

**亿讯安安全服务技术白皮书**

**渗透测试服务**

|  |
| --- |
| 目录 |
| [一. 概述 1](#_Toc3709529)[1.1 基本概念 1](#_Toc3709530)[1.2 渗透测试与脆弱性评估区别 1](#_Toc3709531)[1.3 渗透测试的必要性 1](#_Toc3709532)[1.4 客户收益 2](#_Toc3709533)[二. 服务的实施标准或原则 3](#_Toc3709534)[2.1 政策文件或标准 3](#_Toc3709535)[2.2 服务原则 4](#_Toc3709536)[三. 亿讯安渗透测试服务 6](#_Toc3709537)[3.1 服务范围 6](#_Toc3709538)[3.2 服务方式 6](#_Toc3709539)[3.2.1 内部测试和外部测试 6](#_Toc3709540)[3.2.2 黑盒测试和白盒测试 7](#_Toc3709541)[3.2.3 单次服务和年度服务 7](#_Toc3709542)[3.3 服务流程 7](#_Toc3709543)[3.4 服务特点 9](#_Toc3709544)[3.5 服务报告 10](#_Toc3709545)[3.6 服务注意事项 10](#_Toc3709546)[3.6.1 时间的控制 11](#_Toc3709547)[3.6.2 工具使用 11](#_Toc3709548)[3.6.3 技术手段 11](#_Toc3709549)[3.6.4 监控措施 11](#_Toc3709550)[3.6.5 目标对象的选择 11](#_Toc3709551)[3.6.6 操作记录 12](#_Toc3709552)[3.6.7 沟通 12](#_Toc3709553)[四. 渗透测试方法论 13](#_Toc3709554)[4.1 信息收集技术 13](#_Toc3709555)[4.1.1 系统和应用信息收集 13](#_Toc3709556)[4.1.2 站点信息收集 13](#_Toc3709557)[4.2 溢出攻击技术 13](#_Toc3709558)[4.3 口令猜解技术 14](#_Toc3709559)[4.4 WEB漏洞技术 14](#_Toc3709560)[4.4.1 跨站脚本 14](#_Toc3709561)[4.4.2 注入漏洞 15](#_Toc3709562)[4.4.3 参数错误 15](#_Toc3709563)[4.4.4 信息泄露 15](#_Toc3709564)[4.4.5 其他 16](#_Toc3709565)[五. 相关工具 17](#_Toc3709566)[5.1 信息收集工具 17](#_Toc3709567)[5.2 溢出及口令破解工具 17](#_Toc3709568)[5.3 WEB漏洞挖掘工具 17](#_Toc3709569) |

1. 概述
	1. 基本概念

渗透测试（Penetration Testing）是由具备高技能和高素质的安全服务人员发起、并模拟常见黑客所使用的攻击手段对目标系统进行模拟入侵。

渗透测试服务的目的在于充分挖掘和暴露系统的弱点，从而让管理人员了解其系统所面临的威胁。

渗透测试工作往往作为风险评估的一个重要环节，为风险评估提供重要的原始参考数据。

* 1. 渗透测试与脆弱性评估区别

渗透测试不同于脆弱性评估，而且在实施方式和方向上也与其有着很大的区别。

脆弱性评估是在已知系统上，对已知的弱点进行排查。渗透测试往往是“黑盒测试”，测试者模拟黑客，不但要在未知系统中发现弱点，而且还要验证部分高危险的弱点，甚至还会挖掘出一些未知的弱点。

