杭州融至兴科技有限公司

漏洞扫描系统

白皮书

2023 年 7 月

杭州融至兴科技有限公司

【公司介绍】

杭州融至兴科技有限公司，是一家专业的软件开发公司，致力于为客户提供高质量的定制化软件解决方案。本部位于杭州市西湖区，2014 年起成立南京、宁波、台州、嘉兴、金华、衢州等分公司。公司经营范围包括: 软件产品研发，系统设计服务、定制化开发、技术服务、网络安全服务、网络系统，计算机软硬件，通讯设备，计算机系统集成的设计、安装等；获得了华为、H3C、深信服、安恒、DELL EMC、IBM、宏杉、海康威视、大华、洲明、科达、华平等国内外著名厂家的鼎力支持和全力合作。

公司自成立以来，秉承开拓、进取、创新的创业精神，在完善已有成绩的同时，不断拓宽自己的市场，发展成集计算机网络技术研发、专业化系统集成服务、网络产品销售于一体，在国内计算机网络行业具有重要地位的公司。

目录

1 产品发展背景

随着信息化的普及和发展，计算机在诸多领域得到了广泛应用，互联网已经极大地改变了社会生活和发展。在网络规模持续扩大的背景下，随之衍生的安全问题也愈演愈烈，安全事故发生频率也较之前有所增加。从公开的统计资料可以看到，在 2005 年全球有 70%的大型单位遭受病毒感染而使得业务系统运作受到干扰。即使这些大型单位已经具备了良好的边界安全措施，也普遍部署了病毒防御机制，但仍然不能幸免。攻击者首先通过扫描工具发现漏洞，然后利用相应的攻击工具实施攻击。这种攻击模式简单易行，危害极大。一旦网络自带安全系统被不法分子突破，不仅会导致服务器被病毒入侵，还会使网络资源遭受到难以补救的毁灭性打击。

现有技术并不能杜绝漏洞出现，如果要想最大程度弱化系统漏洞所造成的影响，实证有效的方法便是全面检查计算机系统，确保潜在漏洞可尽快得到处理。在此背景下，漏洞扫描技术应运而生，漏洞扫描的关键是以漏洞数据库为基础，充分利用扫描技术对系统进行全面检测，确保潜在漏洞可被及时发现并得到处理，通过弱化系统脆弱性的方式，为使用者提供理想的网络环境。

2 产品介绍

融至兴漏洞扫描系统是一种自动化的安全工具，它能够及时准确的检测应用程序、操作系统、网络设备等各种系统中的漏洞，以发现系统中存在的安全问题和隐患。网络管理员可以根据扫描的结果调整网络安全漏洞和系统中的错误配置。融至兴漏洞扫描系统是一种主动的前卫防范措施，在黑客攻击前进行防范，可以有效避免黑客攻击行为，做到防患于未然，保证业务顺利的开展，保证业务高效迅速的发展，维护公司、单位、国家所有信息资产的安全。

2.1 市场定位

据业内有关专家估计，目前国内漏洞扫描产品市场容量虽不能和防火墙、防病毒两大巨头比肩，也已经达到入侵检测类产品市场总额的一半左右，市场的光明前景不容置疑。而最近几年以来网络漏洞扫描产品的出现，为网络安全产品厂商供应了一个呈现自身技术水平的更高层次舞台，很多拥有防火墙或入侵检测产品的重量级 IT 厂商纷纷涉足这一市场，相信将逐步转变这片市场上品牌寥寥、竞争松懈的原有面貌，新的市场竞争会逐步在技术、服务以及渠道领域绽开，这对需要更廉价、更尖端产品的用户应当是个好消息。

1) 市场容量有限厂家各行其道

许多新品牌还是采用 OEM 形式，投入的仅仅是营销方面力气，已经可以看出这些厂商的动作并不很大，对相关的技术也不会产生多少推动作用，真正把握核心技术的仍旧是那些长期关注网络安全技术的厂商，市场品牌格局与此之前相比变化并不很大。由此也可以看出，虽然近来出现了许多全新的漏洞扫描品牌，但竞争将很大程度上发生在营销层面，而并不集中于技术领域。

