SINOED GROUP

Fadia道德黑客丛书

ANKIT FADIA 著
孟庆华 译

AN Unofficial Guide to Ethical Hacking

良性入侵

——道德黑客非官方指导

UESTCP 电子科技大学出版社

良性入侵

——道德黑客非官方指导

法迪亚　著

孟庆华　译

电子科技大学出版社

图书在版编目（CIP）数据

良性入侵——道德黑客非官方指导 / 法迪亚著；
孟庆华译. —成都：电子科技大学出版社，2007.6
ISBN 978-7-81114-479-6

Ⅰ.良… Ⅱ.①法…②孟 … 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（2007）第 081083 号

良性入侵——道德黑客非官方指导

法迪亚 著
孟庆华 译

出　　版：电子科技大学出版社（成都市一环路东一段 159 号电子信息产业大厦　邮编：610051）
策划编辑：郭　庆
责任编辑：杜亚提
主　　页：www.uestcp.com.cn
电子邮箱：uestcp@uestcp.com.cn
发　　行：新华书店经销
印　　刷：成都理工大学印刷厂
成品尺寸：185mm×260mm　　印张　32.125　　字数　785　千字
版　　次：2007 年 6 月第一版
印　　次：2007 年 6 月第一次印刷
书　　号：ISBN 978-7-81114-479-6
定　　价：80.00 元

Ankit Fadia 生命中的里程碑

10岁——父母在家给他配置了一台个人电脑。

12 岁——表现出对计算机的超常天赋，成为无师自通的少年黑客。

14岁——出版了第一本个人专著——An Unofficial Guide to Ethical Hacking（良性入侵——道德黑客非官方指导），轰动业界，迅即被翻译成11 种语言，在全球15个国家出版发行，并被亚洲和北美的一些著名高校选作教学用书。

16岁——9·11 事件后，成立了法迪亚道德黑客国际研究院，曾为机密情报机构破译了由本·拉登恐怖分子网络发送的加密的电子邮件。自从那时FADIA就介入了与国际安全和计算机网络有关的多个机密工程，负责处理机密情报机构的亚洲行动。

21岁——成为道德黑客的年轻领袖，出版了11 本畅销书，在25 个国家发表了超过1000 次研讨会,获得了45 个奖励。

22岁——致力于数字智能、安全咨询和培训等方面研究，规划并开发出法迪亚道德黑客培训认证体系，并在新加坡管理大学的信息系统学院、美国圣何塞州立大学得到了成功的应用。

2007年——来到中国。

前　言

随着计算机与互联网的迅速普及，人类对计算机的依赖达到了前所未有的程度，计算机的安全直接关系到个人、企业、国家乃至人类社会的生存和发展。而对计算机与互联网构成最严重威胁的，正是防不胜防的网络黑客。纵观当今的互联网业界，病毒木马泛滥、黑客攻击猖獗，各种病毒变体花样百出，恶意攻击手段层出不穷。如何防黑、反黑、制黑，已成为所有互联网用户共同面对的巨大挑战。

上海兴韦教育集团及旗下的上海托普信息技术学院，利用自身的产业背景和专业优势，首度全面引进了国际互联网界资深反恐反黑精英、少年成名的网络安全大师 ANKIT FADIA 的系列专著——“法迪亚道德黑客丛书”。力图从黑客攻防两个角度，将国际最前沿的网络安全技术介绍给国内读者，帮助国内网络用户知黑、防黑、反黑，共同营造和维护健康、安全的互联网世界。

本书是“法迪亚道德黑客丛书”的奠基力作。此书一版再版，已被翻译成 11 种语言，在 15 个国家畅销。此书在国际上第一次明确提出了“道德黑客”的概念，阐明了“道德黑客”的含义，多角度、多层次地展开了道德黑客的全视野。书中从黑客攻击和安全防护两个角度深入剖析了全方位的安全威胁和良性入侵的各种技术手段，系统描述了各种黑客攻击过程，并且给出了相对应的安全防护策略。此书是“道德黑客”的开山之作，已经被美国圣何塞州立大学选作计算机安全方面的专用教材。

本书主要由孟庆华博士主持翻译、统稿、审校。齐金鹏博士参与翻译了第二章、六章、七章、八章、九章、十章，陆星家博士参与翻译了第三章、四章、五章、十四章、十五章，朱莹博士参与翻译了第一、十一、十二、十三章。由于译者水平有限，翻译不妥或错误之处在所难免，敬请广大读者批评指正。

有关全套“法迪亚道德黑客丛书”的出版情况，敬请登录http://www.e-hacker.info.

