 Unix系统安全必读 本文从系统管理员的角度讨论安全问题.系统管理员是管理系统的人:启动系统,停止系统运行,安装新软件,增加新用户,删除老用户,以及完成保持系统发展和运行的日常事务工作。 1.安全管理 安全管理主要分为四个方面: (1)防止未授权存取:这是计算机安全最重要的问题:未被使用系统的人进入系统.用户意识,良好的口令管理(由系统管理员和用户双方配合),登录活动记录和报告,用户和网络活动的周期检查,这些都是防止未授权存取的关键。 (2)防止泄密:这也是计算机安全的一个重要问题.防止已授权或未授权的用户相互存取相互的重要信息.文件系统查帐,su登录和报告,用户意识,加密都是防止泄密的关键。 (3)防止用户拒绝系统的管理:这一方面的安全应由操作系统来完成.一个系统不应被一个有意试图使用过多资源的用户损害.不幸的是,UNIX不能很好地限制用户对资源的使用,一个用户能够使用文件系统的整个磁盘空间,而UNIX基本不能阻止用户这样做.系统管理员最好用PS命令,记帐程序df和du周期地检查系统.查出过多占用CUP的进程和大量占用磁盘的文件。 (4)防止丢失系统的完整性:这一安全方面与一个好系统管理员的实际工作(例如:周期地备份文件系统,系统崩溃后运行fsck检查,修复文件系统,当有新用户时,检测该用户是否可能使系统崩溃的软件)和保持一个可靠的操作系统有关(即用户不能经常性地使系统崩溃). 本文其余部分主要涉及前两个问题,第三个问题在"安全查帐"一节讨论。 2.超级用户 一些系统管理命令只能

由超级用户运行.超级用户拥有其他用户所没有的特权,超级用户不管文件存取许可方式如何,都可以读,写任何文件,运行任何程序。系统管理员通常使用命令: /bin/su 或以 root 进入系统从而成为超级用户.在后面文章中以#表示应敲入必须由超级用户运行的命令,用$表示应敲入由所有其他用户运行的命令。 3.文件系统安全 (1)UNIX文件系统概述 UNIX文件系统是UNIX系统的心脏部分,提供了层次结构的目录和文件.文件系统将磁盘空间划分为每1024个字节一组,称为块(block)(也有用512字节为一块的,如:SCO XENIX).编号从0到整个磁盘的最大块数.全部块可划分为四个部分,块0称为引导块,文件系统不用该块.块1称为专 用块,专用块含有许多信息,其中有磁盘大小和全部块的其它两部分的大小.从块2开始是i节点表,i节点表中含有i节点,表的块数是可变的,后面将做讨论.i节点表之后是空闲存储块(数据存储块),可用于存放文件内容.文件的逻辑结构和物理结构是十分不同的,逻辑结构是用户敲入cat命令后所看到的文件,用户可得到表示文件内容的字符流.物理结构是文件实际上如何存放在磁盘上的存储格式.用户认为自己的文件是边疆的字符流,但实际上文件可能并不是以边疆的方式存放在磁盘上的,长于一块的文件通常将分散地存放在盘上.然而当用户存取文件时,UNIX文件系统将以正确的顺序取各块,给用户提供文件的逻辑结构.当然,在UNIX系统的某处一定会有一个表,告诉文件系统如何将物理结构转换为逻辑结构.这就涉及到i节点了.i节点是一个64字节长的表,含有有关一个文件的信息,其中有文件大小,文件所有者,文件存取许可方式,以及文件为普通文件,目录文件还是特别文件等.在i节点中最重要的一项是磁盘地址表.该表中有13个块号.前10个块号是文件前10块

