



全彩升级

云视频教学

入门与进阶
本套丛书总销量超过
300000册

黑客攻防 入门与进阶

(第2版)



陈宏波◎编著

图书&光盘

双栏紧排，全彩印刷；大容量多媒体教学光盘收录书中实例视频和模拟练习，播放时间长达18个小时以上；免费赠送15小时《家庭电脑应用》+15小时《电脑组装·维护·故障排除》+15小时《系统安装、重装与优化》+15小时《新手学上网》+15小时《中文版Windows 7》教学演示视频。

贴心服务

精心构建的特色服务论坛 (<http://bbs.btbook.com.cn>) 和技术交流QQ群 (101617400、2463548)，为读者提供24小时便捷的在线服务和免费教学资源。

云视频教学

光盘附赠的云视频教学平台(普及版)，能够让读者轻松访问上百GB容量的免费教学视频学习资源库；该平台拥有目前最主流、最时尚的计算机软硬件应用知识，海量的多媒体教学视频，让您轻松学习，无师自通！



清华大学出版社



黑客攻防 入门与进阶

(第2版)



陈宏波◎编著



清华大学出版社
北京

内 容 简 介

本书是《入门与进阶》系列丛书之一,全书以通俗易懂的语言、翔实生动的实例,全面介绍黑客的攻击方式和防范黑客攻击的相关知识。本书共分10章,内容涵盖了黑客的基础知识、信息数据的嗅探与扫描、密码的攻击与防御、系统漏洞的攻击与防御、木马的攻击与防御、网络中的攻击与防御、黑客的入侵行为、远程控制技术、脚本攻击技术、黑客攻防实用技巧。

本书采用图文并茂的方式,使读者能够轻松上手。全书双栏紧排,全彩印刷,同时配以制作精良的多媒体互动教学光盘,方便读者扩展学习。附赠的DVD光盘中包含18小时与图书内容同步的视频教学录像和3~5套与本书内容相关的多媒体教学视频。此外,光盘中附赠的云视频教学平台(普及版)能够让读者轻松访问上百GB容量的免费教学视频学习资源库。

本书面向电脑初学者,是广大电脑初中级用户、家庭电脑用户,以及不同年龄阶段电脑爱好者的首选参考书。

本书封面贴有清华大学出版社防伪标签,无标签者不得销售。

版权所有,侵权必究。侵权举报电话:010-62782989 13701121933

图书在版编目(CIP)数据

黑客攻防入门与进阶 / 陈宏波 编著. —2版. —北京:清华大学出版社, 2013.7
(入门与进阶)

ISBN 978-7-302-31626-8

I. ①黑… II. ①陈… 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(2013)第037343号

责任编辑:胡辰浩 袁建华

装帧设计:牛静敏

责任校对:邱晓玉

责任印制:杨 艳

出版发行:清华大学出版社

网 址: <http://www.tup.com.cn>, <http://www.wqbook.com>

地 址:北京清华大学学研大厦A座 邮 编:100084

社总机:010-62770175 邮 购:010-62786544

投稿与读者服务:010-62776969, c-service@tup.tsinghua.edu.cn

质量反馈:010-62772015, zhiliang@tup.tsinghua.edu.cn

印装者:北京亿浓世纪彩色印刷有限公司

经 销:全国新华书店

开 本:150mm×215mm 印 张:16.75 插 页:4 字 数:418千字
(附光盘1张)

版 次:2010年1月第1版 2013年7月第2版 印 次:2013年7月第1次印刷

印 数:1~5000

定 价:29.80元

产品编号:046553-01

读者意见调查表

尊敬的读者：

衷心感谢您购买和阅读我们的图书。为了给您提供更好的服务，帮助我们改进和完善图书出版，请填写本读者意见调查表，并按底部的地址邮寄给我们。我们将定期选出若干名热心读者，免费赠送我们出版的图书。同时，我们将充分考虑您的建议，并尽可能给您满意的答复。谢谢！

姓名：	性别： ☐ 男 ☐ 女	年龄：
职业：	文化程度：	电话：
通信地址：	电子信箱：	
购买的图书：	书号：	

1. 您是如何获知本书的：

☐朋友推荐 ☐书店 ☐图书目录 ☐杂志、报纸、网络等 ☐其他

2. 您从哪里购买本书：

☐新华书店 ☐计算机专业书店 ☐网上书店 ☐其他

3. 您对本书的评价是：

技术内容	☐ 很好	☐ 一般	☐ 较差	☐ 理由 _____
文字质量	☐ 很好	☐ 一般	☐ 较差	☐ 理由 _____
版式封面	☐ 很好	☐ 一般	☐ 较差	☐ 理由 _____
印装质量	☐ 很好	☐ 一般	☐ 较差	☐ 理由 _____
图书定价	☐ 太高	☐ 合适	☐ 较低	☐ 理由 _____

