从新手到高手

黑客入门与网络安全实用手册

安全技术全新升级

# 黑客攻防与电脑安全

## 从新手到高手（超值版）

网络安全技术联盟 编著


一线网络安全技术联盟倾心打造

海量王牌资源超值赠送

超值赠送1 1000分钟精品教学视频

超值赠送2 教学用PPT课件

超值赠送3 黑客防守工具包

超值赠送4 107个黑客工具速查手册

超值赠送5 160个常用黑客命令速查手册

超值赠送6 180页常见故障维修手册

超值赠送7 191页Windows10系统使用和防护技巧

清华大学出版社

从新手到高手155

# 黑客攻防与电脑安全

（超值版）

清华大学出版社
北京

## 内容简介

本书在剖析用户进行黑客防御中迫切需要或想要用到的技术时，力求对其进行傻瓜式的讲解，使读者对网络防御技术有一个系统的了解，能够更好地防范黑客的攻击。全书共分为17章，包括电脑安全快速入门、系统漏洞与安全的防护策略、系统入侵与远程控制的防护策略、电脑木马的防护策略、电脑病毒的防护策略、系统安全的终极防护策略、文件密码数据的防护策略、磁盘数据安全的防护策略、系统账户数据的防护策略、网络账号及密码的防护策略、网页浏览器的防护策略、移动手机的防护策略、平板电脑的防护策略、网上银行的防护策略、手机钱包的防护策略、无线蓝牙设备的防护策略、无线网络安全的防护策略等内容。

另外，本书还赠送海量王牌资源，包括1000分钟精品教学视频、107个黑客工具速查手册、160个常用黑客命令速查手册、180页常见故障维修手册、191页Windows 10系统使用和防护技巧、教学用PPT课件以及随书攻防工具包，帮助读者掌握黑客防守方方面面的知识。

本书内容丰富、图文并茂、深入浅出，不仅适用于网络安全从业人员及网络管理员，而且适用于广大网络爱好者，也可作为大、中专院校相关专业的参考书。



**图书在版编目(CIP)数据**

黑客攻防与电脑安全从新手到高手：超值版 / 网络安全技术联盟编著. —北京：清华大学出版社，2017
（从新手到高手）
ISBN 978-7-302-47371-8

Ⅰ ①黑… Ⅱ. ①网… Ⅲ. ①黑客—网络防御 Ⅳ. ①TP393.081

中国版本图书馆CIP数据核字（2017）第124150号

**责任编辑：**张　敏
**封面设计：**杨玉兰
**责任校对：**徐俊伟
**责任印制：**沈　露

**出版发行：**清华大学出版社
网　　址：http://www.tup.com.cn，　http://www.wqbook.com
地　　址：北京清华大学学研大厦A座　　邮　　编：100084
社 总 机：010-62770175　　邮　　购：010-62786544
投稿与读者服务：010-62776969, c-service@tup.tsinghua.edu.cn
质量反馈：010-62772015, zhiliang@tup.tsinghua.edu.cn
**印 装 者：**北京嘉实印刷有限公司
**经　　销：**全国新华书店
**开　　本：**185mm×260mm　　**印　　张：**20　　**字　　数：**503千字
**版　　次：**2017年9月第1版　　**印　　次：**2017年9月第1次印刷
**印　　数：**1～4000
**定　　价：**59.80元

产品编号：074521-01

# Preface 前言

随着手机、平板电脑的普及，无线网络的防范就变得尤为重要，为此，本书除了讲解有线网络的攻防策略外，还把目前市场上流行的无线攻防、移动端攻防、手机钱包等热点融入本书中。

**本书特色**

知识丰富全面：知识点由浅入深，涵盖了所有黑客攻防知识点，由浅入深地掌握黑客攻防方面的技能。

图文并茂：注重操作，在介绍案例的过程中，每一个操作均有对应的插图。这种图文结合的方式使读者在学习过程中能够直观、清晰地看到操作的过程以及效果，便于更快地理解和掌握。

案例丰富：把知识点融汇于系统的案例实训当中，并且结合经典案例进行讲解和拓展，进而达到“知其然，并知其所以然”的效果。

提示技巧、贴心周到：本书对读者在学习过程中可能会遇到的疑难问题以“提示”的形式进行了说明，以免读者在学习的过程中走弯路。

**超值赠送**

本书将赠送1000分钟精品教学视频、107个黑客工具速查手册、160个常用黑客命令速查手册、180页常见故障维修手册、191页Windows 10系统使用和防护技巧，读者可扫描二维码获取海量王牌资源，也可联系QQ群223145261获得更多赠送资源（包括黑客防守工具包），掌握黑客防守方方面面的知识。

