超值赠送1：950分钟实战教学视频

超值赠送2：188页Windows 8系统使用和防护技巧

超值赠送3：180页常见故障维修手册

超值赠送4：160个常用黑客命令速查手册

超值赠送5：107个黑客工具速查手册

超值赠送6：教学用PPT课件

网络安全必备手册

黑客攻防实战从入门到精通

风云工作室　编著

知识丰富：涵盖了所有黑客攻防知识点，除了讲解有线端的攻防策略外，还融入了时下流行的无线攻防、移动端攻防、手机钱包等热点。

图文并茂：注重操作，图文并茂，在介绍案例的过程中，每一个操作均有对应的插图。

案例丰富：把知识点融于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：赠送封面所述的大量资源，读者可以全面掌握黑客攻防的方方面面的知识。

化学工业出版社
全国百佳出版单位

黑客攻防实战从入门到精通

风云工作室　编著

化学工业出版社
·北　京·

本书在剖析用户进行黑客防御中迫切需要用到或迫切想要用到的技术时力求对其进行傻瓜式的讲解，使读者对网络防御技术形成系统的了解，从而能够更好地防范黑客的攻击。全书共分为21章，包括黑客文化漫谈、防黑必备技能、黑客常用入侵工具、系统漏洞与安全的防黑实战、系统入侵与远程控制的防黑实战、文件密码数据的防黑实战、系统账户数据的防黑实战、网络账号及密码的防黑实战、电脑木马的防黑实战、U盘病毒的防黑实战、网页浏览器的防黑实战、无线蓝牙设备的防黑实战、无线网络安全的防黑实战、虚拟专用网的防黑实战、移动手机的防黑实战、手机钱包的防黑实战、平板电脑的防黑实战等内容。

本书内容丰富、图文并茂、深入浅出，不仅适用于广大网络爱好者，而且适用于网络安全从业人员及网络管理员。

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.
北京 : 化学工业出版社，2015.10
ISBN 978-7-122-25050-9

Ⅰ. ①黑… Ⅱ. ①风… Ⅲ. ①计算机网络-安全技术 Ⅳ. ①TS393.08

中国版本图书馆 CIP 数据核字(2015)第 207228 号

责任编辑：张 敏　　装帧设计：尹琳琳
责任校对：程晓彤

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　　装：北京盛通印刷股份有限公司
787mm×1092mm　1/16　印张 23　字数 575 千字　2015 年 11 月北京第 1 版第 1 次印刷

购书咨询：010-64518888（传真：010-64519686）　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

Preface 前言

目前市场上的有关黑客的图书知识相对比较旧，一般讲解PC端的黑客攻防知识。随着手机、平板电脑的普及，无线网络的防范变得尤为重要，为此本书除了讲解有线端的攻防策略外，还把目前市场上流行的无线攻防、移动端攻防、手机钱包等热点融入本书中。

本书特色

- 知识丰富全面：知识点由浅入深，涵盖了所有黑客攻防知识点，能够使读者由浅入深地掌握黑客攻防方面的技能。
- 图文并茂：注重操作，图文并茂，在介绍案例的过程中，每一个操作均有对应的插图。这种图文结合的方式使读者在学习过程中能够直观、清晰地看到操作的过程以及效果，便于更快地理解和掌握。
- 易学易用：颠覆传统“看”书的观念，变成一本能“操作”的图书。
- 案例丰富：把知识点融于系统的案例实训当中，并且结合经典案例进行讲解和拓展，从而使读者达到“知其然，并知其所以然”的效果。
- 提示技巧、贴心周到：本书对读者在学习过程中可能遇到的疑难问题以“提示”和“知识链接”的形式进行了说明，以免读者在学习的过程中走弯路。
- 超值赠送：950分钟实战教学视频、教学用PPT、188页Windows 8系统使用和防护技巧、180页常见故障维修手册、160个常用黑客命令速查手册、107个黑客工具速查手册，读者可加入QQ群221376441获得相关资源。

读者对象

本书不仅适用于广大网络爱好者，而且适用于网络安全从业人员及网络管理员。

写作团队

本书由孙若淞主编，本书主编长期研究网络安全知识，另外胡同夫、梁云亮、王攀登、王婷婷、陈伟光、包慧利、孙若淞、肖品、王维维和刘海松等人参与了本书的编写工作。

在编写过程中，本书编者尽己所能将最好的讲解呈现给读者，但难免有疏漏和不妥之处，敬请广大读者不吝指正。若读者在学习中遇到困难或疑问，或有建议，可联系QQ群221376441获得编者的在线指导。

最后，需要提醒大家：根据国家有关法律规定，任何利用黑客技术攻击他人的行为都属于违法行为，希望读者在阅读本书后不要使用本书介绍的黑客技术对他人进行攻击，否则后果自负，切记!

