Covers all Exam Objectives for CEHv6

Includes Real-World Scenarios, Hands-On Exercises, and Leading-Edge Exam Prep Software Featuring:

- Custom Test Engine
- Hundreds of Sample Questions
- Electronic Flashcards
- Entire Book in PDF

CEH™

Certified Ethical Hacker

STUDY GUIDE

Exam 312-50
Exam ECO-350

Kimberly Graves

SYBEX | SERIOUS SKILLS.

Table of Contents

Chapter 1

Introduction to Ethical Hacking, Ethics, and Legality

CEH EXAM OBJECTIVES COVERED IN THIS CHAPTER:

- ✓ Understand ethical hacking terminology
- ✓ Define the job role of an ethical hacker
- ✓ Understand the different phases involved in ethical hacking
- ✓ Identify different types of hacking technologies
- ✓ List the five stages of ethical hacking
- ✓ What is hacktivism?
- ✓ List different types of hacker classes
- ✓ Define the skills required to become an ethical hacker
- ✓ What is vulnerability research?
- ✓ Describe the ways of conducting ethical hacking
- ✓ Understand the legal implications of hacking
- ✓ Understand 18 USC §1030 US 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 out passwords, account numbers, or other confidential data. In reality, a good hacker, or security professional acting as an ethical hacker, just has to understand how a computer system works and know what tools to employ in order to find a security weakness. This book will teach you the same techniques and software tools that many hackers use to gather valuable data and attack computer systems.

The realm of hackers and how they operate is unknown to most computer and security professionals. Hackers use specialized computer software tools to gain access to information. By learning the same skills and employing the software tools used by hackers, you will be able to defend your computer networks and systems against malicious attacks.

The goal of this first chapter is to introduce you to the world of the hacker and to define the terminology used in discussing computer security. To be able to defend against malicious hackers, security professionals must first understand how to employ ethical hacking techniques. This book will detail the tools and techniques used by hackers so that you can use those tools to identify potential risks in your systems. This book will guide you through the hacking process as a *good guy*.

Most ethical hackers are in the business of hacking for profit, an activity known as *penetration testing*, or *pen testing* for short. Pen testing is usually conducted by a security professional to identify security risks and vulnerabilities in systems and networks. The purpose of identifying risks and vulnerabilities is so that a countermeasure can be put in place and the risk mitigated to some degree. Ethical hackers are in the business of hacking and as such need to conduct themselves in a professional manner.

Additionally, state, country, or international laws must be understood and carefully considered prior to using hacking software and techniques. Staying within the law is a must for the ethical hacker. An ethical hacker is acting as a security professional when performing pen tests and must always act in a professional manner.

Defining Ethical Hacking

The next section will explain the purpose of ethical hacking and exactly what ethical hackers do. As mentioned earlier, ethical hackers must always act in a professional manner to differentiate themselves from malicious hackers. Gaining the trust of the client and taking

all precautions to do no harm to their systems during a pen test are critical to being a professional. Another key component of ethical hacking is to always gain permission from the data owner prior to accessing the computer system. This is one of the ways ethical hackers can overcome the stereotype of hackers and gain the trust of clients.

The goals ethical hackers are trying to achieve in their hacking attempts will be explained as well in this section.

Understanding the Purpose of Ethical Hacking

When I tell people that I am an ethical hacker, I usually hear snickers and comments like "That's an oxymoron." Many people ask, "Can hacking be ethical?" Yes! That best describes what I do as a security professional. I use the same software tools and techniques as malicious hackers to find the security weakness in computer networks and systems. Then I apply the necessary fix or patch to prevent the malicious hacker from gaining access to the data. This is a never-ending cycle as new weaknesses are constantly being discovered in computer systems and patches are created by the software vendors to mitigate the risk of attack.

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.

The term *cracker* describes a hacker who uses their hacking skills and toolset for destructive or offensive purposes such as disseminating viruses or performing denial-of-service (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*.

