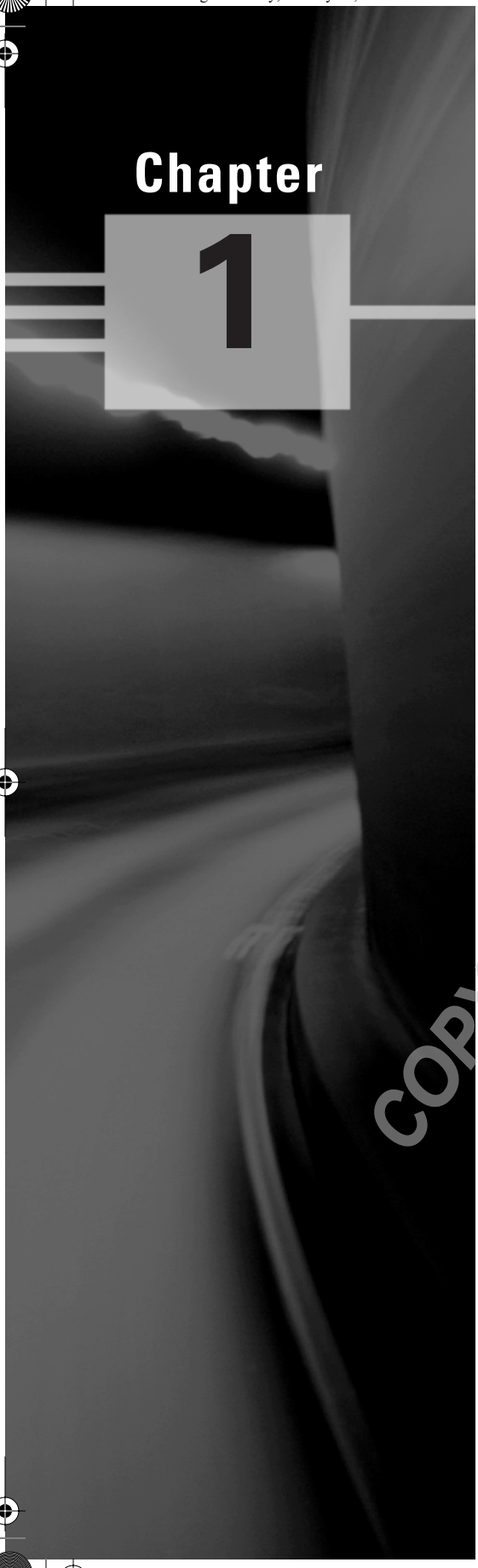
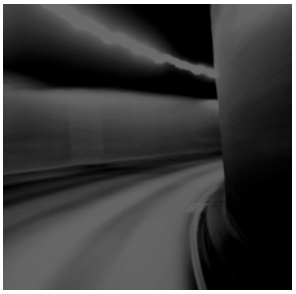


Chapter 1

Introduction to Ethical Hacking, Ethics, and Legality

CEH EXAM OBJECTIVES COVERED IN THIS CHAPTER:

- ✓ Understanding Ethical Hacking Terminology
- ✓ Identifying Different Types of Hacking Technologies
- ✓ Understanding the Different Phases Involved in Ethical Hacking and Listing the Five Stages of Ethical Hacking
- ✓ What Is Hacktivism?
- ✓ Listing Different Types of Hacker Classes
- ✓ Defining the Skills Required to Become an Ethical Hacker
- ✓ What Is Vulnerability Research?
- ✓ Describing the Ways to Conduct Ethical Hacking
- ✓ Understanding the Legal Implications of Hacking
- ✓ Understanding 18 U.S.C. § 1029 and 1030 U.S. Federal Law



Most people think hackers have extraordinary skill and knowledge that allow them to hack into computer systems and find valuable information. The term *hacker* conjures up images of a young computer whiz who types a few commands at a computer screen—and poof! The computer spits back account numbers or other confidential data. In reality, a good hacker just has to understand how a computer system works and know what tools to employ in order to find a security weakness.

