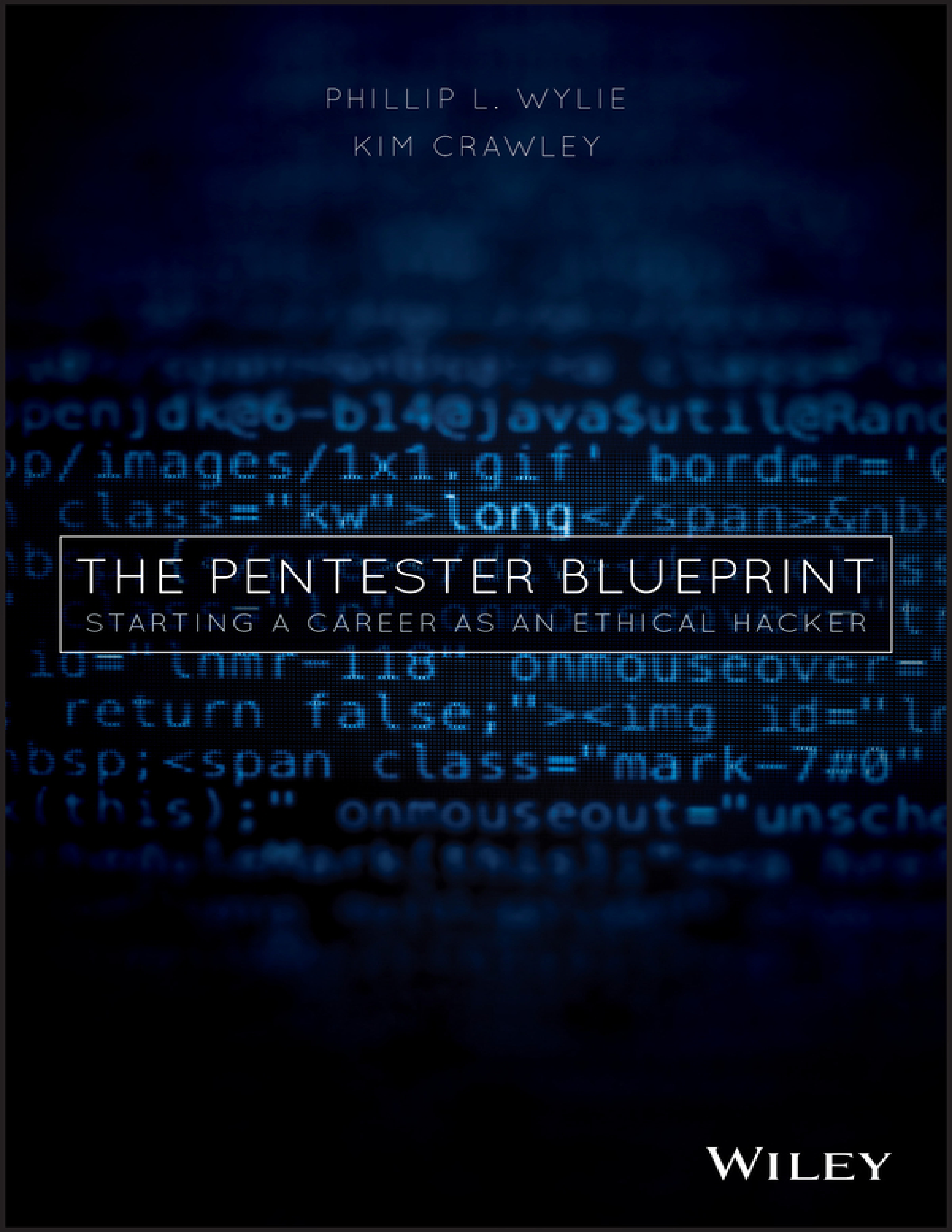
PHILLIP L. WYLIE

KIM CRAWLEY



THE PENTESTER BLUEPRINT

STARTING A CAREER AS AN ETHICAL HACKER

WILEY

Table of Contents

List of Tables

Chapter 7

List of Illustrations

Chapter 3

The Pentester Blueprint

Starting a Career as an Ethical Hacker

Phillip L. Wylie

Kim Crawley

WILEY

Foreword

I'd say the most coveted positions in cybersecurity and information technology as a whole are roles as penetration testers, or *pentesters*, also known as *ethical hackers*. I want to emphasize the ethical part of that last sentence. There are many that go down the path of self-study, trying to get into the field, who end up crossing the line into unethical and even illegal behavior.

