第1章　Web渗透测试快速入门

随着信息时代的发展和网络的普及，越来越多的人走进了网络生活，然而人们在享受网络带来的便利的同时，也时刻面临着黑客们残酷攻击的危险。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 Web 渗透测试知识。

1.1　认识 Web 安全

随着社交网络、微博、微信等一系列新型的互联网产品的诞生，基于 Web 环境的互联网应用越来越广泛，企业信息化的过程中各种应用都架设在 Web 平台上，Web 业务的迅速发展也引起了黑客的强烈关注，接踵而至的就是 Web 安全问题。

1.1.1　Web 安全的提出

在 Web 安全问题中，常见的就是黑客利用操作系统的漏洞和 Web 服务程序的 SQL 注入漏洞等得到 Web 服务器的控制权限，轻则篡改网页内容，重则窃取重要内容数据，更为严重的则是在网页中植入恶意代码，使得网站访问者受到侵害，这也使得越来越多的用户关注应用层的安全问题，对 Web 应用安全的关注度也逐渐升温，“Web 安全”的概念由此而提出。

最初，Web 安全主要是指计算机安全。不过，随着 Java 语言的普及，利用 Java 语言进行传播和资料获取的病毒开始出现，最为典型的代表就是 Java Snake 病毒，还有一些利用邮件服务器传播和破坏的病毒，这些病毒会严重影响互联网的效率。

进入 21 世纪以来，随着互联网的飞速发展，各种 Web 应用开始增多，“计算机安全”逐步演化为“计算机信息系统安全”。这时，“安全”的概念也不再仅仅是计算机本身的安全，也包括软件与信息内容的安全。

1.1.2　Web 安全的发展历程

通俗地讲，互联网就是网络与网络之间串连成的庞大网络，自互联网诞生起，互联网的发展大致经历了三个阶段，分别为：Web 1.0、Web 2.0 和 Web 3.0。相对应地，Web 安全的发展历程也经历了三个阶段。

1. 宣传启蒙阶段

第一代互联网 Web 1.0。从 1995 年至 2005 年，大约十年的时间，Web 1.0 是只读互联网，用户只能收集、浏览和读取信息，网络的编辑管理权限掌握在开发者手中，用户只能被动获取信息，网络提供什么，用户就只能看到什么，只能做一个读者。Web 1.0 是平台向用户的单向传播模式，它的表现形式是各种各样的门户网站，比如 Google、网易、百度、搜狐、新浪等。如图 1-1 所示为百度首页。

在此阶段，Web 安全主要是指计算机的实体安全。而且这一阶段国家也没有相关的法律法规，更没有较为完整意义的专门针对计算机系统安全方面的规章，安全标准也比较少，只是在物理安全及保密通信等个别环节上有些规定；广大应用部

门也基本上没有意识到计算机安全的重要性，只在个别部门中少数有些计算机安全意识的人们开始在实际工作中进行摸索。

图 1-1　百度首页

2. 开始发展阶段

第二代互联网 Web 2.0。Web 2.0 在 2005 年初具雏形，大规模应用是在 2014 年，Web 2.0 是可读写、交互的互联网，用户不仅可以读取信息，还可以转发、分享、评论、互动等，同时还可以自己创建文字、图片和视频，并上传到网上。

Web 2.0 真正实现了用户与用户之间的双向互动，让每一个用户不再仅仅是互联网的读者，同时也成为互联网的作者。Web 2.0 的具体表现形式是各类的 App，比如 QQ、微信、抖音等，但这些 App 的开发商都是中心化的机构，用户发布的内容都是存储在开发商的数据库里，很容易出现网络安全问题，比如信息丢失、泄露，这也是这一阶段的 Web 安全最需要解决的问题。如图 1-2 所示为微信好友聊天界面。

在此阶段，Web 安全逐渐被人们重视起来。许多企事业单位开始把信息安全作为系统建设中的重要内容之一来对待，加大了投入，开始建立专门的安全部门来开展信息安全工作。还有一个重要的变化就是一些学校和研究机构开始将信息安全作为大学教程和研究课题，安全人才的培养开始起步。这也是我国安全产业发展的重要标志。

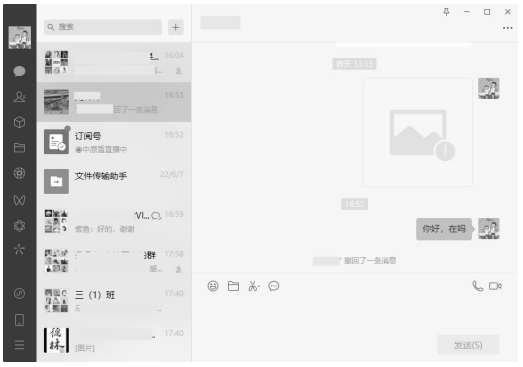

图 1-2　微信好友聊天界面

3. 逐步正规阶段

第三代互联网 Web 3.0。与 Web 1.0 和 Web 2.0 相比，Web 3.0 最大的不同是去中心化。说到去中心化，就会想到区块链，Web 3.0 是基于区块链技术建立的点对点的去中心化的智能互联网。目前处于基础建设时期，包括分布式存储、物联网、生态公链、云计算等方面，Web 3.0 将区块链的加密、不可篡改、点对点传输和共识算法技术添加到应用程序中，开发出去中心化的应用程序 DAPP。如图 1-3 所示为物联网相关示意图。

图 1-3　物联网示意图

Web 3.0 将更加以人为本，更加倾向于保护隐私，将数据回归到个人所有，逐渐摆脱中心化机构的控制。当下正处于 Web 2.0 和 Web 3.0 的交接阶段，新的时代必定带来新的机遇。

在此阶段，随着互联网的高速发展，

我国安全产业进入快速发展阶段，逐步走向正轨。而标志安全产业走向正轨的重要特征，就是国家高层领导开始重视信息安全工作，并为此出台了一系列重要政策和措施。

纵观多年的安全发展史，我们不难发现，其实一直都是安全在被动局面下的转变过程。面对安全威胁的层出不穷，想做到安全的主动防御是相当困难的，因此必须保持这种动态发展规则，了解安全本身的发展和变化，才能采取正确的对策。

1.1.3　Web 安全的发展现状

“没有网络安全就没有国家安全”。可以看出，网络安全已经全面渗透到政治、经济、文化等领域。高度重视网络安全力量建设已经成为维护网络空间主权、安全和发展利益的必由之路。

随着各行各业信息化的不断推进，互联网的不安全因素也在逐日扩张，病毒木马、垃圾邮件、间谍软件等也在困扰着所有网络用户，这也让企业认识到网络安全的重要性。然而在网络安全产品的选择上，很多企业却显得无所适从，因为目前的网络安全市场正可谓是群雄并起、各成一家。这一现象表明，目前的网络安全市场似乎还未走上成熟。

尽管网络安全产品市场错综复杂，但是网络安全市场的增长是有目共睹的。从国内市场上看，由于目前网络安全行业还未出现领导者，专业公司比较少，整个行业呈现一片蓬勃的生机。另外，网络安全核心技术具有的较大的不可模仿性，使得行业从整体上看仍然属于卖方市场，这也是目前 Web 安全的发展现状。

1.2　什么是 Web 渗透测试

Web 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的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 Web 渗透测试的实施步骤与各种攻击方式。

1.2.1　认识 Web 渗透测试

Web 渗透测试主要是对 Web 应用程序和相应的软硬件设备配置的安全性进行测试，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。

进行 Web 渗透测试的安全人员必须遵循一定的渗透测试准则，不能对被测系统进行破坏活动。Web 安全渗透测试一般是经过客户授权的。

1.2.2　Web 渗透测试的分类

实际上，Web 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

根据渗透方法进行分类，渗透测试 / 攻击可分为以下两类。

（1）黑盒（Black Box）渗透

黑盒（Black Box）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。

（2）白盒（White Box）渗透

白盒（White Box）渗透测试又被称为“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

根据渗透测试目标分类，渗透测试又可分为以下几种。

（1）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。

（2）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。

（3）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。

（4）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。

（5）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来分，渗透测试可分为下面两类。

（1）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。

（2）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。

1.2.3 渗透攻击与普通攻击的不同

渗透攻击与普通攻击的不同在于：普通的攻击只是单一类型的攻击；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，而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，渗透攻击与普通攻击相比，渗透攻击具有攻击目的明确性、攻击手段多样性和综合性等特点。

1.3　Web 应用程序概述

Web应用程序是一种利用网络浏览器和网络技术在互联网上执行任务的计算机程序。本节就来介绍什么是Web应用程序。

1.3.1　认识 Web 应用程序

Web应用程序使用服务器端脚本（PHP和ASP）的组合来处理信息的存储和检索，并使用客户端脚本（JavaScript和HTML）将信息呈现给用户。常见的Web应用程序有在线表单、内容管理系统、购物车等，通过这些应用程序可以与公司互动。此外，这些应用程序还允许用户创建文档、共享信息、协作项目以及在共同的文档上工作，而不受地点或设备的限制。

Web应用程序通常用浏览器支持的语言（例如JavaScript和HTML）来编写，因为这些语言依赖浏览器来呈现程序可执行文件。一些应用程序是动态的，需要服务器端处理，一些应用程序则完全是静态的，无须在服务器上进行任何处理。

