服务器知识手册（十五）

狄登峰 主编

需要全本请访问 www.ertongbook.com

目　　录

UNIX 系列 1
UNIX 安全构架的九点经验 1
SCOUnix 系统中如何使用 Modem 8
UNIX 应急启动盘制作与安全管理 14
UNIX 防止非法用户注册的技术 16
为 UNIX 服务器设置 Oracle 全文检索 19
运用 CrackLib 构建安全的 Unix 口令 30
下一代系统日志工具(syslog-ng) 36
四种实时操作系统的分析比较 50
制作 Unix 系统备份 57
高端 UNIX 服务器介绍 62
在 HP－UX 服务器上实现用户空间限制 80
HP-UX 系统备份与恢复全功略 83
第二代的 UNIX 系统----AIX 96
拯救 UNIX 系统技巧二则 98
HPMC/ServiceGuard 的安装和配置 100
IBMAix 上 Qmail 的建立 107
HPMC/ServiceGuard 背景知识和原理 112
HP/IEI 大容量电子邮件系统方案 123

UNIX 系列

UNIX 安全构架的九点经验

下面是一些个人的经验的总结，相信对于是否受到入侵的 UNIX 或者 UNIX-clonefreebsd,openbsd，netbsd,linux,etc)都是有用的：

首先大家可以通过下面的系统命令和配置文件来跟踪入侵者的来源路径：

1.who------(查看谁登陆到系统中)

2.w--------(查看谁登陆到系统中，且在做什么)

3.last-----(显示系统曾经被登陆的用户和 TTYS）

4.lastcomm-(显示系统过去被运行的命令)

5.netstat--(可以查看现在的网络状态，如 telnet 到你机器上来的用户的 IP 地址,还有一些其它的网络状态。)

6.查看 router 的信息。

7./var/log/messages 查看外部用户的登陆状况

8.用 finger 查看所有的登陆用户。

9.查看用户目录下/home/username 下的登陆历史文件(.history.rchist,etc).后注:'who','w','las和'lastcomm这些命令依靠的是/var/log/pacct,/var/log/wtmp,/etc/utmp 来报告信息给你。许多精明的系统管理员对于入侵者都会屏蔽这些日志信息(/var/log/*,/var/log/wtmp,etc)建议大家安装 tcp_wrapper 非法登陆到你机器的所有连接)

接下来系统管理员要关闭所有可能的后门，一定要

防止入侵者从外部访问内部网络的可能。如果入侵者发现系统管理员发现他已经进入系统，他可能会通过 rm-rf/*试着隐蔽自己的痕迹.

第三，我们要保护下面的系统命令和系统配置文件以防止入侵者替换获得修改系统的权利。

1./bin/login

2./usr/etc/in.*文件(例如:in.telnetd)

3.inetd 超级守护进程(监听端口，等待请求，派生相应服务器进程)唤醒的服务.(下列的服务器进程通常由 inetd 启动:

fingerd(79),ftpd(21),

rlogind(klogin,eklogin,etc),rshd,talkd,telnetd(23),tftpd.inetd 还可以启动其它内部服务，

/etc/inetd.conf 中定义的服务.

4.不允非常 ROOT 用户使用 netstat,ps,ifconfig,su

第四，系统管理员要定期去观察系统的变化（如：文件，系统时间，等）

1.#ls-lac 去查看文件真正的修改时间。

2.#cmpfile1file2 来比较文件大小的变化。

第五，我们一定要防止非法用户使用 suid(set-user-id)程序来得到 ROOT 的权限。

1.首先我们要发现系统中所有的 SUID 程序。

#find/-typef-perm-4000-ls

2.然后我们要分析整个系统，以保证系统没有后门。

第六，系统管理员要定时的检查用户的.rhosts,.forward 文件

1.#find/-name.rhosts-ls-o-name.forward-ls

来检查.rhosts 文件是否包含'++'有则用户可以远程

修改这个文件而不需要任何口令。

2.#find/-ctime-2-ctime+1-ls

来查看不到两天以内修改的一些文件，从而判断是否有非法用户闯入系统。

第七，要确认你的系统当中有最新的 sendmail 守护程序，因为老的 sendmail 守护程序允许其它 UNIX 机器远程运行一些非法的命令。

第八，系统管理员应当要从你机器，操作系统生产商那里获得安全补丁程序，如果是自由软件的话(如 Linux 平台，建议大家可以到 linux.box.sk 来获得最好的安全程序和安全资料。)

