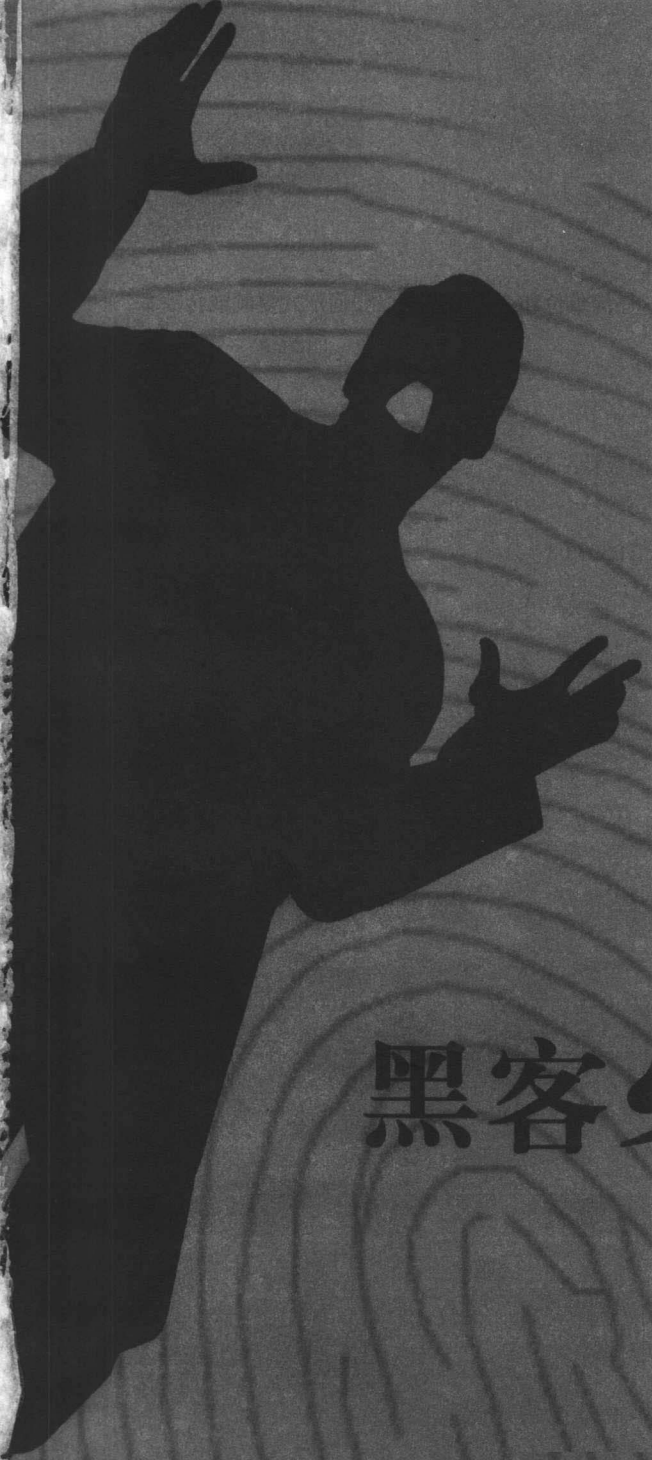
100个精彩的黑客攻防案例
100招黑客攻击的必杀密技
100次挑明黑客攻击的底细
100项安全技术与黑客软件
100种万无一失的防御方法

