doi:10.3969/j.issn.1000-436x.2014.z1.003

校园网服务器安全扫描告警系统的设计与实现

庞滨[1]，李华[1,2]，王友义[2]，闫帅[2]，杨智和[2]
（1. 内蒙古大学 网络信息中心，内蒙古 呼和浩特 010021；2. 内蒙古大学 计算机学院，内蒙古 呼和浩特 010021）

摘 要：提出了一种利用开源的安全检测工具构造校园网服务器扫描告警系统，对需要监控的服务器进行定时扫描，将发现的威胁进行自动分析，并报告管理员。通过对服务器进行从硬件到软件，从操作系统到服务进程以及动态页面脚本的多方面、可定制、灵活组合的定时安全扫描，构建对服务器全方位的检测并搜集扫描结果进行分析，将告警信息直接通过邮件等形式发送给管理员，并提出修补建议，以此达到对服务器安全漏洞的抢先发现，及时修补的目的。实验结果表明，通过建立安全漏洞扫描告警系统，将校园网服务器的安全提升到了一个比较可靠的程度。

关键词：校园网；安全漏洞；4 层架构；扫描告警
中图分类号：TP393.08 **文献标识码**：A **文章编号**：1000-436X(2014)Z1-0010-04

Design and implementation of server security alarm system in campus network

PANG Bin[1], LI Hua[1,2], WANG You-yi[2], YAN Shuai[2], YANG Zhi-he[2]
(1. Network and Information Center, Inner Mongolia University, Hohhot 010021, China;
2. School of Computer Science, Inner Mongolia University, Hohhot 010021, China)

Abstract: A safety test using open source tools was put forward to construct four layer network scan architecture pattern for monitoring server safety, it also can get an automatic analysis report of threaten for the administrators. Through the timing detection mechanism based on process from hardware to software, from the operating system to the service application even to the dynamic page script to build a full range, customizable，flexible combination of multi-level security scan and collect the results which are analyzed, the results are directly sent the mail to the administrators, and the suggestions for repair are put forward. Therefore, the server security vulnerabilities can be found and the purpose of repair can be achieved in time. And this method can reduce the burden of manual detection monitoring server for administrators, and effectively avoid security problems for administrators' technical reasons. Finally the experimental results also show that the establishment of security vulnerability scanning alarm system will make the security of campus network servers more reliable than before.

Key words: campus network; security vulnerabilities; four-layer architecture; scan and alarm

1 引言

随着高校校园网的普及，校园网络各种服务也逐渐在完善和增多，如面向互联网的网站、邮件系统、教务系统等，以及面向校园内部的一卡通、学籍、财务、办公等服务系统等。由于各个高校管理机制的差异，大部分提供各种服务的系统分属不同部门、科系，并且各种服务开通的时间不同、服务器的型号、所使用的操作系统、提供应用的软件等等差异也非常大，同时各个部门管理人员技术水平参差不齐以及工作分工、精力分配等问题，不可能长时间关注各种网络服务的运行情况是否是安全

收稿日期：2014-10-15
基金项目：国家自然科学基金资助项目(61163011)；内蒙古自然科学基金项目(2012MS0922)
Foundation Items: The National Natural Science Foundation of China (61163011); The Natural Science Foundation of Inner Mongolia (2012MS0922)

的。因此，如何及时发现校园网各个服务器的漏洞并加以防范也成为越来越重要的实用研究课题。

随着高校网络建设的深入，网站等服务器平台已从一个简单的信息发布、展示平台，逐步转变为汇集了招生就业、远程教育、成果共享、招标采购等功能的综合性业务平台。高校网站已积聚了教育信息化建设中大量的信息资源，成为高校成熟的业务展示和应用平台，对于它的攻击者可能来自于内部和外部两方面。近年来针对高校网站的攻击热点已经从单纯的网站攻击行为衍生到有目的组织的网页篡改、攻击利益链模式，许多高校都遭受了形象及经济方面的损失。

