第 1 章 网络渗透快速入门

自网络诞生以来，网络攻击事件频繁发生。但是，对于众多的网络工作者来说，导致网络攻击事件频繁发生的原因并不重要，重要的是攻击者是如何进行攻击的，以及如何更好地防御攻击者的入侵等。那么，作为电脑或网络终端设备的用户，要想使自己的设备不受或少受攻击，就需要掌握一些相关的网络渗透测试知识。

1.1 网络渗透概述

网络渗透是保护信息和网络安全的重要途径，也是受信任的第三方进行的一种评估网络安全的活动，它通过运用黑客攻击的方法与工具，对目标网络进行各种手段的攻击来找出系统存在的漏洞，从而给出网络系统存在的安全风险的一种实践活动。

1.1.1 网络渗透攻击的概念

网络渗透是攻击者常用的一种攻击手段，也是一种综合的高级攻击技术，同时网络渗透也是安全工作者所研究的一个课题，在他们口中通常被称为“渗透测试”。其实，无论是网络渗透还是渗透测试，其实质是同一内容，也就是研究如何一步步攻击入侵某个大型网络主机服务器群组。只不过从实施的角度上看，前者是攻击者的恶意行为，后者则是网络安全工作者模拟入侵攻击测试，进而寻找最佳安全防护方案的正当手段。

在各种网络维护工作中，网络安全维护更是重中之重。为了保障网络安全，网络管理员往往会严格地规划网络的结构，区分内部与外部网络进行网络隔离，设置网络防火墙，安装杀毒软件，并做好各种安全保护措施。然而绝对的安全是不存在的，潜在的危险和漏洞总是相对存在的。

面对越来越多的网络攻击事件，网络管理员们采取了积极主动的应对措施，大大提高了网络的安全性。恶意的入侵者想要直接攻击一个安全防御到位的网络，已经变得非常困难了，于是，“网络渗透攻击”出现了。“网络渗透攻击”是对大型的网络主机服务器群组采用的一种迂回渐进式的攻击方法，通过长期而有计划地逐步渗透攻击进入网络，最终完全控制整个网络。

“网络渗透攻击”之所以能够成功是因为网络上总会有一些或大或小的安全缺陷或漏洞。攻击者利用这些小缺口一步一步地将这些缺口扩大，扩大，再扩大，最终导致整个网络安全防线的失守，从而掌控整个网络的权限。因此，作为网络管理员，完全有必要了解甚至掌握网络渗透入侵的技术，这样才能有针对性地进行防御，从而保障网络的真正安全。

1.1.2 渗透攻击与普通攻击的区别

网络渗透攻击与普通网络攻击的不同在于：普通的网络攻击只是单一类型的攻击；网络渗透攻击则与此不同，它是一种系统渐进型的综合攻击方式，其攻击目标是明确的，攻击目的往往不那么单一，危害性也非常严重。

例如，在普通的网络攻击事件中，攻击者可能仅仅是利用目标网络的 Web 服务器漏洞，入侵网站更改网页，或者在网页上挂马。也就是说，这种攻击是随机的，其目的也是单一而简单的。

在渗透入侵攻击的过程中，攻击者会有针对性地对某个目标网络进行攻击，以获取其内部的商业资料，进行网络破坏等。其实施攻击的步骤是非常系统的，假设其获取了目标网络中网站服务器的权限，则不会仅满足于控制此台服务器，而是会利用此台服务器继续入侵目标网络，获取整个网络中所有主机的权限。

另外，为了实现渗透攻击，攻击者采用的攻击方式绝不仅限于一种简单的 Web 脚本漏洞攻击，而是会综合运用远程溢出、木马攻击、密码破解、嗅探、ARP 欺骗等多种攻击方式，逐步控制网络。

总之，与普通网络攻击相比，网络渗透攻击具有攻击目的明确性、攻击步骤逐步与渐进性、攻击手段的多样性和综合性等特点。

1.1.3 学习网络渗透测试的意义

渗透测试是受信任的第三方进行的一种评估网络安全的活动，它通过运用各种黑客攻击方法与工具，对企业网络进行各种手段的攻击，以便找出系统存在的漏洞，给出网络系统存在的安全风险，是一种攻击模拟行为。

目前，网络渗透测试已经成为安全工作者的一个课题，其发展前景不可估量。作为一名网络管理员或安全工作者，如果有能力实施基本渗透测试，那么其价值将是极大的，一切日常安全维护操作将更加有针对性，也更加有效。

另外，在网络安全领域，最让安全工作者头疼的就是分析入侵攻击者的行为。如攻击者是如何入侵的？攻击者在入侵时做了什么事情？攻击者在入侵中运用了哪些技术？攻击者使用了哪些攻击工具等？

对于绝大多数安全管理者来说，对这些问题并不十分了解，对于这些渗透入侵技术也并不具备。但是，如果这些安全管理员学习了网络渗透测试的相关知识，就可以完全模拟攻击者可能使用的漏洞检测与攻击技术，对目标网络系统的安全进行深入的检测，探寻出网络系统中最脆弱的安全环节，从而让管理人员能够直观地知道其网络所面临的问题。

1.2 渗透测试需要掌握的知识

网络渗透测试所涉及的内容很多，覆盖的范围也广，对于一个新手来说，了解和掌握一些有关操作系统的知识就显得尤为重要。如在操作系统中经常遇到的进程、端口、服务、文件系统以及注册表等常见的术语。只有掌握了这些内容，才能提高攻击的成功率。


微视频

1.2.1 进程、端口和服务

进程、端口和服务是计算机操作系统中不可缺少的部分，一个进程对应着一个程序，服务和端口常常被联系在一起，一个端口对应着一个服务，如 Web 服务默认对应 80 端口等。

1. 进程

进程是程序在计算机上的一次执行活动。当运行一个程序，就启动了一个进程。显然，程序是

静态的，进程是动态的。进程可以分为系统进程和用户进程两种。凡是用于完成操作系统的各种功能的进程就是系统进程；凡是由用户启动的进程就是用户进程。

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 系统桌面中，单击“开始”菜单，在弹出的菜单列表中选择“任务管理器”命令，如图 1-1 所示。

Step02 随即打开“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 1-2 所示。

图 1-1　“任务管理器”菜单命令

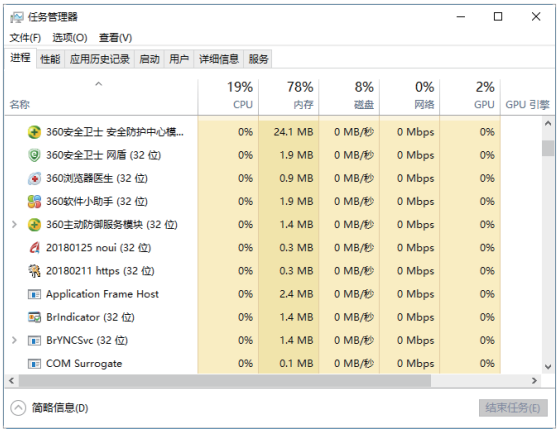

图 1-2　“任务管理器”窗口

提示：通过在 Windows 10 系统桌面上按下 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。

2. 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 65536（即 256×256）个，端口是通过端口号来标记的，端口号只能是整数，范围是 0 ～ 65535（256×256−1）。

服务器上所开放的端口往往是黑客潜在的入侵通道，对目标主机进行端口扫描能够获得许多有用的信息，常用的方法是使用端口扫描工具对指定 IP 或 IP 地址段进行扫描，下面介绍使用 ScanPort 扫描器扫描端口的方法，具体操作步骤如下：

Step01 下载并运行 ScanPort 程序，即可打开 ScanPort 主窗口，在其中设置起始 IP 地址、结束 IP 地址以及要扫描的端口号，如图 1-3 所示。

Step02 单击“扫描”按钮，即可进行扫描，从扫描结果中可以看出设置的 IP 地址段中计算机开启的端口，如图 1-4 所示。

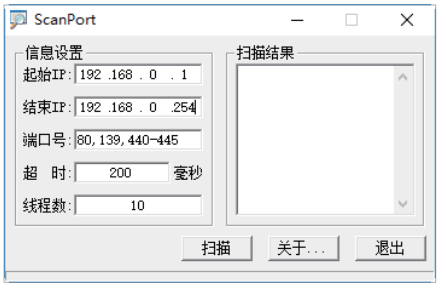

图 1-3　ScanPort 主窗口

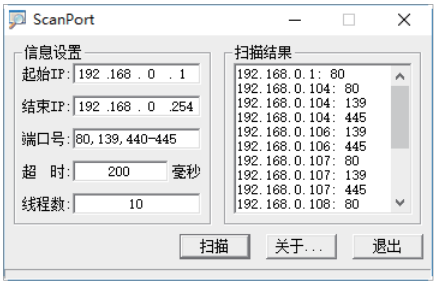

图 1-4　开始扫描

Step03 如果扫描某台计算机中开启的端口，则将开始 IP 和结束 IP 都设置为该主机的 IP 地址，如图 1-5 所示。

Step04 在设置完要扫描的端口号之后，单击“扫描”按钮，即可扫描出该主机中开启的端口（设置端口范围之内），如图 1-6 所示。

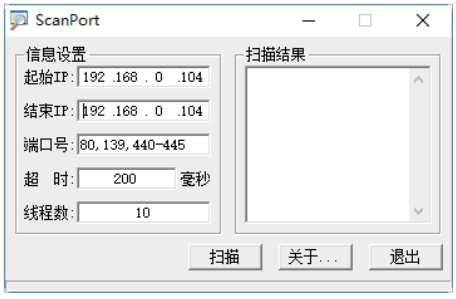

图 1-5 设置单一主机的 IP

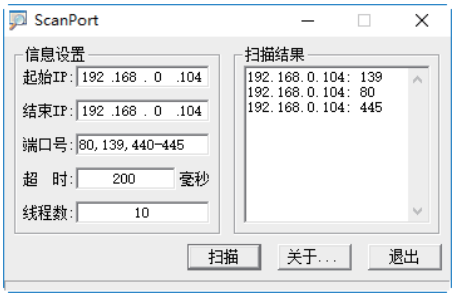

图 1-6 开始扫描单个主机的端口

3. 服务

在计算机中安装好操作系统之后，通常系统会默认启动许多服务，且每项服务都有一个具体的文件存在，一般存储在 C:\Windows\system32 文件夹中，其扩展名一般是 .exe、.dll、.sys 等。另外，操作系统中还可以根据自己的需要开启相应的服务和关闭不必要的服务。以开启 WebClient 服务为例，具体操作步骤如下：

Step01 右击“开始”菜单，在弹出的快捷菜单中选择“控制面板”命令，如图 1-7 所示。

Step02 打开“控制面板”窗口，双击“管理工具”图标，如图 1-8 所示。

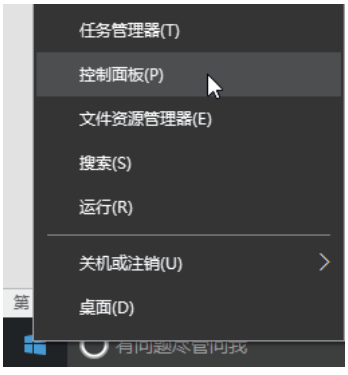

图 1-7 选择“控制面板”命令

图 1-8 “控制面板”窗口

Step03 打开“管理工具”窗口，双击“服务”图标，如图 1-9 所示。

Step04 打开“服务”窗口，找到 WebClient 服务项，如图 1-10 所示。

Step05 双击该服务项，弹出“WebClient 的属性”对话框，单击“启动类型”右侧的下拉按钮，在弹出的下拉菜单中选择“自动”选项，如图 1-11 所示。

Step06 单击“应用”按钮，激活“服务状态”下的“启动”按钮，如图 1-12 所示。

Step07 单击“启动”按钮，即可启动该项服务，再次单击“应用”按钮，在“WebClient 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”，如图 1-13 所示。