通常情况下，Web应用程序需要一个Web服务器来管理来自客户端的请求，一个应用服务器来执行所请求的任务，有时还需要一个数据库来存储信息。

下面是一个典型的Web应用程序使用流程。

（1）用户通过网络浏览器或应用程序的用户界面，通过互联网触发对网络服务器的请求。

（2）Web服务器将此请求转发到适当的Web服务器。

（3）Web服务器执行请求任务（例如查询数据库、处理数据），然后生成请求数据的结果。

（4）Web服务器将处理后的数据或请求的信息或已处理过的数据发送到Web服务器。

（5）Web服务器用所请求的信息响应客户端，该信息随后出现在用户的显示屏上。

总之，Web应用程序的真正核心主要是用户的业务需求和对数据库进行处理，比如管理信息系统（Management Information System，MIS）就是这种架构最典型的应用。

1.3.2　Web 应用程序的好处

使用Web应用程序的好处如下：

（1）只要浏览器兼容，Web应用程序可以在多个平台上运行，不受操作系统或设备的影响。

（2）所有用户都访问同一版本，消除了所有兼容性问题。

（3）Web应用程序并未安装在硬盘驱动器上，因此消除了空间限制。

（4）Web应用程序降低了企业和最终用户的成本，因为企业所需的支持和维护更少，对最终用户的计算机的要求也更低。

1.4　Web 应用程序的组件及架构

Web应用程序架构展示了包含所有组件（例如数据库、应用程序和中间件）以

及它们如何相互交互的布局。它定义了数据如何通过 HTTP 传递，并确保客户端服务器和后端服务器能够理解。

1.4.1 Web 应用程序架构组件

Web 应用程序架构确保所有用户请求中都存在有效数据，它创建和管理记录，同时提供基于权限的访问和身份验证。

通常，基于 Web 的应用程序架构包括三个核心组件。

（1）Web 浏览器：浏览器或客户端组件或前端组件是与用户交互、接收输入并管理表示逻辑同时控制用户与应用程序交互的关键组件。如果需要，也会验证用户输入。

（2）Web 服务器：Web 服务器也称为后端组件或服务器端组件，通过将请求路由到正确的组件并管理整个应用程序操作来处理业务逻辑和用户请求。它可以运行和监督来自各种客户端的请求。

（3）数据库服务器：数据库服务器为应用程序提供所需的数据，它处理与数据相关的任务。

1.4.2 Web 应用程序架构的类型

Web 应用程序的体系结构可以根据软件开发和部署模式分为不同的类别。下面介绍几种常见的 Web 应用程序架构类型。

1. 单体架构

单体架构是一种传统的软件开发模型，也称为 Web 开发架构。整个软件开发为通过传统瀑布模型的单个代码。这意味着所有组件都是相互依赖和互连的，并且每个组件都需要运行应用程序。要更改或更新特定功能，需要更改要重写和编译的整个代码。

由于单体架构将整个代码视为一个程序，因此构建新项目、应用框架、脚本、模板和测试变得简单易行，部署也很容易。但是，随着代码越来越大，管理或更新变得困难。即使是很小的变化，也需要经历 Web 开发架构的整个过程。由于每个元素都是相互依赖的，因此扩展应用程序并不容易。此外，单体架构不可靠，因为单点故障可能会导致应用程序崩溃。

2. 微服务架构

微服务架构解决了单体环境中遇到的几个挑战。在微服务架构中，每个微服务都包含自己的数据库并运行特定的业务，这意味着用户可以轻松开发和部署独立的服务。微服务架构提供了更新、修改和扩展独立服务的灵活性，这使得开发变得简单高效，对于高度可扩展和复杂的应用程序，微服务是一个不错的选择。

微服务架构也有缺点，在运行时部署多个服务是一项挑战。当服务数量增加时，管理它们的复杂性也会增加。此外，微服务应用程序共享分区数据库。这意味着用户需要确保受事务影响的多个数据库之间的一致性。

3. 集装箱架构

集装箱架构也被称为容器技术，它是部署微服务的最佳选择。容器是对可以在计算机或虚拟机上运行的应用程序的轻量级运行环境的封装。因此，应用程序在从开发人员设备到生产环境的一致环境中运行。通过在操作系统级别抽象执行，容器化允许用户在单个操作系统实例中运行多个容器。在减少开销和提升处理能力的同时，它也提高了效率。

4. 无服务器架构

无服务器架构是开发软件应用程序的模型。在此结构中，底层基础设施的供应由基础设施服务提供商管理。这意味着用户只需为使用中的基础架构付费，而不是为空闲 CPU 时间或未使用的空间付费。

无服务器计算降低了成本，因为资源

仅在应用程序执行时使用。缩放任务由云提供商处理。此外，后端代码得到简化，这样减少了开发工作和成本，并缩短了上市时间。常见的多媒体处理、直播、聊天机器人、物联网传感器消息等都是无服务器计算的一些应用实例。

1.5　渗透测试的流程

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定渗透入侵的方案，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 1-4 所示为攻击者渗透入侵的几个阶段。

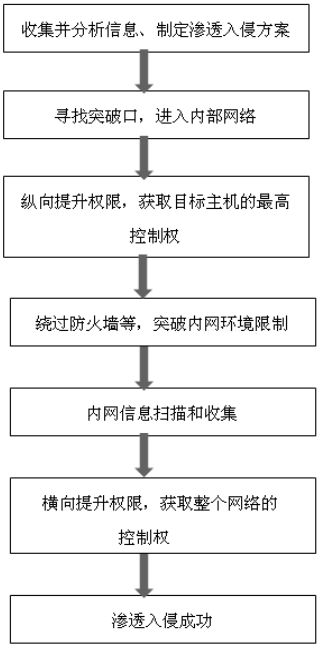

图 1-4　渗透入侵的几个阶段

1. 收集并分析信息、制定渗透入侵方案

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的一些小小的漏洞、开放的端口等。

（1）信息收集

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 等服务。

（2）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。

（3）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 脚本入侵和木马攻击。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，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. 内网信息扫描和收集

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

经过上述的操作步骤，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的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。

1.6　实战演练

1.6.1　实战 1：查找 IP 地址与 MAC 地址

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

1. IP地址

使用 ipconfig 命令可以获取本地计算机的 IP 地址和物理地址，具体的操作步骤如下。

Step 01 右击“开始”按钮，在弹出的快捷菜单中执行“运行”命令，如图 1-5 所示。

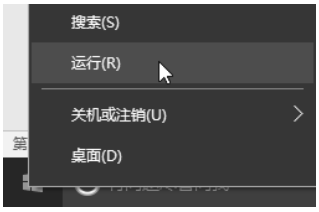

图 1-5　“运行”菜单

Step 02 打开“运行”对话框，在“打开”后面的文本框中输入“cmd”命令，如图 1-6 所示。

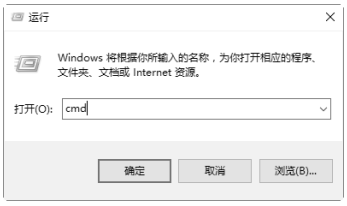

图 1-6　输入“cmd”命令

Step 03 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 1-7 所示。

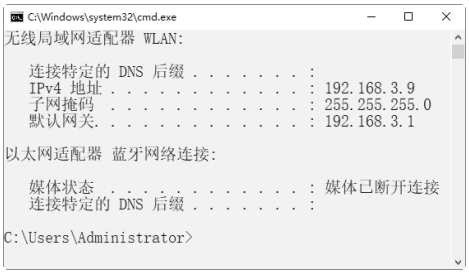

图 1-7　查看 IP 地址

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。

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在硬件内部。MAC 地址与网络无关，也即无论将带有这个地址的硬件（如网卡、集线器、路由器等）接入网络的何处，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“-”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，这就是用户自己的计算机的网卡地址，它是唯一的，如图 1-8 所示。

图 1-8　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用不同的地址。

1.6.2　实战 2：获取系统进程信息

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：

Step 01 在 Windows 10 系统桌面中，单击“开始”按钮，在弹出的菜单列表中选择“任务管理器”菜单命令，如图 1-9 所示。

图 1-9 “任务管理器”菜单命令

Step 02 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 1-10 所示。

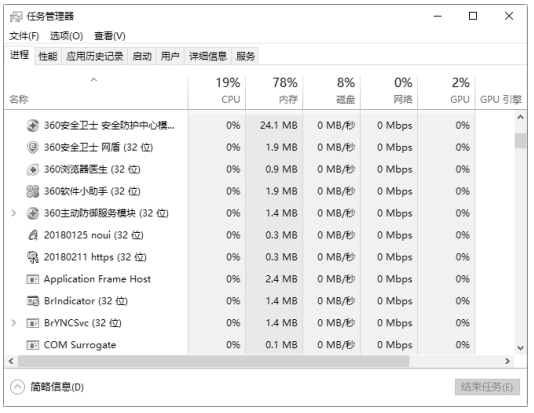

图 1-10 “任务管理器”窗口

提示：通过在 Windows 10 系统桌面上，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。

第2章　搭建Web渗透测试环境

安全测试环境是安全工作者需要了解和掌握的内容。对于Web安全初学者来说，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，这就需要通过搭建Web安全测试环境来解决这个问题。本章就来介绍Web渗透测试环境的搭建。