The realm of hackers and how they operate is unknown to most computer and security professionals. The goal of this chapter is to introduce you to the world of the hacker and to define the terms that will be tested on the Certified Ethical Hacker (CEH) exam.

Understanding Ethical Hacking Terminology

Being able to understand and define terminology is an important part of a CEH's responsibility. In this section, we'll discuss a number of terms you need to be familiar with.

A *threat* is an environment or situation that could lead to a potential breach of security. Ethical hackers look for and prioritize threats when performing a security analysis.

In computer security, an *exploit* is a piece of software that takes advantage of a bug, glitch, or vulnerability, leading to unauthorized access, privilege escalation, or denial of service on a computer system.

There are two methods of classifying exploits:

A *remote exploit* works over a network and exploits security vulnerabilities without any prior access to the vulnerable system.

A *local exploit* requires prior access to the vulnerable system to increase privileges.

An exploit is a defined way to breach the security of an IT system through a vulnerability.

A *vulnerability* is an existence of a software flaw, logic design, or implementation error that can lead to an unexpected and undesirable event executing bad or damaging instructions to the system.

A *target of evaluation* is a system, program, or network that is the subject of a security analysis or attack.

An *attack* occurs when a system is compromised based on a vulnerability. Many attacks are perpetuated via an exploit. Ethical hackers use tools to find systems that may be vulnerable to an exploit because of the operating system, network configuration, or applications installed on the systems, and prevent an attack. This book provides you the toolset necessary to become an ethical hacker.

In addition to knowing these terms, it's also important to identify the differences between an ethical hacker and a malicious hacker, and to understand what ethical hackers do.

Identifying Different Types of Hacking Technologies

Many methods and tools exist for locating vulnerabilities, running exploits, and compromising systems. Trojans, backdoors, sniffers, rootkits, exploits, buffer overflows, and SQL injection are all technologies that can be used to hack a system or network. These technologies and attack methods will each be discussed in later chapters. Many are so complex that an entire chapter is devoted to explaining the attack and applicable technologies.

Most hacking tools exploit weaknesses in one of the following four areas:

Operating systems Many systems administrators install operating systems with the default settings, resulting in potential vulnerabilities that remain unpatched.

Applications Applications usually aren't tested for vulnerabilities when developers are writing the code, which can leave many programming flaws that a hacker can exploit.

Shrink-wrap code Many off-the-shelf programs come with extra features the common user isn't aware of, which can be used to exploit the system. One example is macros in Microsoft Word, which can allow a hacker to execute programs from within the application.

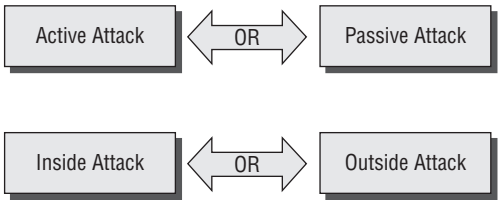
Misconfigurations Systems can also be misconfigured or left at the lowest common security settings to increase ease of use for the user, which may result in vulnerability and an attack.

This book will cover all these technologies and hacking tools in depth in later chapters. It's necessary to understand the types of attacks and basics of security before you learn all the technologies associated with an attack.

In addition to the various types of technologies a hacker can use, there are different types of attacks. Attacks can be categorized as either *passive* or *active*. Passive and active attacks are used on both network security infrastructures and on hosts. Active attacks actually alter the system or network they're attacking, whereas passive attacks attempt to gain information from the system. Active attacks affect the availability, integrity, and authenticity of data; passive attacks are breaches of confidentiality.

In addition to the active and passive categories, attacks are categorized as either *inside* or *outside* attacks. Figure 1.1 shows the relationship between passive and active attacks, and inside and outside attacks. An attack originating from within the security perimeter of an organization is an inside attack and usually is caused by an "insider" who gains access to more resources than expected. An outside attack originates from a source outside the security perimeter, such as the Internet or a remote access connection.

