信息安全必读系列

师鸣若 袁 磊 韩 晟 等编著

网络攻防

工具

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

信息安全必读系列——

网络攻防工具

师鸣若　袁　磊　韩　晟　等编著

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

内 容 简 介

本书以“实用”为原则，通过大量的实例介绍了目前最常用的黑客攻击防御实用工具软件，包括黑客攻击必备工具、黑客入侵攻击、计算机安全防范等 3 个部分的软件。全书共分 11 章，以“常用工具”为出发点，介绍了 IP 代理工具、信息搜集工具、扫描检测工具、脚本注入工具、拒绝服务工具、远程监控及木马后门、嗅探监听工具、加密破解工具、网吧黑客工具、安全防范工具、计算机网络维护和恢复工具等方面的内容。

本书适合广大对网络攻防和信息安全感兴趣的新手学习使用，也适合从事网络管理和维护的人员、网络应用开发者和有关方面研究工作的广大工程技术人员参考。

图书在版编目（CIP）数据

网络攻防工具 / 师鸣若等编著.—北京：电子工业出版社，2009.9
(信息安全必读系列)
ISBN 978-7-121-09255-8

Ⅰ. 网… Ⅱ.师… Ⅲ.计算机网络－安全技术 Ⅳ.TP393.08

中国版本图书馆 CIP 数据核字（2009）第 116918 号

策划编辑：祁玉芹
责任编辑：段春荣
印　　刷：北京市天竺颖华印刷厂
装　　订：三河市鑫金马印装有限公司
出版发行：电子工业出版社
　　北京市海淀区万寿路 173 信箱　邮编 100036
开　　本：787×1092　1/16　印张：22.5　字数：576 千字
印　　次：2009 年 9 月第 1 次印刷
定　　价：42.00 元

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

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

服务热线：（010）88258888。

前言

我们所处的时代是信息技术高速发展的时代，人们的生活越来越多地依赖于信息技术。信息技术一方面提高了人们的生活品质，另一方面也给人们带来了烦恼，其中一个最大的问题就是如何在信息社会中保护自己的隐私、防范自己的利益不被黑客侵犯，这是摆在当前这个时代的所有人面前的一个挑战问题。黑客和反黑客将是信息社会经久不衰的话题。

知己知彼，百战不殆。本书从介绍最常用的黑客工具出发，针对这些工具的原理，介绍相应的防范措施和工具的使用，读者也可以从对黑客工具的了解中自行设定相应的防范方法。

第一部分介绍黑客攻击必备工具，包括 IP 隐藏工具、代理转换工具、跳板肉鸡常用工具，和 IP 地址、MAC 地址、DNS、操作系统等信息搜集工具。

第二部分介绍黑客入侵攻击工具，包括扫描检测工具、脚本注入工具、拒绝服务工具、远程监控及木马后门、嗅探监听工具、加密/破解工具、网吧黑客工具。

第三部分介绍计算机安全防范工具，包括各种常见杀毒软件、防火墙等工具的使用、病毒、木马的清除技巧、系统的备份与恢复等。

在众多介绍黑客工具的图书中，本书的特点是突出“实用”，由编著者根据实践经验选取当下实用的工具进行介绍，并通过大量的实例介绍了目前最常用的黑客攻击防御实用工具软件，了解黑客的攻击手法及其如何来进行相应的防范而制定反黑技术；了解各种方法的同时掌握相应的对策，以保障自己系统、信息安全，完善自己的网络环境；学习 Web 脚本漏洞攻击和防御技巧，学会加固主机系统，抵御各种攻击；透彻领会和熟练掌握网络安全与防火墙、操作系统安全、安全审核、攻击和威胁分析等方面的理论和技能。可以帮助系统管理员、安全人员和网络管理员，以及其他从事网络安全的工作人员学习攻击者如何工作的，以及防御自己的系统免受攻击所用技术，以加固他们的系统，抵御各种攻击。紧紧围绕黑客的攻与防展开学习内容，在详细描述黑客攻击手段的同时，介绍了相应的防范方法，使学员对攻防技术形成系统的了解，能够更好地防范黑客的攻击。

