

Internal Penetration Testing

Uncover Internal Threats Before Attackers Do

Your organisation's internal network can be just as vulnerable as its external perimeter. Liquid C2's Internal Penetration Testing helps identify and remediate misconfigurations, privilege escalation paths, and lateral movement opportunities before they can be exploited by malicious insiders or compromised accounts.

This service is designed to validate the effectiveness of internal security controls and ensure compliance with regulatory and industry requirements. The scope includes internal IPs and infrastructure.

Internal Penetration Testing Packages		
Silver Package	Gold Package	Platinum Package
<p>Best for: Organizations looking to establish a baseline understanding of internal network vulnerabilities.</p>	<p>Best for: Security-conscious teams seeking a deeper assessment of internal threat exposure and network segmentation.</p>	<p>Best for: Organisations requiring the most extensive internal security testing, including advanced Active Directory exploitation.</p>
<p>Includes:</p> <ul style="list-style-type: none"> <input checked="" type="checkbox"/> Automated Vulnerability Scanning on provided internal IP addresses <input checked="" type="checkbox"/> Manual Validation of Discovered Vulnerabilities <input checked="" type="checkbox"/> Network Discovery (Ping Sweep, ARP Scan, DNS, SNMP) <input checked="" type="checkbox"/> Detection of Open Ports, Outdated Services, Missing Patches <input checked="" type="checkbox"/> Risk Prioritisation & Remediation Guidance <input checked="" type="checkbox"/> Black Box Testing 	<p>Includes:</p> <ul style="list-style-type: none"> <input checked="" type="checkbox"/> All features of the Silver Package <input checked="" type="checkbox"/> Network Exploitation Techniques (e.g., Man-in-the-Middle, Spoofing, SMB Attacks) <input checked="" type="checkbox"/> Credential Harvesting & Reuse <input checked="" type="checkbox"/> Pivoting and Lateral Movement within Internal Segments (excluding AD-focused attacks) <input checked="" type="checkbox"/> Identification of Segmentation Flaws & Access Control Issues 	<p>Includes:</p> <ul style="list-style-type: none"> <input checked="" type="checkbox"/> All features of the Gold Package <input checked="" type="checkbox"/> Active Directory Enumeration & Exploitation (Kerberoasting, AS-REP Roasting, ACL Abuse) <input checked="" type="checkbox"/> Privilege Escalation to Domain Admin <input checked="" type="checkbox"/> AD Misconfiguration Detection
<p>Deliverables: Technical Report with Vulnerabilities Risk Rating</p>	<p>Deliverables: Technical Report with Vulnerabilities Risk Rating + Remediation Roadmap</p>	<p>Deliverables: Technical Report with Vulnerabilities Risk Rating + Full Remediation Roadmap</p>

Why Choose Us?

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

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.

Email: C2_info@liquid.tech | **Website:** www.liquidC2.com