**读者对象**

本书不仅适用于网络安全从业人员及网络管理员，而且适用于广大网络爱好者，也可作为大、中专院校相关专业的参考书。

**写作团队**

本书由长期研究网络安全知识的网络安全技术联盟编著，另外还有王莉、方秦、程木香、李小威、刘辉、刘尧、任志杰、王朵朵、王猛、王婷婷、张芳、张桐嘉、王英英、王维维、肖品等人也参与了编写工作。在编写过程中，尽所能地将最好的讲解呈现给读者，但也难免有疏漏和不妥之处，敬请不吝指正。若您在学习中遇到困难或疑问，或有何建议，可联系QQ群223145261和作者QQ625948078，获得作者的在线指导和本书海量资源。

编　者

# Contents 目录

# 第1章　电脑安全快速入门

作为计算机或网络终端设备的用户，要想使自己的设备不受或少受黑客的攻击，就必须了解一些黑客常用的入侵技能以及学习一些计算机安全方面的基础知识，本章将介绍有关这方面的知识，如什么是端口、IP地址以及黑客常用的攻击命令等。

## 1.1　IP地址与MAC地址

在互联网中，一台主机只有一个IP地址，因此，黑客要想攻击某台主机，必须找到这台主机的IP地址，然后才能进行入侵攻击，可以说IP地址是黑客实施入侵攻击的一个关键。

### 1.1.1　认识IP地址

IP地址用于在TCP/IP通信协议中标记每台计算机的地址，通常使用十进制来表示，如192.168.1.100，但在计算机内部，IP地址是一个32位的二进制数值，如11000000 10101000 00000001 00000110（192.168.1.6）。

一个完整的IP地址由两部分组成，分别是网络号部分和主机号部分。网络号表示其所属的网络段编号，主机号则表示该网段中该主机的地址编号。

按照网络规模的大小，IP地址可以分为A、B、C、D、E5类，其中A、B、C类是3种主要的类型地址，D类专供多目传送地址，E类用于扩展备用地址。

- A类IP地址。一个A类IP地址由1个字节的网络地址和3个字节的主机地址组成，网络地址的最高位必须是“0”，地址范围从1.0.0.0 ~ 126.0.0.0。
- B类IP地址。一个B类IP地址由2个字节的网络地址和2个字节的主机地址组成，网络地址的最高位必须是“10”，地址范围从128.0.0.0~191.255.255.255。
- C类IP地址。一个C类IP地址由3个字节的网络地址和1个字节的主机地址组成，网络地址的最高位必须是“110”。地址范围从192.0.0.0~223.255.255.255。
- D类IP地址。用于多点广播（Multicast）。D类IP地址第一个字节以“10”开始，它是一个专门保留的地址。它并不指向特定的网络，目前这一类地址被用在多点广播（Multicast）中。多点广播地址用来一次寻址一组计算机，它标识共享同一协议的一组计算机。
- E类IP地址。以“10”开始，为将来使用保留，全“0”（0.0.0.0）IP地址对应于当前主机；全“1”的IP地址（255.255.255.255）是当前子网的广播地址。

具体来讲，一个完整的IP地址信息应该包括IP地址、子网掩码、默认网关和DNS等4部分。只有这4部分协同工作，才能与互联网中的计算机相互访问。

- 子网掩码：子网掩码是与IP地址结合使用的一种技术。主要作用有两个：一是用于确定IP地址中的网络号和主机号；二是用于将一个大的IP网络划分为若干小的子网络。

- 默认网关：默认网关意为一台主机如果找不到可用的网关，就把数据包发送给默认指定的网关，由这个网关来处理数据包。
- DNS：DNS服务用于将用户的域名请求转换为IP地址。

### 1.1.2 认识MAC地址

MAC地址是在媒体接入层上使用的地址，也称为物理地址、硬件地址或链路地址，由网络设备制造商生产时写在硬件内部。MAC地址与网络无关，也即无论将带有这个地址的硬件（如网卡、集线器、路由器等）接入到网络的何处，MAC地址都是相同的，它由厂商写在网卡的BIOS里。

MAC地址通常表示为12个十六进制数，每2个十六进制数之间用冒号隔开，如：08:00:20:0A:8C:6D就是一个MAC地址，其中前6位（08:00:20）代表网络硬件制造商的编号，它由IEEE分配，而后3位（0A:8C:6D）代表该制造商所制造的某个网络产品（如网卡）的系列号。

