揭开黑客神秘面纱，保障网络安全

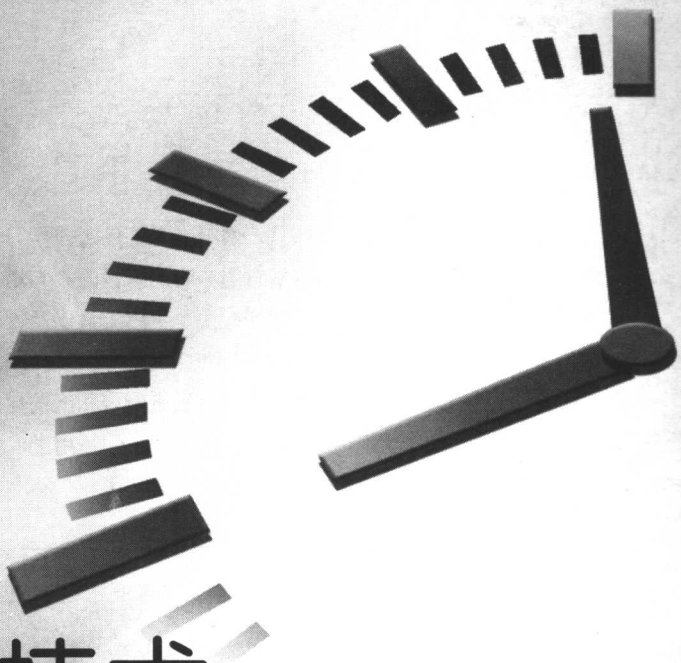
黑客攻防技术

24小时轻松掌握

武新华 主编
唐坚明 段玲华 编著

* 科学安排，学会不难
* 按图索骥，提高最快
* 边学边练，事半功倍

中国铁道出版社
CHINA RAILWAY PUBLISHING HOUSE



黑客攻防技术

24小时轻松掌握

武新华　主　编

唐坚明　段玲华　编　著

中国铁道出版社
CHINA RAILWAY PUBLISHING HOUSE

内 容 简 介

在当今这个科技发达的时代，网络在人们的工作学习中起着重要作用，但目前大多数人的网络安全意识还很匮乏，在遇到别有用心者的入侵时不知道如何应对。本书的主要目的就是让读者在尽可能短的时间内，了解黑客的起源、常用工具以及攻击方式，并在熟悉基本网络安全知识的前提下，掌握基本的反黑知识、工具和修复技巧，从而揭开黑客的神秘面纱，让广大用户对网络安全高度重视起来，从而采取相关的方法来制定相应的自救措施。

本书内容丰富全面，图文并茂，深入浅出，适用于广大网络爱好者，同时可作为一本速查手册，可用于网络安全从业人员及网络管理者。

图书在版编目（CIP）数据

黑客攻防技术24小时轻松掌握 / 武新华主编；唐坚明，段玲华编著. —北京：中国铁道出版社，2006.5
（24小时轻松掌握系列）
ISBN 7-113-07116-3

Ⅰ.黑… Ⅱ.①武…②唐…③段… 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（2006）第055649号

书　　名：黑客攻防技术24小时轻松掌握
作　　者：武新华　唐坚明　段玲华
出版发行：中国铁道出版社（100054，北京市宣武区右安门西街8号）
策划编辑：严晓舟　魏　春
责任编辑：苏　茜　荆　波　郑　双
封面设计：梵绅数字
封面制作：白　雪
责任校对：张国成
印　　刷：北京鑫正大印刷有限公司
开　　本：787×1092　1/16　**印张**：20.25　**字数**：478千
版　　本：2006年7月第1版　　2006年7月第1次印刷
印　　数：1～5 000册
书　　号：ISBN 7-113-07116-3/TP·1857
定　　价：28.00元


系列丛书
外行学电脑
一点通
轻松易学
一点就通
赠送光盘
动画教学
外行学电脑
一点通
入门篇
文军科技 编著
中国铁道出版社
外行学电脑
一点通
应用篇
外行学电脑
一点通
上网篇
外行学电脑
一点通
笔记本电脑
操作与维护
16开
双色印刷
外行学电脑
一点通
五笔打字
和排版
外行学电脑
一点通
Word
文档处理
外行学电脑
一点通
Excel
电子表格

