开源软件应用技能系列教材
LUPA职业技能认证指定教材

Linux
信息安全实用教程

陈胤 唐云廷/主编
麻志勇 赵斌/副主编

LUPA®

科学出版社
www.sciencep.com

TP316.89/125
2007

开源软件应用技能系列教材
LUPA 职业技能认证指定教材

Linux 信息安全实用教程

陈 胤 唐云廷 主 编
麻志勇 赵 斌 副主编

科学出版社
北 京

内 容 简 介

本书根据作者多年的开发和教学经验，结合大量的实例，系统地介绍了在 Linux 系统中信息安全的主要知识点和安全配置，使读者通过本书的学习，快速掌握在 Linux 系统中进行安全设置的方法和技巧，并具备 Linux 系统信息安全防护的能力。主要内容包括 BIOS 的设置、Linux 引导程序、常用安全命令与设置、系统进程管理、日志安全管理、远程访问、防火墙配置、系统服务的安全设置及常用安全工具的使用等。

本书是开放源代码高校推进联盟“Linux 安全管理员职业技能资格”认证考试指定用书，旨在为信息安全管理人员提供快速掌握 Linux 系统安全管理技能的方式方法，使其能从事有关网络游戏服务器的维护，或大型企业网上交易平台的维护及管理，电信、金融、经贸、商场、宾馆、饭店计算机系统的安全维护工作及机密文件的安全管理工作。

本书适合作为高等院校计算机专业、信息安全专业、信息管理专业、其他电子类和自动控制类专业学生的信息安全教材或参考书，也可供各类信息安全培训班使用。

图书在版编目(CIP)数据

Linux 信息安全实用教程/陈胤，唐云廷主编. —北京：科学出版社，2007
ISBN 978-7-03-019965-2

Ⅰ. L… Ⅱ. ①陈… ②唐… Ⅲ. Linux 操作系统-安全技术-教材
Ⅳ. TP316.89

中国版本图书馆 CIP 数据核字（2007）第 141580 号

责任编辑：吕建忠 陈砺川 / 责任校对：刘彦妮
责任印制：吕春珉 / 封面设计：耕者设计工作室

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

铭浩彩色印装有限公司印刷

科学出版社发行 各地新华书店经销

*

2007 年 9 月第 一 版 开本：787×1092 1/16
2007 年 9 月第一次印刷 印张：15 1/4
印数：1—3 000 字数：332 000

定价：20.00 元

（如有印装质量问题，我社负责调换〈环伟〉）

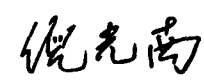
销售部电话 010-62136131 编辑部电话 010-62135763-8001

序

开放源代码高校推进联盟（LUPA），秉承“开源、创新、创业、就业”的宗旨，致力于开源人才的培养和开源技术在高校的推广、应用，几年来在培养大批开源软件人才的过程中，积累了丰富的经验。最近，LUPA 应教育部高教司及浙江省教育厅的要求，邀请了国内知名大学的教授及企业资深专家编写了“开源软件应用技能系列教材”。

“开源软件应用技能系列教材”面向企业、强调实用、体系完整，重在培养应用型、技能型的开源人才，其模块化的课程体系和工程化的教学模式，容易适应当前流行的、以市场需求为导向，人才培养和需求单位之间实行订单式培养的方式，特别有利于培养企业所需要的各种开源岗位专业人才，从操作员、管理员、程序员、技术员到拥有各种专门技能的工程师，都能全面覆盖，从而能满足社会上对不同层次开源人才的需求。此外，本系列教材重视核心课程及实践环节，有利于提高学生自主创新及创业能力；内容全面、符合潮流，可以支持高等院校增设具有前瞻性、与国际国内开源软件产业相适应、市场潜力大的学科专业。

