第1章　计算机安全快速入门

作为计算机或网络终端设备的用户，要想使自己的设备不受或少受黑客的攻击，就需要了解一些黑客常用的入侵技能及学习一些计算机安全方面的知识。本章主要内容包括IP地址、MAC地址、端口及黑客常用DOS命令的应用等。

1.1　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，找到目标主机的IP地址是黑客实施入侵攻击的一个关键。

1.1.1　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等5类，其中A、B、C类是3种主要的类型地址，D类用于组播网络，E类用于扩展备用地址。

- A类IP地址。一个A类IP地址由1个字节的网络地址和3个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）的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，在互联网中计算机才能相互访问。

- 子网掩码：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：默认网关意为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：DNS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，在一定程度上就实现了黑客入侵的前提工作。使用ipconfig命令可以获取本地计算机的IP地址和物理地址，具体的操作步骤如下。

Step 01 右击“⊞”按钮，在弹出的快捷菜单中选择“运行”选项，如图1-1所示。

图 1-1 “运行”选项

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1-2所示。

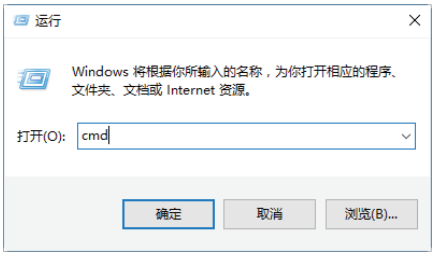

图 1-2 输入 cmd 命令

Step 03 单击“确定”按钮，打开“命令提示符”窗口，在其中输入ipconfig命令，按Enter键即可显示出本机的IP配置相关信息，如图1-3所示。

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。

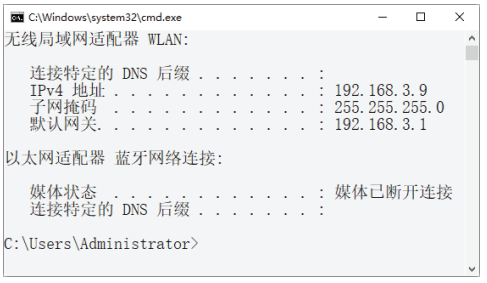

图 1-3 查看 IP 地址

1.1.2 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，由网络设备制造商在生产时写在硬件内部。MAC地址与网络无关，也就是说无论将带有这个地址的硬件（如网卡、集线器、路由器等）接入网络的何处，MAC地址都是相同的，它由厂商写在网卡的BIOS里。

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其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，能够具体标识。这两种地址均有各自的长处，使用时也因条件不同而采用不同的地址。

2. 查看MAC地址

在“命令提示符”窗口中输入ipconfig/all命令，然后按Enter键，可以在显示的结果中看到一个物理地址：00-23-24-DA-43-8B，这就是用户自己的计算机的网卡地址，它是唯一的，如图1-4所示。

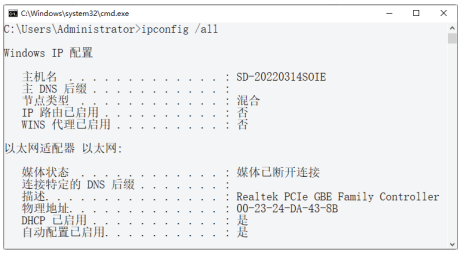

图 1-4　查看 MAC 地址

1.2　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（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）。

1.2.1　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1-5所示。

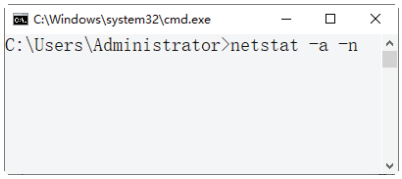

图 1-5　输入 netstat -a -n 命令

Step 02 按Enter键，可看到以数字显示的TCP和UDP连接的端口号及其状态，如图1-6所示。

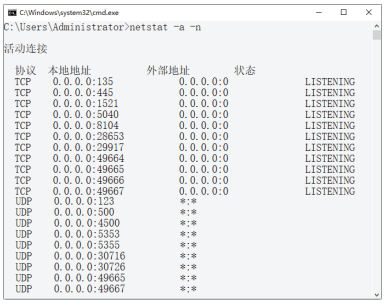

图 1-6　TCP 和 UDP 连接的端口号

1.2.2　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“⊞”按钮，在弹出的快捷菜单中选择“控制面板”选项，如图1-7所示。

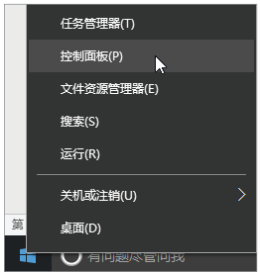

图 1-7　“控制面板”选项

Step 02 打开“控制面板”窗口，双击“管理工具”图标，如图1-8所示。

图 1-8　“控制面板”窗口

Step 03 打开“管理工具”窗口，双击“服务”图标，如图1-9所示。

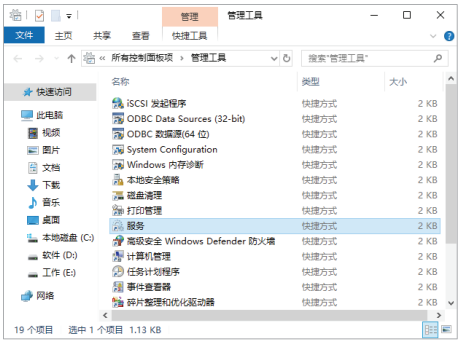

图 1-9 “服务”图标

Step 04 打开“服务”窗口，找到WebClient服务项，如图1-10所示。

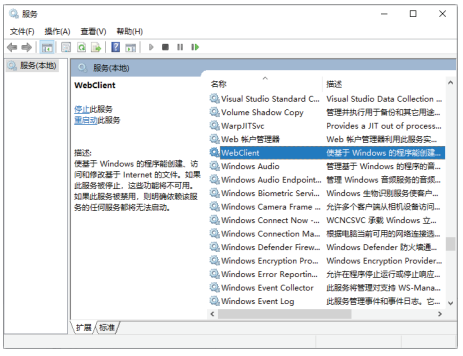

图 1-10 “服务”窗口

Step 05 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1-11所示。

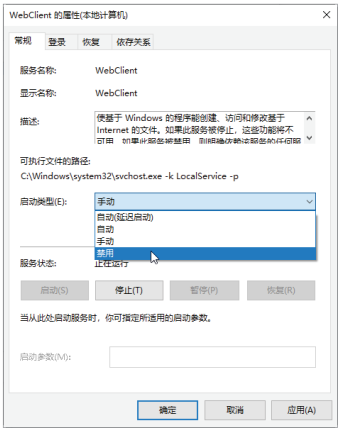

图 1-11 选择“禁用”选项

1.2.3 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。

Step 01 这里以上述停止的WebClient服务端口为例。在“WebClient的属性”对话框中单击“启动类型”右侧的下拉按钮，在弹出的下拉菜单中选择“自动”，如图1-12所示。

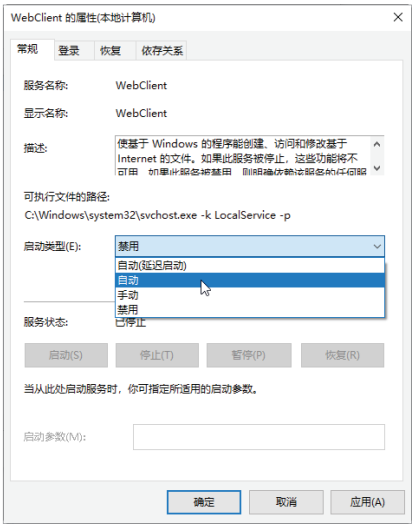

图 1-12 选择“自动”选项

Step 02 单击“应用”按钮，激活“服务状态”下的“启动”按钮，如图1-13所示。

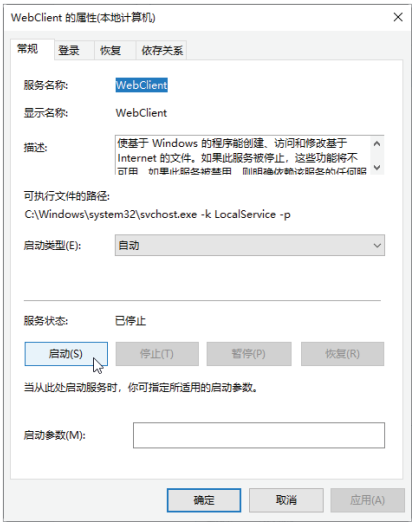

图 1-13 选择“启动”按钮

Step 03 单击“启动”按钮，即可启动该项服务，再次单击“应用”按钮，在“WebClient的属性”对话框中可以看到该服务的“服务状态”已经变为“正在运行”，如图1-14所示。

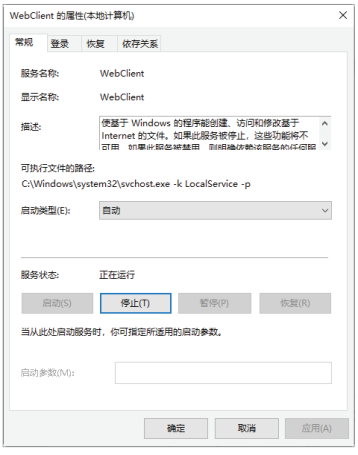

图 1-14　启动服务项

Step 04 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1-15所示。

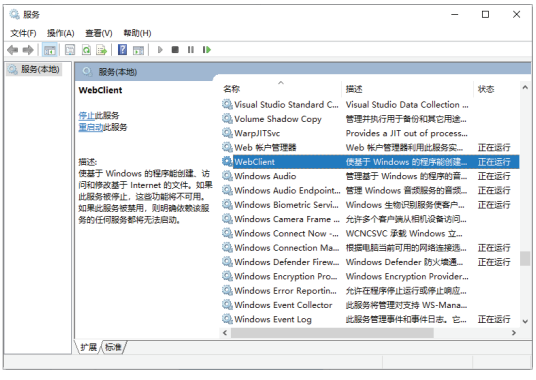

图 1-15　WebClient 服务的状态为“正在运行”

1.3　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。了解这些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。

1.3.1　cd命令

cd（Change Directory）命令的作用是改变当前目录，该命令用于切换路径目录。cd命令主要有以下3种使用方法。

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

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

（3）cd\：表示当前无论在哪个子目录下，通过该命令可立即返回根目录下。

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

Step 01 在“命令提示符”窗口中输入cd c:\命令，按Enter键即可将目录切换为C:\，如图1-16所示。

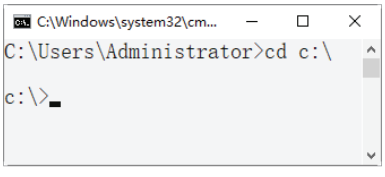

图 1-16　目录切换到 C

Step 02 如果想进入C:\Windows\system32目录中，则需在上面的“命令提示符”窗口中输入cd Windows\system32命令，按Enter键即可将目录切换为C:\Windows\system32，如图1-17所示。

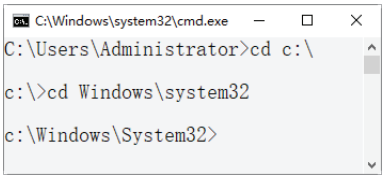

图 1-17　切换到 C 盘子目录

Step 03 如果想返回上一级目录，可以在“命

令提示符”窗口中输入cd..命令，按Enter键即可，如图1-18所示。

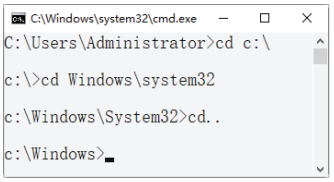

图 1-18　返回上一级目录

Step 04 如果想返回根目录，可以在“命令提示符”窗口中输入cd\命令，按Enter键即可，如图1-19所示。

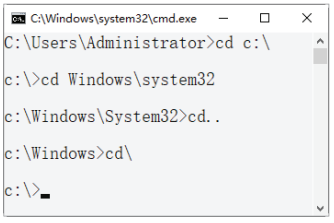

图 1-19　返回根目录

1.3.2　dir命令

dir命令的作用是列出磁盘上所有的或指定的文件目录，可以显示的内容包含卷标、文件名、文件大小、文件建立日期和时间、目录名、磁盘剩余空间等。dir命令的格式如下。

```
dir [盘符][路径][文件名][/P][/W][/A:属性]
```

其中各个参数的作用如下。

（1）/P：当显示的信息超过一屏时暂停显示，直至按任意键才继续显示。

（2）/W：以横向排列的形式显示文件名和目录名，每行5个（不显示文件大小、建立日期和时间）。

（3）/A:属性：仅显示指定属性的文件，无此参数时，dir显示除系统和隐含文件外的所有文件。可指定为以下几种形式。

① /a:s，显示系统文件的信息。

② /a:h，显示隐含文件的信息。

③ /a:r，显示只读文件的信息。

④ /a:a，显示归档文件的信息。

⑤ /a:d，显示目录信息。

使用dir命令查看磁盘中的资源，具体的操作步骤如下。

Step 01 在“命令提示符”窗口中输入dir命令，按Enter键即可查看当前目录下的文件列表，如图1-20所示。

图 1-20　Administrator 目录下的文件列表

Step 02 在“命令提示符”窗口中输入dir d:/a:d命令，按Enter键即可查看D盘下的所有文件的目录，如图1-21所示。

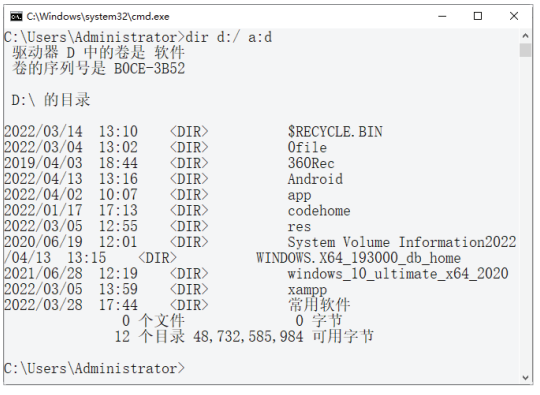

图 1-21　D 盘下的文件列表

Step 03 在“命令提示符”窗口中输入dir c:\windows /a:h命令，按Enter键即可列出c:\windows目录下的隐藏文件，如图1-22所示。

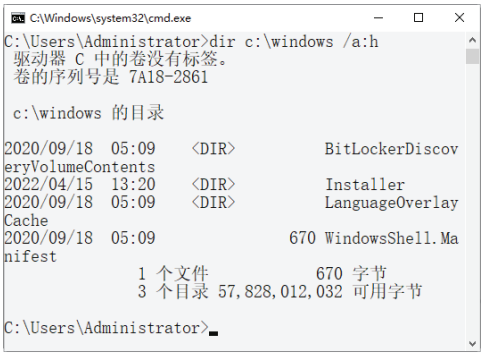

图 1-22　C 盘下的隐藏文件

1.3.3　ping命令

ping命令是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1-23所示。

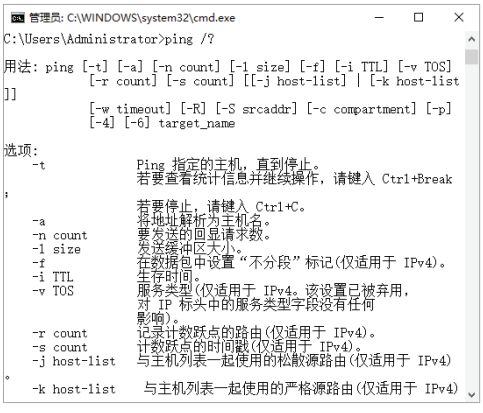

图 1-23　ping 命令帮助信息

使用ping命令对计算机的连接状态进行测试的具体操作步骤如下。

Step 01 使用ping命令来判断计算机的操作系统类型。在“命令提示符”窗口中输入ping 192.168.3.9命令，运行结果如图1-24所示。

Step 02 在“命令提示符”窗口中输入ping 192.168.3.9 -t -l 128命令，可以不断向某台主机发出大量的数据包，如图1-25所示。

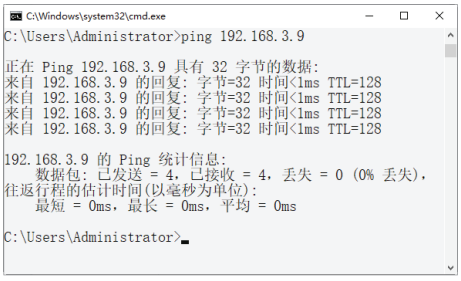

图 1-24　判断计算机的操作系统类型

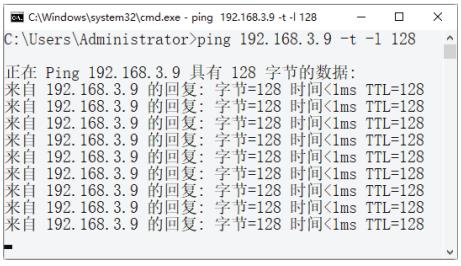

图 1-25　发出大量数据包

Step 03 判断本台计算机是否与外界网络连通。在“命令提示符”窗口中输入ping www.baidu.com命令，其运行结果如图1-26所示，图中说明本台计算机与外界网络连通。

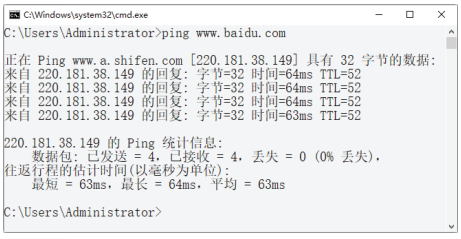

图 1-26　网络连通信息

Step 04 解析某IP地址的计算机名。在“命令提示符”窗口中输入ping -a 192.168.3.9命令，其运行结果如图1-27所示，可知这台主机的名称为SD-20220314SOIE。

