<<网络安全技术内幕>>

图书基本信息

书名：<<网络安全技术内幕>>

13位ISBN编号：9787030213747

10位ISBN编号：7030213742

出版时间：2008-5

出版时间：科学出版社

作者：肖松岭

<<网络安全技术内幕>>

内容概要

破坏操作系统、获得超级用户权限的恶意行为，对所有系统管理员来说都将是一场噩梦。
本书主要讨论Windows、UNIX、Linux等操作系统，各类黑客入侵的手段及其防护措施。
本书共分4个部分：第一部分首先介绍了网络安全必备的基本意识和基础知识，接着讨论了Windows及其应用程序IIS、SOL Server以及Web的安全问题及攻击的方法。
第二部分讨论了LNIX和Llnux网络的安全问题，包括Linux安全硬化、服务器安全策略、虚拟专用网、防火墙技术、OpenSSH加密以及评估与入侵事件。
第三部分主要从网络架构OSI各层协议的安全问题着手，对各类操作系统的网络安全及其防护给出了具体实现方法。
从技术角度上看，涉及各个操作平台，包括网络安全原理、IP层安全协议、传输层安全协议、应用层安全协议、防火墙技术以及加密和认证技术等。
第四部分重点介绍Cisco设备安全问题。
网络安全的诸多问题及其安全防护措施，包括防火墙技术，数据加密技术，入侵检测系统，认证、授权和记账以及无线网络的安全性等内容，书中都作了十分详细的剖析，指导性、实用性和可操作性强。
本书适合从事网络安全工作的工程技术人员、网管员和大专院校师生阅读，对网络爱好者也有很好的指导作用。

<<网络安全技术内幕>>

书籍目录

<<网络安全技术内幕>>

章节摘录

第一部分 Windows安全篇第一章 初识Windows安全1.1 网络安全服务为了适应网络技术的发展，ISO（InternationalOrganizationforStandardization，国际标准化组织）的计算机专业委员会根据开放系统互联参考模型，制定了一个网络安全体系结构模型，这个三维模型从比较全面的角度来考虑网络与信息的安全问题。
网络安全需求应该是全方位的、整体的。
在OSI（OpenSystemInterconnectionReferenceModel，开放式通信系统互联参考模型）7个层次的基础上，将安全体系划分为4个级别：网络级安全、系统级安全、应用级安全及企业级的安全管理，而安全服务渗透到每一个层次，从尽量多的方面考虑问题，有利于减少安全漏洞和缺陷。
针对网络系统受到的威胁，0S1安全体系结构提出了以下几类安全服务：身份认证这种服务是在两个开放系统同等层中的实体建立连接和数据传送期间，为提供连接实体身份的鉴别而规定的一种服务。
这种服务防止冒充或重传以前的连接，也即防止伪造连接初始化这种类型的攻击。
这种鉴别服务既可以是单向的，也可以是双向的。
访问控制（AccessContr01）访问控制服务可以防止未经授权的用户非法使用系统资源。
这种服务不仅可以提供给单个用户，也可以提供给封闭的用户组中的所有用户。
数据保密（DataConfidentiality）数据保密服务的目的是保护网络中各系统之间交换的数据，防止因数据被截获而造成的泄密。
数据完整性（DataIntegrity）这种服务用来防止非法实体对用户的主动攻击（对正在交换的数据进行修改、插入，使数据延时以及丢失等），以保证数据接收方收到的信息与发送方发送的信息完全一致。
不可否认性这种服务有两种形式。
第一种形式是源发证明，即某一层向上一层提供的服务，它用来确保数据是由合法实体发出的，它为上一层提供对数据源的对等实体进行鉴别，以防假冒。
第二种形式是交付证明，用来防止发送数据方发送数据后否认自己发送过数据，或接收方接收数据后否认自己收到过数据。
审计管理对用户和程序使用资源的情况进行记录和审查，可以及早发现入侵活动，以保证系统安全，并帮助查清事故原因。
可用性保证信息使用者都可得到相应授权的全部服务。

<<网络安全技术内幕>>

编辑推荐

《网络安全技术内幕》适合从事网络安全工作的工程技术人员、网管员和大专院校师生阅读，对网络爱好者也有很好的指导作用。

<<网络安全技术内幕>>

版权说明