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。

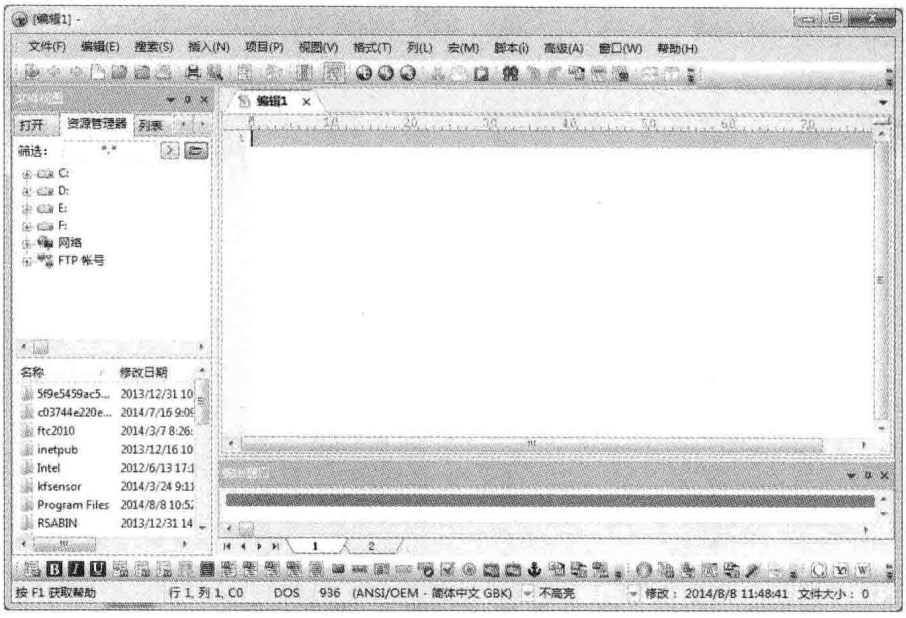

图 1-1 UltraEdit 主窗口

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。

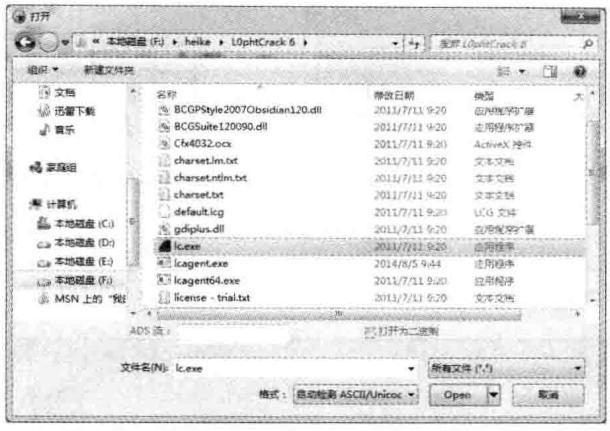

图 1-2 “打开”对话框

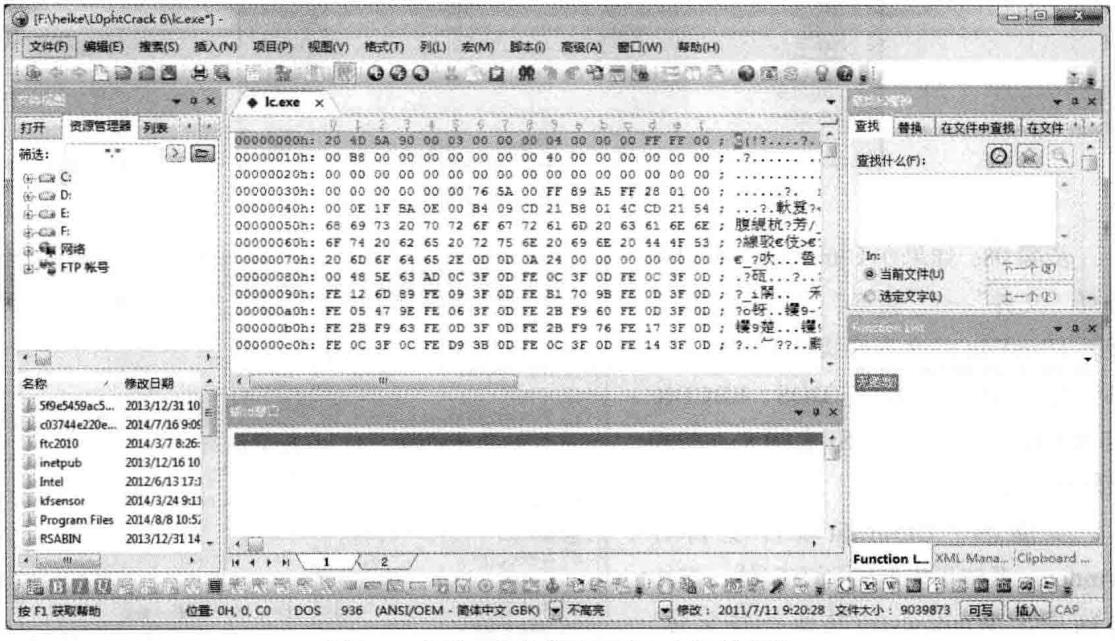

图 1-3 查看应用程序对应的十六进制编码

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

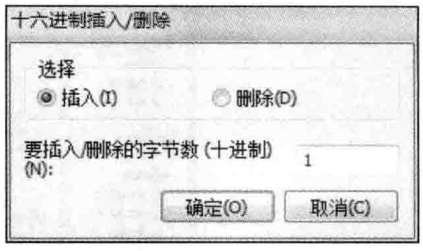

图 1-5 “十六进制插入 / 删除”对话框