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，也被称作为安全测试环境。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　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　什么是虚拟系统

虚拟系统就是在现有操作系统的基础上，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。

（1）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。

（2）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。

（3）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　安装与创建虚拟机

使用虚拟机构建渗透测试环境是一个非常好的选择，本节介绍安装与创建虚拟机的方法。

2.2.1　下载虚拟机软件

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：

Step 01 使用浏览器打开虚拟机官方网站https:

//www.vmware.com/products/workstation-pro/workstation-pro-evaluation.html，进入虚拟机软件下载页面，如图 2-1 所示。

图 2-1　虚拟机软件下载页面

Step 02 在下载页面找到“Workstation 17 Pro for Windows”对应选项，单击下方的“DOWNLOAD NOW”超链接，开始下载，如图 2-2 所示。

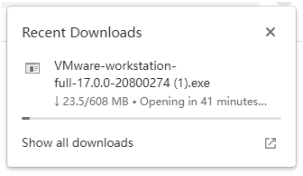

图 2-2　开始下载

2.2.2　安装虚拟机软件

虚拟机软件下载完成后，接下来就可以安装了。安装虚拟机的具体操作步骤如下：

Step 01 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 2-3 所示。

图 2-3 “安装向导”窗口

Step 02 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 2-4 所示。

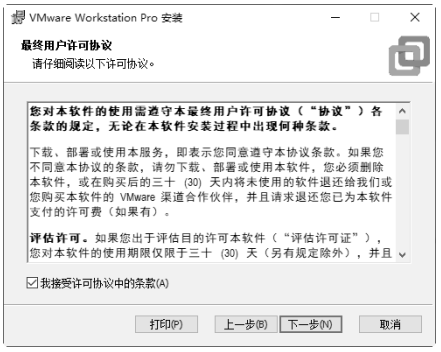

图 2-4 “最终用户许可协议”窗口

Step 03 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 2-5 所示。

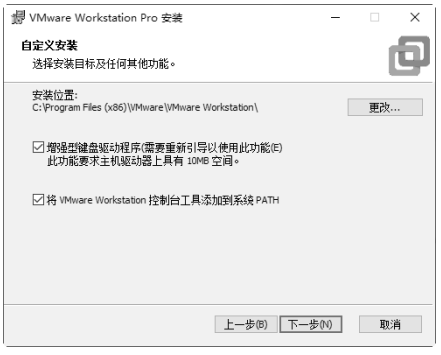

图 2-5 “自定义安装”窗口

Step 04 单击“下一步”按钮，进入“用户体验设置”窗口，这里采用系统默认设置，如图 2-6 所示。

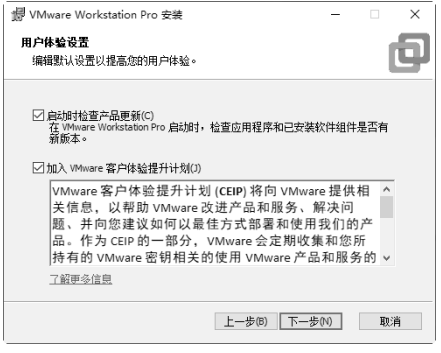

图 2-6 “用户体验设置”窗口

Step 05 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，这里保持默认设置，如图 2-7 所示。

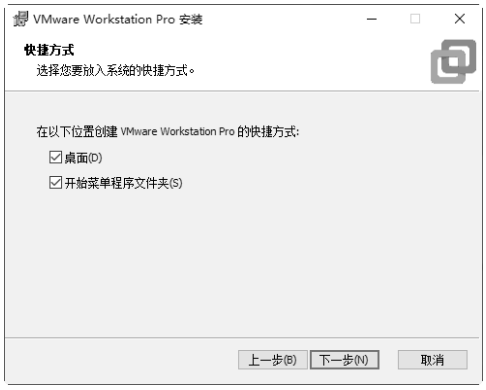

图 2-7 “快捷方式”窗口

Step 06 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 2-8 所示。

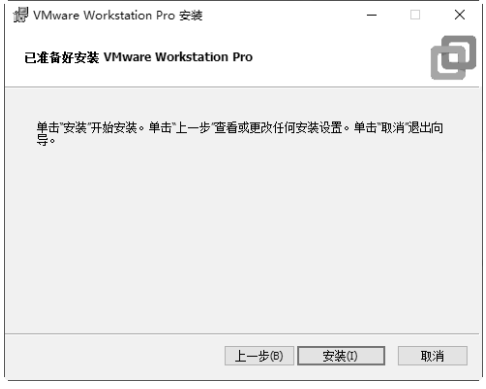

图 2-8 “已准备好安装 VMware Workstation Pro”窗口

Step 07 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 2-9 所示。

Step 08 虚拟机安装完成后，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 2-10 所示。

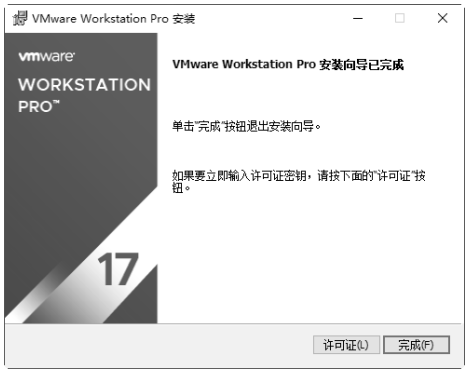

图 2-9 “VMware Workstation Pro 安装向导已完成”窗口

图 2-10　重新启动系统

2.2.3　创建虚拟机系统

安装完虚拟机以后，就需要创建一台真正的虚拟机，为后续的测试系统做准备。创建虚拟机的具体操作步骤如下：

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 2-11 所示。

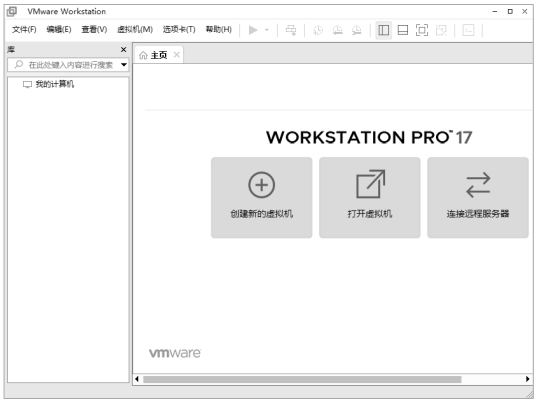

图 2-11　VMware 虚拟机软件

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，在其中选中“自定义”单选按钮，如图 2-12 所示。

图 2-12 “新建虚拟机向导”对话框

Step 03 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 2-13 所示。

图 2-13 “选择虚拟机硬件兼容性”对话框

Step 04 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 2-14 所示。

图 2-14 “安装客户机操作系统”对话框

Step 05 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“Linux”单选按钮，如图 2-15 所示。

图 2-15 “选择客户机操作系统”对话框

Step 06 单击“版本”下方的下拉按钮，在弹出的下拉列表中选择“其他 Linux 5.x 内核 64 位”版本系统，这里的系统版本与主机系统版本无关，可以自由选择，如图 2-16 所示。

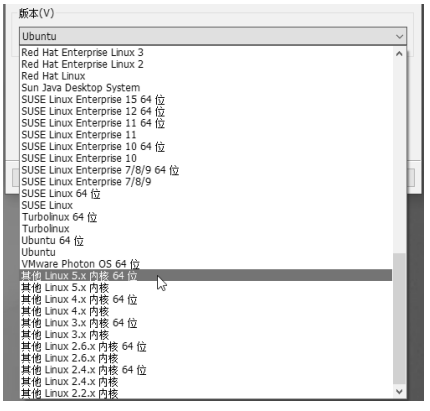

图 2-16 选择系统版本

Step 07 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 2-17 所示。

Step 08 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 2-18 所示。

图 2-17 “命名虚拟机”对话框

图 2-18 “处理器配置”对话框

Step 09 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 2048MB（即 2GB）内存，如图 2-19 所示。

图 2-19 “此虚拟机的内存”对话框

Step 10 单击“下一步”按钮，进入“网络类型”对话框，这里选中“使用网络地址转换（NAT）”单选按钮，如图 2-20 所示。

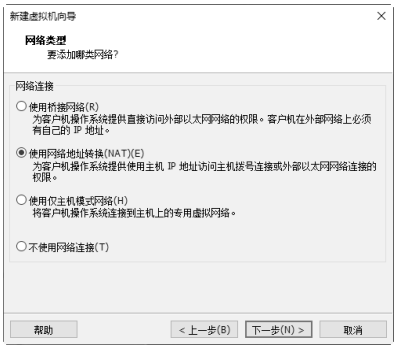

图 2-20 “网络类型”对话框

Step 11 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”单选按钮，如图 2-21 所示。

图 2-21 “选择 I/O 控制器类型”对话框

Step 12 单击“下一步”按钮，进入“选择磁盘类型”对话框，这里选中“SCSI”单选按钮，如图 2-22 所示。

图 2-22 “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，这里选中“创建新虚拟磁盘”单选按钮，如图 2-23 所示。

