

万水 Linux 技术丛书

Red Hat Linux 安全与优化

[美] Mohammed J. Kabir 著

邓少鹄 等译

中国水利水电出版社

内 容 提 要

全书共 21 章, 分为五个部分, 全面覆盖系统性能、网络和服务性能、系统安全、网络服务安全、防火墙等。书中介绍了大量与应用程序相关的性能和测试技术, 并讲解如何调整计算机和网络的性能。本书覆盖所有主要的 Red Hat Linux 应用程序, 比如 Apache Web 服务器、WuFTP 服务器、FTP 服务器、BIND DNS 服务器、Sendmail SMTP 服务器等, 并针对如何增强它们的安全性进行了深入而详尽的讨论。本书讲解翔实, 内容丰富, 适合广大 Linux 或 UNIX 系统管理员以及对安全方面感兴趣的读者阅读。

图书在版编目 (CIP) 数据

Red Hat Linux 安全与优化/(美)卡比尔(Kabir,M.J.)著;邓少鹞等译. —北京:中国水利水电出版社, 2003

(万水 Linux 技术丛书)

ISBN 7-5084-1984-7

I. R… II. ①卡… ②邓… III. ①Linux 操作系统—安全技术②Linux 操作系统—系统性能—最佳化 IV. TP316.89

中国版本图书馆 CIP 数据核字 (2003) 第 118710 号

书 名	Red Hat Linux 安全与优化
作 者	[美] Mohammed J.Kabir 著 邓少鹞 等译
出版、发行	中国水利水电出版社 (北京市三里河路 6 号 100044) 网址: www.waterpub.com.cn E-mail: mchannel@public3.bta.net.cn (万水) sale@waterpub.com.cn
经 售	电话: (010) 63202266 (总机)、68331835 (营销中心)、82562819 (万水) 全国各地新华书店和相关出版物销售网点
排 版	北京万水电子信息有限公司
印 刷	北京市天竺颖华印刷厂
规 格	787×1092 毫米 16 开本 31.25 印张 715 千字
版 次	2004 年 1 月第一版 2004 年 1 月北京第一次印刷
印 数	0001—5000 册
定 价	48.00 元

凡购买我社图书, 如有缺页、倒页、脱页的, 本社营销中心负责调换
版权所有·侵权必究

译者序

Linux 的产生、发展和如今的流行，无不得益于互联网络。在如今的 Internet 上，有许许多多的 Linux 系统提供了各种各样的网络服务。但是 Internet 在给 Linux 的发展带来前所未有的机遇的同时，也让它们面临更多的安全隐患。任何一个操作系统都不是完全安全的。如何增强系统的安全性以及调整其运行性能，是 Linux 系统管理员最关心的问题之一。每个合格而敬业的系统管理员，都应该勇敢地面对并认真思索自己面临的任何问题。

在所有关于 Linux 用户和系统/网络管理员的 Linux 邮件列表中，充斥着如何保护 Linux 服务器的安全问题以及如何在 Linux 平台上进行安全电子交易的讨论。而根据 IDC 的数据，在美国，Red Hat Linux 控制着 70% 的 Linux 市场。Linux 操作系统的下载数量，根据估计大约已经高达数百万份。

本书展示了如何保护 Linux 系统的每一个构件的安全，包括 FTP、Sendmail 和 Apache 服务器等。从防火墙到 root 账号再到文件系统安全，书中展示了如何只进行简单地预防就能够减少被攻击的机会，另外还包括对系统进行优化调整所使用的性能和测试技术。

本书是针对 Linux 高级用户和管理人员的一本参考手册，覆盖了所有的安全问题，包括文件系统安全、保护 root 账号以及防火墙。其他的安全书籍经常讨论如何使用某些补丁来修复安全问题，但是本书展示如何让所有的应用程序变得安全，从而使得被攻击的可能性变得很小。

本书介绍了大量与应用程序相关的性能和测试技术，并讲解如何调整计算机和网络的性能。本书覆盖所有主要的 Red Hat Linux 应用程序，比如 Apache Web 服务器、WuFTP 服务器、FTP 服务器、BIND DNS 服务器、Sendmail SMTP 服务器等，并针对如何增强它们的安全性进行了深入而详尽的讨论。除了 Apache Web 服务器之外，本书还讨论了如何保护 NFS 和 Samba 服务器的安全。