24小时轻松掌握
系列图书

◇丛书特色

科学安排，学会不难
按图索骥，提高最快
边学边练，事半功倍

◇丛书简介

操作电脑脱胎换骨，学会电脑一点不难
——《电脑入门24小时轻松掌握》
管理电脑随心所欲
——《Windows XP 24小时轻松掌握》
突破每分钟100字，电脑打字训练手册
——《五笔打字24小时轻松掌握》
解读电脑DNA密码，轻松完成系统设置
——《Windows注册表24小时轻松掌握》
打通任督二脉，造就新一代电脑高手
——《电脑BIOS设置24小时轻松掌握》
揭开黑客神秘面纱，保障网络安全
——《黑客攻防技术24小时轻松掌握》
断网，死机，黑屏……不心慌
——《电脑故障排除24小时轻松掌握》

丛书序 只需 24 小时，轻松具备一种电脑技能

进入 21 世纪的你，如果还不能熟练地使用电脑，不能不说是一种遗憾。

电脑的世界是十分美妙的世界，我们通过 Internet 了解世界，通过 E-mail 和朋友们沟通，上网购买所需要的图书……电脑，越来越成为生活的必需品，给我们的工作、学习和生活带来了巨大的帮助。

只要会中文，就可以享受高科技带来的便利

可是，在今天，还是有不少读者朋友，不会使用电脑，或者说不能熟练地驾驭电脑，让电脑帮我们完成各种工作，体验电脑文化带给我们的神奇感觉，享受高科技的产品带给我们的便利。

很多读者向我们抱怨，电脑学习这么难，而且，没有足够的时间去学习……根据我们多年的教学经验，只要会中文，可以阅读中文书籍，就能够看懂电脑的中文应用界面，培养基本的电脑技能，并逐步地熟练。只要你能定期抽出一个小时的完整时间，认真地实践我们提供的技能培养计划，就一定可以成功地驾驭电脑，并可以体验学习新知识的快乐。

科学安排，学会不难

我们把常用的电脑技能，分解成一个一个的学习单元。只要能定期抽出一个小时的空余时间，按照本书的安排，学习其中一个单元，一个小时一点进步，一个小时一点提高。由慢到快，电脑技能很快就可以上一个新的台阶。

按照我们的学习安排，只要 24 小时，一定可以掌握一种电脑应用技能。这个时候，学习的流程安排和内容就相当重要。

根据作者多年的经验，我们在这 24 个小时里面的每一个小时，或者安排读者学习某种技能；或者让读者跟我们学做某个实例；或者让读者强化训练某项技能。这 24 个小时的安排串联起来，就是一张电脑技能的学习地图，它伴随读者探索电脑奥秘的全过程。加上一定时间的训练，一定能教会读者应用电脑，并熟练起来。

按图索骥，提高最快

针对任何一项电脑技能的学习，24 小时培养计划，犹如学习中的 24 级台阶，由作者精心设计。读者可按这个学习顺序，由浅入深，由易到难，逐步掌握好有用的电脑技能。

学习是一个由慢到快的过程。每个人的情况不一样，一般来说，前面的基础打好了，后面的学习速度就会越来越快。所以，在一些内容的安排上，

我们遵循了这个特点。在最后的几个小时的学习计划中，学习内容具有并列特性，读者可根据自己的需要选择学习的顺序。

另外，作为正文的补充，有的图书我们还提供了附录，供读者查询某些资料。

边学边练，事半功倍

学习电脑技能，还要讲究一定的技巧。有了完美的学习方案，还得有足够的练习。

根据我们的经验，电脑技能的学习，上机练习非常重要。所以，建议读者在学习的过程中，同时找一台电脑练习所学内容。

一本图书，一台电脑，一边学习，同时按书中所讲练习，可加深印象，更能巩固技能，越用越熟练，越用越体会到使用电脑的乐趣。希望我们的每一本书，加上读者的 24 小时自我训练，能使读者的电脑水平在某一个方面得到飞快地提升。