根据近几年网络安全事故的分析[1]，发现网络安全漏洞造成损失主要和以下几个因素有关。第一，网络服务器负责管理人员发现漏洞不及时。第二，对设备的软硬件没有及时升级打补丁使得黑客有机可乘。第三，很多管理员对网络技术并不熟悉。因此急需开发一套针对高校校园网可行的、对于大多数管理员可以接受的实用的网络服务器安全漏洞扫描告警系统，保护高校校园网络不受大部分可预防攻击的侵害，减轻网络管理员的负担，同时加强网络服务的健壮性和可用性，不会因为网络基本安全漏洞造成大范围长时间的断网、无法提供服务问题。以前的漏洞扫描工具可以分为自主设计或者二次开发。本次设计将二者思路结合，基于 Kali Linux [2]提供的扫描工具进行信息收集，设计生成扫描脚本，在此基础上使用 Linux 系统提供的定时轮询机制 Crontab 对指定的服务器扫描条目进行检查，执行对应的自行设计的扫描脚本，将扫描成果获得的信息进行保存。本次设计的宗旨是对监控服务器信息的维护做到最大限度的灵活，并减轻管理人员大量重复工作。

本文主要贡献如下。1) 对于服务器设计了 4 种扫描机制包括硬件扫描，即对服务器硬件是否做过替换或更改，服务器是否仍然存活并正常工作进行探测；操作系统扫描，即对服务器所安装的操作系统进行检测，包括操作系统的类型、版本、内核版本、补丁信息等进行扫描；服务器所使用的服务程序信息扫描，包括使用的服务程序的名称、版本、打开的服务端口号等进行扫描分析，针对不同的服务应用提供有针对性的扫描和分析；站点脚本的扫描分析，各个站点使用的脚本语言、服务机制以及后台数据库等也各不相同，需要灵活的根据站点所采用的脚本来调整实用的扫描工具和扫描方式。这 4 种机制可以灵活组合、自由定制、自由切换。2) 在设计之初考虑了系统的可扩展性、可用性及实用性。例如可以提供及时扫描，易于集成各种其他安全扫描工具。3) 对于扫描结果给出了进一步的分析整合、具有个性化定制服务的特点。

2　网络服务扫描告警系统设计

2.1　需求分析

在网络中，所有的应用程序都存在服务器上，因此必须对其进行有针对性的安全检测与管理。一般服务器上提供应用服务系统的不安全来源主要可能来自内部和外部两方面。内部主要来源于管理人员的疏忽和技术手段的限制，以及管理员因为没有及时关注操作系统以及服务程序的漏洞公告进行及时地打补丁等工作给攻击者造成可乘之机。对于外部威胁来说，主要需防范大范围的针对特定服务端口的扫描攻击和发布在公共网络上站点的脚本漏洞攻击，如果管理人员能够利用一些更新及时的站点扫描工具预先扫描，发现漏洞及时补上，也可以防范朱大部分的外部攻击。这样就能够使整个服务器做到很大程度的安全。同时为了使漏洞扫描对服务器繁忙时不增加服务期负担，但又保证检测的有效性，需要设计可以设定时间、设定轮询方式的检测机制，达到高效率低影响的监测效果。

本系统架构大体由 3 部分构成：按需扫描、结果分析、告警服务。按需扫描主要对被监控的服务器按照设定的时间点和时间周期按对应服务内容进行安全漏洞扫描，本次先设计 4 种扫描，可以依据需要扩展扫描方法，例如以后可以加入云技术支持的扫描工作。系统的结构设计如图 1 所示。

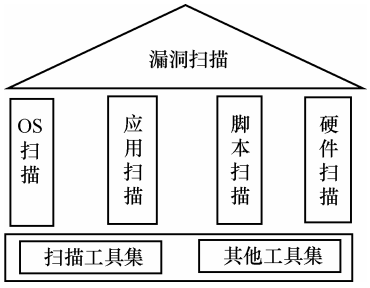

图 1　系统架构

上述 4 种扫描可以灵活进行组合和定制，形成

一个立体的对于特定服务器的安全漏洞扫描体系，可以在一个服务器上根据不同的时间点和不同的时间频率来设计全套的扫描计划，也可以根据需要只设定扫描服务器是否还正常工作，有无响应即可。

