



东方飘云倾情演示
黑客攻防经典案例



防黑档案

——黑客新招曝光 (第二版)

郭 鑫(东方飘云)

编著

飞思科技产品研发中心

监制



电子工业出版社

PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
<http://www.phei.com.cn>

黑客基本功

谁动了我的QQ

说出你的秘密

E-mail安全吗

警惕Web攻击

增强你的病毒免疫力

操作系统的漏洞隐患

神秘的特洛伊

黑客工具防不胜防

热门黑客技术曝光——数据库注入



东方飘云倾情演示
黑客攻防经典案例

飞思科技产品研发中心总策划

飞思在线: <http://www.fecit.com.cn>



策划编辑: 何郑燕

王蒙

责任编辑: 武嘉

责任美编: 王嵩

ISBN 7-121-01125-5



9 787121 011252 >

本书贴有激光防伪标志, 凡没有防伪标志者, 属盗版图书。

ISBN 7-121-01125-5 定价: 29.00 元 (含光盘1张)



防黑档案

——黑客新招曝光 (第二版)

郭 鑫(东方飘云)

编 著

飞思科技产品研发中心

监 制

电子工业出版社

Publishing House of Electronics Industry

北京·BEIJING

内 容 简 介

本书为畅销书《防黑档案》的升级版,由业内知名黑客“东方飘云”编写,对第一版的内容进行了全面的调整和完善,删掉了部分过时的内容,增加了近期最新出现的网络漏洞及攻防技术。本书最大程度地沿袭了第一版优秀的畅销书特质,以精辟的语言深入浅出地讲解了在日常的网络生活中广大网友经常会遇到的一些安全性问题,包括即时通信工具、Mail、Web、病毒、系统安全、后门木马、黑客工具、数据库注入等攻防技术,以及当前的热点加密解密技术。本书旨在让读者快速形成正确的网络安全观念,并掌握维护与防范的技巧,能够从容应对来自网络的形形色色的威胁,从而更大程度地享受网络带给我们的巨大乐趣。附书光盘内容为网络攻防视频演示文件。

本书既可作为从事网络安全工作人员的参考资料,也可作为网络爱好者充实自己的学习和辅导用书。

未经许可,不得以任何方式复制或抄袭本书之部分或全部内容。
版权所有,侵权必究。

图书在版编目(CIP)数据

防黑档案——黑客新招曝光 / 郭鑫(东方飘云)编著. —2版. —北京:电子工业出版社, 2005.5
(网络安全专家)

ISBN 7-121-01125-5

I.防... II.郭... 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(2005)第033969号

责任编辑:武 嘉

印 刷:北京智力达印刷有限公司

出版发行:电子工业出版社

北京海淀区万寿路173信箱 邮编:100036

经 销:各地新华书店

开 本:787×1092 1/16 印张:18 字数:460.8千字

印 次:2005年5月第1次印刷

印 数:7000册 定价:29.00元(含光盘1张)

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

作者介绍

姓名：郭鑫

网名：东方飘云

年龄：不详

全国十大黑客之一

资深网络安全顾问

业绩：

创办中国安全在线<http://www.safen.org>，并担任站长。

现任瑞泰讯杰信息技术有限公司
网络安全顾问。

曾参与主持多个国家级项目的安全评估。

序

随着信息化进程的深入和因特网的迅速发展,人们的工作、学习和生活方式正在发生巨大变化,效率大为提高,信息资源得到最大程度的共享。但必须看到,紧随信息化发展而来的网络安全问题日渐突出,如果不能很好地解决这个问题,必将阻碍信息化发展的进程。

在各领域的计算机犯罪和网络侵权方面,无论是数量、手段,还是性质、规模,都已经到了令人咋舌的地步。据有关方面统计,目前美国每年由于网络安全问题而遭受的经济损失超过170亿美元,德国、英国也均在数十亿美元以上,法国为100亿法郎,日本、新加坡的问题也很严重。在国际刑法界列举的现代社会新型犯罪排行榜上,计算机犯罪已名列榜首。2003年,CSI/FBI调查所接触的524个组织中,有56%遇到电脑安全事件,其中38%遇到1~5起,16%以上遇到11起以上。因与因特网连接而成为频繁攻击点的组织连续3年不断增加;遭受拒绝服务攻击则从2000年的27%上升到2003年的42%。调查显示,521个接受调查的组织中96%有网站,其中30%提供电子商务服务,这些网站在2003年1年中有20%发现未经许可入侵或误用网站现象。更令人不安的是,有33%的组织说他们不知道自己的网站是否受到损害。据统计,全球平均每20秒就发生1次网上入侵事件,黑客一旦找到系统的薄弱环节,所有用户均会遭殃。