Remember always to use your superpowers for good. Funny enough, when people find out that I'm an ethical hacker, many ask me to break into something for them. They also ask how they can learn what I know so that they can get a cool job. I certainly will point them to two books that I co-authored with Jennifer Jin, *Tribe of Hackers: Cybersecurity Advice from the Best Hackers in the World* and *Tribe of Hackers Red Team: Tribal Knowledge from the Best in Offensive Cybersecurity,* both published by Wiley in 2019, to which my friends Kim Crawley and Phillip Wylie contributed.

If I were to point someone trying to get into this line of work, I'd most certainly point them to Phillip Wylie. Phillip is the only person I know that can teach you how to break into a company ethically for security purposes and to have wrestled a bear and lived to talk about it. Like many of our backgrounds, Phillip's was unique and something that should be embraced. There is no one correct path to be a penetration tester.

Phillip continues to pay it forward by helping tons of people to learn about ethical hacking and volunteering hundreds of hours helping people learn. You will learn a lot from this book, and I'm going to ask you a favor: Please pay it forward and help someone else by teaching them something that you already know or learn from this book which can help them out.

I just want to thank Phillip for being such a blessing to so many people. I hope you learn a lot or even fill in some blanks in your knowledge. I wish you an abundance of success on your journey.

Marcus J. Carey
Creator of Tribe of Hackers Series

Introduction

The Pentester Blueprint was born from ethical hacker Phillip Wylie's excellent pentesting curriculum of the same name. Whether or not you're able to attend one of the many workshops and classes that Phil gives every year, this book will teach you not only how to become a pentester but also how to become a successfully employed pentester! By reading this book, you have started the journey on your ethical hacking career. The future looks bright for you!

How I Became a Pentester

> *“My journey to becoming a pentester started with my first IT job as a system administrator. In my previous career as a draftsman, I learned about the system administrator role. It intrigued me and seemed more interesting that creating drawings on AutoCAD. I taught myself how to build computers and about a year later I took a certified NetWare engineer (CNE) certification course and learned the Novell NetWare network operating system. Not long after completing the course I got my first system administrator job and spent a little over six years in that IT discipline. I got interested in information security three years into my system administrator career and later moved into a network security role at the company where I worked. One and a half years later I became part of a newly formed two person application security team. I got to learn how to use web application vulnerability scanners and learned about penetration testing, which became my next career move. Almost seven years later I was part of a layoff and was fortunate enough to land my first penetration testing job working as a consultant for a cyber security consulting company. That was the start of my eight and a half penetration testing career.”*

Who Should Read This Book

This book is for individuals of all ages who are considering a career in the pentesting field. All genders and walks of life can appreciate this book, as long as you can develop the hacker mindset! Of course, we will explain that mindset to you and help you out every step of the way. Whether you already work in IT or you haven't worked with computers professionally before, we've done our best to make our ideas accessible to you.

What You Will Learn

Pentesting requires not only computer technology skill but also practical thinking. Most of your work will be with computers and their networks, but not all of it! Pretending to be a con artist and lockpicking can also be useful skills for an ethical hacker, as malicious cyberattackers also fool human beings and physically penetrate buildings.

We'll teach you how to do some of that cool Hollywood hacking stuff for real, but only with consenting targets. Most importantly, we'll also show you how you can get hired to do that sort of work!

We share our expertise, but we also made sure to get ideas from many other gainfully employed pentesters in this book. You will benefit from our wide range of experiences and what we've learned while being “good hackers” in real life.

How This Book Is Organized

We strongly recommend that you read this book in a linear fashion, because each new chapter builds upon the previous chapter.

Chapter 1: What Is a Pentester?

In this chapter, we introduce you to the concept of pentesting. Why do companies need pentests? How will your work help to improve your clients' security? There are also different types of pentesting, which we will summarize within this chapter.