Step08 单击“确定”按钮，返回“服务”窗口，此时即可发现 WebClient 服务的“状态”变为“正

在运行”，这样就可以成功开启 WebClient 服务对应的端口，如图 1-14 所示。

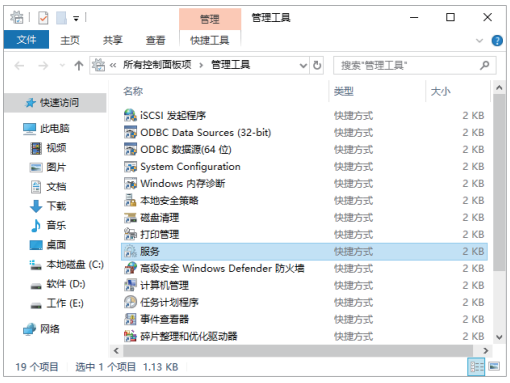

图 1-9　“服务”图标

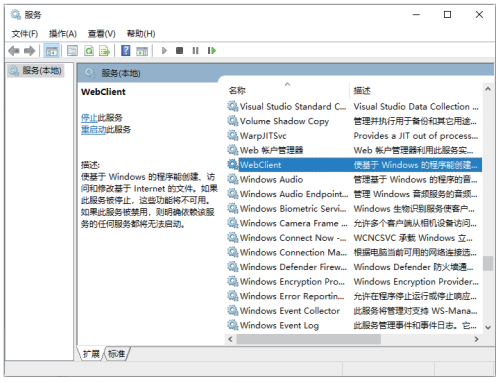

图 1-10　“服务”窗口

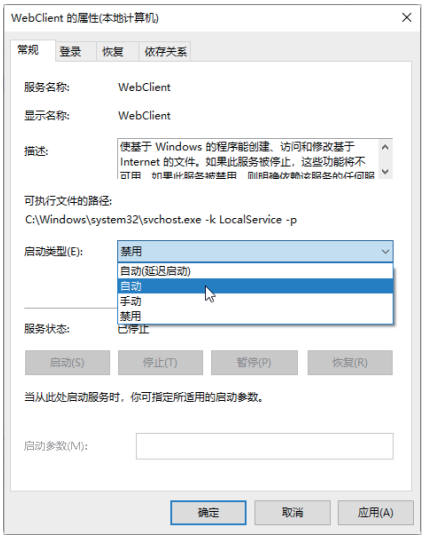

图 1-11　选择“自动”选项

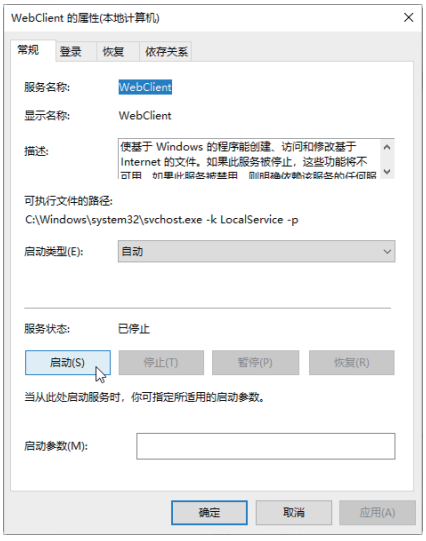

图 1-12　单击“启动”按钮

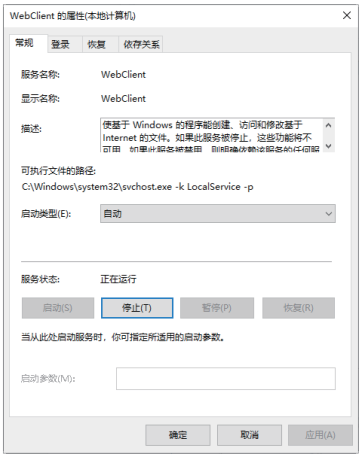

图 1-13　启动服务项

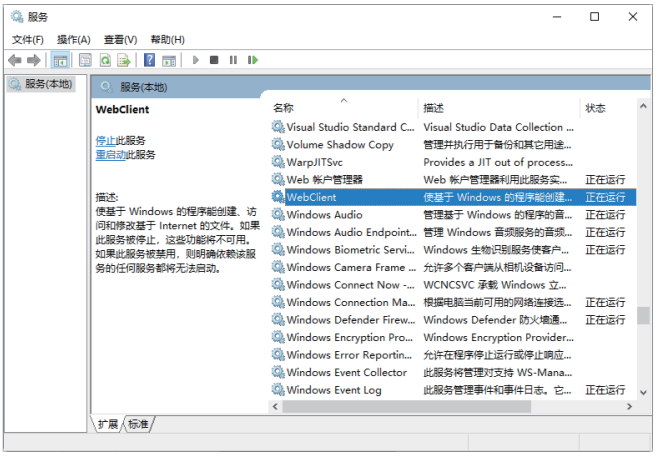

图 1-14　WebClient 服务的状态为“正在运行”

1.2.2 文件和文件系统

文件是存储于外存储器中具有名字的一组相关信息集合，在 Windows 系统中所有的程序和数据均以文件形式存入磁盘。文件是由文件名和图标组成的，一种类型的文件具有相同的图标，文件名不能超过 255 个字符（包括空格）。

文件名由 4 部分组成：[< 盘符 >][< 路径 >]< 文件名 >[<.. 扩展名 >]，其作用是唯一标识一个文件。文件名由 1 ～ 8 个字符组成，构成文件名的字符分为如下 3 类：

（1）26 个英文字母：a ～ z 或 A ～ Z。

（2）10 个阿拉伯数字：0 ～ 9。

（3）一些专用字符：$、#、&、@、!、%、()、{}、-、一。

注意：在文件名中不能使用“<”“>”“\”“//”“[、]”“:”“!”“+”“=”，以及小于 20H 的 ASCII 字符。另外，可根据需要自行命名文件，但不可与 DOS 命令文件同名。

操作系统中负责管理和存储文件信息的软件机构称为文件管理系统，简称文件系统。文件系统由三部分组成，与文件管理有关的软件、被管理的文件以及实施文件管理所需的数据结构。从系统角度来看，文件系统是对文件存储器空间进行组织和分配，负责文件的存储并对存入的文件进行保护和检索的系统。

文件系统是用于组织和存储文件的目录结构，也是操作系统用于明确磁盘或分区上的文件的方法和数据结构，即在磁盘上组织文件的方法。磁盘或分区和它所包括的文件系统的不同是很重要的。少数程序（包括最有理由的产生文件系统的程序）直接对磁盘或分区的原始扇区进行操作，这可能破坏一个存在的文件系统。一个分区或磁盘能作为文件系统使用前，需要初始化，并将记录数据结构写到磁盘上，这个过程就是建立文件系统。


微视频

1.2.3 IP 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，可以说找到 IP 地址是黑客实施入侵攻击的一个关键。

1. 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，通常使用十进制数来表示，如 192.168.1.100。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。

Step01 右击“开始”按钮，在弹出的快捷菜单中执行“运行”命令，如图 1-15 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 1-16 所示。

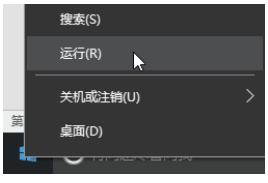

图 1-15 “运行”菜单

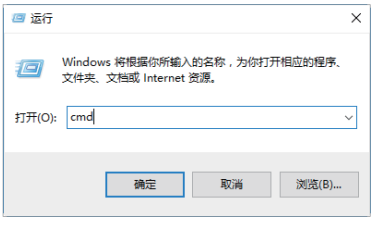

图 1-16 输入“cmd”命令

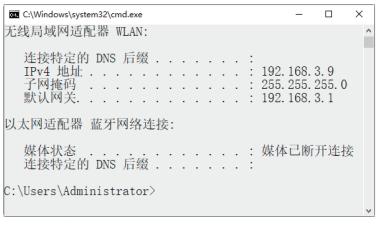

图 1-17 查看 IP 地址

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，即可显示出本机的 IP 配置相关信息，如图 1-17 所示。

提示：在“命令提示符”窗口中，192.168.0.130 表示本机在局域网中的 IP 地址。

2. 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入硬件内部。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。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，这就是用户自己计算机的网卡地址，它是唯一的，如图 1-18 所示。

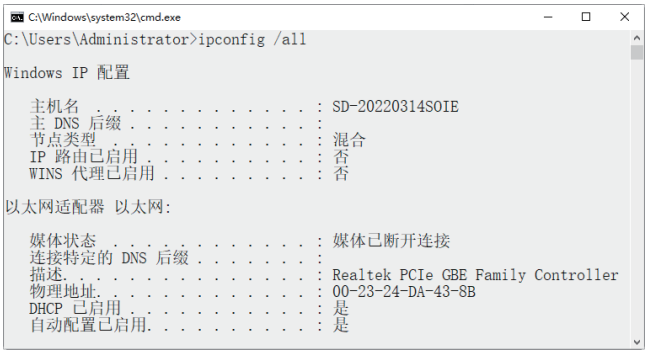

图 1-18　查看 MAC 地址

注意：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。

1.2.4　Windows 注册表

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。

Step01 在 Windows 操作系统中选择“开始”→“运行”菜单项，打开“运行”对话框，在其中输入命令“regedit”，如图 1-19 所示。

Step02 单击“确定”按钮，即可打开“注册表编辑器”窗口，在其中查看注册表信息，如图 1-20 所示。

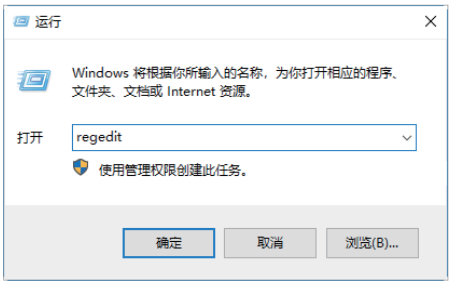

图 1-19　“运行”对话框

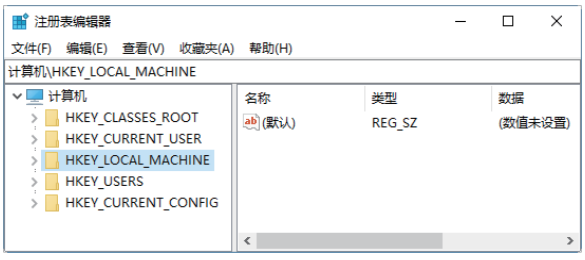

图 1-20　“注册表编辑器”窗口

1.3 网络渗透测试与攻击

网络渗透测试是一把双刃剑，它可以成为网络管理员和安全工作者保护网络安全的重要实施方案，也可以成为攻击者手中一种破坏性极强的攻击手段。因此，作为网络管理员和安全工作者要想保障网络的安全，就必须了解和掌握网络渗透测试的实施步骤与各种攻击方式。

1.3.1 网络渗透测试与攻击的分类

网络渗透攻击，或者说网络渗透测试，是完全模拟黑客可能使用的攻击技术和漏洞发现技术，对目标系统的安全做深入的探测，发现系统最脆弱的环节，渗透测试能够直观地让管理人员知道自己网络所面临的问题。

实际上网络渗透测试并没有严格的分类方式，但根据实际应用，普遍认同的几种分类方法如下。

1. 根据渗透方法分类

根据渗透方法不同，渗透测试 / 攻击可分为以下两类。

- 黑盒（Black Box）渗透

黑盒渗透测试又被称为 zero-knowledge testing，渗透者完全处于对目标网络系统一无所知的状态，通常这类测试只能通过 DNS、Web、E-mail 等网络对外公开提供的各种服务器进行扫描探测，从而获得公开的信息，以决定渗透的方案与步骤。

- 白盒（White Box）渗透

白盒渗透测试又称为“结构测试”，渗透测试人员可以通过正常渠道，向请求测试的机构获取目标网络系统的各种资料，包括用户账号和密码、操作系统类型、服务器类型、网络设备型号、网络拓扑结构、代码等信息，这与黑盒渗透测试相反。

2. 根据渗透测试目标分类

根据渗透测试目标不同，渗透测试又可分为以下几种。

- 主机操作系统渗透

对目标网络中的 Windows、Linux、UNIX 等不同操作系统主机进行渗透测试。

- 数据库系统渗透

对 MS-SQL、Oracle、MySQL、INFORMIX、SYBASE、DB2 等数据库系统进行渗透测试，这通常是对网站的入侵渗透过程而言的。

- 网站程序渗透

渗透的目标网络系统都对外提供了 Web 网页、E-mail 邮箱等网络程序应用服务，这是渗透者打开内部渗透通道的重要途径。

- 应用系统渗透

对渗透目标提供的各种应用，如 ASP、CGI、JSP、PHP 等组成的 WWW 应用进行渗透测试。

- 网络设备渗透

对各种硬件防火墙、入侵检测系统、路由器和交换机等网络设备进行渗透测试。此时，渗透者通常已入侵进入内部网络中。

3. 按网络环境分类

按照渗透者发起渗透攻击行为所处的网络环境不同，渗透测试可分为下面两类。

- 外网测试

外网测试指的是渗透测试人员完全处于目标网络系统之外的外部网络，模拟对内部状态一无所知的外部攻击者的行为。渗透者需要测试的内容包括：对网络设备的远程攻击、口令管理安全性

测试、防火墙规则试探和规避、Web 及其他开放应用服务等。

- 内网测试

内网测试指的是渗透测试人员由内部网络发起的渗透测试，这类测试能够模拟网络内部违规操作者的行为。同时，渗透测试人员已处于内网之中，绕过了防火墙的保护。因此，渗透控制的难度相对已减少了许多，各种信息收集与渗透实施更加方便，经常采用的渗透方式为：远程缓冲区溢出，口令猜测，以及 B/S 或 C/S 应用程序测试等。

1.3.2　渗透测试过程与攻击的手段

一般情况下，黑客在实施渗透攻击的过程中，多数采用的是从外部网络环境发起的非法的黑盒测试，对攻击的目标往往是一无所知。因此，这时就需要先采用各种手段来收集攻击目标的详细信息，然后通过获取的信息制订渗透入侵的方案，从而打开进入内网的通道，最后再通过提升权限进而控制整个目标网络，完成渗透攻击，如图 1-21 所示为攻击者渗透入侵的几个阶段。

