1

Introduction to Ethical Hacking

Cybersecurity is one of the most exciting and rapidly growing fields in the world. Each day, security professionals and researchers are discovering new and emerging threats at an increasing rate, and many organizations are discovering that their systems and networks have been compromised by malicious actors, while there are so many other companies without proper cyber defenses to detect threats and determine whether their assets have been compromised or not. Due to the increase in cyber-attacks and threats around the world, more cybersecurity-related jobs are being created within many organizations that seek to acquire industry experts and skilled professionals who can help improve their cyber defenses and safeguard their assets from cyber criminals. This book is designed with the intention of providing you with the skills, knowledge, and wisdom that are needed by aspiring ethical hackers and penetration testers for the cybersecurity industry.

During the course of this book, you will develop new skills and learn techniques for simulating real-world cyber-attacks on systems and networks as a cybersecurity professional with the intent to discover hidden security vulnerabilities within organizations, while understanding the **Tactics, Techniques, and Procedures**

(**TTPs**) used by real attackers to compromise their targets. In addition, you will learn how to leverage one of the most popular Linux distributions within the cybersecurity industry, **Kali Linux**, to perform ethical hacking and penetration testing assessments on targeted systems and network infrastructure. The Kali Linux operation system has tons of pre-installed Linux packages (applications) and security tools that are commonly used by industry experts, hence it's an arsenal packed with everything you'll need as an ethical hacker and penetration tester. Throughout this book, we'll be using a student-centric and learner-friendly approach, filled with a lot of practical and hands-on exercises to help you gradually progress from beginner-friendly to intermediate and advanced topics.

In this chapter, you will learn about various types of threat actors and the intentions/motives behind their attacks on targets. You will discover how various key factors play an important role for attackers when planning a cyber-attack, and how such factors determine the level of complexity to compromise a targeted system, network, or organization as compared to cybersecurity professionals such as ethical hackers and penetration testers who are hired to discover hidden vulnerabilities within a company. Furthermore, you will learn about the various phases of ethical hacking and penetration testing approaches that are commonly used by industry professionals.

Lastly, you will gain a solid understanding of how the **Cyber Kill Chain** framework is used to help cybersecurity professionals to better understand cyber-attacks, and how each phase can be aligned with penetration testing techniques.

In this chapter, we will cover the following topics:

- Understanding the need for cybersecurity
- Exploring the importance of penetration testing
- Identifying threat actors and their intent
- Understanding what matters to threat actors
- Exploring the importance of penetration testing
- Penetration testing methodologies
- Discovering penetration testing approaches
- Types of penetration testing
- Exploring the phases of penetration testing
- Understanding the Cyber Kill Chain framework

I hope you're as excited as I am to begin this awesome journey. Let's dive in!

Understanding the need for cybersecurity

Cybersecurity focuses on protecting systems, networks, and organizations from specialized attacks and threats that are designed by cyber criminals with the intention to cause harm or damage. These cyber criminals are commonly referred to as **threat actors**. As time continues, more users and organizations are connecting their systems and networks to the largest network in the world, the internet, and cyber criminals are developing new strategies to steal money from potential victims.

For instance, many cyber criminals are developing more sophisticated threats, such as **ransomware**. Let's use this example to underscore the importance of cybersecurity. Ransomware is a type of crypto-malware that's designed to encrypt all data found on a victim's system, except the host operating system. The intention is to encrypt the victim's most valuable asset on the compromised system, the data stored on local storage media, and request a ransom payment in the form of cryptocurrencies to obtain the decryption keys to recover the data. The longer the ransomware is on a compromised system, the ransomware agent could establish a **Command and Control** (**C2**) communication channel with one or more C2 servers that are owned and managed by cyber criminals to receive updates and additional instructions. The threat actor can push updates to the ransomware agent to frequently update the cryptographic keys that are used to encrypt the victim's data – therefore, reducing the likelihood that the victim is able to safely recover their data from the ransomware. During this time, the threat actor is also exfiltrating the data found on the victim's system and selling it on various marketplaces on the *Dark Web* to the highest bidder. Cyber criminals are intelligent; they are very aware that organizations know the value of data that is stored on their computers and servers, and will do almost anything to recover their data as soon as possible.

NOTE

Ransomware has the capability of also compromising the data stored in various cloud storage services that are linked to the infected system. For instance, imagine a user's system has a cloud storage agent running to ensure the user's data is constantly synchronized. If the system is infected with ransomware, the infection will encrypt all data on the local storage drives, including those that are synchronized to the cloud service provider platform. However, various cloud storage providers have built-in protection against these types of threats.

From a cybersecurity perspective, it's not recommended to pay the ransom as there's no guarantee or reassurance that the threat actors will release the encrypted data or even provide the right decryption key to recover your data. It is important to note that threat actors are not only demanding ransom payment by encrypting data but also by threatening to expose organizational and customer sensitive data by releasing it or onto pastedump sites such as pastebin.com and to the media. This "doubling-down" on the pressure applied makes it difficult for victims not to cave into the ransomware gangs' demands.

For instance, there are many organizations around the world with a reactive approach to cybersecurity, such that they will only react when their systems and network are compromised by a cyber-attack rather than implementing mitigation and countermeasures to prevent future threats. However, if an organization does not implement proper cyber defenses with an effective incident response plan, when ransomware compromises a vulnerable system within a network, it has the potential to automatically spread to other vulnerable systems within the organization to expand its foothold. Therefore, the longer it takes to contain/isolate the threat on the network, the more damage can be done.

NOTE

While working on the previous edition of this book, the technical reviewer, Mr. Rishalin Pillay, mentioned that during his time at

Microsoft, he had seen how attackers “may” give the decryption key to victims; however, the threat actors mostly implant additional malware to return later for more cash gains. Essentially, the targeted organization becomes a “cash cow” for the threat actors (attacking group).

Therefore, without cybersecurity professionals, researchers, and security solutions, many organizations and users are left unprotected from various types of threats. For instance, many banks provide an online banking system that enables their customers to perform various types of transactions such as making payments, transferring funds, and so on. Imagine if cyber criminals discovered weak security controls on a bank’s customer login portal and found a way to take advantage of the security weakness to gain unauthorized access to multiple customers’ accounts, steal their **Personally Identifiable Information** (**PII**), and transfer funds out of their accounts. Therefore, safeguarding customer data is crucial, not only to protect individuals from immediate financial loss but also to prevent their information from being used in future cyber-attacks.

In the next section, you will learn about common security-related terminology in the industry.

Exploring cybersecurity terminology

During your journey in the field of cybersecurity, you’ll discover the jargon and terminology that is commonly used within various research papers, articles, literature, discussions, and learning resources. As an aspiring cybersecurity professional, it's important to be aware of and gain a solid understanding of common terminology and how it is related to ethical hacking and penetration testing.

The following are the most common terms used within the cybersecurity industry:

- **Asset** – Within the field of cybersecurity, we usually define an asset to be anything that has value to an organization or person. For instance, assets are systems within a network that can be interacted with and potentially expose an organization's network infrastructure to security weaknesses that could be compromised and enable unauthorized access to a cyber criminal, while providing a way to escalate their privileges on the compromised system from standard user to administrator-/root-level privileges. However, it's important to mention that assets are not and should not be limited to technical systems. In addition, other forms of assets include people (humans), physical security controls, and even the data that resides within the network and systems we aim to protect. Assets are commonly categorized as follows:
  - **Tangible** – Tangible assets are simply described as any physical object with value, such as computers, servers, networking devices (routers, switches, etc.), and security appliances (firewalls). Computers and other end devices help typical users and employees access the resources on a network and perform their daily duties within an organization. Servers are typically used to store and host applications and provide services that are needed within typical network infrastructures. Networking devices contain configurations that are used to forward network traffic between systems, and security appliances are implemented to filter unwanted traffic and prevent

    threats between networks and systems. If these systems and devices are compromised, cyber criminals will be able to redirect network traffic to malicious websites that are owned by malicious actors and expand their operations.
  - **Intangible** – Intangible assets are things without a physical form that have value, such as applications, software license keys, intellectual property, business plans and models, and data.
  - **People** – This type of asset is the customers and employees of an organization. Protecting customers' data from being stolen and leaked on the *Dark Web*, and safeguarding employees from various types of threats are of paramount importance. It is important to identify all the assets of an organization and potential threats that can cause harm and damage to them.
- **Threat** – In the context of cybersecurity, a threat is anything that has the potential to cause harm or damage to a system, network, or person. Whether you're focusing on the offensive or defensive path in cybersecurity, it's important to identify various types of threats. Many organizations around the world encounter different types of threats each day, and cybersecurity teams work around the clock to ensure their company's assets are safeguarded from cyber criminals.

  One of the most exciting but also overwhelming aspects of cybersecurity is industry professionals always need to stay one step ahead of threat actors to quickly find security weaknesses in systems, networks, and applications and implement countermeasures to mitigate any potential threats those assets.

- **Vulnerability** – A vulnerability is a security weakness or flaw that exists within a system that enables hackers to exploit it in order to gain unautho-

rized access or control over systems within a network. Common vulnerabilities that exist within organizations include human error (the greatest of vulnerabilities on a global scale), misconfiguration of devices, weak user credentials, poor programming practices, unpatched operating systems, outdated applications on host systems, default against configurations on systems, and so on.
A threat actor usually looks for the *lowest-hanging fruits* such as the vulnerabilities that are the easiest to exploit on a targeted system. The same concept applies to penetration testing. During a security assessment, the penetration tester will use various techniques and tools to discover vulnerabilities and will attempt to exploit the easy ones before moving on to more complex security flaws on a targeted system.

