文章编号: 1008-1542(2007)03-0234-04

校园网中 Linux 系统安全与管理

孟军英[1], 朱艳红[2], 赵 艳[3]

(1. 石家庄学院计算机系, 河北石家庄 050035; 2. 石家庄邮电职业技术学院计算机系, 河北石家庄 050021; 3. 河北科技大学信息科学与工程学院, 河北石家庄 050054)

摘 要: 校园网作为学校重要的基础设施, 其安全状况直接影响着学校的教学活动。Linux 是一个开放式系统, 可以在网络上找到许多现成的程序和工具, 这既方便了用 Linux 系统的校园网用户, 也给黑客提供了入侵的便利。介绍了 Linux 系统功能的一些设定方法, 以及日常需要采取的一些防护措施, 为提高 Linux 系统的安全性提供一些建议。

关键词: 校园网; Linux; 安全管理

中图分类号: TP391 文献标识码: A

Security and management of Linux system in the campus network

MENG Jun-ying[1], ZHU Yan-hong[2], ZHAO Yan[3]

(1. Department of Computer, Shijiazhuang University, Shijiazhuang Hebei 050035, China; 2. Department of Computer, Shijiazhuang Post and Telecommunication Technical College, Shijiazhuang Hebei 050021, China; 3. College of Information Science and Engineering, Hebei University of Science and Technology, Shijiazhuang Hebei 050054, China)

Abstract: Campus network is the most important part of the college, and its safety status directly influences the teaching activities. Meanwhile, Linux is an open system, and many programs and development tools for it could be found from Internet. This status not only brings great convenience, but also opens a gate for the hackers. This paper introduces some setting methods of Linux system functions, and some protective measures in routine maintenance. It also puts forward some advice on strengthening the security of Linux system.

Key words: campus network; Linux; security management

1 校园网的特点及安全威胁

现在 TCP/IP 协议广泛用于各种网络。但是 TCP/IP 协议起源于 Internet, 而 Internet 在其早期是一个开放的为研究人员服务的网际网, 是完全非赢利性的信息共享载体, 所以几乎所有的 Internet 协议都没有考虑安全机制。网络不安全的另一个因素是因为人们很容易从 Internet 上获得相关的核心技术资料, 特别是有关 Internet 自身的技术资料及各类黑客软件, 很容易造成网络安全问题。

校园网是以教学活动为中心的, 网络的安全问题也有自己的特点。主要表现为不良信息的传播、病毒的危害、非法访问、恶意破坏、口令入侵等。校园网的安全主要可以归结为 2 个方面: 一个是网络方面的, 另一个是系统方面的。解决网络平台安全问题的安全措施包括防火墙、Internet 访问控制管理、通用网络计费、防病毒网关、基于网络的实时入侵检测系统等。解决系统平台的安全问题, 安全措施包括对主机操作系统的安全配置、安全漏洞扫描和评估、网络防病毒体系、网站监控与恢复系统等。同硬件系统相比, 软件系统的安全问题是最多的, 也是最复杂的。

收稿日期: 2007-01-26; 修回日期: 2007-06-08; 责任编辑: 李 穆

作者简介: 孟军英(1974-), 男, 河北晋州人, 工程师, 硕士, 主要从事计算机网络及嵌入式系统方面的研究。

Linux 是 Unix 的克隆或 Unix 风格的操作系统。在源代码级上兼容绝大部分 Unix 标准, 是一个支持多用户、多进程、多线程实时性较好的功能强大而稳定的操作系统。它可以运行在 x86PC, sun sparc, Digital Alpha, 680x0, powerPC, MIPS 等平台上, 可以说 Linux 是目前可运行于硬件平台最多的操作系统[1]。由于 Linux 是一个开放源代码的免费操作系统, 使得用户能够不用花钱就能得到 Linux 的很多版本以及为其开发的应用软件, 可以满足校园师生的探索和交流要求, 因此校园网中 Linux 操作系统非常普及, 校园中学生的好奇心、试探欲给校园网带来了很多安全问题, 也使得 Linux 系统的安全面临各种风险。

2　Linux 系统的安全措施

即使普遍认为较安全的 Linux 系统, 也就需要系统管理员针对校园网的特点仔细设定 Linux 的各种功能, 采取适当的安全措施来防护系统[2~5]。

2.1　加强用户安全

1) 口令的设置　口令的设置可以说是系统的第 1 道防线, 目前网上大部分对系统的攻击都是从截获或猜测口令开始的, 一旦黑客进入了系统, 那么前面的防卫措施几乎就没有作用。所以对口令进行安全管理可以说是系统管理员的重要职责。

