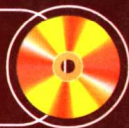


Hacker Mission and Protection for Windows on Internet
本书详细讨论在 Internet 上 Windows 计算机的各种黑客入侵手法与有效防护



北京希望电子出版社 总策划
程秉辉 John Hawke 编 著

黑客任务实战

Windows 全攻略

- * 最详尽的 Windows 入侵完整流程与攻防操作
- * 磁盘共享密码破解全攻略
- * 远程查看、编辑他人电脑中的注册表 (Registry)
- * 如何在他人计算机创建 Telnet 后门
- * 电子信箱、Web-Mail、FTP 密码破解全攻略
- * 获取与查看他人在各种邮件程序中的信件
- * 截取他人一般信箱与 Web-Mail 的信件
- * 直接发信到对方信箱，不必使用发信服务器
- * MS-Word、Excel、Access...各版本密码破解全攻略
- * ZIP、RAR、ACE、ARJ 压缩文件密码破解全攻略
- * ICQ 与 OICQ 密码、好友名单、聊天记录...攻防操作
- * 邮件、ICQ、OICQ 找出他人 IP 地址详细操作
- * 附全球 IP 详细列表、端口列表说明

本书中所有操作都经过多次的严格测试，绝不告诉你无法做到的方法！

“很强的可操作性，结构上标新立异，相当的人性化。”

计算机应用文摘



北京希望电子出版社
Beijing Hope Electronic Press
www.bhp.com.cn

“十五”国家重点电子出版物规划项目·计算机网络技术和网络教室系列

Hacker's Mission and Protection for Windows on Internet
本书详细讨论在 Internet 上 Windows 计算机的各种黑客入侵手段



北京希望电子出版社 总策划
程秉辉 John Hawke 编 著

黑客任务实战

Windows全攻略

- * 最详尽的 Windows 入侵完整流程与技巧
 - * 磁盘共享密码破解全攻略
 - * 远程查看、编辑他人电脑中的注册表
 - * 如何在他人计算机创建 Telnet 后门
 - * 电子信箱、Web-Mail、FTP 密码破解
 - * 获取与查看他人在各种邮件程序中的邮件
 - * 截取他人一般信箱与 Web-Mail 的信箱
 - * 直接发信到对方信箱，不必使用发信程序
 - * MS-Word、Excel、Access...各版本密码
 - * ZIP、RAR、ACE、ARJ 压缩文件密码破解
 - * ICQ 与 OICQ 密码、好友名单、聊天记录
 - * 邮件、ICQ、OICQ 找出他人 IP 地址与姓名
 - * 附全球 IP 详细列表、端口列表说明
- 本书中所有操作都经过多次的严格测试，绝不告诉你无法做到的方法！

电脑——以用为本！

计算机应用文摘

“很强的可操作性，结构上标新立异，相当的人性化。”



北京希望电子出版社
Beijing Hope Electronic Press
www.bhp.com.cn

内 容 简 介

黑客任务实战系列推出两年以来广受读者的支持与爱护,由于各种黑客技巧也是随着时间而不断更新,因此本书对 Windows 的入侵攻略与防护进行彻底的整理与翻修,加入了最新、最酷的黑客技巧与攻防,并提供更新、更方便的各种黑客工具,希望能帮助你充分了解黑客的各种手法与行为。同时,针对这些黑客手法也提出有效的防护方式,让你的电脑不再成为黑客下手的目标。

本书中告诉你最完整详尽的 Windows 入侵流程与操作,还包含操作时可能遇到的各种状况与注意事项,让你不必具备丰富的网络知识与经验就可以轻而易举的实现各项黑客任务。黑客入侵他人电脑后会对那些文件或数据有兴趣?如何查看各种邮件程序的信件内容?破解各版本 MS-Office 文件、各种压缩文件(ZIP、RAR、ACE、ARJ)的密码?找出 ICQ、OICQ 密码、好友名单、聊天记录?破解电子信箱、Web-Mail 密码?获取 FTP 帐户与密码后更改他人网页?在他人电脑中打开 Telnet 后门?在本书中都有详细的黑客操作与防护说明。