黑客必杀技100例

吴博维 袁博/编著

赠送：
免费提供本书所讲实例中涉及的黑客技术资料与相关软件，下载精华包或完全包请访问 www.21books.com

中国青年出版社
http://www.21books.com http://www.cgchina.com



黑客必杀技100例

吴博维 袁博/编著

中国青年出版社
CHINA YOUTH PRESS
http://www.21books.com http://www.cgchina.com

（京）新登字083号

图书在版编目(CIP)数据

黑客必杀技100例 / 吴博维 袁博 编著；北京：中国青年出版社，2003

ISBN 7-5006-5482-0

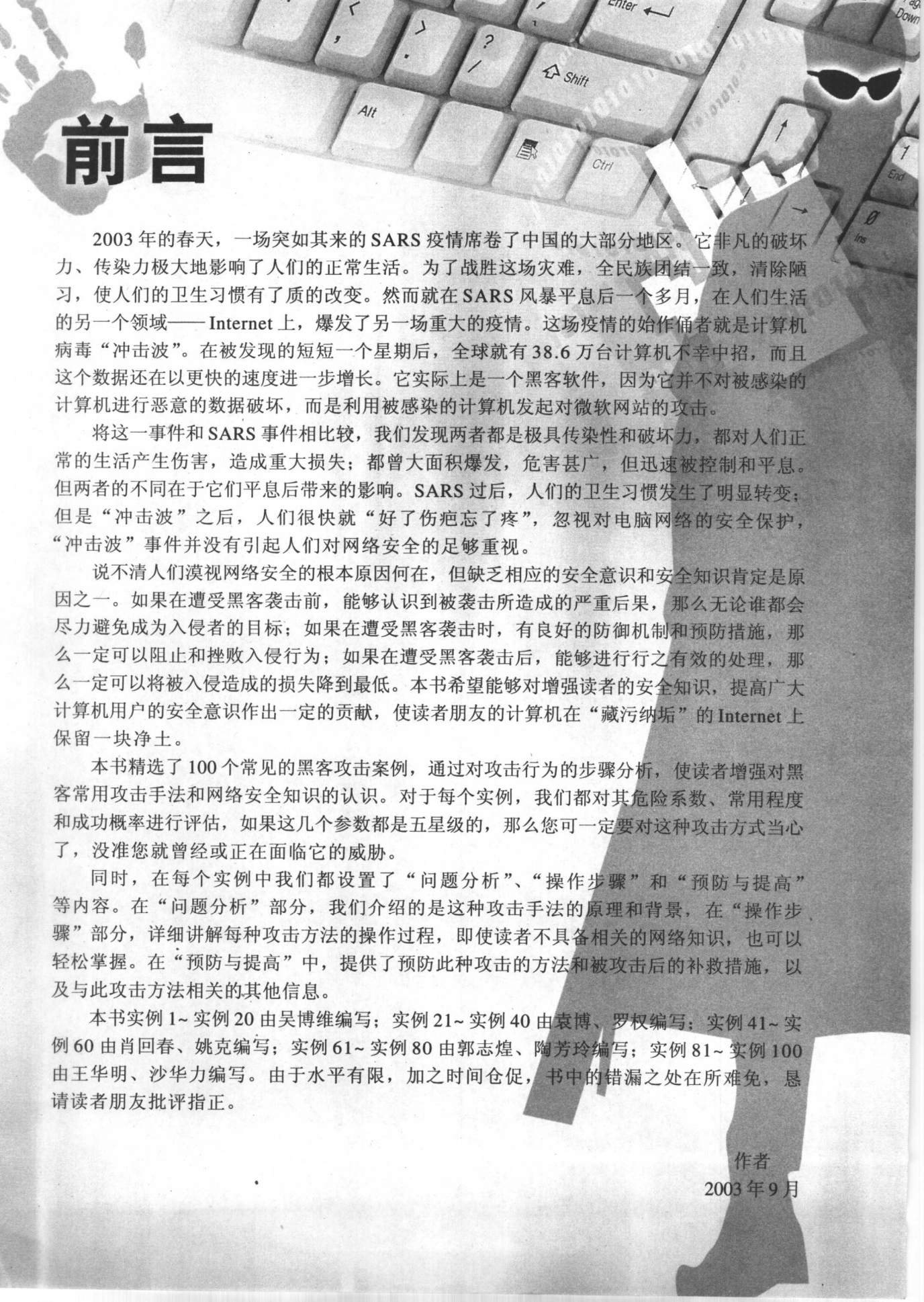
I. 黑... II.①吴...②袁... III.计算机网络—安全技术， IV. TP393.08

中国版本图书馆CIP数据核字（2003）第090668号

责任编辑：陈建华
　　肖　辉
　　刘利平
责任校对：王志红

书　　名：黑客必杀技100例
编　　著：吴博维 袁博
出版发行：中国青年出版社
　　地址：北京市东四十二条21号　邮政编码：100708
　　电话：(010) 84015588　传真：(010) 64053266
印　　刷：中国农业出版社印刷厂
开　　本：787×1092　1/16　印　张：23.75
版　　次：2003年11月北京第1版
印　　次：2003年11月第1次印刷
书　　号：ISBN 7-5006-5482-0/TP·353
定　　价：35.00元

前言



2003 年的春天，一场突如其来的 SARS 疫情席卷了中国的大部分地区。它非凡的破坏力、传染力极大地影响了人们的正常生活。为了战胜这场灾难，全民族团结一致，清除陋习，使人们的卫生习惯有了质的改变。然而就在 SARS 风暴平息后一个多月，在人们生活的另一个领域——Internet 上，爆发了另一场重大的疫情。这场疫情的始作俑者就是计算机病毒“冲击波”。在被发现的短短一个星期后，全球就有 38.6 万台计算机不幸中招，而且这个数据还在以更快的速度进一步增长。它实际上是一个黑客软件，因为它并不对被感染的计算机进行恶意的数据破坏，而是利用被感染的计算机发起对微软网站的攻击。

将这一事件和 SARS 事件相比较，我们发现两者都是极具传染性和破坏力，都对人们正常的生活产生伤害，造成重大损失；都曾大面积爆发，危害甚广，但迅速被控制和平息。但两者的不同在于它们平息后带来的影响。SARS 过后，人们的卫生习惯发生了明显转变；但是“冲击波”之后，人们很快就“好了伤疤忘了疼”，忽视对电脑网络的安全保护，“冲击波”事件并没有引起人们对网络安全的足够重视。