本书适用于广大对网络攻防和信息安全感兴趣的新手学习使用，也适合从事网络管理和维护的人员、网络应用开发者和有关方面研究工作的广大工程技术人员参考。

本书得到以下项目资助：

人才强教：“北京市属高等学校人才强教计划资助项目（项目编号：PHR200906210）”

科研基地：“北京市教育委员会科研基地建设项目”

科研课题：“北京市教育委员会科技计划项目（KM200810037001）”。

本书由师鸣若、袁磊、韩晟等编著，此外参与本书编写的还有何征艰、王运松、韩凌云、姜文录、扈彩艳、徐津、王大印、阎芳、赵明茹、张凤全、李荣花、艾思杰等。本书在编著过程中，得到了很多老师的帮助，在此一并表示感谢。由于信息技术发展迅速，作者水平有限，加之时间仓促，书中难免有错漏之处，恳请读者批评指正。

我们的 E-mail 地址：qiyuqin@phei.com.cn

编　者

2009 年 5 月

目录

CONTENTS

第 1 章　常用 IP 保护伞工具 1

1.1　概述 1
1.2　获取免费代理服务器工具 3
1.2.1　常用代理查询工具——代理猎手 3
1.2.2　专业代理搜索工具——代理服务器搜索者 8
1.2.3　下载量最大的国产代理服务器工具——代理公布器 10
1.3　IP 隐藏工具 12
1.3.1　全功能的 IP 代理工具——代理超人 12
1.3.2　智能化绿色代理工具——代理之狐 14
1.3.3　体贴入微的高智能代理工具——花刺代理 14
1.3.4　烈火代理——Proxyfire 15
1.3.5　在网络邻居上隐藏自己的计算机——net config server 18
1.4　代理转换工具 19
1.4.1　国内著名代理转换工具——WaysOnline 20
1.4.2　Socks2HTTP 23
1.5　跳板肉鸡工具 23
1.5.1　SkSockserver 24
1.5.2　使用跳板——远程桌面连接工具 29
1.6　小结 34

第 2 章　信息搜集工具 35

2.1　IP 信息搜集工具 35
2.1.1　查找网站 IP 地址 35
2.1.2　确认网站服务器所在的地区及 IP 35
2.1.3　找出非固定 IP 上网用户的当前 IP——Netstat 35
2.1.4　找出邮件发件人的 IP——Foxmail 35
2.2　测试物理网络工具——Ping 36
2.2.1　Ping 命令介绍 36
2.2.2　用 Windows 自带工具探测主机操作系统类型 36
2.3　查看 IP、MAC、DNS 工具 37
2.3.1　查看 Windows 系统信息——Winipcfg/Ipconfig 37
2.3.2　查看远程服务器 DNS——NsLookup 38

2.3.3 辅助工具——无处藏身（Seekyou） 49
2.4 探测多种信息的工具 51
2.4.1 显示详细网络信息的工具——Nbtstat 51
2.4.2 详细显示端口及网络资料——Netstat 53
2.4.3 查看系统进程信息—Tasklist 54
2.4.4 Windiows 2000 刺探工具——Snmputil 56
2.4.5 查看到达目标主机所经过的网络数和路由器数——TraceRoute 57
2.5 功能超强的 Net 命令 60
2.5.1 查看共享资源列表——Net View 60
2.5.2 查看系统/网络服务——Net Start 60
2.5.3 启动/停止系统/网络服务命令——Net Start/Stop 61
2.5.4 查看用户账号信息——Net User 61
2.5.5 网络映射命令——Net Use 62
2.5.6 查看/添加/更改计算机本地组——Net Localgroup 65
2.5.7 发送消息命令——Net Send 65
2.5.8 管理主机共享资源命令——Net Share 67
2.6 综合信息搜索工具 68
2.6.1 WhereIsIP 68
2.6.2 Visual IP Trace 70
2.6.3 集成 TCP/IP 实用工具为一体的 IP-Tools 74
2.6.4 Whois 查询工具——Free Whois Anywhere 76
2.6.5 图形监测工具——MultiPing 77
2.7 小结 80

