兼容 OVAL 的多平台 VAS 设计与实现

王旭冬,高 岭,张 林
WANG Xu-dong,GAO Ling,ZHANG Lin

西北大学 信息科学与技术学院,西安 710127
Department of Information Science and Technology,Northwest University,Xi'an 710127,China
E-mail:wangxudong@nwu.edu.cn

WANG Xu-dong,GAO Ling,ZHANG Lin.Design and implementation of OVAL-compatible VAS on multi-platform.Computer Engineering and Applications,2009,45(36):82-85.

Abstract: Aiming at the flaws of current interoperability problem brought by different information expressing standards between different security products and present situation that a network generally includes several kinds of platforms,a design of manager/agent architecture-based,OVAL-compatible multi-platform Vulnerability Assessment System(VAS) is given.This system takes OVAL as vulnerability assessment standard and takes lightweight Web server as communicating measure.It supports multi-platform vulnerability assessment and sharing security data with other OVAL-compatible tools with high accuracy,assessing completeness and functional expansibility.

Key words: interoperability;multi-platform;Vulnerability Assessment System(VAS);Open Vulnerability and Assessment Language(OVAL)

摘 要:针对不同厂商安全软件之间的信息表示格式差异带来的软件联动问题,以及一个网络内通常存在多种平台主机的现状,提出一种"管理者/代理"架构的、兼容 OVAL 的多平台 VAS(弱点评估系统)。系统以 OVAL 作为弱点评估标准,以轻量级 Web server 为通讯手段,支持多平台主机弱点评估,在保证评估高精度的同时,支持与 OVAL 兼容的其他安全软件共享安全数据,具有更高的评估完备性和功能扩展性。

关键词:联动;多平台;弱点评估系统;开放弱点评估语言
DOI:10.3778/j.issn.1002-8331.2009.36.024 **文章编号:**1002-8331(2009)36-0082-04 **文献标识码:**A **中图分类号:**TP393

1 引言

随着计算机技术和网络通信技术的飞速发展,各种主流计算机操作系统和应用软件暴露出越来越多的弱点。根据 CERT 的统计,2007 年公布了 7 236 个弱点。从 1995 年到 2007 年公布的总数已经达到 38 016 个,这些弱点已经严重威胁到计算机的安全[1]。计算机弱点也叫漏洞或脆弱性,是指系统设计、实现或操作管理中存在的,可被利用于侵害系统安全策略的缺陷[2],而弱点评估就是对目标系统进行弱点分析,这里的系统可以是一个服务,也可以是一个网络上的计算机,还可以是整个计算机网络[3]。当前,弱点评估连同入侵检测和补丁管理等,已经成为网络安全方案的重要组成部分,但因为一个安全产品往往不能兼顾所有功能,所以如果不同厂商安全软件采用同一种信息表示格式,就可以进行信息共享,实现多产品联动,进一步提高网络的安全性。此外,一个计算机网络往往由多种操作系统平台主机组成,如果安全软件不能同时支持各种操作系统,网络的安全性难以得到高质量保证。

OVAL 是国际上知名安全组织 MITRE 发布的一种弱点评估标准,该文应用了该标准,设计实现出一种新型的基于"管理者/代理"的兼容 OVAL 的多平台弱点评估系统(VAS)。管理者可以通过系统中的中心服务器端向网络内任意一台安装有代理的主机指派弱点评估任务,扫描的结果回传到中心服务器,以便于管理以及被其他 OVAL 兼容的系统加以利用,例如补丁安装系统等。系统可以在保证弱点评估精度的前提下,实现弱点评估的网络化支持和多操作系统平台支持,使管理员能够及时、准确地了解网络上所有主机的安全状况。此外,由于系统兼容 OVAL,数据信息文件可以方便地被其他兼容 OVAL 的安全系统利用[4],从而进一步保证多平台网络的安全性。

2 开放弱点评估语言 OVAL

开放弱点评估语言(Open Vulnerability and Assessment Language,OVAL)是一个弱点评估语言,同时也是一个标准,用于把安全工具和服务运行中所有范围内的传输信息标准化[5],

