

黑客

杀狼
破狼

攻防秘技入门

武新华 陈芳 段玲华 等编著

- 例说黑客入侵与防御
- Windows 系统漏洞攻防实战
- 木马的植入与防杀：远程控制技术大集合
- 伸向 QQ 和 MSN 的黑手
- 防范自己的邮箱被偷窥和轰炸
- 防不胜防的 IE 浏览器恶意攻击
- 必不可少的超级经典小工具
- 全面飚升网络控制的权限
- 防止 IIS 服务器被恶意攻击



机械工业出版社
CHINA MACHINE PRESS



未破译——黑客攻防秘技入门

武新华 陈 芳 段玲华 等编著



机械工业出版社

本书紧紧围绕黑客的攻防来介绍,在详细介绍黑客攻击手段的同时,介绍了相应的防范方法,使读者对于攻防技术有系统的了解,能够更好地防范黑客的攻击。全书共分 11 章,包括黑客入侵与防御方法、Windows 系统漏洞攻防实战、木马的植入方法与防杀、远程控制技术大集合、QQ 和 MSN 黑客防御、防范自己的邮箱被偷窥和轰炸、如何防止浏览器被恶意攻击、常用超级小工具、全面提升网络控制权力、如何防止 IIS 服务器被恶意攻击、打好网络安全防御战等。

本书内容丰富,图文并茂,深入浅出,适用于广大网络爱好者,同时可作为一本速查手册,适用于网络安全从业人员及网络管理员。

图书在版编目(CIP)数据

杀破狼——黑客攻防秘技入门/武新华,陈芳,段玲华等编著.

-北京:机械工业出版社,2006.4

ISBN 7-111-18870-5

I. 杀… II. ①武… ②陈… ③段… III. 计算机网络-安全技术-基本知识 IV. TP393.08

中国版本图书馆 CIP 数据核字(2006)第 031574 号

机械工业出版社(北京市百万庄大街 22 号 邮政编码 100037)

策划编辑:夏孟瑾 责任编辑:李虎斌 版式设计:崔俊利

三河市宏达印刷有限公司印刷

2006 年 5 月第 1 版第 1 次印刷

184mm×260mm·22 印张·489 千字

0001—5000 册

定价:32.00 元

凡购本图书,如有缺页、倒页、脱页,由本社发行部调换

本社购书热线电话:(010) 68326294

封面无防伪标均为盗版

前 言

随着计算机技术的飞速发展，网络的安全问题也日益严重。也许仅仅是晚几天没有升级杀毒软件的病毒库或不小心点击了一个链接，都有可能带来巨大的损失。想必大家听说过“冰河”、“欢乐时光”、“漏洞攻击”吧，但这些只是黑客惯用伎俩中很小的一部分，黑客攻击的手段实在是太多了，因为每一台与互联网连接的计算机都可能成为黑客的攻击对象，当然其中也包括我们的计算机。

对于那些防范意识较差或对网络安全知识不甚了解的用户，常常极易成为黑客攻击的目标。因此，为了让所有计算机使用者能够防患于未然，对于书中几乎所有的内容，作者都在写作时直接用连接 Internet 的计算机进行了实践，并对黑客常用的一些攻击手段进行了详尽的分析，分析得到的结果便是使读者在实际应用中碰到黑客攻击时，能够做到“胸有成竹”，避免因遭受攻击与破坏而造成损失。

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，都结合实际例子来进行介绍，以使读者能够对这些黑客的攻防技术有更加感性的认识。

应该说，在黑客攻防方面历来都是“道高一尺，魔高一丈”，没有哪本书可以把黑客所有的攻击手段都剖析清楚，本书也只是讲述了一些最常见的黑客攻击手段，但与市面上种类繁多的黑客类图书相比，本书仍然具有如下几个方面的优点：

1. 实用价值高。
2. 通俗易懂，使枯燥的学习过程更轻松。
3. 经验性强，能够把使用过程中的问题描绘得清清楚楚，便于分辨正误。
4. 犹如老师在旁边亲自指导，有种亲临现场的感觉。