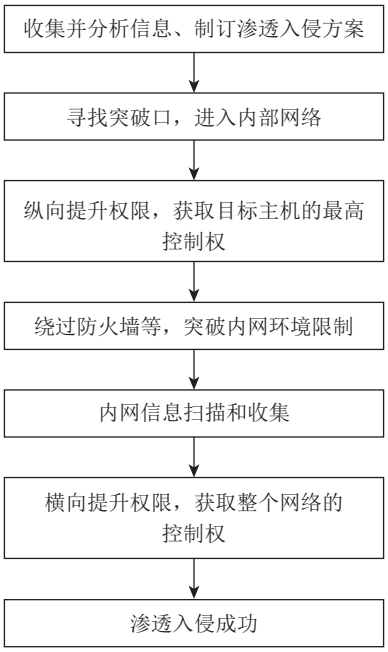

图 1-21　渗透测试的几个阶段

1. 收集并分析信息、制订渗透入侵方案

信息的收集是非常重要的，它决定了攻击者是否能准确地定位目标网络系统安全防线上的漏洞，攻击者所收集的一切信息，一般都是目标系统中一些小小的漏洞、开放的端口等。

信息收集主要分为以下几类。

- 边缘信息收集

在这一过程中获取的信息内容和方式主要是目标网络系统中的一些边缘信息，如目标网络系统公司的结构、各部门职能、内部员工账号组成、邮件联系地址、QQ 或 MSN 号码、各种社交网络账号与信息等。

- 网络信息收集

在这一过程中需要收集目标网络的各种网络信息，所使用的手段包括 Google Hacking、WHOIS

查询、DNS 域名查询和网络扫描器等。

网络信息收集的最终目的是要获取目标网络拓扑结构、公司网络所在区域、子公司 IP 地址分布、VPN 接入地址、各种重要服务器的分布、网络连接设备等信息。

- 端口 / 服务信息收集

在这一过程中，攻击者会利用各种端口服务扫描工具来扫描目标网络中对外提供服务的服务器，查询服务器上开放的各种服务，如 Web、FTP、MySQL、SNMP 等。

- 漏洞扫描

通过上述的信息收集，在获得目标网络各服务器开放的服务之后，就可以对这些服务进行重点扫描，扫描出其所存在的漏洞。

常用的扫描工具主要有：针对操作系统漏洞扫描的工具，包括 X-Scan、ISS、Nessus、SSS、Retina 等；针对 Web 网页服务的扫描工具，包括 SQL 扫描器、文件 PHP 包含扫描器、上传漏洞扫描工具，以及各种专业全面的扫描系统（如 AppScan、Acunetix Web Vulnerability Scanner 等）；针对数据库的扫描工具，包括 Shadow Database Scanner、NGSSQuirreL，以及 SQL 空口令扫描器等。另外，许多入侵者或渗透测试员也有自己的专用扫描器，其使用更加个性化。

- 制订渗透方案

在获取了全面的网络信息并查询到远程目标网络中的漏洞后，攻击者就可以开始制订渗透攻击的方案了。入侵方案的制订，不仅要考虑到各种安全漏洞设置信息，更重要的是利用网络管理员心理上的安全盲点，制订攻击方案。

2. 寻找突破口，进入内部网络

渗透攻击者可以结合上面扫描获得的信息，来确定自己的突破方案。例如，针对网关服务器进行远程溢出，或者是从目标网络的 Web 服务器入手，也可以针对网络系统中的数据库弱口令进行攻击等。寻找内网突破口，常用的攻击手法有：

- 利用系统或软件漏洞进行的远程溢出攻击；
- 利用系统与各种服务的弱口令攻击；
- 对系统或服务账号的密码进行暴力破解；
- 采用 Web 脚本入侵、木马攻击。

最常用的两种手段是 Web 脚本攻击和木马欺骗。攻击者可以通过邮件、通信工具或挂马等方式，将木马程序绕过网关的各种安全防线，发送到内部诈骗执行，从而直接获得内网主机的控制权。

3. 纵向提升权限，获取目标主机的最高控制权

通过上面的步骤，攻击者可能已成功入侵目标网络系统对外的服务器，或者内部某台主机，但是这对于进一步的渗透攻击来说还是不够。例如，攻击者入侵了某台 Web 服务器，上传了 Webshell 控制网站服务器，但是却没有权限安装各种木马后门，或运行一些系统命令，此时就需要提升自己的权限，从而完全获得主机的最高控制权。有关提升权限的方法会在以后的章节中介绍，这里不做详细的说明。

4. 绕过防火墙等，突破内网环境限制

在对内网进行渗透入侵之前，攻击者还需要突破各种网络环境限制，例如网络管理员在网关设置了防火墙，从而导致无法与攻击目标进行连接等。突破内网环境限制所涉及的攻击手段多种多样，如防火墙杀毒软件的突破、代理的建立、账号后门的隐藏破解、3389 远程终端的开启和连接等。

其中最重要的一点是如何利用已控制的主机，连接攻击其他内部主机。采用这种方式的原因是目标网络内的主机是无法直接进行连接的，因此攻击者往往会使用代理反弹连接到外部主机，会将已入侵的主机作为跳板，利用远程终端进行连接入侵控制。

5. 内网信息扫描与收集

在成功完成上述步骤后，攻击者就完全控制了网关或内部的某台主机，并且拥有了对内网主机的连接通道，这时就可以对目标网络的内部系统进行渗透入侵了。但是，在进行渗透攻击前，同样需要进行各种信息的扫描和收集，尽可能地获得内网的各种信息。例如，当获取了内网网络的分布结构信息，就可以确定内网中最重要的关键服务器，然后对重要的服务器进行各种扫描，寻找其漏洞，以确定进一步的入侵控制方案。

6. 横向提升权限，获取整个网络的控制权

经过上述操作步骤，攻击者虽然获得了当前主机的最高系统控制权限，然而当前的主机在整个内部网络中可能仅仅是一台无关紧要的客服主机，那么，攻击者要想获取整个网络的控制权，就必须横向提升自己在网络中的权限。

在横向提升自己在网络中的权限时，往往需要考虑到内网中的网络结构，确定合理的提权方案。例如，对于小型的局域网，可以采用嗅探的方式获得域管理员的账号、密码，也可以直接采用远程溢出的方式获得远程主机的控制权限。对于大型的内部网络，攻击者可能还需要攻击内部网网络设备，如路由器、交换机等。

总之，横向提升自己在网络中的权限，所用到的攻击手段，依旧是远程溢出、嗅探、密码破解、ARP 欺骗、会话劫持和远程终端扫描破解连接等。

7. 渗透入侵成功

攻击者在获得内网管理员的控制权后，整个网络就在自己的掌握之中了，渗透入侵成功。

1.4　实战演练

1.4.1　实战 1：查看进程起始程序


微视频

Step 01 用户通过查看进程的起始程序，可以判断哪些进程是恶意进程。查看进程起始程序的具体操作步骤如下：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 1-22 所示。

Step 02 按 Enter 键，即可在反馈的信息中查看每个进程的起始程序或文件列表，这样就可以根据相关知识来判断是否为病毒或木马发起的程序，如图 1-23 所示。

图 1-22　输入命令

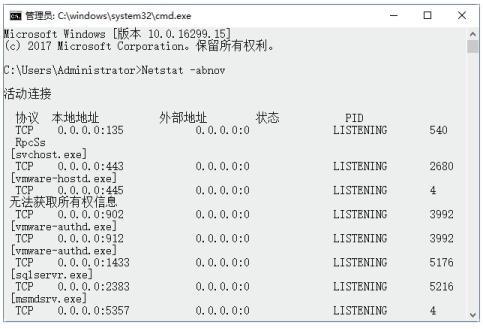

图 1-23　查看进程起始程序

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。

具体操作步骤如下。

Step01 单击“开始”菜单，在弹出的“开始屏幕”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 1-24 所示。

Step02 打开“查看”选项卡，在打开的功能区域中选择“显示 / 隐藏”区域中的“文件扩展名”复选框，如图 1-25 所示。

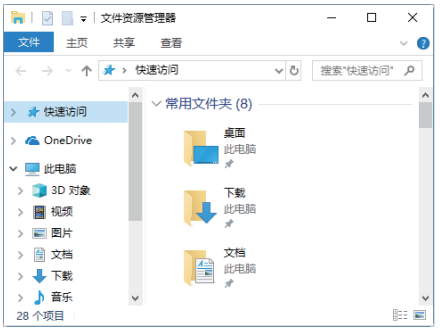

图 1-24 “文件资源管理器”窗口

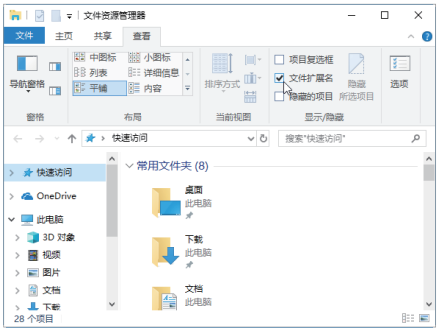

图 1-25 “查看”选项卡

Step03 此时打开一个文件夹，用户便可以查看到文件的扩展名，如图 1-26 所示。

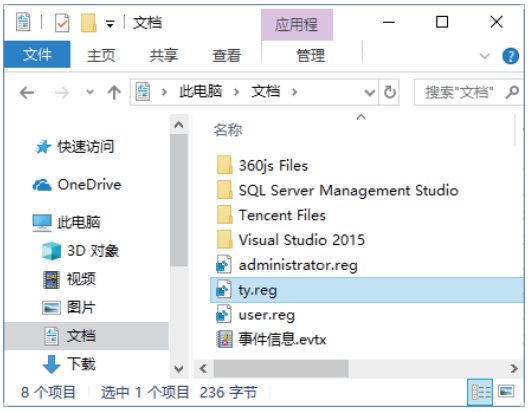

图 1-26 查看文件的扩展名

第2章 搭建网络渗透测试环境

安全测试环境是黑客攻防实战必备的内容，也是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渗透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，该系统中可以进行测试和模拟黑客入侵方式。

2.1.1 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 运用具有最新的 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虚拟出 Windows 环境，在该环境中可以同时运行多个应用程序。

2.1.2 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个。

- 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，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，同时还可以快速还原之前的快照，避免错误操作造成系统崩溃。

2.2.1 下载虚拟机软件

微视频

在使用虚拟机之前，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，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，VMware 支持中文页面，正常注册即可，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。

图 2-2 打开“所有产品”选项卡

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 2-3 “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 弹出“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。

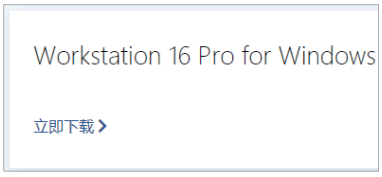

图 2-4　VMware 下载页面

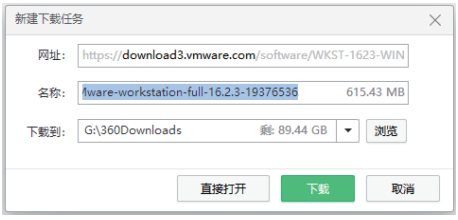

图 2-5　“新建下载任务”对话框

2.2.2　安装虚拟机软件


微视频

虚拟机软件下载完成后就可以安装了，这里下载的是目前最新版本“VMware-workstation-full-16.2.3-19376536.exe”，用户可根据实际情况选择当前最新版本下载即可，安装虚拟机的具体操作步骤如下。

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

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

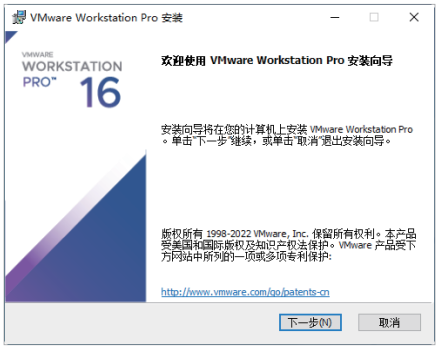

图 2-6　“安装向导”对话框

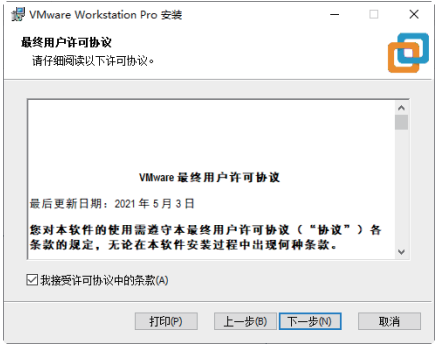

图 2-7　“最终用户许可协议”对话框

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

Step04 单击“下一步”按钮，进入“用户体验设置”对话框，这里采用系统默认设置，如图 2-9 所示。

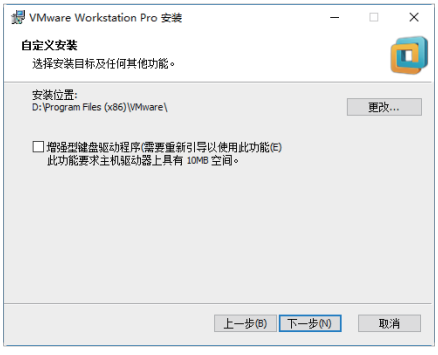

图 2-8　“自定义安装”对话框

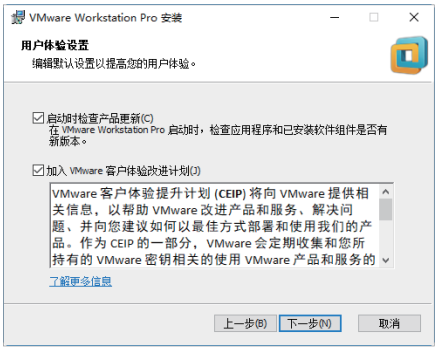

图 2-9　“用户体验设置”对话框

Step05 单击“下一步”按钮，进入“快捷方式”对话框，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”对话框，开始准备安装虚拟机软件，如图 2-11 所示。

