HZ BOOKS
华章科技

学电脑从入门到精通

THE SECRETS OF BEING AN EXPERT
IN COMPUTER FROM A BEGINNER

# 黑客攻防
## 从入门到精通
## （黑客与反黑工具篇）

李书梅 等编著

- 任务驱动，自主学习，理论+实战+图文=让您快速精通
- 讲解全面，轻松入门，快速打通初学者学习的重要关卡
- 实例为主，易于上手，模拟真实攻防环境，解决各种疑难问题

入门到精通丛书
累计销售
30万册

机械工业出版社
China Machine Press

# 黑客攻防
## 从入门到精通
### （黑客与反黑工具篇）

李书梅 等编著

机械工业出版社
China Machine Press

**图书在版编目（CIP）数据**

黑客攻防从入门到精通（黑客与反黑工具篇）/ 李书梅等编著．—北京：机械工业出版社，2015.3

ISBN 978-7-111-49738-7

I. 黑… II. 李… III. 计算机网络－安全技术 IV. TP393.08

中国版本图书馆 CIP 数据核字（2015）第 058302 号

# 黑客攻防从入门到精通（黑客与反黑工具篇）

出版发行：机械工业出版社（北京市西城区百万庄大街 22 号　邮政编码：100037）

责任编辑：李华君　陈佳媛　　责任校对：殷　虹

印　　刷：三河市宏图印务有限公司　　版　　次：2015 年 4 月第 1 版第 1 次印刷

开　　本：185mm×260mm　1/16　　印　　张：24.5

书　　号：ISBN 978-7-111-49738-7　　定　　价：59.00 元

凡购本书，如有缺页、倒页、脱页，由本社发行部调换

客服热线：（010）88378991　88361066　　投稿热线：（010）88379604

购书热线：（010）68326294　88379649　68995259　　读者信箱：hzjsj@hzbook.com

# 前言

在大家眼中“黑客”一词具有一定的神秘性，其定义范围包括了计算机天才，也包括恶意病毒的编写者。因此，如同在媒体故事中所描述的那样，现代黑客试图攻击网络，从而进行识别偷窃、窃取信用卡账号、勒索银行或发起拒绝服务攻击等。随着计算机网络的普及、黑客工具的传播，使得一些有黑客之名无黑客之实的人，只要使用简单的工具，就可对一些疏于防范的计算机进行攻击，并在受侵入的计算机里为所欲为。当受侵入者发现自己的密码被盗、资料被修改或删除、硬盘变作一片空白之时，再想亡羊补牢，却为时已晚。

## 关于本书

在现实生活中，黑客可能是那些非常有天赋的程序员，他们将众多强大的工具组合起来解决自己的需求，还可能是那些使用“合法的”工具来绕过审查机构限制并窃取他人隐私的人。俗话说：害人之心不可有，防人之心不可无。知己知彼方能百战不殆。

本书便是基于这样一个目的而诞生的。了解基础的网络知识，知晓通常的黑客攻击手段与常用黑客软件，从而用知识与技巧将自己的计算机与网络很好地保护起来，达到防患于未然的目的。

## 本书内容

本书紧紧围绕“攻”、“防”两个不同的主题，在讲解黑客攻击手段的同时，介绍了相应的防范方法，图文并茂地再现了网络入侵与防御的全过程。本书涵盖了

黑客必备小工具、扫描与嗅探工具、注入工具、密码攻防工具、病毒攻防工具、木马攻防工具、网游与网吧攻防工具、黑客入侵检测工具、清理入侵痕迹工具、网络代理与追踪工具、局域网黑客工具、远程控制工具、QQ 聊天工具、系统和数据的备份与恢复工具、系统安全防护工具等内容，由浅入深地讲述了黑客攻击的原理、常用手段，让读者在了解黑客技术的同时学习拒敌于千里的方法。

## 本书特色

本书由浅入深地讲解了黑客攻击和防范的具体方法和技巧，通过具体形象的案例向读者展示了多种攻击方法和攻击工具的使用。通过完成一个个实践任务，读者可以轻松掌握各种知识点，在不知不觉中快速提升实战技能。

- 任务驱动，自主学习，理论 + 实战 + 图文 = 让读者快速精通。
- 讲解全面，轻松入门，快速打通初学者学习的重要关卡。
- 实例为主，易于上手，模拟真实工作环境，解决各种疑难问题。

本书以实例分析加案例剖解为主要手段，以图文并茂、按图索骥方式详细讲解黑客的攻击手法和相应的网络安全管理防御技术，并采用案例驱动的写作方法，照顾初级读者，详细分析每一个操作案例，力求通过一个个知识点的讲解，让读者用更少的时间尽快掌握黑客编程技术，理解和掌握类似场合的应对思路。

## 本书适合人群

本书是一本面向广大网络爱好者的速查手册。适合于以下读者学习使用：

- 没有多少计算机操作基础的广大读者；
- 需要获得数据保护的日常办公人员；
- 喜欢看图学习的广大读者；
- 相关网络管理人员、网吧工作人员等；
- 明确学习目的、喜欢钻研黑客技术但编程基础薄弱的读者；
- 网络管理员及广大网友等。

# 目录

## 第3章 注入工具 / 63



## 第4章 密码攻防工具 / 82

## 第5章 病毒攻防常用工具 / 117



## 第6章 木马攻防常用工具 / 140

## 第7章 网游与网吧攻防工具 / 172



## 第8章 黑客入侵检测工具 / 188



## 第9章 清理入侵痕迹工具 / 211

## 第12章 远程控制工具 / 269



## 第13章 QQ聊天工具 / 294

## 第14章 系统和数据的备份与恢复工具 / 308



## 第15章 系统安全防护工具 / 341

# 第1章 黑客必备小工具

在黑客试图攻击他人计算机并进行一系列破坏性操作时，往往会借助各种各样的工具。本章主要介绍黑客必备的各种小工具，例如文本编辑工具、免杀辅助工具、入侵辅助工具，有助于读者对这些工具有一个比较全面的了解，并学会使用这些工具。

本章要点：

- 文本编辑工具
- 免杀辅助工具
- 入侵辅助工具

# 1.1 文本编辑工具

在对文件进行修改时，经常会用到文本编辑工具，如 UltraEdit 编辑器、WinHex 以及 PE 文件编辑工具 PEditor。黑客通常借助于这些工具来修改木马病毒的特征码，以避开杀毒软件的查杀。

## 1.1.1 UltraEdit 编辑器

UltraEdit 是一套功能强大的文本编辑器，该工具可以编辑文本、十六进制编码、ASCII 码等，甚至可取代记事本。该编辑器内建英文单词检查，C++ 及 VB 指令，可同时编辑多个文件。该软件又附有 HTML 标签颜色显示、搜寻替换及无限制还原功能，可修改 EXE 或 DLL 文件。

该工具的具体使用步骤如下。

步骤 01：下载并安装 UltraEdit，双击该工具的快捷图标，即可打开 UltraEdit 主窗口。在 UltraEdit 工具中可以查看各种应用软件的十六进制编码，如图 1-1 所示。

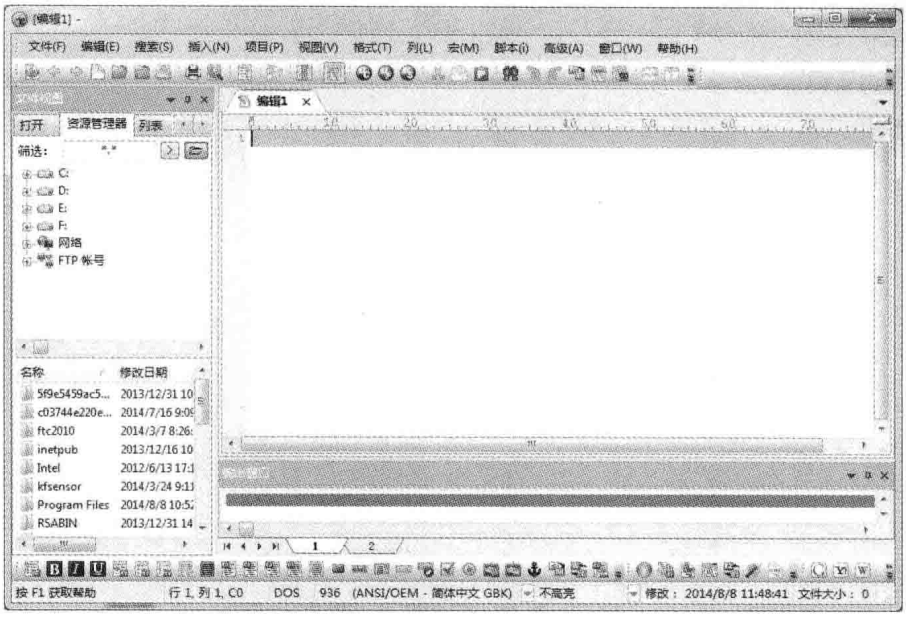


图 1-1 UltraEdit 主窗口

步骤 02：选择“文件”→“打开”菜单项，即可打开“打开”对话框，如图 1-2 所示。

步骤 03：在其中选择相应的应用程序，单击“打开”按钮，即可在 UltraEdit 主窗口中看到该应用程序对应的十六进制编码，如图 1-3 所示。

步骤 04：UltraEdit-32 支持多文件的查找替换，如果想把打开的几个文件中的“/index.htm”全部替换为“../index.htm”，在 UltraEdit 主窗口中选择“搜索”→“替换”选项，即可打开“替换”对话框。在其中分别输入要查找的词和要替换的词，如图 1-4 所示。单击“全部

替换”按钮，即可进行替换操作。

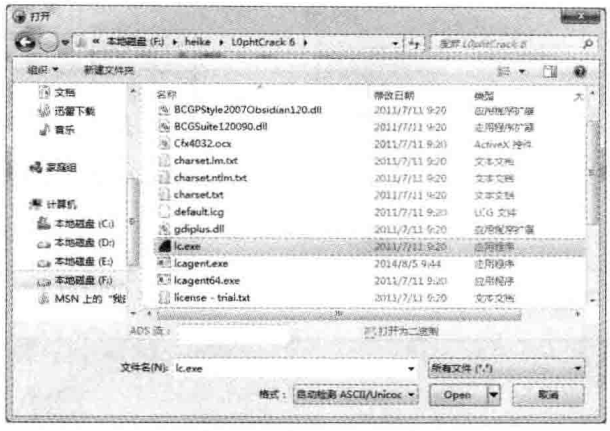


图 1-2 “打开”对话框

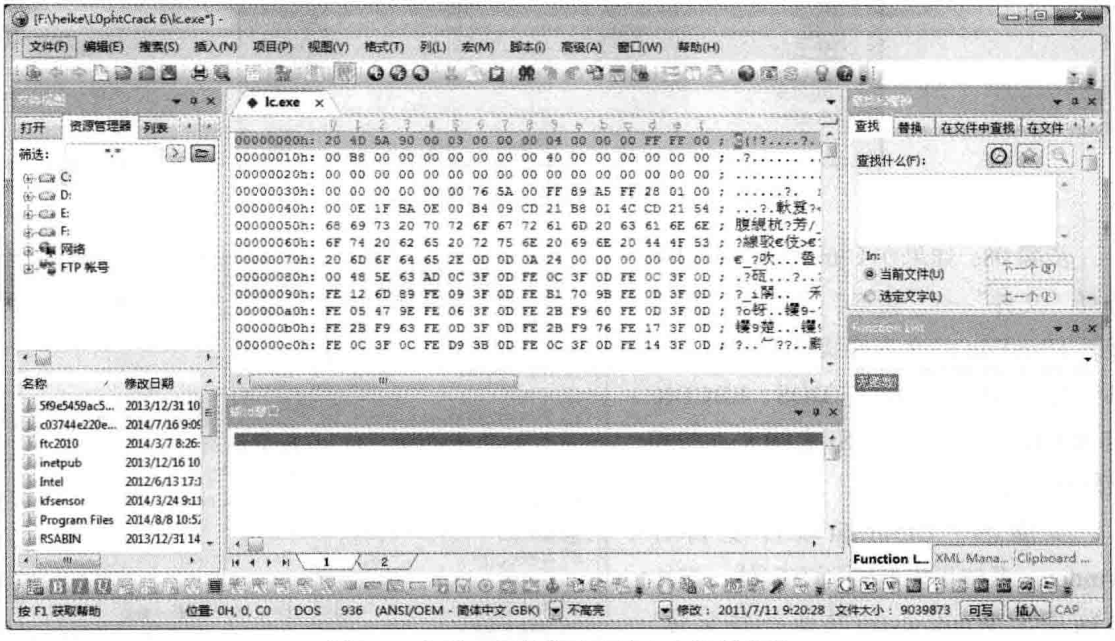


图 1-3 查看应用程序对应的十六进制编码

步骤 05：在 UltraEdit 编辑工具中还可以插入或删除十六进制数据。在 UltraEdit 主窗口中选择“编辑”→“十六进制功能”→“十六进制插入 / 删除”菜单项，即可打开“十六进制插入 / 删除”对话框，如图 1-5 所示。

步骤 06：在 UltraEdit 主窗口中选择“插入”→“在每一个增量处字符串”菜单项，即可打开“用指定增量插入字符串”对话框，在其中设置要插入的字符、文件偏移开始点等属性。单击“确定”按钮，即可添加指定的字符串。

步骤 07：还可以让 UltraEdit 软件打开指定类型的文件，其具体的添加方法为，在 UltraEdit 主窗口中选择“高级”→“配置”菜单项，即可打开“配置”对话框。在“文件类型”

选项卡下就可以添加新的文件类型，如图 1-6 所示。


图 1-4 “替换”对话框

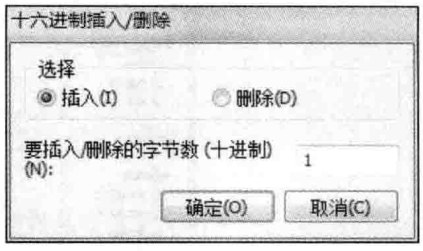


图 1-5 “十六进制插入 / 删除”对话框

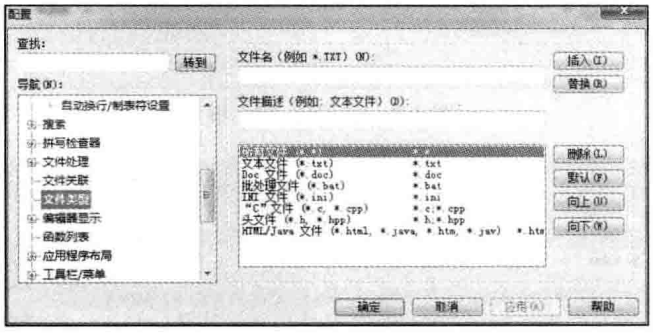


图 1-6 “配置”对话框

步骤 08：如果在 UltraEdit 主窗口中选择“文件”→“转换”菜单项，则可展开 UltraEdit 的文本格式转换菜单，在其中进行 UNIX/MAC 与 DOS、EBCDIC 与 ASCII、OEM 与 ANSI 之间文本的相互转换，如图 1-7 所示。

步骤 09：UltraEdit 软件支持在 Windows 系统里安装的所有字体，其中包括中文 Windows 和其他外挂字体。如果要选择显示字体，在 UltraEdit 主窗口中选择“视图”→“设置字体”菜单项，即可打开“字体”对话框，如图 1-8 所示。

步骤 10：在 UltraEdit 软件中还可以直接调用 DOS 和 Windows 命令。在 UltraEdit 主窗口中选择“高级”→“DOS 命令”菜单项或按 F9 键，即可打开“Dos 命令”对话框，如图 1-9 所示。

