聚铭网络脆弱性扫描系统产品白皮书

南京聚铭网络科技有限公司

2021 年 09 月 02 日

目录

声明

南京聚铭网络科技有限公司（以下简称为聚铭网络、JUMING）。

JUMING 聚铭图标为南京聚铭网络科技有限公司的商标。对于本手册出现的其他公司的商标、产品标识和商品名称，由各自权利人拥有。

除非另有约定，本手册仅作为使用指导，本手册中的所有陈述、信息和建议不构成任何明示或暗示的担保。

本手册内容如发生更改，恕不另行通知。

如需要获取最新手册，请联系南京聚铭网络科技有限公司技术服务部。

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

全国客服电话：400-1158-400

1 前言

随着信息系统越来越复杂，系统脆弱性的种类及数量呈现爆炸性增长。

近年来，利用漏洞进行攻击的事件逐年增加，攻击形式从单一简单攻击，逐渐发展为组织复杂攻击。攻击仍然会利用系统脆弱性，但攻击手法多变。常见的脆弱性包含操作系统漏洞、应用漏洞、弱口令、网站漏洞、系统配置脆弱点等。

面对如此情况，网络安全管理人员，使用传统的漏洞扫描工具已经很难完成信息系统脆弱性的治理。

随着信息化的发展，很多企业建立了跨地域的办公网络，安全要求集中监控，因此要求脆弱性扫描类产品能够支持分布式部署，集中化监控。另外，虚拟化技术的发展，云平台的建设，IPV6 网络的普及等各种新技术的发展，要求网络脆弱性扫描系统适应新的环境。

2 客户需求

2.1. 配置管理需求

2.1.1. 设备或系统种类繁多

安全运维人员需要面对种类繁多的设备和应用，如何管理这些设备和应用的配置，成为他们在安全运维过程中遇到的巨大问题和挑战。由于需要管理的设备分布范围广且分属不同的业务系统，如何能快捷、方便的收集和分析这些脆弱性，也成为安全运维人员的一个巨大难题。

配置管理方面，日常运维人员需要收集和分析各种主机系统、网络设备、数据库系统以及其它中间件（如 Weblogic、WebSphere 等）的配置；这些配置的收集和分析存在以下问题：

1. 部署位置多种多样；

2. 配置的表现形式和存储样式不尽相同，如有的在配置文件中，有的在注册表中，有的配置文件是一般文本，而有的又是 XML 形式；

3. 采集过程中可能还需要穿越网关设备或堡垒主机；

4. 采集时还需要一些辅助的命令或设置，如采集 Oracle 时，需要知道实例名等。

配置在形式上存在千差万别，如何准确地分析则成为困难的事情。

2.1.2. 配置标准难于统一

目前，由于业界还没有形成统一的配置问题审计的行业标准，因此各厂商提出的标准也是不一而足，而且这些标准也是被频繁地修改，造成维护和定位困难；一般用户很难自己去跟踪和修订标准。

就当前而言，我们能接触到的标准就包括了 CIS（来自美国）、中国石化、

中国移动信息管理部、中国移动、中国电信以及聚铭内部标准；这些标准不仅在支持的设备类型和应用类型上存在差异，就是针对几乎相同的检查点（配置项）而言，做法也不尽相同。

上述差异的处理对研究、开发、维护安全配置基线是一项工作量巨大的任务。

2.1.3. 配置管理自动化程度低

以往，对于设备或应用的配置审计，一般都是通过人工方式进行，仅在上线前进行一次评估（安全加固），这样做的缺点是显而易见的：

1. 纯粹依赖手工方式，效率低下；

2. 在设备或应用上线后，不能定时地或经常性地进行评估，从而无法反映现网设备或应用的配置情况，这导致系统存在巨大的安全隐患（如未能按口令复杂度设置管理员账号）结果比较零散，只能依赖于人工汇总；