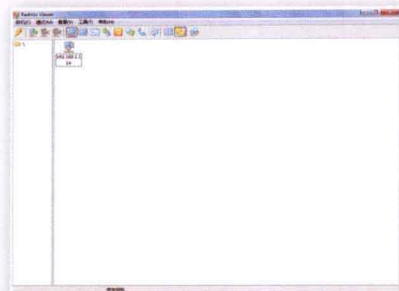
4. 您希望我们的图书在哪些方面进行改进？

5. 您最希望我们出版哪方面的图书？

6. 特别说明：

如果您是学校或者培训班教师，选用了本书作为教材，请在这里注明您对本书作为教材的评价，我们会尽力为您提供更多方便教学的材料，谢谢！

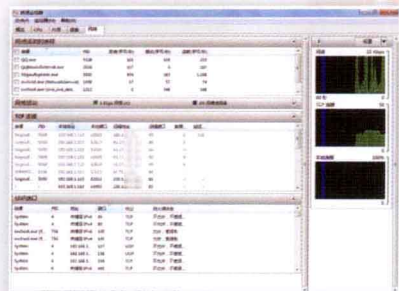
● 请寄：北京市清华大学南门内300米处出版社绿楼一层第五事业部 胡辰浩收
邮编：100084 电话：010-62796045 E-mail: huchenhao@263.net



