

## <<Linux 系统安全>>

### 图书基本信息

书名：<<Linux 系统安全>>

13位ISBN编号：9787505396265

10位ISBN编号：7505396269

出版时间：2004-4

出版时间：电子工业

作者：(美)Scott Mann

页数：514

字数：845000

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>

## &lt;&lt;Linux 系统安全&gt;&gt;

## 内容概要

本书从安全性的角度介绍了Linux系统的安装。

配置和维护。

第1章至第4章概述性地介绍了系统的脆弱性、安全策略、密码技术以及网络互联，并且对用户账户、文件权限以及文件系统选项等方面的内容进行了研究；第7章和第8章主要阐述了系统账户管理和系统记录，它们在保护系统安全性方面发挥着重要的作用；第5章、第6章和第9章至第17章是本书的核心部分，这些章节描述了如何利用Linux系统特有的安全性和公开可获得的工具来增加系统的安全性；第18章则展示了如何执行本书所涉及到的所有应用工具。

通过阅读本书，读者将会全面了解Linux系统的安全管理。

本书可以作为系统管理员在Linux系统上实施安全性措施以及使用安全性工具的指南，也可以作为研究Linux系统安全性的软硬件设计师和工程师的参考书。

主要内容：

- 为生产环境配置Linux系统
- 使用Bastille审查Linux
- 防止特洛伊木马、后门、密码破解、缓冲区溢出、电子欺骗、DoS攻击的破坏
- 用OpenSSH消除窃听、连接欺骗和其他网络级的攻击
- 使用网络嗅探程序和扫描程序来检测侵入
- 保护Linux/UNIX系统环境
- 理解安全策略的概念
- 有关防火墙、电子邮件、Web服务、文件系统的知识

## <<Linux 系统安全>>

### 作者简介

Scott Mann：是一名Linux软件工程师，在科罗拉多LeftHand Networks工作。他在SGI和Sun Microsystems从事过Linux和UNIX系统的研究工作。

Ellen L.Mitchell：是得克萨斯A&M大学的安全分析人员，负责校园网的安全维护、开发和管理。她维护过Tiger UNIX安全工具。

Mitchell

## 书籍目录

第1章 系统脆弱性调查1.1 系统存在的问题1.2 本书的目的1.3 关于系统脆弱性和攻击性的调查1.4 小结1.5 参考资料第2章 安全策略2.1 什么是计算机和网络安全2.2 增强计算机和网络的安全性2.3 用户隐私与管理道德规范2.4 小结2.5 参考资料第3章 背景信息3.1 基本输入输出系统口令3.2 Linux安装和Linux装载程序3.3 启动脚本3.4 Red Hat软件包管理器3.5 TCP/IP网络互联概述3.6 Internet标准3.7 密码技术3.8 测试和生产环境第4章 用户、权限和文件系统4.1 用户账户管理4.2 根用户账户4.3 工作组账户管理4.4 文件和目录权限4.5 使用xlock和xscreensaver4.6 文件系统限制4.7 访问控制清单和扩展属性4.8 小结4.9 参考资料第5章 插入式身份认证模块5.1 PAM概述5.2 PAM管理5.3 PAM记录5.4 可用PAM模块5.5 PAM - aware应用5.6 关于配置PAM的注意事项5.7 PAM的未来5.8 小结5.9 参考资料第6章 一次性口令6.1 一次性口令的用途6.2 S / Key程序6.3 应该使用哪一种OTP系统6.4 S / Key的脆弱性6.5 小结6.6 参考资料第7章 系统账户管理7.1 一般的系统账户管理7.2 连接账户管理7.3 进程账户管理7.4 账户管理文件7.5 小结7.6 参考资料第8章 系统记录8.1 syslog系统记录工具8.2 其他日志文件8.3 syslog的替代方案8.4 auditd实用程序8.5 小结8.6 参考资料第9章 超级用户9.1 sudo是什么9.2 获取和执行sudo9.3 使用sudo9.4 禁止根用户访问9.5 sudo的脆弱性9.6 小结9.7 参考资料第10章 加强网络服务的安全10.1 使用xinetd10.2 小结10.3 参考资料第11章 安全shell11.1 SSH的可用版本11.2 第1版SSH概述11.3 第2版SSH概述11.4 安装OpenSSH11.5 配置安全shell11.6 使用SSH11.7 配置SSH认证行为11.8 开发ssh的功能11.9 SSH的替代物11.10 小结11.11 参考资料第12章 设置安全口令的重要性12.1 获取Crack12.2 Crack的主要组件12.3 Crack概述12.4 建立Crack12.5 编译和连接Crack12.6 Crack字典12.7 使用Crack12.8 Crack的正规用法12.9 小结12.10 参考资料第13章 使用Bastille审查系统13.1 Bastille概述13.2 获取和安装Bastille13.3 配置Bastille13.4 在其他主机上复制设置13.5 撤销命令13.6 运行AutomatedBastille13.7 小结第14章 设置陷阱14.1 Tripwire概述14.2 获取和安装Tripwire14.3 Tripwire 2.3.1 - 5版14.4 配置Tripwire14.5 Tripwire配置文件14.6 Tripwire策略文件14.7 tripwire命令14.8 初始化Tripwire数据库14.9 Tripwire有效初始化14.10 Tripwire比较模式14.11 Tripwire更新模式14.12 更新策略文件模式14.13 测试电子邮件通知功能14.14 twprint工具14.15 小结14.16 参考资料第15章 使用ipchains15.1 防火墙的定义15.2 报文过滤15.3 为ipchains配置内核15.4 ipchains概述15.5 ipchains的使用规则15.6 报文分组15.7 IP伪装15.8 添加用户自定义规则链15.9 反欺骗规则15.10 规则链中规则的存放顺序15.11 保存与恢复规则15.12 编写和记录规则的注意事项15.13 建立防火墙15.14 ipchains并不只用于防火墙15.15 进一步讨论15.16 补充功能15.17 ipchains的发展15.18 小结15.19 参考资料第16章 网络过滤器iptables16.1 网络过滤器概述16.2 iptables工具16.3 iptables实例16.4 小结16.5 参考资料第17章 扫描程序、嗅探程序和探测程序17.1 引言17.2 扫描程序17.3 嗅探程序17.4 探测程序17.5 小结17.6 参考资料第18章 日志文件管理18.1 通常的日志文件管理18.2 logrotate程序18.3 swatch程序18.4 logcheck程序18.5 小结第19章 实现与管理系统的真实性19.1 从这里开始19.2 减少工作量19.3 系统已经处于生产环境中19.4 内部网19.5 防火墙和DMZ19.6 侵入恢复19.7 添加新软件19.8 深入学习附录A Internet资源附录B 其他工具附录C OPIE附录D 网络安全服务：TCP\_wrappers和portmap附录E 加密文件系统和透明加密文件系统术语表

#### 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>