

Easy
to learn!

“买书抽奖 境外游”



超好學! 黑客攻防入門

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!

超好學! 黑客攻防入門


全圖解
100%
all diagrammattized

九天科技 編著



中國鐵道出版社
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)

版权所有 侵权必究

凡购买铁道版的图书,如有印制质量问题,请与本社发行部联系调换。

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

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。

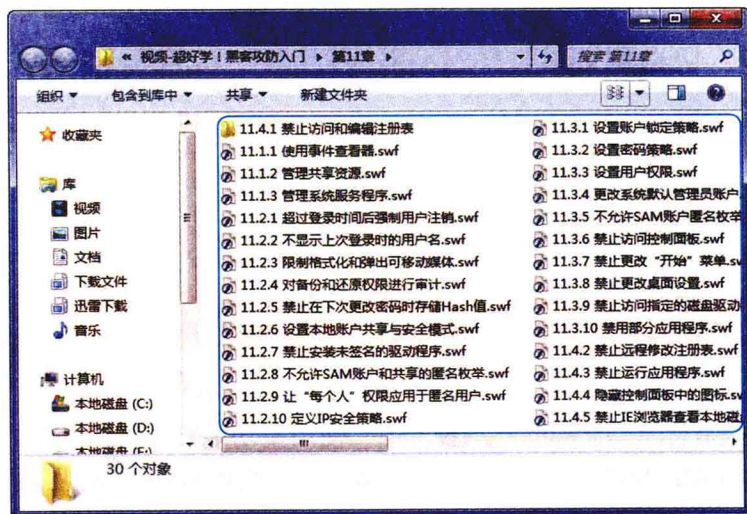


- ① 光盘目录导航
- ② 赠送光盘视频
- ③ 选择背景音乐
- ④ 音量控制滑块
- ⑤ 退出光盘

② 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

- ① 《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。
- ② 《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

- ③ CPU：Pentium 4 及以上。
- ④ 内存：512MB 及以上。
- ⑤ 硬盘剩余空间：200MB 及以上。
- ⑥ 屏幕分辨率：1024 × 768 像素。
- ⑦ 其他：4 倍速以上 DVD 光驱。

目录 CONTENTS



第1章 黑客攻防新手入门

1.1 走近神秘的黑客.....2

1.1.1 黑客的起源.....2

1.1.2 黑客的组成.....3

1.1.3 黑客的主要类型.....3



1.2 黑客必经两道门——IP

地址与端口.....4

1.2.1 认识IP地址.....4

1.2.2 黑客的专用通道——

端口.....6



1.3 黑客常用的DOS命令...12

1.3.1 ping命令.....13

1.3.2 net命令.....15

1.3.3 netstat命令.....19

1.3.4 telnet命令.....20

1.3.5 ftp命令.....21

1.3.6 ipconfig命令.....23



1.4 实战演练——安装虚拟机

测试环境.....23

1.4.1 本例操作思路.....24

1.4.2 本例实战操作.....24

新手有问必答

1. 黑客与骇客有什么区别?.....31

2. 端口的作用主要有哪些?.....31

3. 什么是虚拟机?为何要安装虚拟机?.....31

第2章 信息收集、嗅探与扫描



2.1 探测攻击目标重要

信息.....33

2.1.1 获取目标主机的IP

地址.....33

2.1.2 获取目标主机的

地理位置.....33

2.2 利用扫描器寻找攻击

目标.....34

2.2.1 扫描器的工作原理.....34

2.2.2 扫描器的主要作用.....34

2.3 使用端口扫描器.....35

2.3.1 SuperScan扫描器.....35

2.3.2 Nmap扫描器.....37



2.4 使用多功能扫描器.....38

2.4.1 流光扫描器.....38

2.4.2 SSS扫描器.....43

2.4.3 X-Scan扫描器.....48



2.5 使用网络嗅探工具.....50

2.5.1 嗅探利器SmartSniff.....50

2.5.2 Iris网络嗅探器.....51

2.6 实战演练——使用网络

数据包嗅探专家.....54

2.6.1 本例操作思路.....55

2.6.2 本例实战操作.....55

1. 如何获取网站的备案信息? 56
2. 当今最为流行扫描器的特点和性能是什么? 56
3. 嗅探可以做什么? 为什么需要嗅探? 57

第3章 Windows 系统安全漏洞攻防

- | | |
|--|--|
| <p>3.1 Windows 系统漏洞及其产生原因 59</p> <p>3.1.1 什么是Windows系统漏洞 59</p> <p>3.1.2 Windows系统漏洞的产生原因 59</p> | <p>3.2 系统漏洞攻击与防御 59</p> <p>3.3 实战演练——系统自动更新与使用 360 安全卫士 65</p> <p>3.3.1 利用Windows “自动更新” 功能 65</p> <p>3.3.2 使用360安全卫士 67</p> |
|--|--|



