易学易用系列

新手学黑客攻防

神龙工作室　编著

人 民 邮 电 出 版 社

图书在版编目（CIP）数据

新手学黑客攻防 / 神龙工作室编著．—北京：人民邮电出版社，2007.4
（易学易用系列）

ISBN 978-7-115-15729-4

Ⅰ．新… Ⅱ．神… 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（2007）第 016451 号

内 容 提 要

本书是指导初学者快速掌握黑客攻防操作和应用的入门书籍。书中详细地介绍了初学者必须掌握的基本知识、使用方法和操作步骤，并对初学者在学习过程中经常会遇到的问题进行了专家级的指导，以免初学者在起步的过程中走弯路。全书共分 10 章，分别介绍了漫话黑客，Windows 系统中的漏洞，Windows 系统漏洞攻击的防范，信息搜集、嗅探与扫描，远程控制技术，木马的植入与查杀，QQ 攻防战，E-mail 攻防战，Web 攻防战以及防范扫描与木马攻击等内容。

本书附带一张精心开发的专业级多媒体教学光盘，它采用了全程语音讲解、情景式教学、详细的图文对照和真实的情景演示等方式，紧密结合书中的内容对各个知识点进行了深入的讲解，大大扩充了本书的知识范围。

同时在光盘中提供了 300 个经典的电脑安全防护技巧和一些重要的常见木马连接端口、常见端口服务和常见进程的介绍，相当于赠送了一本 300 页的电脑安全防护技巧大全类图书。

本书及配套的多媒体光盘主要面向黑客初级读者使用，同时也可以作为黑客攻防培训班的培训教材或者学习辅导书。

易学易用系列

新手学黑客攻防

- 编　　著　神龙工作室
  责任编辑　魏雪萍
- 人民邮电出版社出版发行　　北京市崇文区夕照寺街 14 号
  邮编　100061　　电子函件　315@ptpress.com.cn
  网址　http://www.ptpress.com.cn
  北京　　印刷厂印刷
  新华书店总店北京发行所经销
- 开本：787×1092　1/16
  印张：18.75
  字数：462 千字　　2007 年 4 月第 1 版
  印数：1 - 8 000 册　　2007 年 4 月北京第 1 次印刷

ISBN 978-7-115-15729-4/TP・5986

定价：00.00 元（附光盘）

读者服务热线：(010)67132692　印装质量热线：(010)67129223

前　言

本次推出的《易学易用》丛书是对原**全国优秀畅销书**《易学易用》丛书的全新改版，新版丛书在保留原版特点的同时又增加了许多新的特色，以满足广大读者的实际需求。

丛书主要内容

本套丛书涵盖了电脑应用的常见领域，在涉及到软硬件介绍时都以大家经常使用的版本为主要的讲述对象，在必要的地方也兼顾了软硬件的其他版本，以满足不同读者的需求。本套丛书主要包括以下图书。

《新手学电脑》	《新手学电脑家庭应用》	《新手学电脑常见问题解答》
《新手学电脑办公》	《新手学电脑办公应用》	《新手学电脑办公常见问题解答》
《新手学上网》	《新手学上网常见问题解答》	《新手学处理数码照片》
《新手学五笔打字》	《新手学修改 BIOS 与注册表》	《新手学组建局域网》
《新手学 Windows XP》	《新手学 Windows XP 常见问题解答》	《新手学使用笔记本电脑》
《新手学电脑急救与数据恢复》	《新手学电脑故障诊断与排除》	《新手学 Flash 动画制作》
《新手学电脑组装与维护》	《新手学 CorelDRAW 图形图像制作》	《新手学 Photoshop 图像处理》
《新手学安装与重装系统》	《新手学安装与卸载多操作系统》	《新手学建网站》
《新手学 Excel 制作电子表格》	《新手学 Excel 常见问题解答》	《新手学 Dreamweaver 制作网页》
《新手学 Excel 公式·函数与图表》	《新手学 PowerPoint 制作演示文稿》	《新手学制作网页常见问题解答》
《新手学移动商务办公》	《新手学 AutoCAD 辅助绘图》	《新手学黑客攻防》

写作特色一览

❖ **双栏排版、超大容量：**本书采用了双栏排版的格式，信息量大。其中本书 260 多页的篇幅容纳了传统图书 400 多页的内容。这样，我们就能在有限的篇幅内为读者奉献更多的知识和实战案例。

❖ **买一送一、物超所值：**随书光盘中附赠了 300 个经典的电脑安全防护技巧和一些重要的常见木马连接端口、常见端口服务和常见进程的介绍，相当于赠送了一本 300 页的电脑安全防护技巧大全的图书。

❖ **一步一图、以图析文：**在介绍具体操作的过程中，每一个操作步骤后均附上对应的插图，这种图文结合的方法，便于读者在学习的过程中能够直观、清晰地看到操作的效果，易于读者理解和掌握。

