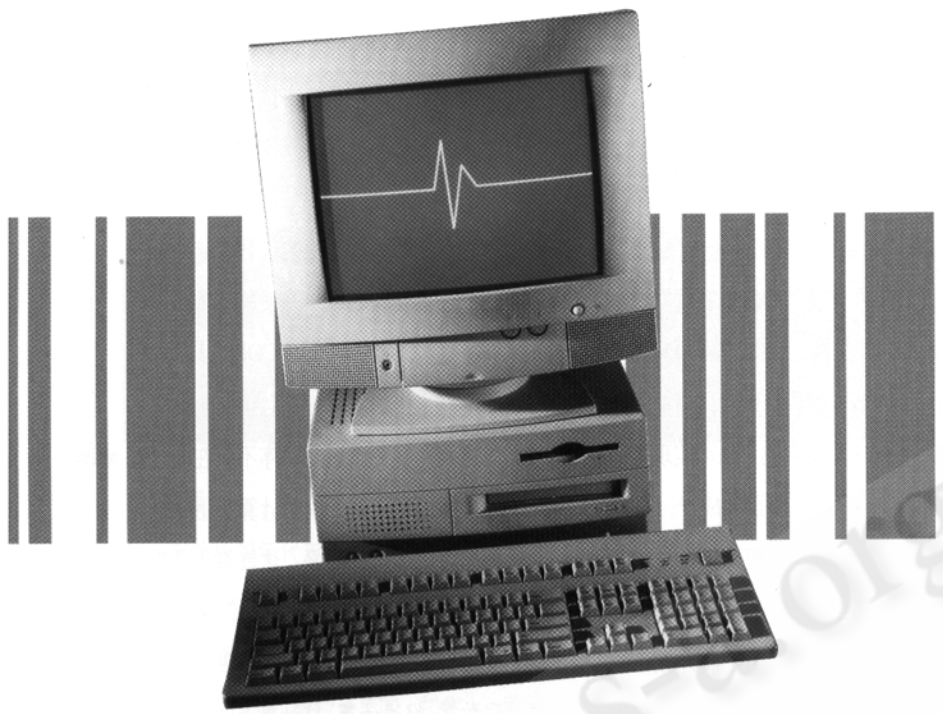


Unix/Linux 操作系统安全(二)

卿斯汉 (中科院信息安全技术工程研究中心 100080)

2.4 审计

Unix 系统的审计机制监控系统中发生的事件,以保证安全机制正确工作并及时对系统异常报警提示。审计结果常写在系统的日志文件中。丰富的日志为 Unix 的安全运行提供了保障。常见的日志文件有:

acct 或 pacct 记录每个用户使用过的命令

aculog 拨出 modems (自动呼叫部件) 记录

lastlog 记录用户最后一次成功登陆时间和最后一次登陆失败的时间

loginlog 不良的登录尝试记录

messages 记录输出到系统主控台以及由syslog系统服务程序产生的信息

sulog 记录 su 命令的使用情况

utmp 记录当前登录的每个用户

utmpx 扩展的 utmp

wtmp 记录每一次用户登录和注销的历史信息,以及系统关和开

wtmpx 扩展的 wtmp

vold.log 记录使用外部介质 (如: 软盘或光盘) 出现的错误

xferlog 记录 ftp 的存取情况

其中, 最常用的大多数版本的 Unix 都具备的审计服务程序是 syslogd, 它可实现灵活配置、集中式管理。运行中, 需要对信息作登记的的单个软件发送消息给 syslogd, 根据配置 (/etc/syslog.conf), 按照消息的的来源和重要程度情况, 这些消息可记录到不同的文件、设备或其他主机中。

Linux 日志与 Unix 类似, 非常普遍存在于系统、应用和协议层。大部分 Linux 把输出的日志信息放入标准或共享的日志文件里。大部分日志存在于/var/log。相应的, Linux 有许多日志工具, 像 lastlog 跟踪用户登录, last 报告用户的最后登录。Xferlog 记录 FTP 文件传输, 还有 Httpd 的 access-log,error-log。系统和内核消息由 syslogd 和 klogd 处理。

当前的 Unix/Linux 系统很多都支持 "C2 级审计", 即达到了由 TCSEC (可信任的计算机系统评价规范) 所规定的 C2 级的审计标准。

2.5 密码

加密 (encryption) 是指一个消息 (plaintext, 称为明文) 用一个数学函数和一个专门的加密口令 (称为密钥) 转换为另一个消息 (ciphertext, 称为密文) 的过程。解密 (decryption) 是一个相反的过程: 密文用一个数学函数和一个密钥转换为明文。

