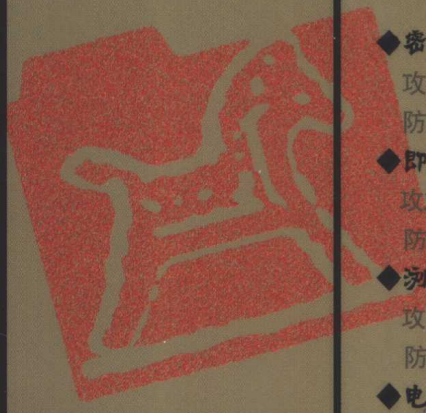
Book 远望图书 微型计算机 MicroComputer
www.cbook.com.cn

十余位资深安全专家打造
上百个黑客攻防实例重现

黑客攻防必杀技

远望图书部 编

攻篇 多种方法，不同思路，攻得精彩
防篇 多管齐下，不留纰漏，防得稳固



◆密码攻防必杀技
攻篇：Office 文档、压缩文件、论坛、Web 邮箱、系统登录……密码信手拈来
防篇：Office 文件、电子邮件、光盘、系统文件、PDF 文件……加密滴水不漏

◆即时通信软件攻防必杀技
攻篇：QQ 恶意代码、软件探测 QQ 密码、获取 ICQ 密码、MSN 消息攻击机……
防篇：斩断 QQ 的“尾巴”、QQ 防黑秘技、各类型 QQ 黑软的分析与防范……

◆浏览安全攻防必杀技
攻篇：攻破加密网页、跨站 Script、有害 Java 程序揭密……
防篇：注册表解锁、关闭网页恶意共享、给网页加锁……

◆电子邮件攻防必杀技
攻篇：嗅探工具、邮件炸弹、OE6.0 漏洞……攻击无处不在
防篇：防止邮件地址泄漏、给邮件加锁、数字签名……筑起铜墙铁壁

◆系统漏洞攻防必杀技
攻篇：共享漏洞、IDQ 漏洞、Unicode 漏洞、论坛漏洞……一网打尽
防篇：服务器安全、操作系统安全、关闭常见端口……查缺补漏

◆病毒攻防必杀技
攻篇：蠕虫病毒、宏病毒、网页病毒……全面解析
防篇：诺维格(Mydoom)、冲击波……清除各类病毒

◆木马攻防必杀技
攻篇：各类木马曝光、揭密木马隐身术、自做木马……
防篇：扫描木马、检查端口、软件查杀、手工清除……

◆黑客软件攻防必杀技
攻篇：端口攻击、扫描、嗅探、DDoS、洪水 Ping……轮番上阵
防篇：反监听追踪黑客、抓住木马黑手、狙击远程控制……

配套光盘

〖视频教学〗
IP 地址攻防
QQ 诈骗攻防
软件下载攻防
垃圾邮件防范
聊天室炸弹攻防
冰河木马攻防

〖视频演示〗
Foxmail 密码攻防
GOP 木马盗 QQ 号攻防
RPC 漏洞防范
黑洞 2001 木马攻防
冲击波病毒查杀
SuperScan 使用

人民交通出版社

黑客攻防必杀技

远望图书部 编

人民交通出版社

内容提要

本书每一章节均划分为“攻篇”及“防篇”，精选了100多个精彩的黑客攻击与防范实例。通过对攻击行为的步骤分析，使您学习到黑客常用攻击手法和相关网络安全知识。通过对防御手段的剖析，让您对保障网络安全有更直观的了解。

本书中的实例设置了“问题分析”、“实际操作”和“实现效果”等内容。在介绍每种攻击、防御手法的原理和背景的同时，还一步一步地详细讲解每种攻击、防御手法的操作过程，即使您不具备相关的网络知识，也可以轻松快速地掌握。

