第 1 章

老铁，你所在的网络安全吗

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，也时刻面临着攻击者残酷攻击的危险，这里问一句，你所在的网络安全吗？

1.1 网络中的相关概念

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

1.1.1 互联网与因特网

互联网是指将两台计算机或者两台以上的计算机终端、客户端、服务端，通过计算机信息技术的手段互相联系起来的结果。互联网在现实生活中的应用很广泛，在互联网上人们可以聊天、玩游戏、查阅资料等。互联网是全球性的，这就意味着这个网络不管是谁发明了它，都是属于全人类的。图 1-1 所示为互联网的结构示意图。

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

图 1-1　互联网结构示意图

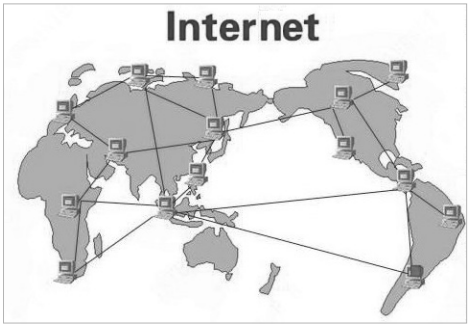

图 1-2　因特网结构示意图

1.1.2 万维网与浏览器

万维网（World Wide Web，WWW）简称为 3W，它是无数个网络站点和网页的集合，也是

Internet 提供的最主要的服务。它是由多媒体链接而形成的集合，通常人们上网看到的内容就是万维网的内容。图 1-3 所示为使用万维网打开的百度首页。

提示：凡是能彼此通信的设备组成的网络就称为互联网。所以，即使仅有两台计算机，不论用何种技术使其彼此通信，也可称为互联网。

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

图 1-3　百度首页

图 1-4　Microsoft Edge 浏览器

1.1.3　URL 地址与域名

URL（Uniform Resource Locator）即统一资源定位器，也就是网络地址，是 Internet 上用来描述信息资源，并将 Internet 提供的服务统一编址的系统。简单来说，通常在 IE 浏览器或 Netscape 浏览器中输入的网址就是 URL 的一种，如百度网址 http://www.baidu.com。

图 1-5　使用 URL 地址打开的网页

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

1.1.4　IP 与 MAC 地址

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

MAC 地址与网络无关，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，都是相同的 MAC 地址，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，例如，08:00:20:0A:8C:6D 就是一个 MAC 地址。

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

1.1.5　网络通信协议

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

1. TCP/IP 协议

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

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

2. IP 协议

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

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

3. ARP 协议

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

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

4. ICMP 协议

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

ICMP 协议对于网络安全非常重要，因为 ICMP 协议本身的特点，决定了它非常容易被用来攻击网络上的路由器和主机。例如，可以利用操作系统规定的 ICMP 数据包最大尺寸不超过 64KB 这一规定，向主机发起 Ping of Death（死亡之 Ping）攻击。

1.2 网络系统面临的安全威胁

网络系统所面临的安全威胁主要是指针对网络本身的安全攻击，如恶意代码、远程入侵、拒绝服务攻击、身份假冒、信息窃取和篡改等。这些攻击手段的目的就是破坏网络的可用性、完整性和保密性，从而窃取敏感信息、干扰正常业务或造成经济损失。

1.2.1 恶意代码

恶意代码，又称恶意软件或恶意程序，是指那些在计算机系统中，未经用户授权或同意，即自行安装并执行对系统造成损害或窃取用户数据的程序。这些软件也可称为广告软件（adware）、间谍软件（spyware）或恶意共享软件（malicious shareware），有时也被称为流氓软件。

另外，恶意代码还指故意编制或设置的、对网络或系统会产生威胁或潜在威胁的计算机代码。最常见的恶意代码有计算机病毒（简称病毒）、特洛伊木马（简称木马）、计算机蠕虫（简称蠕虫）、后门、逻辑炸弹等。这些恶意软件可能会潜伏在下载的软件、邮件附件或链接中，一旦运行，就会破坏计算机系统、窃取数据或控制设备。例如，勒索病毒会加密重要文件，要求支付赎金才能解锁。

1.2.2 远程入侵

信息化在人们生活中普及的程度已经相当高了，远程访问的需求也越来越高。虽然远程访问的便捷使得人们的工作效率大大提升，但同时也增加了网络的危险性，因为大多数的远程访问应用程序本身并没有安全策略，所以远程入侵又成了网络安全的新隐患。

最典型的远程入侵就是攻击者可以远程激活计算机上的摄像头，来获取视频资料，从而截获或篡改计算机数据。

1.2.3 拒绝服务攻击

拒绝服务攻击（DoS 攻击）是一种网络攻击手段，该攻击方式通过消耗目标系统的网络或系统资源，导致服务暂时中断或停止。拒绝服务攻击问题一直存在的原因是网络协议本身的安全缺陷，这就导致拒绝服务攻击成为了攻击者的终极手法。

攻击者进行拒绝服务攻击，实际上就是让服务器实现两种效果：一种是迫使服务器的缓冲区满，不接收新的请求；另一种是使用 IP 欺骗，迫使服务器把非法用户的连接复位，影响合法用户的连接。

常见的 DoS 攻击包括 SYN Flood，这是一种利用 TCP 协议缺陷的攻击方式，通过发送大量伪造的 TCP 连接请求，使被攻击方的资源耗尽。当服务器为了维护大量的半连接列表而消耗大量资源时，正常的用户请求就无法得到处理，从而导致服务中断。

1.2.4 身份假冒

根据网络安全基础，网络攻击可分为主动攻击和被动攻击，主动攻击包括假冒、重放、修改信

息和拒绝服务等，因此身份假冒属于网络攻击手段中的主动攻击类型。

身份假冒就是攻击者冒充合法用户的身份获得访问权限或发起攻击。例如，攻击者通过各种手段获取账号密码登录到银行账户，或者盗用社交账号、游戏账号等进行非法活动。还有一些攻击者会利用人性的弱点，如好奇心、同情心等，通过欺骗手段获取用户的信任，从而获取敏感信息，再伪装成熟人向用户求助，借机询问密码等重要信息。

1.2.5　信息窃取和篡改

窃取或篡改信息的攻击方式有很多，常见的有网络诈骗、个人信息泄露、网络钓鱼等。网络诈骗是指不法分子通过各种手段，如虚假网站、中奖信息、网络兼职等，诱骗用户提供个人信息或转账汇款，从而达到骗取钱财的目的。还有冒充公检法机关进行诈骗，声称用户涉及某项重大案件，要求将资金转移到“安全账户”配合调查。

在网上注册账号、填写表单、使用公共 WiFi 等时，个人信息可能会被攻击者窃取或非法收集，从而导致个人信息泄露，甚至被用于非法活动。例如，一些不法分子获取个人信息后进行精准的电话推销或诈骗。

网络钓鱼是攻击者通过发送看似来自合法机构的电子邮件或短信，引导用户单击链接并输入个人敏感信息，从而实施诈骗。此外，还有“伪基站”钓鱼，通过伪装成运营商基站发送虚假短信，骗取用户信息。

1.3　网络安全的研究内容

随着网络技术的不断发展，网络安全威胁也日益复杂多变，因此，构建一个完善的网络安全体系对企业和个人而言都至关重要。

1.3.1　网络安全体系

网络安全体系是指为保护网络环境免受恶意攻击、数据泄露等威胁而建立的一系列制度、技术和管理措施的总和，覆盖了从物理层到应用层的全方位防护，是确保信息安全、维护网络稳定的重要保障。

网络安全体系按照 OSI 七层模型，可以划分为物理层、数据链路层、网络层、传输层、会话层、表示层和应用层，每个层次都有其特定的安全关注点和防护措施。例如，物理层关注数据中心的物理访问控制；数据链路层则负责数据帧的传输错误检测；网络层处理数据包传输和路径选择的安全问题；传输层则通过数据加密和完整性验证来确保数据传输的安全。这种层次化的结构有助于用户针对性地解决不同层面的安全问题，形成全面而有效的防护网。图 1-6 所示为网络安全体系 OSI 七层模型。

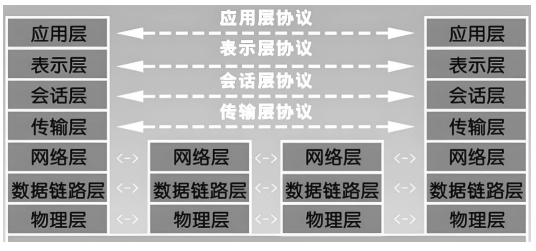

图 1-6　网络安全体系 OSI 七层模型

1.3.2 网络攻击技术

常见的网络攻击技术包括网络监听、网络扫描、网络入侵、网络后门、网络隐身等。其中，网络监听是通过在计算机上设置程序来监听目标计算机与其他计算机的通信数据；网络扫描是利用程序扫描目标计算机的开放端口，从而发现漏洞，为入侵做准备，当探测到对方存在漏洞后，就可以入侵目标计算机来获取信息。最后，入侵成功后，就会在目标计算机中种植木马等后门程序，实现长期控制。有时，为了防止被管理员发现，还会进行网络隐身，即清除入侵痕迹。

常见的网络攻击手段主要包括以下几种：

（1）口令入侵：攻击者通过非法手段获取用户的账户和密码，然后登录到用户的系统或应用中实施攻击活动。

（2）特洛伊木马：攻击者会伪装成一个看似无害的文件或程序（即“鱼饵”），诱骗用户下载、安装和运行。一旦运行，特洛伊木马就会潜伏在用户的系统中，窃取用户的账户信息、密码等敏感数据。

（3）网站欺骗：攻击者会伪造一个与目标网站相似的虚假网站（B 网站），当用户试图访问目标网站（A 网站）时，会被重定向到虚假网站上。在虚假网站上，攻击者可以欺骗用户输入个人信息或进行其他恶意操作。

（4）电子邮件攻击：攻击者会向用户的邮箱发送大量的垃圾邮件或包含恶意代码的邮件，这些邮件可能会导致用户的系统瘫痪、泄露个人信息或执行其他恶意操作。

（5）节点攻击：攻击者会先攻击并控制用户的计算机（称为“肉鸡”或“僵尸机”），然后利用这些计算机作为跳板去攻击其他重要的网站或系统。由于攻击路径被隐藏，因此事后调查往往只能追溯到被控制的计算机。

（6）黑客软件：攻击者使用黑客软件非法取得用户计算机的管理者权利，然后对其进行完全控制。黑客软件不仅可以进行文件操作，还可以进行桌面抓图、获取密码等操作。

（7）安全漏洞：许多系统都存在安全漏洞（Bugs），如 Windows 操作系统经常需要打补丁来弥补这些漏洞。如果漏洞没有被及时修复，攻击者就可以利用这些漏洞获取用户的计算机权限或数据。

这些网络攻击手段虽然看似复杂多样，但其实都是通过一系列的技术操作来达到控制、窃取及破坏的目的。因此，用户需要提高网络安全意识，采取必要的防护措施来抵御这些攻击。

1.3.3 网络防御技术

防范网络攻击手段需要用户从多个层面入手，构建全方位的安全防护体系。下面介绍一些具体的防范措施。

1. 个人意识方面

网络用户要保持安全警惕，对不明来源的信息保持高度警惕，不要轻易单击陌生人发来的链接或附件；对于声称来自银行、政府机构等的重要通知，一定要通过官方渠道进行核实。

当需要进行密码保护时，一定要使用复杂且独特的密码，包含字母、数字和特殊字符，且长度不少于 8 位，还要避免在多个网站使用相同的密码，并定期更换密码。另外，不要在公共场合或不安全的网络环境下透露个人敏感信息，谨慎处理垃圾邮件和陌生人的社交信息。

