增强 LINUX 系统安全的措施

the defence measure of improving security on linux operation system

傅　斌（河南郑州解放军信息工程大学信息工程学院研究生 450002）

摘要：本文主要针对 Linux 操作系统的不安全因素，从防御者的角度系统阐述了增强 linux 操作系统安全性的防御措施。

关键词：linux　安全

1　基本安全措施

(1) 只安装必需的软件包

Linux 发布时会在系统中配置大量不必要的服务。有缺陷的软件会危及系统，因此，只安装必需的软件包对于需要建立安全的 Linux 环境的用户来讲绝对是颠扑不破的真理。

2　root 登录 tty 设备

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
```

这样只允许 root 在 tty1 终端登录。

3　阻止 linux 操作系统响应任何从外部/内部来的 ping 请求

如果没有人能 ping 通你的机器并收到响应，系统安全性会大大增强。可以把这一行加到“ /etc /rc.d /rc. local”文件中去，这样当系统重新启动的时候，该命令就会自动运行。

```
echo 1 > /proc /sys /net /ipv4 /icmp_echo_ignore_all
```

运行完这个命令后，系统对 ping 就没有反应了。对 ping 命令没有反应，可以把绝大多数的黑客排除到系统之外，因为黑客不可能知道你的服务器在哪里。重新恢复对 ping 的响应，可以用下面的命令：

```
echo 0 > /proc /sys /net /ipv4 /icmp_echo_ignore_all"
```

4　SYN 潮涌攻击对策

最好的办法是增加队列容量，并缩短超时值，从而更加难以填满。可以修改 linux 目录下 /proc 下的几项，以缩短等待 SYN|ACK 的超时时间并增加队列中 SYN 数据包的最大的数目：

```
# cat /proc /sys /net /ipv4 /vs /timeout_synack
100
# cat /proc /sys /net /ipv4 /vs /timeout_synrecv
10
# cat /proc /sys /net /ipv4 /tcp_max_syn_backlog
128
```

如果正在遭到 SYN 攻击，可以增加 tcp_max_syn_backlog 的值并减少 timeout_* 的值。

5　使“/etc/services”文件免疫

使“ /etc /services”文件免疫，防止未经许可的删除或添加服务：

```
[root@kapil /]# chattr +i /etc /services
```

6　禁止 Control－Alt－Delete 键盘关闭命令

在“ /etc /inittab” 文件中注释掉下面这行(使用 #)：

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

改为：

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

为了使这项改动起作用，输入下面这个命令：

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

7　隐藏系统信息

在缺省情况下，当你登陆到 linux 系统，它会告诉你该 linux 发行版的名称、版本、内核版本、服务器的名称。对于黑客来说这些信息足够它入侵你的系统了。你应该只给它

显示一个"login:"提示符。

第一步:

编辑"/etc/rc.d/rc.local"文件,在下面显示的这些行前加一个"#",把输出信息的命令注释掉。

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

第二步:

删除"/etc"目录下的"isue.net"和"issue"文件:

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

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

8 LILO Security

在"/etc/lilo.conf"文件中加入下面三个参数:time-out,restricted,password。这三个参数可以使你的系统在启动 lilo 时就要求密码验证。

第一步:

编辑 lilo.conf 文件(vi /etc/lilo.comf),假如或改变这三个参数:

boot= /dev/hda

map= /boot/map

install= /boot/boot.b

time-out=00 #把这行该为 00

prompt

Default=linux

restricted #加入这行

password=<password>#加入这行并设置自己的密码

image= /boot/vmlinuz-2.2.14-12

label=linux

initrd= /boot/initrd-2.2.14-12.img

root= /dev/hda6

read-only

第二步:

因为"/etc/lilo.conf"文件中包含明文密码,所以要把它设置为 root 权限读取。

[root@kapil /]# chmod 600 /etc/lilo.conf

第三步:

更新系统,以便对"/etc/lilo.conf"文件做的修改起作用。

[Root@kapil /]# /sbin/lilo -v

第四步:

使用"chattr"命令使"/etc/lilo.conf"文件变为不可改变。

[root@kapil /]# chattr +i /etc/lilo.conf

这样可以防止对"/etc/lilo.conf"任何改变(以外或其他原因)

9 阻止源路由

源路由(source routing)允许发送者指定数据包到达目的前在 internet 上经由的路径。这一特点对于网络勘探和调试很有用,但也能用来绕过安全网关和地址转换。如果攻击者能够向某个网络发送源路由数据包,就更容易伪装成该网络上的地址。

以下命令可以确定系统是否允许源路由数据包。

cat /proc/sys/net/ipv4/conf/eth0/accept_source_route

1

0 表示不允许,1 表示允许

除非需要接受源路由,否则就应当关闭 linux 内核中的源路由,可使用如下命令:

echo 0 > /proc/sys/net/ipv4/conf/eth0/accept_source_route

参考文献

1 Brian Hatch, James Lee. Hacking Linux Exposed: linux security secrets & solutions,清华大学出版社。

2 汪辉、张冕洲,linux 安全最大化,电子工业出版社。

(上接第 73 页)

为方便读者,本文中的例程已经放在互联网上,下载地址:http://oldsong.nease.net/callback-sample.zip

参考文献

1 王晓武、陈宗敏、杜兴国, MapBasic 程序设计[M],电子工业出版社,2000。

2 潘爱民、王国印 译, Visual C++技术内幕第四版[M],清华大学出版社,1999。