FIGURE 1.1 Types of attacks

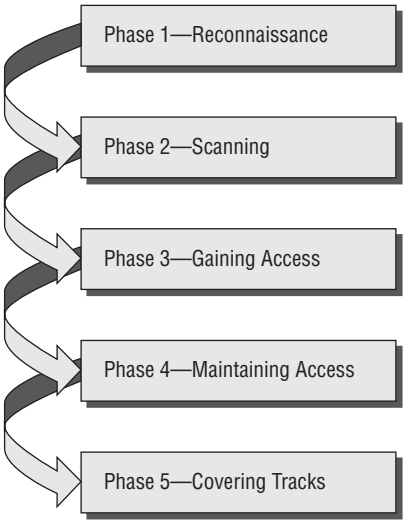


Most network security breaches originate from within an organization—usually from the company's own employees or contractors.

Understanding the Different Phases Involved in Ethical Hacking and Listing the Five Stages of Ethical Hacking

An ethical hacker follows processes similar to those of a malicious hacker. The steps to gain and maintain entry into a computer system are similar no matter what the hacker's intentions are. Figure 1.2 illustrates the five phases that hackers generally follow in hacking a system. The following sections cover these five phases.

FIGURE 1.2 Phases of hacking



Phase 1: Passive and Active Reconnaissance

Passive reconnaissance involves gathering information regarding a potential target without the targeted individual's or company's knowledge. Passive reconnaissance can be as simple as watching a building to identify what time employees enter the building and when they leave. However, it's usually done using Internet searches or by Googling an individual or company to gain information. This process is generally called *information gathering*. Social engineering and dumpster diving are also considered passive information-gathering methods.

Sniffing the network is another means of passive reconnaissance and can yield useful information such as IP address ranges, naming conventions, hidden servers or networks, and other available services on the system or network. Sniffing network traffic is similar to building monitoring: A hacker watches the flow of data to see what time certain transactions take place and where the traffic is going.

Active reconnaissance involves probing the network to discover individual hosts, IP addresses, and services on the network. This usually involves more risk of detection than passive reconnaissance and is sometimes called *rattling the doorknobs*. Active reconnaissance can give a hacker an indication of security measures in place (is the front door locked?), but the process also increases the chance of being caught or at least raising suspicion.

Both passive and active reconnaissance can lead to the discovery of useful information to use in an attack. For example, it's usually easy to find the type of web server and the operating system (OS) version number that a company is using. This information may enable a hacker to find a vulnerability in that OS version and exploit the vulnerability to gain more access.

Phase 2: Scanning

Scanning involves taking the information discovered during reconnaissance and using it to examine the network. Tools that a hacker may employ during the scanning phase can include dialers, port scanners, network mappers, sweepers, and vulnerability scanners. Hackers are seeking any information that can help them perpetrate attack such as computer names, IP addresses, and user accounts.

The methods and tools used in scanning are discussed in detail in Chapter 3, "Scanning and Enumeration."

Phase 3: Gaining Access

This is the phase where the real hacking takes place. Vulnerabilities discovered during the reconnaissance and scanning phase are now exploited to gain access. The method of connection the hacker uses for an exploit can be a local area network (LAN, either wired or wireless), local access to a PC, the Internet, or offline. Examples include stack-based buffer overflows, denial of service (DoS), and session hijacking. These topics will be discussed in later chapters. Gaining access is known in the hacker world as *owning* the system.

Phase 4: Maintaining Access

Once a hacker has gained access, they want to keep that access for future exploitation and attacks. Sometimes, hackers *harden* the system from other hackers or security personnel by securing their exclusive access with backdoors, rootkits, and Trojans. Once the hacker owns the system, they can use it as a base to launch additional attacks. In this case, the owned system is sometimes referred to as a *zombie* system.

Phase 5: Covering Tracks

Once hackers have been able to gain and maintain access, they cover their tracks to avoid detection by security personnel, to continue to use the owned system, to remove evidence of hacking, or to avoid legal action. Hackers try to remove all traces of the attack, such as log files or intrusion detection system (IDS) alarms. Examples of activities during this phase of the attack include steganography, the use of tunneling protocols, and altering log files. Steganography and use of tunneling for purposes of hacking will be discussed in later chapters.

