EMAGINED SECURITY

Emagined Security
2816 San Simeon Way
San Carlos, CA, 94070

Phone: (415) 944-2977
www.emagined.com

Date: April 20, 2020

To: Ivanti Customer

Subject: Emagined Security and Ivanti Security and Penetration Testing 2020

The Emagined Security Information Security Team in collaboration with Ivanti will be performing enhanced and progressive penetration testing on the Ivanti applications listed below in 2020. This partnership has been formed to ensure that Ivanti applications meet exceedingly more comprehensive testing methods to provide its customers a secure application platform for their data. With the enhanced attacks that both Emagined Security and Ivanti have seen over the past few years, we know the best way to secure our applications is with continued and expanded security testing. With this in mind, Ivanti has determined it will be performing progressive testing on the following applications in 2020:

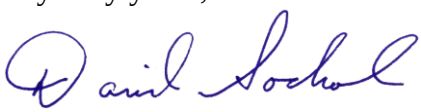
- Ivanti Cloud
- Ivanti Endpoint Manager (EPM)
    - Emphasis on EPM client agent and Cloud Service Appliance.
- Supply Chain
    - Emphasis on Avalanche and Studio
- Patch for Linux, Unix, and Mac
- Identity Director
- Service Desk (powered by LANDesk)
- Workspace Control powered by RES
- AppSense Suite
    - Emphasis on Workspace Manager, Environment Manager, and Performance Manager
- Device Control (IDAC)

As with any penetration testing, product vulnerabilities found will be remediated within appropriate timeframes.

Criticality	Timeline
Critical (9.0-10.0)	During the current development iteration or cycle, prior to release of application to production
High (7.0-8.9)	During the current development cycle or scheduled for a release to be completed within 90 days of current release.
Medium (4.0-6.9)	Bugs must be opened for tracking purposes, but remediation is at discretion of development.
Low (.1-3.9)	Bugs must be opened for tracking purposes, but remediation is at discretion of development.

If you have any questions on the application and network methodologies or any additional details on the penetration testing that may not be covered in the appendixes you may reach out to Paul Underwood, Chief Operations Officer, Emagined Security. Paul Underwood can be reached at 801-294-2917 or paulunderwood@emagined.com.

Very truly yours,



David Sockol

President & CEO

Emagined Security, Inc.

Ivanti & Emagined Security Penetration Testing Services Methodology – Appendix 1

Prepared For:
Ivanti Customers
1/15/2020

Prepared By:
Emagined Security
2816 San Simeon Way
San Carlos, CA 94070
650-593-9829
www.emagined.com

Emagined Security is the leading professional services provider for Information Security & Compliance solutions. Emagined Security focuses on securing business solutions by providing a full complement of proactive, real-time, reactive, and knowledge sharing security services.

Emagined Security's commercial clients cover a wide range of U.S. and global Fortune 500 organizations, including the financial services, energy, healthcare, high tech, manufacturing, & insurance industries. Emagined Security prides ourselves with only employing well-known and respected individuals from the security community. Emagined Security offers consultants with high levels of knowledge, industry certifications and practical experience.

EMAGINED SECURITY

Ethical Hacking / Penetration Test Methodology

This document contains a general outline of the procedures to complete a vulnerability assessment / penetration test / ethical hack. Emagined Security defines each of the types of these tasks as follows:

- *Expanded Penetration Test (Level 3 – Red Team):* This version includes the Defined Penetration Test and adds attempts to use the exploited vulnerabilities to compromise systems behind the initial targets. Additionally, Expanded Penetration Testing can be used to:
    - Evaluate the organization's security awareness
    - Validate the effectiveness of existing security controls
    - Attempt to compromised and / or circumvent security control undetected
    - Evaluate intrusion detection effectiveness
    - Assess incident response identification and response effectiveness
    - Test incident response capabilities

  This is an exercise designed to demonstrate what an extremely skilled and dedicated attacker might reasonably accomplish during the testing period. This is the most extensive version of the test.
- *Defined Penetration Test (Level 2):* This version includes the Vulnerability Assessment and adds exploitations of the vulnerabilities within the defined scope. This is the standard version of the test.
- *Vulnerability Assessment (Level 1):* This version includes only scans and validation of vulnerabilities. It is minimal version of the test.
- *Vulnerability Scan (Level 0):* This version includes a basic scan to satisfy regulatory requirements utilizing a single vulnerability tool. The associated deliverable is limited to only raw reports from the tool. No CONSULTANT analysis on results will be performed.

