网管员必读

NETWORK ADMINISTRATOR

——网络安全

王 达 编著
飞思科技产品研发中心 监制

電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
http://www.phei.com.cn

网管员必读

NETWORK ADMINISTRATOR

—— 网络安全

王 达 编著
飞思科技产品研发中心 监制

電子工業出版社
Publishing House of Electronics Industry
北京·BEIJING

内容简介

本书是以企业网络应用的安全需求为出发点而编写的，不是市面上通常所见的黑客攻击类图书。书中不仅介绍了常见的病毒、木马和黑客攻击的防护方法，还更多地从全局的战略高度分析了企业网络中存在的安全隐患，并用一章的篇幅介绍了对应隐患的安全防御方案。

本书共 10 章，介绍的内容包括恶意软件（病毒、木马和蠕虫等）的深度防御方法，黑客的主要类型和防御方法，企业网络内、外部网络防火墙系统的部署方法，入侵检测系统的应用，网络隔离技术及应用，Windows Server 2003 系统用户账户安全策略及权限配置，公钥基础结构和计算机证书技术及应用，文件加密，数字签名和电子签章技术及应用，远程网络访问安全配置和数据备份与恢复。这些内容虽然不能说是非常全面地概括了企业网络安全的方方面面，但从大的方面来说，基本上都已囊括在其中了。读者通过对本书的学习可以为自己所在的企业部署全面、完善的安全防御系统，而不再是传统意义上的简单的病毒防护系统+防火墙了。

本书非常适合各类网络爱好者、企业 IT 经理和网络管理员，以及网络安全工程师自学选用，也可作为高职院校的选用教材。

图书在版编目（CIP）数据

网管员必读——网络安全 / 王达编著. —北京：电子工业出版社，2005.11
ISBN 7-121-01776-8

Ⅰ.网... Ⅱ.王... Ⅲ.①计算机网络－基本知识②计算机网络－安全技术－基本知识 Ⅳ.TP393

中国版本图书馆 CIP 数据核字（2005）第 108893 号

责任编辑：何郑燕
印　　刷：北京天宇星印刷厂
出版发行：电子工业出版社
　　北京海淀区万寿路 173 信箱　邮编：100036
经　　销：各地新华书店
开　　本：850×1168　1/16　印张：31　字数：843.2 千字
印　　次：2005 年 11 月第 1 次印刷
印　　数：6 000 册　　定价：45.00 元

凡购买电子工业出版社的图书，如有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系，联系电话：010-68279077。质量投诉请发邮件至 zlts@phei.com.cn，盗版侵权举报请发邮件至 dbqq@phei.com.cn。

前　言

关于本丛书

随着网络和信息技术的高速发展和普及，信息化已经成为现代企业生存和发展的必备条件。在此背景下，网管员（Network Administrator）作为一种职业应运而生。劳动和社会保障部日前颁布了第四批国家职业标准，明确规定计算机网络管理员已经成为当今社会生活中的一个新兴职业。网管员职业要求从业者具备一系列专业、高端的计算机及网络操作技能。因此，网管员在从业前必须进行系统的培训和学习。

《网管员必读》系列图书由飞思科技产品研发中心，经过周密细致的市场调研与知识体系研发，聘请著名培训学校的资深教师、具有多年经验的专业网管员，以及业内权威杂志《网管员世界》联手打造的，从而使内容的广度和深度有所保障。本丛书从网管员这个职业切入，以网管员的具体工作内容为线索，分阶段地全面呈现了网管员所需的各项技术，并融入了作者多年工作的经验总结，以及对网管员这个职业的高屋建瓴式的理解，是目前市场上惟一从“网管员职业塑身”角度切入的精品丛书。《网管员必读》系列共推出 8 本：

《网管员必读——网络基础》
《网管员必读——网络应用》
《网管员必读——网络管理》
《网管员必读——故障排除》
《网管员必读——网络安全》
《网管员必读——网络组建》
《网管员必读——超级网管经验谈》
《网管员必读——服务器与数据存储》

