浅谈 PCI DSS 标准要求的渗透测试

作者：张力

2020 年 5 月

关键词：渗透测试、弱点扫描、CDE、分段控制

atsec(Beijing) information technology Co., Ltd
Floor 3, Block C, Building 1, Boya C-Center,
Beijing University Science Park, Life Science Park
Changping District, Beijing, Postcode: 102206
P.R.China
Tel：+86-10-53056681
Fax：+86-10-53056678
www.atsec.cn

1 概述

根据支付卡产业数据安全标准 PCI DSS（PCI DSS: Payment Card Industry Data Security Standard）11.3 的要求：

11.3 外部和内部渗透测试每年至少执行一次，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）也应执行。此类渗透测试必须包括以下内容：

11.3.a 获取最近的渗透测试的结果并进行检查，以确定该渗透测试至少每年执行一次，而且在环境有任何重大变动后都会执行。确定发现的漏洞都已纠正并且执行重复测试。

11.3.b 确定执行测试的是具有相关资质的内部人员或外部第三方，如有可能，应确保测试方的机构独立性（不是必须为 QSA 或 ASV）。

本文基于 PCI DSS 中对渗透测试工作的要求，描述了针对 PCI DSS 标准的渗透测试范围、渗透测试内容、以及渗透测试方法等信息。

2 PCI DSS 渗透测试范围

渗透测试范围，如 PCI DSS 标准 11.3 章节中的定义，必须包含整个持卡人数据环境 CDE（Cardholder Data Environment）边界与影响 CDE 安全的关键系统，包括 CDE 的外部边界（面向公共攻击层面）与内部边界（局域网间攻击层面）。持卡人数据环境包括存储、处理或传输持卡人数据或敏感认证数据的人员、流程与技术，具体如下：

- 外部渗透测试范围是指暴露在 CDE 的外部边界和能连接或可访问公共网络架构的关键系统。应评估从公共网络访问到此范围的任意唯一访问，包括限制到独立外部 IP 可访问的服务。测试必须包括应用层与网络层的测试。
- 内部渗透测试范围是指从局域网分段范围外的视角方面考虑的 CDE 的内部边界。关键系统或影响 CDE 安全的其它系统也被包含在范围之内。测试必须包括应用层测试与网络层测试。
- 如果实现了分段控制以分离环境，应执行分段检查以验证非持卡人数据环境是按照预想的完全从 CDE 边界分隔出来。这种评估的目的是验证分段控制的有效性。
- 被考虑为 PCI DSS 范围外的系统组件必须从 CDE 中隔离出来，如果范围外系统组件被破坏，它不能影响 CDE 的安全。因而渗透测试可以包括不直接关系到处理、传送或存储持卡人数据的系统，以保证即使它们被破坏也不影响 CDE 的安全。

可能存在 CDE 边界外的影响 CDE 安全的附加系统，这些系统也被考虑为关键系统。通常关系到渗透测试的关键系统可能包括安全系统，比如，防火墙、IDS/IPS、认证服务器、电子商务重定向服务器等等，或由特权用户使用的用于支持与管理 CDE 的任何资产。

被测试机构负责定义 CDE 与任何重要的系统。建议被测试机构与测试人员、评估人员一起工作来验证没有组件被忽略，确定是否附加的系统需要被包含进测试范围内。

3 PCI DSS 渗透测试内容

PCI DSS 渗透测试包括网络层渗透测试、应用层渗透测试与分段控制渗透测试等内容。

3.1 网络层渗透测试

为了识别与挖掘网络、系统与设备的漏洞。模拟攻击者（测试人员）获得端系统的访问，包括发现用户认证凭证、管理特权提升、深度包检测绕过、尝试环境破坏等等。
测试人员使用自动化工具和手工测试的方法识别服务、软件版本、错误配置与漏洞。简单地运行自动化工具并不能满足渗透测试的要求，自动化工具仅能提供对环境潜在攻击的基线指示。渗透测试人员必须依据自动化工具的结果，判断是否所发现的漏洞存在误报，并进一步执行深入的测试。如果客户在测试前提供了 CDE 的网络拓扑图文档，测试人员应验证仅授权的服务暴露在 CDE 边界，测试人员应尝试从所有网段绕过认证控制，包括被授权访问 CDE 的网段和不被授权访问 CDE 的网段。

