渗透测试助力 PCI DSS 合规建设

atsec 信息安全 陈谨运 2011 年 7 月 5 日

关键词：PCI、渗透测试、支付卡行业、atsec 、安全评估、ASV 、授权扫描商

atsec(Beijing) information technology Co., Ltd

Room 119, Building 2, No.1, Street 7, Shangdi,

Haidian District, Beijing, P.R.China 10085
Tel +86-10-84834011
Fax +86-10-82890017

www.atsec-information-security.cn
www.atsec.com

渗透测试与 PCI DSS 的关系

PCI（Payment Card Industry）中文全称为：支付卡产业。在这个产业里存在一个标准组织，称为--支付卡行业安全标准委员会，英文简写为 PCI SSC（Payment Card Industry Security Standards Council）。PCI 安全标准委员会是由国际知名的五家支付品牌共同建立而成，他们是美国运通（American Express）、美国发现金融服务公司（Discover Financial Services）、JCB、全球万事达卡组织（MasterCard）及 Visa 国际组织。PCI SSC 一共维护了三个安全标准：PCI DSS（Payment Card Industry Data Security Standard 支付卡行业数据安全标准）、PCI PA-DSS（Payment Card Industry Payments Application Data Security Standard 支付卡行业支付应用数据安全标准）以及 PTS（PIN Transaction Security PIN 传输安全标准）。从下图可以很清楚的反应这三个标准之间的关系。

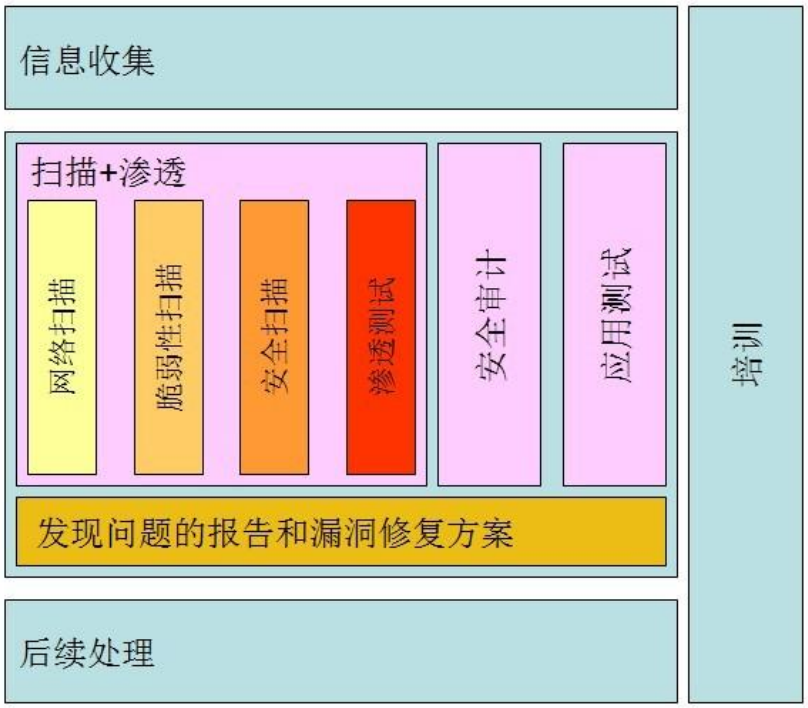
无论是 PTS 还是 PCI PA DSS，其最根本的目的是为了使最终的客户能够满足 PCI DSS 的要求。（关于 PTS 和 PA DSS 更多的介绍可参见 PCI 官方网站 *www.**pci**securitystandards.org* 和 atsec 官方网站 *www.atsec-information-security.cn*）。

在 PCI DSS 第 11.3 中有这样的要求“ Perform external and internal penetration testing at least once a year and after any significant infrastructure or application upgrade or modification (such as an operating system upgrade, a sub-network added to the environment, or a web server added to the environment). These penetration tests must include the following： Network-layer penetration tests and Application-layer penetration tests”其转译中文意思是：至少每年或者在基础架构或应用程序有任何重大升级或修改后（例如操作系统升级、环境中添加子网络或环境中添加网络服务器）都需要执行内部和外部基于应用层和网络层的渗透测试。