2) 市场格局尚待形成

考虑到网络安全技术对于政府、军队、公安、保密等领域的特别重要性，国内品牌产品受到一定的照看，所以国内厂家目前在市场上处于活跃状态。然而，随着市场容量的不断增长，技术走高、价格下落的趋势会越来越明显，在技术、品牌、渠道、销售几个方面综合优势不足的企业必将渐渐遭到淘汰。

3) 服务竞争是趋势

目前，漏洞扫描厂家供应的服务水平差异很大，比如漏洞库的更新，有些厂家的服务几乎是免费的，有些则远远高于产品本身的价格，甚至开出了天价，这也说明漏洞扫描市场的竞争还特别不充分。在将来的网络漏洞扫描市场上，竞争一定会逐步从单纯的技术和渠道领域扩散到服务领域，更廉价、更便捷、更有效的服务将成为厂家争夺用户的砝码。

2.2 目标客户群体

1) 企业和组织：

各类企业和组织，无论规模大小，都需要保护自己的信息资产安全。漏洞扫描系统可以帮助企业发现和修复网络中存在的漏洞和安全弱点，提高其网络安全防护水平。

2) 政府机构和公共部门：

政府机构和公共部门承载着大量的敏感信息和服务，需要进行定期的网络安全评估和漏洞扫描。漏洞扫描系统可以帮助它们识别潜在的风险，并采取相应的安全措施。

3) 金融机构：

银行、保险公司和其他金融机构需要保护其客户的财务信息和敏感数据。漏洞扫描系统对于金融行业来说尤为重要，可以帮助其发现并修复可能导致数据泄露和金融欺诈的安全漏洞。

4) 医疗机构：

医院、诊所和其他医疗机构拥有大量的患者健康记录和敏感的医疗数据。漏洞扫描系统可以帮助他们识别可能导致数据泄露和违规访问的漏洞，并采取相应的保护措施。

5) 教育机构：

学校、大学和其他教育机构也需要确保其网络安全，防止敏感学生数据和研究成果的泄露。漏洞扫描系统可以帮助他们发现并修复潜在的安全漏洞。

3 产品属性

3.1 产品迭代

迭代版本	版本说明
迭代 1.0（目前）	支持本地服务漏洞检测；
迭代 2.0	漏洞扫描系统能力逐渐转向云平台；

4 产品体系架构

4.1 工作原理

安全漏洞扫描技术是一种基于 Internet 远程检测目标网络或本地主机安全性脆弱点的技术。通过对网络的扫描，网络管理员可以了解网络的安全配置和运行的应用服务，能够及时发现安全漏洞，客观评估网络风险等级。通过网络安全漏洞扫描，系统管理员能够发现所维护的 Web 服务器的各种 TCP/IP 端口的分配、开放的服务、 Web 服务软件版本和这些服务及软件呈现在 Internet 上的安全漏洞。网络安全漏洞扫描技术也是采用积极的、非破坏性的办法来检验系统是否有可能被攻击崩溃，对此进行客观评估和网络风险等级划分。其利用了一系列的脚本模拟对系统进行攻击的行为，并对结果进行分析。

