EMAGINED SECURITY®

Emagined Security Penetration Test Overview

2018

Sections

Penetration Testing Levels

Penetration Test Levels

- Level 0: Vulnerability Scan
  - Basic automated scan to satisfy regulatory requirements utilizing a single vulnerability tool.
  - The associated deliverable is limited to only raw reports from the tool.
  - No analysis on results is performed.
- Level 1: Vulnerability Assessment
  - Automated scanning with minimal manual validation of discovered issues.
  - Limited analysis on automated results is performed.
- **Level 2: Penetration Test (default)**
  - Automated and manual scanning with full manual validation of discovered issues.
  - Full analysis on automated results is performed.
- Level 3: Expanded Penetration Test
  - Automated and manual scanning with full manual validation of discovered issues.
  - Includes advanced exploitation, persistence and pivoting.
  - Full analysis on automated results is performed.

Penetration Test Levels

- Level 4 – Escalating Penetration Test
  - This version includes all tasks performed in the Expanded Penetration Test (Level 3) and adds in attack aggressiveness and sophistication over time with each subsequent test. Escalating Penetration Testing includes:
    - One (1) penetration test to establish a CUSTOMER baseline
    - Three (3) follow-on penetration tests within the same 12-month contiguous period which increases in attack aggressiveness and sophistication over time, and with each subsequent test iteration
  - These tests are designed to demonstrate what a trained and dedicated attacker might accomplish over an extended period of time. Additionally, this test will be enhanced to include as needed the following:
    - Industry Monitoring
    - Dedicated research of CUSTOMER specific, potential or requested vulnerabilities
    - Validation of newly discovered attack vectors
    - Application of industry currently emerging threats
    - Attack Recidivism

Penetration Test – Types (Color Boxes)

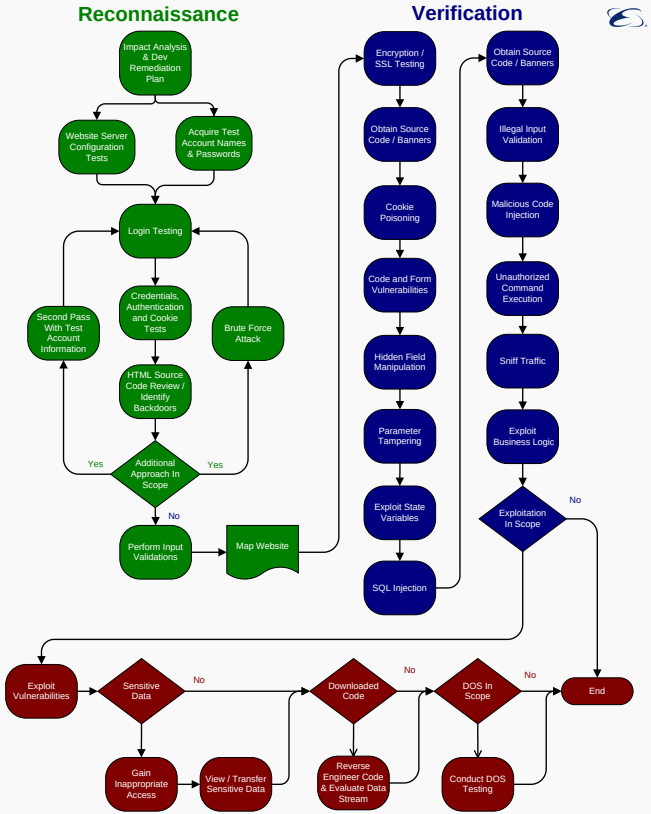
- Black
  - Closest in scope and focus to an actual attack. No pre-knowledge of the target is presumed
  - Pros: Lowest customer effort, extends best across all tests – less internal red tape usually to start
  - Cons: Does not maximize “testing” time as efforts are often spent researching and exploring
- Grey
  - Mixture in scope and focus of black and white. Assumes some knowledge of the target
  - Pros: Allows for viable testing while still permitting most in-place defenses and avoiding time-sinks
  - Cons: Assumptions may be drawn incorrectly about the actual security posture from the results
- White
  - Farthest in scope and focus to an actual attack. Knowledge about the target is readily available
  - Pros: Maximizes use of time, tends toward fuller coverage and allows for targeted defenses testing
  - Cons: Highest level of Customer workload as it requires increased effort to provide knowledge; internal red tape
- Emagined Security prefers a black to grey approach in most cases

Application Penetration Test

Application Penetration Test

- Designed to detect and validate the existence of security and information technology vulnerabilities within a Customer application (e.g., web, thin, thick, etc.)
- Vulnerabilities detected include exploitable and non-exploitable (e.g. less severe)
- Enables Customers to proactively identify, assess and remedy security issues prior to applications being placed into production or released for common use
- Involves automated and manual scanning and testing at unauthenticated and authenticated levels
- Follows industry standards and methodology for reproducible results

Application Penetration Test – Methodology (abbreviated)



Application Penetration Test - Reconnaissance

- Represents the information gathering and enumeration phase of an attack
- Data is collected passively or actively (i.e. by probing) about the application through automated and manual means
- The application is spidered, browsed or reversed to determine the extent and content of the application
- Key components of the application are documented and noted for exposure / follow on
- Application traffic is passed through a proxy and interrogated for further detail

Application Penetration Test - Verification

- Represents the vulnerability identification and validation phase of an attack
- Key components of the application are tested for vulnerabilities and exposures. These include:
  - Authentication, Authorization & Roles (e.g. Privileges and Permissions)
  - Data Input Validation, Handling & Processing
  - Sessions, Encryption & Sequencing
  - Business Logic, Source Code & Parameter and/or Field Manipulation
- Includes automated and manual identification and manual validation
- Culminates with validation of vulnerabilities that can or may be exploited