- **Exploit** – An exploit is anything such as a tool or code that is used to take advantage of security vulnerabilities on a system. For instance, take a hammer, a piece of wood, and a nail. The vulnerability is the soft, permeable nature of the wood, the exploit is the act of hammering the nail into the piece of the wood, while the hammer is the threat. Once a security vulnerability is found on a targeted system, the threat actor or penetration tester will either acquire an exploit from various online sources or develop one on their own that has the capability of taking advantage of the security weakness.
  If you've acquired or developed an exploit, it's important that you test the exploit on a system to ensure it has the capabilities to compromise the targeted system and works as expected. Sometimes, an exploit may work on one system and not on another. Hence, it's a common practice that seasoned penetration testers will test and ensure their exploits are working as expected and graded on their rate of success for a vulnerability.

- **Attack** – An attack is simply a method or technique that is used by a threat actor to take advantage of (exploit) a security vulnerability (weakness) within a system. There are various types of attacks that are commonly used by cyber criminals to compromise the confidentiality, integrity, and/or availability of a targeted system. For instance, the LockBit 3.0 ransomware focuses on exploiting the security vulnerabilities that are found on internet-facing systems that do not have their language settings configured to match a specific exclusion list. The attack launches ransomware on the internet; it will automatically seek and compromise vulnerable systems.

  NOTE

  To learn more about the LockBit 3.0 ransomware, please see the official **Cybersecurity and Infrastructure Security Agency** (**CISA**) advisory at https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-075a.

- **Attack vector** – An attack vector is simply an area or pathway through which a targeted system, network, or organization can be compromised by a threat actor.

  The following are common attack vectors:

  - **Direct access** – Physical access to the targeted computer or network
  - **Wireless** – Exploiting security vulnerabilities found within the target's wireless network infrastructure
  - **Email** – Sending malicious email messages containing links to malware-infected services, fake websites, and malicious attachments

  - **Supply chain** – Compromising the security of a vendor or supplier to gain access to a target
  - **Social media** – Using deceptive messages or **malicious advertising** (**malvertising**) to trick the target into revealing sensitive information or downloading a malicious file
  - **Removable media** – Connecting malware-infected media to the targeted system
  - **Cloud** – Exploiting security vulnerabilities within cloud services and its infrastructure

  These are the infrastructures in which an attacker can deliver a malicious payload to a target.

- **Risk** – Risk is the potential impact that a vulnerability, threat, or attack presents to the assets of an organization and the likelihood an attack or threat has to cause harm systems. Evaluating risk helps to determine the likelihood of a specific issue causing a data breach that will cause harm to an organization's finances, reputation, or regulatory compliance. Reducing risk is critical for many organizations. There are many certifications, regulatory standards, and frameworks that are designed to help companies understand, identify, and reduce risks.

While it may seem like ethical hackers and penetration testers are hired to simulate real-world cyber-attacks on a target organization, the goal of such engagements is much deeper than it seems. At the end of the penetration test, the cybersecurity professional will present all the vulnerabilities and possible solutions to help the organization mitigate and reduce the risk of a potential cyber-attack while reducing the attack surface of the company.

- **Attack surface** – This is all the vulnerable points of entry into a system, network, or organization that can be exploited by a threat actor to gain unauthorized access and expand their foothold on the network. Ethical hackers and penetration testers focus on identifying these vulnerability points of entry to determine the attack surface of an organization and how a cyber criminal would potentially exploit those weaknesses to compromise their target.
- **Zero-day** – A zero-day is when a threat actor discovers a security vulnerability within a product or application and is able to exploit it before the vendor is either aware of the vulnerability or has time to develop a security patch to resolve the issue. These attacks are commonly used in nation-state attacks, **Advanced Persistent Threat** (**APT**) groups, and large criminal organizations. The discovery of a zero-day vulnerability can be very valuable to ethical hackers and penetration testers and can earn them a bug bounty. These bounties are fees paid by vendors to security researchers who discover unknown vulnerabilities in their applications.

  There are many bug bounty programs that allow security researchers, professionals, and anyone with the right skill set to discover security vulnerabilities within an application or system owned by a vendor and report them for a reward. The person who reports the security vulnerability, usually a zero-day flaw, is often given a financial reward. However, there are threat actors who intentionally attempt to exploit the targeted system for personal gain, which is commonly referred to as the *hack value* of the target.

So far, you have learned about the importance and need for cybersecurity within various industries around the world. Next, let's learn about various types of threat actors and the motives behind their cyber-attacks.

Identifying threat actors and their intent

As an aspiring ethical hacker and penetration tester, it's important to develop a good moral compass and understand the differences between various types of threat actors and the motives behind their cyber-attacks. Let's take a closer look at the following list of common types of threat actors in the cybersecurity industry:

- **Script kiddie** – A script kiddie is a common type of threat actor who is not necessarily a young adult or kid. Rather, it is someone who does not fully understand the technical details of cybersecurity to perform a cyber-attack or develop a threat on their own. However, a script kiddie usually follows the instructions or tutorials of real hackers to perform their own attacks against a targeted system or network.

  While you may think a script kiddie is harmless because the person does not have the required knowledge and skills, they can create an equal amount or more damage as real hackers, simply by following the instructions and tutorials of malicious actors on the internet. This type of hacker makes use of tools for which they do not know how they properly work, thus causing more harm and damage.

- **Cyber terrorist** – Cyber terrorists perform cyber-attacks that are designed to compromise communication channels and systems, with the intention to cause enough damage and disruption to create fear and/or intimidate a targeted society to achieve an ideological goal.
- **Hacktivist** – Across the world, there are many social and political agendas in many countries, and there are many persons and groups who are either supportive or not supportive of these agendas. You will commonly find protesters

who organize rallies and marches or even perform illegal activities such as the defacement of public property.

This is a type of threat actor who uses their hacking skills to perform malicious activities such as defacing websites or launching **Denial of Service** (**DoS**) attacks in support of a political or social agenda. While some hacktivists use their hacking skills for good reasons, keep in mind that hacking is still an illegal act and the threat actor can face legal action by law enforcement. Therefore, ethical hackers and penetration testers are required to obtain legal permission prior to performing any attacks on the target.

- **Insider** – Many threat actors know it's more challenging to break into an organization through the internet and it's easier to do it from within the targeted organization's network. Some threat actors will create a fake identity and curriculum vitae with the intention of applying for a job within their targeted organization and becoming an employee; this threat actor is commonly referred to as a *malicious insider*. Once this type of threat actor becomes an employee, the person will have access to the internal network and gain better insights into the network architecture and security vulnerabilities of the company. Therefore, this type of threat actor can implement network implants on the network and create backdoors for remote access to critical systems.

Note

Network implants can be software- or hardware-based. Software-based network implants are malicious code that is installed and running on a compromised system that enables the threat actor to remotely access and control the target. However, hardware-based

> network implants are physical devices that are directly connected to the target's internal network, enabling the attacker to remotely connect to the hardware-based network implant and perform attacks. These network implants are commonly used for monitoring, control, and data exfiltration.

In addition, there are *unintentional insiders* who are the legitimate employees of the organization who unintentionally cause harm to the organization's systems and network due to negligence such as connecting a personal USB flash drive onto the organization's computer.

- **State-sponsored** – This type of threat actor is commonly referred to as a **nation-state actor**. While many nations will send their army of soldiers to fight a war, many battles are now fought within cyberspace (including espionage, disruption, influence operations, and preparing the battlefield for potential physical conflicts); this is known as *cyber warfare*. Many nations have realized the need to develop and enhance their cyber defenses to protect their citizens, national assets, and critical infrastructure from cyber criminals and other nations with malicious intent.
  Therefore, a government may hire state-sponsored hackers who are responsible for performing reconnaissance (intelligence gathering) on other countries and protecting their own country from cyber-attacks and emerging threats. Some nations use this type of threat actor to gather intelligence on other countries and even compromise the systems that control the infrastructure of public utilities or other critical resources. Keep in mind that state-sponsored threat actors are not only employed by governments but can also include groups or

individuals funded, directed, or aligned and supported by national governments.

> **Note**
>
> Cyber espionage involves the stealthy extraction of classified, sensitive, or proprietary information. This can include technological blueprints, government plans, or even personal information of key individuals.

- **Organized crime** – Around the world, we commonly read and hear about many crime syndicates and organized crime groups. Within the cybersecurity industry, there are also crime organizations made up of a group of people with the same goals in mind. Each person within the group is usually an expert or has a specialized skill set, such as one person may be responsible for performing extensive reconnaissance on the target, including additional roles such as social engineering experts, network penetration specialists, malware analysts, money laundering specialists, and legal advisors. Each role contributes to the syndicate's success by leveraging specific expertise.
  When this level of effort and resources is brought to bear, the group becomes an **APT**. Within this organized crime group, there is usually a person who is responsible for financially funding the group to provide the best available resources money can buy to ensure the attack is successful. The intention of this type of threat actor is usually big, such as stealing their target's data and selling it for financial gain.

