JUMING 聚铭

聚铭网络脆弱性扫描系统

产品白皮书

聚铭网络科技有限公司

2026 年 2 月

目录

声明

未经本公司书面许可，任何单位和个人不得擅自摘抄、复制本书内容的部分或全部，并不得以任何形式传播。

在本文中如无特别说明，聚铭网络均指南京聚铭网络科技有限公司和北京聚铭信安科技有限公司。

JUMING 聚铭图标为聚铭网络的商标。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，请联系聚铭网络技术服务部。

联系信息

南京总部：南京市雨花台区软件大道 180 号南京大数据产业基地 7 栋 4 层

电　　话：025-52205520/52205570

传　　真：025-52205565

全国服务热线：400-1158-400

网　　址：www.juminfo.com

产品支持：support@juminfo.com

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 用户需求

2.1. 企业安全管理问题

随着信息系统越来越复杂，导致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，攻击手法多变，但攻击仍然会利用系统脆弱性。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、违规外联等。

面对如此情况，网络安全管理人员，使用传统的漏洞扫描系统已经很难完成信息系统脆弱性的发现及修复。

随着信息化的发展，很多企业多建立了跨地域的办公网络，安全要求集中监控，那么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。

2.2. 建设需求

2.2.1. 配置方面

2.2.1.1. 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或应用，如何管理这些设备和应用的配置，是他们在安全运维过程中遇到的巨大问题和挑战。

而且，由于需管理的设备分布范围广、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，则成为横卧在安全运维人员面前的一个巨大难题。

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、视频监控设备、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

由于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。

2.2.1.2. 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。

上述的差异造成研究、开发、维护安全配置基线是一项工作量巨大的任务。

2.2.1.3. 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。

2.2.2. 漏洞方面

2.2.2.1. 网站漏洞

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：泄漏用户敏感数据、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。那么要求，网站漏洞扫描具有主流安全漏洞扫描的能力，包含 CGI 攻击、LFI、RFI、REDIRECT、敏感信息泄露、目录遍历、SQL 注入、跨站攻击、暗链攻击等漏洞类型。通过任务的形式可以进行实时脆弱性扫描，也可以进行定时巡检。并能够对网站进行脆弱性评估，对网站的安全性一目了然。

2.2.2.2. 系统漏洞

1、系统种类繁多，漏洞隐藏较深

2、漏洞披露逐年上升，种类庞大

3、黑客常利用漏洞进行攻击，窃取企业机密

2.2.3. 视频终端方面

1. 众多资产无法自动梳理，容易遗漏

面对视频专网众多不同厂商和型号的前端设备接入，存在着资产管理难度增大、资产摸牌不清晰以及容易被遗漏的问题。

2. 视频终端违规外联

需要能够有效地检测和预防未经授权的视频专网设备外联行为，以防止敏感数据泄露或恶意软件感染。

3. 视频专网内脆弱性难以及时发现，被通报工作压力大

通用的检测工具难以符合公安及公共视频专网标准，容易被上级监管通报。

3 产品架构及功能

在网络脆弱性扫描系统中，功能主要由资产管理、脆弱性管理、边界完整性管理、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，以下为功能介绍

3.1. 产品架构

图片说明 2 技术架构图

3.2. 资产管理

资产是脆弱性扫描系统管理对象，高效纵深的资产自动摸底，快速对视频监控网络资产扫描，寻找现网存活设备，对其进行资产识别并进行资产管理。

3.2.1. 资产识别

1. 可识别服务器（业务服务器、数据库服务器、WEB服务器、代理服务器等）、终端（手机、摄像头、打印机、媒体设备等）、网络设备（交换机、无线设备等）、安全设备（防火墙、入侵防御、WAF等）、视频监控系统（摄像头、硬盘录像机等）。

2. 可以识别资产IP地址、MAC地址、品牌、系统、软硬件版本号、开放的端口及服务等详细信息。

3. 资产盘点为安全检测提供检测目标，为安全检测报告的生成、平台展示所需的数据分析提供数据来源。

3.2.2. 资产管理

系统的资产管理支持用户录入、导入或自动发现资产。

为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。

3.3. 弱口令扫描

资产弱口令扫描是网络安全管理中的一项重要活动，目的是为了发现和纠正网络中资产（包括服务器、网络设备、应用程序账户、摄像头等）使用的易被猜测或破解的简单密码。执行弱口令扫描可以帮助组织识别安全隐患，从而采取措施强化账户安全。

弱口令扫描引擎可以根据协议、软件平台的登录过程，分析并制定特定的弱口令字典库，实现对摄像头、数据库服务器、终端、邮件服务器、网络设备、安全设备等弱口令扫描。具体引擎优势如下：