❖ **双色印刷、轻松阅读：**本书采用了以黑色印刷为主，而“小提示”、“小知识”等重要知识点图标则采用红色印刷。这样，既美观大方，又突出重点、难点。

❖ **书盘结合、互动教学：**本书配套多媒体教学光盘内容与书中知识紧密结合并互相补充，大大扩充了本书的知识范围。

配套光盘扫描

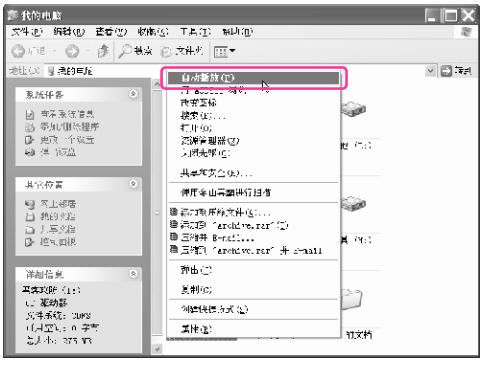
本书的配套光盘是一张精心开发的专业级多媒体教学光盘，它采用了全程语音讲解、情景式教学、详细的图文对照和真实的情景演示等方式，紧密结合书中的内容，对各个知识点

此为试读，需要完整PDF请访问：www.ertongbook.com

进行深入讲解的同时又做了一定的扩展延伸。

❖ 光盘自动运行

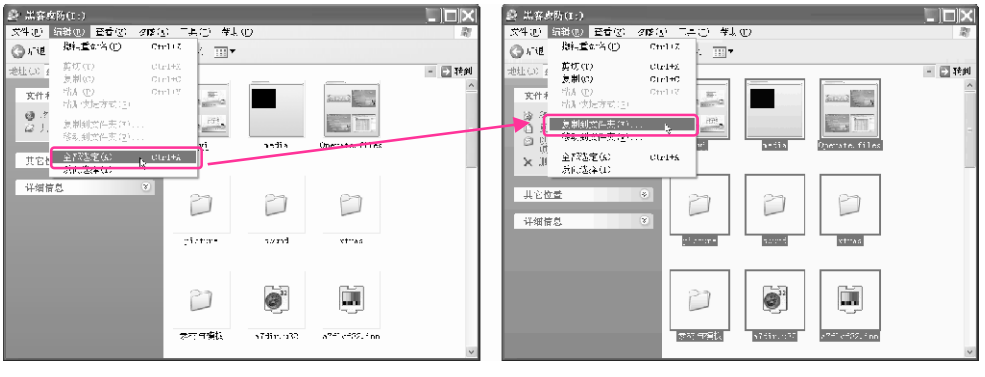
1. 将光盘印有文字的一面朝上放入光驱中，几秒钟后光盘就会自动运行。
2. 若光盘没有自动运行，则可双击桌面上的【我的电脑】图标打开【我的电脑】窗口，然后双击光盘图标，或者在光盘图标上单击鼠标右键，从弹出的快捷菜单中选择【自动播放】菜单项，光盘就会运行。



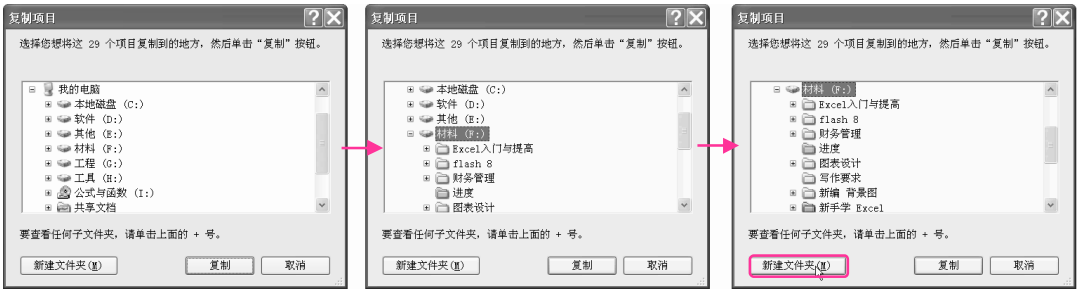
❖ 在硬盘上运行

1. 将光盘放入光驱中，如果光盘自动运行，则需要先在主界面中单击【退出】按钮退出，否则直接进入第2步。
2. 双击桌面上的【我的电脑】图标打开【我的电脑】窗口，然后在光盘图标上单击鼠标右键，从弹出的快捷菜单中选择【打开】菜单项打开【黑客攻防】光盘。

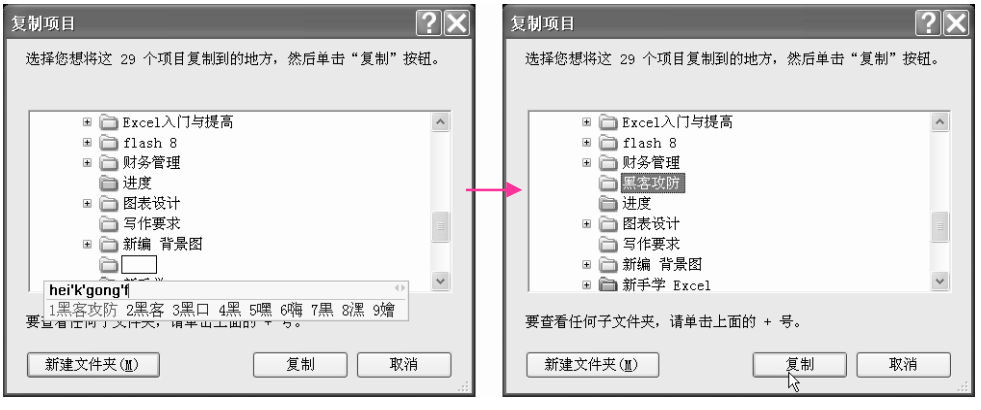
3. 选择【编辑】➢【全部选定】菜单项，然后选择【编辑】➢【复制到文件夹】菜单项。