计算机系统遭受病毒感染和破坏的情况相当严重。据国家计算机病毒应急处理中心副主任张健介绍,从国家计算机病毒应急处理中心日常监测结果看来,计算机病毒呈现出异常活跃的态势。据2001年调查,我国约73%的计算机用户曾感染病毒,2003年上半年升至83%。其中,感染3次以上的用户高达59%,而且病毒的破坏性较大,被病毒破坏全部数据的占14%,破坏部分数据的占57%。

电脑黑客活动已形成重要威胁。网络信息系统具有致命的脆弱性、易受攻击性和开放性,从国内情况来看,目前我国95%与因特网相连的网络管理中心都遭受过境内外黑客的攻击或侵入,其中银行、金融和证券机构是黑客攻击的重点。

信息基础设施面临网络安全的挑战。面对信息安全的严峻形势,我国的网络安全系统在预测、反应、防范和恢复能力方面存在许多薄弱环节。据英国《简氏战略报告》和其他网络组织对各国信息防护能力的评估,我国被列入防护能力最低的国家之一,不仅大大低于美国、俄罗斯和以色列等信息安全强国,而且排在印度、韩国之后。近年来,国内与网络有关的各类违法行为以每年30%的速度递增。

网络环境的复杂性、多变性,以及信息系统的脆弱性,决定了网络安全威胁的客观存在。我国日益开放并融入世界,但加强安全监管和建立保护屏障不可或缺。本书将从因特网安全的各个方面逐一讲解,希望能给广大读者耳目一新的感觉!

感谢父母、黄丽等所有在写书过程中给予我支持和帮助的人,感谢你们!

郭鑫(东方飘云)

飞思人理念

我们经常感谢生活的慷慨，让我们这些原本并不同源的人得以同本，为了同一个梦想走到一起。

因为身处科技教育前沿，我们深感任重道远；因为伴随知识更新节奏，我们一刻不敢停歇。虽然我们年轻，但我们拥有：

“严谨、高效、协作”的团队精神

全方位、立体化的服务意识

实力雄厚的作者群和开发队伍

当然，最重要的是我们拥有：

恒久不变的理想和永不枯竭的激情和灵感

正因如此，我们敢于宣称：

飞思科技=丰富的内容+完美的形式

这也是我们共同精心培育的品牌  的承诺。

“问渠哪得清如许，为有源头活水来”。路再远，终需用脚去量；风景再美，终需自然抚育。

年轻的飞思人愿为清风细雨、阳光晨露，滋润您发芽、成长；更甘当坚实的铺路石，为您铺就成功之路。

我们的联系方式如下：

咨询电话：(010) 68134545 68131648

电子邮件：support@fecit.com.cn

服务网址：http://www.fecit.com.cn http://www.fecit.net

通用网址：计算机图书、飞思、飞思教育、飞思科技、FECIT

飞思科技产品研发中心

目 录

第 1 章 黑客基本功	1
1.1 认识 IP 地址	2
1.1.1 什么是 IP 地址	2
1.1.2 IP 地址划分方法	2
1.1.3 如何查询 IP 地址	3
1.2 黑客入手之门	4
1.3 TCP/IP	5
1.3.1 TCP/IP 组件的 4 个层次及功能	5
1.3.2 TCP/IP 的分层	8
1.4 黑客常用指令	10
1.4.1 ping	10
1.4.2 ipconfig	13
1.4.3 tracert	14
1.4.4 netstat	15
1.4.5 net	18
1.4.6 at	20
1.4.7 telnet	20
1.4.8 ftp	20
1.4.9 copy	21
1.4.10 set	21
1.4.11 echo	22
1.4.12 attrib	23
1.4.13 net start	23
1.5 了解网络专有名词	24
1.6 黑客入侵流程	26
第 2 章 谁动了我的 QQ	29
2.1 认识 QQ 黑客软件	30
2.1.1 侦听工具	30
2.1.2 窃听工具	31
2.1.3 炸弹工具	31
2.2 轻松找到你的踪迹	32
2.2.1 IPLocate	32
2.2.2 QQ 查 IP 补丁	33
2.3 小心有人偷窥你的聊天记录	33
2.4 完全可以把 IP 隐藏起来	34
2.5 谁也偷不走我的 QQ	36

