

<<操作系统安全>>

图书基本信息

书名：<<操作系统安全>>

13位ISBN编号：9787115266125

10位ISBN编号：7115266123

出版时间：2012-8

出版时间：人民邮电出版社

作者：张波云，鄢喜爱，范强 主编

页数：275

字数：440000

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>

<<操作系统安全>>

内容概要

《教育部高职高专电子信息类专业教学指导委员会规划教材：操作系统安全》在计算机信息系统的整体安全性中具有至关重要的作用，没有操作系统提供的安全性，计算机系统的安全性是没有基础的。

《教育部高职高专电子信息类专业教学指导委员会规划教材：操作系统安全》全面介绍了操作系统安全的基本理论和关键技术，包括安全操作系统的研究发展历程、安全策略、安全模型和安全机制、安全体系结构、知名安全操作系统介绍、安全操作系统测评以及安全操作系统的应用等，同时注重理论联系实际，重点介绍了当前主流操作系统的安全设置和安全管理及安全增强技术。

《教育部高职高专电子信息类专业教学指导委员会规划教材：操作系统安全》可作为高职高专信息安全专业、计算机相关专业学生的教材，也可作为广大计算机用户、系统管理员、计算机安全技术人员的技术参考书。

同时，也可作为计算机信息安全职业培训的教材。

<<操作系统安全>>

书籍目录

第1章 绪论

第一部分 教学组织

第二部分 教学内容

1.1 操作系统面临的安全威胁

1.1.1 信息安全的发展过程

1.1.2 操作系统安全威胁

1.2 操作系统安全和信息系统安全

1.3 安全操作系统的研究发展

1.4 操作系统安全的基本定义及术语

本章小结

课后习题

第2章 操作系统安全理论基础概述

第一部分 教学组织

第二部分 教学内容

2.1 操作系统安全机制

2.1.1 标识与鉴别机制

2.1.2 访问控制

2.1.3 最小特权管理

2.1.4 可信通路

2.1.5 安全审计机制

2.1.6 存储保护、运行保护和I/O保护

2.2 操作系统安全模型

2.2.1 状态机模型

2.2.2 存取矩阵模型

2.2.3 BLP模型

2.2.4 Biba模型

2.2.5 Clark-Wilson模型

2.2.6 ChineseWall模型

2.2.7 RBAC模型

2.2.8 其他模型

2.3 安全体系结构

2.3.1 安全体系结构的含义及类型

2.3.2 计算机系统安全体系结构设计的基本原则

2.3.3 Flask体系和权能体系

本章小结

课后习题

第3章 Windows系统安全要素

第一部分 教学组织

第二部分 教学内容

3.1 Windows系统安全模型

3.1.1 Windows系统安全模型组件

3.1.2 Windows系统安全模型构成

3.1.3 WindowsVista的安全模型

3.2 对象与共享资源

3.2.1 对象

<<操作系统安全>>

3.2.2 共享资源

3.3 文件系统

3.3.1 FAT文件系统

3.3.2 NTFS

3.3.3 其他常用文件系统

3.4 域和工作组

3.4.1 域

3.4.2 域控制器

3.4.3 域和委托

3.4.4 工作组

3.5 用户账号

3.5.1 账号

3.5.2 用户管理

3.6 用户组

3.7 注册表

3.7.1 注册表概述

3.7.2 注册表的功能及结构

3.8 进程、线程和服务

3.8.1 作业对象

3.8.2 进程

3.8.3 线程

3.8.4 服务及服务控制管理

3.8.5 服务对象安全性及服务启动

3.9 驱动程序

本章小结

实验：Windows2003域和工作组的配置

课后习题

第4章 Windows账户安全管理

第一部分 教学组织

第二部分 教学内容

4.1 账户的基本概念

4.1.1 本地用户账户

4.1.2 本地组账户

4.2 用户账户的管理

4.2.1 本地用户账户的创建

4.2.2 设置本地账户属性

4.2.3 本地用户账户的删除

