天翼云 • 渗透测试服务
用户使用指南

中国电信股份有限公司云计算分公司

目录

1 产品概述

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。

注：天翼云渗透测试服务基于传统的 B/S 结构，暂不支持对 APP 类的应用渗透测试。

渗透测试进行到何种程度需和客户沟通，证明存在漏洞，还是需要利用漏洞。

1.2 服务特点

1.专业团队

渗透测试团队人员具有多年丰富的项目经验，可将漏洞评级与业务层面相结合，展示客户真实存在的业务风险。

2.安全保密

渗透测试团队人员均可签署用户保密协议，不公开任何关于客户漏洞的相关情况，使客户的漏洞隐私的到保障。

3. 遵守 owasp 道德准则

https://www.owasp.org/index.php/About_The_Open_Web_Application_Security_Project#Code_of_Ethics

渗透测试团队人员遵守以下道德准则：

1) 根据所有适用法律和最高道德准则，履行所有专业活动和职责；

2) 贯彻执行应用安全法规标准、程序与控制；

3) 在专业活动过程中，对专有或其他敏感信息进行保密；

4) 勤勉尽责地履行职业责任；

5) 开诚布公与沟通；

6) 避免任何可能对雇主、信息安全专业人员或组织声誉造成利益冲突或损害的活动；

7） 维护和确定客观性和独立性；

8） 免于来自行业或其他方面的压力；

9） 不要故意伤害或者泄露同事、客户或雇主的专业声誉；

10）尊重每一个人；

11）避免可能会损害（或者可能看起来会损害）OWASP 客观性和独立性的关系。

1.3 产品功能

1. 注入漏洞挖掘

测试概述：注入类型的漏洞通常是出现在用户和服务器进行信息交互的接口处，这种漏洞使得服务器的后台数据库内的信息很有可能直接暴露出来，造成机密信息的泄漏。如果其中包含管理员的账号信息，其危害也就不言而喻了。更重要的是站在系统用户的角度来说，这种问题的出现严重影响到了系统在客户心中的信誉度。

2. 跨站漏洞检测

测试概述：跨站脚本攻击漏洞通常出现在用户和应用程序进行信息交互的接口处，这种漏洞使用户访问应用程序的时候执行恶意代码，可以直接导致用户数据的泄漏，最终不但有损系统的信誉度，同时还威胁到服务器的安全性。

3. 错误信息挖掘

测试概述：通过发送特殊的字符串参数导致系统错误，根据返回的错误信息分析得到有价值的内容。

4. 业务逻辑测试

测试概述： 在一个多功能动态 Web 应用程序中进行业务逻辑漏洞测试需要非常规的思维方式。 例如，如果应用程序认证机制是采取步骤 1,2,3 执行验证，那么如果你从第 1 步直接跳转到第 3 步会发生什么样的情况？在这简单的例子中，应用程序是否通过打开失败、拒绝访问、或只是报告一个 500 错误信息？这样的案例有很多，但是一个恒定的课程是“ 跳出传统的智能” 。漏洞扫描器无法检测到这种类型的漏洞， 而只可依赖渗透测试者的技巧和创造力。并且这种

类型的漏洞通常是难以发现的。同时如果被加以利用，这种漏洞通常也是应用程序最严重的安全问题。

5. 暴力破解测试

测试概述：暴力破解包括系统性地列举所有可能的方案，并检查是否每个方案符合所描述的问题。在 Web 应用测试中，我们常常面对的问题通常是需要一个有效账户进入应用的

内部。因此，我们要检查不同类型的身份验证模式和不同暴力破解攻击的效。

6. 用户枚举测试

测试概述：这项测试的范围是为了验证是否有可能通过与应用的认证机制互动而收集到一套有效的用户。这项测试将是有益于蛮力测试。通过这种测试我们验证是否通过一个有效的用户名，就可以找到相应的密码。通常情况下，当用户名在系统中存在时，由于错误配置或设计本身的原因导致应用程序泄露相关信息。例如，有时，当我们提交错误证书时，我们收到一条说明用户名存在或密码错误的信息。如果攻击者得到这种信息就可以利用他获得一系列系统用户名。这种信息还可以用来攻击 web 应用程序。如：使用暴力破解或默认用户名/密码攻击。

7. 目录遍历测试

测试概述：许多 Web 应用程序日常操作的一部分就是使用和管理文件。 通过使用没有设计或部署好的输入验证方法， 攻击者可以利用该系统读/写原本不能访问的文件。在特定情况下，它有可能执行任意代码或系统命令。

8. 提权测试

测试概述：一个用户获得比平时更多的资源或功能时就发生了权限升级。应用程序本应阻止这种变化。但通常是由于应用程序存在漏洞导致有可能发生特权升级。结果就是应用程序执行操作时拥有的权限比开发者或系统管理员分配的还要多。