什么是渗透测试

渗透测试是通过模拟来自恶意的黑客或者骇客攻击，以评估计算机系统或者网络环境安全性的活动。从渗透测试的定义我们能够清楚的了解到渗透测试它是一项模拟的活动，主要的目的是进行安全性的评估，而不是摧毁或者破坏目标系统。

从下图我们可以看到，渗透测试与网络扫描，脆弱性扫描，安全扫描和安全审计其实并不相同。渗透测试是介于安全扫描和安全审计之间，它并不是纯粹的扫描工作，但是它执行的深度又没有安全审计那么深入。渗透测试是从攻击者的角度，试图通过各种技术手段或者社交手段去发现和挖掘系统的漏洞，最终达到获取系统最高权限的目的。无论是从测试的覆盖面和测试的深度来看，渗透测试都要比网络扫描，脆弱性扫描和安全扫描更为深入。



渗透测试的目的

对于渗透测试而言，除了满足某些特定标准（如 PCI DSS）的要求之外，渗透测试还会有如下的好处：

- 识别和发现机构可能被攻击的薄弱环节
- 通过外部独立的第三方评估机构的安全评估提高客户自身的安全级别和降低安全风险
- 提高人员对于信息安全的意识

渗透测试的方法论和业界参考实践

对于任何测试而言，都会相应的测试方法或者规则。在渗透测试领域，业界的渗透测试方法论或者最佳实践可以作为一个很好的参考，但是测试人员在测试过程当中更多的是依靠自身的能力和经验去完成测试工作，因为在测试过程当中可能会遇到各种各样的问题。下面是行业中被广泛接受的测试方法或者渗透测试的最佳实践：

OWASP（Open Web Application Security Project）Testing Guide -- 关注在 web 应用安全测试的测试指导。该测试指导涵盖了 web 应用程序大部分功能点的安全性测试，测试指导同时会给出一些测试的实例进行简单的说明。

OSSTMM（Open Source Security Testing Methodology Manual） -- 开放源代码安全测试方法手册。OSSTMM 是一个关注在安全测试和评价的方法论。OSSTMM 的测试用例分为五个方面：信息和数据控制；人员安全意识水平；欺诈和社会工程学控制水平；计算机和电信网络，无线设备，移动设备以及物理安全访问控制；安全流程，如建筑物，周边环境，以及军事基地的物理位置等安全流程。

Special Publication 800-115 Technical Guide to Information Security Testing and Assessment – 美国 NIST 发布的针对信息安全测试和评估的技术指导

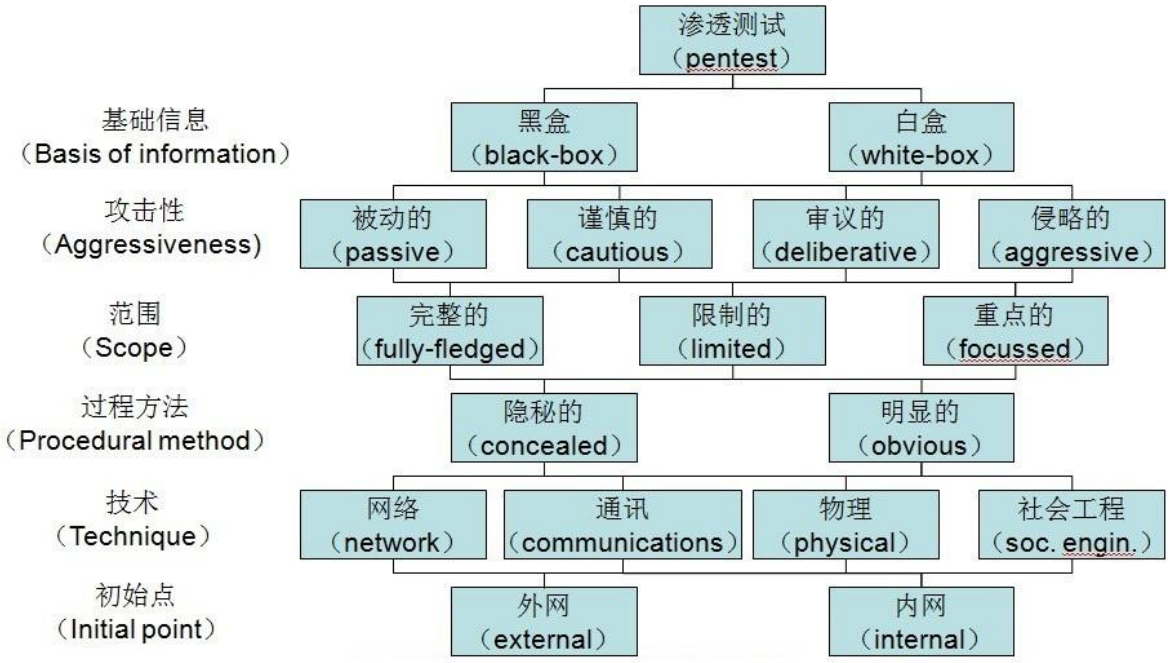
ISSAF（Information Systems Security Assessment Framework）-- 关注在信息系统安全评估的框架