译　者

兴韦—法迪亚网络与信息安全中心（中国）

上海托普信息技术学院

2007 年 5 月 18 日

目　录

第一章　究竟是谁扮演了黑客的角色

黑客：他们究竟是谁？
住在路那头的14岁小男孩难道会是罪犯？
黑客：由灵感而发的成功事例。

多数人认为黑客是摧残计算机的家伙。但，如果叫一个真正的黑客为罪犯，不出我所料，他一定会大发其火。黑客不是计算机罪犯。为什么大多数人要那样认为呢？这跟媒体的错误导向有关。人们会不假思索地相信报纸和杂志上的内容。媒体把黑客的形象描述成为摧残计算机的家伙，他们潜入服务器、损坏文件系统、制造和散布病毒、破坏网站等无恶不作。

真正的黑客称那些潜入系统的人叫“解密高手”。事实上，编写以及散布病毒的人并不一定是黑客，他们只是编写代码的程序员。

一般来说，黑客是计算机怪人，他们熟谙所有计算机知识，包括硬件的和软件的，而且由于知识宽泛而受到器重。但是近几年，黑客的声誉慢慢下降，如今人们都惧怕他们，他们被看成是社会中的底层人物。

黑客熟谙所有软件及其应用的工作原理，他们具有破解看似不可能解决问题的超凡能力。

他们不按照常规的软件使用说明来使用软件，而是以他们自己所需要的方式使用软件。他们调试代码、不断地进行试错实验来发现未知的和新的花招秘密。他们试着闯入系统并不是堂而皇之地想要破坏什么、或者盗取密码什么的，相反，他们向系统管理员报告漏洞和缺陷。他们尝试突破常规、发现新特征。可以见得，黑客是有关知识的一门学科，他们是信息源广进的高智商人群，他们知道普通人所不知道的事情。

以下三个特征就能判断此人不是真正的黑客：

1．他使用奇怪的头衔，比如 Avenger，Dark Cloud，Skull，Kewl Dude 等，然而这些都是吓唬小孩子的。

2．他总是吹嘘自己懂得很多，其实什么都不会。

3．网络新手问他问题，他总是激动或者发火，但从来却不帮助他们解决问题。

真正的黑客是你能从他那里学到很多东西的人，他们会用智慧和知识为你提供帮助。

但是，我这里要阐明的是，必须要承认黑客（正派的人）和破坏者（不是很正派的人）之间的界线不很明显，而且多数黑客无法抵抗地会逾越这条界线而沦为破坏者。

所谓黑客会一念之差而沦陷为破坏者的原因就是能够一夜成名，但他们却没有意识到这种成名是声名狼藉，引来憎恨而非尊重。相信我，闯入系统并不是好事，会造成一场浩

劫。做这样的傻事可能会让你在秘密黑客阻止里小有名气，但这种尊敬是暂时的。如今，黑客的数量与日俱增，人们很快就会忘记你曾经的辉煌。

而且，一般人不会认为你做的事情有多么的伟大。他们并不相信摧毁网站、进行拒绝服务攻击、散布病毒的人有多么的值得尊重。上述这些再加上媒体的大肆宣传，人们更愿给黑客冠上计算机罪犯的名头。

破坏者只在秘密组织中小有名气。而一名道德黑客，在整个社会部分中备受景仰。相信我，在正常人群中出名的黑客也会被破坏者所羡慕和尊重。

而且，破坏者被系统管理员和警察所厌恶和唾弃。告诉系统管理员其系统的缺陷问题，他毫无疑问地将会崇拜你。在对你表示感谢之后，他很可能会给予你进入其系统的特权。哇!!! 这是不是所有黑客做梦也想要得到的事情？