2.2　系统工作流程设计

整个系统的工作流程设计如下。首先进行服务器自然信息的搜集保存到数据库，通过这些搜集的信息建立服务器进行下一步安全漏洞扫描的基准数据，比如记录中服务器本不应该打开的端口被扫描发现打开了，很有可能已经被安装后门程序。第二，对需要集成进入系统的扫描工具进行命令参数的脚本生成以及运行环境设定，保证扫描程序针对特定服务器均能正常运行并返回结果。第三，对扫描服务器和对应脚本建立扫描记录，并按时间进行调度，系统的调度程序每隔一定时间唤醒一次，对设定的扫描任务进行读取并执行相应的扫描脚本，执行完脚本后搜集结果并保存，再取下一条任务直到所有设定的任务执行完毕。最后将扫描结果进一步的分析提取结果报告管理人员，提供可选的方式通知管理人员对安全漏洞进行进一步的处理。本系统的流程设计如图 2 所示。

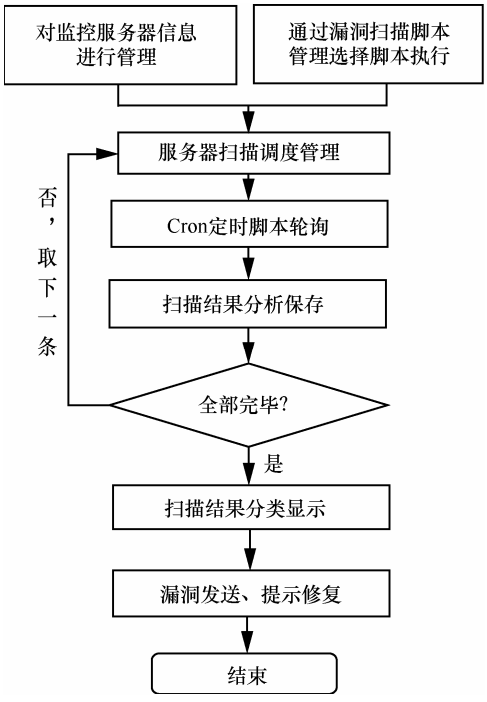

图 2　系统流程

如此反复直到所有服务器的扫描任务都被执行，执行的流程灵活性高，可以提高对于新型漏洞的反应速度和效率。

2.3　服务器收集信息设计

整个系统的第一步是对所管辖范围内的服务器进行自然信息的搜集，一个服务器需要搜集的信息设计如表 1 所示。

表 1　　服务器自然信息

字段	说明
ID	唯一标识
服务器描述	文字性描述
所属单位	属于哪个部门如党办
文存放位置	本地存放还是托管到中心
管理人员	服务器具体管理者
管理者电话	手机
管理者邮箱	必填，发送安全信息
服务器型号	判断合法基础
服务器网卡数量	检测基础
服务器每网卡 MAC	检测基础
服务器每网卡 IP	检测基础
服务器 OS	检测基础
服务器使用服务程序	是 ASP PHP JSP Apache IIS 等
服务器开放端口	检测端口是否过多开放
服务器安装数据库	监测数据库漏洞

搜集到上述信息后，同上述服务器的自然信息进行比对，如果发现扫描结果和数据库记录服务器的自然信息不匹配，则应进一步的分析是正常升级维护还是非正常被篡改，如果是后者需要进行报警处理。

2.4　智能扫描分析告警方法

在系统轮询结束后，需要将获得有效信息全部保存到数据库中，接下来系统将扫描软件返回的大量信息，通过相应的软件工具，比如支持正则表达式的 awk、sed 等工具，按照规则切出有用的信息，保存到数据库对应的表格里。当管理员登录系统时，系统会在今日提示页面将警告信息以人性化的可读形式按照日期和重要程度进行排序后显示给管理人员，并且在每条警告的后面给出处理此类告警信息的处理方法的链接，同时如果此服务器的管理人员属于学校的其他部门，则在条目最后提供按钮，提示是否发送给服务器具体管理员邮件，提示管理员进行漏洞的进一步处理。