本书采用最为通俗易懂的图文解说，即使是计算机新手也可轻松通读；由浅入深的黑客软件讲解，详尽揭秘黑客攻击的手法；全新的黑客技术大盘点，让用户实现“先下手为强”；攻防互参的防御方法，全面确保用户的网络安全。

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御方法去了解黑客，进而构筑自己的“铜墙铁壁”，使自己的网络更加安全。

本书言简意赅，内容详实，能够使读者在学习有关黑客知识时而不觉得乏味，在轻松和趣味中不知不觉地学习到防杀黑客的基本知识，从而使自己在以后使用计算机时能够防止黑客的攻击与破坏，保护自己计算机中的资料不被黑客看到和破坏。

本书由众多经验丰富的高校教师编写，并得到了众多热心网友的支持，在此一并表示衷心的感谢。本书的编写情况是：武新华负责第 1、2、3、4、8 章，段玲华负责第 5、6 章，陈芳负责第 7、11 章，安向东负责第 9、10 章，最后由武新华统审全稿。由于作者水平有限，加之创作时间仓促，本书难免有疏漏之处，欢迎广大读者朋友批评指正。

最后，请读者一定要注意一点：不要迷信书，要相信自己的实践。由于软件的更新换代，任何一本书都不能保证书中的内容和实际应用中的软件完全一致，所以书中的疏漏和错误在所难免，当然本书也不例外。如果读者觉得本书中有不妥或需要改进之处，可以登录 www.newtop01.com 与笔者联系，笔者衷心感谢提供建议的读者，并真心希望和广大读者互动的过程中能得到提高，在此致谢！

最后，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一定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！

为便于读者阅读和理解，本书在写作中使用了如下图标约定：



对文中所涉及到的一些小知识进行描述，让读者在遇到类似问题时，能够理解应用，方便其操作。



设置问题，考察读者对操作的掌握情况。



对文章中所涉及到的一些内容进行特别描述，提醒读者注意操作到此处时，切忌不要犯的一些常识性错误。



提示读者关于文中所述内容的一些相关信息，以及对文中表述不清的内容进行进一步的阐述。



对实际操作中的一些小技巧进行阐述，教给读者应该如何进行具体操作。

编 者

目 录

前言

第 1 章 黑浪滔天话黑客——例说黑客入侵与防御	1
1.1 功能强大的黑客工具——“冰河” 2005	2
1.1.1 揭开“冰河”木马的神秘面纱	2
1.1.2 配置“冰河”木马的被控端程序	3
1.1.3 搜索、远控目标计算机	4
1.1.4 “冰河”木马的使用	7
1.1.5 如何卸载和清除“冰河”木马	8
1.1.6 用“冰河陷阱”诱骗黑客	10
1.2 守好那扇进出的门——IPC\$漏洞入侵与防御	12
1.2.1 何谓 IPC\$漏洞的入侵	12
1.2.2 实现 IPC\$漏洞扫描	13
1.2.3 探测 IPC\$的用户列表	14
1.2.4 如何连接到目标主机	15
1.2.5 如何防范 IPC\$漏洞的入侵	17
1.3 黑客的常用伎俩——命令行下的远程控制 PsExec	21
1.4 一双偷窥的眼睛——远程开启视频木马初探	22
1.4.1 如何开启远程视频	22
1.4.2 如何清除服务器端	24
1.5 为你通风报信的“灰鸽子”	25
1.5.1 配置自己的“灰鸽子”	25
1.5.2 实施远程木马控制	26
1.5.3 如何卸载“灰鸽子”	28
1.6 可能出现的问题与解决	29
1.7 总结与经验积累	29
第 2 章 全面堵截系统漏洞——Windows 系统漏洞攻防实战	31
2.1 Windows 系统的登录口令攻防	32
2.1.1 设置 Windows 2000 系统的账户登录口令	32
2.1.2 入侵与防御 Windows 2000 系统的输入法漏洞	33
2.1.3 Windows 2000 系统崩溃漏洞的攻防	38

