Penetration Testing Saves Time and Money

Nothing reveals weaknesses quite like a full-on cyber-attack. For precisely that reason, smart organizations conduct penetration testing. A penetration test simulates an actual attack but under controlled conditions. This allows the cyber security team to proactively address vulnerabilities before hackers can exploit them.

Penetration testing offers several key benefits. In the first place, it provides a clear picture of the company's security stance from the perspective of a motivated attacker. Testers not only identify vulnerabilities but also determine the level of risk involved. Using this information, the organization can prioritize risk and develop an effective cyber security plan.

A successful breach can cost millions of dollars, and the longer the hacker lives in the system, the more damage they can do. Finding and remediating security flaws before an attack occurs saves money, reduces downtime, preserves the company's reputation, informs strategy, and supports compliance and privacy initiatives.

Understand the Stages of a Penetration Test

A typical penetration test includes five phases:

1. Reconnaissance – During the first phase of the test, the "attackers" gather as much information about the target system as they can. This includes using network scanning tools to identify open ports, running services and other access points. It also involves scanning for known vulnerabilities in the system.

Additionally, testers may comb through publicly available information such as social media accounts, company websites and other public domains.

2. Gaining access – With a map of the system and an understanding of where the vulnerabilities lie, the testers use various techniques to gain unauthorized access. This involves a combination of social engineering, exploitation of software vulnerabilities and password cracking.

3. Exploitation – Once the attackers find a way into the system, they focus on collecting evidence such as privileged information or credentials. Then they attempt to expand their control over the system. This can include privilege escalation, creating back doors for future access and moving laterally through the system.

   During this phase, the testers will work to cover their tracks, just as a malicious attacker would do. This may involve disabling security controls, clearing logs, and otherwise making it difficult for security personnel to detect their presence.

4. Reporting – A critical part of penetration testing includes reporting. The testers should deliver a prioritized list of security issues along with a step-by-step description of how to replicate the process. Reports may also detail weak and reused credentials. This information will prove essential in fixing the problems and preventing real attacks.

5. Remediation – Finally, the security provider will suggest strategies for improvement based on the results of the test.

Types of Penetration Tests

Security providers may offer different types of penetration testing, depending on the type of organization and business needs. Each type of testing has different methods and objectives. For instance, in an external penetration test the ethical hacker attempts to breach security through external-facing technology such as websites or external servers.

An internal penetration test, on the other hand, involves the tester attempting to cause damage using the organization's internal network. This delivers visibility into the types of damage an unhappy employee or a hacker with stolen credentials could cause.

Additional types of tests include attacks through social engineering or IoT devices. Some organizations will commission a red team attack. Through a multi-layered attack simulation, this test measures the effectiveness of network and application security, human security awareness and physical security all at once.

Not a "Once and Done" Process

Penetration testing done five years ago will have little benefit now. Organizations should conduct penetration testing on a regular basis. Testing should occur at least annually. Additionally, any important change should trigger testing. This could include infrastructure or application upgrades, new offices or significant changes to assets and services.

Ensuring Customer Safety

Responsible security providers take great care to protect their customers during penetration testing. This means carefully controlling the testing environment with multiple safety measures in place. For

instance, testers should work with the organization prior to conducting the test to determine any activities and devices that should be excluded from the testing process.

Advantages of eCare Penetration Testing

eMazzanti consultants have conducted thousands of penetration tests using an advanced penetration testing framework combined with our expert manual penetration methodology. By using both automated scanning and manual testing, we replicate the attacker mindset and highlight more weaknesses.

Using the results of the penetration testing we will assist your organization with choosing and implementing security strategies specifically designed to optimize investment and provide the best protection.