- **Black hat** – A black hat hacker is a threat actor who uses their hacking skills for malicious reasons. This is a broad category; these hackers can be anyone and their reason for performing a hack against a targeted system or network can be random. Sometimes they may hack to destroy their target's reputation, steal data, or even as a personal challenge to prove a point for fun.
- **White hat** – White hat hackers form another broad category, encompassing the industry's good people. This type of hacker uses their skills to help organizations and people secure their networks and safeguard their assets from malicious hackers. Ethical hackers and penetration testers are examples of white hat hackers as these people use their skills to help others in a positive and ethical manner.
- **Gray hat** – A gray hat hacker metaphorically sits between the boundary of a white hat and a black hat hacker. This means the gray hat hacker has a hacking skill set and uses their skills to help people and organizations during the day as a cybersecurity professional but uses their skills at night for malicious reasons. As previously mentioned, ethical hackers and penetration testers have a good moral compass, but gray hat hackers go outside the good moral zone and may use their skills for malicious intentions.

With the continuous development of new technologies, the curious minds of many will always find a way to gain a deeper understanding of the underlying technologies of a system. This often leads to discovering security flaws in the design and eventually enabling a person to exploit the vulnerability. Having completed this section, you have discovered the characteristics of various threat actors and their intentions for performing a cyber-attack. Next, you will gain a deeper understanding of what matters to threat actors when planning a cyber-attack on a target.

Understanding what matters to threat actors

From a cybersecurity perspective, hacking into a system or device has always been interesting and fascinating to many people around the world. Reverse engineering a system to better understand how it works has always attracted curious minds. Similarly, hacking focuses on gaining a better understanding of how a system operates and functions, whether there are any flaws within its programming or design, and whether these security flaws can be exploited to alter the functionality of the system to enable the curious mind to take advantage of it.

However, before a cyber criminal launches any attack on a targeted organization, it's important to plan the attack and evaluate the time and resources that are needed to perform the cyber-attack. Furthermore, the complexity of the attack and the hack value of the target help the threat actor determine whether it's worth moving forward with the plan of attack or not.

Time

Determining the amount of time it will take from gathering information about the target to meeting the objectives of the attack is important. Sometimes, a cyber-attack can take a threat actor anything from days to a few months of careful planning to ensure each phase of the *Cyber Kill Chain* is successful when executed in the proper order. We will discuss this further in the *Understanding the Cyber Kill Chain framework* section later in this chapter.

Threat actors also need to consider the possibility that an attack or exploit might not work on the targeted system and this will create an unexpected delay during the process, which increases the time taken to meet the goals of the hack. The time to achieve objectives is not just about gaining access but also what happens afterward, such as maintaining persistence, lateral movement, and data exfiltration.

Similarly, this concept can be applied to both ethical hackers and penetration testers as they need to determine how long it will take to complete a penetration test for a customer and present a report with the findings and security recommendations to help the customer improve their security posture.

Resources

Without the right set of resources, it will be a challenge to complete a task. Threat actors need to have the right set of resources; these are software- and hardware-based tools. While skilled and seasoned hackers can manually discover and exploit security weaknesses in targeted systems, it can be a time-consuming process. However, using the right set of tools can help automate these tasks and improve the time taken to find security flaws and exploit them. Additionally, without the right skill set, a threat actor may experience some challenges in being successful in performing the cyber-attack. This can lead to seeking the support of additional persons with the skills needed to assist and contribute to achieving the objectives of the cyber-attack. Once again, this concept can be applied to security professionals such as penetration testers within the industry. Not everyone has the same skills and a team may be needed for a penetration test security assessment for a customer.

Financial factors

Another important resource is financial factors. Sometimes a threat actor does not need any additional resources and can perform a successful cyber-attack and compromise their targets. However, there may be times when additional software- or hardware-based tools are needed to increase the potential of compromising the target. Having a budget allows the threat actors to purchase the additional resources needed. Similarly, penetration testers are well-funded by their employers to ensure they have access to the best tools within the industry to excel at their jobs.

Hack value

Finally, the hack value is simply the motivation or the reason for performing a cyber-attack against a targeted system, network, or organization. For a threat actor, it’s the value of accomplishing the objectives and goals of compromising the system. Threat actors may not target an organization if they think it’s not worth the time, effort, or resources to compromise its systems. Other threat actors may target the same organization with another motive.

Having completed this section, you have learned about some of the important factors that matter to threat actors prior to performing a cyber-attack on an organization. In the next section, you will discover the importance of penetration testing and how it helps organizations improve their cyber defenses.

Exploring the importance of penetration testing

Each day, cybersecurity professionals are in a race against time with threat actors in discovering vulnerabilities in systems and networks. Imagine that threat actors are able to exploit a security vulnerability on a targeted system before a cybersecurity professional can find it and implement security controls and countermeasures to mitigate the threat. The longer cybersecurity professionals take to identify hidden security flaws in systems, the more time threat actors have to improve their cyber operations, exploit their targets, and expand their foothold on a compromised network. This would leave the cybersecurity professional to perform incident handling and response to contain and eradicate the threat and recover any compromised systems back to an acceptable working state.

Organizations are realizing the need to hire white hat hackers such as ethical hackers and penetration testers with the skills needed to simulate real-world cyber-attacks on their systems and networks to discover and exploit hidden vulnerabilities and better understand the TTPs of cyber criminals. Furthermore, penetration testing helps organizations improve their incident response plans, enhances their security posture, and creates a culture of continuous improvement in cybersecurity practices.

These techniques enable the ethical hacker and penetration tester to perform the same type of attacks as a real hacker; the difference is the penetration tester is hired by the organization and has been granted legal permission to conduct such intrusive security testing.

Note

Penetration testers usually have a strong understanding of computers, operating systems, networking, and programming, as well as how these technologies work together. Most importantly, you need creativity. Creative thinking enables a person to think *outside the box*, go beyond the intended uses of technologies, and find new and exciting ways to implement them.

At the end of the penetration test, both an executive and technical report are presented to the organization's stakeholders detailing all the findings, such as vulnerabilities and how each weakness can be exploited. The reports also contain recommendations on how to mitigate and prevent a possible cyber-attack on each vulnerability found. This allows the organization to better understand what type of information and systems a hacker will discover if they are targeted and the countermeasures that are needed to reduce the risk of a future cyber-attack. Some organizations will even perform a second penetration test after implementing the recommendations outlined in the penetration test reports to determine whether all the vulnerabilities have been fixed, whether the security controls are working as expected to mitigate the threats, and whether the attack surface is reduced. By providing feedback to the organization's security team, the interaction ensures that security vulnerabilities are better understood and the recommendations are feasible and effective within the context of the organization’s mission.

Penetration testing methodologies

Many learners are eager and excited to get started with learning about ethical hacking and penetration testing, and can’t wait to compromise their first targeted system. Some would be too eager and may overlook the fundamentals or forget to perform an important step during a process to reach their objectives. As a result, the desired outcome may not be achieved for this reason. Hence, various penetration testing methodologies help ethical hackers and penetration testers take a specific course of action during security assessments to ensure all in-scope systems, networks, and applications are thoroughly tested for security vulnerabilities.

The following are common penetration testing methodologies/frameworks:

- **Penetration Testing Execution Standard** (**PTES**)
- **Payment Card Industry Data Security Standard** (**PCI DSS**)
- **Penetration Testing Framework** (**PTF**)
- Technical Guide to Information Security Testing and Assessment
- Open Source Security Testing Methodology Manual
- OWASP Web Security Testing Guide
- OWASP Mobile Security Testing Guide
- OWASP Firmware Security Testing Methodology

As shown in the preceding list, there are various penetration testing methodologies that can be applied to organizations based on their operating industry, category of business, the goals of performing ethical hacking and penetration testing, and the scope of the security assessment.

> To learn more about each penetration testing methodology, please see **https://owasp.org/www-project-web-security-testing-guide/latest/3-The_OWASP_Testing_Framework/1-Penetration_Testing_Methodologies**.

To better understand the importance of each phase of penetration testing, let's take a closer look at the PTES methodology as it is applicable to many scenarios.

Pre-engagement phase

During the pre-engagement phase, key personnel are selected. These individuals are key to providing information, coordinating resources, and helping the penetration testers understand the scope, breadth, and rules of engagement in the assessment. This phase also covers legal requirements, which typically include a **Non-Disclosure Agreement** (**NDA**) and a **Consulting Services Agreement** (**CSA**).

