

黑客攻防

■ 龙马工作室 编著

从
新手

到
高手

权威作者团队

资深计算机安全工程师与经验丰富的电脑教师联手编著。

为新手量身打造

从零开始、由浅入深，融合大量实战案例，采用图解和视频教学双模式，立体化辅助学习，使初学者能够真正掌握并熟练应用。

精选经典案例

结合日常生活、学习、工作中常见的案例和问题，以实用为宗旨，真正做到学以致用。

高手指导学习

『高手私房菜』和『高手秘籍篇』，帮助读者完成从新手到高手的蜕变。



18小时与本书内容同步的视频教学录像
93个精选电脑使用技巧电子书
60个精选电脑维护与故障处理技巧电子书
常见Windows 7蓝屏代码含义速查表
本书所有内容的教学用PPT

 **人民邮电出版社**
POSTS & TELECOM PRESS



黑客攻防



人民邮电出版社

北京

图书在版编目(CIP)数据

黑客攻防从新手到高手 / 龙马工作室编著. — 北京 : 人民邮电出版社, 2011. 2
ISBN 978-7-115-24414-7

I. ①黑… II. ①龙… 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(2010)第242612号

内 容 提 要

本书以零基础讲解为宗旨,深入浅出地讲解黑客攻防的各种方法和操作技巧,用实例引导读者深入学习数据保护、防范黑客攻击等知识。

本书共分7篇:第1篇【新手入门篇】主要讲解黑客的定义、黑客必备知识和黑客常用的攻击方法等;第2篇【木马与病毒攻防篇】主要讲解木马攻防与病毒攻防等;第3篇【系统攻防篇】主要讲解操作系统中的各种攻防技法,包括IE浏览器攻防、注册表攻防、系统漏洞攻防以及系统入侵与远程控制攻防等;第4篇【密码攻防篇】主要讲解加密与解密基础和各类密码的攻防,包括Windows密码的攻防、网络账号及密码的攻防和文件密码的攻防等;第5篇【网站攻防篇】主要讲解网站攻防和恶意网页代码攻防等;第6篇【QQ攻防篇】主要讲解QQ账号与密码攻防、QQ聊天攻防等;第7篇【高手秘籍篇】主要讲解黑客高手的操作技巧,包括后门技术、黑客足迹清除以及黑客游戏攻略等。

本书附赠一张DVD多媒体教学光盘,包含18小时与图书内容同步的视频教学录像,并附赠电脑使用技巧电子书、电脑维护与故障处理技巧电子书、Windows 7蓝屏代码含义速查表和本书内容的教学用PPT等,便于读者扩展学习。

本书不仅适合需要了解黑客攻防知识的初、中级读者学习使用,同时也可作为各类院校相关专业学生和电脑培训班学员的教材或辅导用书。

黑客攻防从新手到高手

- ◆ 编 著 龙马工作室
责任编辑 张 翼
- ◆ 人民邮电出版社出版发行 北京市崇文区夕照寺街14号
邮编 100061 电子函件 315@ptpress.com.cn
网址 <http://www.ptpress.com.cn>
北京铭成印刷有限公司印刷
- ◆ 开本: 787×1092 1/16
印张: 28.75 彩插: 1
字数: 702千字 2011年2月第1版
印数: 1—5000册 2011年2月北京第1次印刷

ISBN 978-7-115-24414-7

定价: 59.00元(附光盘)

读者服务热线: (010)67132692 印装质量热线: (010)67129223

反盗版热线: (010)67171154

广告经营许可证: 京崇工商广字第0021号

前言

电脑是现代信息社会的重要标志,掌握丰富的电脑知识、正确熟练地操作电脑已成为信息时代对每个人的要求。为满足广大读者的学习需要,我们针对不同学习对象的接受能力,总结了多位电脑高手、高级设计师及计算机教育专家的经验,精心编写了这套“从新手到高手”丛书。



丛书主要内容

本套丛书涉及读者在日常工作和学习中各个常见的电脑应用领域,在介绍软硬件的基础知识及具体操作时均以读者经常使用的版本为主,在必要的地方也兼顾了其他版本,以满足不同领域读者的需求。本套丛书主要包括以下品种。