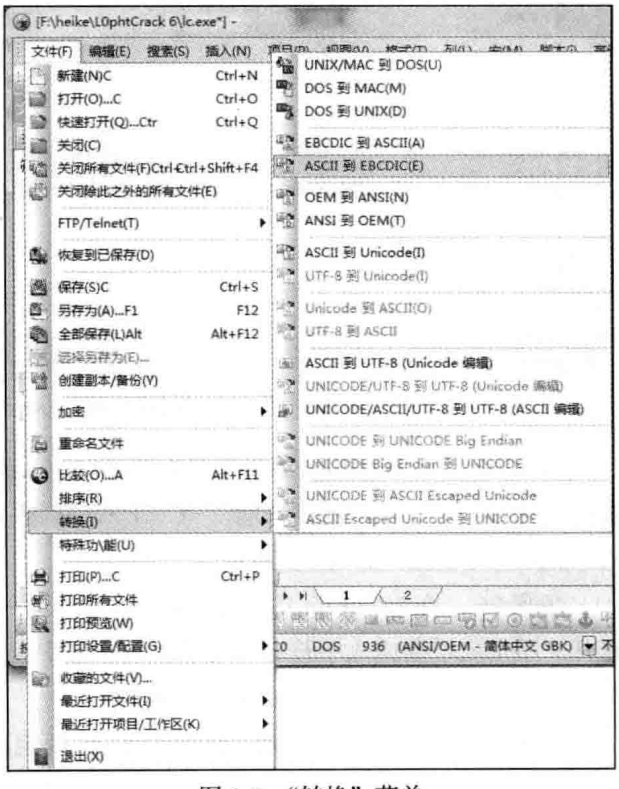


图 1-7 “转换”菜单

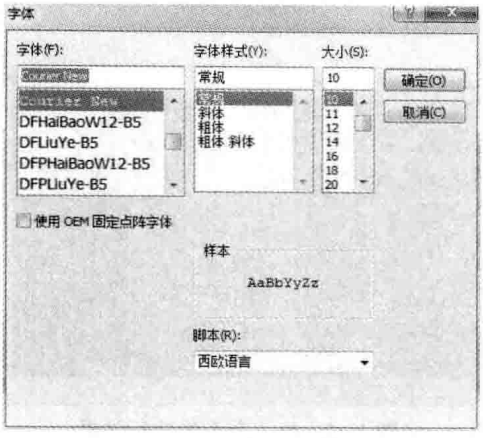


图 1-8 “字体”对话框

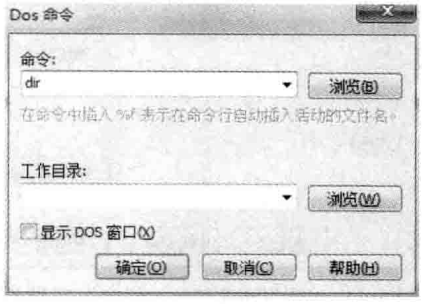


图 1-9 “Dos 命令”对话框

步骤 11：在“命令”文本框中输入 Dos 命令，如 dir、ping 等，单击“确定”按钮，即可在 UltraEdit 主窗口的编辑区中看到该命令的具体执行结果。利用这项功能可以截取 Dos 窗口运行的文本信息，如图 1-10 所示。

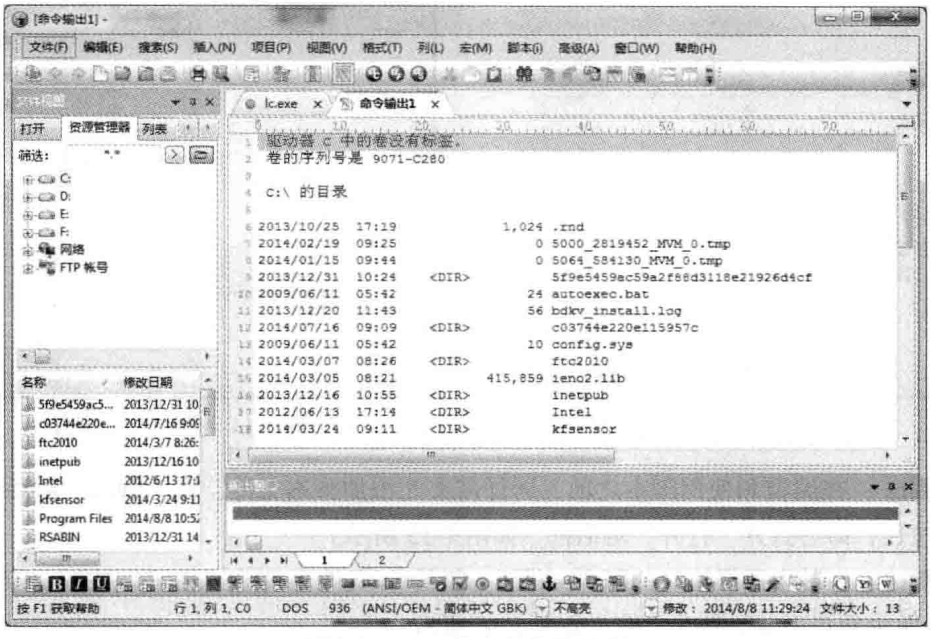


图 1-10 Dos 命令的执行结果

步骤 12：如果想运行 Windows 程序，则在 UltraEdit 主窗口中选择“高级”→“运行 Windows 程序”菜单项或按 F10 键，即可打开“运行 Windows 程序”对话框，如图 1-11 所示。

步骤 13：在“命令”文本框中输入命令调用 Windows 应用程序（如 cmd），单击“确定”按钮，即可打开“命令提示符”窗口，在其中看到 UltraEdit 软件的安装路径，如图 1-12 所示。

步骤 14：UltraEdit 工具还可以编辑和使用宏，在使用宏之前需要先定义宏。在 UltraEdit 主窗口中选择“宏”→“录制”菜单项，即可打开“宏定义”对话框，如图 1-13 所示。在其

中输入宏的名称和热键后，单击“确定”按钮，即可录制宏。


图 1-11 “运行 Windows 程序”对话框

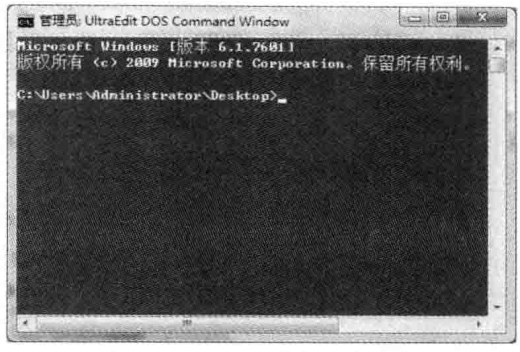


图 1-12 Dos 命令的执行结果

步骤 15：如果想在 UltraEdit 工具中插入并使用已经存在的脚本文件，则在 UltraEdit 主窗口中选择“脚本”→“脚本”菜单项，即可打开“脚本”对话框。在其中可进行添加、编辑、删除脚本操作，如图 1-14 所示。

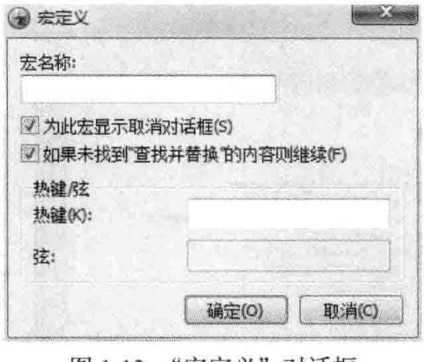


图 1-13 “宏定义”对话框

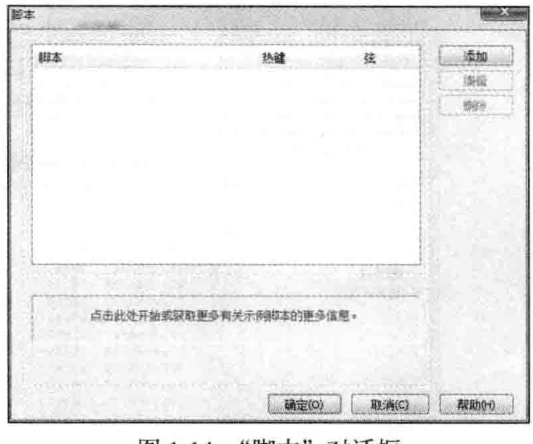


图 1-14 “脚本”对话框

步骤 16：在编辑和使用脚本之前，同样需要先添加脚本文件。在“脚本”对话框中单击“添加”按钮，即可打开“打开”对话框，如图 1-15 所示。

步骤 17：在其中选择相应的脚本文件（一般是 .js 文件），单击“打开”按钮，即可在“脚本”对话框中看到添加的脚本文件，如图 1-16 所示。

步骤 18：单击“确定”按钮，返回 UltraEdit 主窗口中的“脚本列表”窗口中，即可看到刚添加的脚本文件，如图 1-17 所示。

步骤 19：利用 UltraEdit 软件还可以对应用程序进行加密和解密操作。在 UltraEdit 主窗口中选择“文件”→“加密”→“加密文件”菜单项，即可打开“加密文件”对话框，在“密码”和“确认密码”文本框中分别输入要设置的密码，如图 1-18 所示。

步骤 20：单击“确定”按钮，即可打开“加密 – 删除文件”对话框，如图 1-19 所示。如果不想删除应用程序源文件，则单击“否”按钮，即可进行加密操作。


图 1-15 “打开”对话框

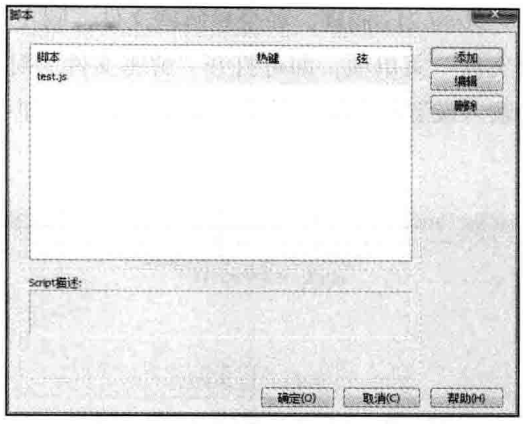


图 1-16 添加的脚本文件

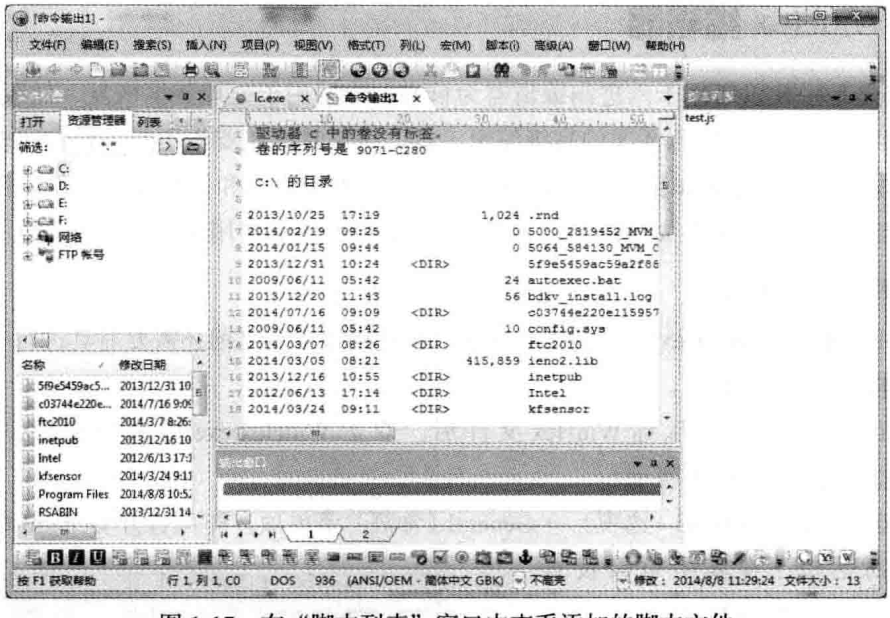


图 1-17 在“脚本列表”窗口中查看添加的脚本文件

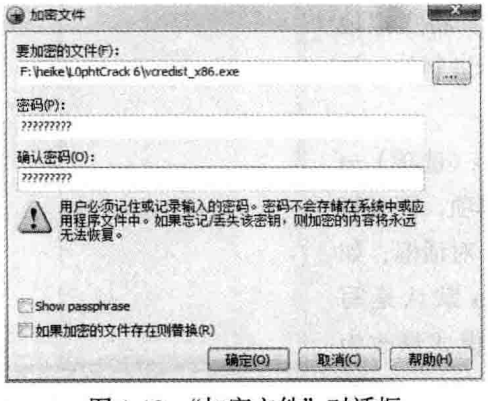


图 1-18 “加密文件”对话框

步骤 21：同理，如果想解密文件，则在 UltraEdit 主窗口中选择“文件”→“加密”→“解密文件”菜单项，即可打开“解密文件”对话框，如图 1-20 所示。在其中选择要解密的文件并输入设置的密码，单击“确定”按钮，即可进行解密操作。

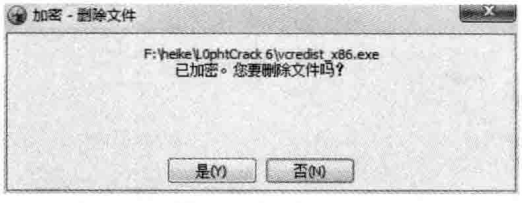


图 1-19 “加密 – 删除文件”对话框

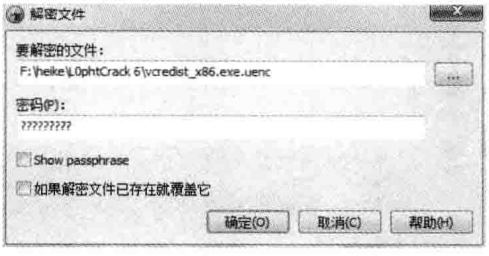


图 1-20 “解密文件”对话框

## 1.1.2 WinHex 编辑器

WinHex 是一款以通用十六进制编辑器为核心，专门用于处理数据恢复、低级数据处理、IT 安全性以及各种日常紧急情况的高级编辑工具。该工具的主要作用是分析和比较文件、磁盘克隆、数据擦除、搜索和替换等，利用该工具可以进行检查和修复各种文件、恢复删除文件、硬盘损坏造成的数据丢失等操作。下面将介绍如何配置和使用 WinHex 编辑器。

### （1）配置 WinHex

为了充分地利用 WinHex 工具的强大功能，在使用该工具之前还需要对其进行一些简单的配置。具体的操作步骤如下。

步骤 01：下载并解压缩 WinHex 文件后，双击 WinHex.exe 可执行文件，即可打开 WinHex 主窗口，如图 1-21 所示。

步骤 02：选择 Options（选项）→ General（常规）菜单项，即可打开 General Options（常规选项）对话框，在其中可以设置临时文件的文件夹的存放位置，如：C:\Users，并勾选 Hexadecimal offsets（十六进制偏移量）复选框，将虚拟地址和偏移地址都设置为十六进制的，如图 1-22 所示。

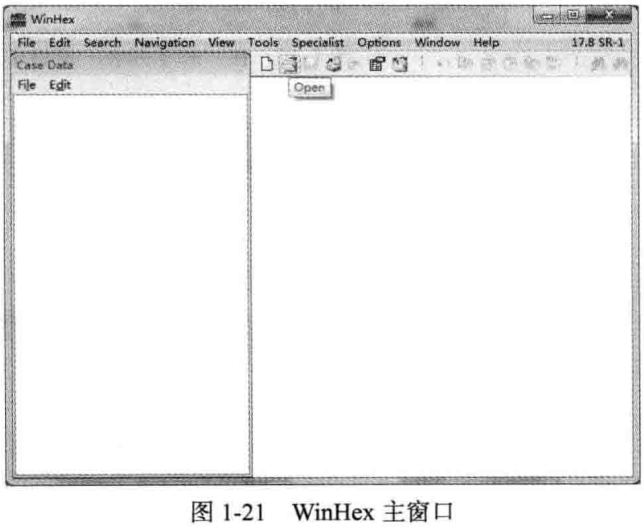


图 1-21 WinHex 主窗口

步骤 03：选择 Options（选项）→ Edit Mode（编辑模式）菜单项，即可打开 Select Mode（选择模式）对话框，如图 1-23 所示。由于 WinHex 默认是写保护方式的，这里将编辑模式修改为 Default Edit Mode(=deitale)（默认的编

辑模式（= 可编写））选项。

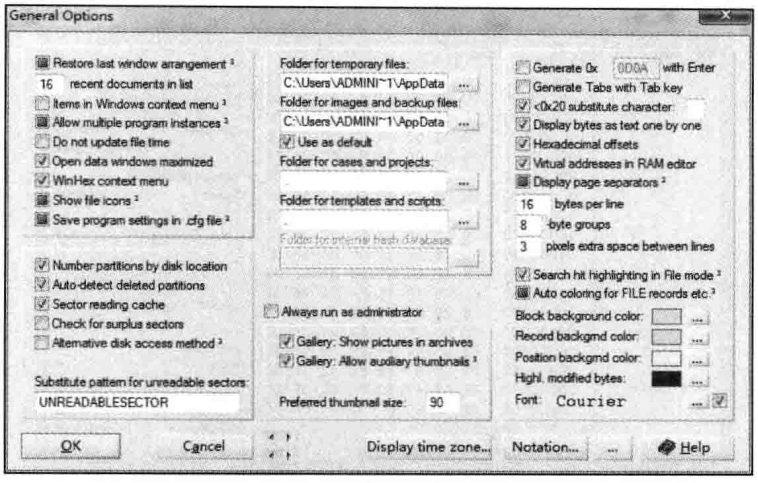


图 1-22 “常规选项”对话框

步骤 04：选择 Options（选项）→ Data Interpreter Options（数据解析器选项）菜单项，即可打开 Data Interpreter Options 对话框，可在其中设置数据解析器各个属性，如图 1-24 所示。

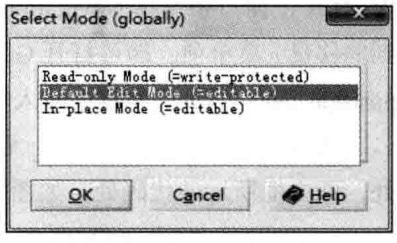


图 1-23 “选择模式”对话框

### （2）WinHex 的使用

WinHex 的主要功能是以十六进制方式编辑和修改机器码，另外还有编辑文本、文件比较及内存编辑等功能。该工具的具体使用步骤如下。

步骤 01：在 WinHex 主窗口中选择 File → Open 菜单项，即可打开 Open Files（打开文件）对话框，在其中选择需要打开的应用程序，如图 1-25 所示。