3. 黑客入侵后植入木马程序、提权、修改配置及注册表、开放端口等都无法及时发现。

2.2. 漏洞管理需求

2.2.1. 企业网站漏洞攻击形式复杂

随着网络的不断发展，Web 应用系统呈现出爆炸式的增长，由于 WEB 应用系统的易用性，越来越多的企业在电子办公上倾向于使用 WEB 应用系统。然而 Web 应用系统在被广泛应用的同时，因其互联、开放等特性，更容易遭受黑客的攻击，虽然企业网络安全基础设施的建设已经初具规模，但是仍然无法抵御针对 WEB 应用系统漏洞的攻击。据 CNCERT 统计，2016 年，我国 82072 个网站存在被植入后门的情况，其中 2361 个为政府网站。Web 应用被攻击可能给提供或接受服务者造成威胁如：泄漏客户敏感数据、web 数据被篡改导致发布非法言论、web 网站成为钓鱼平台导致用户资金账户被盗等，根据 Gartner

的数据分析，80%基于 WEB 的应用系统或多或少都存在安全问题，其中很大一部分是相当严重的问题。WEB 应用系统的安全性越来越引起人们的高度关注。

2.2.2. 系统漏洞及弱口令难于发现

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。

2.2.3. 传统手段无法解决

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。

3 聚铭网络脆弱性扫描系统解决方案

3.1. 技术方案

聚铭网络脆弱性扫描系统，协助用户完成企业内安全脆弱性问题的发现、分析、加固指导等工作。它主要包括五大引擎：

图片说明 1 五大引擎特性

3.2. 主要功能

图片说明 2 技术架构

3.2.1. 安全基线管理

在网络脆弱性扫描系统中，安全基线是指各类系统、设备的配置标准；而安全配置的违规问题是指实际的系统或设备的配置违反了基线的要求。例如是

否存在不允许的用户账号、账号的口令策略存在一定问题（不满足复杂度、长度、更改时间的要求）等等。

安全基线管理的作用主要体现在如下几个方面：

1.安全评估工作常态化；

2.有利于提高设备自身防护的能力；

3.为安全风险评估提供基础材料。

安全基线可被划分为账号类、口令类、授权类、日志配置类、路由配置类等等，例如：应删除或锁定与设备运行、维护等工作无关的账号等。

目前，支持的系统或设备主要包括：

1.主流操作系统（Linux/Unix、Windows 等）；

2.主流路由器/交换机；

3.主流防火墙；

4.主流数据库；

5.主流 Web 中间件。

3.2.2. 变更检查管理

变更管理检查计算机系统的文件、端口、进程等的变化信息，以监控系统的变更状况发现其中的异常，以便及时采取相应措施保护系统安全。

目前，支持的系统或设备主要包括：

1.主流操作系统（Linux/Unix、Windows 等）；

2.主流路由器/交换机；

3.主流防火墙；

4.主流数据库；

5.主流 Web 中间件。

变更检查可以解决一下问题：

1.记录已加固设备状态，当设备配置发生变化后，可以参考变更检查记录的加固状态进行配置；

2.发现潜在的黑客入侵，通过检测进程、端口、启动项，来发现是否有黑客入侵启动了恶意进程及端口。

3.2.3. 系统漏洞管理

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。

在任务管理中，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，并产生报告，提供详细的漏洞解决方案。

通过扫描器发现的系统漏洞脆弱性，具备国际上标准的 CVE 编号及 CNVD、CNNVD、Bugtrag 标准的支持。

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。

3.2.4. 弱口令扫描

通常认为，容易被猜测或者破解工具破解到的口令均为弱口令。假如信息系统中存在弱口令，就像家门钥匙放在家门口的垫子下面一样。目前聚铭网络脆弱性扫描系统具备弱口令扫描引擎，可以发现信息系统中存在的弱口令。具体引擎优势如下：

