

<<信息安全之个人防护>>

图书基本信息

书名：<<信息安全之个人防护>>

13位ISBN编号：9787121063374

10位ISBN编号：7121063379

出版时间：2008-8

出版时间：电子工业出版社

作者：国家反计算机入侵和防病毒研究中心 编

页数：305

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>

<<信息安全之个人防护>>

内容概要

本书围绕个人用户使用计算机和网络过程中遇到的安全问题，介绍了信息安全基础知识和安全威胁，结合个人用户常使用的Windows XP系统，介绍了Windows XP系统的基本安全设置、文件安全操作、数据安全保护、系统进程管理、网络故障差错和安全模板的配置与管理知识。

围绕用户使用Internet和网络应用服务，介绍了Internet网络及应用遇到的安全问题和防范技能，帮助用户有效防范计算机病毒和木马的攻击威胁，能够安全使用常见的计算机远程管理手段，帮助用户提高信息网络安全防范意识，掌握个人计算机及网络安全防范技能，防止常见的网络攻击手段对信息系统的侵害。

本教程内容适合于信息系统的普通用户培训和学习，如组织中的管理人员、财务和市场业务人员、技术支持人员，通过学习提高个人对信息安全威胁的防护意识和技能。

本教程同时也可供大中专院校和职业技术学校的相关专业，作为信息安全专业基础课程教材，为进一步学习安全专业课程奠定基础。

<<信息安全之个人防护>>

书籍目录

第1章 信息安全概述	1.1 信息与信息资产	1.1.1 信息的定义	1.1.2 信息的特点	1.2 信息安全基本概念
	1.2.1 信息安全问题的发展	1.2.2 信息安全的定义	1.2.3 信息安全的基本属性	1.3 信息安全典型事件
	1.3.1 计算机病毒事件	1.3.2 黑客攻击事件	1.3.3 垃圾邮件的骚扰	1.3.4 网络金融账户失窃案件
	1.3.5 网络不良信息资源的毒害	1.4 信息安全问题的根源	1.4.1 物理安全问题	1.4.2 方案设计的缺陷
	1.4.3 系统的安全漏洞	1.4.4 人的因素	1.5 信息安全解决之道	1.5.1 信息安全技术体系结构
	1.5.2 信息安全管理	1.5.3 信息安全法律法规	1.6 信息安全个人防护	1.6.1 形成良好的计算机操作规范
	1.6.2 谨防“网络钓鱼”欺骗	1.6.3 个人隐私保护	1.7 小结 习题1	第2章 Windows XP系统基本安全
	2.1 什么是操作系统	2.2 系统启动与登录	2.2.1 系统启动过程	2.2.2 交互式登录的系统组件
	2.2.3 启动的安全模式	2.2.4 启动的隐藏之处	2.3 账户与特权	2.3.1 账户与口令安全
	2.3.2 账号安全策略	2.3.3 合理管理用户密码	2.4 默认安装服务的问题	2.4.1 查看正在启用的服务项目
	2.4.2 必须禁止的服务	2.4.3 可以禁止的服务	2.5 系统优化与维护	2.5.1 开机优化
	2.5.2 硬件优化	2.5.3 磁盘碎片整理	2.5.4 虚拟内存	2.5.5 Windows系统优化工具
	2.6 常用的安全措施	2.6.1 禁用“开始”菜单命令	2.6.2 桌面相关选项的禁用	2.6.3 禁止访问“控制面板”
	2.6.4 及时使用Windows Update更新系统	2.6.5 个人防火墙	2.7 小结习题2	第3章 Windows XP系统文件安全
	3.1 什么是文件系统	3.1.1 文件系统的格式	第4章 Windows XP系统数据安全
	第5章 Windows XP系统高阶安全	第6章 Internet上网安全	第7章 Internet网络应用安全	第8章 计算机木马防范
	第9章 计算机病毒防范	第10章 计算机远程管理		

章节摘录

第1章 信息安全概述1.3 信息安全典型事件1.3.2 黑客攻击事件“黑客”一词由英语Hacker音译而来，是指专门研究、发现计算机和网络漏洞的计算机爱好者。

他们伴随着计算机和网络的发展而产生成长。

黑客对计算机有着狂热的兴趣和执着的追求，他们不断地研究计算机和网络知识，发现计算机和网络中存在的漏洞，喜欢挑战高难度的网络系统并从中找到漏洞，然后向管理员提出解决和修补漏洞的方法。

但是到了今天，黑客一词已被用于泛指那些专门利用计算机搞破坏或恶作剧的家伙，对这些人的正确英文叫法是Cracker，有人也翻译成“骇客”或是“入侵者”，也正是由于入侵者的出现玷污了黑客的声誉，使人们把黑客和入侵者混为一谈，黑客被人们认为是在网上到处搞破坏的人。

本文向读者介绍黑客攻击事件，就属于非法入侵。

虽然个人电脑很少成为黑客攻击的终极目标，但由于黑客会通过程序（网上一般称为“僵尸程序”）控制普通用户的个人电脑作为黑客攻击过程的跳板，这种被黑客控制了电脑，被称为“肉鸡”，由许多“肉鸡”组成的计算机网络称为“僵尸网络”，它们常被用来当做垃圾邮件发送的中继站、放置恶意网站或者发起攻击。

2005年，国家计算机网络应急技术处理协调中心（CNCERT/CC）发现超过5000个节点规模的僵尸网络有143个，其中最大的单个僵尸网络节点超过15万个。

2005年境外合作CERT'组织发现一个超过120万个节点的僵尸网络，其中我国被控制的IP数量达到29万个。

<<信息安全之个人防护>>

编辑推荐

生活在信息社会的人们，沉浸在信息化技术带来的便捷体验的同时。病毒、黑客攻击、计算机网络犯罪也开始向人类发起了挑战。当越来越依赖信息系统，生活越来越信息化，信息安全问题逐渐成为人们生活和工作中的重要威胁，这时候，选择逃避已是无路可退，唯有武装自己，提高信息安全防范意识和技能，做好个人防护，才是最有效的安全解决出路。

学习《安全技术大系·INSPC认证培训教程系列：信息安全之个人防护》，您将可以获得最佳的安全基本技能，应付日常安全问题，可以得心应手！

内容特色：知己知彼，了解操作系统安全奥秘，不再因操作系统莫名其妙死机、运行变慢而束手无策！

网络冲浪、信息搜索，不再担心网络黑手窃取您的个人隐私！

轻松玩转“电子邮件、网络聊天、网络购物”等应用服务，不必担心垃圾信息和网络诈骗的侵犯！

从计算机中揪出潜伏的木马程序和病毒，让它们无处容身！

远程连接。

安全控制计算机，修身“网络达人”。

<<信息安全之个人防护>>

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>