- 从基本命令和实用工具讲起，让初学者快速入门
- 结合实例详尽剖析黑客攻击技术和防御技巧
- 涉及扫描和嗅探、欺骗与陷阱、木马和间谍、注入攻击、编程攻击等实用内容和最新应用
- 提供常见问题解答与高手经验，真正做到无师自通和提升技能

黑客 教学基地

VIP精品课程
特别奉献

黑客攻防秘技

实战解析

- 1DVD多媒体教学软件
- 44堂多媒体语音视频教程，全程演示核心课程的完整操作

武新华 编著

中国人民大学出版社

北京科海电子出版社
www.khp.com.cn

黑客教学基地

VIP精品课程
特别奉献

黑客攻防秘技
实战解析

武新华 编著

中国人民大学出版社
北京科海电子出版社
www.khp.com.cn

图书在版编目(CIP)数据

黑客攻防秘技实战解析/武新华编著.
北京：中国人民大学出版社，2008
ISBN 978-7-300-09028-3

Ⅰ.黑…
Ⅱ.武…
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（2008）第 024990 号

黑客攻防秘技实战解析

出版发行	中国人民大学出版社　北京科海电子出版社		
社　　址	北京中关村大街 31 号	**邮政编码**	100080
	北京市海淀区上地七街国际创业园 2 号楼 14 层	**邮政编码**	100085
电　　话	（010）82896442　62630320		
网　　址	http: //www.crup.com.cn		
	http: //www.khp.com.cn（科海图书服务网站）		
经　　销	新华书店		
印　　刷	北京市鑫山源印刷有限公司		
规　　格	185×260mm　1/16 开本	**版　　次**	2008 年 4 月第 1 版
印　　张	23.5	**印　　次**	2008 年 4 月第 1 次印刷
字　　数	572 000	**定　　价**	38.00 元（含 1DVD 价格）

前　言

或许大家都曾碰到过这样的情况：当自己正在为精彩的网页着迷时，突然硬盘狂响不止，然后发现所有的程序都不能运行了；正在为网友写E-mail时，突然弹出一个对话框，上面写着“我是幽灵，我要毁了你的电脑！”；正在聊天室里与网友激情聊天时，突然弹出一堆对话框，无论怎么关都关不掉，最后只能无奈地重启计算机；在登录QQ时，却提示密码错误，试遍所有可能的密码却依然不能通过，这时可以确定自己的QQ密码被盗了。

随着互联网的迅猛发展，这些“信息垃圾”、“邮件炸弹”、“病毒木马”、“网上黑客”等也越来越多地威胁着网络的安全。本书紧紧围绕黑客的攻与防，并以其为主线，告诉读者如何构建个人电脑的安全防护措施，使自己从此远离黑客攻击的困扰，确保自己电脑数据的安全。

本书目的在于让读者了解黑客的攻击与防守技术，使读者在实际应用中碰到黑客攻击时，能够做到“胸有成竹”。我们不提倡那些肤浅的入侵、进攻以及破坏，那些都是作为一个真正黑客所鄙视的。本书最主要的精髓在于：希望读者能够运用本书介绍的黑客攻击防守方法去了解黑客，进而防范黑客的攻击，使自己的计算机更加安全。

本书在围绕“攻与防”来展开叙述的同时，特别注重实际例子的演示作用，针对每一种攻防手段，都结合实际的例子来进行介绍，以期读者能够对这些黑客的攻防技术有更加感性的认识。

作者采用最为通俗易懂的图文解说，即使你是电脑新手也能读懂全书；任务驱动式的黑客软件讲解，揭秘每一种黑客攻击的手法；最新的黑客技术盘点，让你实现“先下手为强”；攻防互参的防御方法，全面确保你的计算机安全。

本书适合经常上网但对网络安全和黑客知之甚少的人员阅读，也可作为计算机网络与系统安全爱好者或从业人员的自学参考书。

编者

08年1月

目 录

第 1 章 实战黑客常用命令 1

1.1 测试物理网络 2
1.1.1 认识 Ping 命令 2
1.1.2 Ping 命令的使用 2
1.2 显示端口信息 4
1.2.1 认识 Netstat 命令 4
1.2.2 Netstat 命令的使用 5
1.3 查看 IP、DNS 和 MAC 6
1.3.1 IPconfig 命令介绍 7
1.3.2 IPconfig 命令的使用 7
1.4 查看对方计算机名、所在组、域和当前名称 9
1.5 在网络邻居中隐藏自己的计算机 10
1.6 路由跟踪命令 11
1.6.1 认识 Tracert 命令 12
1.6.2 Tracert 命令的使用 12
1.7 可能出现的问题与解决方法 13
1.8 总结与经验积累 14

第 2 章 揭秘黑客的常用工具 15

2.1 揭秘注入类黑客工具 16
2.2 揭秘扫描类黑客工具 18
2.2.1 端口扫描工具 SuperScan 18
2.2.2 多线程扫描工具 X-Scan 21
2.3 揭秘扩大攻击类黑客工具 26
2.3.1 IRIS 的配置 26
2.3.2 IRIS 的具体使用 28
2.4 揭秘溢出类黑客工具 30
2.5 揭秘木马类黑客工具 31
2.6 揭秘综合类黑客工具 34
2.7 可能出现的问题与解决方法 36
2.8 总结与经验积累 36

