EXAM OBJECTIVES

- Understanding penetration testing
- Knowing penetration testing terminology
- Being familiar with CompTIA's penetration testing phases

Chapter 1
Introduction to Penetration Testing

The CompTIA PenTest+ certification exam is designed to test your knowledge of performing penetration tests either for third-party clients or for the company that employs you as a security professional. Although the fun part of penetration testing is diving in and trying to bypass the security controls put in place to help protect company assets, you have much work to do before that can happen. You have to make sure you take the time to prepare, which includes defining the goals and restrictions for the penetration test.

In this chapter, you learn about the basics of penetration testing, starting with an overview of penetration testing and penetration testing terminology. You then learn the four major phases to CompTIA's penetration testing process: planning and scoping; information gathering and vulnerability identification; attacks and exploits; and reporting and communication.

Penetration Testing Overview

Penetration testing, also known as *ethical hacking,* involves an information technology (IT) professional using the techniques a hacker uses to bypass the security controls of a network and its system. A *security control* is a protection element, such as permissions or a firewall, that is designed to keep unauthorized

individuals out of a system or network. The act the IT professionals are performing is known as a *penetration test,* or *pentest* for short (which is where CompTIA's term, PenTest+, came from). The penetration test follows the process the hacker would take, including the discovery of targets and the exploitation of targets.

From a company's point of view, the ultimate goal of a penetration test is to have an ethical person perform attacks on different assets to determine whether those assets could be penetrated, and if the attacks are successful, what remediation steps a company could take to prevent a real attack from being successful.

FOR THE EXAM

For the PenTest+ certification exam, remember that remediation steps within the report are a must for any successful penetration test.

A key point to remember is that the person performing the penetration test — the *pentester* — is taking the mindset of a hacker and following the process a hacker takes. This involves much planning, as only 10 to 15 percent of the penetration test is actually performing the attacks. Like hacking, penetration testing is 85 percent preparation so that by the time the attack is performed, the hacker or pentester is quite sure the attack will be successful. You can compare this process to robbing a bank. A bank robber will spend the most time planning the robbery. When it comes time to rob the bank, the actual act of robbing the bank is done in minutes (or so I hear).

Reasons for a pentest

Why would a company conduct a penetration test? The purpose of a penetration test is to obtain a real-world picture of the effectiveness of the security controls put in place to protect the company's assets. Instead of taking the word of the security team that configured the security of the environment, you can put the security to the test by having someone take the steps a hacker would take and see if the security holds up. In performing such a test, the pentester can also obtain a list of steps the company could take to prevent real attacks from being successful.

Another reason to perform penetration testing is to be in compliance with regulations. Depending on the industry a company services, organizations may be governed by regulations that require penetration testing to be performed on a regular basis to ensure the security of the organization. For example, companies that collect and store sensitive payment card information are governed by the Payment Card Industry Data Security Standard (PCI DSS). The PCI DSS has strict requirements for activities that must be performed to help keep sensitive payment card information secure. Check out "Best Practices for Maintaining PCI DSS Compliance" and "Penetration Testing Guidance" at `www.pcisecuritystandards.org` to learn more about PCI DSS compliance requirements.

Table 1-1 summarizes two key requirements from the best practices document published by the PCI Security Standards Council. These requirements specify that organizations must perform an annual penetration test and implement any remediation actions identified by the test. Organizations must also perform a network segmentation penetration test every six months to maintain compliance.

TABLE 1-1 **PCI DSS Best Practices Requirements**

Requirement	Title	Description
11.3	Penetration testing	Perform annual penetration testing against preordinated use cases/attack scenarios and perform remediation actions to address any identified vulnerabilities
11.3.4.1	Six-month penetration testing for segmentation	Bi-annual penetration testing conducted for network segmentation controls

Source: PCI Security Standards Council. Best Practices for Maintaining PCI DSS Compliance. January 2019: pp 46-47. Available at `www.pcisecuritystandards.org`.

The PCI Security Standards Council's "Penetration Testing Guidance" document gives more detail on compliance requirements such as the fact that you must also perform a penetration test any time major changes are made to the network infrastructure or to applications within the organization (on top of doing annual penetration testing).

The key point here is that compliance requirements could drive the need to perform penetration tests on a regular basis.

FOR THE EXAM

For the PenTest+ certification exam, remember the two main reasons to perform a penetration test: (1) to get an accurate picture of the results of an attack, and (2) to be in compliance with industry regulations.

Who should perform a pentest

Now that you know what a penetration test is, the next logical question is who should perform the penetration test? You have two choices when it comes to who performs the penetration test: internal staff or an external third-party company.

