第 1 章 电脑安全快速入门

作为电脑或网络终端设备的用户，要想使自己的设备不受或少受黑客的攻击，就需要了解一些黑客常用的入侵手段及学习电脑安全方面的知识。本章介绍一些电脑安全方面的基础知识，主要内容包括 IP 地址、MAC 地址、端口及黑客常用的 DOS 命令等。

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 IP 地址是黑客实施入侵攻击的一个关键。

1.1.1 IP 地址


微视频

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 共 5 类，其中 A、B、C 类 3 种是主要的类型地址，D 类专供多目传送地址，E 类用于扩展备用地址。

- A 类 IP 地址。一个 A 类 IP 地址由 1 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”，地址范围为 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”，地址范围为 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”。地址范围为 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，它是一个专门保留的地址。它并不指向特定的网络，目前这一类地址被用在多点广播（Multicast）中。多点广播地址用来一次寻址一组计算机，它标识共享同一协议的一组计算机。
- E 类 IP 地址。以“10”开始，为将来使用保留，全“0”（0.0.0.0）IP 地址对应于当前主机；

全“1”的 IP 地址（255.255.255.255）是当前子网的广播地址。

具体来讲，一个完整的 IP 地址信息应该包括 IP 地址、子网掩码、默认网关和 DNS 等 4 个部分。只有这些部分协同工作，互联网中的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。

Step01 右击“开始”按钮，在弹出的快捷菜单中选择“运行”选项，如图 1-1 所示。

Step02 弹出“运行”对话框，在“打开”文本框中输入 cmd 命令，如图 1-2 所示。

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 1-3 所示。

图 1-1　选择“运行”选项

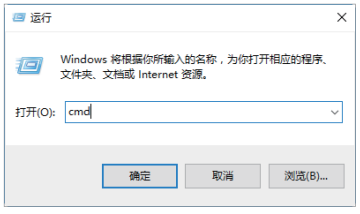

图 1-2　输入 cmd 命令

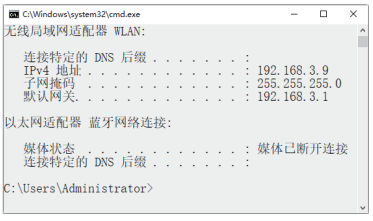

图 1-3　查看 IP 地址

提示：在“命令提示符”窗口中，192.168.0.130 表示本机在局域网中的 IP 地址。

1.1.2　MAC 地址


微视频

MAC 地址是在媒体接入层上使用的地址，也称为物理地址、硬件地址或链路地址，由网络设备制造商生产时写在硬件内部。MAC 地址与网络无关，即无论将带有这个地址的硬件（如网卡、集线器、路由器等）接入到网络的何处，MAC 地址都是相同的，它由厂商写在网卡的 BIOS 里。

1. 认识MAC地址

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

知识链接

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

2. 查看MAC地址

在“命令提示符”窗口中输入 ipconfig /all 命令，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。

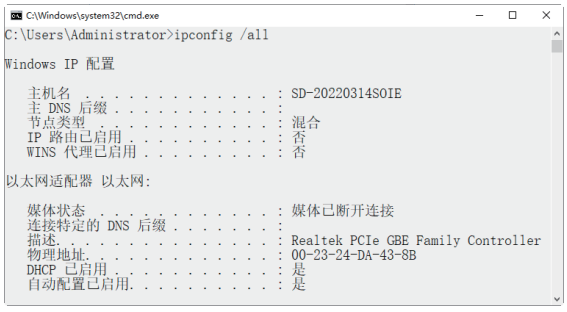

图 1-4　查看 MAC 地址

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


微视频

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。

Step01 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。

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 1-6 所示。

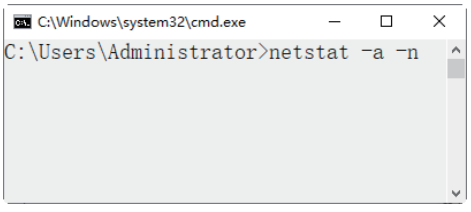

图 1-5　输入 netstat -a -n 命令

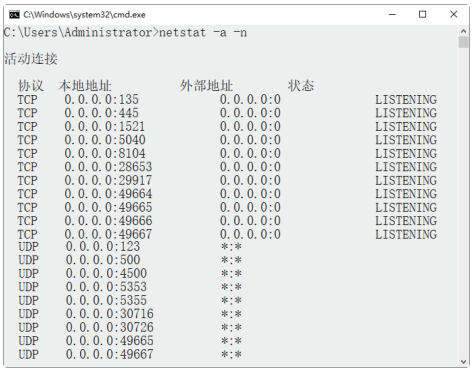

图 1-6　TCP 和 UCP 连接的端口号

1.2.2　关闭不必要的端口


微视频

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

下面以关闭 WebClient 服务为例，具体的操作步骤如下。

Step01 右击“开始”按钮，在弹出的快捷菜单中选择“控制面板”选项，如图 1-7 所示。

Step02 打开“控制面板”窗口，双击“管理工具”图标，如图 1-8 所示。

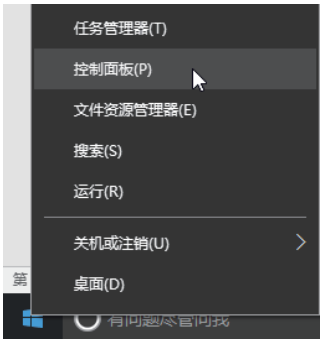

图 1-7　选择“控制面板”选项

图 1-8　“控制面板”窗口

Step03 打开“管理工具”窗口，双击“服务”图标，如图 1-9 所示。

Step04 打开“服务”窗口，找到 WebClient 服务项，如图 1-10 所示。

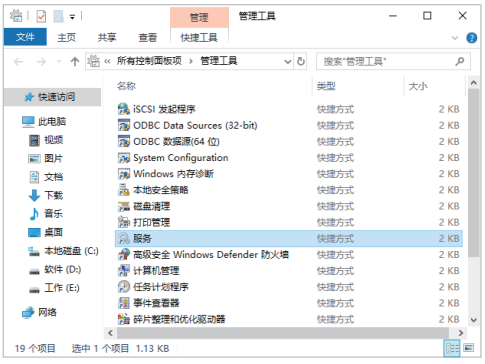

图 1-9　“服务”图标

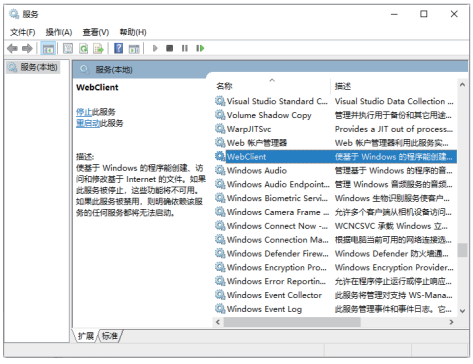

图 1-10　“服务”窗口

Step05 双击该服务项，弹出“WebClient 的属性”对话框，在“启动类型”下拉列表中选择“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。

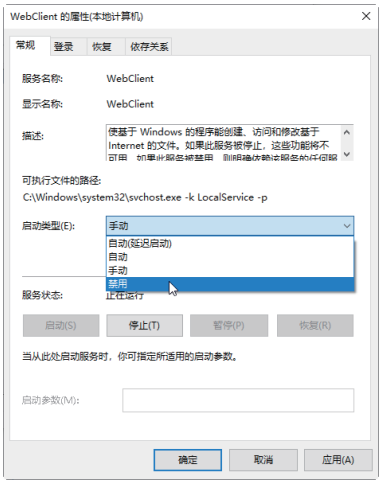

图 1-11　选择“禁用”选项

1.2.3　启动需要开启的端口

微视频

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

Step01 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。

Step02 单击“应用”按钮，激活“服务状态”下的“启动”按钮，如图 1-13 所示。

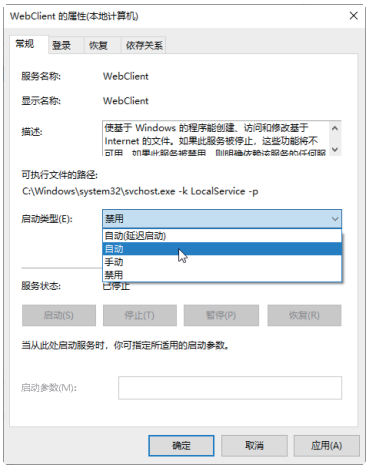

图 1-12　选择“自动”选项

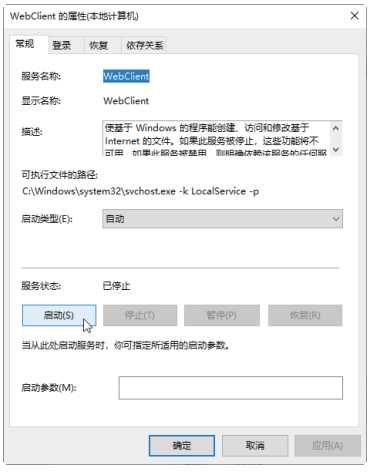

图 1-13　单击“启动”按钮

Step03 单击“启动”按钮，启动该项服务，再次单击“应用”按钮，在“WebClient 的属性”对话框中可以看到该服务的“服务状态”已经变为“正在运行”，如图 1-14 所示。