为了改变过去我国软件教学中偏重于私有软件的倾向，近年来，教育部采取了一系列举措，旨在逐步改变这种状况。例如，在全国 40 所高等院校中设置 Linux 培训中心等，支持出版这套教材也是这种努力的一部分。众所周知，中国软件产业的前途取决于我们所培养的软件人才，因为人才的知识技能的倾向将决定未来中国软件产业的走向。因此，强化开源软件的教学，不仅是提高软件人才素质的需要，而且是增强中国软件自主创新能力、建设中国自主软件产业的需要。在这个意义上，我们欢迎“开源软件应用技能系列教材”的出版，希望这套教材能有力地推进开源软件在中国的推广应用。



“开源软件应用技能系列教材”出版说明

一、本套教材书目

“开源软件应用技能系列教材”包括以下书目：

- 《Linux 系统操作员实用教程》
- 《Linux 网络管理员实用教程》
- 《Linux 信息安全实用教程》
- 《Linux 程序员（C 语言）实用教程》
- 《Linux 程序员（JAVA 语言）实用教程》
- 《Linux 嵌入式技术员实用教程》
- 《Linux 系统维护工程师实用教程》
- 《Linux 软件工程师（C 语言）实用教程》
- 《Linux 软件工程师（JAVA 语言）实用教程》
- 《Linux 数据库工程师实用教程》
- 《LAMP 系统工程师实用教程》
- 《Linux 嵌入式工程师实用教程》

二、本套教材特点

本套教材具有如下特点。

（1）系统性

本套教材从国家推广 Linux 要求与企业需求出发，从职业化与技能化出发，从生产实践过程的各项要求出发，设计 LUPA 课程体系。

（2）实用性

本套教材根据行业特色，结合 IT 行业的开发经验，采用工学结合原则，应用大量的应用实例与对实例的思考，使读者系统地、快速地掌握 Linux 在各职业方向上的主要知识点和实用技巧。

（3）完整性

本套教材从 Linux 基本操作的认知开始到程序设计、网站建设、网络服务、网络安全、嵌入式系统应用与设计，均做了较为全面的规划。

（4）层次性

本套教材适合于不同的读者层次需求。所规划的 Linux 课程有适合于扩大 Linux 的认知群的 Linux 推广目标的，有适合于高职院校推广 Linux 的应用技能的，也有适用于本科与研究生层次所需的应用与设计技能的。

1）适合中职、高职、广大公务员等对 Linux 认知的课程：《Linux 系统操作员实用教程》。

此为试读，需要完整PDF请访问：www.ertongbook.com

2）适合高等职业院校与技术员的课程：

- 《Linux 网络管理员实用教程》
- 《Linux 信息安全实用教程》
- 《Linux 程序员（C 语言）实用教程》
- 《Linux 程序员（JAVA 语言）实用教程》
- 《Linux 嵌入式技术员实用教程》
- 《Linux 系统维护工程师实用教程》
- 《LAMP 系统工程师实用教程》

3）适合本科生或研究生的课程：

- 《Linux 网络管理员实用教程》
- 《Linux 信息安全实用教程》
- 《Linux 系统维护工程师实用教程》
- 《Linux 软件工程师（C 语言）实用教程》
- 《Linux 软件工程师（JAVA 语言）实用教程》
- 《Linux 数据库工程师实用教程》
- 《Linux 嵌入式工程师实用教程》

三、“LUPA 职业技能认证”考试课程设计

目前的“LUPA 职业技能认证”考试的课程设计如下。

- Linux 系统操作员职业技能
- Linux 网络管理员职业技能
- Linux 安全管理员职业技能
- Linux 程序员（C 语言）职业技能
- Linux 程序员（JAVA 语言）职业技能
- Linux 嵌入式技术员职业技能
- Linux 系统维护工程师职业技能
- Linux 网络工程师职业技能
- Linux 软件工程师职业技能（C 语言）
- Linux 软件工程师职业技能（JAVA 语言）
- Linux 数据库工程师职业技能
- LAMP 系统工程师职业技能
- Linux 嵌入式工程师职业技能

四、部分课程的技能要求与职业规划

（1）Linux 系统操作员

熟悉 Linux 系统的基本操作，掌握菜单和窗口的操作，文件和文件夹的创建，文件的移动、删除、复制、更名以及属性设置，系统的属性设置等；掌握 OpenOffice.org Writer 字符格式设置、段落设置、页面设置，表格制作、属性设置，对象及图形的插入；

