter entrances and critical access points. Activity can be either monitored live by a security officer, or recorded and reviewed later. If no one is monitoring the CCTV system, it effectively becomes a detective control because it will not prevent a crime. In these situations, the organization is effectively alerted to the crime only after the fact, when the recordings are reviewed.

Physical Access Controls

A physical access control can be defined as any mechanism by which an individual can be granted or denied physical access. One of the oldest forms of access control is the mechanical lock. Other types of physical access control include ID badges, tokens, and biometrics.

Locks

Chapter 2

Locks, which come in many types, sizes, and shapes, are an effective means of physical access control. Locks are by far the most widely implemented security control due largely to the wide range of options available as well as the low costs of the devices.

Lock types include the following:

- **Mechanical**—Warded and pin and tumbler
- **Cipher**—Smart and programmable

Warded locks are the simplest form of mechanical lock. The design of mechanical locks uses a series of wards that a key must match up to in order to open the lock. While it is the cheapest type of mechanical lock it is also the easiest to pick. Pin and tumbler locks are considered more advanced. These locks contain more parts and are harder to pick than warded locks. When the correct key is inserted into the cylinder of a pin and tumbler lock, the pins are lifted to the right height so that the device can open or close. More advanced and technically complex than warded or pin and tumbler locks are cipher locks, which have a keypad of fixed or random numbers that requires a specific combination to open the lock.

Before selecting a lock, consider the fact that not all locks are alike, and locks come in different grades. The grade of the lock specifies its level of construction. The three basic grades of locks are as follows:

- **Grade 1**—Commercial locks with the highest security
- **Grade 2**—Light-duty commercial locks or heavy-duty residential locks
- **Grade 3**—Consumer locks with the weakest design

NOTE

Although a Grade 3 lock is fine for use in residential applications, it is not acceptable for a critical business asset. Always check the grade of a lock before using it to protect the assets of a company.

Lock Picking

While locks are good physical deterrents and work quite well as a delaying mechanism, a lock can be bypassed through lock picking. Criminals tend to pick locks because it is a stealthy way to bypass a lock and can make it harder for the victim to determine what has happened.

The basic components used to pick locks are these:

- **Tension wrenches**—Like small, angled flathead screwdrivers. They come in various thicknesses and sizes.
- **Picks**—Just as the name implies, similar to dentist picks: small, angled, and pointed.

NOTE

Chapter 2

Before purchasing a lock picking set, be sure to investigate local laws on the matter. In some states, the mere possession of a lock picking set can be a felony. In other states, possession of a lock picking set is not a crime in and of itself, but using the tools during the commission of a crime is.

Together, these tools can be used to pick a lock. One example of a basic technique used to pick a lock is scraping. With this technique, tension is held on the lock with the tension wrench while the pins are scraped quickly. Pins are then placed in a mechanical bind and will be stuck in the unlocked position. With practice, this can be done quickly so that all the pins stick and the lock is disengaged.

Tokens and Biometrics

Tokens and biometrics are two ways to control individuals as they move throughout a facility or attempt to access specific areas. Tokens are available in many types and can range from basic ID cards to more intelligent forms of authentication systems. Tokens used for authentication can make an access decision electronically and come in several different configurations, including the following:

- **Active electronic**—The access card has the ability to transmit electronic data.
- **Electronic circuit**—The access card has an electronic circuit embedded.
- **Magnetic stripe**—The access card has a stripe of magnetic material.
- **Magnetic strip**—The access card contains rows of copper strips.
- **Contactless cards**—The access card communicates with the card reader electronically.

Contactless cards do not require the card to be inserted or slid through a reader. These devices function by detecting the proximity of the card to the sensor. An example of this technology is radio frequency ID (RFID). RFID is an extremely small electronic device that is composed of a microchip and antenna. Many RFID devices are passive devices. Passive devices have no battery or power source because they are powered by the RFID reader. The reader generates an electromagnetic signal that induces a current in the RFID tag.

Another form of authentication is **biometrics**. Biometric authentication is based on a behavioral or physiological characteristic that is unique to an individual. Biometric authentication systems have gained market share because they are seen as a good replacement for password-based authentication systems. Different biometric systems have various levels of accuracy. The accuracy of a biometric device is measured by the percentage of Type 1 and Type 2 errors it produces. Type 1 errors or false rejections are reflected by what is known as the **false rejection rate (FRR)**. This is a measurement of the percentage of individuals who should have been granted, but were not allowed access. A Type 2 error or false acceptance is reflected by the **false acceptance rate (FAR)** which is a measurement of the percentage of individuals who have gained access but should not have been granted such.

