**商业银行渗透测试方案**

**一、渗透****测试****背景**

　　银行是网络信息技术应用最密集、应用水平最高的行业之一，基于计算机网络的各类银行信息系统已经成为银行产品的开发推广、银行业务的展开、银行日常管理和决策的所依赖的关键组成部分。这种依赖性使得银行面临着由于网络信息系统本身所带来的银行信息技术风险。

　　银行信息技术风险的主要挑战来自于基础网络信息技术的复杂性和变化，其中面对**互联网**主要有以下几个方面风险：

　　基于网络的电子银行，需要有完善的安全体系架构；

　　面向Internet的银行业务面临着各种各样的互联网威胁；

　　远程移动用户接入和内部用户接入Internet，都可能引入不同类型的威胁源；

　　钓鱼网站对于银行网上业务和企业信誉的损害。

　　伴随银行业务的发展，原有的网上银行、门户网站等都进行了不同程度的功能更新和系统投产，同时，行内系统安全要求越来越高，可能受到的恶意攻击包括：信息篡改与重放、信息销毁、信息欺诈与抵赖、非授权访问、网络间谍、“黑客”入侵、病毒传播、特洛伊木马、蠕虫程序、逻辑炸弹等。这些攻击完全能造成信息系统瘫痪、重要信息流失。

**二、渗透测试的目标**

　　本项目通过渗透测试的方式，模拟黑客的攻击思路与技术手段，达到以下目标：

　　从攻击者角度，发现网银系统、信用卡网站、门户网站和中间业务等应用系统及网关入口设备存在的安全隐患；

　　检测对外提供服务的业务系统（如网银系统、信用卡网站、门户网站等）以及行内重要业务系统的威胁防御能力。

　　深度挖掘渗透测试范围内应用系统各个层面（应用层、网络层、系统层）的安全漏洞；

　　检验当前安全控制措施的有效性，针对发现的安全风险及时进行整改，增强系统自身防御能力，提升安全保障体系的整体健壮性。

**三、渗透测试原则与风险控制原则**

**遵循规范**

　　渗透测试通过可控的**安全测试**技术对限定范围内的应用系统进行渗透测试，同时结合以下业界著名的测试框架组合成最佳实践进行操作：

　　ISECOM制定的开源安全测试方法OSSTMM-v2.2

　　开放Web应用安全项目OWASP-v3

**风险控制**

　　渗透测试过程最大的风险在于测试过程中对业务产生影响，为此我们在实施渗透测试中采取以下措施来减小风险：

　　● 双方确认

　　进行每一阶段的渗透测试前，必须获得客户方的书面同意和授权。对于任何渗透测试的对象的变更和测试条件的变更也都必须获得双方的同意并达成一致意见，方可执行。

　　● 工具选择

　　为防止造成真正的攻击，在渗透性测试项目中，启明星辰会严格选择测试工具，杜绝因工具选择不当造成的将病毒和木马植入的情况发生。

　　● 时间选择

　　为减轻渗透性测试对用户网络和系统的影响，安排在不影响正常业务运作的时间段进行，具体时间主要限制双方协调和商定的时间范围内。

　　● 范围控制

　　启明星辰承诺不会对授权范围之外的网络设备、主机和系统进行漏洞检测、攻击测试，严格按照渗透测试范围内限定的应用系统进行测试。

　　● 策略选择

　　为防止渗透性测试造成用户网络和系统的服务中断，启明星辰在渗透性测试中不使用含有拒绝服务的测试策略，不使用未经许可的方式进行渗透测试。

　　● 操作过程审计

　　为保证测试过程可审计，启明星辰将在测试过程中开启测试工具的审计**日志**功能，阶段性测试目标测试结束后，会将审计日志提交用户，以便用户监控测试过程。

　　● 项目沟通

　　启明星辰建议：在项目实施过程中，除了确定不同阶段的测试人员以外，还要确定各阶段的客户方配合人员，建立双方直接沟通的渠道；项目实施过程中需要客户方人员同时在场配合**工作**，并保持及时、充分、合理的沟通。

　　● 系统备份和恢复措施

　　为避免实际渗透测试过程中可能会发生不可预知的风险，因此在渗透测试前相关管理人员应对系统或关键数据进行备份、确保相关的日志审计功能正常开启，一旦在出现问题时，可以及时的恢复运转。

**四、渗透测试工作内容与方法**

　　● 渗透测试方法

　　渗透测试完全模拟黑客的入侵思路与技术手段，黑客的攻击入侵需要利用目标网络的安全弱点，渗透测试也是同样的道理。以人工渗透为主，以攻击工具的使用为辅助，这样保证了整个渗透测试过程都在可以控制和调整的范围之内。