Internal staff

Many organizations opt to have their internal security staff perform penetration testing. This is a good idea as it will save money, but you must make sure there is no conflict of interest with the group performing the pentest. You must also make sure the people performing the pentest are qualified to conduct a pentest.

(I discuss the qualifications needed by pentesters in "Qualified pentesters" later in this chapter.)


TIP

The members of the internal team performing the penetration test should not be part of the team who installed, configured, or manages the systems or networks being assessed. They should also not be the persons responsible for implementing the security of the systems, as that is a direct conflict of interest. A separate team should be dedicated to assessing security within the organization and performing the penetration tests.

Companies may also create separate internal teams — a red team and a blue team — to help assess the security of assets within the organization. The *red team* is an internal security group that performs attacks on company assets, such as a penetration test and social engineering attacks to validate whether there is enough protection on the company assets. The *blue team* is the internal security group within the company that is focused on protecting the assets. This includes monitoring the security controls, the intrusion detection systems, and the logs to protect the asset and identify when a security breach occurs. It is important to note that the red team's job is to stay up-to-date on any new attack methods, while the blue team must be current on any new technologies used to protect assets from attacks. The red team and blue team should also meet regularly to update the other team on lessons learned so that both teams are fully aware of current attacks and mitigation strategies.


TIP

Penetration testing can be a costly affair, so having an internal team can save the company lots of money and allow for more regular pentests.

External third party

Going with a third-party company to perform the penetration test also has its benefits. For example, the third-party company is most likely not familiar with the organization's environment (as a hacker would not be), so it can provide an even better picture of an attack because the third party would have to discover all the systems (depending on the type of pentest, which I talk about later in this chapter). Using third-party external testers is also beneficial because you have a fresh set of eyes looking at your network and systems. Internal staff have designed the defensive posture based on the attack vectors they are aware of, while external testers may have knowledge of different attack vectors and may take a totally different approach to exploiting systems.

However, using a third-party company also raises some concerns. For example, what are the qualifications of the consultants doing the pentest? And how will the details and results of the pentest be kept confidential? With a third-party company involved, confidentiality can be a bit more challenging than if a company used internal testers.

A final concern is cost. Going with a third-party company can be very costly, as penetration testing is a time-consuming process and requires a specialized skill.

Qualified pentesters

Whether you choose to use internal staff or an external third-party company to perform the penetration test, it is critical you validate the qualifications of the individuals performing the penetration test prior to the engagement.

The first qualification to look for in a pentester is whether or not that person holds industry-standard certifications that prove the individual's penetration testing knowledge. For example, you may require that all individuals performing a penetration test have their CompTIA PenTest+ certification.

However, certification is not enough. The pentester should also have prior experience performing penetration testing. Following are some questions to ask when hiring a third-party company to perform a penetration test:

- Does the penetration testing team have experience with prior penetration tests?
- Has the penetration testing team performed a penetration test against a similarly sized organization before?
- Does the penetration testing team have experience with the types of systems and platforms being used by the company?
- Does the penetration testing team have experience with network-layer testing (networking systems and configuration)?
- Does the penetration testing team have experience with performing application layer testing, and is it familiar with Open Web Application Security Project (OWASP) Top 10 validation techniques? (OWASP Top 10 is the top ten methods hackers are using to exploit web applications.)

How often a pentest should be performed

There is no concrete answer to how frequently you should perform a penetration test; however, it's best to perform a pentest annually and after any major change to the infrastructure.

Standards such as the PCI DSS state that in order to be compliant, organizations should perform *external* testing once a year, plus after making any major changes to the network infrastructure or application environments. The PCI DSS also states that you should perform *internal* testing once a year and after any major changes.

Regular schedule

If your organization is not governed by regulations that dictate when you need to perform a penetration test, you can create your own schedule that works for you. Hiring an external team of penetration testers can be expensive, so one option may be to create a schedule that uses internal staff to test internal and external assets more frequently than an external company. For example, a schedule could look like this:

- **Every 12 months:** Penetration testing of internal assets is performed by internal staff.
- **Every 12 months:** Penetration testing of external assets is performed by internal staff.
- **Every 24 months:** Penetration testing of internal and external assets is performed by a third-party company.

TIP

Using internal staff for penetration testing can help you reduce costs of penetration testing while still performing them on a regular basis. However, you should have a third-party company perform a penetration test at some point because it is a great way to get a real-world picture of your assets' vulnerabilities.

After major changes

You should also perform a penetration test after making any major changes to the network infrastructure or application environments, such as upgrades to software. Some examples of infrastructure changes could be adding a new server to the network, replacing a server with a new server, or adding a new network segment. These changes could introduce new ways for hackers to get into the network, so you want to make sure you perform a penetration test to verify all is secure.