第九，下面有一些检查方法来监测机器是否容易受到攻击。

1.#rpcinfo-p 来检查你的机器是否运行了一些不必要的进程。

2.#vi/etc/hosts.equiv 文件来检查你不值得信任的主机，去掉。

3.如果没有屏蔽/etc/inetd.conf 中的 tftpd,请在你的/etc/inetd.conf 加入 tftpdgramudpwaitnobody/usr/etc/in.tftpd in.tftpd-s/tftpboot

4.建议你备份/etc/rc.conf 文件，写一个 shellscript 定期比较 cmprc.confbackup.rc.conf

5.检查你的 inetd.conf 和/etc/services 文件，确保没有非法用户在里面添加一些服务。

6.把你的系统的/var/log/*下面的日志文件备份到一个安全的地方，以防止入侵者#rm/var/log/*

7.一定要确保匿名 FTP 服务器的配置正确，我的机器用的是 proftpd,在 proftpd.conf 一定要配置正确。

需要全本请访问 www.ertongbook.com

8.备份好/etc/passwd,然后改变 root 口令。一定要确保此文件不能够入侵者访问，以防止它猜测。

9.如果你还不能够防止入侵者的非法闯入，你可以安装 ident 后台守护进程和 TCPD 后台守护进程来发现入侵者使用的帐号！

10.确保你的控制台终端是安全的，以防止非法用户能够远程登陆你的网络上来。

11.检查 hosts.equiv,.rhosts,hosts,lpd 都有注释标识#，如果一个入侵者用它的主机名代替了#，那么就意味着他不需要任何口令就能够访问你的机器。

UNIX 如何实现拨号上网

现在虽然 Windows 是主流，但在金融等行业的网络应用中，经常使用 UNIX 平台，这类平台又该如何实现拨号上网呢?让 e 博士来回答你吧!

一、配置前的准备工作

配置拨号连接前，请先使用 pkginfo 命令确认系统已经安装了 uucp 和 ppp。可能有时候使用该命令无法得到必要的信息·那么可以检查是否有系统目录/usr/lib/uucp 存在；如果安装并启动了 pppd，通过命令：

ps-ef|grep"pppd"

可以看到两条以上信息显示。

注意：在配置拨号连接过程中，pppd 有可能被关闭，这时最好重新启动系统。

二、安装调制解调器

1.将你的调制解调器连接到计算机的 COM1 口，加电打开机器和调制解调器，以 root 身份登录系统后，输入 scoadminmodem。

进入 ModemManager 界面，该界面的操作可以通过

Tab 或箭头键进行切换，用空格键或回车键选中或确认。

2.选择菜单命令“Modem/Add/ManualConfiguration...”添加 Modem（也可以采用自动检测方式，但是当系统的硬件支持列表中不包含你所用的 Modem 时，检测会失败），进入 ModemConfiguration 界面。

3.在 ModemVendor（Modem 提供商）选项：选择所用的 Modem 的型号，如果不能确定所用的 Modem 具体型号最好选择第一项•StandardModemType•；

4.ModemModel•Modem 类型•选项：可以按照所使用的 Modem 的速率来选择，也可以选择最后一项——StandardModem；

5.Modemport 选项：从列表中选择一个端口，如果列表为空则在其右侧的 Addport...中增加一个端口，一般是在 COM1 上添加一个最高速率无应答方式的端口 tty1A；

6.Linespeed（bps）：选择合适的速率；

7.Answermode 请选择 off；

8.设置完成后选“OK”回到主 ModemManager 界面。这时你应该看到有如下一条信息：

StandardModemNotty1A38400Standard_Modem

选择菜单命令“Host/Exit”退出。

三、添加 PPP 连接

1.在命令行提示符下键入以下命令：

scoadminnetwork 或 netconfig

这就进入了 NetworkConfigurationManager 界面；

2.选择“Hardware/CreateaNewWANconnection”菜单命令，在“AddnewWANconnection”界面中选择“SWSCOTCP/IPPPPDriver”项，OK 之后询问添加什么协议，选择

TCP/IP 协议；

3.下一步出现 PPPConnectionType 设置界面。选择 ManualOutgoing（手工拨出）；

4.接着出现 PPPManualOutgoingLinkConfiguration 配置界面，请按如下方式配置，其他项为空即可：

AttachName：163

HostIPaddress：0.0.0.0

DestinationIPaddress：0.0.0.0

Netmask：255.255.255.0

Gateway：<*>Yes<>No

5.完成后“OK”回到主 NetworkConfigurationManager 界面，系统会提示是否配置其他的 link，选择 No，然后系统会提示 re-linkedkernel，在 re-linkedkernel 的过程中系统有两个提问，全部选择 y。

