第 1 章 网络安全快速入门

随着信息时代的发展和网络的普及，越来越多的人步入了网络生活，然而人们在享受网络带来便利的同时，也时刻面临着黑客们残酷攻击的危险。本章就来介绍网络安全的相关技术信息，主要内容包括网络中的相关概念、网络通信的相关协议、IP 地址、MAC 地址、端口、系统进程等。

1.1 网络中的相关概念

在网络安全中，经常会接触到很多和网络有关的概念，如浏览器、URL、FTP、IP 地址及域名等，理解了这些概念，对保护网络安全有一定的帮助。

1.1.1 互联网与因特网

互联网是指将两台计算机或者是两台以上的计算机终端、客户端、服务端通过计算机信息技术的手段互相联系起来构成的网络。互联网在现实生活中应用很广泛，在互联网上人们可以聊天、玩游戏、查阅资料等。互联网是全球性的，这就意味着这个网络不管是谁发明了它，是属于全人类的。图 1-1 为互联网的结构示意图。

因特网是一个把分布于世界各地的计算机用传输介质互相连接起来的网络。因特网是基于 TCP/IP 实现的。TCP/IP 由很多协议组成，不同类型的协议又被放在不同的层，其中位于应用层的协议就有很多，比如 FTP、SMTP、HTTP。图 1-2 为因特网的结构示意图。

图 1-1　互联网结构示意图

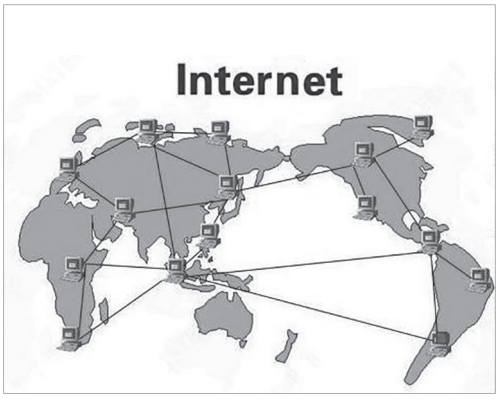

图 1-2　因特网结构示意图

1.1.2 万维网与浏览器

万维网（world wide web，WWW）简称为 3W，是无数个网络站点和网页的集合，也是因特网提供的最主要的服务。它是由多媒体链接而形成的集合，通常我们上网看到的内容就是万维网的内容。图 1-3 为使用万维网打开的百度首页。

提示：互联网、因特网、万维网三者的关系是互联网包含因特网，因特网包含万维网。凡是能彼此通信的设备组成的网络就叫互联网。所以，即使仅有两台机器，不论用何种技术使其彼此通信，也叫互联网。

浏览器是将互联网上的文本文档（或其他类型的文件）翻译成网页，并让用户与这些文件交互的一种软件工具，主要用于查看网页的内容。目前最常用的浏览器有微软公司的 Microsoft Edge，图 1-4 是使用 Microsoft Edge 浏览器打开的页面。

图 1-3　百度首页

图 1-4　Microsoft Edge 浏览器

1.1.3 URL 地址与域名

图 1-5　使用 URL 地址打开的网页

URL（uniform resource locator）即统一资源定位器，也就是网络地址，是在因特网上用来描述信息资源，并将因特网提供的服务统一编址的系统。简单来说，通常在浏览器中输入的网址就是 URL 的一种，如百度网址 https://www.baidu.com。

域名（domain name）类似于互联网上的门牌号，是用于识别和定位互联网上计算机的层次结构的字符标识，与该计算机的因特网协议（IP）地址相对应。相对于 IP 地址而言，域名更便于使用者理解和记忆。URL 和域名是两个不同的概念，如 https://www.sohu.com/ 是 URL，而 www.sohu.com 是域名，图 1-5 为使用 URL 地址打开的网页。

1.1.4 IP 与 MAC 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）。

MAC 地址与网络无关，也就是无论将带有这个地址的硬件（如网卡、集线器、路由器等）接入网络的何处，都是相同的 MAC 地址，它是由厂商写在网卡的 BIOS 里。

MAC 地址通常表示为 12 个十六进制数，每两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（电气电子工程学会）分配，而后 6 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 字节都相同，后 3 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。

提示：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。

1.2　认识网络通信协议

网络通信协议是计算机网络的一个重要组成部分，是不同网络之间通信、“交流”的公共语言。有了它，使用不同系统的计算机或网络之间才可以彼此识别，识别出不同的网络操作指令，建立信任关系。

1.2.1　TCP/IP

TCP/IP 包括两个子协议，即 TCP（transmission control protocol，传输控制协议）和 IP（internet protocol，因特网协议）。在这两个子协议中又包括许多应用型的协议和服务，使得 TCP/IP 的功能非常强大。

TCP/IP 中除了包括 TCP、IP 两个协议外，还包括许多子协议。它的核心协议包括用户数据报协议（UDP）、地址解析协议（ARP）及因特网控制消息协议（ICMP）等。

1.2.2　IP

IP 也称互联网协议，可实现两个基本功能：寻址和分段。IP 可以根据数据报报头中包括的目的地址将数据报传送到目的地址。另外，IP 使用 4 个关键技术提供服务：服务类型、生存时间、选项和报头校验码。

IP 的基本任务是通过互联网传送数据报，各个 IP 数据报之间是相互独立的。IP 从源运输实体取得数据，通过它的数据链路层服务传给目的主机的 IP 层。在传送时，高层协议将数据传给 IP，IP 再将数据封装为互联网数据报，并交给数据链路层协议通过局域网传送。

1.2.3　ARP

ARP（address resolution protocol，地址解析协议）的基本功能是通过目标设备的 IP 地址，查询目标设备的 MAC 地址，以保证通信的顺利进行。在局域网中，网络中实际传输的是“帧”，帧里面是有目标主机 MAC 地址的。

在以太网中，一个主机要和另一个主机进行直接通信，必须要知道目标主机的 MAC 地址，这个 MAC 地址就是通过地址解析协议获得的。所谓地址解析，就是主机在发送数据帧前将目标 IP 地址转换成目标 MAC 地址的过程。

1.2.4 ICMP

ICMP（internet control message protocol，因特网控制消息协议）是 TCP/IP 中的子协议，主要用于在 IP 主机、路由器之间传递控制消息。控制消息是指网络通不通、主机是否可达、路由是否可用等网络本身的消息。这些控制消息虽然并不传输用户数据，但是对于用户数据的传递起着重要作用。

ICMP 对于网络安全非常重要，常被用来攻击网络上的路由器和主机。例如，可以利用操作系统规定的 ICMP 数据包最大尺寸不超过 64KB 这一规定，向主机发起“Ping of Death”（死亡之 Ping）攻击。

1.3 计算机基本信息的获取

一台计算机的基本信息包括 IP 地址、物理地址、端口信息、系统进程信息、注册表信息等各种系统信息。用户要想提高计算机的安全系数，必须要学会查看计算机基本信息的方法。

1.3.1 获取本机的 IP 地址

微视频

图 1-6 “运行”菜单

在互联网中，一台主机只有一个 IP 地址。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。使用 ipconfig 命令可以获取本地计算机的 IP 地址，具体的操作步骤如下：

Step01 右击“开始”按钮，在弹出的快捷菜单中选择“运行”选项，如图 1-6 所示。

Step02 打开“运行”对话框，在“打开”后面的文本框中输入 cmd 命令，如图 1-7 所示。

Step03 单击“确定”按钮，打开“命令提示符”窗口，在其中输入 ipconfig，按 Enter 键，显示出本机的 IP 配置相关信息，如图 1-8 所示。

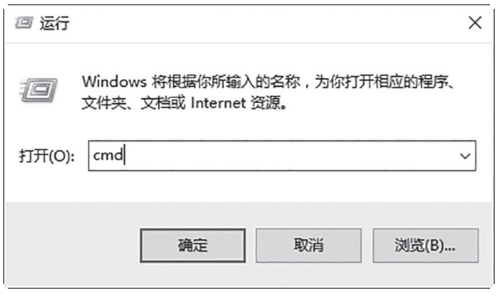

图 1-7 输入 cmd 命令

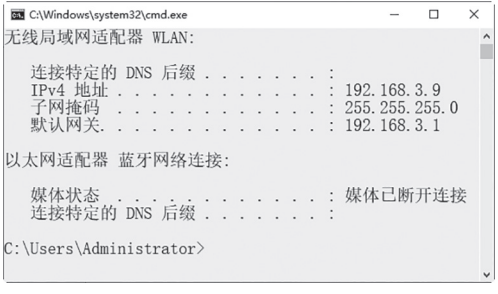

图 1-8 查看 IP 地址

提示：在“命令提示符”窗口中，192.168.3.9 表示本机在局域网中的 IP 地址。

1.3.2 获取本机的物理地址

微视频

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：00-23-24-DA-43-8B，这就是本机的物理地址，也是本机的网卡地址，它是唯一的，如图 1-9 所示。

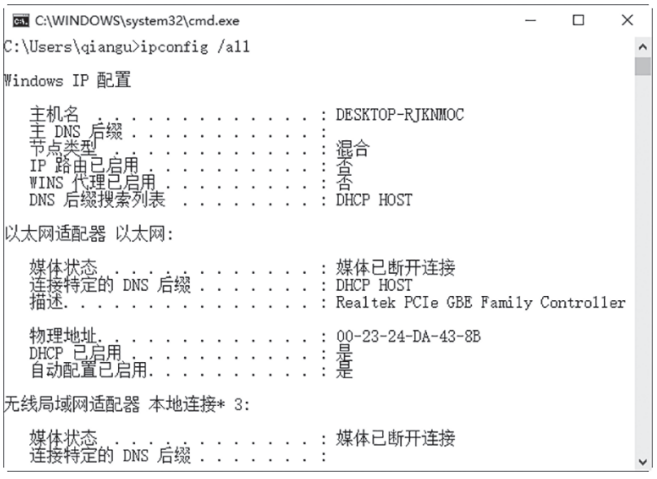

图 1-9　查看物理地址

1.3.3　查看系统开放的端口


微视频

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查看系统安全状况，防止黑客通过端口入侵计算机。用户可以使用 netstat 命令查看自己系统的端口状态，具体的操作步骤如下：