全书共 21 章，分为五个部分，全面覆盖系统性能、网络和服务性能、系统安全、网络安全、防火墙等。5 个附录包括详细的背景资料备查和相应的参考链接。

作者以其丰富的工程实践和严谨的治学作风，揭开深藏在安全这个神秘的领域中的敏感世界，将这一切奉献给读者。本书讲解翔实，内容丰富，适合广大 Linux 或 UNIX 系统管理员以及对安全方面感兴趣的读者阅读。

本书由邓少鹑、江峰、吴超亮、余陈钢、曾生根等完成主要章节的翻译工作，参加录入、校对和排版的其他人员还有王江书、刘培英、何易非、任芳、金姜、刘益玲、周建飞、祝琳等，全文由邓劲生统校。尽管我们在这段时间里都全身心地投入，力图早日将这本佳作早日奉献给广大用户，但是由于时间仓促及译者水平有限，书中若有偏差或错误之处，敬请广大读者批评指正。

译者
2003 年 9 月

前 言

本书集中讲述 Red Hat Linux 系统管理的两个主要方面：性能管理和安全。书中所讲述的性能管理方案有助于读者更好地使用 Red Hat Linux 系统。本书第二部分所讨论的实用安全方案可以极大地提高系统的安全性。如果想节省时间，可以只阅读性能管理和安全方面的实用解决方案。

本书是如何组织的

本书包括五部分和四个附录。

第一部分：系统性能

本部分重要讲述了测量系统性能，配置 Red Hat Linux 内核的基础，以便调整操作系统。可以管理硬盘、日志及系统文件，来提高文件系统的可靠性和健壮性。

第二部分：网络和服务性能

本部分说明了如何管理网络服务，包括 Apache Web 服务器、Sendmail 和 postfix 邮件服务器、Samba 和 NFS 文件及打印机共享服务。

第三部分：系统安全

本部分主要讲述了如何用基于内核的 Linux 入侵检测系统（Linux Intrusion Detection System, LIDS）和 Libsafe 缓冲区溢出保护机制来保护系统。只要学会如何保护 Red Hat Linux 内核，就可以用各种工具来保护文件系统。在学会保护内核和文件系统之后，就可以用各种工具来放心地让用户访问系统。可以使用的工具有嵌入式认证模块（Pluggable Authentication Module, PAM）、开放安全套接字层（Open Source Secure Socket Layer, OpenSSL）、安全远程口令（Secure Remote Password, SRP）及 xinetd 等。

第四部分：网络服务安全

本部分主要描述了如何保护 Apache Web 服务器、BIND DNS 服务器、Sendmail 和 postfix 等 SMTP 服务器、POP3 邮件服务器、Wu-FTPd 和 ProFTPD FTP 服务器以及 Samba 和 NFS 服务器。

第五部分：防火墙

本部分主要讲述了如何用 iptables 创建报文过滤防火墙；如何建立虚拟专网；如何用基于 SSL 的通道来保护对系统和服务的访问。最后介绍了大量的安全工具，比如安全评估工具、端口扫描器、日志检测和分析工具、CGI 扫描器、口令破译器、入侵检测工具、报文过滤工具和其他各种不同的管理工具。

附录

附录包括对 Linux 网络用户来说较为重要的参考。

书中程序都已运行通过，读者可以到中国水利水电出版社网站上下载本书源代码，网

址：www.waterpub.com.cn。

本书约定

读者阅读本书时，只需要记住通常的规则，不需要了解新的约定。常用的规则有：

- ◇ 当要求输入命令时，在命令提示符下输入完命令后需要按 Enter 键或 Return 键结束。
- ◇ 等宽字体用来描述结构或代码片段
- ◇ 斜体文本需要被相关信息代替

