

Vista
XP
全适用

The Bible of Internet Security and Protection (Ultimate Version)

光盘内容

- 15套防毒、防骇、漏洞检查工具全面严防危险入侵!!

网络安全问题层出不穷，千万不要因为无知而成为下一个受害者!!

重拳出击

Windows 防黑杀毒大作战

本书中所有实例都经过多次的严格测试，绝不告诉你无法做到的方法!

- 抛开聊胜于无的 Windows 防火墙，建立更安全稳固的**专属防火墙**
- 有效抓出与系统挂钩的可疑程序
- 拦截透过系统文件或元件连接网络的不速之客
- 利用虚拟 IP 或隐藏 IP 来防止黑客入侵
- 防止无线网络被盗用的 10 种防护方法
- 哪些程序正在连线？使用哪个端口？与哪个远程 IP 连线？
- 不速之客藏匿的 11 个地方，如何找出与干掉它？!
- 木马、恶意或间谍程序、傀儡或僵尸程序、后门程序、跳板程序、病虫、病毒等的寻找、判断、歼灭
- 各种下载文件的病毒查杀、测试
- 电子邮件、Java、ActiveX、注册项文件、批处理文件的完全防护
- 寄件者 IP、所在国家、地区的电子邮件大追踪
- 仿冒网页（网页钓鱼，Phishing）手法大公开与有效防护
- 从各种安全日志（log）中判断黑客或病虫入侵及状况

北京希望电子出版社 总策划
程秉辉 John Hawke 合 著



科学出版社
www.sciencepress.com



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

Vista
XP
全适用

The Bible of Internet Security and Protection (Ultimate Version)



光盘内容

15套防毒、防骇、漏洞检查
工具全面严防危险入侵!!

网络安全问题层出不穷，千万不要因为无知
而成为下一个受害者!!

重拳出击

Windows 防黑杀毒大作战

本书中所有实例都经过多次的严格测试，绝不告诉你无法做到的方法!

- 抛开聊胜于无的 Windows 防火墙，建立更安全稳固的专属防火墙
- 有效抓出与系统挂钩的可疑程序
- 拦截透过系统文件或元件连接网络的不速之客
- 利用虚拟 IP 或隐藏 IP 来防止黑客入侵
- 防止无线网络被盗用的 10 种防护方法
- 哪些程序正在连线？使用哪个端口？与哪个远程 IP 连线？
- 不速之客藏匿的 11 个地方，如何找出与干掉它？!
- 木马、恶意或间谍程序、傀儡或僵尸程序、后门程序、跳板程序、病毒、病毒等的寻找、判断、歼灭
- 各种下载文件的病毒查杀、测试
- 电子邮件、Java、ActiveX、注册项文件、批处理文件的完全防护
- 寄件者 IP、所在国家、地区的电子邮件大追踪
- 仿冒网页（网页钓鱼、Phishing）手法大公开与有效防护
- 从各种安全日志（log）中判断黑客或病毒入侵及状况

北京希望电子出版社 总策划
程秉辉 John Hawke 合 著



科学出版社
www.sciencepress.com



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

内 容 简 介

这是一本基于 Windows 操作系统上网用户的系统及网络安全图书。

网络安全问题层出不穷,千万不要因为缺乏准备的头脑而成为下一个替罪羔羊! Internet 安全已经成为所有电脑用户不可或缺的基本知识——除非你不准备上网,而使用 Windows 防火墙或者安装杀毒软件就能万事无忧了吗?当然是 Mission Impossible!! 在各种木马、恶意或间谍程序、傀儡或僵尸程序、后门程序、跳板程序、蠕虫、病毒……四处横行的 Internet 世界,仅仅使用功能简单的 Windows 防火墙或者防病毒软件已经不可能保障你的电脑安全。然而求人不如求己,每位上网者必须充实与了解网络安全的基本知识,然后才可能针对各种不同的黑客手法进行有效防范,有效地保障浏览网页、收发 E-mail、下载资料、聊天等操作的安全。

本书适合每位 Windows 联网用户以及各类网络办公企业。同时也适合 Windows——特别是 Vista 和操作系统 DIY 爱好者,更对社会培训班、现代办公企业受益匪浅。

光盘内容为书中所用部分工具的安装程序。

图书在版编目(CIP)数据

重拳出击—Windows 防黑杀毒大作战 / 程秉辉等著.