1.支持快速、轻量、全面的对终端设备、服务器、中间件、应用、视频监控、

网站系统等各类业务进行弱口令扫描。

2.支持 10 种类型口令扫描；

3.用户可以自定义用户名字典及密码字典；

4.支持用户名加通配符方式弱密码库扫描；

5.支持弱口令查询，输入相关查询字段进行查询弱密码支持。

6.支持自定义弱口令扫描应用端口

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。

3.4. 系统漏洞管理

通过 AI 智能归类技术，对各类资产针对性的匹配漏洞特征库，可实现全面、高效的大规模视频监控网络安全漏洞检测。

3.4.1. 漏洞扫描任务配置

1. 配置扫描任务

根据目标系统的特点，配置扫描任务的相关参数，如扫描范围、扫描策略、扫描深度等。同时支持设置 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。

针对视频专网系统的特定漏洞，如流媒体传输漏洞、视频编码库漏洞等，设置相应的扫描规则。

2. 执行扫描

自研高性能漏扫引擎，可以实现快速无损扫描，对重点区域定期高频扫描，运行扫描工具对目标系统进行扫描，检测可能存在的安全漏洞和配置错误。

3.4.2. 漏洞自动化验证及复核

支持自动验证产生的告警是否为真实漏洞，并在修复后利用自动化复核功能确认问题已解决，以此完成漏洞处理的整个闭环。

3.4.3. 漏洞持续监测和分析

1. 持续监控

建立持续的安全监控机制，对资产进行定期的漏洞扫描和安全评估。

2. 实时漏洞库更新

具备国际上标准的 CVE 编号及 CNVD、CNNVD、Bugtrag 标准的支持，同时内置公安行业视频专网标准全量插件族，提供云端漏洞实时更新。

3. 自动生成漏洞任务报告

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。

3.5. 边界网络完整性检查

采用无侵入远程扫描方式，智能检测出终端设备通过智能手机热点、USB 共享网络等方式进行的非法外联行为，以及网络中私自接入的 NAT 路由设备、无线 AP 设备等违规内联行为，并完成自动通报。

3.5.1. 违规外联检测

通过违规外联检测引擎主动定期扫描全网的终端资产，结合探测技术促使终端发起对指定监控点的外联行为，检测出终端设备通过智能手机等方式进行的非法外联行为，通过在外网部署微服务的方式，自动邮件通知到负责人，完成自动通报。

可精准识别外联主机并告警，包括：出口IP地址、私网IP地址、外联时间、外联次数等，主动监测边界状态，预防出现跨网信息交互事件。

违规外联主动扫描方式检测速度快、范围广、无需部署任何插件。

3.5.2. 非法内联检测

基于扫描方式全面识别网络资产，并快速检测网络中私自扩展的非法内联设备，可识别类型如下：

1. 私自接入的路由、随身 Wi-Fi

随身 Wifi 设备以 USB 方式接入终端 PC 或笔记本后，会自动变身成一无线 AP，并以 NAT（地址转换）的方式为智能手机、平板设备提供无线 Wifi 接入，既隐蔽又难以监管。

2. BYOD 路由器设备

BYOD（Bring Your Own Device）指携带自己的设备办公，这些设备包括个人电脑、智能手机、平板等。

3.5.3. 终端双网卡检测

智能检测出终端设备双网卡，一机多用等违规行为。

3.6. 安全基线管理

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。利用积累的各类设备配置合规性知识，可实现对设备配置的全面自动化检测，确保各项设置符合既定的安全标准。

1. 安全基线管理能力主要体现在如下几个方面：

- 利用积累的各类设备合规性知识，可以实现对设备配置的全面自动化检测，确保各项设置符合既定的安全标准。

- 违规列表：显示系统内所有的违规信息情况，以列表方式呈现。
- 违规详细查看：在安全基线违规列表中，选择某个违规信息，可进一步查看该违规的详细信息。
- 行业基线等级保护策略（军工、医疗、公安、高校等）。

2. 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；

6.监控系统（摄像头、录像机）。

3.7. 变更检查管理

基于先进的变更检查技术，可以定期且自动地对业务中各类设备的关键配置进行审查，审查包括设备系统的文件、端口、进程等的变化信息，以便及时发现配置变更，从而降低配置变更造成的风险。

- 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；

6.监控系统（摄像头、录像机）。

- 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.发现设备中潜在的黑客入侵，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。

3.8. WEB 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中 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。

3.9. 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。

3.10. 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、WEB 漏扫报表、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。

4 产品价值

1. 主动安全防御

通过定期扫描网络中的所有资产，包括服务器、网络设备、视频监控设备、应用程序等，发现潜在的安全漏洞和弱点，使组织能够提前采取措施修复，从而转变为更加主动的安全防御姿态。

2. 优化资源分配

通过识别不必要的开放端口、过时的服务和未打补丁的系统，优化 IT 资源利用，减少维护成本和提高运营效率。

3. 满足等保合规要求

满足行业标准和法律法规要求企业定期进行安全审计和漏洞管理。使用专业脆弱性扫描产品可以帮助企业满足 GB28181 和 GB35114 等合规要求，避免因安全疏忽而面临的通报。

4. 减少通报压力

系统内置了符合公安行业标准的检测机制，能够定期自动识别业务网络及视频网络系统的脆弱性，及时修复潜在风险，从而减轻因安全问题被通报而带来的工作压力。