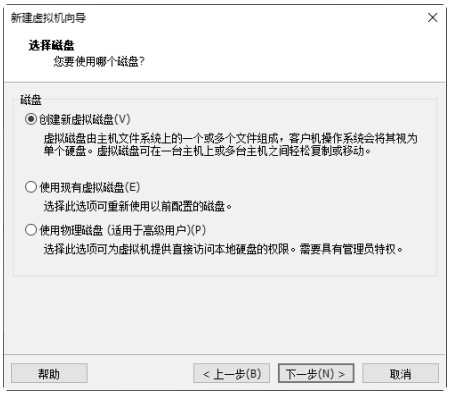

图 2-23 “选择磁盘”对话框

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 8GB 空间即可，选中“将虚拟磁盘拆分成多个文件”单选按钮，如图 2-24 所示。

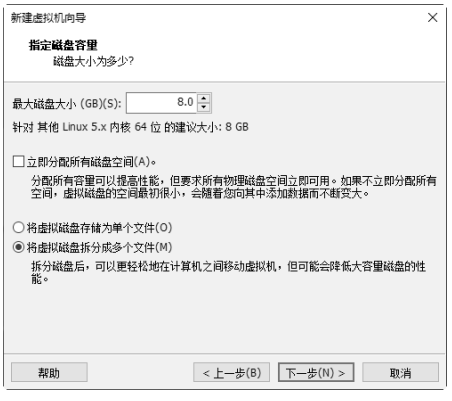

图 2-24 “指定磁盘容量”对话框

Step 15 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 2-25 所示。

Step 16 单击“下一步”按钮，进入“已准备好创建虚拟机”对话框，如图 2-26 所示。

Step 17 单击“完成”按钮，至此，便创建了一个新的虚拟机，如图 2-27 所示，这当中的硬件配置，可以根据实际需求再进行更改。

图 2-25 “指定磁盘文件”对话框

图 2-26 “已准备好创建虚拟机”对话框

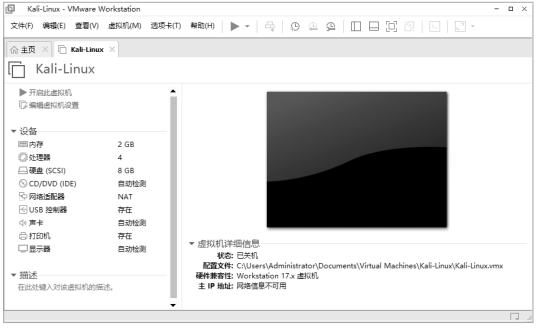

图 2-27 创建新虚拟机

2.3 安装 Kali Linux 操作系统

现实中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。本节介绍如何安装 Kali 操作系统。

2.3.1　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：

Step 01 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 2-28 所示。

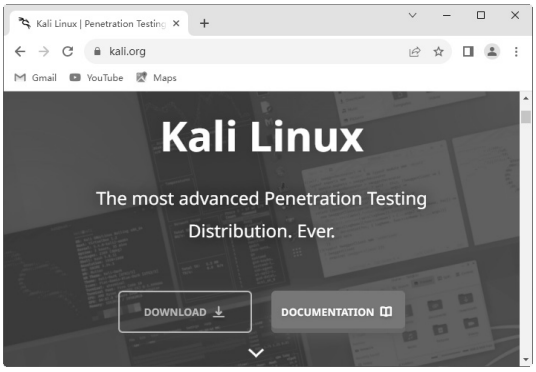

图 2-28　Kali 官方网站

Step 02 单击“Downloads”菜单，在弹出的菜单列表中选择 Kali Linux 版本，如图 2-29 所示。

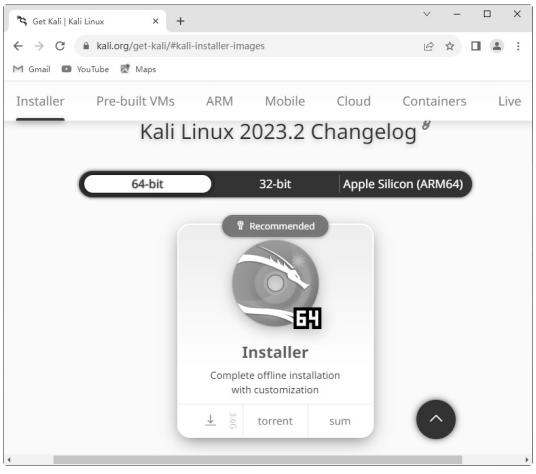

图 2-29　选择 Kali Linux 版本

Step 03 单击“⭳”按钮，即可开始下载 Kali Linux，并显示下载进度，如图 2-30 所示。

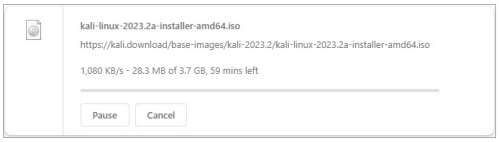

图 2-30　下载进度

2.3.2　安装 Kali Linux 系统

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 Linux 系统的具体操作步骤如下：

Step 01 打开安装好的虚拟机，单击“CD/DVD”选项，如图 2-31 所示。

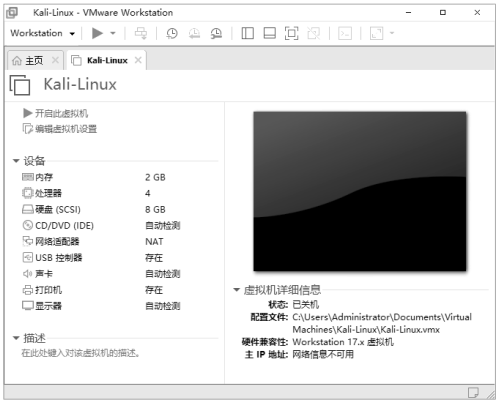

图 2-31　选择“CD/DVD”选项

Step 02 在打开的“虚拟机设置”页面中选中“使用 ISO 映像文件”单选按钮，如图 2-32 所示。

图 2-32　“虚拟机设置”对话框

Step 03 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 2-33 所示。

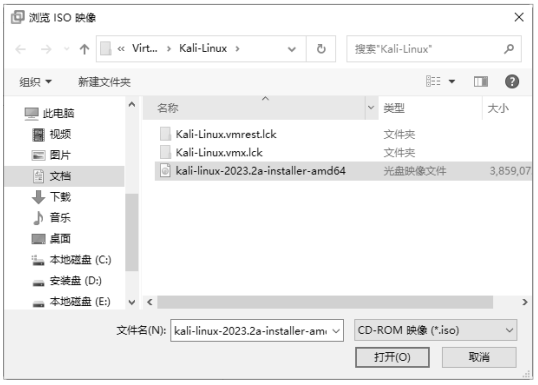

图 2-33 “浏览 ISO 映像”对话框

Step 04 单击“打开”按钮，返回到虚拟机设置页面，单击“开启此虚拟机”选项，便可以启动虚拟机，如图 2-34 所示。

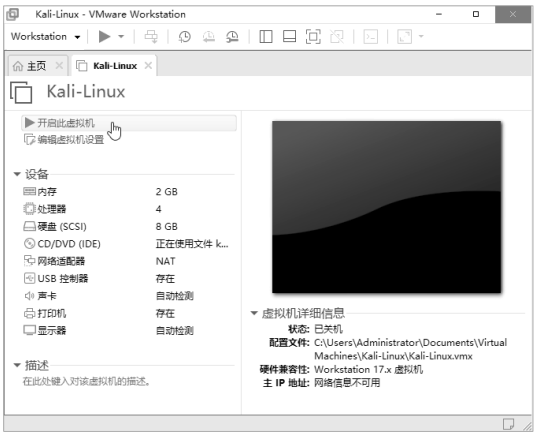

图 2-34 虚拟机设置页面

Step 05 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 2-35 所示。

Step 06 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 2-36 所示。

Step 07 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 2-37 所示。

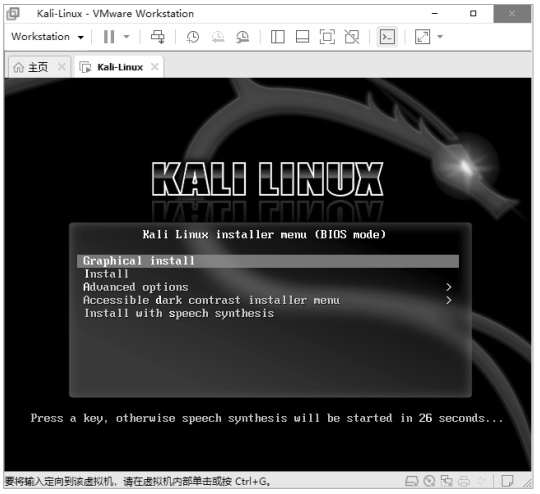

图 2-35 选择“Graphical install”选项

图 2-36 语言选择页面

图 2-37 语言确认页面

Step 08 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 2-38 所示。

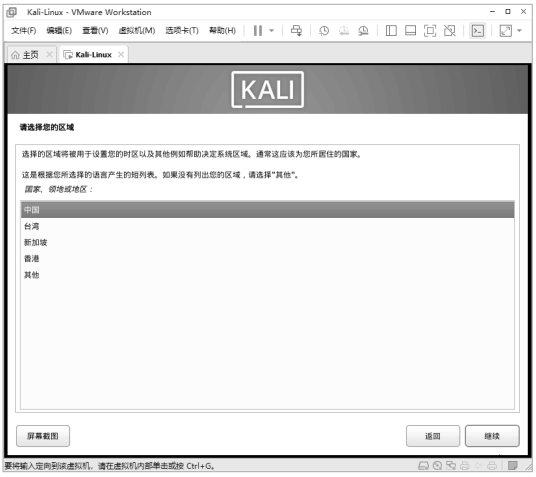

图 2-38 “请选择您的区域”页面

Step 09 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 2-39 所示。

图 2-39 “配置键盘”页面

Step 10 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。如图 2-40 所示为安装基本系统界面。

