Easy to learn!

“买书抽奖 境外游”

超好學！黑客攻防入门

全图解 100% all diagrammatized

九天科技 编著

- 系统安全防护自己搞定！
- 安全防御软件轻松使用！
- 远程监控/木马/网页攻防轻松掌握！
- 邮件/QQ与MSN/U盘攻防快速出击！

超满载 超值光盘内容

300分钟视频让您“坐享其成”！
2本最畅销图书视频光盘全赠送！
专业级多媒体演示，跟着视频做练习！

中国铁道出版社
CHINA RAILWAY PUBLISHING HOUSE

Easy to learn!

超好学！黑客攻防入门

全图解 100% all diagrammatized

九天科技　编著

中国铁道出版社
CHINA RAILWAY PUBLISHING HOUSE

内 容 简 介

本书在从“攻”与“防”两个不同的角度进行展示，在介绍黑客攻击手段的同时，在此基础上介绍了相应的防范措施。全书内容包括：黑客攻防新手入门，信息收集、嗅探与扫描，Windows 系统安全漏洞攻防，密码设置、破解与防御，远程监控攻防技术，木马植入攻防，恶意网页代码攻防，电子邮件攻击与防御，QQ 与 MSN 攻防实战，U 盘病毒攻防，系统安全防护策略，以及使用安全防御软件等。

本书特别适合电脑维护人员、IT 从业人员，以及对黑客攻防和安全维护感兴趣的读者自学参考，也可作为大中专院校和各种电脑培训班的学习教材。

图书在版编目（CIP）数据

超好学！黑客攻防入门全图解/九天科技编著. --
北京：中国铁道出版社，2012.7
ISBN 978-7-113-14509-5

Ⅰ. ①超… Ⅱ. ①九… Ⅲ. ①计算机网络-安全技术
－图解 Ⅳ. ①TP393.08-64

中国版本图书馆 CIP 数据核字（2012）第 063708 号

书　　名：超好学！黑客攻防入门全图解
作　　者：九天科技　编著

策划编辑：武文斌　　**读者热线电话：**010-63560056
责任编辑：苏　茜　　**特邀编辑：**赵树刚
责任印制：赵星辰

出版发行：中国铁道出版社（北京市西城区右安门西街 8 号　　邮政编码：100054）
印　　刷：北京铭成印刷有限公司
版　　次：2012 年 7 月第 1 版
开　　本：700mm×1000mm　1/16　**印张：**15.25　**字数：**296 千
书　　号：ISBN 978-7-113-14509-5
定　　价：39.00 元（附赠光盘）

前言 FOREWORD

内容综述

人们越来越离不开网络，与此同时网络安全问题也就越来越成为人们关注的热点。对于一般用户而言，掌握一定的黑客攻防技术不仅能够帮助用户保护电脑中数据的安全，还可以帮助用户更好地维护电脑，保障其安全、稳定地运行。本书从“攻”与“防”两个不同的角度进行展示，在介绍黑客攻击手段的同时，还详细介绍了相应的防范措施。

本书共分为 12 章，主要内容包括：黑客攻防新手入门，信息收集、嗅探与扫描，Windows 系统安全漏洞攻防，密码设置、破解与防御，远程监控攻防技术，木马植入攻防，恶意网页代码攻防，电子邮件攻击与防御，QQ 与 MSN 攻防实战，U 盘病毒攻防，系统安全防护策略，以及使用安全防御软件等。

本书特色

◎ **从零起步、简单易学：**针对初学者，内容涵盖新手学习黑客攻防的各个方面，深入浅出，简单易学，让读者一看就懂，一练就会。

◎ **丰富全面、专业指导：**内容囊括黑客“攻”与“防”的各个方面，并进行专业指导，使读者全面掌握黑客攻防入门知识。

◎ **快速入门、注重方法：**“授人以鱼，不如授人以渔”，本书注重培养读者正确、高效的学习方法，使其快速入门，以达到立竿见影的学习效果。

◎ **举一反三、轻松掌握：**深入剖析了黑客攻防的全部过程，使读者不仅能轻松掌握具体的操作方法，还可以做到举一反三，融会贯通。

◎ **全程图解、版式时尚：**本书全程图解剖析，版式美观大方、新鲜时尚，并在每页开设“行家提醒”和“操作提示”栏目，带给读者全新的学习体验。

适用读者

本书特别适合电脑维护人员、IT 从业人员以及对黑客攻防和安全维护感兴趣的读者自学参考，也可作为大中专院校和各种电脑培训班的学习教材。

售后服务

如果读者在使用本书的过程中遇到问题或者有任何意见或建议，可以通过电子邮件（E-mail：jtbook@yahoo.cn）或者即时通信软件（QQ：843688388）联系我们，我们将及时予以回复，并尽最大努力提供学习上的指导与帮助。