《学电脑从新手到高手》	《学上网从新手到高手》
《Windows 7 从新手到高手》	《笔记本电脑应用从新手到高手》
《电脑维护与故障处理从新手到高手》	《系统安装、重装、备份与还原从新手到高手》
《黑客攻防从新手到高手》	《PowerPoint 2010 从新手到高手》
《Office 2010 办公应用从新手到高手》	《Office 2003 办公应用从新手到高手》
《Excel 2010 从新手到高手》	《Excel 2003 从新手到高手》
《Word/Excel 2010 办公应用从新手到高手》	《Word/Excel/PowerPoint 2010 三合一从新手到高手》
《Photoshop CS5 从新手到高手》	《AutoCAD 2011 从新手到高手》
《Dreamweaver CS5 从新手到高手》	《Flash CS5 从新手到高手》



本书特色

❖ 零基础、入门级的讲解

无论读者是否从事计算机相关行业,是否接触过黑客技术,都能从本书中找到最佳的起点。本书入门级的讲解,可以帮助读者快速地从新手向高手行列迈进。

❖ 精心排版,实用至上

双色印刷既美观大方又能够突出重点、难点。精心编排的内容可帮助读者对所学知识深化理解、触类旁通。

❖ 实例为主,图文并茂

在介绍过程中,每一个知识点均配有实例辅助讲解,每一个操作步骤均配有对应的插图加深认识。这种图文并茂的方法,能够使读者在学习过程中直观、清晰地看到操作过程和效果,

便于深刻理解和掌握。

❖ 高手指导，扩展学习

本书在每章的最后以“高手私房菜”的形式为读者提炼了各种高级操作技巧，同时在全书最后的“高手秘籍篇”中，还总结了大量系统实用的操作方法，以便读者学习到更多的内容。

❖ 双栏排版，超大容量

本书采用双栏排版的格式，大大扩充了信息容量，在400多页的篇幅中容纳了传统图书700多页的内容。这样，就能在有限的篇幅中为读者奉送更多的知识和实战案例。

❖ 超值随身速查手册

随书赠送黑客技巧查询手册，包括常用系统运行命令查询、常用命令行命令查询、黑客常用工具查询、黑客常用注册表修改技巧查询和黑客游戏集锦等，随用随查，方便携带。

❖ 书盘结合，互动教学

本书配套的多媒体教学光盘内容与书中知识紧密结合并互相补充。在多媒体光盘中，我们仿真工作、学习中的真实场景，帮助读者体验实际工作环境，并借此掌握日常所需的知识和技能以及处理各种问题的方法，达到学以致用目的，从而大大增强了本书的实用性。

📖 光盘特点

❖ 18小时全程同步视频教学录像

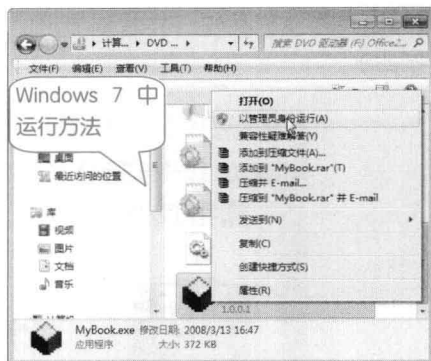
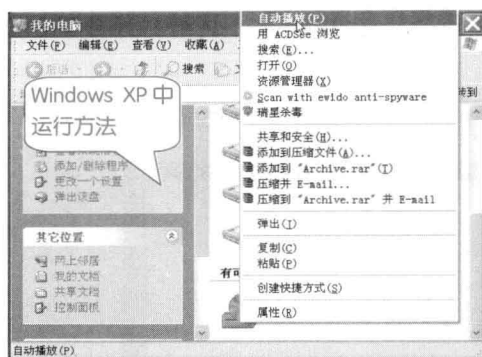
涵盖本书所有知识点，详细讲解每个实例及实战案例的操作过程及关键点。读者可以轻松掌握书中所有的黑客攻防的技巧，而且扩展的讲解部分可使读者获得更多的知识。

❖ 超多、超值资源大放送

随书赠送电脑使用技巧电子书、电脑维护与故障处理技巧电子书、Windows 7蓝屏代码含义速查表和本书内容的教学用PPT文件等，便于读者扩展学习。

📖 配套光盘运行方法

- ① 将光盘印有文字的一面朝上放入光驱中，几秒钟后光盘就会自动运行。
- ② 若光盘没有自动运行，可以双击桌面上的【我的电脑】图标打开【我的电脑】窗口，然后双击【光盘】图标，或者在【光盘】图标上单击鼠标右键，在弹出的快捷菜单中选择【自动播放】菜单项，光盘即可运行。（在Windows 7操作系统下第1次运行光盘，需要双击桌面上的【计算机】图标，然后右击【光盘】图标，在弹出的快捷菜单中选择【打开】，在打开的光盘文件夹中右击【MyBook.exe】，在弹出的快捷菜单中选择【以管理员身份运行】。以后运行光盘，则直接双击光盘图标即可。）