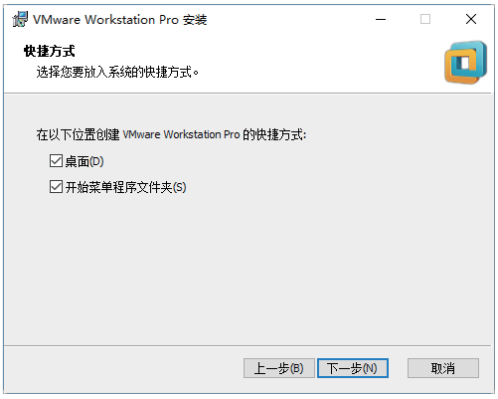

图 2-10 “快捷方式”对话框

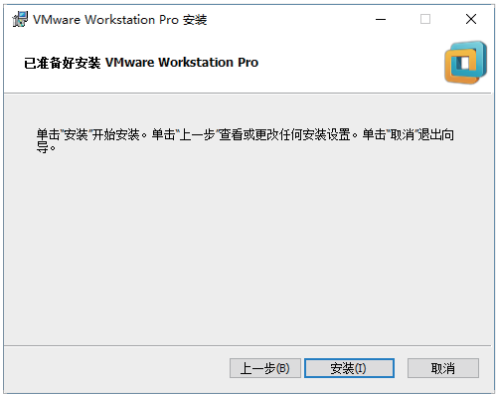

图 2-11 “已准备好安装 VMware Workstation Pro”对话框

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

Step08 虚拟机安装完成并重新启动系统后，才可以使用虚拟机，至此，便完成了 VMware 虚拟机的下载与安装，如图 2-13 所示。

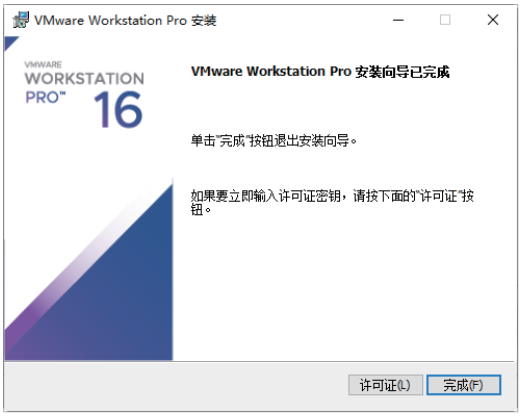

图 2-12 “安装向导已完成”对话框

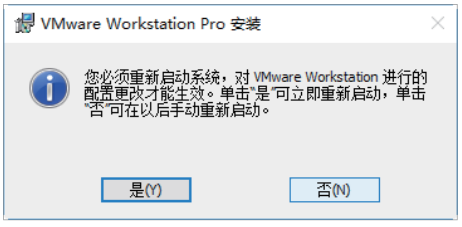

图 2-13 重新启动系统

2.3 安装 Windows 操作系统

现实中组装好计算机以后需要给它安装一个操作系统，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 10 操作系统

在虚拟机中安装 Windows 10 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 10 操作系统了。具体操作步骤如下。

Step01 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。

Step02 单击“创建新的虚拟机”按钮，进入“欢迎使用新建虚拟机向导”对话框，在其中选中“自定义”单选按钮，如图 2-15 所示。

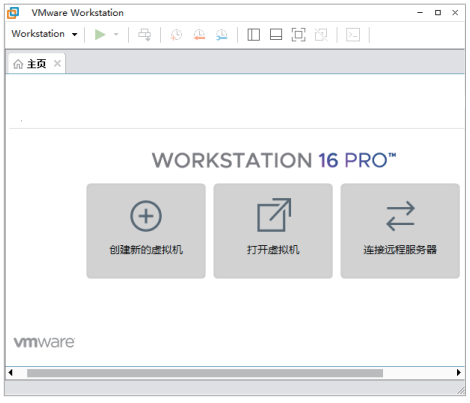

图 2-14　VMware 虚拟机软件

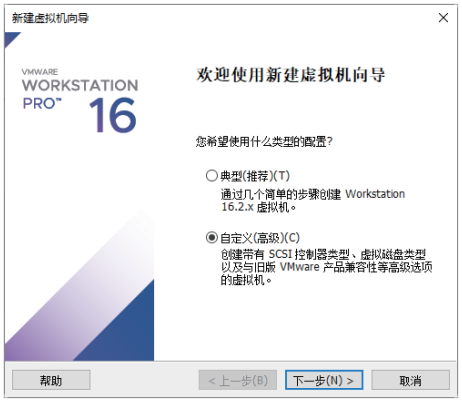

图 2-15　“欢迎使用新建虚拟机向导”对话框

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，这里采用默认设置，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，在其中选择“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

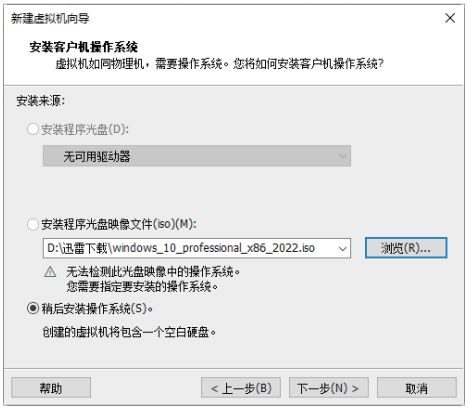

图 2-17　“安装客户机操作系统”对话框

Step05 单击“下一步”按钮，进入“选择客户机操作系统”对话框，在其中选择“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。

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。

图 2-18 “选择客户机操作系统”对话框

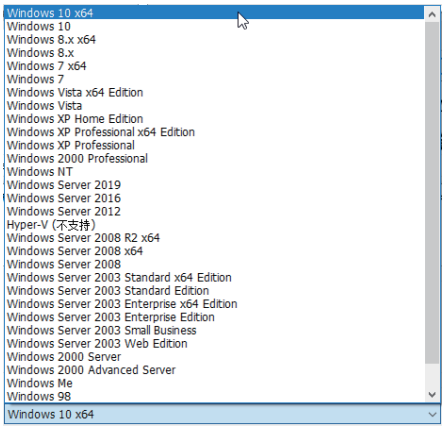

图 2-19 选择系统版本

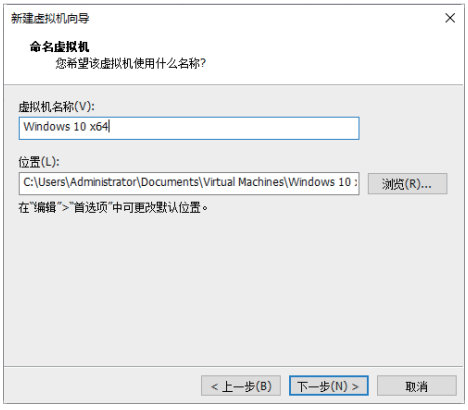

图 2-20 “命名虚拟机”对话框

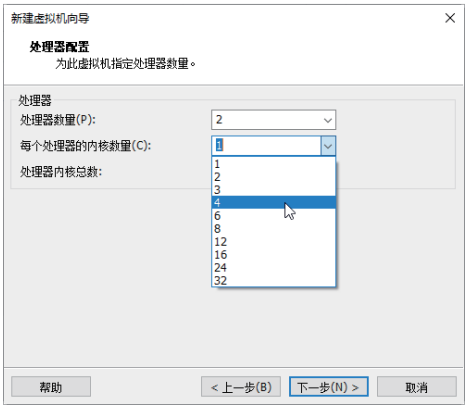

图 2-21 “处理器配置”对话框

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，最小内存不要低于 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，这里选择“使用网络地址转换（NAT）”单选按钮，如图 2-23 所示。

图 2-22 “此虚拟机的内存”对话框

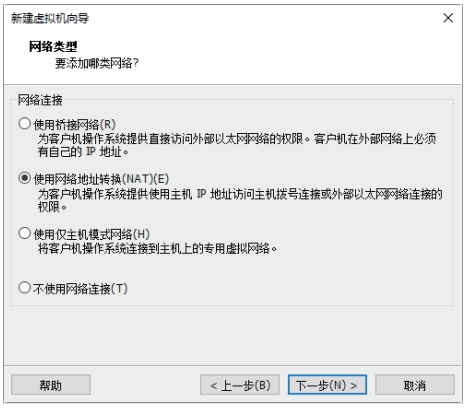

图 2-23 “网络类型”对话框

Step11 单击“下一步”按钮，进入“选择 I/O 控制器类型”对话框，这里选择 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，这里选择 NVMe 单选按钮，如图 2-25 所示。

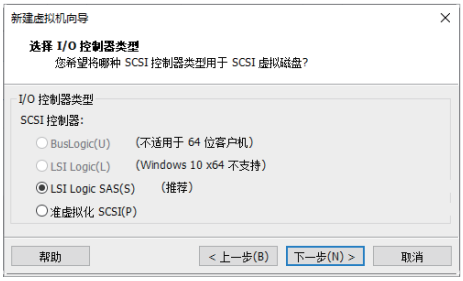

图 2-24　“选择 I/O 控制器类型”对话框

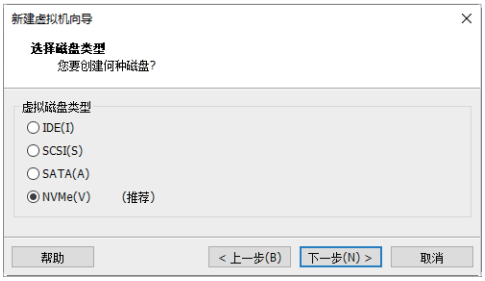

图 2-25　“选择磁盘类型”对话框

Step13 单击“下一步”按钮，进入“选择磁盘”对话框，这里选择“创建新虚拟磁盘”单选按钮，如图 2-26 所示。

Step14 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”设置为 60GB 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。

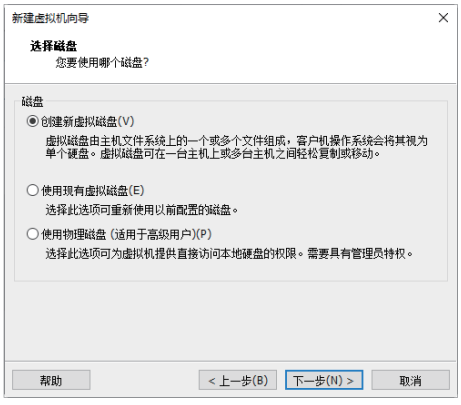

图 2-26　“选择磁盘”对话框

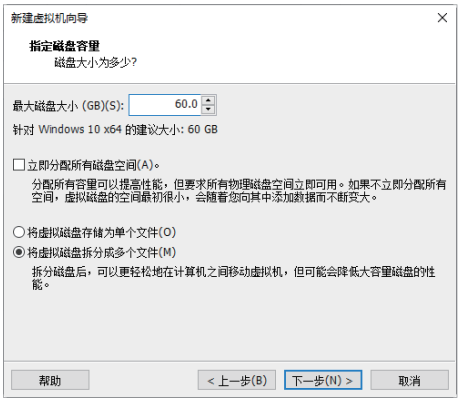

图 2-27　“指定磁盘容量”对话框

Step15 单击“下一步”按钮，进入“指定磁盘文件”对话框，这里保持默认设置即可，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

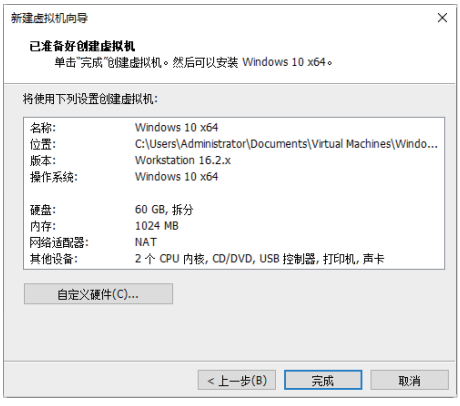

图 2-29　“已准备好创建虚拟机”对话框

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，这一步相当于组装了一台裸机，这当中的硬件配置，可以根据实际需求再进行更改。