Chapter 2: Prerequisite Skills

Here we explain the computer technical skills that you'll need before you focus on learning ethical hacking skills. These skills pertain to operating systems and computer networking. We also explain a wide range of cybersecurity concepts. All areas of cybersecurity are interconnected, so understanding them is essential.

Chapter 3: Education of a Hacker

In this chapter, we explain the general ethical hacking skills that you'll need in your pentesting career. We also introduce the hacker mindset and the Pentester Blueprint Formula!

Chapter 4: Education Resources

Next we explain how you can continue to learn about pentesting after you've read this book. We recommend specific books and training programs. The pentesting lab you'll build in the next chapter also helps.

Chapter 5: Building a Pentesting Lab

Here we explain how you can build your very own pentesting lab, both in the comfort of your own home and in forms that you can take with you on the go. We'll explain how to simulate hacking systems and targets.

Chapter 6: Certifications and Degrees

There are many certifications and resources available that can help you become an employed pentester. We'll explain which ones are the most important in this chapter.

Chapter 7: Developing a Plan

Here we will help you analyze which skills you already have and figure out those skills that you'll need to acquire.

Chapter 8: Gaining Experience

Getting a job can be a chicken-and-egg problem. You can't get a job without experience, and you can't get experience without a job! We'll explain how you can avoid that trap.

Chapter 9: Getting Employed as a Pentester

Now that you have some ethical hacking experience, we'll show you how to become employed as a pentester.

How to Contact the Authors

You can find Phillip Wylie online at:

LinkedIn: www.linkedin.com/in/phillipwylie

Twitter: twitter.com/PhillipWylie

You can find Kim Crawley online at:

LinkedIn: www.linkedin.com/in/kimcrawley

Twitter: twitter.com/kim_crawley

If you believe you have found an error in this book, and it is not listed on the book's page at www.wiley.com, you can report the issue to our customer technical support team at support.wiley.com.

1
What Is a Pentester?

What is a pentester? Although the term may have you thinking of someone who works in quality assurance for an ink pen manufacturing plant, it's actually short for “penetration tester.” Pentesters are commonly known as *ethical hackers*.

When you think of the term penetration tester, it makes more sense when you think about someone trying to penetrate the security of a computer, a network, the building in which a network is located, or a website. While the term ethical hacker is a little easier to understand, people are surprised to hear that such a job exists. *Pentesters* assess the security of computers, networks, and websites by looking for and exploiting vulnerabilities–commonly known as *hacking*.

To be clear, not all hackers are bad. Nevertheless, the terms hacker and hacking have been vilified for many years. Ethical hackers use their skills for good to help uncover vulnerabilities that could be exploited by malicious hackers.

The hackers you hear about in the news who are committing crimes should be labeled as cyber criminals. While they are using hacking to commit illegal activities, the intent and purpose of their efforts should be distinguished from pentesting, which is a way to see how cyberattackers can exploit a network for the benefit of security.

Before we get further into the topic, consider the wisdom of a particular philosopher:

With great power comes great responsibility.

François Voltaire

You will need permission to hack; otherwise, it would be considered illegal. This quote is a good way to ingrain that message. Prior to starting a pentest, written permission must be obtained.

Synonymous Terms and Types of Hackers

Various terms are synonymous with pentesters and malicious hackers, and we will discuss them to help you understand what each means. The following terms are often used interchangeably and are useful to know.

The most common types of hackers are known as white hat, gray hat, and black hat hackers. These terms were taken from old westerns, where hats were used as a descriptor to tell the good guys from the bad guys:

> **White hat hackers** Ethical hackers (aka pentesters).
>
> **Gray hat hackers:** Gray hats fall into a fuzzy area. Their intent is not always malicious, but it is not always ethical either.
>
> **Black hat hackers:** Their intent and purpose are illegal. Cyber criminals fall into this category.