的存放地址.这10个块号能给出一个至多10块长的文件的逻辑结构,文件将以块号在磁盘地址表中出现的顺序依次取相应的块。 当文件长于10块时又怎样呢?磁盘地址表中的第十一项给出一个块号,这个块号指出的块中含有256个块号,至此,这种方法满足了至多长于266块的文件(272,384字节).如果文件大于266块,磁盘地址表的第十二项给出一个块号,这个块号指出的块中含有256个块号,这256个块号的每一个块号又指出一块,块中含256个块号,这些块号才用于取文件的内容.磁盘地址中和第十三项索引寻址方式与第十二项类似,只是多一级间接索引。 这样,在UNIX系统中,文件的最大长度是16,842,762块,即17,246,988,288字节,有幸是是UNIX系统对文件的最大长度(一般为1到2M字节)加了更实际的限制,使用户不会无意中建立一个用完整个磁盘窖所有块的文件.文件系统将文件名转换为i节点的方法实际上相当简单.一个目录实际上是一个含有目录表的文件:对于目录中的每个文件,在目录表中有一个入口项,入口项中含有文件名和与文件相应的i节点号.当用户敲入cat xxx时,文件系统就在当前目录表中查找名为xxx的入口项,得到与文件xxx相应的i节点号,然后开始取含有文件xxx的内容的块。 (2)保持系统安全 . 考虑系统中一些关键的薄弱环节: a. 系统是否有MODEM?电话号码是否公布 b. 系统是否连接到?还有什么系统也连接到该网络 c. 系统管理员是否使用未知来处或来处不可靠的程序 d. 系统管理员是否将重要信息放在系统中 e. 系统的用户是熟悉系统的使用还是新手 f. 用户是否很重视关心安全 g. 用户的管理部门是否重视安全 . 保持系统文件安全的完整性.检查所有系统文件的存取许可,任何具有SUID许可的程序都是非法者想偷换的选择对象. . 要特别注意设备文

件的存取许可. . 要审查用户目录中具有系统ID/系统小组的SUID/SGID许可的文件. . 在未检查用户的文件系统的SUID/SGID程序和设备文件之前,不要安装用户的文件系统. . 将磁盘的备份存放在安全的地方. . 设置口令时效,如果能存取UNIX的源码,将加密口令和信息移到仅对root可读的文件中,并修改系统的口令处理子程序.这样可增加口令的安全.修改passwd,使passwd能删去口令打头和末尾的数字,然后根据spell词典和/etc/passwd中用户的个人信息,检查用户的新口令,也检查用户新口令中子串等于登录名的情况.如果新口令是spell词典中的单词,或/etc/passwd中的入口项的某项值,或是登录名的子串,passwd将不允许用户改变口令. . 记录本系统的用户及其授权使用的系统. . 查出久未使用的登录户头,并取消该户头. . 确保没有无口令的登录户头. . 启动记帐系统. . 查出不寻常的系统使用情况,如大量的占用磁盘,大量的使用CPU时间,大量的进程,大量的使用su的企图,大量无效的登录,大量的到某一系统的网络传输,奇怪的uucp请求. . 修改shell,使其等待了一定时间而无任务时终止运行. . 修改login,使其打印出用户登录的最后时间,三次无效登录后,将通讯线挂起,以便系统管理员能检查出是否有人试图非法进入系统.确保login不让root在除控制台外的任何地方登录. . 修改su,使得只有root能以过期口令通过su进入某一户头. . 当安装来源不可靠的软件时,要检查源码和makefile文件,查看特殊的子程序调用或命令. . 即使是安装来源可靠的软件,也要检查是否有SUID(SGID)程序,确认这些许可的确是必要的.如果可能,不要让这些程序具有系统ID(或组)的SUID(SGID)许可,而应该建立一个新用户(或给)供该软件运行. . 如果系统在办公室中,门应上锁,将重要数据保

存在软盘上或带上,并锁起来. . 将secure,perms和任何其它做安全检查的shell程序存取许可置为仅执行,更好的是将这些shell程序存于可拆卸的介质上. . 记住,只要系统有任何人都可调用的拨号线,系统就不可能真正的安全.系统管理员可以很好地防止系统受到偶然的破坏.但是那些有耐心,有计划,知道自己在干什么的破坏者,对系统直接的有预谋的攻击却常常能成功. . 如果系统管理员认为系统已经泄密,则应当设法查出肇事者.若肇事者是本系统的用户,与用户的管理部门联系,并检查该用户的文件,查找任何可疑的文件,然后对该用户的登录小心地监督几个星期.如果肇事者不是本系统的用户,可让本公司采取合法的措施,并要求所有的用户改变口令,让用户知道出了安全事故,用户们应当检查自己的文件是否有被窜改的迹象.如果系统管理员认为系统软件已被更改了,就应当从原版系统带(或.软盘)上重装入所有系统软件,保持系统安全比道歉更好. 