Broadview
www.broadview.com.cn

LAMP技术大系

曹江华作品系列

本书特色

- 详细介绍了Linux下最主要服务器的安全策略，几乎涉及所有主流Linux擅长的领域，弥补了国内图书在Linux安全领域的空白。
- 针对服务器领域使用最为广泛的红帽企业版，同时兼顾一些Linux发行版。
- 第2版重点关注了开源数据库安全、Linux无线安全、Selinux配置、内核安全审计等其他国内图书甚少涉及的领域。
- 第2版根据广大读者的反馈信息进行了合理的内容调整，修改的篇幅比较多，更加符合现在Linux服务器安全领域的现状。

Linux 服务器安全策略详解（第2版）

曹江华 著

電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
http://www.phei.com.cn

畅销书升级版

LAMP技术大系

曹江华作品系列

Linux服务器安全策略详解（第2版）

曹江华 著

電子工業出版社
Publishing House of Electronics Industry
北京•BEIJING

内 容 简 介

“Linux 就是服务器，或者换句话说，是服务器成就了 Linux。”相信读者对于这样的判断肯定会有不同意见。这里不是以偏概全，只为强调 Linux 与服务器与生俱来的天然联系。实际上，对于 Linux 厂商而言，约 90%以上的收入都来自服务器应用市场。Linux 主要用于架设网络服务器。如今关于服务器和网站被黑客攻击的报告几乎每天都可以见到，而且随着网络应用的丰富多样，攻击的形式和方法也千变万化。如何增强 Linux 服务器的安全性是 Linux 系统管理员最关心的问题之一。

本书共 28 章和 1 个附录。概括而言，实质是五部分内容：第一部分分级介绍对 Linux 服务器的攻击情况，以及 Linux 网络基础；第二部分是本书的核心，针对不同的 Linux 服务器分别介绍各自的安全策略；第三部分介绍 Linux 服务器的安全工具；第四部分是 Linux 下开源数据库安全以及 Linux 下新闻组服务器构建、网络钓鱼的防范、Linux 无线网络构建及其安全策略、使用 Linux 安全审计以及使用 Selinux 保护 Linux 服务器的方法；第五部分是 1 个附录，介绍 Linux 服务器应急响应流程与步骤。

本书适合作为大专院校计算机专业师生的教材或教学参考书，也适合于 Linux 网络管理员和系统管理员，以及对安全方面感兴趣的读者。

图书在版编目（CIP）数据

Linux 服务器安全策略详解 / 曹江华著. —2 版. —北京：电子工业出版社，2009.6
（LAMP 技术大系）
ISBN 978-7-121-08680-9

I. L… Ⅱ. 曹… 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 060276 号

策划编辑：李 冰
责任编辑：江 立
印 刷：北京天宇星印刷厂
装 订：三河市皇庄路通装订厂
出版发行：电子工业出版社
北京市海淀区万寿路 173 信箱 邮编 100036
开 本：860×1092 1/16 印张：49.5 字数：1304 千字
印 次：2009 年 6 月第 1 次印刷
印 数：4000 册 定价：89.00 元

凡所购买电子工业出版社图书有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系，联系及邮购电话：（010）88254888。

质量投诉请发邮件至 zlts@phei.com.cn，盗版侵权举报请发邮件至 dbqq@phei.com.cn。

服务热线：（010）88258888。

前　言

Linux 系统属于开放源代码软件，由于 Linux 系统具有稳定、安全、网络负载力强、占用硬件资源少等技术特点，自问世以来得到了迅速推广和应用，并已发展为当今世界的主流操作系统之一。目前对 Linux 感兴趣的用户主要集中在一些垂直行业当中。在国外，企图提升利润率的有零售、家电行业，包括石油、动画设计等在内的计算密集型应用企业，还有想通过 Linux 的成本控制来提高企业竞争优势的一些电信、政府和医疗行业。对于零售行业的 POS 终端和数据中心而言，Linux 既可靠又便宜。石油行业则通常利用上千个结点的 Linux 集群来承担石油勘探中的大量运算工作。国内的企业应用同样也迅速普及。由于电子政务的“崛起”，政府行业已占据了 Linux 市场的大量份额。能源行业的 Linux 应用在国内市场份额上也名列前茅。金融、电信等传统大行业应用 Linux 的趋势已然显露。可以总结出 Linux 的擅长应用领域是：

1．单一应用的基础服务器，如 DNS 和 DHCP 服务器、Web 服务器、防火墙、文件和互联网代理服务器。

2．界定清晰，与其他系统没有交叉的应用。

3．高性能计算及计算密集型应用，如风险分析、数据分析、数据建模等。

4．中小型数据库。

对于那些应用很单纯的企业，购买 Linux 软件的成本优势则十分明显。与 Windows 系列相比，Linux 令人欣慰的一点是其出色的安全性，可以降低管理成本。这也是使很多公司转向 Linux 的一个非常重要的原因。在 Windows 服务器上，补丁让人应接不暇，耗费大量时间和精力。于是，人们选择了 Linux。尽管 Linux 也会受病毒和黑客的侵扰，但是 Linux 内核毕竟是由众多具有黑客背景的程序员逐步完善而来的，相对安全一些。

目前，关于 Linux 方面的书虽然较多，但大多数都是介绍如何安装，以及如何使用像 KDE 和 GNOME 这类图形界面的，对 Linux 作为服务器应用的介绍相对较少，Linux 真正的优势和发展方向是作为服务器操作系统。根据需要，Linux 可安装成各种各样的服务器。

Linux 是一个十分稳定的操作系统，目前用户已逾千万。但是，Linux 服务器是否安全，这对 Linux 的用户来说是十分关心的问题。本书的目的，就是要说明 Linux 服务器通过加固配置后是安全的。

