KH 科海图书

送给自己、送给孩子、送给朋友一门 实用的技能

新手学

黑客攻防（入门篇）

梵绅科技 编著

「超值实用版」 全彩印刷+多媒体光盘

1CD 播放时间长达110分钟！

CD

为你全面剖析黑客攻防的操作模式

教你查漏补缺作好防范工作，保证电脑安全

教学演示视频
书中百余技法实例，全面分类收录

+

加赠
《新概念计算机组装与维护教程》视频教程
1本书价格 2本书内容哦

=

超值!!

中国人民大学出版社
北京科海电子出版社
www.khp.com.cn

新手学

黑客攻防(入门篇)

梵绅科技 编著

中国人民大学出版社
·北京·

北京科海电子出版社
www.khp.com.cn

图书在版编目(CIP)数据

新手学黑客攻防：入门篇/梵绅科技编著.
北京：中国人民大学出版社，2008
ISBN 978-7-300-10053-1

Ⅰ.新…
Ⅱ.梵…
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（2008）第 191331 号

新手学黑客攻防（入门篇）
梵绅科技　编著

出版发行　中国人民大学出版社　北京科海电子出版社
社　　址　北京中关村大街 31 号　　邮政编码　100080
　　北京市海淀区上地七街国际创业园 2 号楼 14 层　　邮政编码　100085
电　　话　（010）82896442　62630320
网　　址　http: //www.crup.com.cn
　　http: //www.khp.com.cn（科海图书服务网站）
经　　销　新华书店
印　　刷　北京市雅彩印刷有限责任公司
规　　格　140mm×210mm　32 开本　　版　　次　2009 年 2 月第 1 版
印　　张　7.75　　印　　次　2009 年 2 月第 1 次印刷
字　　数　377 000　　定　　价　22.00 元（含 1CD 价格）

前言

随着互联网技术的不断发展，信息交流更加高效、便捷，各种新的网络功能不断涌现，网络在促进经济发展、推动社会进步和提高人们的生活质量等方面发挥着越来越重要的作用。然而与此同时，网络的安全问题也变得日趋严重，需要引起每一个电脑用户的重视。

在网络中有一群被称为“黑客”的神秘人物。最早黑客是指热心于计算机技术、水平高超的电脑专家，尤指程序设计人员。但到了今天，黑客已被用于泛指那些专门利用电脑搞破坏或恶作剧的家伙。作为一个有一定操作经验的电脑用户，读者有必要了解一些黑客的知识，通过模拟黑客的行为准则以及入侵网络的方式、方法，反过来发现自身存在的问题，做好防范工作，从而最终保证自己的数据信息和网络财产的安全。

本书共11章。第1章介绍黑客的基础知识，包括黑客入侵的途径、入侵命令以及入侵的方式。第2章介绍Windows系统中存在的安全隐患和漏洞。第3章介绍针对Windows系统中存在的漏洞如何设置电脑，从而实现防范黑客通过漏洞攻击电脑的目的。第4章~第6章介绍黑客从信息收集、植入木马、到最后进行远程控制与入侵的一个完整流程。第7章~第9章介绍黑客如何对QQ、电子邮件与网页进行攻击，以及电脑用户应该怎样防范。第10章介绍防范木马与黑客的一些小方法。最后的第11章介绍被黑客入侵后，如何隐藏信息与创建后门。

本书采用全彩印刷，配1张多媒体教学视频光盘。彩色印刷能使图文对比更加鲜明、直观，使学习过程更加愉悦。多媒体教学视频让读者像看电视一样学电脑，学习效果立竿见影。

由于笔者水平有限，在本书的编写过程中难免会有疏漏之处，希望广大读者发现后批评指正，并提出宝贵意见。读者可通过电子邮件kh_reader@163.com，或者加本书专用客服QQ 260157084与我们取得联系，我们将尽可能地为读者解疑释惑、提供帮助。

编著者

2009年1月

多媒体光盘使用说明

多媒体光盘的内容

本书配套多媒体光盘内容包括36个重点设置的视频教程，对应书中各章节内容，Step by Step详细地讲解具体操作步骤。读者可以先阅读图书再浏览光盘，也可以直接通过光盘学习防范电脑被黑客攻击的方法。

另外，为拓展读者的知识面，本光盘还贴心地赠送了科海出版的《新概念计算机组装与维护教程（升级版）》一书的视频教程。具体内容包括计算机硬件构成及其连接方法、电脑的工作原理、安装Windows XP/Vista操作系统的方法、BIOS设置和分区的方法等。丰富的光盘内容，真正做到花一本书的价钱、享受两本书的学习内容，绝对物超所值！