3　示例实现

为了验证本文设计的可行性，完成了一个 Web 服务器漏洞扫描告警系统实现示例，当管理员登录系统后，系统会按照时间和安全事件的重要程度对

所扫描的服务器进行显示，提醒管理员注意。如图 3 所示，经过一段时间运行，结果显示整个校园监控下的 Web 服务器安全性能有明显的提高。

图 3　系统实现截图

4　相关工作介绍

Kali Linux 是一个高级渗透测试和安全审计 Linux 发行版，集成了精心挑选的渗透测试和安全审计的工具，供渗透测试和安全设计人员使用，特别适合做安全漏洞测试平台或者框架，其自身的安全性比其他系统好。其他相关的安全漏洞测试工具多是针对某一网段进行无目标的扫描，或针对某一层次特定的漏洞进行，如脚本语言的漏洞[3~6]，以及针对网页某些数据包特定字段等[7]，或根据特定的需求进行专门的系统开发设计，周期长，更新缓慢、只针对特定的漏洞，还有的漏洞扫描在智能化[8,9]、集成云端技术[10]进行了有益的探索，总体还处于起步阶段，随着云技术和大数据等新兴技术的发展运用，安全扫描也正在进一步的发展与融合。

5　结束语

本文将高校网络服务器的安全漏洞分为 4 种进行防御，用来对高校这一特定环境下的各种服务器实现尽可能全方位的安全防护，并初步实现了该告警系统。目前实验表明系统的运行大大减轻了网络管理人员监控网络安全漏洞的人工负担，对网络漏洞的及时发现与修补提供了及时快速的解决方案。进一步的研究工作主要从以下 2 个方面着手：一是在保证效率的前提下，提高准确度；二是为安全监测构造更为自动化的方法。接下来还将在更大规模的平台上研究试验基于网络服务器安全监测的自动化方法。

参考文献：

[1] http://www.cert.org.cn/publish/main/46/2014/20140603151551324380013/20140603151551324380013_.html[EB/OL].

[2] http://www.kali.org[EB/OL].

[3] XIE Y C, AIKEN A. Static detection of security vulnerabilities in scripting languages[A]. 15th USENIX Security Symposium[C].2006. 179-192.

[4] Analysis of network security threats and vulnerabilities by development & implementation of a security network monitoring solution[EB/OL]. http://www.bth.se/fou/cuppsats.nsf 01/2010.

[5] 彭亚发，陈华. 基于系统漏洞扫描和防病毒技术的网络安全的设计[J]. 商情, 2013,(12):261-263.
PENG Y F, CHEN H. Network security design based on system vulnerability scanning and anti-virus technology[J]. Shangqing, 2013, 12: 261-263.

[6] 陈俊华. 网络漏洞扫描系统研究与设计[J]. 信息网络安全, 2013,(5): 64-66.
CHEN J H, Network vulnerability scanning system research and design[J]. Netinfo Security,2013,(5):64-66.

[7] FONSECA J, SEIXAS N, VIEIRA M, *et al*. Analysis of field data on Web security vulnerabilities[J]. IEEE Transactions Dependable and Secure Computing, 2014, 11(2): 89-100.

[8] SHAHRIAR H. Security vulnerabilities and mitigation techniques of web applications[A].The 6th International Conference on Security of Information and Networks[C]. Aksaray, Turkey, 2013.459-459.

[9] LI D, HONG X, WITT D. ProtoGENI, a prototype GENI under security vulnerabilities: an experiment-based security study[J]. IEEE Systems Journal, 2013, 7(3): 478-488.

[10] RISTOV S, GUSEV M, DONEVSKI A. OpenStack cloud security vulnerabilities from inside and outside[A]. The Fourth International Conference on Cloud Computing, GRIDs, and Virtualization[C]. Valencia, Spain, 2013.101-107.

作者简介：

庞滨（1978-），男，内蒙古呼和浩特人，内蒙古大学博士生，主要研究方向为计算机网络、网络安全等。

李华（1964-），女，内蒙古呼和浩特人，内蒙古大学教授，主要研究方向为网络协议测试、计算机网络、网络安全等。

王友义（1991-），男，山东临沂人，内蒙古大学硕士生，主要研究方向为计算机网络、网络安全等。

闫帅（1993-），男，内蒙古包头人，内蒙古大学硕士生，主要研究方向为计算机网络、网络安全等。

杨智和（1990-），男，内蒙古巴彦淖尔人，内蒙古大学硕士生，主要研究方向为计算机网络、网络安全等。