要注意一些偶尔出现的突出显示的段落图标。



注意图标表示一些信息需要较详细解释。



提示图标告知一些可以节省时间和精力信息。



警告图标提示注意一些潜在的危险。



交叉引用图标告知在其他的章节里可以找到的相关信息。

告诉我们您对本书的看法

我和 Hungry Minds 希望能够得到您对本书的看法。请在 Hungry Minds 站点上 (www.hungryminds.com) 注册本书并向我们提供反馈意见。如果想和我直接通信，可以发电子邮件，我的信箱是 kabir@evoknow.com。我将尽量及时地给予答复。

关于作者

Mohammed Kabir 是 Evoknow, Inc.的创建者和 CEO。他的公司主要业务是开放源码解决方案和客户关系管理软件开发。当他不是很忙于管理软件项目或者编写图书时，他喜欢在世界各地旅游。Kabir 曾经在 Sacramento 的 California State University 学习计算机。他还是 Red Hat Linux Server and Apache Server Bible 一书的作者。可以通过 kabir@evoknow.com 联系到他本人。

致 谢

当写这本书时，我经常需要向本书中所涉及到的一些工具的开发者的咨询。我要特别感谢这些开发者们，他们无私地给我提供了大量的辛勤劳动。

Huagang Xie 是 LIDS 项目的发起人和主要的开发者。特别地感谢他答复我的电子咨询及给我提供关于该主题的大量信息。

Timothy K. Tsai、Navjot Singh 和 Arash Baratloo 是 Libsafe 小组的三个成员，他们在提供 Libsafe 信息方面给了我极大的帮助。非常感谢 Tim 及时答复我的电子邮件，并给我提供该主题的大量信息。

我要感谢 Red Hat 出版社和 Hungry Minds 组，是他们使得本书得以出版。在这里不可能列出所涉及到的每个人，但我还是要提一下下面的个人：

Debra Williams Cauley 给我提供了写这本书的机会，并且使我看到出书的过程。感谢 Debra。

编辑 Terri Varveris 在 Debra 不在的时候接任 Debra 的工作。是她确保我能够得到所需要的所有帮助，感谢 Terri。

项目进展编辑 Pat O'Brien 使得该项目得以进行。如果没有他的无私帮助和建议，我真的不知道该如何做。感谢 Pat。

技术评论家 Matt Hayden 提供了大量技术上的建议、提示和技巧，其中有许多已经和本书融为一体。感谢 Matt。

我的妻子 Sheila Kabir 在写这本书的几个月中花了许多工作时间。谢谢你，Sheila Kabir。

目 录

译者序
前言
致谢

第一部分 系统性能

第 1 章	性能的基本要求.....	2
1.1	测量系统性能.....	2
1.1.1	使用 ps 监控系统性能.....	3
1.1.2	使用 top 跟踪系统行为.....	4
1.1.3	使用 vmstat 检测内存以及 I/O.....	6
1.1.4	运行 vtad 分析系统.....	7
1.2	小结.....	7
第 2 章	内核调整.....	8
2.1	编译和安装自定义内核.....	8
2.1.1	下载最新的内核源代码.....	8
2.1.2	创建/usr/src/linux 符号链接.....	9
2.1.3	选择内核配置方法.....	9
2.1.4	使用 menuconfig.....	10
2.1.5	编译内核.....	22
2.1.6	启动新内核.....	23
2.2	运行高要求应用程序.....	25
2.3	小结.....	26
第 3 章	文件系统调整.....	27
3.1	硬盘调整.....	27
3.2	ext2 文件系统调整.....	31
3.2.1	改变 ext2 文件系统的块尺寸.....	31
3.2.2	使用 e2fsprogs (ext2 文件系统磁盘工具) 调整 ext2 文件系统.....	31
3.3	使用日志式文件系统.....	34
3.3.1	编译和安装 ReiserFS 文件系统.....	35
3.3.2	使用 ReiserFS 文件系统.....	36
3.3.3	基准测试 ReiserFS 文件系统.....	36
3.4	管理逻辑卷.....	38

3.4.1	编译和安装 LVM 内核模块.....	38
3.4.2	创建逻辑卷.....	40
3.4.3	向逻辑卷添加一个新磁盘或分区.....	44
3.4.4	从卷组中删除一个磁盘或分区.....	46
3.5	使用 RAID、SAN 或存储应用.....	47
3.5.1	使用 Linux 软件 RAID.....	47
3.5.2	使用硬件 RAID.....	47
3.5.3	使用 SAN.....	48
3.5.4	使用存储应用.....	48
3.6	使用基于 RAM 的文件系统.....	48
3.7	小结.....	51