* 1. 渗透测试的必要性

渗透测试是脆弱性评估的一种很好的补充。

同时，由于主持渗透测试的测试人员一般都具备丰富的安全经验和技能，所以其针对性比常见的脆弱性评估会更强、粒度也会更为细致。

另外，渗透测试的攻击路径及手段不同于常见的安全产品，所以它往往能暴露出一条甚至多条被人们所忽视的威胁路径，从而暴露整个系统或网络的威胁所在。

最重要的是，渗透测试最终的成功一般不是因为某一个系统的某个单一问题所直接引起的，而是由于一系列看似没有关联而且又不严重的缺陷组合而导致的。日常工作中，无论是进行怎么样的传统安全检查工作，对于没有相关经验和技能的管理人员都无法将这些缺陷进行如此的排列组合从而引发问题，但亿讯安的渗透测试人员却可以靠其丰富的经验和技能将它们进行串联并展示出来。

* 1. 客户收益

对于客户而言，渗透测试可以带来以下收益：

* 明确安全隐患点

渗透测试是一个从空间到面再到点的过程，测试人员模拟黑客的入侵，从外部整体切入最终落至某个威胁点并加以利用，最终对整个网络产生威胁，以此明确整体系统中的安全隐患点。

* 提高安全意识

如上所述，任何的隐患在渗透测试服务中都可能造成“千里之堤溃于蚁穴”的效果，因此渗透测试服务可有效督促管理人员杜绝任何一处小的缺陷，从而降低整体风险。

* 提高安全技能

在测试人员与用户的交互过程中，可提升用户的技能。另外，通过专业的渗透测试报告，也能为用户提供当前流行安全问题的参考。

1. 服务的实施标准或原则
	1. 政策文件或标准

亿讯安渗透测试服务将参考下列国内、国际与渗透测试有关的标准进行工作。

**国内可参考的标准、指南或规范**

* ISO/IEC 27001:2005信息技术-安全技术-信息系统规范与使用指南
* ISO/IEC 13335-1: 2004 信息技术-安全技术-信息技术安全管理指南
* ISO/IEC TR 15443-1: 2005 信息技术安全保障框架
* ISO/IEC PDTR 19791: 2004 信息技术 安全技术 运行系统安全评估
* GB/T 20984-2007信息安全技术 信息安全风险评估规范
* GB/T 19715.1-2005 信息技术-信息技术安全管理指南
* GB/T 19716-2005 信息技术-信息安全管理实用规则
* GB/T 18336-2001 信息技术-安全技术-信息技术安全性评估准则
* GB/T17859-1999 计算机信息系统安全保护等级划分准则
* GB/T 20984-2007信息安全技术 信息安全风险评估规范
* GB/T 20988-2007信息系统灾难恢复规范
* GB/Z 20986-2007信息安全事件分类分级指南
* 亿讯安渗透测试最佳实践
* 亿讯安安全服务工作规范、渗透测试实施规范
* ……

**国际可参考的标准、指南或规范**

* 信息系统审计标准（ISACA）G3 利用计算机辅助审计技术
* 信息系统审计标准（ISACA）G7 应有的职业谨慎
* 信息系统审计标准（ISACA）G9 不正当行为的审计考虑
* 信息系统审计标准（ISACA）G18 信息系统管理
* 信息系统审计标准（ISACA）G19 不正当及非法行为
* 信息系统审计标准（ISACA）G33 对网络使用的总体考虑
* CESG (CHECK) IT Health Check方法
* OWASP OWASP\_Testing\_Guide\_v3
* OWASP OWASP\_Development\_Guide\_2005
* OWASP OWASP\_Top\_10\_2010\_Chinese\_V1.0
* OSSTMM OSSTMM\_Web\_App\_Alpha
* Web应用安全委员会（WASC）WASC Threat Classification v2
* 亿讯安 Penetration Testing Guide v2
* ……
	1. 服务原则

亿讯安在提供渗透测试服务中，将遵循下列原则。

* 保密性原则

保密性原则是渗透测试服务中最重要的原则，它是鼓励客户实施渗透测试服务的心理基础，同时也是对客户隐私权的最大尊重。渗透测试的保密范围，包括实施过程的保密性和输出成果的保密性。对服务过程中获知的任何客户系统信息均属秘密信息，不得泄露给第三方单位或个人，不得利用这些信息进行任何侵害客户的行为；对服务的报告提交不得扩散给未经授权的第三方单位或个人。

