What is Penetration Testing and How Does It Work?

TechRounder PDF Edition

Live article: https://www.techrounder.com/development/what-is-penetration-testing-and-how-does-it-work/

By Vipin PG | Published February 6, 2023 | Updated January 4, 2026 | Format: Explainer | 5 min read

In brief

A simulated cyber-attack on a computer system, network, or online application, commonly referred to as "pen testing," is done to assess the system's security. It aims to identify vulnerabilities that a malicious attacker could exploit and provide recommendations for improving the target's security posture.

A simulated cyber-attack on a computer system, network, or online application, commonly referred to as "pen testing," is done to assess the system's security. It aims to identify vulnerabilities that a malicious attacker could exploit and provide recommendations for improving the target's security posture.

Pen tests can be conducted using manual techniques or automated tools ranging from simple simulated attacks to complex, multi-stage attacks. Various companies provide penetration testing services to help you secure your network and enhance the security of your overall company environment.

The results of the test help organizations understand the risks associated with their systems and prioritize their security efforts. Pen testing should be performed regularly to maintain the security of an organization's information assets.

What is Penetration Testing?

Using a proper manner, a penetration test can easily dive into many aspects of the system. Penetration testing can be performed using various techniques, such as manual or automated tools, ranging from simple simulated attacks to complex multi-stage attacks.

The test results provide organizations with an understanding of the strengths and weaknesses of their security measures, enabling them to make informed decisions about how to improve their security posture.

Penetration testing can also be used to comply with various regulations and standards, such as PCI DSS, HIPAA, and ISO 27001. These regulations require organizations to have robust security measures to protect sensitive information and assess their security controls' effectiveness regularly.

Why is Penetration Testing Services Important?

Employees with little to no professional experience in security are typically responsible for designing, constructing, and maintaining surroundings. The resulting report can allow you to fix problems before attackers use them. In an ideal world, software and systems would have been created from the ground up to be free of harmful security defects. Unfortunately, most people do penetration testing for the following reasons:

- To locate any faults in the incident response strategy and any specific vulnerabilities in their network's cybersecurity architecture that may be remedied.

- To raise upper management’s understanding of cybersecurity risks, which may lead to higher budgetary support for security efforts such as additional defenses and security education, training, and awareness campaigns.

Both goals help an organization’s overall cybersecurity, which is always advantageous. However, penetration testing is not a "one-and-done" solution; it is crucial to keep this in mind. The network’s assets, the software running on those assets, or even new attack strategies focusing on previously undisclosed weaknesses could all change over time. Therefore, organizations must routinely conduct fresh pen tests to maintain excellent vulnerability management.

Every organization will do penetration tests at a different frequency, though. For example, how often should your own company do pen tests? In addition, the size of your business, how regularly you upgrade your network’s software or hardware, and the unique cybersecurity laws that apply to your sector will influence the response.

How the Penetration Testing Services Works?

Penetration testing methods

Pen testing can be divided into various types, such as external testing, internal testing, and social engineering testing.

External Penetration Testing

It is a type of security assessment that simulates an attack from an external attacker without prior knowledge of the system being tested. The aim is to identify vulnerabilities in the system and provide recommendations for remediation. The test typically covers network perimeter, web applications, and other public-facing systems.

Internal Penetration Testing

An Internal Pen Test is a type of security assessment that simulates an attack from an internal attacker with knowledge of the system being tested. This test aims to identify vulnerabilities and security weaknesses within the organization’s internal network and systems.

This type of test is conducted from the perspective of an insider with access to the network, such as an employee, contractor, or vendor. The test covers network infrastructure, servers, and endpoints and can also include social engineering tactics to test employee awareness and security practices.

Social Engineering Penetration Testing

This test is a type of security assessment that focuses on testing an organization’s human defenses against malicious attacks. It simulates real-world social engineering tactics, such as phishing emails, impersonation, and pretexting, to determine employees’ susceptibility to such attacks.

The test is to identify any weaknesses in the human component of the organization’s security posture and to educate employees on the importance of security awareness. This type of testing can be conducted in person, via phone, or digitally and can be used to test employee awareness, training, and policies.

Stages of a Penetration Test

The tests are done in 5 stages:

1. Planning and reconnaissance: This stage of the test involves defining the scope and goal of the test, including the systems and methods which are to be involved. It also includes gathering intelligence, like names of networks and domains, mail servers, etc., to understand the vulnerabilities and the target's working.

2. Scanning: This step is done using Static and Dynamic analysis. In static, the code of an application is inspected to estimate its behavior with the tools that can scan it in one go. In dynamic analysis, the code is inspected in a running state, making it more practical as it provides a real-time view of the application's performance.

3. Gaining Access: The penetration testing service providers now use web application attacks to uncover the target's vulnerabilities. The testers then try to exploit these weaknesses by escalating privileges, intercepting traffic, stealing data, etc., to understand better the damage they can cause.

4. Maintaining Access: The aim is to see if the weaknesses can be used to achieve a persistent presence in the exploited system for a longer duration to gain in-depth access.

5. Analysis: The results are now analyzed and compiled into a report that includes the exploited vulnerabilities, the sensitive data that can be accessed, and the duration the pen tester could stay undetected in the system.

Conclusion

Penetration testing should be performed regularly, as it helps organizations stay ahead of potential threats and ensures that their information assets are protected. However, the testing frequency depends on the organization's size, complexity, and the criticality of the tested systems.

Trained and experienced penetration testing service providers like Kiss.Software performing pen testing ensures that it is controlled and systematic, minimizing any potential negative impact on production systems.

The pen test should be continuous as technology evolves and new security threats emerge. The test results should be documented and used to track the organization's progress in terms of its security posture. Furthermore, the pen test findings should be shared with relevant stakeholders, such as the CEO, CIO, and IT department, to ensure that the organization is taking the necessary steps to secure its systems.

It is an essential aspect of information security and helps organizations protect their assets and avoid potential threats. Therefore, it should be performed regularly and by experienced professionals to ensure that it is controlled and effective.

References

1. kiss.software - what-we-do-details / penetration-tests - https://kiss.software/what-we-do-details/penetration-tests

2. crowdstrike.com - cybersecurity-101 / vulnerability-management - https://www.crowdstrike.com/cybersecurity-101/vulnerability-management/