视频教程

1. 目前Windows 7操作系统的安全漏洞有哪些? 68
2. 系统漏洞补丁为何安装不上? 68
3. 使用360安全卫士为系统打补丁有哪些优势? 69

第4章 密码设置、破解与防御

- | | |
|--|--|
| <p>4.1 为操作系统加密 71</p> <p>4.1.1 设置CMOS开机密码 ... 71</p> <p>4.1.2 设置系统启动密码 72</p> <p>4.1.3 设置屏幕保护密码 73</p> <p>4.2 对文件进行加密 74</p> <p>4.2.1 为Word文档加密 74</p> <p>4.2.2 为Excel表格加密 75</p> <p>4.2.3 为电子邮件加密 76</p> <p>4.2.4 为压缩文件加密 77</p> <p>4.3 使用加密软件加密 77</p> <p>4.3.1 文本文件专用加密器 ... 77</p> <p>4.3.2 文件夹加密精灵 79</p> | <p>4.3.3 终极程序加密器 80</p> <p>4.4 破解管理员账户 82</p> <p>4.4.1 使用Administrator 账户登录 82</p> <p>4.4.2 强制清除管理员密码 ... 83</p> <p>4.4.3 创建密码恢复盘 83</p> <p>4.4.4 使用密码恢复软件 85</p> <p>4.5 实战演练——使用 万能加密器 86</p> <p>4.5.1 本例操作思路 87</p> <p>4.5.2 本例实战操作 87</p> |
|--|--|



视频教程



视频教程



视频教程



视频教程



视频教程



1. 黑客比较常用的密码破解方法有哪些? 91
2. 如何破解常用办公软件的密码? 91
3. 如何破解ADSL密码? 91

第5章 远程监控攻防技术

5.1 基于注册表的远程

连接与安全 93

5.1.1 开启远程注册表服务 ... 93

5.1.2 修改注册表实现
远程监控 94



视频教程

5.2 基于认证的远程

连接与安全 95

5.2.1 IPC\$入侵与防范 95

5.2.2 Telnet入侵 102



视频教程

5.3 通过 Windows XP 远程

控制入侵 104

5.3.1 Windows XP系统的
远程协助 104

5.3.2 Windows XP远程
关机 105

5.4 实战演练——使用远程

控制软件入侵 107

5.4.1 本例操作思路 107

5.4.2 本例实战操作 107

新手有问必答

1. 什么是远程控制和远程唤醒? 109
2. 常规远程控制软件和木马有什么区别? 109
3. 什么是网络人 (Netman)? 它的主要用途有哪些? 109

第6章 木马植入攻防

6.1 木马的入侵与伪装

手段 111

6.1.1 木马的结构组成 111

6.1.2 木马常用的入侵
手段 111

6.1.3 木马常用的伪装
手段 113



视频教程

6.2 木马的捆绑、生成与

攻击 115

6.2.1 使用“EXE捆绑机”
捆绑木马 115

6.2.2 自解压木马的制作

与查杀 116

6.2.3 使用网页木马
生成器 118



视频教程

6.3 木马的清除与防御 119

6.3.1 使用木马清道夫
清除木马 119

6.3.2 防范木马常见措施 122



视频教程

6.4 黑客常用的木马工具 ... 124

6.4.1 “冰河”木马 124

6.4.2 “广外女生”木马 129

6.5 实战演练——捆绑 CHM 电子书木马.....	131
--------------------------------	-----

6.5.1 本例操作思路.....	132
6.5.2 本例实战操作.....	132

新手有问必答

1. 如何轻松地识别木马程序?	134
2. 什么是“灰鸽子”木马?	134
3. 什么是木马克星? 它的主要功能有哪些?	134

第7章 恶意网页代码攻防

7.1 认识恶意网页代码.....	136
-------------------	-----

7.2 恶意网页代码的 防范和清除.....	136
---------------------------	-----

7.2.1 恶意网页代码的 防范.....	136
7.2.2 恶意网页代码的 清除.....	137



7.3 常见恶意网页代码攻击 与防御方法.....	138
------------------------------	-----

7.3.1 启动时自动弹出 对话框和网页.....	138
7.3.2 修改起始页和默认 主页.....	139
7.3.3 强行修改IE标题栏.....	140