目前大多数的 Linux 系统都将用户帐号信息和加密口令分开存放, 在 /etc/passwd 文件中不再包含加密口令, 而加密口令是存放在/etc/shadow 文件中, 该文件只有超级用户(root)可读。在这里特别需注意的是一些系统帐号, 如 uucp, ftp, news 等, 一定不要给它们设置 /bin/sh, /bin/csh 等 Shell 变量, 可以在/etc/passwd 中将它们的 Shell 变量置空, 或设为 /bin/ftponly 等。对有权使用超级用户的人员, 也不要经常以超级用户身份登录, 此外为使系统更加安全运行, 在开机前进行 BIOS 密码设置。

2) 设定用户帐号的安全等级　在 Linux 上每个帐号可以被赋予不同的权限, 因此在建立一个新用户 ID 时, 系统管理员应该根据需要赋予该帐号不同的权限, 并且归并到不同的用户组中。

在 Linux 系统上的 tcpd 中, 可以设定允许上机和不允许上机人员的名单。其中, 允许上机人员名单在/etc/hosts.allow 中设置, 不允许上机人员名单在/etc/hosts.deny 中设置。设置完成后, 需要重新启动 Inetd 程序才会生效。此外 Linux 将自动把允许进入或不允许进入的结果记录到/rar/log/secure 文件中, 系统管理员可以据此查出可疑的进入记录。

每个帐号 ID 应该有专人负责。如果负责某个 ID 的职员离职, 管理员应立即从系统中删除该帐号, 很多入侵事件都是借用了那些很久不用的帐号。

3) 超级用户帐号的管理　在用户帐号之中黑客最喜欢具有 root 权限的帐号, 这种超级用户有权修改或删除各种系统设置, 可以在系统中畅行无阻。因此, 在给任何帐号赋予 root 权限之前, 都必须仔细考虑。Linux 系统中的/etc/securetty 文件包含了一组能够以 root 帐号登录的终端机名称。

root 是 Linux 保护的重点, 由于它权力无限, 因此最好不要轻易将超级用户授权出去。但是, 有些程序的安装和维护工作必须要求超级用户的权限, 在这种情况下, 可以利用其他工具让这类用户有部分超级用户的权限。sudo 就是这样的工具, sudo 程序允许一般用户经过组态设定后, 以用户自己的密码再登录一次, 取得超级用户的权限, 但只能执行有限的几个指令。它不但限制了用户的权限, 而且还将每次使用 sudo 所执行的指令记录下来。值得一提的是 sudo 并不能限制所有的用户行为, 尤其是当某些简单的指令没有设置限定时, 就有可能被黑客滥用。例如: 一般用来显示文件内容的/etc/cat 指令, 如果有了超级用户的权限, 黑客就可以用它修改或删除一些重要的文件。

2.2　改进登录服务器

将系统的登录服务器移到一个单独的机器中会增加系统的安全级别, 使用一个更安全的登录服务器来取代 Linux 自身的登录工具也可以进一步提高安全性。

在大的 Linux 网络中, 最好使用一个单独的登录服务器用于 syslog 服务, 它必须是一个能够满足所有系统登录需求并且拥有足够的磁盘空间的服务器系统。更安全地登录服务器会大大削弱入侵者透过登录系统篡改日志文件的能力。

安全 syslog 即使使用单独的登录服务器, Linux 自身的 syslog 工具也是相当不安全的。因此, 有人开发了所谓的安全 log 服务器, 将密码签名集成到日志中, 这会确保入侵者即使在篡改系统日志以后也无法做

到不被发现。例如: 用于 Linux 的 NIS(网络信息服务) 和 Kerberos 等单一登录系统, 不仅可以减轻管理员的负担, 同时还提高了安全级别。

2.3 使用 **Linux** 的文件分区及防护系统

1) 设置文件分区 在 Linux 的文件系统中, 分别为不同的应用安装单独的主分区, 将关键的分区设置为只读属性将大大提高文件系统的安全性。这种设置主要是由 Linux 自身的 ext3 文件系统的只添加和不可变两种属性决定的。例如: 可以将文件系统分成几个主要分区, 每个分区分别进行不同的配置和安装, 一般情况下可以建立/, /usr, /boot, /var 和/home 等分区。/usr 可以安装成只读和不可变属性, 如果/usr 中有任何文件发生了改变, 那么系统将立即发出安全警报。其他的/lib, /boot, /sbin 的分区安装和设置也一样, 尽量设为只读属性, 那么对它们的文件、目录和属性进行的任何非法修改都会导致系统报警。

