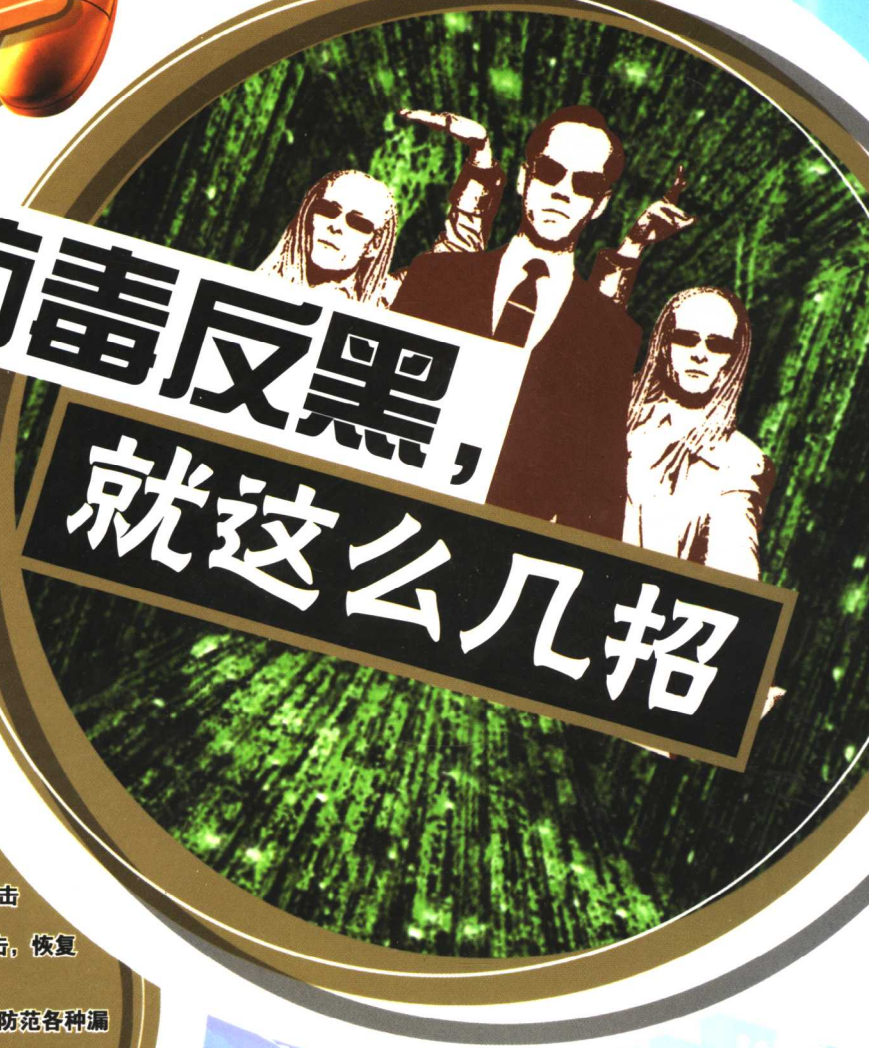
58分钟的视频教程演示了几个典型的防毒反黑案例
超值赠送长达88分钟的Windows XP多媒体教程