2.1.4	SAM 数据库安全漏洞攻防实战	39
2.1.5	NetBIOS 漏洞的入侵与防御	41
2.1.6	实战 Windows 系统 RPC 漏洞的攻防	44
2.1.7	用启动脚本法实现系统登录	46
2.1.8	Windows XP 的账户登录口令	46
2.2	守好组策略与注册表的登录之门	49
2.2.1	组策略登录安全之账户锁定策略	49
2.2.2	组策略登录安全之密码策略	50
2.2.3	组策略登录安全之更改 Administrator 账户	51
2.2.4	组策略登录安全之设置用户权限	53
2.2.5	阻止访问和非法编辑注册表编辑器	55
2.2.6	保护自己的屏幕保护程序	56
2.2.7	注册表登录安全之口令保护策略	57
2.2.8	注册表登录安全之隐藏保护策略	58
2.3	Windows 系统常见密码攻防实战	59
2.3.1	取消共享和隐藏共享文件夹	59
2.3.2	揭秘文件的属性加密	61
2.3.3	方便好用的新概念文件加密器	64
2.3.4	值得一提的“紫电文件夹加密保护神”	65
2.3.5	功能强大的密码破解器	66
2.3.6	如何解除分级审查密码	68
2.3.7	用“超级密码卫士”管理密码	69
2.4	解除注册表自动运行中的恶意程序	71
2.4.1	解除自动运行的木马	71
2.4.2	解除 Windows 程序的自启动	72
2.4.3	如何设置 Windows 的自动登录	74
2.4.4	只允许运行指定的程序	75
2.4.5	设置启动信息或增加警告标题	76
2.4.6	让某个用户自动登录	76
2.5	可能出现的问题与解决	77
2.6	总结与经验积累	77
第 3 章	揭秘悄悄潜入计算机的间谍——木马的植入与防杀	79
3.1	揭开木马神秘的面纱	81
3.1.1	了解形形色色的木马	81
3.1.2	如何识破木马的伪装	82
3.1.3	木马是如何被启动的	83

3.1.4 如何知道自己是否中了木马	85
3.2 木马的植入与潜藏	86
3.2.1 利用合成工具 Exebinder 伪装木马	86
3.2.2 利用“万能文件捆绑器”伪装木马	87
3.2.3 利用合成工具 Joine 伪装木马	88
3.2.4 伪装木马的利器——网页木马生成器	88
3.2.5 扫描装有木马程序的计算机	89
3.2.6 创建与目标计算机木马程序的连接	90
3.3 都有哪些最为常用的木马	90
3.3.1 “黑暗天使”木马的使用和预防	90
3.3.2 剖析 BackOrifice 2000 木马	92
3.3.3 驾驭好这头默不作声的“网络公牛 (Netbull)”	95
3.3.4 远程监控杀手——“网络精灵”木马 (netspy)	98
3.3.5 远程控制少不了它——“广外女生”木马	100
3.3.6 网络江湖的神秘高手——网络神偷	102
3.4 木马的杀除和预防	103
3.4.1 使用 Trojan Remover 清除木马	103
3.4.2 使用 BoDetect 检测和清除 BO2K 木马	104
3.4.3 使用“木马克星”来清除木马	105
3.4.4 如何使用 The Cleaner 来清除木马	107
3.4.5 使用 LockDown2000 防火墙防范木马	108
3.4.6 如何手动清除木马	111
3.5 可能出现的问题与解决	112
3.6 总结与经验积累	113
第 4 章 新鲜刺激的远程控制——远程控制技术大集合	115
4.1 用 Serv-U 创建 FTP 服务器	116
4.1.1 Serv-U 的安装	116
4.1.2 如何配置自己的 Serv-U	117
4.1.3 详细设置自己的 Serv-U	119
4.2 修改注册表实现远程监控	121
4.2.1 通过注册表开启终端服务	122
4.2.2 突破 telnet 中的 NTLM 权限验证	122
4.3 端口监控与远程信息监控	123
4.3.1 监控端口的利器——SuperScan	123
4.3.2 URLy Warning 实现远程信息监控	125
4.4 几款实现远程控制技术的实际体验	126

