网络安全专家

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

電子工業出版社
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

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。

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 定价：29.00 元（含光盘1张）

网络安全专家

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

電子工業出版社

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。

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 zlts@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。
现任瑞索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

```
:78054201 FF15DC720578          Call dword ptr [780572DC]
:78054207 85FF                  test edi, edi
:78054209 751B                  jne 78054226
:7805420B 8D45FC                lea eax, dword ptr [ebp-04]
:7805420E 8D8D78FFFFFF          lea ecx, dword ptr [ebp+FFFFFF78]
:78054214 50                    push eax
:78054215 51
```

CHAPTER 1

黑客基本功

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！

```
:7805421F B801000000
:78054224 EB79

* Reference
|:78054209(
|
:78054226 8
:7805422C 8
:78054232 5
:78054233 5

* Reference
`
:78054234 F
:7805423A 5
:7805423B 8
:78054241 5
:78054242 F
:78054247 5
:78054248 8
:7805424E 5

* Reference

:7805424F F
:78054255 8
:78054258 1
:7805425A F
:7805425C 8

* Reference(s) by a (U)nconditional or (C)onditional Jump at Address:
|:7805421D(C)
|
:7805425F 33FF                  xor edi, edi
:78054261 B801000000            mov eax, 00000001
:78054266 397DFC                cmp dword ptr [ebp-04], edi
:78054269 7534
```

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。

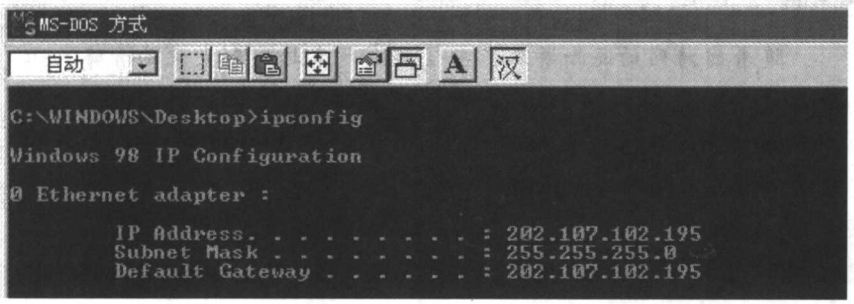

图1-1 IP地址

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：

0xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx

（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：

10xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx

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。

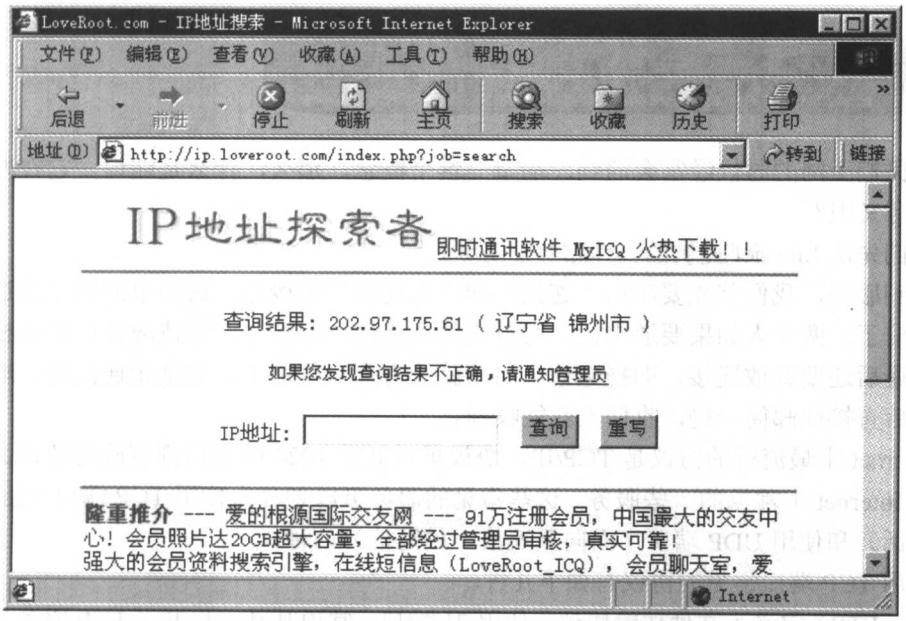

图 1-2　查 IP 地址网页

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。