了解黑客的攻击方式，
拒绝黑客攻击！

电脑秘笈
量贩店

防毒反黑，就这么几招

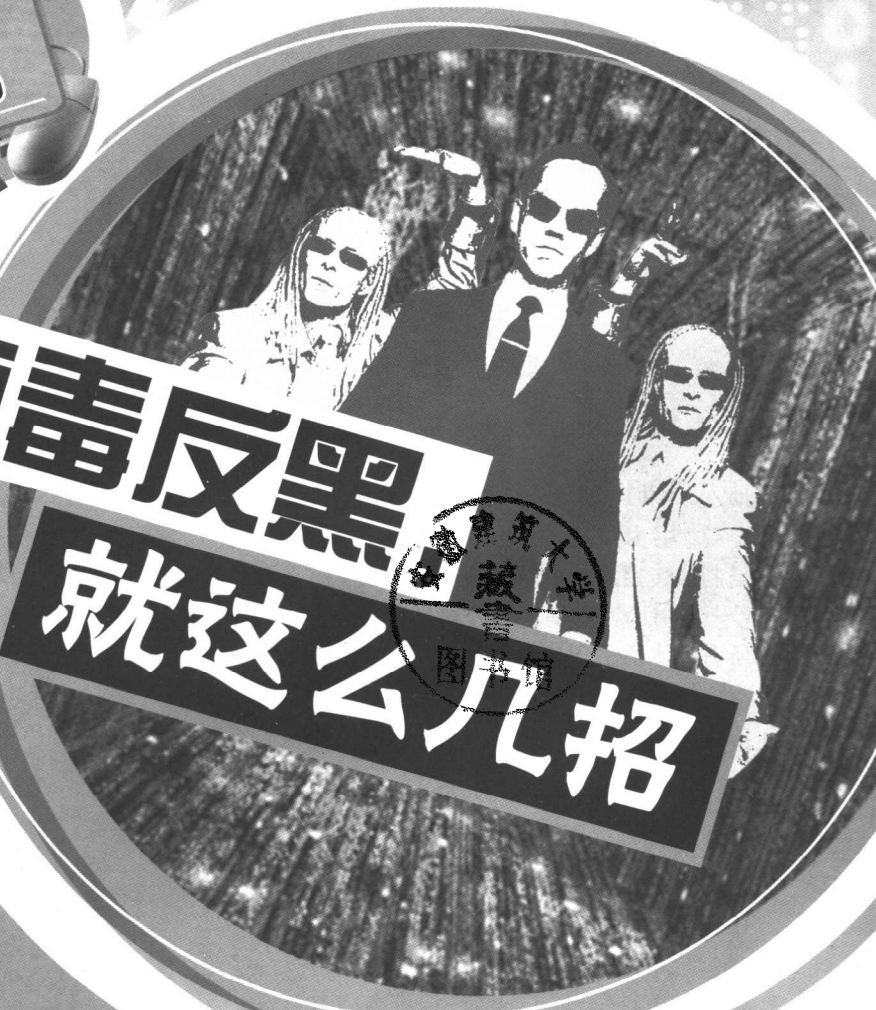
蔡勇 钱兆丰 何正宏 编著



- 准确判断是否感染病毒和木马，拒绝病毒和木马的攻击
- 完全防范QQ、电子邮件攻击，恢复被恶意网页代码篡改的系统
- 修复系统和应用软件漏洞，防范各种漏洞攻击
- 深入探讨扫描、拒绝服务攻击等高级攻击手段，并针对自己的计算机定制防火墙

中国电力出版社
www.infopower.com.cn

电脑秘笈
量贩店



防毒反黑就这么几招

蔡勇　钱兆丰　何正宏　编著

中国电力出版社
www.infopower.com.cn

内 容 简 介

本书系统介绍了计算机病毒、网络安全相关技术知识，并详细讲解了黑客常用的攻击手段以及相应的防范措施，内容包括病毒、电子邮件、QQ、网页、木马、系统漏洞、密码破解、数据加密、扫描器、拒绝服务攻击、防火墙技术以及入侵检测等攻击与防范技术，实践性非常强。读者在阅读本书后，能够对病毒和黑客的攻防技术有比较系统的了解，从而更好地防范病毒和黑客的攻击。

