

## <<Linux信息安全实用教程>>

### 图书基本信息

书名：<<Linux信息安全实用教程>>

13位ISBN编号：9787030199652

10位ISBN编号：7030199650

出版时间：2007-9

出版时间：科学出版社

作者：陈胤，唐云廷主编

页数：222

版权说明：本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问：<http://www.tushu007.com>

## 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具备足够的基础知识和实际的安全防范经验。

## <<Linux信息安全实用教程>>

### 内容概要

《Linux信息安全实用教程》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系统中信息安伞的主要知识点和安伞配置，使读者通过《Linux信息安全实用教程》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、常用安伞命令与设置、系统进程管理、日志安伞管理、远程访问、防火墙配置、系统服务的安伞设置及常用安伞工具的使用等。

《Linux信息安全实用教程》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伞维护工作及机密文件的安伞管理工作。

《Linux信息安全实用教程》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，也可供各信息安伞培训班使用。

## 书籍目录

第1章 安全概述1.1 影响计算机安全的几种因素1.2 信息安全保密防范对策思考与实验第2章 安全设置第一关2.1 物理安全介绍2.2 BIOS安全设置2.2.1 AWARD BIOS安全设置2.2.2 AMI BIOS安全设置2.2.3 Phoenix BIOS安全设置2.3 BIOS常见错误信息和解决方法思考与实验第3章 Linux引导程序设置3.1 Linux引导程序的基本概念3.2 引导程序菜单界面3.3 设置引导程序的密码3.3.1 直接在GRUB配置文件中设置密码3.3.2 用md5加密校验GRUB密码思考与实验第4章 Linux常用命令4.1 man帮助命令4.2 文件系统命令4.3 系统管理常用命令4.4 网络安全常用命令4.5 系统管理安全常用命令思考与实验第5章 文件与文件系统安全5.1 文件权限安全设置5.1.1 文件访问权限的表示5.1.2 改变文件的访问权限5.1.3 改变文件的所有权5.1.4 图形模式下修改文件或目录的访问权限5.1.5 umask设置5.2 超级权限的安全控制5.2.1 用户身份切换5.2.2 使用sudo命令5.3 用户账号安全管理5.3.1 口令安全5.3.2 禁用用户账号5.4 病毒防范5.4.1 MailScanner的安装与配置5.4.2 杀毒软件Clam Antivirus的安装、配置及使用思考与实验第6章 Linux安全设置6.1 限制shell命令记录集6.2 系统服务的访问控制6.2.1 访问控制简介6.2.2 语法规则6.3 Linux身份验证6.4 修改密码长度6.5 禁止系统响应ping请求6.6 启动过程中重启系统的控制思考与实验第7章 进程安全管理7.1 进程简介7.1.1 进程的状态7.1.2 进程的分类7.1.3 进程的属性7.1.4 父进程和子进程7.2 进程管理7.2.1 启动进程7.2.2 进程查看7.2.3 相关终止进程的命令思考与实验第8章 日志安全分析8.1 Linux日志8.1.1 连接时间日志8.1.2 进程统计日志8.1.3 错误日志8.1.4 日志文件8.2 syslog日志文件配置8.2.1 启动syslog服务8.2.2 syslog服务的配置文件8.3 日志管理和分析工具8.3.1 查看系统日志8.3.2 日志管理工具logrotate8.3.3 分析工具Swatch8.4 日志安全分析实例思考与实验第9章 远程安全访问9.1 telnet的使用和安全设置9.1.1 telnet服务的配置9.1.2 telnet服务的安全配置9.2 用安全的ssh来代替telnet9.2.1 配置OpenSSH服务器9.2.2 安全使用OpenSSH服务器9.3 VNC的使用和安全设置9.3.1 配置VNC服务器9.3.2 客户端访问控制VNC服务器9.3.3 VNC服务的安全配置思考与实验第10章 防火墙10.1 Linux防火墙介绍10.2 Linux防火墙配置10.2.1 在图形模式下配置10.2.2 在终端模式下配置10.3 Linux防火墙应用实例10.3.1 普通Linux主机防火墙配置10.3.2 Linux服务器防火墙配置10.3.3 Linux边界防火墙配置思考与实验第11章 常用安全工具的使用11.1 协议分析工具Etherear11.1.1 Ethereal的安装11.1.2 Ethereal的使用11.1.3 利用Ethereal分析常见协议11.2 网络监测工具tcpdump11.2.1 tcpdump的工作原理11.2.2 tcpdump的安装11.2.3 tcpdump的使用11.3 网络端口扫描工具nmap11.3.1 nmap的安装11.3.2 nmap的使用11.3.3 nmap的注意事项思考与实验第12章 服务器安全12.1 增强Apache服务安全12.1.1 Apache简介及原理12.1.2 Apache启动12.1.3 Apache测试12.1.4 实现用户认证12.2 增强FTP服务安全12.2.1 vsftpd.conf配置文件相关安全设置项12.2.2 用OpenSSL实现加密数据传输12.3 增强Sendmail安全性12.3.1 Sendmail的安全设置项12.3.2 SMTP认证12.3.3 使用Procmail过滤邮件思考与实验附录1 开发工具的安装附录2 iptables参数说明参考文献

章节摘录

插图：1.1 影响计算机安全的几种因素1.黑客攻击黑客攻击是计算机网络所面临的最大威胁。

此类攻击又可分为两种：一种是破坏性攻击，指以某种方式有选择地破坏信息的有效性和完整性，是纯粹的信息破坏；另一种是非破坏性攻击，指在不影响网络正常工作的情况下，进行截获、窃取、破译以获得重要机密信息。

这两种攻击可对计算机网络造成极大危害，并导致机密数据的泄密。

2.人为因素人为因素多种多样，如操作员安全设置不当、资源访问控制设置不合理、用户口令选择不慎、用户与别人共享网络资源或将自己的账号转借他人以及内部人员有意无意泄密、内部非授权人员有意无意偷窃机密信息、更改网络配置和记录信息、内部人员破坏网络系统等，都会对网络安全带来威胁。

3.计算机病毒计算机病毒是指在计算机程序中毁坏数据或者扰乱功能，能自我复制并影响计算机使用的一组计算机指令或程序代码。

计算机病毒随着软件的不不断发展而发展，它具有传染性、潜伏性、隐蔽性、破坏性和可执行性等特点。

随着计算机技术的不断发展和信息网络规模的日益扩大，计算机病毒的传播能力、破坏能力、适应能力、变化能力不断增强，计算机病毒已成为信息安全的重要隐患。

4.电磁泄露随着计算机技术的广泛应用，很多信息都利用计算机系统存储或通过计算机网络传输。但计算机系统与其他电子系统一样，不可避免地存在电磁泄露问题。

如计算机主机、显示器、键盘、打印机、传输线路、网络端口等都不同程度地存在电磁辐射，这些泄露的电磁信息可以还原成原始的信息。

实验证明，未加防范的计算机设施开始工作后，用普通计算机装上截获装置，可以在1千米之内获取其内容，目前窃取显示器的显示内容已是一项成熟技术。

## <<Linux信息安全实用教程>>

### 编辑推荐

《Linux信息安全实用教程》为科学出版社出版发行。

版权说明

本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问:<http://www.tushu007.com>