第 3 章 网络代理与日志清除 37

3.1 跳板与代理服务器 38
3.1.1 代理服务器概述 38
3.1.2 跳板概述 39
3.1.3 代理服务器的设置 40
3.1.4 制作自己的一级跳板 42
3.2 代理工具的使用 44
3.2.1 代理软件 CCProxy 中的漏洞 44
3.2.2 代理猎手使用技巧 50
3.2.3 代理跳板的创建 55
3.2.4 利用 SocksCap 设置动态代理 57
3.2.5 用 MultiProxy 自动设置代理 61
3.3 巧妙清除日志文件 64
3.3.1 利用 elsave 清除日志 65
3.3.2 手工清除服务器日志 65
3.3.3 用清理工具清除日志 67
3.4 恶意进程的追踪与清除 67
3.4.1 理解进程和线程 68
3.4.2 查看、关闭和重建进程 69
3.4.3 隐藏进程和远程进程 71
3.4.4 杀死自己机器中的病毒进程 73
3.5 可能出现的问题与解决方法 75
3.6 总结与经验积累 76

第 4 章 轻松实现远程监控 77

4.1 修改注册表实现远程监控 78
4.1.1 通过注册表开启终端服务 78
4.1.2 Telnet 中的 NTLM 权限验证 81
4.2 端口监控与远程信息监控 84
4.2.1 监控端口的利器 PORT Reporter 84

4.2.2 URLy Warning 实现远程信息监控.....87
4.3 远程控制技术实际体验.....91
4.3.1 用 CuteFTP 实现上传下载.....92
4.3.2 通过 WinVNC 体验远程控制.....97
4.3.3 用 WinShell 自己定制远程服务端.....100
4.3.4 进行多点控制的利器 QuickIP.....102
4.3.5 定时抓屏的好帮手：屏幕间谍.....106
4.3.6 实现远程控制的魔法控制.....108
4.4 远程控制工具 pcAnywhere.....112
4.4.1 安装 pcAnywhere 程序.....112
4.4.2 设置 pcAnywhere 的性能.....115
4.4.3 用 pcAnywhere 进行远程控制.....120
4.5 可能出现的问题与解决方法.....123
4.6 总结与经验积累.....124

第 5 章 QQ 与 MSN 的攻击与防御.....125

5.1 QQ 攻防实战.....126
5.1.1 QQ 是如何被攻击的.....126
5.1.2 用“QQ 登录号码修改专家”查看聊天记录.....128
5.1.3 防止用 QQ 掠夺者盗取 QQ 密码.....132
5.1.4 防止用“QQ 枪手”在线盗取密码.....133
5.1.5 防止“QQ 机器人”在线盗取密码.....134
5.1.6 QQ 的自带防御功能.....135
5.2 防不胜防的 QQ 远程盗号.....136
5.2.1 防止并不友好的“好友号好好盗”.....136
5.2.2 防止远程控制的“QQ 远控精灵”.....138
5.2.3 不可轻信“QQ 密码保护”骗子.....140
5.2.4 防范 QQ 密码的在线破解.....141
5.3 预防 QQ 信息炸弹与病毒.....147
5.3.1 用 QQ 狙击手 WinPcap 进行信息轰炸.....147
5.3.2 在对话模式中发送消息炸弹的常用工具.....152
5.3.3 向指定的 IP 地址和端口号发送信息炸弹.....154
5.3.4 对付 QQ 信息炸弹.....155
5.4 斩断伸向 MSN 的黑手.....156
5.4.1 Msn Messenger Hack 盗号揭秘.....156
5.4.2 用 Messen Pass 查看本地密码.....159
5.5 可能出现的问题与解决方法.....160
5.6 总结与经验积累.....160

第 6 章 电子邮箱的偷窥与轰炸.....161

6.1 Web-Mail 的用户名和密码.....162
6.1.1 获取 Web-Mail 的用户名和密码.....162
6.1.2 用 WebCracker 破解网络上的用户名和密码.....163
6.2 极易被用户忽略的欺骗法.....166
6.2.1 用邮件地址欺骗获取用户名和密码.....166
6.2.2 用 Outlook Express 漏洞欺骗获取用户名和密码.....166
6.2.3 用 Foxmail 邮件欺骗获取密码方法.....171
6.2.4 绕过 SMTP 服务器的身份验证.....175
6.3 轻松防范电子邮箱轰炸.....176
6.3.1 轻松使用 QuickFyre 邮箱炸弹.....176
6.3.2 实现不间断发信的 KaBoom! 邮箱炸弹.....177
6.3.3 如何防范邮箱炸弹.....178
6.4 邮件收发软件的漏洞攻防.....181
6.4.1 用 Outlook Express 让联系人地址暴露.....181
6.4.2 Foxmail 的账户口令封锁.....184
6.4.3 清除发送邮件时留下的痕迹.....186
6.4.4 加密与解密邮箱与账户.....187
6.5 可能出现的问题与解决方法.....189
6.6 总结与经验积累.....189