第二部分 网络和服务性能

第 4 章	网络性能.....	53
4.1	优化以太网局域网或广域网.....	53
4.1.1	使用网络分割技术提高性能.....	54
4.1.2	用交换机取代集线器.....	57
4.1.3	使用高速以太网.....	58
4.1.4	使用主干网.....	58
4.1.5	理解和控制网络数据流量.....	59
4.1.6	使用 DNS 服务器均衡负载.....	60
4.2	IP Accounting.....	61
4.2.1	在 Linux 网关系统上使用 IP accounting.....	61
4.3	小结.....	62
第 5 章	Web 服务器性能.....	63
5.1	编译有特定要求的 Apache 服务器.....	63
5.2	调整 Apache 配置.....	68
5.2.1	控制 Apache 进程.....	68
5.2.2	控制系统资源.....	71
5.2.3	使用动态模块.....	73
5.3	加速静态 Web 页面.....	74
5.3.1	利用减少磁盘输入/输出加速静态页面传送.....	74
5.3.2	使用内核 HTTP 守护进程.....	75
5.4	加速 Web 应用.....	75
5.4.1	使用 mod_perl 模块.....	75
5.4.2	使用 FastCGI.....	82
5.4.3	为 Apache 安装配置 FastCGI 模块.....	82

5.4.4	使用 Java Servlet	84
5.4.5	使用 Squid 代理缓存服务器.....	85
5.5	小结.....	88
第 6 章	E-mail 服务器性能.....	89
6.1	如何选择 MTA.....	89
6.2	调整 Sendmail.....	90
6.2.1	控制消息的最大尺寸.....	91
6.2.2	高速缓存连接.....	91
6.2.3	控制同时连接数.....	93
6.2.4	通过 Sendmail 限制负载.....	93
6.2.5	处理邮件队列时如何节约内存.....	94
6.2.6	控制等待队列中的消息数.....	94
6.2.7	控制整个队列状态.....	94
6.3	调整 Postfix	94
6.3.1	安装 Postfix	95
6.3.2	限制使用的进程数.....	96
6.3.3	限制消息的最大尺寸.....	96
6.3.4	限制队列中的消息数.....	96
6.3.5	限制同时发送给一个站点的邮件数量.....	96
6.3.6	控制整个队列状态.....	96
6.3.7	控制等待队列中的消息长度.....	97
6.3.8	控制消息队列处理频率.....	97
6.4	使用 PowerMTA 处理大量外发邮件.....	97
6.4.1	使用多重 spool 目录以提高速度.....	98
6.4.2	设置文件描述符的最大个数.....	98
6.4.3	设置用户进程的最大数目.....	98
6.4.4	设置并发 SMTP 连接的最大数.....	98
6.4.5	性能管理.....	99
6.5	小结.....	100
第 7 章	NFS 和 Samba 服务器性能.....	101
7.1	优化 Samba 服务器.....	101
7.1.1	控制 TCP socket 选项.....	101
7.2	优化 Samba 客户端.....	104
7.3	优化 NFS 服务器.....	104
7.3.1	优化读/写块的大小.....	105
7.3.2	设定合适的最大传输单元.....	107
7.3.3	运行合理数目的 NFS 守护进程.....	107

