nuHarbor

SERVICE OVERVIEW

PENETRATION TESTING SERVICES

Validate Security. Reduce Risk. Strengthen Resilience.

Vulnerability scans and compliance assessments flag potential weaknesses. Penetration testing proves the gaps and misconfigurations attackers can actually exploit across applications, infrastructure, and networks. nuHarbor provides independent validation of your security posture, translating technical findings into clear business risk so you know exactly where attackers could get in and what they could reach.

Why Penetration Testing Matters

Find gaps before attackers do

Identify and eliminate exploitable vulnerabilities before they become business-impacting incidents.

Strengthen your security posture

Evaluate controls across applications, infrastructure, cloud environments, and user workflows.

Enable informed business decisions

Executive-ready reporting summarizes risk to help justify and prioritize security investment.

Protect data & user accounts

Test authentication, authorization, and app workflows to reduce data exposure and account compromise.

Prioritize remediation with confidence

Get a clear, risk-based roadmap that focuses your team on the vulnerabilities that matter most.

Support compliance & audits

Satisfy security testing requirements for PCI DSS, HIPAA, SOC 2, ISO 27001, and more.

Verify security after major changes

Confirm migrations, segmentation, and new deployments haven't introduced new risk.

nuHarbor Penetration Testing Service Offerings

Web Application Testing

In-depth assessment of web apps and APIs, covering OWASP Top 10 and business-logic flaws that automated tools miss.

Internal Penetration Testing

Simulated insider attack testing privilege escalation, lateral movement, and reach to critical assets.

External Penetration Testing

Simulated attack on internet-facing systems such as servers, firewalls, VPNs, and cloud to find remotely exploitable flaws.

Wireless Penetration Testing

Testing Wi-Fi authentication, encryption, segmentation, and rogue / evil-twin device attack vectors.

What's Included

Strategic Scoping & Test Design
We define objectives, critical assets, and a tailored methodology upfront so testing stays focused and aligned to your goals.

Daily Engagement Updates
Concise start-of-day and end-of-day communications give visibility into progress and what comes next.

Immediate Escalation of Critical Findings
Discover a critical risk and we pause, document, and notify your team right away, no waiting for the report.

Multi-Layer Peer-Reviewed Reporting
Findings are documented by the lead operator, reviewed by a second consultant, and finalized by a senior reviewer.

Findings Review Meeting
A guided walkthrough of key findings, business impact, and remediation priorities for technical teams and leadership.

Optional Follow-up Session
Deeper technical questions, remediation planning, or leadership-level context after you review internally.

Optional Retesting
Targeted retesting of critical and high-risk findings to validate that corrective actions were successful.

Why nuHarbor

Experienced Operators
Senior consultants who test the way real adversaries do, backed by deep offensive-security expertise.

Human-Led Testing
Hands-on-keyboard testing uncovers business-logic and chained vulnerabilities automated scanners miss.

Peer-Reviewed Reporting
Every finding is validated through multiple layers of review before it ever reaches your team.

Tailored Engagements
Scope, methodology, and reporting are shaped around your environment, compliance needs, and goals.

Long-Term Security Partnership
We stay with you well beyond the test, a trusted harbor rather than a one-time vendor.

Clear, Actionable Results
Technical findings translated into prioritized business risk, so you know exactly what to fix first.

Explore Comprehensive Cybersecurity Protection Today

Talk with our team about scoping a penetration test for your environment.

nuharborsecurity.com/services/penetration-testing

Get a Pen Test Quote →