Linux 系统安全加固

1、如果是新安装系统，

对磁盘分区应考虑安全性：

1）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；

2）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、对于/tmp 和/var 目录所在分区，大多数情况下不需要有 suid 属性的程序，所以应为这些分区添加 nosuid 属性；

方法一：修改/etc/fstab 文件，添加 nosuid 属性字。例如：

/dev/hda2 /tmp ext2 exec,dev,nosuid,rw 0 0

方法二：如果对/etc/fstab 文件操作不熟，建议通过 linuxconf 程序来修改。

1. 运行 linuxconf 程序；
2. 选择"File systems"下的"Access local drive"；

* 选择需要修改属性的磁盘分区；
* 选择"No setuid programs allowed"选项；
* 根据需要选择其它可选项；
* 正常退出。（一般会提示重新 mount 该分区）

2、安装

1、对于非测试主机，不应安装过多的软件包。这样可以降低因软件包而导致出现安全漏洞的可能性。

2、对于非测试主机，在选择主机启动服务时不应选择非必需的服务。例如 routed、ypbind 等。

3、安全配置与增强

内核升级。起码要升级至 2.2.16 以上版本。

GNU libc 共享库升级。（警告：如果没有经验，不可轻易尝试。可暂缓。）

关闭危险的网络服务。echo、chargen、shell、login、finger、NFS、RPC 等

关闭非必需的网络服务。talk、ntalk、pop-2 等

常见网络服务安全配置与升级

确保网络服务所使用版本为当前最新和最安全的版本。

取消匿名 FTP 访问

去除非必需的 suid 程序

使用 tcpwrapper

使用 ipchains 防火墙

日志系统 syslogd

4.一些具体的细节：

1.操作系统内部的 log file 是检测是否有网络入侵的重要线索。当然这个假定你的 logfile 不被侵入者所破坏，如果你有台服务器用专线直接连到 Internet 上，这意味着你的 IP 地址是永久固定的地址，你会发现有很多人对你的系统做 telnet/ftp 登录尝试，试着运行#more /var/log/secure | grep refused 去检查。

2. 限制具有 SUID 权限标志的程序数量。具有该权限标志的程序以 root 身份运行，是一个潜在的安全漏洞，当然，有些程序是必须要具有该标志的，象 passwd 程序。

3.BIOS 安全。设置 BIOS 密码且修改引导次序禁止从软盘启动系统。

4.用户口令。用户口令是 Linux 安全的一个最基本的起点，很多人使用的用户口令就是简单的‘password''，这等于给侵入者敞开了大门，虽然从理论上说没有不能确解的用户口令，只要有足够的时间和资源可以利用。比较好的用户口令是那些只有他自己能够容易记得并理解的一串字符，并且绝对不要在任何地方写出来。

5./etc/exports 文件。如果你使用 NFS 网络文件系统服务，那么确保你的/etc/exports 具有最严格的存取权限设置，不意味着不要使用任何通配符，不允许 root 写权限，mount 成只读文件系统。编辑文件/etc/exports 并且加：例如：

```
/dir/to/export host1.mydomain.com(ro,root_squash)

/dir/to/export host2.mydomain.com(ro,root_squash)
```

/dir/to/export 是你想输出的目录，host.mydomain.com 是登录这个目录的机器名，

ro 意味着 mount 成只读系统，root_squash 禁止 root 写入该目录。

为了让上面的改变生效，运行/usr/sbin/exportfs -a

[NextPage]

6.确信/etc/inetd.conf 的所有者是 root，且文件权限设置为 600 。

```
[root@deep]# chmod 600 /etc/inetd.conf

ENSURE that the owner is root.

[root@deep]# stat /etc/inetd.conf

File: "/etc/inetd.conf"
```

```
Size: 2869 Filetype: Regular File

Mode: (0600/-rw-------) Uid: ( 0/ root) Gid: ( 0/ root)

Device: 8,6 Inode: 18219 Links: 1

Access: Wed Sep 22 16:24:16 1999(00000.00:10:44)

Modify: Mon Sep 20 10:22:44 1999(00002.06:12:16)

Change:Mon Sep 20 10:22:44 1999(00002.06:12:16)
```

