



Internet Security for Your PC or Server
本书列举出123个问题彻底帮助你免于黑客或病毒的威胁与伤害

本书光盘包含：端口列表/Currports/NetInfo/SyGate Personal Firewall/TaskInfo/Startup/
Magic Mail Monitor/FolderShield/Spybot-Search & Destroy/N-Stealth/GetRight/IPNetInfo/Netcraft Toolbar



— 黑客防护实战 —



防黑缉毒擒木马



绝命追杀

第三版

北京希望电子出版社
程秉辉 John Hawke

总策划
编 著

- * 全球最完整、详尽的黑客病毒防护操作
- * 利用**仿真IP**或**隐藏IP**来防止黑客入侵
- * 如何针对自己的计算机或服务器**定制防火墙**
- * 检查与判断是否正有黑客连接到我的计算机
- * Windows入侵的完全阻挡和防护
- * 如何找出与清除**隐藏**在你计算机中的木马程序
- * 电子邮件、Java、ActiveX、批处理文件……完全防护
- * IE被强迫更改、功能不可用……**完全复原**
- * 快速查找与修补系统及各类软件的漏洞
- * 从各种安全日志 (Log) 中判断是否有黑客入侵或病毒感染
- * 如何防止**安全日志**被黑客删除或修改
- * 追踪黑客IP的讨论与研究
- * 蠕虫病毒、拒绝服务攻击、分布式攻击……研究与讨论
- * 最新无线网络防护的研究与讨论
-

本书中所有内容都经过严格的测试，决不告诉你无法做到的方法！



 科学出版社
www.sciencep.com



Internet Security for Your PC or Server

本书列举出123个问题彻底帮助你免于黑客或病毒的威胁与伤害

本书光盘包含：端口列表/Currports/NetInfo/SyGate Personal Firewall/TaskInfo/Startup/
Magic Mail Monitor/FolderShield/Spybot-Search & Destroy/N-Stealth/GetRight/IPNetInfo/Netcraft Toolbar



— 黑客防护实战 —



防黑缉毒擒木马



绝命追杀

第三版

北京希望电子出版社 总策划
程秉辉 John Hawke 编 著

- * 全球最完整、详尽的黑客病毒防护操作
- * 利用仿真IP或隐藏IP来防止黑客入侵
- * 如何针对自己的计算机或服务器定制防火墙
- * 检查与判断是否正有黑客连接到我的计算机
- * Windows入侵的完全阻挡和防护
- * 如何找出与清除隐藏在你计算机中的木马程序
- * 电子邮件、Java、ActiveX、批处理文件……完全防护
- * IE被强迫更改、功能不可用……完全复原
- * 快速查找与修补系统及各类软件的漏洞
- * 从各种安全日志 (Log) 中判断是否有黑客入侵或病毒感染
- * 如何防止安全日志被黑客删除或修改
- * 追踪黑客IP的讨论与研究
- * 蠕虫病毒、拒绝服务攻击、分布式攻击……研究与讨论
- * 最新无线网络防护的研究与讨论
-

本书中所有内容都经过严格的测试，决不告诉你无法做到的方法！



 科学出版社
www.sciencepress.com

内 容 简 介

本书对 Windows 下的各种可能出现的漏洞进行彻底的整理, 加入了大量新的黑客技巧与攻防, 提供更新、更方便的各种防黑防毒的操作。本书畅销两岸三地数年, 现技术全面更新出版。

主要内容包括: 利用仿真 IP 或隐藏 IP 来防止黑客入侵, 设置个人防火墙, 检查与判断是否正有黑客连接到我的计算机, Windows 入侵的完全阻挡防护, 找出并干掉隐藏在计算机中的木马程序, 电子邮件、Java、ActiveX、批处理文件的完全防护, IE 被强迫更改、快速查找与修改系统与各类软件的漏洞, 从各种安全日志中判断是否有黑客或病毒入侵, 防止安全日志被黑客删除或修改, 追踪黑客 IP 的讨论与研究, 蠕虫病毒、拒绝服务攻击、分布式攻击讨论与研究。另外, 对最新的无线网络防护手段进行了详细讲解并给出具体操作。