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。

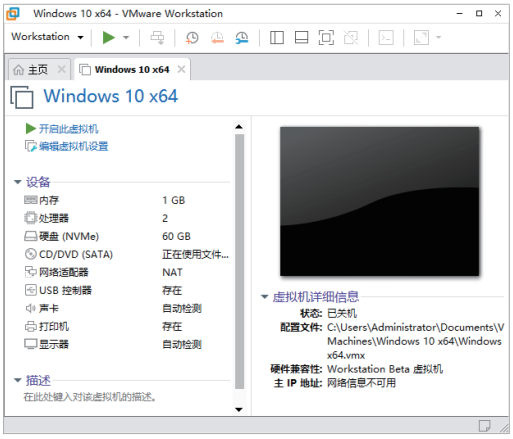

图 2-30　创建的新虚拟机

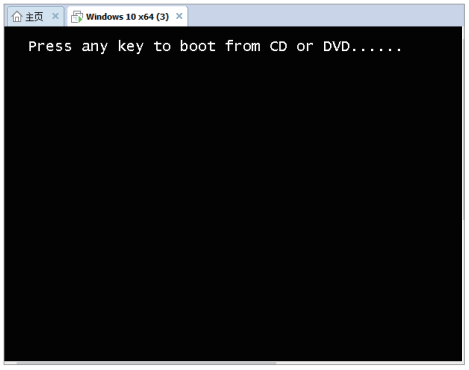

图 2-31　安装过渡窗口

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

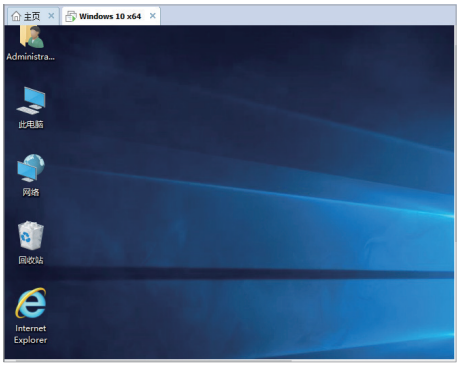

图 2-33　操作系统界面

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。

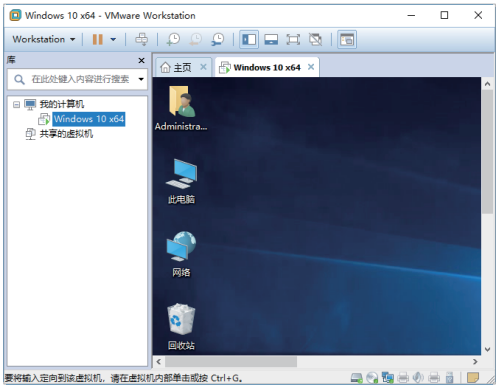

图 2-34　进入虚拟系统

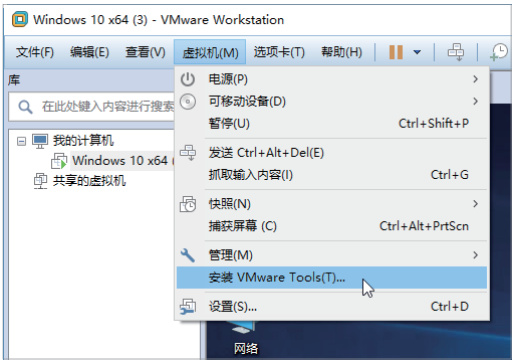

图 2-35　“安装 VMware Tools”命令

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

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

图 2-36　“欢迎使用 VMware Tools 的安装向导”对话框

图 2-37　“选择安装类型”对话框

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

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

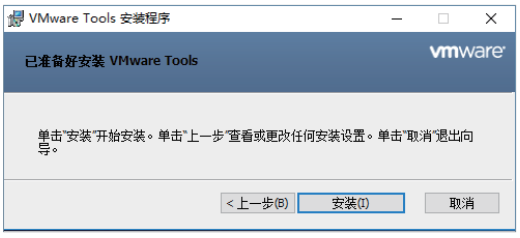

图 2-38　“已准备好安装 VMware Tools”对话框

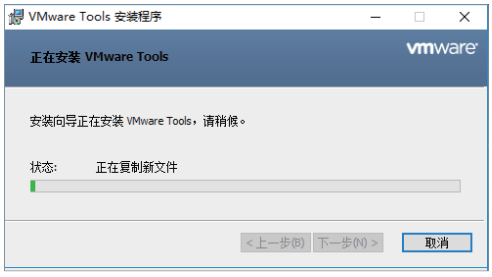

图 2-39　“正在安装 VMware Tools”对话框

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

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。

图 2-40 “VMware Tools 安装向导已完成”对话框

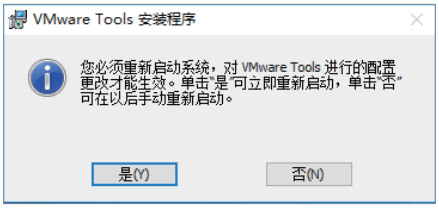

图 2-41 信息提示框

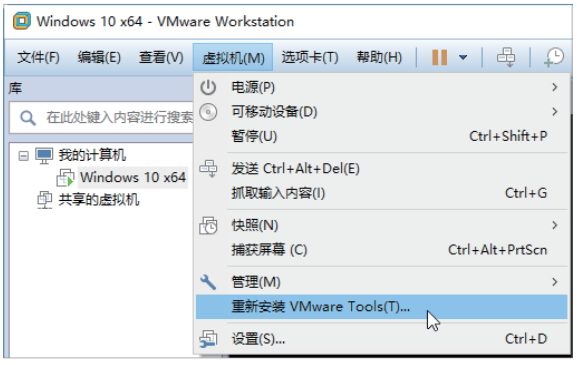

图 2-42 “重新安装 VMware Tools”菜单命令

Step09 单击“是”按钮，系统即可自动启动，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。

2.4 安装 Kali Linux 操作系统

本节来介绍如何给虚拟机安装 Kali 操作系统。

2.4.1 下载 Kali Linux 系统

Kali Linux 是基于 Debian 的 Linux 发行版，设计用于数字取证操作系统。下载 Kali Linux 系统的具体操作步骤如下。

Step01 在浏览器中输入 Kali Linux 系统的网址“https://www.kali.org”，打开 Kali 官方网站，如图 2-43 所示。

Step02 单击 DOWNLOAD 菜单，在弹出的菜单列表中选择 Kali Linux 版本，如图 2-44 所示。

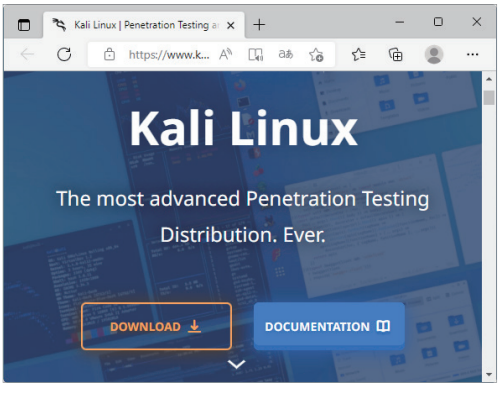

图 2-43 Kali 官方网站

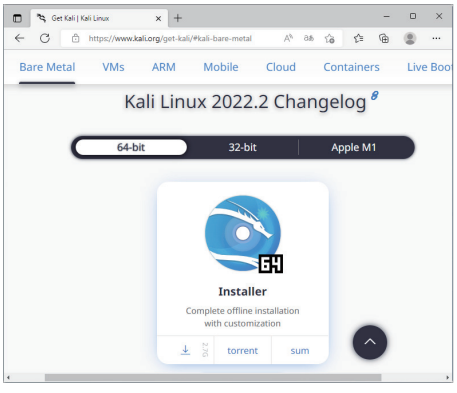

图 2-44 选择 Kali Linux 版本

并显示下载进度，如图 2-45 所示。

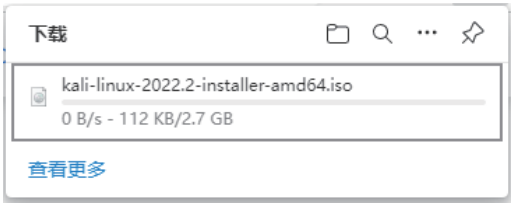

图 2-45　下载进度

2.4.2　安装 Kali Linux 系统


微视频

架设好虚拟机并下载好 Kali Linux 系统后，接下来便可以安装 Kali Linux 系统了。安装 Kali 操作系统的具体操作步骤如下：

Step01 打开安装好的虚拟机，选择“CD/DVD”选项，如图 2-46 所示。

Step02 在打开的“虚拟机设置”页面中选择“使用 ISO 映像文件”单选按钮，如图 2-47 所示。

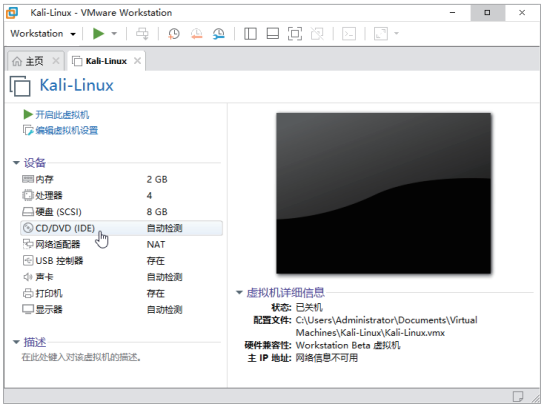

图 2-46　选择“CD/DVD”选项

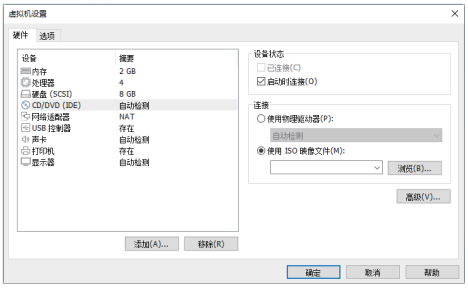

图 2-47　“虚拟机设置”对话框

Step03 单击“浏览”按钮，打开“浏览 ISO 映像”对话框，在其中选择下载好的系统映像文件，如图 2-48 所示。

Step04 单击“打开”按钮，返回到虚拟机设置页面，这里单击“开启此虚拟机”选项，便可以启动虚拟机，如图 2-49 所示。

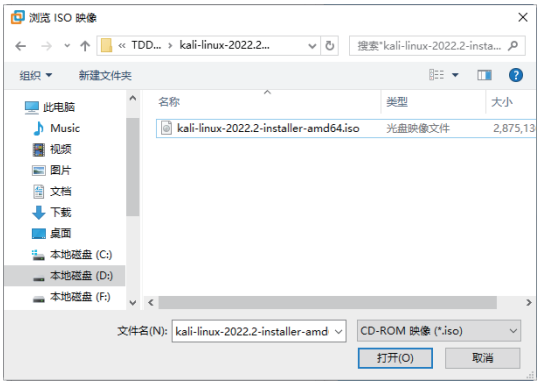

图 2-48　“浏览 ISO 映像”对话框

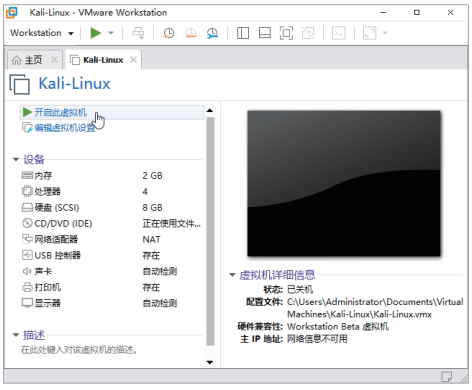

图 2-49　虚拟机设置页面

Step05 启动虚拟机后会进入启动选项页面，用户可以通过键盘上下键选择 Graphical Install 选项，如图 2-50 所示。

Step06 选择完毕后，按 Enter 键，进入语言选择页面，这里选择“中文（简体）”选项，如图 2-51 所示。

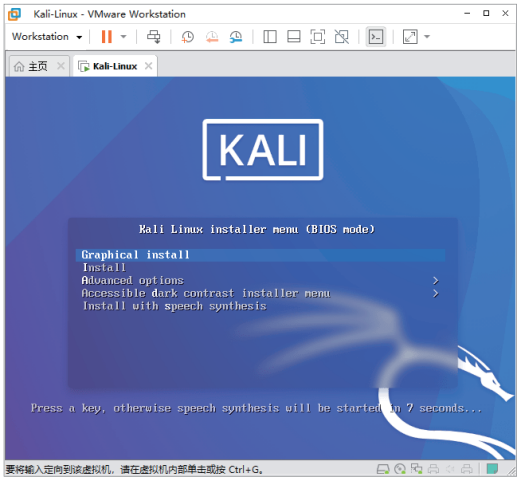

图 2-50　选择 Graphical Install 选项

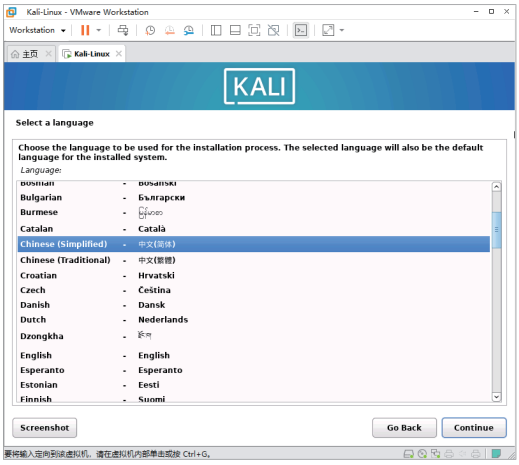

图 2-51　语言选择页面

Step07 单击 Continue 按钮，进入选择语言确认页面，保持系统默认设置，如图 2-52 所示。

Step08 单击“继续”按钮，进入“请选择您的区域”页面，它会自动上网匹配，即使不正确也没有关系，系统安装完成后还可以调整，这里保持默认设置，如图 2-53 所示。