Hackers can be divided into three groups:

White Hats Good guys, ethical hackers

Black Hats Bad guys, malicious hackers

Gray Hats Good or bad hacker; depends on the situation

Ethical hackers usually fall into the white-hat category, but sometimes they're former gray hats who have become security professionals and who *now* 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. White-hat hackers are prime candidates for the exam. White hats are those who hack with permission from the data owner. It is critical to get permission prior to beginning any hacking activity. This is what makes a security professional a white hat versus a malicious hacker who cannot be trusted.

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 systems, with malicious intent. Having gained unauthorized access, black-hat hackers destroy vital data, deny legitimate users service, and just cause problems for their targets. Black-hat hackers and crackers can easily be differentiated from white-hat hackers because their actions are malicious. This is the traditional definition of a hacker and what most people consider a hacker to be.

Gray Hats

Gray hats are hackers who may work offensively or defensively, depending on the situation. This is the dividing line between hacker and cracker. Gray-hat hackers may just be interested in hacking tools and technologies and are not malicious black hats. Gray hats 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.

The difference between white hats and gray hats is that *permission* word. Although gray hats might have good intentions, without the correct permission they can no longer be considered ethical.

Now that you understand the types of hackers, let's look at what hackers do. This may seem simple—they hack into computer systems—but sometimes it's not that simple or nebulous. There is a process that should be followed and information that needs to be documented. In the next section, we'll look at what hackers, and most importantly ethical hackers, do.

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,* or *pen 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. A pen test is no more than just performing those same steps with the same tools used by a malicious hacker to see what data could be exposed using hacking tools and techniques.

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. A penetration test plan can then be built around the data that needs to be protected and potential risks.

Documenting the results of various tests is critical in producing the end product of the pen test: the pen test report. Taking screenshots of potentially valuable information or saving log files is critical to presenting the findings to a client in a pen test report. The pen test report is a compilation of all the potential risks in a computer or system. More detail about the contents of the pen test report will be covered in the last chapter of this book.

Goals Attackers Try to Achieve

Whether perpetuated by an ethical hacker or malicious hacker, all attacks are an attempt to breach computer system security. 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. For example, in performing a *denial-of-service (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 the sender intended it. A bit-flipping attack is an attack on a cryptographic cipher: the attacker changes the cipher text in such a way as to result in a predictable change of the plain text, although the attacker doesn't learn the plain text itself. This type of attack isn't directed 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* attack because it allows an unauthorized device to connect to the network when Media Access Control (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.

An Ethical Hacker's Skill Set

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 for ethical hackers because of the length of time and level of concentration required for most attacks to pay off. Networking, web programming, and database skills are all useful in performing ethical hacking and vulnerability testing.

Most ethical hackers are well rounded with wide knowledge on computers and networking. In some cases, an ethical hacker will act as part of a "tiger team" who has been hired to test network and computer systems and find vulnerabilities. In this case, each member of the team will have distinct specialties, and the ethical hacker may need more specialized skills in one area of computer systems and networking. Most ethical hackers are knowledgeable about security areas and related issues but don't necessarily have a strong command of the countermeasures that can prevent attacks.

Ethical Hacking Terminology

Being able to understand and define terminology is an important part of a CEH's responsibility. This terminology is how security professionals acting as ethical hackers communicate. This "language" of hacking is necessary as a foundation to the follow-on concepts in later chapters of this book. In this section, we'll discuss a number of terms you need to be familiar with for the CEH certification exam:

Threat 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. Malicious hackers and their use of software and hacking techniques are themselves threats to an organization's information security.

Exploit A piece of software or technology that takes advantage of a bug, glitch, or vulnerability, leading to unauthorized access, privilege escalation, or denial of service on a computer system. Malicious hackers are looking for exploits in computer systems to open the door to an initial attack. Most exploits are small strings of computer code that, when executed on a system, expose vulnerability. Experienced hackers create their own exploits, but it is not necessary to have any programming skills to be an ethical hacker as many hacking software programs have ready-made exploits that can be launched against a computer system or network. An exploit is a defined way to breach the security of an IT system through a vulnerability.

Vulnerability The 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. Exploit code is written to target a vulnerability and cause a fault in the system in order to retrieve valuable data.

