linux 系统安全设置总结

众所周知，网络安全是一个非常重要的课题，而服务器是网络安全中最关键的环节。Linux 被认为是一个比较安全的 Internet 服务器，作为一种开放源代码操作系统，一旦 Linux 系统中发现有安全漏洞，Internet 上来自世界各地的志愿者会踊跃修补它。然而，系统管理员往往不能及时地得到信息并进行更正，这就给黑客以可乘之机。相对于这些系统本身的安全漏洞，更多的安全问题是由不当的配置造成的，可以通过适当的配置来防止。服务器上运行的服务越多，不当的配置出现的机会也就越多，出现安全问题的可能性就越大。对此，下面将介绍一些增强 Linux/Unix 服务器系统安全性的知识。

一、系统安全记录文件

操作系统内部的记录文件是检测是否有网络入侵的重要线索。如果您的系统是直接连到 Internet，您发现有很多人对您的系统做 Telnet/FTP 登录尝试，可以运行\"#more /var/log/secure | grep refused\"来检查系统所受到的攻击，以便采取相应的对策，如使用 SSH 来替换 Telnet/rlogin 等。

二、启动和登录安全性

1．BIOS 安全

设置 BIOS 密码且修改引导次序禁止从软盘启动系统。

2．用户口令

用户口令是 Linux 安全的一个基本起点，很多人使用的用户口令过于简单，这等于给侵入者敞开了大门，虽然从理论上说，只要有足够的时间和资源可以利用，就没有不能破解的用户口令，但选取得当的口令是难于破解的。较好的用户

口令是那些只有他自己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。

3．默认账号

应该禁止所有默认的被操作系统本身启动的并且不必要的账号，当您第一次安装系统时就应该这么做，Linux 提供了很多默认账号，而账号越多，系统就越容易受到攻击。 可以用下面的命令删除账号。

```
# userdel 用户名
```

或者用以下的命令删除组用户账号。

```
 # groupdel username
```

4．口令文件

chattr 命令给下面的文件加上不可更改属性，从而防止非授权用户获得权限。

```
# chattr +i /etc/passwd    # chattr +i /etc/shadow

# chattr +i /etc/group    # chattr +i /etc/gshadow
```

5．禁止 Ctrl+Alt+Delete 重新启动机器命令

修改/etc/inittab 文件，将\"ca::ctrlaltdel:/sbin/shutdown -t3 -r now\"一行注释掉。然后重新设置/etc/rc.d/init.d/目录下所有文件的许可权限，运行如下命令：

```
# chmod -R 700 /etc/rc.d/init.d/*
```

这样便仅有 root 可以读、写或执行上述所有脚本文件。

6．限制 su 命令

如果您不想任何人能够 su 作为 root，可以编辑/etc/pam.d/su 文件，增加如下两行：

```
auth sufficient /lib/security/pam_rootok.so debug

auth required /lib/security/pam_wheel.so group=isd
```

这时，仅 isd 组的用户可以 su 作为 root。此后，如果您希望用户 admin 能够 su 作为 root，可以运行如下命令：

```
# usermod -G10 admin
```

7．删减登录信息

默认情况下，登录提示信息包括 Linux 发行版、内核版本名和服务器主机名等。对于一台安全性要求较高的机器来说这样泄漏了过多的信息。可以编辑/etc/rc.d/rc.local 将输出系统信息的如下行注释掉。

```
# This will overwrite /etc/issue at every boot. So， ma
ke any changes you

# want to make to /etc/issue here or you will lose the
m when you reboot.

# echo \"\" > /etc/issue

# echo \"$R\" >> /etc/issue

# echo \"Kernel $(uname -r) on $a $(uname -m)\" >> /et
c/issue
```

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

# echo >> /etc/issue
```

然后，进行如下操作：

```
# rm -f /etc/issue    # rm -f /etc/issue.net    # touch /etc/issue    # touch /etc/issue.net
```

三、限制网络访问

1．NFS 访问

如果你使用 NFS 网络文件系统服务，应该确保您的/etc/exports 具有最严格的访问权限设置，也就是意味着不要使用任何通配符、不允许 root 写权限并且只能安装为只读文件系统。编辑文件/etc/exports 并加入如下两行。

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

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

/dir/to/export 是您想输出的目录，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。为了使改动生效，运行如下命令：

```
  # /usr/sbin/exportfs -a
```

2．Inetd 设置

首先要确认/etc/inetd.conf 的所有者是 root，且文件权限设置为 600。设置完成后，可以使用\"stat\"命令进行检查。

```
# chmod 600 /etc/inetd.conf
```

然后，编辑/etc/inetd.conf 禁止以下服务。

```
ftp telnet shell login exec talk ntalk imap pop-2 po
p-3 finger auth
```

如果您安装了 ssh/scp，也可以禁止掉 Telnet/FTP。为了使改变生效，运行如下命令：

```
#killall -HUP inetd
```

默认情况下，多数 Linux 系统允许所有的请求，而用 TCP_WRAPPERS 增强系统安全性是举手之劳，您可以修改/etc/hosts.deny 和/etc/hosts.allow 来增加访问限制。例如，将/etc/hosts.deny 设为\"ALL: ALL\"可以默认拒绝所有访问。然后在/etc/hosts.allow 文件中添加允许的访问。例如，

\"sshd: 192.168.1.10/255.255.255.0 gate.openarch.com\"表示允许 IP 地址 192.168.1.10 和主机名 gate.openarch.com 允许通过 SSH 连接。

配置完成后，可以用 tcpdchk 检查: # tcpdchk

tcpchk 是 TCP_Wrapper 配置检查工具，它检查您的 tcp wrapper 配置并报告所有发现的潜在/存在的问题。

3．登录终端设置

/etc/securetty 文件指定了允许 root 登录的 tty 设备，由/bin/login 程序读取，其格式是一个被允许的名字列表，您可以编辑/etc/securetty 且注释掉如下的行。 #tty1 # tty2 # tty3 # tty4 # tty5 # tty6

这时，root 仅可在 tty1 终端登录。

4．避免显示系统和版本信息。

如果您希望远程登录用户看不到系统和版本信息，可以通过一下操作改变/etc/inetd.conf 文件：

```
    telnet stream tcp nowait root /usr/sbin/tcpd in.telnet
d –h
```

加-h 表示 telnet 不显示系统信息，而仅仅显示\"login:\"

四、防止攻击

1．阻止 ping

如果没人能 ping 通您的系统，安全性自然增加了。为此，可以在/etc/rc.d/rc.local 文件中增加如下一行：

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

2．防止 IP 欺骗

编辑 host.conf 文件并增加如下几行来防止 IP 欺骗攻击。

order bind，hosts　multi off　nospoof on　3．防止 DoS 攻击

对系统所有的用户设置资源限制可以防止 DoS 类型攻击。如最大进程数和内存使用数量等。例如，可以在/etc/security/limits.conf 中添加如下几行：

```
    * hard core 0    * hard rss 5000    * hard nproc 20
```

然后必须编辑/etc/pam.d/login 文件检查下面一行是否存在。

session required /lib/security/pam_limits.so

上面的命令禁止调试文件，限制进程数为 50 并且限制内存使用为 5MB。

经过以上的设置，你的 Linux 服务器已经可以对绝大多数已知的安全问题和网络攻击具有免疫能力，但一名优秀的系统管理员仍然要时刻注意网络安全动态，随时对已经暴露出的和潜在安全漏洞进行修补。