What Is Hacktivism?

Hacktivism refers to hacking for a cause. These hackers usually have a social or political agenda. Their intent is to send a message through their hacking activity while gaining visibility for their cause and themselves.

Many of these hackers participate in activities such as defacing websites, creating viruses, DoS, or other disruptive attacks to gain notoriety for their cause. Hacktivism commonly targets government agencies, political groups, and any other entities these groups or individuals perceive as "bad" or "wrong."

Listing Different Types of Hacker Classes

Hackers can be divided into three groups: white hats, black hats, and grey hats. Ethical hackers usually fall into the white-hat category, but sometimes they're former grey hats who have become security professionals and who use their skills in an ethical manner.

White hats White Hats are the good guys, the ethical hackers who use their hacking skills for defensive purposes. White-hat hackers are usually security professionals with knowledge of hacking and the hacker toolset and who use this knowledge to locate weaknesses and implement countermeasures.

Black hats Black hats are the bad guys: the malicious hackers or *crackers* who use their skills for illegal or malicious purposes. They break into or otherwise violate the system integrity of remote machines, with malicious intent. Having gained unauthorized access, black-hat hackers destroy vital data, deny legitimate users service, and basically cause problems for their targets. Black-hat hackers and crackers can easily be differentiated from white-hat hackers because their actions are malicious.

Grey hats Grey hats are hackers who may work offensively or defensively, depending on the situation. This is the dividing line between hacker and cracker. Both are powerful forces on the Internet, and both will remain permanently. And some individuals qualify for both categories. The existence of such individuals further clouds the division between these two groups of people.

In addition to these groups, there are self-proclaimed ethical hackers, who are interested in hacker tools mostly from a curiosity standpoint. They may want to highlight security problems in a system or educate victims so they secure their systems properly. These hackers are doing their "victims" a favor. For instance, if a weakness is discovered in a service offered by an investment bank, the hacker is doing the bank a favor by giving the bank a chance to rectify the vulnerability.

From a more controversial point of view, some people consider the act of hacking itself to be unethical, like breaking and entering. But the belief that "ethical" hacking excludes destruction at least moderates the behavior of people who see themselves as "benign" hackers. According to this view, it may be one of the highest forms of hackerly courtesy to break into a system and then explain to the system operator exactly how it was done and how the hole can be plugged; the hacker is acting as an unpaid—and unsolicited—*tiger team* (a group that conducts security audits for hire). This approach has gotten many ethical hackers in legal trouble. Make sure you know the law and your legal liabilities when engaging in ethical hacking activity.

Many self-proclaimed ethical hackers are trying to break into the security field as consultants. Most companies don't look favorably on someone who appears on their doorstep with confidential data and offers to "fix" the security holes "for a price." Responses range from "thank you for this information, we'll fix the problem" to calling the police to arrest the self-proclaimed ethical hacker.

Being able to identify the types of hackers is important, but determining the differences is equally—if not more—important. We'll look at this in the following sections.

Ethical Hackers and Crackers—Who Are They?

Many people ask, "Can hacking be ethical?" Yes! Ethical hackers are usually security professionals or network penetration testers who use their hacking skills and toolsets for defensive and protective purposes. Ethical hackers who are security professionals test their network and systems security for vulnerabilities using the same tools that a hacker might use to compromise the network. Any computer professional can learn the skills of ethical hacking.

As we mentioned earlier, the term *cracker* describes a hacker who uses their hacking skills and toolset for destructive or offensive purposes such as disseminating viruses or performing DoS attacks to compromise or bring down systems and networks. No longer just looking for fun, these hackers are sometimes paid to damage corporate reputations or steal or reveal credit-card information, while slowing business processes and compromising the integrity of the organization.

Another name for a cracker is a *malicious hacker*.

What Do Ethical Hackers Do?