步骤 02：单击“打开”按钮，即可在 WinHex 主窗口中看到该文件的十六进制代码，如图 1-26 所示。

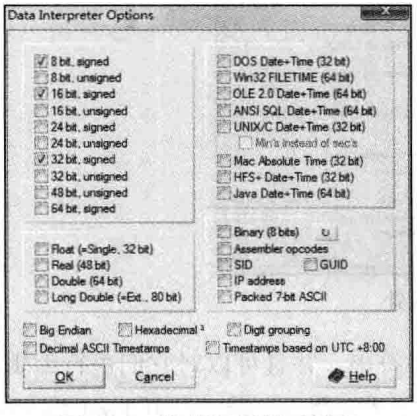


图 1-24 数据解析器对话框

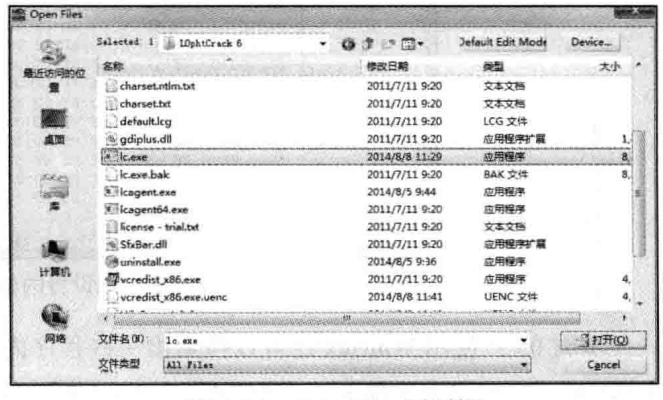


图 1-25 Open Files 对话框

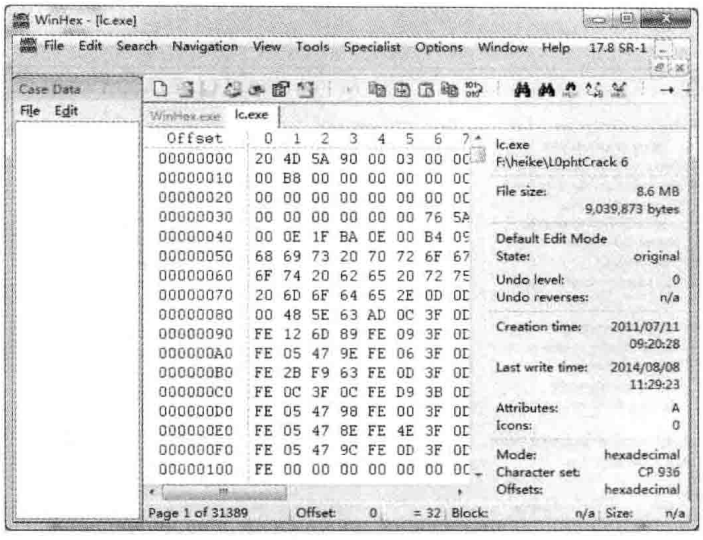


图 1-26　在 WinHex 主窗口中查看应用程序对应的十六进制代码

步骤 03：在 WinHex 可以定位到某个偏移地址处，在 WinHex 主窗口中选择 Navigation（浏览）→ Go To Offset（转到偏移量）菜单项，即可打开 Go To Offset 对话框，在 New position（新位置）文本框中输入 0000050，如图 1-27 所示。

步骤 04：单击 OK 按钮，即可将光标转到相应的地址处，即方框所示的代码处，如图 1-28 所示。

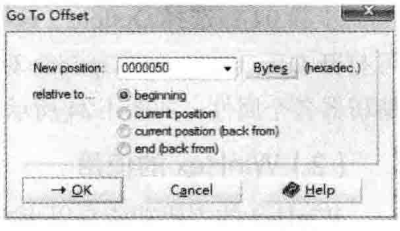


图 1-27　Go To Offset 对话框

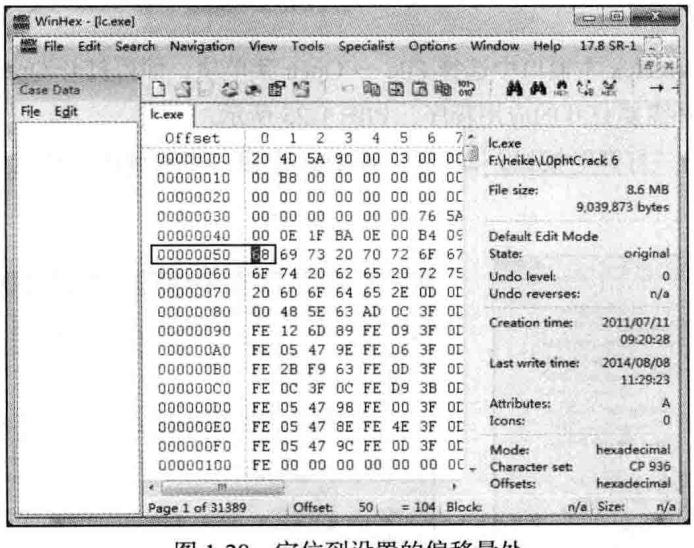


图 1-28　定位到设置的偏移量处

步骤 05：使用 WinHex 还可以搜索出一些程序内的字符串，并且可以对它们进行编辑。在 WinHex 主窗口中选择 Search（搜索）→ Find Text（查找文本）命令，即可打开 Find Text 对话框，在其中输入需要修改的字符串，如 run in DOS mode，将搜索方式设置为 ASCII/Code

page 选项，如图 1-29 所示。

步骤 06：单击 OK 按钮，即可看到已经跳转到要搜索字符串的地址处，如图 1-30 所示。在窗口右侧文本区域中进行字符串的修改，单击工具栏上的保存按钮，即可保存。

步骤 07：利用 WinHex 软件还可以对文件进行连接、分割、合并、不可逆转删除和比较等操作。在解密时经常用到的功能是比较，即通过比较解密前后的文件看出解密者对程序中的哪些代码做了修改，最后生成一个文本方式差别报告。在 WinHex 主窗口中选择 Tools(工具) → Files Tools(文件工具) → Compare(比较)菜单项，即可打开 Compare File/Disks（比较文件 / 硬盘）对话框，如图 1-31 所示。

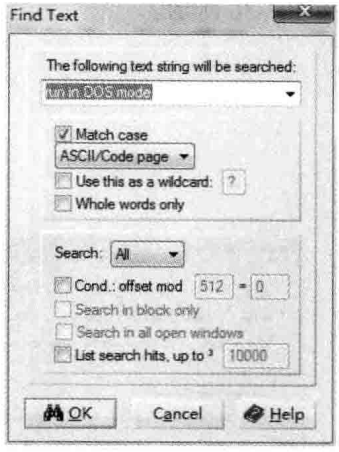


图 1-29 “查找文本”对话框

步骤 08：单击 2nd file 文本框后面的浏览按钮 ...，即可打开 Start Center（启动中心）对话框，如图 1-32 所示。

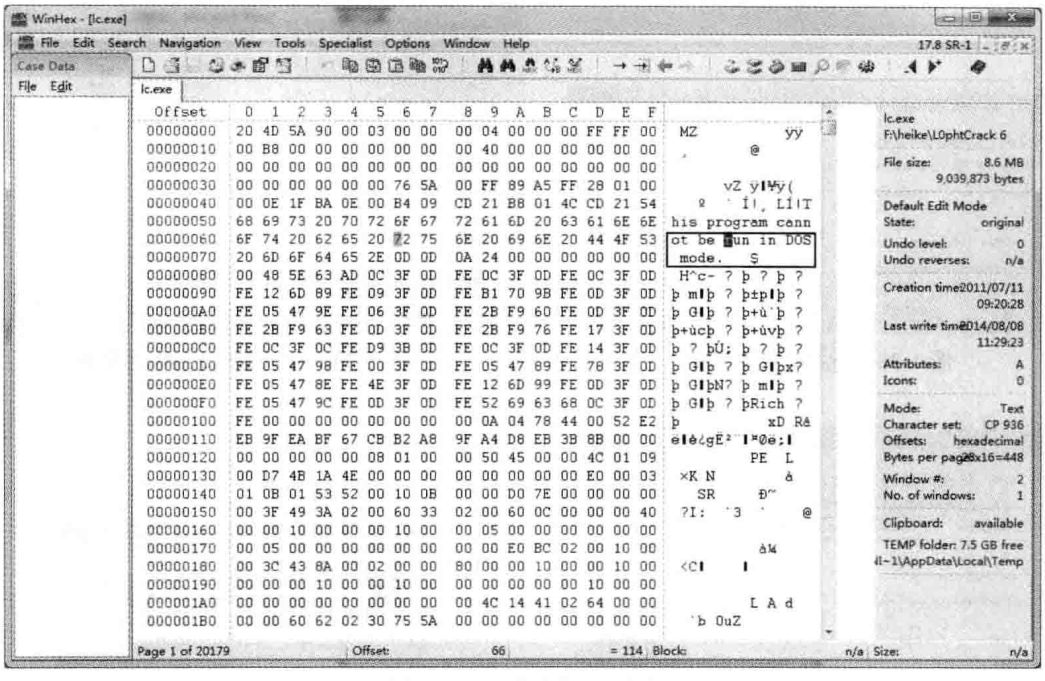


图 1-30 查找到的字符串

步骤 09：单击 Open File（打开文件）按钮，在 Open Files 对话框中选择需要比较的文件，单击“打开”按钮，即可返回“启动中心”对话框。单击 OK 按钮返回比较文件 / 硬盘对话框，即可看到选择的需要比较的文件，如图 1-33 所示。

步骤 10：单击 Save reportsas（保存报告）文本框后面的浏览按钮，即可打开 Save Report As（保存报告为）对话框，在其中设置报告的保存位置和名称，如图 1-34 所示。

步骤 11：单击“保存”按钮，即可返回到比较文件 / 硬盘对话框，在其中可看到报告的

具体保存位置，如图 1-35 所示。单击 OK 按钮，即可打开可以用记事本程序查看报告提示框，如图 1-36 所示。

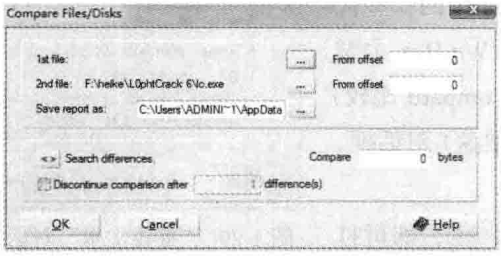


图 1-31　比较文件 / 硬盘对话框


图 1-32　Start Center 对话框

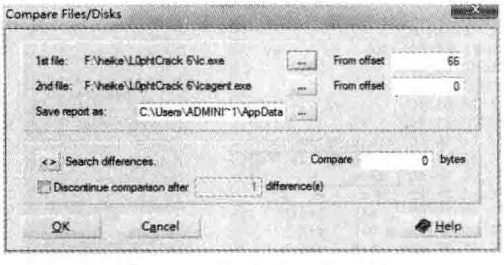


图 1-33　选择的比较文件


图 1-34　Save Report As 对话框

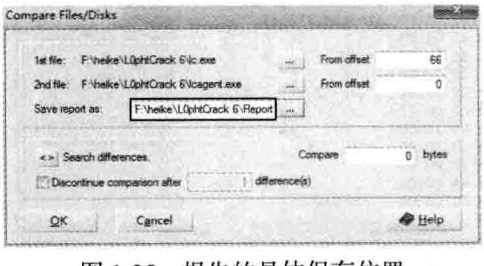


图 1-35　报告的具体保存位置

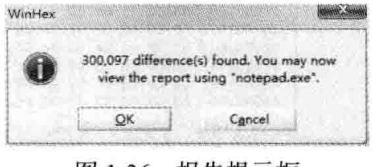


图 1-36　报告提示框

步骤 12：当系统完成文件的比较之后，将会产生一个文本文件，从中可以看到不同代码处的偏移地址、代码内容和差别总数等信息，如图 1-37 所示。

步骤 13：在 WinHex 软件中还可以将应用程序分割为指定大小的文件。在 WinHex 主窗口中选择 Tools（工具）→ Files Tools（文件工具）→ Split（分割）菜单项，即可打开 Split File（分割文件）对话框，在其中选择需要分割的文件，如图 1-38 所示。

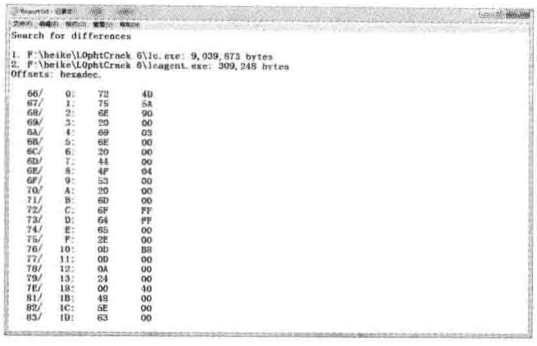


图 1-37 查看比较文件生成的报告


图 1-38 Split File 对话框

步骤 14：单击 Split（分割）按钮，即可打开 Desired file size（定义文件大小）对话框，在其中设置文件的大小，如图 1-39 所示。

步骤 15：单击 OK 按钮，即可打开 Destination File（目标文件）对话框，在其中设置目标文件的保存位置，如图 1-40 所示。单击“保存”按钮，即可进行文件分割。

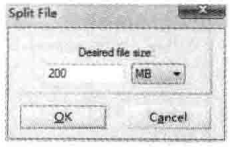


图 1-39 Desired file size 对话框


图 1-40 Destination File 对话框

## 1.1.3 PE 文件编辑工具 PEditor

PEditor 是一款 PE 文件编辑工具，有转存进程、在 SoftICE 中插入中断、编辑 PE 文件的导入表、节表、重建校验和重建程序等功能。与其他 PE 编辑工具相比，PEditor 可把所有的功能都集中在主窗口中，从而方便修改 PE 文件。使用 PEditor 编辑 PE 文件的操作步骤如下。

步骤 01：下载并运行 PEditor 1.7 汉化版程序，即可打开 PEditor 1.7 主窗口，如图 1-41 所示。单击“浏览”按钮，即可打开“选择你要查看的文件”对话框，如图 1-42 所示。

步骤 02：在选择要查看特征码的文件后，单击“打开”按钮，即可在 PEditor 1.7 主窗口中看到该文件的各种特征码信息，如图 1-43 所示。在“入口点”文本框中将其特征码修改为“000021A0”，如图 1-44 所示。该种方法可以使木马程序避开一般的杀毒软件。


图 1-41　PEditor 1.7 主窗口

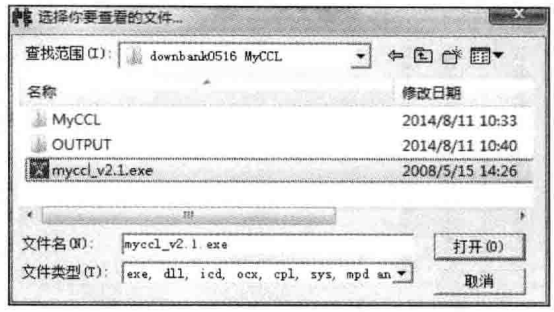


图 1-42　“选择你要查看的文件”对话框


图 1-43　文件的各种特征码信息


图 1-44　修改入口点特征码

步骤 03：单击“应用更改”按钮，即可打开“此文件更新成功”提示框，如图 1-45 所示。单击“确定”按钮，即可完成修改入口点的防特征码免杀设置。

步骤 04：在 PEditor 1.7 主窗口中单击“分割节”按钮，即可打开“3 区段及 PE 头成功转存”提示框，如图 1-46 所示。单击“确定”按钮，即可转存 3 区段和 PE 头文件。

步骤 05：在 PEditor 1.7 主窗口中单击“调试器中中断”按钮，即可打开“调试器中中断”对话框，在“虚拟地址”文本框中输入虚拟地址，如图 1-47 所示。

步骤 06 单击“运行”按钮，即可打开“ myccl_v2.1.exe 已停止工作”提示框，如图 1-48 所示。单击“关闭程序”按钮，即可中断 myccl_v2.1.exe 程序。


图 1-45　“此文件更新成功”提示框

步骤 07：在 PEditor 1.7 主窗口中单击 FLC 按钮，即可打开“文件地址计算器”对话框，在其中选择“相对虚拟地址”单选项并输入相对虚拟地址，如图 1-49 所示。