另外，法律已经开始审判计算机犯罪，将其看作为一种严重的侵权。计算机犯罪的普通惩罚有进监狱、大额罚款，甚至终身禁止使用计算机。而且，计算机罪犯不容易获得保释。

这里我们不讨论法律问题。让我给各位举一个生动的例子，让你能明晰地判别破坏者和黑客之间的区别。

美国曾经有位 13 岁的黑客，他和他的黑客朋友经常沉浸于写代码和调试。他们常常互相闯入各自的系统来证明他们的成就。他们不仅聪颖过人，而且拥有敏锐的商业头脑。

这些把戏也能使他们跨过底线沦为破坏者去干傻事而毁坏大好前程。但所幸的是，他们并没有那样做，这同时也给我们带来了福音。今天，我们知道他们就叫 Bill Gates 和 Paul Allen。他们两个是世人皆知的亿万富翁践行者。

如果他们逾越了那条底线，那么他们就会在监狱里度过下半辈子。人们会称其为计算机罪犯，系统管理员更想要了他们的命。不过，他们很精明，如今坐上了世人羡慕的巨富的宝座。

我并没有建议大家不要做黑客。我真诚地支持黑客事业，希望更多的人成为黑客，闯入系统，做正确的事情。不要做伤害别人的事情。真正的黑客知道黑客道德的首要就是从不删除任何文件、不破坏你已经闯入的系统。利用好你的知识不干违法的事，提高公司的服务质量，协助软件产业的发展，推动经济欣欣向荣。如果你做到了以上的每一件事情，那么我敢保证，你必定会成名，前方一座金灿灿的金山正在等着你呢！

第二章 Windows 攻击

- ▲ 密码破解
- ▲ Window 欺诈
- ▲ 清除 Web 站点浏览记录
- ▲ 编辑操作系统
- ▲ Window 注册破解
- ▲ Cokies

BIOS 密码破解

本章节将使你学会如何进行 Windows 攻击，以及如何利用 Windows 进行攻击。一旦完成本章的学习，你能够对 Windows 操作系统更为精通，并从所有黑客中脱颖而出。

BIOS 密码是你计算机中最为基本的设置，比如，系统的磁盘驱动器类型和数量，并对重新启动等选项进行设置。这些选项主要通过主板上的 CMOS 芯片进行设置。一块微型电池提供该芯片正常运行的电能，因此，即使你的计算机处于关闭状态，该芯片仍然记录着系统的设置信息。

进入 BIOS 设置通常的方法是在启动的过程中按“Del”键。另外的方法有，比如同时按“Crtl+Alt+Esc”键，或者只按“Crt+Esc”键。大多数计算机都可以通过 CMOS 设置开机密码。如果设置该密码，那么在开启计算机时，就需要在开机前键入正确的密码。如果不能正确输入，那么就不能正常进入系统。由于进入 BIOS 需要知道 BIOS 密码，所以不能对该密码进行重新设置或者使之失效。那么如何对 BIOS 设置进行破解而不被追踪呢？为了使 BIOS 密码失效，你需要进入 BIOS。但是，一旦你进入 BIOS，BIOS 就需要进行密码验证。破解该密码的最通用的办法就是使 BIOS 恢复默认的设置。一些通常的密码如下：

lkwpeter	AMI	cmos
j262	Award	,AMI!SW1
AWARD_SW	bios	AMI?SW1
AWARD_PW	BIOS	password
Biostar	setup	hewittrand

BIOS 密码破解的更多部分请参考密码破解章节。

“j262”对于大多数的 Award BIOS 版本开放，并在 80%情况下是可用的。“AWARD_SW”以及“AWARD_PW”也应用在目前的一些计算机上，但不是经常被用到。在一些 BIOS 中，键组合“shift+syxz”也是可用的。寻找各个版本 BIOS 默认密码的最好办

法就是访问以下网址：http//astalavista.box.sk ，该网址是寻找安全相关内容的最好搜索引擎。在那里会找到各种 BIOS，以及每个 BIOS 的各种版本。因此，可以到特定的 BIOS 公司的网站去寻找该 BIOS 的默认密码。目前应用最广泛的 BIOS 公司的网址主要有 award.com, megatrends.com, 以及 mrbios.com.

