精品丛书“24小时轻松掌握系列”
全新改版，重装上市

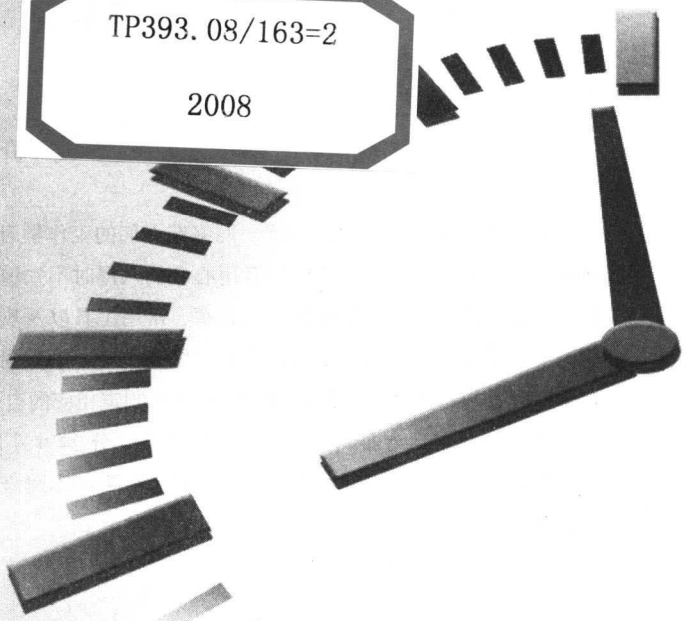
黑客攻防技术（第2版）

24小时轻松掌握

武新华　张慧娟　段玲华　编著

- 打破常规，24小时学习模式，科学高效。
- 层层递进，揭开黑客神秘面纱，知己知彼。
- 身临其境，实例再现攻防实战，学以致用。

中国铁道出版社
CHINA RAILWAY PUBLISHING HOUSE



黑客攻防技术24小时轻松掌握（第2版）

武新华　张慧娟　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，分 24 个小时的章节排版，让读者学习起来更轻松，步步为赢，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，张慧娟，段玲华编著. —2 版. —北京：中国铁道出版社，2007.12
（24 小时轻松掌握系列）
ISBN 978-7-113-08459-2

Ⅰ.黑… Ⅱ.①武… ②张… 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（2007）第 195561 号

书　　名：黑客攻防技术 24 小时轻松掌握（第 2 版）
作　　者：武新华　张慧娟　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　荆　波
责任编辑：荆　波　王　欣
封面制作：白　雪
印　　刷：三河市华晨印务有限公司
开　　本：787×1092　1/16　**印张**：19　**字数**：447 千
版　　本：2008 年 2 月第 2 版　2008 年 2 月第 1 次印刷
印　　数：1～6 000 册
书　　号：ISBN 978-7-113-08459-2/TP・2639
定　　价：29.00 元

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，还要有足够的练习。

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，同时按书中所讲进行练习，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。希望我们的这一本书，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：jb18803242@yahoo.com.cn。

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

2007 年 12 月

前言

古时候，人们谈虎色变。而在计算机和网络技术日益发达的今天，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，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。

本书为《黑客攻防技术 24 小时轻松掌握（第 2 版）》，我们在第 1 版的基础上，根据技术的发展和读者的意见，对内容和版式作了适当的修改，使第 2 版更完善，更实用。

内容共分为四部分：

第一部分 知己知彼，百战不殆

介绍关于黑客的基本知识，主要讲述黑客的行动和攻击方式，让读者熟悉黑客的攻击路径；掌握其根本并用准确的方法，最终做到知己知彼，百战不殆。

第二部分 深度攻击，全力防范

着重讲述在平时应该怎样保护计算机和网络免受攻击，防毒和检测工具的使用方法，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 切莫惊慌，沉着应战

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。

第四部分 疆场厮杀，显我神威

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。

全书充分地考虑到初学者的实际需要，对那些迫切想要保护计算机隐私、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计算机隐私、防病毒、防黑客的方法。

本书由武新华、张慧娟、段玲华编著。参与本书编写的还有曹燕华、安向东、李秋菊、陈艳艳、柳勇良、张鑫、李防、王英英、齐伟、张旭、欧阳代义等，在此一并表示感谢。

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。

最后需要提醒的是：

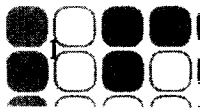
根据国家有关法律规定：任何利用黑客技术攻击他人的行为都属于违法行为，本书旨在希望读者阅读后能够做到“知己知彼”，更好的防护自己的计算机，切记一定不要以本书中介绍的黑客技术对他人进行攻击，否则后果自负。

