电脑报 总策划

全程助学 多媒体教学

黑客攻防轻松入门

电脑报 编

黑客攻防真枪实弹

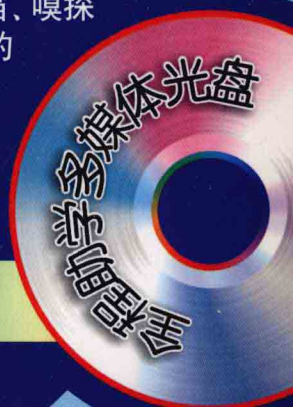
以实例为主，详细解析黑客攻防的基本知识和操作要领，让读者轻松迈进黑客的世界

黑客常用招法大曝光

全面展现各类黑客攻防技巧，从扫描、嗅探到远程控制……看看黑客是怎样炼成的

追踪黑客有高招

帮助读者快速地寻找线索，查找黑客行踪，让电脑远离黑客入侵



电脑报电子音像出版社

黑客攻防

轻松入门

《轻松入门》多媒体互动教学丛书编委：

主　编　黄　斌

编　委　杨　阳　李　勇　张　涛

邢政义　连　果　周一鹏

黄　翮　何　磊　胡　涛

电脑报

电子音像出版社

CEAP ELECTRONIC & AUDIOVISUAL PRESS

内容简介

本书及多媒体教学光盘是为初级读者量身定制而成的，本书以详细的实例为读者演示了黑客入侵的全过程，通过本书的学习，即使是对网络不熟悉的初学者也能轻松了解黑客的世界，包括侦察、扫描、远程控制、信息搜集以及掩盖踪迹等。

本书详细解析了黑客各阶段中所使用的工具和技术手段，以及相应的防御方法，并将零散的黑客知识系统地展现在读者的眼前，让读者在研究和学习过程中全面把握，少走弯路。本书不仅能够满足普通网络爱好者的应用需求，也适合网络安全从业人员及网络管理员研习之用。

警告：使用网络技术攻击他人电脑属于违法行为，读者切勿用本书介绍的方法对他人电脑进行恶意攻击，否则后果自负！

光盘内容

配套光盘采用全程语音讲解、情景式教学的方式，并与书中所涉及的内容互动，可以使读者更好更快地理解电脑应用中的各个难点，大大地提高学习效率。图书配套多媒体教程如下：

1.Windows远程协助视频教程
2.pcAnywhere远程控制视频教程
3.DameWare连接视频教程
4.IPC连接漏洞视频教程
5.开启Telnet后门视频教程
6.Telnet登录视频教程
7.黑洞开启摄像头视频教程
8.清除Office密码视频教程

书　　名：黑客攻防轻松入门
编　　者：电脑报
技术编辑：何　磊
封面设计：陈鲁豫
出版单位：电脑报电子音像出版社
地　　址：重庆市双钢路3号科协大厦
邮政编码：400013
对外合作：(023)63658933
发　　行：电脑报电子音像出版社
经　　销：各地新华书店、报刊亭
CD生产：四川省蓥山数码科技有限公司
文本印刷：重庆联谊印务有限公司
开本规格：787mm×1092mm 1/16　16印张　200千字
版　　号：978-7-900729-40-8
版　　次：2008年3月第1版　2008年3月第1次印刷
定　　价：28.00元(1CD+配套书)

