


# chapter 10

## Security Testing

**After reading this chapter and completing the exercises, you will be able to:**

- Provide an overview of security testing fundamentals
- Identify the difference between security testing and security auditing
- Describe the methodology used to perform a security test
- Define common techniques that intruders use to gather information
- Describe common methods used to gain unauthorized access into a system
- Identify common strategies used to escalate one's privileges in a system



## Security In Your World

Erin and Jeff have been dating for several years. Erin is a network engineer who runs her own consulting firm out of the home, while Jeff is a business entrepreneur who develops custom database applications on the side to make ends meet. They both had their own separate clientele, but they occasionally referred clients to one another to increase their businesses and better support their customers' needs. Living together side by side, they worked for several years without combining the two businesses for fear of the personal conflict that might result from sharing a business.

Over time, Jeff and Erin's personal relationship deteriorated and they agreed on a trial separation. Jeff moved into a leased space temporarily, hoping for some type of near-future reconciliation, while Erin remained at their previously shared home. After a few months apart, Jeff received a call from one of his customers inquiring about a message that Erin had left with their answering service. It seems that Erin had been in contact with many of Jeff's clients in hopes of promoting an expansion of his business that included custom application development. Furious and taken aback, Jeff realizes that he must immediately take steps to protect his company and the data within it. Not only does Erin have the passwords to his main business accounts, but she was also an integral player in the initial construction of his company's security architecture.

Aware of Erin's level of expertise, Jeff calls a security professional for support in the rebuilding of his company's security architecture. Sparing no cost, the two of them completely replace the existing architecture, changing both the physical and logical environment in hopes of thwarting any attempts that Erin may make at obtaining more information. Excessive measures were taken to secure the network. Confident in his efforts as well as in the security professional whom he hired, Jeff was excited about the end results.

A few weeks had passed when Jeff's security alerts suggested that an unauthorized intruder had obtained remote access to the environment. To his dismay, and despite all of his efforts, it appeared that Erin had found her way back into his network. Further exploration discovered that documents had been destroyed and customers had been removed from the database. Forced to inform his customers of the recent intrusion, many began to search elsewhere for application development needs. Jeff's future was jeopardized due to this incident.

So where did Jeff go wrong? Regardless of the level of security that Jeff had put into place, he did not schedule resources for security penetration testing. Confident that his excessive measures of security would prevent any intrusions (a common

*(continued)*



misconception), and being aware of the enormous time and cost associated with the security testing process, he did not find it necessary.

The amount and level of security put into place is irrelevant if penetration testing is not conducted at the end of implementation. In the end, penetration testing should be the final confirmation that an environment is reasonably secure. The strength of security offered to a network can be measured by its weakest component, so identification of a weakness is vital within all architectures. This chapter explores the process of security and penetration testing and provides models from which security testing plans can be developed. Time and resources will be considered as well.

## Security Testing

There is much confusion and conflicting data regarding the distinction between security auditing and security testing. **Security testing** refers to the process of identifying the feasibility and impact of an attack or intrusion of a system by simulating active exploitation and executing potential attacks within that environment. It offers a way to actively evaluate the security measures implemented within an environment in terms of strength and loss potential by focusing primarily on the actual security measures implemented (e.g., hardware, software). It is conducted from an attacker's perspective and is typically outsourced to a third-party organization or application developed specifically for testing weaknesses of a system.

Security audits, on the other hand, are conducted to locate potential weaknesses found within the company's internal controls. Security audits are different from security testing in that they include areas such as security policies, human resource information, and legal or standards compliance, areas security testing does not cover. Auditing compares the documentation with the architecture to ensure accuracy and reliability of an environment, whereas security testing measures the strength and effectiveness of the environment. Auditing also requires a great deal of knowledge about the infrastructure to be completed, whereas security testing can be conducted with no prior knowledge at all.

Although both security auditing and security testing are laborious and resource intensive, penetration testing is more costly and time consuming. Therefore, security tests are better suited for evaluating the security on a small group of assets, such as when broken down departmentally. They become too impractical if the goal is to test an entire architecture complete with hundreds of systems; when compared with audits, given this scenario, they provide less information at a much higher cost. Security testing provides a more accurate picture of the strength of architecture, but because of lack of resources, testing is often conducted with a very narrow scope defined.

Characteristics required for a security tester are very similar to those needed for a security auditor. The main difference is that a security tester must have the ability to think and act like a potential intruder. Often, security testing focuses on a specific well-known attack (e.g., spoofing an account) and lacks a strong understanding of the steps that an attacker might take to achieve a goal, which makes effective testing virtually impossible. Effective

security testers understand how attackers think and behave. They are armed with a toolbox full of ideas for ways to break a system, and they are creative in their attack attempts.



