聚铭漏洞扫描管理系统

产品白皮书

南京聚铭网络科技有限公司

2016 年 6 月

版权声明

商标声明

联系信息

地　　址：南京市雨花区软件大道 180 号 07 栋 406 室

邮　　编：210000

电　　话：025-52205520 025-52205570

传　　真：025-52205565

邮　　箱：support@juminfo.com

网　　址：www.juminfo.com

全国服务热线：400-1158-400

目录

目录.....3

1 漏洞管理存在的问题.....4

2 传统手段无法解决.....4

3 漏洞扫描管理系统的解决方案.....4

4 系统功能概述.....6

4.1 功能概述.....6

4.2 漏洞管理.....6

4.3 安全仪表板.....7

4.4 个人工作台.....7

4.5 资产管理.....7

4.6 告警管理.....8

4.7 报表管理.....8

4.8 知识库管理.....9

4.9 系统管理.....9

5 优势概述.....9

5.1 简便易用的界面风格.....9

5.2 灵活通用的系统设计.....10

5.3 极度快速的处理性能.....10

5.4 基于本地扫描的深度解决方案.....10

1 漏洞管理存在的问题

漏洞指硬件、软件、协议的具体实现或系统安全策略上存在的缺陷，从而可以使攻击者能够在未授权的情况下访问或破坏系统。如在 Intel Pentium 芯片中存在的逻辑错误，在 Sendmail 早期版本中的编程错误，SSH 协议上的缓冲区溢出攻击，在 NFS 协议中认证方式上的弱点，在 Unix 系统管理员设置匿名 FTP 服务时配置不当的问题都可能被攻击者使用，威胁到系统的安全。因而这些都可以认为是系统中存在的安全漏洞。

目前，攻击者未必会利用零日漏洞，实际上，大多数攻击都是利用的已知漏洞。对于攻击者来说，IT 系统的各方面都会存在脆弱性，这些方面包括常见的操作系统漏洞、数据库漏洞、应用系统漏洞、弱口令等，也包括容易被忽视的错误安全配置问题，以及违反最小化原则开放的不必要的账号、服务、端口等。

2 传统手段无法解决

而一般安全管理员不会经常扫描所管理的系统或设备；另外，随着大量 IT 系统被广泛使用，大、中型企业还存在为数众多的下属部门，这对漏洞检查的广度和深度提出了更高的要求，而传统的漏洞检查系统无法满足这些要求。简而言之，传统的漏洞检查工具或系统存在如下几个方面的问题：

1. 检查漏洞缺乏一定的实时性，待发现系统有漏洞被利用而造成信息泄露或服务停止，方采取措施进行防护；
2. 只能针对各类系统开放的端口进行远程检查，无法进行本地方式的漏洞扫描，故检查结果十分有限；
3. 不能检查系统的配置情况，如口令策略、日志设置、访问控制策略设置等；
4. 无法集中化地管理、分析和统计漏洞问题；
5. 无法对存在漏洞的系统或设备进行风险评估；
6. 无法突出用户需要关注的漏洞或安全配置上存在的问题。

上述问题所带来的后果就是，用户无法集中化地管理、评估、修补各种漏洞。

3 漏洞扫描管理系统的解决方案

漏洞扫描管理系统是聚铭网络自主研发的拥有自主知识产权的专业漏洞管理产品。它协助用户实现企业内安全配置的集中采集、风险分析、处理的工作，它提供分布式的部署和管理方式，它是企业日常信息安全工作的重要支撑。

图 1 漏洞扫描管理系统的解决方案

漏洞问题管理：全面集中扫描和分析用户各类信息系统或设备存在的安全漏洞问题，以用户业务为视角，自动地完成以往需安全专家才能完成的风险分析工作。

扫描报告管理：提供全面、详尽、清晰的扫描报告管理功能，并能对不同的扫描结果进行比对。

安全运维管理：建立日常运维工作的服务保障体系：包括各种资产配置库、报表管理、安全知识管理等

它主要解决企业日益繁重的安全配置管理问题。作为统一的安全配置核查和管理系统，能够准确、快速、及时地发现、汇总企业中不同厂商不同种类的网络设备、主机、防火墙、数据库、中间件的安全配置问题，它主要包括如下主要功能：

