<<网络安全实用教程>>

图书基本信息

书名：<<网络安全实用教程>>

13位ISBN编号：9787115248879

10位ISBN编号：7115248877

出版时间：2011-4

出版时间：人民邮电

作者：刘远生 编

页数：302

<<网络安全实用教程>>

内容概要

本书介绍了计算机网络安全的基本知识、安全技术和应用实践。
主要内容可分为三大部分：第一部分为网络安全基础，主要介绍了网络安全的基本知识、安全风险和安全威胁、OSI安全体系结构等；第二部分介绍了网络安全涉及的各种安全技术，如密码技术、防火墙、安全认证、EFS、IPSec、黑客攻击及防范、漏洞扫描、网络监听、入侵检测、病毒防治等；第三部分为网络安全应用实践，主要介绍了一些比较重要的网络产品(如路由器、交换机、服务器、VPN及软件工具)的安全配置及其技术应用。

本书内容丰富，概念清楚，语言精练，通俗易懂，理论联系实际，易于教学。
本书可作为高等院校计算机、通信和信息安全等专业的教材，也可以作为网络安全工程师、网络管理员和计算机用户的参考用书，以及网络安全培训教材。

作者简介

刘远生，现任上海交通大学技术学院常务副院长/教授，院职称评审组组长，院教学委员会主任。
参与国家自然科学基金项目“ 数据加密标准的应用研究 ”和“ 信道编码理论在VLSI信号处理中的应用 ”的研究。
主持人民银行总行科研项目“ 金融电子化的发展对各层次计算机专业人才需求的研究 ”和“ 基于计算机网络的多媒体CAI教学环境的研究 ”。

<<网络安全实用教程>>

书籍目录

章节摘录

版权页：插图：防护是根据系统可能出现的安全问题采取一些预防措施，通过一些传统的静态安全技术及方法来实现。
通常采用的主动防护技术有：数据加密、身份验证、访问控制、授权和虚拟专用网技术等；被动防护技术有：防火墙技术、安全扫描、入侵检测、路由过滤、数据备份和归档、物理安全、安全管理等。
安全防护是P2DR模型中最重要的部分，通过它可以预防大多数的入侵事件。
防护包含系统安全、网络安全和信息安全三种防护类型。
系统安全防护指操作系统的安全防护，即各个操作系统的安全配置、使用和打补丁等，不同操作系统有不同的防护措施和相应的安全工具。
网络安全防护指网络管理的安全及网络传输的安全。
信息安全防护指数据本身的保密性、完整性和可用性，数据加密就是信息安全防护的重要技术。
（3）Detection（检测）攻击者如果穿过防护系统，检测系统就需要将其检测出来，如检测入侵者的身份、攻击源点和系统损失等。
防护系统可以阻止大部分的入侵事件，但不能阻止所有的入侵事件，特别是那些利用新的系统缺陷、新的攻击手段的入侵。
如果入侵事件发生，就要启动检测系统进行检测。
检测与防护有根本的区别。
防护主要是修补系统和网络的缺陷，增强系统安全性能，从而消除攻击和入侵的条件，避免攻击的发生；而检测是根据入侵事件的特征找出可能发生的入侵。
因黑客往往是利用网络和系统缺陷进行攻击的，所以入侵事件的特征一般与系统缺陷的特征有关。
在P2DR模型中，防护和检测有互补关系。
如果防护系统可靠，绝大部分入侵事件被阻止，那么检测系统的任务就减少了。

<<网络安全实用教程>>

编辑推荐

《网络安全实用教程》在介绍网络安全基本知识的基础上，重点介绍了网络安全技术及其应用。
各章在介绍的相关网络安全技术后都配以相应的应用实例和实践内容，强调理论联系实际，体现培养学生的网络管理、安全技术应用能力和实践操作技能的特色，旨在培养学生的实践动手能力和解决问题的实际操作技能。
《网络安全实用教程》对网络安全的理论和技术原理等介绍适度，典型实例的应用性和可操作性强，章末配有的思考题、习题和实验题，便于学生学习和实践。
重点介绍网络安全技术及其应用配以丰富的应用实例和实践内容培养学生网络管理、安全技术应用能力和实践操作技能

<<网络安全实用教程>>

版权说明