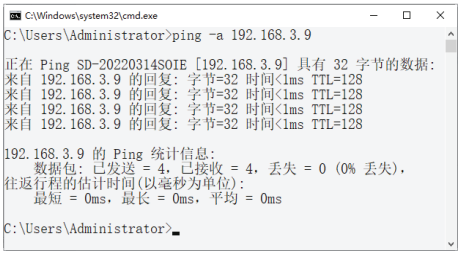

图 1-27　解析某 IP 地址的计算机名

1.3.4 net命令

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

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

查询本台计算机开启哪些Windows服务的具体操作步骤如下：

Step 01 使用net命令查看网络状态。打开“命令提示符”窗口，输入net start命令，如图1-28所示。

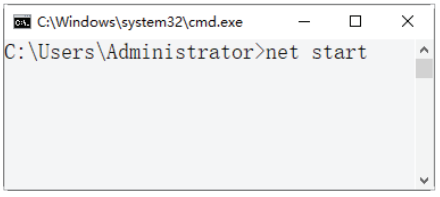

图 1-28　输入 net start 命令

Step 02 按Enter键，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1-29所示。

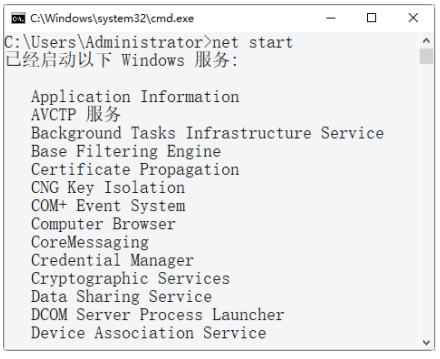

图 1-29　计算机所启动的 Windows 服务

1.3.5 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1-30所示。

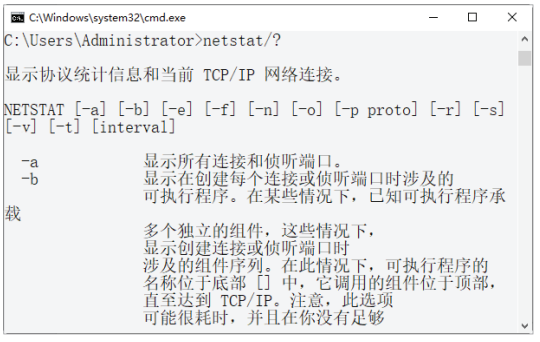

图 1-30　netstat 命令帮助信息

该命令的语法格式信息如下：

```
    NETSTAT [-a] [-b] [-e] [-n] [-o] [-p
proto] [-r] [-s] [-v] [-t] [interval]
```

其中比较重要的参数的含义如下。

- -a：显示所有连接和监听端口。
- -n：以数字形式显示地址和端口号。

使用netstat命令查看网络连接的具体操作步骤如下。

Step 01 打开“命令提示符”窗口，在其中输入netstat -n或netstat命令，按Enter键即可查看服务器活动的TCP/IP连接，如图1-31所示。

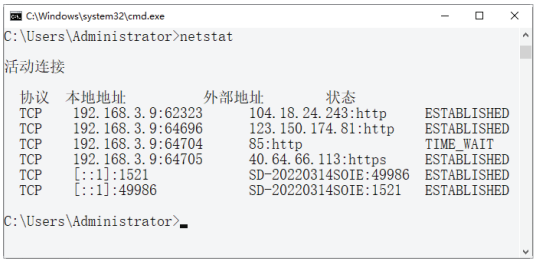

图 1-31　服务器活动的 TCP/IP 连接

Step 02 在“命令提示符”窗口中输入netstat -r命令，按Enter键即可查看本机的路由信息，如图1-32所示。

Step 03 在“命令提示符”窗口中输入netstat -a命令，按Enter键即可查看本机所有活动的TCP连接，如图1-33所示。

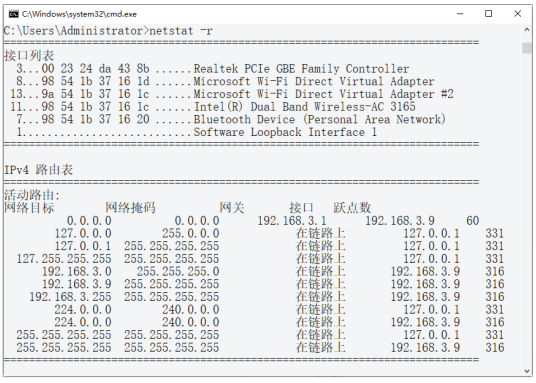

图 1-32　查看本机的路由信息

图 1-33　查看本机活动的 TCP 连接

Step 04 在“命令提示符”窗口中输入netstat -n -a命令，按Enter键即可显示本机所有连接的端口及其状态，如图1-34所示。

图 1-34　查看本机所有连接的端口及其状态

1.3.6　tracert命令

使用tracert命令可以查看网络中路由节点信息，最常见的使用方法是在tracert命令后追加一个参数，表示检测和查看连接当前主机经历了哪些路由节点，适合用于大型网络的测试，该命令的语法格式信息如下。

```
    tracert [-d] [-h MaximumHops] [-j
Hostlist] [-w Timeout] [TargetName]
```

其中各个参数的含义如下。

- -d：防止解析目标主机的名字，可以加速显示tracert命令结果。
- -h MaximumHops：指定搜索到目标地址的最大跳跃数，默认为30个跳跃点。
- -j Hostlist：按照主机列表中的地址释放源路由。
- -w Timeout：指定超时时间间隔，默认单位为毫秒。
- TargetName：指定目标计算机。

例如：如果想查看www.baidu.com的路由与局域网络连接情况，则在“命令提示符”窗口中输入tracert www.baidu.com命令，按Enter键，其显示结果如图1-35所示。

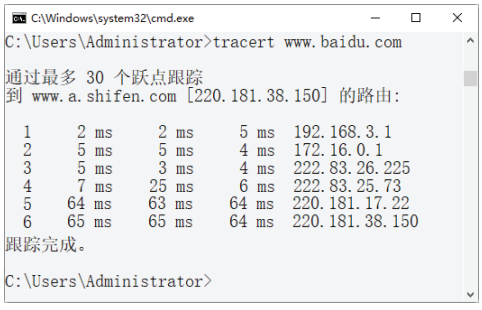

图 1-35　查看网络中路由节点信息

1.3.7　Tasklist命令

Tasklist命令用来显示运行在本地或远程计算机上的所有进程，带有多个执行参数。Tasklist命令的格式如下。

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

其中各个参数的作用如下：

- /S system：指定连接到的远程系统。
- /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，有效值为TABLE、LIST、CSV。
- /NH：指定输出中不显示栏目标题。只对TABLE和CSV格式有效。

利用Tasklist命令可以查看本机中的进程，还查看每个进程提供的服务。下面将介绍使用Tasklist命令的具体操作步骤。

Step 01 在“命令提示符”窗口中输入Tasklist命令，按Enter键即可显示本机的所有进程，如图1-36所示。在显示结果中可以看到映像名称、PID、会话名、会话#和内存使用5部分。

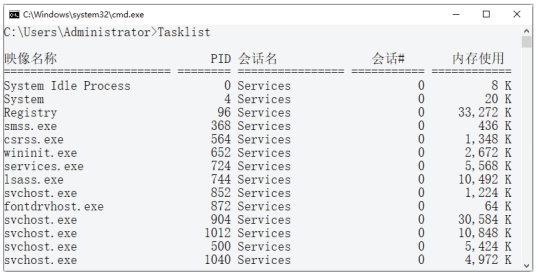

图 1-36　查看本机进程

Step 02 Tasklist命令不但可以查看系统进程，而且还可以查看每个进程提供的服务。例如查看本机进程svchost.exe提供的服务，在“命令提示符”窗口中输入Tasklist /svc命令即可，如图1-37所示。

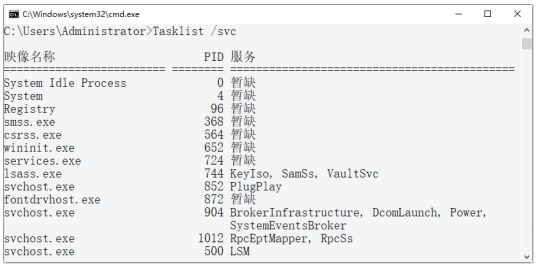

图 1-37　查看本机进程 svchost.exe 提供的服务

Step 03 要查看本地系统中哪些进程调用了shell32.dll模块文件，只需在“命令提示符”窗口中输入Tasklist /m shell32.dll命令，即可显示这些进程的列表，如图1-38所示。

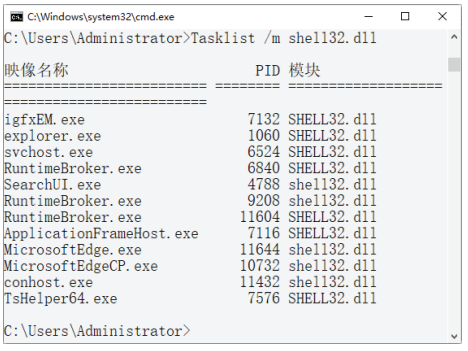

图 1-38　显示调用 shell32.dll 模块的进程

Step 04 使用筛选器可以查找指定的进程，在“命令提示符”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1-39所示。其中/FI为筛选器参数，ne和eq为关系运算符“不相等”和“相等”。

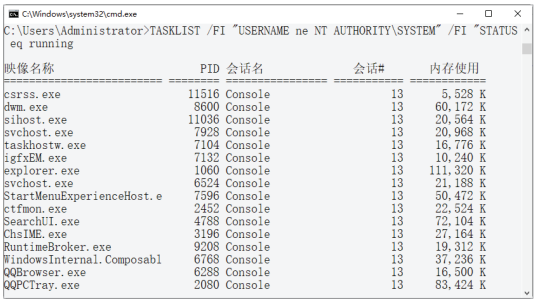

图 1-39　列出系统中正在运行的非 SYSTEM 状态的所有进程

1.4　实战演练

1.4.1　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“⊞”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1-40所示。

图 1-40　“命令提示符”窗口

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1-41所示。

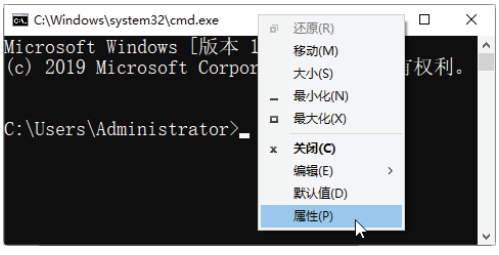

图 1-41　“属性”选项

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1-42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1-43所示。

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1-44所示。

图 1-42　设置屏幕背景

图 1-43　设置屏幕文字

图 1-44　以白底黑字样式显示命令提示符窗口

1.4.2　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。

Step 01 在“命令提示符”窗口中输入shutdown/s /t 40命令，如图1-45所示。

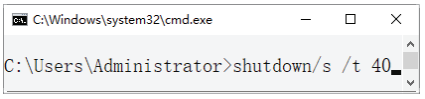

图 1-45　输入 shutdown/s /t 40 命令

Step 02 弹出一个即将注销用户登录的信息提示框，这样计算机就会在规定的时间内关机，如图1-46所示。

Step 03 如果此时想取消关机操作，可在“命令提示符”窗口中输入shutdown /a命令后按Enter键，桌面右下角出现如图1-47所示的弹窗，表示取消成功。

图 1-46　信息提示框

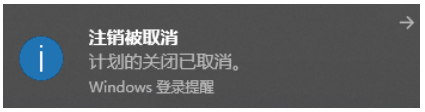

图 1-47　取消关机操作

第2章　常用扫描与嗅探工具

要想成为一名黑客，常用的扫描与嗅探工具当然是不可缺少的。网络扫描与嗅探是黑客进行攻击之前的第一步，也是必备的操作武器。本章就来介绍常用扫描与嗅探工具的使用。

2.1　常见端口扫描器工具

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。黑客常用的端口扫描器有ScanPort扫描器、极速端口扫描器、Nmap扫描器等。

2.1.1　ScanPort扫描器

ScanPort软件不但可以用于网络扫描，同时还可以用于探测指定IP及端口，速度比传统软件快，且支持用户自设IP端口又提高了其灵活性。具体的使用方法如下。

Step 01 下载并运行ScanPort程序，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2-1所示。

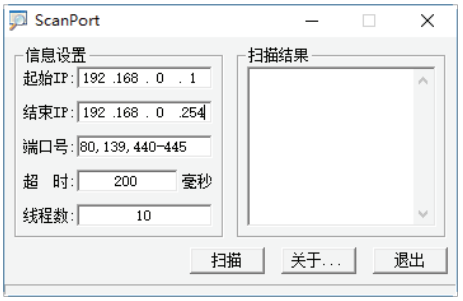

图 2-1　ScanPort 主窗口

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2-2所示。

Step 03 如果扫描某台计算机中开启的端口，则将开始IP和结束IP都设置为该主机的IP地址，如图2-3所示。

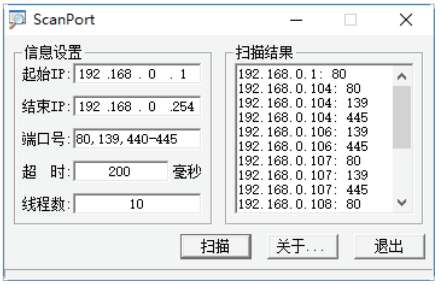

图 2-2　开始扫描

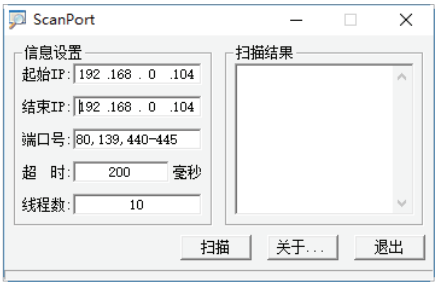

图 2-3　设置单一主机的 IP

Step 04 在设置完要扫描的端口号之后，单击“扫描”按钮，可扫描出该主机中开启的端口（设置端口范围之内），如图2-4所示。

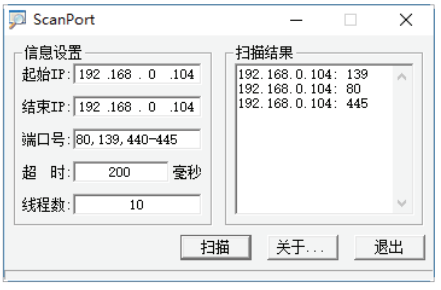

图 2-4　开始扫描单个主机的端口

2.1.2 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，利用该工具不仅可以扫描端口，还可以实现在线更新IP地址，另外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。

Step 01 下载并运行“极速端口扫描器V2.0.500”，打开“极速端口扫描器”主窗口，如图2-5所示。

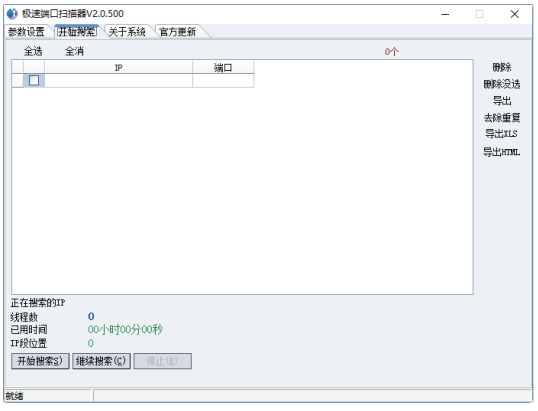

图 2-5 “极速端口扫描器”主窗口

Step 02 切换到“参数设置”选项卡下，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2-6所示。

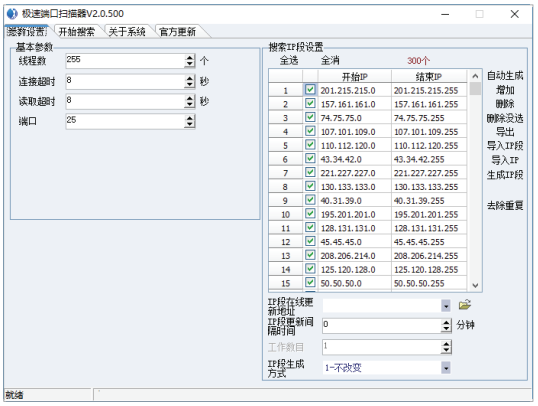

图 2-6 “参数设置”选项卡

Step 03 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”选项卡下单击“增加”按钮，打开“IP段编辑”对话框，如图2-7所示。

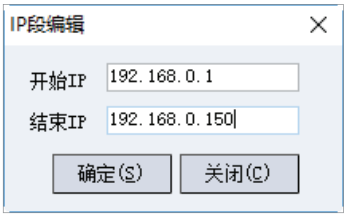

图 2-7 “IP 段编辑”对话框

Step 04 在“开始IP”和“结束IP”文本框中分别输入起始IP地址之后，单击“确定”按钮，可将该IP段添加到“搜索IP段设置”列表中，如图2-8所示。

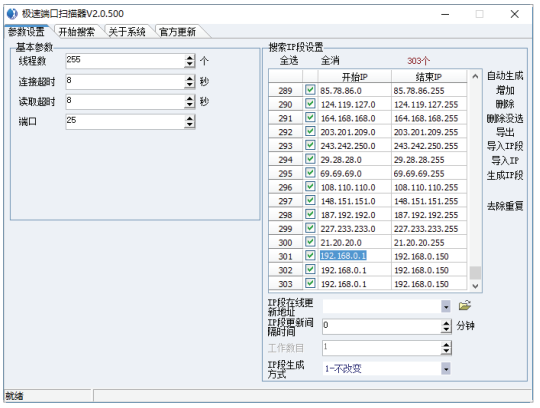

图 2-8 设置扫描 IP 段

Step 05 单击“全消”按钮，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2-9所示。

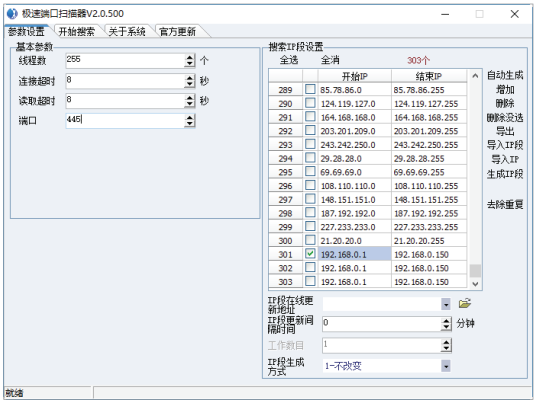

图 2-9 选择要扫描的 IP 段

Step 06 设置完毕后，切换到“开始搜索”选

项卡下，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2-10所示。

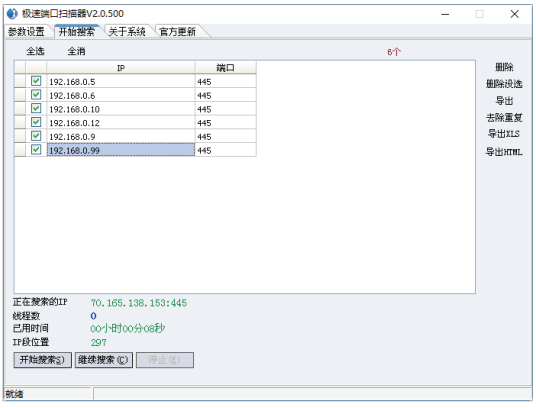

图 2-10　扫描指定的 IP 段

Step 07 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”选项卡下，单击“导出”按钮，打开“另存为”对话框，如图2-11所示。

