渗透测试

用户使用指南

天翼云科技有限公司

目 录

1. 产品介绍

1.1. 产品定义

渗透测试是通过模拟恶意黑客的攻击方法，来评估计算机网络系统安全的一种评估方法。这个过程包括对系统的任何弱点、技术缺陷或漏洞的主动分析，这个分析是从一个攻击者可能存在的位置来进行的，并且从这个位置有条件主动利用安全漏洞，提前查找自身系统所存在的风险，避免风险给系统造成严重的影响。

渗透测试服务能够对目标网络、主机、数据库与应用系统的安全性做深入的探测，发现系统薄弱环节的过程。能够直观的让管理人员知道当前网络、主机、数据库与应用系统存在的安全弱点以及可能造成的影响，以便采取必要的防范措施。

1.2. 产品优势

专业的安全团队

安全服务团队拥有 CISP、CISSP、ISO27001、Security+等专业资质和多年积累的丰富项目经验。

可靠的实践能力

遵循国际国家规范，通过标准的服务流程、完善的项目管理、质量保障机制，提供可靠的安全服务。

可控的安全风险

根据客户实际情况，在评估开始前制定相应的应急预案，控制在评估过程中引发的风险，降低渗透测试带来的影响。

多种服务模式

多样化的服务价格体系可满足各种客户不同规模的服务需求。

1.3. 功能特性

应用系统渗透测试

对渗透目标提供的各种应用，如 Tomcat、ASP、NGINX、JSP、PHP 等组成的 WWW 应用进行渗透测试。

主机系统渗透测试

通过 Web 系统对 Windows、Linux 等操作系统本身进行渗透测试。

数据库系统渗透测试

通过 Web 系统对 MySQL、MS-SQL、Oracle、Access 等数据库应用系统进行渗透测试。

突出的安全风险检测能力

支持 cookies 注入漏洞，文件上传截断漏洞，URL 跳转漏洞，在线编辑器漏洞，网站身份验证过滤漏洞，PHP 远程代码执行漏洞，数据库暴库漏洞，网站路径漏洞，默认后台及弱口令漏洞，网站代码远程溢出漏洞，修改任意账号密码漏洞，程序功能上的逻辑漏洞，任意次数短信发送、任意手机号码或邮箱注册漏洞，后台或者 API 接口安全认证绕过漏洞等漏洞的检测。

Web 安全测试

支持 SQL 注入攻击、跨站脚本攻击（XSS）、跨站点伪造请求（CSRF）、服务器端请求伪造（SSRF）、任意文件上传、任意文件下载、任意目录遍历、信息泄露、CRLF 注入、命令/代码执行漏洞、URL 重定向、第三方组件安全、本地/远程文件、安全配置错误、不安全的加密存储、已存在的脚本木马等漏洞的检测。

业务逻辑安全测试

支持身份认证管理、验证码机制、业务数据篡改、业务流程乱序、业务接口恶意调用、用户账号枚举、用户密码枚举、用户弱口令、会话标志固定攻击、越权访问等业务逻辑的安全测试。

应用框架及中间件安全测试

支持 Webloigc 反序列化命令执行、Bash 远程解析命令执行漏洞、Websphere 反序列化命令执行、Jenkins 反序列命令执行、Jboss 反序列化命令执行、Struts2 远程命令执行、OPENSSL 心脏滴血漏洞、shiro 反序列化命令执行等漏洞的检测。

1.4. 应用场景

应用系统安全隐患

从攻击者的角度检验客户应用系统，检查初次安装、未经测试上线以及版本更新后的业务系统安全防护措施是否有效，各项安全管理措施是否得到贯彻落实。

安全风险认知

将客户应用系统潜在的安全风险以真实事件的方式凸现出来，提高相关人员对安全问题的认识。使对应用系统安全风险不了解的系统管理员、开发人员、维护人员以及应用人员，整体了解应用系统面临的安全风险。