9. 认证模式绕过测试

测试概述：通过简单地跳过登录页面和直接调用一个理应在认证通过后才能访问的内部网页，就可以绕过认证计划。而这个往往是由于对安全威胁的疏忽，无知或简单认知导致的。此外， 常常可以通过篡改要求和假装通过验证的手法绕过验证措施。 这些可以通过修改 URL 参数， 操纵表格和假冒会话的方法来完成。

10. 隐藏文件探测

测试概述：通过隐藏文件的智能探测，除了已有的所有公开页面以外，智能搜索并探测在这些目录下是否存在隐藏文件。这些文件很有可能就是系统的一些配置文件，或者是系统管理员忘记删除的程序说明书，或者是系统后台登录的重要文件。这些文件极有可能导致系统重要数据的泄漏，最终导致整个系统权限的沦陷。

11. 记住密码和密码重置弱点测试

测试概述：如果用户忘记了自己的密码， 大多数 Web 应用程序允许用户重置密码， 通常应用程序是给用户发送密码重置的电子邮件和/或要求他们回答一个或多个“ 安全问题” 。 在这个测试中，我们检查这一职能是否被正确编写并且确认这一功能没有给认证模

式引入任何漏洞。 我们还检查应用程序是否允许用户在浏览器中存储密码（ “记住密码”功能）。

1.4 应用场景

1. 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。

2. 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。

3. 网络信息系统承担重要任务前的安全性测试

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。

2 产品帮助

什么是天翼云安全渗透测试服务？

天翼云安全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。

天翼云渗透测试如何收费？

天翼云渗透测试为线上购买，线下服务，服务定价为：

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

天翼云渗透测试服务有哪些功能？

注入漏洞挖掘、跨站漏洞检测、错误信息挖掘、业务逻

辑测试、暴力破解测试、用户枚举测试、目录遍历测试、提权测试、认证模式绕过测试、隐藏文件探测、记住密码和密码重置弱点测试等。

天翼云渗透测试有哪些特点？

1. 专业团队

渗透测试团队人员具有多年丰富的项目经验，可将漏洞评级与业务层面相结合，展示客户真实存在的业务风险。

2. 安全保密

渗透测试团队人员均可签署用户保密协议，不公开任何关于客户漏洞的相关信息，使客户的漏洞隐私的到保障。

3. 遵守 owasp 道德准则

渗透测试团队人员经过 owasp 培训，遵守以下道德准则：

1）根据所有适用法律和最高道德准则，履行所有专业活动和职责；

2）贯彻执行应用安全法规标准、程序与控制；

3）在专业活动过程中，对专有或其他敏感信息进行保密；

4）勤勉尽责地履行职业责任；

5）开诚布公与沟通；

6）避免任何可能对雇主、信息安全专业人员或组织声誉造成利益冲突或损害的活动；

7）维护和确定客观性和独立性；

8）免于来自行业或其他方面的压力；

9）不要故意伤害或者泄露同事、客户或雇主的专业声誉；

10）尊重每一个人；

11）避免可能会损害（或者可能看起来会损害）OWASP 客观性和独立性的关系。

天翼云渗透测试有哪些规格？

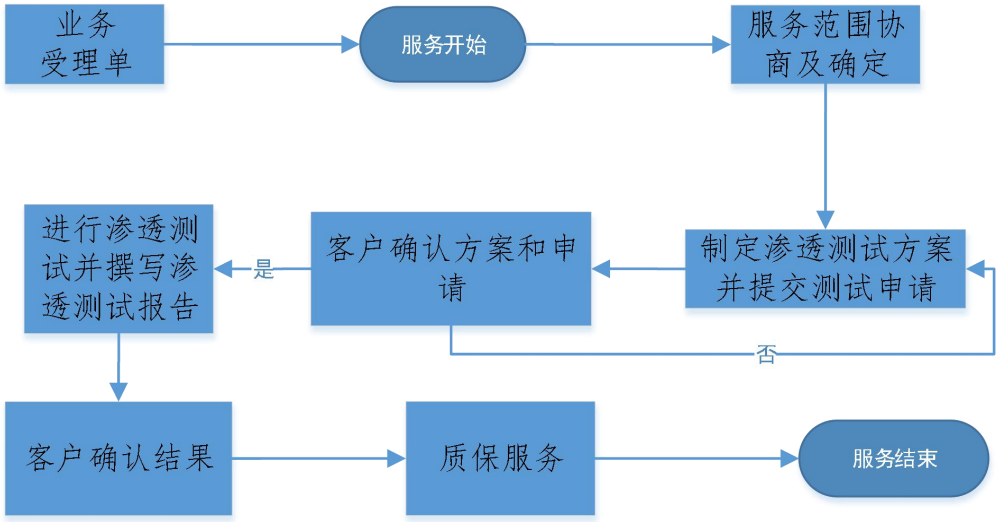
不同企业建议根据实际情况分成三种规格：小型应用系统，最多 1 个应用系统 3 人/日；中型应用系统，最多 5 个应用系统 12 人/日；大型应用系统，最多 20 个应用系统 21 人/日。其他规格需要根据实际情况协商确定。