* 标准性原则

亿讯安渗透测试服务将在国家法律、法规允许的范围内进行，特别是遵照并履行《中华人民共和国人民警察法》第六条第十二款、《全国人大常委会关于维护互联网安全的决定》、《刑法》第二百八十五条、第二百八十六条等相关规定等。

遵守国内、国际与渗透测试有关的标准进行工作。同时在道德方面，也会严格遵守业界普遍认同的《计算机道德10个戒律》、《信息安全职业道德规范》、以及《网络道德的基本原则》。

* 规范性原则

亿讯安渗透测试服务将按照亿讯安安全服务工作规范、亿讯安渗透测试实施规范进行严格落实。实施必须由专业的安全服务人员依照规范的操作流程进行，对操作过程和结果要有相应的记录，提供完整的服务报告。

* 可控性原则

可控性原则就是渗透测试服务中对被测试系统造成的可能的各种影响要能够控制得住，既要全面测试，又不能影响生产，服务的工具、方法和过程要在双方认可的范围之内，服务的过程中，避免出现被测试系统运行不稳定，影响生产运行的情况。

* 整体性原则

整体性原则是系统思维方法的一条基本原则。整体原则认为，世界上任何一个有机整体系统，不但内部各组成要素之间是相互联系的，而且系统与外部环境之间也是有机联系的。我们在处理与解决问题时，应当从整体出发，从分析整体内部各组成部分的关系以及整体与外部环境之间的关系入手，去揭示与掌握其整体性质。在原则指导下的渗透测试服务，强调以综合为基础，在综合的控制与指导下，分析发现的安全问题，对分析结果进行恰当的综合。

* 最小影响原则

渗透测试服务工作应尽可能小的影响被测试系统和网络的正常运行，不能对现有系统、网络的运行和业务的正常运行产生显著影响。

1. 亿讯安渗透测试服务
	1. 服务范围

亿讯安渗透测试服务的范围主要包括了操作系统、应用系统、WEB程序和网络设备。

**操作系统包括：**

Windows、发行版Linux、AIX、Solaris、FreeBSD等主流系统。

**应用系统包括：**

Oracle、MySQL、MSSQL、Sybase、DB2、Informix等主流数据库，Apache、IIS、Tomcat、Weblogic等主流WEB服务器，FTP、DNS等主流应用服务器。

**WEB程序包括：**

ASP、PHP、JSP、.NET、Perl、Python、Shell等语言编写的WEB程序。

**网络设备包括：**

常见厂商的路由器、交换机等设备。

* 1. 服务方式

目前，亿讯安的渗透测试服务根据测试的位置不同可以分为内部测试和外部测试；根据测试的方法不同分为黑盒测试和白盒测试两类；根据服务的周期不同分为单次服务和年度服务两种类型。

* + 1. 内部测试和外部测试

内部测试是指经过用户授权后，测试人员到达用户工作现场，根据用户的期望测试的目标直接接入到用户的办公网络甚至业务网络中。这种测试的好处就在于免去了测试人员从外部绕过防火墙、入侵保护等安全设备的工作。一般用于检测内部威胁源和路径。

外部测试与内部测试相反，测试人员无需到达客户现场，直接从互联网访问用户的某个接入到互联网的系统并进行测试即可。这种测试往往是应用于那些关注门户站点的用户，主要用于检测外部威胁源和路径。

* + 1. 黑盒测试和白盒测试

黑盒测试是指测试人员对除目标系统的IP或域名以外的信息一无所知的情况下对系统发起的测试工作，这种方式可以较好的模拟黑客行为，了解外部恶意用户可能对系统带来的威胁。