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

本书配套的多媒体教学光盘内容对应书中各章节的内容安排，为各章节内容的重点知识，播放时间长达 300 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学习黑客攻防的相关知识。

多媒体教学光盘的使用

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”窗口中双击 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 退出光盘

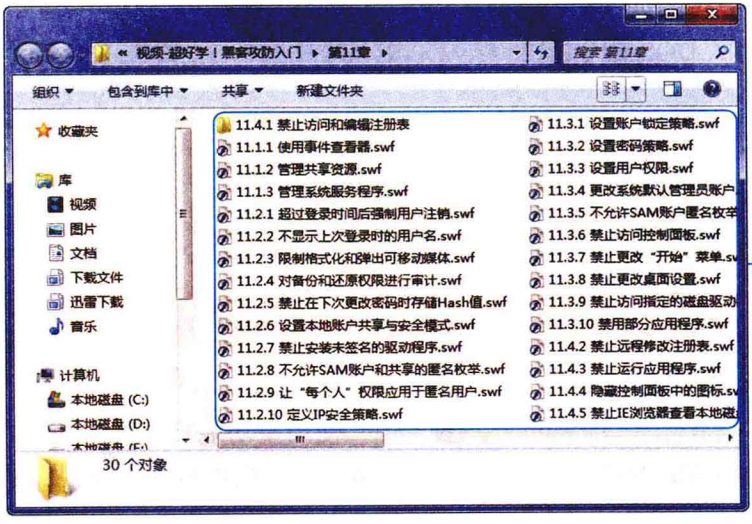
❷ 光盘主界面中显示各章的链接，单击进入本章的二级界面，如下图（上）所示。单击“点击查看”超链接，即可打开视频教程所在的文件夹，如下图（下）所示，双击选择需要播放的视频文件，即可观看视频。

⑥ 小节目录

⑦ 返回上一节

⑧ 进入下一节

⑨ 返回主界面



⑩ 双击观看视频

光盘超值附赠视频

- 《电脑常见故障诊断与排除从新手到高手》光盘视频
  长达 320 分钟多媒体教学视频，全面介绍了各种电脑常见故障的诊断与排除方法等知识。
- 《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，指导初学者快速掌握系统安装、重装与优化的相关知识与技巧。

光盘最佳运行环境

- CPU：Pentium 4 及以上。
- 内存：512MB 及以上。
- 硬盘剩余空间：200MB 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 1 章 黑客攻防新手入门