图 2-52　语言确认页面

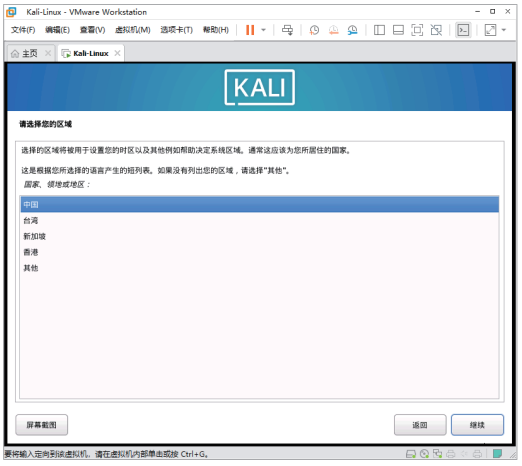

图 2-53　“请选择您的区域”页面

Step09 单击“继续”按钮，进入“配置键盘”页面，同样系统会根据语言选择来自行匹配，这里保持默认设置，如图 2-54 所示。

Step10 单击“继续”按钮，按照安装步骤的提示就可以完成 Kali Linux 系统的安装了，图 2-55 所示为安装基本系统界面。

Step11 系统安装完成后，会提示用户重启进入系统，如图 2-56 所示。

Step12 按 Enter 键，安装完成后重启，进入“用户名”页面，在其中输入 root 管理员账号，如图 2-57 所示。

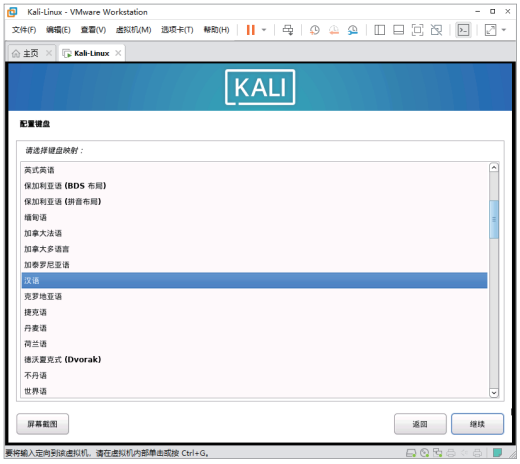

图 2-54　“配置键盘”页面

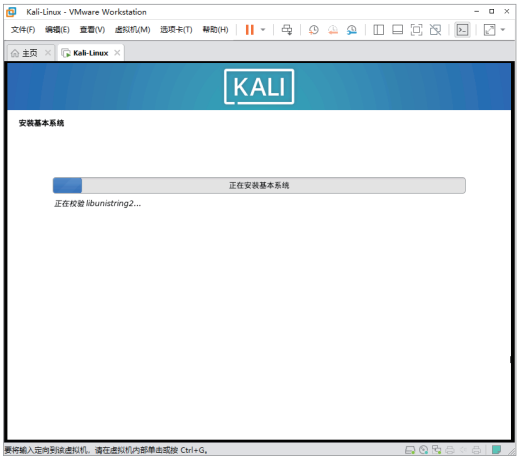

图 2-55　安装基本系统界面

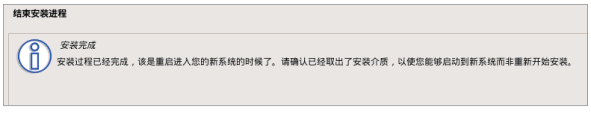

图 2-56　安装完成

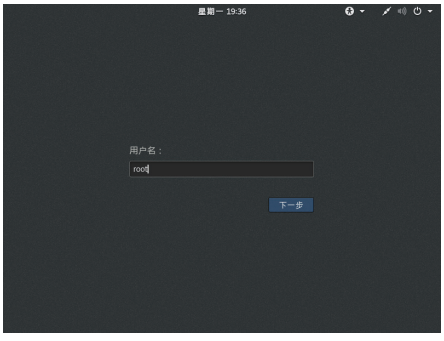

图 2-57　“用户名”页面

Step13 单击“下一步”按钮，进入登录密码页面，在其中输入设置好的管理员密码，如图 2-58 所示。

Step14 单击“登录”按钮，至此便完成了整个 Kali Linux 系统的安装工作，如图 2-59 所示。

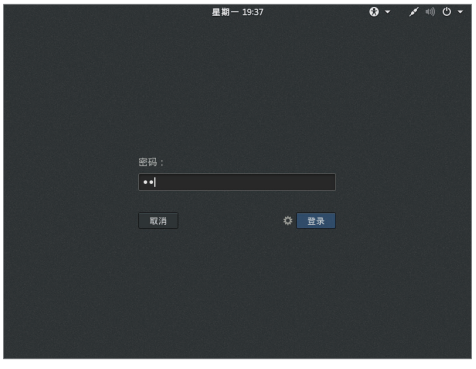

图 2-58　输入密码

图 2-59　Kali Linux 系统页面

2.4.3　更新 Kali Linux 系统

初始安装的 Kali 系统如果不及时更新是无法使用的，下面介绍更新 Kali 系统的方法与步骤。

Step01 双击桌面上 Kali 系统的终端黑色图标，如图 2-60 所示。

Step02 打开 Kali 系统的终端设置界面，在其中输入命令“apt update”，然后按 Enter 键，即可获取需要更新软件的列表，如图 2-61 所示。

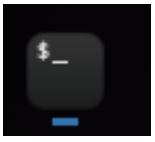

图 2-60　Kali 系统图标

图 2-61　需要更新软件的列表

Step03 获取完更新列表，如果有需要更新的软件，可以运行 apt upgrade 命令，如图 2-62 所示。

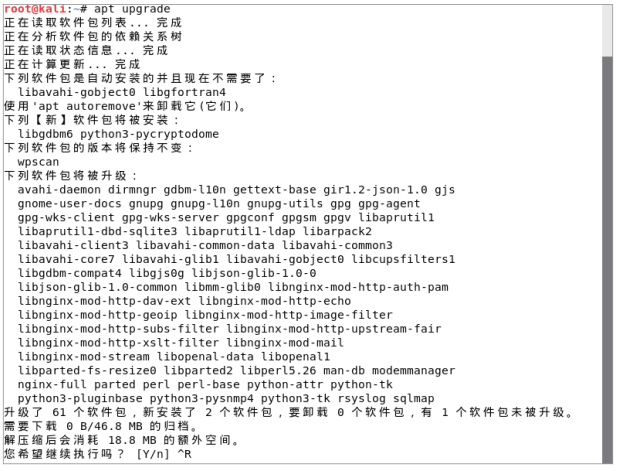

图 2-62　运行 apt upgrade 命令

Step04 运行命令后会有一个提示，此时按键盘上的 Y 键，即可开始更新，更新中状态如图 2-63 所示。

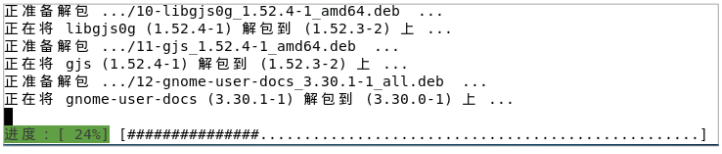

图 2-63　开始更新

注意：由于网络原因可能需要多执行几次更新命令，直至更新完成。另外，如果个别软件已经存在升级版本问题（如图 2-64 所示），这时，可以先卸载旧版本，例如卸载 wpscan 软件，可以运行“apt-get remove wpscan”命令，如图 2-65 所示，此时按键盘上的 Y 键即可卸载。

图 2-64　升级版本问题

卸载完旧版本后，可以运行“apt-get install wpscan”命令，如图 2-66 所示，此时按键盘上的 Y 键即可开始安装新版本。

```
root@kali:~# apt-get remove wpscan
正在读取软件包列表... 完成
正在分析软件包的依赖关系树
正在读取状态信息... 完成
下列软件包是自动安装的并且现在不需要了：
  ruby-ethon ruby-ffi ruby-ruby-progressbar ruby-terminal-table ruby-typhoeus
  ruby-unicode-display-width ruby-yajl
使用'apt autoremove'来卸载它(它们)。
下列软件包将被【卸载】：
  kali-linux-full wpscan
升级了 0 个软件包，新安装了 0 个软件包，要卸载 2 个软件包，有 0 个软件包未被升级。
解压缩后将会空出 267 kB 的空间。
您希望继续执行吗？ [Y/n] y
```

图 2-65　卸载旧版本

```
root@kali:~# apt-get install wpscan
正在读取软件包列表... 完成
正在分析软件包的依赖关系树
正在读取状态信息... 完成
下列软件包是自动安装的并且现在不需要了：
  ruby-terminal-table ruby-unicode-display-width
使用'apt autoremove'来卸载它(它们)。
将会同时安装下列软件：
  ruby-cms-scanner ruby-opt-parse-validator ruby-progressbar
下列软件包将被【卸载】：
  ruby-ruby-progressbar
下列【新】软件包将被安装：
  ruby-cms-scanner ruby-opt-parse-validator ruby-progressbar wpscan
升级了 0 个软件包，新安装了 4 个软件包，要卸载 1 个软件包，有 0 个软件包未被升级。
需要下载 0 B/112 kB 的归档。
解压缩后会消耗 594 kB 的额外空间。
您希望继续执行吗？ [Y/n] y
```

图 2-66　安装新版本

最后，再次运行“apt upgrade”命令，如果显示无软件需要更新，此时系统更新完成，如图 2-67 所示。

```
root@kali:~# apt upgrade
正在读取软件包列表... 完成
正在分析软件包的依赖关系树
正在读取状态信息... 完成
正在计算更新... 完成
下列软件包是自动安装的并且现在不需要了：
  ruby-terminal-table ruby-unicode-display-width
使用'apt autoremove'来卸载它(它们)。
升级了 0 个软件包，新安装了 0 个软件包，要卸载 0 个软件包，有 0 个软件包未被升级。
```

图 2-67　系统更新完成

2.5　实战演练

2.5.1　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就运行，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 按键盘上的 Ctrl+Alt+Del 组合键，打开如图 2-68 所示的界面。

Step02 单击“任务管理器”选项，打开“任务管理器”窗口，如图 2-69 所示。

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 2-70 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 2-71 所示。

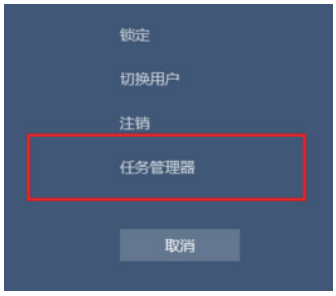

图 2-68 “任务管理器”选项

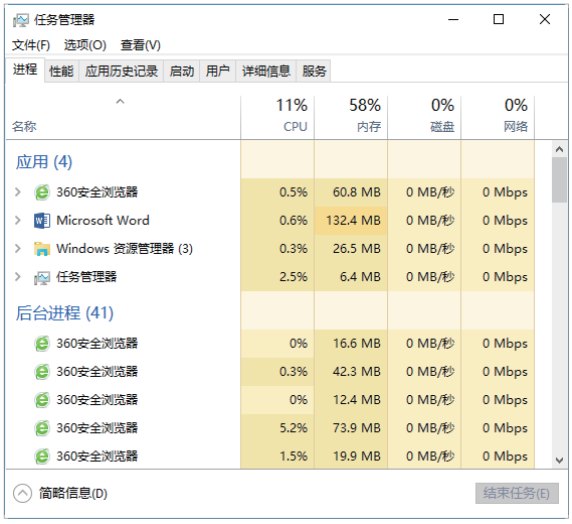

图 2-69 “任务管理器”窗口

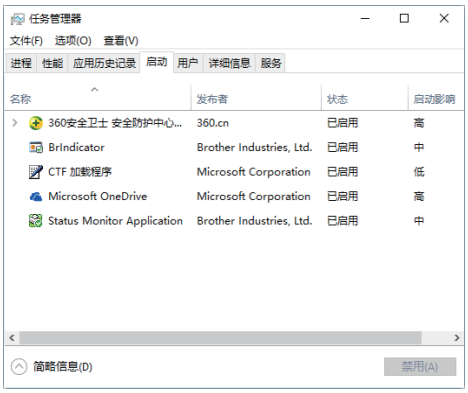

图 2-70 “启动”选项卡

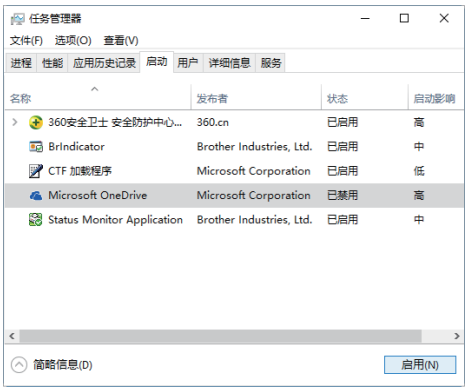

图 2-71 禁止开机启动项


微视频

2.5.2 实战 2：在安全模式下查杀病毒

安全模式的工作原理是在不加载第三方设备驱动程序的情况下启动电脑，使电脑运行在系统最小模式，这样用户就可以方便地查杀病毒，还可以检测与修复计算机系统的错误。下面以 Windows 10 操作系统为例介绍在安全模式下查杀并修复系统错误的方法。