Step 01 打开“命令提示符”窗口，在其中输入 netstat -a -n 命令，如图 1-10 所示。

Step 02 按 Enter 键，可看到以数字显示的 TCP 和 UCP 连接的端口号及其状态，如图 1-11 所示。

图 1-10　输入 netstat -a -n 命令

图 1-11　TCP 和 UCP 连接的端口号

1.3.4　查看系统注册表信息


微视频

注册表（Registry）是 Microsoft Windows 中的一个重要的数据库，用于存储系统和应用程序的设置信息。通过注册表，用户可以添加、删除、修改系统内的软件配置信息或硬件驱动程序。查看 Windows 系统中注册表信息的操作步骤如下：

Step 01 在 Windows 操作系统中选择“开始”→“运行”选项，打开“运行”对话框，在其中输入命令 regedit，如图 1-12 所示。

Step 02 单击“确定”按钮，打开“注册表编辑器”窗口，在其中查看注册表信息，如图 1-13 所示。

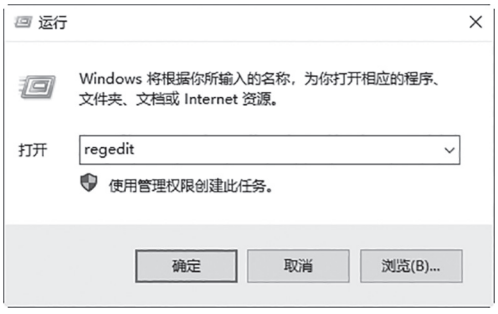

图 1-12 “运行”对话框

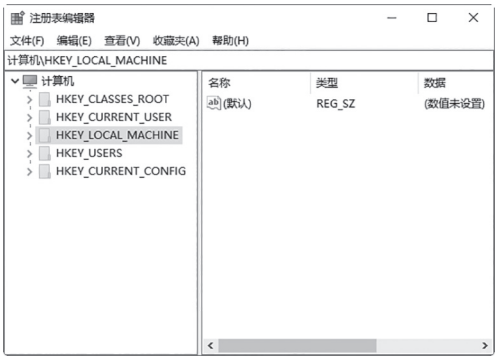

图 1-13 “注册表编辑器”窗口

1.3.5 获取系统进程信息

微视频

在 Windows 10 系统中，可以在“Windows 任务管理器”窗口中获取系统进程，具体的操作步骤如下：

Step01 在 Windows 10 系统中，右击“开始”按钮，在弹出的快捷菜单中选择“任务管理器”选项，如图 1-14 所示。

Step02 打开“任务管理器”窗口，在其中即可看到当前系统正在运行的进程，如图 1-15 所示。

图 1-14 “任务管理器”选项

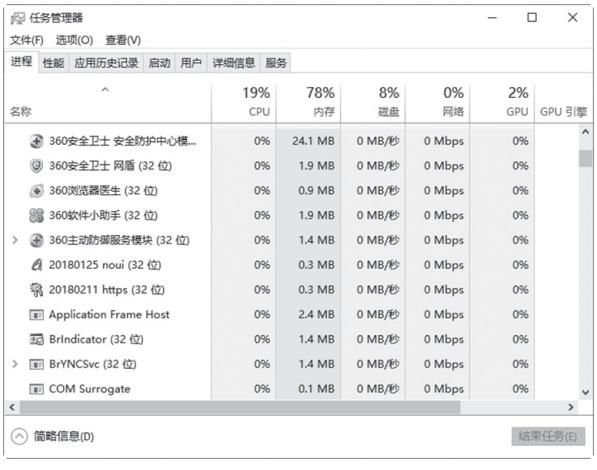

图 1-15 “任务管理器”窗口

提示：通过在 Windows 10 系统中按 Ctrl+Del+Alt 组合键，在打开的工作界面中单击“任务管理器”链接，也可以打开“任务管理器”窗口，在其中查看系统进程。

1.4 实战演练

1.4.1 实战 1：查看进程起始程序

微视频

用户通过查看进程的起始程序，可以来判断哪些是恶意进程。查看进程起始程序的具体操作步骤如下：

Step01 在“命令提示符”窗口中输入查看 svchost 进程起始程序的“Netstat -abnov”命令，如图 1-16 所示。

Step02 按 Enter 键，在反馈的信息中查看每个进程的起始程序或文件列表，然后就可以根据相关的知识来判断是否为病毒或木马发起的程序，如图 1-17 所示。

图 1-16　输入命令

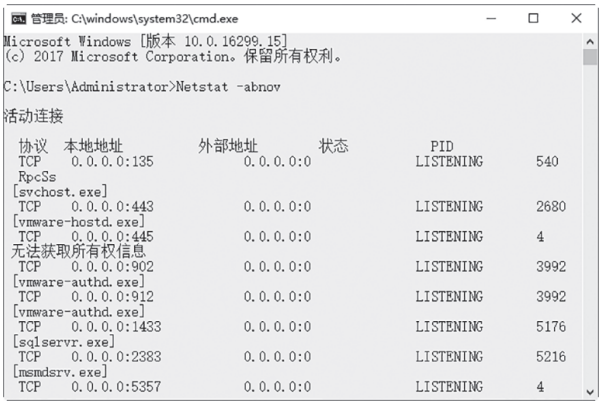

图 1-17　查看进程起始程序

1.4.2　实战 2：显示系统文件的扩展名

微视频

Windows 10 系统默认情况下并不显示文件的扩展名，用户可以通过设置显示文件的扩展名，具体的操作步骤如下：

Step01 右击“开始”按钮，在弹出的快捷菜单中选择“文件资源管理器”选项，打开“文件资源管理器”窗口，如图 1-18 所示。

Step02 选择“查看”选项卡，在打开的功能区域中勾选“显示 / 隐藏”区域中的“文件扩展名”复选框，如图 1-19 所示。

Step03 此时打开一个文件夹，用户便可以看到文件的扩展名，如图 1-20 所示。

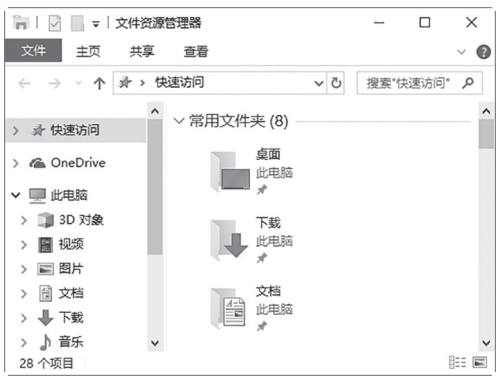

图 1-18　“文件资源管理器”窗口

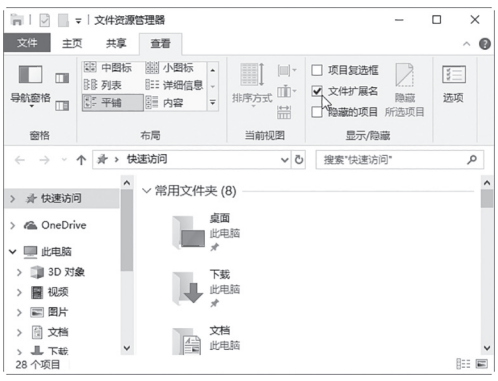

图 1-19　“查看”选项卡

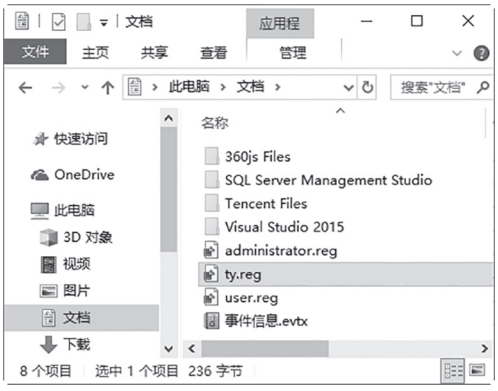

图 1-20　查看文件的扩展名

第 2 章

搭建网络安全测试环境

网络安全测试环境是黑客攻防实战必备的内容，也是网络安全工作者需要了解和掌握的内容。另外，对于黑客初学者来说，在学习过程中需要找到符合条件的目标计算机，并进行模拟攻击，而这些攻击目标并不是初学者能够从网络上搜索到的，这就需要通过搭建网络安全测试环境来解决这个问题。

2.1 认识安全测试环境

所谓安全测试环境就是在已存在的一个系统中，利用虚拟机工具创建出的一个内在的虚拟系统。该系统与外界独立，但与已存在的系统建立有网络关系，在系统中可以进行测试和模拟黑客入侵。

2.1.1 什么是虚拟机软件

虚拟机软件是一种可以在一台计算机上模拟出很多台计算机的软件，而且每台计算机都可以运行独立的操作系统，且不相互干扰，实现了一台计算机运行多个操作系统的功能，同时还可以将这些操作系统连成一个网络。

常见的虚拟机软件有 VMware 和 Virtual PC 两种。VMware 是一款功能强大的桌面虚拟计算机软件，支持在主机和虚拟机之间共享数据，支持第三方预设置的虚拟机和镜像文件，而且安装与设置都非常简单。Virtual PC 具有最新的 Microsoft 虚拟化技术。用户可以使用这款软件在同一台计算机上同时运行多个操作系统。操作起来非常简单，用户只需单击一下，便可直接在计算机上的虚拟出 Windows 环境，并在该环境中可以同时运行多个应用程序。