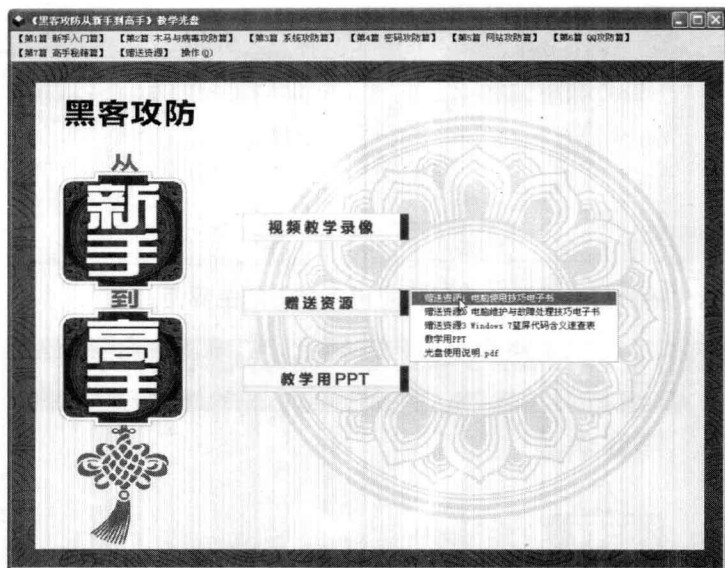
③ 光盘运行后会首先播放片头动画，之后便可进入光盘的主界面。



④ 单击【视频教学录像】按钮，在右侧弹出的菜单中依次选择相应的篇、章、录像名称，即可播放本节录像。



- ⑤ 单击【赠送资源】按钮，在右侧弹出的菜单中选择赠送资源名称，即可打开相应的赠送资源文件或文件夹。



- ⑥ 单击【教学用PPT】按钮，可打开相对应的【教学用PPT】文件夹。
- ⑦ 光盘使用详细说明请参阅光盘中“其他内容”文件夹下的“光盘使用说明.pdf”文档。
- ⑧ 选择【操作】>【退出本程序】菜单项，或者单击光盘主界面右上角的✕按钮，即可退出本光盘系统。

创作团队

本书由龙马工作室策划编写，王英英、侯永刚任主编，参与本书编写、资料整理、多媒体开发及程序调试的人员有孔万里、李震、王果、陈小杰、胡芬、陈芳、乔娜、王金林、刘卫卫、李强、周奎奎、彭超、李东颖、左琨、邓艳丽、任芳、王杰鹏、崔姝怡、左花苹、刘锦源、普宁、王常吉、师鸣若、杨雪青、孙娟和王菲等。

在编写过程中，我们竭尽所能地将最好的讲解呈现给读者，但也难免有疏漏和不妥之处，敬请广大读者不吝指正。若您在学习过程中产生疑问，或有任何建议，可发送电子邮件至 march98@163.com。

本书责任编辑的联系信箱：zhangyi@ptpress.com.cn。

龙马工作室

目 录

CONTENT

第1篇 新手入门篇

“黑客”是个神秘的群体，本篇将带领你揭开这层神秘的面纱，领略黑客的精彩世界。

第1章 认识黑客 ----- 2

 本章视频教学录像：19 分钟

有关黑客的信息很多，但大部分人都并不了解黑客，本章就带领大家来认识黑客这个群体。

1.1 黑客与骇客 -----	3
1.2 黑客的道德准则 -----	3
1.3 黑客所具备的技能 -----	4
1.4 骇客的违法行为和事件 -----	4
1.5 本书的目的 -----	6

第2章 黑客必备知识 ----- 7

 本章视频教学录像：51 分钟

黑客往往都是电脑高手，要成功地防御黑客，你也必须学会相关知识。

2.1 进程、端口和服务知多少 -----	8
2.2 Windows注册表 -----	10
2.3 常见网络协议 -----	14
2.4 黑客实战1——关闭和开启端口 -----	17
2.5 黑客实战2——关闭和开启服务 -----	19
2.6 黑客实战3——使用Ping命令测试网络 -----	21