第 3 章 扫描检测工具 81

3.1 常用入侵命令 81
3.1.1 传输协议 FTP 上传下载 81
3.1.2 传输协议 TFTP 上传下载 82
3.1.3 计划任务的添加、查看和启动服务 83
3.1.4 用 At 命令添加计划任务 86
3.1.5 复制命令——Copy 89
3.1.6 利用 Echo 工具黑掉主页 90
3.1.7 替换文件命令——Replace 命令 94
3.1.8 更改文件扩展名的关联——ASSOC 命令 94
3.1.9 远程注册表命令——Reg 95
3.1.10 注销/关闭/重启远程计算机——Shutdown 命令 101
3.2 字典工具 103
3.2.1 易优超级字典生成器 103
3.2.2 黑客字典 104
3.2.3 生日密码生成器 104
3.3 扫描检测工具 104
3.3.1 最简单的踩点工具——X-Scan 104

3.3.2 多线程扫描工具——X-Way26 106
3.3.3 俄罗斯安全界专业扫描软件——SSS 106
3.3.4 SQL 注入漏洞扫描器 107
3.3.5 多线程 IP、SNMP 扫描器商用扫描程序——eEye 扫描器 108
3.3.6 批量检测工具——MAC 扫描器 108
3.3.7 挖掘鸡 109
3.3.8 其他扫描器 109
3.4 小结 110

第 4 章 脚本注入工具 111

4.1 PHP 注入工具 111
4.1.1 超强的 PHP 注入工具——Casiv4.0 111
4.1.2 PHP 注入 KEvinSI 114
4.2 Access 注入工具 117
4.3 SQL 注入工具 117
4.3.1 强大的 SQL 检测注入工具——BSQLBF 117
4.3.2 超酷注入工具——阿 D-SQL 120
4.3.3 SQL 注入中文转换器 122
4.3.4 MSSQL2005 注射器 122
4.3.5 SQLMAP 124
4.4 综合注入工具 126
4.4.1 传说中的 NBSI 126
4.4.2 Domain 明小子注入工具 130
4.4.3 教主的 HDSI 136
4.4.4 批量入侵网站猎手 142
4.4.5 小榕工具 Wis 和 Wed 144
4.4.6 小幽的狂注幽灵 145
4.4.7 科汛 0day 注入工具 147
4.4.8 Oracle 专用注入器 147
4.5 小结 148

第 5 章 拒绝服务攻击工具 149

5.1 多网段 DDOS 攻击利器——DDoSPing 149
5.2 老牌洪水攻击 UDP Flooder 151
5.3 傀儡僵尸 DDOS 攻击集合 152
5.4 Land 攻击器 152
5.5 XFlood 攻击器 153
5.6 小结 154

第 6 章　远程监控及木马后门 155

6.1　灰鸽子 155
6.2　上兴远程控制 160
6.3　Radmin 162
6.4　黑洞 163
6.5　PcShare 165
6.6　VNC 168
6.7　任我行 171
6.8　网络神偷 177
6.9　WinShell 178
6.10　小结 178

第 7 章　嗅探监听工具 179

7.1　WinPcap 179
7.2　局域网嗅探专家 Sniffer Pro 180
7.3　影音嗅探专家 187
7.4　FileMon 187
7.5　小结 188

第 8 章　加密/破解工具 189

8.1　加密基本知识 189
8.1.1　基本算法 189
8.1.2　Windows 口令保护 189
8.2　文件加密工具 191
8.2.1　Windows 自带加密文件系统 EFS 191
8.2.2　Word 自带的加密功能 193
8.2.3　Word 文档加密器 195
8.2.4　PDF 文件加密器 197
8.3　文件夹加密工具 201
8.3.1　文件夹加密超级大师 201
8.3.2　CryptoExpert 204
8.3.3　文件加密箱 211
8.4　其他加密工具 214
8.4.1　WINRAR 合并压缩加密 214
8.4.2　网页加密——“雅典娜”网页密码锁 216
8.4.3　U 盘加密——U 盘超级加密 221
8.5　系统解密工具 224
8.5.1　L0phtcrack 224