第 2 版说明

本书第 1 版在 2007 年 7 月出版后，得到广大读者的关注，同时也得到一些热心读者的宝贵意见和反馈。所以在第 2 版中做了一些内容的添加和删除。在第 8 章 FTP 服务器安全策略部分删除了现在 Linux 平台应用比较少的 Wu-ftp 和 ProFTPD 两种服务器的内容。从 21 章开始是第 2 版添加的主要内容，首先使用三章的篇幅详细论述了两大开源数据库 MySQL 和 PostgreSQL 安全策略。然后以此介绍了 Linux 下新闻组服务器构建、网络钓鱼的防范、Linux 无线网络构建及其安全策略、使用 Linux 安全审计以及使用 Selinux 保护 Linux 服务器的方法。附录部分笔者介绍了 Linux 服务器应急响应的流程与步骤。

限于本书的篇幅已经比较多了，关于虚拟化、集群、Web 2.0 等内容本书没有介绍，对此感兴趣的读者可以查看笔者的《Red Hat Enterprise Linux 5.0 服务器构建与故障排除》。另外对于第 1 版的附录也做了较大的修改。删除了 Linux 命令的介绍，这么做的原因是考虑到目前已经有专门介绍 Linux 命令的相关图书，于是这里笔者节省了宝贵的篇，对此感兴趣的读者可以查看笔者的《Linux 系统最佳实践工具:命令行技术》。

本书主要内容

本书共分 28 章和 1 个附录。

第一部分分级介绍对 Linux 服务器的攻击情况，以及 Linux 网络基础。

第二部分是这本书的核心，针对不同的 Linux 服务器分别介绍各自的安全策略。该部分重点介绍了 Linux 下各种服务器的安全和管理，这些内容在 Linux 系统的学习中非常重要，涉及到 Linux 系统的高级应用，是专业人员必须掌握的内容。这部分内容主要包括 DNS 服务器、DHCP 服务器、Samba 服务器的配置、NFS 服务器、Squid 服务器、Web 服务器、FTP 服务器和电子邮件服务器等。

第三部分介绍 Linux 服务器的安全工具。这些工具并不是 Linux 所特有的，但有几个在 Linux 系统中较为常用。另外，还介绍了 Linux 备份和恢复技术。

第四部分使用三章的篇幅详细论述了两大开源数据库 MySQL 和 PostgreSQL 安全策略。然后依次介绍了 Linux 下新闻组服务器构建、网络钓鱼的防范、Linux 无线网络构建及其安全策略、使用 Linux 安全审计以及使用 Selinux 保护 Linux 服务器的方法。

第五部分是附录 A，介绍 Linux 服务器应急响应流程与步骤。

本书中各章描述了下列主题：

章　　节	主要内容
第 1 章　Linux 网络基础与 Linux 服务器的安全威胁	第 1 章重点介绍 Linux 网络基础和 Linux 的 TCP/IP 网络配置，然后解析对 Linux 服务器攻击和开源软件网络安全概述
第 2 章　OpenSSL 与 Linux 网络安全	第 2 章重点介绍理解 SSL 和 OpenSSL 如何工作，理解服务器证书（CA）、安装和配置 OpenSSL、理解服务器证书、数字证书在客户端的应用、OpenSSL 面临安全问题及其解决思路
第 3 章　PAM 与 Open LDAP	第 3 章重点介绍 PAM 工作原理和理解 PAM 配置文件工作，然后介绍建立 PAM 应用程序，使用不同的 PAM 模块来增强安全性。安全应用 PAM，动手制作 Linux 下基于 PAM 机制的 USB Key。然后对 Liunx 目录服务器进行介绍，安装配置 OpenLDAP 服务器及 OpenLDAP 客户端。监控 OpenLDAP 服务器，安全管理 OpenLDAP 服务器
第 4 章　Linux 网络服务和 xinetd	第 4 章重点介绍 Linux 启动过程、Linux 守护进程的概念和结构、xinetd 以及 Linux 服务管理工具、如何安全选择 Linux 服务
第 5 章　DNS 服务器的安全策略	第 5 章重点介绍 DNS 服务器工作原理、DNS 服务器面临的安全问题和应对策略，以及如何建立一个完整的 DNS 系统，掌握 DNS 故障排除工具。动手加固 DNS 服务器和 DNS 服务器安全策略
第 6 章　Web 服务器的安全策略	第 6 章重点介绍 Web 面临的主要威胁，并结合在 Linux 中使用最多的 Apache 服务器，介绍进行 Web 服务器安全配置的技巧
第 7 章　电子邮件服务器的安全策略	第 7 章重点介绍电子邮件系统组成以及相关协议和电子邮件服务器工作原理。阐述电子邮件服务器面临的安全隐患，安装安全 sendmail 服务器和 postfix 服务器

