

GOTOP

黑客密技 全报导



狗仔队系列

狗仔队长



■不谈高深理论，只问能否不被“黑”到。

■让你享受防“黑”的快乐，不体验学习知识的痛苦。

■实际体验各种黑客工具的使用方法。

■实际操作工具，快速建立成就感。

■从防“黑”中认识黑客工具的原理，体验无痛苦学习法。

中国铁道出版社
CHINA RAILWAY PUBLISHING HOUSE

黑客密技 全报导



狗仔队系列

狗仔队长



中国铁道出版社

2004·北京

(京)新登字063号

北京市版权局著作权合同登记号: 01-2003-6747号

版 权 声 明

本书中文繁体字版由台湾碁峯资讯股份有限公司出版。中文简体字版经台湾碁峯资讯股份有限公司授权由中国铁道出版社出版。任何单位或个人未经出版者书面允许,不得以任何手段复制或抄袭本书内容。

图书在版编目(CIP)数据

黑客密技全报导 / 狗仔队长编著. —北京: 中国铁道出版社, 2003. 11

(狗仔队系列)

ISBN 7-113-05644-X

I. 黑... II. 狗... III. 计算机网络—安全技术—基本知识 IV. TP393.08

中国版本图书馆CIP数据核字(2003)第109332号

书 名: 黑客密技全报导

作 者: 狗仔队长

出版发行: 中国铁道出版社(100054, 北京市宣武区右安门西街8号)

策划编辑: 严晓舟 郭毅鹏

责任编辑: 苏 茜 张丽群

封面设计: 孙天昭

印 刷: 北京市彩桥印刷厂

开 本: 880 × 1230 1/32 印张: 9.75 字数: 282千

版 本: 2004年1月第1版 2004年1月第1次印刷

印 数: 1~5000册

书 号: ISBN 7-113-05644-X/TP·1084

定 价: 14.00 元

版权所有 侵权必究

凡购买铁道版的图书, 如有缺页、倒页、脱页者, 请与本社计算机图书批销部调换。

编辑企划序



网络虚拟社会所遇上的困扰，并不亚于现实世界，试问网络族最担心的问题是什么，第一个当然是人见人怕的“病毒”，其次就是神龙见首不见尾的“黑客”。

网络日益普及，便利快速之余却隐藏了潜在的危机。你知道每天上网时，有多少黑客正在浏览你计算机里的重要数据吗？可是无论再怎样危险，总不能因噎废食吧？若要真正防“黑”，当然必须先知道黑客究竟如何入侵你的计算机。所以本书先介绍黑客必备的工具，让读者先具备基础的防黑能力。

- **黑客必备工具：**奠定黑客基础观念与技能，不得不学……
- **黑客防黑客：**黑上瘾之前请特别小心，注意对方是否也拥本书自重……

培养了基本能力之后，把椅子摆正、把嘴巴合拢，准备进入黑客的神秘领域。

- **木马攻击：**木马攻击无声无息，准备一场屠城大战……
- **远程攻击：**黑人于无形之间，让对方怎么被黑的都不知道。
- **密码破解：**密码谁知道？其实大家都一清二楚……
- **QQ攻击：**一边聊天一边窃取数据，或者送给对方一颗大炸弹……
- **网页攻击：**喜欢成天挂在网络上闲逛？小心危机就在你身边……
- **NT系统攻击：**NT系统滴水不漏？嘿嘿，有胆子就试试看吧……

前阵子掀起一股黑客热潮，各大书局的榜首热门书都是黑客类，这是黑客的神秘感加上新鲜感所致。黑客话题虽然已经逐渐降温，但是真正的黑客与黑客工具，仍然在不断地翻新求变。本书可以说是2004年最新版的黑客工具书，将再度引领读者进入黑客的黑暗世界，体验黑客之道热闹的嘉年华会！