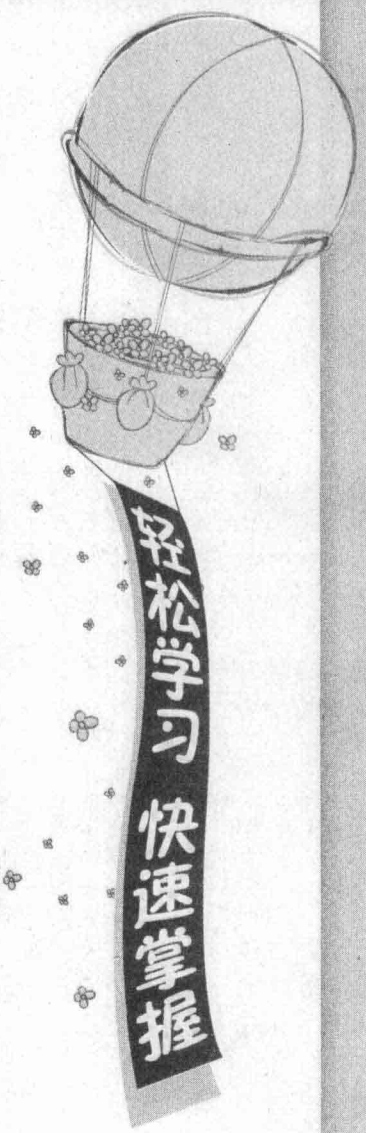
前言

FOREWORD

多媒体光盘互动教学丛书

电脑报自1992年创刊以来，已成为国内发行量最大的计算机专业报。由电脑报策划和编写的计算机图书，一直秉承了电脑报“通俗实用、注重实战”的风格，多年来深受广大读者的认可，成为读者首选的电脑读物。

如今电脑的普及和应用已深入千家万户，人们学习电脑更是有了新的要求。为此，电脑报特别为初学者量身定制了这套《轻松入门》双色图解丛书，旨在提倡新的学习模式，迅速帮助读者学用电脑、精通电脑。丛书除坚持电脑报一贯风格外着重强调“轻松学习，快速掌握”的基本理念。以帮助初学者快速掌握电脑应用的基本操作。



丛书包括以下分册图书

《学电脑轻松入门》	《电脑组装轻松入门》
《五笔与办公轻松入门》	《系统安装与重装轻松入门》
《Windows XP系统应用轻松入门》	《电脑故障排除轻松入门》
《Windows Vista系统操作轻松入门》	《组建局域网轻松入门》
《Office 2007办公应用轻松入门》	《Photoshop CS3图像处理轻松入门》
《Excel函数与图表轻松入门》	《黑客攻防轻松入门》
《电脑上网轻松入门》	

丛书特色一览

步骤分明、以图析文：丛书在介绍具体知识与操作过程时，图文并茂，细致入微。每一个步骤都以鲜明的色块表现，附有清晰的插图，读者在阅读的过程中能够直观、清晰地看到操作的效果，从而加深理解和掌握相关的操作和应用。

前言

FOREWORD

多媒体光盘互动教学丛书

书盘结合、互动教学：丛书配套有多媒体辅助教学光盘，光盘采用语音讲解、图文对照、动画演示等方式，紧密结合书中内容对各重点知识进行深入讲解，立体直观，形象生动。读者结合光盘进行互动学习，可起到事半功倍的效果。

版式新颖、轻松阅读：丛书采用了独特的版式编排，将基础知识和应用技巧有机地结合在一起。可以让读者系统掌握知识的同时提高了操作应用技能。

双色印刷、重点突出：丛书采用双色印刷整体页面美观舒适，同时又层次分明、重点突出，为读者提供了良好的阅读性。

本套图书由电脑报编委会总策划，配套的多媒体教程光盘由聚商网络制作。在此特别感谢以下作者的辛勤劳动、创意和支持：向光祥、王世高、李锐、张瀚文、马洪波、张轩涛、熊菲、胥阳、张剑、刘文舟、王星、钟声、杨文锐、肖光渝、黄继东。由于时间仓促，书中难免有疏漏和不妥之处，恳请广大读者不吝批评指正。