It is important to point out that auditing is no more effective than security testing, just as security testing is no more effective than auditing. An effective security strategy includes both auditing and testing, but these are only two of the several components that should exist in the process of securing an environment.

## Security Testing Classification

As mentioned earlier, you must understand the behavior and mind-set of a potential attacker to effectively test the security of a network. Therefore, successful security testing in a database environment is conducted from the attacker's perspective and is categorized in terms of the viewpoint from which it is conducted. We most often think of an attacker as an external force whose primary goal is to break into a network or a database environment, but, as mentioned earlier in the book, intruders can exist internally as well. Internal users are just as dangerous, if not more dangerous, than those unauthorized external ones. Therefore, to be successful, testing that is conducted from the attacker's perspective must include both internal and external vantage points. The following list identifies the different perspectives from which security testing within a database environment can be conducted:

- **Internal testing**—Internal testing is conducted within the organization's security border. This type of testing will display vulnerabilities that exist among internal users such as employees and contractors. Testing will identify attacks and the damage that can be caused within the database environment itself. A task conducted during an internal security assessment might include an evaluator who logs in to a user's computer in an attempt to extend his or her privileges on a particular database system.
- **External testing**—External testing is conducted outside the organization's network security border. This type of testing will display attacks and liabilities that can be exploited externally from competitors, remote users, and hackers. Initial tasks most commonly completed during external testing outside a database environment primarily involve information gathering—because an intruder must gain information about an infrastructure to break into it. A security consultant who attempts to use SQL injections to gather information about an environment using external Web forms and Web applications is an example of someone conducting external security tests within a database environment.
- **Black box testing**—Black box testing is conducted with no prior knowledge of the system or infrastructure that is being tested. This testing is most often conducted externally because external intruders do not typically have prior knowledge of the existing infrastructure. Black box testing can also be seen as a type of exploratory testing. There is not one specific focus and not all systems will be tested. A black box test often weighs heavily on gathering information because the ability to gather information is what provides external intruders a way into the system. Because of this, the test identifies the most fundamental weaknesses of an infrastructure. Overall, this test will determine just how far external users can get into the system without



prior knowledge. SQL injections, more specifically, blind loop statements used in SQL injections, are most often used to obtain information through black box testing.

- **White box testing**—White box testing (target testing) is conducted by an intruder who already has existing information about the system or the infrastructure. It is also known as *targeted testing* because prior knowledge exists and known weaknesses within the infrastructure allow intruders to focus on specific areas of the infrastructure. The goal is to assess the damage that can be done by those users who understand the infrastructure they are attempting to intrude; the results will provide a more comprehensive, thorough picture of specific system weakness than that found in black box testing. White box testing is most often associated with internal testing. The assumption is that internal users will most likely have some knowledge of the infrastructure, yet white box testing can be conducted internally or externally. Consider the external intruder who obtains information by using blind SQL injections. This intruder has obtained information about the system and can now target an individual database, or table within a database, based on the information he or she has obtained. Another example of someone who might have information about a database system and might attempt to intrude is a disgruntled former employee. These individuals have information about the environment from their work history and can use this information to aid their efforts to access a system.

One last note to consider about the different categories of testing is the skill sets required to conduct each type of test. External and black box testing require assessors who hold a more broad and diverse range of skills. The tester must have a great amount of knowledge of the different network and security technologies to defeat them and gain access. The tester also needs to be flexible and creative in his or her attempts because the possibilities and potential for different types and combinations of security measures are endless. Although a tester should be experienced and flexible, internal or white box testing can be conducted by someone with less expertise because these testers have more knowledge and awareness of the environment that they are trying to intrude.

10

## The Goal of Security Testing

The general goal of a security assessment within any environment is to test the strength of security measures put into place. A security assessment can be conducted to test database security measures both broad and narrow. It can be used to test an intruder's potential for breaking into the environment or to test the appropriateness of the privilege assignment within a particular database. Therefore, the goals of a security test vary and depend on both the type of test conducted (e.g., black box, external, white box, internal) as well as the scale for which the testing takes place. For example, external black box tests are often not focused on one particular area of the network because little is known about the environment, so the goal of these tests is typically to determine how deeply an intruder can obtain access. In contrast, internal or white box testing involves a specific target within the database environment, so the goals are likely to be further defined. A security tester may assess the security measure's ability to block intruders from obtaining administrative rights to a mission-critical database.

Other common testing goals within a database environment include the ability to block access to the physical location of the database; retrieve stored, confidential information; use SQL injection to exploit; escalate privileges within the database; deny users access to their tables and records; destroy applications or files; and evade an intrusion-detection system.