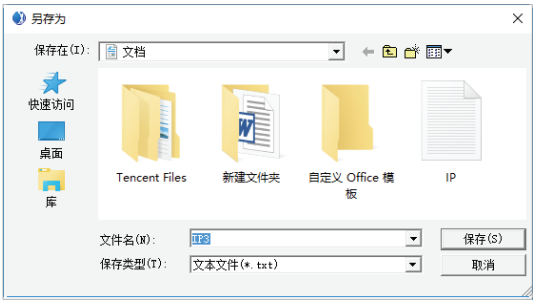

图 2-11　“另存为”对话框

Step 08 在设置完保存名称和路径后，单击“保存”按钮，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2-12所示。

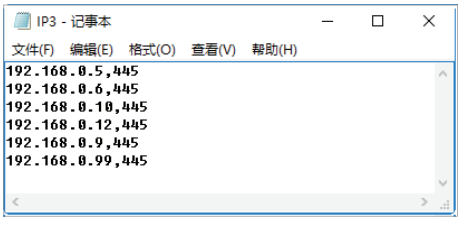

图 2-12　记事本文件

2.1.3　Nmap扫描器

Nmap扫描器是一款针对大型网络的端口扫描工具，包含多种扫描类型。它对网络中被检测到的主机按照选择的扫描选项和显示节点进行探查。用户可以建立一个需要扫描的范围，这样就不需要再输入大量的IP地址和主机名了。

使用Nmap进行扫描的具体操作方法如下。

Step 01 在桌面上双击Nmap程序图标，打开Nmap操作界面，如图2-13所示。

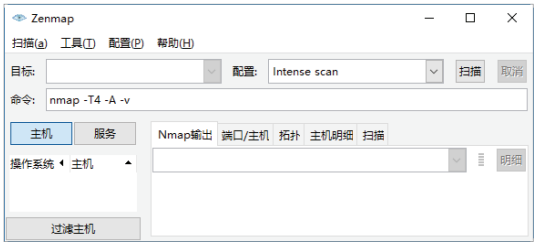

图 2-13　Nmap 操作界面

Step 02 要扫描单台主机，可以在“目标”后的文本框内输入主机的IP地址或网址，要扫描某个范围内的主机，可以在该文本框中输入192.168.0.1-150，如图2-14所示。

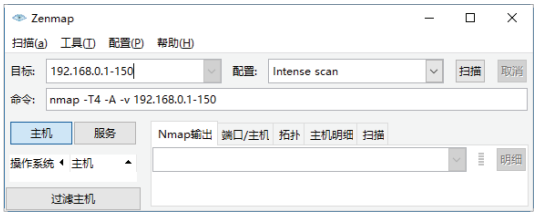

图 2-14　输入主机的 IP 地址

提示：在扫描时，还可以用“*”替换掉IP地址中的任何一部分，如192.168.1.*等同于192.168.1.1-255；要扫描一个更大范围内的主机，可以输入192.168.1，2，3.*，此时将扫描192.168.1.0、192.168.2.0、192.168.3.0三个网络中的所有地址。

Step 03 要设置网络扫描的不同配置文件，可以单击“配置”后的下拉列表框，从中选择Intense scan、Intense scan plus UDP、Intense scan，all TCP ports等选项，从而对网络主

机进行不同方面的扫描，如图2-15所示。

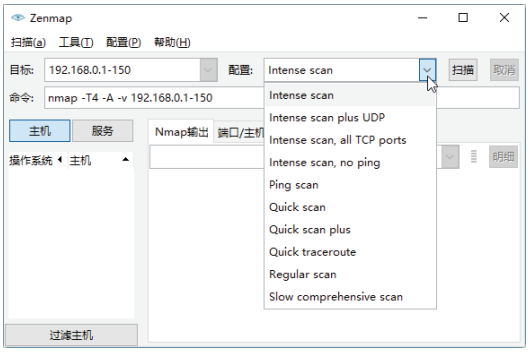

图 2-15　选择配置文件

Step 04 单击“扫描”按钮开始扫描，稍等一会儿即可在“Nmap输出”选项卡中显示扫描结果信息。在扫描结果信息中，可以看到扫描对象当前开放的端口，如图2-16所示。

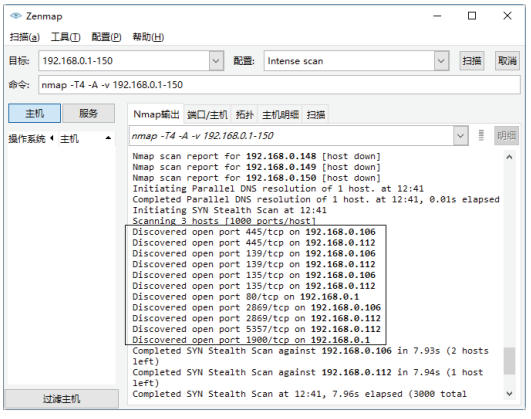

图 2-16　显示扫描结果信息

Step 05 选择“端口/主机”选项卡，在打开的界面中可以看到当前主机显示的端口、协议、状态和服务等信息，如图2-17所示。

图 2-17　“端口 / 主机”选项卡

Step 06 选择“拓扑”选项卡，在打开的界面中可以查看当前网络中计算机的拓扑结构，如图2-18所示。

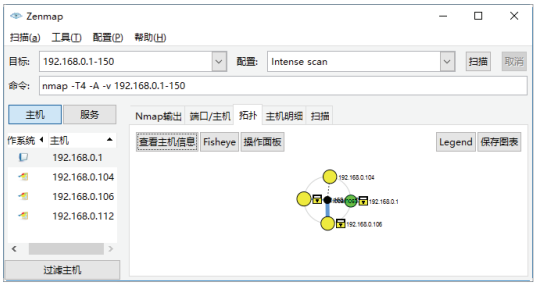

图 2-18　“拓扑”选项卡

Step 07 单击“查看主机信息”按钮，打开“查看主机信息”窗口，在其中可以查看当前主机的一般信息、操作系统等信息，如图2-19所示。

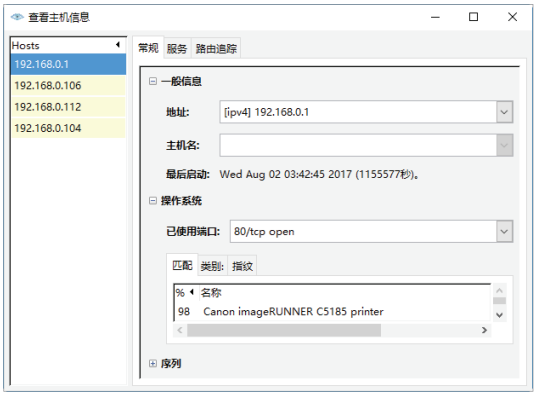

图 2-19　“查看主机信息”窗口

Step 08 在“查看主机信息”窗口中选择“服务”选项卡，可以查看当前主机的服务信息，如端口、协议、状态等，如图2-20所示。

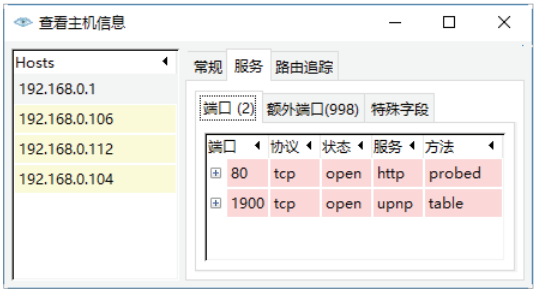

图 2-20　查看当前主机的服务信息

Step 09 选择“路由追踪”选项卡，在打开的界面中可以查看当前主机的路由器信息，如图2-21所示。

图 2-21　查看当前主机的路由器信息

Step 10 在Nmap操作界面中选择“主机明细”选项卡，在打开的界面可以查看当前主机的明细信息，包括主机状态、地址列表、操作系统等，如图2-22所示。

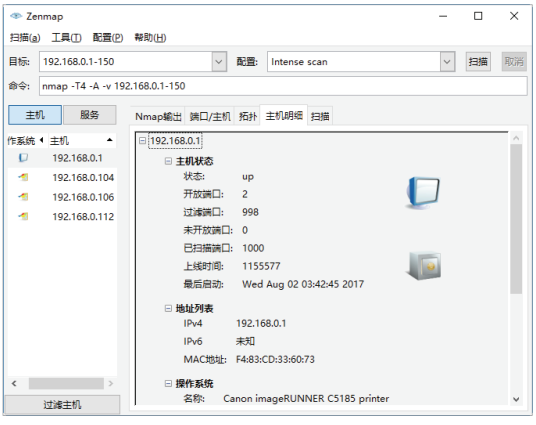

图 2-22　查看当前主机的明细信息

2.2　常见多功能扫描器工具

除了上面讲述的两种端口扫描器以外，还有很多具备诸多不同功能的扫描器，黑客们比较常用的多功能扫描器有流光扫描器、X-Scan扫描器、S-GUI Ver扫描器等，下面将分别进行介绍。

2.2.1　流光扫描器

流光扫描器是一款非常出名的中文多功能专业扫描器，其功能强大、扫描速度快、可靠性强，为广大电脑黑客迷们所钟爱。

流光扫描器可以探测POP3、FTP、HTTP、PROXY、FROM、SQL、SMTP和IPC等各种漏洞，并针对个中漏洞设计不同的破解方案。

1. 探测开放端口

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。

Step 01 单击桌面上的流光扫描器程序图标，启动流光扫描器，如图2-23所示。

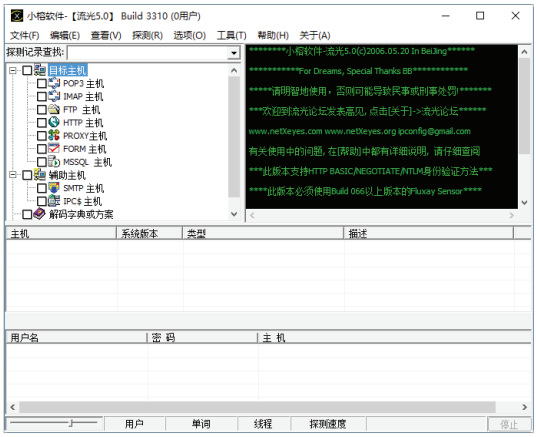

图 2-23　流光扫描器

Step 02 单击“选项”→“系统设置”，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2-24所示。

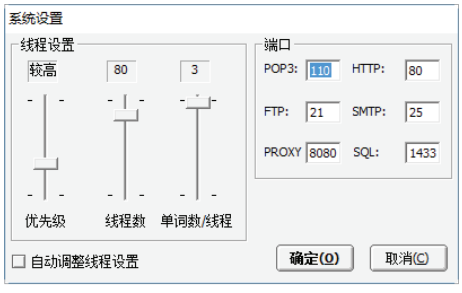

图 2-24　“系统设置”对话框

Step 03 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”选项，如图2-25所示。

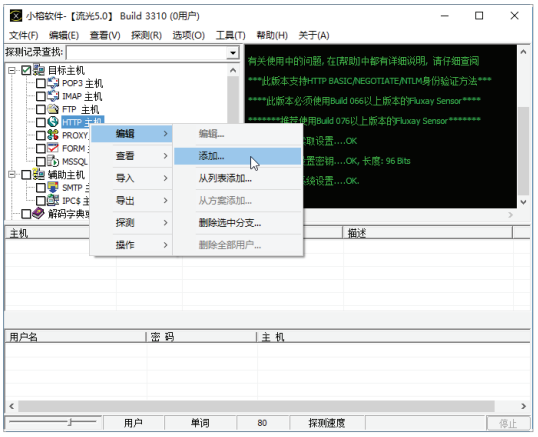

图 2-25 “添加”选项

Step 04 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2-26所示。

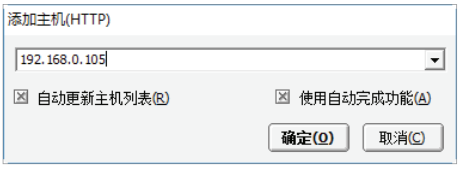

图 2-26 输入要扫描主机的 IP 地址

Step 05 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”选项，如图2-27所示。

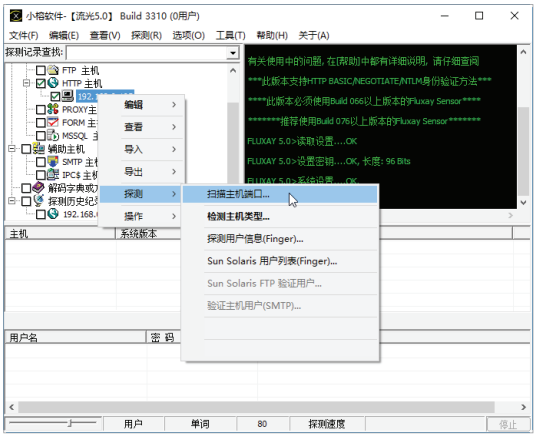

图 2-27 “扫描主机端口”选项

Step 06 打开“端口探测设置”对话框，在该对话框中勾选“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2-28所示。

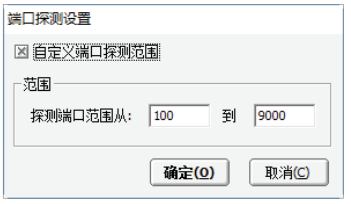

图 2-28 设置要探测端口的范围

Step 07 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2-29所示。

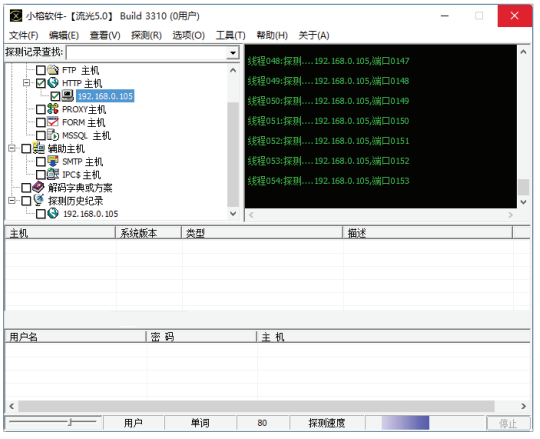

图 2-29 探测目标主机开放端口

Step 08 扫描完毕后，将会自动打开“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2-30所示。

图 2-30 “探测结果”对话框

2. 探测目标主机的IPC$用户列表

IPC$（Internet Process Connection）是

共享“命名管道”资源，是为了远程通信而开放的命名管道，可以通过验证用户名和密码获得相应的权限，在远程管理计算机和查看计算机的共享资源时使用。

利用IPC$可以与目标主机建立一个空的连接，连接者可以利用这个空的连接获得目标主机上的用户列表，通过猜测密码或者穷举密码，从而获得管理员权限。利用流光扫描器探测目标主机的IPC$用户列表的具体操作方法如下。

Step 01 在流光扫描器主窗口中勾选“IPC$主机”复选框，然后右击，在弹出的快捷菜单中选择“编辑”→“添加”选项，如图2-31所示。

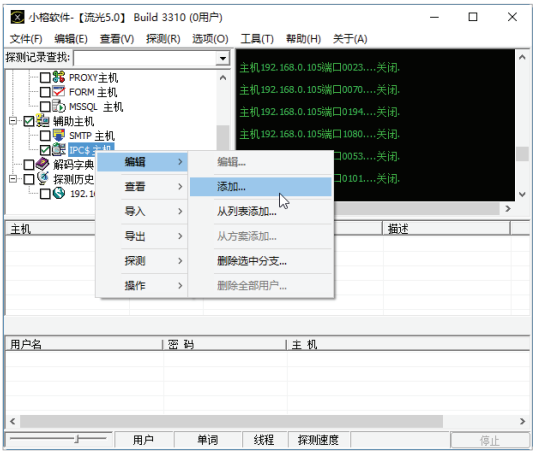

图 2-31　“添加”选项

Step 02 打开“添加主机（NT Server）”对话框，在其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2-32所示。

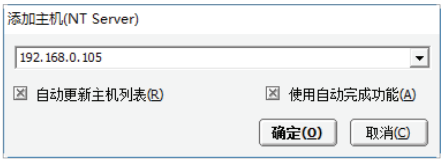

图 2-32　“添加主机”对话框

Step 03 选中刚刚添加的IPC$主机，然后右击，在弹出的快捷菜单中选择“编辑”→“探测IPC$用户列表”选项，如图2-33所示。

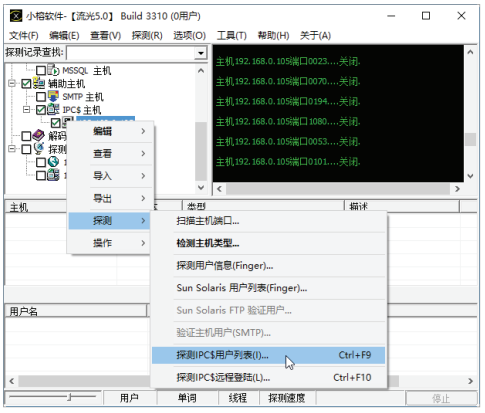

图 2-33　“探测 IPC$ 用户列表”选项

Step 04 打开“IPC自动探测”对话框，提示用户是否在成功获得用户名后立即开始简单模式探测，如图2-34所示。

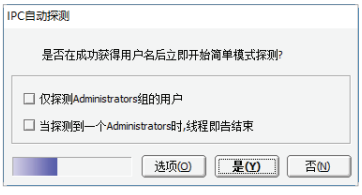

图 2-34　“IPC 自动探测”对话框

Step 05 单击“选项”按钮，在打开的“用户列表选项”对话框中进行设置，如图2-35所示。

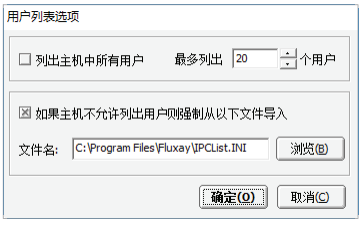

图 2-35　“用户列表选项”对话框

Step 06 单击“确定”按钮，程序开始自动探测目标主机，如图2-36所示。

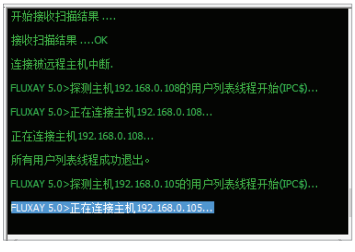

图 2-36　探测目标主机

3. 扫描指定地址范围内的目标主机

使用流光扫描器的高级扫描向导，可以快速地对指定地址范围内的目标主机进行扫描，具体的操作步骤如下。

Step 01 在流光扫描器主窗口中执行“文件”→“高级扫描向导”命令，如图2-37所示。

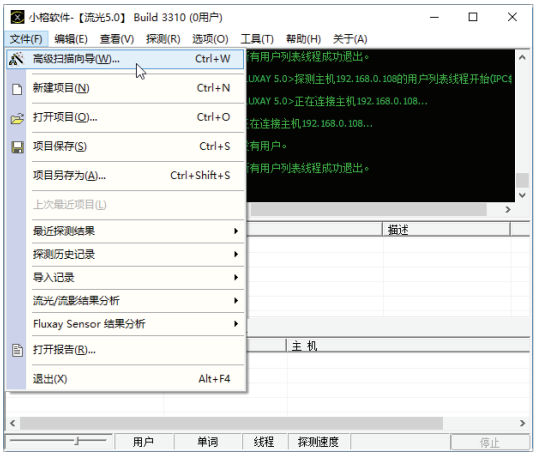

图 2-37 “高级扫描向导”命令

Step 02 打开“设置”对话框，在“起始地址”和“结束地址”文本框中分别输入指定地址范围的开始和结束IP地址，并勾选“获取主机名”和“PING检查”复选框，如图2-38所示。