本书由碁峰资讯股份有限公司提供版权，经中国铁道出版社计算机图书中心审选，李林果、武莹、罗心晶、闫卫星等同志完成了本书的整稿工作。

中国铁道出版社

2003年12月

A35214/06

INSIDE STORY · TOP SECRET

目 录



CHAPTER 1. 黑客必备指令 1

1-1 知道自己的IP	2
1-2 测试计算机是否在线—ping	4
1-3 检视网络路由节点—Tracert	8
1-4 查询网络状态与共享资源—Net	10
1-5 网络连接监视—Netstat	12
1-6 获知对方计算机信息—Nbtstat	14

CHAPTER 2. 黑客必备工具 17

2-1 Port扫描工具	18
2-2 使用NetView扫描共享资源	20
2-3 共享扫描工具	23
2-4 字典文件制作工具I—Txt2Dic	26
2-5 字典文件制作工具II—Create Dictionary	29
2-6 字典文件制作工具III—Superdic	32

CHAPTER 3. 黑客防黑客 41

3-1 安全漏洞检测	42
3-2 木马扫描仪	46
3-3 邮件炸弹防制工具 I	48

3-4 邮件炸弹防制工具 II	52
3-5 一次设置多个邮件炸弹防制帐号	57
3-6 入侵检测工具	62
3-7 拆解网页炸弹	65
3-8 防火墙工具	68

CHAPTER 4. 黑客密码破解 75

4-1 破解星号密码I	76
4-2 破解星号密码II	78
4-3 破解共享文件夹的密码	80
4-4 破解RAR压缩文件密码	83
4-5 破解压缩文件密码	86
4-6 破解BIOS的密码	91
4-7 破解屏幕保护程序密码	92
4-8 破解简易网页密码	96

CHAPTER 5. 黑客入侵应用实录 99

5-1 破解POP3邮件信箱密码	100
5-2 破解网站密码	106
5-3 DNS查询	110
5-4 破解新闻服务器	112
5-5 攻击服务器	115
5-6 破解FTP密码	118

CHAPTER 6. 炸弹攻击实录 123

6-1 IP炸弹	124
6-2 网页炸弹	126
6-3 邮件炸弹 I	128
6-4 邮件炸弹 II	132
6-5 匿名信件寄炸弹 I	135
6-6 匿名信件寄炸弹 II	138
6-7 硬盘炸弹	140
6-8 ICQ炸弹	142
6-9 按不完的消息窗口	146
6-10 从NT漏洞自由进出	152

CHAPTER 7. 黑客伪装术 157

7-1 隐藏自己的上网IP	158
7-2 伪装病毒或木马做成小游戏 I	160
7-3 伪装病毒或木马做成小游戏 II	164
7-4 伪装病毒或木马变成新的图标	168
7-5 伪装病毒或木马做成图片文件	174
7-6 一次伪装多个病毒或木马图标I	178
7-7 一次伪装多个病毒或木马图标 II	182