BIOS 的公司名称和版本信息在每次系统启动时都会出现在显示屏上。

如果默认的密码失效，那就要用到更为有效的攻击方法。为了能恢复 BIOS 的默认设置，使每次进入系统都不需要密码验证，需要进行以下操作：

首先要打开计算机，然后找到一个圆形的锂电池，看上去像一个银币。移除该电池，30 秒钟后再将其重新安装回原位置。一些计算机可能需要重新设置条线，寻找有 3 个管脚的条线，并使其复原。比如在最普通的计算机上可以找到一个带有第一个与第二个针相连的 3 个管脚设备。如果使第二个与第三根针连接，并停留超过 5 秒钟，就将重新设置 CMOS。

BIOS 也能用来对你的计算机进行超频。更多 CPU 超频的内容请访问以下网址：http://www.overcloking.com.

当重新启动计算机时，一些 BIOS 会给出“BIOS 被重新设置或被修改”的出错信息，该信息并不是系统攻击的大障碍。

注意！ 搞乱 CMOS 芯片与条线远比编辑系统文件更具危害性，因此，每步操作都要格外小心。

多数计算机都可以通过一组按键破解密码程序。

为此，先重启计算机，等待密码输入框，然后再持续按 Esc 键 50 到 100 次。这将破解密码程序，并使计算机继续启动。然而，该方法仅局限于一些特定的计算机。

还有另外一种更容易破解 BIOS 密码的方法。KillCMOS 程序就可以解决该问题，该软件可以从www.koasp.com下载，或者可在 astalavista.box.sk 上搜索到。另外，还有很多其他的 CMOS 密码破解软件可以从各种黑客网站下载。

Windows 登录密码破解

当破解了 BIOS 密码后，Windows 系统紧接着就会要求你登录密码。对于黑客而言，破解该密码要比破解 CMOS 的密码更为容易。你将发现黑客认为 Windows 系统是跛脚的，并会一直嘲笑微软的安全漏洞问题。

为破解 Windows 登录密码，需要重新启动并等待一下信息：

“Starting Windows 9x”

当你看到该屏幕时，按 F8 键。将会出现启动菜单。选择第 7 项，进入 DOS 启动。然后直接键入：

C:\> cd windows

与启动过程相关的键有 F4，F5，F6，F8，Shift+F5，Control+F5，以及 Shift+F8。尽力尝试每个组合，看会有哪些情况发生。然后，通过键入下列命令将所有文件的扩展名改为.pwl：

C:\windows> ren *.pwl* .xyz

或者用下面命令删除它们。

C:\windows> del *.pwl* .xyz

当 Windows 密码登录窗口出现时，现在输入任意的符号就可以通过密码验证。由于前面已经对密码文件重新命名（或删除，但重新命名并不会使受害计算机察觉系统已受到攻击，因此要比删除更好些）。由于 Windows 找不到该密码文件，因此当键入密码时就会使用默认的最原始的密码值。

以下方法可使 F8 或重新启动键失效。具体过程如下所示：

1．对系统文件进行操作十分危险。恢复磁盘上或者启动磁盘上的系统文件就属于该情况之一，因此，在出现错误的时候就需要修复 msdos.sys 文件。

2．可以在 C:\msdos.sys 目录下找到该 msdos.sys 文件。由于属于隐藏文件，需要通过键入下列命令更改其文件属性，使该文件可写：

C：\Windows>cd\

然后通过键入下列命令，使 msdos.sys 文件可写，并处于非隐藏状态：

C：\attrib msdos.sys –h –w

3．在 WordPad 中打开 msdos.sys 文件。

4．打开的文件显示如下：

```
;FORMAT
[Paths]
WinDir=C:\WINDOWS
WinBootDir= C:\WINDOWS
HostWinBootDrv=C
[Options]
BootMenu=0 (default)
BootMulti=1
BootGUI=1
Double Buffer=1
AutoScan=1
Win Ver=4.10.1998
;
；需要保留下面的空白行，以保持与其他程序的一致性。
；请不要移除（==）、
```

为能使在重新启动过程中的功能键失效，需要直接插入下列代码：

“BootKeys=0”（没有过程调用）

现在，也可以插入下列命令取代上面的代码行。

“BootDelay=0”