Ethical hackers are motivated by different reasons, but their purpose is usually the same as that of crackers: They're trying to determine what an intruder can see on a targeted network or system, and what the hacker can do with that information. This process of testing the security of a system or network is known as a *penetration test*.

Hackers break into computer systems. Contrary to widespread myth, doing this doesn't usually involve a mysterious leap of hackerly brilliance, but rather persistence and the dogged repetition of a handful of fairly well-known tricks that exploit common weaknesses in the security of target systems. Accordingly, most crackers are only mediocre hackers.

Many ethical hackers detect malicious hacker activity as part of the security team of an organization tasked with defending against malicious hacking activity. When hired, an ethical hacker asks the organization what is to be protected, from whom, and what resources the company is willing to expend in order to gain protection.

Goals Attackers Try to Achieve

Security consists of four basic elements:

- Confidentiality
- Authenticity
- Integrity
- Availability

A hacker's goal is to exploit vulnerabilities in a system or network to find a weakness in one or more of the four elements of security. In performing a DoS attack, a hacker attacks the availability elements of systems and networks. Although a DoS attack can take many forms, the main purpose is to use up system resources or bandwidth. A flood of incoming messages to the target system essentially forces it to shut down, thereby denying service to legitimate users of the system. Although the media focuses on the target of DoS attacks, in reality such attacks have many victims—the final target and the systems the intruder controls.

Information theft, such as stealing passwords or other data as it travels in cleartext across trusted networks, is a confidentiality attack, because it allows someone other than the intended recipient to gain access to the data. This theft isn't limited to data on network servers. Laptops, disks, and backup tapes are all at risk. These company-owned devices are loaded with confidential information and can give a hacker information about the security measures in place at an organization.

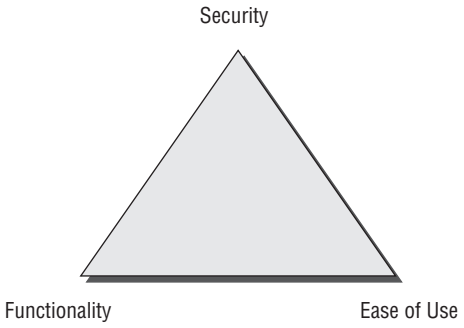
Bit-flipping attacks are considered integrity attacks because the data may have been tampered with in transit or at rest on computer systems; therefore system administrators are unable to verify the data is as it the sender intended it. A bit-flipping attack is an attack on a cryptographic cipher: The attacker changes the ciphertext in such as a way as to result in a predictable change of the plaintext, although the attacker doesn't learn the plaintext itself. This type of attack isn't directly against the cipher but against a message or series of messages. In the extreme, this can become a DoS attack against all messages on a particular channel using that cipher. The attack is especially dangerous when the attacker knows the format of the message. When a bit-flipping attack is applied to digital signatures, the attacker may be able to change a promissory note stating "I owe you $10.00" into one stating "I owe you $10,000."

MAC address spoofing is an authentication attacks because it allows an unauthorized device to connect to the network when MAC filtering is in place, such as on a wireless network. By spoofing the MAC address of a legitimate wireless station, an intruder can take on that station's identity and use the network.

Security, Functionality, and Ease of Use Triangle

As a security professional, it's difficult to strike a balance between adding security barriers to prevent an attack and allowing the system to remain functional for users. The security, functionality, and ease of use triangle is a representation of the balance between security and functionality and the system's ease of use for users (see Figure 1.3). In general, as security increases, the system's functionality and ease of use decrease for users.

FIGURE 1.3 Security, functionality, and ease of use triangle



In an ideal world, security professionals would like to have the highest level of security on all systems; however, sometimes this isn't possible. Too many security barriers make it difficult for users to use the system and impede the system's functionality. Suppose that in order to gain entry to your office at work, you had to first pass through a guard checkpoint at the entrance to the parking lot to verify your license plate number, then show a badge as you entered the building, then use a passcode to gain entry to the elevator, and finally use a key to unlock your office door. You might feel the security checks were too stringent! Any one of those checks could cause you to be detained and consequently miss an important meeting—for example, if your car was in the repair shop and you had a rental car, or you forgot your key or badge to access the building, elevator, or office door.