事前主动防范

网络信息系统承担重要任务前应该多采取主动防止出现事故的安全措施，从技术上和管理上加强对网络安全和信息安全的重视，形成立体防护，由被动修补变成主动的防范，最终把出现事故的概率降到最低。

1.5. 术语解释

后门

攻击者为了对主机进行长期的控制，在机器上终止的一段程序或留下的一个“入口”。

WebShell

通过 Web 入侵后留下的后门工具，可以在受感染的 Web 服务器上创建一个命令执行环境，从而允许攻击者在受感染的服务器上执行各种操作。

Exp

即 Exploit，漏洞利用程序的简称。漏洞利用程序，简单讲就是一段可以发挥漏洞价值的程序，比如：目标存在一个 SQL 注入漏洞，然后被你知道了，然后你编写了一个程序，通过这个 SQL 注入漏洞，拿到了目标的权限，那么这个程序就是所谓的 Exp 了。当然，如果你没有使用这个漏洞，它就这么放着，那么这个漏洞，对你来说可以认为是没有价值的。

Payload

指攻击载荷，指成功 exploit 之后，真正在目标系统执行的代码或指令。

POC

即 Proof of Concept（概念验证），用于验证漏洞的存在代码。

0day

指尚未公开披露的漏洞，攻击者可以利用它来渗透系统。

1day

指已经被公开披露但未被厂商修补的漏洞，攻击者可以尝试利用它来渗透系统。

nday

指已经公开披露并且已经被厂商修补的漏洞。

提权

指攻击者通过利用漏洞或其他手段从低权限提权系统管理员权限。

2. 计费说明

2.1. 产品价格

渗透测试资费标准价格如下：

描述	规格	单价
小型	1 个应用系统 3 人/日	10,000 元/次
中型	<=5 个应用系统 12 人/日	40,000 元/次
大型	<=10 个应用系统 21 人/日	70,000 元/次

例如：

- 门户网站（仅包含信息展示页面）为一个应用系统，属于小型系统。
- 办公系统，包含邮箱系统、财务系统、工时系统，为三个应用系统，属于中型系统。
- 网银系统，包含门户网站、个人网银、企业网银、手机银行、微信银行、App 用户端，为六个应用系统，属于大型系统。