许多人不了解 BootDelay=0 命令。该命令与 BootKey 命令确实能使你的系统更加安全。然后存储 msdos.sys。

5．由于 msdos.sys 是重要的系统文件之一，需要恢复其只读和隐藏的文件属性。

C：> attrib msdos.sys +h +r

实际上，如果运行的 Windows 95 或 Windows 98 系统没有联入局域网中，你则不必执行以上步骤。你只需要在 Windows 登录对话框出现时点击取消按钮即可。总之，技术高明的黑客需要了解所有的攻击方法。通过安装在 Windows 系统中的破解软件 pwledit 也可以取消 Windows 密码。你可以通过路径“开始→程序→附件→系统工具”找到该软件。若没有找到，可以从 Windows 95 安装盘中安装该软件。该软件在 d:\admin\apptools\pwledit 目录中。你可以搜索 Windows 98 系统安装 CD 盘找到该软件。

想有一张启动盘吗？想知道如何创建吗？制作过程很简单。插入一张空软盘到软盘驱动器中，并进入控制面板。点击添加/删除程序，然后点击“制作启动盘”标签，随后点击“创建磁盘”按钮。

详细资料请参考.pwl 文件破解的网站：

http:\\www.hackingmobilephones.com

更改 Windows 界面

你已经知道如何闯入一台本地运行 Windows 的计算机，下面我们将学习一些有用的 Windows 诀窍，以加深印象。如果你计算机处于正常的运行状态，则在每次启动时出现一个蓝屏的“欢迎使用 Windows 95”干扰界面。你想将其换成一个头骨与鲜血的恐怖画面吗？该部分内容将一步一步教你如何更换启动屏幕以及令人厌烦的关机屏幕。

为更换 Win98 系统中的启动屏幕，需要找到 C：\logo.sys 文件。由于该文件为系统文件，其文件属性可能为隐藏的，因此不能直接在 Windows 浏览器中直接打开。为了能破除其属性限制，可先进入 MSDOS 并通过以下命令阅读所有的.sys 系统文件：

C：\> Attrib *.sys

屏幕上将出现以下的信息：

SHR C：\MSDOS.sys

SHR C：\IO.sys

A SHR C：\CONFIG.sys

A SHR C：\logo.sys

在 C：\根目录下已经存在了 logo.sys 文件。现在 SHR 表示该 logo.sys 是一个系统文件，其文件属性为隐藏并只读。

一些计算机中可能没有该 C: \logo.sys 文件。多数情况下，建议你通过以下的 MSDOS

命令从 Windows 目录下直接复制该文件。

C:\>cd windows

C:\>cd windows> copy logow.sys c:

正如前所述，现在的 logo.sys 文件为只读文件，并不能被编辑。为使其可写，可通过下面命令改变其属性：

步骤 1. 进入 MSDOS

步骤 2. 键入下列命令：

C:\>Windows>cd\

C:\>attrib logo.sys –s –h –r

目前，还有破解 Windows 密码的另一种方法。直接按 F5 而不是 F8 可使系统直接进入安全模式。当 Windows 系统以安全模式启动，并不需要登录密码，因此你可在安全模式下工作。这也是绕过密码验证的另一种方法。有些情况下 F8，F5 等键失效时就可以利用手头的启动盘。在 BIOS 密码破解以后，就可进入 BIOS（多数计算机可在启动时通过按 Del 键进入 BIOS 设置）并设置从 A: 盘启动。插入启动盘后等待出现 DOS 命令对话框，然后就可键入相应命令破解密码。

该步骤可使 logo.sys 文件具有可写性。通过下面步骤就可以更换你想要的 Windows 欢迎屏。

步骤 1. 打开 MSPaint

步骤 2. 从文件菜单中选择“打开”

步骤 3. 打开 c:\logo.sys

步骤 4. 打开闪动的启动屏后，你就可以通过带体该文件，制作自己喜欢的欢迎屏。

见图 2-1。

图 2-1　Windows 登录界面

然后将其保存为 c:\logo.sys. 通过键入下面的 MSDOS 命令恢复该文件的原始属性。

C:\>attrib logo.sys +h +r +s

现在，重新启动你的系统就会看到你更换后的启动欢迎屏。通过类似操作，你也可以

更换系统关闭屏。进入命令对话框通过如上的命令设置 logow.sys 文件可写，并在画图中打开，编辑并保存到 c:\windows\logow.sys. 随后（通过使用 C:\>attrib logo.sys –s –h –r 命令）恢复该文件的正常属性。现在你系统的关闭屏也已经被修改成功了。

