

Penetration Testing

Proactively Identify and Remediate Security Gaps

Cyber threats evolve daily, and attackers continuously seek vulnerabilities to exploit. Liquid C2's penetration testing services help organisations identify, assess, and remediate security weaknesses before they become entry points for cybercriminals. Our certified security experts simulate real-world attack scenarios across various environments to enhance your security posture and meet compliance requirements.

Our Penetration Testing Services

Application Penetration Testing

Determine whether your web, mobile, API, or desktop applications have exploitable vulnerabilities with our test methodology based on the OWASP application testing guidelines.

External Penetration Testing

Meet your compliance requirements and test the effectiveness of your perimeter security controls in preventing and detecting attacks against your internet-facing assets by an external attacker.

Internal Penetration Testing

Meet your compliance requirements and test the effectiveness of your internal controls in preventing an adversary from laterally moving across your internal network and compromising your organisation's crown jewels.

Wireless Penetration Testing

Determine if an adversary can exploit your internal systems through your wireless services and validate the configuration and encryption of your access points to identify vulnerabilities and provide remediation advice.

Container Penetration Testing

Determine externally whether the clusters' assets are misconfigured or vulnerable to attacks and identify how far an attacker can go if a container is compromised or if the clusters' API services and CI/CD tools are misconfigured.

Why Choose Liquid C2?

Certified Security Experts

OSWE, OSCE, OSCP, OSWP, GPEN, GWAPT, CEH, CISSP, among others

Industry-Recognised Testing Methodologies

OWASP, MITRE ATT&CK

Customisable Testing Approach

Based on Your Business Risks

Detailed Remediation

Guidance to Strengthen Your Security Posture

Pentesting Service Packages

Essential Penetration Testing Package (Basic Security Validation)	Advanced Penetration Testing Package (Comprehensive Security Assessment)	Enterprise Penetration Testing Package (Full-Scope Security Testing)
Best for: Organisations looking to meet basic security requirements and compliance mandates.	Best for: Businesses seeking a more in-depth security review and regulatory compliance readiness.	Best for: Large enterprises, financial institutions, and high-risk industries requiring a robust cybersecurity defence strategy.
Includes: <ul style="list-style-type: none"> <input checked="" type="checkbox"/> External Penetration Testing <input checked="" type="checkbox"/> Web Application Penetration Testing (1 application) <input checked="" type="checkbox"/> High-Level Security Report & Recommendations <input checked="" type="checkbox"/> One Retest After Fixing Identified Issues 	Includes: <ul style="list-style-type: none"> <input checked="" type="checkbox"/> Everything in the Essential Package <input checked="" type="checkbox"/> Internal Penetration Testing <input checked="" type="checkbox"/> Wireless Penetration Testing <input checked="" type="checkbox"/> Mobile Application Penetration Testing (1 application) <input checked="" type="checkbox"/> Detailed Risk-Based Report with Actionable Insights <input checked="" type="checkbox"/> Two Retests & Security Advisory Session 	Includes: <ul style="list-style-type: none"> <input checked="" type="checkbox"/> Everything in the Advanced Package <input checked="" type="checkbox"/> Container Penetration Testing <input checked="" type="checkbox"/> Red Teaming & Social Engineering Simulations <input checked="" type="checkbox"/> Custom Testing Scope Based on Business Risks <input checked="" type="checkbox"/> Continuous Security Monitoring for 30 Days Post-Test

Get started today!

Secure your business before cyber attackers do. Contact us for a consultation and choose the right penetration testing package for your needs.

Learn more at www.LiquidC2.com

Email c2_info@liquid.tech