

图书基本信息

书名：<<HARDENING Linux中文版/网络与信息安全技术经典丛书>>

13位ISBN编号：9787302122586

10位ISBN编号：730212258X

出版时间：2006-2

出版时间：清华大学

作者：托普斯特

页数：387

字数：568000

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>

## 内容概要

“Hardening”系列是美国McGraw-Hill公司新近推出的又一套信息安全系列丛书，与久负盛名的“黑客大曝光”系列携手，为信息安全界奉献了一道饕餮大餐。

本书是“Hardening”系列成员之一，由数位信息安全领域的著名专家编写，通过四段式系统强化教学法，从技术和管理制度两方面，详细介绍Linux系统的安全防护工作，对系统管理员容易疏忽或犯错的细节进行深入探讨，旨在帮助读者把Linux系统建设成信息安全堡垒。

全书共分4大部分16章，第1部分给出降低系统威胁的7个关键步骤，是系统阻止入侵的必要措施；第2部分则是本书的重中之重，自顶向下系统讲述强化Linux系统的具体方法和措施；第3部分告诫人们：一劳不能永逸，需要利用各种监控技术持续监控系统，教会读者阅读各种日志文件内容、判断系统受损程度；第4部分对信息安全工作的预算制订和审批工作进行讨论，同类书中少见。

本书是Linux系统管理员的福音，所有对Linux系统安全感兴趣者必备。

## 作者简介

John H.Terpstra是PrimaStasys公司的总裁兼CTO,该公司的主要任务是向各类信息技术公司提供人员技术培训,并帮助对方进行业务流程重组以提高其赢利能力。

他是Desktop Linux Consortium (桌面Linux论坛) 决策委员会的成员之一, Samba Team (Samba团队), Open Source组织的重

## 书籍目录

第1部分 做好开门七件事 第1章 重要的前期步骤 1.1 检查系统是否已被黑客侵入 1.1.1 终结非授权用户 1.1.2 找出并关闭非授权进程 1.1.3 查看日志文件,寻找黑客入侵活动的蛛丝马迹 1.1.4 检查系统文件是否完好无损 1.2 检查系统的稳定性和可用性 1.2.1 检查硬件操作是否正常 1.2.2 确保电源不会成为隐患第2部分 从根本入手:循序渐进的系统强化流程 第2章 强化网络:禁用不必要的服务 2.1 第1步:让机器脱离网络 2.2 第2步:确定必要服务 2.2.1 Red Hat Enterprise Linux AS 3.0提供的基准服务 2.2.2 SLES8提供的基准服务 2.2.3 考虑是否还要激活其他服务 2.3 第3步:确定各项服务之间的依赖关系 2.4 第4步:禁止不必要的服务运行 2.4.1 利用软件工具修改启动脚本 2.4.2 禁用不必要的服务:命令行工具 2.5 第5步:重新启动系统 2.6 第6步:复查非必要服务的配置情况 2.6.1 对有关配置进行复查:GUI工具 2.6.2 对有关配置进行复查:命令行工具 2.7 第7步:复查必要服务的配置情况 2.7.1 检查系统服务的配置情况 2.7.2 测试这项服务是否在运行 2.7.3 在系统内存里检查这项服务是否存在 2.8 第8步:让机器重返网络 第3章 安装防火墙和过滤器 3.1 摸清家底 3.1.1 检查系统是否已经存在防火墙规则 3.1.2 网络基本知识 3.1.3 防火墙基本知识 3.2 按照预防为主的原则确定防火墙需求 3.2.1 制定预防策略 3.2.2 配置防火墙 第4章 强化软件的访问权限 4.1 确定必不可少的软件 4.2 确定软件之间的依赖关系 4.3 删除或限制不必要的软件 4.4 安全地安装软件 4.4.1 安装由Linux发行商提供的可信软件 4.4.2 安装其他可信来源的软件 4.5 监控系统 第5章 做好迎接灾难的准备 5.1 什么是灾后恢复 5.2 不要建立一个定制的内核 5.3 把服务器设置和系统配置变动情况记录在案 5.4 系统自动安装/恢复 5.4.1 使用Red Hat的Kickstart安装工具 5.4.2 使用SUSE的YaST自动安装工具 第6章 强化访问控制 6.1 Linux文件的权限和所有权 ..... 第7章 强化数据存储 第8章 强化身份验证机制和用户身份 第9章 强化软件运行环境 第10章 强化网络通信第3部分 一劳不能永逸 第11章 安装网络监控软件 第12章 建立日志文件自动化扫描/报警机制 第13章 补丁的管理和监控 第14章 系统自我监控工具第4部分 Linux系统强化工作的成功之道 第15章 编制安防预算,赢得公司支持 第16章 发动一场信息安全战役附录 Linux信息安全资源

### 编辑推荐

本书以Red Hat Enterprise Linux AS 3.0和Novell公司SUSE Linux的SLES8和SLES9版本为例，从底层开始系统讲述强化网络安全的所有细节，并对如何让信息安防计划赢得企业上下全面支持的种种策略做了全面深入的探讨。

本书适用于该方面的兴趣爱好者!

#### 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>