高手私房菜 ----- 21

技巧1：新建和关闭系统进程 -----	22
技巧2：减少开机的滚动条时间 -----	23

第3章 黑客常用的攻击方法 ----- 24

 本章视频教学录像：58 分钟

只有充分了解黑客的常用攻击方法，才能有效地实施防御。

3.1 口令猜解攻击 -----	25
3.2 恶意代码攻击 -----	28
3.3 缓冲区溢出攻击 -----	29
3.4 网络欺骗攻击 -----	32

3.5 黑客实战1——恢复被恶意篡改的IE首页	34
3.6 黑客实战2——暴力破解压缩包的密码	35



高手私房菜	37
-------	----

技巧1: 查看ARP缓存表	37
技巧2: 在【网络邻居】中隐藏自己的计算机	37

第2篇 木马与病毒攻防篇

复杂的网络世界，病毒和木马横行。本篇带领你了解病毒和木马的原理和制作方法，以便进行有效的防范。

第4章 木马攻防 40

 本章视频教学录像：1小时6分钟

“木马”一词来源于“特洛伊木马”的典故，具有超强的隐蔽性。它可以不知不觉地在你的电脑中打开一扇后门，悄悄地偷走你的资料。

4.1 认识木马	41
4.2 木马自我保护	45
4.3 一览无余——常见木马攻击	50
4.4 木马无处遁形——木马清除软件	58
4.5 黑客实战1——如何检测木马是否加过壳	69
4.6 黑客实战2——木马预防实战	70



高手私房菜	71
-------	----

技巧1: 黑客如何将木马伪装成电子书	71
技巧2: 黑客如何修改木马服务端的图标	73

第5章 病毒攻防 75

 本章视频教学录像：1小时11分钟

了解病毒的原理以及防御技巧，不再“谈毒色变”。

5.1 认识病毒真面目	76
5.2 Windows系统病毒	77
5.3 U盘病毒	81
5.4 邮箱病毒	83
5.5 病毒的防御	83
5.6 查杀病毒	92
5.7 监控程序文件以防御病毒	97
5.8 黑客实战——熊猫烧香病毒的预防	99



高手私房菜	100
-------	-----

技巧1: 如何在Word2003中预防宏病毒	100
------------------------	-----

技巧2: 通过修改文件的关联性预防病毒	101
技巧3: 预防邮件病毒	102

第3篇 系统攻防篇

黑客往往以侵入系统为目的。掌握了操作系统, 就等于掌握了一切。

第6章 IE浏览器攻防 105

 本章视频教学录像: 47 分钟

IE 浏览器是最常用的上网软件之一, 也就顺理成章地成为了黑客眼中的香饽饽。

6.1 常见IE浏览器攻击方式	106
6.2 IE浏览器的自我防护	115
6.3 使用第三方软件保护IE浏览器	117
6.4 黑客实战1——浏览器网址泄密的预防	128
6.5 黑客实战2——如何在浏览器窗口中屏蔽广告	130



高手私房菜 131

技巧1: 清除IE浏览器中的表单	131
技巧2: IE炸弹的防御	132
技巧3: 设置IE浏览器项目	133

第7章 注册表攻防 134

 本章视频教学录像: 53 分钟

注册表是操作系统的核心, 控制了注册表就等于控制了操作系统。

7.1 常见注册表入侵方式	135
7.2 注册表的防护	136
7.3 使注册表轻装上阵	140
7.4 医治“生病”的注册表	148
7.5 黑客实战1——设置注册表隐藏保护策略	154
7.6 黑客实战2——设置Windows系统自动登录	155



高手私房菜 156

技巧1: 如何禁止访问控制面板	156
技巧2: 只允许运行指定的程序	157

第8章 系统漏洞攻防 159

 本章视频教学录像: 1 小时 15 分钟

操作系统和软件都可能存在各种各样的漏洞, 利用这些漏洞, 进入操作系统如入无人之境。

8.1 系统漏洞概述	160
------------	-----



8.2	RPC服务远程漏洞攻击	164
8.3	IDQ漏洞攻击	168
8.4	WebDAV漏洞攻击	171
8.5	系统漏洞防御	173
8.6	黑客实战1——防火墙也不安全	183
8.7	黑客实战2——HTTP CONNECT代理“请求”不可信	184