白盒测试则是指测试人员通过用户授权获取了部分信息的情况下进行的测试，如：目标系统的帐号、配置甚至源代码。这种情况用户模拟并检测内部的恶意用户可能为系统带来的威胁。

* + 1. 单次服务和年度服务

单次服务是指亿讯安一次性为客户的被测系统提供渗透测试服务，服务完成后提交测试报告并指导客户进行问题修复。单次服务仅能够就目前可能存在的各种安全问题展开测试，对于一些将来可能会暴露出来的安全问题无能为力。

年度服务是指亿讯安以一定的时长（可以是半年、年等）为单位向客户提供有限次数（每月/双月/季度/半年）的渗透测试服务，每次测试均会提供详细的渗透报告。年度服务能够持续跟进系统的安全情况，在服务期限内最大限度保证系统的安全。

* 1. 服务流程

亿讯安渗透测试服务主要分为四个阶段，包括测试前期准备阶段、测试阶段实施、复测阶段实施以及成果汇报阶段：

* 前期准备阶段

在实施渗透测试工作前，技术人员会和客户对渗透测试服务相关的技术细节进行详细沟通。由此确认渗透测试的方案，方案内容主要包括确认的渗透测试范围、最终对象、测试方式、测试要求的时间等内容。同时，客户签署渗透测试授权书。

* 测试阶段实施

在测试实施过程中，亿讯安测试人员首先使用自动化的安全扫描工具，完成初步的信息收集、服务判断、版本判断、补丁判断等工作。

然后由人工的方式对安全扫描的结果进行人工的确认和分析。并且根据收集的各类信息进行人工的进一步渗透测试深入。

结合自动化测试和人工测试两方的结果，测试人员需整理渗透测试服务的输出结果并编制渗透测试报告，最终提交客户和对报告内容进行沟通。

* 复测阶段实施

在经过第一次渗透测试报告提交和沟通后，等待客户针对渗透测试发现的问题整改或加固。经整改或加固后，测试人员进行回归测试，即二次复测。复测结束后提交给客户复测报告和对复测结果进行沟通。

* 成果汇报阶段

根据一次渗透测试和二次复测结果，整理渗透测试服务输出成果，最后汇报项目领导。



渗透测试服务流程

* 1. 服务特点
* 全程化服务，有效保证服务质量

亿讯安可以为客户提供约定期限内的全程化渗透测试服务。服务的过程不仅仅是帮助客户发现问题，也会为客户的问题修补提供专业的建议和指导，做到问题发现、修补、验证的全程跟踪，每一次服务都会在前一次的基础上寻找新的突破口，力求最大程度地保证测试目标的安全。

* 专家级解决方案，一切以解决问题为目标

亿讯安有着专业的安全服务团队，团队成员无论是在风险评估、安全加固、渗透测试，还是在代码审计等领域均有着丰富的经验，所有问题的解决方案均由团队成员根据多年经验总结而来，方案确实可行。

* 降低成本，节省投资

在亿讯安为客户打造的年度服务方案中，服务人员第一次测试的结果将会成为后续审计服务的参考依据，避免了单次服务中每次都会为某一特定问题所累，节省了测试时间，同时也降低了客户在每个阶段的投入。

* 1. 服务报告

在渗透测试实施工作完成后三个工作日内，渗透测试人员将出示一份渗透测试报告。

根据测试结果，亿讯安测试人员将针对每种威胁进行详细描述，描述内容至少包括了测试范围、过程、使用的技术手段以及获得的成果。

除此之外，亿讯安测试人员还将结合测试目标的具体威胁内容编写解决方案和相关的安全建议，为管理员的维护和修补工作提供参考。输出如下报告：

* 《XX系统渗透测试报告》
	1. 服务注意事项

为保障客户系统在渗透测试过程中稳定、安全的运转，我们将提供以下多种方式来进行风险规避。

* + 1. 时间的控制

从时间安排上，测试人员将将尽量避免在数据高峰时进行测试，以此来减小测试工作对被测试系统带来的压力。

另外，测试人员在每次测试前也将通过电话、邮件等方式告知相关人员，以防止测试过程中出现意外情况。

* + 1. 工具使用

在使用工具测试的过程中，测试人员会通过设置线程、插件数量等参数来减少其对系统的压力，同时还会去除任何可能对目标系统带来危害的插件，如：远程溢出攻击类插件、拒绝服务攻击类插件等等。