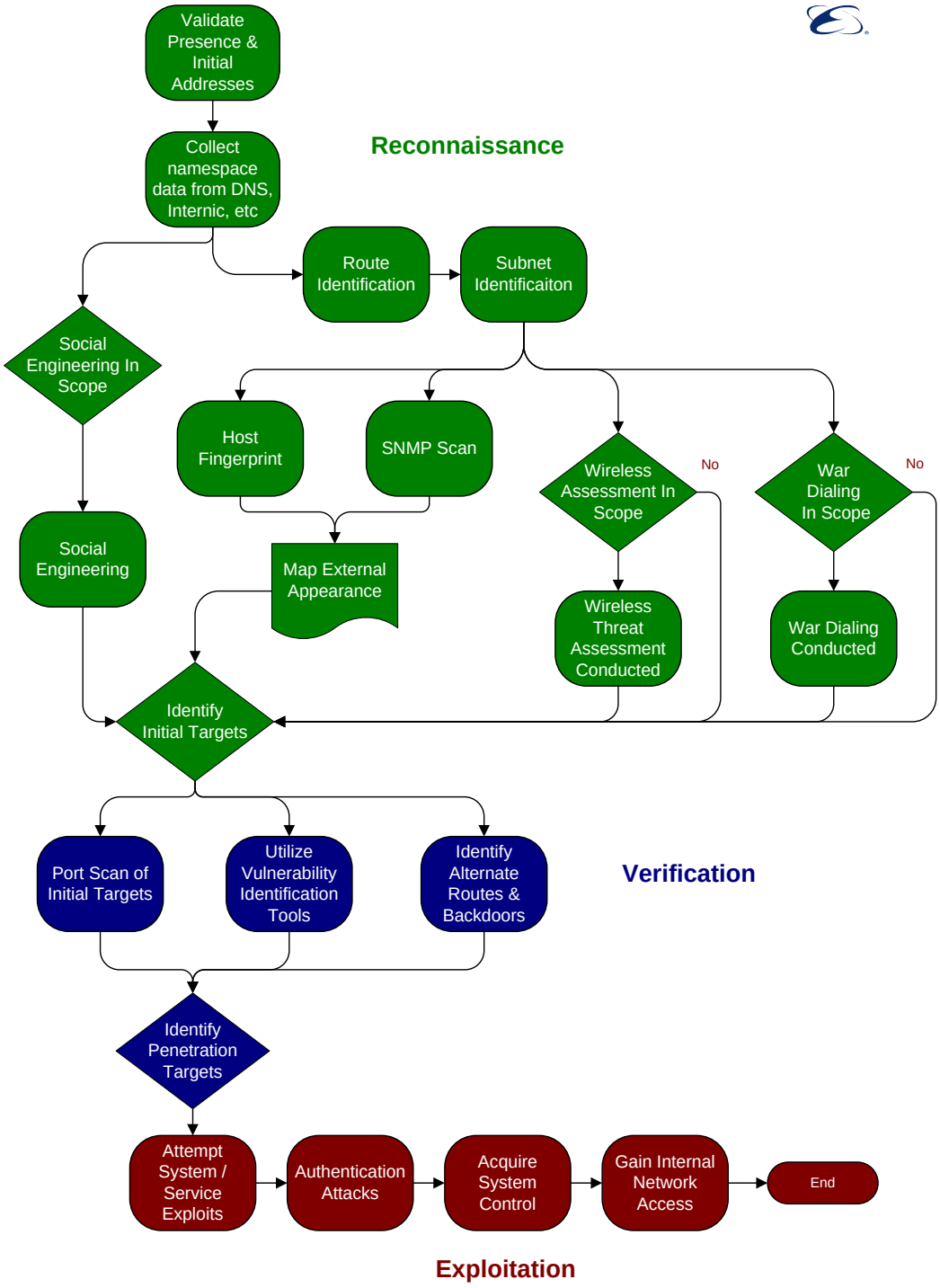
In this document, the versions of the test will be referred to as Penetration Tests. This document covers Emagined Security's Penetration Testing methodology at a high level; it does not enumerate the specific steps included in our procedures. Penetration tests are broken into three phases. While each phase is separate, not all phases are independent of each other. Some activities such as avoiding detection are listed as a separate phase, but they in reality typically also occur during all other phases of a test.

Before the penetration test begins the client must determine several parameters. These include:

- *Attacker Persona*: Will the penetration test mimic the actions of an outsider to the company, or a company employee, or some combination? For those studies coming from the outside efforts will center on only Internet connectivity, or will efforts such as partner locations be used as points to the network?
- *Methods Allowed*: The exact types of methods should be enumerated. This includes whether certain classes of attacks (e.g., Buffer Overflows, Denial of Service (DoS)) will be used.
- *Access to Results*: Who has access to the results of the test must be agreed upon beforehand. This also will limit those individuals that can be present during the actual test. (See monitoring below)
- *Systems Allowed*: This will identify the systems being tested and enumerate those specific systems that are "off limits" and cannot be tested.
- *Monitoring*: High level logs of activities must be kept and made available to the client. This also includes if the client must be present during all activities.
- *Professional Manner*: Company should require persons conducting test to act in a professional manner, meaning that they will not try attacks known to violate parameters established in the methods section and adhering to the C|EH or CISSP rules. Unprofessional conduct includes, for example, using known DoS attacks when DoS attacks have specifically been excluded.
- *Social Engineering*: Emagined Security does not routinely conduct "social engineering" attacks on customer support organizations because those are typically highly destructive. Emagined Security will work with a customer to design an assessment program that measures vulnerability to a social engineering attack without performing the deceitful activities commonly referred to as social engineering.