Defining the Skills Required to Become an Ethical Hacker

Ethical hackers who stay a step ahead of malicious hackers must be computer systems experts who are very knowledgeable about computer programming, networking and operating systems. In-depth knowledge about highly targeted platforms (such as Windows, Unix, and Linux) is also a requirement. Patience, persistence, and immense perseverance are important qualities that many hackers possess because of the length of time and level of concentration required for most attacks/compromises to pay off.

Most ethical hackers are knowledgeable about security areas and related issues but don't necessarily have a strong command of the countermeasure that can prevent attacks. The following chapters of this book will address both the vulnerabilities and the countermeasures to prevent certain types of attacks.

What Is Vulnerability Research?

Vulnerability research is the process of discovering vulnerabilities and design weaknesses that could lead to an attack on a system. Several websites and tools exist to aid the ethical hacker in maintaining a current list of vulnerabilities and possible exploits for their systems or networks. It's essential that a systems administrator keep current on the latest viruses, Trojans, and other common exploits in order to adequately protect their systems and network. Also, by becoming familiar with the newest threats, an administrator can learn how to detect, prevent, and recover from an attack.

Describing the Ways to Conduct Ethical Hacking

Ethical hacking is usually conducted in a structured and organized manner, usually as part of a penetration test or security audit. The depth and breadth of the systems and applications to be tested are usually determined by the needs and concerns of the client. Many ethical hackers are members of a tiger team.

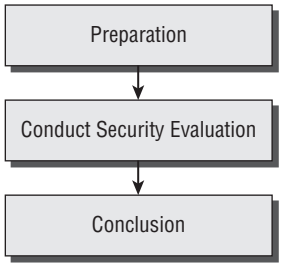
The following steps are a framework for performing a security audit of an organization:

1. Talk to the client, and discuss the needs to be addressed during the testing.
2. Prepare and sign nondisclosure agreement (NDA) documents with the client.
3. Organize an ethical hacking team, and prepare a schedule for testing.
4. Conduct the test.
5. Analyze the results of the testing, and prepare a report.
6. Present the report to the client.

In-depth penetration testing and security auditing information is discussed in EC-Council's Licensed Penetration Tester (LPT) certification.

Creating a Security Evaluation Plan

Many ethical hackers acting in the role of security professionals use their skills to perform security evaluations or penetration tests. These tests and evaluations have three phases, generally ordered as follows:



The Preparation phase involves a formal agreement between the ethical hacker and the organization. This agreement should include the full scope of the test, the types of attacks (inside or outside) to be used, and the testing types: white, black, or grey box. (These types are defined later, in the section "Testing Types.")

During the Conduct Security Evaluation phase, the tests are conducted, after which the tester prepares a formal report of vulnerabilities and other findings. The findings are presented to the organization in the Conclusion phase along with any recommendations to improve security.

Types of Ethical Hacks

Ethical hackers can use many different methods to breach an organization's security during a simulated attack or penetration test. The most common methods follow:

Remote network A remote network hack attempts to simulate an intruder launching an attack over the Internet. The ethical hacker tries to break or find a vulnerability in the outside defenses of the network, such as firewall, proxy, or router vulnerabilities.

Remote dial-up network A remote dial-up network hack tries to simulate an intruder launching an attack against the client's modem pools. *War dialing* is the process of repetitive dialing to find an open system and is an example of such an attack.

Local network A local network hack simulates someone with physical access gaining additional unauthorized access using the local network. The ethical hacker must gain direct access to the local network in order to launch this type of attack.

Stolen equipment A stolen-equipment hack simulates theft of a critical information resource such as a laptop owned by an employee. Information such as usernames, passwords, security settings, and encryption types can be gained by stealing a laptop.