Some common biometric systems include the following:

- **Finger scan systems**—Widely used, popular, installed in many new laptops

Chapter 2

- **Hand geometry systems**—Accepted by most users; functions by measuring the unique geometry of a user's fingers and hand to identify them
- **Palm scan systems**—Much like the hand geometry system, except it measures the creases and ridges of a user for identification
- **Retina pattern systems**—Very accurate; examines the user's retina pattern
- **Iris recognition**—Another eye recognition system that is also very accurate; it matches the person's blood vessels on the back of the eye
- **Voice recognition**—Determines who you are by using voice analysis
- **Keyboard dynamics**—Analyzes the user's speed and pattern of typing

No matter what means of authentication you use, a physical access control needs to fit the situation in which will be applied. As an example, if the processing time of a biometric system is slow, users tend to just hold the door open for others rather than wait for the additional processing time. Another example is an iris scanner, which may be installed at all employee entrances, yet later causes complaints from employees who are physically challenged or in wheelchairs because they cannot easily use the newly installed system. Consider who will be using the system and if it may be appropriate given the situation and user base.

Avoiding Common Threats to Physical Security

With so much talk in this chapter of controls and items to look for during an assessment, it is important to be aware of some of the threats an organization can face. Some common threats include these:

- Natural/human/technical threats
- Physical keyloggers
- Sniffers
- Wireless interception
- Rogue access points

Natural, Human, and Technical Threats

Every organization must deal with the threats that are present in the environment each day. Threats can be natural, human, or technical. Natural threats can include items such as fires, floods, hurricanes, tropical storms, tidal waves, and earthquakes.

Human threats are not always as predictable as natural threats. For example, anyone living in California knows that earthquakes will hit, but they just can't say when. However, an organization may expect someone to attempt or even succeed in breaking in to the company, but the attempt may never come. The point here is that aside from natural disasters, you must think of other threats such as hackers who do not issue notices when an attack is coming. Any organization can be threatened by outsiders or insiders: people that are apparently trusted or unknown individuals.

Human threats can include the following:

Chapter 2

- **Theft**—Theft of company assets can range from mildly annoying to extremely damaging. A CEO's laptop may be stolen from the hotel lobby; but is the real loss the laptop or the plans for next year's new software release?
- **Vandalism**—From broken windows caused by a teenager just having some malicious fun to the hacker who decides to change your company's Web page, each is destroying company property.
- **Destruction**—This threat can come from insiders or outsiders. Destruction of physical assets can cost organizations money that was destined to be spent on other items.
- **Terrorism**—This form of threat is posed by individuals or groups that wish to prove a point or draw attention to a cause
- **Accidental**—Accidents are bound to happen sooner or later and their effects can be varied depending on the situation. Damage could range from lost data or an attacker obtaining access where they should not have.

Any company can also be at risk due to technical issues. A truck driver can knock down a power pole in front of the company, or a hard drive in a server might fail. Each can and will affect the capability of the company to continue to provide needed services. Whenever a security professional is asked to perform a physical review, don't neglect physical controls that are needed to protect against these or any of the various types of issues that are present. Any equipment failure and loss of service can affect the physical security of the organization.

Physical Keyloggers and Sniffers

Hardware keyloggers are physical devices used to record everything a person types on the keyboard. These devices are usually installed while the user is away from the desk. Keystroke loggers can be used for legal or illegal purposes, such as the following:

- Monitoring employee productivity and computer activity
- Law enforcement
- Illegal spying

Physical keyloggers can store millions of keystrokes on a small device that is plugged in between the keyboard and the computer. Some keyloggers are built into keyboards. The process is transparent to the end user and can be detected only by finding the keylogger.

Keyloggers can be the following:

- Attached to the keyboard cable, as inline devices
- Installed inside standard keyboards
- Installed inside replacement keyboards
- Installed on a system along with other software

NOTE

Even if the IT or security department of your company is planning to use these devices for legal purposes, always consult with a lawyer or with the human resources department. Use of such devices in some instances can be a serious legal issue and expose the company to legal action.

Sniffing is the basis for a large number of network-based attacks. If attackers can gain access to the network via a physical network connection, they can begin to capture traffic. Sniffing can be passive or active. Passive sniffing relies on a feature of network cards called "promiscuous mode." When placed in promiscuous mode, a network card passes all packets on to the operating system, rather than just those unicast or broadcast to the host.