4.3 用户组的管理

4.3.1 创建本地组

4.3.2 删除本地组

4.4 系统账户权限设置

4.4.1 理解权限

4.4.2 用户安全设置

4.4.3 本地安全设置

本章小结

实验：WindowsServer2003管理员密码的破解

课后习题

<<操作系统安全>>

第5章 Windows系统资源的安全保护

第一部分 教学组织

第二部分 教学内容

5.1 文件系统和共享资源的安全设置

5.1.1 Windows中的常用文件系统

5.1.2 EFS加密原理

5.1.3 资源共享

5.1.4 资源访问权限的控制

5.2 打印机的安全管理

5.2.1 打印服务器的安装

5.2.2 共享网络打印机

5.2.3 打印机权限的设置

5.3 注册表的安全管理

5.3.1 管理和维护注册表

5.3.2 利用注册表优化设计Windows系统安全

5.4 审核策略和安全记录分析

5.4.1 审核策略简介

5.4.2 审核策略的设置

5.4.3 安全记录分析

本章小结

实验：EFS加密文件系统的使用

课后习题

第6章 Windows操作系统安全测评

第一部分 教学组织

第二部分 教学内容

6.1 Windows操作系统安全漏洞扫描

6.1.1 漏洞扫描的功能

6.1.2 漏洞扫描系统及其分类

6.1.3 Windows下的漏洞扫描系统MBSA

6.2 操作系统安全测评

6.2.1 可信系统评价标准（TCSEC）

6.2.2 操作系统评测框架

6.2.3 基本功能测评

本章小结

实验：X-Scan漏洞扫描

本章习题

第7章 Windows系统安全增强

第一部分 教学组织

第二部分 教学内容

7.1 Windows系统安全设置

7.1.1 端口控制

7.1.2 服务

7.1.3 通信协议

7.1.4 应用实例

7.2 Windows系统安全加固与管理

7.2.1 补丁管理

7.2.2 新装机器步骤

<<操作系统安全>>

7.2.3 病毒防范

7.2.4 用户管理及密码策略

7.2.5 屏幕锁定

7.2.6 本地策略

7.2.7 文件共享服务的加固

7.2.8 双网卡机器管理

7.3 WindowsTCP/IP端口控制操作

7.3.1 Windows2000TCP/IP端口控制操作

7.3.2 WindowsNT4.0TCP/IP端口控制操作

本章小结

实验：Windows端口安全加固设置

课后习题

第8章 Linux操作系统用户安全管理策略

第一部分 教学组织

第二部分 教学内容

8.1 Linux操作系统概述

8.1.1 Linux与UNIX

8.1.2 Linux系统的组成

8.1.3 Linux系统的特点和应用

8.2 保护用户口令策略

8.2.1 Linux的用户与用户组概述

8.2.2 用户标识符安全

8.2.3 安全用户口令的设定原则

8.2.4 用户口令加密函数

8.2.5 使用密码分析工具验证

8.3 账号与组安全管理策略

8.3.1 用户与用户组账号文件

8.3.2 用户与用户组影子文件

8.3.3 账号与组管理安全

8.3.4 账号与组文件的安全性保护

8.4 用户访问控制策略

8.4.1 su命令和sudo命令

8.4.2 查询用户

8.4.3 访问控制

本章小结

实验：Linux基本安全命令使用

课后习题

第9章 Linux操作系统文件系统安全

第一部分 教学组织

第二部分 教学内容

9.1 分区的安全策略

9.1.1 块设备和分区

9.1.2 使用fdisk进行分区

9.1.3 使用parted进行分区

9.2 文件共享安全

9.2.1 常见的文件共享安全方式

9.2.2 NFS快速配置与安全策略

<<操作系统安全>>

9.3 文件系统的安全加载

9.3.1 安装文件系统

9.3.2 标签、UUID和链接

9.3.3 引导时间和fstab

9.4 保持文件系统的完整性

9.4.1 检查文件系统

9.4.2 监控磁盘可用空间

9.4.3 修复文件系统

9.4.4 高级工具

