Chapter

1

Penetration Testing

Hackers employ a wide variety of tools to gain unauthorized access to systems, networks, and information. Automated tools, including network scanners, software debuggers, password crackers, exploitation frameworks, and malware, do play an important role in the attacker's toolkit. Cybersecurity professionals defending against attacks should have access to the same tools in order to identify weaknesses in their own defenses that an attacker might exploit.

These automated tools are not, however, the most important tools at a hacker's disposal. The most important tool used by attackers is something that cybersecurity professionals can't download or purchase. It's the power and creativity of the human mind. Skilled attackers leverage quite a few automated tools as they seek to defeat cybersecurity defenses, but the true test of their ability is how well they are able to synthesize the information provided by those tools and pinpoint potential weaknesses in an organization's cybersecurity defenses.

What Is Penetration Testing?

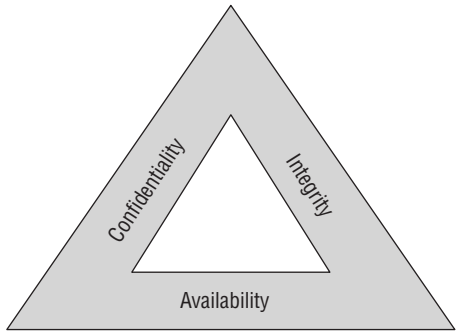
Penetration testing seeks to bridge the gap between the rote use of technical tools to test an organization's security and the power of those tools when placed in the hands of a skilled and determined attacker. Penetration tests are authorized, legal attempts to defeat an organization's security controls and gain unintended access. The tests are time-consuming and require staff who are as skilled and determined as the real-world attackers who will attempt to compromise the organization. However, they're also the most effective way for an organization to gain a complete picture of its security vulnerability.

Cybersecurity Goals

Cybersecurity professionals use a well-known model to describe the goals of information security. The CIA triad, shown in Figure 1.1, includes the three main characteristics of information that cybersecurity programs seek to protect:

- *Confidentiality* measures seek to prevent unauthorized access to information or systems.
- *Integrity* measures seek to prevent unauthorized modification of information or systems.
- *Availability* measures seek to ensure that legitimate use of information and systems remains possible.

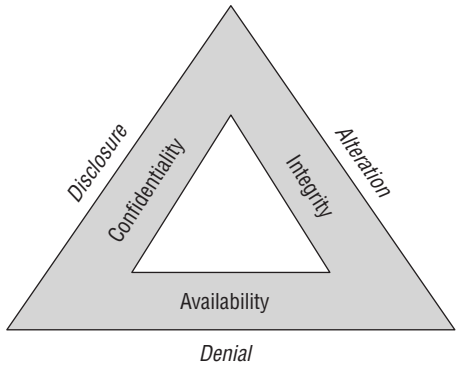
FIGURE 1.1 The CIA triad



Attackers, and therefore penetration testers, seek to undermine these goals and achieve three corresponding goals of their own. The attackers' goals are known as the DAD triad, shown in Figure 1.2:

- *Disclosure* attacks seek to gain unauthorized access to information or systems.
- *Alteration* attacks seek to make unauthorized changes to information or systems.
- *Denial* attacks seek to prevent legitimate use of information and systems.

FIGURE 1.2 The DAD triad



These two models, the CIA and DAD triads, are the cornerstones of cybersecurity. As shown in Figure 1.2, the elements of both models are directly correlated, with each leg of the attackers' DAD triad directly corresponding to a leg of the CIA triad that is designed to counter those attacks. Confidentiality controls seek to prevent disclosure attacks. Integrity controls seek to prevent alteration attacks. Availability controls seek to keep systems running, preventing denial attacks.

Adopting the Hacker Mindset

If you've been practicing cybersecurity for some time, you're probably intimately familiar with the elements of the CIA triad. Cybersecurity defenders spend the majority of their time thinking in these terms, designing controls and defenses to protect information and systems against a wide array of known and unknown threats.

Penetration testers must take a very different approach in their thinking. Instead of trying to defend against all possible threats, they only need to find a single vulnerability that they might exploit to achieve their goals. To find these flaws, they must think like the adversary who might attack the system in the real world. This approach is commonly known as adopting the *hacker mindset*.