Phases of the Network Penetration Test

Penetration tests typically follow a structured approach that may be modified slightly in response to data as it is collected.



High Level Descriptions

Reconnaissance:

The initial phase of any security review involves extensive data collection. Penetration tests are no exception. The following methods may be used as part of this information-gathering phase:

- Web searches and newsgroup browsing
- DNS zone transfers, interNIC queries
- Route and Subnet Identification
- Host Fingerprinting (IP scanning) and SNMP sweeps
- Network mapping with traceroute and other tools
- Social Engineering (if allowed)
- Wireless Testing (when in scope)
- War Dialing (when in scope)
- Initial target identification

Verification:

Once the Verification phase is begun, targets are more likely to be alerted to suspicious activity. This phase serves to identify potential or known vulnerabilities that could be exploited by intruders. This is the main analysis phase that correlates the information gathered in the first two stages. Methods of performing this phase can include:

- Vulnerability scanning
- Port scanning
- Alternate route & backdoors identification
- Identify exploitation targets

Exploitation:

The exploitation phase is typically only used when a client needs to demonstrate actual data or system compromises. This phase involves actually utilizing identified vulnerabilities to gain access to internal systems and networks. This phase typically utilizes many tools that may be available in the public domain and are used by actual intruders. This methods used during this phase are tightly controlled by the penetration agreement and activities; highest consideration is always paid to avoid damaging or disrupting any customer computing resource or information. All activities are extensively logged.

Detailed Descriptions

Reconnaissance Details:

1. Reconnaissance

   This phase involves the gathering of information about the client's network. Some attack methods may only apply to "insider" reviews. The methods employed include:

   - Going to the Company Web Site (Internet or Intranet), and collecting information, such as location, phone number, systems employed, configuration information, etc.
   - Performing Domain Name Server (DNS) lookups, or contacting InterNIC directly to obtain a list of IP addresses for the client, and possibly to gain information about the client's ISP.
   - Using traceroute to help determine the structure and layout of the network.
   - Using nslookup to identify authoritative and secondary DNS servers and to identify IP addresses between which zone transfers occur.
   - Using traceroute to help determine the structure of the network.
   - Social Engineering to gain information about the organization of the client, key personnel, important individuals (when in scope).
   - Looking through public information about the company, annual reports, press releases, etc. (when in scope).
   - "Dumpster Diving," gathering information by going through the client's garbage (when in scope).
   - Using access to company directories and organizational charts to discover names, titles, and positions of employees for future exploit.
   - Newsgroup reviews. Go to the major newsgroup archives and look for posting by client employees, or about client networks, products, etc.
   - Using ping or another form of network scanning to detect those machines that are on the Internet and available from a given location and performing host fingerprinting.
   - Operating System fingerprinting to help determine what OS a machine in the target network is running.
   - Simple Network Management Protocol (SNMP) scanning to determine the machines that are running SNMP and if they have a strong or easily-guessed SNMP password.
   - Wireless Testing, used to determine if Wireless LANs are vulnerable to attack (when in scope).
   - War Dialing to determine if the client has modems listening on phone lines that may allow access to the network (when in scope).
   - War Driving and similar methods to find unsecured or rogue access points (when in scope).
   - Wireless Threat Assessments and similar methods. Used to find unsecured or rogue wireless access points.
   - Initial target identification.

Verification Details:

2. Service Availability

   This phase involves the service level information about the client. The methods employed include:

   - Port Scanning, to gain a list of those services (Ports) that are available.

- Null Session connections and scanning (Windows Machines Only). This is used to determine the services available, lists of users, and other login information.
- Share Scanning to determine what shares machines have available.
- NetBIOS name and service scanning on Windows machines to determine services running.
- Utilize vulnerability testing tools (e.g.)[1]
  - Nessus
  - Nmap
  - SAINT
- Identify alternate routes & backdoors
- Identify exploitation targets for the next phase

Exploitation Details:

The exploitation phase is typically used only when a client needs tangible evidence of actual data or system compromises. This phase involved exploiting identified vulnerabilities to gain access to internal systems, services, and networks. This phase typically utilizes many tools available in the public domain and used by attackers in real-life settings. To provide a more complete test, Emagined Security penetration testers also use proprietary (commercial) tools. In performing the System / Service exploit attempts, authentication attacks, and attempts to gain control of systems and internal networks, the following methods may be performed:

3. Avoid Detection

   While avoiding detection is shown as its own phase, typically the testers will attempt to avoid detection during all phases of the penetration test. Activities testers may employ to avoid detection include:

   - Using "Stealth Scans" to avoid detection.
   - Deletion of System logs to eliminate a record of what was done on a machine.
   - Disabling of logging functions on a particular machine while testing activities occur (typically left on to ensure full data is archived).
   - "Selective" editing of log data to remove suspicious activity.
   - Creation of scripts that generate large amounts of log "noise" to fill up logs, cause logs to reset, or obscure suspicious entries in the logs.
   - Placement of hidden files/directories (possibly orphaned), backdoors, or Trojan Horse tools to hide the existence of files placed on the machine by the testers. (For example a "ls" command in Unix that does not show files located in a specific directory)

If any modification of client files (such as logs) is performed, it must be only with the client's express written permission. Ideally, a client representative such as a system or network administrator will also be present when any modifications of files (e.g., system configuration files) must be made in according with testing procedures.