联系作者，答疑解难

每一个读者，都有不同的基础和学习经验。我们虽然设计了大多数读者的学习地图，但由于每位读者电脑配置不一定相同，学习碰到的问题也可能各不相同。所以，除了本书之外，我们特地开辟了读者答疑邮箱：beone2000@126.com。

如果读者在应用电脑的过程中碰到疑难问题，可以发邮件给我们，我们很乐意为您解答，并将典型问题放在下一版的图书中。

编 者

2006 年 5 月

前言

古时候，人们谈虎色变。而在科技发达的今天，人们则谈“黑”色变，是因为在网络用户中存在着一些“危险分子”——黑客。同时，人们的网络安全意识不够强，使这些黑客有机可乘。而本书就是让读者在短短 24 小时的时间里了解黑客的起源、黑客的基本工具和攻击方式，并在熟悉基本网络安全知识的前提下，掌握基本的反黑知识、工具以及修复技巧，从此不再害怕他们的侵扰。

为区别于市场上同类的反黑客类书籍，本书在写作上摒弃了同类书通常采用一本正经教学的方式，代之以丝丝入扣、生动曲折的故事情节和幽默风趣、闲话家常般的写作手法，使枯燥乏味的黑客攻防技术学习变得生动起来，让读者的网络安全应用技术随着对本书的阅读而逐步提高。