注意：

具体以各版本的订购页面和控制台展示为准。

2.2. 变更续订及退订

变更

渗透测试服务下单后不允许规格变更，如您有特殊情况需要处理，请您联系客户经理沟通。

续订

渗透测试服务为单次服务，如需再次使用，请重新购买。

退订

渗透测试服务不支持退订。

3. 快速入门

3.1. 购买流程

1. 在天翼云官网注册账户后，进入天翼云官网首页，在产品按钮中选择“安全及管理 > 安全服务 > 渗透测试”，进入渗透测试页面。

2. 点击渗透测试服务的“立即订购”，按需求填写购买即可。

3. 您可以选择小型、中型、大型三种规格。

4. 用户指南

4.1. 服务流程

渗透测试服务以人工服务为主，我们的渗透测试人员在取得您的授权后，将对目标系统进行全面的渗透测试工作，总体流程如下：

1. 客户订购与需求匹配的服务规格并下单付款。
2. 客户经理会与您取得联系，协助您完成《业务需求单》及《渗透测试授权书》的填写，您需要如实填写以下内容：
   - 域名备案信息比对，必须为真实、合法信息。
   - 被检测的 IP 主机信息。
   - 如您为天翼云托管用户，需要提供域名清单，解析后必须为天翼云主机 IP，才可提供渗透测试服务。
   - 您所提供的应用 URL 描述须写明功能是什么或用途是什么。
   - 业务接口人联系方式，您需提供一个具有对渗透测试方案及渗透测试过程中出现的问题有决定权的业务接口人联系人。
   - 如您有安全防护设备，应在渗透测试开始阶段将渗透测试所用的公网 IP 加入安全防护设备白名单，避免因渗透测试工作带来的告警。（如在渗透测试开始阶段客户未将渗透测试所用的公网 IP 加入安全防护设备白名单，由此产生的告警及对渗透测试结果的影响，我方不承担责任。）
   - 您需签订渗透测试授权书。
3. 我们会根据您提供的信息，与您进行沟通，编写渗透测试方案，并与您确认测试细节，双方确认无误后，将进入渗透测试环境，渗透测试工作主要包含如下步骤：
   - 明确目标：确定渗透测试的范围，如 IP、域名、内外网、整站或部分模块，确定规则，如能渗透到什么程度，是发现漏洞为止还是继续利用漏洞，确定需求，如 Web 应用的漏洞，业务逻辑漏洞，人员权限管理漏洞。
   - 信息收集：在信息收集阶段要尽量收集关于项目软件的各种信息，例如，对于一个 Web 应用程序，要收集脚本类型、服务器类型、数据库类型以及项目所用到的框架、开源软件等。
   - 漏洞探测：进行漏洞探测，包括手动和自动探测。
   - 漏洞验证：对探测出的漏洞进行验证，确定其真实存在。

- 信息分析：对收集到的信息进行分析，尝试利用漏洞获取数据。
- 利用漏洞获取数据：如果能够利用漏洞获取数据，则进行数据获取。
- 信息整理：对获取到的数据进行整理，方便后续分析。
- 形成报告：根据渗透测试的实际情况，形成详细、专业的报告。

4. 形成报告后，我们会将报告发送给您，您可以根据报告内容，发现系统漏洞，及时加固完善。

以上为渗透测试的基本服务流程，如您在服务过程中有任何问题，请您与客户经理联系并反馈，我们会尽快为您处理。

5. 常见问题

5.1. 服务类

5.1.1. 天翼云渗透测试有哪些优势?

- 业内领先的咨询顾问团队

  参考国际和国家规范，对系统进行科学有效的风险评估，顾问团队拥有 CISP、CISSP、ISO27001、 Security+等专业资质和多年丰富的项目经验。

- 运营商级别的实践能力

  技术顾问具备多年的信息系统安全评估和保障服务经验，具有丰富的网络和系统整改项目经验。

  通过科学、标准的服务流程，以及完善的项目管理和质量保障机制，提供全面可靠的安全服务。

5.1.2. 天翼云渗透测试有哪些规格?

不同企业建议根据实际情况分成三种规格：

- 小型应用系统，最多 1 个应用系统。
- 中型应用系统，最多 5 个应用系统。
- 大型应用系统，最多 10 个应用系统。

其他规格需要根据实际情况协商确定。

5.1.3. 天翼云渗透测试服务内容包括哪些?

