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

希望 Beijing Hope Electronic Press www.bhp.com.cn

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 —

Windows 黑客任务实战系列 程秉辉

防黑绯毒擒木马之绝命追杀 第二版

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！

Win9x.WinMe 完全适用 高手指点 Win2k.WinXP

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

Windows黑客任务实战系列 程秉辉

— 黑客防护实战 —

防黑绯毒搪木马之绝命追杀 第二版

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！

Win9X.WinMe 完全适用 高手指点 Win2k.WinXP

科学出版社
www.sciencep.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的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 开本：787×960 1/16

2006 年 4 月第一次印刷 印张：32 1/2

印数：1-5000 册 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
EMail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 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）

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）

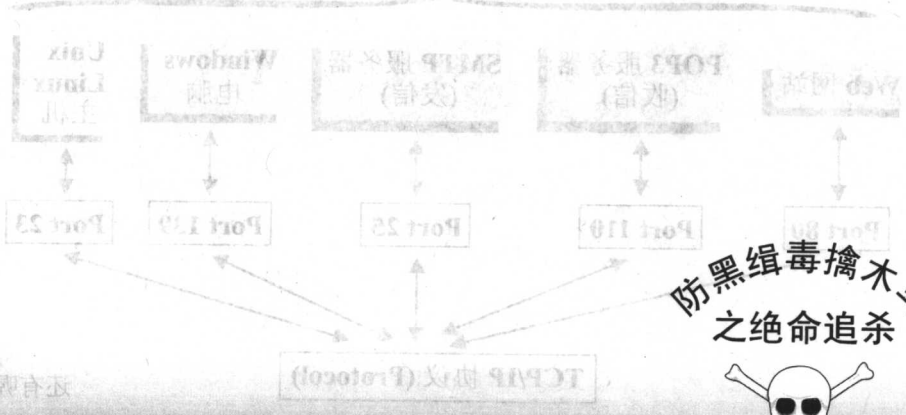
Part 6 网络服务器的黑客病毒防护
（Virus and Hacker Defense for Internet 服务器）

附 录

PART 1

病毒入侵观念、下手目标与黑客行为

Internet Concept and Hacker, Virus Intrusion



防黑绝毒擒木马
之绝命追杀

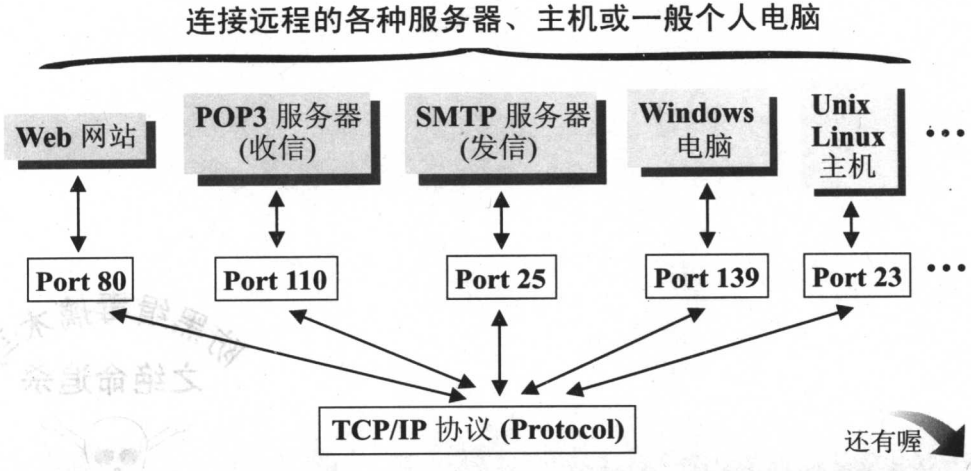
菜鸟解难 DIY 系列

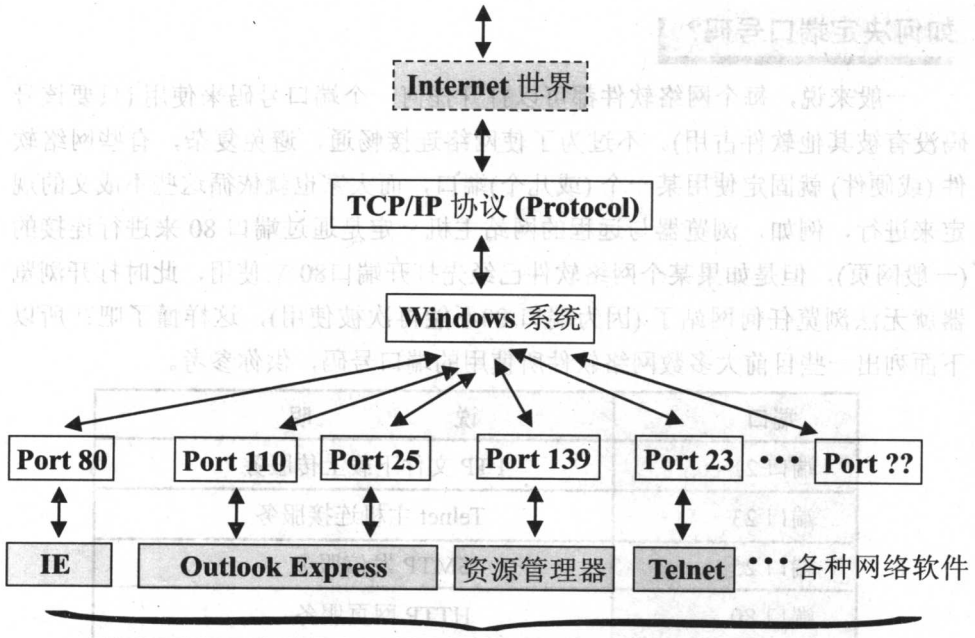
知己知彼，百战百胜。要对网络黑客的入侵或攻击进行有效地防御，就必须先了解黑客入侵、攻击的基本方法，下手的目标以及各种可能的黑客行为，然后再针对这些不同的方法和环节来找出围堵与防御之道。如此才能有效地将黑客阻拦于门外，以保护我们的系统。

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。





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?……下面就逐一来为你解答。

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。