Step 11 系统安装完成后，会提示用户重启进入系统，如图 2-41 所示。

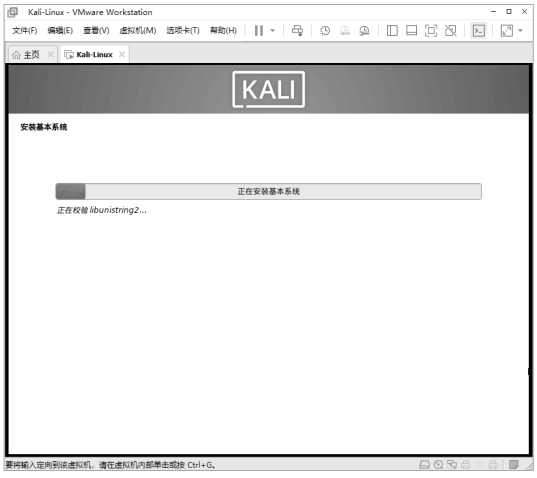

图 2-40　安装基本系统界面

图 2-41　安装完成

Step 12 按 Enter 键，安装完成后重启，进入“用户名”页面，在其中输入 root 管理员账号与密码，如图 2-42 所示。

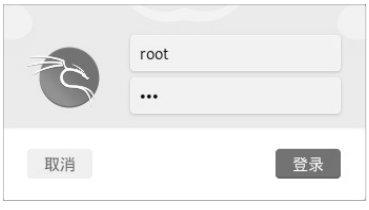

图 2-42 “用户名”页面

Step 13 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 2-43 所示。

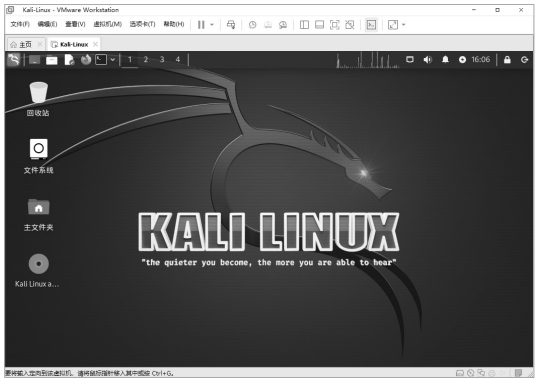

图 2-43　Kali Linux 系统页面

2.3.3　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。

Step 01 双击桌面上 Kali 系统的终端黑色图标，如图 2-44 所示。

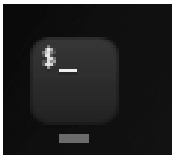

图 2-44　Kali 系统图标

Step 02 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 2-45 所示。

图 2-45　需要更新软件的列表

Step 03 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 2-46 所示。

图 2-46　“apt upgrade”命令

Step 04 运行命令后会有一个提示，此时按 Y 键，即可开始更新，更新中状态如图 2-47 所示。

图 2-47　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。

如果个别软件已经安装，存在升级版本问题，如图 2-48 所示。这时，可以先卸载旧版本，运行“apt-get remove < 软件名 >”命令，如图 2-49 所示，此时按 Y 键即可卸载。

