

信息科学与技术丛书

李洋 等编著

Linux

安全策略与实例

- ◎ Linux 系统安全
- ◎ Linux 用户和组管理安全
- ◎ SELinux 原理及使用
- ◎ Linux 网络安全



机械工业出版社
CHINA MACHINE PRESS

信息科学与技术丛书

Linux 安全策略与实例

李洋 等编著



机械工业出版社

本书对 Linux 安全策略进行了全面、深入和系统的分析。全书可分为 Linux 系统安全策略和 Linux 网络安全策略两大部分。第一部分着重介绍了 Linux 文件系统安全管理、Linux 用户和组安全管理、Linux 进程安全管理、Linux 磁盘安全管理、SELinux 安全机制等内容；第二部分对 Web 服务安全、FTP 服务安全、SMTP 服务安全、远程登录服务安全、网络流量管理安全及 IDS、防火墙等内容进行了详细介绍。书中给出大量针对 Linux 安全策略的实例，便于读者参照和迅速掌握所学内容。

本书适合中高级 Linux 用户、网络管理员和信息安全工作者，并可作为高等院校计算机和信息安全专业师生的参考用书。

图书在版编目 (CIP) 数据

Linux 安全策略与实例 / 李洋等编著. —北京: 机械工业出版社, 2009.9

(信息科学与技术丛书)

ISBN 978-7-111-28378-2

I. L… II. 李… III. Linux 操作系统—安全技术 IV. TP316.89
TP393.08

中国版本图书馆 CIP 数据核字 (2009) 第 171931 号

机械工业出版社 (北京市百万庄大街 22 号 邮政编码 100037)

策划编辑: 车 忱

责任编辑: 车 忱

责任印制: 乔 宇

北京机工印刷厂印刷 (兴文装订厂装订)

2009 年 11 月·第 1 版第 1 次印刷

184mm × 260mm · 26.5 印张 · 655 千字

0 001—3 500 册

标准书号: ISBN 978-7-111-28378-2

定价: 48.00 元

凡购本书, 如有缺页、倒页、脱页, 由本社发行部调换

电话服务

网络服务

社服务中心: (010) 88361066

门户网: <http://www.cmpbook.com>

销售一部: (010) 68326294

教材网: <http://www.cmpedu.com>

销售二部: (010) 88379649

读者服务部: (010) 68993821

封面无防伪标均为盗版

出版说明

随着信息科学与技术的迅速发展，人类每时每刻都会面对层出不穷的新技术和新概念。毫无疑问，在节奏越来越快的工作和生活中，人们需要通过阅读和学习大量信息丰富、具备实践指导意义的图书来获取新知识和新技能，从而不断提高自身素质，紧跟信息化时代发展的步伐。

众所周知，在计算机硬件方面，高性价比的解决方案和新型技术的应用一直备受青睐；在软件技术方面，随着计算机软件的规模和复杂性与日俱增，软件技术不断地受到挑战，人们一直在为寻求更先进的软件技术而奋斗不止。目前，计算机在社会生活中日益普及，随着Internet延伸到人类世界的方方面面，掌握计算机网络技术和理论已成为大众的文化需求。由于信息科学与技术 在电工、电子、通信、工业控制、智能建筑、工业产品设计与制造等专业领域中已经得到充分、广泛的应用。所以这些专业领域中的研究人员和工程技术人员越来越迫切需要汲取自身领域信息化所带来的新理念和新方法。

针对人们了解和掌握新知识、新技能的热切期待，以及由此促成的人们对语言简洁、内容充实、融合实践经验的图书迫切需要的现状，机械工业出版社适时推出了“信息科学与技术丛书”。这套丛书涉及计算机软件、硬件、网络 and 工程应用等内容，注重理论与实践的结合，内容实用、层次分明、语言流畅，是信息科学与技术领域专业人员不可或缺的参考书。

目前，信息科学与技术的发展可谓一日千里，机械工业出版社欢迎从事信息技术方面工作的科研人员、工程技术人员积极参与我们的工作，为推进我国的信息化建设作出贡献。

机械工业出版社

前 言

Linux 是一个优秀的、日益成熟的操作系统，它支持多用户、多进程及多线程，实时性好，功能强大而稳定。同时，它又具有良好的兼容性和可移植性。在网络技术日益发展的今天，凭借其在安全性、稳定性等方面的巨大优势，正受到越来越多的用户的青睐，一些大型的网络及网站服务器，都建立在 Linux 平台之上。然而，随着互联网的发展以及 Linux 应用的普及，Linux 系统的安全问题也日益突出。权限滥用、用户误操作、文件系统安全、垃圾邮件、病毒、木马、拒绝服务攻击等问题正威胁着 Linux。解决 Linux 系统的安全问题已成为 Linux 用户和网络管理员的当务之急，也是当前网络信息安全领域研究的热点和难点。

本书从 Linux 系统安全和 Linux 网络服务安全两个方面入手，系统、全面、深入地向读者介绍了 Linux 系统安全和网络服务安全的原理、技术及应用方法，并通过具体的实例来剖析 Linux 安全的实质，以及如何有效运用相关的技术和软件工具来保障 Linux 的系统安全和网络服务安全。