7.3.4 管理报文碎片	108
7.4 小结	108

第三部分 系统安全

第 8 章 内核安全	110
8.1 使用 Linux 闯入者侦测系统 (LIDS)	110
8.1.1 建立基于 LIDS 的 Linux 系统	111
8.1.2 管理 LIDS	116
8.2 用 libsafe 保护程序的堆栈	123
8.2.1 编译和安装 libsafe	124
8.2.2 使用 libsafe	126
8.3 小结	126
第 9 章 保护文件和文件系统的安全	127
9.1 管理文件、目录和组用户权限	127
9.1.1 理解文件的所有权和访问权限	127
9.1.2 用 chown 命令修改文件和目录的所有权	128
9.1.3 用 chgrp 修改文件和目录的组所有权	129
9.1.4 使用八进制数来设置文件和目录的访问权限	129
9.1.5 使用访问字符串来设置访问权限	131
9.1.6 用 chmod 改变文件和目录的存取权限	131
9.1.7 管理符号链接	132
9.1.8 管理用户组权限	133
9.2 检查用户和组的一致性	135
9.3 保证文件和目录的安全	141
9.3.1 理解文件系统的层次结构	142
9.3.2 使用 umask 设置系统级的默认访问控制模型	144
9.3.3 处理完全访问文件	145
9.3.4 处理 set-UID 和 set-GID 程序	147
9.4 使用 ext2 文件系统的安全特性	150
9.4.1 使用 chatter	151
9.4.2 使用 lsattr	151
9.5 使用文件完整性检测器	152
9.5.1 使用自己的文件完整性检测器	152
9.5.2 使用 Linux 版本中开放源代码的 Tripwire	156
9.6 安装完整性检测器	167
9.6.1 安装 AIDE	167
9.6.2 安装 ICU	168

9.7	创建权限策略.....	174
9.7.1	设置用户对配置文件的访问权限.....	174
9.7.2	为用户设置文件的默认访问权限.....	174
9.7.3	设置可执行文件的访问权限.....	175
9.8	小结.....	175
第 10 章	PAM	176
10.1	什么是 PAM.....	176
10.1.1	使用 PAM 配置文件工作.....	177
10.2	建立 PAM-aware 应用程序.....	179
10.3	使用不同的 PAM 模块来增强安全性.....	181
10.3.1	通过时间控制访问.....	185
10.3.2	限制除了 root 用户之外所有用户的访问.....	186
10.3.3	在用户之间管理系统资源.....	187
10.3.4	使用 mod_console 对控制台进行安全的访问.....	188
10.4	小结.....	189
第 11 章	OpenSSL.....	190
11.1	理解 SSL 如何工作.....	190
11.1.1	对称加密.....	191
11.1.2	非对称加密.....	191
11.1.3	SSL 是数据加密的一个协议.....	191
11.2	理解 OpenSSL.....	192
11.2.1	使用 OpenSSL.....	192
11.2.2	获得 OpenSSL.....	193
11.3	安装和配置 OpenSSL.....	193
11.3.1	OpenSSL 先决条件.....	193
11.3.2	编译和安装 OpenSSL.....	193
11.4	理解服务器证书.....	195
11.4.1	什么是证书.....	195
11.4.2	什么是认证机构.....	196
11.4.3	商业 CA.....	196
11.4.4	自我验证的个人 CA.....	197
11.5	从商业 CA 获得服务器证书.....	197
11.6	创建个人 CA.....	198
11.7	小结.....	199
第 12 章	屏蔽密码和 OpenSSH.....	200
12.1	理解用户账号的风险.....	200
12.2	保护用户账号的安全.....	201

12.2.1	使用屏蔽的密码和组.....	202
12.2.2	检查密码一致性.....	204
12.2.3	清除风险性的 shell 服务.....	204
12.3	使用 OpenSSH 进行安全远程访问.....	206
12.3.1	获取并安装 OpenSSH.....	206
12.3.2	配置 OpenSSH 服务.....	207
12.3.3	连接到 OpenSSH 服务器.....	212
12.4	管理 root 账号.....	216
12.4.1	限制 root 账号的访问.....	217
12.4.2	使用 su 命令成为 root 用户或其他用户.....	218
12.4.3	使用 sudo 委派 root 用户访问.....	219
12.5	监控用户.....	223
12.5.1	列出当前登录系统的用户.....	223
12.5.2	记录曾经访问过系统的用户.....	225
12.6	创建用户访问安全策略.....	225
12.7	创建用户终止安全策略.....	225
12.8	小结.....	226
第 13 章	安全远程密码.....	227
13.1	设置安全远程密码支持.....	227
13.2	建立指数密码系统 (EPS).....	228
13.2.1	使用 EPS PAM 模块进行密码验证.....	228
13.2.2	将标准密码转换成 EPS 格式.....	229
13.3	使用启用 SRP 的 Telnet 服务.....	229
13.3.1	在非 Linux 平台上使用启用 SRP 的 Telnet 客户机.....	231
13.4	使用启用 SRP 的 FTP 服务.....	231
13.4.1	在非 Linux 平台上使用启用 SRP 的 FTP 客户机.....	234
13.5	小结.....	234
第 14 章	xinetd.....	235
14.1	什么是 xinetd.....	235
14.2	设置 xinetd.....	236
14.2.1	获得 xinetd.....	236
14.2.2	编译和安装 xinetd.....	237
14.2.3	配置 xinetd 服务.....	240
14.3	启动、重新加载和停止 xinetd 服务.....	243
14.4	加强/etc/xinetd.conf 配置文件中默认值的安全性.....	243
14.5	使用 xinetd 运行 Internet 后台进程.....	244
14.6	用名字或 IP 地址控制访问.....	245

