HALOCK®

WIRELESS PENETRATION TEST

What is a Wireless Network Penetration Test?

Wireless penetration tests assess the adequacy of multiple security controls designed to protect unauthorized access to wireless services. Testing attempts to exploit wireless vulnerabilities to gain access to private (protected) wireless SSIDs or to escalate privileges on guest SSIDs intended to be isolated from private networks.

Why should we conduct a Wireless Penetration Test?

The wireless network brings convenience and mobility to internal users, but with this convenience comes additional risks. An attacker does not need to gain physical access if vulnerable wireless networks can be compromised from a safe distance. Wireless access provided to guests and visitors needs to be isolated from protected environments. Wireless provided to employees needs to protect those connections and the data transmitted over the air. Testing wireless networks is a critical activity to ensure wireless networks are providing the intended access and only the intended access.

Why should HALOCK perform our Wireless Penetration Test?

HALOCK has the experience to best assess the adequacy of multiple security controls designed to protect unauthorized access wireless services. For over two decades, HALOCK has conducted thousands of successful penetration tests for companies of all sizes, across all industries.

HALOCK's dedicated penetration test team is highly **qualified**, possesses advanced certifications, and is equipped with the labs, tools, and methodologies necessary to consistently deliver quality, **accurate**, detailed, and meaningful results.

HALOCK leverages industry standard methodologies to ensure a thorough and **comprehensive** test is conducted under safe and controlled conditions. HALOCK's reports are content rich, regularly stand the scrutiny of regulatory requirements, **exceed expectations** of auditors, and frequently receive the praise of our customers. HALOCK does not simply validate automated scans. HALOCK's **expert** team discovers vulnerabilities not yet published and often not yet discovered. Exploits are pursued, documented step by step, with screen capture walkthroughs, to provide both the technical and visual **clarity** necessary to ensure corrective actions can be prioritized and remediation is **effective**.

How do I choose which wireless networks and sites to test?

Testing should include each type of wireless network, including guest networks, BYOD, private, and facilities. The configurations for each type are as unique to the intended purpose of the deployments. When wireless networks span many physical locations, but are centrally managed with common configurations, sampling is often utilized to test each unique wireless setup such that recommendations can be implemented across the enterprise. The key to selecting the scope of a wireless penetration test is to ensure each unique type of wireless is tested to produce comprehensive results without performing unnecessary and redundant testing.

"Thank you for all your help."

-Professional Association

HALOCK®

WIRELESS PENETRATION TEST

A Comprehensive Testing Methodology

Wireless Reconnaissance

Detecting and identifying authentication methods supported, encryption requirements, MAC address restrictions, and the technologies in use.

Network Reconnaissance

Exploring connected networks to identify lateral targets, test segmentation, and bypass intended restrictions on movement within the wireless network.

Mac Address Filtering Bypass

Attempts to bypass evaluate the effectiveness of MAC address filtering through cloning, enumeration, and bypass attacks.

Encryption Exploits

Testing encryption methods and effectiveness, attempts to intercept information from other connected users, and performing decryption attacks.

Authentication Attacks

Tests targeting password complexity, authentication handshake manipulation, and password cracking attempts.

Session Management

Targeting legitimate end users, attempts to inject or hijack existing sessions, bypass replay protection mechanisms, manipulate session state or session assignment methods, or leverage insecure wireless session management.

Privilege Escalation

Identifying potential targets on the protected network, bypassing segmentation rules, and leveraging the wireless network to pursue further internal attacks.

Deliverables

Project Plan: Prior to testing, HALOCK will develop a project plan detailing the specific plan, timing, and related considerations. This ensure all parties know what to expect throughout the execution of testing and reporting.

Penetration Test Report: The complete results of the penetration test are documented in our content rich report which includes the background, summary of findings, detailed findings, scope and methodology, and supplemental content for context and reference. **Samples available upon request.**

- **Background:** An introduction of the general purpose, scope, methodology, and timing of the penetration test.
- **Summary of Findings:** A concise overview summarizing the results at a glance, such as key critical findings requiring priority attention, system or recurring issues, and other general results.
- **Detailed Findings:** Comprehensive results of each vulnerability, including a description of the vulnerability observed, the impact, recommendations for remediation, evidence where the vulnerability was observed, step-by-step demonstrations of exploits performed, and additional reference materials.
- **Scope and Methodology:** A detailed recap of the specific scope of what was tested, the methodologies utilized, and related historical information necessary for audiences such as auditors to understand the specifics of the test approach.
- **Supplemental Content:** Additional content and guidance, such as recommended post assessment activities.

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, enhance social responsibility, and achieve corporate goals. With HALOCK, organizations can establish reasonable security and acceptable risk. HALOCK's services include: Security and Risk Management, Compliance Validation (HIPAA, PCI DSS, CCPA), Penetration Testing, Incident Response Readiness, Security Organization Development, and Security Engineering.

HALOCK | halock.com | 847-221-0200 | Incident Response Hotline: 800-925-0559