



黑客攻防实战

从入门到精通

第2版

风云工作室 编著



内容丰富：除讲解有线端的攻防策略外，还融入了无线攻防、移动端攻防、手机钱包等热点。

图文并茂：注重操作、图文并茂，在讲解案例的过程中，每一步操作均有对应的插图。

案例丰富：把知识点融入系统的案例实训当中，并且结合经典案例进行讲解和拓展。

超值赠送：赠送大量实用资源，可以全面掌握黑客攻防的方方面面知识。

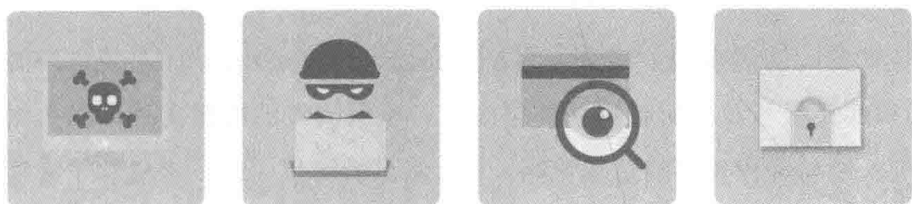


超值赠送：

- ✓ 950分钟实战教学视频
- ✓ 精美教学用的幻灯片
- ✓ 108个黑客工具速查手册
- ✓ 160个常用黑客命令速查手册
- ✓ 180页常见故障维修手册
- ✓ 188页Windows 10系统使用和防护技巧



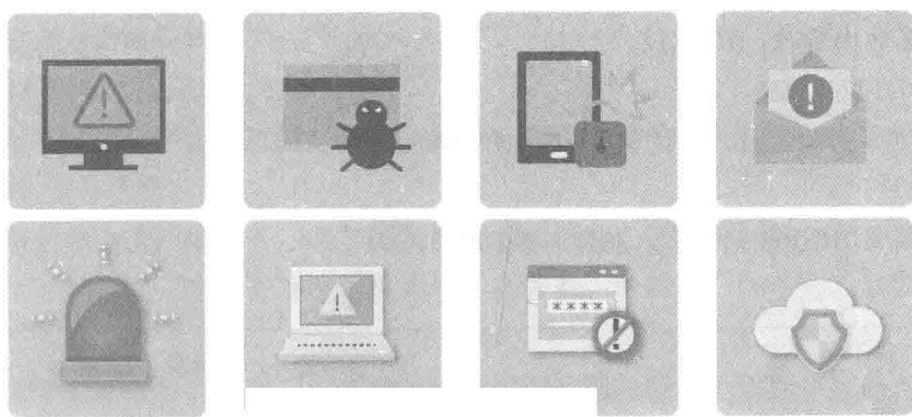
化学工业出版社



黑客攻防实战

从入门到精通 第2版

风云工作室 编著



化学工业出版社

· 北京 ·

本书采用通俗易懂的语言，对读者进行黑客防御时迫切需要和想要用到的技术进行了详细的讲解，使读者对网络防御技术形成系统了解，从而能够更好地防范黑客的攻击。

全书共分为18章，包括熟悉黑客和红客，防黑必备技能大放送，防范黑客入侵的工具，系统漏洞与安全的防黑实战，电脑木马的防黑实战，Windows 10系统账户的防黑实战，网游、QQ和邮箱账号及密码数据的防黑实战，电脑病毒的防黑实战，网页浏览器的防黑实战，系统入侵与远程控制的防黑策略，U盘病毒的防黑实战，手机和平板病毒防范与清除，网站安全的防黑策略，磁盘数据安全的终极防黑实战，虚拟专用网的防黑实战，局域网的防黑实战，无线网络安全的防黑实战，手机钱包的防黑实战等内容。

本书内容丰富、图文并茂、深入浅出，不仅适合广大网络爱好者使用，也同样适合网络安全从业人员及网络管理员阅读。

图书在版编目(CIP)数据

黑客攻防实战从入门到精通/风云工作室编著. —2版.

—北京：化学工业出版社，2018.11

ISBN 978-7-122-32938-7

I. ①黑… II. ①风… III. ①计算机网络-网络安全

IV. ①TP393.08

中国版本图书馆CIP数据核字（2018）第200921号

责任编辑：孙 炜 李 辰

装帧设计：尹琳琳

责任校对：边 涛

出版发行：化学工业出版社（北京市东城区青年湖南街13号 邮政编码100011）

印 刷：三河市航远印刷有限公司

装 订：三河市瞰发装订厂

787mm×1092mm 1/16 印张20 字数500千字 2019年1月北京第2版第1次印刷

购书咨询：010-64518888 售后服务：010-64518899

网 址：<http://www.cip.com.cn>

凡购买本书，如有缺损质量问题，本社销售中心负责调换。

定 价：59.80元

版权所有 违者必究

Preface

前言

随着手机、平板电脑的普及，无线网络的防范就变得尤为重要，为此本书除了讲解有线端的攻防策略外，还把目前流行的无线攻防、移动端攻防、手机钱包防黑等热点融入本书中。

(1) 本书特色

①知识点丰富、全面：本书涵盖了绝大多数黑客攻防知识点，由浅入深地讲解黑客攻防方面的技能。

②图文并茂：注重操作，图文并茂。在介绍案例的过程中，每一步操作都配有对应的插图。这种图文结合的方式使读者能够直观、清晰地看到操作的过程以及最终效果，便于更快地理解和掌握。