2.5.1	盗 QQ 木马介绍	36
2.5.2	QQ 新防偷术	38
2.6	防范 QQ 的黑客程序	38
第 3 章	说出你的秘密	41
3.1	Office 文档破解	42
3.1.1	利用工具破解 Office 文档	42
3.1.2	防范方法	43
3.2	WinRAR 压缩包破解	43
3.2.1	如何破解 WinRAR 压缩包	44
3.2.2	防范方法	45
3.3	Windows 98 共享破解	45
3.3.1	通过注册表查看共享密码	46
3.3.2	防范方法	48
3.4	Windows 2000 清空密码进入系统	48
3.4.1	删除 SAM 文件进入系统	48
3.4.2	防范方法	49
3.5	CMOS 密码破解	49
3.5.1	通用密码破解法	49
3.5.2	DEBUG 和工具破解法	50
3.5.3	万能放电法	51
3.6	屏幕保护密码破解	51
3.7	对系统密码进行深度加密	54
3.8	巧用 PGP 工具加密文件	55
3.8.1	什么是 PGP	55
3.8.2	使用方法	56
第 4 章	E-mail 安全吗	59
4.1	不需密码, 轻易查看邮件	60
4.2	无需破解, 轻松捕捉邮件密码	64
4.2.1	利用 IRIS 捕捉邮件密码	64
4.2.2	防范方法	65
4.3	破解邮箱密码	65
4.3.1	利用工具破解邮件密码	65
4.3.2	防范方法	66
4.4	邮件炸弹攻击	66
4.4.1	用邮件炸弹堵满目标的邮箱	67
4.4.2	防范方法	68
4.5	群发邮件攻击	68
4.5.1	利用群发邮件宣传产品	68
4.5.2	防范方法	75

4.6	查出匿名邮件的背后黑手	75
4.6.1	概述	75
4.6.2	邮件头分析	75
4.6.3	邮件传输过程	76
4.6.4	邮件头分析实例	78
4.6.5	邮件伪造	79
4.6.6	匿名邮件分析	79
4.6.7	总结	82
4.7	防范垃圾邮件	83
4.7.1	利用邮件网关进行垃圾邮件的防范	83
4.7.2	自定义策略, 防范垃圾邮件	93
第 5 章	警惕 Web 攻击	95
5.1	加密、解密网页	96
5.1.1	最简单的加密解密	96
5.1.2	转义字符“\”的妙用	97
5.1.3	使用 Microsoft 出品的 Script Encoder 来进行编码	98
5.1.4	任意添加 NULL 空字符	100
5.1.5	无用内容混乱及换行空格 Tab 方法	100
5.1.6	自写解密函数法	101
5.1.7	错误的利用	102
5.2	破解网页密码	102
5.3	利用脚本使硬盘共享	104
5.3.1	硬盘共享脚本分析	104
5.3.2	防范方法	105
5.4	利用脚本进行网页欺骗	106
5.4.1	跨站脚本介绍及其利用	107
5.4.2	防范方法	108
5.5	恶意修改注册表网页	108
5.5.1	恶意修改注册表介绍	108
5.5.2	如何防范、杜绝恶意修改	110
5.6	浏览器炸弹	111
5.6.1	无限窗口炸弹	111
5.6.2	浏览器锁死炸弹	112
5.6.3	浏览器炸弹的防御方法	114
5.7	防范网页黑手策略	116
5.7.1	网页黑手	116
5.7.2	防范策略	117
第 6 章	增强你的病毒免疫力	119
6.1	计算机病毒的分类	120