## Testing Methodology

The security testing process, even in its narrowest form, can be a painstakingly time- and resource-intensive process. An unstructured approach to security testing is very ineffective and can result in wasted resources. Knowing this, even attackers do not conduct their attacks in a haphazard fashion. Having a clearly defined, well-thought-out standardized testing methodology allows an assessor to do the following:

- Address resource constraints through prioritization.
- Decrease the time required for an assessment by avoiding redundancy.
- Create an improved picture of security strength using enforced consistent testing.
- Communicate recommendations more efficiently by utilizing standardized reports.

Therefore, a structured and methodical approach is greatly beneficial to any organization. This section identifies a methodical strategy to security assessment and penetration testing using a phased approach.

### Planning and Preparation Phase

In this phase of the security assessment methodology, the assessor defines a scope, gathers information about potential weak areas of the network, identifies potential attacks, classifies and prioritizes assets, specifies objectives and goals, and lists resources required.

**Defining the Scope** The security scope defines the perimeter of the overall security assessment, the physical and logical area included within the assessment. Areas for security testing can be defined as a group of systems or applications (e.g., database servers), a department within the organization (e.g., Finance), an attack strategy (e.g., injections), and, in some cases such as those scenarios that include white box testing, the level of access achieved (e.g., privileges escalated). This section identifies the process for developing a scope, a scope perimeter, and white box and black box scenarios.

As mentioned in the previous sections, due to the resource-intensive nature of security testing, the scope of a security assessment is often narrow in size. Therefore, in scenarios that include white-box-type assessments, defining the perimeter of the scope is a pretty straightforward process. The goal of a particular security test is the primary factor used for defining the area and tasks included within the assessment. The white-box-type assessments provide the assessor with information about the infrastructure prior to testing, so the infrastructure can be used to determine those things that should be included within the scope. For example, if the goal is to ensure that privileges cannot be escalated by unauthorized users on the database servers, then the infrastructure can be analyzed and all hardware, software, and related tasks that the assessor needs to utilize in testing would be included within the scope. All other hardware, software, and unrelated tasks would be considered out of scope.

Defining the scope in a black-box-type assessment scenario is much more difficult. Because little to no information is given to the assessor prior to the test, the perimeter cannot be defined in terms of the locations of the systems within the infrastructure unless the target system is completely isolated from the rest of the network. In these situations, scopes are often defined by analyzing the level of access achieved by the attacker necessary to achieve the goal of the assessment. Potential intrusions are analyzed prior to testing and a



determination is made as to how much information would need to be obtained to access different levels of the infrastructure and subsequently achieve the assessment goal. The scope boundary is then defined in terms of the assessor's ability to reach this specific depth within the environment. For example, consider a scenario in which an exploratory black box test is planned within an environment where the goal is to ensure that database privileges cannot be obtained by unauthorized external users. Prior to the test, no information is given, so the scope perimeter is much broader and is defined as the point at which the assessor either cannot access any more information or has obtained the escalated privileges. Having information about the infrastructure prior to testing poses a great advantage to defining the scope perimeter.

Other tasks involved in developing a scope for a security assessment include defining a contract or service-level agreement, conducting a threat assessment, scheduling an assessment, and listing the resources needed to complete the assessment.

**Gathering Information** There are two types of information gathering: that which is done prior to the assessment as a way to prioritize and identify goals and that which is done during the assessment as a way to identify information leaks within the infrastructure. Information gathering that occurs during assessment is also known as information reconnaissance and will be discussed in later sections. This section explores the information that is often acquired prior to testing. Information that should be obtained prior to the database security assessment includes the following:

- Infrastructure information found in network diagrams and database schematics
- A prioritized set of data storage server and information assets
- Weak areas of the database infrastructure, those areas lacking sufficient defense
- Areas that have the highest potential for an attack (sensitive data)
- Areas that can offer entry points for intruders
- Potential attack strategies based on infrastructure or recent and past trends of intruders

10

This information can have a big impact on the assessment. Depending on what information is obtained, this gathering process can change the original course of direction for the assessment, help to prioritize assessments, and dictate the goals of the security assessment. The list just provided is not exhaustive and the more information that you can obtain about the network and security trends, the better the results of the security assessment. Also, keep in mind that this information is only provided in a white box scenario; black box scenarios do not offer any information prior to testing.

Much of the preassessment information gathering can be done with the help of network tools available throughout the industry. For example, port and vulnerability scanning tools can be utilized to identify open areas of the network, patch configuration levels, and patch known bugs for system versions. Surveillance cameras can also be used to identify weaknesses in the physical security of the network.

## Execution Phase

In this phase, the actual database security assessment is conducted. The tasks completed here are dependent on a great number of factors, including the area tested, the type of test being conducted, the scope of the test, and the priority of a particular test. For instance, an external

test that is conducted on the mission-critical database is going to be quite different from an internal test that is conducted on the privileges of users. This section covers the techniques of a black box security assessment execution, from the perspective of an intruder. This is to ensure that the most comprehensive approach is covered. Keep in mind that not all actions listed within this section are necessary for white-box-type assessments.

