第 1 章

无线网络快速入门

无线网络，特别是无线局域网给我们的生活带来了极大的方便，为我们提供了无处不在的、高带宽的网络服务。但是，由于无线信道特有的性质，使得无线网络连接具有不稳定性，且容易受到黑客的攻击，从而大大影响了服务质量，本章就来介绍一些无线网络基础常识。

1.1 什么是无线网络

无线网络（wireless network）是采用无线通信技术实现的网络，与有线网络的用途十分类似，最大的不同在于传输媒介的不同，一般来说，无线网络可以分为狭义无线网络和广义无线网络两种。

1.1.1 狭义无线网络

狭义无线网络就是我们常说的无线局域网，是基于802.11b/g/n 标准的 WLAN 无线局域网，具有可移动性、安装简单、高灵活性和高扩展能力等特点。作为对传统有线网络的延伸，这种无线网络在许多特殊环境中得到了广泛的应用，如企业、学校、家庭等。这种网络的缺点是覆盖范围小，使用距离在 5m ～ 30m 范围内。如图 1-1 所示为一个简单的无线网络示意图。

图 1-1　无线网络示意图

随着无线数据网络解决方案的不断推出，全球 Wi-Fi 设备迅猛增长，相信在不久的将来，“不论在任何时间、任何地点都可以轻松上网”这一目标就会被实现。下面介绍一些有关无线网络的概念。

1. 无线网络的起源

无线网络的起源，可以追溯到第二次世界大战期间，当时的美军采用无线电信号进行资料传输，他们研发出了一套无线电传输科技，并且采用相当高强度的加密技术。当初美军乃至盟军都广泛使用这项技术。

这项技术让许多学者得到了灵感，1971 年，夏威夷大学（University of Hawaii）的研究员创造了第一个基于封包式技术的无线电通信网络。这个被称作 ALOHNET 的网络，可以算是相当早期的无线局域网络（WLAN）了。这最早的 WLAN 包括了 7 台计算机，它们采用双向星型拓扑（bi-directional

star topology），横跨四座夏威夷的岛屿，中心计算机放置在瓦胡岛（Oahu Island）上。从这时开始。无线网络可说是正式诞生了。如图 1-2 所示为一个星型拓扑结构示意图。

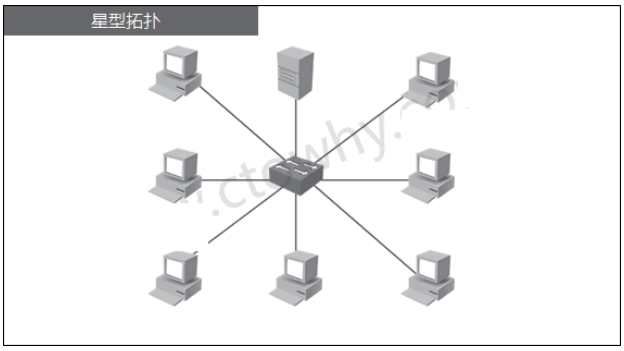

图 1-2　星型拓扑结构

2. 802.11 标准

802.11 标准第一个版本发表于 1997 年，其中定义了介质访问接入控制层（MAC 层）和物理层。物理层定义了工作在 2.4GHz 的 ISM 频段上的两种无线调频方式和一种红外传输的方式，总数据传输速率设计为 2Mb/s。两个设备之间的通信可以以自由直接（ad hoc）的方式进行，也可以在基站（Base Station，BS）或者访问点（Access Point，AP）的协调下进行。

作为无线网络重要发展标准，用户还是有必要了解一下 802.11 标准的发展的，具体内容如表 1-1 所示。

表 1-1　802.11 标准的发展史

标　　准	说　　明
802.11	1997 年，原始标准（2Mb/s，工作在 2.4GHz）
802.11a	1999 年，物理层补充（54Mb/s，工作在 5GHz）
802.11b	1999 年，物理层补充（11Mb/s，工作在 2.4GHz）
802.11c	符合 802.1d 的媒体接入控制层桥接（MAC Layer Bridging）
802.11d	根据各国无线电规定做的调整
802.11e	对服务等级（Quality of Service，QoS）的支持
802.11f	基站的互连性（IAPP，Inter-Access Point Protocol），2006 年 2 月被 IEEE 批准撤销
802.11g	2003 年，物理层补充（54Mb/s，工作在 2.4GHz）
802.11h	2004 年，无线覆盖半径的调整，室内（indoor）和室外（outdoor）信道（5GHz 频段）
802.11i	2004 年，无线网络的安全方面的补充
802.11n	2009 年 9 月通过正式标准，WLAN 的传输速率由 802.11a 及 802.11g 提供的 54Mb/s，提高达 350Mb/s 甚至高达 475Mb/s
802.11p	2010 年，这个协定主要用在车用电子的无线通信上

目前，无线网络及设备主要使用的是 802.11b/g/n 标准，尤其以 802.11g 最为普及，不过 802.11n 正在以飞快的速度赶超。

除了上面的 IEEE 标准，另外有一个被称为 IEEE 802.11b+ 的技术，通过 PBCC 技术（Packet

Binary Convolutional Code）在 IEEE 802.11b（2.4GHz 频段）基础上提供 22Mb/s 的数据传输速率。但这事实上并不是一个 IEEE 的公开标准，而是一项产权私有的技术。

3. Wi-Fi 联盟

Wi-Fi 联盟成立于 1999 年，是一家全球性的非盈利的商业联盟，拥有几百家企业会员，致力解决符合 802.11 标准的产品的生产和设备兼容性问题，从而推动无线局域网产业的发展，以增强移动无线、便携、移动和家用设备的用户体验为目标。自 2003 年 3 月 Wi-Fi 联盟开展此项认证以来，已经有超过 4000 多种产品获得了 Wi-Fi GERTIFIED 指定认证标志，有力地推动了 Wi-Fi 产品和服务在消费者市场和企业市场两方面的全面开展。

如图 1-3 所示为 Wi-Fi 联盟认证标志，该标志就是无线技术支持的象征，被广泛应用在智能手机、平板电脑、笔记本电脑和各种便携式设备上。

图 1-3　Wi-Fi 联盟认证标志

4. 无线网络的组成

无线网络有以下几个部分组成。

（1）站点（Station）：网络最基本的组成部分，通常指的是无线客户端。

（2）基本服务单元（Basic Service Set，BSS）：网络最基本的服务单元。最简单的服务单元可以只由两个无线客户端组成，客户端可以动态地连接（Associate）到基本服务单元中。

（3）分配系统（Distribution System，DS）：用于连接不同的基本服务单元。分配系统使用的媒介在逻辑上和基本服务单元使用的媒介是截然分开的，尽管它们物理上可能会是同一个媒介，例如同一个无线频道。

（4）接入点（Access Point，AP）：无线接入点既有普通有线接入点的能力，又有接入到上一层网络的能力。其实 AP 和无线路由器是有区别的，相比来说，无线路由器的功能更多，不过在基本功能上，两者并无实质性的区别，所以在实际应用中，都会将无线路由器称之为 AP。

（5）扩展服务单元（Extended Service Set，ESS）：由分配系统和基本服务单元组合而成。这种组合是逻辑上的，并非物理上的，不同的基本服务单元有可能在地理位置上相差甚远。分配系统也可以使用各种各样的技术。

（6）关口（Portal）：用于将无线局域网和有线局域网或其他网络联系起来，是一个逻辑成分。

以上组成部分使用了 3 种媒介——站点使用的无线媒介，分配系统使用的媒介，以及和无线局域网集成一起的其他局域网使用的媒介，物理上它们可能相互重叠。IEEE 802.11 只负责在站点使用的无线媒介上寻找地址，分配系统和其他局域网的寻址不属于无线局域网的范围。

5. 无线网络的运行原理

要想建立一个有效运行的无线网络，首先需要至少一个接入点，即 AP，如无线路由器，然后是至少一个无线客户端，即装有无线网卡的便携式设备，如笔记本电脑、手机、平板电脑等。硬件准备完成后，AP 每 100ms 将 SSID 信号封包广播一次，无线客户端可以借此决定是否要和这一个 SSID 的 AP 连接，使用者还可以设定要连接到哪一个 SSID。这就好比用户使用智能手机连接周边的 Wi-Fi 一样，可以有选择地进行连接，如图 1-4 所示。同时，Wi-Fi 系统开放对客户端的连接并支持漫游，这是 Wi-Fi 的优点。

图 1-4　智能手机连接 Wi-Fi

1.1.2 广义无线网络

广义无线网络主要包含 3 个方面，分别是无线个域网（WPAN）、无线局域网（WLAN）和无线广域网（WWAN），下面分别进行介绍。

1. 无线个域网

WPAN 是 Wireless Personal Area Network 的缩写，指无线个人局域网通信技术，即常说的无线个（人）域网。无线个（人）域网是一种采用无线连接的个人局域网。它通常被用在诸如电话、计算机、附属设备以及小范围（个人局域网的工作范围一般是在 10 米以内）内的数字助理设备之间的通信。

无线个（人）域网是一种与无线广域网、无线局域网并列但覆盖范围相对较小的无线网络。在网络构成上，无线个域网位于整个网络链的末端，用于实现同一地点终端与终端间的连接，如连接手机和蓝牙耳机等，其设备通常具有价格便宜、体积小、易操作和功耗低等优点。如图 1-5 所示为一个蓝牙耳机的外观。

支持无线个（人）域网的技术包括：蓝牙、ZigBee、超宽带（UWB）、红外技术（IrDA）、家庭射频（HomeRF）等，其中蓝牙技术在无线个（人）域网中使用最广泛。下面就来介绍几种主要的技术。

图 1-5　蓝牙耳机外观

图 1-6　蓝牙设置界面

（1）蓝牙（Bluetooth）：蓝牙是一种短距离无线通信技术，它可以用于在较小的范围内通过无线连接的方式实现固定设备或移动设备之间的网络互联，从而在各种数字设备之间实现灵活、安全、低动耗、低成本的语音和数据通信。

蓝牙技术的一般有效通信范围为 10m，强的可以达到 100m 左右，其最高速率可达 1Mb/s。其传输使用的功耗很低，广泛应用于无线设备，如 PDA、手机、智能电话等领域。如图 1-6 所示为一个智能手机的蓝牙设置界面，在其中可以开启与关闭蓝牙。

（2）红外技术（IrDA）：IrDA 是红外数据组织（Infrared Data Association）的简称，目前广泛采用的 IrDA 红外连接技术就是由该组织提出的。到目前为止，全球采用红外技术的设备超过了 5000 万部。

红外技术的主要特点有：利用红外传输数据，无须专门申请特定频段的使用执照；设备体积小、功率低；由于采用点到点的连接，数据传输所受到的干扰较小，数据传输速率高，可达 lGb/s。但存在一定的技术缺陷，如传输距离短、要求通信设备的位置固定、其点对点的传输连接无法灵活地组成网络等。如图 1-7 所示为计算机的红外线接口。

2. 无线局域网

WLAN 即 Wireless Local Area Networks 的缩写，指的就是无线局域网，也就是上面所说的“狭

义无线网络”，具体请参考上面狭义无线网络的内容。

3. 无线广域网

WWAN 是 Wireless Wide Area Network 的缩写，指无线广域网通信技术，即常说的无线广域网。无线广域网技术是使得笔记本电脑或者其他的设备装置在蜂窝网络覆盖范围内可以在任何地方连接到互联网。目前全球的无线广域网络主要采用 GSM 及 CDMA 技术，其他还有 4G 或者 5G 等技术。

简单来说，无线广域网指的就是通过通信设备和通信网络来上网，不管是以前的 GSM、EDGE 和 CDMA，还是现在的 4G、5G 网络，只要用电脑中的 PC 卡装 SIM 卡，或者把手机连在笔记本电脑上当做 Modem（“猫”）联网，都叫 WWAN。如图 1-8 所示为手机 SIM 卡，通过 SIM 卡，用户可以实现手机上网。

图 1-7　计算机的红外线接口

图 1-8　SIM 卡

1.2　认识无线路由器

无线路由器是用户用于上网、带有无线覆盖功能的路由器。它和有线路由器的作用是一样的，不同的是无线路由器多了一个或者几个天线，其作用就是提供无线网络的支持。除此以外，其他无论是外观，或者是内在配置页面都和同款型的有线路由器基本一模一样。

市面上每一个厂商的无线产品都有自己的特点，如图 1-9 所示为美版思科 Linksys WRT1900AC 双频无线路由器。该路由器有 4 个天线，支持用户根据需要对天线拆卸和换装，非常方便。另外，该路由器支持 802.11b/g 协议，其特点是使用多个天线来分工进行无线数据的接收与发送。

目前，市场占有率比较高的无线路由器是 TP-LINK 无线路由器，其性价比较高。如图 1-10 所示为 TP-LINK 千兆无线路由器，具有高速双核、覆盖更远、家长控制、一键禁用等功能。

图 1-9　双频无线路由器

图 1-10　TP-LINK 千兆无线路由器

为方便大家选购无线路由器，下面把目前市面上常见的无线设备厂商列举出来，包括厂商名称、官方网站以及个人建议等信息，如表 1-2 所示。

表 1-2　常见无线路由器

厂商名称	官方网站	个人建议
Linksys（领势）	www.linksys.com/cn/	价格昂贵，性能好
D-LINK（友讯）	www.dlink.com.cn	性价比不错，性能稳定
TP-LINK（普联）	www.tp-link.com.cn	性价比较高，市场占有率较高
Netgear（网件）	www.netgear.com.cn	价格比较贵，性能不错
ASUS（华硕）	www.asus.com.cn	不太稳定，价格还可以
Tenda（腾达）	www.tenda.com.cn	性价比较高，性能稳定
MERCURY（水星）	www.mercurycom.com.cn	价格较高，性能比较稳定

1.3　了解无线网卡

对于初次接触无线网络的用户来说，对无线网卡与无线上网卡是有些迷惑的，本节就来介绍什么是无线网卡，什么是无线上网卡。

1.3.1　无线网卡

无线网卡是终端无线网络设备，是不通过有线连接，采用无线信号进行数据传输的终端，有时也被称为 Wi-Fi 卡，根据接口类型的不同，主要有 PCI 无线网卡、PCMCIA 无线网卡、USB 无线网卡、Mini-PCI 无线网卡几类产品。

PCI 无线网卡：主要用于台式电脑，如图 1-11 所示为 TP-LINK 出品的 PCI 无线网卡。

PCMCIA 无线网卡：主要用于笔记本电脑，如图 1-12 所示为 Linksys 出品的 PCMCIA 无线网卡。

USB 无线网卡：这种网卡不管是台式机用户还是笔记本用户，只要安装了驱动程序（也有免安装驱动产品），都可以使用，如图 1-13 所示为 LB-LINK 出品的 USB 无线网卡。

图 1-11　PCI 无线网卡

图 1-12　PCMCIA 无线网卡

图 1-13　USB 无线网卡

Mini-PCI 无线网卡：为内置型无线网卡，被广泛应用于笔记本电脑，其优点是无须占用 PC 卡或 USB 插槽，并且免去了随身携一张 PC 卡或 USB 卡的麻烦。

这几种无线网卡在价格上差距不大，在性能和功能上也差不多，用户可根据自己的需要来选择。在距离上来说，无线网卡是依靠接收附近无线网络信号来上网的，这个信号源不能离得太远，一般是配合无线路由器来使用的，使用距离在 5m ～ 30m。

1.3.2　无线上网卡

无线上网卡指的是无线广域网卡，是依靠接收无线宽带运营商在公共场所发出的网络信号来上网的，这个信号源可以离无线上网的电脑很远，如联通的 CDMA1X 上网卡、移动的 GPRS 无线上网卡、电信的 EVDO 无线上网卡以及移动 / 联通的 4G、5G 卡等。

无线上网卡的作用与功能相当于有线的调制解调器，也就是我们俗称的“猫”。它可以在拥有无线信号覆盖的任何地方，利用无线上网卡来连接到互联网。从理论上来讲，假如你购买了移动的无线上网卡，那么在有移动基站信号覆盖的地方都可以进行无线上网。

一般来讲，无线上网卡的信号强度要比有线宽带差一些，但也能满足一些基础的网络应用，如浏览网页、收发邮件、QQ 聊天等。不过，随着无线网络技术发展，尤其是现在的 EVDO、TD-CDMA 等 4G/5G 技术的出现，无线上网速度已经大大提升。如图 1-14 所示为中国电信出品的天翼 4G 无线上网卡。