北京: 科学出版社, 2008.2

ISBN 978-7-03-020691-6

I. 重... II. 程... III. ①窗口软件, Windows②计算机
网络—安全技术 IV. TP316.7 TP393.08

中国版本图书馆 CIP 数据核字 (2007) 第 184169 号

责任编辑: 但明天

/ 责任校对: 全 卫

责任印刷: 媛 明

/ 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

*

2008 年 2 月第 一 版

开本: 787×960 1/16

2008 年 2 月第一次印刷

印张: 31 3/4

印数: 1—5000

字数: 566 080

定价: 48.00 元 (配 1 张光盘)

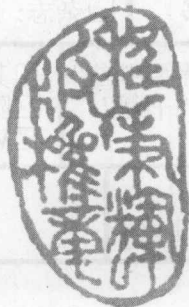
作者感言

网络世界中的各种恶意……甚至是犯罪行为，各种手法随着时间的推移不断地改进与创新，攻防双方势力的消长，又衍生出许多新形态的黑客手法与攻击方式，让许多人防不胜防、疲于奔命，而面对似毒非毒的间谍、恶意、傀儡或僵尸程序更是不知所措，甚至毫不自知。据统计，平均一台电脑中至少有 3~4 个间谍、恶意、傀儡或僵尸程序 (不包含木马或病毒)……这实在相当可怕，事实上大多数网民普遍对于网络安全的常识不足，甚至根本不重视，因此小弟认为这应该是保守估计，实际的情况肯定更加严重。

预防永远胜于治疗，防止各种不速之客进入你电脑中并不如想像中的困难，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。在本书中，我们改用更新、更聪明的防火墙，不仅可以把守网络重要关卡，也能监控可疑或恶意行为；对于找出木马、恶意或间谍程序、傀儡或僵尸程序、后门程序、跳板程序、病虫、病毒……提出更有效的防护与抓出不速之客的方法；而仿冒网页 (网页钓鱼, Phishing) 的诈骗手法也有更新、更彻底的防护之道，相信必定能让你的电脑或网络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，多达 42 页来详细研究与讨论，并提出 10 个方法来彻底保障你的无线网络不会被盗用，相当用心良苦，也是坊间各书籍中说明最详尽的，绝对可以保障你无线网络的安全。

请填写本书光盘中的读者服务卡或下一页的读者服务卡，然后
E-mail 到 hawkegg@gmail.com。



程秉辉
Hawke Cheng
2007.10.27

请将下表数据填妥后 E-mail 到 hawkegg@gmail.com
 我们将会不定期地提供给你有关各种 Windows、Internet
 与多媒体的最新信息与相关软件，请多多利用，谢谢！
 你也可以到我们的网站: <http://www.faqdiy.cn/>
 来获得相关的更新文件与最新信息!!



若你可以使用电子邮件，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。

讀者服務卡 REGISTER CARD			
书名	Windows 防黑杀毒大作战		本书序列号 北京希望2K71201
姓名		性别 ☐ 先生 ☐ 小姐	年龄
学历	☐ 博士 ☐ 硕士 ☐ 学士 ☐ 大专 ☐ 中专 ☐ 中学及以下		
你的电邮地址			
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 ☐ 其他: _____		
职业	☐ 学生 ☐ 电脑业或 IT 部门 ☐ 非电脑业 ☐ 其他: _____	你觉得本书	☐ 简单 ☐ 适中 ☐ 艰深
使用 Windows 时常遇到什么样的困扰与麻烦?			
你从何处知道本书	☐ 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: _____		
你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: _____		
你对本书有何建议			

目 录

Windows 防黑杀毒大作战



Part 1 防毒、防黑的认知与基本观念

(Understand and Realize about AntiHacker, AntiVirus)

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	5
病毒的定义与说明	7
讨论与研究	8
Q1 黑客或病毒通常使用哪些方法来入侵或攻击一般上网的个人机? 如何针对这些方法进行围堵与防御以达到有效防护?	10
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?	10