图书在版编目（CIP）数据

黑客攻防必杀技／远望图书部编．—北京：人民交通出版社，2004.3

ISBN 7-114-04968-4

Ⅰ.黑… Ⅱ.远… Ⅲ.计算机网络—安全技术

Ⅳ.TP393.08

中国版本图书馆CIP数据核字（2004）第010210号

监　　制／谢　东　　策　划／车东林　张仪平

项目主任／王　炜　戚　斌

执行编辑／莫海雄　张武龙　李　梁

责任编辑／杨　捷

《黑客攻防必杀技》

《Heike Gongfang Bishaji》

远望图书部　编

正文设计：李明忠　　责任校对：莫海雄　　责任印制：张　恺

人民交通出版社出版

北京中交盛世书刊有限公司发行

(100013 北京和平里东街10号 010 64212684)

各地新华书店经销

北京鑫正大印刷有限公司印刷

开本：787×1092　1/16　印张：19　字数：35万字

2004年3月　第1版

2004年3月　第1版　第1次印刷

ISBN 7-114-04968-4

定价：25.00元

（图书+配套光盘）

前言

随着全球信息化的飞速发展，网络作为一种重要的信息传递手段，对于经济的发展和人们之间的交流起着越来越重要的作用。近几年，我国的网络建设突飞猛进，尤其是宽带网建设更是遍地开花，我国互联网用户已经跃居世界第二，成为世界网络大国。网络已经进入我们的日常生活，它与我们的工作、学习、生活息息相关。在网络建设蓬勃发展的同时，网络安全问题也到了令人堪忧的地步。目前，利用计算机网络进行各类违法行为的数量呈上升之势。黑客的攻击方法已超过计算机病毒的种类，总数达近千种。怎样提高网络安全防范水平，防止网络遭到黑客的攻击已成为急需解决的问题。

而对于普通用户来说，QQ密码被盗、游戏账号被盗、遭遇恶意网站……都是经常碰到的烦心事；病毒导致系统瘫痪、被人"种"下木马……也威胁着用户的网络安全；QQ炸弹、邮箱炸弹、聊天室炸弹更让人防不胜防……如何识破"温柔的陷阱"，保护密码的安全？如何给自己的网络筑起"铜墙铁壁"，御黑客于门外？

为了解决读者对网络安全和防范黑客攻击的强烈需求，我们推出了《黑客攻防必杀技》。

本书定位在初中级读者，特别针对黑客攻击手段和网络安全防御，每一个必杀技都以普通读者可能遇到的安全问题提出讲解的线索，力求将黑客和网络安全的实际操作、实际问题讲详细、讲透彻。

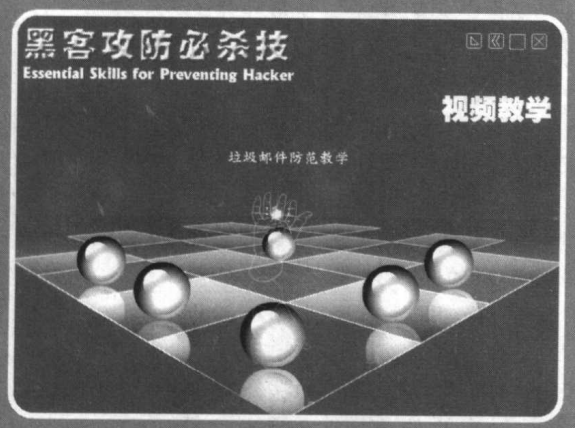
针对读者可能遇到的网络安全问题，将攻篇／防篇的实例根据实际情况划分成"问题分析"（攻击／防守目的分析）、"实际操作"（实际攻击／防守过程）、"实际效果"来讲解，每一个必杀技解决一个到几个网络安全的实际问题，读者可以根据每一篇必杀技速查实际操作，迅速掌握。

针对读者关心，以往类似图书忽略的问题，本书将"攻篇"和"防篇"两部分有机结合，攻篇详细剖析攻击手段是为了更好地防御，防篇揭示预防措施和心得主要是帮助读者提高网络安全程度，使读者阅读一篇必杀技之后能够及时总结和提高。另外，书中将会对第一次出现的黑客攻防相关名词术语等以"小知识"等形式加以注释，以便让读者及时补充相关理论知识。