4.4.1	用 CuteFTP 实现上传下载.....	126
4.4.2	通过 WinVNC 来体验一把远程控制.....	130
4.4.3	用 WinShell 自己定制远程服务端.....	131
4.4.4	进行多点控制的利器——QuickIP.....	133
4.4.5	定时抓屏的好帮手——屏幕间谍.....	135
4.4.6	用“魔法控制 2005”实现远程控制.....	137
4.5	远程控制的好帮手——pcAnywhere.....	140
4.5.1	安装 pcAnywhere 程序.....	140
4.5.2	设置 pcAnywhere 的性能.....	141
4.5.3	如何用 pcAnywhere 进行远程控制.....	142
4.6	可能出现的问题与解决.....	145
4.7	总结与经验积累.....	146
第 5 章	伸向 QQ 和 MSN 的黑手——给聊兴正浓的朋友泼点冷水.....	147
5.1	为什么 QQ 不安全.....	148
5.1.1	QQ 是如何被攻击的.....	148
5.1.2	利用“QQ 登录号码修改专家”查看聊天记录.....	150
5.1.3	盗取 QQ 密码的强盗——QQ 掠夺者.....	153
5.1.4	盗取 QQ 密码的利器——“QQ 破密使者”和“QQ 密码使者”.....	154
5.1.5	给你一双窃取 QQ 密码的黑眼睛.....	156
5.1.6	浅析偷看聊天记录和 QQ 视频欺骗.....	157
5.2	QQ 密码在线攻防.....	158
5.2.1	用“QQ 枪手”在线盗取密码.....	158
5.2.2	用 QQExplorer 在线破解 QQ 密码.....	158
5.2.3	疯狂的盗号者——QQ 机器人.....	160
5.2.4	用盗号木马也可以取走 QQ 密码.....	161
5.3	防不胜防的远程盗号.....	162
5.3.1	通过消息诈骗获取 QQ 密码.....	162
5.3.2	并不友好的“好友号好好盗”.....	163
5.3.3	可以进行远程控制的“QQ 远控精灵”.....	164
5.3.4	千万别轻信“QQ 密码保护”骗子.....	165
5.3.5	防范 QQ 密码的在线破解.....	166
5.4	让 QQ 冲破代理的封锁.....	168
5.4.1	通过 CCProxy 突围 QQ 代理.....	168
5.4.2	如何让 QQ 动态代理 IP.....	170
5.5	学会对付企鹅杀手——QQ 信息炸弹与病毒.....	172
5.5.1	用 QQ 狙击手 IpSniper 进行信息轰炸.....	172

5.5.2	如何在对话模式中发送消息炸弹.....	173
5.5.3	向指定的 IP 地址和端口号发送消息炸弹.....	175
5.5.4	学会对付 QQ 消息炸弹.....	176
5.6	伸向 MSN 号码的黑手.....	178
5.6.1	用 MSN Messenger Hack 盗号揭秘.....	178
5.6.2	用 MessenPass 查看本地密码.....	179
5.7	可能出现的问题与解决.....	180
5.8	总结与经验积累.....	181
第 6 章	防范自己的邮箱被偷窥和轰炸——最安全的地方并不安全.....	183
6.1	揭秘 POP3 邮箱密码探测.....	184
6.1.1	使用“流光”探测 POP3 邮箱密码.....	184
6.1.2	黑雨——POP3 邮箱密码探测器.....	186
6.2	警惕自己的 Web-Mail 用户名和密码.....	187
6.2.1	Web 上的解密高手——Web Cracker 4.0.....	187
6.2.2	获取密码的帮凶——“溯雪”Web 密码探测器.....	188
6.3	黑客的惯用伎俩——欺骗法获取用户信息.....	191
6.3.1	利用 Outlook Express 漏洞欺骗获取用户名和密码.....	191
6.3.2	利用 Foxmail 邮件欺骗获取密码大法.....	194
6.3.3	如何实现 TXT 文件欺骗.....	197
6.4	谁炸了我的电子邮箱.....	199
6.4.1	用 QuickFyre 炸弹炸邮箱真的很简单.....	199
6.4.2	可实现不间断发信的 KaBoom! 邮箱炸弹.....	199
6.4.3	如何防范邮件炸弹.....	200
6.4.4	邮件炸弹的克星——E-Mail Chomper.....	203
6.5	功能强大的邮件收发软件依然存在漏洞.....	204
6.5.1	使用 Outlook Express 让联系人地址暴露.....	204
6.5.2	Foxmail 的账户口令封锁.....	207
6.5.3	如何清除发送邮件时留下的痕迹.....	208
6.5.4	如何快速、可靠地传输自己的电子邮件.....	208
6.6	可能出现的问题与解决.....	210
6.7	总结与经验积累.....	210
第 7 章	我的 IE 浏览器被恶意攻击了——防不胜防的恶意攻击.....	213
7.1	揭开网页恶意攻击的神秘面纱.....	214
7.1.1	剖析网页攻击的恶意代码.....	214
7.1.2	并非花开绚烂的“万花谷”病毒.....	215
7.2	摆脱网页恶意代码的陷害.....	217

