**Penetration Testing Strategies**

**Penetration Testing Strategies**

* **Black box tests** are performed with [no prior knowledge](https://biztechmagazine.com/article/2018/08/top-penetration-testing-tools-and-types-safeguard-against-cybersecurity-threats-perfcon) of the tested network ecosystem. A black box test is an objective assessment of security as seen from outside the network by third parties. It’s a test of software security operations, versus a white box test (which is structural).  
    
  Examples of black box testing include functional testing, non-functional testing, and [regression testing](https://smartbear.com/learn/automated-testing/what-is-regression-testing/). However, a standard black box test likely wouldn’t involve a tactic like a denial-of-service (DoS) attack, which could cause severe damage to the network.
* **White box tests** are performed with full knowledge of the internal design and structure of the tested ecosystem.  
    
  White box testing is used to logic test software for gaps in code and security, instead of behavior testing against malicious outside agents. Path testing, loop testing, and condition testing are all white box.
* **Grey box tests** combine aspects of white and black box testing into one. For this variety of test, experts will assess the level of software security seen by a legitimate user with an account.  
    
  These tests give access to the software or product, along with general information about the internal ecosystem. They combine operational testing from a third party perspective with a more advanced internal understanding of the software.

Selecting the right approach to testing is essential for success. A white box test may uncover where a developer accidentally left credentials in the software code, but be wholly inadequate to uncover vulnerabilities in open ports or third-party integrations.

## Common types of penetration test

* **External network pen test** — A black box test designed to use footprint analysis to identify publicly available information about the network and organization, including IP addresses, ranges, and key personal information (email addresses, passwords, etc.) Using this information, an expert will locate potential vulnerabilities.
* **Internal network pen test** — A white or grey box test designed to simulate what could happen if a user’s account is compromised.

Pen tests can be tailored to search for vulnerabilities in web apps, mobile devices, and wireless networks.

* **Black box tests** are performed with [no prior knowledge](https://biztechmagazine.com/article/2018/08/top-penetration-testing-tools-and-types-safeguard-against-cybersecurity-threats-perfcon) of the tested network ecosystem. A black box test is an objective assessment of security as seen from outside the network by third parties. It’s a test of software security operations, versus a white box test (which is structural).  
    
  Examples of black box testing include functional testing, non-functional testing, and [regression testing](https://smartbear.com/learn/automated-testing/what-is-regression-testing/). However, a standard black box test likely wouldn’t involve a tactic like a denial-of-service (DoS) attack, which could cause severe damage to the network.
* **White box tests** are performed with full knowledge of the internal design and structure of the tested ecosystem.  
    
  White box testing is used to logic test software for gaps in code and security, instead of behavior testing against malicious outside agents. Path testing, loop testing, and condition testing are all white box.
* **Grey box tests** combine aspects of white and black box testing into one. For this variety of test, experts will assess the level of software security seen by a legitimate user with an account.

**Penetration Testing Strategies**

## Black Box Penetration Testing

In black box penetration testing, tester has no idea about the systems that he is going to test. He is interested to gather information about the target network or system. For example, in this testing, a tester only knows what should be the expected outcome and he does not know how the outcomes arrives. He does not examine any programming codes.

### Advantages of Black Box Penetration Testing

It has the following advantages −

* Tester need not necessarily be an expert, as it does not demand specific language knowledge
* Tester verifies contradictions in the actual system and the specifications
* Test is generally conducted with the perspective of a user, not the designer

### Disadvantages of Black Box Penetration Testing

Its disadvantages are −

* Particularly, these kinds of test cases are difficult to design.
* Possibly, it is not worth, incase designer has already conducted a test case.
* It does not conduct everything.

## White Box Penetration Testing

This is a comprehensive testing, as tester has been provided with whole range of information about the systems and/or network such as Schema, Source code, OS details, IP address, etc. It is normally considered as a simulation of an attack by an internal source. It is also known as structural, glass box, clear box, and open box testing.

White box penetration testing examines the code coverage and does data flow testing, path testing, loop testing, etc.

### Advantages of White Box Penetration Testing

It carries the following advantages −

* It ensures that all independent paths of a module have been exercised.
* It ensures that all logical decisions have been verified along with their true and false value.
* It discovers the typographical errors and does syntax checking.
* It finds the design errors that may have occurred because of the difference between logical flow of the program and the actual execution.

## Grey Box Penetration Testing

In this type of testing, a tester usually provides partial or limited information about the internal details of the program of a system. It can be considered as an attack by an external hacker who had gained illegitimate access to an organization's network infrastructure documents.

### Advantages of Grey Box Penetration Testing

It has the following advantages −

* As the tester does not require the access of source code, it is non-intrusive and unbiased
* As there is clear difference between a developer and a tester, so there is least risk of personal conflict
* You don’t need to provide the internal information about the program functions and other operations

**Black box test**

**White box test**

**Grey box testing**