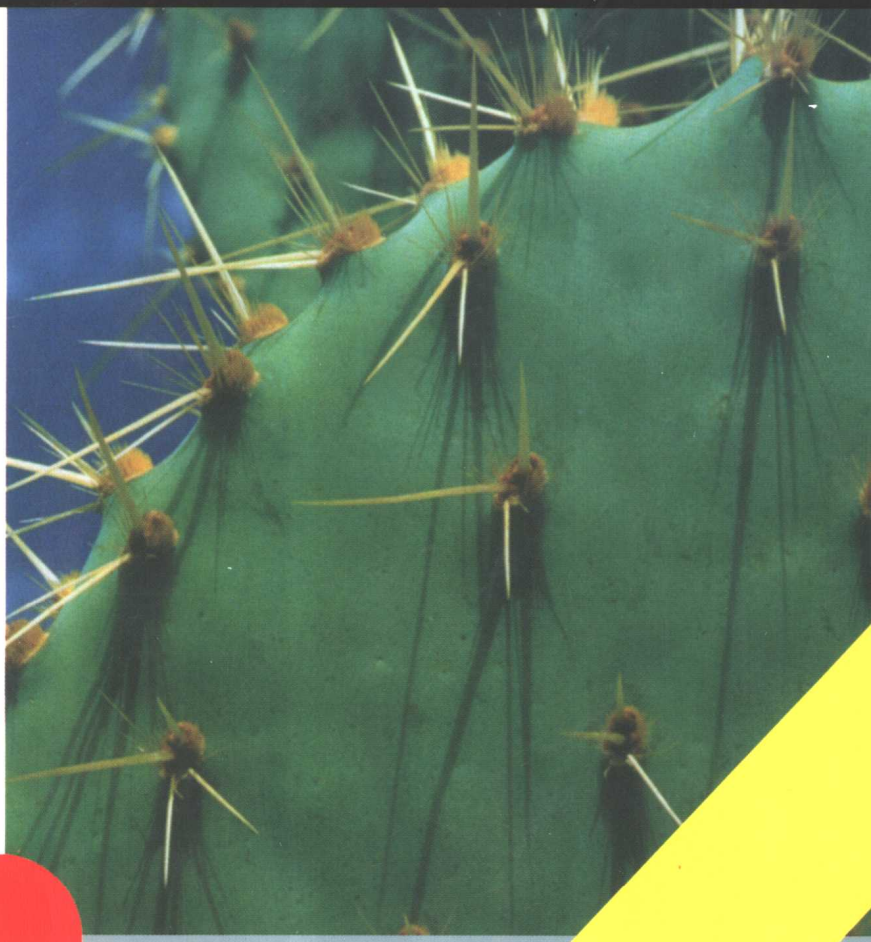
THOMSON
COURSE TECHNOLOGY

Linux
网络与安全指南

Nicholas Wells 编著
张震宇 刘 伟 译



科学出版社
www.sciencep.com

Linux 网络与安全指南

Nicholas Wells 编著

张震宇 刘 伟 译

科学出版社

北 京

图字：01-2003-4432 号

内 容 简 介

本书针对 Red Hat Linux 9.0 版本详细介绍了 Linux 系统的网络安全知识。主要内容包括网络的组建、网络协议和服务，以及网络安全知识。

本书中不乏大量的实例和图表，其中大多数都适用于当前所有 Linux 版本。书中各章后都有数十道精选的、有代表性的习题供读者练习，以巩固所学习的知识，同时提供了几个实验和案例分析，帮助初学者学习。

本书内容完整、实用性强，既可作为本科教材、网络工程技术人员的参考书，又可作为相关认证考试的教材。

图书在版编目(CIP)数据

Linux 网络与安全指南/（美）韦尔斯（Wells，W.）编著；张震宇，刘伟译. —北京：科学出版社，2004.4

ISBN 7-03-013216-5

Ⅰ. L… Ⅱ.①韦…②张…③刘… 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（2004）第 026624 号