9.5 文件系统的数据备份

9.5.1 使用tar和afio进行备份

9.5.2 完全备份、增量备份和差分备份

9.5.3 专有的备份软件

本章小结

实验：Linux文件系统管理

课后习题

第10章 Linux系统安全增强

第一部分 教学组织

第二部分 教学内容

10.1 系统安全设置技巧

10.1.1 启动和登录安全性设置

10.1.2 网络访问安全性设置

10.1.3 安装系统安全补丁包

10.2 日志和审计工具的使用

10.2.1 UNIX的日志系统

10.2.2 syslog-ng工具及使用

10.2.3 其他日志工具

10.3 入侵检测工具及使用

10.3.1 入侵检测概述

10.3.2 入侵检测系统的分类

10.3.3 常用手工入侵检测方法 with 命令

10.3.4 入侵检测工具Snort及使用技巧

本章小结

实验：Linux系统安全增强综合实验

课后习题

第11章 安全操作系统应用

第一部分 教学组织

第二部分 教学内容

11.1 操作系统安全与WWW安全

11.1.1 WWW概述

11.1.2 安全WebServer概念的提出及相应的解决方案

11.1.3 基于BLP模型的SecWeb系统描述

11.2 操作系统安全与防火墙安全

11.2.1 防火墙介绍

11.2.2 防火墙涉及的安全技术

11.2.3 防火墙利用安全操作系统的保护机制

本章小结

<<操作系统安全>>

实验：配置Linux下的防火墙

课后习题

参考文献

<<操作系统安全>>

章节摘录

版权页：插图：可信通路是用户能够借以直接同可信计算基通信的一种机制。

用户进行与安全有关的操作时，如登记、定义用户的安全属性、改变文件的安全等级等操作，必须保证是与计算机系统的安全核心通信。

特权用户在进行特权操作时，也要确保从终端输出的信息是正确的，而不是来自于特洛伊木马。

这些都需要一个机制保障用户和内核的通信，这种机制就是由可信通路提供的。

可信通路能够保证用户确定是和安全核心通信、防止不可信进程如特洛伊木马等模拟系统的登录过程而窃取用户的口令。

提供可信通路的最简单的办法是为每个用户提供两台终端，一台用于处理日常工作，另一台专门用于实现与安全内核的硬连接及专职执行安全敏感操作。

这种办法虽然简单，但是十分昂贵。

2.1.5 安全审计机制 审计机制一般对系统定义了一个固定审计事件集，即必须审计事件的集合。

要实现审计机制，首先要解决系统如何才能保证所有安全相关的事件都能够被审计的问题。

用户程序与操作系统的唯一接口是系统调用，用户请求系统服务时，必须经过系统调用。

所以，如果能找到系统调用的总入口，在这个审计点增加审计控制，就可以成功地调用审计系统，同时成功地审计系统中所有使用内核服务的事件。

审计机制一般是通过对日志的分析来完成的。

日志就是记录的事件或统计数据，这些事件或统计数据能提供关于系统使用及性能方面的信息。

审计就是对日志记录的分析并以清晰的、能理解的方式表述系统信息。

系统的安全审计就是对系统中有关安全的活动进行记录、检查及审核。

审计通过事后分析的方法认定违反安全规则的行为，从而保证系统的安全。

安全操作系统一般将要审计的事件分为3类：使用系统的事件，注册事件，利用隐蔽通道的事件。

第一类属于系统外部事件，即准备进入系统的用户产生的事件；后两类属于系统内部事件，即已经进入系统的用户产生的事件。

审计机制的主要作用如下。

能够详细记录与系统安全有关的行为，并对这些行为进行分析，发现系统中的不安全因素，保障系统安全。

能够对违反安全规则的行为或企图提供证据，帮助追查违规行为发生的地点、过程以及对应的主体。

<<操作系统安全>>

编辑推荐

《教育部高职高专电子信息类专业教学指导委员会规划教材:操作系统安全》可作为高职高专信息安全专业、计算机相关专业学生的教材，也可作为广大计算机用户、系统管理员、计算机安全技术人员的技术参考书。

同时，也可作为计算机信息安全职业培训的教材。

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>