Application Penetration Test - Exploitation

- Represents the exploitation and compromise phase of an attack
- Leverages vulnerabilities identified in the earlier phase(s) to successfully penetrate security controls
- Includes mostly manual attacks with semi-automated support
- Concludes with Tester gaining access to application data, roles and/or permissions (e.g. access) not previously available to the Tester
- In some cases, application exploitation may not be possible given the security controls present, the complexity of the attack (e.g. undocumented) and the time allotment for testing

Application Penetration Test – Comprehensive

Some examples include:

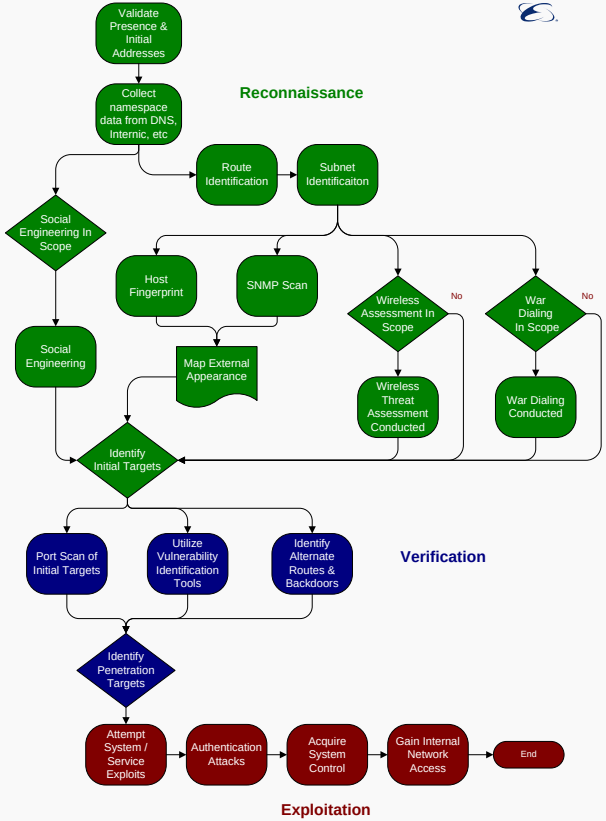
- Privilege escalation (horizontal, vertical)
- Encryption / SSL and data security (in-flight, at-rest)
- Cookie poisoning
- Code & Form vulnerabilities
- Hidden Field manipulation
- Parameter tampering
- Exploit state variables
- SQL Injection issues
- Source code / banners
- Input validation errors
- Malicious code
- Command / Client-Side injection (XSS, CSRF, HTML, XPath, XXE, etc.)
- Session replay, predictable sequencing & similar attacks
- Business logic errors
- OWASP Top 10

Network Penetration Test

Network Penetration Test

- Designed to detect and validate the existence of security and information technology vulnerabilities within a Customer network
- Vulnerabilities detected include exploitable and non-exploitable (e.g. less severe)
- Enables Customers to proactively identify, assess and remedy security issues on external and/or internal networks
- Involves automated and manual scanning and testing at an unauthenticated level to emulate an actual attack
- Follows industry standards and methodology for reproducible results

Network Penetration Test – Methodology (abbreviated)



Network Penetration Test - Reconnaissance

- Represents the information gathering and enumeration phase of an attack
- Network asset information and data is collected passively or actively (i.e. by probing) through automated and manual means
- Data collection involves, but is not limited to, DNS, ping, port-mapping, service identification, etc.
- Common network ports, protocols and services are confirmed, and noted for exposure / follow on
- Network traffic may also be passively collected (i.e. sniffed) or interrogated for further detail

Network Penetration Test - Verification

- Represents the vulnerability identification and validation phase of an attack
- Network assets are tested for vulnerabilities and exposures. These may include:
  - Servers & Workstations
  - Switches & Routers
  - Firewalls & Security Appliances
  - Network-Attached Storage & Print Devices
  - Management Systems & Administrative Interfaces
- Includes automated and manual vulnerability identification and manual validation
- Culminates with validation of vulnerabilities that can or may be exploited

Network Penetration Test - Exploitation

- Represents the exploitation and compromise phase of an attack
- Leverages vulnerabilities identified in the earlier phase(s) to successfully penetrate security controls
- Includes automated and manual attacks using industry tools, common and custom exploits
- Concludes with Tester gaining access to network data, roles (e.g. Domain Administrator) and/or permissions (e.g. authenticated access) not previously available to the Tester
- In some cases, network exploitation may not be possible given the security controls present, the complexity of the attack (e.g. undocumented) and the time allotment for testing

Network Penetration Test – Comprehensive

Some examples include:

- Privilege escalation (horizontal, vertical, pass the hash, token delegation, etc.)
- Null sessions
- Excessive permissions
- Unnecessary services (e.g., extraneous, Unix small services, web server instances, etc.)
- Unpatched systems, services and operating environments
- Outdated/EOL software
- Default SNMP community strings
- Multiple-source information disclosures (e.g. HTTP headers, version disclosure, verbose error messaging, etc.)
- Insufficient access controls / authorization
- Weak ciphers / cryptography
- Vulnerable software versions in use

Database Penetration Test

Database Penetration Test

- Designed to detect and validate the existence of security and information technology vulnerabilities within a Customer database
- Vulnerabilities detected include exploitable and non-exploitable (e.g. less severe)
- Enables Customers to proactively identify, assess and remedy security issues
- Involves automated and manual scanning and testing at unauthenticated and authenticated levels to emulate actual attacks
- May involve some custom requirements or objectives as requested by Customer