* + 1. 技术手段

亿讯安的渗透测试人员都具有丰富的经验和技能，在每一步测试前都会预估可能带来的后果，对于可能产生影响的测试（如：溢出攻击）将被记录并跳过，并在随后与客户协商决定是否进行测试及测试方法。

* + 1. 监控措施

针对每一系统进行测试前，测试人员都会告知被测试系统管理员，并且在测试过程中会随时关注目标系统的负荷等信息，一旦出现任何异常，将会停止测试。

* + 1. 目标对象的选择

为更大程度的避免风险的产生，渗透测试还经常选择对备份系统进行测试。因为备份系统与在线系统所安装的应用和承载的数据差异较小，而其稳定性要求又比在线系统低，因此，选择对备份系统进行测试也是规避风险的一种常见方式。

* + 1. 操作记录

测试人员会在测试过程中形成操作记录文档，以便出现意外后进行追溯。

* + 1. 沟通

测试过程中，确定测试人员和客户方配合人员的联系方式，便于及时沟通并解决工程中的难点。

1. 渗透测试方法论
	1. 信息收集技术

无论是恶意用户的攻击还是安全人员的渗透测试工作，信息采集都是非常必要的一步工作，只有做到了“知己知彼”，才有可能针对被测试目标的弱点进行深度的挖掘和测试工作。

* + 1. 系统和应用信息收集

通过对远程服务的所启动的服务进行扫描和手工提交等工作，根据其返回信息可以获取远程系统及应用的版本号等信息，对于存在弱点的应用还可以进一步挖掘更多的系统信息，例如：SMB、SNMP等。

* + 1. 站点信息收集

站点信息主要包括三个部分：WEB服务信息，数据库信息和站点结构。

通过上面所介绍的手段可获取WEB和数据库信息。而若想进一步获取站点结构，需要使用爬虫程序。目前，一般WEB扫描器都具备比较强大的爬虫功能，通过爬虫程序可以快速的遍历出站点结构，这对于后期的漏洞挖掘是必不可少的基础信息。

* 1. 溢出攻击技术

溢出是比较传统却又很常见的一种漏洞。

溢出攻击的测试过程中，测试人员将根据收集的信息以确认应用或系统的版本，从而判断在当前应用或系统上是否存在已知溢出漏洞和可利用的攻击程序，同时，测试人员会在攻击程序对系统的稳定运行不产生影响的前提下使用攻击程序发起溢出攻击。

* 1. 口令猜解技术

大部分常见的操作系统及应用均使用帐号/口令的认证方式，因此，在渗透测试过程中，对用户口令的猜解测试也是一个重要的工作环节，亿讯安在渗透测试过程中，根据系统的不同，至少可以进行以下服务或应用的口令测试：

* SMB/CIFS
* TELNET
* SSH
* FTP
* POP/SMTP/IMAP
* Terminal Service
* MySQL
* MSSQL
* Oracle
* HTTP
* HTTP Form
	1. WEB漏洞技术

WEB应用与操作系统不同，WEB应用可很容易的根据用户需求而进行编写，因此，大部分WEB应用并不具备“通用的漏洞”。因此，这就决定了渗透测试人员需具备一定的WEB漏洞挖掘能力，这样才能保证在面对陌生系统时进行有针对性的测试工作。

