Linux专家之路

Linux 网络与安全管理

宁磊　周卫　编著　　雨人科技　策划

人民邮电出版社
www.pptph.com.cn

附光盘
CD-ROM

Linux专家之路

Linux

网络与安全管理

宁磊　周卫　编著　　雨人科技　策划

人民邮电出版社

图书在版编目（CIP）数据

Linux 网络与安全管理/宁磊，周卫编著. —北京：人民邮电出版社，2001.11

（Linux 专家之路）

ISBN 7-115-09789-5

I.L… II.①宁…②周… III. Linux 操作系统—安全技术 IV.TP316.89

中国版本图书馆 CIP 数据核字（2001）第 079743 号

内 容 提 要

本书通过大量的 Linux 程序实例，系统地介绍了 Linux 系统的网络和安全管理。本书语言生动、结构严谨、通俗易懂，能够使读者在最短的时间内完全掌握 Linux 系统管理技术的精髓。

全书共分 11 章，第 1 章初步介绍网络安全的基本知识以及启动、关闭系统的方式；第 2 至 4 章详细介绍 Linux 系统管理中的用户管理、进程管理和网络管理三个方面；第 5 至 11 章主要介绍网络安全方面的具体内容，包括网络的基础、数据包结构和防火墙设置等重要内容。

本书主要适合那些对 Linux 操作系统有所了解，并希望深入学习有关网络管理方面技术的读者阅读，也可作为技术开发人员的参考资料。

linux 专家之路

Linux 网络与安全管理

◆ 编　　著　宁　磊　周　卫
策　　划　雨人科技
责任编辑　张瑞喜
执行编辑　郭立罡

◆ 人民邮电出版社出版发行　北京市崇文区夕照寺街 14 号
邮编　100061　　电子函件　315@ pptph.com.cn
网址　http://www.pptph.com.cn
读者热线　010－67129212　010－67129211(传真)
北京汉魂图文设计有限公司制作
北京顺义振华印刷厂印刷
新华书店总店北京发行所经销

◆ 开本：787×1092　1/16
印张：27
字数：655 千字　　2001 年 11 月第 1 版
印数：1－5 000 册　　2001 年 11 月北京第 1 次印刷

ISBN 7-115-09789-5/TP·2538

定价：48.00 元(附光盘)

前　言

Linux 是当今互联网络发展中较为出色的操作系统之一。我们可以借助 Linux 的共享源代码编写一套完全中文化的系统，这将告别汉化“别人的系统”的时代，实现一个中国人自己的操作系统。

在互联网上，许许多多的网络爱好者都对它投入了无比的热情，他们就如同对待婴儿一般地呵护它、保护它。使得 Linux 飞速发展成为可以与微软公司的 Windows 操作系统相比拼的系统。在当今微软一统天下的局势下，Linux 异军突起，举起了对抗微软垄断个人计算机操作系统的大旗。

自从 Linux 的诞生到现在，它始终是结合 Internet 的进步而成长的。可以说，Linux 离不开 Internet，也只有 Internet 的不断发展，Linux 才具有更强壮的生命力。

随着 Linux 进军服务器市场，对于它的系统安全要求也就越来越高。本书是根据作者多年使用 Linux 操作系统的经验，并结合设置网络服务器的防火墙开发实例而编写的。全书以开发实例为主线，在基于 Linux 操作系统平台和 ipchains 开发工具的基础上，详细描述了网络安全管理的具体过程。本书的第 1 章初步介绍了 Linux 操作系统的基础知识；第 2 章至第 4 章则主要介绍了超级用户的几种管理模式；第 5 章至第 11 章详细介绍网络安全方面理论和防火墙实例及调试防火墙等内容。本书配有光盘。光盘内容包括部分习题参考答案，本书的源代码压缩文件，雨人科技技术支持文档，相关软件：APACHE 服务器配置的所有相关文件、CVS 配置文件、邮件服务器配置文件等。

周卫负责全书的设计、统稿和修改，并编写了第 1、5、6、7、8、9、10、11 章；宁磊负责编写了第 2、3、4 章，并负责光盘内容的制作和例子测试。参加本书编写和指导工作的还有刘会双、赵中伟及刘馨宇等同志。在此对所有关心、支持和帮助过本书编写工作的同志表示诚挚的谢意！