6.1.1	按照计算机病毒攻击的系统分类	120
6.1.2	按照计算机病毒的攻击机型分类	120
6.1.3	按照计算机病毒的链接分类	121
6.1.4	按照计算机病毒的破坏情况分类	121
6.1.5	按照计算机病毒的寄生部位或传染对象分类	122
6.1.6	按照计算机病毒的传播媒介分类	122
6.2	计算机病毒传播途径	123
6.3	病毒技术	123
6.3.1	Internet 病毒技术	123
6.3.2	破坏性感染病毒技术	124
6.3.3	隐藏性病毒技术	124
6.3.4	多态性病毒技术	125
6.3.5	病毒自动生产技术	125
6.4	预防病毒的方法	126
6.4.1	计算机病毒的预防措施	126
6.4.2	计算机病毒的预防技术	129
6.5	病毒的诊断原理	130
6.5.1	计算机病毒比较法诊断原理	130
6.5.2	计算机病毒校验和诊断原理	131
6.5.3	计算机病毒扫描法诊断原理	132
6.5.4	计算机病毒行为监测法诊断原理	132
6.6	病毒的消除方法	133
6.7	病毒消除原理	134
6.7.1	引导型病毒的消毒原理	134
6.7.2	文件型病毒的消毒原理	134
第 7 章	操作系统的漏洞隐患	135
7.1	IPC\$默认共享漏洞的应用	136
7.1.1	概述	136
7.1.2	入侵方法及过程	136
7.2	Unicode 与二次解码漏洞的应用	141
7.2.1	漏洞描述	141
7.2.2	漏洞应用	142
7.2.3	防范策略	145
7.3	IDQ 溢出漏洞应用	145
7.3.1	漏洞描述	145
7.3.2	漏洞应用	145
7.3.3	防范策略	147
7.4	WebDAV 溢出漏洞应用	147
7.4.1	漏洞描述	147

7.4.2	漏洞应用	148
7.4.3	防范策略	149
7.5	SQL 空密码漏洞应用	150
7.5.1	漏洞描述	150
7.5.2	漏洞应用	150
7.5.3	防范策略	153
7.6	DDoS 拒绝服务攻击	154
7.6.1	什么是 DDoS	154
7.6.2	DDoS 检测	155
7.6.3	DDoS 攻击工具	155
7.6.4	DDoS 攻击防范策略	157
7.7	清除攻击后的痕迹	157
7.7.1	攻击后会留下哪些痕迹	157
7.7.2	彻底清除痕迹	159
7.8	加固你的服务器, 拒绝黑客入内	163
7.8.1	IIS 安全配置	163
7.8.2	FTP 安全配置	172
7.8.3	各种日志审核配置	176
7.8.4	SMTP 服务器安全性设置	179
7.8.5	定制自己的 Windows 2000 Server	184
7.8.6	正确安装 Windows 2000 Server	185
7.8.7	安全配置 Windows 2000 Server	185
7.8.8	需要注意的一些事情	188
第 8 章	神秘的特洛伊	189
8.1	什么是特洛伊木马	190
8.1.1	特洛伊木马名称的由来	190
8.1.2	特洛伊木马的组成	190
8.2	特洛伊木马的特性	190
8.2.1	木马的隐蔽性	190
8.2.2	木马的自动运行性	191
8.2.3	木马的自动恢复性	191
8.2.4	木马的主动性	191
8.2.5	木马的特殊性	191
8.3	特洛伊木马的种类	192
8.3.1	破坏型	192
8.3.2	密码发送型	192
8.3.3	远程访问型	192
8.3.4	键盘记录型	193
8.3.5	拒绝服务攻击型	193

8.3.6	代理型	193
8.3.7	FTP 型	193
8.3.8	程序杀手型	193
8.3.9	反弹端口型	194
8.4	木马的启动方式	194
8.5	木马的隐藏方式	195
8.5.1	在任务栏里隐藏	196
8.5.2	在任务管理器里隐藏	196
8.5.3	在端口中隐藏	196
8.5.4	在通信中隐藏	196
8.5.5	在加载文件中隐藏	196
8.5.6	最新隐藏方式	197
8.6	木马的伪装方式	197
8.6.1	木马的伪装方式分类	197
8.6.2	被感染后的紧急措施	198
8.7	揭开木马神秘的面纱	198
8.7.1	基础篇	199
8.7.2	攻防技巧篇	201
8.7.3	DLL 木马篇	201
8.8	透视木马开发技术	202
8.8.1	木马的隐藏技术	203
8.8.2	程序的自加载运行技术	204
8.9	防范木马的策略与方法	206
8.9.1	用 DOS 命令检查特洛伊木马	206
8.9.2	手工清除电脑里的特洛伊木马	208
8.10	找出控制木马的黑客	209
8.10.1	反弹端口木马的原理	209
8.10.2	使用监听工具查木马	209
第 9 章	黑客工具防不胜防	211
9.1	扫描工具——寻找攻击目标	212
9.1.1	ShadowSecurityScanner	212
9.1.2	SuperScan	225
9.2	破解工具——进入攻击目标	228
9.2.1	溯雪	228
9.2.2	L0phtcrack	233
9.3	攻击工具	235
9.3.1	srv.exe	235
9.3.2	IDQ 溢出工具	235
9.3.3	NC.exe	236