The following is a typical process overview of what is required prior to the actual penetration testing:

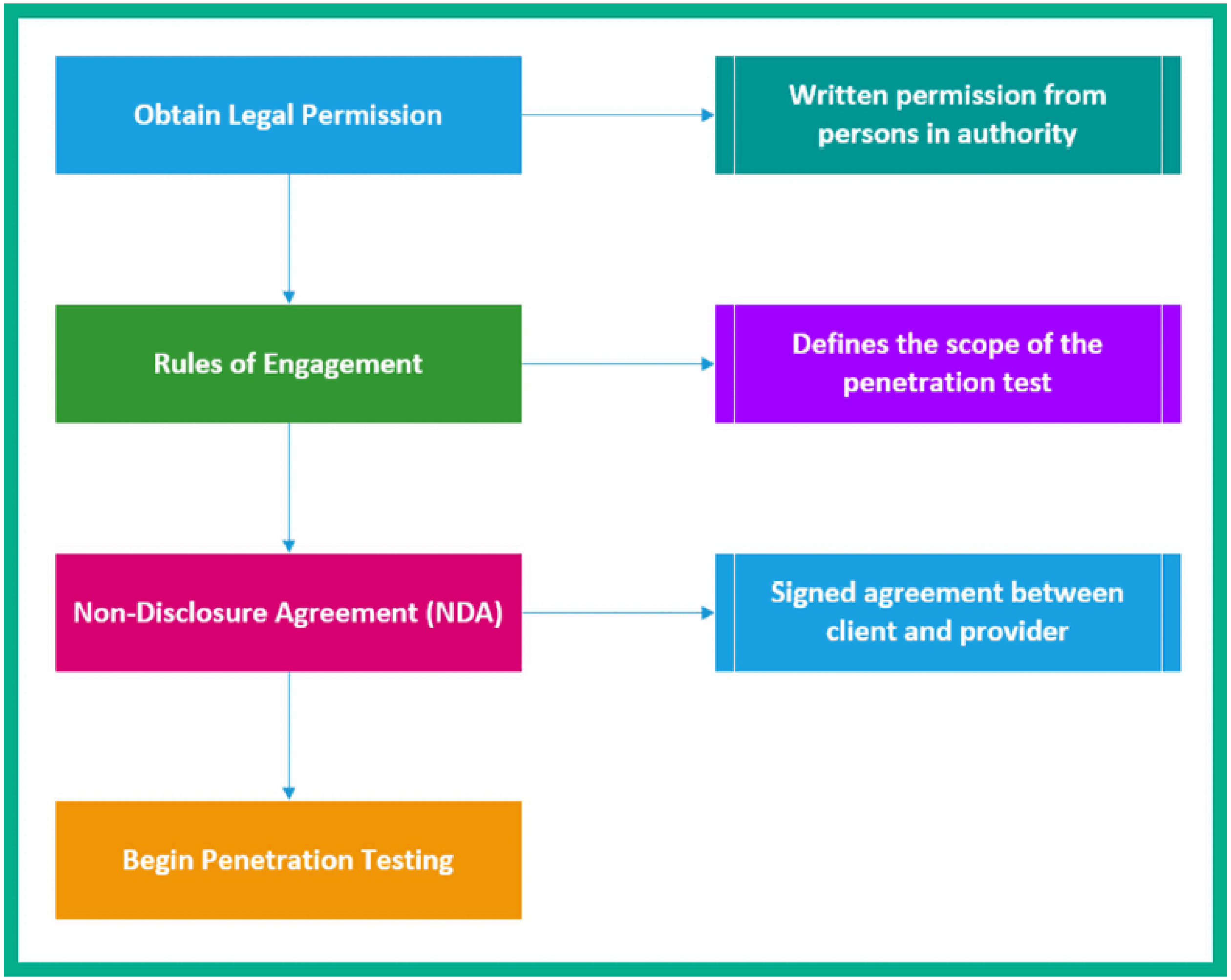
Obtain Legal Permission
Written permission from persons in authority
Rules of Engagement
Defines the scope of the penetration test
Non-Disclosure Agreement (NDA)
Signed agreement between client and provider
Begin Penetration Testing

Figure 1.1: Pre-engagement phase elements

As shown in the previous diagram, it’s important to obtain legal permission from the persons who are in authority at the targeted organization. This is simply your *get-out-of-jail card* in the event that law enforcement is contacted to investigate a possible cyber-attack during the time of the penetration test at the organization. Next, the rules of engagement can be coupled with the CSA. The CSA is a contractual agreement between the service provider who is offering penetration testing services and the customer. The CSA defines the terms and conditions of work to be performed, which includes the work schedule timelines, scope of work, deliverables, payment terms, and more prior to starting any work on the customer's systems and networks.

An NDA is a legal agreement that specifies that a penetration tester and their employer will not share or hold onto any sensitive or proprietary information that is encountered during the assessment. This is important to the customer as the penetration tester will be accessing their systems and may find confidential information. Companies usually sign these agreements with cybersecurity companies who will, in turn, sign them with the employees who are working on the project. In some cases, companies sign these agreements directly with the penetration testers from the company carrying out the project.

The scope of a penetration test, also known as the *rules of engagement*, defines the systems and networks the penetration tester is authorized to perform security assessments on. The scope should be directly aligned with the testing objectives to ensure the relevance and effectiveness of the assessment.

In other words, it defines what the penetration tester is permitted and not permitted to hack, and whether there are any restricted tools and attacks. This ensures the penetration tester remains within legal boundaries. This is a mutual agreement between the client (customer) and the service provider (penetration tester). It also defines sensitive systems and their IP addresses as well as testing times, and which systems require special testing time-windows. It's incredibly important for penetration testers to pay close attention to the scope of a penetration test and the location they are testing in order to always stay within the testing constraints.

The following are some general pre-engagement questions to help you define the scope of a penetration test:

- What is the size/class (IP addresses and/or network blocks) of the external network? (Network penetration testing)
- What is the size/class (IP addresses and/or network blocks) of the internal network? (Network penetration testing)
- What is the purpose and goal of the penetration test? (Applicable to any form of penetration testing)
- How many site pages does the web application have? (Web application penetration testing)

This is not an extensive list of pre-engagement questions, and all engagements should be given thorough thought to ensure that you ask all the important questions so you don't *under-scope* or under-price the security assessment.

Now that you've understood the legal limitation stages of penetration testing, let's move on to learn about the information-gathering phase and its importance.

Information-gathering phase

Penetration testing is a lot like real-world hacking with the exception the penetration tester is limited to the scope and time allocated for the security assessment to be completed. Therefore, like a real cyber-attack, penetration testers need to perform sufficient reconnaissance to collect information from various data sources to create a profile about the targeted organization and identify security vulnerabilities. Information gathering is essential to ensure that penetration testers have access to key information that will assist them in successfully conducting their security assessments.

A seasoned professional will normally spend a day or two conducting extensive reconnaissance on their target. The more knowledge that is known about the target, the better the penetration tester will be able to identify the attack surface, such as points of entry in the targeted systems and networks. Additionally, this phase also helps the penetration tester identify the employees, infrastructure, and geolocation for physical access, network details, servers, and other valuable information about the targeted organization.

Understanding the target is very important before launching any type of attack as a penetration tester, as it helps in creating a profile of the potential target and determining which types of attacks are most effective based on the attack surface. Additionally, recovering user credentials/login accounts in this phase, for instance, will be valuable in later phases of penetration testing as it will help ethical hackers and penetration testers gain access to vulnerable systems and networks.

Threat modeling

Threat modeling is a process used to assist penetration testers and network security defenders to better understand the threats that inspired the security assessment or the threats that applications or networks are most prone to. This data is used to help penetration testers simulate, assess, and address the most common threats that an organization, network, or application faces.

Overall, threat modeling helps organizations and cybersecurity professionals better understand and evaluate the cyber risks and threats that have the potential to negatively affect the assets of a company. In addition, it helps cybersecurity professionals determine the potential each threat has to successfully compromise an asset, together with the likelihood and the ability of the organization to respond to a security incident.

The following are common threat models:

- **Spoofing identity, tampering with data, repudiation threats, information disclosure, denial of service, and elevation of privilege** (**STRIDE**)
- **Process for attack simulation and threat analysis** (**PASTA**)

Let's assume we want to perform threat modeling for an online banking system from a cybersecurity perspective using STRIDE:

- **Spoofing identity** – As a threat, the malicious actor can attempt to impersonate the identity of a legitimate user to gain unauthorized access to the online banking portal. For mitigation, the bank can implement **multi-factor authentication** (**MFA**) to improve the verification process of legitimate users.
- **Tampering with data** – As a threat, a malicious actor can attempt to intercept and alter sensitive financial data that is being transmitted, causing unauthorized transfer of funds from the victim's account. As a mitigation, the bank can implement end-to-end data encryption technologies such as using digital cer-

tificates and signatures to protect the data and its integrity during transmission.

- **Repudiation threats** – As a threat, a threat actor can perform a DoS attack on the bank's online platform to deny any legitimate requests from authorized and trusted users. This would create a potential financial loss in transactions performed by the online banking system. As a mitigation technique, the cybersecurity team of the bank can implement transactional logging systems to record each user's transaction on the platform and to further validate that each transaction is associated with a unique identifier such as a digital signature to enforce non-repudiation, where a user cannot deny their action on a system.
- **Information disclosure** – As a threat, the customer's sensitive data can be exposed to unauthorized persons, either through a security vulnerability within the bank's database or insecure API technologies and implementation. For mitigation, the bank can implement security access controls and data encryption technologies to the web application and its database.
- **Denial of service** – As a threat, the malicious actor can flood unsolicited request messages to the bank's online system, causing the system resources of the hosting server to be overwhelmed and become unavailable to process legitimate requests from authorized users. As a mitigation, the bank can implement CAPTCHA technologies and **intrusion prevention systems** (**IPSs**) to detect and prevent malicious network traffic.
- **Elevation of privileges** – As a threat, the malicious actor may exploit a web application vulnerability on the bank's online portal to escalate their privileges and obtain unauthorized access to administrative areas of the online banking system. As a mitigation, implementing the principle of least privileges helps

ensure that users have only the minimum level of access needed to perform their tasks. Furthermore, regular auditing of users' privileges helps in recognizing suspicious activities.