图 2-48　升级版本问题

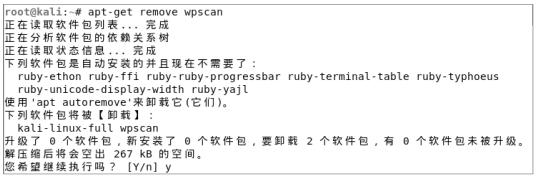

图 2-49　卸载旧版本

卸载完旧版本后，可以运行“apt-get install < 软件名 >”命令，如图 2-50 所示，此时按 Y 键即可开始安装新版本。

```
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 2-50　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 2-51 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 2-51　系统更新完成

2.4　安装 Windows 系统

在虚拟机中安装 Windows 操作系统是搭建网络安全测试环境最重要的步骤，本节介绍如何在虚拟机中安装 Windows 操作系统。

2.4.1　安装 Windows 操作系统

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 2-52 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，在其中选中“自定义”单选按钮，如图 2-53 所示。

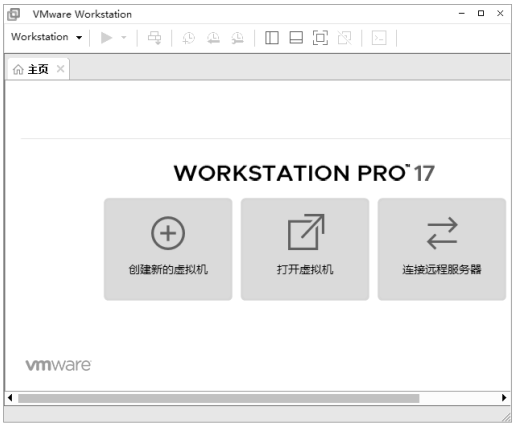

图 2-52　VMware 虚拟机软件

图 2-53　“新建虚拟机向导”对话框

Step 03 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 2-54 所示。

图 2-54　“选择虚拟机硬件兼容性”对话框

Step 04 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 2-55 所示。

图 2-55 “安装客户机操作系统”对话框

Step 05 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 2-56 所示。

图 2-56 “选择客户机操作系统”对话框

Step 06 单击“版本”下方的下拉菜单，在弹出的下拉列表中选择“Windows 10 x64”版本系统，这里的系统版本与主机系统版本无关，可以自由选择，如图 2-57 所示。

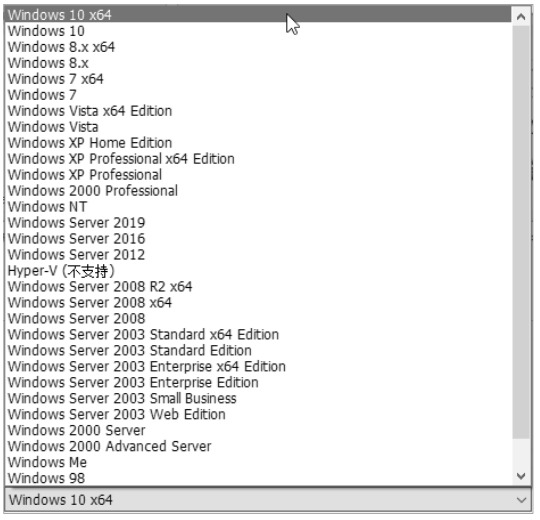

图 2-57 选择系统版本

Step 07 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 2-58 所示。

图 2-58 “命名虚拟机”对话框

Step 08 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 2-59 所示。

Step 09 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（即1GB）内存，如图2-60所示。

图2-59 “处理器配置”对话框

图2-60 “此虚拟机的内存”对话框

Step 10 单击“下一步”按钮，进入“网络类型”对话框，这里选中“使用网络地址转换（NAT）”单选按钮，如图2-61所示。

图2-61 “网络类型”对话框

Step 11 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2-62所示。

图2-62 “选择I/O控制器类型”对话框

Step 12 单击“下一步”按钮，进入“选择磁盘类型”对话框，这里选中“NVMe”单选按钮，如图2-63所示。

图2-63 “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，这里选中“创建新虚拟磁盘”单选按钮，如图2-64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“将虚拟盘拆分成多个文件”单选按钮，如图2-65所示。

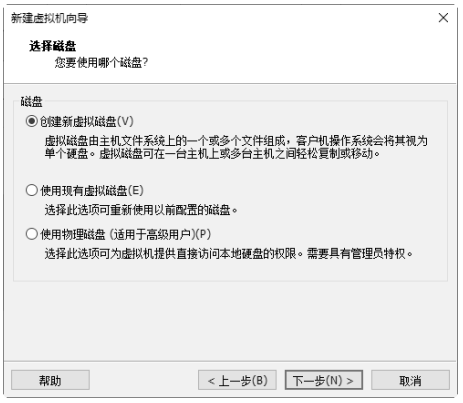

图 2-64 “选择磁盘”对话框

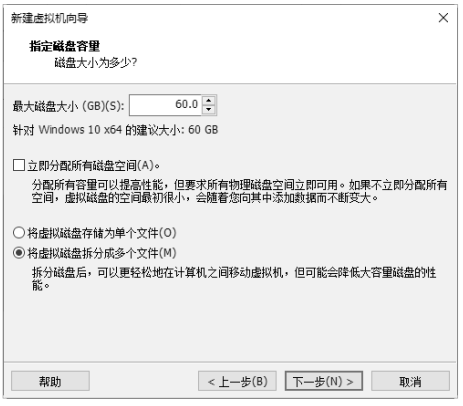

图 2-65 “指定磁盘容量”对话框

Step 15 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 2-66 所示。

图 2-66 “指定磁盘文件”对话框

Step 16 单击“下一步”按钮，进入“已准备好创建虚拟机”对话框，如图 2-67 所示。

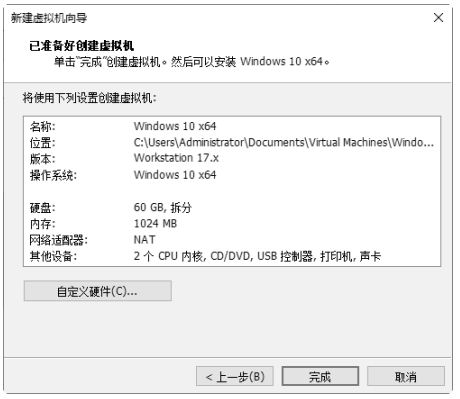

图 2-67 “已准备好创建虚拟机”对话框

Step 17 单击“完成”按钮，至此，便创建了一个新的虚拟机，如图 2-68 所示，这当中的硬件配置，可以根据实际需求再进行更改。

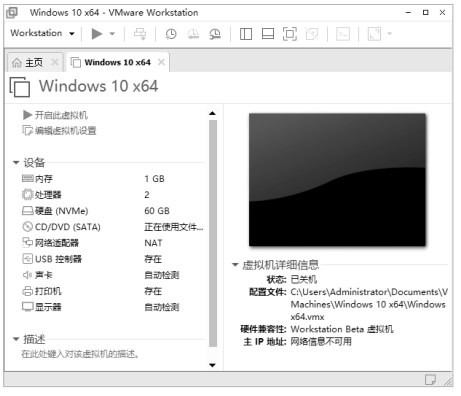

图 2-68 创建新虚拟机

Step 18 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 2-69 所示。

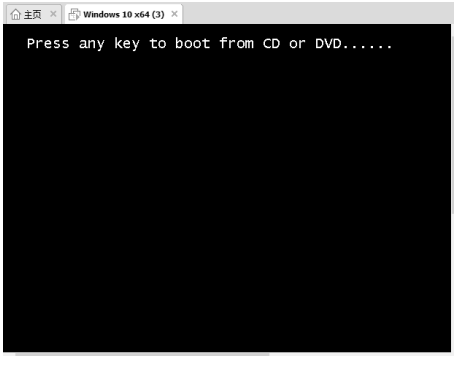

图 2-69 安装过渡窗口

Step 19 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 2-70 所示。

图 2-70　准备要安装的文件

Step 20 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中，如图 2-71 所示。

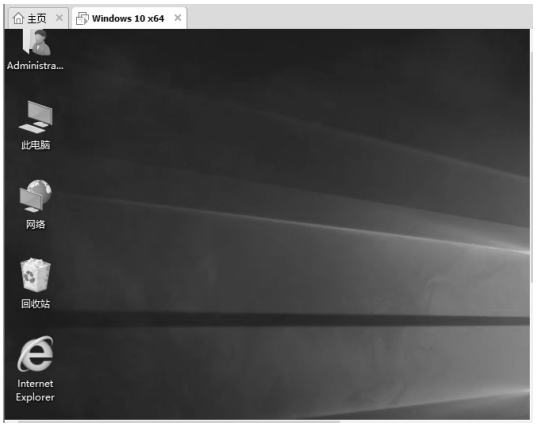

图 2-71　操作系统界面

2.4.2　安装 VMware Tools 工具

安装好 Windows 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：

Step 01 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 2-72 所示。

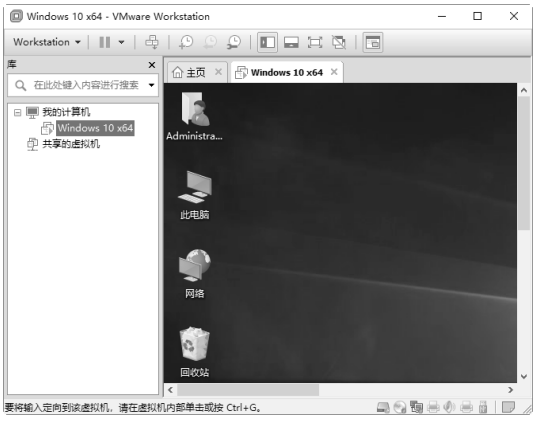

图 2-72　进入虚拟系统

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。

Step 02 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 2-73 所示。

图 2-73　“安装 VMware Tools”命令

Step 03 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 2-74 所示。

Step 04 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，这里选中“典型安装”单选按钮，如图 2-75 所示。

图 2-74 “欢迎使用 VMware Tools 安装向导”窗口

图 2-75 “选择安装类型”窗口

Step 05 单击“下一步”按钮，进入“已准备好安装 VMware Tools”对话框，如图 2-76 所示。

图 2-76 “已准备好安装 VMware Tools”窗口

Step 06 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 2-77 所示。

图 2-77 “正在安装 VMware Tools”窗口

Step 07 安装完成后，进入“VMware Tools 安装向导已完成”窗口，如图 2-78 所示。

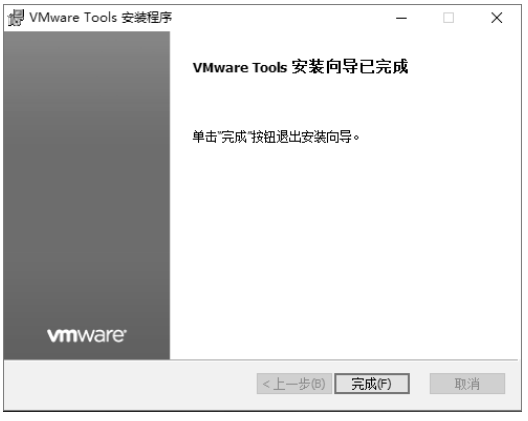

图 2-78 “VMware Tools 安装向导已完成”窗口

Step 08 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 2-79 所示。

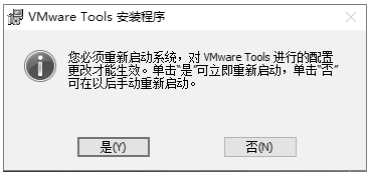

图 2-79 信息提示框