Step04 单击“确定”按钮，返回“服务”窗口，此时即可发现 WebClient 服务的“状态”变为“正在运行”，这样就可以成功开启 WebClient 服务对应的端口，如图 1-15 所示。

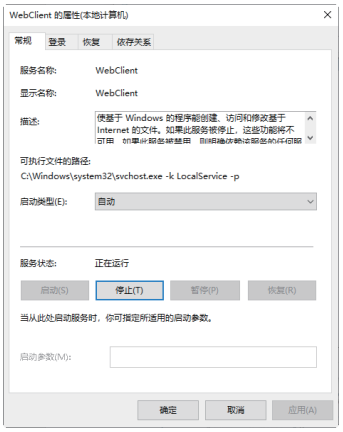

图 1-14　启动服务项

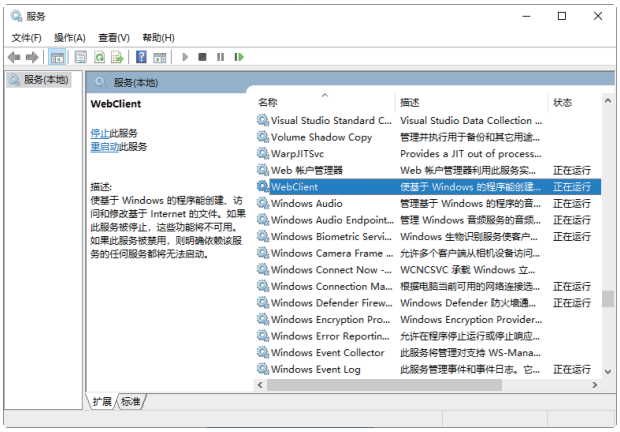

图 1-15　WebClient 服务的状态为“正在运行”

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，本节介绍黑客常用的一些 DOS 命令。了解这样的命令可以帮助计算机用户追踪黑客的踪迹，从而提高个人计算机的安全性。


微视频

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。

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

Step01 在“命令提示符”窗口中输入 cd c:\ 命令，按 Enter 键将目录切换为 C:\，如图 1-16 所示。

Step02 如果想进入 C:\Windows\system32 目录中，则需在上面的“命令提示符”窗口中输入 cd Windows\system32 命令，按 Enter 键将目录切换为 C:\Windows\system32，如图 1-17 所示。

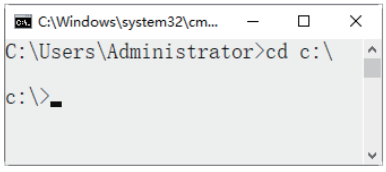

图 1-16　目录切换到 C 盘根目录

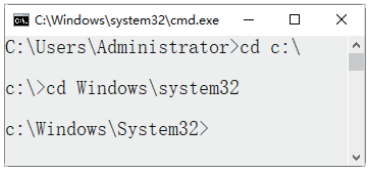

图 1-17　切换到 C 盘子目录

Step03 如果想返回上一级目录，则可以在“命令提示符”窗口中输入 cd.. 命令，按 Enter 键，如图 1-18 所示。

Step04 如果想返回根目录，则可以在“命令提示符”窗口中输入 cd\ 命令，按 Enter 键，如图 1-19 所示。

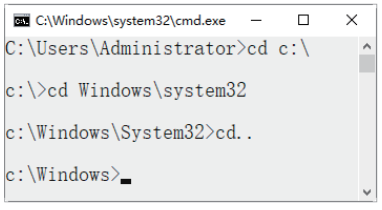

图 1-18　返回上一级目录

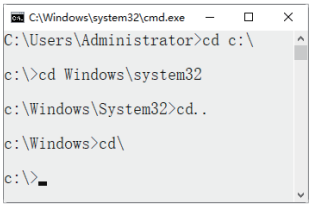

图 1-19　返回根目录


微视频

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。

Step01 在“命令提示符”窗口中输入 dir 命令，按 Enter 键，查看当前目录下的文件列表，如图 1-20 所示。

Step02 在“命令提示符”窗口中输入 dir d:/ a:d 命令，按 Enter 键，查看 D 盘下的所有文件的目录，如图 1-21 所示。

Step03 在“命令提示符”窗口中输入 dir c:\windows /a:h 命令，按 Enter 键，列出 C:\windows 目录下的隐藏文件，如图 1-22 所示。

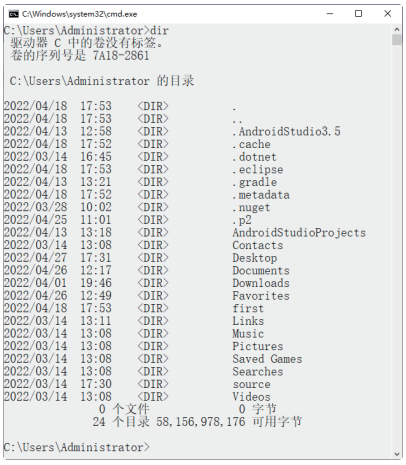

图 1-20　Administrator 目录下的文件列表

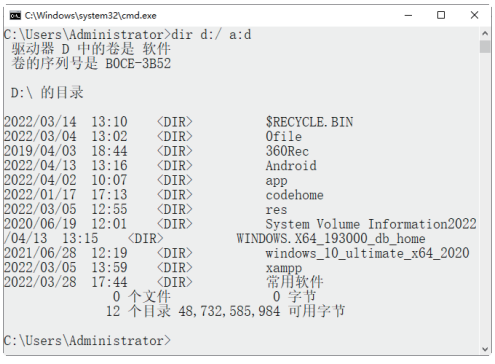

图 1-21　D 盘下的文件列表

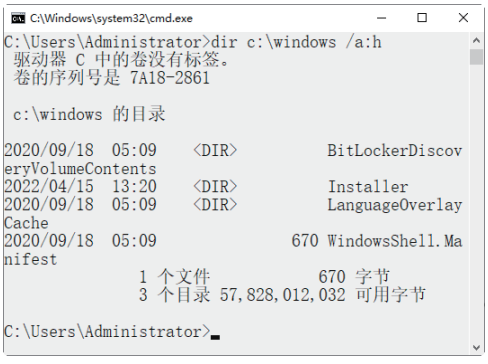

图 1-22　C 盘下的隐藏文件

1.3.3　ping 命令

ping 命令是 TCP/IP 中常用的命令，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。

使用 ping 命令对计算机的连接状态进行测试的具体操作步骤如下。

Step01 使用 ping 命令来判断计算机的操作系统类型。在“命令提示符”窗口中输入 ping 192.168.3.9 命令，运行结果如图 1-24 所示。

Step02 在“命令提示符”窗口中输入 ping 192.168.3.9 -t -l 128 命令，可以不断向某台主机发出大量的数据包，如图 1-25 所示。

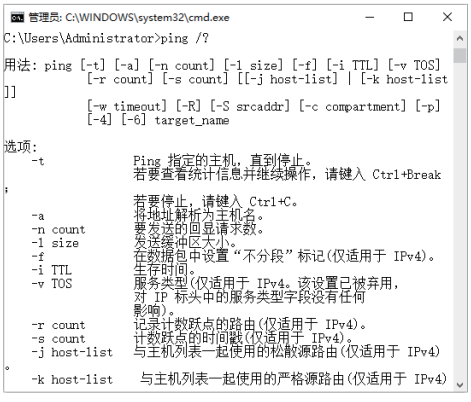

图 1-23　ping 命令的帮助信息

Step03 判断本台计算机是否与外界网络连通。在“命令提示符”窗口中输入 ping www.baidu.com 命令，其运行结果如图 1-26 所示，图中说明本台计算机与外界网络连通。

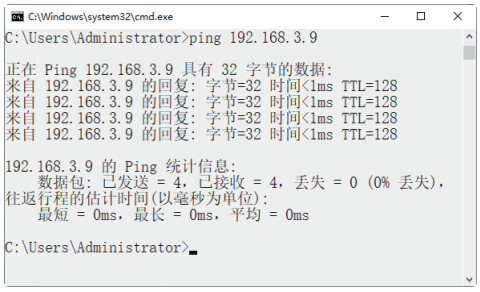

图 1-24　判断计算机的操作系统类型

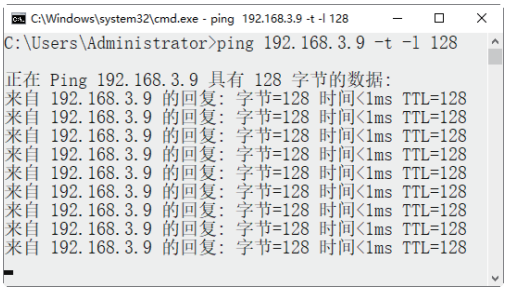

图 1-25　发出大量数据包

Step04 解析某 IP 地址的计算机名。在“命令提示符”窗口中输入 ping -a 192.168.3.9 命令，其运行结果如图 1-27 所示，可知这台主机的名称为 SD-20220314SOIE。