2.1.2 什么是虚拟系统

虚拟系统就是在已有的操作系统的基础上，安装一个新的操作系统或者虚拟出系统本身的文件，该操作系统允许在不重启计算机的基础上进行切换。

创建虚拟系统的好处有以下几种。

- 虚拟技术是一种调配计算机资源的方法，可以更有效、更灵活地提供和利用计算机资源，降低成本，节省开支。
- 在虚拟环境里更容易实现程序自动化，有效地减少了测试要求和应用程序的兼容性问题，并在系统崩溃时更容易实施恢复操作。
- 虚拟系统允许跨系统进行安装，如在 Windows 10 的基础上可以安装 Linux 操作系统。

2.2　下载与安装虚拟机软件

对于网络安全初学者，使用虚拟机构建网络安全测试环境是一个非常好的选择，这样既可以快速搭建测试环境，还可以快速还原之前快照，避免因错误操作造成系统崩溃。

2.2.1　下载虚拟机软件


微视频

虚拟机使用之前，需要从官网上下载虚拟机软件 VMware，具体的操作步骤如下：

Step01 使用浏览器打开虚拟机官方网站 https://my.vmware.com/cn.html，进入虚拟机官网页面，如图 2-1 所示。

图 2-1　虚拟机官网页面

Step02 这里需要注册一个账号，用户可以注册一个账号，VMware 支持中文页面注册。注册完成后，进入所有下载页面，并切换到“所有产品”选项卡，如图 2-2 所示。

Step03 在下拉页面找到“VMware Workstation Pro”对应选项，单击右侧的“查看下载组件”超链接，如图 2-3 所示。

图 2-2　“所有产品”选项卡

图 2-3　“查看下载组件”超链接

Step04 进入 VMware 下载页面，在其中选择 Windows 版本，单击“立即下载”超链接，如图 2-4 所示。

Step05 打开“新建下载任务”对话框，单击“下载”按钮进行下载，如图 2-5 所示。

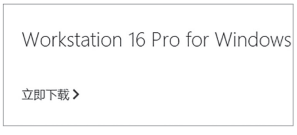

图 2-4　VMware 下载页面

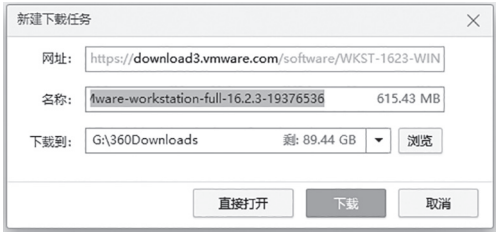

图 2-5　“新建下载任务”对话框


微视频

2.2.2 安装虚拟机软件

虚拟机软件下载完成后，接下来就可以安装虚拟机软件了，这里下载的是目前的最新版本“VMware-workstation-full-16.2.3-19376536.exe”，用户可根据实际情况选择相应的版本下载即可。安装虚拟机的具体操作步骤如下：

Step01 双击下载的 VMware 安装软件，进入“欢迎使用 VMware Workstation Pro 安装向导”窗口，如图 2-6 所示。

Step02 单击“下一步”按钮，进入“最终用户许可协议”窗口，勾选“我接受许可协议中的条款”复选框，如图 2-7 所示。

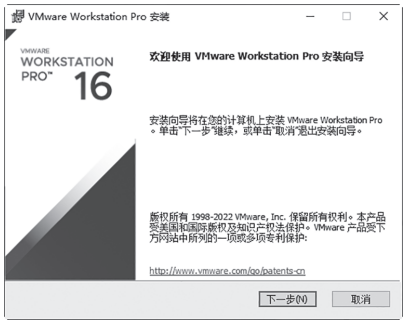

图 2-6 “安装向导”窗口

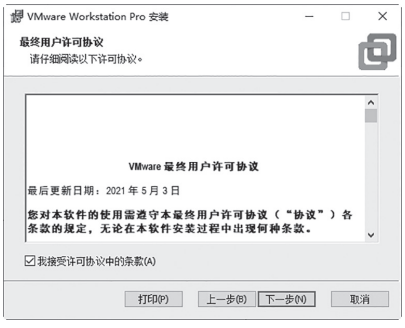

图 2-7 “最终用户许可协议”窗口

Step03 单击“下一步”按钮，进入“自定义安装”窗口，在其中可以更改安装路径，也可以保持默认，如图 2-8 所示。

Step04 单击“下一步”按钮，进入“用户体验设置”窗口，这里选用系统默认设置，如图 2-9 所示。

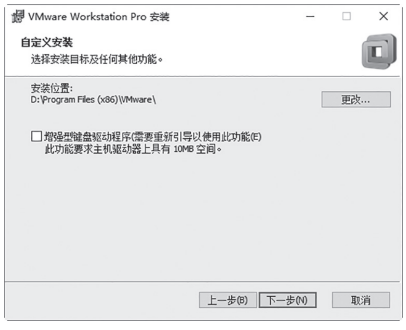

图 2-8 “自定义安装”窗口

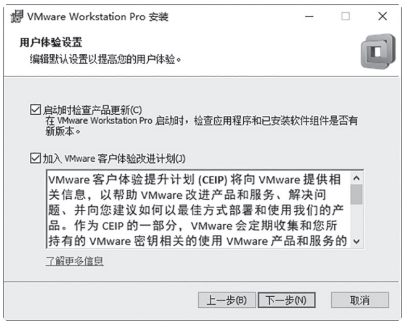

图 2-9 “用户体验设置”窗口

Step05 单击“下一步”按钮，进入“快捷方式”窗口，在其中可以创建用户快捷方式，这里可以保持默认设置，如图 2-10 所示。

Step06 单击“下一步”按钮，进入“已准备好安装 VMware Workstation Pro”窗口，开始准备安装虚拟机软件，如图 2-11 所示。

Step07 单击“安装”按钮，等待一段时间后虚拟机便可以安装完成，并进入“VMware Workstation Pro 安装向导已完成”窗口，单击“完成”按钮，关闭虚拟机安装向导，如图 2-12 所示。

Step08 虚拟机安装完成后，要重新启动系统后才可以使用虚拟机。至此，便完成了 VMware 虚拟机的安装，如图 2-13 所示。

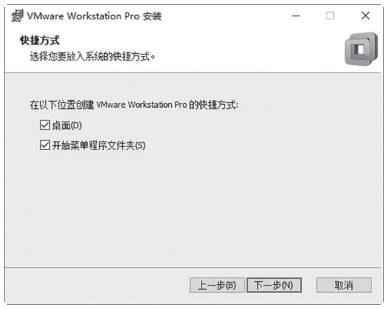

图 2-10　“快捷方式”窗口

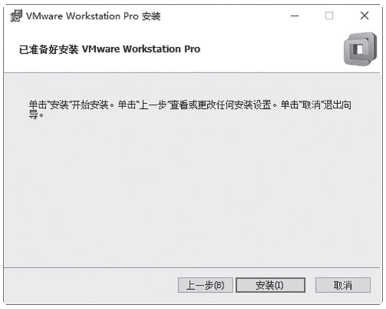

图 2-11　“已准备好安装 VMware Workstation Pro”窗口

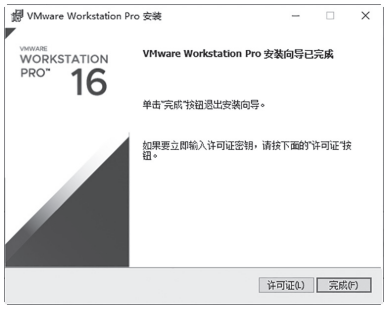

图 2-12　“VMware Workstation Pro 安装向导已完成”窗口

图 2-13　重新启动系统

2.3　安装虚拟机软件系统

组装好计算机以后需要给它安装一个系统，这样计算机才可以正常工作，虚拟机也一样，同样需要安装一个操作系统，如 Windows、Linux 等，这样才能使用虚拟机创建的环境来实现网络安全测试。

2.3.1　安装 Windows 操作系统

微视频

在虚拟机中安装 Windows 操作系统是搭建网络安全测试环境的重要步骤，所有准备工作就绪后，接下来就可以在虚拟机中安装 Windows 操作系统了，具体的操作步骤如下：

Step 01 双击桌面安装好的 VMware 虚拟机图标，打开 VMware 虚拟机软件，如图 2-14 所示。

Step 02 单击“创建新的虚拟机”按钮，进入“新建虚拟机向导”对话框，选中“自定义”单选按钮，如图 2-15 所示。

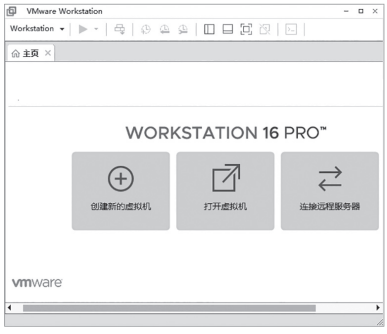

图 2-14　VMware 虚拟机软件

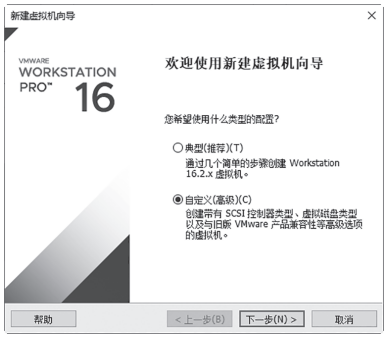

图 2-15　“新建虚拟机向导”对话框

Step03 单击“下一步”按钮，进入“选择虚拟机硬件兼容性”对话框，在其中设置虚拟机的硬件兼容性，这里选用默认设置，如图 2-16 所示。

Step04 单击“下一步”按钮，进入“安装客户机操作系统”对话框，在其中选中“稍后安装操作系统”单选按钮，如图 2-17 所示。

图 2-16 “选择虚拟机硬件兼容性”对话框

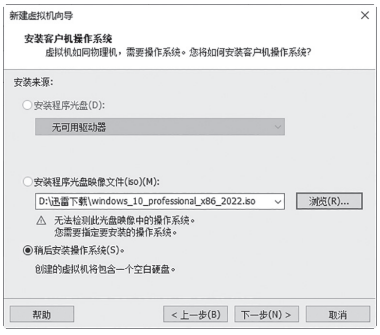

图 2-17 “安装客户机操作系统”对话框

Step05 单击“下一步”按钮，进入“选择客户机操作系统”对话框，在其中选中“Microsoft Windows（W）”单选按钮，如图 2-18 所示。

Step06 单击“版本”下方的下拉按钮，在弹出的下拉列表中选择“Windows 10 x64”系统版本，这里的系统版本与主机系统版本无关，可以自由选择，如图 2-19 所示。

