PENETRATION TESTING & VULNERABILITY SCANNING

CYBERLEAF

Find It Before They Exploit It

Penetration Testing vs. Vulnerability Scanning

Most breaches exploit gaps you already have—automated scans catch known signatures, but they can't chain vulnerabilities together the way a real adversary would. Understanding the difference between penetration testing and vulnerability scanning is the first step toward closing the gaps that actually lead to breaches.

Penetration Testing	Vulnerability Scanning
How It Works • Manual + automated testing by certified experts (OSCP, GPEN, GXPN) • Simulates real-world attack paths and chains vulnerabilities together • Tests networks, applications, people, and processes	**How It Works** • Automated tools scan systems for known CVEs • Checks for missing patches and misconfigurations • Runs continuously or on a scheduled cadence
What It Tells You • What can actually be breached • How far an attacker can move laterally • Business impact of successful attacks	**What It Tells You** • What might be vulnerable • Missing patches and outdated software • Configuration weaknesses across your environment
Best For • Measuring true organizational risk • Validating security controls & defenses • Regulatory, compliance, or customer assurance	**Best For** • Ongoing security hygiene & patch management • Continuous compliance monitoring • Broad coverage across large environments
What You Get • Proof-of-concept exploitation for every finding • Mapped attack paths with severity ratings • Prioritized remediation with business impact analysis • Executive summary + technical detail report	**Limitations** • No actual exploitation of vulnerabilities • Possible false positives requiring analyst review • Limited business context without manual validation • Cannot test detection & response capabilities

Compliance Frameworks That Require Testing

SOC 2 | HIPAA | CMMC | NIST 800-171 | PCI DSS | ISO 27001

Cyberleaf's 4-Step Testing Methodology

Scope Define rules of engagement, success criteria, and map your attack surface.	**Test & Exploit** Automated scanning + manual exploitation mirroring real adversary techniques.	**Analyze & Report** Detailed findings with severity ratings, PoC evidence, and remediation steps.	**Remediate & Retest** Validate fixes are effective and no new issues were introduced.

Ready to test your defenses? Start a conversation @ cyberleaf.io