第34卷 第18期 计 算 机 工 程 2008年9月
Vol.34 No.18 Computer Engineering September 2008
·安全技术· 文章编号：1000—3428(2008)18—0161—03 文献标识码：A 中图分类号：TP391.76

新型主动式漏洞检测系统

赖维莹，陈秀真，李建华
(上海交通大学电子信息与电气工程学院，上海 200240)

摘 要：介绍了一种采用C/S结构的新型主动式漏洞检测系统。该系统利用了OVAL漏洞检测定义，包括检测代理和控制台两大模块。其中，检测代理是基于OVAL Schema的漏洞扫描器，能在不对本地计算机系统和网络系统造成任何损害的情况下，全面有效地检测主机漏洞，并将漏洞信息结果上报给控制台，而控制台端实现了同时控制局域网内多台主机的漏洞扫描，并将整个局域网的漏洞信息汇总。大量实验测试证明，该系统是可行且具有先进性的。

关键词：主动式漏洞检测；检测代理；控制台；漏洞扫描

Novel Active Vulnerability Detection System

LAI Wei-ying, CHEN Xiu-zhen, LI Jian-hua
(School of Electronic, Information and Electrical Engineering, Shanghai Jiaotong University, Shanghai 200240)

【Abstract】 The paper proposes a novel active vulnerability detection system based on C/S mode. This system is composed of two modules: agent and console. The detection agent, which is a vulnerability scanner based on OVAL Schema, can give an effective and all-sided vulnerability scan as well as reporting the result to the console without any damage to the network. At the same time, the console realizes remote control against the process of scans on several computers and gathering of scan results of the whole network. The test result proves that this system is feasible and advanced.

【Key words】 active vulnerability detection; detection agent; console; vulnerability scan

1 概述

随着黑客入侵的日益猖獗，人们对网络安全的重视度空前提高，网络安全研究领域的攻与防愈演愈烈。漏洞检测就是对计算机或网络设备进行安全测试，找出安全隐患或者可能被利用的缺陷。

下面是常用的漏洞检测方式。基于网络的漏洞检测是根据不同漏洞的特性，服务器构造网络数据包，发给网络中的一个或多个目标，以判断某个特定的漏洞是否存在。这种方式不需要在目标主机上安装任何东西，维护简便，但是因为不能直接访问目标系统的文件系统，相关的一些漏洞不能检测到，并且在扫描端口时可能不能通过防火墙。与此相似的是基于Web的漏洞检测，用来管理和集合的服务器程序是运行在软件供应商的服务器上，而不是在客户自己的机器上。这种方式的优点在于检测方式能够保证经常更新，缺点在于需要依赖软件供应商的服务器来完成扫描工作。还有基于主机的漏洞检测，通常在每个目标主机系统安装了一个代理漏洞检测程序，在本地对本操作系统的各种配置、权限、补丁等方面进行检测，由一个控制台对各个代理进行管理[1]。

本文利用 Mitre 组织开发的 OVAL，设计并开发了新型漏洞检测系统。该漏洞检测系统本质上是基于主机的检测，由检测代理单独完成漏洞检测，但同时会上传到控制台实现管理和报告浏览。该系统具有以下特点：(1)采用多个检测代理，可以完成全网范围内的安全扫描漏洞过程。(2)能够对多种平台下的主机进行漏洞扫描，在不同平台的终端可以安装针对不同操作系统的扫描器。(3)采用 C/S 模式，实现控制台控制扫描过程和结果汇总处理，所有扫描的指令，均从控制台进行控制。(4)采用统一的漏洞库，当有新的漏洞发布时不需要更新软件代码，只需要更新包含有漏洞定义信息的 XML 文件。同时还具有翔实的漏洞结果报告。(5)不使用模拟攻击，软件本身不存在安全隐患，控制台和代理之间只有通信及结果传输，不扫描端口或发送数据包，占用网络资源少。(6)由于漏洞扫描都在检测代理完成，检测代理和控制台之间，只需要在扫描之前和扫描结束之后，建立必要的通信链路。因此，对于配置了防火墙的主机，漏洞扫描器能够完成漏洞扫描的工作，并且只需要在防火墙上开放通信所需的端口就可以完成控制台对检测代理的控制。