本书可作为所有计算机用户的安全手册, 同时对网络管理员和致力于网络安全开发人员有很大参考价值。

本书光盘中包含各种必备网络安全工具。

图书在版编目 (CIP) 数据

防黑缉毒擒木马之绝命追杀 / 程秉辉, John Hawke 编

著: —3 版. 北京: 科学出版社, 2006.4

(黑客防护实战)

ISBN 7-03-016854-2

I. 防... II. ①程... ②J... III. 电子计算机—安全技术
IV. TP309

中国版本图书馆 CIP 数据核字 (2006) 第 008368 号

责任编辑: 李兴旺 / 责任校对: 但明天

责任印刷: 双 青 / 封面设计: 刘孝琼

科 学 出 版 社 出 版

北京东黄城根北街 16 号
邮政编码: 100717

<http://www.sciencep.com>

北京媛明印刷厂印刷

科学出版社发行 各地新华书店经销

*

2006 年 4 月第 一 版

2006 年 4 月第一次印刷

印数: 1-5000 册

开本: 787×960 1/16

印张: 32 1/2

字数: 584 000

定价: 46.00 元 (配 1 张光盘)

作者感言

一波未平、一波又起，是许多人面对病毒与黑客入侵的无奈。随着时间的推移，攻防双方势力的消长，又衍生出许多新型的入侵手法与攻击方式，让许多人防不胜防、疲于奔命，而面对似毒非毒的间谍或恶意程序更是不知所措。据统计，平均每台电脑中至少有 3~4 个间谍或恶意程序 (还不包含木马或病毒)，实在可怕。事实上，大多数上网者对于网络安全常识的掌握还远远不够，甚至根本不重视，小弟认为这应该是保守估计，实际情况可能更加严重。

事前预防永远胜于事后治疗。小弟与 John Hawke 老兄再度尝遍万毒，观察与研究自己惨死时的状况，再找出相关的处理方式与防护之道，写入本书与您共享。其实，防止黑客或病毒进入你的电脑中并不像我们想象的那么困难，只要坚守一些基本原则，防护好几个重要的关卡，就可以让它们很难越雷池一步。对于间谍、恶意程序或各种网络钓鱼 (Phishing) 诈骗手法等则一定要提高警惕，及时学习网络安全基本知识，再配合本书中小弟在痛苦经验中所获得的防护方式，必定能让你的电脑或服务器从此远离各种伤害与威胁。

无线网络的防护也是本书中重要的一环，小弟用了 38 页进行了详细地研究与讨论，并提出 10 个方法来彻底保障你的无线网络不会被盗用，算是用心良苦了，也是现在此类书籍中介绍得最详尽的，希望您不吝参考与指教。

请填写本书光盘中的读者服务卡或
下一页的读者资料卡，然后

E-Mail 到 hawkegg@gmail.com



程秉辉
Hawke Cheng

请将下表数据填妥后 EMail 到 hawkes@ms29.hinet.net ,
我们将会不定期地为您提供有关 Windows、Internet 和多
媒体的各种最新信息和软件。您也可以到我们的网站
<http://www.faqdiy.cn/> 获得相关的更新文件与最新信
息。请多多利用, 谢谢!