在使用网络时，尤其在使用公共无线网络时要格外小心，避免进行敏感的金融交易或输入个人隐私信息，可以使用虚拟专用网络（VPN）来加密网络连接，提高安全性。不要浏览不正规的网站，避免下载来路不明的软件。

对于重要数据，如文件、照片、联系人等，要定期备份，以防数据丢失。用户可以使用外部硬盘、云存储等多种方式进行备份，并确保备份数据的安全性。

2. 技术防护措施

除了个人的安全防护意识，还需要一些技术方面的防护措施，比如，在设备上安装可靠的杀毒软件和防火墙，定期进行全盘扫描和病毒查杀，防火墙可以有效监控和阻止恶意流量的入侵，杀毒软件可以查杀设备上的病毒。

启用双重身份验证是保护账户安全的一项重要措施。例如，可以为重要账户启用双重身份验证功能，如短信验证码、指纹识别、面部识别等，这可以增加一层额外的安全保护，防止未经授权访问账户。

对于操作系统，要及时安装系统补丁和更新，修复已知的安全漏洞，还要开启自动更新功能，确保设备在有新的安全补丁时自动进行更新。对于内部网络要进行运行监控、流量监控和威胁监控，从而生成网络安全日志，以便及时发现和响应异常行为。

3. 针对特定攻击类型的防范措施

用户首要注意的是防范网络钓鱼，注意识别可疑的电子邮件、链接和网站。不要轻易输入个人信息或从不信任的网站下载文件。对于 DDoS 攻击行为，要使用防火墙或入侵防御系统（IPS）来检测和响应流量异常，同时还要将服务器部署在不同的数据中心，以实现网络冗余和故障切换。

对于 SQL 注入的防范，要确保 Web 开发人员已正确清理所有输入，验证输入数据以符合预定义标准，还要使用参数化查询和存储过程来防止 SQL 注入攻击。

总之，防范网络攻击需要用户从多个层面入手，包括提高个人安全意识，养成良好的网络使用习惯，采取技术防护措施，以及针对特定攻击类型制定防范措施等。只有这样，才能构建稳固的安全防护体系，确保网络环境的稳定和安全。

4. 网络安全检测工具

当然，还有一些简单且实用的网络安全检测工具，可以帮助用户提升网络安全性，分别介绍如下：

1）漏洞扫描工具

Nessus 是一款 UNIX 平台的漏洞评估工具，被认为是最好的、免费的网络漏洞扫描程序。它拥有超过 11000 个插件，可以快速识别网络中的安全漏洞。Nessus 的关键特性包括安全和本地的安全检查、GTK 图形接口的客户端/服务器体系结构，以及一个嵌入式脚本语言，方便用户编写自己的插件或理解现有的插件。

OpenVAS 也是一款强大的开源漏洞扫描器，可以检测网络上的各种漏洞。它提供了丰富的扫描选项和报告功能，可以帮助用户全面了解网络的安全状况。

2）网络流量分析工具

Wireshark 是一款开源的网络协议分析程序，支持 UNIX 和 Windows 两种平台。它允许用户从一个活动的网络或磁盘上的捕获文件来检查数据，交互地浏览捕获的数据，并深入探究数据包的详细信息。Wireshark 拥有丰富的显示过滤程序语言和查看一次 TCP 会话的结构化数据流的能力，是分析网络流量的必备工具。

Tcpdump 是一款经典的网络监视和数据获取嗅探程序。在 Wireshark 之前，Tcpdump 曾被广泛使用。它虽然没有华丽的图形用户界面，但几乎没有什么安全漏洞，并且需要很少的系统资源。Tcpdump 对于跟踪网络问题或监视网络活动而言是一个极有价值的工具。

3）入侵检测系统（IDS）

Snort 是一个开源的入侵检测系统，对 IP 网络中的通信分析和数据包的日志记载都表现出色。通过协议分析、内容搜索及各种各样的预处理程序，Snort 可以检测成千上万的蠕虫、漏洞、端口

扫描和其他许多可疑行为。它还提供了一个分析 Snort 警告的 Web 界面，方便用户查看和管理安全事件。

4）其他实用工具

Nmap 是一个非常好的端口扫描应用，支持 Linux 和 Windows 平台。它可以从命令或图形用户界面（GUI）执行任务，具有 TCP 扫描、UDP 扫描和操作系统识别等多种功能。Nmap 是渗透测试人员常用的工具之一，可以帮助他们发现目标系统上的开放端口和服务。

Nikto 是一个综合性的开源 Web 扫描程序，可以对 Web 服务器的多种项目进行扫描操作，包括潜在的危险文件和特定服务器上的问题。它采用 Whisker/libwhisker 支持其底层功能，并经常更新扫描项目和插件，以保持其准确性。

这些工具都具有各自的特点和优势，可以根据自身需求选择合适的工具进行检测。同时，为了提升网络安全水平，建议用户定期更新这些工具并保持警惕，及时发现潜在的安全威胁。

1.3.4 密码技术应用

在网络通信中，密码技术是保证通信安全的重要手段，通过使用加密算法对传输的数据进行加密处理，可以防止信息在传输过程中被窃听或篡改。

密码技术是一门涉及信息安全和隐私保护的学科，其核心原理在于利用数学和计算机科学原理，设计并实现加密算法、密钥管理及安全协议等技术手段。密码技术的主要任务包括信息加密、解密、完整性验证和身份认证。通过加密，明文信息被转换成难以理解的密文，确保信息在传输和存储过程中的机密性，解密则是将密文还原为明文的过程。

密码技术主要分为对称加密、非对称加密、哈希函数和数字签名等几大类。在网络通信中，密码技术是保证通信安全的重要手段。通过使用加密算法对传输的数据进行加密处理，可以防止信息在传输过程中被窃听或篡改。同时，密码协议用于实现安全通信，包括身份认证、密钥协商和安全传输等。例如，在 VPN（虚拟专用网络）和 SSL/TLS（安全套接层/传输层安全协议）中，密码技术被广泛应用于建立安全的通信通道，保护网络通信的机密性和完整性。

1.4 网络设备信息的获取

网络设备包含的类型有很多，如路由器、计算机、手机、平板电脑等，但最主要的还是计算机，下面以获取计算机设备信息为例，来介绍网络设备信息获取的方法。一台计算机的基本信息包括 IP 地址、物理地址、端口信息等。

1.4.1 获取 IP 地址

IP 地址用于在 TCP/IP 通信协议中标记每台计算机的地址，通常使用十进制来表示，如 192.168.1.100。计算机的 IP 地址一旦被分配，就是固定不变的，因此，查询出计算机的 IP 地址，在一定程度上就实现了攻击者入侵的前提工作。

使用 ipconfig 命令可以获取计算机的 IP 地址，具体的操作步骤如下：

步骤 01 右击“开始”按钮，在弹出的快捷菜单中选择“运行”命令，如图 1-7 所示。

步骤 02 弹出“运行”对话框，在“打开”后面的文本框中输入 cmd 命令，如图 1-8 所示。

图 1-7　选择“运行”命令

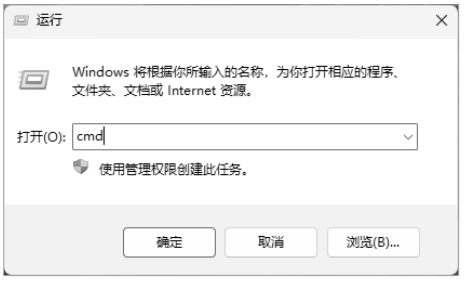

图 1-8　输入 cmd 命令

步骤 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 1-9 所示。

提示：在“命令提示符”窗口中，192.168.2.125 表示本机在局域网中的 IP 地址。

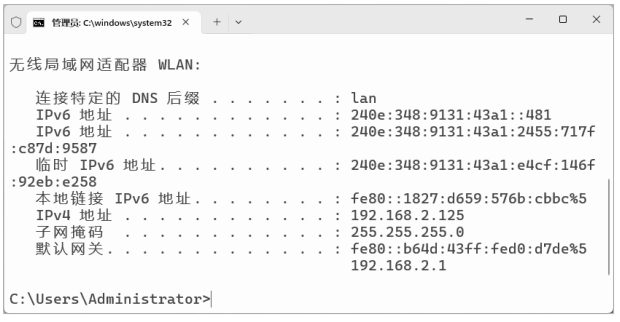

图 1-9　查看 IP 配置信息

1.4.2　获取物理地址

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，都是相同的 MAC 地址，它由厂商写在网卡的 BIOS 里。

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-D9-B6-E5，这就是本台计算机的网卡地址，它是唯一的，如图 1-10 所示。

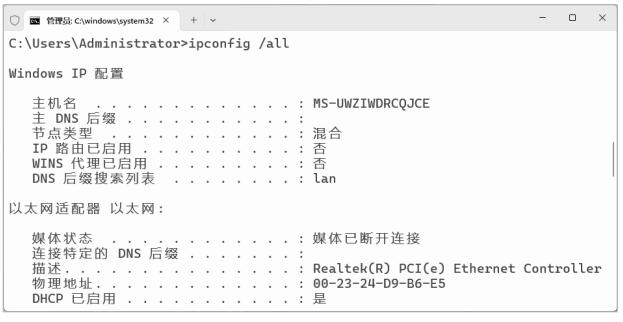

图 1-10　查看 MAC 地址

提示：IP 地址与 MAC 地址的区别在于，IP 地址基于逻辑，比较灵活，不受硬件限制，也容易记忆；MAC 地址在一定程度上与硬件一致，基于物理，能够被具体标识。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。

1.4.3　查看开放端口

“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，端口号只有整数，范围为 0 ～ 65535（256×256−1）。经常查看系统开放端口的状态变化，可以帮助用户及时检测异常连接，防止攻击者通过端口入侵计算机。

用户可以使用 netstat 命令查看自己系统的端口状态，具体操作步骤如下：

步骤 01 打开“命令提示符”窗口，输入 netstat –a –n 命令，如图 1-11 所示。

步骤 02 按【Enter】键，即可看到以数字显示的 TCP 和 UCP 连接的端口号及其状态，如图 1-12 所示。

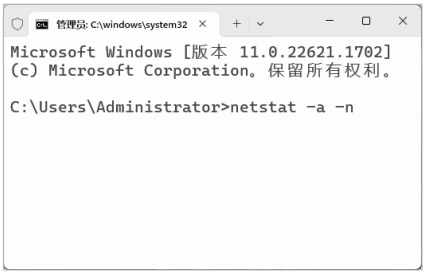

图 1-11　输入 netstat –a –n 命令

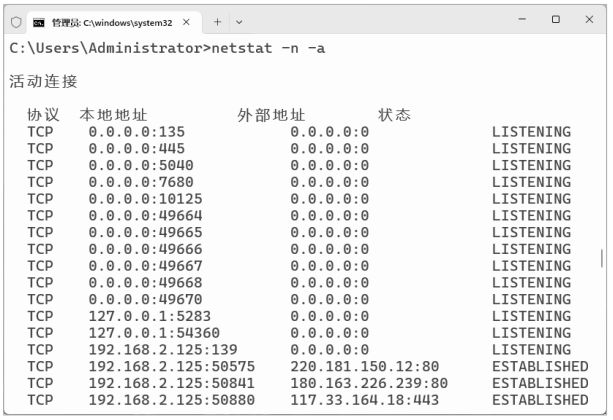

图 1-12　TCP 和 UCP 连接的端口号

1.5　实战演练

1.5.1　实战 1：查看系统进程

系统进程是指正在运行的程序实体，并且包括这个运行的程序中占据的所有系统资源。在 Windows 系统中，可以在“任务管理器”窗口中获取系统进程。

具体的操作步骤如下：

步骤 01 在 Windows 系统桌面中，右击“开始”按钮，在弹出的快捷菜单中选择“任务管理器”命令，如图 1-13 所示。

步骤 02 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 1-14 所示。

图 1-13　选择“任务管理器”命令

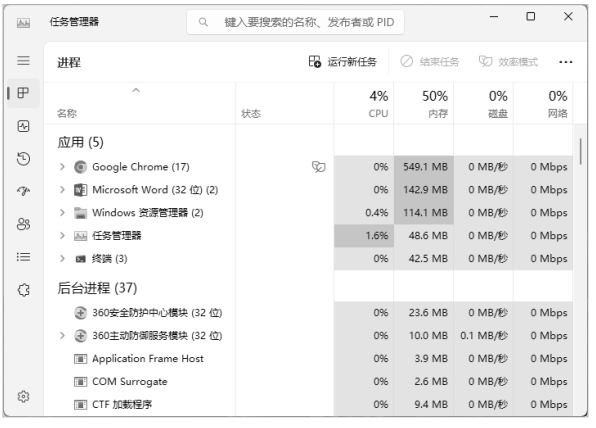

图 1-14　“任务管理器”窗口

提示：在 Windows 系统桌面上，按【Ctrl+Alt+Delete】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。