2 系统原理及设计

2.1 系统总体框架设计

新型主动式漏洞检测系统的结构如图 1 所示，分为agent和console两大模块。在局域网内，检测控制台可以同时向多个安装了检测代理并处于监听中的主机发送检测连接信号，每个代理主机上运行OVAL漏洞扫描器，扫描结束后，分别将漏洞检测结果传回控制台。在控制台主机上有标准的CVE漏洞库，它查询漏洞库，把检测结果中的每个CVE号所对应的漏洞信息显示给系统管理员[2]。由于控制台不需要串行扫描各客户端以获得漏洞信息，各检测代理并行扫描漏洞，速度快，网络资源也得到很大节省。采用统一的漏洞库，只要更新包含有漏洞定义信息的XML文件，就可以方便地更新系

基金项目：国家自然科学基金资助项目(60605019)
作者简介：赖维莹(1984－)，女，硕士研究生，主研方向：漏洞检测，信息安全检测与评估；陈秀真，讲师、博士；李建华，教授、博士生导师
收稿日期：2007-10-18 **E-mail：**abuiris@126.com

统了。

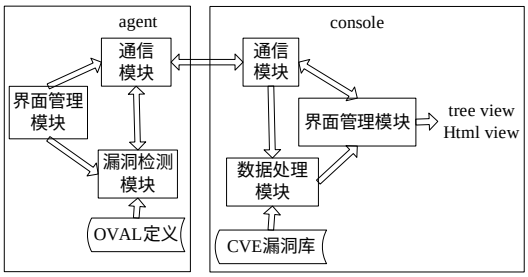

图 1　漏洞检测系统的系统结构

2.2　漏洞检测原理

本文提出的漏洞检测器基于开放性漏洞评估语言(Open Vulnerability and Assessment Language, OVAL)，是一个国际化的信息安全组织标准[3]。OVAL标准化 3 个检测漏洞的步骤如下：通过一系列测试收集系统信息和配置信息；检测系统是否存在特定的安全漏洞和配置问题；漏洞检测结果的输出。

OVAL 与 CVE 兼容，可以与其他 CVE 兼容的工具或数据库协同工作，根据所收集的系统信息的特征来判断是否存在漏洞。OVAL 漏洞检测器的操作流程如图 2 所示。首先要收集计算机系统信息，将收集到的信息和开放漏洞定义大纲(OVAL definition)所定义的漏洞信息进行比对，用一系列的正则表达式来判断系统中是否存在某一漏洞。最后以 OVAL 规定的格式输出漏洞检测结果。

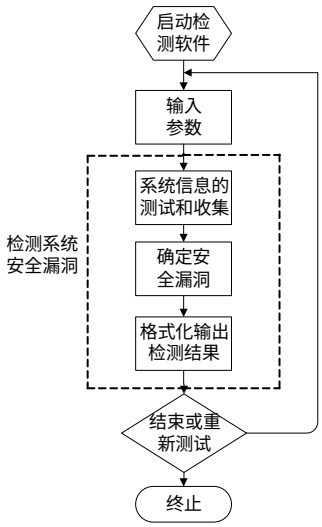

图 2　OVAL 漏洞检测器的操作流程

3　系统实现

3.1　检测代理实现

在系统设计中，检测代理要运行在多个平台上，考虑到跨平台的可操作性，本文设计了 2 种操作系统下的检测代理：Linux 和 Windows。以 Linux 下的 QT 和 Windows 下的 MFC 制作友好的图形用户界面，采用高效的 C++作为编程语言，保证漏洞扫描部分的许多代码是在 2 种操作系统下可重用的。检测代理主要有 3 大模块用于实现其功能：界面管理模块，通信模块，漏洞扫描模块。同时检测代理提供 2 种工作模式：单机模式和 C/S 模式。模块关系如图 1 的左边部分所示。

3.1.1　界面管理模块

界面管理模块主要用于设置漏洞扫描的参数、界面的管理、以及扫描状态的显示等。参数的设置是为漏洞扫描过程指定工作环境。

3.1.2　通信模块

通信模块用于同控制台的通信，并在通信成功时启动漏洞扫描模块。在检测代理启动时，使其处于 C/S 模式的侦听状态，当接收到来自控制台的指令时，就为漏洞扫描开辟一个线程。这个过程主要由 2 个函数 Listen 和 ListenThread 实现。在 Listen 函数中，首先创建一个 Socket 对象的实例，然后使用 Bind 方法绑定所指定的接口使 Socket 与一个本地终结点相联，并通过 Listen 方法侦听该接口上的请求。在 ListenThread 这个线程函数中，当侦听到用户端的连接时，调用 Accept 完成连接的操作，创建新的 Socket 以处理传入的连接请求，调用函数 Interpretermain 启动扫描，在扫描结束后会调用 sendFile 函数发送检测结果到控制台。