Database Penetration Test - Reconnaissance

- Represents the information gathering and enumeration phase of an attack
- Database information and data is collected passively or actively (i.e. by probing) through automated and manual means
- Testing may involve relational (e.g. SQL) or distributed (e.g. NoSQL) databases
- Data collection and analysis of database traffic dictates input for the verification phase
- Reconnaissance may involve legacy-based systems such as mainframes depending upon Customer

Database Penetration Test - Verification

- Represents the vulnerability identification and validation phase of an attack
- Database assets are tested for vulnerabilities and exposures. These tests may include:
  - Authentication and authorization
  - Role-based access controls and permissions
  - Encryption / dataflow protections and data governance
  - Monitoring, alerting and logging
  - Network and database segmentation, compartmentalization and isolation
- Includes automated and manual vulnerability identification and manual validation
- Culminates with validation of vulnerabilities that can or may be exploited

Database Penetration Test - Exploitation

- Represents the exploitation and compromise phase of an attack
- Leverages vulnerabilities identified in the earlier phase(s) to successfully penetrate security controls
- Includes automated and manual attacks using industry tools, common and custom exploits
- Concludes with Tester gaining access to the database, other roles (e.g. Database Administrator) and/or permissions (e.g. content or privilege access) not previously available to the Tester
- In some cases, database exploitation may not be possible given the security controls present, the complexity of the attack (e.g. undocumented) and the time allotment for testing

Database Penetration Test – Comprehensive

Some examples of comprehensive testing include:

- Privilege escalation (horizontal, vertical)
- Excessive or insufficient authentication
- Excessive or insufficient permissions
- Unpatched / Broken systems and software
- Insufficient access controls / authorization
- Weak ciphers / cryptography / data-at-rest encryption
- Data governance, dataflow protections and data integrity
- Availability-based attack vectors, where authorized
- Segmentation, compartmentalization and isolation
- SQL injection
- Business logic and functionality abuses
- Default credentials, misconfigurations and deployment issues/failures
- Common vulnerabilities (e.g. data leakage, TNS listener poisoning, etc.)

Mobile Penetration Test

Mobile Penetration Test

- Hybrid test designed to identify and exploit vulnerabilities present within the Mobile platform
- Focus tends to be largely on the Mobile Application but encompasses, at a minimum, partial hardware / physical device testing
- Follows a process methodology similar to standard Application and Network Penetration Testing
- Testing consists of unauthenticated and authenticated access

Mobile Penetration Test - Reconnaissance

- Represents the information gathering and enumeration phase of an attack
- Mobile application and asset information is collected passively or actively (i.e. by probing) through automated and manual means
- Data collection involves, but is not limited to, mobile application package (e.g. *.apk, *.ipa) reversal and analysis
- Data and communication exchanges and methods are logged, analyzed, and documented for further follow on
- Mobile traffic may also be passively collected (i.e. sniffed) or interrogated for further detail

Mobile Penetration Test - Verification

- Represents the vulnerability identification and validation phase of an attack
- Mobile applications and assets are tested for vulnerabilities and exposures. These may include:
  - Application signing, logging & debugging
  - Insecure API calls, key management, random number generation & encryption
  - Data caching (e.g. keyboard, device, application, clipboard, etc.)
  - Content providers, security providers & cert pinning
  - Application permissions, custom URL schemes, object persistence & WebViews
- Includes automated and manual vulnerability identification and manual validation
- Culminates with validation of vulnerabilities that can or may be exploited

Mobile Penetration Test - Exploitation

- Represents the exploitation and compromise phase of an attack
- Leverages vulnerabilities identified in the earlier phase(s) to successfully penetrate security controls
- Includes automated and manual attacks using industry tools, common, uncommon and custom exploits
- Concludes with Tester gaining access to mobile data, the mobile application itself, and/or permissions (e.g. elevated access) not previously available to the Tester
- In some cases, mobile exploitation may not be possible given the security controls present, the complexity of the attack (e.g. undocumented) and the time allotment for testing

Mobile Penetration Test – Comprehensive

- Application Based Mobile Device Protection
  - Failure to Restrict URL Access
  - Certificate / Key Storage
  - Insecure Cryptographic Storage
  - Hardware Encryption
  - Login testing - user accounts and passwords
  - Network Isolation
  - Antiforensics – Local Data Encryption
  - Jailbreak Detection
  - Secure Application Deployment
- Application Data Security
  - Data Segmentation
  - Database encryption
  - Data retention (on device)
  - Data time to live
  - Encryption/SSL testing
- Dynamic Application Testing
  - Application code, back door or debug option weaknesses
  - Broken Authentication and Session Management
  - Cookie poisoning
  - Cross Site Request Forgery (CSRF)
  - Cross Site Scripting (XSS)
  - Executable code testing such as buffer overflows
  - Form vulnerabilities
  - Hidden field manipulation
  - Injection
  - Insecure Direct Object References
  - Parameter tampering
  - Unvalidated Redirects and Forwards
  - Denial of Service
  - Data exfiltration
  - Code obfuscation

Mobile Penetration Test – Comprehensive (cont.)