策划编辑：李佩乾/责任编辑：朱凤成

责任印制：吕春珉/封面制作：东方人华平面设计部

科学出版社 出版

北京东黄城根北街16号

邮政编码:100717

http://www.sciencep.com

新蕾印刷厂 印刷

科学出版社发行 各地新华书店经销

*

2004 年 4 月第 一 版 开本：787×1092 1/16

2004 年 4 月第一次印刷 印张：29

印数：1—4 000 字数：661 000

定价：48.00 元

（如有印装质量问题，我社负责调换〈环伟〉）

前　言

不知从什么时候开始，在大型机构和实验室中，计算机联网成为大多数人日常工作的一部分。我们和朋友之间经常发送电子邮件、通过全世界范围的金融网络使用信用卡和 ATM 机、在网上做生意；通过许多不同的 Internet 服务寻找最新的影片、天气和体育得分。Linux 成为 Internet 的一部分已经有将近十年的历史了，它为每个主要的 Internet 协议和服务提供低价、稳定的支持。最近，由于许多第三方软件厂家的支持，Linux 正在本地网络中被用作服务器、提供文件和打印服务、数据库、内部网以及其他许多服务。

虽然很多人担心将如此多的信息量放在公开的网络上会有危险，但还是不断出现了这类网络。在全球范围的网络上匿名使用计算机的风险和报纸上不断出现的、可怕的事故，使人们在将自己的财务和个人信息交给这些机器处理之前不得不考虑再三。

然而，信息技术人员正在用 Linux 之类的健壮系统，伴随着适当的安全措施，使得整个 Linux 系统变得日益完善、运行平滑而且非常安全。

Linux 是专业的攻击者以及那些需要不断地屏蔽攻击信件并将其扔到垃圾箱里的二流专家的首选。

本书是一个系列中的第二本，第一本是《Linux 安装和系统管理指南》。要充分学习并利用本书提供的知识，您必须熟练地使用 Linux，首先要安装 Linux，然后还需要有使用 Linux 图形环境运行程序的经验，最好是能养成习惯用 Linux 命令行查询、使用常用系统工具、管理用户号以及 Linux 文件系统。在此基础上，本书将介绍基础的网络知识，尤其是 Linux 网络以及网络安全。其中列举的素材不仅可以使您能顺利通过 Linux 资格考试，还可以使您熟练地掌握基于 Linux 网络安全的重要理论和实践知识。

如今有很多 Linux 的认证程序。本书及其姐妹篇——《Linux 安装和系统管理指南》，为您通过 SAIR/GNU Linux 认证管理员（LCA）认证程序，以及 Linux 专业协会（LPI）水平认证都提供了充分的材料。还有两种常见的 Linux 认证在此没有列出，它们是 CompTIA 的 Linux+认证（参见 www.comptia.com）和 Red Hat 认证工程师认证。Linux+认证是一种技术相对不太严格的认证程序，本书及其姐妹篇也适用。Red Hat 认证工程师认证是一种更严格的认证，需要对 Red Hat Linux 加深了解并完成本书每章后的案例分析练习。

Linux 专业协会(LPI)是几个大公司联合发起的，它们是 Caldera International、Hewlett Packard 以及 IBM，这是一个非营利的组织，由很多部门一起负责，从各种 Linux 组织的成员收集意见，发展成一种公认的认证目标、考试手段以及长远计划。LPI 已经预计实施一个三步的认证程序，其中第一步就是使用这本教材，包括两种基本的 Linux 熟练程度考试。

Sair/GNU 认证由 Tobin Maginnis 发起，他是密西西比大学的教授。他领导的组织同世界一流的自由软件热爱者合作创立了 LCA 考试目标和考试程序。要通过 LCA 认证，必须通过四个考试。前两个考试的材料在《Linux 安装和系统管理指南》中提供，本书中提供了后两个考试的材料。附录 A 中提供了完成本书时 LPI 和 LCA 认证目标的一些

常见知识以及这些知识在本书及其姐妹篇中的位置。当然我们也考虑到这种认证考试将来可能会有变动，关于认证变动的详细信息请参照 www.course.com /networking。

