The Association of Banks in Singapore

Penetration Testing Guidelines For the Financial Industry in Singapore

31 July 2015

TABLE OF CONTENT

1. Executive Summary

The security of online systems is paramount to maintaining trust and confidence in the online financial services provided by the Financial Institutions in Singapore to their customers.

This document is a set of guidelines for penetration testing to ascertain the effectiveness of the security controls put in place to preserve the confidentiality, integrity and availability of online systems.

The scope of this document is for penetration testing of online systems which are publicly accessible from the Internet.

Financial institutions have the option of adopting the methodology detailed in this guideline for non-Internet facing services within their own organisations.

2. Introduction

Audience

This document is intended to be read by Financial Institutions, members of The Association of Banks in Singapore, participating in the industry penetration testing, and their agents and contractors relevant to performing security assessments.

The Technology Risk Management Guidelines published by the Monetary Authority of Singapore may be read as a reference for the reader to understand the expectations set out by the regulator.

Purpose and Scope

This document provides the guidelines and requirements for penetration testing for Financial Institutions in Singapore

Definitions

i. FI refers to the financial institutions, members of the Association of Banks in Singapore, to which these guidelines are addressed.

ii. UAT (User Acceptance Test) environment or Pre-Production environment refers to a copy of the environment to be deployed in production once the implementation is complete.

iii. Production environment refers to the environment providing the service to customers (internal or external).

iv. Online System refers to a system with services which are publicly available to the Internet.

v. Online services refer to services (e.g. banking, trading, insurance) provided by FIs over Internet.

vi. Blackbox Testing refers to testing without any prior knowledge of the environment except for the IP address ranges and known URLs.

vii. Greybox testing in this document refers to testing with credentials. The security assessor is authenticated with the same rights as a normal customer.

viii. OWASP refers to the "Open Web Application Security Project" (owasp.org) that provides best security practice recommendations and maintains a list of Top 10 Web Application findings. (https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project).

ix. SANS refers to the "SysAdmin, Audit, Networking, and Security" Institute (sans.org) that provides best security practice recommendations and maintains a list of the Top 25 Most Dangerous Software Errors (http://www.sans.org/top25-software-errors/).

x. CVE refers to Common Vulnerability and Exposures. CVE is a dictionary of publicly known information security vulnerabilities and exposures. CVE's

common identifiers enable data exchange between security products and provide a baseline index point for evaluating coverage of tools and services.

xi. CVSS refers to Common Vulnerability Scoring System. CVSS provides a universal open and standardized method for rating IT vulnerabilities.

xii. CWE refers to Common Weakness Enumeration, a formal list or dictionary of common software weaknesses that can occur in software's architecture, design, code or implementation that can lead to exploitable security vulnerabilities.

xiii. Software weaknesses refers to flaws, faults, bugs, vulnerabilities, and other errors in software implementation, code, design, or architecture that if left unaddressed could result in systems and networks being vulnerable to attack. Example software weaknesses include: buffer overflows, format strings, etc.; structure and validity problems; common special element manipulations; channel and path errors; handler errors; user interface errors; pathname traversal and equivalence errors; authentication errors; resource management errors; insufficient verification of data; code evaluation and injection; and randomness and predictability.

xiv. Common Attack Pattern Enumeration and Classification (CAPEC) refers to the most common methods attackers use to exploit vulnerabilities resulting from CWEs. Used together, CWE and CAPEC provide understanding and guidance to software development personnel of all levels as to where and how their software is likely to be attacked, thereby equipping them with the information they need to help them build more secure software.

3. Requirements

Overview

i. Penetration testing provides a snapshot of the security posture or point-in-time security assessment of the FI's online services and Internet infrastructure.

ii. This chapter provides guidance for the following areas:

a. Test Scope
b. Test Environments
c. Test Methodology
d. Risk Rating
e. Reporting
f. Security Assessor Selection Criteria

iii. It is expected that requirements in this document be incorporated into the FI's penetrating testing methodology.

iv. Holistic approach
a. As an attacker is not limited to a set of defined activities, penetration testing should also adopt a holistic approach.
b. Network and application testing should be evaluated as a whole rather than separate activity. As an example, during the network discovery phase, an admin console (without known vulnerability) should be reported as it represents a weakness in design and should trigger an application test on that exposed service.

v. The application penetration test should cover the critical risks identified in OWASP Top Ten list for web application and mobile security as well as CWE Top 25 Most Dangerous Software Errors, but not limited to. CAPEC may also be referenced when assessing the types of attack patterns that would apply to the targeted system.

vi. Social engineering refers to the manipulation of people into performing actions or divulging confidential information, for the purpose of information gathering, fraud, or system access. Social-engineering identifies risks associated with end users' failure to follow policies and procedures, and should be scoped such that it is appropriate for the complexity of the FI, and the maturity of the FI's security awareness program. FIs can incorporate such test into its penetration testing exercise to determine the effectiveness of its security awareness program.