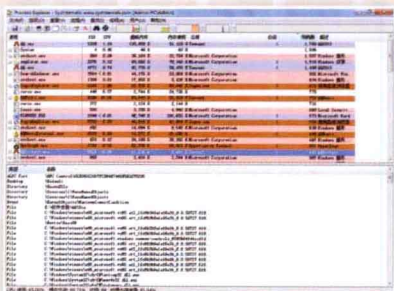
使用Radmin远程控制工具



使用啊D注入工具



使用系统资源监视器



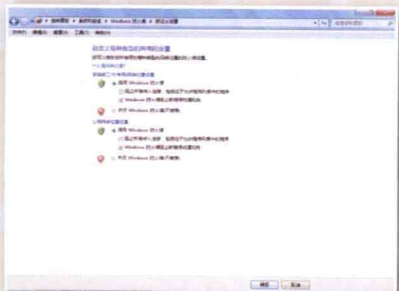
使用Process Explorer任务查看器



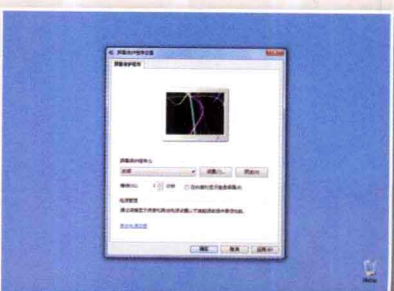
备份Windows7系统



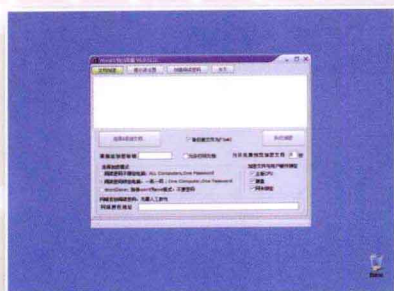
启动Telnet功能



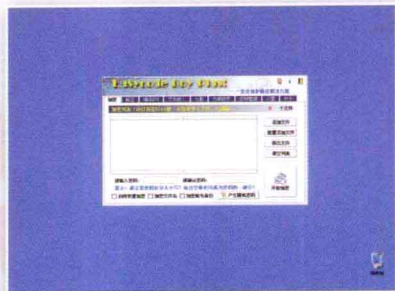
打开系统防火墙



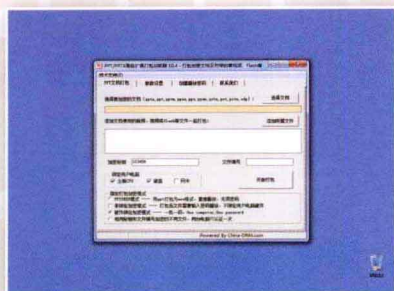
设置屏幕保护功能



使用Word文档加密器加密Word文档



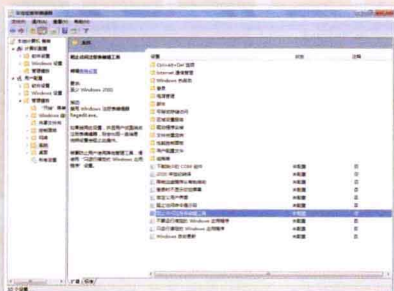
使用万能加密器工具



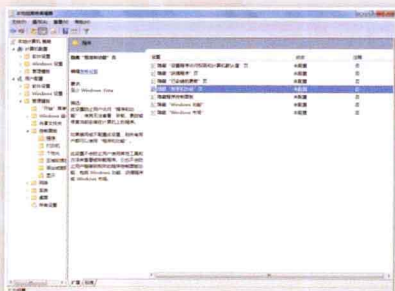
使用PPTX扩展打包器



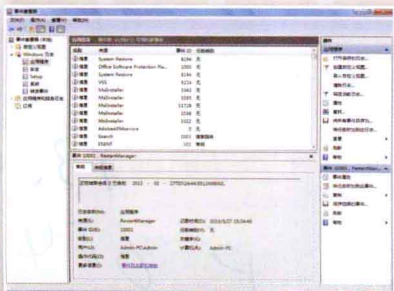
查看安装过的安全补丁编号



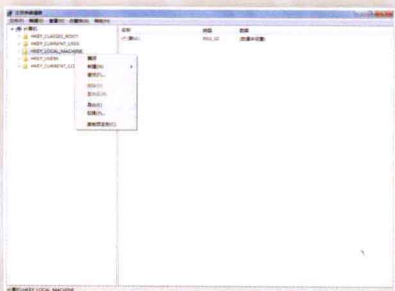
设置禁止访问注册表



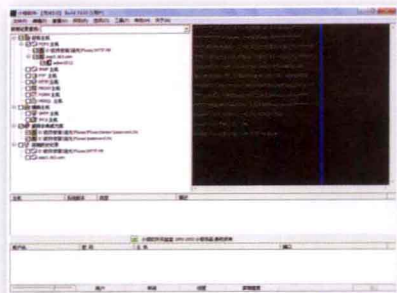
隐藏控制面板中的图标



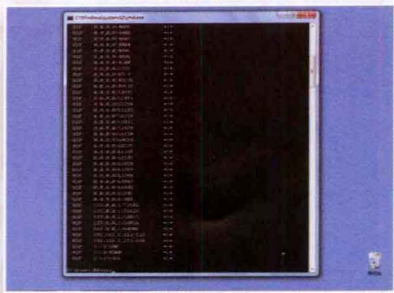
使用事件查看器



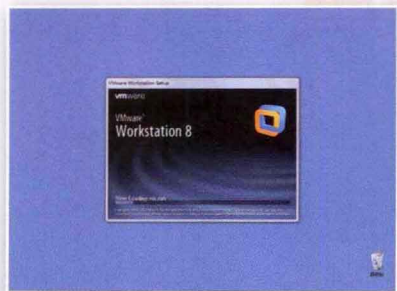
备份注册表



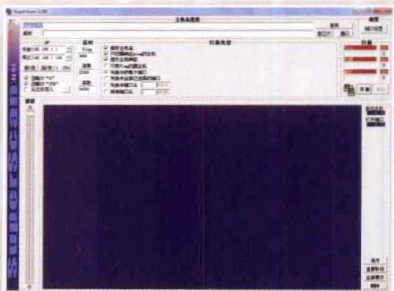
使用流光扫描器进行扫描



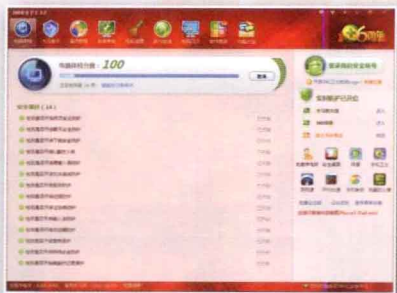
查看系统开放的端口