本书适合于所有上网用户增强网络安全意识,同时对网络管理员和致力于网络安全的开发人员有很大参考价值。

本书 CD 包含全球各地 IP 地址详细列表、端口列表以及 NetInfo、NetScan Pro、NetBrute Scanner 等各种必备网络工具。

盘 书 系 列 名 :“十五”国家重点电子出版物规划项目 计算机网络技术与网络教室系列

盘 书 名 :黑客任务实战——Windows全攻略

总 策 划 :北京希望电子出版社

文 本 著 作 者 :程秉辉 John Hawke

C D 制 作 者 :希望多媒体开发中心

C D 测 试 者 :希望多媒体测试部

责 任 编 辑 :大成

出版、发行者 :北京希望电子出版社

地 址 :北京市海淀区知春路甲 63 号卫星大厦三层 100080

网 址 www.bhp.com.cn E-mail: lwm@bhp.com.cn

电话:010-62520290, 62521724, 62528991, 62630301, 62524940, 62521921,(发行)

82675588-318,62532258,62522329 (门市) 010-82675588-501,82675588-201

(编辑部)

经 销 :各地新华书店、软件连锁店

排 版 :希望图书输出中心

CD 生 产 者 :北京中新联光盘有限责任公司

文 本 印 刷 者 :北京双青印刷厂

开 本 / 规 格 :787 毫米×1092 毫米 16 开本 32.125 印张 586 千字

版 次 / 印 次 :2003 年 6 月第 1 版 2003 年 6 月第 1 次印刷

印 数 :0001-5000 册

本 版 号 :ISBN 7-900088-03-2

定 价 :45.00 元(本版 CD)

说明:凡我社产品如有缺页,可执相关凭证与本社调换。

作者感言

黑客任务实战一攻略篇推出近两年以来，受到许多读者的支持与爱护，也给了我们相当多的批评与指教，而各种黑客技巧也是随着时间而不断的日新月异，因此我们就对原来攻略篇中的内容进行彻底的整理与翻修，删除较旧、不合时宜的内容，加入了最新、最酷的黑客技巧与攻防，并提供您更新、更方便的各种黑客工具，希望能帮助您充分了解黑客的各种手法与行为，同样的，我们也针对各种黑客手法提出有效的防护方式，让您的电脑不再成为黑客下手的目标。

本书的内容虽然丰富，但仍然不可能包含许多旁枝末节或其他主题的各种相关黑客技术与技巧，因此如果您已经有**黑客任务实战一个人机漏洞篇**、**服务器攻防篇**、**木马全攻略** (尚未出版)，来交互参考与搭配运用，必定可以让您学习黑客攻防如虎添翼、事半功倍，这是提供您参考并非绝对必要。

由于现在每天要处理的信件很多，所以目前我们只回复与书中内容或所介绍的软件有关的信件，其他不相关的信件将不处理，请您能理解与见谅，毕竟小弟不是 Bill 老大，可以依照不同的问题收取不同的费用来捞钱。另外我们并不会帮任何人或组织去破解或入侵某个网站、某台计算机或各种密码，也无法查看您的文件是否有毒、帮您测试软件、帮您找软件…等，我们很愿意帮各位解决问题，但实在无法处理这些超出范围的要求，非常谢谢您的合作！

请注意:

- 若您使用电子邮件则填写本书光盘中的读者服务卡。
- 下一页读者资料卡中的电子邮件地址请写清楚, 不要太草!

请电邮到: hawkes@ms29.hinet.net

请注意: 本书内容完全以学术与技术操作的角度来针对有关黑客攻略与防护进行讨论与研究, 所以若有将本书内容使用于任何违反法律之行为, 必须自行承担各种相关的法律责任, 请各位读者慎之! 慎之!

