基于 Samba 服务器的管理体系研究与应用

王 杨[1,2,3]，王朝斌[1,2]，钟乐海[1,2]

(1. 西华师范大学 计算机学院，四川 南充 637002；2. 西华师范大学 微机应用研究所，四川 南充 637002；3. 安徽师范大学 计算机科学系，安徽 芜湖 241000)

摘 要：Samba 是一组基于 SMB 协议的应用程序。Samba 服务器能够方便地实现异构网络环境下 Windows 与 UNIX/Linux 之间的资源共享。通过对 SMB 协议的分析，提出了完整的 Samba 服务器管理体系，主要包括五个层次：操作系统管理、Samba 安全配置、访问控制、日志管理、系统备份与恢复。对于每个层次的安全策略也进行了相应的分析。最后，介绍了对 Samba 服务器实施管理的一种高效工具 Webmin。

关键词：Samba 服务器；管理体系；安全策略；资源共享

中图法分类号：TP393 **文献标识码**：A **文章编号**：1001-3695(2005)07-0248-03

Research and Application on Management Architecture and Secure Policy Based on Samba Server

WANG Yang[1,2,3], WANG Chao-bin[1,2], ZHONG Le-hai[1,2]

(1. *School of Computer, China West Normal University, Nanchong Sichuan* 637002, *China*; 2. *Microcomputer Application Institute, China West Normal University, Nanchong Sichuan* 637002, *China*; 3. *Dept. of Computer Science, Anhui Normal University, Wuhu Anhui* 241000, *China*)

Abstract: Samba is a kit of application program based on SMB protocol Samba server is often used to share resource between Windows and UNIX/Linux in the LAN with different OS. The paper proposed all-round management hierarchy including OS management, Samba security configuration, access control, log management, system backup and restore, in addition, analysis about security strategy also was preformed as to every part. Finally, introduced a kind of effective management tool named Webmin which can be used to manage Samba server.

Key words: Samba Server; Management Architecture; Security Policy; Resource Share

Samba 服务器方便了 UNIX/Linux 与 Windows 主机之间的资源共享，它不仅可以作为文件服务器，也可以作为打印服务器。对于 Samba 服务器的构建与应用已有很多文章[1,2,5]作了介绍，而对于如何高效、安全地对 Samba 服务器进行管理问题却很少讨论。当我们享受资源共享之便利时，也同时意味着承担着可能遭受攻击的风险。因为从支持 Samba 的操作系统、TCP/IP 到 Samba 服务器本身都存在着安全漏洞，尽管这些漏洞在不断地得到修正，但是未知的不安全元素无时不在。因此应用 Samba 服务器的同时，必须对其实施安全有效的管理。

1 Samba 概述

Samba 是一套使用 SMB(Server Message Block)协议的一种应用程序，通过支持这个协议，Samba 允许 Linux 服务器与 Windows 系统之间进行通信，使跨平台的互访成为可能。Samba 服务器采用客户机/服务器模式，其工作机制是让 NetBIOS(Windows 网上邻居的通信协议)和 SMB 两个协议运行于 TCP/IP 通信协议之上，并且用 NetBEUI 协议让 Windows 在“网上邻居”中能浏览 Linux 服务器。Samba 服务器包括两个后台应用程序：Smbd 和 Nmbd。Smbd 是 Samba 的核心，主要负责建立 Linux Samba 服务器与 Samba 客户机之间的对话，验证用户身份并提供对文件和打印系统的访问；Nmbd 主要负责对外发布 Linux Samba 服务器可以提供的 NetBIOS 名称和浏览服务，使 Windows 用户可以在“网上邻居”中浏览 Linux Samba 服务器中共享的资源。另外 Samba 还包括一些管理工具，如 Smbclient, Smbtar, Testparm, Smbpasswd 等程序。Samba 服务器可实现如下功能：WINS 和 DNS 服务；网络浏览服务；Linux 和 Windows 域之间的认证和授权；UNICODE 字符集和域名映射；满足 CIFS 协议的 UNIX 共享等。SMB 协议与其他协议之间的依赖关系如图 1 所示。

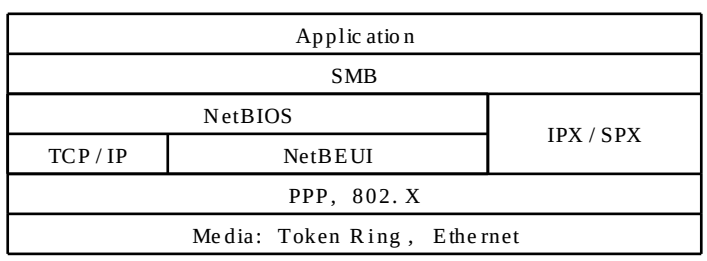

图 1 SMB 与其他协议之间的依赖关系

2 SAMBA 服务器的安全管理体系

通过对 SMB 协议的分析，对 Samba 服务器的管理内容应包括操作系统的安全管理、Samba 的安全配置、共享资源的控制管理、日志管理等内容，如图 2 所示。

