Linux服务器基本安全配置的实现

Realization of Basic Security Configuration on Linux Server

汤 凌（华中师范大学物理科学与技术学院通信工程专业 430079）
刘 磊（华中师范大学物理科学与技术学院电信专业 430079）

摘 要：Linux在作为服务器使用时，其配置管理的复杂性易带来大量安全隐患。本文通过对常见的安全隐患的分析，以Red Hat8.0为例，从帐号管理、文件系统、应用服务等多方面较全面的介绍了Linux服务器的基本安全配置过程。

关键词：Linux 服务器 安全配置

1 前言

Linux操作系统因其强大的性能和配置的灵活性在网络服务器上的应用已经越来越普及。从实际情况看，Linux系统由于其配置管理的复杂性，对于没有长期维护经验的管理员来说，容易产生大量安全隐患。下面以Red Hat 8.0为例，结合笔者管理经验，分析常见Linux系统服务器安全隐患，并介绍安全配置的基本操作。

2 安全隐患分析

从网络安全角度，常见的安全隐患有以下方面：

（1）非法登陆，包括尝试穷举破解密码、窃取帐号密码等；

（2）针对服务端口的数据攻击，如发送大量数据包引起系统崩溃；

（3）由病毒造成的数据丢失、系统崩溃等；

（4）系统管理员或用户的误操作；

（5）系统漏洞产生的缓冲区溢出安全隐患；

通过以上分析，我们不难发现，Linux安全配置的关键在于根据统一策略针对以上隐患进行全面的安全配置，确保服务器能正常提供各种应用服务。

3 具体操作

3.1 物理安全

首先应确保服务器本身的安全，避免机箱被非法打开。同时为防止在机箱内接入外来驱动器并被更改启动顺序，应对BIOS设置密码。

3.2 帐号安全

（1）用户帐号设置。为将非法用户登录的可能性降低至最小，首先应当根据需要删除/etc/passwd和/etc/shadow中的绝大部分默认系统帐号，如news、uucp、gopher等；同时针对在此服务器上有限应用，分别为具体应用设置用户帐号，并赋予相应访问权限，如关闭匿名ftp，启用专用的ftp帐户，只对其分配对基本数据目录的访问权限等。

（2）登陆过程管理。为防止登陆帐号泄露，对/etc/passwd和/etc/shadow应设置访问权限，使只有系统管理员才能访问并进行修改。

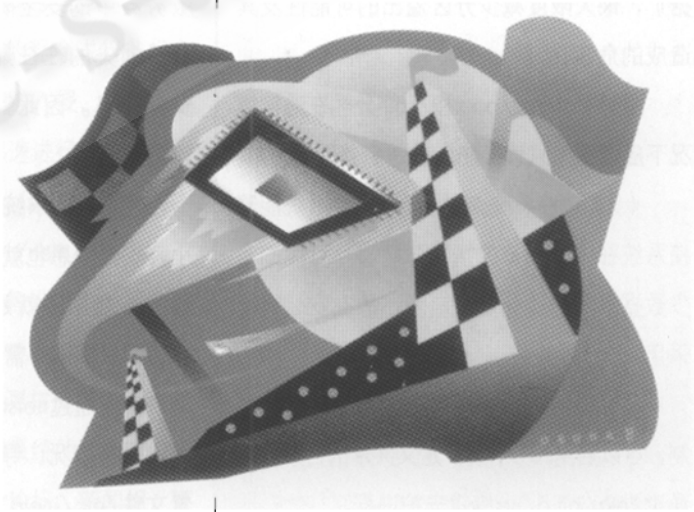
为减少在系统维护时被窃取权限的可能性，系统管理员应当只有在不得以的情况下才使用root帐号或采用su命令运行配置程序。

在管理帐号登录时首先应通过修改/etc/login.defs文件增加对登录错误延迟、记录日志、登录密码长度限制、过期限制等设置。具体如下：

```
/etc/login.defs
#登录密码有效期
PASS_MAX_DAYS 30
#登录密码最短修改时间
PASS_MIN_DAYS 1
#登录密码最小长度
PASS_MIN_LEN 8
```

其次，限制root登录的终端窗口，使root只能从console或者使用ssh登陆。即修改/etc/securetty文件，同时配置/etc/pam.d/su文件，限制通过su命令使用root权限的用户只能为wheel组，这样可以进一步避免用户的误操作。具体方法如下：

```
/etc/securetty
```