程秉辉
Hawke Cheng
8.27.2003

目 录

Part 1 Windows 入侵基本原理与观念 (Basic Concept for Windows Intrusion)

Internet 世界的基本原理.....	3
Port 的角色与功能.....	5
黑客任务的方法	14
Windows 入侵原理	17

Part 2 查找与锁定目标 (Search and Lock Target)

Q1: 如何找出特定目标的 IP 地址?.....	23
Q2: 如何由网址 (Address)、FTP 地址、域名 (Domain Name) 找出 IP 地址?	23
Q3: 如何找出使用动态 IP 上网者当前 IP 地址?.....	30
Q4: 如何得知固定 IP 上网者的 IP 地址?.....	30
Q5: 如何从电子邮件中找出他人的上网 IP 地址?	30
Q6: 如何由 ICQ 或 OICQ 找到对方的 IP 地址?.....	30
Q7: 如何防止别人利用邮件或 ICQ、OICQ 获取我的上网 IP?.....	30
Q8: 如何随意查找下手目标?.....	55
Q9: 如何从特定族群的 IP 地址来快速查找下手的对象?	55
Q10: 我使用 IP 扫描工具经常找了许多都没有结果, 有什么快速有效的查找技巧?	55
Q11: 如何防止被黑客随机选定为下手的目标?	55
Q12: 如何快速找到某个学校、公司或单位中连接到 Internet 的一般电脑, 是使用 Windows 而且打开端口 139?	66
Q13: 为什么有些网站或个人机的 IP 地址都未找到?	71
Q14: 对方明明就是使用固定 IP 上网, 但为何就是未找到?	71
Q15: 为何未找到网吧中某台电脑的 IP 地址?	71
Q16: 某人现在就在上网, 为何就是未找到 IP 地址? 但别人却可以找到?.....	71
Q17: 若下手的目标是以仿真 IP 方式或通过局域网中的其他电脑连接到 Internet, 要如何入侵或攻击?	71
Q18: 如何知道所要下手的目标位于那个国家或地区?	75
Q19: 如何查出某个网站、某个服务器、某个 IP 地址...是在那国家的那个地区?	

可以找出详细的街道图?.....	75
------------------	----

Part 3 Windows 黑客攻防秘技 (Hacking and Defense for Windows)

Q20: 那些目标最适合使用 Windows 直接入侵 (Port 139 入侵)?	85
Q21: Windows 直接入侵 (Port 139 入侵) 的详细流程与步骤为何?	85
Q22: Windows 直接入侵 (Port 139 入侵) 入侵会遇到那些困难与麻烦? 如何解決?	85
Q23: 若 Windows 直接入侵 (Port 139 入侵) 不成功, 还有那些方法可以 入侵 Windows 电脑?	85
Q24: 对于没有磁盘共享的电脑, 有什么方法可以将磁盘共享出来?	130
Q25: 如何利用设置注册表项就可以让他人电脑的磁盘共享出来?	130
Q26: 如何将需要键入密码的磁盘改为不必键入密码就可进入?	130
Q27: 如何彻底防止黑客利用项来将我的磁盘设置共享?	130
Q28: 如何利用具有默认共享漏洞的 WinNT 或 Win2K 电脑来入侵?	144
Q29: 每次启动进入 Windows 系统都会自动打开默认共享, 如何始终关闭它来 防止黑客入侵?	144
Q30: 对方电脑已将默认共享彻底关闭, 要如何打开?	144
Q31: WinNT、Win2K 与 WinXP 的用户名与密码藏在那里? 如何破解它?	157
Q32: 有那些方式或技巧比较快速、容易猜到磁盘共享密码?	157
Q33: 如何找出磁盘共享的电脑有设置那些用户名?	157
Q34: 如何有效防止黑客猜中磁盘共享密码?	157
Q35: 目标电脑的磁盘只能只读 (Read Only), 如何更改成可读写?	176
Q36: 如何在别人的 WinNT、Win2K、WinXP 电脑中创建最高权限帐户?	176
Q37: 如何防止共享磁盘被黑客更改成可读写?	176
Q38: 如何找出有 FTP 服务 (Port 21) 的电脑?	187
Q39: 怎样入侵有 FTP 服务的电脑?	187
Q40: 如何提高猜中进入 FTP 服务器密码的概率? 猜中后就可以更改他人网页	187
Q41: 如何防止黑客入侵有 FTP 服务的电脑?	187
Q42: 如何利用 Telnet (Port 23) 入侵 WinNT、Win2K 或 WinXP 系统的 电脑?	206
Q43: 如何让 Win2K 或 WinXP 电脑提供 Telnet 服务?	206
Q44: 为什么电脑有 Telnet 提供服务, 我却没发现?	206