由于 Samba 服务器运行在 UNIX/Linux 系统上，对操作系统的管理是管理 Samba 服务器的基础。其中 TCP/IP 协议的不安全[4]带来 Samba 服务器管理上的难度。用户认证功能可由

收稿日期：2004-04-17；修返日期：2004-09-04

Samba 服务器自身提供,也可由代理认证服务器完成。访问控制的管理是对共享资源的读、写等控制。日志管理和系统备份与恢复是当系统受到攻击后的管理措施。

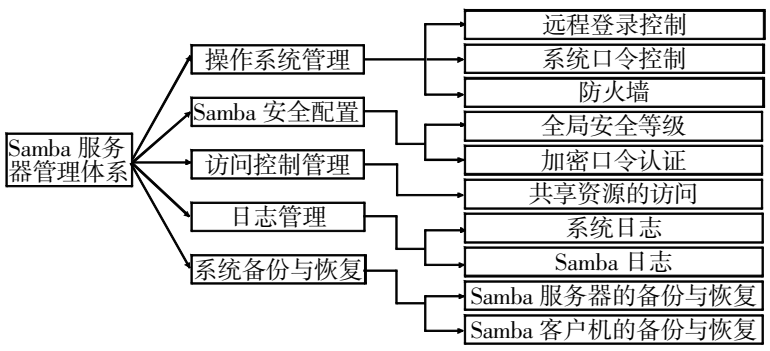

图 2　Samba 服务器的管理体系

3　Samba 服务器的安全管理策略

3.1　操作系统的安全防范

由于 Samba 服务器运行在 UNIX/Linux 平台和 TCP/IP 协议之上,因此操作系统的漏洞和 TCP/IP 不安全会带来 Samba 的不安全。如何加强系统管理以防范攻击,有很多文献可供参考[3,4]。此外, UNIX/Linux 中提供了防火墙保护来加强系统安全性能。在 Samba 服务器的管理过程中,如果防火墙设置不当,将会导致 Samba 用户找不到访问路径等问题。

3.2　用户认证管理

3.2.1　Samba 用户

Samba 服务器在使用过程中,经常涉及三类用户: Windows 用户、UNIX/Linux 用户、Samba 用户。Samba 用户是 Windows 用户与 UNIX/Linux 用户的共同包含的部分,但要注意这样几点: ①只有 Samba 用户才可以合法使用 Samba 服务器。②Samba 用户必须首先是 UNIX/Linux 用户,反之不一定成立。③将 UNIX/Linux 用户转换为 Samba 用户时,名称可以改变。④Samba 用户可以不是 Windows 用户。此时当 Windows 主机对 Samba 服务器(全局安全等级不是 Share) 访问时,如果当前 Windows 账户所用的用户名和密码与 Samba 服务器上的不同,就会出现连接对话框,要求输入 Samba 的合法用户名与密码。下面以 Linux 为操作平台,介绍如何添加 SMB 用户。

(1)　dduser user1//添加 user1 为 Linux 用户

　　passwd user1//设置 user1 的密码

(2) smbadduser user1: user1　//将 Linux 用户 user1 转换为 Smb 用户,名称改为 user1。为了解决两种系统的用户名之间不匹配的问题, Samba 服务器采用建立映射表的方法实现[7]。Samba 服务器定义的所有用户映射关系保存在文件/etc/samba/user. map 中,可以使用 VI 编辑。建立映射的格式是: samba 用户名 = Windows 用户名。这样当 Windows 客户机提出服务请求时, Samba 服务器若发现当前的 Windows 用户不是 Samba 用户,就去查找映射表,提高了客户机的访问效率。

3.2.2　Samba 用户的安全等级

(1) 安全等级

Samba 中可以设置四种安全等级[5],从低到高分别为: Share, User, Server, Domain。Share 模式下用户访问 Samba 服务器不需要提供用户名和口令,安全性能较低; User 是 Samba 服务器默认的安全等级,每一个共享目录只能被一定的用户访问,并由 Samba 服务器负责检查账号和密码的正确性; Server 为服务器安全级别,依靠其他 Windows NT/2000 或 Samba 服务器来验证用户的账号和密码,是一种代理验证 Server 为服务器级安全,此种安全模式下,系统管理员可以把所有的 Windows 用户和口令集中到一个 NT 系统上,使用 Windows NT 进行 Samba 认证,远程服务器可以自动认证全部用户和口令,如果认证失败, Samba 将使用用户级安全模式作为替代的方式; Domain 为域安全级别,使用主域控制器(PDC) 来完成认证。要想安全管理 Samba 服务器,后两种方式具有较强的安全性,尤其是 Domain 等级。为更好地说明问题,下面以 Server 安全等级方式的认证机制为例加以介绍。