- Mobile Application Configuration
  - Application patching and configurations
  - Credential, authentication and cookie testing
  - Jailbreak Detection
  - Repackaging Weakness
  - Proxy Configuration
  - Local File Manipulation
  - Location Awareness (Geo-Fencing)
- Backend Connected Systems
  - Backend Patching and Configurations
  - Backend Server Configuration
  - Direct Server Access
  - Unauthenticated Analysis
  - Parameter Manipulation
  - Client Validation
  - Denial of Service
  - Full Application Test
- Mobile Device Analysis
  - Application Context Device Vulnerabilities
  - Buffer/Heap Overflow
  - Insecure Object Reference
  - Application Information Disclosure
  - Physical Controls
- OWASP Mobile Top 10 (2016)
  - Improper Platform Usage
  - Insecure Data Storage
  - Insecure Communication
  - Insecure Authentication
  - Insufficient Cryptography
  - Insecure Authorization
  - Client Code Quality
  - Code Tampering
  - Reverse Engineering
  - Extraneous Functionality

Wireless Penetration Test

Wireless Penetration Test

- Designed to detect and validate the existence of security and information technology vulnerabilities within a Customer's wireless network
- Vulnerabilities detected include exploitable and non-exploitable (e.g. less severe)
- Enables Customers to proactively identify, assess and remedy security issues on internal, guest and public-facing / public use wireless networks
- Involves automated and manual scanning and testing at unauthenticated and authenticated levels
- Can be incorporated into traditional network penetration testing or purchased standalone

Wireless Penetration Test - Reconnaissance

- Represents the information gathering and enumeration phase of an attack
- Wireless asset information and data is collected passively or actively (i.e. deauth, injection, etc.) through automated and manual means
- Data collection involves, but is not limited to querying wireless access points (WAP), capturing wireless beacons and broadcasts, and impersonating clients
- Common wireless network ports, protocols, encryption levels / types, and services are confirmed and noted for exposure / follow on
- Wireless traffic is routinely collected (i.e. sniffed) and interrogated for further detail

Wireless Penetration Test - Verification

- Represents the vulnerability identification and validation phase of an attack
- Wireless network assets are tested for vulnerabilities and exposures. These may include:
  - Weak initialization vectors (IVs) and encryption
  - 4-way handshake
  - WEP, WPS, WPA and similar legacy protocols
  - Brute-force, password-guessing
  - Misconfigurations, default / vendor set ups, and similar implementation issues
- Includes automated and manual vulnerability identification and manual validation
- Culminates with validation of vulnerabilities that can or may be exploited

Wireless Penetration Test - Exploitation

- Represents the exploitation and compromise phase of an attack
- Leverages vulnerabilities identified in the earlier phase(s) to successfully penetrate security controls
- Includes automated and manual attacks using industry tools, common and custom exploits
- Concludes with Tester gaining access to the wireless network, wireless data, and/or permissions (e.g. unauthorized access) not previously available to the Tester
- In some cases, wireless network exploitation may not be possible given the security controls present, the complexity of the attack (e.g. undocumented) and the time allotment for testing

Wireless Penetration Test - Comprehensive

- Some examples of comprehensive testing efforts include:
  - Confirming WLAN and WAPs SSID(s), channels and operating frequency
  - Identifying accessibility and range of wireless networks/WAPs from outside the physical location(s)
  - Connecting to target access point
  - Impersonating an AP
  - Impersonating a STA (e.g. wireless client)
  - Interrogating wireless infrastructure and supporting switches, routers and PEPs
  - Capturing information transmitted over the air (confirm encryption)
  - Decrypting and reading transmitted information (analyze traffic to map other network components)
  - Further mapping/identifying internal network
  - Gathering information from client computer
  - Deauthentication, chop-chop and similar attack vectors susceptibility
  - Capturing and interrogation of the 4-way handshake
  - Password / passphrase cracking or brute-forcing
  - BlueTooth, NFC, RF-based assessments and attack vectors, when and where applicable

Web Services / Application Programming Interface (API) Penetration Test

Web Services / API Penetration Test

- Designed to detect and validate the existence of security and information technology vulnerabilities within a Customer application (e.g., web, thin, thick, etc.)
- Vulnerabilities detected include exploitable and non-exploitable (e.g. less severe)
- Enables Customers to proactively identify, assess and remedy security issues prior to applications being placed into production or released for common use
- Involves automated and manual scanning and testing at unauthenticated and authenticated levels
- Follows industry standards and methodology for reproducible results

Web Services / API Penetration Test - Reconnaissance

- Represents the information gathering and enumeration phase of an attack
- Data is collected passively or actively (i.e. fuzzing) about the application through automated and manual means
- Application functionality is determined and documented through a combination of calls submissions, sample project package (e.g. POSTMAN, SOAP, etc.) analysis and WS/API documentation reviews
- Key parameters are documented and noted for exposure / further follow on
- Web service application traffic is passed through a proxy and interrogated for further detail

Web Services / API Penetration Test - Verification

- Represents the vulnerability identification and validation phase of an attack
- Key components of the web services application are tested for vulnerabilities and exposures. These include:
  - Authentication, Authorization & Roles (e.g. Privileges and Permissions)
  - Data Input Validation, Handling & Processing
  - Encryption & Sequencing
  - Business Logic, Source Code & Parameter Manipulation
- Includes automated and manual identification and manual validation
- Culminates with validation of vulnerabilities that can or may be exploited

Web Services / API Penetration Test - Exploitation

- Represents the exploitation and compromise phase of an attack
- Leverages vulnerabilities identified in the earlier phase(s) to successfully penetrate security controls
- Includes mostly manual attacks with semi-automated support
- Concludes with Tester gaining access to web services application data and/or permissions (e.g. access) not previously available to the Tester
- In some cases, web services application exploitation may not be possible given the security controls present, the complexity of the attack (e.g. undocumented, or not enough documentation/context) and the time allotment for testing

Web Services / API Penetration Test – Comprehensive

Some examples of comprehensive testing include:

- Fuzzing
- Identification, Authentication & Authorization
- Encryption / SSL and data security (in-flight, at-rest)
- Other communication protection mechanisms (e.g. freshness)
- Web service chains
- Parameter tampering
- Schema validation
- Content validation
- Output encoding
- Malicious code / Virus protection
- Command / Client-side injection (XSS, CSRF, HTML, XPath, XXE, etc.) – particularly for upstream or downstream consumers
- Message size
- DoS protections and availability
- Business logic errors