说不清人们漠视网络安全的根本原因何在，但缺乏相应的安全意识和安全知识肯定是原因之一。如果在遭受黑客袭击前，能够认识到被袭击所造成的严重后果，那么无论谁都会尽力避免成为入侵者的目标；如果在遭受黑客袭击时，有良好的防御机制和预防措施，那么一定可以阻止和挫败入侵行为；如果在遭受黑客袭击后，能够进行行之有效的处理，那么一定可以将被入侵造成的损失降到最低。本书希望能够对增强读者的安全知识，提高广大计算机用户的安全意识作出一定的贡献，使读者朋友的计算机在“藏污纳垢”的 Internet 上保留一块净土。

本书精选了 100 个常见的黑客攻击案例，通过对攻击行为的步骤分析，使读者增强对黑客常用攻击手法和网络安全知识的认识。对于每个实例，我们都对其危险系数、常用程度和成功概率进行评估，如果这几个参数都是五星级的，那么您可一定要对这种攻击方式当心了，没准您就曾经或正在面临它的威胁。

同时，在每个实例中我们都设置了“问题分析”、“操作步骤”和“预防与提高”等内容。在“问题分析”部分，我们介绍的是这种攻击手法的原理和背景，在“操作步骤”部分，详细讲解每种攻击方法的操作过程，即使读者不具备相关的网络知识，也可以轻松掌握。在“预防与提高”中，提供了预防此种攻击的方法和被攻击后的补救措施，以及与此攻击方法相关的其他信息。

本书实例 1~ 实例 20 由吴博维编写；实例 21~ 实例 40 由袁博、罗权编写；实例 41~ 实例 60 由肖回春、姚克编写；实例 61~ 实例 80 由郭志煌、陶芳玲编写；实例 81~ 实例 100 由王华明、沙华力编写。由于水平有限，加之时间仓促，书中的错漏之处在所难免，恳请读者朋友批评指正。

作者

2003 年 9 月

目录

实例 1 如何破解 Access 2000 文件的密码 …… 1
实例 2 如何破解 Office XP 文件的密码 …… 4
实例 3 如何修复注册表 …… 8
实例 4 如何破解 IE 分级审查密码 …… 11
实例 5 如何查看“*”隐藏的密码 …… 13
实例 6 如何清除硬盘分区表信息 …… 15
实例 7 如何破解 Windows 2000 登录密码 …… 18
实例 8 如何不用密码进入 Windows XP …… 20
实例 9 如何破解.zip 文件的密码 …… 22
实例 10 如何破解开机密码 …… 25
实例 11 如何破解 Windows 98 共享密码 …… 27
实例 12 如何破解.RAR 文件的密码 …… 31
实例 13 如何破解屏幕保护的密码 …… 35
实例 14 如何清除笔记本电脑密码 …… 37
实例 15 如何破解 Foxmail 密码 …… 39
实例 16 如何破解 PCAnyWhere 的密码 …… 43
实例 17 如何利用 WinRAR 自解压程序绑定木马 …… 45
实例 18 如何使用 QQ 发送大字和图案 …… 49
实例 19 如何在 QQ 中查看对方的 IP …… 52
实例 20 QQ 炸弹——飘叶千夫指 …… 54
实例 21 如何通过后台记录破解 QQ 密码 …… 57
实例 22 如何使用 QQ 木马盗取 QQ …… 59
实例 23 如何使用“广外幽灵”盗取 QQ …… 61
实例 24 如何使用软件探测 QQ 的密码 …… 63
实例 25 如何使用 Hiddukel 窃取 QQ 密码 …… 66
实例 26 如何监听“联众密码” …… 69
实例 27 如何窃取《传奇》的密码 …… 71

实例 28 如何破解网吧管理软件密码 ……74
实例 29 如何破解硬盘保护卡 ……77
实例 30 如何攻击 Windows 系统的 IP Hacker ……79
实例 31 系统炸弹 WinNuke ……81
实例 32 如何利用 Ghost Mail 发送匿名邮件 ……83
实例 33 邮件炸弹 ……86
实例 34 如何将网页浏览者的硬盘改为共享 ……88
实例 35 如何利用共享进行攻击 ……92
实例 36 如何攻击 HTML 留言板 ……94
实例 37 Net 命令的常见用法 ……97
实例 38 超级扫描器 SuperScan …… 105
实例 39 如何利用“小区宽带”漏洞进行攻击 …… 110
实例 40 如何对网络入侵命令进行防范 …… 112
实例 41 如何使用流光探测目标主机打开的端口 …… 116
实例 42 如何使用流光探测 SQL 主机 …… 120
实例 43 使用“流光”进行 IPC 探测 …… 124
实例 44 如何使用流光的 Sensor …… 128
实例 45 如何用 X-WAY 对端口进行扫描 …… 132
实例 46 如何应用端口扫描软件 NetBrute …… 136
实例 47 如何破解 E-mail 账号 …… 140
实例 48 如何破解电子邮件密码 …… 144
实例 49 如何破解收费网站 …… 146
实例 50 如何破解基于 Windows 2000 的聊天室 …… 149
实例 51 Windows 2000 的 Telnet 客户端 …… 152
实例 52 多功能后门程序 wollf …… 156
实例 53 如何应用与防范冰河 …… 160
实例 54 如何判断一个主机的安全 …… 168

