实用技术：
Linux安全最大化

Maximum Linux Security

〔美〕Anonymous（佚名） 著
王 泓 路晓村 王景中 等译
薛荣华 审校

Surfing
Linux World

SAMS

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

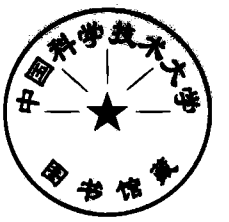
实用技术:Linux 安全最大化

Maximum Linux Security

[美] Anonymous(佚名) 著

王 泓 路晓村 王景中 等译

薛荣华 审校



電子工業出版社

Publishing House of Electronics Industry

北京·BEIJING

内 容 提 要

Linux 是一个十分稳定的操作系统，目前用户已逾千万。但是，Linux 是否安全？这对 Linux 的新用户来说是十分关心的问题。本书的目的就是要说明 Linux 是安全的。全书包括五大部分：Linux 安全基础；Linux 用户安全；Linux 网络安全；Linux Internet 安全；附录。本书全面介绍了实现 Linux 安全保障的内容，附带的光盘上还提供了大量的 Linux 安全工具和联机参考资料以及众多的信息来源，使你能够更好地驾驭 Linux 系统的安全问题。

读者对象：计算机系统管理人员、网络系统管理人员、广大 Linux 用户、大专院校计算机专业师生。

图书在版编目(CIP)数据

实用技术：Linux 安全最大化/(美)佚名著；王泓等译. -北京：电子工业出版社，2000.5

书名原文：Maximum Linux Security

ISBN 7-5053-5948-7

Ⅰ.实… Ⅱ.①佚…②王… Ⅲ.Linux 操作系统-安全技术 Ⅳ.TP316.89

中国版本图书馆 CIP 数据核字(2000)第 09484 号

书　　名：**实用技术：Linux 安全最大化**
原 书 名：Maximum Linux Security
著　　者：[美]Anonymous(佚名)
译　　者：王　泓　路晓村　王景中　等
审 校 者：薛荣华
责任编辑：周宏敏
特约编辑：屈　健
排版制作：电子工业出版社计算机排版室监制
印 刷 者：北京天竺颖华印刷厂
出版发行：电子工业出版社　URL：http://www.phei.com.cn
　　北京市海淀区万寿路 173 信箱　邮编 100036
经　　销：各地新华书店
开　　本：787×1092　1/16　印张：35.25 字数：902 千字
版　　次：2000 年 5 月第 1 版　2000 年 5 月第 1 次印刷
书　　号：ISBN 7-5053-5948-7 / TP·3113
印　　数：6000 册　定价：69.00 元(含光盘)
版权贸易合同登记号　图字：01-1999-3786

译者的话

自1991年一个免费的操作系统Linux发布以来，由于其公开源代码、与UNIX十分相似、稳定性好、具有丰富的开发工具、特别适合网络应用等许多突出的特性，故其发展极为迅速，目前已有近千万用户。但是，Linux是否安全？这一直是系统管理员最关心的问题。本书就是论述Linux安全问题的专著。要使自己的系统安全，首先要了解黑客们及恶意破坏系统的攻击者们是如何闯入系统的、使用什么工具和手段入侵你的系统，才能有目的地找出系统中的漏洞和易受攻击之处，并采取适当的防范措施。本书作者曾是一位黑客，有丰富的黑客经验，了解攻击系统的各种方法和工具。这对于想保护自己系统安全的系统管理员来说是十分宝贵的。

本书论述Linux系统全面的安全问题，共分五大部分。第一部分是Linux安全基础，包括物理安全、安装问题和基本Linux系统管理。第二部分是Linux用户安全，包括口令安全和恶意代码。第三部分是Linux网络安全，包括网络嗅探和电子窃听、扫描器以及如何保护传输中的数据。第四部分是Linux因特网安全，介绍因特网上的各种服务的安全问题、防火墙、日志、入侵检测及灾难恢复等。第五部分是附录，列举了各种Linux安全命令，总结了过去的Linux安全问题并介绍许多有用的Linux安全工具以及丰富的Linux安全信息来源。本书是一本极为珍贵的Linux系统安全资料，对Linux系统管理员和一般的计算机系统和网络管理员来说均有极高的使用价值，即使你的系统使用其他操作系统，书中论述的内容也有参考价值。