Q45: 如何查看我的电脑是否有提供 Telnet 服务?.....	206
Q46: 如何防止黑客利用 Telnet 服务进行入侵?.....	206
Q47: 如何对 Internet 任何一台使用 Windows 的电脑发送信息吓对方?.....	228
Q48: 如何假冒他人名义发送信息给 Internet 上的任意 Windows 电脑?.....	228
Q49: 如何让自己的电脑不再收到 Internet 上任意散发的垃圾信息?.....	228

Part 4 入侵后的攻防实录 (Hacker Mission After Intrude Windows)

Q50: 黑客进入别人的电脑中通常会进行那些工作?.....	241
Q51: 那些文件、数据是黑客最可能的下手目标?.....	241
Q52: 如何防范容易被黑客窃取或查看的文件与文件夹?.....	241
Q53: 如何在被黑者电脑中打开一个安全、方便使用又不容易被发现的后门?.....	249
Q54: 如何防范黑客在你的电脑中创建帐户与打开 Telnet 服务?.....	249
Q55: 如何查看、修改与删除它人电脑的注册表 (Registry)?.....	255
Q56: 系统注册表 (Registry) 中那些项最可能会被黑客更改而要经常查看?.....	255
Q57: 如何防止黑客查看、更改或删除我的注册表 (Registry)?.....	255
Q58: 那些方法可以获得别人的拨号上网密码?.....	270
Q59: 使用他人的拨号帐户上网有什么法律责任?.....	270
Q60: 如何防止黑客获取我的拨号上网密码?.....	270
Q61: Cookies 文件中可能包含那些信息?.....	286
Q62: 如何分析获取 Cookies 文件中进入某些网站或 Web-Mail 的帐户?.....	286
Q63: 如何有效防止黑客获取我的 Cookies 文件?.....	286
Q64: 如何破解 ZIP、RAR、ACE、ARJ 压缩文件的密码?.....	293
Q65: 如何尽可能防止 ZIP、RAR、ACE、ARJ 压缩文件的密码被破解?.....	293
Q66: 如何破解各版本 MS-Word、Excel、Access 文件的密码?.....	301
Q67: 如何防止各版本 MS-Word、Excel、Access 文件的密码被破解?.....	301
Q68: 如何找出与使用 CuteFTP 各种版本的所有 FTP 帐户?.....	310
Q69: 如何有效防范 FTP 帐户被黑客窃取使用?.....	310
Q70: 平常应该对重要文件进行那些防护措施, 万一不幸被黑客入侵才不致造成 重大伤害或被窃取重要数据?.....	318
Q71: 如何在连接网络时将重要文件夹隐藏, 如此就可避免黑客窃取重要文件?.....	318
Q72: 如何有效防止黑客利用 at 命令运行你电脑中的各种程序文件?.....	318

Part 5 电子邮件攻防战 (Hacker Mission for E-Mail)

Q73: 如何获取与查看他人电脑中电子邮件文件中的信件?	332
Q74: 如何查看 Outlook Express、Netscape Messenger、Eudora、FoxMail 等 各种邮件程序 (含不同版本) 的信件文件?	332
Q75: 如何尽可能防止黑客获取你在电脑中保存的电子邮件?	332
Q76: 有那些方法可以破解或获取电子邮件帐户 (含 Web-Mail) 的用户名与 密码?	342
Q77: 如何破解或获取 Outlook Express 的用户名与密码?	342
Q78: 如何有效防止电子邮件帐户的密码被黑客获取?	342
Q79: 如何截取他人还未读取的电子邮件而不被对方发现?	364
Q80: 如何防止自己还未读取的信件被别人查看?	364
Q81: 如何瘫痪某个电子信箱, 让它无法收信?	376
Q82: 如何对某个电子信箱进行邮件炸弹攻击?	376
Q83: 受到邮件炸弹攻击时如何脱困?	376
Q84: 如何有效避免或防止受到邮件炸弹的攻击?	376
Q85: 如何对他人发黑信来恶作剧, 而且对方无法知到是谁?	395
Q86: 如何避免收到匿名的恶作剧信件?	395
Q87: 有那些方法可以将窗口炸弹送到对方电脑中?	399
Q88: 窗口炸弹对 Windows 系统有那些破坏与影响?	399
Q89: 如何避免受到窗口炸弹的攻击?	399
Q90: 我受到窗口炸弹的攻击, 一打开信件程序就会不断的冒出许多窗口, 根本无法收信与寄信, 如何解决?	399