Part 2 IP、端口防护与架构专属防火墙 (含无线上网防护)

(Protection for IP, Port and Build Personal Firewall)

Q3 如何对一般上网电脑进行有效的预防措施, 以防止黑客或病毒的入侵或破坏?	23
Q4 有哪些防护措施是一般上网的个人机必须要实现的?	23
Q5 一般上网个人机的防黑杀毒流程是为何?	23
Q6 一般上网电脑如何将自己上网的 IP 地址隐藏起来, 使黑客无法找到以避免被入侵或攻击?	27
Q7 有哪些方式可以将自己的 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虚拟 IP 地址来上网?	35
Q9 一般上网电脑如何使用虚拟 IP 的方式来避免黑客的直接入侵与攻击?	35
Q10 虚拟 IP 一定要使用路由器 (Router) 或集线器 (HUB) 才能实现吗?	35
Q11 如何以最低的成本来架构出虚拟 IP?	35
Q12 一定要使用 DHCP 才能让网络中的每台电脑都有 IP 地址上网吗?	35
Q13 如何监控我的电脑中各网络程序的进出状况, 并针对可疑的程序进行拦截查看?	38
Q14 如何对可疑的程序在网络存取时进行阻挡, 不让它运行?	38
Q15 如何让我来决定哪些程序可以进行网络存取, 哪些不行?	38

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?	54
Q17	如何依照自己的网络状况与需求来制定专属的防火墙规格?	54
Q18	如何对已知木马程序所用的端口进行阻挡?	54
Q19	我有使用网络防护程序 (或防火墙软件), 但经常不断出现某个端口被扫描 (或要连接) 的信息, 实在烦不胜烦, 要如何有效阻挡而且不会弹出信息来烦我?	54
Q20	如何查看与判断当前是否正有黑客连接到我的电脑?	66
Q21	如何查看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?	66
Q22	如何关闭当前正在进行的可疑连接, 并干掉该连接的程序?	66
Q23	黑客如何偷用你的无线网络? 哪些原因让无线网络门户大开?	75
Q24	黑客入侵无线网络后会造成哪些问题?	75
Q25	如何有效防范黑客偷用我的无线网络? 有哪些防护方法? 各有何缺点? 如何补救?	75

Part 3 Windows 系统防毒防黑

(AntiVirus and AntiHacker for Windows)

入侵的基本原理与对象	118
黑客或病毒通过 Windows 的入侵流程	118
端口 139 的防护	120
磁盘共享防护	121
默认共享漏洞防护	121
RPC 防护	121
FTP 防护	121
Telnet 防护	121
终端机服务防护	122
漏洞修补与防护	122
浏览器与电子邮件防护	122
死机攻击防护	123
恶意信息防护	123
讨论与研究	123
Q26 如何关闭端口 139, 杜绝黑客利用此管道入侵?	125
Q27 防止黑客通过端口 139 入侵 Windows, 有哪几道防御措施?	125

Q28	我需要与其他电脑进行网络连接, 所以必须打开端口 139, 这时如何防止黑客入侵呢?	125
Q29	我的电脑必须打开磁盘共享, 这时该如何有效防止黑客入侵?	125
Q30	如何防止黑客利用病毒将我的磁盘设置成共享或设置成可读写?	152
Q31	如何防止黑客利用病毒将磁盘共享密码设置成不必输入密码就可进入?	152
Q32	如何有效防止黑客猜中磁盘共享密码?	152
Q33	如何修补 Win9x 与 WinME 的资源共享密码漏洞?	152
Q34	如何防止黑客在 WinVista、WinXP、Win2k 电脑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?	168
Q36	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?	168
Q37	如何防止黑客将默认共享打开?	168
Q38	为什么电脑有终端机服务与 Telnet 服务, 我却没发现?	173
Q39	如何查看我的电脑是否提供有终端机服务与 Telnet 服务?	173
Q40	如何防止黑客打开我电脑的终端机服务与 Telnet 服务?	173
Q41	如何彻底关闭我电脑的终端机服务与 Telnet 服务, 杜绝黑客使用它们入侵?	173
Q42	为何我在上网时经常出现奇怪的广告或垃圾信息窗口?	178
Q43	如何让自己的电脑完全不再收到 Internet 上任意散发的垃圾信息?	178
Q44	Windows 中所提供的系统服务中, 有哪些可能会被黑客利用? 会使用在哪些黑客行为上? 如何彻底有效地防止?	181
Q45	什么是远程运行命令 at? 如何防止黑客利用 at 命令运行你电脑中的各种程序文件? 如何关闭 at 远程运行命令?	181
Q46	什么是远程注册表服务? 如何防止黑客利用远程注册表服务更改或破坏你 Windows 系统的注册表? 如何关闭远程注册表服务?	181
Q47	什么是资源共享服务? 如何防止黑客利用资源共享服务来入侵我的磁盘或文件夹? 如何关闭资源共享服务?	181
Q48	如何对 Windows 系统的漏洞进行修补防护?	189
Q49	如何对重要文件夹与文件隐藏或加锁, 万一不幸被黑客入侵才不致造成重大伤害或被偷取重要数据?	189
Q50	Windows 系统有文件与文件夹的加密功能吗? 它有什么缺点? 为何不建议使用?	189