下面以本套丛书中《新手学电脑（入门篇）》的多媒体光盘演示效果为例，介绍光盘的使用方法。本书的光盘形式与之类似，可参考操作。

光盘使用方法

1. 将本书的配套光盘放入光驱后会自动运行多媒体程序，并进入光盘的主界面，如图1所示。如果光盘没有自动运行，只需在“我的电脑”中双击CD光驱的盘符进入配套光盘，然后双击“AutoRun.exe”文件即可。

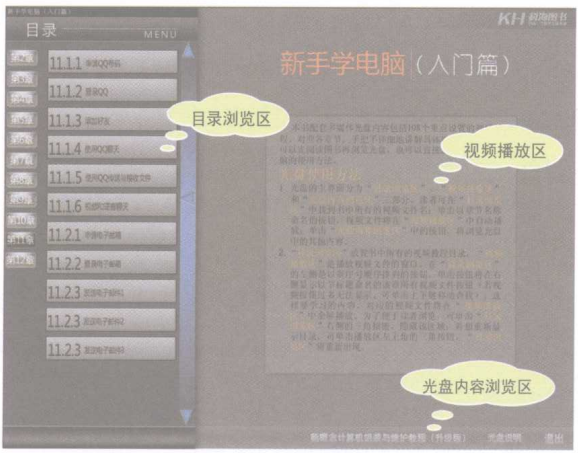

图1　光盘主界面

2. 光盘的主界面分为“目录浏览区”、“视频播放区”和“光盘内容浏览区”三部分（见图1的图注）。读者可在“目录浏览区”中找到书中所有的视频文件名；单击以章节名称命名的按钮，视频文件将在“视频播放区”中自动播放；单击“光盘内容浏览区”中的按钮，将浏览光盘中的其他内容。

目录浏览区和视频播放区

“目录浏览区”放置书中所有的视频教程目录，“视频播放区”是播放视频文件的窗口。在“目录浏览区”的左侧有以章序号顺序排列的按钮，单击按钮将在右侧显示以节标题命名的该章所有视频文件按钮（若视频按钮过多无法显示，可单击 ▲▼ 键移动查找），如图2所示。选择要学习的内容，对应的视频文件将在“视频播放区”中全屏播放，为了便于读者浏览，可单击“目录浏览区”右侧的◀按钮，隐藏该区域，如图3所示；若想重新显示目录，可单击屏幕左上角的▶按钮，“目录浏览区”将重新出现。

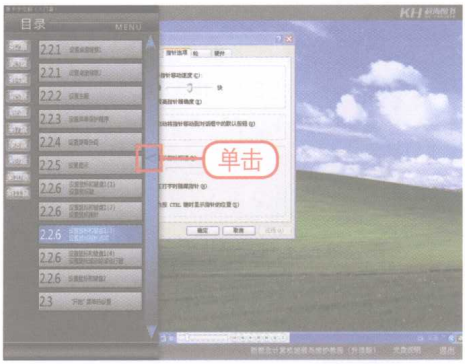

图2　显示视频信息

图3　使用自带的播放器观看视频

光盘内容浏览区

单击“新概念计算机组装与维护教程（升级版）”按钮，即可看到赠送的本书视频教程，如图4所示。读者可选取感兴趣的内容进行学习。

单击“光盘说明”按钮，可以查看使用光盘的设备要求。

单击“退出”按钮，退出多媒体教学系统，并显示光盘的制作人员姓名。

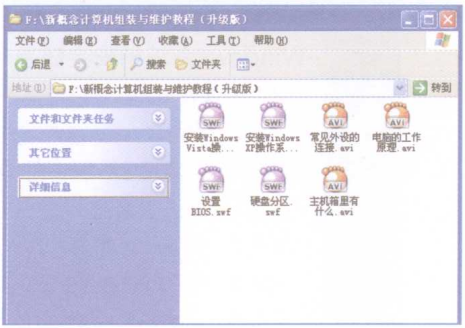

图4　赠送的视频文件

Contents 目录

Contents 目录

Contents 目录

视频教程

视频教程

视频教程

Contents 目录

第1章

黑客往往被人们看做是神秘的、不可琢磨的、难以接近的万能人，他的出现让网络上的人们感到恐慌，更是让网上财产安全陷入危机。本章将针对黑客介绍其基本的概念及其常用的入侵方式。