Let's perform threat modeling for the online banking system using PASTA:

1. **Define the objectives** – Ensuring the information security and technologies of the online banking system to protect the customers' data, preventing financial fraud, and sustaining the availability of the system to users. It's important to establish the goals of this phase such as identifying any potential threats and vulnerabilities that can compromise the online banking system.
2. **Define technical scope** – The online banking system may include web and mobile applications, backend database servers and hosting services, third-party vendor technology integration, and usage of **application programming interfaces** (**APIs**). The technical scope focuses on identifying the technical boundaries of the system for analysis that may be susceptible to cyber-attacks and threats.
3. **Decompose the application** – Identifying and documenting various components, data flows, and functionality within the online banking system. It's important to break down the online banking system into different parts to better understand its architectures and dependencies. This information helps you better understand the attack surface that an attacker can exploit to gain unauthorized access to the system.
4. **Analyze the threats** – Performing threat analysis to identify potential threats and attack scenarios that can be used to exploit security vulnerabilities in the online banking system. This stage focuses on developing ideas and analyzing

how a threat actor can identify and exploit security vulnerabilities in the system.

5. **Vulnerability analysis** – Identifying and assessing the security vulnerabilities found in the online banking system that can be exploited by a malicious actor. This phase is performed using code analysis, vulnerability scanning, and assessment tools.
6. **Attack analysis** – Simulating real-world cyber-attacks based on the identified security vulnerabilities and potential threats that can compromise the system. This phase involves creating the attack scenario and using the TTPs that real threat actors employ to compromise their targets.
7. **Risk and impact analysis** – This phase focuses on evaluating the risk (likelihood) and potential impact each identified cyber threat would have on compromising the online banking system.

> To learn more about threat modeling and various frameworks, please see **https://www.crowdstrike.com/cybersecurity-101/threat-modeling/**.

Having understood the importance and need for threat modeling, the next step is to perform a vulnerability assessment on the assets to further determine the risk rating and severity.

Vulnerability analysis

During the vulnerability analysis phase, the ethical hacker or penetration tester performs both manual and automated testing on targeted systems to identify hidden and unknown security flaws. Identifying security vulnerabilities within systems helps organizations better understand the attack surface, which is the vulnerable point of entry within their systems and network infrastructure. While many organizations implement and use automated vulnerability scanning tools, it's also recommended to perform manual testing to determine whether a security vulnerability exists on a system and how it can be exploited by a real adversary, hence the need for penetration testing.

Furthermore, the vulnerability analysis helps the stakeholders and decision-makers in the organization better determine how to allocate resources to higher-priority systems. For instance, many automated vulnerability scanners provide a vulnerability score between 0 (lowest) and 10 (most severe) for each security flaw found on a system. The vulnerability scores can help organizations determine which security vulnerability on a system requires more attention and higher priority due to the potential impact if the vulnerability were to be exploited by an adversary. However, not all vulnerabilities with high scores are equally critical in every context. The criticality of a vulnerability may depend on factors such as the system's role, the data it handles, and its accessibility to the internet.

In the later chapters of the book, you will learn how to perform vulnerability assessments using various tools and techniques on targeted systems. After identifying the security weaknesses in a targeted system or network, the next phase is exploitation.

Exploitation

As an ethical hacker and penetration tester, the next steps are discovering vulnerabilities in a targeted system, performing manual testing to validate whether these security vulnerabilities exist, and determining how a real threat actor can compromise the system. Exploitation is sometimes the most challenging phase during a penetration test since you will need to either develop or acquire an exploit and modify and test it thoroughly to ensure it has the capability of taking advantage of the vulnerability in the targeted system. Exploitation is the ammunition or evidence that helps articulate why the vulnerability matters and illustrates the impact that the vulnerability could have on the organization. Furthermore, without exploitation, the assessment is not truly a penetration test and is nothing more than a vulnerability assessment, which most companies can conduct in-house better than a third-party consultant could. For many cybersecurity professionals, exploitation is the most exciting phase due to the feeling of breaking into a system.

To put it simply, during the information-gathering phase, a penetration tester profiles the target and identifies any vulnerabilities. Vulnerability assessments play a critical role in identifying and prioritizing vulnerabilities for remediation. They are a fundamental component of a comprehensive security program, providing a broad overview of an organization’s security posture. Using the information about the vulnerabilities, the penetration tester will do their research and create specific exploits that will take advantage of the vulnerabilities of the target – this is exploitation. We use exploits (malicious code) to leverage a vulnerability (weakness) in a system, which will allow us to execute arbitrary code and commands on the targeted system(s).

Often, after successfully exploiting a targeted system or network, we may think the task is done – but it isn't just yet. There are tasks and objectives to complete after breaking into the system. Next, we'll discuss the post-exploitation phase in penetration testing.

Post-exploitation

After a threat actor compromises a targeted system, the adversary usually attempts to expand their foothold on the network by compromising additional systems and setting up backdoor access. This provides additional points of entry into the network infrastructure of the targeted organization. Similarly, ethical hackers and penetration testers apply common post-exploitation techniques such as *lateral movement* to compromise other systems on the network and set up **C2** operations to control multiple systems simultaneously.

During post-exploitation, the primary goal is typically to demonstrate the impact that the vulnerability and access gained can pose to the targeted organization. This impact assists in helping executive leadership and decision-makers to better understand the risks, vulnerabilities, and damage it could cause to the organization if a threat were to target their company and assets.

Report writing

Report writing is exactly as it sounds and is one of the most important elements of any penetration test. Penetration testing may be the service, but report writing is the deliverable that the client/customer sees and is the only tangible element given to the client at the end of the security assessment. Reports should be given as much attention and care as the testing.

Report writing involves much more than listing the security vulnerabilities that were found, their impact, and recommendations. It is the medium through which you convey risk and business impact, summarize your findings, and include remediation steps. A good penetration tester also needs to be a good report writer or the issues they find will be lost and may never be understood by the customer who hired them to conduct the assessment. It's crucial that the report is understandable to a range of stakeholders, including those without technical backgrounds. This means explaining technical vulnerabilities in a way that is accessible to non-experts and illustrating the potential business impacts of these vulnerabilities.

Having completed this section, you are now able to describe each phase of a penetration test and have gained a better idea of the expectations of penetration testers in the industry. Next, we will dive into understanding various penetration testing approaches.

Discovering penetration testing approaches

Each penetration test approach is a bit different from the others, and it's important that you know about all of them. Imagine a potential client calling to request a black box test on their external network infrastructure; as a penetration tester, we must be familiar with the terminology and what is expected by the customer. The following are the approaches used:

- A **white box** assessment is typical of web application testing but can extend to any form of penetration testing. The key difference between white, black, and gray box testing is the amount of information provided to the penetration testers prior to the engagement. In a white box assessment, the penetration tester is provided with full information about the targeted applications, systems, and networks, and is usually given user credentials with varying degrees of access to quickly and thoroughly identify vulnerabilities in the targeted systems and networks. This approach reduces the time required by the ethical hacker and penetration tester to perform reconnaissance to identify the attack surface of the target. Not all security testing is done using the white box approach; sometimes, only the target organization's name is provided to the penetration tester.
- **Black box** assessments are one of the most common forms of network penetration testing and are most typical among external network penetration tests and social engineering penetration tests. In a black box assessment, the penetration testers are given very little or no information about the targeted organization, its networks, or its systems except the organization's name. This particular form of testing is efficient when trying to determine what a real adversary will find and their strategies to gain unauthorized access to the organization's network and techniques for compromising their systems.
- **Gray box** assessments are a hybrid of white and black box testing and are typically used to provide a realistic testing scenario while also giving penetration testers enough information to reduce the time needed to conduct reconnaissance and other black box testing activities. In addition, it's important in any assessment to ensure you are testing all in-scope systems. In a true black box, it's possible to miss systems, and as a result, they are left out of the assessment.

Having completed this section, you have learned about white, gray, and black box security testing approaches. Up next, you will learn about different types of penetration testing in the industry.

Types of penetration testing

As an aspiring ethical hacker and penetration tester, it’s important to understand the difference between a **vulnerability assessment** and **penetration testing**. In a vulnerability assessment, the cybersecurity professional uses a vulnerability scanner to perform authenticated and unauthenticated scans, which is used to help identify the security posture of the targeted systems within the organization. These vulnerability scanners use various techniques to automate the process of discovering a wide range of security weaknesses in systems.

The downside of using an automated vulnerability scanning tool is its incapability to identify the issues that manual testing can via penetration testing to validate the vulnerabilities that actually exist on the target, and this is one of the many reasons why organizations hire penetration testers to perform these assessments on their systems. However, if the penetration tester only delivers the reports of the vulnerability scanning tools instead of performing manual testing during a network-based penetration test, in my opinion, this is highly unethical. Keep in mind that most effective security assessments often involve a combination of automated scanning and manual penetration testing. Automated tools can quickly cover a broad surface area, allowing manual testers to focus their efforts on more complex and potentially high-impact vulnerabilities. During the course of this book, you will learn how to perform successful penetration testing using industry practices, tools, and techniques.

In the upcoming subsections, you will learn about common types of penetration testing and their use cases.

Web application penetration testing

Web application penetration testing (**WAPT**), is the most common form of penetration testing and is likely to be the first penetration testing job most people reading this book will be involved in. WAPT is the act of performing manual identification and exploitation of security vulnerabilities in a targeted web application using techniques such as **SQL injection** (**SQLi**), **cross-site scripting** (**XSS**), and business logic errors that automated tools might miss.

In the later chapters of this book, you will gain the skills and hands-on experience of getting started with WAPT.

