第 1 章 Web 安全快速入门

随着信息时代的发展和网络的普及，越来越多的人走进了网络生活，然而人们在享受网络带来便利的同时，也时刻面临着黑客们残酷攻击的危险。本章介绍 Web 安全的相关技术信息，主要内容包括什么是 Web 安全、Web 应用程序的安全与风险、网络中的相关概念、网络通信的相关协议、IP 地址、MAC 地址、端口、系统进程等。

1.1 什么是 Web 安全

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

1.1.1 Web 安全概述

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

最初，Web 安全主要是指计算机安全。不过，随着万维网上 Java 语言的普及，利用 Java 语言进行传播和获取资料的病毒开始出现，最为典型的代表就是 Java Snake 病毒，还有一些利用邮件服务器进行传播和破坏的病毒，这些病毒会严重影响互联网的效率。

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

1.1.2 Web 安全的发展历程

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

1. 宣传启蒙阶段

第一代互联网 Web 1.0。从 1995 年至 2005 年，大约十年的时间，Web 1.0 是只读互联网，用户只

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

图 1-1　百度首页

在此阶段，Web 安全主要是指计算机的实体安全。而且这一阶段国家也没有相关的法律法规，更没有较为完整意义的专门针对计算机系统安全方面的规章，安全标准也比较少，只是在物理安全及保密通信等个别环节上有些规定；广大应用部门也基本上没有意识到计算机安全的重要性，只在个别部门中少数有些计算机安全意识的人们开始在实际工作中进行摸索。

2. 开始发展阶段

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

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

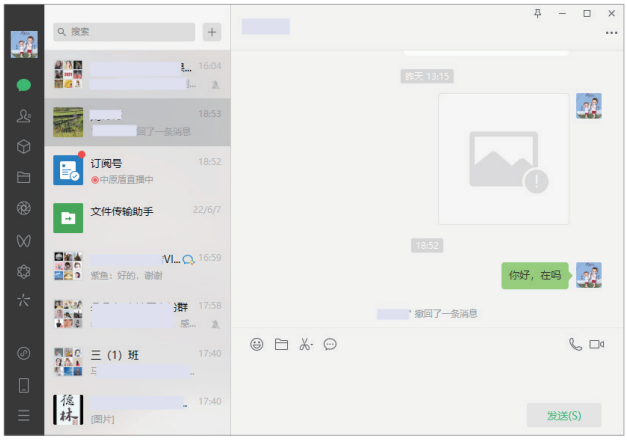


图 1-2　微信好友聊天界面

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

3. 逐步正规阶段

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

图 1-3　物联网示意图

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

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

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

1.1.3　Web 安全的发展现状

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

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

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

1.2 网络中的相关概念

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

1.2.1 互联网与因特网

互联网是指将两台计算机或者是两台以上的计算机终端、客户端、服务端通过计算机信息技术的手段互相联系起来的结果。互联网在现实生活中应用很广泛，在互联网上人们可以聊天、玩游戏、查阅资料等。互联网是全球性的，这就意味着这个网络不管是谁发明了它，是属于全人类的。图 1-4 所示为互联网的结构示意图。

图 1-4 互联网结构示意图

因特网是一个把分布于世界各地的计算机用传输介质互相连接起来的网络。因特网是基于 TCP/IP 协议实现的，TCP/IP 协议由很多协议组成，不同类型的协议又被放在不同的层，其中，位于应用层的协议就有很多，比如 FTP、SMTP、HTTP。图 1-5 所示为因特网的结构示意图。

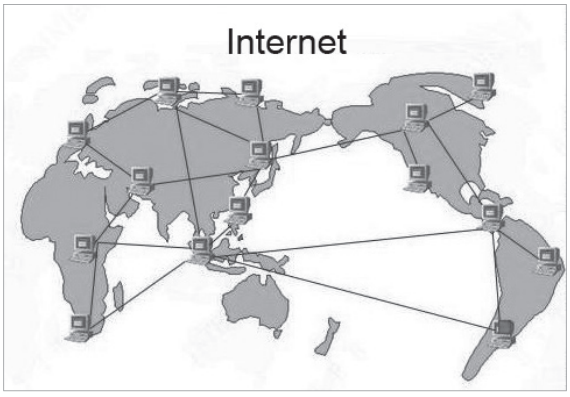


图 1-5 因特网的结构示意图

1.2.2 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，通常我们上网看到的内容就是万维网的内容。

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

浏览器是将互联网上的文本文档（或其他类型的文件）翻译成网页，并让用户与这些文件交互的一种软件工具，主要用于查看网页的内容。目前最常用的浏览器有为微软公司的 Microsoft Edge，图 1-6 所示是使用 Microsoft Edge 浏览器打开的页面。

图 1-6　使用 Microsoft Edge 浏览器打开的页面

1.2.3　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，是在 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。

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 1-7 所示为使用 URL 地址打开的网页。

图 1-7　使用 URL 地址打开的网页

1.2.4 IP 地址与 MAC 地址

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

MAC 地址与网络无关，也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 2 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。

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

1.2.5 上传和下载

上传（Upload）是从本地计算机（一般称客户端）向远程服务器（一般称服务器端）传送数据的行为和过程。下载（Download）是从远程服务器取回数据到本地计算机的过程。

1.3 认识网络通信协议

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

1.3.1 HTTP

HTTP（Hyper Text Transfer Protocol，超文本传输协议）是访问万维网使用的核心通信协议，也是今天所有 Web 应用程序使用的通信协议。HTTP 协议运行在 TCP 之上，用于指定客户端可能发送给服务器什么样的消息以及得到什么样的响应，这个简单模型是早期 Web 成功的有功之臣，因为它使开发和部署非常地直截了当。

1.3.2 TCP/IP

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

1.3.3 IP

IP 协议，即互联网协议（Internet Protocol），可实现两个基本功能：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。

1.3.4　ARP

ARP 协议（Address Resolution Protocol，地址解析协议）的基本功能就是通过目标设备的 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，必须要知道目标主机的 MAC 地址，这个 MAC 地址就是通过地址解析协议获得的。所谓“地址解析”就是主机在发送数据帧前将目标 IP 地址转换成目标 MAC 地址的过程。

1.3.5　ICMP

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

ICMP 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。

1.4　网络设备信息的获取

在一个完整的网络中，网络设备是必不可少的，如计算机、手机、平板电脑、打印机等，下面以计算机为例，来介绍获取网络设备信息的方法。

1.4.1　获取 IP 地址


微视频

在互联网中，一台计算机只有一个 IP 地址，因此，黑客要想攻击某台计算机，必须找到这台计算机的 IP 地址，然后才能进行入侵攻击，可以说 IP 地址是黑客实施入侵攻击的一个关键。使用 ipconfig 命令可以获取本地计算机的 IP 地址，具体的操作步骤如下。

Step 01 右击“开始”按钮，在弹出的快捷菜单中执行“运行”命令，如图 1-8 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 1-9 所示。

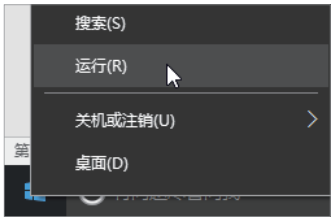


图 1-8　执行“运行”命令

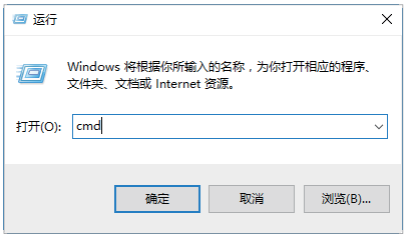


图 1-9　输入 cmd 命令

Step03 单击“确定”按钮，打开“命令提示符”窗口，在其中输入 ipconfig，按 Enter 键，即可显示出本机的 IP 配置相关信息，如图 1-10 所示。

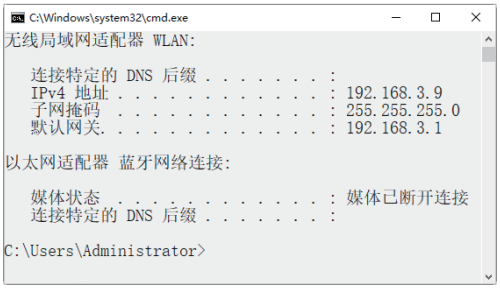
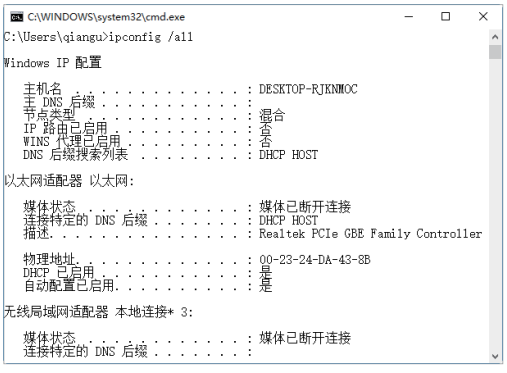


图 1-10　查看 IP 地址

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。


微视频




微视频

图 1-11　查看物理地址

1.4.2　获取物理地址

在“命令提示符”窗口中输入 ipconfig /all 命令，然后按 Enter 键，可以在显示的结果中看到一个物理地址：00-23-24-DA-43-8B，这就是本机的物理地址，也是本机的网卡地址，它是唯一的，如图 1-11 所示。

1.4.3　查看系统开放的端口

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，具体操作步骤如下。

Step01 打开“命令提示符”窗口，在其中输入 netstat –a –n 命令，如图 1-12 所示。

Step02 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 1-13 所示。

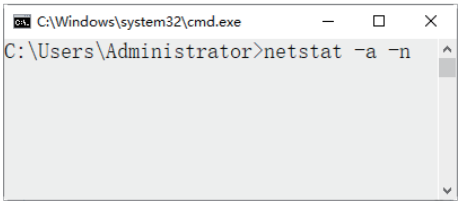


图 1-12　输入 netstat –a –n 命令

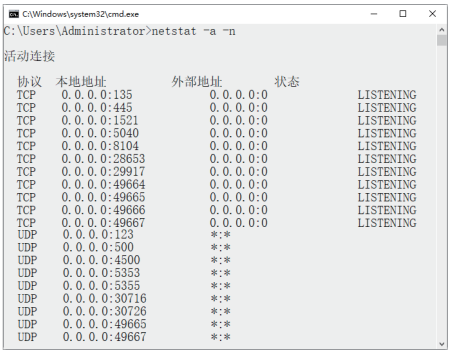


图 1-13　TCP 和 UCP 连接的端口号及其状态


微视频

1.4.4　查看系统注册表信息

注册表（Registry）是 Windows 中一个重要的数据库，用于存储系统和应用程序的设置信息。通过注册表，用户可以添加、删除、修改系统内的软件配置信息或硬件驱动程序。查看 Windows 系

统中注册表信息的操作步骤如下。

Step01 在 Windows 操作系统中选择“开始”→“运行”菜单项，打开“运行”对话框，在其中输入命令 regedit，如图 1-14 所示。

Step02 单击“确定”按钮，即可打开“注册表编辑器”窗口，在其中可查看注册表信息，如图 1-15 所示。

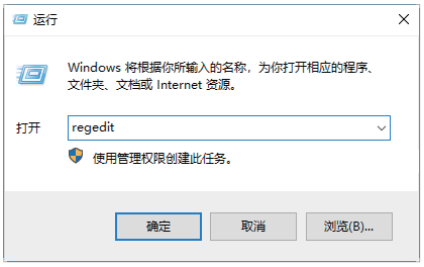


图 1-14　“运行”对话框

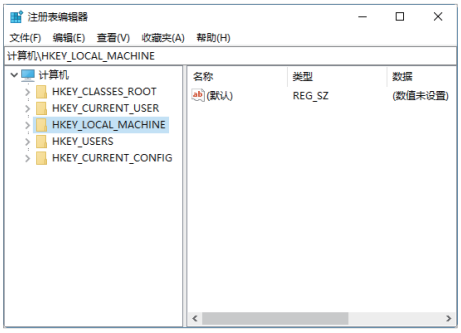


图 1-15　“注册表编辑器”窗口

1.4.5　获取系统进程信息


微视频

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

Step01 在 Windows 10 系统中，单击“开始”按钮，在弹出的菜单中选择“任务管理器”命令，如图 1-16 所示。

Step02 随即打开“任务管理器”窗口，在其中即可看到当前系统正在运行的进程，如图 1-17 所示。

图 1-16　“任务管理器”命令

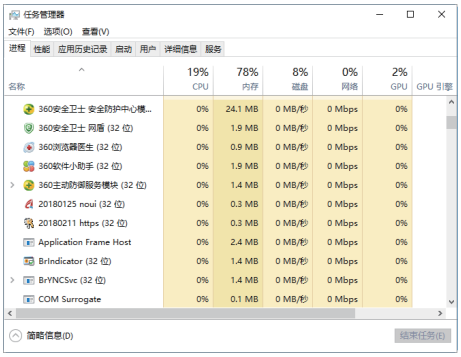


图 1-17　“任务管理器”窗口

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

1.5　实战演练

1.5.1　实战 1：查看进程起始程序


微视频

用户通过查看进程的起始程序，可以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 1-18 所示。

Step02 按 Enter 键，即可在反馈的信息中查看每个进程的起始程序或文件列表，这样就可以根据相关的知识来判断是否为病毒或木马发起的程序，如图 1-19 所示。

图 1-18　输入命令

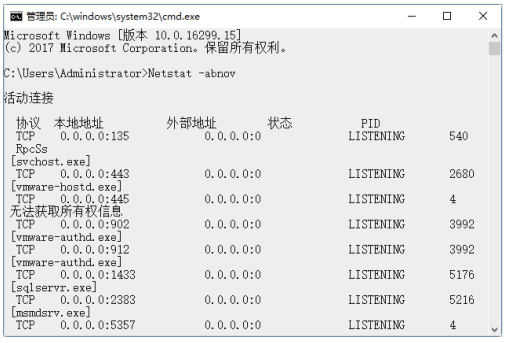


图 1-19　查看进程起始程序

微视频

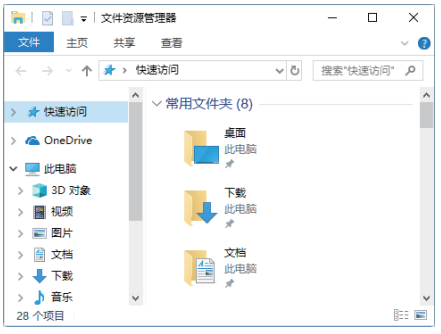


图 1-20　“文件资源管理器”窗口

1.5.2　实战 2：显示系统文件的扩展名

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

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 1-20 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 1-21 所示。

Step03 此时打开一个文件夹，用户便可以查看文件的扩展名，如图 1-22 所示。

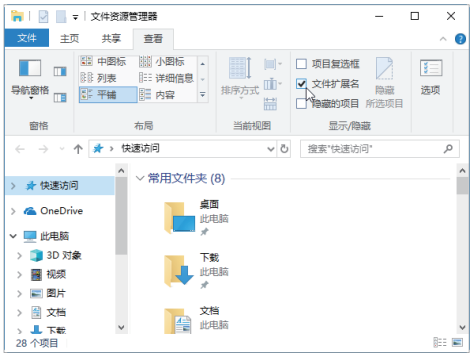


图 1-21　“查看”选项卡

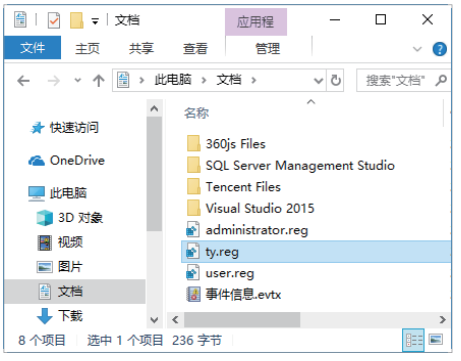


图 1-22　查看文件的扩展名

第 2 章 搭建 Web 安全测试环境

安全测试环境是安全工作者需要了解和掌握的内容。对于 Web 安全初学者来说，在学习过程中需要找到符合条件的目标计算机，并进行模拟攻击，而这些攻击目标并不是初学者能够从网络上搜索到的，这就需要通过搭建 Web 安全测试环境来解决这个问题。本章介绍 Web 安全测试环境的搭建，主要内容包括虚拟机的创建、Kali Linux 操作系统的创建等。