Part 4 木马、间谍、恶意、傀儡、僵尸程序、病毒—防护与歼灭 (Search and Destroy for Trojan、Spyware、Bot、Zombi、Virus etc.)

- Q51 木马、恶意或间谍程序、傀儡或僵尸程序、后门程序、跳板程序、病虫是什么？与病毒有何差别？它们可以帮黑客做什么事？如何对它们进行防护？.....199
- Q52 如何有效地预防木马、恶意或间谍程序、傀儡或僵尸程序、后门程序、跳板程序、病虫进入我的电脑中？.....203
- Q53 黑客通常使用哪些方式将木马、恶意或间谍程序、傀儡或僵尸程序、后门程序、跳板程序、病虫.....植入被黑电脑或服务中？.....203
- Q54 如何有效测试与查看下载的文件是否包含木马、恶意或间谍程序 (含批处理文件与项文件)、傀儡或僵尸程序、后门程序、跳板程序、病虫、病毒等？.....207
- Q55 我下载的文件是压缩文件，这样可以查看出其中是否含木马、恶意或间谍程序 (含批处理文件与项文件)、傀儡或僵尸程序、后门程序、跳板程序、病虫、病毒等？.....207
- Q56 使用杀毒软件或网络防御程序查看木马、恶意或间谍程序 (含批处理文件与项文件)、傀儡或僵尸程序、后门程序、跳板程序、病虫、病毒等，要注意哪些地方？.....211
- Q57 若杀毒软件或网络防御程序发现了木马、恶意或间谍程序 (含批处理文件与项文件)、傀儡或僵尸程序、后门程序、跳板程序、病虫、病毒等，要怎样处理最好？.....211
- Q58 需要杀毒软件或网络防御软件不断监控系统吗？如何使用才会有最佳的效果，也不影响系统性能？.....211
- Q59 如何查看或找出你的电脑是否被植入木马、恶意或间谍程序 (含批处理文件与项文件)、傀儡或僵尸程序、后门程序、跳板程序、病虫、病毒等，然后将它彻底干掉？ 227
- Q60 被黑客植入的木马、恶意或间谍程序、傀儡或僵尸程序、后门程序、跳板程序、病虫、病毒.....都藏匿在哪些地方？如何找出来砍头？.....231
- Q61 木马、恶意或间谍程序、傀儡或僵尸程序、后门程序、跳板程序、病虫、病毒.....有哪些方法设置一进入 Windows 就自动运行？.....231
- Q62 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、恶意或间谍程序、傀儡或僵尸程序、后门程序、跳板程序、病虫、病毒等？.....231
- Q63 如何查看目前正在运行的 EXE 或 DLL 程序，找出可疑的程序将它干掉？.....263
- Q64 为何杀毒软件或我自己操作都无法将 DLL 木马、恶意或间谍程序、傀儡或僵尸程序、后门程序、跳板程序、病虫、病毒.....从电脑中卸载？.....263
- Q65 经过伪装或整容后的木马、恶意或间谍程序、傀儡或僵尸程序、后门程序、跳板程序、病虫、病毒.....要如何辨识出来，然后将它们彻底终结掉？.....271