Step 09 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 2-80 所示。

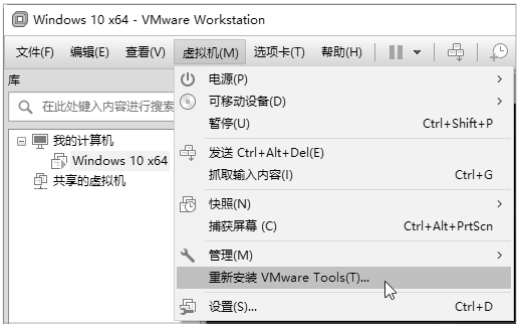

图 2-80 “重新安装 VMware Tools”菜单命令

2.5 实战演练

2.5.1 实战 1：显示系统文件的扩展名

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。

Step 01 单击“开始”按钮，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 2-81 所示。

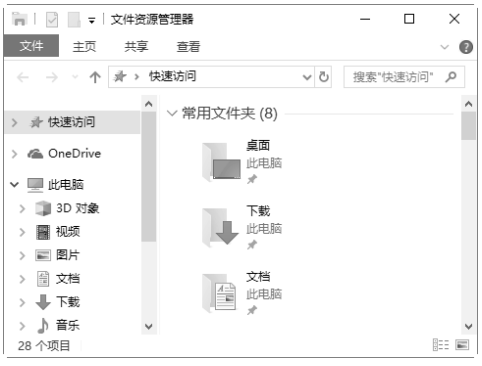

图 2-81 “文件资源管理器”窗口

Step 02 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 2-82 所示。

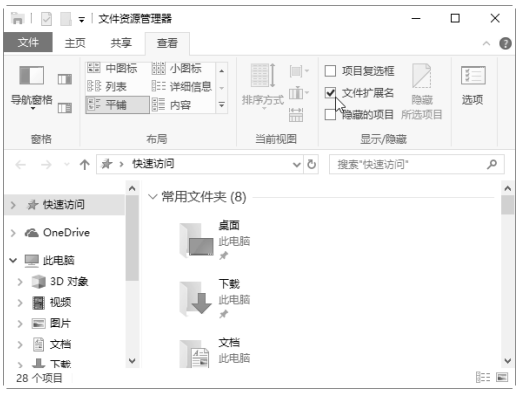

图 2-82 “查看”选项卡

Step 03 此时打开一个文件夹，用户便可以查看文件的扩展名，如图 2-83 所示。

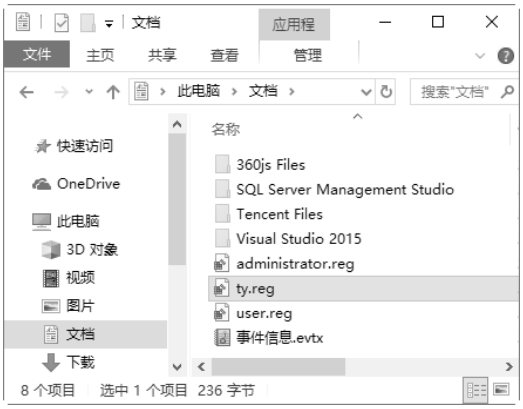

图 2-83 查看文件的扩展名

2.5.2 实战 2：关闭开机多余启动项

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。

Step 01 按 Ctrl+Alt+Delete 组合键，打开如图 2-84 所示的界面。

图 2-84 “任务管理器”选项

Step 02 单击“任务管理器”选项，打开“任务管理器”窗口，如图 2-85 所示。

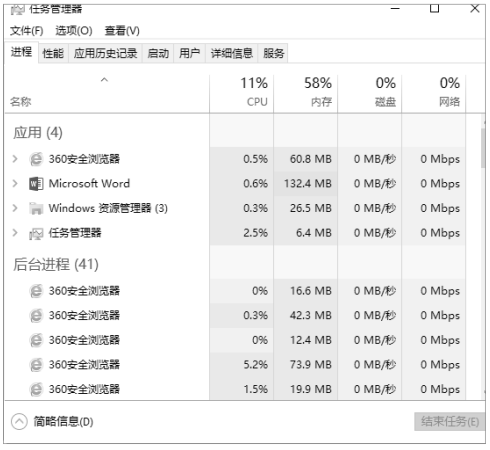

图 2-85 “任务管理器”窗口

Step 03 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 2-86 所示。

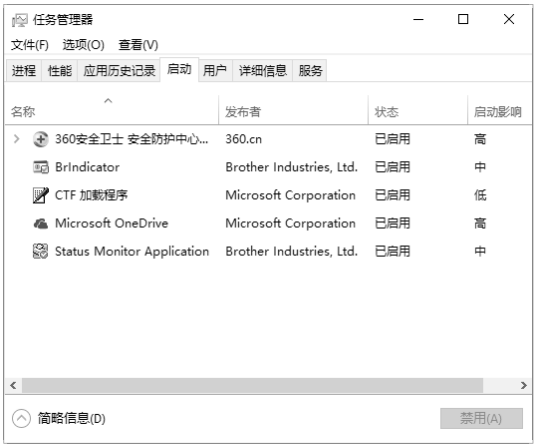

图 2-86 “启动”选项卡

Step 04 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 2-87 所示。

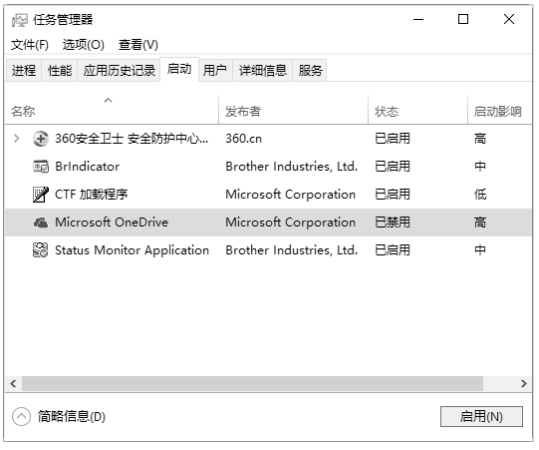

图 2-87 禁止开机启动项

第3章　渗透测试中的DOS命令

熟练掌握DOS系统中常用的命令是进行渗透测试的基本功。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。本章介绍Windows系统自带的DOS命令。

3.1　进入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。

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”按钮，在弹出的菜单列表中选择“Windows”→“命令提示符”菜单命令，如图3-1所示。

图3-1　“命令提示符”菜单命令

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3-2　“管理员：命令提示符”窗口

3.1.2　运用“运行”对话框进入DOS窗口

除使用菜单的形式进入DOS窗口，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：

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”菜单命令。随即弹出“运行”对话框，在其中输入“cmd”命令，如图3-3所示。

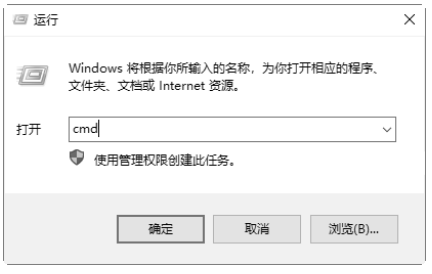

图3-3　“运行”对话框

Step 02 单击“确定”按钮，即可进入DOS窗口，如图3-4所示。

图 3-4　DOS 窗口

3.1.3　通过浏览器进入 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。

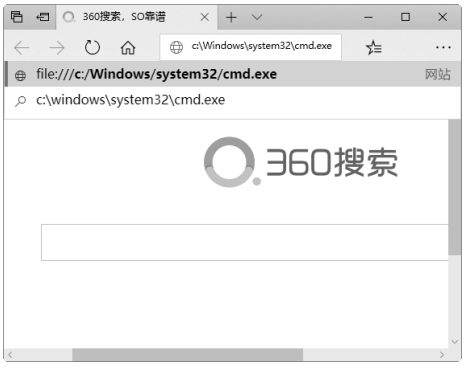

图 3-5　Microsoft Edge 浏览器

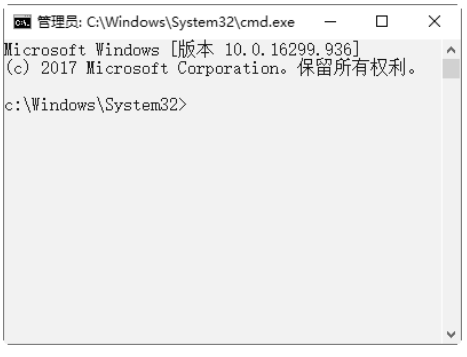

图 3-6　DOS 窗口

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

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。

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 3 种使用方法。

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

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

（3）cd\：表示当前无论在哪个子目录下，通过该命令可立即返回到根目录下。

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

Step 01 在“命令提示符”窗口中输入 cd c:\ 命令，按 Enter 键，即可将目录切换为 C:\，如图 3-7 所示。

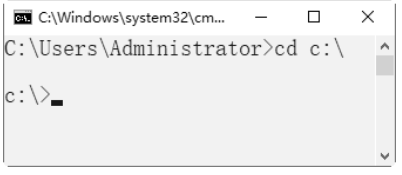

图 3-7　切换到 C 盘根目录

Step 02 如果想进入 C:\Windows\system32 目录中，则需在上面的“命令提示符”窗口中

输入 cd Windows\system32 命令，按 Enter 键即可将目录切换为 C:\Windows\system32，如图 3-8 所示。

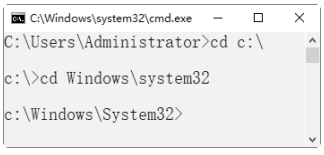

图 3-8　切换到 C 盘子目录

Step 03 如果想返回上一级目录，则可以在“命令提示符”窗口中输入 cd.. 命令，按 Enter 键即可，如图 3-9 所示。

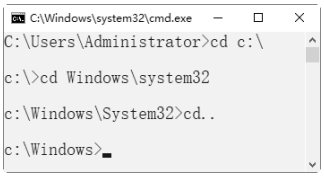

图 3-9　返回上一级目录

Step 04 如果想返回到根目录，则可以在“命令提示符”窗口中输入 cd\ 命令，按 Enter 键即可，如图 3-10 所示。

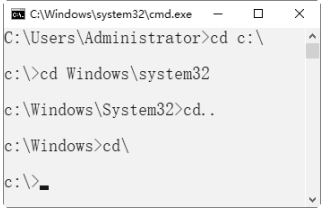

图 3-10　返回根目录

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。

Step 01 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 3-11 所示。

图 3-11　Administrator 目录下的文件列表

Step 02 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 3-12 所示。

Step 03 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 3-13 所示。

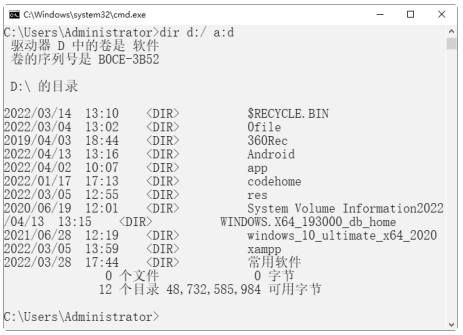

图 3-12　D 盘下的文件列表

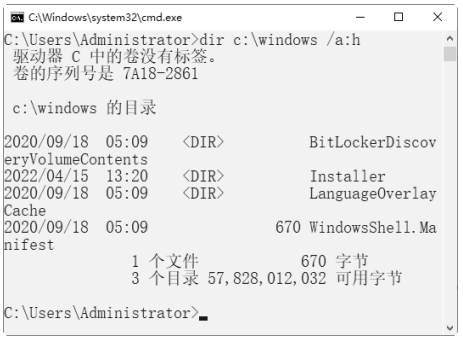

图 3-13　C 盘下的隐藏文件

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 3-14 所示。

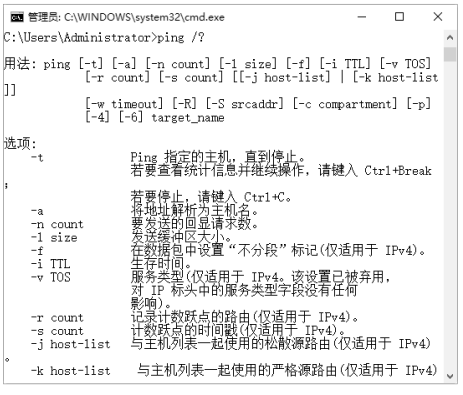

图 3-14　ping 命令帮助信息

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。

Step 01 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 3-15 所示。

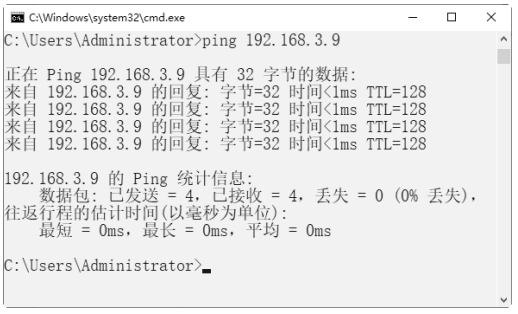