实例 55 端口监听工具 LockDown Port Monitor ····· 172
实例 56 如何用 ASP 程序漏洞取得系统管理员权限 ····· 178
实例 57 检测入侵的方法 ····· 180
实例 58 恶意捆绑.EXE 文件 ····· 184
实例 59 如何利用 Word 的漏洞进行攻击 ····· 186
实例 60 DoS 之洪水攻击 ····· 188
实例 61 Telnet 客户端 cterm 2000 ····· 190
实例 62 如何利用 MIME 的漏洞执行.exe 文件 ····· 195
实例 63 如何破解 Microsoft Outlook 2002 ····· 198
实例 64 pcAnywhere 的局域网控制 ····· 200
实例 65 pcAnywhere 远程控制 ····· 204
实例 66 pcAnywhere 的远程文件传输 ····· 210
实例 67 如何防范 idq 溢出攻击 ····· 215
实例 68 IIS ISAPI Printer 远程溢出攻击 ····· 218
实例 69 如何手工防范的 Unicode 漏洞 ····· 221
实例 70 如何利用 Unicode 漏洞发起的攻击 ····· 226
实例 71 如何模拟 IPC 入侵过程 ····· 231
实例 72 如何利用 IPC$ 取得主机管理员权限 ····· 234
实例 73 如何关闭默认共享 ····· 239
实例 74 如何在 Windows 2000 下防范 IPC$ 空连接 ····· 243
实例 75 如何在 Windows XP 下防范 IPC$ 空连接 ····· 249
实例 76 如何利用输入法漏洞进入 Windows 2000 ····· 252
实例 77 如何独享远程桌面连接的端口 ····· 257
实例 78 如何在 Windows NT/2000 主机中提升权限 ····· 260
实例 79 得到 Admin 权限后能做什么 ····· 262
实例 80 如何使局域网内的计算机成为自己的代理服务器 ····· 268
实例 81 如何安装后门 ····· 272

实例 82 如何制作代理跳板 …… 277
实例 83 如何使用代理突破网关限制 …… 282
实例 84 如何用.chm 帮助文件进行攻击 …… 286
实例 85 如何利用 IE6 漏洞读取系统文件 …… 288
实例 86 来自 Web 的攻击与防范 …… 290
实例 87 如何配置 Windows 2000 服务器的属性 …… 294
实例 88 如何进行 Windows 2000 远程访问策略的配置 …… 301
实例 89 如何配置一个安全的 Windows 2000 服务器 …… 310
实例 90 黑客如何躲避检测 …… 322
实例 91 如何查找潜伏的木马 …… 325
实例 92 对 UNIX 服务器的简单入侵及防范 …… 328
实例 93 电脑幽灵 pcGhost …… 333
实例 94 网络精灵 NetSpy …… 335
实例 95 网络公牛 Netbull …… 344
实例 96 如何应用网络神偷 …… 348
实例 97 139 端口漏洞 …… 353
实例 98 无赖小子 WAY …… 355
实例 99 网络嗅探器 Spynet Sniffer …… 358
实例 100 网页欺骗 …… 368

实例 1　如何破解 Access 2000 文件的密码

危险程度：☠☠☠☠

使用频率：💡💡💡

操作难度：🔧🔧

成 功 率：90%

问题分析

Access2000 的密码字符，是以一种特殊的格式存储在该文件内部。因此，如果要破解该文件的密码，只要从文件中取得相应的密码字符即可。当前常见的 Access 密码破解软件，都是利用这种原理来操作的。

