

计算机网络安全 知识问答

李桂玲 主 编 ○

吕家国 徐洪志 副主编 ○



中国电力出版社

www.infopower.com.cn

要 索 容 内

计算机网络安全 知识问答

李桂玲 主 编 ○

吕家国 徐洪志 副主编 ○

王舒晟 杨堃社 张爱军 参 编 ○



中国电力出版社

www.infopower.com.cn

内 容 提 要

本书分为基础篇和应用篇两部分。在基础篇中,主要解答了计算机及网络安全的基础知识及病毒、黑客、防火墙、防病毒软件的相关问题。在应用篇中,主要以实例的方式讲解了计算机的各种安全设置和遇到病毒、黑客攻击时的处理方法及对策。

本书适合作为高等院校和高职院校培养计算机应用型人才的教材或教学参考书,以及相关培训用书,也适合于从事计算机网络安全管理、安全设计的人员阅读。

图书在版编目(CIP)数据

计算机网络安全知识问答 / 李桂玲主编. —北京: 中国电力出版社, 2008.6
ISBN 978-7-5083-7168-9

I. 计… II. 李… III. 计算机网络-安全技术-问答 IV. TP393.08-44

中国版本图书馆 CIP 数据核字 (2008) 第 060977 号

责任编辑: 杜长清
责任校对: 崔燕菊
责任印制: 郭华清

书 名: 计算机网络安全知识问答
编 著: 李桂玲

出版发行: 中国电力出版社

地址: 北京市三里河路 6 号 邮政编码: 100044

电话: (010) 68362602

传真: (010) 68316497

印 刷: 汇鑫印务有限公司

开本尺寸: 185mm × 260mm 印 张: 11.25

字 数: 246 千字

书 号: ISBN 978-7-5083-7168-9

版 次: 2008 年 6 月北京第 1 版

印 次: 2008 年 6 月第 1 次印刷

印 数: 0001—3000 册

定 价: 19.00 元

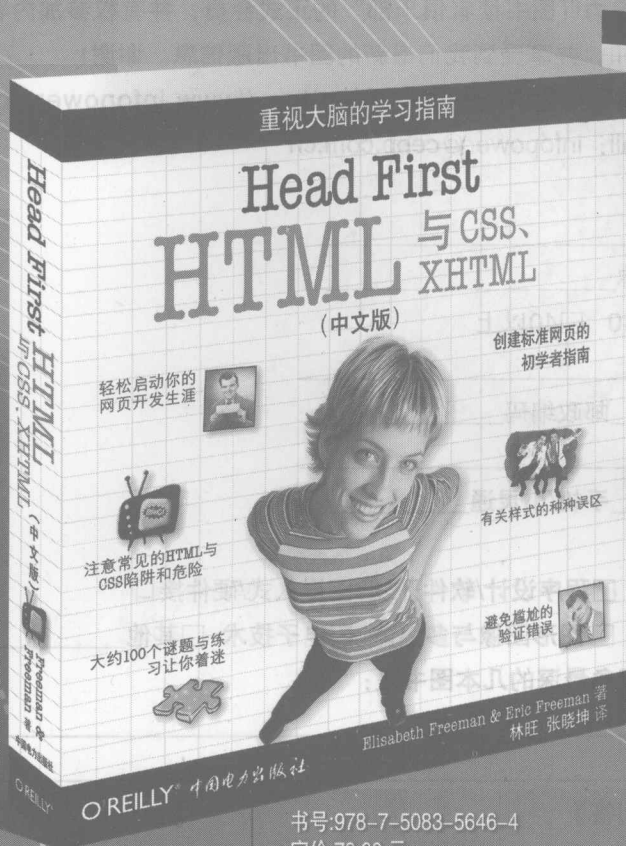
敬 告 读 者

本书封面贴有防伪标签,加热后中心图案消失
本书如有印装质量问题,我社发行部负责退换

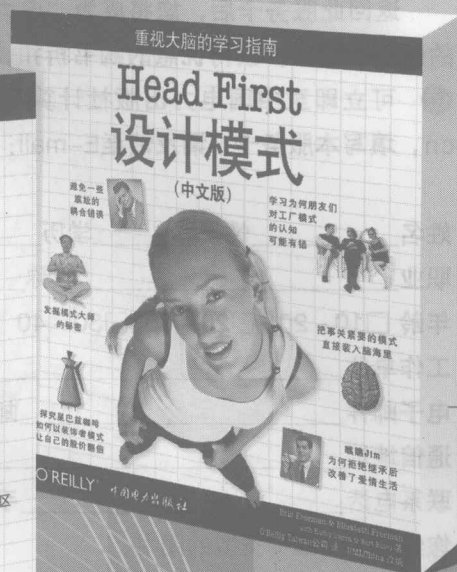
版 权 专 有 翻 印 必 究

风靡全球、屡获大奖

中文版 Head First 系列



书号:978-7-5083-5646-4
定价:79.00 元



书号:978-7-5083-5393-7
定价:98.00 元

2007互动、当当IT类图书
销量第一

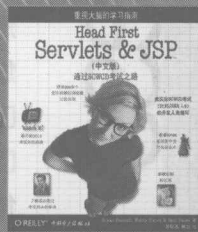
妙趣横生，
学习乐在其中



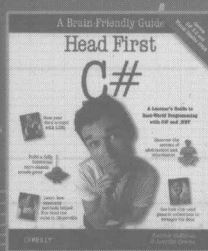
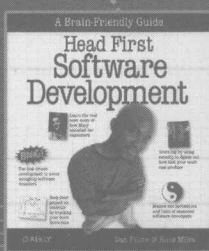
书号:7-5083-3889-8
定价:79.00 元



书号:978-7-5083-4498-0
定价:79.00 元



书号:7-5083-4284-4
定价:98.00 元



即将出版

权威、经典
源自专业品质



中国电力出版社
www.infopower.com.cn

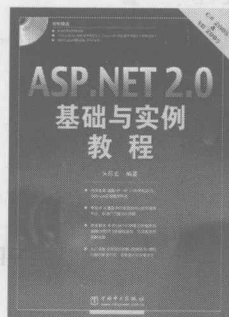
地址:北京市西城区三里河路6号
邮编:100044
电话:010-58383336

新书新势力 精编版!