续表

章　节	主要内容
第 8 章　FTP 服务器的安全策略	第 8 章重点介绍 FTP 工作原理以及 FTP 服务面临的安全隐患。然后介绍如何配置安全的 Wuftpd 服务器及 ProFTPD 服务器、Vsftpd 服务器和安全应用客户端 FTP 软件
第 9 章　Samba 服务器的安全策略	第 9 章重点介绍 Samba 工作原理，安装配置 Samba 服务器，配置 Samba 服务器共享文件以及打印机，其他配置 Samba 方法和用好 Linux 下的网络邻居。然后介绍 Samba 服务面临的安全隐患以及 Samba 文件服务器安全策略
第 10 章　NFS 服务器的安全策略	第 10 章重点介绍 NFS 服务器工作原理和安装配置 NFS 服务器，应用 NFS 客户端。然后介绍 NFS 服务器面临的安全隐患以及 NFS 服务器的安全策略
第 11 章　DHCP 服务器的安全策略	第 11 章重点介绍 DHCP 服务器工作原理和安装 DHCP 服务器、DHCP 服务器的故障排除和 DHCP 服务器的安全策略
第 12 章　Squid 服务器的安全策略	第 12 章重点介绍代理服务器工作原理以及安装安全 squid 代理服务器。然后阐述代理服务器面临的安全隐患和代理服务器 Squid 安全策略。全面监控代理服务器 Squid 运行，关注 Squid 代理服务器的日志和为 Squid 代理服务器串列 HAVP
第 13 章　SSH 服务器的安全策略	第 13 章重点介绍 SSH 服务器工作原理和安装 SSH 服务器。然后阐述 SSH 服务器面临的安全隐患，以及 SSH 服务器的安全策略和如何安全应用 SSH 客户端
第 14 章　Linux 防火墙	第 14 章重点介绍防火墙工作原理和 Linux 防火墙 iptables 以及 iptables 防火墙的配置实例
第 15 章　Linux 网络环境下的 VPN 构建	第 15 章重点介绍 VPN 概述和 Linux 下实现 VPN 技术软件概述。然后分别介绍构建基于 CIPE 技术的 Linux VPN、构建基于 PPTP 技术的 Linux VPN、构建基于 SSH VNC 技术的 Linux VPN 和构建基于 IPsec 技术的 Linux VPN
第 16 章　使用 IDS 保护 Linux 服务器	第 16 章重点介绍 IDS 概念，然后介绍 Linux 下配置基于主机的 IDS 和 Linux 下配置基于网络的 IDS、Snort 的安装配置和建立分布式 snort 入侵检测系统
第 17 章　Linux 网络监控策略	第 17 章重点介绍 SNMP 简介和 MRTG 监控过程。然后介绍安装配置 NTOP 监控 Linux 网络和 NTOP 的安全策略
第 18 章　Linux 常用安全工具	第 18 章重点介绍使用 SAINT 执行安全审核、使用端口扫描软件 nmap、使用网络数据采集分析工具 TcpDump、使用 Ethereal 分析网络数据、使用 EtherApe 分析网络数据、使用 GunPGP 进行数据加密和其他安全工具简介
第 19 章　防范嗅探器攻击和 Linux 病毒	第 19 章重点介绍防范嗅探器攻击和 Linux 病毒的防范。
第 20 章　Linux 数据备份恢复技术	第 20 章重点介绍 Linux 备份恢复基础以及 Linux 备份恢复策略，然后介绍 Linux 常用备份恢复工具和 Linux 备份恢复实例
第 21 章　数据库简介 Linux 开源数据库安全现状	第 21 章数据库简介 Linux 开源数据库安全现状。本章将重点数据库模型及其相关内容，然后介绍了 Linux 开源数据库安全现状
第 22 章　MySQL 数据库服务器安全	第 22 章首先介绍 MySQL 数据库简介及 MySQL 数据库在 Linux 中的安装配置，然后重点介绍 MySQL 数据库安全隐患、最大漏洞以及应对措施
第 23 章　PostgreSQL 数据库服务器安全	第 23 章首先介绍 PostgreSQL 数据库及其在 Linux 中的安装配置，然后重点介绍 PostgreSQL 数据库安全隐患、最大漏洞以及应对措施
第 24 章　搭建 Linux 新闻组服务器	第 24 章重点介绍 Linux 下两大新闻组服务器：inn 和 Dnews，以及一些新闻组客户端的应用
第 25 章　在 Linux 网络环境下防范网络钓鱼	第 25 章重点介绍网络钓鱼的产生以及钓鱼实施的过程，然后介绍如何防范网络钓鱼
第 26 章　Linux 无线网络构建及其安全策略	第 26 章重点介绍无线网络标准、Linux 无线网卡驱动安装、Linux 无线网络构建，然后介绍 Linux 无线网络的安全策略
第 27 章　Linux 安全审计系统	第 27 章重点介绍 Linux 内核中的安全审计系统配置和使用方法
第 28 章　使用 SELinux 系统	第 28 章首先介绍 Selinux 的历史和框架，然后重点介绍 Selinux 的使用方法
附录 A　Linux 服务器应急响应流程与步骤	附录 A 重点介绍 Linux 服务器遭到攻击时的应急响应流程与步骤，另外还介绍了计算机辨识学和 Linux 常用端口使用情况

本书特色

- 各章目标。每章的开头都详细地列出了本章中要掌握的概念。
- 插图和表格。本书中有很多 Linux 工具的插图和概念的表格，帮助您直观地、更好地理解 Linux 的工具和技术方面的概念。
- 详细的附录。
- 本书详细介绍了 Linux 下最主要服务器的安全策略，几乎涉及所有主流 Linux 擅长的领域，弥补了国内图书在 Linux 安全领域的空白。
- 本书针对服务器领域使用最为广泛的红帽企业版，同时兼顾一些 Linux 发行版。
- 相对第一版，第二版重点关注了开源数据库安全、Linux 无线安全、Selinux 配置、内核安全审计等其他国内图书甚少涉及的领域。
- 相对第一版，第二版根据广大读者反馈的信息进行了合理的内容调整，修改的篇幅比较多，更加符合现在 linux 服务器安全领域的现状。

读者对象

- 大专院校计算机专业师生。
- IT 行业的相关人员。
- Linux 应用爱好者。
- Linux 网络管理员和系统管理员，以及 Linux 信息安全、网络安全、管理、维护的从业人员。

致谢

首先，感谢编写过程中领导、朋友和家人的支持及帮助，包括 51CTO 网站编辑杨文飞、刘兵、李棉等人。另外，电子工业出版社的李冰和江立编辑在我写书的过程中给了我无私的帮助和鞭策，为了使本书能尽快与读者见面，李冰多次邀请专家对此书提出有益意见，对于此书的修改和完善起到了重要作用。

由于作者水平有限，书中不足及错误之处在所难免，敬请专家和读者给予批评指正。

曹江华

2009 年 3 月

電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
Broadview®
www.broadview.com.cn

《Linux 服务器安全策略详解（第 2 版）》读者交流区

尊敬的读者：

感谢您选择我们出版的图书，您的支持与信任是我们持续上升的动力。为了使您能通过本书更透彻地了解相关领域，更深入的学习相关技术，我们将特别为您提供一系列后续的服务，包括：