每个网络制造商必须确保它所制造的每个以太网设备前3个字节都相同，后3个字节不同，这样，就可以保证世界上每个以太网设备都具有唯一的MAC地址。

**知识链接**

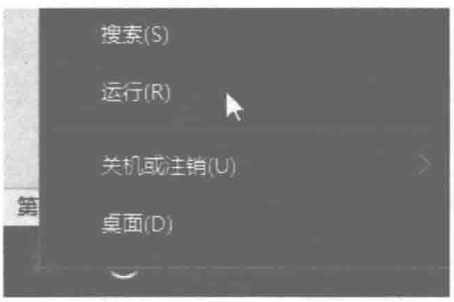
IP地址与MAC地址的区别在于：IP地址基于逻辑，比较灵活，不受硬件限制，也容易记忆。MAC地址在一定程度上与硬件一致，基于物理，能够具体标识。这两种地址均有各自的长处，使用时也因条件不同而采取不同的地址。

### 1.1.3 查看IP地址

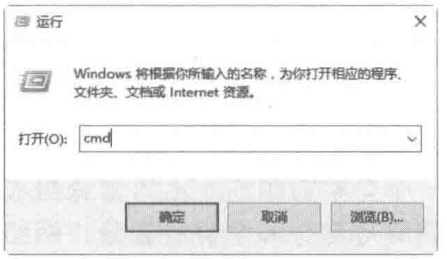
计算机的IP地址一旦被分配，可以说是固定不变的，因此，查询出计算机的IP地址，在一定程度上就实现了黑客入侵的前提工作。使用ipconfig命令可以获取本地计算机的IP地址和物理地址。

具体的操作步骤如下。

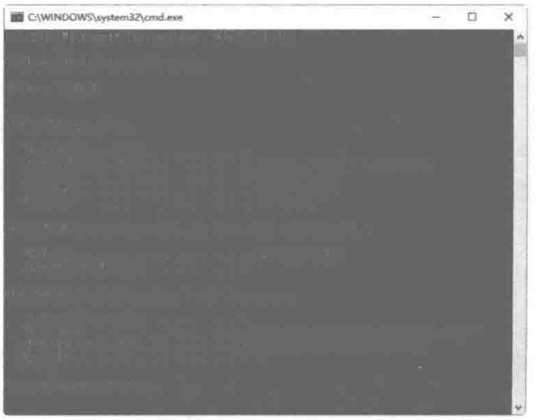
**Step 01** 右击【开始】按钮，在弹出的快捷菜单中执行【运行】命令。




**Step 02** 打开【运行】对话框，在【打开】后面的文本框中输入cmd命令。



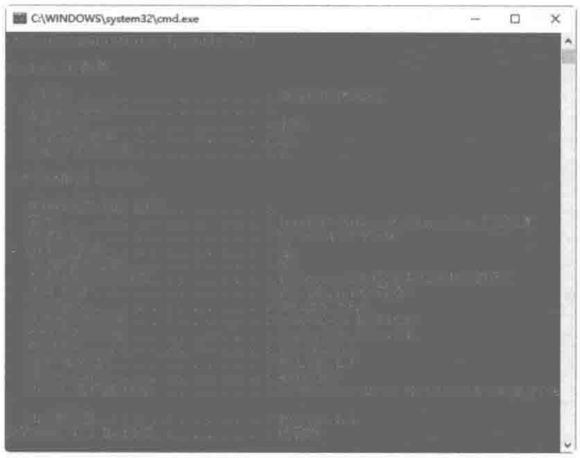

**Step 03** 单击【确定】按钮，打开【命令提示符】窗口，在【命令提示符】窗口中输入ipconfig，按Enter键，即可显示出本机的IP配置相关的信息。



提示：在【命令提示符】窗口中，192.168.0.102表示本机在局域网中的IP地址。

### 1.1.4　查看MAC地址

在【命令提示符】窗口中输入ipconfig /all命令，然后按Enter键，可以在显示的结果中看到一个物理地址：6C-0B-84-3E-F7-AB，这就是用户自己的计算机的网卡地址，它是唯一的。