③案例丰富：把知识点融入系统的案例实训当中，并且结合经典案例进行讲解和拓展，进而达到“知其然，并知其所以然”的效果。

④提示技巧、贴心周到：本书对读者在学习过程中可能会遇到的疑难问题以“提示”的形式进行了说明，避免读者在学习的过程中走弯路。

⑤超值赠送：本书赠送了大量实用的资源，读者可以通过本书以及赠送的资源，掌握黑客攻防方方面面的知识。

(2) 读者对象

本书不仅适合广大网络爱好者，而且适合网络安全从业人员及网络管理员阅读。

(3) 写作团队

本书主要由王维维编著，参与编著的还包括王猛、王婷婷、张芳、王英英、张桐嘉、肖品、胡同夫、梁云亮、王攀登、包慧利、孙若淞、贺盼盼、郑玉超、唐跃爱、郭红侠、贺金刚、郭红梅、郑思贤、贾福运、贺单单、王二帅、郭红民、邓爱玲、谢德胜、李友洪、贾文学、郭推等。在编写过程中，笔者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，敬请不吝指正。若您在学习中遇到困难或疑问，或有何建议，可加入QQ群389543972，获得作者的在线指导。

编著者
2018.3

Contents

目 录

第1章 熟悉黑客和红客 1	
1.1 黑客的过去、现在和未来..... 1	
1.1.1 黑客的发展历史..... 1	
1.1.2 黑客的现状以及发展..... 1	
1.1.3 哪些是黑客 做下的“事”..... 3	
1.2 黑客与红客的区别..... 3	
1.3 防范黑客需要掌握的资源..... 4	
1.4 防患于未然——黑客是如何 攻击电脑的..... 4	
1.5 步步为营——黑客攻击的流程..... 5	
第2章 防黑必备技能大放送 6	
2.1 黑客攻击的入口——端口..... 6	
2.1.1 查看系统的开放端口..... 6	
2.1.2 关闭不必要的端口..... 6	
2.1.3 启动需要开启的端口..... 7	
2.2 查看IP地址与MAC地址..... 8	
2.2.1 查看IP地址..... 8	
2.2.2 查看MAC地址..... 9	
2.3 熟悉黑客常用的DOS 命令..... 9	
2.3.1 cd命令..... 9	
2.3.2 dir命令..... 10	
2.3.3 ping命令..... 11	
2.3.4 net命令..... 12	
2.3.5 netstat命令..... 12	
2.3.6 tracert命令..... 13	
2.4 新手练兵场——限制访问 指定的端口..... 14	
2.5 高手秘籍..... 17	
2.5.1 秘籍1：使用netstat命令 快速查找对方IP地址..... 17	
2.5.2 秘籍2：使用代码检查 指定端口开放状态..... 18	
第3章 防范黑客入侵的工具 20	
3.1 端口扫描器工具..... 20	
3.1.1 ScanPort..... 20	
3.1.2 极速端口扫描器..... 20	
3.1.3 Nmap扫描器..... 22	
3.2 常见多功能扫描器工具..... 24	
3.2.1 流光扫描器..... 24	
3.2.2 X-Scan扫描器..... 28	
3.2.3 S-GUI Ver扫描器..... 31	
3.3 常用网络嗅探工具..... 32	
3.3.1 嗅探利器SmartSniff..... 33	
3.3.2 网络数据包嗅探 专家..... 34	
3.4 新手练兵场——通过隐藏自己 防范黑客工具..... 34	
3.5 高手秘籍..... 35	
3.5.1 秘籍1：查看系统中的 ARP缓存表..... 35	
3.5.2 秘籍2：网络嗅探器影音 神探..... 36	