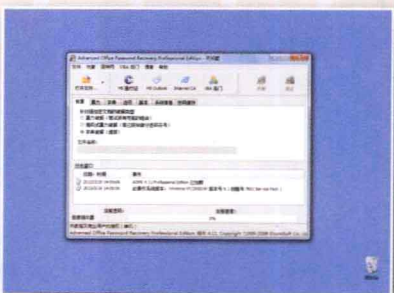
创建虚拟机



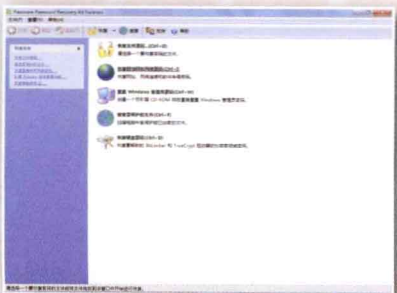
使用Super Scan扫描器进行扫描



使用360安全卫士



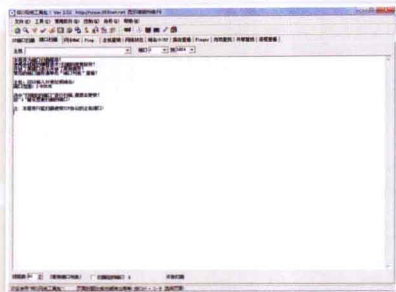
解密Word文档



使用密码恢复工具



解密压缩包文件



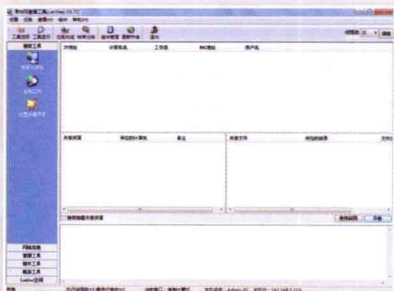
使用Armitage网络工具包进行扫描



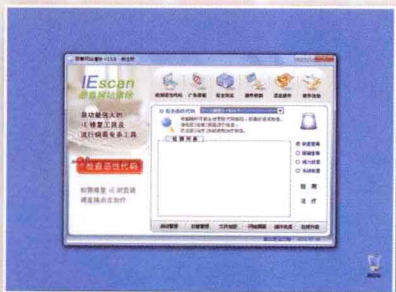
使用反间谍专家



使用Windows清理助手



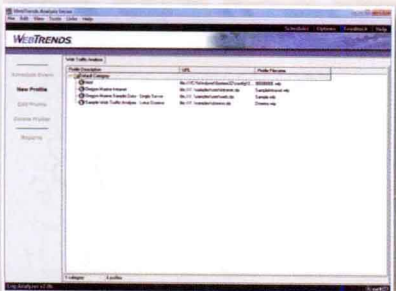
使用局域网查看工具



使用恶意代码清除器工具



使用Easyspy工具



使用日志分析工具



使用CCleaner工具进行系统优化

光盘主要内容

本光盘为《入门与进阶》丛书的配套多媒体教学光盘，光盘中的内容包括 18 小时与图书内容同步的视频教学录像、相关素材文件和模拟练习。光盘采用全程语音讲解、互动练习、真实详细的操作演示等方式，详细讲解了电脑以及各种应用软件的使用方法和技巧。此外，本光盘附赠大量学习资料，其中包括 3 ~ 5 套与本书内容相关的多媒体教学演示视频。

光盘运行环境

- 赛扬 1.0GHz 以上 CPU
- 512MB 以上内存
- 500MB 以上硬盘空间
- Windows XP/Vista/7 操作系统
- 屏幕分辨率 1024×768 以上
- 8 倍速以上的 DVD 光驱

光盘操作方法

将 DVD 光盘放入 DVD 光驱，几秒钟后光盘将自动运行。如果光盘没有自动运行，可双击桌面上的【我的电脑】或【计算机】图标，在打开的窗口中双击 DVD 光驱所在盘符，或者右击该盘符，在弹出的快捷菜单中选择【自动播放】命令，即可启动光盘进入多媒体互动教学光盘主界面。