**Information Reconnaissance** The complex nature of today's network structures works as an advantage toward the efforts of keeping our environments secure. Intrusion would require much less time and energy were the environments less varied and multifaceted. The first step in obtaining access from any infrastructure is information gathering. Unfortunately for administrators, finding information is much easier than hiding it. With remote access becoming more necessary, and intrusion aid tools increasing by the minute, no system infrastructures are completely hidden from the outside world. Given enough time and resources, some information can be discovered either directly or indirectly from any existing system or infrastructure. The greatest security defense is time. Security measures that are built strongly enough to keep intruders busy for long periods of time are more likely to thwart those who are looking for a quick avenue, and the longer an intruder attempts to access the system, the better chance there is that security logs will capture their presence. This section discusses information reconnaissance and explores techniques that intruders use in an attempt to gather information from a system infrastructure.

**Information reconnaissance** is the process of gathering information either directly (e.g., actively) or indirectly (e.g., passively) from a system or the system's environment. There are two types of information reconnaissance, passive and active.

- **Passive reconnaissance**—**Passive reconnaissance** involves the use of passive investigation methods to gather information about a system or an infrastructure indirectly. An example of a passive reconnaissance attack is a user who utilizes tools such as a network sniffer to obtain information about a system or network infrastructure. A **network sniffer** is a utility that monitors and captures network activity, enabling the owner of the utility to gain an understanding of the amount, frequency, and type of communication occurring on a network. A network sniffer combined with a bit of expertise provides a great tool for gathering information about a network environment, including things like the type of applications that are running and a general idea of the number of users within a network. Database and SQL sniffers exist that are intended to help database administrators and developers monitor their own database systems. These tools can provide unauthorized individuals the means by which to obtain information from the database without ever having to directly communicate with it. Information gathered through passive reconnaissance is not necessarily directly applicable, but it provides information that will eventually lead toward more active information-gathering methodology.
- **Active reconnaissance**—**Active reconnaissance** involves the use of active investigation methods to gather information about a system or an infrastructure directly. An example of an active reconnaissance attack is a user who sends SQL injections to a system in hopes of generating some type of error or system response to use to make inferences about the system or environment. Automated tools are also available that will send pings and packets to systems to initiate a response. Many of these tools will also make determinations based on system responses they receive, providing data to the user,



such as the current operating system, the services running, the firewall, the applications, or the topology of an infrastructure.

Active and passive reconnaissance are two very useful methods for gathering information. Passive reconnaissance requires much more time than active reconnaissance, but it is very difficult to detect. For both active and passive reconnaissance, several freely downloadable tools are available to aid in the information-gathering process. Although it offers more information, active reconnaissance can lead to detection of an intruder on a system. Because it involves active communication with the system, logs and activity reports can potentially show the identity of an attacker; therefore, the less time spent actively gathering information, the better.



It is important to point out that information reconnaissance does not always involve technology. Social engineering can be used as a form of active reconnaissance. A person sitting outside a company warehouse taking notes of incoming and outgoing packages is an example of a nontechnical application of passive reconnaissance.

To better understand the concept of passive and active reconnaissance, consider this scenario. A man decides that he is going to rob the local convenience store. He begins by using passive reconnaissance methods to gather information about the store security. He sits in his car across the street day after day taking notes of shift changes, looking for security guards and outdoor cameras. He watches the counter clerks as they interact with customers, gaining a basic understanding of their personalities, enabling him to form assumptions as to which clerks are most likely to fight rather than flee. He pays attention to their routines, finding out when they stock shelves, change the register drawers, and open the safe. After obtaining enough information about the store security and management from the outside, active reconnaissance can commence. At this point, he begins to actively shop at the store, taking note of the position of the internal cameras and talking to the clerks to obtain a better understanding of their psyche. He takes a closer look at the positioning of the safe, and looks for phones, alert buttons, or any way that the clerk could call for help. With all of the information gathered, the robber can plan his attack, and, having built a relationship of trust with each of the clerks, they won't know what hit them!

10

**Obtaining Access** A common initial milestone in the security assessment process is obtaining access into a system infrastructure. The way this milestone is achieved will depend on system responses as well as the goals of the security assessment. Several different entrance doors provide access into a network; from the physical server to the wireless network, an opportunity for penetration exists within each. This section explores the most common doors through which intruders obtain access into a foreign environment externally and blindly.