4 在弹出的【复制项目】对话框中选中【材料（F:）】，然后单击 新建文件夹(M) 按钮。



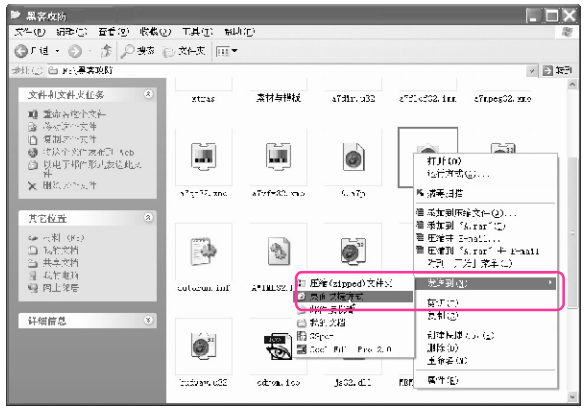
5 在文本框中输入“黑客攻防”（也可以输入英文字母），输入完后按回车键。选中【黑客攻防】文件夹，然后单击 复制 按钮即可将光盘内容复制到 F 盘的【黑客攻防】文件夹中了。



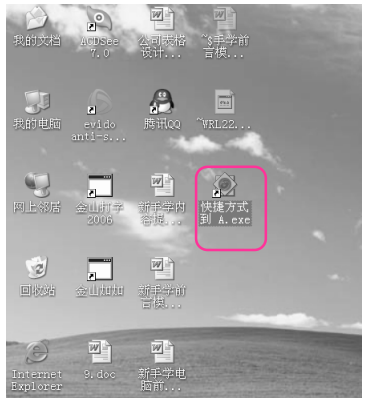
6 从【我的电脑】中打开 F 盘中的【黑客攻防】文件夹，选择【工具】➢【文件夹选项】菜单项，在打开的【文件夹选项】对话框中切换到【查看】选项卡，然后撤选【隐藏已知文件类型的扩展名】复选框（即去掉左侧的对勾）。

7 单击 确定 按钮关闭【文件夹选项】对话框。

8 将鼠标移到 A.exe 文件上单击鼠标右键，从弹出的快捷菜单中选择【发送到】➢【桌面快捷方式】菜单项。



9 关闭【黑客攻防】文件夹窗口。现在桌面上就多了一个 A.exe 的快捷方式图标，以后不用插光盘而直接双击这个快捷方式图标就可以观看多媒体教学内容了。



本书由神龙工作室编著，参与资料收集和整理工作的有王耀东、高秀英、辛全华、蔡玉冬、姜永水、张相红、徐晓丽、刘淑珍、王福艳、宋真真、辛令霞、骆建玲、李轶君、侯军兰、宫明文、姜惠翠等。由于时间仓促，书中难免有疏漏和不妥之处，恳请广大读者不吝批评指正。

我们的联系信箱：zhiyin101@tom.com。

另外，网站 http://www.shenlongs.cn 将提供全面的技术支持。

编者

目　录

第 1 章　漫话黑客……1

1.1　揭开黑客的神秘面纱……2
1.2　认识 IP 地址……3
1.2.1　什么是 IP 地址……3
1.2.2　IP 地址的划分……3
1.3　黑客的专用通道——端口……4
1.3.1　端口的分类……4
1. 按端口号分布划分……4
2. 按协议类型划分……5
1.3.2　查看端口……6
1.3.3　关闭/开启端口……6
1. 关闭端口……7
2. 开启端口……8
3. 限制端口的方法……8
1.4　黑客常用的命令……9
1.4.1　ping 命令……10
1.4.2　net 命令……11
1. 工作组和域……11
2. net 命令介绍……12
1.4.3　telnet 命令……17
1. 常用的 telnet 命令……17
2. 使用 telnet 命令登录远程计算机……18
1.4.4　ftp 命令……18
1.4.5　netstat 命令……20
1.4.6　其他命令……21
1. tracert 命令……21
2. ipconfig 命令……21
3. route 命令……22
4. netsh 命令……23
5. arp 命令……25

第 2 章　Windows 系统中的漏洞……27

2.1　Windows 系统的安全隐患……28
2.1.1　Windows 系统的漏洞产生原因……28
2.1.2　Windows 系统中的安全隐患…28
1. Windows 操作系统中的安全隐患……28
2. Windows 系统中的 bug……30
2.2　Windows 操作系统中的漏洞……31
2.2.1　Windows 98 中的漏洞……31
1. IGMP 漏洞……31
2. 系统文件检查器漏洞……31
3. 共享密码校验漏洞……31
4. 共享访问客户端类型检测漏洞……32
5. 共享服务文件句柄漏洞……32
6. NetBIOS over TCP/IP 耗尽资源漏洞……32
7. NetBIOS 漏洞……32
8. 屏幕保护程序漏洞……33
2.2.2　Windows 2000 中的漏洞……33
1. 输入法漏洞……33
2. Unicode 漏洞……33
3. ISAPI 缓冲区扩展溢出漏洞…34
4. MS SQL Server 的 SA 空密码漏洞……34
5. 系统管理权限漏洞……34
6. 路径优先漏洞……35
7. NetDDE 消息权限提升漏洞…35
8. RDP 拒绝服务漏洞……35
9. 域控制器拒绝服务漏洞……36
10. 事件查看器存在缓冲区溢出·36
11. UDP 套接字拒绝服务漏洞…36
12. 安全账户管理漏洞……36
13. IIS 5.0 的 HTR 映射远程堆溢出漏洞……36
14. IIS5.0 的 ASP 缓冲溢出漏洞……37
15. Narrator 本地密码信息泄露漏