光盘运行后会自动播放一段片头动画，若您想直接进入主界面，可单击鼠标跳过片头动画。



进入普通视频教学模式

进入学习进度查看模式

进入模拟练习操作模式

打开素材文件夹

退出光盘学习

进入自动播放演示模式

阅读本书内容介绍

打开赠送的学习资料文件夹

单击进入云视频教学界面

单击进入官方学习论坛

普通视频教学模式



图1



图2



图3



光盘使用说明



视频播放控制进度条

控制背景和解说音量大小



同步显示解说文字内容



模拟练习操作模式



图1



图2

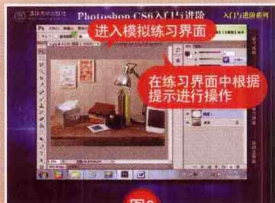


图3

学习进度查看模式



图1



图2



图3

自动播放演示模式



图1



图2

赠送的教学资料



图1



图2



丛书序

首先,感谢并恭喜您选择本系列丛书!《入门与进阶》系列丛书挑选了目前人们最关心的方向,通过实用精炼的讲解、大量的实际应用案例、完整的多媒体互动视频演示、强大的网络售后教学服务,让读者从零开始、轻松上手、快速掌握,让所有人都能看得懂、学得会、用得着电脑知识,真正做到满足工作和生活的需要!

丛书、光盘和网络服务特色

双栏紧排,彩色印刷,超大容量:本丛书采用双栏紧排的格式,使图文排版紧凑实用,其中260多页的篇幅容纳了传统图书一倍以上的内容。从而在有限的篇幅内为读者奉献更多的电脑知识和实战案例,让读者的学习效率达到事半功倍的效果。

结构合理,内容精炼,技巧实用:本丛书紧密结合自学的特点,由浅入深地安排章节内容,让读者能够一学就会、即学即用。书中的范例通过添加大量的“知识点滴”和“高手点拨”的注释方式突出重要知识点,使读者轻松领悟每一个范例的精髓所在。

书盘结合,互动教学,操作简单:丛书附赠一张精心开发的多媒体教学光盘,其中包含了18小时左右与图书内容同步的视频教学录像。光盘采用全程语音讲解、真实详细的操作演示等方式,紧密结合书中的内容对各个知识点进行深入的讲解。光盘界面注重人性化设计,读者只需要单击相应的按钮,即可方便地进入相关程序或执行相关操作。

免费赠品,素材丰富,量大超值:附赠光盘采用大容量DVD格式,收录书中实例视频、源文件、模拟练习以及3~5套与本书内容相关的多媒体教学视频。此外,光盘附赠的云视频教学平台(普及版)能够让读者轻松访问上百GB容量的免费教学视频学习资源库。让读者花最少的钱学到最多的电脑知识,真正做到物超所值。

特色论坛,在线服务,贴心周到:本丛书通过技术交流QQ群(101617400、2463548)和精心构建的特色服务论坛(<http://bbs.btbook.com.cn>),为读者提供24小时便捷的在线服务。用户登录官方论坛不但可以下载大量免费的网络教学资源,还可以参加丰富多彩的有奖活动。

读者对象和售后服务

本丛书是广大电脑初中级用户、家庭电脑用户和中老年电脑爱好者,或学习某一应用软件用户的首选参考书。

最后感谢您对本丛书的支持和信任,我们将再接再厉,继续为读者奉献更多更好的优秀图书,并祝愿您早日成为电脑高手!

如果您在阅读图书或使用电脑的过程中有疑惑或需要帮助,可以登录本丛书的信息支持网站(<http://www.tupwk.com.cn/improve2>)或通过E-mail(wkservice@vip.163.com)联系,也可以在博图官方论坛(<http://bbs.btbook.com.cn>)上留言,本丛书的作者或技术人员会提供相应的技术支持。



前言

电脑操作能力已经成为当今社会不同年龄层次的人群必须掌握的一门技能。为了使读者在短时间内轻松掌握电脑各方面应用的基本知识,并快速解决生活和工作中遇到的各种问题,我们组织了一批教学精英和业内专家特别为电脑学习用户量身定制了这套《入门与进阶》系列丛书。

《黑客攻防入门与进阶(第2版)》是这套丛书中的一本,该书从读者的学习兴趣和实际需求出发,合理安排知识结构,由浅入深、循序渐进,通过图文并茂的方式讲解黑客攻击和防范黑客攻击的各种应用方法。全书共分为10章,主要内容如下。

- 第1章:介绍黑客的概念及相关基础知识。
- 第2章:介绍在黑客攻防中信息数据的嗅探与扫描技巧。
- 第3章:介绍在黑客攻防中密码的攻击与防御技巧。
- 第4章:介绍在黑客攻防中系统漏洞的攻击与防御技巧。
- 第5章:介绍在黑客攻防中木马的攻击与防御技巧。
- 第6章:介绍在网络中的攻击与防御技巧。
- 第7章:介绍在黑客攻防中的入侵技巧。
- 第8章:介绍在黑客攻防中的远程控制技术及应用技巧。
- 第9章:介绍在黑客攻防中的脚本攻击技术及应用技巧。
- 第10章:介绍在黑客攻防中的常用攻防实用技巧。