Target of Evaluation (TOE) A system, program, or network that is the subject of a security analysis or attack. Ethical hackers are usually concerned with high-value TOEs, systems that contain sensitive information such as account numbers, passwords, Social Security numbers, or other confidential data. It is the goal of the ethical hacker to test hacking tools against the high-value TOEs to determine the vulnerabilities and patch them to protect against exploits and exposure of sensitive data.

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 to prevent an attack.

There are two primary methods of delivering exploits to computer systems:

Remote The exploit is sent over a network and exploits security vulnerabilities without any prior access to the vulnerable system. Hacking attacks against corporate computer systems or networks initiated from the outside world are considered remote. Most people think of this type of attack when they hear the term *hacker*, but in reality most attacks are in the next category.

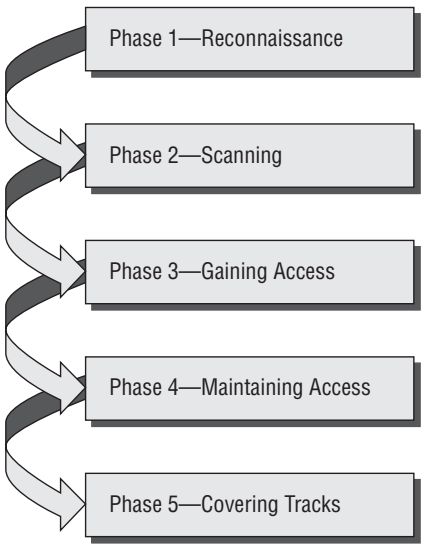
Local The exploit is delivered directly to the computer system or network, which requires prior access to the vulnerable system to increase privileges. Information security policies should be created in such a way that only those who need access to information should be allowed access and they should have the lowest level of access to perform their job function. These concepts are commonly referred as "need to know" and "least privilege" and, when used properly, would prevent local exploits. Most hacking attempts occur from within an organization and are perpetuated by employees, contractors, or others in a trusted position. In order for an insider to launch an attack, they must have higher privileges than necessary based on the concept of "need to know." This can be accomplished by privilege escalation or weak security safeguards.

The Phases of Ethical Hacking

The process of ethical hacking can be broken down into five distinct phases. Later in this book, hacking software programs and tools will be categorized into each of these steps.

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 1.1 illustrates the five phases that hackers generally follow in hacking a computer system.

FIGURE 1.1 Phases of hacking



Phase 1: Passive and Active Reconnaissance

Passive reconnaissance involves gathering information about 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, most reconnaissance is done sitting in front of a computer.

When hackers are looking for information on a potential target, they commonly run an Internet search on an individual or company to gain information. I'm sure many of you have performed the same search on your own name or a potential employer, or just to gather information on a topic. This process when used to gather information regarding a TOE is generally called *information gathering*. Social engineering and dumpster diving are also considered passive information-gathering methods. These two methods will be discussed in more detail later in this chapter.

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. Sniffing network traffic is a common hook for many ethical hackers. Once they use some of the hacking tools and are able to see all the data that is transmitted in the clear over the communication networks, they are eager to learn and see more.

Sniffing tools are simple and easy to use and yield a great deal of valuable information. An entire chapter in this book (Chapter 6, "Gathering Data from Networks: Sniffers") is dedicated to these tools, which literally let you see all the data that is transmitted on the network. Many times this includes usernames and passwords and other sensitive data. This is usually quite an eye-opening experience for many network administrators and security professionals and leads to serious security concerns.

Active reconnaissance involves probing the network to discover individual hosts, IP addresses, and services on the network. This process 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. Many software tools that perform active reconnaissance can be traced back to the computer that is running the tools, thus increasing the chance of detection for the hacker.

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 include

- Dialers
- Port scanners
- Internet Control Message Protocol (ICMP) scanners

- Ping sweeps
- Network mappers
- Simple Network Management Protocol (SNMP) sweepers
- Vulnerability scanners

Hackers are seeking any information that can help them perpetrate an attack on a target, such as the following:

- Computer names
- Operating system (OS)
- Installed software
- IP addresses
- User accounts

The methods and tools used in scanning are discussed in detail in Chapter 3, "Gathering Network and Host Information: Scanning and Enumeration."