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。

特别是禁止那些 r 命令.如果你用 ssh/scp，那么你也可以禁止掉 telnet/ftp。

为了使改变生效，运行#killall -HUP inetd

你也可以运行#chattr +i /etc/inetd.conf 使该文件具有不可更改属性。

只有 root 才能解开，用命令

#chattr -i /etc/inetd.conf

7. TCP_WRAPPERS

默认地，Redhat Linux 允许所有的请求,用 TCP_WRAPPERS 增强你的站点的安全性是举手之劳，你可以放入

“ALL: ALL”到/etc/hosts.deny 中禁止所有的请求，然后放那些明确允许的请求到/etc/hosts.allow 中，如:

sshd: 192.168.1.10/255.255.255.0 gate.openarch.com

对 IP 地址 192.168.1.10 和主机名 gate.openarch.com，允许通过 ssh 连接。

配置完了之后，用 tcpdchk 检查

[root@deep]# tcpdchk

tcpchk 是 TCP_Wrapper 配置检查工具，

它检查你的 tcp wrapper 配置并报告所有发现的潜在/存在的问题。

8. 别名文件 aliases

编辑别名文件/etc/aliases（也可能是/etc/mail/aliases)，移走/注释掉下面的行。

```
# Basic system aliases -- these MUST be present.
MAILER-DAEMON: postmaster
postmaster: root
# General redirections for pseudo accounts.
bin: root
daemon: root
#games: root ?remove or comment out.
#ingres: root ?remove or comment out.
nobody: root
#system: root ?remove or comment out.
#toor: root ?remove or comment out.
#uucp: root ?remove or comment out.
# Well-known aliases.
#manager: root ?remove or comment out.
#dumper: root ?remove or comment out.
#operator: root ?remove or comment out.
# trap decode to catch security attacks
```

```
    #decode: root

    # Person who should get root''s mail

    #root: marc
```

最后更新后不要忘记运行/usr/bin/newaliases，使改变生效。

[NextPage]

9.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
```

10. 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
```

加-h 标志在最后使得 telnet 后台不要显示系统信息，而仅仅显示 login:

11.The /etc/host.conf file

编辑 host.conf 文件(vi /etc/host.conf)且加下面的行：

```
    # Lookup names via DNS first then fall back to /etc/host
s.
```

```
    order bind,hosts

    # We don''t have machines with multiple IP addresses on
the same card

    (like virtual server,IP Aliasing).

    multi off

    # Check for IP address spoofing.

    nospoof on

    IP Spoofing: IP-Spoofing is a security exploit that wor
ks by tricking

    computers in a trust relationship that you are someone
that you really aren''t.
```

12. The /etc/securetty file

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。

13. 特别的帐号

禁止所有默认的被操作系统本身启动的且不需要的帐号，当你第一次装上系统时就应该做此检查，Linux 提供了各种帐号，你可能不需要，如果你不需要这个帐号，就移走它，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@deep]# userdel username
```

为删除你系统上的组用户帐号，用下面的命令：

```
[root@deep]# groupdel username
```

在终端上打入下面的命令删掉下面的用户。

```
[root@deep]# userdel adm

[root@deep]# userdel lp

[root@deep]# userdel sync

[root@deep]# userdel shutdown

[root@deep]# userdel halt

[root@deep]# userdel mail
```

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

```
[root@deep]# userdel news

[root@deep]# userdel uucp

[root@deep]# userdel operator
```

```
[root@deep]# userdel games
```

如果你不用 X windows 服务器，就删掉这个帐号。

```
[root@deep]# userdel gopher

[root@deep]# 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@deep]# groupdel adm

[root@deep]# groupdel lp

[root@deep]# groupdel mail
```

如不用 Sendmail 服务器，删除这个组帐号

```
[root@deep]# groupdel news

[root@deep]# groupdel uucp

[root@deep]# groupdel games
```

如你不用 X Windows，删除这个组帐号

```
[root@deep]# groupdel dip

[root@deep]# groupdel pppusers

[root@deep]# groupdel popusers
```

如果你不用 POP 服务器，删除这个组帐号

```
[root@deep]# groupdel slipusers
```

用下面的命令加需要的用户帐号

```
[root@deep]# useradd username
```

用下面的命令改变用户口令

```
[root@deep]# passwd username
```

用 chattr 命令给下面的文件加上不可更改属性。

```
[root@deep]# chattr +i /etc/passwd

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

[root@deep]# chattr +i /etc/group

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

[NextPage]
```

14. 阻止任何人 su 作为 root.

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@deep]# usermod -G10 admin
```

