

<<Linux安全体系分析与编程>>

图书基本信息

书名：<<Linux安全体系分析与编程>>

13位ISBN编号：9787121050190

10位ISBN编号：7121050196

出版时间：2007-11

出版时间：电子工业

作者：倪继利

页数：769

字数：1254000

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>

<<Linux安全体系分析与编程>>

内容概要

本书选择经典的开放源代码，全面系统地分析了Linux安全机制。本书共有17章，前10章着重介绍了Linux操作系统的安全机制及实现方法，阐述了公钥设施的基本概念和使用openssl库接口进行编程的方法。后7章介绍了可信平台模块框架规范和可信网络连接框架规范，并分析了可信平台模块的驱动程序的实现机制。另外，作者还结合实际代码归纳了Linux系统编程的编程模式，介绍了Makefile生成方法和ELF文件执行过程。

本书主要针对从事Linux系统编程的中、高级读者及开发者，也可作为大学与计算机相关的专业的教材和参考书。

<<Linux安全体系分析与编程>>

书籍目录

第1章 Linux安全框架	1.1 Linux安全概述	1.1.1 安全评价标准	1.1.2 操作系统安全特性
	1.1.3 网络安全的OSI安全模型	1.1.4 数据库安全	1.2 Linux安全框架
第2章 日志系统与审计系统	2.1 Linux日志系统	2.1.1 Linux日志系统概述	2.1.2 syslog系统构架
	2.1.3 printk及控制台的日志级别	2.1.4 printk打印消息机制	2.1.5 sys_syslog系统调用
2.2 审计系统	2.2.1 审计系统构架	2.2.2 用户空间审计系统应用程序	2.2.3 内核审计缓冲区管理机制
	2.2.4 审计事件分类	2.2.5 内核审计系统的接口函数	2.2.6 内核审计系统初始化
	2.2.7 与用户空间审计系统的netlink通信机制	2.2.8 利用规则链表进行审计事件过滤	2.3 进程的审计
	2.3.1 进程审计上下文	2.3.2 系统调用记录审计信息的过程	2.3.3 进程辅助审计数据
	2.4 文件系统变化监视机制	2.4.1 文件系统改变发起事件的机制	2.4.2 用于文件系统监视的数据结构
	2.4.3 inotify机制的事件处理	2.4.4 文件系统变化的审计	2.4.5 用户空间inotify机制
第3章 SELinux访问控制机制	3.1 SELinux概述	3.1.1 Linux与SELinux在安全管理上的区别	3.1.2 Flask安全框架概述
	3.1.3 安全模块 (LSM) 框架	3.1.4 内核SELinux的组织结构	3.2 SELinux策略配置语言
	3.2.1 基本概念	3.2.2 TE规则的描述	3.2.3 RBAC规则的描述
	3.2.4 限制规则	3.2.5 标识安全上下文	3.2.6 boolean及条件描述语句
	3.3 SELinux策略配置	3.3.1 策略文件的配置	3.3.2 系统启动时的策略
	3.3.3 在/proc和/selinux文件系统中的策略	3.3.4 SELinux设置分析工具	3.3.5 策略的编译与装载
	3.4 参考策略	3.4.1 安全策略的概念	3.4.2 target二进制策略目录与文件说明
	3.4.3 参考策略源代码分析	3.4.4 如何创建一个策略模块	3.5 用户空间客体管理器
	3.5.1 客体管理器机制概述	3.5.2 使用客体管理器的样例	3.5.3 客体管理器接口说明
	3.5.4 libselinux库初始化	3.5.5 函数avc_init分析	3.5.6 netlink机制获取内核SELinux实时消息
	3.5.7 函数avc_has_perm分析	3.6 内核策略库及库管理.....	
第4章 文件权限管理			
第5章 PAM用户认证机制			
第6章 ClamAV杀毒应用程序			
第7章 On_access文件访问拦截			
第8章 防火墙			
第9章 PKI公钥设施			
第10章 OpenSSL			
第11章 可信计算与内核加密接口			
第12章 内核密钥环			
第13章 加密文件系统			
第14章 数字版权管理			
第15章 ELF文件执行过程			
第16章 应用程序编译方法			
第17章 编程模式参考文献			

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>