无线上网卡一般只针对笔记本电脑用户，常用的接口类型为 USB 接口，但也有 PCMCIA 接口类型的，如图 1-15 所示为中兴的 4G 无线上网卡。作为硬件，一般在用户购买无线上网套餐的时候，运营商会赠送无线上网卡。

图 1-14　天翼 4G 无线上网卡

图 1-15　中兴 4G 无线上网卡

1.4　了解天线

无线局域网中的天线可以扩展无线网络的覆盖范围。天线有多种类型，根据方向性的不同，有全向和定向两种。

1.4.1　全向天线

全向天线，即在水平方向上表现为 360° 都均匀辐射，也就是通常所说的无方向性；在垂直方向上表现为有一定宽度的波束，一般情况下波束宽度越小，增益越大。全向天线在移动通信系统中一般应用于郊区和乡村，覆盖范围大。如图 1-16 所示为连接在无线网卡上的全向天线。

图 1-16　无线网卡上的全向天线

室内全向天线适合于无线路由器之类的需要广泛覆盖信号的设备。它可以将信号均匀分布在中心点周围 360° 全方位区域，适用于连接点距离较近、分布角度范围大，且数量较多的情况，如无线路由器上的天线就是室内全向天线。如图 1-17 所示为目前常见的无线路由器天线形状。

图 1-17　无线路由器天线形状

简单来说，全向天线就相当于以天线为圆心，以传输距离为半径，画一个圆，这个圆内就是无线信号的覆盖范围。一般来说，在实际应用过程中，其半径多为 10m ～ 30m，这也是能在街道探测到那些穿出墙壁的信号的原因之一。如图 1-18 所示为全向天线的信号辐射示意图。

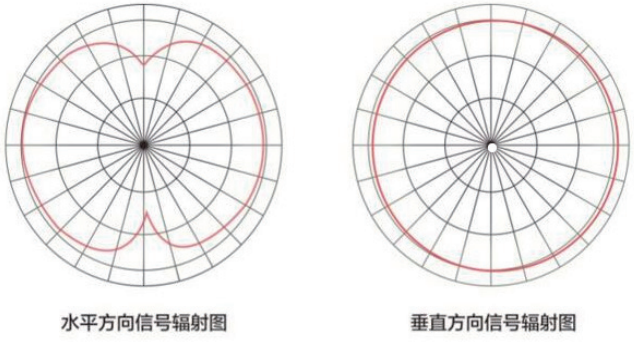

图 1-18　全向天线的信号辐射示意图

图 1-19　室外全向天线外观

如果将全向天线安装在户外，则必须安装在大楼顶端或高处，并且位于信号覆盖区的中央位置，以便于其他指向性天线装置通信，构成单点对多点的星型拓扑。如图 1-19 所示为一个室外全向天线的外观。

1.4.2　定向天线

定向天线在水平方向上表现为一定角度范围辐射，也就是通常所说的有方向性。与全向天线一样，波束宽度越小，增益越大。定向天线在通信系统中一般应用于通信距离远、覆盖范围小、目标密度大、频率利用率高的环境。

定向天线有各种不同的款式与形状，如贴片（Patch）天线、平板（Panel）天线和八木天线等，通常用于无线区域网络中短距离的桥接，例如跨马路的两栋大楼，或者空间扩展的厂房、仓库等。如图 1-20 所示左侧为八木天线，右侧为平板天线。

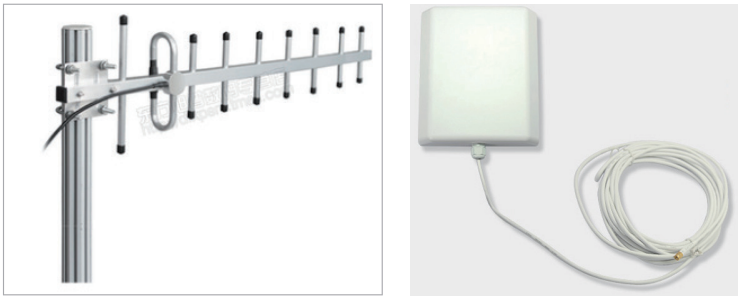

图 1-20　八木天线与平板天线

我们也可以这样来思考全向天线和定向天线之间的关系：全向天线会向四面八方发射信号，前后左右都可以接收到信号；定向天线就好像在天线后面罩一个碗状的反射面，信号只能向前面传递，射向后面的信号被反射面挡住并反射到前方，加强了前面的信号强度，可以想象定向天线的主要辐射范围像一个倒立的不太完整的圆锥，如图 1-21 所示为定向天线的信号辐射图。

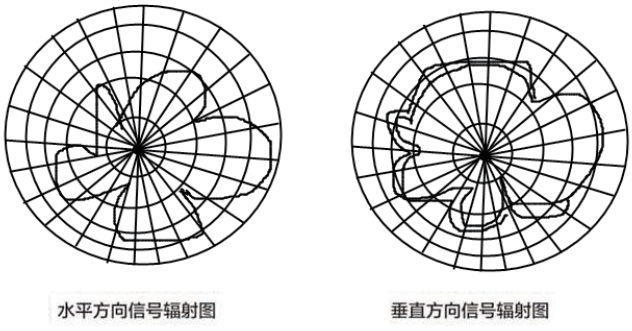

图 1-21　定向天线的信号辐射图

此外，还有专门用于长距离通信的高方向性天线，有极窄的波束宽度和很高的增益值，也被称为高增益指向性天线，如碟形天线和格状天线，通常用于点对点的通信连接，传输距离可高达 40km。因为这种天线的波束非常窄，天线彼此之间必须很精准地瞄准，而且天线之间可视且必须没有任何阻碍物。如图 1-22 所示为一个远距离栅格天线的使用示意图。

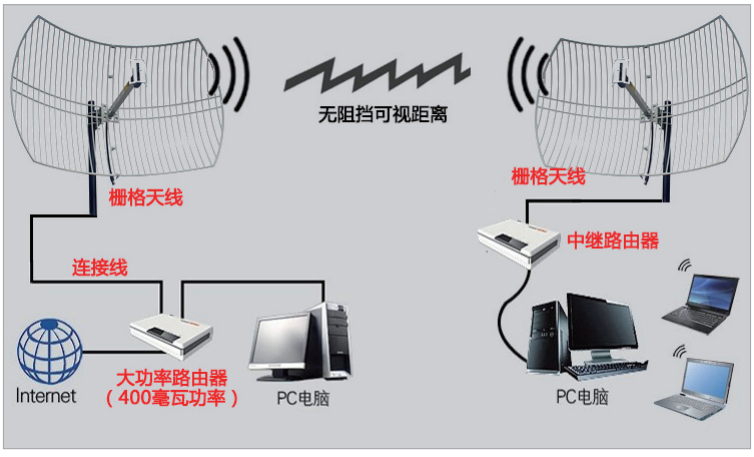

图 1-22　远距离栅格天线

图 1-23　室外定向天线

通过上文我们能够形象认识到什么是全向天线，什么是定向天线，那么在实际应用时该注意些什么呢？如果需要满足多个站点，并且这些站点是分布在 AP 的不同方向时，需要采用全向天线；如果集中在一个方向，建议采用定向天线；另外，还要考虑天线的接头形式是否和 AP 匹配、天线的增益大小等是否符合自己的需求。如图 1-23 所示为一个频率为 800-2500MHz、增益为 8/9dbi 的室外定向天线。

对于室外天线，在安装的过程中，天线与无线 AP 之间需要增加防雷设备；定向天线要注意天线的正面朝向远端站点的方向；天线应该安装在尽可能高的位置，和站点之间尽可能满足视距，即肉眼可见，中间避开障碍。

1.5　熟悉无线网络的术语

下面是无线网络安全中常会涉及的基本术语，了解这些术语，可以帮助用户更好地维护无线网络安全。

（1）Wi-Fi：一种允许电子设备连接到一个无线局域网的技术，通常使用 2.4G UHF 或 5G SHF ISM 射频频段。连接到无线局域网通常是有密码保护的；但也可是开放的，这样就允许任何在 WLAN 范围内的设备可以连接上。

（2）SSID：Service Set Identifier 的缩写，意思是服务集标识符。SSID 技术可以将一个无线局域网分为几个需要不同身份验证的子网络，每一个子网络都需要独立的身份验证，只有通过身份验证的用户才可以进入相应的子网络，防止未被授权的用户进入本网络。SSID 可以是任何字符，最大长度为 32 个字符。

（3）WAP：Wireless Application Protocol 的缩写，无线应用协议，是一项全球性的网络通信协议。它使移动互联网有了一个通行的标准，其目标是将互联网的丰富信息及先进的业务引入移动电话等无线终端之中。

（4）AP：Wireless Access Point 的缩写，无线访问接入点。如果将无线网卡看作有线网络中的以太网卡，AP 就是传统有线网络中的 HUB，也是目前组建小型无线局域网时最常用的设备之一。AP 相当于一个连接有线网和无线网的桥梁，其主要作用是将各个无线网络客户端连接到一起，然后将无线网络接入以太网。

（5）WEP：Wired Equivalent Privacy 的缩写，是目前比较常用的无线网络认证机制之一，它是 802.11 标准定义下的一种加密方式，简单地说，就是先在无线 AP 中设定一组密码，使用者要连接上这个无线 AP 时，必须输入相同的密码才能连接上，可以有效防止非法用户窃听或侵入无线网络。

（6）WPA：是 Wi-Fi Protected Access 的缩写，是一种基于标准的可互操作的 WLAN 安全性增强解决方案，可大大增强现有以及未来无线局域网系统的数据保护和访问控制水平。分为个人版（WPA-Personal）与企业版（WPA-Enterprise）两种。

（7）EAP：Extensible Authentication Protocol 的缩写，可扩展认证协议，为网络接入客户和认证服务器提供基础设施，为当前和未来的身份认证方法准备插件模块，通过支持多种认证协议来提供通信安全鉴权机制。

（8）GPS：全球定位系统 Global Positioning System 的缩写，又称全球卫星定位系统，是一个中

距离圆形轨道卫星导航系统。它可以为地球表面绝大部分地区（98%）提供准确的定位、测速和高精度的时间标准。

1.6　实战演练

1.6.1　实战 1：查看进程起始程序

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

Step01 在“命令提示符”窗口中输入查看 Svchost 进程起始程序的“Netstat-abnov”命令，如图 1-24 所示。

Step02 按 Enter 键，在反馈的信息中即可查看每个进程的起始程序或文件列表，这样就可以根据相关的知识来判断是否为病毒或木马发起的程序，如图 1-25 所示。

图 1-24　输入命令

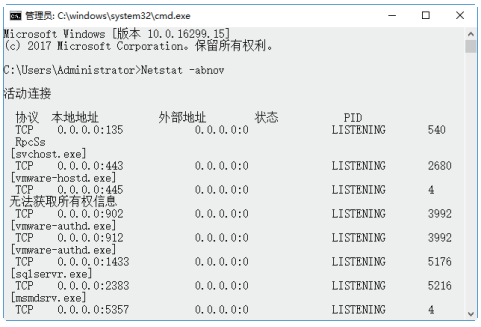

图 1-25　查看进程起始程序

1.6.2　实战 2：显示文件的扩展名

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

Step01 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 1-26 所示。

Step02 选择“查看”选项卡，在打开的功能区域中勾选“显示 / 隐藏”区域中的“文件扩展名”复选框，如图 1-27 所示。

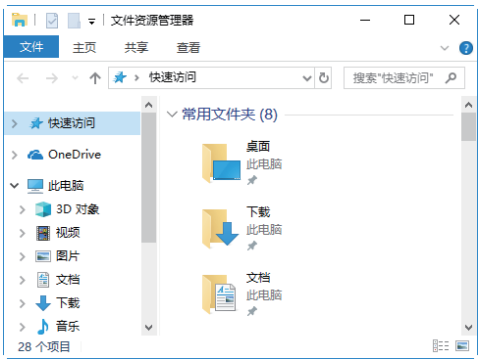

图 1-26　“文件资源管理器”窗口

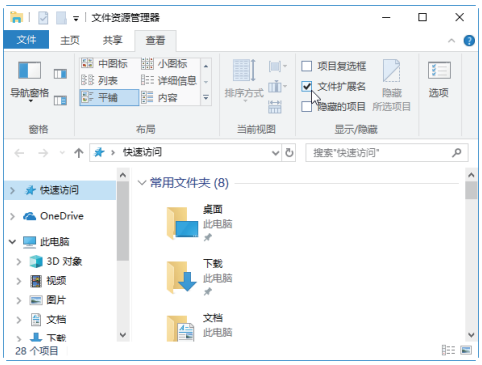

图 1-27　“查看”选项卡

Step 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 1-28 所示。

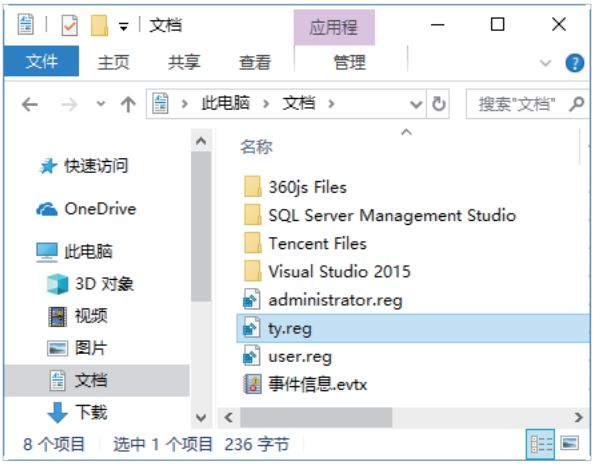

图 1-28　查看文件的扩展名

第 2 章

无线网络攻防必备知识

作为无线网络中的电脑或终端设备用户，要想使自己的设备不受或少受黑客的攻击，就必须了解一些黑客常用的入侵技能以及学习一些无线网络安全方面的基础知识，本章就来介绍有关这方面的内容，如无线网络的协议标准、IP 地址、端口以及黑客常用的攻击命令等。

2.1 无线网络协议标准

无线局域网（Wireless Local Area Network，WLAN）利用射频（Radio Frequency，RF）或是红外线（InfraRed Radiation，IR）技术，以无线的方式连接 2 部或多部需要交换数据的计算机设备，与以有线方式所构成的区域网络相比，无线局域网能利用简单的存取架构，利用无线的高移动性来应用于各个需要的应用领域之中。

无线网络的通信协议标准为 IEEE 802.11 协议族，主要包括 802.11、802.11b、802.11a、802.11g、802.11n 等。其中，802.11n 是在 802.11g 和 802.11a 之上发展起来的一项技术，最大的特点是速率提升，理论速率最高可达 600Mb/s，而目前业界主流为 300Mb/s。802.11 协议族相互之间的关系如图 2-1 所示。

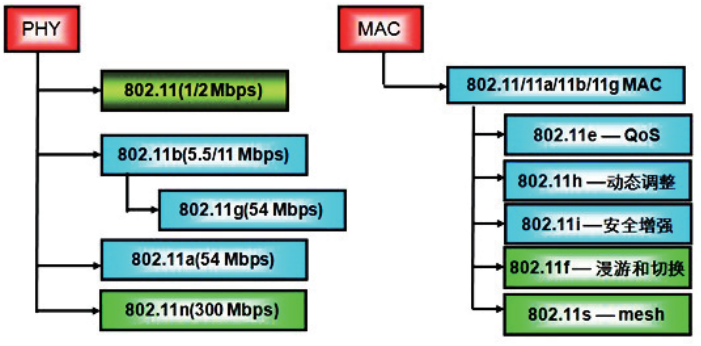

图 2-1　802.11 协议族相互之间的关系

IEEE 802.11 协议族各个协议发布的时间以及使用频率等信息如表 2-1 所示。

表 2-1　802.11 协议族的详细信息

	802.11	802.11b	802.11a	802.11g
标准发布时间	1997.7	1999.9	1999.9	2003.6
合法频率	83.5MHz	83.5MHz	32.5MHz	83.5MHz
频率范围	2.400-2.483GHz	2.400-2.483GHz	5.150-5.350GHz 5.725-5.850GHz	2.400-2.483GHz
非重叠信道	3	3	12	3
调制技术	FHSS/DSSS	CCK/DSSS	OFDM	CCK/OFDM
物理发送速率	1，2	1，2，5.5，11	6，9，12，18，24，36，48，54	6，9，12，18，24，36，48，54
理论上的最大 UDP 吞吐量（1500 byte）	1.7Mb/s	7.1Mb/s	30.9Mb/s	30.9Mb/s
理论上的最大 TCP/IP 吞吐量（1500 byte）	1.6Mb/s	5.9Mb/s	24.4Mb/s	24.4Mb/s
兼容性	N/A	与 11g 可互通	与 11b/g 不能互通	与 11b 可互通
无线覆盖范围	N/A	100m	50m	<100m