Access 2000 是常见的数据库文件类型，它的扩展名为.mdb。Access 2000 支持用户密码，为 Access 文件加密的方法如下：

（1）单击“文件>打开”，在“打开”对话框中选择欲添加密码的文件，然后单击“打开”按钮右边的小箭头，从下拉菜单中选择“以独占方式打开”，如图 1-1 所示。

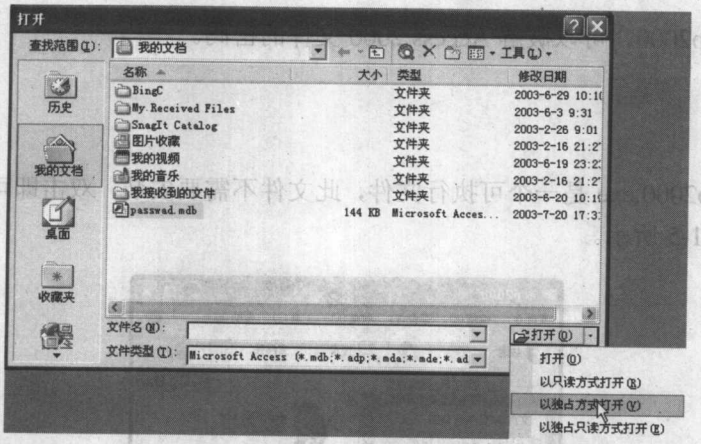


图 1-1　以独占方式打开文件

（2）从 Access 的菜单中选择“工具>安全>设置数据库密码”，如图 1-2 所示。

（3）打开的“设置数据库密码”对话框如图 1-3 所示。

MJS22/10

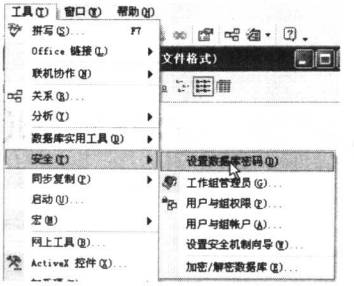


图 1-2　设置数据库密码

从这里就可以为数据库文件添加密码了。

（4）数据库文件添加密码以后，再次尝试打开该文件，就会打开一个“输入密码”对话框，要求首先输入密码。如图 1-4 所示。

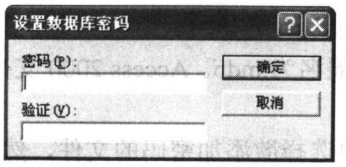


图 1-3　“设置数据库密码”对话框

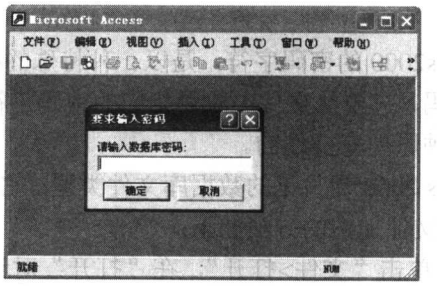


图 1-4　“输入密码”对话框

使用软件 acp2000，可以破解 Access 2000 文件的密码。

操作步骤

步骤 1　acp2000.exe 是一个可执行文件，此文件不需要安装，双击即可运行，文件大小为 28 KB，如图 1-5 所示。

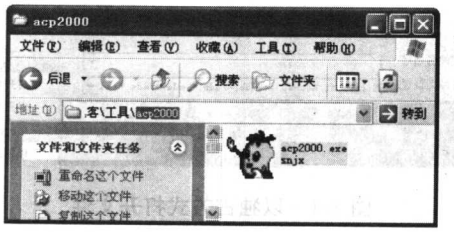


图 1-5　acp2000.exe

步骤 2　双击该文件，可以看到其程序主界面，如图 1-6 所示。

步骤 3　程序使用很简单。单击“浏览”按钮，从对话框中选择欲进行解密的文件，如图 1-7 所示。

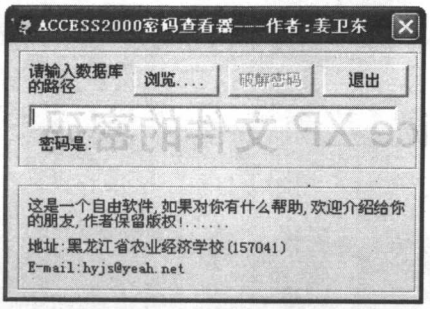


图 1-6　程序主界面

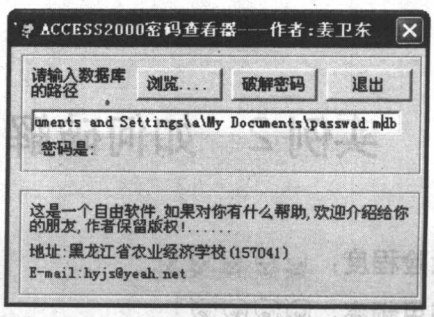


图 1-7　选择进行解密的文件

步骤 4　单击“破解密码”按钮，则该文件的密码将显示在窗口中，如图 1-8 所示。

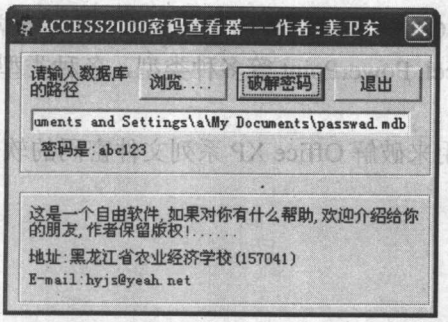


图 1-8　破解密码

步骤 5　在打开 Access 文件的“要求输入密码”对话框中，输入通过破解得到的 abc123，文件将顺利被打开。

预防与提高

目前常见的数据库密码破解软件都是针对 Access 2000 的。所以如果要防止密码被破解，只需使用其他大型数据库管理系统，例如 SQL Server 或 Oracle 等即可。

如果没有换用其他数据库管理系统的条件，而不得不使用 Access 的话，那么除了为 Access 文件加密码外，还可以同时使用其他安全措施，例如将文件存放在不易被发现的目录中，对目录进行加密等。特别重要的文件，可以将其存放在可移动介质上，进行物理上的保密存放。