第 7 章 木马和间谍软件攻防实战 191

7.1 捆绑木马和反弹端口木马 192
7.1.1 什么是木马 192
7.1.2 极易上当的 WinRAR 捆绑木马 201
7.1.3 轻松制作捆绑木马 204
7.1.4 用“网络精灵”木马（netspy）实现远程监控 206
7.1.5 初识反弹端口木马“网络神偷” 209
7.2 反弹型木马的经典灰鸽子 212
7.2.1 生成木马的服务端 212
7.2.2 木马服务端的加壳保护 214
7.2.3 把木马植入他人的电脑中 215
7.2.4 小心别被对方远程控制 215
7.2.5 灰鸽子的手工清除 219
7.3 全面防范网络蠕虫 221
7.3.1 网络蠕虫概述 222
7.3.2 网络蠕虫病毒实例分析 223
7.3.3 网络蠕虫病毒的全面防范 225
7.4 自动安装“后门程序”的间谍软件 227
7.4.1 用 Spybot 揪出隐藏的间谍 227
7.4.2 间谍广告的杀手 AD-Aware 230
7.4.3 对潜藏的“间谍”学会说“不” 232
7.5 可能出现的问题与解决方法 235
7.6 总结与经验积累 235

第 8 章 扫描、嗅探和欺骗 237

8.1 扫描与反扫描工具精粹 238
8.1.1 用 MBSA 检测 Windows 系统是否安全 238
8.1.2 深入浅出 RPC 漏洞扫描 240
8.1.3 WebDAVScan 服务器漏洞扫描 241
8.1.4 用网页安全扫描器查看网页是否安全 243
8.1.5 防御扫描器追踪的 ProtectX 246
8.1.6 网页信息收集器 248
8.2 几款经典的网络嗅探器 251
8.2.1 用嗅探器 Sniffer Pro 捕获数据 251
8.2.2 用嗅探器 SpyNet Sniffer 实现多种操作 255
8.2.3 捕获网页内容的艾菲网页侦探 256
8.2.4 局域网中的嗅探精灵 IRIS 258
8.3 网络上的欺骗与陷阱 260
8.3.1 具备诱捕功能的蜜罐 261
8.3.2 拒绝恶意接入的网络执法官 264
8.4 可能出现的问题与解决方法 269
8.5 总结与经验积累 270

第 9 章 黑客入侵防御实例详解 271

9.1 木马病毒入侵入梦来：冰河 272
9.1.1 冰河木马使用流程 272
9.1.2 配置冰河木马的被控端 273
9.1.3 搜索、远控目标计算机 274
9.1.4 卸载和清除冰河木马 276
9.2 黑客的掌上明珠：SSS 277
9.3 当代的千里眼：流萤 282
9.3.1 配置服务端 282
9.3.2 监听主机 283
9.3.3 接入控制 283
9.3.4 服务端的卸载 284
9.4 运用 SQL 注入解密电影网站 284
9.5 急需设防的 139 端口 286
9.6 可能出现的问题与解决方法 289
9.7 总结与经验积累 289

第 10 章 编程攻击与防御实例 291

10.1 通过编程创建木马 292
10.1.1 编程实现木马攻击 292
10.1.2 防御简单木马攻击 297
10.2 隐藏防拷贝程序 298
10.3 可能出现的问题与解决方法 300
10.4 总结与经验积累 300

第 11 章 注入攻击与防范应用实战 301

11.1 SQL 的隐形杀手：NBSI 302
11.1.1 NBSI 注入实战 302

11.1.2 具体的防御措施 304
11.2 尘缘雅境图文系统入侵工具 305
11.3 辅助注入工具 WIS 应用实战 306
11.4 剖析桂林老兵动网上传专用程序 308
11.5 SQL 攻击与防护 310
11.6 可能出现的问题与解决方法 312
11.7 总结与经验积累 312

第 12 章 留后门与清脚印 313

12.1 给自己的入侵留后门 314
12.1.1 手工克隆账号 314
12.1.2 命令行方式下制作后门账号 317
12.1.3 克隆账号工具 319
12.1.4 用 Wollf 留下木马后门 320
12.1.5 SQL 后门 323
12.2 清除登录服务器的日志清单 324
12.2.1 手工清除服务器日志 324
12.2.2 使用批处理清除远程主机日志 325
12.2.3 通过工具清除事件日志 326
12.2.4 清除 WWW 和 FTP 日志 326
12.3 清除日志工具 elsave 和 CleanIISLog 327
12.3.1 日志清除工具 elsave 的使用 328
12.3.2 日志清除工具 CleanIISLog 的使用 329
12.4 可能出现的问题与解决方法 329
12.5 总结与经验积累 329

第 13 章 打好网络安全防御战 331

13.1 建立系统漏洞防御体系 332
13.1.1 检测系统是否存在可疑漏洞 332
13.1.2 修补系统漏洞 335
13.1.3 Web 服务安全设置 339
13.1.4 监视系统的操作进程 342
13.1.5 防火墙安装应用实例 344
13.2 使用和维护硬盘数据恢复 353
13.2.1 什么是数据恢复 353
13.2.2 造成数据丢失的原因 353
13.2.3 数据恢复工具 Easy Recovery 和 Final Data 354
13.3 杀毒软件使用实战 358
13.3.1 瑞星杀毒软件使用实战 358
13.3.2 江民杀毒软件 KV2008 使用实战 359
13.3.3 金山毒霸使用实战 361
13.3.4 卡巴斯基使用实战 363
13.4 可能出现的问题与解决方法 366
13.5 总结与经验积累 367