图 2-18 “选择客户机操作系统”对话框

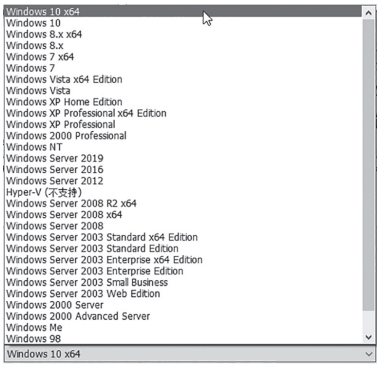

图 2-19 选择系统版本

Step07 单击“下一步”按钮，进入“命名虚拟机”对话框，在“虚拟机名称”文本框中输入虚拟机名称，在“位置”中选择一个存放虚拟机的磁盘位置，如图 2-20 所示。

Step08 单击“下一步”按钮，进入“处理器配置”对话框，在其中选择处理器数量，一般普通计算机都是单处理，所以这里不用设置，处理器内核数量可以根据实际处理器内核数量设置，如图 2-21 所示。

Step09 单击“下一步”按钮，进入“此虚拟机的内存”对话框，根据实际主机进行设置，最少内存不要低于 768MB，这里选择 1024MB 也就是 1GB 内存，如图 2-22 所示。

Step10 单击“下一步”按钮，进入“网络类型”对话框，选中“使用网络地址转换”单选按钮，如图 2-23 所示。

Step11 单击“下一步”按钮，进入“选择 I/O 控制器类型”对话框，这里选中 LSI Logic SAS 单选按钮，如图 2-24 所示。

Step12 单击“下一步”按钮，进入“选择磁盘类型”对话框，选中 NVMe 单选按钮，如图 2-25 所示。

图 2-20　“命名虚拟机”对话框

图 2-21　“处理器配置”对话框

图 2-22　“此虚拟机的内存”对话框

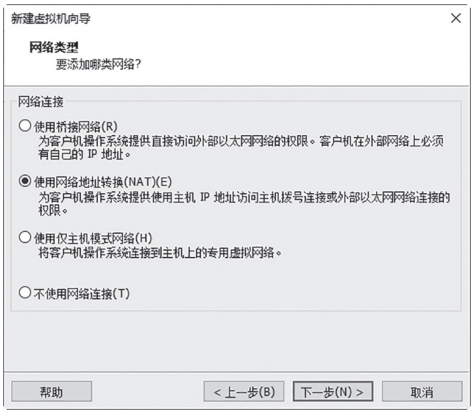

图 2-23　“网络类型”对话框

图 2-24　“选择 I/O 控制器类型”对话框

图 2-25　“选择磁盘类型”对话框

Step 13 单击“下一步”按钮，进入“选择磁盘”对话框，选中“创建新虚拟磁盘”单选按钮，如图 2-26 所示。

Step 14 单击“下一步”按钮，进入“指定磁盘容量”对话框，这里最大磁盘大小设置 60GB 空间即可，选中“将虚拟磁盘拆分成多个文件”单选按钮，如图 2-27 所示。

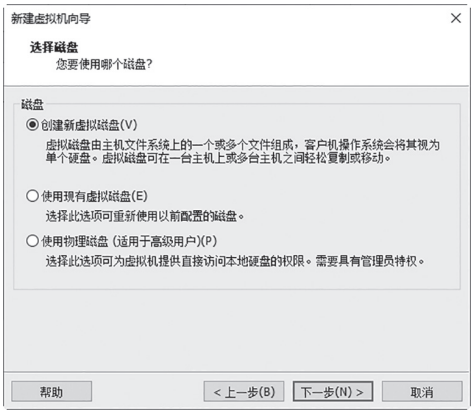

图 2-26 “选择磁盘”对话框

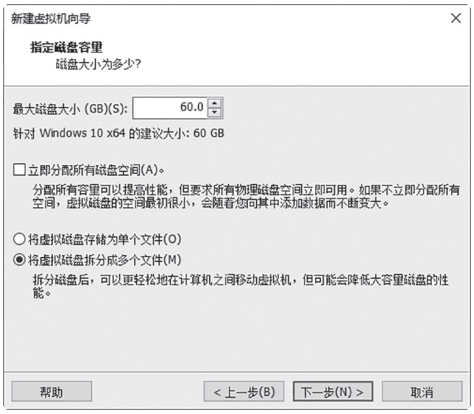

图 2-27 “指定磁盘容量”对话框

Step15 单击“下一步”按钮，进入“指定磁盘文件”对话框，这里保持默认即可，如图 2-28 所示。

Step16 单击“下一步”按钮，进入“已准备好创建虚拟机”对话框，如图 2-29 所示。

图 2-28 “指定磁盘文件”对话框

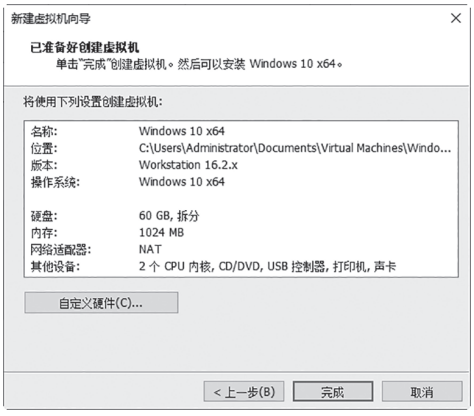

图 2-29 “已准备好创建虚拟机”对话框

Step17 单击“完成”按钮，至此，便创建了一个新的虚拟机，如图 2-30 所示。这相当于组装了一台裸机，其中的硬件配置，可以根据实际需求进行更改。

Step18 单击“开启此虚拟机”链接，稍等片刻，Windows 10 操作系统进入安装过渡窗口，如图 2-31 所示。

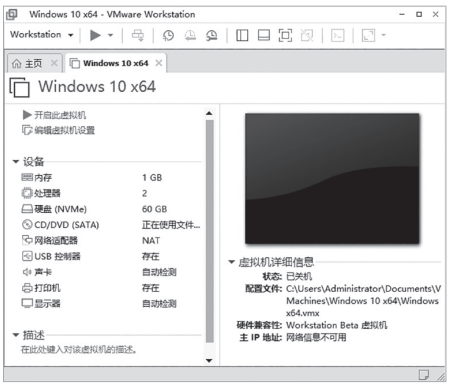

图 2-30 创建新虚拟机

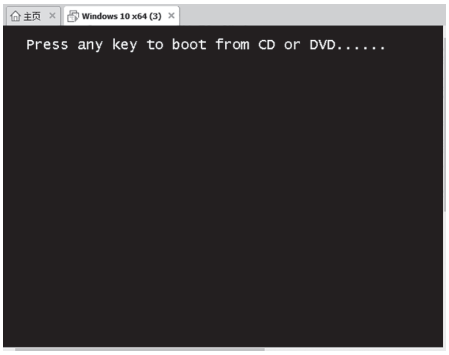

图 2-31 安装过渡窗口

Step19 按任意键即可打开 Windows 安装程序运行界面，安装程序将开始自动复制安装的文件并准备要安装的文件，如图 2-32 所示。

Step20 安装完成后，将显示安装后的操作系统界面。至此，整个虚拟机的设置创建即可完成，安装的虚拟操作系统以文件的形式存放在硬盘之中，如图 2-33 所示。

图 2-32　准备要安装的文件

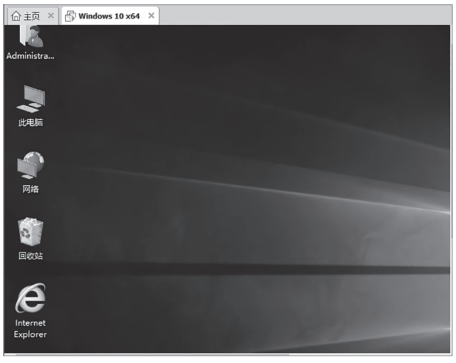

图 2-33　操作系统界面

2.3.2　安装 VMware Tools 工具

众所周知，本地计算机安装好操作系统之后，还需要安装各种驱动，如显卡、网卡、显卡等驱动，作为虚拟机也需要安装一定的虚拟工具才能正常运行。安装 VMware Tools 工具的操作步骤如下：

