Part I

The Business and Legal Issues of Ethical Hacking

CHAPTER 1

Introduction to Ethical Hacking

Because of the increased interconnection among information systems and networks, the consequences of successful attacks by malicious individuals can have far-reaching implications. In addition, numerous scripts available to unskilled individuals can be used to initiate various types of harmful attacks. The results of malicious attacks can include financial loss, loss of reputation, a drop in the value of a company's stock, and many legal issues. Ethical hacking is a defensive tool that can be applied before an attack occurs to uncover vulnerabilities in information systems and network security and provide the basis for remediation of these weaknesses. As such, the candidate for the CEH certification must be well grounded in the fundamentals of information system security.

The chapters in this text address the fundamentals of information system security; the rationale for ethical hacking; relevant technologies and terminology; the legal ramifications of ethical hacking; corresponding laws and regulations; types of attacks; and the steps involved in ethical hacking.

Terminology

The basic tenets of information system security are *confidentiality, integrity*, and *availability*, sometimes known as the CIA triad. Confidentiality ensures that the

information is not disclosed to unauthorized persons or processes. Integrity is achieved by accomplishing the following three goals:

1. Preventing the modification of information by unauthorized users
2. Preventing the unauthorized or unintentional modification of information by authorized users
3. Preserving internal and external consistency:
   a. Internal consistency refers to a logical connection among data in the system. For example, assume that an internal database holds the number of units of a particular item in each department of an organization. The sum of the number of units in each department should equal the total number of units that the database has recorded internally for the whole organization.
   b. External consistency refers to a logical connection among objects in the real world and their representations in the system. Using the example previously discussed in (a), external consistency means that the number of items recorded in the database for each department is equal to the number of items that physically exist in that department.

Availability ensures that a system's authorized users have timely and uninterrupted access to the information in the system.

Additional factors that support information system security are:

Authenticity. The confirmation of the origin and identity of an information source

Identification. A user claiming an identity to an information system

Authentication. The confirmation and reconciliation of evidence of a user's identity

Accountability. Assigning responsibility for a user's actions

Privacy. Protection of individually identifiable information

Organizational Security Policy. A high-level statement of management intent regarding the control of access to information and the personnel authorized to receive that information

When viewing an information system through the eyes of an ethical hacker, system threats, vulnerabilities, risks, attacks, targets of evaluation, and exploits have to be taken into account. The formal definitions of these terms are given as follows:

Threat. An event or activity that has the potential to cause harm to the information systems or networks

Vulnerability. A weakness or lack of a safeguard that can be exploited by a threat, causing harm to the information systems or networks; can exist in hardware, operating systems, firmware, applications, and configuration files

Risk. The potential for harm or loss to an information system or network; the probability that a threat will materialize

Attack. An action against an information system or network that attempts to violate the system security policy; usually the result of a threat realized

Target of Evaluation. An IT product, element, or system designated to have a security evaluation

Exploit. A means of exploiting a weakness or vulnerability in an IT system to violate the system's security

Hackers, Crackers, and Other Related Terms

Originally, the term hacker did not have negative connotations. A *hacker* was a computer person who was intellectually curious and wanted to learn as much as possible about computer systems. A person who was "hacking" was developing and improving software to increase the performance of computing systems.

A *cracker* was an individual using his or her capabilities for harmful purposes against computer systems.

Over time, the terms hacker and cracker both took on the definition of an individual who used offensive skills to attack computer systems. Therefore, an *ethical hacker* is security professional who uses his or her computing capabilities for defensive purposes and to increase the security posture of information systems.

A *phreaker* is a hacker who focuses on communication systems to steal calling card numbers, make free phone calls, attack PBXs, and acquire access, illegally, to communication devices. A *whacker* is a novice hacker who attacks Wide Area Networks (WANs) and wireless networks. A *script/kiddie* is usually a young individual without programming skills who uses attack software that is freely available on the Internet and from other sources. The *cyber-terrorist* is an individual who works for a government or terrorist group that is engaged in sabotage, espionage, financial theft, and attacks on a nation's critical infrastructure.

Hactivism

Hackers and crackers have a variety of motivations and justifications for their activities. Some of these individuals believe that information should be free and they are doing their part in this cause. Hackers who conduct their activities for

a cause are said to be practicing *hactivism*. Thus, their targets are any organizations that they perceive are behind social injustice. They attack government organizations and agencies, international economic organizations, and any other entities that they define as being responsible for social and economic inequities. Through their hactivism, they gain publicity for their cause and for themselves to help build their reputation. No matter what the justification, breaking into computers and networks is illegal.