Mobile application penetration testing

As you may have noticed, the different types of penetration testing each have specific objectives. Mobile application penetration testing is similar to WAPT but it's specific to mobile applications, which contain their own attack vectors and threats. This is a rising form of penetration testing with a great deal of opportunity for those who are looking to break into this field and have an understanding of mobile application development.

Social engineering penetration testing

Social engineering is the art of manipulating basic human psychology (the mind) to find human-based vulnerabilities and trick potential victims into doing things they may not otherwise do. The primary goal of social engineering penetration testing is to identify vulnerabilities in an organization's security awareness and procedures and to measure how employees respond to social engineering attacks.

For instance, adversaries will attempt to trick an employee within a targeted organization into connecting a malware-infected USB drive to their computer or opening a malware-infected attachment within an email message. In my opinion, it is the most adrenaline-filled type of security assessment.

In this form of penetration testing, you may be asked to do activities such as sending phishing emails, making vishing phone calls, or talking your way into secure facilities and connecting a USB drive to the system to determine what a real adversary could achieve. There are many types of social engineering attacks, which will be covered later on in this book.

Network penetration testing (external and internal)

Network penetration testing focuses on identifying security weaknesses in a targeted environment. The penetration test objectives are to identify the flaws in the targeted organization's systems, their networks (wired and wireless), and their networking devices such as switches and routers.

The following are some tasks that are performed using network penetration testing:

- Bypassing an **intrusion detection system** (**IDS**)/**IPS**
- Bypassing firewall appliances
- Password cracking
- Gaining access to end devices and servers
- Exploiting misconfigurations on switches and routers

External network penetration testing focuses on performing security testing from the internet to identify any security vulnerabilities that a malicious actor can identify and exploit to gain authorized access to the organization's internal network. In internal penetration testing, the penetration tester deploys their attack machine, which is directly connected to the organization's internal network; therefore, the penetration testing is no longer concerned about bypassing the organization's perimeter firewall.

Cloud penetration testing

Cloud penetration testing involves performing security assessments to identify the risks on cloud-based platforms to discover any security vulnerabilities that may expose confidential information to malicious actors. Before attempting to directly engage a cloud platform, ensure you have legal permission from the cloud provider. For instance, if you are going to perform penetration testing on the Microsoft Azure platform, you'll need legal permission from both the cloud provider (Microsoft), as your actions may affect other users and services who are sharing the data center, and the customer who is hiring you for the service.

Cloud penetration testing can include various aspects such as testing the cloud provider's infrastructure, the customer's cloud-based applications, and the configuration of cloud services such as **Software as a Service** (**SaaS**), **Platform as a Service** (**PaaS**), and **Infrastructure as a Service** (**IaaS**).

Physical penetration testing

Physical penetration testing focuses on testing the physical security access control systems in place to protect an organization's data. Security controls exist within offices and data centers to prevent unauthorized persons from entering secure areas of a company.

Physical security controls include the following:

- **Security cameras and sensors** – Security cameras are used to monitor physical actions within an area.
- **Biometric authentication systems** – Biometrics are used to ensure that only authorized people are granted access to an area.
- **Doors and locks** – Locking systems are used to prevent unauthorized persons from entering a secure room or area.
- **Security guards** – Security guards are people who are assigned to protect something, someone, or an area.

Having completed this section, you are now able to describe various types of penetration testing. Your journey ahead won't be complete without understanding the phases of hacking. The different phases of hacking will be covered in the next section.

Exploring the phases of penetration testing

Ethical hackers and penetration testers are white hat hackers, and it's important to understand the general phases of hacking and how each phase is typically aligned to penetration testing. During any penetration testing training, you'll encounter the five phases of hacking.

The following are the general five phases of hacking:

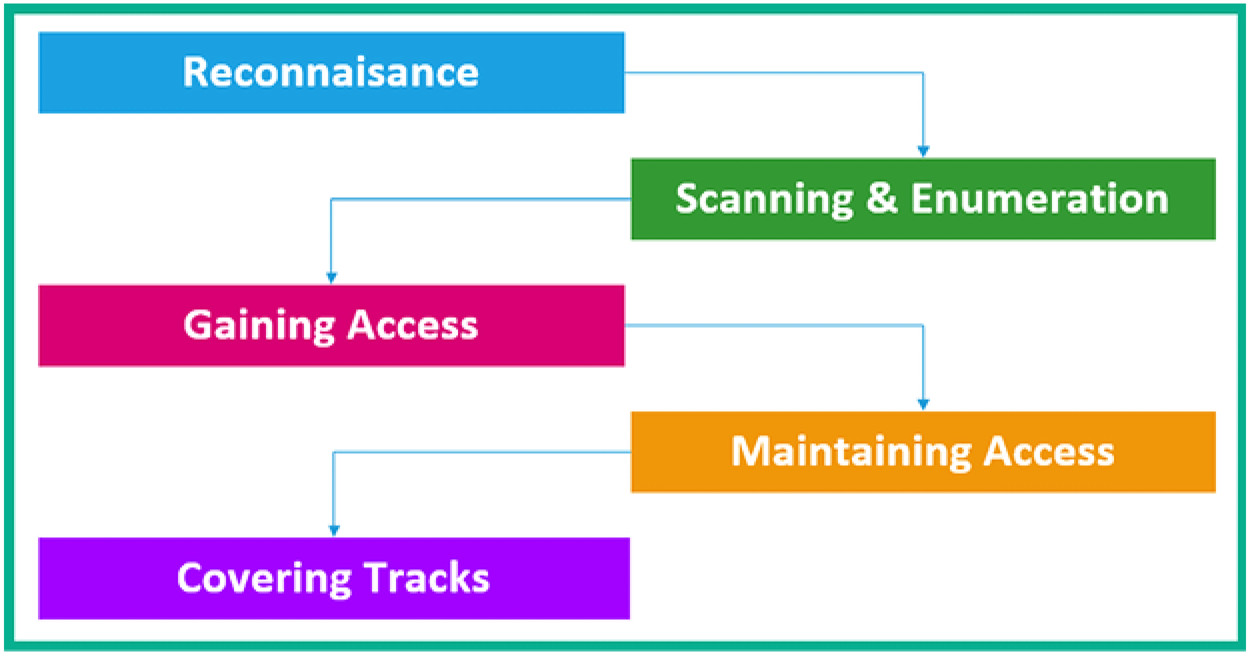

Figure 1.2: Phases of penetration testing

As shown in the preceding diagram, a threat actor performs reconnaissance on the targeted system, network, or organization to collect as much information as possible to better understand the attack surface of the target before moving forward and launching an attack to compromise the target. In the following subsections, you will learn more about the purpose of each phase and how it aligns with ethical hacking and penetration testing.

Reconnaissance

Reconnaissance, commonly referred to as the *information-gathering* phase, is where the threat actor focuses on acquiring meaningful information about their target. The collected information is analyzed to create context and develop a profile about the targeted system, network, or organization. The collected information helps the threat actor better understand the target's attack surface and develop/acquire specific exploits that are suitable for compromising targeted systems.

The following are techniques used in the reconnaissance phase:

- Using internet search engines to gather information
- Using social networking platforms
- Performing Google hacking techniques
- Performing **Domain Name System** (**DNS**) interrogation
- Using social engineering techniques

During this phase, the objective is to gather as much information as possible about the target. Next, we will discuss using a more direct approach: engaging the target to get specific and detailed information.

Scanning and enumeration

The second phase of hacking is scanning. Scanning involves using a direct approach via active reconnaissance in engaging the target to obtain information that is not accessible via passive information-gathering techniques. This phase also involves profiling the targeted organization, its systems, and network infrastructure by sending specially crafted probes to the target.

The following are techniques used in the scanning phase:

- Performing host discovery
- Checking for firewalls and testing their rules
- Checking for open network ports and running services
- Checking for security vulnerabilities
- Creating a network topology of the target network

This phase is very important as it helps us improve the profile of the target. The information found in this phase will help us move on to performing exploitation on the targeted system or network.

Gaining access (exploitation)

This phase can sometimes be the most challenging phase of all. During this phase, the threat actor uses information obtained from the previous phases to either craft an exploit or acquire one from online sources that is designed to compromise the security vulnerability of the target. In addition, the threat actor needs to test the exploit to ensure it's working as expected before delivering and executing it on the targeted system.

The following can occur once access is gained on a targeted system or network:

- Retrieving and cracking stored passwords on systems
- Escalating privileges
- Transferring additional payloads and malware

The gaining access (exploitation) phase can at times be difficult as exploits may work on one targeted system and not on another. Once an exploit is successful and system access is acquired, the next phase is to ensure the threat actor expands their foothold on the compromised system and network.

Maintaining access

After gaining access to a system, the threat actor usually attempts to implement additional backdoors on the compromised system to expand their foothold. In addition, the threat actor usually performs lateral movement on the network by compromising other systems and setting up backdoors for persistent access to the victim's network. Therefore, if a compromised system is offline, the attacker can attempt to remotely connect to another to regain access to the targeted network.

The objectives of maintaining access are as follows:

- Lateral movement
- Exfiltration of data

- Creating backdoor and persistent connections

Maintaining access is important to ensure that you, the penetration tester, always have access to the targeted systems or network. Once the technical aspect of the penetration test is completed, it's time to clean up the network.