编　者

2007 年 12 月

目 录

Part 1 知己知彼，百战不殆



Part 2　深度攻击，全力防范

Part 3 切莫惊慌，沉着应战

Part 4　疆场厮杀　显我神威

Part 1

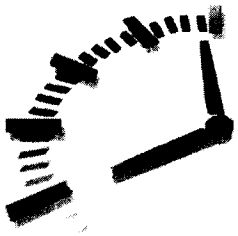
知己知彼，百战不殆

本部分重点：

- 黑客必知的网络知识
- 黑客常用的命令
- 黑客的常用工具
- 黑客的攻击方式

特别提醒：

根据国家有关法律规定，任何利用黑客技术攻击他人的行为都属于违法行为，本书旨在希望读者阅读后能够做到“知己知彼”，更好地防护自己的计算机，切记一定不要使用本书中介绍的黑客技术对他人进行攻击，否则后果自负！



第 1 小时 黑客必知的网络知识

学习目的和重点：

- 网络协议
- 服务器与服务端
- IP 地址于端口
- 系统与系统环境
- 系统漏洞

黑客（hacker）一词最初是给一位天才程序员起的术语，他能够把一个应用程序组合起来或拆开来解决问题。现今，黑客已被定义为非法搜索和渗透计算机网络访问和使用数据的人。黑客就好像一个计算机数据信息的窃贼，即不被允许便闯入一个系统，利用其窃取信息。无论哪种情况，黑客的最终目的都是发现并利用存储在网络上的信息。

“黑客”大体上应该分为“正”、“邪”两类，正派黑客依靠自己掌握的知识帮助系统管理员找出系统中的漏洞并加以完善，而邪派黑客则是通过各种黑客技能对系统进行攻击、入侵或做其他一些有害于网络的事情，因为邪派黑客所从事的事情违背了《黑客守则》，所以他们真正的名字应该叫“骇客”（Cracker）而非“黑客”（Hacker），也就是平时经常听说的“黑客”（Cacker）和“红客”（Hacker）。

无论那类黑客，他们最初的学习内容和掌握的基本技能都是一样的，即使日后他们各自走上了不同的道路，但是所做的事情也相差无几，只不过出发点和目的不尽相同而已。

无论是想攻击别人还是要防范别人，都需要对网络知识进行了解。

1-1 网络协议

当用户使用浏览器在 Internet 这个“高速公路”纵横驰骋时，需要用到诸如 Http、FTP 之类的传输控制协议来准确寻找资源，获取文件，这类传输控制协议就好比是公路上的交通标志一样，如果不了解它的含义，就无法到达希望去的地方。

网络中不同的工作站、服务器之间能相互传输数据，就是源于协议的存在。随着网络的发展，不同的开发商开发了不同的通信方式，为了使通信成功可靠，网络中的所有主机都必须使用同一种语言。因而必须制定严格的标准，定义主机之间每个包中每个字中的每一个位。这些标准多来自于多个组织的努力，约定好通用的通信方式（即协议），使网络间的相互通信变得更加容易。

在网络的各层中存在着许多协议，它是定义通过网络进行通信的规则。因此，接收方和发送方同层的协议必须一致，否则一方将无法识别另一方发出的信息，以这种规则规定双方完成信息在计算机之间的传送过程。

网络协议（Protocol）是网络上所有设备（网络服务器、计算机及交换机、路由器、防火墙等）之间通信规则的集合，它定义了通信时信息必须采用的格式和这些格式的意义。大多数网络都采用分层的体系结构，每一层都建立在其下层之上，向其上一层提供一定的服务，而把如何实现这一服务的细节对上一层加以屏蔽。一台设备上的第 *n* 层与另一台设备上的第 *n* 层进行通信的规则就是第 *n* 层协议。

网络协议使网络上各种设备能够相互交换信息。网络协议的本质是规则，即各种硬件和软件必须遵循的共同守则。

网络协议并不是一套单独的软件，它融入其他所有的软件系统中，因此可以说，协议在网络中无处不在。网络协议遍及 OSI 通信模型的各个层次，从非常熟悉的 TCP/IP、Http、FTP 协议，到 OSPF、IGP 等协议，数量有上千种之多。

对于普通用户而言，不需要关心太多的底层通信协议，只需要了解其通信原理即可。在实际管理中，底层通信协议一般会自动工作，不需要人工干预。但对于第三层以上的协议，就经常需要人工干预了，比如 TCP/IP 协议就需要人工配置它才能正常工作。