Test Scope

i. All online services and infrastructure that are Internet facing and within the FI direct control are in scope.

ii. All Internet services that are publicly accessible via the Internet and within the FI direct control are in scope.

iii. Greybox testing with user credentials will be restricted to only Business to Customer (B2C) services such as Online Banking Platform for Retail, Online Corporate Banking for Corporate customers, Online Trading for Securities, etc.

iv. For outsourced environment, outsourcing vendor should also conduct annual penetration testing for their public Internet facing network infrastructures. Outsource vendors are expected to follow the methodology as laid out in this document.

Test Environments

i. The assessment should be performed against the production environment. However should the nature of the test be intrusive or intensive and may result in the possibility of an outage, the specific test could be conducted against the UAT/Pre-Production environment.

ii. The mention of the environment in which the assessment is performed on should be clearly specified in the final report.

Penetration Test Methodology

i. Penetration testing should comprise the following:
   a. Network penetration testing; and
   b. Application penetration testing.

ii. Network Penetration Testing
   a. The purpose of Network Penetration Testing is the identification and assessment of weaknesses that may lead to vulnerabilities on host systems and network devices exploitable remotely from an external attacker's perspective.

   b. The Assessment should include:
      i. Network discovery; and
      ii. Network weakness / Vulnerability assessment.

iii. Network discovery should incorporate the following:
   a. Network mapping;
   b. Host Identification; and
   c. Service Enumeration.

   As part of the Network weakness/vulnerability assessment, unnecessary or unauthorised hosts and services should be identified.

iv. Application Penetration Testing

   a. The purpose of application penetration testing is the identification and assessment of weaknesses and vulnerabilities on online systems exploitable remotely from an external attacker's perspective. It refers to any service and application discovered in the previous section.

   b. Application penetration testing should comprise the following:
      i. Blackbox Testing for all identified services and applications found in the network discovery phase; and

ii. Greybox Testing for a specific set of applications defined above in the Test Scope section – URL will then be provided as well as users' credentials.

c. Native mobile applications may contain weaknesses or vulnerabilities in the communications channel, server side infrastructure and client software running on the mobile device. The following tests should apply:

- Files content (temporary, cached, configuration, databases, etc.) on the local file system
- Insecure file permissions
- Application authentication & authorization
- Error handling & session management
- Business logic testing
- Decompiling, analysing and modifying the installation package
- Client-side injections

Rooting or Jailbreaking the device may be necessary to achieve some test cases.

Weakness and Vulnerability Scoring

i. Common Vulnerability Scoring System (CVSS) is used within the industry for scoring of vulnerabilities and is often chosen for its simplicity. The severity of the findings should therefore follow the CVSSv2 or CVSSv3.

ii. Risk rating will be based on High, Medium and Low. Critical may be adopted when CVSSv3 becomes official.

iii. The following risk rating mapping to CVSS scoring is recommended for consistency:

Risk Rating	CVSSv2 Score	CVSSv3 Score
Critical	N/A	9.0-10
High	7.0-10.0	7.0-8.9
Medium	4.0-6.9	4.0-6.9
Low	0.0-3.9	0.0-3.9

iv. The tracking and the resolution of findings will follow FI's internal remediation procedures and timelines.

Reporting

i. The security assessor should provide a report to the FI providing a summary of the penetration testing.

ii. This report will be structured as follows:
   a. Executive Summary
   b. Project Scope
   c. Methodology
   d. Environment tested (UAT/Pre-Production, or Production)
   e. Findings Overview (number of open vulnerabilities – Critical, High, Medium, Low)

f. Findings Register (Reference, Severity, Title, Impact summary, Status – Open/Closed)
g. Individual findings

iii. Each individual finding should will be structured as follows:
a. Reference number
b. Severity
c. Title
d. CWE ID
e. CVSS Vector and Score
f. Scope (URL + Parameter or IP + Port)
g. Impact
h. Recommendation (with literature references when applicable)
i. Details of the finding with sufficient elements to reproduce the findings, supported by screenshots when available.

Remediation

i. The FI should formalise a remediation timeline based on risk appetite, the threat vectors and compensating controls.
ii. The risk assessment would need to take in consideration the sensitivity of the data residing in the systems and the location of the system.
iii. Compensating controls may be in place to reduce or remediate the vulnerability.