1.5.2　实战 2：显示文件扩展名

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

步骤 01 打开“此电脑”窗口，然后单击“···”按钮，在打开的下拉列表框中选择“选项”选项，如图 1-15 所示。

步骤 02 弹出“文件夹选项”对话框，选择“查看”选项卡，在“高级设置”列表框中取消选择“隐藏已知文件类型的扩展名”复选框，如图 1-16 所示。

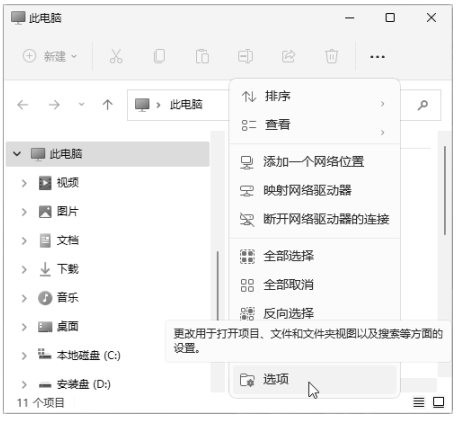

图 1-15　选择“选项”菜单选项

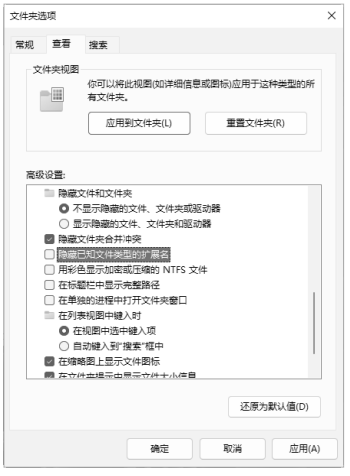

图 1-16　“文件夹选项”对话框

步骤 03 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 1-17 所示。

提示：在“此电脑”窗口中单击“查看”按钮，在打开的下拉列表框中选择“显示”→“文件扩展名”选项，可以快速显示文件的扩展名，如图 1-18 所示。

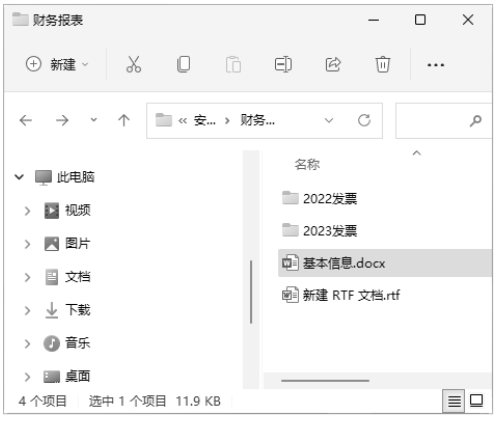

图 1-17　显示文件的扩展名

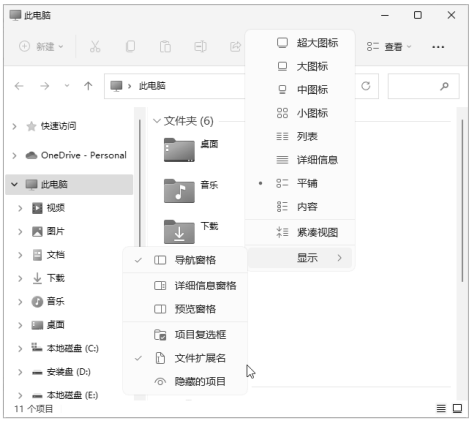

图 1-18　快速显示文件的扩展名

第 2 章

练好基本功，搭建网络安全测试环境

安全测试环境是网络安全工作者需要了解和掌握的内容。另外，对于网络安全初学者来说，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，而初学者并不能从网络上搜索到这些攻击目标，此时就需要通过搭建网络安全测试环境来解决这个问题。

2.1 认识安全测试环境

所谓安全测试环境，就是在已存在的一个系统中，利用虚拟机工具创建出的一个内在的虚拟系统。该系统与外界独立，但与已存在的系统建立有网络关系，在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情况下进行切换。

创建虚拟系统的好处有以下几种：

- 虚拟技术是一种调配计算机资源的方法，可以更有效、更灵活地提供和利用计算机资源，降低成本，节省开支。
- 在虚拟环境里更容易实现程序自动化，有效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 VMware

对于无线安全初学者，使用虚拟机构建无线测试环境是一个非常好的选择，这样既可以快速搭建测试环境，还可以快速还原之前的快照，避免错误操作造成系统崩溃。

2.2.1　下载 VMware 软件

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：

步骤 01 使用浏览器打开 VMware Workstation 下载页面，如图 2-1 所示。

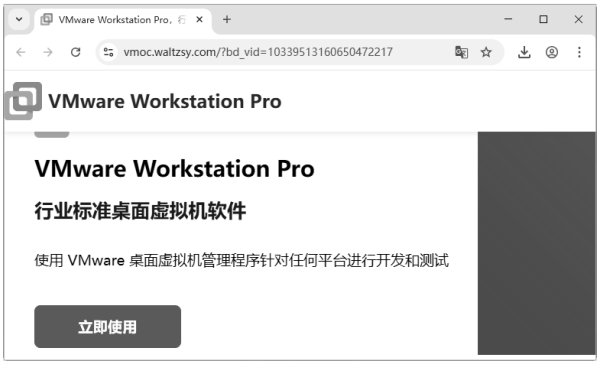

图 2-1　VMware Workstation 下载页面

步骤 02 在页面中找到 VMware Workstation Pro 对应的下载区域，在其中选择需要的版本，单击“立即下载”按钮，如图 2-2 所示。

步骤 03 弹出“新建下载任务”对话框，单击“下载”按钮进行下载，如图 2-3 所示。

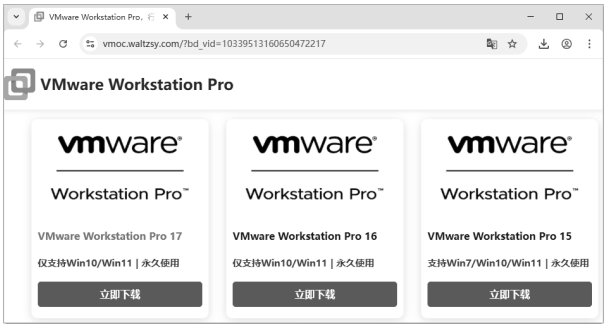

图 2-2　VMware 下载区域

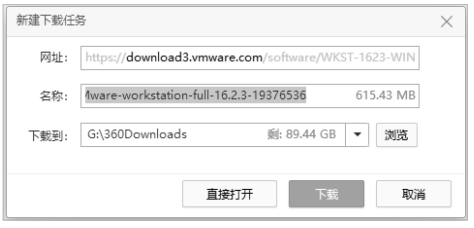

图 2-3　“新建下载任务”对话框

2.2.2　安装 VMware 软件

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：

步骤 01 双击下载的 VMware 安装软件，弹出“欢迎使用 VMware Workstation Pro 安装向导”窗口，如图 2-4 所示。

步骤 02 单击“下一步”按钮，进入“最终用户许可协议”窗口，选择“我接受许可协议中的条款”复选框，如图 2-5 所示。

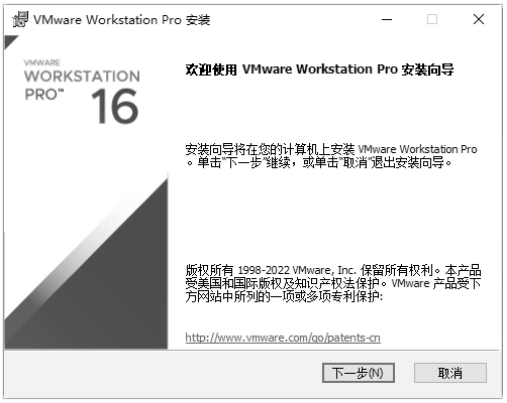

图 2-4 “欢迎使用 VMware Workstation Pro 安装向导”窗口

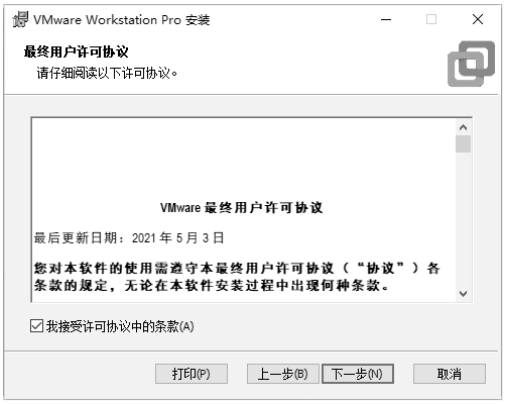

图 2-5 “最终用户许可协议”窗口

步骤 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，也可以保持默认设置，如图 2-6 所示。

步骤 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 2-7 所示。

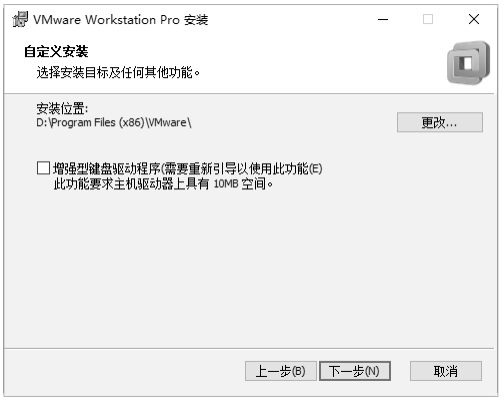

图 2-6 “自定义安装”窗口

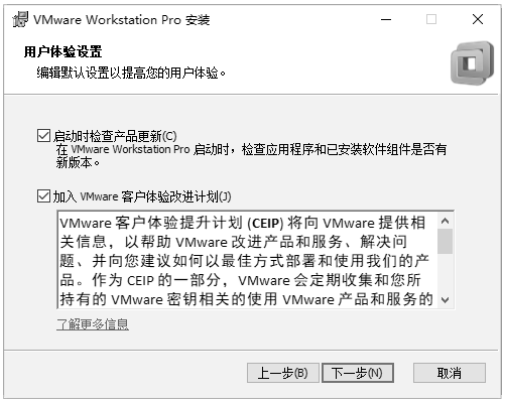

图 2-7 “用户体验设置”窗口

步骤 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，这里可以保持默认设置，如图 2-8 所示。

步骤 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 2-9 所示。

步骤 07 单击“安装”按钮，等待一段时间后虚拟机便安装完成，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 2-10 所示。