#屏蔽以下终端窗口的root登录，并限制同时打开终端的个数。

#tty1

#tty2

#tty7

#tty8

#tty9

/etc/pam.d/su

auth sufficient /lib/security/pam_wheel.so debug

#密码验证

auth required /lib/security/pam_wheel.so use_uid

#限制wheel组用户才可以切换到root

3.3 文件系统安全

（1）文件分区。目前因文件分区配置产生的安全隐患中，常见的为/root分区被日志或垃圾邮件占据和对/home的大量数据写入导致系统崩溃，因此除系统要求的/、/boot、/swap分区外，建议还应设置/var分区（用于记录日志和邮件）、/home分区（防止溢出）、/usr分区（限制用户数据），最大限度减少分区溢出的可能性及其造成的危害；

同时对/lib、/boot和/sbin分区在通常情况下应设置为只读，防止被恶意修改。

（2）文件系统。由于ext3文件系统能够使系统在突然失电的情况下能够尽可能的减少数据损失并避免系统崩溃，故在安装时应采用ext3文件系统。

同时，为进一步对用户共享目录进行限制，可以启用NFS系统，定义共享的目录。即通过/etc/init.d/nfs编辑守护进程。

（3）文件目录安全。利用Linux强大的用户文件权限设置功能，对系统重要配置文件修改访问权限并增加只读属性。具体文件参考如下：

建议设置 chmod 750 的文件：

/etc/pam.d

/etc/rc.d/init.d/

/etc/rc.d/init.d/*

建议设置 chmod 700 的文件：

/bin/rpm

/etc/security

建议设置 chmod 600 的文件：

/etc/xinetd.conf

/etc/inetd.conf

/etc/crontab

/etc/lilo.conf

/etc/securetty

修改属性

chattr +i /etc/services

chattr +i /etc/group

chattr +i /etc/gshadow

chattr +i /etc/hosts.*

chattr +i /etc/xinetd.conf

chattr +i /etc/exports

chattr +i /bin/login

chattr +a /var/log/message

3.4 应用服务

以上的操作主要是为消除在直接使用服务器中的安全隐患，而在实际情况中，造成损失的往往是由网络应用服务引起的安全隐患。因此针对应用服务的安全配置就更为重要。

按照网络系统安全理论，系统的规模越小，安全隐患也就越小。因此，应用服务配置的首要原则就是精简服务器所提供的服务，即只保留必需项。具体方法如下：

首先通过netstat -a命令观察系统目前的网络服务情况，寻找多余的网络服务并在配置文件/etc/inetd.conf中将其注释掉,在通常情况下，exec、talk、ntalk、imap、pop-2、pop-3都是不会被使用的，建议去掉。之后用killall -HUP inetd使改变立即生效。特别需要强调的是建议采用ssh替代使用明文传输的telnet，并去掉rsh、rlogin、rexec（除非有特殊需要）。

其次，编辑.rc配置文件，去除不需要的启动进程。即在/etc/rc.d/rc3.d(文本启动环境)或/etc/rc.d/rc5.d（Xwindow启动环境）中将对应服务（以S开头）去除（简单方法是将S改为s即可）。常见的可去除或漏洞较多的服务有：

S20rstatd　远程用户可以从中获取很多信息

S34yppasswdd　NIS服务器

S35ypserv　NIS服务器

S55routed　RIP

S60nfs　NFS服务器

S95innd　News服务器

再者，增加超级守护进程的限制。通过修改/etc/xinetd.conf文件对远程连接的时间，访问网段等限制等安全设置。这些设置将对由超级守护进程管理的进程生效。设置如下：

/etc/xinetd.conf

defaults

{

#仅允许两个网段访问

only_from=192.168.10.0 192.168.11.0

#禁止其他网段访问

no_access = 0.0.0.0

#限制访问时间

access_times = 8:00-17:00

}

includedir /etc/xinetd.d

最后，运行漏洞扫描程序，检测有无遗忘的端口。

3.5 日志维护

作为系统管理员，一项很重要的工作即是通过对日志及其相关告警信息的分析进行系统维护。根据日志记录中对异常事件进行分析，阻止正在进行的入侵；对入侵已经造成的损失进行数据恢复，并作好安全事件记录。