1.支持 10 种类型口令扫描；

2.用户可以自定义用户名字典及密码字典；

3.支持用户名加通配符方式弱密码库扫描；

4.支持弱口令查询，输入相关查询字段进行查询弱密码支持。

另外对于扫描到的弱口令还可以应用的系统漏洞扫描中，发现弱口令设备上更多的脆弱点。

3.2.5. 网站漏洞扫描

通过深度探测端口与服务扫描网站站点信息遍历整个 WEB 框架目录结构，自动分析产品源代码，通过匹配插件库与测试验证来证明漏洞的存在。

通过内置或指定的扫描任务，配置任务周期来执行扫描指定的站点、资产、URL 等。

执行结果的任务产生任务报告，报告内指出发现哪些漏洞、次数，在某个设备某个 URL 上发现漏洞，并可导出报告文件。

在 WEB 漏洞管理中，能够集中查看、统计站点存在的 WEB 漏洞，还可以指定扫描策略及任务，对域名内站点安全进行一次或周期性的扫描。

3.2.6. 资产管理

安全资产是网络脆弱性扫描系统管理对象。与 ISO27001 的关于资产的定义略有不同，聚铭网络脆弱性扫描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。

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。

3.2.7. 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、安全基线违规问题等。

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）或转工单；

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、暂存数据（用户可以将数据保存在临时表中作为其它策略的输入）等。

3.2.8. 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、安全基线报表、配置变更报表、漏洞报表、工单报表等。

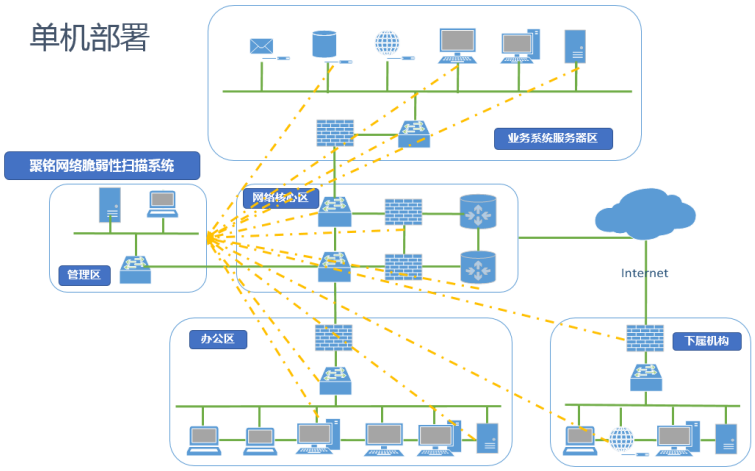
用户可以定义相关条件以生成报表，它们均可以导出为 Excel、PDF、Word、HTML 等格式。

3.3. 部署方案

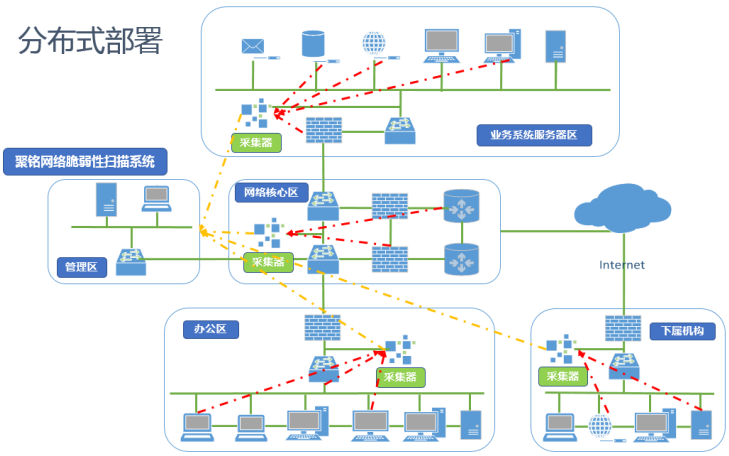
聚铭网络脆弱性扫描系统支持单机部署及分布式部署。

企业网络较为简单，可以采用单机部署。对于企业网络架构复杂，需要跨

网络运营，可采用分布式部署。



图片说明 3 单机部署



图片说明 4 分布式部署