任务制定：提供灵活的功能用于制定不同类型或周期的检查任务，任务中可以方便地设置检查对象和检查策略。

采集分析：全面集中检查和分析各类系统存在的本地安全配置问题，减轻用户因对不同设备分散管理而带来的冗余工作。

系统加固：提供详尽的、可实际运用的系统加固方案，以指导用户对产生的安全问题进行解决。

4 系统功能概述

4.1 功能概述

漏洞扫描管理系统是由综合展现层、业务功能层、分析处理层、采集层等部分组成，如下图所示：

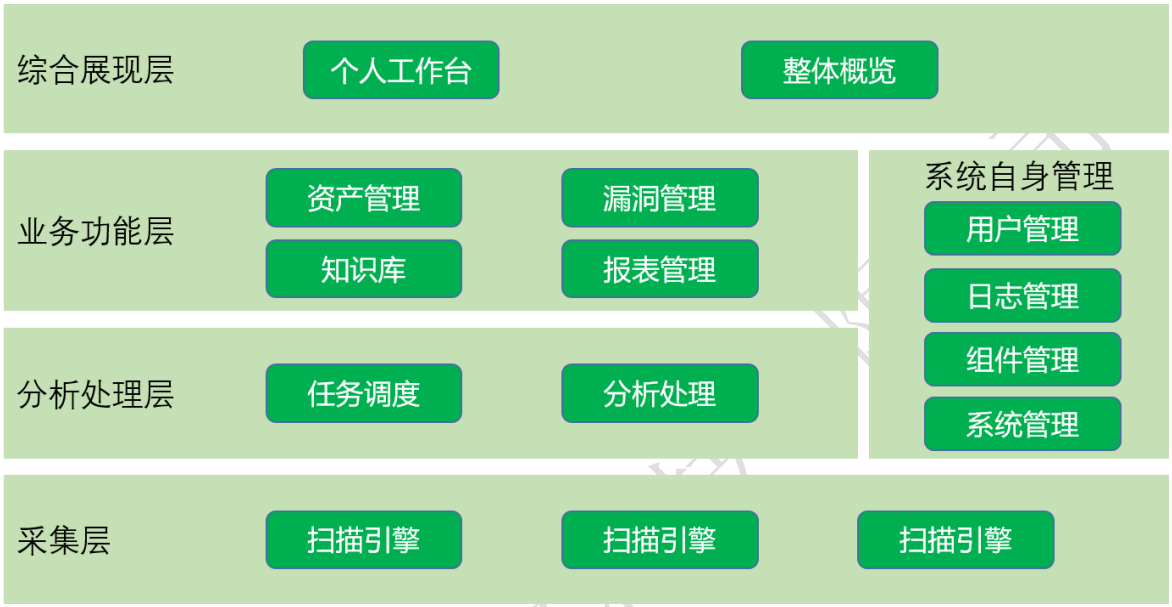

图 1 漏洞扫描管理系统功能架构

在漏洞扫描管理系统中，Web 主要由漏洞管理、整体概览、个人工作台、资产管理、告警管理、报表管理、知识库管理、系统管理组成；下面的章节会较为详尽地介绍每个部分。

4.2 漏洞管理

所谓漏洞是脆弱性的一个子集，专指可通过扫描器发现的脆弱性，其中部分具有国际上标准的 CVE 编号；而如企业没有安全管理负责人之类的脆弱性则不被认为是漏洞。

系统支持分布式的漏洞扫描模式以及集中的漏洞分析、处理。

在漏洞管理中，能够集中查看、统计系统存在的系统漏洞。还可以制定扫描策略及任务，对系统内安全资产进行一次或周期性的扫描。

系统支持设置 IPv4 地址段或选择资产的方式扫描对象；也可以支持对单个 IPv6 地址对象扫描。

漏洞管理主要分以下模块：

1. 漏洞查看：列表查看登录用户权限范围存在的漏洞，显示某漏洞在哪些资产上存在；可显示相关漏洞的全部详细情况；

2. 扫描任务管理：漏洞任务管理包括三个部分：任务列表、正在执行的任务以及已完成的任务，报告可以导出为 Word、PDF、HTML 等格式；对于正在执行的任务用户可以停止、暂停或继续任务的执行；

3. 扫描策略管理：用户可以自定义漏洞扫描策略（通过选择系统内存在的插件）。

4. 系统提供定期的扫描插件升级服务。

4.3 安全仪表板

安全仪表板是系统风险的集中展示区域，也是系统展现给用户的第一个视觉界面；它支持以 TAB 页及微件（Widget）形式展现，用户也可对仪表的布局和内容进行定义和调整。

系统支持如下类型的仪表板：

1. 整体安全概况
2. 安全资产概况
3. 告警概况
4. 脆弱性概况
5. 任务概况

4.4 个人工作台

个人工作台是登录用户用于便捷操作的窗口。它固定的放置于页面的一个位置（通常是顶部），起到管理入口的作用。它主要包含了与登录用户相关的一些信息，但需对用户的权限进行过滤，其功能主要包括：

1. 对象快捷创建菜单，菜单中包含：资产、用户、任务
2. 个人待办事宜：告警
3. 通知功能：任务完成情况

4.5 资产管理

安全资产是漏洞扫描管理系统管理对象。与 ISO27001 的关于资产的定义略有不同，漏洞扫描管理系统中的资产是特指具有 IP 地址的 IT 类设备及其之上运行的、可管理的服务、应用。

一般而言，安全管理中的资产具备如下两类属性：

1. 基本属性：名称、编号、系统类型（产品类型、操作系统类型、版本等）、IP 地址（支持 IPv4 核 IPv6 格式）、响应人（出现安全问题应由何人处理）、登录凭证、上架信息等；
2. 安全属性：完整性、可用性、保密性、风险信息、开放端口、漏洞信息题等。