若您使用电子邮件则请使用本书光盘中所附
的读者服务卡, 不必使用这个读者服务卡。

读者服务卡 REGISTER CARD

书名	防黑缉毒擒木马之绝命追杀				
姓名		性别	☐ 先生 ☐ 小姐	年龄	
学历	☐ 研究所 ☐ 大学 ☐ 专校 ☐ 高中职 ☐ 中学 ☐ 小学				
您的电子邮件					
传真号码					
购买地区 (选择最 近城市)	☐ 北京 ☐ 上海 ☐ 南京 ☐ 广州 ☐ 深圳 ☐ 武汉 ☐ 重庆 ☐ 成都 ☐ 福州 ☐ 天津 ☐ 大连 ☐ 南昌 ☐ 苏州 ☐ 杭州 ☐ 青岛 ☐ 长沙 ☐ 开封 ☐ 合肥 ☐ 哈尔滨 其它:				
职业	☐ 学生 ☐ 电脑业或 IT 部门 ☐ 非电脑业 ☐ 其他:		您认为 本书	☐ 简单 ☐ 适中 ☐ 很难	
您在写程序时 常遇到什么样的 困扰与麻烦?					
您从何处 知道 本书?	☐ 连锁书店 ☐ 一般书店 ☐ 电脑专卖店 ☐ 同学 ☐ 展览 ☐ 亲友 ☐ 广告函 ☐ 因特网 ☐ 报纸: ☐ 杂志: ☐ 其他:				
您还需要哪些 方面的书籍?	☐ 其他Windows排困解难 ☐ 黑客攻防研究 ☐ 防黑防毒 ☐ 网页设计排困解难 ☐ Java语言设计 ☐ Windows程序设计(MFC,SDK) 其他:				
您对本书 有何建议?					

目 录

Part 1 病毒入侵观念、下手目标与黑客行为

(Internet Concept and Hacker, Virus Intrusion)

Internet 世界的基本原理	2
端口的角色与功能	3
黑客与病毒入侵或攻击的目标	6
病毒的定义与说明	8
讨论与研究	9
 Q1 黑客或病毒通常使用哪些方法来入侵或攻击一般上网电脑的？ 如何针对这些方法来进行围堵与防御，以有效地防护我们的上网电脑？	 11
 Q2 黑客或病毒通常使用哪些方法来入侵或攻击网站与各类型的服务器？ 如何针对这些方法进行围堵与防御，以达到有效防护的目的？	 18

Part 2 IP、端口防护与架构个人防火墙（含无在线网防护）

(Protection for IP,Port and Build your personal firewall)

Q3 如何对一般上网电脑进行有效地预防，以防止黑客或病毒的入侵或破坏？	23
Q4 一般上网电脑必须采取哪些防护措施？	23
Q5 一般上网电脑的防黑防毒流程是什么？	23
 Q6 如何隐藏一般电脑的 IP 地址， 避免黑客找到我电脑的 IP 地址、进行入侵或攻击？	 27
Q7 有哪些方式可以将一般电脑的 IP 地址隐藏，不让别人找到？或找起来很困难？ ...	27
Q8 有哪些方法可以架构出仿真 IP 地址？	36
Q9 一般上网电脑如何使用仿真 IP 的方式来避免黑客的直接入侵与攻击？	36
Q10 仿真 IP 一定要使用路由器（Router）或集线器（HUB）才能实现吗？	36
Q11 如何用最低的成本架构出仿真 IP？	36
Q12 必须使用 DHCP 才能让网络中的每台电脑都有 IP 地址上网吗？	36
Q13 如何监控我的电脑中各网络程序的状态，并针对可疑的程序进行拦截检查？	39
Q14 如何阻挡正在进行存取的可疑的网络程序，不让它继续进行？	39

Q15	可以让我决定哪些程序可以进行网络存取, 哪些程序不能进行网络存取吗?	39
Q16	如何对没有必要或未使用的 Internet 协议 (Protocol) 与端口进行阻挡设置?	45
Q17	如何根据自己的网络状况与需求来设置个人防火墙?	45
Q18	如何对已知木马程序所使用的端口进行阻挡?	45
Q19	我使用了网络防护程序 (或防火墙软件), 经常出现某个端口被扫描 (或连接) 的信息, 实在很烦人, 应该如何有效阻挡它而且不再弹出信息来烦我?	45
Q20	如何检查与判断当前是否有黑客正在连接到我的电脑?	76
Q21	如何检查当前我的电脑中有哪些程序正在上网连接? 与哪个网站或 IP 地址进行连接?	76
Q22	如何关闭当前正在进行的可疑连接, 并关闭与该连接对应的程序?	76
Q23	黑客是如何偷用无线网络的? 是什么原因让无线网络门户大开?	85
Q24	黑客入侵无线网络后会造成哪些问题?	85
Q25	如何有效防范黑客偷用我的无线网络? 有哪些防护措施? 各有何缺点? 如何补救?	85