步骤 08 虚拟机安装完成以后，需要重新启动系统才可以使用虚拟机。至此，便完成了

VMware 虚拟机的下载与安装，如图 2-11 所示。

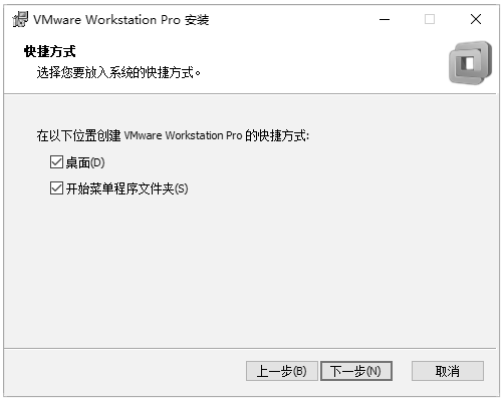

图 2-8 “快捷方式”窗口

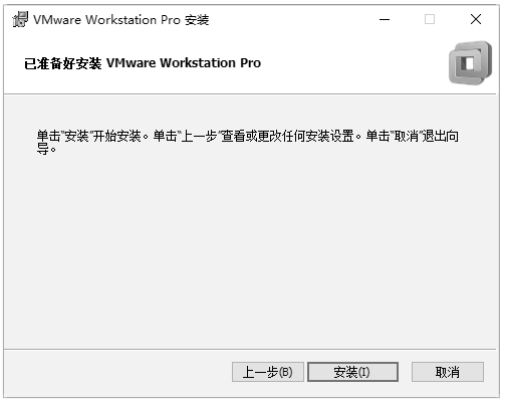

图 2-9 “已准备好安装 VMware Workstation Pro”窗口

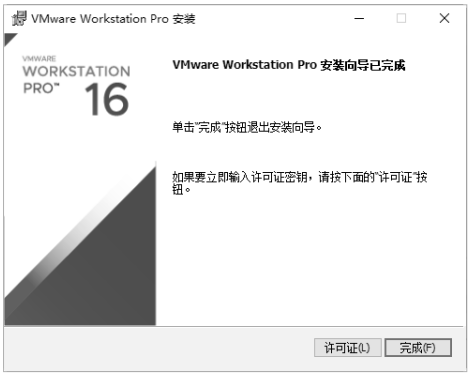

图 2-10 “VMware Workstation Pro 安装向导已完成”窗口

图 2-11　重新启动系统提示框

2.3　在虚拟机中安装操作系统

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，如 Windows、Linux 等，这样才能使用虚拟机创建的环境来实现网络安全测试。

2.3.1　安装 Windows 操作系统

在虚拟机中安装 Windows 操作系统是搭建网络安全测试环境的一个重要步骤，所有准备工作就绪后，接下来就可以在虚拟机中安装 Windows 操作系统了。具体操作步骤如下：

步骤 01 双击桌面的 VMware 虚拟机图标，启动 VMware 虚拟机软件，如图 2-12 所示。

步骤 02 单击“创建新的虚拟机”按钮，弹出“新建虚拟机向导”对话框，在其中选中“自定义”单选按钮，如图 2-13 所示。

步骤 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 2-14 所示。

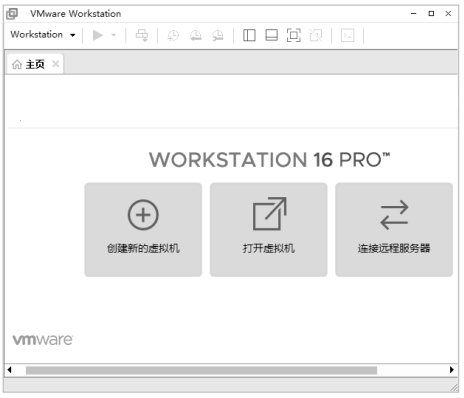

图 2-12　VMware 虚拟机软件

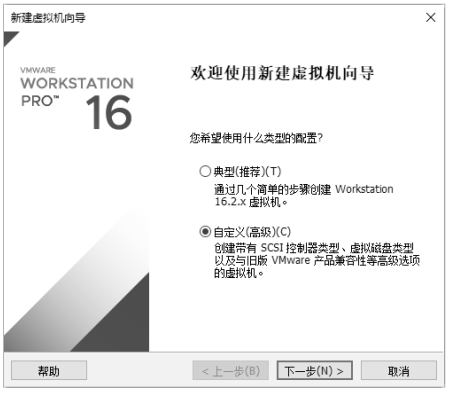

图 2-13　“新建虚拟机向导”对话框

步骤 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“安装程序光盘映像文件”单选按钮，如图 2-15 所示。

图 2-14　“选择虚拟机硬件兼容性”对话框

图 2-15　“安装客户机操作系统”对话框

步骤 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 2-16 所示。

步骤 06 单击“版本”下方的下拉按钮，在打开的下拉列表框中选择“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 2-17 所示。

图 2-16　“选择客户机操作系统”对话框

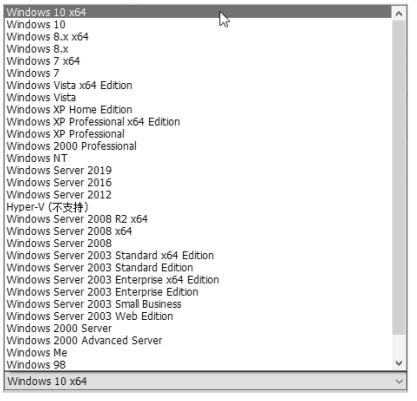

图 2-17　选择系统版本

步骤 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 2-18 所示。

步骤 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 2-19 所示。

图 2-18 “命名虚拟机”对话框

图 2-19 “处理器配置”对话框

步骤 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，注意内存不要低于 768MB，这里选择 1024MB 也就是 1GB 内存，如图 2-20 所示。

步骤 10 单击“下一步”按钮，进入“网络类型”对话框，选中“使用网络地址转换（NAT）（E）”单选按钮，如图 2-21 所示。

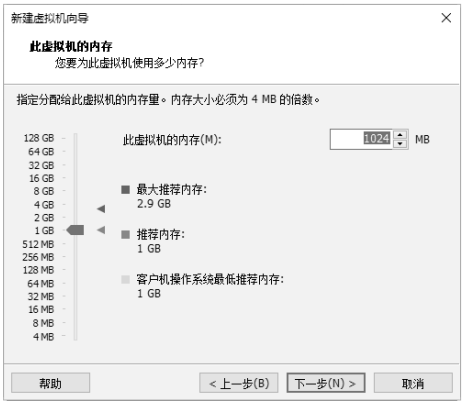

图 2-20 “此虚拟机的内存”对话框

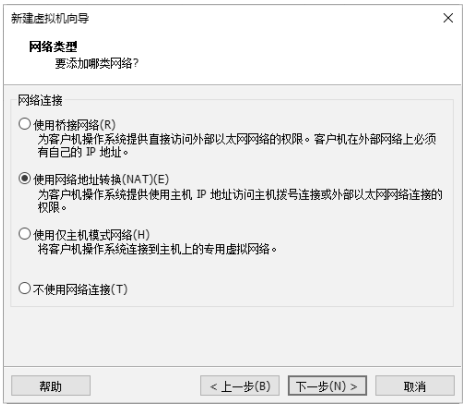

图 2-21 “网络类型”对话框

步骤 11 单击“下一步”按钮，进入“选择 I/O 控制器类型”对话框，选中“LSI Logic SAS”单选按钮，如图 2-22 所示。

步骤 12 单击“下一步”按钮，进入“选择磁盘类型”对话框，选中“NVMe”单选按钮，如图 2-23 所示。

步骤 13 单击“下一步”按钮，进入“选择磁盘”对话框，选中“创建新虚拟磁盘”单选按钮，如图 2-24 所示。

步骤 14 单击“下一步”按钮，进入“指定磁盘容量”对话框，设置“最大磁盘大小”为 60GB，选中“将虚拟磁盘拆分成多个文件”单选按钮，如图 2-25 所示。

图 2-22 “选择 I/O 控制器类型”对话框

图 2-23 “选择磁盘类型”对话框

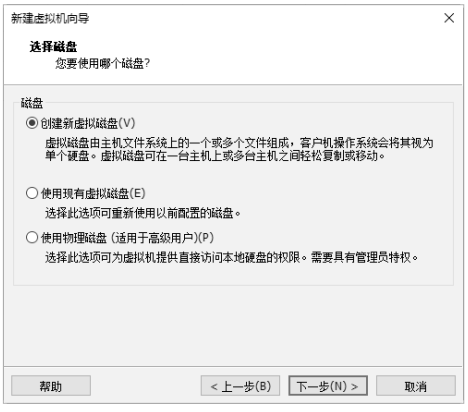

图 2-24 “选择磁盘”对话框

图 2-25 “指定磁盘容量”对话框

步骤 15 单击“下一步”按钮，进入“指定磁盘文件”对话框，这里保持默认设置即可，如图 2-26 所示。

步骤 16 单击“下一步”按钮，进入“已准备好创建虚拟机”对话框，如图 2-27 所示。

图 2-26 “指定磁盘文件”对话框

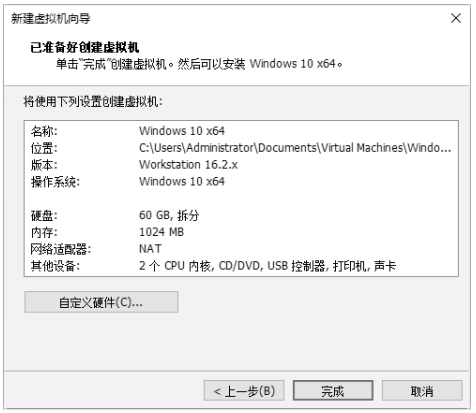

图 2-27 “已准备好创建虚拟机”对话框

步骤 17 单击“完成”按钮，便创建了一个新的虚拟机，如图 2-28 所示。这一步相当于组装了一台裸机计算机，其中的硬件配置可以根据实际需求进行更改。

步骤 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 2-29 所示。

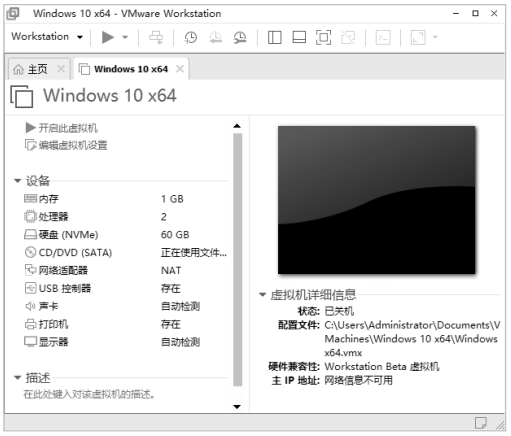

图 2-28　创建新虚拟机

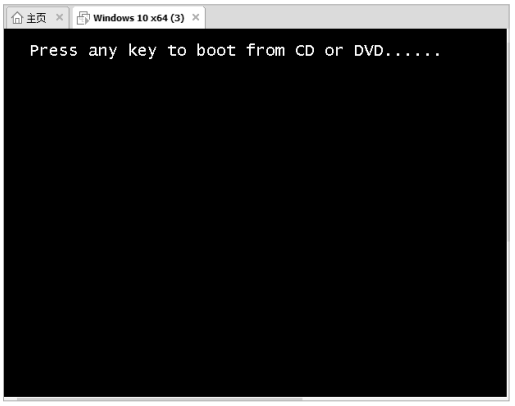

图 2-29　安装过渡窗口

步骤 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 2-30 所示。

步骤 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就完成了，安装的虚拟操作系统以文件的形式存放在硬盘中，如图 2-31 所示。