OpenOffice.org Calc 工作表的基本操作、计算、格式化以及图表的应用、数据的管理；OpenOffice.org Impress 基本操作，演示文稿的编辑、插入及修饰，设置演示文稿的放映效果；OpenOffice.org Draw/Math 的基本操作，Linux 下使用光盘和优盘、播放音频和视频，以及一些常用命令的使用。精通 Linux 操作员职业技能，可以从事政府机构和企事业单位的办公自动化，文字处理等工作。

（2）Linux 网络管理员职业技能

掌握 Linux 常用安装方法，常用命令的使用方法，掌握基本的 shell 编程，了解对 TCP/IP 局域网的构建和架设，掌握 Linux 操作系统的使用与管理；熟练掌握 DHCP 服务器、SAMBA 服务器、数据库服务器、DNS 服务器、Apache 服务器、邮件服务器、FTP 服务器、流媒体服务器等的配置，掌握动态站点和虚拟主机的搭建。精通 Linux 网络管理员职业技能，可以从事中、小型企业的 Linux 服务器的日常维护、性能调整、系统架设、服务器安装、网络管理和维护等工作。

（3）Linux 安全管理员职业技能

熟悉 Linux 系统的引导过程，掌握系统监视、进程管理、日志查看及管理，精通 Linux 系统下的用户管理，掌握 Linux 系统文件的安全，掌握加密文件数据并保护数据。掌握 Linux 系统安全管理技能，可以从事有关网络游戏服务器的维护，在大型企业中实现网上交易平台的维护及管理，电信、金融、经贸、商场、宾馆、饭店计算机系统的安全维护工作及机密文件的安全管理工作。

（4）Linux 程序员（C 语言）职业技能

熟悉 Linux 操作系统下的 C 编程环境，掌握 gcc 编译工具及 gdb 调试方法，学习 C 语言编程的基本概念，掌握分支程序设计、循环程序设计、一维数组的应用、一维数组与指针、指针数组、标准 I/O 库等，使学生掌握 Linux 操作系统下 C 程序开发的方法和技巧，并具备开发应用程序的能力。

（5）Linux 嵌入式技术员职业技能

了解嵌入式在日常生活中的应用；了解嵌入式主流芯片与嵌入式操作系统、各厂商主流产品；掌握嵌入式系统的开发流程与嵌入式系统调试方法、嵌入式硬件开发平台的搭建；了解 Linux 系统调用及用户编程接口，掌握不带缓存的文件 I/O 操作与嵌入式 Linux 串口应用程序开发；了解 Linux 下进程及进程通信与进程控制；熟悉 Linux 守护进程；掌握管道通信和信号通信；了解 Linux 内核结构和 Linux 操作系统移植；会编译 Linux 内核；掌握 Linux 文件系统；掌握内核移植的方法；了解 Linux 下设备的驱动；掌握设备驱动的模块化编程；掌握字符设备驱动、键盘驱动、鼠标驱动、LCD 驱动、音频输入/输出驱动等程序的设计。精通 Linux 嵌入式技术员职业技能，可以在嵌入式生产流程线上从事生产、测试、组装等工作，也可以从事嵌入式实验室平台搭建与嵌入式实验室维护工作，从事嵌入式模块化设计与生产。