步骤 08：单击“执行”按钮，即可计算出输入的“相对虚拟地址”对应的虚拟地址、十六进制偏移、十进制偏移以及字节内容，如图 1-50 所示。

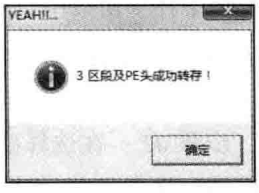


图 1-46　“3 区段及 PE 头成功转存”提示框

步骤 09：在 PEditor 1.7 主窗口中单击“校验和”按钮，即可

打开“校验和修正器”对话框，在其中输入当前校验和与修正校验和，如图 1-51 所示。单击“修正”按钮，即可打开“校验和更新成功”提示框，如图 1-52 所示。

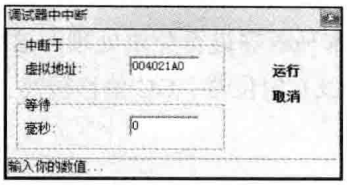


图 1-47 “调试器中中断”对话框

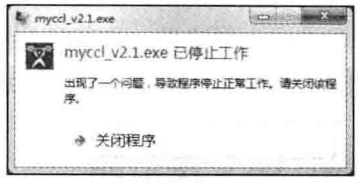


图 1-48 已停止工作提示框

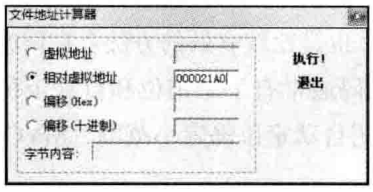


图 1-49 “文件地址计算器”提示框


图 1-50 计算相对虚拟地址对应的各项值


图 1-51 “校验和修正器”提示框

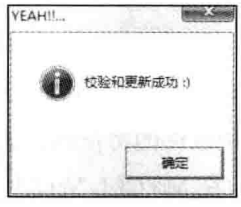


图 1-52 “校验和更新成功”提示框

步骤 10：在 PEditor 1.7 主窗口中单击“重建程序”按钮，即可打开“重建器”对话框，在其中勾选相应的复选框，如图 1-53 所示。单击“执行”按钮，即可重建打开的应用程序，如图 1-54 所示。

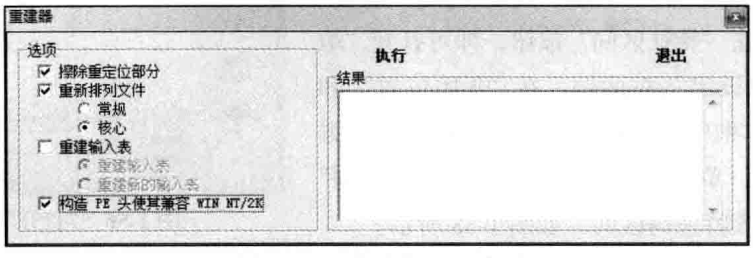


图 1-53 “重建器”提示框


图 1-54 重建打开的应用程序

# 1.2 免杀辅助工具

在黑客进行入侵之前，往往使用免杀辅助工具对其木马程序进行免杀处理，这样才可以成功避开目标主机杀毒软件。常见的免杀辅助工具有 MYCLL 定位器、OC 偏移转换工具等。

## 1.2.1 MYCLL 定位器

当杀毒软件遇到新的病毒时，就会从该病毒程序中截取一段二进制程序代码（特征码），以判断是否是病毒，所以更改特征码就成为免杀最常见，也是比较有效的方法。在修改文件特征码之前，往往需要先对特征码进行定位，而定位特征码通常有手工定位和自动定位两种方法。在一般情况下，先使用手工定位确定大范围，再使用自动定位确定小范围，MYCLL 就是一款非常经典的特征码定位软件。

使用 MYCLL 特征码定位器定位特征码的具体操作步骤如下。

步骤 01：下载并运行“MYCLL 特征码定位器 V2.1”软件，即可打开 MYCLL Ver2.1 主窗口，在其中可以查看应用软件的特征码，如图 1-55 所示。


图 1-55 “MYCLL Ver2.1”主窗口

步骤 02：在 MYCLL Ver2.1 主窗口中单击右边的“文件”按钮，即可打开“打开”对话框，在其中选择需要定位特征码的文件，如图 1-56 所示。


图 1-56 “打开”对话框

步骤 03：单击“打开”按钮，即可在 MYCLL Ver2.1 主窗口中下半部分看到该文件包含的 PE 文件信息，如图 1-57 所示。

步骤 04：单击“特征区间”按钮，即可打开“填充 / 特征码 区间设定”对话框。在“开始位置”和“结束位置”文本框中分别输入开始位置和结束位置对应的特征码后，单击“添加已确定的特征码范围”按钮，即可添加该特征码区间，如图 1-58 所示。

步骤 05：单击 MYCLL Ver2.1 主窗口中的“生成”按钮，即可打开“程序将清除目录中的所有文件”提示框，如图 1-59 所示。

步骤 06：单击 Yes 按钮，即可打开“请对生成目录进行杀毒”提示框，如图 1-60 所示。单击 OK 按钮，即可在 MYCLL Ver2.1 主窗口中看到生成文件的具体路径，如图 1-61 所示。

步骤 07：单击“二次处理”按钮，即可在 MYCLL Ver2.1 主窗口中看到复合特征码定位结果，如图 1-62 所示。

步骤 08：根据定位的结果在专门修改特征码工具中打开该木马文件，将特征码所在的位

置替换为0。再使用杀毒软件进行杀毒，如果没有报病毒就表明定位的结果是正确的，同时也完成特征码的修改。

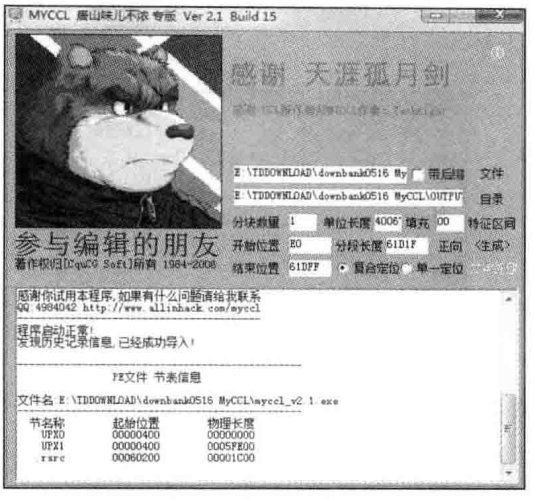


图 1-57 查看文件包含的 PE 文件信息

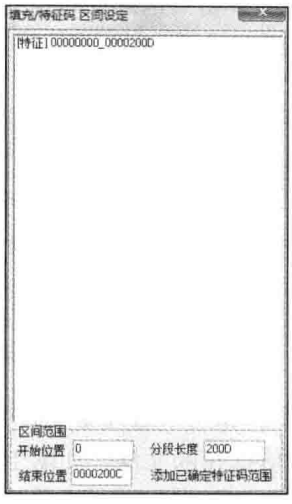


图 1-58 “填充 / 特征码区间设定”对话框

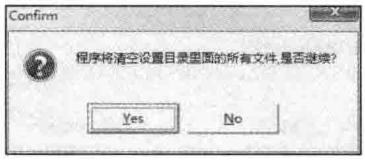


图 1-59 清除所有文件

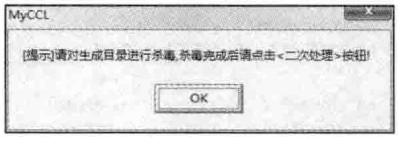


图 1-60 “请对生成目录进行杀毒”提示框

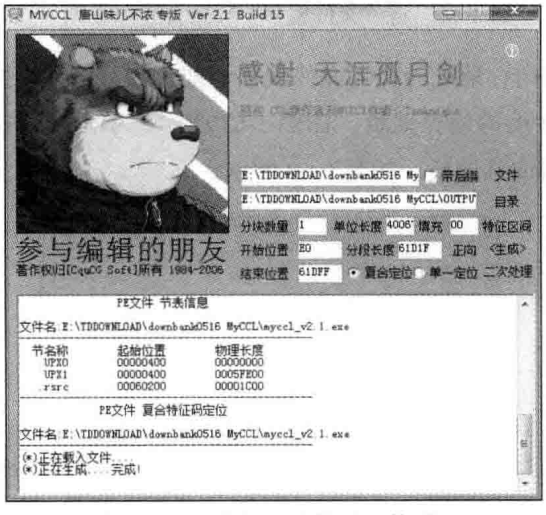


图 1-61 查看生成文件的具体路径

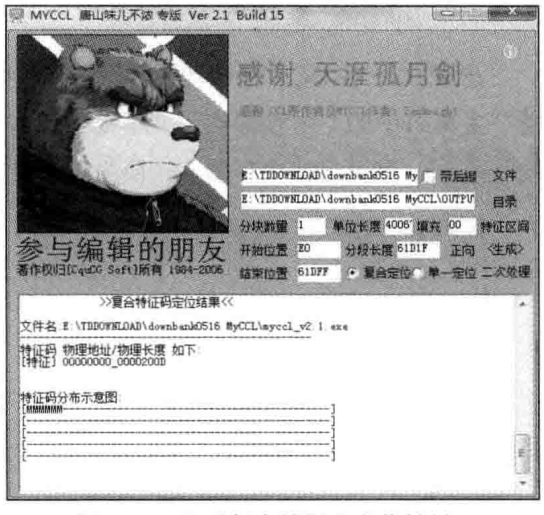


图 1-62 查看复合特征码定位结果

## 1.2.2 OC 偏移量转换器

OC 偏移量转换器是一款偏移量转换工具，利用该工具可以将文件偏移量转换为内存地

址，也可以将内存地址转换为文件偏移量。该工具的具体使用步骤如下。

步骤 01：下载并运行“OC 偏移量转换器”软件，即可打开“地址转换器”主窗口，如图 1-63 所示。单击“选择要转换地址的文件”文本框后面的“浏览”按钮，即可打开“打开”对话框，如图 1-64 所示。


图 1-63 “地址转换器”主窗口

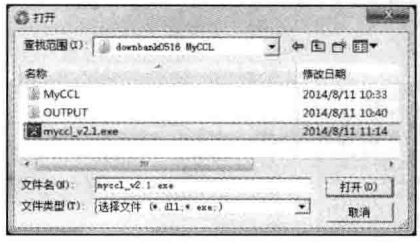


图 1-64 “打开”对话框

步骤 02：在其中选择需要转换地址文件，单击“打开”按钮，即可在“地址转换器”主窗口中看到所选择的文件，如图 1-65 所示。在“文件偏移”文本框中输入文件偏移地址，单击转换按钮 >>>> ，即可将该文件偏移地址转换为“内存偏移”，如图 1-66 所示。

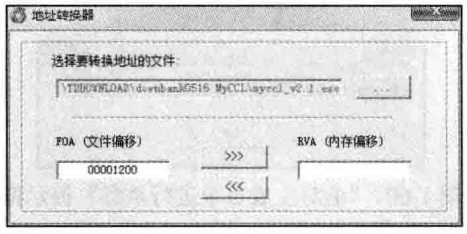


图 1-65 查看所选择的文件


图 1-66 将“文件偏移”转换为“内存偏移”

步骤 03：在 OC“地址转换器”中还可以将内存地址转换为文件偏移地址。在“地址转换器”主窗口中的“内存偏移”文本框中输入要转换的内存地址，如图 1-67 所示。单击转换按钮 <<<< ，即可将该内存偏移转换为对应的文件偏移地址，如图 1-68 所示。


图 1-67 输入要转换的内存偏移地址


图 1-68 将该内存偏移地址转换为文件偏移地址

## 1.2.3 ASPack 加壳工具

ASPack 是一款专门对 Win32 可执行程序进行压缩的工具，而且压缩后程序能正常运行。另外即使将 ASPack 从硬盘中删除，曾经压缩过的文件仍可正常使用。

利用 ASPack 对木马进行加壳的具体操作步骤如下。

步骤 01：下载并运行 ASPack2.28 软件，即可打开 ASPack 2.28 主窗口，如图 1-69 所示。在“选项”选项卡中勾选“压缩资源”、“加载后立即运行”及“使用 Windows DLL 加载器”等复选项，如图 1-70 所示。


图 1-69 ASPack 2.28 主窗口


图 1-70 “选项”选项卡

步骤 02：选择“打开文件”选项卡，单击“打开”按钮，即可打开“选择要压缩的文件”对话框，在其中选择需要加壳的文件，如图 1-71 所示。

步骤 03：单击“打开”按钮，即可开始进行压缩，如图 1-72 所示。在“压缩”选项卡中可进行压缩、测试操作，并在完成之后生成加壳后的文件。

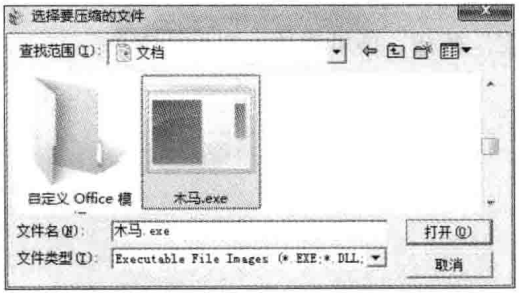


图 1-71 “选择文件压缩”对话框

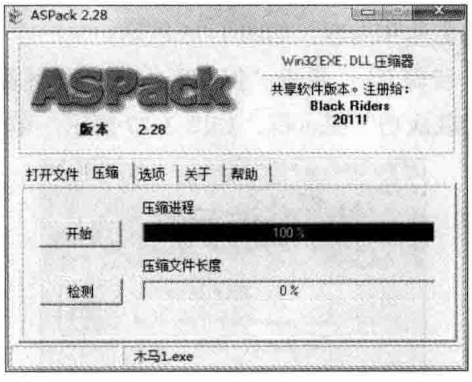


图 1-72 进行压缩

## 1.2.4 超级加花器

“超级加花器”是一款加花指令工具，该工具支持附加数据自动检测，对于存在附加数据的 EXE、DLL 等程序加花后仍可执行。使用“超级加花器”工具加花指令的具体操作如下。

步骤 01：下载并运行“超级加花器 v1.9”工具，即可打开“超级加花器”主窗口，如图 1-73 所示。直接拖动需要加花指令的程序到“文件名”文本框中并释放鼠标；在“花指令”下拉列表中选择相应的花指令，如图 1-74 所示。


图 1-73 “超级加花器”窗口


图 1-74 添加程序并选择花指令

步骤 02：单击“加花”按钮，即可看到“添加成功”提示框，如图 1-75 所示。单击“确定”按钮，即可完成加花操作。

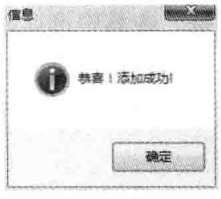


图 1-75 “添加成功”提示框

步骤 03：在“超级加花器”工具中还可以添加自定义的花指令。在“花指令名称”和“花指令内容”文本框中分别输入花指令的名称和内容，如图 1-76 所示。

步骤 04：单击“保存”按钮，即可看到“添加花指令成功，并加载成功”提示框，如图 1-77 所示。单击“确定”按钮，即可成功添加该花指令。


图 1-76 输入花指令名称和内容

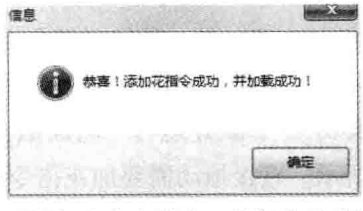


图 1-77 “添加花指令成功，并加载成功”提示框

# 1.3 入侵辅助工具

黑客在入侵过程中，往往会用到一些辅助工具，如在入侵注册表时使用 RegSnap 注册表快照工具获得目标主机注册表和系统的信息；而在进行密码破解时则使用字典制作工具制作字典，从而实现暴力破解密码的目的。

## 1.3.1 RegSnap 注册表快照工具

RegSnap 是一个优秀的注册表快照工具，可以详细地报告注册表及其他与系统有关项目的修改变化情况，且其报告结果既可以纯文本方式，也可以 HTML 网页方式显示。除报告系统注册表修改信息外，RegSnap 还可以报告系统的其他情况，如 Windows 的系统目录和系统的 system 子目录下文件的变化情况；Windows 的系统配置文件 win.ini 和 system.ini 的变化情况；以及自动批处理文件是否被修改过等。该工具的具体使用步骤如下。

步骤 01：下载 RegSnap 软件后，双击 RegSnap.exe 即可打开 regsnap 主窗口，如图 1-78 所示。

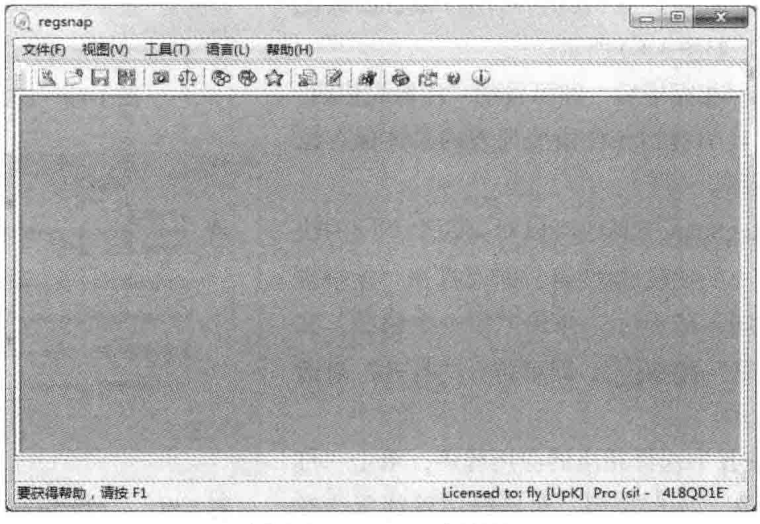


图 1-78 regsnap 主窗口

步骤 02：选择“文件”→“新建”菜单项或单击工具栏中的按钮，即可打开“保存快照”对话框，如图 1-79 所示。在其中看到有 3 种快照方式，各种快照的作用如下。