8.5.2 SAMInside 231
8.5.3 Password Recovery 239
8.6 小结 242

第 9 章 网吧黑客工具 243

9.1 解除网吧硬盘限制工具 243
9.1.1 破解硬盘限制方法 243
9.1.2 破解硬盘限制工具 246
9.1.3 修改硬盘盘符 246
9.2 网吧免费上网工具 247
9.2.1 多功能数据库浏览器 248
9.2.2 利用收银台计算机漏洞入侵工具 248
9.2.3 Pubwin EP 冲值工具 251
9.3 网吧电脑限制解除工具 251
9.3.1 批处理命令工具 251
9.3.2 重设回收站属性 263
9.3.3 显示“开始”菜单项 264
9.3.4 系统配置 264
9.3.5 解锁注册表限制 266
9.3.6 去除鼠标右键限制 267
9.3.7 解锁显示控制面板 268
9.3.8 突破 IE 分析审查 269
9.3.9 突破 IE“另存为”限制 270
9.3.10 突破“源文件”禁用限制 271
9.3.11 用 Internet 选项工具突破下载 272
9.3.12 用利用网页源码突破下载 273
9.4 网吧攻击破解工具 273
9.4.1 破解网吧 Pubwin 管理程序工具 273
9.4.2 破解冰点还原工具 274
9.4.3 网吧突袭击者 Bulider2006 279
9.4.4 精锐网吧辅助工具 280
9.5 局域网查看工具 281
9.5.1 局域网终结者 X++ 281
9.5.2 超级网络邻居 281
9.5.3 局域网超级工具（NetSuper） 282
9.5.4 局域网中的嗅探及工具 284
9.5.5 网络执法官 288
9.6 小结 289

第 10 章 安全防范工具 291

10.1 杀毒软件 291

10.1.1 卡巴斯基反病毒软件 291
10.1.2 BitDefender 296
10.1.3 北信源 VRV 301
10.1.4 瑞星杀毒 303
10.1.5 大蜘蛛杀毒软件 305
10.2 防火墙 307
10.2.1 IE 防火墙 307
10.2.2 冰盾 DDOS 防火墙 308
10.2.3 龙盾 IIS 防火墙 308
10.2.4 天网防火墙 313
10.2.5 BlackICE PC Protection 315
10.3 其他安全工具 316
10.3.1 奇虎 360 安全卫士 316
10.3.2 Local Administrator Checker 318
10.3.3 IceSword 冰刃 319
10.3.4 Autoruns 321
10.3.5 APORTS 321
10.3.6 Process Explorer 322
10.3.7 Trojan Remover 323
10.3.8 Loaris Trojan Remover 324
10.3.9 Microsoft Baseline Security Analyzer（MBSA） 325
10.3.10 KillBox 327
10.3.11 TCPVIEW 327
10.4 小结 328

第 11 章 计算机系统维护和数据恢复工具 329

11.1 备份和恢复 329
11.1.1 用 Ghost 备份和恢复系统 329
11.1.2 Windows 系统的备份工具 333
11.1.3 Windows 系统还原 335
11.1.4 蚂蚁驱动备份专家 338
11.1.5 Windows 注册表的备份与恢复 339
11.1.6 专业级的 Windows 注册表优化和管理软件——Registry Help Pro 340
11.2 数据恢复工具 342
11.2.1 EasyRecovery 342
11.2.2 FinalData 344
11.2.3 R-Studio 345
11.2.4 CD DVD Data Recovery 347
11.2.5 RecoverMyFiles 348
11.3 小结 350

第 1 章　常用 IP 保护伞工具

本章重点：

- 代理服务器基础。
- 代理服务器搜索、验证工具及其使用方法。
- 隐藏 IP 的工具及其使用方法。
- 代理转换工具及其使用方法。
- 跳板肉鸡的常用工具及其使用方法。

代理服务器是黑客攻防工具中最基础的一类，本章就代理服务器的基础知识和一些常用工具的使用方法进行了重点介绍。

1.1　概　　述

1. 代理服务器的定义

代理服务器（proxy server）是客户端和应用服务器建立的连接之间起媒介作用的服务器，可以是一台计算机，也可以是一个应用程序。客户端连接到一个代理服务器，提出访问其他服务器上资源或服务（比如文件，网页，连接等）的请求，代理服务器根据自己设定的过滤规则检验客户端的请求，如果请求符合过滤规则，代理服务器就连接被请求的服务器，转发客户端的服务请求，并把服务器的响应转发给客户端。