（1）使用日志服务器。通过日志服务

器，将客户机的日志信息进行备份。即修改/etc/sysconfig/syslog文件
以接收远程日志记录。如下：

/etc/sysconfig/syslog

SYSLOGD_OPTIONS="-m r 0"

设定日志远程保存。修改/etc/syslog.conf文件以加入日志服务器的设置。如下：

/etc/syslog.conf

. @log_server_IP

（2）使用logwatch工具。Red Hat Linux中提供了logwatch工具，定期自动检查日志并发送邮件到管理员信箱。即修改/etc/log.d/conf/ logwatch.conf文件，在MailTo = root参数后增加管理员的邮件地址。Logwatch会定期检查日志，并过滤有关使用root、sudo、telnet、ftp登录等信息，协助管理员分析日常安全。

（3）在进程管理中建立日志记录。针对具体进程建立日志，作为对系统日志的补充。如通过修改/etc/ftpaccess或者/etc/inetd.conf，记录关于ftp的连接日志。具体办法如下：

/etc/inetd.conf

ftp stream tcp nowait root /usr/sbin/tcpd in.ftpd -l -L -i -o

#-l 记录每一个ftp连接

#-L 记录用户的每一个命令

#-i 记录文件上传

#-o 记录文件下载

（4）防止非授权用户查看日志。日志文件可以反映系统运行状态，并对非法入侵进行记录。故对于入侵者而言,日志文件对于进一步入侵系统并掩盖入侵痕迹有很大价值。因此必须限制对 / var / log文件的访问，禁止一般权限的用户去查看日志文件。

3.6 网络连接安全

通过对相关文件的修改限制网络连接。首先通过/etc/hosts.deny禁止来自任何地方对所有服务的访问，然后在/etc/hosts.allow中添加要授权的机器及服务。具体如下：

/etc/hosts.deny

#拒绝所有访问（除在/etc/hosts.allow之外）

ALL: ALL@ALL, PARANOID

/etc/hosts.allow

#允许访问ftp服务的IP地址及主机名

ftp: 202.114.36.28 test.com

同时避免设置缺省路由，即default route。应为每一个子网或网段单独设置路由。通过指定路由可以避免通过缺省路由的非授权访问。

3.7 其他要点

（1）防止系统提示泄露信息：对于入侵者，服务器所采用的操作系统内核版本等信息具有很高的价值，因此应防止系统提示泄露有关信息。具体做法：删除/etc/issue以及/etc/issue.net文件，防止登陆时的信息泄露。

（2）口令检测：应定期更换用户口令，并要求用户使用具备一定复杂性的口令。采用专门软件如npasswd进行模拟攻击，检查口令是否符合基本安全要求。

（3）备份：对重要的程序进行备份，使发生安全事件（如系统被入侵、管理员误操作、病毒破坏等）能迅速进行系统恢复。建议备份以下程序：/bin/su、/bin/ps、/bin/rpm、/usr/bin/top、/sbin/ifconfig、/bin/mount。并使用专门备份工具对用户数据进行备份。

（4）补丁、漏洞检测与反病毒：系统管理员应随时跟踪所使用系统的更新升级情况，并经常访问有关安全论坛、新闻组，下载最新补丁与漏洞检测程序。对Red Hat来说，以下关于安全的网址和邮件列表能提供大量有用信息：

http://www.redhat.com/corp/support/errata/ 最新的补丁提供下载

linux-alert-request@RedHat.com 关于安全警告的邮件列表

linux-security-request@RedHat.com 关于安全问题的邮件列表

securedistros@nl.linux.org 大量的安全信息的邮件列表

www.drsolomon.com 大量病毒信息通告

4 结束语

以上措施只是根据普遍情况对Red Hat8.0 Linux服务器做的系统安全基本配置，并未涉及具体的服务组件（如Apache）等。从以上措施可以看出，任何单一的安全防护措施都无法提供足够安全强度，必须针对不同隐患产生的原因进行全面安全配置。同时，网络安全仅靠系统管理员对服务器的安全配置是远远不够的，必须制定较完备的安全规则，并不断提高用户的安全意识。

参考文献

1 Anonymous:Maximum Security(Second Edition), Sams Publishing,1998。

2 Brian Hatch,James Lee,George Kurtz: Hacking Linux Exposed:Linux Security Secrets & Solutions, McGraw-Hill,2001。

3 吴绍伟，Linux 系统管理，人民邮电出版社，2002。