Social engineering A social-engineering attack checks the integrity of the organization's employees by using the telephone or face-to-face communication to gather information for use in an attack. Social engineering attacks can be used to acquire usernames, passwords, or other organizational security measures.

Physical entry A physical-entry attack attempts to compromise the organization's physical premises. An ethical hacker who gains physical access can plant viruses, Trojans, rootkits, or hardware key loggers (physical device used to record keystrokes) directly on systems in the target network.

Testing Types

When performing a security test or penetration test, an ethical hacker utilizes one or more types of testing on the system. Each type simulates an attacker with different levels of knowledge about the target organization. These types are as follows:

Black box Black-box testing involves performing a security evaluation and testing with no prior knowledge of the network infrastructure or system to be tested. Testing simulates an attack by a malicious hacker outside the organization's security perimeter.

White box White-box testing involves performing a security evaluation and testing with complete knowledge of the network infrastructure such as a network administrator would have.

Grey box Grey-box testing involves performing a security evaluation and testing internally. Testing examines the extent of access by insiders within the network.

Ethical Hacking Report

The result of a network penetration test or security audit is an ethical hacking report. This report details the results of the hacking activity, the types of tests performed, and the hacking methods used. These results are compared against the work scheduled prior to the Conduct Security Evaluation phase. Any vulnerabilities identified are detailed, and countermeasures are suggested. This document is usually delivered to the organization in hard-copy format, for security reasons.

The details of the ethical hacking report must be kept confidential, because they highlight the organization's security risks and vulnerabilities. If this document falls into the wrong hands, the results could be disastrous for the organization.

Understanding the Legal Implications of Hacking

An ethical hacker should know the penalties of unauthorized hacking into a system. No ethical hacking activities associated with a network-penetration test or security audit should begin until a signed legal document giving the ethical hacker express permission to perform the hacking activities is received from the target organization. Ethical hackers need to be judicious with their hacking skills and recognize the consequences of misusing those skills.

Computer crimes can be broadly categorized into two categories: crimes facilitated by a computer and crimes where the computer is the target.

The two most important U.S. laws regarding computer crimes are described in the following section. Although the CEH exam is international in scope, make sure you familiarize yourself with these two U.S. statutes and the punishment for hacking. Remember, intent doesn't make a hacker above the law; even an ethical hacker can be prosecuted for breaking these laws.

The Cyber Security Enhancement Act of 2002 mandates life sentences for hackers who "recklessly" endanger the lives of others. Malicious hackers who create a life-threatening situation by attacking computer networks for transportation systems, power companies, or other public services or utilities can be prosecuted under this law.

Understanding 18 U.S.C. § 1029 and 1030 U.S. Federal Law

The U.S. Code categorizes and defines the laws of the United States by titles. Title 18 details "Crimes and Criminal Procedure." Section 1029, "Fraud and related activity in connection with access devices," states that if you produce, sell, or use counterfeit access devices or telecommunications instruments with intent to commit fraud and obtain services or products with a value or $1,000, you have broken the law. Section 1029 criminalizes the misuse of computer passwords and other access devices such as token cards.

Section 1030, "Fraud and related activity in connection with computers," prohibits accessing protected computers without permission and causing damage. This statute criminalizes the spreading of viruses and worms and breaking into computer systems by unauthorized individuals.

The full text of the Section 1029 and 1030 laws is included as an appendix in this book for your reference.

Exam Essentials

Understand essential hacker terminology. Make sure you're familiar with and can define the terms *threat*, *exploit*, *vulnerability*, *target of evaluation*, and *attack*.

Understand the difference between ethical hackers and crackers. Ethical hackers are security professionals who act defensively. Crackers are malicious hackers who choose to inflict damage on a target system.

Know the classes of hackers. It's critical to know the differences among black-hat, white-hat, and grey-hat hackers for the exam. Know who the good guys are and who the bad guys are in the world of hacking.

Know the phases of hacking. Passive and active reconnaissance, scanning, gaining access, maintaining access, and covering tracks are the five phases of hacking. Know the order of the phases and what happens during each phase.