本书由路晓村(第一部分)、王景中(第二部分)、刘娟(第三部分)、王泓(第四部分)和闫慧娟(第五部分)翻译，由薛荣华审校和统稿。参加本书译、录、校工作并给予大力协助的还有徐小青、陈立志、徐亮、王畅、雪山、于秀山、矫克民、严丹青、郭思佳、石垣、刘波涛、申明、薛飞、孔浩然、曹汉、童彤、张巧英、方绛、蒋文静、锺良知、于宾等同志。电子工业出版社外版书编辑部的编辑们为此书的出版做了大量艰苦细致的工作，译者谨向他们表示衷心感谢！

译　者

作者简介

Anonymous(佚名)是一位Linux和Perl语言程序员，他与妻子Michelle及6台计算机共同生活在南加州。目前他经营着一家因特网安全顾问公司，并承担了为数家《财富》全球500强公司编程的合同。他最近所做的项目是为数家注册会计师事务所设计的基于Linux系统的交钥匙(turn-key)防火墙系统。

谨以此书献给 Rosemarie

致　谢

本书的出版离不开以下人士的帮助：Michael Michaleczko、Alex Brittain、John Sale、Marty Rush、Lloyd Reese、David Pennells 和 David Fugate。

此外，衷心地感谢工作卓越的编辑人员，他们是：Mark Taber、Scott Meyers、Randi Roger、John Ray、Christopher Blizzard、Billy Barron、Sean Medlock、Karen Walsh、Rebecca Mounts、Mary Ellen Stephenson 和 Dan Scherf。

请告诉我们您的想法

作为本书的读者，您是我们最重要的批评家和评论家。我们十分珍视你的意见，希望知道自己哪些地方做得对，哪些地方可以做得更好，还希望我们出版哪些图书以及其他可以转告给我们的忠告。

你可以直接通过传真、电子邮件和信函，让我们知道你对本书的观点和意见，以便使我们能够把图书做得更好。

请读者注意我不能帮助你解决本书涉及的技术问题，此外因为收到的邮件数量很大，可能不能回答每一封来信。

在你的信件中一定注明本书的书名和作者名以及你的名字和电话或传真号码。我一定会认真考虑你的意见，并把它们转达给本书的作者和编辑。

传真：317-518-4770

电子信箱：webdev _ sams@mcp.com

地址：Mark Taber

Associate Publisher

Sams Publishing

201 West 103rd Street

Indianapolis, IN 46290 USA

前　言

大多数有关安全的图书的销量适中，然而《Maximum Security II》的成功使人感到惊讶。使我感到最惊讶的是收到的读者反馈信息数量之多。读者们不但需要这些素材，而且还希望得到更多的资料。正是这些原因使得我感到应该再写一部此类书籍。

我在和编辑讨论此书时，他们反复提到这样的观点，即许多读者都认为《Maximum Security II》很好，然而能不能集中讨论具体的一个操作系统？我认为原则上讲这是一个好主意，但是问题是：我们讨论哪个操作系统？最后我们选择了 Linux，这里我可以说一下选择它的理由。

多年来 Linux 可以说是一匹黑马，对于反崇拜的人们来说，它是替代微软产品的选择。在产品推出的初期，Linux 的处境还很孤单。我记得和一些抱怨他们使用的操作系统存在问题的朋友们讨论过这些问题。他们没有源代码，他们抱怨支付了高额的开发工具等费用。这时我总是提供同一建议：采用 Linux。然而，他们总是对此犹犹豫豫，还提出了许多各种不愿意使用的理由（缺少技术支持是第一位的）。

