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”的快感，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

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

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……

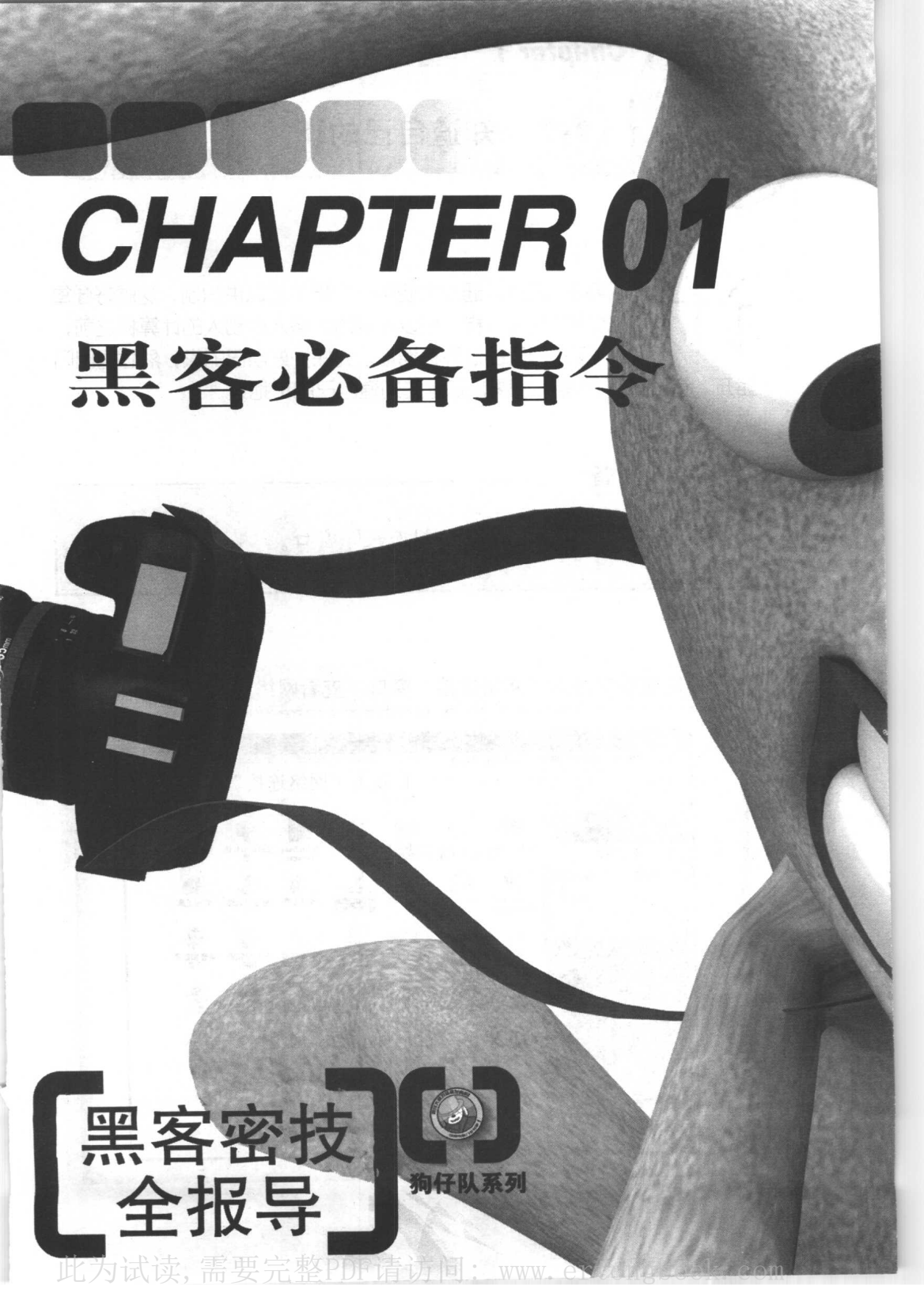
前阵子掀起一股黑客热潮，各大书局的榜首热门书都是黑客类，这是黑客的神秘感加上新鲜感所致。黑客话题虽然已经逐渐降温，但是真正的黑客与黑客工具，仍然在不断地翻新求变。本书可以说是2004年最新版的黑客工具书，将再度引领读者进入黑客的黑暗世界，体验黑客之道热闹的嘉年华会！