7.2.1	剖析 Office 宏删除硬盘文件的攻击	217
7.2.2	剖析 ActiveX 对象删除硬盘文件的攻击	219
7.2.3	如何防止硬盘文件被删除	220
7.2.4	如何清除恶毒网站的恶意代码	221
7.3	最让人心有余悸的 IE 炸弹	221
7.3.1	IE 炸弹攻击的表现形式	222
7.3.2	IE 死机共享炸弹的攻击	223
7.3.3	IE 窗口炸弹的防御	223
7.4	实现 IE 处理异常的 MIME 漏洞攻防	224
7.4.1	使用木马攻击浏览网页的计算机	224
7.4.2	对浏览网页的用户执行恶意指令攻击	226
7.4.3	如何防范 IE 异常处理 MIME 漏洞的攻击	229
7.5	破坏性极强的 IE 执行任意程序攻防	229
7.5.1	利用 chm 帮助文件执行任意程序攻击	229
7.5.2	chm 帮助文件执行任意程序的防范	231
7.5.3	利用 IE 执行本地可执行文件进行攻击	232
7.6	极易忽视的 IE 浏览泄密	233
7.6.1	IE 浏览网址 (URL) 泄密	233
7.6.2	Cookie 泄密的解决方法	234
7.6.3	Outlook Express 的查看邮件信息漏洞攻击	235
7.6.4	通过 IE 漏洞读取客户机上的文件	237
7.7	可能出现的问题与解决	238
7.8	总结与经验积累	239
第 8 章	扫描、嗅探与欺骗——必不可少的超级经典小工具	241
8.1	扫描与反扫描工具精粹	242
8.1.1	用 MBSA 检测 Windows 系统是否安全	242
8.1.2	深入浅出 RPC 漏洞扫描	245
8.1.3	个人服务器漏洞扫描的利器——WebDAVScan	245
8.1.4	用网页安全扫描器查看你的网页是否安全	246
8.1.5	防御扫描器追踪的好帮手——ProtectX	247
8.2	介绍几款经典嗅探器	248
8.2.1	用嗅探器 Sniffer Portable 捕获数据	249
8.2.2	局域网中的嗅探精灵——Iris	250
8.2.3	用嗅探器 SpyNet Sniffer 实现多种操作	252
8.2.4	能够捕获网页内容的“艾菲网页侦探”	253
8.3	看不见的管理员——谁在欺骗我们的网络	255

8.3.1	小心具备诱捕功能的蜜罐	255
8.3.2	拒绝恶意接入的“网络法官”	256
8.4	可能出现的问题与解决	259
8.5	总结与经验积累	260
第 9 章	全面飚升网络控制的权限——是否可以使自己权力更大	261
9.1	必不可少的下载限制突破	262
9.1.1	如何利用“网络骆驼”突破下载限制	262
9.1.2	使用 SWF 文件实现顺利下载	265
9.1.3	顺利下载被保护的图片	266
9.1.4	如何下载有限制的影音文件	267
9.2	是谁限制了我们的网页	269
9.2.1	右键锁定真的能够锁定吗	269
9.2.2	即使禁用了复制/保存功能也没用	269
9.2.3	网页信息解密大法	270
9.2.4	如何有效预防网页破解	271
9.3	别以为网管的限制就牢不可破	273
9.3.1	用 Sygate 突破封锁上网	273
9.3.2	手工实现网吧限制的突破	275
9.3.3	在网吧中一样可以实现下载	275
9.3.4	用导入注册表法解除网吧限制	276
9.4	让网络广告不再烦人	277
9.4.1	弹出式广告的过滤杀手——遨游 Maxthon	277
9.4.2	用广告杀手 Ad Killer 过滤网络广告	278
9.4.3	能够实现智能拦截的 Zero Popup	279
9.4.4	能够轻松使用 MSN 的 MSN Toolbar	279
9.5	可能出现的问题与解决	280
9.6	总结与经验积累	281
第 10 章	IIS 服务器被恶意攻击	283
10.1	剖析 IIS 服务器的漏洞入侵	284
10.1.1	IIS 服务器是怎样被漏洞入侵的	284
10.1.2	如何设置自己的 IIS 服务器	286
10.2	实战 Unicode 漏洞攻防	287
10.2.1	使用 RangeScan 查找 Unicode 漏洞	288
10.2.2	黑客利用 Unicode 漏洞修改目标主页揭密	289
10.2.3	黑客通过 Unicode 漏洞攻击目标主机文件揭密	290
10.2.4	利用 Unicode 漏洞进一步控制该主机	292