本书是一本全面介绍 Linux 安全技术的专著，具有很强的实用性和可操作性，不仅适合中高级 Linux 用户、网络管理员、网络工程师、网络信息安全工作者和研究者，也可作为高等院校计算机软件和信息安全专业师生的参考用书。并且，本书内容不局限于任何一个 Linux 发行套件，对各 Linux 套件的用户都有很强的实用性和指导作用。

本书的作者具有多年从事 Linux 安全研究及开发的工作经验，本书是他们多年来学习、工作和从事重大项目开发经验的结晶。本书由李洋主持编写，参与编写的作者还有王俊丽、邓柱中、姚秋林、舒承椿、丁凡、汪浩、王曦爽、张磊、张鹏。全书由李洋统稿并审校。

由于水平和时间所限，不妥或错误之处在所难免，敬请广大读者批评指正。

目 录

出版说明

前言

第 1 章 Linux 系统简介	1	2.5.3 加固 GRUB	19
1.1 Linux 的发展历史	1	第 3 章 Linux 文件系统安全	20
1.2 Linux 与 GNU、GPL 以及 POSIX 的关系	2	3.1 Linux 文件系统基本原理和 概念	20
1.2.1 GNU	2	3.1.1 Linux 常用的文件系统	20
1.2.2 GPL	2	3.1.2 Linux 文件	23
1.2.3 POSIX	3	3.1.3 Linux 目录	24
1.3 Linux 的特性	3	3.1.4 Linux 目录结构	26
1.4 Linux 的应用领域	4	3.2 文件/目录访问权限管理	27
1.5 Linux 的内核及发行版本	5	3.2.1 文件/目录访问权限	27
1.6 常见的 Linux 发行版本	5	3.2.2 使用 chmod 改变文件/目录的 访问权限	28
1.6.1 Red Hat Linux	5	3.2.3 使用命令 chown 更改文件/ 目录的所有权	30
1.6.2 Fedora Core/Fedora	6	3.2.4 使用 setuid/setgid 改变执行 权限	30
1.6.3 Debian	6	3.3 使用文件系统检查工具保证 文件系统安全	32
1.6.4 Ubuntu	7	3.3.1 Tripwire 工具简介	32
1.6.5 SuSE Linux	7	3.3.2 Tripwire 工作原理	32
1.7 Linux 的主要组成部分	7	3.3.3 安装 Tripwire	38
1.7.1 内核	8	3.3.4 配置和使用 Tripwire	38
1.7.2 Shell	8	3.3.5 使用 Tripwire 进行文件监控	42
1.7.3 文件结构	8	3.3.6 使用 Tripwire 的技巧	43
1.7.4 实用工具	9	第 4 章 Linux 用户和组管理安全	44
1.8 Linux 最新内核版本的新 特性	10	4.1 Linux 下的用户和组管理安全 概述	44
第 2 章 Linux 系统启动安全	11	4.2 几个关键的用户和组文件	44
2.1 引导装载程序原理	11	4.2.1 用户账号文件——passwd	44
2.2 Linux 系统运行级别	12	4.2.2 用户影子文件——shadow	46
2.3 LILO 引导装载程序	13	4.2.3 用户组账号文件——group	48
2.4 GRUB 引导装载程序	15	4.2.4 组账号文件——gshadow	49
2.5 Linux 系统启动安全保障 技术	17	4.2.5 Linux 用户口令加密函数	50
2.5.1 卸载 LILO 防止入侵	17		
2.5.2 为 LILO 的单用户模式添加 口令	18		

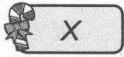


4.2.6 使用 pwck 和 grpck 命令验证 用户和组文件	50	5.3.1 使用 PROC 查看进程	77
4.3 安全管理用户和组	53	5.3.2 内核模块介绍	79
4.3.1 使用 useradd 命令添加用户	53	5.3.3 PROC 常用的调用接口	81
4.3.2 使用 usermod 命令修改 用户信息	55	第 6 章 Linux 中的日志管理	85
4.3.3 使用 userdel 命令删除用户	55	6.1 Linux 日志管理简介	85
4.3.4 使用 groupadd 命令创建 用户组	55	6.2 Linux 基本日志管理机制	86
4.3.5 使用 groupmod 命令修改用户 组属性	56	6.2.1 who 命令	86
4.3.6 使用 groupdel 命令删除 用户组	57	6.2.2 users 命令	87
4.4 用户口令的安全性保证	57	6.2.3 last 命令	87
4.4.1 安全用户口令的设定原则	57	6.2.4 ac 命令	87
4.4.2 使用密码分析工具验证	58	6.2.5 lastlog 命令	88
4.5 用户和组文件的安全性保证	60	6.3 使用 syslog 设备	88
4.6 使用嵌入式认证模块—— PAM	61	6.3.1 syslog 简介	88
4.6.1 PAM 的起源	61	6.3.2 syslog 配置文件	88
4.6.2 Linux-PAM 的分层体系结构	62	6.3.3 syslog 进程	90
4.6.3 Linux-PAM 的应用	62	6.3.4 实际应用中的 syslog 调用 接口	91
第 5 章 Linux 进程管理安全	67	6.4 Linux 日志使用注意事项	93
5.1 Linux 中的进程原理	67	6.5 Linux 日志输出查看方式	93
5.1.1 进程类型	67	6.5.1 dmesg	93
5.1.2 进程的状态	67	6.5.2 tail	95
5.1.3 进程的主要工作模式	68	6.5.3 more 和 less	95
5.1.4 Linux 下的守护进程	69	6.5.4 其他方式	97
5.1.5 Linux 系统关键进程介绍	69	第 7 章 Linux 磁盘安全管理	98
5.2 Linux 进程管理	71	7.1 安全管理磁盘	98
5.2.1 使用 ps 命令查看进程状态	71	7.1.1 磁盘存储设备的命名	98
5.2.2 使用 top 命令查看进程状态	73	7.1.2 管理磁盘空间	99
5.2.3 使用 kill 命令终止进程	74	7.2 硬件状态监控	106
5.2.4 使用 sleep 命令暂停进程	75	7.2.1 获取和安装 dmidecode 工具	106
5.2.5 使用 nice 改变进程执行 优先级	76	7.2.2 使用硬件状态监控工具	106
5.2.6 使用 renice 修改优先级	76	7.3 安全管理磁盘阵列	108
5.2.7 使用 pgrep 命令查找进程	76	7.3.1 磁盘阵列原理	108
5.3 Linux 进程文件系统 PROC	77	7.3.2 磁盘阵列的分类	108
		7.3.3 Linux 下使用磁盘阵列	110
		7.4 Linux 下的备份机制	113
		7.4.1 常用备份命令	113
		7.4.2 常用开源备份软件	115
		7.4.3 备份策略	117
		第 8 章 SELinux 原理	121