Threats

Threats from hackers can take on a variety of forms. The relevant threats are summarized in Table 1-1.

Table 1-1: Example Threats

THREAT	DESCRIPTION
Information Warfare	Computer-related attacks for military or economic purposes
Cyber Terrorism	Attacks against a nation's critical infrastructure such as power plants, chemical plants, refineries, economic centers, transportation systems, and so on
Criminal	Theft, fraud, physical damage
Violation of Data Integrity	Theft of data, modification of data, loss of data
Late or Delayed Processing	Delays in processing that lead to reduced income, penalties, or additional expenses
Acquiring High Sensitivity Data	Using inference, data aggregation, or other methods to acquire data of higher sensitivity than allowed to the normal user
Malware	Viruses, Trojan horses, worms, and other software that cause harm to information systems
Denial or Interruption of Service	Denial of service or distributed denial of service attacks that saturate an information system's resources so that important processing tasks are delayed or cannot be done
Personnel-Related	Unauthorized access to personnel records or attacks by disgruntled employees
Environmental	Failures and damage caused by environmental issues, such as temperature, power failures, fire, flood, and so on caused naturally or by intervention from an attacker

Hacking History

Hacking began in the 1960s at MIT when students attempted to learn more about mainframe computing systems and improve their skills. The telephone systems were tempting to phreakers, and one John Draper, known as Captain Crunch, used a whistle packaged in Captain Crunch cereal to generate a 2600 Hz tone that allowed access to the AT&T long distance network. This discovery led to Draper and others designing and building a so called "blue box" that generated the 2600 Hz signal and other tones for use in making long distance phone calls without paying. Steve Jobs and Steve Wozniak, who later founded Apple Computer, were also makers of blue boxes.

In the 1980s, hackers began to share information and stolen passwords on electronic computer bulletin boards such as "Sherwood Forest." Hacking clubs began to form with names like the German "Chaos Computer Club."

In 1982, teenagers in Wisconsin (area code 414), known as the 414 Gang, launched attacks into the Sloan-Kettering Cancer Hospital's medical records systems. Two years later, the hacker magazine *2600* made its debut under editor Eric Corley, aka "Emmanuel Goldstein." In November 1988, the Morris Internet Worm spread through the Internet and resulted in a large scale Denial of Service (DoS). The cause of this disruption was a small program written by Robert Tappan Morris, a 23-year-old doctoral student at Cornell University. The worm infected approximately 6,000 networked computers.

In 1986, attacks were launched against U.S. classified computer systems by Germans affiliated with the Chaos Computer Club and working for the KGB. This drama is described in the book *The Cuckoo's Egg*, written by Clifford Stoll (Clifford Stoll, *The Cuckoo's Egg*, Doubleday, copyright 1989; ISBN 0-385-24946-2). Stoll uncovered this activity after he noticed a 75-cent error in a computer account at the Lawrence Livermore Laboratories.

In 1990, a hacker named Kevin Poulson, with some associates, hacked a radio station's phone system to ensure they won a call-in contest for Porsches and other prizes. Poulson, who was also wanted for phreaking, was apprehended and sentenced to five years in prison. He was released in 1996.

The first hacking conference, called Def Con, was held in Las Vegas in 1993 and is still held annually.

The notorious hacker Kevin Mitnick was arrested in 1995 for, among other crimes, attacks against telephone systems. Mitnick was convicted in 1989 for computer and access device fraud but eluded police and the FBI for more than two years while he was on probation. On Christmas 1995, he broke into the computers of Tsutomu Shimomura in San Diego, California. Tsutomu tracked down Mitnick after a cross-country electronic pursuit, and he was arrested by the FBI in Raleigh, North Carolina, on February 15, 1995. Mitnick pleaded guilty to charges at his trial in March 1999, and his sentence was nearly equal

to his time served. He is now an independent information security consultant and author.

Also in 1995, Russian hacker Vladimir Leven and associates performed electronic transfers of $10 million to a number of international banks. Leven was captured and tried in the U.S. and sentenced to three years' confinement. In 1998, "The Cult of the Dead Cow" announced and released very effective Trojan horse software called Back Orifice at Def Con. Back Orifice provided remote access to Windows 98 and Windows 95 computers.

In February 2000, hackers launched Distributed DoS attacks against Yahoo!, Amazon.com, and ZDNet. Microsoft Corporation's network was hacked in October 2000 by an attacker who gained access to software under development.