2.1.1　802.11

IEEE 802.11 是无线局域网通用的标准，是由 IEEE 所定义的无线网络通信的标准。虽然 Wi-Fi 使用了 802.11 的媒体访问控制层（MAC）和物理层（PHY），但是两者并不完全一致。

802.11 采用 2.4GHz 和 5GHz 这两个 ISM 频段。其中 2.4GHz 的 ISM 频段为世界上绝大多数国家采用，5GHz ISM 频段在一些国家和地区的使用情况比较复杂。

2.1.2　802.11a

802.11a 是 802.11 原始标准的一个修订标准，于 1999 年获得批准。802.11a 标准采用了与原始标准相同的核心协议，工作频率为 5GHz，最大原始数据传输率为 54Mb/s，达到了现实网络中等吞吐量（20Mb/s）的要求。

802.11a 的传输技术为多载波调制技术，被广泛应用在办公室、家庭、宾馆、机场等众多场合。它工作在 5GHzU-NII 频带，物理层速率可达 54Mb/s，传输层可达 25Mb/s；可提供 25Mb/s 的无线 ATM 接口和 10Mb/s 的以太网无线帧结构接口，以及 TDD/TDMA 的空中接口；支持语音、数据、图像业务；一个扇区可接入多个用户，每个用户可带多个用户终端。

由于 2.4GHz 频带使用率远高于 5GHz，采用 5GHz 的频带会让 802.11a 具有更少冲突的优点。然而，高载波频率也带来了负面效果。802.11a 几乎被限制在直线范围内使用，这导致必须使用更多的接入点；同样还意味着 802.11a 不能传播很远。

2.1.3　802.11b

802.11b 的出现是为了解决传输速率低的问题，如以前无线局域网的速率只有 1 ～ 2Mb/s，而许多应用是根据 10Mb/s 以太网速率设计的，这就限制了无线产品的应用种类。802.11b 从根本上改变了无线局域网的设计和应用现状。

1. 802.11b 标准简介

802.11b 无线局域网的带宽最高可达 11Mb/s，是 802.11 标准的 5 倍，扩大了无线局域网的应用领域。另外，也可根据实际情况采用 5.5Mb/s、2 Mb/s 和 1 Mb/s 带宽，实际的工作速率在 5Mb/s 左右，与普通的 10Base-T 规格有线局域网几乎处于同一水平。作为公司内部的设施，可以基本满足使用要求。802.11b 使用的是开放的 2.4GHz 频段，不需要申请就可使用。既可作为对有线网络的补充，也可独立组网，从而使网络用户摆脱网线的束缚，实现真正意义上的移动应用。

2. 802.11b 优点

802.11b 具有如下优点：

- 使用范围。802.11b 支持以百米为单位的范围（在室外为 300m，在办公环境中最长为 100m）。
- 可靠性。与以太网类似的连接协议和数据包确认提供可靠的数据传送和网络带宽的有效使用。
- 互用性。与以前的标准不同的是，802.11b 只允许一种标准的信号发送技术。
- 电源管理。802.11b 提供了网卡休眠模式，访问点将信息缓冲到 AP 端，延长了笔记本电脑电池的寿命。
- 漫游支持。当用户在楼房或公司部门之间移动时，允许在访问点之间进行无缝连接。

3. 802.11b 运作模式

802.11b 运作模式基本分为两种，点对点模式和基本模式。

（1）点对点模式是指无线网卡和无线网卡之间的通信方式，只要 PC 插上无线网卡即可与另一台具有无线网卡的 PC 连接，对于小型的无线网络来说，是一种方便的连接方式，最多可连接 256 台 PC。

（2）基本模式是指无线网络规模扩充或无线和有线网络并存时的通信方式，这是 802.11b 最常用的方式。此时，插上无线网卡的 PC 需要由接入点与另一台 PC 连接。接入点负责频段管理及漫游等指挥工作，一个接入点最多可连接 1024 台 PC（无线网卡）。

4. 802.11b 的典型解决方案

802.11b 无线局域网由于其便利性和可伸缩性，特别适用于小型办公环境和家庭网络。在室内环境中，针对不同的实际情况可以有不同的典型解决方案。

1）对等解决方案

对等解决方案是一种最简单的应用方案，只要给每台电脑安装一个无线网卡，即可相互访问。如果需要与有线网络连接，可以为其中一台电脑再安装一个有线网卡，无线网中其余电脑即利用这台电脑作为网关，访问有线网络或共享打印机等设备。

但对等解决方案是一种点对点方案，网络中的电脑只能一对一互相传递信息，而不能同时进行多点访问。如果要实现与有线局域网一样的互通功能，则必须借助接入点。

2）单接入点解决方案

接入点相当于有线网络中的集线器。无线接入点可以连接周边的无线网络终端，形成星型网络结构，同时通过 10Base-T 端口与有线网络相连，使整个无线网的终端都能访问有线网络的资源，并可通过路由器访问外部网络。

2.1.4　802.11g

与以前的 IEEE 802.11 协议标准相比，802.11g 草案有以下两个特点：一个是在 2.4GHz 频段使用正交频分复用（OFDM）调制技术，使数据传输速率提高到 20Mb/s 以上；另一个是能够与

802.11b 的 Wi-Fi 系统互联互通，可共存于同一 AP 的网络里，从而保障了后向兼容性。这样原有的 WLAN 系统可以平滑地向高速 WLAN 过渡，延长了 802.11b 产品的使用寿命，从而降低了用户的投资。

802.11g 的物理帧结构分为前导信号（preamble）、信头（header）和负载（payload）。前导信号主要用于确定移动台和接入点之间何时发送和接收数据，传输进行时告知其他移动台以免冲突，同时传送同步信号及帧间隔。前导信号完成，接收方才开始接收数据。信头在前导信号之后，用来传输一些重要的数据，比如负载长度、传输速率、服务等信息。由于数据率及要传送字节的数量不同，负载的包长变化很大，可以十分短也可以十分长。

在一帧信号的传输过程中，前导信号和信头所占的传输时间越多，负载用的传输时间就越少，传输的效率就越低。综合上述 3 种调制技术的特点，802.11g 采用了 OFDM 等关键技术来保障其优越的性能，分别对前导信号、信头、负载进行调制，这种帧结构称为 OFDM/OFDM 方式。

802.11g 兼容性指的是 802.11g 设备能和 802.11b 设备在同一个 AP 节点网络里互联互通。802.11g 的一个最大特点就是要保障与 802.11bWi-Fi 系统兼容，802.11g 可以接收 OFDM 和 CCK 数据，但传统的 Wi-Fi 系统只能接收 CCK 信息，这就产生了一个问题，即在两者共存的环境中如何解决由于 802.11b 不能解调 OFDM 格式信息帧头所带来的冲突问题。而为了解决上述问题，802.11g 采用了 RTS/CTS 技术。

2.1.5 802.11n

802.11n 是在 802.11g 和 802.11a 之上发展起来的一项技术，最大的特点是速率提升，理论速率最高可达 600Mb/s（目前业界主流为 300Mb/s）。802.11n 可工作在 2.4GHz 和 5GHz 两个频段。

802.11n 对用户应用的另一个重要好处是无线覆盖的改善。由于采用了多天线技术，无线信号（对应同一条信道）将通过多条路径从发射端到接收端，从而提供了分集效应。802.11n 的物理层与 MAC 层模型如图 2-2 所示。

图 2-2　802.11n 的物理层与 MAC 层模型

另外，除了吞吐和覆盖的改善，802.11n 技术还有一个重要的功能就是要兼容传统的 802.11 a/b/g，以保证现有网络的运行。

2.2 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。

2.2.1 IP 地址

IP 地址用于在 TCP/IP 通信协议中标记每台计算机的地址，通常使用十进制来表示，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）。

1. 认识 IP 地址

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

按照网络规模的大小，IP 地址可以分为 A、B、C、D、E 五类，其中 A、B、C 类 3 种为主要的类型地址，D 类专供多目传送地址，E 类用于扩展备用地址。

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

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

- 子网掩码：是与 IP 地址结合使用的一种技术。其主要作用有两个：一是用于确定 IP 地址中的网络号和主机号；二是用于将一个大的 IP 网络划分为若干小的子网络。
- 默认网关：一台主机如果找不到可用的网关，就把数据包发送给默认指定的网关，由这个网关来处理数据包。
- DNS：其服务用于将用户的域名请求转换为 IP 地址。

2. 查看 IP 地址

计算机的 IP 地址一旦被分配，可以说是固定不变的，因此，查询出计算机的 IP 地址，在一定程度上就完成了黑客入侵的前提工作。使用 ipconfig 命令可以获取本地计算机的 IP 地址和物理地址，具体的操作步骤如下：

Step 01 右击“开始”按钮，在弹出的快捷菜单中选择“运行”选项，如图 2-3 所示。

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 2-4 所示。

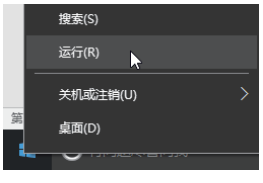

图 2-3　选择“运行”选项

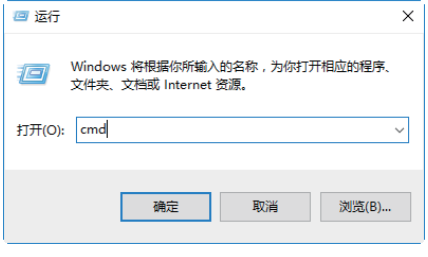

图 2-4　输入“cmd”命令

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，可显示出本机的 IP 配置相关信息，如图 2-5 所示。

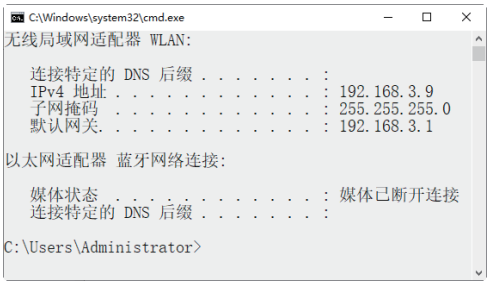

图 2-5　查看 IP 地址

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。

2.2.2　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，即无论将带有这个地址的硬件（如网卡、集线器、路由器等）接入到网络的何处，MAC 地址都是相同的，它由厂商写在网卡的 BIOS 里。

1. 认识 MAC 地址

MAC 地址通常表示为 12 个十六进制数，每两个十六进制数之间用冒号隔开，如 08:00:20:0A:8C:6D 就是一个 MAC 地址，其中前 6 位（08:00:20）代表网络硬件制造商的编号，它由 IEEE 分配，而后 3 位（0A:8C:6D）代表该制造商所制造的某个网络产品（如网卡）的系列号。每个网络制造商必须确保它所制造的每个以太网设备前 3 个字节都相同，后 3 个字节不同，这样，就可以保证世界上每个以太网设备都具有唯一的 MAC 地址。

知识链接　IP 地址与 MAC 地址的区别在于：IP 地址基于逻辑，比较灵活，不受硬件限制，也容易记忆；MAC 地址在一定程度上与硬件一致，基于物理层面，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。

2. 查看 MAC 地址

在“命令提示符”窗口中输入“ipconfig /all”命令，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，这就是用户计算机的网卡地址，它是唯一的，如图 2-6 所示。

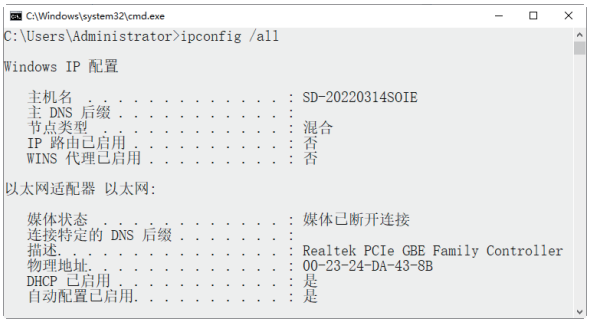

图 2-6　查看 MAC 地址

2.3　认识端口

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，范围是 0 ～ 65535（256×256-1）。

2.3.1　查看系统的开放端口

经常查看系统开放端口的状态变化，可以帮助计算机用户及时提高系统安全，防止黑客通过端口入侵计算机。用户可以使用 netstat 命令查看自己系统的端口状态，具体的操作步骤如下：

Step 01 打开“命令提示符”窗口，在其中输入“netstat -a -n”命令，如图 2-7 所示。

Step 02 按 Enter 键，可看到以数字显示的 TCP 和 UCP 连接的端口号及其状态，如图 2-8 所示。

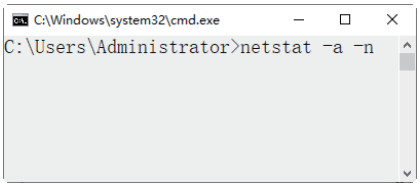

图 2-7　输入“netstat -a -n”命令

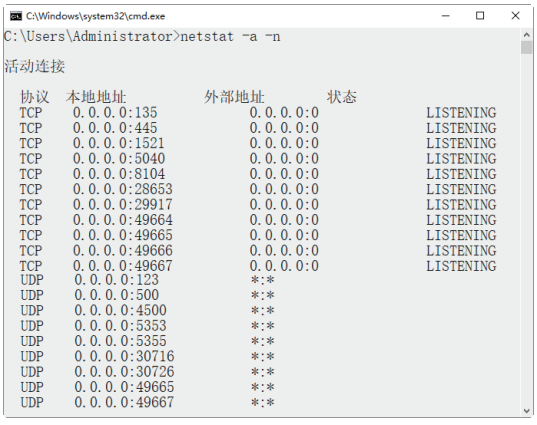

图 2-8　TCP 和 UCP 连接的端口号

2.3.2　关闭不必要的端口

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

以关闭 WebClient 服务为例，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选择“控制面板”选项，如图 2-9 所示。

Step 02 打开“控制面板”窗口，双击“管理工具”图标，如图 2-10 所示。

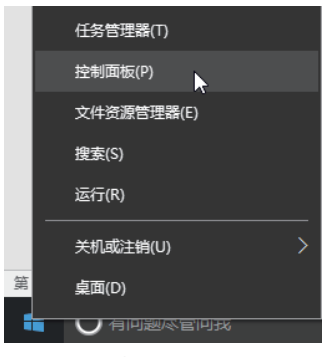

图 2-9　选择“控制面板”选项

图 2-10　“控制面板”窗口

Step03 打开“管理工具”窗口，双击“服务”图标，如图 2-11 所示。

Step04 打开“服务”窗口，找到 WebClient 服务项，如图 2-12 所示。

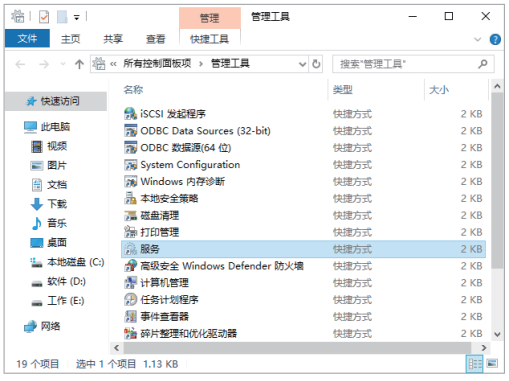

图 2-11 “服务”图标

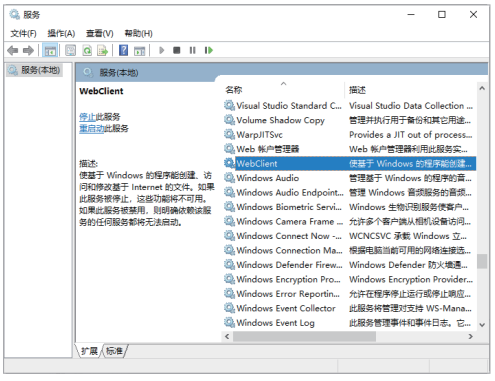

图 2-12 “服务”窗口

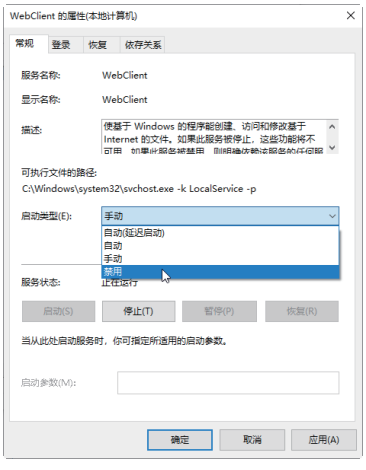

图 2-13 选择“禁用”选项

Step05 双击该服务项，打开“WebClient 的属性”对话框，在“启动类型”下拉列表框中选择“禁用”选项，然后单击“确定”按钮禁用该服务项的端口，如图 2-13 所示。

