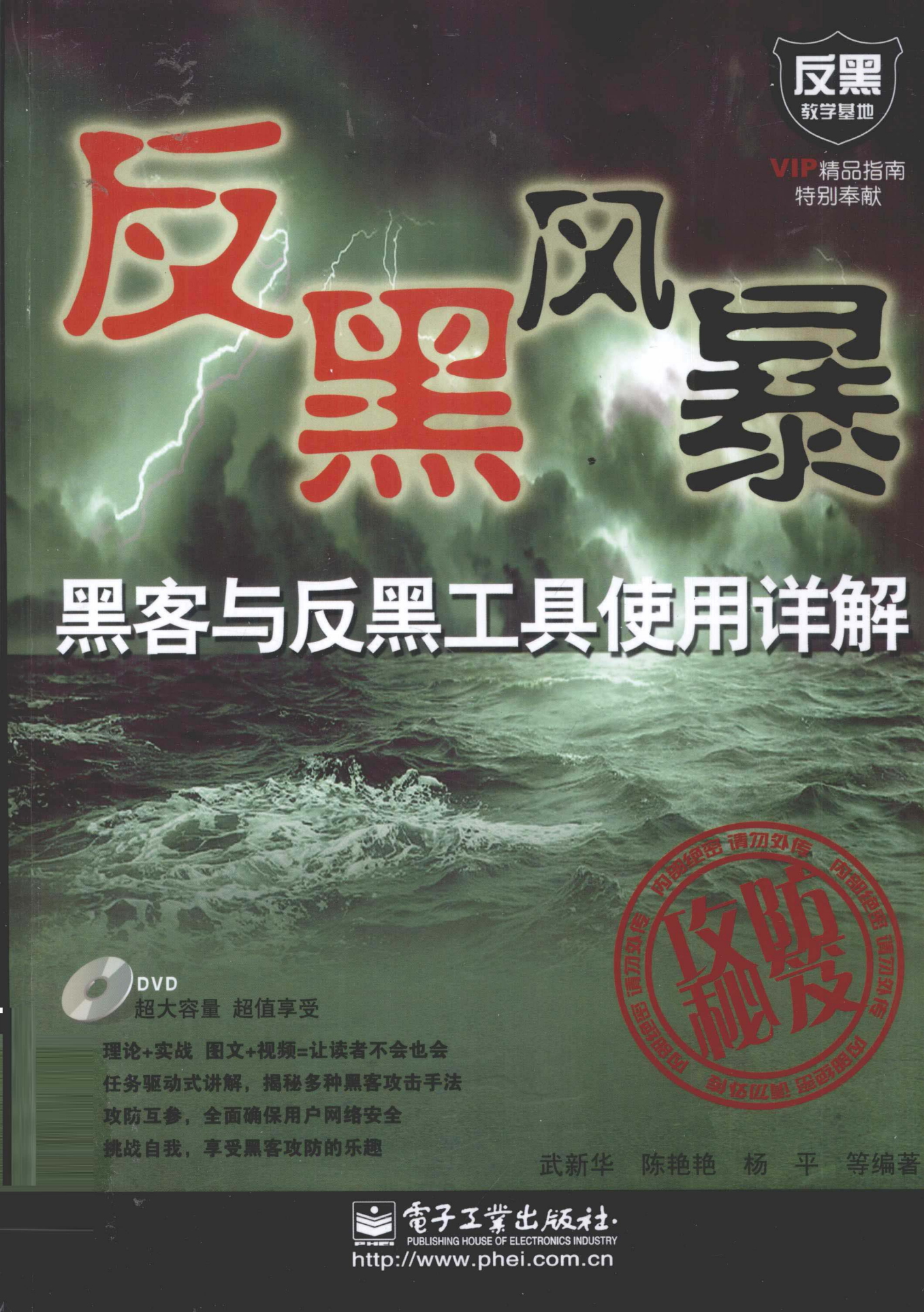
反黑
教学基地

VIP精品指南
特别奉献

反黑风暴

黑客与反黑工具使用详解



DVD
超大容量 超值享受

理论+实战 图文+视频=让读者不会也会
任务驱动式讲解，揭秘多种黑客攻击手法
攻防互参，全面确保用户网络安全
挑战自我，享受黑客攻防的乐趣

武新华 陈艳艳 杨 平 等编著

電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
http://www.phei.com.cn

反黑风暴

黑客与反黑工具使用详解

武新华　陈艳艳　杨　平　等编著

電子工業出版社
Publishing House of Electronics Industry
北京·BEIJING

内 容 简 介

本书由浅入深、图文并茂地再现了网络入侵与防御的全过程，内容涵盖：黑客必备小工具、扫描与嗅探工具、QQ 聊天工具、注入工具、远程控制工具、木马和间谍常用工具、网游与网吧攻防工具、密码攻防工具、网络代理与追踪工具、局域网黑客工具、黑客入侵行为检测、清理入侵痕迹工具、巧用防护软件保护系统安全等一些应用技巧，并通过一些综合应用案例，向读者讲解了黑客与反黑客工具多种应用的全面技术。

本书内容丰富全面，图文并茂，深入浅出，面向广大网络爱好者，同时可作为一本速查手册，也适用于网络安全从业人员及网络管理者。

图书在版编目（CIP）数据

黑客与反黑工具使用详解/武新华等编著. —北京：电子工业出版社，2011.1
（反黑风暴）
ISBN 978-7-121-12577-5

Ⅰ. ①黑… Ⅱ. ①武… Ⅲ. ①计算机网络－安全技术 Ⅳ. ①TP393.08

中国版本图书馆 CIP 数据核字(2010)第 247366 号

策划编辑：郭鹏飞
责任编辑：鄂卫华
印　　刷：中国电影出版社印刷厂
装　　订：中国电影出版社印刷厂
出版发行：电子工业出版社
　　北京市海淀区万寿路 173 信箱　邮编 100036
开　　本：787×1092　1/16　印张：26　字数：666 千字
印　　次：2011 年 1 月第 1 次印刷
定　　价：56.00 元（含光盘 1 张）

凡所购买电子工业出版社图书有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系，联系及邮购电话：（010）88254888。

质量投诉请发邮件至 zlts@phei.com.cn，盗版侵权举报请发邮件至 dbqq@phei.com.cn。

服务热线：（010）88258888。

前 言 FREFACE

当结束了白日喧嚣，繁华的都市像个玩累了的孩子慢慢安静了下来，在静寂得令人窒息的黑夜里，某个都市的角落，微弱的光亮笼罩着一个不大的房间，黑暗中，显示屏不时闪耀出深蓝色的光芒。一个人，一台笔记本，一杯热了又凉、凉了又热的咖啡，一根还没有抽完的烟，还有那台不知处于何处的服务器，依旧继续着……