1 实战黑客常用命令

技术要点：

- 测试物理网络
- 显示端口信息
- 查看 IP、DNS、MAC 等
- 查看对方计算机名、所在组、域和当前名称
- 在网络邻居中隐藏自己的计算机
- 路由跟踪命令

学习目标：

作为一名黑客，很有必要熟知一些关于网络操作的命令（当然不是全部掌握，但要有一部分是必须熟练使用的），这样才能有效地收集更多的信息，为自己实现入侵和安全防御带来更大便利。

黑客常用的命令也都是 Windows 系统自带的一些网络命令，这些简单常用的命令是一个黑客菜鸟应该会使用的。

1.1 测试物理网络

测试物理网络的命令 Ping（Packet Internet Grope，因特网包探索器），是用于测试网络连接量的程序。它发送一个 ICMP 响应请求消息给目的地，并报告是否收到所希望的 ICMP 应答，校验与远程计算机或本地计算机的连接。

1.1.1 认识 Ping 命令

Ping 命令只有在安装有 TCP/IP 网络协议的计算机中才能使用，主要用于验证看起来已经用网络连接上的计算机是否已经连通了。TCP/IP 协议可在【本地连接属性】中进行设置，如图 1-1 所示。在设置好 TCP/IP 协议之后，就可以使用 Ping 命令了。

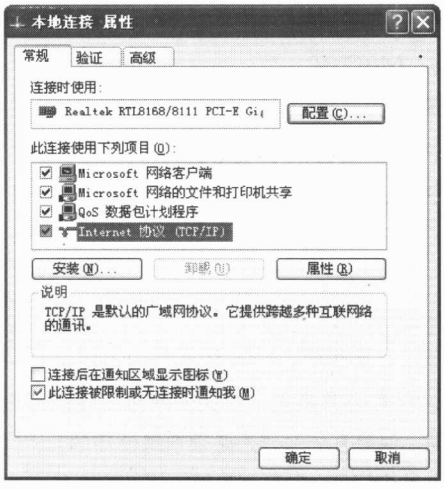

图 1-1 TCP／IP 协议

Ping 命令的工作原理是：利用用户的计算机向待验证连通与否的计算机发送一些包含了特定数据的数据包，并等待这些计算机返回特定的数据包。

1.1.2 Ping 命令的使用

在【运行】对话框的“打开”文本框中输入“cmd”命令，单击【确定】按钮，即可打开 DOS 命令提示符窗口，其中的“Administrator”即为本计算机的名字，如图 1-2 所示。

这时输入“cd\”命令，返回到 C 盘根目录下之后，再输入格式为“Ping+空格+IP 地址”的指令，如输入“Ping 192.168.0.8”，如图 1-3 所示。其中 192.168.0.8 是目标地址，发送包大小是 32 字节。在命令执行结束之后，可以看到发了几个包，收到几个包，还可以看到丢包率。

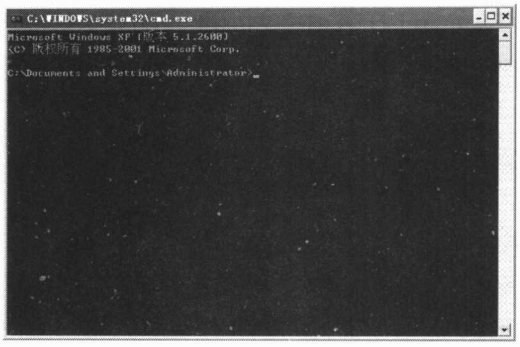

图 1-2　命令提示符窗口

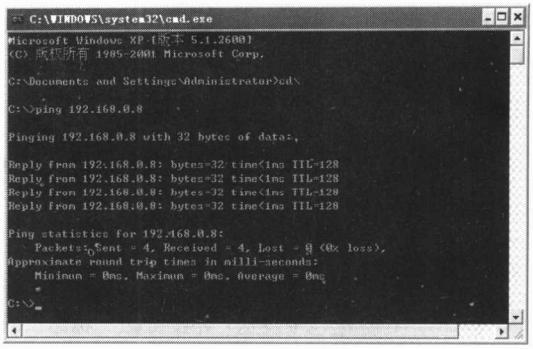

图 1-3　目标地址和发送包大小

如果想长时间测试，则可以在命令后加一参数“-t”，以一直对目标地址执行 Ping 命令。如想结束命令，则可按“Ctrl+C”组合键，并且可以看到一共发了多少个包，丢了多少包，还可以查看丢包率。如果不想中断命令就查看这些信息，也可按“Ctrl+Pause”组合键查看丢包率，如图 1-4 所示。

当要访问一个站点（例如 www.newtop01.com）时，可以利用 Ping 程序来测试目前连接该网站的速度（如输入“Ping www.newtop01.com”），如图 1-5 所示。