**The Use of Automated Tools** Several automated tools have been developed to defeat network security measures. These tools contain features that enable their owners to capture data transmitted during transit, to crack passwords, and to find vulnerabilities within an infrastructure. Many of these tools also have the capability to identify software, hardware, and network devices found within the infrastructure and some go as far as providing a map of the overall topology of a network. All of the tools listed in this section are downloadable free from the Internet and offer significant means by which to gain access to a system infrastructure and network environment:

- **Network port scanners**—Network ports are the most common way to access resources available throughout the environment. **Network port scanners** are automated tools that are designed to traverse the network in an attempt to locate available vulnerable ports and identify the services that they use. Why is this important? A network port is a number-addressed channel created for communication to and from services and processes. Ports are assigned addresses ranging from 0 to 65,535, and most port numbers are designed to indicate a specific type of service request that is associated with that port. The term associated is used lightly here, because port numbers can be changed and services can be forced to communicate on different ports than those for which they were originally intended. For example, port 21 is reserved for FTP communication; this means that, in theory, this port should only accept FTP-type service requests, but services and ports can be manipulated. Although some ports have been deemed more dangerous than others, they all offer a way to access a system and intruders can abuse ports by passing Trojans and other types of malware through them. Therefore, if an open port is available on a router or within an operating system, an intruder can hijack the port and send malicious code by way of it. Code such as a key logger can be inserted into the port to further obtain information. A **key logger** is a piece of malware constructed to log every stroke a user types on the keyboard. Key loggers record the keystrokes of a user into a text file that is sent back to the attacker for a specific period of time and frequency. Not only do ports offer access into an infrastructure, but key loggers provide a grand opportunity for attackers to retrieve passwords and sensitive data from a machine. Imagine the amount of information that can be gathered from a key logger that remains on a database server for over a month, logging every action the database administrator takes. The amount of sensitive information that would be compromised is immeasurable. Refer to Table 10-1 for a list of common port addresses and their associated services.
- **Password scanners**—Essentially, **password scanners** traverse the network searching for passwords from remote authentication systems. Password scanners capture, record, and return passwords as they are sent across the network. The risk that a password scanner poses is obvious and is the primary reason passwords should never be sent to a remote machine without some type of encryption. Some password scanners include the capability of cracking the passwords as well. This adds significant complexity for those attempting to protect transmitted passwords, but as a rule of thumb, the greater the complexity of the encryption, the more difficult and time consuming it is to decode.
- **Network sniffers**—Essentially, network sniffers traverse the network searching for packets of data from which information can be extracted. Network sniffers can identify missing software patches, application types, application version numbers, open ports, operating systems, and firewalls, to name a few. Sniffers offer a quick way for an intruder to search for all vulnerabilities within an infrastructure. Like all of the other scanners, network sniffers can be found and downloaded free online.
- **Wireless scanners**—With wireless network popularity, wireless scanning applications are at an all-time high. **Wireless scanners** identify vulnerabilities within a wireless network, which includes missing encryption keys and poor security measures. Some wireless scanners can also locate vulnerability and risks within Bluetooth environments. Wireless networks can be scanned both actively and passively. Passive wireless



Port address	Service	Comments
21	File Transfer Protocol (FTP)	Used for FTP file transfers, uploading and downloading files from a server
23	Telnet	Used for all Telnet sessions, connecting to a remote machine
25	Simple Mail Transfer Protocol	Used for sending outgoing mail
53	Domain Name Service (DNS)	Used to transfer domain name information
67	Dynamic Host Configuration Protocol (DHCP)	Used for allocating new leases and IP addressing information
80	Hypertext Transfer Protocol (HTTP)	Used for Internet traffic and requests
110	Post Office Protocol 3 (POP3)	Used to support incoming e-mail messages
161	Simple Network Management Protocol	Used to gather information about network device status
1433	SQL Server and SQL Server Replication	Used as the default connection to a Microsoft SQL Server database and for replication of Microsoft SQL servers
1434	SQL Server Monitoring	Used by Microsoft SQL Server for monitoring performance of the database servers
1521	Oracle	Used as the default connection to an Oracle database
3306	MySQL	Used as the default connection to a MySQL database

Table 10-1 Common port addresses

scanning captures information about wireless activity, device types, device addresses, and data transmitted, aiding the intruder looking to further explore unauthorized networks.

- **Wired Equivalent Privacy (WEP) crackers**—An encrypted-key password is often used to secure a wireless network environment. A wireless router creates an encrypted string of letters and numbers from an inputted user password; this is a WEP key and is used to log in to a wireless network environment. **Wired Equivalent Privacy**, or **WEP crackers**, are software applications that are used to decrypt WEP keys. They provide attackers with entry into a wireless environment by breaking its password-encrypted code.