Step01 启动虚拟机进入虚拟系统，然后按 Ctrl+Alt 组合键，切换到真实的计算机系统，如图 2-34 所示。

注意：如果是用 ISO 文件安装的操作系统，最好重新加载该安装文件并重新启动系统，这样系统就能自动找到 VMware Tools 的安装文件。

Step02 执行“虚拟机”→“安装 VMware Tools”命令，此时系统将自动弹出安装文件，如图 2-35 所示。

Step03 安装文件启动之后，将会弹出“欢迎使用 VMware Tools 的安装向导”窗口，如图 2-36 所示。

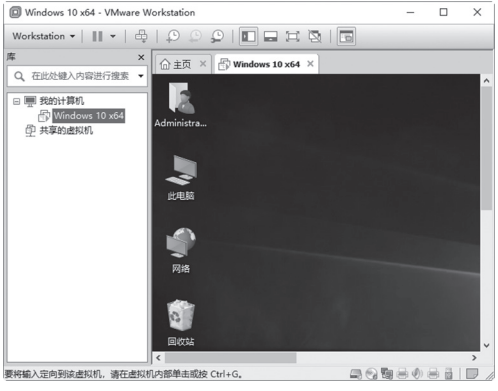

图 2-34　进入虚拟系统

图 2-35　“安装 VMware Tools”命令

图 2-36　“安装向导”窗口

Step04 单击“下一步”按钮，进入“选择安装类型”窗口，根据实际情况选择相应的安装类型，选中“典型安装”单选按钮，如图 2-37 所示。

Step05 单击“下一步”按钮，进入“已准备好安装 VMware Tools”窗口，如图 2-38 所示。

图 2-37 “选择安装类型”窗口

图 2-38 “已准备好安装 VMware Tools”窗口

Step06 单击“安装”按钮，进入“正在安装 VMware Tools”窗口，在其中显示了 VMware Tools 工具的安装状态，如图 2-39 所示。

Step07 安装完成后，进入“VMware Tools 安装向导已完成”窗口，如图 2-40 所示。

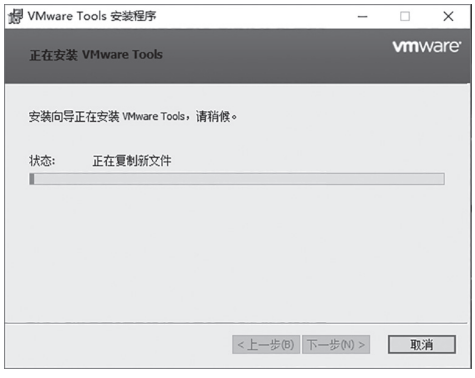

图 2-39 “正在安装 VMware Tools”窗口

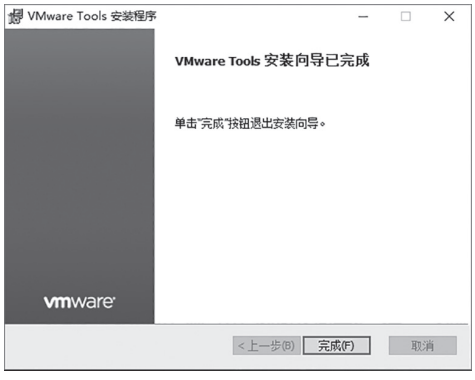

图 2-40 “VMware Tools 安装向导已完成”窗口

Step08 单击“完成”按钮，弹出一个信息提示框，要求必须重新启动系统，这样对 VMware Tools 进行的配置更改才能生效，如图 2-41 所示。

Step09 单击“是”按钮，系统重新启动。虚拟系统重新启动之后即可发现虚拟机工具已经成功安装，再次选择“虚拟机”菜单命令，可以看到“安装 VMware Tools”菜单命令变成了“重新安装 VMware Tools”菜单命令，如图 2-42 所示。

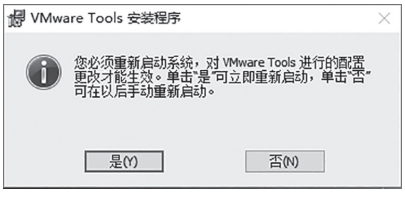

图 2-41 信息提示框

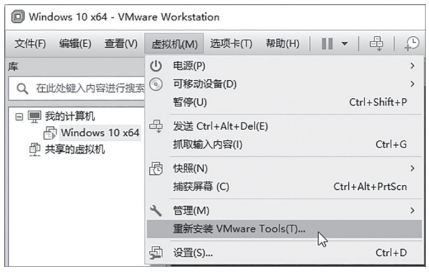

图 2-42 “重新安装 VMware Tools”菜单命令

2.4　实战演练

2.4.1　实战 1：关闭开机多余启动项目


微视频

在计算机启动的过程中，自动运行的程序称为开机启动项，有时一些木马程序会在开机时运行，用户可以通过关闭开机启动项来提高系统安全性，具体的操作步骤如下：

Step01 按 Ctrl+Alt+Del 组合键，打开如图 2-43 所示的界面。

Step02 选择“任务管理器”选项，打开“任务管理器”窗口，如图 2-44 所示。

图 2-43　“任务管理器”选项

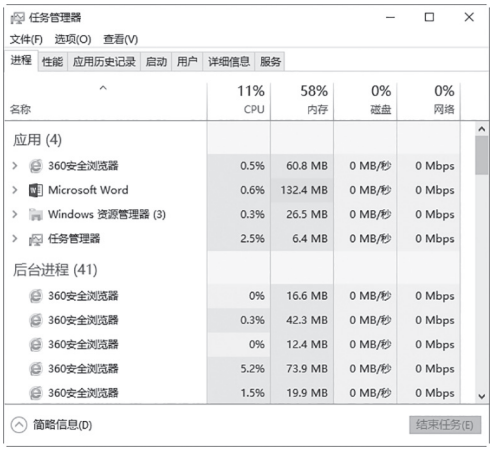

图 2-44　“任务管理器”窗口

Step03 选择“启动”选项卡，进入“启动”界面，在其中可以看到系统中的开机启动项列表，如图 2-45 所示。

Step04 选择开机启动项列表中需要禁用的启动项，单击“禁用”按钮即可禁止该启动项开机自启，如图 2-46 所示。

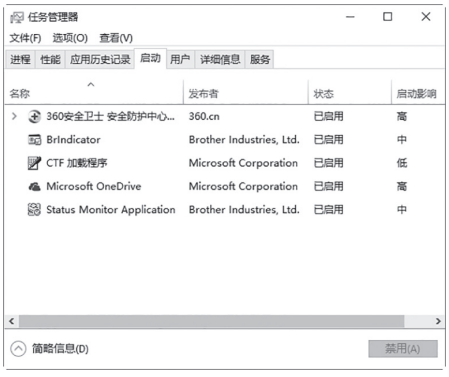

图 2-45　“启动”选项卡

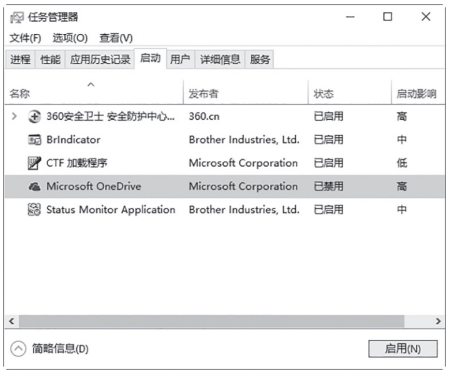

图 2-46　禁止开机启动项

2.4.2　实战 2：诊断和修复网络不通的问题


微视频

当计算机不能上网时，说明计算机与网络连接不通，这时就需要诊断和修复网络，具体的操作步骤如下：

Step01 打开“网络连接”窗口，右击需要诊断的网络图标，在弹出的快捷菜单中选择“诊断”选项，打开“Windows 网络诊断”对话框，并显示网络诊断的进度，如图 2-47 所示。

Step02 诊断完成后，将会在下方的窗格中显示诊断的结果，如图 2-48 所示。

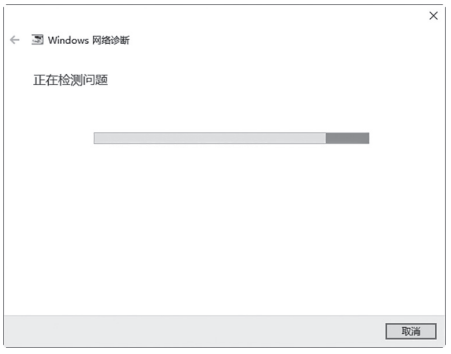

图 2-47　显示网络诊断的进度

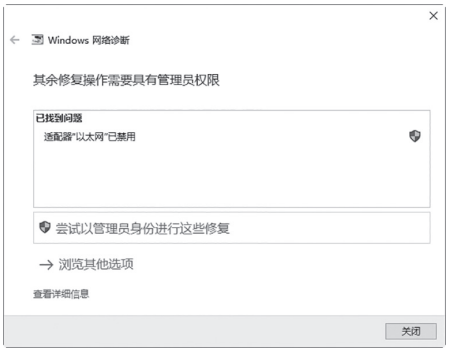

图 2-48　显示诊断的结果

Step03 单击“尝试以管理员身份进行这些修复”连接，开始对诊断出来的问题进行修复，如图 2-49 所示。

Step04 修复完毕后，会给出修复的结果，提示用户疑难解答已经完成，并在下方显示已修复信息提示，如图 2-50 所示。

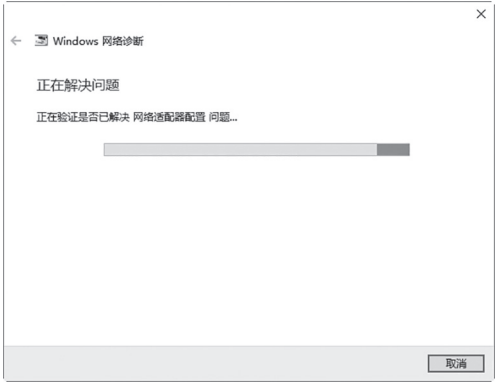

图 2-49　修复网络问题

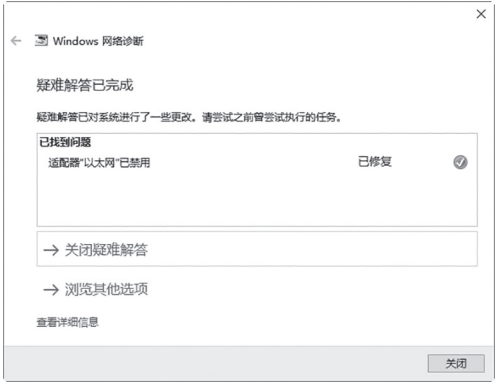

图 2-50　显示已修复信息

第 3 章

认识 DOS 窗口与 DOS 命令

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，有必要了解一些计算机中的基础知识，本章就来认识 Windows 系统中的 DOS 窗口与 DOS 命令。