* + 1. 跨站脚本

跨站脚本（XSS，Cross Site Script），指服务端程序在接收用户提交信息时没有对信息进行必要的检查或编码而导致页面包含了可能对客户端造成伤害的脚本。跨站脚本直接对客户端浏览器产生影响，如：窃取敏感信息、下载恶意程序、钓鱼等，而由于跨站而形成的XSS Worm可能造成更大的威胁。

测试人员根据经验，在可能出现程序交互的位置插入自己构造的测试脚本进行提交，观察返回结果并判断插入的测试脚本是否生效，如不生效则结合返回结果对测试脚本进行进一步的修正，如此反复最终形成可利用的攻击脚本。

* + 1. 注入漏洞

注入漏洞中常见的为SQL注入（SQL Injection），SQL注入是指当服务端接受客户端信息时，未对客户端信息进行任何校验就将其送入数据库中进行查询操作，而恶意用户只需对客户端提交信息进行一定的构造，就可以导致数据执行一些危险操作。

类似的，注入漏洞还存在其他方式，如：LDAP注入、XPath注入、系统命令注入等。

测试人员在测试注入漏洞前，会先根据收集到的一些信息判断远程目标系统类型、编写程序脚本所使用的语言以及后台数据库类型等信息，然后结合交互查询过程中产生的信息提交测试脚本，以确认系统是否存在注入漏洞。

* + 1. 参数错误

参数错误与注入漏洞相似，但一般参数错误漏洞是直接作用在WEB程序本身，而不像注入漏洞那样作用于后台支撑的应用。

参数错误主要是指在程序接收客户端参数时（一般为GET和POST两种参数），对客户端提交参数未做过滤，而同时WEB脚本之间又不具备严格的访问控制，进而导致通过错误的参数直接浏览、修改甚至获得WEB Shell。

对于错误参数的测试，测试人员需对网站的整体结构有一定的了解，通过测试人员对站点结构的精确掌握，构造错误的参数便可能造成恶意修改站点数据。

* + 1. 信息泄露

信息泄露往往来自多个层面，而其中由于服务配置错误引起的信息泄露最为常见。

测试人员在测试信息泄露时，需收集应用服务器的信息，结合该信息测试人员可确认该应用上可能出现的错误配置，并通过各种手段针对每种可能的错误配置进行逐一排查。

除此之外，测试人员还会结合个人经验对站点的一些目录或文件进行猜解，例如：针对后台管理地址的猜解。

* + 1. 其他

除以上四种常见WEB漏洞外，还有很多可能造成WEB应用被入侵的问题。例如，最为常见的是口令易被猜解和用户之间存在越权访问，这些问题在漏洞挖掘过程中，测试人员都会根据现场情况并结合个人经验进行必要的测试工作。

1. 相关工具

本章节列出部分常见的渗透测试工具，但并不能完整包括真实环境下全部渗透测试工具。

* 1. 信息收集工具

信息收集工具

|  |  |
| --- | --- |
| **工具名称** | **官方地址** |
| **RSAS** | http://www.nsfocus.com |
| **Nmap** | http://nmap.org/ |
| **httprecon** | http://www.computec.ch/projekte/httprecon/ |
| **nikto** | http://cirt.net/nikto2 |
| **Wapiti** | http://sourceforge.net/projects/wapiti/ |
| **NC** | http://joncraton.org/files/nc111nt.zip |
| **oscanner** | http://www.cqure.net/wp/oscanner/ |

* 1. 溢出及口令破解工具

溢出及口令破解工具

|  |  |
| --- | --- |
| **工具名称** | **官方地址** |
| **Metasploit** | http://www.metasploit.com/ |
| **Hydra** | http://freeworld.thc.org/thc-hydra/ |

* 1. WEB漏洞挖掘工具

WEB漏洞挖掘工具

|  |  |
| --- | --- |
| **工具名称** | **官方地址** |
| **Absinthe** | http://0x90.org/ |
| **Fiddler** | http://www.fiddler2.com/fiddler2/ |
| **Perl** | http://www.perl.org/ |