Penetration Testing Framework -- 渗透测试的框架，该测试框架是渗透测试实践的操作总结，它非常详细的描述了渗透测试过程当中每一步应该做什么，怎么去做。该份测试的框架对于渗透测试的实际操作有着非常好的参考价值。

渗透测试的流程

对于渗透测试，其流程大体包括：测试协议和方法确定，免责条款签署，信息收集，脆弱性分析，对脆弱性进行渗透和利用，权限提升，最终评估和报告编写以及客户根据渗透测试发现问题的整改和追踪等环节。以下是对于上述各个环节的简要介绍：

- 渗透测试与恶意黑客的攻击最大的区别就是：恶意黑客为了获得想要的信息可以不计后果对目标系统进行攻击测试，而渗透测试人员的所执行的测试活动是需要在特定的测试协议下执行的。因此在正式执行渗透测试之前，明确测试协议与测试方法是最重要的工作，测试协议与测试方法是后续测试人员开展渗透测试的参照标准。对于渗透测试协议和方法的确定，下述图示展示了 atsec 结合了前文所提及的方法论和业界参考实践的经验总结。



- 在渗透测试中，根据客户提供信息的多少，我们可以人为的将渗透测试分为黑盒测试和白盒测试。所谓的黑盒测试是客户尽可能少的给测试人员提供测试目标的信息，测试人员在不了解目标系统的情况下展开测试。白盒测试是测试人员在完全了解系统的设计和架构或者网络配置的情况下对目标进行渗透，以确保所有安全问题都被发现了。
- 从测试人员测试活动的攻击性的角度评价，可以将渗透测试划分成四种情况：
  - 被动的测试活动，在此种情况下测试人员不会主动向目标系统发送攻击指令，测试人员通常会执行信息捕获的工作。
  - 谨慎的测试活动，在此种情况下测试人员通常会对目标系统执行嗅探工作并根据嗅探获得的漏洞进行分析和评估。
  - 审议的测试活动，在此种情况下测试人员通常会将发现的漏洞信息与客户进行讨论，以明确哪些漏洞在测试过程当中需要执行实际的漏洞验证和利用。
  - 具有侵略性的测试活动，在此种情况下测试人员通常会根据所发现的漏洞信息进行逐个验证，此时测试人员考虑更多的是如何最大限度获得目标系统的系统权限或者获得目标系统上存储的信息。
- 从测试范围的选择，客户可以指定整体网络环境的系统组件，或者是部分的网络环境的系统组件，又或者是对于特定的目标系统进行测试。
- 对于测试人员在测试过程当中的活动，客户可以要求测试人员隐秘的执行渗透测试活动，又或者明确测试人员并不需要隐藏测试活动可以公开执行渗透测试工作。
- 在渗透测试活动中，客户可以要求测试人员对如下方面执行渗透测试工作：对互联网络执行渗透（如互联网上的 web 服务器，数据库服务器，网络设备等等）；对通讯执行渗透测试（如 PSTN 网络，电信网络，3G 网络等方面）；对物理安全执行渗透测试（如目标系统的物理防护，电磁辐射等方面）；执行社会工程学测试（主要是为了测试员工的安全意识）。

- 在测试方法设定的时候，客户还可以要求测试人员以外网或者内网作为渗透测试活动的出发点。

- 在确定测试协议和方法之后，测试人员通常会要求客户出具一份渗透测试的免责声明，该声明中会明确声明测试人员不需要为测试过程中产生的任何风险承担法律责任。这份免责声明，对于渗透测试人员而言是很好的法律保护，因为任何的测试活动都不可能百分之百安全，在某些测试过程（如对漏洞进行渗透和利用）当中难免会存在一些安全风险，如果没有此份声明测试人员迫于法律的限制不可能完成后续的测试工作。