9.3.4	webdav.exe	238
9.3.5	SqlExec.exe	238
9.3.6	UDP Flooder.....	239
9.4	监听工具——扩大攻击成果	239
9.4.1	Iris.....	239
9.4.2	Xsniff.....	244
9.5	后门木马工具——留出后门方便下次进入	246
9.5.1	冰河	246
9.5.2	网络神偷	249
第 10 章	热门黑客技术曝光——数据库注入.....	253
10.1	什么是数据库注入 (SQL injection)	254
10.1.1	数据库注入技术 (SQL injection) 的发展史	254
10.1.2	什么是数据库注入 (SQL injection)	254
10.2	初识数据库注入技术	254
10.2.1	数据库注入介绍	254
10.2.2	数据库注入技术基础介绍	255
10.3	数据库注入应用之收费电影网站	264
10.4	利用数据库注入技术进入某黑客网站后台	266
10.5	如何防范数据库注入	268
10.5.1	如何防范 ASP 数据库注入	268
10.5.2	如何防范 PHP 数据库注入	270

```
:78054201 FF15DC720578
:78054207 85FF
:78054209 751B
:7805420B 8D45FC
:7805420E 8D8D78FFFFFFF
:78054214 50
:78054215 51
```

```
Call dword ptr [780572DC]
test edi, edi
jne 78054226
lea eax, dword ptr [ebp-04]
lea ecx, dword ptr [ebp+FFFFFF78]
push eax
```

CHAPTER 1

黑客基本功

```
:7805421F B801000000
:78054224 EB79
```

* Reference

```
:78054209
```

```
:78054226
```

```
:7805422C
```

```
:78054232
```

```
:78054233
```

* Reference

```
:78054234
```

```
:7805423A
```

```
:7805423B
```

```
:78054241
```

```
:78054242
```

```
:78054247
```

```
:78054248
```

```
:7805424E
```

* Reference

```
:7805424F
```

```
:78054255
```

```
:78054258
```

```
:7805425A
```

```
:7805425C
```

* Reference

```
:7805421D
```

```
:7805425F 33FF
```

```
:78054261 B801000000
```

```
:78054266 397DFC
```

```
:78054269 7534
```

```
xor edi, edi
mov eax, 00000001
cmp dword ptr [ebp-04], edi
jne 7805429F
```

随着因特网的逐渐普及，安全技术越来越受到大家的青睐。但学习提高都是有一个从低到高的过程，在这一章里，我们首先一起来熟悉一些因特网的基本常识，以及一些常用的网络命令，为以后的学习提高打下坚实的基础！

1.1 认识 IP 地址

具体的介绍如下。

1.1.1 什么是 IP 地址

在网络中，我们经常会遇到 IP 地址这个概念，这也是网络中的一个重要概念。所谓 IP 地址就是给每个连接在 Internet 上的主机分配一个在全世界范围内惟一的 32 位地址。IP 地址的结构使我们可以在 Internet 上很方便地寻址。IP 地址通常用更直观的、以圆点分隔的 4 个十进制数字表示，每一个数字对应于 8 个二进制数字的比特串，如图 1-1 所示。

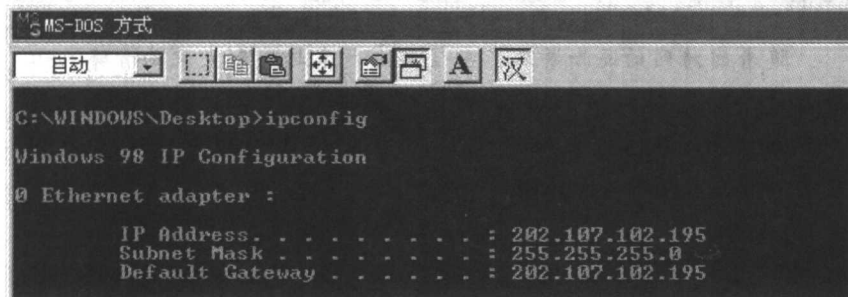


图 1-1 IP 地址

Internet IP 地址由 InterNIC (Internet 网络信息中心) 统一负责全球地址的规划和管理，同时由 InterNIC、APNIC、RIPE 三大网络信息中心具体负责美国及其他地区的 IP 地址分配。通常每个国家需成立一个组织，统一向有关国际组织申请 IP 地址，然后再分配给用户。

