Do You Need Penetration Testing?

The Security Benefits You Need

What Is Penetration Testing?

Penetration testing ("pen testing") is an attempt to evaluate the strength of an IT infrastructure's security defenses. Overall, pen testing is a "simulated attack" to discover vulnerabilities that may result from outdated or unpatched operating systems, improper security configurations, software application flaws, service flaws, or risky end-user behavior. Pen testing typically includes application pen testing, network pen testing of the underlying hosts and infrastructure, and wireless network pen testing. Pen testing may also include social engineering, where the employees are the target.

Penetration Testing Exposes

- ✓ Encryption Problems
- ✓ Improper Network Configurations
- ✓ Backdoors
- ✓ Weak Passwords
- ✓ Risky User Behaviors
- ✓ Outdated or Unpatched Operating Systems
- ✓ Application Flaws
- ✓ Remote Work Setup Configurations

Implementing a Pen Test Strategy

- **Schedule Regular Pen Tests:** Your routine risk assessment strategy should include routine pen testing, especially if any of your staff work remotely.
- **Pen Testing vs. Vulnerability Scanning:** Vulnerability scans identify potential vulnerabilities and report risk exposure. Pen testing attempts to exploit identified vulnerabilities to simulate an attack. Think of it as "you *might* be vulnerable" (scan) vs. "I owned your server by using this exploit" (pen test).
- **States of Pen Testing:** Your penetration strategy can be broken down into five stages: Planning, Scanning, Exploitation, Maintaining Access and Analysis.
- **Discover your vulnerabilities:** Schedule a regular pen test with our experts today!

Types of Pen Testing include essentially three questions:

1. Where is the attack coming from? (Internal vs. External)
2. How much information does the tester have on the target? (White Box – full information, Black Box – only enough info to establish the target and Grey Box – limited information)
3. Do the employees (especially the SOC) know the test is occurring? (Covert vs. Overt)

www.aisn.net | P: 888.401.AISN | **E:** sales@aisn.net