实例 2　如何破解 Office XP 文件的密码

危险程度：

使用频率：

操作难度：

成 功 率：88%

Office XP 是 Microsoft Office 系列软件的最新版本，也是最常用的办公系列软件。Office 系列包括 Word, Access, Excel, PowerPoint 等多种类型，各种类型的软件，所对应的文件的扩展名也不相同。

AOXPPR 是一款专门用来破解 Office XP 系列文件密码的软件。本例仅以 Word 和 Access 为例，介绍其具体用法。

问题分析

本实例分两个部分，分别介绍了对 Office XP 中的 Access 和 Word 的破解方法，因为 AOXPPR 对这两种类型的文件采取了不同的破解原理。

对于 Access 类型的文件，由于其密码字符串以一种特殊的格式保存在文件内部。因此，只要读取该字符串就可以获得密码。而对于 Word 类型的文件，则要用“穷举法”来验证。所谓“穷举法”就是使用所有的包括字母、数字和特殊符号在内的字符，按照所有可能的排列顺序来一一尝试，直到能够打开该文件为止。

操作步骤

Access 是常见的数据库文件类型，它的扩展名为.mdb。本例以文件 Password.mdb 和 Password2.mdb 两个带密码的文件进行介绍。

步骤 1　AOXPPR 支持英文和俄文两个语种，默认的界面是英文的，如图 2-1 所示。

步骤 2　单击工具栏最左边的“打开文件”按钮，从中选择欲进行解密的文件，首先选择 password.mdb，如图 2-2 所示。

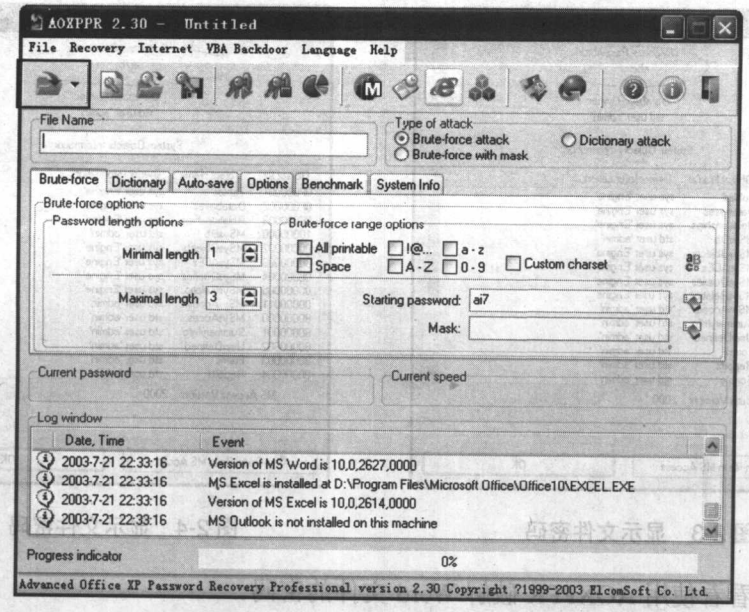


图 2-1　AOXPPR 界面

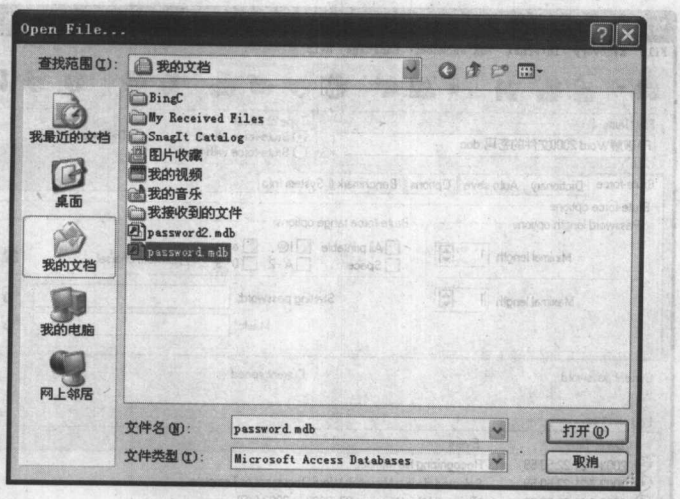


图 2-2　选择 password.mdb 文件