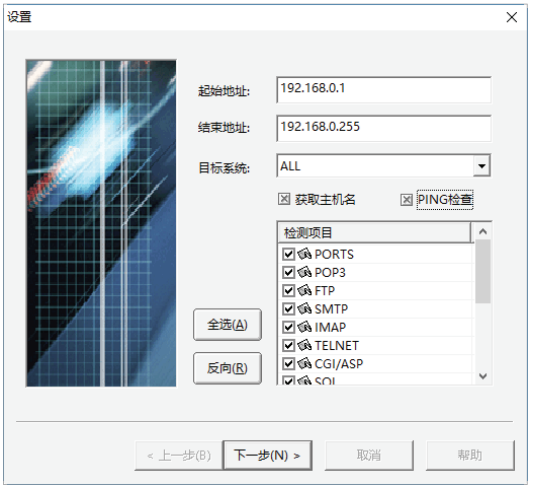

图 2-38 “设置”对话框

Step 03 单击“下一步”按钮，打开PORTS对话框，在该对话框中可以对要扫描的端口范围进行设置，这里勾选“标准端口扫描”复选框，如图2-39所示。

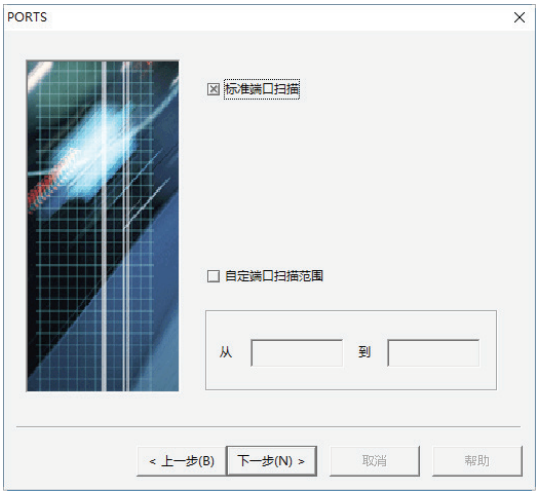

图 2-39 PORTS 对话框

Step 04 单击“下一步”按钮，打开POP3对话框，在其中可以对POP3检测项目进行设置，这里勾选“获取POP3版本信息”和“尝试猜解用户”复选框，如图2-40所示。

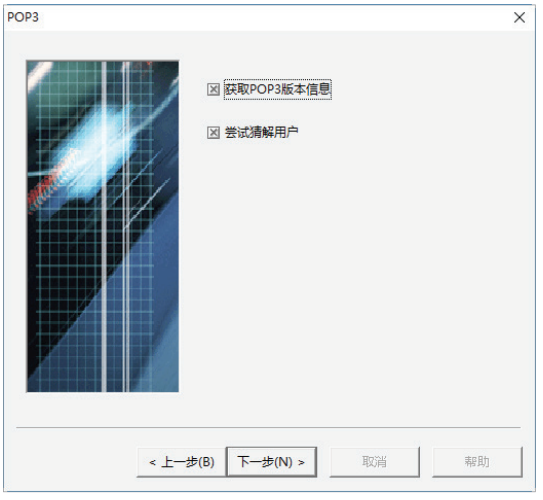

图 2-40 POP3 对话框

Step 05 单击“下一步”按钮，打开IPC对话框，在该对话框中可以对IPC检测项目进行设置，这里取消勾选“仅对Administraotors组进行猜解”复选框，如图2-41所示。

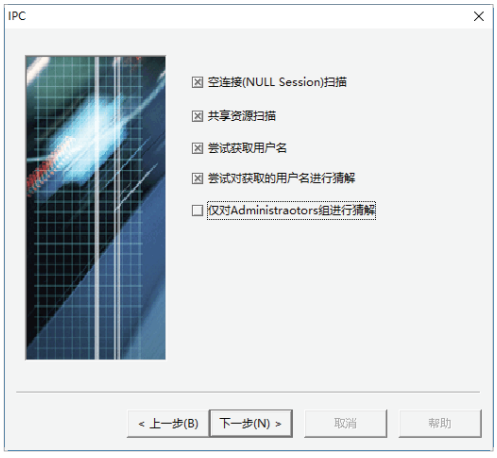

图 2-41　IPC 对话框

Step 06 单击“下一步”按钮，直至系统打开“选项”对话框，在该对话框中设置用户名字典、密码字典和扫描报告的保存路径等，如图2-42所示。

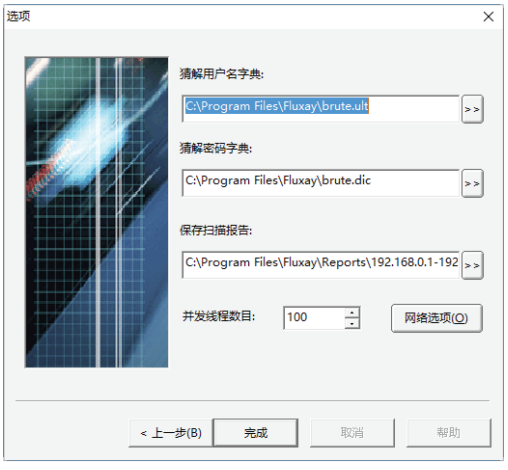

图 2-42　“选项”对话框

Step 07 单击“完成”按钮，打开“选择流光主机”对话框，如图2-43所示。

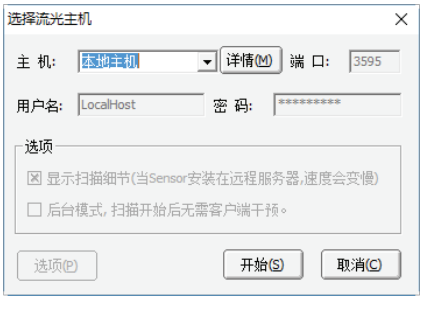

图 2-43　“选择流光主机”对话框

Step 08 单击“开始”按钮，程序开始扫描指定的地址范围，这可能需要较长时间，在扫描过程中会打开探测结果对话框提示用户，如图2-44所示。

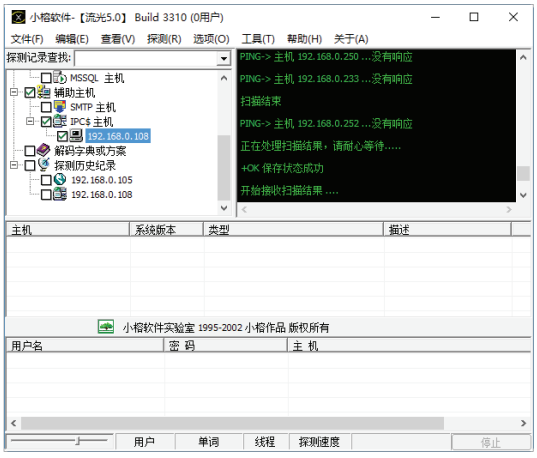

图 2-44　扫描指定的地址范围

提示：扫描完毕后，系统会打开“注意”提示信息框提醒用户是否要查看扫描报告，单击“是”按钮，此时会打开一个HTML格式的扫描报告，其中列出了扫描到的主机的详细信息，如图2-45所示。

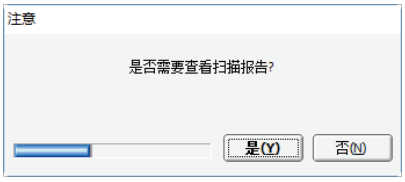

图 2-45　信息提示框

2.2.2　X-Scan扫描器

X-Scan是国内最著名的综合扫描器之一，该工具采用多线程方式对指定IP地址段（或单机）进行安全漏洞检测，且支持插件功能。它可以扫描出目标主机操作系统类型及版本、标准端口状态及端口BANNER信息、CGI漏洞、IIS漏洞、RPC漏洞、SQL-SERVER、FTP-SERVER、SMTP-SERVER、POP3-SERVER、NT-SERVER弱口令用户、NT服务器NETBIOS等信息。

1. 设置X-Scan扫描器

在使用X-Scan扫描器扫描系统之前，需要先对该工具的一些属性进行设置，例如扫描参数、检测范围等。设置和使用X-Scan的具体操作步骤如下。

Step 01 在X-Scan文件夹中双击X-Scan_gui.exe应用程序，打开X-Scan v3.3 GUI主窗口。在其中可以浏览此软件的功能简介、常见问题解答等信息，如图2-46所示。

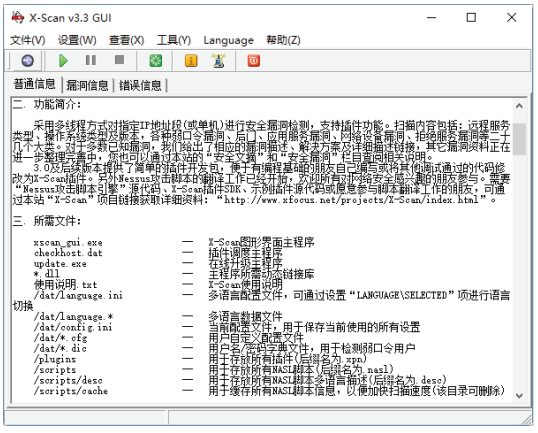

图 2-46　X-Scan v3.3 GUI 主窗口

Step 02 单击工具栏中的“扫描参数”按钮，打开“扫描参数”对话框，如图2-47所示。

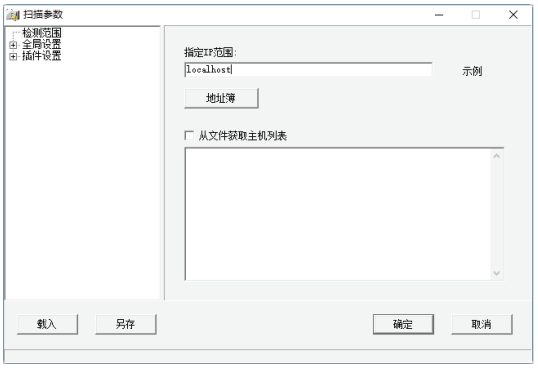

图 2-47　“扫描参数”对话框

Step 03 在左边的列表中单击“检测范围”选项卡，然后在“指定IP范围”文本框中输入要扫描的IP地址范围。若不知道输入的格式，单击“示例”按钮即可打开“示例”对话框。在其中可看到各种有效格式，如图2-48所示。

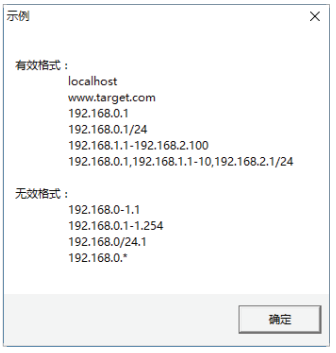

图 2-48　“示例”对话框

Step 04 切换到“全局设置”选项卡下，并单击其中的“扫描模块”子项，在其中即可选择扫描过程中需要扫描的模块。在选择扫描模块的同时，还可在右侧窗格中查看勾选的模块的相关说明，如图2-49所示。

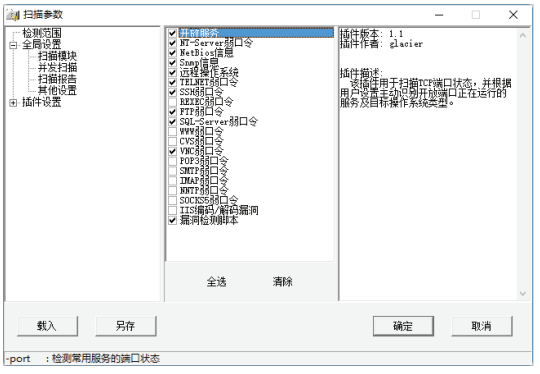

图 2-49　“全局设置”选项卡

Step 05 由于X-Scan是一款多线程扫描工具，在“并发扫描”子项中可以设置扫描时的线程数量，如图2-50所示。

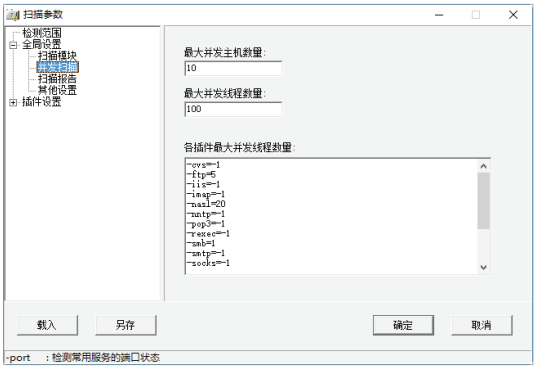

图 2-50　“并发扫描”子项

Step 06 切换到“扫描报告”子项下，在其中可以设置扫描报告存放的路径和文件格式，如图2-51所示。

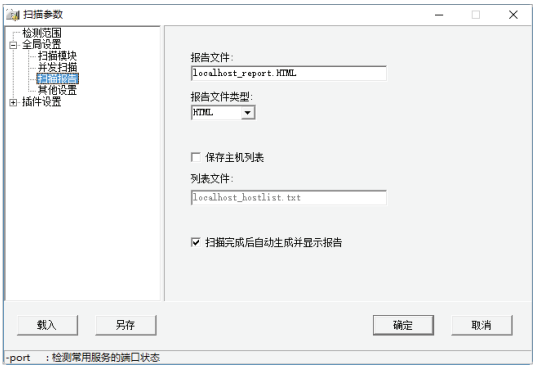

图 2-51 “扫描报告”子项

提示：如果需要保存自己设置的扫描IP地址范围，可在勾选“保存主机列表”复选框后，输入保存文件名称，以后就可以直接调用这些IP地址范围；如果用户需要在扫描结束时自动生成报告文件并显示报告，则可勾选“扫描完成后自动生成并显示报告”复选框。

Step 07 切换到“其他设置”子项下，在其中可以设置扫描过程的其他属性，如设置扫描方式、显示详细进度等，如图2-52所示。

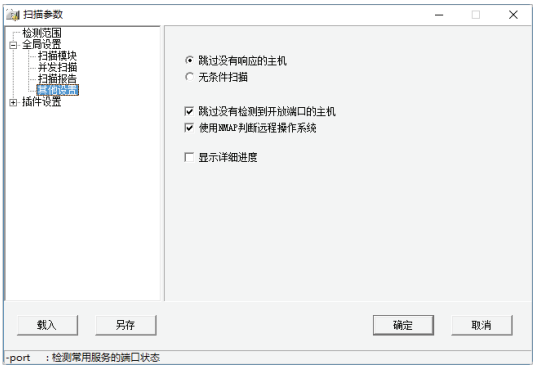

图 2-52 “其他设置”子项

Step 08 切换到“插件设置”选项卡下，并单击其中的“端口相关设置”子项，在其中可设置扫描端口范围以及检测方式，这里检测方式为“TCP”，如图2-53所示。

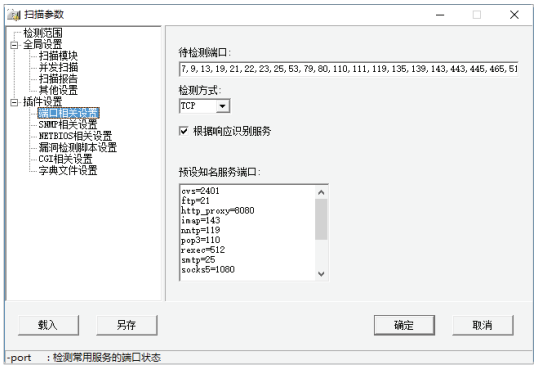

图 2-53 “端口相关设置”子项

Step 09 切换到“SNMP相关设置”子项下，在其中勾选相应的复选框来设置在扫描时获取SNMP信息的内容，如图2-54所示。

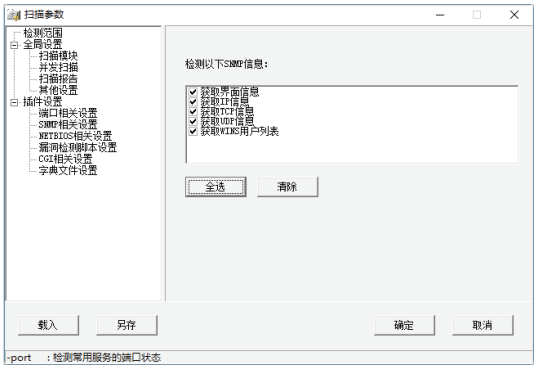

图 2-54 “SNMP 相关设置”子项

Step 10 切换到“NETBIOS相关设置”子项下，在其中设置需要获取的NETBIOS信息类型，如图2-55所示。

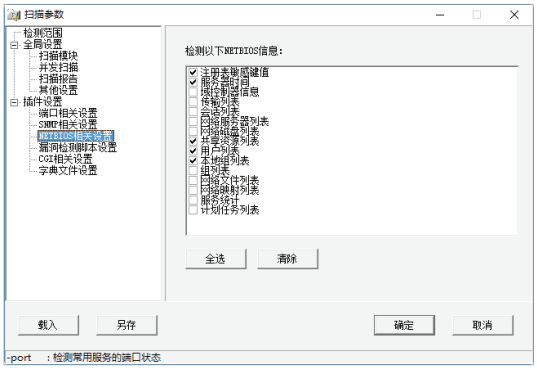

图 2-55 “NETBIOS 相关设置”子项

Step 11 切换到“漏洞检测脚本设置”子项下，取消勾选“全选”复选框之后，单击

“选择脚本”按钮，打开Select Script（选择脚本）对话框，如图2-56所示。

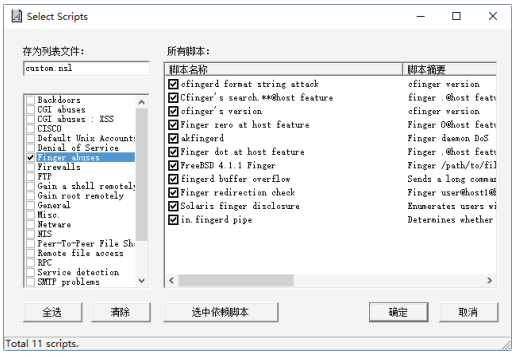

图 2-56　Select Script 对话框

Step 12 在选择检测的脚本文件之后，单击“确定”按钮返回“扫描参数”对话框中，并分别设置脚本运行超时和网络读取超时等属性，如图2-57所示。

图 2-57　“扫描参数”对话框

Step 13 在“CGI相关设置”子项下，在其中可设置扫描时需要使用的CGI选项，如图2-58所示。

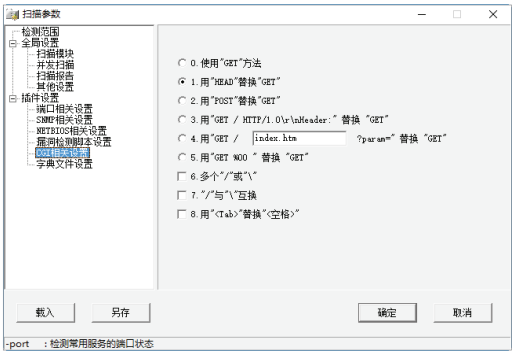

图 2-58　“CGI 相关设置”子项

Step 14 切换到“字典文件设置”子项下，然后可以通过双击字典类型，打开“打开”对话框，如图2-59所示。

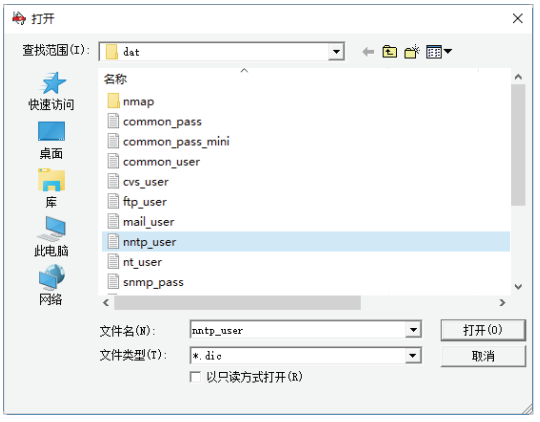

图 2-59　“打开”对话框

Step 15 在其中选择相应的字典文件后，单击“打开”按钮，返回“扫描参数”对话框，可看到选中的字典类型及字典文件名。在设置好所有选项之后，单击“确定”按钮即可完成设置，如图2-60所示。