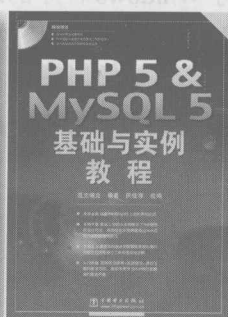
HOT!

学习Web应用开发 就从这里开始

Learning Web application development from here



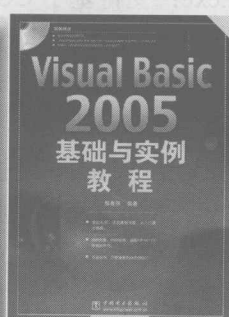
978-7-5083-5375-8
定价: 39.80元



978-7-5083-5367-8
定价: 39.00元

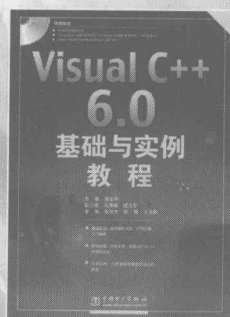


978-7-5083-5641-9
定价: 39.00元

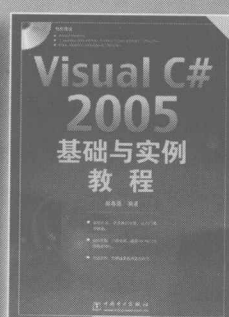
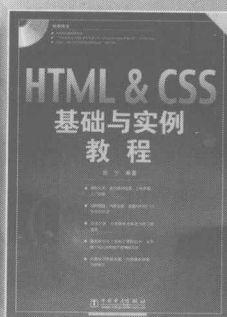


978-7-5083-5659-4
定价: 32.00元

零起点,
内容全面,
实例丰富,
一学就会



978-7-5083-5657-0
定价: 35.00元

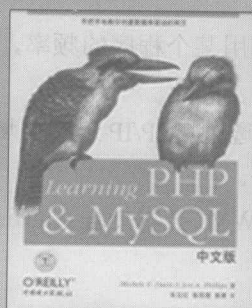


978-7-5083-6133-8
定价: 35.00元

外版经典 重装上阵



978-7-5083-5152-0
定价: 128.00元



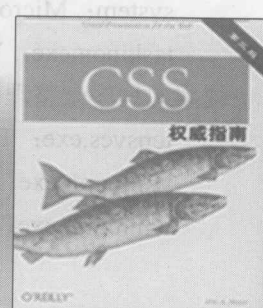
手把手教你创建数据库驱动的网页

978-7-5083-5380-7
定价: 36.00元



JSP2.0 & JSTL 1.1

978-7-5083-2273-8
定价: 79.00元



CSS权威指南第三版
网站的视觉展示



中国电力出版社
www.infopower.com.cn

中国电力出版社计算机与艺术图书中心
地址: 北京市西城区三里河路6号 (100044)
电话: 010-88519189/332 传真: 010-88518169
E-mail: ky_market@epw.com.cn 网址: www.infopower.com.cn

中国电力出版社读者服务卡

非常感谢您选择中国电力出版社计算机与艺术类图书，您的支持是对我们工作最大的肯定！请对我们的图书提出宝贵的意见和建议，以帮助我们不断提升图书质量，继续推出更符合读者需求、更实用、品质更高的计算机与艺术设计类图书。

返回此服务卡后，您将成为“电力IT图书读者俱乐部”的正式会员，并有权参加内容丰富的俱乐部活动，获得优惠的购书折扣，并享受到我们最新的图书出版信息。谢谢！

● 可立即至中国电力出版社计算机与艺术图书中心网站<http://www.infopower.com.cn>，填写本服务卡，请反馈至E-mail: infopower@cepp.com.cn

姓名_____性别_____学历_____

职业_____职称_____

年龄 ☐ 10~20 ☐ 20~30 ☐ 30~40 ☐ 40以上

工作单位_____

电子邮件_____邮政编码_____

通信地址_____

联系电话_____手机/小灵通_____

您经常阅读哪种类型的图书：

☐ 操作系统 ☐ 数据库 ☐ 网络/通信 ☐ 程序设计/软件开发 ☐ 嵌入式/硬件接口

☐ 工业设计 ☐ Web设计 ☐ 自动化 ☐ 图形图像与多媒体 ☐ 电子技术 ☐ 其他_____

您对中国电力出版社计算机类图书印象最深的几本图书是：

本书书名：《计算机网络安全知识问答》

您对本书的评价：

您认为计算机类图书的价格定位在多少合适？_____

您最希望我们出版哪些内容的图书？

☐ 操作系统 ☐ 数据库 ☐ 网络/通信 ☐ 程序设计/软件开发 ☐ 嵌入式/硬件接口

☐ 工业设计 ☐ Web设计 ☐ 自动化 ☐ 图形图像与多媒体 ☐ 电子技术 ☐ 其他_____

您希望成为我们的作译者吗？

您准备编写的图书名称：_____

您可以翻译的图书类型（从事的专业或研究方向）_____

您推荐引进出版的_____

您的其他建议_____

地址：北京市三里河路6号中国电力出版社计算机与艺术图书中心（100044）

电话：010-58383411 传真：010-58383267 E-mail: infopower@cepp.com.cn

新书查询、网上购书、售后资讯下载、读者俱乐部最新动态，敬请访问www.infopower.com.cn



前 言

计算机网络的不断发展,给人们的生活和工作带来了极大的方便,你可以通过网络查阅资料、购物、发送订单等,甚至不用出家门就可以在网上完成你能想到的任何工作。但是,由于计算机网络的安全问题,限制了你想做的许多工作。有些事情想做而不敢做,有些事情做了,却带来了一系列的隐患。可以说网络是一把双刃剑,能给我们的生活和工作带来方便,也能给我们的生活和工作带来困扰。

针对日益突出的网络安全问题,计算机操作系统本身在设计时对安全选项的考虑越来越多,计算机操作系统中有许多安全选项是可以根据用户的不同需要而设置的,同时针对安全的第三方防护系统也越来越多。但事实上,许多用户经常遭到黑客和病毒的攻击,其主要原因是用户缺乏必要的安全知识,不知道怎样安全地使用计算机。本书的作者是计算机网络管理人员,从事计算机及网络安全管理工作多年,非常了解普通计算机用户经常遇到的安全问题。他们在工作中经常帮助用户解决一些安全问题,因此,积累了一些应对计算机病毒及黑客攻击的方法,同时把用户经常需要解答的一些安全问题整理汇总在一起,在此献给广大的计算机用户,以帮助大家安全地使用计算机网络。

本书分为基础篇和应用篇两部分。在基础篇中,通过问答的方式为用户解答一些常用的计算机网络安全基础知识,以帮助用户树立计算机网络安全的基本概念。在应用篇中,以实例的方式介绍了许多在实际使用计算机过程中遇到安全问题的处理方法,介绍了怎样设置计算机的各种安全选项以保证计算机的安全使用。

在本书的编写过程中,得到了许多朋友和同事的大力帮助,在此表示感谢!