Phase 3: Gaining Access

Phase 3 is when the real hacking takes place. Vulnerabilities exposed during the reconnaissance and scanning phase are now exploited to gain access to the target system. The hacking attack can be delivered to the target system via 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, and session hijacking. These topics will be discussed in later chapters. Gaining access is known in the hacker world as *owning* the system because once a system has been hacked, the hacker has control and can use that system as they wish.

Phase 4: Maintaining Access

Once a hacker has gained access to a target system, 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
- Using a tunneling protocol
- Altering log files

Steganography, using tunneling protocols, and altering log files for purposes of hacking will be discussed in later chapters.

Identifying Types of Hacking Technologies

Many methods and tools exist for locating vulnerabilities, running exploits, and compromising systems. Once vulnerabilities are found in a system, a hacker can exploit that vulnerability and install malicious software. Trojans, backdoors, and rootkits are all forms of malicious software, or *malware*. Malware is installed on a hacked system after a vulnerability has been exploited.

Buffer overflows and SQL injection are two other methods used to gain access into computer systems. Buffer overflows and SQL injection are used primarily against application servers that contain databases of information.

These technologies and attack methods will each be discussed in later chapters. Many are so complex that an entire chapter (Chapter 9, "Attacking Applications: SQL Injection and Buffer Overflows") is devoted to explaining the attack and applicable technologies.

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

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

Applications Applications usually aren't thoroughly tested for vulnerabilities when developers are writing the code, which can leave many programming flaws that a hacker can exploit. Most application development is "feature-driven," meaning programmers are under a deadline to turn out the most robust application in the shortest amount of time.

Shrink-Wrap Code Many off-the-shelf programs come with extra features the common user isn't aware of, and these features can be used to exploit the system. The macros in Microsoft Word, for example, 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; this 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.

Identifying Types of Ethical Hacks

Ethical hackers use many different methods to breach an organization's security during a simulated attack or penetration test. Most ethical hackers have a specialty in one or a few of the following attack methods. In the initial discussion with the client, one of the questions that should be asked is whether there are any specific areas of concern, such as wireless networks or social engineering. This enables the ethical hacker to customize the test to be performed to the needs of the client. Otherwise, security audits should include attempts to access data from all of the following methods.

Here are the most common entry points for an attack:

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 vulnerability in the outside defenses of the network, such as firewall, proxy, or router vulnerabilities. The Internet is thought to be the most common hacking vehicle, while in reality most organizations have strengthened their security defenses sufficient to prevent hacking from the public network.

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. Many organizations have replaced dial-in connections with dedicated Internet connections so this method is less relevant than it once was in the past.

Local Network A local area network (LAN) 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. Wireless LANs (WLANs) fall in this category and have added an entirely new avenue of attack as radio waves travel through building structures. Because the WLAN signal can be identified and captured outside the building, hackers no longer have to gain physical access to the building and network to perform an attack on the LAN. Additionally, the huge growth of WLANs has made this an increasing source of attack and potential risk to many organizations.

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. This is usually a commonly overlooked area by many organizations. Once a hacker has access to a laptop authorized in the security domain, a lot of information, such as security configuration, can be gathered. Many times laptops disappear and are not reported quickly enough to allow the security administrator to lock that device out of the network.

Social Engineering A social-engineering attack checks the security and 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. Social-engineering scenarios

usually consist of a hacker calling the help desk and talking the help desk employee into giving out confidential security information.

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. Additionally, confidential documents that are not stored in a secure location can be gathered by the hacker. Lastly, physical access to the building would allow a hacker to plant a rogue device such as a wireless access point on the network. These devices could then be used by the hacker to access the LAN from a remote location.

Understanding 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. Black-box testing can take the longest amount of time and most effort as no information is given to the testing team. Therefore, the information-gathering, reconnaissance, and scanning phases will take a great deal of time. The advantage of this type of testing is that it most closely simulates a real malicious attacker's methods and results. The disadvantages are primarily the amount of time and consequently additional cost incurred by the testing team.