CHAPTER 8. 黑客木马攻击实录 189

8-1 共享全开加上登录门户大开	190
8-2 系统完全操控	192

8-3 经典木马 I	196
8-4 经典木马II	204
8-5 经典木马III	214
8-6 让对方共享全开	220

CHAPTER 9. 狗仔队抓黑实录 223

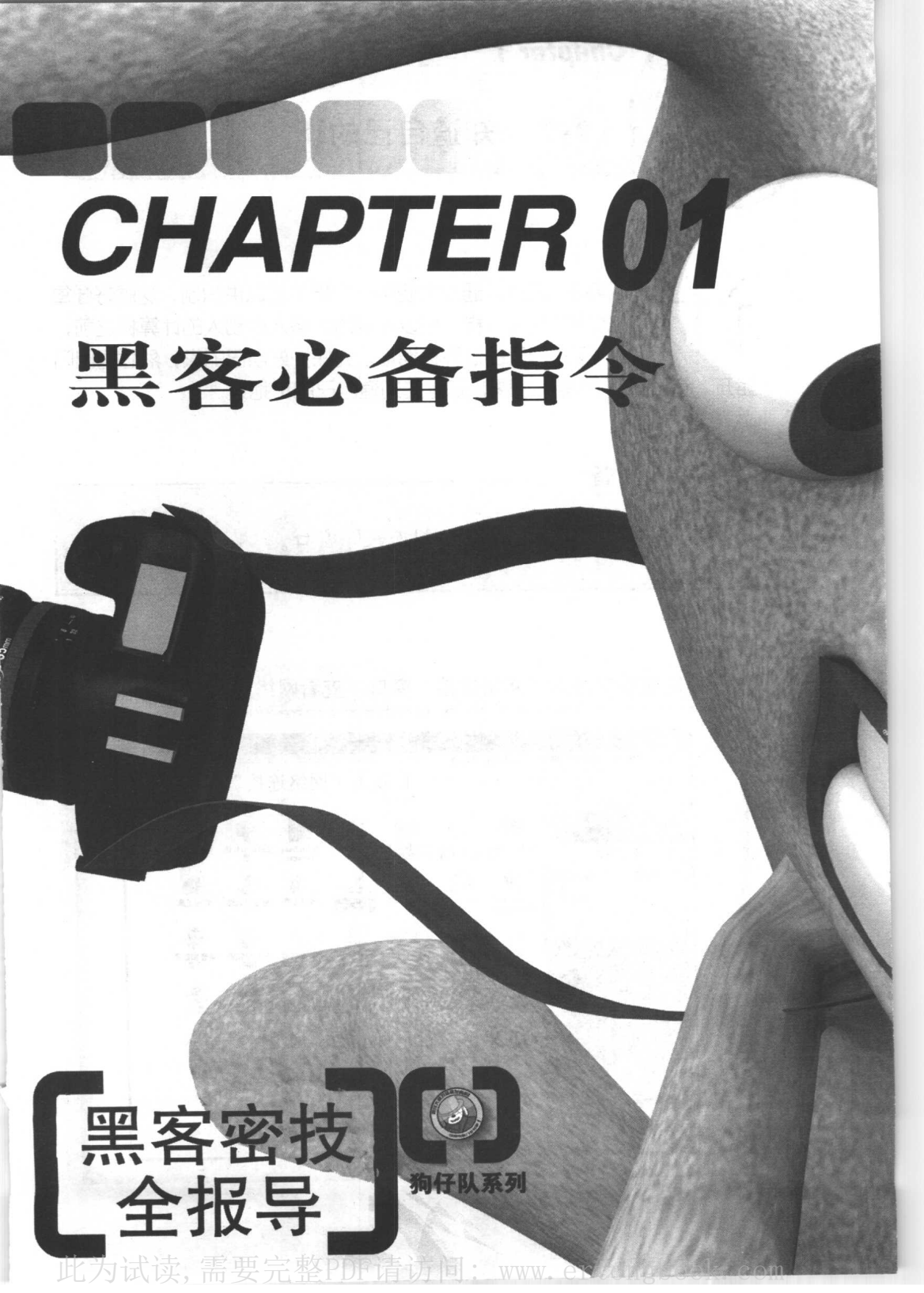
9-1 取得他人信箱密码	224
9-2 计算机记录完全监控	230
9-3 键盘操作完全记录	240
9-4 邮件完全监控	243
9-5 计算机操控完全录制	246

CHAPTER 10. QQ攻击实录 251

10-1 盗取QQ密码	252
10-2 查看好友的IP	274
10-3 消息炸弹攻击—飘叶千夫指	276

CHAPTER 11. 网页/邮件攻击实录 279

11-1 格式化危险文件	280
11-2 格式化电子邮件	286
11-3 杀光硬盘内的文件	290
11-4 绑架鼠标右键	294
11-5 首页绑架事件	297
11-6 掩人耳目的文本文件	302



CHAPTER 01

黑客必备指令

黑客密技
全报导



狗仔队系列

此为试读, 需要完整PDF请访问: www.erongbook.com



1-1 知道自己的IP

计算机连接上网时，通常会使用一个IP地址以供识别，这就好像每个人家里的住址一样。所以在成为黑客入侵别人的计算机之前，需要先了解自己的计算机地址，先保护好自己的家，然后再出门游玩，因此入门的第一步骤，就是先知道自己的IP地址。