本丛书具有如下特色：

- 实用。本丛书中所选应用实例均来源于实际工作中的经验总结，在实际应用中是完全必需的，而不是纯理论的介绍。
- 专业。本丛书中所介绍的各种技术都有非常专业的理论和实际应用配置介绍，而非泛泛而谈。
- 系统。本丛书所介绍的各种网络知识，全部是围绕企业的实际网络应用而选择的，形成了一个系统而完备的网管知识体系。读者通过对本丛书的系统学习，即可掌握网管员日常工作中的全部知识，有效地解决工作中遇到的大部分问题。

关于本书

目前，“病毒入侵”和“黑客攻击”仍是企业网络安全的最重要的两个方面。要有效地搞好企业网络安全工作，我们不能停留在表面含义上，而应充分领会企业网络中这两个主要安全隐患的内涵。在企业网络中，它们已不再是我们平常在个人计算机使用中所谈论的“病毒入侵”和“黑客攻击”了，它们所包含的内涵比起个人计算机中要广泛许多。在个人计算机使用中，我们预防这两个安全威胁所采取的方法基本上就是安装杀病毒软件和防火墙，高级一些的还会想到系统漏洞，及时下载、安装一些系统补丁。因为个人计算机的使用基本上不存在其他安全因素，几乎所有的安全威胁都来自互联网。但在企业网络中，仅有这方面的认识和知识是远远不够的，因为它不仅有个人计算机使用中的互联网应用，还有与其他企业局域网的连接，以及自身局域网，这些同样可能带来巨大的安全威胁。所以，在企业网络中，网络安全因素增多了，病毒入侵和黑客攻击的途径更广了，安全系统的部署难度更大了。

在企业网络中，网络用户的非法访问和网络数据的存储与备份都可能是非常重要的安全

隐患，措施不当同样可以致使整个企业网络瘫痪，网络服务器系统崩溃。预防这类安全事件发生的措施主要是通过用户权限配置、数据加密和完善的企业容灾策略，而这些恰恰是许多读者朋友，甚至网络管理员朋友所忽视的，致使企业网络安全漏洞百出，从而花高代价部署了高性能防火墙和网络杀毒软件系统。由此可见，在企业网络中的安全系统部署远不再是个人计算机系统中的一个杀病毒软件和防火墙就能全部搞定的。

本书不仅全面介绍了大家容易想到的病毒防护、木马防护、漏洞检测技术和黑客攻击防护知识、方法，还从深层次分析了恶意软件（包括病毒、木马防护和黑客程序等）的防御方法，企业内、外部网络的防火墙部署、入侵检测和网络隔离技术和应用，Windows 系统的用户账户权限配置、安全策略配置、文件加密和数字签名技术及应用、远程访问安全配置和数据备份与恢复等，可以说，基本上囊括了企业网络安全的各主要方面。通过对本书的学习，读者可以全面为自己所在企业部署一个比较完善的网络安全防御系统，而不再像个人计算机防御体系中的杀病毒软件和防火墙那么简单。正因如此，笔者认为，本书可能是目前 IT 图书市场上惟一一本真正从企业网络安全应用角度出发，真正想企业用户之所想，急 IT 经理和网络管理员们之所急的一本全面深层剖析企业网络安全隐患、全面提供解决方案的网络安全类图书。我们真诚地希望，这本书能实实在在地给各位网管朋友以帮助，而不是像一些同类图书那样，给人以肤浅的感觉。因为我们不是要做黑客，而是要做一个合格的企业网络安全工程师。真正的网络安全工程师就应该有全局的观念，从深层次分析网络安全威胁的来源，并给出适当的安全解决方案。这就是我们的最终追求。