Part 6 ICQ 与 OICQ 攻防战 (Hacker Mission for ICQ and OICQ)

Q91: 进入他人电脑中, 如何获取对方的 ICQ 帐户、密码与好友名单?	411
Q92: 如何查看他人的 ICQ 聊天记录?	411
Q93: 如何有效防止黑客获取我的 ICQ 密码与好友名单?	411
Q94: 进入他人电脑中, 如何获取对方的 OICQ 帐户密码与好友名单?	429
Q95: 如何从他人电脑中获取 OICQ 帐户密码?	429
Q96: 不必知道密码就可以用他人帐户登录 OICQ, 要如何做到?	429
Q97: 如何有效防止黑客获取我的 OICQ 帐户与好友名单?	429

附录 A	各地 IP 地址详细列表	448
附录 B	端口列表	450
附录 C	NetInfo	451
附录 D	NetScan Pro	453
附录 E	NetBrute Scanner	455
附录 F	Angry IP Scanner	457
附录 G	NeoTrace	459
附录 H	VisualRoute	461
附录 I	Pqwak	463
附录 J	SuperScan	465
附录 K	Cain	467
附录 L	Folder Shield	469
附录 M	Mailbag Assistant	471
附录 N	Brutus-AET2	473
附录 O	Magic Mail Monitor	475
附录 P	Mail Direct	477
附录 Q	Advanced Archive Password Recovery	482
附录 R	Advanced Instant Messengers Password Recovery	484
附录 S	Advanced Office XP Password Recovery Pro	486
附录 T	ICQr Information	488
附录 U	GetRight	490
附录 V	TCPView	495
附录 W	流光 (Fluxay)	497
附录 X	wwwhack	502
附录 Y	QQ 补丁程序	504
附录 Z	EmEditor	506

PART 1

Windows 入侵基本原理与观念

Basic Conecpt for Windows Intrusion



黑客任务实战



Windows 全攻略系列
因解难 DIY

黑客任务实战系列受到许多读者的支持与爱护，我们也收到许许多多读者反应的各种问题与意见，其中发现仍然有许多的读者在对于黑客入侵的观念相当不正确，甚至完全没有概念，甚至提出一些让小弟哭笑不得的问题，所以在本章中将详细的帮你创建正确的黑客观念、Internet 世界的架构与 Windows 入侵的基本原理，而站在防护的角度也必须彻底了解这些观念与内容，如此才可对症下药，阻挡黑客的入侵与攻击。

Note

如果你对这些内容已经很熟悉，就不需要再看本章的说明与讨论。

建立正确的观念

对方电脑有打开端口 139，为什么我无法进入？

对方电脑已打开端口 80，我要如何入侵？

有什么方法一定可以入侵某台电脑？

有什么工具或方法一定可以让我进入某台电脑或破解某个密码？

为什么我无法破解进入某台电脑或网站的密码？

...and More

相信只要有些基础概念的读者一定都会觉得这些问题有些不可思议，如果只是打开某些端口就可轻易进入，那谁还敢上网进入 Internet 中？怎么可能有一定可以入侵电脑或破解密码的方法呢？