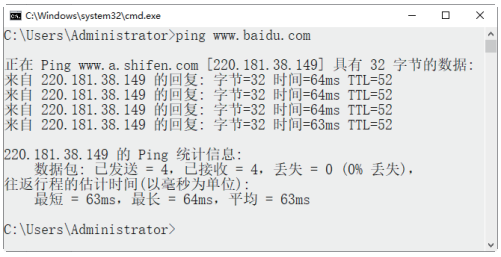

图 1-26　网络连通信息

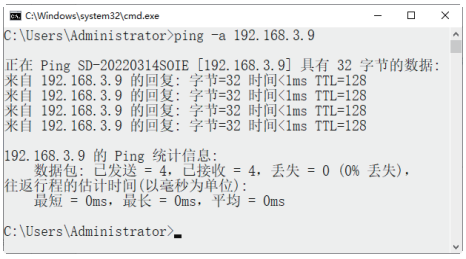

图 1-27　解析某 IP 地址的计算机名


微视频

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。

Step01 使用 net 命令查看网络状态。打开“命令提示符”窗口，输入 net start 命令，如图 1-28 所示。

Step02 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。

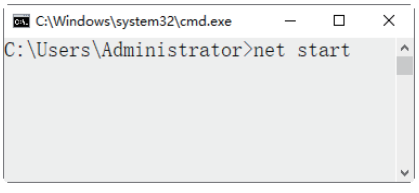

图 1-28　输入 net start 命令

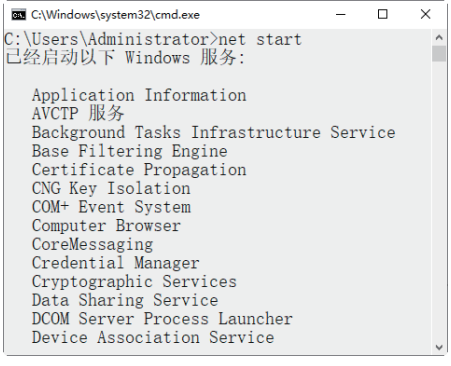

图 1-29　计算机所启动的 Windows 服务

1.3.5　netstat 命令


微视频

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/?，可以得到这条命令的帮助信息，如图 1-30 所示。

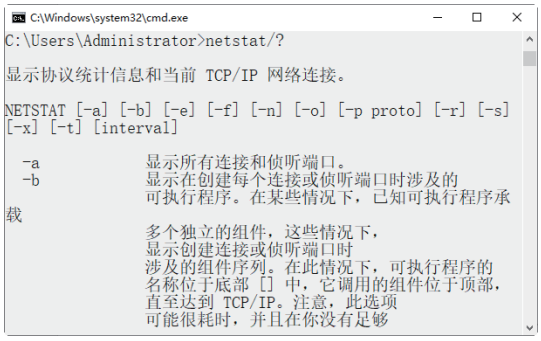

图 1-30　netstat 命令帮助信息

该命令的语法格式信息如下：

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

其中比较重要的参数的含义如下。

- -a：显示所有连接和监听端口。
- -n：以数字形式显示地址和端口号。

使用 netstat 命令查看网络连接的具体操作步骤如下。

Step01 打开“命令提示符”窗口，在其中输入 netstat -n 或 netstat 命令，按 Enter 键，查看服务器活动的 TCP/IP 连接，如图 1-31 所示。

Step02 在“命令提示符”窗口中输入 netstat -r 命令，按 Enter 键，查看本机的路由信息，如图 1-32 所示。

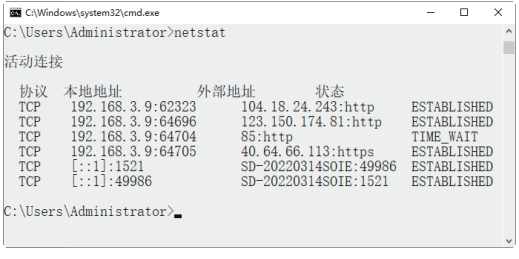

图 1-31　服务器活动的 TCP/IP 连接

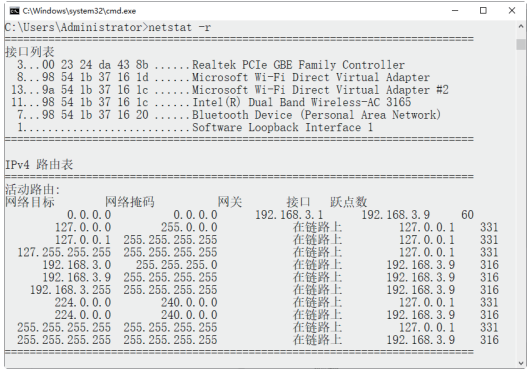

图 1-32　查看本机的路由信息

Step03 在“命令提示符”窗口中输入 netstat -a 命令，按 Enter 键，查看本机所有活动的 TCP 连接，如图 1-33 所示。

Step04 在“命令提示符”窗口中输入 netstat -n -a 命令，按 Enter 键，显示本机所有连接的端口及其状态，如图 1-34 所示。

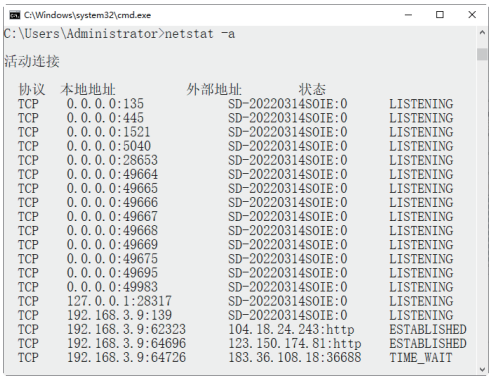

图 1-33　查看本机所有活动的 TCP 连接

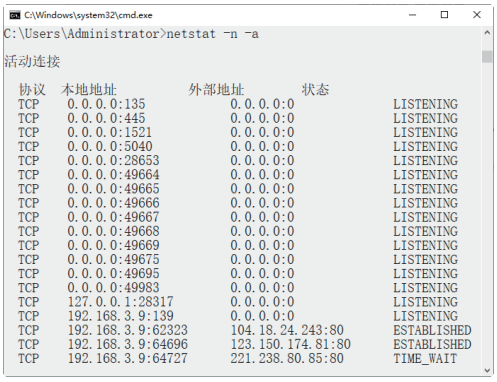

图 1-34　显示本机所有连接的端口及其状态


微视频

1.3.6　tracert 命令

使用 tracert 命令可以查看网络中路由节点信息，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：指定搜索目标地址的最大跳跃数，默认为 30 个跳跃点。
- -j Hostlist：按照主机列表中的地址释放源路由。
- -w Timeout：指定超时时间间隔，默认单位为 ms。
- TargetName：指定目标计算机。

例如：如果想查看 www.baidu.com 的路由与局域网络连接情况，则在“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。