Part 3 Windows 的黑客病毒入侵防护

(Hacker and Virus Defense for Windows)

入侵基本原理与对象	124
黑客或病毒通过 Windows 的入侵流程	124
端口 139 的防护	126
磁盘共享防护	127
默认共享漏洞防护	127
RPC 防护	127
FTP 防护	127
Telnet 防护	127
终端机服务防护	128
漏洞修补与防护	128
电子邮件防护	129
死机攻击防护	129
恶意信息防护	129
讨论与研究	130

Q26	如何关闭端口 139, 彻底杜绝黑客利用此端口入侵我们的电脑?	131
Q27	防止黑客通过端口 139 入侵 Windows 系统, 有哪几道防御措施?	131
Q28	我需要与其它电脑进行网络连接, 所以必须打开端口 139, 这样该如何防止黑客入侵呢?	131
Q29	我的电脑必须打开磁盘共享, 该如何有效防止黑客入侵?	131
Q30	如何防止黑客利用注册表将我的磁盘设置成共享或可读写?	152
Q31	如何防止黑客利用注册表将磁盘共享密码设置成不需输入密码就可进入?	152
Q32	如何有效地防止黑客猜中磁盘共享密码?	152
Q33	如何修补 Windows 9x/ME 的资源共享密码漏洞?	152
Q34	如何防止黑客在 Windows NT/2000/XP 系统中创建最高权限帐户?	152
Q35	什么是默认共享漏洞? 它的原理是什么?	169
Q36	Windows 系统每次启动时都会自动打开默认共享, 如何始终关闭它来防止黑客入侵?	169
Q37	如何防止黑客将默认共享打开?	169
Q38	为什么我的电脑提供了 Telnet 服务, 我却没发现?	175
Q39	如何检查我的电脑是否有提供 Telnet 服务?	175
Q40	如何防止黑客打开 Telnet 服务?	175
Q41	如何彻底关闭 Telnet 服务, 杜绝黑客使用此方式入侵?	175
Q42	为何我在上网时经常遇到奇怪的广告或垃圾信息窗口?	180
Q43	如何让自己的电脑完全阻止 Internet 上任意散发的垃圾信息?	180
Q44	我使用的是 Windows 9x/ME, 如何才能快速地关闭或打开磁盘共享? 有什么更好的方法?	183
Q45	我仅一块网卡, 上网或连接到局域网时都要将网线拔来拔去, 实在很麻烦, 有什么好的解决方式?	183
Q46	如何对 Windows 系统的漏洞进行修补?	185
Q47	如何在连接网络时将重要文件夹隐藏或将重要文件加锁, 万一被黑客入侵才不会造成重大伤害或重要数据被偷取?	185
Q48	如何防止黑客利用 at 远程运行命令运行你电脑中的各种程序? 如何关闭 at 命令?	185

Part 4 木马、后门与病毒的防护、搜索与摧毁

(Search and Destroy for Trojan、Back Door Programs and Virus)