具体的操作步骤如下。

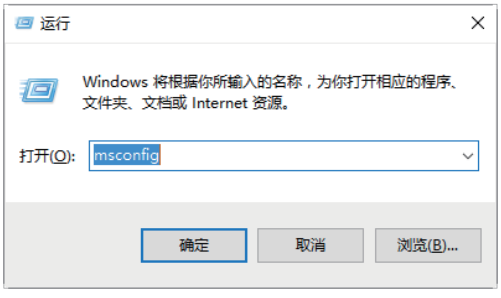

图 2-72 “运行”对话框

Step 01 按 Win+R 组合键，弹出“运行”对话框，在“打开”文本框中输入“msconfig”命令，单击“确定”按钮，如图 2-72 所示。

Step02 弹出“系统配置”对话框，打开“引导”选项卡，在“引导”选项卡中，选择“安全引导”复选框和“最小”单选按钮，如图 2-73 所示。

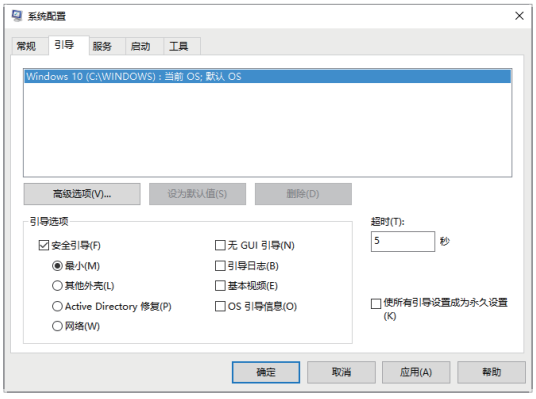

图 2-73　“系统配置”对话框

Step03 单击“确定”按钮，即可进入系统的安全模式，如图 2-74 所示。

Step04 进入安全模式后，即可运行杀毒软件，进行病毒的查杀，如图 2-75 所示。

图 2-74　系统安全模式

图 2-75　查杀病毒

第 3 章

DOS 窗口与 DOS 命令

熟练掌握 DOS 系统常用的命令是进行网络渗透测试的基本功，只有熟悉和掌握了这些命令，才可以为日后进行网络渗透测试提供便利。本章就来介绍 Windows 系统自带的 DOS 命令。

3.1 认识系统中的 DOS 窗口

Windows 10 操作系统中的 DOS 窗口，也称为“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。

微视频

3.1.1 使用菜单的形式进入 DOS 窗口

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 单击桌面上的“开始”菜单，在弹出的菜单列表中选择 Windows →“命令提示符”命令，如图 3-1 所示。

Step 02 随即弹出“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”命令

图 3-2 “管理员 : 命令提示符”窗口

微视频

3.1.2 运行“运行”对话框进入 DOS 窗口

除使用菜单的形式进入 DOS 窗口外，用户还可以运用“运行”对话框进入 DOS 窗口，具体的操作步骤如下。

Step01 在 Windows 10 操作系统中，右击桌面上的“开始”菜单，在弹出的快捷菜单中选择“运行”命令。随即弹出“运行”对话框，在“打开”文本框中输入“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。

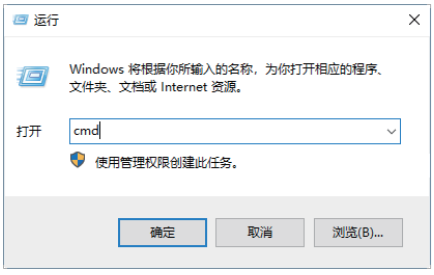

图 3-3　“运行”对话框

图 3-4　DOS 窗口

3.1.3　通过浏览器进入 DOS 窗口

微视频

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 操作系统中访问 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。

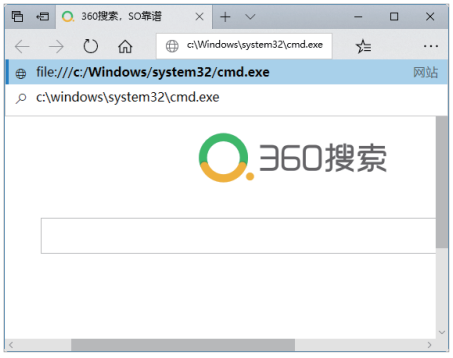

图 3-5　Microsoft Edge 浏览器

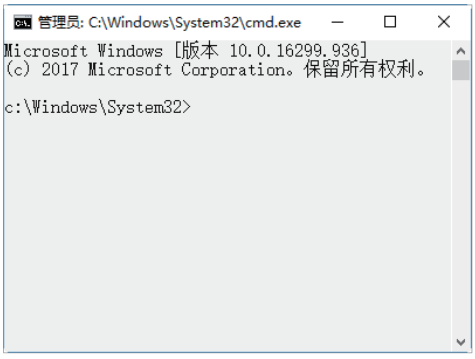

图 3-6　DOS 运行窗口

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

3.1.4　编辑命令提示符窗口中的代码

微视频

当在 Windows 10 中启动命令行时，就会弹出相应的命令行窗口，在其中显示当前操作系统的版本号，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。

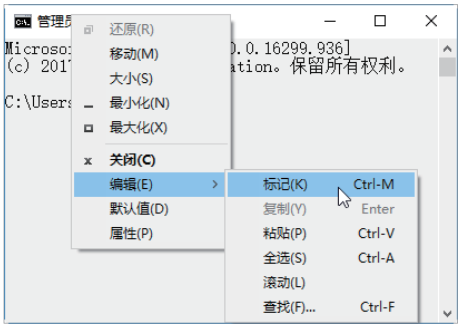

图 3-7 “标记”选项

图 3-8 “复制”选项

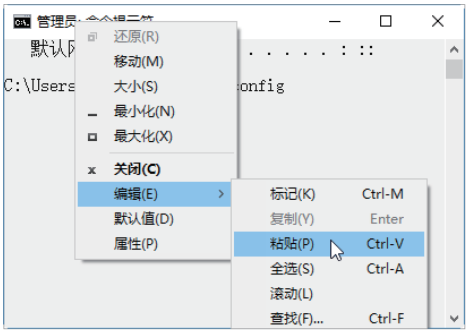

图 3-9 “粘贴”选项

Step03 在需要粘贴该命令行的位置处右击，即可完成粘贴操作，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。

提示：当然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。

微视频

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，在弹出菜单中选择“属性”选项，即可打开“‘命令提示符’属性”对话框，如图 3-10 所示。

Step02 打开“颜色”选项卡，在其中可以对相关选项进行颜色设置。选择“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 “命令提示符”属性

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，即可保存设置，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

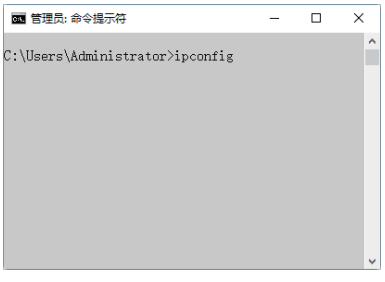

图 3-15　自定义显示风格

3.2　常见 DOS 命令的应用

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。


微视频

3.2.1 切换当前目录路径的 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 命令主要有以下三种使用方法。

（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:\Win- dows，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。

Step01 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:\，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。

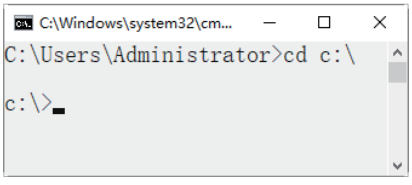

图 3-16 目录切换到 C:\

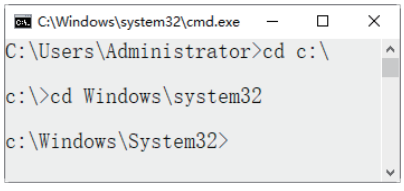

图 3-17 切换到 C 盘子目录

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，如图 3-19 所示。

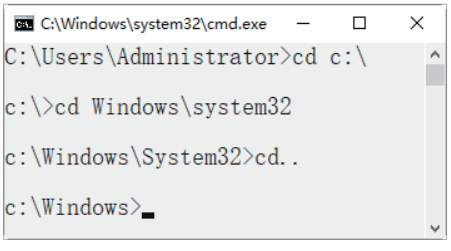

图 3-18 返回上一级目录

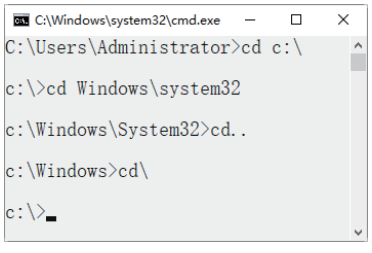

图 3-19 返回根目录


微视频

3.2.2 列出磁盘目录文件的 dir 命令

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。

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，具体操作步骤如下。

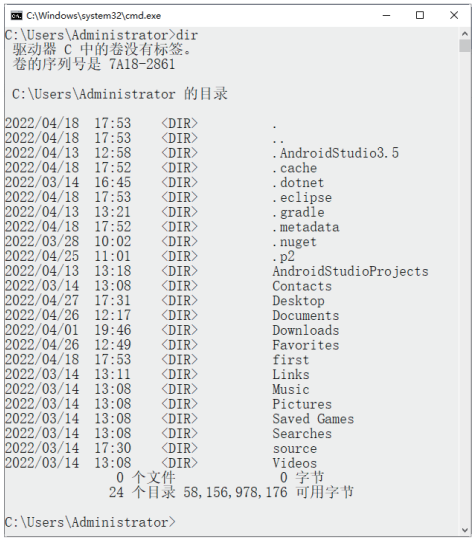

图 3-20　Administrator 目录下的文件列表

Step01 在“命令提示符”窗口中输入 dir 命令，按 Enter 键，即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，即可查看 D 盘下的所有文件的目录，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，即可列出 c:\windows 目录下的隐藏文件，如图 3-22 所示。