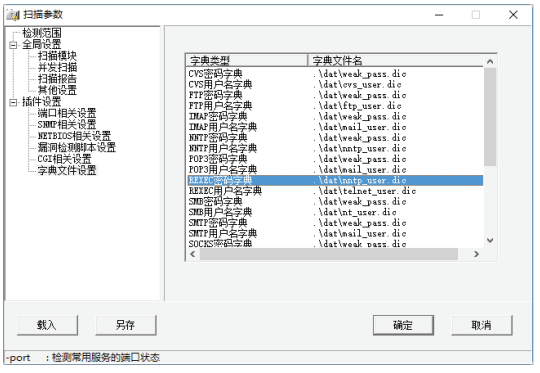

图 2-60　“扫描参数”对话框

2. 使用X-Scan进行扫描

在设置完X-Scan各个属性后，就可以利用该工具对指定IP地址范围内的主机进行扫描，具体的操作步骤如下。

Step 01 在X-Scan v3.3 GUI主窗口中单击“开始扫描”按钮即可进行扫描，在扫描的同时可显示扫描进程和扫描所得到的信息，如图2-61所示。

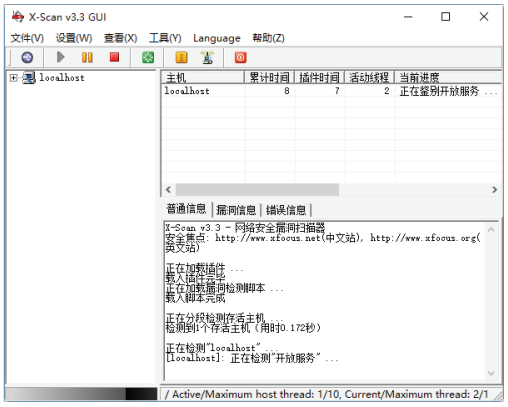

图 2-61　扫描主机信息

Step 02 在扫描完成之后，可看到HTML格式的扫描报告。在其中可看到活动主机IP地址、存在的系统漏洞和其他安全隐患，如图2-62所示。

图 2-62　HTML 格式的扫描报告

Step 03 在X-Scan v3.3 GUI主窗口中切换到“漏洞信息”选项卡下，在其中可看到存在漏洞的主机信息，如图2-63所示。

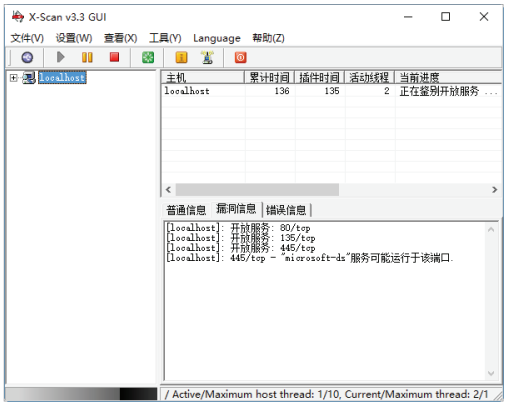

图 2-63　“漏洞信息”选项卡

2.2.3　S-GUI Ver扫描器

S-GUI Ver扫描器是以S.EXE为核心的可视化的端口扫描工具，支持多端口扫描、线程控制、隐藏扫描、扫描列表、去掉端口、自动整理扫描结果等，是一款使用起来比较方便的端口扫描工具。

使用S-GUIVer扫描端口的具体操作步骤如下。

Step 01 下载并解压S-GUI Ver2.0软件，并双击其中的S-GUI Ver2.0.exe，可打开S-GUI Ver2.0主窗口，如图2-64所示。

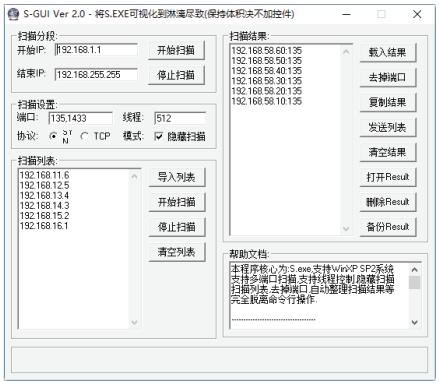

图 2-64　S-GUI Ver2.0 主窗口

Step 02 在S-GUI Ver2.0窗口的“扫描分段”选项框中分别输入开始扫描的IP地址和结果扫描的IP地址，然后在“扫描设置”选项框中的“端口”文本框中输入要扫描的端口，最后在“协议”选项区中选中TCP单选按钮，如图2-65所示。

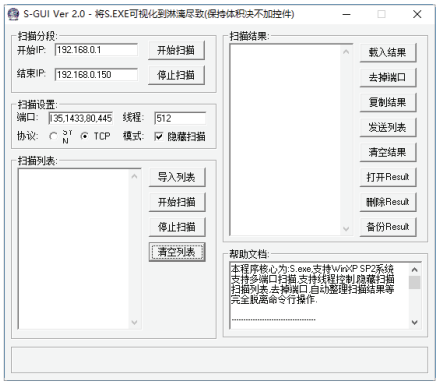

图 2-65　输入扫描 IP 地址段

Step 03 设置完毕后，单击“开始扫描”按

钮，打开“提示”对话框，在其中即可看到“扫描已经开始，正在扫描中，扫描完毕后有提示”的提示信息，如图2-66所示。

Step 04 单击“确定”按钮，打开Windows Script Host对话框，在其中即可看到“扫描完毕！请载入结果……”提示信息，如图2-67所示。

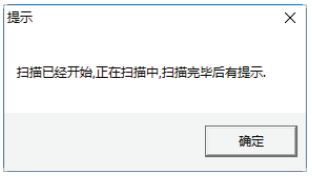

图 2-66 “提示”对话框

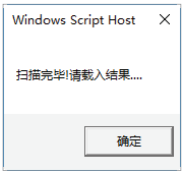

图 2-67 扫描完毕

Step 05 单击“确定”按钮，返回S-GUI Ver2.0主窗口，然后单击右侧的 载入结果 按钮，打开“提示”对话框，在其中即可看到“你真的要[载入结果]吗？如果‘是’将会覆盖掉[扫描结果]中的原有数据”提示信息，如图2-68所示。

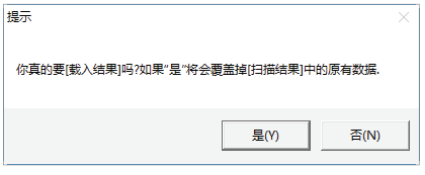

图 2-68 “提示”对话框

Step 06 单击“是”按钮，将扫描结果添加到“扫描结果”文本区域中，在其中可看到扫描到的开放指定端口主机的IP地址以及端口号，如图2-69所示。

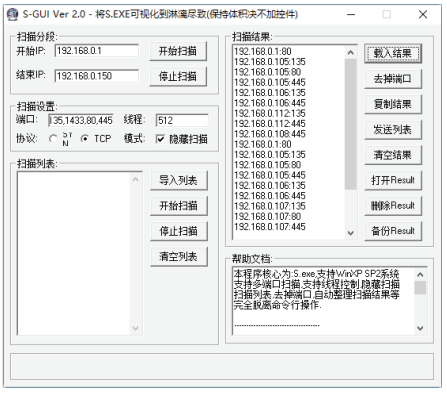

图 2-69 “扫描结果”文本区域

Step 07 如果想要将扫描结果内容放入左侧扫描列表中，则需要单击“发送列表”按钮，打开“提示”对话框，在其中即可看到“你真的要将[扫描结果]发送到[扫描列表]吗？如果‘是’将会覆盖掉[扫描列表]中的原有数据”提示信息，如图2-70所示。

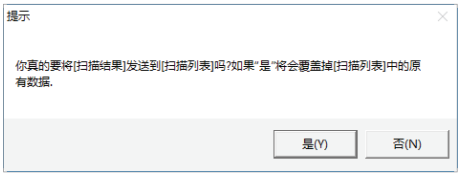

图 2-70 “提示”对话框

Step 08 单击“是”按钮，打开“已经发送到[扫描列表]中并去掉了端口号”提示框，如图2-71所示。

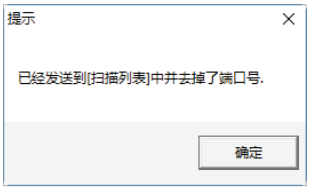

图 2-71 信息提示框

Step 09 单击“确定”按钮，可在S-GUI Ver2.0主窗口左侧的“扫描列表”中看到扫描到的主机列表，如图2-72所示。

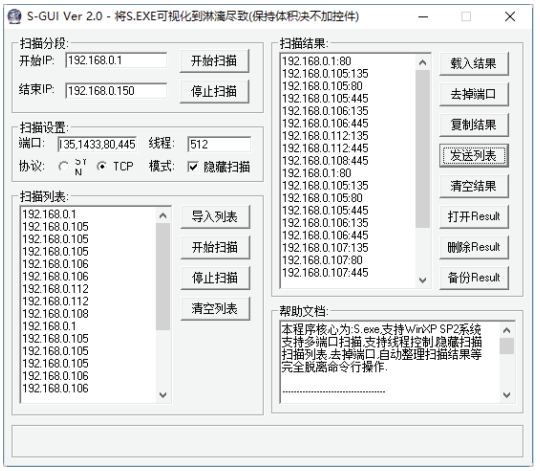

图 2-72 扫描到的主机列表

Step 10 单击“打开Result”按钮，以记事本的形式打开Result记事本文件，在其中可看到具体的扫描信息，如图2-73所示。

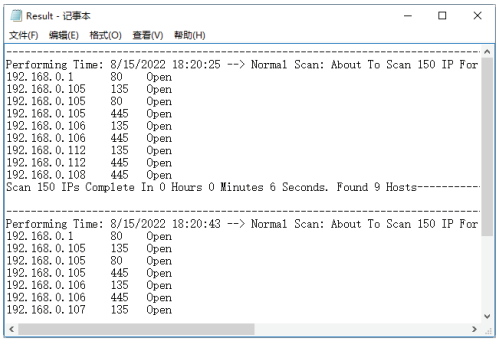

图 2-73　“Result”记事本文件

2.3　常用网络嗅探工具

网络嗅探的基础是数据捕获，其系统是并接在网络中来实现数据捕获的。这种方式和入侵检测系统相同。

2.3.1　嗅探利器SmartSniff

SmartSniff可以让用户捕获自己网络适配器的TCP/IP数据包，并且可以按顺序查看客户端与服务器之间会话的数据。用户可以使用ASCII模式（用于基于文本的协议，如HTTP、SMTP、POP3与FTP）、十六进制模式来查看TCP/IP会话（用于基于非文本的协议，如DNS）。

利用SmartSniff捕获TCP/IP数据包的具体操作步骤如下。

Step 01 单击桌面上的SmartSniff程序图标，打开SmartSniff主窗口，如图2-74所示。

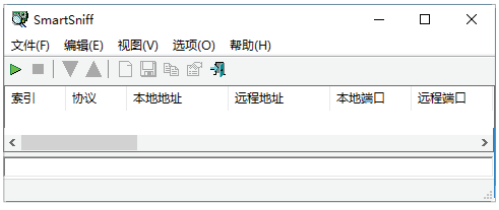

图 2-74　SmartSniff 主窗口

Step 02 单击“开始捕获”按钮或按F5键，开始捕获当前主机与网络服务器之间传输的数据包，如图2-75所示。

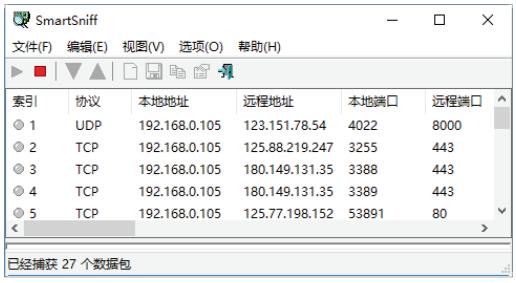

图 2-75　捕获数据包信息

Step 03 单击“停止捕获”按钮或按F6键，停止捕获数据，在列表中选择任意一个TCP类型的数据包，可查看其数据信息，如图2-76所示。

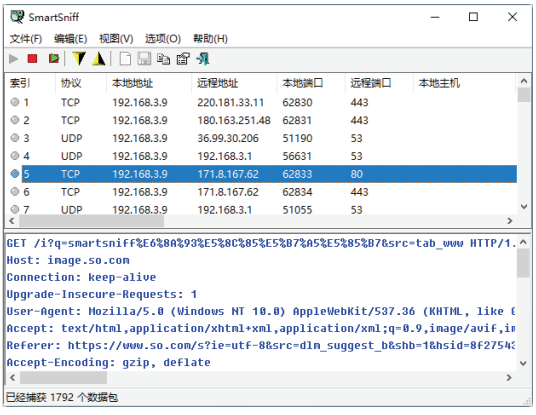

图 2-76　停止捕获数据

Step 04 在列表中选择任意一个UDP协议类型的数据包，可查看其数据信息，如图2-77所示。

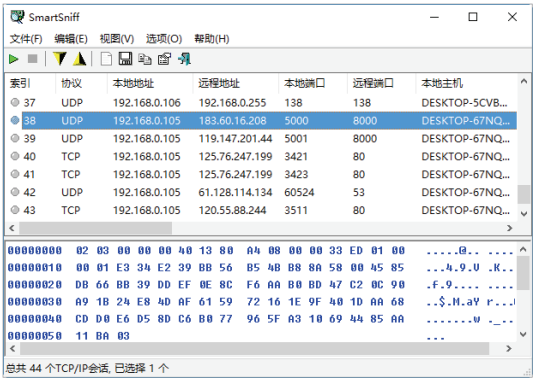

图 2-77　查看数据信息

Step 05 在列表中选中任意一个数据包，执行“文件”→“属性”命令，在打开的“属

性”对话框中可以查看其属性信息，如图2-78所示。

图 2-78 “属性”对话框

Step 06 在列表中选中任意一个数据包，执行“视图”→“网页报告-TCP/IP数据流”命令，可以网页形式查看数据流报告，如图2-79所示。

图 2-79 查看数据流报告

2.3.2 网络数据包嗅探专家

网络数据包嗅探专家是一款监视网络数据运行的嗅探器，能够完整地捕捉到所处局域网中所有计算机的上行、下行数据包。用户可以将捕捉到的数据包保存下来，以进行监视网络流量、分析数据包、查看网络资源利用、执行网络安全操作规则、鉴定分析网络数据，以及诊断并修复网络问题等操作。

