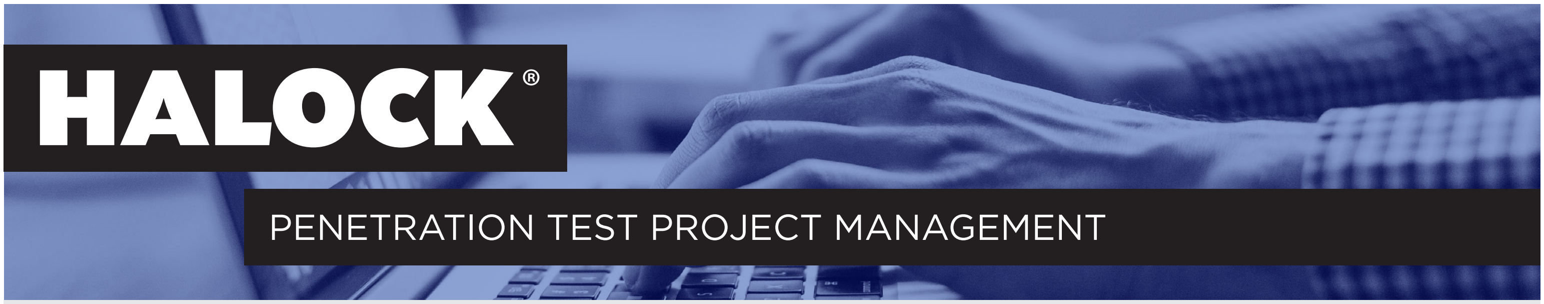
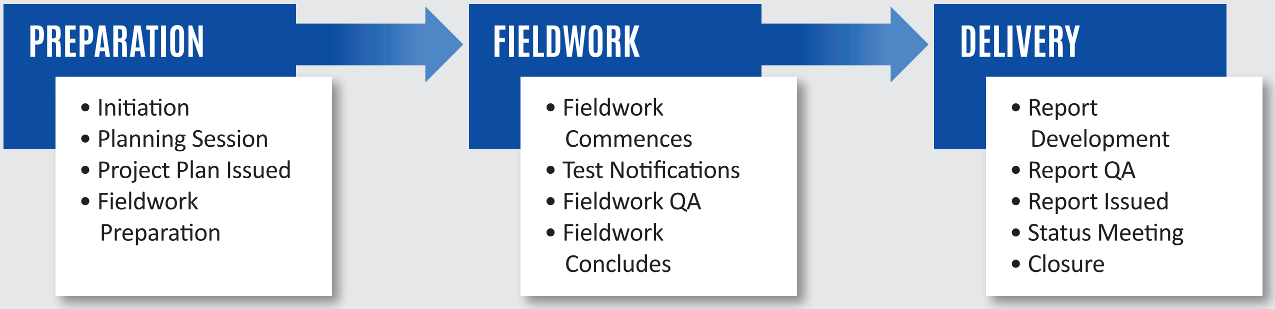


HALOCK®

PENETRATION TEST PROJECT MANAGEMENT

Penetration tests performed as a "point in time" engagements incorporate preparation, fieldwork, and delivery activities:



PREPARATION
- Initiation
- Planning Session
- Project Plan Issued
- Fieldwork Preparation

FIELDWORK
- Fieldwork Commences
- Test Notifications
- Fieldwork QA
- Fieldwork Concludes

DELIVERY
- Report Development
- Report QA
- Report Issued
- Status Meeting
- Closure

Penetration tests involving multiple phases or recurring testing utilize the same phases, however apply the approach in a recursive manner.

PREPARATION

Preparing for a penetration test requires careful planning and collaboration between all parties involved. This begins with Initiation and involves several activities:

- Initiation: Upon initiation, HALOCK contacts the sponsor, typically within one business day, to acknowledge receipt, coordinate the planning session date and time, and issue invitations to the necessary stakeholders.
- Planning Session: The planning session is conducted as scheduled. Led by the assigned HALOCK project manager, the scope of services is reviewed, technical requirements are discussed, scheduling, and other planning considerations are discussed. Time is reserved during the planning session for other questions or considerations stakeholders may have.
- Project Plan Issued: Following the conclusion of the initial planning session, HALOCK develops a project plan containing the specifics discussed during the planning session. The project plan is issued, accompanied with a summary of open items, and updated throughout preparation as activities are completed.
- Fieldwork Preparation: Additional preparation tasks may also be executed, where required by the scope of review. For example, if certain connectivity requirements were identified during planning, these are validated in advance of fieldwork. Lab equipment or similar dependencies may also be prepared.

FIELDWORK

Fieldwork involves executing the testing, as scheduled in the project plan, and includes several activities:

- Fieldwork Commences: The first test shift begins as scheduled, observing the testing methodology as provided.
- Testing Notifications: A test start notification is issued at the start of each testing shift. A test stop notification is issued at the completion of each shift. These notifications continue for each subsequent test shift as scheduled.
- Fieldwork QA: Throughout testing, regular internal reviews are performed to verify the test scope and schedule are on track for completion as planned.
- Fieldwork Concludes: All testing concludes as scheduled and delivery efforts begin.

DELIVERY

Following the conclusion of fieldwork, HALOCK compiles the complete results of the penetration test in the penetration test report. The following activities are performed:

- Report Development: Findings, recommendations, and supporting evidence are documented and compiled. The report is assembled and submitted to QA.
- Report Quality Assurance: The report is subjected to HALOCK's internal QA process.
- Report Issued: The report is issued for review and review sessions or status meetings are scheduled, as applicable.
- Status Meeting: HALOCK and project stakeholders discuss key findings, answer questions, discuss remediation approaches, and review next steps.
- Closure: The penetration test is complete. Remediation, planning for subsequent phases of testing, or other post assessment activities begin as defined in the scope of review.

PENETRATION TEST METHODOLOGY

Web Application Penetration Test

OVERVIEW

For critical web applications, an in-depth review is appropriate. As web applications vary greatly depending on the purpose, function, architecture, and code base, the specific approaches, testing perspectives, and utilized test profiles can vary.

Multiple factors influence whether an attacker can gain access to the web application. There may be numerous methods to approach gaining access and exploit identified issues, but an attacker only needs to be successful in linking one path through the application.

There are nearly 100 common application weaknesses. HALOCK's approach to Web Application Penetration Testing provides a flexible framework for comprehensively identifying and evaluating technical vulnerabilities. The following areas are considered and typically incorporated into the review, as they apply to the target web application:

INFORMATION GATHERING

Initial information gathering is required to understand the application platform, technology, structure, and behavior. The following methods may be utilized, as applicable:

- Conduct search engine discovery and reconnaissance for information leakage
- Fingerprint web server
- Review webserver metafiles for information leakage
- Enumerate applications on webserver
- Review webpage comments and metadata for information leakage
- Identify application entry points
- Map execution paths through application
- Fingerprint web application framework
- Fingerprint web application
- Map network and application architecture

CONFIGURATION AND DEPLOY MANAGEMENT TESTING

Once the application has been mapped, additional configuration management checks assess the security of the host and application:

- Network/infrastructure configuration
- Application platform configuration
- File extensions handling for sensitive information
- Testing for the presence of old, backup and unreferenced files for sensitive information
- Infrastructure and application administrative interfaces
- HTTP methods
- HTTP strict transport security (HSTS)
- RIA cross domain policy

IDENTITY MANAGEMENT TESTING

Verification, where appropriate, for account provisioning considerations, such as testing:

- Role definitions
- User registration process
- Account provisioning process (when self-registration is available)
- Account enumeration and guessable user accounts
- Weak or unenforced username policy

AUTHENTICATION TESTING

Testing for authentication related weaknesses, such as:

- Credentials transported over an encrypted channel
- Default credentials

Web Application Penetration Test

- Weak lock out mechanisms
- Bypassing authentication schema
- Remember password functionality
- Browser cache weakness
- Weak password policy
- Weak security question/answer
- Weak password change or reset functionalities
- Weak authentication in alternative channels, where available

AUTHORIZATION TESTING

Testing to validate the security of authorization controls such as:

- Directory traversal/file include
- Bypassing authorization schema
- Privilege escalation
- Insecure direct object references

SESSION MANAGEMENT TESTING

An evaluation of session-related vulnerabilities involves testing:

- Bypassing session management schema
- Cookies attributes
- Session fixation
- Exposed session variables
- Cross-site request forgery (CSRF)
- Logout functionality
- Session timeout
- Session puzzling

DATA VALIDATION TESTING

Testing for data validation involves manipulation of input fields, query strings, hidden parameters, and related input methods.