Industrial Control Systems (ICS) / Supervisory Control And Data Acquisition (SCADA) Penetration Test

ICS / SCADA Penetration Test

- Designed to detect and validate the existence of security and information technology vulnerabilities within a Customer's ICS/SCADA network
- Vulnerabilities detected include exploitable and non-exploitable (e.g. less severe)
- Enables Customers to proactively identify, assess and remedy security issues on industrial control systems networks
- Involves manual testing at an unauthenticated level
- Purposefully designed to be non-invasive as ICS/SCADA networks are generally fragile, implement weaker security controls and are more prone to availability-based issues

ICS / SCADA Penetration Test - Reconnaissance

- Represents the information gathering and enumeration phase of an attack
- ICS / SCADA asset information and data is collected passively through manual means – depending upon network stability some automation may be used
- Data collection involves, but is not limited to, OC network isolation, ARP scanning, port scanning, passive enumeration and physical inspection, where permissible
- Commonly used network ports, protocols and services are confirmed, and noted for exposure / follow on
- Network traffic may also be passively collected (i.e. sniffed) for further detail

ICS / SCADA Penetration Test - Verification

- Represents the vulnerability identification and validation phase of an attack
- ICS / SCADA network assets are tested for vulnerabilities and exposures. These may include:
  - Legacy exposures – technologies not initially built with security in mind
  - Operation Control (OC) network isolation from IT networks
  - Internet-accessibility, dependency, reliance or other exposures
  - Unnecessary and extraneous services
  - Insufficient or missing authentication, identification and authorization controls
- Includes manual vulnerability identification with manual validation – some traditional penetration testing tools may be used depending upon network stability
- Culminates with validation of vulnerabilities that can or may be exploited

ICS / SCADA Penetration Test - Exploitation

- Represents the exploitation and compromise phase of an attack
- Leverages vulnerabilities identified in the earlier phase(s) to hypothetically* penetrate security controls – *ICS / SCADA networks do not generally respond well to exploitation
- Includes manual attacks using industry tools, common and custom exploits
- Concludes with Tester demonstrating how access to ICS network data, and/or permissions (e.g. unauthorized access) may be obtained
- In most cases, ICS / SCADA network exploitation is not attempted due to network fragility, the criticality of the assets / network involved (i.e. critical infrastructure), and the lack of sufficient test and/or backup environments

ICS / SCADA Penetration Test – Comprehensive

Some examples of comprehensive testing include:

- OC v. IT network segmentation and isolation
- Passive and active (e.g. ARP scanning) enumeration and port scanning
- Excessive permissions
- Unnecessary services
- Unpatched systems, services and operating environments
- Outdated/EOL software
- Default SNMP community strings
- Multiple-source information disclosures
- Insufficient access controls / authorization
- Weak ciphers / cryptography
- Vulnerable software versions in use
- Legacy services enabled and/or actively in use
- Embedded device exposures and public exploits

Internet of Things (IoT) Penetration Test

Internet of Things (IoT) Penetration Test

- Designed to detect and validate the existence of security and information technology vulnerabilities within a Customer IoT device or appliance and the extended network
- Vulnerabilities detected include exploitable and non-exploitable (e.g. less severe)
- Enables Customers to proactively identify, assess and remedy security issues for IoT devices / appliances
- Involves automated and manual scanning and testing at an unauthenticated level (i.e. “black box”) to emulate an actual attack
- Follows industry trends and emerging technologies attack vectors

IoT Penetration Test - Reconnaissance

- Represents the information gathering and enumeration phase of an attack
- IoT asset information and data is collected passively or actively (i.e. by probing) through automated and manual means
- Data collection involves, but is not limited to, embedded devices, firmware, wireless protocols, IoT applications, cloud services and supporting infrastructure
- Common network ports, protocols and services are confirmed, and noted for exposure / follow on
- Device traffic is also collected (i.e. sniffed) and interrogated for further detail

IoT Penetration Test - Verification

- Represents the vulnerability identification and validation phase of an attack
- IoT assets are tested for vulnerabilities and exposures. These tests may include:
  - Embedded device and associated sensors receivers and actuators
  - Mobile applications and C2 (i.e. Command and Control) functionality
  - Cloud-based services, including hosting/administration, API and web
  - Network communication protocols (e.g. 802.11, 802.3, etc.)
  - Intra-component communications (e.g. 802.15, etc.)
- Includes automated and manual vulnerability identification and manual validation
- Culminates with validation of vulnerabilities that can or may be exploited

IoT Penetration Test - Exploitation

- Represents the exploitation and compromise phase of an attack
- Leverages vulnerabilities identified in the earlier phase(s) to successfully penetrate security controls
- Includes automated and manual attacks using industry tools, common and custom exploits
- Concludes with Tester gaining access to IoT data and/or permissions (e.g. elevated access) not previously available to the Tester
- In some cases, exploitation may not be possible given the security controls present, the complexity of the attack (e.g. undocumented) and the time allotment for testing

IoT Penetration Test – Comprehensive

Some examples of comprehensive testing include:

- Privilege escalation (horizontal, vertical)
- Protocol tampering (e.g. TCP, UDP, Wireless, BlueTooth, Zigbee, RF, etc.)
- Excessive or insufficient permissions
- Unnecessary services or functionality
- Insufficient access controls / authorization
- Weak ciphers / cryptography
- OWASP Top 10 and Mobile Top 10
- Physical inspection, JTAG, Serial and chip-off (i.e. time-intensive and expensive)
- Web service and API communications and functionalities
- OSINT data collection and attack proliferation research – e.g. forums, release boards, etc.
- Replay and similar session-based attacks
- C2, authentication, trust and similar identity-based attacks
- Operating system and embedded device exposures and vulnerabilities