Ethical Hacking Objectives and Motivations

An ethical hacker attempts to duplicate the intent and actions of malicious hackers without causing harm. Ethical hackers conduct *penetration tests* to determine what an attacker can find out about an information system, whether a hacker can gain and maintain access to the system, and whether the hacker's tracks can be successfully covered without being detected.

The ethical hacker operates with the permission and knowledge of the organization they are trying to defend and tries to find weaknesses in the information system that can be exploited. In some cases, to test the effectiveness of their information system security team, an organization will not inform their team of the ethical hacker's activities. This situation is referred to as operating in a *double blind* environment.

To operate effectively, the ethical hacker must be informed of the assets that should be protected, potential threat sources, and the extent to which the organization will support the ethical hacker's efforts.

Steps in Malicious Hacking

Hacking with malicious intent comprises the following steps, as shown in Figure 1-1:

1. Reconnaissance
   a. Active
   b. Passive

2. Scanning
3. Gaining access
   a. Operating system level
   b. Application level
   c. Network level
   d. Denial of service
4. Maintaining access
   a. Uploading programs/data
   b. Downloading programs/data
   c. Altering programs/data
5. Covering, clearing tracks, and installing back doors

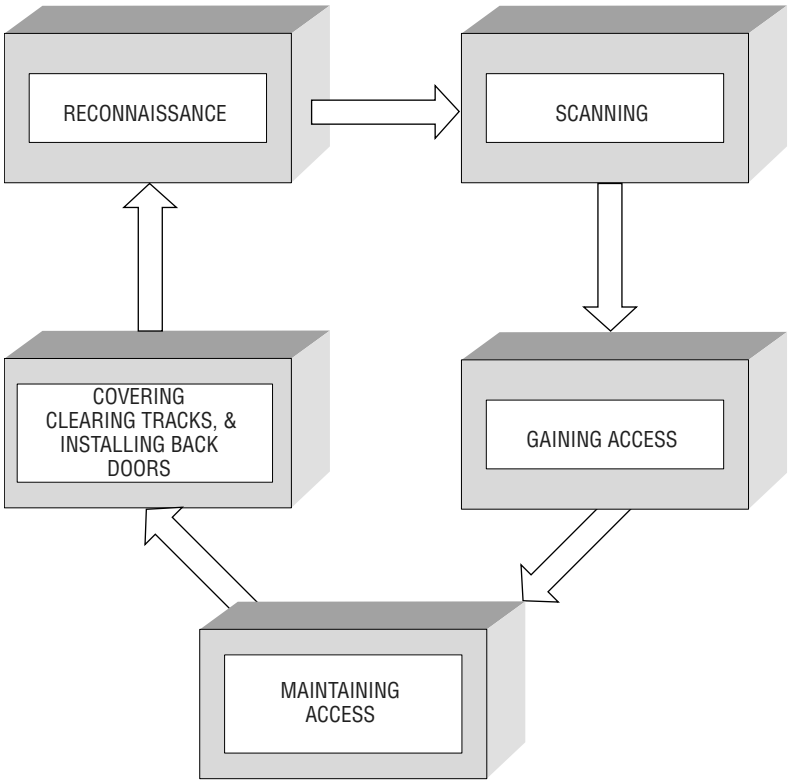

Figure 1-1: Malicious hacking steps

Reconnaissance

Reconnaissance is a preliminary activity in which an attacker attempts to gather information about a target preparatory to launching an attack. It includes scanning the network from the inside or outside without the authority to do so. In this phase, the risk to the organization is classified as "notable" because it is an early attempt to gather information about the network and information systems.

Reconnaissance can either be passive or active. Passive reconnaissance is accomplished by monitoring the network using sniffers or other mechanisms to acquire information about the network and IT systems. The hacker can also use other means, such as dumpster diving, to acquire information, which involves searching through an organization's or person's discarded material.

Conversely, active reconnaissance "probes" the network to acquire information about the operating systems being used, available services, open ports, routers, and hosts.

Scanning

Scanning is the activity that precedes the actual attack and involves acquiring more detailed information based on the data obtained during the reconnaissance phase. Some of the tools used in the scanning phase include vulnerability scanners, ports scanners, and war dialers. Using these tools, the hacker might be able to acquire information concerning users' accounts, possible entry points, and possible security mechanisms such as intrusion detection systems. They can also monitor registry entries in operating systems to determine whether particular patches have been installed. Obtaining this information is sometimes known as *enumeration*.

Examples of security scanning tools are *Nmap* and *Nessus*. Nmap can be used to identify network computers and operating systems, enumerate open ports on potential target computers, determine applications and versions running on potential target computers, and determine the general security posture of a network.