8.1 Linux 操作系统安全性分析	121	9.5.2 端口分类	169
8.1.1 Linux 操作系统安全级别	121	9.5.3 常用端口介绍	169
8.1.2 Linux 操作系统主要安全机制	123	9.5.4 网络端口扫描工具 nmap	170
8.2 操作系统安全原理	124	9.6 Linux 网络安全管理命令	174
8.2.1 BLP 安全模型	124	9.6.1 ifconfig: 网络配置命令	174
8.2.2 RBAC 模型	125	9.6.2 ifup/ifdown: 网卡激活/停用命令	175
8.2.3 多级别安全机制	126	9.6.3 hostname: 主机名更改命令	175
8.2.4 常见的操作系统加固技术	127	9.6.4 route: 路由配置命令	175
8.3 SELinux: Linux 安全增强机制	128	9.6.5 ping: 网络连通测试命令	176
8.3.1 SELinux 的来源	128	9.6.6 Traceroute: 网络路径跟踪命令	176
8.3.2 SELinux 机制介绍	128	9.6.7 netstat: 网络状态查询命令	176
8.3.3 SELinux 与传统 Linux 的区别	129	9.6.8 arp 命令	177
8.3.4 SELinux 中的上下文	130	9.6.9 arpswatch: 监听 ARP 记录命令	177
8.3.5 SELinux 中的目标策略	134	9.7 使用 xinetd 管理 Linux 网络服务	177
8.3.6 SELinux 配置文件和策略目录介绍	140	9.7.1 xinetd 原理	177
8.3.7 使用 SELinux 的准备	142	9.7.2 /etc/xinetd.conf 文件	178
8.3.8 SELinux 中布尔变量的使用	145	9.7.3 xinetd 服务配置文件	179
8.4 国内外相关安全标准概述	148	9.7.4 通过文件配置使用 xinetd	180
第 9 章 Linux 网络原理	151	9.7.5 通过图形用户界面配置使用 xinetd	181
9.1 计算机网络体系结构和参考模型	151	第 10 章 Linux 网络安全威胁	182
9.1.1 计算机网络简介及模型	151	10.1 网络安全简介	182
9.1.2 OSI 七层模型	152	10.1.1 网络信息安全的要素	184
9.1.3 TCP/IP 四层模型	154	10.1.2 网络中存在的威胁	185
9.2 TCP/IP 协议栈原理	155	10.1.3 网络信息安全领域的研究重点	185
9.2.1 IP	156	10.2 Linux 网络面临的常见威胁	187
9.2.2 TCP	159	10.2.1 端口扫描	187
9.2.3 UDP	161	10.2.2 主机扫描	188
9.3 IPv6	162	10.2.3 操作系统“指纹”扫描	189
9.4 重要相关协议介绍	164	10.2.4 木马	189
9.4.1 ICMP	164	10.2.5 DoS 攻击和 DDoS 攻击	192
9.4.2 ARP/RARP	165		
9.4.3 SNMP	167		
9.5 Linux 重要网络应用端口	168		
9.5.1 端口技术原理	168		