- Reflected cross-site scripting (XSS)
- Stored cross-site scripting (XSS)
- HTTP verb tampering
- HTTP parameter pollution
- SQL injection
- LDAP injection
- ORM injection
- XML injection
- SSI injection
- XPath injection
- IMAP/SMTP injection
- Code injection (local and/or remote)
- Command injection
- Buffer overflow
- Heap overflow
- Stack overflow
- Format string
- Incubated vulnerabilities
- HTTP splitting/smuggling

Web Application Penetration Test

TESTING FOR ERROR HANDLING

Testing error handling issues, as they relate to security, such as analysis of Error Codes and Stack Traces.

TESTING FOR WEAK CRYPTOGRAPHY

Testing to evaluate the effectiveness of encryption related protections, such as:
- Weak SSL/TLS ciphers
- Insufficient transport layer protection
- Sensitive information sent via unencrypted channels

BUSINESS LOGIC TESTING

Testing to determine if the flow or architecture of the application can be manipulated to gain access to sensitive information through flaws in business logic, such as:
- Business logic data validation
- Ability to forge requests
- Integrity checks
- Process timing
- Number of times a function can be used
- Circumvention of workflows
- Defenses against application misuse
- Upload of unexpected file types
- Upload of malicious files

CLIENT-SIDE TESTING

Assessing vulnerabilities that commonalty affect the client side of the application session, such as:
- DOM based cross-site scripting (XSS)
- JavaScript execution
- HTML injection
- Client-side URL redirect
- CSS injection
- Client-side resource manipulation
- Cross-origin resource sharing (CORS)
- Cross-site flashing
- Clickjacking
- Web Socket insecurities
- Web messaging
- Local storage

PENETRATION TEST METHODOLOGY

External Network Penetration Test

OVERVIEW

External penetration tests are different from automated vulnerability scans in that penetration tests are comprehensive, attempt to exploit identified vulnerabilities, and follow manual practices used by hackers to take advantage of weak security systems or processes. External network penetration testing, as detailed in the scope section earlier in this proposal, is performed remotely to simulate an external attack.

HALOCK will attempt to exploit vulnerabilities identified on networks, systems, and responding services to gain access to sensitive information assets using any appropriate means at their disposal. Testing is performed under controlled conditions to minimize the risk for system or network disruption. The test provides comprehensive detail regarding security weaknesses that are present in the environment. HALOCK's approach to Penetration Testing locates target hosts and services, evaluates the security of those targets utilizing penetration test tools and methods, attempts to gain access to the target hosts, and finally escalates privileges throughout the environment.

Multiple factors influence whether an attacker can gain access to the environment from an external perspective. There may be numerous methods to approach gaining access and exploit identified issues, but an attacker only needs to be successful in linking one path into the environment.

Penetration testing is an iterative process. Each stage in the process may yield additional information that warrants revisiting earlier phases, equipped with new information. For example, passwords cracked resulting in the exploit of a domain controller later in the process may be fed back into earlier reconnaissance stages to determine if additional hosts can be accessed as a result.
HALOCK's approach to External Network Penetration Testing provide a flexible framework for comprehensively identifying and evaluating technical vulnerabilities. The following phases are typically incorporated into the penetration test, as they apply to the target environment:

RECONNAISSANCE

An attacker first must discover the target environment, beginning on the perimeter. To gain knowledge about the target environment and develop a list of potential targets, the attacker performs a series of initial reconnaissance activities. There are over 130,000 possible services on a single IP address that could potentially be assigned. To focus effort where most productive and minimize the impact of discovery, reconnaissance is typically performed in stages. The stages of reconnaissance begin broad, at the network, narrow to specific hosts, and finally services exposed within those hosts.

- **Network Discovery:** Each target ISP range included in the scope of review contains both assigned and unassigned IP addresses. To determine which of these IP addresses represent potential targets, network discovery is performed. Network Discovery consists of performing limited port scanning, network mapping, ICMP requests, DNS queries, and similar probes. At this stage, comprehensive discovery is not necessary as a single response is sufficient to consider an IP address a potential target.
- **Host Discovery:** The subset of IP addresses that responded to discovery are then subjected to more comprehensive discovery to identify the services exposed on a given IP address. This involves subjecting live IP addresses to additional port scanning. This port scanning sends up to 1,000 requests to commonly utilized TCP and UDP ports. The number of ports probed varies based on network stability, response times, and other factors.
- **Service Discovery:** While TCP and UDP ports are typically associated to standard service, such as TCP80 for HTTP or UDP53 for DNS, they may also be assigned to nonstandard port numbers. Service Discovery is leveraged to increase confidence in the host discovery results. TCP/IP stack fingerprinting, OS fingerprinting on redirected ports, NetBIOS queries, banner requests, and similar methods can provide an attacker with details such as the specific software build version of a web hosting platform, if an SMTP service accepts relay, or if an FTP service is anonymous versus restricted to authenticated users.

The results of these activities are parsed and compiled into the initial target list. This list serves as the basis for later activities and is updated as additional information is obtained in later stages of the penetration test.

TARGET PLANNING

Using the results of the reconnaissance stage, a list of primary targets is selected. These "targets of interest" represent those the attacker perceives as potential high return entry points into the environment.

The total number selected is defined by the scope of review and may include sampling. When sampling is utilized, targets are chosen based on perceived opportunity, with consideration of establishing a representative view of varying technologies, geographies, or other unique factors.

Hosts initially excluded may later be reconsidered as targets, such as when an exploit involves the interaction between multiple hosts within the environment.

VULNERABILITY ENUMERATION

There are over 100,000 known (published) vulnerabilities documented on public sources such as CVE, Vendor References, Bugtraq, and other repositories. Many of these can be excluded using the results of the reconnaissance stage, such as when a given vulnerability check applies to a technology not located in the environment. Further, an attacker is primarily focused on vulnerabilities with associated exploits that present an opportunity to either gain entry, or provide useful information that may help refine related exploits.

Vulnerability enumeration involves the use of automated scanners configured to search for specific published vulnerabilities with known associated exploits. Manual vulnerability tests are performed to identify vulnerabilities scanners are not well suited to identify, such as unpublished (zero day) vulnerabilities, network layer weaknesses, vulnerabilities on services unique to the environment (such as custom web applications), or when environments are observed to be unstable.

Tests are run using minimal bandwidth and limit the number of hosts and services tested in parallel to minimize risk for disruption. The enumeration and detection process runs in an iterative fashion for each target. All vulnerabilities detected are considered “potential”, and considered for the exploit phases.

VULNERABILITY VALIDATION

Any vulnerabilities identified are viewed as potential at this stage. Additional testing is required to (a) confirm the vulnerability is valid or (b) confirm it is a false positive. The methods utilized vary greatly based on the vulnerability being subjected to validation. Validation may involve the use of secondary purpose build scanning tools, manual tests to reproduce scanner results, or the development and execution of scripted methods when no known methods are available to validate.

Vulnerabilities confirmed to be applicable to the service being tested are also subjected to single stage exploits, where such tests can be performed under safe and controlled conditions. These tests are performed to attempt to establish an initial level of access, obtain configuration details, or yield other useful information to support exploit scenarios. The goal of this stage is to eliminate attack scenarios perceived as low value or otherwise nonproductive, identify hosts that may not be stable or suitable to targeting, and establish as many entry points as feasible.