最后选择“Hardwaew/Exit”菜单命令退出。

由于系统重新连接了内核，最好用 ps-ef|grepppd 再检查一下 pppd 守护进程是否仍在运行，否则请重新启动系统。

四、完善工作

以上配置完成后，运行 scoadminppp 命令进一步完善，进入 PPPManager 界面后，应该看到如下一条信息：

KMManualDialupfrom0.0.0.0to0.0.0.0

选择菜单命令“Endpoint/Modify...”，进入该配置信息的详细配置界面 ManualDialupConfiguration。其中各项应按如下配置：

Remotesystem：163

PhoneNumber：163

Localaddress：0.0.0.0

Remoteaddress：0.0.0.0

Netmask：255.255.255.0

AttachName：163

进入 Editscript……，**将登录脚本中的** UserName **和** Password **改成合法的用户名和口令字符串。最后选**“OK”**回到主界面，选择菜单命令**“Host/Exit”**退出。**

五、有关命令和系统文件

以上配置完成后，就可以利用命令 pppattach163 **拨号上网了。拨号连通后有时可能无法生成正确的路由，可以创建如下脚本文件：**

```
vidialon
#•/bin/sh
#Scriptfordialto163
pppattach163
sleep50
whiletrue
do
iftest-n"‘/etc/ifconfig-a|grep’ppp0’‘"
then
ADDRESS="‘/etc/ifconfigppp0|grep’inet’|awk’•print$
2’‘"
routedeletedefault>/dev/null
routeadddefault$ADDRESS>/dev/null
echo"Ontheline•"&&exit1
else
echo"Can’tconnecttotheNetwork，failtodial•"
exit0
fi
```

done

存盘退出后，将 dialon 文件赋予可执行权限：

chmod+xdialon

这样，也可以运行./dialon 拨号上网。当需要挂断拨号连接时，使用命令 ifconfigppp0down 即可。

SCOUnix 系统中如何使用 Modem

SCOUnix 是 PC 机上常用的一种 Unix 操作系统，被广泛地应用在银行、保险、税务等大型的应用系统中。在这些系统中，经常要通过电话线进行远距离的通信。为了完成这一功能，就要在装有 SCOUnix 操作系统的计算机上安装调制解调器（Modem）。但是，在 SCOUnix 操作系统下安装调制解调器要比在其他操作系统下安装有一定的难度。因此，本文将介绍一种在 SCOUnix 系统下对调制解调器进行安装与设置的方法和过程，供大家参考。

1、串行端口的选择

对于内部调制解调器，由于难调试，有时会出现一些不易解决的中断冲突，因此建议采用外部调制解调器。要采用外部调制解调器，必须选择一个用来连接外部调制解调器的串行端口。在表 1 中列出带有或不带有调制解调器控制的串行端口的常用设备的名称。

表常用串行端口

设备名	功能
/dev/tty1a	无调制解调器控制的串行端口 1（COM1）

/dev/tty1A	有调制解调器控制的串行端口 1（COM1）
/dev/tty2a	无调制解调器控制的串行端口 2（COM2）
/dev/tty2A	有调制解调器控制的串行端口 2（COM2）

/dev/tty1a 与/dev/tty1A 实际上是同一个串行端口（/dev/tty2a 与/dev/tty2A 也是如此）。对于每一种设备，操作系统使用不同的设备驱动子程序。决不可同时使用有调制解调器控制的端口和无调制解调器控制的端口，否则将会看到警告信息：

Cannotopen：devicebusy

对于包含多口串行卡的系统，设备/dev/tty[1,2][a-m]使用无调制解调器控制的端口，设备/dev/tty[1,2][A-M]使用有调制解调器控制的端口。

2、调制解调器的安装

2.1.拨出调制解调器的安装

为安装拨出的调制解调器，可按照下面的步骤进行：

(1).保证已经安装了 uucp。如果没有安装，可用 Custom（ADM）进行安装。

(2).保证所选的用于拨出调制解调器的串行口在系统自举时能被识别。如果采用的是内部调制解调器，则须保证为内部调制解调器设置的 COM 端口不会与其他设备发生冲突。

(3).通过输入 disable（C）使端口被禁止。disablettyname

(4).用直通线缆把调制解调器与计算机连接。

(5).把正确的项加到/dev/lib/uucp/Devices 文件中。

需要全本请访问 www.ertongbook.com

对于每个用于调制解调器的串行端口，该文件应该有两项，当使用调制解调器（ACU 线，ACU 表示自动呼叫单元）启动呼叫时，使用其中的一个项，另一条线通过标准 Hays 命令集配置调制解调器。用户应该按下述方法使用这些项，通过 COM1 对工作在 2400 波特的 Hays 兼容的调制解调器进行设置：