**Exploiting Network Hardware** Network hardware can be used to access the network in several ways. Some of these techniques involve installing rogue devices, whereas others are exploited through identified vulnerabilities:

- **Rogue access points**—Wireless networks are expensive and difficult to secure. A wireless network can be compromised in several ways, but rogue access points are

currently the most common and most difficult to identify. A **rogue access point** is a wireless access point (e.g., wireless router) that is installed within a company's wireless range without authorization, exposing the entire network, leaving it open for anyone and everyone to navigate. For example, let's say that an intruder purchases a wireless access point at the local computer store. Subsequently, this intruder installs his new access point, with an SSID of Finance, in the range of ABCConsulting. The wireless devices within the existing ABCConsulting (e.g., laptops, Blackberries) network will be redirected and begin to connect to Finance to access the network. The intruder is also able to connect to Finance, using his own wireless device to obtain access to ABCConsulting, implement an attack, and obtain sensitive information. In fact, anyone within the wireless range of ABCConsulting's new access point can connect as an unauthorized user as well.

- **Firewall penetration**—Firewalls are the largest contributors to the security of an infrastructure of all the security measures that can be placed within an environment. They work tirelessly to keep unauthorized users and traffic from entering a network. Although they are invaluable assets to an infrastructure, as with other security tools, they, too, can fall prey to intrusion attacks. The strength of a firewall, like many other technical devices, is dependent on the manufacturer, the hardware from which it is built, and the length of time that it has been in production. Firewalls tend to lose their effectiveness with time as new and improved attacks are discovered by intruders. Older firewalls contain services and default accounts with known security vulnerabilities. Network scans can provide intruders with information about a firewall's manufacturer and model number. Armed with this information, an attacker can conduct a simple Internet search to find out more information, and, in cases where the firewall is a bit aged, the attacker can exploit the services, accounts, and any other well-known vulnerability for the specific make and model.

Another well-known technique used to gain access to an unauthorized network via a firewall is by using port redirection and reverse Telnet. Port redirection works by redirecting packets into unauthorized territory, by taking advantage of an existing trust between the firewall and a system. Essentially, an attacker Telnets into a trusted system and through reverse Telnet redirects commands to another shell located within a firewalled perimeter.

**Exploiting the Operating System** An operating system manages every aspect of a computer, including resource allocation, data access, and user authentication. Without an operating system, our computers, servers, and networks would be useless. With this power comes great risk. The operating system was designed to make computers effortlessly interact with people, other hardware, other software, and all network environments, yet very little concentration has been placed on security. Operating systems are often placed on the market with a limited amount of debugging satisfied. Because it is virtually impossible for an operating system manufacturer to test the systems against every single component and custom-made application within our complex networks, many operating system vendors are left to rely on customers for reporting security vulnerabilities. Unfortunately, most security vulnerabilities that exist are not found until a breach occurs. Therefore, these vulnerabilities often go unnoticed for quite some time. To make matters worse, once patches are created to secure the identified risks, it is up to the administrators to apply these patches. This could result in even more time that the vulnerable



operating system is in production and the network environment is virtually exposed. Outdated operating systems or those that have not had the most recent security patches applied are one of the most common vulnerabilities that are exploited through the network.

**Exploiting Web Applications** Web applications interact with servers, so they offer a legitimate way for intruders to gain access to the infrastructure. For example, network, database, and SQL sniffers can be used to obtain the identification of the database applications being used within the environment. A quick Internet search can identify vulnerabilities that exist within this application, and these vulnerabilities can be exploited as a way to gain access to the database itself. Once access has been achieved, SQL statements can be used to construct the database schema and escalate user privileges. Similar to operating systems, applications that have not been effectively debugged and patched provide a door into the network. Figure 10-1 displays this process of intrusion.



**Figure 10-1** The process of intrusion  
© Cengage Learning 2012

## Escalating Privileges

Once access has been achieved, the next step for an assessor or an intruder is to escalate the privileges of the current user so that more rights are available. Once access has been obtained, privileges can be escalated by a few methods, but these methods depend on a number of factors, including the way the user is physically connecting to the database as well as the user account with which the attacker is currently logged in. The following list details the most common methods unauthorized users use to escalate their account privileges:

*Note:* SQL injection techniques described in Chapter 8 can be utilized in situations where the database is being accessed remotely.

- Guest accounts can be manipulated to provide improved account capabilities.
- Passwords can be obtained from the OS, from the network, or from within the database itself. If encrypted, using a password cracker can help to decrypt the passwords.

Copyright 2011 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s). Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

- Network sniffers can be installed locally to discover passwords traveling across the network.
- Windows services that are written to be executed as the local system account can be manipulated.
- Third-party tools that are designed to allow users to run code for escalating privileges can be used locally or remotely.
- Cross-site scripting techniques can be utilized to run malicious code on the local machine using the Web browser.
- Brute force strategies can be attempted as a way to increase user credentials and privileges.
- Passive information-gathering techniques can be conducted using the individual's current system privileges as an attempt to learn more about the system's security structure.