本书由飞思科技产品研发中心策划并组织编写，王达主笔并统稿，在写作过程中广州凌云计算机图书创作中心的何艳辉、王珂、何江林、刘凤竹、尚宝宏、马平、卢京华、王正安、姚学军、李敏、周志雄、高平复、洪武、周建辉、孔平、李翔、刘学、沈芝兰等提供了许多非常有价值的实用经验，并在审稿和排版方面给予了大力支持，在此一并表示由衷的感谢！由于笔者自身水平和时间都比较有限，尽管在编写过程中力图尽善尽美，但可能仍存在一些错误，还望读者朋友批评指正，万分感谢！广州凌云计算机图书创作中心的网址为 http://www.bookb2b.com/studio/user/lingyun，期待见到您的留言。

我们的联系方式如下：
咨询电话：（010）68134545　　88254160
电子邮件：support@fecit.com.cn
服务网址：http://www.fecit.com.cn　　http://www.fecit.net
通用网址：计算机图书、飞思、飞思教育、飞思科技、FECIT

飞思科技产品研发中心

目 录

第1章 企业网络安全概述

网络安全伴随着网络的产生而产生，有网络的地方就存在着网络安全隐患。像病毒入侵和黑客攻击之类的网络安全事件，目前主要是通过网络进行的，而且几乎每时每刻都在发生，遍及全球。网络安全事件所带来的危害，相信我们每个计算机用户都或多或少地亲身体验过一些，轻则可能使你的电脑系统运行不正常，重则可以使整个计算机系统中的磁盘数据全盘覆灭，甚至导致磁盘、计算机等硬件的损坏。对于个人来说所带来的损失可能还不足以令人重视，一般来说大不了重新买个二手硬盘，重装系统，继续使用。因为这类用户的电脑中本身就没有多少自己的东西，全部装的都是软件和游戏，这些都可以重装。但对于企业用户来说，可能会是灭顶之灾。因为这些用户在服务器磁盘中每天都要存储许多非常重要的工作文件和数据库文件，一旦出现网络安全事故，就可能使整个企业网络系统瘫痪，甚至磁盘系统损坏，其损失往往是难以估计的。如本中心前几天发生的一宗安全事故，令我追悔莫及，无法接受——由于没有及时对每天的工作进行备份，使得近一个月来所写的一部图书因一次病毒入侵毁坏殆尽。尽管事后我们采取了一切措施，愿不惜一切代价对损坏的磁盘数据进行恢复，并找了好多家专门做数据恢复的公司，但最终还是回天乏力，其损失何止万元。

为了防范这些网络安全事故的发生，我们每个计算机用户，特别是企业网络用户，必须采取足够的安全防范措施，甚至可以说要在利益均衡情况下不惜一切代价。但要注意，企业网络安全策略的实施是一个系统工程，它涉及许多方面，既要充分考虑到那些平时我们经常提及的外部网络威胁，又要对来自内部网络安全隐患有足够的重视。我们不能孤立地看待任何一个安全隐患和安全措施，因为这些安全隐患爆发的途径可以是多方面的，而许多安全措施都是相辅相存的。事实上，有许多网管员朋友，虽然知道网络安全的重要性，却不知道网络安全隐患来自何方，更别说采取什么措施来防范了。本章主要从宏观的角度阐述企业网络安全方面的一些基础知识，如病毒入侵的基础知识、常见的网络攻击类型等；介绍企业网络安全隐患来源，以及企业网络安全策略的基本设计思路等。具体的安全防范措施将在本书后面的各章详细介绍。