此为试读，需要完整PDF请访问：www.ertongbook.com

洞……37
16. SMTP 认证漏洞……37
17. IIS 5.0/5.1 验证漏洞……37
18. SQL Server 的函数库漏洞……37
19. IIS5.0 伪造拒绝服务漏洞……38
20. 调试寄存器漏洞……38
21. drwtsn32.exe 文件漏洞……38
22. 快捷方式漏洞……38
23. UTF 漏洞……39
24. IIS 5.0 SEARCH 方法远程攻击漏洞……39
25. LDAP 漏洞……39
26. IIS5.0 拒绝服务漏洞……39
27. Telnet 漏洞……39
28. 登录服务恢复模式空密码漏洞……40
29. 默认注册许可漏洞……40
30. 域账号锁定漏洞……40
31. 终端服务器登录缓存溢出漏洞……41
32. ActiveX 参数漏洞……41
33. IIS5.0 Cross-Site Scripting 漏洞……41
34. 组策略漏洞……41
35. 数字签名缓冲区溢出漏洞……41
36. ActiveX 控件漏洞……42
37. SMB 漏洞……42
38. 网络连接管理器漏洞……42
2.2.3 Windows XP 系统中的漏洞……42
1. UPNP 服务漏洞……42
2. 升级程序漏洞……43
3. 帮助和支持中心漏洞……43
4. 压缩文件夹漏洞……43
5. 服务拒绝漏洞……43
6. Windows Media Player 漏洞……44
7. RDP 漏洞……44
8. VM 漏洞……44
9. 热键漏洞……44
10. 账号快速切换漏洞……45
2.3 黑客常用的入侵方式……45
1. 数据驱动攻击……45
2. 系统文件非法利用……45
3. 伪造信息攻击……45
4. 针对信息协议弱点攻击……45
5. 远端操纵……45
6. 利用系统管理员失误攻击……46
7. 重新发送（REPLAY）攻击……46
8. 对 ICMP 报文攻击进行……46
9. 针对源路径选项的弱点攻击……46
10. 以太网广播攻击……46
11. 跳跃式攻击……46
12. 窃取 TCP 协议连接……46
13. 夺取系统控制权……47
2.4 个人电脑安全防护策略……47
1. 杀（防）毒软件不可少……47
2. 个人防火墙不可替代……47
3. 分类设置复杂密码……47
4. 防止网络病毒与木马……47
5. 警惕“网络钓鱼”……48
6. 防范间谍软件……48
7. 只在必要时共享文件夹……48
8. 不要随意浏览黑客网站和非法网站……48
9. 定期备份重要数据……48
第 3 章 Windows 系统漏洞攻击的防范……49
3.1 设置好组策略的安全登录……50
3.1.1 组策略的含义和作用……50
1. 什么是组策略……50
2. 组策略的版本……50
3. 在 Windows 中运行组策略……50
4. 组策略中的管理模板……51
3.1.2 重命名默认账户……52
3.1.3 账户锁定策略……53
3.1.4 密码策略……54
3.1.5 隐藏桌面上的系统图标……55
3.1.6 设置用户权限……55
3.1.7 其他策略……56
1. 禁止更改桌面设置……56
2. 禁止访问【控制面板】……56

3. 防止用户使用【添加或删除程序】……57
4. 禁止更改【开始】菜单和任务栏……57
5. 限制使用应用程序……58
3.2 用好你的注册表……59
3.2.1 禁止访问和编辑注册表……59
3.2.2 设置注册表防止系统隐私信息被泄露……62
3.2.3 在注册表中关闭默认共享保证系统安全……62
1. 防范 IPC$攻击……62
2. 修改注册表关闭默认共享……63
3.2.4 略施小计吓跑不怀好意的菜鸟……63
3.2.5 修改系统注册表防止 SYN 洪水攻击……64
3.2.6 驱除系统中的随机启动木马……66
1. 斩除注册表中的自启动木马…66
2. 检查系统配置文件……66
3.2.7 设置 Windows 的自动登录……68
3.2.8 用注册表清除恶意代码……69
3.3 密码与加密……71
3.3.1 设置 Windows XP 的登录密码……71
3.3.2 电源管理密码设置……72
3.3.3 屏幕保护程序密码的设置和破解……73
1. 设置屏幕保护程序密码……73
2. 破解……73
3. 保护自己的屏幕保护程序……74
3.4 Windows XP 的安全设置……76
3.4.1 充分利用防火墙功能……76
3.4.2 网络初始化……77
3.4.3 利用 IE6.0 来保护个人隐私……78
3.4.4 封闭网络中的 NetBIOS 和 SMB 端口……79
3.4.5 利用加密文件系统加密……79
3.4.6 其他安全设置……79
1. 屏蔽不需要的服务组件……79
2. 锁定计算机……80
第 4 章 信息搜集、嗅探与扫描……81
4.1 搜索网络中的重要信息……82
4.1.1 获取目标主机的 IP 地址……82
4.1.2 由 IP 地址获取目标主机的地理位置……82
1. WHOIS 服务页面……82
2. IP 探索者网站……83
4.1.3 了解网站备案信息……83
4.2 检测系统漏洞……85
4.2.1 什么是扫描器……85
1. 什么是扫描器……85
2. 扫描器的工作原理……85
3. 扫描器能干什么……85
4.2.2 搜索共享资源……85
1. 使用工具 IPScan……85
2. 使用局域网查看工具……86
4.2.3 全能搜索利器 LanExplorer……88
4.2.4 使用 MBSA 检测系统安全性…91
1. MBSA 的下载与安装……91
2. 扫描单台计算机……93
3. 扫描多台计算机……97
4. 选择/查看安全报告……99
5. MBSA 使用注意事项……99
4.3 端口扫描……100
4.3.1 端口扫描的原理与分类……100
1. 端口扫描的原理……100
2. 端口扫描的分类……101
4.3.2 端口扫描工具 X-Scan……102
4.3.3 扫描器 SuperScan 使用指南…108
1. 域名（主机名）和 IP 相互转换……109
2. ping 功能的使用……111
3. 端口检测……111
4.4 嗅探器的应用……115
4.4.1 嗅探器简介……115
4.4.2 看不见的网管专家 Sniffer Portable……115
1. 捕获面板……116