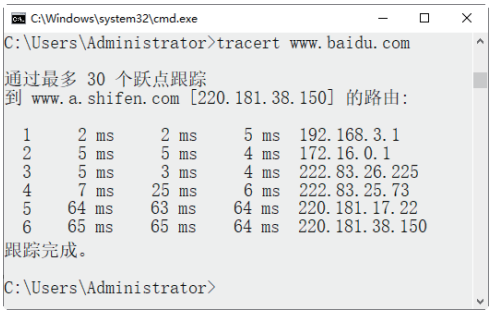

图 1-35　查看网络中路由节点信息

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]
```

其中各个参数的含义如下。

- /S system：指定连接到的远程系统。
- /U [domain\]user：指定使用哪个用户执行这个命令。
- /P [password]：为指定的用户指定密码。
- /M [module]：列出调用指定的 DLL 模块的所有进程。如果没有指定模块名，显示每个进程加载的所有模块。
- /SVC：显示每个进程中的服务。
- /V：显示详细信息。
- /FI filter：显示一系列符合筛选器指定的进程。
- /FO format：指定输出格式，有效值：TABLE、LIST、CSV。
- /NH：指定输出中不显示栏目标题。只对 TABLE 和 CSV 格式有效。

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

Step01 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。

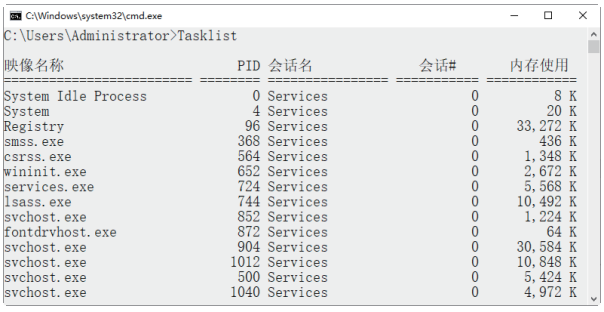

图 1-36　查看本机进程

Step02 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，如图 1-37 所示。

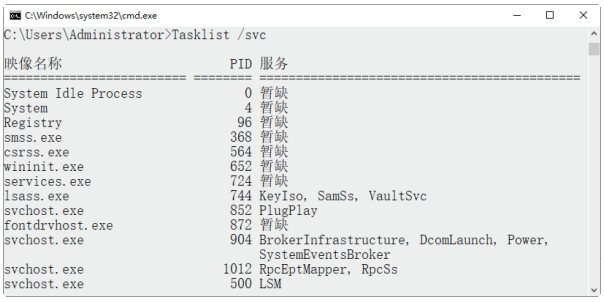

图 1-37　查看本机进程 svchost.exe 提供的服务

Step03 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。

Step04 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”。

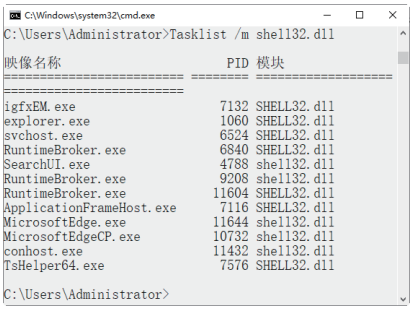

图 1-38　显示调用 shell32.dll 模块的进行

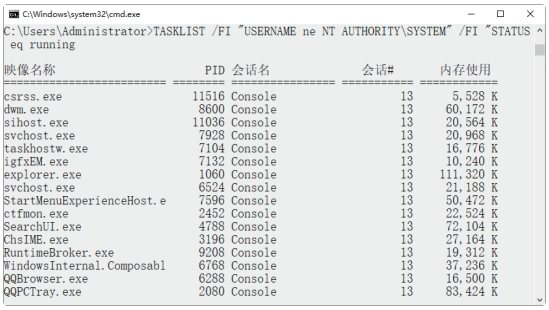

图 1-39　列出系统中正在运行的非 SYSTEM 状态的所有进程

1.4　实战演练


微视频

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。

Step01 右击“开始”按钮，在弹出的快捷菜单中选择“运行”选项，弹出“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。

Step02 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。

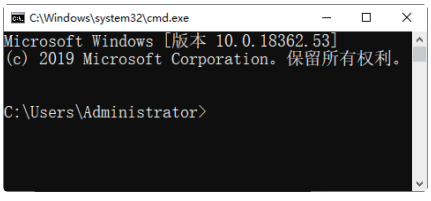

图 1-40　“命令提示符”窗口

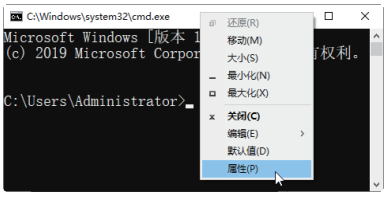

图 1-41　“属性”选项

Step03 弹出“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。

Step04 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。

图 1-42　设置屏幕背景

图 1-43　设置屏幕文字

Step 05 单击“确定”按钮，返回“命令提示符”窗口，可以看到命令提示符窗口的显示方式变为白底黑字样式，如图 1-44 所示。

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


微视频

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。

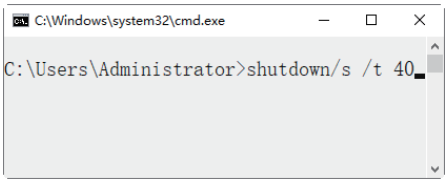

图 1-45　输入 shutdown/s /t 40 命令

Step 02 弹出一个即将注销用户登录的信息对话框，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，可在命令行中输入 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　信息对话框

图 1-47　取消关机操作

第 2 章

电脑系统漏洞的安全防护

目前，用户普遍使用的操作系统为 Windows 10 操作系统。该系统也存在这样或那样的漏洞，这就给黑客留下了入侵攻击的机会。因此，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。本章介绍电脑系统漏洞的安全防护，主要内容包括系统漏洞的相关概述、典型系统漏洞的入门与防御及系统漏洞的修补等。

2.1 系统漏洞概述

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，从而达到其控制目标主机或造成一些更具破坏性影响的目的。

2.1.1 什么是系统漏洞

系统漏洞是指应用软件或操作系统软件在逻辑设计上的缺陷或在编写时产生的错误。某个程序（包括操作系统）在设计时未被考虑周全，则这个缺陷或错误将可能被不法分子或黑客利用，通过植入木马病毒等方式来攻击或控制整个计算机，从而窃取计算机中的重要资料和信息，甚至破坏系统。

系统漏洞又称为安全缺陷，可对用户造成不良后果，若漏洞被恶意用户利用，会造成信息泄露。黑客攻击网站即是利用网络服务器操作系统的漏洞，对用户操作造成不便，如出现不明原因的死机和丢失文件等情况。

2.1.2 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。归结起来，其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：由于硬件的原因，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发展水平所限，在程序中难免存在不足之处，而这些不足恰恰会导致系统漏洞的产生。