3.1.3　漏洞扫描

启动的漏洞扫描过程，主要又可分为 3 个步骤：系统信息收集，确定安全漏洞，输出检测结果。

(1)系统信息收集

系统信息收集以 OVAL 定义文件中的漏洞测试的基本方面，来测试计算机的当前状态，其流程如图 3 所示。

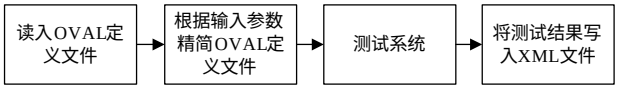

图 3　系统信息测试流程

因为 Windows 和 Linux 在系统原理上有很大不同，所以系统信息收集所要做的测试也不相同。Windows 下主要测试了服务、文件系统、配置信息、注册表等信息；Linux 下主要测试了文件信息、网络、进程、rpm 包和硬件等。

(2)确定安全漏洞

把第一步的测试结果与 OVAL 定义文件 definitions.xml 中的漏洞定义相比较，以确定主机的安全漏洞。程序依次读入 OVAL 的定义文件中的 definition 项，这里每个 definition 都是一个关于漏洞的描述。然后程序分析每个 definition 中的 criteria 项，从之前测试结果的文件中找出相关的所有测试，并判断测试真假，最后根据 operator 运算符来确定 criteria 的结果是否为真，如果是真则判定漏洞存在。

(3)输出检测结果

以 OVAL 定义的格式输出漏洞扫描结果。图 4 是检测代理在 Windows 下的图形界面。可以看到，界面左边主要是参数设置和界面管理，右边区域显示了扫描器当前的状态，通过这里的信息提示能了解当前漏洞扫描进行的状况。

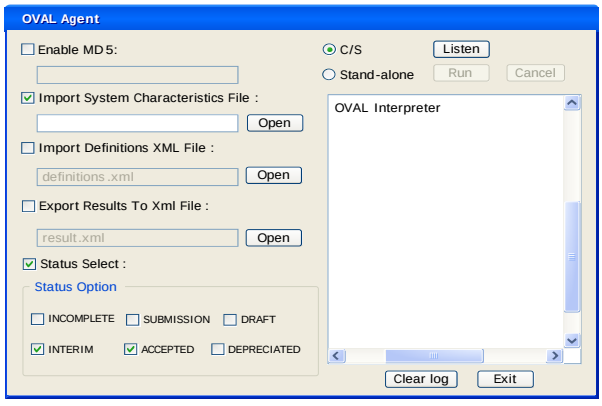

图 4　Windows 下检测代理的图形界面

3.2 控制台实现

控制台的主要功能是远程控制扫描过程和结果汇总处理，方便操作者进行阅读和总计，也是以后制定相应安全策略工作的基础。控制台通过 TCP/IP 协议与各个检测代理进行多线程并行的通信，可同时向多个代理发起扫描请求，也可以同时接收多个检测结果文件，各个检测代理分别扫描自身漏洞并上传结果，相互之间没有影响。凡是检测成功并且将结果传回的代理，在控制台端主机的磁盘上都会有其漏洞信息文件的纪录。在控制台查看结果时通过输入 IP 地址显示相应的主机的漏洞信息。如图 1 右边部分所示，由如下几个模块来实现其功能：界面管理模块，通信模块，数据处理模块。

3.2.1 界面管理模块

根据系统设计的要求，为方便用户的操作，控制台端运行于 Windows 操作系统，利用图形界面简化参数的设置和系统的控制工作，选择 MFC 开发环境进行控制台端程序设计。为了易于操作并且界面友好，同时使扫描配置过程更简单有效，控制台提供了指定 IP 或 IP 段的主机扫描，显示连接状态和错误报告等功能。

3.2.2 通信模块

控制台与检测代理之间是一对多的通信模式，因此可以对局域网内的单个主机或者某个网段内的所有主机同时发起扫描漏洞的命令。这里利用 Socket 安全套接字来完成通信。Socket 是应用程序与 TCP/IP 协议交互的编程接口，主要用于开发 Client/Server 方式的应用程序。Window 和 Linux 的 C++ 都有非阻塞式的 Socket 通信，运用快速安全的 TCP/IP 协议，完成数据流的传输。

开始时，目标主机处于侦听状态时，控制台主机创建一个套接字 Socket，通过调用函数 connect()连接目标主机，如果目标主机接受请求以后，就返回给控制台主机，并开始进行文件传输操作，完成了一次完整的 3 次握手过程。否则，在等待超时以后，结束连接并返回失败信息。

