天翼云 • 漏洞扫描服务
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

漏洞扫描是通过对网络主机的扫描及时发现安全漏洞，客观评估系统风险等级。

天翼云漏洞扫描服务提供主机系统漏洞发现、开放端口扫描、弱口令检测及配置脆弱性检测，并对扫描检测结果进行分析形成报告，由专家提供解读及指导服务，方便管理员对主机的安全进行检查和分析，及时修复漏洞提高系统安全防护能力。

1.2 产品优势

天翼云漏洞扫描服务是一个具有高效、报告详尽、漏洞准确性强等特性的漏洞扫描服务产品，拥有超过 50,000 个漏洞的漏洞库和插件，每天自动更新漏洞库插件，可以更加全面的覆盖最新漏洞，准确发现扫描目标系统漏洞风险。

结合资深安全专家、最新业界安全形势、大数据分析、威胁情报分析等输出有深度、有广度的专业漏洞扫描评估报告，并提出切实可行的安全整改建议，有利于用户全面掌握漏洞风险态势，合理高效安排加固工作。

快速发现

- 能够准确、快速的发现主机存在的漏洞风险，对发现的漏洞进行分析，及时提供专业含切实可行整改建议的扫描报告。

准确详尽

- 详尽描述系统存在的漏洞种类、安全漏洞数量，危害级别等。
- 描述漏洞时提供可行解决方案。

准确性强

- 插件扩展性强、功能强大，可以对多种安全漏洞进行漏洞发现，使用多个扫描工具交叉扫描，降低误报，提高漏洞准确性。

1.3 产品功能

产品主要定位主机系统漏洞发现，弱口令检测、配置脆弱性检测，扫描覆盖多种系统环境，如：Windows、UNIX、Linux、Solaris 等，帮助客户发现主机中存在的漏洞风险，根据不同漏洞提供解决建议。

1.3.1 漏洞扫描

多种评估类型： 评估主机系统，网络和应用程序的弱点，检测系统内的恶意软件，发现 Web 服务器和服务的弱点。

丰富的评估能力：网络设备，包括下一代防火墙，操作系统，数据库，Web 应用，虚拟和云环境等，扫描 IPv4，IPv6 和混合网络，可根据需求设置扫描任务运行时间和频率。

两种扫描模式：漏洞扫描器在选择扫描方式时可使用非登录扫描和登录扫描方式，登录扫描能够更深入全面的发现主机漏洞。

持续管理：扫描器可以配置为自动更新，扫描器不断更新高级威胁及零日漏洞插件。

多种报告：自定义报告以按漏洞或主机排序，创建执行摘要或比较扫描结果以突出显示更改，可提供 XML，PDF，CSV 和 HTML 类型的报告。

1.3.2 开放端口

SYN 扫描：端口扫描是计算机入侵者常用的一种漏洞发现方式，攻击者可以通过它了解到主机攻击弱点，一个开放端口就是一个潜在的通信通道，也就是一个入侵通道。如主机开启 FTP 服务，默认会开放两个端口，一般为 20 和 21 端口，入侵者使用端口扫描发现这两个开放状态的端口后将针对展开入侵行为，成功入侵将对企业造成不可估量损失。

而网络运营者主动通过端口扫描发现开放端口，分析开放端口潜在风险，做好开放端口访问限制，识别不必要的开放端口并及时关闭，可避免端口被入侵者利用，提高主机防护能力。

1.3.3 弱口令检测

通过弱口令字典，检测用户 SSH、RDP 等服务是否使用了弱密码，及时更改弱口令有效防备暴力破解入侵。

1.3.4 配置脆弱性检测

配置脆弱性检测也就是基线检查，指针对 IT 设备的安全特性，选择合适的安全控制措施，定义不同 IT 设备的最低安全配置要求，则该最低安全配置要求就称为安全基线，天翼云漏洞扫描服务平台整合操作系统、数据库等系统环境基线规范，通过基线规范逐项比对