本章重点

- 企业网络安全隐患来源
- 病毒的主要特点及常见类型
- 常见的网络攻击类型
- 企业网络安全策略设计原则
- 企业网络安全策略设计思路

1.1 企业网络安全考虑

说到企业网络安全，有不少刚涉入网管行业的网管员往往把它与个人网络安全混为一谈，其实这是极其错误的。因为个人网络安全一般来说都仅限于与互联网连接时的网络安全，它惟一的安全隐患来源就是互联网，但对于企业网络，其网络安全隐患不仅来自像互联网这样的外网，内部局域网的安全隐患也十分值得重视，而且外网中存在的安全隐患同样可以在内网中发生。也就是企业网络安全隐患有内、外网之分。针对两者的安全防范措施有很大区别，这一点我们可以通过本书后面介绍的各种安全防范措施深刻地理解到。但要注意的是，在企业网络中，内、外网安全隐患又不是完全孤立的，在许多情况下，外网安全威胁的最终来源是内网。

作为企业 IT 经理或网管员，要为自己的企业部署网络安全系统，首先需要弄清楚的当然就是自己企业网络安全隐患的主要来源。现在网络安全系统所要防范的不再是简单的病毒感染，更多的是那些基于网络的非法入侵、攻击与访问。如果认识不足，很可能给企业网络留下许多的安全隐患。由于企业网络安全隐患的来源有内、外网之分，所以作为 IT 经理或企业网管员必须要全面地考虑问题，不要顾此失彼，千万别小看内部网络中存在的安全隐患，在很多情况下内部网络的安全威胁要远远大于外部网络，因为在内部网络中实施入侵和攻击更加容易。下面是笔者总结的，作为 IT 经理或网络管理员在为自己企业部署网络安全防御系统时应考虑的几个主要方面，也是企业网络安全威胁的主要来源。

- 病毒入侵和黑客攻击
- 基于操作系统安全漏洞的攻击
- 网络用户密码盗用与权限滥用
- 重要文件或邮件的非法窃取、访问与操作
- 关键部门的非法访问
- 外网的非法入侵
- 备份数据和存储媒体的损坏、丢失

下面对以上这些安全隐患来源进行简单的介绍，具体的防范措施将在本书后面各章分别介绍。

1.1.1 病毒入侵和黑客攻击的基本防护

这是我们最常见、最普遍的网络安全隐患。目前所见到的安全事件绝大多数属于这两种类型。同时，这两种安全隐患爆发的概率是最大的，因为它们几乎是无孔不入、无处不在的，防不胜防，一不小心就会中招。现在如果说有人不安装任何防毒系统和防火墙系统就直接上互联网，那简直不可思议。

1. 病毒和黑客程序简介

病毒的历史最悠久，早在 DOS 时代就非常盛行，至今已发现的病毒种类数以万计，其危害性足以令人谈毒色变。它可以使整个计算机系统、整个网络处于瘫痪，使所有保存在磁盘中的数据化为乌有。同时，新病毒种类在不断出现，危害性在不断增强，更让人们处处担惊受怕。

与病毒程序相伴相随的是黑客程序。它的出现虽然要比病毒程序晚许多年，其盛行只是近几年随着计算机网络的普及才开始的，但它的威胁性和破坏性比病毒更大。黑客程序通常

是一类具有远程控制、连续攻击、远程侦听等能力的计算机程序。有人称之为“间谍程序”，还有人把它统称为病毒程序。其实笔者认为这是不妥的，毕竟它与普通的病毒程序相比有太多的不同之处。如病毒程序一般具有复制能力，而黑客程序则通常没有。但它们都具有一定的破坏性。如病毒程序可以破坏系统或数据文件，使系统瘫痪或数据丢失；至于黑客程序，除了一些木马类程序主要用来控制目标计算机、非法获取对方重要信息外，还有一些黑客程序会对系统安全漏洞进行攻击，使系统崩溃。它们各自的主要特点将在本章后面详细介绍。