在大家眼中，“黑客”一词具有一定的神秘性，其定义范围包括了反社会的计算机天才到恶意病毒的编写者。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，使用简单的工具，对一些疏于防范的电脑作出攻击，并在受侵入的电脑里为所欲为。当发现自己的密码被盗、资料被修改删除、硬盘变作一团空白之时，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分的程序员，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保护个人隐私的人。欲话说：害人之心不可有，防人这心不可无。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，了解除基础的网络知识、通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”两个不同的角度，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。本书内容涵盖了黑客必备小工具、扫描与嗅探工具、QQ 聊天工具、注入工具、远程控制工具、木马和间谍常用工具、网游与网吧攻防工具、密码攻防工具、网络代理与追踪工具、局域网黑客工具、黑客入侵行为检测、清理入侵痕迹工具、巧用防护软件保护系统安全等，由浅入深地讲述了黑客攻击的原理、常用手段，让读者在了解的同时学习到如何拒敌于千里的方法。

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介绍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+视频=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
- 书盘结合，互动教学，在学习案例过程中掌握知识点和技能

本书以实例分析加案例剖解为主要脉络，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，力求通过一个知识点的讲解，实现读者用更少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

本书紧紧围绕“攻”、“防”两个不同的角度，讲解了黑客与反黑工具使用方法，作为一本面向广大网络爱好者的速查手册，适合于如下读者学习使用：

- 没有多少电脑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
- 明确学习目的的读者、喜欢钻研黑客技术但编程基础薄弱的读者
- 网络管理员、广大网友等