编者

2015.8

Contents

目 录

第1章 黑客文化漫谈 …… 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 黑客需要掌握的资源 …… 4

第2章 防黑必备技能 …… 5

2.1 IP地址与MAC地址 …… 5

2.1.1 查看IP地址 …… 5

2.1.2 查看MAC地址 …… 5

2.2 端口 …… 6

2.2.1 查看系统的开放端口 …… 6

2.2.2 关闭不必要的端口 …… 6

2.2.3 开启端口 …… 7

2.3 黑客常用的DOS命令 …… 7

2.3.1 cd命令 …… 7

2.3.2 dir命令 …… 8

2.3.3 ping命令 …… 9

2.3.4 net命令 …… 10

2.3.5 netstat命令 …… 10

2.3.6 tracert命令 …… 11

2.4 上机练一练 …… 12

2.4.1 上机目标 …… 12

2.4.2 上机练习 …… 12

2.5 高手秘籍 …… 12

2.5.1 秘籍1：使用netstat命令快速查找对方IP地址 … 12

2.5.2 秘籍2：使用代码检查指定端口开放状态 …… 13

第3章 黑客常用入侵工具 …… 15

3.1 目标扫描工具 …… 15

3.1.1 X-Scan端口扫描器 …… 15

3.1.2 SSS漏洞扫描器 …… 18

3.2 目标入侵工具 …… 21

3.2.1 NetCut局域网攻击工具 …… 21

3.2.2 WinArpAttacker攻击工具 …… 22

3.3 嗅探工具 …… 24

3.3.1 影音神探嗅探器 …… 24

3.3.2 SpyNet Sniffer嗅探器 … 26

3.4 加壳工具 …… 28

3.4.1 UPX加壳工具 …… 28

3.4.2 ASPack加壳工具 …… 29

3.5 脱壳工具 …… 30

3.5.1 UnPECompact脱壳工具 …… 30

3.5.2 ProcDump脱壳工具 …… 31

3.5.3 UN-PACK脱壳工具 …… 31

3.6 上机练一练 …… 32

3.6.1 上机目标 …… 32

3.6.2 上机练习 …… 32

3.7 高手秘籍 …… 32

3.7.1 秘籍1：网络路由追踪工具（NeroTrace Pro） …… 32

3.7.2 秘籍2：缓冲区溢出攻击工具（Metasploit Framework） …… 35

第4章 系统漏洞与安全的防黑实战 …… 41

4.1 系统漏洞概述 …… 41

4.1.1 什么是系统漏洞 …… 41

4.1.2 系统漏洞产生的原因 … 41
4.1.3 常见的系统漏洞类型 … 41
4.2 RPC服务远程漏洞的防黑实战 …… 43
4.2.1 什么是RPC服务远程漏洞 …… 43
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 IDQ漏洞的防黑实战 …… 47
4.3.1 什么是IDQ漏洞 …… 48
4.3.2 IDQ漏洞入侵演示 …… 48
4.3.3 IDQ漏洞的防御 …… 49
4.4 WebDAV漏洞的防黑实战 …… 50
4.4.1 什么是WebDAV缓冲区溢出漏洞 …… 50
4.4.2 WebDAV缓冲区溢出漏洞入侵演示 …… 50
4.4.3 WebDAV缓冲区溢出漏洞的防御 …… 51
4.5 系统漏洞的防黑实战 …… 52
4.5.1 使用Windows Update及时为系统打补丁 …… 52
4.5.2 使用360安全卫士下载并安装补丁 …… 54
4.5.3 使用瑞星安全助手修复系统漏洞 …… 55
4.6 系统安全的防黑实战 …… 55
4.6.1 使用任务管理器管理进程 …… 56
4.6.2 卸载流氓软件 …… 58
4.6.3 查杀恶意软件 …… 59
4.7 上机练一练 …… 60
4.7.1 上机目标 …… 60
4.7.2 上机练习 …… 60
4.8 高手秘籍 …… 60
4.8.1 秘籍1：使用系统自动工具整理碎片 …… 60
4.8.2 秘籍2：关闭开机启动项目 …… 61

