第一图书网, tushu007.com

<<UNIX/Linux应用基础教程>>

图书基本信息

书名：<<UNIX/Linux应用基础教程>>

13位ISBN编号：9787302255468

10位ISBN编号：7302255466

出版时间：2011-10

出版时间：清华大学出版社

作者：范伟，杨宏雨，张栋，王森　主编

页数：241

版权说明：本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问：http://www.tushu007.com

第一图书网, tushu007.com

<<UNIX/Linux应用基础教程>>

内容概要

《UNIX/Linux应用基础教程》系统地介绍了unix／linux操作系统的基本概念和操作，并给出了unix／linux操作系统的应用实例，以便读者能全面了解基于unix／linux环境下的应用，并对如何创建unix／linux的网络应用有所掌握。

初学者通过学习《UNIX/Linux应用基础教程》会对unix／linux系统有一个全面的认识。《UNIX/Linux应用基础教程》对unix／linux的中、高级用户也具有较大的参考价值。

第一图书网, tushu007.com

<<UNIX/Linux应用基础教程>>

书籍目录

第1章 概述
1.1 认识操作系统
1.1.1 操作系统的功能
1.1.2 普通用户看操作系统
1.1.3 程序员看操作系统
1.1.4 系统设计人员看操作系统
1.2 从unix到linux
1.3 unix／linux的特点(从用户角度看unix)
1.4 unix／linux的应用
本章小结
习题
第2章 了解应用环境
2.1 登录和注销
2.1.1 登录过程(界面)
2.1.2 退出系统
2.2 命令使用基础
2.2.1 命令的结构
2.2.2 简单命令
2.3 特殊符号的含义
2.3.1 &后台命令
2.3.2][重定向
2.3.3 管道
2.3.4 *?匹配
2.4 使用帮助
2.4.1 man的使用
2.4.2 技术手册的使用
2.4.3 网上资源
本章小结
习题
第3章 系统安装、引导与关闭
3.1 安装unix／linux的过程
3.1.1 安装前的准备工作
3.1.2 系统安装过程
3.1.3 软件安装与配置
3.2 unix／linux系统启动过程
3.2.1 启动过程及相关内容
3.2.2 改变系统引导过程
3.3 关机过程
本章小结
习题
第4章 文件系统入门
4.1 文件系统的结构
4.1.1 目录结构与文件名
4.1.2 绝对路径与相对路径
4.2 文件系统的使用

4.2.1 查看当前工作目录
4.2.2 改变当前目录
4.2.3 查看目录内容
4.2.4 查看文件类型
4.2.5 更改文件权限和存取时间
4.2.6 查看文件内容
4.2.7 创建和删除目录
4.2.8 复制、移动、删除、链接
4.2.9 统计、排序、比较
4.2.10查找文件
4.2.11文件内容检索
本章小结
习题
第5章 vi文本编辑工具
5.1 进入和退出vi
5.1.1 进入vi
5.1.2 退出vi
5.2 vi的工作方式
5.3 使用vi
5.4 vi的配置
5.5 vi命令表
本章小结
习题
第6章 shell编程
6.1 shell基础
6.1.1 shell基本概念
6.1.2 shell编程语言
6.1.3 shell脚本的生成和执行
6.2 shell语法
6.2.1 shell的变量
6.2.2 位置变量
6.2.3 shell的流向控制
6.2.4 特殊的shell命令
6.3 here文档
6.4 shell的高级使用
6.4.1 信号
6.4.2 函数
6.4.3 跟踪和调试
本章小结
习题
第7章 系统日常管理
7.1 用户管理
7.1.1 系统配置文件
7.1.2 用户登录环境的管理
7.2 文件系统的管理与维护
7.2.1 文件系统维护策略
7.2.2 文件系统的空间维护方法

第一图书网, tushu007.com

7.3 进程管理
7.3.1 与进程相关的概念
7.3.2 进程状态的检查
7.3.3 进程管理与作业调度
7.3.4 作业调度
7.4 性能调整
7.4.1 性能调整的方法
7.4.2 sar命令的使用
7.5 设备管理与维护
7.5.1 设备文件
7.5.2 设备管理命令
本章小结
习题
第8章 网络管理基础
8.1 tcp／ip入门知识
8.1.1 osi模型
8.1.2 tcp／ip协议
8.2 网络服务应用——telnet服务
8.2.1 telnet服务的安装
8.2.2 telnet的基本配置
8.2.3 启动和停止telnet服务
8.2.4 telnet客户端的使用
8.3 网络服务应用——vnc服务
8.3.1 vnc服务的概述
8.3.2 vnc服务的安装
8.3.3 vnc服务的启动配置和停止vnc服务
8.3.4 检测vnc服务
8.3.5 vnc服务的配置
8.3.6 vnc客户端的配置
8.4 网络服务应用——-ftp服务
8.4.1 ftp服务概述
8.4.2 vshpdftp服务的安装
8.4.3 pureftpd服务器的安装与配置
8.4.4 ftp客户端的配置与访问
本章小结
习题
第9章 开发环境介绍
9.1 数据处理工具
9.1.1 正则表达式
9.1.2 awk
9.1.3 sed及grep(egrepfgrep)
9.1.4 grep命令
9.1.5 peri语言
9.2 开发工具——c语言
9.2.1 cc命令
9.2.2 编译简单的程序
9.3 有多个源文件的编译