ATTACK PLANNING

At this stage of the penetration test, the attacker has a much more detailed understanding of the components in the target environment, higher confidence in which services are likely to present opportunity to gain access, if payloads are available or require development, which exploits can and cannot be pursued under safe and controlled conditions, if expanded sampling is needed (such as when the initial targets yield little opportunity for exploit), and which exploits are likely to yield the greatest potential for gaining access.

EXPLOIT EXECUTION

The primary goal for the exploit stage is to establish command and control, ideally with persistence, of one or more hosts within the environment, pursued under controlled conditions. The attacker pursues and documents each step of an exploit to demonstrate the steps required to compromise the host or service being targeted. These exploits may include the use of publicly available tools and methods, or an approach developed by the attacker in real time. The latter is common when zero-day vulnerabilities are identified and exploited.

Each exploit targeting a host, service, network, application, or other asset is initially focused on compromising that specific asset, however may also yield opportunity to incorporate additional components in the environment. Defense evasion tactics are utilized to avoid or bypass controls as observed in the environment.

- **Host Exploits:** The specific tests performed vary greatly based on the services detected, but typically leverage server misconfigurations, missing patches, or other weaknesses.
- **Web Application Exploits:** In the event web applications are detected during discovery, additional application layer tests may be performed.

External Network Penetration Test

These tests are performed without authentication unless authenticated access is achieved as a direct result of an identified vulnerability. Tests are performed targeting most common or critical vulnerabilities as applicable, but may include other checks specific to the application function or technology. Comprehensive web application testing is not performed during a network penetration test, however any web application perceived as a potential entry point may be targeted to gain access.

- **Network Exploits:** Numerous protocols and network traffic traverse the public internet using clear text or otherwise insecure methods. HALOCK will perform tests to monitor, intercept, and record communications. The tests may vary based on the design of the infrastructure and types of network devices in place.

Exploits perceived to provide opportunity to pivot laterally within a network, across networks, escalate privileges, or yield more information are advanced to the next stage of the penetration test.

PRIVILEGE ESCALATION AND LATERAL MOVEMENT

When access to a given host or service is achieved, additional post exploit actions may allow an attacker to gain additional access, potentially allowing the attacker to penetrate the internal environment. These attacks involve both privilege escalation on the target host as well as attempts to escalate privileges laterally throughout the environment. This often involves leveraging information obtained at other stages of the penetration tests.

- When attempts to access a host results in limited privileges, passwords obtained from other hosts compromised may be utilized to elevate to a more privileged role.
- Configuration weaknesses on a compromised host may allow the attacker to identify additional derivative vulnerabilities, each of which may provide additional opportunity to bypass security controls and elevate access.
- Compromised services running under a more privileged context than the attacker possesses may be leveraged as an intermediary to perform actions on the behalf of the attacker.
- Integration considerations, such as centralized authentication or shared services, may allow an attacker to obtain sensitive information that could be used to access otherwise secured hosts. For example, compromising an edge network device that is also used as a VPN endpoint may provide an attacker an opportunity to subsequently compromise peer devices bridging remote networks.

When a compromised host is determined to share a common internal (private) network, other hosts either not exploited or otherwise not previously visible become potential targets. Attempts to utilize the compromised host as an intermediary may allow an attacker to move laterally throughout the environment. These exploit scenarios are explored as opportunity presents and may result in the identification of additional targets, derivative vulnerabilities, and exploits. Testing at this stage is highly iterative and often involves some or all the stages listed above.

Additional evidence, information, and examples are gathered to facilitate development of findings (which discuss impact) or exploit walkthroughs (which depict impact).

DATA EXFILTRATION

Among the many threats security controls are designed to protect against, unauthorized access to protected information is key. A common target for attackers is this protected information. When access to a given host or service is achieved, searches are conducted to attempt to locate sensitive information. Examples are cited where observed to demonstrate impact.

While an actual attacker would likely attempt to exfiltrate large volumes of bulk data for offline review, this is not necessary during a controlled penetration test. To validate if exfiltration is possible, the most common approach is to transfer a non-sensitive test file out of the organization (egress) to demonstrate the methods in which the observed live data could have been exfiltrated.

PENETRATION TEST METHODOLOGY

Internal Network Penetration Test

OVERVIEW

Internal penetration tests are different from automated vulnerability scans in that penetration tests are more manual, attempt to exploit identified vulnerabilities, and follow practices used by hackers to take advantage of weak security systems or processes. Internal network penetration testing, as detailed in the scope section earlier in this proposal, is performed remotely to simulate an attack performed from within the private network. This simulates conditions such as when an attacker is a malicious individual internal to the organization, when an external attacker has achieved internal access by compromising an internal endpoint, or has achieved entry point through an external host.

HALOCK will attempt to exploit vulnerabilities identified on networks, systems, and responding services to gain access to sensitive information assets using any appropriate means at their disposal. Testing is performed under controlled conditions to minimize the risk for system or network disruption. The test provides comprehensive detail regarding security weaknesses that are present in the environment. HALOCK's approach to Penetration Testing locates target hosts and services, evaluates the security of those targets utilizing penetration test tools and methods, attempts to gain access to the target hosts, and finally escalates privileges throughout the environment.

Multiple factors influence whether an attacker can elevate access to the environment while positioned from an internal perspective. There may be numerous methods to approach gaining access and exploit identified issues, but an attacker only needs to be successful in linking one path into the environment.

Penetration testing is an iterative process. Each stage in the process may yield additional information that warrants revisiting earlier phases, equipped with new information. For example, passwords cracked resulting in the exploit of a domain controller later in the process may be fed back into earlier reconnaissance stages to determine if additional hosts can be accessed as a result.

HALOCK's approach to Internal Network Penetration Testing provide a flexible framework for comprehensively identifying and evaluating technical vulnerabilities across an enterprise network. The following phases are typically incorporated into the penetration test, as they apply to the target environment:

RECONNAISSANCE

An attacker first must discover the target environment. To gain knowledge about the target environment and develop a list of potential targets, the attacker performs a series of initial reconnaissance activities. When the scope of review defines multiple points of origin within an internal network, discovery is repeated from these perspectives to better understand not only what an attacker may target, but from where they may do so. There are over 130,000 possible services on a single IP address that could potentially be assigned. To focus effort where most productive and minimize the impact of discovery, reconnaissance is typically performed in stages. The stages of reconnaissance begin broad, at the network, narrow to specific hosts, and finally services exposed within those hosts.

- **Network Discovery:** Each target ISP range included in the scope of review contains both assigned and unassigned IP addresses. To determine which of these IP addresses represent potential targets, network discovery is performed. Network Discovery consists of performing limited port scanning, network mapping, ICMP requests, DNS queries, and similar probes. At this stage, comprehensive discovery is not necessary as a single response is sufficient to consider an IP address a potential target.
- **Host Discovery:** The subset of IP addresses that responded to discovery are then subjected to more comprehensive discovery to identify the services exposed on a given IP address. This involves subjecting live IP addresses to additional port scanning. This port scanning sends up to 1,000 requests to commonly utilized TCP and UDP ports. The number of ports probed varies based on network stability, response times, and other factors.
- **Service Discovery:** While TCP and UDP ports are typically associated to standard service, such as TCP80 for HTTP or UDP53 for DNS, they may also be assigned to nonstandard port numbers. Service Discovery is leveraged to increase confidence in the host discovery results. TCP/IP stack fingerprinting, OS fingerprinting on redirected ports, NetBIOS queries, banner requests, and similar methods can provide an attacker with details such as the specific software build version of a web hosting platform, if an SMTP service accepts relay, or if an FTP service is anonymous versus restricted to authenticated users.

