HALOCK®

ONSITE SOCIAL ENGINEERING PENETRATION TEST

Securing the premises.

What is an Onsite Social Engineering Penetration Test?

Onsite social engineering penetration tests are 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.

Why should we conduct an Onsite Social Engineering Penetration Test?

The most secure locks on a door mean nothing if a well intending employee holds the door open to the attacker. Security awareness extends well beyond identifying malicious email. Performing onsite social engineering is a highly effective method for confirming physical security controls work, that employees are not negating these controls, and that the interior of a facility is well defended against the uninvited visitor. Controlled tests allow an organization to evaluate the effectiveness of each physical layer, beginning with the exterior. If a visitor is granted access, onsite social engineering can confirm if that access is appropriately limited.

Why should HALOCK perform our Onsite Social Engineering Penetration Test?

HALOCK has the experience to evaluate employee security awareness on office premises. 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**.

Which facilities should be considered for testing?

It depends. For organizations comprised of a single location, the answer is simple. When organizations span multiple locations, each site may have a unique set of requirements specific to the purpose of that site. For example, a high security data center may have very restrictive access controls. A remote field office may present different challenges to secure the site and require different methods to validate. Any facility can be considered for onsite social engineering. When sampling is implemented, site selection is typically influenced by sensitivity, regulatory requirements, and related considerations unique to each categorical site classification.

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®

ONSITE SOCIAL ENGINEERING PENETRATION TEST

A Comprehensive Testing Methodology

Information Gathering

Activities performed prior to testing to gather the necessary information to prepare one or more strategies for each target site such as visitor and/or guest access procedures, facility layouts, locating cameras and detection systems, and observing entry methods.

Attack Planning and Preparation

Development and preparation of strategies for gaining access determined to have the highest likelihood of success, such as fabricating access badges, cloning RFID keycard access, deploying wireless capture devices, or leveraging other weaknesses unique to the site.

Entry Exploits

Initial attempts are unassisted to gain access beyond the perimeter using methods prepared during attack planning and establishing a presence internal to the site.

Establish Persistence

Attempts to establish a return entry point are conducted to ensure the attacker has reliable internal access using methods such as rogue wireless access deployment, establishing remote command and control on unattended endpoint systems, or performing other suitable methods as opportunity presents.

Network Exploits

Gathering supporting evidence, identify network weaknesses that could be leveraged by an onsite attacker, and identify potential secondary lateral targets on the network.

Testing Physical Vulnerabilities

Pursuing physical vulnerabilities such as deploying/retrieving keystroke loggers, accessing sensitive information not secured within the environment, or escalating access to higher security areas within the site such as server rooms.

Disengaging

Winding down access, removing persistence, and obtaining any remaining evidence or artifacts required for reporting purposes.

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.