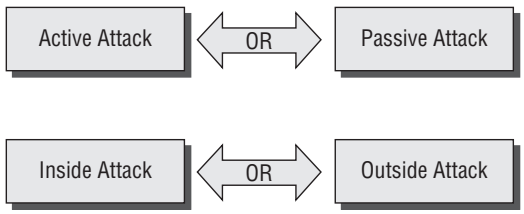
White Box White-box testing involves performing a security evaluation and testing with complete knowledge of the network infrastructure such as a network administrator would have. This testing is much faster than the other two methods as the ethical hacker can jump right to the attack phase, thus bypassing all the information-gathering, reconnaissance, and scanning phases. Many security audits consist of white-box testing to avoid the additional time and expense of black-box testing.

Gray Box Gray-box testing involves performing a security evaluation and testing internally. Testing examines the extent of access by insiders within the network. The purpose of this test is to simulate the most common form of attack, those that are initiated from within the network. The idea is to test or audit the level of access given to employees or contractors and see if those privileges can be escalated to a higher level.

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 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 attacks* or *outside attacks*. Figure 1.2 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 1.2 Types of attacks

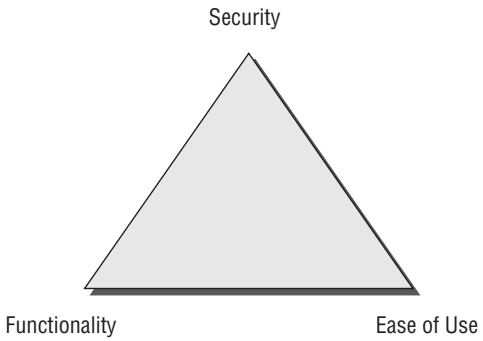


Most network security breaches originate from within an organization—usually from the company's own employees or contractors.

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.

Real World Scenario

Usability vs. Security

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. This is an example of tension between usability and security.

In many cases, if security checks are too stringent people will bypass them completely. For example, people might prop open a door so they can get back in the building. When I am doing a physical security audit during a penetration test, I just carry a box toward the door of the building; invariably people will hold the door open for someone carrying something. It is just human nature and is an easy way for a hacker to bypass security measures.

Vulnerability Research and Tools

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 against systems or networks. It's essential that system administrators 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.

Vulnerability research is different from ethical hacking in that research is passively looking for possible security holes whereas ethical hacking is trying to see what information can be gathered. It is similar to an intruder casing a building and seeing a window at ground level and thinking "Well, maybe I can use that as an entry point." An ethical hacker would go and try to open the window to see if it is unlocked and provide access to the building. Next they would look around the room they entered through the building for any valuable information. Each entry into a system and additional level of access gives a foothold to additional exploits or attacks.

Ethical Hacking Report

The result of a network penetration test or security audit is an ethical hacking, or pen test report. Either name is acceptable, and they can be used interchangeably. This report details the results of the hacking activity, the types of tests performed, and the hacking methods used. The results are compared against the expectations initially agreed upon with the customer. 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. It would essentially give someone the roadmap to all the security weaknesses of an organization.

How to Be Ethical

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. A tiger team works together to perform a full-scale test covering all aspects of network, physical, and systems intrusion.

The ethical hacker must follow certain rules to ensure that all ethical and moral obligations are met. An ethical hacker must do the following:

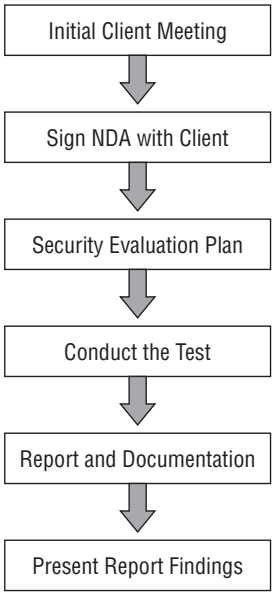
- Gain authorization from the client and have a signed contract giving the tester permission to perform the test.
- Maintain and follow a nondisclosure agreement (NDA) with the client in the case of confidential information disclosed during the test.
- Maintain confidentiality when performing the test. Information gathered may contain sensitive information. No information about the test or company confidential data should ever be disclosed to a third party.
- Perform the test up to but not beyond the agreed-upon limits. For example, DoS attacks should only be run as part of the test if they have previously been agreed upon with the client. Loss of revenue, goodwill, and worse could befall an organization whose servers or applications are unavailable to customers as a result of the testing.