作为增值服务，配套光盘将收录各种有代表性的攻击手段、防范措施的全过程视频教学，给读者直观的认识。

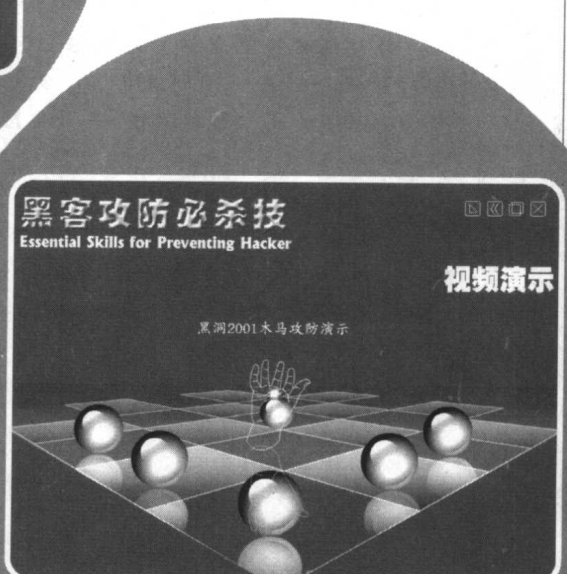
如果您在阅读本书时有任何问题或者意见，请光临远望书盘论坛（http：bbs.cniti.com）"远望图书及光盘"专区并留言，我们将及时予以答复。

光盘导航



[视频教学]

IP 地址攻防
QQ 诈骗攻防
软件下载攻防
垃圾邮件防范
聊天室炸弹攻防
冰河木马攻防



[视频演示]

Foxmail 密码攻防
GOP 木马盗 QQ 号攻防
RPC 漏洞防范
黑洞 2001 木马攻防
冲击波病毒查杀
SuperScan 使用

目 录

第一卷 密码攻防必杀技

作者简介 Tanker，对网络安全有深入了解，涉及个人安全与企业安全。为某网站做过攻防实验室，并担任过劳动部信息安全比赛出题组组长。

【攻 篇】

【防 篇】

第二卷 即时通信软件攻防必杀技

作者简介 蓝雪幽灵，安全站点“蓝色安全实验室”核心成员，爱好编程，专注于网络安全领域，对即时通信软件攻防有深入研究。

【攻 篇】

目 录

第三卷 浏览安全攻防必杀技

作者简介 风之梦，曾为某安全杂志特约作者，对网页浏览攻防颇有心得。在《网管员世界》等报刊发表多篇安全文章。

第四卷 电子邮件攻防必杀技

作者简介 亦可，1997年开始接触网络，2000年起主攻网络安全技术，参与数十本安全图书的编著工作，2003年推出网络安全著作《黑客技术十日通》。

作者简介 冬无秋，主攻计算机网络，对网络安全有多年研究，作为某黑客杂志的在线编辑，个人曾推出数本网络安全专著。

【防 篇】

第五卷 系统漏洞攻防必杀技

作者简介 KAWEN，2000年创建影子鹰安全网络，个人熟悉计算机系统漏洞应用，有多年的网络攻防经验。

【攻 篇】

目 录

第六卷 病毒攻防必杀技

作者简介 do I do，金山毒霸论坛版主，对计算机病毒有独到见解，在金山毒霸在线网站、《电脑报》等发表过多篇计算机病毒文章。

第七卷 木马攻防必杀技

作者简介 飘零雪，某安全杂志在线编辑，曾在多家IT媒体上发表网络安全文章，曾被读者评为最佳文章。
作者简介 劲刀狂舞，研究网络安全多年，对木马、溢出攻击等比较熟悉。现任黑客X元素网站副站长、中华盾网络安全联盟核心成员。