第4章 系统漏洞与安全的防黑

实战.....	40
4.1 系统漏洞概述.....	40
4.1.1 什么是系统漏洞.....	40
4.1.2 系统漏洞产生的原因.....	40
4.1.3 常见系统漏洞类型.....	40
4.2 RPC服务远程漏洞的防黑实战.....	42
4.2.1 什么是RPC服务远程漏洞.....	42
4.2.2 RPC服务远程漏洞入侵演示.....	45
4.2.3 RPC服务远程漏洞的防御.....	46
4.3 WebDAV漏洞的防黑实战.....	47
4.3.1 什么是WebDAV缓冲区溢出漏洞.....	47
4.3.2 WebDAV缓冲区溢出漏洞入侵演示.....	48
4.3.3 WebDAV缓冲区溢出漏洞的防御.....	49
4.4 系统漏洞的防黑实战.....	50
4.4.1 使用Windows更新及时更新系统.....	50
4.4.2 使用360安全卫士下载并安装补丁.....	51
4.4.3 使用瑞星安全助手修复系统漏洞.....	52
4.5 系统安全的防黑实战.....	53
4.5.1 使用任务管理器管理进程.....	53
4.5.2 卸载流氓软件.....	55
4.5.3 查杀恶意软件.....	57
4.5.4 删除上网缓存文件.....	57
4.5.5 删除系统临时文件.....	58
4.6 新手练兵场——使用Windows Defender保护系统.....	60
4.7 高手秘籍.....	60
4.7.1 秘籍1：使用系统工具整理碎片.....	60
4.7.2 秘籍2：关闭开机多余启动项目.....	62

第5章 电脑木马的防黑实战..... 64

5.1 什么是电脑木马.....	64
5.1.1 常见的木马类型.....	64
5.1.2 木马常用的入侵方法.....	65
5.2 木马常用的伪装手段.....	65
5.2.1 伪装成可执行文件.....	66
5.2.2 伪装成自解压文件.....	68
5.2.3 将木马伪装成图片.....	69
5.3 木马的自我保护.....	70
5.3.1 给木马加壳.....	70
5.3.2 给木马加花指令.....	72
5.3.3 修改木马的入口点.....	73
5.4 木马常见的启动方式.....	73
5.4.1 利用注册表启动.....	73
5.4.2 利用系统文件启动.....	74
5.4.3 利用系统启动组启动.....	74
5.4.4 利用系统服务启动.....	74
5.5 查询系统中的木马.....	75
5.5.1 通过启动文件检测木马.....	75
5.5.2 通过进程检测木马.....	75
5.5.3 通过网络连接检测木马.....	77

5.6	使用木马清除软件清除 木马.....	78	6.3.5	删除用户账户.....	99
5.6.1	使用木马清除大师清除 木马.....	78	6.3.6	设置屏幕保护密码.....	100
5.6.2	使用木马清除专家清除 木马.....	80	6.3.7	创建密码恢复盘.....	101
5.6.3	使用金山贝壳木马专杀清除 木马.....	83	6.4	Microsoft账户的防黑实战.....	102
5.7	新手练兵场——轻松清除 木马.....	84	6.4.1	注册并登录Microsoft 账户.....	102
5.8	高手秘籍.....	87	6.4.2	设置账户登录密码.....	104
5.8.1	秘籍1：将木马伪装成 网页.....	87	6.4.3	设置PIN密码.....	104
5.8.2	秘籍2：在组策略中启动 木马.....	88	6.4.4	使用图片密码.....	106
第6章	Windows 10系统账户的 防黑实战.....	90	6.5	别样的系统账户数据防黑 实战.....	107
6.1	了解Windows 10的账户类型.....	90	6.5.1	更改系统管理员账户 名称.....	107
6.1.1	认识本地账户.....	90	6.5.2	通过伪造陷阱账户保护 管理员账户.....	108
6.1.2	认识Microsoft账户.....	90	6.5.3	限制Guest账户的操作 权限.....	111
6.1.3	本地账户和Microsoft 账户的切换.....	90	6.6	通过组策略提升系统账户密码的 安全.....	111
6.2	破解管理员账户的方法.....	92	6.6.1	设置账户密码的 复杂性.....	111
6.2.1	强制清除管理员账户 密码.....	92	6.6.2	开启账户锁定功能.....	113
6.2.2	绕过密码自动登录操作 系统.....	93	6.7	新手练兵场——利用组策略 设置用户权限.....	114
6.3	本地系统账户的防黑实战.....	93	6.8	高手秘籍.....	115
6.3.1	启用本地账户.....	94	6.8.1	秘籍1：禁止Guest账户 在本系统登录.....	115
6.3.2	更改账户类型.....	95	6.8.2	秘籍2：找回Microsoft 账户的登录密码.....	116
6.3.3	设置账户密码.....	95	第7章	网游、QQ和邮箱账号及 密码数据的防黑实战.....	118
6.3.4	设置账户名称.....	98	7.1	网游账号及密码的防黑实战.....	118