图 2-30　准备要安装的文件

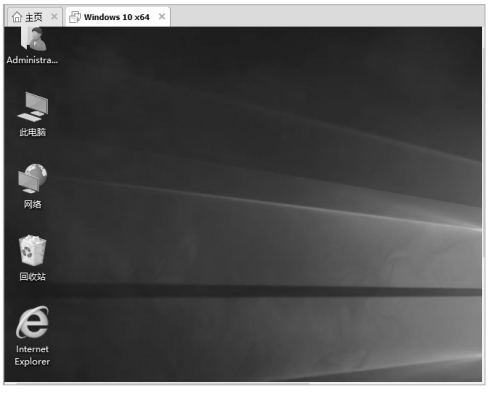

图 2-31　虚拟机操作系统界面

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后还需要安装各种驱动，如显卡、网卡、显卡等，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 工具的具体操作步骤如下：

步骤 01 启动虚拟机进入虚拟系统，如图 2-32 所示，然后按【Ctrl+Alt】组合键，切换到真实的计算机系统。

步骤 02 选择“虚拟机”→“安装 VMware Tools”命令，如图 2-33 所示，此时系统将自动弹出安装文件。

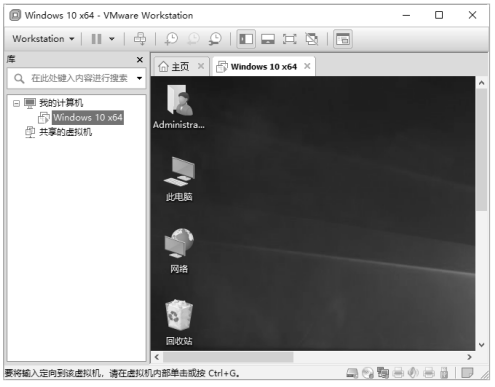

图 2-32　进入虚拟系统

图 2-33　选择“安装 VMware Tools”命令

步骤 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 2-34 所示。

步骤 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 2-35 所示。

图 2-34　“欢迎使用 VMware Tools 的安装向导”窗口

图 2-35　“选择安装类型”窗口

步骤 05 单击“下一步”按钮，进入“已准备好安装 VMware Tools”窗口，如图 2-36 所示。

步骤 06 单击“安装”按钮，进入“正在安装 VMware Tools”窗口，其中显示了 VMware Tools 工具的安装状态，如图 2-37 所示。

图 2-36　“已准备好安装 VMware Tools”窗口

图 2-37　“正在安装 VMware Tools”窗口

步骤 07 安装完成后，进入“VMware Tools 安装向导已完成”窗口，如图 2-38 所示。

步骤 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 2-39 所示。

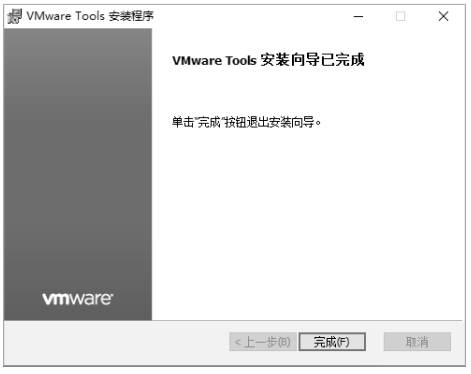

图 2-38 “VMware Tools 安装向导已完成”窗口

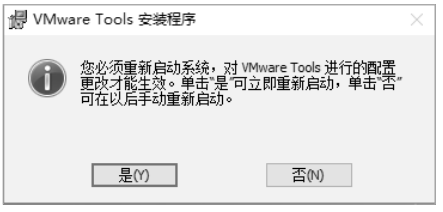

图 2-39　信息提示框

步骤 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”命令变成了“重新安装 VMware Tools”命令，如图 2-40 所示。

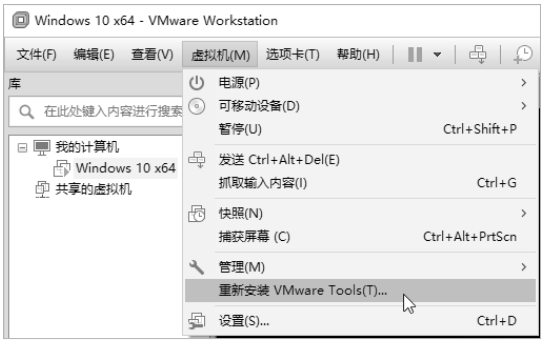

图 2-40 “重新安装 VMware Tools”命令

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。

2.4　Windows 操作系统中的 Hyper-V

Hyper-V 是微软的一款虚拟化技术，和 VMware、virtual 一样，都是主流的虚拟机工具。Hyper-V 的优势在于它与 Windows 操作系统紧密集成，不需要额外安装第三方虚拟化软件。

2.4.1　开启 Hyper-V 管理器

启用 Hyper-V，要求用户的系统是 Windows 10 或者 Windows 11 的专业版或企业版。启动

Hyper-V 之前，还需要先检查计算机是否开启了虚拟化。具体方法为：用鼠标右键单击任务栏，在弹出的快捷菜单中选择“任务管理器”命令，如图 2-41 所示。打开“任务管理器”窗口，在“性能”选项卡中选择“CPU”选项，可以看到“虚拟化”的状态是“已启用”，如图 2-42 所示。

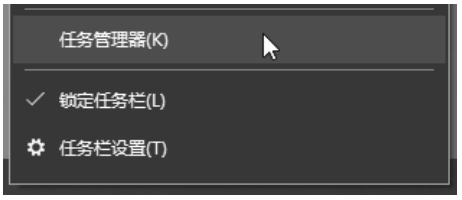

图 2-41　选择“任务管理器”命令

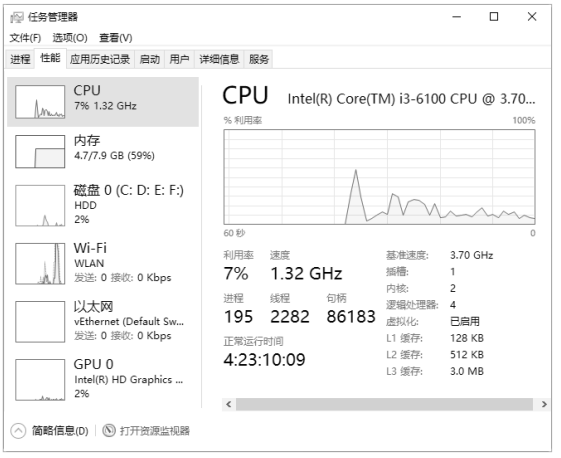

图 2-42　“任务管理器”窗口

计算机的虚拟化状态开启后，下面就可以开启 Hyper-V 了，具体操作步骤如下：

步骤 01 单击“开始”按钮，在打开的菜单中选择“Windows 系统”→“控制面板”命令，如图 2-43 所示。

步骤 02 打开“所有控制面板项”窗口，选择“程序和功能”选项，如图 2-44 所示。

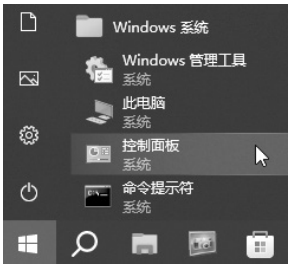

图 2-43　选择“控制面板”命令

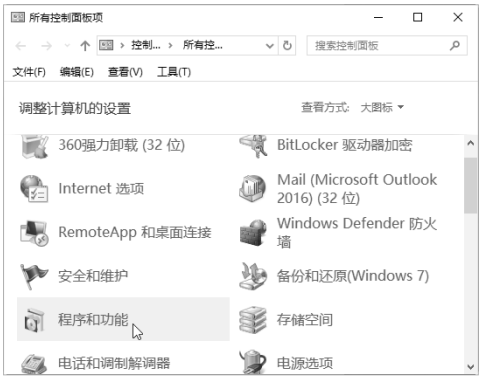

图 2-44　“所有控制面板项”窗口

步骤 03 在打开的“程序和功能”窗口中选择“启动或关闭 Windows 功能”选项，如图 2-45 所示。

步骤 04 打开“Windows 功能”窗口，选择 Hyper-V 复选框，如图 2-46 所示。

步骤 05 单击“确定”按钮，即可开始搜索需要的文件，如图 2-47 所示。

步骤 06 搜索完成后，会弹出“Windows 已完成请求的更改”信息提示框，单击“立即重新启动”按钮，即可开启 Hyper-V 功能，如图 2-48 所示。

步骤 07 计算机重启之后，单击“开始”按钮，在打开的菜单中选择“Windows 管理工具”→“Hyper-V 管理器”命令，如图 2-49 所示。

步骤 08 打开“Hyper-V 管理器”窗口，这样 Windows 自带的虚拟机工具就已经安装完成，如图 2-50 所示。

图 2-45　选择“启动或关闭 Windows 功能”选项

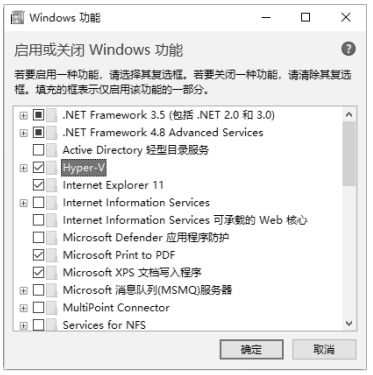

图 2-46　选择 Hyper-V 复选框

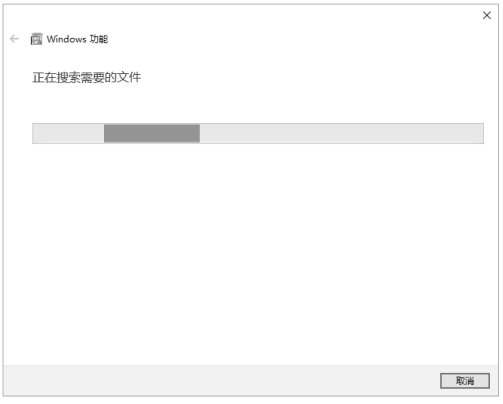

图 2-47　搜索需要的文件

图 2-48　开启 Hyper-V 功能

图 2-49　选择“Hyper-V 管理器”命令

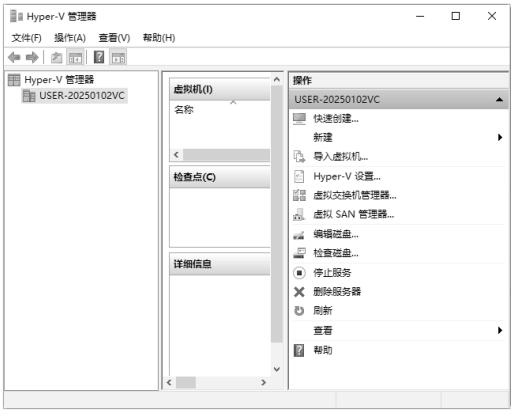

图 2-50　“Hyper-V 管理器”窗口

2.4.2　创建虚拟机

开启 Hyper-V 管理器后，就可以创建虚拟机了，具体操作步骤如下：

步骤 01 在“Hyper-V 管理器”窗口中，单击右侧“操作”工作区域中的“新建”选项，在弹出的快捷菜单中选择“虚拟机”选项，如图 2-51 所示。

步骤 02 打开“新建虚拟机向导”对话框，如图 2-52 所示。

图 2-51 选择“虚拟机”选项

图 2-52 “新建虚拟机向导”对话框

步骤 03 单击“下一步”按钮，打开“指定名称和位置”对话框，在这里设置虚拟机的名称和存储位置，如图 2-53 所示。

步骤 04 单击“下一步”按钮，打开“指定代数”对话框，如果想创建新版本的虚拟机，则选中“第二代”单选按钮，如图 2-54 所示。

图 2-53 “指定名称和位置”对话框

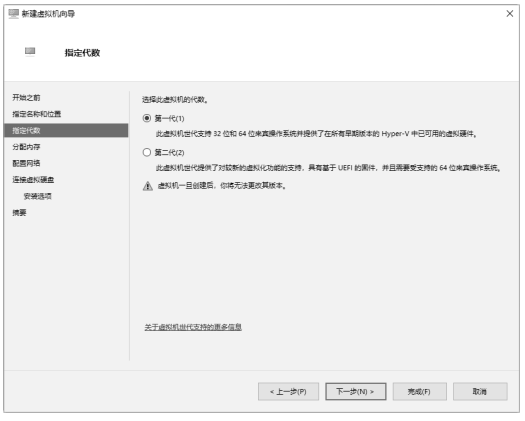

图 2-54 “指定代数”对话框

步骤 05 单击“下一步”按钮，打开“分配内存”对话框，可以根据内存的实际情况进行内存的分配操作，如图 2-55 所示。

步骤 06 单击“下一步”按钮，打开“配置网络”对话框，选择“未连接”选项，如图 2-56 所示。

步骤 07 单击“下一步”按钮，打开“连接虚拟硬盘”对话框，选中“创建虚拟硬盘”单选按钮，并设置硬盘的名称、位置与大小，如图 2-57 所示。

步骤 08 单击“下一步”按钮，打开“安装选项”对话框，选中“从可启动的 CD/DVD-ROM 安装操作系统”单选按钮，然后再选中“映像文件”单选按钮，如图 2-58 所示。