2.3.3 启动需要开启的端口

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

Step01 这里以上述停止的 WebClient 服务端口为例。在“WebClient 的属性”对话框中的“启动类型”下拉列表框中选择“自动”选项，如图 2-14 所示。

Step02 单击“应用”按钮，激活“服务状态”下的“启动”按钮，如图 2-15 所示。

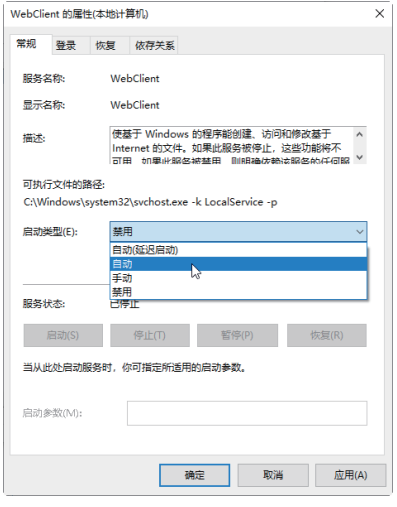

图 2-14 选择“自用”选项

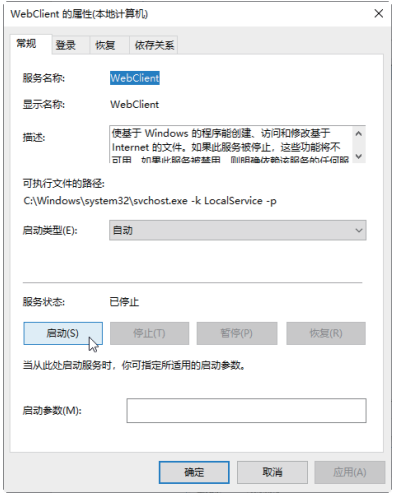

图 2-15 选择“启动”按钮

Step03 单击“启动”按钮，启动该项服务，再次单击“应用”按钮，在“WebClient 的属性”对话框中可以看到该服务的“服务状态”已经变为“正在运行”，如图 2-16 所示。

Step04 单击“确定”按钮，返回“服务”窗口，此时即可发现 WebClient 服务的“状态”变为“正在运行”，这样就成功开启了 WebClient 服务对应的端口，如图 2-17 所示。

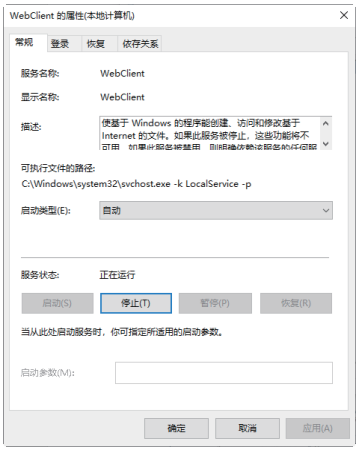

图 2-16　启动服务项

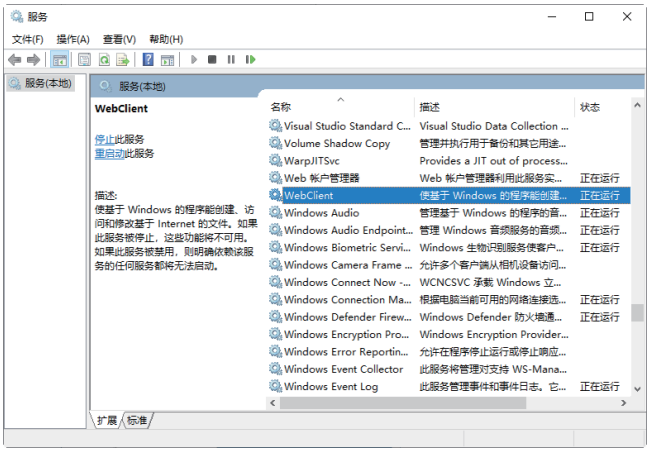

图 2-17　WebClient 服务的状态为“正在运行”

2.4　黑客常用的 DOS 命令

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

2.4.1　切换目录路径的 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，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：

Step01 在“命令提示符”窗口中输入“cd c:\”命令，按 Enter 键，将目录切换为 C:\，如图 2-18 所示。

Step02 如果想进入 C:\Windows\system32 目录中，则需在上面的“命令提示符”窗口中输入“cd Windows\system32”命令，按 Enter 键即可将目录切换为 C:\Windows\system32，如图 2-19 所示。