我们的联系信箱是：rumen@cpcwi.com，欢迎读者来信询问关于丛书及电脑应用中的各类问题，我们都将及时给予解答。

编者

2008年3月

目录

CONTENTS

多媒体光盘互动教学丛书

第一章 黑客基础入门

第二章 扫描网络与锁定目标

目录

第三章 Windows远程控制详解

目录

第四章 基于认证漏洞入侵Windows及其防范

第五章 Windows系统安全与防范

目录

第六章 木马植入攻防要略

第七章 突破限制与隐藏身份

目录

第八章 QQ盗号与安全防范

第九章 嗅探器截取信息与防范

目录

第十章 常用软件密码解除

目录

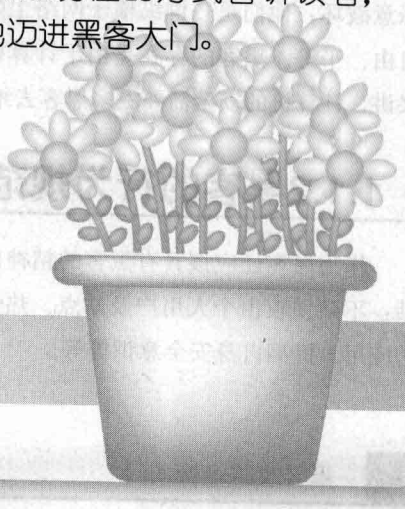
第十一章 网络安全与黑客防范

附录 黑客常用命令详解

Chapter 1

黑客基础入门

初学者在学习黑客知识的时候会遇到各种网络基础概念，例如 IP、端口、网关、映射等等，当读者遇上这一连串的概念问题时，会很迷茫，不知从何学起，从而对黑客技术产生畏惧感，这样会大大打击大家的学习积极性。作为新手学黑客的开篇，我们有必要将黑客基础的概念以浅显易懂的方式告诉读者，让读者轻松地迈进黑客大门。



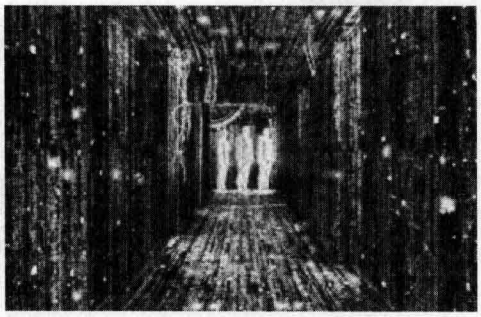
黑客是网络中的侠客，他们身怀绝技，自由地穿梭于网海之中；“黑”人电脑，又不留痕迹地飘然而去……正因为黑客在网络中表现出高超的网络攻防技巧，引发了人们对黑客的无限遐想！

1.1 揭开黑客神秘面纱

1.1.1什么是黑客

事实上，人们对黑客也存在不同的理解，有的人认为黑客是一群狂热的技术爱好者，他们无限度地追求技术的完美；而有的人认为他们肆意地破坏系统、盗取资料释放病毒，是网络世界的破坏者。在这里，我们没必要对黑客是非争论不休，我们所要知道的就是黑客究竟是什么！

“黑客”一词是由英语 Hacker 英译而来，是指专门研究、发现计算机和网络漏洞的计算机爱好者。他们伴随着计算机和网络的发展而产生、成长。黑客对计算机有着狂热的兴趣和执着的追求，他们不断地研究计算机和网络知识，发现计算机和网络中存在的漏洞，喜欢挑战高难度的网络系统并从中找到漏洞，然后向管理员提出解决和修补漏洞的方法。



黑客的出现推动了计算机和网络的发展与完善。黑客所做的不是恶意破坏，他们是一群纵横于网络上的大侠，追求共享、免费，提倡自由、平等。黑客的存在是由于计算机技术的不健全，从某种意义上来讲，计算机的安全需要更多黑客去维护。

Notice

“Hacker”这个称谓在早期是令人自豪、羡慕与崇拜的，直到现在还是有人以被称为“Hacker”而自豪,而骄傲！并且努力与那些所谓的“黑客”、“怪客”（Cracker）区分开来。

1.1.2黑客的行为规范和准则

作为黑客还应该具有黑客的精神以及行为规范。黑客行为主要包括：不随便攻击个人用户及站点、热忱帮助电脑初学者迅速掌握电脑的应用、提高自身安全意识等等。

新手点拨

学习黑客技术跟学习其他知识一样，都是要下功夫、要靠灵感、要靠自己思考的。很多黑客就是利用最基本的人性而攻破电脑，靠合法的程序而摧毁电脑的。所以知识不是死的，不是千遍一律的，要灵活掌握自己所学会的知识才是最重要的。

Notice

黑客必须在技术上有过硬的本领，并且热衷于解决问题，能够无偿帮助别人。

1.1.3如何涉足黑客世界

要涉足黑客的世界，首先得熟知网络，特别是IP与端口的概念，这些知识会贯穿于整个黑客的学习之中，关于这些基础知识，我们将在1.2和1.3节中介绍。黑客的攻击方式一般分为以下几种，具体内容我们将在本书的各个章节进行详细介绍。