Be aware of the types of attacks. Understand the differences between active and passive and inside and outside attacks. The ability to be detected is the difference between active and passive attacks. The location of the attacker is the difference between inside and outside attacks.

Know the ethical hacking types. Hackers can attack the network from a remote network, a remote dial-up network, or a local network, or through social engineering, stolen equipment, or physical access.

Understand the security testing types Ethical hackers can test a network using black-box, white-box, or grey-box testing techniques.

Know the contents of an ethical hacking report. An ethical hacking report contains information on the hacking activities performed, network or system vulnerabilities discovered, and countermeasures that should be implemented.

Know the legal implications involved in hacking. The Cyber Security Enhancement Act of 2002 can be used to prosecute ethical hackers who recklessly endanger the lives of others.

Be aware of the laws and punishment applicable to computer intrusion. Title 18 sections 1029 and 1030 of the U.S. Code carry strict penalties for hacking, no matter what the intent.

Review Questions

1. Which of the following statements best describes a white-hat hacker?
   - **A.** Security professional
   - **B.** Former black hat
   - **C.** Former grey hat
   - **D.** Malicious hacker

2. A security audit performed on the internal network of an organization by the network administration is also known as _____.
   - **A.** Grey-box testing
   - **B.** Black-box testing
   - **C.** White-box testing
   - **D.** Active testing
   - **E.** Passive testing

3. What is the first phase of hacking?
   - **A.** Attack
   - **B.** Maintaining access
   - **C.** Gaining access
   - **D.** Reconnaissance
   - **E.** Scanning

4. What type of ethical hack tests access to the physical infrastructure?
   - **A.** Internal network
   - **B.** Remote network
   - **C.** External network
   - **D.** Physical access

5. The security, functionality, and ease of use triangle illustrates which concept?
   - **A.** As security increases, functionality and ease of use increase.
   - **B.** As security decreases, functionality and ease of use increase.
   - **C.** As security decreases, functionality and ease of use decrease.
   - **D.** Security does not affect functionality and ease of use.

6. Which type of hacker represents the highest risk to your network?
   - **A.** Disgruntled employees
   - **B.** Black-hat hackers
   - **C.** Grey-hat hackers
   - **D.** Script kiddies

7. What are the three phases of a security evaluation plan? (Choose three answers.)
   - **A.** Conduct Security Evaluation
   - **B.** Preparation
   - **C.** Conclusion
   - **D.** Final
   - **E.** Reconnaissance
   - **F.** Design Security
   - **G.** Vulnerability Assessment

8. Hacking for a cause is called _____.
   - **A.** Active hacking
   - **B.** Hacktivism
   - **C.** Activism
   - **D.** Black-hat hacking

9. Which federal law is most commonly used to prosecute hackers?
   - **A.** Title 12
   - **B.** Title 18
   - **C.** Title 20
   - **D.** Title 2

10. When a hacker attempts to attack a host via the Internet it is known as what type of attack?
    - **A.** Remote attack
    - **B.** Physical access
    - **C.** Local access
    - **D.** Internal attack

Answers to Review Questions

1. A. Explanation: A white-hat hacker is a "good" guy who uses his skills for defensive purposes.
2. C. Explanation: White-box testing is a security audit performed with internal knowledge of the systems.
3. D. Explanation: Reconnaissance is gathering information necessary to perform the attack.
4. D. Explanation: Physical access tests access to the physical infrastructure.
5. B. Explanation: As security increases it makes it more difficult to use and less functional.
6. A. Explanation: Disgruntled employees have information which can allow them to launch a powerful attack.
7. A, B, C. Explanation: The three phases of a security evaluation plan are preparation, conduct security evaluation, and conclusion.
8. B. Explanation: Hacktivism is performed by individual who claim to be hacking for a political or social cause.
9. B. Explanation: Title 18 of the U.S. Code of law is most commonly used to prosecute hackers
10. A. Explanation: An attack from the Internet is known as a remote attack.