现在，我收到这些朋友们的电话都是向我介绍使用 Linux 的最新经验。有些人已经学习过 Perl，而另一些人已经十分熟悉 Expect 编程技术了。时代可能发生了变化。作为一种桥梁，Linux 已经有了长足的进步，它已经成熟了。即使某个系统已经向黑客们公开，但是 Linux 还是天天都被安装到公司的环境里。

从 Linux 的成长历史可以看出它的发展过程。长期以来 Linux 已经被证明十分稳定且值得一用。事实上，现在已经几乎没有障碍能够妨碍在各类任务的关键服务器上安装 Linux 了。

当然还有一种障碍，常常在一些技术会议上被集中提出来：Linux 安全。每当客户提出这样的问题时，例如“Linux 真的安全吗？”，“比 NT 还要安全吗？”，“我们都十分了解 NT”，我都尽自己所能进行解释。可能最常见到的抱怨就是找不到十分简单地讨论 Linux 安全的书籍。

总之，我撰写《实用技术：Linux 安全最大化》这部专著的目的就是要说明 Linux 是安全的，我能够提供有关 Linux 安全的资料。我希望本书达到了这个目的。

本书的组织

通过几本书的撰写，我已经掌握了书的组织结构方面的技术。根据这些要领，我又检验了以前的几本专著，发现了很多缺点，造成读者不能快速地找到重要资料。为了防止这种情况的再次发生，我运用新的方法来撰写本书。

在《实用技术：Linux 安全最大化》一书中，特别加入了交叉参考的方法，因而使得本书的资源更具使用价值。这种交叉参考毫无疑问地使得本书也能更好地标引出关键问题，而它们在其他类似图书中往往会被忽略。

事实上，本书最具价值的是如何组织这种交叉参考。下面我简单地介绍一下这种方法。

如何使用本书的交叉参考

一些图书的著者往往对自己撰写书籍的某些优点感到自豪。例如，假设有一本书的书名叫做《NT 最高安全技术》，我可以很快把它写完，向那些已经有多年经验(但不是 NT 的经验，也许是在 Windows 3、3.1、3.11、95 和 98 上面的经验)的 Windows NT 用户介绍很多知识。的确我的读者可以很快地理解和掌握书中的每一项建议和技巧。

但是本书的情况独特。虽然 Linux 的用户已经达到千万，但是他们中的大多数人使用 Linux 的时间还不到一年。实际上，很多人是刚刚才掌握它的。此外，虽然通过联机方式也可以获得完整的有关 Linux 安全的文档，但是专门讨论有关这方面内容的图书几乎没有。这和 Windows NT 的情况产生鲜明对照。

此外，很多 Linux 安全的应用程序都是基于命令行模式产生若干文件的。这样你常常需要熟悉文件的不同配置和执行单一任务的命令。这种情况使得 Linux 和其他 GUI 模式的操作系统不同。

为了说明它们的区别，我编辑了一个假定的 Windows 安全应用程序，名字叫 Acme Ace 防火墙工具，可以参阅图 1.1。

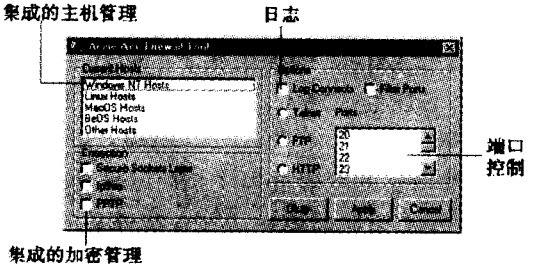


图 I.1　Acme Ace 防火墙工具

注意 Acme Ace 把所有的安全功能集中到一个清晰的界面上。从这个界面上，你可以：

- 管理主机
- 管理日志
- 使用过滤器和加密

这种方式是很常见的。但是它是静态的，你不能够超越程序员划出的范围，另外它只能局限在窗口系统中。Linux 安全工具是唯一的例外，它的工作方式不同。

Linux 开发商们常常把一些基本功能分割成独立的命令或文件，或命令和文件。最好的例子可以算是 tcpd 系统，它可以让你接受或拒绝接受来自特定主机或主机层次上的网络连接。为了能够熟练地使用 tcpd，你必须先熟悉以下一些命令和文件：

