全方位的功能讲解 ● 全程图解的易学模式 ● 注重实用的实例演练 ● 良心品质

轻松学习 实例演练 良心品质

# 轻松学

九天科技 编著

# 黑客攻防

全彩印刷+多媒体光盘

高品质的全彩图书

全方位的功能讲解、全程图解的易学模式、注重实用的实例演练

超丰富的视频光盘

120分钟超长播放的多媒体视听教学光盘，一套生动鲜明的“活教材”

买一送二超值附赠

赠送《轻松学电脑办公》和《轻松学系统安装、重装与优化》全部教学视频



长达120分钟的视频教学

中国铁道出版社
CHINA RAILWAY PUBLISHING HOUSE

轻松学习 实例演练 良心品质

# 轻松学

九天科技 编著

# 黑客攻防

全彩印刷+多媒体光盘


中国铁道出版社
CHINA RAILWAY PUBLISHING HOUSE

## 内 容 简 介

本书的编写目的是帮助初学者学习电脑安全及黑客攻防的相关知识。本书通过简单实用的操作，介绍了黑客入侵手段、QQ攻防、电子邮箱攻防等内容。这些内容让读者快速掌握电脑安全设置知识和防范黑客入侵电脑的方法。

本书适合没有任何电脑黑客攻防知识的初学者以及大中专院校的在校学生和社会电脑安全培训机构的学员使用，也可作为网络安全从业人员、网络管理员的参考用书。

**图书在版编目（CIP）数据**

轻松学黑客攻防/九天科技编著. —北京：中国铁道出版社，2011.5

ISBN 978-7-113-12609-4

Ⅰ.①轻… Ⅱ.①九… Ⅲ.①计算机网络－安全技术 Ⅳ.①TP393.08

中国版本图书馆CIP数据核字（2011）第029477号

**书　　名**：轻松学黑客攻防
**作　　者**：九天科技 编著

**责任编辑**：苏 茜　　**读者热线电话**：400-668-0820
**编辑助理**：刘建玮
**封面设计**：张 丽　　**封面制作**：郑少云
**责任印制**：李 佳

**出版发行**：中国铁道出版社（北京市宣武区右安门西街8号　　邮政编码：100054）
**印　　刷**：北京捷迅佳彩印刷有限公司
**版　　次**：2011年5月第1版　　2011年5月第1次印刷
**开　　本**：880mm×1230mm　1/32　　**印张**：7.625　　**字数**：291千
**书　　号**：ISBN 978-7-113-12609-4
**定　　价**：28.00元（附赠光盘）

# 前言 Foreword

电脑与网络在促进经济发展、推动社会进步和提高人们生活品质等方面发挥着越来越突出的作用，与此同时网络安全问题也变得日趋严重，大量电脑病毒、木马和黑客攻击不断涌现，其花样还时常翻新，严重威胁着我们的电脑安全，需要引起我们格外的重视。

本书的编写目的就是帮助初学者学习电脑安全及黑客攻防的相关知识，并通过简单实用的系统安全设置、修复系统漏洞等操作，常见的黑客入侵手段介绍以及利用 QQ 攻防、电子邮箱攻防等具体的实例演练等内容，让读者快速掌握电脑安全设置知识以及防范黑客入侵电脑的方法。

本书共分为 12 章，其中：第 1 章介绍黑客攻防基础知识入门；第 2 章介绍扫描网络与锁定目标；第 3 章介绍 Windows 远程控制攻防战；第 4 章介绍 Windows 系统漏洞攻防战；第 5 章介绍木马植入攻防战；第 6 章介绍聊天工具攻防战；第 7 章介绍电子邮件攻防战；第 8 章介绍网页攻防战；第 9 章介绍 U 盘病毒攻防战；第 10 章介绍系统安全策略攻防战；第 11 章介绍系统与文件加密；第 12 章介绍黑客攻防实用技巧。

