Learn about Penetration Testing

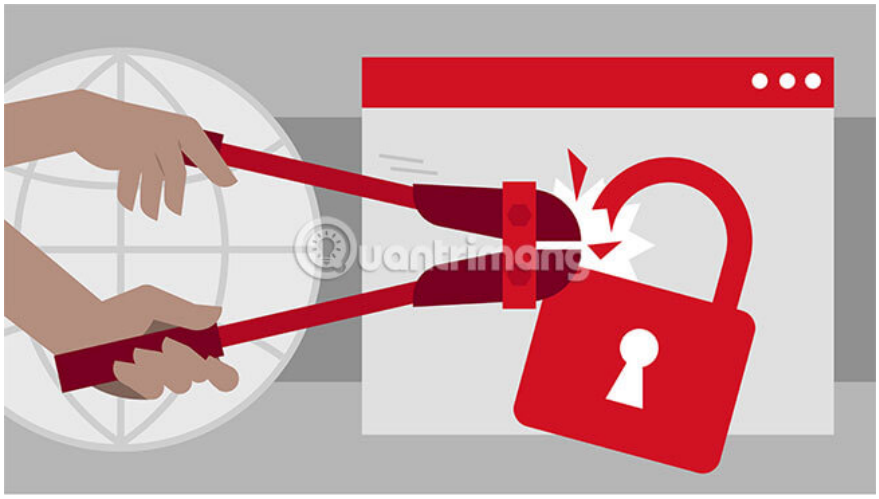
Penetration Testing, also called pen test, is a simulated network attack on a computer system to check for vulnerabilities that can be exploited.

Penetration Testing is an authorized simulated network attack on a computer, to assess the security of the system. The testing process is performed to identify both weaknesses (also known as vulnerabilities), including the possibility that parties are not allowed to access system features and data, as well as strengths that allow Risk assessment throughout the system.

What is Penetration Testing (Penetration Testing)?

What is Penetration Testing?

Penetration Testing, also called pen test, is a simulated network attack on a computer system to check for vulnerabilities that can be exploited. In web application security, Penetration Testing is often used to enhance the Web Application Firewall (WAF).

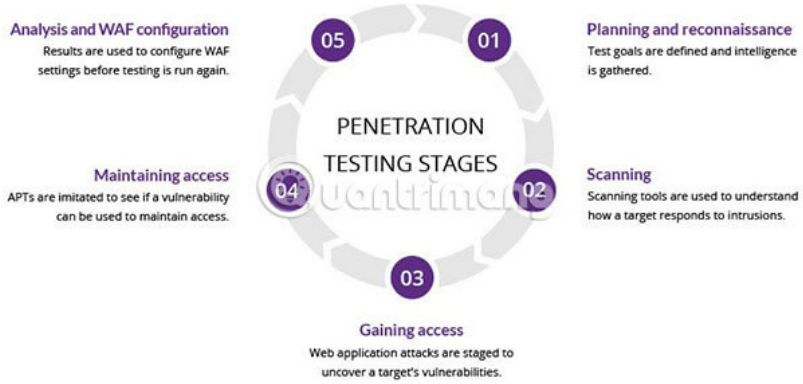


Pen testing may involve trying to violate any number of application systems, (eg Application Protocol Interface - API, frontend / backend) to detect holes Vulnerabilities, such as unconfirmed input, are vulnerable to malicious attacks by transmitting malicious code.

Detailed information provided by the penetration testing process can be used to refine WAF security policies and patch detected vulnerabilities.

The stages in Penetration Testing

The process of pen test can be divided into 5 stages.



1. Planning and surveying in advance

The first phase includes:

1. Determine the scope and objectives of the test, including the systems to be processed and the testing methods to be used.
2. Collect information (such as network name and domain name, mail server) to better understand how its goals and potential vulnerabilities are.

2. Scan

The next step is to understand how the target application will react to different intrusion factors. This is usually done using:

1. Static analysis method - Check the application's code to determine its behavior while running. These tools can scan all code in one run.
2. Dynamic analysis method - Check the application code in running state. This is a more realistic scanning method, as it provides a real-time view of application performance.