主机安全配置项的配置情况，发现配置薄弱点，反馈检查参数，针对加固，避免因配置薄弱导致的入侵风险。

1.3.5 专业的漏洞分析

漏洞扫描结束后扫描器将自动输出扫描结果，描述漏洞风险、漏洞数量以及整改建议，电信云安全专家对扫描器结果结合应用环境、最新业界安全形势、大数据分析、威胁情报分析等整理输出一份有深度、有广度的专业漏洞扫描评估报告，并提出切实可行的安全整改建议，帮助客户全面掌握漏洞风险态势，合理高效安排加固工作。

1.4 应用场景

1.4.1 定期的网络安全自我检测、评估

配备漏洞扫描系统，网络管理人员可以定期的进行网络安全检测服务，安全检测可帮助客户最大可能的消除安全隐患，尽可能早地发现安全漏洞并进行修补，有效的利用已有系统，优化资源，提高网络的运行效率。

1.4.2 网络建设和网络改造前后的安全规划评估和成效检验

网络建设者必须建立整体安全规划，以统领全局，高屋建瓴。在可以容忍的风险级别和可以接受的成本之间，取得恰当的平衡，在多种多样的安全产品和技术之间做出取舍。配备网络漏洞扫描/网络评估系统可以让您很方便的进行安全规划评估和成效检验。

1.4.3 网络承担重要任务前的安全性测试

网络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。配备网络漏洞扫描/网络评估系统可以让您很方便的进行安全性测试。

1.4.4 满足合规性需求（网络安全法、等保）

定期开展漏洞扫描发现主机风险，主动防御风险也是公安局主推的等保要求以及网络安全法要求中的合规要求，其主要目的是：消除与降低安全隐患、周期性的评估和加固工作相结合，尽可能避免安全风险的发生。

2 产品帮助

1、 什么是漏洞扫描服务？

漏洞扫描服务是通过在公网或内网，基于漏洞数据库，通过扫描对指定的远程或者本地计算机系统的安全脆弱性检测，发现可利用漏洞的一种安全检测行为。可对公网或内网的资产进行扫描，扫描完成后出具专业扫描报告，并提供漏洞修复建议。

2、漏洞扫描服务有哪些功能？

多种评估类型： 评估主机系统，网络和应用程序的弱点，检测系统内的恶意软件，发现 Web 服务器和服务的弱点。

两种扫描模式：漏洞扫描器在选择扫描方式时可使用非登录扫描和登录扫描方式，登录扫描能够更深入全面的发现主机漏洞。

丰富的评估能力：网络设备，包括下一代防火墙，操作系统，数据库，Web 应用，虚拟和云环境等，扫描 IPv4，IPv6 和混合网络，可根据需求设置扫描任务运行时间和频率。

持续管理：扫描器可以配置为自动更新，扫描器不断更新高级威胁及零日漏洞插件。

多种报告：自定义报告以按漏洞或主机排序，创建执行摘要或比较扫描结果以突出显示更改，可提供 XML，PDF，CSV 和 HTML 类型的报告。

3、漏洞扫描服务有什么优势？

快速发现：能够准确、快速的发现主机存在的漏洞风险，对发现的漏洞进行分析，及时提供专业含切实可行整改建议的扫描报告。

准确详尽：详尽描述系统存在的漏洞种类、安全漏洞数量，危害级别等，描述漏洞时提供可行解决方案。

准确性强：插件扩展性强、功能强大，可以对多种安全漏洞进行漏洞发现，使用多个扫描工具交叉扫描，降低误报，提高漏洞准确性。

4、漏洞扫描服务包括哪些内容？

安全漏洞扫描包括主机扫描、端口扫描等，可根据客户的实际情况协商确定。

5、安全漏洞扫描是否存在安全风险？

由于安全漏洞扫描使用的自动化扫描工具的部分功能选项是采用模拟攻击方法进行测试，以及客户具体系统架构等因素，在扫描的过程中可能会对系统造成一定的影响，引入不确定的系统停机、服务停止风险。具体风险会在评估前确定，并制定应急预案。

