HALOCK®

INTERNAL NETWORK PENETRATION TEST

Because your internal assets are meant to stay internal.

What is an Internal Network Penetration Test?

Internal penetration tests are more thorough than automated vulnerability scans in that comprehensive testing efforts focusing on exploiting weaknesses with the intent of gaining access to assets positioned within the private network. They are performed internal to the environment to simulate insider threats, targeting networks, hosts, and responding services.

Why should we conduct an Internal Network Penetration Test?

The perimeter cannot be relied upon exclusively to protect internal systems. An attacker needs only one path to gain access. Once inside, an insecure internal network can be exploited to rapidly escalate privileges. Internal network safeguards are critical to prevent a malicious user from achieving unauthorized access to protected data. Internal attacks have severe results and often go undetected for longer periods of time. Performing internal testing identifies vulnerabilities on critical internal assets, demonstrates the impact if exploited, and provides clear direction on improvements that can be implemented to mitigate that risk. PCI DSS requires internal network pen tests and network segmentation testing annually, unless you are a service provider, which requires testing every six months.

Why should HALOCK perform our Internal Network Penetration Test?

HALOCK has the **experience** to best simulate internal network testing conditions, such as when an attacker is a malicious individual internal to the organization, when an external attacker has achieved internal access by compromising an internal endpoint, or has achieved entry point through an external host. 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**.

What internal networks should we test?

Rarely does an attacker gain access by directly targeting a specific sensitive asset. This is intuitive because those sensitive assets are typically the most protected. In most cases, attackers gain initial access by targeting networks and services that are perceived as a lesser concern to the organization. The security is commonly less robust, allowing the attacker to gain an initial foothold. From this position, the attacker then escalates and pivots until they amass the rights needed to gain access to the critical asset. A smaller organization may include the entire environment. A larger organization typically selects representative ranges spanning servers, workstations, networks, voice, and other assets. This allows the penetration tester to explore controls across the spectrum of the organization and the relationship between the components of the environment.

While you cannot always choose ***if*** a penetration test needs to be conducted,
you ***can*** choose the provider that will deliver the results you expect.

HALOCK®

INTERNAL NETWORK PENETRATION TEST

A Comprehensive Testing Methodology

Reconnaissance

Initial reconnaissance activities to locate responding hosts and services across each public IP range and facilitate the development of the target list.

Target Planning

Initial targets are selected based on perceived opportunity and prioritized for first stage attacks.

Vulnerability Enumeration

Vulnerabilities, both published and undocumented, are enumerated to identify potential exploits to pursue on each targeted host.

Vulnerability Validation

Additional testing to confirm valid vulnerabilities, eliminate false positives, and validate target selection.

Attack Planning

Utilizing the information gathered, the methods, tools, and approaches are selected to pursue services likely to present opportunity to gain access.

Exploit Execution

Tests are conducted to establish command and control, ideally with persistence, to vulnerable hosts, applications, networks, and services.

Privilege Escalation and Lateral Movement

Post exploit actions are performed to gain additional access, penetrate further into the internal environment, escalate privileges, compromise lateral hosts, and harvest additional information.

Data Exfiltration

Locating sensitive information, configuration information, and other evidence is gathered to demonstrate impact.

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.

Background: An introduction of the general purpose, scope, methodology, and timing of the penetration test.

Summary of Findings: A brief but 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, that provides added value to the audience of the report.

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.