黑客基础知识

1.1 黑客的概述

黑客最早源自英文hacker，早期在美国的电脑界是带有褒义的。但在媒体报导中，黑客一词往往指那些“软件骇客”（software cracker）。

黑客一词，原指热心于计算机技术，水平高超的电脑专家，尤其是程序设计人员。对这些人的正确英文叫法是cracker，有人翻译成“骇客”。黑客和骇客根本的区别是：黑客们建设，而骇客们破坏，也有人把黑客叫做hacker。但到了今天，黑客一词已被用于泛指那些专门利用电脑搞破坏或恶作剧的人。

黑客的原意是指那些精通操作系统和网络技术，并利用其专长编制新程序的人。这些人往往都掌握着非凡的计算机技术和网络知识，除了无法通过正当的手段物理性破坏他人的计算机和帮助他人重装操作系统外，其他大部分电脑操作他们都能通过网络做到。例如，将别人的计算机当作跳板盗取其他计算机内的文件，造成别人的计算机崩溃，磁盘格式化，监视他人计算机或者偷窥他人隐私，远程控制他人计算机，入侵网站服务器替换该网站的主页，下载用户数据库造成商业损失，攻击网站服务器使其无法被用户访问等。黑客技术现在已经逐渐被越来越多的人掌握和开发。目前世界上有许多黑客网站，这些站点都会介绍一些常用的攻击方法和系统的一些漏洞，并免费提供攻击软件供网友下载和使用，这样系统和站点遭受网民攻击的可能性就变大了。但是黑客技术同时又是一把双刃剑，如果我们了解了常用的黑客技术，就可以更好地保护自己的计算机不被恶意攻击。

在发展初期，网络方面的立法还不够健全，黑客在法律的漏洞下可以为所欲为。目前各国法律的发展速度还远远地落后于互联网的发展速度，在黑客活动转入地下以后其攻击的隐蔽性更强，使得当前的法律和技术缺乏针对网络犯罪卓有成效的反击和跟踪手段，无规范的黑客活动已成为网络安全的重要威胁。

1.2 黑客必经的两道门：IP地址与端口

端口就是计算机与外界通信交流的出口，而IP地址则相当于网络主机的一个虚拟地址，黑客如果想要攻击某个网络主机，首先要确定该目标的域名或者IP地址，然后通过端口来攻击该主机。

1.2.1 IP和IP地址

IP地址就像是家庭住址一样，例如你要写信给一个人，你就要知道他的地址，这样邮递员才能把信送到，计算机发送信息就像邮递员，它必须知道唯一的“家庭地址”才能不把信送错。只不过人们的地址使用文字来表示，计算机的地址用十进制数字表示。

1. IP

IP是英文 Internet Protocol的缩写，意思是“网络互联协议”，也就是为计算机网络相互连接进行通信而设计的协议。在因特网中，它是能使连接到网上的所有计算机

实现相互通信的一套规则，规定了计算机在因特网上进行通信时应当遵守的规则。任何厂家生产的计算机系统，只要遵守 IP协议就可以与因特网互连互通。正是因为有了IP协议，因特网才得以迅速发展成为世界上最大的、开放的计算机通信网络。因此，IP协议也叫做“因特网协议”。

2．IP地址

所谓IP地址就是给每个连接在互联网上的主机分配的一个32位地址。按照TCP/IP规定，IP地址用二进制表示，每个IP地址长32位，32位换算成字节，就是4字节。例如，一个采用二进制形式的IP地址是00001010000000000000000000000001，这么长的地址，处理起来太费劲。为了方便人们的使用，IP地址经常被写成十进制的形式，中间使用符号“.”分开。于是，上面的IP地址可以表示为10.0.0.1。IP地址的这种表示法叫做“点分十进制表示法”，这显然比1和0容易记忆得多。

有人会以为，一台计算机只能有一个IP地址，这种观点是错误的。通常可以指定一台计算机具有多个IP地址，因此在访问互联网时，不要以为一个IP地址就是一台计算机。另外，通过特定的技术，也可以使多台服务器共用一个IP地址，这些服务器在用户看起来就像一台主机。

3．IP地址的分类

互联网中的每个接口都必须有一个唯一的IP地址，该地址并不采用平面形式的地址空间，例如1、2、3等。IP地址具有一定的结构，分为5类。

（1）A类地址保留给政府机构，一个A类IP地址由1字节的网络地址和3字节主机地址组成，网络地址的最高位必须是0，地址范围是1.0.0.1～126.255.255.254，可用的A类网络有126个，每个网络能容纳1亿多个主机。