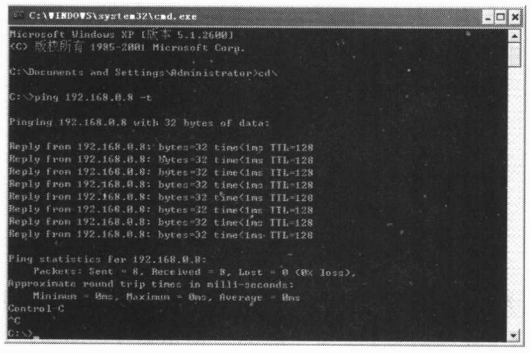

图 1-4　查看丢包率

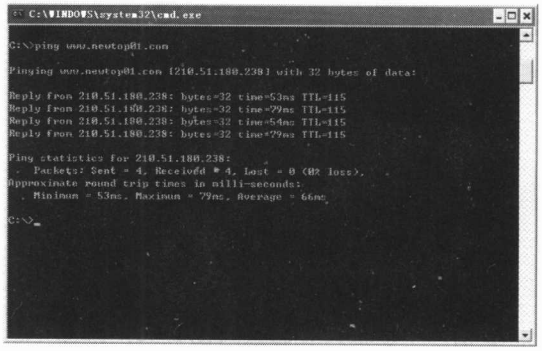

图 1-5　Ping 网站的运行窗口

当输入“Ping www.newtop01.com”命令之后，该程序就会向指定的 Web 网址主服务器发送一个 32 字节的消息，并将服务器的响应时间记录下来。

Ping 程序将会向用户显示 4 次响应结果，响应时间低于 300 毫秒都可以认为是正常的；时间超过 400 毫秒则较慢；出现“请求暂停（Request time out）”信息意味着网址没有在 1 秒内响应，这表明服务器没有对 Ping 做出响应或者网址反应极慢。

如果看到 4 个“请求暂停”信息，说明网址拒绝 Ping 请求。因为过多的 Ping 测试本身会产生瓶颈，因此，许多 Web 管理员不让服务器接受此测试。如果网址很忙或出于其他原因运行速度很慢，如硬件动力不足，数据信道比较狭窄，过一段时间可以再试一次以确定网址是不是真的有故障。如果多次测试都存在问题，则可以认为是用户的主机和该网址站点没有连接上，用户应该及时与因特网服务商或网络管理员联系。

Ping 命令的使用格式为“Ping [-t] [-a] [-n count] [-l length] [-f] [-i ttl] [-v tos] [-r count] [-s count] [-j computer-list] | [-k computer-list]] [-w timeout] destination-list”。

各参数说明如下。

◎ -t：对要验证连通与否的计算机进行验证直到被中断，可用“Ctrl+C”组合键终止。

◎ -a：将地址解析为计算机名。

◎ -n count：发送 count 指定的响应数据包数，默认数值为 4。

◎ -l length：发送包含由 length 指定数据量的响应数据包，默认为 32B（字节），最大值为 65 527。

◎ -f：在数据包中发送“不要分段”标志。一般情况下，发送给对方的数据包都会被路由上的网关分段，使用该参数之后，所发送的数据包就不会被分段了。

◎ -i ttl：指定 ttl 值在对方系统中停留的时间。

◎ -v tos：将“服务类型”设置为 tos 指定的值。

◎ -r count：在“记录路由”字段中记录传出和返回数据包的路由。count 最少可以指定 1 台，最多指定 9 台计算机。

◎ -s count：指定 count 值的跃点数和时间戳。

◎ -j computer-list：利用 computer-list 指定的计算机列表路由数据包。连续计算机可以被中间网关分隔（路由稀疏源），IP 允许的最大数量为 9。

◎ -k computer-list：利用 computer-list 指定的计算机列表路由数据包。连续计算机不能被中间网关分隔（路由严格源），IP 允许的最大数量为 9。

◎ -w timeout：指定超时间隔，单位为毫秒。

◎ destination-list：指定要 Ping 的远程主机。

1.2 显示端口信息

在 Internet 上，各主机间通过 TCP/TP 协议发送和接收数据包，各个数据包根据其目的主机的 IP 地址，来进行互联网络中的路由选择。网络上的电脑进行通信，都是通过电脑开放的端口来完成的。形象地说，每个开放的端口就像一扇打开的门。因此，要想保证电脑的安全，就最好守好这些打开的门。

1.2.1 认识 Netstat 命令

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

使用格式：Netstat [-a] [-e] [-n] [-o] [-p Protocol] [-r] [-s] [Interval]

各参数说明如下。

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

◎ –e：显示以太网的统计信息，如发送和接收的字节数、数据包数。该参数可以与–s 结合使用。

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

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

◎ –p Protocol：显示 Protocol 所指定的协议连接，可以是 TCP、UDP、TCPv6 或 UDPv6 等。如果该参数与–s 一起使用，按协议显示的统计信息，则 Protocol 可以是 TCP、UDP、ICMP、IP、TCPv6、UDPv6、ICMPv6 或 IPv6 等。

◎ –s：按协议显示统计信息。默认情况下，显示 TCP、UDP、ICMP 和 IP 协议的统计信息。如果安装了 Windows XP 的 IPv6 协议，则显示有关 IPv6 上的 TCP、UDP、ICMP 等协议统计信息（可以使用–p 参数指定协议集）。