2.2　RPC 服务远程漏洞

RPC 协议是 Windows 操作系统使用的一种协议，提供了系统中进程之间的交互通信，允许在远程主机上运行任意程序。在 Windows 操作系统中使用的 RPC 协议，包括 Microsoft 及其他一些特定的扩展。系统大多数的功能和服务都依赖于它，是操作系统中极为重要的一个服务。

2.2.1　认识 RPC 服务远程漏洞


微视频

RPC 全称是 Remote Procedure Call，在操作系统中，它默认是开启的，为各种网络通信和管理提供了极大的方便，但也是危害极为严重的漏洞攻击点，曾经的冲击波、震荡波等大规模攻击和蠕虫病毒都是 Windows 系统的 RPC 服务漏洞造成的。可以说，每一次的 RPC 服务漏洞的出现且被攻击，都会给网络系统带来一场灾难。

启动 RPC 服务的具体操作步骤如下。

Step01 在 Windows 操作界面中选择“开始”→“Windows 系统”→“控制面板”→“管理工具”选项，打开“管理工具”窗口，如图 2-1 所示。

Step02 在“管理工具”窗口中双击“服务”图标，打开“服务”窗口，如图 2-2 所示。

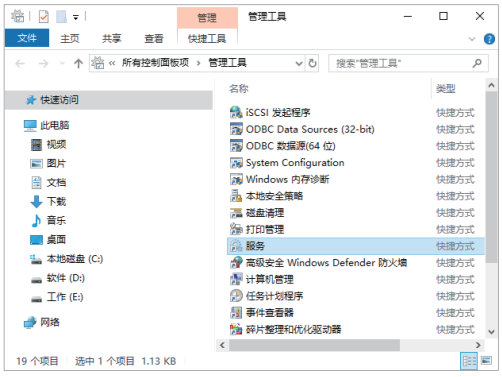

图 2-1　“管理工具”窗口

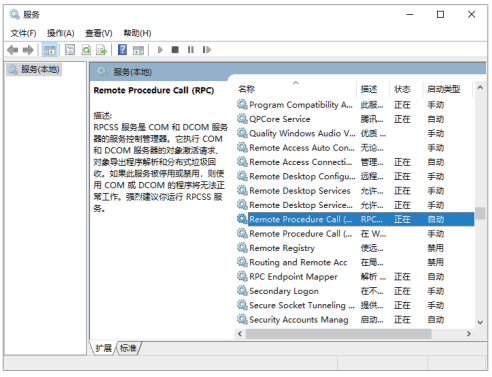

图 2-2　“服务”窗口

Step03 在服务（本地）列表中双击“Remote Procedure Call（RPC）”选项，弹出“Remote Procedure Call（RPC）属性”对话框，在“常规”选项卡中可以查看该协议的启动类型，如图 2-3 所示。

Step04 选择“依存关系”选项卡，在显示的界面中可以查看一些服务的依赖关系，如图 2-4 所示。

图 2-3　“常规”选项卡

图 2-4　“依存关系”选项卡

分析：从上图的显示服务可以看出，受 RPC 服务影响的系统组件有很多，其中包括了 DCOM 接口服务，这个接口用于处理由客户端机器发送给服务器的 DCOM 对象激活请求（如 UNC 路径）。攻击者若成功利用此漏洞则可以以本地系统权限执行任意指令，还可以在系统上执行任意操作，如安装程序，查看、更改或删除数据，建立系统管理员权限的账户等。

若想对 DCOM 接口进行相应的配置，其具体操作步骤如下。

Step01 执行“开始”→“运行”命令，在弹出的“运行”对话框中输入 Dcomcnfg 命令，如图 2-5 所示。

Step02 单击“确定”按钮，打开“组件服务”窗口，单击“组件服务”前面的“ ”号，依次展开各项，直到出现“DCOM 配置”选项为止，即可查看 DCOM 中各个配置对象，如图 2-6 所示。

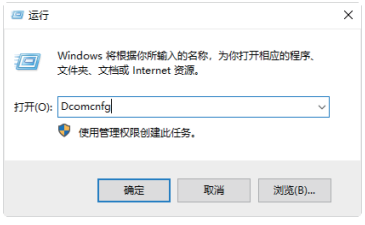

图 2-5 “运行”对话框

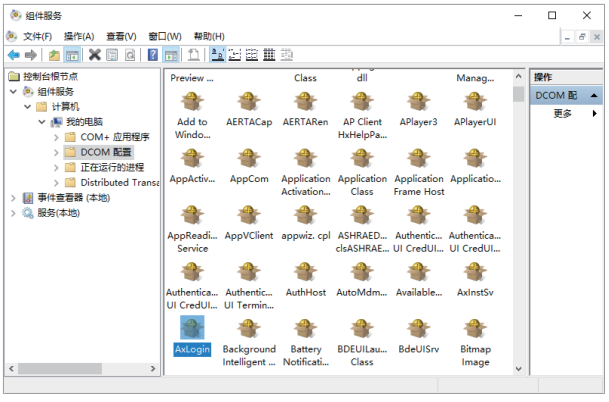

图 2-6 “组件服务”窗口

Step03 根据需要选择 DCOM 配置的对象，如 AxLogin，选定其并右击，从弹出的快捷菜单中选择“属性”选项，弹出“AxLogin 属性”对话框，在“身份验证级别”下拉列表中根据需要选择相应的选项，如图 2-7 所示。

Step04 选择“位置”选项卡，在打开的界面中对 AxLogin 对象进行位置的设置，如图 2-8 所示。

图 2-7 “AxLogin 属性”对话框

图 2-8 “AxLogin 位置”选项卡

Step05 选择“安全”选项卡，在打开的界面中对 AxLogin 对象的启动和激活权限、访问权限和配置权限进行设置，如图 2-9 所示。

Step06 选择“终结点”选项卡，在打开的界面中对 AxLogin 对象进行终结点的设置，如图 2-10 所示。

Step07 选择“标识”选项卡，在打开的界面中对 AxLogin 对象进行标识的设置，选择运行此应用程序的用户账户。设置完成后，单击“确定”按钮，如图 2-11 所示。

图 2-9　“AxLogin 安全”选项卡

图 2-10　“AxLogin 终结点”选项卡

图 2-11　“AxLogin 标识”选项卡

提示：由于 DCOM 可以远程操作其他计算机中的 DCOM 程序，而技术使用的是用于调用其他计算机所具有的函数的 RPC（在远程过程中调用），因此，利用这个漏洞，攻击者只需要发送特殊形式的请求到远程计算机上的 135 端口，轻则可以造成拒绝服务攻击，重则远程攻击者可以以本地管理员权限执行任何操作。

2.2.2　RPC 服务远程漏洞入侵演示

微视频

DcomRpc 接口漏洞对 Windows 操作系统乃至整个网络安全的影响，可以说超过了以往任何一个系统漏洞。其主要原因是 DCOM 是目前几乎各种版本的 Windows 系统的基础组件，应用比较广泛。下面以 DcomRpc 接口漏洞的溢出为例，为大家详细讲述溢出的方法。

Step01 将下载好的 DComRpc.xpn 插件复制到 X-Scan 的 plugins 文件夹中，作为 X-Scan 插件，如图 2-12 所示。

Step02 运行 X-Scan 扫描工具，选择“设置”→“扫描参数”选项，弹出“扫描参数”对话框，再选择“全局设置”→“扫描模块”选项，即可看到添加的“DcomRpc 溢出漏洞”模块，如图 2-13 所示。

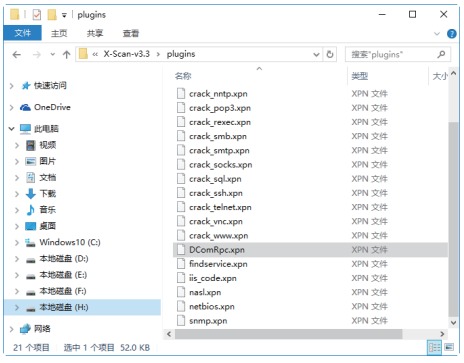

图 2-12　plugins 文件夹

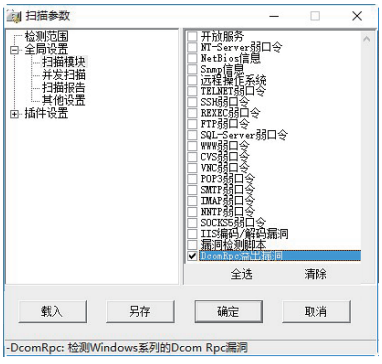

图 2-13　“扫描参数”对话框

Step 03 在使用 X-Scan 扫描到具有 DcomRpc 接口漏洞的主机时，可以看到在 X-Scan 中有明显的提示信息，并给出相应的 HTML 格式的扫描报告，如图 2-14 所示。

Step 04 如果使用 RpcDcom.exe 专用 DcomRPC 溢出漏洞扫描工具，则可先打开“命令提示符”窗口，进入 RpcDcom.exe 所在文件夹，执行“RpcDcom -d　IP 地址”命令后开始扫描并会给出最终的扫描结果，如图 2-15 所示。