（2）B类地址分配给中等规模的公司，一个B类IP地址由2字节的网络地址和2字节的主机地址组成，网络地址的最高位必须是10，地址范围是128.0.0.1～191.255.255.254。可用的B类网络有16 382个，每个网络能容纳6万多个主机 。

（3）C类地址分配给任何需要的人，一个C类IP地址由3字节的网络地址和1字节的主机地址组成，网络地址的最高位必须是110。地址范围是192.0.0.1～223.255.255.254。C类网络可达209万余个，每个网络能容纳254个主机。

（4）D类地址用于组播，第一个字节以1110开始，它是一个专门保留的地址，并不指向特定的网络，目前这一类地址被用在多点广播中。多点广播地址用来一次寻址一组计算机，它标识共享同一协议的一组计算机。地址范围是224.0.0.1～239.255.255.254。

（5）E类地址用于实验，E类地址不分网络地址和主机地址，它的第1字节的前5位固定为11110，地址范围是240.0.0.1～255.255.255.254。

1.2.2 端口的概述

随着计算机网络技术的发展，原来物理上的接口已不能满足网络通信的要求，而TCP/IP作为网络通信的标准就解决了这个通信难题。TCP/IP集成到操作系统的内核中，这就相当于在操作系统中引入了一种新的输入/输出接口技术，因为在TCP/IP中引入了一种称为Socket的应用程序接口。有了这样一种接口技术，一台计算机就可以通过软件的方式与任何一台具有Socket接口的计算机进行通信。端口在计算机编程上也就相当于Socket接口。简言之，端口就是计算机与外界通信交流的出口。

1. 端口

计算机“端口”是英文port的译义，可以认为是计算机与外界通信交流的出口。其中硬件领域的端口又称接口，如USB端口、串行端口等。软件领域的端口一般指网络中面向连接服务和无连接服务的通信协议端口，是一种抽象的软件结构，包括一些数据结构和I/O缓冲区。在网络技术中，端口有好几种意思。集线器、交换机、路由器的端口指的是连接其他网络设备的接口，如RJ-45端口、Serial端口等。这里的端口不是物理意义上的端口，而是特指TCP/IP中的端口，是逻辑意义上的端口。

2. 端口的分类

逻辑意义上的端口有多种分类标识，常见的分类标准有以下两种。

（1）按端口分布划分

按端口分布划分可以分为“公认端口”、“注册端口”以及“动态和/或私有端口”等。

① 公认端口

公认端口也称为“常用端口”。这类端口的端口号为0～1 023，它们紧密地绑定于一些特定的服务。通常这些端口的通信明确地表明了某种服务的协议，不可再重新定义它的作用对象。例如21端口分配给FTP服务，而23号端口是Telnet服务专用的，25端口分配给SMTP服务，80端口是HTTP通信所使用的，135端口分配给RPC服务，这些端口通常不会被像木马这样的黑客程序利用。

② 注册端口

注册端口的端口号为1 024～19 151，它们松散地绑定于一些服务，也就是说有许多服务绑定于这些端口，这些端口同样用于许多其他的目的。这些端口多数没有明确的定义服务对象，不同的程序可以根据实际需要自己定义，如后面要介绍的远程控制软件和木马程序中都会有这些端口的定义。记住这些常见的程序端口在木马程序的防护和查杀方面是非常有必要的。

③ 动态和/或私有端口

动态和/或私有端口的端口号为49 152～65 535。从理论上讲，不应该把常用服务分配在这些端口上。但实际上有些较为特殊的程序，特别是一些木马程序就非常喜欢使用这些端口，因为这些端口常常不会引起注意，容易隐蔽。

（2）按协议类型划分

根据所提供的服务方式的不同，端口又可以分为“TCP端口”和“UDP端口”两种。由于TCP和UDP两个协议是独立的，因此各自的端口号也相互独立，比如TCP有235端口，UDP也可以有235端口，两者并不冲突。

① 使用TCP协议的常见端口

- FTP：定义了文件传输协议，使用21端口。某计算机开了FTP服务便启动了文件传输服务。下载文件和上传文件都用到FTP服务。
- Telnet：一种用于远程登录的端口，用户可以以自己的身份远程连接到计算机上，通过这种端口可以提供一种基于DOS模式下的通信服务。如以前的BBS是纯字符界面，支持BBS的服务器会将23端口打开，以对外提供服务。
- SMTP：简单邮件传送协议，现在很多邮件服务器使用的都是这个协议，用于发送邮件。如常见的免费邮件服务中使用的就是这个邮件服务端口，所以在电子邮件设置中经常会看到有SMTP端口设置，服务器开放的是25号端口。