- /etc/hosts.allow——主机访问规则表
- /etc/hosts.deny——主机拒绝访问规则表
- hosts_access——建立访问规则的系统和语言
- hosts_options——hosts_access 的扩展

- tcpd——TCP 的守护程序
- tcpdchk——核实 tcpd 中心配置的工具
- tcpdmatch——以交互方式说明你的规则的工具

这些规则对于第一次使用 Linux 的用户来说是难以理解的。他们可能失去信心，不相信自己能够正确地配置好所有的命令和文件。可以理解为什么 Linux 有难以配置的操作系统的名声。

最后，Linux 遵循的公理对于 Perl 的程序员来说是极为熟悉的："可以有不止一个办法实现某个目标"。Linux 常常有几条命令具有相同(或本质上相同)的功能。

本人撰写该书的主要目的是全面阐述 Linux 安全的思想，特别是对于新用户。为了实现这个目标，我需要使用一种能够明确说明和交叉参考以下内容的方法。

- 必须协同使用的命令和文件组；
- 可以执行类似任务的命令组。

我把一些内容放到一起，叫做集群。利用图表来找出需要的命令和文件以及相关或类似的工具。这样便形成了一种与上下文有关连的交叉参考层次，这在其他技术图书中是很少见的。让我们看一下下面这个例子。

第 4 章"基本 Linux 系统管理"包含了系统的基本管理任务，例如：增加和删除用户等。你可以使用一种工具来实现这个目的，即 usercfg。usercfg 集群可以提供对此类工具的基本总结：

应用程序：usercfg

要求：usercfg + python

配置文件：/usr/lib/rhs/control-panel/usercfg. init，/usr/lib/rhs/usercfg，/usr/lib/rhs/usercfg/usercfg.py，/usr/lib/rhs/usercfg/usercfg.pyc

安全历史：传统的安全漏洞(1996 年公开的 python 类漏洞)是允许攻击者获得对/etc/shadow 文件的读访问。它的利用可以参阅：http://safenetworks. com/Linux/shadow. html。

说明：usercfg 是一种独立式账户管理工具，但是在使用过程中，你必须掌握 python 语言和它的程序库(如果你使用的是完全安装，就不应该出现问题。如果你是有选择地使用开发工具，没有选中 usercfg，也没有选中 python，应该立即进行安装)。usercfg 放在/usr/bin 目录下(注意，usercfg 的图形界面可能有些不同，在有些情况下，它是 X 方式，有时它还可以通过一个 shell 在 LISA 对话驱动中运行或从命令提示符下运行)。

新用户可以从中获利，因为他们可以很快地见到不同命令或文件之间的关系。在主要工具和许多独立的配置文件有关联时，这一点特别重要，例如 tcpd 的情况。

但是这还不是全部。这种双向的、根据内容的交叉参考(即使没有集群图)在本书中处处可见。在讨论一种工具时，只要可能，我就会交叉参考本书其他章节中出现的类似的或有关联的工具。这种相关查找不但能简单地标出有关的章节，指出页数，而且还能补充联机信息。

下面是在附录 A："Linux 安全命令参考"中的一个实例。

amadmin

说明：控制 Amanda 备份的管理界面。

安全问题：使用 amadmin 可以配置 amanda 备份系统。详细内容参阅本书第 21 章"灾难

恢复"和本附录中的 amanda、amcheck 和 amcleanup 以及 amadmin 手册页或者 http://www.cs.umd.edu/projects/amanda/amanda.html。

这种双重参考方法可以充实本书的内容,使你可以很快地找到更为详实的资料。

如何使用本书

为了读懂本书中的实例,你还需要具备以下条件:

- Linux(包括 Craftworks, Debian, Delix DLD, Eagle Group, Eurielec, Kheops, Linux Universe, MNIS, OpenLinux, Red Hat, S.U.S.E, SlackWare, Stampede Linux, TransAmeritech, TurboLinux, Yggdrasil 等等)。
- 完全安装,包括标准的 TCP/IP 客户和服务器系统,C 和 Perl 等。

注释 这些实例可能是 Linux 专用版本,也可能是应用程序版本。例如,有些工具需要使用最新的 Perl 版本,有些则要求使用 gtk,还有些要求支持 a.out,当然大多数要求支持 ELF (Executable and Linking Format)格式。你最好能够安装近期销售的 Linux 版本,以便满足这些要求(有些实例是使用 Caldera OpenLinux 1.3 和 Red Hat Linux 5.1 版本生成的)。

因特网连接的要求一般不严格。但是有许多实例是使用一台连网机器在本地的 Web 服务器上反复实验的。然而,我特别建议你至少使用企业内联网。还有些实例,例如试验防火墙规则等要求使用多种设备。

毫无例外这些实例没有不使用专用工具就能获得安全的,这些专用工具常常包含在商业版的 Linux 中。我使用这种方法是要保证这些材料能够和所有的 Linux 版本相近。此外,这种方法将保证新用户不但能理解怎样实现这些安全方法,而且还能知道它们是如何工作的。

最后,我在撰写本书时的目的是鉴于大多数读者掌握的知识能够安装和使用 Linux,但是他们却具备很少,甚至没有安全方面的经验。对于经验丰富的用户可以试一下他们的耐心,但是我希望本书对他们也有利。

其他

最后还有一些需要说明:

- 链接与主页。在前几本书中,我是直接和二进制文件链接,常常略去销售商或作者的主页。在本书中,我采取了不同的方式。如果有销售商要求你在下载需要的工具前应该先注册,我可以提供注册用的 URL。另外,当我和一位软件作者的主页链接时,我只是链接这个页面,而不是具体的文件。我认为这样做是公平的,因为这些人总是说在他们的站点上面有一些有价值的工具或资料。但是他们常常改变文件名,特别是文件进行更新之后。例如地址 http://www.mysite.org/mytool.tgz 后来可能会换成 http://www.mysite.org/mytool. version2.tgz。在采用这些新方法时,我希望避免出现过多的 404 错误。

在大多数情况下，我的确提供了很多新发现的 URL。这样做可以节省你的时间。例如，当我提到一种工具时，不会简单地建议你访问销售商的主页。而是建议你链接到可以下载这种工具的页面上，这样做避免你再花费寻找的时间。

注释 这个原则有时也有例外，有些站点是通过 CGI 快速生成 URL 的。因为这些 URL 是动态的（经常取决于 Web 客户所在的州名和地址等信息），他们是不可靠的。针对这种情况，我总是在可能的情况下引用静态的 URL。

- 关于在本书中提到的产品。在本书中我会提到很多产品（有些属于商业产品，有些则不是），我不是这些产品的分销商。如果我提到一种工具，纯粹是因为使用的实例是用这种工具生成的。可以说，我十分感谢开发商能够对他们的产品提供技术支持。对于他们的帮助我万分感谢。
- 错误。如果你发现本书提到的产品存在某种错误，请与 Sams 出版公司联系。

小结

至此，我希望你能够从本书中获益，认为这是一部好书。虽然本书不能认为已经尽善尽美，然而它能够包含基本的 Linux 安全任务的内容。此外，通过本书附带的 CD-ROM 和提供的许多联机参考可以为你提供不可多得的工具和额外的信息源。这些优点可以使得你能够更好地驾驭你的 Linux 系统的安全问题。