Q49	木马、后门或跳板程序是什么？与病毒有何关系？	201
Q50	木马、后门或跳板程序可以帮黑客进行哪些工作？	201
Q51	防卸木马病毒入侵的方式都由哪些？	201
Q52	如何有效地预防被黑客植入木马病毒？	205
Q53	黑客通常使用哪些方式将木马病毒植入他人的电脑或服务器中？	205
Q54	如何有效测试与检查下载的文件没有包含各种木马病毒、 恶意或间谍程序？	209
Q55	我每次下载文件后都要使用杀毒软件检查，如何设置为下载完成后 就自动检查？	209
Q56	我下载的文件是压缩文件，这样可以检查出其中是否有木马病毒、 恶意或间谍程序吗？	209
Q57	如何检查或找出你的电脑中是否被植入了木马病毒或跳板程序， 将它彻底干掉？	216
Q58	使用杀毒软件或网络防御程序检查各类木马病毒，要注意哪些地方？	218
Q59	如果杀毒软件或网络防御程序发现了木马病毒，应该如何处理最好？	218
Q60	要将杀毒软件或网络防御软件常驻吗？ 如何使用才有最佳的效果，也不影响系统性能？	218
Q61	被黑客植入的木马程序都藏匿在哪些地方？如何找出来砍头？	234
Q62	木马病毒使用哪些方法设置一进入 Windows 就自动运行？	234
Q63	如何判断与找出隐藏在注册表 (Registry) 或系统服务中设置运行的木马病毒？	234
Q64	如何检查正在运行的.exe 或.dll 程序，找出可疑的程序将它干掉？	265
Q65	为何杀毒软件或我自己手动操作都无法将.dll 木马病毒从电脑中卸载？	265
Q66	经过伪装或易容的木马程序如何才能辨识出来， 然后将它彻底干掉？	273

Part 5 浏览器与电子邮件的入侵防护

(Virus and Hacker Defense for E-Mail Programs and Browser)

Q67	电子邮件通常会受到黑客或病毒的哪些方式的入侵与攻击? 如何各个击破?	277
Q68	如何避免受到邮件炸弹或一堆邮件的攻击?	284
Q69	受到邮件炸弹或一堆邮件的攻击时如何脱困?	284
Q70	如果有人发一大堆的邮件给我, 该如何解决?	284
Q71	有哪些方法可以防止与避免邮件被他人截取?	295
Q72	若发现邮件被他人截取, 要采取什么样的补救措施以减少可能的损害?	295
Q73	如何查看电子邮件的附件中是否有木马、病毒程序或各类具有破坏性的 注册表文件和批处理文件?	299
Q74	如何对邮件中的 Java 恶意源代码进行防护?	306
Q75	如何避免遭到窗口炸弹或其它 Java 恶意源代码的攻击?	306
Q76	我遭到了窗口炸弹的攻击, 一打开邮件程序就会不断地冒出许多窗口, 根本无法收信与寄信, 该如何解决?	306
Q77	如何对邮件中的 ActiveX 恶意源代码进行防护?	316
Q78	通常黑客利用 ActiveX 程序进行哪些恶意行为?	316
Q79	如何避免遭到 ActiveX 恶意源代码的攻击?	316
Q80	如何对邮件中夹带的批处理文件进行判断与防护?	325
Q81	为何杀毒软件或网络防护程序无法找出批处理文件病毒?	325
Q82	如何查出某一封电子邮件是从哪个国家的哪个地区寄出来的?	328
Q83	如何查出某个邮件地址是在哪个国家或哪个地区?	328
Q84	如何查出寄件者的寄送邮件时的 IP 地址?	328
Q85	为什么所有程序都无法运行?	338
Q86	控制面板中的所有项目都无法运行, 而且还出现未找到文件的错误信息, 如何解决?	338
Q87	为什么我的注册表编辑器不可用? 如何解决?	343
Q88	为什么在  菜单中的  运行(R)... 不见了? 如何恢复?	343