Before we explore the hacker mindset in terms of technical systems, let's explore it using an example from the physical world. If you were responsible for the physical security of an electronics store, you might consider a variety of threats and implement controls designed to counter those threats. You'd be worried about shoplifting, robbery, and employee embezzlement, among other threats, and you might build a system of security controls that seeks to prevent those threats from materializing. These controls might include the following items:

- Security cameras in high-risk areas
- Auditing of cash register receipts
- Theft detectors at the main entrance/exit of the store
- Exit alarms on emergency exits
- Burglar alarm wired to detect the opening of doors outside of business hours

Now, imagine that you've been engaged to conduct a security assessment of this store. You'd likely examine each one of these security controls and assess its ability to prevent each of the threats identified in your initial risk assessment. You'd also look for gaps in the existing security controls that might require supplementation. Your mandate is broad and high-level.

Penetration tests, on the other hand, have a much more focused mandate. Instead of adopting the approach of a security professional, you adopt the mindset of an attacker. You don't need to evaluate the effectiveness of each security control. You simply need to find either one flaw in the existing controls or one scenario that was overlooked in planning those controls.

In this example, a penetration tester might enter the store during business hours and conduct reconnaissance, gathering information about the security controls that are in place and the locations of critical merchandise. They might notice that although the burglar alarm is tied to the doors, it does not include any sensors on the windows. The tester might then return in the middle of the night, smash a window, and grab valuable merchandise. Recognizing that the store has security cameras in place, the attacker might wear a mask and park a vehicle outside of the range of the cameras. That's the hacker mindset. You need to think like a criminal.

There's an important corollary to the hacker mindset that is important for both attackers and defenders to keep in mind. When conducting a penetration test (or a real-world attack),

the attacker needs to win only once. They might attempt hundreds or thousands of potential attacks against a target. The fact that an organization's security defenses block 99.99 percent of those attacks is irrelevant if one of the attacks succeeds. Cybersecurity professionals need to win *every* time. Attackers need to win only once.

Ethical Hacking

While penetration testers certainly must be able to adopt the hacker mindset, they must do so in a manner that demonstrates their own professionalism and integrity. Penetration testing is a subset of *ethical hacking*, which is the art of using hacking tools and techniques but doing so within a code of ethics that regulates activity. Some of the key components of ethical hacking programs are:

- Performing background checks on all members of the penetration testing team to identify and resolve any potential issues
- Adhering to the defined scope of a penetration testing engagement
- Immediately reporting any active security breaches or criminal activity detected during a penetration test
- Limiting the use of penetration testing tools to approved engagements
- Limiting the invasiveness of a penetration test based on the scope of the engagement
- Protecting the confidentiality of data and information related to or uncovered during a penetration test

Cybersecurity professionals engaged in penetration testing work that exceeds the bounds of ethical hacking may find themselves subject to fees, fines, or even criminal charges depending on the nature of the violation.

Reasons for Penetration Testing

The modern organization dedicates extensive time, energy, and funding to a range of security controls and activities. We install firewalls, intrusion prevention systems, security information and event management (SIEM) solutions, vulnerability scanners, and many other tools. We equip and staff 24-hour security operations centers (SOCs) to monitor those technologies and watch our systems, networks, and applications for signs of compromise. There's more than enough work to completely fill our days twice over. Why would we want to take on the additional burden of performing penetration tests? After all, they are time-consuming to perform internally and expensive to outsource.

The answer to this question is multifaceted and includes direct benefits as well as the need for adherence to applicable laws and regulatory requirements. Penetration testing provides us with visibility into the organization's security posture that simply isn't available by other means. Penetration testing does not seek to replace all the other cybersecurity activities of the organization. Instead, it complements and builds on those efforts. Penetration testers bring

their unique skills and perspectives to the table and can take the outputs of security tools and place them within the attacker's mindset, asking the question, "If I were an attacker, how could I use this information to my advantage?"

Benefits of Penetration Testing

We've already discussed *how* penetration testers carry out their work at a high level, and the remainder of this book is dedicated to exploring penetration testing tools and techniques in detail. Before we dive into that, let's take a moment to consider *why* we conduct penetration testing. What benefits does it bring to the organization?

First and foremost, penetration testing provides us with knowledge that we can't obtain elsewhere. By conducting thorough penetration tests, we learn whether an attacker with the same knowledge, skills, and information as our testers would likely be able to penetrate our defenses. If they can't gain a foothold, we can then be reasonably confident that our networks are secure against attack by an equivalently talented attacker under the present circumstances.

Second, in the event that attackers are successful, penetration testing provides us with an important blueprint for remediation. As cybersecurity professionals, we can trace the actions of the testers as they progressed through the different stages of the attack and close the series of open doors the testers passed through. Doing so provides us with a more robust defense against future attacks.

