黑魔方
www.heimofang.com

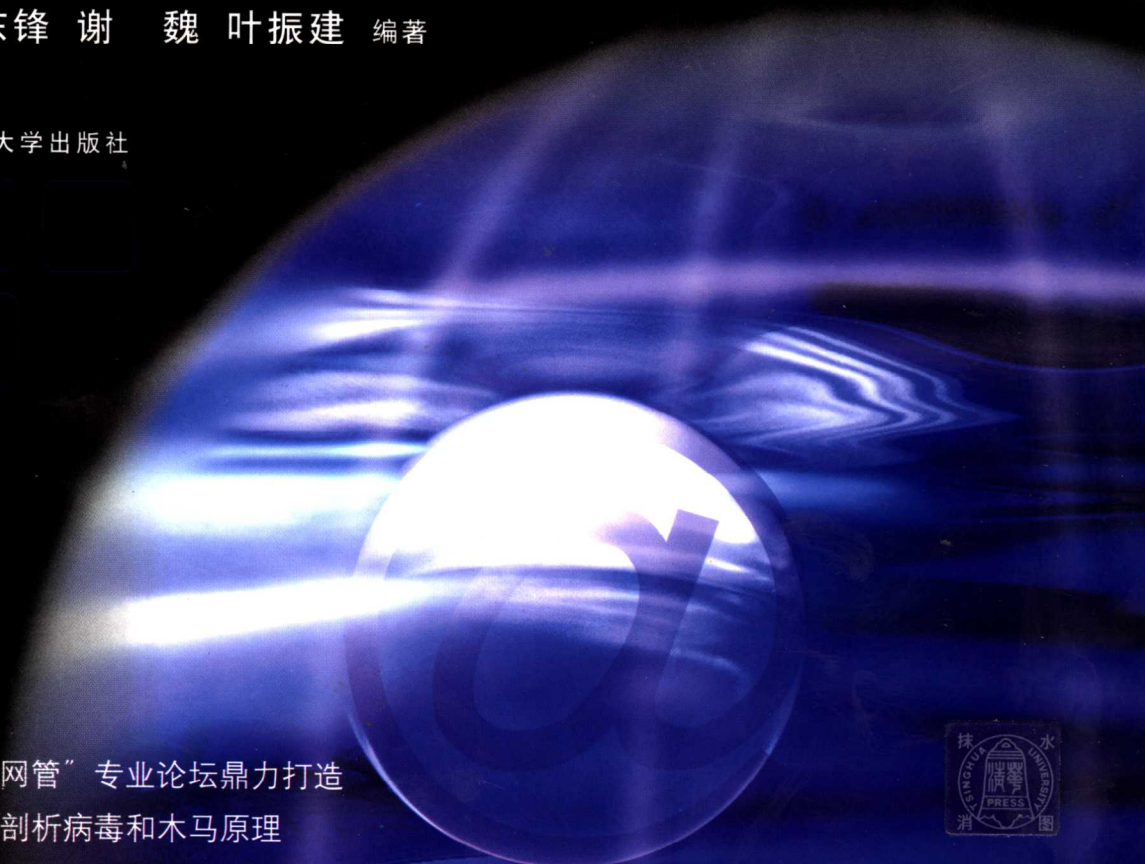
专家门诊系列

网络安全管理技术

专家门诊

张　涛　主编
阴东锋　谢　魏　叶振建　编著

清华大学出版社



"我是网管"专业论坛鼎力打造
彻底剖析病毒和木马原理
完美演绎系统防御的方法
提供实时的在线技术支持

专家门诊系列

网络安全管理技术

专家门诊

张　涛　主编
阴东锋　谢　魏　叶振建　编著

清华大学出版社

“我是网管”专业论坛鼎立打造
彻底剖析病毒和木马原理
完美演绎系统防御的方法
提供实时的在线技术支持

内容简介

本书重点介绍各种常见的网络安全方面的问题，包括了对黑客的认识、网络安全基础、网络工具的使用、计算机病毒、特洛伊木马、日常上网安全防护、Windows 2000 系统安全、应用程序安全、缓冲区溢出等方面的内容。本书强调理论与实践相结合，注重技术的可操作性，采用面向问题的讲述方式，列举了大量典型的实例。