本书作者：

本书作者团队长期从事网络安全管理工作，都具有较强的实践操作能力及一线拼杀经验，可带领广大醉心技术者穿越迷雾，把黑客们的伎俩看清楚。本书的编写情况是：杨平负责第 1 章，王英英负责第 2 章，陈艳艳负责第 3、4、5 章，安向东负责第 6 章，李伟负责第 7 章，郑静负责第 8 章，王肖苗负责第 9 章，吕志华负责第 10 章，张晓新负责第 11 章，孙世宁负责第 12 章，齐伟负责第 13 章，最后由武新华统审全稿。最后，需要提醒大家的是：根据国家有关法律规定，任何利用黑客技术攻击他人的行为都属于违法行为，希望读者在阅读本书后最好不要使用本书中介绍的黑客技术对别人进行攻击，否则后果自负，切记切记！

我们的联系方式：zhangbg@phei.com.cn

编著者

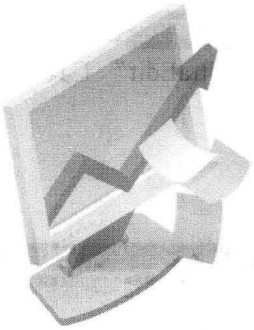
2010 年 10 月

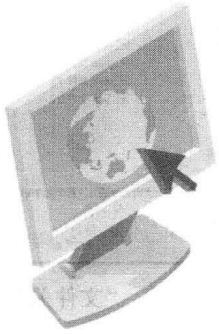
目 录 FREFACE

第1章 黑客必备小工具

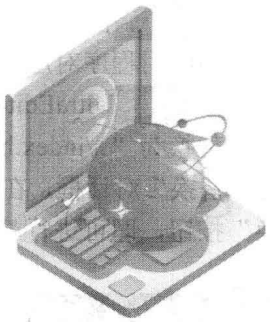
重点提示：

- 文本编辑工具
- 免杀辅助工具
- 破解辅助工具
- 其他工具





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、破解辅助工具以及其他一些工具，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。



在黑客试图攻击他人计算机并进行一系列破坏性操作时，如果要实现攻击目的，往往会借助各种各样的工具，如文本编辑工具、免杀辅助工具、破解辅助工具等。

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 和 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。

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、十六进制数、ASCII 码等，甚至可取代记事本，该编辑器中内建英文单字检查、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“文件关联”对话框，在其中可以看到 UltraEdit 支持多种文件格式，例如*.txt、*.doc、*.Bat、*.ini、（C 语言源程序）*.c 和*.cpp、头文件*.h 和*.hpp、HTML 语言*.html 和*.htm、Java 语言*.java 和*.jav 等，这些文件类型基本覆盖了所有的常见文件类型，如图 1-1 所示。

步骤 02 在其中勾选相应的复选框，单击“确定”按钮，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代码，如图 1-2 所示。

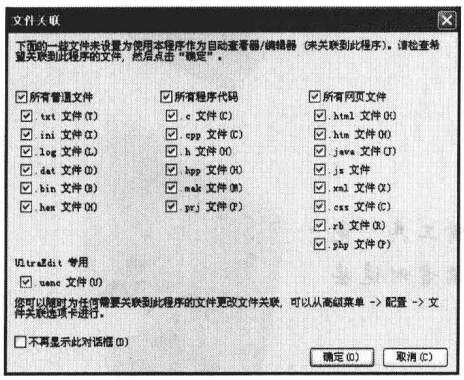


图 1-1 “文件关联”对话框

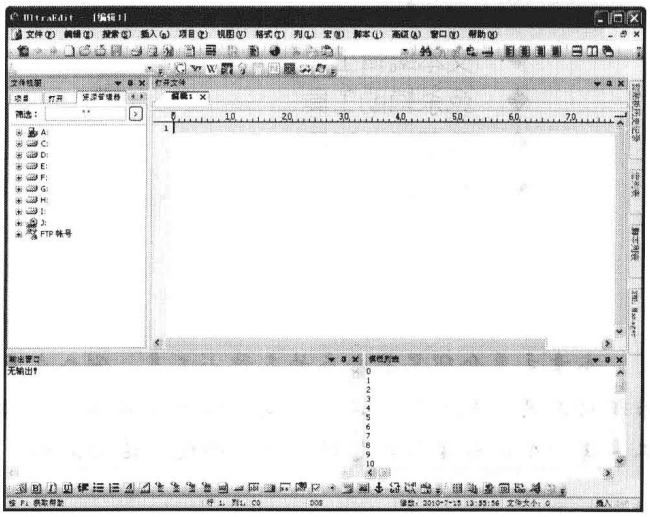


图 1-2 “UltraEdit”主窗口

步骤 03 选择“文件”→“打开”菜单项，即可打开“打开”对话框，如图 1-3 所示。

步骤 04 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 1-4 所示。

步骤 05 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 1-5 所示。单击“全部替换”按钮，即可进行替换操作。