由于作者水平有限,书中难免有疏漏之处,恳请读者批评指正。

编 者

2008年1月



目 录

前 言

第一部分 基础篇

第 1 章 计算机及网络安全常识	2
1-1 什么是计算机网络？它主要功能有哪些？	2
1-2 计算机网络按其覆盖范围的不同通常分为哪几类？各类的特点是什么？	2
1-3 计算机网络的拓扑结构主要有哪些？	3
1-4 什么是网络协议？常用的网络协议有哪些？	3
1-5 什么是 TCP/IP？	3
1-6 针对 TCP/IP 安全设计缺陷的攻击有哪些？	4
1-7 什么是 MAC 地址？	5
1-8 什么是 IP 地址？	5
1-9 IPv6 提供了哪些网络安全机制？	5
1-10 什么是域名？	6
1-11 什么是域名服务（DNS）？	7
1-12 什么是 WWW 服务？	7
1-13 什么是超级链接？	7
1-14 什么是 HTML 语言？	8
1-15 什么是文件传输（FTP）服务？	8
1-16 什么是电子邮件（E-mail）服务？	8
1-17 什么是远程登录（Telnet）服务？	9
1-18 什么是电子布告栏（BBS）服务？	9
1-19 什么是因特网？	9
1-20 什么是端口号？	10
1-21 常用端口号有哪些？	10
1-22 什么是 Cookies？	10
1-23 后缀为 DLL 的文件是什么文件？	11
1-24 什么是进程？	11
1-25 什么是计算机安全？其特性是什么？	11
1-26 国际通用的计算机安全标准是什么？	12

1-27	我国的计算机安全标准是怎样划分的？	13
1-28	什么是计算机网络安全？	14
1-29	计算机网络安全特性包括哪些方面？	15
1-30	对计算机网络安全的威胁主要来自哪些方面？	16
1-31	常用的网络安全机制有哪些？	17
1-32	常用的网络安全防范手段有哪些？	18
1-33	什么是加密技术？	19
1-34	网络传输加密方法有哪些？	19
1-35	什么是链路加密？	19
1-36	什么是节点对节点加密？	20
1-37	什么是端对端加密？	20
1-38	网络存储加密方法有哪些？	20
1-39	网络身份认证方法有哪些？	21
1-40	什么是防火墙？它是如何确保网络安全的？	21
1-41	防火墙可分为哪几类？	22
1-42	防火墙有哪些局限性？	22
1-43	网络防火墙有什么功能？	22
1-44	如何在个人计算机上正确配置网络防火墙？	23
1-45	选择防火墙应遵循的原则是什么？	23
1-46	什么是 VPN？	24
1-47	Web 服务器记录用户的哪些信息？	24
1-48	什么是入侵检测？	24
1-49	什么叫数据包监测？它有什么作用？	24
1-50	什么是“蜜罐”技术？	25
1-51	什么是无线局域网（WLAN）技术？	25
1-52	什么是 802.11 标准？	25
1-53	无线网络存在的安全问题主要有哪些？	25
1-54	什么是访问控制？	26
1-55	访问控制方法有哪些？	26
1-56	什么是迅驰技术？	26
1-57	什么是蓝牙技术？	26
第 2 章 计算机病毒及其防护		28
2-1	什么是计算机病毒？	28
2-2	计算机病毒由哪些部分组成？	28
2-3	什么是计算机病毒对抗？	28
2-4	计算机病毒有哪些主要特点？	29
2-5	计算机病毒分为哪几类？	30
2-6	什么是引导型病毒？	30
2-7	什么是文件型病毒？	30
2-8	什么是宏病毒？	30
2-9	什么叫蠕虫？	31
2-10	什么是操作系统型病毒？	31

2-11	什么是混合型病毒？	31
2-12	什么是网络病毒？	31
2-13	网络病毒有哪些特点？	32
2-14	什么是电子邮件病毒？	33
2-15	计算机病毒的主要危害有哪些？	33
2-16	什么是超级计算机病毒？	33
2-17	什么是病毒自动生产技术？	33
2-18	最流行的病毒捆绑器有哪些？	34
2-19	什么是手机病毒？	34
2-20	杀毒软件的主要功能及组成是什么？	35
2-21	什么是病毒库？	35
2-22	什么是扫描引擎？	35
2-23	为什么需要经常更新扫描引擎和病毒库？	35
第3章 计算机黑客攻击及其防护		36
3-1	什么是计算机黑客？	36
3-2	什么是计算机犯罪？	36
3-3	什么是网络安全漏洞？为什么会存在网络安全漏洞？	36
3-4	网络安全漏洞是怎样形成的？	38
3-5	网络安全漏洞可能造成的威胁有哪些？	38
3-6	黑客常用的攻击手段有哪些？可分为哪几类？	41
3-7	什么是主动攻击与被动攻击？	41
3-8	什么是本地攻击与远程攻击？	41
3-9	什么是窃密性攻击与破坏性攻击？	41
3-10	什么是系统型攻击与数据型攻击？	42
3-11	口令破解有哪些模式？	42
3-12	什么是口令破解器？	42
3-13	软件中的口令是如何被破解的？	42
3-14	什么是网络扫描？	43
3-15	网络扫描工具有哪些？	43
3-16	什么是网络窃听？	44
3-17	什么是网络监听？网络监听的目的是什么？	44
3-18	局域网监听是如何实现的？	44
3-19	常用的嗅探软件有哪些？	45
3-20	什么是密码破译？	45
3-21	什么是口令攻击？	45
3-22	什么是拒绝服务攻击？	46
3-23	拒绝服务攻击的方式有哪些？	46
3-24	什么是DDoS？	47
3-25	什么是僵尸网络？其特征是什么？	48
3-26	什么是服务端口攻击？	48
3-27	电子邮件的攻击方式有哪些？	48
3-28	网络内部的ARP攻击是指什么？	48