清除历史记录

当输入特定 Web 站点的 URL 时会有什么情况发生呢？浏览器与你刚键入的 Web 站点建立链接，访问并下载你所访问页面的所有图像和文本，并保存在本地硬盘缓存上。因此，当有人登录到你计算机时就会发现你所访问过的网站。假如你在公司工作的同时想要找份更好的工作，你在网上寻找新的工作机会，并访问了许多的工作搜索站点。如果你的上司追踪公司的 Internet 账户，就会从硬盘缓存中发现你寻找新工作所访问过的上网记录。无疑地，你的上司肯定对你会有意见。因此，如何从硬盘中清除所有我们访问过站点的记录呢？Netscape Navigator 和 Microsoft Internet 浏览器都存储了你最近访问过网页的 URL 记录和其他程序所使用过的所有图像文件，以备将来使用。

删除 Internet 浏览器记录

为了删除所有 Internet 浏览器的所有记录：

1．在 Internet 浏览器窗口点击 View（是否为“工具”）菜单项；

2．从菜单底部选择“Internet 选项”；

3．在历史窗体中点击“清除历史记录”。

通过以上步骤将清除 Internet 浏览器上所有的历史记录。但有些时候还需要通过以下步骤删除所选定的条目：

1．打开 Internet 浏览器；

2．从 Internet 浏览器上点击“历史”按钮；

3．靠近窗口左侧会出现一个新的历史记录窗体；

4．在选定的条目上单击右键，从快捷菜单上选择“删除”，或者单击左键再从键盘上选择“Del”键即可删除。

每台上网的计算机都会分配一个 IP 地址，如果你想与特定的计算机建立链接，就要首先知道其 IP 地址。但由于 IP 地址很长，不利于记忆。如何解决该问题呢？主机名可以解决该问题，主机名就是用人类语言对 IP 地址进行命名。如果你想访问 hotmail.com 网站，不必记住其 IP 地址，你仅需记住 hotmail.com。当你键入主机名时，浏览器就会与 DNS 服务器或者域名服务器联系。这些服务器上存储着主机名称及其对应的 IP 地址。更多内容请参考网络工具章节。