4. Acquire a User Account

   This phase involves the acquisition of a working user account. The ultimate goal of any penetration test is to gain access to either root (in Unix systems), Domain Administrator in Windows systems, or Supervisor/Administrator in Novell NetWare systems. Using the information gained during the

[1] Emagined Security routinely reviews and updates tools based upon industry standards and new technology advancements.

reconnaissance phase, our pen testers' attacks are focused on machines running exploitable services. Methods we typically use include:

- Guessing passwords for accounts.
- Using automated password cracking tools to try large numbers of different potential passwords on a specific account.
- Using known exploits, including buffer overruns and format strings, to gain root/Administrator access.
- Using known exploits to gain access to the password file on a machine and then using "cracking" software to extract valid username and password combinations.
- Social Engineering to get users to reveal their username and password or other information canin order to facilitate a successful attack if the persons performing the test act as client employees or service providers.
- Shoulder surfing, or watching as other personnel login at their terminals.
- Harvesting passwords and encryption keys from the cache or memory pages of machines used in obtaining remote access to superuser accounts.
- Employing "sniffers" to watch traffic on the network and extract passwords and usernames. This also may include "hi-jacking" of telnet sessions. Techniques may also include capturing login information and replaying it later to login as that user.
- Tricking users to install Trojan horse software on their machines, enabling the testers to gain access later. (Loki, SubSeven, NetBus, Rootkit.Gen, Win32Beagle, and more)
- Installing Trojan horse software to capture keystrokes, passwords, or other information. (Keylogger, KeyCap, PassFilt.dll)
- Exploiting access granted to unauthenticated users (FTP, web browsing, registry) to gain access to sensitive files, such as the password file, or to expand existing access.
- Installation of an access point through some other means, such as creating new user accounts, placing back doors, or starting easily exploited services/ports.

5. Access Resource Over the Network

After a user account has been established on one machine, the testers then try to branch out and gain access to other information via the network. This can be as simple as stolen credentials to access Human Resource files (if the account belonged to an HR staff member). This phase of the test involves attempting to access sensitive data and information that the client wants to protect. This portion of the test should almost always have a client representative present to help ensure that testers are not blamed for accessing out of bounds material. Methods to perform this portion of the test include:

- Exploiting weak internal data access rules that allow regular user accounts to access what should be restricted data.
- Executing exploits available to users, such as registry exploits, installation of Trojan horses, etc.
- Using files found on one machine that may contain login or access information about other machines. (.rhosts, hosts, NIS maps, etc. on Unix and Linux machines.)
- After access is gained, the testers will typically create other methods for easy access. This may include creating new user accounts, placing back doors, or starting easily exploited services/ports.

6. Denial of Service (DoS)

This phase involves testing the network to see if it is susceptible to DoS attacks. Typically these attacks are used to deny service to either network resources or a particular machine. However, these attacks can be used as part of an effort to break in, especially if a trojan horse requiring a reboot of a machine has been installed. From a penetration test standpoint, the only testing for DoS attacks will

center on whether the machines/systems being tested are vulnerable. Unlike the other phases of the penetration test, we will notify the IS staff before launching these attacks, and only attacks for which a patch is available are launched. For example, the client who wants to know if systems are vulnerable to the Sockstress [2]attack on a Windows server would first apply the patch for the vulnerability. Emagined Security would then launch the attack to determine if the patch was successful in eliminating the exposure. DoS testing is typically done only during non-business hours. DoS testing should not be taken lightly, and should only be performed when the customer understands the risks and has individuals standing by during the test if a system, application, or the network becomes non-responsive.