Q89	通常浏览器会受到黑客或病毒的哪些攻击和入侵方式？如何防护？ 有什么彻底有效的解决方式？	346
Q90	什么是网页钓鱼法（Phishing）？黑客如何利用它来窃取各种帐户与密码？ 如何防护？	346
Q91	如何借助网站的相关信息来判断是否为钓鱼的假网页？	352
Q92	我的 IE 每次打开时都自动连接到某个网站，无法改回来， 该如何解决？	354
Q93	我的 IE 主页与上方标题被改成某个网站， 无法改回来或改回来后又被改回去，该怎么办？	354
Q94	我的 IE 有许多功能被关闭（如右键菜单、Internet 选项、高级设置、 查看邮件源文件等都不可用），如何打开？	354
Q95	在 IE 工具栏中加入了指向某网站的按钮，该如何将它去掉？	354
Q96	如何找出与干掉藏匿在我的电脑中偷改 IE 各项设置的可恶程序？	354
Q97	什么是间谍或恶意源代码？会造成哪些伤害与影响？	365
Q98	如何找出并干掉电脑中被某些网站植入的恶意源代码、间谍程序、 Cookies 或注册项？	365
Q99	如何管理、判断电脑中已存在的 Cookies 信息？	365
Q100	当有 Cookies 要写入到电脑中时，可以让我决定是否保存吗？ 该怎么做？	365
Q101	恶意或间谍防护软件有哪些不足之处？如何补其不足？	365
Q102	如何对任何软件（特别是共享软件或免费软件）的可疑网络连接 进行判断与阻挡？	365
Q103	如何提高 IE 浏览器发送数据的安全性？	378
Q104	如何降低浏览器数据包被破解的概率？	378
Q105	如何升级 IE 浏览器到 128 位的加密版本？	378
Q106	如何防止木马程序、病毒或破坏程序利用邮件程序 或浏览器漏洞进行入侵？	386
Q107	如何快速对 IE 或 Outlook 漏洞进行修补？	386

Part 6 网络服务器的黑客病毒防护

(Virus and Hacker Defense for Internet 服务器)

入侵或攻击方式	394
安全与防护	401
找出幕后的黑手(黑客的追踪与研究)	406
Q108 什么是蠕虫病毒? 它有何破坏与影响?	407
Q109 蠕虫病毒是如何寄生、扩散与攻击的? 如何有效防护它?	407
Q110 什么是拒绝服务攻击? 它会造成哪些影响?	411
Q111 拒绝服务攻击(DoS, Denial of Service)通常有哪些方式? 各有何优缺点? 基本原理为何?	411
Q112 什么是分布式攻击(DDoS)? 它与一般拒绝服务攻击(DoS)有何不同?	411
Q113 什么是 SMB 缓冲区溢出漏洞? 如何修补它?	424
Q114 如何对自己的服务器进行测试和检查, 以找出可能的漏洞?	434
Q115 如何查找 Windows 系统、IIS、Apache、SQL 服务器中是否有新的漏洞? 如何修补?	434
Q116 如何设置 Windows 2000/XP 系统的防火墙功能?	445
Q117 如何为我的服务器打造专用的防火墙?	445
Q118 如何从安全日志中判断是否有黑客或病毒入侵?	454
Q119 如何查看与判断系统日志、任务计划记录、IIS 记录?	454
Q120 如何判断安全日志是否被黑客删除?	454
Q121 如何防止安全日志被黑客删除或修改?	454
Q122 如何追踪并查出黑客的位置, 进一步查出黑客是谁?	470
Q123 黑客都是使用哪几种方式隐藏自己的 IP 来进行入侵的? 如何追踪?	470