基金项目:国家科技支撑计划项目(the National Key Technology R&D Program of China under Grant No.2007BAH08B01);陕西省自然科学基金(the Natural Science Foundation of Shaanxi Province of China under Grant No.2005f36)。

作者简介:王旭冬(1983-),男,硕士,主要研究领域为网络安全技术;高岭(1964-),男,博士生导师,教授,主要研究领域为计算机网络性能分析、服务质量及其应用研究;张林(1982-),男,硕士,主要研究领域为网络安全技术。

收稿日期:2008-12-26 **修回日期:**2009-03-05

从而为安全产品之间的交互提供条件。每个 OVAL 定义的弱点都具有对应的 CVE[6]编号,CVE(Common Vulnerabilities and Exposures)是一个著名的安全漏洞库,它是对目前各主流操作系统平台已知漏洞和安全缺陷的标准化名称的列表,目的是能更加快速而有效地鉴别、发现和修复软件产品的安全漏洞。通过 CVE 编号,可以方便地查找出每一个 OVAL 定义的弱点对应的补丁情况,从而通过补丁的安装来完善操作系统和软件的安全性。

2.1　OVAL 的组成结构

OVAL 社区开发了三种使用 XML(eXtensible Markup Language,扩展标记语言)编写的模式,用于 OVAL 语言的框架和词汇。OVAL 系统特征模式(OVAL System Characteristics schema)来表示系统信息;OVAL 定义模式(OVAL Definition schema)用于表达一个指定机器状态;OVAL 结果模式(OVAL Results schema)来报告评估结果。而每种模式又由两部分组成:一个核心模式("core" schema)和一系列的组件模式("component" schema)。核心模式用于定义 OVAL 本身的结构以及与测试无直接联系的因素,比如受影响的平台,弱点的描述等等;每个组件模式定义和描述了某个特定平台的弱点测试。

2.2　OVAL 兼容性

OVAL 兼容性是指:一个产品或者服务使用 OVAL 作为漏洞、补丁、安全配置和其他机器状态信息的传输细节,那么该产品或服务就被认为是 OVAL 兼容的。如果说一个产品的某个功能是 OVAL 兼容的,那么它必须符合 OVAL 的某个或者多个模式(系统特征,定义,结果),可以是一个生产者,生成符合某个 OVAL 模式的数据,或者是一个消费者,利用一个已存在的 OVAL 数据集,或者二者兼有[7]。目前在国外已经有一些兼容 OVAL 的软件和服务,例如,作为 OVAL 定义的消费者的 GFI LANguard Network Security Scanner[8],以及作为 OVAL 定义生产者的 Red Hat Security Advisories[9]。通过使产品或服务兼容 OVAL,提供给用户的各种安全产品便可以实现安全信息共享,协同工作,并减少安全产品冗余评估的比例,提高工作效率[10],共同组成一个安全体系来保护计算机安全。

3　兼容 OVAL 的多平台 VAS 设计与实现

3.1　系统模型设计

结合 OVAL 的特点,兼容 OVAL 的多平台 VAS 主要分为中心服务器端和代理端两部分。中心服务器端负责从外部网络进行弱点定义数据的更新,以及整个网络的弱点评估管理。代理端作为一个服务进程运行在被评估主机上,负责通过与中心服务器端通讯,来完成本机弱点评估。系统是 Manager/Agent 架构的,为了减轻中心服务器的负载和提高弱点扫描效率,中心服务器只负责发起弱点评估请求,具体的弱点评估工作由代理端在宿主主机上完成。

为了保证系统自身通讯安全,管理者、中心服务器端以及代理端之间的数据传输采用 SSL128 位加密,另外,管理员登录中心服务器端,中心服务器端连接代理端都需要认证。为了实现管理员、中央服务器端和代理端三方之间的通信,中央服务器端和代理端都实现了一个轻量级 Web Server 来接受和处理请求。系统结构图如图 1 所示。

3.2　弱点评估流程

弱点评估流程分四个阶段:弱点定义获取与分析,系统信息收集,弱点判断,结果处理。前三部分分别对应 OVAL 结构中的三种模式,以实现对 OVAL 的兼容。弱点评估的流程如图 2 所示:

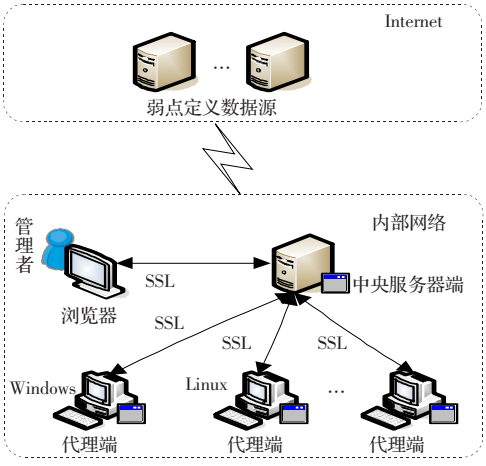

图 1　系统结构图

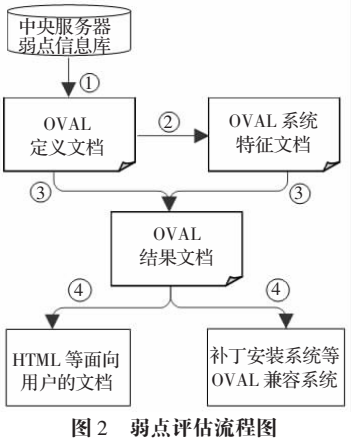

图 2　弱点评估流程图

因为不同操作系统版本对应着不同内容的 OVAL 定义,所以每个代理端在启动的时候,会主动向中央服务器注册本机操作系统版本信息,中央服务器根据代理端所在主机的平台,向代理端下发平台对应的 OVAL 定义文档,代理端分析该文档,对系统进行弱点信息收集,生成 OVAL 系统特征文档,再将收集到的特征信息与 OVAL 定义文档中的判定标准进行比较,并根据 OVAL 定义文档中的判定规则来判定弱点的存在,将评估结果保存在 OVAL 结果文档中,回传给中央服务器。中央服务器再将结果文档转换成 HTML 页面呈现给用户,并将结果文档进行保存,用于与其他 OVAL 兼容的安全软件进行信息共享。所以,从 OVAL 兼容性角度分析,该系统是 OVAL 定义的消费者,同时是 OVAL 系统特征的生产者与消费者,另外还是 OVAL 结果的生产者。

3.3　功能模块设计

为了便于多平台开发,代理端的功能简单,主要负责向中央服务器端提供操作系统版本信息和本机弱点评估工作;中央服务器端除了负责管理网络内各主机的弱点评估任务外,还负责更新 OVAL 模式文件以及定义文件。系统主要功能模块如图 3 所示。

操作系统信息收集模块:收集本地操作系统版本信息(Linux 系统通过调用 uname,返回操作系统版本信息结构体;Windows 系统通过查找注册表键值获取操作系统版本信息)。

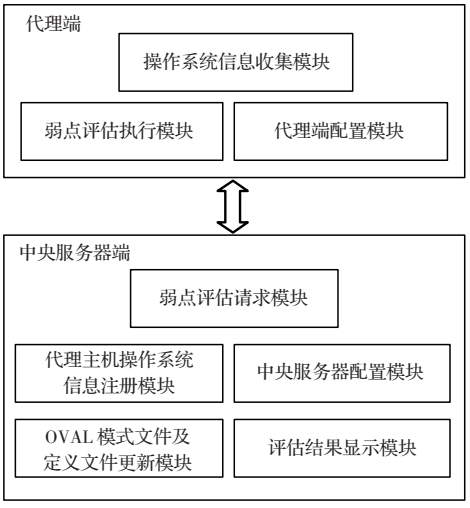

图 3 系统主要功能模块

弱点评估执行模块:接收中央服务器发出的弱点评估请求,对本机执行弱点评估,该模块由 OVAL 定义解析模块、OVAL 系统特征信息收集模块与 OVAL 结果分析模块组成,三个子模块依次执行,完成弱点评估任务。