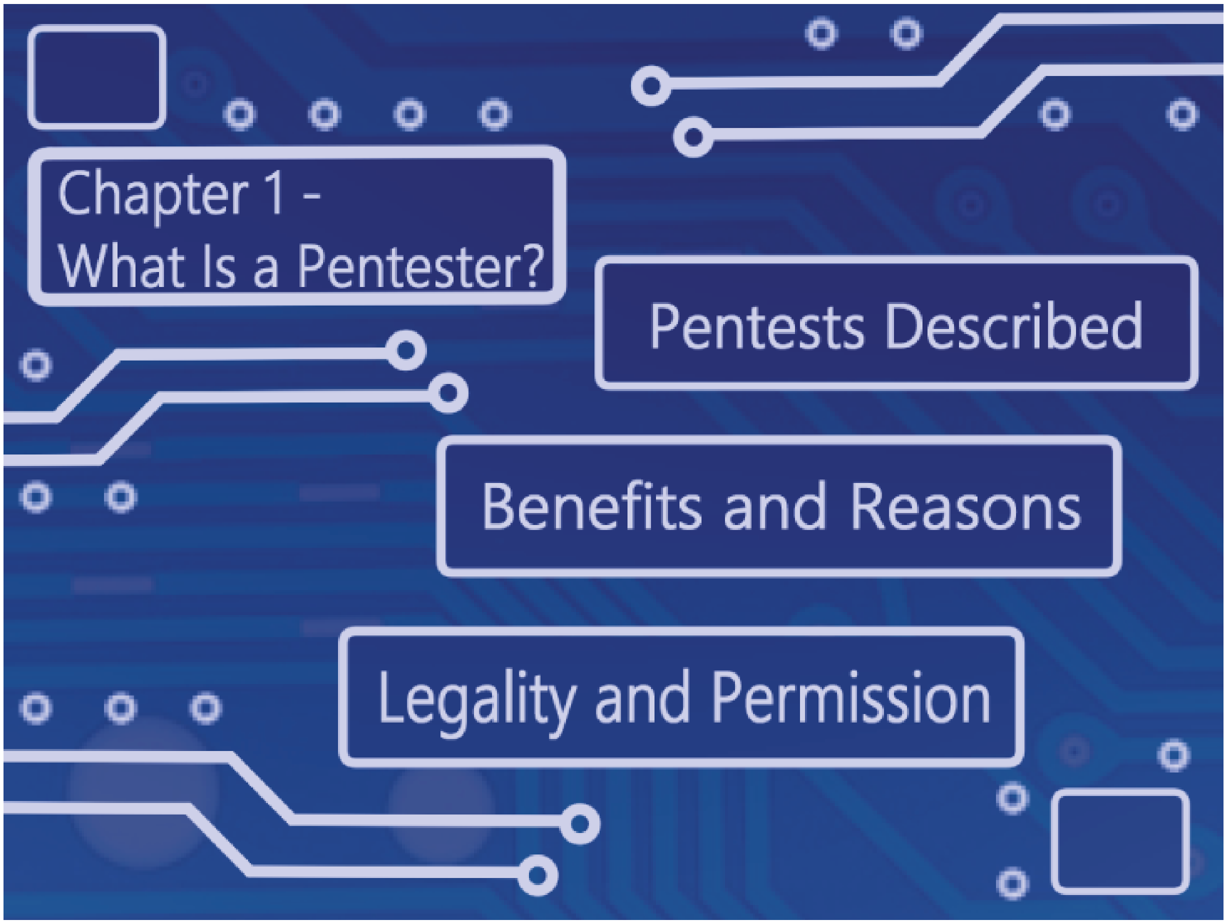
Other commonly used terms for pentesting and pentesters include ethical hackers, offensive security, and adversarial security.

Pentesters are sometimes referred to as the *red team*, and defensive security is referred to as the *blue team*. Although red team is used for offensive security in general, true red teams perform adversarial simulation to emulate malicious hackers and test the blue team. Sometimes companies will also have a purple team. Mix red and blue and you get purple! A *purple team* is simply a small group of people who help to facilitate communication between the red team and blue team. The red team finds vulnerabilities and exploits, and the blue team uses the red team's findings to security harden their networks.

There are also commonly used terms for malicious hackers. Out of respect for good hackers, it is advised that you use these terms rather than the generic term “hacker”:

- Threat actor
- Cyber criminals
- Black hat hackers, or black hats for short

Another way that hacking is used is through *hacktivism*. *Hacktivists* are activists that use their hacking skills to support social change, human rights, freedom of speech, or environmental causes. These are still cyberattacks. Even though the hacktivists' motivation may be to help a good cause, these activities are still illegal.