The results of these activities are parsed and compiled into the initial target list. This list serves as the basis for later activities and is updated as additional information is obtained in later stages of the penetration test.

PENETRATION TEST METHODOLOGY

Internal Network Penetration Test

TARGET PLANNING

Using the results of the reconnaissance stage, a list of primary targets is selected. These “targets of interest” represent those the attacker perceives as potential high return entry points into the environment.

The total number selected is defined by the scope of review and may include sampling. When sampling is utilized, targets are chosen based on perceived opportunity, with consideration of establishing a representative view of varying technologies, geographies, or other unique factors.

Hosts initially excluded may later be reconsidered as targets, such as when an exploit involves the interaction between multiple hosts within the environment.

VULNERABILITY ENUMERATION

There are over 100,000 known (published) vulnerabilities documented on public sources such as CVE, Vendor References, Bugtraq, and other repositories. Many of these can be excluded using the results of the reconnaissance stage, such as when a given vulnerability check applies to a technology not located in the environment. Further, an attacker is primarily focused on vulnerabilities with associated exploits that present an opportunity to either gain entry, or provide useful information that may help refine related exploits.

Vulnerability enumeration involves the use of automated scanners configured to search for specific published vulnerabilities with known associated exploits. Manual vulnerability tests are performed to identify vulnerabilities scanners are not well suited to identify, such as unpublished (zero day) vulnerabilities, network layer weaknesses, vulnerabilities on services unique to the environment (such as custom web applications), or when environments are observed to be unstable.

Tests are run using minimal bandwidth and limit the number of hosts and services tested in parallel to minimize risk for disruption. The enumeration and detection process runs in an iterative fashion for each target. All vulnerabilities detected are considered “potential”, and considered for the exploit phases.

VULNERABILITY VALIDATION

Any vulnerabilities identified are viewed as potential at this stage. Additional testing is required to (a) confirm the vulnerability is valid or (b) confirm it is a false positive. The methods utilized vary greatly based on the vulnerability being subjected to validation. Validation may involve the use of secondary purpose build scanning tools, manual tests to reproduce scanner results, or the development and execution of scripted methods when no known methods are available to validate.

Vulnerabilities confirmed to be applicable to the service being tested are also subjected to single stage exploits, where such tests can be performed under safe and controlled conditions. These tests are performed to attempt to establish an initial level of access, obtain configuration details, or yield other useful information to support exploit scenarios. The goal of this stage is to eliminate attack scenarios perceived as low value or otherwise nonproductive, identify hosts that may not be stable or suitable to targeting, and establish as many entry points as feasible.

ATTACK PLANNING

At this stage of the penetration test, the attacker has a much more detailed understanding of the components in the target environment, higher confidence in which services are likely to present opportunity to gain access, if payloads are available or require development, which exploits can and cannot be pursued under safe and controlled conditions, if expanded sampling is needed (such as when the initial targets yield little opportunity for exploit), and which exploits are likely to yield the greatest potential for gaining access.

EXPLOIT EXECUTION

The primary goal for the exploit stage is to establish command and control, ideally with persistence, of one or more hosts within the environment, pursued under controlled conditions. The attacker pursues and documents each step of an exploit to demonstrate the steps required to compromise the host or service being targeted. These exploits may include the use of publicly available tools and methods, or an approach developed by the attacker in real time. The latter is common when zero-day vulnerabilities are identified and exploited.

PENETRATION TEST METHODOLOGY

Internal Network Penetration Test

Each exploit targeting a host, service, network, application, or other asset is initially focused on compromising that specific asset, however may also yield opportunity to incorporate additional components in the environment. Defense evasion tactics are utilized to avoid or bypass controls as observed in the environment.

- **Host Exploits:** The specific tests performed vary greatly based on the services detected, but typically leverage server misconfigurations, missing patches, or other weaknesses.
- **Web Application Exploits:** In the event web applications are detected during discovery, additional application layer tests may be performed. These tests are performed without authentication unless authenticated access is achieved as a direct result of an identified vulnerability. Tests are performed targeting most common or critical vulnerabilities as applicable, but may include other checks specific to the application function or technology. Comprehensive web application testing is not performed during a network penetration test, however any web application perceived as a potential entry point may be targeted to gain access.
- **Network Exploits:** Numerous protocols and network traffic traverse the public internet using clear text or otherwise insecure methods. HALOCK will perform tests to monitor, intercept, and record communications. The tests may vary based on the design of the infrastructure and types of network devices in place. If traffic interception and / or redirection can be performed without disruption, man-in-the-middle attacks may be performed or otherwise simulated to determine if the potential exists.

Exploits perceived to provide opportunity to pivot laterally within a network, across networks, escalate privileges, or yield more information are advanced to the next stage of the penetration test.

PRIVILEGE ESCALATION AND LATERAL MOVEMENT

When access to a given host or service is achieved, additional post exploit actions may allow an attacker to gain additional access. These attacks involve both privilege escalation on the target host as well as attempts to escalate privileges laterally throughout the environment. This often involves leveraging information obtained at other stages of the penetration tests.

- When attempts to access a host results in limited privileges, passwords obtained from other hosts compromised may be utilized to elevate to a more privileged role.
- Configuration weaknesses on a compromised host may allow the attacker to identify additional derivative vulnerabilities, each of which may provide additional opportunity to bypass security controls and elevate access.
- Compromised services running under a more privileged context than the attacker possesses may be leveraged as an intermediary to perform actions on the behalf of the attacker.
- Integration considerations, such as centralized authentication or shared services, may allow an attacker to obtain sensitive information that could be used to access otherwise secured hosts. For example, compromising an edge network device that is also used as a VPN endpoint may provide an attacker an opportunity to subsequently compromise peer devices bridging remote networks.

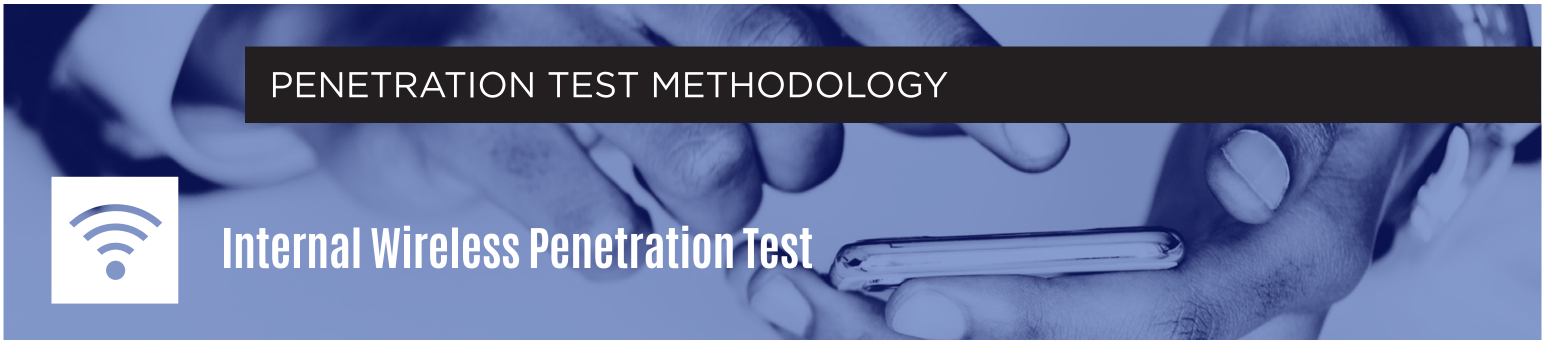
When a compromised host is determined to share a common internal (private) network, other hosts either not exploited or otherwise not previously visible become potential targets. Attempts to utilize the compromised host as an intermediary may allow an attacker to move laterally throughout the environment. These exploit scenarios are explored as opportunity presents and may result in the identification of additional targets, derivative vulnerabilities, and exploits. Testing at this stage is highly iterative and often involves some or all the stages listed above.