10.2.5	Unicode 漏洞解决方案	293
10.3	CGI 解译错误漏洞攻防	294
10.3.1	认识 CGI 漏洞检测工具	294
10.3.2	guestbook.cgi 漏洞分析	294
10.4	深度剖析.printer 缓冲区漏洞	295
10.4.1	利用 IIS5.0 的.printer 溢出漏洞实施攻击	295
10.4.2	利用.printer 的远程溢出漏洞实施攻击	298
10.5	可能出现的问题与解决	300
10.6	总结与经验积累	300
第 11 章	打好网络安全防御战——构筑自己的铜墙铁壁	303
11.1	如何防御间谍软件	304
11.1.1	轻松拒绝潜藏的间谍	304
11.1.2	用 Spybot 揪出隐藏的间谍	305
11.1.3	间谍广告的杀手——AD-aware	307
11.2	如何关闭端口和隐藏 IP	308
11.2.1	如何关闭和开启自己的端口	308
11.2.2	学会隐藏自己的 IP	309
11.2.3	对不必要的防火墙端口进行限制	312
11.2.4	通过安全策略关闭危险端口	313
11.3	网络防火墙的安装与使用	317
11.3.1	如何使用“天网防火墙”防御网络攻击	317
11.3.2	功能强大的网络安全特警 2005	324
11.3.3	黑客程序的克星——Anti Trojan Elite（反黑精英）	329
11.3.4	免费的个人网络防火墙——ZoneAlarm	331
11.4	可能出现的问题与解决	335
11.5	总结与经验积累	335

第 7 章

黑浪滔天话黑客

——例说黑客入侵与防御

本章重点:

- ◆ 功能强大的黑客工具——“冰河” 2005
- ◆ 守好那扇进出的门——IPC\$漏洞入侵与防御
- ◆ 黑客的常用伎俩——命令行下的远程控制 PsExec
- ◆ 一双偷窥的眼睛——远程开启视频木马初探
- ◆ 为你通风报信的灰鸽子

案例目标:

在本章中将着重介绍黑客的一些入侵方法与步骤,让读者掌握一些防止黑客攻击的基本技巧,以及 IPC\$漏洞入侵与防御、命令行下的远程控制 PsExec 和如何远程开启视频木马等内容。

黑客在大多数人心里，往往是魔鬼的化身。由于他们掌握着最前沿的系统和网络技术，因此他们自称为网络时代的精英；但因为他们搞破坏的力量实在是太大，所以不得不把他们和魔鬼联系到一起。

下面就一起来看看黑客必知而又威力无穷的“秘技”，不过操作起来确实十分容易，看后大概能使大家有两种感觉：一种是蠢蠢欲动，自己想动手攻击一下别人；另一种就是会觉得黑客也不过如此。好了，闲话少说，请看实例。

1.1 功能强大的黑客工具——“冰河” 2005

进行远程控制的工具很多，大多数都是称之为木马的软件。在国内影响最大的远程控制木马工具莫过于“冰河”。从某种意义上讲，“冰河”的开发者在设计之初，可能仅仅是想打造一款功能强大的远程控制软件，但十分不幸的是，“冰河”从一开始就远远偏离了这个目的，并且更为令人吃惊的是，它的诞生标志着“洋”木马一统天下局面的结束，并一度成为“木马”的代名词（国内受“冰河”木马感染的计算机多不胜数）。