高手私房菜	187
-------	-----

技巧1：如何让Windows 7安装完补丁后不自动重启	187
技巧2：使用金山卫士修复Windows 7操作系统	188

第9章 系统入侵与远程控制攻防 190



本章视频教学录像：1小时42分钟

黑客入侵操作系统的最终目的，就是实现远程控制。

9.1	计算机系统知多少	191
9.2	虎视眈眈——入侵计算机系统	191
9.3	对症下药——抢救被入侵的系统	197
9.4	利用系统自带功能实现远程控制	201
9.5	经典远程控制工具——PcAnywhere	203
9.6	其他远程控制工具	209
9.7	防止主机成为“肉鸡”的安全措施	213
9.8	实时保护系统安全	218
9.9	黑客实战1——使用MT工具创建复制账号	221
9.10	黑客实战2——使用天网防火墙防护系统安全	222



高手私房菜	224
-------	-----

技巧1：禁止更改【开始】菜单和任务栏	224
技巧2：确定可能开放的端口服务	225

第4篇 密码攻防篇

即使为文件加再多的锁，黑客也能轻松找到钥匙。

第10章 加密与解密基础 228



本章视频教学录像：16分钟

电脑世界中的锁和钥匙是这样打造的。

10.1	什么是密码学	229
10.2	密码体制的分类	229
10.3	破解密码的常用方式	230

第11章 Windows密码的攻防 -----234



本章视频教学录像：44分钟

掌握了Windows的密码，就能轻而易举地攻破操作系统，因此应加强密码的设置。

11.1 Windows密码那些事	235
11.2 为Windows各个账户设置密码	235
11.3 针锋相对——破解Windows各个账户的密码	238
11.4 未雨绸缪——加强Windows账户密码的管理	242
11.5 黑客实战1——如何判断Guest账户是否被利用	248
11.6 黑客实战2——加强对Guest账户的管理	248



高手私房菜 -----249

技巧1：设置屏幕保护密码	249
技巧2：破解屏幕保护密码	250

第12章 网络账号及密码的攻防 -----252



本章视频教学录像：49分钟

网络账号是用户在网上的身份证，获取了这些身份证，黑客们就可以对用户的网络资料为所欲为。

12.1 MSN账号及密码攻防	253
12.2 网银账号及密码攻防	256
12.3 邮箱账号及密码攻防	270
12.4 网游账号及密码攻防	274
12.5 黑客实战1——攻击CS服务器解析	279
12.6 黑客实战2——用内存补丁破解传奇外挂	280



高手私房菜 -----282

技巧1：如何将收到的“邮件炸弹”标记为垃圾邮件	282
技巧2：股票防盗安全系统的使用	283

第13章 文件密码的攻防 -----285



本章视频教学录像：1小时5分钟

为文件配备一把锁和钥匙。

13.1 加密、解密Word文件	286
13.2 加密、解密Excel文件	290
13.3 加密、解密PDF文件	294
13.4 加密、解密EXE文件	299
13.5 加密、解密压缩文件	302
13.6 黑客实战1——如何利用系统自带的“加密文件系统”进行加密	308
13.7 黑客实战2——如何备份系统	309



高手私房菜	312
技巧1: 通过加壳保护文件	312
技巧2: 如何突破试用软件的时间限制	314

第5篇 网站攻防篇

网站是展示和发布信息的窗口，这些窗口也给了黑客可乘之机。

第14章 网站攻防 317

本章视频教学录像：1 小时 6 分钟

增强网站的安全，避免各种形式的攻击，以免网站顷刻间变为摆设。

14.1 网站基础知识	318
14.2 DoS（拒绝服务）攻击	320
14.3 DDoS（分布式拒绝服务）攻击	325
14.4 SQL注入攻击	330
14.5 网站攻击的防御	334
14.6 黑客实战——分析网站漏洞	338



高手私房菜	340
技巧1: 如何保护本机中的数据库	340
技巧2: 保护网站安全技巧	341

第15章 恶意网页代码攻防 343

本章视频教学录像：39 分钟

网页常常成为黑客藏匿木马和病毒的载体，本章为你揭秘精彩网页背后的秘密。

15.1 恶意网页代码概述	344
15.2 恶意网页代码攻击形式	345
15.3 恶意网页代码的修复与防范	352
15.4 黑客实战1——利用点歌台漏洞攻击论坛	360
15.5 黑客实战2——利用恶意网页脚本攻击论坛	361