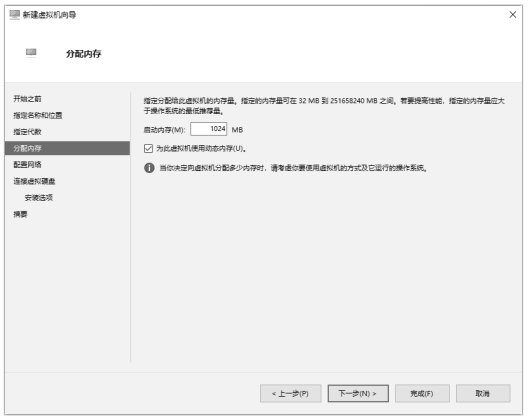

图 2-55 “分配内存”对话框

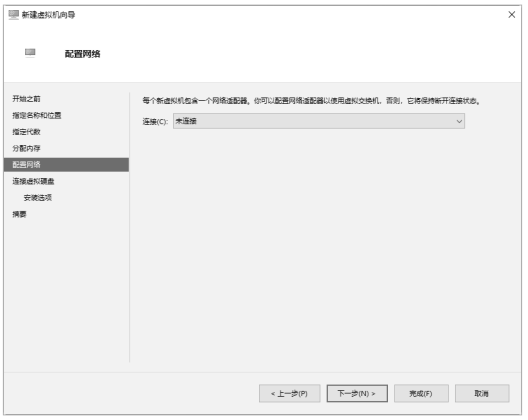

图 2-56 “配置网络”对话框

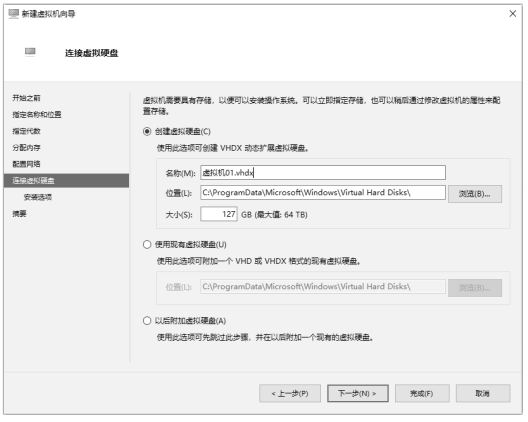

图 2-57 “连接虚拟硬盘”对话框

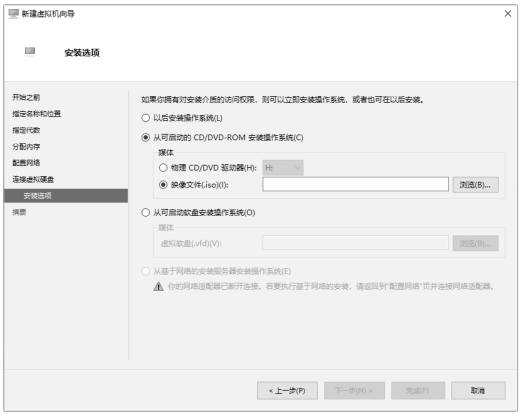

图 2-58 “安装选项”对话框

步骤 09 单击“浏览”按钮，弹出“打开”对话框，在其中选择 Windows 10 的 ISO 镜像文件，如图 2-59 所示。

步骤 10 单击“打开”按钮，返回到“安装选项”对话框，在其中可以看到所添加的镜像文件，如图 2-60 所示。

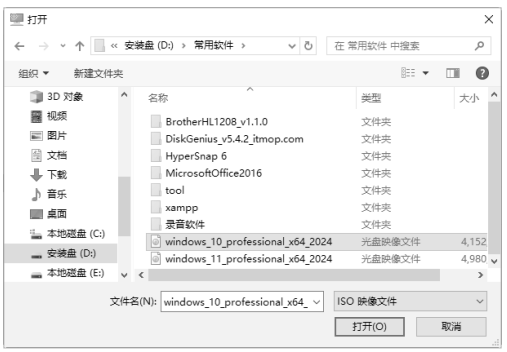

图 2-59 “打开”对话框

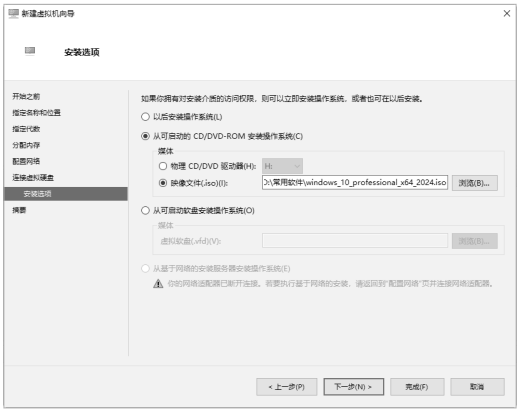

图 2-60 “安装选项”对话框

步骤 11 单击“下一步”按钮，打开“正在完成新建虚拟机向导”对话框，提示用户已经成功完成了新建虚拟机向导，如图 2-61 所示。

步骤 12 单击“完成”按钮，即可开始配置虚拟机参数，并显示配置进度，如图 2-62 所示。

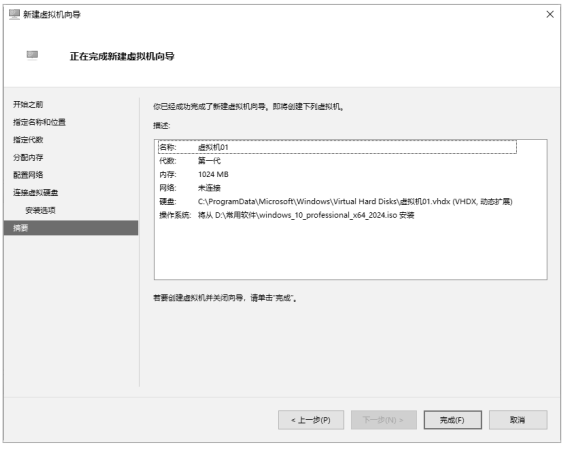

图 2-61 “正在完成新建虚拟机向导”对话框

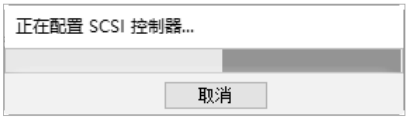

图 2-62 配置进度

步骤 13 配置完成后，打开“Hyper-V 管理器”窗口，在其中可以看到新创建的虚拟机，该虚拟机的名称为“虚拟机 01”，如图 2-63 所示。

图 2-63 “Hyper-V 管理器”窗口

2.4.3 为虚拟机安装操作系统

虚拟机创建完成后，就可以为虚拟机安装操作系统了，具体操作步骤如下：

步骤 01 单击“启动”按钮，开启虚拟机，如图 2-64 所示。

步骤 02 单击“连接”按钮，打开“虚拟机连接”窗口，提示用户正在连接到“虚拟机 01”，如图 2-65 所示。

步骤 03 如果是首次开启虚拟机，可能会出现如图 2-66 所示的报错信息。

步骤 04 单击 Restart now 按钮，重新启动虚拟机，就可以从刚才挂载的 ISO 镜像启动，如图 2-67 所示。

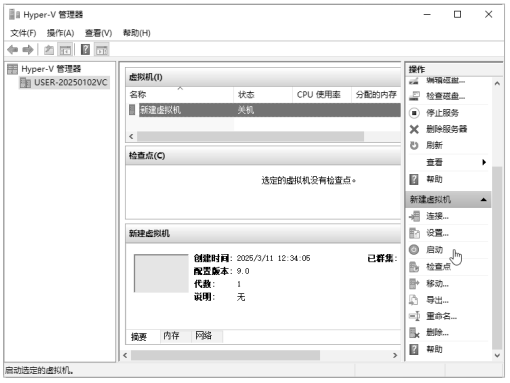

图 2-64　开启虚拟机

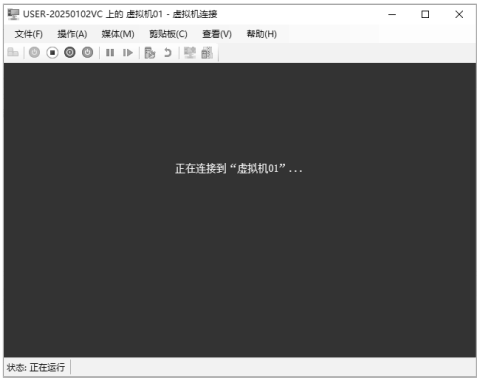

图 2-65　“虚拟机连接”窗口

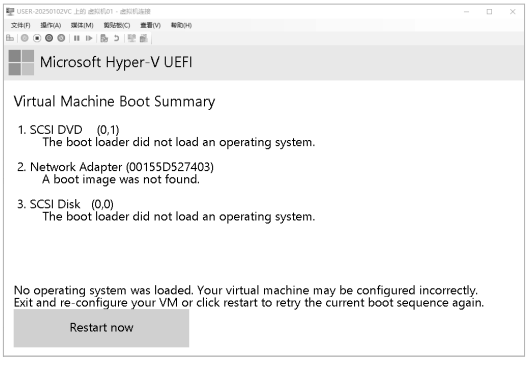

图 2-66　信息提示界面

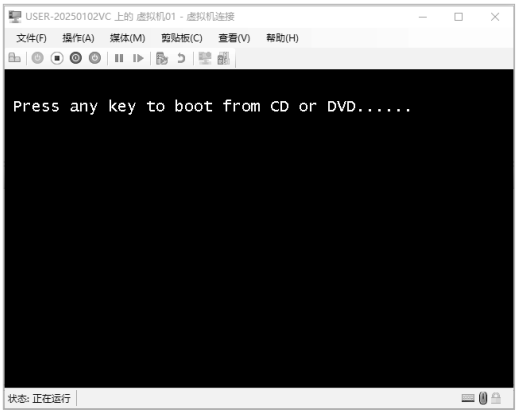

图 2-67　ISO 镜像启动

步骤 05 这样就可以安装 Windows 10 操作系统，进入 Windows 10 的安装过程，期间可能会有数次重启，如图 2-68 所示。

步骤 06 系统安装成功后，就会在 Hyper-V 虚拟机上拥有一个装有 Windows 10 系统的虚拟机，如图 2-69 所示。

图 2-68　安装过程

图 2-69　Windows 10 系统

2.4.4 管理和设置虚拟机

在 Hyper-V 管理器中，可以对虚拟机进行管理与设置，具体操作步骤如下：

步骤 01 在 Hyper-V 管理器中，选择虚拟机 01，然后单击鼠标右键，在弹出的快捷菜单中选择相应的命令，如“设置”“强行关闭”“关机”“保存”等，可以对虚拟机进行管理，如图 2-70 所示。