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

目 录



CHAPTER 01

黑客必备指令

黑客密技全报导

狗仔队系列

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

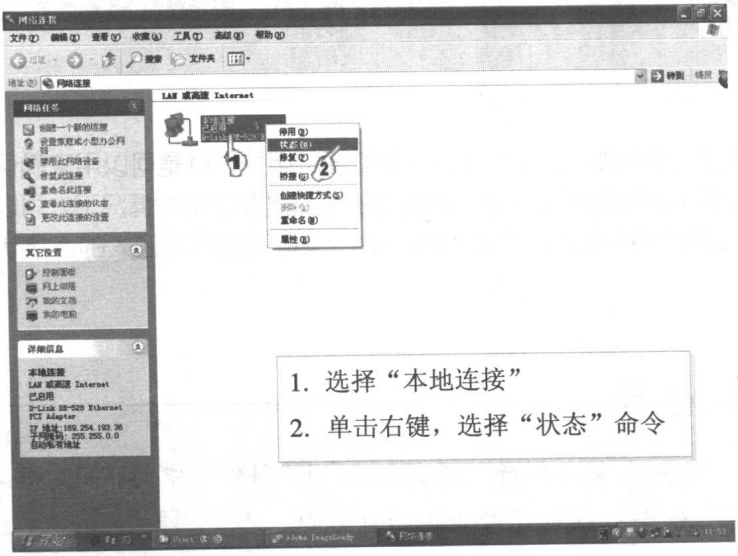
》从“开始”菜单打开“控制面板”窗口。

Step 1

从控制面板中进入“网络连接”窗口，查看网络选项。

Step 2

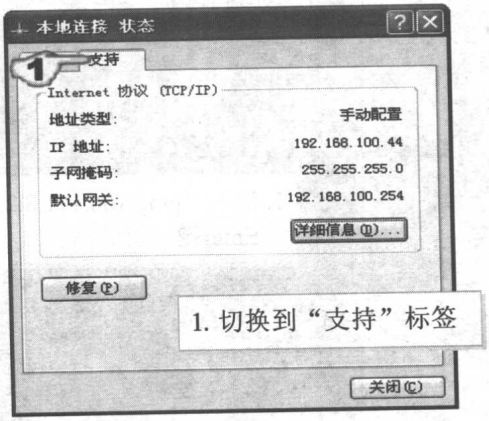
从“网络连接”设定窗口中，查看连接状态。



1. 选择“本地连接”
2. 单击右键，选择“状态”命令

Step 3

从状态窗口中，可以得知自己计算机的IP地址是什么。



1. 切换到“支持”标签

1-2 测试计算机是否在线—ping

INSIDE STORY · TOP SECRET

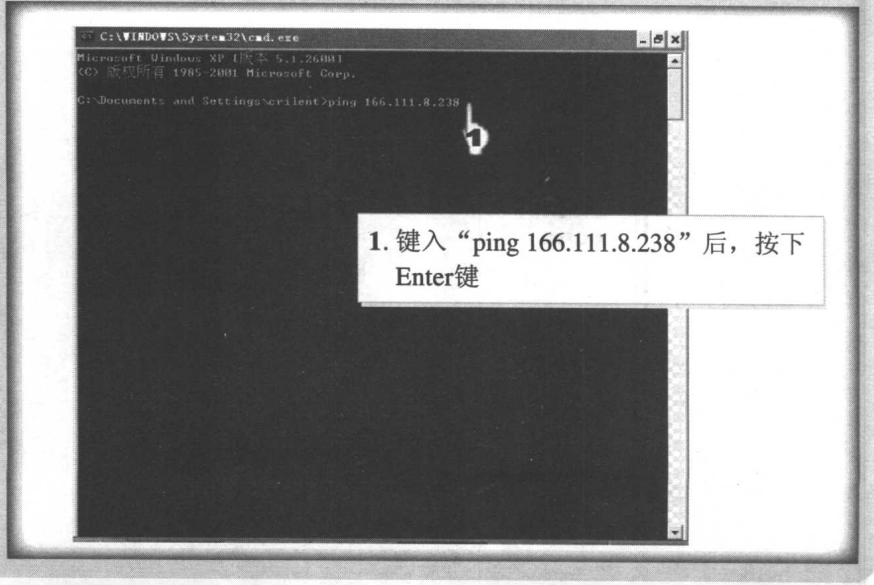
P可以用来做什么呢？其中一个重要的用途，就是可以用来确认计算机是不是在网络上活动。假设你的连接是在正常的情况下，可以通过在MS-DOS模式中使用Ping指令，来得知自己或他人的连接状况。