7. Exploit Physical Access to Workstations/Servers

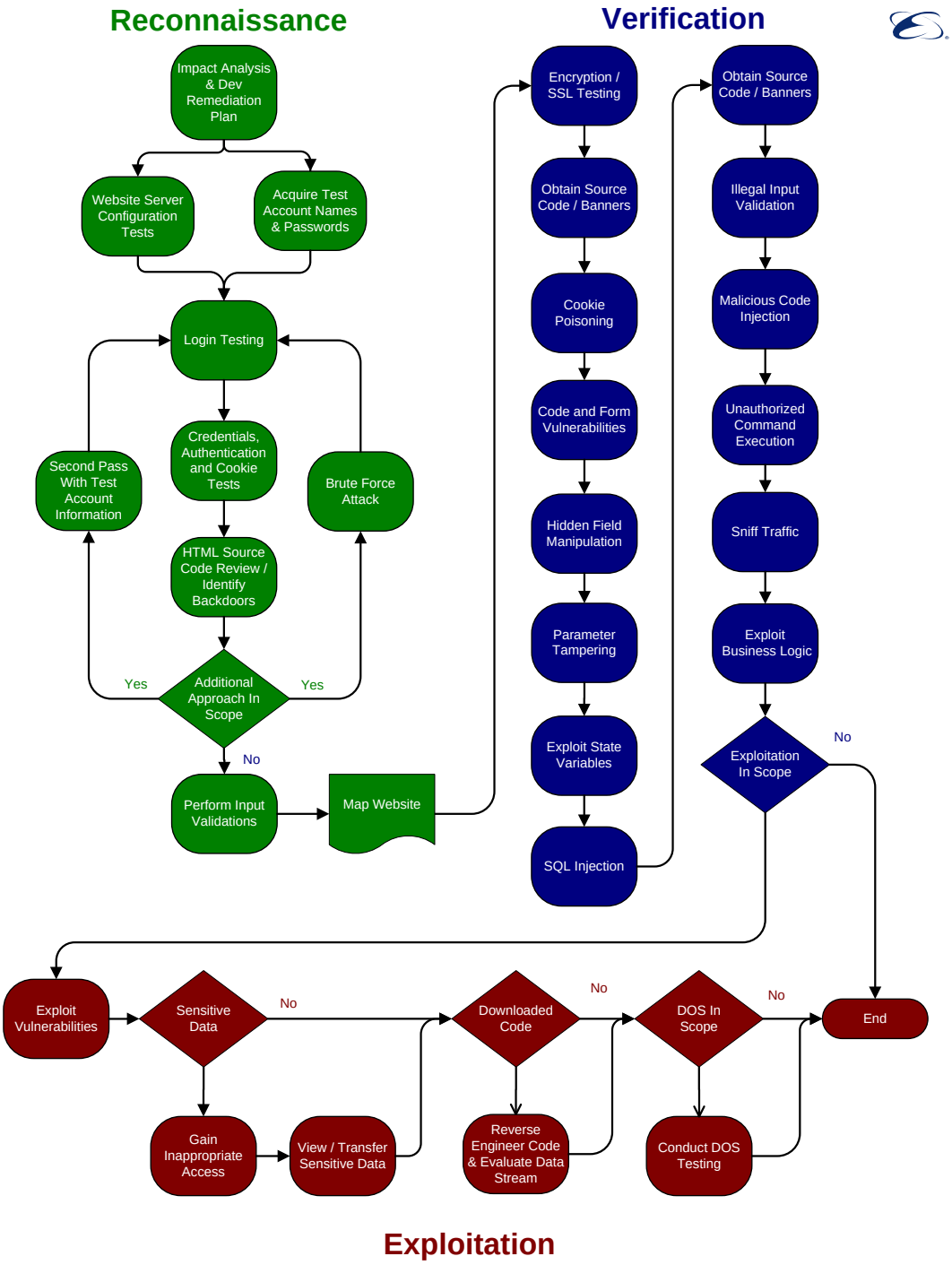
   This phase is for internal tests only and uses exploits for physical access to the network/network computers. Tactics include:

   - IP Spoofing to impersonate trusted machines.
   - Sniffing network traffic to get additional passwords for more powerful users.
   - Using boot disks to create accounts/change passwords for powerful accounts.
   - Removal of hard drives for exploit at other locations.
   - Removal of information in printouts by removing from premises.
   - USB boot-keys, key loggers and attempts to have employees connect to insecure systems to download/exploit login scenarios.

[2] In a Sockstress attack an attacker attempts to exploit a vulnerability in the TCP/IP stack of Windows systems by sending an extremely large number of specially crafted packets in which the TCP receive window size is very small.

Phases of the Web Application Penetration Test

Penetration tests typically follow a structured approach that may be modified slightly in response to data as it is collected.



High Level Descriptions

Reconnaissance:

The Web Application Ethical Hack begins with Reconnaissance that can be designed to evade detection. Emagined Security tests each application's security controls to determine if an attack may result in inappropriate viewing, altering, copying or deleting information. During Reconnaissance, Emagined Security performs the testing activities mimicking two types of users:

- The unauthorized user attempting to gain access
- As an authorized user trying to acquire and utilize enhanced or inappropriate privileges

In addition the following is tested:

- Brute force authentication techniques, if authorized
- Perform credentials, authentication and cookie testing
- Review source code and identify backdoors
- Perform input validations
- Map website

Verification:

The assessment then moves into Verification where the majority of website manipulation takes place. Through our automated and manual process, Emagined Security reviews for many security risks. Emagined Security reviews for these risks by first performing system identification. Once Emagined Security has determined the operating system, web server versions and other associated systems, Emagined Security is able to quickly identify well-known system vulnerabilities. Emagined Security attempts to identify security risks resulting from weaknesses such as:

- Weak or no encryption / SSL vulnerabilities
- Obtain unprotected source code
- Cookie Poisoning
- Code & Form Vulnerabilities
- Hidden Field Manipulation
- Parameter Tampering
- Exploit state variables
- SQL Injection Issues
- Source code / banners
- Input validation errors
- Malicious Code or Command Injection
- Sniffable traffic
- Executable code vulnerabilities such as buffer overflow conditions and IIS weaknesses
- Identification and exploitation of Business Logic

Exploitation:

Finally, the assessment escalates to Exploitation where Emagined Security attempts to fully compromise the pre-agreed to target(s) (e.g., web infrastructures). Before Emagined Security begins any security assessments, Emagined Security works with the specified website owner to determine the ground rules for vulnerability exploitation.