16. 资源限制

对你的系统上所有的用户设置资源限制可以防止 DoS 类型攻击（denial of service attacks）

如最大进程数，内存数量等。例如，对所有用户的限制象下面这样：

编辑/etc/security/limits.con 加：

```
* hard core 0

* hard rss 5000

* hard nproc 20
```

你也必须编辑/etc/pam.d/login 文件加/检查这一行的存在。

```
session required /lib/security/pam_limits.so
```

上面的命令禁止 core files“core 0”，限制进程数为“nproc 50“，且限制内存使用为 5M“rss 5000”。

17. The /etc/lilo.conf file

a) Add: restricted

加这一行到每一个引导映像下面，就这表明如果你引导时用(linux single),则需要一个 password.

b) Add: password=some_password

当与 restricted 联合用，且正常引导时，需要用户输入密码，你也要确保 lilo.conf

文件不能被不属于 root 的用户可读，也免看到密码明文。下面是例子：

编辑/etc/lilo.conf 加：

```
boot=/dev/sda

map=/boot/map

install=/boot/boot.b

prompt

timeout=50

Default=linux

restricted ?add this line.

password=some_password ?add this line.

image=/boot/vmlinuz-2.2.12-20

label=linux

initrd=/boot/initrd-2.2.12-10.img

root=/dev/sda6

read-only

[root@deep]# chmod 600 /etc/lilo.conf (不再能被其他用户可读).

[root@deep]# /sbin/lilo -v (更新 lilo 配置).

[root@deep]# chattr +i /etc/lilo.conf（阻止该文件被修改）
```

18. 禁止 Control-Alt-Delete 重启动机器命令

```
[root@deep]# vi /etc/inittab

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

```
To

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

[root@deep]# /sbin/init q
```

19. 重新设置/etc/rc.d/init.d/目录下所有文件的许可权限

```
[root@deep]# chmod -R 700 /etc/rc.d/init.d/*
```

仅仅 root 可以读，写，执行上述所有 script file.

20. The /etc/rc.d/rc.local file

默认地，当你 login 到 linux server 时，它告诉你 linux 版本名，内核版本名和服务器

主机名。它给了你太多的信息，如果你就希望得到提示 login: ,编辑

/etc/rc.d/rc.local 放#在下面的行前面：

```
# This will overwrite /etc/issue at every boot. So, mak
e 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
```

然后，做下面的事情:

```
[root@deep]# rm -f /etc/issue

[root@deep]# rm -f /etc/issue.net

[root@deep]# touch /etc/issue

[root@deep]# touch /etc/issue.net
```

21. 被 root 拥有的程序的位。

移走那些被 root 拥有程序的 s 位标志，当然有些程序需要这个，用命令‘chmod a-s’完成这个。

注：前面带（*）号的那些程序一般不需要拥有 s 位标志。

```
 [root@deep]# find / -type f ( -perm -04000 -o -perm -02000 ) -exec ls –lg {} ;