书中不足之处敬请读者指正，以便再版时修订。

联系邮箱：yurennet@263.net

雨人科技网站：www.yurennet.com

编著者

2001 年 8 月

目　录

第1章

概述

开机引导和关机过程

UNIX 相关常识

小结与练习

对于 Linux 操作系统的网络管理，最重要的工作就是确保它的安全性，本书正是为那些希望成为管理 Linux 系统、防范黑客入侵的优秀系统管理员而设计编写的。本章主要介绍 Linux 系统的一些基础知识，以及引导和关闭过程中会出现的问题。还包括对一些文件和目录许可的问题。

1.1 开机引导和关机过程

开启计算机并引导加载操作系统的过程称为开机引导。

启动过程中，计算机首先加载一小段 bootstrap loader 程序之后再启动操作系统。bootstrap loader 通常存储在硬盘或软盘的固定位置。由于操作系统庞大而复杂，而计算机加载的这段代码很小，这样就可以避免固件不必要的复杂化。

不同计算机的 bootstrap 是不同的。对于 PC 机，它的 BIOS 通过读取软盘或硬盘的第一个扇区来引导系统。而 bootstrap loader 正是包含在这个扇区中，它加载位于磁盘和其他地方的操作系统。

Linux 的核心被读入内存才是真正的启动，因为在核心被读入之后它要做以下的最基本的工作：

- 由于 Linux 的核心是压缩在固定位置的，它首先需要对自身解压缩。在核心的映像文件开头有一段解压缩程序可以进行解压缩的工作。
- 核心检查计算机系统安装的硬件，包括硬盘、软驱、网卡等，并为它们配置适当的驱动输出相关信息。
- 核心装载文件系统。文件系统的位置在编译时设置。如果读者没有为核心指定相关的文件系统驱动，那么文件系统的装载就会失败，启动停止。
- 核心在后台运行程序 init，这是一个进程号为 1 的进程。
- init 进程通过配置文件，切换系统运行等级，并启动 getty 提供虚拟控制台和串行线。getty 是提供用户通过虚拟控制台和串行线来登录 Linux 系统的一个程序。

这样，开机引导过程结束。

Linux 核心主要包括：进程管理、存储器管理、硬件设备驱动、文件系统驱动、网络管理和其他部分管理。其中最重要的是进程管理和存储器管理。进程管理可以产生进程并管理各种进程使之协调工作，从而实现 Linux 系统的多任务功能。存储管理则负责管理各个进程的存储区域和交换空间。

用户在第一次接触 Linux 系统时，并不一定很清楚开机引导过程的整个经过。在这个过程中，如果使用的是已经设置好的 X Window，并选择图形界面登录系统，便可看到如图 1.1 所示的窗口。

作为系统的管理员，有时候必须要了解在启动过程中，系统都做了什么事情。假使 Linux 开机后没有经过这个引导过程，一般都要求管理员清楚地知道系统什么位置出了问题，以及如何解决这样的问题。

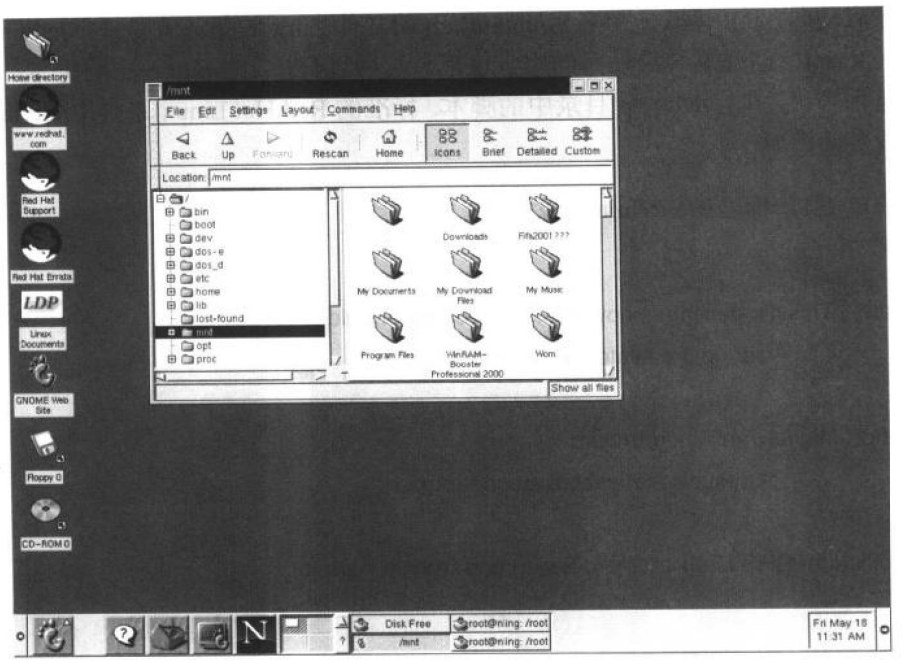

图 1.1　图形界面

注意：在引导系统时，读者可以通过 Shift+PageUp 键，在控制台前查看系统引导信息。系统引导后，也可以运行 dmesg 程序查看引导信息。

Linux 系统可以在控制台上显示出启动过程中系统运行的所有命令，以及系统进行开机引导时执行任务的情况。这些信息可以使管理员很方便地了解自己的系统正在执行的命令。