【小知识】

木马，也称特洛伊木马，英文名称为 Trojan。其本身就是为了入侵个人计算机而做的，藏在计算机中和工作时是很隐蔽的，它的运行和黑客的入侵不会在计算机的屏幕上显示出任何痕迹。Windows 本身没有监视网络的软件，所以不借助其他工具软件，许多时候是很难知道木马的存在和黑客的入侵的。

1.1.1 揭开“冰河”木马的神秘面纱

“冰河”是一个基于 TCP/IP 协议和 Windows 操作系统的网络工具，所以首先应确保该协议已被安装且网络连接无误，然后配置服务器程序（如果不进行配置则取默认设置），并在欲监控的计算机上运行服务器端监控程序即可。在本节中将以经典的“冰河 v8.4”专版为例，来说明一下如何使用冰河木马，以及如何防御冰河木马。

从网上下载“冰河”软件并将其解压之后，将看到 3 个文件：G_Server.exe（服务器端程序）、G_Client.exe（客户端程序）和 Readme.txt（说明文件），如图 1-1 所示。要使用“冰河”木马，首先需要用客户端程序对服务器进行配置。



图 1-1 认清冰河的客户端与服务端



【提示】

G_Server.exe 是用来安装在别人计算机里的文件，可以任意更名，双击时没有任何反应，但其实已经悄悄地安装在计算机中了。G_Client.exe 则安装在自己的计算机中，用来监控别人的计算机。

1.1.2 配置“冰河”木马的被控端程序

服务端程序 G_Server.exe 用于被监控端后台监控程序（运行一次即自动安装，可任意改名），在安装前可以先通过 G_Client 的“配置本地服务器程序”功能进行一些特殊配置，例如是否将动态 IP 发送到指定信箱、改变监听端口、设置访问口令等。

在传输 G_Server.exe 文件前还需要对 G_Client.exe 文件进行一些配置。双击 G_Client.exe 文件，接着进行如下操作：

① 打开瑞士军刀图标的客户端 G_Client.exe，在如图 1-2 所示的主界面中单击【配置本地服务器程序】按钮。

② 在弹出的【服务器配置】对话框中选择【基本设置】选项卡，并在其中设定一个访问口令，如图 1-3 所示。

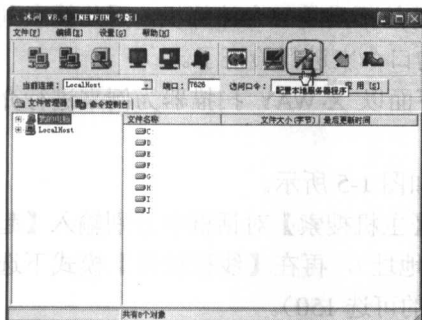


图 1-2 单击【配置本地服务器程序】按钮

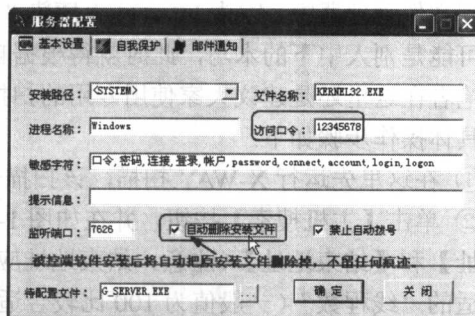


图 1-3 设定访问口令、选中“自动删除安装文件”复选框

这样，只有通过此口令才能访问到被控端的计算机，防止其他装有“冰河”控制端的用户访问。选中“自动删除安装文件”复选框，则被控端软件安装后将自动把原安装文件删除掉。

③ 选择【服务器配置】对话框中的【邮件通知】选项卡，然后输入 E-mail 地址和发送服务器，如图 1-4 所示。这样，被控端软件就可以将对方每次拨号后所产生的 IP 地址都发送到自己设定的 E-mail 中了（由于现在大多用户均采用拨号上网或动态 IP 的 ADSL 宽带上网，其每次拨号后的 IP 都不同。但进行该步设置之后，只要对方开机上网，就可以获得其 IP 并连接到其计算机上了）。