在 Unix 系统中采用加密系统是必要的。假设一个拥有超级用户权限的用户可以绕过文件系统的所有口令检查, 虽然他的权限极大, 但如果文件加密, 他在不知道密钥的情况下仍是无法解密文件的。

当前 Unix 系统中常使用的加密程序有:

crypt: 最初的 Unix 加密程序

des: 数据加密标准 (Data Encryption Standard, DES) 在 Unix 上的应用

pgp: Phil Zimmermann 的 Pretty Good Privary 程序在 Linux 上有相应的实现。

如: 使用 crypt 命令 (不同于更安全 crypt() 库函数) 可提供给用户以加密文件, 使用一个关键词将标准输入的信息编码为不可读的杂乱字符串, 送到标准输出设备。再次使用此命令, 用同一关键词作用于加密后的文件, 可恢复文件内容。加密关键词的选取规则与口令的选取规则相

同。由于crypt程序可能被做成特洛依木马，故不宜用口令做为关键词，最好在加密前用pack或compress命令对文件进行压缩后再加密。

Unix/Linux可以提供一些点对点的加密方法，以保护传输中的数据。一般情况下，当数据在因特网中传输时，可能要经过许多网关。在这个过程中，数据很容易被窃取，各种添加的Linux应用程序可以进行数据加密和打乱数据的操作，这样即使数据被截获，窃取者除了一些乱码外，别无所得，Secure Shell就是有效的利用加密来保证远程登录的安全，Unix也可以对本地文件进行加密，保证文件的一致性，防止文件被非法访问和窜改，可以一定程度的防止病毒、特洛依木马等恶意程序。

例如：一个网络里面通常会有许多用户，通常，这些用户都需要在使用服务时提供密码，系统中都有passwd实用程序，可以用来修改密码。在UNIX类的操作系统中，有很多作法是相同的。比如，用户名和密码均存储于/etc/passwd文件之中，除此之外，此文件还存储有其他重要信息，如：UID、GID等等，这个文件中的信息对维护系统正常运行是必不可少的。如用户认证，权限赋予等。/etc/passwd文件中存储的是加密的密码字串，你在修改密码时，程序使用某种算法(hash)加密输入的字符，再存入文件。在登录时，系统把你输入后加密的字符串和存储的密码串比较，如果一致，则认为通过，哈希算法是不可逆的。Cracker(攻击者)可以先取得密码文件，再使用推测、穷举的笨办法强行"猜出"密码。即，使用程序加密字串，不断和文件里面的密文对比，如果相同，则就找到了密码。可见密码选择的重要。一般在你使用passwd程序修改密码时，如果输入的密码安全性不够，系统会给你警告，说明密码选择很糟糕。这时，最好再换一个。绝对避免使用用户名或者其变化形式，有的破解程序可是上来就使用用户名来回变换测试的。

可是这样安全性仍然不够，下一步是使用更好的加密算法，如MD5(有的Linux发行版安装时可以选择此项)；或者把密码放在其他地方，Unix/Linux一般的解决方案类似于第二个方案，叫做shadow password。在/etc/passwd文件中的密码串被替换成了'x'，组密码也一样处理。系统在使用密码文件时，发现标记会寻找shadow文件，完成相应的操作。而shadow文件只有root用户可存取。还有新的、更安全可靠和经济的认证技术不断出现，如果想使用这些技术，仍然需要修改许多程序，为了达到更经济合理的目的，出现了PAM"Pluggable Authentication Modules"可插入认证模块。它在需要认证的程序和实际认证机制之间引入中间件层。一旦程序是基于PAM发行的，那么，任何PAM支持的认证方法都可以用于程序！这样就没有重新编译所有程序的麻烦了，只要PAM发展了新技术，如数字签名，基于PAM的程序可以马上使用它。这种强大的灵活性能是企业级应用所不可或缺的。

更进一步，普通认证手段难以完善的管理用户、会话数据等工作还可以交给PAM来做，比如，你可以非常容易的禁止某些用户在特定的时间段登录，或要求他们登录时使用特别的认证方式。

2.6 网络

当前的Unix系统通常是运行在网络环境中的，缺省支持TCP/IP协议。网络安全性，主要指通过防止本机或本网被非法侵入、访问，从而达到保护本系统可靠、正常运行的目的。Unix有能力提供网络访问控制和有选择的允许用户和主机与其他主机的连接。