本书共分为如下四部分。

第一部分介绍关于黑客的基本知识，主要讲述黑客的行动方式和攻击方式，从而让读者熟悉黑客的攻击路径；掌握其根底并用准确的方法对付它，最终做到知己知彼，百战不殆。

第二部分着重讲述在平时应该怎样保护计算机和网络免受攻击，许多防毒和检测工具将出现在这里，除此之外，还有部分基本的网络安全知识做铺垫；可以防患于未然。

第三部分有两个阶段：首先会告诉大家如何确定自己的计算机或网络是否受到了攻击或者已经中毒；然后会告诉大家应该如何去修复计算机或网络，沉着应战，取得反击的胜利。

最后一部分，则是根据黑客的攻击方式和行为，精心挑选几个实例，再现“厮杀”场景，让读者对前面的知识理解得更透彻，做到学以致用。

本书充分地考虑了初学者的实际需要，对那些迫切想要保护电脑隐私、防病毒、防黑客的读者，通过学习本书能够轻松地掌握如何保护电脑隐私、防病毒、防黑客的方法。

本书适合经常上网但对网络安全和黑客知之甚少的人员阅读，也可作为计算机网络安全爱好者的自学教材，从而扩大作战的队伍，为计算机网络安全的正义而战。

编　者

2006 年 4 月

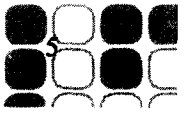
目 录

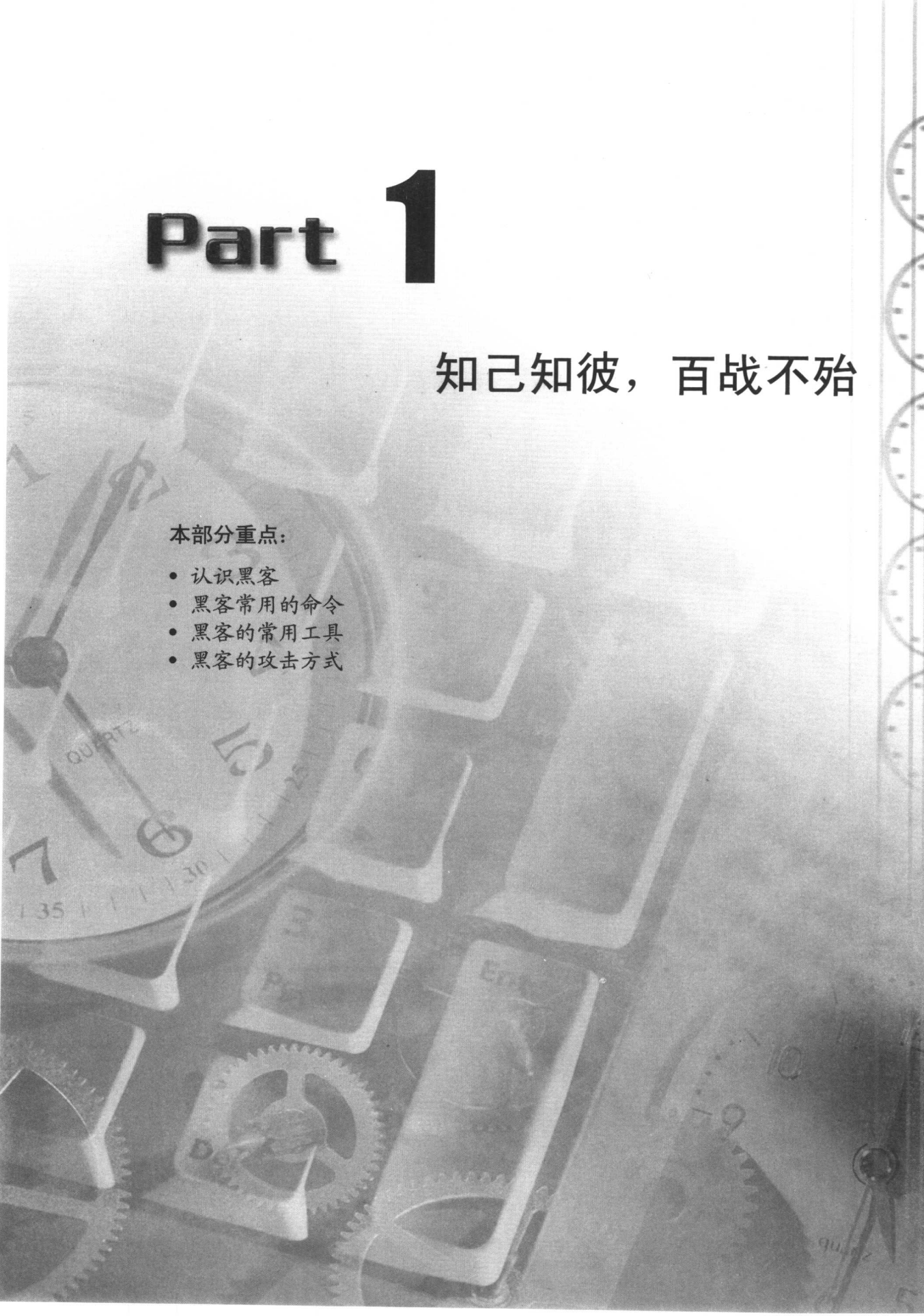
Part 1 知己知彼，百战不殆

Part 2 防患于未然

Part 3 切莫惊慌，沉着应战

Part 4 疆场厮杀 显我神威





Part 1

知己知彼，百战不殆

本部分重点：

- 认识黑客
- 黑客常用的命令
- 黑客的常用工具
- 黑客的攻击方式

第 1 小时 认识黑客

俗话说：害人之心不可有，防人之心不可无。知己知彼方能百战不殆，本书便是基于这样一个目的编写的。了解基础的网络知识、知晓通常的黑客攻击手段与常用黑客软件，从而用知识与技巧将自己的计算机和网络很好地保护起来，达到防患于未然的目的。

学习目的和重点：

- 黑客是什么
- 认识 IP 地址
- IP 地址的获得
- 供黑客进出的门——端口

1-1 黑客是什么

黑客是什么？黑客或许是网络里沿着庞杂的线路潜行的杀手，或许是在攻入你的系统后仅仅留下一纸建议便飘然离去的侠士。然而，随着计算机的普及、网络的流行、黑客工具的传播，有一些仅有黑客之名但无黑客之实的人，仅使用简单的工具，就能对一些疏于防范的电脑进行攻击，并在被侵入的电脑里为所欲为。当发现自己的密码被盗、资料被修改删除、硬盘成为一片空白之时，再想亡羊补牢，却为时已晚（窃取资料或系统崩溃通常会给他们带来成就感与快感）。

其实，许多时候，大多数黑客进行攻击的理由都是很简单的，正如黑客（Hacker）英语动词 hack 的引申含义为“干了一件漂亮的工作”：如想要在别人面前炫耀一下自己的技巧，或者是看不惯同事（同学）的某些做法，又不便当面指则，于是攻击他的电脑，更改他的桌面等；再比如想窥探某人的某些隐私等。这时候，进攻的目的并不是为了破坏，一般来讲也不会造成多大的损失，同样，也不需要多么高深的技术。