木马程序（特洛伊木马）就是一种典型的黑客程序。黑客们通过它们可以获取目标系统中的重要数据。它不仅可以使受攻击的计算机系统损坏、数据丢失，那些掌控这些黑客程序的黑客们，还可以通过这些黑客程序控制被攻击的计算机系统，盗取被攻击计算机系统中的重要信息和数据，如用户账户名和密码、上网账号、银行账户和密码、企业关键部门信息数据等，这些所带来的损坏远比破坏系统更严重。很可能你的上网账户中每月得多交好多钱，你的银行账户中的存款可能不翼而飞，你的公司投标标书中标的事先被竞争对手获知，而致使竞标失败等。当然黑客程序不全部是木马程序，还有些是专门用来入侵、攻击对方网络，使网络服务器系统瘫痪的程序。据有关数据统计，全球 6 000 多个大型网站都遭受过大型的黑客攻击，其中就包括微软、Google 等著名公司的官方网站。我国成为遭受网络攻击最为频繁的国家之一，国内几乎所有的大型网站都受到过黑客的攻击，如网易、新浪、雅虎和腾讯等。

2. 病毒和黑客程序的传播途径

病毒或黑客程序的传播途径可以是多种多样的。可以是文件传播形式，如从网上下载文件时，该文件本身就带有病毒或黑客程序（因为病毒或黑客程序本身非常精小，从容量上不易被发现），当下载运行后，这些病毒或黑客程序就会从下载的文件中脱离，感染其他文件。还有一种典型的传播途径，那就是邮件传播，通过在邮件附件（如 Office 文档）中带有病毒或黑客程序的文件来传播，同样用户只要打开邮件附件中的文件就会感染，如宏病毒、求职信病毒等。目前还出现一种通过网上比较漂亮的女孩图片的传播方式，只要用户一点击这类图片，木马程序就会链接到一个网址，下载木马程序到你的计算机系统中。“传奇木马”变种 GE 系专偷传奇账号的木马病毒，运用键盘和鼠标挂钩技术窃取传奇游戏账号、密码等信息，再通过电子邮件发送给病毒作者。

以上说的传播途径只是几种主要的，还有许多虽然不是主要的，但也经常见到，如网页脚本病毒、控件病毒和动画病毒等。它们可以分别通过执行（有些是自动执行的）网页上的某个脚本文件、控制控件，或点击运行动画等来下载病毒或黑客程序，以达到传播之目的。

3. 病毒和黑客程序的查杀

病毒和黑客程序这两种安全隐患不仅可以来自企业外部网络，还可以通过企业网络内部进行传播，所以我们在预防时要全面兼顾。

病毒与黑客程序其实都是一个个的文件，只是它们与普通文件有些不一样。因为他们可以对其他文件进行破坏，而且还有自我复制及感染、传播其他文件的特点。它们还具有隐蔽性。所以尽管我们知道这些文件危害非常之大，都想把它斩尽杀绝，但却很难凭自己掌握的知识来识别、查杀每个病毒或黑客文件，必须借助专门的工具。对于病毒必须依靠病毒查杀软件进行查杀，典型的杀毒软件，如金山毒霸、瑞星杀毒软件、江民的 KV 杀毒软件和诺顿杀毒软件等，它们目前的最新版本都为 2005 版。而木马等黑客程序必须通过木马查杀软件，如木马克星、反间谍专家、金山木马专杀等来查杀。对其他黑客攻击可以通过路由器和防火墙的包过滤功能来阻止。

以上病毒和黑客程序的查杀只是一个事后补救的措施，而在实际工作中我们应坚持预防第一的原则。在外部网络方面，尽可能不进入非正规网站下载软件；不浏览不健康网站或图片（其中包括大量病毒或黑客程序文件）等内容；不允许用户使用像 QQ、MSN 之类的即时通信软件。因为利用这类工具进行文件传输存在非常大的安全隐患，从源头上尽可能减少外部网络中的病毒和黑客程序的入侵机会。而在企业内部网络中，我们主要是要加强安全意识，规范软盘、光盘的使用，尽可能少地为用户计算机上安装软驱和光驱。安装有软驱、光驱的用户，在使用这些设备读取来自外部网络的数据时也要遵守使用前申请，使用后备案的管理制度。