3.1 认识 Windows 10 系统中的 DOS 窗口

Windows 10 操作系统中的 DOS 窗口，也被称为“命令提示符”窗口，该窗口主要以图形化界面显示，用户可以很方便地进入 DOS 命令窗口并对窗口中的命令行进行相应的编辑操作。

3.1.1 通过菜单进入 DOS 窗口


微视频

Windows 10 的图形化界面缩短了人与机器之间的距离，通过使用菜单可以很方便地进入 DOS 窗口，具体的操作步骤如下：

Step 01 右击桌面上的“开始”按钮，在弹出的快捷菜单中选择 Windows →“命令提示符”选项，如图 3-1 所示。

Step 02 弹出“管理员 : 命令提示符”窗口，在其中可以执行相关 DOS 命令，如图 3-2 所示。

图 3-1 “命令提示符”选项

图 3-2 “管理员 : 命令提示符”窗口

3.1.2 通过“运行”对话框进入 DOS 窗口


微视频

除通过菜单进入 DOS 窗口外，用户还可以通过“运行”对话框进入 DOS 窗口，具体的操作步骤如下：

Step 01 在 Windows 10 操作系统中，右击桌上的“开始”按钮，在弹出的快捷菜单中选择“运行”选项，打开“运行”对话框，在其中输入 cmd 命令，如图 3-3 所示。

Step02 单击“确定”按钮，即可进入 DOS 窗口，如图 3-4 所示。

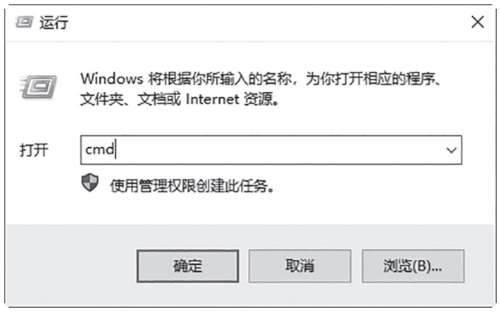

图 3-3 “运行”对话框

图 3-4 DOS 窗口

微视频

3.1.3 通过浏览器访问 DOS 窗口

浏览器和“命令提示符”窗口关系密切，用户可以直接在浏览器中访问 DOS 窗口。下面以在 Windows 10 操作系统下访问 DOS 窗口为例，具体的方法为：在 Microsoft Edge 浏览器的地址栏中输入“c:\Windows\system32\cmd.exe”，如图 3-5 所示。按 Enter 键后即可进入 DOS 运行窗口，如图 3-6 所示。

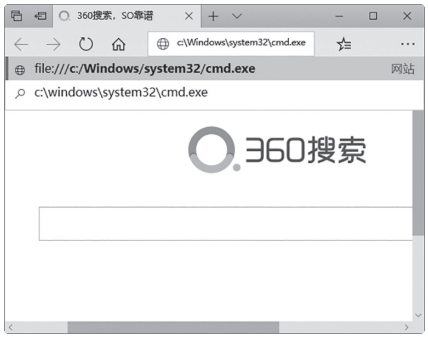

图 3-5 Microsoft Edge 浏览器

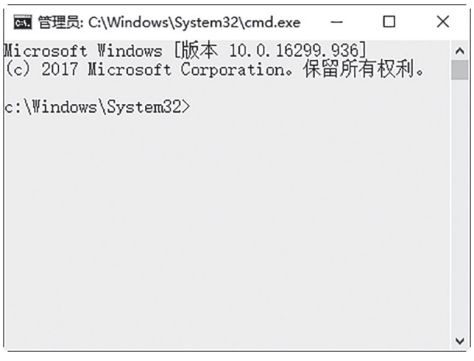

图 3-6 DOS 窗口

注意：在输入地址时，一定要输入全路径，否则 Windows 将无法打开命令提示符窗口。

微视频

3.1.4 编辑“命令提示符”窗口中的代码

图 3-7 “标记”选项

当在 Windows 10 中启动命令行，就会弹出相应的命令行窗口，在其中显示当前的操作系统的版本号，并把当前用户默认为当前提示符。在使用命令行时可以对命令行进行复制、粘贴等操作，具体的操作步骤如下：

Step01 右击“命令提示符”窗口标题栏，将弹出一个快捷菜单。在这里可以对当前窗口进行各种操作，如移动、最大化、最小化、编辑等。选择此菜单中的“编辑”命令，在显示的子菜单中选择“标记”选项，如图 3-7 所示。

Step02 移动鼠标，选择要复制的内容，可以直接按

Enter 键复制该命令行，也可以通过选择“编辑”→“复制”选项来实现，如图 3-8 所示。

Step03 在需要粘贴该命令行的位置处单击鼠标右键，完成粘贴操作，或者右击“命令提示符”窗口的菜单栏，在弹出的快捷菜单中选择“编辑”→“粘贴”选项，也可完成粘贴操作，如图 3-9 所示。

图 3-8　“复制”选项

图 3-9　“粘贴”选项

提示：如果是想再使用上一条命令，可以按 F3 键调用，要实现复杂的命令行编辑功能，可以借助于 DOSKEY 命令。

3.1.5　自定义“命令提示符”窗口的风格

“命令提示符”窗口的风格不是一成不变的，用户可以通过“属性”菜单选项对“命令提示符”窗口的风格进行自定义设置，如设置窗口的颜色、字体的样式等。自定义“命令提示符”窗口的风格的操作步骤如下：

Step01 单击“命令提示符”窗口左上角的图标，在弹出的菜单中选择“属性”选项，打开“命令提示符属性”对话框，如图 3-10 所示。

Step02 选择“颜色”选项卡，在其中可以对相关选项进行颜色设置。选中“屏幕文字”单选按钮，可以设置屏幕文字的显示颜色，这里选择“黑色”，如图 3-11 所示。

图 3-10　“选项”选项卡

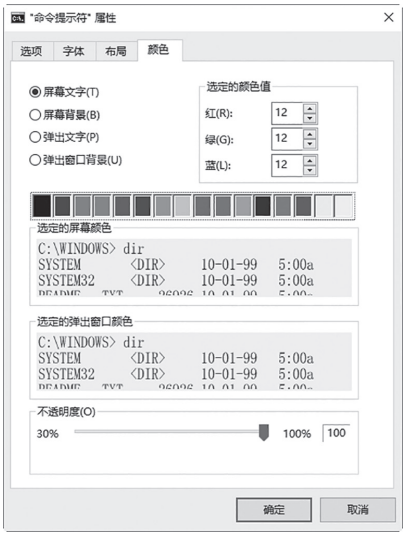

图 3-11　“颜色”选项卡

Step03 选中“屏幕背景”单选按钮，可以设置屏幕背景的显示颜色，这里选择“灰色”，如图 3-12 所示。

Step04 选中“弹出文字”单选按钮，可以设置弹出窗口文字的显示颜色，这里设置蓝色颜色值为 180，如图 3-13 所示。

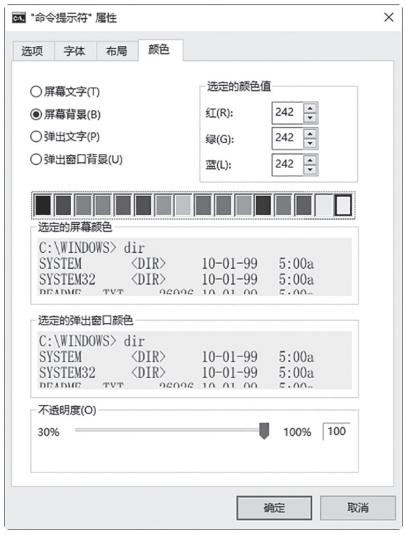

图 3-12　设置屏幕背景颜色

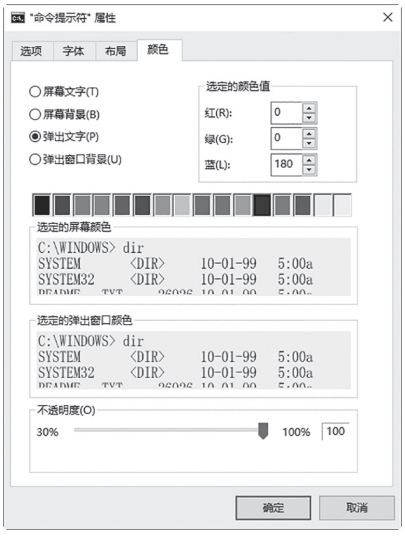

图 3-13　设置文字颜色

Step05 选中“弹出窗口背景”单选按钮，可以设置弹出窗口的背景显示颜色，这里设置颜色值为 125，如图 3-14 所示。

Step06 设置完毕后单击“确定”按钮，保存设置，“命令提示符”窗口的风格如图 3-15 所示。

图 3-14　设置弹出窗口背景颜色

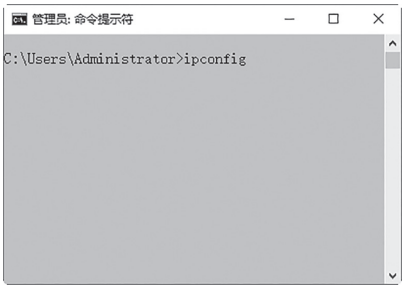

图 3-15　自定义显示风格

3.2　黑客常用 DOS 命令实战

熟练掌握一些 DOS 命令的应用是一名黑客的“基本功”，通过这些 DOS 命令可以帮助计算机用户追踪黑客的踪迹。

3.2.1　切换当前目录路径的 cd 命令


微视频

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，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根目录。

