Trustwave®

Penetration Testing: What It Is and Why It's Crucial to Enterprise Security

While the term is familiar to nearly everyone in the cybersecurity field, penetration testing is often misunderstood or underappreciated. Let's explain this critical component of corporate security, and clear up a few myths.

What is penetration testing?

A penetration test, commonly known as a pen test, is a simulated cyberattack on a computer system and/or network, authorized by its owner. The goal of pen testing is to evaluate the system's security and find any weak spots. As such, it is a component of any enterprise-grade security audit.

Unlike a vulnerability test, pen testing is primarily a manual process in which skilled, experienced teams use a variety of tools and techniques. (We'll say more about vulnerability testing in a moment.)

Because pen testers typically use various automated tools, some security leaders mistakenly believe they're "just running scripts" and question the pen test's value. In reality, the human element makes all the difference. The ability to understand nuances, think creatively, and make and test hypotheses distinguish a human-led penetration test from automated tools.

In most cases, organizations preselect the systems to be targeted in a pen test and give the tester some inside knowledge about them, such as an authorized user might have. This is called **gray box testing**. Other times, pen testers go in with no information about the target to perform **black box testing**, or with a wealth of information and even open dialog with the client security team (**white box testing**).

Each option offers tradeoffs between thoroughness, time required, and ROI. Ultimately, the decision may come down to the goals of the exercise. Some organizations may want to ensure measures they've taken after a previous breach are effective, while others may want to focus on safeguarding their most valuable data from the most skilled intruders.

Why is pen testing important?

Penetration testing helps organizations identify weak spots in their systems that are most likely to be exploited by attackers. A well-run pen test performed by experienced specialists involves not just finding vulnerabilities, but explaining the potential impact if a vulnerability is exploited. In some instances, a single compromise can undermine the integrity of the whole environment, while other vulnerabilities present little practical risk to critical data even if exploited.

Essentially, a pen test is a non-destructive way to find potential security gaps before an attack occurs. That's an important point because reputation and trust are crucial in today's business world. It's not enough to tighten up security in the wake of a breach; organizations must take proactive measures like pen testing to prevent breaches in the first place. In recent years, too many businesses to count have lost trust from consumers, their supplier ecosystem, and the market when sensitive data was stolen.

In many industries and locales, pen testing is also critical for compliance reasons. Businesses in the healthcare, financial services and defense sectors are especially sensitive to regulatory issues. But given today's complex global supply chain, it's likely that regardless of industry, all companies will be forced to demonstrate compliance for some nation or agency.

Vulnerability testing alone isn't enough

We noted above that a vulnerability assessment is a mostly automated process that relies on a scanning tool (or collection of tools) targeting a range of IP addresses. While an important component of any organization's security portfolio, automated vulnerability assessments – even those that use some form of artificial intelligence (AI) – have weaknesses including the following:

- **False positives.** The automated tool thinks it has found an issue that doesn't in fact exist.
- **Erroneous priority ratings.** The tool reports a finding as high priority or even critical, but because the target is on a secure, internal network, the actual risk is lower.
- **Multiple issues stemming from a single root cause.** The tool generates a 1,000-page list of 100 servers, each of which requires the same 30 patches.

The primary difference between an automated vulnerability assessment and a manual penetration test, then, is that the latter adds human intelligence that brings a creative, outside-the-box mindset focused on identifying clues and creating hypotheses to test.

While a vulnerability assessment can tell you where potential flaws are and what needs patching, pen testing demonstrates how vulnerabilities can be exploited, and how likely an exploit may be. Thus, a properly conducted pen test results in a report that both details priority recommendations and takes into account specific business contexts and risks.

A helpful analogy is to consider a break-in targeting your home. A vulnerability assessment can determine whether the locks are secure and a window is ajar. But a penetration test can tell you if a skilled burglar could pick the locks and open the window without leaving telltale evidence.

No substitute for the human touch

We'd all like to think AI tools will solve our security problems. They can certainly help, but the fact is there's no substitute for experienced, knowledgeable humans as a way to prevent potentially catastrophic data breaches. Human-led penetration testing remains a critical component of any enterprise data security program.

To learn more, **contact us** or
see our **Quick Reference Guide on Penetration Testing**.

Trustwave®

www.trustwave.com