请把你的建议和意见发给：maxlinsec@altavista.net。

目　录

第一部分　Linux 安全基础

第 1 章　Linux 概述 …… (3)
1.1　什么是 Linux …… (3)
1.2　Linux 是一个独立的系统 …… (6)
1.3　Linux 作为企业内联网(Intranet)/因特网服务器 …… (7)
1.4　Linux 安全评价 …… (8)
1.5　小结 …… (14)
第 2 章　物理安全 …… (15)
2.1　服务器位置和物理接触 …… (15)
2.2　网络拓扑结构 …… (17)
2.3　网络硬件 …… (21)
2.4　工作站和安全 …… (23)
2.5　小结 …… (33)
第 3 章　安装问题 …… (34)
3.1　有关不同的 Linux 版本、安全性及安装方法 …… (34)
3.2　分区与安全 …… (36)
3.3　安装时选择网络服务软件 …… (53)
3.4　引导装载器 …… (54)
3.5　小结 …… (57)
第 4 章　基本 Linux 系统管理 …… (58)
4.1　基本概念 …… (58)
4.2　创建和管理账号 …… (59)
4.3　使用 su 执行管理任务 …… (68)
4.4　访问控制 …… (70)
4.5　许可与拥有 …… (70)
4.6　进一步了解组 …… (80)
4.7　关闭系统 …… (84)
4.8　小结 …… (85)

第二部分　Linux 用户安全

第 5 章　口令攻击 …… (89)
5.1　什么是口令攻击 …… (89)
5.2　Linux 如何产生和保存口令 …… (89)
5.3　数据加密标准(DES) …… (92)

5.4 案例研究:通过字典攻击对 Linux 口令解密 …… (94)
5.5 口令影像和 shadow 套件 …… (103)
5.6 安装完 shadow 套件之后 …… (115)
5.7 其他口令安全问题 …… (119)
5.8 可插入认证模块 …… (121)
5.9 其他口令安全解决方案 …… (122)
5.10 小结 …… (124)
第 6 章 恶意代码 …… (126)
6.1 什么是恶意代码 …… (126)
6.2 检测恶意代码 …… (130)
6.3 其他文件完整性检测软件 …… (141)
6.4 小结 …… (144)

第三部分 Linux 网络安全

第 7 章 嗅探器和电子窃听 …… (147)
7.1 嗅探程序的工作方式 …… (147)
7.2 案例分析:执行一些简单的嗅探攻击 …… (149)
7.3 其他嗅探软件和网络监听工具 …… (165)
7.4 嗅探所引起的风险 …… (167)
7.5 嗅探器攻击的防范 …… (168)
7.6 进一步阅读 …… (171)
7.7 小结 …… (172)
第 8 章 扫描器 …… (173)
8.1 扫描器简介 …… (173)
8.2 扫描器构成及其发展 …… (180)
8.3 扫描器为什么适用于系统的安全 …… (188)
8.4 不同的扫描器工具 …… (189)
8.5 防范扫描器攻击 …… (204)
8.6 一些令人感兴趣的资源 …… (209)
8.7 小结 …… (210)
第 9 章 电子欺骗 …… (211)
9.1 电子欺骗简介 …… (211)
9.2 TCP 和 IP 欺骗 …… (211)
9.3 案例研究:一个简单的欺骗攻击 …… (213)
9.4 阻止 IP 欺骗攻击 …… (217)
9.5 ARP 欺骗 …… (218)
9.6 DNS 欺骗 …… (220)
9.7 其他奇怪的欺骗攻击 …… (221)
9.8 进一步阅读 …… (223)

9.9 小结 …… (224)
第 10 章 保护传输中的数据 …… (225)
10.1 Secure Shell(ssh) …… (225)
10.2 scp:Secure Copy 远程文件安全拷贝程序 …… (238)
10.3 在不同类型的网络中提供 ssh 服务 …… (238)
10.4 ssh 的安全问题 …… (246)
10.5 附加资源 …… (246)
10.6 小结 …… (247)