1. 提供本书的修订和升级内容、相关配套资料；
2. 本书作者的见面会信息或网络视频的沟通活动；
3. 相关领域的培训优惠等。

请您抽出宝贵的时间将您的个人信息和需求反馈给我们，以便我们及时与您取得联系。

您可以任意选择以下三种方式与我们联系，我们都将记录和保存您的信息，并给您提供不定期的信息反馈。

1．短信

您只需编写如下短信：B08680+您的需求+您的建议

发送到1066 6666 789（本服务免费，短信资费按照相应电信运营商正常标准收取，无其他信息收费）

为保证我们对您的服务质量，如果您在发送短信24小时后，尚未收到我们的回复信息，请直接拨打电话（010）88254369。

2．电子邮件

您可以发邮件至jsj@phei.com.cn或editor@broadview.com.cn。

3．信件

您可以写信至如下地址：北京万寿路173信箱博文视点，邮编：100036。

如果您选择第2种或第3种方式，您还可以告诉我们更多有关您个人的情况，及您对本书的意见、评论等，内容可以包括：

（1）您的姓名、职业、您关注的领域、您的电话、E-mail地址或通信地址；

（2）您了解新书信息的途径、影响您购买图书的因素；

（3）您对本书的意见、您读过的同领域的图书、您还希望增加的图书、您希望参加的培训等。

如果您在后期想退出读者俱乐部，停止接收后续资讯，只需发送“B08680+退订”至10666666789即可，或者编写邮件“B08680+退订+手机号码+需退订的邮箱地址”发送至邮箱：market@broadview.com.cn 亦可取消该项服务。

同时，我们非常欢迎您为本书撰写书评，将您的切身感受变成文字与广大书友共享。我们将挑选特别优秀的作品转载在我们的网站（www.broadview.com.cn）上，或推荐至CSDN.NET等专业网站上发表，被发表的书评的作者将获得价值50元的博文视点图书奖励。

我们期待您的消息！

博文视点愿与所有爱书的人一起，共同学习，共同进步！

通信地址：北京万寿路 173 信箱　博文视点（100036）　　电话：010-51260888

E-mail：jsj@phei.com.cn，editor@broadview.com.cn

反侵权盗版声明

举报电话：（010）88254396；（010）88258888
传　　真：（010）88254397
E-mail：　dbqq@phei.com.cn
通信地址：北京市万寿路 173 信箱
　　电子工业出版社总编办公室
邮　　编：100036