使用网络数据包嗅探专家的具体操作方法如下。

Step 01 打开网络数据包嗅探专家程序，其工作界面，如图2-80所示。

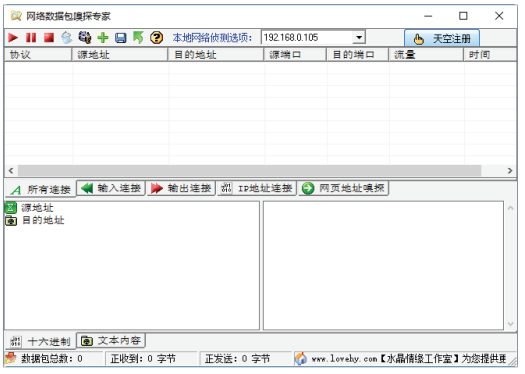

图 2-80 网络数据包嗅探专家

Step 02 单击“▶”按钮，开始捕获当前网络数据，如图2-81所示。

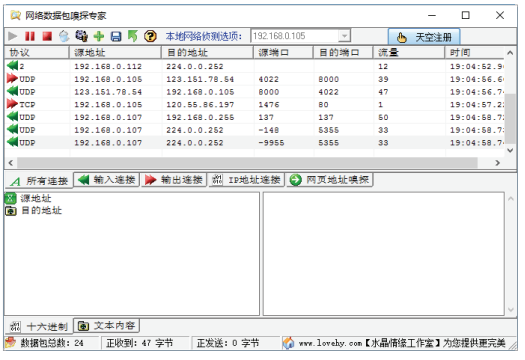

图 2-81 捕获当前网络数据

Step 03 单击“■”按钮，停止捕获数据包，当前的所有网络连接数据将在下方显示出来，如图2-82所示。

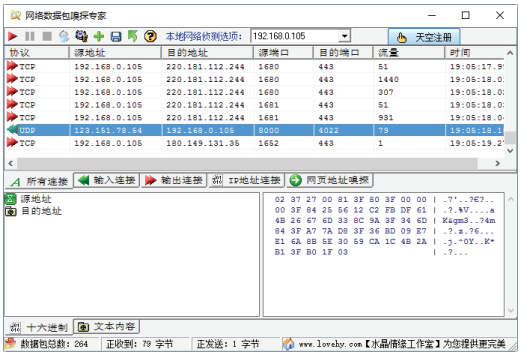

图 2-82 停止捕获数据包

Step 04 单击“IP地址连接”按钮，将在上方窗格中显示前一段时间内输入与输出数据的源地址与目标地址，如图2-83所示。

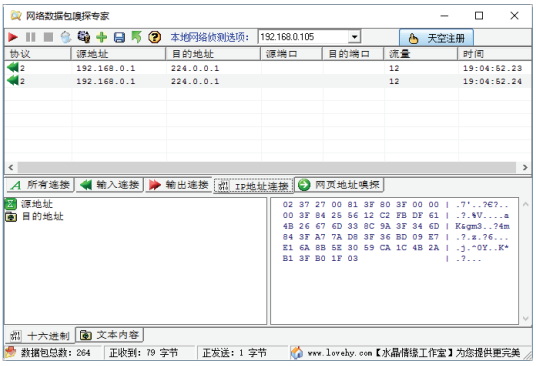

图 2-83　显示源地址与目标地址

Step 05 单击“网页地址嗅探”按钮，可查看当前所连接网页的详细地址和文件类型，如图2-84所示。

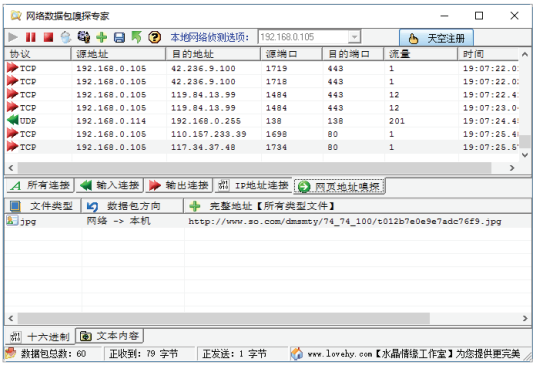

图 2-84　显示详细地址和文件类型

2.4　实战演练

2.4.1　实战1：查看系统中的ARP缓存表

在利用网络欺骗攻击的过程中，经常用到的一种欺骗方式是ARP欺骗，但在实施ARP欺骗之前，需要查看ARP缓存表。那么如何查看系统的ARP缓存表信息呢？

具体的操作步骤如下。

Step 01 右击“⊞”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“打开”文本框中输入cmd命令，如图2-85所示。

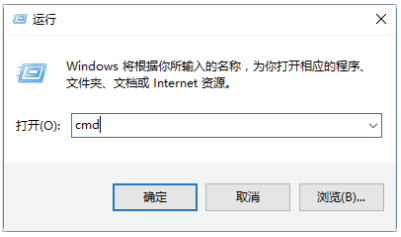

图 2-85　“运行”对话框

Step 02 单击“确定”按钮，打开“命令提示符”窗口，如图2-86所示。

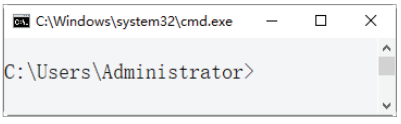

图 2-86　“命令提示符”窗口

Step 03 在“命令提示符”窗口中输入arp -a命令，按Enter键执行命令，可显示出本机系统的ARP缓存表中的内容，如图2-87所示。

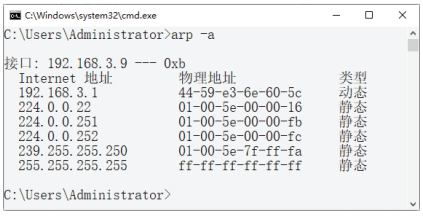

图 2-87　ARP 缓存表

Step 04 在“命令提示符”窗口中输入arp -d命令，按Enter键执行命令，可删除ARP表中所有的内容，如图2-88所示。

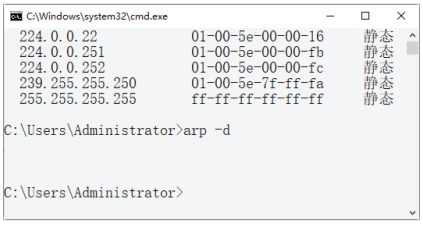

图 2-88　删除 ARP 表

2.4.2　实战2：在网络邻居中隐藏自己

如果不想让别人在网络邻居中看到自己的计算机，可把自己的计算机名称在网

络邻居里隐藏，具体的操作步骤如下。

Step 01 右击“”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“打开”文本框中输入regedit命令，如图2-89所示。

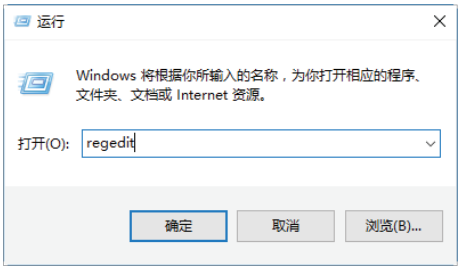

图 2-89 “运行”对话框

Step 02 单击“确定”按钮，打开“注册表编辑器”窗口，如图2-90所示。

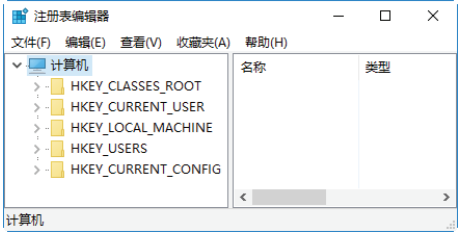

图 2-90 “注册表编辑器”窗口

Step 03 在“注册表编辑器”窗口中，展开分支到HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters子键下，如图2-91所示。

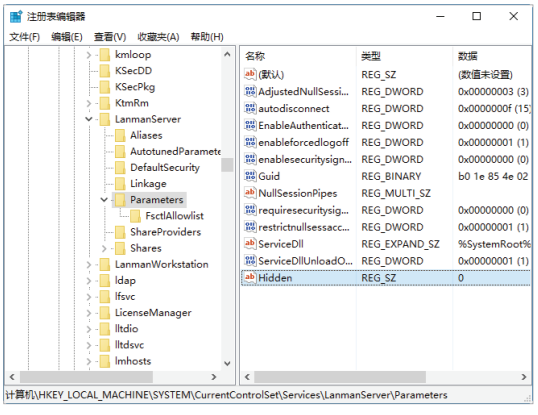

图 2-91 展开分支

Step 04 选中Hidden子键并右击，在弹出的快捷菜单中选择“修改”选项，打开“编辑字符串”对话框，如图2-92所示。

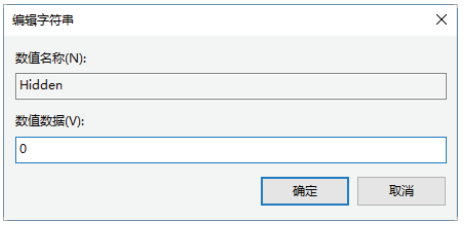

图 2-92 “编辑字符串”对话框

Step 05 在“数值数据”文本框中将数值从0设置为1，如图2-93所示。

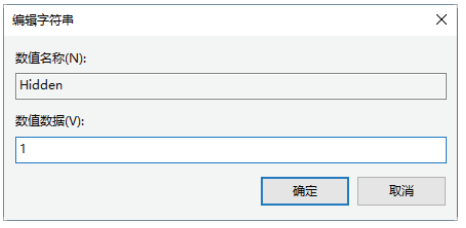

图 2-93 设置数值数据为 1

Step 06 单击“确定”按钮，就可以在网络邻居中隐藏自己的计算机了，如图2-94所示。

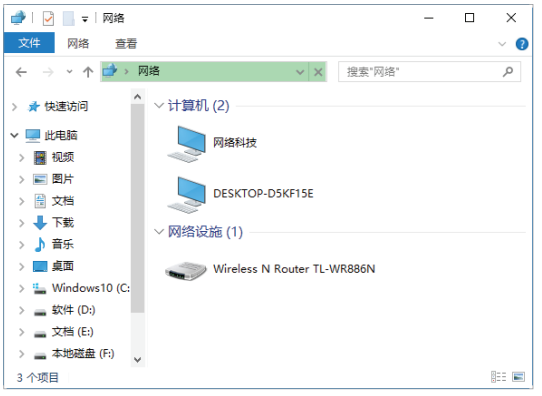

图 2-94 网络邻居

第3章　系统漏洞与安全防护工具

目前，用户普遍使用的操作系统为Windows 10操作系统，不过，该系统也存在有这样或那样的系统漏洞与安全隐患，这就给黑客留下了入侵攻击的机会。作为计算机用户，如何才能有效地防止黑客的入侵攻击，就成了迫在眉睫的问题。本章就来介绍系统漏洞与安全防护工具的使用。

3.1　系统漏洞修补工具

计算机系统漏洞也被称为系统安全缺陷，这些安全缺陷会被技术高低不等的入侵者所利用，从而达到控制目标主机乃至实施破坏的目的。要想防范系统的漏洞，首选就是及时为系统打补丁，下面介绍几种为系统打补丁的方法。

3.1.1　系统漏洞产生的原因

系统漏洞的产生不是安装不当的结果，也不是使用后的结果。归纳起来，系统漏洞产生的原因主要有以下几点：

（1）人为因素，编程人员在编写程序过程中故意在程序代码的隐蔽位置保留了后门。

（2）硬件因素，因为是硬件的原因，编程人员无法弥补硬件的漏洞，从而使硬件问题通过软件表现出来。

（3）客观因素，受编程人员的能力、经验和当时的安全技术及加密方法所限，在程序中不免存在不足之处，而这些不足恰恰会导致系统漏洞的产生。

3.1.2　使用Windows更新修补漏洞

“Windows更新”是系统自带的用于检测系统更新的工具，使用“Windows更新”可以下载并安装系统更新。以Windows 10系统为例，具体的操作步骤如下。

Step 01 单击“”按钮，在打开的菜单中选择“设置”选项，如图3-1所示。

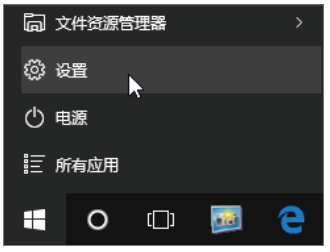

图 3-1　“设置”选项

Step 02 打开“设置”窗口，在其中可以看到有关系统设置的相关功能，如图3-2所示。

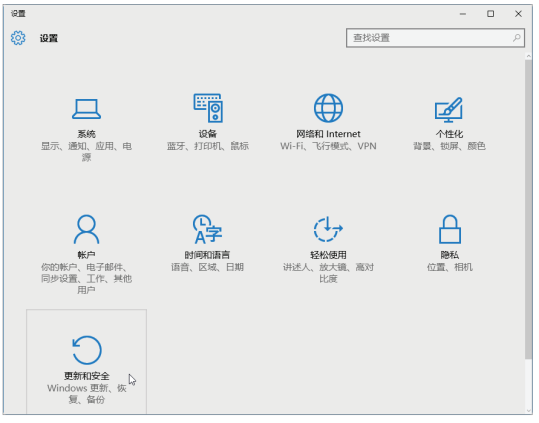

图 3-2　“设置”窗口

Step 03 单击“更新和安全”图标，打开“更新和安全”窗口，在其中选择“Windows更新”选项，如图3-3所示。

Step 04 单击“检查更新”按钮，可开始检查网上是否存在有更新文件，如图3-4所示。

图 3-3 “更新和安全”窗口

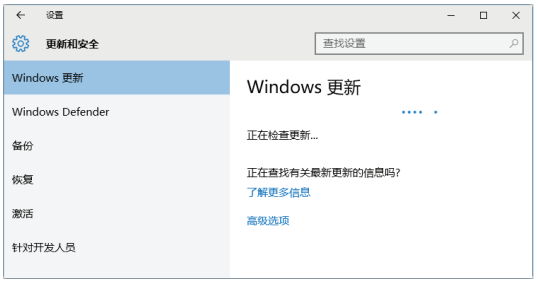

图 3-4 查询更新文件

Step 05 检查完毕后，如果存在更新文件，则会打开如图3-5所示的信息提示，提示用户有可用更新，并自动开始下载更新文件。

图 3-5 下载更新文件

Step 06 下载完成后，系统会自动安装更新文件，安装完毕后，会打开如图3-6所示的信息提示框。

Step 07 单击“立即重新启动”按钮，重新启动电脑，重新启动完毕后，再次打开“Windows更新”窗口，在其中可以看到“你的设备已安装最新的更新”信息提示，如图3-7所示。

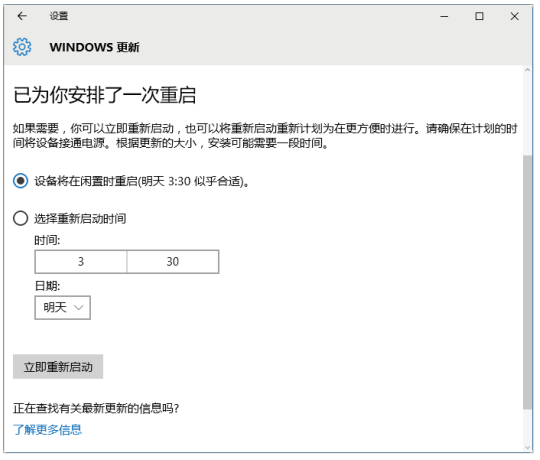

图 3-6 自动安装更新文件

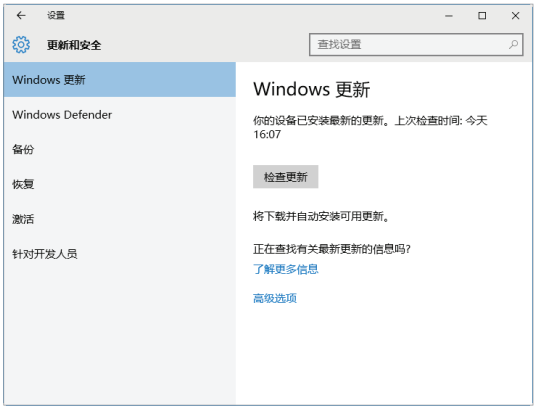

图 3-7 完成系统更新

Step 08 单击“高级选项”超链接，打开“高级选项”设置工作界面，在其中可以选择安装更新的方式，如图3-8所示。

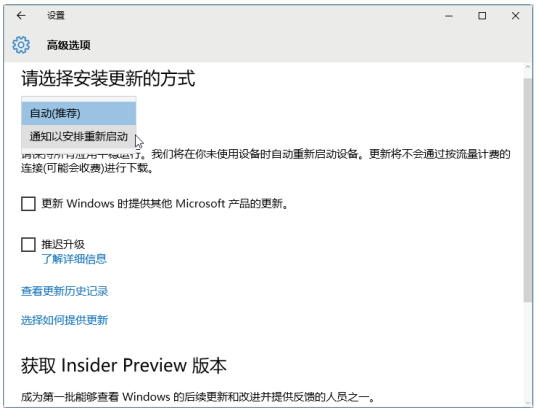

图 3-8 选择更新方式

3.1.3　使用电脑管家修补漏洞

除使用Windows系统自带的Windows更新下载并及时为系统修复漏洞外，还可以使用第三方软件及时为系统下载并安装漏洞补丁，常用的有电脑管家、360安全卫士、优化大师等。

使用电脑管家修复系统漏洞的具体操作步骤如下。

Step 01 双击桌面上的电脑管家图标，打开“电脑管家”窗口，选择“工具箱”选项，进入如图3-9所示页面。

图 3-9　“工具箱”窗口

Step 02 单击“修复漏洞”图标，开始自动扫描系统中存在的漏洞，并在下面的界面中显示出来，用户在其中可以自主选择需要修复的漏洞，如图3-10所示。

图 3-10　“系统修复”窗口

Step 03 单击“一键修复”按钮，开始修复系统存在的漏洞。修复完成后，系统漏洞的状态变为“修复成功”，如图3-11所示。

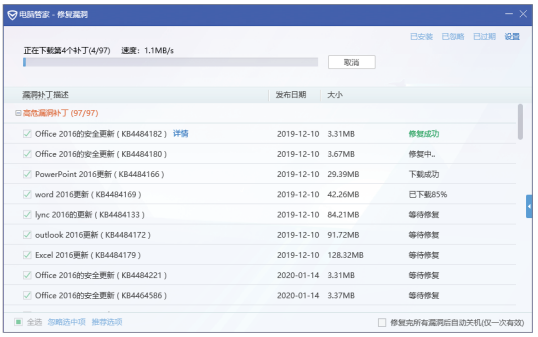

图 3-11　成功修复系统漏洞

3.1.4　使用360安全卫士修补漏洞

使用360安全卫士扫描系统漏洞并修补漏洞的操作步骤如下。

Step 01 双击桌面上的360安全卫士快捷图标，进入360安全卫士工作界面，单击“系统修复”图标，开始检测计算机的状态，检测完毕后即可显示出当前计算机系统漏洞，如图3-12所示。

图 3-12　计算机系统漏洞

Step 02 单击“一键修复”按钮，开始下载并修复系统漏洞，如图3-13所示。

图 3-13　下载并修复系统漏洞

Step 03 修复完成后，会给出相应的修复结果，如图3-14所示。

图 3-14　系统漏洞修复结果

3.2　间谍软件防护工具

间谍软件是一种能够在用户不知情的情况下，在其计算机上安装后门、收集用户信息的软件。间谍软件以恶意后门程序的形式存在，该程序可以打开端口、启动ftp服务器或者搜集击键信息并将信息反馈给攻击者。