速度在大量的端口扫描与数据接收处理中是主要考虑的因素。对每个目标端口及数据接收采用线性的方式，使用单独的连接与接收调用，将会花费相当长时间。Socket 可通过同时打开多个套接字来接收数据，因此可考虑采用多线程方式进行扫描，充分利用 CPU 资源，加快扫描速度。下面是多线程 Socket 通信的主要过程 :向多个检测代理发起扫描命令，为每一个连接都开辟了一个线程，每个线程相互之间不影响，而主线程也可以同时并发执行。在连接开始前，每个检测代理处于不断侦听的状态，当接收到来自控制台的连接请求，就会开始执行扫描漏洞任务。当某个检测代理完成漏洞扫描之后，会把结果文件传回控制台，并由控制台接收后保存在本地，供用户浏览查看或者进一步的分析。

3.2.3 数据处理模块

CVE 漏洞库是目前较为全面和公认的漏洞集合，因此漏洞信息以 CVE 定义的漏洞格式来显示。由代理端发送 CVE 漏洞号到控制台，控制台端以 CVE 漏洞库作为数据库，提供详细的漏洞信息。由于整个系统的设计思想之一是跨平台操作，因此用 XML 作为数据进行存储和操作是很好的选择。

调用微软类库msxml.dll，可以方便地把XML文件解析成树的结构，同时还提供各种功能强大的查询函数。本文写了一个XmlProcess类，来调用msxml.dll中的函数，实现根据CVE漏洞号查询正确的CVE漏洞定义的XML文件[4]，并准确找到相应的漏洞信息，然后以树的形式显示出来。同时还提供一种网页显示的漏洞信息，即IE根据结果定义XML文件的格式写成的XSL文件，解析和显示由代理端传回的结果XML文件。

4 系统测试

由 4 台配置为 P4 2.4 GHz 的计算机构成测试系统。以 192.168.33.23 作为控制台主机，192.168.33.25 和 192.168.33.26 作为 Windows XP 代理端，192.168.33.24 作为 Linux Redhat 代理端测试了系统性能。

首先 3 个代理开始侦听，然后 192.168.33.23 控制台主机向 3 个代理同时发送命令，3 个代理侦听到以后分别开始在本机上搜集漏洞信息。检测完成后，通过控制台查看到了 Linux 代理机上发现的 100 个漏洞的 CVE 漏洞信息，以及分别在 2 台 Window 代理机上发现的 15 个和 20 个漏洞的 CVE 漏洞信息。表 1 给出 192.168.33.25 主机的系统信息和检测到的部分漏洞信息。

表 1 部分漏洞信息

IP 地址	主机名	操作系统	平台
192.168.33.25	lwy	Microsoft Window XP Professional Service Pack 2	INTEL32
OVAL 编号	CVE 编号	描述	
OVAL 100100	CAN-2005-1982	Unknown vulnerability in the PKINIT Protocol could allow a local user to obtain information and spoof a server via a Man-In-The-Middle(MITM) attack between a client and a domain controller when PKINITsmart card Authentication is being used.	

5 结束语

随着网络技术和信息安全技术的发展，信息对抗不断加剧，漏洞扫描与检测技术也需要不断完善与提高，以适应新的需要。本文中所提供的新型漏洞检测系统是一种主动式的漏洞检测工具，它在不影响被测主机性能的情况下实现远程和大范围的扫描，还能对多种平台下的主机进行漏洞扫描。由于采用 C/S 模式，因此远程控制扫描过程和结果汇总处理能力较强。因为采用 OVAL 和 CVE 这 2 个相兼容的漏洞定义库，所以系统升级方便，并且检测结果也较为详细，通用性强。

目前，这个漏洞检测系统的检测代理仅支持 Windows 和 Linux 操作系统，控制台生成漏洞结果报告形式还不够全面，这些都还需要进一步改进。另外，在已知各目标主机的漏洞的基础上，通过攻击路径构建和关键路径分析给出相应的最佳安全策略，这将在以后的工作中展开，进一步完善整个网络安全评估系统。

参考文献

[1] 谈基于网络和基于主机的漏洞扫描[Z]. (2004-11-15). http://channel7.cn/2004/11-15/10574.html.

[2] 林晨光. 网络安全检测与评估系统的研究与实现[D]. 西安: 西安交通大学, 2005.

[3] The MITRE Corporation. About Open Vulnerability Assessment Language[EB/OL]. (2007-01-05). http://oval.mitre.org/oval/about/index.html.

[4] 孙一中. XML 理论和应用基础[M]. 北京: 北京邮电大学出版社, 2000.