7.1.1	使用盗号木马盗取账号的防黑	118	8.2	Windows系统病毒.....	130
7.1.2	使用远程控制方式盗取账号的防黑	119	8.2.1	PE文件病毒.....	130
7.1.3	利用系统漏洞盗取账号的防黑	120	8.2.2	VBS脚本病毒.....	131
7.2	QQ账号及密码的防黑实战	121	8.2.3	宏病毒	131
7.2.1	黑客盗取QQ密码的常用方法	121	8.3	电子邮件病毒.....	132
7.2.2	提升QQ安全设置.....	121	8.3.1	邮件病毒的特点	133
7.2.3	使用金山密保来保护QQ号码.....	123	8.3.2	识别“邮件病毒”	133
7.3	邮箱账号及密码的防黑实战.....	123	8.4	查杀电脑病毒.....	133
7.3.1	黑客盗取邮箱密码的常用方法	124	8.4.1	安装杀毒软件	133
7.3.2	重要邮箱的保护措施	124	8.4.2	升级病毒库	134
7.3.3	找回被盗的邮箱密码	125	8.4.3	设置定期杀毒	136
7.4	新手练兵场——防止垃圾邮件.....	125	8.4.4	快速查杀病毒	136
7.5	高手秘籍.....	126	8.4.5	自定义查杀病毒	138
7.5.1	秘籍1：找回被盗的QQ账号密码	126	8.4.6	查杀宏病毒	138
7.5.2	秘籍2：将收到的“邮件炸弹”标记为垃圾邮件	127	8.5	新手练兵场——自定义杀毒模式.....	139
第8章	电脑病毒的防黑实战	129	8.6	高手秘籍.....	140
8.1	认识电脑病毒.....	129	8.6.1	秘籍1：在Word 2016中预防宏病毒	140
8.1.1	电脑病毒的特征和种类	129	8.6.2	秘籍2：在安全模式下查杀病毒	141
8.1.2	电脑病毒的工作流程	129	第9章	网页浏览器的防黑实战.....	143
8.1.3	电脑中毒的途径	130	9.1	认识网页恶意代码.....	143
8.1.4	电脑中病毒后的表现	130	9.1.1	恶意代码概述	143
			9.1.2	恶意代码的特征	143
			9.1.3	恶意代码的传播方式	143
			9.2	常见恶意网页代码及攻击方法.....	143
			9.2.1	启动时自动弹出对话框和网页	144

9.2.2	利用恶意代码禁用注册表	144
9.3	恶意网页代码的预防和清除	145
9.3.1	恶意网页代码的预防	145
9.3.2	恶意网页代码的清除	145
9.4	常见网页浏览器的攻击方式	147
9.4.1	修改默认主页	147
9.4.2	恶意更改浏览器标题栏	147
9.4.3	强行修改网页浏览器的右键菜单	148
9.4.4	禁用网页浏览器的【源】菜单命令	149
9.4.5	强行修改浏览器的首页按钮	151
9.4.6	删除桌面上的浏览器图标	152
9.5	网页浏览器的自我防护技巧	153
9.5.1	提高IE的安全防护等级	153
9.5.2	清除浏览器中的表单	154
9.5.3	清除浏览器的上网历史记录	154
9.5.4	删除Cookie信息	155
9.6	新手练兵场——保护网页浏览器的安全	156
9.6.1	使用IE修复专家	156
9.6.2	IE修复免疫专家	157
9.6.3	IE伴侣 (IEMate)	161
9.7	高手秘籍	165

9.7.1	秘籍1：查看加密网页的源码	165
9.7.2	秘籍2：屏蔽浏览器窗口中的广告	166

第10章 系统入侵与远程控制的防黑实战

167

10.1	通过账号入侵系统的常用手段	167
10.1.1	使用DOS命令创建隐藏账号入侵系统	167
10.1.2	在注册表中创建隐藏账号入侵系统	168
10.1.3	使用MT工具创建复制账号入侵系统	170
10.2	抢救账号被入侵的系统	172
10.2.1	揪出黑客创建的隐藏账号	172
10.2.2	批量关闭危险端口	173
10.3	通过远程控制工具入侵系统	174
10.3.1	什么是远程控制	174
10.3.2	通过Windows远程桌面实现远程控制	174
10.4	远程控制的防黑实战	176
10.4.1	关闭Windows远程桌面功能	177
10.4.2	开启系统的防火墙	177
10.4.3	关闭远程注册表管理服务	178
10.5	新手练兵场——使用天网防火墙防护系统安全	179
10.6	高手秘籍	181

10.6.1	秘籍1: 禁止访问控制 面板	181
10.6.2	秘籍2: 启用和关闭 快速启动功能	182
第11章 U盘病毒的防黑实战.....		183
11.1	U盘病毒概述	183
11.1.1	U盘病毒的原理和 特点.....	183
11.1.2	常见U盘病毒.....	183
11.1.3	窃取U盘上的资料.....	184
11.2	关闭“自动播放”功能防御 U盘病毒.....	184
11.2.1	使用组策略关闭“自动 播放”功能.....	184
11.2.2	修改注册表关闭“自动 播放”功能.....	185
11.2.3	设置服务关闭“自动 播放”功能.....	185
11.3	查杀U盘病毒.....	186
11.3.1	用WinRAR查杀U盘 病毒.....	186
11.3.2	使用USBKiller查杀 U盘病毒.....	187
11.3.3	使用USBCleaner查杀 U盘病毒.....	190
11.4	新手练兵场——快速查杀 U盘病毒.....	192
11.5	高手秘籍.....	194
11.5.1	秘籍1: U盘病毒的 手动删除.....	194
11.5.2	秘籍2: 通过禁用硬件检测 服务让U盘丧失智能.....	195