In addition, any changes to the software configuration, such as a piece of software being upgraded, should result in a penetration test of that component so that you can verify there are no vulnerabilities in the new software.

FOR THE EXAM

For the PenTest+ certification exam, remember that a penetration test should be performed annually and after any major change to the infrastructure.

Other considerations

A few additional considerations should be taken into account when discussing when a penetration test should occur. For example, one of the risks of a penetration test is that you could end up crashing a system or network. So to ensure your

pentests are successful in providing you with the information you want, you want to make sure you follow these recommendations when possible:

- **Perform pentests in a mockup environment.** When performing penetration testing, you run the risk of crashing systems or networks due to the nature of the attacks. If possible, create copies of systems inside a test environment and perform the penetration test on the test system. It is critical that the test systems are an exact copy so that the penetration test accurately reflects the test of the real system.
- **Perform pentests before deploying the system or application into production.** If possible, before a system or application is put into production, perform a penetration test on that component before it goes live. This will help reduce the cost of maintaining the system, as it is more costly to fix security issues once the system or application is in production.
- **Perform pentests on a regular basis.** Penetration testing is not a one-time thing. It is something that should be performed on a regular basis and after any major changes are made to the environment. For example, if you perform a security test on a web server before it is put in production and you find it is ready for production because all simulated attacks were unsuccessful, it does not mean you do not need to test this system again. You will test the system again during the next annual penetration test.

Defining Penetration Testing Terminology

In addition to understanding what a penetration test is, who should perform the test, and how frequently the tests should be performed, let's take a look at some other penetration testing terminology you need to be familiar with for the CompTIA PenTest+ certification exam.

Types of assessments

The CompTIA PenTest+ certification objectives reference some key terms in regard to the different types of assessments that can be performed. The following are some common types of pentest assessments:

- **Goals-based/objectives-based:** This type of assessment is focused on a specific purpose. For example, you may have installed a new server or piece of software and want to test that specific asset for security flaws. Some examples of goals for goal-based assessments is the company may want to assess the security of only the wireless network, or maybe only perform social

engineering attacks to test the effectiveness of the security education program with the employees. Another common goal may be simply to test the security of a public web site or web application.

- **Compliance-based:** A compliance-based assessment is an assessment that is driven by standards and regulations. With compliance-based assessments, you must follow a standard assessment methodology such as the National Institute of Standards and Technology's (NIST's) SP800-15 series of guidelines or the PCI DSS from the PCI Security Standards Council.
- **Red team/blue team:** The term *red team* refers to the internal team of professionals performing a penetration test acting as hackers. With a red team test you are not as focused on reporting and remediation steps after the fact; you are more focused on trying to bypass security controls and determining how your security team will respond to the attack. The security team responsible for defending against attacks is known as the *blue team.*

Pentest strategy

You can follow several different strategies when performing a penetration test. You can go with an unknown-environment test, a known-environment test, or a partially known-environment test.

- **Unknown-environment:** This test was formerly known as a *black box* test. In an unknown-environment penetration test, the penetration testers are given zero information about the environment and the targets. The goal of the unknown-environment test is to treat the pentesters as if they are hackers — they have to discover the environment before they can attack the environment. In an unknown-environment test, you would not share Internet Protocol (IP) address information, network infrastructure details, or public services on the Internet such as web sites, domain name system (DNS), or file transfer protocol (FTP) servers. It is up to the penetration testers to discover all assets and then try to exploit those assets.
- **Known-environment:** This test was formerly known as a *white box* test. In a known-environment penetration test, the penetration testers are given all of the details of your network environment, including server configurations and the services they run, a network diagram showing different network segments and applications, and IP address information.
- **Partially known-environment:** This test was formerly known as a *gray box* test. In a partially known-environment penetration test, a limited amount of information is given to the penetration testers, such as the IP ranges used by the company or addresses of your public Internet servers. With this information, the pentesters will discover what services are running on each system and then try to exploit those systems.

FOR THE EXAM

For the PenTest+ certification exam, remember the different pentest strategies. Unknown-environment testing is when no details about the target are given; known-environment testing is when all known information about the targets is given to testers; and partially known-environment testing is when limited information, such as IP addresses or server names, is provided to keep the pentest focused on those targets.

Threat actors and threat models

The purpose of penetration testing is to simulate attacks that could occur in real life. A big part of information security — and something all security professionals should be aware of — is who are you protecting against? Who would attack your network or website?

Capabilities and intent

Before we look at the types of hackers and threat models, it is important to understand the different levels of hacking capabilities for each type of hacker, or *threat actor*, and the different reasons or intent for hacking.