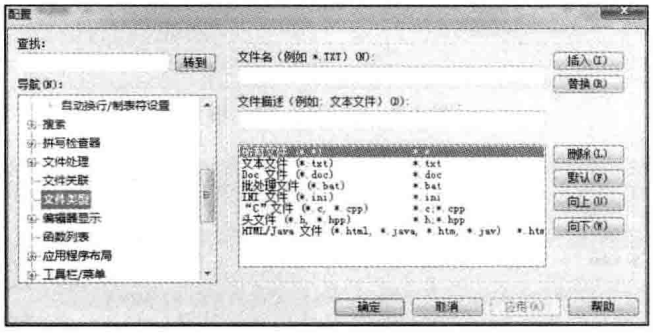

图 1-6 “配置”对话框

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。

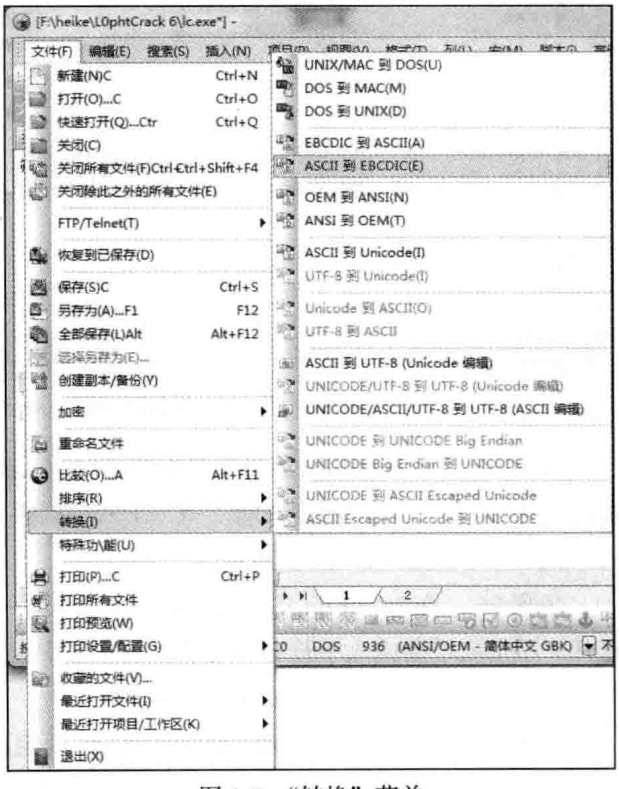

图 1-7 “转换”菜单

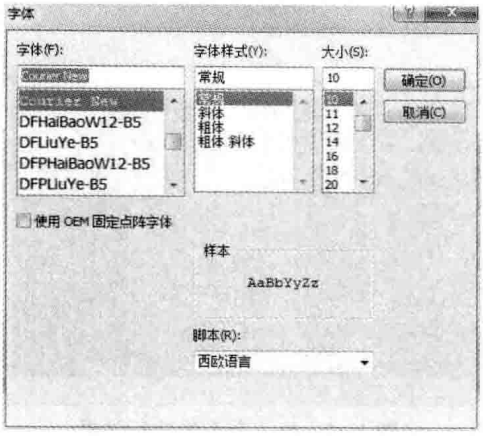

图 1-8 “字体”对话框

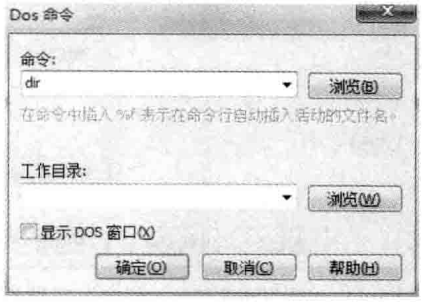

图 1-9 “Dos 命令”对话框

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。

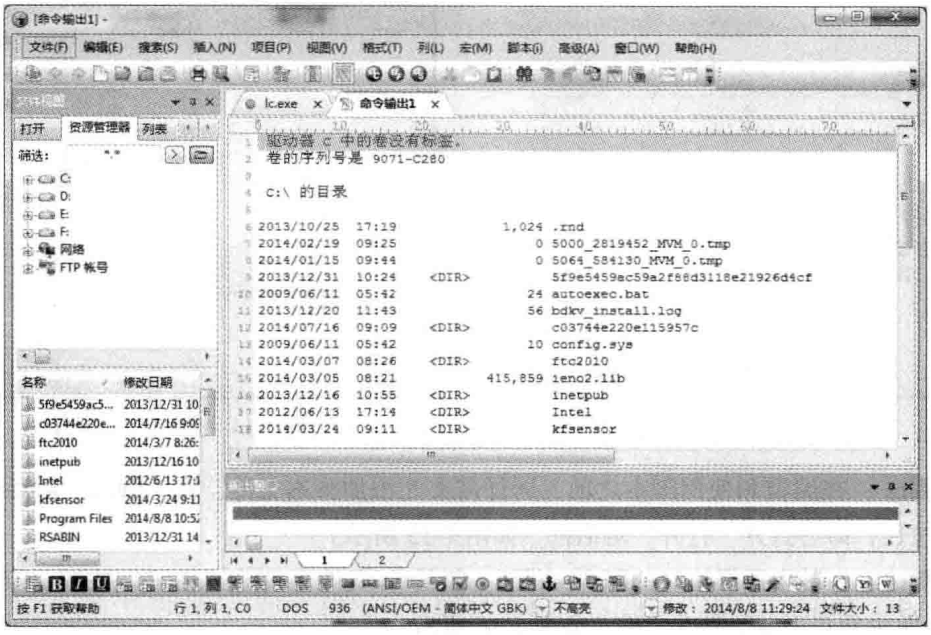

图 1-10 Dos 命令的执行结果

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