Finally, penetration tests can provide us with essential, focused information about specific attack targets. We might conduct a penetration test prior to the deployment of a new system that is specifically focused on exercising the security features of that new environment. Unlike an open-ended penetration test, which is broad in nature, focused tests can drill into the defenses around a specific target and provide actionable insight that can prevent a vulnerability from initial exposure.

Threat Hunting

The discipline of *threat hunting* is closely related to penetration testing but has a separate and distinct purpose. Like penetration testers, cybersecurity professionals engaged in threat hunting seek to adopt the hacker's mindset and imagine how attackers might seek to defeat an organization's security controls. The two disciplines diverge in what they accomplish with this information.

Penetration testers seek to evaluate the organization's security controls by testing them in the same manner an attacker might, whereas threat hunters use the hacker mindset to search the organization's technology infrastructure for the artifacts of a successful attack. They ask themselves what an attacker might do and what type of evidence they might leave behind and then go in search of that evidence.

Threat hunting builds on a cybersecurity philosophy known as the *presumption of compromise*. This approach assumes that attackers have already successfully breached an organization and searches out the evidence of successful attacks. When threat hunters discover a potential compromise, they then kick into incident-handling mode, seeking to contain, eradicate, and recover from the compromise. They also conduct a postmortem analysis of the factors that contributed to the compromise in an effort to remediate deficiencies. This post-event remediation is another similarity between penetration testing and threat hunting: Organizations leverage the output of both processes in similar ways.

Regulatory Requirements for Penetration Testing

There is one last reason that you might conduct a penetration test—because you must! The most common regulatory requirement for penetration testing comes from the Payment Card Industry Data Security Standard (PCI DSS). This regulation is a private contractual obligation that governs all organizations involved in the storage, processing, or transmission of credit and debit card transactions. Nestled among the more than 300 pages of detailed security requirements for cardholder data environments (CDEs) is Section 11.4, which reads as follows:

> External and internal penetration testing is regularly performed, and exploitable vulnerabilities and security weaknesses are corrected.

There are some additional requirements for how the organization's penetration testing methodology should be conducted that appear in the detailed Requirement 11.4.1. According to that requirement, the organization should have a penetration testing methodology that is "defined, documented, and implemented by the entity, and includes:

- Industry accepted penetration testing approaches.
- Includes coverage for the entire CDE perimeter and critical systems.
- Testing from both inside and outside the network.
- Testing to validate any segmentation and scope-reduction controls.
- Application-layer penetration testing to include, at a minimum, the vulnerabilities listed in Requirement 6.2.4.
- Network-layer penetration tests that encompass all components that support network functions as well as operating systems.
- Review and consideration of threats and vulnerabilities experienced in the last 12 months.
- Documented approach to assessing and addressing the risk posed by exploitable vulnerabilities and security weaknesses found during penetration testing.
- Retention of penetration testing results and remediation activities results for at least 12 months."

> *Source:* **Payment Card Industry Data Security Standard Version 4.0**

Requirement 6.2.4 includes a listing of common vulnerabilities, such as SQL and other injections, buffer overflow, insecure cryptographic implementations, insecure communications, cross-site scripting, improper access controls, cross-site request forgery, broken authentication, and other "high-risk" vulnerabilities.

That section of PCI DSS provides a useful set of requirements for anyone conducting a penetration test. It's also a nice blueprint for penetration testing, even for organizations that don't have PCI DSS compliance obligations.

The standard goes on to include additional requirements that describe the frequency and scope of penetration tests:

11.4.2. Internal penetration testing is performed:

- Per the entity's defined methodology.
- At least once every 12 months.
- After any significant infrastructure or application upgrade or change.
- By a qualified internal resource or qualified external third-party.
- Organizational independence of the tester exists (not required to be a QSA or ASV).

11.4.2 External penetration testing is performed:

- Per the entity's defined methodology.
- At least once every 12 months.
- After any significant infrastructure or application upgrade or change.
- By a qualified internal resource or qualified external third-party.
- Organizational independence of the tester exists (not required to be a QSA or ASV).

11.4.4. Exploitable vulnerabilities and security weaknesses found during penetration testing are corrected as follows:

- In accordance with the entity's assessment of the risk posed by the security issue as defined in Requirement 6.3.1.
- Penetration testing is repeated to verify the corrections.

11.4.5 If segmentation is used to isolate the CDE from other networks, penetration tests are performed on segmentation controls as follows:

- At least once every 12 months and after any changes to segmentation controls/methods.
- Covering all segmentation controls/methods in use.
- According to the entity's defined penetration testing methodology.
- Conforming that the segmentation controls/methods are operational and effective and isolate the CDE from all out-of-scope systems.
- Performed by a qualified internal resource or qualified external third party.
- Organizational independence of the tester exists (not required to be a QSA or ASV).