本书附赠一张多媒体教学光盘，读者可以通过观看光盘中的操作演示，掌握几种典型的病毒和黑客防范手段。

本书实例丰富，深入浅出，非常适合广大网络爱好者学习，对网络管理员和系统管理员也有重要的参考价值。

图书在版编目（CIP）数据

防毒反黑，就这么几招／蔡勇，钱兆丰，何正宏编著. 北京：中国电力出版社，2005
（电脑秘笈量贩店）
ISBN 7-5083-3272-5

Ⅰ.防… Ⅱ.①蔡…②钱…③何… Ⅲ.计算机网络－安全技术 Ⅳ.TP393.08

中国版本图书馆 CIP 数据核字（2005）第 029545 号

策　　划：裴红义
　　马首鳌
责任编辑：马首鳌
责任校对：崔燕菊
责任印制：李志强

丛 书 名：电脑秘笈量贩店
书　　名：防毒反黑，就这么几招
编　　著：蔡勇　钱兆丰　何正宏
出版发行：中国电力出版社
　　地址：北京市三里河路 6 号　邮政编码：100044
　　电话：（010）88515918　传真：（010）88518169
印　　刷：汇鑫印务有限公司
开本尺寸：185 × 230　　印　张：22.25
书　　号：ISBN 7-5083-3272-5
版　　次：2005 年 6 月北京第 1 版
印　　次：2005 年 6 月第 1 次印刷
印　　数：1~5000
定　　价：32.00 元（含 1CD）

丛书序

学习电脑最重要的一点就是要能将所学到的知识灵活熟练地应用到生活和工作中，这也是电脑高手和初学者的本质差别。而要学习电脑知识，成为电脑专家，最重要的就是挑选一套知识全面、案例实用、查找方便、学习轻松的电脑图书。

为了满足广大电脑初学者的需求，中国电力出版社在总结畅销丛书《电脑狂人笔记》和《电脑技能十全劲补》的成功经验基础上，经过长期的市场调研和分析，组织了有丰富实践经验的高校专业教师和科研工作者倾心编写了《电脑秘笈量贩店》这套丛书。我们特意聘请外企专业培训讲师审读定稿，并为每本书精心制作了一张教学演示光盘，力求使读者能快速、全面掌握所需的电脑知识，并能将其熟练应用到日常生活和工作中去。

丛书的特点

学以致用： 书中对知识点的讲解主要通过日常生活和工作中的典型应用实例来进行，使读者不再只是简单掌握，而且还能够根据需要灵活应用这些知识点。

即学即用： 读者在遇到实际问题时，可以不必系统地学完本书，只要通过目录快速查找到相关知识点，参照教学实例进行操作，即可解决问题。

巧学活用： 本套丛书都配有教学光盘，读者可以参照光盘中的教学演示进行操作，学习和应用起来简单直观、易于掌握。

读者定位

- 电脑初学者
- 家庭电脑用户
- 上班族
- 电脑数码爱好者
- 电脑培训班

丛书内容

本套丛书包括：

- 《电脑特训基地——电脑入门全攻略》
- 《弹指神通——五笔打字高手速成》
- 《电脑百宝箱——常用工具使用指南》
- 《电脑梦工厂——电脑选购、组装与维护》
- 《电脑医生——电脑常见软硬件故障诊断与排除典型实例》
- 《网管特训基地——局域网组装、管理与维护》
- 《BIOS& 注册表完全攻略——设置、优化、安全、排障、维护、个性化典型实例》
- 《Windows 大玩家——系统安装、配置与优化全攻略》
- 《防毒反黑，就这么几招》
- 《全民刻光盘—— CD、VCD、DVD 光盘刻录全攻略》
- 《数码相机完全攻略》
- 《数码照片梦工厂—— Photoshop 数码相片处理典型应用》
- 《DV 梦工厂——数码摄像与处理典型实例》
- 《电脑影音梦工厂—— CD、VCD、DVD 影音转录、剪辑和烧录技巧》

丛书阅读指南

如果您是一名电脑的初学者，《电脑特训基地——电脑入门全攻略》将帮助您快速入门，熟练掌握电脑的基础知识、操作系统的使用技巧和办公软件的应用技能。此外，您还可以通过《弹指神通——五笔打字高手速成》一书来学习五笔字型输入法，提高自己的打字速度。

如果您想更进一步提升自己的电脑水平，成为电脑应用的专家，可以阅读《电脑百宝箱——常用工具使用指南》、《电脑梦工厂——电脑选购、组装与维护》、《电脑医生——电脑常见软硬件故障诊断与排除典型实例》、《网管特训基地——局域网组装、管理与维护》、《BIOS&注册表完全攻略——设置、优化、安全、排障、维护、个性化典型实例》、《Windows 大玩家——系统安装、配置与优化全攻略》、《防毒反黑，就这么几招》、《全民刻光盘——CD、VCD、DVD 光盘刻录全攻略》等书。