附 录

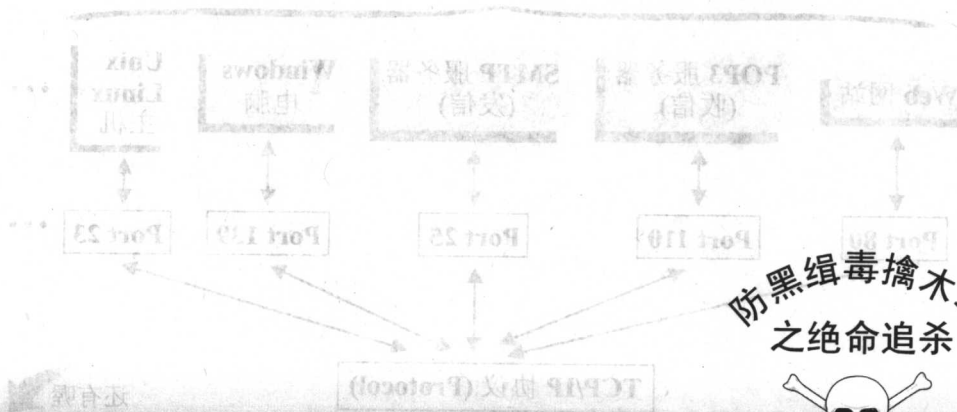
附录 A 端口列表	476
附录 B Currports	477
附录 C NetInfo	478
附录 D SyGate Personal Firewall	480

附录 E	TaskInfo	482
附录 F	Startup	487
附录 G	Magic Mail Monitor.....	489
附录 H	FolderShield.....	491
附录 I	Spybot - Search & Destroy	492
附录 J	N-Stealth	495
附录 K	GetRight.....	497
附录 L	IPNetInfo	502
附录 M	File Encryption Shell Extension	503
附录 N	eMailTrackerPro	504
附录 O	Netcraft Toolbar.....	505
附录 P	Cookies Wall.....	506

PART 1

病毒入侵观念、下手目标与黑客行为

Internet Concept and Hacker, Virus Intrusion



防黑缉毒擒木马
之绝命追杀



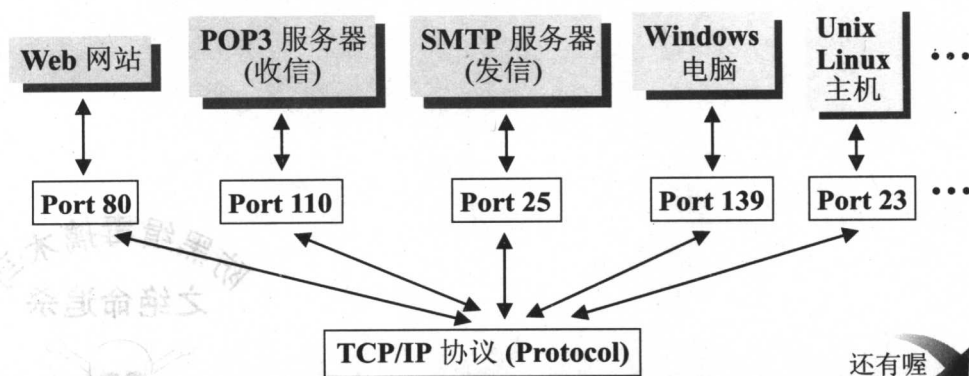
知己知彼，百战百胜。要对网络黑客的入侵或攻击进行有效地防御，就必须先了解黑客入侵、攻击的基本方法，下手的目标以及各种可能的黑客行为，然后再针对这些不同的方法和环节来找出围堵与防御之道。如此才能有效地将黑客阻拦于门外，以保护我们的系统。