【攻 篇】

【防 篇】

第八卷 黑客软件攻防必杀技

作者简介 剑尘，毕业于计算机网络专业，2000年开始接受朋友委托，担任国内某知名黑客网站的技术总监。

【攻 篇】

附录

作者简介 孙成，某公司网管，对计算机网络有丰富实践经验，潜心研究网络安全知识，为多家知名IT媒体特约作者。

第一卷

密码攻防必杀技

加密与解密就如同矛与盾的关系，两者相互依存、缺一不可。在互联网迅速发展的今天，许多重要的机密文件或软件在传输与发布过程中都会有泄密的危险，如果经过了加密，那么就会让文件多一种保护机制，而且也能够让软件不会轻易地被人盗版。而解密则是逆加密而行，是使用一定手段来破解一些加了密或是被限制了功能的文件或软件。种种原因使得破解与加密在攻与防的斗争中成长，本卷就针对这方面的内容进行讲解。

攻 篇

Office文档密码破解

[问题分析]

为了保证自己的文档不被别人随意查看和修改，在制作Microsoft Office文档的时候，常常要用到Microsoft Office自带的加密功能，为文件加一把“锁”，只有知道密码的人才可以打开文档了解其中的内容。但是有时把文档的密码忘掉了，又不清楚文档里是什么内容，此时就只能破解这个文档的密码，来获得文档中的信息了。

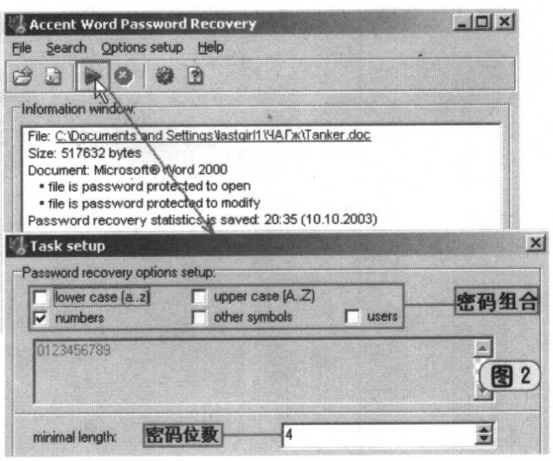
[实际操作]

1.破解Word文档

Word是使用频率很高的文字处理软件，如果遗忘了加密密码可以通过“Accent Word Password Recovery”轻松找回遗忘的Word密码。这是一款体积小但功能强大的MS Word密码恢复工具软件，使用起来相当简单，支持三种口令恢复方法：字典破解、暴力破解以及快速破解。

第一步，运行“Accent Word Password Recovery”，在菜单栏中依次点击“File”→“Open”(快捷键为“Ctrl+O”)，或是在工具栏中单击“Open a Document”(打开一个文档)按钮，找到需要找回密码的加密Word文件后，双击鼠标左键将其加载到破解软件窗口中(图1)。

第二步，在“Information window”信息窗口会显示要破解密码文件的路径、大小、版本以及设置密码的日期。单击工具栏中的“Start a search”按钮，会弹出“Task Setup”设置对话框，在最上方设置密码组合，有小写a~z、大写A~Z、数字等选项。在“minimal length”中设置要破解的密码位数(图2)。



第三步，完成设置后，只要再单击“OK”按钮，就可以开始寻找密码了。找到密码后，会在“information window”窗口中的“file is password protected to open后面显示出正确的密码，就可以使用这个密码来打开该Word文件了(图3)。

注意

在不知道密码的情况下设置密码位数时最好选择1～4。如果破解不成功，可以增大密码的长度范围或者改变密码组合。

2. 破解Excel文档

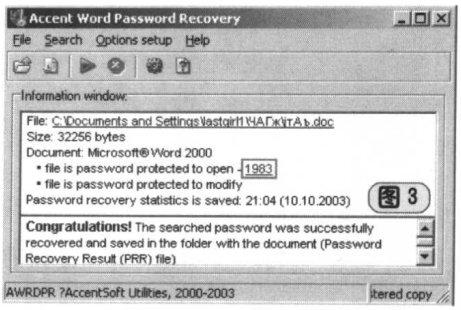


图3

遗失密码会导致无法访问设有密码保护的Excel工作簿。要解开未知密码的加密Excel文档，可以使用Accent Excel Password Recovery。这是一款体积小但功能强大的MS Excel 97/2000/XP密码恢复工具，它能够将Excel 97/2000/XP文档的密码很快找回来，也支持三种密码恢复方法:字典破解、暴力破解以及快速破解。