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，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 Virtual PC 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

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

创建虚拟系统的好处有以下几种。

- 虚拟技术是一种调配计算机资源的方法，可以更有效、更灵活地提供和利用计算机资源，降低成本，节省开支。

- 在虚拟环境里更容易实现程序自动化，有效地减少了测试要求和应用程序的兼容性问题，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 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，也可以快速还原之前快照，避免错误操作造成系统崩溃。

2.2.1 下载虚拟机软件

微视频

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

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

图 2-1 虚拟机官网页面

Step02 用户需要注册一个账号，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 2-2 所示。

图 2-2 “所有产品”选项卡

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

图 2-3 “查看下载组件”超链接

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

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

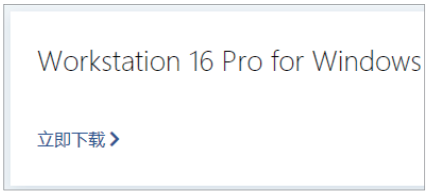


图 2-4　VMware 下载页面

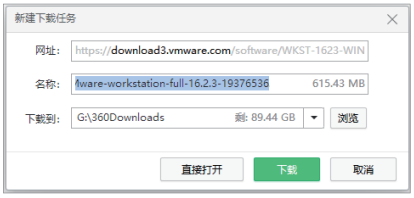


图 2-5　“新建下载任务”对话框

2.2.2　安装虚拟机软件

微视频

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

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

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

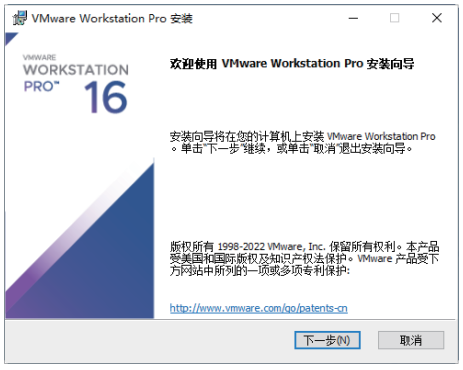


图 2-6　“欢迎使用 VMware Workstation Pro 安装向导”窗口

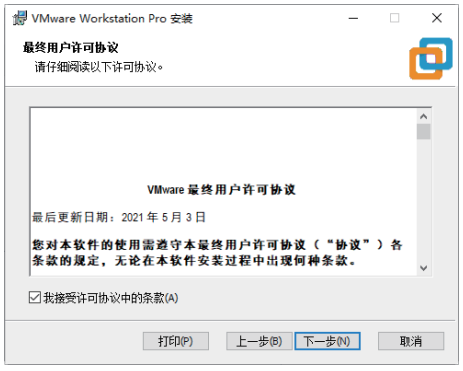


图 2-7　“最终用户许可协议”窗口

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

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

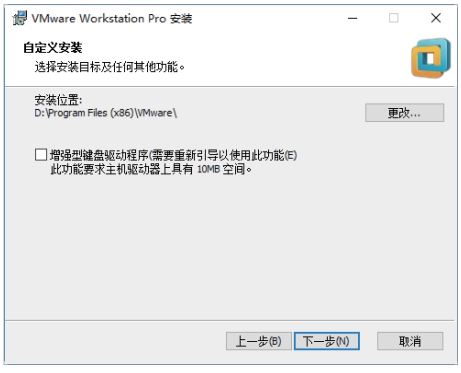


图 2-8　“自定义安装”窗口

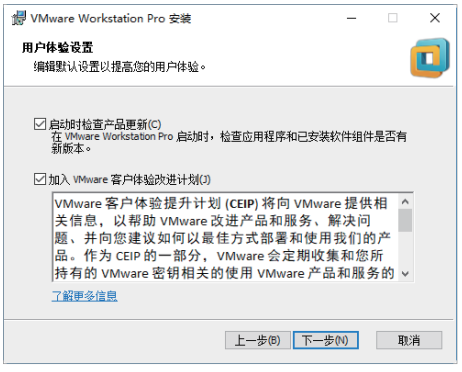


图 2-9　“用户体验设置”窗口

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

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

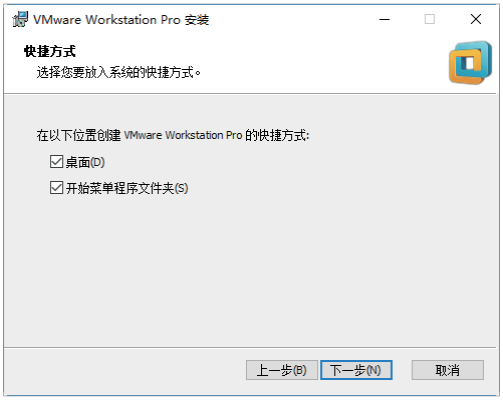


图 2-10 “快捷方式”窗口

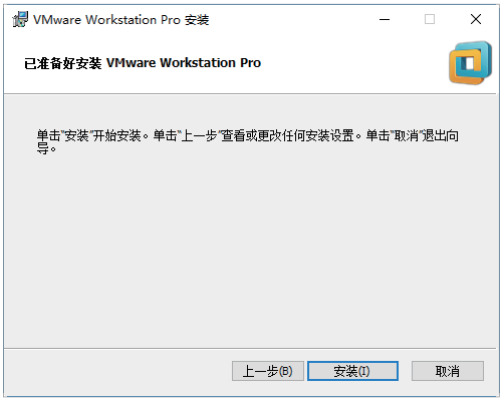


图 2-11 “已准备好安装 VMware Workstation Pro”窗口

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

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

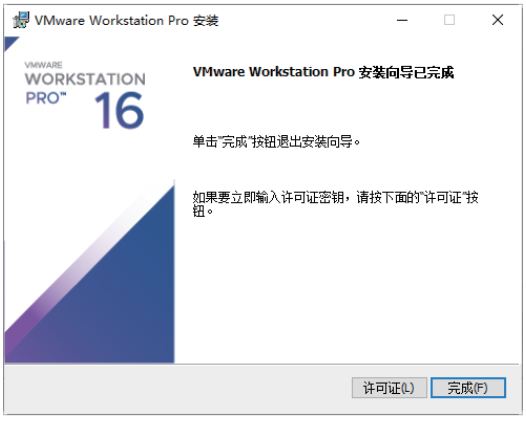


图 2-12 “VMware Workstation Pro 安装向导已完成”窗口

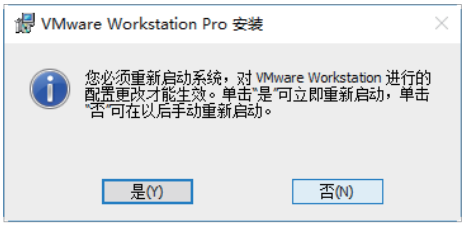


图 2-13 重新启动系统

微视频

2.2.3 创建虚拟机系统

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

Step01 双击桌面安装好的 VMware 虚拟机图标，打开 VMware 虚拟机软件，如图 2-14 所示。

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

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

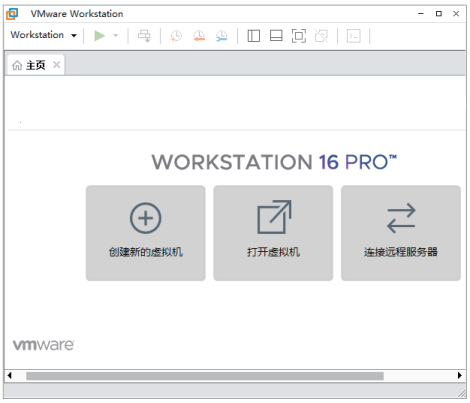


图 2-14　VMware 虚拟机软件

图 2-15　“新建虚拟机向导”对话框

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

图 2-16　“选择虚拟机硬件兼容性”对话框

图 2-17　“安装客户机操作系统”对话框

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

Step06 单击“版本”下方的下拉按钮，在弹出的下拉列表中选择“其他 Linux 5.x 内核 64 位”版本系统，这里的系统版本与主机系统版本无关，可以自由选择，如图 2-19 所示。

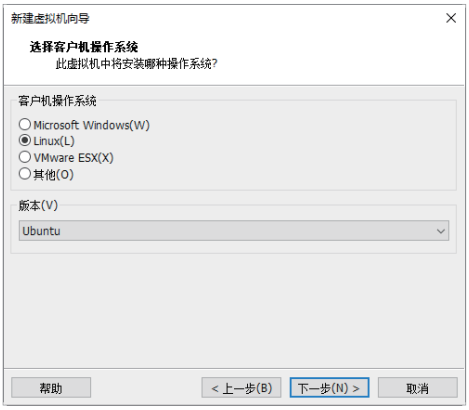


图 2-18　“选择客户机操作系统”对话框

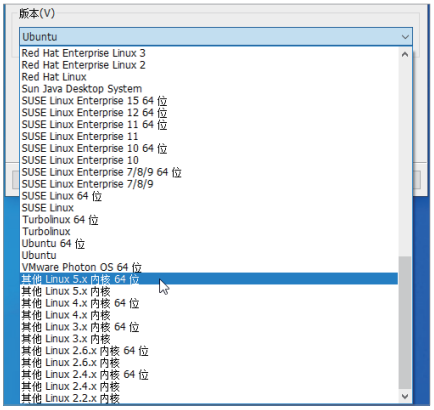


图 2-19　选择系统版本

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

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

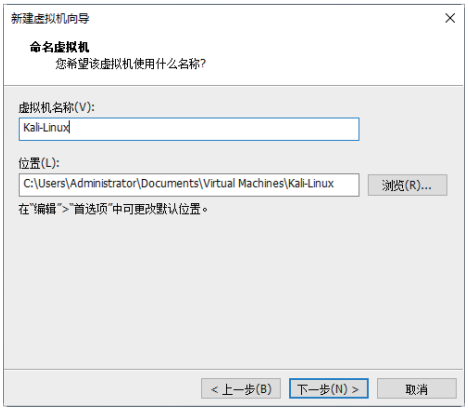


图 2-20 “命名虚拟机”对话框

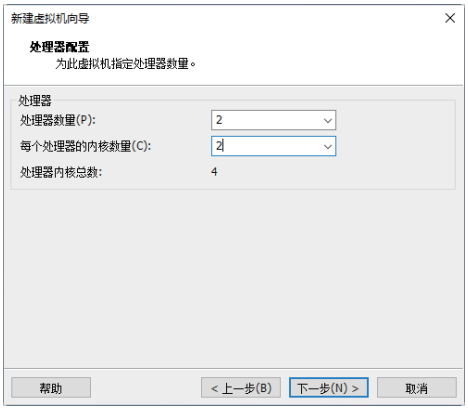


图 2-21 “处理器配置”对话框

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

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

图 2-22 “此虚拟机的内存”对话框

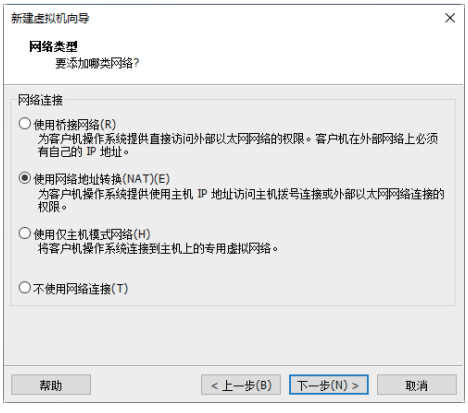


图 2-23 “网络类型”对话框

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

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

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

Step14 单击“下一步”按钮，进入“指定磁盘容量”对话框，这里“最大磁盘大小”设置 8GB 空间即可，选中“将虚拟盘拆分成多个文件”单选按钮，如图 2-27 所示。

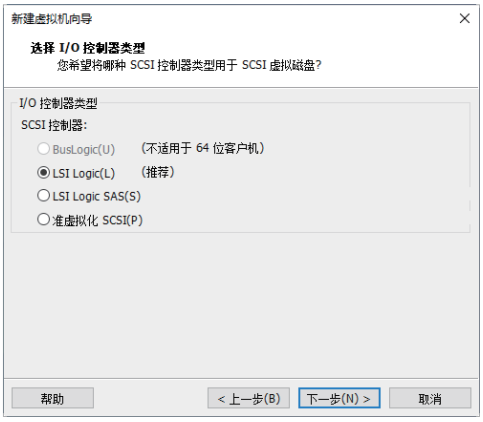


图 2-24　“选择 I/O 控制器类型”对话框

图 2-25　“选择磁盘类型”对话框

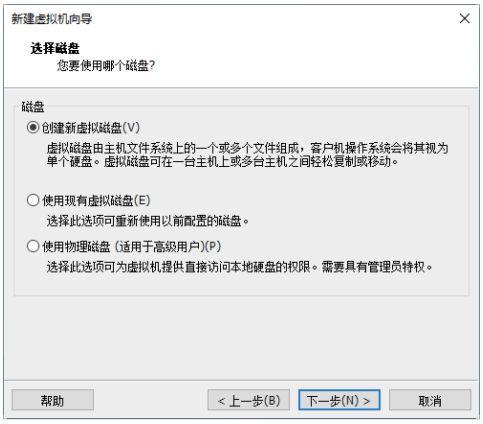


图 2-26　“选择磁盘”对话框

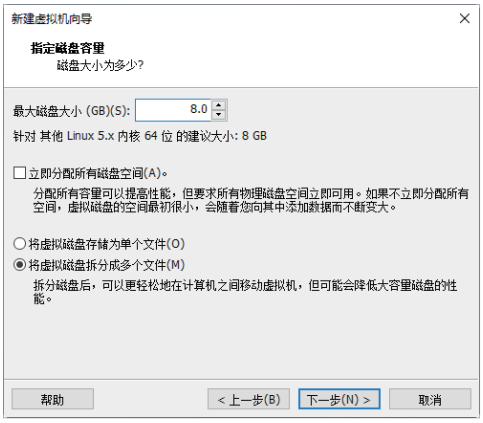


图 2-27　“指定磁盘容量”对话框

Step 15 单击“下一步”按钮，进入“指定磁盘文件”对话框，这里保持默认设置即可，如图 2-28 所示。

Step 16 单击“下一步”按钮，进入“已准备好创建虚拟机”对话框，如图 2-29 所示。

图 2-28　“指定磁盘文件”对话框

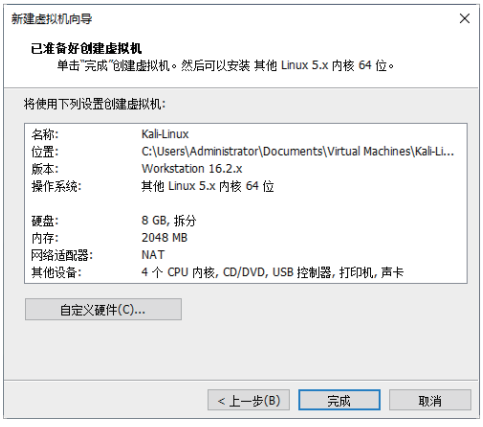


图 2-29　“已准备好创建虚拟机”对话框

Step 17 单击“完成”按钮，至此，便创建了一个新的虚拟机，如图 2-30 所示。以上操作相当于组装了一台裸机，其硬件设备可以根据实际需求再进行更改。

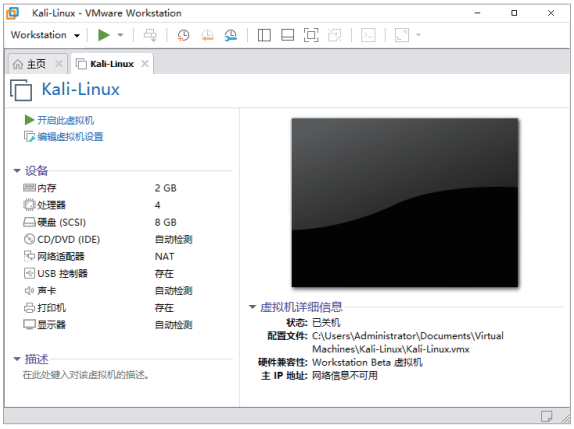


图 2-30　创建新的虚拟机

2.3　安装 Kali Linux 操作系统

现实中组装好计算机以后需要给它安装一个操作系统，这样计算机才可以正常工作，虚拟机也一样，同样需要安装一个操作系统。本节介绍如何安装 Kali Linux 操作系统。