10.2.6	Linux 下的病毒	196	流量	226	
10.2.7	IP 地址欺骗	198	第 12 章 构建安全的 Web 服务	228	
10.2.8	ARP 欺骗	198	12.1 Web 服务器简介	228	
10.2.9	网络钓鱼	198	12.1.1 HTTP 基本原理	228	
10.2.10	僵尸网络	201	12.1.2 Apache 服务器简介	229	
10.2.11	跨站脚本攻击	202	12.2 Apache 服务器面临的网络 威胁	231	
10.2.12	零日攻击	202	12.3 安装 Apache 的最新版本	231	
第 11 章 构建安全的 DNS 服务	204	12.3.1 获取 Apache 安装包	231	12.3.2 使用 httpd-2.2.11.tar.gz 软件包安装 Apache	232
11.1 DNS 服务安全简介	204	12.3.3 使用 httpd-2.2.11.tar.bz2 软件包安装 Apache	232	12.4 安全配置 Apache 服务器	233
11.1.1 DNS 服务简介	204	12.4.1 httpd.conf 配置文件格式	233	12.4.2 安全设定 httpd.conf 文件中的 全局配置选项	234
11.1.2 DNS 服务存在的问题和 面临的威胁	207	12.5 使用特定的用户运行 Apache 服务器	237	12.6 配置隐藏 Apache 服务器的 版本号	238
11.2 安装 DNS 的最新版本	208	12.7 实现访问控制	240	12.7.1 访问控制常用配置指令	240
11.3 正确配置 DNS 相关文件	209	12.7.2 使用 .htaccess 文件进行访问 控制	241	12.8 使用认证和授权	244
11.3.1 几个重要的 DNS 服务器 配置文件类型	209	12.8.1 认证和授权指令	244	12.8.2 管理认证口令文件和认证组 文件	245
11.3.2 named.conf 主配置文件	210	12.8.3 认证和授权使用实例	245	12.9 设置虚拟目录和目录权限	247
11.3.3 区文件	212	12.10 使用 Apache 中的安全 模块	249	12.10.1 Apache 服务器中安全 相关模块	249
11.3.4 DNS 服务器配置实例	213	12.10.2 开启安全模块	250	12.11 使用 SSL 保证安全	251
11.3.5 使用 Dlint 工具进行 DNS 配置文件检查	215	12.11.1 SSL 简介	251	12.11.2 Apache 中运用 SSL 的	
11.3.6 使用命令检验 DNS 功能	216				
11.4 配置辅助域名服务器进行 冗余备份	219				
11.5 配置高速缓存服务器缓解 DNS 访问压力	220				
11.6 配置 DNS 负载均衡	222				
11.7 安全配置和使用 DNS	222				
11.7.1 限制名字服务器递归查询 功能	222				
11.7.2 限制区传送	222				
11.7.3 限制查询	223				
11.7.4 分离 DNS	223				
11.7.5 隐藏 BIND 的版本信息	224				
11.7.6 使用非 root 权限运行 BIND	224				
11.7.7 删除 DNS 上不必要的其他 服务	225				
11.7.8 合理配置 DNS 的查询方式	225				
11.8 使用 dnstop 监控 DNS					

基本原理	252	端口工作	284
12.11.3 安装和启动 SSL	254	13.7.5 配置虚拟 FTP 服务器	285
12.12 设置虚拟主机	257	13.7.6 使用 Linux-PAM 控制 vsftpd 用户的登录	287
12.12.1 设置 IP 型虚拟主机	257	13.8 安全配置 Wu-ftp	288
12.12.2 设置名字型虚拟主机	260	13.8.1 配置 ftpaccess 文件	288
12.13 Apache 日志记录	261	13.8.2 配置 ftphosts 文件	294
第 13 章 构建安全的 FTP 服务	265	13.8.3 配置/etc/ftpservers 文件	295
13.1 FTP 简介	265	13.8.4 配置 ftpusers 文件	295
13.1.1 FTP 协议简介	265	第 14 章 构建安全的电子邮件 服务	297
13.1.2 FTP 服务器连接过程及模式	265	14.1 电子邮件系统原理	297
13.1.3 FTP 文件类型	266	14.1.1 邮件传递代理	297
13.1.4 FTP 文件结构	267	14.1.2 邮件存储和获取代理	297
13.1.5 FTP 传输模式	267	14.1.3 邮件客户代理	298
13.1.6 FTP 常用命令	267	14.1.4 电子邮件系统的常用协议	298
13.1.7 FTP 典型消息	268	14.2 SMTP 介绍	299
13.2 FTP 服务面临的安全威胁	268	14.2.1 SMTP 的模型	299
13.3 安装最新版本的 vsftpd 服务器	269	14.2.2 SMTP 的基本命令	300
13.4 安全配置 vsftpd.conf 文件	270	14.2.3 电子邮件的结构	301
13.4.1 设定独立模式的相关配置	270	14.2.4 Open Relay 的原理	303
13.4.2 设定登录的相关配置	271	14.2.5 电子邮件系统与 DNS	304
13.4.3 设定工作目录和 chroot “监牢”的相关配置	272	14.3 电子邮件系统面临的安全 威胁	304
13.4.4 设定文件下载与上传的 相关配置	273	14.4 安全使用 sendmail Server	305
13.4.5 设定消息的相关配置	274	14.4.1 安装最新版本的 sendmail 服务器	305
13.4.6 设定显示的相关配置	274	14.4.2 安全设置 sendmail.cf 文件 中的选项	305
13.4.7 设定日志的相关配置	275	14.4.3 使用 sendmail.mc 文件	308
13.4.8 设定连接参数	275	14.4.4 使用 access 数据库	309
13.4.9 其他设定	276	14.4.5 配置带 SMTP 认证的 sendmail 服务器	310
13.5 安全配置 vsftpd.ftpusers 文件	276	14.5 安全使用 Postfix 电子邮件 服务器	311
13.6 安全配置 vsftpd.user_list 文件	277	14.5.1 安全配置 Postfix 邮件 服务器	311
13.7 安全使用 vsftpd 服务器	278	14.5.2 Postfix 使用 SMTP 安全 认证	313
13.7.1 匿名用户使用 vsftpd 服务器	278		
13.7.2 本地用户使用 vsftpd 服务器	279		
13.7.3 虚拟用户使用 vsftpd 服务器	282		
13.7.4 配置 vsftpd 服务器在非标准			