本书的最大特点是从问题出发，在简单的基础理论之上以实际应用为主，体现了“以防为主、攻防兼备”的写作特色。本书所给出的问题在论坛中也经常出现，都是网络爱好者比较关心的问题，可以提供很强的参考作用。

本书内容丰富，语言通俗易懂，实用性非常强，是一本很适合入门及初级读者的网络安全教程。

图书在版编目（CIP）数据

网络安全管理技术专家门诊 / 张涛主编；阴东锋，谢魏，叶振建编著. —北京：清华大学出版社，2005.2
（黑魔方丛书）
ISBN 7-302-10295-3

Ⅰ.网… Ⅱ.①张…②阴…③谢…④叶… 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（2005）第 000673 号

出 版 者：清华大学出版社
地　　址：北京清华大学学研大厦
http://www.tup.com.cn
邮　　编：100084
社 总 机：010-62770175
客户服务：010-62776969
责任编辑：魏江江
装帧设计：吴文越

印 刷 者：北京市鑫丰华彩印有限公司
装 订 者：三河市金元装订厂
发 行 者：新华书店总店北京发行所
开　　本：185×230 **印张**：23.75 **插页**：2 **字数**：497 千字
版　　次：2005 年 2 月第 1 版 2005 年 2 月第 1 次印刷
书　　号：ISBN 7-302-10295-3/TP · 1140
印　　数：1～3000
定　　价：32.00 元

形成知識体系 着重实际
应用导引自主學習促进
社會普及

祝贺

計算機大型系列丛書出版

張效祥

二〇二三年十月

总序

四十多年前，当我国刚刚研制出最初的几台计算机时，只有极少数科学家会使用计算机来做科学计算。那时，在一般人的眼中，计算机是非常神秘的，更不用说去使用它了。然而，时至今日，计算机已经走下科学家的殿堂，来到了老百姓的身边。现在，使用计算机已变成了人们的“家常便饭”，甚至连儿童也会用计算机来玩游戏和上网了。确实，今天我们正处在一个信息时代，计算机已经无所不在，它进入了各行各业，它改变着人们的工作、学习和生活，它已经成为人们不可或缺的工具和伴侣；于是，使用计算机也就从早期的少数专家特有的本领变成了如今人人都可拥有的基本技能。但随之，人们也就面临一个新问题：这就是如何普及计算机教育？如何使广大群众更快、更好地掌握使用计算机的技能？如何使他们能用计算机为国家、为社会、为自己做更多的工作，创造更多的财富？显然，要解决好这个问题，迫切需要一套为普及计算机使用技能而专门设计的好书，正是在这种需求下，清华大学出版社的《黑魔方丛书》应运而生了。

从这套丛书的出版思路、体系结构和进度计划来看，它具有不同于一般丛书的特点：

一、它建立了一个较为科学的计算机图书出版体系，这对于今后计算机图书出版的规范化将起到良性的引导作用。《黑魔方丛书》涉及到计算机应用的各个方面，它既可以单独学习也可以连续深入钻研，这对于普及计算机应用是很有积极意义的。该丛书的丰富内容可以说是对现在市场上铺天盖地的计算机图书所做的系统提炼，在知识更新率极高的计算机图书领域，该丛书起到了承上启下的作用。

二、它创造了一种由读者自由选择学习内容的体系。读者可根据《计算机学习金手册》，对照自己的实际情况选择适用的图书，这可以使读者更有目的地进行学习，与盲目找书、盲目学习相比，显然可以节约时间和金钱。

三、它可以帮助读者掌握学习方法、找准学习方向。在学习中，有时人们会抱怨，花了很大力气却学不到什么东西，这往往是没有掌握学习方法，没有找准学习方向。《黑魔方丛书》在这方面下了功夫，它可以有效地帮助读者掌握学习方法、找准学习方向。这样，这套图书的作用就不仅仅是灌输知识，它还能帮助读者提高学习效率、提升思维能力。

最近，我国载人飞船顺利升空，这标志着我国在发展科学技术方面取得了重大进展。但是在欢庆这一重大成就的同时，我们也应清醒地认识到，我国还是一个发展中国家，在计算机方面也还远远落后于发达国家。为此，我们必须奋起直追，大力普及计算机教育。我们相信《黑魔方丛书》将为此发挥重要的作用，它也将因此得到广大读者的喜爱。

