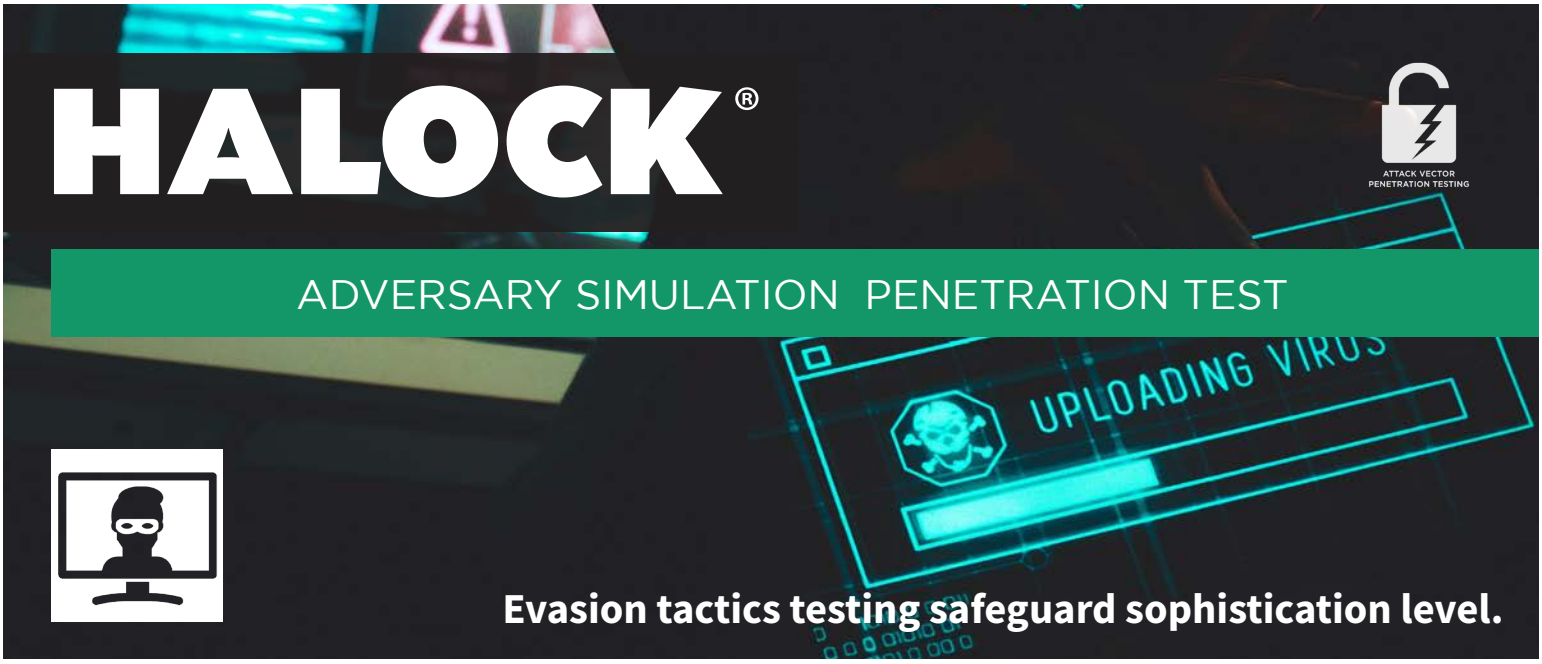
HALOCK®

ATTACK VECTOR PENETRATION TESTING

ADVERSARY SIMULATION PENETRATION TEST



Evasion tactics testing safeguard sophistication level.

Are the organization's investments into incident response technologies, processes, and third-party monitoring providers producing the expected results? Are they able to identify more sophisticated, longer-term attacks in a timely manner and ensure rapid response and containment?

HALOCK's Adversary Simulation Penetration Test is a comprehensive, highly targeted, and covert test. Experienced Penetration Testers attempt to infiltrate the environment while evading detection by in-house or third-party monitoring technologies and processes. These technological investments and third-party vendors usually represent a significant financial expenditure and are expected to quickly identify an attacker as well as prevent further damage in the event they have bypassed the security perimeter. This simulation tests whether business goals are being met using existing methodologies and third-party vendors contracted as a safeguard.

Starting with spear phishing messages, HALOCK will try to gain access without advance knowledge or special allowances. Once access is established, testers attempt to bypass the controls, expand, and escalate access gradually, and utilize evasion techniques to NOT set off the alarms. Highly sophisticated techniques are utilized to determine if safeguards are effective in recognizing the not-so-obvious methods for infiltrating a network.

Adversary Simulation differentiates itself from other services and service providers in its pacing and purpose, representing the most tailored and targeted methods a determined attacker would utilize. The core of the approach is stealth, testing for loopholes and workarounds. The goal is not to comprehensively identify potential vulnerabilities but rather to gain access, maintain persistence, and expand the compromise as broadly as possible, without detection.

Exploitation | Long-term, Persistent Testing of Controls | Reporting | Remediation Recommendations

HALOCK®

ADVERSARY SIMULATION 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