Covering your tracks

The last phase is to cover your tracks. This ensures that you do not leave any traces of your presence on a compromised system or network. As penetration testers, we would like to be as undetectable as possible on a targeted network, not triggering any alerts on security sensors and appliances while we remove any residual traces of the actions performed during the penetration test. Covering your tracks ensures that you don't leave any trace of your presence on the network, as a penetration test is designed to be stealthy and simulate real-world attacks on an organization to both identify hidden security vulnerabilities and test the effectiveness of the cyber defenses of the organization.

Having completed this section, you have gained the knowledge to describe the various phases of hacking that are commonly used by threat actors. In the next section, you will discover the Cyber Kill Chain framework, which we are going to leverage in the training and exercises throughout this book.

Understanding the Cyber Kill Chain framework

As an aspiring ethical hacker and penetration tester who's breaking into the cybersecurity industry, it's essential to understand the mindset of threat actors, adversaries, and malicious actors. To be better at penetration testing, you need to develop a very creative and strategic mindset. To put it simply, you need to think like a real hacker if you are to compromise systems and networks as a cybersecurity professional.

Cyber Kill Chain is a seven-stage framework developed by Lockheed Martin, an American aerospace corporation. This framework outlines each critical step a threat actor will need to perform before they are successful in meeting the objectives and goals of the cyber-attack against their targets. Cybersecurity professionals will be able to reduce the likelihood of the threat actor meeting their goals and reduce the amount of damage if they are able to stop the attacker during the earlier phases of the Cyber Kill Chain.

The following diagram shows the seven stages of the Cyber Kill Chain that are used by threat actors:

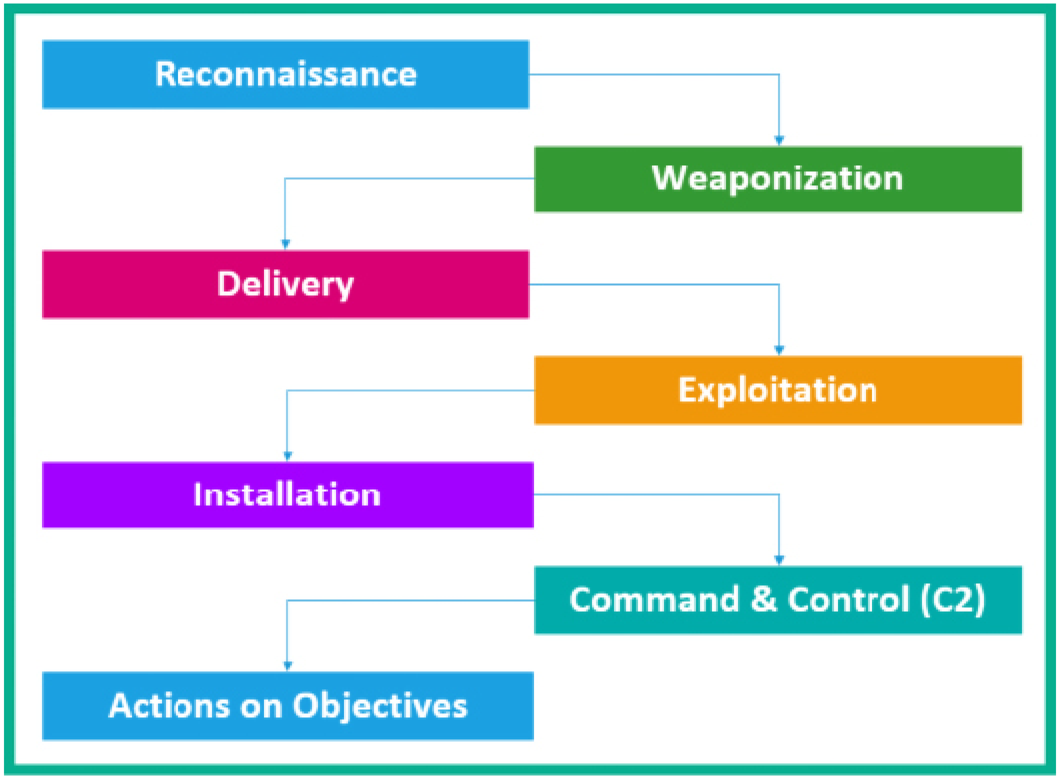

Figure 1.3: Cyber Kill Chain phases

As shown in the preceding diagram, each stage of the Cyber Kill Chain flows into the other until the adversary reaches the last phase, *actions on objectives*, in which the threat actor has successfully achieved the goals of their cyber-attack, and neither the cyber defenses nor cybersecurity team of the compromised organization were able to stop the attack or hacker in their tracks. This is the typical operation of a red team, to simulate real-world adversary threats that are similar to APTs. Unlike penetration testers who are given a time constraint and scope for testing, red teamers do not typically have a scope or time constraint to perform their security testing on a target. However, red teamers still need legal permission prior to any security testing.

On the blue team side of cybersecurity operations, security engineers need to ensure the systems and networks are very well protected and monitored for any potential threats. If a threat is detected, the blue team needs to analyze and contain (isolate) the threat as quickly as possible, preventing it from spreading to other devices on the network. However, as aspiring ethical hackers and penetration testers, we can apply the techniques and strategies used by threat actors that are associated with each stage of the Cyber Kill Chain to achieve our objectives during a real-world penetration test for an organization.

In the next few sections, you will learn about the fundamentals of each stage of the Cyber Kill Chain, how each is used by threat actors, and how penetration testers apply these strategies within their security assessments.

Reconnaissance

As with every battle plan, it's important to know a lot about your opponent before starting a war. The reconnaissance phase focuses on gathering a lot of information and intelligence about the target, whether it's a person or an organization. Threat actors and penetration testers use this stage to create a profile of their targets, which contains IP addresses, operating systems, open service ports, running applications, security vulnerabilities, and any sensitive resources that may be unintentionally exposed that can increase the attack surface.

NOTE

The reconnaissance stage involves both passive and active information-gathering techniques, which will be covered in later chapters of this book. You will also discover tools and techniques to improve your information-collecting and analysis skills during a penetration test.

Threat actors will spend a lot of time researching their target to determine the geolocation of any physical offices, online services, domain names, network infrastructure, online servers, web applications, employees' contact details, telephone numbers, email addresses, and so on. The main objective is to know as much information about the target as possible. Sometimes, this phase can take a long time. Compared to a penetration tester who has a specific time period to perform the entire penetration test, it can take 1 to 2 days of intensive research before moving on to the next phase. However, since adversaries do not have any time constraints like ethical hackers and penetration testers, they can spend a lot more time collecting information, looking for security vulnerabilities, and better planning their cyber-attacks on the target.

Weaponization

Using the information gathered from the reconnaissance phase, the threat actor and penetration tester can use it to better craft a weapon, also referred to as an exploit, which can take advantage of a security vulnerability in the targeted system. The weapon (exploit) has to be specially crafted and tested to ensure it is successful when launched by the threat actor or penetration tester. The objective of the exploit is to compromise the **confidentiality, integrity, and/or availability (CIA)** of the systems or networks that are owned by the targeted organization.

Both threat actors and penetration testers need to consider the likelihood that their exploit will be detected by any antimalware, **endpoint detection and response (EDR)**, and any threat detection solutions that monitor the targeted systems and network. Therefore, it's important to encode or disguise the exploit to reduce triggering any security sensors and alerting the security team.

An exploit takes advantage of a vulnerability. After that happens, what's next? To be a bit more strategic, threat actors and penetration testers will couple their exploit with additional payloads. The payload is unleashed after the exploit has compromised the system. As a simple example, a payload can be used to create a persistent backdoor on the targeted system to allow the threat actor or the penetration tester remote access to the system at any time when the compromised system is online.

Delivery

After creating the exploit (weapon), the threat actor or penetration tester has to use an attack vector as a method to deliver the exploit onto the targeted system. Delivery can be done using the creative mindset of the attacker, whether using email messaging, instant messaging services, or even by creating drive-by downloads on compromised web services. Another technique is to copy the exploit onto multiple USB drives and drop them within the compound of the target organization, with the hope that an employee will find it and connect it to an internal system due to human curiosity.

The following is a picture of a USB Rubber Ducky, which is commonly used during ethical hacking and penetration testing:

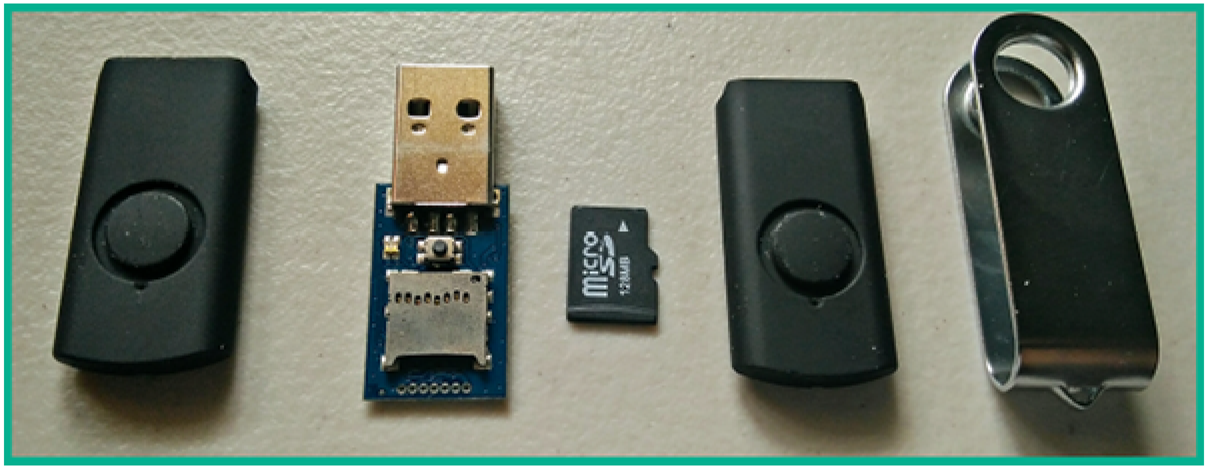

Figure 1.4: USB rubbery ducky

As shown in the preceding image, the USB Rubber Ducky enables a penetration tester to load malicious scripts onto a memory card. Once this device is connected to a computer, it is detected as a **human interface device** (**HID**) such as a keyboard, and then executes the script on the targeted system. This is just one of many creative ideas for delivering a payload to a target.

