---

# Chapter 2. Penetration Testing Methodology

**Penetration testing**, often abbreviated as **pentest** , is a process that is followed to conduct an in-depth security assessment or audit. A **methodology** defines a set of rules, practices, and procedures that are pursued and implemented during the course of any information security audit program. A **penetration testing methodology** defines a roadmap with practical ideas and proven practices that can be followed to assess the true security posture of a network, application, system, or any combination thereof. This chapter offers summaries of several key penetration testing methodologies. Key topics covered in this chapter include:

- A discussion on two well-known types of penetration testing—black box and white box
- Describing the differences between the vulnerability assessment and penetration testing
- Explaining several industry-acceptable security testing methodologies and their core functions, features, and benefits
- A general penetration testing methodology that incorporates the 10 consecutive steps of a typical penetration testing process
- The ethical dimension of how the security testing projects should be handled

Penetration testing can be carried out independently or as a part of an IT security **risk management** process that may be incorporated into a regular development life cycle (for example, Microsoft SDLC). It is vital to notice that the security of a product not only depends on the factors that are related to the IT environment but also relies on product-specific security best practices. This involves the implementation of appropriate security requirements, performing risk analysis, threat modeling, code reviews, and operational security measurement.

Penetration testing is considered to be the last and most aggressive form of security assessment. It must be handled by qualified professionals and can be conducted with or without prior knowledge of the targeted network or application. A pentest may be used to assess all IT infrastructure components including applications, network devices, operating systems, communication medium, physical security, and human psychology. The output of penetration testing usually consists of a report divided into several sections that address the weaknesses found in the current state of the target environment, followed by potential countermeasures and other remediation recommendations. The use of a methodological process provides extensive benefits to the **pentester** to understand and critically analyze the integrity of current defenses during each stage of the testing process.

## Types of penetration testing

Although there are different types of penetration testing, the two most general approaches that are widely accepted by the industry are the black box and white box. These approaches will be discussed in the following sections.

### Black box testing

While applying this approach, the security auditor will be assessing the network infrastructure and will not be aware of any internal technologies deployed by the targeted organization. By employing a number of real-world hacker techniques and going through organized test phases, vulnerabilities may be revealed and potentially exploited. It is important for a pentester to understand, classify, and prioritize these vulnerabilities according to their level of risk (low, medium, or high). The risk can be measured according to the threat imposed by the vulnerability in general. An ideal penetration tester would determine all attack vectors that could cause the target to be compromised. Once the testing process has been completed, a report that contains all the necessary information regarding the targets' real-world security posture, categorizing, and translating the identified risks into a business context, is generated. Black box testing can be a more expensive service than white box testing.

### White box testing

An auditor involved in this kind of penetration testing process should be aware of all the internal and underlying technologies used by the target environment. Hence, it opens a wide gate for a penetration tester to view and critically evaluate the security vulnerabilities with minimum possible efforts and utmost accuracy. It does bring more value to the organization in comparison to the black box approach in the sense that it will eliminate any internal security issues lying at the target infrastructure's environment, thus making it more difficult for a malicious adversary to infiltrate from the outside. The number of steps involved in white box testing is similar to that of black box testing. Moreover, the white box approach can easily be integrated into a regular development life cycle to eradicate any possible security issues at an early stage before they get disclosed and exploited by intruders. The time, cost, and knowledge level required to find and resolve the security vulnerabilities is comparably less than with the black box approach.