如果您是一名数码爱好者，可以通过学习《数码相机完全攻略》一书来掌握数码相机的使用方法、拍摄技巧、照片处理和打印输出。另外，《数码照片梦工厂——Photoshop数码相片处理典型应用》一书将全方位讲解数码照片的处理艺术，包括从相机导出照片，照片的浏览、缩放、旋转、裁切、调色等基本处理方法，以及消除红眼、调整曝光、拼接照片、去除背景、消除眼袋等修饰技术。如果您拥有或即将购买DV，可以阅读《DV梦工厂——数码摄像与处理典型实例》，该书将教会您如何选购DV，如何拍摄不同的场景，如何导出影片并进行编辑处理、刻录成 VCD 等。如果您对电脑影音感兴趣，可以阅读《电脑影音梦工厂——CD、VCD、DVD影音转录、剪辑和烧录技巧》一书，该书将教会您播放各种格式的影音媒体，并掌握它们之间的相互转换、剪辑和烧录技巧，特别是通过该书您将能从任何格式的媒体中将您喜欢的影音转换成MP3，导入到您的MP3随身听中。

从书的第2批出版计划将包括Office、Photoshop、Flash、Dreamweaver、3ds max、VB、VC、C#、Java等书，帮助您成为相关领域的专家。

结束语

全面、实用的知识内容，细致入微的讲解，大量的典型应用案例，轻松愉快的学习方式，直观的教学光盘，精美的印装质量，造就出了《电脑秘笈量贩店》这套高品质的电脑丛书，希望它能带领每一位读者轻松成为电脑应用高手。

中国电力出版社
2005.1.1

前　言

Internet 的高速发展使得黑客的攻击行为也逐步升级，采用适当的安全技术已成为保证网络系统正常运转的必要条件。从功能的角度来讲，绝对孤立的计算机，即不与外界发生任何信息交互的计算机，相对来说是安全的。然而，在现实生活中，这是不大可能的，计算机不是通过移动载体与外界发生信息交互，就是通过网络进行信息的相互交换。由于各种操作系统、有关软硬件系统的缺陷以及各种系统管理方面的漏洞，导致了许多安全隐患，使得计算机系统经常受到病毒和黑客的攻击，出现了许多严重的安全问题。

本书是一本关于计算机病毒防治、网络攻击与防御的入门普及书，侧重于对攻击者所采用的技术和工具进行分析，并提出合理的防御策略，一切以实用性为中心来进行组织，而不是对原理进行枯燥乏味地阐释。本书既能为那些被网络安全所困扰的人排忧解难，也能使所有普通用户走向通往计算机安全领域的大门。

本书共分为 14 章，从各个方面讲述了常见的黑客攻击方法及相应的防范措施。

第 1 章　对病毒的相关概念、计算机病毒的预防与清除方法以及一些常见病毒的防治等知识进行了系统的介绍。

第 2 章　从本地邮箱的安全开始，对黑客邮件攻击与防范、Webmail 攻防、电子邮件炸弹进行了详细的介绍。最后，对电子邮件的一些注意事项和安全措施进行了汇总。

第 3 章　对 QQ 与聊天室的一些安全隐患。常见的攻击措施以及相应的防御方法进行了深入的介绍。

第 4 章　详细介绍了通过网页浏览对操作系统、浏览器造成的攻击以及相应的防范方法。最后，还对 Web 欺骗攻击与防范进行了叙述。

第 5 章　首先对一些典型的木马（冰河、广外女生、灰鸽子、广外幽灵）攻击与防范方法进行了详细的介绍，然后还对木马的种植、木马的防杀技术进行了系统的介绍。

第 6 章　把网络攻击的步骤分为攻击准备阶段、攻击实施阶段、攻击善后工作 3 个阶段，并对这些阶段的具体内容进行了详细描述。最后，通过一个具体实例的讲解来进一步深化读者的认识。

第 7 章　首先介绍了选择安全密码的注意事项，然后对 Unix 密码、Windows 密码的破解方法进行了详细介绍。最后，还对远程密码破解工具——流光进行了详细描述。