3.2.1　通过事件查看器抓住隐藏的间谍软件

不管我们是不是计算机高手，都要学会自己根据Windows自带的“事件查看器”对应用程序、系统、安全和设置等进程进行分析与管理。

通过事件查看器查找间谍软件的操作步骤如下。

Step 01 右击“此电脑”图标，在弹出的快捷菜单中选择“管理”选项，如图3-15所示。

Step 02 打开“计算机管理”对话框，在其中可以看到系统工具、存储、服务和应用程序3个方面的内容，如图3-16所示。

Step 03 在左侧依次展开“计算机管理（本地）”→“系统工具”→“事件查看器”选项，可在下方显示事件查看器所包含的内容，如图3-17所示。

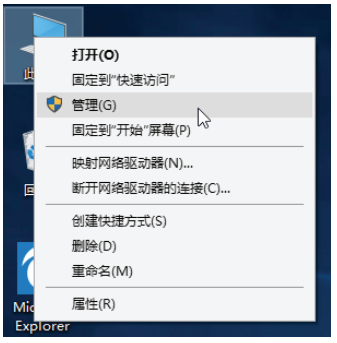

图 3-15　“管理”选项

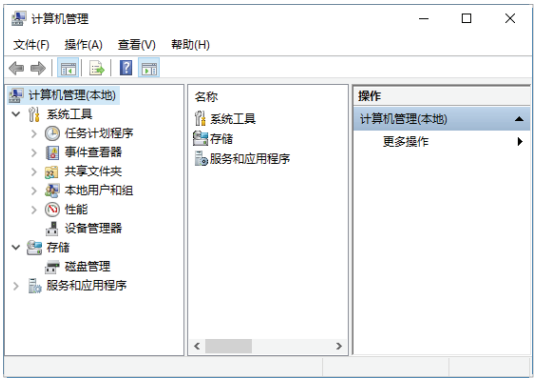

图 3-16　“计算机管理”对话框

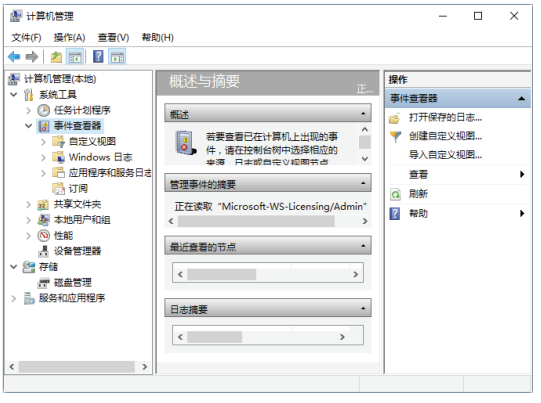

图 3-17　事件查看器

Step 04 双击“Windows日志”选项，可在右侧显示有关Windows日志的相关内容，包括应用程序、安全、设置、系统和已转发事件等，如图3-18所示。

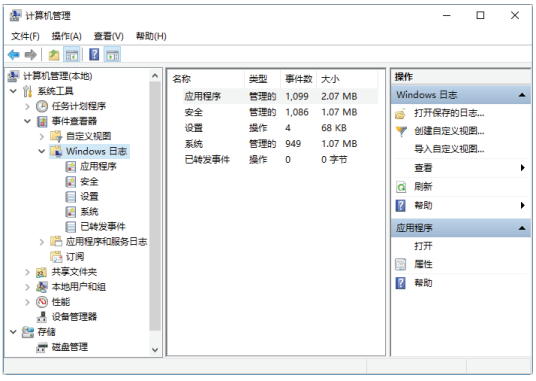

图 3-18　Windows 日志信息

Step 05 双击右侧区域中的“应用程序”选项，可在打开的界面中看到非常详细的应用程序信息，其中包括应用程序被打开、修改、权限过户、权限登记、关闭以及重要的出错或者兼容性信息等，如图3-19所示。

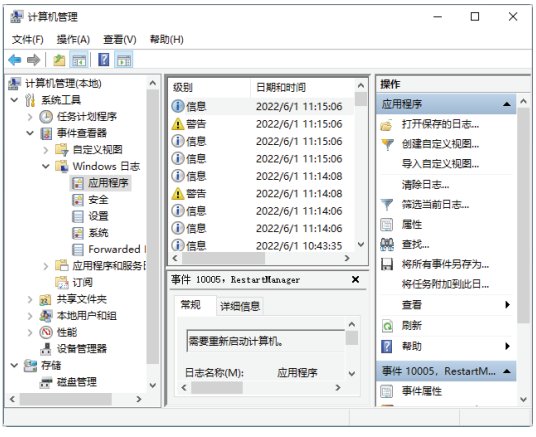

图 3-19　应用程序信息

Step 06 右击其中任意一条信息，在弹出的快捷菜单中选择“事件属性”选项，如图3-20所示。

Step 07 打开“事件属性”对话框，在该对话框中可以查看该事件的常规属性以及详细信息等，如图3-21所示。

Step 08 右击其中任意一条应用程序信息，在弹出的快捷菜单中选择“保存选择的事件”选项，打开“另存为”对话框，在“文件名”文本框中输入事件的名称，并选择事件保存的类型，如图3-22所示。

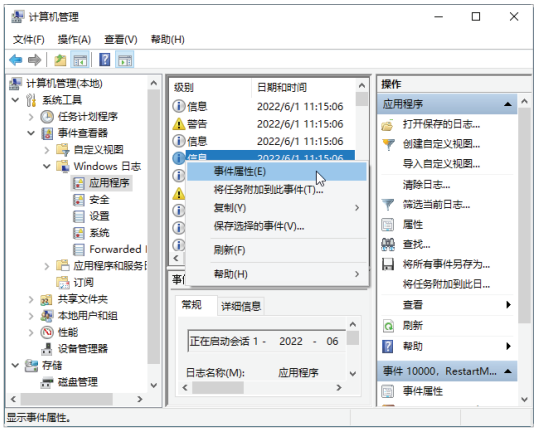

图 3-20　“事件属性”选项

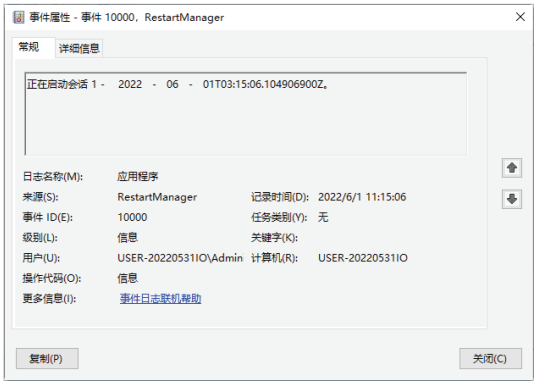

图 3-21　“事件属性”对话框

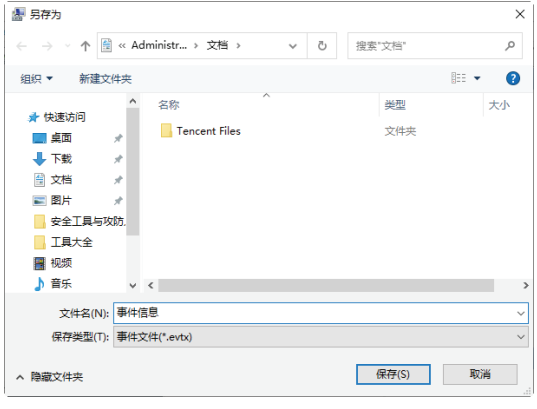

图 3-22　“另存为”对话框

Step 09 单击“保存”按钮，保存事件，并打开“显示信息”对话框，在其中设置是否要在其他计算机中正确查看此日志，设置完毕后，单击“确定”按钮即可保存设置，如图3-23所示。

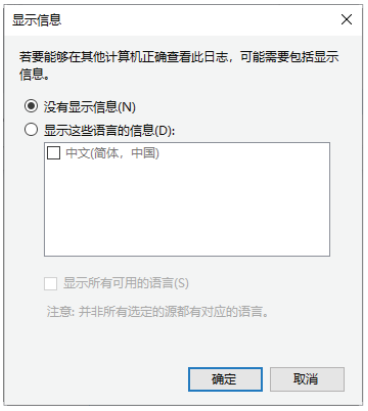

图 3-23 “显示信息”对话框

Step 10 双击左侧的“安全”选项，可以将计算机记录的安全性事件信息全都显示于此，用户可以对其进行具体查看和保存、附加程序等，如图3-24所示。

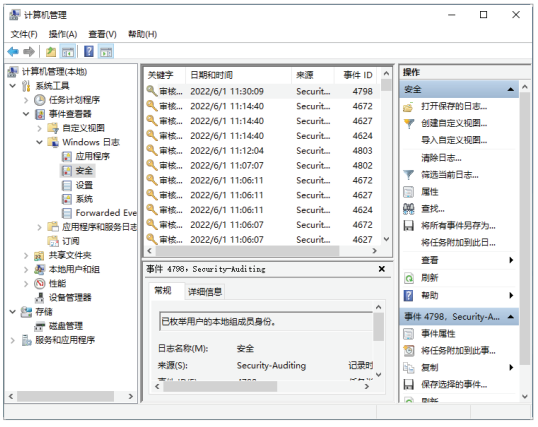

图 3-24 “安全”选项

Step 11 双击左侧的“设置”选项，在右侧将会展开系统设置详细内容，如图3-25所示。

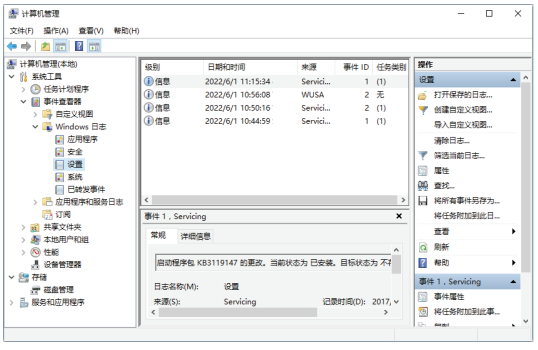

图 3-25 “设置”选项

Step 12 双击左侧的“系统”选项，会在右侧看到Windows操作系统运行时内核以及上层软硬件之间的运行记录，这里面会记录大量的错误信息，是黑客们分析目标计算机漏洞时最常用到的信息库，用户最好熟悉错误码，这样可以提高查找间谍软件的效率，如图3-26所示。

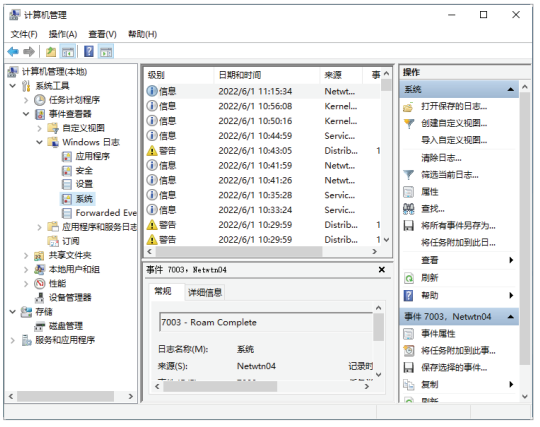

图 3-26 “系统”选项

3.2.2 使用反间谍专家揪出隐藏的间谍软件

使用反间谍专家可以扫描系统薄弱环节以及全面扫描硬盘，智能检测和查杀超过上万种木马、蠕虫、间谍软件等，并终止它们的恶意行为。当检测到可疑文件时，该工具还可以将其隔离，从而保护系统的安全。

下面介绍使用反间谍专家软件的基本步骤。

Step 01 运行反间谍专家程序，打开“反间谍专家”主界面，从中可以看出反间谍专家有“快速查杀”和“完全查杀”两种方式，如图3-27所示。

Step 02 在“查杀”栏目中单击“快速查杀”按钮，然后右边的窗口中单击“开始查杀”按钮，打开“扫描状态”对话框，如图3-28所示。

图 3-27　“反间谍专家”主界面

图 3-28　“扫描状态”对话框

Step 03 在扫描结束之后，打开“扫描报告”对话框，在其中列出了扫描到的恶意代码，如图3-29所示。

图 3-29　“扫描报告”对话框

Step 04 单击“选择全部”按钮，可选中全部的恶意代码，然后单击“清除”按钮，快速杀除扫描到的恶意代码，如图3-30所示。

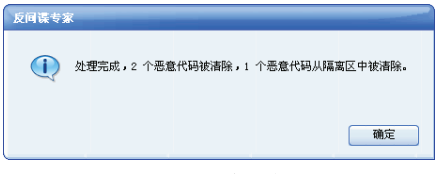

图 3-30　清除恶意代码

Step 05 如果要彻底扫描并查杀恶意代码，则需采用“完全查杀”方式。在“反间谍专家”主窗口中，单击“完全查杀”按钮，打开“完全查杀”对话框。从中可以看出完全查杀有三种快捷方式供选择，这里选中“扫描本地硬盘中的所有文件”单选项，如图3-31所示。

图 3-31　“完全查杀”对话框

Step 06 单击“开始查杀”按钮，打开“扫描状态”对话框，在其中可以查看查杀进程，如图3-32所示。

图 3-32　“扫描状态”对话框

Step 07 待扫描结束之后，打开“扫描报告”对话框，在其中列出所扫描到的恶意代码。勾选要清除的恶意代码前面的复选框后，单击“清除”按钮，即可删除这些恶意代码，如图3-33所示。

Step 08 在“反间谍专家”主界面中切换到“常用工具”栏目中，单击“系统免疫”按钮，打开“系统免疫”对话框，单击“启用”按钮即可确保系统不受到恶意程序的攻击，如图3-34所示。

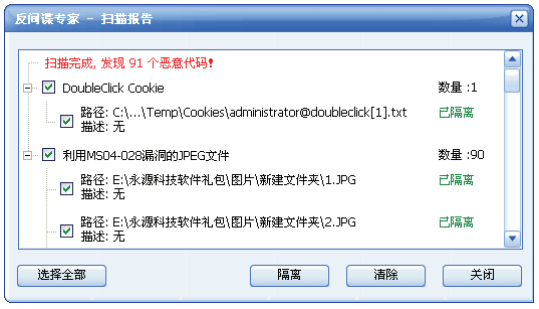

图 3-33　清除恶意代码

图 3-34　“系统免疫”对话框

Step 09 单击“IE修复”按钮，打开“IE修复”对话框，在勾选需要修复的项目之后，单击“立即修复”按钮，可将IE恢复到其原始状态，如图3-35所示。

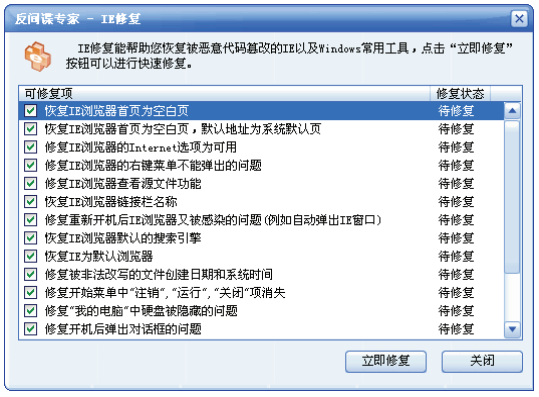

图 3-35　“IE 修复”对话框

Step 10 单击“隔离区”按钮，则可查看已经隔离的恶意代码，选择隔离的恶意项目可以对其进行恢复或清除操作，如图3-36所示。

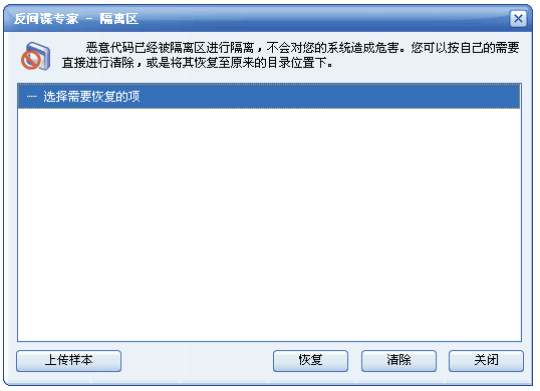

图 3-36　查看隔离的恶意代码

Step 11 单击“高级工具”功能栏，进入“高级工具”设置界面，如图3-37所示。

图 3-37　“高级工具”设置界面

Step 12 单击“进程管理”按钮，打开“进程管理器”对话框，在其中对进程进行相应的管理，如图3-38所示。

图 3-38　“进程管理器”对话框

Step 13 单击“服务管理”按钮，打开“服务

管理器”对话框，在其中可对服务进行相应的管理，如图3-39所示。

图 3-39　“服务管理器”对话框

Step 14 单击“网络连接管理”按钮，打开“网络连接管理器”对话框，在其中可对网络连接进行相应的管理，如图3-40所示。

图 3-40　“网络连接管理器”对话框

Step 15 选择“工具”→“综合设定”菜单项，打开“综合设定”对话框，在其中可对扫描设定进行相应的设置，如图3-41所示。

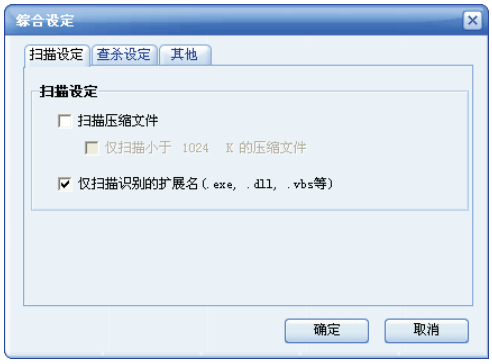

图 3-41　“综合设定”对话框

Step 16 选择“查杀设定”选项卡，进入“查杀设定”设置界面，在其中可设定发现恶意程序时的缺省动作，如图3-42所示。

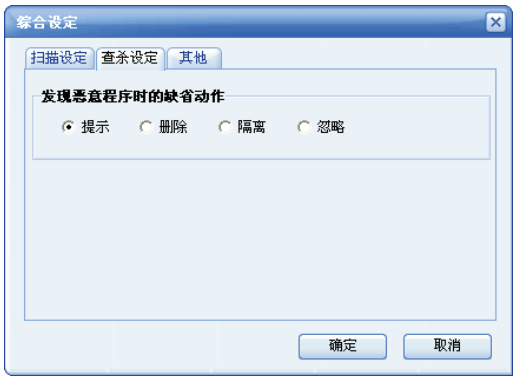

图 3-42　“查杀设定”选项卡

Step 17 选择“其他”选项卡，进入“其他”设置界面，在其中勾选“允许右键菜单选择扫描”复选框，单击“确定”按钮即可完成设置操作，如图3-43所示。

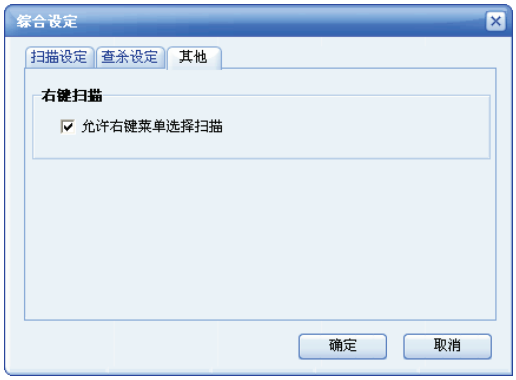

图 3-43　“其他”选项卡

3.2.3　用SpyBot-Search&Destroy查杀间谍软件

SpyBot-Search&Destroy是一款专门用来清理间谍程序的工具。目前，它已经可以检测1万多种间谍程序（Spyware），并对其中的1000多种进行免疫处理。这个软件是完全免费的，并有中文语言包支持，可以在Server级别的操作系统上使用。