2. 捕获过程报文统计……116
3. 捕获报文查看……117
4. 设置捕获条件……118
5. 编辑报文发送……120
4.4.3 网络间谍软件——CaptureNet……121
1. CaptureNet 的安装……122
2. CaptureNet 的基本使用……122
3. 过滤器设置……123
4.4.4 监控利器——艾菲网页侦探……125
4.4.5 浅谈 Sniffer 的原理与防范……127
1. Sniffer 的原理……127
2. Sniffer 的防范……127

第 5 章 远程控制技术……129

5.1 基于认证入侵……130
5.1.1 IPC$入侵……130
1. 什么是 IPC……130
2. 什么是 Windows 系统的默认共享……130
3. 使用 IPC$进行入侵……130
4. 关于 IPC$空连接漏洞……132
5. IPC$漏洞入侵的防范……132
5.1.2 Telnet 简介……135
1. 什么是 Telnet……135
2. Telnet 可以用来做什么……135
3. 关于 NTLM 验证……135
4. 使用 Telnet 登录……135
5.1.3 Telnet 入侵……136
5.2 利用注册表入侵……139
5.2.1 修改注册表实现远程监控……139
5.2.2 开启远程注册表服务……140
5.2.3 通过注册表开启终端服务……141
5.3 远程监视与控制……142
5.3.1 局域网内我做主——网络执法官……143
1. 网络执法官的功能……143
2. 网络执法官的安装……144
3. 网络执法官的基本功用……144
4. 网络执法官的使用……147
5.3.2 实用小工具——WinVNC……151
5.3.3 使用 QuickIP 进行多点控制……152

第 6 章 木马的植入与查杀……157

6.1 什么是木马……158
6.1.1 木马的定义与结构……158
1. 木马的定义……158
2. 木马的结构……158
6.1.2 木马的特征……158
1. 隐蔽性……158
2. 自动运行性……159
3. 欺骗性……159
4. 自动恢复功能……159
5. 能自动打开特别的端口……159
6. 功能的特殊性……159
6.1.3 木马的种类……159
1. 远程控制木马……159
2. 密码发送木马……159
3. 键盘记录木马……160
4. 破坏性质的木马……160
5. DoS 攻击木马……160
6. 代理木马……160
7. FTP 木马……160
8. 程序杀手木马……160
9. 反弹端口型木马……160
6.1.4 木马常用的入侵手法……161
1. 在 win.ini 文件中加载……161
2. 在 system.ini 文件中加载……161
3. 在 Winstart.bat 中启动……161
4. 启动组……161
5. *.INI……161
6. 修改文件关联……161
7. 捆绑文件……162
6.1.5 揭露木马的伪装手段……162
1. 修改图标……162
2. 捆绑文件……162
3. 出错显示……162
4. 定制端口……162
5. 木马更名……162