步骤 3　单击“打开”按钮，打开文件信息对话框。从中可以看到文件的密码已经显示出来，如图 2-3 所示。

步骤 4　破解速度太快，以至怀疑这是因为密码设置过于简单的原因，于是试着来打开 password2.mdb，同样密码应声而出，如图 2-4 所示。

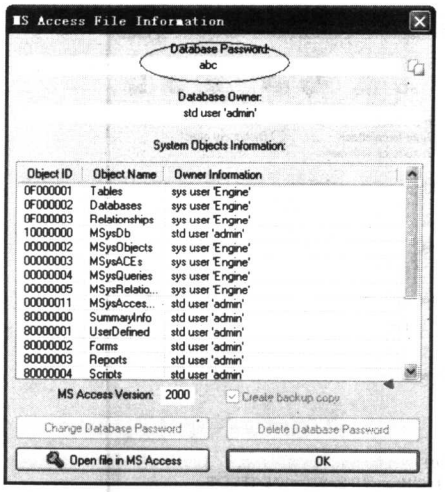


图 2-3　显示文件密码

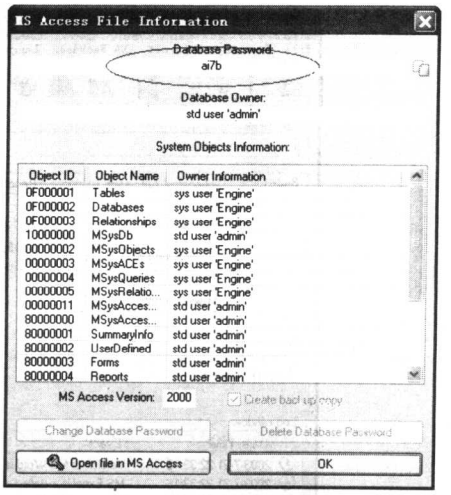


图 2-4　显示文件密码

接下来，看看使用 AOXPPR 破解 Word 文件的密码。

步骤 1　首先选中欲进行解密的文件，如图 2-5 所示。

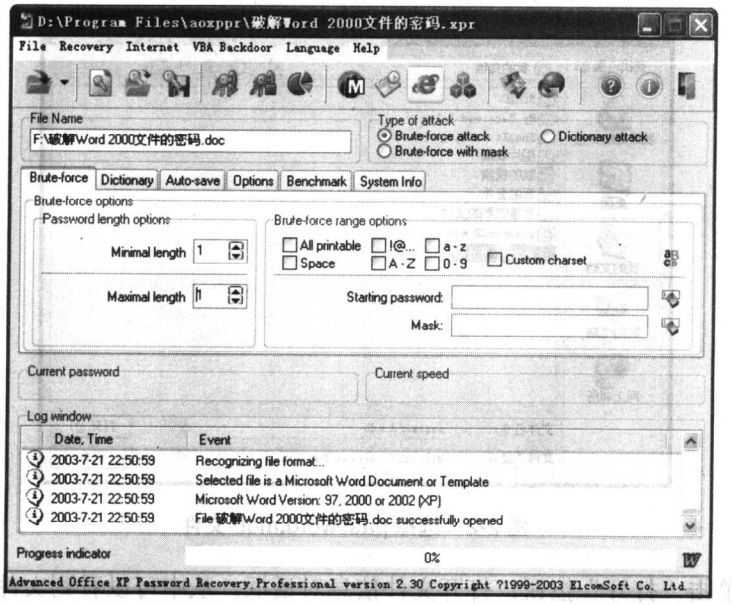


图 2-5　打开 Word 文件

步骤 2　在 Brute-force 选项卡中，如图 2-6 所示设置 Password length option 和 Brute-force range option 中的各选项。

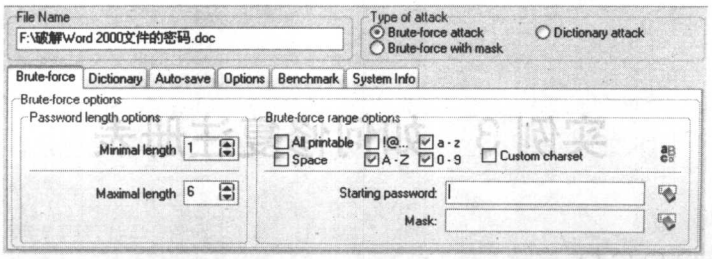


图 2-6　Brute-force 选项卡

步骤 3　在 Options 选项卡中，按如图 2-7 所示进行设置。

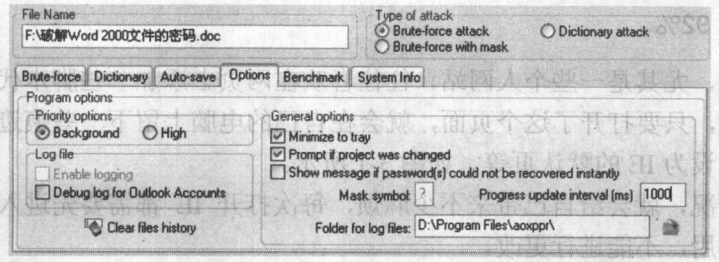


图 2-7　Options 选项卡

步骤 4　单击 Start Rescovery 按钮，破解结果立刻将显示在对话框中，如图 2-8 所示。

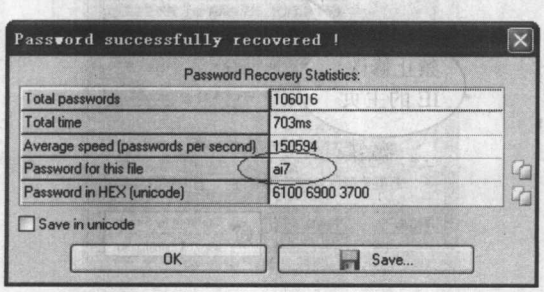


图 2-8　破解结果

从中可以看到 AOXPPR 的破解速度非常快。

预防与提高

此软件对 Access 和 Word 文件的解密采用了两种不同的原理。解密 Access 文件时，采用解析文件的方法得到密码；而解密 Word 文件时，采用了穷举法。