6、实施过程中需要遵守的原则包括但不限于：

（1）规范性原则：整个扫描工作过程和所有文档，应具有很好的规范性，以便于项目的跟踪和控制。

（2）可控性原则：在保证扫描质量的前提下，按计划进度执行，需要保证对漏洞扫描工作的可控性。漏洞扫描的工具、方法和过程要在双方认可的范围之内合法进行。

（3）整体性及有限性原则：漏洞扫描的内容应包括用户等各个层面，漏洞扫描的对象应包括和仅限于用户所指定的具体设备及系统，未经用户授权不得减小或扩大漏洞扫描的范围和对象。

（4）最小影响原则：漏洞扫描工作应避免影响系统和网络的正常运行，尽量不对正常运行的系统和网络构成破坏和造成停产。

（5）保密原则：漏洞扫描的过程和结果应严格保密，不能泄露扫描项目所涉及的任何打印和电子形式的有效数据和文件以及其它的网络数据。

7、漏洞扫描服务的安全性如何保障？

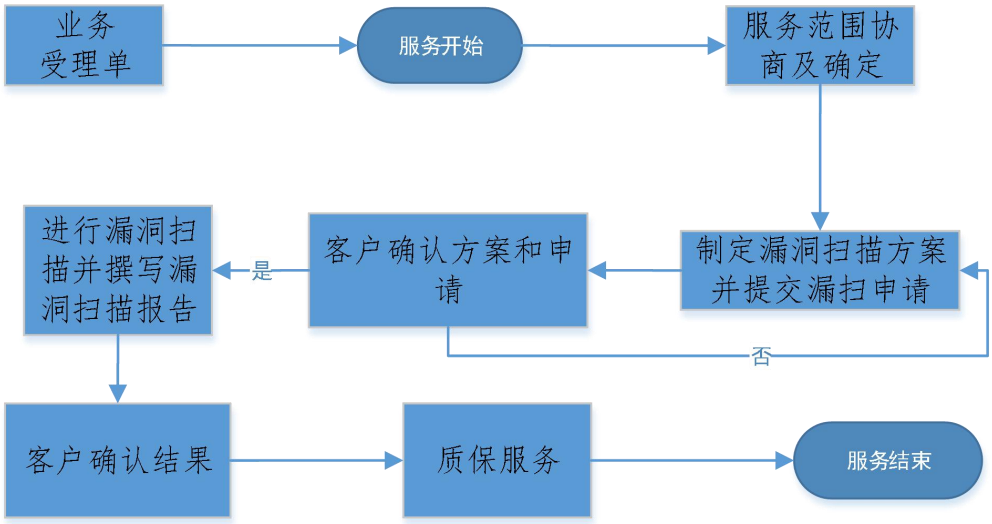
登录扫描过程中或客户需要代为执行基线配置检查脚本，应提供管理员权限的临时账号，并配置登陆地址白名单，天翼云安全人员将通过堡垒机进行操作，操作有授权及审计，记录操作日志，报告中将记录各部分检查内容操作负责人员。当扫描检查完成后客户对临时账号进行销毁，并进行销毁验证。

