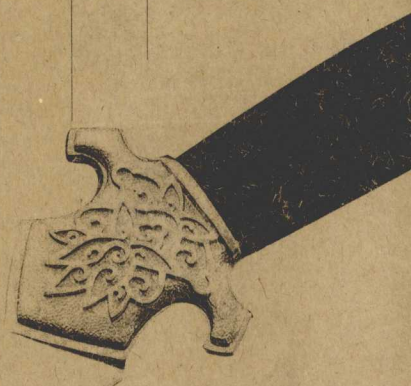
电脑迷 精品图书

黑客

兵刃大曝光

信息安全资深作者
踏雪无痕 燕归来 联合编著

黑客秘招，招招致命；
黑客兵刃，样样惊心；
黑客兵器谱完全展示！

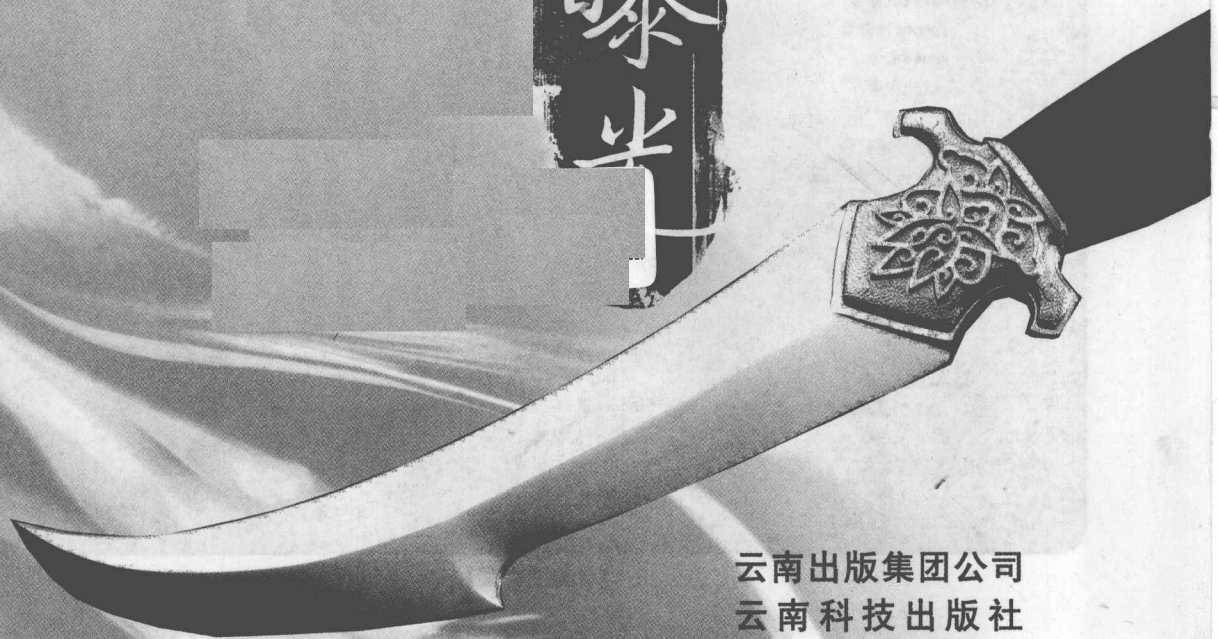


云南出版集团公司
云南科技出版社

电脑迷 精品图书

黑客

兵刃大曝光



云南出版集团公司
云南科技出版社

书　名：《黑客兵刃大曝光》
策　　划：蒲 涛
编　　著：踏雪无痕 燕归来
责任编辑：欧阳鹏 孙玮贤
执行编辑：李 超 彭 葵
组版编辑：周 平 钟 蓓
封面设计：汤 立
光盘制作：史 祺

出版单位：云南出版集团公司 云南科技出版社
技术支持：（023）63658888-13140
邮购热线：（023）63658888-13126

发　行：重庆中科普传媒发展股份有限公司发行部
电　话：（023）63658888－12060
传　真：（023）63659779
经　销：各地新华书店、报刊亭
光盘生产：苏州新海博数码科技有限公司
文本印刷：重庆升光电力印务有限公司
开本规格：188×266毫米 正度16开 20印张