2) 设置文件属性 使用 ext3 文件系统上的只添加和不可变这 2 种文件属性可以进一步提高安全级别。不可变和只添加属性是 2 种扩展 ext3 文件系统的属性标志的方法, 一个标记为不可变的文件不能被修改, 甚至不能被根用户修改; 一个标记为只添加属性的文件可以被修改, 但只能在它的后面添加内容, 即使根用户也只能如此。这 2 个文件属性在检测黑客企图在现有的文件中安装入侵后门时是很有用的, 为了安全起见, 一旦检测到这样的活动就应该立即将其阻止并发出报警信息。如果你的关键的文件系统安装成只读的并且文件被标记为不可变的, 入侵者必须重新安装系统才能删除这些不可变的文件, 但这会立刻产生报警, 这样就大大减少了被非法入侵的机会。

3) 保护 log 文件 当 log 文件和 log 备份一起使用时, 不可变和只添加这 2 种文件属性特别有用。系统管理员应该将活动的 log 文件属性设置为只添加。当 log 被更新时, 新产生的 log 备份文件属性应该设置成不可变的, 而新的活动的 log 文件属性变成了只添加。一般需要在 log 更新脚本中添加一些控制命令来达到目的。

2.4 定期对服务器备份

在完成 Linux 系统的安装以后应该对整个系统进行备份, 以后可以根据这个备份来验证系统的完整性, 这样就可以发现系统文件是否被非法篡改过。除了对全系统进行每月一次的备份外, 还应对修改过的数据进行每周一次的备份。同时应该将修改过的重要的系统文件存放在不同的服务器上, 以便在系统万一崩溃时(通常是硬盘出错) 可以及时将系统恢复到最佳状态。如果发生系统文件已经被破坏的情况, 也可以使用系统备份来恢复到正常的状态[6]。

常用的方式就是光盘备份, 可以定期将系统与光盘内容进行比较以验证系统的完整性是否遭到破坏。如果对安全级别的要求特别高, 那么可以将光盘设置为可启动的并且将验证工作作为系统启动过程的一部分。这样只要通过光盘启动就说明系统尚未被破坏过。对其他不经常进行修改的文件, 可以备份到另一个系统(如磁带) 或压缩到一个只读的目录中。这种方法可以在使用光盘映像进行验证的基础上再进行额外的系统完整性检查。

2.5 改进 **Linux** 的系统安全控制机制

改进系统内部安全机制可以通过改进 Linux 操作系统的内部功能来防止缓冲区溢出攻击这种破坏力极强却又最难预防的攻击方式。缓冲区溢出实施时, 入侵者必须能够判断潜在的缓冲区溢出何时出现以及它在内存中的什么位置出现。缓冲区溢出预防也很困难, 系统管理员必须完全去掉缓冲区溢出存在的条件才能防止这种方式的攻击。因此针对这种攻击的安全补丁安装是十分重要而有效的方式[7~11]。

2.6 对病毒入侵的安全防范

尽管现在流行的病毒多是针对 Windows 操作系统, 但是并不表明 Linux 或 Unix 系统中没有病毒存在, 事实上世界上第 1 个计算机病毒就是 Unix 病毒。如果 Linux 系统中一旦发生病毒泛滥, 后果将不堪设想。现在很多种病毒都用标准的 C 程序来编写, 以适应任何类的 Linux 和 Unix 操作系统, 并且它们可以用 make 程序跨平台编译。例如: Morris, Ramen, Lion 等蠕虫病毒都曾经先后对 Linux 甚至 Unix 系统进行过攻击。

一般大多数的 Linux 网络主要是由一台或多台安装 Linux 操作系统的服务器做 Web Server 或 FTP Server, 通常也会有 Mail Server。目前工作站端大多是安装了 Windows9X/Me/NT/2000/XP 等操作系统的计算机, 对这种 Linux 网络计算机病毒防护主要还是基于工作站的单机防护。

2.7 设置陷阱和蜜罐

所谓陷阱就是激活后能够触发报警事件的软件, 而蜜罐(honey pot) 程序是指设计来引诱入侵企图者触

发专门的报警的陷阱程序, 通过设置陷阱和蜜罐程序, 一旦出现入侵事件系统可以很快报警。在许多大的网络中, 一般都设计有专门的陷阱程序。陷阱程序一般分为 2 种: 一种是只发现入侵者而不对其采取报复行动, 另一种是同时采取报复行动。设置蜜罐的一种常用方法是故意声称 Linux 系统使用了具有许多脆弱性的 IMAP 服务器版本。当入侵者对这些 IMAP 服务器进行大容量端口扫描就会落入陷阱并且激发系统报警。例如: 系统管理员可以设置假的 phf 脚本, 向入侵者返回假信息并且同时向系统管理员发出报警。另外也可以通过在防火墙中将入侵者的 IP 地址设置为黑名单来立即拒绝入侵者继续进行访问。Linux 内核中的防火墙代码非常适合于这样做。