本书附赠一张精心开发的DVD多媒体教学光盘,其中包含了18小时左右与图书内容同步的视频教学录像。光盘采用全程语音讲解、情景式教学、互动练习、真实详细的操作演示等方式,紧密结合书中的内容对各个知识点进行深入的讲解。让读者在阅读本书的同时,享受到全新的交互式多媒体教学。

此外,本光盘附赠大量学习资料,其中包括3~5套与本书内容相关的多媒体教学视频和云视频教学平台(普及版)。该平台能够让读者轻松访问上百GB容量的免费教学视频学习资源库。使读者在短时间内掌握最为实用的电脑知识,真正达到轻松进阶,无师自通的效果。

除封面署名的作者外,参加本书编辑和制作的人员还有洪妍、方峻、何亚军、王通、高娟妮、杜思明、张立浩、孔祥亮、陈笑、王维、牛静敏、牛艳敏、何俊杰、葛剑雄、王璐、何美英、陈彬、刘芸、沈亚静、吕斌、庄春华等人。由于作者水平所限,本书难免有不足之处,欢迎广大读者批评指正。我们的邮箱是huchenhao@263.net,电话是010-62796045。

《入门与进阶》丛书编委会
2013年5月

第1章 黑客的基础知识



1.1 认识黑客	2
1.1.1 黑客的由来	2
1.1.2 黑客的定义	2
1.1.3 黑客的特点	2
1.2 认识IP地址	4
1.2.1 IP地址的定义	4
1.2.2 IP地址的分类	4
1.2.3 IP地址的组成	5
1.3 认识端口	6
1.3.1 端口的分类	6
1.3.2 查看系统开放的端口	6
1.3.3 关闭访问指定的端口	7
1.3.4 限制访问指定的端口	7
1.4 黑客的术语与常见命令	10
1.4.1 黑客常用术语	10

1.4.2 ping命令	11
1.4.3 netstat命令	12
1.4.4 tracer命令	12
1.4.5 net命令	12
1.4.6 telnet命令	13
1.4.7 FTP命令	14
1.4.8 ipconfig命令	14
1.5 创建系统测试环境	15
1.5.1 安装虚拟机	15
1.5.2 创建虚拟机	16
1.6 进阶练习	18
1.6.1 新建Windows 7系统	18
1.6.2 使用系统防火墙	19
1.7 高手解答	20

第2章 信息数据的嗅探与扫描



2.1 获取网络中的信息	22
2.1.1 获取目标IP地址	22
2.1.2 获取目标所属地区	22
2.1.3 查看网站备案信息	22
2.2 端口扫描工具	23
2.2.1 扫描器的工作原理	23
2.2.2 Super Scan扫描器	24
2.2.3 X-Scan扫描器	25
2.2.4 阻止端口扫描	28
2.3 漏洞扫描工具	28
2.3.1 安装更新补丁	29
2.3.2 SSS扫描器	29

2.3.3 流光扫描器	34
2.3.4 使用第三方软件修复	37
2.4 常用嗅探工具	38
2.4.1 IRIS网络嗅探工具	38
2.4.2 【影音神探】嗅探器	41
2.5 加壳与脱壳工具	44
2.5.1 加壳工具	44
2.5.2 脱壳工具	45
2.5.3 查壳工具	45
2.6 进阶练习	46
2.7 高手解答	47

第3章 密码的攻击与防御



3.1 设置系统密码	50
-------------------	-----------

3.1.1 设置系统启动密码	50
----------------	----

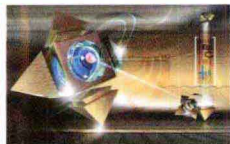
3.1.2 设置屏幕保护密码	51
3.2 办公文件的加密与解密	51
3.2.1 Word加密与解密	52
3.2.2 Excel加密与解密	54
3.2.3 PDF加密与解密	56
3.2.4 压缩文件加密与解密	58
3.2.5 文件夹加密与解密	61
3.3 使用加密与解密软件	63
3.3.1 Windows加密大师	63
3.3.2 文件夹加密精灵	64