2.3.1　下载 Kali Linux

微视频

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

Step01 在浏览器中输入 Kali Linux 系统的网址 https://www.kali.org，打开 Kali 官方网站，如图 2-31 所示。

Step02 单击 DOWNLOADS 菜单，在弹出的菜单中选择 Kail Linux 版本，如图 2-32 所示。

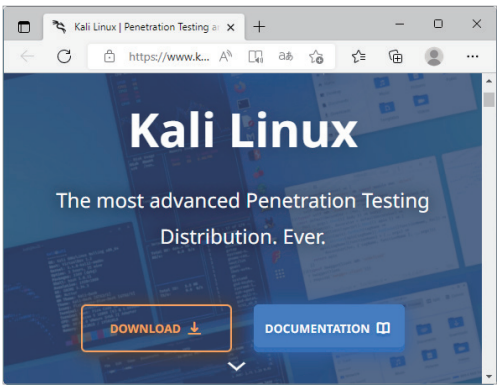


图 2-31　Kali 官方网站

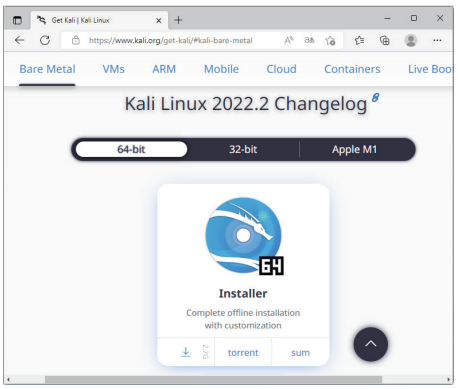


图 2-32　选择 Kail Linux 版本

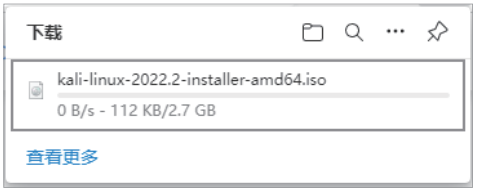


图 2-33　下载进度

Step03 单击“下载”按钮，即可开始下载 Kail Linux，并显示下载进度，如图 2-33 所示。

2.3.2　安装 Kali Linux


微视频

架设好虚拟机并下载好 Kali Linux 后，接下来便可以安装 Kali Linux 了。安装 Kali Linux 的具体操作步骤如下。

Step01 打开安装好的虚拟机，单击 CD/DVD 选项，如图 2-34 所示。

Step02 在打开的“虚拟机设置”页面中选中“使用 ISO 映像文件”单选按钮，如图 2-35 所示。

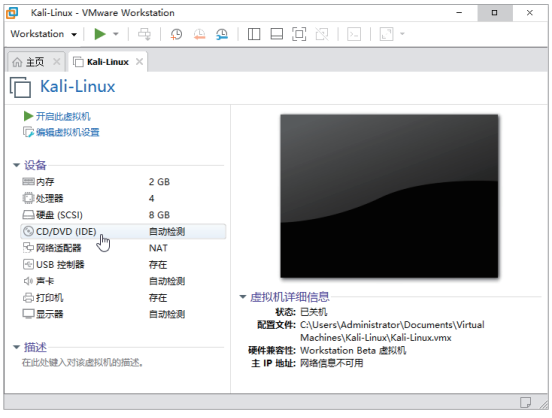


图 2-34　CD/DVD 选项

图 2-35　“虚拟机设置”对话框

Step03 单击“浏览”按钮，打开“浏览 ISO 映像”对话框，在其中选择下载好的系统映像文件，如图 2-36 所示。

Step04 单击“打开”按钮，返回虚拟机设置页面，单击“开启此虚拟机”选项，便可以启动虚拟机，如图 2-37 所示。

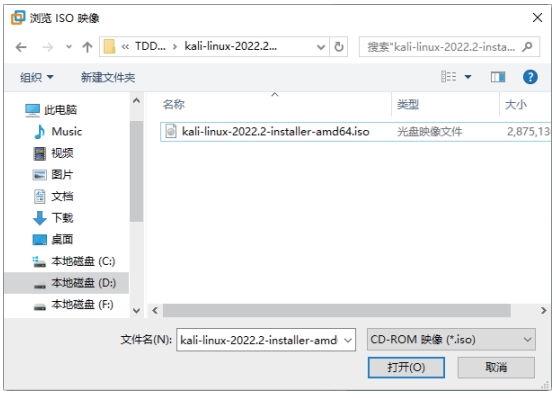


图 2-36　“浏览 ISO 映像”对话框

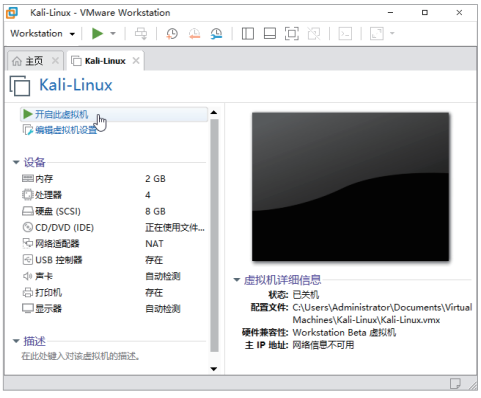


图 2-37　虚拟机设置页面

Step05 启动虚拟机后会进入启动选项页面，用户可以通过上下键选择 Graphical Install 选项，如图 2-38 所示。

Step06 选择完毕后，按 Enter 键，进入语言选择页面，这里选择简体中文选项，如图 2-39 所示。

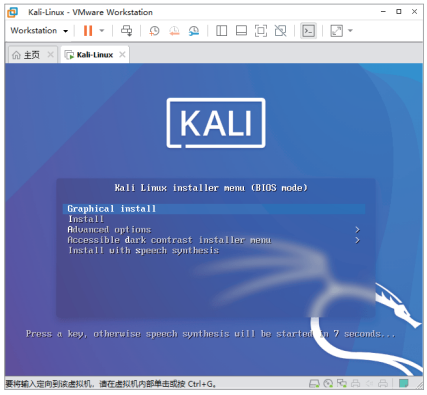


图 2-38　选择 Graphical Install 选项

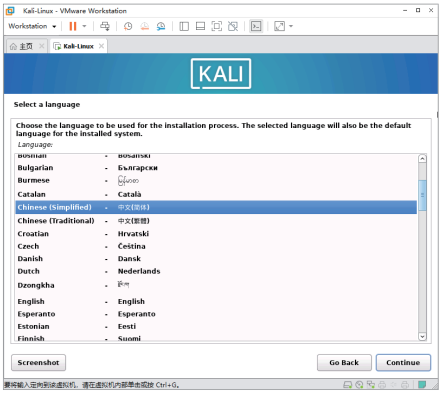


图 2-39　语言选择页面

Step07 单击 Continue 按钮，进入语言确认页面，保持系统默认设置，如图 2-40 所示。

Step08 单击“继续”按钮，进入“请选择您的区域”页面，它会自动上网匹配，即使不正确也没有关系，系统安装完成后还可以调整，这里保持默认设置，如图 2-41 所示。

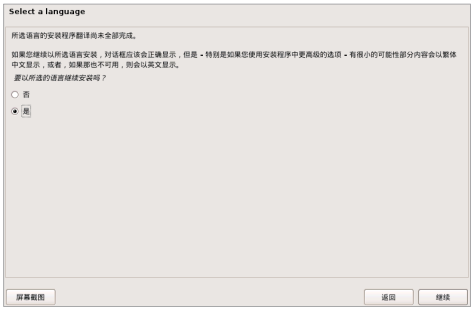


图 2-40　语言确认页面

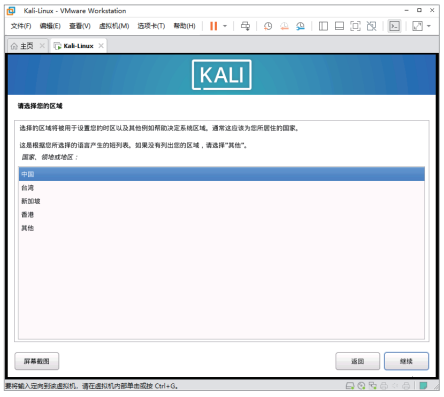


图 2-41　“请选择您的区域”页面

Step09 单击“继续”按钮，进入“配置键盘”页面，同样系统会根据语言选择来自行匹配，这里保持默认设置，如图 2-42 所示。

Step10 单击“继续”按钮，按照安装步骤的提示就可以完成 Kali Linux 的安装了。图 2-43 所示为安装基本系统界面。

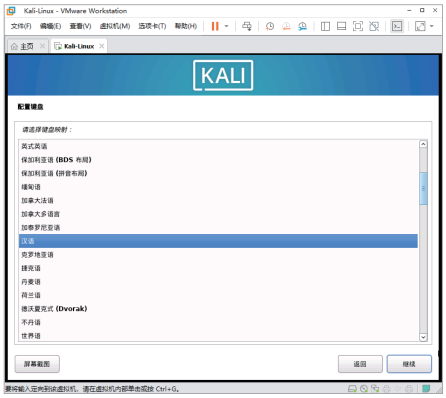


图 2-42　“配置键盘”页面

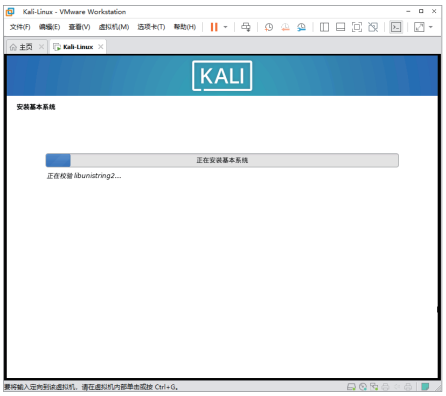


图 2-43　安装基本系统界面

Step 11 系统安装完成后，会提示用户重启进入系统，如图 2-44 所示。

Step 12 按下 Enter 键，安装完成后重启，进入“用户名”页面，在其中输入 root 管理员账号，如图 2-45 所示。

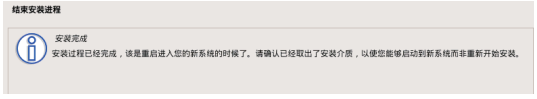


图 2-44　安装完成

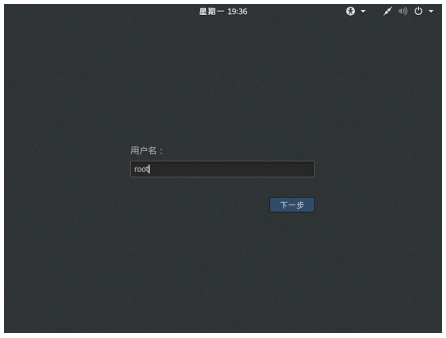


图 2-45　“用户名”页面

Step 13 单击“下一步”按钮，进入登录密码页面，在其中输入设置好的管理员密码，如图 2-46 所示。

Step 14 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 2-47 所示。

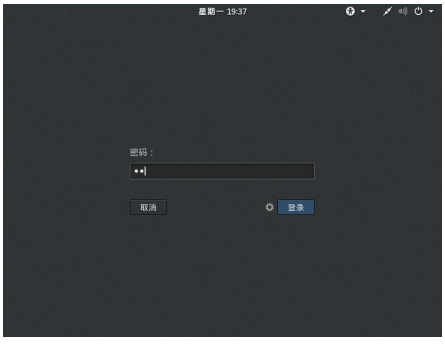


图 2-46　输入密码

图 2-47　Kail Linux 系统页面

2.3.3　更新 Kali Linux

微视频

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

Step 01 双击桌面上 Kali Linux 的终端黑色图标，如图 2-48 所示。

Step 02 打开 Kali Linux 的终端设置界面，在其中输入命令 apt update，然后按 Enter 键，即可获取需要更新软件的列表，如图 2-49 所示。

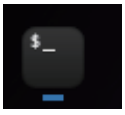


图 2-48　Kali Linux 图标

图 2-49　需要更新软件的列表

Step03 如果有需要更新的软件，可以运行 apt upgrade 命令，如图 2-50 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，如图 2-51 所示。