The following steps (shown in Figure 1.4) are a framework for performing a security audit of an organization and will help to ensure that the test is conducted in an organized, efficient, and ethical manner:

1. Talk to the client, and discuss the needs to be addressed during the testing.
2. Prepare and sign 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 findings to the client.

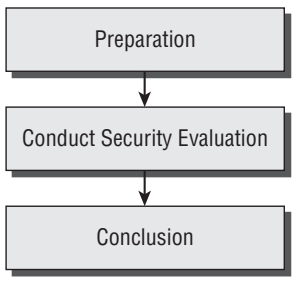
FIGURE 1.4 Security audit steps



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

Performing a Penetration Test

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:



Preparation This 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 gray box.

Conduct Security Evaluation During this phase, the tests are conducted, after which the tester prepares a formal report of vulnerabilities and other findings.

Conclusion The findings are presented to the organization in this phase, along with any recommendations to improve security.

Notice that the ethical hacker does not "fix" or patch any of the security holes they may find in the target of evaluation. This is a common misconception of performing security audits or penetration tests. The ethical hacker usually does not perform any patching or implementation of countermeasures. The final goal or deliverable is really the findings of the test and an analysis of the associated risks. The test is what leads to the findings in the final report and must be well documented.

Contrary to popular belief, ethical hackers performing a penetration test must be very organized and efficient, and they must document every finding by taking screenshots, copying the hacking tool output, or printing important log files. Ethical hackers must be very professional and present a well-documented report to be taken seriously in their profession. More information on performing a penetration test can be found in Chapter 15, "Performing a Penetration Test."

Defining 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, and implementing 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."

Keeping It Legal

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.

Real World Scenario

Hacking Attempt Liability

A website operated by a securities brokerage firm suffers a hacking attack. As a result of the attack, the firm's customers are unable to conduct trades for several hours. On the day of the attack, the stock market is volatile, and many customers are trying unsuccessfully to buy or sell stocks. The customers are very unhappy and blame the firm for failing to prevent, detect, and recover from the attack.

In this situation, the hackers are the ones to blame. But what about the brokerage firm itself? Customers are relying on the firm's website to make trades. Are the brokerage firm and their network providers vulnerable to a lawsuit from unhappy clients who lost money as a result of the shutdown? Does the brokerage firm have any liability because they were unable to prevent the shutdown of the website-driven trading system? Some of the laws discussed in this chapter will address this issue of liability after hacking attacks.

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

The most important U.S. laws regarding computer crimes are described in the following sections. Although the CEH exam is international in scope, make sure you familiarize yourself with these 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.

Cyber Security Enhancement Act and SPY ACT

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.

The Securely Protect Yourself Against Cyber Trespass Act of 2007 (SPY ACT) deals with the use of spyware on computer systems and essentially prohibits the following:

- Taking remote control of a computer when you have not been authorized to do so
- Using a computer to send unsolicited information to people (commonly known as spamming)
- Redirecting a web browser to another site that is not authorized by the user
- Displaying advertisements that cause the user to have to close out of the web browser (pop-up windows)
- Collecting personal information using keystroke logging

- Changing the default web page of the browser
- Misleading users so they click on a web page link or duplicating a similar web page to mislead a user

The SPY ACT is important in that it starts to recognize annoying pop-ups and spam as more than mere annoyances and as real hacking attempts. The SPY ACT lays a foundation for prosecuting hackers that use spam, pop-ups, and links in emails.

18 USC §1029 and 1030

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 over $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.

U.S. State Laws

In addition to federal laws, many states have their own laws associated with hacking and auditing computer networks and systems. When performing penetration testing, review the applicable state laws to ensure that you are staying on the right side of the law. In many cases, a signed testing contract and NDA will suffice as to the intent and nature of the testing.

The National Security Institute has a website listing all the state laws applicable to computer crimes. The URL is

```
http://nsi.org/Library/Compsec/computerlaw/statelaws.html
```

Federal Managers Financial Integrity Act

The Federal Managers Financial Integrity Act of 1982 (FMFIA) is basically a responsibility act to ensure that those managing financial accounts are doing so with the utmost

responsibility and are ensuring the protection of the assets. This description can be construed to encompass all measurable safeguards to protect the assets from a hacking attempt. The act essentially ensures that

- Funds, property, and other assets are safeguarded against waste, loss, unauthorized use, or misappropriation.
- Costs are in compliance with applicable laws.