3-29	什么叫欺骗攻击? 它有哪些攻击方式?	49
3-30	什么是特洛伊木马攻击?	49
3-31	特洛伊木马是如何工作的?	49
3-32	常见的特洛伊木马程序有哪些? 可分为哪几类?	50
3-33	什么是逻辑炸弹攻击?	50
3-34	什么是后门?	51
3-35	什么是后门攻击?	51
3-36	什么是缓冲区溢出?	51
3-37	什么是缓冲区溢出攻击?	52
3-38	缓冲区溢出攻击的危害是什么?	52
3-39	什么是网络欺骗攻击? 可分为哪几类?	52
3-40	什么是 IP 欺骗?	52
3-41	什么是电子邮件欺骗?	53
3-42	什么是 DNS 欺骗?	53
3-43	什么是 Web 欺骗?	53
3-44	什么是黑客破解密码的穷举法?	53
3-45	什么是黑客解密码的字典法?	53
3-46	什么是黑客破解密码的猜测法?	54
3-47	网上共享资源安全性设置常存在哪些问题?	54
3-48	什么是网络钓鱼?	54
3-49	网络钓鱼的手段和危害有哪些?	55
3-50	什么是流氓软件?	55
3-51	流氓软件的分类及其危害是什么?	55
3-52	什么是网络入侵检测?	56
3-53	黑客攻击分为几个阶段进行?	56
3-54	网络安全防范体系设计应遵循什么准则?	57
3-55	因特网的不安全因素有哪些?	59
第 4 章 计算机电磁泄漏及其防护		60
4-1	什么是计算机电磁泄漏?	60
4-2	计算机电磁泄漏有哪些危害?	60
4-3	什么是计算机电磁辐射标准?	60
4-4	什么是 CISPR 标准?	61
4-5	计算机电磁泄漏防护主要有哪些措施?	61
4-6	电磁屏蔽主要有哪些措施?	63
4-7	在计算机网络建设过程中怎样实现电磁泄漏防护?	64
第二部分 应用篇		
第 5 章 系统与网络		66
5-1	怎样启动和关闭服务?	66
5-2	计算机中哪些服务可以停止?	67
5-3	为什么计算机中存在共享文件夹不安全?	68

101	5-4 如何加密、隐藏“共享”文件夹？	68
101	5-5 怎样找到计算机上隐藏的共享文件夹？	69
101	5-6 Windows 2000/XP 中隐藏共享 IPC\$ 的危害是什么？	69
101	5-7 如何禁止建立空链接？	70
101	5-8 怎样清除计算机中存在的默认共享？	70
101	5-9 如何删除硬盘上的“怪文件”？	71
101	5-10 如何设置计算机的三级密码？	72
101	5-11 怎样通过本地安全策略设置安全登录？	73
101	5-12 Windows 的主要安全隐患有哪些？	75
101	5-13 上互联网时通常应注意哪些事项？	75
101	5-14 拨号上网如何提高安全性？	76
101	5-15 如何保护电子邮件安全？	77
101	5-16 上网记录有哪些？如何清除？	77
101	5-17 如何防止计算机 NetBIOS 信息泄密？	81
101	5-18 为什么需要屏蔽掉系统中的 Guest 账户？	82
101	5-19 如何保护 Windows 日志文件？	83
101	5-20 如何禁止开机自动运行某些应用程序？	84
101	5-21 怎样快速查看计算机的 MAC 地址？	84
101	5-22 怎样确保 IP 地址的安全使用？	85
101	5-23 怎样解决 Windows Update 错误号 0x80070424 导致系统不能升级的问题？	86
101	5-24 注册表的作用是什么？怎样防止注册表被修改？	88
101	5-25 怎样禁用注册表编辑器？	88
101	5-26 如何让其他人仅使用计算机上指定的程序？	88
101	5-27 如何设置文件和文件夹的权限？	89
101	5-28 新购置的计算机怎样处理更安全有效？	89
101	5-29 为什么说在计算机上安装多个操作系统存在安全隐患？	91
101	5-30 怎样禁止其他人对桌面进行任意设置？	91
101	5-31 如何去掉桌面上经常跳出来的“信使服务”？	91
101	5-32 怎样更好地发挥屏幕保护程序的作用？	92
101	5-33 怎样隐藏“开始”菜单中的各个项目？	92
101	5-34 怎样禁用“显示属性”对话框？	93
101	5-35 怎样隐藏“控制面板”中的部分“敏感”项目？	93
101	5-36 怎样禁用“控制面板”？	95
101	5-37 怎样禁止使用任务管理器？	95
101	5-38 怎样隐藏桌面上的某些项目？	96
101	5-39 怎样禁用“系统属性”对话框中的各选项卡？	96
101	5-40 怎样禁止建立新的拨号连接？	97
101	5-41 怎样查看计算机在启动时加载了哪些应用程序？	97
101	5-42 怎样禁止他人随意添加、删除打印机或更改打印机设置？	98
101	5-43 怎样利用“冒充法”加密文件？	99
101	5-44 怎样利用“类标识符”加密文件？	100
101	5-45 怎样通过注册表彻底隐藏文件？	100
101	5-46 怎样解决无法显示隐藏文件的问题？	101