6. 扩展名欺骗……162
7. 自我销毁……163
6.1.6 火眼金睛识木马……163
6.1.7 防范木马的入侵……164
1. 不要执行任何来历不明的软件……164
2. 谨慎使用自己的邮箱……164
3. 不要轻信他人……164
4. 不要随便留下自己的个人资料……164
5. 养成良好的网络道德……164
6. 不要随便下载软件……164
7. 最好使用第三方邮件程序……164
8. 不要轻易打开不明附件和链接……165
9. 始终显示 Windows 文件的扩展名……165
10. 尽量少用共享文件夹……165
11. 给电子邮件加密……165
12. 隐藏 IP 地址……165
13. 运行反木马实时监控程序…165
6.2 木马的捆绑生成……165
6.2.1 使用 Exebinder 捆绑木马……165
6.2.2 免杀捆绑器……166
1. 可以设置属性的捆绑器……166
2. 图标欺骗捆绑器……167
6.2.3 网页木马生成器……168
6.3 监视你的一举一动——远程控制任我行……169
6.3.1 远程控制任我行的功能……169
6.3.2 配置远程控制任我行……169
6.3.3 植入木马……173
6.3.4 监视并控制远程计算机……173
6.4 黑客的首选工具——“冰河”木马……179
6.4.1 “冰河”木马功能简介……179
6.4.2 配置“冰河”木马的服务端程序……180
6.4.3 使用“冰河”木马控制远程计算机……181
6.4.4 卸载和清除“冰河”木马……186
1. 使用控制端程序卸载……186
2. 清理注册表……186
3. 使用“冰河陷阱”……187
6.5 “广外女生”木马……189
6.5.1 “广外女生”功能简介……189
6.5.2 配置“广外女生”服务端程序……189
6.5.3 使用“广外女生”进行远程控制……191
1. 获取 IP……191
2. 进行远程控制……192
6.5.4 清除“广外女生”木马……195
第 7 章 QQ 攻防战……197
7.1 QQ 的常用攻击方式……198
1. 利用炸弹攻击……198
2. 获得对方 QQ 密码……198
7.2 本地侵犯 QQ 使用者的方式……199
7.2.1 使用“聊天记录查看器”查看聊天记录……199
7.2.2 破解本地 QQ 密码软件……199
1. QQ 破密使者……200
2. 用“QQ 眼睛”获取 QQ 号及密码……200
7.3 远程攻击 QQ 方式……201
7.3.1 强制聊天……201
7.3.2 使用“狙击手 IpSniper”进行 IP 探测……202
7.4 保护好自己的 QQ……204
7.4.1 防止 QQ 密码被破译……204
7.4.2 防范 IP 地址被探测……205
7.4.3 防范 QQ 炸弹和木马……206
第 8 章 E-mail 攻防战……207
8.1 获取 E-mail 密码的方式……208
8.1.1 使用流光软件探测 E-mail 账号与密码……208
8.1.2 使用“溯雪 Web 密码探测器”获取邮箱密码……210

此为试读，需要完整PDF请访问：www.ertongbook.com

8.1.3 使用“Web Cracker4.0”获取 Web 邮箱密码……211
8.1.4 使用“黑雨”软件暴力破解邮箱密码……212
8.1.5 使用“E-mail 网页神抓”获取 E-mail 网页地址……213
8.2 常见 E-mail 攻击手段与防范……214
8.2.1 使用邮箱炸弹进行攻击……214
8.2.2 对付邮箱炸弹及病毒的方法……215
1. 防止邮箱被炸……215
2. 防范邮箱病毒的侵袭……217
8.3 E-mail 的前景……217

第 9 章 Web 攻防战……219

9.1 什么是恶意代码?……220
9.1.1 恶意代码的特征……220
9.1.2 非过滤性病毒……220
9.1.3 恶意代码的传播方式和传播趋势……221
1. 恶意代码的传播方式……221
2. 恶意代码的传播趋势……221
9.2 恶意代码对注册表的侵袭……222
9.2.1 自动弹出网页和对话框……222
1. 通过注册表清除弹出的网页……222
2. 通过注册表清除弹出的对话框……222
3. 利用杀毒软件……223
9.2.2 浏览网页注册表被禁用……223
9.2.3 IE 标题栏、默认首页被强行修改……224
1. 对标题栏的修改……224
2. 对默认主页的修改……224
9.2.4 IE 查看“源文件”被禁用……224
9.3 危险的浏览器……225
9.3.1 IE 炸弹攻击类型、后果……225
9.3.2 对网页炸弹的防范与补救……227
9.4 Web 攻击与防范举例……228
9.4.1 常见 ASP 脚本攻击与防范……228
9.4.2 跨站 Script 攻击和防范……229
1. 跨站 Script 的攻击……229
2. 防范措施……230
9.5 让 IE 浏览器更安全……230
9.5.1 莫要进入“万花谷”……230
1. 巨大的破坏性……230
2. 对此类破坏的防范和修复……231
9.5.2 防止 IE 浏览器网址泄密……231
9.5.3 清除网络实名……232
9.5.4 屏蔽各种广告……233

第 10 章 防范扫描与木马攻击……235

10.1 保护好自己的 IP 和端口……236
10.1.1 设置代理服务器……236
10.1.2 关闭端口……237
1. 查找开放的端口……237
2. 关闭端口……237
10.1.3 配置安全策略保护端口……239
10.2 驱逐间谍软件……244
10.2.1 使用 Ad-aware 驱逐间谍软件……244
10.2.2 反间谍高手——安博士……245
10.3 木马清除软件……247
10.3.1 使用【Windows 进程管理器】管理进程……247
10.3.2 使用“超级兔子”清除木马……250
1. 超级兔子清理王……250
2. 超级兔子 IE 修复专家……251
3. 使用超级兔子保护自己的 IE……251
10.3.3 使用 Trojan Remover 清除木马……253
10.3.4 使用 360 安全卫士维护系统安全……255
1. 查杀恶意软件……255
2. 卸载多余插件……256
3. 查杀病毒……257
4. 修复 IE 浏览器……257

5. 修复系统漏洞……257
6. 修复 LSP 连接……257
7. 全面诊断……258
8. 使用工具清理系统……258
附录 电脑安全防护技巧……259

第 1 章
漫话黑客

在今天，互联网在人们的生活、学习和工作等许多方面起着举足轻重的作用，人们已经无法离开网络。然而与此同时，网络的安全问题也随之凸现。在网络世界中有一类神秘的人物，有的时候他们会义务维护着网络的安全，有的时候却又以网络破坏者和大盗的面目出现，这就是黑客。本章将揭开黑客的神秘面纱，并对与他们有关的常用的知识进行初步的介绍。