### Reporting Phase

This is the final step of the security assessment. It is here that the results are analyzed and a report is drawn describing in detail the discovered security vulnerabilities as well as potential remediation. The format of the written report is dependent on the organization's standard, yet the writing should provide enough detail to fully prepare administrators to fix the problems at hand. Common components that are found in a written security assessment report include the following:

- The gathered background information
- The defined perimeter and scope
- The objective of the security assessment
- The key findings
- The remediation recommendations, including deliverables, required resources, and a time frame
- Information about the methodology that was used for penetration testing

Following up on the remediation recommendations is vital to the confidentiality, integrity, and availability of the network as a whole. Therefore, a process should also be identified within the report that clearly details the steps for remediation, including a schedule for a repeat security assessment for remediated areas.

---

## Chapter Summary

- Security testing is the process of penetrating the security of an environment to measure its strength and determine the feasibility of an attack.
- Security auditing differs from security testing in that security auditing is used to determine vulnerabilities within internal controls and the reliability of the processes, whereas security testing measures the strength and effectiveness of an environment's security as well as the potential for an attack.
- Security tests are often too laborious and resource intensive to be conducted for all areas of an organization at the same time. Therefore, security tests are best suited for evaluating the security of small groups of assets within an organization.



- The security assessor should have a great amount of intrusion experience and must be able to think from the perspective of an attacker.
- Security testing and auditing are equally as effective, and an ideal security strategy includes both testing and auditing.
- Internal security tests are conducted within the organization's security perimeter and are most often conducted with information about the organization given to the assessor prior to the penetration.
- External security tests are conducted outside the organization's security perimeter and are often done blindly with little to no information given about the environment prior to the test.
- Black box testing is conducted under the assumption that the intruder has no prior knowledge of the organization's infrastructure. Black box testing is normally more broad and exploratory than white box testing.
- White box testing is conducted under the assumption that the potential intruder is internal or has some knowledge about the infrastructure. White box testing is typically focused on a specific target and is often done in reaction to a recent attack.
- An auditor requires much more expertise to conduct effective black box testing due to its ambiguous nature.
- To define an appropriate scope for security testing, both the physical and logical areas need to be included.
- Defining a scope for a black box test is much more difficult than for a white box test scenario. Because no prior information about the infrastructure exists, scopes for black box testing are defined by how successful an attack is in penetrating the system. The end of a security test is often identified by the intruder's ability to obtain a certain level of access into a system.
- Planning and preparation for a security test is dependent on the type of test being conducted. Planning for a white box test includes pretest information gathering, scope and perimeter definition, contract development, assessment scheduling, and threat prioritization. Planning for a black box test does not include threat prioritization and pretest information gathering.
- Information gathering for white box testing scenarios includes the review of network diagrams, database schematics, network assets, areas of weakness, areas with the highest potential of attacks, and historic attack strategies.
- Intruders attempt to gather information from a foreign environment in two ways, passive reconnaissance and active reconnaissance.
- Passive reconnaissance is a strategy for gathering information about an infrastructure indirectly—tools such as network sniffers and port scanners are included.
- Active reconnaissance involves direct system probing to obtain information. The strategy can be detected by logs and monitoring devices.
- Passive reconnaissance helps an intruder obtain enough information to conduct active reconnaissance, which in turn aids them in creating custom system attacks.
- Obtaining access is the initial goal of a potential attacker because it gives them the opportunity to escalate privileges and subsequently take over a system.

- Several automated tools are available from the Internet that help an intruder obtain access into a system. These include port scanners, network sniffers, password and wireless scanners, and WEP crackers.
- Rogue access points and firewall penetration techniques are two ways that network hardware can be used to obtain access into a system.
- Poorly written code and misconfigured applications are two ways that intruders can use software and operating systems to obtain access.
- Several techniques can be used to escalate privileges once access has been obtained, for example, automated tools and brute force attacks.
- The security test report will include the background information, the scope, the defined perimeter, the goal, the methodology, and the key findings.
- Remediation actions are defined by a set of deliverables and should include a schedule for completion.

---

## Key Terms

**active reconnaissance** The use of active investigation methods for gathering information about a system or an infrastructure directly.

**black box testing** An assessment that is conducted with no prior knowledge of the system or infrastructure that is being tested.

**external testing** An assessment that is conducted outside the organization's security border; this type of testing will display attacks and liabilities that can be exploited externally from competitors, external users, and hackers. Initial tasks most commonly completed during external testing involve information gathering. An external intruder must gain information from a system or an infrastructure to break into it.

**information reconnaissance** The process of gathering information either directly (e.g., actively) or indirectly (e.g., passively) from a system or the system's environment.

**internal testing** An assessment that is conducted within the organization's security border that will display vulnerabilities that exist among internal users such as employees and contractors. It also identifies attacks and the damage that can be caused within the network itself. A task conducted during an internal security assessment might include an evaluator logging in to a user's computer in an attempt to raise the user's privileges on a particular system.