1）生成所有项目的快照：除记录注册表的数据外，还可记录系统目录、系统子目录、系统配置文件、系统自动批处理文件及引导文件的情况等信息，默认选中该选项。

2）仅生成注册表的快照：该选项仅对注册后的用户开放，主要是选择记录局域网上某台计算机的注册表情况。

3）远程 PC 的注册表：记录远程计算机注册表的数据，但是只适用与 RegSnap 专业版。

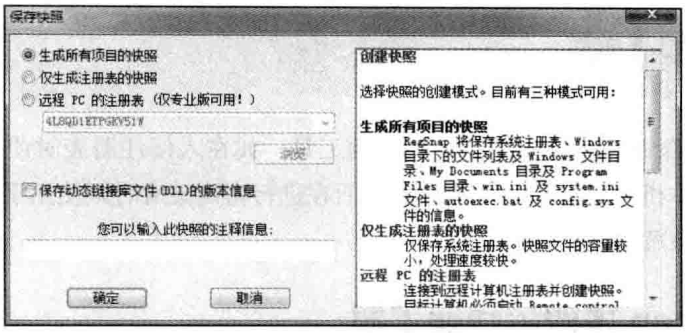


图 1-79 “保存快照”对话框

**注意**

“保存动态链接库文件的版本信息”复选框的作用还可以记录每个键值及 DLL 文件的变动情况。

步骤 03：在其中选择“生成所有项目的快照”单选项，单击“确定”按钮，即可对系统注册表进行快照，同时显示具体处理进度情况，向用户报告已经记录了多少个键值，如图 1-80 所示。


图 1-80 进行快照

步骤 04：在照相完毕后，即可看到“注册表快照”信息提示框，在其中看到各种快照列表的具体保存位置，如图 1-81 所示。

步骤 05：RegSnap 工具还可以对比两个不同的快照，单击工具栏上的比较按钮，即可打开“比较快照”对话框，如图 1-82 所示。单击“第一个快照”文本框后面的“浏览”按钮，即可打开“打开”对话框，如图 1-83 所示。


图 1-81 “注册表快照”信息提示框

步骤 06：在其中选择相应的应用程序，单击“打开”按钮，即可在“比较快照”对话框中看到所选择的快照文件，如图 1-84 所示。

步骤 07：采用同样方法选择第二个快照文件后，单击“确定”按钮，即可将这两个快照文件进行比较，具体比较结果如图 1-85 所示。通过比较快照文件，可以掌握注册表变动情况。

步骤 08：在 regsnap 主窗口中选择“工具”→“统计”菜单项，即可打开“完成注册表快照”信息框，在其中可看到注册表中各个项目的统计信息，如图 1-86 所示。

步骤 09：在 regsnap 主窗口中选择“工具”→“编辑快照注释”菜单项，即可打开“快照注释”对话框，在其中输入快照注释，如图 1-87 所示。单击“确定”按钮，即可为该快照文

件添加注释。

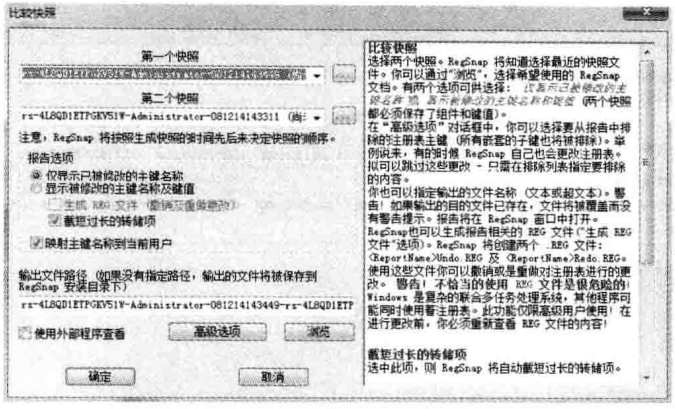


图 1-82 "比较快照"对话框

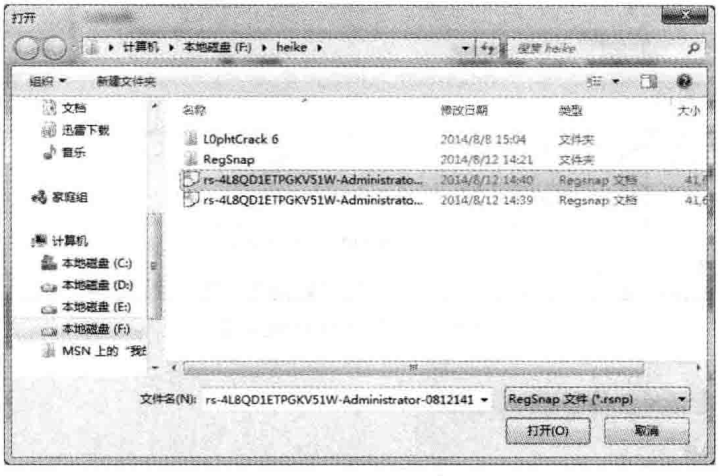


图 1-83 "打开"对话框

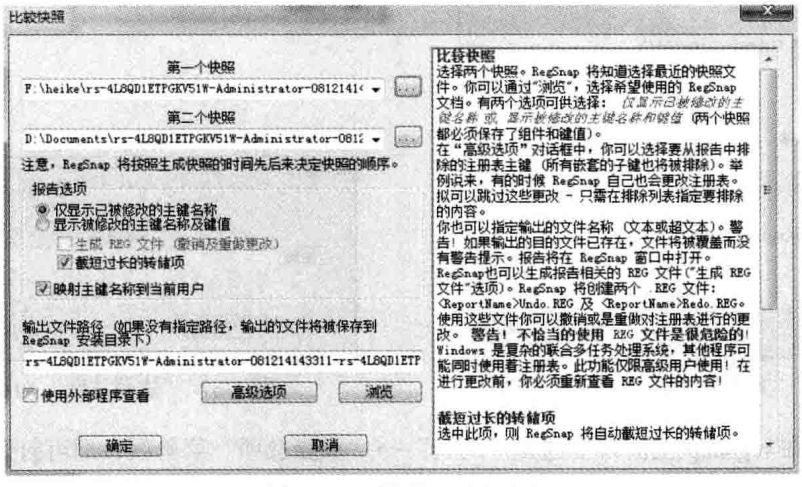


图 1-84 选择的快照文件

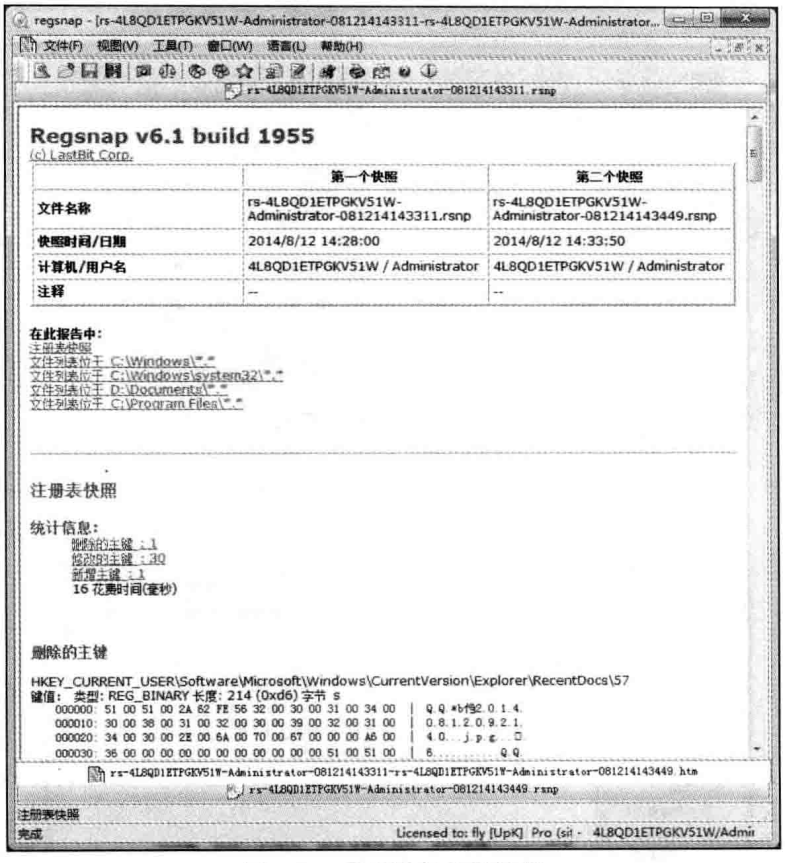


图 1-85 快照文件比较结果

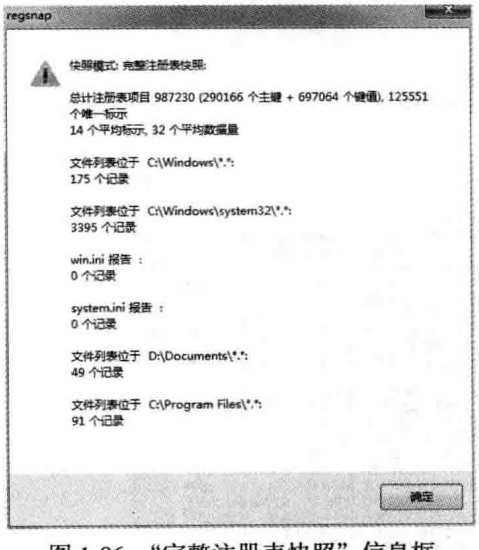


图 1-86 “完整注册表快照”信息框

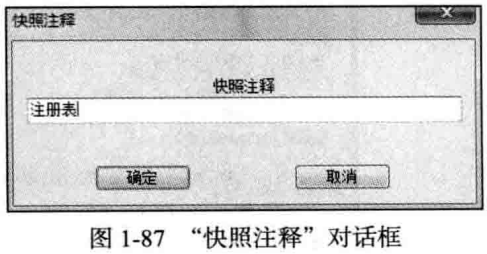


图 1-87 “快照注释”对话框

步骤 10：在 regsnap 主窗口中选择“工具”→“重置选项”菜单项，即可打开“你确定吗”提示框，如图 1-88 所示。单击“是”按钮，即可重置 regsnap 程序。

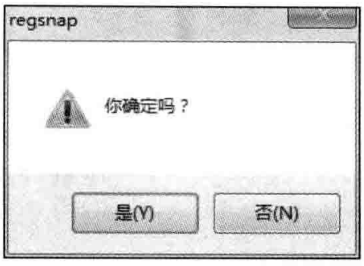


图 1-88 “你确定吗”提示框

## 1.3.2 字典制作工具

密码暴力破解虽然是黑客攻击比较基本的一项技术，但要成功破解密码并非那么简单。破解的成功率取决于多方面的因素，例如字典的制作、工具的使用等。目前可以用来制作字典的工具很多，如万能钥匙字典文件制作工具、易优超级字典生成器以及流光自带的字典制作工具等。这里以使用易优超级字典生成器为例介绍黑客字典的具体制作方法。

使用易优超级字典生成字典文件的具体操作步骤如下。

步骤 01：下载并运行“易优超级字典生成器”工具，即可打开“易优软件 – 超级字典生成器”主窗口，在其中可以看到易优超级字典生成器的主要功能，如图 1-89 所示。

步骤 02：选择“基本字符”选项卡，在其中选择字典文件需要数字、字母以及其他字符，如图 1-90 所示。

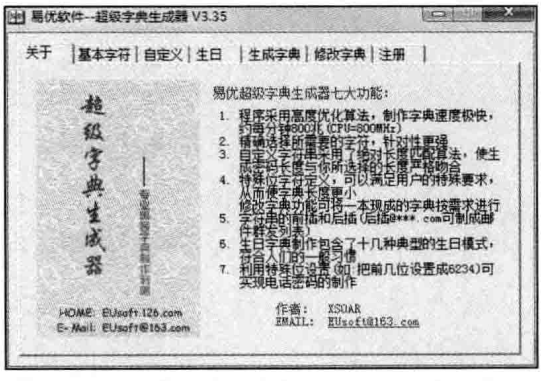


图 1-89 “易优软件 – 超级字典生成器”主窗口


图 1-90 “基本字符”选项卡

步骤 03：在“生日”选项卡中设置生日的范围以及显示模式等属性，如图 1-91 所示。

步骤 04：选择“生成字典”选项卡，通过单击“浏览”按钮设置要生成字典文件的保存位置，如图 1-92 所示。

步骤 05：在设置完“密码位数”属性后，单击“生成字典”按钮，即可看到“真的要生成字典吗”提示框，如图 1-93 所示。单击“确定”按钮，即可开始生成字典文件，待完成后将会出现一个“字典制作完成”提示框，如图 1-94 所示。

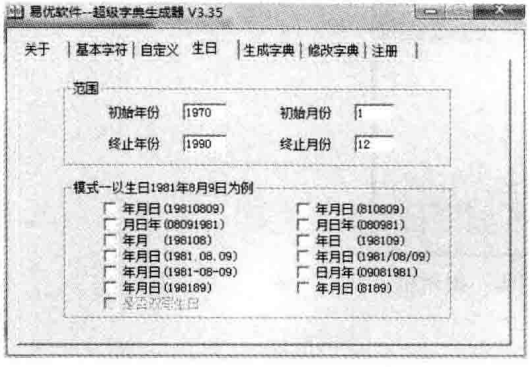


图 1-91 “生日”选项卡


图 1-92 “生成字典”选项卡

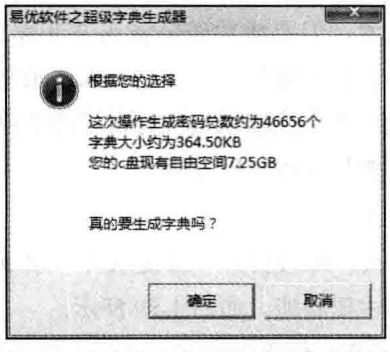


图 1-93 “真的要生成字典吗”提示框

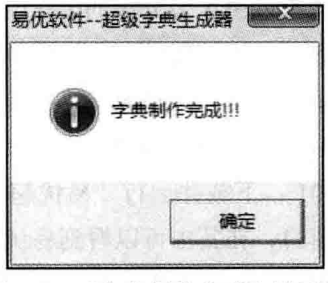


图 1-94 “字典制作完成”提示框

# 第2章 扫描与嗅探工具

黑客在进行攻击前，常常会利用专门的扫描和嗅探工具对目标计算机进行扫描。在分析目标计算机的各种信息之后，才会对其进行攻击。本章将介绍几款常见的嗅探与扫描工具。

扫描工具和嗅探工具是黑客使用最频繁的工具，只有充分掌握了目标主机的详细信息，才可以进行下一步操作。同时合理地利用扫描和嗅探工具，还可以实现配置系统的目的。

本章要点：

- 端口扫描器
- 漏洞扫描器
- 常见的嗅探工具
- Real Spy Monitor 监控网络

# 2.1 端口扫描器

由于网络服务和端口是一一对应的，如 FTP 服务通常开设在 TCP 21 端口，Telnet 服务通常开设在 TCP 23 端口，所以黑客在攻击前要进行端口扫描，其主要目的是取得目标主机开放的端口和服务信息，从而为“漏洞检测”做准备。

## 2.1.1 X-Scan 扫描器

X-Scan 工具采用多线程方式对指定 IP 地址段（或单机）进行安全漏洞检测，且支持插件功能。它可以扫描出操作系统类型及版本、标准端口状态及端口 BANNER 信息、CGI 漏洞、IIS 漏 洞、RPC 漏 洞、SQL-SERVER、FTP-SERVER、SMTP-SERVER、POP3-SERVER、NT-SERVER 弱口令用户、NT 服务器 NETBIOS 等信息。

### （1）设置 X-Scan 扫描器

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

步骤 01：在 X-Scan 文件夹中双击 X-Scan_gui.exe 应用程序，即可打开 X-Scan v3.3 GUI 主窗口，在其中可以浏览此软件的功能简介、常见问题解答等信息，如图 2-1 所示。单击工具栏中的扫描参数按钮，即可打开“扫描参数”对话框，如图 2-2 所示。