第12章 手机和平板病毒防范与 清除.....		197
12.1	手机病毒的来源.....	197
12.1.1	硬件环境	197
12.1.2	软件环境	197
12.1.3	通信环境	197
12.1.4	人为环境	198
12.2	手机病毒的传染途径.....	198
12.2.1	通过网络下载	198
12.2.2	利用红外或蓝牙 传输	198
12.2.3	短信与乱码传播	199
12.2.4	利用手机BUG传播	199
12.2.5	手机炸弹攻击	199
12.3	手机病毒的特点.....	200
12.4	平板电脑的攻击手法.....	201
12.5	平板电脑的防黑实战.....	201
12.5.1	自动升级固件	201
12.5.2	重装系统	203
12.5.3	为视频加锁	203
12.5.4	开启“查找我的iPad” 功能	205
12.5.5	远程锁定iPad	206
12.5.6	远程清除iPad中的 信息	207
12.6	新手练兵场——手机的防黑 实战.....	207
12.6.1	关闭手机蓝牙功能	207
12.6.2	保证手机下载的应用 程序的安全性	208
12.6.3	关闭乱码电话, 删除 怪异短信	208

12.6.4	安装手机卫士 软件	209	13.5.2	秘籍2: 保护网站安全 技巧	230	
12.6.5	经常备份手机中的个人 资料	209	第14章 磁盘数据安全的终极 防黑实战		231	
12.7	高手秘籍	209	14.1	数据丢失的原因	231	
12.7.1	秘籍1: 使用手机交流 工作问题	209	14.1.1	数据丢失的原因	231	
12.7.2	秘籍2: 苹果手机的 “白苹果”现象	210	14.1.2	发现数据丢失后的 操作	231	
第13章 网站安全的防黑策略			211	14.2	备份磁盘各类数据	231
13.1	网站维护基础知识	211	14.2.1	分区表数据的防黑 实战	232	
13.1.1	网站的种类和特点	211	14.2.2	引导区数据的防黑 实战	232	
13.1.2	网站的维护与安全	211	14.2.3	驱动程序的防黑 实战	233	
13.2	网站的常见攻击方式	212	14.2.4	电子邮件的防黑 实战	235	
13.2.1	DOS攻击	212	14.2.5	磁盘文件数据的防黑 实战	237	
13.2.2	DDOS攻击	213	14.3	各类数据丢失后的补救 策略	239	
13.3	网站安全的防黑	220	14.3.1	分区表数据丢失后的 补救	239	
13.3.1	检测上传文件的 安全性	220	14.3.2	引导区数据丢失后的 补救	239	
13.3.2	设置网站访问权限	222	14.3.3	驱动程序数据丢失后的 补救	240	
13.3.3	在注册表中预防SYN 系统攻击	223	14.3.4	电子邮件丢失后的 补救	242	
13.3.4	DDOS攻击的防御 措施	224	14.3.5	磁盘文件数据丢失后的 补救	243	
13.3.5	全面防御SQL注入 攻击	225	14.4	恢复丢失的数据	245	
13.3.6	备份网站数据	226				
13.4	新手练兵场——恢复被黑客 攻击的网站	228				
13.5	高手秘籍	229				
13.5.1	秘籍1: 保护本机中的 数据库	229				