要点导航

- 揭开黑客的神秘面纱
- 认识 IP 地址
- 黑客的专用通道——端口
- 黑客常用的命令

1.1 揭开黑客的神秘面纱

一提起黑客，人们总感到他们身上带有一种神秘的色彩，仿佛这些人是不可琢磨、难以接近的高超人物。黑客是一个什么样的角色？他们从事什么样的活动？黑客也许是网络里沿着庞杂的线路潜行的杀手，也许是在攻入用户的系统后提醒用户其系统漏洞所在并留下建议便悄然离去的侠士；也许是一位声名显赫的大人物，也许只是一个初显锋芒的少年……。

黑客又称骇客，是英文单词 Hacker 一词的中文音译。他们进行黑客活动的理由往往都非常简单，正如“Hack”一词的引申含义为“干了一件漂亮的工作”那样，许多人只是为了炫耀一下自己的计算机技巧而已，或者开一些善意的玩笑。如今黑客俨然成了一些人自我炫耀的一个头衔。随着计算机的普及、网络的流行和黑客工具的传播，一些人会使用简单的工具对一些疏于防范的电脑进行攻击并进行破坏，这就不再属于“黑客”的范畴，而是属于犯罪活动了。在日常生活中，许多计算机故障都是出自黑客之手，例如某些网站无法访问，在 ATM 机上提款失败，等等。

黑客的原意是指那些精通操作系统和网络技术、并利用其专业知识编制新程序的人。这些人往往都掌握有非凡的计算机技术和网络知识，除了无法通过正当的手段物理性地破坏他人的计算机和帮助他人重装操作系统外，其他的几乎绝大部分的电脑操作他们都能通过网络做到，例如将别人的计算机当做跳板盗取其他计算机内的文件、造成别人的计算机崩溃、格式化磁盘、监视他人计算机或者偷窥他人隐私、远程控制他人计算机、入侵网站服务器替换该网站的主页、下载用户数据库造成商业损失、攻击网站服务器使其无法被用户访问等。了解了上面的内容，现在对“黑客”这个词应该不会感到陌生了吧。黑客技术现在已经逐渐地被越来越多的人掌握和发展。目前世界上有许多黑客网站，这些站点都会介绍一些常用的攻击方法和系统的一些漏洞，并免费提供攻击软件供网友下载和使用，这样系统和站点遭受普通网民攻击的可能性就变大了。但是黑客技术同时又是一把双刃剑，我们了解了常用的黑客技术，就可以更好地保护自己的计算机不被恶意攻击。

在网络发展的初期，网络方面的立法都还不够健全，黑客在法律的漏洞下可以为所欲为。目前各国法律的发展速度还远远地落后于互联网的发展速度，在黑客活动转入地下以后其攻击的隐蔽性更强，使得当前的法律和技术还缺乏针对网络犯罪的卓有成效的反击和跟踪的手段，无规范的黑客活动已成为网络安全的重要威胁。

黑客是一种技术上的行家或热衷于解决问题、克服限制的人。在精神上，黑客们并不单指这种软件 hacker 的文化，在任何一种科学或艺术的最高境界，用户都可以发现 hacker 的特质。他们有自己的处事态度：解决问题并创造新东西，相信自由并自愿地互相帮助。他们有自己的精神：

1. 这世上充满着等着被解决的迷人问题。
2. 没有任何人必须一再地解决同一个问题。
3. 无聊而单调的工作是有害的。
4. 自由才好。
5. 态度并非不等效于能力。

随着黑客们素质的不断提高，一些默认的规则开始在真正的黑客之间流行并被遵守：

1. 不恶意地破坏任何系统，恶意破坏他人的软体将要负法律责任。千万不要破坏别人的软体或资料。
2. 不修改任何的系统档，如果是为了要进入系统而修改它，在达到目的后要将其改回原状。
3. 不要轻易地将你要 Hack 的站点告诉你不信任的朋友。

4 不要在 BBS 上谈论你的任何黑客行为。
5 在 Post 文章的时候不要使用真名。
6 正在入侵的时候不要随意地离开你的电脑。
7 不要侵入或破坏政府机关的主机。
8 不在电话中谈论你的任何黑客行为。
9 将你的笔记放在安全的地方。
10 想要成为黑客就要成为真正的“Hacking”，应读遍所有的有关系统安全或系统漏洞的文件。
11 已侵入电脑中的账号不得清除或修改。
12 不得修改系统档案，如果为了隐藏自己的侵入而做的修改则不在此限，但仍需维持原来系统的安全性，不得因得到系统的控制权而将门户大开。
13 不将已破解的账号分享给你的朋友。

1.2 认识 IP 地址

在现实生活中，每个人都有一个名字，一个人可能有多个名字，多个人也有可能使用一个相同的名字。Internet 中的网络主机也是这样，可以使用域名来为其命名。因此在网络上能够真正标识主机的便是 IP 地址。在网络连通的情况下，只要利用域名或者 IP 地址都是可以找到目标主机的，因此如果想要攻击某个网络主机，就要首先确定该目标的域名或者 IP 地址。