14.6	垃圾邮件防范技术	314	16.1	IDS 简介	340
14.6.1	常用技术	315	16.2	IDS 分类	341
14.6.2	设置 sendmail 防范垃圾邮件	316	16.3	Snort 介绍	343
14.6.3	安全配置 Postfix 防范垃圾邮件	317	16.4	安装 Snort	344
14.6.4	客户端配置垃圾邮件防护功能	317	16.5	Snort 的工作模式	344
第 15 章 使用防火墙保证 Linux 网络安全			16.6 使用 Snort		
15.1 防火墙简介			16.6.1 命令简介		
15.2 防火墙的主要分类			16.6.2 查看 ICMP 数据报文		
15.2.1 按防火墙的软、硬件形式划分			16.6.3 配置 Snort 的输出方式		
15.2.2 按防火墙的发展技术划分			16.6.4 配置 Snort 规则		
15.2.3 按防火墙的结构划分			16.7 编写 Snort 规则		
15.2.4 按防火墙的应用部署位置划分			16.7.1 规则动作		
15.3 防火墙技术及其特点			16.7.2 协议		
15.3.1 数据包过滤防火墙技术			16.7.3 IP 地址		
15.3.2 应用层网关防火墙技术			16.7.4 端口号		
15.3.3 代理防火墙技术			16.7.5 方向操作符		
15.4 新一代防火墙的主要技术特点			16.7.6 activate/dynamic 规则对		
15.4.1 传统防火墙的发展历史			16.7.7 一些重要的指令		
15.4.2 防火墙体系结构			16.7.8 规则选项		
15.4.3 新一代分布式防火墙概述			16.7.9 一些 Snort 规则的应用举例		
15.4.4 新一代嵌入式防火墙技术			16.8 Linux 内核 IDS: LIDS		
15.4.5 新一代智能防火墙技术			16.8.1 LIDS 简介		
15.4.6 防火墙技术的发展趋势			16.8.2 LIDS 安装		
15.5 使用 Netfilter/iptables 防火墙框架			16.8.3 配置和使用 LIDS		
15.5.1 Netfilter/iptables 框架简介			第 17 章 构建安全的 Linux 远程登录		
15.5.2 安装 Netfilter/iptables 系统			17.1 SSH 服务简介		
15.5.3 iptables 工作原理			17.2 安装最新版本的 OpenSSH		
15.5.4 使用 iptable 的过滤规则			17.3 安全配置 openSSH		
15.5.5 使用 iptables 保障网络服务安全			17.4 SSH 的密钥管理		
第 16 章 使用 IDS 保证 Linux 网络安全			17.5 使用 scp 命令远程复制文件		
16.1 IDS 简介			17.6 使用 SSH 设置“加密通道”		
16.2 IDS 分类			17.7 配置 SSH 的客户端		
16.3 Snort 介绍			17.8 配置 SSH 自动登录		
16.4 安装 Snort			17.9 使用 Xmanager 3.0 实现 Linux 远程登录管理		
16.5 Snort 的工作模式					
16.6 使用 Snort					
16.6.1 命令简介					
16.6.2 查看 ICMP 数据报文					
16.6.3 配置 Snort 的输出方式					
16.6.4 配置 Snort 规则					
16.7 编写 Snort 规则					
16.7.1 规则动作					
16.7.2 协议					
16.7.3 IP 地址					
16.7.4 端口号					
16.7.5 方向操作符					
16.7.6 activate/dynamic 规则对					
16.7.7 一些重要的指令					
16.7.8 规则选项					
16.7.9 一些 Snort 规则的应用举例					
16.8 Linux 内核 IDS: LIDS					
16.8.1 LIDS 简介					
16.8.2 LIDS 安装					
16.8.3 配置和使用 LIDS					



第 18 章 Linux 网络流量安全管理 ...	386
18.1 网络流量管理简介	386
18.1.1 流量识别	386
18.1.2 流量统计分析	387
18.1.3 流量限制	388
18.1.4 其他方面	388
18.2 需要管理的常见网络流量 ...	388
18.3 网络流量捕捉：图形化	
工具 Wireshark	389
18.3.1 Wireshark 简介	389
18.3.2 层次化的数据包协议分析	
方法	390
18.3.3 基于插件技术的协议分析器 ...	391
18.3.4 安装 Wireshark	391
18.3.5 使用 Wireshark	392
18.4 网络流量捕捉：命令行工具	
tcpdump	396
18.4.1 tcpdump 简介	396
18.4.2 安装 tcpdump	396
18.4.3 使用 tcpdump	397
18.5 网络流量分析——Ntop	400
18.5.1 Ntop 介绍	400
18.5.2 安装 Ntop	401
18.5.3 使用 Ntop	402
18.6 网络流量限制——TC 技术 ...	405
18.6.1 TC 技术原理	405
18.6.2 使用 Linux TC 进行流量	
控制实例	405
18.7 网络流量管理的策略	409
18.7.1 管理目标	409
18.7.2 具体策略	410