3.2 应用层渗透测试

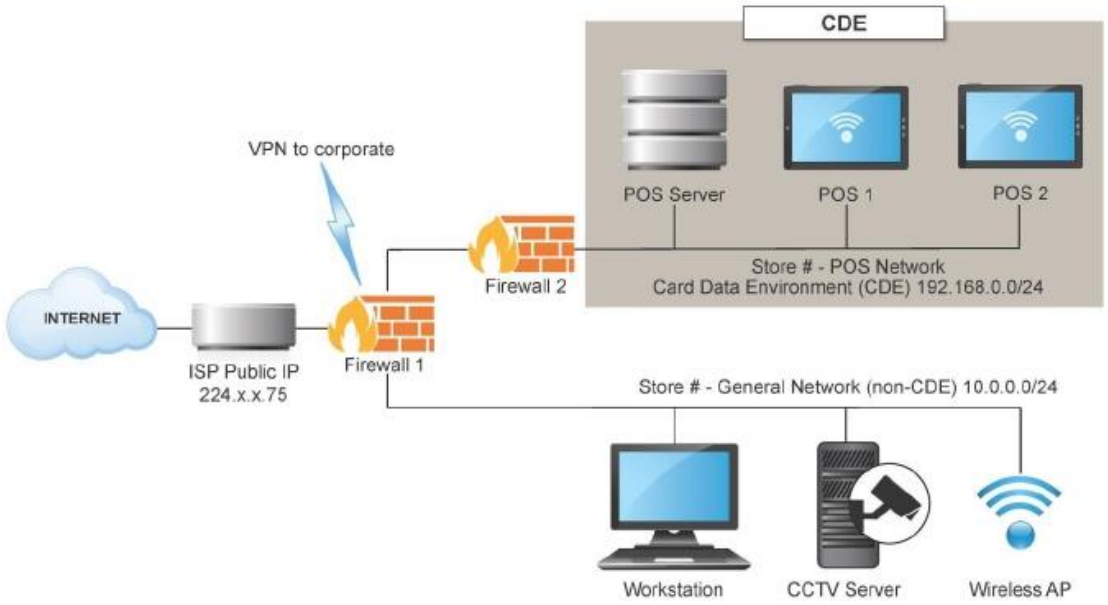
识别与挖掘 web 应用漏洞，主要考虑 OWASP 方法论，包括但不限于如下：

- 参数篡改；
- cookie 污染；
- 会话劫持；
- 用户特权提升；
- 后门与调试选项发现；
- web 与应用服务器错误配置；
- 输入验证绕过；
- SQL 注入；
- 跨站脚本等等。

渗透测试人员将从应用定义的角色方面执行测试。一般会鼓励被测试机构提供账号信息以进行深入的测试。测试人员能够通过测试确定是否可能通过给定的账号提升权限，从而获得超过这个账号本身所能获得的信息。

3.3 分段控制渗透测试

针对实施了分段控制的被测试机构，通过渗透测试验证分段控制是有效的，隔离了所有范围外的系统。PCI DSS 标准 11.3.4 要求针对分段控制执行至少每年一次的渗透测试，如果是支付服务提供商，要求每半年执行一次渗透测试。在具有众多内部 LAN 分段的大型网络中，渗透人员不可能从每个独立的 LAN 分段进行专门测试，在这种情况下，为了验证分段控制的有效性需要制定计划检查实施的分段方法论，例如防火墙、VLAN ACL 规则等等。
下面是一个典型的店铺网络示意图：



包括两个网段:

- POS 网络 – 持卡人数据环境（CDE）
  - 2 POS 设备
  - 1 POS 服务器
- 店铺普通网络 （非 CDE）
  - 1 经理工作站
  - 1 CCTV 服务器

分段控制渗透测试要求：从商店一般网络（10.0.0.0/24）进入商店 POS 网络（192.168.0.0/24）没有任何端口和服务的访问。

4 PCI DSS 渗透测试方法

常见的渗透测试方法包括三种类型：黑盒测试、白盒测试与灰盒测试。

- 黑盒测试，客户不提供任何信息给测试人员；
- 白盒测试，客户会提供测试人员完整与详细的网络与应用细节，渗透测试范围内的任意组件的详细文档，包括详细的网络拓扑图、持卡人数据流图、以及已被从 CDE 中隔离以缩小范围的所有网段的列表等；
- 灰盒测试，客户会提供测试人员目标系统的部分细节。

渗透测试通常是白盒或灰盒测试，这两种类型测试比纯黑盒测试提供更为详细的测试和产生更为精确的结果，也可以帮助被测试机构发现更多的问题。

在渗透测试开始前，建议通知所有相关的人员所进行的测试类型，即内部、外部渗透测试，应用层或网络层渗透测试。并与相关人员同步怎样测试将会如何被执行、测试目标是什么。通过协商和沟通这些细节，可以避免 CDE 范围定义不适当或因为其它问题导致重新测试的风险。

5 PCI DSS 渗透测试的流程

对于 PCI DSS 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。

- 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。
- 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；
  - 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。
- 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被测试机构业务的正常运转（当然被测试机构的特殊要求除外），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，在进行真正渗透测试之前，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。
- 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。

6 渗透测试对 PCI DSS 合规建设的意义

如上所述，PCI DSS 渗透测试是针对 CDE、以及影响 CDE 的关键系统进行的渗透测试，一方面通过外部渗透测试防范黑客对 CDE 的攻击，另一方面通过内部渗透测试防范内部员工未经授权的访问系统、文件、日志和/或持卡人数据，确认 PCI DSS 所需的控制是否到位并有效促进 PCI DSS 的合规。渗透测试工作是审查并验证企业 PCI DSS 标准实施合规建设的有效技术手段。

7 参考文献

[1] Penetration Testing Guidance 1.1

[2] Payment Card Industry (PCI) Data Security Standard, version 3.2.1

[3] Payment Card Industry (PCI) Data Security Standard Approved Scanning Vendors Program Guide 3.1