Pentests Described

Pentests assess security from an adversarial perspective. This type of security assessment is the only way to uncover exploitable vulnerabilities and understand their risks. Vulnerability scanning alone or running an application to find vulnerabilities in targeted computers and devices only detects limited vulnerabilities, and by successfully exploiting or hacking the discovered vulnerabilities, it is possible to find ones that would have otherwise gone undetected.

This approach to security testing allows pentesters to mimic a malicious hacker in order to traverse the complex layers of systems to detect vulnerabilities beneath the surface. A vulnerability scan alone misses exploitable security flaws that are only visible on the surface of the system. Getting past the initial system layer allows you to assess security to see how far an attacker could get into your system, or to see if the possibility exists to access and compromise other systems or networks.

Pentesters use similar, or sometimes the same, tactics, techniques, and procedures (TTPs) as are used by cyber criminals. The emulation of an adversary can vary with the type and scope of a test, which we will cover in greater depth in the sections that follow. Pentests are performed on a variety of computers and networking devices. As humans are often fooled in order to conduct cyberattacks, sometimes you may be asked to test them as well. As technology evolves, newer technologies can become targets for testing. Too seldom, security is an afterthought when it should be considered up-front in the design phase.

Benefits and Reasons

The benefits and reasons for conducting pentests have become more recognized by private- and public-sector organizations, and the need to conduct them continues to grow. A decade ago, pentests were typically performed by consultants or contractors. Most companies did not employ their own pentesters, but as the need increased, more companies built their own pentesting teams.

The benefit of pentesting is that it provides a view of the security posture from an adversary's point of view. As we discussed, the best way to understand how an adversary sees security is to have a pentest performed.

Some of the most common reasons for pentests are as follows:

- Discovering and remediating vulnerabilities in order to mitigate possible breaches.

- Regulatory compliance is a major driver for companies to conduct pentests. Of course, this should not be the only reason—security should be the main purpose. Nonetheless, Payment Card Industry-Data Security Standard (PCI-DSS) and General Data Protection Regulation (GDPR) are two major regulations. They pertain to payment systems ranging from those seen in brick-and-mortar stores to those implemented in ecommerce.

Knowledge of pentesting techniques is helpful to more than just pentesters. Understanding how malicious hackers think, as well as the TTPs used by cyber criminals, are helpful to defenders in all areas of information security.

Some areas that can benefit from an understanding of pentesting are as follows:

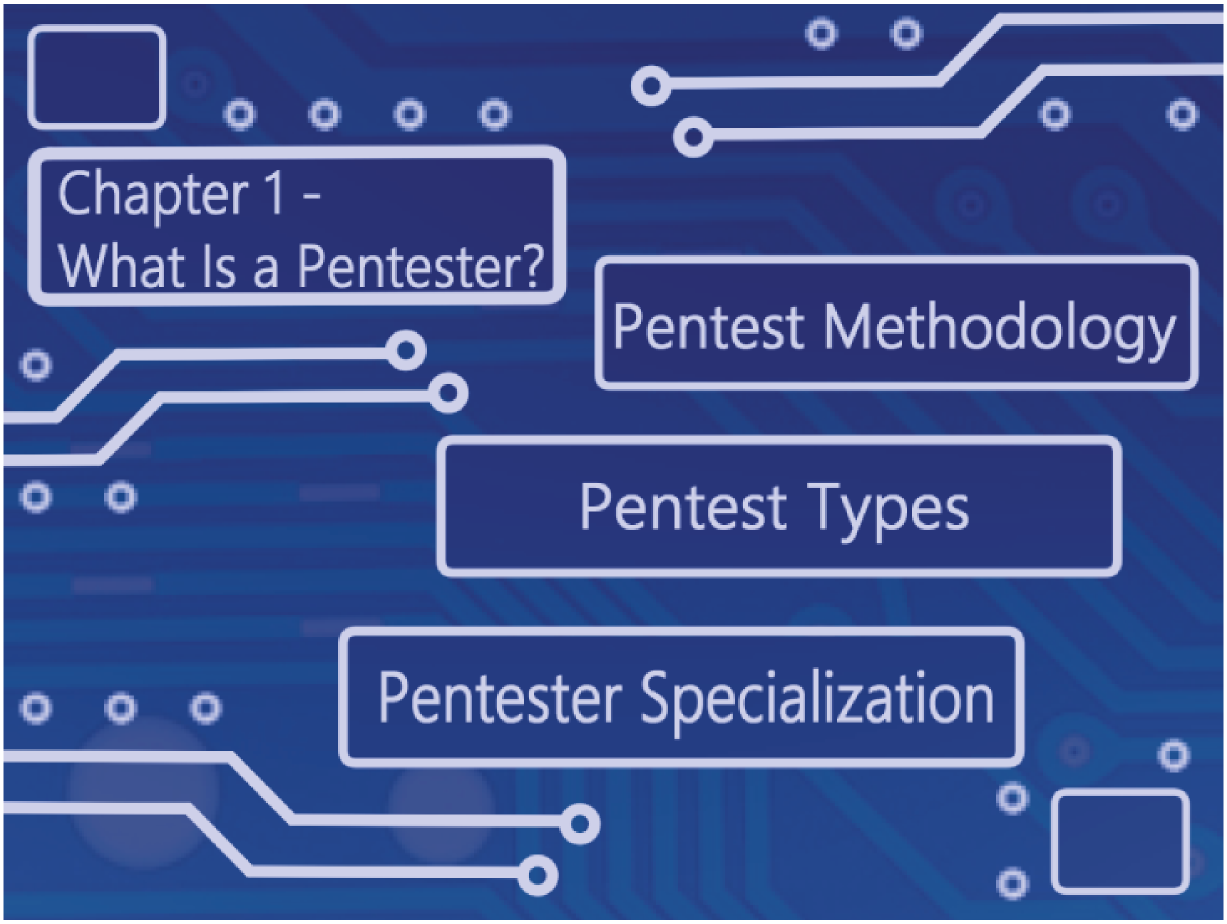
- Security operations center (SOC) analysts
- Network security analysts and engineers
- Digital forensics and incident response (DFIR)
- Purple teams (a collaboration of defensive and offensive security)
- Application security

SOC analysts and network security personnel can better understand malicious network traffic with pentesting knowledge. DFIR investigators benefit from understanding cyberattacks, which can be learned from pentesting. Purple teams attack and defend digital assets, so pentesting knowledge is essential. Pentesting is useful for application security analysts, and it can be used to assess and secure applications. Knowledge of pentesting is useful throughout all areas of information security. This knowledge is helpful in defending networks, computing platforms, applications, and other technology assets. Understanding pentesting is useful for those working with pentesters. An educated consumer can better select consultants or contractors to conduct pentests or to hire permanent staff for pentesting.

Legality and Permission

Hacking is illegal without permission, so getting written permission prior to starting a pentest is absolutely necessary. Without it, if the pentest causes an outage or damage to a system, it could lead to legal problems. Without written permission, it's the pentester's word against the client’s.

The *statement of work* (*SOW*) should include verbiage giving pentesters permission to perform the pentest. It is important that the pentest adhere to a well-defined scope in order to prevent legal problems and customer dissatisfaction. Such permission can also include a document referred to as a *get-out-of-jail-free card*, which can offer legal protection if you make certain mistakes within the scope defined by the SOW. This is especially necessary when performing pentests against buildings, as it may be useful when being questioned by building security or law enforcement.



Pentest Methodology

A methodology is required in order to provide consistent and thorough pentests. A pentest methodology ensures that all of the steps were completed during a pentest. A *pentest methodology* is a repeatable process that other pentesters on a team can duplicate to deliver consistent quality. Methodologies are especially important when training new pentesters, giving them a checklist to follow that helps them make sure that they complete all of the required steps in a pentest.