The Nessus security scanner provides the capability to detect local flaws, uninstalled patches, and weaknesses in network hosts. Nessus maintains a database of recent security vulnerabilities updated on a daily basis.

The risk to the organization or business is considered "high" in the scanning phase because it enables access to the network and consequential harmful activities. The risk can be reduced by turning off all applications and ports that are not needed on the network computers. This practice is called *deny all*.

Acquiring Access

The Acquiring Access phase is where the actual attack is implemented; therefore, the business risk is designated at the "highest" level. During this phase, the attacker accesses the operating system and network and can launch denial of service attacks, buffer overflow attacks, and application-based attacks. In addition, the attacker can insert viruses and Trojan horses and can engage in other types of malicious behavior.

Another goal of the attacker in the Acquiring Access phase is to obtain system privileges not normally available to the conventional user. With these *elevated or escalated privileges*, a hacker can execute commands and access parts of the systems and networks reserved for individuals such as system administrators.

Maintaining Access

Once the hacker has acquired access to the network and associated computers, he or she wants to maintain that access. Typical activities involved in maintaining access include downloading password files that can be used to reenter the system at a later time, installing software such as Trojan horses and Rootkits, and installing sniffers to monitor user keystrokes. A *Trojan horse* is code hidden as part of a legitimate and useful program. When the legitimate program is executed, the Trojan horse software will run, unbeknownst to the user, and can implement malicious behavior. A *Rootkit* is software that provides an attacker with the ability to access a host or network but is designed to avoid detection.

To maintain "ownership" of the compromised system, an attacker might repair the vulnerability that allowed him or her to gain access to the networks and hosts in the first place, in order to prevent other hackers from successfully attacking the same IT elements.

Covering, Clearing Tracks, and Installing Back Doors

It is in the best interest of the attacker to make sure that no one is aware of his or her unauthorized malicious activities on the computer systems. Again, Rootkits are effective in covering these tracks. In addition, a hacker might delete or modify log files to mask harmful or unusual events. Because a malicious intruder might install programs to monitor or manipulate data, these programs have to be hidden from view in the computer system. Some mechanisms that can be used to hide these programs and files and for clearing tracks include hidden directories, hidden attributes, tunneling, steganography, and Alternate Data Streams (ADS).

ADS is a compatibility feature of the Windows NT File System (NTFS) that provides the ability to fork file data into existing files without modifying characteristics such as the file's size or function. This feature provides a means of concealing Rootkits and other malicious code, which can be executed in a hidden manner.

Hacker and Ethical Hacker Characteristics and Operations

Hackers can be categorized into the three general classes of black hats, gray hats, and white hats. A *black hat* hacker or cracker has the necessary computing expertise to carry out harmful attacks on information systems. A *gray hat* is a hacker with a split personality. At times, this individual will not break the law and, in fact, might help to defend a network. At other times, the gray hat hacker reverts to black hat activities. The *white hat* individual usually has exceptional computer skills and uses his or her abilities to increase the security posture of information systems and defend them from malicious attacks. This individual might be an information security consultant or security analyst.

Entities that perform ethical hacking functions for organizations usually fall into one of three categories: white hats, former black hats, and independent consulting organizations. The *white hat ethical hacker* has the appropriate computer skills and understanding of the black hat hacker mentality and methods. This person might be an independent consultant hired to perform ethical hacking activities. The *former black hat hacker* is, we might hope, reformed and brings actual black hat experience to his or her work. There is a concern about this individual in that you can never be certain that he or she will not revert to their former malicious activities. The third category of ethical hacker is taken by *consulting companies* that perform a variety of services for organizations including accounting, auditing, and information system security.

Skills Needed by an Ethical Hacker

An ethical hacker must have a variety of in-depth computer skills to conduct business successfully. Because not everyone can be an expert in all the required fields, ethical hacking might be conducted by teams whose members' skills complement each other.

Organizations have a variety of computer systems that have to probed, so the team must have expertise in a variety of operating systems such as UNIX, Windows, Linux, and Macintosh. They must also be familiar with the different

hardware platforms and networks that they might encounter, as well as be knowledgeable in the fundamental principles of information system security. Figure 1-2 summarizes these and additional ethical hacker required knowledge areas.