代理服务器可以放置在客户端上，或者在客户端和被请求的服务器，以及 Internet 之间的任何位置，如图 1-1 所示。

图 1-1　代理服务器

2. 代理服务器的分类

（1）　透明代理和非透明代理

按照IETF组织的RFC 2616文档给出的定义，代理服务器分成透明代理和非透明代理两种。

透明代理服务器不对请求和响应做非必要的修改，修改仅限于代理服务器身份认证和识别的需要。该代理服务器通常称为网关（gateway）或隧道代理（tunneling proxy）。客户端无需做任何设置，即客户端在不知情的情况下，发出的服务请求就被透明代理服务器直接转发

到被请求的服务器。

非透明代理服务器可能修改客户端发出的请求，或者服务器的响应，以提供额外的服务，比如媒体类型转换等。代理服务器有时甚至不连接被请求的服务器而代为做出响应，这时一般是因为代理服务器已经对相应服务响应做了缓存。该代理服务器通常叫做逆向代理（reverse proxy）。逆向代理通常放置在一组应用服务器附近，所有来自网络的对这些应用服务器的请求都要先经过该逆向代理服务器，以提供 SSL 加密代理、负载平衡、内容缓存等服务，还能为网页服务器提供一定的安全保护。

（2） SOCKS 代理和 HTTP 代理

HTTP 代理是最常见的一种代理服务器类型，仅分析收到请求的 HTTP 头，因此只能代理转发 HTTP 数据流。其他还有 FTP 代理、HTTPS 代理等，只能代理转发特定协议的数据。

SOCKS 代理则使用一种握手协议将客户端和代理服务器连接起来，可用于任何 TCP 或 UDP 连接，也就是 SOCKS 代理也可用来转发 HTTP、FTP、HTTPS 等数据流等。SOCKS5 代理服务器在将客户端的通信请求发送给真正服务器的过程中，对于请求数据包本身不加任何改变。SOCKS5 代理服务器接收到真正服务器的响应后，也原样转发给客户端。

从协议的角度来说，SOCKS 是一种协助客户端/服务器类型的网络数据包通过代理服务器转发的网络协议，位于 OSI 模型的第五层——会话层（Session Layer）。SOCKS 最初是由 MIPS Computer Systems 的系统管理员 David Koblas 开发的，Koblas 在 1992 年的 Usenix Security Symposium 会议上发布了 SOCKS。SOCKS 有两个版本 SOCKS4 和 SOCKS5，它们的主要区别是：

- SOCKS4 不支持用户身份认证，而 SOCKS5 支持多种身份认证机制。
- SOCKS4 不支持对 UDP 协议的代理，而 SOCKS5 支持。
- SOCKS4 需要客户支持 DNS，而 SOCKS5 的客户端可以依靠 SOCKS5 代理服务器查询 DNS。

3. 代理服务器的用途

代理服务器有下列用途：

- 保护客户端的地址不泄露，使它在应用服务器看来是匿名的。
- 内容过滤，使客户只能获取指定类型的资源或服务。
- 加速访问速度，通常用于缓存网页，视频等信息。
- 监听客户端和外部网络的数据流。
- 代理服务器还可用来绕过一些限制性的代理服务器，使得用户获得比较高的访问权限。比如 elgooG 就曾经是一些地区的用户访问 Google 的代理服务器。

4. 使用代理服务器的风险

恶意的代理服务器可能获得登录名、口令等私密信息。中间经过多个代理服务器时，虽然被请求服务器不能获得请求客户的信息，但是客户有更多的痕迹留在中间的每个代理服务器上，可能被这些代理服务器利用来追踪客户的活动，而客户却错误地以为自己的隐私得到了很好的保护。因此，正确的方法是只使用有一定信用度的代理服务器，比如代理服务器的管理者是可信的，有清晰的隐私策略。如果没有选择或难以区分，在使用代理服务的时候不要通过代理服务器发送任何未经加密的隐私信息。