5-47	怎样恢复系统中丢失或不正常的“回收站”？	101
5-48	怎样恢复丢失或出错的快速启动工具栏？	101
5-49	怎样恢复任务栏中丢失的输入法标志 En？	102
5-50	怎样恢复任务栏中丢失的小喇叭？	102
5-51	怎样通过更改 VBS 文件的打开方式避免感染脚本病毒？	102
5-52	Windows XP 下修复主页设置的有效方法是什么？	103
5-53	如何关掉笔记本上多余的接口？	103
5-54	如何关闭计算机网络端口？	103
5-55	如何紧急恢复受损的系统？	104
5-56	如何解决 DLL 文件丢失的问题？	106
5-57	如何知道 DLL 文件被几个程序使用？	107
5-58	如何清除 Cookies？	107
5-59	如何利用系统提供的命令监测系统的安全状况？	108
第 6 章 存储设备		111
6-1	文件在磁盘上的存放格式及读写过程是怎样的？	111
6-2	磁盘格式化对磁盘上数据的影响？	112
6-3	为什么磁盘格式化后以及文件被删除后还能恢复出来？	113
6-4	怎样有效彻底删除磁盘上的文件？	113
6-5	使用什么样的磁盘分区比较安全？分区之间怎样转换？	113
6-6	硬盘主引导区有什么作用？如何备份硬盘分区表？	114
6-7	如何隐藏硬盘？	114
6-8	报废软盘怎样处理？	115
6-9	报废硬盘怎样处理？	115
6-10	如何防止移动存储设备泄密？	115
6-11	U 盘坏了应怎样处理？	115
第 7 章 病毒与黑客		116
7-1	如何选择计算机病毒防治产品？	116
7-2	怎样知道 Word 文档是否感染了宏病毒？	116
7-3	怎样避免 Word 文档感染宏病毒？	116
7-4	怎样清除 Word 宏病毒？	117
7-5	怎样防范 Word 文档的个人隐私被他人窃取？	118
7-6	为什么安装杀毒软件后还能感染病毒？	119
7-7	为什么用杀毒软件也不能杀除某些病毒？遇到这种情况怎样处理？	119
7-8	计算机上安装的应用软件为什么会无法打开？	119
7-9	计算机感染病毒的症状一般有哪些？	120
7-10	怎样预防计算机病毒？	120
7-11	怎样清除引导型病毒？	121
7-12	怎样反网络病毒？	122
7-13	为什么 U 盘无法双击打开？	123
7-14	怎样避免感染 U 盘（闪存）病毒？	123
7-15	怎样清除 U 盘病毒？	124

7-16	手机病毒是怎么破坏手机的？	124
7-17	如何防止智能手机病毒？	125
7-18	怎样通过进程列表查看计算机是否中了木马？	125
7-19	怎样判断 Windows 是否被流氓软件侵入？	125
7-20	如何防备网络钓鱼？	126
7-21	怎样找到木马和窃听器？	127
7-22	怎样用组策略防止木马的运行？	128
7-23	怎样全面清除 KL 木马下载器？	129
7-24	什么是 KeyboardGhost，如何清除？	130
7-25	什么是万能钥匙 Xkey？	130
7-26	什么是“冰河”？如何清除？	130
7-27	怎样通过修改注册表避免病毒与黑客的入侵？	131
7-28	为什么不同的计算机上存在的漏洞数量不同？	132
7-29	已知的 Windows XP 家族常见的安全漏洞有哪些？如何堵塞这些漏洞？	133
7-30	计算机安全漏洞造成的威胁有哪些？	134
7-31	怎样堵塞网络安全漏洞？	135
7-32	宽带用户防范“黑客”攻击的方法有哪些？	135
7-33	如何抵御网络扫描？	138
7-34	怎样防止网络窃听？	138
7-35	哪几类密码最危险？	138
7-36	怎样保护口令的安全？	139
7-37	怎样防止电子邮件轰炸？	139
7-38	怎样防止分布式拒绝服务攻击？	139
7-39	怎样防止逻辑炸弹攻击？	139
7-40	怎样防止后门攻击？	140
7-41	怎样防止缓冲区溢出攻击？	140
7-42	怎样防止 IP 欺骗？	140
7-43	怎样防止电子邮件欺骗？	140
7-44	怎样防止 DNS 欺骗？	141
7-45	怎样防止 Web 欺骗？	141
7-46	网上浏览时应注意哪些安全问题？	141
7-47	如何拒绝网络 Ping 入计算机和网络 ICMP 攻击？	142
7-48	如何才能抵御 Telnet 入侵？	145
7-49	如何正确设置软件防火墙？	146
7-50	怎样避免被“黑”？	146
7-51	使用防火墙后是不是就可以避免被“黑”？	147
7-52	陷阱账号的作用是什么？怎样创建陷阱账号？	147
7-53	Carnivore “食肉动物”软件的危害？	147
7-54	什么是 BO2K？BO2K 具体可以对计算机进行哪些远程控制？	147
7-55	如何清除 BO2K？	149
7-56	购买电磁干扰器应注意的问题有哪些？	149
7-57	如何使用系统配置实用程序 msconfig？	149
7-58	常用的网络命令有哪些？怎样使用？	151