-rwsr-xr-x 1 root root 33120 Mar 21 1999 /usr/bin/at

*-rwsr-xr-x 1 root root 30560 Apr 15 20:03 /usr/bin/chage

*-rwsr-xr-x 1 root root 29492 Apr 15 20:03 /usr/bin/gpasswd

-rwsr-xr-x 1 root root 3208 Mar 22 1999 /usr/bin/disable-paste

-rwxr-sr-x 1 root man 32320 Apr 9 1999 /usr/bin/man
```

```
   -r-s--x--x 1 root root 10704 Apr 14 17:21 /usr/bin/pass
wd

   -rws--x--x 2 root root 517916 Apr 6 1999 /usr/bin/suidp
erl

   -rws--x--x 2 root root 517916 Apr 6 1999 /usr/bin/sperl
5.00503

   -rwxr-sr-x 1 root mail 11432 Apr 6 1999 /usr/bin/lockfi
le

   -rwsr-sr-x 1 root mail 64468 Apr 6 1999 /usr/bin/procma
il

   -rwsr-xr-x 1 root root 21848 Aug 27 11:06 /usr/bin/cron
tab

   -rwxr-sr-x 1 root slocate 15032 Apr 19 14:55 /usr/bin/s
locate

   *-r-xr-sr-x 1 root tty 6212 Apr 17 11:29 /usr/bin/wall

   *-rws--x--x 1 root root 14088 Apr 17 12:57 /usr/bin/chf
n

   *-rws--x--x 1 root root 13800 Apr 17 12:57 /usr/bin/chs
h

   *-rws--x--x 1 root root 5576 Apr 17 12:57 /usr/bin/newg
rp

   *-rwxr-sr-x 1 root tty 8392 Apr 17 12:57 /usr/bin/write

   -rwsr-x--- 1 root squid 14076 Oct 7 14:48 /usr/lib/squi
d/pinger

   -rwxr-sr-x 1 root utmp 15587 Jun 9 09:30 /usr/sbin/utem
pter
```

```
   *-rwsr-xr-x 1 root root 5736 Apr 19 15:39 /usr/sbin/use
rnetctl

   *-rwsr-xr-x 1 root bin 16488 Jul 6 09:35 /usr/sbin/trac
eroute

   -rwsr-sr-x 1 root root 299364 Apr 19 16:38 /usr/sbin/se
ndmail

   -rwsr-xr-x 1 root root 34131 Apr 16 18:49 /usr/libexec/
pt_chown

   -rwsr-xr-x 1 root root 13208 Apr 13 14:58 /bin/su

   *-rwsr-xr-x 1 root root 52788 Apr 17 15:16 /bin/mount

   *-rwsr-xr-x 1 root root 26508 Apr 17 20:26 /bin/umount

   *-rwsr-xr-x 1 root root 17652 Jul 6 09:33 /bin/ping

   -rwsr-xr-x 1 root root 20164 Apr 17 12:57 /bin/login

   *-rwxr-sr-x 1 root root 3860 Apr 19 15:39 /sbin/netrepo
rt

   -r-sr-xr-x 1 root root 46472 Apr 17 16:26 /sbin/pwdb_ch
kpwd

   [root@deep]# chmod a-s /usr/bin/chage

   [root@deep]# chmod a-s /usr/bin/gpasswd

   [root@deep]# chmod a-s /usr/bin/wall

   [root@deep]# chmod a-s /usr/bin/chfn

   [root@deep]# chmod a-s /usr/bin/chsh

   [root@deep]# chmod a-s /usr/bin/newgrp

   [root@deep]# chmod a-s /usr/bin/write
```

```
[root@deep]# chmod a-s /usr/sbin/usernetctl

[root@deep]# chmod a-s /usr/sbin/traceroute

[root@deep]# chmod a-s /bin/mount

[root@deep]# chmod a-s /bin/umount

[root@deep]# chmod a-s /bin/ping

[root@deep]# chmod a-s /sbin/netreport
```

你可以用下面的命令查找所有带 s 位标志的程序：

```
[root@deep]# find / -type f ( -perm -04000 -o -perm -02000 ) -exec ls -lg {} ;

>; suid-sgid-results
```

把结果输出到文件 suid-sgid-results 中。

[NextPage]

为了查找所有可写的文件和目录，用下面的命令：

```
[root@deep]# find / -type f ( -perm -2 -o -perm -20 ) -exec ls -lg {} ; >; ww-files-results

[root@deep]# find / -type d ( -perm -2 -o -perm -20 ) -exec ls -ldg {} ; >; ww-directories-results
```

用下面的命令查找没有拥有者的文件：

```
[root@deep]# find / -nouser -o -nogroup >; unowed-results
```

用下面的命令查找所有的.rhosts 文件：