- 身份认证测试

  检查是否满足安全设计要求中的身份认证要求，检查是否存在密码被破解、登录被回放、登录被绕过的缺陷，确保登录验证安全有效。

- 授权管理测试

  检查页面是否满足安全设计要求中的访问控制要求，检查用户在未授权的情况下是否成功办理需要授权的业务。

检查是否存在跨站请求伪造、路径遍历、授权绕过、会话重放等。

- 数据验证测试

  检查是否满足安全设计要求中输入验证的要求，确保应用系统正常显示业务办理信息。

  检查是否存在 SQL 注入、跨站脚本攻击、 XPATH 注入、SSI 注入、命令注入、缓冲区溢出、上传文件验证、未经验证的 URL 重定向。

- 可用性测试

  检查系统是否存在帐号锁定设计缺陷及应用拒绝服务缺陷。

- 配置管理测试

  检查存在中间件配置缺陷导致的应用系统漏洞。

  检查是否存在 SSL 漏洞、敏感信息泄露、默认文件和目录、基础结构配置管理、非必要文件检索、HTTP 请求方法滥用、目录索引

- 后门测试

  检查应用系统各页面是否存在后门程序。

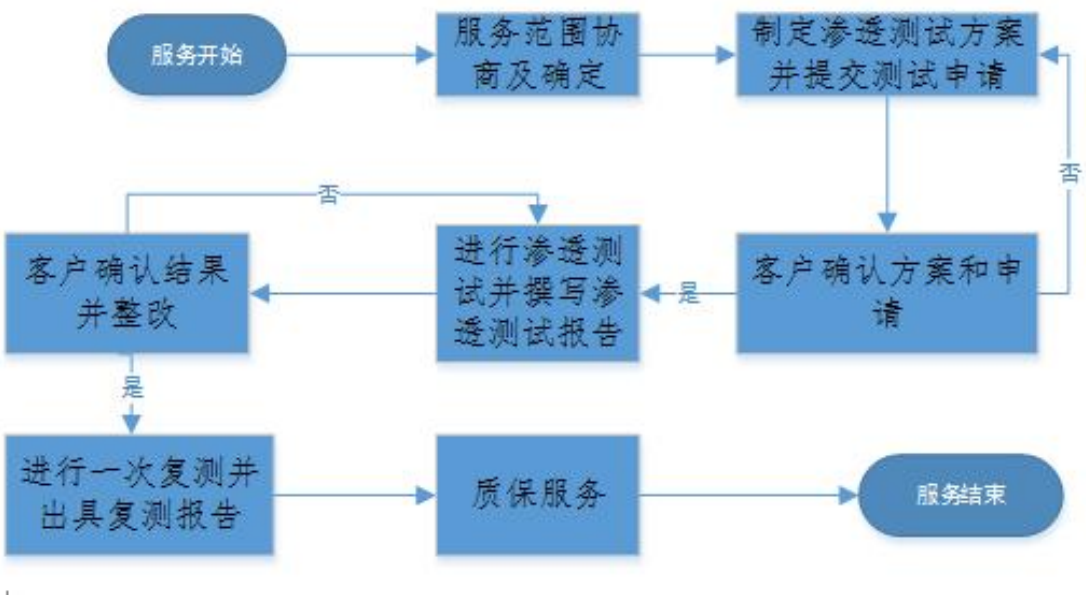
5.1.4. 天翼云安全渗透测试服务各阶段时间安排?

- 客户确认阶段：第 1 周，预计一周时间供双方协商测试方案。
- 进行测试阶段：第 2-3 周，预计两周时间。
- 整改复测阶段：提交测试报告后 1 个月内客户可以提交复测申请，复测在 1 周内完成。
- 质保服务阶段：从报告交付日开始，为期 12 个月。

5.1.5. 天翼云安全渗透测试服务网络要求？

应用系统网络与扫描器网络可达即可提供渗透测试。Internet 默认可达，内网地址需部署扫描器在内网即可。

5.1.6. 天翼云安全渗透测试服务流程是怎样的?



5.1.7. 渗透测试是不是相当于入侵系统？

渗透测试和黑客入侵最大区别在于渗透测试是经过客户授权，采用可控制、非破坏性的方法和手段发现目标和网络设备中的弱点，帮助管理者知道自己网络所面临的问题。

渗透测试是一种对抗性和定制化要求都非常高的一类安全测试，安全工程师在书面授权后尽可能完整的模拟黑客可能使用的漏洞发现技术与攻击技术（与黑客攻击相比其结果是可预知性的），对目标网络、主机、数据库与应用系统的安全性做深入的探测，发现系统薄弱环节的过程。能够直观的让管理人员知道当前网络、主机、数据库与应用系统存在的安全弱点以及可能造成的影响，以便采取必要的防范措施。

5.1.8. 渗透测试是否会对业务系统的运行产生影响？

渗透测试是模拟黑客攻击，对目标系统进行安全探测，以发现系统最脆弱的环节。在实施渗透测试时，可能会对业务系统的正常运行产生一定的影响。

具体影响的大小取决于渗透测试的具体实施方式和实施范围。如果渗透测试的范围较小，只针对部分系统或特定服务进行测试，对业务系统整体运行的影响可能较小。但如果渗透测试的范围较大，涉及到整个业务系统或关键业务组件，就可能对系统的正常运行产生较大的影响。