图 1-3 “打开”对话框

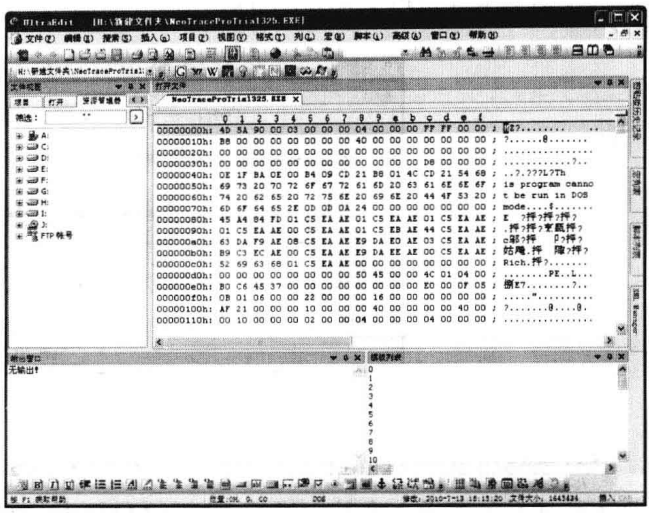


图 1-4 查看应用程序对应的十六进制编码

步骤 06 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 1-6 所示。

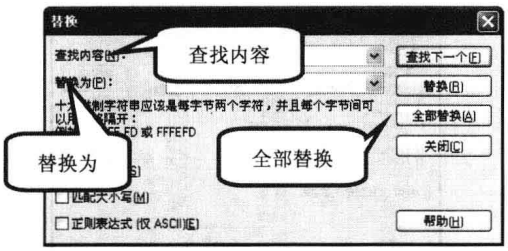


图 1-5 “替换”对话框

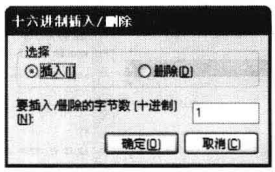


图 1-6 “十六进制插入/删除”对话框

步骤 07 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，如图 1-7 所示。单击“确定”按钮，即可添加指定的字符串。

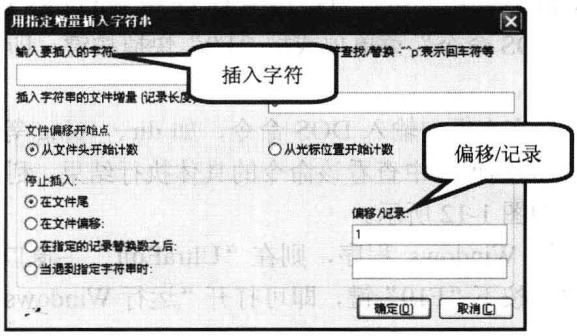


图 1-7 “用指定增量插入字符串”对话框

步骤 08 还可以让 UltraEdit 软件自己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 1-8 所示。