本书配套的多媒体教学光盘，提供累计时间长达 120 分钟的多媒体教学视频，以全过程语音讲解、情景式教学等方式对书中知识点进行深入讲解，逐步使读者掌握黑客攻防知识。此外还随盘赠送《轻松学电脑办公》和《轻松学系统安装、重装与优化》全部光盘资料。

本书适合没有任何电脑黑客攻防知识的初学者以及大中专院校的在校学生和社会电脑安全培训机构的学员使用，也可作为网络安全从业人员、网络管理员的参考用书。

如果读者在使用本书的过程中遇到问题或者有好的意见或建议，可以通过发送电子邮件：E-mail：jtbook@yahoo.cn 或者在线 QQ：843688388 联系我们，我们将及时予以回复，并尽最大努力为您提供学习上的指导与帮助。

本书的编写目的绝不是为那些怀有不良动机的人提供支持，编者及出版社不承担因为技术被滥用所产生的连带责任。本书的目的在于最大限度地唤起大家的网络安全意识，正视网络世界所面临的一场危机并采取相应行动。特此声明！

编 者

2011 年 2 月

# 多媒体光盘使用说明

# How to use the DVD-ROM

## 多媒体教学光盘的内容简介

本书配套的多媒体教学光盘内容包括 113 个视频教程，视频教程对应书中各章节的内容安排，为各章节内容的操作步骤配置演示视频，播放时间长达 120 分钟。读者可以先阅读图书再浏览光盘，也可以直接通过光盘来学习。本光盘内容仅供安全之用，如应用于非法操作，与本社及作者无关。

## 多媒体教学光盘的播放方法

❶ 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，如下图所示。如果光盘没有自动运行，只需在“我的电脑”中双击 DVD 光驱的盘符进入配套光盘，然后双击 Autorun.exe 文件即可。


❶ 光盘目录导航

❷ 赠送光盘视频

❸ 选择背景音乐

❹ 音量控制滑块

❺ 光盘素材文件

❻ 退出光盘

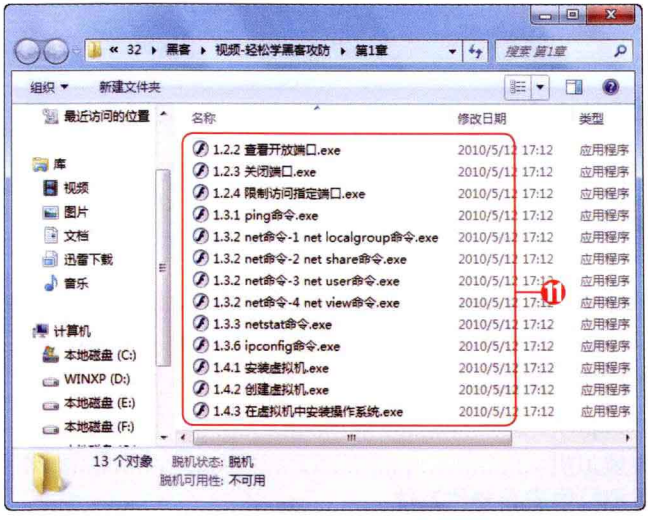
❷ 光盘主界面中显示各章的链接，单击进入本章的二级界面，如下图（上）所示。单击“点击查看”按钮，即可打开视频教程所在的文件夹，如下图（下）所示。双击选择需要播放的视频文件，即可观看视频。


❼ 点击查看视频

❽ 返回上一节

❾ 进入下一节

❿ 返回主界面





⓫ 双击观看视频

## 光盘超值附赠视频

- 《轻松学电脑办公》光盘视频
  长达 180 分钟多媒体教学视频，全面介绍了电脑办公的必备操作技能和方法。
- 《轻松学系统安装、重装与优化》光盘视频
  长达 150 分钟多媒体教学视频，使读者能够快速掌握系统安装、重装及优化方面的知识。