Within the realm of Exploitations, Emagined Security performs services based on the type of website:

- The basic service includes identifying and exploiting the implemented security controls or lack of controls
- For applications with sensitive data, we attempt to gain unauthorized access and transfer data between test accounts and/or perform other transactions without providing appropriate target authentication
- For web applications that use downloadable code, we attempt to identify vulnerabilities associated with installing and operating the executable
- Perform a DoS attack on the websites included in the agreed upon scope of testing

Detailed Descriptions

Reconnaissance:

1. Testing Preparation

   Emagined Security will start the project by assessing the impact of potential interruptions on the business's operations and business. Emagined Security will explain the ramifications of each identified potential interruption and inform the website owners of the processes necessary to reduce the risks from effects of conducting the testing. Emagined Security further performs scheduled and selective probes of the network's communication services, operating systems, key applications, and network equipment in search of those vulnerabilities. The following steps of the methodology will be completed:

   - Prepare Impact Analysis & Remediation Plan
   - Acquire Test Account Names & Passwords

   Emagined Security typically requires the following information prior to starting testing:

   - Network diagrams of the Internet Gateway Infrastructure
   - IP address of the firewalls, DNS servers, routers, hubs, load balancers, supporting systems, as well as other network devices
   - IP addresses of the associated internal systems
   - Available documentation describing system process flows

2. Website Mapping

   Emagined Security will test application security controls to determine if an attack may result in unauthorized viewing, altering, copying or deleting information. During Reconnaissance, Emagined Security will perform the testing activities mimicking two types of users:

   - Unauthorized user attempting to gain access
   - Authorized user trying to acquire and utilize enhanced or inappropriate privileges

   During this part of the test, Emagined Security will attempt to gain access as an authenticated user to information not associated with that user. Emagined Security will also attempt to elevate user levels to privileged accounts or to other individual's accounts. Emagined Security will attempt to login to the system as various users and swap sessions or transfer sessions to another user. Emagined Security will also assess what happens when a user attempts an unauthorized transaction and when timeouts occur. Emagined Security will also attempt to evaluate how error-handling processing takes place when a user tries an unauthorized transaction. Emagined Security will accomplish this by conducting the following tests:

   - Server and web server configuration updating and patching failures or weaknesses
   - Login exposures due to weak credentials (e.g., easy-to-guess passwords)
   - Credentials Authentication and Cookie Tests
   - An HTML Source/Application Code Review, looking for back doors or debug option weaknesses
   - Input validation including behavior to typical commands such as GET, POST, HEAD and PUT.

Examples of these tests include:

- Wherever there is a login prompt, Emagined Security will attempt to login using various names and passwords. Emagined Security will also attempt to guess usernames on well-known default and generic legacy accounts.
- Emagined Security will attempt to use "forgotten password" procedures, if they exist, to attempt to acquire information that could result in access.
- If there is a backend database, Emagined Security will attempt to acquire direct access, login and request information based on backend database passwords (especially well-known default passwords). Once Emagined Security has acquired access, Emagined Security will attempt to gain user information from the backend database.
- If in scope, Emagined Security will perform brute force username and password attacks.
- Emagined Security will search through html source code to attempt to identify hard coded names and passwords and identify backdoors that could be used to access backend database information without authorization. As described above, once we have gained access, we will attempt to acquire user information from the backend database.
- Perform input validation tests to identify issues with system client / server communication protection mechanisms.
- If within scope, Emagined Security will launch man-in-the-middle (MITM) attacks that could result in sniffing names and passwords if sessions are not SSL-protected.

During this phase, Emagined Security will also search through html source codes to attempt to identify hard coded information that could lead to identification of the associated web application scripts. Once Emagined Security has identified and acquired files with scripts, Emagined Security will attempt to analyze the business logic built in to Java, CGI, or PHP scripts used that would allow a user to exploit vulnerabilities in a web or database server. Emagined Security will also attempt to use any error checking or script documentation to our advantage in performing the assessment.

Verification:

3. Vulnerability Identification

The assessment then moves into Verification where the majority of website manipulation takes place. Through our automated and manual processes, Emagined Security will look thoroughly for a wide range of security risks. Emagined Security will try to identify these risks by first locating and identifying systems. Once Emagined Security has determined the type of operating system, version of web server, and other critical information concerning other systems, we are normally able to quickly discover well-known system vulnerabilities. Emagined Security will also assess security risk due to problems such as:

- Weak or no encryption / SSL vulnerabilities
- Obtain unprotected source code
- Cookie Poisoning
- Code & Form Vulnerabilities
- Hidden Field Manipulation
- Parameter Tampering
- Exploit state variables
- SQL Injection Issues
- Source code / banners
- Input validation errors
- Malicious Code or Command Injection
- Sniffable cleartext traffic

- Executable code vulnerabilities such as buffer overflow conditions and a variety of other web server bugs
- Exploitation of state information in URLs and cookies
- Identification and exploitation of Business Logic