7.3.4 强行修改右键菜单.....	140
7.3.5 禁用注册表.....	141

7.4 IE浏览器的安全设置.....	141
---------------------	-----

7.4.1 清除IE各项内容.....	141
7.4.2 IE的ActiveX控件 设置.....	143
7.4.3 限制他人访问不良 站点.....	144
7.4.4 设置安全级别和 隐私设置.....	144

7.5 实战演练——使用“瑞星 卡卡上网助手”.....	145
---------------------------------	-----

7.5.1 本例操作思路.....	145
7.5.2 本例实战操作.....	145

新手有问必答

1. 如何判断自己的电脑是否遭到了恶意网站的攻击?	149
2. 常用的浏览器防御方法有哪些?	149
3. 如何使用360安全卫士进行修复浏览器?	149

第8章 电子邮件攻击与防御

8.1 电子邮件病毒.....	151
-----------------	-----

8.1.1 认识“邮件病毒”.....	151
8.1.2 “邮件病毒”识别 技巧.....	151

8.2 制作电子邮件炸弹.....	152
-------------------	-----

8.2.1 认识电子邮件炸弹.....	152
8.2.2 电子邮件炸弹的 制作方法.....	152



视频教程

8.3 破解电子邮箱密码.....153

- 8.3.1 使用“流光”破解密码.....153
- 8.3.2 使用“黑雨”破解密码.....154
- 8.3.3 使用“流影”破解密码.....155



视频教程

8.4 电子邮件安全防御.....156

- 8.4.1 电子邮箱安全防范措施.....156
- 8.4.2 找回邮箱密码.....157
- 8.4.3 防止炸弹攻击.....157



视频教程

8.5 实战演练——使用“溯雪”窃取邮箱密码.....159

- 8.5.1 本例操作思路.....159
- 8.5.2 本例实战操作.....159

新手有问必答

- 1. 为邮箱设置安全密码的技巧有哪些?161
- 2. 发现邮箱被探测的处理方法有哪些?161
- 3. 什么是邮件炸弹的克星?161

第9章 QQ与MSN攻防实战



视频教程

9.1 攻击QQ.....163

- 9.1.1 QQ消息“炸弹”攻击.....163
- 9.1.2 破解本地QQ密码.....164
- 9.1.3 非法获取用户IP地址.....164
- 9.1.4 查询本地聊天记录.....165

9.2 QQ安全防御.....167

9.2.1 保护QQ密码.....167

9.2.2 防范IP地址探测.....169



视频教程

9.3 MSN的攻击与防御.....170

9.3.1 攻击MSN.....170

9.3.2 MSN安全防御.....171



视频教程

9.4 实战演练——加密QQ

聊天记录.....172

9.4.1 本例操作思路.....172

9.4.2 本例实战操作.....172

- 1. 目前黑客常用的窃取QQ密码的工具具有哪些?173
- 2. 如何防御QQ消息“炸弹”的攻击?174
- 3. 什么是“QQ医生”? 它主要有什么作用?174

第10章 U盘病毒攻防

10.1 U盘病毒简介.....176

- 10.1.1 U盘病毒的运行原理.....176

10.1.2 常见的几种U盘病毒.....176



视频教程

10.2 U盘病毒的防御.....177

10.2.1 关闭“自动播放” 功能.....177	 10.4 U 盘病毒的查杀.....180
10.2.2 避免U盘感染病毒....178	10.4.1 用WinRAR查杀 U盘病毒.....180
10.3 autorun.inf 文件的构造 和运行机制.....178	10.4.2 手动删除U盘病毒....181
10.3.1 autorun.inf文件 简介.....178	 10.5 实战演练—使用 USBCleaner 查杀 U 盘 病毒.....181
10.3.2 autorun.inf文件的 构造.....179	10.5.1 本例操作思路.....182
10.3.3 autorun.inf文件的 编写.....179	10.5.2 本例实战操作.....182

新手有问必答

1. 当电脑被U盘病毒感染时有哪些症状表现?	183
2. 当U盘感染病毒时有哪些症状表现?	183
3. 目前常用的U盘病毒专杀工具有哪些?	183

第 11 章 系统安全防护策略



视频教程

11.1 设置计算机管理.....185

11.1.1 使用事件查看器.....185
11.1.2 管理共享资源.....186
11.1.3 管理系统服务程序...187



视频教程

11.2 设置系统安全.....188

11.2.1 超过登录时间后强制 用户注销.....189
11.2.2 不显示上次登录时的 用户名.....189
11.2.3 限制格式化和弹出 可移动媒体.....190
11.2.4 对备份和还原权限 进行审计.....191
11.2.5 禁止在下次更改密码时 存储Hash值.....191
11.2.6 设置本地账户共享 与安全模式.....192