第 8 章　对一些常用的扫描器工具（扫描器之王——Nmap、漏洞检查利器——Nessus、大范围扫描工具——X-Scan）进行了详细介绍。最后，还介绍了 Sniffer 的攻击与防范。

第 9 章　首先对拒绝服务攻击的一些基本知识进行了概述，然后介绍了几种常见的拒绝服务攻击及其防御方法。最后，对最新的拒绝服务攻击方式——DDoS 的原理、攻击方法、防范方法进行了系统阐述。

第 10 章　主要对一些常见的系统漏洞（比如 Unicode 漏洞、IIS 漏洞、IDQ 漏洞、Web 漏洞）以及由其引发的攻击方法进行了系统而详细的描述，同时还给出了相应的防御措施。

第 11 章　对一些其他的攻击技巧（欺骗攻击、渗透攻击、中间人攻击、对路由的攻击）进行了系统介绍，并给出了相应的防范措施。

第 12 章　主要对攻击的善后工作（比如清除日志记录、设置后门等）进行了详细介绍。

第 13 章　首先对防火墙的一些基本知识进行了介绍，然后介绍了几种典型的防火墙。最后，还对防火墙的攻击与防御进行了详细描述。

第 14 章　主要对数据加密技术与入侵检测技术进行了系统描述，同时还介绍了一些相关的工具。

本书由蔡勇、钱兆丰、何正宏、刘绪崇等编写，由于时间紧迫，加之编者水平有限，错误和疏漏在所难免，恳请广大读者批评指正。

作　者

2005 年 1 月

目　录

第 3 章 即时聊天软件的攻击与防范

第 4 章 网页浏览攻击与防范

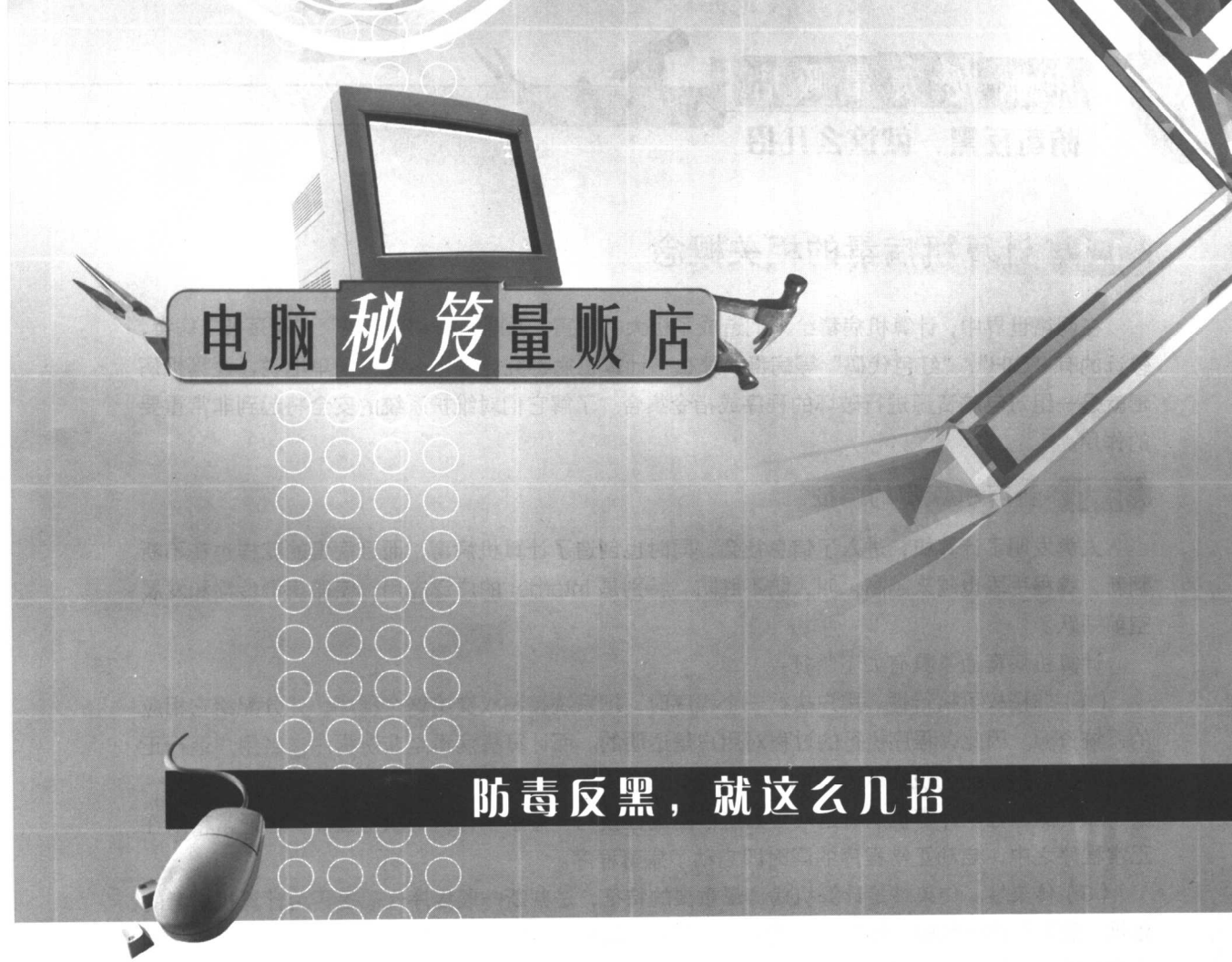
第 5 章 木马攻击与防范

第 11 章 其他攻击技巧

第 12 章　攻击的善后工作

第 13 章　防火墙技术

第 14 章 数据加密技术与入侵检测



第1章 计算机病毒

本章主要内容：

- 计算机病毒的相关概念
- 预防和清除计算机病毒
- 几种典型病毒的防治

1.1 计算机病毒的相关概念