图 2-50　apt upgrade 命令

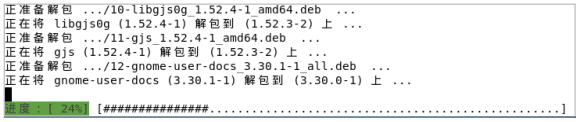


图 2-51　开始更新

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存在升级版本问题，如图 2-52 所示，这时可以先卸载旧版本。运行“apt-get remove < 软件名 >”命令，如图 2-53 所示，此时按 Y 键即可卸载旧版本。

```
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 2-52　升级版本问题

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

图 2-53　卸载旧版本

卸载完旧版本后，可以运行“apt-get install < 软件名 >”命令，如图 2-54 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 2-54　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，此时系统更新完成，如图 2-55 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 2-55　系统更新完成

2.4　安装 Windows 操作系统和 VMware Tools 工具

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。

2.4.1　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。

Step01 双击桌面安装好的 VMware 虚拟机图标，打开 VMware 虚拟机软件，如图 2-56 所示。

Step02 单击“创建新的虚拟机”按钮，进入“欢迎使用新建虚拟机向导”对话框，在其中选中“自定义”单选按钮，如图 2-57 所示。

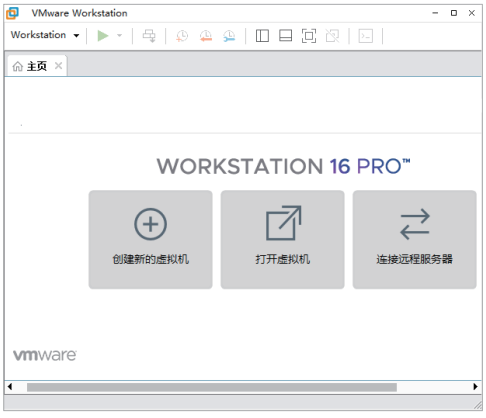


图 2-56　VMware 虚拟机软件

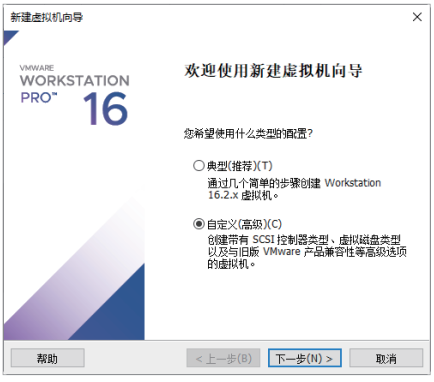


图 2-57　“欢迎使用新建虚拟机向导”对话框

Step03 单击“下一步”按钮，进入“选择虚拟机硬件兼容性”对话框，在其中设置虚拟机的硬件兼容性，这里采用默认设置，如图 2-58 所示。

Step04 单击“下一步”按钮，进入“安装客户机操作系统”对话框，在其中选中“稍后安装操作系统”单选按钮，如图 2-59 所示。

Step05 单击“下一步”按钮，进入“选择客户机操作系统”对话框，在其中选中 Microsoft Windows 单选按钮，如图 2-60 所示。

Step06 单击“版本”下方的下拉按钮，在弹出的下拉列表中选择 Windows 10 x64 版本系统，这里的系统版本与主机系统版本无关，可以自由选择，如图 2-61 所示。

图 2-58 “选择虚拟机硬件兼容性”对话框

图 2-59 “安装客户机操作系统”对话框

图 2-60 “选择客户机操作系统”对话框

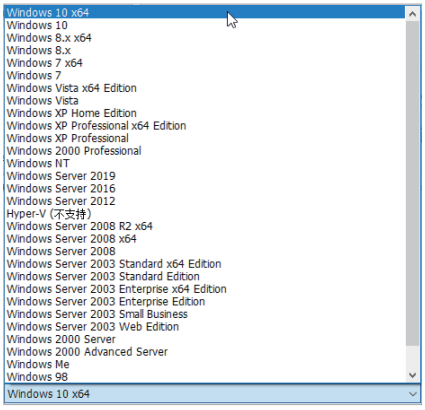


图 2-61 选择系统版本

Step07 单击“下一步”按钮，进入“命名虚拟机”对话框，在“虚拟机名称”文本框中输入虚拟机名称，在“位置”中选择一个存放虚拟机的磁盘位置，如图 2-62 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；“处理器内核总数”可以根据实际处理器内核数量设置，如图 2-63 所示。

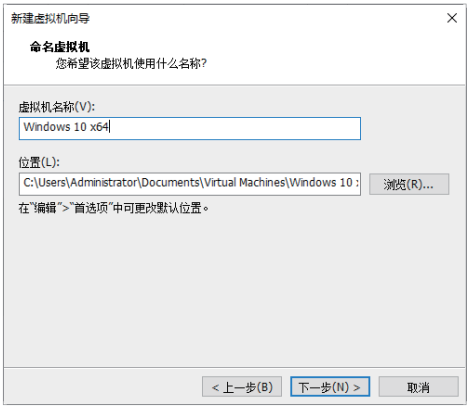


图 2-62 “命名虚拟机”对话框

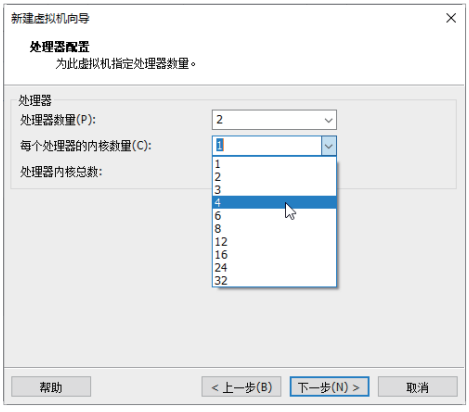


图 2-63 “处理器配置”对话框

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，内存不要低于 768MB，这里选择 1024MB 也就是 1GB 内存，如图 2-64 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（NAT）”单选按钮，如图 2-65 所示。

图 2-64　“此虚拟机的内存”对话框

图 2-65　“网络类型”对话框

Step11 单击“下一步”按钮，进入“选择 I/O 控制器类型”对话框，这里选中 LSI Logic SAS 单选按钮，如图 2-66 所示。

Step12 单击“下一步”按钮，进入“选择磁盘类型”对话框，这里选中 NVMe 单选按钮，如图 2-67 所示。

图 2-66　“选择 I/O 控制器类型”对话框

图 2-67　“选择磁盘类型”对话框

Step13 单击“下一步”按钮，进入“选择磁盘”对话框，这里选中“创建新虚拟磁盘”单选按钮，如图 2-68 所示。

Step14 单击“下一步”按钮，进入“指定磁盘容量”对话框，这里最大磁盘大小设置 60GB 空间即可，选中“将虚拟盘拆分成多个文件”单选按钮，如图 2-69 所示。

Step15 单击“下一步”按钮，进入“指定磁盘文件”对话框，这里保持默认设置即可，如图 2-70 所示。

Step16 单击“下一步”按钮，进入“已准备好创建虚拟机”对话框，如图 2-71 所示。

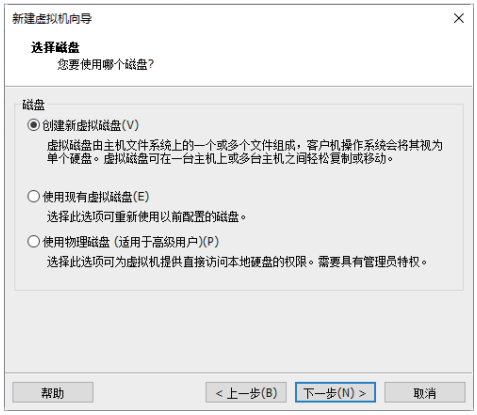


图 2-68 “选择磁盘”对话框

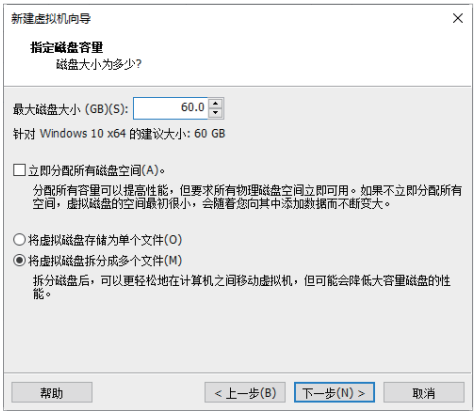


图 2-69 “指定磁盘容量”对话框

图 2-70 “指定磁盘文件”对话框

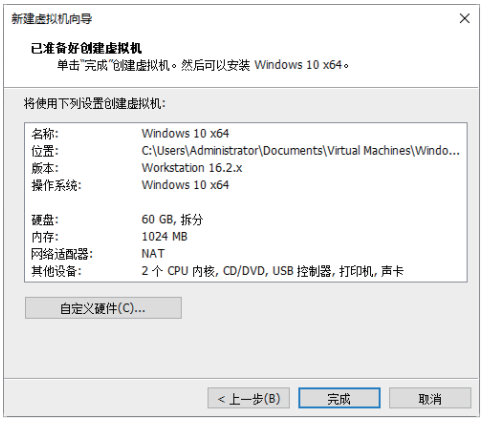


图 2-71 “已准备好创建虚拟机”对话框

Step17 单击“完成”按钮，至此，便创建了一个新的虚拟机，如图 2-72 所示。以上操作相当于组装了一台裸机，其中的硬件设配可以根据实际需求再进行更改。

Step18 单击“开启此虚拟机”链接，稍等片刻，Windows 10 操作系统进入安装窗口，如图 2-73 所示。

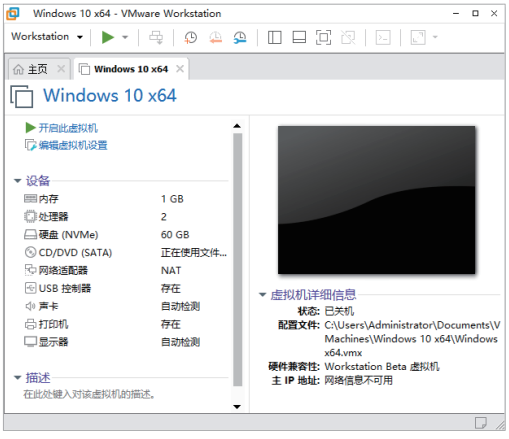


图 2-72 创建的新虚拟机

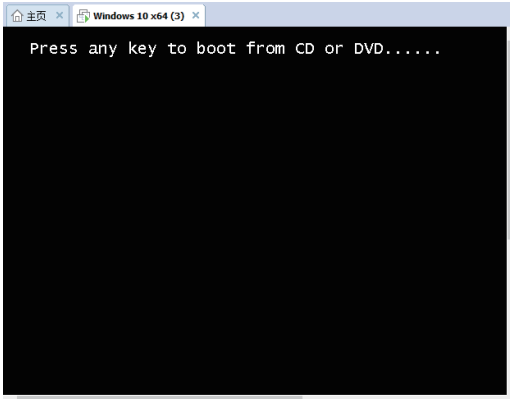


图 2-73 安装窗口

Step19 按任意键，即可打开 Windows 安装程序运行界面，安装程序将开始自动复制安装的文件并准备要安装的文件，如图 2-74 所示。

Step20 安装完成后，将显示安装后的操作系统界面，如图 2-75 所示。至此，整个虚拟机创建完成，安装的虚拟操作系统以文件的形式存放在硬盘之中。

图 2-74　准备要安装的文件

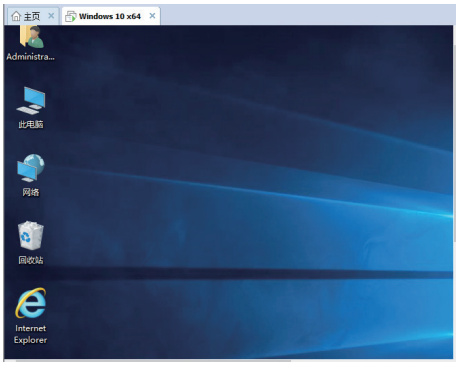


图 2-75　操作系统界面

2.4.2　安装 VMware Tools 工具

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

Step01 启动虚拟机进入虚拟系统，然后按 Ctrl+Alt 组合键，切换到真实的系统，如图 2-76 所示。

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

Step02 执行“虚拟机”→“安装 VMware Tools”命令，此时系统将自动弹出安装文件，如图 2-77 所示。

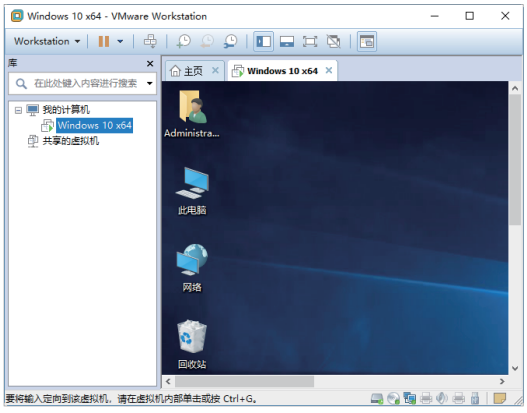


图 2-76　进入虚拟系统

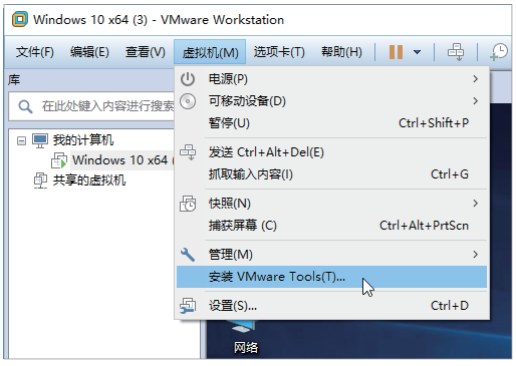


图 2-77　“安装 VMware Tools”命令

Step03 安装文件启动之后，将会弹出“欢迎使用 VMware Tools 的安装向导”窗口，如图 2-78 所示。

Step04 单击“下一步”按钮，进入“选择安装类型”窗口，根据实际情况选择相应的安装类型，这里选中“典型安装”单选按钮，如图 2-79 所示。

图 2-78 “欢迎使用 VMware Tools 的安装向导”窗口

图 2-79 “选择安装类型”窗口

Step 05 单击“下一步”按钮，进入“已准备好安装 VMware Tools”窗口，如图 2-80 所示。