专家委员会

成员（按姓氏笔画排序）

孙家广　教授 中国工程院院士
国家 CAD 支撑软件工程技术研究中心主任

李三立　教授 中国工程院院士
清华大学计算机科学与工程研究所所长 上海大学计算机学院院长

李国杰　研究员 中国工程院院士
计算机学会常务副理事长

张效祥　研究员 中国科学院院士
中国计算机学会名誉理事长

求伯君　金山电脑公司董事长

吴文虎　教授 博士生导师 教育部远程教育专家委员会主任
全国高等院校计算机基础教育研究会副会长

杨芙清　研究员 中国科学院院士
北大青鸟集团董事长

倪光南　研究员 博士生导师 中国工程院院士
中国中文信息学会副理事长

谭浩强　教授 全国高等院校计算机基础教育研究会会长
教育部计算机应用技术证书考试委员会主任委员

丛书编委会

成员

谭浩强	吴文虎	王克宏	柳西玲	潘爱民
黄淼云	李也白	吴文越	陈　跃	李秋弟
蔡鸿程	卢先和	汤斌浩	丁　岭	徐培忠
林慕新	刘　华	李江涛	魏江江	田在儒

出版说明

新世纪应该有新气象，“黑魔方”就是这样。

作为一套建设中的计算机大型系列丛书，“黑魔方”将以图书出版为纽带，带动计算机技术与经验的广泛交流、积累，在图书编写、出版、推广、服务等方面进行有意义的探索和创新，积极促进计算机技术的社会应用普及。

现在，“黑魔方”图书已陆续和读者见面了。细心的读者会发现，“黑魔方”有很多与众不同之处。但这也仅仅是开始，随着更多读者和其他热心人的参与和支持，“黑魔方“必将越做越好，最终为社会贡献出一套由广大读者、作者、编辑和其他人士共同参与建设起来的精品计算机丛书。

为了便于读者更深入地了解“黑魔方”，这里我们把策划和出版“黑魔方”丛书的一些思路和想法简要说明一下，希望能和更多的读者交流、探讨。

有关体系和规范

计算机的应用领域十分广泛，各种新技术也层出不穷，这便给计算机的学习者带来困难。学什么，往哪个方向学，采用什么学习方法，前景如何？等等，这些问题是很多学习者无法真正搞清楚的。如果搞不清楚，在选择学习用书时就会有一定的盲目性。如何帮读者解决这个问题？“黑魔方”进行了积极的摸索。“学习蓝图”和《计算机学习金手册》是“黑魔方”的第一次尝试。它们从实用的角度出发，将计算机在人们生活和工作中的主要应用状况加以归纳，尽可能地理清脉络、形成体系并提供简要介绍，以期给读者和出版者提供较为一致的选择图书和出版图书的参考依据。

促进计算机图书的出版走向规范化，则是“黑魔方”考虑的另一个重要问题。“黑魔方”首先尝试从书名、层次划分等方面加以规范。在“黑魔方”中，每本书的书名都是严格按照丛书编委会制定的统一标准命名的。一个书名中代表的难易层次和写作风格都是固定的，避免出现同样叫“*****精通”的两本书所讲述内容和难易程度迥然不同的情况。

有关出版模式和作者队伍

“黑魔方”采用开放式的图书出版模式。一者，“黑魔方”的丛书体系构成比较开放，没有固定的图书品种、出版周期等方面的限制，随时可以根据社会发展需要加以变通和完善；二者，专门为“黑魔方”开设了一个专题网站，作为一个联结读者、作者、编辑的广泛交流平台，在此平台基础上任何一位热心者均可以参与“黑魔方”的规划建设，并从中受益。

另外，在丛书作者队伍方面也采用开放形式，面向全社会，任何一位有能力的作者均可以加入到“黑魔方”的作者队伍中来。“黑魔方”采用科学的淘汰和奖惩机制，以保证作者

队伍的健壮。

有关出版印刷和配套服务

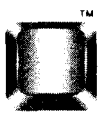
在图书定价与印刷质量权衡的问题上，每个出版者或读者都会有不同的观点。“黑魔方”在寻求二者平衡点的同时，始终把读者的感受放在第一位，在每一本“黑魔方”图书的出版印刷的每一个细节上都反复审度，以求带给读者更舒服的读书享受。比如，在正文印刷字体、字号的选择上，就经过反复的比较、试验，才最终选择了现在的字体、字号，因为这种字样在视觉上比较整洁舒服，长期阅读不容易劳累；在正文印刷用纸上，选择了质地轻软、手感柔和的再生纸，等等。