另外，渗透测试的时机也会影响其对业务系统运行的影响。如果选择在业务系统的非高峰期进行测试，可以最大程度地减少对业务系统正常运行的影响。但如果测试时间安排在业务高峰期，就可能对业务系统的正常运行产生较大的影响。

因此，在进行渗透测试时，需要综合考虑测试范围、实施方式、时机等多个因素，以尽可能地减少对业务系统正常运行的影响。同时，为了确保渗透测试的准确性和有效性，还需要选择专业的渗透测试团队或机构进行测试。

天翼云渗透测试服务在开始服务前，会为您提供详细渗透测试方案，在时间安排上，我们会将测试时间安排在非高峰期，不会对业务系统的连续性产生影响。

5.1.9. 天翼云渗透测试支持对哪些系统测试？

天翼云渗透测试服务通过真实模拟攻击使用的工具、分析方法来对业务系统进行深度漏洞挖掘，利用系统漏洞获取权限从而获取敏感数据的测试，由测试人员进行深入的手工测试和分析，识别工具无法发现的问题。

主要分析测试内容包括但不限于逻辑缺陷、上传绕过、输入输出校验绕过、数据篡改、功能绕过、异常错误等以及其他专项内容测试与分析。

测试范围：Web 系统、移动应用 APP、公众号、小程序等。

5.1.10. 渗透测试如何识别一个应用系统？

以一个三级域名作为一个应用系统的唯一标识，多个三级域名将被视为多个应用系统。

如 www.ctyun.cn 为一个应用系统，www.ctyun.cn/+路径也为同一个应用系统；反之不同三级域名为不同的应用系统，如 www.ctyun.cn 与 desk.ctyun.cn 为 2 个不同的应用系统。

5.1.11. 渗透测试是否只针对天翼云的租户，异网客户是否可以购买开通？

云上租户，异网客户均可购买使用，前提条件需要有天翼云账号，能正常购买渗透测试产品，且保证需要测试的域名公网可访问。

服务开始前，您需要提供渗透测试授权函，我们会为您提供详细的渗透测试方案，确定服务细节及测试范围，得到您的授权后，开展渗透测试服务，并提供渗透测试报告。

5.2. 计费类

5.2.1. 渗透测试支持哪些计费模式？

描述	规格	单价
小型	1 个应用系统 3 人/日	10,000 元/次
中型	<=5 个应用系统 12 人/日	40,000 元/次
大型	<=10 个应用系统 21 人/日	70,000 元/次

5.2.2. 如何购买渗透测试服务？

客户在天翼云官网注册账户后，点击“产品”，搜索“渗透测试”，点击“立即订购”，按自己需求购买即可。

5.2.3. 渗透测试规格可以变更吗？

渗透测试下单后不允许变更规格。

5.3. 操作类

5.3.1. 购买天翼云渗透测试业务后如何填写受理单内容？

客户应如实填写以下信息：

- 被检测的 IP 主机信息。
- 域名备案信息比对，必须为客户本人真实、合法信息。
- 客户为天翼云托管用户，用户提供域名清单，解析后必须为天翼云主机 IP，才可提供渗透测试服务。
- 客户提供的应用 URL 描述须写明功能是什么或用途是什么。
- 业务接口人联系方式，客户需提供一个具有对渗透测试方案及渗透测试过程中出现的问题有决定权的业务接口人联系人。
- 客户如有安全防护设备，应在渗透测试开始阶段将渗透测试所用的公网 IP 加入安全防护设备白名单，避免因渗透测试工作带来的告警。（如在渗透测试开始阶段客户未将渗透测试所用的公网 IP 加入安全防护设备白名单，由此产生的告警及对渗透测试结果的影响，乙方不承担任何责任。）
- 客户需签订渗透测试授权书。