Step 06 单击“安装”按钮，进入“正在安装 VMware Tools”窗口，在其中显示了 VMware Tools 工具的安装状态，如图 2-81 所示。

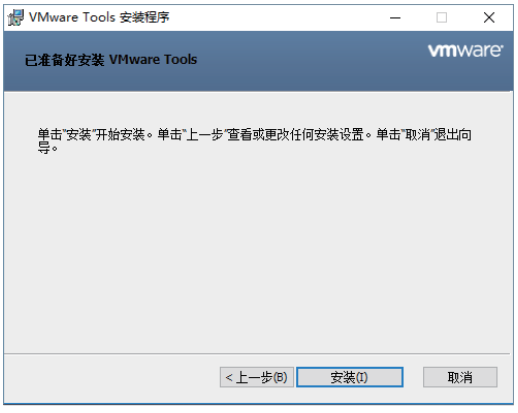


图 2-80 “已准备好安装 VMware Tools”窗口

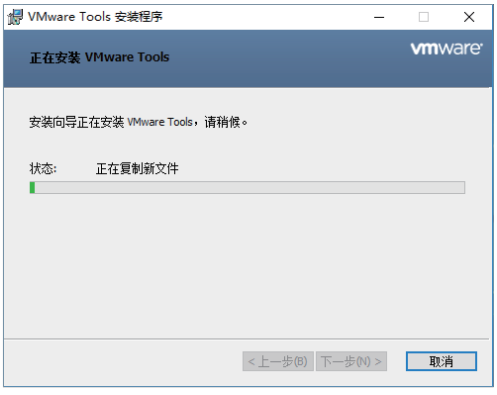


图 2-81 “正在安装 VMware Tools”窗口

Step 07 安装完成后，进入“VMware Tools 安装向导已完成”窗口，如图 2-82 所示。

Step 08 单击“完成”按钮，弹出一个信息提示框，要求必须重新启动系统，这样对 VMware Tools 进行的配置更改才能生效，如图 2-83 所示。

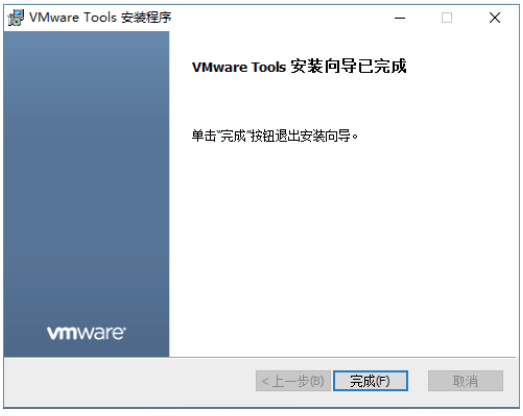


图 2-82 “VMware Tools 安装向导已完成”窗口

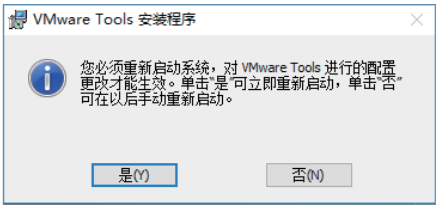


图 2-83 信息提示框

Step09 单击“是”按钮，系统即可自动启动，虚拟系统重新启动之后即可发现虚拟机工具已经成功安装，再次选择“虚拟机”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 2-84 所示。

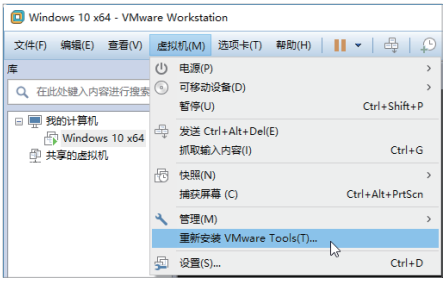


图 2-84　“重新安装 VMware Tools”菜单命令

2.5　实战演练

2.5.1　实战 1：关闭开机多余启动项目

微视频

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

Step01 按 Ctrl+Alt+Delete 组合键，打开如图 2-85 所示的界面。

Step02 单击“任务管理器”选项，打开“任务管理器”窗口，如图 2-86 所示。

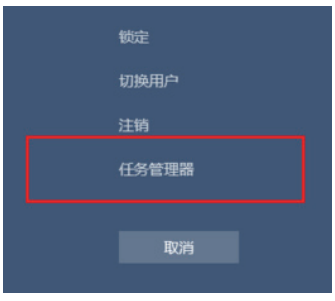


图 2-85　“任务管理器”选项

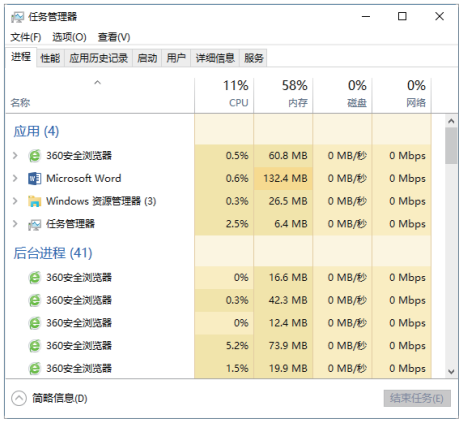


图 2-86　“任务管理器”窗口

Step03 选择“启动”选项卡，进入“启动”界面，在其中可以看到系统中的开机启动项列表，如图 2-87 所示。

Step04 选择开机启动项列表中需要禁用的启动项，单击“禁用”按钮，即可禁止该启动项开机自启，如图 2-88 所示。

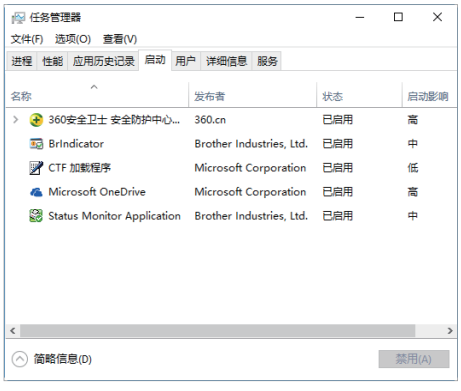


图 2-87　“启动”选项卡

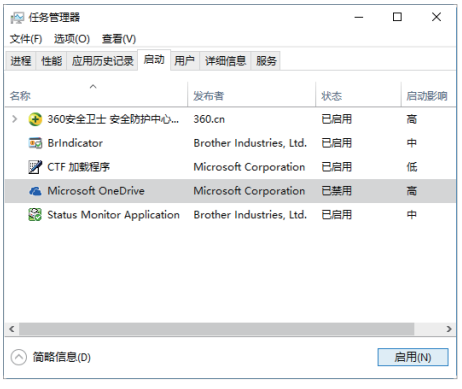


图 2-88　禁止开机启动项


微视频

2.5.2 实战 2：诊断和修复网络不通的问题

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

Step01 打开“网络连接”窗口，右击需要诊断的网络图标，在弹出的快捷菜单中选择“诊断”选项，弹出“Windows 网络诊断”对话框，并显示网络诊断的进度，如图 2-89 所示。

Step02 诊断完成后，将会在下方的窗格中显示诊断的结果，如图 2-90 所示。

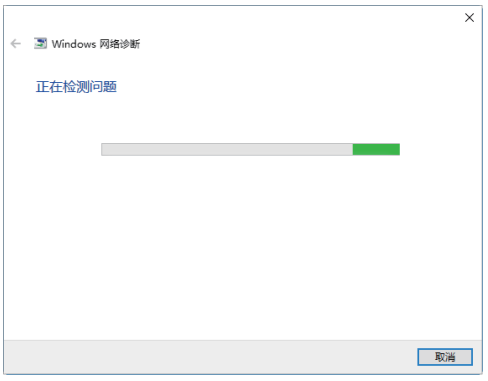


图 2-89 显示网络诊断的进度

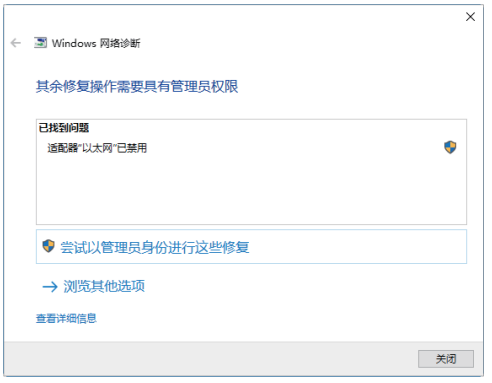


图 2-90 显示诊断的结果

Step03 单击“尝试以管理员身份进行这些修复”链接，即可开始对诊断出来的问题进行修复，如图 2-91 所示。

Step04 修复完毕后，会给出修复的结果，提示用户疑难解答已经完成，并在下方显示已修复信息，如图 2-92 所示。

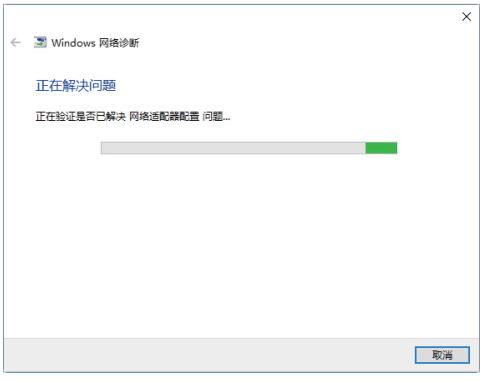


图 2-91 修复网络问题

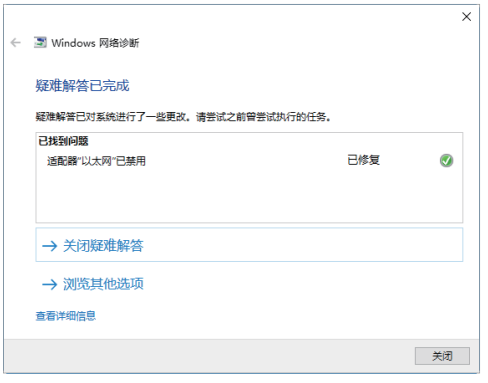


图 2-92 显示已修复信息

第 3 章

信息收集与踩点侦察

黑客在入侵之前，都会进行踩点以收集相关信息，在信息收集中，最重要的就是收集服务器的配置信息和网站的敏感信息，其中包括域名及子域名信息、确定扫描的范围以及获取相关服务与端口信息、CMS 指纹以及目标网站的 IP 地址等。本章介绍 Web 安全之踩点侦察的相关知识。

3.1 收集域名信息

在知道目标的域名之后，首先需要做的事情就是获取域名的注册信息，包括该域名的 DNS 服务器信息、备案信息等。收集域名信息的常用方法有以下几种。

3.1.1 Whois 查询

微视频

一个网站在制作完毕后，要想发布到互联网上，还需要向有关机构申请域名，申请到的域名信息将被保存到域名管理机构的数据库中，任何用户都可以进行查询，这就使黑客有机可乘了。因此，踩点流程中就少不了查询 Whois。

（1）在中国互联网信息中心查询。

中国互联网信息中心是非常权威的域名管理机构，在该机构的数据库中记录着所有以 .cn 为结尾的域名注册信息。查询 Whois 的操作步骤如下。

Step01 在 Microsoft Edge 浏览器的地址栏中输入中国互联网信息中心的网址 http://www.cnnic.net.cn/，即可打开其首页，如图 3-1 所示。

Step02 在“查询”区域的文本框中输入要查询的中文域名，如这里输入“淘宝 .cn”，然后输入验证码，如图 3-2 所示。

Step03 单击“查询”按钮，打开“验证码”对话框，在“验证码”文本框中输入验证码，如图 3-3 所示。

Step04 单击“确定”按钮，即可看到要查询域名的详细信息，如图 3-4 所示。

图 3-1 中国互联网信息中心首页

图 3-2　输入中文域名

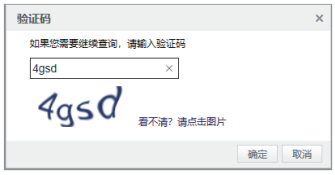


图 3-3　“验证码”对话框

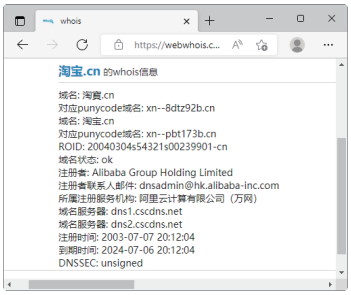


图 3-4　域名详细信息

（2）在万网查询。

万网是中国最大的域名和网站托管服务提供商，它提供 .cn 的域名注册信息，而且还可以查询 .com 等域名信息。查询 Whois 的操作步骤如下。

Step01 在 Microsoft Edge 浏览器的地址栏中输入万网的网址 https://wanwang.aliyun.com/，即可打开其首页，如图 3-5 所示。

Step02 在“域名”文本框中输入要查询的域名，然后单击“查询域名”按钮，即可看到相关的域名信息，如图 3-6 所示。

图 3-5　万网首页

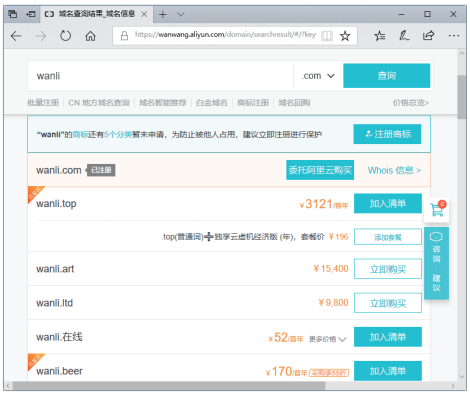


图 3-6　域名详细信息

Step03 在域名信息右侧，单击“Whois 信息”超链接，即可查看 Whois 信息，如图 3-7 所示。

图 3-7　Whois 信息

3.1.2　DNS 查询

DNS 即域名系统，是 Internet 的一项核心服务。简单地说，利用 DNS 服务系统可以将互联网上的域名与 IP 地址进行域名解析，因此，计算机只认识 IP 地址，不认识域名。该系统作为可以将域名和 IP 地址相互转换的一个分布式数据库，能够帮助用户更为方便地访问互联网，而不用记住被机器直接读取的 IP 地址。

目前，查询 DNS 的方法比较多，常用的方式是使用 Windows 系统自带的 nslookup 工具来查询 DNS 中的各种数据。下面介绍两种使用 nslookup 查看 DNS 的方法。

（1）使用命令行方式。

该方式主要是用来查询域名对应的 IP 地址，即查询 DNS 的记录，通过该记录黑客可以查询该域名的主机所存放的服务器，其命令格式为：nslookup 域名。

若想要查看 www.baidu.com 对应的 IP 信息，其具体的操作步骤如下。

Step01 打开“命令提示符”窗口，在其中输入 nslookup www.baidu.com 命令，如图 3-8 所示。

Step02 按 Enter 键，即可得出其运行结果，在运行结果中可以看到“名称”和 Addresses 行分别对应域名和 IP 地址，而最后一行显示的是目标域名并注明别名，如图 3-9 所示。

图 3-8　输入命令

图 3-9　查询域名和 IP 地址

（2）交互式方式。

可以使用 nslookup 的交互模式对域名进行查询，具体的操作步骤如下。