Additional evidence, information, and examples are gathered to facilitate development of findings (which discuss impact) or exploit walkthroughs (which depict impact).

DATA EXFILTRATION

Among the many threats security controls are designed to protect against, unauthorized access to protected information is key. A common target for attackers is this protected information. When access to a given host or service is achieved, searches are conducted to attempt to locate sensitive information. Examples are cited where observed to demonstrate impact.

While an actual attacker would likely attempt to exfiltrate large volumes of bulk data for offline review, this is not necessary during a controlled penetration test. To validate if exfiltration is possible, the most common approach is to transfer a non-sensitive test file out of the organization (egress) to demonstrate the methods in which the observed live data could have been exfiltrated.



PENETRATION TEST METHODOLOGY

Internal Wireless Penetration Test

OVERVIEW

Wireless penetration tests assess the adequacy of multiple security controls designed to protect unauthorized access to wireless services. Testing attempts to exploit wireless vulnerabilities to gain access to private (protected) wireless SSIDs or to escalate privileges on guest SSIDs intended to be isolated from private networks. HALOCK's testing methodology incorporates a collaborative approach that comprehensively identifies vulnerabilities commonly affecting wireless environments including authentication weaknesses, authorization bypass, encryption adequacy, and network segmentation.

The intended purpose of a wireless network also influences the tests performed. For example, a private wireless network utilized by employees with company managed systems assumes the employees are provisioned with authorized access. Testing focuses on attempts to bypass these controls, simulating an external attacker attempting to gain access to the protected network. Alternatively, guest wireless networks are commonly provided for individuals with systems not managed by the organization. These networks often permit self-registration by the user. Testing focuses on attempts to bypass segmentation between the guest and private networks or explore misuse scenarios.

WIRELESS RECONNAISSANCE

The first step is to map the extent and boundaries of the wireless infrastructure. Positioned within range of the in-scope wireless SSIDs, reconnaissance is performed to determine authentication methods supported, encryption requirements, MAC address restrictions, and the technologies in use. When other devices are visible on the wireless network, such as the devices bellowing to the users connected to the network, attempts to intercept useful traffic, MAC addresses, or authentication traffic is performed.

NETWORK RECONNAISSANCE

When access is allowed, such as in the case of guest networks permitting self-registration, network reconnaissance provides visibility into what networks can be access while connected. This may incorporate both internal and external network destinations. For example, internal network segmentation may be established to permit access to certain resources while preventing access to others. External content filters may define what egress internet traffic is permitted by the users of the wireless network.

MAC ADDRESS FILTERING BYPASS

When MAC address filtering is implemented to prevent unauthorized devices form joining a network, attempts to bypass evaluate the effectiveness of the method implemented. These tests vary based on the wireless technology in use, but typically involve MAC cloning attacks. These attacks are designed to impersonate another user who has been granted access, allowing the attacker to utilize their system identification to join an otherwise unauthorized device to the network.

ENCRYPTION EXPLOITS

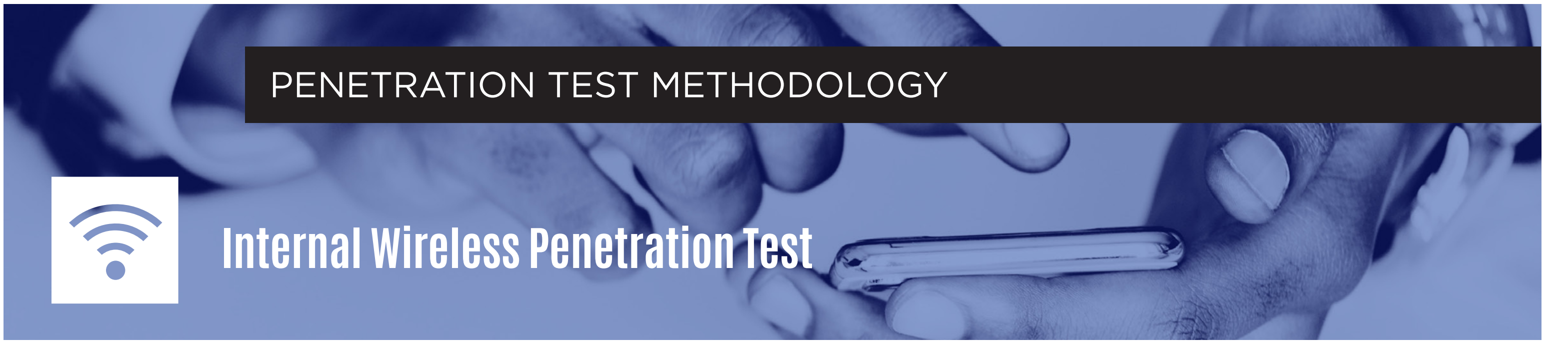
Insecure encryption methods, such as WEP, are often enabled on wireless networks. The reasons may vary from unintended misconfiguration, device default settings, or to support backwards compatibility requirements. These weak methods can be exploited by an attacker to gain access by leveraging the less secure method. Further, traffic transmitted over these protocols can be collected and subjected to decryption attacks.

AUTHENTICATION ATTACKS

The strength of other methods, such as WPA and WPA2, rely upon the complexity of the password used to access the network. When these are determined to be in use, the attacker will attempt to collect traffic packets destined for the target network and crack the password. For example, packets may be observed during an authentication attempt as part of the handshake. When no authentication attempts are observed, attempts to force re-authentication are attempted to terminate a connected client session. Traffic obtained may also be subjected to offline brute force attacks, when encryption strength is perceived as insufficient.

SESSION MANAGEMENT

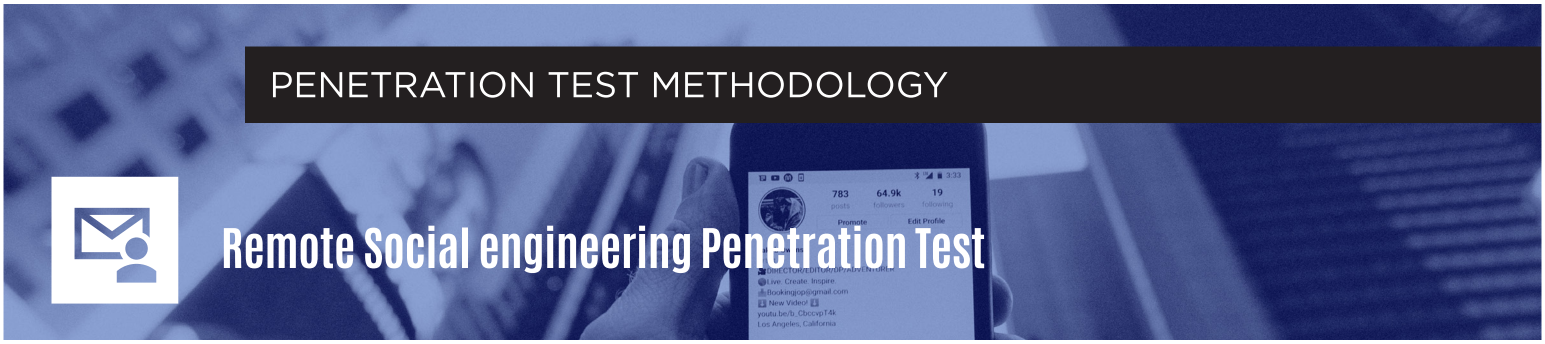
When wireless traffic from legitimate end users is observed, attempts to inject or hijack existing sessions may be possible. The specific methods vary based on the wireless technology in use, but typically involves attempts to bypass replay protection mechanisms, manipulate session state or session assignment methods, or leverage insecure wireless session management.