Again, though these requirements are only mandatory for organizations subject to PCI DSS, they provide an excellent framework for any organization attempting to plan the frequency and scope of their own penetration tests. We'll cover compliance requirements for penetration testing in greater detail in Chapter 2, "Planning and Scoping Penetration Tests."

Organizations that must comply with PCI DSS should also read the detailed *Information Supplement: Penetration Testing Guidance* available from the PCI Security Standards Council at `www.pcisecuritystandards.org/documents/Penetration-Testing-Guidance-v1_1.pdf`. This document covers in great detail how organizations should interpret these requirements.

Who Performs Penetration Tests?

Penetration testing is a highly skilled discipline, and organizations often try to have experienced penetration testers for their testing efforts. Given that you're reading this book and are preparing for the PenTest+ certification, you likely already understand and recognize this.

If you don't have experience conducting penetration tests, that doesn't mean that all hope is lost. You may be able to participate in a test under the mentorship of an experienced penetration tester, or you may be able to conduct penetration testing in your organization simply because there's nobody with experience available to conduct the test.

Penetration tests may be conducted by either internal teams, consisting of cybersecurity employees from the organization being tested, or external teams, consisting of contractors.

Internal Penetration Testing Teams

Internal penetration testing teams consist of cybersecurity professionals from within the organization who conduct penetration tests on the organization's systems and applications. These teams may be dedicated to penetration testing on a full-time basis or they may be convened periodically to conduct tests on a part-time basis.

There are two major benefits of using internal teams to conduct penetration testing. First, they have contextual knowledge of the organization that can improve the effectiveness of testing by providing enhanced subject matter expertise. Second, it's generally less expensive to conduct testing using internal employees than it is to hire a penetration testing firm, provided that you have enough work to keep your internal team busy!

The primary disadvantages to using internal teams to conduct penetration testing stem from the fact that you are using internal employees. These individuals may have helped to design and implement the security controls that they are testing, which may introduce conscious or unconscious bias toward demonstrating that those controls are secure. Similarly, the fact that they were involved in designing the controls may make it more difficult for them to spot potential flaws that could provide a foothold for an attacker.

There's a bit of tricky language surrounding the use of the words *internal* and *external* when it comes to penetration tests. If you see these words used on the exam (or in real life!), be sure that you understand the context. Internal penetration tests may refer either to tests conducted by internal teams (as described in this section) or to tests conducted from an internal network perspective. The latter tests are designed to show what activity a malicious insider could engage in and may be conducted by either internal or external teams. Similarly, an external penetration test may refer to a test that is conducted by an external team or a test that is conducted from an external network perspective.

If you do choose to use an internal penetration testing team, it is important to recognize that team members might be limited by a lack of independence. If at all possible, the penetration testing team should be organizationally separate from the cybersecurity team that designs and operates controls. However, this is usually not possible in any but the largest organizations due to staffing constraints.

External Penetration Testing Teams

External penetration testing teams are hired for the express purpose of performing a penetration test. They may come from a general cybersecurity consulting firm or one that specializes in penetration testing. These individuals are usually highly skilled at conducting penetration tests because they perform these tests all day, every day. When you hire a professional penetration testing team, you generally benefit from the use of very talented attackers.

If you are subject to regulatory requirements that include penetration testing, be sure to understand how those requirements impact your selection of a testing team.

External penetration testing teams also generally bring a much higher degree of independence than internal teams. However, organizations using an external team should still be aware of any potential conflicts of interest the testers may have. It might not be the best idea to hire the cybersecurity consultants who helped you design and implement your security controls to perform an independent test of those controls. They may be inclined to feel that any negative report they provide is a reflection on the quality of their own work.

Selecting Penetration Testing Teams

Penetration testing is not a one-time process. Organizations may wish to require penetration testing for new systems upon deployment, but it is important to repeat those tests on a periodic basis for three reasons.

First, the technology environment changes. Systems are reconfigured, patches are applied, updates and tweaks are made on a regular basis. Considered in isolation, each of these changes may have only a minor impact on the environment and may not reach the threshold

for triggering a "significant change" penetration test, but collectively they may change the security posture of the environment. Periodic penetration tests have a good chance of detecting security issues introduced by those environmental changes.