Step01 在“命令提示符”窗口中运行 nslookup 命令，然后按 Enter 键，即可得出其运行结果，如图 3-10 所示。

Step02 在“命令提示符”窗口中输入命令 set type=mx，然后按 Enter 键，进入命令运行状态，如图 3-11 所示。

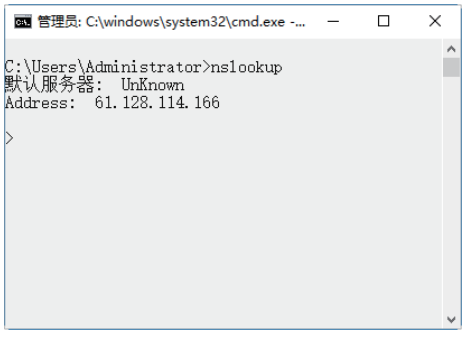


图 3-10　运行 nslookup 命令

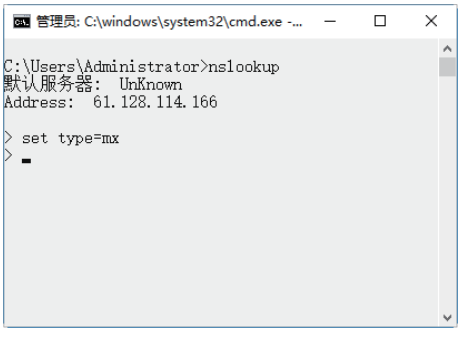


图 3-11　运行 set type=mx 命令

Step03 在“命令提示符”窗口中再输入想要查看的网址（必须去掉 www），如 baidu.com，按

Enter 键，即可得出百度网站的相关 DNS 信息，即 DNS 的 MX 关联记录，如图 3-12 所示。

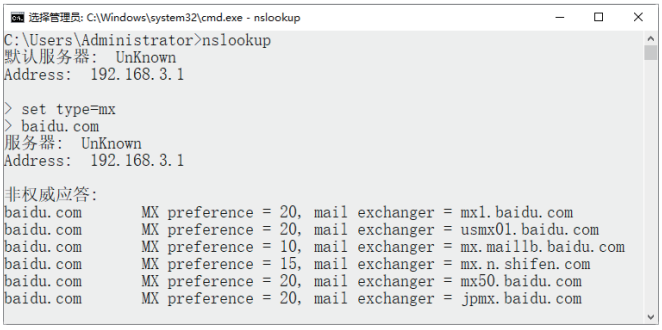


图 3-12　查看 DNS 信息

3.1.3　备案信息查询

根据我国国家法律法规的规定，网站的所有者应向国家有关部门申请备案，即网站备案。这是国家有关部门对网站进行的管理，防止网站从事非法经营活动。

常用的查询备案信息的网站有以下三个。

（1）ICP 备案查询网：http://www.beianx.cn/。

（2）天眼查：https://www.tianyancha.com/。

（3）站长工具：https://icp.chinaz.com/。

图 3-13 所示为在站长工具网站查询网址为 https://www.baidu.com/ 的备案信息。

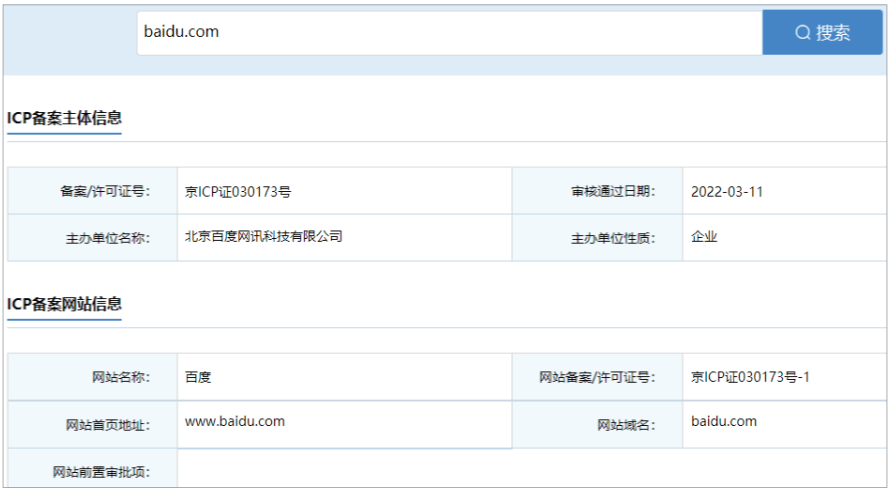


图 3-13　网站备案信息

3.1.4　敏感信息查询

百度是世界上流行的搜索引擎，对于一位 Web 安全工作者而言，它可能是一款绝佳的查询工具。我们可以通过构造特殊的关键字语法来搜索互联网上的相关敏感信息。百度的常用语法及说明如表 3-1 所示。

例如，想要搜索一些学校网站的后台，语法为“site:edu.cn intext: 后台管理”，意思是搜索网站正文中含有“后台管理”并且域名后缀是 edu.cn 的网站，搜索结果如图 3-14 所示。

表 3-1　百度的常用语法及其说明

关　键　字	说　　明
site	指定域名
inurl	URL 中存在关键字的网页
intext	网页正文中的关键字
filetype	指定文件类型
intitle	网页标题中的关键字
link	link:baidu.com 表示返回所有和 baidu.com 做了链接的 URL
info	查找指定站点的一些基本信息
cache	搜索百度里关于某些内容的缓存

图 3-14　搜索结果

利用百度搜索引擎，我们可以轻松地得到想要的信息，还可以用它来收集数据库文件、SQL 注入，配置信息、源代码泄露，未授权访问和 robots.txt 等敏感信息。当然，除了百度搜索引擎外，我们还可以在 Bing、Google 等搜索引擎上搜索敏感信息。

3.2　收集子域名信息

子域名是指顶级域名下的域名，也被称为二级域名。假设我们的目标网络规模较大，直接从主域中入手显然是很不理智的，因为对于规模化的目标，一般其主域名都是重点防护区域，所以不如直接进入目标的某个子域中，再想办法接近真正的目标。下面介绍收集子域名信息的方法。

3.2.1　使用子域名检测工具

用于子域名检测的工具主要有 Layer 子域名挖掘机、K8、wydomain、dnsmaper、站长工具等。这里推荐使用 Layer 子域名挖掘机和站长工具。

Layer 子域名挖掘机的使用方法比较简单，在域名对话框中直接输入域名就可以进行扫描，它显示的信息比较详细，有域名、解析 IP、开放端口、WEB 服务器和网站状态等，如图 3-15 所示。

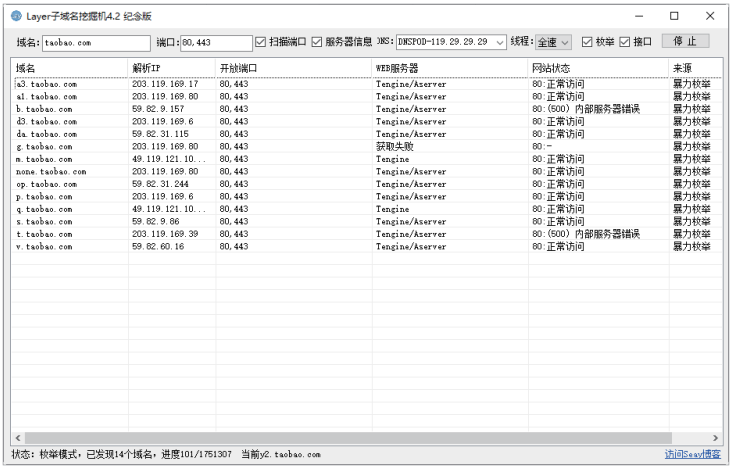


图 3-15　Layer 子域名挖掘机工作界面

图 3-16　查询子域名

站长工具是站长的必备工具。经常使用站长工具可以了解站点的 SEO 数据变化，还可以进行网站死链接检测、蜘蛛访问、HTML 格式检测、网站速度测试、友情链接检查、域名和子域名查询等。站长工具的使用方法比较简单，在域名对话框中直接输入域名就可以进行子域名的查询了，如图 3-16 所示。

3.2.2　使用搜索引擎查询

使用搜索引擎可以收集子域名信息，例如要搜索百度旗下的子域名就可以使用 site:baidu.com 语句，如图 3-17 所示。

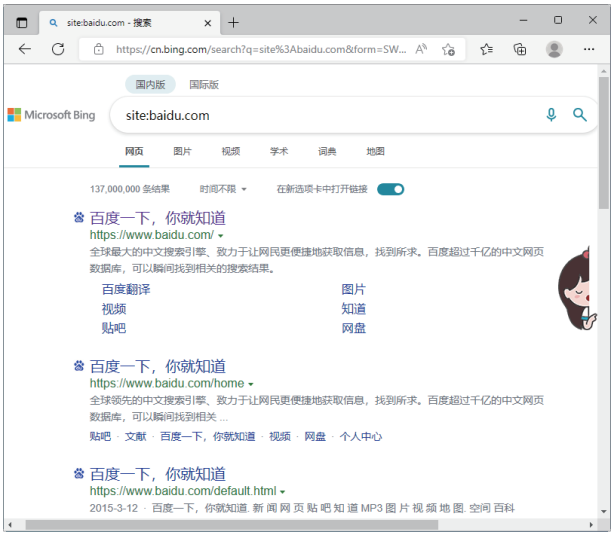


图 3-17　使用搜索引擎查询子域名

3.2.3　使用第三方服务查询

很多第三方服务汇聚了大量 DNS 数据库，通过它们可以检索某个给定域名的子域名。只需在其搜索栏中输入域名，就可以检索到相关的域名信息。例如，可以利用 DNSdumpster 网站（https://dnsdumpster.com/）搜索出指定域潜藏的大量子域名。

在浏览器的地址栏中输入 https://dnsdumpster.com/ 网址，打开 DNSdumpster 网站首页，在搜索文本框中输入 baidu.com，如图 3-18 所示。

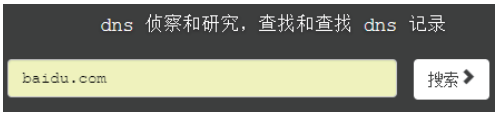


图 3-18　DNSdumpster 网站首页

单击“搜索”按钮，即可显示出 baidu.com 的查询信息。图 3-19 所示为 DNS 服务器信息。

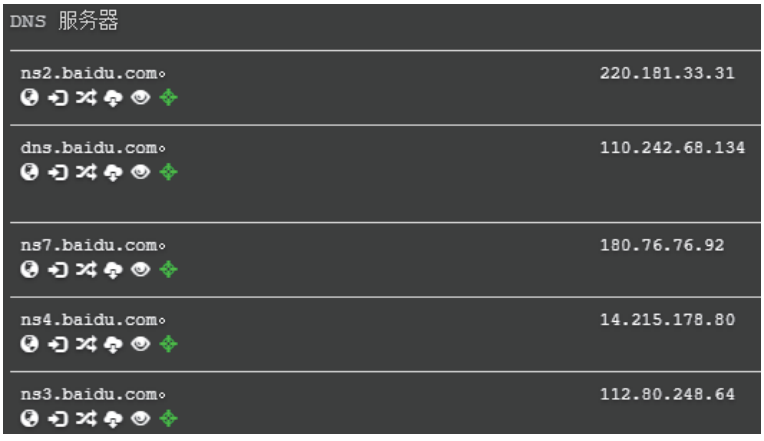


图 3-19　DNS 服务器信息

图 3-20 所示为邮件服务器信息。

图 3-20　邮件服务器信息

图 3-21 所示为查询到的子域名信息。

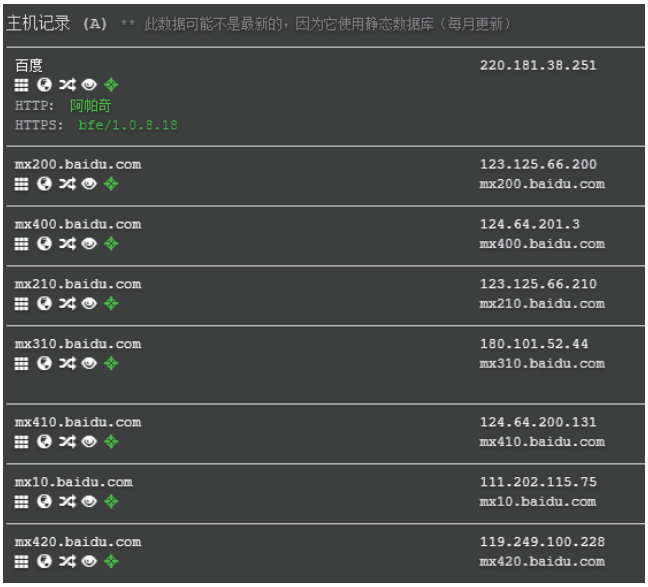


图 3-21　子域名信息

单击子域名下方的图标，跳转到另一个网页，再单击“快速扫描”按钮，即可查看子域名开放的端口，如图 3-22 所示。

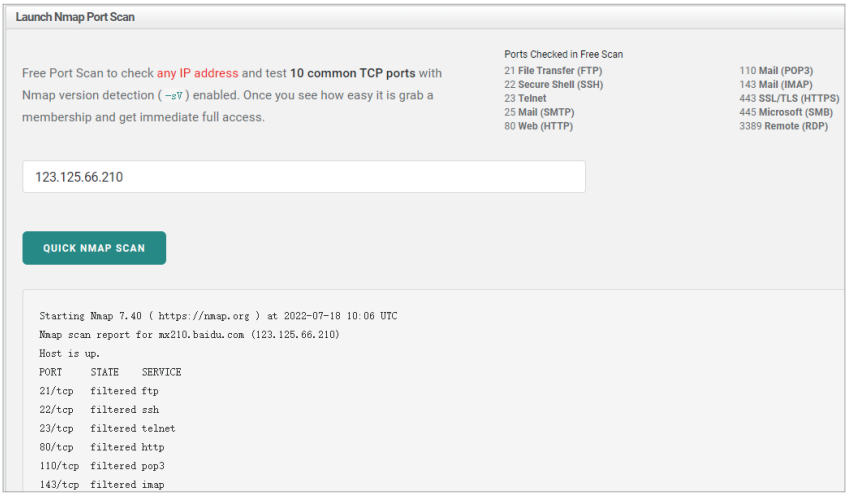


图 3-22　子域名开放的端口

3.3　网络中的踩点侦察

踩点，概括地说就是获取信息的过程。踩点是黑客实施攻击之前必须要做的工作之一，踩点过程中所获取的目标信息也决定着攻击是否成功。下面具体介绍实施踩点的具体流程，可以帮助用户更好地防护自己计算机的安全。

微视频

3.3.1　侦察对方是否存在

黑客在攻击之前，需要确定目标主机是否存在，目前确定目标主机是否存在最为常用的方法就

是使用 Ping 命令。Ping 命令常用于对固定 IP 地址的侦察，下面介绍侦察某网站的 IP 地址的侦察步骤。

Step01 在 Windows 10 系统界面中，右击“开始”按钮，在弹出的快捷菜单中单击“运行”菜单项，打开“运行”对话框，在“打开”文本框中输入 cmd，如图 3-23 所示。

Step02 单击“确定”按钮，打开“命令提示符”窗口，在其中输入 ping www.baidu.com，如图 3-24 所示。

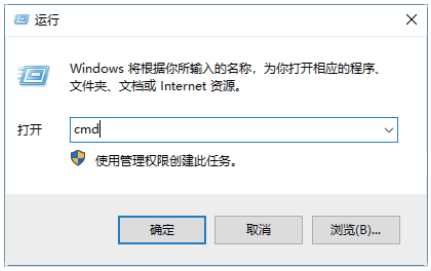


图 3-23　“运行”对话框

图 3-24　“命令提示符”窗口

Step03 按 Enter 键，即可显示出 ping 百度网站的结果，如果 ping 通过了，将会显示该 IP 地址返回的 byte、time 和 TTL 的值，说明该目标主机一定存在于网络之中，这样就具有了进一步攻击的条件，而且 time 时间越短，表示响应的时间就越快，如图 3-25 所示。

Step04 如果 ping 不通过，则会出现“无法访问目标主机”提示信息，这就表明对方要么不在网络中，要么没有开机，要么是对方存在，但是设置了 ICMP 数据包的过滤等。如图 3-26 所示就是 ping IP 地址为“192.168.0.100”不通的结果。

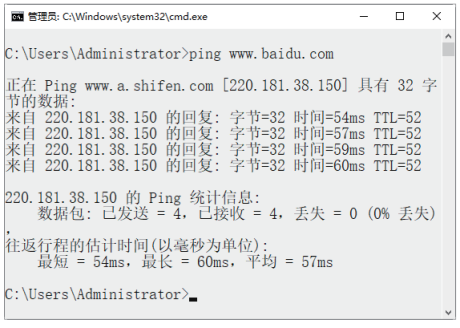


图 3-25　ping 百度网站的结果

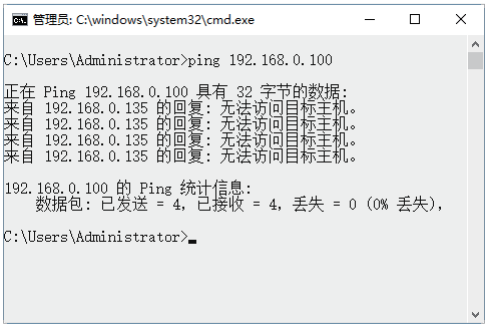


图 3-26　ping 命令不通过的结果

注意：在 ping 没有通过，且计算机又存在网络中的情况下，要想攻击该目标主机，就比较容易被发现，达到攻击目的就比较难。

另外，在实际侦察对方是否存在的过程中，如果一个 IP 地址一个 IP 地址地侦察，将会浪费很多精力和时间，那么有什么方法来解决这一问题呢？其实这个问题不难解决，因为目前网络上存在多种扫描工具，这些工具的功能非常强大，除了可以对一个 IP 地址进行侦察，还可以对一个 IP 地址范围内的主机进行侦察，从而得出目标主机是否存在，以及开放的端口和操作系统类型等，常用的工具有 SuperSsan、nmap 等。