新手有问必答

第 2 章 信息收集、嗅探与扫描

第 5 章 远程监控攻防技术

新手有问必答

第 6 章 木马植入攻防

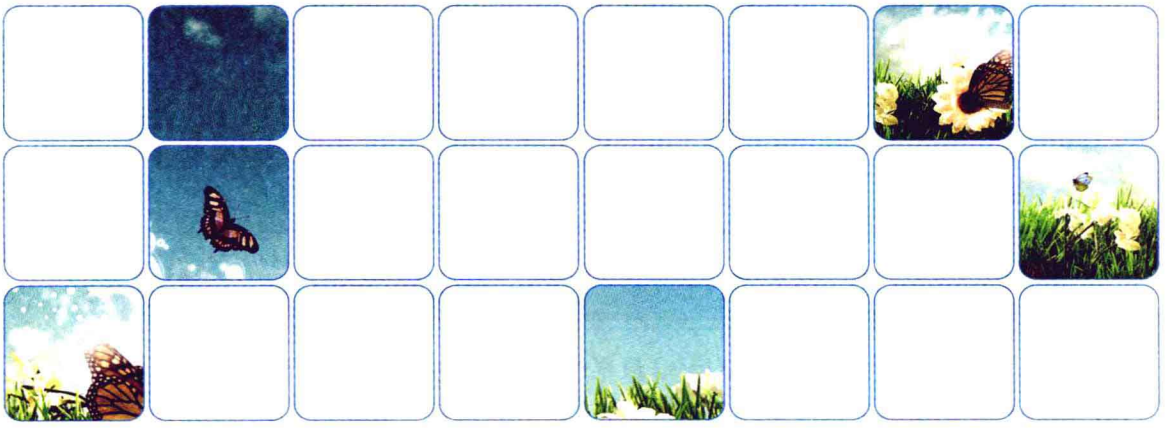
第 9 章 QQ 与 MSN 攻防实战

第 10 章 U 盘病毒攻防

新手有问必答

第 11 章 系统安全防护策略

第 12 章 使用安全防御软件



Chapter 01

黑客攻防新手入门

作为一名黑客，道德和法律常识是非常重要的，这往往决定一个黑客的前途和命运。如果开始学习时就是为了扬名或非法获利，那就不能称为黑客。在学习黑客攻防之前，首先需要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

- ◎ 走进神秘的黑客
- ◎ 黑客常用的DOS命令
- ◎ 黑客必经两道门——IP地址与端口
- ◎ 实战演练——安装虚拟机测试环境

1.1 走近神秘的黑客

谈到网络安全，不自觉间就会联想到黑客，人们往往会将他们同破坏网络安全、盗取用户账号、偷窃个人私密信息联系起来。其实黑客也有好坏之分，他们并不全是网络上的“捣乱分子”，其中也有一部分是网络上的“安全卫士”。下面就来揭开黑客的神秘面纱，让用户详细了解一下黑客到底是一群什么样的人。

在黑客圈中，“Hacker”一词早期无疑是带有正面的意义，但到了今天，“黑客”一词已经被用于那些专门利用计算机进行破坏或入侵的代名词，其实对这些人正确的叫法应该是 Cracker，有人翻译成“骇客”。也正是由于这些人的出现玷污了“黑客”一词，使人们把黑客和骇客混为一体。黑客和骇客根本的区别是：黑客们修补系统漏洞，而骇客们利用系统漏洞进行破坏。

>> 1.1.1 黑客的起源

黑客最早始于 20 世纪 50 年代，最早的计算机 1946 年在宾夕法尼亚大学出现，而最早的黑客出现于麻省理工学院，贝尔实验室也有。最初的黑客一般都是一些高级技术人员，他们热衷于挑战、崇尚自由，并主张信息共享。

1994 年以来，因特网在全球的迅猛发展为人们提供了方便、自由和无限的财富，政治、军事、经济、科技、教育、文化等各个方面都越来越网络化，并且逐渐成为人们生活、娱乐的一部分。可以说，信息时代已经到来，信息已成为物质和能量以外维持人类社会的第三资源，它是未来生活中的重要介质。随着计算机的普及和因特网技术的迅速发展，黑客也随之出现了。

“黑客”一词一般有以下 4 种意义：

◎ 一个对（某领域内的）编程语言有足够了解，可以不经长时间思考就能创造出有用的软件的人。

◎ 一个试图恶意（一般是非法地）破解或破坏某个程序、系统及网络安全的人。这个意义常常对那些符合第一个条件的“黑客”造成严重困扰，他们建议媒体将这群人称为“骇客”。

◎ 一个试图破解某系统或网络，以提醒该系统所有者的系统安全漏洞，这群人往往被称做“红客”。这样的人许多是电脑安全公司的雇员，并在完全合法的情况下攻击某系统。

行家提醒

在我国，人们经常把黑客与骇客搞混，实际区别很大。其实两者之间的根本区别是：黑客从事安全建设，而骇客主要从事破坏活动。

◎ 一个通过知识或猜测而对某段程序做出（往往是好的）修改，并改变（或增强）该程序用途的人。

现在，网络上出现了越来越多的骇客，他们只会入侵，使用扫描器到处乱扫，用 IP 炸弹轰炸，毫无目的地入侵、破坏。他们并无益于电脑技术的发展，反而有害于网络的安全、造成网络瘫痪，为人们带来巨大的经济和精神损失。