5. 代理服务器的使用设置

很多应用程序的客户端都可以设置使用代理，下面以最常用的浏览器（Internet Explorer 6.0 及以上）为例介绍如何设置使用代理服务器。

- 单击 Internet Explorer “工具” → “Internet 选项” → “连接”。
- 如果使用的是拨号上网，单击“设置”进入“宽带连接设置”；如果使用的是局域网上网方式，单击“局域网（LAN）设置”中的“局域网设置”。
- 勾选上“使用代理服务器”，在“地址”和“端口”框内，分别填入代理服务器地址和端口号。如果需要，勾选上“跳过本地地址的代理服务器”。
- 如果网络对不同的服务（如 HTTP、HTTPS、FTP 或 SOCKS）需要单独的代理地址，可单击“高级”按钮，然后键入要使用的单独代理服务器地址和端口。
- 单击 “确定”，直到返回 Internet Explorer。

1.2 获取免费代理服务器工具

1.2.1 常用代理查询工具——代理猎手

代理猎手（Proxy hunter）是太阳风工作室开发的一款国产自由软件，可快速搜索网络上的免费代理，验证网络上公布的代理服务器，官方地址是 http://www.proxyhunter.net。下面以 v3.1 beta 1 为例讲解该软件的使用方法。

1. 软件设置

在如图 1-2 所示中的初始界面中依次单击系统→参数设置，可得到如图 1-3 所示的参数设置面板，在搜索验证设置中的搜索方法，选定启用先 ping 后连的机制，其他参数可按照默认设置不变或者按自己网络的实际情况填写。