The capabilities of a hacker will vary depending on the type of threat actor the hacker is and the types of attacks being performed. Some attacks are basic in nature, so you may find that all types of hackers can perform these attacks, while more sophisticated attacks are performed by hackers with more detailed knowledge of the underlining technologies being hacked, their vulnerabilities, and how to exploit those vulnerabilities.

A hacker may be motivated to hack for many reasons, such as for financial gain (for example, hacking into bank accounts or selling sensitive data obtained in the hack) or for the fame or notoriety earned by hacking into a big-name company. A hacker may also be motivated by a personal cause or a group cause, as is the case with terrorists or activists.

Threat actor

A *threat actor* is a person or entity that causes the threat against your assets. When it comes to hacking, you should be aware of some common threat actors:

- **Script kiddies:** A script kiddie is a person who does not necessarily have much background on how attacks work; they simply run some automated tools to try to exploit systems. Their intent is typically for the challenge, and also bragging rights.

- **Hacktivist:** A hacktivist is a person who hacks for a cause, such as for political purposes or for social change. The capabilities of the hacktivist can range from basic to advanced hacking knowledge, such as is the case with the infamous hacking group called "Anonymous."
- **Insider threat:** Insider threats are threats from inside your organization or inside your network. These can be very serious threats of malicious destruction from a disgruntled employee or even innocent mistakes made by other employees.
- **APT:** An Advanced Persistent Threat (APT) is an advanced hacking process such as one found in a nation-state–sponsored group or person that gains unauthorized access to a network for political or economic reasons. The attack typically happens to gain unauthorized access for a long period of time, such as many months, by planting malicious software on the system that will monitor activity, collect sensitive data, or damage the system. APT also includes advanced hacks on financial institutions, defense contractors, and software companies such as Twitter or Facebook, which would contain a wealth of sensitive information the hacker would like to collect.

Adversary tier

Threat actors are typically identified in an adversary tier that ranks the threat actors by their capabilities and the damage they can perform. The threat actors discussed earlier are ranked based on their threat level and capabilities as follows (1=low, 4=high):

1. Script kiddie
2. Insider threat
3. Hacktivist
4. APT

Figure 1-1 summarizes the adversary tier with script kiddies at the bottom of the skillset and APT at the top.

Threat modeling

Penetration testing typically involves an exercise known as threat modeling. *Threat modeling* refers to the act of documenting company assets and then defining the types of attacks or threats against those assets. The threats are then assigned a likelihood (the chances the attack will happen) and impact (how serious the result of the attack if successful) so that the threats can be prioritized. Based on the priority of the threats, security professionals put security controls in place to prevent those threats from occurring or to minimize the impact.

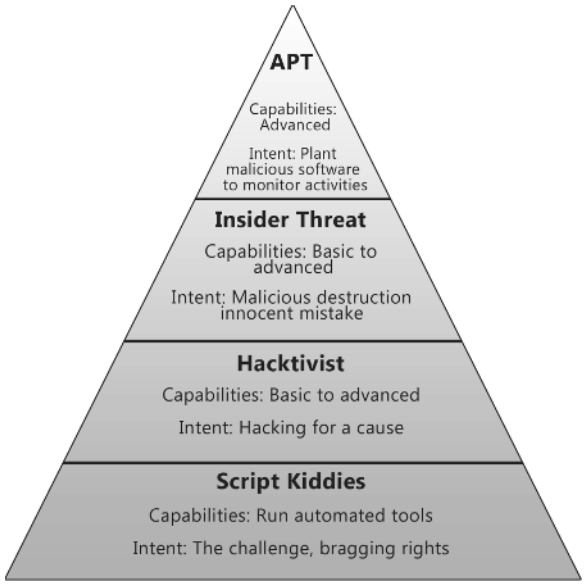

FIGURE 1-1: The adversary tier.

Graphic designed and created by Brendon Clarke.

Looking at CompTIA's Penetration Testing Phases

The CompTIA penetration testing process involves four major phases:

1. Planning and scoping
2. Information gathering and vulnerability identification
3. Attacks and exploits
4. Reporting and communication

Over the course of this book, I go into detail about each of these penetration testing phases. Here, I provide a high-level overview of each one.

Planning and scoping

The first phase of the penetration testing process is planning and scoping. This phase is important as it is when you identify the goals of the penetration test, the timeframe, and the rules of engagement (the types of attacks you are allowed and not allowed to perform during the pentest).

The planning and scoping phase should start with a pre-engagement meeting that determines the extent of the penetration test, such as whether the testing will include internal and external assets. In this phase, you will also determine what systems need to be tested, the best time for testing, and the types of attacks that are allowed and not allowed.