151	7-59 怎样使用 netstat 命令?	151
152	7-60 怎样使用 net 命令?	152
159	7-61 怎样使用 ping 命令?	159
159	7-62 怎样使用 nbtstat 命令?	159
160	7-63 怎样使用 tracert 命令?	160
161	7-64 怎样使用 ipconfig 命令?	161
162	7-65 怎样使用 at 命令?	162
162	7-66 Windows 2000 系统的进程有哪些?	162
164	7-67 Windows XP 系统的进程有哪些?	164
130	7-52 什么是“木马”?	130
130	7-53 怎样防止木马攻击?	130
131	7-54 什么是“后门”?	131
131	7-55 怎样防止后门攻击?	131
132	7-56 什么是“钓鱼”?	132
132	7-57 怎样防止钓鱼攻击?	132
133	7-58 什么是“僵尸网络”?	133
133	7-59 怎样防止僵尸网络攻击?	133
134	7-60 什么是“蠕虫”?	134
134	7-61 怎样防止蠕虫攻击?	134
135	7-62 什么是“病毒”?	135
135	7-63 怎样防止病毒攻击?	135
136	7-64 什么是“黑客”?	136
136	7-65 怎样防止黑客攻击?	136
137	7-66 什么是“漏洞”?	137
137	7-67 怎样防止漏洞攻击?	137
138	7-68 什么是“拒绝服务”?	138
138	7-69 怎样防止拒绝服务攻击?	138
139	7-70 什么是“中间人”?	139
139	7-71 怎样防止中间人攻击?	139
140	7-72 什么是“嗅探”?	140
140	7-73 怎样防止嗅探攻击?	140
140	7-74 什么是“社会工程学”?	140
140	7-75 怎样防止社会工程学攻击?	140
141	7-76 什么是“物理攻击”?	141
141	7-77 怎样防止物理攻击?	141
141	7-78 什么是“无线攻击”?	141
141	7-79 怎样防止无线攻击?	141
142	7-80 什么是“移动设备攻击”?	142
142	7-81 怎样防止移动设备攻击?	142
142	7-82 什么是“云攻击”?	142
142	7-83 怎样防止云攻击?	142
143	7-84 什么是“物联网攻击”?	143
143	7-85 怎样防止物联网攻击?	143
143	7-86 什么是“大数据攻击”?	143
143	7-87 怎样防止大数据攻击?	143
144	7-88 什么是“人工智能攻击”?	144
144	7-89 怎样防止人工智能攻击?	144
144	7-90 什么是“量子攻击”?	144
144	7-91 怎样防止量子攻击?	144
145	7-92 什么是“区块链攻击”?	145
145	7-93 怎样防止区块链攻击?	145
145	7-94 什么是“数字货币攻击”?	145
145	7-95 怎样防止数字货币攻击?	145
146	7-96 什么是“自动驾驶攻击”?	146
146	7-97 怎样防止自动驾驶攻击?	146
146	7-98 什么是“无人机攻击”?	146
146	7-99 怎样防止无人机攻击?	146
147	7-100 什么是“机器人攻击”?	147
147	7-101 怎样防止机器人攻击?	147
147	7-102 什么是“网络钓鱼攻击”?	147
147	7-103 怎样防止网络钓鱼攻击?	147
148	7-104 什么是“网络蠕虫攻击”?	148
148	7-105 怎样防止网络蠕虫攻击?	148
148	7-106 什么是“网络病毒攻击”?	148
148	7-107 怎样防止网络病毒攻击?	148
149	7-108 什么是“网络黑客攻击”?	149
149	7-109 怎样防止网络黑客攻击?	149
149	7-110 什么是“网络漏洞攻击”?	149
149	7-111 怎样防止网络漏洞攻击?	149
150	7-112 什么是“网络拒绝服务攻击”?	150
150	7-113 怎样防止网络拒绝服务攻击?	150
150	7-114 什么是“网络中间人攻击”?	150
150	7-115 怎样防止网络中间人攻击?	150
151	7-116 什么是“网络嗅探攻击”?	151
151	7-117 怎样防止网络嗅探攻击?	151
151	7-118 什么是“网络社会工程学攻击”?	151
151	7-119 怎样防止网络社会工程学攻击?	151
152	7-120 什么是“网络物理攻击”?	152
152	7-121 怎样防止网络物理攻击?	152
152	7-122 什么是“网络无线攻击”?	152
152	7-123 怎样防止网络无线攻击?	152
153	7-124 什么是“网络移动设备攻击”?	153
153	7-125 怎样防止网络移动设备攻击?	153
153	7-126 什么是“网络云攻击”?	153
153	7-127 怎样防止网络云攻击?	153
154	7-128 什么是“网络物联网攻击”?	154
154	7-129 怎样防止网络物联网攻击?	154
154	7-130 什么是“网络大数据攻击”?	154
154	7-131 怎样防止网络大数据攻击?	154
155	7-132 什么是“网络人工智能攻击”?	155
155	7-133 怎样防止网络人工智能攻击?	155
155	7-134 什么是“网络量子攻击”?	155
155	7-135 怎样防止网络量子攻击?	155
156	7-136 什么是“网络区块链攻击”?	156
156	7-137 怎样防止网络区块链攻击?	156
156	7-138 什么是“网络数字货币攻击”?	156
156	7-139 怎样防止网络数字货币攻击?	156
157	7-140 什么是“网络自动驾驶攻击”?	157
157	7-141 怎样防止网络自动驾驶攻击?	157
157	7-142 什么是“网络无人机攻击”?	157
157	7-143 怎样防止网络无人机攻击?	157
158	7-144 什么是“网络机器人攻击”?	158
158	7-145 怎样防止网络机器人攻击?	158
158	7-146 什么是“网络网络钓鱼攻击”?	158
158	7-147 怎样防止网络网络钓鱼攻击?	158
159	7-148 什么是“网络网络蠕虫攻击”?	159
159	7-149 怎样防止网络网络蠕虫攻击?	159
159	7-150 什么是“网络网络病毒攻击”?	159
159	7-151 怎样防止网络网络病毒攻击?	159
160	7-152 什么是“网络网络黑客攻击”?	160
160	7-153 怎样防止网络网络黑客攻击?	160
160	7-154 什么是“网络网络漏洞攻击”?	160
160	7-155 怎样防止网络网络漏洞攻击?	160
161	7-156 什么是“网络网络拒绝服务攻击”?	161
161	7-157 怎样防止网络网络拒绝服务攻击?	161
161	7-158 什么是“网络网络中间人攻击”?	161
161	7-159 怎样防止网络网络中间人攻击?	161
162	7-160 什么是“网络网络嗅探攻击”?	162
162	7-161 怎样防止网络网络嗅探攻击?	162
162	7-162 什么是“网络网络社会工程学攻击”?	162
162	7-163 怎样防止网络网络社会工程学攻击?	162
163	7-164 什么是“网络网络物理攻击”?	163
163	7-165 怎样防止网络网络物理攻击?	163
163	7-166 什么是“网络网络无线攻击”?	163
163	7-167 怎样防止网络网络无线攻击?	163
164	7-168 什么是“网络网络移动设备攻击”?	164
164	7-169 怎样防止网络网络移动设备攻击?	164
164	7-170 什么是“网络网络云攻击”?	164
164	7-171 怎样防止网络网络云攻击?	164
164	7-172 什么是“网络网络物联网攻击”?	164
164	7-173 怎样防止网络网络物联网攻击?	164
165	7-174 什么是“网络网络大数据攻击”?	165
165	7-175 怎样防止网络网络大数据攻击?	165
165	7-176 什么是“网络网络人工智能攻击”?	165
165	7-177 怎样防止网络网络人工智能攻击?	165
166	7-178 什么是“网络网络量子攻击”?	166
166	7-179 怎样防止网络网络量子攻击?	166
166	7-180 什么是“网络网络区块链攻击”?	166
166	7-181 怎样防止网络网络区块链攻击?	166
167	7-182 什么是“网络网络数字货币攻击”?	167
167	7-183 怎样防止网络网络数字货币攻击?	167
167	7-184 什么是“网络网络自动驾驶攻击”?	167
167	7-185 怎样防止网络网络自动驾驶攻击?	167
168	7-186 什么是“网络网络无人机攻击”?	168
168	7-187 怎样防止网络网络无人机攻击?	168
168	7-188 什么是“网络网络机器人攻击”?	168
168	7-189 怎样防止网络网络机器人攻击?	168
169	7-190 什么是“网络网络网络钓鱼攻击”?	169
169	7-191 怎样防止网络网络网络钓鱼攻击?	169
169	7-192 什么是“网络网络网络蠕虫攻击”?	169
169	7-193 怎样防止网络网络网络蠕虫攻击?	169
170	7-194 什么是“网络网络网络病毒攻击”?	170
170	7-195 怎样防止网络网络网络病毒攻击?	170
170	7-196 什么是“网络网络网络黑客攻击”?	170
170	7-197 怎样防止网络网络网络黑客攻击?	170
