<<网络安全原理与应用>>

图书基本信息

书名：<<网络安全原理与应用>>

13位ISBN编号：9787121171901

10位ISBN编号：7121171902

出版时间：2012-6

出版时间：电子工业出版社

作者：陈志德，许力　主编

页数：344

字数：580000

<<网络安全原理与应用>>

内容概要

本书主要系统地介绍了网球安全的基本原理和基本应用。
全书主要分理论篇和试验篇，共19章，主要包括引论、对称密码、公钥密码、安全协议、操作性也安全、多媒体信息安全、防火墙、入侵检测、病毒原理与防范、数据库安全技术、无限网络安全等网络安全原理，以及Windows
Server服务器安全配置试验、Web检测试验、密码试验、系统扫描试验、网络监控与嗅探试验、破译与攻击试验、防火墙试验和入侵检测试验等网络安全实验与应用。

<<网络安全原理与应用>>

书籍目录

章节摘录

版权页： 插图： 教学提示：随着网络技术的日益更新，计算机网络已从单一化的发展逐渐形成复杂的网络系统。
网络资源的共享为用户带来方便的同时，也使网络产生内部攻击、外部攻击和误操作的安全问题，入侵检测正是作为一种积极主动的安全防护技术应用于网络。
作为网络安全的主要技术之一，入侵检测技术通过对计算机网络中信息的收集与分析，采取相应的安全策略，使网络的安全的风险能有效地降低。
教学目标：掌握入侵检测系统的基本概念与定义，了解入侵检测发展的历程与分类方法，理解入侵检测系统的体系结构与检测技术，并通过对入侵检测系统实例Snort的分析，对入侵检测系统有了一个比较全面的理解。
8.1 入侵检测概述 8.1.1 入侵检测的必要性 传统的网络安全技术主要包括：加密和数字签名机制、身份认证与访问控制机制、认证授权、安全审计、系统脆弱性检测、构筑防火墙系统等。
这些技术都发展得比较成熟，特别是防火墙技术，它能有效地控制内部网络与外部网络之间的访问及数据传送，从而达到保护内部网络的信息不受外部非授权用户的访问和过滤信息的目的，防火墙配置的多样性和防护的有效性使它成为网络安全防线的中流砥柱。
然而任何一种单一的安全技术都并非万能，而且随着攻击者经验日趋丰富，攻击工具与手法的日趋复杂多样，传统单一的安全技术和策略已经无法满足对安全高度敏感的部门的需要。
因此，网络安全的防卫必须采用一种纵深的、多样的手段，形成一个多层次的防护体系，不再是单一的安全技术和安全策略，而是多种技术的融合，关键是各种安全技术能够起到相互补充的作用，这样，即使当某一种措施失去效能时，其他的安全措施也能予以弥补。
传统的安全技术虽然取得了很大的成效，但是它也存在一些固有的缺陷，比如访问控制可以拒绝未授权用户的访问，却并不能防止已授权访问用户获取系统中未授权信息；防火墙可以将危险挡在外面，却无法挡住内部的入侵。
从网络安全的角度看，公司的内部系统被入侵、破坏与泄密是一个严重的问题，以及由此引出的更多有关网络安全的问题都应该引起重视。
据统计，全球80%以上的入侵来自于内部。
因此，传统的安全技术更多的是一种基于被动的防护，而如今的攻击和入侵要求主动地检测、发现和排除安全隐患，正是在这样的环境下，入侵检测系统开始崭露头角，成为安全市场上和研究上新的热点，不仅愈来愈多地受到人们的关注，而且已经开始在各种不同的环境中发挥越来越重要的作用。

<<网络安全原理与应用>>

编辑推荐

《高等学校计算机规划教材:网络安全原理与应用》可作为大专院校网络安全、信息安全及计算机、电子、通信等领域相关专业的教学用书，也可供相关领域从业人员及科研人员参考。
《高等学校计算机规划教材:网络安全原理与应用》实现了理论与实践相结合，是获得网络安全知识的重要途径。

<<网络安全原理与应用>>

版权说明