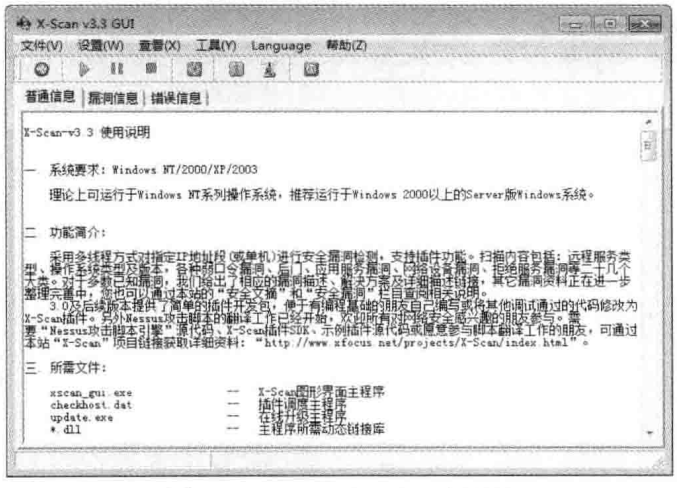


图 2-1 X-Scan v3.3 GUI 主窗口

步骤 02：在左边的列表中单击“检测范围”选项卡，在“指定 IP 范围”文本框中输入要扫描的 IP 地址范围。若不知道输入的格式，则可以单击“示例”按钮，即可打开“示例”提示框，在其中看到各种有效格式，如图 2-3 所示。

步骤 03：在“全局设置”选项卡中单击“扫描模块”子选项，即可选择扫描过程中需要扫描的模块，还可在右侧窗格中查看选择的模块的相关说明，如图 2-4 所示。

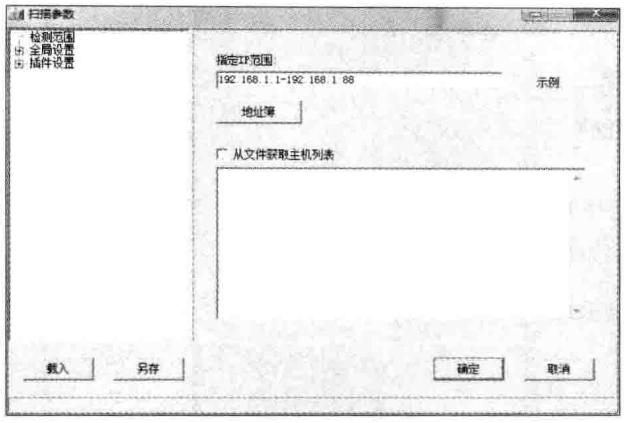


图 2-2 “扫描参数”对话框


图 2-3 “示例”提示框

步骤 04：由于 X-Scan 是一款多线程扫描工具，所以可以在“并发扫描”子选项中设置扫描时的线程数量，如图 2-5 所示。在“扫描报告”子选项中可以设置扫描报告存放的路径和文件格式，如图 2-6 所示。

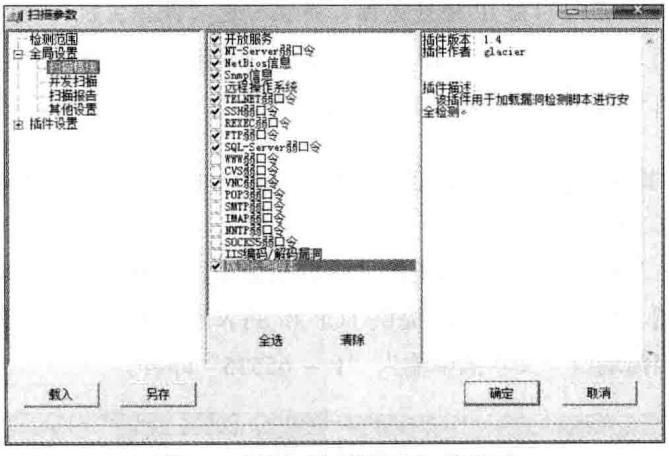


图 2-4 设置“扫描模块”子选项

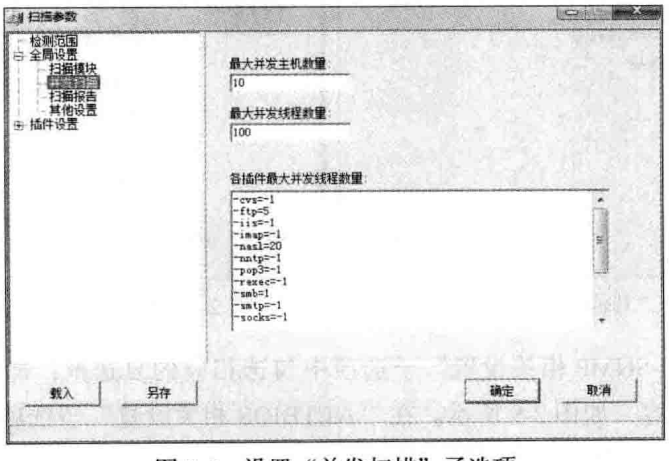


图 2-5 设置“并发扫描”子选项

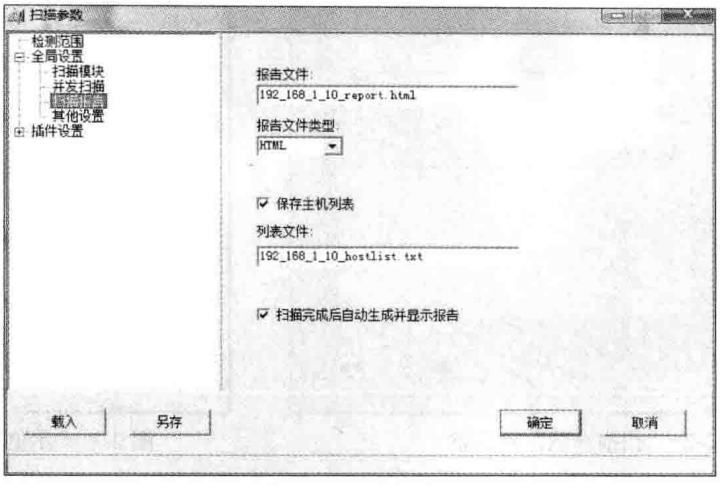


图 2-6　设置“扫描报告”子选项

**提示**

如果需要保存设置的扫描 IP 地址范围，则在勾选“保存主机列表”复选框后输入保存文件名称，就可以直接调用这些 IP 地址范围了。如果在扫描结束时自动生成报告文件并显示报告，则可勾选“扫描完成后自动生成并显示报告”复选框。

步骤 05：在“其他设置”子项中可以设置扫描过程的其他属性，如设置扫描方式、显示详细进度等，如图 2-7 所示。

步骤 06：单击“插件设置”选项下的“端口相关设置”子选项，即可设置扫描端口范围以及检测方式，如图 2-8 所示。X-Scan 提供 TCP 和 SYN 两种扫描方式；若要扫描某主机的所有端口，则在“待扫描端口”文本框中输入“1 ~ 65535”即可。

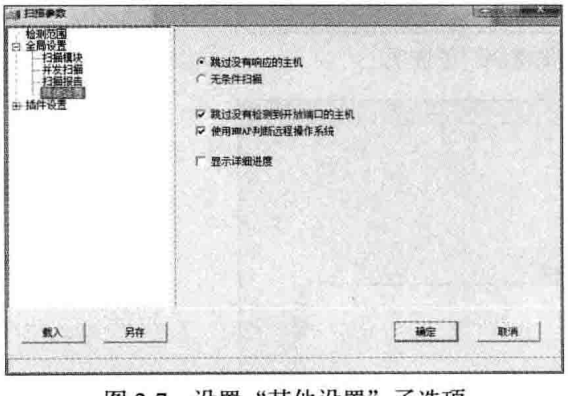


图 2-7　设置“其他设置”子选项

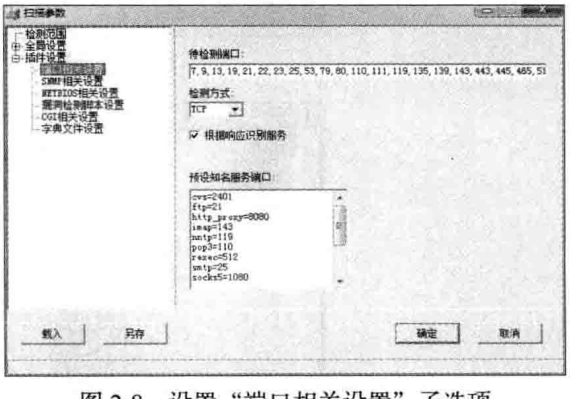


图 2-8　设置“端口相关设置”子选项

步骤 07：在“SNMP 相关设置”子选项中勾选相应的复选框，即可设置在扫描时获取 SNMP 信息的内容，如图 2-9 所示。在“NETBIOS 相关设置”子选项中设置需要获取的 NETBIOS 信息类型，如图 2-10 所示。

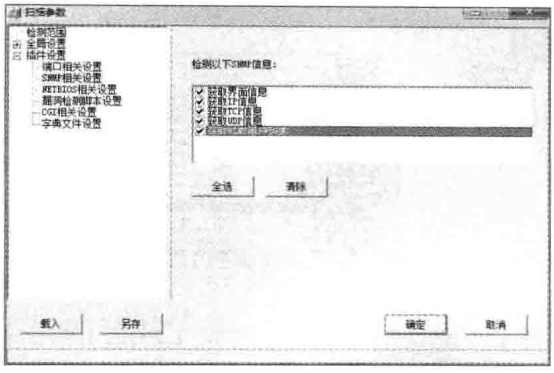


图 2-9 设置“SNMP 相关设置”子选项

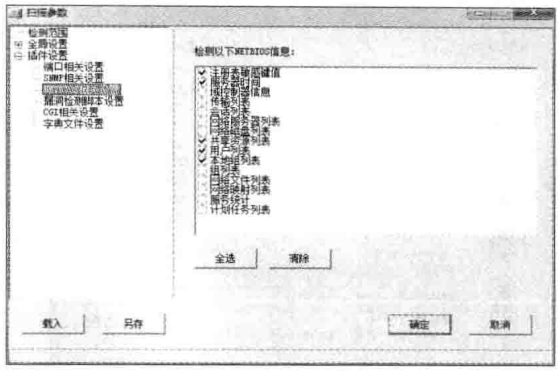


图 2-10 设置“NETBIOS 相关设置”子选项

步骤 08：在“漏洞检测脚本设置”子选项中取消勾选“全选”复选框之后，单击“选择脚本”按钮，即可打开 Select Scripts（选择脚本）对话框，如图 2-11 所示。

步骤 09：在选择检测的脚本文件之后，单击“确定”按钮返回“扫描参数”对话框中，分别设置脚本运行超时和网络读取超时等属性，如图 2-12 所示。

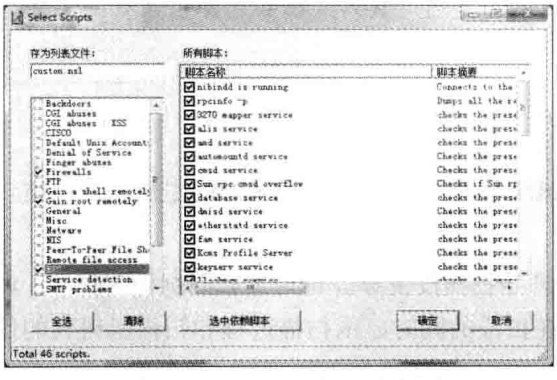


图 2-11 Select Scripts 对话框

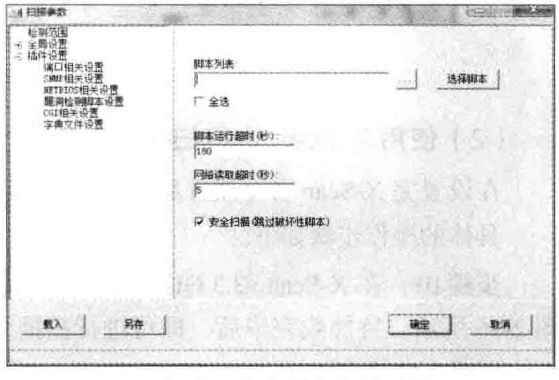


图 2-12 设置脚本运行属性

步骤 10：在“CGI 相关设置”子选项中可设置扫描时需要使用的 CGI 选项，如图 2-13 所示。在“字典文件设置”子选项中双击字典类型，即可打开“打开”对话框，如图 2-14 所示。

步骤 11：在其中选择相应的字典文件，单击“打开”按钮返回到“扫描参数”对话框，即可看到选中的文件名字和可以选择的字典文件，如图 2-15 所示。在设置好所有选项之后，单击“确定”按钮，即可完成设置。

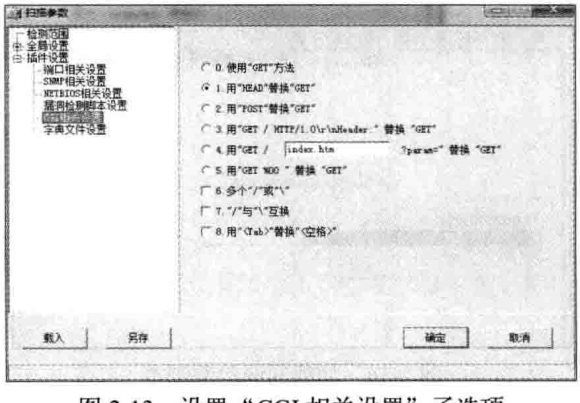


图 2-13 设置“CGI 相关设置”子选项


图 2-14 “打开”对话框

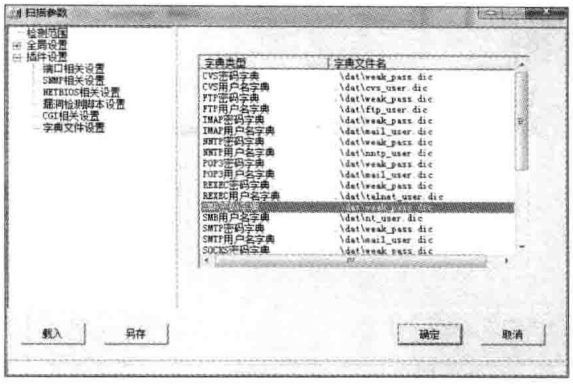


图 2-15 设置“字典文件设置”子选项

## 小技巧

将来如果还想使用相同设置进行扫描，则可以对本次设置进行保存。在“扫描参数”对话框中单击“另存”按钮，即可打开“另存为”对话框，在其中设置保存的位置和名称。单击“确定”按钮完成设置。而当再次使用时只需单击“载入”按钮选择已保存的文件即可。

### （2）使用 X-Scan 进行扫描

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

步骤 01：在 X-Scan v3.3 GUI 主窗口中单击开始扫描按钮 ▶，即可加载漏洞检测脚本，如图 2-16 所示。待加载完毕后，即可进行扫描，在扫描的同时显示扫描进程和扫描所得到的信息，如图 2-17 所示。

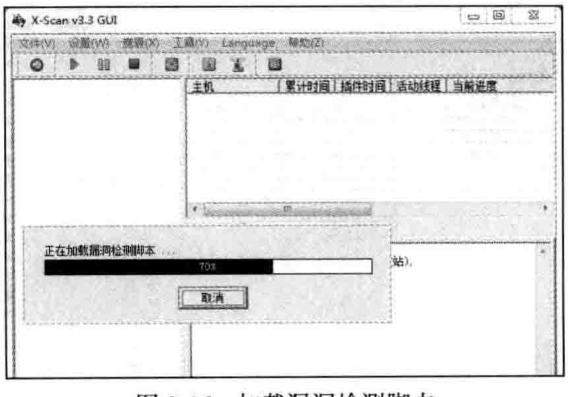


图 2-16 加载漏洞检测脚本


图 2-17 显示扫描进程和信息

步骤 02：在扫描完成之后，即可看到 HTML 格式的扫描报告，可看到活动主机 IP 地址、存在的系统漏洞和其他安全隐患，同时还提出了安全隐患的解决方案，如图 2-18 所示。