As an aspiring ethical hacker and penetration tester, ensure you have multiple methods of delivering the weapon to the target, such that, in the event that one method does not work, you have alternative solutions.

Exploitation

After the weapon (exploit) is delivered to the target, the attacker needs to ensure that when the exploit is executed, it is successful in taking advantage of the security vulnerability of the targeted system as intended. If the exploit does not work, the threat actor or penetration tester may be detected by the organization's cyber defenses and this can create a halt in the Cyber Kill Chain. The attacker needs to ensure the exploit is tested properly before executing it on the targeted system.

Installation

After the threat actor has exploited the targeted system, the attacker will attempt to create multiple persistent backdoor accesses to the compromised system. This allows the threat actor or the penetration tester to have multiple channels of entry back into the system and network. During this stage, additional applications may be usually installed while the threat actor takes a lot of precautions to avoid detection by any threat detection systems.

Command and Control (C2)

An important stage in a cyber-attack is creating **C2** communication channels between the compromised systems and a C2 server on the internet. This allows the threat actor to centrally control a group of infected systems (zombies) in a collection of a botnet using a C2 server that is managed by the adversary. This allows the threat actor to create an army of zombies, all controlled and managed by a single threat actor. The following diagram shows an example of C2:

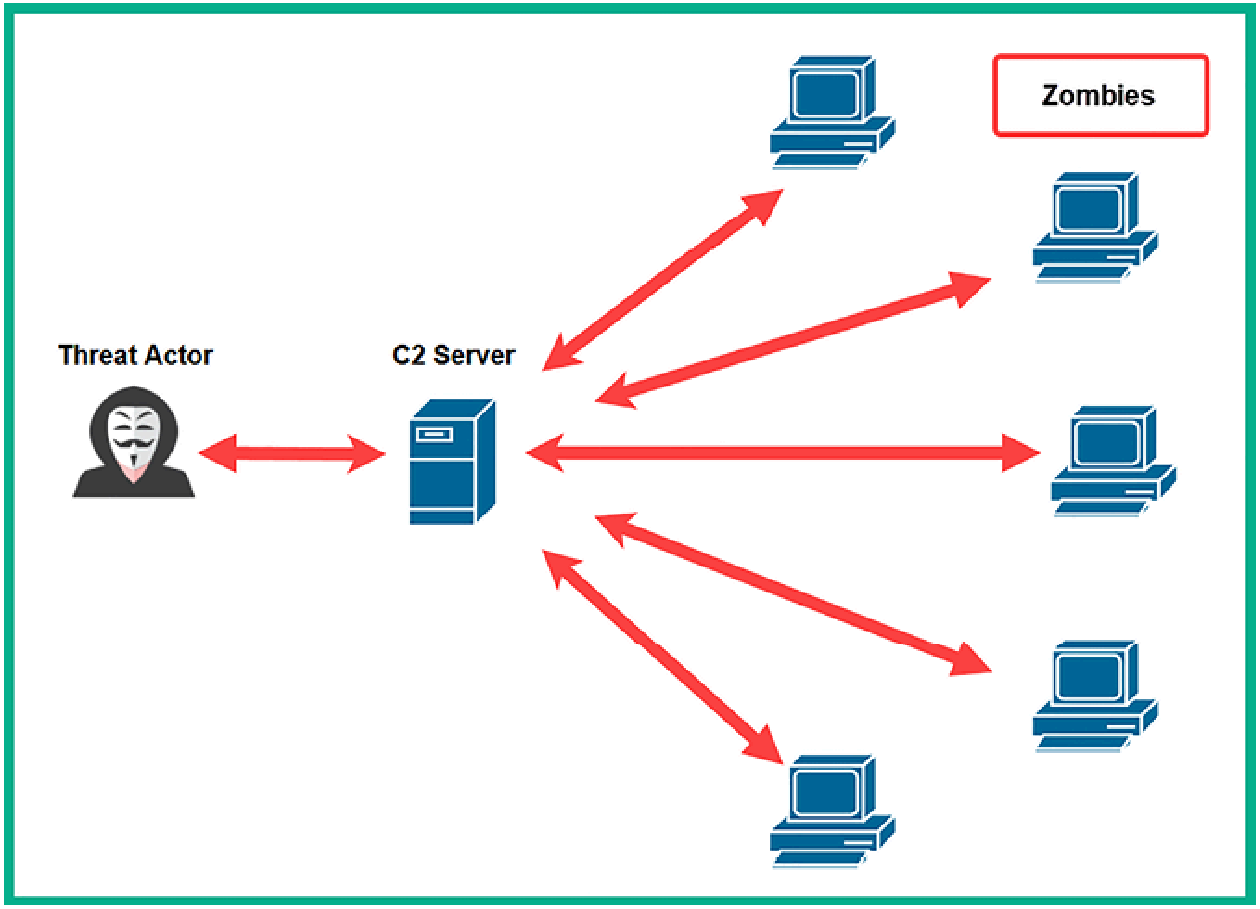

Figure 1.5: Command and Control operations

The threat actor uses data encryption, encapsulation, and various tunneling techniques to evade threat detection systems within target organizations. Similarly, there is an advanced stage of penetration testing known as red teaming where there are no limitations (rules of engagement) on the methods and techniques used to compromise a target organization, with the objective of simulating the closest thing to a real advanced cyber-attack of a malicious cyber army. However, keep in mind that legal permission is still needed for any type of red team engagement.

Actions on objectives

If the threat actor or penetration tester is able to reach this stage of the Cyber Kill Chain, the organization's blue team has failed to stop the attacker and prevent the cyber-attack. At this stage, the threat actor has completed their objectives and achieved the goals of the attack. In this phase, the attacker can complete the main objective of the attack, whether it's exfiltrating data from the organization and selling it on the Dark Web or even extending their botnet for a larger-scale cyber-attack on another target organization.

Stopping the threat actor or penetration tester at this phase is considered to be extremely difficult as the attacker would have already established multiple persistent backdoor accesses with encrypted C2 communication channels on many compromised systems within the targeted organization. Furthermore, the threat actor will also be clearing traces of any evidence or artifacts that could help cybersecurity professionals trace the source attack to the threat actor.

Having completed this section, you have learned about the various stages of the Cyber Kill Chain and how it helps cybersecurity professionals understand the intentions of threat actors. Additionally, you have learned how penetration testers can implement these strategies within their penetration testing engagements.

Summary

In this chapter, you have learned about the importance and need for cybersecurity professionals and solutions around the world to safeguard assets from cyber criminals. Furthermore, you now have a better understanding of different types of threat actors and their reasons for performing cyber-attacks on their targets. In addition, you have explored what matters to threat actors and how various factors can affect their motives and determine whether it's truly worth attacking a system or organization.

You have also learned about the various phases of penetration testing that are commonly used by threat actors. Each phase of penetration testing is important to ensure the ethical hacker and penetration tester is efficiently able to test the cyber defenses of a targeted organization and discover hidden security vulnerabilities.

I trust that the knowledge presented in this chapter has provided you with valuable insights, supporting your path toward becoming an ethical hacker and penetration tester in the dynamic field of cybersecurity. May this newfound understanding empower you in your journey, allowing you to navigate the industry with confidence and make significant contributions. In the next chapter, *Chapter 2*, *Building a Penetration Testing Lab*, you will learn how to design and build a virtualized penetration testing lab on your personal computer that will be used to hone your new skills in a safe environment.

Further reading

- The Cyber Kill Chain – https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html
- MITRE ATT&CK tactics – https://attack.mitre.org/tactics/enterprise/
- **Penetration Testing Execution Standard** (PTES) – http://www.pentest-standard.org/index.php/PTES_Technical_Guidelines
- **Payment Card Industry Data Security Standard** (PCI DSS) – https://www.pcisecuritystandards.org/documents/Penetration-Testing-Guidance-v1_1.pdf
- **Penetration Testing Framework** (PTF) – http://www.vulnerabilityassessment.co.uk/Penetration%20Test.html
- Technical Guide to Information Security Testing and Assessment – https://csrc.nist.gov/publications/detail/sp/800-115/final
- Open Source Security Testing Methodology Manual – https://www.isecom.org/OSSTMM.3.pdf
- OWASP Web Security Testing Guide – https://owasp.org/www-project-web-security-testing-guide/
- OWASP Mobile Security Testing Guide – https://owasp.org/www-project-mobile-app-security/
- OWASP Firmware Security Testing Methodology – https://github.com/scriptingxss/owasp-fstm

Join our community on Discord

Join our community's Discord space for discussions with the author and other readers:

https://packt.link/SecNet