高手私房菜	362
技巧1: 如何查看加密网页的源码	363
技巧2: 利用电影网站中的SQL注入漏洞获取管理员权限	364

第6篇 QQ攻防篇

QQ已经成为网民们必备的聊天工具之一，而黑客和网民们也一直在为QQ的安全周旋着。

第 16 章 QQ 账号与密码攻防 ----- 367

 本章视频教学录像：50 分钟

QQ 中一长串的好友列表，如果不想顷刻全无，本章的这些内容务必要了解。

16.1 忘了QQ密码怎么办 -----	368
16.2 盗取QQ账号及密码 -----	371
16.3 不需要密码登录QQ -----	380
16.4 QQ密码防护 -----	381
16.5 黑客实战1——清除QQ木马 -----	385
16.6 黑客实战2——防范QQ木马 -----	388



高手私房菜 ----- 389

技巧1：使用QQ维护王维护QQ的安全 -----	389
技巧2：安全快捷QQ -----	390
技巧3：利用QQ远程协助 -----	392

第 17 章 QQ 聊天攻防 ----- 393

 本章视频教学录像：31 分钟

警惕黑客们在 QQ 聊天中的恶作剧。

17.1 聊天记录攻防 -----	394
17.2 强制聊天 -----	396
17.3 QQ信息炸弹 -----	398
17.4 黑客实战——使用QQ远程攻击器发送信息炸弹 -----	403



高手私房菜 ----- 404

技巧1：在QQ群共享中共享文件 -----	404
技巧2：在网页中登录QQ -----	405
技巧3：在QQ群中进行多人语音聊天 -----	405
技巧4：从好友的账号中删除我的QQ号 -----	406

第7篇 高手秘籍篇

看看黑客中的高手在网络中逍遥的绝技。

第 18 章 保留一把钥匙——后门技术 ----- 408

 本章视频教学录像：40 分钟

为自己保留一把钥匙，方便下次再来，这就是黑客技术中的后门。

18.1 什么后门 -----	409
18.2 账号后门 -----	409
18.3 漏洞后门 -----	415



18.4	系统服务后门	416
18.5	木马后门	421
18.6	黑客实战1——利用系统漏洞自动加载后门	422
18.7	黑客实战2——利用Regedt32克隆管理员账号	425



高手私房菜	426
-------	-----

技巧1: 删除各种脚本对象以禁止asp木马运行	426
技巧2: 设置网站访问权限	427
技巧3: 利用SRVINSTW删除系统服务	428

第 19 章 大雪无痕——黑客足迹清除方法 430



本章视频教学录像: 31 分钟

来无影、去无踪, 不在“房间”留下任何“足迹”和“指纹”。

19.1	黑客留下的足迹——日志	431
19.2	清除日志文件	432



高手私房菜	438
-------	-----

技巧1: 清除WWW和FTP日志	438
技巧2: 使用批处理清除远程主机日志	440
技巧3: 后门程序的上传与隐藏	440

第 20 章 检测你的黑客水平——黑客游戏攻略 442



本章视频教学录像: 12 分钟

通过本书, 你学到了多少, 赶紧通过游戏检测一下吧!

20.1	层级1——关卡型黑客游戏	443
20.2	层级2——任务型黑客游戏	444

赠送资源 (光盘中)

赠送资源1 电脑使用技巧电子书

赠送资源2 电脑维护与故障处理技巧电子书

赠送资源3 Windows 7蓝屏代码含义速查表

第1篇

新手入门篇

- ▶ 第1章 认识黑客
- ▶ 第2章 黑客必备知识
- ▶ 第3章 黑客常用的攻击方法

第 1 章

认识黑客



本章视频教学录像：19分钟

高手指引

随着网络的发展和普及，电子邮件、网站、电子商务、病毒等名词扑面而来，越来越多的人走进了网络生活。然而，网络中有这样一群人，他们具有高超的计算机技术和网络技术，部分人进行着网络安全的维护，被称之为“黑客”，部分人利用网络进行破坏，被称之为“骇客”。

重点导读

- + 了解黑客与骇客的区别
- + 了解黑客的道德准则
- + 了解黑客所具备的技能
- + 了解骇客的违法行为和事件
- + 了解本书的目的