Understanding Penetration Testing

What every business owner should know about ethical hacking

What Is Penetration Testing?

Penetration testing — often called a pen test — is an authorized, simulated cyberattack on your IT environment performed by security professionals. The goal is simple: find the weaknesses in your network, applications, and people before a real attacker does. A good pen test goes beyond automated scans and applies the same creativity and persistence a determined criminal would use.

Why It Matters for Small & Medium Businesses

43% of cyberattacks target small businesses, and most successful breaches exploit vulnerabilities that have been known for months or years. Penetration testing tells you exactly which doors are unlocked in your environment, prioritized by risk, so you can fix what matters most without burning budget on theoretical threats.

The Five Phases of a Pen Test

- Planning & scoping — agree on systems, rules of engagement, and goals
- Reconnaissance — gather public information about your business and assets
- Exploitation — actively attempt to breach systems using identified weaknesses
- Post-exploitation — see how far an attacker could move once inside
- Reporting & remediation — clear findings, severity ratings, and fix guidance

How Often Should You Test?

At minimum, run a full penetration test once a year. Re-test after any major infrastructure change — a new firewall, a cloud migration, a merger, or a significant application release. Many compliance frameworks (PCI DSS, HIPAA, SOC 2) either require or strongly recommend annual testing.

Pen Test vs. Vulnerability Scan

A vulnerability scan is automated and tells you what could be wrong. A penetration test is human-led and proves what an attacker can actually do with those weaknesses. Both belong in a mature security program, but only a pen test simulates a real adversary.