171	7-198 什么是“网络网络网络漏洞攻击”?	171
171	7-199 怎样防止网络网络网络漏洞攻击?	171
171	7-200 什么是“网络网络网络拒绝服务攻击”?	171
171	7-201 怎样防止网络网络网络拒绝服务攻击?	171
172	7-202 什么是“网络网络网络中间人攻击”?	172
172	7-203 怎样防止网络网络网络中间人攻击?	172
172	7-204 什么是“网络网络网络嗅探攻击”?	172
172	7-205 怎样防止网络网络网络嗅探攻击?	172
173	7-206 什么是“网络网络网络社会工程学攻击”?	173
173	7-207 怎样防止网络网络网络社会工程学攻击?	173
173	7-208 什么是“网络网络网络物理攻击”?	173
173	7-209 怎样防止网络网络网络物理攻击?	173
174	7-210 什么是“网络网络网络无线攻击”?	174
174	7-211 怎样防止网络网络网络无线攻击?	174
174	7-212 什么是“网络网络网络移动设备攻击”?	174
174	7-213 怎样防止网络网络网络移动设备攻击?	174
175	7-214 什么是“网络网络网络云攻击”?	175
175	7-215 怎样防止网络网络网络云攻击?	175
175	7-216 什么是“网络网络网络物联网攻击”?	175
175	7-217 怎样防止网络网络网络物联网攻击?	175
176	7-218 什么是“网络网络网络大数据攻击”?	176
176	7-219 怎样防止网络网络网络大数据攻击?	176
176	7-220 什么是“网络网络网络人工智能攻击”?	176
176	7-221 怎样防止网络网络网络人工智能攻击?	176
177	7-222 什么是“网络网络网络量子攻击”?	177
177	7-223 怎样防止网络网络网络量子攻击?	177
177	7-224 什么是“网络网络网络区块链攻击”?	177
177	7-225 怎样防止网络网络网络区块链攻击?	177
178	7-226 什么是“网络网络网络数字货币攻击”?	178
178	7-227 怎样防止网络网络网络数字货币攻击?	178
178	7-228 什么是“网络网络网络自动驾驶攻击”?	178
178	7-229 怎样防止网络网络网络自动驾驶攻击?	178
179	7-230 什么是“网络网络网络无人机攻击”?	179
179	7-231 怎样防止网络网络网络无人机攻击?	179
179	7-232 什么是“网络网络网络机器人攻击”?	179
179	7-233 怎样防止网络网络网络机器人攻击?	179
180	7-234 什么是“网络网络网络网络钓鱼攻击”?	180
180	7-235 怎样防止网络网络网络网络钓鱼攻击?	180
180	7-236 什么是“网络网络网络网络蠕虫攻击”?	180
180	7-237 怎样防止网络网络网络网络蠕虫攻击?	180
181	7-238 什么是“网络网络网络网络病毒攻击”?	181
181	7-239 怎样防止网络网络网络网络病毒攻击?	181
181	7-240 什么是“网络网络网络网络黑客攻击”?	181
181	7-241 怎样防止网络网络网络网络黑客攻击?	181
182	7-242 什么是“网络网络网络网络漏洞攻击”?	182
182	7-243 怎样防止网络网络网络网络漏洞攻击?	182
182	7-244 什么是“网络网络网络网络拒绝服务攻击”?	182
182	7-245 怎样防止网络网络网络网络拒绝服务攻击?	182
183	7-246 什么是“网络网络网络网络中间人攻击”?	183
183	7-247 怎样防止网络网络网络网络中间人攻击?	183
183	7-248 什么是“网络网络网络网络嗅探攻击”?	183
183	7-249 怎样防止网络网络网络网络嗅探攻击?	183
184	7-250 什么是“网络网络网络网络社会工程学攻击”?	184
184	7-251 怎样防止网络网络网络网络社会工程学攻击?	184
184	7-252 什么是“网络网络网络网络物理攻击”?	184
184	7-253 怎样防止网络网络网络网络物理攻击?	184
185	7-254 什么是“网络网络网络网络无线攻击”?	185
185	7-255 怎样防止网络网络网络网络无线攻击?	185
185	7-256 什么是“网络网络网络网络移动设备攻击”?	185
185	7-257 怎样防止网络网络网络网络移动设备攻击?	185
186	7-258 什么是“网络网络网络网络云攻击”?	186
186	7-259 怎样防止网络网络网络网络云攻击?	186
186	7-260 什么是“网络网络网络网络物联网攻击”?	186
186	7-261 怎样防止网络网络网络网络物联网攻击?	186
187	7-262 什么是“网络网络网络网络大数据攻击”?	187
187	7-263 怎样防止网络网络网络网络大数据攻击?	187
187	7-264 什么是“网络网络网络网络人工智能攻击”?	187
187	7-265 怎样防止网络网络网络网络人工智能攻击?	187
188	7-266 什么是“网络网络网络网络量子攻击”?	188
188	7-267 怎样防止网络网络网络网络量子攻击?	188
188	7-268 什么是“网络网络网络网络区块链攻击”?	188
188	7-269 怎样防止网络网络网络网络区块链攻击?	188
189	7-270 什么是“网络网络网络网络数字货币攻击”?	189
189	7-271 怎样防止网络网络网络网络数字货币攻击?	189
189	7-272 什么是“网络网络网络网络自动驾驶攻击”?	189
189	7-273 怎样防止网络网络网络网络自动驾驶攻击?	189
190	7-274 什么是“网络网络网络网络无人机攻击”?	190
190	7-275 怎样防止网络网络网络网络无人机攻击?	190
190	7-276 什么是“网络网络网络网络机器人攻击”?	190
190	7-277 怎样防止网络网络网络网络机器人攻击?	190
191	7-278 什么是“网络网络网络网络网络钓鱼攻击”?	191
191	7-279 怎样防止网络网络网络网络网络钓鱼攻击?	191
191	7-280 什么是“网络网络网络网络网络蠕虫攻击”?	191
191	7-281 怎样防止网络网络网络网络网络蠕虫攻击?	191
192	7-282 什么是“网络网络网络网络网络病毒攻击”?	192
192	7-283 怎样防止网络网络网络网络网络病毒攻击?	192
192	7-284 什么是“网络网络网络网络网络黑客攻击”?	192
192	7-285 怎样防止网络网络网络网络网络黑客攻击?	192
193	7-286 什么是“网络网络网络网络网络漏洞攻击”?	193
193	7-287 怎样防止网络网络网络网络网络漏洞攻击?	193
193	7-288 什么是“网络网络网络网络网络拒绝服务攻击”?	193
193	7-289 怎样防止网络网络网络网络网络拒绝服务攻击?	193
194	7-290 什么是“网络网络网络网络网络中间人攻击”?	194
194	7-291 怎样防止网络网络网络网络网络中间人攻击?	194
194	7-292 什么是“网络网络网络网络网络嗅探攻击”?	194
194	7-293 怎样防止网络网络网络网络网络嗅探攻击?	194
195	7-294 什么是“网络网络网络网络网络社会工程学攻击”?	195
195	7-295 怎样防止网络网络网络网络网络社会工程学攻击?	195
195	7-296 什么是“网络网络网络网络网络物理攻击”?	195
195	7-297 怎样防止网络网络网络网络网络物理攻击?	195
196	7-298 什么是“网络网络网络网络网络无线攻击”?	196
196	7-299 怎样防止网络网络网络网络网络无线攻击?	196
196	7-300 什么是“网络网络网络网络网络移动设备攻击”?	196
196	7-301 怎样防止网络网络网络网络网络移动设备攻击?	196
197	7-302 什么是“网络网络网络网络网络云攻击”?	197
197	7-303 怎样防止网络网络网络网络网络云攻击?	197
197	7-304 什么是“网络网络网络网络网络物联网攻击”?	197
197	7-305 怎样防止网络网络网络网络网络物联网攻击?	197
198	7-306 什么是“网络网络网络网络网络大数据攻击”?	198
198	7-307 怎样防止网络网络网络网络网络大数据攻击?	198
198	7-308 什么是“网络网络网络网络网络人工智能攻击”?	198
198	7-309 怎样防止网络网络网络网络网络人工智能攻击?	198
199	7-310 什么是“网络网络网络网络网络量子攻击”?	199
199	7-311 怎样防止网络网络网络网络网络量子攻击?	199
199	7-312 什么是“网络网络网络网络网络区块链攻击”?	199
199	7-313 怎样防止网络网络网络网络网络区块链攻击?	199
200	7-314 什么是“网络网络网络网络网络数字货币攻击”?	200
200	7-315 怎样防止网络网络网络网络网络数字货币攻击?	200
200	7-316 什么是“网络网络网络网络网络自动驾驶攻击”?	200
200	7-317 怎样防止网络网络网络网络网络自动驾驶攻击?	200
201	7-318 什么是“网络网络网络网络网络无人机攻击”?	201
201	7-319 怎样防止网络网络网络网络网络无人机攻击?	201
201	7-320 什么是“网络网络网络网络网络机器人攻击”?	201
201	7-321 怎样防止网络网络网络网络网络机器人攻击?	201
202	7-322 什么是“网络网络网络网络网络网络钓鱼攻击”?	202
202	7-323 怎样防止网络网络网络网络网络网络钓鱼攻击?	202

