

<<企业网络安全致胜宝典>>

图书基本信息

书名：<<企业网络安全致胜宝典>>

13位ISBN编号：9787121050954

10位ISBN编号：7121050951

出版时间：2007-10

出版时间：电子工业

作者：郭鑫

页数：315

字数：394

版权说明：本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问：<http://www.tushu007.com>

<<企业网络安全致胜宝典>>

内容概要

本书从介绍信息安全基本概念开始，介绍信息安全建设可以依据的各类体系结构，堪称网络安全致胜宝典。

书中详细地讲解企业网络的个人计算机安全、企业服务器安全、网站程序安全、增强企业网络病毒的免疫力、木马如何控制企业网络、黑客入侵网络方式、网络安全产品、安全风险管理和企业应急响应案例等，最后得出结论：构筑企业网络安全体系，应该融合技术和管理的內容，并充分考虑到人、流程和工具这3个因素综合作用所构建的体系结构。

书中对网络管理员比较关心的大型网络入侵响应、犯罪取证和入侵事件的调查过程，做了全面的流程分析和操作，以使网络管理员改掉不良习惯，把网络安全风险降到最低限度。

通过阅读本书，网络管理员及相关读者，一定能够更加有效地对网络进行安全加固和维护。

本书适合网络管理员、系统管理员阅读，对网络爱好者、网络使用者也有较高的参考价值。

<<企业网络安全致胜宝典>>

书籍目录

第1章 网络安全基础	1.1 认识IP地址	1.2 端口	1.3 TCP/IP	1.4 网络常用指令	1.5 网络专用
1.6 黑客入侵流程	第2章 增强企业网络病毒的免疫力	2.1 计算机病毒的分类	2.2 计算机病毒传播途径	2.3 病毒技术	2.4 预防病毒的方法
2.5 病毒的诊断原理	2.6 病毒消除方法	2.7 病毒消除原理	第3章 神秘的特洛伊木马	3.1 什么是特洛伊木马	3.2 特洛伊木马的特性
3.3 特洛伊木马的种类	3.4 木马启动方式	3.5 木马隐藏方式	3.6 木马伪装方式	3.7 揭开木马的神秘面纱	3.8 透
3.9 木马开发技术	3.10 找出控制木马的黑客	第4章 操作系统漏洞隐患	4.1 IP默认共享漏洞应用	4.2 Unicode与二次解码漏洞的应用	4.3 IDQ溢出漏洞应用
4.4 Webdav溢出漏洞应用	4.5 SQL空密码漏洞应用	4.6 DDoS拒绝服务攻击	4.7 清除攻击后的痕迹	第5章 企业服务	5.1 Windows Server 2003安全配置
5.2 Linux系统安全配置	5.3 FreeBSD系统安全配置	5.4 A系统安全配置	5.5 Solaris系统安全配置	第6章 企业网站安全	6.1 什么是数据库注入
6.2 初识数据库注入技术	6.3 如何防范ASP数据库	第7章 安全网络所需的安全产品	7.1 防泄密网安全产品	7.2 防火墙	7.3 入侵检测系统
7.4 防垃圾邮件系统	7.5 防DDoS系统	第8章 安全风险	8.1 安全风险	8.2 安全风险	8.3 安全风险
8.4 评估风险	8.5 实施决策支持	第9章 企业应急响应案例	9.1 某网通入侵响应案例	9.2 某企业病毒响应	9.3 某企业犯罪取证案例
9.4 某企业入侵响应案例					

编辑推荐

随着IT应用的日益普及，计算机网络技术广泛应用于各个行业，形成各自网络，为资源共享、信息交换和分布处理提供了广而又良好的环境。

计算机网络具备分布广域性、结构开放性、资源共享性和信道公用性的特点。

因此，在增加网络使用性的同时，不可避免地带来了系统的脆弱性，使其面临着严重的安全问题。

现在，随着计算机网络资源共享的进一步加强，随之而来的网络安全问题日益突出，人们对计算机信息安全的要求也越来越高。

计算机网络技术的普及和随之而来的网络完全问题，使得计算机网络安全保护变得越来越重要。

黑客的攻击技术、网络通信安全技术策略和管理机制等，直接影响网络安全，已被越来越多的网络用户所关注

<<企业网络安全致胜宝典>>

版权说明

本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问:<http://www.tushu007.com>