第一步，安装好软件后，选择开始菜单中的“File” →“Open”，或是在工具栏中单击“Open a Document”(打开一个文档)按钮(图4)。

第二步，找到需要找回密码的Excel文件，然后双击此文件或单击“打开”按钮将文件加载到破解软件中(图5)。

图4

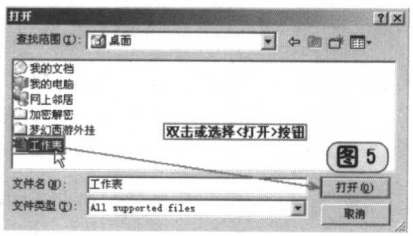


图5

第三步，然后再单击工具栏中的“Start a search”按钮，会弹出“Task Setup”设置对话框，在“Password recovery options setup”中设置好要破解的密码组合，在“minimal length”中设置要破解的密码位数，然后单击“OK”按钮进行破解。最后的破解结果则在“information window”窗口的“file is password protected to open 后面显示出来。

小知识

破解长度大于7位的密码时一般花的时间较多。如果密码很长，不能短时间内破译，可以将进度停止，当计算机空闲时再调入软件目录下保存的文件继续进行破解(图6)。

图6

3. 破解Access文档

破解Access密码的软件很多，其方法也跟Word密码的破解大同小异。可以通过“Accent Access Password Recovery”软件找回遗记的密码。

第一步，运行“Accent Access Password Recovery”，单击“Open a Document”按钮，找到需要找回密码的Access文档，单击“打开”按钮(图7)。

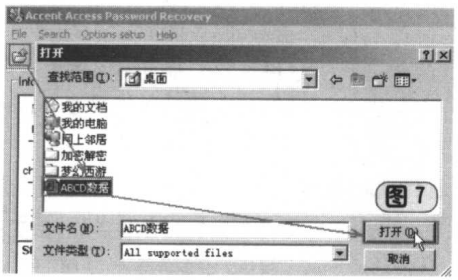


图7

第二步，在工具栏中单击第一个绿色的小箭头“Start a search”，在弹出的“Task Setup”设置对话框中设置密码组合和破解的密码位数，单击“OK”按钮就开始了找回密码的过程。

这个过程的时间长短根据用户设置的密码的复杂程度而定。

第三步，破解完成后，就可以在窗口中看到该Access加密文件的密码了。需要说明的是，该软件是一款共享软件，未注册时只能找回四位密码。

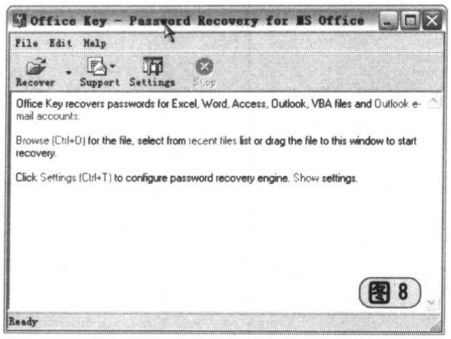


图 8

4. 破解PowerPoint文档密码

要解开未知密码的加密PowerPoint文档，可以使用Passware PassPowerPoint Recovery Kit软件。这是一套密码恢复软件包，能恢复17种软件的密码。如果不需要用到全部17种密码恢复软件，可以只下载所需要的单独软件。