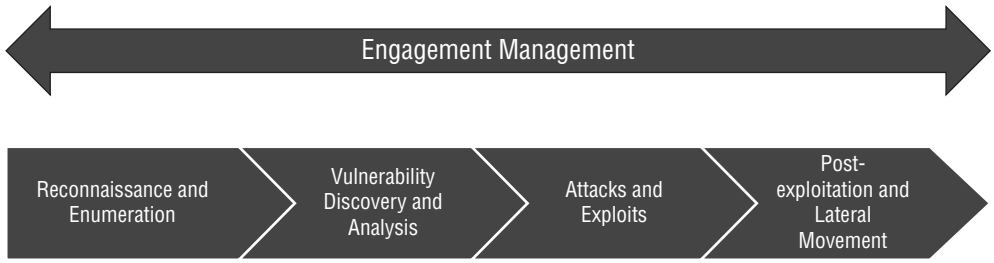
Second, attack techniques evolve over time as well, and updated penetration tests should reflect changing attack techniques. A system developed and tested today may receive a clean bill of health, but the exact same system tested two years from now may be vulnerable to an attack technique that simply wasn't known at the time of the initial test.

Finally, each team member brings a unique set of skills, talents, and experiences to the table. Different team members may approach the test in different ways, and a team conducting a follow-on test differently may discover a vulnerability that went unnoticed by the initial team. To maximize your chances of discovering these issues, you should take care when you select the members of a penetration testing team. When possible, rotating team members so they are testing systems, environments, and applications that they have never tested before helps bring a fresh perspective to each round of penetration tests.

The CompTIA Penetration Testing Process

The CompTIA PenTest+ curriculum divides the penetration testing process into five stages, as shown in Figure 1.3.

FIGURE 1.3 CompTIA penetration testing stages



This process captures the major activities involved in conducting a penetration test and will be the way that we approach organizing the content in the remainder of this book.

If you look at CompTIA's PenTest+ Certification Exam Objectives document, you'll find that there are actually five domains of material covered by the exam. The five domains shown in Figure 1.3 each map to one of the stages of the penetration testing process.

Engagement Management

The military has a saying that resonates in the world of cybersecurity: "Prior planning prevents poor performance!" Although this sentiment is true for almost any line of work, it's especially important for penetration testing. Testers and their clients must have a clear understanding of what will occur during the penetration test, outline clear rules of engagement, and decide what systems, data, processes, and activities are within the authorized scope of the test. There's a fine line between penetration testing and hacking, and a written statement of work that includes clear authorization for penetration testing activities is crucial to ensuring that testers stay on the right side of the law and meet client expectations.

Engagement management activities occur throughout the penetration test, but they do tend to be focused at the beginning and end of the process. For this reason, we cover the early-stage objectives in Chapter 2, and then we come back to the concluding objectives toward the end of the book in Chapter 11, "Reporting and Communication." Specifically, you'll learn how to meet the five objectives of this domain:

- 1.1 Summarize pre-engagement activities.
- 1.2 Explain collaboration and communication activities.
- 1.3 Compare and contrast testing frameworks and methodologies.
- 1.4 Explain the components of a penetration test report.
- 1.5 Given a scenario, analyze the findings and recommend the appropriate remediation within a report.

Reconnaissance and Enumeration

Once a penetration testing team has a clearly defined scope and authorization to proceed with their work, they move on to the reconnaissance and enumeration phase. During this stage, they gather as much information as possible about the target environment.

This information-gathering process is crucial to the remainder of the penetration test, as the vulnerabilities identified during this stage provide the road map for the remainder of the test, highlighting weak links in an organization's security chain and potential paths of entry for attackers.

We cover reconnaissance and enumeration in Chapters 3 and 12. In Chapter 3, "Information Gathering," you'll learn about the use of open source intelligence and the Nmap scanning tool. In Chapter 12, "Scripting for Penetration Testing," you will learn about scripting. Together, these two chapters cover the four objectives of this domain:

- 2.1 Given a scenario, apply information gathering techniques.
- 2.2 Given a scenario, apply enumeration techniques.
- 2.3 Given a scenario, modify scripts for reconnaissance and enumeration.
- 2.4 Given a scenario, use the appropriate tools for reconnaissance and enumeration.

As you plan your cybersecurity certification journey, you should know that there is significant overlap between the material covered in this domain and the material covered in Domain 2 (Vulnerability Management) of the Cybersecurity Analyst+ (CySA+) exam. There is also quite a bit of overlap between the basic security concepts and tools covered by both exams. If you successfully pass the PenTest+ exam, you might want to consider immediately moving on to the CySA+ exam because you'll already have mastered about a third of the material covered on that test.