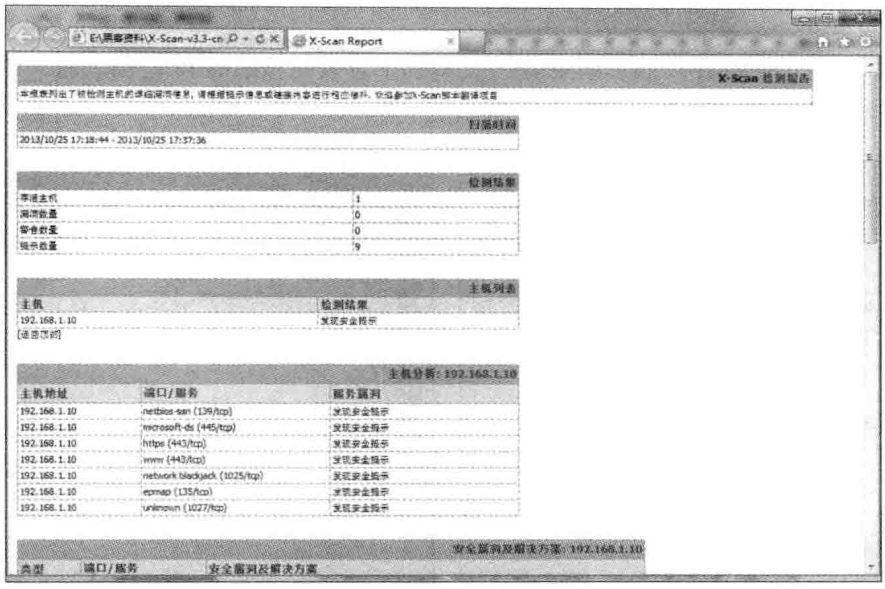


图 2-18 HTML 格式的扫描报告

步骤 03：在 X-Scan v3.3 GUI 主窗口中选择“漏洞信息”选项卡，即可看到存在漏洞的主机信息。

步骤 04：利用 X-Scan 扫描工具不仅可以扫描目标计算机开放端口及存在的安全隐患，还具有查询目标计算机物理地址、检测本地计算机网络信息和 Ping 目标计算机等功能。在 X-Scan 窗口中选择“工具”→“物理地址查询”菜单项，即可打开“工具”对话框，在“IP 地址 / 主机名”文本框中输入相应的 IP 地址，如图 2-19 所示。


图 2-19 输入 IP 地址

步骤 05：单击“查询物理地址”按钮，即可查看目标计算机的信息。在 ARP query（ARP 查询）选项卡中单击 Query（查询）按钮，即可显示出本机所在局域网中所有主机的 IP 地址和物理地址。在该工具中还可以执行域名查询、路由跟踪等操作。

## 2.1.2 SuperScan 扫描器

扫描类黑客工具 SuperScan 自带有一个木马端口列表 Trojans.lst，通过这个列表可以检测目标计算机是否有木马，也可以自定义修改这个木马端口列表。主要功能有通过 Ping 检验 IP 是否在线、IP 和域名相互转换、检验目标计算机提供的服务类别、检验一定范围目标计算机是否在线和端口情况等。使用 SuperScan 进行扫描的具体操作步骤如下。

步骤 01：下载 SuperScan 工具之后，运行其中的 SuperScan.exe 应用程序，即可打开

SuperScan 4.0 主窗口，如图 2-20 所示。

步骤 02：在“开始 IP”和“结束 IP”文本框中设置要扫描的 IP 范围之后，单击 按钮，即可将其添加到右边的列表中，如图 2-21 所示。


图 2-20　SuperScan 4.0 主窗口

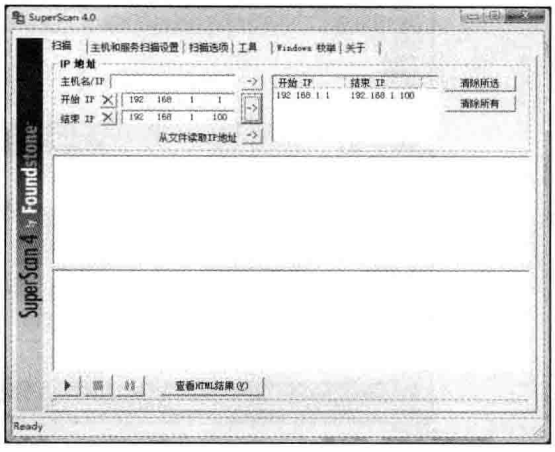


图 2-21　添加 IP 地址范围

步骤 03：在设置完毕之后，单击 按钮，即可开始扫描。在扫描结束之后，SuperScan 将提供一个主机列表，用于显示每台扫描过的主机被发现的开放端口信息，如图 2-22 所示。

步骤 04：SuperScan 还有选择以 HTML 格式显示信息的功能，单击“查看 HTML 结果”按钮，即可打开 SuperScan Report 页面，在其中显示扫描了的主机和以及每台主机中开放的端口，如图 2-23 所示。


图 2-22　查看扫描结果

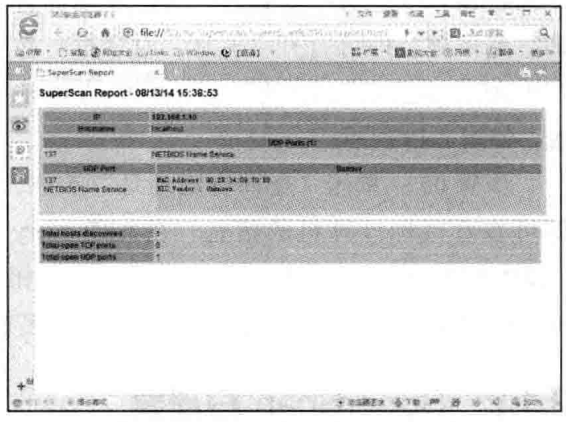


图 2-23　SuperScan Report 页面

步骤 05：在 SuperScan 软件中还可自己定制扫描方式。在 SuperScan 4.0 主窗口中单击“Windows 枚举”选项卡，在“主机名 /IP/URL”文本框中输入目标主机的 IP 地址，如图 2-24 所示。单击“枚举”按钮，即可在列表中看到该主机各种信息，如图 2-25 所示。

步骤 06：在“主机和服务扫描设置”选项卡中可以设置扫描主机和服务的各种属性，如

图 2-26 所示。如在“查找主机”栏目将“发现主机”方法设置为“回显请求”；在“UDP 端口扫描”和“TCP 端口扫描”栏目中设置要扫描的端口。因为一般的主机都有超过 65000 个的 TCP 和 UDP 端口，若对每个可能开放端口的 IP 地址进行超过 130000 次的端口扫描，将无疑需要耗费太长的时间。这里需要自己定义要扫描端口范围，也可以只扫描常用的几个端口。


图 2-24 “Windows 枚举”选项卡

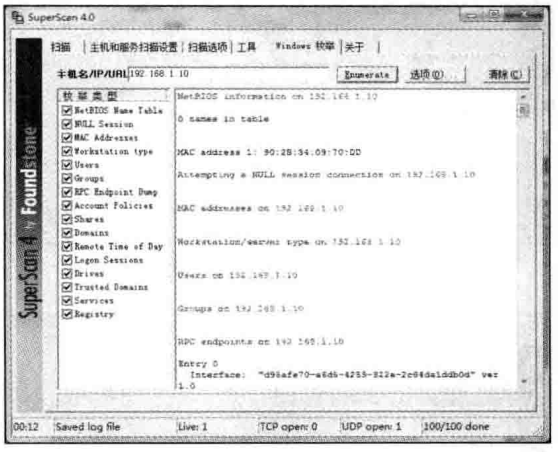


图 2-25 枚举目标主机信息

**提示**

在“主机和服务扫描设置”选项卡中选择的选项越多，则扫描用的时间就越长。如果用户正在试图尽量多地收集一个明确的主机信息，建议先执行一次常规的扫描以发现主机，再利用可选的请求选项来扫描。

步骤 07：在“扫描选项”选项卡中设置与扫描有关的各种属性，如将“检测开放主机次数”设置为 1，如图 2-27 所示。还可以设置扫描速度和通过扫描的数量，其中“查找主机名”选项可设置主机名解析通过的数量（默认值是 1）。当扫描速度设置为 0 时，虽然扫描速度最快，但却存在数据包溢出的可能。如果担心 SuperScan 引起的过量包溢出，则最好调慢 SuperScan 扫描的速度。

**提示**

“获取标志”选项用于显示一些信息尝试得到远程主机的回应（默认延迟是 8000 毫秒），如果所连接主机较慢，则该段时间就不够长。旁边滚动条是扫描速度调节选项，用于调节 SuperScan 在发送每个包时所要等待的时间（调节滚动条为 0 时扫描速度最快）。

步骤 08：在“工具”选项卡中可利用 SuperScan 提供的各种工具得到目标主机的各种信息，如图 2-28 所示。如果想得到目标主机的主机名，则在“主机名 /IP/URL”文本框中输入目标主机 IP 地址，单击“查找主机名 /IP”按钮，即可得到该主机的主机名，如图 2-29 所示。

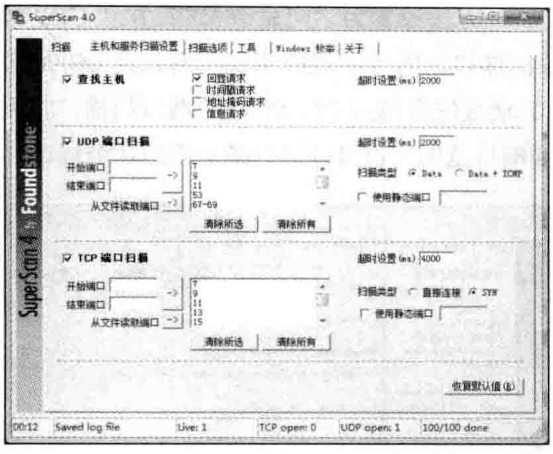


图 2-26 “主机和服务扫描设置”选项卡


图 2-27 “扫描选项”选项卡


图 2-28 “工具”选项卡


图 2-29 查询目标主机的主机名

## 2.1.3 ScanPort

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

步骤 01：下载并运行 ScanPort 程序，即可打开 ScanPort 主窗口，在其中设置起始 IP 地址、结束 IP 地址以及要扫描的端口号，如图 2-30 所示。单击“扫描”按钮，即可进行扫描，从扫描结果中可以看出设置的 IP 地址段中计算机开启的端口，如图 2-31 所示。

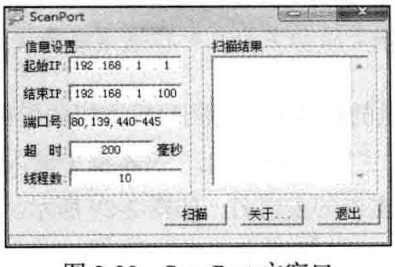


图 2-30 ScanPort 主窗口

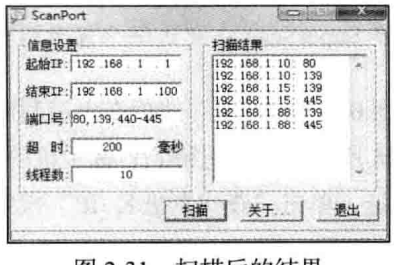


图 2-31 扫描后的结果

步骤 02：如果扫描某台计算机中开启的端口，则将开始 IP 和结束 IP 都设置为该主机的 IP 地址，如图 2-32 所示。在设置完要扫描的端口号之后，单击“扫描”按钮，即可扫描出该主机中开启的端口（设置端口范围之内），如图 2-33 所示。

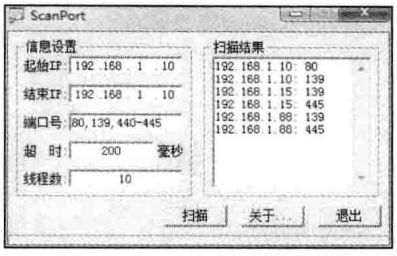


图 2-32 扫描某台计算机开启的端口

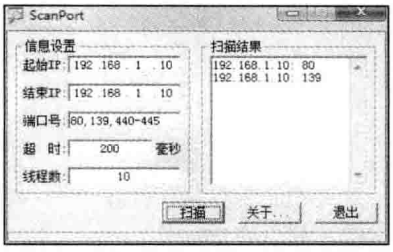


图 2-33 扫描该主机中开启的端口

## 2.1.4 极速端口扫描器

利用扫描端口的工具“极速端口扫描器”不仅可以扫描端口，还可以实现在线更新 IP 地址，将扫描结果导出为纯文本、网页以及 XLS 格式。使用该工具扫描端口的操作步骤如下。

步骤 01：下载并运行“极速端口扫描器 V2.0.500”，即可打开“极速端口扫描器”主窗口，如图 2-34 所示。切换到“参数设置”选项卡，即可看到该工具自带的 IP 地址段以及各种参数，如图 2-35 所示。

图 2-34 “极速端口扫描器”主窗口

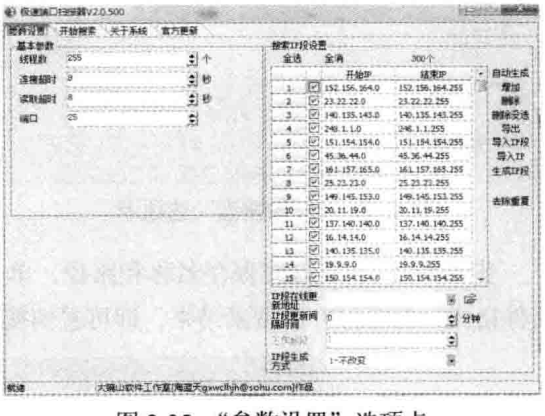

图 2-35 “参数设置”选项卡

步骤 02：如果要对目标主机进行扫描，则需添加指定的 IP 段。在“参数设置”选项卡中单击“增加”按钮，即可打开“IP 段编辑”对话框，如图 2-36 所示。

步骤 03：在“开始 IP”和“结束 IP”文本框中分别输入起始 IP 地址和结束 IP 地址，单击“确定”按钮，即可将该 IP 段添加到“搜索 IP 段设置”列表中，如图 2-37 所示。

步骤 04：单击“全消”按钮，即可取消选择所有的 IP 段。在其中勾选刚添加的 IP 段，将要扫描的端口设置为 80，如图 2-38 所示。

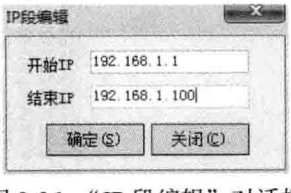


图 2-36 “IP 段编辑”对话框

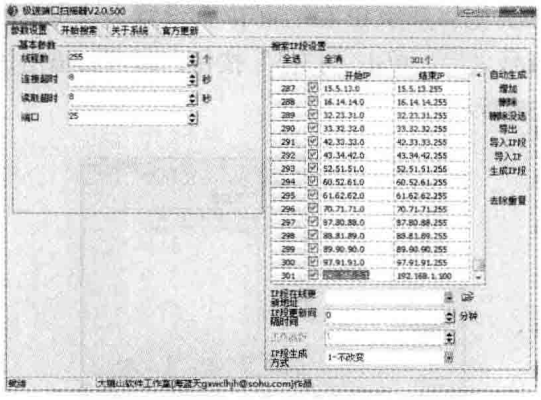

图 2-37 将 IP 段添加到“搜索 IP 段设置”列表中

图 2-38 设置扫描参数

步骤 05：选择“开始搜索”选项卡，在其中单击“开始搜索”按钮，即可扫描指定的 IP 段，扫描结果如图 2-39 所示。可以将扫描的结果保存为纯文本、网页、XLS 等格式。在“开始搜索”选项卡中单击“导出”按钮，即可打开“另存为”对话框，如图 2-40 所示。

图 2-39 “开始搜索”选项卡


图 2-40 “另存为”对话框

步骤 06：在设置完保存名称和路径，单击“保存”按钮，即可将扫描结果保存为记事本文件格式。打开保存的搜索结果，即可看到搜索到的 IP 地址及搜索的端口，如图 2-41 所示。

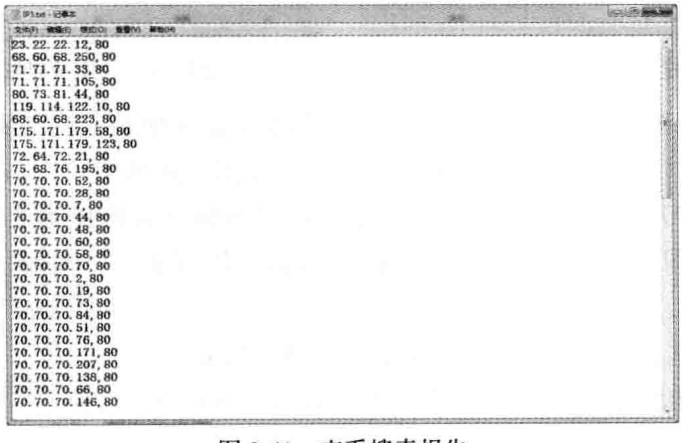


图 2-41 查看搜索报告

## 2.2 漏洞扫描器

安全管理员还需要做很多工作，如漏洞的及时升级、及时给系统打补丁、设置正确的用户权限等，而漏洞扫描工具可以帮助管理员查找系统中的缺陷。

### 2.2.1 SSS 扫描器

系统漏洞扫描器 SSS（Shadow Security Scaner）的功能很强大，如端口探测、端口 banner 探测、CGI/ASP 弱点探测、Unicode/Decode/printer 探测、*nix 弱点探测、（POP3/FTP）密码破解、拒绝服务探测、操作系统探测、NT 共享 / 用户探测。对于探测出的漏洞，有详细的说明和解决方法。利用 SSS 扫描器对系统漏洞进行扫描的具体操作步骤如下。

步骤 01：在安装好 SSS 软件后，双击 Shadow Security Scaner 图标，即可打开 Shadow Security Scaner 主窗口，如图 2-42 所示。单击工具栏中的 New session（新建项目）按钮，即可打开 New session 窗口，如图 2-43 所示。