Active sniffing, on the other hand, relies on injecting packets into the network, causing traffic that should not be sent to your system to be sent to your system. Active sniffing was developed largely in response to switched networks. Sniffing is dangerous in that it allows hackers access to traffic they should not see. An example of a sniffer capture is shown in [Figure 4-1](#).

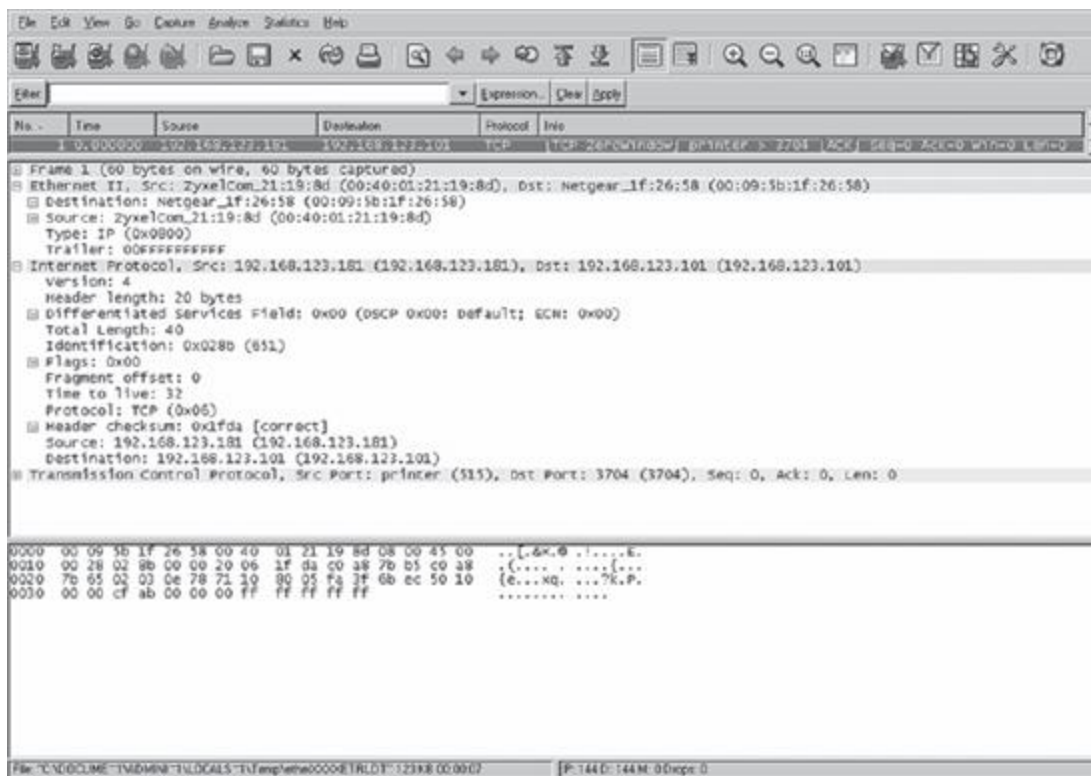


Figure 4-1. Wireshark sniffer.

Wireless Interception and Rogue Access Points

While you will read more about wireless networks and their security vulnerabilities in [Chapter 8](#), we will mention some of the basics here as a brief introduction. Sniffing is not restricted to wired networks. Wireless signals emanating from cell phones, wireless local area networks (WLANs), Bluetooth devices, and other modern equipment can also be intercepted and analyzed by an

Chapter 2

attacker with the right equipment. Even when signals cannot be intercepted, they can still potentially be jammed. For example, a cell phone jammer could transmit a signal on the same frequencies that cell phones do and then prevent all cell phone communication within a given area.

Moving on to other current technologies, the discussion now turns to another wireless technology: **Bluetooth**, which is a short-range communication technology that has been shown to be vulnerable to attack. One such attack is Bluejacking, which allows an individual to send unsolicited messages over Bluetooth to other Bluetooth devices. WLANs are also vulnerable to attacks. These attacks can be categorized into four basic categories: eavesdropping, open authentication, rogue access points, and denial of service.

Finally, the attacker may attempt to set up a fake access point to intercept wireless traffic. Such techniques make use of a rogue access point. This fake access point is used to launch a man-in-the-middle attack. Attackers simply place their own access points in the same area as users and attempt to get them to log on.