通俗地说，网络协议就是网络之间沟通、交流的桥梁，只有相同网络协议的计算机才能进行信息的交流。这就好比人与人之间交流所使用的各种语言一样，只有使用相同语言才能正常、顺利地进行交流。

从专业角度定义，网络协议是计算机在网络中实现通信时必须遵守的约定，也就是通信协议。主要是对信息传输的速率、传输代码、代码结构、传输控制步骤、出错控制等作出规定并制定出标准。即网络协议是指在各台计算机之间进行数据交换的工具，不同的计算机之间必须使用相同的网络协议才能进行通信。

TCP/IP（Transmission Control Protocol/Internet Protocol，传输控制协议/互联网络协议）是一种网络通信协议，它规范了网络上的所有通信设备，尤其是一个主机与另一个主机之间的数据往来格式以及传送方式。

IPX/SPX 是基于施乐的 XEROX'S Network System（XNS）协议，而 SPX 是基于施乐的 XEROX'S SPP（Sequenced Packet Protocol，顺序包协议）协议，它们都是由 Novell 公司开发出来应用于局域网的一种高速协议。和 TCP/IP 最显著不同就是其不使用 IP 地址，而使用网卡的物理地址（即 MAC 地址）。

NetBEUI（NetBios Enhanced User Interface，NetBios 增强用户接口）是 NetBios 协议的增强版本，NetBEUI 协议是一种短小精悍、通信效率高的广播型协议，安装后不需要进行设置，特别适合于在“网络邻居”传送数据。

网络协议至少要包括三个要素，如表 1-1 所示。

表 1-1　网络协议三要素

要　素	说　明
语法	用来规定信息格式
语义	用来说明通信双方应当怎么做
时序	详细说明事件的先后顺序

1-2 服务器与客户端

服务器（Server）是指管理和传输信息的一种计算机系统，在网络计算环境中提供服务的一方。这里涉及到其他两个概念：一个是网络计算环境，一个是提供服务。

硬件意义上的服务器，其含义是在网络计算中提供服务的计算机硬件。它有两层含义：一是服务器生存在网络计算环境中的；二是在网络计算中向网络的其他计算机提供服务。

软件意义上的服务器，其含义是指一个计算机程序，该程序用来执行客户端提出的请求。

服务器是一种高性能计算机，作为网络的节点，存储、处理网络上 80%左右的数据、信息，因此也被称为网络的灵魂。做一个形象的比喻：服务器就像是邮局的交换机，而微型计算机、笔记本、PDA、手机等固定或移动的网络终端，就如散落在家庭、各种办公场所、公共场所等处的电话机。我们日常的生活、工作中的电话交流、沟通，必须经过交换机，才能到达目标电话。同样，网络终端设备（如家庭、企业中的微型计算机上网，获取资讯，与外界沟通、娱乐等）也必须经过服务器，因此也可以说是服务器在“组织”和“领导”这些设备。

虽然服务器是在网络环境中为客户端（Client）提供各种服务的、特殊的专用计算机，但在实际的网络环境中，服务器还承担着数据的存储、转发、发布等关键性任务，是各类基于客户端、服务器模式网络中不可或缺的重要组成部分。

其实对于服务器硬件并没有一定硬性的规定，特别是在中、小型企业，它们的服务器可能就是一台性能较好的 PC 机，不同的只是其中安装了专门的服务器操作系统，所以能够让这样一台 PC 机担当服务器的角色，俗称 PC 服务器，由它来完成各种所需的服务器任务。

当然，由于 PC 机与专门的服务器在性能方面差距较远，因此可以想象，由 PC 机担当的服务器无论是在网络连接性能，还是在稳定性等各方面，都不能承担高负荷任务，只能适用于小型且任务简单的网络。

不过，服务器其实也是一种计算机，也是由 PC 机发展过来的。在早期网络不是很普及时，并没有服务器这个名称，当时在整个计算机领域只有大型计算机和微型计算机两大类。不过，随着网络特别是局域网的发展和普及，“服务器”这个中间层次的计算机开始得到业界的接受，并随着网络的普及和发展不断得到发展。

尽管如此，服务器与普通所见的计算机又不完全一样，都是因为服务器的特殊性要求导致的，这就是服务器的四大主要特性（通常称之为“四性”）。

虽然服务器也与 PC 机一样是由诸如主板、CPU、内存、硬盘等硬件组成，尽管外观上基本类似，但这些硬件均不是普通 PC 机所用的，而是专门开发，用于服务器环境的。也正因如此，服务器的价格通常非常高，中档的服务器都在几万元左右，高档的达几十万甚至上百万。