版本号：ISBN978-7-900747-01-3
版　次：2008年1月第1版
定　价：29.80元（1CD+1手册）

为什么购买

开篇声明：本书仅从技术角度出发，对黑客的各种攻击入侵工具以实例的形式进行展示，全部是经过实战检验的。但——害人之心不可有，读者请勿将本书内容用于任何违法行为，否则一切法律责任请自负！

黑客秘笈，招招致命！
黑客兵刃，样样惊心！
这就是你的黑客兵器谱！

- 黑客攻击真实案例的图解讲述，以实战讲解黑客的工具的用法
- 黑客兵器的修炼秘笈，带你进入真实世界的“黑客帝国”

本书适用于对网络安全及黑客工具应用感兴趣的读者，旨在增强网民的安全防范意识，减少电脑和网络的安全隐患。

光盘内容：

- 视频讲解黑客软件的操作过程，
- 直接观看各类黑客工具的具体操作

光盘使用说明

特别说明：本光盘提供的黑客软件演示仅供研究使用，切勿利用来破坏他人的计算机或数据，否则一切后果自负。

点击任意视频按钮，即可直接播放界面列表中的黑客教学视频。

【光盘主界面】

目录
CONTENTS

第1章 黑客常用系统命令

在学习黑客技术之前，对计算机操作系统以及黑客常用命令有一个全面的了解是必要且非常关键的，因为使用系统命令是黑客技术的基石。本章将为读者介绍一些黑客常用的系统命令。

本章要点

- 操作系统
- DOS操作系统
- ping命令
- net和netstat命令
- telnet和ftp命令
- tracert命令
- ipconfig命令
- route命令
- netsh命令
- arp命令

1.1 操作系统与MS-DOS

操作系统是管理计算机硬件的程序，它为应用程序提供基础，并且充当计算机硬件和计算机用户的中介。所以，操作系统是用户操作计算机的基础。常见的操作系统有Windows、Linux、Unix、DOS等。

1.1.1 DOS简介及原理

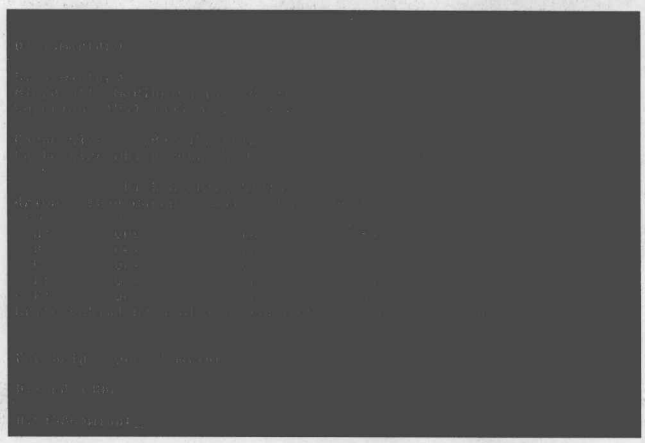
DOS（Disk Operation System）的全称是磁盘操作系统，DOS主要是一种面向磁盘的系统软件。打个比喻，DOS就是人与机器的一座桥梁，是罩在机器硬件外面的一层“外壳”，有了DOS，就不必去深入了解机器的硬件结构，也不必死记硬背那些枯燥的机器命令，只需通过一些接近于自然语言的DOS命令，就可以轻松地完成绝大多数的日常操作。另外，DOS还 能有效地管理各种软硬件资源，对它们进行合理的调度，所有的软件和硬件都在DOS的监控和管理之下，有条不紊地进行着自己的工作。

DOS主要由三个基本文件和一些外部命令构成。这三个基本文件是 MSDOS.SYS，IO.SYS和COMMAND.COM（如果是PC-DOS，则为IBMDOS.COM，IBMBIO.COM和 COMMAND.COM）。