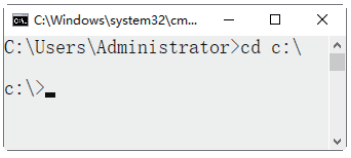

图 2-18　目录切换到 C 盘

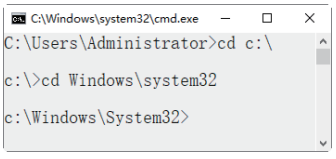

图 2-19　切换到 C 盘子目录

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 2-20 所示。

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 2-21 所示。

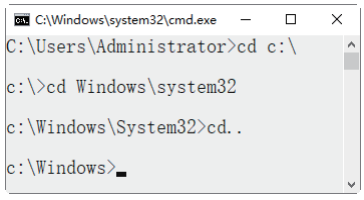

图 2-20　返回上一级目录

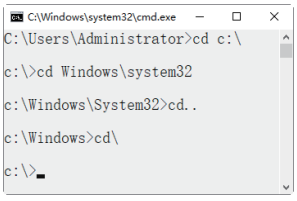

图 2-21　返回根目录

2.4.2　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 命令的语法格式如下：

```
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。

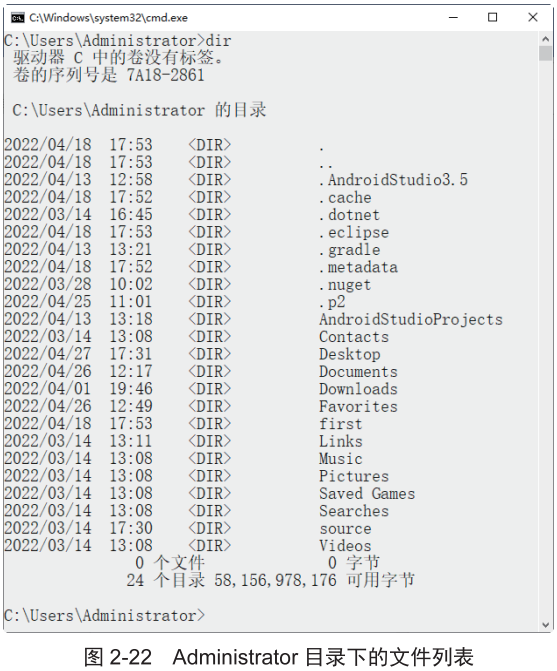

图 2-22　Administrator 目录下的文件列表

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，具体的操作步骤如下：

Step 01 在“命令提示符”窗口中输入“dir”命令，按 Enter 键，查看当前目录下的文件列表，如图 2-22 所示。

Step 02 在“命令提示符”窗口中输入“dir d:/ a:d”命令，按 Enter 键，查看 D 盘下的所有文件的目录，如图 2-23 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，列出 c:\windows 目录下的隐藏文件，如图 2-24 所示。

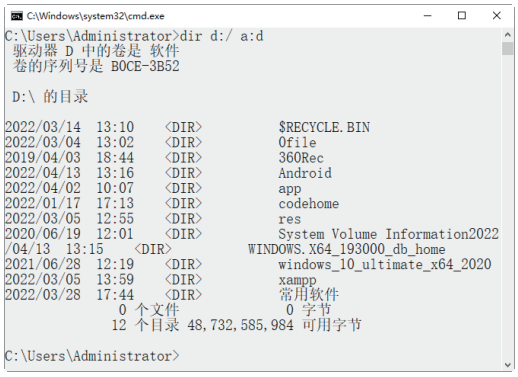

图 2-23　D 盘下的文件列表

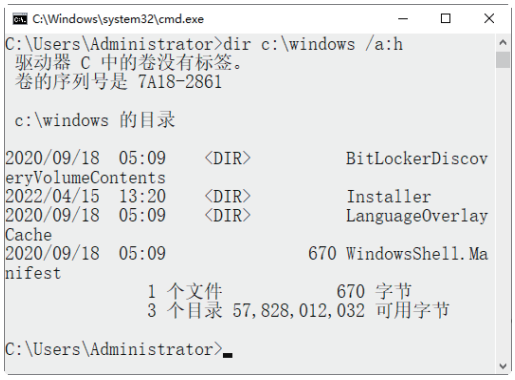

图 2-24　C 盘下的隐藏文件

2.4.3　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 2-25 所示。

图 2-25　ping 命令帮助信息

使用 ping 命令对计算机的连接状态进行测试的具体操作步骤如下：

Step01 使用 ping 命令来判断计算机的操作系统类型。在“命令提示符”窗口中输入“ping 192.168.3.9”命令，运行结果如图 2-26 所示。

Step02 在“命令提示符”窗口中输入“ping 192.168.3.9 -t -l 128”命令，可以不断向某台主机发出大量的数据包，如图 2-27 所示。

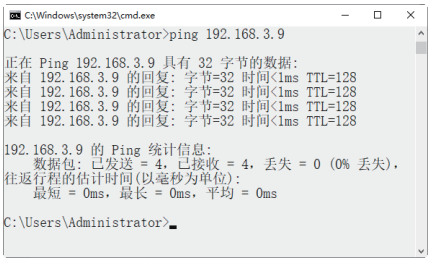

图 2-26　判断计算机的操作系统类型

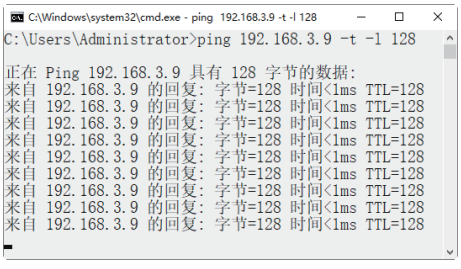

图 2-27　发出大量数据包

Step03 判断本台计算机是否与外界网络连通。在“命令提示符”窗口中输入“ping www.baidu.com”命令，其运行结果如图 2-28 所示，图中说明本台计算机与外界网络连通。

Step04 解析某 IP 地址的计算机名。在“命令提示符”窗口中输入“ping -a 192.168.3.9”命令，其运行结果如图 2-29 所示，可知这台主机的名称为 SD-20220314SOIE。

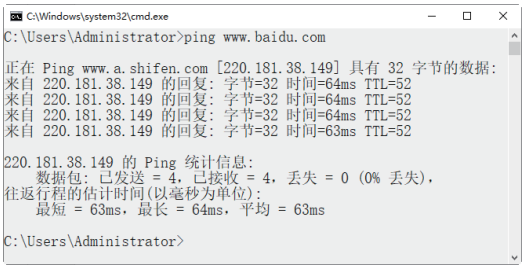

图 2-28　网络连通信息

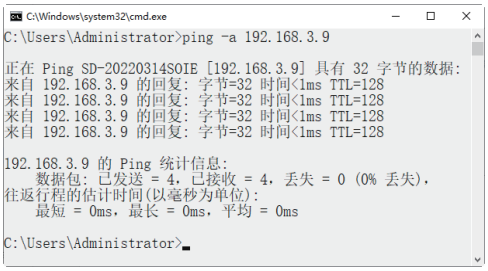

图 2-29　解析某 IP 地址的计算机名

2.4.4　查询网络状态与共享资源的 net 命令

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

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

查询本台计算机开启哪些 Windows 服务的具体操作步骤如下：

Step01 使用 net 命令查看网络状态。打开“命令提示符”窗口，输入“net start”命令，如图 2-30 所示。

Step02 按 Enter 键，则在打开的“命令提示符”窗口中可以显示计算机所启动的 Windows 服务，如图 2-31 所示。

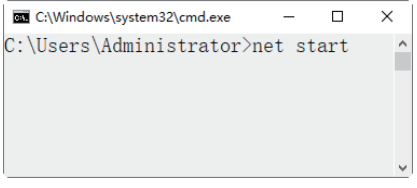

图 2-30　输入“net start”命令

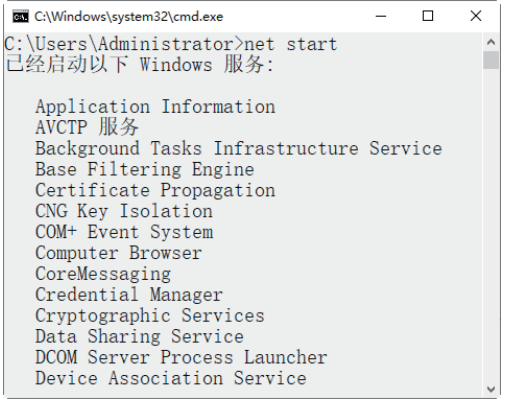

图 2-31　计算机所启动的 Windows 服务

2.4.5　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，可以让用户得知系统中目前都有哪些网络连接正常。

在“命令提示符”窗口中输入“netstat/?”命令，可以得到这条命令的帮助信息，如图 2-32 所示。

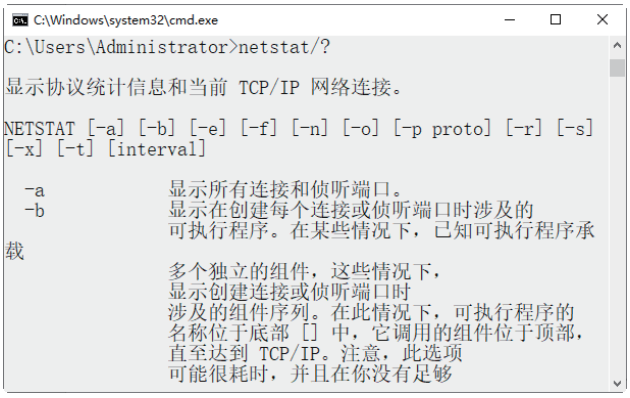

图 2-32　netstat 命令帮助信息

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：

Step01 打开“命令提示符”窗口，在其中输入“netstat -n”或“netstat”命令，按 Enter 键，查看服务器活动的 TCP/IP 连接，如图 2-33 所示。

Step02 在“命令提示符”窗口中输入“netstat -r”命令，按 Enter 键，查看本机的路由信息，如图 2-34 所示。

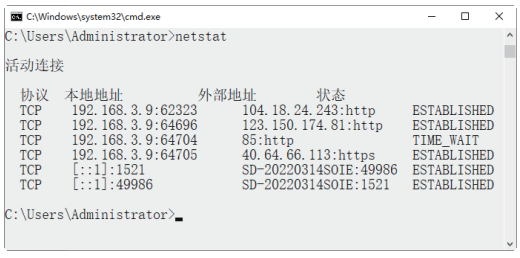

图 2-33　查看服务器活动的 TCP/IP 连接

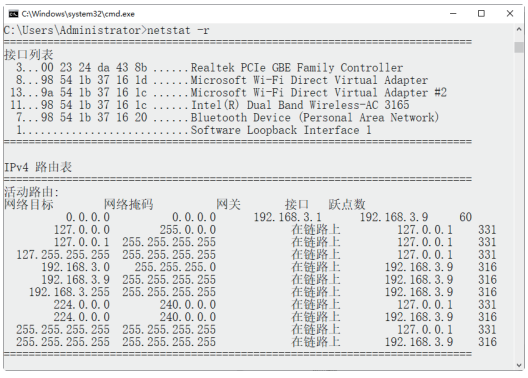

图 2-34　查看本机的路由信息

Step03 在“命令提示符”窗口中输入“netstat -a”命令，按 Enter 键，查看本机所有活动的 TCP 连接，如图 2-35 所示。

Step04 在“命令提示符”窗口中输入“netstat -n -a”命令，按 Enter 键，显示本机所有连接的端口及其状态，如图 2-36 所示。

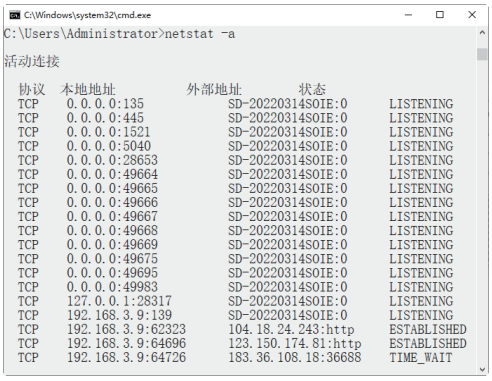

图 2-35　查看本机所有活动的 TCP 连接

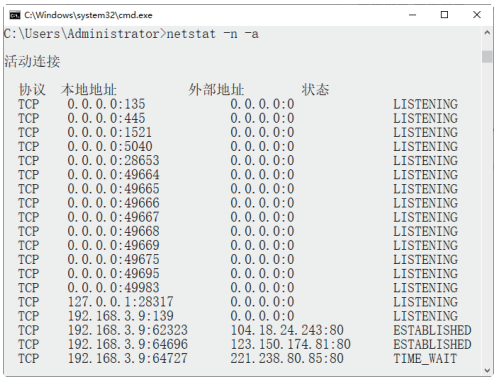

图 2-36　查看本机连接的端口及其状态

2.4.6　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 ms。
- 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，则可在“命令提示符”窗口中输入“tracert www.baidu.com”命令，按 Enter 键，其显示结果如图 2-37 所示。

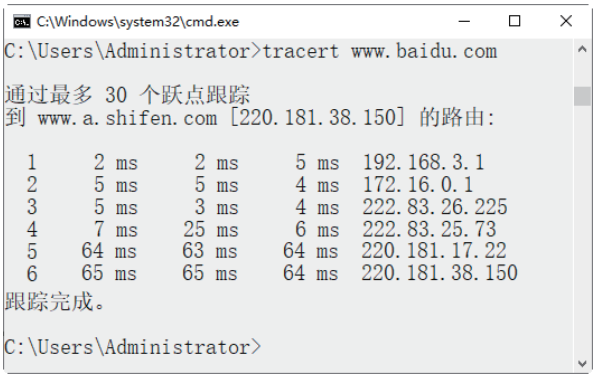

图 2-37　查看网络中路由节点信息

2.4.7　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 命令的语法格式如下：

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

其中各个参数的含义如下：

- /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，还查看每个进程提供的服务。下面将介绍使用 Tasklist 命令的具体操作方法。

（1）在“命令提示符”窗口中输入“Tasklist”命令，按 Enter 键即可显示本机的所有进程，如图 2-38 所示。在显示结果中可以看到映像名称、PID、会话名、会话 # 和内存使用等 5 部分。

图 2-38　查看本机进程

（2）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”窗口中输入“Tasklist /svc”命令即可，如图 2-39 所示。

图 2-39　查看本机进程提供的服务

（3）要查看本地系统中哪些进程调用了 shell32.dll 模块文件，只需在“命令提示符”窗口中输入“Tasklist /m shell32.dll”命令即可显示这些进程的列表，如图 2-40 所示。

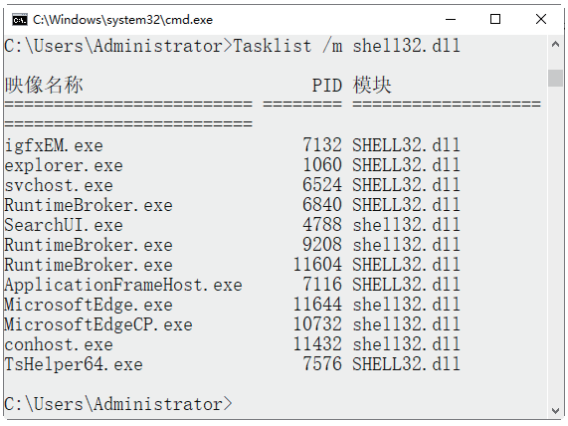

图 2-40　显示调用 shell32.dll 模块的进行

（4）使用筛选器可以查找指定的进程，在“命令提示符”窗口中输入“TASKLIST /FI "USERNAME ne NT AUTHORITY\SYSTEM" /FI "STATUS eq running”命令，按 Enter 键即可列出系统中正在运行的非 SYSTEM 状态的所有进程，如图 2-41 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”。

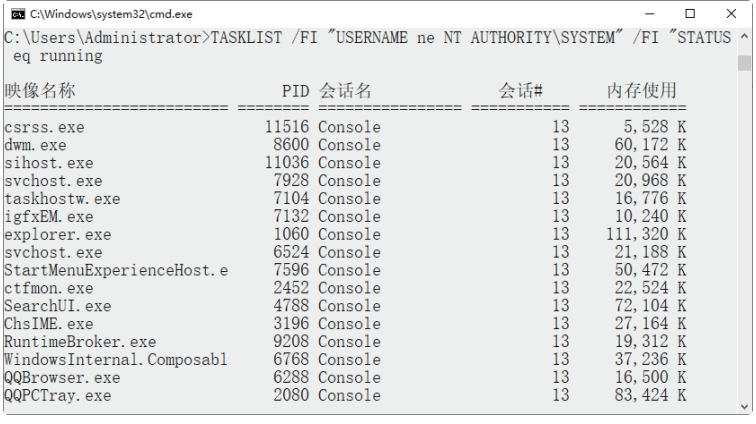

图 2-41　列出系统中正在运行的非 SYSTEM 状态的所有进程

2.5　实战演练

2.5.1　实战 1：自定义命令提示符窗口的显示效果

系统默认的“命令提示符”窗口显示的背景色为黑色，文字为白色，那么如何自定义显示效果呢？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选择“运行”选项，打开“运行”对话框，在其中输入“cmd”命令，单击“确定”按钮，打开“命令提示符”窗口，如图 2-42 所示。

Step 02 右击窗口的顶部，在弹出的快捷菜单中选择“属性”选项，如图 2-43 所示。

图 2-42　“命令提示符”窗口

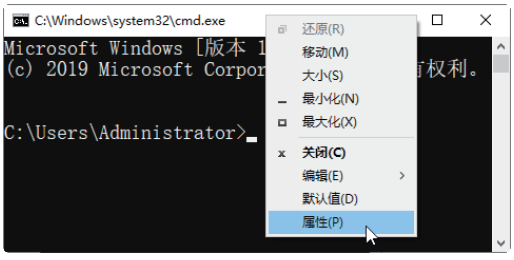

图 2-43　选择“属性”选项

Step 03 打开“属性”对话框，选择“颜色”选项卡，选中“屏幕背景”单选按钮，在颜色条中选中白色色块，如图 2-44 所示。

Step 04 选择“颜色”选项卡，选中“屏幕文字”单选按钮，在颜色条中选中黑色色块，如图 2-45 所示。

图 2-44　设置屏幕背景

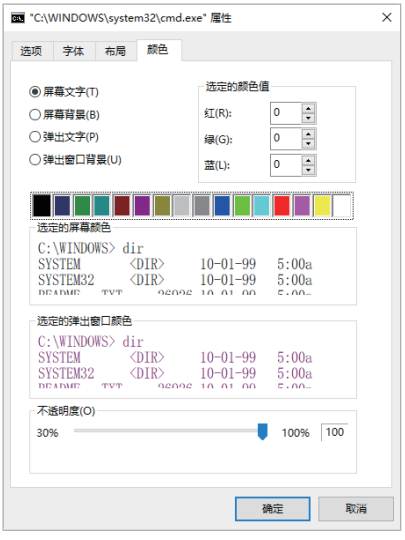

图 2-45　设置屏幕文字

Step 05 单击“确定”按钮，返回“命令提示符”窗口，可以看到命令提示符窗口的显示方式变为白底黑字样式，如图 2-46 所示。

图 2-46　以白底黑字样式显示“命令提示符”窗口

2.5.2　实战 2：使用 shutdown 命令实现定时关机

使用 shutdown 命令可以实现定时关机的功能，具体的操作步骤如下：

Step01 在“命令提示符”窗口中输入“shutdown/s /t 40”命令，如图 2-47 所示。

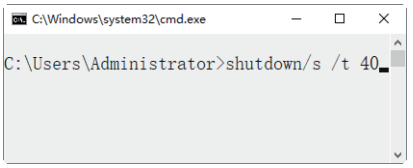

图 2-47　输入“shutdown/s /t 40”命令

Step02 弹出一个即将注销用户登录的信息提示框，这样计算机就会在规定的时间内关机，如图 2-48 所示。

Step03 如果此时想取消关机操作，可在命令行中输入“shutdown /a”命令后按 Enter 键，桌面右下角出现如图 2-49 所示的弹窗，表示取消成功。

图 2-48　信息提示框

图 2-49　取消关机操作

第 3 章 搭建无线测试系统

无线技术在给人们带来极大方便的同时，也带来了极大的信息安全风险。目前，无论是企事业单位还是家庭用户，信息安全意识依然薄弱。本章就来介绍无线测试系统环境的搭建，主要内容包括虚拟机的创建、Kali Linux 操作系统的创建等。

3.1 安装与创建虚拟机

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，同时还可以快速还原之前快照，避免因错误操作造成系统崩溃。

3.1.1 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://my.vmware.com/cn，进入虚拟机官网页面，如图 3-1 所示。

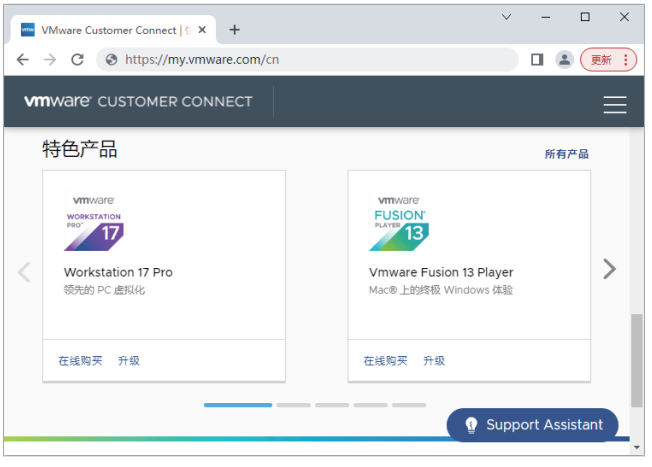

图 3-1 VMware 官网页面

Step 02 这里需要注册一个账号，注册完成后，进入所有下载页面，并切换到“所有产品”选项卡，如图 3-2 所示。

图 3-2 “所有产品”选项卡

Step 03 在下拉页面找到“VMware Workstation Pro”对应选项，单击右侧的“查看下载组件”超链接，如图 3-3 所示。

图 3-3 “查看下载组件”超链接

Step 04 进入到 VMware 下载界面，在其中选择 Windows 版本，单击“立即下载”超链接，如图 3-4 所示。

Step 05 打开“新建下载任务”对话框，单击“下载”按钮进行下载，如图 3-5 所示。

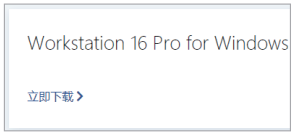

图 3-4 VMware 下载界面

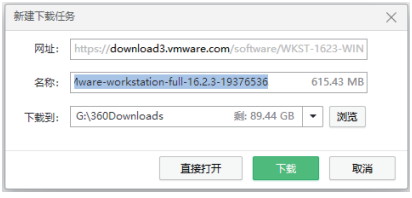

图 3-5 “新建下载任务”对话框

3.1.2 安装虚拟机软件

虚拟机软件下载完成后，接下来就可以安装虚拟机软件了，这里下载的是“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：

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”对话框，如图 3-6 所示。