14.4.1	从回收站中还原	245	15.4	高手秘籍	268
14.4.2	清空回收站后的 恢复	246	15.4.1	秘籍1: 无线网络的 优化	268
14.4.3	使用EasyRecovery恢复 数据	247	15.4.2	秘籍2: 网络安全性的 解决方法	268
14.4.4	使用FinalRecovery恢复 数据	250	第16章 局域网的防黑实战		270
14.4.5	使用FinalData恢复 数据	251	16.1	局域网安全介绍	270
14.4.6	使用“数据恢复大师” 恢复数据	253	16.1.1	局域网基础知识	270
14.5	新手练兵场——找回格式化 硬盘后的数据	256	16.1.2	局域网安全隐患	270
14.6	高手秘籍	258	16.2	查看局域网中的信息	271
14.6.1	秘籍1: 恢复丢失的 磁盘簇	258	16.2.1	使用LanSee工具	271
14.6.2	秘籍2: 还原已删除或 重命名的文件	259	16.2.2	使用IPBook工具	275
第15章 虚拟专用网的防黑 实战		261	16.3	攻击局域网的方式	278
15.1	虚拟专用网的原理	261	16.4	熟悉局域网安全的辅助 软件	278
15.1.1	虚拟专用网的组件	261	16.4.1	聚生网管	278
15.1.2	隧道协议	261	16.4.2	长角牛网络监控机	284
15.1.3	无线VPN	262	16.5	新手练兵场——有效保护 局域网安全	288
15.2	虚拟专用网的攻防实战	263	16.6	高手秘籍	290
15.2.1	攻击PPTP VPN	263	16.6.1	秘籍1: 诊断和修复网络 不通的问题	290
15.2.2	攻击启用IPSec加密的 VPN	265	16.6.2	秘籍2: 屏蔽网页广告 弹窗	291
15.2.3	本地破解VPN登录 账户名及密码	267	第17章 无线网络安全的防黑 实战		292
15.3	虚拟专用网的防护及 改进	267	17.1	组建无线网络	292
			17.1.1	搭建无线网环境	292
			17.1.2	配置无线局域网	292
			17.1.3	将电脑接入无线网	293
			17.1.4	将手机接入Wi-Fi	294
			17.2	电脑和手机共享无线上网	295

17.2.1	手机共享电脑的 网络	295
17.2.2	电脑共享手机的 网络	297
17.2.3	加密手机的WLAN 热点功能	298
17.3	无线网络的安全策略	298
17.3.1	设置管理员密码	298
17.3.2	修改Wi-Fi名称	299
17.3.3	无线网络WEP加密	299
17.3.4	WPA-PSK安全加密 算法	300
17.3.5	禁用SSID广播	302
17.3.6	媒体访问控制 (MAC) 地址过滤	303
17.4	高手秘籍	304
17.4.1	秘籍1——控制无线网中 设备的上网速度	304

17.4.2	秘籍2: 诊断和修复网络 不通的问题	304
--------	-----------------------------	-----

第18章 手机钱包的防黑实战 305

18.1	手机钱包的攻击手法	305
18.1.1	手机病毒	305
18.1.2	盗取手机	305
18.2	手机钱包的防黑策略	306
18.2.1	手机盗号病毒的 防范	306
18.2.2	手机丢失后的手机 钱包的防范	306
18.3	新手练兵场——加强手机 钱包的支付密码	306
18.4	高手秘籍	307
18.4.1	秘籍1: 手机钱包如何 开通	307
18.4.2	秘籍2: 手机钱包如何 充值	307

第1章 熟悉黑客和红客

黑客 (hacker) 最初是指那些热衷于电脑, 并能够把一些应用程序组合起来或拆开来解决问题的人; 但如今, 黑客被定义为非法搜索和渗透计算机网络访问和使用数据的人。黑客之所以存在的原因主要是由于系统、网络和软件在一定程度上都存在有安全漏洞, 黑客就是利用这些漏洞来攻击目标主机的。

1.1 黑客的过去、现在和未来

随着Internet的迅速发展、网络带宽的快速提升、网络用户群体的增加, 网络的安全问题也变得越来越突出。网络攻击的便利性和简易性以及我国网络信息系统的安全脆弱性, 进而导致了黑客攻击的多发性。

1.1.1 黑客的发展历史

随着Internet在中国迅速发展、国内上网的人数的持续翻番以及网民的日益活跃, “黑客”事件也时有发生。国内黑客发展主要经历如下3个阶段:

①第1代 (1996~1998年)。1996年因特网在中国兴起, 但是由于受到各种条件的制约, 很多人根本没有机会接触网络。当时计算机也没有达到普及的程度, 大部分地区还没有开通因特网的接入服务, 所以中国第1代黑客大都是从事科研、机械等方面工作的人, 只有他们才有机会频繁地接触计算机和网络。他们有着较高的文化素质和计算机技术水平, 凭着扎实的技术和对网络的热爱迅速发展成为黑客。有的专门从事网络安全技术研究或成为网络安全管理员, 有的则开了网络安全公司, 演变为派客 (由黑客转变为网络安全者)。

1998年8月爆发了东南亚金融危机, 并且在一些地区发生了严重的针对华人的暴

乱, 当时残害华人的消息在新闻媒体上报道后, 国内计算机爱好者怀着一片爱国之心和对同胞惨遭杀害的悲痛之心, 纷纷对这些行为进行抗议。中国黑客对这些地区的网站发动了攻击, 众多网站上悬挂起中华人民共和国的五星红旗。当时黑客代表组织为“绿色兵团”。

②第2代 (1998~2000年)。随着计算机的普及和因特网的发展, 有越来越多的人有机会接触计算机和网络, 在第1代黑客的影响和指点下, 中国出现了第2代黑客。他们一部分是从事计算机的工作者和网络爱好者, 另一部分是在校学生。这一代的兴起是由1999年5月8日某国轰炸驻中国南斯拉夫大使馆事件引发, 黑客代表组织为原“中国黑客联盟”。