本书适合的读者

本书适用的对象包括那些需要了解 Linux 服务器的基本计算机网络和安全技术的学生和教师。虽然本书从讨论网络（第 1 章）和安全（第 7 章）的理论开始，但是最终着眼于实践，而且提供了大量系统管理员日常工作必备的有力工具和站点的各种案例。本书致力于为众多有一些操作系统背景而且习惯于使用 Linux/UNIX 命令行的爱好者提供一本入门教材。书中每章都带有一些实验，可以一步一步地带领读者完成各种常用的网络安全操作。同时，每章还有几个案例，使读者可以利用本章中所学到的知识解决真实环境中可能遇到的种种问题。

各章概要

各章分别讨论了以下话题：

第 1 章：网络基本原理

介绍了目前的网络技术，包括网络的硬件部分和基本的网络理论、以及 Linux 中使用的一些基本网络协议。

第 2 章：配置基本网络

介绍了在 Linux 中如何使用网络设备、以及如何用命令行和图形工具配置网络地址和基本的路由信息。本章中还提到了用于测试网络的基本命令行工具。

第 3 章：配置客户服务

介绍了如何建立域名解析、拨号网络访问以及使用 X Window 系统进行远程访问。本章还解释了 Web 浏览器和邮件客户端的基本概念，介绍了一些常用的软件。

第 4 章：使用简单的网络服务

本章中介绍如何建立 Linux 超级服务器来管理各种接入的网络服务请求，还讲述了一些最基本的服务和依赖于网络的关键管理手段，例如登录和打印。

第 5 章：配置文件共享服务

讨论了四种 Linux 支持的文件共享技术：网络文件系统（NFS）、NetWare NCP 文件共享、文件传输协议（FTP）以及 Microsoft Windows 系统使用的服务器消息块机制（SMB）协议。

第 6 章：配置主要的网络服务

讨论了四种 Linux 著名的网络服务：域名服务（DNS）、动态包路由、利用 sendmail 的邮件服务以及使用 Apache Web 服务器的 Web 服务。

第 7 章：安全、伦理和隐私

从系统管理员和网络管理员职业的角度，论述了网络安全及其伦理的联系，从而引出了本书的后半部分。本章中还从伦理方面和网络管理员关注的角度将个人信息隐私做了一番讨论。

第 8 章：数据安全

讨论了数据加密技术，阐述了基本的概念，同时介绍了目前用以保护网络数据安全

的协议，还谈到了常用的 Linux 加密工具。

第 9 章：用户安全

本章中向用户介绍了网络管理员用以保护用户账号信息的手段，以及网络管理员如何引导普通用户正常地操作来增加系统安全性。本章中还介绍了一些用于增加用户安全的软件工具和安全策略。

第 10 章：文件安全

讨论了如何跟踪重要系统文件的变化，由此可以看出是否有人曾经攻击过你的服务器。本章还介绍了一些用于保护这些文件的特殊工具和加密技术。

第 11 章：网络安全基础

本章介绍了用户和文件安全基础上的网络安全、防火墙等相关概念，以及利用特殊的路由技术来保护局域网络。

第 12 章：网络入侵检测

本章聚焦于攻击技术，继续上一章的内容讨论网络安全以及如何使用嗅探系统和各种系统缺陷探测工具来防止攻击。

附录 A：Linux 认证目标

提供了一个 SAIR/GNU Linux 和 Linux 职业协会（LPI）认证程序的目标列表，以及各个认证目标在本书（或本书的姐妹篇）各章节中出现的位置。

附录 B：命令汇总

提供了一个包含所有 Linux 命令行工具、服务器守护进程以及本书中的各种图形工具（包括本书的姐妹篇中系统安装和系统管理部分的各种图形工具）的列表。

本书的特点

为了帮助读者充分地理解网络概念，本书还有很多独特的地方可以帮助读者更充分地学习。

章节目标：每一章的开始处都详细列出了在本章中读者需要掌握的基本概念。这一项内容不仅给读者提供了一个了解本章内容的捷径，也是一个很有用的辅助工具。

简图和列表：大量关于网络概念、协议的使用以及涉及安全的方法的插图有助于读者理解这些概念。另外，书中的大量表格也为读者提供了必要的参考，如命令行选项和在线信息资源的简明介绍。

