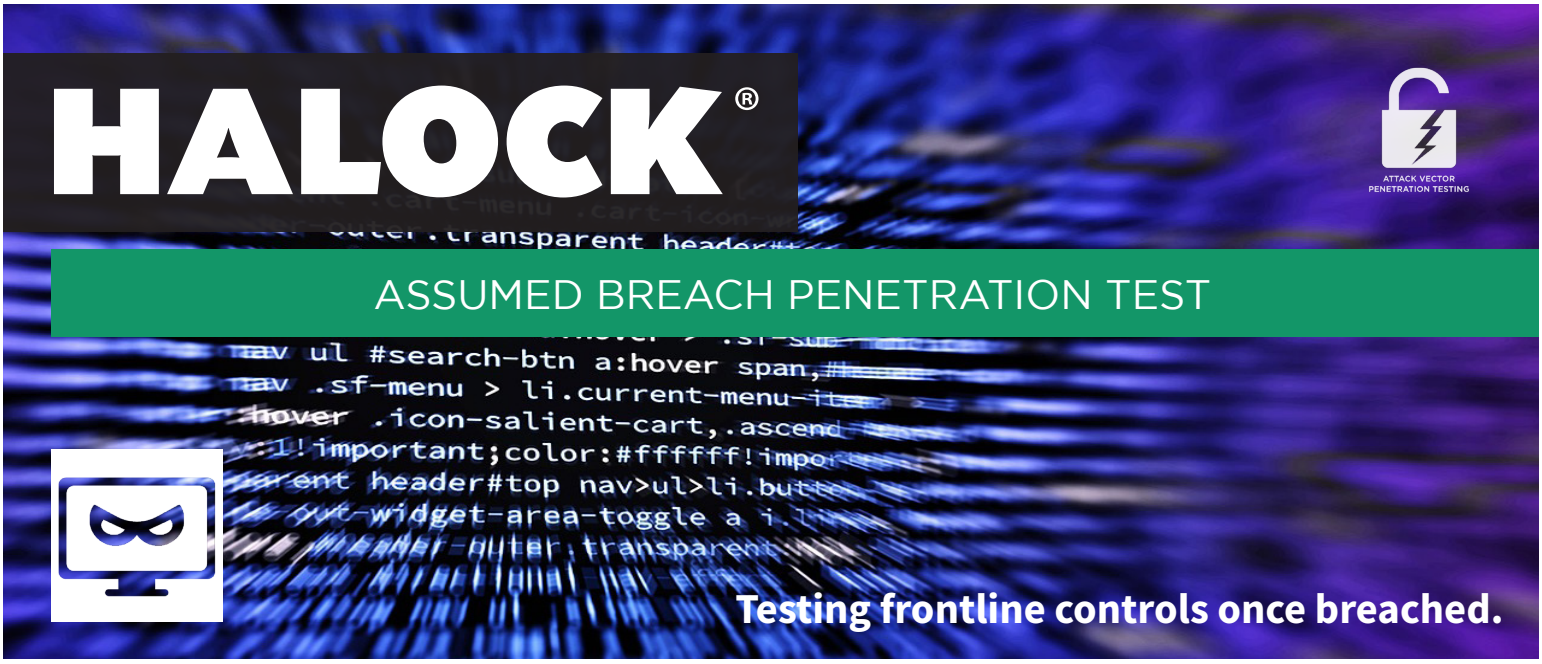
HALOCK®

ATTACK VECTOR PENETRATION TESTING

ASSUMED BREACH PENETRATION TEST



In the event the organization was breached, what is the impact? How far can the attacker go before being halted or contained by investments made into existing safeguards? How much sensitive data can be accessed via a single end user's credentials? Can the technology that has been deployed to contain a breach be relied upon?

HALOCK's Assumed Breach Penetration Test is an offering that addresses what happens following a successful spear phishing attack. Under these test conditions, spear phishing is not conducted. The engagement begins under breach conditions. Security awareness lost the battle, but still has a chance to win the war.

Expert Penetration Testers begin with the compromised endpoint system and take a deeper dive into what kinds of data can be accessed through the entry point (laptop/desktop), how far the attacker can go before any safeguard measures (people or technology) stop them, and if technical defense mechanisms can be relied upon to minimize the impact of a successful spear phishing attack. Attempts to bypass existing controls, escalate privileges, move laterally throughout the environment, exfiltrate data, establish persistent access, and expand the compromise to connected systems are designed to access valuable or sensitive data.

The Assumed Breach methodology service is a rapid and cost-effective method to validate the effectiveness of existing controls such as endpoint security, malware controls, egress restrictions, network segmentation, data leak prevention, and related to determine whether the organization's most sensitive data can be accessed through a compromised end user account or system.

If the organization is already implementing security awareness training, but you want to test your frontline controls should a breach occur, the Assumed Breach offering will answer these questions and provide recommendations into which controls can be improved to reduce the impact of a successful attack.

Assumed Breach | Intensified Short-Term Exploitation | Reporting | Remediation Recommendations

HALOCK | halock.com | 847-221-0200 | Incident Response Hotline: 800-925-0559

HALOCK®

ASSUMED BREACH 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.

HALOCK | halock.com | 847-221-0200 | Incident Response Hotline: 800-925-0559