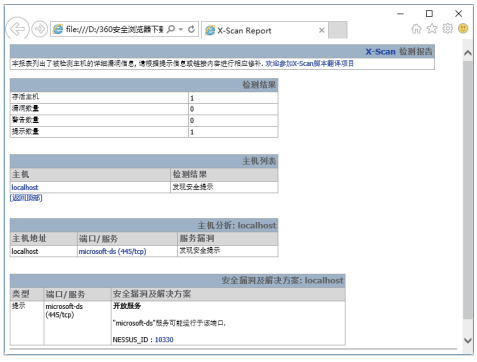

图 2-14　扫描报告

图 2-15　“命令提示符”窗口


微视频

2.2.3　修补 RPC 服务远程漏洞

RPC 服务远程漏洞可以说是 Windows 系统中最为严重的一个系统漏洞，下面介绍几个 RPC 服务远程漏洞的防御方法，以使自己的计算机或系统处于相对安全的状态。

1. 及时为系统打补丁

防御系统出现漏洞最直接、有效的解决方法是打补丁，对于 RPC 服务远程溢出漏洞的防御也是如此。不过在对系统打补丁时，务必要注意补丁相应的系统版本。

2. 关闭RPC服务

关闭 RPC 服务也是防范 DcomRpc 漏洞攻击的方法之一，而且效果非常彻底。其具体的方法为：选择“开始”→“设置”→“控制面板”→“管理工具”选项，在打开的“管理工具”窗口中双击“服务”图标，打开“服务”窗口。在其中双击“Remote Procedure Call”服务项，打开其属性窗口。在属性窗口中将启动类型设置为“禁用”，这样自下次开机开始 RPC 将不再开机启动，如图 2-16 所示。

另外，还可以在注册表编辑器中将 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\RpcSs 的 Start 的值由 4 变成 2，重新启动计算机，如图 2-17 所示。

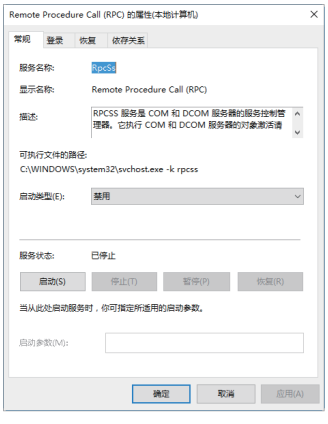

图 2-16　“常规”选项卡

图 2-17　设置 Start 的值为 2

不过，进行这种设置后，将会给 Windows 的运行带来很大的影响，如 Windows 10 从登录系统到显示桌面画面，要等待相当长的时间。这是因为 Windows 的很多服务依赖于 RPC，在将 RPC 设置为无效后，这些服务将无法正常启动。所以，这种方式的弊端非常大，一般不能采用。

3. 手动为计算机启用（或禁用）DCOM

针对具体的 RPC 服务组件，用户还可以采用具体的方法进行防御。例如，禁用 RPC 服务组件中的 DCOM 服务。可以采用如下方式进行，这里以 Windows 10 操作系统为例，其具体的操作步骤如下。

Step01 选择“开始”→“运行”选项，弹出“运行”对话框，输入 Dcomcnfg 命令，单击“确定”按钮，打开“组件服务”窗口，选择“控制台根目录”→“组件服务”→“计算机”→“我的电脑”选项，进入“我的电脑”文件夹。对于本地计算机，需要右击“我的电脑”选项，从弹出的快捷菜单中选择“属性”选项，如图 2-18 所示。

Step02 弹出“我的电脑 属性”对话框，选择“默认属性”选项卡，进入“默认属性”设置界面，取消对“在此计算机上启用分布式 COM（E）”复选框的勾选，然后单击“确定”按钮即可，如图 2-19 所示。

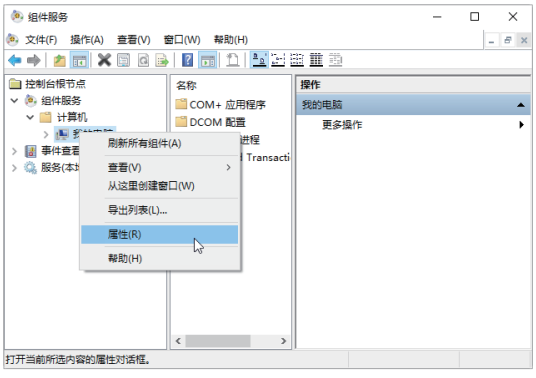

图 2-18　“属性”选项

图 2-19　“我的电脑 属性”对话框

Step03 若对于远程计算机，则需要右击“计算机”选项，从弹出的快捷菜单中选择“新建”→“计算机”选项，弹出“添加计算机”对话框，如图 2-20 所示。

Step04 在“添加计算机”对话框中，直接输入计算机名或单击右侧的“浏览”按钮来搜索计算机，如图 2-21 所示。

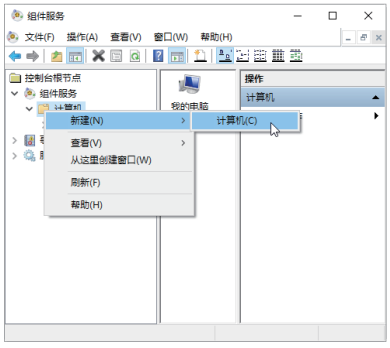

图 2-20　“计算机”选项

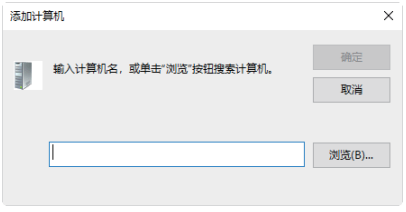

图 2-21　“添加计算机”对话框

2.3 WebDAV 缓冲区溢出漏洞

WebDAV 漏洞也是系统中常见的漏洞之一，黑客利用该漏洞进行攻击，可以获取系统管理员的最高权限。

2.3.1 认识 WebDAV 缓冲区溢出漏洞

WebDAV 缓冲区溢出漏洞出现的主要原因是 IIS 服务（Internet Information Server，互联网信息服务）默认提供了对 WebDAV 的支持。WebDAV 可以通过 HTTP 向用户提供远程文件存储的服务，但是该组件不能充分检查传递给部分系统组件的数据，这样远程攻击者利用这个漏洞就可以对 WebDAV 进行攻击，从而获得 LocalSystem 权限，进而完全控制目标主机。


微视频

2.3.2 WebDAV 缓冲区溢出漏洞入侵演示

下面简单介绍 WebDAV 缓冲区溢出攻击的过程。入侵之前攻击者需要准备两个程序，即 WebDAV 漏洞扫描器——WebDAVScan.exe 和溢出工具 webdavx3.exe，其具体的操作步骤如下。

Step01 下载并解压缩 WebDAV 漏洞扫描器，在解压后的文件夹中双击 WebDAVScan.exe 可执行文件，打开其操作主界面，在“起始 IP”和“结束 IP”文本框中输入要扫描的 IP 地址范围，如图 2-22 所示。

Step02 输入完毕后，单击“扫描”按钮，开始扫描目标主机，该程序运行速度非常快，可以准确地检测出远程 IIS 服务器是否存在 WebDAV 漏洞，在扫描列表中的 WebDAV 列中凡是标明 Enable 的则说明该主机存在漏洞，如图 2-23 所示。

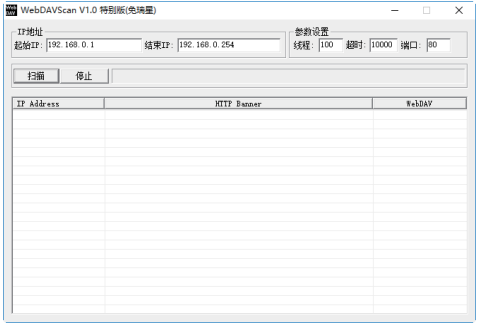

图 2-22 设置 IP 地址范围

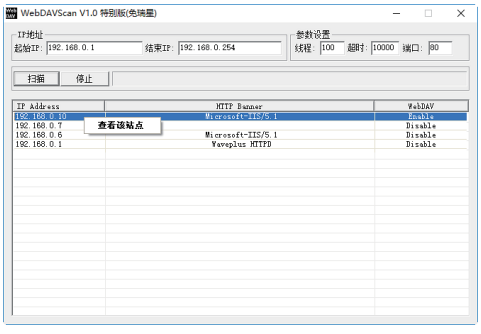

图 2-23 扫描结果

Step03 选择“开始”→“运行”选项，在弹出的“运行”对话框中输入 cmd 命令，单击“确定”按钮，打开“命令提示符”窗口，输入 cd c:\ 命令，进入 C 盘目录之中，如图 2-24 所示。

Step04 在 C 盘目录之中输入 webdavx3.exe 192.168.0.10 命令，并按 Enter 键，开始溢出攻击，如图 2-25 所示。

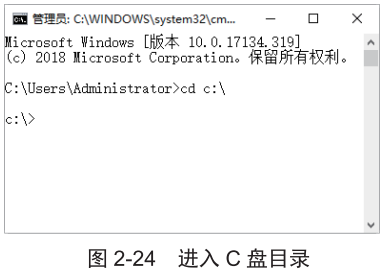

图 2-24 进入 C 盘目录

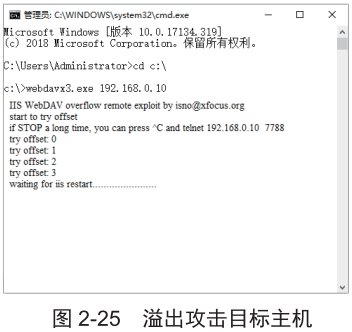

图 2-25 溢出攻击目标主机

其运行结果如下：