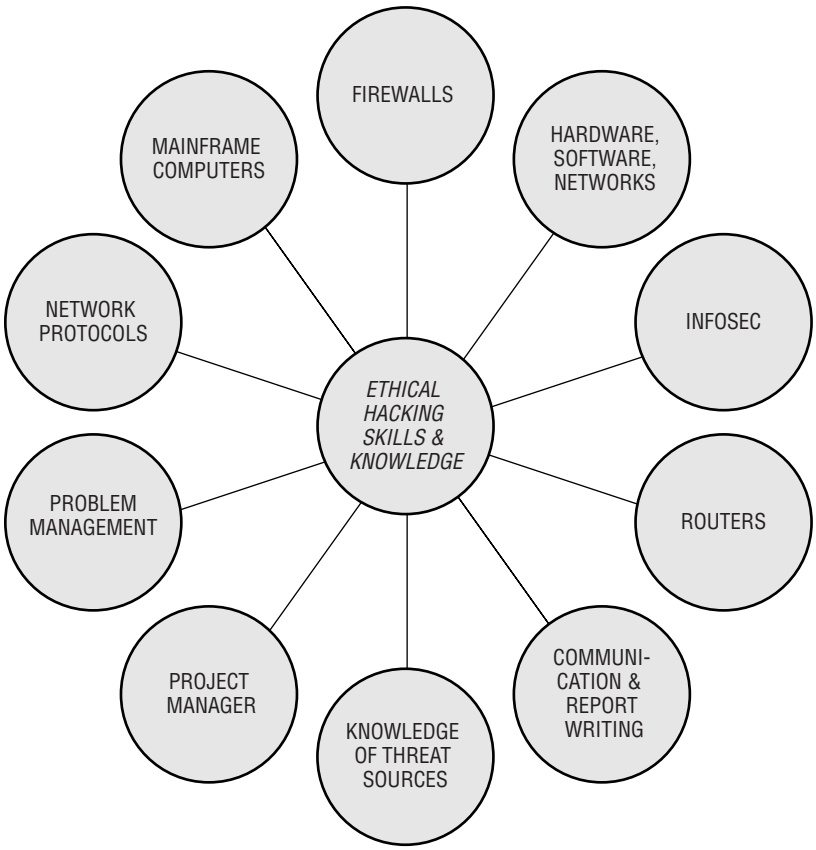

Figure 1-2: Required ethical hacker skills

Steps in an Infosec Evaluation

The ethical hacking project comprises three phases, summarized as follows:

1. Preparation: Contract terms are agreed upon, and a contract is signed detailing the work to performed, schedules, deliverables, and resources to be provided to the ethical hacking team. The contract should also protect the team against prosecution for their activities and should contain a nondisclosure agreement.

2. Conduct: The ethical hacking activities are conducted, vulnerabilities are identified, and a technical report is generated.
3. Conclusion: The results of the ethical hacking effort are communicated to the sponsoring organization, along with remediation recommendations. The recommendations are then usually acted upon by the organization.

Types of Information System Security Testing

An ethical hacker will explore all the available avenues of gaining access to an organization's network and information systems. For example, an ethical hacker will dial into an organization's telephone exchange and try to locate an open modem that will provide access. Another approach is to attempt to access an organization's network directly through a local area connection used by employees. A third method is to gain access remotely through the Internet. An additional valuable resource for an ethical hacker would be to obtain an employee's laptop and use it to enter an organization's network and access computer resources. Wireless networks in organizations provide opportunities for creative ethical hackers to get into an organization's network. Social engineering also provides the ethical hacker with an opportunity to gain information from unsuspecting employees. Finally, as a complement to all these methods, an ethical hacker can physically access computer hardware and software resources.

In summary, these methods of ethical hacking are:

- Dial-up network connection
- Insider local network connection
- Remote outsider network connection
- Stolen equipment connection
- Wireless network connection
- Social engineering–enabled connection
- Physical entry attack

Evaluation of an information system by an ethical hacker can also be categorized by the amount of knowledge and information provided to the ethical hacking team a priori. These categories of security testing are summarized as follows:

Full knowledge (Whitebox) test. The team has as much knowledge as possible about the network and computing resources to be evaluated.

Partial knowledge (Graybox) test. The testing team has knowledge that might be relevant to a specific type of attack by a person internal to the organization. It determines what areas and resources that might be accessed and available to an insider.

Zero knowledge (Blackbox) test. The testing team is provided with no information and begins the testing by gathering information on its own initiative. This type of test simulates attacks perpetrated by outsiders. Because the ethical hacking team has to begin from scratch to gather knowledge about the target information system, this type of test usually takes longer to execute and, consequently, costs more to implement.