如果真能如此，那 Windows 还能用吗？Bill 老大还混的下去吗？

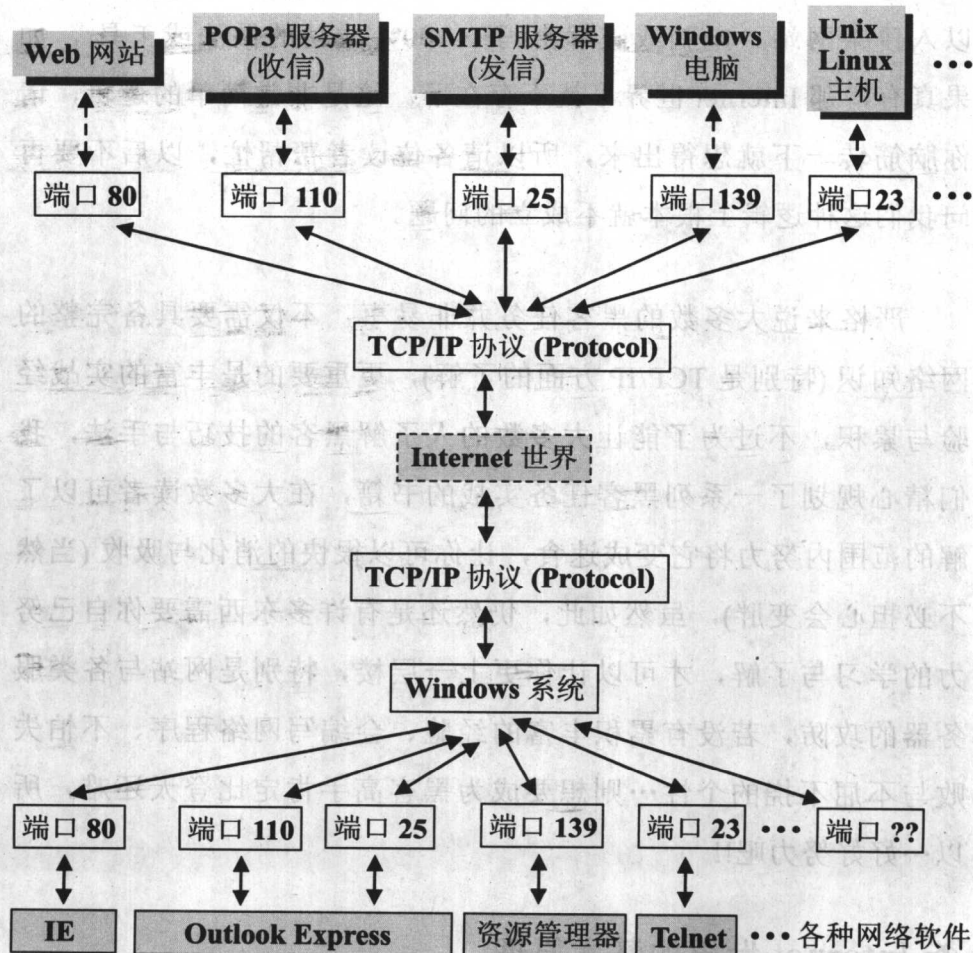
答案当然是否定的，小弟必须强调许多黑客任务虽然没有想像中的困难，但也没有那么容易就可以轻易完成，更没有一定可以入侵某网站、电脑或破解密码… 100% 成功的做法或工具，如果真有，那 Internet 世界早就不存在了。这是非常简单的逻辑，请你脑筋转一下就想得出来，所以请各位读者帮帮忙，以后不要再问我们这种逻辑上根本就不成立的问题。

严格来说大多数的黑客任务并非易事，不仅需要具备完整的网络知识 (特别是 TCP/IP 方面的了解)，更重要的是丰富的实战经验与累积，不过为了能让大多数的人了解黑客的技巧与手法，我们精心规划了一系列黑客任务实战的书籍，在大多数读者可以了解的范围内努力将它变成速食，让你可以很快的消化与吸收 (当然不必担心会变胖)，虽然如此，仍然还是有许多东西需要你自己努力的学习与了解，才可以让你更上一层楼，特别是网站与各类服务器的攻防，若没有累积丰富的经验、会编写网络程序、不怕失败与不屈不挠的个性… 则想要成为黑客高手肯定比登天还难，所以… 好好努力吧!!