Internal Wireless Penetration Test

PRIVILEGE ESCALATION

When access is achieved, an attack shifts focus from wireless weakness to identifying potential targets on the protected network. When wireless testing is being performed in conjunction with an Internal Network Penetration Test, correlation between the two is often possible. When not performed in conjunction with an Internal Network Penetration Test, limited internal network discovery, target selection, and exploits may be performed to demonstrate how wireless weaknesses can be used to achieve the internal access necessary to pursue further attacks. Comprehensive testing is not pursued. These are performed to gather evidence network access was achieved, that this access presents opportunity to move into the protected network, and document a proof of concept scenario that an attacker would likely attempt. For example, port scans can be utilized to target hosts outside the intended access of the target network to demonstrate network visibility.



PENETRATION TEST METHODOLOGY

Remote Social engineering Penetration Test

OVERVIEW

Remote social engineering penetration tests are performed under controlled conditions to validate the effectiveness of user security awareness and incident response processes. 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 evaluate the effectiveness of preventative controls such as malware defenses, local permissions, and egress protections.

Remote social engineering penetration tests involve several stages, first by targeting employees with carefully crafted email messages, establishing a foothold on compromised systems, and escalating privileges to access information or lateral systems within the environment. These stages of testing provide visibility into the effectiveness of security awareness, incident response, malware defenses, perimeter security controls, data loss prevention, and related controls relied upon to protect the environment.

HALOCK has developed numerous fictitious websites, designed to mimic legitimate organizations, that are leveraged to gain initial access through spear phishing attacks via email. Each site has a specific purpose, such as collecting login credentials, establishing remote command and control, or harvesting information.

INFORMATION GATHERING

Prior to beginning testing, a list of authorized contacts is provided. This ensures only the intended individuals are directly targeted and that resources outside the scope of the engagement are not. The targets may contain employees of a common role with similar responsibilities or may contain a diverse group of roles spanning different working groups, organizational units, or geographies. Using this list, initial reconnaissance activities are performed to gather the necessary information to prepare suitable and credible messaging. The information gathered to prepare varies, but commonly includes attempts to locate information such as:

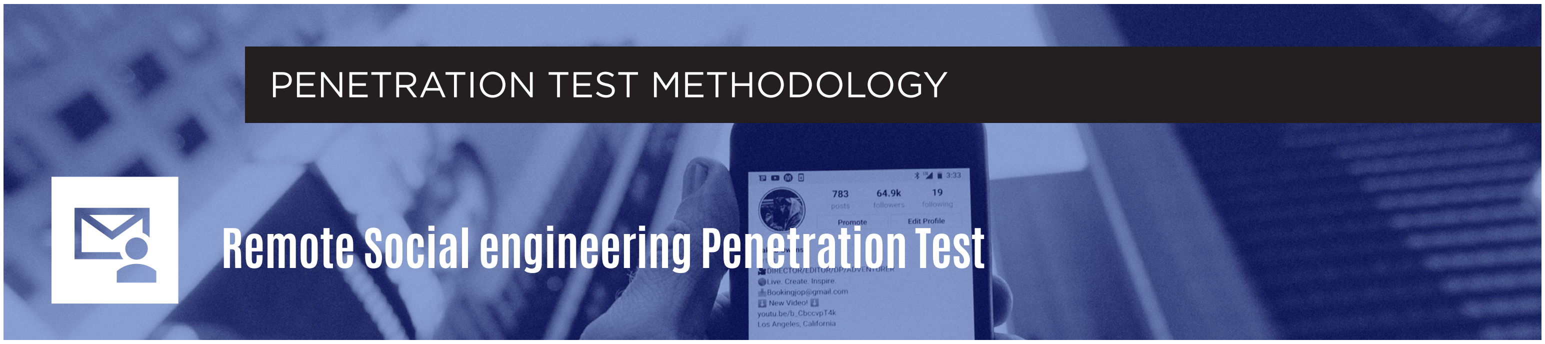
- Services the target organization offers
- Relationships between varying business units or divisions
- Registered domains and subdomains that may reveal lines of business the organization is engaged in
- Published documents, document metadata, and information that could potentially aide in refining attacks
- Employee or corporate specific information on social media sites such as photographs, or internal company information
- Configuration data, information exposed to search engines or public websites, or other externally exposed details that provide insights into the inner workings of the organization
- Technologies used by the organization that may influence the methods selected for content and payload delivery

INFRASTRUCTURE PREPARATION

Executing spear phishing campaigns are complex and require a variety of supporting components. At a minimum, systems to transport email, track responses and activity, and host content are needed. Additional systems are required to leverage the activity of users to establish access, escalate privileges, and pursue exploit scenarios. To support the campaigns, common components deployed include:

- Domains and name resolution, with suitable domain names, are registered and configured to support services needed to conduct spear phishing attacks.
- Email servers and relays require compliant configurations to ensure messages can be validated by receiving listeners performing reverse lookups, name resolution requests, or spam compliance checks.
- Content servers hosting the websites or receiving content a target is presented with when they visit a link provided in an email, track click through activity, or establish perceived legitimacy as a sending organization.
- Payload servers both host the simulated malware payload binaries for delivery as well as the necessary underlying services required to respond to execute actions.
- Command and control systems establish the necessary functionality to receive call backs, establish access, and provide a means for the attacker to interact with compromised endpoints.
- Supporting infrastructure components, such as servers, network devices, and related components necessary for the components above to function.

Prior to use, these services are tested in a controlled environment to identify and resolve issues prior to launching campaigns.



PENETRATION TEST METHODOLOGY

Remote Social engineering Penetration Test

CAMPAIGN PREPARATION

To maximize the likelihood of establishing access, the targets lists are grouped and sequenced to avoid concentrating phishing messages in any one area of the organization or to attack the attention of security personnel. The campaign batches are configured and scheduled to begin covertly, with reduced volume, but gradually increase the frequency and intensity of the attack over the course of testing. These batches include both primary targets, suspected based on perceived opportunity, as well as secondary targets that may be targeted in the event the primary target list is exhausted. Past engagements are also reviewed, when applicable, to minimize the potential for repeating previously utilized methods.

CAMPAIGN LAUNCH

Initial test messages are issued to identify delivery issues or other response behavior that might warrant revising the planned approach. Successive messages are issued, adjusting as appropriate, while continuing to monitor response activity.

INITIAL EXPLOITS

HALOCK's spear phishing capabilities are diverse and comprehensive, including:

- Credential Phishing Payloads
- HTA Payloads
- OLE / DDE Office Document payloads
- Macro-Enabled Office Document payloads
- Scripted payloads
- Unsigned browser plugins
- Fictitious software update alerts
- Custom developed executables and DLLs

The level of access achieved resulting from the victim's action can vary greatly based on network or system security controls encountered, technologies in use by the organization, employee behavior, and related considerations. Further, to ensure conducting social engineering can be performed under safe and controlled conditions, the simulated malware or payloads issued do not persist. A simple reboot is typically sufficient to kill the access. These factors often result in temporary or unreliable connection states.

While performing a comprehensive internal network penetration test of the full environment is beyond the intent or scope of review of remote social engineering penetration testing, targeted tests are pursued where appropriate to determine impact and provide examples of how an attacker could leverage the access achieved. The focus is to identify as many opportunities to improve security controls as possible, given the conditions available. Many activities performed at the exploit stage provide insights into not only security awareness, but the effectiveness of technical controls that are designed to limit or halt a spear phishing attack.

A prioritized approach is utilized to gather evidence and pursue further exploits. The attacker adapts based on the conditions, but typically prioritizes as follows:

- Gather basic supporting evidence, where necessary, to correlate the compromised system to a targeted user. This commonly involves running basic commands native to the operating system, under the context of the compromised user, to establish key details such as hostname, IP address, running services, or other activities necessary to identify the system.
- Enumerate the local environment for details such as service state, patch levels, recent command usage, installed software, or other system specific details.
- Pursue interactive methods to gather additional local information to aid reconnaissance, to increase chances of success with subsequent targets. This may include the use of key loggers, searching for password files, or locating other local resources that may be of value to the attacker.
- Identify potential secondary lateral targets on the network, determining the purpose of those hosts, and attempting to identify lateral services that may be of value to the attacker.
- If the target is determined to be viable, connections are stabilized with one to one persistent access between the compromised host and the attacker's command and control system.