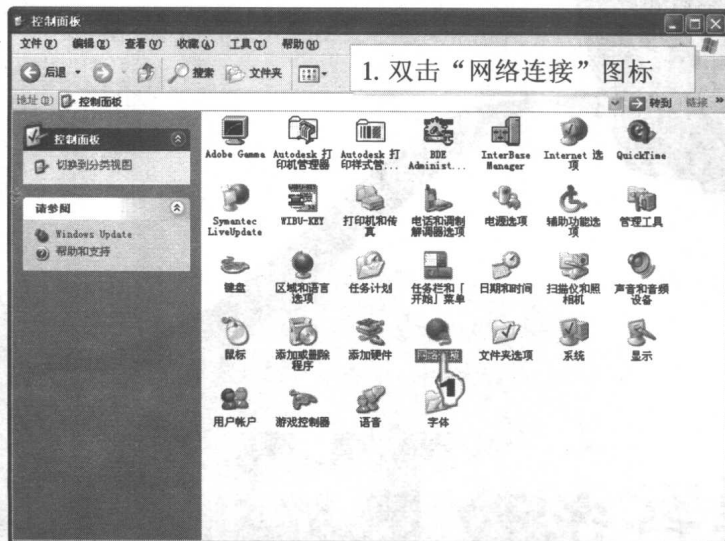
学 前 准 备

》从“开始”菜单打开“控制面板”窗口。

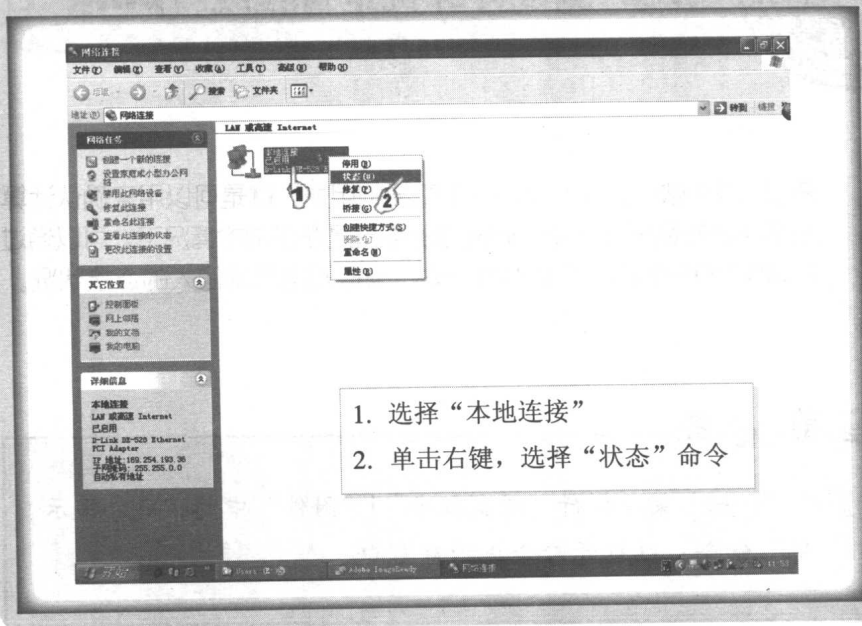
Step

1

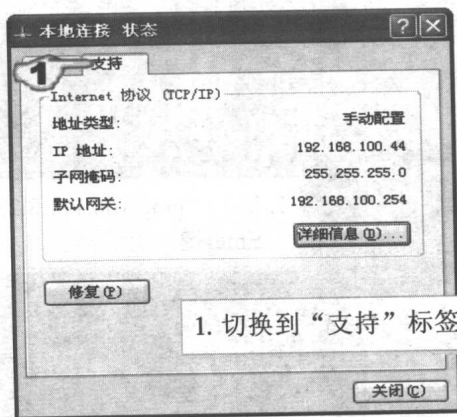
从控制面板中进入“网络连接”窗口，查看网络选项。



从“网络连接”设定窗口中，查看连接状态。



从状态窗口中，可以得知自己计算机的IP地址是什么。





1-2 测试计算机是否在线—ping

P可以用来做什么呢？其中一个重要的用途，就是可以用来确认计算机是不是在网络上活动。假设你的连接是在正常的情况下，可以通过在MS-DOS模式中使用Ping指令，来得知自己或他人的连接状况。