9.4 关于ar命令
9.5 关于lint命令
9.6 用make实现自动编译
9.6.1 make命令的语法和选择项
9.6.2 makefile简介
9.6.3 一般语法
9.7 sccs文件
9.8 java环境
本章小结
习题
第10章 构建数据共享服务
10.1 nfs服务
10.1.1 nfs服务概述
10.1.2 nfs服务的组件
10.1.3 nfs服务的安装与配置
10.1.4 在客户端挂载nfs文件系统
10.2 samba服务
10.2.1 sambaserver概述
10.2.2 samba服务的配置文件
10.2.3 samba服务的安全级别
10.2.4 访问samba共享资源
本章小结
习题
第11章 构建apacheweb服务
11.1 web服务的概述
11.1.1 web服务简介
11.1.2 http协议
11.1.3 流行www服务器软件
11.2 apache服务器简介
11.2.1 apache的历史
11.2.2 apache的特性
11.3 apache服务器的安装
11.3.1 apache的安装
11.3.2 apache服务的启动与停止
11.4 apache配置文件详解
11.4.1 httpd.conf文件的格式
11.4.2 apache服务的基本配置
11.5 apache服务器控制存取的方式
11.5.1 options选项
11.5.2 浏览权限的设置
11.6 apache的高级配置
11.6.1 虚拟目录
11.6.2 用户认证
11.6.3 虚拟主机
11.7 配置动态web站点
11.7.1 创建cgi动态网站
11.7.2 创建php动态网站

11.7.3 创建jsp动态网站
11.8 apacheh志管理和统计分析
11.8.1 配置访问日志
11.8.2 配置错误日志
11.8.3 日志统计分析
11.8.4 日志文件的压缩备份
本章小结
习题
第12章 系统安全基础
12.1 普通用户的安全
12.1.1 口令安全
12.1.2 文件许可权
12.1.3 目录许可
12.1.4 umask命令
12.1.5 设置用户id和同组用户id许可
12.1.6 cp、mv、1n和cpio命令
12.1.7 su和newgrp指令
12.1.8 文件加密
12.1.9 其他的安全问题
12.2 程序员的安全性考虑
12.2.1 系统子程序
12.2.2 标准c库
12.3 超级用户的安全
12.3.1 超级用户
12.3.2 安全管理
12.3.3 文件系统安全
12.3.4 find命令
12.4 unix网络安全相关文件
12.4.1 网络配置文件
12.4.2 tcp／ip守护进程
本章小结
习题

第一图书网, tushu007.com

章节摘录

版权页：插图：下面更进一步考察这些观点的有关内容。
除了“一个人一个口令”（oneperson，onepasswor-d）的防御措施外，还可以采用更加复杂的口令以便提高其安全性。
计算机用户经常用他们的姓，或者配偶或宠物的名字，或者生日来作为口令。
不幸得很，在破译口令中一台计算机能迅速地扫描一个由姓或英语中20000个最常用单词组成的阵表。
一种可供选择的口令的更加复杂的方案是有六个字符组成的口令，字符可以是数字或字母。
这样的口令是极其难以破译的。
当然，口令必须不是任何时候都用的，即在用过一定次数以后，口令必须被更改，还要根据系统安全的级别来确定识别的强度。
这里还要强调责任的重要性，确定计算机系统所涉及的人——用户、管理员和主管人员。
例如，所有的计算机使用都要由主管人的授权，以便决定管理的任务，掌握由谁和出于何种目的使用计算机。
最后，每台计算机都应该有授权用户表，此外，即使是普通的使用也应有一个公司可以访问的计算机目录，其中包括与特殊计算机、电话号码、系统管理员和有关部门的识别。
在这个计算机安全检查表中，最后要强调的一点是专用软件包的使用，通过限制对独立用户文件的一般性访问以提高安全程度。
可以通过限制特殊文件及其建立的软件访问，来保护计算机文件中的信息，直到准许其他人访问为止。
另一种限制访问的方法是使用拦截访问的硬件，要求核实口令，并且可以收回目录的授权用户成员表。
除此之外，其他的安全软件包可以跟踪非授权的可疑访问。
例如，可以在军事安全（Militarysecurity）标准下来控制计算机运行。
要补充一点，用于控制加密信息破译的计算机安全费用高得惊人。
因此，为了保持一个高水平的计算机安全环境，通常对计算机采用隔离法和设置物理进入系统的障碍。
随着计算机安全技术的发展，可以有助于减少这种隔离措施。
换句话说，可以通过建立全面的安全控制，对合法用户（1egitimateusers）提供更大的透明度。
实际上，正如人们致力于开发的计算机拥有更多的“用户友好”（userfriendly）界面——在发展或提高计算机系统安全性能时，也应该把用户的需要牢记在心头。
对通过通信线路入侵计算机的防范和检测技术与系统识别电话号码一样简单，这种技术一方面可以允许授权电话号码表的安全性检查，另一方面也能够提供非授权访问企图的跟踪记录。
这种技术目前已经应用于计算机化的商业通信系统中，通常是用于这些公司提供系统服务的线路，而且正在向全国范围的远程通信线路方面推广。

第一图书网, tushu007.com

编辑推荐

《UNIX/Linux应用基础教程》是由清华大学出版社出版的。

第一图书网, tushu007.com

<<UNIX/Linux应用基础教程>>

版权说明

本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问:http://www.tushu007.com