在网络世界中，计算机病毒给人们造成了极大的危害，近期的如“冲击波”、“震荡波”病毒，较远的有“CIH”、“红色代码”等病毒。那么，计算机病毒究竟是什么呢？简单地说，计算机病毒就是一组对电脑资源进行破坏的程序或指令集合。了解它们对维护系统的安全将起到非常重要的作用。

1.1.1 计算机病毒的特征

人类发明了计算机，进入了信息社会，同时也创造了计算机病毒，而且病毒的花样也在不断翻新，编程手段也越来越高，叫人防不胜防。特别是 Internet 的广泛应用，使得病毒传播和发展空前活跃。

计算机病毒通常具有如下特征：

（1）非授权可执行性。用户执行一个程序时，把系统控制权交给这个程序，并分配给它相应的系统资源。因此，程序执行的过程对用户是透明的。而计算机病毒是非法程序，当用户运行正常程序时，病毒会伺机窃取系统的控制权抢先运行。

（2）隐蔽性。计算机病毒是一种具有很高编程技巧、短小精悍的可执行程序。它通常粘附在正常程序之中，启动正常程序的同时即启动了病毒程序。

（3）传染性。传染性是计算机病毒最重要的特征，是判断一段程序代码是否为计算机病毒的依据。病毒程序一旦侵入计算机系统就开始搜索可以传染的程序或者磁介质，然后通过自我复制迅速传播。目前，计算机网络日益发达，计算机病毒可以在极短的时间内通过 Internet 传遍世界。

（4）潜伏性。计算机病毒具有依附于其他媒体而寄生的能力。依靠病毒的寄生能力，病毒传染给合法的程序和系统后，不立即发作，而是悄悄隐藏起来，然后在用户未察觉的情况下进行传染。

（5）表现性或破坏性。无论何种病毒程序一旦侵入系统都会对操作系统的运行造成不同程度的影响。即使不直接产生破坏作用的病毒程序也要占用系统资源（如占用内存空间、占用磁盘存储空间以及系统运行时间等）。有些破坏性大的病毒程序则删除文件，加密磁盘中的数据，甚至摧毁整个系统和数据使之无法恢复，造成无可挽回的损失。因此，病毒程序的副作用一般表现为轻者降低系统工作效率，重者导致系统崩溃、数据丢失。

（6）可触发性。计算机病毒一般都有一个或者几个触发条件，满足其触发条件或者激活病毒的传染机制时，病毒就会进行传染。