No.01 信息搜索

黑客入侵的第一步首先是收集信息，信息搜集包括端口扫描、漏洞扫描、弱口令扫描等。只有尽可能多地获取目标主机的信息后，成功入侵的机会才越大。

No.02 漏洞入侵

由于程序设计的复杂性，人们会经常发现软件中的漏洞，漏洞对黑客来说是最重要的信息，黑客要经常学习发现的漏洞，努力寻找未知漏洞，并从多种漏洞中寻找有价值的、可被利用的漏洞进行试验，当然黑客的目的可能是通过漏洞进行破坏或者修补上这个漏洞。

No.03 种植木马

随着漏洞被发现，软件也会不断升级，如果漏洞被修补，黑客就需要采取其他入侵方法了，使用木马就是一个很典型的方法，事实上现在很多盗号与信息泄密都与木马有关，当木马控制了被黑主机后，黑客甚至可以完全夺取该主机的控制权，做任何想做的事情。

No.04 伪装

黑客对目标主机的任何操作都会被对方系统以日志的形式记录下来，如果黑客在没有伪装的情况下就冒然行动，是很容易被对方追查到行踪，所以黑客通常会伪装自己的IP地址以及身份标识。

No.05 密码破解

黑客一直热衷于破解各种系统或软件的口令密码，在没有其他办法的情况

新手点拨

黑客可能会对漏洞或被黑主机做如下事情：

获得系统信息：有些漏洞可以泄漏系统信息，暴露敏感资料，从而进一步入侵系统；

入侵系统：通过漏洞进入系统内部、或取得服务器上的内部资料、或完全掌管服务器；

寻找下一个目标：黑客往往充分利用自己已经掌管的主机作为工具，寻找并入侵下一个系统；

做一些有利于自己的事：如果漏洞主机有利用价值，他们可能会在该主机上植入木马或者后门，便于下一次来访。

Notice

通过代理上网是伪装IP最常用的方法，代理同样是突破局域网中人为限制的关键技术。

下，通常黑客会通过枚举猜解的方法来破解。

黑客的大多数活动都是在网络上进行的，想要熟悉网络，就不能不了解 IP 地址，黑客的入门就得从 IP 地址学起。

1.2.1什么是IP地址

我们都知道在邮寄信件时寄信人和收信人一般都拥有一个通信地址，只要按照这个通信地址就可以把信件安全送到收信者的手中。计算机之间的通信也是如此，IP 地址通俗地说就是每个计算机的通信地址。两个计算机之间的通信可以想象成下面的对话：

计算机 A：“你好，请把这个包裹（数据包）发到计算机 B，通信地址（IP）是这个。”

Internet 邮局：“好的，我会派邮递员把你的包裹送到这个通信地址（IP）的。”

经过 Internet 上的邮递员（路由器）的传递，将这个包裹成功地传到计算机 B 的通信地址（IP）上。

从上面的对话我们可以得出结论，那就是如果你的计算机连到网络上，要与其他机器进行数据的传输的话，就一定要有网络世界中的通信地址（IP 地址），否则跟不上网没有任何区别。

1.2.2公网IP与私有IP

在 IPv4 通信协议里面就有两种 IP 的类别，分别是：公网 IP（Public IP）和私有 IP（Private IP）。

No.01 公网IP

经由 INTERNIC（Integrated Network Information Center 专门负责 IP 分配事务的机构）所统一规划的 IP，有这种 IP 才可以直接连上 Internet；

No.02 私有IP

不能直接连上 Internet 的 IP，主要用于局域网。

如何区别公网 IP 和私有 IP 呢？这里有一个规则很好区分，当我们查询自己的 IP 时，发现地址在如下三个区域的话，则说明是私有 IP。

- 10.0.0.0 ~ 10.255.255.255

Notice

除了口令密码外，对于高强度的加密会将文件加密为暗文，这种需要算法的加密方法安全性通常是国家级的，黑客也很难破译。

1.2 认识IP地址

Notice

现有的互联网是在 IPv4 协议的基础上运行的。我们主要也是围绕 IPv4 协议进行讲述。IP 地址是由 4 个数据组成的，每个数据之间用“.”隔开。例如 192.168.0.1、61.153.2.54 这种形式。从这些数字我们可以看出 IP 地址是属于公网还是内部局域网的地址，稍候将会详细介绍。