（1）MSDOS.SYS称为DOS内核（可见MSDOS.SYS是个非常重要的文件），它主要是用来管理和启动系统的各个部件，为DOS的引导作好准备工作。

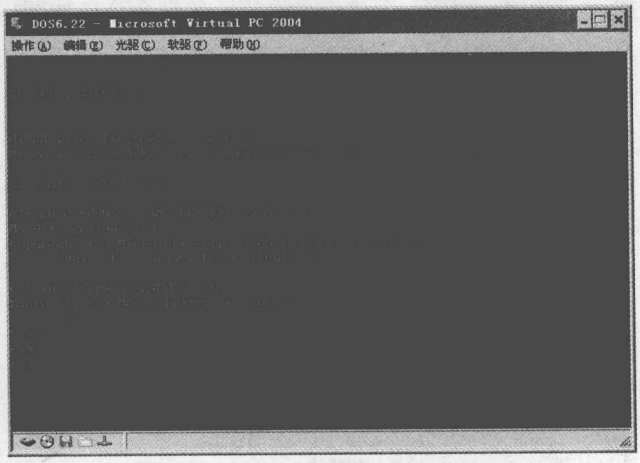
（2）IO.SYS（IO为Input&Output的缩写，意即“输入输出”）主要负责系统的基本输入和输出，即 DOS与各部件之间的联系。

（3）COMMAND.COM文件（COMMAND是“命令”的意思）是DOS与用户的接口，它主要提供了一些DOS的内部命令，接受、判别并执行用户输入的命令。磁盘是否具有启动DOS的能力，就看是否具备这三个文件，具有这三个文件的磁盘，就称作引导盘。而除此之外还包含许多 DOS外部命令的磁盘则称为系统盘，如图1-1所示的基本的DOS命令。



【图1-1】基本的DOS命令

自从DOS在1981年问世以来，版本就不断更新，从最初的DOS1.0升级到了最新的DOS8.0（Windows ME系统），纯DOS 的最高版本为DOS6.22，如图1-2所示的DOS6.22版本在虚拟机上的效果。这以后的新版本DOS都是由Windows系统所提供的，并不单独存在。



【图1-2】DOS6.22版本在虚拟机上的效果

DOS的优点是快捷。熟练的用户可以通过创建BAT或CMD批处理文件完成一些烦琐的任务，通过一些判断命令（IF、|）甚至可以编写一些小程序。因此，即使在Windows XP下CMD还是高手的最爱。目前常用的DOS包括：MS-DOS（微软公司出品）、 PC-DOS（IBM公司出品）、FreeDOS、ROM-DOS等，眼下流行的Windows系统是以MS-DOS为基础的。

MS-DOS的主要功能是进行内存管理、文件管理和输入/输出管理。为了实现这些功能，MS-DOS主要由四个部分组成：文件管理系统、输入/输出管理系统、命令处理系统和外部命令集，如图1-3所示。

```
C:\>mem
Memory Type         Total   =    Used   +    Free
----------------  --------   --------   --------
Conventional          640K        35K       605K
Upper                 155K       155K         0K
Reserved              384K       384K         0K
Extended (XMS)     23,397K    22,373K     1,024K
----------------  --------   --------   --------
Total memory       24,576K    22,947K     1,629K

Total under 1 MB      795K       190K       605K

Largest executable program size  605K (619,216 bytes)
Largest free upper memory block    0K       (0 bytes)
MS-DOS is resident in the high memory area.

C:\>
```

【图1-3】MS-DOS命令行格式

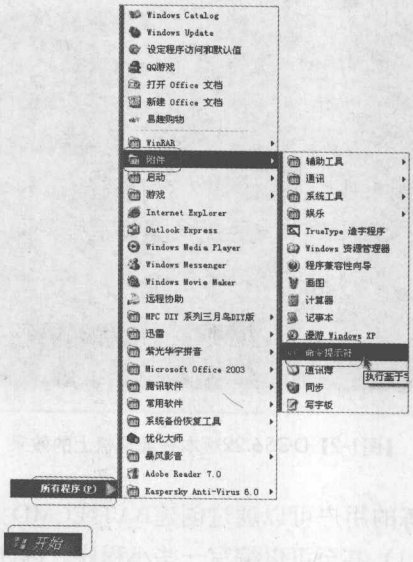
1.1.2 Windows NT/2000/XP下的启动法

在WindowNT/2000/XP下，系统提供了一个字符操作界面，可以在此界面下运行DOS命

令，进行操作，而且不必进行Window操作系统与DOS操作系统之间的转换，比较便捷高效，本章中的DOS命令均在此字符界面进行操作，下面介绍运行“DOS的字符界面”的三种方法。