第 1 章 Linux 系统简介

Linux 是一个日益成熟的操作系统，现在已经拥有大量的用户。由于其安全、高效、适合构建安全的网络应用，已被越来越多的人了解和使用。Linux 是芬兰的 Linus Torvalds 开发的，任何人都可以自由地复制、修改、套装发行、销售，但是不可以在发行时加入任何限制，而且所有源代码必须是公开的，以保证任何人都可以无偿取得所有可执行文件及其源代码。本章将着重介绍 Linux 的发展历史、特性、主要应用领域、主要发行版本、Linux 内核基本原理等。

1.1 Linux 的发展历史

要讲 Linux 的发展历史，不能不提到 UNIX 和 MINIX。UNIX 的早期版本源代码可以免费获得，但是当 AT&T 发布 UNIX 7 时，开始认识到 UNIX 的商业价值，于是发布的版本 7 许可证禁止在大学课程中研究其源代码，以免其商业利益受到损害。许多学校为了遵守该规定，就在课程中略去 UNIX 的内容而只讲操作系统理论。

只讲理论使学生对实际的操作系统产生了片面的认识。为了扭转这种局面，坦尼鲍姆决定编写一个在用户看来与 UNIX 完全兼容，然而内核全新的操作系统——MINIX。坦尼鲍姆希望读者通过 MINIX 可以剖析一个操作系统，研究其内部如何运作。MINIX 的名称源于“Mini-UNIX”。MINIX 一直恪守“Small is beautiful”（小即是美）的原则，其最早的版本甚至不需要硬盘就可以运行，这使得许多学生有能力负担其硬件的要求。随着其功能和规模的增长，大多数人希望在 MINIX 中加入一些新特性以使之更大、更有用，但 MINIX 的作者一直坚持不增加新特性，使 MINIX 保持短小精悍的特点，便于学生理解。此后，芬兰学生 Linus Torvalds 决定编写一个类似 MINIX 的系统，其特征繁多且面向实用而非教学。他编写的这个操作系统就是 Linux。

1990 年，Linus Torvalds 用汇编语言写了一个在 80386 保护模式下处理多任务切换的程序，后来从 MINIX 中得到灵感，他开始写了一些硬件的设备驱动程序、一个小的文件系统，这样 0.0.1 版本的 Linux 就诞生了，但是它必须在有 MINIX 的计算机上编译以后才能运行。后来 Linus 决定彻底抛弃 MINIX，编写一个完全独立的操作系统。1991 年 10 月 5 日 Linus 发布了 Linux 0.0.2 版本。这个版本已经可以运行 bash（一种用户与操作系统内核通信的命令解释软件）和 GCC（GNU C 编译器）了。

Linus 从一开始就决定免费发布 Linux。他把源代码发布在网上，随即就引起爱好者的注意，他们通过互联网也加入了 Linux 的内核开发工作，一大批高水平程序员的加入，使得 Linux 迅猛发展。到 1993 年底，Linux 1.0 终于诞生。Linux 1.0 已经是一个功能完备的操作系统了，其内核写得紧凑高效，可以充分发挥硬件的性能，在 4MB 内存的 80386 机器上也表现



得非常好。

Linux 从 1.3 版本之后开始向其他硬件平台上移植。目前 Linux 能将硬件的性能充分发挥出来，可以囊括从低端到高端的所有应用。现在 Linux 可以在 Intel、DEC 的 Alpha、Motorola 的 M68k、Sun Sparc、PowerPC、MIPS 等处理器上运行。

Linux 虽然加入 GNU 并遵循 GPL，但是并不排斥商家的参与，不排斥在 Linux 上开发商业软件，故而使 Linux 开始了新的飞跃，出现了很多的 Linux 发行版，如 Slackware、Red Hat、Suse、TurboLinux、OpenLinux 等，而且现还在增加。许多大公司还在 Linux 上开发商业软件或把其他 UNIX 平台的软件移植到 Linux 上来。如今很多 IT 界的大腕如 IBM、Intel、Oracle、Infomix、Sysbase、Corel、CA、Novell 等都宣布支持 Linux。商家的加盟弥补了纯自由软件的不足和发展障碍，使 Linux 得以迅速普及。

1.2 Linux 与 GNU、GPL 以及 POSIX 的关系

1.2.1 GNU

GNU 是 GNU's Not UNIX（网站为 www.gnu.org）的递归缩写，是由自由软件大师 Richard Stallman 在 1983 年 9 月 27 日公开发起的。它的目标是创建一套完全自由的操作系统。

为保证 GNU 软件可以自由地使用、复制、修改和发布，所有 GNU 软件必须遵循 GPL 协议（见 1.2.2 节）。

1985 年 Richard Stallman 又创立了自由软件基金会（Free Software Foundation）来为 GNU 计划提供技术、法律以及财政支持。尽管 GNU 计划大部分时候是由个人自愿无偿贡献的，但 FSF 有时还是会出资聘请程序员编写软件。当 GNU 计划开始逐渐获得成功时，一些商业公司开始介入开发和技术支持。其中最著名的就是之后被 Red Hat 兼并的 Cygnus Solutions。

到了 1990 年，GNU 计划已经开发出的软件包括了一个功能强大的文字编辑器 EMACS，C 语言编译器 GCC，以及大部分 UNIX 系统的程序库和工具。

Linus Torvalds 编写出了与 UNIX 兼容的 Linux 操作系统内核并在 GPL 条款下发布后，许多程序员参与了开发与修改。1992 年 Linux 与其他 GNU 软件结合，完全自由的操作系统正式诞生。因此，严格地说，Linux 应该称为 GNU/Linux。许多 UNIX 系统上也安装了 GNU 软件，因为某些 GNU 软件的质量比之前 UNIX 的软件还要好。GNU 工具还被广泛地移植到 Windows 和 Mac OS 上。