(2) Server 安全级别的认证机制

Server 安全级别可以充分利用已有网络中已存在的服务器资源来进行用户认证。使用 Server 安全级别时,必须同时使用全局参数 password server。password server 可以指定一台机器,也可以是以逗号分隔的计算机列表或* ,* 号由 Samba 服务器去尝试定位网络中的主/备份/控制器。采用这种方式时,需要先将 Samba 服务器配置文件 smb. conf 中的[global] 节作如下修改: Security = server

password server = 210. 41. 196. 10　//这是作为 password server 的机器的 IP 地址,也可以用机器名。这种方式的具体认证过程如下:

①Windows 客户机向 Samba 服务器发出服务请求。

②Samba 服务器验证 Windows 当前用户是否为合法 Samba 用户,若不是,出现连接窗口,请求输入合法的 Samba 用户名和密码。

③将合法的 Samba 用户名和密码提交给 Samba 服务器。

④Samba 服务器判断认证服务器是否启动并正常工作,若为否,由 Samba 服务器按照 User 安全等级进行用户验证及服务,否则,将用户名及密码提交给 password server。

⑤password server 将验证后得到的 Token 令牌返回 Samba 服务器。

⑥Samab 服务器再将验证的 Token 令牌返回 Windows 客户端。

⑦Windows 客户端得到 Token 令牌后,访问 Samba 服务器。

3.2.3　基于口令的认证

在 Windows 95 及以前的版本中,在访问 Samba 服务器时使用普通的明文密码,从而造成很大的安全漏洞。从 Windows 98 和 Windows NT 4.0 SP3 之后的 Samba 客户机均使用加密的口令认证方式,但 Samba 服务器无法区分明文密码和加密密码,口令在网络上明文传输的安全漏洞问题仍然存在。解决这个问题的最好方法是让 Samba 支持加密口令认证,使用独立于 Linux 系统口令文件之外的认证系统,表示在进行身份认证时,要对用户的密码进行加密。RedHat 中的 Samba 软件包已经预先编译成支持加密口令认证功能,可直接使用。为使 Samba 服务器识别加密的口令,须对配置文件中全局部分的 security, encrypt passwords, null passwords, smb password file 四个参数进行设定,见如下(以 user 安全等级为例) :

```
Security = user
encrypt passwords = yes
null passwords = no
smb password file = /etc/samba/smbpassword
```

Samba 服务器也允许使用未经加密的用户密码,但既麻烦又不安全[1]。

3.3 资源访问控制管理

经过身份认证表明该用户是一个合法的 Samba 用户,但对于 Samba 服务器上共享资源是否能够访问及访问的方式,Samba 服务器可以通过资源控制进行管理。资源控制管理主要考虑三个层面:①UNIX/Linux 系统中的哪些资源可以共享。②共享的资源对哪些主机或用户开放。③用户对共享资源的使用设置何种访问权限。对三个层面的管理主要通过设置 smb.conf 中的对应参数,如表 1 所示。限于篇幅,对于参数的具体含义可参见文献[5~7]。

表 1 资源控制管理三个层面的相关参数

层面一的参数	层面二的参数		层面三的参数
[客户机上显示的目录名]	admin users	allow trusted domains	writeable
path	host allow	host deny	browseable
comment	public	guest ok	read only
available	only guest	valid user	printable
	invalid user	write list	

3.4 日志管理

日志分为系统日志和 Samba 日志。日志中记录了大量有利于管理的信息。系统日志的设置与管理可参阅 UNIX/Linux 有关文献。这里主要讨论 Samba 的日志管理。Samab 服务器的日志用于记录 Samba 的使用情况,设置恰当的日志参数可以对 Samba 服务器进行事后监督,并进一步提高管理水平。在 smb.conf 的[global]节中可以设置有关日志参数[7]。