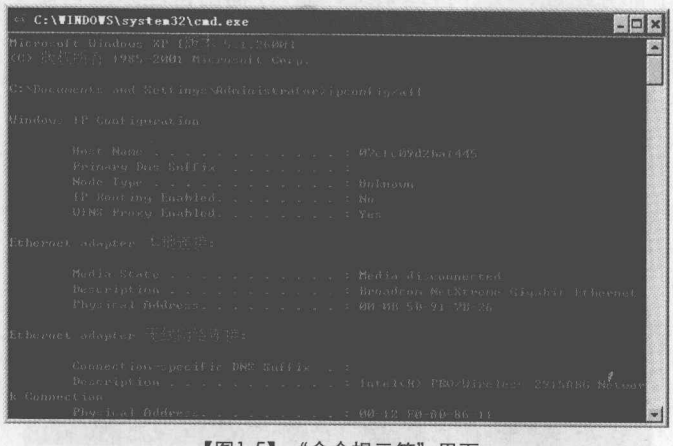
方法一：利用开始菜单进入DOS字符界面

（1）依次单击执行“开始→程序→附件→命令提示符”命令，如图1-4所示。



【图1-4】“命令提示符”选项

（2）弹出“命令提示符”界面，如图1-5所示。在此界面输入DOS命令，例如输入：ipconfig/all（查看IP地址）命令，然后单击回车键即可执行。



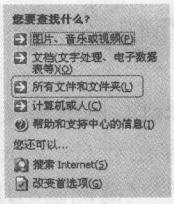
【图1-5】“命令提示符”界面

方法二：使用“搜索”功能进入DOS字符界面

（1）单击“开始”按钮，在弹出的开始菜单中单击“搜索”选项，如图1-6所示。

（2）在搜索界面中单击“所有文件和文件夹”，如图1-7所示。

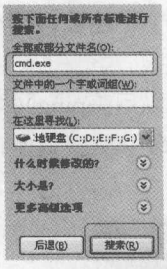
【图1-6】“搜索”选项



【图1-7】“搜索”界面

(3) 在搜索的“全部或部分文件名”中输入“cmd.exe”，然后单击“搜索”按钮，如图1-8所示。

(4) 开始搜索，在搜索结果中会出现一个C盘盘符标志的名为“cmd”的文件，如图1-9所示。双击该文件即可弹出用于键入DOS命令的命令提示符界面。



【图1-8】搜索内容

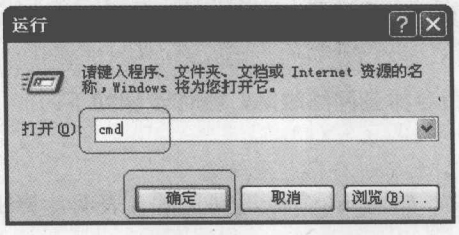
【图1-9】搜索结果

方法三：通过“运行”命令启动

(1) 单击“开始”按钮，在弹出的开始菜单中单击“运行”选项，如图1-10所示。

【图1-10】“运行”选项

(2) 在弹出的“运行”对话框中输入“cmd”命令，然后单击“确定”按钮，如图1-11所示。即可弹出用于键入DOS命令的命令提示符界面了。



【图1-11】运行命令

1.2 ping命令

Ping是用来进行网络连接测试的一个程序，对应的文件名为“Ping.exe”（在Windows XP系统下此文件存在于 C:\Windows\System32文件夹下）。此工具的最简单的用法是：“Ping xxx.xxx.xxx.xxx”（欲测试的IP地址），根据不同的测试目的可以带上不同的参数。使用 ping 可以测试计算机名和计算机的IP地址，验证与远程计算机的连接，通过将icmp回显数据包发送到计算机并侦听回显回复数据包来验证与一台或多台远程计算机的连接，此命令只有在安装了TCP/IP协议后才可以使用。