最后要提醒大家的是，在网络中目前出现一种网络病毒——可以很迅速地在整个网络中传播，破坏性极强，你根本不可能在连接网络的情况下对任何一台计算机进行病毒查杀，而应就整个网络同步查杀，或者断开网络连接后独立查杀。对于企业用户来说应该采取更加严密的网络防毒系统，而不是像个人那样采用单机版的防毒软件。具体网络防病毒系统的部署和病毒查杀方法参见本系列图书《网管员必读——超级网管经验谈》一书。

1.1.2 对基于操作系统的安全漏洞的攻击的防护

黑客为了达到他们的攻击目的，就必须寻找一个攻击入口，这些入口通常被称为“安全漏洞”。所有软件都可能存在安全漏洞，但操作系统的安全漏洞最多，也是黑客们认为最有利用价值的，因为利用这些操作系统的安全漏洞最容易实现他们预期的攻击目标。同时，操作系统是控制整个计算机和网络系统的安全核心，选择操作系统的安全漏洞进行攻击，可以迅速产生巨大的破坏性，使被攻击方迅速处于瘫痪或崩溃状态。正因如此，黑客们在实施攻击前，往往首先要寻找的就是对方操作系统的安全漏洞，然后再有针对性地利用相应攻击手段，实现攻击。

1. 操作系统安全漏洞的来源

操作系统的安全漏洞可能是多方面的。有些是操作系统程序本身自带的，这主要是由于开发商在进行程序开发时没有考虑周全（俗称有“Bug”），这些漏洞一般都可以通过安装开发商提供的安全补丁程序来修复。还有一些是用户自身配置不当造成的，如打开一些非必要的端口，设置了过多、过高权限的磁盘和文件共享，或者用户权限的配置不当（有的还可能是在注册表中）等。这些漏洞就不能通过安装补丁来修复了，而必须由用户自己重新设置来解决。

黑客们经过潜心研究终于发现，现在主流的操作系统都存在许多安全漏洞，特别是容易操作、广受喜爱的微软 Windows 操作系统。于是早在 20 世纪中后期微软就迫于黑客们的压力不断地为自己的软件开发各种各样的安全漏洞补丁软件。尽管如此，还是不时地从各种途径得知，某某 Windows 系统又发现重大安全漏洞之类的消息。正因如此，有人开始认为，微软的 Windows 系统自身确实存在许多安全问题，在安全性方面远不如 UNIX 或其他操作系统。其实这不完全正确。微软的 Windows 的确比其他主要以命令行方式操作的操作系统更为脆弱，因为它的配置基本上都是采用非常容易掌握的图形界面，这样同样也就降低了黑客们入侵、攻击 Windows 系统的门槛，加上使用 Windows 的用户本来就多，有句古话不是说“木秀于林，风必摧之”吗？微软的 Windows 受到这么多用户的喜爱，必然所受的攻击也多些，这不难理解，谁会找那些很少人用的系统来攻击呢？其实 UNIX 和 Linux 同样存在这样或那样的安全漏洞，而且由于它们所带来的损失要远比 Windows 系统的损失多，因为使用 UNIX 或 Linux 系统的企业用户通常是大型企业，或者关键数据企业，如金融、电信、证券和保险等，它们

的数据比一般企业更加重要。只不过因为用这类系统的用户相对比较少，所以黑客们关注的程度不像广为使用的 Windows 系统那样，这样所发现的 UNIX 和 Linux 系统的安全漏洞也就少了许多，从某种意义上来说，是更加安全些。