An important part of the planning and scoping phase is to create a statement of work that specifies exactly what is to be tested and to get written authorization from a person of authority for the business that gives you permission to perform the penetration test. Remember that attacking and exploiting systems without prior authorization is illegal.

FOR THE EXAM

For the PenTest+ certification exam, remember to get written authorization from an authorized party such as the company owner or an upper-level manager before moving on to phase two of the penetration testing process.

Chapter 2 covers planning and scoping.

Information gathering and vulnerability identification

The second phase of the penetration testing process is the information gathering and vulnerability identification phase, which is also known in other pentest models as the "reconnaissance phase." This phase can be broken into two subphases: information gathering as the first subphase, and vulnerability identification as the second subphase.

Information gathering

The information gathering part of the penetration test is a time-consuming part of the penetration test. It involves both passive and active information gathering.

With *passive information gathering*, you use public Internet resources to collect information about the target such as public IP addresses used, names and email addresses of persons that could be targets to a social engineer attack, DNS records, and information about products being used. This is called passive information gathering because you are not actually communicating with the company's live systems (unless you surf its website); instead, you are collecting public information that anyone can access and it will not look suspicious. Note that passive information gathering is also known as *passive reconnaissance*.

Active information gathering involves using tools to communicate with the company's network and systems to discover information about its systems. For example, doing a port scan to find out what ports are open on the company's systems is considered *active* because in order to know what ports are open on each system, you have to communicate with those systems. Once you start communicating with the company's network, you risk detection, which is why these techniques are categorized differently than passive information gathering techniques. Note that active information gathering is also known as *active reconnaissance*.

Vulnerability identification

Once the information gathering subphase is complete, you should now have a listing of the ports open on the system and potentially a list of the software being used to open those ports. In the vulnerability identification subphase, you research the vulnerabilities that exist with each piece of software being used by the target. Vulnerability identification also involves using a vulnerability scanner to automate the discovery of vulnerabilities that exist on the target networks and systems.

Chapters 3 and 4 cover information gathering and vulnerability identification.

Attacks and exploits

The third phase of the penetration testing process is to perform the attacks and exploit systems. In this phase, with knowledge of the vulnerabilities that exist on the targets, you can then break out the penetration tools to attack and exploit the systems. This involves social engineering attacks, network attacks, software attacks such as SQL injection, and wireless attacks against wireless networks.

Once a system is compromised, you can then perform post-exploitation tasks, which involve collecting more information about the system or planting a backdoor to ensure you can gain access at a later time.

Chapters 5 through 10 cover attacks and exploits.

Reporting and communication

The fourth and final phase of the penetration testing process is reporting and communication. These tasks are the reason the penetration test was performed in the first place: to report on the findings and specify remediation steps the customer can take to reduce or eliminate the threats discovered.

During this phase, you will write a report of the actions you performed during the penetration test and the results of the testing. You will also include recommendations on how to better secure the systems in the report. The report will be

delivered to the customer in the sign-off meeting, and the customer will sign-off on the completion of the penetration test.

Chapter 11 covers reporting and communication.

TIP

Knowing the phases to the CompTIA penetration testing process is critical on the job and for the exam. Refer to Figure 1-2 for a summary of what occurs at each phase.

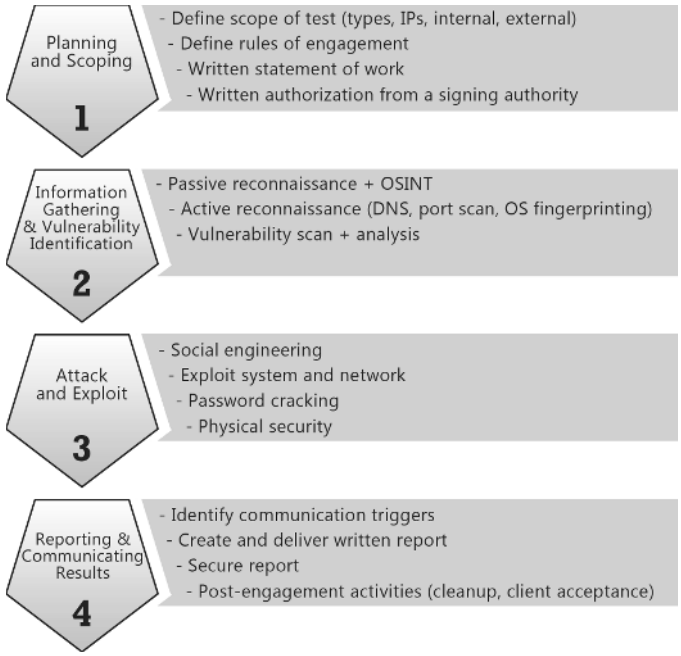

FIGURE 1-2: The CompTIA penetration testing process.