Security Assessor Selection Criteria

i. Although it is difficult to recommend security assessor skill set, below are some guidance that can be used to help the FIs in making their assessment:
a. Gain accreditation with recognised technical certification. Some recommended certification are:
- CREST Registered Penetration Tester, CREST Certified Web Application Tester, CREST Certified Infrastructure Tester from CREST
- OSCP, OSWP, OSCE, OSEE, OSWE from Offensive Security
- GMOB, GPEN, GXPN, GAWN and GWAPT from SANS Institute

Details given in the Reference Section
b. Good track record in Blackbox Penetration Testing and Greybox Testing for FIs.
c. The security assessor should also possess the required expertise, in network, system, application or mobile penetration test that is relevant to the scope of work. The number of engagements, scope of work as well as scale of penetration testing engagements performed previously by the security assessor may be used to gauge whether the security assessor has sufficient experience within the relevant penetration testing areas.
d. The assessor may be tested against a Vulnerability-Lab hands-on assessment, preferably performed on a new environment for each security assessor or during technical interviews with subjects matter experts within the FI.
e. The security assessor may demonstrate his/her knowledge by publishing publicly recognized security advisories or speaking in public during technical security conferences.

f. This listing above is in no way exhaustive and the subjects matter experts within the FI should exercise his/her judgment when selecting vendors.

ii. The choice of Security Assessor to conduct the penetration test is left to the FI. The FIs should consider incorporating the above guidance into their selection criteria.

iii. In the selection of the security assessor, the scope and methodology for the security assessment should meet the expectations of this guideline. The assessment should be performed by an independent party (e.g. 3rd party vendors, independent testers within the organisation).

iv. FIs should consider rotating security assessors to avoid complacency of the vendors and blind spots. For assessments performed by independent testers within the organisation, the FI should consider engaging 3rd party vendors periodically.

v. In engaging penetration testing service providers, FIs should obtain assurance of their policies and procedures on penetration testing engagement methodologies, reporting, and data handling, as well as employee background checks on security assessors to protect the interest of FIs. The assurance could be provided for through avenues such as reviews conducted by FIs and accreditations by qualified parties (eg. CREST).

References

i. OWASP Testing Guide
https://www.owasp.org/index.php/OWASP_Testing_Guide_v3_Table_of_Contents
https://www.owasp.org/index.php/OWASP_Testing_Project

ii. OWASP Top Ten
https://www.owasp.org/index.php/Top_10_2013-Top_10
https://www.owasp.org/index.php/OWASP_Mobile_Security_Project#tab=Top_Ten_Mobile_Risks

iii. CVSS
http://www.first.org/cvss/cvss-guide
http://www.first.org/cvss/v3/development

iv. NIST - Technical Guide to Information Security Testing and Assessment
http://csrc.nist.gov/publications/nistpubs/800-115/SP800-115.pdf

v. Open Source Security Testing Methodology Manual (OSSTMM)
http://www.isecom.org/research/osstmm.html

vi. PTES (Penetration Testing Execution Standard) Technical Guidelines
http://www.pentest-standard.org/index.php/PTES_Technical_Guidelines

vii. PCI Security Standards Council - Penetration Test Guidance
https://www.pcisecuritystandards.org/documents/Penetration_Testing_Guidance_March_2015.pdf

viii. MITRE – Making Security Measurable
http://measurablesecurity.mitre.org/

Common Vulnerabilities Enumeration (CVE)
Common Attack Patterns Enumeration and Classification (CAPEC)
Common Weakness Enumeration (CWE)
Common Weakness Scoring System (CWSS)
Including the CWE-Top25 (http://cwe.mitre.org/top25/)
Common Vulnerability Scoring System (CVSS)

Open Vulnerability and Assessment Language (OVAL)
Security Content Automation Protocol (SCAP)

Common Platform Enumeration (CPE)
Common Configuration Enumeration (CCE)

ix. Information Security Certifications by Offensive Security
http://www.offensive-security.com/information-security-certifications/
Offensive Security Certified Professional – OSCP
Offensive Security Wireless Professional – OSWP
Offensive Security Certified Expert – OSCE
Offensive Security Exploitation Expert – OSEE
Offensive Security Web Expert – OSWE

x. Information Security Certifications by SANS Institute
   http://pen-testing.sans.org/certification/
   http://www.sans.org/media/security-training/roadmap.pdf
   GIAC Mobile Device Security Analyst - GMOB
   GIAC Assessing and Auditing Wireless Networks - GAWN
   GIAC Web Application Penetration Tester - GWAPT
   GIAC Penetration Tester - GPEN
   GIAC Exploit Researcher and Advanced Penetration Tester – GXPN

xi. Penetration Testing Framework
   http://www.vulnerabilityassessment.co.uk/Penetration%20Test.html

xii. CREST Ethical Security Testers
   http://www.crest-approved.org/
   http://www.crest-approved.org/professional-examinations/registered-tester/index.html
   http://www.crest-approved.org/professional-examinations/certified-web-application-tester/index.html
   http://www.crest-approved.org/professional-examinations/certified-infrastructure-tester/index.html