第一步，下载此软件到硬盘，双击kitd.exe进行安装。

第二步，选择开始菜单→“程序”→“Passware”→“Office key”，运行PowerPoint破解软件，其界面如图8所示。

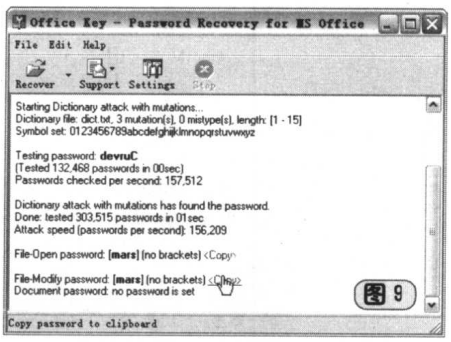


图 9

第三步，将要寻找密码的文件用鼠标拖放到软件窗口中或者单击“Recover”按钮，在弹出的窗口中指定要寻找密码的文件。

第四步，软件将很快找到密码并将密码显示在其窗口中，例如加密的文档密码是“mars”，可以单击密码后面的“copy”将密码复制到剪贴板(图9)。

小知识

PassPowerPoint Recovery Kit软件包中的部分软件可以通过在工具栏中选择“Settings”按钮启动“Brute－force Settings”对话框来设定口令的字符范围、长度范围、样式等选项。通过这些选项的设置能够加快软件寻找密码的速度。

压缩文件的密码破解

[问题分析]

在备份文件的时候，一般都习惯于将自己的文档备份为压缩格式，这样不仅节省硬盘空间，而且还易于管理。而一般情况下，所备份的这些文件都是比较重要的，所以文件加密也就成为一种常用的保护文件的方式。而由于文件长时间没有使用等原因，常常忘记了加密的密码，就只有破解这个密码了。

[实际操作]

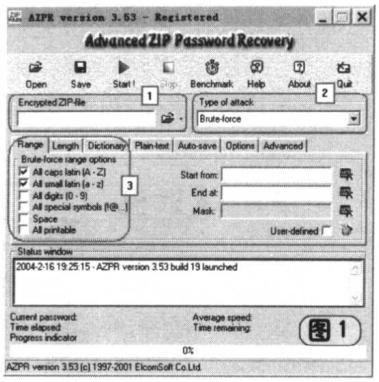
破解加密压缩文件的工具软件建议使用ElcomSoft公司出的AZPR(Advanced ZIP Password Recovery，高级ZIP文件密码破解)和ARPR(Advanced RAR Password Recovery，高级RAR文件密码破解)。下面以AZPR(图1)为例来讲解破解过程。

第一步，在“Encrypted ZIP-file”中选择要破解的加密ZIP文件。

第二步，在“Type of attack”中选择需要采用的破解方式，如果有破解字典，选择“Dictionary”一般选用“Brute-Force(暴力穷举破解)”。

第三步，在“Range”标签页中选择密码所有可能的组成字母，建议首先选择“All caps latin(A-Z)”，不行可以再多选择一个，最后才选择“All printable”，这样可以相对节省一些时间。

设置完毕后，单击“Start!”按钮，经过一段时间之后密码就会显示出来了。



破解屏幕保护的密码

[问题分析]

为了在暂时离开计算机时，保证计算机的安全，人们一般都设置了屏幕保护的密码。这不失为一个好办法。但有时由于屏幕保护密码的设置时间较长，又想不起来密码，而文件还没有保存，不能以重新启动的方式解除屏幕保护，就只能破解这个屏幕保护密码。

[实际操作]

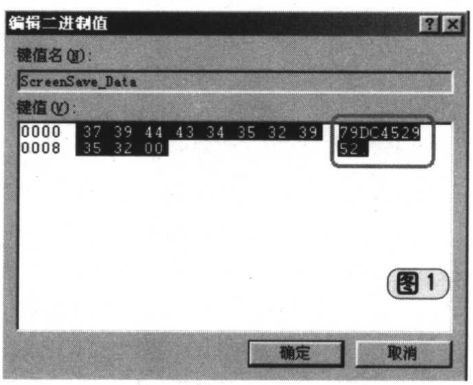
1.简单去除法

在注册表中HKEY_CURRENT_USER\Control Panel\Desktop找到ScreenSaveUsePassword，如果有密码，它的值为“1”，改为“0”就没密码了。

