Vista XP 全适用

The Bible of Internet Security and Protection (Ultimate Version)

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!!

光盘内容
- 15套防毒、防骇、漏洞检查工具全面严防危险入侵!!

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.sciencep.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.sciencep.com

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

Part 1 防毒、防黑的认知与基本观念 (Understand and Realize about AntiHacker, AntiVirus)

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)

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.)

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)

Part 6 网络服务器的防毒防黑
（AntiVirus and AntiHacker for Internet Server）

PART 1

防毒、防黑的认知与基本观念

Understand and Realize about AntiHacker, AntiVirus

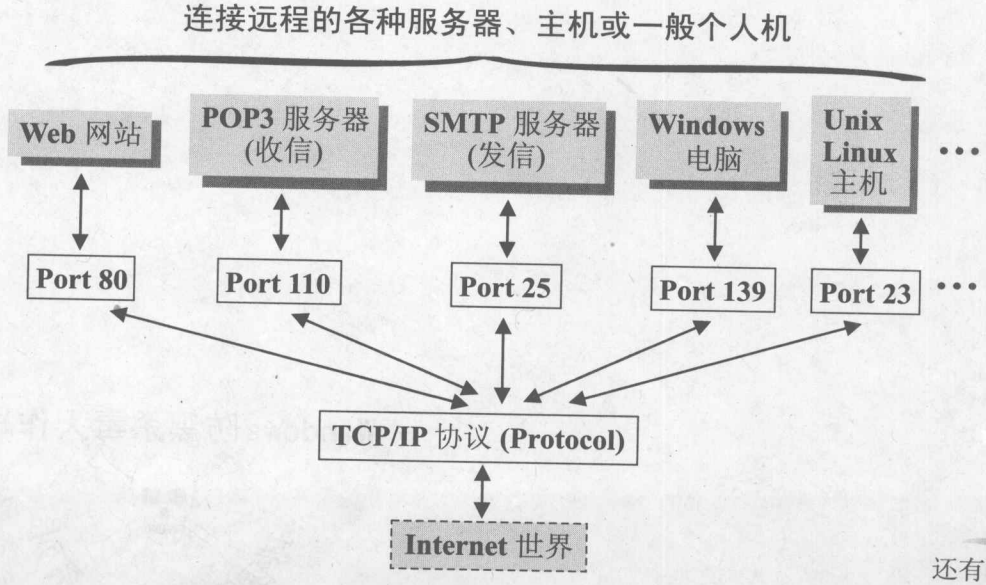
Windows防黑杀毒大作战

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。

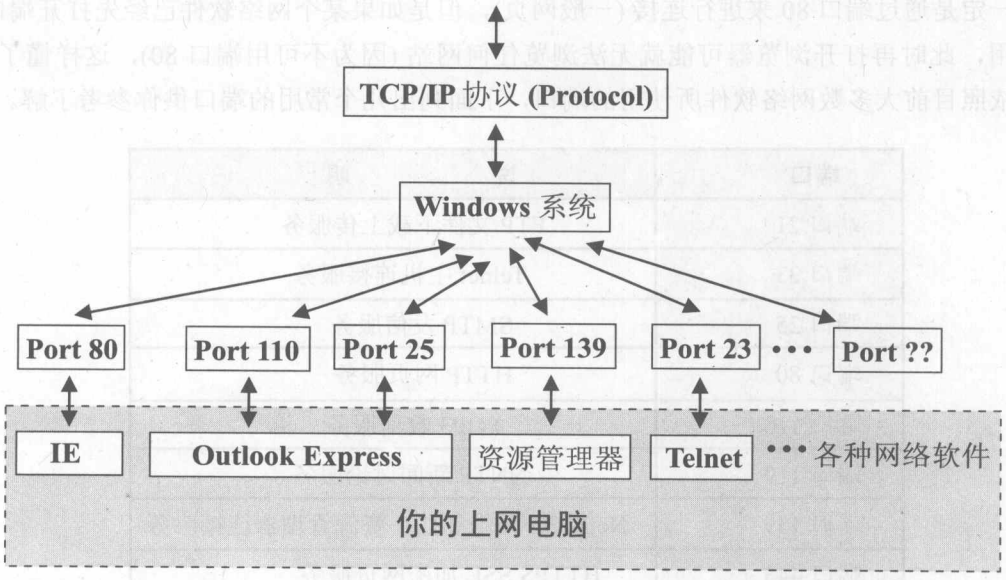
不过在我们收到黑客任务实战系列书籍的读者反应发现：许多读者的网络观念并不清楚，例如：以为某个端口打开就会被入侵或可入侵该电脑、使用某种方法就一定可以入侵他人电脑或破解密码等诸如此类严重的错误观念，因此在研究黑客的各种行为之前，我们先要了解一般上网电脑与 Internet 之间的关系，还有 Internet 世界的基本架构、端口 的意义与角色……如此才能更清楚地了解黑客是如何使用这些架构上的弱点与漏洞来进行入侵或攻击的，而不是人云亦云、道听涂说，用不正确的或错误的观念来进行黑客防护，如此不仅事倍功半，甚至没有防护效果。

✍ 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。



还有喔



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?……下面就逐一来为你解答。

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。