>> 1.1.2 黑客的组成

到了今天，黑客已经不像以前那种是少数现象，他们已经发展成网络上的一个独特的群体。他们有着与常人不同的思维方法，有着自己独特的行为模式，网络上现在出现了很多由一些志同道合的人组织起来的黑客组织。但是这些人从什么地方来？他们是什么样的人？其实除了极少数的职业黑客以外，大多数都是业余的，而黑客其实和现实中的平常人没有两样，或许他就是一个普通的高中学生。

有人曾经对黑客年龄方面进行过调查，组成黑客的主要群体是在 18 ～ 30 岁之间的年轻人，大多是男性，不过现在有很多女生也加入到这个行列。他们大多是在校的学生，因为他们有着很强的电脑爱好和时间，好奇心强，精力旺盛等使他们步入了黑客的行列。还有一些黑客大多都有自己的事业或工作，大致分为程序员、资深安全员、安全研究员、职业间谍、安全顾问等。当然这些人的技术和水平是刚刚入门的“小黑客”所无法相比的，不过他们也是从这步一点点地走过来的。

>> 1.1.3 黑客的主要类型

“黑客”大体上分为“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、入侵或做一些其他有害于网络的事情。

无论哪类黑客，他们最初的学习内容都将是本书所涉及的内容，而且掌握的基本技能也都是一样的。即使日后他们各自走上了不同的道路，但是所做的事情也差不多，只不过出发点和目的不一样而已。

黑客的行为主要有以下几种。

其一，学习技术：互联网上的新技术一旦出现，黑客就必须立刻学习，并用最短的时间掌握这项技术。这里所说的掌握并不是一般的了解，而是阅读有关的“协议”、深入了解此技术的机理。否则一旦停止学习，那么依靠他以前掌握的内容，并不能维持他的“黑客”身份超过一年。

其二，伪装自己：黑客的一举一动都会被服务器记录下来，所以黑客都会伪装自己，使得对方无法辨别其真实身份。这需要有熟练的技巧，用来伪装自己的 IP 地址、使用跳板逃避跟踪、清理记录扰乱对方线索、巧妙躲开防火墙等。

行家提醒

黑客会不断地研究计算机和网络知识，发现其中存在的漏洞，喜欢挑战高难度的网络系统并从中找到漏洞，提出解决和修补漏洞的方法。

伪装是需要非常过硬的基本功才能实现的，初学者不可能短时间学会伪装，如果将伪装用于不良目的，一旦自己的行迹败露，最终害的还是自己。

其三，发现漏洞：漏洞对黑客来说是最重要的信息，黑客要经常学习发现别人的漏洞，并努力自己寻找未知漏洞，并从海量的漏洞中寻找有价值的、可被利用的漏洞进行试验。当然，他们最终的目的是通过漏洞进行破坏或修补。

其四，利用漏洞：对于正派黑客来说，漏洞要被修补；对于邪派黑客来说，漏洞用来搞破坏。

作为一名黑客，道德是非常重要的，这往往决定一个黑客的前途和命运。如果开始学习时就是为了扬名或非法获利，那就不能称为黑客。但是，虚拟的网络世界不能用现实中的规范去管理，而黑客又是在这个虚拟世界里渴望自由和共享的。虽然网络上的黑客道德或守则出现很多，也有很多黑客章程，但是这些所谓的道德往往成为一张白纸，而黑客们真正遵守的是来自内心真诚的道德，是一种信仰而不是人为的外在的一种守则。也只有这些来自于黑客们内心中的道德才可以真正地约束他们。

现在有不少人以盗取他人的游戏账号、盗取银行卡号、窃取公司机密、攻击别人网站、敲诈、欺骗等非法获利，这些人都不能称为“黑客”，对于他们应该称为“骇客”更为合适，他们最终会受到法律的制裁和良心的谴责。

1.2 黑客必经两道门——IP地址与端口

黑客进行网络攻击必经的两道门就是 IP 地址与端口，下面将分别对其进行介绍，为后面的学习打下坚实的基础。

>> 1.2.1 认识IP地址

就像每一个人的手机都有一个唯一的号码一样，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，即“IP 地址”。

1. IP 地址的定义

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，就要知道他（她）的地址，这样才能走到。计算机信息也是一样，必须知道另一台计算机的“家庭

行家提醒

漏洞是在硬件、软件和协议的具体实现或系统安全策略上存在的缺陷，从而可以使攻击者能够在未授权的情况下访问或破坏系统。