如果自己仅仅是一个经常上网者，就有可能会非常害怕自己的机器被别人“黑”了，其实完全不用太担心，在网络上，自己被黑的几率是很小的。但也不能因此而掉以轻心，最好还是做一些必要的预防工作，比如使用杀毒软件、安装防火墙等，同时了解一些黑客方面的知识，就会知道采取什么样的措施能够更有效地预防黑客的攻击了。

本书就是出于满足广大读者的这一需求而写的，因此，阅读本书并不需要具备多么高深的电脑知识，只要准备好自己的电脑，然后联上网就可以了。

也不排除某些别有用心者和某些仅仅只是出于好奇，利用遍布网络的“傻瓜”式工具进行攻击的攻击者，因为从某种意义上来说，他们并不代表真正意义上的黑客。

1-2 认识 IP 地址

每个人都有自己的名字，Internet 上的每一台网络主机是用域名来为其命名的，一个人可能

会有几个名字，域名的定义也同样如此。因此，在网上能真正标识主机的便是 IP 地址了（就好比每个人的身份证号是不会轻易因个人的名字改变而改变一样）。这样一来，域名就成了为用户使用 IP 地址指定的主机便于好记而起的名字。

由此可知，一般情况下只要利用域名或 IP 地址都是可以顺利找到主机的，除非是大家使用的网络没有联通。

因此，如果想要攻击某台电脑，就首先要确定所攻击的目标，也就是说要知道这台被攻击主机的域名或者 IP 地址，例如：www.heike.com 或 192.168.0.8 等。

1. 什么是 IP 地址

所谓 IP 地址其实就是在 Internet 上分配给每台计算机或网络设备的 32 位数字标识。在网络上，每台计算机或网络设备的 IP 地址都是全世界唯一的。

IP 地址的格式是 xxx.xxx.xxx.xxx，其中 xxx 是 0～255 之间的任意整数。

IP 地址分为固定 IP 和动态 IP，其中固定 IP 地址是长期分配给一台计算机或网络设备使用的 IP 地址，一般来说，采用专线上网的计算机才拥有固定的 IP 地址。而动态 IP 则是由于通过 Modem、ISDN、ADSL、有线宽频、小区宽频等方式上网的计算机，每次上网所分配到的 IP 地址都不相同，这就是动态 IP 地址。因为 IP 地址资源很宝贵，大部分用户都是通过动态 IP 地址上网的。

2. IP 地址的划分

互联网上的每个接口必须有一个唯一的 IP 地址，IP 地址长 32 位。Internet 地址并不采用平面形式的地址空间，如 1、2、3 等。IP 地址具有一定的结构，五类不同的互联网地址格式如图 1-1 所示。

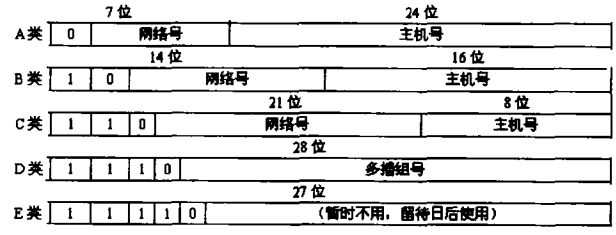


图 1-1　五类互联网地址

这些 32 位的地址通常写成 4 个十进制的数，其中每个整数对应一个字节。这种表示方法称作“点分十进制表示法（Dotted decimal notation）”。如笔者的系统就是一个 C 类地址，它表示为：222.137.158.102。区分各类地址的最简单方法是看它的第一个十进制整数。如表 1-1 所示列出了各类地址的起止范围。

需要再次指出的是，多接口主机具有多个 IP 地址，其中每个接口都对应一个 IP 地址。

表 1-1　各类 IP 地址的起点范围

类　　型	范　　围
A	0.0.0.0～127.255.255.255
B	128.0.0.0～191.255.255.255
C	192.0.0.0～223.255.255.255
D	224.0.0.0～239.255.255.255
E	240.0.0.0～247.255.255.255