相关的配置文件有：

/etc/inetd.conf文件内容是系统提供哪些服务。

/etc/services文件里罗列出了端口号、协议和对应的名称。

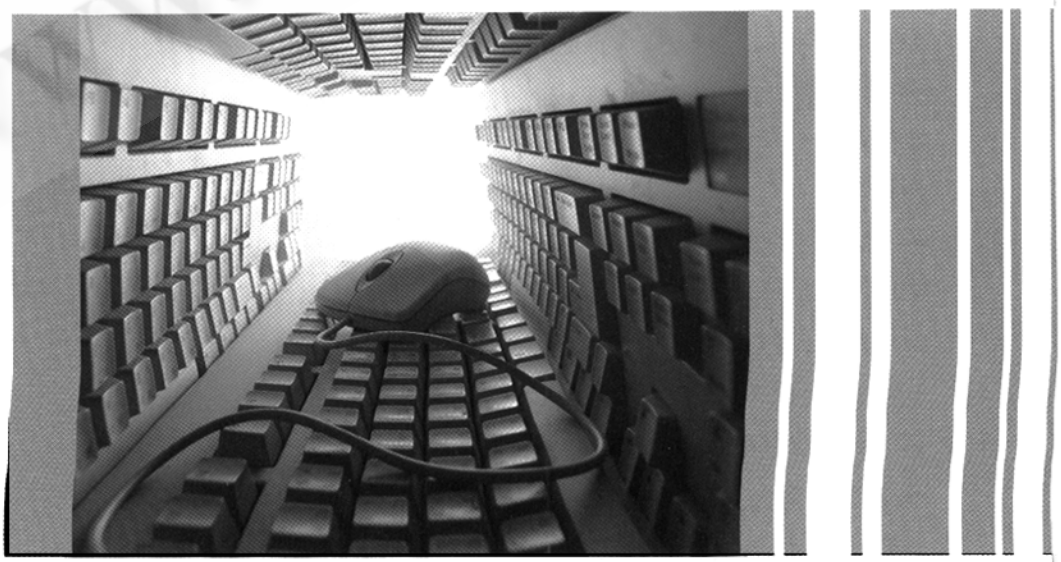
TCP-WRAPPERS由如下两个文件控制。

/etc/hosts.allow

/etc/hosts.deny

它可以使你很容易的控制哪些IP地址禁止登录，哪些可以。加入服务限制条件，可以更好的管理系统。系统在使用它们的时候，先检查前一个文件，从头到尾扫描，如果发现用户的相应记录标记，就给用户连接他要求的服务。如果没有找到记录，就像刚才一样扫描hosts.deny文件，查看是否有禁止用户的标记。如果发现记录，就不给用户提供相应服务。如果仍然没有找到记录，则使用系统默认值：开放服务。

网上访问的常用工具有telnet、ftp、rlogin、rcp、rcmd等网络操作命令，对它们的使用必须加以限制。最简单的方法是修改/etc/services中相应的服务端口号，使其完全拒绝往外的这类访



问。或者，对网上的访问做有条件的限制(或允许)。另外，NFS使网络上的主机可以共享文件；NIS又称黄页服务，可将网络上每台主机的配置文件集中到一个NIS服务器上来实现，这些配置包括用户账号信息、组信息、邮件别名等。

(1) 当远程使用ftp访问本系统时，UNIX系统首先验证用户名和密码，无误后查看/etc/ftpusers文件(不受欢迎的ftp用户表)，一旦其中包含登录所用用户名则自动拒绝连接，从而达到限制作用。因此我们只要把本机内除匿名ftp以外的所有用户列入ftpusers文件中，即使入者获得本机内正确的用户信息，也无法登录系统。需对外发布的信息，放到/usr/ftp/bub下，让远方通过匿名ftp获取。使用匿名ftp，不需密码，不会对本机系统的安全构成威胁，因为它无法改变目录，也就无法获得本机内的其他信息。使用远程注册数据文件(.netrc文件)配置，需注意保密，防止泄露其他相关主机的信息。

(2) UNIX系统没有直接提供对telnet的控制。但我们知道，/etc/profile是系统默认shell变量文件，所有用户登录时必须首先执行它。故可修改该文件达到安全访问目的。