2.从原理入手

一般屏保的密码为8位，再多设也无意义，所以可以从原理入手破译密码。

在注册表的HKEY_CURRENT_USER\Control Panel\desktop中找到ScreenSaveUsePassword，鼠标双击它后出现“编辑二进制”窗口，在下面的键值中看最右边的字符，图1所示密码为两行，视密码具体设置而有所不同。



假设注册表的密码为“12345”，则显示为: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。但这种方法比较复杂，不建议使用。

3.硬件冲突法

如果用户的计算机在局域网内，就可以利用另外一台计算机作为解码机，将解码计算机的IP地址改为用户机的IP地址，利用硬件冲突优先级高的原理跳过屏幕保护。

第一步，在解码机依次单击“开始”→“设置”→“控制面板”，进入“控制面板”后，双击“网络”图标，进入“网络”对话框。

第二步，选择“配置”选项卡，然后双击“TCP/IP”，进入“TCP/IP属性”→“IP地址”选项卡，将解码机的IP地址改为要破解密码的计算机的IP地址，完成后单击“确定”按钮。

第三步，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，当弹出“IP地址产生硬件冲突”的提示框(图2)时，只要在设了屏保密码的计算机屏幕上点击“确定”按钮，就直接进入操作系统的桌面了。

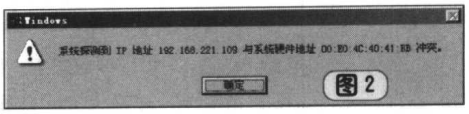


图2

注意

在解密的过程中，确保设有屏幕保护的计算机上还没有出现要求用户输入屏幕保护程序的密码的对话框，否则即使通过设置造成了局域网中的硬件冲突，单击“硬件冲突”对话框中的“确定”按钮后，系统还是会要求输入屏幕保护程序的密码的。

BIOS密码破解

[问题分析]

BIOS密码设置也称为CMOS密码设置。设置密码的作用是防止别人随意修改BIOS设置，以保证计算机的正常运行;限制他人使用计算机，从而最大限度地保护计算机中的数据。一旦设置了密码后，其他人就不能进入BIOS或不能进入计算机进行操作。但是，如今要记的密码实在是太多了，当忘记BIOS密码时的破解就显得尤为重要了。

[实际操作]

1.万能密码法

对于早期的主板，大部分生产厂家都设有万能密码(一般附在主板说明书上)。对于这类主板，无论BIOS密码是如何设置的，用万能密码均可以进入BIOS设置和操作系统。值得注意的是:BIOS种类不同，其万能密码也不同。

(1)对于Award BIOS,可以试试下面的密码:

AWARD_SW、j262、HLT、SER、1EAAh、256256、admin、alfarome、aLLy、aPAf、award、award.sw、award_?、award_ps、AWARD_PW、BIOS、bios*、biosstar、biostar、CONDO、djonet、efmukl、g6PJ、h6BB、HELGA-S、HLT、j09F、j256、j262、j322、j64、PASSWORD、SER、setup、SKY_FOX、SWITCHES_SW、Sxyz、SZYX SKY_FOX、BIOSTAR、ALFAROME、lkwpeter、j256、AWARD?SW、LKWPETER、Syxz、aLLy、589589、589721、awkward、CONCAT(注意大小写)。

(2)对于AMI BIOS,可以试试下面的密码:

AMI、AMI!SW、AMI.KEY、ami.kez、AMI~、ami°、amiami、amidecod、AMIPSWD、amipswd、AMISETUP、bios310、BIOSPASS、CMOSPWD、BIOS、PASSWORD、HEWITTRAND、AMI?SW、AMI_SW、LKWPETER(注意大小写)。

(3)对于Phoenix BIOS,其万能密码为phoenix。

2.用Debug破解法

这种方法适用于可进入操作系统，但进入BIOS设置时需要输入密码的情况。具体方法是:将计算机切换到DOS状态，然后在提示符“C:\>”后面输入以下密码清除指令:

```
debug
-o 70 10
-o 71 ff
-q
```

需要注意的是“o”为字母“o”，而不是数字“0”。