Step 02 单击“下一步”按钮，进入“最终用户许可协议”对话框，勾选“我接受许可协议中的条款”复选框，如图 3-7 所示。

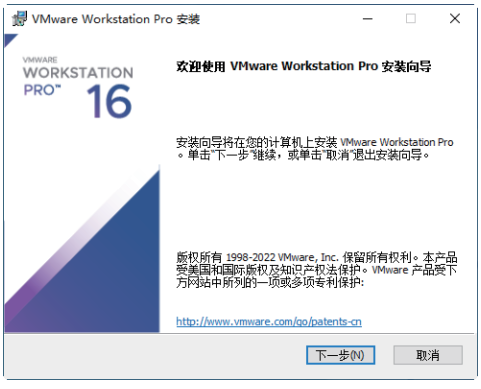

图 3-6 “安装向导”对话框

图 3-7 “最终用户许可协议”对话框

Step03 单击“下一步”按钮，进入“自定义安装”对话框，在其中可以更改安装路径，也可以保持默认，如图 3-8 所示。

Step04 单击“下一步”按钮，进入“用户体验设置”对话框，这里采用系统默认设置，如图 3-9 所示。

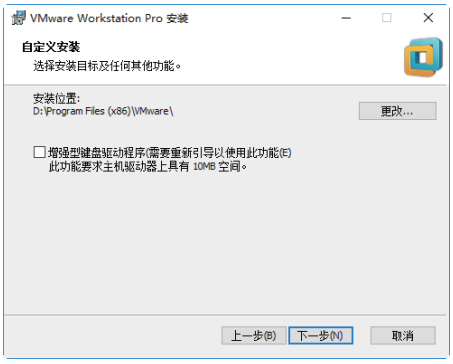

图 3-8　“自定义安装”对话框

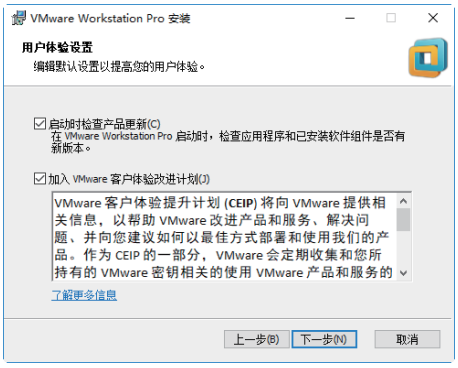

图 3-9　“用户体验设置”对话框

Step05 单击“下一步”按钮，进入“快捷方式”对话框，在其中可以创建用户快捷方式，这里可以保持默认设置，如图 3-10 所示。

Step06 单击“下一步”按钮，进入“已准备好安装 VMware Workstation Pro”对话框，开始准备安装虚拟机软件，如图 3-11 所示。

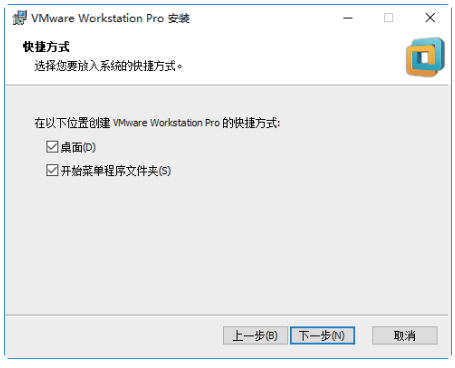

图 3-10　“快捷方式”对话框

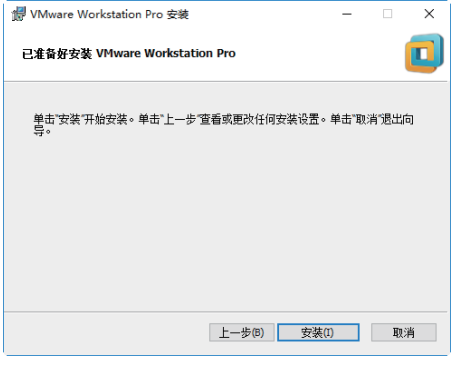

图 3-11　“已准备好安装 VMware Workstation Pro”对话框

Step07 单击“安装”按钮，等待一段时间后虚拟机便可以安装完成，并进入“VMware Workstation Pro 安装向导已完成”对话框，单击“完成”按钮，关闭虚拟机安装向导，如图 3-12 所示。

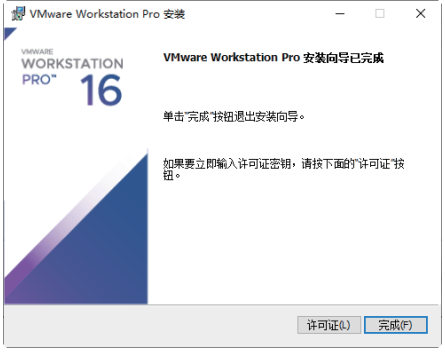

图 3-12　“VMware Workstation Pro 安装向导已完成”对话框

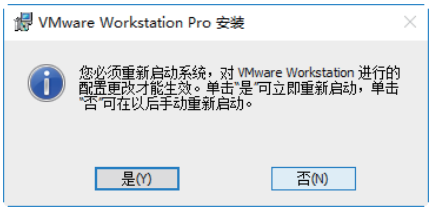

图 3-13　重新启动系统

Step 08 虚拟机安装完成后，需重新启动系统才可以使用。至此，便完成了 VMware 虚拟机的下载与安装，如图 3-13 所示。

3.1.3　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，为后续的系统测试做准备。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 3-14 所示。

Step 02 单击“创建新的虚拟机”按钮，进入“新建虚拟机向导”对话框，在其中选中“自定义”单选按钮，如图 3-15 所示。

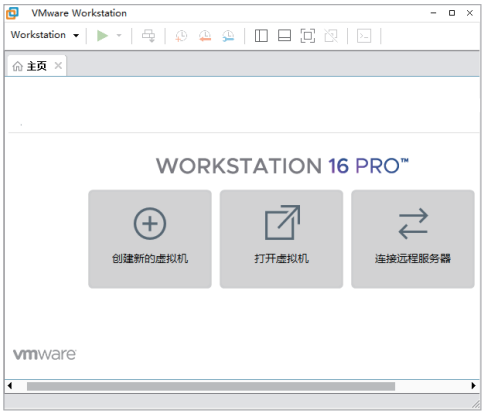

图 3-14　VMware 虚拟机工作界面

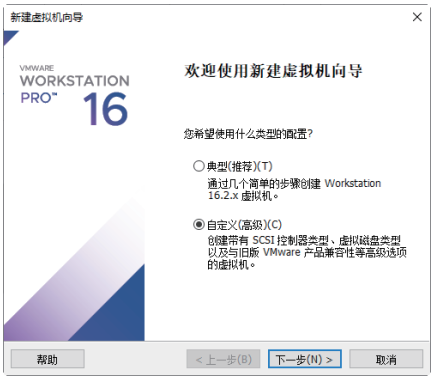

图 3-15　“新建虚拟机向导”对话框

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 3-16 所示。

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 3-17 所示。

图 3-16　“选择虚拟机硬件兼容性”对话框

图 3-17　“安装客户机操作系统”对话框

Step05 单击“下一步”按钮，进入“选择客户机操作系统”对话框，在其中选中“Linux”单选按钮，如图 3-18 所示。

Step06 单击“版本”下方的下拉按钮，在弹出的下拉列表中选择“其他 Linux 5.x 内核 64 位”或更高版本系统。这里的系统版本与主机系统版本无关，可以自由选择，如图 3-19 所示。

图 3-18　“选择客户机操作系统”对话框

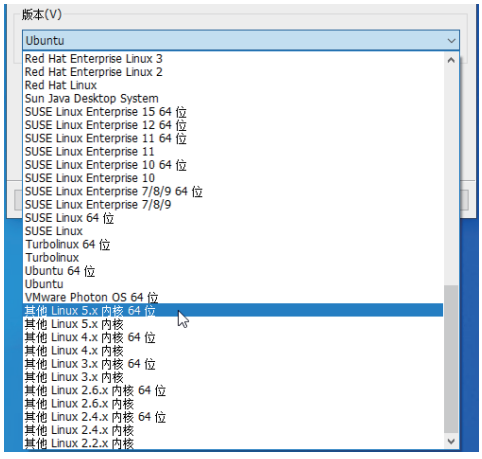

图 3-19　选择系统版本

Step07 单击“下一步”按钮，进入“命名虚拟机”对话框，在“虚拟机名称”文本框中输入虚拟机名称，在“位置”中选择一个存放虚拟机的磁盘位置，如图 3-20 所示。

Step08 单击“下一步”按钮，进入“处理器配置”对话框，在其中选择处理器数量，一般普通计算机都是单处理，所以这里不用设置，处理器内核数量可以根据实际处理器内核数量设置，如图 3-21 所示。

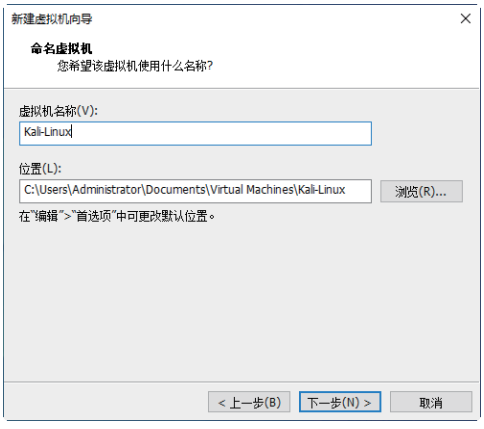

图 3-20　“命名虚拟机”对话框

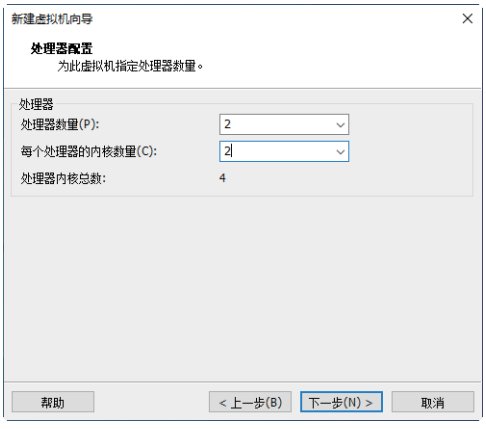

图 3-21　“处理器配置”对话框

Step09 单击“下一步”按钮，进入“此虚拟机的内存”对话框，根据实际主机进行设置，最少内存不要低于 768MB，这里选择 2048MB，也就是 2GB 内存，如图 3-22 所示。

Step10 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”单选按钮，如图 3-23 所示。

图 3-22 “此虚拟机的内存”对话框

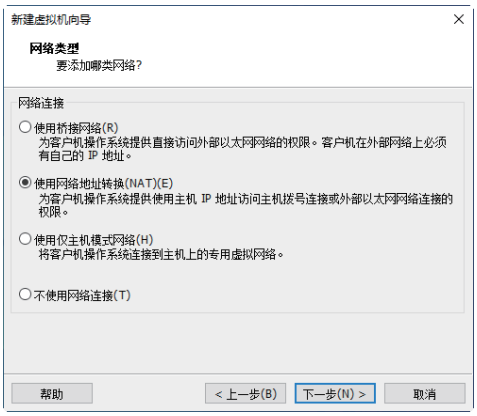

图 3-23 “网络类型”对话框

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 3-24 所示。

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 3-25 所示。

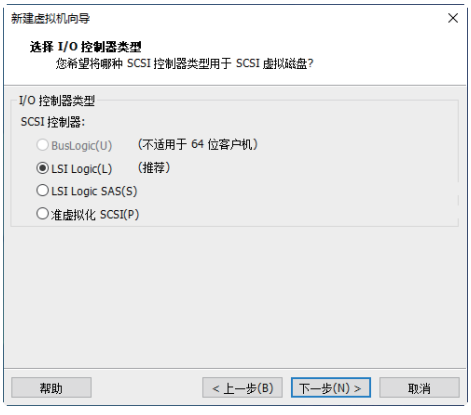

图 3-24 “选择 I/O 控制器类型”对话框

图 3-25 “选择磁盘类型”对话框

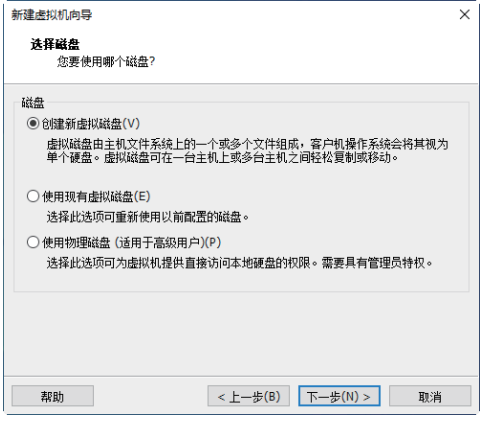

图 3-26 “选择磁盘”对话框

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 3-26 所示。

Step 14 单击“下一步”按钮，进入“指定磁盘容量”对话框，这里最大磁盘大小设置为 8GB 即可，选中“将虚拟盘拆分成多个文件”单选按钮，如图 3-27 所示。

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 3-28 所示。

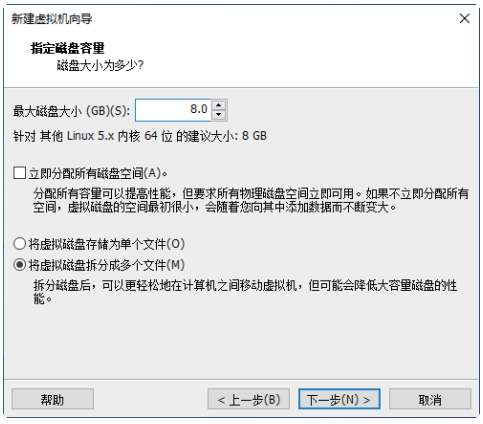

图 3-27　“指定磁盘容量”对话框

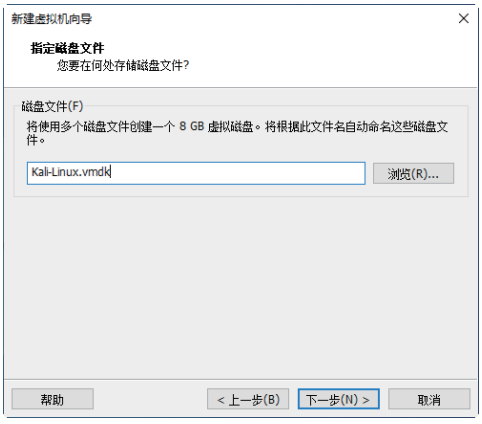

图 3-28　“指定磁盘文件”对话框

Step16 单击“下一步”按钮，进入“已准备好创建虚拟机”对话框，如图 3-29 所示。

Step17 单击“完成”按钮，至此，便创建了一个新的虚拟机，如图 3-30 所示。

图 3-29　“已准备好创建虚拟机”对话框

图 3-30　创建新虚拟机

3.2　安装 Kali Linux 操作系统

现实中组装好电脑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 Linux 操作系统。

3.2.1　下载 Kali Linux 系统

Kali Linux 是基于 Debian 的 Linux 发行版，设计用于数字取证和渗透测试操作系统。下载 Kali Linux 系统的具体操作步骤如下：

Step01 在浏览器中输入 Kali Linux 系统的网址 https://www.kali.org，打开 Kali 官方网站，如图 3-31 所示。

Step02 单击“DOWNLOAD”选项，在弹出的菜单列表中选择 Kail Linux 版本，如图 3-32 所示。

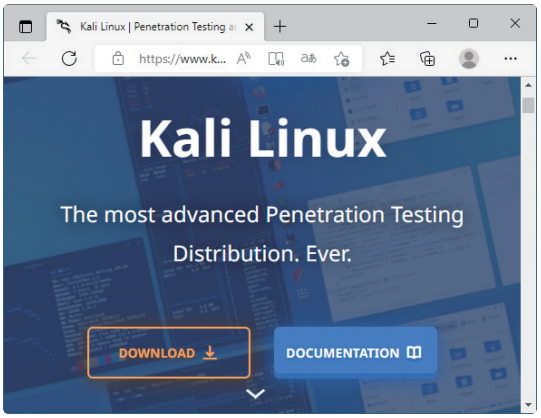

图 3-31　Kali 官方网站

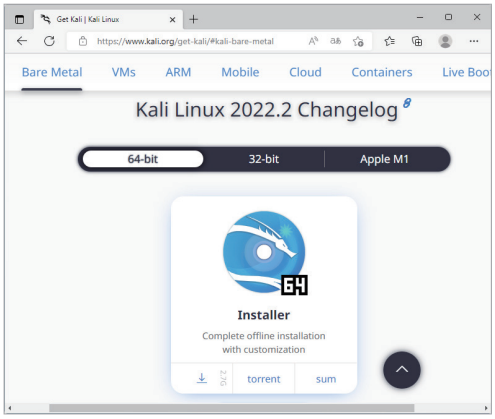

图 3-32　选择 Kail Linux 版本

Step03 单击“↓”按钮，开始下载 Kail Linux，并显示下载进度，如图 3-33 所示。

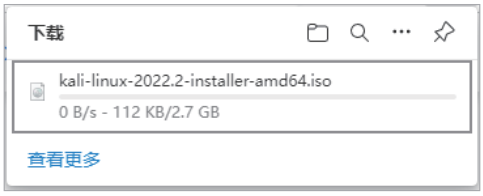

图 3-33　下载进度

3.2.2　安装 Kali Linux 系统

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

Step01 打开安装好的虚拟机，单击“CD/DVD”超链接，如图 3-34 所示。

Step02 在打开的“虚拟机设置”对话框中选中“使用 ISO 映像文件”单选按钮，如图 3-35 所示。

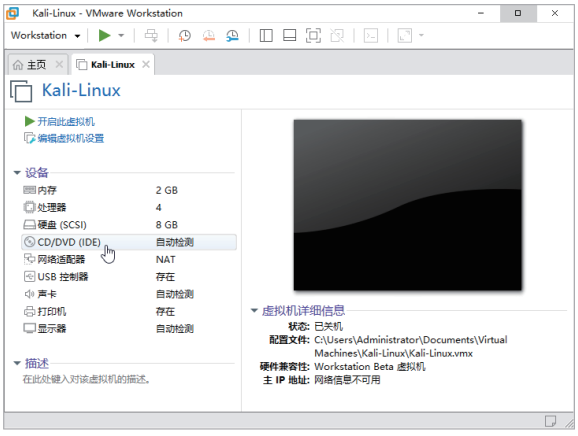

图 3-34　单击“CD/DVD”超链接

图 3-35　“虚拟机设置”对话框

Step03 单击“浏览”按钮，打开“浏览 ISO 影像”对话框，在其中选择下载好的系统映像文件，如图 3-36 所示。

Step04 单击“打开”按钮，返回虚拟机设置界面，这里单击“开启此虚拟机”超链接，如图 3-37 所示。

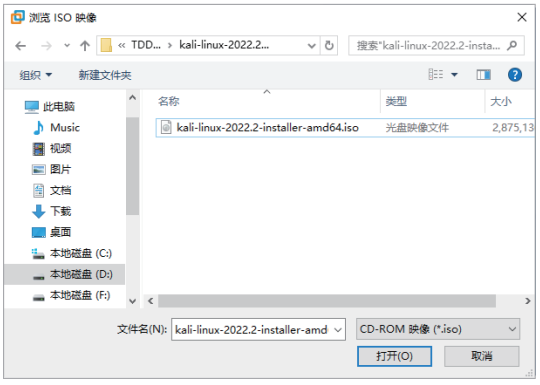

图 3-36　“浏览 ISO 影像”对话框

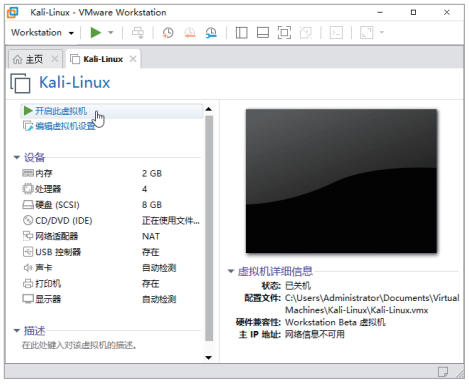

图 3-37　虚拟机设置界面

Step05 启动虚拟机后会进入启动选项界面，用户可以通过键盘上下键选择“Graphical Install”选项，如图 3-38 所示。

Step06 选择完毕后，按 Enter 键，进入语言选择界面，这里选择“简体中文”选项，如图 3-39 所示。

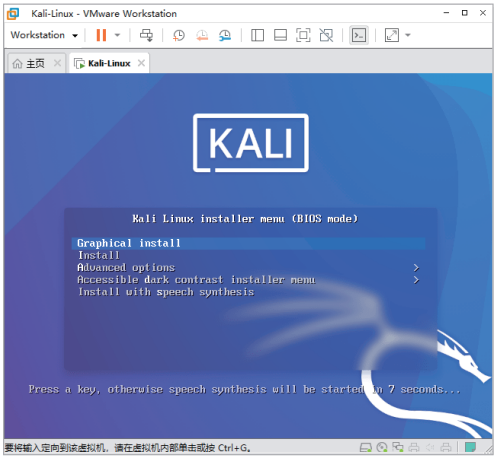

图 3-38　选择“Graphical Install”选项

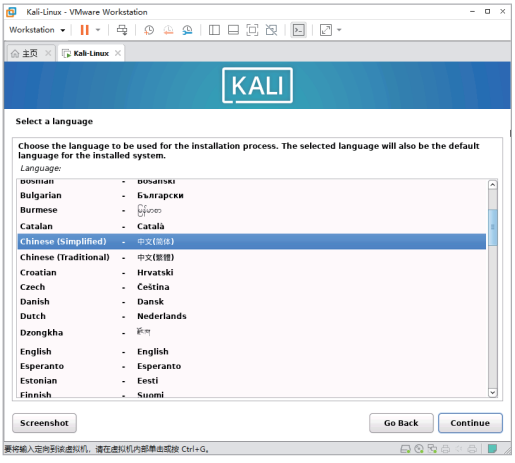

图 3-39　语言选择界面

Step07 单击 Continue 按钮，进入选择语言确认界面，保持系统默认设置，如图 3-40 所示。

Step08 单击“继续”按钮，进入“请选择您的区域”界面。这时它会自动联网匹配，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 3-41 所示。

Step09 单击“继续”按钮，进入“配置键盘”界面，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 3-42 所示。

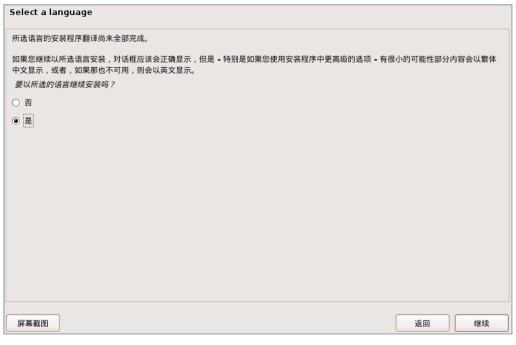

图 3-40　语言确认页面

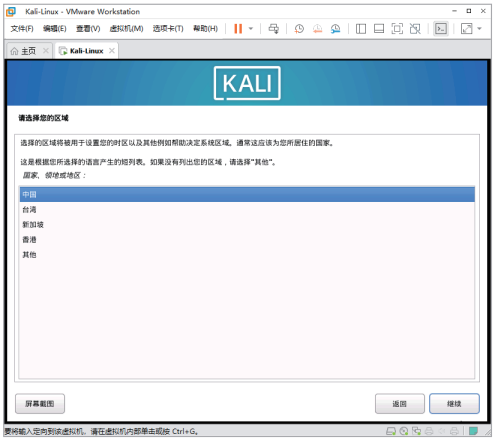

图 3-41 “请选择您的区域”界面

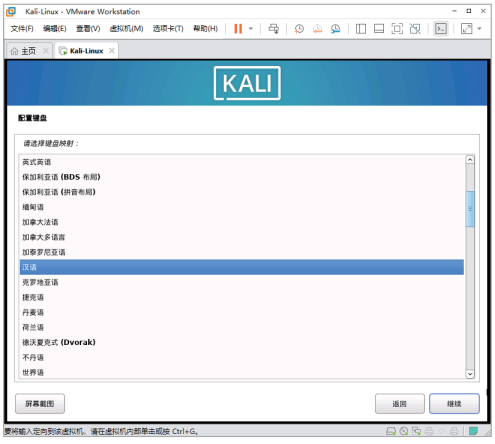

图 3-42 “配置键盘”界面

Step 10 单击“继续”按钮，按照安装步骤提示就可以完成 Kali Linux 系统的安装了，如图 3-43 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 3-44 所示。

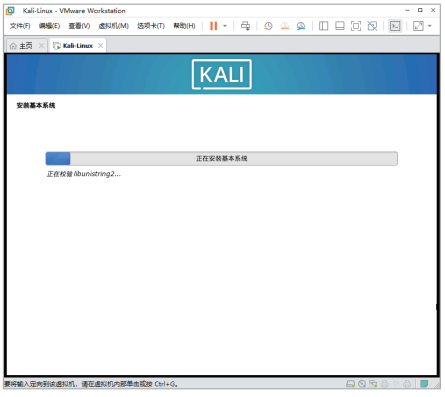

图 3-43 安装基本系统界面

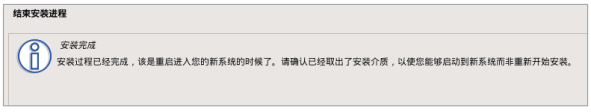

图 3-44 安装完成

Step 12 按 Enter 键，安装完成后重启，进入“用户名”界面，在其中输入 root 管理员账号，如图 3-45 所示。

Step 13 单击“下一步”按钮，进入登录密码界面，在其中输入设置好的管理员密码，如图 3-46 所示。

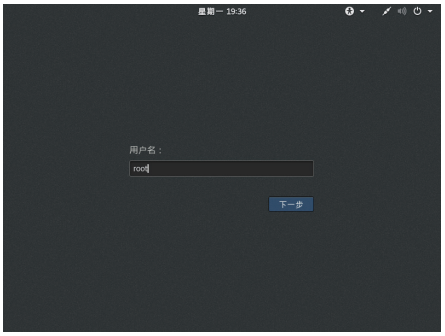

图 3-45 “用户名”界面

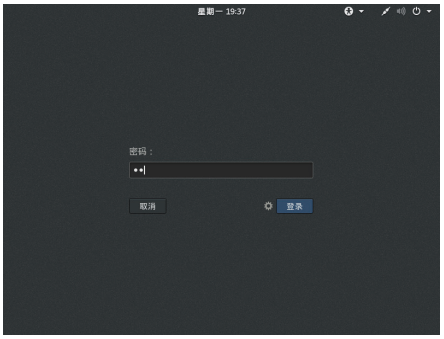

图 3-46 输入密码

Step14 单击“登录”按钮，至此便完成了整个 Kail Linux 系统的安装工作，如图 3-47 所示。

图 3-47　Kail Linux 系统界面

3.2.3　更新 Kali Linux 系统

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

Step01 双击桌面上 Kali Linux 系统的终端黑色图标，如图 3-48 所示。

Step02 打开 Kali Linux 系统的终端设置界面，在其中输入“apt update”命令，然后按 Enter 键，获取需要更新软件的列表，如图 3-49 所示。

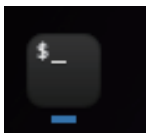

图 3-48　Kali Linux 系统图标

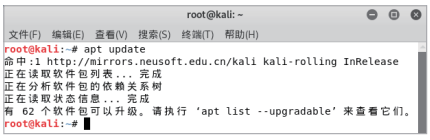

图 3-49　需要更新软件的列表

Step03 获取完更新列表后如果有需要更新的软件，可以运行“apt upgrad”命令，如图 3-50 所示。

Step04 运行命令后会有一个提示，此时按 Y 键即可开始更新，更新中的状态如图 3-51 所示。

图 3-50　运行“apt upgrad”命令

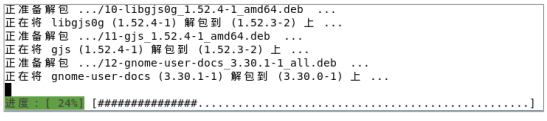

图 3-51　开始更新

注意：由于网络原因可能需要多执行几次更新命令，直至更新完成。另外，如果个别软件已经安装会出现升级版本问题，如图 3-52 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
下列软件包的版本将保持不变：
  wpscan
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 1 个软件包未被升级。
```