防止文件被解密的方法，就是使用其他一些安全性较高的办公软件。同时，对保存文件的文件夹进行加密，也是增加安全系数的一种方法。有必要的话，可以对秘密文件的存储介质进行物理隔离。

实例 3　如何修复注册表

危险程度：

使用频率：

操作难度：

成 功 率：92%

有很多网站，尤其是一些个人网站，往往喜欢在网页上添加一些脚本代码，使用户在网络上浏览的时候，只要打开了这个页面，就会在自己的电脑上留下一些痕迹，例如将网站地址加入收藏夹、设为 IE 的默认页等。如图 3-1 所示。

遇到这种情况，就会给自己带来不少麻烦，每次打开 IE 都需要先进入那个页面，而且主页更改还被禁用，不能进行更改。

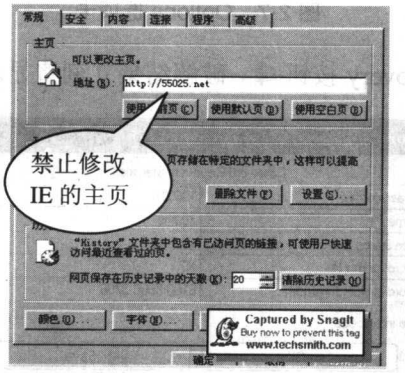


图 3-1　Internet 选项

问题分析

其实，是否允许修改主页设置，是由注册表中的一个选项控制的。接下来就介绍如何通过修复注册表来清理这些限制。

操作步骤

“Windows 优化大师”是一款优秀的 Windows 辅助工具，它提供的注册表清理功能也非常强大，可以完全清除各种注册表限制。

步骤 1　打开“Windows 优化大师”，在左边的分类列表中选择“系统性能优化”下的“网络系统优化”，如图 3-2 所示。

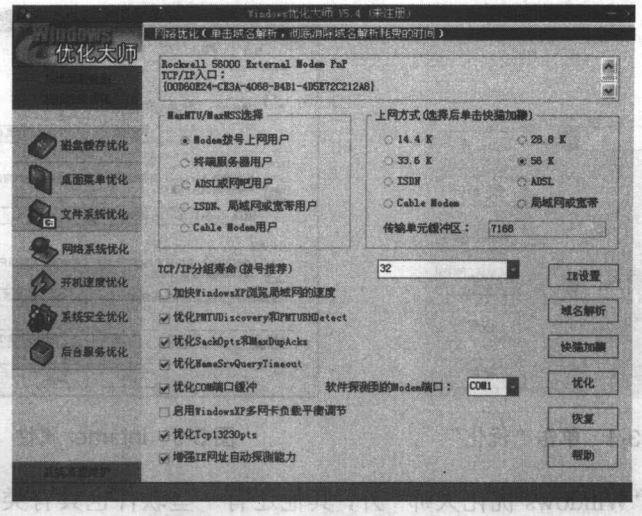


图 3-2　Windows 优化大师

步骤 2　在对应的页面中单击“IE 设置”按钮，打开“IE 浏览器设置”对话框，如图 3-3 所示。

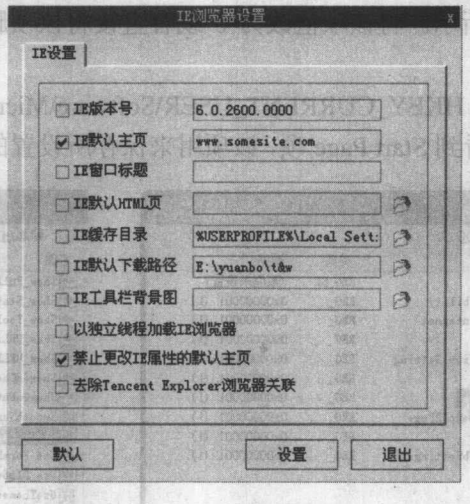


图 3-3　IE 浏览器设置

步骤 3　从中将“IE 默认主页”和“禁止更改 IE 属性的默认主页”复选框取消，并删除“IE 默认主页”后面的网站地址，然后单击“设置”按钮，确认设置并返回主界面。

步骤 4　在程序主界面上单击“优化”按钮，使用前面的设置优化网络，如图 3-4 所示。

步骤 5　不用重启，打开“Internet 属性”对话框，可以看到限制已经取消，如图 3-5 所示。单击“使用空白页”按钮，即可将 IE 启动时打开的页面设置为空白页。