视频教程

11.2.7 禁止安装未签名的 驱动程序.....192
11.2.8 不允许SAM账户和 共享的匿名枚举.....193
11.2.9 让“每个人”权限 应用于匿名用户.....193
11.2.10 定义IP安全策略194

11.3 设置系统组策略.....197

11.3.1 设置账户锁定策略...198
11.3.2 设置密码策略.....198
11.3.3 设置用户权限.....199
11.3.4 更改系统默认 管理员账户.....201
11.3.5 不允许SAM账户 匿名枚举.....201
11.3.6 禁止访问控制面板...202
11.3.7 禁止更改“开始” 菜单.....203



11.3.8 禁止更改桌面设置 ...	203
11.3.9 禁止访问指定的 磁盘驱动器	204
11.3.10 禁用部分应用 程序	204



视频教程

11.4 设置注册表	205
11.4.1 禁止访问和编辑 注册表	206
11.4.2 禁止远程修改 注册表	207



视频教程

11.4.3 禁止运行应用程序 ...	208
11.4.4 隐藏控制面板中的 图标	209
11.4.5 禁止IE浏览器查看 本地磁盘	210
11.4.6 关闭默认共享	210
11.5 实战演练——禁止更改 系统登录密码	211
11.5.1 本例操作思路	211
11.5.2 本例实战操作	212

新手有问必答

1. 为什么最好禁用无关用户的账户? 213
2. 为什么使用Ghost备份与还原系统盘? 213
3. 无法打开注册表怎么办? 213

第12章 使用安全防御软件



视频教程

12.1 使用杀毒软件查杀 病毒	215
12.1.1 卡巴斯基的使用	215
12.1.2 瑞星杀毒软件的 使用	217
12.1.3 金山毒霸的使用	221
12.1.4 Norton的使用	223



视频教程

12.2 使用 Windows 防火墙 抵御网络攻击	224
-------------------------------------	-----

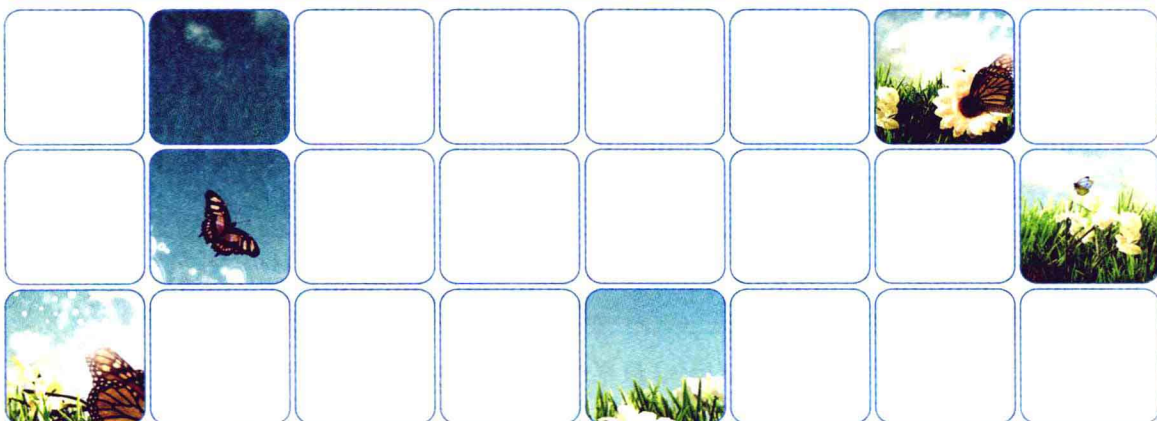


视频教程

12.2.1 Windows自带防火墙 简介	224
12.2.2 启用Windows系统 自带的防火墙	225
12.2.3 设置例外程序	225
12.2.4 防火墙高级设置	226
12.3 实战演练——使用 360 安 全卫士木马云查杀	226
12.3.1 本例操作思路	227
12.3.2 本例实战操作	227

新手有问必答

1. 如何处理已经感染病毒的电脑? 228
2. 360安全卫士都有哪些强大的功能? 228
3. 什么是“天网”防火墙? 229



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
- ◎ 黑客必经两道门——IP地址与端口
- ◎ 黑客常用的DOS命令
- ◎ 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。





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。