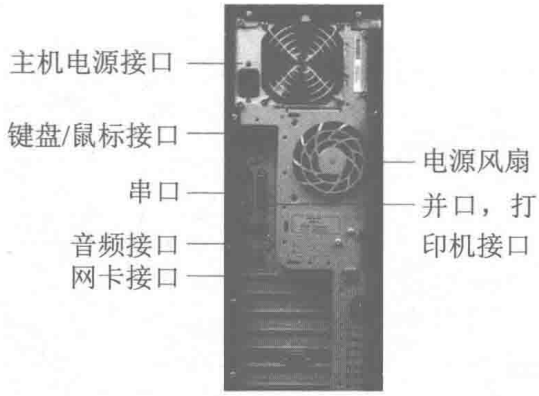



## 1.2　什么是端口

“端口”可以认为是计算机与外界通信交流的出口。一个IP地址的端口可以有65 536（即256×256）个，端口是通过端口号来标记的，端口号只有整数，范围是0~65 535（256×256-1）。

### 1.2.1　认识端口

计算机领域可分为硬件领域和软件领域，在硬件领域中，端口又被称作为接口，如常见的USB端口、网卡接口、串行端口等；在软件领域中，端口一般是指网络中面向连接服务和无连接服务的通信协议端口，是一种抽象的软件结构，包括一些数据结构和I/O（基本输入输出）缓冲区。



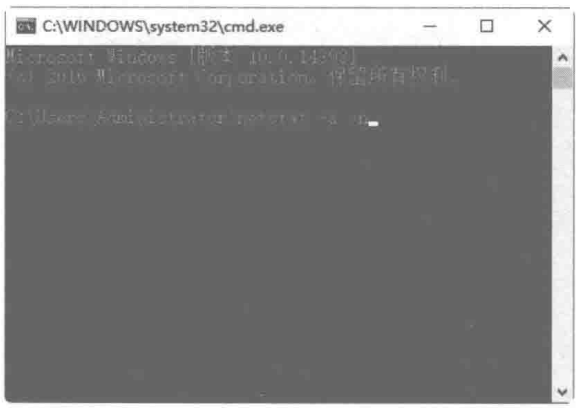

在网络技术中，端口又有几种含义：其中，一种是物理意义上的端口，如集线器、交换机、路由器等连接设备，用于连接其他的网络设备的接口，常见的有RJ-45端口、Serial端口等；另一种是逻辑意义上的端口，一般指TCP/IP协议中的端口，范围是0~65 535（256×256-1）。

### 1.2.2　查看系统的开放端口

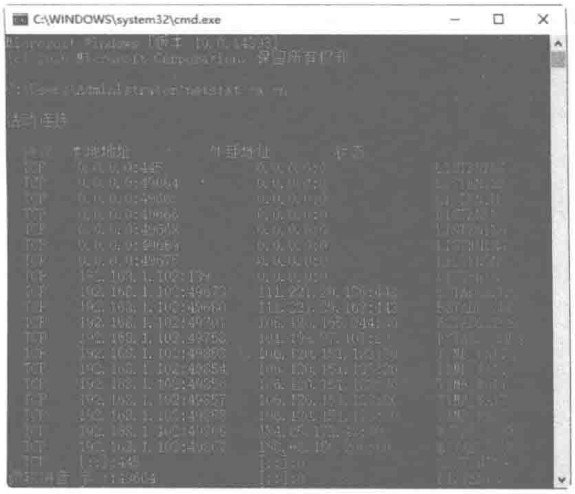
经常查看系统开放端口的状态变化，可以帮助计算机用户及时提高系统安全，防止黑客通过端口入侵电脑，用户可以使用netstat命令查看自己系统的端口的状态。

具体操作步骤如下。

Step 01 打开【命令提示符】窗口，在其中输入netstat -a -n命令。




Step 02 按Enter键，即可看到以数字显示的TCP和UCP连接的端口号及其状态。




### 1.2.3 关闭不必要的端口

默认情况下，计算机系统中有很多没有用或不安全的端口是开启的，这些端口很容易被黑客利用。为保障系统的安全，可以将这些不用的端口关闭。关闭端口的方式有多种，这里介绍通过关闭无用服务来关闭不必要的端口。

以关闭Remote Desktop Help Session Manager（Windows远程协助服务）为例，具体操作步骤如下。

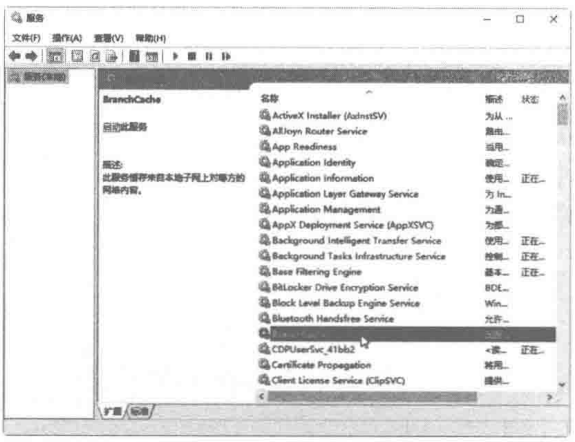
**Step 01** 右击【开始】按钮，在弹出的快捷菜单中执行【控制面板】命令。