Q66	如何对网络数据包进行监控、记录与分析,找出可能藏匿在你电脑中的不速之客?	273
Q67	我不是网络专家,对网络数据包不了解,该如何判断与分析?	273
Q68	如何对注册表 (Registry) 进行监控,找出可能藏匿在你电脑中的不速之客?	273
Q69	黑客会利用哪些方法来偷取各类帐户密码或网络中传递的信息?	279
Q70	哪些方法可以有效预防与阻挡键盘测录、数据包截取木马偷取我的数据?	279
Q71	如何让各种键盘测录木马 (含遥控软件的键盘监控功能) 完全无用武之地?	279
Q72	发现键盘测录、数据包截取木马时,要如何进行紧急补救措施?	279

Part 5 浏览器、邮件、实时通信、聊天室的毒黑防护

(AntiVirus and AntiHacker Browser, E-Mail, Instant Messenger and Chat Room)

Q73	电子邮件通常会受到哪些方式黑客或病毒的入侵与攻击?如何各个击破?	287
Q74	如何避免受到邮件炸弹或一堆信件的攻击?	293
Q75	受到邮件炸弹或一堆信件的攻击时如何脱困?	293
Q76	若有人发一大堆的信件给我,要如何解决?	293
Q77	有哪些方法可以防止与避免被他人截取信件?	301
Q78	若发现被他人截取信件要如何进行补救措施以减少可能的损害?	301
Q79	如何查看信件中所附加的文件中是否有木马、病毒程序或各类破坏项、批处理文件?	305
Q80	如何对信件中的 Java 恶意源码进行防护?	311
Q81	如何避免受到窗口炸弹或其他 Java 恶意源码的攻击?	311
Q82	我受到窗口炸弹的攻击,一打开信件程序就会不断地冒出许多窗口,根本无法收信与寄信,要如何解决?	311
Q83	如何对网页或邮件中的 ActiveX 恶意源码进行防护?	320
Q84	通常黑客利用 ActiveX 程序进行哪些恶意行为?	320
Q85	如何避免受到 ActiveX 恶意源码的攻击?	320
Q86	如何对信件中夹带的批处理文件进行判断与防护?	328

Q87	为何许多杀毒软件或网络防御程序无法找出批处理文件病毒?	328
Q88	如何找出某一封电子邮件是从哪个国家的哪个地区寄出来的?	330
Q89	如何找出某个邮件地址是在哪个国家或哪个地区?	330
Q90	如何找出发信者的寄送信件时的 IP 地址?	330
Q91	为什么所有程序 (或有些程序) 都无法运行?	340
Q92	为什么控制面板中的所有项目 (或部分项目) 都无法运行, 而且还出现未找到的信息? 如何解决?	340
Q93	为什么在开始菜单中的运行不见了? 如何恢复?	345
Q94	为什么注册表编辑器不可用? 为什么注册表项文件 (.reg) 无法运行? 如何解决?	345
Q95	我知道更改某个项值就可将被禁用的注册表编辑器恢复使用, 但就是无法打开它, 要如何更改? 而且我也无法运行恢复正常的项文件, 要如何恢复注册表编辑器可以使用?	345
Q96	通常浏览器会受到哪些方式的黑客攻击或病毒入侵? 如何防护? 有什么彻底有效的解决方法?	349
Q97	什么是网页钓鱼法 (Phishing)? 黑客如何利用它来窃取各种账户与密码? 如何防护?	349
Q98	有哪些方法可以对各种假冒网页 (网页钓鱼, Phishing) 进行有效防护?	355
Q99	如何借由网站的相关信息来判断是否为仿冒的假网页?	355
Q100	我的 IE 每次打开会自动连接到某个网站, 无法改回来, 要如何解决?	363
Q101	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掉, 要怎么办?	363
Q102	我的 IE 有许多功能被关闭 (如右键菜单、Internet 属性、高级设置、查看信件源文件等都不可用), 如何打开?	363
Q103	IE 工具栏被加入指向某网站的按钮, 要如何将它去掉?	363
Q104	如何找出与干掉藏匿在我电脑中偷改 IE 各项设置的可恶程序?	363
Q105	如何预防我的 IE 浏览器被恶意网页或程序绑架或更改任何设置? 要怎么做?	363
Q106	如何防范木马、恶意或间谍程序、傀儡或僵尸程序、后门程序、跳板程序、病虫、病毒等利用邮件程序或浏览器漏洞进行入侵?	374
Q107	如何快速对 IE 或 Windows mail (或 Outlook Express) 漏洞进行修补?	374