**key logger** Malware constructed to log every keyboard stroke that a user types on the keyboard.

**network port scanner** Automated tools that are designed to traverse the network in an attempt to locate available vulnerable ports and identify the services that they use.

**network sniffers** The utilities that monitor the network looking for a number of combined types of vulnerability. Network sniffers can identify missing software patches, application types, application version numbers, open ports, operating systems, and firewalls, to name a few.

**passive reconnaissance** The use of passive investigation methods to gather information about a system or an infrastructure indirectly.



**password scanners** Essentially, network sniffers that traverse the network searching for passwords from remote authentication systems. Password scanners capture passwords as they are sent remotely across the network and record them for the attacker to maintain.

**rogue access point** A wireless access point (e.g., wireless router) that is installed within a company's wireless range without authorization, exposing the entire network and leaving it open for anyone and everyone to navigate.

**security scope** This defines the perimeter of the overall security assessment, the physical and logical area included within the assessment.

**security testing** The process of identifying the feasibility and impact of an attack or intrusion of a system by simulating active exploitation and executing potential attacks within that environment.

**white box testing (target testing)** An assessment that is conducted by an intruder who already has information about the system or the infrastructure. It is also known as targeted testing because prior knowledge exists and known weaknesses within the infrastructure allow for intruders to focus on specific areas of the infrastructure. The goal is to assess the damage that can be done by users who understand the infrastructure that they are attempting to intrude; the results will provide a more comprehensive, thorough picture of specific system weakness than that found in black box testing.

**Wired Equivalent Privacy (WEP) crackers** Software applications that are used to decrypt WEP keys.

**wireless scanners** Utilities that identify vulnerabilities within a wireless network, including missing encryption keys and poor security measures.

## Review Questions

1. Describe how a security test differs from a security audit.
2. List and compare the characteristics of internal and external security tests.
3. Explain how the planning stage for a black box test is different from a white box test.
4. Describe why a black box test requires more expertise than a white box test.
5. Explain why a scope is defined differently for a black box test than it is for a white box test.
6. For what scenario is a security test a better fit than a security audit?
7. List the typical sections of information included within a security test report.
8. Describe the benefits of a standardized security testing methodology.
9. What is the difference between information gathering for preparation of a security test and information gathering during a security test?
10. Explain the difference between passive reconnaissance and active reconnaissance.
11. List at least three ways an intruder can gain access to an infrastructure.
12. Identify at least two ways that an intruder can escalate privileges within a database.

## Case Projects



### Case Project 10-1: Database Security

Use the Internet. Find and describe one automated tool that aids in database security testing. (It is not recommended to install the tool.)

### Case Project 10-2: Passive Reconnaissance Tools

Use the Internet. Find and describe at least two automated tools that can be used for passive reconnaissance. (It is not recommended to install the tools.)

### Case Project 10-3: Active Reconnaissance Tools

Use the Internet. Find and describe at least two automated tools that can be used for active reconnaissance. (It is not recommended to install the tools.)

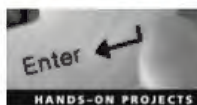
### Case Project 10-4: Capturing Passwords

Use the Internet. Find and describe at least one automated tool for capturing and decrypting passwords within a database. (It is not recommended to install the tool.)

### Case Project 10-5: SQL Server's Security Template

Using this chapter as well as the SQL Server Web site at <http://www.microsoft.com/sqlserver/2008/en/us/>, install the security template available within Server Management Studio. Describe the steps that were taken to do so.

## Hands-On Projects



### Hands-On Project 10-1: White Box Database Security Test

You have been hired as a security professional for your company. You are to create and implement a white box informal database security testing schedule for the organization. Create a paper that addresses the following:

- Create a table that includes a rotating schedule for the 12 months of security testing. Include columns that identify time estimations for each test listed.
- Create a planning and preparation checklist common to all security tests as a whole.
- Identify any special planning and preparation needed for each test.
- Identify the scope for each test and identify any special considerations that need to be addressed.
- Create a list of at least five testing activities for each audit.
- Provide recommendations for securing the database that are unique to Oracle.



- Provide recommendations for securing the database that are unique to MySQL.
- Provide recommendations for securing the database that are unique to SQL Server.

## Hands-On Project 10-2: Black Box Database Security Test

You have been hired as a security consultant for XYZ Company. You are to create and implement a black box, external database security test. Write a paper that responds to the following:

- How will the scope be identified?
- What will indicate the end of a test?
- What special skills or characteristics will be required from the assessor that are not as necessary in white box testing scenarios?
- Identify and describe the first three main goals of the test.
- Explain at least three specific techniques that will be used to gather information.
- Explain at least three specific techniques that will be used as an attempt to obtain access to the system.
- Provide at least two special considerations unique to Oracle.
- Provide at least two special considerations unique to MySQL.
- Provide at least two special considerations unique to SQL Server.