图 3-15　判断计算机的操作系统类型

Step 02 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 3-16 所示。

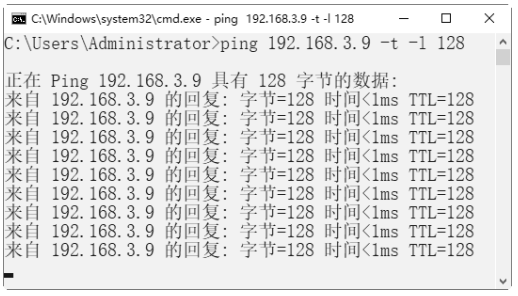

图 3-16　向主机发出大量数据包

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 3-17 所示，说明本台计算机与外界网络连通。

图 3-17　网络连通信息

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 3-18 所示，可知这台主机的名称为 SD-20220314SOIE。

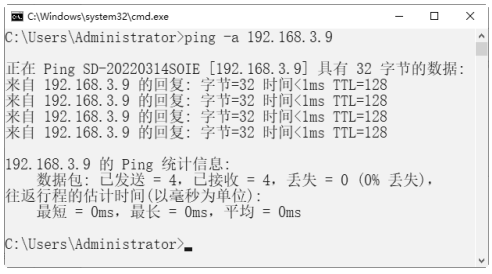

图 3-18　解析某 IP 地址的计算机名

3.2.4　查询网络状态与共享资源的 net 命令

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：

Step 01 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 3-19 所示。

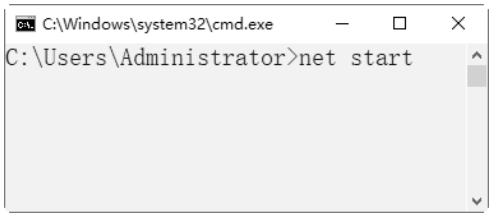

图 3-19　输入 net start 命令

Step 02 按 Enter 键，则在打开的“命令提示符”窗口中可以显示计算机已启动的 Windows 服务，如图 3-20 所示。

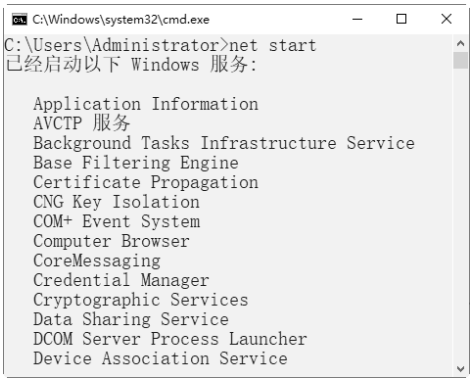

图 3-20　计算机已启动的 Windows 服务

3.2.5　显示网络连接信息的 netstat 命令

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，可以让用户知道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 3-21 所示。

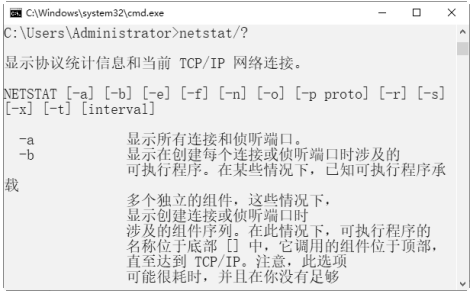

图 3-21　netstat 命令帮助信息

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。

Step 01 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 3-22 所示。

图 3-22　服务器活动的 TCP/IP 连接

Step 02 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 3-23 所示。

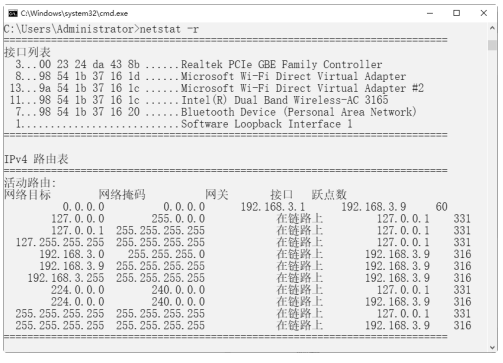

图 3-23　查看本机路由信息

Step 03 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 3-24 所示。

图 3-24　查看本机活动的 TCP 连接

Step 04 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 3-25 所示。

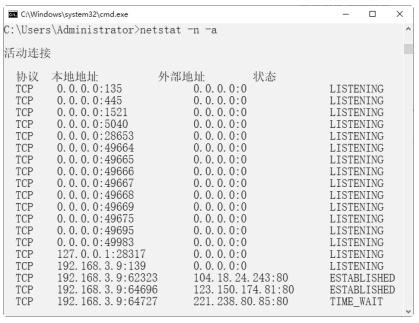

图 3-25　查看本机连接的端口及其状态

3.2.6　检查网络路由节点的 tracert 命令

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。

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 3-26 所示。

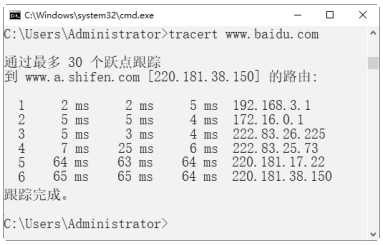

图 3-26　查看网络中路由节点信息

3.2.7　显示主机进程信息的 Tasklist 命令

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：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及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 3-27 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。

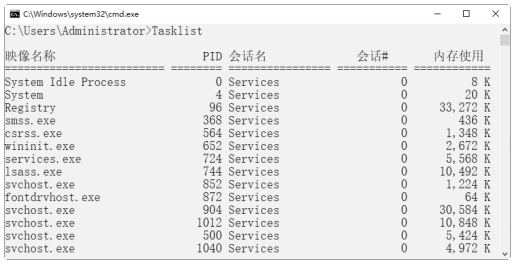

图 3-27　查看本机进程

Step 02 Tasklist 命令不但可以查看系统进程，而且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，在命令提示符下输入 Tasklist /svc 命令即可，如图 3-28 所示。

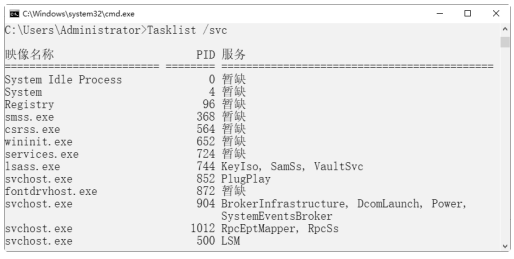

图 3-28　查看本机进程 svchost.exe 提供的服务

Step 03 要查看本地系统中哪些进程调用了 shell32.dll 模块文件，只需在命令提示符下输入 Tasklist /m shell32.dll 即可显示这些进程的列表，如图 3-29 所示。

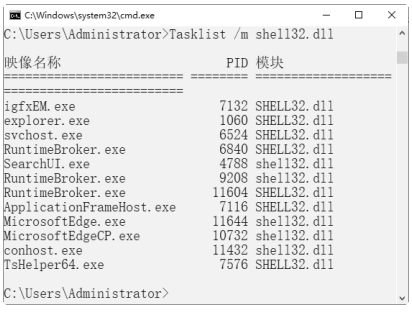

图 3-29　显示调用 shell32.dll 模块的进程

Step 04 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 3-30 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”。

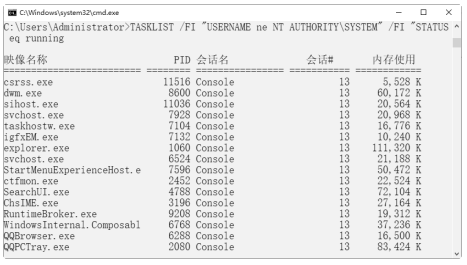

图 3-30 列出系统中正在运行的非 SYSTEM 状态的所有进程

3.3 实战演练

3.3.1 实战 1：使用命令实现定时关机

使用 shutdown 命令可以实现定时关机的功能，具体操作步骤如下。

Step 01 在“命令提示符”窗口中输入 shutdown/s /t 40 命令，如图 3-31 所示。

图 3-31 输入 shutdown/s /t 40 命令

Step 02 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 3-32 所示。

图 3-32 信息提示框

Step 03 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 3-33 所示的弹窗，表示取消成功。

图 3-33 取消关机操作

3.3.2 实战 2：自定义 DOS 窗口的风格

DOS 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 DOS 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风格的操作步骤如下：

Step 01 单击 DOS 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 3-34 所示。

图 3-34 “选项”选项卡

Step 02 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 3-35 所示。

图 3-35 “颜色”选项卡

Step 03 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 3-36 所示。

图 3-36　设置屏幕背景颜色

Step 04 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 3-37 所示。

Step 05 选中“弹出窗口背景”单选按钮，可以设置弹出窗口背景的显示颜色，这里设置颜色值为“125”，如图 3-38 所示。

图 3-37　设置文字颜色

图 3-38　设置弹出窗口背景颜色

Step 06 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 3-39 所示。

图 3-39　自定义命令提示符窗口显示风格