3. Get access

This phase uses web application attacks, such as cross-site scripting, SQL injection and backdoor, to discover target vulnerabilities. Later, testers will try to exploit these vulnerabilities, usually by gaining full control of the system, data theft, traffic blocking, and so on. to know the damage they can cause.

4. Maintain access

The goal of this phase is to see if the vulnerability can be used to exploit long term in compromised systems (long enough for a hacker to have deep access to the system). The idea is to mimic APT attacks, which often exist for months in a system to steal the organization's most sensitive data.

5. Analysis

The results of the penetration test are then compiled into a detailed report, including:

1. Specific vulnerabilities have been exploited
2. Sensitive data is accessed
3. The length of time that the person conducting the pen test can stay in the system is not detected

This information is analyzed by security personnel, helping to configure WAF settings for businesses, offering other application security solutions to patch vulnerabilities and protect against future attacks. .

Penetration Testing methods

External test (External penetration test)

External penetration testing targets the 'assets' of a company that can be seen on the Internet, for example the web application itself, company website, email and domain name server (DNS). The goal is to get access and extract valuable data.

Internal test (Intrusion test from inside)

In internal penetration testing, testers who have access to an application behind the firewall simulate an internal attack. This attack not only alerts the prospect of an internal employee who might be a hacker himself, but also reminds an administrator to prevent an employee in the organization from being logged on after a phishing attack.

Blind test (blind test)

In the blind test test, the tester is only given the name of the target business. This provides security personnel with a real-time view of how an application attack will take place in practice.

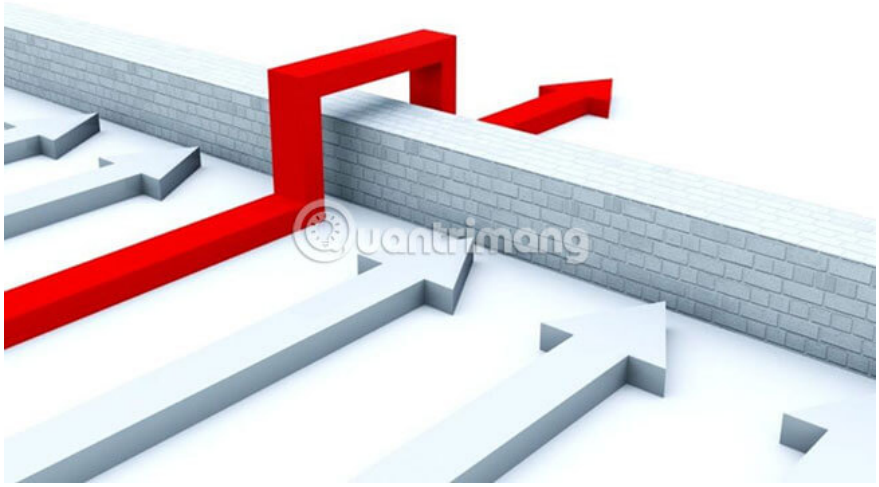
Double blind test

In the double blind test, the security officer didn't know anything in advance about the simulated attack. Like in the real world, attacks are not always known to enhance defensive capabilities.

Targeted test

In this scenario, both the inspector and the security officer will work together and continually evaluate each other's actions. This is a valuable training exercise, providing the team with real-time feedback security from the hacker point of view.

Penetration testing and web application firewall



Penetration testing and WAF are independent security measures, but they also provide mutual benefits.

For many types of pen tests (except for blind tests and double blind tests), testers can use WAF data, such as diaries, to locate and exploit application weaknesses.

In return, WAF administrators can benefit from pen test data. After the test is completed, the WAF configuration can be updated to protect against weaknesses detected during the test.

Finally, pen test meets a number of requirements for compliance with security testing procedures, including PCI DSS and SOC 2. Some standards, such as PCI-DSS 6.6, can only be satisfied through The use of WAF is certified.