What is an External Network Penetration Test?

External penetration tests are more thorough than automated vulnerability scans in that comprehensive testing efforts focus on exploiting weaknesses with the intent of gaining access to the environment. They are performed remote to the environment to simulate an external attack, targeting responding internet facing hosts and services.

Why should we conduct an External Network Penetration Test?

The network edge is the last barrier to the open internet. With increased data breaches and attacks on businesses of all sizes, customers, regulators, and insurers virtually all require regular testing to ensure the perimeter is a reliable stronghold against attackers. PCI DSS requires annual testing. Exploitable vulnerabilities can allow an attacker to compromise an organization's network and gain access to sensitive data. Proactively testing the effectiveness of security controls identifies these weaknesses so companies can implement protective measures to mitigate risk.

Why should HALOCK perform our External Network Penetration Test?

HALOCK has the **experience** to best evaluate security controls. 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 select external networks to be targeted?

Any internet facing network ranges presents an attacker with opportunity to gain access, however those exposing services such as websites, mail servers, customer portals, remote access, and related services are key. An attacker needs just one vulnerable service to gain an initial entry point, therefore subjecting the full ranges to penetration testing is prudent. Organizations with a smaller footprint externally typically include all assets in the scope of review. For organizations with substantial environments, duplication and redundancy, or other considerations, sampling is a common approach to explore all the various types of systems while minimizing the cost and effort needed to comprehensively identify exploitable vulnerabilities.

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®

EXTERNAL NETWORK PENETRATION TEST

A Comprehensive Testing Methodology

HALOCK's approach to External Network Penetration Testing provides a flexible framework for comprehensively identifying and evaluating technical vulnerabilities. The following phases are typically incorporated into the penetration test, as they apply to the target environment:

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 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 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.