③第3代 (2000年~)。这一代黑客主要由在校学生组成, 其技术水平和文化素质与第1代、第2代相差甚远, 大都只是照搬网上一些由前人总结出来的经验和攻击手法。现在网络上所谓的入侵者也是由这一代组成。但领导这一代的核心黑客还是那些第1代、第2代的前辈们。这一代兴起是由2001年4月的一起撞机事件引发, 黑客代表组织为“红客联盟”“中国鹰派”。

1.1.2 黑客的现状以及发展

国内黑客站点门派繁多, 但整体素质

不尽如人意，有的甚至低劣。主要表现在如下6方面：

（1）叫法不一，很不正规

黑客，甚至包括骇客，这两个单词都是可以在相关资料如词典、黑客界等领域有章可循的。目前的对“黑客”一词的各种叫法极不规范。

（2）技术功底薄弱，夸大作风

比如国内几大黑客组织的站点，此类站点只顾如何叫他人攻击别人的电脑，刷Q币，盗密码等，以适应初学者的口味。站点用色彩绚丽的界面和震撼的音乐等手段，来吸引众人尤其是青少年的眼球。青少年不成熟，崇尚自由冒险刺激，有强烈的表现欲，黑客行业正符合这一特点，所以众多黑客站点正投其所好，使之趋之若鹜，来提高自己的站点访问量，而不用靠实力提高站点的质量和知名度。

（3）内容粗制滥造

内容粗制滥造，应付了事，原创作品少，且相互抄袭。曾有某篇文章说，中国的黑客一代不如一代。

（4）效率低，更新少，可读性差，界面杂乱

有些站点很少更新，打不开，站点杂乱，经常有死链接，作品抄袭。

（5）整体技术水平不高，研究层次级别低

目前国内几大黑客站点大都进行商业化运作，安全培训。以追求最大经济效益为目的，只要能赚到钱就够了，至于深层次的研究，是没有的。只是每天更新一些新闻、黑客教程、软件等，用户只能学到一些编程知识、数据库知识，再看看一些教程，借用一些黑客工具，就去黑别人的站点，盗号等。与国外相比，国外的黑客

研究的则是系统级别的漏洞，制造的也是世界级别的系统病毒，扰乱全球网络。

（6）缺少一个统一协调中国黑客界行动发展的组织

虽然目前好多站点都包含有“联盟”字样，但其实是一家，各自为政，这就使得在抗击外来网络入侵时缺少统一指挥，手忙脚乱，大大降低中国黑客界整体的力量。

目前中国黑客的发展总体可以归为5大趋势：

①黑客年轻化。由于中国互联网的普及，形成全球一体化，甚至连很多偏远的地方也可以从网络上接触到世界各地的信息资源，所以越来越多对这方面感兴趣的中学生，也已经踏足到这个领域。

②黑客的破坏力扩大化。由于互联网的普及，电子商务也在蓬勃发展，全社会对互联网的依赖性日益增加，黑客的破坏力也日益扩大化。仅在美国，黑客每年造成的经济损失就超过100亿美元，可想而知，对于安全刚起步的中国，破坏的影响程度就更大了。

③黑客技术的迅速普及。黑客组织的形成和黑客傻瓜式工具的大量出现导致的一个直接后果就是黑客技术的普及，虽然在市面可能看不到一本介绍如何做黑客、传授黑客技术的书，但是在Internet上，黑客与黑客组织办的传授黑客技术的站点却比比皆是。

④黑客技术的工具化。黑客事件越来越多的一个重要原因，是黑客工具越来越多，越来越容易获得，也越来越傻瓜化和自动化，目前黑客运用的软件工具已超过1000种。

⑤黑客组织化。对于黑客的破坏，人们的网络安全意识开始增强，计算机产品的安全性被放在很重要的位置，漏洞和缺陷也越来越难发现；而且因为利益的驱

使，黑客开始由原来的单兵作战变成了有组织的黑客群体。在黑客组织内部，成员之间相互交流技术经验，共同采取黑客行动，成功率增高，影响力也更大，正所谓“道高一尺，魔高一丈”。

1.1.3 哪些是黑客做下的“事”

黑客利用扫描出来的目标主机漏洞主要做如下事情：首先是获得系统信息，有些系统漏洞可以泄漏系统信息，暴露敏感资料，为进一步入侵系统做好准备；其次是入侵系统，通过漏洞进入系统内部，从而取得服务器上的内部资料。