代理端配置模块:配置代理端的运行端口、中央服务器 IP 地址等信息。

代理主机操作系统信息注册模块:接收代理端发出的操作系统信息数据并保存。

中央服务器配置模块:配置中央服务器的运行端口,启用/禁用指定功能模块信息。

OVAL 模式文件及定义文件更新模块:从外部数据源更新 OVAL 的模式文件以及各操作系统版本的 OVAL 弱点定义文件。

评估结果显示模块:将代理端返回的评估结果文档转换为 HTML 页面显示输出。

弱点评估请求模块: 接收管理员发出的弱点评估请求,并向指定主机提供 OVAL 定义文件,发起弱点评估任务。

3.4 关键技术

3.4.1 弱点信息获取

具体的系统弱点评估方法是围绕对 OVAL 定义文档的 XML 文件分析来实现的。在整个分析过程中,弱点信息获取是最主要的一个步骤。弱点信息的获取是基于测试的,形式化的弱点表示如下:

首先定义 3 个集合:弱点定义集 $VD=\{vd_1,vd_2,\cdots,vd_n\}$,测试集 $T=\{t_1,t_2,\cdots,t_m\}$,操作符集 $OP=\{AND,OR,XOR\}$。每个弱点定义由测试集中若干个测试和操作符集中的一个操作符组成,即 $vd_i=\{\{op\},\{t\},\{t\}\times\{op\}\times\{t\}\}$。一个测试的值 TRUE 或 FALSE,当一个弱点所包括的所有测试值都已获得, 再根据 op 来对这些值进行运算,得出最后的计算结果,用于判断弱点是否存在。由于测试的内容各有不同,系统实现了文件探针、注册表探针等不同的探针类型来获取不同类型的系统信息。例如在 Windows 的 OVAL 定义文档中,经常要获取指定 DLL 文件的版本,那么可以调用文件探针来获取该文件的版本。

3.4.2 嵌入式 Web 服务

嵌入式 Web 服务是中央服务器可以和不同平台的代理通信的基础。为了实现管理员、中央服务器端和代理端三方之间的通信,系统采用成熟的 HTTP 作为传输协议。而要使现有的 Web Server 软件完成系统的通信要求,需要进行大量的修改工作,于是系统通过在代理端和中心服务器端都实现一个轻量级的 Web Server 组件和一个功能单一的 Web Client 组件来实现管理员、中心服务器以及代理端的通信。这里的"嵌入式"是指将 Web 组件嵌入应用程序内使用。因为中央服务器与代理端的通信都是标准的 HTTP 请求与响应,所以,在有新的操作系统兼容需求时,不需要对中央服务器进行大的改动,而只需要快速开发出新操作系统对应的代理端,即可使弱点评估系统支持新操作系统主机的弱点评估。HTTP 请求处理流程如图 4:

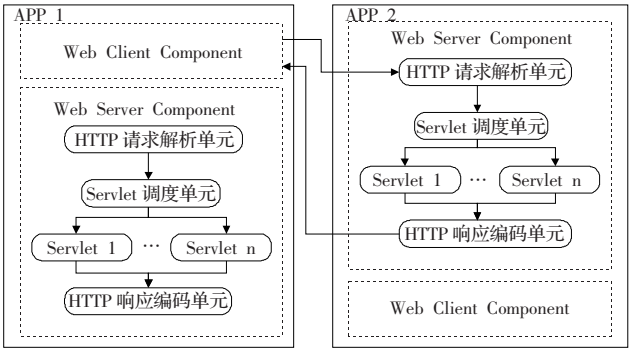

图 4 HTTP 请求处理流程

当应用程序 1 需要应用程序 2 发请求时, 应用程序 1 的 Web Client 组件将请求转化为 HTTP 请求发送给应用程序 2 的 Web Server 组件,该组件通过对请求进行解析,调用指定的 Servlet 实现相应功能, 最后将结果返回给应用程序 1 的 Web Client 组件。因为功能模块的添加不会影响整个系统的结构,所以可以很方便地为系统添加新的功能模块,从而为系统的扩展性提供了保证。