4.2 阶段分析

1） 第一阶段：发现目标主机或网络。

通过 PING 扫描技术，帮助我们识别系统是否处于活动状态。

2） 第二阶段：对目标进一步信息搜集。

包括操作系统类型、运行的服务以及服务软件的版本等。如果目标是一个网络，还可以进一步发现该网络的拓扑结构、路由设备以及各主机的信息。

3） 第三阶段：根据搜集到的信息判断或者进一步测试系统是否存在安全漏洞。

在端口扫描的基础上，通过与目标系统的 TCP/IP 端口连接，并查看该系统处于监听或运行状态的服务，对得到的信息进行相关处理，进而检测出目标系统存在的安全漏洞。

4.3 产品特点

1） 高效性

能够快速地对系统中存在的漏洞和弱点进行检测和识别，并生成详细的报告以供参考。

2） 自动化

自动进行端口扫描、漏洞扫描和安全配置检查等操作，避免了手动操作的繁琐和错误，减少了人力成本和时间成本。

3） 准确性

通过使用多种技术手段来检测漏洞，提高了漏洞识别的准确率，同时还能够对漏洞进行分类和评级，帮助用户更好地了解漏洞的严重程度。

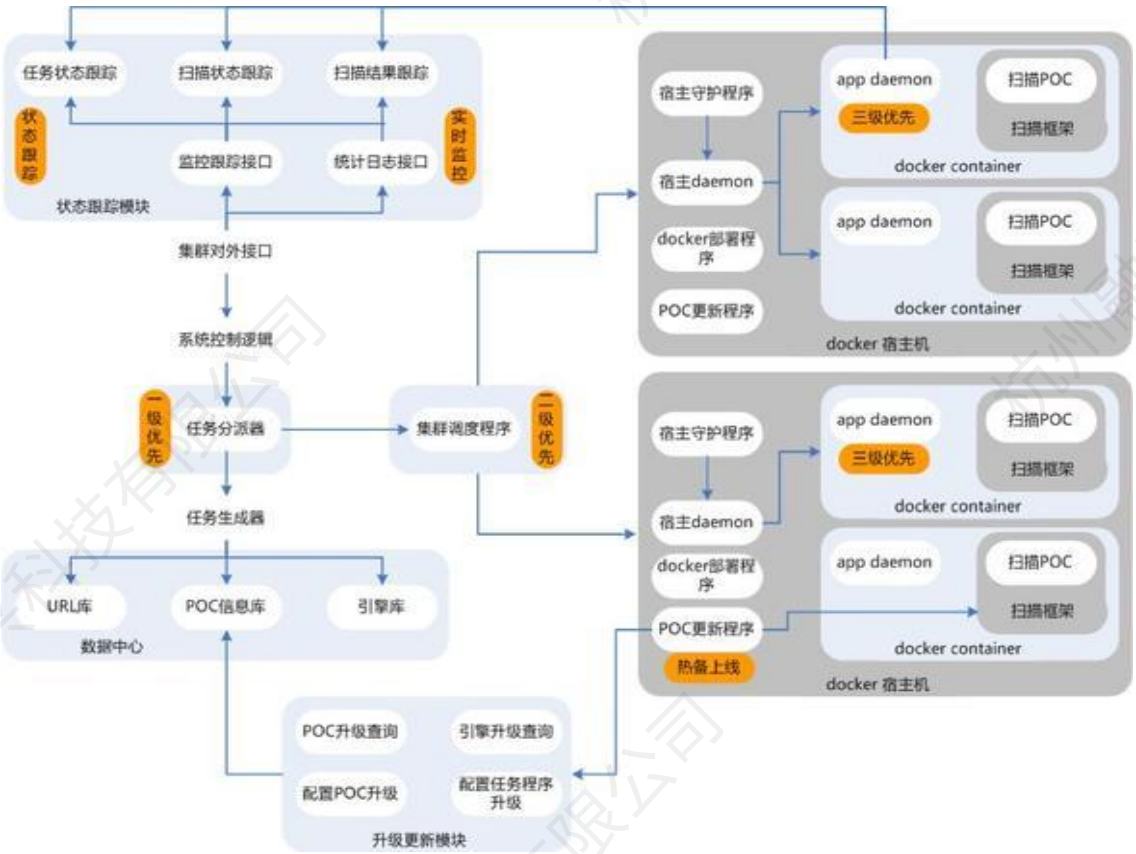
4） 实时性

实时监控系统中存在的安全漏洞和针对系统的攻击，并能够及时警示和处理，在发现安全问题时及时进行预警并采取措施，保证系统的安全性。

5） 灵活性

采用图形用户界面，简单易用，不需要太多的专业知识和技能，方便普通用户使用。根据用户的需求进行定制，帮助用户更好地满足其业务需求。

4.4 逻辑架构图



4.5 系统架构图

5 产品功能

5.1 检测全面，手段丰富

5.1.1 检测机制

本系统采用了多种不同的方法和技术来进行漏洞扫描和安全评估。这些多样化的检测机制能够从不同的角度和层面对扫描对象进行全面检查，以确保尽可能地发现和识别潜在的漏洞和安全弱点。通过各种扫描技术、漏洞数据库、模式匹配、行为分析等手段，提高漏洞扫描的准确性和覆盖范围，帮助用户及时发现系统中的安全隐患，并采取相应的措施予以修复和防范。