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

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

与 Netstat 命令一起使用的参数，必须以连字符（-）而不是以短斜线（/）作为前缀。

Netstat 提供下列统计信息：

◎ Proto：协议的名称（TCP 或 UDP）。

◎ Local Address：本地计算机的 IP 地址和正在使用的端口号。如果不指定–n 参数，则显示与 IP 地址和端口名称对应的本地计算机名称。如端口尚未建立，端口以星号“*”显示。

◎ Foreign Address：连接远程计算机的 IP 地址和端口号码。如果不指定–n 参数，则显示与 IP 地址和端口对应的名称。如端口尚未建立，则端口以星号“*”显示。

◎ State：表明 TCP 连接的状态。

1.2.2 Netstat 命令的使用

Netstat 命令只有当网络协议（TCP/IP）在网络连接中，并安装为网络适配器属性的组件时才可使用，具体表现如下：

◎ 要显示以太网统计信息和所有协议的统计信息，输入命令：Netstat–e–s

◎ 要仅显示 TCP 和 UDP 协议的统计信息，输入命令：Netstat–s–p TCP UDP

Netstat 命令的具体使用实例如下。

◎ 在命令提示符窗口中输入“Netstat –a”并回车，即可显示用户计算机当前所开放的所有端口，其中参数–a 的含义表示显示所有连接和侦听端口，如图 1–6 所示。

◎ 运行“Netstat –s –e”命令，即可显示用户比较详细的网络资料，包括 IP、ICMP、TCP 和 UDP 的统计等，如图 1–7 所示。

◎ 如果运行“Netstat –r”命令，则可显示内核路由表，如图 1–8 所示。

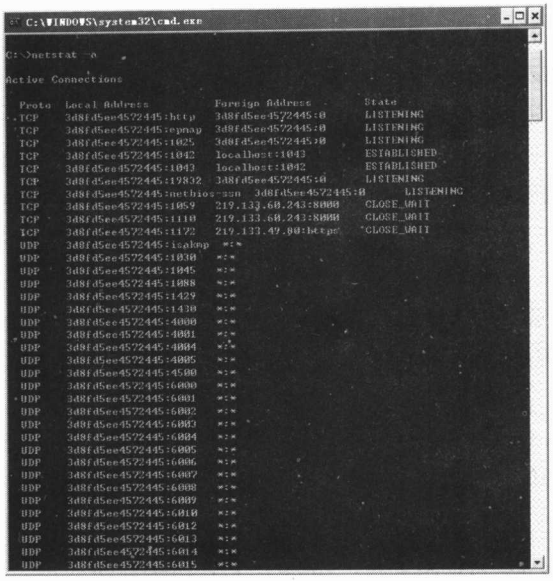

图 1-6 显示当前所开的所有端口

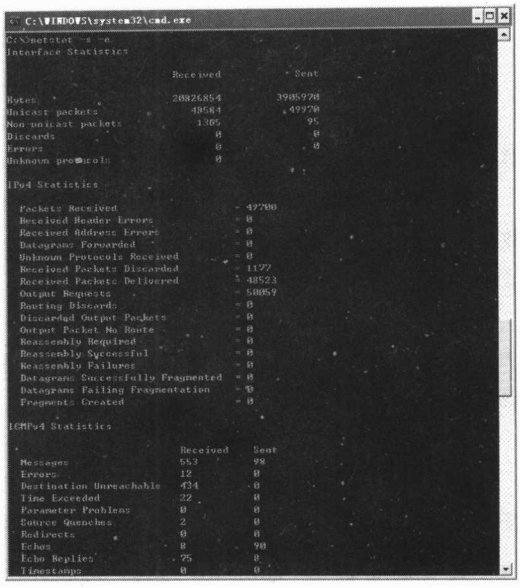

图 1-7 显示端口详细资料

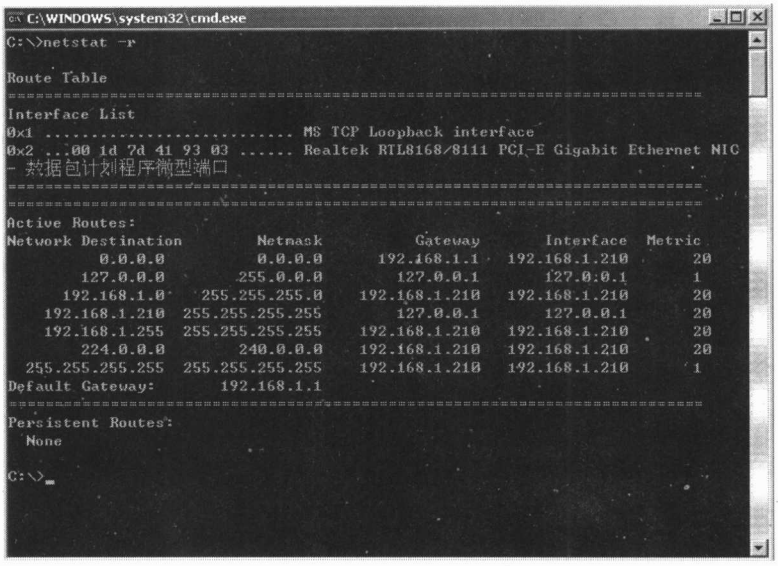

图 1-8 显示路由表

1.3 查看 IP、DNS 和 MAC

IPconfig 也是内置于 Windows 的基于 TCP/IP 的应用程序之一，用于显示本地计算机的 IP 地址配置信息和本机网卡的 MAC 地址。利用 IPconfig 工具，可以查看和修改网络中的 TCP/IP 协议的相关配置，例如 IP 地址、网关、子网掩码等。