步骤 02 右击虚拟机 01，在弹出的快捷菜单中选择“设置”命令，打开“虚拟机 01 的设置”窗口，在“添加硬件”区域中可以对虚拟机的硬件进行设置，如图 2-71 所示。

图 2-70　右键快捷菜单

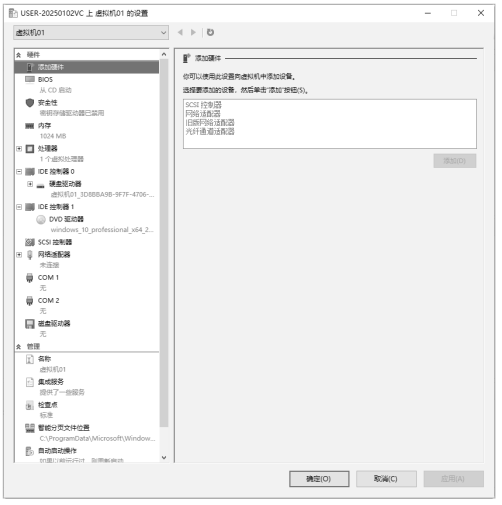

图 2-71　“添加硬件”区域

步骤 03 在“虚拟机 01 的设置”窗口中选择左侧列表框中的“内存”选项，在右侧内存设置区域中可以对虚拟机的内存大小进行设置，如图 2-72 所示。

步骤 04 在“虚拟机 01 的设置”窗口中选择左侧列表框中的“处理器”选项，在右侧处理器设置区域中可以对虚拟机的处理器个数进行设置，如图 2-73 所示。

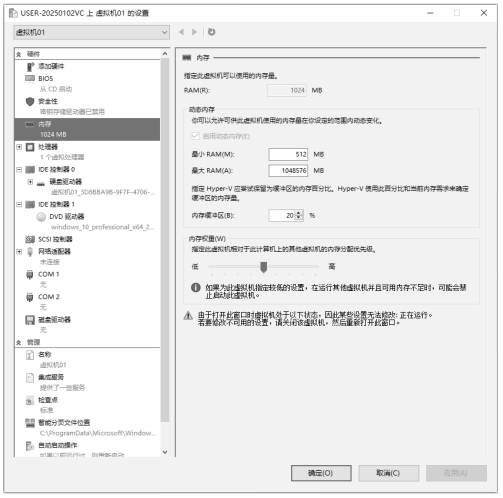

图 2-72　“内存”选项

图 2-73　“处理器”选项

步骤 05 在“虚拟机 01 的设置”窗口中选择左侧列表框中的“DVD 驱动器”选项，在右侧 DVD 驱动器设置区域中可以对虚拟机的映像文件进行设置，如图 2-74 所示。

步骤 06 在“虚拟机 01 的设置”窗口中选择左侧列表框中的“网络适配器”选项，在右侧网络适配器设置区域中可以对虚拟机的虚拟交换机与带宽管理进行设置，如图 2-75 所示。

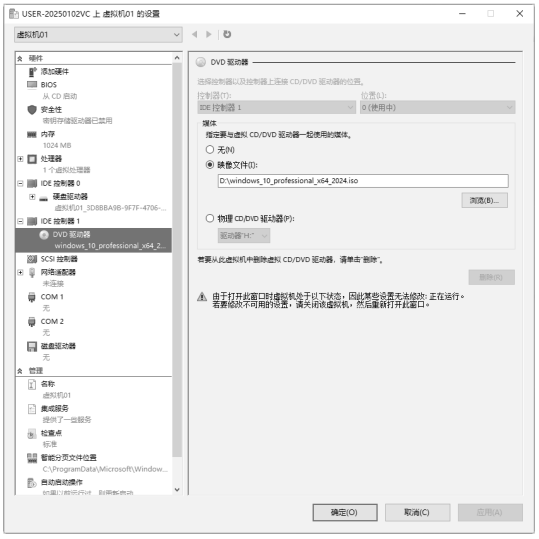

图 2-74 “DVD 驱动器”选项

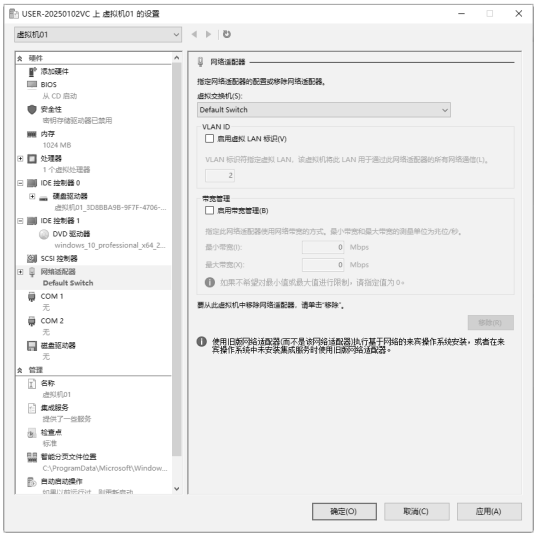

图 2-75 “网络适配器”选项

步骤 07 在“虚拟机 01 的设置”窗口中选择左侧列表框中的“名称”选项，在右侧名称设置区域中可以修改虚拟机的名称，如图 2-76 所示。

步骤 08 在“虚拟机 01 的设置”窗口中选择左侧列表框中的“集成服务”选项，在右侧集成服务设置区域中可以设置 Hyper-V 为虚拟机提供的服务，最后单击“确定”按钮，保存设置，如图 2-77 所示。

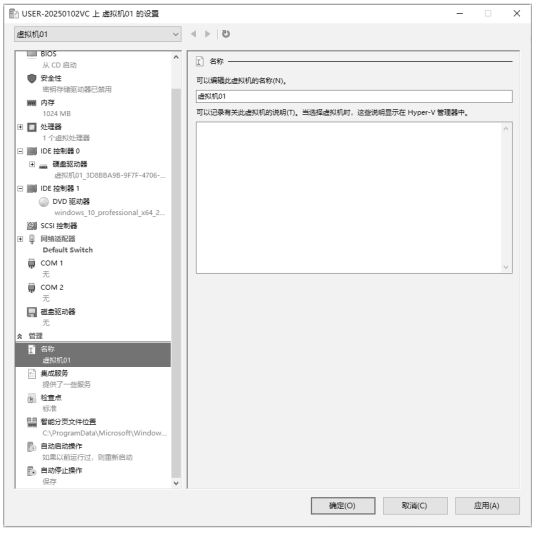

图 2-76 “名称”选项

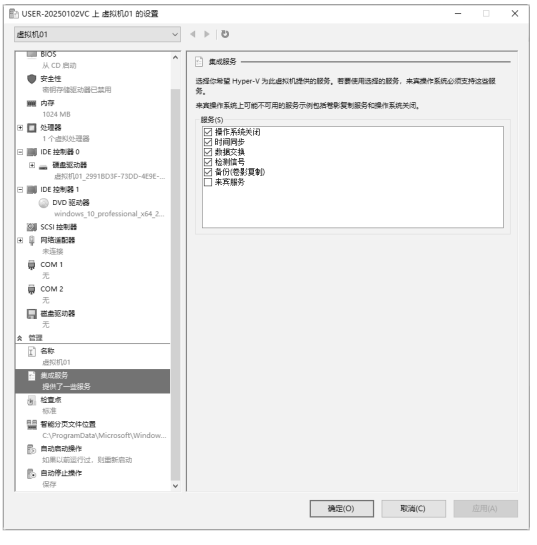

图 2-77 “集成服务”选项

2.4.5 管理和设置 Hyper-V 服务器

在信息化高速发展的今天，服务器作为数据存储和处理的中心，其性能和效率直接关系到业务的运行质量和成本。Hyper-V 作为微软推出的服务器虚拟化技术，为服务器管理带来了革命性的变化。