Each part of this test has an associated, detailed methodology. For example, Emagined Security has a section entitled "Parameter Tampering." In this portion of our methodology we test the effectiveness of an application's error and exception handling capability. By using a smart proxy, Emagined Security can modify information after it has left the browser, but before it arrives at the server. This allows us to ensure that server-level validation is being performed and that the system does not entirely rely on client-side validation. For example, during this test, Emagined Security performs the following steps:

- Emagined Security also has the ability to compromise authorized users' systems and set up a proxy that harvests unencrypted information, even though both the user and the system appear to have an SSL session. This method requires physical access to users' systems and is typically out of scope.
- Verify that end users cannot send data to gain information from other persons, as in SQL injection attacks. Using this technique, Emagined Security may be able to run any SQL command on your database.
- Verify that vulnerabilities that allow unauthorized modification to data are identified and that access authorization is controlled by the system, not the end user.
- Review SQL transactions to ensure that data sent to the user is appropriate and that it does not include unnecessary data.
- Validate that each database sends proper responses based on rights and privileges assigned to each user.
- Identifying cross-site scripting vulnerabilities in which Emagined Security could use a script on a malicious web server to inject malicious code, steal cookies, and initiate other actions that could potentially compromise users' systems.
- If in scope, attempt to corrupt SQL queries in a way that causes a database to crash or reveal information that should not be accessible.

Exploitation:

4. Exploit Identified Vulnerabilities

   Before Emagined Security begins any security assessments, Emagined Security will work with the owner of each targeted website to determine appropriate ground rules for vulnerability exploitation. If Emagined Security identifies security vulnerabilities, Emagined Security will normally have two potential courses of action: 1) stop and report the potential existence of the vulnerability, or 2) fully exploit the vulnerability and determine the extent of potential compromise. Typically, if Emagined Security determines that the exploitation-related risk is high, Emagined Security will normally not attempt to exploit the vulnerability without advance, written approval from the system (or in other cases, data or application) owner. The owner should weigh the risks and benefits associated with the second option before giving approval to carry it out.

   During the basic service, if approved, Emagined Security will attempt to defeat or bypass implemented security controls or exploit any lack of controls. Please note that doing this corresponds to the Exploit Vulnerabilities phase of our penetration testing methodology.

5. Web Application with Sensitive Data Exploitation

For web applications with sensitive data, we will attempt to gain inappropriate access and transfer data between test accounts and/or perform other transactions without providing appropriate target authentication. This is conducted during these phases of the methodology:

- Gain Inappropriate Access
- View Sensitive Data
- Transfer Sensitive Data (e.g. Financial)

In addition, Emagined Security will attempt to view sensitive and private information from test accounts by bypassing normal security controls. We will perform all of this type of testing from this type of account.

6. Downloadable Code Exploitations

For web applications that use downloadable code, Emagined Security will attempt to identify vulnerabilities associated with the installation and operation of the executable. This is conducted during the following phases of the methodology:

- Evaluate Installation & Authentication Process
- Reverse Engineer Code
- Evaluate Data Stream

During this stage, Emagined Security will attempt to identify vulnerabilities associated with the installation and operation of the executable. Specifically, Emagined Security will attempt to perform the following tests:

- For manually installed applications or downloaded applets, Emagined Security will attempt to evaluate the installation procedures and evaluate system modifications.
- Once applications or applets are installed, application processes will be evaluated to determine if any potential vulnerabilities may have been introduced. In addition, Emagined Security will assess the installed software components and configuration files to identify potential modification points that could be used to circumvent security controls.
- For Java applications, Emagined Security will attempt to reverse engineer downloaded software components. Emagined Security will analyze the generated source code to identify potential ways that the code can be manipulated. If successful in modification attempts, Emagined Security will attempt to recompile the code and use it to communicate with the application.
- Emagined Security will attempt to identify hard-coded values in applications and manipulate them in an effort to gain additional privileges and / or modify transactions. Modifications to the Windows registry will also be identified in an attempt to manipulate them for the same purpose.
- Data passed between the client and the web application will be captured and analyzed to identify potential vulnerabilities. Emagined Security will then attempt to manipulate and resend information to evaluate security controls. As feasible, Emagined Security will also attempt to modify the communications in real-time.
- The strength of the authentication process will also be tested to determine whether or not it can withstand typical exploits. As available, logout and timeout functions will also be conducted. In addition, Emagined Security will attempt to bypass any authentication mechanisms used by each tested application.

7. DoS Testing

This phase involves testing the website/application/system to see if it is susceptible to DoS attacks. Typically these attacks are used to deny service to either system resources or a particular machine. However, these attacks can be used as part of an effort to break in, especially if a trojan horse requiring a reboot of a machine has been installed. From a penetration test standpoint, the only testing for DoS attacks will center on whether the websites/systems being tested are vulnerable. DoS testing is typically done only during non-business hours. DoS testing should not be taken lightly, and should only be performed when the customer understands the risks and has individuals standing by during the test if a system, application, or the network becomes non-responsive.