学前准备

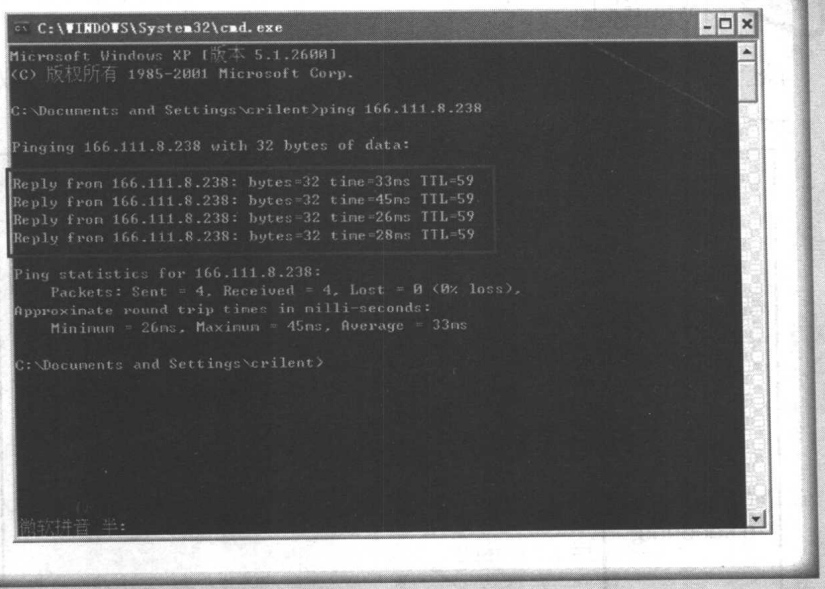
》从“开始”菜单执行“所有程序”|“附件”中的“命令提示符”命令，以打开命令提示符窗口。

Step 1

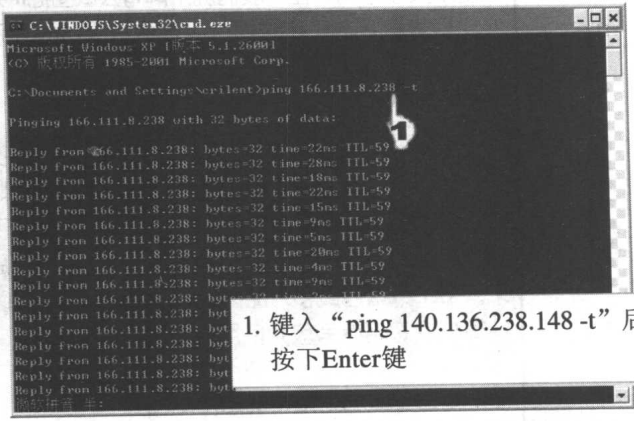
在“命令提示符”窗口中，使用Ping指令来查看自己或他人的连接状态。



若结果显示有时间及信号的响应，那代表网络的连接正常。



关于Ping指令的参数也有许多种应用，例如想要一直知道计算机的网络连接状态，可在Ping指令加IP地址的后方再加上-t的参数，如此即可连续得到该IP地址的连接状态显示；想要停止时，只要按下Ctrl＋C键则可停止。



1. 键入“ping 140.136.238.148 -t”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。