系统的资产管理支持用户录入、导入或自动发现资产。

为了处理不同网络的资产同 IP 问题，系统还支持对于网络和 IP 地址段的管理。

为了用户便于集中、灵活地管理所辖范围内的资产，系统支持用户自定义资产管理视图。

4.6 告警管理

所谓告警是指用户特别需要关注的安全问题，这些问题来源于高危漏洞。

告警管理中包括了如下功能：

1. 告警监控：监控系统内存在的各种告警；用户可以通过定义过滤器以监控需要特别关注的告警信息；用户也可以根据个人需求，设置告警的提示音、界面显示方式等；
2. 告警处理：处理监控列表中相关告警；针对告警，用户可以清除、确认（不能确定是否需要处理）；
3. 策略定义：用户可以定义各类告警产生的策略（系统内置了部分策略）；在告警策略中可以设定对于安全数据的筛选条件、归并字段、时长和次数以及命中后产生何种响应；响应包括包含发送邮件、发送 Syslog 或 SNMP Trap、执行外部程序或脚本等。

4.7 报表管理

报表管理的作用为展示系统安全工作的结果。报表内容包含各种信息的统计情况，包括：告警报表、资产报表、漏洞报表等。

用户可以定义相关条件以生成报表，它们均可以导出为 PDF、Word、HTML 等格式，如下图所示：

漏洞名称: CVE编号: 端口/协议: BUGTRAQ: 严重级别:	Windows 客户端/服务器运行时子系统 (CSRSS) 中的漏洞可能允许特权提升 (2820917) CVE-2013-1295 58886 高级	如果攻击者登录系统并运行特制应用程序，则该漏洞可能允许特权提升。攻击者必须拥有有效的登录凭据并能本地登录才能利用此漏洞。 对于 Windows XP Professional x64 Edition 和 Windows Server 2003 的所有受支持版本，此安全更新等级为“重要”；对于 Windows XP 的所有受支持版本，此安全更新等级为“中等”。 建议: 大多数客户均启用了“自动更新”，他们不必采取任何操作，因为此安全更新将自动下载并安装。尚未启用“自动更新”的客户必须检查更新，并手动安装此更新。有关自动更新中特定配置选项的信息，请参阅 Microsoft 知识库文章 294871。 影响软件/系统: Microsoft Windows XP x32 Edition Service Pack 3及以前版本 Microsoft Windows XP x64 Edition Service Pack 2及以前版本 Microsoft Windows 2003 x32/x64 Edition Service Pack 2及以前版本 Microsoft Windows Vista x32/x64 Edition Service Pack 2及以前版本 Microsoft Windows Server 2008 x32/x64 Edition Service Pack 2及以前版本
漏洞名称: CVE编号: 端口/协议:	Microsoft Internet Explorer 整数越界拒绝服务安全漏洞 CVE-2009-2536, CVE-2009-1692	Microsoft Internet Explorer允许远程攻击者通过为被选对象的长度属性设置超大的整数值造成拒绝服务攻击。 解决方案: 目前厂商已经发布了升级补丁以修复这个安全问题，补丁下载链接: Debian Linux 5.0 alpha Debian libwebkit-1.0-1-dbg_1.0.1-4+lenny2_alpha.deb

图 2 漏洞扫描管理系统的报表管理

4.8 知识库管理

知识库管理为系统运行和维护提供了知识来源以及安全问题的处理依据、方法或参考，目前支持如下几类：

1. 漏洞类：通过扫描器发现的在硬件、软件、协议的具体实现或系统安全策略上存在的缺陷的描述及解决方案；
2. 安全经验类：基于系统安全事件、漏洞、配置问题等信息综合生成的安全警示信息的描述、告警触发建议及解决方案等。

用户可以通过全文检索功能对系统提供的安全知识进行查询。

4.9 系统管理

系统管理的主要功用在于管理支撑平台正常运行的各种基础功能和参数配置。主要功能有：用户管理、系统参数管理、内置对象管理、升级管理、许可证管理、日志管理、口令策略管理等、常用工具。

5 优势概述

聚铭网络提供了业界领先的漏洞管理方案，其主要优势体现在于：

5.1 简便易用的界面风格

系统通过提供入门向导、个人工作台、任务通知、快捷菜单等方式，为用户提供了简单易用的界面，即使是初次使用系统，也完全能在较短的时间内掌握。

5.2 灵活通用的系统设计

从产品设计角度而言，系统具有极大的灵活性，主要体现在如下几个方面：

1. 可扩展的漏洞扫描功能
2. 可配置的安全仪表板
3. 可配置的系统功能菜单
4. 支持用户自定义的检查策略和告警策略
5. 支持灵活的部署方式

5.3 极度快速的处理性能

支持极高的漏洞扫描速度，而且网络占用带宽小。

5.4 基于本地扫描的深度解决方案

能检测本地应用程序、动态库及配置存在的问题，从而极大地对漏洞问题评估提供了手段。