3.3.3 图片保护狗	66
3.3.4 Word文档加密器	67
3.3.5 天盾加密软件	69
3.3.6 万能加密器	70
3.3.7 终极程序加密器	72
3.3.8 文件分割加密	73
3.4 进阶练习	75
3.4.1 PPT/PPTX扩展打包加密器	75
3.4.2 Chop分割工具	76
3.5 高手解答	78

第4章 系统漏洞的攻击与防御

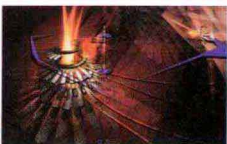
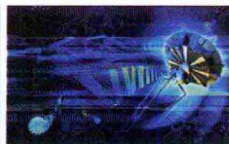
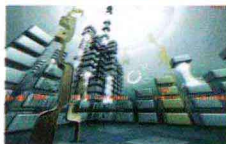


4.1 认识系统漏洞	80
4.1.1 漏洞危害程度的划分	80
4.1.2 Windows安全漏洞	80
4.1.3 查找系统中的漏洞	81
4.1.4 预防溢出型漏洞攻击	82
4.2 注册表编辑器的安全设置	82
4.2.1 入侵注册表	83
4.2.2 禁止访问注册表	83
4.2.3 禁止编辑注册表	84
4.2.4 禁止Remote Registry	85
4.2.5 禁止更改系统登录密码	85
4.2.6 优化注册表	86
4.3 本地组策略编辑器的安全设置	88
4.3.1 增强密码安全性	88
4.3.2 设置账户锁定组策略	90
4.3.3 禁止应用程序的使用	91



4.3.4 禁止安装和卸载程序	92
4.3.5 设置用户权限级别	93
4.3.6 禁用Windows程序	95
4.4 本地安全策略	95
4.4.1 禁止在登录前关机	96
4.4.2 不显示最后的用户名	96
4.5 漏洞利用工具	97
4.5.1 使用WINNTAutoAttack	97
4.5.2 啊D网络工具包	98
4.5.3 RPC漏洞	99
4.6 进阶练习	101
4.6.1 使用事件查看器	101
4.6.2 清除开机自动弹出网页	102
4.6.3 备份与恢复注册表	102
4.7 高手解答	103

第5章 木马的攻击与防御



5.1 木马的基础知识	106
5.1.1 木马的概念	106
5.1.2 木马的种类	106
5.1.3 木马的特点	107
5.2 木马的攻击	107
5.2.1 木马的伪装方式	107

5.2.2 使用文件捆绑器	108
5.2.3 制作自解压木马	110
5.2.4 网页木马生成器	112
5.3 木马的查杀与防范	112
5.3.1 木马清除专家2012	113
5.3.2 使用木马克星	115

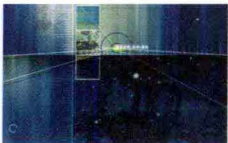
5.3.3 使用木马清道夫.....	117	5.5.2 VBS脚本病毒.....	127
5.4 间谍软件.....	120	5.5.3 U盘病毒.....	128
5.4.1 查找隐藏的间谍.....	120	5.6 进阶练习.....	130
5.4.2 Windows清理助手.....	121	5.6.1 【灰鸽子】远程管理.....	130
5.4.3 AD-Aware广告杀手.....	123	5.6.2 使用【花指令】.....	131
5.5 病毒的防范.....	126	5.7 高手解答.....	131
5.5.1 病毒的概念.....	126		

第6章 网络中的攻击与防御



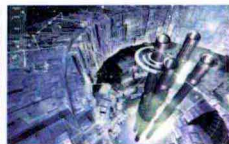
6.1 网络中的欺骗.....	134	6.4 局域网的攻击与防御.....	148
6.1.1 常见欺骗方式.....	134	6.4.1 局域网的拓扑结构.....	148
6.1.2 增强浏览器的防范.....	134	6.4.2 无线局域网的优点.....	148
6.1.3 提高防范意识.....	135	6.4.3 局域网查看工具.....	149
6.2 维护QQ安全.....	135	6.4.4 局域网ARP攻击工具.....	152
6.2.1 QQ强制聊天.....	135	6.4.5 使用网络监控器.....	154
6.2.2 QQ病毒木马专杀工具.....	136	6.5 网页中的恶意代码.....	158
6.2.3 QQ聊天记录查看器.....	138	6.5.1 恶意代码的特征.....	158
6.2.4 QQ安全的保护.....	140	6.5.2 非过滤性病毒.....	158
6.2.5 取回QQ密码.....	142	6.5.3 清除恶意代码.....	158
6.3 电子邮件的安全使用.....	144	6.5.4 提高IE浏览器安全.....	159
6.3.1 电子邮件病毒特点.....	144	6.6 进阶练习.....	161
6.3.2 电子邮件炸弹攻击.....	144	6.6.1 使用Cain&Abel工具.....	161
6.3.3 获取密码的手段.....	145	6.6.2 精锐网吧辅助工具.....	163
6.3.4 找回邮箱密码.....	146	6.7 高手解答.....	165