适应的岗位主要有：

1）在电子技术开发公司从事嵌入式系统的应用与开发工作。

2）在 IT、通信及网络行业从事嵌入式系统的管理、维护工作。

3）在嵌入式系统消费电子、数字家庭和移动通信服务终端从事产品测试、技术支

持等工作。

4）在金融系统从事嵌入式系统的电子设备部门管理、维护工作。

5）在汽车电子、医疗仪器、信息家电、航空航天、军事国防等行业从事嵌入式系统技术支持工作。

6）在嵌入式系统工业控制领域从事相关工作。

（6）Linux 系统维护工程师职业技能

掌握对 Linux 的安装，包括虚拟机、双系统及大型实验室的批量安装以及内核的升级，熟悉主流的网络产品和技术、企业的基本应用系统及其框架，精通对常用软件的安装和卸载，有较强的动手能力和硬件技术服务能力，并懂得对常用的外围设备进行安装，如打印机、数码相机、扫描仪等，掌握常用的 Internet 接入方法和常用的 Linux 命令，懂得计算机系统和网络系统的安装和维护技术，以及对网络安全、数据备份、大型数据库的配置等操作。精通 Linux 系统维护工程师职业技能，可以从事大、中型企业的 Linux 的系统维护等工作，担任系统维护工程师及大型数据维护工程师等工作，并可作为公司或学校的机房管理员。

（7）Linux 软件工程师职业技能（C 语言）

掌握 Linux 环境下程序调试方法，例如 gcc 编译器、gdb 调试器、make 的使用，掌握 Linux 环境下用 C 语言实现的文件操作、标准 I/O 库、进程控制、进程间的通信、Linux 的图形编程、网络编程以及数据库编程，掌握 Linux 操作系统下 C 程序开发的方法和技巧，并具备开发大型应用程序的能力。精通 Linux 软件工程师职业技能，可以从事软件测试、软件编程，软件架构等工作。

（8）LAMP 系统工程师职业技能

掌握 Linux 下常用命令的使用方法，初步掌握 shell 编程，掌握 Linux 下的 Apache 服务器的安装与配置、MySQL 服务器的安装与配置，PHP 的基础知识包括数据类型、变量、常量、运算符、函数、表达式等，PHP 的 MySQL 数据库的编程，构建 PHP 动态网页以及 PHP 的网络编程。精通 LAMP 系统工程师职业技能，可以从事网页制作、网站建设售前工程师、专业网站设计人员、PHP 网站程序开发工程师等工作。

（9）Linux 嵌入式工程师职业技能

了解嵌入式系统的基本概念，能搭建嵌入式 Linux 环境与开发平台，掌握嵌入式 Linux 的 I/O 与文件系统的开发、进程与进程控制开发、进程间通信开发、网络应用开发、设备驱动程序的开发与嵌入式 Linux 图形用户界面的开发。精通 Linux 嵌入式工程师职业技能，可以在制造工业、过程控制、通信、仪器、仪表、汽车、船舶、航空、航天、军事装备、消费类产品等方面从事嵌入式计算机的应用与开发等工作。

前　言

Linux 操作系统是最近几年正在蓬勃发展的自由软件，它在全世界范围内正获得越来越多的公司和团体的支持。近年来出现多种 Linux 发行版本，Red Hat Linux 是最具代表性的版本之一。

在以美国为首的发达国家，Linux 早已涉足政府办公、军事战略以及商业运作等方方面面。在我国，Linux 的起步相对较晚，只是应用在一些诸如政府、军队、金融、电信和证券等比较重要的行业。随着 Linux 在各个行业广泛地成功应用，企业对 Linux 人才的需求也将持续升温。

在网络上，每台计算机系统都连接到另外的计算机或者连接到 Internet，由于经常出现的系统漏洞、病毒、黑客入侵等原因，使得计算机信息安全受到严重的威胁。比如，由于黑客入侵犯罪，在证券交易中使得某些股民损失巨大，以致媒体呼吁“谁来保护我们的网络安全？”Linux 与不开放源代码的操作系统之间的区别在于，开放源代码开发过程本身，由于每个用户和开发者都可以访问其源代码，因而有很多人都在控制和审视源代码中可能的安全漏洞，软件缺陷很快会被发现。因而 Linux 以其可靠性、稳定性、可扩展性、可管理性等性能，得到极大多数用户的认可。Linux 变得越来越流行。

世界上没有绝对安全的系统，即使是普遍认为稳定的 Linux 系统，在管理和安全方面也存在不足之处。要阻止黑客的蓄意入侵，可以减少内网与外界网络的联系，甚至独立于其他网络系统之外。这种方式虽造成网络使用上的不便，但也是最有效的防范措施。Linux 系统管理员或信息安全管理员需要加固 Linux，并建立保护它不受可能攻击的安全机制，期望让系统尽量在承担低风险的情况下工作，这就要求加强对系统安全的管理。