如图 2-2，图 2-3 所示。

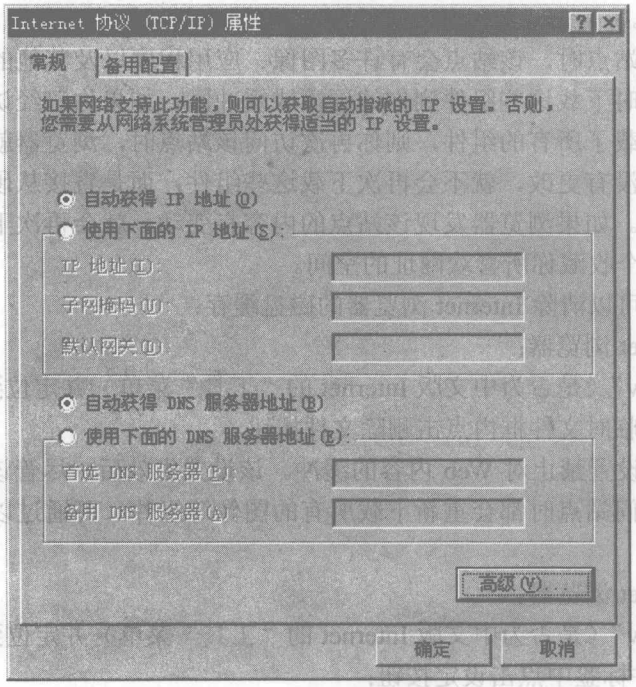

图 2-2　IP 地址设置界面

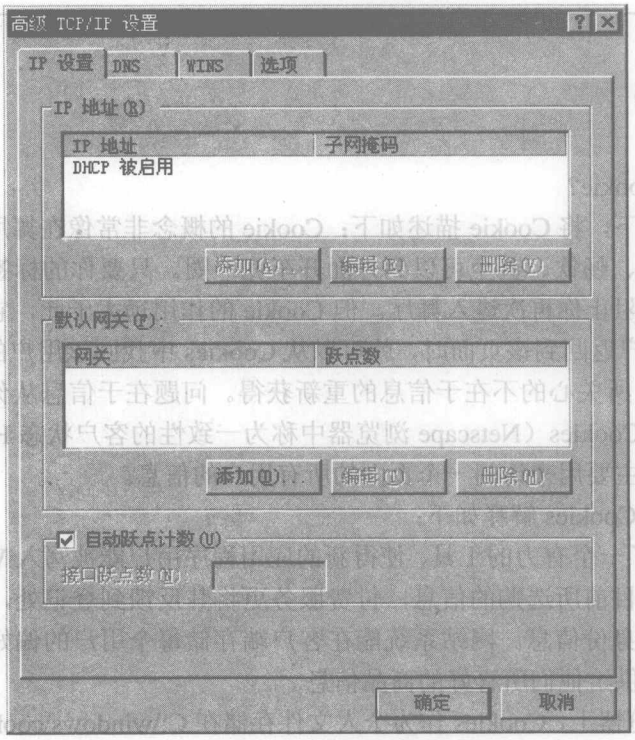

图 2-3　IP 地址设置界面

通过以上操作就可以删除特定站点的所有缓存的页面，该站点的所有记录就将从你的计算机上完全删除。

当你访问一个站点时，该站点会有许多图像、应用程序以及其他的多媒体组件同时运行。浏览器就会同时下载这些组件到你的硬盘或缓冲区。如果你已经访问过该站点，一旦你的浏览器已经下载了所有的组件，则你再次访问该站点时，浏览器就会检查该站点的内容是否更改。如果没有更改，就不会再次下载这些组件，而是直接从硬盘中装载站点的副本，因而节省时间。如果浏览器发现该站点的内容有变动，就会再次下载更新的副本。明显地，缓存是另一个收藏你所喜欢网址的空间。

通过下面步骤可以清除 Internet 浏览器的磁盘缓存：

1．打开 Internet 浏览器；

2．点击“View”（是否为中文版 Internet 的“工具”菜单）并定位到 Internet 选项；

3．在 Internet 临时文件框内点击删除文件按钮。

你也可以通过设置禁止对 Web 内容的缓冲。该设置生效后，尽管该站点的内容没任何变化，你在每次访问站点时都会重新下载所有的图像等组件。可通过以下步骤实现对缓存的禁止作用：

1．打开 Internet 浏览器；

2．点击“View”（是否为中文版 Internet 的“工具”菜单）并定位到 Internet 选项；

3．在程序文件标签中点击设定按钮；

4．拖动指针，将磁盘空间总量设置为 0MB。

删除 Cookies

究竟什么是 Cookie?

最高安全级别下，将 Cookie 描述如下：Cookie 的概念非常像在舞厅中将你的手打上了标签。你可以漫步、畅饮、甚至可以到外面开车兜一圈。只要你的标签在手上，你就不必再次付费，也不会阻止你再次进入舞厅。但 Cookie 的作用远大于此，它记录用户的特定信息，因此，当该用户返回到该页面时，就可以从 Cookies 中找回该用户的相关信息（作为状态信息）。Cookies 所关心的不在于信息的重新获得。问题在于信息从你的硬盘驱动器的哪个位置找回信息。Cookies（Netscape 浏览器中称为一致性的客户状态 HTTP Cookies）是一个存储选项，目前主要用来访问一个页面的所有用户的信息。

Netscape 中将 Cookies 解释如下：

Cookies 提供了一个有力的工具，使得新的应用程序用户能被写入 Web 环境中。购物应用程序能存储客户目前所选购的信息，付费服务更将其反馈到登记处，客户在下次登录时不必再次输入用户身份信息。网站系统能在客户端存储每个用户的偏好信息，并在下次登录系统时向客户提供给他们所喜好的商品信息。

在 Internet 浏览器上，Cookies 作为个人文件存储在 C:\windows\cookies 目录下。也可定位到 C:\windows\cookies 目录下直接删除 Cookie 信息。