Directtty1a1200-2400direct

ACUtty1a1200-2400/usr/lib/uucp/dialHA24

(6).输入下述命令，使 uucp 成为用户所选端口的拥有者：

chownuucp/dev/ttyname

至此，拨出调制解调器设置完成，用户可以准备测试拨出的调制解调器。测试的步骤如下：

(1).通过输入下述命令，测试调制解调器能否正确拨号：

cu-ltty1adir

用户应当看到已被连接的消息。如果看到“cu：dirpermissiondenied”消息，则说明执行 cu 命令的用户对/usr/lib/uucp/Devices 文件不具有写权限。如果用户看不到这一消息，而且不出现表明连接正确的消息，那么说明 cu 命令不对，Devices 文件不对，或者串行端口工作不正常。

(2).如果看到能证实线路连通的消息，可输入下述命令：

AT

屏幕上应回显“OK”。如果设定调制解调器返回的结果码为数字码而不是文本，这时会看到

“0”。

(3).如果不出现上述情况，可按一个键，观察调制解

调器上的“receive”灯是否在闪。如果该灯在闪，表明调制解调器正在接受键盘发来的信号。如果该灯不闪，则应检查线缆及调制解调器开关设置情况。如果该灯在闪，但是仍然得不到调制解调器发来的“OK”响应，可输入下述命令使调制解调器具有回显能力：

ATE1

(4).如果终端上仍然不显示“OK”或者“0”，可将调制解调器连接到另一个端口（COM1 或 COM2）。如果调制解调器用一个新端口工作，则应检查设备所用的中断向量是否正确（COM1 使用中断 4，COM2 使用中断 3）。

(5).接到新的端口后，如果终端不回显“OK”消息，则说明调制解调器已损坏。一旦调制解调器被正确配置后，终端会回送预期的响应，这时可输入下述命令进行拨出：ATDT 电话号码如果已经证实调制解调器可以拨出，可输入下述命令并按回车键，退出 cu，表明拨出调制解调器已经设置完成。

2.2.安装拨入的调制解调器

安装拨入调制解调器可按如下的步骤进行：

(1).紧接在安装拨出调制解调器的步骤之后，继续往下进行，这样可保证硬件的连接是正常的。

(2).某些调制解调器具有开关或者软件命令，用于设置调制解调器。如果用户的调制解调器具有这种设置，则可按照调制解调器手册指出的方法进行设置。

(3).将调制解调器设定成为呼叫进入时能自动应答。多数内部调制解调器没有自动应答，某些外部调制解调器也没有这种设置。如果出现这种情况，可将下述一行内容放到初始化文件/etc/re.d/8/userdef 中：

（stty1200;echo“ATS0=1\r”>/dev/tty1a）<dev/tty1a

tty1a 应该与连接到调制解调器的无调制解调器控制设备相匹配。1200 应当是调制解调器所用的最高波特率。ATS0=1 是使 Hayes 兼容的调制解调器处在自动应答方式的命令。\r 发送回车信号到调制解调器使该命令终止。

(4).对调制解调器进行设置，使得 DTR 线不激活时不作应答，且当 DTR 线从激活变成不激活时调制解调器与当前的连接断开。

(5).CD 线应设置成依照进入的载波，也就是说载波出现时该线为低电平，载波不出现时为高电平。

(6).对调制解调器进行设置，使得它不回显或显示响应。

(7).输入 disable（C）命令确保端口已被去能：

disablettyname

这里 ttyname 为非调制解调器的控制端口。

(8).在/etc/inittab 文件中选择所要求的 gettydefs 项。输入"2"选择 1200-2400-300 周期。

(9).输入 enable（C）命令使能调制解调器正在使用的端口：

enablettyname

这里 ttyname 为有调制解调器的控制端口。

(10).从另外一个调制解调器拨入该调制解调器。

2.3.安装拨入、拨出的调制解调器

SCOUnix 系统支持在同一条调制解调器线路上共用拨入和拨出，不需要去能注册。当拨出程序正在使用线路时，login（注册）被去能。如果当拨出程序打算使用某线路时，有用户在该线路上注册，这时拨出程序无法锁定该设备。为使这一特性能正常工作，必须使用调