(3) 所谓用户等价，就是用户不用输入密码，即可以相同的用户信息登录到另一台主机中。用户等价的文件名为.rhosts，存放在根下或用户主目录下。它的形式如下：

#主机名 用户名

ash020000 root

ash020001 dgxt

主机等价类似于用户等价，在两台计算机除根目录外的所有区域有效，主机等价文件为hosts.equiv，存放在/etc下。

使用用户等价和主机等价这类访问，用户可以不用口令而像其他有效用户一样登录到远程系统，远程用户可使用rlogin直接登录而不需密码，还可使用rcp命令向或从本地主机复制文件，也可使用rcmd远程执行本机的命令等。因此主机访问具有严重的不安全性，必须严格控制或在非常可靠的环境下使用。

(4) 当NFS的客户端试图访问由NFS服务器管理的文件系统时，它需要mount文件系统。如果操作成功，服务器将返回"文件句柄"，该标志在以后的文件操作请求中将作为验证用户是否合法的标准。NFS中，对mount请求的验证是根据IP地址决定的，属于弱验证，容易成为攻破目标。

(5) NIS基于远程过程调用(RPC)。利用RPC，一个主机上的客户进程可调用远程主机上的服务进程。其请求、相应的的安全性有三种模式：

① 无认证检查；

② 使用传统UNIX的基于机器标识和用户标识的认证系统，NFS默认使用该模式；

③ DES认证系统，这种模式最安全。NIS的不安全因素表现在其在RPC级上不完成任何认证，网络上的任何机器可以很容易的通过伪装成NIS服务器来创建假的RPC响应。如图3所示。

2.7 网络监视和入侵检测

入侵检测技术是一项相对比较新的技术，标准的Unix/Linux发布版本也是最近才配备了这种工具的。利用Unix配备的工具和从因特网上下载的工具，可以使系统具备高级的入侵检测能力，包括：让Unix记录入侵企图，当攻击发生时及时通知你；让Unix在规定情况的攻击发生时，采取事先确定的措施；让Unix发出一些错误信息，比如模仿成其他操作系统。

例如，利用嗅探器可以有效的监听网络上的信息。用扫描器可以检测安全漏洞。系统扫描器可以扫描本地主机，防止不严格或者不正确的文件许可权，默认的帐户，错误或重复的UID项等；网络扫描器可以对网上的主机检查各种服务和端口，发现可能被远程攻击者利用的漏洞。像著名的扫描器SATAN等。

2.8 备份/恢复

无论采取怎样的安全措施，都不能消除系统崩溃的可能性。系统的安全性和可靠性是与备份密切相关的。定期备份是一件非常重要的事。它可使你在灾难发生后将系统恢复到一个稳定的状态，将损失减到最小。

备份的常用类型有三种：零时间备份、整体备份、增量备份。系统的备份应根据具体情况制定合理的策略，备份文档应经过处理(压缩、加密等)合理保存。

Unix系统中，有几个专门的备份程序：dump/restore, backup

网络备份程序有：rdump/rstore, rcp, ftp, rdist等最安全的备份方法是把它们备份到别的地方，如：网络上、磁带、可移动驱动器(removable drive)或可写光驱等。

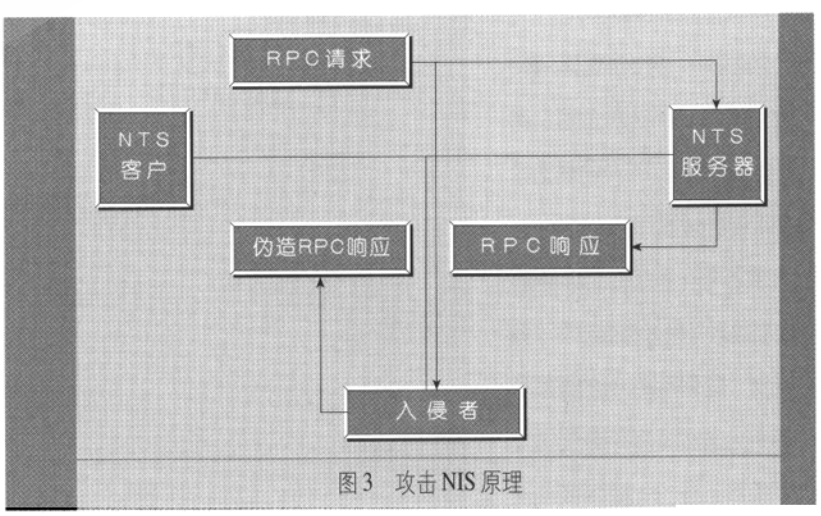


图3 攻击NIS原理