```
IIS WebDAV overflow remote exploit by isno@xfocus.org
start to try offset
if STOP a long time, you can press ^C and telnet 192.168.0.10  7788
try offset: 0
try offset: 1
try offset: 2
try offset: 3
waiting for iis restart.....................
```

Step05 如果出现上面的结果则表明溢出成功，稍等两三分钟后，按 Ctrl+C 组合键结束溢出，再在“命令提示符”窗口中输入 telnet 192.168.0.10 7788 命令，当连接成功后，则就可以拥有目标主机的系统管理员权限，即可对目标主机进行任意操作，如图 2-26 所示。

Step06 例如：在“命令提示符”窗口中输入 cd c:\ 命令，即可进入目标主机的 C 盘目录之下，如图 2-27 所示。

图 2-26　连接目标主机

图 2-27　进入目标主机中

2.3.3　修补 WebDAV 缓冲区溢出漏洞

微视频

如果不能立刻安装补丁或者升级，用户可以采取以下措施来降低威胁。

（1）使用微软提供的 IIS Lockdown 工具防止该漏洞被利用。

（2）可以在注册表中完全关闭 WebDAV 包括的 PUT 和 DELETE 请求，具体的操作步骤如下。

Step01 启动注册表编辑器。在“运行”对话框中输入 regedit 命令，然后按 Enter 键，打开“注册表编辑器”窗口，如图 2-28 所示。

Step02 在注册表中依次找到如下键：HKEY_ LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W3SVC\Parameters，如图 2-29 所示。

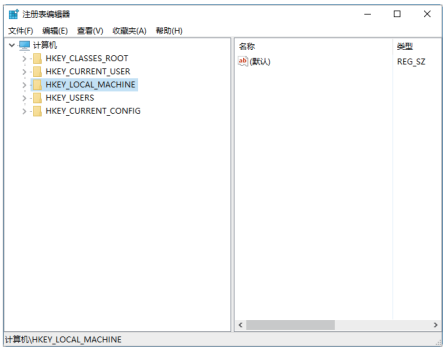

图 2-28　“注册表编辑器”窗口

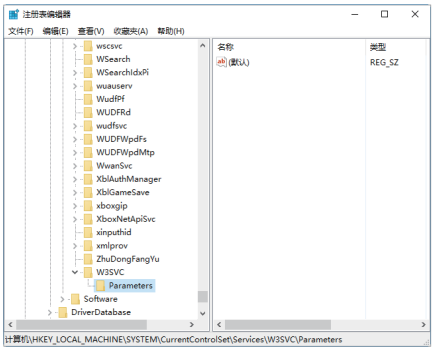

图 2-29　Parameters 项

Step03 选中该键值后右击，从弹出的快捷菜单中选择“新建”选项，即可新建一个项目，并将该项目命名为 DisableWebDAV，如图 2-30 所示。

Step04 选中新建的项目“DisableWebDAV”，在窗口右侧的“数值”下侧右击，从弹出的快捷菜单中选择“DWORD（32 位）值（D）”选项，如图 2-31 所示。

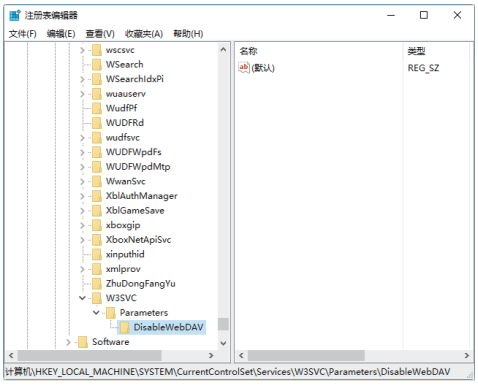

图 2-30　新建 DisableWebDAV

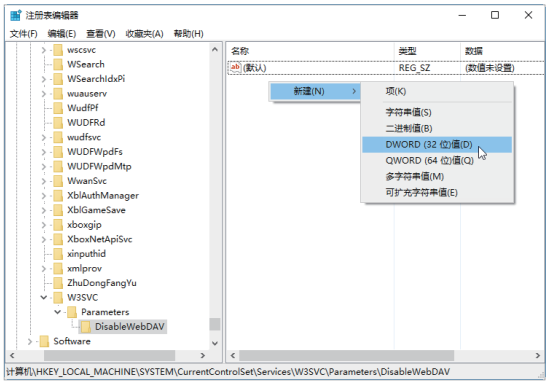

图 2-31　“DWORD（32 位）值（D）”选项

Step05 选择完毕后，即可在“注册表编辑器”窗口中新建一个键值，然后选择该键值，在弹出的快捷菜单中选择“修改”选项，弹出“编辑 DWORD（32 位）值”对话框，在“数值名称”文本框中输入 DisableWebDAV，在“数值数据”文本框中输入“1”，如图 2-32 所示。

Step06 单击“确定”按钮，即可在注册表中完全关闭 WebDAV 包括的 Put 和 Delete 请求，如图 2-33 所示。

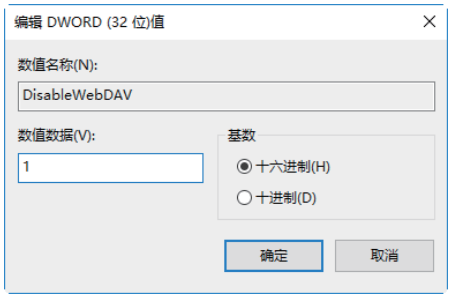

图 2-32　输入数值数据 1

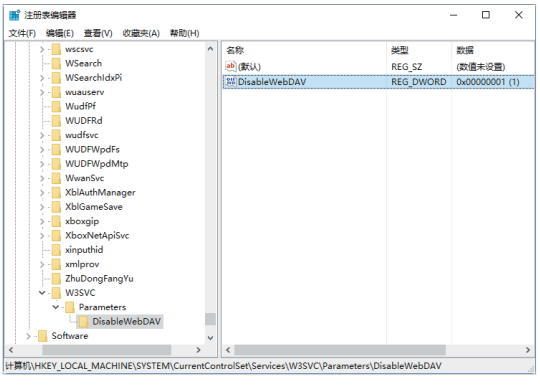

图 2-33　关闭 Put 和 Delete 请求

2.4　修补系统漏洞

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。

2.4.1　使用 Windows 更新修补漏洞

微视频

“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。

Step01 单击“开始”按钮，在打开的菜单中选择“设置”选项，如图 2-34 所示。

Step02 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 2-35 所示。

图 2-34　“设置”选项

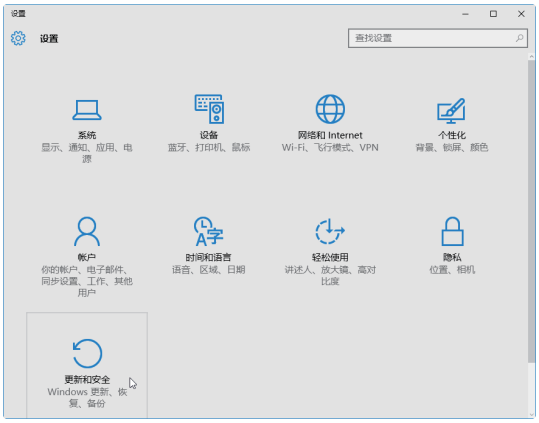

图 2-35　“设置”窗口

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 2-36 所示。

Step 04 单击“检查更新”按钮，即可开始检查网上是否存在有更新文件，如图 2-37 所示。

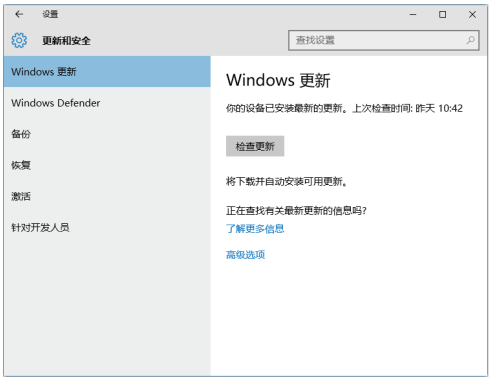

图 2-36　“更新和安全”窗口

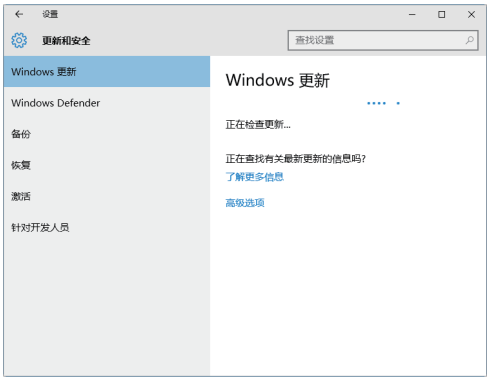

图 2-37　查询更新文件

Step 05 检查完毕后，如果存在更新文件，则会弹出如图 2-38 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。

Step 06 下载完成后，系统会自动安装更新文件，安装完毕后，会弹出如图 2-39 所示的信息对话框。

图 2-38　下载更新文件

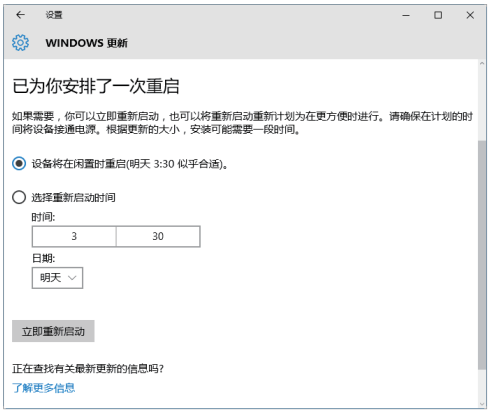

图 2-39　自动安装更新文件