作为开机引导过程的一部分，init 进程运行的程序是非常关键的。它决定了正在启动的系统将会提供什么服务，以及启动其他允许用户登录进行访问的进程。因此，读者可以定制自己的 init，选择系统的服务环境。下面将详细介绍 init 程序的配置。

1.1.1　配置 init

Linux 加载后，init 初始化硬件和设备驱动程序、然后运行 init 进程。UNIX（Linux）系统中最重要的服务都是由 init 提供的。它是 Linux 系统在核心引导时启动的第一个进程。

init 有两种风格：一种是 V 形式的 init；另一种就是 BSD 形式的 init。Red Hat 版本使用的是 UNIX 系统 V 形式的 init。

注意：这两种形式的 init 之间的区别在于：V 形式的 init 需要使用运行等级，而 BSD 形式的 init 不使用运行等级。因为很少有人会使用 BSD 形式的 init。所以本书仅对 V 形式的 init 进行解释。

在程序启动时，init 读取一个名为/etc/inittab 的文件。init 的任务就是根据/etc/inittab 文件中的脚本（Script）创建系统启动后的服务进程。它通过分析/etc/inittab 中的脚本，按照需要或缺省的运行等级，执行/etc/rc.d 目录中的脚本。标准的 Red Hat Linux 系统中/etc/inittab 配置文件格式请参阅清单 1-1。

程序清单 1-1：标准的/etc/inittab 文件

```
#
#  inittab   This file describes how the INIT process should
#                  set up the system in a certain run-level
#
#  Author: Miquel van Smoorenburg,
#                  <miquels@drinkel.nl.mugnet.org>
#
#  Modified for RHS Linux by Marc Ewing and Donnie Barnes
#

#  Default runlevel. The runlevels used by RHS are:
#
#        0 – halt (Do NOT set initdefault to this)
#        1 – Single-user, without NFS (The same as 3., if you do not have networking)
#        3 – Full multi-user mode
#        4 – unused
#        5 – X11
#        6 – reboot (Do NOT set initdefault to this)
#
id: 3:initdefault:
#
#  System initialization
#
si: sysinit:/etc/rc.d/rc.sysinit

10:0:wait:/etc/rc.d/rc 0
11:1wait:/etc/rc.d/rc 1
12:2:wait:/etc/rc.d/rc 2
13:3:wait:/etc/rc.d/rc 3
14:4:wait:/etc/rc.d/rc 4
15:5:wait:/etc/rc.d/rc 5
16:6:wait:/etc/rc.d/rc 6
```

```
#
#   Things to run in every runlevel
#
ud::once:/sbin/update
#
#   Trap CTRL-ALT-DELETE
#
ca:: ctrlaltdel:/sbin/shutdown -t3 -r now

#   When our UPS tells us power has failed, assume we have
#   a few minutes of power left. Schedule a shutdown for
#   2 minutes from now
#
#   This does,of course,assume you have powerd installed and your
#   UPS connected and working correctly.
#
pf:: powerfail:/sbin/shutdown -f -h +2 " power Failure; System Shutting Down "

#if power was restored before the shutdown kicked in,   cancel it
pr: 12345:powerokwait:/sbin/shutdown -c   " power Restored; Shutdown Cancelled "

#   Run gettys in standard runlevels
1:2345:respawn:/sbin/mingetty tty1
2:2345:respawn:/sbin/mingetty tty2
3:2345:respawn:/sbin/mingetty tty3
4:2345:respawn:/sbin/mingetty tty4
5:2345:respawn:/sbin/mingetty tty5
6:2345:respawn:/sbin/mingetty tty6

#   Run xdm in runlevel 5
#   xdm is now a separate service
x: 5:respawn:/usr/bin/X11/xdm –nodaemon
```

注意：开头带有符号“#”的行是注释行，而带有冒号分隔符的字段则都属于 init 配置行。