## 光盘最佳运行环境

- CPU：Pentium 4 及以上。
- 内存：215M 及以上。
- 硬盘剩余空间：200M 及以上。
- 屏幕分辨率：1024 *768（像素）。
- 其他：4 倍速以上 DVD 光驱。

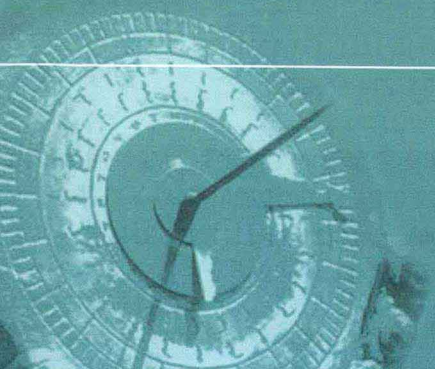
# 目录 · Contents

# 第12章 黑客攻防实用技巧 ..... 208

# 第1章

# 黑客攻防基础知识入门

对防范一个黑客的攻击来说，学会其入侵和破解的方式是必要的。而要做到这一点，则首先要掌握本章所介绍的最基础的知识。因此在学习黑客攻防之前，我们需要先了解一些关于黑客的基础知识，认识 IP 地址、端口和一些黑客常用的 DOS 命令等，为后面的学习打下良好的基础。



本章重点知识

- 认识IP地址
- 黑客攻击的通道——端口
- 黑客常用的命令
- 创建黑客测试环境

# 1.1 认识IP地址

就像每一个人的手机都有一个唯一的电话号码一样，在网络中为了区别不同的计算机，也需要给计算机指定一个号码，这个号码就是“IP 地址”。

## >> 1.1.1 什么是IP地址

IP 地址就像是我们的家庭住址一样，如果你要去别人家串门，你就要知道他（她）的地址，这样才能准确找到。计算机信息也是一样，它必须知道另一台电脑的“家庭地址”才不至于走错。计算机在网络中的地址就是 IP 地址，是用二进制数字表示的。

IP 地址的长度为 32 位，分为 4 个字节，每个字节对应 8 位二进制位，即每部分数字不超过 $2^8$=256。例如，一个用二进制形式记录的 IP 地址可以表示为：11000000 10011110 00000011 00000101。

为了方便使用，IP 地址的每个字节通常用十进制形式表示，每段数字范围为 0 ～ 255，段与段之间用句点隔开，如上面的 IP 地址就可以表示为：192.158.3.5。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。

## >> 1.1.2 IP地址的分类

最初设计互联网络时，为了便于寻址以及层次化构造网络，每个 IP 地址分为网络地址和主机地址两部分。同一个物理网络上的所有主机都使用同一个网络地址，而同一网络上的每个主机都有一个主机地址与其对应。

IP 地址根据网络 ID 的不同分为 5 种类型，即 A 类地址、B 类地址、C 类地址、D 类地址和 E 类地址。

◎ A 类 IP 地址

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”，地址范围为：1.0.0.1 ～ 126.255.255.254（二进制表示为：00000001 00000000 00000000 00000001 ～ 01111110 11111111 11111111 11111110）。可用的 A 类网络有 126 个，每个网络能容纳 16777214 个主机。

◎ B 类 IP 地址

一个 B 类 IP 地址由 2 个字节的网络地址和 2 个字节的主机地址组成，网络地址的最高位必须是“10”，地址范围为：128.1.0.1 ～ 191.255.255.254（二进制表示为：10000000 00000001 00000000 00000001 ～ 10111111 11111111 11111111 11111110）。可用的 B 类网络有 16384 个，每个网络能容纳 65534 个主机。

◎ C 类 IP 地址

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，地址范围为 192.0.1.1 ～ 223.255.255.254（二进制表示为：11000000 00000000 00000001 00000001 ～ 11011111 11111111 11111110 11111110）。C 类网络可达 2097152 个，每个网络能容纳 254 个主机。