Step07 单击“立即重新启动”按钮，立即重新启动计算机，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 2-40 所示。

Step08 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 2-41 所示。

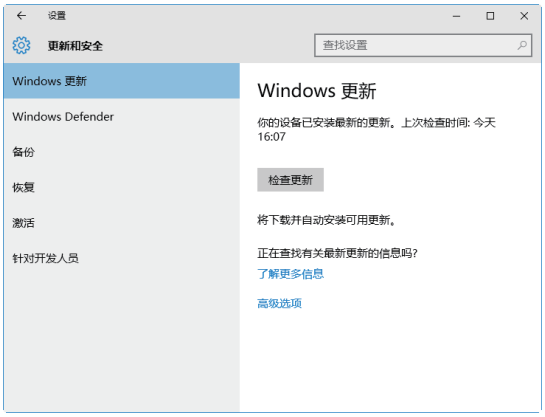

图 2-40　完成系统更新

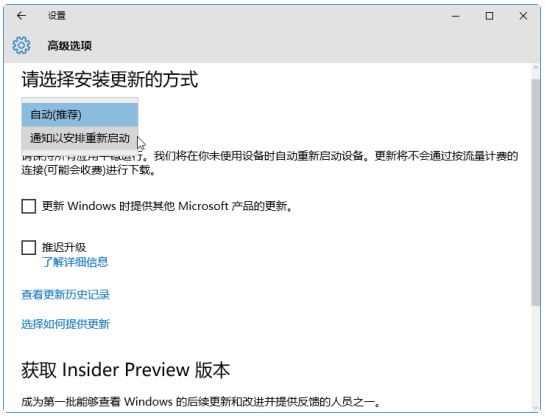

图 2-41　选择更新方式

2.4.2　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 360 安全卫士、优化大师等。

使用 360 安全卫士修复系统漏洞的具体操作步骤如下。

Step01 双击桌面上的电脑管家图标，打开“电脑管家”窗口，如图 2-42 所示。

图 2-42　“电脑管家”窗口

Step02 选择“工具箱”选项，进入如图 2-43 所示的界面。

Step03 单击“修复漏洞”图标，电脑管家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 2-44 所示。

Step04 单击“一键修复”按钮，开始修复系统存在的漏洞，如图 2-45 所示。

图 2-43　“工具箱”窗口

图 2-44　“系统修复”窗口

图 2-45　修复系统漏洞

Step 05 修复完成后，则系统漏洞的状态变为“修复成功”，如图 2-46 所示。

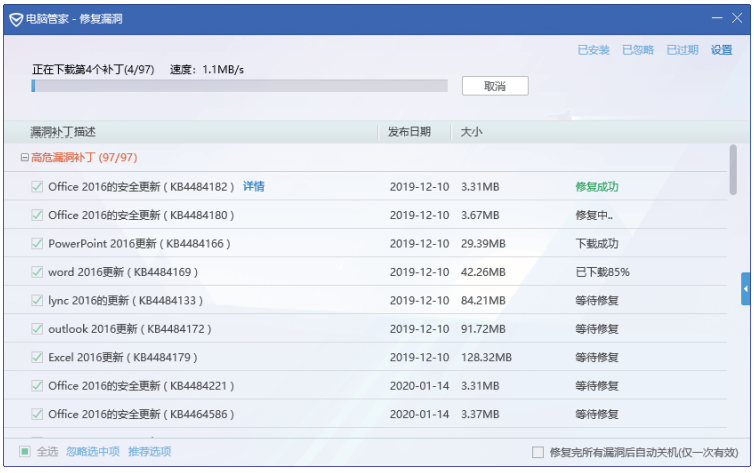

图 2-46　成功修复系统漏洞

2.5　实战演练

2.5.1　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。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 安装完补丁后不自动弹出“重新启动”的信息对话框呢？具体的操作步骤如下。

Step01 单击“开始”按钮，在弹出的快捷菜单中选择“所有程序”→“附件”→“运行”选项，弹出“运行”对话框，在“打开”文本框中输入 gpedit.msc，如图 2-47 所示。

Step02 单击“确定”按钮，即可打开“本地组策略编辑器”窗口，如图 2-48 所示。

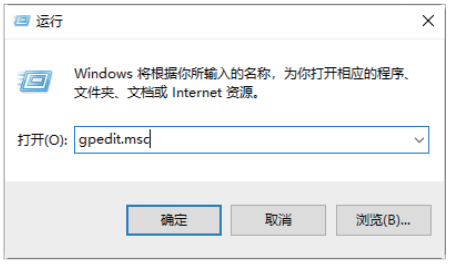

图 2-47　“运行”对话框

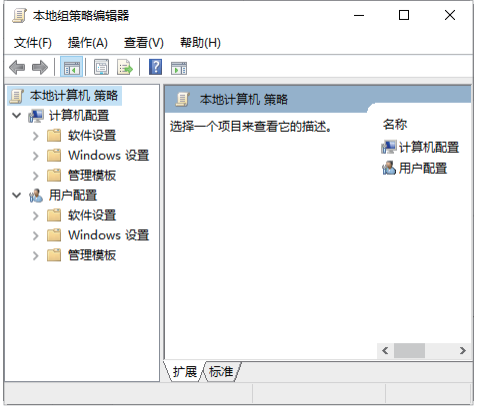

图 2-48　“本地组策略编辑器”窗口

Step03 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 2-49 所示。

Step04 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 2-50 所示。

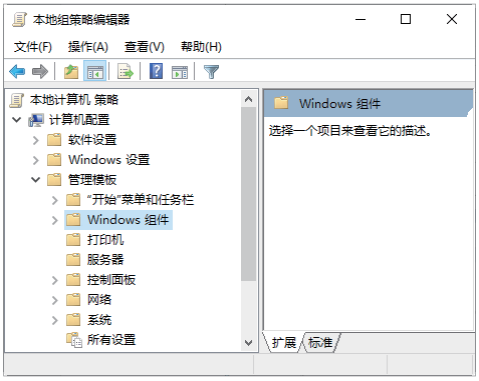

图 2-49　“Windows 组件”选项

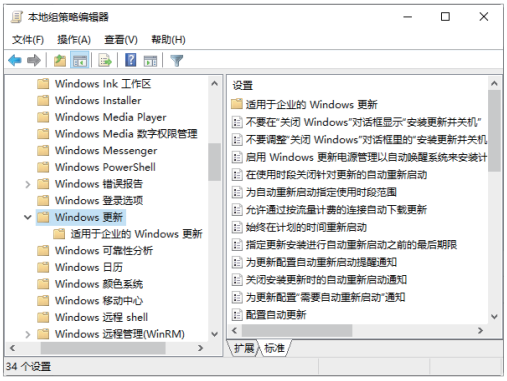

图 2-50　“Windows 更新”选项

Step05 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，从弹出的快捷菜单中选择“编辑”选项，如图 2-51 所示。

Step06 弹出“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 2-52 所示。

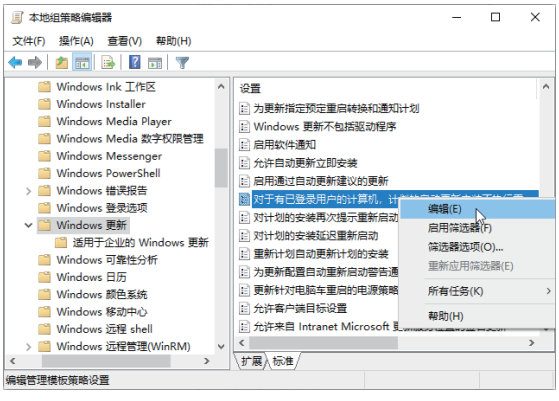

图 2-51　“编辑”选项

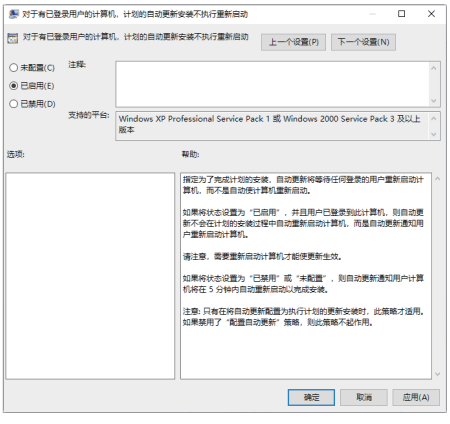

图 2-52　“已启用”单选按钮

Step07 单击“确定”按钮，返回“组策略编辑器”窗口中，此时用户即可看到“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”。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对话框，如图 2-53 所示。

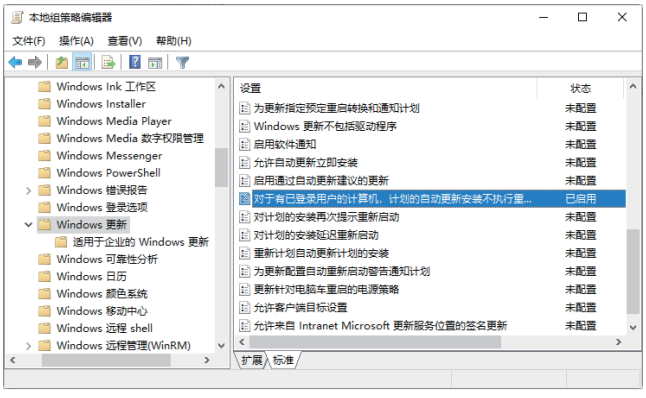

图 2-53　“已启用”状态


微视频

2.5.2 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。

Step01 按 Ctrl+Alt+Delete 组合键，打开如图 2-54 所示的界面。

Step02 选择“任务管理器”选项，打开“任务管理器”窗口，如图 2-55 所示。

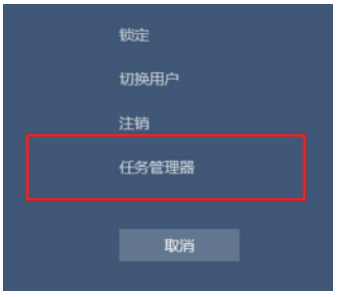

图 2-54 “任务管理器”选项

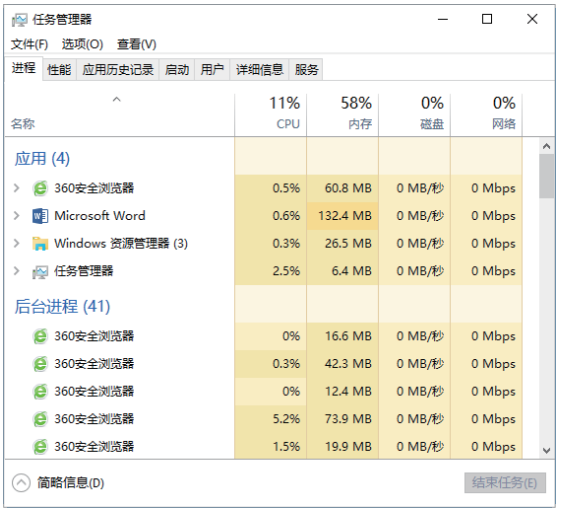

图 2-55 “任务管理器”窗口

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 2-56 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 2-57 所示。

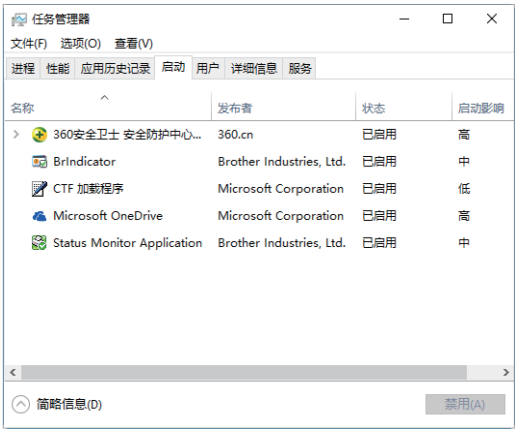

图 2-56 “启动”选项卡

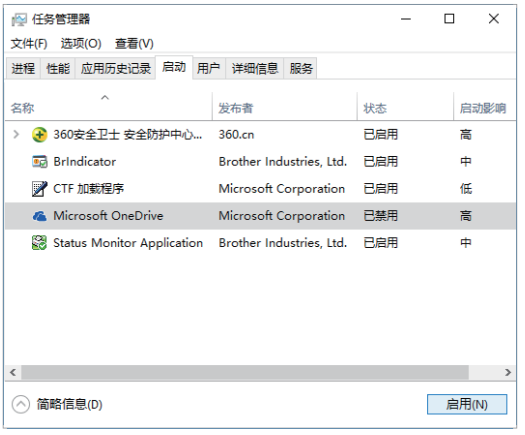

图 2-57 禁止开机启动项