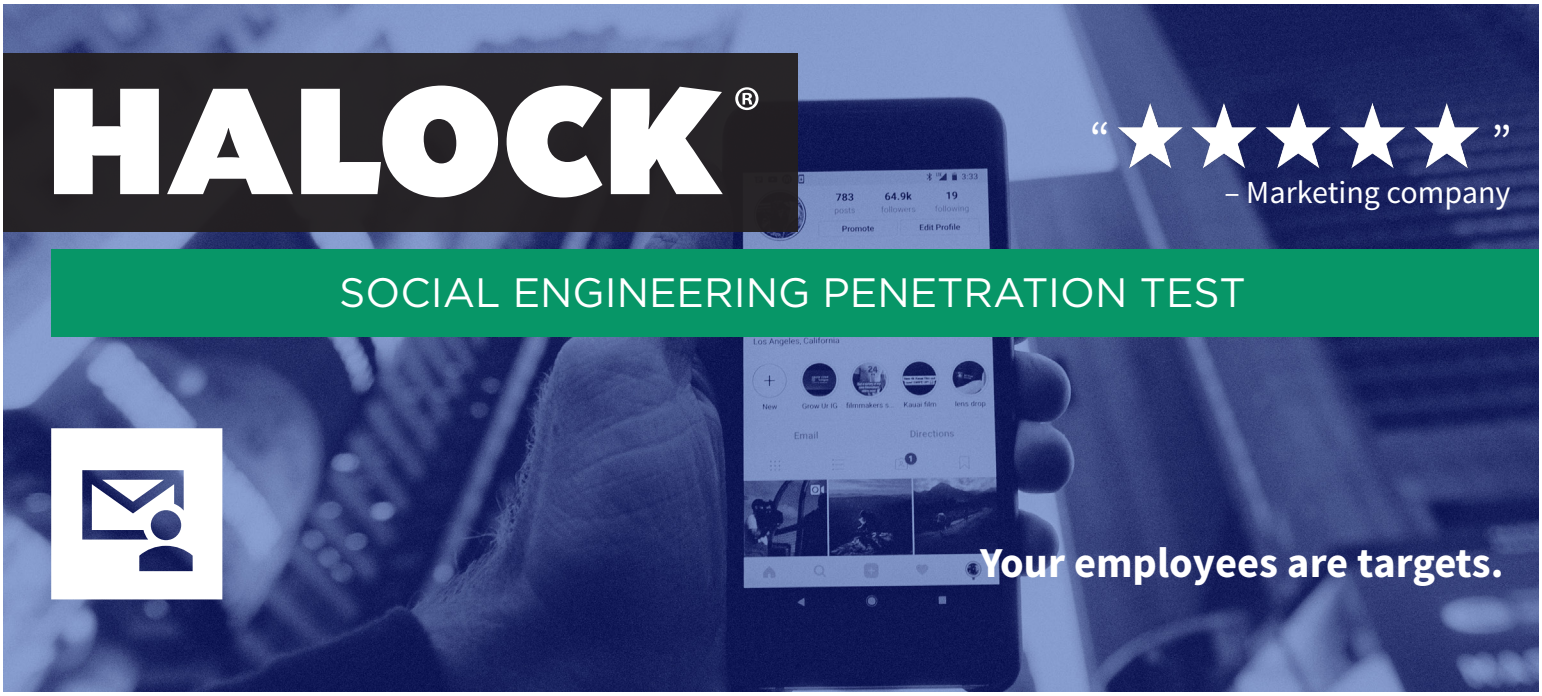
HALOCK®

"★★★★★"
– Marketing company

SOCIAL ENGINEERING PENETRATION TEST



What is a Social Engineering Penetration Test?

Social engineering penetration tests validate the effectiveness of user security awareness, incident response, and network security controls such as malware defenses, local permissions, and egress protections. Performed under controlled conditions, testing involves issuing carefully crafted emails to lure users to fictitious "malicious" websites, attempts to compromise these users, escalate privileges, and penetrate the internal environment.

Why should we conduct a Social Engineering Penetration Test?

Targeting employees is a rapidly increasing threat that attackers use to gain access. Organizations routinely provided trusted employees with access to sensitive data. If an attacker can compromise the user, they instantly have rights to whatever that employee could access. Performing controlled spear phishing exercises test not only employee security awareness and incident response, but also the controls established to minimize the impact of a successful breach. Most security standards and regulations require security awareness training. Social engineering is the most effective method of confirming it works.

Why should HALOCK perform our Social Engineering Penetration Test?

HALOCK has the experience to best assess how well an organization's security awareness policies and procedures are performed. 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 employees to test?

You don't. The attacker does. When preparing for a social engineering test, there may be circumstances where certain employees cannot be included, however all remaining employees should be considered potential targets. An attacker is best equipped with a broad and diverse list of targets spanning multiple business units, job functions, or roles. This allows the attacker to probe and identify where opportunity presents. Information gathered is re-purposed and leveraged for subsequent contact attempts. An attacker will generally not target all employees as doing so increases the likelihood of detection. To simulate these conditions, the penetration tester will select targets from the list, adding targets as testing progresses, with the goal of evading detection for as long as possible.

HALOCK®

SOCIAL ENGINEERING PENETRATION TEST

A Comprehensive Testing Methodology

Information Gathering

Initial reconnaissance activities to gather the necessary information to prepare suitable and credible messaging, such as the services the target organization offers, relationships between varying business units or divisions, information exposed on public sources, and other employee or corporate specific information

Infrastructure Prepartion

Systems to transport email, track responses and activity, and host content are deployed and configured.

Campaign Preparation

Target lists are grouped and sequenced, campaign batches are configured and scheduled, and related preparation tasks are completed.

Campaign Launch

Initial test messages are issued to gauge response behavior, identify technical controls that might warrant revising the planned approach, and fine-tuning attack methods.

Initial Exploits

As sessions are established, initial exploits are pursued to establish baseline access through payloads, command and control, scripted actions, identify secondary targets on the compromised network, and establish persistence.

Secondary Exploits

Attempts to increase a presence throughout the connected environment by bypassing user access controls, identifying internal weaknesses to exploit, leveraging excessive user rights, and compromising connected systems.

Exfiltration

Attempts to identify local data repositories that would be of value to an attacker stored on locations such as local repositories, mapped drives, databases, and file sync folders.

Disengaging

Winding down activities including terminating sessions, gathering evidence necessary for reporting, and preventing continued contact following the conclusion of the campaign.

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