Part 1

第一部分

基础篇

本部分内容

- 第1章 计算机及网络安全常识
- 第2章 计算机病毒及其防护
- 第3章 计算机黑客攻击及其防护
- 第4章 计算机电磁泄漏及其防护

第 1 章



计算机及网络安全常识

1-1 什么是计算机网络？它主要功能有哪些？

计算机网络是计算机技术和通信技术相结合的产物，它是利用通信设备和线路，将分布在不同地理位置、功能相互独立的多个计算机系统连接起来，实现信息传递、资源共享、分布式处理的系统。

1. 信息交换

它是计算机网络最基本的功能，主要完成计算机网络中各个节点之间的数据通信。用户可以在网上传送电子邮件、发布新闻消息、进行电子购物、开展电子贸易、实现远程电子教育等。

2. 资源共享

所谓资源是指构成系统的所有要素，主要包括软、硬件资源，如大容量磁盘、高速打印机、绘图仪、通信线路、数据库、文件和其他计算机上的有关信息。由于受经济和其他因素的制约，这些资源并非（也不可能）所有用户都能独立拥有的，所以网络上的计算机不仅可以使使用自身的资源，也可以共享网络上的资源。因而增强了网络上计算机的处理能力，提高了计算机软、硬件资源的利用率。

3. 分布式处理

一项复杂的任务可以划分成许多部分来完成，由网络内各计算机分别协作并行完成有关部分，使整个系统的性能得到提高。

1-2 计算机网络按其覆盖范围的不同通常分为哪几类？各类的特点是什么？

计算机网络通常可分为局域网、广域网和城域网。

局域网（LAN）是指覆盖地域范围较小（通常从几米到几千米以内）的计算机网络，如一个办公室、一层楼内、一栋大楼内或一个企业单位所在的园区内的计算机网络。局域网具有覆盖范围小和传输速度高等特点。随着光纤通信技术的发展，局域网覆盖范围已可达几十千米，传输速率可达 1Gb/s 以上。

广域网（WAN）是指覆盖地域范围更广的计算机网络，如一个地区、一个国家或全世界范围的计算机网络。通常，两个或多个局域网通过长途通信线路连接起来就形成了广域网，广域网之间再通过长途通信线路连接起来就形成了更大范围的广域网。与局域网相比，