Vulnerability Discovery and Analysis

Penetration testers need information about vulnerabilities to carry out the remainder of their work. After gathering information about the systems and applications on the network, they move on to identify and evaluate specific vulnerabilities that they might later exploit.

In Chapter 4, "Vulnerability Scanning," we begin a two-chapter deep dive into vulnerability scanning, perhaps the most important information-gathering tool available to penetration testers. Chapter 4 covers how testers can design and perform vulnerability scans. In Chapter 5, "Interpreting Vulnerability Scan Results," we move on to the analysis of vulnerability reports and their application to the penetration testing process.

Combined, these chapters cover two objectives from Domain 3:

- 3.1 Given a scenario, conduct vulnerability discovery using various techniques.
- 3.2 Given a scenario, analyze output from reconnaissance, scanning, and enumeration phases.

Attacks and Exploits

After developing a clear testing plan and conducting reconnaissance and vulnerability analysis activities, penetration testers finally get the opportunity to move on to what most of us consider the fun stuff! It's time to attempt to exploit the vulnerabilities discovered during reconnaissance and penetrate an organization's network as deeply as possible, staying within the bounds established in the rules of engagement.

The specific attack techniques used during a penetration test will vary based on the nature of the environment and the scope agreed to by the client, but there are some common techniques used in most tests. Half of this book is dedicated to exploring each of those topics in detail.

Chapter 7, "Exploiting Network Vulnerabilities," dives into attack techniques that focus on network devices and protocols. Chapter 9, "Exploiting Application Vulnerabilities," is about software attacks, and Chapter 10, "Exploiting Host Vulnerabilities," examines issues on servers and endpoints. Chapter 8, "Exploiting Physical and Social Vulnerabilities," reminds us that many vulnerabilities aren't technical at all and that a penetration test that gains physical access to a facility or compromises members of an organization's staff can be even more dangerous than those that arrive over a network.

Finally, Chapter 12, "Scripting for Penetration Testing," covers a topic that's extremely important to penetration testers: applying coding skills to automate aspects of a penetration test. It will introduce you to the analysis of basic penetration testing scripts written in Bash, Python, and PowerShell.

Combined, these chapters cover the following objectives:

Domain 3: Vulnerability Discovery and Analysis

- 3.3 Explain physical security concepts.

Domain 4: Attacks and Exploits

- 4.1 Given a scenario, analyze output to prioritize and prepare attacks.
- 4.2 Given a scenario, perform network attacks using the appropriate tools.
- 4.3 Given a scenario, perform authentication attacks using the appropriate tools.
- 4.4 Given a scenario, perform host-based attacks using the appropriate tools.
- 4.5 Given a scenario, perform web application attacks using the appropriate tools.
- 4.6 Given a scenario, perform cloud-based attacks using the appropriate tools.
- 4.7 Given a scenario, perform wireless attacks using the appropriate tools.
- 4.8 Given a scenario, perform social engineering attacks using the appropriate tools.
- 4.9 Explain common attacks against specialized systems.
- 4.10 Given a scenario, use scripting to automate attacks.

Post-exploitation and Lateral Movement

After successfully gaining access to target systems, penetration testers then try to move around the network during the post-exploitation and lateral movement phases of the process.

Chapter 6, "Exploit and Pivot," includes information on post-lateral movement and Chapter 11, "Reporting and Communication," explains the best practices for sharing penetration testing results with clients. Specifically, these two chapters cover the four objectives of this domain:

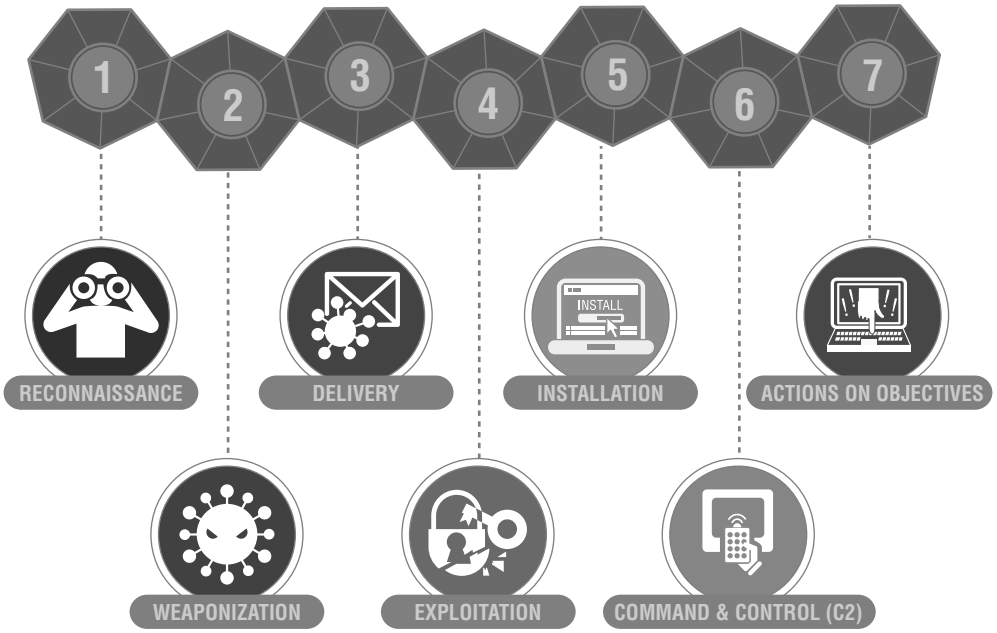
- 5.1 Given a scenario, perform tasks to establish and maintain persistence.
- 5.2 Given a scenario, perform tasks to move laterally throughout the environment.
- 5.3 Summarize concepts related to staging and exfiltration.
- 5.4 Explain cleanup and restoration activities.

The Cyber Kill Chain

The CompTIA penetration testing model described in the previous sections is an important way for penetration testers to structure their activities. There is an equally important counterpart to this model that describes how sophisticated attackers typically organize their

work: the Cyber Kill Chain framework. This approach, pioneered by Lockheed Martin, consists of the seven stages shown in Figure 1.4.

FIGURE 1.4 The Cyber Kill Chain framework



Source: Adapted from Lockheed Martin

Cybersecurity professionals seeking to adopt the hacker mindset can only do so if they understand how attackers plan and structure their work. The Cyber Kill Chain provides this framework.

Captain Chesley "Sully" Sullenberger gave a talk on his heroic landing of US Airways Flight 1549 on New York's Hudson River in January 2009. In addition to being an outstanding pilot, Sully is a noted expert on aviation safety. One portion of his talk particularly resonated with this author and made him think of the Cyber Kill Chain. When describing the causes of aviation accidents, Sully said, "Accidents don't happen as the result of a single failure. They occur as the result of a series of unexpected events."

Security incidents follow a similar pattern, and penetration testers must be conscious of the series of events that lead to cybersecurity failures. The Cyber Kill Chain illustrates this well, showing the many stages of failure that must occur before a successful breach.

Reconnaissance

The reconnaissance phase of the Cyber Kill Chain maps directly to the Reconnaissance and Enumeration phase of the penetration testing process. During this phase, attackers gather

open source intelligence and conduct initial scans of the target environment to detect potential avenues of exploitation.

Weaponization

After completing the Reconnaissance phase of an attack, attackers move into the remaining six steps, which expand on the Vulnerability Discovery and Analysis and Attacking and Exploiting phases of the penetration testing process.

The first of these phases is Weaponization. During this stage, the attackers develop a specific attack tool designed to exploit the vulnerabilities identified during reconnaissance. They often use automated toolkits to develop a malware strain specifically tailored to infiltrate their target.

Delivery

After developing and testing their malware weapon, attackers next must deliver that malware to the target. Delivery may occur through a variety of means, including exploiting a network or application vulnerability, conducting a social engineering attack, distributing malware on an infected USB drive or other media, or sending it as an email attachment or through other means.

Exploitation

Once the malware is delivered to the target organization, the attacker or the victim takes some action that triggers the malware's payload, beginning the Exploitation phase of the Cyber Kill Chain. During this phase, the malware gains access to the targeted system. This may occur when the victim opens a malicious file or when the attacker exploits a vulnerability over the network or otherwise gains a foothold on the target network.

Installation

The initial malware installation is designed only to enable temporary access to the target system. During the next phase of the Cyber Kill Chain, Installation, the attacker uses the initial access provided by the malware to establish permanent, or persistent, access to the target system. For this reason, many people describe the objective of this phase as establishing persistence in the target environment. Attackers may establish persistence by creating a back door that allows them to return to the system at a later date, by creating Registry entries that reopen access once an administrator closes it, or by installing a web shell that allows them to access the system over a standard HTTPS connection.

Command and Control

After establishing persistent access to a target system and network, the attacker may then use a remote shell or other means to remotely control the compromised system. The attacker may manually control the system using the shell or may connect it to an automated command-and-control (C2C) network that provides it with instructions. This automated approach is common in distributed denial-of-service (DDoS) attacks where the attacker simultaneously directs the actions of thousands of compromised systems, known as a botnet.