**Step 02** 打开【控制面板】窗口，双击【管理工具】图标。

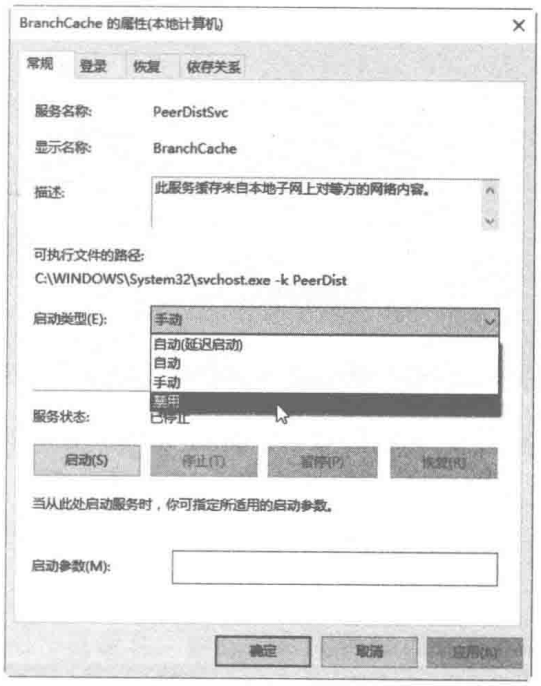
**Step 03** 打开【管理工具】窗口，双击【服务】图标。



**Step 04** 打开【服务】窗口，找到Branch Cache服务项。



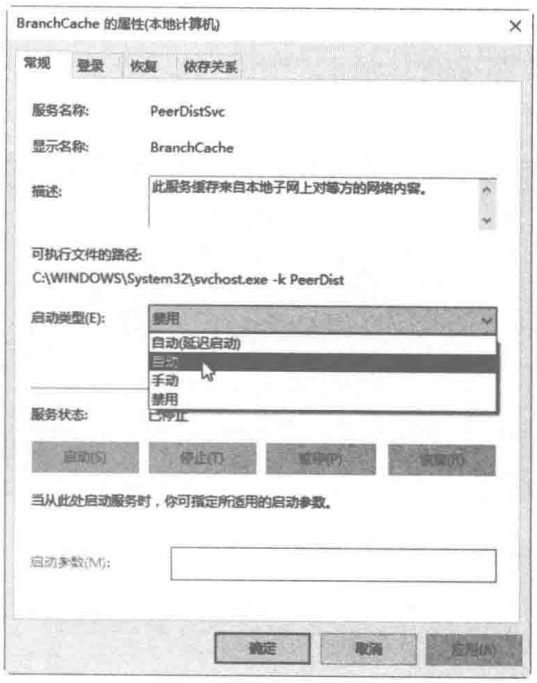

**Step 05** 双击该服务项，弹出【Branch Cache的属性】对话框，在【启动类型】下拉列表中选择【禁用】选项，然后单击【确定】按钮禁用该服务项的端口。



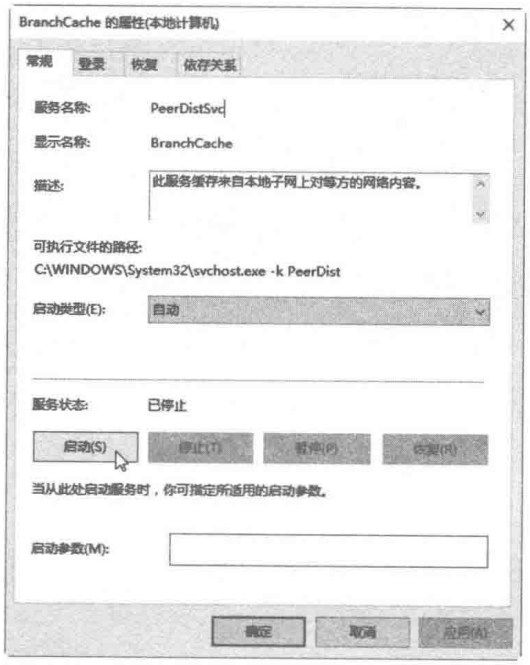

## 1.2.4　启动需要开启的端口

开启端口的操作与关闭端口的操作类似，下面具体介绍通过启动服务的方式开启端口的具体操作步骤。

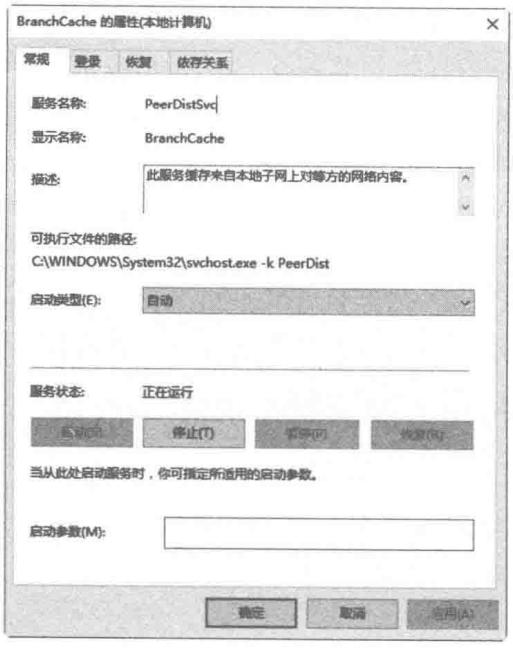
**Step 01** 这里以上述停止的Branch Cache服务端口为例。在【Branch Cache的属性】对话框中单击【启动类型】右侧的下拉按钮，在打开的下拉菜单中选择【自动】。




**Step 02** 单击【应用】按钮，激活“服务状态”下的【启动】按钮。




**Step 03** 单击【启动】按钮，即可启动该项服务，再次单击【应用】按钮，在【Branch Cache的属性】对话框中可以看到该服务的【服务状态】已经变为【正在运行】。




**Step 04** 单击【确定】按钮，返回【服务】窗口，此时即可发现Branch Cache服务的【状态】变为【正在运行】，这样就可以成功开启Branch Cache服务对应的端口。

## 1.3 黑客常用的DOS命令

熟练掌握一些DOS命令是一名黑客的基本功，下面就来介绍黑客常用的一些DOS命令，了解这样命令可以帮助计算机用户追踪黑客的踪迹，从而提高个人计算机的安全性。