```
[root@deep]# find /home -name .rhosts >; rhost-results
```

5.建议替换的常见网络服务应用程序

5.1 WuFTPD

WuFTD 从 1994 年就开始就不断地出现安全漏洞，黑客很容易就可以获得远程 root 访问（Remote Root Access）的权限，而且很多安全漏洞甚至不需要在 FTP 服务器上有一个有效的帐号。最近，WuFTP 也是频频出现安全漏洞。

它的最好的替代程序是 ProFTPD。ProFTPD 很容易配置，在多数情况下速度也比较快，而且它的源代码也比较干净（缓冲溢出的错误比较少）。有许多重要的站点使用 ProFTPD。sourceforge.net 就是一个很好的例子（这个站点共有 3,000 个开放源代码的项目，其负荷并不小啊！）。一些 Linux 的发行商在它们的主 FTP 站点上使用的也是 ProFTPD，只有两个主要 Linux 的发行商（SuSE 和 Caldera）使用 WuFTPD。

ProFTPD 的另一个优点就是既可以从 inetd 运行又可以作为单独的 daemon 运行。这样就可以很容易解决 inetd 带来的一些问题，如：拒绝服务的攻击（denial of service attack），等等。系统越简单，就越容易保证系统的安全。WuFTPD 要么重新审核一遍全部的源代码（非常困难），要么完全重写一遍代码，否则 WuFTPD 必然要被 ProFTPD 代替。

5.2 Telnet

Telnet 是非常非常不安全的，它用明文来传送密码。它的安全的替代程序是 OpenSSH。

OpenSSH 在 Linux 上已经非常成熟和稳定了，而且在 Windows 平台上也有很多免费的客户端软件。Linux 的发行商应该采用 OpenBSD 的策略：安装 OpenSSH 并把它设置为默认的，安装 Telnet 但是不把它设置成默认的。对于不在美国的 Linux 发行商，很容易就可以在 Linux 的发行版中加上 OpenSSH。美国的 Linux 发行商就要想一些别的办法了(例如：Red Hat 在德国的 FTP 服务器上(ftp.redhat.de)就有最新的 OpenSSH 的 rpm 软件包）。

Telnet 是无可救药的程序。要保证系统的安全必须用 OpenSSH 这样的软件来替代它。

5.3Sendmail

最近这些年，Sendmail 的安全性已经提高很多了（以前它通常是黑客重点攻击的程序）。然而，Sendmail 还是有一个很严重的问题。一旦出现了安全漏洞（例如：最近出现的 Linux 内核错误），Sendmail 就是被黑客重点攻击的程序，因为 Sendmail 是以 root 权限运行而且代码很庞大容易出问题。

几乎所有的 Linux 发行商都把 Sendmail 作为默认的配置，只有少数几个把 Postfix 或 Qmail 作为可选的软件包。但是，很少有 Linux 的发行商在自己的邮件服务器上使用 Sendmail。SuSE 和 Red Hat 都使用基于 Qmail 的系统。

Sendmail 并不一定会被别的程序完全替代。但是它的两个替代程序 Qmail 和 Postfix 都比它安全、速度快，而且特别是 Postfix 比它容易配置和维护。

5.4 su

su 是用来改变当前用户的 ID，转换成别的用户。你可以以普通用户登录，当需要以 root 身份做一些事的时候，只要执行“su”命令，然后输入 root 的密码。

su 本身是没有问题的，但是它会让人养成不好的习惯。如果一个系统有多个管理员，必须都给他们 root 的口令。

su 的一个替代程序是 sudo。Red Hat 6.2 中包含这个软件。sudo 允许你设置哪个用户哪个组可以以 root 身份执行哪些程序。你还可以根据用户登录的位置对他们加以限制（如果有人“破”了一个用户的口令，并用这个帐号从远程计算机登录，你可以限制他使用 sudo）。Debian 也有一个类似的程序叫 super，与 sudo 比较各有优缺点。

让用户养成良好的习惯。使用 root 帐号并让多个人知道 root 的密码并不是一个好的习惯。这就是 www.apache.org 被入侵的原因，因为它有多个系统管理员他们都有 root 的特权。一个乱成一团的系统是很容易被入侵的。

5.5 named

大部分 Linux 的发行商都解决了这个问题。named 以前是以 root 运行的，因此当 named 出现新的漏洞的时候，很容易就可以入侵一些很重要的计算机并获得 root 权限。现在只要用命令行的一些参数就能让 named 以非 root 的用户运行。而且，现在绝大多数 Linux 的发行商都让 named 以普通用户的权限运行。命令格式通常为：named -u ; -g ;

5.6 INN

在 INN 的文档中已经明确地指出：“禁止这项功能（verifycancels），这项功能是没有用的而且将被除掉”。大约在一个月前，一个黑客发布了当“verifycancels”生效的时候入侵 INN 的方法。Red Hat 是把“verifycancels”设为有效的。任何 setuid/setgid 的程序或网络服务程序都要正确地安装并且进行检查以保证尽量没

有安全漏洞。

6.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。