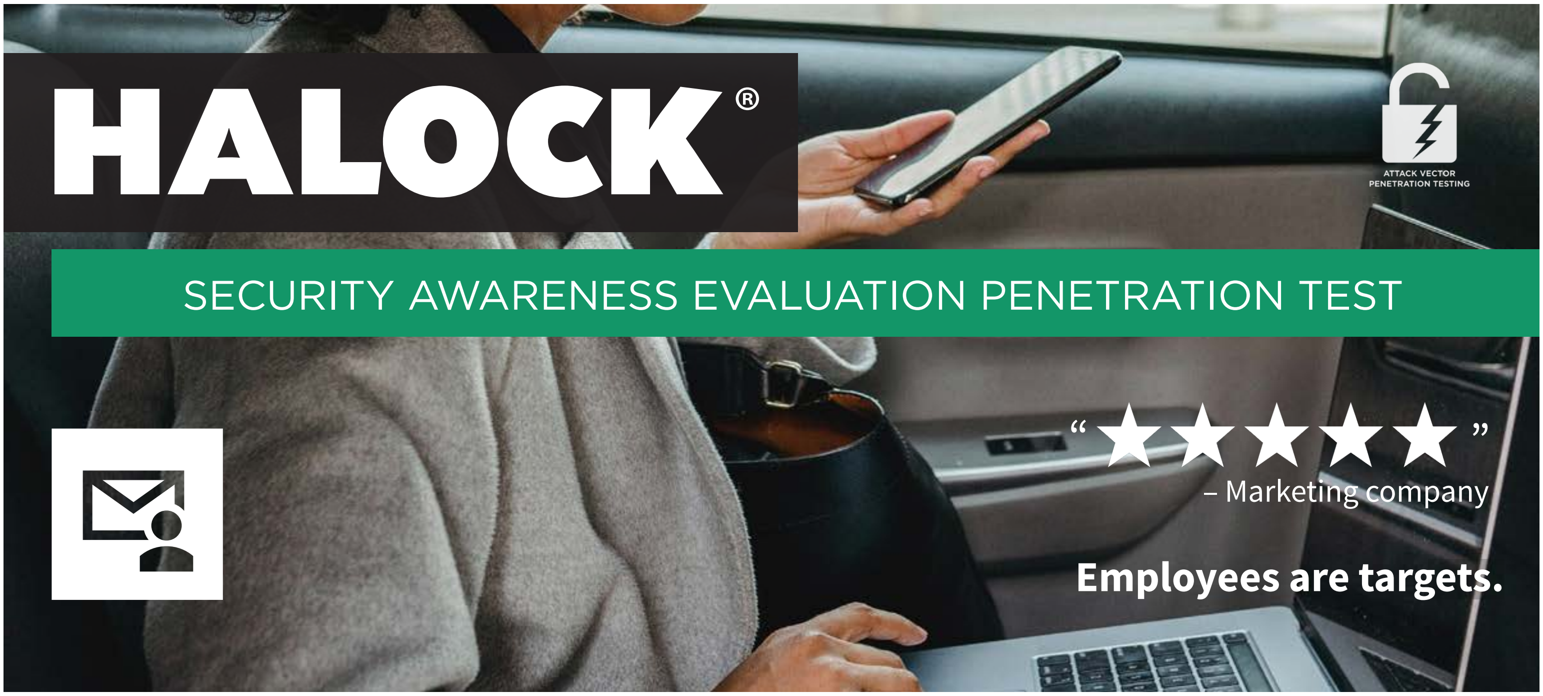

HALOCK®

SECURITY AWARENESS EVALUATION PENETRATION TEST

“★★★★★”

– Marketing company

Employees are targets.

How educated are members of the organization?
How effective are the spam and malware filters?
And what is the likelihood of the team being compromised?

HALOCK’s Security Awareness Evaluation Penetration Test utilizes Spear Phishing attempts to exploit vulnerabilities by targeting employees. Testing is conducted under controlled conditions. The testing presents a phishing email containing red flags that users who have completed security awareness training could identify. The messages are designed to bait users into clicking simulated malicious links to determine if security awareness training was effective. With increases in remote working environments, email as an attack vector is the most common.

The assessment puts the organization’s security awareness training to the test. Mistakes such as clicking on malicious links or providing sensitive information are identified and recorded. The report details how many users did and did not fall for the scam, which methods were most successful, and insights into where security awareness training can be improved to better educate employees to reduce the risk of a successful spear phishing attack.

The results help the organization make informed decisions on how training can be improved and what adjustments are needed to ensure better awareness and more effective controls.

Reconnaissance | Spear Phishing | Exploitation | Reporting | Remediation Recommendations

SECURITY AWARENESS EVALUATION 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.

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 risk management and 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 and Forensics, Security Organization Development, and Security Engineering.