14.7	根据一天中的某个时段控制访问.....	246
14.8	减少拒绝服务攻击的风险.....	246
14.8.1	限制服务器的数目.....	246
14.8.2	限制 log 文件大小.....	247
14.8.3	限制负载.....	247
14.8.4	限制连接速率.....	248
14.9	创建有区别的访问服务.....	248
14.10	重定向和转发客户请求.....	249
14.11	使用 xinetd 的 TCP Wrapper.....	251
14.12	将 sshd 作为 xinetd 运行.....	251
14.13	使用 xadmin.....	252
14.14	小结.....	254

第四部分 网络服务安全

第 15 章	Web 服务器安全.....	256
15.1	了解 Web 风险.....	256
15.2	为 Apache 配置切实可行的安全措施.....	257
15.2.1	为 Apache 使用专门的用户和组.....	257
15.2.2	使用一个安全的目录结构.....	257
15.2.3	使用相应的文件和目录权限.....	258
15.2.4	使用目录索引文件.....	259
15.2.5	禁止默认访问.....	261
15.2.6	禁止用户重载.....	261
15.3	使用偏执的配置.....	262
15.4	减少 CGI 风险.....	262
15.4.1	信息漏洞.....	263
15.4.2	系统资源的消耗.....	263
15.4.3	通过 CGI 脚本进行系统命令的欺骗.....	263
15.4.4	禁止用户输入对系统不安全的调用.....	264
15.4.5	在 HTML 页面中隐藏数据的用户修改.....	267
15.5	包装 CGI 脚本.....	272
15.5.1	SuEXEC.....	273
15.5.2	CGIWrap.....	275
15.5.3	隐藏有关 CGI 脚本的线索.....	276
15.6	减少 SSI 风险.....	277
15.7	记录任何事件.....	278
15.8	限制对敏感内容的访问.....	279

15.8.1	使用 IP 或主机名	280
15.8.2	使用 HTTP 验证方案	281
15.8.3	控制 Web Robot	285
15.9	内容发布指导方针	287
15.10	使用 Apache-SSL	287
15.10.1	编译和安装 Apache-SSL 补丁	288
15.10.2	为 Apache-SSL 服务器创建一个证书	288
15.10.3	为 SSL 配置 Apache	289
15.10.4	测试 SSL 连接	291
15.11	小结	291
第 16 章	域名服务器安全	292
16.1	理解什么是 DNS 欺骗	292
16.2	使用 Dlint 检查 DNS 配置	293
16.2.1	获得 Dlint	293
16.2.2	安装 Dlint	293
16.2.3	运行 Dlint	294
16.3	配置安全的 BIND	296
16.3.1	将事务签名 (TSIG) 用于区带传输	297
16.3.2	非 root 用户运行 BIND	300
16.3.3	隐藏 BIND 的版本号	300
16.3.4	请求限制	300
16.3.5	关闭 glue fetching	301
16.3.6	为域名服务器创建 chroot	301
16.3.7	使用 DNSSEC (签字区带)	302
16.4	小结	303
第 17 章	E-mail 服务器安全	304
17.1	什么是开放式邮件中继	304
17.2	电子邮件服务器是否易于攻击	305
17.3	保护 Sendmail	308
17.3.1	控制邮件中继	309
17.3.2	允许 MAPS 实时黑洞列表 (RBL) 支持	311
17.3.3	使用 procmail 清理输入邮件	315
17.3.4	只发出邮件	320
17.3.5	在没有 root 特权的情况下运行 Sendmail	321
17.4	保护 Postfix	322
17.4.1	拒收垃圾邮件	322
17.4.2	通过伪装来隐藏内部邮件地址	324