Q108	如何对实时通信软件, 如Windows Live Messenger(MSN)、Skype、雅虎实时通、ICQ、QQ进行有效防毒防黑?	380
Q109	实时通信软件可以禁止下载文件吗? 要如何做?	380
Q110	如何彻底禁用各种实时通信软件?	380

Part 6 网络服务器的防毒防黑

(AntiVirus and AntiHacker for Internet Server)

入侵或攻击方式	384
安全与防护	390
找出幕后的黑手 (黑客的追踪与研究)	394
Q111 什么是病毒? 它有何破坏与影响?	395
Q112 病毒是如何寄生、扩散与攻击? 如何有效防护它?	395
Q113 什么是拒绝服务攻击? 它会造成哪些影响?	399
Q114 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?	399
Q115 什么是分布式攻击 (DDoS)? 它与一般拒绝服务攻击 (DoS) 有何不同?	399
Q116 什么是 SMB 缓冲区溢出漏洞? 如何修补它?	411
Q117 如何对自己的服务器进行测试查看, 找出可能的漏洞?	419
Q118 如何查找 Windows 系统、IIS、Apache、SQL 服务器是否有新的漏洞出现? 如何修补?	419
Q119 如何为网络服务器打造专属的防火墙?	427
Q120 如何从安全日志中判断是否有黑客或病毒入侵?	430
Q121 如何查看与判断系统日志、任务计划记录、IIS 日志?	430
Q122 如何判断安全日志是否被黑客删除?	430
Q123 如何有效防止安全日志被黑客删除或修改?	430
Q124 如何追踪与找出黑客的所在, 进一步找出黑客是谁?	442
Q125 黑客有哪几种方式隐藏自己的 IP 来进行入侵? 如何追踪?	442

附录 A 端口列表.....	448
附录 B CurrPorts.....	449
附录 C Jetico 个人防火墙.....	450
附录 D Comodo 个人防火墙.....	456
附录 E TaskInfo.....	457
附录 F Startup.....	460
附录 G MailBell.....	461
附录 H Hide Folders XP.....	463
附录 I Spybot - Search & Destroy.....	466
附录 J Shadow Security Scanner.....	469
附录 K avast! Home.....	471
附录 L IPNetInfo.....	479
附录 M Packetizer.....	480
附录 N eMailTrackerPro.....	482
附录 O Netcraft Toolbar.....	483
附录 P Comodo VerificationEngine.....	484
附录 Q Arovax Shield.....	485
附录 R NetInfo.....	487