图 3-52　升级版本问题

这时，可以先卸载旧版本，运行“apt-get remove < 软件名 >”命令，如图 3-53 所示，此时按 Y 键即可卸载。

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

图 3-53　卸载旧版本

卸载完旧版本后，再运行“apt-get install < 软件名 >”命令，如图 3-54 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 3-54　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，表明此时系统更新已完成，如图 3-55 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 3-55　系统更新完成

3.3　安装 CDlinux 系统

CDlinux 是一种小型的迷你 GNU/Linux 发行版软件，其名称取自英文的 Compact Distro Linux。CDlinux 的体形小巧，功能却很强大。

3.3.1　CDlinux 简介

使用者可以把 CDlinux 看作是一个“移动操作系统”，把它装到随身 U 盘中，无论走到哪里，只要是能支持 U 盘启动的电脑，就可以插上 U 盘来启动 CDlinux 操作系统，从而把这台电脑变成自己的移动工作站。

CDlinux 里集成了最新的 Linux 内核、Xorg 图形界面、Xfce 窗口管理器以及很多其他流行软件，如 Firefox 浏览器、Pidgin 即时通信程序、GIMP 图像处理程序等，这就使得移动工作更加方便。

另外，还可以把 CDlinux 当作一件随身的系统修复 / 维护工具。这是因为在 CDlinux 标准版里集成了大量的系统修复 / 维护工具，如 parted、partimage、partclone、testdisk、foremost 等，使用这些工具完全可以满足日常系统维护 / 修复工作的需要。

目前，CDlinux 对简体中文提供全面支持，这极大地方便了使用中文的用户。

3.3.2　配置 CDlinux

创建 CDlinux 虚拟机的操作步骤如下：

Step01 打开 VMware 虚拟机，其工作界面如图 3-56 所示。

Step02 单击“创建新的虚拟机”按钮，进入“新建虚拟机向导”对话框，保持默认“典型（推荐）”，如图 3-57 所示。

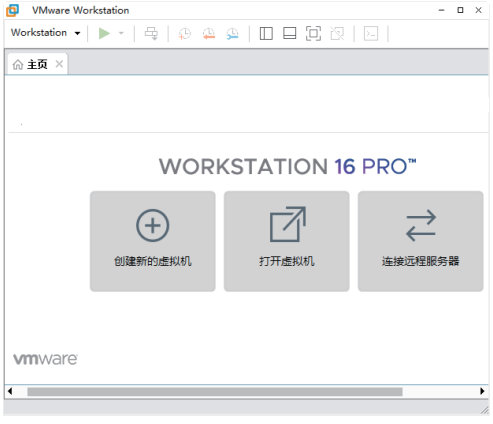

图 3-56　WMware 虚拟机工作界面

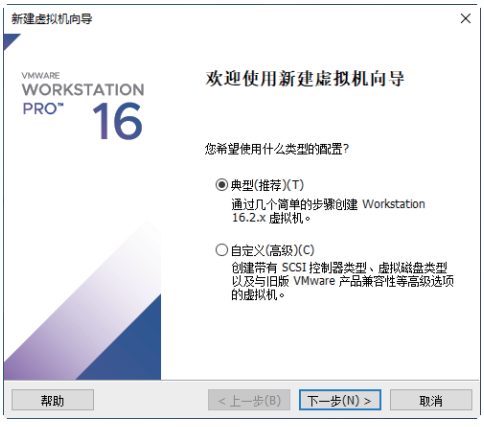

图 3-57　“新建虚拟机向导”对话框

Step03 单击“下一步”按钮，在“安装客户机操作系统”对话框中选中“安装程序光盘映像文件（iso）”单选按钮，并为其添加 CDlinux 光盘文件，如图 3-58 所示。

Step04 单击“下一步”按钮，在“选择客户机操作系统”对话框中选择“Linux”选项，版本中选择“其他 Linux 5.x 内核 64 位”，如图 3-59 所示。

Step05 单击“下一步”按钮，在“命名虚拟机”对话框中单击“浏览”按钮，为虚拟机选择一个保存位置，如图 3-60 所示。

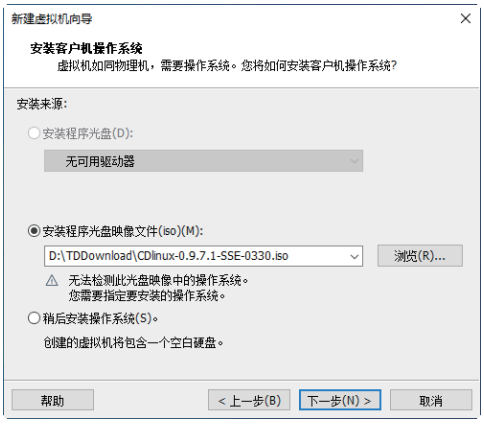

图 3-58　添加 CDlinux 光盘文件

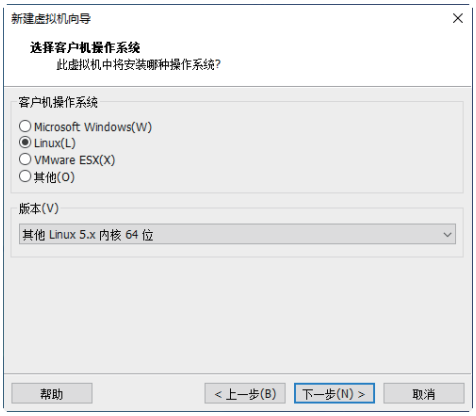

图 3-59　选择“Linux”选项

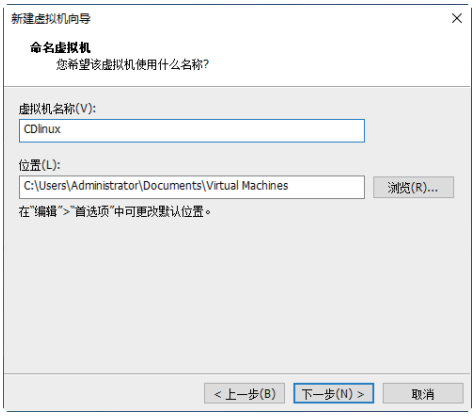

图 3-60　“命名虚拟机”对话框

Step06 单击“下一步”按钮，在“指定磁盘容量”对话框保持默认即可，如图 3-61 所示。

Step07 单击“下一步”按钮，至此便配置好了 CDlinux 系统，单击“完成”按钮完成虚拟机创建，如图 3-62 所示。

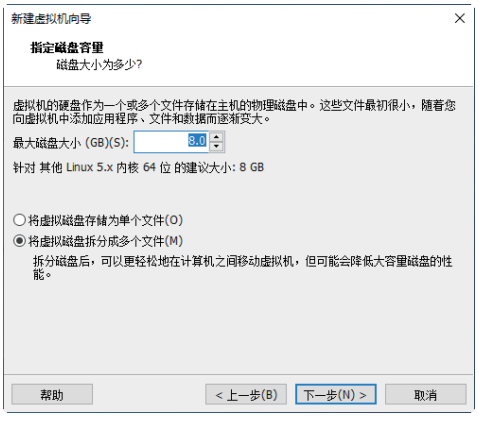

图 3-61　“指定磁盘容量”对话框

图 3-62　配置好 CDlinux 系统

Step08 在配置好的虚拟机启动界面，单击“开启此虚拟机”超链接启动虚拟机，如图 3-63 所示。

Step09 在虚拟机启动过程中可以选择语言环境，如图 3-64 所示。

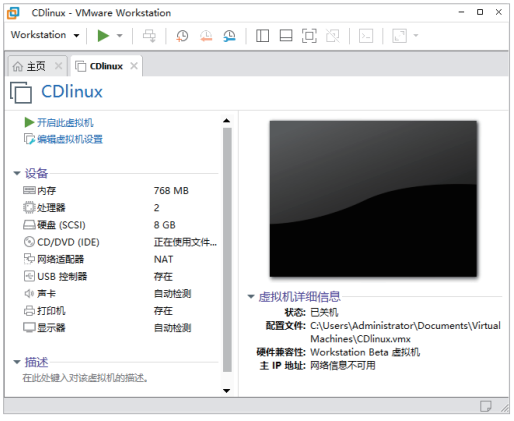

图 3-63　启动虚拟机

图 3-64　选择语言环境

Step10 启动 CDlinux 系统，启动完成后的桌面如图 3-65 所示。

图 3-65　CDlinux 系统工作界面

3.4　靶机的安装与使用

拿到局域网权限后需要后续的渗透测试，这里选取一款比较好的靶机——Metasploitable。该靶机中包含了大量的系统漏洞，用户使用该靶机可以做日常的无线网络安全练习，进而提高自身的安全技术。

3.4.1　认识靶机

Metasploitable 漏洞演练系统，是基于 Ubuntu 操作系统设计，本身设计作为安全工具测试和演示常见漏洞攻击的环境。它的作用是用来作为 MSF 攻击用的靶机，是一个具有无数未打补丁漏洞与开放了无数高危端口的渗透演练系统，可以用来进行练习。