SECONDARY EXPLOITS

When stable and persistent access is achieved, the focus of the attack shifts to maximizing the use of the compromised system and determine if there is opportunity to increase a presence throughout the connected environment. These secondary exploits typically focus first on privilege escalation on the direct host the attacker has access to. Common activities include:

- Bypassing user access controls, such as UAC
- Identifying misconfigurations, vulnerable software, or other security weaknesses present on the system that can be leveraged to escalate privileges
- Leveraging excessive user rights to obtain local power user or administrative rights
- Leverage the rights of the compromised user to access systems the user/system is granted rights to. For example, if the compromised user is a member of IT, they may already possess elevated rights the attacker can leverage to access other systems using standard user methods.
- Capture and exfiltrate the contents of information in memory contents, such as cached credentials.
- Additional methods to target nearby systems, utilizing the compromised host as a proxy.

EXFILTRATION

As the system being accessed is unlocked by the victim user, whole disk encryption has already been bypassed. Compromised systems often present a wealth of information to an attacker. When the duration of access permits, HALOCK attempts to identify local data repositories that would be of value to an attacker. These often include locally stored files, local databases, mapped drives, and file sync folders. Examples of these locations are logged, with descriptions, however attempts to bulk transfer this data is not performed.

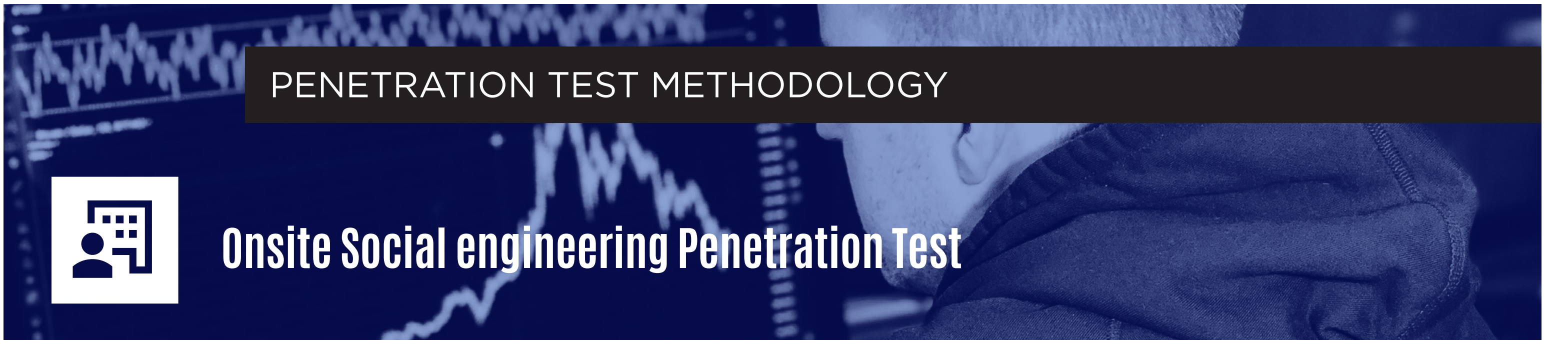
DISENGAGING

Disengaging from a target or targets occurs most commonly when:

- Access is lost or the connection otherwise becomes unusable
- Sufficient visibility has been explored and additional targets await evaluation
- The scheduled test window closes

As HALOCK disengages from each host and, ultimately, from all hosts, information is organized sequentially to facilitate the development of exploit walkthroughs, findings and recommendations, and related supporting information required to produce the penetration test report.

Services provisioned during preparation are decommissioned, listeners are closed to prevent continued contact, and any remaining sessions are exited.



PENETRATION TEST METHODOLOGY

Onsite Social engineering Penetration Test

OVERVIEW

Performed under controlled conditions, onsite social engineering penetration tests are performed to assess the effectiveness of physical and perimeter security controls, employee security awareness and response to suspicious behavior, and derivative tests to validate that network security controls prevent an attacker within the physical perimeter from gaining access to the network, establishing return back door access, or performing other activities that leverage observed security weaknesses.

Onsite social engineering penetration tests involve several stages, beginning with performing reconnaissance and information gathering about organization and target facilities, developing a plan to gain initial access through persuasion or other tactics, accessing restricted areas within the facility, establishing persistence to the environment, escalating access and privileges, and pursuing derivative exploits to demonstrate impact. This methodology provides visibility into the effectiveness of security awareness, incident response, malware defenses, perimeter security controls, data loss prevention, and related controls relied upon to protect the environment.

INFORMATION GATHERING

Prior to beginning testing, the locations of the target facilities are provided. If restrictions or limitations on activities apply, these are documented to ensure only the intended locations approved for testing are targeted and that unapproved methods are not incorporated into scenario planning.

Initial reconnaissance activities are performed prior to testing to gather the necessary information to prepare one or more strategies for the test. The information gathered to prepare varies, but commonly includes attempts to locate information such as:

- Services the target organization offers
- The business units or divisions located within the target site
- Visitor and/or guest access procedures
- Visitor identification methods
- Layouts or plans for the facility, where publicly available
- Technologies in use at the target location
- Visible perimeter monitoring controls such as cameras or security personnel
- Perimeter access controls such as keycard locks or pin pads
- Employee traffic patterns in and out of the facility
- Other public information located, such as employee lists, that may be useful to an attacker

ATTACK PLANNING AND PREPARATION

Prior to testing, HALOCK will develop one or more strategies for gaining access, based on perceived opportunity, determined to have the highest likelihood of success. Secondary exploits may also be planned for prior to testing when information gathering results in known potential weaknesses specific to the environment. When know weaknesses are not identified prior to testing, commonly successful methods are prepared and incorporated into the attack plan.

Once onsite, an attacker has at their disposal only what they bring or otherwise already exists onsite. Further, while the approach for gaining initial access may be very structured, activities performed thereafter and may vary greatly as opportunity presents. To ensure the attacker is equipped to pursue observed vulnerabilities, a toolkit is needed. Common assets that may be required for onsite testing include:

- Fabricated visitor access badges or identification
- RFID keycard scanners
- RFID keycard cloning equipment
- Covert devices for establishing persistence through remote command and control utilities
- Wireless traffic capturing devices
- Portable systems preloaded and configured with common penetration test tools and software
- Covert mobile testing platforms embedded in devices commonly found in corporate environments
- Human interface device utilities for performing man-in-the-middle attacks or capturing keyboard input for offline analysis
- Software defined radio devices for capturing radio traffic utilized in access control devices

Onsite Social engineering Penetration Test

- Live boot distribution media for accessing on premise endpoints and storage devices
- Rogue wireless access points for performing wireless man-in-the-middle attacks, establishing wireless access, and performing similar attacks
- Additional assets may be included, such as when observations specific to the target environment warrant customized techniques unique to the facility.

Note: due to pending legislative clarification at municipal, state, and federal levels, HALOCK does not currently utilize drone technologies for onsite social engineering.

ENTRY EXPLOITS

The specific methods used to gain access vary greatly based on perceived opportunity.

Initial attempts are unassisted, assuming a scenario where the attacker has no legitimate purpose to access the facility.

HALOCK will visit each target location and attempt to gain physical access using a variety of approaches including establishing fictitious identification, falsified meeting invitations, tailgating or shoulder surfing, or other tactics appropriate to the site and observed behavior of employees.

If gaining access is successful through these methods, HALOCK will proceed to secondary exploits as described below. Following the conclusion of secondary exploits, HALOCK will exit and attempt to regain access using additional methods to explore other security controls. For example, if HALOCK gains additional access by tailgating an employee into the facility, HALOCK will later attempt to gain access through secondary methods such as RIFD badge cloning or other methods suitable to the environment. This allows multiple perimeter controls to be evaluated, rather than limiting testing exclusively to the first control deficiency. These secondary techniques are also utilized when initial attempts to gain access are unsuccessful.