目　录

第 1 章　Linux 网络基础与 Linux 服务器的安全威胁……1

1.1　Linux 网络基础……1

1.1.1　Linux 网络结构的特点……1

1.1.2　TCP/IP 四层模型和 OSI 七层模型……2

1.1.3　TCP/IP 提供的主要用户应用程序……4

1.1.4　端口号分配……5

1.2　Linux 的 TCP/IP 网络配置……7

1.2.1　Linux 的 TCP/IP 网络配置文件……7

1.2.2　网络配置工具……8

1.2.3　配置网络接口……9

1.3　分级解析对 Linux 服务器的攻击……16

1.3.1　攻击者使用什么操作系统……16

1.3.2　典型的攻击者有什么特征……16

1.3.3　攻击者典型的目标是什么……16

1.3.4　实施攻击的原因是什么……17

1.3.5　攻击级别……17

1.3.6　反击措施……20

1.4　开源软件网络安全概述……20

1.5　本章小结……22

第 2 章　OpenSSL 与 Linux 网络安全……23

2.1　理解 SSL 和 OpenSSL 如何工作……23

2.1.1　SSL 功能……23

2.1.2　SSL 协议简介……24

2.1.3　SSL 工作流程……24

2.1.4　OpenSSL 简介……26

2.1.5　OpenSSL 的组成……27

2.2　理解服务器证书（CA）……27

2.2.1　X.509 协议简介……27

2.2.2　金字塔结构的优缺点……28

2.2.3　相关名词解释……28

2.3　Linux 下安装和配置 OpenSSL……30

2.3.1　下载 OpenSSL 源代码……30

2.3.2　安装 OpenSSL……30

2.3.3　产生 CA 凭证……31

2.3.4　CA 产生次级凭证……32

2.3.5　OpenSSL 应用……34

2.3.6　OpenSSL 常用命令……37

2.4　数字证书在客户端的应用……39

2.5　OpenSSL 面临的安全问题及其解决思路……40

2.5.1　OpenSSL 面临的安全问题……40

2.5.2　解决思路……41

2.6　本章小结……42

第 3 章　PAM 与 Open LDAP……43

3.1　PAM 工作原理……43

3.1.1　什么是 PAM……43

3.1.2　为什么使用 PAM……44

3.1.3　PAM 体系结构……44

3.1.4　PAM 工作流程图……45

3.2　PAM 配置文件……46

3.3　建立 PAM 应用程序……47

3.4　PAM 常用认证模块及其应用……49

3.4.1　PAM 常用认证模块……49

3.4.2　PAM 模块应用实例……51

3.5　安全应用 PAM……51

3.5.1　删除不再需要的 PAM 配置文件和模块……51

3.5.2　对 PAM 配置进行备份……51

3.5.3　设置资源限制……52

3.5.4　限制 su 命令……52

3.6　动手制作 Linux 下基于 PAM 机制的 USB Key……52

3.6.1　什么是 USB Key……52

3.6.2 建立 pam_usb 应用 ……53
3.7 Liunx 目录服务器介绍 ……55
3.8 安装配置 OpenLDAP 服务器 ……56
3.8.1 安装 OpenLDAP 服务器 ……56
3.8.2 配置 OpenLDAP 服务器 ……57
3.8.3 启动 OpenLDAP 服务器 ……59
3.9 配置 OpenLDAP 客户端 ……60
3.9.1 配置 Linux OpenLDAP 客户端 ……60
3.9.2 Outlook 如何使用 OpenLDAP ……60
3.10 监控 OpenLDAP 服务器 ……61
3.10.1 使用 uptime 命令 ……61
3.10.2 使用 cron 命令定时监测系统负载 ……61
3.10.3 OpenLDAP 进程的监控 ……62
3.10.4 端口的监控 ……62
3.11 安全管理 OpenLDAP 服务器 ……62
3.11.1 自动启动 OpenLDAP 服务器 ……62
3.11.2 使用访问控制（Access Control）实现用户认证 ……62
3.11.3 禁止整个服务器的匿名访问 ……63
3.11.4 配置 OpenLDAP 使用 TLS 通信 ……63
3.11.5 管理 OpenLDAP 服务器 ……64
3.11.6 OpenLDAP 在 Linux 上集群的应用 ……66
3.12 本章小结 ……66
第 4 章 Linux 网络服务和 xinetd ……67
4.1 Linux 启动过程 ……67
4.1.1 Linux 的启动过程详解 ……67
4.1.2 Linux 运行级 ……71
4.1.3 /etc/inittab 文件详解 ……72
4.1.4 init 和/etc/inittab ……74
4.2 守护进程 ……75
4.2.1 Linux 守护进程的概念 ……75
4.2.2 Linux 系统提供的服务及其守护进程列表 ……75
4.2.3 Linux 守护进程的运行方式 ……79
4.3 xinetd ……81
4.3.1 什么是 xinetd ……81
4.3.2 xinetd 的特色 ……81
4.3.3 使用 xinetd 启动守护进程 ……82
4.3.4 解读/etc/xinetd.conf 和/etc/xinetd.d/* ……83
4.3.5 配置 xinetd ……84
4.3.6 xinetd 防止拒绝服务攻击（Denial of Services）的原因 ……89
4.4 Linux 服务管理工具 ……90
4.4.1 redhat-config-services ……90
4.4.2 ntsysv ……91
4.4.3 chkconfig ……92
4.5 安全选择 Linux 服务 ……92
4.6 本章小结 ……92
第 5 章 DNS 服务器的安全策略 ……93
5.1 DNS 服务器的工作原理 ……93
5.2 域名服务的解析原理和过程 ……94
5.3 DNS 服务器面临的安全问题 ……95
5.3.1 DNS 欺骗 ……97
5.3.2 拒绝服务攻击 ……99
5.3.3 缓冲区漏洞攻击 ……99
5.3.4 分布式拒绝服务攻击 ……99
5.3.5 缓冲区溢出漏洞攻击 ……99
5.3.6 不安全的 DNS 动态更新 ……100
5.4 增强 DNS 安全性的方法 ……100
5.4.1 选择安全没有缺陷的 DNS 版本 ……100
5.4.2 保持 DNS 服务器配置正确、可靠 ……101
5.5 建立一个完整的 DNS ……102
5.5.1 DNS 分类 ……102
5.5.2 安装 BIND 域名服务器软件 ……102
5.5.3 named 配置文件族内容 ……102
5.5.4 配置惟高速存域名服务器 ……103
5.5.5 配置主域名服务器 ……103
5.5.6 配置辅助域名服务器 ……105
5.5.7 配置域名服务器客户端 ……106
5.6 DNS 故障排除工具 ……107
5.6.1 dlint ……107
5.6.2 DNS 服务器的工作状态检查 ……108
5.7 全面加固 DNS 服务器 ……110
5.7.1 使用 TSIG 技术 ……110

5.7.2 使用 DNSSEC 技术……113
5.8 配置安全的 DNS 服务器……114
5.8.1 隔离 DNS 服务器……114
5.8.2 为 BIND 创建 chroot……114
5.8.3 隐藏 BIND 的版本号……114
5.8.4 避免透露服务器的信息……115
5.8.5 关闭 DNS 服务器的 gluefetching 选项……115
5.8.6 控制区域（zone）传输……115
5.8.7 请求限制……115
5.8.8 其他强化措施……116
5.8.9 为 DNS 服务器配置 DNS Flood Detector……117
5.8.10 建立完整的域名服务器……118
5.8.11 建立 DNS 日志……119
5.8.12 增强 DNS 服务器的防范 DoS/DDoS 功能……120
5.8.13 使用分布式 DNS 负载均衡……121
5.8.14 防范 DNS 服务器网络……121
5.8.15 配置防火墙……121
5.9 本章小结……121
第 6 章 Web 服务器的安全策略……122
6.1 Web 服务器软件 Apache 简介……122
6.1.1 Apache 的发展历史……122
6.1.2 市场情况……123
6.1.3 Apache 的工作原理……124
6.1.4 Apache 服务器的特点……125
6.2 Apache 服务器面临的安全问题……126
6.2.1 HTTP 拒绝服务……127
6.2.2 缓冲区溢出……127
6.2.3 攻击者获得 root 权限……128
6.3 配置一个安全的 Apache 服务器……128
6.3.1 勤打补丁……128
6.3.2 隐藏和伪装 Apache 的版本……128
6.3.3 建立一个安全的目录结构……129
6.3.4 为 Apache 使用专门的用户和用户组……129
6.3.5 Web 目录的访问策略……130
6.3.6 Apache 服务器访问控制方法……130
6.3.7 管理 Apache 服务器访问日志……131
6.3.8 Apache 服务器的密码保护……139
6.3.9 减少 CGI 和 SSI 风险……142
6.3.10 让 Apache 服务器在“监牢”中运行……142
6.3.11 使用 SSL 加固 Apache……145
6.3.12 Apache 服务器防范 DoS……150
6.3.13 利用 LDAP 对 Apache 进行认证……150
6.3.14 其他安全工具……151
6.4 本章小结……152
第 7 章 电子邮件服务器的安全策略……153
7.1 电子邮件系统的组成和相关协议……153
7.1.1 操作系统……154
7.1.2 邮件传输代理 MTA……154
7.1.3 邮件分发代理 MDA……156
7.1.4 邮件用户代理 MUA……156
7.1.5 电子邮件服务器协议及其相关命令……157
7.2 电子邮件服务器的工作原理……163
7.2.1 电子邮件的工作流程……163
7.2.2 电子邮件的历史……163
7.2.3 电子邮件地址的组成……164
7.2.4 电子邮件系统和 DNS 的联系……165
7.3 电子邮件服务器面临的安全隐患……166
7.3.1 Linux 病毒……166
7.3.2 网络攻击……166
7.3.3 垃圾邮件及其防范……166
7.4 安装安全的 Sendmail 服务器……170
7.4.1 安装 Sendmail 服务器……170
7.4.2 提高 Sendmail 的防垃圾邮件能力……171
7.4.3 其他保护 Sendmail 的安全措施……173
7.4.4 配置基于 Sendmail 的 Webmail……174
7.4.5 增强 Webmail 邮件服务器的安全……179
7.4.6 监控 Sendmail 的日志文件……180
7.5 安装安全的 Postfix 服务器……181
7.5.1 安装 Postfix 服务器……181
7.5.2 保护 Postfix 服务器……185
7.5.3 自动监控 Postfix 邮件服务器……186
7.6 本章小结……189