下面介绍一些历史上比较著名的黑客事件，从而进一步帮助读者了解黑客。

1983年，凯文·米特尼克因被发现使用一台大学里的电脑擅自进入今日互联网的前身ARPA网，并通过该网进入了美国五角大楼的电脑。

1999年，梅利莎病毒使世界上300多家公司的电脑系统崩溃，该病毒造成的损失接近4亿美元，它是首个具有全球破坏力的病毒。

2000年，绰号“黑手党男孩”的黑客在2000年2月6日到2月14日情人节期间成功侵入包括雅虎、eBay和Amazon在内的大型网站服务器，他成功阻止服务器向用户提供服务。

2008年，一个全球性的黑客组织，利用ATM欺诈程序在一夜之间从世界49个城市的银行中盗走了900万美元。黑客们攻破的是一种名为RBS WorldPay的银行系统，并在11月8日午夜，利用团伙作案从世界49个城市总计超过130台ATM机上提取了900万美元。

2009年7月7日，黑客对韩国总统府、国会和国防部等国家机关，以及金融界、

媒体和防火墙企业网站进行了攻击。9日韩国国家情报院和国民银行网站无法被访问，韩国国会、国防部等机构的网站一度无法打开，这是韩国遭遇的有史以来最强的一次黑客攻击。

2010年1月12日上午7点钟开始，全球最大中文搜索引擎“百度”遭到黑客攻击，长时间无法正常访问，主要表现为跳转到雅虎出错页面、出现“天外符号”等，范围涉及四川、福建、江苏、吉林、浙江、北京、广东等国内绝大部分省市，这是自百度建立以来，所遭遇的持续时间最长、影响最严重的黑客攻击。

这些事件的发生，表明黑客渐趋于普遍化。计算机网络安全问题关系到国家的安全，关系到国家经济秩序的稳定，也关系到自由通信会不会受到来路不明的黑客袭击或干扰。

1.2 黑客与红客的区别

“黑客”大体上可以分为“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、入侵或做其他一些有害于网络的事情，正是因为邪派黑客所从事的事情违背了《黑客守则》，所以他们真正的名字应该叫“骇客”（Cracker）而非“黑客”（Hacker），这也就是平时经常听说的“黑客”（Cacker）和“红客”（Hacker）。

不管是“黑客”或者是“红客”，他们最初的学习内容和掌握的基本技能都是一样的，即便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。

知识链接

什么是黑客守则

目前，网络上总结出来的黑客守则有很多，主要包括以下几个方面。

- ①不得恶意破坏任何的系统。
- ②不得恶意修改任何系统文件。
- ③不要轻易将要攻击的网站告诉不信任的朋友。
- ④不要在论坛上谈论关于攻击的任何事情。
- ⑤正在入侵的时候，不要随意离开电脑。
- ⑥不要侵入或破坏政府机关的主机。
- ⑦将黑客笔记放在安全的地方。
- ⑧已侵入电脑中的账号不得清除或涂改。
- ⑨不得恶意修改系统档案。
- ⑩不将已破解的账号与朋友分享。

1.3 防范黑客需要掌握的资源

一般来讲，做什么事情都是入门难。要想防范黑客的进攻，就需要了解黑客都需要掌握哪些知识，其实也是一个不断学习的过程，那么比较简便的方法就是借助网络和书籍。比较常见的书籍有以下几种类型

①基础知识类。一般来说新手朋友的基础是比较差的，甚至一些基本常识都不知道，所以有几本基础知识的书作为参考是必不可少的，比如关于TCP/IP、网络、操作系统以及局域网等，甚至是关于DOS、Windows基础的书都是很有必要的。此类书籍关键在于它的通俗易懂性，不要追求多么深入，对新手来说，急于求成是最要不得的。

②大众杂志类。此类书籍的精华在于其合订本，比如电脑报合订本、电脑应用合订本等，就相当于一个大百科，具有分类详细、内容丰富的特点。此类书籍的优势在于内容全面，各个方面都能涉及，查找方便，但因其定位在大众杂志，内容相对比较基础，适合新手做全方位了解。

③hack杂志类。比如《黑客防线》

《黑客X档案》《黑客手册》等，此类杂志专业性较强，内容由浅入深，讨论详细，并附送光盘，对比较富裕的朋友来说是个不错的选择。这是一种比较好的入门方法。

④查看电子教程。在网络中搜索查看电子教程是能让自己快速进步的方法之一，如到各大安全站点的文章系统中去找，或者去相关论坛或Google中去搜索。

1.4 防患于未然——黑客是如何攻击电脑的

黑客攻击电脑的方式是多种多样的，绝大多数攻击是利用系统配置的缺陷、操作系统的安全漏洞以及通信协议的安全漏洞等进行攻击的。目前，黑客攻击的主要方式有以下几种：

(1) 拒绝服务攻击

在一般情况下，拒绝服务攻击是通过使被攻击对象（工作站或重要服务器）的系统关键资源过载，从而使被攻击对象停止部分或全部服务。目前拒绝服务攻击是最基本的入侵攻击手段，也是最难对付的黑客攻击之一，SYN Flood攻击、Ping