The Institute for Security and Open Methodologies (`www.isecom.org/`) has developed an Open Source Security Testing Methodology Manual (OSSTMM) (`www.osstmm.org`) that provides guidance and metrics for conducting security tests. It has test cases that "are divided into five channels (sections) which collectively test: information and data controls, personnel security awareness levels, fraud and social engineering control levels, computer and telecommunications networks, wireless devices, mobile devices, physical security access controls, security processes, and physical locations such as buildings, perimeters, and military bases." The manual is applicable to ethical hacking, penetration tests, vulnerability, and other types of security assessments.

Ethical Hacking Outputs

Up to this point, we have described the required ethical hacker skills and ethical hacking approaches and methods. To complete the process, the ethical hacker should define the output of his or her efforts. The primary output is a report that provides a background of the project, a detailed description of the work accomplished as the result of ethical hacking, and corresponding remediation recommendations.

The report should provide a description of the ethical hacking efforts and results and compare them to the schedule agreed upon at the beginning of the project. The results include vulnerabilities and remediation recommendations treated as sensitive information and delivered to the sponsor in a secure manner. Both sides should be party to a nondisclosure agreement.

Protections and Obligations for the Ethical Hacker

When an ethical hacker agrees to conduct penetration tests for an organization and probe the weaknesses of their information systems, he or she can be open

to dismissal and prosecution unless contract terms are included to protect the individuals conducting the test. It is vitally important that the organization and ethical hacking team have an identical understanding of what the team is authorized to do and what happens if the team inadvertently causes some damage.

For his or her own protection, the ethical hacker should keep the following items in mind:

Protect information uncovered during the penetration test. In the course of gaining access to an organization's networks and computing resources, the ethical hacker will find that he or she has access to sensitive information that would be valuable to the organization's competitors or enemies. Therefore, this information should be protected to the highest degree possible and not divulged to anyone, either purposely or inadvertently.

Conduct business in an ethical manner. Ethics is a relative term and is a function of a number of variables, including background, religion, ethnicity, upbringing, and so on. However, the ethical hacker should conduct his or activities in an ethical fashion and in the best interest of the organization that commissioned the penetration testing. Similarly, the organization should treat the ethical hacker with the same respect and ethical conduct.

Limitation of liability. As discussed earlier in this section, during a penetration test, the ethical hacking team will most likely have access to sensitive files and information. The ethical hacker is trained not to cause any harm, such as modifying files, deleting information, and so on, in the course of his or her activities. But, since errors do occur, the organization and ethical hacker should have terms in the contract that address the situation where harm is done inadvertently. There should be a limitation to the liability of the ethical hacker if this scenario occurs. Another option commonly used by consultants is to obtain an insurance policy that will cover the consultant's activities in his or her chosen profession.

Remain with the scope of the assignment. The scope of the penetration testing should be delineated beforehand and agreed upon by all parties involved. With that accomplished, the testing team should conduct the testing strictly within those bounds. For example, only the networks and computing resources specified should come under penetration testing as well as the methods and extent of trying to "break in" to the information system.

Develop a testing plan. As with any endeavor, the ethical hacking team should develop a test plan in advance of the testing and have it approved by the hiring organization. The plan should include the scope of the test, resources to be tested, support provided by the hiring organization, times for the testing, location of the testing, the type of testing (Whitebox, Graybox, or Blackbox), extent of the penetration, individuals to contact in the event of problems, and deliverables.

Comply with relevant laws and regulations. Business organizations are required to comply with a variety of laws and regulations, including the Health Insurance Portability and Accountability Act (HIPAA), Sarbanes-Oxley, and the Gramm-Leach-Bliley Act (GLBA). These acts are one of the reasons that companies hire ethical hackers and demonstrate that they are acting to protect their information resources. Penetration testers also have to make sure that they comply with the appropriate laws.

Related Types of Computer Crime

A variety of hacking attacks are considered computer crimes. In the U.S., a large number of statutes have been generated to deal aggressively with hackers who maliciously and without authorization penetrate computer systems. In general, computer crimes fall into three categories: crimes committed against the computer, crimes using the computer, and crimes in which the computer is incidental. The following is a general listing of the most prominent types of computer crimes related to hacking:

Theft of passwords. Illegally acquiring a password to gain unauthorized access to an information system

Social engineering. Using social skills to obtain information, such as passwords or PIN numbers, to be used in an attack against computer-based systems

Denial of Service (DoS) and Distributed Denial of Service. Overwhelming a system's resources so that it is unable to provide the required services; in the distributed mode, messages to a target computer can be launched from large numbers of hosts where software has been planted to become active at a particular time or upon receiving a particular command