第7章 黑客的入侵行为



7.1 入侵检测分类.....	168	7.3.1 保护用户隐私.....	180
7.1.1 入侵检测系统分类.....	168	7.3.2 魔方优化大师.....	182
7.1.2 网络入侵检测.....	168	7.3.3 使用CCleaner工具.....	183
7.1.3 使用Domain工具.....	172	7.3.4 使用IIS服务器日志.....	186
7.1.4 入侵检测所利用的信息.....	174	7.4 进阶练习.....	189
7.2 清理入侵痕迹.....	174	7.4.1 设置访问过的链接颜色.....	189
7.2.1 黑客留下的痕迹.....	174	7.4.2 清除【运行】历史记录.....	190
7.2.2 使用日志分析工具.....	176	7.5 高手解答.....	191
7.3 清除使用痕迹.....	180		

第8章 远程控制技术



8.1 远程协助的使用	194	8.2.4 使用pcAnywhere工具	204
8.1.1 远程协助的应用	194	8.3 正向与反向远程控制	208
8.1.2 连接远程桌面	194	8.3.1 木马的正向连接	208
8.1.3 使用远程关机	197	8.3.2 反向连接远程控制	208
8.2 远程控制工具	198	8.3.3 远程控制的防范	209
8.2.1 使用QQ远程协助	199	8.4 进阶练习	211
8.2.2 使用Radmin工具	199	8.5 高手解答	212
8.2.3 使用【网络人】工具	202		

第9章 脚本攻击技术



9.1 脚本注入技术的分析	214	9.2.5 防范脚本攻击	223
9.1.1 脚本的攻击	214	9.3 Access数据库的注入	225
9.1.2 脚本的编辑语言	214	9.3.1 Access数据库的作用	225
9.1.3 使用脚本注入工具	215	9.3.2 打开Access数据库	225
9.1.4 编辑脚本的规则	216	9.3.3 使用啊D进行SQL注入	226
9.1.5 注入辅助工具IAT	217	9.4 MSSQL数据库	227
9.2 SQL注入攻击	219	9.4.1 安装MSSQL数据库	227
9.2.1 NBSI注入工具	219	9.4.2 创建SQL数据库	228
9.2.2 查找动态URL	220	9.5 进阶练习	231
9.2.3 查找特殊动态URL	221	9.6 高手解答	233
9.2.4 PHP注入工具	222		

第10章 黑客攻防实用技巧



10.1 系统设置技巧	236	10.1.8 设置系统防火墙	244
10.1.1 系统资源监视器	236	10.2 常用黑客工具的使用	248
10.1.2 使用任务查看器工具	237	10.2.1 网络检测工具	248
10.1.3 加快系统启动速度	240	10.2.2 多功能系统工具	251
10.1.4 加快系统关闭速度	241	10.2.3 瑞星杀毒软件	253
10.1.5 设置开机启动项	241	10.3 进阶练习	257
10.1.6 关闭自动更新重启提示	242	10.4 高手解答	259
10.1.7 磁盘配额管理技巧	243		

第1章

黑客的基础知识



说起网络安全，大多数人会自然而然地联想到黑客，并将黑客与窃取资料、破解密码、破坏网络安全等行为联系起来。其实黑客并不完全是网络上的“破坏者”，也有一部分是网络中的“保护者”。



例1-1 查看系统中开放的端口
例1-2 关闭系统中指定的端口
例1-3 限制访问系统中的指定端口
例1-4 使用ping命令查看网络
例1-5 使用netstat命令查看网络
例1-6 启动telnet功能

例1-7 查看IP地址
例1-8 安装虚拟机
例1-9 创建虚拟机
例1-10 在虚拟机中安装系统
例1-11 打开系统防火墙