linux安全策略

1：磁盘分区合理性，把分区设置成只读。

如果是新安装系统，对磁盘分区应考虑安全性：

根目录（/）、用户目录（/home）、临时目录（/tmp）和/var目录应分开到不同的磁盘分区；

以上各目录所在分区的磁盘空间大小应充分考虑，避免因某些原因造成分区空间用完而导致系统崩溃；

2：禁止无用的网络服务。

编辑/etc/inetd.conf禁止以下服务：

ftp, telnet, shell, login, exec, talk,

ntalk, imap, pop-2, pop-3, finger,

auth, etc. 除非你真的想用它。

4：不显示操作系统和版本信息。（远程）（本地）

不要显示出

操作系统

和版本信息。

如果你希望某个人远程登录到你的服务器时不要显示操作系统和版本信息，你能改变

/etc/inetd.conf中的一行象下面这样：

telnet stream tcp nowait root /usr/sbin/tcpd in.telnetd

–h

如果你希望某个人本地登陆时不显示linux版本名，内核版本名和服务器

主机名。你可以,编辑下面文件。

/etc/rc.d/rc.local放#在下面的行前面：

# This will overwrite /etc/issue at

every boot. So, make any changes you

# want to make to /etc/issue here or you

will lose them when you reboot.

#echo "" > /etc/issue

#echo "$R"

>> /etc/issue

#echo "Kernel $(uname -r) on $a $(uname -m)" >>

/etc/issue

#cp -f /etc/issue /etc/issue.net

#echo >>

/etc/issue

[root@kiss]# rm -f /etc/issue

[root@kiss]# rm -f

/etc/issue.net

[root@kiss]# touch /etc/issue

[root@kiss]# touch

/etc/issue.net

5：设置root可以登陆的控制台

该文件指定了允许root登录的tty设备，/etc/securetty被/bin/login程序读取,它的

格式是一行一个被允许的名字列表，如你可以编辑/etc/securetty且注释出下面的行。

tty1

#tty2

#tty3

#tty4

#tty5

#tty6

#tty7

#tty8

-意味着root仅仅被允许在tty1终端登录。

6：删除无用的系统用户

当你第一次装上系统时系统会建立很多的内制用户， 一般情况下用处不大，你有的帐号越多，就越容易受到攻击。

为删除你系统上的用户，用下面的命令：

[root@kiss]# userdel username

为删除你系统上的组用户帐号，用下面的命令：

[root@kiss]# groupdel username

在终端上打入下面的命令删掉下面的用户。

root@kiss]# userdel adm

[root@kiss]# userdel

lp

[root@kiss]# userdel sync

[root@kiss]# userdel shutdown

[root@kiss]#

userdel halt

[root@kiss]# userdel mail

如果你不用sendmail服务器，procmail.mailx,就删除这个帐号。

[root@kiss]# userdel

news

[root@kiss]# userdel uucp

[root@kiss]# userdel

operator

[root@kiss]# userdel games

如果你不用X windows 服务器，就删掉这个帐号。

[root@kiss]# userdel

gopher

[root@kiss]# userdel ftp

如果你不允许匿名FTP，就删掉这个用户帐号。

打入下面的命令删除组帐号

[root@kiss]# groupdel adm

[root@kiss]# groupdel lp

[root@kiss]#

groupdel mail

如不用Sendmail服务器，删除这个组帐号

[root@kiss]# groupdel

news

[root@kiss]# groupdel uucp

[root@kiss]# groupdel

games

如你不用X Windows，删除这个组帐号

[root@kiss]# groupdel

dip

[root@kiss]# groupdel pppusers

[root@kiss]# groupdel

popusers

如果你不用POP服务器，删除这个组帐号

[root@kiss]# groupdel

slipusers

7：给重要文件加入不可更改属性

用chattr命令给下面的文件加上不可更改属性。

[root@kiss]# chattr +i

/etc/passwd

[root@kiss]# chattr +i /etc/shadow

[root@kiss]# chattr +i

/etc/group

[root@kiss]# chattr +i /etc/gshadow

[root@kiss]# chattr +i /etc/services

chattr命令不能保护/、/dev、/tmp、/var目录

8：禁止使用su命令

如果你不想任何人能够su作为root,你能编辑/etc/pam.d/su加下面的行：

auth sufficient

/lib/security/pam\_rootok.so debug

auth required /lib/security/pam\_wheel.so

group=isd

意味着仅仅isd组的用户可以su作为root.