1.3.1 IPconfig 命令介绍

IPconfig 是调试计算机网络的常用命令，通常使用它显示计算机中网络适配器的 IP 地址、子网掩码以及默认网关。尤其当网络设置的是 DHCP（动态 IP 地址配置协议）时，利用 IPconfig 命令可以很简单地了解到 IP 地址的实际分配情况。

IPconfig 的命令格式：IPconfig [/? | /all | /renew [adapter] | /release [adapter] | /flushdns | /displaydns | /registerdns | /showclassid | /setclassid adapter [classid]]

各参数说明如下。

◎ /all：将配置完整显示。如果省去所有参数，则执行后只显示 IP 地址、子网掩码和每个网卡的默认网关值。

◎ /renew [adapter]：更新 DHCP 配置参数。这个参数只能在运行有 DHCP 客户端软件的系统上使用。若要指定适配器名称，则输入不带有参数的 IPconfig 命令，即可显示适配器名称。

◎ /release [adapter]：发布当前的 DHCP 配置。这个参数将禁用本地系统上的 TCP/IP，并只在 DHCP 客户端上可用。

◎ /flushdns：清除本地 DNS 缓存内容。

◎ /displaydns：显示本地 DNS 的内容。

◎ /registerdns：使所有 DNS 客户端手工向服务器进行注册。

◎ /showclassid：显示所有 DHCP 考虑到适配器的身份证。

◎ /batch 文件名：将 IPconfig 所显示信息以文本方式写入指定文件。此参数可用来备份本机的网络配置。

1.3.2 IPconfig 命令的使用

IPconfig 命令允许用户决定由 DHCP 配置的值。综合而言，IPconfig 是一个功能相当强大的工具。如果在一台 IP 地址为 192.168.0.1 的计算机上运行“IPconfig /all/batch 01.txt”命令，则可以将运行结果存到文件 01.txt（文件名称请自己设定）中，打开文件可查看相关的结果。

IPconfig 命令使用实例如下：

◎ 使用 IPconfig 查看本机 IP 地址的演示界面如图 1-9 所示。

◎ 使用参数/all 的运行结果，是将本地当前 TCP/IP 协议的配置全部显示，包括网卡物理地址、计算机 IP 地址、子网掩码和网关等信息，如图 1-10 所示。

◎ 再来看看参数-release 的使用，它将会禁用 TCP/IP 协议，返回 IP 地址和默认子网掩码都是 0.0.0.0，如图 1-11 所示。

如果没有参数，则 IPconfig 命令将向用户提供所有当前的 TCP/IP 配置值，包括 IP 地址和子网掩码。“IPconfig /release”和“IPconfig /renew”是两个附加选项，只能在向 DHCP 服务器租用其 IP 地址的计算机上起作用。如果输入“IPconfig /renew”命令，则本地计算机便设法与 DHCP 服务器取得联系，并租用一个 IP 地址。