第四部分 Linux 的 Internet 安全

第 11 章 FTP 安全 …… (251)
11.1 文件传输协议 …… (251)
11.2 FTP 默认的安全性能 …… (253)
11.3 SSLftp …… (258)
11.4 特定 FTP 应用的安全 …… (259)
11.5 小结 …… (260)
第 12 章 电子邮件安全 …… (261)
12.1 SMTP 服务器和客户 …… (261)
12.2 sendmail 安全基础 …… (267)
12.3 用 Qmail 替代 sendmail …… (279)
12.4 小结 …… (283)
第 13 章 Telnet 安全 …… (284)
13.1 评定 Telnet 服务的需求 …… (284)
13.2 Telnet 的安全历史 …… (284)
13.3 安全 Telnet 系统 …… (286)
13.4 deslogin …… (286)
13.5 来自得克萨斯农业与机械大学的 SRA Telnet …… (291)
13.6 斯坦福的 SRP Telnet/FTP 包 …… (292)
13.7 小结 …… (293)
第 14 章 Web 服务器安全 …… (294)
14.1 去除不必要的服务 …… (294)
14.2 Web 服务器的安全 …… (300)
14.3 用基本 HTTP 认证增加目录访问控制 …… (309)
14.4 基本 HTTP 认证的弱点 …… (314)
14.5 HTTP 和加密认证 …… (315)
14.6 运行 chroot Web 环境 …… (316)
14.7 授权和证书 …… (317)
14.8 小结 …… (319)
第 15 章 安全 Web 协议 …… (320)

15.1 问题……(320)
15.2 来自 Netscape Communications 公司的安全套接层(SSL)……(320)
15.3 安装 Apache-SSL ……(323)
15.4 其他安全协议:IPSEC ……(339)
15.5 小结……(339)
第 16 章 安全 Web 开发……(340)
16.1 开发风险因素概述……(340)
16.2 产生 Shell ……(340)
16.3 缓存溢出……(347)
16.4 路径、目录和文件 ……(350)
16.5 其他安全程序和测试工具……(352)
16.6 其他在线资源……(353)
16.7 小结……(354)
第 17 章 拒绝服务攻击 ……(355)
17.1 什么是拒绝服务攻击……(356)
17.2 拒绝服务攻击带来的危险……(356)
17.3 本章如何组织……(357)
17.4 网络硬件 DoS 攻击 ……(357)
17.5 对 Linux 网络的攻击……(360)
17.6 对 Linux 应用的攻击……(370)
17.7 其他 DoS 攻击 ……(373)
17.8 防范拒绝服务攻击……(375)
17.9 在线资源……(376)
17.10 小结 ……(376)
第 18 章 Linux 和防火墙 ……(378)
18.1 什么是防火墙……(378)
18.2 你是否真的需要防火墙……(380)
18.3 tcpd: TCP Wrappers ……(381)
18.4 ipfwadm ……(386)
18.5 ipchains ……(389)
18.6 Linux 免费防火墙工具 ……(390)
18.7 商用防火墙……(391)
18.8 其他资源……(393)
18.9 小结……(394)
第 19 章 日志和审计追踪 ……(395)
19.1 什么是日志……(395)
19.2 Linux 的日志 ……(395)
19.3 其他日志和审计工具……(411)
19.4 小结……(414)

第 20 章　入侵检测 …… (415)
20.1　什么是入侵检测 …… (415)
20.2　入侵检测基本概念 …… (416)
20.3　一些有趣的入侵检测工具 …… (417)
第 21 章　灾难恢复 …… (425)
21.1　什么是灾难恢复 …… (425)
21.2　在建立 Linux 网络前采取的步骤 …… (425)
21.3　选择备份工具 …… (427)
21.4　简单存档：tar 和 Zip 文件和目录 …… (428)
21.5　备份类型和备份策略 …… (431)
21.6　备份包 …… (434)
21.7　其他 …… (435)
21.8　小结 …… (436)

第五部分　附　录

附录 A　Linux 安全命令参考 …… (439)
附录 B　Linux 安全索引——过去的 Linux 安全问题 …… (465)
附录 C　其他有用的 Linux 安全工具 …… (475)
附录 D　更多的信息来源 …… (498)
附录 E　词汇表 …… (522)

第一部分　Linux 安全基础

在这部分中，包括：

第 1 章　Linux 概述
第 2 章　物理安全
第 3 章　安装问题
第 4 章　基本 Linux 系统管理