“黑魔方”不仅仅重视图书质量，而且重视图书的售后服务。包括，建立了“黑魔方”专题网站、设立了直接意见反馈渠道、设立了技术支持及问题解答的专线，同时，根据需要还将开展配套的培训服务、电视讲座服务、在线指导服务、作者巡回报告服务，等等。一切有利于读者计算机学习的服务均将先后开展。

以上的说明，只是介绍了“黑魔方”某些方面，“黑魔方”还包含有很多很多的创意和革新，需要读者去慢慢发现和理解。

“它山之石，可以攻玉”。“黑魔方”的成长和壮大，仅仅依靠一个出版社的力量是远远不够的，我们期望能有越来越多的人士或团体加入到“黑魔方”的建设队伍中来，和我们一道为探索计算机图书出版的变革，以及为推动我国计算机事业的发展做出贡献！

清华大学出版社
2004 年 1 月



导读

首先，非常感谢您阅读本书，希望本书不同于其他同类的书籍，能确确实实地给您带来一些收获。当您仔细阅读完本书后，您就已经进入了一扇通往网络安全的大门。为了能更好地帮助您学习本书的知识，请仔细阅读下面的内容。

本书的读者对象

本书是一本面向大众的网络安全基础类书籍，风格简洁明了，文字通俗易懂，采用一问一答的形式，对常见的各种网络安全事项进行了详细的剖析，并通过实际例子手把手地教您学习网络安全的基础知识。

本书适合广大在校大学生、网络管理员、家庭用户、宽带用户，以及广大网络安全爱好者阅读，是一本很实用的入门级读物。

如果您要阅读并掌握本书的内容，您需要对 Windows 操作系统和网络基础知识有一定的认识，并有一定的实际操作能力。

本书的写作环境

本书除第 4、5、6 章在 Windows XP 环境下完成写作外，其他所有内容都在 Windows 2000 环境下完成，如在书中未进行特别说明，则技术和方法可以在其他 Windows 环境下使用。

本书中介绍的所有软件，其版本均以软件抓图或文章描写为准。

本书的学习方法

网络安全重在预防，学习并领会这种思想才是本书的精神所在，而这种思想的实践基础就是本书介绍的各种技术和方法。

要更好地学习本书的内容，建议您先快速浏览整本书，在看第二遍时做好这两方面：仔细阅读，认真领会，最好能作笔记；多做实验，胆大心细，不要怕失败。如果您对其中的一些术语或简单知识不了解，建议您到搜索引擎先查找并掌握相关基础知识。

在本书出版的同时，www.54master.com 将同时开设相应的读者交流版块，在您阅读本书过程中，您的任何建议、要求、疑问等，都可以到此版块发表。同时您还可以通过电子邮件方式同作者取得联系，联系方式：security@54master.com。

IT 书吧（http://www.itbook8.com）提供相关图书资讯及相关资料下载。

作者介绍

本书所有内容由“我是网管”论坛的三位管理员所写。

原攻防技术版版主“SimpleLove”（阴东锋），熟悉 Windows、FreeBSD 和 Linux 安全，精通各种协议，有一定的网络攻防能力，编写了第 1、2、3、8、9 章。

坛主“红色代码”（张涛），熟悉各种 Windows 系统的安全配置，精通各类计算机病毒

的原理和查杀办法，多次在各种杂志发表文章，编写了第 4、5、6 章。

总版主“xieweinick”（谢魏），精通服务器、网络攻防、SQL，可熟练配置各种网络环境下的 ISA Server 和 Exchange Server，编写了第 7 章。

特别感谢

“我是网管”论坛：http://www.54master.com

微软中国：http://www.microsoft.com/china

安全焦点：http://www.xfocus.net

绿盟科技：http://www.nsfocus.net

CVC 电脑病毒论坛：http://www.retcvc.com/

另外，还要感谢广大网友和兄弟论坛提出的意见和建议，感谢很多前辈的指点和教导，感谢李婷婷、刘飞倩及孟宪芳三位同志在整个写作过程中的大力支持。

目录

第 4 章 计算机病毒