Graphic designed and created by Brendon Clarke.

Identifying Testing Standards and Methodologies

Over the years a number of security assessment and penetration testing methodologies have been developed. In this section, you learn about some of the common security assessment methodologies. Keep in mind that you should be familiar with these for the exam, but you do not need to know the detailed steps performed by each methodology.

MITRE ATT&CK

MITRE ATT&CK is a recognized knowledge base of tactics and techniques used by attackers to compromise systems. The goal of MITRE ATT&CK is to use the information collected and presented in the standard as a basis for threat modeling and analysis. At the MITRE ATT&CK website you can choose a threat and read the details about the threat, including how the threat can be detected and mitigated.

To learn more about MITRE ATT&CK, visit `https://attack.mitre.org`.

Open Web Application Security Project (OWASP)

The OWASP Foundation is a nonprofit foundation focused on improving the security of software. OWASP released the very popular OWASP Top 10 document that lists the ten most common security flaws in web applications that may put your organization at risk. The OWASP Foundation has other projects as well, including its OWASP Mobile Security Testing Guide. Following are the URLs for each of these projects:

- **OWASP Top 10:** `https://owasp.org/www-project-top-ten`
- **OWASP Mobile Security Testing Guide:** `https://owasp.org/projects,/mstg/2021/07/29/MSTG-Release.html`

OWASP Top 10 (2017)

Following is a summary of the 2017 version of the OWASP Top 10 Web Application Security Risks that you should be familiar with for the PenTest+ exam:

- **A1:2017-Injection:** The number one flaw found in web applications is injection flaws. *Injection flaws* occur when data is input into an application but the input is not sanitized or validated by the developer of the application.
- **A2:2017-Broken Authentication:** The second most common flaw in web application is flaws in authentication or session management. This may allow attackers to access passwords, keys, or session tokens.
- **A3:2017-Sensitive Data Exposure:** The third most common flaw in web applications is sensitive data exposure flaws that involve web applications or APIs not protecting sensitive data within the application. This could be financial data, healthcare data, or Personally Identifiable Information (PII) data. This could be due to a lack of encryption at rest and in transit, or other missing access control methods.

- **A4:2017-XML External Entities (XXE):** Poorly configured XML processors can use external entities to disclose internal files or internal file shares, and possibly perform remote code execution or denial of service (DoS) attacks.
- **A5:2017-Broken Access Control:** Many web applications do not enforce restrictions on what an authenticated user can do within the application. An attacker that exploits this flaw can gain access to sensitive information or perform undesired actions.
- **A6:2017-Security Misconfiguration:** Applications should have their default settings altered and security configuration settings reviewed as security misconfigurations is a common flaw in web applications.
- **A7:2017-Cross-Site Scripting (XSS):** XSS flaws occur when an application processes and displays untrusted data in a web application without validating the information. XSS flaws enable attackers to execute malicious code in a victim's browser and possibly hijack the session.
- **A8:2017-Insecure Deserialization:** Insecure deserialization flaws may result in an attacker being able to perform remote code execution, replay attacks, injection attacks, and privilege escalation attacks.
- **A9:2017-Using Components with Known Vulnerabilities:** *Components* are libraries of code that an application may use. Your application may be following secure coding best practices, but once you call a third-party library, that component may be developed in an unsecure manner that exposes your application to security flaws.
- **A10:2017-Insufficient Logging and Monitoring:** Lack of logging and monitoring means that an application or system does not have the capabilities to detect and log breaches in security. Adequate logging and monitoring should be configured within an application or system to help determine the extent of a security breach during incident response.

FOR THE EXAM

For the PenTest+ exam, know the different categories of vulnerabilities listed in the 2017 Top 10 Web Application Security Risks document.

OWASP Top 10 (2021)

The OWASP Top 10 flaws were updated in 2021. Many of the flaws were relabeled and regrouped, with a few changes to the order of the most common flaws:

- **A01:2021-Broken Access Control:** Broken access control moved up from the fifth most common flaw in 2017 to the most common flaw in 2021.

