HALOCK®

PENETRATION TESTING SERVICES

What types of penetration tests can be performed?

External Network Penetration Test
Performed remote to the perimeter to simulate an external attack, comprehensive testing focuses on exploiting weaknesses on internet facing hosts and services with the intent of escalating access to the protected environment.

Internal Network Penetration Test
Performed from within, internal attack scenarios are pursued to identify exploits that could be leveraged by a malicious insider, threats from across the wide area network, or the extent a compromised system could be leveraged to escalate access to systems deployed across the local area network.

Web Application Penetration Test
For custom developed web applications, a comprehensive review is necessary to identify vulnerabilities such as SQL injection. The test approach is fully customized to ensure the functionality available to the various users of the web application is comprehensively tested for weaknesses.

Internal Wireless Penetration Test
Wireless penetration tests assess the adequacy of multiple security controls designed to protect access to wireless services. Testing attempts to exploit wireless vulnerabilities to gain access or escalate privileges within private or guest wireless networks.

Onsite Social Engineering Penetration Test
Onsite testing is performed to assess the effectiveness of physical security controls, employee response to suspicious behavior, perimeter defenses, and validate that network security controls prevent an attacker from gaining network access.

Remote Social Engineering Penetration Test
Covert testing designed to validate the effectiveness of user security awareness, incident response, malware defenses, local permissions, and egress protections. Testing involves issuing carefully crafted emails designed to lure users to fictitious "malicious" websites, compromise endpoints, escalate privileges, and establish access to the internal environment.

Remediation Verification Penetration Test Attempts to reproduce vulnerabilities and associated exploits are performed to verify if vulnerabilities have been successfully remediated, providing independent confirmation that corrective measures have been implemented.

What deliverables do HALOCK's penetration tests provide?

The complete results of the penetration test are documented in our content rich HALOCK Penetration Test Report which include summary of findings, detailed findings, test timeline, scope and methodology, and supplemental content for context and reference. The comprehensive results document and explain each vulnerability, the impact, evidence, instances observed, and recommendations for remediation. Exploits are visually documented step by step to demonstrate impact and ensure a complete understanding of how the exploit is performed.

About HALOCK

Founded in 1996, HALOCK Security Labs is a thought-leading information security firm, that combines strengths in strategic management consulting with deep technical expertise. HALOCK's service philosophy is to apply just the right amount of security to protect critical assets, satisfy compliance requirements and achieve corporate goals. HALOCK's services include: Security and Risk Management, Compliance Validation, Penetration Testing, Incident Response Readiness, Security Organization Development, and Security Engineering.