3　安全管理与预防

除了必要的技术手段还要加强对系统安全的管理, 要阻止黑客的蓄意入侵, 可以减少校园网与外界网络的联系, 不用的服务与功能要屏蔽, 甚至独立于其他网络系统之外, 这种方式虽然造成网络使用上的不便, 但也是最有效的防范措施。

针对黑客入侵, 第 1 件事应该做好日常的预防工作, 作为系统管理员一定要保证自己管理的系统在安全上没有漏洞, 这样一来就不会给非法用户可乘之机。要提前做好预防工作, 主要有以下几点[12~14]。

1) 提前关闭所有可能的系统后门, 以防止入侵者利用系统中的漏洞入侵。例如: 用“rpcinfo-p”来检查机器上是否运行了一些不必要的远程服务。一旦发现, 立即停掉, 以免给非法用户留下系统的后门。

2) 确认系统当中运行的是较新的 Linux, Unix 守护程序, 因为老的守护程序允许其他机器远程运行一些非法的命令。

3) 定期从操作系统那里获得安全补丁程序。

4) 安装加强系统安全的程序。

5) 可以搭建网络防火墙, 防止网络受到攻击。

6) 多订阅一些安全通报, 多访问安全站点, 以获得及时的安全信息来修补系统软件的漏洞。

7) 要每天对系统进行安全检查, 随时观察系统的变化情况, 如系统中进程、文件、时间等的变化情况。具体可以采用以下几个方法: 充分利用 Linux 和 Unix 系统中内置的检查命令来检测系统; 定期检查系统中的日志、文件、时间和进程信息; 另外还要定期定时做好完整的数据备份, 有了完整的数据备份, 在遭到攻击或系统出现故障时也能迅速恢复系统。

4　结　语

从计算机安全的角度看, 世界上没有绝对安全的计算机系统, 使用 Linux 系统的校园网也不例外。校园网中的 Linux 系统需要采取多种措施进行安全防护, 系统管理员需时刻跟踪 Linux 安全技术的发展动向, 要适时采用更先进的 Linux 安全工具。还需要借助防火墙、入侵检测系统等工具, 共同防御非法入侵。

参考文献:

[1] 冯建华, 王钦克, 郝东升, 等. Linux 高级网络管理[M]. 北京: 清华大学出版社, 2000.
[2] KABIR M J. Red Hat Linux 系统管理员手册[M]. 魏永明, 郑　翔, 孙登峰, 等译. 北京: 电子工业出版社, 2000.
[3] KABIR M J. Red Hat Linux 安全与优化[M]. 邓少鹃译. 北京: 中国水利水电出版社, 2004.
[4] 王永滨, 袁智忠, 张　吉. Linux 防火墙的 Web 设置系统[J]. 河北科技大学学报, 2001, 22(4): 46-49.
[5] 邢建民, 马风彬. 增强 Linux 系统安全性的措施[J]. 河北工业科技, 2002, 19(6): 8-11.
[6] 袁　礼. 校园网信息系统安全研究与实践[J]. 科技资讯, 2006, (25): 249-250.
[7] 简　明. 计算机网络信息安全及其防护策略的研究[J]. 科技资讯, 2006, (28): 83-85.
[8] 杨　健, 卜红杰, 张英彩. 网络防火墙技术浅析[J]. 河北工业科技, 2003, 20(4): 25-27.
[9] 张　翔. 李雅峰, 张自宾, 等. 网络入侵技术漫谈[J]. 河北工业科技, 2004, 21(2): 30-32.
[10] 张　健. 电子政务网络信息安全探析[J]. 河北工业科技, 2004, 21(4): 43-45.
[11] 张　妍, 许云峰. Windows 2000 下详细配置虚拟专用网络[J]. 河北工业科技, 2005, 22(6): 377-379.
[12] 锐捷网络. 网络互联与实现[M]. 北京: 北京希望电子出版社, 2006.
[13] 周　围, 回文博, 赵丽莉. 防火墙在校园网中的应用[J]. 河北科技大学学报, 2001, 22(4): 50-52.
[14] 王　缜, 叶　林. 电子商务中的安全技术[J]. 河北工业科技, 2002, 19(4): 44-47.