各章总结：每一章结束时都有一个本章小节，概括介绍这一章中讲到的概念。

专业术语：每一章中用黑体字表示的所有术语都收集在这章结尾处的专业术语列表中。这样，读者可以以此来检验自己对本章中所出现的术语的理解程度。

习题：为了进一步充实内容，每一章都包含一系列习题。能够回答这些问题就意味着读者已经掌握了这一章中的重要概念。

实验：虽然理解 Linux 操作系统的理论很重要，但这些远远不能增加在现实工作中的经验。因此，每一章都提供了大量的实验，并对其进行了详细的注解，其目的正是为了使读者提高在现实工作中解决问题的能力。

案例：每一章的结尾处有若干个案例。要完成这些练习，读者需要结合前面介绍的技术来考虑现实工作中的实际情况。

写在前面的话

本书中的实验将有助于读者学习运用从书中学到的有关 Linux 网络与安全的知识。下面列出了完成书中所有实验所需要的硬件和软件最低配置。除了这里提到的之外，读者还必须有工作站管理员的访问权限，本书中的大多数案例对这一点都有要求。

本书中列出的示例程序并不是仅适用于 Red Hat Linux 的，事实上本书的多数实例所使用到的知识都适用于现有的 Linux 版本，如 Caldera、SuSE、Debian、TurboLinux、Corel Linux、Mandrake 等。当然，在书中例子里所使用到的某些工具，以及目录结构中特定文件所在的位置可能会有出入。凡是出现这种情况时，书中会特别指明使用 Red Hat，以便使读者注意到：在非 Red Hat 的系统中该处会有所不同。还有一点值得说明，许多案例中所使用的都是 Red Hat Linux，这样做将比把项目定位于所有的 Linux 版本中的通用最低水平上更为复杂。

对实验环境的最低要求

❖ 硬件

- 每个工作站以及每一台作为服务器的计算机都要求最低 64MB 内存、200MHz 或更高工作频率的奔腾或者兼容的处理器，硬盘上最少有 1.5GB 的自由空间。当然有更多硬盘空间更好，但 1.5GB 就已经足够安装上所有要求较高的网络服务了。
- 计算机还需要有一块网卡。本书中都假设为以太网，其他如令牌环形网也是可以的。
- 在许多实验中，需要所有的工作站都互联起来，使用简单的以太网集线器就可以做到这一点。实际上不需要专门的线路，也没有对速度的特殊要求，只要工作站之间可以通信，可以练习使用网络与安全的协议和工具就可以了。
- 在一些实验中，需要学生工作站能够访问 Internet 以便调查研究主题和产品。但是一定要小心，让工作站通过一个大型组织的局域网访问 Internet 可不是绝对安全的，因此，实验中用到的一些工具或者相关技术很可能使局域网的管理员非常反感。

❖ Red Hat Linux 9.0 发行版本

从 Red Hat 公司购买到的 Red Hat Linux 产品中，包含有完整的 Red Hat Linux 版本、Red Hat 的文档，可能还包含有对 Red Hat Linux 的技术支持。用户也可以从 Red Hat 公司购买技术支持。用户可以通过 Red Hat 公司的 Internet 站点（www.redhat.com）从公司购买 Red Hat 的产品和技术支持。在装有 Red Hat Linux 的 CD 光盘的信封上贴有一个标签（这个标签也可能是贴在信封里边文档的背面）。当撕开这个信封之后，就意味着你已经接受了信封文档里所讲的条件。

致谢

如果你的工作得到了某些专家或者高手的支持，那么你要成为一名 Linux 高级用户

就会更容易。因此，我要在此向帮助我顺利推进这个项目的所有的专家表达忠心的感谢。

本套丛书的主编是 Will Pitkin，回忆起在大学期间（他学的是工商专业，我学的是法律专业）与他在筹备出书的时候互相勉励的日子，我很欣慰。至少，我只需要负责一本书，而不是像他一样，需要负责整个相关技术的网络丛书。虽然没有遇到太大的困难，但是我仍然希望我的项目助理 Amy Lyon 能明白，我十分欣赏她的乐观态度和令人愉快的工作。作为作者，与我交流最多的是我的编辑 Deb Kaufmann。Deb 为我润色本书，找出书中我没有表达清楚的地方，他还周密地安排为我整理其他人的工作（我为了减轻我的负担把工作分配给了几名同事）。因此，我希望能无数次地说："谢谢你，Deb"。