　　● 应用系统渗透测试方法

　　针对各应用系统的渗透测试方法包括以下方法但不局限于以下方法：

|  |  |
| --- | --- |
| 测试类型 | 测试描述 |
| 信息收集 | 信息收集是渗透攻击的前提，通过信息收集可以有针对性地制定模拟攻击测试计划，提高模拟攻击的成功率，同时可以有效的降低攻击测试对系统正常运行造成的不利影响。信息收集的方法包括端口扫描、操作系统指纹判别、应用判别、账号扫描、配置判别等。 |
| 端口扫描 | 通过对目标地址的TCP/UDP端口扫描，确定其所开放的服务的数量和类型，这是所有渗透测试的基础。通过端口扫描，可以基本确定一个系统的基本信息，结合安全工程师的经验可以确定其可能存在以及被利用的安全弱点，为进行深层次的渗透提供依据。 |
| 口令猜测 | 本阶段将对暴露在公网的所有登陆口进行口令猜解的测试，找出各个系统可能存在的弱口令或易被猜解的口令。猜解成功后将继续对系统进行渗透测试，挖掘嵌套在登录口背后的漏洞、寻找新的突破口以及可能泄漏的敏感信息，并评估相应的危害性。猜解的对象包括：WEB登录口、FTP端口、数据库端口、远程管理端口等。 |
| 远程溢出 | 这是当前出现的频率最高、威胁最严重，同时又是最容易实现的一种渗透方法，一个具有一般网络知识的入侵者就可以在很短的时间内利用现成的工具实现远程溢出攻击。对于在防火墙内的系统存在同样的风险，只要对跨接防火墙内外的一台主机攻击成功，那么通过这台主机对防火墙内的主机进行攻击就易如反掌。 |
| 本地溢出 | 本地溢出是指在拥有了一个普通用户的账号之后，通过一段特殊的指令代码获得管理员权限的方法。使用本地溢出的前提是首先要获得一个普通用户的密码。也就是说由于导致本地溢出的一个关键条件是设置不当的密码策略。多年的实践证明，在经过前期的口令猜测阶段获取的普通账号登录系统之后，对系统实施本地溢出攻击，就能获取不进行主动安全防御的系统的控制管理权限。 |
| 脚本测试 | 脚本测试专门针对Web服务器进行。根据最新的技术统计，脚本安全弱点为当前Web系统尤其存在动态内容的Web系统存在的主要比较严重的安全弱点之一。利用脚本相关弱点轻则可以获取系统其他目录的访问权限，重则将有可能取得系统的控制权限。因此对于含有动态页面的Web系统，脚本测试将是必不可少的一个环节。 |
| 权限获取 | 通过初步信息收集分析，存在两种可能性，一种是目标系统存在重大的安全弱点，测试可以直接控制目标系统；另一种是目标系统没有远程重大的安全弱点，但是可以获得普通用户权限，这时可以通过该普通用户权限进一步收集目标系统信息。接下来尽最大努力取得超级用户权限、收集目标主机资料信息，寻求本地权限提升的机会。这样不停的进行信息收集分析、权限提升的结果形成了整个的渗透测试过程。 |

　　● 网银客户端安全测试方法

　　针对网银客户端的的渗透测试方法包括以下方法但不局限于以下方法：

|  |  |
| --- | --- |
| 测试类型 | 测试描述 |
| 键盘钩子测试 | 钩子是Windows系统中非常重要的系统接口，用它可以截获并处理送给其他应用程序的消息，来完成普通应用程序难以实现的功能。在测试中主要利用Ring3钩子和Ring0钩子。其中Ring3钩子是本地系统钩子，它仅在指定的消息由一个单一线程处理时被调用；Ring0是全局钩子，它当指定的消息被任何应用程序在整个系统上所处理时被调用。本项测试主要检测网银客户端是否容易被键盘记录程序或盗号木马利用获取账户与口令信息。 |
| 客户端完整性测试 | 通过本项测试验证网银客户端的自身安全防护能力，主要为：反逆向调试和防篡改能力，通过各种逆向工程的测试方法检测网银客户端是否容易被恶意软件篡改，如植入假登录框等。 |
| 内存读取密码测试 | 通过本项测试验证网银客户端在运行期间的数据存取安全性，通过搜索内存与进程内容的方法验证敏感的账户信息是否以加密的方式进行临时存放，确保用户信息存放的安全性。 |
| 屏幕截图和屏幕录像测试 | 通过本项测试验证用户在使用账户/口令登录网银客户端过程中，是否可能屏幕捕获的恶意记录程序所利用。 |
| 截取发包测试 | 通过本项测试验证用户在使用账户/口令登录网银客户端过程以及操作与交易的过程中，数据包传输的安全性。通过网络层的捕获/截取等技术手段，记录登录与操作过程中产生的数据包，并分析数据包中的内容是否包含明文的用户身份信息或容易被反向猜解的身份信息，确保数据在传输过程中的安全性。 |

● 渗透测试流程

　　渗透测试流程严格依照下图执行，采用可控制的、非破坏性质的渗透测试，并在执行过程中把握好每一个步骤的信息输入/输出，控制好风险，确保对光大银行网络不造成破坏性的损害，保证渗透测试前后信息系统的可用性、可靠性保持一致。



　　图1渗透测试流程

　　● 渗透测试内容

　　通过可控的安全测试技术对限定范围内的应用系统进行渗透测试，同时结合业界著名的OSSTMM与OWASP测试框架组合成最佳实践进行操作。