第 8 章　FTP 服务器的安全策略……190
8.1　FTP 的工作原理……190
8.1.1　FTP 简介……190
8.1.2　FTP 的功能……191
8.1.3　FTP 服务器登录方式的分类……191
8.1.4　FTP 的工作原理……191
8.1.5　FTP 的典型消息和子命令……193
8.1.6　Linux 服务器端的主要 FTP 软件……196
8.2　FTP 服务器面临的安全隐患……197
8.2.1　缓冲区溢出攻击……197
8.2.2　数据嗅探……198
8.2.3　匿名访问缺陷……198
8.2.4　访问漏洞……198
8.3　配置安全的 Vsftpd 服务器……198
8.3.1　快速构建 Vsftpd 服务器……198
8.3.2　Vsftpd 配置文件……200
8.3.3　Vsftpd 的设置选项……200
8.3.4　通过 Web 浏览器管理 Vsftpd 服务器……207
8.3.5　分析 Vsftpd 服务器的日志文件……209
8.3.6　使用 BlockHosts 对抗暴力破解……210
8.3.7　在 RHEL 4.0 下安装支持 SSL 的最新版本的 Vsftpd……210
8.3.8　使用 quota 为 ftpuser 加入磁盘限额……211
8.3.9　配置 Linux FTP 服务器 vsftpd 以支持 IPv6……211
8.4　安全使用客户端工具……212
8.4.1　命令行模式……212
8.4.2　图形界面模式（gFTP）……212
8.4.3　使用 Windows FTP 客户端……217
8.5　本章小结……219
第 9 章　Samba 服务器的安全策略……220
9.1　Samba 简介……220
9.1.1　什么是 Samba……220
9.1.2　Samba 的历史起源……221
9.1.3　SMB 协议……221
9.1.4　为什么使用 Samba……222
9.1.5　Samba 软件包的功能……222
9.2　安装配置 Samba 服务器……223
9.2.1　安装 Samba 服务器……223
9.2.2　Samba 配置文件……224
9.2.3　设置 Samba 密码文件……228
9.2.4　启动 Samba 服务器……229
9.2.5　测试 Samba 配置文件……229
9.2.6　在 Windows 环境测试 RHEL 4.0 默认配置……229
9.3　配置 Samba 服务器共享文件及打印机……231
9.3.1　配置文件共享……231
9.3.2　配置共享打印机……232
9.3.3　在 Linux 环境下应用 Samba 服务……234
9.4　其他配置 Samba 的方法和用好 Linux 下的网络邻居……235
9.4.1　图形化配置工具 system-config-samba……235
9.4.2　使用 SWAT 管理工具管理 Samba……237
9.4.3　其他工具……239
9.4.4　用好 Linux 下的网络邻居……240
9.5　Samba 服务器面临的安全隐患……243
9.5.1　非法访问数据……243
9.5.2　计算机病毒……243
9.5.3　Samba 文件服务器的安全级别……243
9.6　提升 Samba 服务器的安全性……245
9.6.1　不要使用明语密码……245
9.6.2　尽量不使用共享级别安全……245
9.6.3　尽量不要浏览器服务访问……245
9.6.4　通过网络接口控制 Samba 访问……245
9.6.5　通过主机名称和 IP 地址列表控制 Samba 访问……245
9.6.6　使用 pam_smb 对 Windows NT/2000 服务器的用户进行验证……246
9.6.7　为 Samba 配置防范病毒软件……247
9.6.8　使用 Iptables 防火墙保护 Samba……248
9.6.9　使用 Gsambad 管理监控 Samba 服务器…248
9.6.10　使用 SSL 加固 Samba……250
9.7　本章小结……251

第 10 章　NFS 服务器的安全策略……252
10.1　NFS 服务器的工作原理……252
10.1.1　NFS 简介……252
10.1.2　为何使用 NFS……253
10.1.3　NFS 协议……253
10.1.4　什么是 RPC（RemoteProcedure Call）……254
10.2　安装配置 NFS 服务器……256
10.2.1　NFS 网络文件的系统结构……257
10.2.2　配置/etc/exports 文件……257
10.2.3　激活服务 portmap 和 nfsd……258
10.2.4　exportfs 命令……258
10.2.5　检验目录/var/lib/nfs/xtab……259
10.2.6　showmount……259
10.2.7　观察激活的端口号……259
10.2.8　NFS 服务器的启动和停止……260
10.3　NFS 的图形化配置……260
10.3.1　NFS 服务器配置窗口……260
10.3.2　添加 NFS 共享……261
10.3.3　常规选项……261
10.3.4　用户访问……262
10.3.5　编辑 NFS 共享……262
10.4　NFS 的客户端配置……263
10.4.1　使用 mount 命令……263
10.4.2　扫描可以使用的 NFS Server 目录……264
10.4.3　卸载 NFS 网络文件系统……264
10.4.4　应用实例……265
10.4.5　其他挂载 NFS 文件系统的方法……265
10.5　NFS 服务器面临的安全隐患……266
10.6　提升 NFS 服务器的安全性……266
10.6.1　使用 tcp_wrappers……266
10.6.2　注意配置文件语法错误……267
10.6.3　使用 Iptables 防火墙……267
10.6.4　把开放目录限制为只读权限……267
10.6.5　禁止对某些目录的访问……268
10.6.6　root Squashing 访问问题……268
10.6.7　使用 nosuid 和 noexec 选项……268
10.6.8　保护 portmap 的安全性……269
10.6.9　保留 ACL……269
10.7　本章小结……270
第 11 章　DHCP 服务器的安全策略……271
11.1　DHCP 服务器的工作原理……271
11.1.1　DHCP 简介……271
11.1.2　为什么使用 DHCP……272
11.1.3　DHCP 的工作流程……272
11.1.4　DHCP 的设计目标……273
11.2　安装 DHCP 服务器……273
11.2.1　DHCP 配置文件……273
11.2.2　配置实例……275
11.2.3　启动 DHCP 服务器……276
11.2.4　设置 DHCP 客户端……278
11.3　DHCP 服务器的故障排除……280
11.3.1　客户端无法获取 IP 地址……280
11.3.2　DHCP 客户端程序和 DHCP 服务器不兼容……280
11.4　提升 DHCP 服务器的安全性……281
11.4.1　管理监控 DHCP 服务器……281
11.4.2　让 DHCP 服务器在监牢中运行……283
11.4.3　提供备份的 DHCP 设置……285
11.5　本章小结……286
第 12 章　Squid 服务器的安全策略……287
12.1　代理服务器的工作原理……287
12.1.1　各种代理服务器的比较……287
12.1.2　Squid 工作原理和流程图……288
12.1.3　代理服务器的优点……289
12.1.4　代理服务器的分类及特点……290
12.2　配置安全的 Squid 代理服务器……291
12.2.1　Squid 的启动……291
12.2.2　Squid 的配置文件……292
12.2.3　Squid 的命令参数……293
12.3　代理服务器面临的安全隐患……295
12.3.1　客户端非法访问不良网站……295
12.3.2　计算机病毒……295