在网络中攻击现实中的主机是一种违法行为，一旦被对方发现可能会遭受被起诉的风险。因此使用 Metasploitable 系统来练习，不但可以更加直观地感受漏洞利用的过程，还可以学会如何修补防御这些漏洞。

3.4.2　安装靶机

目前 Metasploitable 已经推出 3 个系列，这里选用 Metasploitable2。下载并安装 Metasploitable2 的操作步骤如下：

Step01 在浏览器中输入 http://sourceforge.net/projects/metasploitable/files/Metasploitable2/，在打开的页面中找到下载界面，如图 3-66 所示。

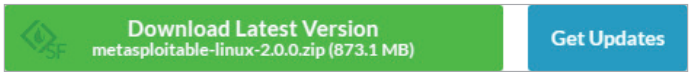

图 3-66　下载界面

Step02 单击下载界面中的下载按钮，并选择软件的保存路径，下载完成后会有一个“metasploitable-linux-2.0.0.zip”的压缩包文件，打开压缩包如图 3-67 所示。

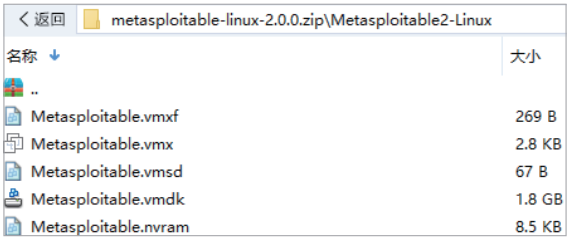

图 3-67　压缩包文件

Step03 将该压缩包文件解压到磁盘当中，双击打开该目录，查看解压后的文件是否缺少，如图 3-68 所示。

图 3-68　解压压缩包文件

注意：这里存放的路径是创建虚拟机后的路径，因此选择一块空间充足并且便于记忆的位置。

Step04 打开 VMware 虚拟机，进入虚拟机的工作界面，如图 3-69 所示。

Step05 单击“打开虚拟机”按钮，打开“打开”对话框，在其中找到解压目录，如图 3-70 所示。

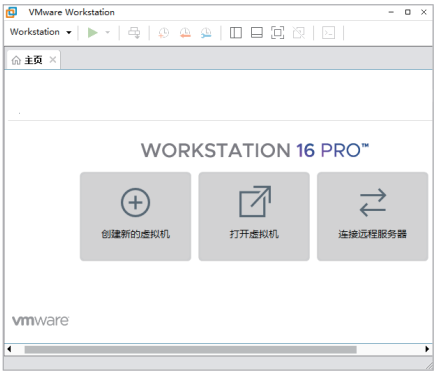

图 3-69　虚拟机的主页面

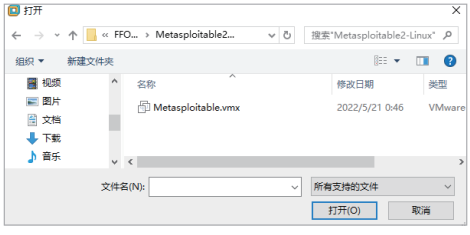

图 3-70　“打开”对话框

图 3-71　创建虚拟机

Step06 选中目录中的虚拟机文件，单击“打开”按钮，这样便创建好了虚拟机，如图 3-71 所示。

Step07 单击“开启此虚拟机”超链接，会弹出一个提示框，如图 3-72 所示。

Step08 单击“我已复制该虚拟机”按钮，启动 Metasploitable2，这样就完成了靶机的安装，如图 3-73 所示。

注意：虚拟机镜像创建的虚拟机默认账号密码均为 mfsadmin，可以通过 passwd 命令修改密码。

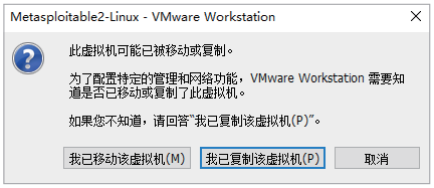

图 3-72　信息提示框

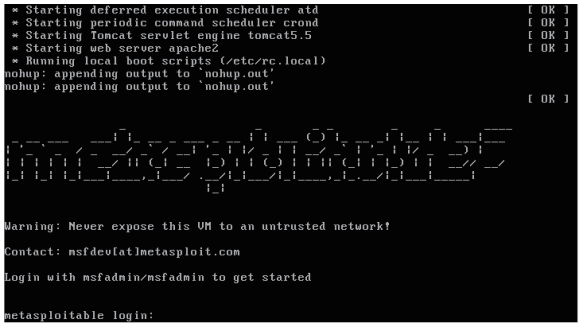

图 3-73　启动 Metasploitable2

Step09 登录进入虚拟机以后建议更改该初始密码，修改密码使用“passwd msfadmin”命令，输入完命令后会要求输入原始密码，原始密码正确后会要求输入新密码，输入两次一样的密码后修改密码完成，如图 3-74 所示。

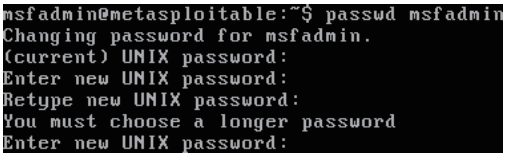

图 3-74　修改密码

注意：Linux 系统中输入密码是不显示的，直接输入即可，不要以为没有输入。另外，如果输入密码过短系统也会提示要求输入一个较长的密码。

3.4.3　靶机的使用

靶机安装完成后，就可以使用该靶机了。使用方法非常简单，启动虚拟机后，靶机系统也会启动。用户就可以使用各种扫描工具来扫描靶机中的系统漏洞，进入演示使用漏洞攻击系统的过程。

3.5　实战演练

3.5.1　实战 1：设置 Kail 虚拟机与主机共享文件夹

通过安装虚拟机工具设置 Kali 虚拟机与主机实现共享文件，具体的操作步骤如下：

Step01 在 VMware 工具栏中选择“虚拟机”菜单项，在弹出的菜单列表中选择“设置”菜单命令，如图 3-75 所示。

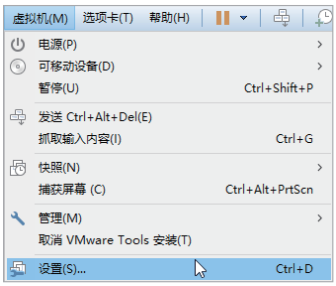

图 3-75　“设置”菜单命令

Step02 打开“虚拟机设置”对话框，选择“选项”选项卡，并在“设置”列表中选择“共享文件夹”选项，如图 3-76 所示。

Step03 单击“添加”按钮，打开“添加共享文件夹向导”对话框，如图 3-77 所示。

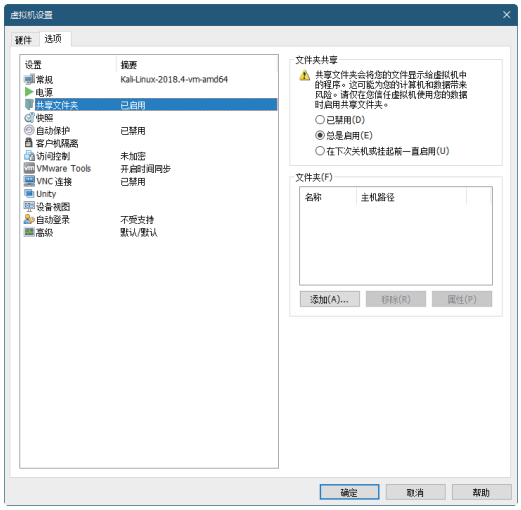

图 3-76 “虚拟机设置”对话框

图 3-77 “添加共享文件夹向导”对话框

Step04 单击“下一步”按钮，在打开的“命令共享文件夹”对话框中输入文件夹名称，并选择一个共享文件夹路径，如图 3-78 所示。

Step05 单击“下一步”按钮，进入“指定共享文件夹属性”对话框，指定共享文件夹属性，也可以保持默认设置，最后单击“完成”按钮，完成共享文件夹的设置操作，如图 3-79 所示。

图 3-78 “命令共享文件夹”对话框

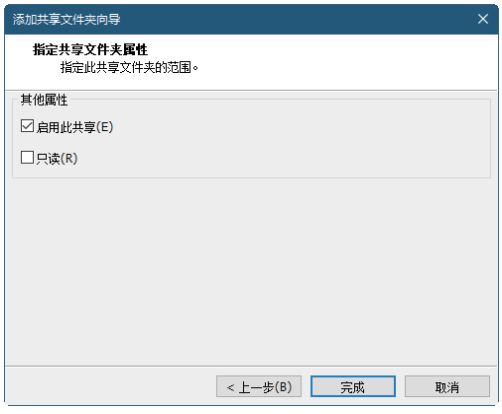

图 3-79 “指定共享文件夹属性”对话框

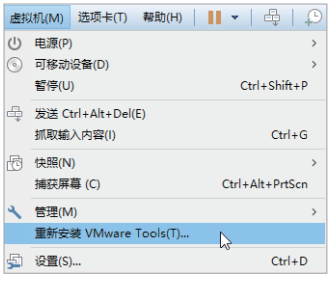

图 3-80 “虚拟机”菜单命令

Step06 在 VMware 菜单中选择“虚拟机”菜单项，在弹出的菜单列表中选择“重新安装 VMware Tools”菜单命令，如图 3-80 所示。

Step07 此时会在 Kali 虚拟机中弹出一个安装光盘，打开光盘后，里面会有 5 个文件，如图 3-81 所示。

Step08 复制压缩包文件“VMwareTools-10.2.5-8068393.tar.gz”到 Downloads 目录下，如图 3-82 所示。

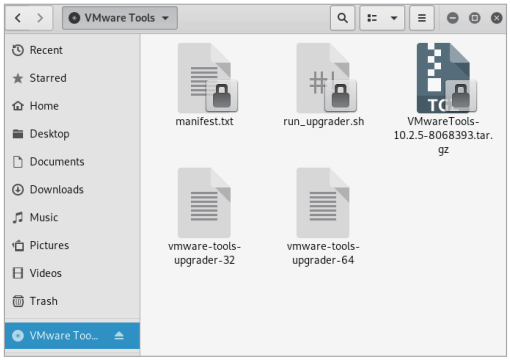

图 3-81　光盘文件

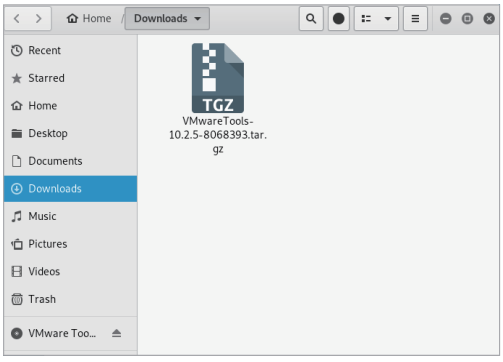

图 3-82　复制压缩包文件

Step09 选中压缩包文件，右击，在弹出的快捷菜单中选择“提取到此处”选项，如图 3-83 所示。

Step10 开始解压文件夹，解压完成后，在内部发现一个“vmware-install.pl”文件，如图 3-84 所示。

图 3-83　选择“提取到此处”选项

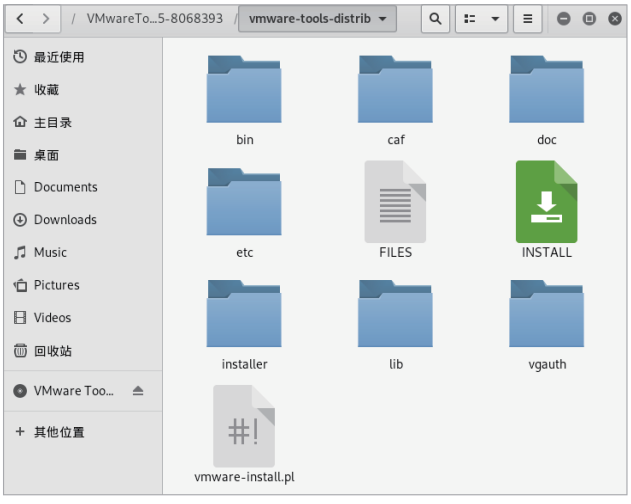

图 3-84　解压文件夹

Step11 鼠标移动到文件夹空白区域，右击，在弹出的快捷菜单中选择“在终端打开”选项，如图 3-85 所示。

Step12 这时在终端中执行“./ vmware-install.pl”命令，执行结果如图 3-86 所示。

图 3-85　选择“在终端打开”选项

```
root@kali:~/Downloads/VMwareTools-10.2.5-8068393/vmware-tools-distrib# ./vmware-install.pl
The installer has detected an existing installation of open-vm-tools packages
on this system and will not attempt to remove and replace these user-space
applications. It is recommended to use the open-vm-tools packages provided by
the operating system. If you do not want to use the existing installation of
open-vm-tools packages and use VMware Tools, you must uninstall the
open-vm-tools packages and re-run this installer.
The packages that need to be removed are:
open-vm-tools
Packages must be removed with the --purge option.
The installer will next check if there are any missing kernel drivers. Type yes
if you want to do this, otherwise type no [yes] y
```

图 3-86　执行命令结果

Step13 如果安装过程中提示 [yes]，按 Y 键或 Enter 键直到安装完成，安装完成后，在 mnt 目录中会多出一个共享文件夹“hgfs”，如图 3-87 所示。

```
root@kali:/# cd mnt
root@kali:/mnt# ls
hgfs
root@kali:/mnt# cd hgfs
root@kali:/mnt/hgfs# ls
ShareDir
root@kali:/mnt/hgfs# cd ShareDir/
root@kali:/mnt/hgfs/ShareDir#
```

图 3-87　共享文件夹“hgfs”

3.5.2　实战 2：设置 Kali 虚拟机的上网方式

Kali 虚拟机可以设置三种网络模式，设置上网方式的操作步骤如下：

Step 01 在 VMware 菜单项中选择“虚拟机”→“可移动设备”→“网络适配器”→“设置”菜单命令，如图 3-88 所示。

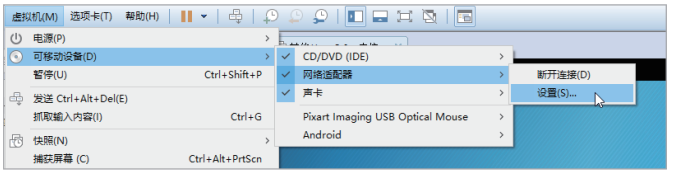

图 3-88　“设置”菜单命令

Step 02 打开“虚拟机设置”对话框，在其中选择“网络适配器”选项，在右侧可以看到“网络连接”设置界面，这里提供的连接方式有 3 种，如图 3-89 所示。

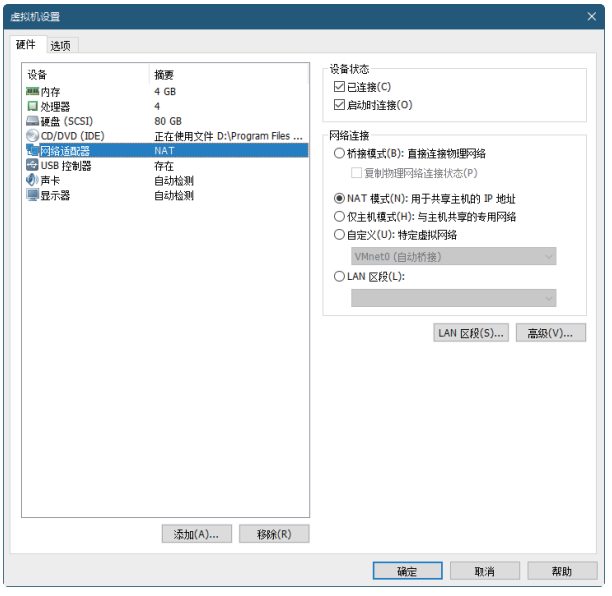

图 3-89　“虚拟机设置”对话框

3 种网络连接方式介绍如下：

（1）桥接模式：如果选择该连接模式，虚拟机可以获取独立的 IP 地址，通过独立 IP 地址可以进行上网。

（2）NAT 模式：如果选择该连接模式，虚拟机将与主机共用一个 IP 地址，通过主机 IP 地址实现 NAT 转换上网。

（3）仅主机模式：如果选择该连接模式，虚拟机仅同主机进行通信，不能接入互联网。