在本书中，编者的目标是介绍对于 Linux 信息安全来说非常重要的主题，这些主题的涵盖面非常广泛。编者对本书的内容组织进行了精心的安排，以帮助读者更多地了解 Linux 所提供的功能，而不管读者现有的经验有多少。Linux 信息安全是一个很广的领域，编者的目标是对广泛领域中的大量主题都进行介绍，从而让读者在每个主题上都能够具备足够的基础知识和实际的安全防范经验。

本书的主要特点

涵盖 Linux 系统安全的主要主题，简单易懂、内容广泛，所有的基础知识和实际的安全设置都以实例的方式给出，并有详细的步骤和说明。

本书的读者对象

- 如果读者是一位信息或网络安全管理人员，希望利用 Linux 提供的安全命令、安全工具，检测系统、网络的安全防护状况，尽量减少检测时间，并让读者的系统与网络充分利用 Linux 系统所提供的安全功能，那么本书将非常适用。
- 如果读者是一位学生，希望有一本 Linux 系统、网络安全的书，有明确清晰的解释和详细的安全设置步骤，帮助读者迅速了解 Linux 系统安全、掌握主要与 Linux 相关的安全技术，那么本书将非常适用。

本书的主要内容

第 1 章～第 4 章，介绍信息安全基础知识和 Linux 安全初步防护，包括 BIOS 安全设置、Linux 引导程序安全设置、Linux 系统中安全设置相关的命令。

第 5 章～第 9 章，介绍 Linux 系统安全，包括系统文件、进程、日志安全分析和管理，Linux 系统远程访问的安全设置，系统自带防火墙的安全设置。

第 10 章～第 12 章，介绍 Linux 网络安全，包括 Linux 常用安全工具使用、网络服务器安全设置、安全设置小技巧。

第 1 章主要论述了信息安全存在的问题。安全问题产生的最根本原因在于信息安全技术的滞后性和信息网络自身的脆弱性。学完本章，读者将了解影响计算机信息安全的几种主要因素，知道一些信息安全保密的常用防范对策。

第 2 章论述了计算机的物理安全，重点介绍如何安全设置计算机主板 BIOS。学完本章，读者将掌握虽不是 Linux 系统本身，但和 Linux 系统密切相关的物理安全和计算机主板 BIOS 的安全设置。

第 3 章论述了 Linux 系统当前使用最广泛的引导程序 GRUB，重点介绍如何安全设置 Linux 的引导程序。学完本章，读者将了解如何在进入系统前的引导程序中加把安全的锁，掌握为 GRUB 设置密码和用 md5 加密校验 GRUB 密码。

第 4 章论述了 Linux 操作系统中一些基本命令的用法，从而能高效快速地完成大多数操作。学完本章，读者将了解一些 Linux 的基本命令，掌握 Linux 系统中和安全相关的命令。

第 5 章主要讲解文件权限的安全设置，Linux 超级权限的安全控制，以及用户账号方面的安全管理与相关设置。另外，还讲述了如何安装杀毒软件，如何对邮件病毒和文件病毒加以防范。学完本章，读者将了解 Linux 系统和文件相关的安全设置，掌握文件、账号的安全设置和管理，掌握 Linux 下邮件和文件型病毒查杀工具的安装使用。

第 6 章详细介绍了 Linux 一些实用的安全管理小技巧。学完本章，读者将了解和掌握 Linux 系统中很实用的安全设置技术：包括限制 shell 命令记录大小、访问控制、密码长度设置、特别账号处理和设置启动过程中不允许按 Ctrl+Alt+Delete 重启系统等。

第 7 章讲述了进程管理的基本概念和进程管理工具介绍。文中重点介绍了进程管理中的进程分类、进程的启动及进程查看，用大量实例介绍了进程管理中常用命令的使用方法。学完本章，读者将了解和掌握 Linux 系统下进程安全的管理和设置。