下面介绍管理与设置 Hyper-V 服务器的具体操作步骤。

步骤 01 在 Hyper-V 管理器中，选择左侧“操作”窗口中的“Hyper-V 设置”选项，如图 2-78 所示。

步骤 02 打开“Hyper-V 设置”窗口，选择“虚拟硬盘”选项，在打开的界面中可以指定存储虚拟硬盘文件的默认文件夹，如图 2-79 所示。

图 2-78 选择“Hyper-V 设置”选项

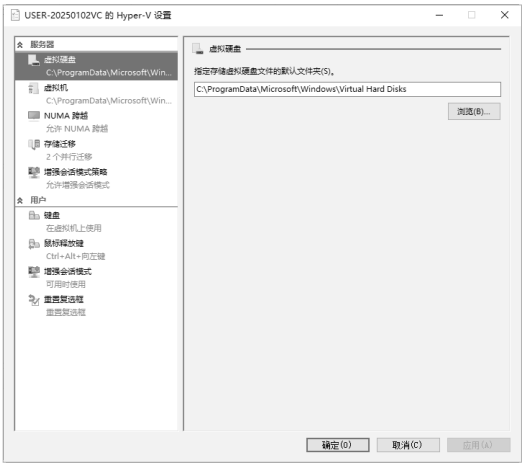

图 2-79 “虚拟硬盘”选项

步骤 03 在“Hyper-V 设置”窗口中选择“虚拟机”选项，在打开的界面中可以指定存储虚拟机配置文件的默认文件夹，如图 2-80 所示。

步骤 04 在“Hyper-V 设置”窗口中选择“NUMA 跨越”选项，选择“允许虚拟机跨越物理 NUMA 节点”复选框，如图 2-81 所示。

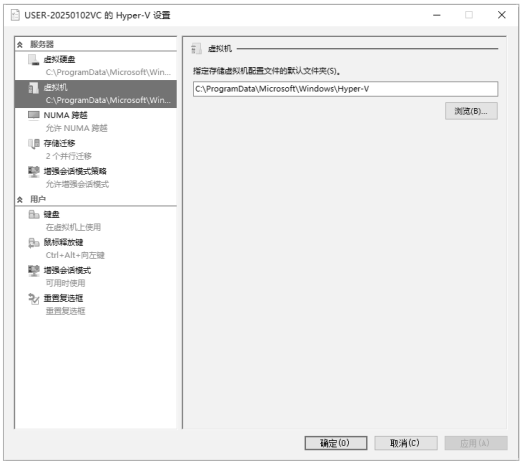

图 2-80 “虚拟机”选项

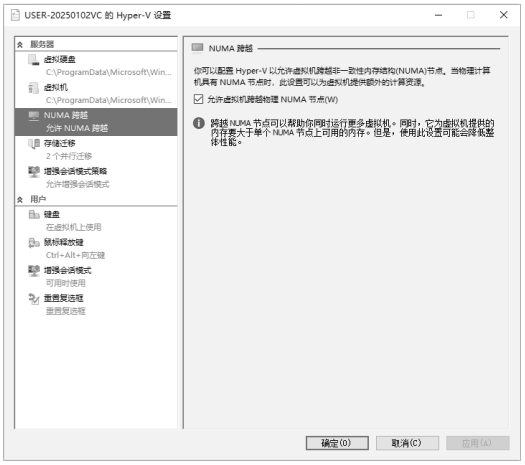

图 2-81 “NUMA 跨越”选项

步骤 05 在“Hyper-V 设置”窗口中选择“存储迁移”选项，在打开的界面中可以指定此计算机上可以同时执行的存储迁移数量，如图 2-82 所示。

步骤 06 在“Hyper-V 设置”窗口中选择“增强会话模式策略”选项，选择“允许增强会话模式”复选框，如图 2-83 所示。

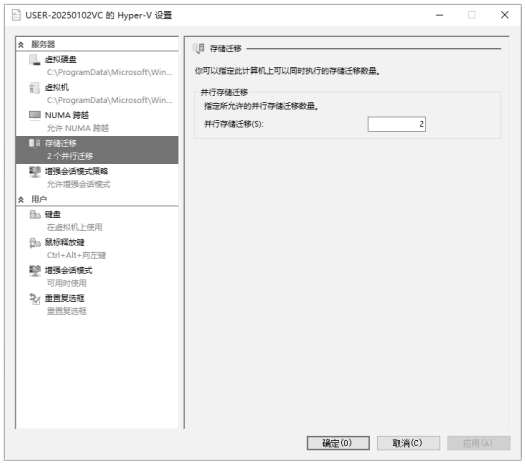

图 2-82 “存储迁移”选项

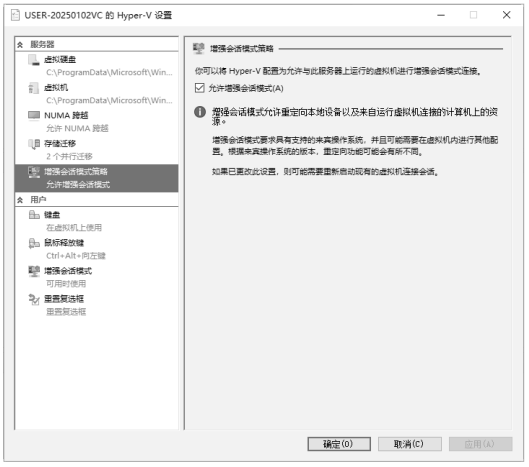

图 2-83 “增强会话模式策略”选项

步骤 07 在“Hyper-V 设置”窗口中选择“键盘”选项，在打开的界面中选中“在虚拟机上使用”单选按钮，这样当运行虚拟机连接时，可以在虚拟机上使用 Windows 键组合，如图 2-84 所示。

步骤 08 在“Hyper-V 设置”窗口中选择“鼠标释放键”选项，可以在“释放键”下拉列表框中选择释放鼠标的快捷键组合，如图 2-85 所示。

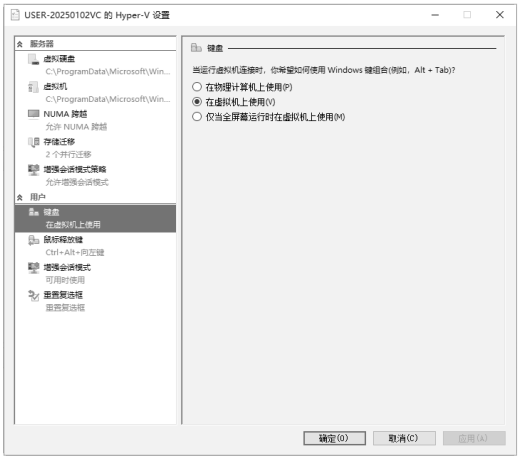

图 2-84 “键盘”选项

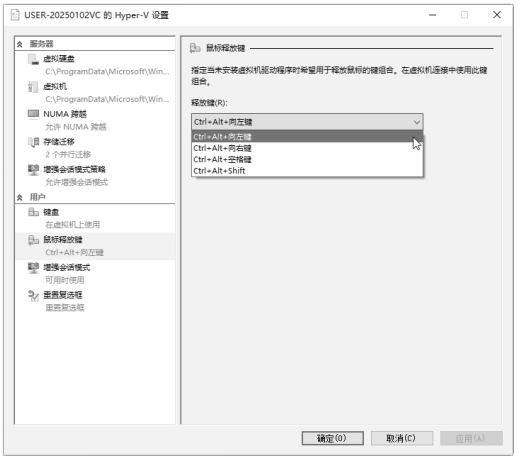

图 2-85 “鼠标释放键”选项

步骤 09 在“Hyper-V 设置”窗口中选择“增强会话模式”选项，在打开的界面中选择“使用增强会话模式”复选框，如图 2-86 所示。

步骤 10 在“Hyper-V 设置”窗口中选择“重置复选框”选项，在打开的界面中单击“重置虚拟机”按钮，可以清除选中时隐藏页面和消息的所有复选框，如图 2-87 所示。

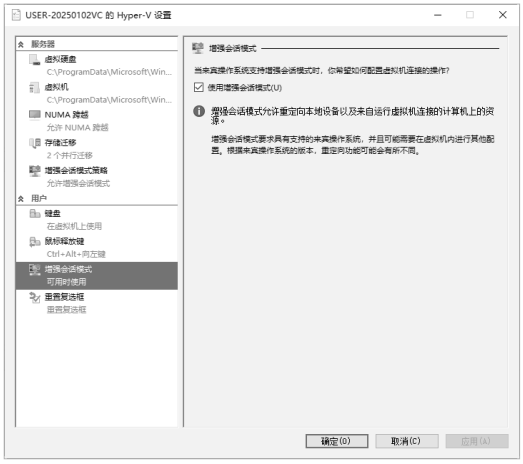

图 2-86 “增强会话模式”选项

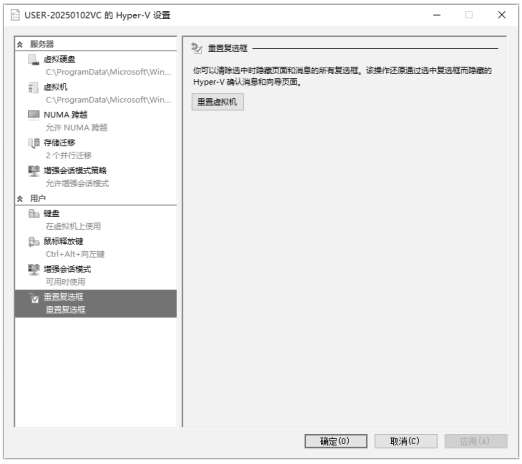

图 2-87 “重置复选框”选项

2.5 实战演练

2.5.1 实战 1：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，具体操作步骤如下：

步骤 01 右击桌面上的“开始”按钮，在弹出的快捷菜单中选择“任务管理器”命令，如图 2-88 所示。

步骤 02 打开“任务管理器”窗口，如图 2-89 所示。

图 2-88 选择“任务管理器”命令

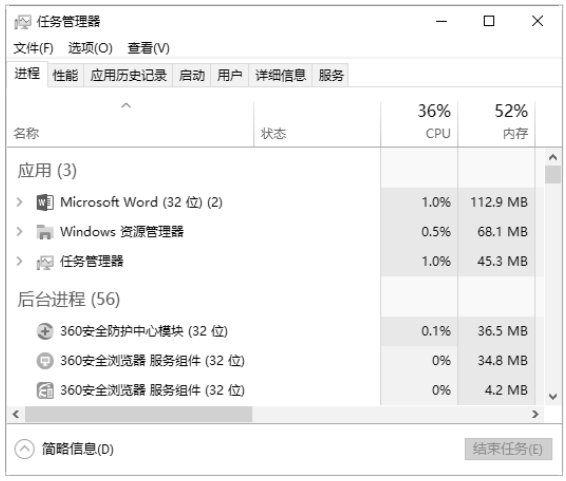

图 2-89 “任务管理器”窗口

步骤 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 2-90 所示。

步骤 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，禁止该启动项开机自动运行，如图 2-91 所示。

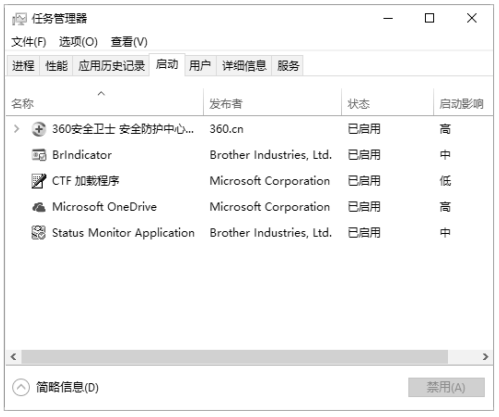

图 2-90 “启动”选项卡

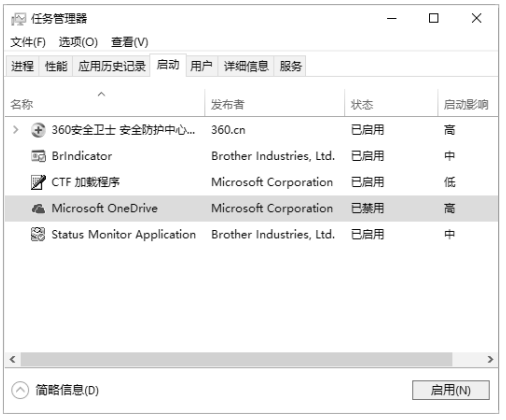

图 2-91　禁止开机启动项

2.5.2　实战 2：通过网络共享打印机

共享打印机是指将本地打印机通过网络共享给其他用户，这样其他用户也可以使用打印机完成打印服务。共享打印机的具体操作步骤如下：

步骤 01 右击“开始”按钮，在弹出的快捷菜单中选择“设置”命令，如图 2-92 所示。

步骤 02 打开“设置”窗口，选择“蓝牙和其他设备”选项，进入“蓝牙和其他设备”窗口，如图 2-93 所示。

图 2-92　选择“设置”命令

图 2-93 “蓝牙和其他设备”窗口

步骤 03 选择“打印机和扫描仪”选项，进入“打印机和扫描仪”窗口，如图 2-94 所示。

步骤 04 选择本台计算机中的打印机“Brother HL-1208 Printer”选项，显示打印机设置列表，如图 2-95 所示。

图 2-94 “打印机和扫描仪”窗口

图 2-95 打印机设置列表

步骤 05 选择“打印机属性”选项，弹出“Brother HL-1208 Printer 属性”对话框，选择“共享”选项卡，在其中选择“共享这台打印机”复选框，并设置打印机的共享名为“Brother HL-1208 Printer”，如图 2-96 所示。

步骤 06 双击桌面上的“此电脑”图标，打开“此电话”窗口，在左侧选择“网络”→MYCOMPUTER 选项，打开 MYCOMPUTER 对话框，在其中显示共享的打印机设备，如图 2-97 所示。

图 2-96 选择“共享这台打印机”复选框

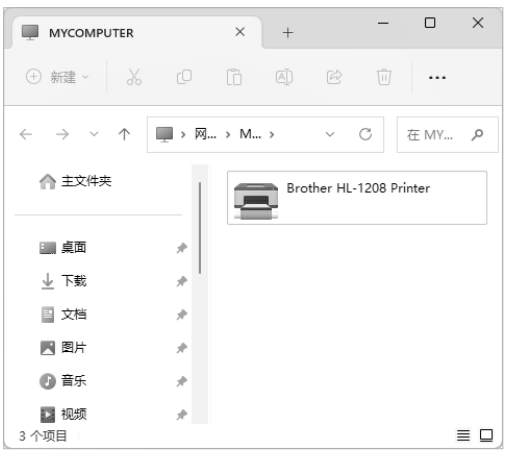

图 2-97 显示共享打印机设备