1.2.1 使用方式图解

Ping命令的使用很简单，键入ping后，再空格，然后键入一个IP地址。那么就会显示此IP地址的响应时间等信息，以显示是否连接。

Ping命令既可以用来ping自己的IP地址检查网络状况。又可以用来ping网络中其他计算机的IP地址，比如要传文件给网络中其他计算机之前，可以用ping命令测试其他计算机是否开机或者网络是否畅通，如图1-12所示。

【图1-12】ping命令测试其他计算机

1.2.2 使用实战

ping的一个重要用途是检查和排除本机网络故障。

巧妙使用ping命令可以快速排查网络故障。如果计算机接入互联网后，发现不能上网，则使用ping命令，逐步进行一系列测试，就能够找到并排除故障。

『案例1-1』使用ping命令排查网络故障，操作步骤如下：

1.ping 127.0.0.1

测试环回地址是否正常。如果ping命令返回正常，表明计算机安装的TCP/IP协议工作正常，如图1-13所示。

【图1-13】ping 127.0.0.1

127.0.0.1是网卡的环回地址。所谓环回地址，是在网卡的网络接口处设置一个环回路径，用于将本机发出的目的地到本机的报文，通过环回路径送回给本机上层协议，以用来测试自身网络协议是否工作正常。环回地址也可以用来进程间通信。

2.ping 本机IP地址

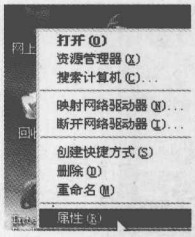
本机IP地址可以通过自动分配获得，也可以人工配置。如果事先不知道本机的IP地址，可以通过ipconfig命令查看（具体内容参看1.6节）。这里设本机IP地址为127.36.78.30，如图1-14所示。

【图1-14】ping本机IP地址

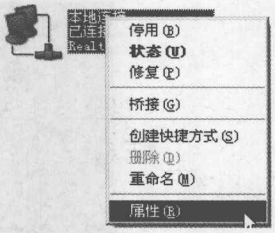
手动配置IP地址，首先需要询问网管，从网管处获得配置所需的参数。配置的方法如下：

（1）在桌面“网上邻居”图标上单击鼠标右键，在弹出的下拉菜单中选择“属性”命令，如图1-15所示。

（2）在弹出的“网络连接”窗口中，“本地连接”图标上单击鼠标右键，在弹出的菜单中单击“属性”，如图1-16所示。



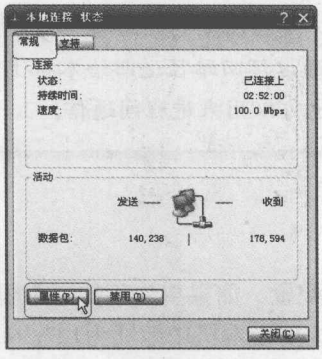
【图1-15】“网上邻居”中单击“属性”



【图1-16】“本地连接”中单击“属性”

(3) 在弹出的“本地连接 状态”对话框中，在“常规”选项卡下，单击“属性”按钮，如图1-17所示。

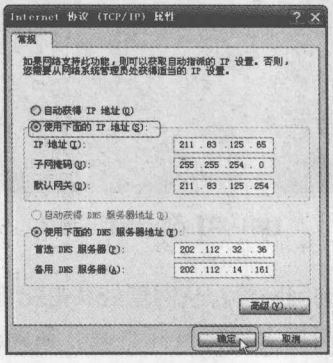
(4) 在弹出的“本地连接 属性”对话框中单击“Internet协议（TCP/IP）属性”，然后单击“属性”按钮，如图1-18所示。



【图1-17】“本地连接 状态”对话框

【图1-18】“本地连接 属性”对话框

(5) 在弹出的“Internet协议（TCP/IP）属性”对话框中配置IP地址、子网掩码、默认网关以及DNS等信息。由于是手动设置，所以先选择“使用下面的IP地址”，然后分别输入IP地址、子网掩码、默认网关和DNS服务器地址，最后单击“确定”按钮完成设置，如图1-19所示。



【图1-19】配置IP地址

(6) 如果在自动分配中分得了IP地址，那么在“Internet协议（TCP/IP）属性”对话框