1） 主动扫描

针对计算机系统、应用程序或网络进行主动探测和评估的技术。它通过对目标系统发送特定的请求和数据包，尝试使用已知的攻击技术和漏洞利用方法来检测目标系统的脆弱性，模拟来自潜在攻击者的攻击行为，以寻找系统中潜在的漏洞和安全弱点。

1） 分析目标系统的响应和反应；

2） 发送各种类型的网络请求；

2） 安全扫描

用于检测和评估计算机系统、应用程序或网络中潜在漏洞和安全弱点的技术。它通过使用自动化工具和漏洞数据库，对目标系统进行主动扫描和测试，以发现可能存在的漏洞，并提供修复建议。

3） 环境注入错误

在操作系统或应用程序运行时自动设置的全局变量，用于存储与系统环境相关的信息，例如路径、密钥、数据库连接字符串等。应用程序通常使用这些环境变量来获取配置参数和敏感信息。

5.1.2 检测手段

通过多种探测手段，发现单位资产是否存在漏洞风险，并对资产进行全生命周期的管理。主动进行网络主机探测、端口扫描，硬件特性及版本信息检测，时刻了解网络设备、安全设备、数据库、中间件、应用组件等资产的安全情况。

1） 多任务并发扫描

在多任务并发扫描中，可以同时执行多个扫描任务，每个任务独立运行，相互不会干扰。这些任务可以是对不同目标系统进行扫描，或者对同一个目标系统进行不同类型的扫描，例如漏洞扫描、弱密码扫描、配置审计等。

1） 将整体扫描时间大幅缩短，提高扫描效率；

2） 充分利用计算资源，加快扫描速度；

3） 同时扫描不同类型的漏洞或安全问题，以满足特定的安全需求；

4） 多任务并发扫描可以将不同任务隔离开来，避免相互干扰；

2） 多主机并发扫描

同时对多个目标主机进行扫描的安全扫描方法，提高扫描效率，快速地对多个主机进行全面的安全评估。在多主机并发扫描中，可以使用多个扫描引擎或工具，并行地对多个目标主机进行扫描。这些扫描任务是相互独立的，通过并发执行，能够减少扫描时间，并更好地利用计算资源。

1） 对不同的主机进行同时的漏洞扫描、端口扫描、服务识别等；

2） 多个处理器核心或计算节点同时用于扫描任务；

3） 多线程并发扫描

使用多个线程同时执行扫描任务的安全扫描方法。在多线程并发扫描中，可以将扫描任务划分成多个子任务，并使用多个线程同时执行这些子任务。每个线程独立执行，相互之间不会干扰，从而加快扫描速度。