然后，如果你希望用户admin能su作为root.就运行下面的命令

[root@kiss]# usermod -G10 admin

9：禁止 Control-Alt-Delete

重启动机器命令

[root@kiss]# vi

/etc/inittab

ca::ctrlaltdel:/sbin/shutdown -t3 -r

now

#ca::ctrlaltdel:/sbin/shutdown -t3 -r now

[root@kiss]# /sbin/init

10：设置目录权限

新设置/etc/rc.d/init.d/目录下所有文件的许可权限

[root@kiss]# chmod -R 700

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

仅仅root可以读，写，

10：阻止你的系统响应任何从外部/内部来的ping请求。

既然没有人能ping通你的机器并收到响应，你可以大大增强你的站点的安全性。你可以加下面的一行命令到/etc/rc.d/rc.local，以使每次启动后自动运行。

echo 1 >

/proc/sys/net/ipv4/icmp\_echo\_ignore\_all

11：选择正确的密码

在选择正确密码之前还应作以下修改：

修改密码长度：在你安装linux时默认的密码长度是5个字节。但这并不够，要把

它设为8。修改最短密码长度需要编辑login.defs文件

（vi /etc/login.defs），把下面这行

PASS\_MIN\_LEN&#58853;&#58853;5

改为

PASS\_MIN\_LEN&#58853;&#58853;8

login.defs文件是login程序的配置文件。

12：设置系统会自动注销root账户

root账户是具有最高特权的。如果系统管理员在离开系统之前忘记注销

通过修改账户中“TMOUT”参数，可以实现此功能。TMOUT按秒计算。编辑你的profile文件（vi /etc/profile）,

在"HISTFILESIZE="后面加入下面这行：

TMOUT=3600 （秒）也就是1小时。那么系统会自动注销这个账户。

13：bash\_history

文件中保存了500条使用过的命令 每个在系统中拥有账号的用户在他的目录下都有一个“.bash\_history”文件。bash shell应该保

存少量的命令，并且在每次用户注销时都把这些历史命令删除。

第一步：

“/etc/profile”文件中的“HISTFILESIZE”和“HISTSIZE”行确定所有用户的

“.bash\_history”文件中可以保存的旧命令条数。强烈建议把

“/etc/profile”文件中的“HISTFILESIZE”和“HISTSIZE”行的值设为一个较

小的数，比如30。编辑profile文件（vi

/etc/profile），把下面这行改为：

HISTFILESIZE=30

HISTSIZE=30

这表示每个用户的“.bash\_history”文件只可以保存30条旧命令。

第二步：

删除还应该在"/etc/skel/.bash\_logout" 文件中添加下面这行"rm

-f&#58853;

$HOME/.bash\_history"

。这样，当用户每次注销时，“.bash\_history”文件都

会被删除。

编辑.bash\_logout文件(vi

/etc/skel/.bash\_logout) ，添加下面这行：

rm -f $HOME/.bash\_history

14：关闭服务

因为有些服务会为您的系统带来麻烦。默认的linux系统，运行了很多的服务。但有许多服务是不需要的，很容易引起安全风险。第一个文件是/etc/inetd.conf，它制定了/usr/sbin/inetd将要监听的服务，你可能只需要其中的两个：telnet和ftp，其他的许多如popd,imap

d和rsh都是有可能引发安全问题的。用下面的命令显示没有被注释掉的服务：

# grep -v

"#" /etc/inetd.conf

ftp　　 stream

tcp　　 nowait　root

/usr/sbin/tcpd　in.ftpd -l -a

telnet　stream　tcp　　 nowait

root　　/usr/sbin/tcpd　in.telnetd

shell　 stream　tcp　　 nowait　root　　/usr/sbin/tcpd

in.rshd

login　 stream　tcp　　 nowait　root　　/usr/sbin/tcpd

in.rlogind

talk　　dgram　 udp　　 wait

nobody.tty　　　/usr/sbin/tcpd

in.talkd

ntalk　 dgram　 udp　　 wait　　nobody.tty

/usr/sbin/tcpd　in.ntalkd

pop-3　 stream　tcp　　 nowait　root　　/usr/sbin/tcpd　ipop3d

imap　　stream　tcp　　 nowait　root　　/usr/sbin/tcpd　imapd

finger　stream　tcp　　 nowait

nobody　/usr/sbin/tcpd　in.fingerd

用下面命令察看哪些服务在运行

netstat -na

--ip

要在启动时禁止某个服务

输入/usr/sbin/setup，然后选择"system

services",就可以定制系统启动时跑哪些服务。另外一个选择是chkconfig命令，很多linux版本的系统都自带这个工具。

安全守则

1.

废除系统所有默认的帐号和密码。

2. 在用户合法性得到验证前不要显示公司题头、在线帮助以及其它信息。

3. 废除“黑客”可以攻击系统的网络服务。

4. 使用6到8位的字母数字式密码。

5. 限制用户尝试登录到系统的次数。

6. 记录违反安全性的情况并对安全记录进行复查。

7. 对于重要信息，上网传输前要先进行加密。

8. 重视专家提出的建议，安装他们推荐的系统“补丁”。

9. 限制不需密码即可访问的主机文件。

10.修改网络配置文件，以便将来自外部的TCP连接限制到最少数量的端口。不允许诸如tftp,sunrpc,printer,rlogin或rexec之类的协议。

11.用upas代替sendmail。sendmail有太多已知漏洞，很难修补完全。

12.去掉对操作并非至关重要又极少使用的程序。

13.使用chmod将所有系统目录变更为711模式。这样，攻击者们将无法看到它们当中有什么东西，而用户仍可执行。

14.只要可能，就将磁盘安装为只读模式。其实，仅有少数目录需读写状态。

15.将系统软件升级为最新版本。老版本可能已被研究并被成功攻击，最新版本一般包括了这些问题的补救