4 实验与结果

实验主要从精度和速度两方面进行,以客观反映系统的弱点评估精度和速度性能。在精度实验中, 针对 1 台安装有 Windows XP SP2 的主机(192.168.31.14)进行弱点评估测试。而在性能实验中,目前已开发出 Windows 和 Red Hat Linux 两个版本的代理端,所以待测主机包含 2 台 Windows XP SP2 主机(192.168.31.14-192.168.31.15)和 2 台 Red Hat Linux AS3(192.168.31.12-192.168.31.13)主机,以证明系统的多平台评估的可行性。用于弱点评估的 OVAL 定义文档采用 2008 年 10 月 15 日,OVAL 官方更新的 OVAL 定义文档(microsoft.windows.xp.xml,red.hat.enterprise.linux.3.xml)。

4.1 评估精度测试

在系统的评估精度测试中,分别使用国内安全厂商瑞星发布的瑞星漏洞扫描工具(2008 年 10 月 15 日更新)和兼容 OVAL 的多平台 VAS 对安装有 Windows XP SP2 的主机 192.168.31.14 进行评估。瑞星漏洞扫描工具共检测出 75 个弱点,扫描用时 11 秒,兼容 OVAL 的多平台 VAS 共查出 79 个弱点,扫描用时 45 秒。经过结果对比,发现兼容 OVAL 的多平台 VAS 查出了瑞星漏洞扫描工具查出的所有弱点,瑞星漏洞扫描工具未检测到的 4 个弱点如表 1 所示。

通过 CVE 编号跟踪得知,4 个弱点对应的补丁编号为:MS08-033,MS07-064,MS07-042,MS05-050,目前微软官方网站都已提供对应补丁。在对应补丁安装完毕后,重新用该系统对该主机进行弱点评估,4 个弱点的值均由真转为假。在同时

表 1　瑞星漏洞扫描工具未检测到的 4 个弱点信息

CVE ID	弱点描述
CVE-2008-0011	MJPEG Decoder Vulnerability
CVE-2007-3895	Microsoft DirectX Code Execution Vulnerability
CVE-2007-2223	Vulnerability in Microsoft XML Core Services Could Allow Remote Code Execution
CVE-2005-2128	WinXP,SP2 DirectShow Malicious avi File Vulnerability

采用最新的弱点定义库的条件下，兼容 OVAL 的多平台 VAS 利用了 OVAL 的开放性和社区安全领域专家的支持,提高了系统的弱点评估粒度和范围。

4.2　评估速度测试

为了测试系统的网络评估速度,分别使用知名的网络弱点扫描工具 Nessus 和兼容 OVAL 的多平台 VAS 对 4 台局域网主机(192.168.31.12-192.168.31.15)进行 4 次评估,评估台数分别为 1、2、3、4。评估速度结果如图 5 所示:

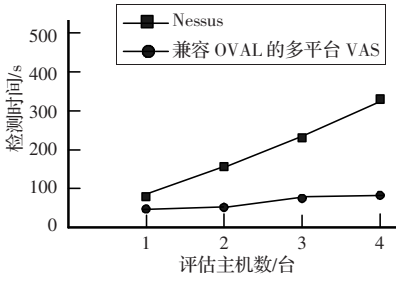

图 5　评估速度统计结果

根据图 5 的结果可知,兼容 OVAL 的弱点评估系统评估一台主机消耗的时间约为 45 秒。另外,因为多台主机的弱点评估是由相同数量的主机共同完成的,所以,虽然在单机扫描时,与 Nessus 的性能差距不明显,但随着主机数目的增加,评估时间并没有成倍增长,采用代理来进行弱点评估的效果明显。与瑞星等同样以内部查询机制工作的工具相比,系统对单台主机的弱点评估时间较长。根据对系统弱点评估过程的跟踪发现,评估耗时大部分是在 XML 文件的解析上，而主流操作系统平台的 XML 弱点定义文件体积庞大,导致整个弱点评估过程较慢。在待测主机由 2 台增至 3 台时,评估时间有较明显增加,也是因为前两次评估没有 Windows 主机参与，而在第三次评估时，加入了一台 Windows 主机，而 Windows 主机的弱点定义文件相对 Linux 而言,体积更庞大。