The FMFIA is important to ethical hacking as it places the responsibility on an organization for the appropriate use of funds and other assets. Consequently, this law requires management to be responsible for the security of the organization and to ensure the appropriate safeguards against hacking attacks.

Freedom of Information Act (FOIA)

The Freedom of Information Act (5 USC 552), or FoIA, makes many pieces of information and documents about organizations public. Most records and government documents can be obtained via the FoIA. Any information gathered using this act is fair game when you are performing reconnaissance and information gathering about a potential target.

Federal Information Security Management Act (FISMA)

The Federal Information Security Management Act (FISMA) basically gives ethical hackers the power to do the types of testing they perform and makes it a mandatory requirement for government agencies.

FISMA requires that each federal agency develop, document, and implement an agency-wide information security program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source. The information security program must include the following:

- Periodic assessments of the risk and magnitude of the harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support the operations and assets of the agency
- Policies and procedures that are based on risk assessments, cost-effectively reduce information security risks to an acceptable level, and ensure that information security is addressed throughout the life cycle of each agency information system
- Subordinate plans for providing adequate information security for networks, facilities, information systems, or groups of information systems, as appropriate
- Security awareness training to inform personnel (including contractors and other users of information systems that support the operations and assets of the agency) of the information security risks associated with their activities and their responsibilities in complying with agency policies and procedures designed to reduce these risks

- Periodic testing and evaluation of the effectiveness of information security policies, procedures, and practices (including the management, operational, and technical controls of every agency information system identified in their inventory) with a frequency depending on risk, but no less than annually
- A process for planning, implementing, evaluating, and documenting remedial action to address any deficiencies in the information security policies, procedures, and practices of the agency
- Procedures for detecting, reporting, and responding to security incidents (including mitigating risks associated with such incidents before substantial damage is done and notifying and consulting with the federal information security incident response center, and as appropriate, law enforcement agencies, relevant Offices of Inspector General, and any other agency or office, in accordance with law or as directed by the President
- Plans and procedures to ensure continuity of operations for information systems that support the operations and assets of the agency

This act is guaranteed job security for ethical white hat hackers to perform continual security audits of government agencies and other organizations.

Privacy Act of 1974

The Privacy Act of 1974 (5 USC 552a) ensures nondisclosure of personal information and ensures that government agencies are not disclosing information without the prior written consent of the person whose information is in question.

USA PATRIOT Act

This act, with the official name Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001, gives the government the authority to intercept voice communications in computer hacking and other types of investigations. The Patriot Act was enacted primarily to deal with terrorist activity but can also be construed as a wiretap mechanism to discover and prevent hacking attempts.

Government Paperwork Elimination Act (GPEA)

The Government Paperwork Elimination Act (GPEA) of 1998 requires federal agencies to allow people the option of using electronic communications when interacting with a government agency. GPEA also encourages the use of electronic signatures. When valuable government information is stored in electronic format, the targets and stakes for hackers is increased.

Cyber Laws in Other Countries

Other countries each have their own applicable laws regarding protection of information and hacking attacks. When you're performing penetration testing for international organizations, it is imperative to check the laws of the governing nation to make sure the testing is legal in the country. With the use of the Internet and remote attacks, regional and international borders can be crossed very quickly. When you're performing an outside remote attack, the data may be stored on servers in another country and the laws of that country may apply. It is better to be safe than sorry, so do the research prior to engaging in a penetration test for an international entity. In some countries, laws may be more lenient than in the United States, and this fact may work to your advantage as you perform information gathering.

Summary

Ethical hacking is more than just running hacking tools and gaining unauthorized access to systems just to see what is accessible. When performed by a security professional, ethical hacking encompasses all aspects of reconnaissance and information gathering, a structured approach, and postattack analysis. Ethical hackers require in-depth knowledge of systems and tools as well as a great deal of patience and restraint to ensure no damage is done to the target systems. Hacking can be performed ethically and in fact is being mandated by government and the private sector to ensure systems security.

