万水 Linux 技术丛书

Red Hat Linux 安全与优化

[美] Mohammed J. Kabir 著

邓少鹃 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;邓少鹃等译. —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 邓少鹃 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 电话：（010）63202266（总机）、68331835（营销中心）、82562819（万水）
经　　售	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

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、网络服务安全、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。

本书由邓少鹃、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的信息。

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

第二部分 网络和服务性能

第三部分 系统安全

第四部分 网络服务安全

第五部分 防火墙