1.1.2 IP 地址划分方法

IP 地址可以被划分成不同的类，根据最左边 4 个地址位的值决定具体的网络类型。例如，所有的 A 类网络地址最左边一位的值均为 0，而剩余 31 位的值既可以取 0 也可以取 1。即：

0xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx

(x 代表 0 或 1，下同)

根据 A 类网络地址的规定，我们可以推算出该类型网络的有效地址范围是从 0.0.0.0 到 127.255.255.255。

B 类网络地址从左向右第一位必须为 1，第二位必须为 0，其他 30 位则可以自由取值。即：

10xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx

因此，B 类型网络地址的有效取值范围是从 128.0.0.0 到 191.255.255.255。同样地，除第一位必须为 1 之外，C、D 和 E 类网络地址的第二、三和四位都应当分别为 1。我们在表

1-1 中对不同网络类型 IP 地址的划分进行了总结。

表 1-1 IP 地址的划分

网 络 类 型	特征地址位	起 始 地 址	结 束 地 址
A	0XXX	0XXX	127.255.255.255
B	10XX	128.0.0.0	191.255.255.255
C	110X	192.0.0.0	223.255.255.255
D	1110	224.0.0.0	239.255.255.255
E	1111	240.0.0.0	255.255.255.255

1.1.3 如何查询 IP 地址

经常有人问到如何查询 IP 地址，在这里我给大家介绍两种方法。

第一种就是通过网页来查询 IP 地址的所在地。这样的网页在网上有很多，比如 <http://ip.loveroot.com/index.php>，这里就可以通过 IP 来查询所在地。我们这里用 202.97.175.61 来举例，进入该网页后，在“IP 地址”一栏里输入想查找的 IP，然后单击【查询】按钮，就会显示出该 IP 对应的地址了，如图 1-2 所示。

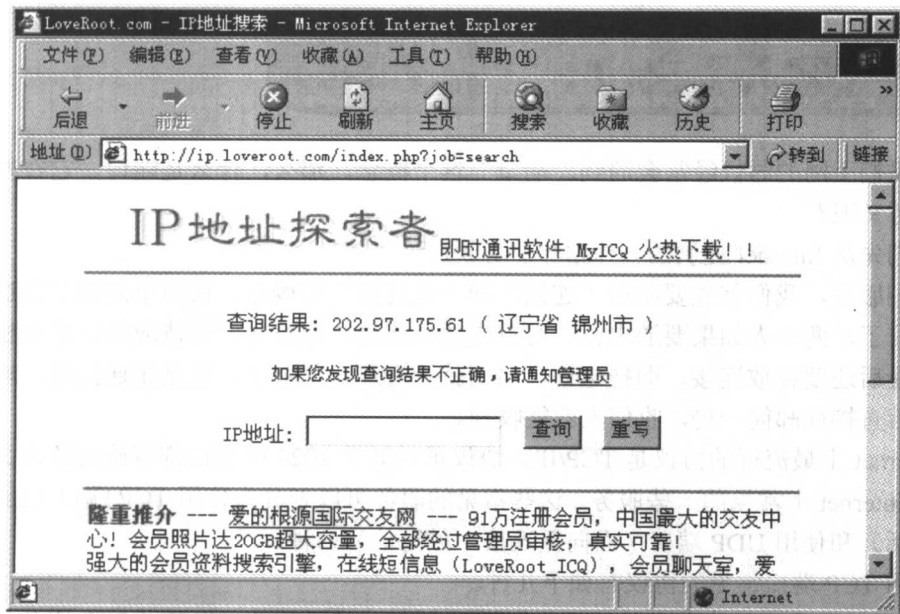


图 1-2 查 IP 地址网页

第二种就是利用专用的查 IP 软件。这里我们介绍国内最著名的查 IP 软件“追捕”。打开软件，在输入框里输入待查的 IP 地址 202.97.175.61，然后单击【追捕！】按钮，目标 IP 的数据就会显示在软件界面中，如图 1-3 所示。

查看 IP 地址的方法还有很多，希望大家在熟悉上面两种方法的基础上，再去接触更多的方法。