Network intrusions. Malicious, unauthorized penetration into information systems

Fraud. Using computers or the Internet to commit crimes (for example, by not delivering goods paid for by a customer)

Software piracy. Illegal copying and use of software

Dumpster diving. Obtaining information that has been discarded as garbage in dumpsters or at recycling locations

Malicious code. Programs (such as viruses, Trojan horses, and worms) that, when activated, cause harm to information systems

Spoofing of IP addresses. Inserting a false IP address into a message to disguise the original location of the message or to impersonate an authorized source

Embezzlement. Illegally acquiring funds, usually through the manipulation and falsification of financial statements

Data-diddling. The modification of data

Information warfare. Attacking the information infrastructure of a nation — including military/government networks, communication systems, power grids, and the financial community — to gain military and/or economic advantages

Masquerading. Pretending to be someone else, usually to gain higher access privileges to information that is resident on networked systems

Use of readily available attack scripts on the Internet. Scripts that have been developed by others and are readily available through the Internet, which can be employed by unskilled individuals to launch attacks on networks and computing resources

A problem with prosecuting hackers that have violated the law is that many jurisdictions around the world have different and inconsistent laws relating to computer crime. For example, a hacker might be launching attacks against U.S. government agencies from Russia.

Some of the international organizations addressing computer crime are the United Nations, Interpol, the European Union, and the G8 leading industrial nations.

Because of the high rate of development of new technologies, laws usually lag behind. In order to address computer crime, law enforcement can use traditional laws against embezzlement, fraud, DoS, and wiretapping to prosecute computer criminals.

Assessment Questions

You can find the answers to the following questions in Appendix A.

1. The goals of integrity do *not* include:
   a. Accountability of responsible individuals
   b. Preventing the modification of information by unauthorized users
   c. Preventing the unauthorized or unintentional modification of information by authorized users
   d. Preserving internal and external consistency
2. Which of the following items is *not* a description of the best way to apply ethical hacking as a defensive tool?
   a. Before an attack
   b. To uncover vulnerabilities
   c. To provide a basis for remediation
   d. After an attack to evaluate damage
3. The fundamental tenets of information security are:
   a. Confidentiality, integrity, and availability
   b. Confidentiality, integrity, and assessment
   c. Integrity, authorization, and availability
   d. Security, integrity, and confidentiality
4. Which one of the following best describes authentication?
   a. A user claiming an identity to an information system
   b. The confirmation and reconciliation of evidence of a user's identity
   c. Assigning responsibility for a user's actions
   d. The confirmation of the origin and identity of an information source
5. Which one of the following best describes a threat?
   a. A weakness or lack of a safeguard that can be exploited, causing harm to the information systems or networks
   b. The potential for harm or loss to an information system or network
   c. An action against an information system or network that attempts to violate the system security policy
   d. An event or activity that has the potential to cause harm to the information systems or networks

6. Which of the following is the best definition of a hacker?
   a. Initially, a person who was intellectually curious about computer systems and then took on the definition of a person who uses offensive skills to attack computer systems
   b. A person who uses computer skills to defend networks
   c. A person with computer skills who intends to do no harm
   d. A person who uses computer skills to play games
7. A phreaker is which one of the following?
   a. A young individual without programming skills who uses attack software that is freely available on the Internet and from other sources
   b. A novice hacker that attacks WANs and wireless networks
   c. A hacker that focuses on communication systems to steal calling card numbers and attack PBXs
   d. An individual who works for a government or terrorist group that is engaged in sabotage, espionage, financial theft, and attacks on a nation's critical infrastructure
8. An IT product, element, or system designated to have a security evaluation is called which one of the following:
   a. Evaluation object
   b. Evaluation system
   c. Target element
   d. Target of evaluation
9. Hackers who conduct their activities for a cause are said to be practicing:
   a. Causation
   b. Hactivism
   c. Protesting
   d. Hacking conscience
10. Which one of the following *best* describes information warfare?
    a. Theft, fraud, physical damage
    b. Delays in processing that lead to reduced income, penalties, or additional expenses
    c. Computer-related attacks for military or economic purposes
    d. Theft of data, modification of data, loss of data