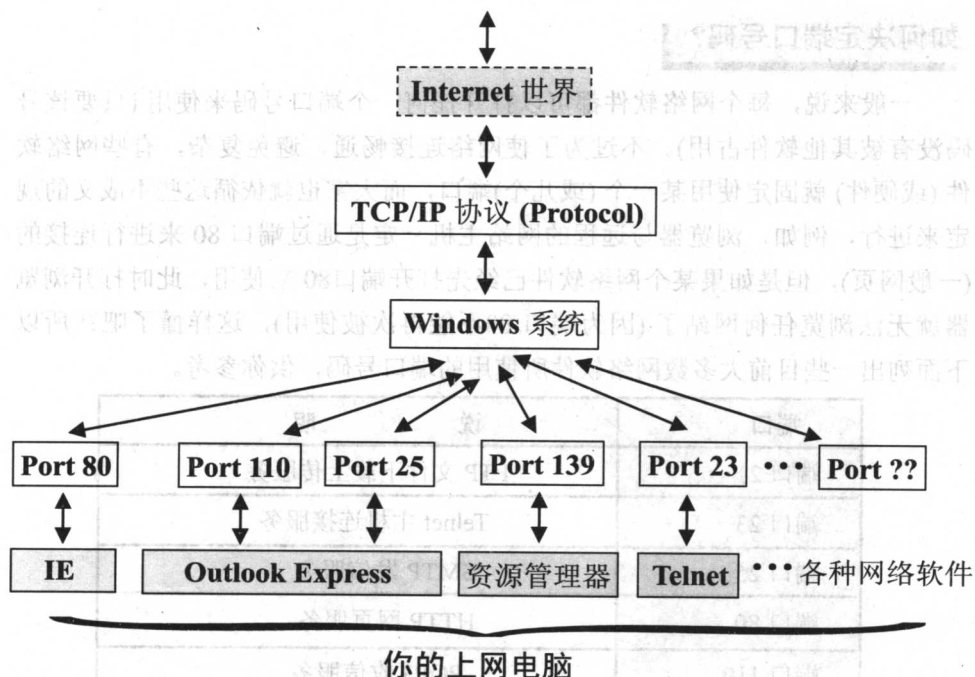
不过，我们从黑客任务实战系列书籍读者的反应中发现：许多读者的网络观念并不清楚，例如，以为某个端口打开就会被入侵或者可入侵该电脑、使用某种方法就一定可以入侵他人电脑或破解密码等诸如此类严重的错误观念。因此在研究黑客的各种行为之前，我们要先了解一般上网电脑与 Internet 之间的关系，以及 Internet 的基本架构、端口的意义与角色等，如此才能更清楚地了解黑客是如何利用这些架构上的弱点与漏洞来进行入侵或攻击的，而不是人云亦云、道听途说，用错误的观念进行黑客防护，这样不仅事倍功半甚至白忙一场。

Internet 的基本原理

不论是想做黑客或是防止被黑，都必须先了解我们的 Windows 系统以及相关的网络程序是如何与 Internet 中的各种服务器、网站主机、一般个人电脑等建立网络连接的，也就是 Internet 的基本原理架构啦！如下图所示。

连接远程的各种服务器、主机或一般个人电脑





从上面的图中可以清楚地看出上网电脑中的各种网络软件都是经过某个端口后再通过 Windows 系统的 TCP/IP 模块 (协议) 连接到 Internet 中的。同样, 各种远程服务器、网站主机或一般电脑也是以相同的方式连接到 Internet 后才与你的电脑完成连接的, 然后我们才能进行数据交换、信息存取等动作。

端口的角色与功能

由前面的图解与说明可以看出, 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 (或多个) 门 (即端口) 之后才能与 Internet 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。说到这里, 许多读者可能有些疑问: 网络软件如何决定打开哪些端口号码呢? 为什么浏览网页要使用端口 80? 是如何决定出来的?……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 (只要该号码没有被其他软件占用)。不过为了使网络连接畅通, 避免复杂, 有些网络软件 (或硬件) 就固定使用某一个 (或几个) 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 来进行连接的 (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了 (因为端口 80 不能再次被使用), 这样懂了吧?! 所以下面列出一些目前大多数网络软件所使用的端口号码, 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

盲区说明: 前面说过, 这些端口的定义都是不成文的规定, 也就是说如果你发现某个软件正在打开与使用某个端口 (例如, 27374), 并不表示一定就是被 Subseven 木马程序入侵 (参考上表), 也可能是某个软件暂时打开该端来使用, 所以不必太惊慌, 例如, IE 在打开网页时除了打开端口 80 外也会打开其他端口来使用。