Defense in Depth

Something that has been mentioned indirectly a few times already is the concept of defense in depth. The concept of defense in depth originated from the military and was seen as a way to delay rather than prevent an attack. As an information security tactic, it is based on the concept of layering more than one control. These controls can be physical, administrative, or technical in design. We have looked at a variety of physical controls in this chapter such as locks, doors, fences, gates, and barriers. Administrative controls include policies and procedures on (among other things) how you recruit, hire, manage, and fire employees. During employment, administrative controls such as least privilege, separation of duties, and rotation of duties are a few of the items that must be enforced. When employees leave or are fired, their access needs to be revoked, accounts blocked, property returned, and passwords changed. Technical controls are another piece of defense in depth and can include items such as encryption, firewalls, and IDS.

NOTE

Another way to think of defense in depth is as avoiding putting all your eggs in one basket.

For the physical facility, a security professional should strive for a minimum of three layers of physical defense. The first line of defense is the building perimeter. Barriers placed here should delay and deter attacks. Items at this layer include fences, gates, and bollards. These defenses should not reduce visibility of CCTV and/or guards. Items such as shrubs should be 18 to 24 inches away from all entry points, and hedges should be cut six inches below the level of all windows.

The second layer of defense is the building exterior: roof, walls, floor, doors, and ceiling. Windows are a weak point here. Any opening 18 feet or less above the ground should be considered a potential easy access and should be secured if greater than 96 square inches.

Chapter 2

The third layer of physical defense is the interior controls: locks, safes, containers, cabinets, interior lighting. It can even include policies and procedures that cover what controls are placed on computers, laptops, equipment, and storage media. This third layer of defense is important when you consider items such as the data center or any servers kept onsite. A well-placed data center should not be above the second floor of a facility because a fire might make it inaccessible. Likewise, you wouldn't want the data center located in the basement because it could be subject to flooding. A well-placed data center should have limited accessibility—typically no more than two doors. Keep these items in mind because they will help you secure the facility.

CHAPTER SUMMARY

This chapter is unique in that so much of ethical hacking and penetration testing is about IT and networks. However, the reality is that attackers will target an organization any way that they can. Not all attacks will be logical in nature; many are physical. If attackers can gain physical access to a facility, many potentially damaging actions can occur: from simply unplugging a server and walking out with it to sniffing traffic on the network.

Physical controls can take many forms and be implemented for any number of reasons. Consider that physical controls such as doors, fences, and gates represent some of the first barriers that an attacker will encounter. When constructed and placed properly, fences can provide a tremendous security benefit, stopping all but the most determined attacker. Other types of controls that can be layered into the existing physical security system include alarm and intrusion detection systems, both of which provide an early warning of intrusions.

KEY CONCEPTS AND TERMS

- Biometrics
- Bluetooth
- Bollard
- False acceptance rate (FAR)
- False rejection rate (FRR)
- Lock
- Turnstile

CHAPTER 2 ASSESSMENT

1. Physical security is less important than logical security.
 1. True
 2. False
2. _____ is a common physical control that can be used as both a detective and reactive tool.
 1. A fence
 2. An alarm
 3. CCTV

Chapter 2

4. A lock
3. For a fence to deter a determined intruder, it should be at least _____ feet tall.
 1. Four
 2. Five
 3. Six
 4. Ten
4. A(n) _____ is used to prevent cars from ramming a building.
5. While guards and dogs are both good for physical security, which of the following more commonly applies to dogs?
 1. Liability
 2. Discernment
 3. Dual role
 4. Multifunction
6. What grade of lock would be appropriate to protect a critical business asset?
 1. Grade 4
 2. Grade 2
 3. Grade 1
 4. Grade 3
7. _____ defines the camera's effectiveness in viewing objects from a horizontal and vertical view.
 1. Granularity
 2. Ability to zoom
 3. Field of view
 4. Focal length
8. In the field of IT security, the concept of defense in depth is layering more than one control on another.
 1. True
 2. False
9. _____ is an intrusion detection system used exclusively in conjunction with fences
 1. Infrared wave patten
 2. Motion detector
 3. RFID
 4. PIDAS
10. A Type 2 error is also known as what?
 1. False rejection rate
 2. Failure rate
 3. Crossover error rate
 4. False acceptance rate
11. Which type of biometric system is frequently found on laptops?
 1. Retina
 2. Fingerprint
 3. Iris
 4. Voice recognition
12. What do lock pick sets typically contain at a minimum?
 1. Tension wrenches and drivers
 2. A pick

Chapter 2

3. A pick and a driver
 4. A pick and a tension wrench
13. During an assessment, you discovered that the target company was using a fax machine. Which of the following is the *least* important?
1. The phone number is publicly available.
 2. The fax machine is in an open, unsecured area.
 3. Faxes frequently sit in the printer tray.
 4. The fax machine uses a ribbon.