- **A02:2021-Cryptographic Failures:** Previously known as *Sensitive Data Exposure* in 2017, this common flaw was renamed Cryptographic Failures and was also moved to the second most common web application flaw in 2021.
- **A03:2021-Injection:** Injection attacks have moved down to the third most common flaw in 2021. This flaw also encompasses the cross-site scripting (XSS) category from 2017.
- **A04:2021-Insecure Design:** *Insecure design* is a new category in 2021 and covers risk-related design flaws in applications. This new category looks to improve on the use of threat modeling and secure design patterns and principles during the development of the application.
- **A05:2021-Security Misconfiguration:** *Secure misconfiguration* includes the Secure Misconfiguration and XML External Entities (XXE) flaws from the 2017 Top 10 list.
- **A06:2021-Vulnerable and Outdated Components:** This Top 10 category for 2021 is a relabeled version of the Using Components with Known Vulnerabilities flaw in 2017. Note that this flaw has moved up three spots in 2021!
- **A07:2021-Identification and Authentication Failures:** This category was known as Broken Authentication in the 2017 Top 10 listing. Note that it has been renamed and also fell to the seventh position in 2021.
- **A08:2021-Software and Data Integrity Failures:** Another new category for the 2021 Top 10 security flaws list, this flaw pertains to failures when verifying the integrity of components when applying software updates or updates to critical data. Note that Insecure Deserialization from 2017 is included in this category.
- **A09:2021-Security Logging and Monitoring Failures:** Logging and Monitoring has moved up one position in 2021.
- **A10:2021-Server-Side Request Forgery:** A new category for the 2021 Top 10 list is Server-Side Request Forgery. This security flaw enables attackers to invoke requests from a vulnerable web application to another system.

National Institute of Standards and Technology (NIST)

The National Institute of Standards and Technology (NIST) is a federal agency designed to improve science, standards, and technology. Over the years, NIST has created many publications related to information security and recommendations on how to secure different types of systems. In recent years, the NIST has created

Special Publication (SP) documents that relate to many aspects of security, security controls, penetration testing, and cybersecurity. Following are some key special publications to be aware of:

- **NIST SP 800-30:** This special publication provides guidance related to risk assessment.
- **NIST SP 800-53:** This special publication provides guidance related to security and privacy controls.
- **NIST SP 800-39:** This special publication provides guidance on risk management strategies.

There are a number of other standards and recommendations published by NIST that are designed to help organizations improve security:

- **NIST Cybersecurity Framework (CSF):** The NIST CSF is designed to help organizations create a solid cybersecurity program. The framework is organized into five functions to help identify assets within the business and reduce the risk against those assets. The five functions are identify, protect, detect, respond, and recover.
- **NIST SP 800-115:** In this special publication the NIST makes recommendations on steps to take when performing information security testing and assessments.

OSSTMM, PTES, and ISSAF

The *Open-Source Security Testing Methodology Manual* (OSSTMM) is a methodology for security testing that is maintained by the Institute for Security and Open Methodologies (ISECOM). You can download the OSSTMM document from `www.isecom.org/OSSTMM.3.pdf`.

The *Penetration Testing Execution Standard* (PTES) is a methodology for performing penetration tests. PTES breaks the penetration test down into seven phases: pre-engagement interactions, intelligence gathering, threat modeling, vulnerability analysis, exploitation, post-exploitation, and reporting. You can learn more about PTES and the technical guidelines to performing a pentest at `www.pentest-standard.org/index.php/Main_Page`.

The *Information Systems Security Assessment Framework* (ISSAF) is a methodology that provides technical guidance related to performing a penetration test. There are a number of ISSAF technical documents that discuss a wide range of security assessment categories such as wireless LAN security assessment, Windows

security assessments, VPN security assessments, and so on. To see a list of these documents check out the following URL:

```
https://sourceforge.net/projects/isstf/files/issaf%20document/
issaf0.1
```

FOR THE EXAM

Be sure to understand the general purpose of each of the security testing methodologies mentioned here. Specifically note MITRE ATT&CK, OWASP Top 10, and PTES.

Reviewing Key Concepts

This chapter highlights a number of concepts and terminology related to penetration testing that you should be familiar with when preparing for the CompTIA PenTest+ certification exam. Following is a quick review of some of the key points to remember from this chapter:

- Two reasons to conduct a penetration test are to better secure the company assets, or to be compliant with regulations governing your organization.
- You can have a penetration test performed by internal staff or an external third party. If internal staff is used, be sure those conducting the penetration test are not members of the team responsible for managing or configuring the systems being tested.
- You should perform a penetration test annually and be sure to test external and internal assets.
- You can follow several different strategies when performing a penetration test. You can do an unknown-environment test (black box test), for which the pentester is given no information about the target environment. You can do a known-environment test (white box test), for which the pentester is given all of the information about the environment being tested. Or you can do a partially known-environment test (gray box test), for which limited information is given to the pentester to ensure the test is focused and timely.
- A threat actor is someone or something that may perform an attack on your systems or environment.
- The OWASP Top 10 document is a listing of the ten most common security flaws found in web applications and is a great resource for pentesters.
- The four phases to the CompTIA penetration testing process are: planning and scoping, information gathering and vulnerability identification, attacks and exploits, and reporting and communication.