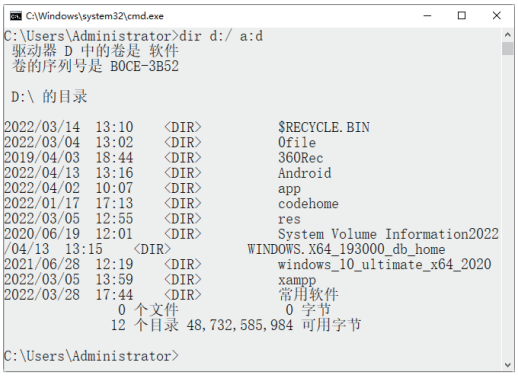

图 3-21　D 盘下的文件列表

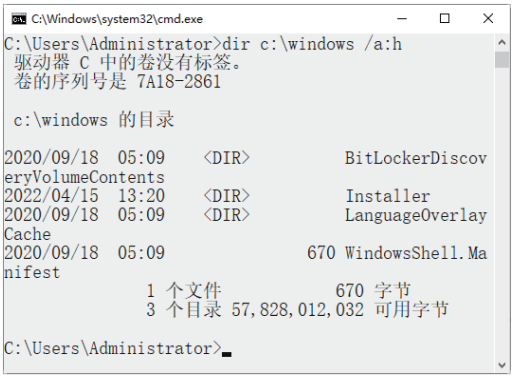

图 3-22　C 盘下的隐藏文件

3.2.3　检查计算机连接状态的 ping 命令

微视频

ping 命令是 TCP/IP 协议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。

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。

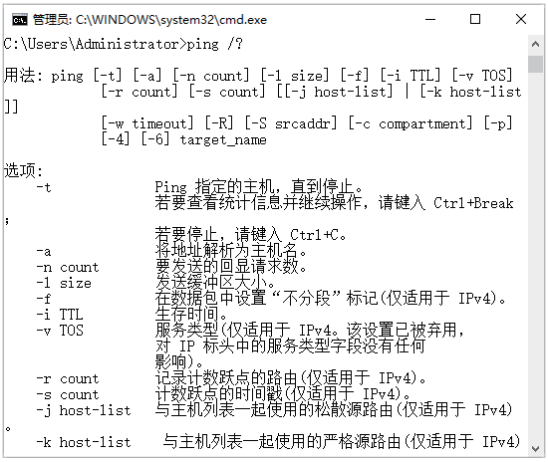

图 3-23　ping 命令的帮助信息

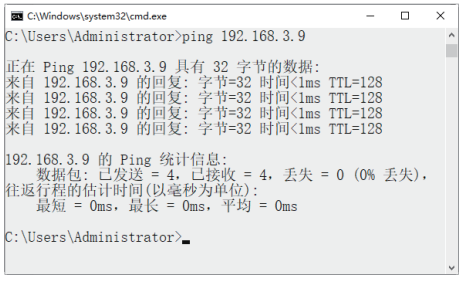

图 3-24　判断计算机的操作系统类型

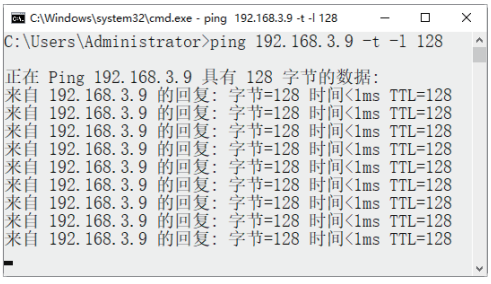

图 3-25　发出大量数据包

Step 03 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。

Step 04 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-20220314S0IE。

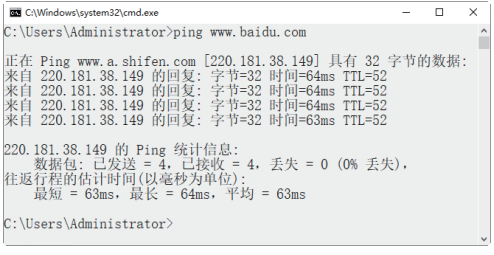

图 3-26　网络连通信息

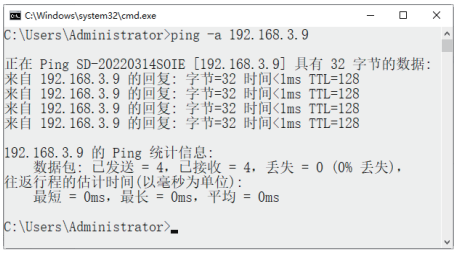

图 3-27　解析某 IP 地址的计算机名


微视频

3.2.4　查询网络状态与共享资源的 net 命令

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，则在打开的“命令提示符”窗口中显示计算机启动的 Windows 服务，如图 3-29 所示。

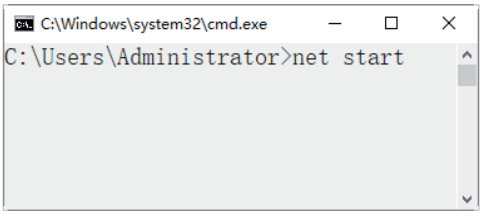

图 3-28　输入 net start 命令

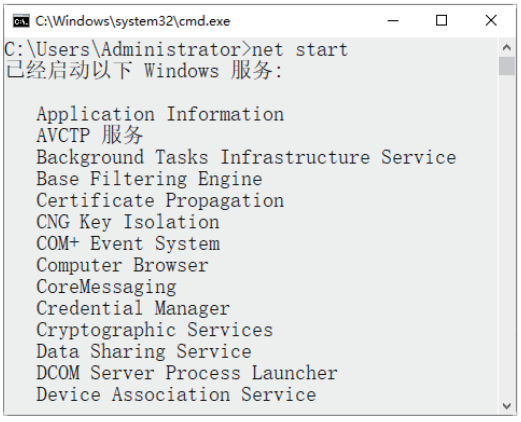

图 3-29　计算机启动的 Windows 服务

3.2.5　显示网络连接信息的 netstat 命令

微视频

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，可以让用户得知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/?”，可以得到这条命令的帮助信息，如图 3-30 所示。

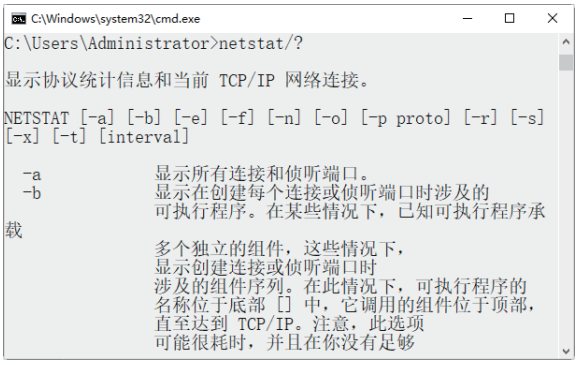

图 3-30　netstat 命令帮助信息

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：显示所有连接和侦听端口。
- -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，即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，即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

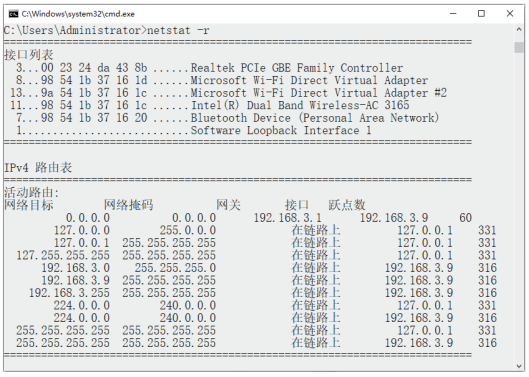

图 3-32　查看本机路由信息

Step03 在“命令提示符”窗口中输入“netstat -a”命令，按 Enter 键，即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，即可显示本机所有连接的端口及其状态，如图 3-34 所示。

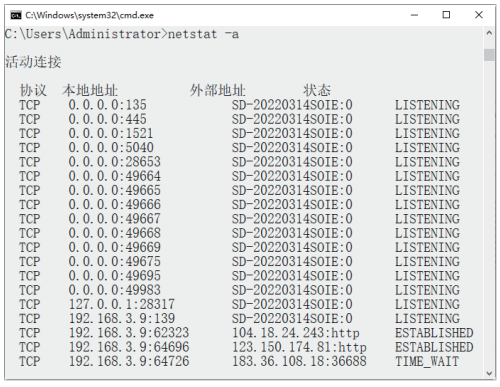

图 3-33　查看本机活动的 TCP 连接

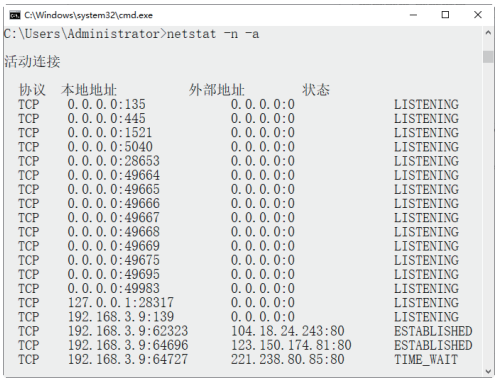

图 3-34　查看本机连接的端口及其状态


微视频

3.2.6　检查网络路由节点的 tracert 命令

使用 tracert 命令可以查看网络中的路由节点信息，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。

例如：如果想查看 www.baidu.com 的路由与局域网络连接情况，则在“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。

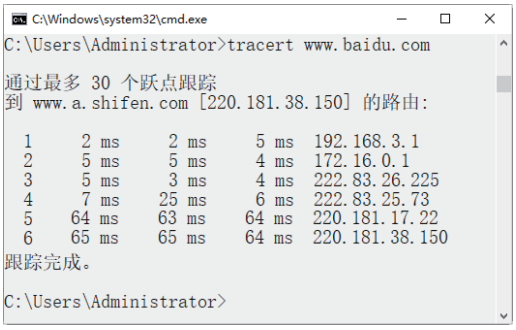

图 3-35　查看网络中路由节点信息

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，则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，其有效值为 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。

Step 01 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 # 和内存使用等 5 部分。

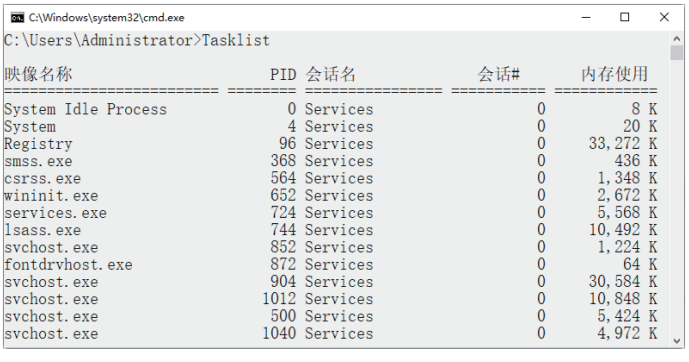

图 3-36　查看本机进程

Step02 Tasklist 命令不但可以用来查看系统进程，而且还可以用来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，在命令提示符下输入“Tasklist /svc”命令即可，如图 3-37 所示。

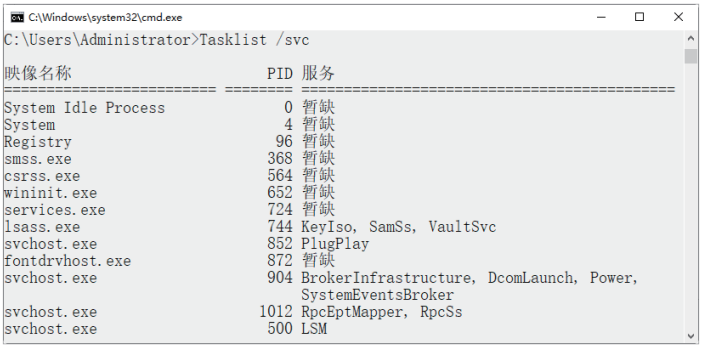

图 3-37　查看本机进程 svchost.exe 提供的服务

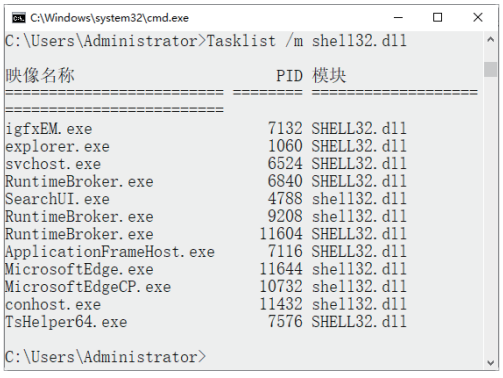

图 3-38　显示调用 shell32.dll 模块的进程

Step03 要查看本地系统中哪些进程调用了 shell32.dll 模块文件，只需在命令提示符下输入“Tasklist /m shell32.dll”即可显示这些进程的列表，如图 3-38 所示。

Step04 使用筛选器可以查找指定的进程，在命令提示符下输入“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”。

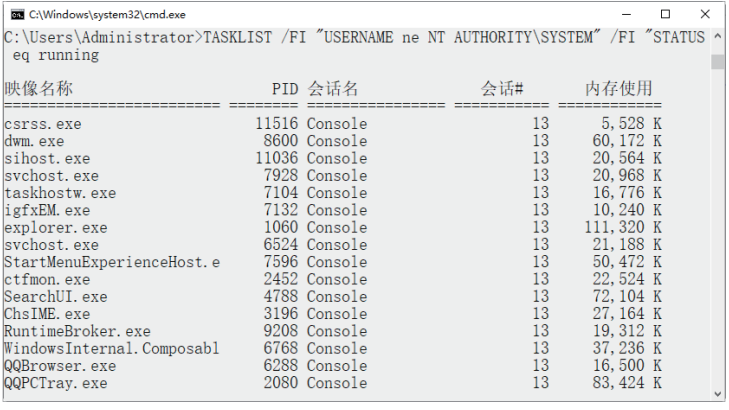

图 3-39　列出系统中正在运行的非 SYSTEM 状态的所有进程

3.3　实战演练

3.3.1　实战 1：使用命令清除系统垃圾


微视频

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。

Step01 打开记事本文件，在其中输入可以清除系统垃圾的代码：

```
@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，就可以快速清理系统垃圾，如图 3-41 所示。

图 3-40　编辑代码

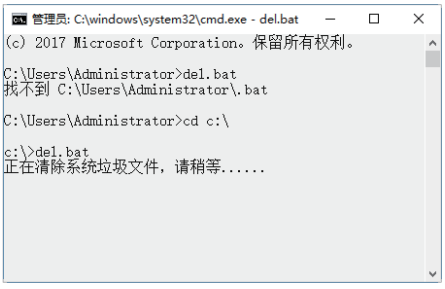

图 3-41　自动清理垃圾

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。

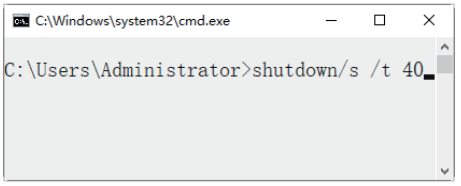

图 3-42　输入 shutdown/s /t 40 命令

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“命令提示符”窗口中输入命令“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