1.2.2 GPL

GNU 通用公共许可证（GNU General Public License，简称为 GPL），是由自由软件基金会发行的一种计算机软件许可证（网站为 <http://www.gnu.org/licenses/gpl.html>），最初由 Richard Stallman 为 GNU 计划撰写。目前大多数的 GNU 程序和超过半数的自由软件使用此许可证。此许可证最新版本为“版本 3”，于 2007 年 6 月发布。

GPL 不会授予许可证接受人无限的权利。再发行权的授予需要许可证接受人开放软件的

源代码及所有修改，且复制件、修改版本都必须以 GPL 为许可证。这些要求就是“copyleft”，它的基础就是作品在法律上版权所有。由于版权所有，许可证接受人就无权进行修改和再发行，除非它有一个 copyleft 条款。如果某人发行软件时违反了 GPL（比如说，在享受了 GPL 带来的权利的前提下，而未履行开放源代码的义务），他就有可能被原作者起诉。copyleft 利用版权法来达到与其相反的目的：copyleft 给人不可剥夺的权利，而不是版权法所规定的诸多限制。这也是 GPL 被称作“被黑的版权法”的原因。许多 GPL 软件发行者都把源代码与可执行程序捆绑起来。另一方式就是以物理介质（比如 CD）为载体提供源代码。在实践中，许多 GPL 软件都是在互联网上发行的，源代码也有许多可通过 FTP 方式得到。copyleft 只在程序再发行时发生效力。对软件的修改可以不公开或开放源代码，只要不发行即可。值得注意的是，copyleft 只对软件有效力，而对软件的输出并无效力（除非输出的是软件本身）。

GPL 设计为一种许可证，而不是合同。在英美法系国家，许可证与合同有法律上的明确区别：合同由合同法保障效力，而 GPL 作为一种许可证由版权法保障效力。不过在许多采用大陆法系的国家并无此种区别。GPL 的原理很简单：在版权法下，用户不遵守 GPL 的条款和条件就没有相应权利。而作品在没有 GPL 的情况下，版权法作为默认条款发生效力，而不是作品进入公有领域。

1.2.3 POSIX

POSIX 表示可移植操作系统接口（Portable Operating System Interface, POSIX）。电气和电子工程师协会（Institute of Electrical and Electronics Engineers, IEEE）最初开发 POSIX 标准，是为了提高 UNIX 环境下应用程序的可移植性。然而，POSIX 并不局限于 UNIX。许多其他的操作系统，例如 DEC OpenVMS 和 Microsoft Windows NT，都支持 POSIX 标准，尤其是 IEEE Std. 1003.1-1990（1995 年修订）或 POSIX.1。POSIX.1 提供了源代码级别的 C 语言应用编程接口（API）给操作系统的服务程序，例如读写文件。POSIX.1 已经被国际标准化组织（International Standards Organization, ISO）接受，命名为 ISO/IEC 9945-1:1990 标准。

POSIX 现在已经发展成为一个非常庞大的标准族，某些部分正处在开发过程中。而 Linux 的目标是保持和 POSIX 的兼容。

1.3 Linux 的特性

Linux 从一个由个人开发的操作系统雏形经过短短十多年时间就发展成为今天举足轻重的操作系统，与 Windows、UNIX 一起形成操作系统领域三足鼎立的局势，必定有其原因。Linux 自身的特点就是其获得成功的原因。Linux 具有以下特性：

(1) 公开源码：作为程序员，通过阅读 Linux 内核和 Linux 下其他程序的源代码，可以学到很多编程经验和其他知识；作为最终用户，使用 Linux 避免了使用盗版 Windows 的尴尬，也避免了使用正版 Windows 的庞大费用。一个比较著名的例子是，墨西哥政府采用 Linux 替代 Windows，大约节省了 1.24 亿美元。

(2) 系统稳定：Linux 采用了 UNIX 的设计体系，汲取了 UNIX 系统二十多年的发展经

验。Linux 操作系统体现了现代操作系统的设计理念和最经得住时间考验的设计方案。在服务器操作系统市场上，Linux 已经超过 Windows 成为服务器首选操作系统。

(3) 性能突出：德国 C'T 最近公布了最新的 Windows 和 Linux 之间的测试结果。测试是由 Jurgen Schmidt 组织的，结果表明，在各种应用情况下，尤其是在网络应用环境中，Linux 的总体性能更好。

(4) 设备独立性：设备独立性是指操作系统把所有外围设备统一当作成文件来看待，只要安装它们的驱动程序，任何用户都可以像使用文件一样，操纵、使用这些设备，而不必知道它们的具体存在形式。Linux 是具有设备独立性的操作系统，它的内核具有高度适应能力，随着更多的程序员加入 Linux 编程，会有更多硬件设备加入到各种 Linux 内核和发行版本中。另外，由于用户可以免费得到 Linux 的内核源代码，因此，用户可以修改内核源代码，以便适应新增加的外围设备。

(5) 安全性强：各种病毒的频繁出现使得微软几乎每隔几天就要为 Windows 公布补丁。针对 Linux 的病毒则比较少，而且 Linux 的开源代码的开发方式使得各种漏洞都能够在 Linux 上得到及早发现和弥补。