In the event entry exploits are unsuccessful after several attempts, scenario testing shifts to the perspective of an authorized visitor. In these situations, HALOCK is provided limited access representative of what would be provided to a visitor to facilitate the testing of interior controls.

ESTABLISH PERSISTENCE

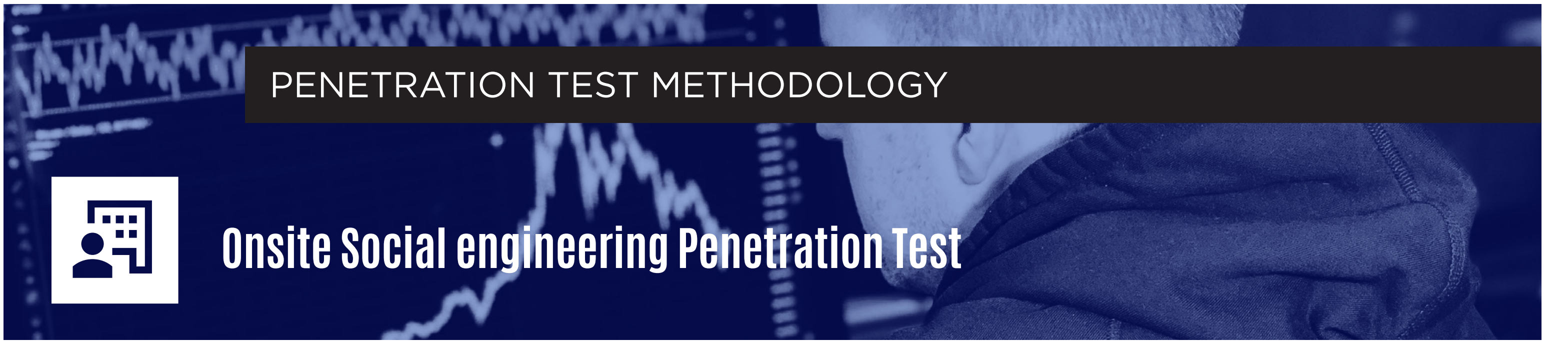
When entry is achieved, or provided following unsuccessful attempts, HALOCK will attempt to establish a return entry point. The purpose of this stage of the attack is to ensure the attacker has internal access, even if physical access is disrupted. Commonly utilized methods for establishing persistence involve the deployment of rogue wireless access, devices connected to the wired network that establish a secure tunnel to a remote attacker, enabling command and control on unattended endpoint systems already connected to the environment, gaining access to internal wireless networks, cloning RFID access badges, or performing other suitable methods as opportunity presents.

NETWORK EXPLOITS

When network access is achieved, limited internal network penetration testing is performed to determine if internal vulnerabilities could yield access or information. While performing a comprehensive internal network penetration test of the full environment is beyond the intent or scope of review of onsite social engineering penetration testing, targeted tests are pursued where appropriate to determine impact and provide examples of how an attacker could leverage the access achieved. The focus is to identify as many opportunities to improve security controls as possible, given the conditions available. Activities performed at the network exploit stage provide insights into the effectiveness of technical controls that are designed to limit the access a visitor has when onsite.

A prioritized approach is utilized to gather evidence and pursue further exploits. The attacker adapts based on the conditions, but typically prioritizes as follows:

- Gather basic supporting evidence, where necessary, to locate targets on the internal network. This commonly involves running limited network discovery and enumeration to locate key assets such as domain controllers.
- Identify weaknesses that could be leveraged to gain access to an insecure system due to missing patches, misconfiguration, or other vulnerabilities that can be quickly exploited with a high value return on the effort.
- Utilize devices to pursue information harvesting on the network through man-in-the-middle attacks or similar attacks targeting users and systems observed on the network.



Onsite Social engineering Penetration Test

- Identify potential secondary lateral targets on the network, determining the purpose of those hosts, and attempting to identify lateral services that may be of value to the attacker.

PHYSICAL VULNERABILITIES

Pursuing physical vulnerabilities is performed when an onsite presence can be maintained. These vary greatly based on perceived opportunity, but typically include:

- Deploying, and later collecting, keystroke loggers
- Viewing sensitive information not secured within the environment, such as printouts awaiting retrieval, documents left in the open in violation of clean desk policies, or content not properly disposed of. Note HALOCK does not remove these artifacts. Notes are captured that detail the type of document, categorical contents, location observed, and other details for reference.
- When secondary interior layer controls are in place, attempts to bypass these are pursued. For example, if anyone can enter the lobby, but only employees can enter the perimeter, and only a subset of employees can access a secure storage facility, HALOCK will attempt to escalate physical access through these layers to determine the extent in which an unauthorized individual could freely travel through the environment.
- Additional methods may be pursued, as opportunity presents.

DISENGAGING

Disengaging occurs most commonly when:

- All access, physical or logical, is lost or blocked
- Sufficient visibility into security controls has been explored
- The scheduled test window closes
- HALOCK is detailed by security personnel

When HALOCK disengages independently, attempts are made to retrieve all devices deployed during testing, close remote access where achieved, and render useless and access devices made such as visitor badges or cloned RFID cards. When this cannot be achieved, HALOCK notifies the project planning contact and requests assistance to complete this task.

Information is organized sequentially to facilitate the development of exploit walkthroughs, findings and recommendations, and related supporting information required to produce the penetration test report.

Services provisioned during preparation are decommissioned, listeners are closed to prevent continued contact, and any remaining sessions are exited.

PENETRATION TEST METHODOLOGY

Remediation Verification Penetration Test

OVERVIEW

Following the conclusion of a penetration test, remediation of identified vulnerabilities begins. The duration needed to implement recommendations and corrective actions to mitigate identified vulnerabilities varies based on the complexity of the required tasks, the volume of findings requiring attention, or other constraints specific to the organization. Following completion of remediation, validation is needed to ensure remediation activities were successful in achieving the intended result. Remediation verification testing is a process involving attempts to reproduce the vulnerabilities and associated exploits, providing confirmation that corrective measures have been implemented in a manner that prevents exploitation. Remediation verification testing involves the following activities:

PLANNING

Prior to initiating verification testing, planning may be required to establish test conditions, such as when access was required to perform the initial test. In some situations, supporting information may be requested by HALOCK to facilitate testing. The permitted testing dates and times are confirmed and the project plan is updated.

TESTING

HALOCK performs remediation verification testing to validate vulnerabilities have been resolved on the hosts they were observed during the initial test. Each documented vulnerability is reviewed and attempts to repeat the previous exploits are performed. The most common approach is to reperform the activities as performed during the initial test, however adjustments to the methods may be required when the configuration of the host, test conditions, or other factors warrant. In certain situations, variations of the previous exploit or vulnerability check may be necessary to validate remediation.

PENETRATION TEST REPORT REVISIONS

The previously issued penetration test report is updated to reflect observations and results of the remediation verification test.

- Vulnerabilities that can be fully confirmed to be remediated are marked as “remediated”.
- Vulnerabilities that are observed to remain unaddressed are marked as “not remediated”.
- Vulnerabilities that are observed to be partially resolved, but altered in some way that affects the previous finding, are marked as “partially remediated” in the report. Additionally, the finding is revised to reflect the specific observations resulting from remediation verification testing and may also results in revised exploit walkthroughs, where applicable.
- Vulnerabilities that cannot be verified due to test conditions are marked as “indeterminate”.

Following testing, the revised detailed report is issued. The summary letter, if applicable, is developed and issued following remediation verification testing. The letter summarizes the scope, timing, and methodology of the penetration test, and attests that verification of remediation was independently verified. As the summary letter is intended for consumption by external audiences, it is sanitized of sensitive details.