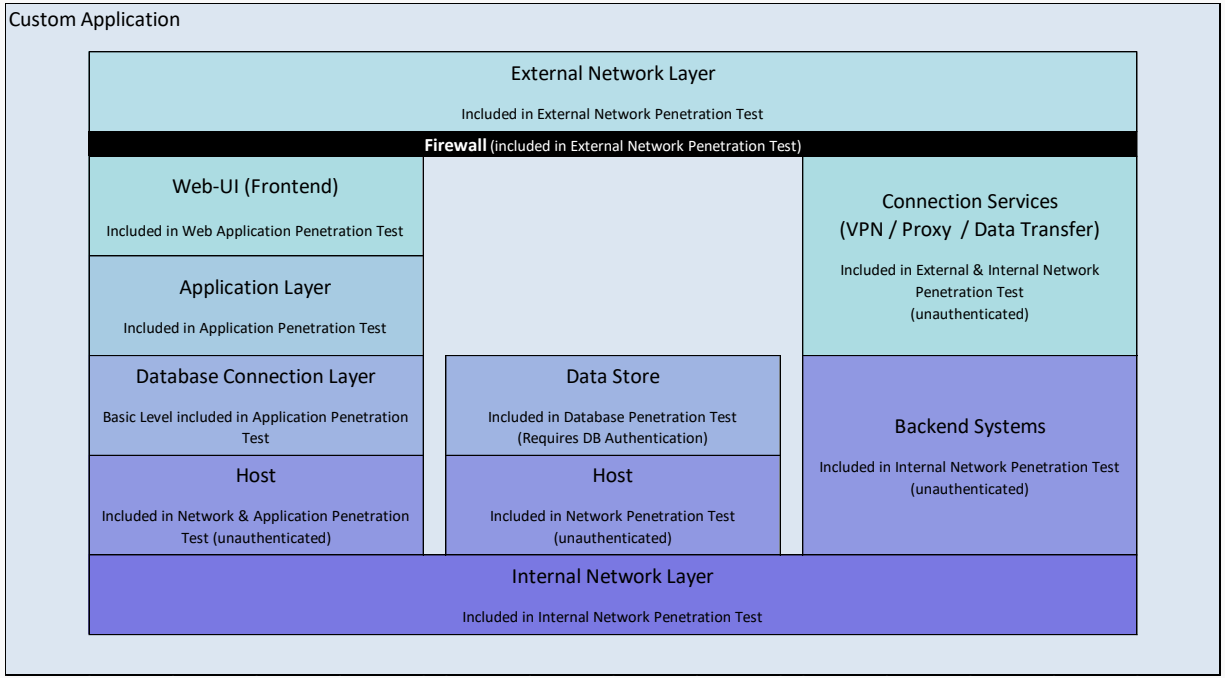
Custom Penetration Test

Custom Penetration Test

- Uniquely-defined test designed to meet specific Customer objectives, tasks and goals
- Focus will be set by Customer and mutually agreed upon by Emagined Security
- Emagined Security retains the right to decline custom engagements at its discretion
- Follows a process methodology similar to standard Application and Network Penetration Testing unless otherwise defined by Customer
- Testing may consist of unauthenticated and/or authenticated access, external and/or internal assets, hardware and/or software, or any other number of testing options or derivatives

Custom Penetration Test

- Custom penetration tests often incorporate multiple testing areas:



Penetration Test Process

Penetration Test Process - Preparation & Scoping

- Designed to assess the impact of potential interruptions on operations and business prior to scoping
- Utilizes engagement questionnaires to define boundaries and establish Rules of Engagement (RoE)
- Scope is determined through a series of prepatory conference calls, in-person meetings (if applicable), and/or application demonstrations / walk-throughs
- Scope will be clearly documented and communicated by Emagined Security and agreed upon by the Customer

Penetration Test Process - Engagement Manager

- Every penetration test is managed by an engagement manager
- Engagement manager is assigned at the project's outset, and serves as the Customer's primary point of contact (PPoC)
- Coordinates project kick-off and debrief meetings, daily / weekly status calls, distributes daily start and stop notifications for testing, and provides daily updates
- Assists Customer with managing and coordinating all facets of testing; helps to resolve testing issues on the rare chance they occur
- Facilitates communications between Customer and the testing team

Penetration Test Process - Execution

- Project scoping is performed in advance of testing and actively engages Customer
  - A kick-off meeting occurs a few days prior to testing commencement (e.g. week preceding)
  - Tests that incur a delayed start date automatically extend the testing schedule accordingly

- Optimized attack surface approach under enhanced methodology
  - All penetration testers follow a numerically ordered approach
  - Penetration testers work as a team, and know exactly what has been performed at a given point in time based upon numerical ordering

- Internal attestations are required
  - Penetration testers are required to sign off on testing components to ensure thoroughness
  - Management reviews both the attestations and deliverables on every pen test to ensure comprehensive coverage

Penetration Test Process - Methodology Attestation Example

Scoping

Define application name and project identifiers:
Define deadlines:
Define testing windows:

Notes

Background

Ensure the background details of the application are known. Understand the business purpose of the application, and the roles in scope.

1 Define roles in the project wiki, associated with any credentials.
2 Request role matrix.
  2.1 Provide client instructions on how to get this.
3 Receive a demo of the application.
  3.1 Obtain use-case documentation.
4 Request sitemap of the application.

Notes

Unauthenticated Analysis

Perform a full analysis of the application without any authentication.