Internet 世界的基本原理

不论是想做黑客或是防止被黑，都必须先了解我们电脑中的

程序、Windows 系统如何与 Internet 世界中的各种服务器、网站主机、一般电脑...建立网络连接的关系, 也就是 Internet 世界的基本原理架构啦! 如下图。



从上面的图中你可以清楚的看出在你电脑中的各种网络软件都是经由某个端口再通过 Windows 系统的 TCP/IP 模块连接到 Internet 世界中, 而同样的远程的服务器、网站主机或一般电脑也是以相同的方式来接收你电脑的信息 (或发送信息给你的电脑), 以此方式达成网络连接。

端口的角色与功能

由前面的图解与说明中你可以看出端口是你电脑进出 Internet 的大门, 任何一个网络软件都必须打开一个 (或数个) 门 (端口) 之后才能与 Internet 世界沟通, 当任何一个网络软件退出时也必须将所打开的端口全部关闭才行, 说到这里许多读者肯定有些疑问: 网络软件如何决定打开那些端口号码呢? 为什么浏览网页要使用端口 80, 如何决定出来的? ... 下面就逐一为你解答。

如何决定端口号码?

一般来说每个网络软件都可以打开任何一个端口号码来使用 (只要该号码没有其他软件在使用), 不过为了在网络连接时的畅通与避免复杂, 有些网络软件 (或硬件) 就会固定使用某一个 (或数个) 端口, 而大家也就依循这些不成文的规定来进行, 例如: 浏览器与远程的网站主机一定是通过端口 80 来进行连接 (一般网页), 但是如果某个网络软件已经先打开端口 80 来使用, 此时打开浏览器就无法浏览任何网站 (因为不可用端口 80), 这样懂了吧?!

所以依照目前大多数网络软件所使用的端口号码，下面列出常用的几个端口供你参考。

端口	说 明
端口 21	FTP 文件下载上传服务
端口 23	Telnet 主机连接服务
端口 25	SMTP 发信服务
端口 80	HTTP 网页服务
端口 110	POP3 收信服务
端口 119	NNTP 新闻讨论服务
端口 139	NetBIOS 网上邻居、资源管理器连接服务
端口 443	HTTPS SSL 加密网页服务
端口 1243, 27374	Subseven 木马程序使用
端口 5631	PCAnywhere 使用
端口 12345	Netbus 木马程序使用

若要查看更多端口已经默认给那些软硬件使用，可查看本书光盘根目录下的 **PortList.txt**，不过请注意下面三点。

- 虽然看来好像大多数的端口号码都已经默认给某个功能使用，但对大多数一般上网的电脑而言其实用到的很少，也就是说除了上表中那些较常使用的网络功能之外(木马程序不算)，大多数的端口号码根本就没有使用到。

- 有些网络软件会因为某些功能或连接上的需要打开某些端口号码，当你不再使用该功能或不需要时就会自动关闭该端口，例如：IE 浏览器在连接到某些网站时可能会再打开 1~2 个端口，当你不再浏览该网站后就自动关闭。
- 对于黑客而言，若要与植入的木马程序连接，则所使用的端口当然是避开被黑者最常 (或最可能) 使用的端口号码，应该不会笨到使用端口 80 吧?! 只要被黑者无法浏览网站就可能发现有其他程序正在使用端口 80，这不是打草惊蛇吗? 不过在大多数情况下只要不去使用上表中的那些端口号码，则其他号码随便用应该都不会有问题 (当然还是有可能出现意外)。

你的电脑目前打开那些端口?

查看目前是否有黑客入侵你电脑的最好方法就是查看目前你的电脑打开那些端口，而这些端口又与那个网站或电脑连接，这里我们告诉你两种方法来查看。

方法① 使用 netstat

这是各版本 Windows 都有提供的基本功能之一，它是显示目前有那些 IP 地址正通过那个端口与你的电脑连接中，以此方式来查看是否有黑客或不明程序正在进行见不得光的勾当，操作方式如下。