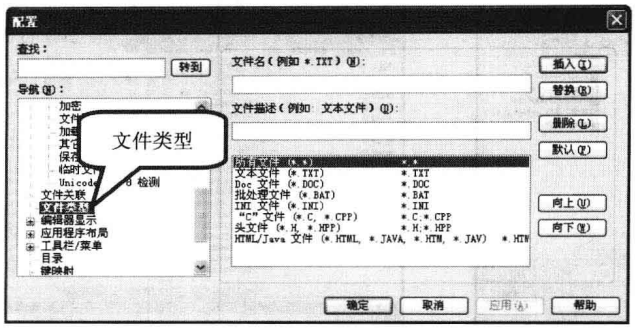


图 1-8 “配置”对话框

步骤 09 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 1-9 所示。

步骤 10 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 1-10 所示。

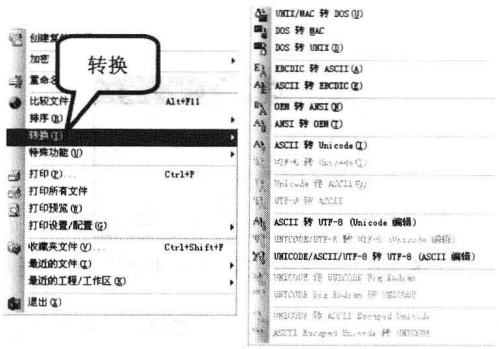


图 1-9 “转换”菜单

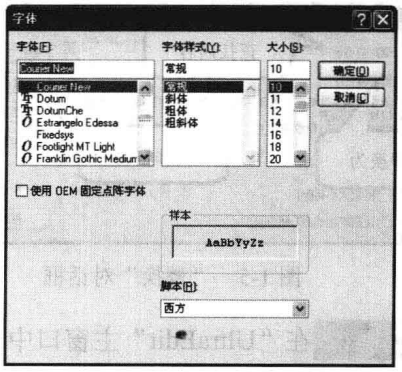


图 1-10 “字体”对话框

步骤 11 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”快捷按键，即可打开“DOS 命令”对话框，如图 1-11 所示。

步骤 12 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”主窗口的编辑区中查看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 1-12 所示。

步骤 13 如果想运行 Windows 程序，则在“UltraEdit”主窗口中选择“高级”→“运行 Windows 程序”菜单项或按下“F10”键，即可打开“运行 Windows 程序”对话框，如图 1-13 所示。

步骤 14 在“命令”文本框中输入调用 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 1-14 所示。

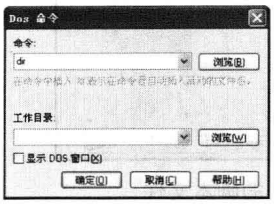


图 1-11 “Dos 命令”对话框

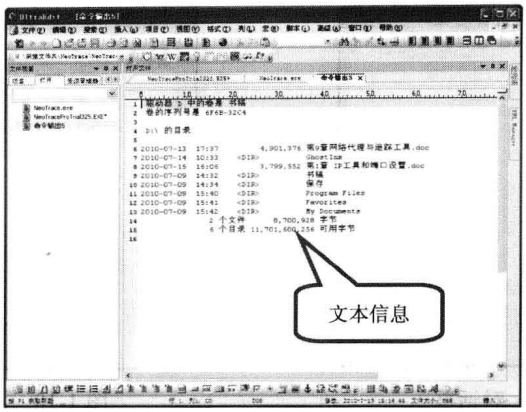


图 1-12 Dos 命令的执行结果

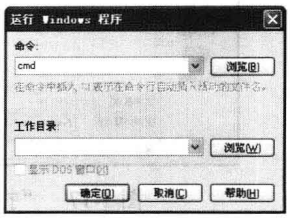


图 1-13 “运行 Windows 程序”对话框

步骤 15 在 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 1-15 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。

步骤 16 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，在其中进行添加、编辑、删除脚本操作，如图 1-16 所示。

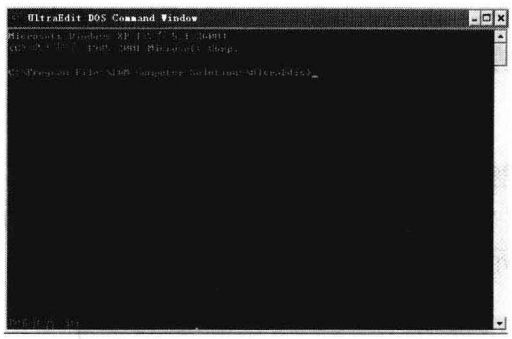


图 1-14 “命令提示符”窗口

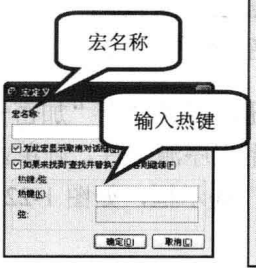


图 1-15 “宏定义”对话框

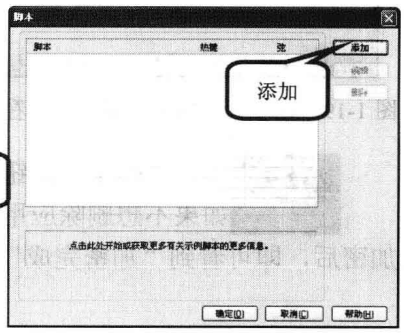


图 1-16 “脚本”对话框

步骤 17 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 1-17 所示。

步骤 18 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 1-18 所示。

步骤 19 单击“确定”按钮，返回到“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 1-19 所示。