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如下：

Step01 在“命令提示符”窗口中输入 cd c:\ 命令，按 Enter 键，将目录切换为 C:\，如图 3-16 所示。

Step02 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，如图 3-17 所示。

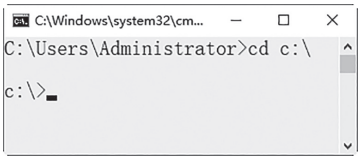

图 3-16　目录切换到 C

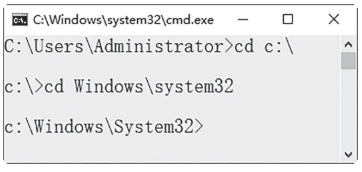

图 3-17　切换到 C 盘子目录

Step03 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，如图 3-18 所示。

Step04 如果想返回根目录，则可以在“命令提示符”窗口中输入 cd\ 命令，按 Enter 键即可，如图 3-19 所示。

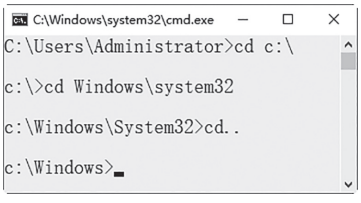

图 3-18　返回上一级目录

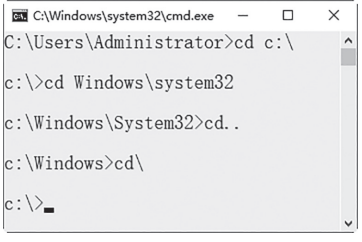

图 3-19　返回根目录

3.2.2　列出磁盘目录文件的 dir 命令


微视频

dir 命令的作用是列出磁盘上所有的或指定的文件目录，可以显示的内容包含卷标、文件名、文件大小、文件建立日期和时间、目录名、磁盘剩余空间等。dir 命令的格式如下：

```
dir [盘符][路径][文件名][/P][/W][/A：属性]
```

其中各个参数的作用如下。

（1）/P：当显示的信息超过一屏时暂停显示，直至按任意键才继续显示。

（2）/W：以横向排列的形式显示文件名和目录名，每行 5 个（不显示文件大小、建立日期和时间）。

（3）/A：属性：仅显示指定属性的文件，无此参数时，dir 显示除系统和隐含文件外的所有文件。可指定为以下几种形式。

① /A:S：显示系统文件的信息。

图 3-20　Administrator 目录下的文件列表

② /A:H：显示隐含文件的信息。

③ /A:R：显示只读文件的信息。

④ /A:A：显示归档文件的信息。

⑤ /A:D：显示目录信息。

使用 dir 命令查看磁盘中的资源，具体的操作步骤如下：

Step01 在“命令提示符”窗口中输入 dir 命令，按 Enter 键，可查看当前目录下的文件列表，如图 3-20 所示。

Step02 在“命令提示符”窗口中输入 dir d:/ a:d 命令，按 Enter 键，可查看 D 盘下所有文件的目录，如图 3-21 所示。

Step03 在“命令提示符”窗口中输入 dir c:\windows /a:h 命令，按 Enter 键，可列出 c:\windows 目录下的隐藏文件，如图 3-22 所示。

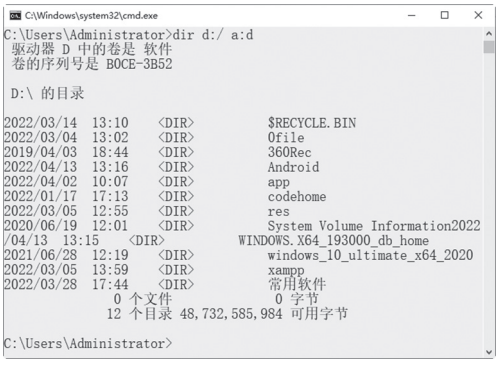

图 3-21　D 盘下的文件列表

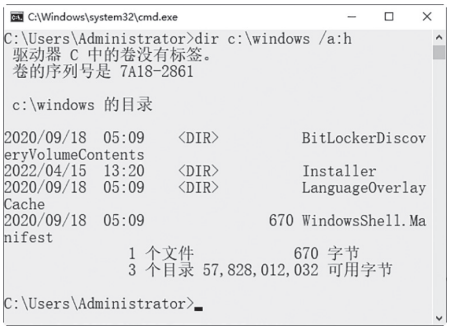

图 3-22　C 盘下的隐藏文件


微视频

3.2.3　检查计算机连接状态的 ping 命令

ping 命令是协议 TCP/IP 中最为常用的命令之一，主要用来检查网络是否通畅或者网络连接的速度。对于一名计算机用户来说，ping 命令是第一个必须掌握的 DOS 命令。在“命令提示符”窗口中输入 ping /?，可以得到这条命令的帮助信息，如图 3-23 所示。

图 3-23　ping 命令帮助信息

使用 ping 命令对计算机的连接状态进行测试的具体操作步骤如下：

Step01 使用 ping 命令来判断计算机的操作系统类型。在“命令提示符”窗口中输入 ping 192.168.3.9 命令，运行结果如图 3-24 所示。

Step02 在“命令提示符”窗口中输入 ping 192.168.3.9 -t -l 128 命令，可以不断向某台主机发出大量的数据包，如图 3-25 所示。

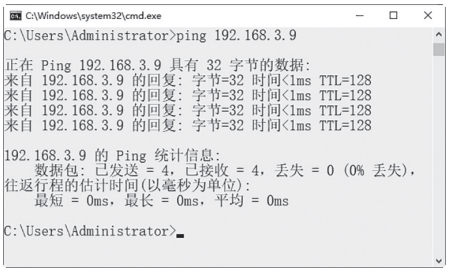

图 3-24　判断计算机的操作系统类型

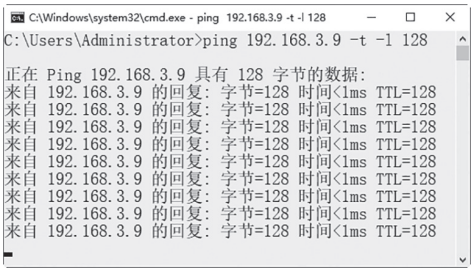

图 3-25　发出大量数据包

Step03 判断本台计算机是否与外界网络连通。在“命令提示符”窗口中输入 ping www.baidu.com 命令，其运行结果如图 3-26 所示，图中说明本台计算机与外界网络连通。

Step04 解析某 IP 地址的计算机名。在“命令提示符”窗口中输入 ping -a 192.168.3.9 命令，其运行结果如图 3-27 所示，可知这台主机的名称为 SD-20220314SOIE。

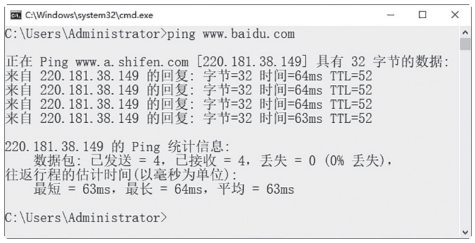

图 3-26　网络连通信息

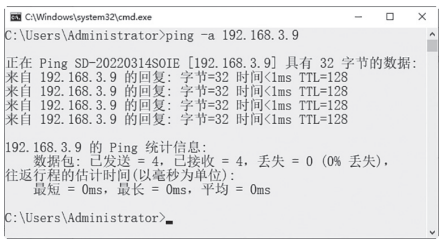

图 3-27　解析某 IP 地址的计算机名

3.2.4　查询网络状态与共享资源的 net 命令


微视频

使用 net 命令可以查询网络状态、共享资源及计算机所开启的服务等，该命令的语法格式信息如下：

```
NET [ ACCOUNTS | COMPUTER | CONFIG | CONTINUE | FILE | GROUP | HELP | HELPMSG |
LOCALGROUP | NAME | PAUSE | PRINT | SEND | SESSION | SHARE | START | STATISTICS |
STOP | TIME | USE | USER | VIEW ]
```

查询本台计算机开启哪些 Windows 服务的具体操作步骤如下：

Step01 使用 net 命令查看网络状态。打开“命令提示符”窗口，输入 net start 命令，如图 3-28 所示。

Step02 按 Enter 键，在打开的“命令提示符”窗口中可以显示计算机所启动的 Windows 服务，如图 3-29 所示。

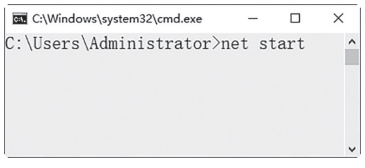

图 3-28　输入 net start 命令

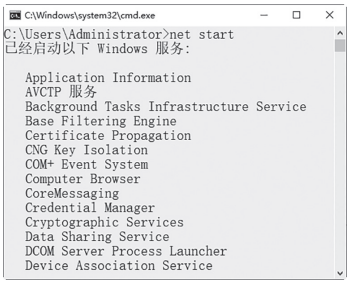

图 3-29　计算机所启动的 Windows 服务


微视频

3.2.5 显示网络连接信息的 netstat 命令

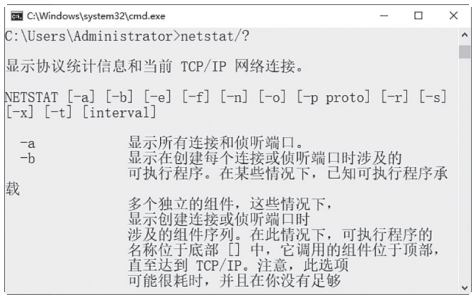

图 3-30 netstat 命令帮助信息

netstat 命令主要用来显示网络连接的信息，包括显示活动的 TCP 连接、路由器和网络接口信息，是一个监控 TCP/IP 网络非常有用的工具，可以让用户了解系统中目前都有哪些网络连接正常。

在“命令提示符”窗口中输入 netstat/? 命令，可以得到这条命令的帮助信息，如图 3-30 所示。

该命令的语法格式信息如下：

```
    NETSTAT [- a] [-b] [-e] [-n] [-o] [-p proto] [-r] [-s] [-v] [interval]
```