利用 SuperScan 扫描 IP 地址范围内的主机的操作步骤如下。

Step01 双击下载的 SuperScan 可执行文件，打开 SuperScan 操作界面，在“扫描”选项卡的“IP 地址”栏目中输入开始 IP 和结束 IP，如图 3-27 所示。

Step02 单击“扫描”按钮，即可进行扫描。在扫描完毕之后，即可在 SuperScan 操作界面中查看到扫描的结果，主要包括在该 IP 地址范围内哪些主机是存在的，非常方便直观，如图 3-28 所示。

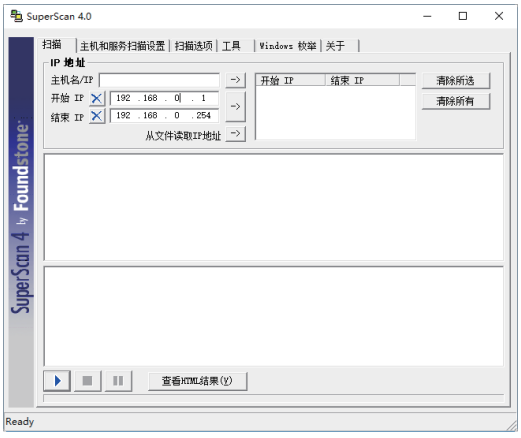


图 3-27　SuperScan 操作界面

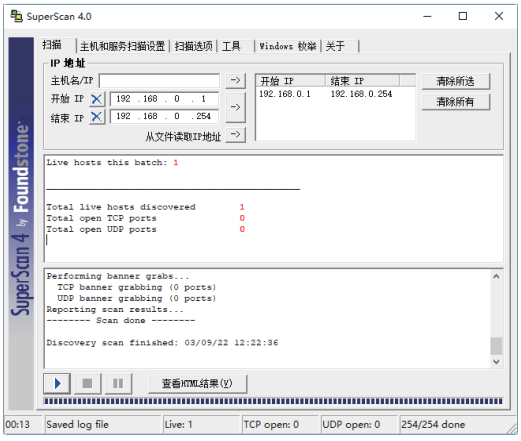


图 3-28　扫描结果


微视频

3.3.2　侦察对方的操作系统

黑客在入侵某台主机时，事先必须侦察出该计算机的操作系统类型，这样才能根据需要采取相应的攻击手段，以达到自己的攻击目的。常用侦察对方操作系统的方法为：使用 ping 命令探知对方的操作系统。

一般情况下，不同的操作系统其对应的 TTL 返回值不相同，Windows 操作系统对应的 TTL 值一般为 128；Linux 操作系统的 TTL 值一般为 64。因此，黑客在使用 Ping 命令与目标主机相连接时，可以根据不同的 TTL 值来推测目标主机的操作系统类型，一般数值在 128 左右的是 Windows 系列，数值在 64 左右的是 Linux 系列。这是因为不同的操作系统的机器对 ICMP 报文的处理与应答也有所不通，TTL 的值是每过一个路由器就会减 1。

在“运行”对话框中输入 cmd，单击“确定”按钮，打开 cmd 命令行窗口，在其中输入 ping 192.168.0.135，然后按 Enter 键，即可返回 Ping 到的数据信息，如图 3-29 所示。

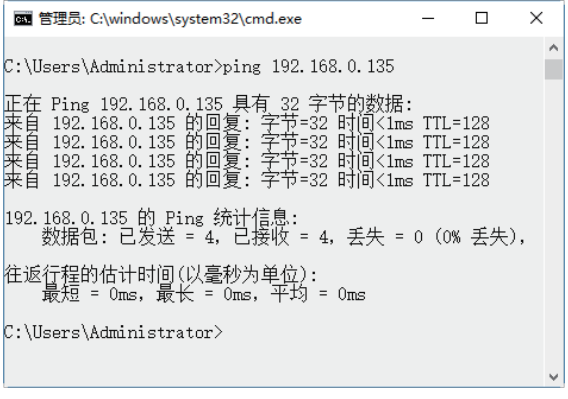


图 3-29　数据信息

分析上述操作代码结果，可以看到其返回 TTL 值为 128，说明该主机的操作系统是一个 Windows 操作系统。

3.3.3　侦察对方的网络结构


微视频

找到适合攻击的目标后，在正式实施入侵攻击之前，还需要了解目标主机的网络机构，只有弄清楚目标网络中防火墙、服务器地址之后，才可进行第一步入侵。可以使用 tracert 命令查看目标主机的网络结构。tracert 命令用来显示数据包到达目标主机所经过的路径并显示到达每个节点的时间。

tracert 命令的功能同 Ping 类似，但所获得的信息要比 Ping 命令详细得多，它把数据包所走的全部路径、节点的 IP 以及花费的时间都显示出来。该命令比较适用于大型网络。tracert 命令的格式：tracert IP 地址或主机名。

例如：要想了解自己的计算机与目标主机 www.baidu.com 之间的详细路径传递信息，就可以在“命令提示符”窗口中输入 tracert www.baidu.com 命令进行查看，进而分析目标主机的网络结构，如图 3-30 所示。

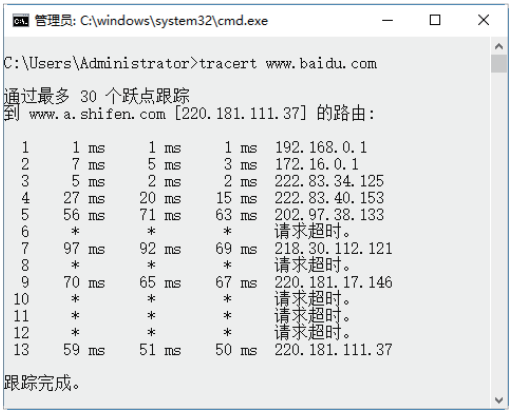


图 3-30　目标主机的网络结构

3.4　确定可能开放的端口服务

服务器上所开放的端口往往是黑客潜在的入侵通道，对目标主机进行端口扫描能够获得许多有用的信息，而进行端口扫描的方法也很多，既可以手工进行扫描，也可以用端口扫描软件进行扫描。黑客常用的端口扫描器有 ScanPort 扫描器、极速端口扫描器和 SuperScan 扫描器等。

3.4.1　ScanPort 扫描器


微视频

ScanPort 软件不但可以用于网络扫描，同时还可以探测指定 IP 及端口，速度比传统软件快，且支持用户自设 IP 端口又增加了其灵活性。具体的操作步骤如下。

Step 01 下载并运行 ScanPort 程序，即可打开 ScanPort 主窗口，在其中设置起始 IP 地址、结束 IP 地址以及要扫描的端口号，如图 3-31 所示。

Step 02 单击“扫描”按钮，即可进行扫描，从扫描结果中可以看出设置的 IP 地址段中计算机开启的端口，如图 3-32 所示。

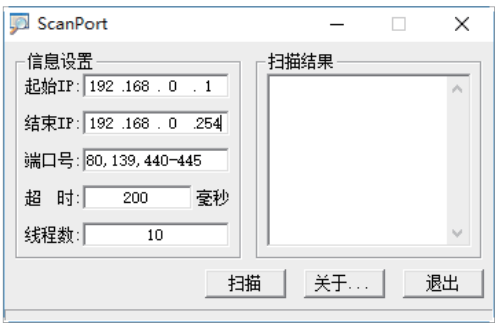


图 3-31　ScanPort 主窗口

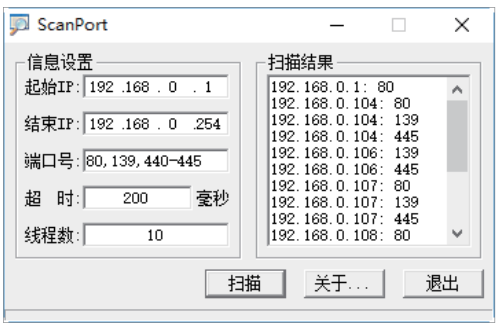


图 3-32　开始扫描

Step 03 如果要扫描某台计算机中开启的端口，则将起始 IP 和结束 IP 都设置为该主机的 IP 地址，如图 3-33 所示。

Step04 在设置完要扫描的端口号之后，单击“扫描”按钮，即可扫描出该主机中开启的端口（设置端口范围之内），如图 3-34 所示。

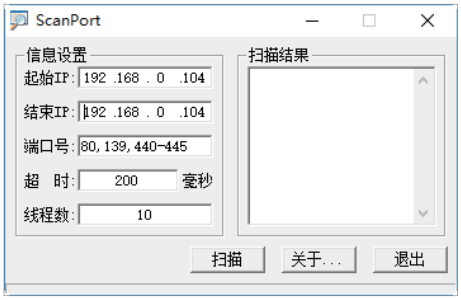


图 3-33 设置单一主机的 IP

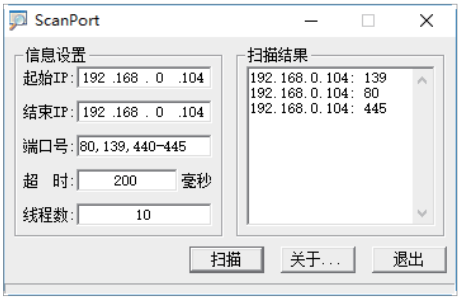


图 3-34 开始扫描单个主机的端口

微视频

3.4.2 极速端口扫描器

极速端口扫描器是一款专门扫描端口的工具，利用该工具既可以扫描端口，也可以实现在线更新 IP 地址，还可以将扫描结果导出为记事本、网页以及 XLS 格式。

使用该工具扫描端口的具体操作步骤如下。

Step01 下载并运行“极速端口扫描器 V2.0.500”，即可打开“极速端口扫描器”主窗口，如图 3-35 所示。

Step02 切换到“参数设置”选项，在其中即可看到该工具自带的 IP 地址段以及各种参数，如图 3-36 所示。

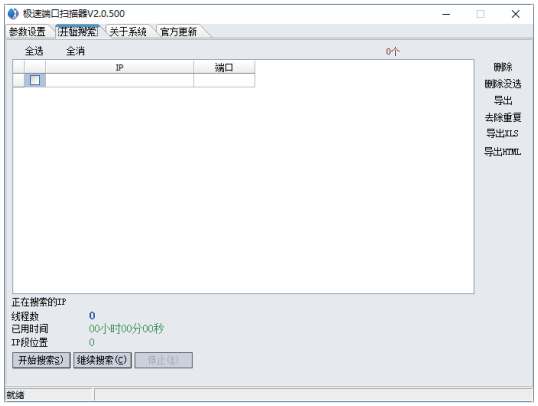


图 3-35 “极速端口扫描器”主窗口

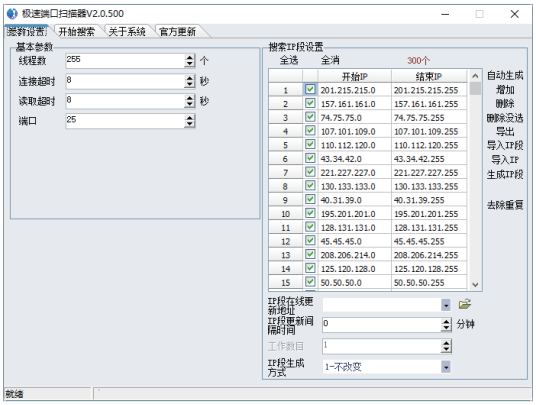


图 3-36 “参数设置”选项卡

Step03 如果要对目标主机进行扫描，则需添加指定的 IP 段。在“参数设置”选项卡中单击“增加”按钮，即可打开“IP 段编辑”对话框，如图 3-37 所示。

Step04 在“开始 IP”和“结束 IP”文本框中分别输入 IP 地址之后，单击“确定”按钮，即可将该 IP 段添加到“搜索 IP 段设置”列表中，如图 3-38 所示。

Step05 单击“全消”按钮，即可取消选择所有的 IP 段，然后勾选刚添加的 IP 段，并将要扫描的端口设置为 445，如图 3-39 所示。

Step06 设置完毕后，切换到“开始搜索”选项卡，并单击“开始搜索”按钮，即可扫描指定的 IP 段，最终的扫描结果如图 3-40 所示。

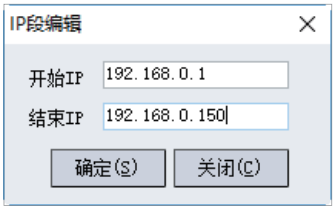


图 3-37　“IP 段编辑”对话框

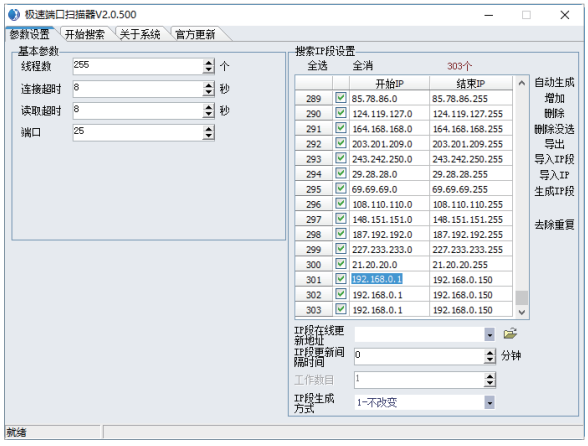


图 3-38　设置要扫描的 IP 段

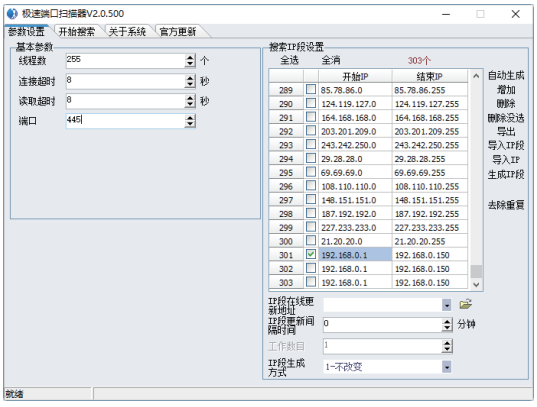


图 3-39　选择要扫描的 IP 段

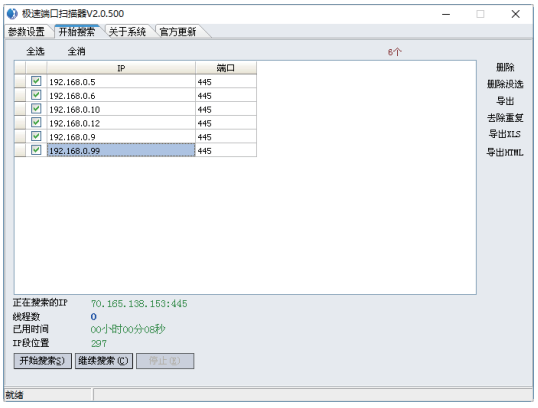


图 3-40　扫描指定的 IP 段

Step07 可以将扫描的结果保存为记事本、网页、XLS 等格式。在“开始搜索”选项卡中单击“导出”按钮，即可打开“另存为”对话框，如图 3-41 所示。

Step08 设置完保存名称和路径后，单击“保存”按钮，即可将扫描结果保存为记事本文件格式。打开保存的搜索结果，在其中即可看到搜索到的 IP 地址以及搜索的端口，如图 3-42 所示。

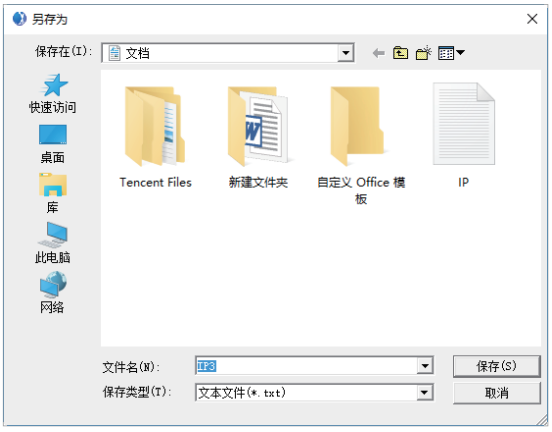


图 3-41　“另存为”对话框

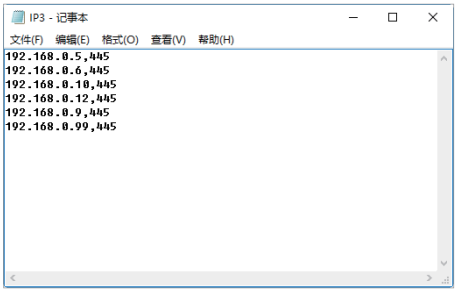


图 3-42　记事本文件


微视频

3.4.3 SuperScan 扫描器

SuperScan 是功能强大的端口扫描工具，可以扫描局域网内所有的活动主机或某一台主机所开放的端口。具体的操作步骤如下。

Step01 在“命令提示符”窗口中输入 netstat -a -n 命令，按 Enter 键即可查看本机中开启的端口，在运行结果中可以看到以数字形式显示的 TCP 和 UDP 连接的端口号及其状态，如图 3-43 所示。