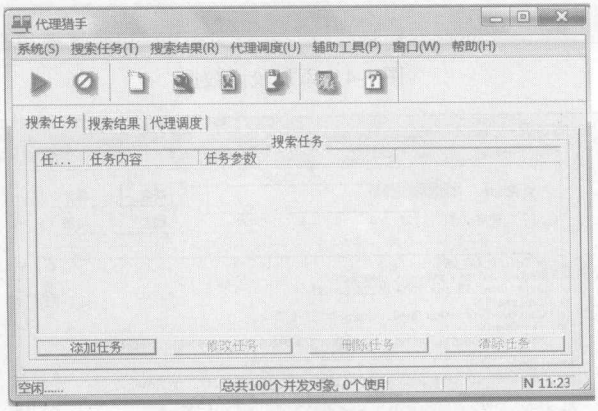

图 1-2 代理猎手界面

我们还需要设置验证参数，用于检验搜索到的代理是否可用。该软件已经设置一些默认的验证数据，我们可以选择添加自己喜欢的验证数据，比如谷歌网址（如图 1-4 所示）。

手工输入验证名，验证地址后，单击“获取”按钮，弹出“获取网络资源”的面板，单击该面板上的“获取”，得到一些数据，如图 1-5 所示。

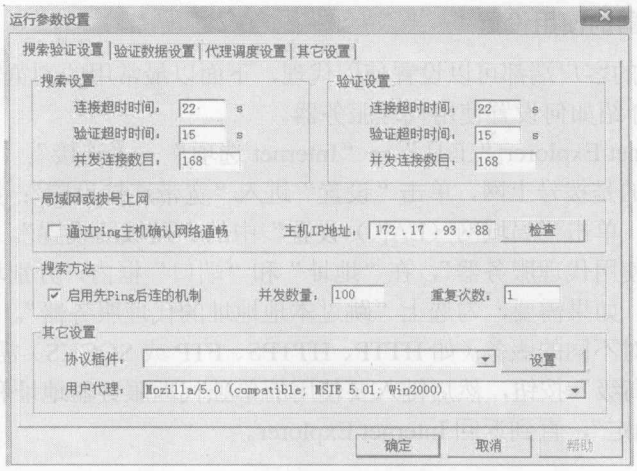

图 1-3　运行参数设置

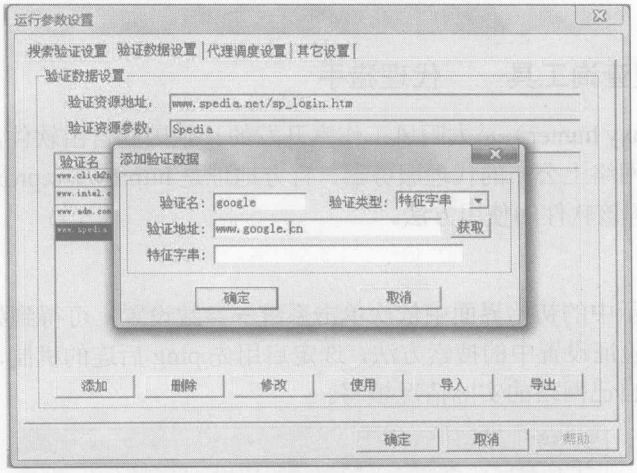

图 1-4　添加验证数据

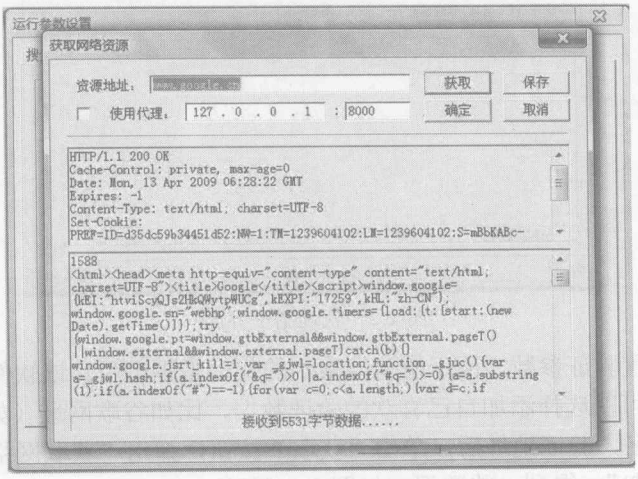

图 1-5　获取网络资源

在图 1-5 中下侧的对话框中选中处于<title>和</title>之间的内容，这里是“Google”，单击鼠标右键选择复制，并单击该面板中的“确定”按钮，得到“特征字串”，如图 1-6 所示。