第 8 章论述了与 Linux 系统安全相关的所有记录——系统日志，详细介绍了通过系统日志分析，找出受到攻击时攻击者留下的痕迹。学完本章，读者将了解 Linux 系统日志，掌握 Linux 系统日志管理和分析工具，掌握常见日志安全分析方法。

第 9 章详细介绍 Linux 的三种远程访问控制的方法，介绍了如何加强远程访问控制的安全。学完本章，读者将了解和掌握通过 telnet、OpenSSH 和 VNC 远程管理控制 Linux 系统，掌握如何提高远程访问的安全级别。

第 10 章详细介绍了 Linux 系统提供的内置防火墙。学完本章，读者将能把许多潜在的威胁用防火墙阻隔在系统之外。

第 11 章介绍了 Linux 系统中比较常用的、具有代表性的安全防护工具。学完本章，

读者将能通过工具分析某个协议是否安全、会不会在传输时泄密，并能分析某网段内是否有服务器，它们有什么服务器软件、什么端口在开放着。

第 12 章介绍了 Linux 主要服务器软件的安全设置。学完本章，读者将能加强 Linux 系统常见服务器软件 Apache、FTP、Samba、Sendmail 等的安全性。

如果要保护系统的安全，针对黑客入侵，我们要做的第一步应该就是把预防工作提前做好。作为一名系统管理员，一定要保证自己管理的系统在安全上没有漏洞，这样就不会给非法用户可乘之机。

本书向读者介绍的是 Linux 系统下的信息安全。为了帮助读者更好地理解各章的内容，希望读者在阅读书中的示例时实际配置一下，这将提供一个很好的安全设置体验并将鼓励读者提升系统的安全级别。本书中还提供许多对知识内容扩充的思考题、实验题，希望读者能够将阅读本书的过程和在自己的 Linux 系统上的实践结合起来，动手思考、设计和配置所有的思考和实验题。

当然，本书并不是一本 Linux 安全的万能秘方，要真正地做到系统安全，除了需要管理员掌握书中所列的方法、技巧外，最重要的是养成安全防范的习惯，在大体的安全管理上实施书中所列的知识与技术。

本书由开放源代码高校推进联盟（简称 LUPA）组织各高校教师进行编写，参加编写的作者均对 Linux 有着丰富的研究经验和实践经验。在这里，作者对在编写本书过程中给予大力支持的中国工程院院士倪光南、教育部高教司、浙江省教育厅表示衷心的感谢。书中有些素材来自网络，对网络上提供材料的朋友们表示衷心的感谢，可以说没有他们的无私帮助，是不可能完成此书的。

本书由陈胤、唐云廷任主编，麻志勇、赵斌任副主编，由陈胤、唐云廷、麻志勇、季江民、张益先、赵斌、刘加海、周南、桑世庆等老师编写，全书由陈胤统稿。

本书配有教学大纲和课件，以及师生用的自学视频。由于时间仓促及作者水平有限，书中难免存在疏漏和不妥之处，敬请广大读者批评指正。批评与建议欢迎发送邮件到 ljhqyyq@yahoo.com.cn，以便及时修订。

此为试读，需要完整PDF请访问：www.ertongbook.com

开源软件应用技能系列教材

编 委 会

主　任　张建华　开放源代码高校推进联盟主席

委　员　宫　敏　中国开源软件推进联盟专家委员会委员
Linux 资深专家

倪光南　中国工程院院士
中国科学院计算技术研究所研究员

陈　钟　北京大学软件与微电子学院院长

薛安克　杭州电子科技大学校长

俞仲文　深圳职业技术学院院长

陈丽能　浙江经济职业技术学院院长

目　录

第1章 安全概述

本章重点

- 影响计算机信息安全的几种因素。
- 信息安全保密防范对策。

本章导读

信息安全技术的滞后性和信息网络自身的脆弱性，是信息安全问题产生的最根本原因。本章具体介绍影响计算机信息安全的几种因素。

此为试读，需要完整PDF请访问：www.ertongbook.com