使用SpyBot软件查杀间谍软件的基本步骤如下。

Step 01 安装Spybot-Search&Destroy并完成初始化设置之后，打开其主窗口，如图3-44所示。

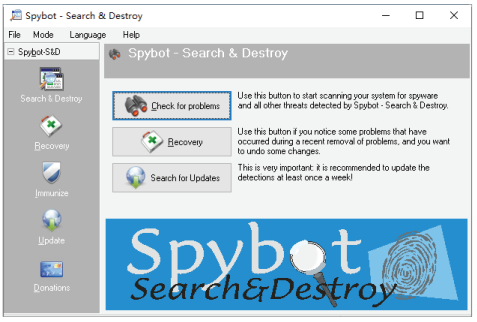

图 3-44　Spybot-Search&Destroy 工作界面

Step 02 由于该软件支持多种语言，可以在其主窗口中执行Languages→“简体中文”命令，将程序主界面切换为中文模式，如图3-45所示。

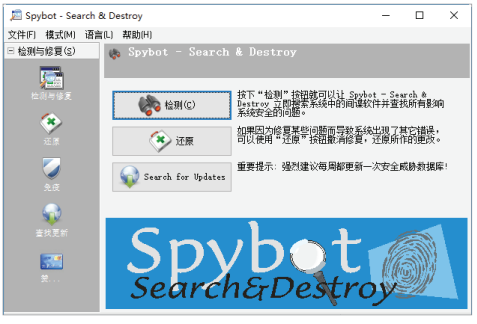

图 3-45　中文模式

Step 03 单击其中的“检测”按钮或单击左侧的“检查与修复”按钮，打开“检测与修复”窗口，单击“检测与修复”按钮，此时即可开始检查系统找到的存在的间谍软件，如图3-46所示。

图 3-46　“检测与修复”窗口

Step 04 在软件检查完毕之后，检查页上将会列出在系统中查到的可能有问题的软件。选取某个检查到的问题，再点击右侧的分栏箭头即可查询到有关该问题软件的发布公司，软件功能、说明和危害种类等信息，如图3-47所示。

图 3-47　显示检测到的信息

Step 05 选中需要修复的问题程序，单击“修复”按钮，打开“将要删除这些项目”提示信息框，如图3-48所示。

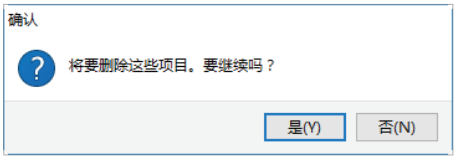

图 3-48　确认信息框

Step 06 单击“是”按钮，可看到在下次系统启动时自动运行提示框，如图3-49所示。

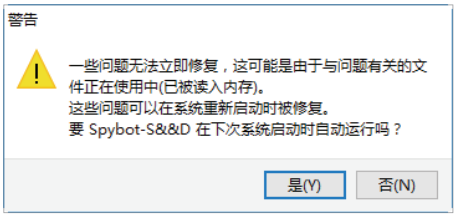

图 3-49　警告信息框

Step 07 单击“是”按钮，可将选取的间谍程序从系统中清除。修复后的结果如图3-50所示，其中以✔标识已经成功修复的问题，以✘标识修复不成功的问题。

Step 08 待修复完成后，可看到“确认”对话框。在其中会显示成功修复以及尚未修复

问题的数目，并建议重启计算机。此时只需单击“确定”按钮重启计算机修复未修复的问题即可，如图3-51所示。

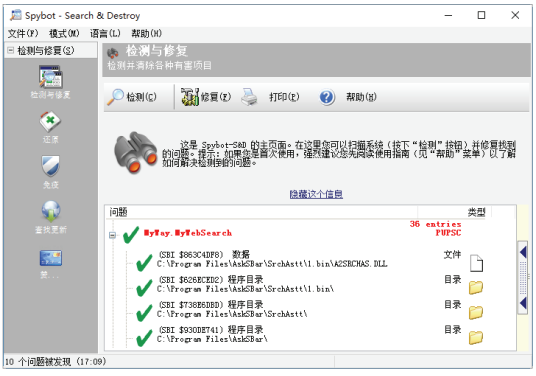

图 3-50　清除间谍程序

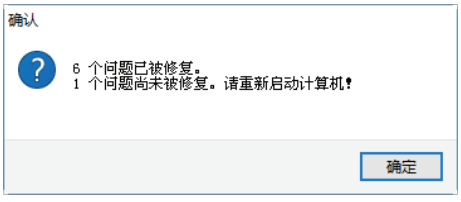

图 3-51　“确认”对话框

Step 09 选择“还原”选项，在打开的界面中选择需要还原的项目，单击“还原”按钮，如图3-52所示。

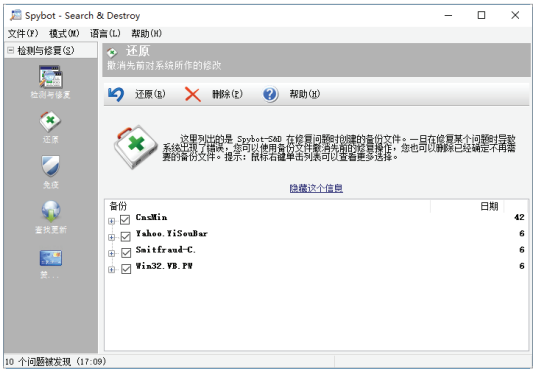

图 3-52　选择需要还原的项目

Step 10 打开“确认”信息提示框，提示用户是否要撤销先前所做的修改，如图3-53所示。

Step 11 单击“是”按钮，可将修复的问题还原到原来的状态，还原完毕后打开“信息”提示框，如图3-54所示。

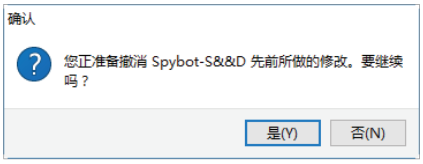

图 3-53　“确认”信息提示框

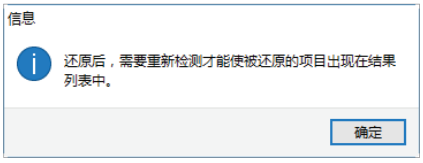

图 3-54　“信息”提示框

Step 12 选择“免疫”选项，进入“免疫”设置界面，免疫功能能使用户的系统具有抵御间谍软件的免疫效果，如图3-55所示。

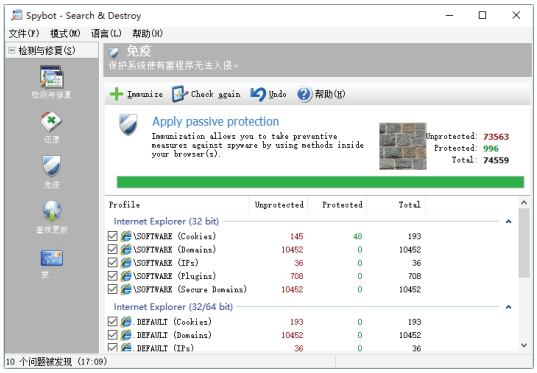

图 3-55　“免疫”设置界面

3.3　流氓软件清除工具

软件在安装的过程中，一些流氓软件也有可能会趁机强制安装进信息，并会在注册表中添加相关的信息，普通的卸载方法并不能将流氓软件彻底删除，如果想将其所有的信息删除掉，可以使用第三方软件来卸载。

3.3.1　使用360安全卫士卸载流氓软件

使用360软件管理可以卸载流氓软件，具体的操作步骤如下。

Step 01 启动360安全卫士，在打开的主界面中选择“电脑清理”选项，进入电脑清理

界面，如图3-56所示。

图 3-56　电脑清理界面

Step 02 在电脑清理界面中选择“清理插件”选项，然后单击“一键扫描”按钮，可扫描当前系统中的流氓软件，如图3-57所示。

图 3-57　扫描系统中的流氓软件

Step 03 扫描完成后，单击“一键清理”按钮，可对扫描出来的流氓软件进行清理，并给出清理完成后的信息提示，如图3-58所示。

图 3-58　清理流氓软件

Step 04 另外，还可以在“360安全卫士”窗口中单击“软件管家”按钮，进入“360软件管家”窗口，选择“卸载”选项卡，在“软件名称”列表中选择需要卸载的软件，如图3-59所示。

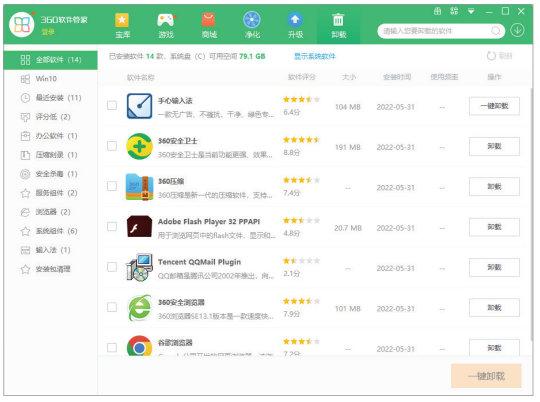

图 3-59　“360 软件管家”窗口

3.3.2　使用金山清理专家清除恶意软件

金山清理专家的首要功能就是查杀恶意软件，在安装完软件之后就可以对本地机器上恶意软件进行查杀，具体的操作步骤如下。

Step 01 双击桌面上的金山清理专家快捷图标，进入“金山清理专家”主窗口，如图3-60所示。

图 3-60　“金山清理专家”主窗口

Step 02 在“恶意软件查杀”选项卡中，可以对恶意软件、第三方插件和信任插件进行查杀，单击“恶意软件”选项，自动对恶意软件进行扫描，如图3-61所示。

Step 03 在扫描结束之后将显示出的扫描结

果，如果本机存在有恶意软件，在勾选扫描出的恶意软件之后，单击“清除选定项”按钮，可将恶意软件删除掉，如图3-62所示。

图 3-61　扫描恶意软件

图 3-62　删除恶意软件

3.4　实战演练

3.4.1　实战1：修补系统漏洞后手动重启

一般情况下，在Windows 10每次自动下载并安装好补丁后，就会每隔10分钟弹出窗口要求重启启动。如果不小心单击了“立即重新启动”按钮，则有可能会影响当前计算机操作的资料。那么如何才能不让Windows 10安装完补丁后自动弹出“重新启动”的信息提示框呢？具体的操作步骤如下。

Step 01 单击“⊞”按钮，在弹出的快捷菜单中选择“所有程序”→“附件”→“运行”选项，打开“运行”对话框，在“打开”文本框中输入gpedit.msc，如图3-63所示。

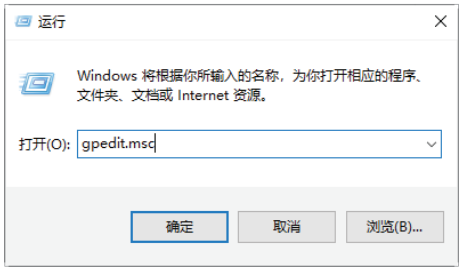

图 3-63　“运行”对话框

Step 02 单击“确定”按钮，打开“本地组策略编辑器”窗口，如图3-64所示。

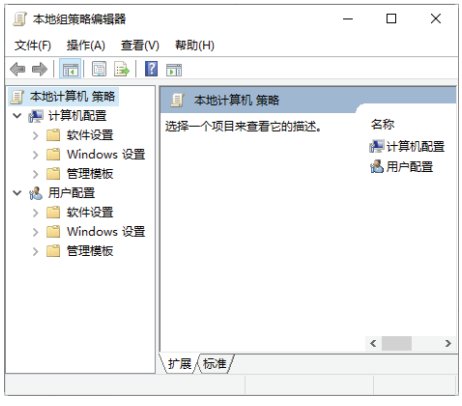

图 3-64　“本地组策略编辑器”窗口

Step 03 在窗口的左侧依次选择“计算机配置”→“管理模板”→“Windows 组件”选项，如图3-65所示。

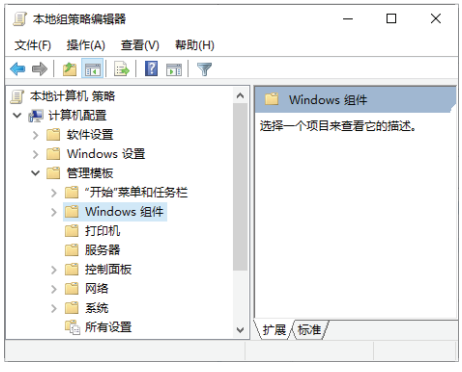

图 3-65　“Windows 组件”选项

Step 04 展开“Windows 组件”选项，在其子菜单中选择“Windows 更新”选项。此时，在右侧的窗格中将显示Windows更新的所有设置，如图3-66所示。

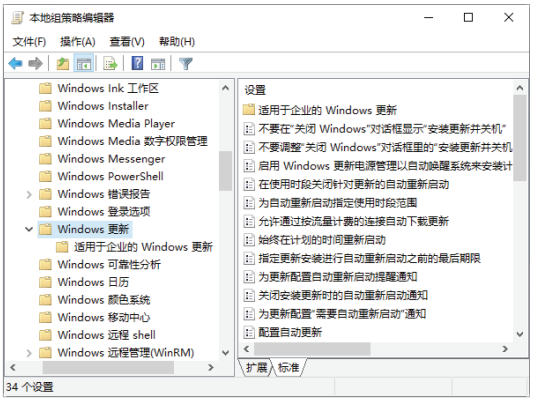

图 3-66 “Windows 更新”选项

Step 05 在右侧的窗格中选中“对于有已登录用户的计算机，计划的自动更新安装不执行重新启动”选项并右击，在弹出的快捷菜单中选择“编辑”选项，如图3-67所示。

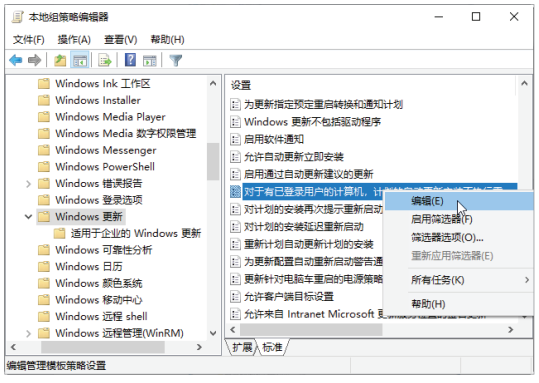

图 3-67 “编辑”选项

Step 06 随即打开“对于有已登录用户的计算机，计划的自动更新安装不执行重新启动”对话框，在其中选中“已启用”单选按钮，如图3-68所示。

Step 07 单击“确定”按钮，返回“组策略编辑器”窗口，此时用户可看到“对于有已登录用户的计算机，计划的自动更新安装不执行重新启动”选择的状态是“已启用”，如图3-69所示。这样，在自动更新完补丁后，将不会再弹出重新启动计算机的信息提示框。

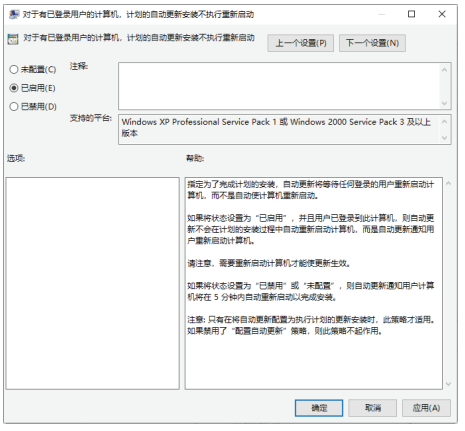

图 3-68 “已启用”单选按钮

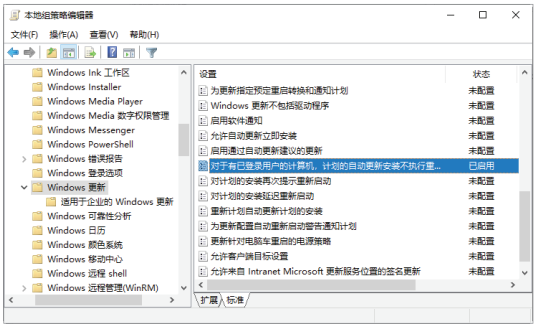

图 3-69 “已启用”状态

3.4.2 实战2：关闭开机多余启动项目

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

Step 01 按下键盘上的Ctrl+Alt+Delete组合键，打开如图3-70所示的界面。

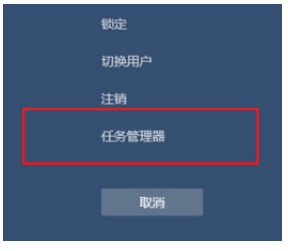

图 3-70 “任务管理器”选项

Step 02 单击“任务管理器”选项，打开“任务管理器”窗口，如图3-71所示。

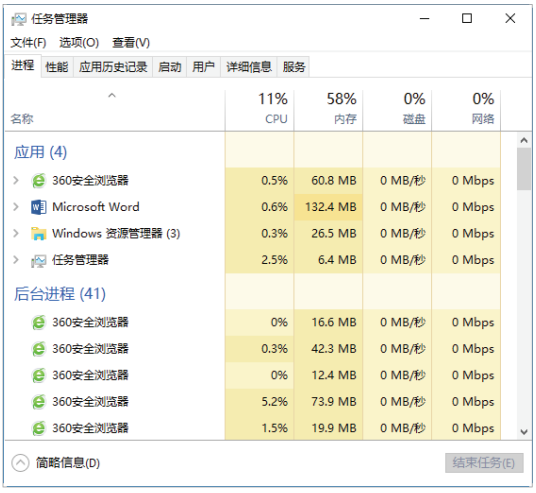

图 3-71 “任务管理器”窗口

Step 03 选择“启动”选项卡，进入“启动”界面，在其中可以看到系统中的开机启动项列表，如图3-72所示。

Step 04 选择开机启动项列表中需要禁用的启动项，单击“禁用”按钮，即可禁止该启动项开机自启，如图3-73所示。

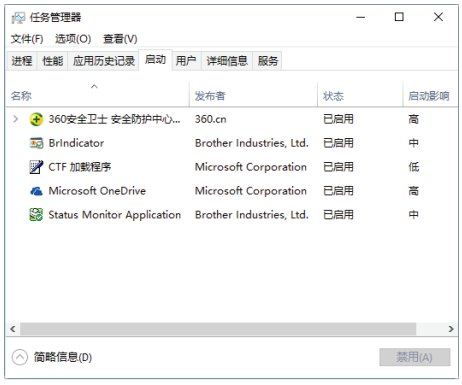

图 3-72 “启动”选项卡

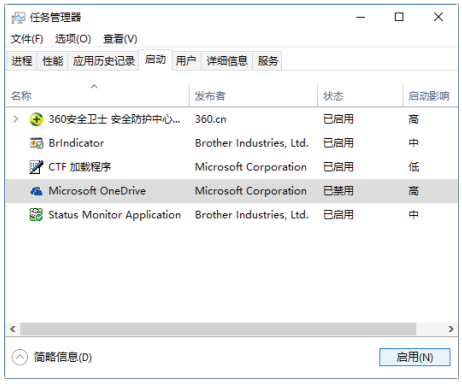

图 3-73　禁止开机启动项