3.5 系统备份与恢复

当 Samba 服务器出现问题后,用户希望尽快恢复系统,使之正常工作。做到这一点,应当在 Samba 服务器正常工作时,对系统进行备份,以防患于未然。系统备份的方式可以通过本地完成,也可以远程操作。备份内容的选择上既可以是整个系统,也可以是仅与 Samba 服务器有关的配置文件和日志文件。完成备份工作后,一旦 Samba 服务器出现问题,就可以及时恢复。Samba 客户机的备份相对较简单,因为 Samba 对客户机只要求支持 TCP/IP,有必要的情况下,可对 Windows 用户进行备份。最后,着重介绍一下系统管理与维护工具的选取。以往在局域网内对 Samba 服务器的管理进行远程“遥控”时,需要在本机上手动对系统中的通信协议进行参数设置,这种方法不仅需要大量的时间进行安装和调试,而且维护工作也非常烦琐。并且常用的 Telnet 等命令是一种基于字符的应用程序,对于远程系统操作时很不方便。比较优秀的系统及 Samba 服务器管理工具有 Linuxconf 和 Webmin,推荐使用 Webmin 来管理 Samba 服务器。Webmin 是一个基于 Web 的 Linux 系统管理工具,功能强大,操作界面非常友好,安全性较高[7],是一个理想的对 Samba 服务器和 UNIX/Linux 系统进行远程管理的有力工具。在 Samba 服务器上安装 Webmin 后,既可以在本地实施操作,也可以远程操作,方法如下:

(1) 选取与 Samba 服务器联网的任何一台远程机器(Windows 系统或 UNIX/Linux 系统)。

(2) 在 Web 浏览器(IE 或 Mozila 等)地址栏中输入 Samba 服务器的主机地址及端口号,如 http://210.41.196.1:10000(Webmin 的默认端口),此时出现 Webmin 系统管理员 Admin 的认证窗口。

(3) 输入正确的用户名及密码,认证通过后,就可以使用 Webmin 图形化远程网络管理界面对 Samba 服务器进行管理与维护。

4 结束语

处于异构网络中的 Samba 服务器,方便了 Windows 和 UNIX/Linux 系统之间的资源共享,但是无法保证它的绝对安全,尽管它需要安全。因此,有效地对 Samba 服务器进行管理,将能够在很大程度上减少不安全的因素。为了使 Samba 服务器更加安全,有必要构建系统完整的 Samba 服务器管理体系,并从各个层次实施安全管理策略。在具体应用过程中,用户可以根据不同的安全要求,定制不同的安全管理方案。使用 Samba 服务器不仅应用方便,而且安全可靠。

参考文献:

[1] 邹念,唐宁九,林锋.用 Samba 实现 Linux 和 Windows 之间的文件共享[J]. 计算机应用研究,2002,19(1):152-153.

[2] 韩德志,鄢让.利用 Samba 实现 Linux 与 Windows 98 的资源共享[J]. 计算机应用研究,2001,18(5):131-134.

[3] 陈旭,温阳东. Linux 系统网络安全问题分析及对策[J]. 合肥工业大学学报 2002,25(3):396-397.

[4] Dominic Baines. Samba 技术内幕[M]. 沈立,等. 北京:机械工业出版社,2000.

[5] 谭良,等. Samba 服务器共享资源安全层次模型研究[J]. 计算机应用,2004,24(2):115-117.

[6] 肖文鹏. 高效架设 RedHat Linux 服务器[M]. 天津:天津电子出版社,2003.

[7] 宋利军. RedHat Linux 9.0 实用教程[M]. 北京:科学出版社,2003.

作者简介:

王杨(1971-),男,安徽芜湖人,讲师,在读硕士生,主要从事计算机网络技术研究;王朝斌(1970-),男,重庆忠县人,讲师,在读硕士生,主要从事计算机网络技术研究;钟乐海(1963-),男,四川广安人,教授,硕士生导师,博士,主要从事计算机网络教学和研究。

(上接第 245 页) 采用 UTF-8 的编码方式,因此支持中文,一般一个中文字符由三个字节表示。

4 小结

本文针对目前对即时通通信监控的需要,对 ICQ, AIM, MSN 和雅虎通等几个主流即时通软件最新版本的文本消息传输协议进行了分析、比较和说明,为进一步对这些软件的文本消息监控提供了依据,同时为这些软件协议的进一步深入分析,如文件传输、音频消息传送、视频数据传送、文件共享等协议的分析提供了参考。

参考文献:

[1] SCAR (ICQ v7/v8/v9) Protocol Documentation[EB/OL]. http://iserverd1.khstu.ru/oscar/families.html, 2003-06-13.

[2] Yahoo Messenger Protocol(v10)[EB/OL]. http://www.venkydude.com/articles/yahoo.htm, 2003-09-01.

[3] MSN Messenger Service 1.0 Protocol[EB/OL]. http://www.hypothetic.org/docs/msn/sitev1/index.php, 2003-09-02.

作者简介:

李远杰(1972-),男,讲师,硕士研究生,主要研究方向为网络安全、软件理论与应用;刘渭锋(1978-),男,硕士研究生,主要研究方向为软件理论与应用、网络安全;张玉清,副研究员,主要研究方向为网络安全;梁力,副教授,硕士生导师,主要研究方向为软件理论与应用。