5　结束语

分析了现有弱点评估系统所存在的问题,提出了一种兼容 OVAL 的新型的网络弱点评估系统。该系统有以下优点:弱点评估精度高;具有 OVAL 兼容性,安全信息数据可以和其他 OVAL 兼容的安全产品共享利用；只需要开发不同系统的代理端,即可实现支持多平台弱点评估。通过在弱点评估方向采用一致的标准 OVAL，将使弱点评估软件的完备性进一步提高,应用范围进一步扩展。

下一步工作:针对 Windows 平台的客户机安装软件的具体状况,设计 OVAL 定义文档重组算法,进一步提高系统弱点评估的时间性能。

参考文献:

[1] A complete report of all of the statistics CERT has available cataloged vulnerabilities[EB/OL].(2007-04-30).http://www.cert.org/stats/fullstats.html.

[2] Glossary of terms used in security and intrusion detection[EB/OL].(2008-07-20).http://www.sans.org/resources/glossary.php.

[3] 邢栩嘉,林闯,蒋屹新.计算机系统脆弱性评估研究[J].计算机学报,2004,27(1):1-10.

[4] 段丹青,陈松乔,杨卫平.漏洞扫描与入侵检测联动系统的研究[J].计算机应用研究,2007,24(7):128-130.

[5] An introduction to the OVAL language[EB/OL].(2007-07-11).http://oval.mitre.org/oval/documents/docs-06/an_introduction_to_the_oval_language.pdf.

[6] CVE-Common Vulnerabilities and Exposures[EB/OL].(2008-07-20).http://cve.mitre.org.

[7] An introduction to OVAL compatibility[EB/OL].(2006-07-16).http://oval.mitre.org.

[8] Network security scanning,patch management,vulnerability management[EB/OL].(2008-05-15).http://www.gfi.com/lannetscan.

[9] Red Hat announces OVAL security compatibility[EB/OL].(2008-07-24).http://www.redhat.com/about/news/prarchive/2006/oval_mitre.html.

[10] Martin R A.Transformational vulnerability management through standards[C]//Systems & Software Technology Conference,2005.

(上接 7 页)

统的基于散射模型的分类方法,有两个不足:第一,所分地物类别有限;第二,精度不高。该文提出了一种基于四分量散射模型的全极化 SAR 分类方法，该算法可以根据实际地物种类覆盖情况灵活选择要分的类别数目,为了验证算法的有效性,用日本机载 L 波段 PiSAR 全极化 SAR 数据进行实验,实验表明,该算法比 FCM 聚类算法和四分量算法分类效果都好，为了对算法进行进一步的验证，还把该文算法和经典 H-alpha-wishart 算法相比较,对两种算法的实验结果从主观和客观两方面进行比较分析,表明,该文算法比 H-alpha-wishart 算法分类效果要好。

参考文献:

[1] Cloude S R,Pottier E.A review of target decomposition theorems in radar polarimetry[J].IEEE Trans Geosci and Remote Sens,1996,34(2):498-518.

[2] Freeman A,Durden S L.A three-component scattering model for polarimetric SAR data[J].IEEE Trans Geosci and Remote Sens,1998,36(3):963-973.

[3] Yamaguchi Y,Moriyama T,Ishido M,et al.Four-component scattering model for polarimetric SAR image decomposition[J].IEEE Trans Geosci and Remote Sens,2005,43(8):1699-1706.

[4] Yamaguchi Y,Yajima Y,Yamada H.A four-component decomposition of POLSAR images based on the coherency matrix[J].IEEE Geoscience and Remote Sensing Letters,2006,3(3):292-296.

[5] 刘蕊洁,张金波,刘锐.模糊 C 均值聚类算法[J].重庆工学院学报:自然科学版,2008,22(2):139-141.

[6] Ferro-Famil L,Pottier E,Lee Jong-Sen.Unsupervised classification of multifrequency and fully polarimetric SAR images based on the H/A/Alpha-Wishart classifier[J].IEEE Trans Geosci and Remote Sens,2001,39(11):2332-2342.