<<Linux安全技术内幕>>

图书基本信息

书名：<<Linux安全技术内幕>>

13位ISBN编号：9787302223146

10位ISBN编号：7302223149

出版时间：2010-7

出版时间：清华大学

作者：李洋

页数：626

前言

随着黑客攻击问题的不断加剧，木马、病毒、网络钓鱼、分布式拒绝服务攻击、僵尸网络等网络威胁的不断涌现，信息安全问题已经成为国家、社会和企业关注的焦点问题。
信息安全问题的范围已经扩展到计算机和通信领域的方方面面，其中作为基础软件的操作系统也不例外。
作为一种优秀的开源网络操作系统，Linux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，正受到越来越多用户的青睐，一些大型网络及网站服务器都建立在Linux平台之上。
然而，其在系统管理、网络服务管理等方面的安全问题仍然不可小视，针对该系统安全问题的分析和相应的安全技术保障已成为广大网络和系统管理员以及众多操作系统用户的迫切需求。
本书从黑客攻击的基本技术、Linux面临的安全威胁、Linux安装与启动、Linux系统安全管理、Linux网络服务安全管理、Linux核心安全技术、Linux优秀开源安全工具等多个层面，力求系统、全面、科学地讲述和揭示与Linux相关的原理、技术、机制等安全内幕。
本书所讲述的Linux安全内容覆盖范围广，适用人群广。
在写作思路上强调在“授人以渔”的前提下“授人以鱼”，对每个知识点的介绍争取做到深入浅出，从系统、科学的原理和机制介绍出发，并通过丰富多样的图表配以具体的步骤实现和详细的讲解。
并且，编者精心选择了目前市面上最为流行和稳定的Fedora 10 Linux操作系统版本进行实例讲解，以方便读者在实际L,inux安全的管理和操作中进行对照学习，提高学习效率。

<<Linux安全技术内幕>>

内容概要

本书系统、全面、科学地讲述和揭示了与Linux相关的原理、技术、机制等安全内幕，全书共分25章，对Linux安全内幕进行了全面、深入，和系统的分析，内容包括黑客攻击的基本技术、Linux面临的安全威胁、Linux安装与启动、Linux系统安全管理、Linux网络服务安全管理、Linux核心安全技术、Linux优秀开源安全工具等。

本书的讲解和分析深入透彻，适用于众多Linux爱好者、中高级Linux用户、IT培训人员及IT从业者，同时也兼顾网络管理员和信息安全工作者，并可作为高等院校计算机和信息安全专业学生的教学参考书。

作者简介

李洋，博士，信息安全专家，项目经理。
10余年来一直从事计算机网络信息安全领域研发工作，曾主持和参与多项国家重点项目以及信息安全系统和企业信息安全系统的研发工作。
在IEEE、ACM、《计算机世界》、《网管员世界》、51CTo等国际和国内知名会议、期刊和媒体上发表学术论文和各类技术文章百余篇，并出版相关专著多部。

<<Linux安全技术内幕>>

书籍目录

<<Linux安全技术内幕>>

章节摘录

插图：由上述介绍可知，Linux操作系统的安全级别仅为C2级，安全级不高，很重要的一个原因就是超级用户具有所有特权，而普通用户不具有任何特权。
操作系统的这种特权管理机制便于系统的维护和配置，但是不利于保证系统的安全性。
一方面，一旦超级用户的口令丢失或者口令让不法用户获取，那么将会对系统造成极大的损失；另一方面，超级用户的误操作以及权限的滥用也对系统的安全构成了极大的威胁。
因此，必须针对该操作系统实行最小特权管理机制。
最小特权管理的主要思想比当前Linux系统的机制更为安全，它指的是系统不赋予用户超过执行任务所需特权之外的特权，也就是说，不存在具有所有权限的用户。
例如，可以将超级用户的特权划分为一组细粒度的特权，分别授予不同的系统管理员或者是相关的操作人员，使得系统中的这些人员只能够使用自己的特权完成相应的属于自己的工作，从而减少了由于特权用户的口令丢失或者是误操作所引起的不必要的损失。
并且，为了保证系统的安全性，不应当将特权集于某个用户，且对其赋予一个以上的职责，这样，就不会由于一权独揽造成权限滥用的不良后果。
当然，根据实际的应用，还是可以按情况对某个用户的权限进行必要的改变和增加，但是在执行这种变化时必须充分考虑到这些改变和权限的增加对系统安全性造成的影响，因此，可以在具体的设计过程中根据实际应用情况进行分别细致的考虑。

编辑推荐

《Linux安全技术内幕》是由清华大学出版社出版的。

版权说明