3 操作指导

天翼云安全渗透测试服务网络要求？

非电信客户应用系统网络与扫描器网络可达即可提供渗透测试。天翼云渗透测试服务基于传统的 B/S 结构，暂不支持对 APP 类的应用渗透测试。

天翼云安全渗透测试服务流程



业务受理单：（见附件一）

客户应如实填写以下信息（必须填满）

1、被检测的 IP 主机信息；

2、域名备案信息比对，必须为客户本人真实、合法信息；

3、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；

4、客户提供的应用 url 描述须写明功能是什么或用途是什么？

5、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；

6、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）

7、客户需签订渗透测试授权书。（附件二）

一、受理阶段

1、输入业务受理单

客服确认业务受理单内容必须填满，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）。

备注：客服 1 个工作日内完成业务受理单信息

2、实施阶段

渗透测试团队接收到客服的业务受理单后，需确认受

理单信息，同时需与客户确认受理单内容。

备注：确认过程 1 个工作日。

3、输出：

业务受理单无问题进入下一阶段；如有问题返回客服，由客服继续与客户沟通，直到业务受理单填写无问题。

二、实施阶段

业务受理单无问题后，进入实施阶段。

1、渗透测试方案（附件三）

渗透测试项目经理需编写渗透测试方案（方案中写明使用哪个地址进行渗透测试，渗透测试时间明确告知客户，与客户沟通在渗透测试实施阶段，客户应将渗透测试使用的地址加入安全防护设备白名单等），同时需与客户确认渗透测试工作需进行到何种程度。

由于在渗透测试期间客户方未关闭安全防护设备所造成的渗透测试结果，乙方不承担责任。

备注：渗透测试方案确认过程 1 个工作日。

2、渗透测试实施

小型应用系统，最多 1 个应用系统 3 人/日；中型应用系统，最多 5 个应用系统 12 人/日；大型应用系统，最多 20 个应用系统 21 人/日。

服务实施操作：开始漏洞扫描收集信息，同时进行人工渗透测试；

问题沟通：对实施过程中发生的问题与客户实时沟通。

3、编写渗透测试报告

输出服务报告：渗透测试完成后输出渗透测试服务报告，报告编写时间 2 个工作日。

备注：渗透测试报告编写 2 个工作日。

4、报告审核修订

报告审核修订：由专人对输出的渗透测试服务报告进行审核修订，审核修订时间 1 个工作日。

备注：渗透测试报告审核修订 1 个工作日。

5、报告提交

报告采用客户通过邮件发起报告申请，渗透测试项目经理将渗透测试服务报告以回复邮件方式发送给客户。

6、质保服务

在客户收到渗透测试服务报告后，乙方参与渗透测试项目的专家为客户持续提供 5 天时间，用于咨询报告中的不明事项。

7、服务结束

在完成以上各阶段工作后，渗透测试项目经理告知客服此次渗透测试服务结束。

天翼云安全渗透测试服务各阶段时间安排？

受理阶段：

客户填写业务受理单并签署渗透测试授权书，交由客服确认，确认后转交渗透测试团队，1 个工作日。

渗透测试团队对客服转交的业务受理单信息再次与客户确认，1 个工作日。如业务受理单出现问题，将返回客服，直到业务受理单无问题，才可进入实施阶段。

实施阶段：

1）渗透测试方案与客户进行确认，1 个工作日；

2）渗透测试实施，小型应用系统，最多 1 个应用系统 3 人/日；中型应用系统，最多 5 个应用系统 12 人/日；大型应用系统，最多 20 个应用系统 21 人/日（至多 10 个工作日内完成）。

服务实施操作：开始漏洞扫描收集信息，同时进行人工渗透测试；

问题沟通：对实施过程中发生的问题与客户实时沟通。

3）输出服务报告：渗透测试完成后输出渗透测试服务报告，报告编写时间 2 个工作日。

4）报告审核修订：由专人对输出的渗透测试服务报告进行审核修订，审核修订时间 1 个工作日。

5）报告采用客户通过邮件发起报告申请，渗透测试项目经理将渗透测试服务报告以回复邮件方式发送给客户。

6）在客户收到渗透测试服务报告后，乙方参与渗透测试项目的专家为客户持续提供 5 天时间，用于咨询报告中的不明事项。