12.4 提升 Squid 代理服务器的安全性 ……296
12.4.1 控制对客户端访问 ……296
12.4.2 管理代理服务器端口 ……297
12.4.3 使用用户认证 ……298
12.5 全面监控 Squid 代理服务器的运行 ……299
12.6 关注 Squid 代理服务器的日志 ……304
12.6.1 Squid 日志格式 ……304
12.6.2 分析 access.log 日志文件 ……304
12.6.3 使用 Linux 命令 ……305
12.6.4 使用专业软件分析 ……305
12.7 为 Squid 代理服务器串联 HAVP ……309
12.8 本章小结 ……311
第 13 章 SSH 服务器的安全策略 ……312
13.1 SSH 服务器的工作原理 ……312
13.1.1 传统远程登录的安全隐患 ……312
13.1.2 SSH 能保护什么 ……313
13.1.3 SSH 服务器和客户端工作流程 ……313
13.2 安装配置 OpenSSH 服务器 ……314
13.2.1 安装与启动 OpenSSH ……314
13.2.2 配置文件 ……315
13.3 SSH 服务器面临的安全隐患 ……318
13.3.1 软件漏洞 ……318
13.3.2 口令暴力破解 ……318
13.3.3 SSH 所不能防范的网络攻击 ……318
13.3.4 OpenSSH 中可能安放有特洛伊木马 ……319
13.4 提升 SSH 服务器的安全性 ……319
13.4.1 升级旧版本 ……319
13.4.2 使用 xinetd 模式运行 OpenSSH ……319
13.4.3 使用 BlockHosts 对抗暴力破解 ……320
13.4.4 使用 TCP 会绕程序 ……320
13.4.5 管理 SSH 监听端口 ……322
13.4.6 关闭 Telnet 服务 ……322
13.4.7 禁止 root 用户登录 SSH 服务器 ……323
13.4.8 启用防火墙保护 OpenSSH 服务器 ……323
13.4.9 使用 Protocol 2 ……323
13.4.10 不使用 r 系列命令 ……323
13.4.11 修改配置文件 ……323
13.5 如何安全应用 SSH 客户端 ……325
13.5.1 安全应用 Linux 下的 SSH 客户端 ……325
13.5.2 生成密钥对 ……329
13.5.3 命令测试 ……331
13.5.4 使用 Windows SSH 客户端登录 OpenSSH 服务器 ……333
13.6 本章小结 ……338
第 14 章 Linux 防火墙 ……339
14.1 防火墙简介 ……339
14.1.1 什么是防火墙 ……339
14.1.2 防火墙的功能 ……339
14.1.3 防火墙技术分类 ……340
14.2 Linux 防火墙 ……342
14.2.1 Linux 防火墙的历史 ……342
14.2.2 Netfilter/Iptables 系统是如何工作的 ……343
14.2.3 Iptables 的基础 ……345
14.2.4 建立规则和链 ……351
14.3 Iptables 配置实战 ……355
14.3.1 初试化配置方案 ……356
14.3.2 Web 服务器设置 ……356
14.3.3 DNS 服务器设置 ……356
14.3.4 邮件服务器 Sendmail 设置 ……356
14.3.5 不回应 ICMP 封包 ……356
14.3.6 防止 IP Spoofing ……357
14.3.7 防止网络扫描 ……357
14.3.8 允许管理员以 SSH 方式连接到防火墙修改设定 ……357
14.3.9 快速构架 Linux 个人防火墙 ……357
14.4 升级 Iptables 控制 BT ……362
14.4.1 P2P 应用现状 ……362
14.4.2 下载软件 ……362
14.4.3 安装 ……363
14.4.4 测试 ……363
14.4.5 使用 ……364
14.5 本章小结 ……364
第 15 章 Linux 网络环境下的 VPN 构建 ……366
15.1 VPN 概述 ……366