17.5	小结.....	324
第 18 章	FTP 服务器安全	325
18.1	保证 WU-FTPD 的安全	325
18.1.1	通过用户名限制 FTP 访问	326
18.1.2	设置 FTP 默认文件许可	327
18.1.3	使用 FTP 会话限制	328
18.1.4	使用/etc/ftpaccess 中的选项保护 WU-FTPD.....	331
18.2	使用 ProFTPD.....	333
18.2.1	下载、编译和安装 ProFTPD.....	333
18.2.2	配置 ProFTPD.....	334
18.2.3	监控 ProFTPD.....	337
18.2.4	保证 ProFTPD 的安全.....	338
18.3	小结.....	344
第 19 章	Samba 服务器和 NFS 服务器安全	345
19.1	Samba 服务器的安全性	345
19.1.1	选择合适的安全级别.....	345
19.1.2	避免明语密码.....	347
19.1.3	允许来自信任域的用户进行访问.....	348
19.1.4	通过网络接口控制 Samba 访问	348
19.1.5	通过主机名和 IP 地址控制 Samba 访问.....	349
19.1.6	使用 pam_smb 对 Windows NT 服务器的所有用户进行验证	349
19.1.7	将 OpenSSL 用于 Samba.....	351
19.2	NFS 服务器安全性.....	352
19.3	使用密码文件系统.....	355
19.4	小结.....	355

第五部分 防火墙

第 20 章	防火墙、虚拟专网和 SSL 通道.....	357
20.1	报文过滤防火墙.....	357
20.1.1	在内核中启用 netfilter	361
20.2	利用 iptables 创建报文过滤规则.....	362
20.2.1	创建默认的策略.....	362
20.2.2	添加规则.....	362
20.2.3	列出规则.....	363
20.2.4	删除规则.....	363
20.2.5	在链中插入新规则.....	363
20.2.6	在链中更换规则.....	363

20.3	创建 SOHO 报文过滤防火墙	364
20.3.1	允许专网用户访问外部 Web 服务器.....	366
20.3.2	允许外部 Web 浏览器访问防火墙上的 Web 服务器	367
20.3.3	DNS 客户端和单一高速缓存服务	368
20.3.4	SMTP 客户服务	369
20.3.5	POP3 客户服务.....	370
20.3.6	被动模式的 FTP 客户服务	370
20.3.7	SSH 客户服务.....	371
20.3.8	其他的新客户服务	371
20.4	创建简单防火墙	372
20.5	创建透明代理地址解析协议防火墙	373
20.6	创建组织防火墙.....	374
20.6.1	内部防火墙的目的.....	374
20.6.2	主防火墙的目的.....	375
20.6.3	安装内部防火墙.....	375
20.6.4	安装主防火墙.....	376
20.7	安全的虚拟专网.....	384
20.7.1	编译和安装 FREE S/WAN	385
20.7.2	创建虚拟专网.....	386
20.8	Stunnel: 通用的 SSL 包装.....	390
20.8.1	编译和安装 Stunnel.....	390
20.8.2	保障 IMAP 安全.....	391
20.8.3	保障 POP3 安全.....	391
20.8.4	为特殊情况保障 SMTP 安全.....	392
20.9	小结.....	392
第 21 章	防火墙安全工具.....	393
21.1	使用安全评估(审核)工具.....	393
21.1.1	利用 SAINT 执行安全审核	393
21.1.2	SARA	399
21.1.3	VetesCan	399
21.2	使用端口扫描器.....	399
21.2.1	使用 nmap 执行痕迹分析.....	399
21.2.2	使用 PortSentry 监视连接.....	401
21.2.3	使用 Nessus 安全扫描器.....	405
21.2.4	使用 Strobe	408
21.3	使用日志监视和分析工具.....	408
21.3.1	使用日志检查来探测不寻常的日志条目	408