第5章 系统入侵与远程控制的防黑实战 …… 63

5.1 通过账号入侵系统的常用手段 …… 63
5.1.1 使用DOS命令创建隐藏账号入侵系统 …… 63
5.1.2 在注册表中创建隐藏账号入侵系统 …… 64
5.1.3 使用MT工具创建复制账号入侵系统 …… 66
5.2 抢救被账号入侵的系统 …… 67
5.2.1 揪出黑客创建的隐藏账号 …… 67
5.2.2 批量关闭危险端口 …… 68
5.3 通过远程控制工具入侵系统 … 69
5.3.1 什么是远程控制 …… 70
5.3.2 Telnet技术 …… 70
5.3.3 通过Windows远程桌面实现远程控制 …… 71
5.4 远程控制的防黑实战 …… 73
5.4.1 关闭Windows远程桌面功能 …… 73
5.4.2 开启系统的防火墙 …… 73
5.4.3 使用天网防火墙防护系统安全 …… 74
5.4.4 关闭远程注册表管理服务 …… 77
5.5 上机练一练 …… 78
5.5.1 上机目标 …… 78
5.5.2 上机练习 …… 78
5.6 高手秘籍 …… 78
5.6.1 秘籍1：禁止访问控制面板 …… 78
5.6.2 秘籍2：通过注册表在【计算机】右键菜单中添加或删除命令 …… 79

第6章 系统安全的终极防黑策略 …… 81
6.1 为什么进行系统重装 …… 81
6.1.1 在什么情况下重装系统 …… 81
6.1.2 重装前应注意的事项 … 81
6.2 常见系统的重装 …… 82
6.2.1 重装Windows XP …… 82
6.2.2 重装Windows 7 …… 83
6.3 系统安全提前准备之备份 …… 85
6.3.1 使用Windows系统工具备份系统 …… 85
6.3.2 使用Ghost工具备份系统 …… 87
6.4 系统崩溃后的修复之还原 …… 92
6.5 使用工具一键备份和还原系统 …… 92
6.5.1 安装一键还原精灵 …… 92
6.5.2 使用一键还原精灵备份系统 …… 94
6.5.3 使用一键还原精灵还原系统 …… 95
6.5.4 使用Ghost工具一键备份系统 …… 96
6.5.5 使用Ghost工具一键还原系统 …… 97
6.6 上机练一练 …… 98
6.6.1 上机目标 …… 98
6.6.2 上机练习 …… 98
6.7 高手秘籍 …… 98
6.7.1 秘籍1：创建系统映像 … 98
6.7.2 秘籍2：使用系统映像还原系统 …… 99
第7章 文件密码数据的防黑实战 …… 103
7.1 黑客常用破解文件密码的方式 …… 103
7.1.1 利用Word Password Recovery破解Word文档密码 …… 103
7.1.2 利用AOXPPR破解Word文件密码 …… 104
7.1.3 利用Excel Key破解Excel文件密码 …… 105
7.1.4 利用APDFPR密码破解工具破解PDF文件密码 …… 106
7.2 各类文件密码的防黑 …… 107
7.2.1 利用Word自身功能给Word文件加密 …… 107
7.2.2 利用Excel自身功能给Excel文件加密 …… 108
7.2.3 利用Adobe Acrobat Professional创建并加密PDF文件 …… 111
7.2.4 利用PDF文件加密器给PDF文件加密 …… 112
7.2.5 利用tElock给EXE文件加密 …… 114
7.2.6 利用WinZip的自加密功能加密ZIP文件 …… 116
7.2.7 利用WinRAR的自加密功能加密RAR文件 …… 117
7.2.8 对文件或文件夹进行加密 …… 118
7.3 上机练一练 …… 119
7.3.1 上机目标 …… 119
7.3.2 上机练习 …… 119
7.4 高手秘籍 …… 119
7.4.1 秘籍1：利用加密文件系统进行加密 …… 119
7.4.2 秘籍2：为WPS Office文档加密 …… 120
第8章 系统账户数据的防黑实战 …… 121
8.1 强制清除管理员账户密码 …… 121
8.2 系统账户数据的防黑实战 …… 121