15.1.1 VPN 定义……366
15.1.2 VPN 的功能……367
15.1.3 VPN 的分类……367
15.1.4 VPN 的隧道协议……369
15.2 Linux 下的主要 VPN 技术……370
15.2.1 IPSec（Internet Protocol Security）……370
15.2.2 PPP OVER SSH……370
15.2.3 CIPE（Crypto IP Encapsulation）……371
15.2.4 PPTP……371
15.3 构建基于 CIPE 技术的 Linux VPN……371
15.3.1 CIPE 概述……371
15.3.2 使用 Red Hat Linux 的网络管理工具来配置 CIPE VPN……372
15.3.3 通过配置文件配置 CIPE VPN……376
15.4 构建基于 PPTP 技术的 Linux VPN……380
15.4.1 PPTP 以及 Poptop 简介……380
15.4.2 PPP 简介……381
15.4.3 在 Linux2.4 内核下安装配置 PPTP 服务器……381
15.4.4 在 Linux2.6 内核下安装配置 PPTP 服务器……386
15.4.5 Linux 下 PPTP 客户端连接 VPN 服务器……387
15.5 构建基于 SSH VNC 技术的 Linux VPN……390
15.5.1 VNC 技术概述……390
15.5.2 使用 NHC+SSH 建立 Linux 和 Windows 的安全隧道……391
15.5.3 使用 SSHTools 实现 Linux 下远程 VPN 办公……393
15.5.4 VNC 服务器维护技巧……398
15.6 构建基于 IPSec 技术的 Linux VPN……400
15.6.1 IPSec 及 IKE 简介……400
15.6.2 在 RHEL 4.0 配置 IPSec……401
15.7 本章小结……404
第 16 章 使用 IDS 保护 Linux 服务器……405
16.1 什么是 IDS……405
16.1.1 IDS 定义……405
16.1.2 IDS 的工作流程……405
16.1.3 IDS 部署的位置……406
16.1.4 IDS 的功能……407
16.1.5 IDS（入侵检测系统）模型……407
16.1.6 IDS 分类……408
16.2 Linux 下配置基于主机的 IDS……408
16.2.1 RPM 包管理器作为一种 IDS……408
16.2.2 其他基于主机的 IDS……410
16.2.3 安装配置 Tripwire……410
16.3 Linux 下配置基于网络的 IDS……412
16.3.1 什么是基于网络的 IDS……412
16.3.2 Snort 简介……413
16.4 Snort 的安装配置……414
16.4.1 配置 IDS 的网络拓扑结构……415
16.4.2 安装 Snort……416
16.4.3 建立 Snort 数据库……416
16.4.4 安装配置 ACID……416
16.4.5 配置 Apache 服务器用户认证……417
16.4.6 建立 Snort 规则……417
16.4.7 启动 Apache 和 MySQL 服务进程……418
16.4.8 为 Snort 创建专用的用户和组来启动 Snort……418
16.4.9 使用 Web 浏览器监控 Snort……419
16.5 建立分布式 Snort 入侵检测系统……419
16.5.1 安装 SnortCenter3……419
16.5.2 修改配置文件……420
16.5.3 snortcenter-agent 下载配置步骤……420
16.5.4 完成配置……420
16.6 本章小结……422
第 17 章 Linux 网络监控策略……423
17.1 安装配置 MRTG 监控 Linux 网络……423
17.1.1 SNMP 简介和 MRTG 监控过程……423
17.1.2 Linux 下 MRTG 的安装与配置……424
17.1.3 建立 MRTG 监控中心……426
17.1.4 MRTG 软件的不足和 RRDTool 的对比……426
17.2 安装配置 NTOP 监控 Linux 网络……427

17.2.1 P2P 对于网络流量提出挑战……427
17.2.2 NTOP 的安装……430
17.2.3 软件使用方法……432
17.3 NTOP 的安全策略……438
17.3.1 经常查看 NTOP 的进程和日志……439
17.3.2 进行 Web 访问认证……439
17.3.3 加密连接 NTOP……440
17.3.4 NTOP 使用技巧和总结……441
17.4 本章小结……443
第 18 章 Linux 常用安全工具……444
18.1 使用 SAINT 执行安全审核……444
18.1.1 什么是 SAINT……444
18.1.2 工作模式……445
18.1.3 安装 SAINT……445
18.1.4 SAINT 设置……446
18.1.5 启动 SAINT……447
18.2 使用端口扫描软件 Nmap……451
18.2.1 Nmap 简介……451
18.2.2 使用 Nmap……452
18.2.3 nmap 命令实例……452
18.2.4 Nmap 图形前端……454
18.2.5 Nmap 使用注意事项……455
18.3 使用网络数据采集分析工具 Tcpdump……455
18.3.1 Tcpdump 简介……455
18.3.2 Tcpdump 的安装……456
18.3.3 Tcpdump 的命令行选项……456
18.3.4 Tcpdump 的过滤表达式……457
18.3.5 Tcpdump 过滤数据包实例……458
18.3.6 Tcpdump 的输出结果……458
18.4 使用 Ethereal 分析网络数据……460
18.4.1 Ethereal 简介……460
18.4.2 安装 Ethereal……460
18.4.3 使用 Ethereal……461
18.5 使用 EtherApe 分析网络流量……465
18.5.1 EtherApe 简介……465
18.5.2 EtherApe 软件下载安装……465
18.5.3 EtherApe 软件使用方法……466
18.6 使用 GnuPGP 进行数据加密……468
18.6.1 GnuPGP 简介……468
18.6.2 GnuPGP 安装……468
18.6.3 生成密钥……468
18.6.4 查看密钥……469
18.6.5 公钥的使用……469
18.6.6 GnuPGP 应用实例（软件包签名验证）……470
18.6.7 GnuPGP 应用实例（在 Mutt 中使用 GnuPG）……470
18.7 其他安全工具简介……470
18.7.1 密码分析工具 John the ripper……471
18.7.2 系统管理工具 sudo……471
18.7.3 开放源代码风险评估工具 Nessus……471
18.7.4 网络瑞士军刀 Netcat……471
18.7.5 网络探测工具 Hping2……471
18.7.6 列出打开的文件命令工具 LSOF……471
18.7.7 强大的无线嗅探器 Kismet……471
18.7.8 802.11 WEP 密码破解工具 AirSnort……472
18.7.9 安全管理员的辅助工具 SARA……472
18.7.10 高级的 traceroute 工具 Firewalk……472
18.7.11 主动操作系统指纹识别工具 XProbe2……472
18.8 本章小结……472
第 19 章 防范嗅探器攻击和 Linux 病毒……473
19.1 防范嗅探器攻击……473
19.1.1 嗅探器攻击原理……473
19.1.2 嗅探器的检测技术……475
19.1.3 嗅探器的安全防范……475
19.2 Linux 病毒的防范……477
19.2.1 Linux 病毒的历史……477
19.2.2 Linux 平台下的病毒分类……478
19.2.3 Linux 病毒的防治……479
19.2.4 Linux 防病毒软件……480
19.2.5 安装配置 f-prot 反病毒软件……480
19.3 本章小结……490
第 20 章 Linux 数据备份恢复技术……491
20.1 Linux 备份恢复基础……491