11. A device that generates a 2600 Hz tone to make long distance calls without paying is called a:
    a. Blue box
    b. Tone box
    c. Green box
    d. Phone box
12. In 1988, which one of the following malware items spread through the Internet and caused a large DoS attack?
    a. Love bug
    b. Morris worm
    c. Slammer worm
    d. Klez worm
13. The annual hacking conference, which originated in Las Vegas in 1993, is called:
    a. Hack Con
    b. Pen Con
    c. Mal Con
    d. Def Con
14. Back Orifice is:
    a. A worm
    b. A word processor
    c. Trojan horse software
    d. Scanning software
15. Which one of the following items does *not* describe an ethical hacker?
    a. Attempts to duplicate the intent and actions of black hat hackers without causing harm
    b. An individual who uses his or her capabilities for harmful purposes against computer systems
    c. Conducts penetration tests to determine what an attacker can find out about an information system during the reconnaissance and scanning phases
    d. Operates with the permission and knowledge of the organization they are trying to defend

16. If an ethical hacking team does not inform an organization's information security personnel that they are conducting ethical hacking on the organization's information systems, this situation is called:
    a. A double blind environment
    b. A zero knowledge environment
    c. A gray environment
    d. A black environment
17. To operate effectively, the ethical hacker must be:
    a. Informed of the assets to be protected
    b. Informed of potential threat sources
    c. Informed of the support that the organization will provide
    d. All of the above
18. The steps in malicious hacking are:
    a. Reconnaissance; scanning; gaining access; maintaining access; covering, clearing tracks, and installing back doors
    b. Reconnaissance; preparation; gaining access; maintaining access; covering, clearing tracks, and installing back doors
    c. Reconnaissance; scanning; gaining access; disengaging; covering, clearing tracks, and installing back doors
    d. Reconnaissance; scanning; gaining access; maintaining access; malicious activity
19. In hacking, the two types of reconnaissance are:
    a. Active and invasive
    b. Preliminary and invasive
    c. Active and passive
    d. Preliminary and active
20. In the "gaining access" phase of malicious hacking, which one of the following is *not* a level that is a target for access?
    a. Layered level
    b. Operating system level
    c. Application level
    d. Network level
21. Uploading programs/data, downloading programs/data, and altering programs/data are activities of which phase of malicious hacking?
    a. Disengaging

b. Reconnaissance
c. Gaining access
d. Maintaining access

22. Dumpster diving is usually performed in what phase of malicious hacking?
    a. Gaining access
    b. Reconnaissance
    c. Maintaining access
    d. Preparation
23. Nmap and Nessus are examples of:
    a. Security scanning tools
    b. Viruses
    c. Worms
    d. Virus removers
24. The high risk in the scanning phase of malicious hacking can be reduced by turning off all applications and ports that are not needed on the network computers. This practice is called:
    a. Close ports
    b. System secure
    c. Deny all
    d. Black operation
25. Which one of the following is *not* a typical goal of a hacker in the "acquiring access" phase of malicious hacking?
    a. Access the operating system
    b. Launch buffer overflow attacks
    c. Obtain elevated or escalated privileges
    d. Installing Rootkits and sniffers
26. In which phase of malicious hacking would the hacker delete or modify log files to hide any malicious events?
    a. Reconnaissance
    b. Covering, clearing tracks, and installing back doors
    c. Gaining access
    d. Maintaining access

27. A compatibility feature of the Windows NT File System (NTFS) that can be used in the "covering, clearing tracks, and installing back doors" phase of malicious hacking to conceal malicious code is called:
    a. Alternate Clearing of Data (ACD)
    b. Alternate Data Streams (ADS)
    c. NT Compatibility (NTC)
    d. Alternate Data Hiding (ADH)
28. A hacker that has the necessary computing expertise to carry out harmful attacks on information systems is called a:
    a. Gray hat hacker
    b. White hat hacker
    c. Black hat hacker
    d. Blue hat hacker
29. When an organization hires an entity to conduct an ethical hacking project, the people they hire usually fall into one of three categories. Which one of the following is *not* one of those categories?
    a. Black hat hacker
    b. White hat ethical hacker
    c. Former black hat hacker
    d. Consulting organization
30. What are the three general phases of an ethical hacking project?
    a. Preparation, evaluation, conclusion
    b. Preparation, conduct, and conclusion
    c. Study, conduct, and conclusion
    d. Study, preparation, evaluation
31. What are the three categories of information system evaluation by an ethical hacker that are based on the amount of knowledge provided?
    a. Full knowledge (Whitebox), partial knowledge (Graybox), zero knowledge (Blackbox)
    b. Full knowledge (Whitebox), partial knowledge (Graybox), moderate knowledge (Bluebox)
    c. Complete knowledge (Openbox), partial knowledge (Graybox), moderate knowledge (Bluebox)
    d. Full knowledge (Whitebox), masked knowledge (Bluebox), zero knowledge (Blackbox)