虽然系统本身所具有的安全漏洞从理论上说可以完全由开发商自己事先堵住，但事实上，在当前这个“快餐经济”时代，这些软件开发商，包括全球最大的软件开发商微软（Microsoft）也一样，他们通常不是把一款软件设计得十分完善后才推出市场，而是在软件基本成型，当时不存在大的安全和使用隐患的情况下就匆匆上市了。为什么？抢占市场先机啊，竞争这么激烈，时间就是效益，甚至关乎企业的生命。正因如此，所以这些新软件在上市后通常不到二三个月就会被人发现存在许多安全漏洞，然后这些软件开发商就会根据这些被发现的安全漏洞开发相应的补丁进行漏洞修复。微软自 Windows NT 4.0 开始，就开始发布大量的安全或功能补丁，如 Windows NT 4.0 最多有 SP6，最新的 Windows XP 大的补丁为 SP2，小的更是很多了。其他版本也一样。这些都可以从微软的官方网站上直接下载安装，当然必须是正版注册用户。让笔者记忆最深的就是 2003 年的震荡波病毒，它就是利用 Windows XP 和 Windows Server 2003 系统的一种远程服务漏洞进行攻击的，迫使目标计算机系统重新启动。如果没有安装后来的补丁，只要一连上互联网就会很快弹出一个一分钟倒计时重启框，过了一分钟就会强制系统重新启动，根本无法进行任何互联网应用。

2. 操作系统安全漏洞发现

要知道自己的系统到底存在哪些安全漏洞，一般来说只能通过专门的漏洞扫描工具。当然如果你对网络安全方面的知识掌握得非常全面的话，也可以自己去一一发现。不过这类用户的系统中通常就不会具有这些所谓的安全漏洞，因为他们在设置系统前就已清楚了哪里可能存在安全隐患，事先就堵住了。目前一些主要杀毒软件都带有安全漏洞扫描功能，如金山毒霸 2005、瑞星杀毒软件 2005 等，通过它们可以十分方便地查找自己系统的安全漏洞，然后再一一修复。下面仅以金山毒霸 2005 中的漏洞扫描工具为例进行漏洞查找介绍。具体操作步骤如下。