1 Restore Burp Suite Pro to the baseline state.
2 Set the scope to the root directory (as defined in the project wiki).
3 Passive information gathering
  3.1 Use internet searches to view cached/interesting content.
    3.1.1 Access -> Authorization -> Insufficient Authorization
    3.1.2 Environment Analysis -> Configuration -> Information Leakage
    3.1.3 Host Analysis -> Vulnerable OS -> Server Misconfiguration
    3.1.4 Host Analysis -> Vulnerable Application -> Server Misconfiguration
  3.2 Utilize open source intelligence tools (whois / way back machine / google-dorks / etc.) to identify environment details and content.
    3.2.1 Environment Analysis -> Configuration -> Information Leakage
    3.2.2 Host Analysis -> Vulnerable OS -> Server Misconfiguration
    3.2.3 Host Analysis -> Vulnerable Application -> Server Misconfiguration
4 Spider the application (note some environments make this difficult and require manual spidering).
  4.1 Utilize the "Engagement" tools on the target to perform analysis of the data provided. Look for pages, info and details, which should only be available to authenticated users.
    4.1.1 Identify unique static and dynamic URL's.
    4.1.2 Identify all application parameters.
    4.1.3 Identify all JavaScript/JSON functions.
    4.1.4 Identify all application source comments.
5 Environment Analysis
  5.1 Scan the target environment utilizing Nikto (or like tool).
    5.1.1 Access -> Authentication -> Insufficient Authorization
    5.1.2 Access -> Authentication -> Information Leakage
    5.1.3 Access -> Authorization -> Insufficient Authorization

Notes

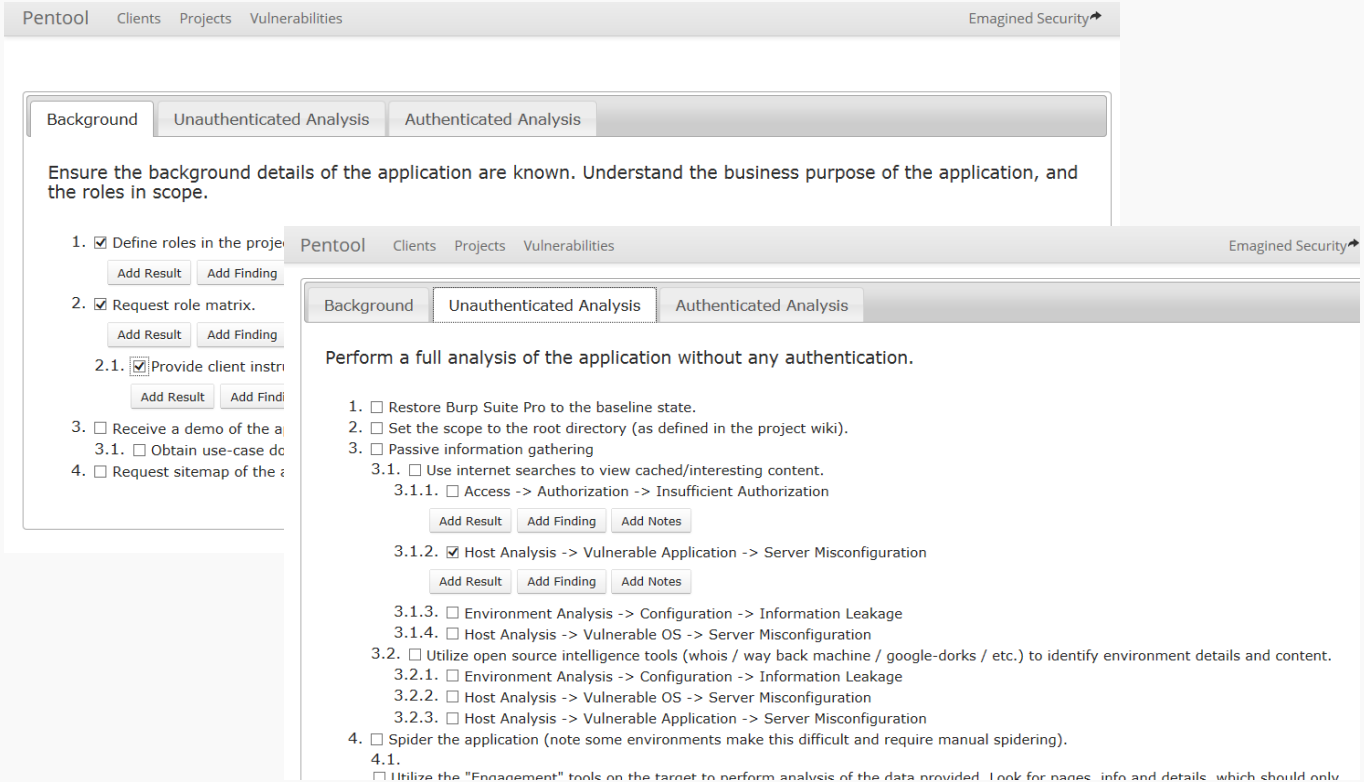
☐ Completed
Finding 3.1.1: _____
Finding 3.1.2: _____
Finding 3.1.3: _____
Finding 3.1.4: _____

☐ Completed
Finding 3.2.1: _____
Finding 3.2.2: _____
Finding 3.2.3: _____

☐ Completed
Finding 4.1.1: _____
Finding 4.1.2: _____
Finding 4.1.3: _____
Finding 4.1.4: _____

☐ Completed
Finding 5.1.1: _____
Finding 5.1.2: _____
Finding 5.1.3: _____

Penetration Test Process - Methodology Attestation Example (cont.)