作为一台服务器首先要求的是它必须可靠，即“可用性”，因为服务器所面对的是整个网络用户，而不是本机登录用户，只要网络中有用户，服务器就不能关闭。

在一些特殊应用领域，即使没用户使用有些服务器也得不间断地工作，因为它必须持续地为用户提供连接服务，而不管是在上班，还是下班，也不管是工作日，还是休息、节假日，这就是为什么服务器首先必须要求具备极高的稳定性能的根本原因。

一般来说，专门的服务器都需要 7*24 小时不间断工作，特别是像一些大型的网络服务器，如大公司所用服务器、网站服务器以及提供公众服务器的 Web 服务器等。这些服务器也许真正工作开机的次数只有一次，那就是它刚买回来全面安装配置好后投入正式使用的那一次，一直到

它彻底报废。如果动不动就出毛病，这样的网络能保持长久正常运作吗？这可算是服务器的最关键性能，也是作为能担当服务器角色的前提，哪怕是一台 PC 机。

还有，服务器要为很多用户提供服务，没有很好连接和运算性能是无法承受的，这就是服务器的“可利用性”。

平时一人用一台计算机都老是觉得慢，如果服务器也像人们平常所用的 PC 一样，那如此多的用户请求又如何能及时得到计算机的响应和完成呢？因此，服务器在性能和速度方面也是与普通 PC 机有很大区别的。

为了实现高速，一般服务器是通过采用对称多处理器安装、插入大量的高速内存等方面来保证，这样也就决定服务器在硬件配置方面也与普通的计算机有着本质的区别。它的主板上可以同时安装几个甚至几十、上百个（如 SUN 的 FIRE 15K 可以支持到 106 个 CPU）服务器专用 CPU（这些 CPU 与普通 PC 机中的 CPU 是完全一样的）。

众所周知，普通 CPU 最重要的参数是主频，主频越高，运算速度越快，但在服务器 CPU 中却不是这样的，通常服务器 CPU 的主频比较低，如现在 Intel 的服务器 CPU 主频通常在 P4 2.0GHz 左右，远低于 PC 机 CPU 的主频，其他品牌的服务器 CPU 主频则更低了，但这些服务器 CPU 都具有非常好的运算性能。一则 CPU 主频越高，工作时所散发的热量就越高，给服务器带来很大的不稳定因素；另一方面，服务器运算性能的提高，不是通过主频的提高来达到的，而是通常在其他参数方面加强得到的，而且多数中、高档服务器还可通过对称多处理器系统来大幅提高服务器的整体运算性能，根本没必要在单个 CPU 中通过主频的提高来提高运算性能。

在 CPU 配置方面还要注意，服务器的 CPU 个数一定是双数，即所谓的“对称多处理器系统”。在内存方面的配置也一样，无论是在内存容量，还是性能、技术等方面，都与普通 PC 机所用内存存在着根本的区别。

另外，服务器还须具有一定的“可扩展性”，那是因为网络不可能长久不变，如果没有一定的可扩展性，当用户一增多就不能胜任的话，一台几万，甚至几十万的服务器如果在短时间内就要遭到淘汰，这是许多企业都无法承受的。

为了保持高的可扩展性，通常需要在服务器上具备一定的可扩展空间和冗余件（如磁盘矩阵位、PCI 和内存条插槽位等）。当然，在服务器的主要特点方面还需要注意一点，那就是服务器必须具备一定的自动报警，并配有相应的冗余、备份、在线诊断和恢复系统，以防备出现故障时及时恢复服务器的运作（即“可管理性”）。

虽然说服务器需要不间断地持续工作，但再好的产品都有可能出现故障的一天。

服务器虽然在稳定性方面有足够的保障，但一旦出现故障怎么办，如果像平时所用的计算机一样停下进行维修，对于一个大型服务器而言是不可能的，这就很可能造成整个网络的瘫痪，所带来的损失是无法用金钱来衡量的。

服务器生产厂商为了解决这一难题，提出了许多新的技术，如冗余技术、系统备份、在线诊断技术、故障预报警技术、内存查纠错技术、热插拔技术和远程诊断技术等，使绝大多数故障能够在不停机的情况下得到及时修复。

在计算机的世界里，凡是提供服务的一方称为服务端（Server），而接受服务的另一方称作客户端（Client）。如在局域网络进行打印操作：提供打印服务的计算机即为打印服务器；而使用打印服务器提供打印服务的另一方，则称作客户端。但谁是客户端谁是服务端也不是绝对的，倘若原提供服务之服务端要使用其他计算机所提供的服务，则所扮演之角色即转变为客户端。