1） 利用多核处理器或多个计算节点的并行计算能力；

2） 根据实际需求和优先级来调整线程的数量和分配方式；

3） 即使某个线程执行失败或遇到问题，其他线程仍可以继续执行；

5.2 扫描快速，类型繁多

5.2.1 主机扫描

对主机系统的软硬件环境进行自动化的扫描、检测、分析，以发现其中存在的各种安全漏洞，包括已知的和未知的漏洞，同时对扫描结果进行报告和提供解决方案。

1） 收集信息

获取待扫描主机的 IP 地址、端口信息以及操作系统等基本信息。

2） 扫描端口

对主机上开放的端口进行扫描，以确认哪些服务正在运行。

3） 识别服务

主动识别正在运行的主机设备，并检查是否有相关的已知漏洞。

4） 验证漏洞

对已发现的漏洞进行验证，判断漏洞是否存在，以及可能对系统造成的影响。

5.2.2 操作系统扫描

对操作系统(Windows、Unix、Linux 等)，进行主动扫描，识别操作系统种存在的漏洞和缺陷，帮助企业更好的对网络安全进行管理。

1） 服务识别

开启服务识别功能，可以更准确地识别目标系统中运行的服务和应用，有助于提高扫描效果。

2） 分析报告

使用扫描工具生成的报告，对扫描结果进行分析和解读，确定安全风险、弱点和漏洞等问题，并制定相应的修复方案。

3） 验证漏洞

对已发现的漏洞进行验证，判断漏洞是否存在，以及可能对系统造成的影响。

5.2.3 WEB 应用系统扫描

对应用系统进行主动或被动扫描，寻找 web 应用系统中可能存在的各种安全漏洞，并提供相应的解决方案。

1） 识别目标

确定待扫描的 web 应用系统，包括其网址、参数等信息。

2） 爬取页面

通过相关技术手段，获取 web 应用程序的页面结构和内容。

3） 攻击检测

通过模拟各种攻击，如 SQL 注入等，检测 web 应用程序中的漏洞。

4） 验证漏洞

对已发现的漏洞进行验证，判断漏洞是否存在，以及可能对系统造成的影响。

5.2.4 弱口令扫描

通过自动或半自动的方式，检测和发现弱密码/弱口令漏洞的安全检测，可以帮助企业或组织发现系统中存在的弱密码问题，提升系统的安全性。

1） 收集口令信息

通过各种途径收集目标系统/应用程序的用户名/密码等弱口令信息。

2） 构造字典库

对准备攻击的口令信息进行分析并构建出密码字典库。

3） 进行爆破攻击

使用所构造的密码字典库对目标系统进行暴力破解攻击，并记录下正确的口

令信息。

4) 分析结果

根据扫描结果，判断口令的复杂度是否符合安全要求，并提出相应的建议以提升口令的安全性。

5.2.5 网络设备扫描

通过对网络设备进行检测，发现并修复可能存在的安全漏洞的过程。网络设备包括路由器、交换机、防火墙、负载均衡器等。

1) 资产排查

确定待扫描的网络设备，包括其 IP 地址、版本信息等。

2) 漏洞库更新

及时更新漏洞数据库，以确保有关已知漏洞信息的准确性。

3) 漏洞扫描

对网络设备进行主动或被动扫描，检测出设备中可能存在的漏洞。

4) 漏洞验证

验证扫描结果，以确定漏洞是否真实存在，以及可能对网络造成的影响。

5.2.6 云环境扫描

对云计算环境中的云服务器、云数据库、容器等进行安全性扫描，发现云环境中可能存在的漏洞，并给出相应的修复建议。

1) 漏洞扫描

通过扫描云环境中的系统、组件和应用程序，检测是否存在已知的漏洞。同时还可以利用该漏洞来获取未经授权的访问权限，从而导致信息泄露和数据丢失等问题。

2） 容器扫描

与传统的虚拟机不同，容器要求一系列微服务部署。因此，需要对容器环境进行定期的漏洞扫描和安全评估，以确保容器的安全性。

3） 恶意代码检测

通过检测可能存在的恶意代码，防止恶意软件通过云应用程序进行攻击。

5.2.7 端口扫描

开放的端口可能会对系统或设备造成潜在的风险和攻击。对计算机系统或网络设备开放的端口进行扫描，以检测可能存在的安全漏洞和风险。通过端口漏洞扫描，可以有效地发现端口漏洞问题，提高计算机系统和网络设备的安全性。