制解调器控制设备，而且调制解调器必须设置成：当载波出现时 CD 为高电平，当载波不出现时为低电平。

下列过程允许用户安装拨入、拨出的调制解调器：

(1).执行安装拨出调制解调器的步骤，再完成安装拨入调制解调器的各步骤。

(2).为了进行拨出，可通过适当的任选项调用。呼出时，线路上的 getty 自动挂起，呼叫时又重新启动。

2.4.拨入用户的计算机

为了允许拨入用户的计算机，必须使用 enable（C）命令使能能识别调制解调器控制信号的串行线。如果使用串行端口 1（COM1），可输入：

disabletty1a

enabletty1A

如果使用串行端口 2（COM2），可输入：

disabletty2a

enabletty2A

注意，tty1A 与 tty1a、tty2A 与 tty2a 涉及同一个串行线路，不要同时在调制解调器和非调制解调器方式下使用同一条线路，否则要出错。

2.5.从用户的计算机拨出

cu（C）和 uucp（C）实用程序呼叫远程系统并在 UNIX 系统上传送数据。/usr/lib/uucp/Devices 包含这二个程序所用的信息，用来确定特定串行线路的特性。文件由好几行内容组成，这些行确定了设备所接的线路、与线路有关的呼叫装置及 UUCP 所用的波特率。

3、结束语

在 SCOUnix 系统下利用 UUCP 构造远程网，Modem（调制解调器）的安装与设置是非常重要的方面。本

文比较全面地讨论了在 SCOUnix 系统下安装 Modem 的方法和过程，并着重介绍了在安装过程中应该注意的一些问题。我们在利用 UUCP 构造“沈阳太平洋保险公司业务管理系统”的远程网时，采用了本文介绍的关于 Modem 的安装方法，使整个系统的安装与调试得以顺利进行，取得了较理想的效果。

UNIX 应急启动盘制作与安全管理

系统崩溃是每个系统管理员都不愿看到的，UNIX 下提供了一个修复错误、安全恢复系统的工具——应急启动盘。怎样利用该工具，很多文章都有介绍，本文不再赘述，这里仅就该启动盘在安全管理上的问题作一番探讨。

先来制作一套应急盘，以超级用户注册或在单用户维护方式下健入：“mkdevfd”,出现提示：

FloppyDiskFilesysetmCreationProgram

Choicesfortypeoffloppyfilesystem.

1.48tpi,doublesided,9sectorspertrack

2.96tpi,doublesided,15sectorspertrack

3.135tpi,doublesided,9sectorspertrack

4.135tpi,doublesided,18sectorspertrack

Enteranoptionorqtoquit:

选择磁盘类型，如 1•44 兆软盘应选"4"。然后出现：

Choicesforcontentsoffloppyfilesystem.

1.Filesystem

2.Bootableonly(96ds15and135ds18only)

3.Rootfilesystemonly(96ds15and135ds18only)

Enteranoptionorqtoquit:

选"2"为建立 Boot 盘，"3"为建立根文件系统盘。之后提示插盘及询问是否先格式化，回答后开始按所选类型建立文件系统，Boot 盘用于启动系统，Rootfilesystem 盘则包含了一个软盘 UNIX 系统所需的各个文件。若系统中安装了较多的应用软件，/unix 文件较大时，可能无法建立 boot 盘，这样的话用系统安装盘中的 N1 盘代替也可。另外，原则上是不同的系统之间应急盘不能互换，但也不排除某些特殊情况。

下面谈谈应急启动盘对系统安全的影响。

众所周知，对系统的最大威胁莫过于非法用户获取了超级用户权限，而掌握了某系统的应急盘，也就相当于控制了该系统，据笔者试验，至少有两种方法可以达到目的。

第一种：找到现有系统的安装盘，在另外一台机器上装系统并制作一套应急启动盘，用 boot 盘启动欲进入之系统，在出现 boot：后按回车，根据提示插入 filesystem 盘并回车，不一会出现"＃"提示符，现在将硬盘挂到软盘上：

＃mount/dev/hd0root/mnt

成功后先备份/etc/passwd、shadow 文件，然后将软盘上的 passwd 及 shadow 文件拷入硬盘，

＃cp/etc/passwd/mnt/etc

＃cp/etc/shadow/mnt/etc

之后卸下硬盘，＃umount/mnt,由硬盘启动，即可以 root 注册，出现"＃"符后将原 passwd 及 shadow 文件恢复过来，这样就不会影响其它用户，再键入 passwd 命令更改 root 口令。这样，非法用户随时可用新的 root 口令

需要全本请访问 www.ertongbook.com