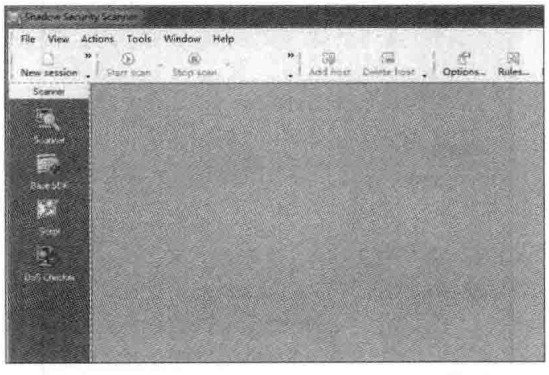


图 2-42 Shadow Security Scaner 主窗口

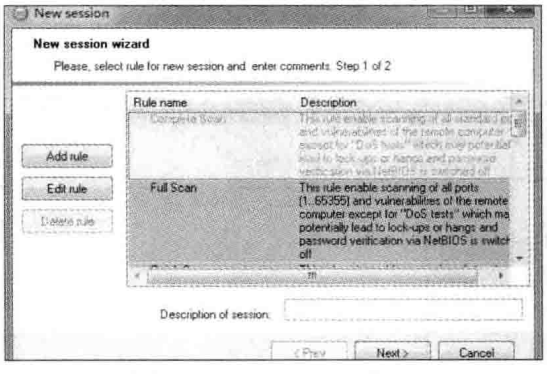


图 2-43 New session 窗口

步骤 02：可选择预设的扫描规则，也可单击 Add rule（添加规则）按钮添加扫描规则。单击“添加规则”按钮，即可打开 Create new rule（创建新规则）对话框，如图 2-44 所示。

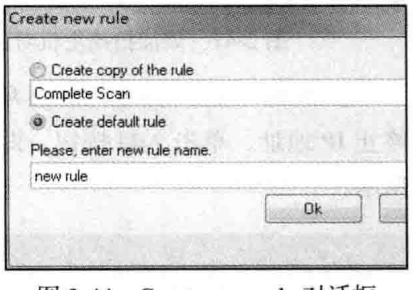


图 2-44 Create new rule 对话框

步骤 03：选中 Create copy of the rule（创建副本的规则）单选项，在其下拉列表中选择 Complete Scan（完全扫描）选项；再输入新创建规则的名称，单击 OK 按钮，即可打开 Security Scanner Rules 窗口，如图 2-45 所示。

步骤 04：在其中设置相应的属性，单击 OK 按钮返回到 New session 窗口，即可看到新创建的规则，如图 2-46 所示。

步骤 05：选中刚创建的规则后，单击 Next（下一步）按钮，即可打开添加扫描主机窗口，

如图 2-47 所示。单击 Add host（添加主机）按钮，即可打开“添加主机”对话框，如图 2-48 所示。

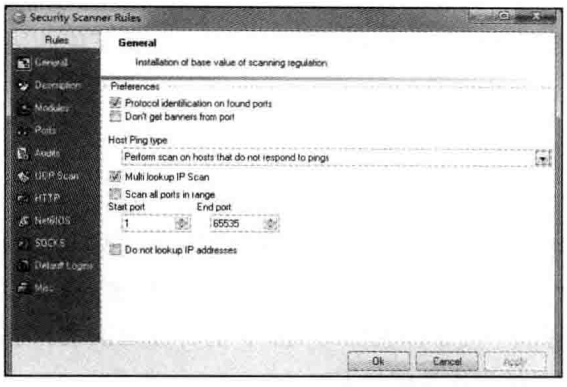


图 2-45　Security Scanner Rules 窗口

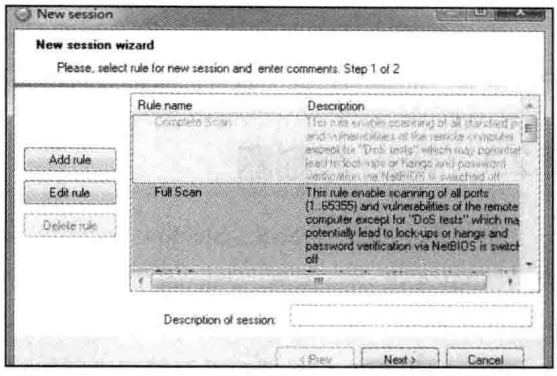


图 2-46　查看新创建的规则

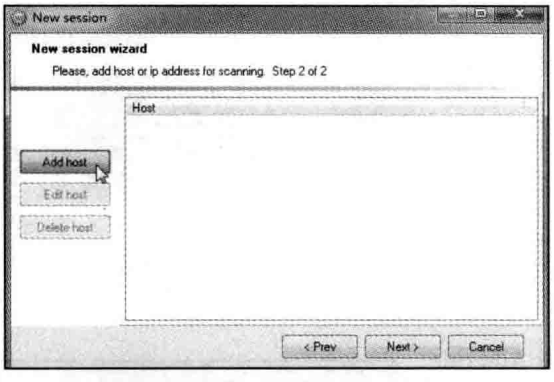


图 2-47　添加扫描主机对话框

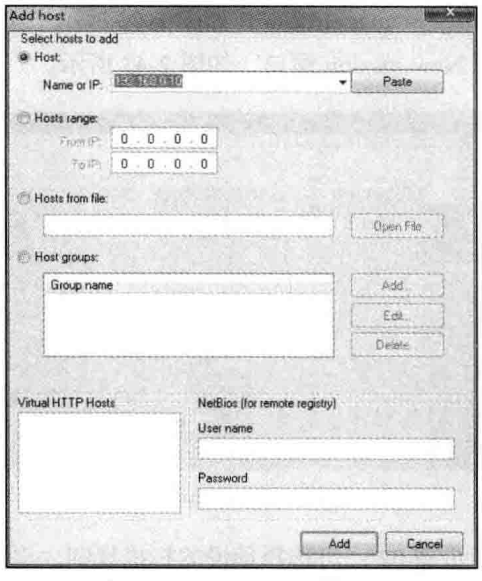


图 2-48　Add host 对话框

步骤 06：选择 Hosts range 单选项，在 From IP 和 To IP 文本框中分别输入起始 IP 地址和终止 IP 地址，单击 Add 按钮，即可在添加扫描主机窗口中看到添加的 IP 地址段，如图 2-49 所示。

**提示**

如果要扫描单个计算机，则需在“添加主机”对话框中选择“Host（主机）”单选项，在 Name or IP 文本框中输入目标计算机的 IP 地址或名称；如果要添加已经存在的主机列表，则选择 Host from file（主机来自于文件）单选项；如果选择 Host groups 单选项，则表示通过添加工作组的方式添加目标计算机。

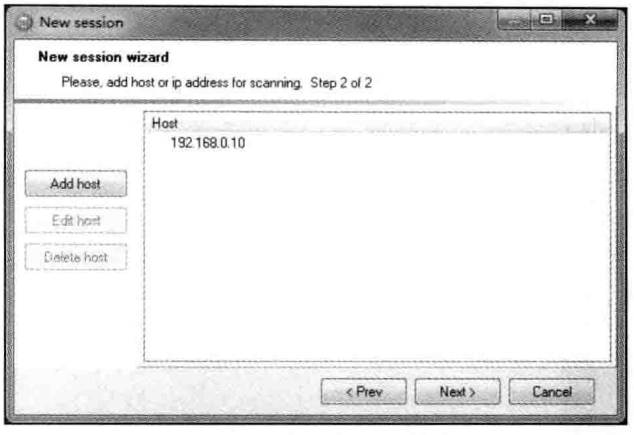


图 2-49 添加的 IP 地址段

步骤 07：单击 Next（下一步）按钮，即可完成扫描项目的创建并返回 Shadow Security Scaner 主窗口，在其中看到所添加的主机。

步骤 08：单击工具栏上的 Start Scan（开始扫描）按钮，即可开始对目标计算机进行扫描，并可在 Statistics 标签卡中查看扫描进程，如图 2-50 所示。

步骤 09：待扫描结束后，在 Vulnerabilities（漏洞）选项卡中可看到扫描出的漏洞程序，单击相应的漏洞程序，在下方看到该漏洞的介绍以及补救措施，如图 2-51 所示。

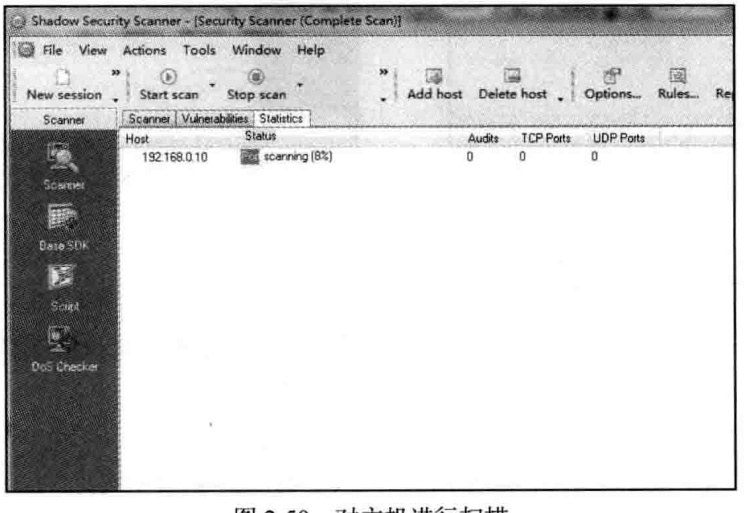


图 2-50 对主机进行扫描

步骤 10：使用 SSS 还可以进行 DoS 安全性进行检测。单击左侧的 DoS Checker（DoS 检查器）按钮，即可打开“DoS 检查器”对话框，如图 2-52 所示。在其中选择检测的项目并设置扫描的线程数（Threads），单击 Start（开始）按钮，即可进行 DoS 检测。

步骤 11：在 Shadow Security Scaner 主窗口中选择 Tools（工具）→ Options（选项）菜单项，即可打开 Security Scaner Options（SSS 选项设置）对话框，在其中可以设置扫描各个选项，如图 2-53 所示。

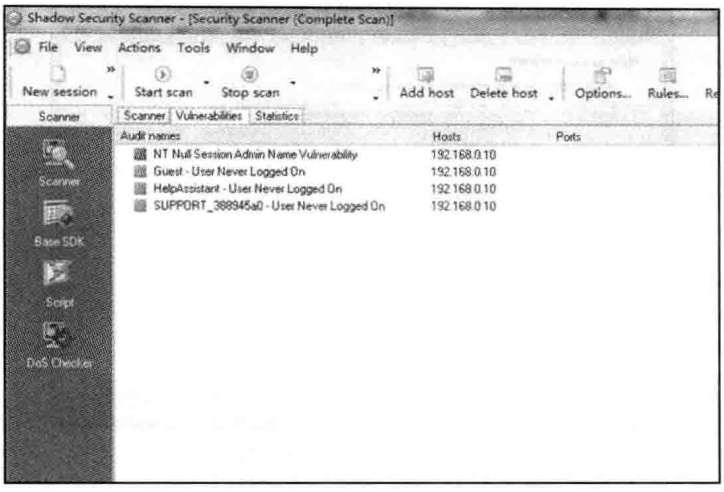


图 2-51 漏洞选项卡

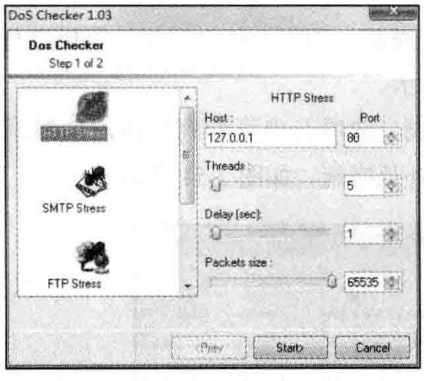


图 2-52 “DoS 检查器”对话框

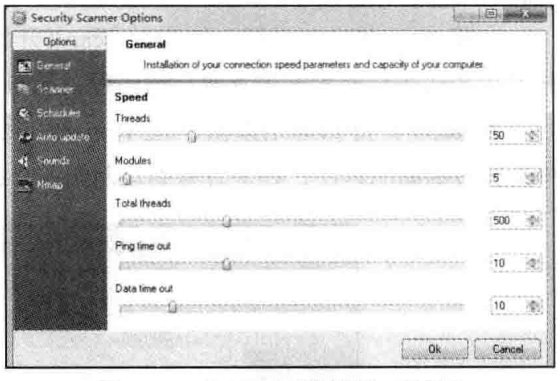


图 2-53 “SSS 选项设置”对话框

## 2.2.2 S-GUI Ver 扫描器

S-GUI Ver 扫描器是以 S.EXE 为核心的可视化端口扫描工具，支持多端口扫描、支持线程控制、隐藏扫描、扫描列表、去掉端口、自动整理扫描结果等。

使用 S-GUI Ver 扫描器扫描漏洞的具体操作步骤如下。

步骤 01：下载并解压 S-GUI Ver2.0 软件，双击其中的 S-GUI Ver2.0.exe 文件，即可打开 S-GUI Ver2.0 主窗口，如图 2-54 所示。

步骤 02：在“扫描分段”选项框中分别输入开始扫描的 IP 地址和结果扫描的 IP 地址，在“扫描设置”选项框中的“端口”文本框中输入要扫描的端口，在“协议”选项区中选择 TCP 单选项，如图 2-55 所示。

步骤 03：单击“开始扫描”按钮，即可打开“提示”信息框，在其中看到“扫描已经开始，正在扫描中，扫描完毕后有提示”的提示信息，如图 2-56 所示。

步骤 04：单击“确定”按钮，即可打开 Windows Script Host 提示框，在其中看到“扫描

完毕！请载入结果…”提示信息，如图 2-57 所示。


图 2-54 S-GUI Ver2.0 主窗口

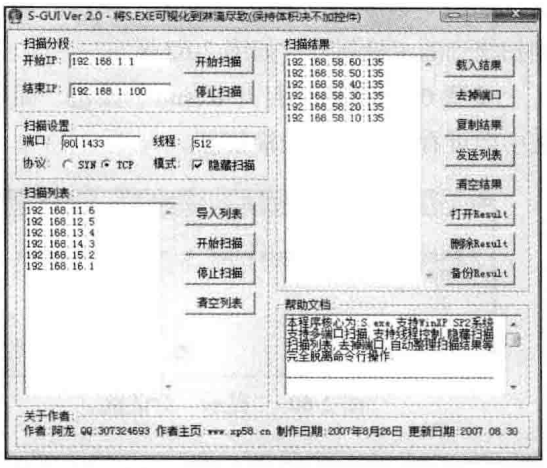


图 2-55 “输入扫描 IP 后的 S-GUI Ver2.0”窗口

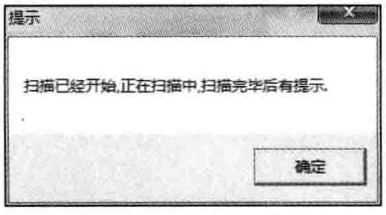


图 2-56 “提示”对话框


图 2-57 “Windows Script Host”对话框

步骤 05：单击“确定”按钮，即可返回 S-GUI Ver2.0 主窗口，单击右侧“载入结果”按钮，即可打开“提示”信息框，在其中看到“你真的要 [ 载入结果 ] 吗？如果‘是’将会覆盖掉 [ 扫描结果 ] 中的原有数据”提示信息，如图 2-58 所示。

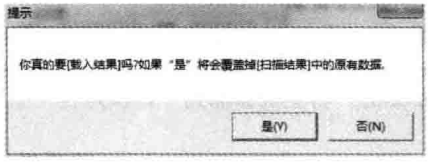


图 2-58 “提示”对话框

步骤 06：单击“是”按钮，即可将扫描结果添加到“扫描结果”文本区域中，在其中看到扫描到的开放指定端口主机的 IP 地址以及端口号，如图 2-59 所示。

步骤 07：如果想要将扫描结果内容放入左侧扫描列表中，单击“发送列表”按钮，即可打开“提示”信息框，在其中看到“你真的要将 [ 扫描结果 ] 发送到 [ 扫描列表 ] 吗？如果‘是’将会覆盖掉 [ 扫描列表 ] 中的原有数据”提示信息，如图 2-60 所示。

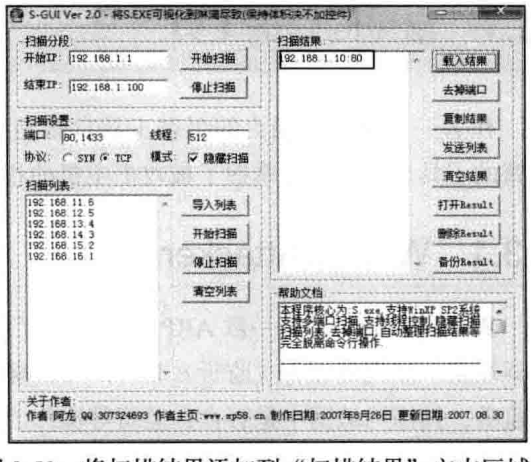


图 2-59 将扫描结果添加到“扫描结果”文本区域中