- 当完成上述两个准备阶段的工作之后，测试人员通常会进入非常重要和关键的一个环节----信息收集。在信息收集过程当中包括但不限于以下信息：IP 地址信息，关联域名信息，域名联系人信息，DNS 服务器信息，邮件服务器信息，IP 地址段路由信息，和目标系统相关的人员信息收集，目标系统漏洞信息，或者通过社会工程学从相关人员口中套取有用的信息等等。信息收集是一门比较高深的学科，如果信息收集得很好，很多时候都不需要使用技术手段对系统漏洞进行渗透利用都能获得系统的权限。

- 对于渗透测试而言，虽然它是一项通过模拟黑客或者骇客的攻击以评估系统或者网络环境安全性的活动，但是渗透测试比真实生活当中的攻击行为有着更多的限制。渗透测试并不以摧毁或者破坏系统的可用性为目的。在渗透测试过程当中，我们需要最大限度的保证客户业务的正常运转（当然客户的特殊要求除外），在这个前提下 尽最大可能发现和挖掘目标系统的脆弱性并进行利用。因此，在进行真正渗透之前，我们通常需要对发现的脆弱性进行分析，分析和评估该脆弱性可能会对目标系统造成的影响，并制定相应的应急预案。对于脆弱性的分析通常会借助外部的脆弱性扫描工具如 Nessus，QualysGuard，WebInspect 或者是 Nikto2 等等进行脆弱性的发现和识别，测试人员会根据所发现脆弱性的类型，CVE（Common Vulnerabilities and Exposures）依据 CVSS（Common Vulnerability Scoring System）对于脆弱性的评分，客户被测目标系统所处的实际环境等因素进行综合考虑以进一步对脆弱性进行分析。在 PCI DSS 第 11.2 中要求客户需要每个季度或者在基础架构或应用程序有任何重大升级或修改后（例如操作系统升级、环境中添加子网络或环境中添加网络服务器）都需要执行内部和外部脆弱性扫描。外部 脆弱性扫描是需要由 PCI SSC 授权的扫描服务提供商执行，业界的术语叫做 ASV（Approved Scanning Vendors）。目前 PCI DSS 对于外部脆弱性扫描活动不仅仅要求需要由 ASV 开展，对于实际执行脆弱性扫描的人员也需要经由 PCI SSC 进行培训，考核并获得相应资质证书之后才能出具具有资格的扫描报告。在渗透测试脆弱性分析的阶段，测试人员可以参考客户提供最近的 ASV 扫描报告作为脆弱性分析的输入数据。

- 在完成对脆弱性分析之后，测试人员会根据与客户之间的渗透测试方法和协议进一步对脆弱性进行渗透或者利用。在测试过程当中，渗透测试人员可能在初次攻击完成之后获得了有限的权限，此时渗透测试方法和协议则是测试人员最好的参考。如果客户允许执行进一步的权限提升操作，测试人员则可能会尝试将以获得的权限提升至管理员级别或者系统级别的权限。

- 在完成对脆弱性的渗透和利用之后，测试人员会对渗透的结果进行评估和判断，以确定脆弱性的可利用价值，同时渗透测试的过程以及测试过程中发现信息将会被编写到最终的渗透测试报告当中。对于在渗透测试过程当中，由于特定的原因（如客户的要求，漏洞利用条件的限制等等）导致脆弱性并没有被实际测试，测试人员将会在报告当中描述恶意人员可能对该脆弱性使用的攻击方法以及该脆弱性被成功利用后可能带来的安全风险。

- 客户根据渗透测试报告中所发现的脆弱性以及测试人员提供的解决方法进行脆弱性修复。对于完整的渗透测试流程通常还会包含对修复后的脆弱性进行验证测试，从第三方的角度去评估脆弱性修复的有效性。

基于应用层和网络层的渗透测试

对于 PCI DSS 第 11.3 中有要求至少每年或者在基础架构或应用程序有任何重大升级或修改后需要执行内部和外部基于应用层和网络层的渗透测试。何为应用层渗透测试？何为网络层渗透测试呢？应用层渗透测试指的是对 web 应用程序进行渗透测试，测试要求覆盖 OWASP Top 10（OWASP 项目组会周期性的根据 OWASP 联盟中应用开发和测试专家反馈的结果定期对 web 应用面临的安全问题进行统计和排名，Top 10 是 web 应用程序前 10 名影响最大的脆弱性）中的所有安全问题。对于网络层的渗透测试，通常是指对操作系统，网络设备等系统组件进行系统级别的渗透测试。