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 gray-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 gray-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 US 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 gray 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.** Gray-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.** Gray-hat hackers
   - **D.** Script kiddies

7. What are the three phases of a security evaluation plan? (Choose three answers.)
   - **A.** 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

11. Which law allows for gathering of information on targets?
    - **A.** Freedom of Information Act
    - **B.** Government Paperwork Elimination Act
    - **C.** USA PATRIOT Act of 2001
    - **D.** Privacy Act of 1974

12. The Securely Protect Yourself Against Cyber Trespass Act prohibits which of the following? (Choose all that apply.)
    - **A.** Sending spam
    - **B.** Installing and using keystroke loggers
    - **C.** Using video surveillance
    - **D.** Implementing pop-up windows

13. Which step in the framework of a security audit is critical to protect the ethical hacker from legal liability?
    A. Talk to the client prior to the testing.
    B. Sign an ethical hacking agreement and NDA with the client prior to the testing.
    C. Organize an ethical hacking team and prepare a schedule prior to testing.
    D. Analyze the testing results and prepare a report.

14. Which of the following is a system, program, or network that is the subject of a security analysis?
    A. Owned system
    B. Vulnerability
    C. Exploited system
    D. Target of evaluation

15. Which term best describes a hacker who uses their hacking skills for destructive purposes?
    A. Cracker
    B. Ethical hacker
    C. Script kiddie
    D. White-hat hacker

16. MAC address spoofing is which type of attack?
    A. Encryption
    B. Brute-force
    C. Authentication
    D. Social engineering

17. Which law gives authority to intercept voice communications in computer hacking attempts?
    A. Patriot Act
    B. Telecommunications Act
    C. Privacy Act
    D. Freedom of Information Act

18. Which items should be included in an ethical hacking report? (Choose all that apply.)
    A. Testing type
    B. Vulnerabilities discovered
    C. Suggested countermeasures
    D. Router configuration information

19. Which type of person poses the most threat to an organization's security?
    - **A.** Black-hat hacker
    - **B.** Disgruntled employee
    - **C.** Script kiddie
    - **D.** Gray-hat hacker
20. Which of the following should be included in an ethical hacking report? (Choose all that apply.)
    - **A.** Findings of the test
    - **B.** Risk analysis
    - **C.** Documentation of laws
    - **D.** Ethics disclosure

Answers to Review Questions

1. A. White-hat hackers are "good" guys who use their skills for defensive purposes.
2. C. White-box testing is a security audit performed with internal knowledge of the systems.
3. D. Reconnaissance is gathering information necessary to perform the attack.
4. D. Physical access tests access to the physical infrastructure.
5. B. As security increases, it makes it more difficult to use and less functional.
6. A. Disgruntled employees have information that can allow them to launch a powerful attack.
7. A, B, C. The three phases of a security evaluation plan are preparation, security evaluation, and conclusion.
8. B. Hacktivism is performed by individuals who claim to be hacking for a political or social cause.
9. B. Title 18 of the US Code is most commonly used to prosecute hackers.
10. A. An attack from the Internet is known as a remote attack.
11. A. The Freedom of Information Act ensures public release of many documents and records and can be a rich source of information on potential targets.
12. A, B, D. Sending spam, installing and using keystroke loggers, and implementing pop-up windows are all prohibited by the SPY ACT.
13. B. Signing an NDA agreement is critical to ensuring the testing is authorized and the ethical hacker has the right to access the client's systems.
14. D. A target of evaluation is a system, program, or network that is the subject of a security analysis. It is the target of the ethical hacker's attacks.
15. A. A cracker is a hacker who uses their hacking skills for destructive purposes.
16. C. MAC address spoofing is an authentication attack used to defeat MAC address filters.
17. A. The Patriot Act gives authority to intercept voice communications in many cases, including computer hacking.
18. A, B, C. All information about the testing process, vulnerabilities discovered in the network or system, and suggested countermeasures should be included in the ethical hacking report.
19. B. Disgruntled employees pose the biggest threat to an organization's security because of the information and access that they possess.
20. A, B. Findings of the test and risk analysis should both be included in an ethical hacking report.