PART 1

防毒、防黑的认知与基本观念

Understand and Realize about AntiHacker, AntiVirus



Windows 防黑杀毒大作战

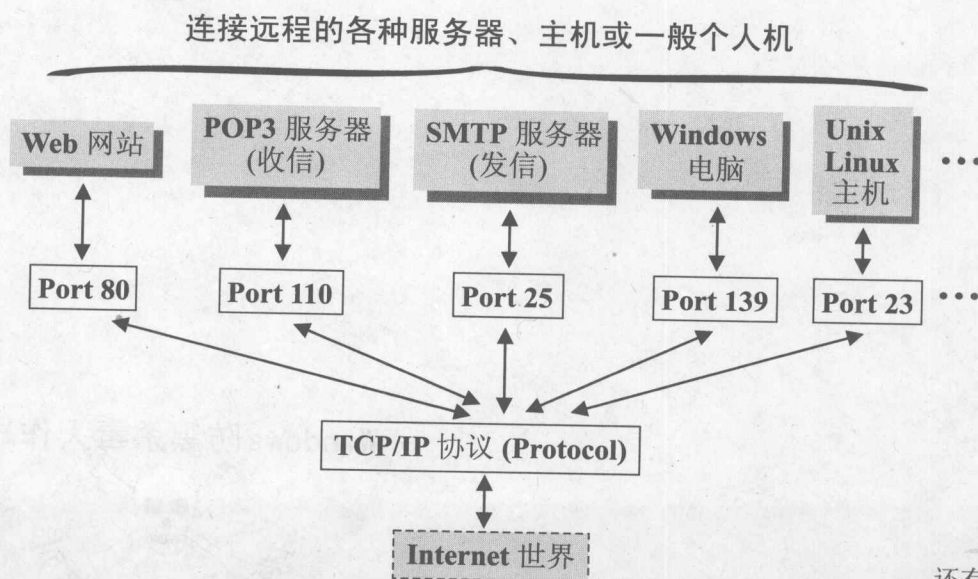


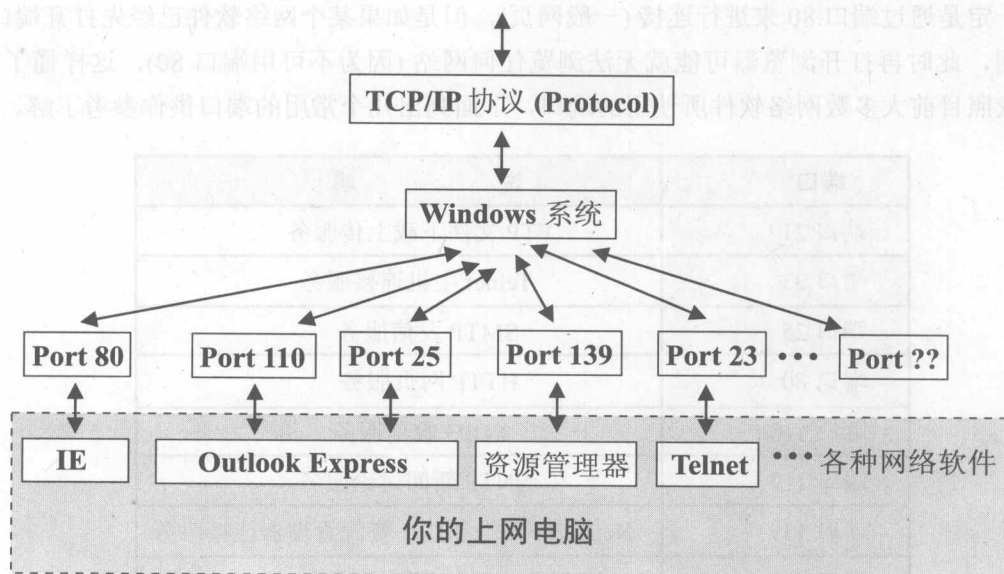
所谓知己知彼，才能百战百胜，要对网络黑客、各种病毒的入侵或攻击进行有效的防御，就必须先了解黑客与病毒入侵、攻击的基本观念，下手的目标与各种可能的黑客行为，然后再针对这些不同的方法与环节来找出围堵与防御之道，如此才能有效地将黑客与病毒阻绝于门外，达到有效的防护系统。

不过在我们收到黑客任务实战系列书籍的读者反应发现：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，我们先要了解一般上网电脑与 Internet 之间的关系，还有 Internet 世界的基本架构、端口的意义与角色……如此才能更清楚地了解黑客是如何使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、道听涂说，用不正确的或错误的观念来进行黑客防护，如此不仅事倍功半，甚至没有防护效果。

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……创建网络连接的关系，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地看出，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 (协议) 连接到 Internet 世界中。同样，远程的各种服务器、网站主机或一般电脑也是以相同的方式连接到 Internet 后，再与你的电脑完成连接，然后进行数据交换、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，说到这里许多读者可能有些疑问：网络软件如何决定打开哪些端口呢？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？

一般来说，每个网络软件都可以打开任何一个端口来使用 (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

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,此时再打开浏览器可能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,下面列出几个常用的端口供你参考了解。

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来使用的,所以不必太惊慌。例如 IE 在浏览网页时除了打开端口 80 外,也会打开数个其他端口来使用,而使用完后就会立刻关闭。

若要查看更多端口已经默认给哪些软硬件使用,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),在大多数时候大部分的端口根本就没被使用。