下图是 2007 年和 2010 年 OWASP Top 10 的排名对比。从图中可以看到 Top 10 的内容在这两年的评估当中出现了变化。所以在渗透测试过程当中我们除了参照 PCI DSS 的要求之外，还需要参照 OWASP 最新的关于 Top 10 的排名情况。

OWASP Top 10 – 2007 排名	OWASP Top 10 – 2010 排名
A2 – Injection Flaws	↑ A1 – Injection
A1 – Cross Site Scripting (XSS)	↓ A2 – Cross Site Scripting (XSS)
A7 – Broken Authentication and Session Management	↑ A3 – Broken Authentication and Session Management
A4 – Insecure Direct Object Reference	= A4 – Insecure Direct Object References
A5 – Cross Site Request Forgery (CSRF)	= A5 – Cross Site Request Forgery (CSRF)
<was T10 2004 A10 – Insecure Configuration Management>	+ A6 – Security Misconfiguration (NEW)
A8 – Insecure Cryptographic Storage	↑ A7 – Insecure Cryptographic Storage
A10 – Failure to Restrict URL Access	↑ A8 – Failure to Restrict URL Access
A9 – Insecure Communications	= A9 – Insufficient Transport Layer Protection
<not in T10 2007>	+ A10 – Unvalidated Redirects and Forwards (NEW)
A3 – Malicious File Execution	- <dropped from T10 2010>
A6 – Information Leakage and Improper Error Handling	- <dropped from T10 2010>

怎样选择合适的渗透测试合作机构

前面介绍了很多关于渗透测试介绍，以及测试流程和方法，然而我们在实际执行渗透测试工作的时候，应该如何选择合适的渗透测试实验室或者渗透测试人员进行测试工作呢？对于渗透测试人员的选择，PCI DSS 在第 11.3 的要求：测试人员可以是内部具有能力且独立的内部人员或者外部合格的第三方评测机构。对于内部人员的选择，技术能力的考虑和测试人员的独立性是最为重要的因素。对于第三方的评测机构的选择，除了技术水平的考虑，以下的参考因素能够为客户在渗透测试过程当中可能会面临的安全风险提供很好的安全保障。

- 专一性，IT 安全是否是该公司的主营的业务？
- 该公司自身是否切实执行 IT 安全流程？
- 评估机构和他们员工是否具有相关的资质？
- 该评估机构是否为行业的领导者，帮助或者能够分享相关的标准信息？
- 该机构是否具有相关的成功项目经验？
- 该评估机构是否能够提供除渗透测试以外其他能够提高客户流程等有价值的服务？
- 该评估机构是否能够在很多不同的技术领域提供专业知识和经验？
- 评估机构安全评测的独立性，是否能够为客户提供第三方独立的不带任何偏见的评估报告？
- 该评估机构是否为客户提供足够的保险和合理的法律协议保障？
- 谁是该评估机构的服务客户？

参考文档和链接

[1] PCI DSS https://www.pcisecuritystandards.org/security_standards/index.php

[2] OWASP Testing Guide https://www.owasp.org/index.php/OWASP_Testing_Project

[3] OSSTMM - ISECOM - Making Sense of Security www.isecom.org/osstmm/

[4] Special Publication 800-115 Technical Guide to Information Security Testing and Assessment
http://csrc.nist.gov/publications/nistpubs/800-115/SP800-115.pdf

[5] ISSAF（Information Systems Security Assessment Framework）www.oissg.org/issaf

[6] Penetration Testing Framework www.vulnerabilityassessment.co.uk/Penetration%20Test.html

[7] OWASP Top 10 OWASP_Top_10_-_2010 Presentation.pptx
http://owasptop10.googlecode.com/files/OWASP_Top_10_-_2010%20Presentation.pptx

[8] Nessus www.tenable.com/products/nessus

[9] QualysGuard www.qualys.com/products

[10] WebInspect https://www.fortify.com/products/web_inspect.html

[11] Nikto2 http://cirt.net/nikto2

[12] CVE http://cve.mitre.org/

[13] CVSS http://www.first.org/cvss/