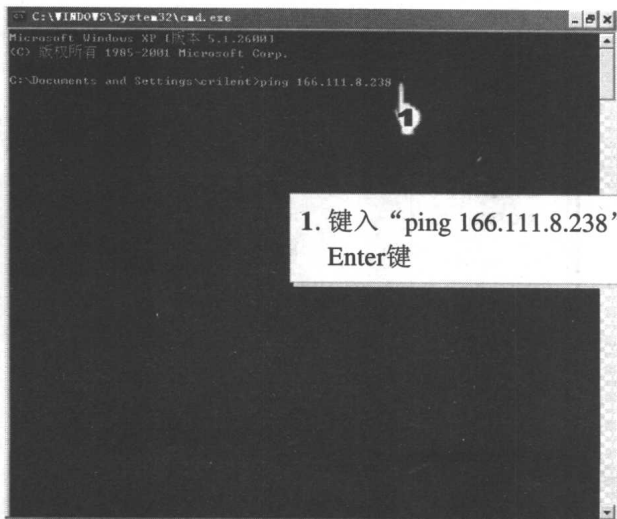
学 前 准 备

》从“开始”菜单执行“所有程序”|“附件”中的“命令提示符”命令，以打开命令提示符窗口。

Step

1

在“命令提示符”窗口中，使用Ping指令来查看自己或他人的连接状态。



1. 键入“ping 166.111.8.238”后，按下Enter键

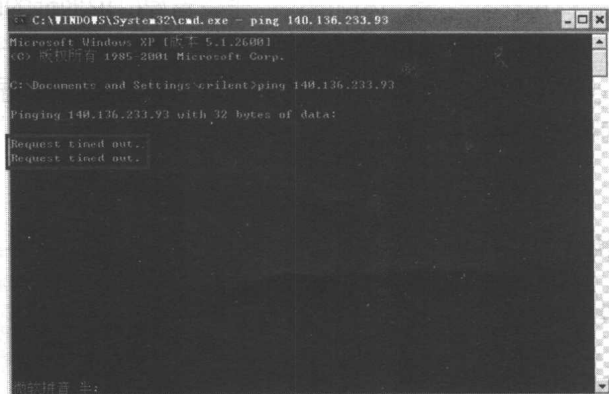
补充说明

除了-t参数之外，Ping还有很多参数可以使用，主要有以下项目：

-a	将目标的主机名称转换为IP地址
-t	若用户不强行中断，将会不断地ping下去
-c count	要求ping指令连续送出数据封包，直到发出并接收到count个请求
-f	是一种快速ping的方式，使ping输出数据包的速度和数据包从远程计算机返回的速度一样快，或者更快，达到每秒100次
-d seconds	在两次数据包送出之间，间隔一定的秒数，并且不能与-f一起使用
-p	保护可以通过这个选项标识的16 pad字节，并将这些字节加入数据包中。当在网络中诊断到与数据有关的错误时，这个选项就非常有用
-q	使ping只在开始和结束时显示一些概要信息
-n	只使用数字方式。在一般情况下ping会试图把IP地址转换成计算机名称，不过这个参数会要求ping显示IP地址，而不去搜索以符号表示的名称
-R	把ICMP RECORD-ROUTE 选项加入到ECHO_REQUEST数据包中，并要求在数据包中记录路由，这样当数据返回时，ping就可以将路由信息列出来。每个数据包最多只能记录9个路由节点，所以许多计算机会忽略或者放弃使用这个参数
-r	使ping指令显示数据包的正常路由表

补充说明

若显示结果为Time out，则可能是检测的对象计算机并没有连上网络。



```
C:\WINDOWS\System32\cmd.exe - ping 140.136.233.93
Microsoft Windows XP [版本 5.1.2600]
(C) 版权所有 1985-2004 Microsoft Corp.

C:\Documents and Settings\erilent>ping 140.136.233.93

Pinging 140.136.233.93 with 32 bytes of data:

Request timed out.
Request timed out.

C:\Documents and Settings\erilent>
```