④ 在【服务器配置】对话框中还可以通过单击...按钮来选择待配置文件（一般取默认值即可），然后设置服务器端的安装路径、更改服务器的文件名、设置访问口令、进程名称、监听端口、是否写入注册表启动项、是否关联文件等。还可以设置是否将“肉鸡”的系统信息、开机口令、共享资源信息等发送到指定 E-mail。

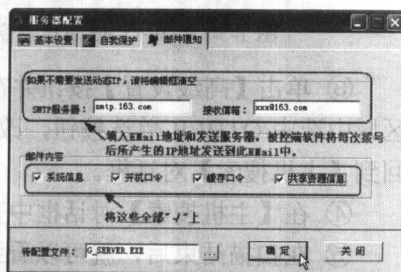


图 1-4 输入 E-mail 地址和发送服务器

⑤ 最后单击【确定】按钮，被控端软件就配置好了。当然，还有一些无关重要的选项，如果需要可以根据自己的实际情况酌情设置，如可以更改监听端口（范围在 1024~32768 之间）。

1.1.3 搜索、远控目标计算机

除从 E-mail 中得到 IP 地址外，还可以通过控制端软件进行自动搜索（当然也可以使用其他搜索工具），单击主界面中的【自动搜索】按钮，在弹出的对话框中输入起始域和起止地址，如搜索 192.168.0.1 到 192.168.0.255 之间的 IP 地址，则可以在【起始域】文本框中输入 192.168.0，在【起始地址】文本框中输入 1，【终止地址】文本框中输入 255，然后单击【开始搜索】按钮即可。

“搜索结果”框中以 OK 开头的 IP 可能就是自己要找的了，控制端软件将会自动将其添加到文件管理器中，因为 Internet 上感染“冰河”木马的不只是一台计算机，因此搜索到的很可能是别人中下的木马，此时就得根据自己设定的口令来进行验证了。

笔者在这里还是建议大家使用专用的扫描工具，下面以 X-WAY 扫描器为例来进行介绍，具体操作步骤如下：

① 在这里先运行 X-WAY 扫描，该扫描器主界面如图 1-5 所示。

② 单击【主机搜索】按钮，并在如图 1-6 所示的【主机搜索】对话框中分别输入【起始地址】和【结束地址】（注意：结束地址应大于起始地址），再在【线程设置】模式下选择合适的“线程数”（一般值为 100 比较合适，网速快的可选 150）。

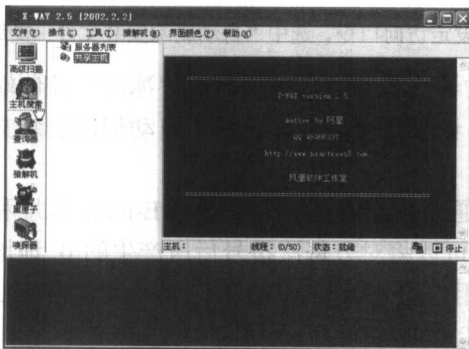


图 1-5 X-WAY 扫描器主窗口

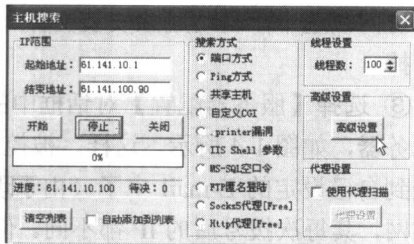


图 1-6 设置主机扫描

③ 单击【高级设置】按钮并在【主机搜索各参数设置】对话框中的【端口设置】选项区域中选中 OTHER 单选按钮，改变其值为 7626，如图 1-7 所示。然后单击【关闭】按钮回到【主机搜索】对话框。

④ 在【主机搜索】对话框中直接单击【开始】按钮即可开始扫描，如图 1-8 所示。

⑤ 在扫描结束后，就可以看到如图 1-9 所示的扫描结果了。



【提示】

为了某些特殊的缘故，笔者对本书中的个别图片会做一些技术上的处理，希