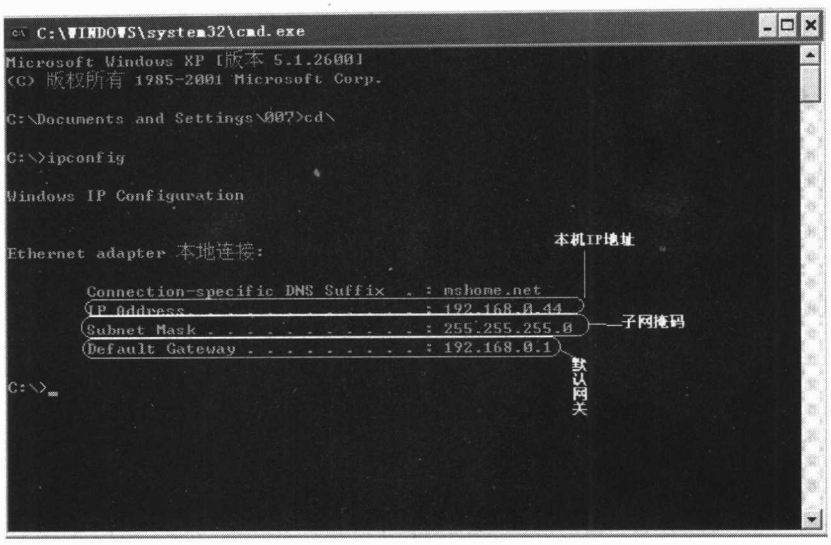

图 1-9　查看本地计算机 IP 地址

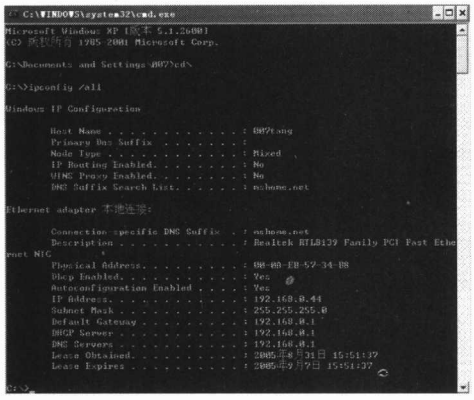

图 1-10　IPconfig /all 运行结果

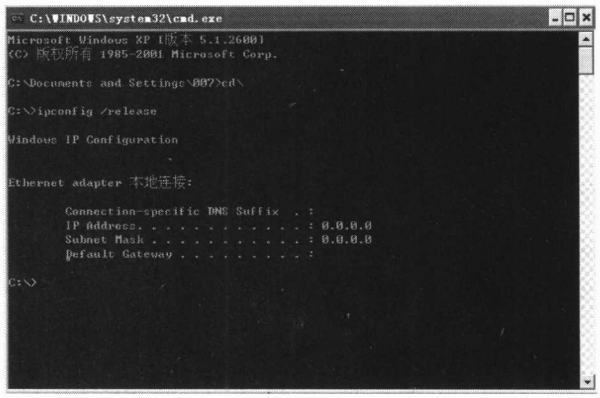

图 1-11　参数 release 的使用

大多数情况下，网卡将被重新赋予和以前相同的 IP 地址。如果网络连通发生故障，且凑巧网卡的 IP 地址是自动分配的，就可以使用下面的命令进行解决了。

◎ IPconfig /release 1，去除网卡（适配器 1）的动态 IP 地址。

◎ IPconfig /renew 1，为网卡重新动态分配 IP 地址。

若要查看远程服务器的 DNS，首先要安装 DNS 服务，具体的操作步骤如下：

Step01 选择【开始】→【设置】→【控制面板】→【添加/删除程序】→【添加/删除 Windows 组件】选项，即可打开【Windows 组件向导】对话框，如图 1—12 所示。

Step02 双击其中的“网络服务”选项，即可打开【网络服务】对话框，并在其中勾选“域名系统（DNS）”复选框，如图 1—13 所示。

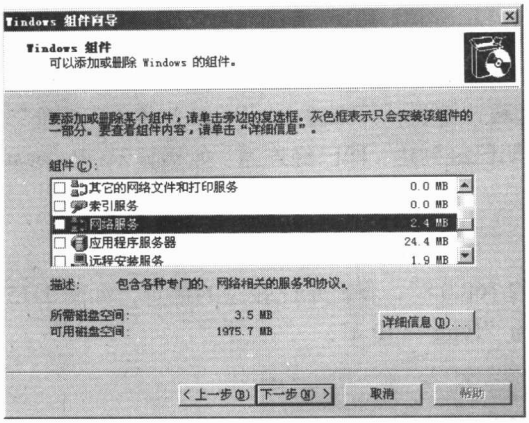

图 1-12 【Windows 组件向导】对话框

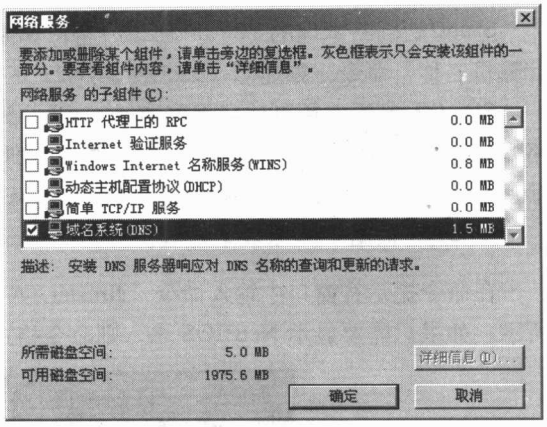

图 1-13 【网络服务】对话框

Step03 单击【确定】按钮返回【Windows 组件向导】对话框之后，单击【下一步】按钮，即可开始安装，并在安装完毕后，弹出【完成“Windows 组件向导”】对话框。

Step04 单击【完成】按钮，即可完成安装，如图 1-14 所示。

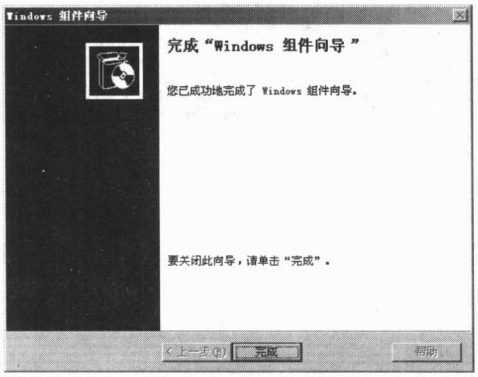

图 1-14 完成 Windows 组件向导

在安装及配置好 DNS 之后，就可以查看服务器的 DNS 了，其命令是：NSLOOKUP。例如，在命令提示符窗口中运行“C:\nslookup”命令之后，将显示如下的结果：

```
Default server:ns. hesjptt.net.cn
Address:202.99.160.68
>
```

可以通过在“>”后面输入“server IP”命令来修改用户的 DNS，比如：>server 202.99.41.2 则将 DNS 改为了 41.2。

1.4 查看对方计算机名、所在组、域和当前名称

查看对方计算机名、所在组、域和当前名称需要有如下几个操作。