The following list contains some common industry-recognized pentesting methodologies:

Penetration Testing Execution Standard (PTES): www.pentest-standard.org

Open Source Security Testing Methodology Manual (OSSTMM): www.isecom.org/OSSTMM.3.pdf

NIST 800-115 (National Institute of Standards and Technology): csrc.nist.gov/publications/detail/sp/800-115/final

OWASP Testing Guide (Open Web Application Security Project): www.owasp.org/images/1/19/OTGv4.pdf

Of the pentest methodologies listed here, the *OWASP Testing Guide* focuses on web application pentests and is the industry standard for those types of pentests. The first three methods are widely used and referenced in books and courses, and some organizations use a combination of these methodologies. Pentest reports and SOWs often document the methodology and the tools used during pentests.

The *Penetration Testing Execution Standard (PTES)* contains the seven main sections of a pentest, which cover all of the required steps of a pentest. Not only does the PTES offer a comprehensive methodology, but PTES offers technical guidelines at www.pentest-standard.org/index.php/PTES_Technical_Guidelines.

The PTES technical guidelines detail procedures to follow during a pentest. The guidelines are a good reference for tools, resources, and tasks. We will go into more detail of the PTES methodology, since it is the most commonly used one. PTES is the result of a collaboration of some of the most respected and knowledgeable information security practitioners in the industry.

The seven sections of the PTES are as follows:

1. Pre-engagement Interactions

2. Intelligence Gathering
3. Threat Modeling
4. Vulnerability Analysis
5. Exploitation
6. Post Exploitation
7. Reporting

These are summarized in the following sections. For more detail, see the PTES website at `www.pentest-standard.org`.

Pre-engagement Interactions

This is the planning phase, and it introduces the tools and techniques to be used during the pentests. The scope of a pentest is defined during this phase, as well as the cost, beginning and ending times, and allowed testing times. Pentesting has the potential to cause outages, so testing times need to be agreed upon with the client, and the hours for testing and start and end dates for the pentest should be included in the SOW. Questionnaires are used to help define the scope of the pentest and to plan it. The goals of the pentest should be discussed during this phase, and understanding them is helpful in scoping a successful pentest. The rules of engagement should be determined, which define how the pentest is to be done.

Intelligence Gathering

In this phase, intelligence is gathered on targets to discover vulnerabilities and information that can be used to exploit the target. Information like operating system (OS) and software versions are useful in determining if a target is vulnerable and exploitable. Other types of intelligence gathering could require finding out information about individuals, companies, and organizations through the

Internet. Intelligence gathering is also referred to as *reconnaissance* and *Open Source Intelligence* (*OSINT*).

Threat Modeling

Threat modeling is a process by which potential threats, such as software or OS vulnerabilities, can be identified, enumerated, and prioritized—all from a hypothetical attacker's point of view. The purpose of threat modeling in pentesting is to provide a systematic analysis of the probable attacker's profile, the most likely attack vectors, and the assets most desired by an attacker. This information is used to attack the target. Threat modeling is especially important on more complex targets, and can be more difficult and time-consuming.

Vulnerability Analysis

Vulnerability analysis is the process of discovering flaws in systems and applications that can be leveraged by an attacker. These flaws can range anywhere from host and service misconfiguration to insecure application design. Tools such as port and service scanners and vulnerability scanners are used to discover vulnerabilities. The discovered vulnerabilities are validated to ensure that they are truly vulnerable and not false positives, and then analyzed to verify if they can be exploited. Note that not all vulnerabilities are exploitable, but they should be included in the report. Vulnerabilities that are not exploitable at the time of the pentest could exploited later if an exploit is developed.

Exploitation

This phase of a pentest focuses solely on hacking vulnerable systems detected during the vulnerability analysis phase of the pentest. There are many different things that you could do in this phase, which will depend on what you're testing, and the scope defined in your SOW. It can include using vulnerability scanners, attempting attacks on web applications, trying to access areas of buildings where outsiders aren't permitted, trying to fool human beings, and various other activities that may be attempted by real cyberattackers. Occasionally, you may have to use your imagination, but be sure only to try what is allowed according to your contract! Chapter 5, “Building a Pentesting Lab,” will explain the many actions you'll take in this phase in much greater detail.

Post Exploitation

The purpose of this phase is to determine the *value* of the compromised system and to maintain control for later use. The value of the system is determined by the sensitivity of the data stored on it and its usefulness in further exploiting other systems.