1） 端口探测

通过本系统技术手段，对全局被扫描的端口进行判断和分析，从而确定哪些端口是开放的。

2） 端口识别

确定开放的端口类型和对应的服务，以便更好地针对该服务进行漏洞扫描。

3） 漏洞扫描

对开放的端口进行扫描，检测出可能存在的漏洞和风险。

4） 漏洞验证

验证扫描结果，以确定漏洞是否真实存在，以及可能对系统造成的影响。

5.2.8 数据库扫描

对数据库系统(Oracle、MS-Sql.MySql 等)进行安全性扫描，发现可能存在的漏洞和安全风险，以便及时采取相应的措施加强数据库的安全性。

1） 数据库版本和补丁扫描

检测数据库版本和相应的补丁。

2） 默认口令和弱口令扫描

检查是否存在默认口令和弱口令等安全性问题。

3） SQL 注入扫描

构造恶意的 SQL 语句来尝试入侵数据库，以检测是否存在 SQL 注入漏洞。

4） 权限配置扫描

检测数据库用户权限是否合理，防止越权操作。

5） 敏感数据泄露扫描

检测是否存在敏感数据泄露的情况，如个人信息泄露等。

6） 数据库异常行为扫描

检测数据库中异常的操作行为，如新增用户、修改数据等。

5.2.9 服务器扫描

对服务器操作系统、应用程序和服务等进行全面的安全性检测，以检测可能存在的漏洞和安全隐患。

1） 操作系统漏洞扫描

检测操作系统相关补丁是否存在，以及相关安全配置是否规范。

2） 服务和应用漏洞扫描

检测常见的服务和应用程序是否存在安全漏洞，如 Web 服务器、FTP 服务器等。

3） 系统配置漏洞扫描

检测系统配置是否规范，如登陆提示、超时设置等。

4） 病毒和木马检测

检测服务器上是否存在病毒和木马等恶意软件。

5.3 报告输出，完整可靠

5.3.1 仪盘表统计分析

由于漏洞所造成的安全问题具备一定的危险性，本系统自动将所有单位扫描出来的漏洞进行统计分析，得出中高危漏洞的数据情况，从而较好的保障软件漏洞分类管理的效率和软件漏洞分类的准确率。

1) 全方位统计高、中、低、无危的漏洞安全等级；
2) 漏洞类型数据分析和排列；
3) 周期性扫描产生的漏斗数量同比、环比分析；
4) 高位漏洞处理效果分析；
5) 资产总数统计分析；
6) 存在漏洞数量最多的资产排名等；

5.3.2 扫描报告分析

系统对特定任务进行扫描后得出结论进行细化分析，以便了解漏洞任务的执行情况、任务内包含的相关资产的漏洞情况，与其他系统组件之间的关联和交互等信息。

1) 包括任务执行状态、完成率、任务可行性、可参考性等信息的分析；
2) 对全局任务扫描的总结性分析；
3) 输出扫描检测的综合结果；
4) 各类资产的扫描后的详细生命安全报告生成；
5) 输出所使用的专业检测方式；
6) 输出所涉及到的参考文献资料；
7) 报告产生时间和报告内的 Log 信息和 Error 信息；
8) 全面分析扫描器所了解到的设备信息；
9) 输出受影响的业务、软件、OS 等信息；
10) 支持在线查看、导出、下载、分析、查看等操作；

5.3.3 漏洞分析

对发现的漏洞进行详细的分析，包括漏洞产生原因、影响范围、攻击方式和可能造成的损失等方面的内容。能够更好地了解和理解漏洞的性质，以便更好地制定相应的修复措施。

1） 漏洞的类型

根据漏洞的性质和特点，将漏洞进行分类，例如 SQL 注入、跨站脚本(XSS)、文件包含漏洞等。

2） 漏洞的影响范围

对漏洞可能造成的影响范围进行分析，例如是否会导致系统崩溃、数据泄露或篡改等。

3） 漏洞的攻击方式

分析漏洞是如何被攻击者利用并利用的可能的攻击方式，以便更好地制定相应的防御策略和措施。

4） 漏洞的修复建议

根据漏洞分析的结果，提出相应的修复建议，例如对代码进行修正、增强身份认证策略或限制访问等。

5.4 配置自定义，方向多元化

5.4.1 端口配置

根据单位现有资产设备中的端口，将其补充至本系统内进行管理和配置，以便于后期操作任务扫描时能够关联指定端口。

1） 对于需要开放的端口，支持自定义配置端口名称、描述；

2） 支持配置端口组，自定义不同类型的端口“TCP”“UDP”等；

3） 将端口关联至目标资产，实现层层嵌套；

4) 配置端口过程中能够排查不安全的协议（如 Telnet、FTP 等）；

5.4.2 目标配置

根据单位现有的所有资产进行配置，全面分析资产情况，帮助单位更好的对资产的生命安全健康进行合理管控，保障资产安全的同时还能有效清点资产情况，做到实时的数据分析统计。

1) 自定义目标资产名称及相关描述信息；
2) 判断是否允许多个端口一键扫描；
3) 判断资产设备的存活状态；
4) 关联资产对应的所有端口信息，保障资产准确性和有效性；

5.4.3 扫描配置

根据扫描目标和实际情况，配置扫描策略，如扫描深度、扫描范围、扫描方式等。默认存在 7 种扫描配置文件，BASE、Discovery 等，展示配置范围内漏洞总数和趋势，定期的查看扫描配置可以及早发现漏洞发展趋势和变化幅度等信息，能够能有效的保障企业网络的安全性和稳定性。