◎ D 类 IP 地址

D 类 IP 地址第一个字节以 1110 开始，地址范围为：224.0.0.1 ～ 239.255.255.254。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（Multicast）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。

◎ E 类 IP 地址

E 类地址仅用做实验和为将来开发而保留，它以 1111 开始，全 0（0.0.0.0）的 IP 地址指任意网络，全 1 的 IP 地址（255.255.255.255）是当前子网的广播地址，如下图所示。


# 1.2 黑客攻击的通道——端口

**如果把 IP 地址比作一间房子，TCP/IP 协议中的端口指的就是出入这间房子的门。真正的房子只有几个门，但是一个 IP 地址的端口可以有 65536（即 256×256）个。端口是通过端口号来标记的，端口号只有整数，范围是从 0~65535［256×（256-1）］。**

## >> 1.2.1 端口的分类

计算机中的端口按不同的标准可以分为很多类，其中最常用的分类标准有以下两种：

**1. 按端口号分布划分**

按端口号分布划分，可以将端口分为三大类，分别为：公认端口、注册端口和动态和 / 或私有端口。

◎ 公认端口

公认端口（WellKnownPorts）是指那些用户所熟知的端口号，范围从 0 到 1023，它们紧密绑定于一些服务。通常这些端口的通信明确表明了某种服务的协议。例如，80 端口分配给 WWW 服务，21 端口分配给 FTP 服务等。

◎ 注册端口

注册端口（RegisteredPorts）的端口号从 1024 到 49151。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目的。这些端口大多数没有明确的定义服务对象，应用程序可以根据自己的需要进行定义。例如，我们常用的聊天软件腾讯 QQ 用的就是 4000 端口。

◎ 动态和 / 或私有端口

动态和 / 或私有端口（Dynamicand/orPrivatePorts）的端口号从 49152 到 65535。理论上，不应为服务分配这些端口。但实际上一些较为特殊的程序，特别是一些木马程序常常会使用这些端口，因为机器通常从 1024 起分配动态端口，其不被人们注意，容易隐藏，如 SUN 的 RPC 端口就是从 32768 端口开始的。

**2. 按通信服务方式划分**

计算机通信的连接方式有以下两种：

第一种是直接与接收方进行的连接，发送信息以后，可以确认信息是否到达，这种方式大多采用 TCP 协议。

第二种是不直接与接收方进行连接，只管把信息放在网上发出去，而不管信息是否到达，也就是“无连接方式”。这种方式大多采用 UDP 协议，IP 协议也是一种无连接方式。

对应使用以上这两种通信协议的服务所提供的端口，也就分为“TCP 协议端口”和“UDP 协议端口”。计算机之间相互通信一般采用这两种通信协议。

使用 TCP 协议的常见端口主要有以下几种：

◎ FTP：定义了文件传输协议，使用 21 端口。用户常说某计算机开启了 FTP 服务，便是启动了文件传输服务，下载文件、上传主页都要用到 FTP 服务。

◎ Telnet：它是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。早期的 BBS 是纯字符界面，支持 BBS 的服务器将 23 端口打开，对外提供服务。

◎ SMTP：定义了简单邮件传送协议，现在很多邮件服务器都用的是这个协议，用于发送邮件。常见的免费邮件服务中用的就是这个邮件服务端口，所以在电子邮件设置中常看到有 SMTP 端口设置栏，服务器开放的是 25 号端口。

◎ POP3：它和 SMTP 对应，POP3 用于接收邮件。通常情况下，POP3 协议所用的是 110 端口。也就是说，只要有相应的使用 POP3 协议的程序（如 Foxmail 或 Outlook），就可以不以 Web 方式登录进邮箱界面，直接用邮件程序就可以收到邮件（例如使用 163 邮箱就没有必要先进入网易网站，再进入自己的邮箱来收信）。