其中比较重要的参数的含义如下。

- -a：显示所有连接和监听端口。
- -n：以数字形式显示地址和端口号。

使用 netstat 命令查看网络连接的具体操作步骤如下：

Step01 打开“命令提示符”窗口，在其中输入 netstat -n 或 netstat 命令，按 Enter 键，可查看服务器活动的 TCP/IP 连接，如图 3-31 所示。

Step02 在“命令提示符”窗口中输入 netstat -r 命令，按 Enter 键，可查看本机的路由信息，如图 3-32 所示。

图 3-31 服务器活动的 TCP/IP 连接

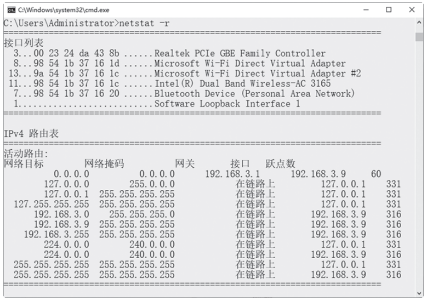

图 3-32 查看本机路由信息

Step03 在“命令提示符”窗口中输入 netstat -a 命令，按 Enter 键，可查看本机所有活动的 TCP 连接，如图 3-33 所示。

Step04 在“命令提示符”窗口中输入 netstat -n -a 命令，按 Enter 键，可显示本机所有连接的端口及其状态，如图 3-34 所示。

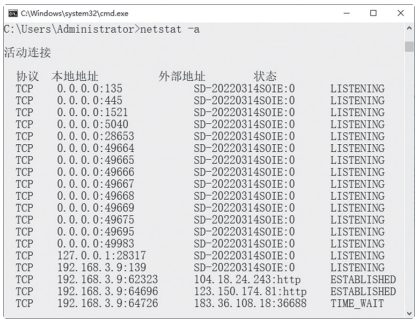

图 3-33 查看本机活动的 TCP 连接

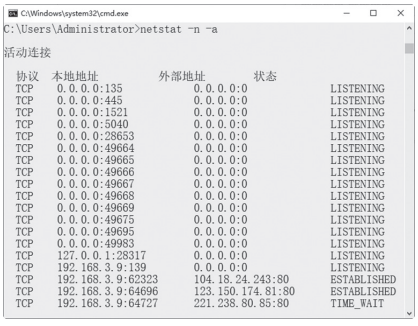

图 3-34 查看本机连接的端口及其状态

3.2.6　检查网络路由节点的 tracert 命令


微视频

使用 tracert 命令可以查看网络中路由节点信息，最常见的使用方法是在 tracert 命令后追加一个参数，表示检测和查看连接当前主机经历了哪些路由节点，适合用于大型网络的测试。该命令的语法格式信息如下：

```
tracert [-d] [-h MaximumHops] [-j Hostlist] [-w Timeout] [TargetName]
```

其中各个参数的含义如下。

- -d：防止解析目标主机的名字，可以加速显示 tracert 命令结果。
- -h MaximumHops：指定搜索到目标地址的最大跳跃数，默认为 30 个跳跃点。
- -j Hostlist：按照主机列表中的地址释放源路由。
- -w Timeout：指定超时时间间隔，默认单位为毫秒。
- TargetName：指定目标计算机。

如果想查看 www.baidu.com 的路由与局域网络连接情况，可在“命令提示符”窗口中输入 tracert www.baidu.com 命令，按 Enter 键，其显示结果如图 3-35 所示。

图 3-35　查看网络中路由节点信息

3.2.7　显示主机进程信息的 Tasklist 命令


微视频

Tasklist 命令用来显示运行在本地或远程计算机上的所有进程，带有多个执行参数。Tasklist 命令的格式如下：

```
Tasklist [/S system [/U username [/P [password]]]] [/M [module] | /SVC | /V] [/FI filter] [/FO format] [/NH]
```

其中各个参数的作用如下。

- /S system：指定连接到的远程系统。
- /U username：指定使用哪个用户执行这个命令。
- /P [password]：为指定的用户指定密码。
- /M [module]：列出调用指定的 DLL 模块的所有进程。如果没有指定模块名，显示每个进程加载的所有模块。
- /SVC：显示每个进程中的服务。
- /V：显示详细信息。
- /FI filter：显示一系列符合筛选器指定的进程。
- /FO format：指定输出格式，有效值有 TABLE、LIST、CSV。
- /NH：指定输出中不显示栏目标题。只对 TABLE 和 CSV 格式有效。

利用 Tasklist 命令可以查看本机中的进程，还可以查看每个进程提供的服务。下面将介绍使用 Tasklist 命令的具体操作步骤：

Step01 在“命令提示符”中输入 Tasklist 命令，按 Enter 键即可显示本机的所有进程，如图 3-36 所示。在显示结果中可以看到映像名称、PID、会话名、会话 # 和内存使用 5 部分。

Step02 Tasklist 命令不但可以查看系统进程，还可以查看每个进程提供的服务。例如，查看本机进程 svchost.exe 提供的服务，在“命令提示符”窗口中输入 Tasklist /svc 命令即可，如图 3-37 所示。

图 3-36　查看本机进程

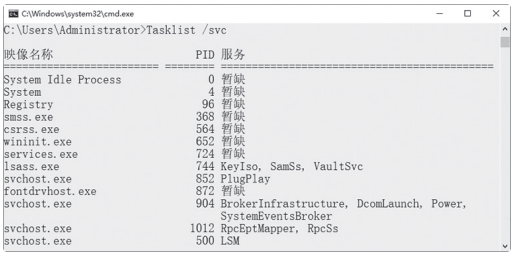

图 3-37　查看本机进程 svchost.exe 提供的服务

Step 03 要查看本地系统中哪些进程调用了 shell32.dll 模块文件，只需在“命令提示符”窗口中输入 Tasklist /m shell32.dll 命令即可显示这些进程的列表，如图 3-38 所示。

Step 04 使用筛选器可以查找指定的进程，在“命令提示符”窗口中输入 TASKLIST /FI “USERNAME ne NT AUTHORITY\SYSTEM” /FI “STATUS eq running” 命令，按 Enter 键即可列出系统中正在运行的非 SYSTEM 状态的所有进程，如图 3-39 所示。其中“/FI”为筛选器参数，“ne”和“eq”为关系运算符“不相等”和“相等”。

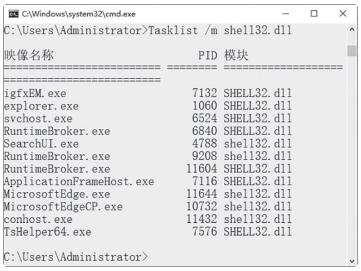

图 3-38　显示调用 shell32.dll 模块的进程

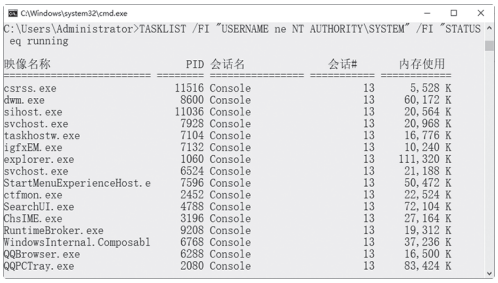

图 3-39　列出系统中正在运行的非 SYSTEM 状态的所有进程

3.3　实战演练


微视频

3.3.1　实战 1：使用命令代码清除系统垃圾文件

使用批处理文件可以快速地清除计算机中的垃圾文件，下面将介绍使用批处理文件清除系统垃圾文件的具体步骤。

Step 01 打开记事本文件，在其中输入可以清除系统垃圾的代码，输入的代码如下：

```
@echo off
echo 正在清除系统垃圾文件，请稍等 ......
del /f /s /q %systemdrive%\*.tmp
del /f /s /q %systemdrive%\*._mp
del /f /s /q %systemdrive%\*.log
del /f /s /q %systemdrive%\*.gid
del /f /s /q %systemdrive%\*.chk
del /f /s /q %systemdrive%\*.old
del /f /s /q %systemdrive%\recycled\*.*
del /f /s /q %windir%\*.bak
del /f /s /q %windir%\prefetch\*.*
rd /s /q %windir%\temp & md %windir%\temp
```

```
del /f /q %userprofile%\cookies\*.*
del /f /q %userprofile%\recent\*.*
del /f /s /q “%userprofile%\Local Settings\Temporary Internet Files\*.*”
del /f /s /q “%userprofile%\Local Settings\Temp\*.*”
del /f /s /q “%userprofile%\recent\*.*”
echo 清除系统垃圾完成!
echo. & pause
```

将上面的代码保存为 del.bat，如图 3-40 所示。

Step02 在“命令提示符”窗口中输入 del.bat 命令，按 Enter 键，可以快速清理系统垃圾，如图 3-41 所示。

图 3-40　编辑代码

图 3-41　自动清理垃圾

3.3.2　实战 2：使用 shutdown 命令实现定时关机


微视频

使用 shutdown 命令可以实现定时关机的功能，具体的操作步骤如下：

Step01 在“命令提示符”窗口中输入 shutdown/s /t 40 命令，如图 3-42 所示。

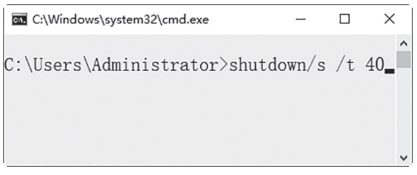

图 3-42　输入 shutdown/s /t 40 命令

Step02 弹出一个即将注销用户登录的信息提示框，这样计算机就会在规定的时间内关机，如图 3-43 所示。

Step03 如果此时想取消关机操作，可在命令行中输入命令 shutdown /a 后按 Enter 键，桌面右下角出现如图 3-44 所示的弹窗，表示取消成功。

图 3-43　信息提示框

图 3-44　取消关机操作