Differentiating Factors

Differentiating Factors

- Emagined Security employs over fifteen (15) differentiating factors collected from over a decade of experienced, proven consulting

- One of those factors is Optional Services that enhance overall penetration testing engagements:
  - High-Level Asset Discovery
  - High-Level Risk Review
  - Hardened Host Assessments

- Additional factors, include, but are not limited to:
  - Enhanced Reporting
  - Exploit Recording
  - Principal-led Engagements
  - Industry-certified, US citizens assigned to all engagements

Differentiating Factors - Enhanced Reporting

- Emagined Security offers several enhanced reporting differentiators, including:

- Intelligent consolidation of findings
  - Report findings are included in intelligent groupings to ensure that similar findings are easier to remediate
    - If requested, non-intelligent groupings can be provided so each finding can be addressed individually
  - Testing areas that did not result in findings are written up to explain what steps were taken / performed
  - Emagined Security can provide historical correlation and finding significance over multiple engagements

- Vulnerability Table
  - When requested, Emagined Security will create a vulnerability table to assist Customers in their remediation efforts

Differentiating Factors – Exploit Recording

- Customers can request recordings of select exploits performed in an engagement for a nominal charge
- Subject matter expertise does not mean that our Customers cannot directly benefit from an exchange of information on the “how” – this is particularly true for common vulnerabilities that plague multiple organizations
- In these recordings, our testers provide a clear walk-through on the steps taken to successfully identify and exploit the selected vulnerabilities
- Customer awareness and peace of mind is never sacrificed in favor of industry speaking engagements on the latest exploits

Differentiating Factors – Principal-led Engagements

- Emagined Security assigns Principals to every engagement, regardless of size
- Additionally, a senior tester will work every engagement as well, regardless of size
- That bears repeating – **two (2) senior testers assigned to every engagement**
- We are not aware of anyone else offering this level of competency in the market
- Most security firms will use smaller engagements to pad their test team with junior or trainee testers – some may 100% outsource

Differentiating Factors - Skilled Personnel

- Customers can rest easy knowing all penetration testers assigned to the engagement are U.S. citizens, and industry-recognized certification holders, including OSCP, CISSP, C|EH and more

- All penetration testers are under a continuous learning regimen and skills assessment:
  - Penetration testers are required to acquire at least one additional certification per year or complete a pre-defined level of CPEs based on job title
  - Our penetration testers are continually identifying ways to improve effectiveness
  - Internal training sessions are held multiple times (3x) throughout the year and are mandatory
  - An annual review process identifies core objectives and skills to develop for the next cycle

- This directly correlates to a better level of service offering and testing execution for our Customers than found in other security firms / competitors with less stringent requirements

Deliverables

Deliverables

- Features a high-quality narrative report documenting the findings and observations from the testing engagement

- The Report is delivered, in most cases, the week after the engagement concludes, and contains the following sections:
  - Executive Summary
    - Addresses the overall security posture of the assets tested, provides areas of strength and opportunity, and a summary findings list
  - Introduction
    - Includes a narrative of the testing objective(s) and a description of the tasks performed
  - Testing Methodology
    - Documents the Emagined Security testing methodology used

Deliverables (cont.)

- Identified Vulnerabilities
  - Contains detailed technical findings and observations from the testing engagement
  - Individual findings are broken down into subsections that address, through a clear and concise narrative, the vulnerability description, its potential or realized impact, the recommended mitigation actions and references for additional reading support
  - Vulnerabilities detailed are assigned one of five rankings:
    - Critical – issues that present eminent threats to the Customer and that require immediate resolution
    - High – issues that pose immediate impact to the Customer and should be addressed immediately
    - Medium – issues that present a moderate impact to the Customer and should be addressed in a timely manner
    - Low – issues that pose limited impact to the Customer and should be considered for remediation
    - Informational – issues that do not constitute a threat or lasting impact, but deviate from expected norms
- Conclusions
  - Details overall conclusions and recommendations based upon testing results
  - Often contains a forward-looking statement on Customer security

Experts In Information Security

THANK YOU!

David Sockol
CEO & President
2816 San Simeon Way
San Carlos, CA 94070
(650) 593-9829

email: davidsockol@emagined.com
web: www.emagined.com

Why Emagined Security

01

Our clients have come to know that working with Emagined Security is a professional, low risk way to develop and secure new business initiatives

02

Emagined Security offers a cost effective, reliable, high-quality alternative to in-house resources for security efforts

03

Emagined Security offers Fortune and Global 1000 corporations a comprehensive array of sophisticated, adaptive security solutions that include both consulting and managed services

Optional / Other Services

High-Level Asset Discovery – Optional Service

- Designed so Customers know exactly what they have for information technology assets
- Affords Customers an objective view of their attack surface
- Uses custom technology to rapidly scan IP ranges and associated URLs for running applications on common web ports
- Once assets are discovered, each is analyzed further to determine complexity and associated security risk vectors
- Allows Customers to establish security baselines and prioritize assets

High-Level Risk Review – Optional Service

- Applies a qualitative risk ranking across multiple assets / IP ranges
- Ranks assets on a number of identifying criteria, including:
  - Asset type and functionality
  - Presence of sensitive data
  - Number of open ports
  - Number and type of enabled services
  - Presence of ‘low-hanging fruit’ vulnerabilities – e.g. information disclosures
  - Juxtaposition against other like assets in scope
- Affords Customer to make educated decisions on where to apply security funds without the need for testing every asset
- Helps Customer determine when and where penetration testing is warranted

Hardened Host Assessment – Optional Service

- Applies a Customer-proprietary or industry hardening baseline (e.g. CIS) / standard
- Assessment focuses on the efficacy of the procedures in meeting the standard, including:
  - Reduction of attack surface
  - Removal of unnecessary and extraneous services
  - Lockdown of permissions and access
  - Confirmation of patching and hotfixes
  - Reduction of exposures and information leakage
  - Validation of security controls and protections
- Allows Customer to confirm vulnerabilities and security issues at the privileged level
- Can be incorporated in a penetration test or purchased standalone

EMAGINED SECURITY®

Security Services

2816 San Simeon Way,
San Carlos, CA 94070
1-415-944-2977

Info@emaginedcom