Course Technology 公司组建了一个庞大的队伍，力求使其每一本书都尽可能完美。这次我有幸推荐一个曾与我共事多年的人作为这个项目的技术编辑，Ed Sawicki 既是我的同事又是我的朋友。Ed 的加入明显提高了本书在技术上的准确度，Ed 以此来回报我，同时他一直以他多年来从事同类教材的教学经验为本书增添一些趣闻和评价。本书中，我在多处将 Ed 的建议作为我自己的话写入了书中。对于 Course 团队中的其他人来说，我几乎没有什么可以居功的，我只是一个受益者。Aimee Poirier 是产品监制人，他为本书消除了最后的几个句法上的问题（我在前边居然漏掉了 Aimee Poirier，真是愚蠢）。为了减少因为我的疏忽给读者带来的麻烦，MQA 部门（质量保证科）的 Nicloe Ashton、Chris Scriver，还有 Serge Palladino 仔细地测试了书中的所有声明和程序，他们的工作都做得十分出色，保证了质量。

除了 Ed 和 Course Technology 的员工以外，我的主编还招募了几个讲师，由他们在整个过程中阅读书稿。我认为他们的加入起到了重要的作用，使这里的材料更加适合于学生的需要；因为他们都有多年从事教育的经验。他们是：

Denny Brown	密苏里通信技术学院
Rick Menking	Hardin-Simmons 大学
Doug Montgomery	麦德森 Area 技术学院
Chris Spreitler	Vatterott 学院

在此，我还希望感谢那些对本套丛书的第一册《Linux 安装和系统管理指南》给予肯定的老师和读者。在这么多人为出版这些书而做出大量努力之后，来自读者的强烈的反馈将是我们每个人继续下一本书时最需要的鼓励。

最后，我要特别感谢的是我的妻子 Anne。在我写书的时候，她始终热情地关注着所有晦涩的网络原理和有关安全的事项；在我度过了一个又一个不眠的夜晚后，又替我照顾着孩子们。最衷心地感谢你，我的妻子！

目　录

第 1 章　网络基本原理

阅读完本章并完成习题后，你将能够：

- 了解计算机网络的用途及其发展过程
- 确定网络硬件的常见类型
- 描述网络软件是怎样运作的
- 了解常用的网络协议在什么时候使用
- 给出网络路由的定义并叙述常见路由协议的用途

在本章中你将了解到有关计算机网络的基本知识，为使用 Linux 操作系统来创建并支持网络而做准备。本章介绍了网络的用途及发展过程，概括了组成网络的物理元件：网线以及保证网络正常运转的计算机部分；本章的第二部分用专业术语描述了网络软件，带领你认识大多数常用网络类型所使用的操作规则——协议。本章没有在更深层次上对网络硬件和协议做出解释，但是为下一章介绍如何配置 Linux 网络打下了基础。在后续章节介绍配置一些特殊服务的时候，你将会接触到更多有关网络协议的知识。

1.1　联网计算机的发展

从最普遍地意义上讲，计算机网络是为了满足更加方便、快捷地实现通信及信息共享的需求而发展起来的。对于商业机构和政府机关来说，共享信息和资源的需求也是最基本的需求。早在 20 世纪四五十年代，昂贵的计算机使得人们不敢去考虑网络（谁能支付得起两台计算机呢？）；八十年代中期，推出的 PC 也不具备联网的能力；然而没过多久，计算机就在大公司和大学校园里流行起来了，网络的需求也随之不断地增加。

把多台计算机和相关设备在一个局域网（LAN）中连接起来可以提供很多优势：

- 实时地共享信息，而不必转换成像软盘或打印输出一样的可传递形式。
- 自动完成涉及多计算机系统的数据处理任务。
- 更高效地利用资源；多人可以通过网络同时使用一台计算机、打印机或其他资源，哪怕是在很远的地方。