Reporting

This phase of the pentest is where the results and findings are documented. The *pentest report* should have an executive summary where the results are communicated in language that can be understood by nontechnical staff. This section of the report is important for explaining the results to management and the various business lines of the organization. Information on vulnerabilities should be documented, reporting on systems that were exploitable and providing details and evidence of the exploitation. Screenshots and ample evidence should be provided to show proof of the vulnerabilities and exploited systems. Recommendations and remediation information, as well as risk ratings for vulnerabilities, should also be contained in the report.

Pentest Types

When a pentest is performed, pentesters are provided with information on the targets that they are testing. This target knowledge can range from minimal information to a great deal of information. You might know absolutely nothing about the system that you're testing, or you might be as familiar with your target as a network administrator! Three main categories define the depth of information provided:

Black box: The target knowledge for this type of pentest is very limited. For a web application, it is typically just the URL of the application. In the case of a network pentest, it can be an IP address or list of IP addresses. In some cases, the pentester may only know the company name, and it is up to the pentester to use reconnaissance to discover IP addresses or URLs to assess. Black box pentests mimic a malicious hacker more than the other methods.

White box: Also referred to as a c*rystal box* pentest, in this type of pentest, the pentester is provided with a lot of detailed information on the target being tested. This information can include documents, diagrams, and the user credentials of different user permissions levels. You want to make sure that a normal user of the application cannot access administrative functions.

Gray box: This type of target knowledge falls between black box and white box testing. Gray box pentests are the most common type of the three. The amount of knowledge that you'll have could be anywhere between the extremes of the ignorance of an outsider up to the familiarity of a network administrator. For instance, you might start with as much knowledge of the network as a company insider who doesn't work in the IT department.

Time can be a factor in deciding between black box, white box, and gray box pentests. The more information the pentester has about the target, the more thoroughly the target can be assessed, so this situation is where a white box pentest would be selected. White box pentests also decrease the time needed to perform a pentest. The less knowledge of the target, the longer the testing time required. The black box pentest requires more reconnaissance, which can add to the amount of time needed to perform the pentest. Gray box pentests are in the middle of the two other methods. Web applications are a type of target that benefit from white box pentests because so many of their vulnerabilities exist in their backends, which aren't obvious from the frontends you see in your web browser.

Vulnerability Scanning

Vulnerability scanning is often part of a pentest, but it is not required. Pentesters can manually discover vulnerabilities without using a vulnerability scanner. Vulnerability scanning is often a job role in a threat and vulnerability management program. *Vulnerability scanners* are used to detect specific vulnerabilities that are publicly known and for which programmers have developed tests, and can help speed up the vulnerability discovery process. Scheduled recurring vulnerability scanning should be part of a threat and vulnerability management program. Vulnerability scanners are an important tool in a pentester's toolbox, and one of the first steps in a pentest. Following are some common vulnerability scanners:

- *Nessus* (`www.tenable.com/products/nessus`) is a vulnerability scanner by Tenable.

- *Nexpose* (www.rapid7.com/products/nexpose) is a vulnerability scanner offered by Rapid7, the creators of the Metasploit exploitation tool.
- *Openvas* (www.openvas.org) is a vulnerability scanner by Greenbone Networks, which offers a free and commercial version of Openvas.
- *Qualys* (www.qualys.com) offers a VMDR cloud-based vulnerability scanner. It's sold through paid subscription, and it is efficient to use, as Qualys's own cloud handles the computing load.

Vulnerability Assessments

Pentests are a type of security assessment, and so are security vulnerability assessments. Sometimes, security vulnerability assessments are requested instead of pentests in order to reduce the risk of a system outage. All of the steps of a pentest are completed except for exploitation (aka hacking). Security vulnerability assessments are a good starting place for junior or entry-level pentesters.

SECURITY VULNERABILITY ASSESSMENT EXAMPLE

One example where a vulnerability assessment was favored over a pentest occurred when I was doing a Wi-Fi pentest for a hospital. The client expressed concern about Wi-Fi-connected medical devices, fearing that an outage or disruption could endanger the health of their patients. Thus, a security vulnerability assessment with a Wi-Fi controller security configuration review was performed instead of a pentest.