3 操作指导

天翼云安全漏洞扫描服务网络要求；

非电信客户的应用系统网络与扫描器网络可达即可提供扫描服务（内网需提供用于部署扫描器的内网主机，内外网需保证路由可达）。

天翼云安全漏洞扫描服务流程



业务受理单：

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、被检测主机的操作系统类型及版本；

3、业务接口人联系方式，客户需指定一个具有对漏洞扫描方案及漏洞扫描过程中出现的问题有决定权的业务接口联系人；

4、客户提供扫描资产时需对所提交资产所有权负责，保证资产归提交人合法所有；

5、客户需签订漏洞扫描授权书；

审核阶段

对委托单位提交的受理单信息进行核查,核查内容：

1、判断资产所在环境是公网还是内网。

2、若是公网需要保证被扫描资产路由可达。

3、若是内网环境，需确认委托单位提供可访问到内网主机的跳板机。

4、受理单审核通过后进入漏洞扫描实施阶段。

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，直到业务受理单填满无问题。

备注：确认过程 1 个工作日

实施阶段

1、漏洞扫描实施方案

业务受理单确认无误后进入实施阶段，漏洞扫描操作人员接到客服的业务受理单后确认受理单信息：Ip、版本、授权等并就扫描计划和受理单内容与客户确认。扫描任务实施前，分析客户主机情况，制定扫描方案，明确漏洞扫描任务具体实施时间、目标范围、合理的扫描方式以及最佳扫描策略，并就扫描方案与客户进行沟通确认，由于在漏洞扫描期间客户方未关闭安全防护设备所造成的漏扫结果不准确，乙方不承担责任。

备注：确认扫描方案 0.5 工作日

2、实施漏洞扫描

扫描实施前若客户网络环境公网不能直达，需部署扫描器，也可配合客户自己部署，策略模板由我们提供，部署时间预计 1 个工作日。

关于扫描进度，目前扫描器扫描一个 C 段地址大约需要 6 个小时左右时间，扫描期间实时就扫描过程中发生的问题与客户沟通，最后扫描的结果将存放到扫描结果专用堡垒机上。

漏洞扫描的风险规避，由于漏洞扫描属于黑盒测试，因此可能对被测试目标造成不可预知的风险；此外对于性能比较敏感的测试目标，如一些实时性要求比较高的系统，由于扫描可能引起网络流量的增加，因此可能会引起被扫描目标的服务质量降低。因此需进行如下的风险规避措施：

1）扫描时段选择：一般会选择在夜间或安排在业务量不大的时段进行漏洞扫描。

2）扫描策略选择：根据系统的具体情况配置合理的扫描策略。

3、编写扫描报

漏洞扫描完成后输出漏洞扫描服务报告，报告编写时间 2 个工作日。

4、报告审核修订

由专人对输出的漏洞扫描服务报告进行审核修订，审核修订时间 1 个工作日。

5、报告提交

报告提交方式采取邮件回复的方式提交：客户通过邮件向天翼云漏洞扫描平台发起

报告接收申请，漏洞扫描服务报告以回复邮件方式给客户。

6、质保服务

在客户收到漏洞扫描服务报告后，乙方参与漏扫项目的专家为客户持续提供 3 天时间用于咨询报告中的不明事项。

7、结束服务

在完成以上各阶段工作后，漏洞扫描项目经理告知客服此次漏扫服务结束。

天翼云安全漏洞扫描服务各阶段时间安排？

受理审核阶段：

客户填写业务受理单并签署漏洞扫描授权书，交由客服确认，确认后转交漏洞扫描团队，漏洞扫描团队对客服转交的业务受理单信息再次与客户确认，约 2 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）漏洞扫描方案与客户进行确认，0.5 工作日。

2）漏洞扫描实施，根据主机数量不同，具体完成时间也不尽相同，但至多 10 个工作日内完成所有工作。

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：漏洞扫描完成后输出漏洞扫描服务报告，报告编写时间 2 个工作日。

4）报告审核修订：由专人对输出的漏洞扫描服务报告进行审核修订，审核修订时间 1 个工作日。

5）报告提交方式采取邮件回复的方式提交：客户通过邮件向天翼云漏洞扫描平台发起报告接收申请，漏洞扫描服务报告以回复邮件方式给客户。

6）在客户收到漏洞扫描服务报告后，乙方参与漏洞扫描项目的专家为客户持续提供 3 天时间，用于咨询报告中的不明事项。