1.2.1 什么是 IP 地址

所谓 IP 地址就是一种主机编址方式，给每个连接在 Internet 上的主机分配的一个 32bit（比特）地址，也称为网际协议地址。

按照 TCP/IP（Transport Control Protocol/Internet Protocol，传输控制协议/Internet 协议）协议的规定，IP 地址用二进制来表示，每个 IP 地址长 32bit，bit 换算成字节就是 4 个字节。例如一个采用二进制形式的 IP 地址是“00001010000000000000000000000001”，这么长的地址人们处理起来会很费劲。为了方便人们的使用，IP 地址经常被写成十进制的形式，中间使用符号“.”分开不同的字节，这样就可以用 XXX.XXX.XXX.XXX 的形式来表现，每组 XXX 代表小于等于 255 的 10 进制数，例如 202.96.155.8。IP 地址的这种表示方法称为“点分十进制表示法”，这显然比二进制的 1 和 0 容易记忆。

或许有人认为一台计算机只能有一个 IP 地址，这种观点是错误的。我们可以指定一台计算机具有多个 IP 地址，因此在访问互联网时，不要以为一个 IP 地址就是一台计算机；另外通过特定的技术，也可以使多台服务器共用一个 IP 地址，这些服务器在用户看起来就像是一台主机。

1.2.2 IP 地址的划分

互联网中的每个接口都必须有一个惟一的 IP 地址，该地址并不采用平面形式的地址空间，例如 1、2、3 等。IP 地址具有一定的结构，一般情况下 IP 地址可以分为 5 大类。

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

在 A 类中，第一个段为网络位，后 3 段为主机位，其范围为 1～127，如 127.255.255.255；在 B 类中，前两段为网络位，后两段为主机位，其范围为 128～191，如 191.255.255.255；在 C 类中，前 3 段为网络位，后 1 段为主机位，其范围为 192～223，如 223.255.255.255；D 类用于多播，也叫组播地址，不能在互联网上作为接点地址使用，其范围为 224～239，如 239.255.255.255；E 类用于科学研究，也不

能在互联网上使用，其范围为 240～254。

需要注意的是：全 0 和全 1 的 IP 地址都不能使用，因为全 0 代表的是本网络，全 1 是广播地址（现在在 CISCO 上可以使用全 0 地址）。一般常用的为 A、B、C 这 3 类地址。

1.3 黑客的专用通道——端口

随着计算机网络技术的发展，原来物理上的接口（如键盘、鼠标、网卡、显示卡等输入/输出接口）已不能满足网络通信的要求，而 TCP/IP 协议作为网络通信的标准协议就解决了这个通信难题。TCP/IP 协议集成到操作系统的内核中，这就相当于在操作系统中引入了一种新的输入/输出接口技术，因为在 TCP/IP 协议中引入了一种称为“Socket（套接字）”的应用程序接口。有了这样一种接口技术，一台计算机就可以通过软件的方式与任何一台具有 Socket 接口的计算机进行通信。端口在计算机编程上也就是“Socket 接口”。简言之，端口就是计算机与外界通信交流的出口。

1.3.1 端口的分类

有了这些端口后，这些端口又是如何工作的呢？例如一台服务器为什么可以同时是 Web 服务器，也可以是 FTP 服务器，还可以是邮件服务器，等等？

在网络传输中，各种服务采用不同的端口分别提供不同的服务。例如通常情况下，TCP/IP 协议规定 Web 采用 80 号端口，FTP 采用 21 号端口等；而邮件服务器则采用 25 号端口。这样通过不同的端口，计算机就可以与外界进行互不干扰的通信。

根据分析，服务器端口数最大可以有 65535 个，但是实际上常用的端口才几十个，由此可以看出未定义的端口相当多。这就是那么多黑客程序都可以采用某种方法，定义出一个特殊的端口来达到入侵目的的原因所在。为了定义出这个端口，就要依靠某种程序在计算机启动之前自动地加载到内存，强行控制计算机打开那个特殊的端口。这个程序就是“后门”程序，也就是常说的木马程序。简单地说，这些木马程序在入侵之前先通过某一种手段在一台个人计算机中植入一个程序，打开某个（些）特定的端口，俗称“后门”（BackDoor），使这台计算机变成一台开放性极高（用户拥有极高权限）的 FTP 服务器，然后从后门就可以达到入侵的目的。

端口分为硬件端口和软件端口两种，其中硬件端口又称为接口，它分为串行和并行接口。串行接口有 USB、COM 和 IEEE 1394 等，最早的串行接口是 RS-232；而我们平常使用的打印机接口就是并行接口。软件接口一般是指网络中面向连接服务和无连接服务的通信协议。

在网络技术中，端口（Port）大致有两种意思：一是物理意义上的端口，例如 ADSL Modem、集线器、交换机、路由器等用于连接其他的网络设备的接口，例如 RJ-45 端口、SC 端口等；二是逻辑意义上的端口，一般是指 TCP/IP 协议中的端口，端口号的范围从 0 到 65535，例如用于浏览网页服务的 80 端口，用于 FTP 服务的 21 端口等。下面要讲述的就是逻辑意义上的端口。

逻辑意义上的端口有多种分类标准，常见的分类标准有以下两种。

1. 按端口号分布划分

按端口号分布划分可以分为“公认端口”、“注册端口”以及“动态和/或私有端口”等。

公认端口

公认端口（Well Known Ports）也称为“常用端口”。这类端口的端口号从 0 到 1023，它们紧密地绑定于一些特定的服务。通常这些端口的通信明确地表明了某种服务的协议，这种端口不可再重新定义它的作用对象。例如 21 端

此为试读，需要完整PDF请访问：www.ertongbook.com