Differentiating Factors

Emagined Security provides value-added features within our service offerings that differentiate us from traditional penetration testing services offered by our competitors.

These value-added features are included in Emagined Security's normal Process and Methodology at no additional cost.

- **Manual Validation:** Emagined Security does not solely rely on automated tools to perform penetration testing and will never simply provide our clients with an automated test result as the sole deliverable. Emagined Security requires manual validation by expert penetration testers to ensure that findings are appropriate and accurate prior to delivery to our clients.
- **Tool Variation:** Emagined Security blends disparate primary tools to perform penetration testing, leveraging a combination of commercial off-the-shelf, open source and proprietary products. Testing is conducted with careful validation and vulnerability checks and balances ensuring results provided are never solely based on a single product's output. While our competition may simply run Nmap or Nessus and be done, we ensure our clients' receive optimal results by correlating output amongst utilities and performing robust tool verification.
- **Extensive Information Gathering:** As appropriate, when Emagined Security identifies applications or systems running on networks, we use internal databases and internet research to identify potential threats that standard tools do not attempt to exploit or identify. For example, if a web server is identified on high level ports (i.e. ephemeral), our team will not stop at simply cataloging the port and assigning a generic web server description. Instead, our testers will proactively research, enumerate and probe the port/service further, and identify or develop exploits for attack. Automated tools do not have the capability to perform this research and testing.
- **Report Enhancements:** In order to provide our customers with high quality reports, Emagined Security may use multiple screenshots of vulnerabilities and exploits to assist in communication of risk details. In contrast to "stock reports," the typical output of automated tools, Emagined Security's report enhancement provides significant benefits. Similarly, our reports are tailored-made for each client and specifically written to and about their environments; we do not provide the "assembly line" reports offered by the bigger firms.
- **Risk Grouping:** If desired, Emagined Security uses risk groupings to ensure that report findings are consolidated and provide actionable results. In addition, for multi-year engagements, Emagined Security provides qualitative data that shows where our clients have both success and challenge in their vulnerability and risk management programs. Trending and system issues are just some of the detail that Emagined Security tracks.
- **Vulnerability Table:** When requested, Emagined Security will create a vulnerability table that lists the identified vulnerabilities, risks and associated information to assist our clients in their remediation efforts. This table provides technical personnel with the

ability to quickly review, remediate and document the remediation efforts in an Excel spreadsheet. While other competitors offer similar information, Emagined Security's data is concise and contained within a single table for quick reference and ease of use.

- **Interim Risk Review:** If desired, Emagined Security provides our clients with an interim risk level review. This review allows clients to calculate appropriate risk levels for identified vulnerabilities taking the raw risk level, internal processes, compensating controls, cost of recommended countermeasures and business and risk mitigation measures into consideration.
- **Proactive Communications:** Emagined Security understands the need for proactive communication when performing penetration testing. With this in mind, Emagined Security recommends that periodic conference calls are held during the engagement as well as during the remediation phase afterwards to ensure all client personnel understand the identified vulnerabilities, risks and remediation requirements regarding all findings.
- **Certifications:** All work is completed by industry certified individuals located in the United States. No testing or data is off-shored. Each of our consultants holds multiple certifications that are some of the most highly-regarded and affluent in the field, including CISSP, OSCP, EnCE, CISA, CISM and more.

The following add-on services are available as extensions to Emagined Security's normal Process and Methodology. They may be contracted separately as needed.

- **Remediation Testing:** Emagined Security understands that our clients like to ensure they have successfully remedied vulnerabilities after they have been identified. Emagined Security can perform an agreed upon number of retests to validate that findings identified in the initial report have been successfully remediated. These retests do not include identifying new issues, whether incurred through remediation changes made to the environment or those occurring externally, or validating any new enhancements, content, or items not originally tested.
- **Remote Remediation Assistance:** Emagined Security regularly uses secure procedures to ensure that a testing machine is placed at the client's location and available upon completion of the initial testing period. This machine may be used by Emagined Security penetration testers to perform additional urgent validation at our client's request without coming onsite or incurring related travel costs and expenses.
- **Exploit Recording:** As contracted, Emagined Security can record live exploits. Exploit recordings are narrated and edited to allow our clients a better understanding of the vulnerability, the exploit and the potential danger. Note: exploit recordings may not be available for every type of vulnerability identified; this service is only performed in conjunction with penetration tests and where previously arranged.
- **Additional Deliverables:** Emagined Security can re-organize and provide multiple reports based on customer needs. Specifics of multiple reports will be agreed upon at the time of request. Any modifications thereafter may incur time and materials costs.
- **Strict Schedules:** In certain cases, Emagined Security understands that scheduling is critical. If needed, Emagined Security can break-up work to be performed outside normal business hours. This might include testing on certain days, nights, and weekends to work around any restricted times. Additionally, Emagined Security can group activities to minimize travel and increase time spent on-site. Any strict schedule considerations must be disclosed during contract negotiations, as they could affect the cost. Schedule considerations that require changes to normal business hours after contract negotiations have concluded will incur an additional 20% of total engagement cost, and will be honored at the sole discretion of Emagined Security.