Penetration Testing

AppSec , Essentials

208.2k views

Learning Objectives

What is penetration testing

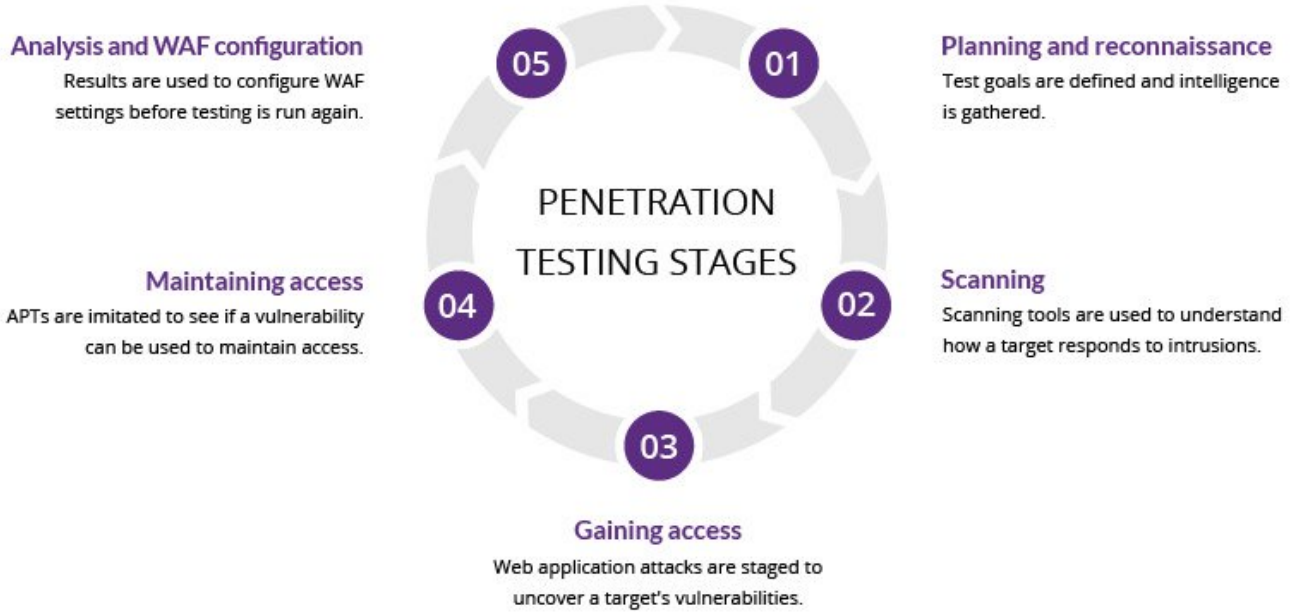
A penetration test, also known as a pen test, is a simulated cyber attack against your computer system to check for exploitable vulnerabilities. In the context of web application security, penetration testing is commonly used to augment a web application firewall (WAF).

Pen testing can involve the attempted breaching of any number of application systems, (e.g., application protocol interfaces (APIs), frontend/backend servers) to uncover vulnerabilities, such as unsanitized inputs that are susceptible to code injection attacks.

Insights provided by the penetration test can be used to fine-tune your WAF security policies and patch detected vulnerabilities.

Penetration testing stages

The pen testing process can be broken down into five stages.



1. Planning and reconnaissance
The first stage involves:

Defining the scope and goals of a test, including the systems to be addressed and the testing methods to be used.

Gathering intelligence (e.g., network and domain names, mail server) to better understand how a target works and its potential vulnerabilities.

2. Scanning
The next step is to understand how the target application will respond to various intrusion attempts. This is typically done using:

Static analysis – Inspecting an application's code to estimate the way it behaves while running. These tools can scan the entirety of the code in a single pass.

Dynamic analysis – Inspecting an application's code in a running state. This is a more practical way of scanning, as it provides a real-time view into an application's performance.

3. Gaining Access
This stage uses web application attacks, such as cross-site scripting, SQL injection and backdoors, to uncover a target's vulnerabilities. Testers then try and exploit these vulnerabilities, typically by escalating privileges, stealing data, intercepting traffic, etc., to understand the damage they can cause.

4. Maintaining access
The goal of this stage is to see if the vulnerability can be used to achieve a persistent presence in the exploited system— long enough for a bad actor to gain in-depth access. The idea is to imitate advanced persistent threats, which often remain in a system for months in order to steal an organization's most sensitive data.

5. Analysis
The results of the penetration test are then compiled into a report detailing:

- Specific vulnerabilities that were exploited
- Sensitive data that was accessed
- The amount of time the pen tester was able to remain in the system undetected

This information is analyzed by security personnel to help configure an enterprise's WAF settings and other application security solutions to patch vulnerabilities and protect against future attacks.

Penetration testing methods

External testing

External penetration tests target the assets of a company that are visible on the internet, e.g., the web application itself, the company website, and email and domain name servers (DNS). The goal is to gain access and extract valuable data.

Internal testing

In an internal test, a tester with access to an application behind its firewall simulates an attack by a malicious insider. This isn't necessarily simulating a rogue employee. A common starting scenario can be an employee whose credentials were stolen due to a phishing attack.

Blind testing

In a blind test, a tester is only given the name of the enterprise that's being targeted. This gives security personnel a real-time look into how an actual application assault would take place.

Double-blind testing

In a double blind test, security personnel have no prior knowledge of the simulated attack. As in the real world, they won't have any time to shore up their defenses before an attempted breach.

Targeted testing

In this scenario, both the tester and security personnel work together and keep each other appraised of their movements. This is a valuable training exercise that provides a security team with real-time feedback from a hacker's point of view.

Penetration testing and web application firewalls

Penetration testing and WAFs are exclusive, yet mutually beneficial security measures.

For many kinds of pen testing (with the exception of blind and double blind tests), the tester is likely to use WAF data, such as logs, to locate and exploit an application's weak spots.

In turn, WAF administrators can benefit from pen testing data. After a test is completed, WAF configurations can be updated to secure against the weak spots discovered in the test.

Finally, pen testing satisfies some of the compliance requirements for security auditing procedures, including PCI DSS and SOC 2. Certain standards, such as PCI-DSS 6.6, can be satisfied only through the use of a certified WAF. Doing so, however, doesn't make pen testing any less useful due to its aforementioned benefits and ability to improve on WAF configurations.