### 1.3.1 cd命令

cd（Change Directory）命令的作用是改变当前目录，该命令用于切换路径目录。

cd命令主要有以下3种使用方法。

（1）cd path：path是路径，例如输入cd c:\命令后按Enter键或输入cd Windows命令，即可分别切换到C:\和C:\Windows目录下。

（2）cd..：cd后面的两个“.”表示返回上一级目录，例如当前的目录为C:\Windows，如果输入cd..命令，按Enter键即可返回上一级目录，即C:\。

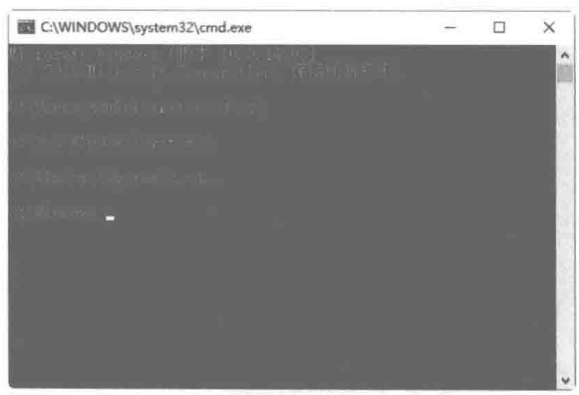
（3）cd\：表示当前无论在哪个子目录下，通过该命令可立即返回到根目录下。

下面将介绍使用cd命令进入C:\Windows\system32子目录，并退回根目录的具体操作步骤。

**Step 01** 在【命令提示符】窗口中输入cd c:\命令，按Enter键，即可将目录切换为C:\。


**Step 02** 如果想进入C:\Windows\system32目录中，则需在上面的【命令提示符】窗口中输入cd Windows\system32命令，按Enter键即可将目录切换为C:\Windows\system32。


**Step 03** 如果想返回上一级目录，则可以在【命令提示符】窗口中输入cd..命令，按Enter键即可。




**Step 04** 如果想返回到根目录，则可以在【命令提示符】窗口中输入cd\命令，按Enter键即可。