Step02 启动 SuperScan 程序，然后切换到“主机和服务器扫描设置”选项卡，在其中对想要扫描的 UDP 和 TCP 端口进行设置，如图 3-44 所示。

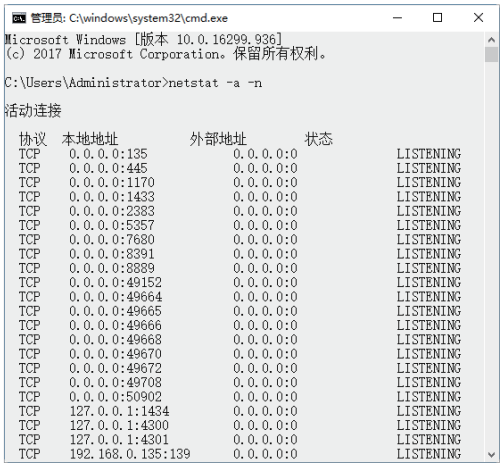


图 3-43 netstat -a -n 命令

图 3-44 设置 UDP 和 TCP 端口

Step03 切换到“扫描”选项卡，在其中输入目标开始 IP 地址和结束 IP 地址，如图 3-45 所示。

Step04 单击 按钮，即可开始扫描地址，在扫描进程结束之后，SuperScan 将提供一个主机列表，用于显示每台扫描过的主机被发现的开放端口信息，如图 3-46 所示。

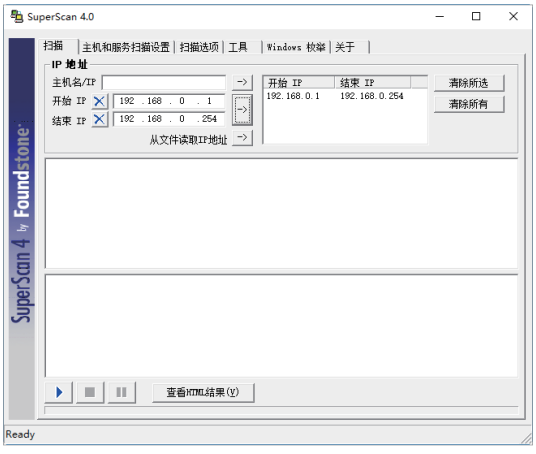


图 3-45 设置 IP 地址段

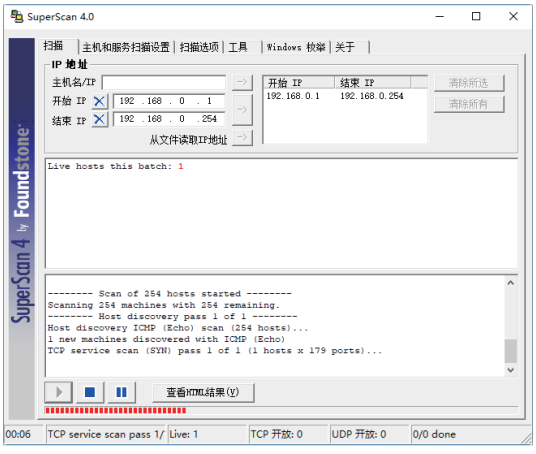
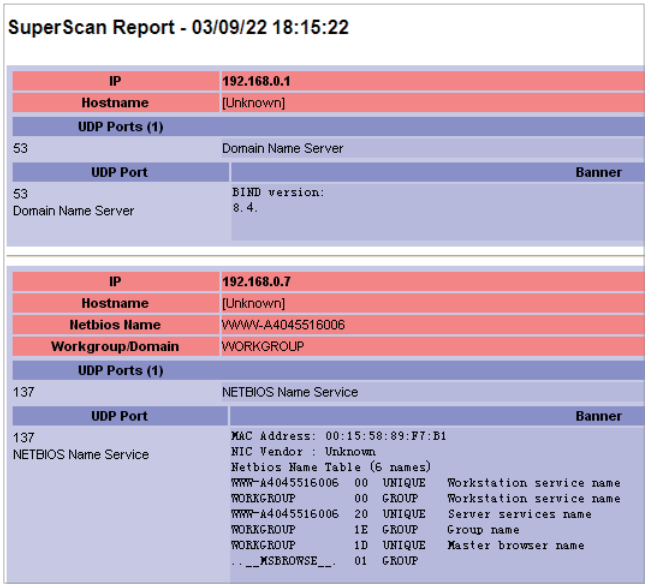


图 3-46 扫描开放端口信息

Step05 SuperScan 还有选择以 HTML 格式显示信息的功能。单击“查看 HTML 结果”按钮，即可显示扫描了哪些主机和在每台主机上哪些端口是开放的，并生成一份 HTML 格式的报告，如图 3-47 所示。



SuperScan Report - 03/09/22 18:15:22

IP	192.168.0.1
Hostname	[Unknown]
UDP Ports (1)	
53	Domain Name Server

UDP Port	Banner
53 Domain Name Server	BIND version: 8.4.

IP	192.168.0.7
Hostname	[Unknown]
Netbios Name	WWW-A4045516006
Workgroup/Domain	WORKGROUP
UDP Ports (1)	
137	NETBIOS Name Service

UDP Port	Banner
137 NETBIOS Name Service	MAC Address: 00:15:58:89:F7:B1 NIC Vendor : Unknown Netbios Name Table (6 names) WWW-A4045516006 00 UNIQUE Workstation service name WORKGROUP 00 GROUP Workstation service name WWW-A4045516006 20 UNIQUE Server services name WORKGROUP 1E GROUP Group name WORKGROUP 1D UNIQUE Master browser name ..__MSBROWSE__. 01 GROUP

图 3-47　HTML 格式的报告

3.4.4　流光扫描器

微视频

利用流光扫描器可以轻松探测目标主机的开放端口，下面将以探测 POP3 主机的开放端口为例进行介绍。

Step01 单击桌面上的流光扫描器程序图标，启动流光扫描器，如图 3-48 所示。

Step02 单击“选项”→“系统设置”命令，打开“系统设置”对话框，对优先级、线程数、单词数 / 线程及扫描端口进行设置，如图 3-49 所示。

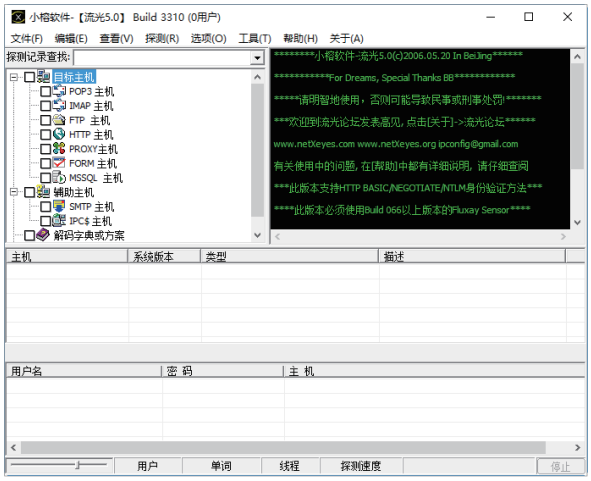


图 3-48　流光扫描器

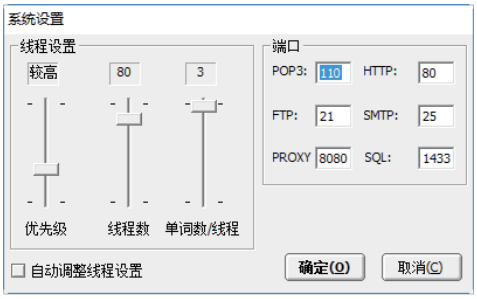


图 3-49　“系统设置”对话框

Step03 在扫描器主窗口中勾选“HTTP 主机”复选框，然后右击，在弹出的快捷菜单中选择“编辑”→“添加”命令，如图 3-50 所示。

Step04 打开“添加主机（HTTP）”对话框，在该对话框的下拉列表框中输入要扫描主机的 IP 地址（这里以 192.168.0.105）为例），如图 3-51 所示。

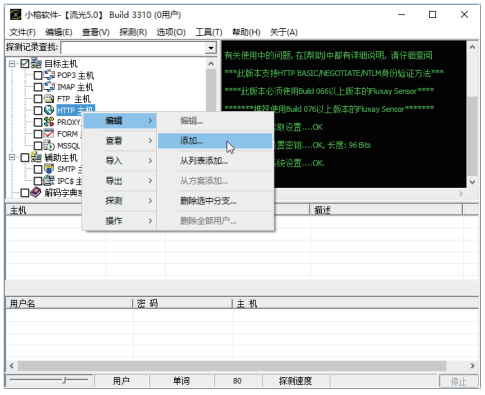


图 3-50 “添加”命令

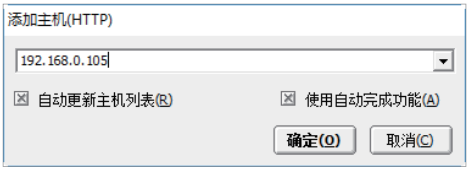


图 3-51 输入要扫描主机的 IP 地址

Step05 此时在主窗口中将显示出刚刚添加的 HTTP 主机，右击此主机，在弹出的快捷菜单中依次选择“探测”→“扫描主机端口”命令，如图 3-52 所示。

Step06 打开“端口探测设置”对话框，勾选“自定义端口探测范围”复选框，然后在“范围”选项区中设置要探测端口的范围，如图 3-53 所示。

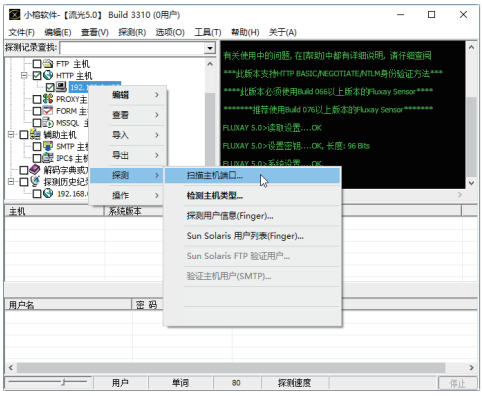


图 3-52 “扫描主机端口”命令

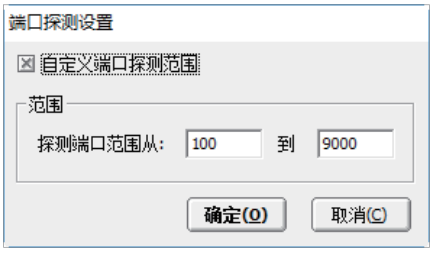


图 3-53 设置要探测端口的范围

Step07 设置完成后，单击“确定”按钮，开始探测目标主机的开放端口，如图 3-54 所示。

Step08 扫描完毕后，将会自动弹出“探测结果”对话框，如果目标主机存在开放端口，就会在该对话框中显示出来，如图 3-55 所示。

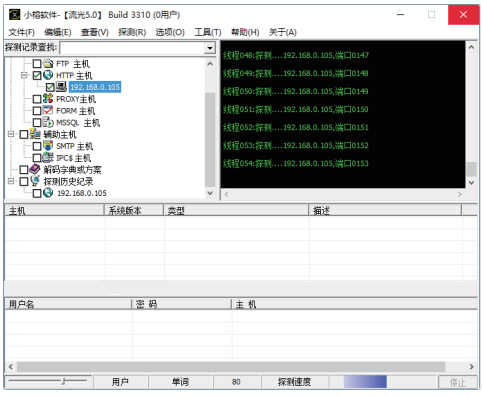


图 3-54 探测目标主机的开放端口

图 3-55 “探测结果”对话框

3.5　实战演练

3.5.1　实战 1：开启计算机 CPU 最强性能

微视频

在 Windows 10 操作系统之中，用户设置系统启动密码，具体的操作步骤如下。

Step01 按 WIN+R 组合键，打开“运行”对话框，在“打开”文本框中输入 msconfig，如图 3-56 所示。

Step02 单击“确定”按钮，在弹出的对话框中选择“引导”选项卡，如图 3-57 所示。

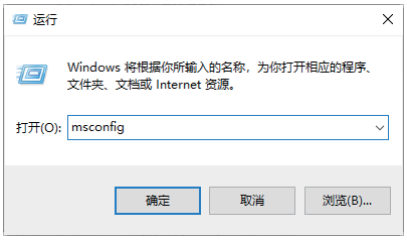


图 3-56　“运行”对话框

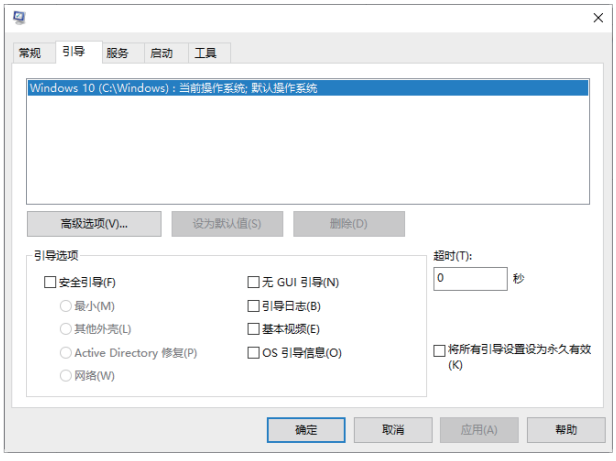


图 3-57　“引导”选项卡

Step03 单击“高级选项”按钮，弹出“引导高级选项”对话框，勾选“处理器个数”复选框，将处理器个数设置为最大值，本机最大值为 4，如图 3-58 所示。

Step04 单击“确定”按钮，弹出“系统配置”对话框，单击“重新启动”按钮，重启计算机，CPU 就能达到最大性能，这样计算机的运行速度就会明显提高，如图 3-59 所示。

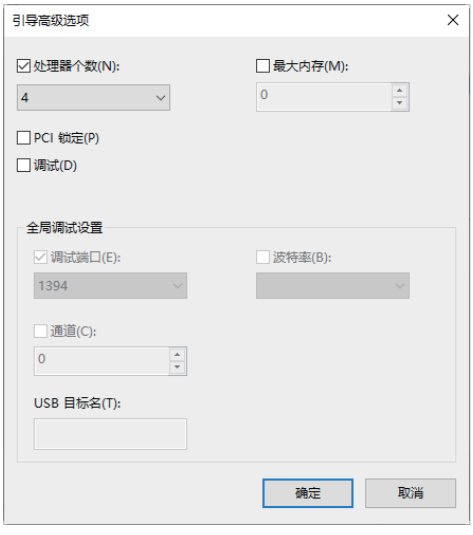


图 3-58　“引导高级选项”对话框

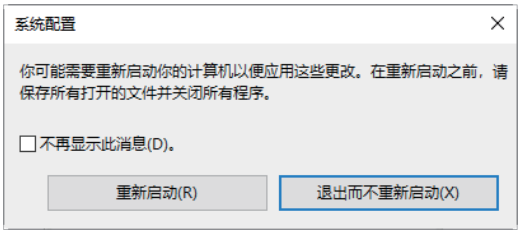


图 3-59　“系统配置”对话框


微视频

3.5.2 实战 2：阻止流氓软件自动运行

在使用计算机时，可能会遇到流氓软件，如果不想程序自动运行，这时就需要用户阻止程序运行。具体的操作步骤如下。

Step01 按 WIN+R 组合键，在打开的“运行”对话框中输入 gpedit.msc，如图 3-60 所示。

Step02 单击“确定”按钮，打开“本地组策略编辑器”窗口，如图 3-61 所示。

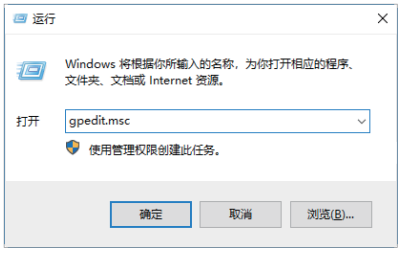


图 3-60 “运行”对话框

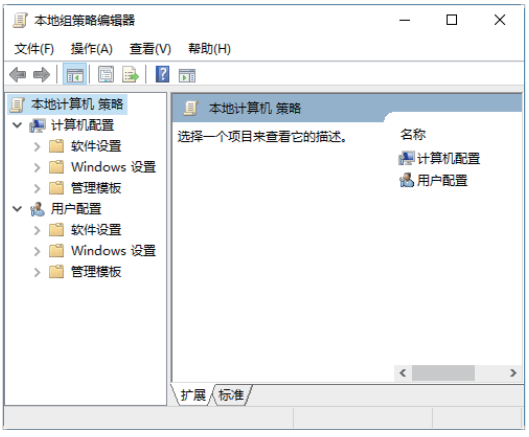


图 3-61 “本地组策略编辑器”窗口

Step03 依次展开“用户配置”→“管理模板”→“系统”文件，双击“不运行指定的 Windows 应用程序”选项，如图 3-62 所示。

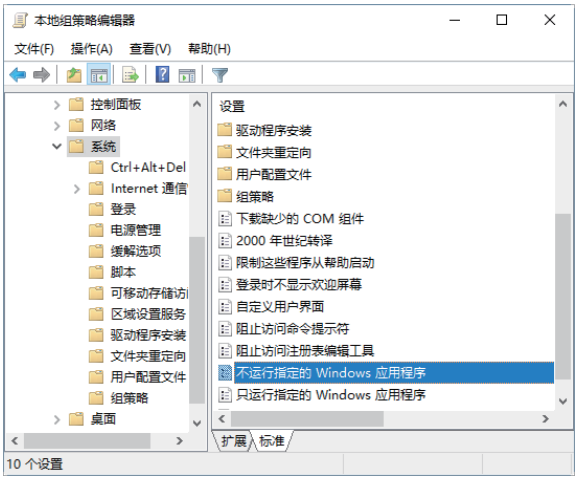


图 3-62 “系统”设置界面

Step04 打开“不运行指定的 Windows 应用程序”窗口，选中“已启用”单选按钮，如图 3-63 所示。

Step05 单击下方的“显示…”按钮，打开“显示内容”窗口，在其中添加不允许的应用程序，如图 3-64 所示。

Step06 单击“确定”按钮，即可把想要阻止的程序名添加进去，此时，如果再运行此程序，就会弹出相应的限制信息提示框了，如图 3-65 所示。

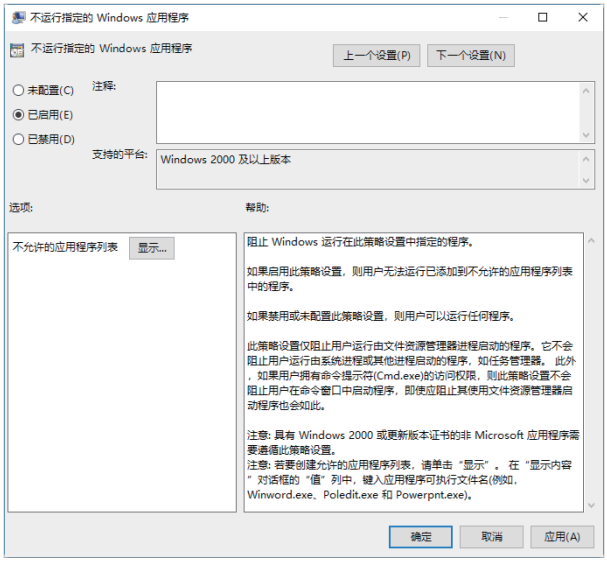


图 3-63　选择“已启用”单选按钮

图 3-64　“显示内容”窗口

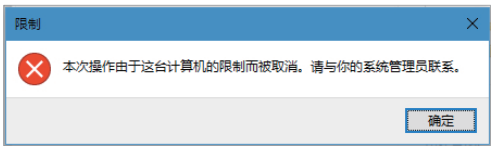


图 3-65　限制信息提示框