(6) 跨平台：Windows 只能在 Intel 构架下运行，但是 Linux 除了可以运行于 Intel 平台外，还可以运行于 Motorola 公司的 68K 系列 CPU，IBM、Apple、Motorola 公司的 PowerPC CPU，Compaq 和 Digital 公司的 Alpha CPU、MIPS 芯片，Sun 公司的 SPARC 和 UltraSparc CPU，Intel 公司的 StrongARM CPU 等处理器系统。

(7) 完全兼容 UNIX：Linux 和现今的 UNIX、System V、BSD 等三大主流的 UNIX 系统几乎完全兼容，在 UNIX 下可以运行的程序，完全可以移植到 Linux 下运行。

(8) 良好的可移植性：Linux 是一种可移植的操作系统，能够在从微型计算机到大型计算机的任何环境中 and 任何平台上运行。可移植性为运行 Linux 的不同计算机平台与其他任何机器进行准确而有效的通信提供了手段，不需要另外增加特殊的和昂贵的通信接口。

(9) 强大的网络服务：Linux 诞生于因特网，它具有 UNIX 的特性，保证了它支持所有标准因特网协议，而且 Linux 内置了 TCP/IP 协议。事实上，Linux 是第一个支持 IPv6 的操作系统。

1.4 Linux 的应用领域

Linux 从诞生到现在，已经在许多领域得到了广泛应用，显示了强大的生命力，其应用范围正日益扩大。下面列举其主要应用领域：

- 教育领域：设计先进和开源代码这两大特性使 Linux 成为了操作系统课程的好范例。
- 网络服务器领域：稳定、健壮、对系统要求低、网络功能强使 Linux 成为现在 Internet 服务器操作系统的首选，现已达到了服务器操作系统市场 25% 的占有率。
- 企业 Intranet：利用 Linux 系统可以使企业用低廉的投入架设 E-mail 服务器、WWW 服务器、代理服务器、透明网关、路由器。
- 视频制作领域：著名的影片《泰坦尼克号》就是由 200 多台装有 Linux 系统的机器协作完成其特技效果的。

1.5 Linux 的内核及发行版本

严格地说, Linux 是在 GPL (GNU General Public License) 版权协议下发行的操作系统内核, 其版权属于 Linus Torvalds。通常所说的 Linux 是指包含 kernel (内核)、utilities (系统工具程序) 以及 applications (应用软件) 的一个完整的操作系统, 它实际上是 Linux 的发行版本, 是某些公司或组织把 Linux 内核、源代码以及相关的应用程序组织在一起发行的。国际上比较著名的 Linux 发行版本有 Red Hat、Slackware、Debian、Fedora、Ubuntu 等。国内也有不少 Linux 的发行版本, 其中最为著名的首推北京中科红旗软件技术有限公司发布的红旗 Linux。

Linux 是 UNIX 的“克隆”, 在源代码级上兼容绝大部分的 UNIX 标准 (如 IEEE POSIX、System V、BSD 等), 并且符合 POSIX 规范。例如对于 System V 来说, 把其上的程序源代码拿到 Linux 下重新编译后就可以运行, 而对于 BSD UNIX 来说, 它的可执行文件可以直接在 Linux 环境下运行。

需要说明的是: GPL 同其他的自由软件许可证一样, 许可公众享有运行、复制软件的自由, 发行传播软件的自由, 获得软件源码的自由, 改进软件并将自己做出的改进版本向社会发行传播的自由。

由于 Linux 的源程序是完全公开的, 任何人只要遵循 GPL, 就可以对内核加以修改并发布给他人使用。Linux 内核的版本在发行上有自己的规则, 可以从其版本号加以识别。版本号的格式为“x.yy.zz”。其中 x 介于 0 到 9 之间, 而 yy, zz 则介于 0 到 99 之间。通常数字越大说明版本越高。而且它有一个非常简单的编号约定: 任何偶数的核心 (例如 2.0.30) 都是一个稳定的核心, 而任何奇数的核心 (例如 2.1.42) 都是一个开发中的核心, 用以进行最新功能的测试, 不建议初学者和生产过程中使用。一些版本号后面有时会见到 pNN 的字样, NN 是介于 0 到 20 之间的数字, 它代表对某一版本的内核“打补丁”或者是修改的次数。

Linux 内核版本发布的官方网站是 <http://www.kernel.org>。新版本的内核分两种, 一种是 full Source 版本, 另外一种 patch 文件, 即补丁。完整的内核版本比较大, 一般是 tar.gz 或.bz2 文件, 二者分别是使用 gzip 或者 bzip2 进行压缩的文件, 使用时需要解压缩。patch 文件则比较小, 一般只有几十 KB 到几百 KB, 但是 patch 文件是针对特定的版本的, 用户需要找到自己对应的版本才能使用。

1.6 常见的 Linux 发行版本

1.6.1 Red Hat Linux

Red Hat Linux 俗称红帽子 Linux, 是应用最广、最为成熟的 Linux 发行版本, 也可以说是最著名的 Linux 版本。Red Hat Linux 已经创造了自己的品牌, 越来越多的人听说过它。Red Hat 在 1994 年创业, 当时聘用了全世界 500 多名员工, 他们都致力于开放的源代码体系。