Prep Test

1. **Bob is using nmap to discover ports that are open on the systems. What form of information gathering is Bob performing?**
   - **(A)** Vulnerability identification
   - **(B)** Active information gathering
   - **(C)** Vulnerability scanning
   - **(D)** Passive information gathering

2. **What type of penetration test involves the tester being given no information about the target environment?**
   - **(A)** Unknown-environment test
   - **(B)** Known-environment test
   - **(C)** Partially known-environment test
   - **(D)** All knowledge test

3. **What type of reconnaissance involves the tester querying the DNS to discover the DNS names and IP addresses used by the customer?**
   - **(A)** Vulnerability identification
   - **(B)** Active information gathering
   - **(C)** Vulnerability scanning
   - **(D)** Passive information gathering

4. **Which of the following represents a reason to perform a penetration test annually?**
   - **(A)** Cost
   - **(B)** Time
   - **(C)** Compliance
   - **(D)** Know-how

5. **Lisa performed a penetration test on your organization and is creating the report. What should Lisa be sure to communicate within the report?**
   - **(A)** How good Lisa is at hacking
   - **(B)** Remediation steps
   - **(C)** Signed authorization
   - **(D)** Resources used

6. **Which of the following is critical to perform during the planning and scoping phase of the penetration test?**

   (A) Port scan

   (B) Vulnerability scan

   (C) Summary of remediation steps

   (D) Obtain written authorization

7. **What type of penetration test involves giving the tester only the IP addresses of the servers that you wish to be tested?**

   (A) Unknown-environment test

   (B) Known-environment test

   (C) Partially known-environment test

   (D) All knowledge test

8. **What is the third phase of the CompTIA penetration testing process?**

   (A) Attacks and exploits

   (B) Reporting and communication

   (C) Planning and scoping

   (D) Information gathering and vulnerability identification

9. **What threat actor has limited knowledge of the attacks being performed and typically just runs prebuilt tools to perform the attack?**

   (A) APT

   (B) Script kiddie

   (C) Hacktivist

   (D) Insider threat

10. **You are part of the team within your organization that performs the attacks during the penetration test. What is the name for your team?**

    (A) Blue team

    (B) Black team

    (C) White team

    (D) Red team

11. **What OWASP Top 10 security flaw is a result of an application not employing encryption technology to protect data in storage or data at rest?**

    (A) Injection

    (B) Sensitive Data Exposure

    (C) Broken Authentication

    (D) Broken Access Control

Answers

1. **B.** Bob is performing active reconnaissance, or active information gathering, when using a port scanner to discover ports that are open on a system. *See "Information gathering and vulnerability identification."*

2. **A.** An unknown-environment test (black box test) is when the pentester is given no knowledge of the environment being tested. *Review "Pentest strategy."*

3. **D.** Passive reconnaissance, or passive information gathering, is when the pentester uses public Internet resources to discover information about the target. *Check out "Information gathering and vulnerability identification."*

4. **C.** Organizations may be governed by regulations that force a company to perform penetration tests on a regular basis in order to be compliant. *Peruse "Reasons for a pentest."*

5. **B.** The purpose of the penetration test is to better the security of the organization. Therefore, it is critical the report contains remediation steps on how to improve the security of vulnerable systems. *Take a look at "Reporting and communication."*

6. **D.** It is imperative that you get written authorization to perform the penetration test before doing any testing. Also, be sure to get written authorization from an authorized party such as the business owner or an upper-level manager. It is not enough to get authorization from a local manager. *Peek at "Planning and scoping."*

7. **C.** A partially known-environment test (gray box test) involves giving limited information to the tester so that the tester is more focused on specific targets during the pentest. *Look over "Pentest strategy."*

8. **A.** The third phase of the CompTIA penetration testing process is attacks and exploits. *Study "Looking at CompTIA's Penetration Testing Phases."*

9. **B.** A script kiddie has limited technical knowledge of the details of the attack and simply runs the tools that are already created. *Peek at "Threat actors and threat models."*

10. **D.** The red team is the name of the penetration testing team that simulates the attacks, while the blue team tries to detect and defend against those attacks. *Peek at "Types of assessments."*

11. **B.** Sensitive Data Exposure (2017 OWASP) is now known as Cryptographic Failures (2021 OWASP) and involves flaws of not protecting sensitive data from unauthorized individuals due to lack of encryption technology. *Peek at "Open Web Application Security Project (OWASP)."*