注意： 本章主要讲述那些常用于局域网（在相对小范围内的网络，如办公室或办公楼内）的技术。跨越更宽阔地域的网络——广域网（WAN）则常常使用不同的技术。随着对 Linux 系统管理、网络及安全的不断学习，广域网将会变得非常重要，但是其详细内容不在本书的范围之内。

以下的三个发展历史，对于今天我们正在使用的各种网络系统有着重要贡献：

- 在联网的用途变得越发显著而且成本降低的时候，个人计算机增加了联网的能力。
- 基于 UNIX 的网络服务计算机的成本降低。
- Internet 爆炸式地膨胀而且变得可以被广泛访问。

注意：早期 Internet 上的大多数大型计算机，都是运行在 UNIX 操作系统下，而 Linux 是以 UNIX 为原型的。因此，Internet 刚刚起步时就使用的网络标准，也是 Linux 创建时就一直使用的网络标准。而其他操作系统（例如 Microsoft Windows 或者 Macintosh OS）的设计者，则必须通过加入 UNIX（Linux）的某些特性来使他们的操作系统包含有 Internet 的特性。因此，可以说 Linux 本身就是支持 Internet 的。

也许你已经知道，Internet 是一个通过高速线路将世界范围内的许多网络连接在一起的网络的集合，Internet 上的通信是基于特定的通信协议或通信规则的。一旦 Internet 普及到一般的商人和学生都可以使用，各种组织也就会开始使用 Internet 协议在组织内部与职员、客户之间共享信息。内联网是一种组织内部的网络，它以 Internet 协议作为基础，实现数据和信息共享。在内联网中，职员可以使用一个 Web 浏览器（在每一台计算机系统上都可用的软件）来获取这个组织的中央 Web 服务器上的信息。这比早期的信息共享系统更有效、也更划算。

计算机有三种通用的配置用以共享信息和资源，它们是终端连接、客户端-服务器计算和对等式网络，下面将分别介绍这三种网络类型。

1. 终端将多人连接到一台主机上

终端连接模式是最早的计算机网络类型，然而今天，世界各地仍然有上百万的用户在使用这种计算机网络。终端由一个键盘和一台显示器组成，用户可以通过它访问远程的中央计算机，但是它本身没有处理数据的能力（参见图 1-1）（正是由于这个原因，它们有时也被称为哑终端。）有些终端使用的是图形用户界面，但大多数终端不使用图形用户界面。图 1-1 显示了多台终端连接到一台计算机上的情况，每个终端向计算机发送键盘输入，计算机根据从终端接收到的键盘输入向相应的终端发送响应信息。从某种意义上讲，这种终端可以看作是远程计算机的一部分。

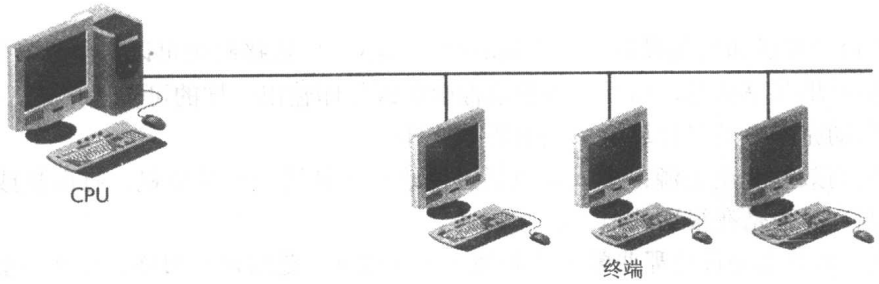


图 1-1 终端允许多个用户同时与一台机器交互

事实上，大多数个人计算机都可以模拟一个终端来连接到另外一台计算机上，并在你自己的终端上向那台计算机发送命令。终端仿真这个词，就是用来表示一个像终端一样可以让你连接到另外一台机器上的程序的。例如，在 Windows 操作系统中包含一个称为 HyperTerminal 的程序，就可以使你的个人计算机像终端一样连接到远程计算机上。对于 Linux 系统，有多种可用的终端仿真程序，xterm 程序是其中使用最广泛的一款程序。你可以在 Linux 系统的图形界面环境中使用 xterm 程序打开一个命令行窗口，并使