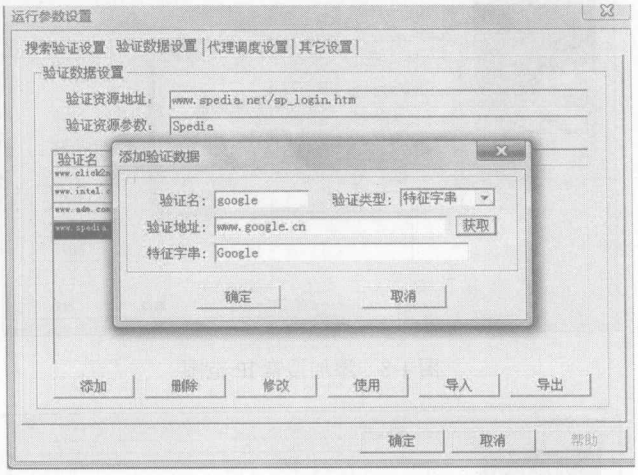

图 1-6　添加验证数据

再次单击“确定”按钮，就可以将谷歌的网址成功添加为验证数据之一了，如图 1-7 所示。

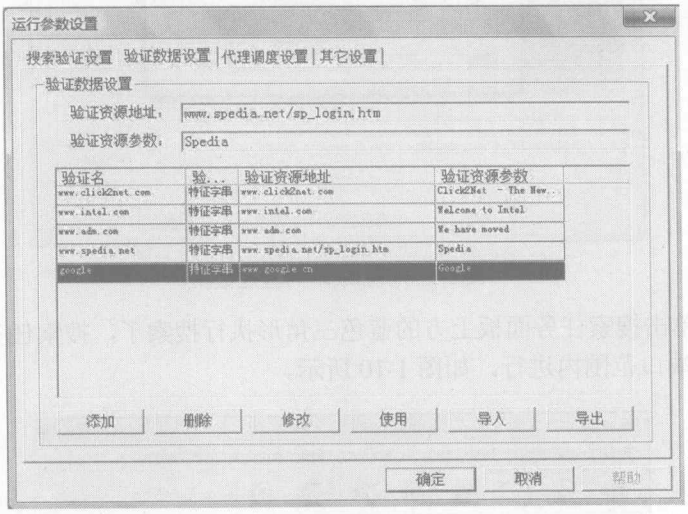

图 1-7　添加成功的验证数据

单击“确定”按钮，完成验证数据的设置。

2. 搜索

返回到初始界面，单击位于左下方的“添加搜索任务”，接下来依次单击下一步→添加按钮，会弹出地址范围类型的选择，如图 1-8 所示。

输入相应的 IP 地址范围或单一 IP 地址后，单击“下一步”按钮，在如图 1-9 所示中设置要搜索的端口号。如果要搜索 http 协议的代理，则必搜的端口号是 80，8080，3128。依次添加要搜索的端口，把其中某些端口设为“必搜”。

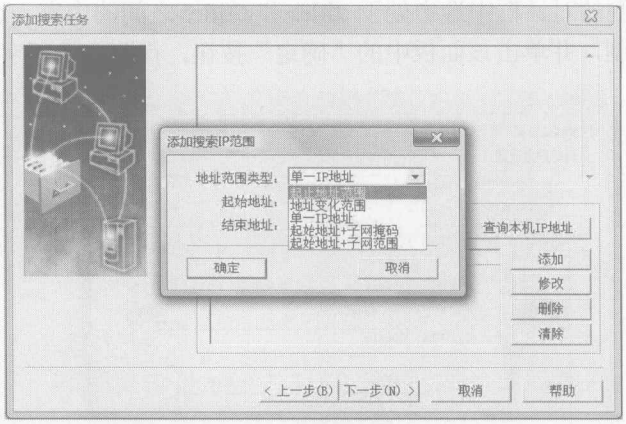

图 1-8　添加搜索 IP 范围

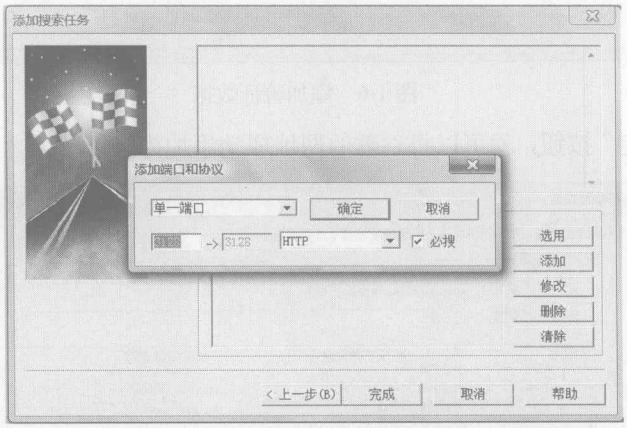

图 1-9　添加成功的验证数据

下面就可以单击搜索任务面板上方的蓝色三角形执行搜索了，搜索任务将在刚才设定的 IP 地址范围内和端口范围内进行，如图 1-10 所示。

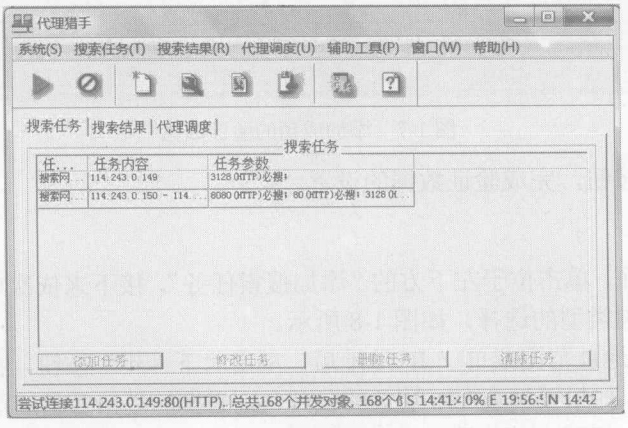

图 1-10　搜索进行中