5.4.4 报告模板配置

默认由厂商配置完成产生报告的模板装置，其中包括不同格式的文件类型，支持不满导出和查看。目前模板类型分为 6 种，包括 Anonymous XML、CSV Results、ITG、PDF、TXT、XML。

5.4.5 扫描器配置

为了及时发现和修复企业网络中可能存在的安全漏洞，默认由厂商配置配置漏洞扫描器从而对企业网络进行定期的扫描，默认配置的扫描器有“CVE”和“OpenVAS Default”。

6 产品后台

6.1 运行环境

序号	设施	环境参数
1	虚拟机	Linux 操作系统、国产龙蜥系统； CPU：8 核；内存：16G 或以上；存储：500G 以上；
2	服务器	Linux 操作系统、国产龙蜥系统； CPU：8 核；内存：16G；存储：10T

6.2 部署方式

默认采购方式为纯软件形式，不携带硬件产品。

6.3 产品界面

1） 仪表盘

2） 扫描任务


漏洞扫描系统
仪表盘
扫描
配置
超级管理员
任务
报告
结果
任务名称:
搜索
重置

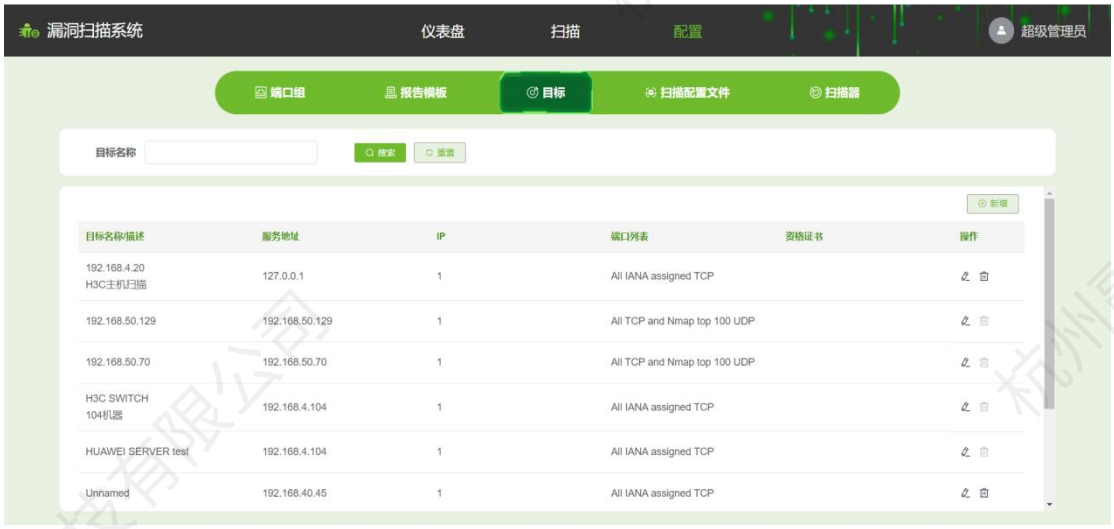
3) 任务报告


漏洞扫描系统
仪表盘
扫描
配置
超级管理员
任务
报告
结果
报告名称:
搜索
重置
创建时间
状态
任务
严重程度
Log
Error
操作

4) 扫描报告

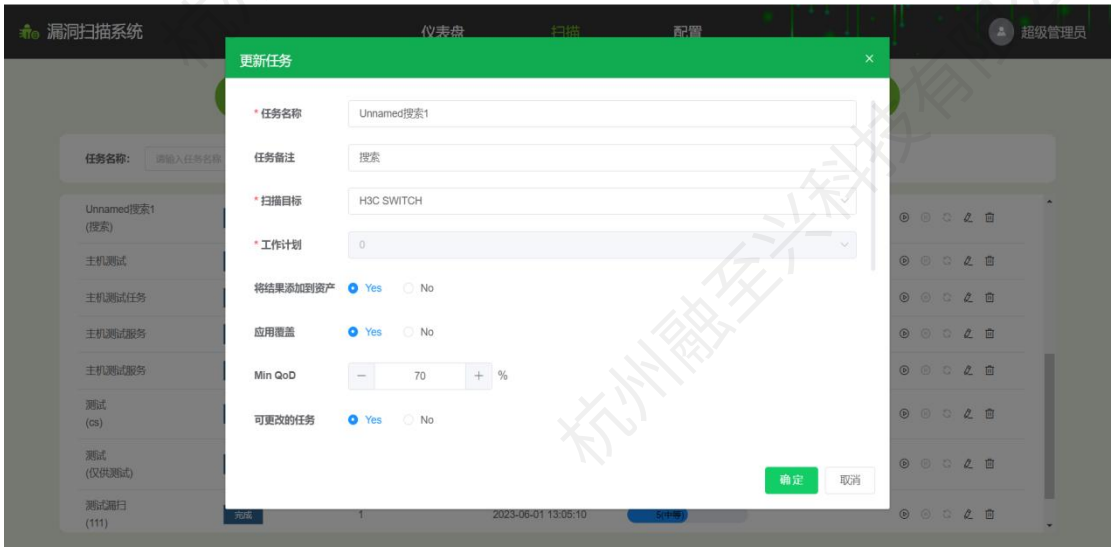

漏洞扫描系统
仪表盘
扫描
配置
超级管理员
任务
报告
结果
结果名称:
搜索
重置
结果名称
严重程度
QoD
IP
位置
创建时间
HTTP Server type and version
ICMP Timestamp Reply Information Disclosure
HTTP Server type and version
Weak Key Exchange (KEX) Algorithm(s) Supported (SSH)
总结
The remote SSH server is configured to allow / support weak key exchange (KEX) algorithm(s).
检测结果
The remote SSH server supports the following weak KEX algorithm(s):