Actions on Objectives

With a C2C mechanism in place, the attacker may then use the system to advance the original objectives of their attack. This may involve pivoting from the compromised system to other systems operated by the same organization, effectively restarting the Cyber Kill Chain.

The Actions on Objectives stage of the attack may also include the theft of sensitive information, the unauthorized use of computing resources to engage in denial-of-service attacks or to mine cryptocurrency, or the unauthorized modification or deletion of information.

Tools of the Trade

Penetration testers use a wide variety of tools as they conduct their testing. The specific tools chosen for each assessment will depend on the background of the testers, the nature of the target environment, and the rules of engagement, among many other factors.

The PenTest+ exam requires that candidates understand the purposes of a wide range of tools. In fact, the official exam objectives include listings of tools that you'll need to understand before taking the exam. Although you must be familiar with these tools, you don't have to be an expert in their use.

Exam Tip

As you prepare for the exam, you should certainly understand the purpose of each tool. You should be able to describe the purpose of each of these tools in a coherent sentence. Additionally, you should be able to read a scenario and perform related tasks using relevant tools, summarize concepts, or explain activities for meeting objectives. Keep this in mind as you work your way through the remainder of this book!

Summary

Penetration testing is an important practice that allows cybersecurity professionals to assess the security of environments by adopting the hacker mindset. By thinking like an attacker, testers are able to identify weaknesses in the organization's security infrastructure and potential gaps that may lead to future security breaches.

The CompTIA penetration testing process includes five phases: Engagement Management, Reconnaissance and Enumeration, Vulnerability Discovery and Analysis, Attacks and Exploits, and Post-exploitation and Lateral Movement. Penetration testers follow each of these phases to ensure that they have a well-designed test that operates using agreed-upon rules of engagement.

Penetration testers use a wide variety of tools to assist in their work. These are many of the same tools used by cybersecurity professionals, malicious actors, network engineers, system administrators, and software developers. Tools assist with all stages of the penetration testing process, especially information gathering, vulnerability identification, and exploiting vulnerabilities during attacks.

Exam Essentials

Know how the CIA and DAD triads describe the goals of cybersecurity professionals and attackers. Cybersecurity professionals strive to protect the confidentiality, integrity, and availability of information and systems. Attackers seek to undermine these goals by achieving the goals of disclosure, alteration, and denial.

Be able to name several important benefits of penetration testing. Penetration testing provides knowledge about an organization's security posture that can't be obtained elsewhere. It also provides a blueprint for the remediation of security issues. Finally, penetration tests provide focused information on specific attack targets.

Understand that penetration testing may be conducted to meet regulatory requirements. The Payment Card Industry Data Security Standard (PCI DSS) requires that organizations involved in the processing of credit card transactions conduct both internal and external penetration tests on an annual basis.

Describe how both internal and external teams may conduct penetration tests. Internal teams have the benefit of inside knowledge about the environment. They also operate more cost-effectively than external teams. External penetration testers have the benefit of organizational independence from the teams who designed and implemented the security controls.

Know the five phases of the penetration testing process. Penetration testers begin in the Engagement Management phase, where they develop a statement of work and agree with the client on rules of engagement. They then move into reconnaissance efforts during the

Reconnaissance and Enumeration phase. The information collected is then used to discover vulnerabilities in the Vulnerability Discovery and Analysis phase and conduct attacks during the Attacks and Exploits phase. After the final phase, Post-exploitation and Lateral Movement, the team shares its findings with the target organization.

Describe the tools used by penetration testers. Tools designed for use by cybersecurity professionals and other technologists may also assist penetration testers in gathering information and conducting attacks. Penetration testers use specialized exploitation frameworks, such as Metasploit, to help automate their work.

Lab Exercises

Activity 1.1: Adopting the Hacker Mindset

Before we dive into the many technical examples throughout this book, let's try an example of applying the hacker mindset to everyday life.

Think about the grocery store where you normally shop. What are some of the security measures used by that store to prevent the theft of cash and merchandise? What ways can you think of to defeat those controls?

Activity 1.2: Using the Cyber Kill Chain

Choose a real-world example of a cybersecurity incident from recent news. Select an example in which there is a reasonable amount of technical detail publicly available.

Describe this attack in terms of the Cyber Kill Chain. How did the attacker carry out each step of the process? Were any steps skipped? If there is not enough information available to definitively address an element of the Cyber Kill Chain, offer some assumptions about what may have happened.