步骤

（1）双击状态栏中的金山毒霸 2005 图标，打开金山毒霸 2005 程序主界面，如图 1-1 所示。

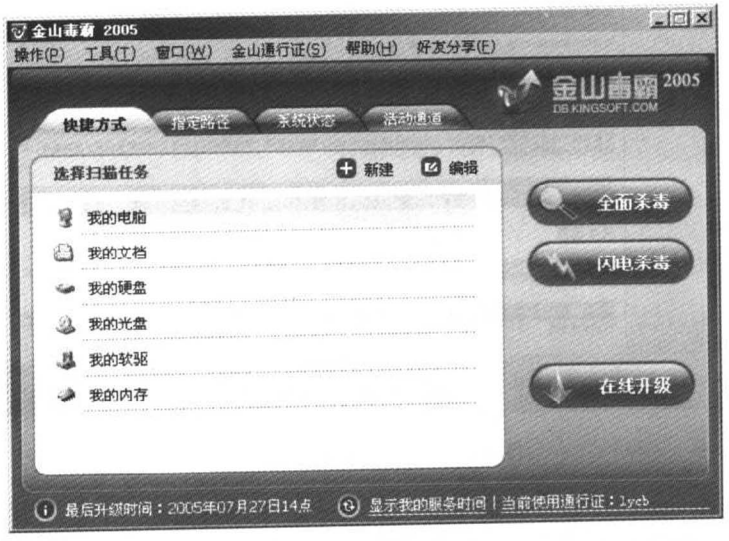

图 1-1　“金山毒霸 2005”主界面

（2）执行【工具】→【系统漏洞扫描】菜单命令，打开如图 1-2 所示的界面。

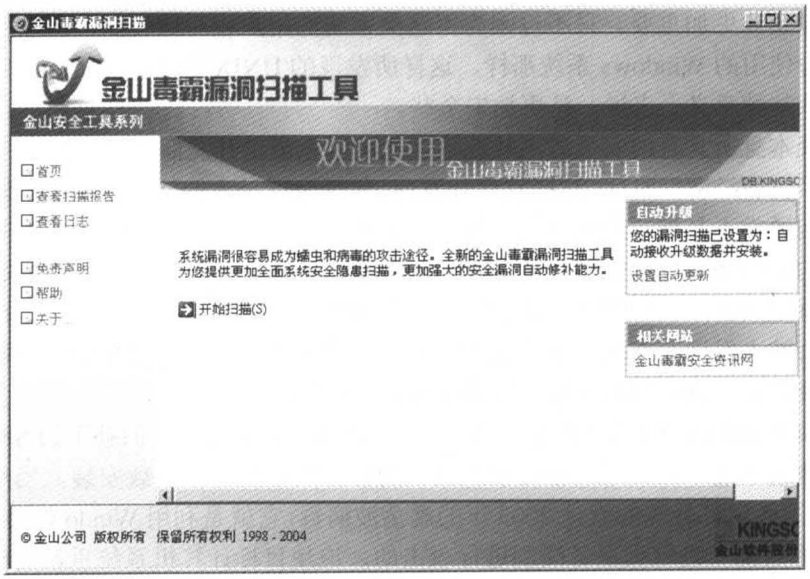

图 1-2 “金山毒霸漏洞扫描”界面

（3）单击“开始扫描”链接，首先会弹出一个使用协议确认对话框，单击【同意】按钮，程序即开始自动扫描。这里需要几分钟时间。完成后会弹出一个检测报告（如图 1-3 所示），在一开始列出您的当前系统的安全等级，然后分类列出各类安全漏洞。有些漏洞通过金山毒霸可以修复，有些可以通过相应漏洞后面的链接从微软的官方网站下载补丁进行修复，还有些是用户账户、共享和注册表设置问题，需要用户自己按提示重新设置来修复。

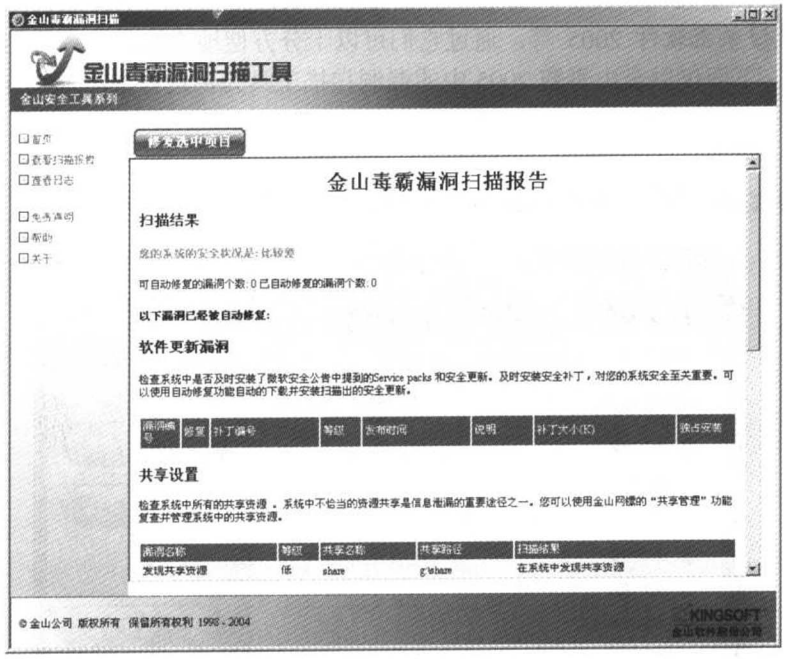

图 1-3 金山毒霸漏洞扫描报告

以上利用漏洞扫描软件进行漏洞修复，只是一种事后补救措施，更多的应该是我们在平常的系统使用中，经常利用 Windows 系统的“自动更新”（在控制面板中）或者“Windows Update”（在 IE 浏览器的“工具”菜单中）进行不定期的补丁更新安装，只有这样才能及时地把这些系统漏洞补上，防止黑客们利用这些漏洞进行攻击。这一点非常重要，特别是对于