5) 目标配置



6) 扫描器配置

7) 任务配置



7 产品应用

7.1 边缘设备漏洞检测

边缘计算，是一种新兴的计算模式，将数据处理从云端转移到离数据源更近的边缘设备，以提高数据处理的效率和响应速度。目前针对边缘计算的漏洞扫描工具还比较少，但是在一些特定的场景下，漏洞扫描仍然是必须的。例如：

1) 当企业将云端的服务部署到本地边缘设备时，需要对这些设备进行安全审计，以确保其不会成为黑客攻击的入口。
2) 在一些对可靠性和安全性要求较高的场景下，如智能制造、自动驾驶等，边缘设备中存在的安全漏洞同样需要进行及时的检测和修复。

7.2 企业内部网络安全评估

Web 应用程序通常容易受到黑客攻击，漏洞扫描工具可以帮助企业评估内部网络的安全性，检测 Web 应用程序否存在安全漏洞，如 SQL 注入、跨站点脚本等，以提高 Web 应用程序的安全性，可以配合安全服务和诱捕防御系统一起评估，给出修复建议，以便企业及时修复。

7.3 外部渗透测试

黑客通常会利用漏洞来攻击目标网络，而漏洞扫描工具可以模拟黑客攻击的方式，检测网络是否存在安全漏洞，可以配合安全服务和诱捕防御系统一起评估，给出修复建议。

7.4 审计工作

1) 安全合规性审计

一些行业如金融、医疗等需要遵守特定的安全合规性标准，如 PCI DSS、

HIPAA 等，漏洞扫描工具可以帮助企业检测是否符合这些标准。

2） 特定设备安全审计

某些设备可能存在特定的漏洞或安全问题，例如物联网设备、边缘计算设备等，漏洞扫描工具可以帮助企业检测这些设备的安全性问题。

8 产品价值

1） 提高安全意识

通过对漏洞进行分析，可以让企业和个人更好地认识到系统安全的重要性，并且激发他们加强安全意识和采取措施的积极性。

2） 防范攻击

漏洞分析可以帮助企业及时发现系统中存在的漏洞，及时采取修复措施，避免黑客利用漏洞攻击系统，造成不必要的损失。

3） 保护数据安全

漏洞分析可以帮助企业更好地了解自身风险状况，加强数据保护和管理，避免数据泄露和损失。

4） 改进产品和服务

通过漏洞分析，可以发现产品或服务中的缺陷和不足，及时进行修复和改进，提升产品和服务的质量和用户体验。

5） 提高企业声誉

企业采取积极的安全防护措施，通过漏洞分析修复存在的安全漏洞，有助于提升企业形象和信誉。