<<Linux安全策略与实例>>

图书基本信息

书名：<<Linux安全策略与实例>>

13位ISBN编号：9787111283782

10位ISBN编号：7111283783

出版时间：2009-11

出版时间：机械工业出版社

作者：李洋

页数：410

前言

Linux是一个优秀的、日益成熟的操作系统，它支持多用户、多进程及多线程，实时性好，功能强大而稳定。
同时，它又具有良好的兼容性和可移植性。
在网络技术日益发展的今天，凭借其在安全性、稳定性等方面的巨大优势，正受到越来越多的用户的青睐，一些大型的网络及网站服务器，都建立在Linux平台之上。
然而，随着互联网的发展以及Linux应用的普及，Linux系统的安全问题也日益突出。
权限滥用、用户误操作、文件系统安全、垃圾邮件、病毒、木马、拒绝服务攻击等问题正威胁着Linux。
解决Linux系统的安全问题已成为Linux用户和网络管理员的当务之急，也是当前网络信息安全领域研究的热点和难点。
本书从Linux系统安全和Linux网络服务安全两个方面入手，系统、全面、深入地向读者介绍了Linux系统安全和网络服务安全的原理、技术及应用方法，并通过具体的实例来剖析Linux安全的实质，以及如何有效运用相关的技术和软件工具来保障Linux的系统安全和网络服务安全。
本书是一本全面介绍Linux安全技术的专著，具有很强的实用性和可操作性，不仅适合中高级Linux用户、网络管理员、网络工程师、网络信息安全工作者和研究者，也可作为高等院校计算机软件和信息安全专业师生的参考用书。
并且，本书内容不局限于任何一个Linux发行套件，对各Linux套件的用户都有很强的实用性和指导作用。
本书的作者具有多年从事：Linux安全研究及开发的工作经验，本书是他们多年来学习、工作和从事重大项目开发经验的结晶。
本书由李洋主持编写，参与编写的作者还有王俊丽、邓柱中、姚秋林、舒承椿、丁凡、汪浩、王曦爽、张磊、张鹏。
全书由李洋统稿并审校。
由于水平和时间所限，不妥或错误之处在所难免，敬请广大读者批评指正。

<<Linux安全策略与实例>>

内容概要

本书对Linux安全策略进行了全面、深入和系统的分析，主要分为Linux系统安全策略和Linux网络安全策略两大部分。
在第一部分，着重介绍了Linux文件系统安全管理、Linux用户和组安全管理、Linux进程安全管理、Linux磁盘安全管理、SELinux安全机制等内容；在第二部分，对Web 服务安全、FTP服务安全、SMTP服务安全、远程登录服务安全、网络流量管理安全及IDS、防火墙等内容进行了详细介绍。
本书针对Linux安全策略都给出了相应的实例，便于读者进行参照和迅速掌握。

<<Linux安全策略与实例>>

书籍目录

章节摘录

插图：第6章 Linux中的日志管理Linux系统中的日志子系统对于系统安全来说非常重要，它记录了系统每天发生的各种各样的事情，包括哪些用户曾经或者正在使用系统，可以通过日志来检查错误发生的原因，更重要的是在系统受到黑客攻击后，日志可以记录攻击者留下的痕迹。
通过查看这些痕迹，系统管理员可以发现黑客攻击的某些手段以及特点，从而能够进行处理工作，为抵御下一次攻击做好准备。
本章主要讲述如何使用工Linux系统中的日志子系统及其命令，从而更好地保护系统安全。
6.1 Linux日志管理简介日志的主要功能是审计和监测。
它还可以用于追踪入侵者等。
在Linux系统中，有四类主要的日志：（1）连接时间日志：由多个程序执行，把记录写入到／var／log／wtmp和／var／run／utmp，login等程序更新wtmp和utmp文件，使系统管理员能够跟踪谁在何时登录到系统。
（2）进程统计：由系统内核执行。
当一个进程终止时，为每个进程向进程统计文件（pacct或acct）中写一个记录。
进程统计的目的是为系统中的基本服务提供命令使用统计。
（3）错误日志：由syslogd（8）守护程序执行。
各种系统守护进程、用户程序和内核通过syslogd（3）守护程序向文件／var／log／messages报告值得注意的事件。
另外有许多Linux程序创建日志。
像HTTP和FTP这样提供网络服务的服务器也保持详细的日志。
（4）实用程序日志：许多程序通过维护日志来反映系统的安全状态。
su命令允许用户获得另一个用户的权限，所以它的安全很重要，它的文件为sulog。
同样重要的还有sudolog。
另外，诸如Apache等Http服务器都有两个日志：access log（客户端访问日志）以及error log（服务出错日志）。
FTP服务的日志记录在xferlog文件当中，Linux中邮件传送服务（sendmail）的日志一般存放在maillog文件当中。
上述四类日志中，常用的日志文件如表6-1所示。

<<Linux安全策略与实例>>

编辑推荐

《Linux安全策略与实例》中涉及到了Linux系统安全，Linux用户和组管理安全中，SELinux原理及使用，Linux网络安全。

版权说明