步骤 20 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 1-20 所示。

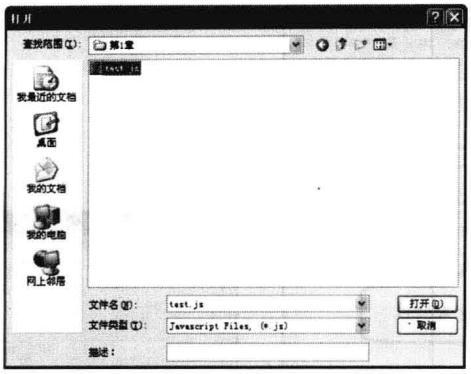


图 1-17 “打开”对话框

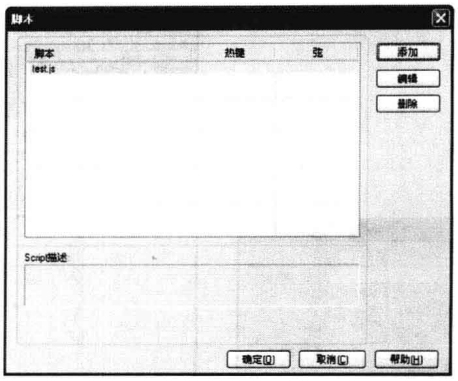


图 1-18 添加的脚本文件

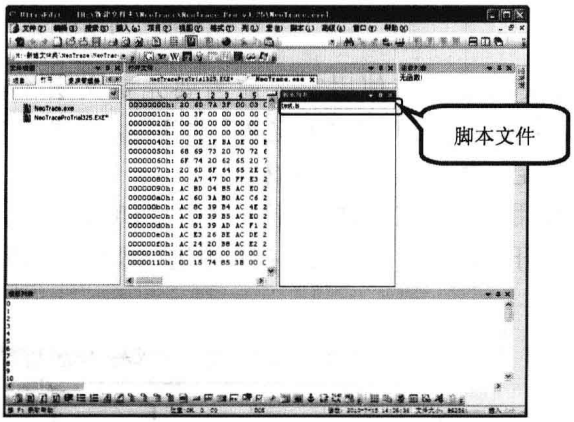


图 1-19 在“脚本列表”窗口中查看添加的脚本文件

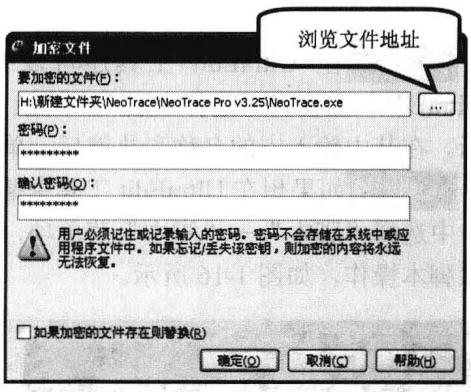


图 1-20 “加密文件”对话框

步骤 21 单击“确定”按钮，即可打开“加密-删除文件”对话框，如图 1-21 所示。

步骤 22 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。待成功加密后，即可看到“加密完成”提示框，如图 1-22 所示。

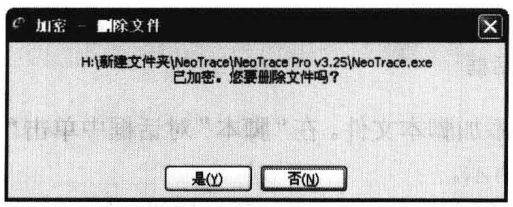


图 1-21 “加密-删除文件”对话框

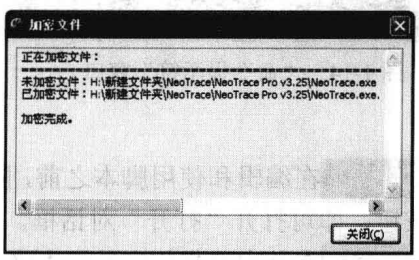


图 1-22 “加密完成”提示框

步骤 23 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 1-23 所示。

步骤 24 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。待成功解密后，即可看到“解密完成”提示框，如图 1-24 所示。