8.2.1 设置BIOS开机密码 …… 122
8.2.2 设置系统管理员启动密码 …… 123
8.2.3 设置来宾账户密码 …… 125
8.2.4 设置屏幕保护密码 …… 126
8.2.5 创建密码恢复盘 …… 127
8.3 别样的系统账户数据防黑实战 …… 128
8.3.1 更改系统管理员账户名称 …… 128
8.3.2 通过伪造陷阱账户保护管理员账户 …… 129
8.3.3 限制Guest账户的操作权限 …… 131
8.4 通过组策略提升系统账户密码的安全 …… 132
8.4.1 设置账户密码的复杂性 …… 132
8.4.2 开启账户锁定功能 …… 133
8.4.3 利用组策略设置用户权限 …… 134
8.5 上机练一练 …… 135
8.5.1 上机目标 …… 135
8.5.2 上机练习 …… 135
8.6 高手秘籍 …… 135
8.6.1 秘籍1：破解屏幕保护密码 …… 135
8.6.2 秘籍2：禁止Guest账户在本系统登录 …… 136

第9章 网络账号及密码的防黑实战 …… 137

9.1 QQ账号及密码的防黑实战 …… 137
9.1.1 盗取QQ密码的方法 …… 137
9.1.2 使用“QQ简单盗”来盗取QQ账号与密码 …… 137
9.1.3 提升QQ安全设置 …… 139
9.1.4 使用金山密保来保护QQ号码 …… 140
9.2 MSN账号及密码的防黑实战 … 141
9.2.1 使用MSN Messenger Hack获取MSN账号密码 …… 141
9.2.2 使用Messen Pass查看本地密码 …… 142
9.2.3 使用MSN Messenger Keylogger查看密码 …… 142
9.2.4 设置复杂的MSN密码 … 143
9.2.5 找回被盗的MSN密码 … 144
9.3 邮箱账号及密码的防黑实战 … 145
9.3.1 盗取邮箱密码的常用方法 …… 145
9.3.2 重要邮箱的保护措施 … 146
9.3.3 找回被盗的邮箱密码 … 147
9.3.4 通过邮箱设置防止垃圾邮件 …… 147
9.4 网游账号及密码的防黑实战 … 148
9.4.1 用木马盗取账号的防黑 …… 148
9.4.2 用远程控制方式盗取账号的防黑 …… 150
9.4.3 利用系统漏洞盗取账号的防黑 …… 151
9.5 上机练一练 …… 152
9.5.1 上机目标 …… 152
9.5.2 上机练习 …… 152
9.6 高手秘籍 …… 152
9.6.1 秘籍1：找回被盗的QQ密码 …… 152
9.6.2 秘籍2：将收到的“邮件炸弹”标记为垃圾邮件 … 155

第10章 磁盘数据安全的防黑实战 …… 157

10.1 数据丢失的原因及操作 …… 157
10.1.1 数据丢失的原因 …… 157

10.1.2 发现数据丢失后的操作 …… 157
10.2 备份磁盘各类数据 …… 157
10.2.1 分区表数据的防黑实战 …… 158
10.2.2 引导区数据的防黑实战 …… 158
10.2.3 驱动程序的防黑实战 159
10.2.4 IE收藏夹的防黑实战 … 163
10.2.5 电子邮件的防黑实战 165
10.2.6 磁盘文件数据的防黑实战 …… 167
10.3 各类数据丢失后的补救策略 … 169
10.3.1 分区表数据丢失后的补救 …… 169
10.3.2 引导区数据丢失后的补救 …… 170
10.3.3 驱动程序数据丢失后的补救 …… 170
10.3.4 IE收藏夹丢失后的补救 …… 171
10.3.5 电子邮件丢失后的补救 …… 172
10.3.6 磁盘文件数据丢失后的补救 …… 174
10.4 恢复丢失的数据 …… 175
10.4.1 从回收站中还原 …… 176
10.4.2 清空回收站后的恢复 …… 176
10.4.3 使用EasyRecovery恢复数据 …… 178
10.4.4 使用FinalRecovery恢复数据 …… 180
10.4.5 使用FinalData恢复数据 …… 181
10.4.6 使用数据恢复大师恢复数据 …… 183
10.4.7 格式化硬盘后的恢复 …… 186
10.5 上机练一练 …… 187
10.5.1 上机目标 …… 187
10.5.2 上机练习 …… 187
10.6 高手秘籍 …… 188
10.6.1 秘籍1：恢复丢失的磁盘簇 …… 188
10.6.2 秘籍2：还原已删除或重命名的文件 …… 188

第11章 电脑木马的防黑实战 … 189

11.1 什么是电脑木马 …… 189
11.1.1 常见的木马类型 …… 189
11.1.2 木马常用的入侵方法 … 190
11.2 木马常用的伪装手段 …… 191
11.2.1 伪装成可执行文件 …… 191
11.2.2 伪装成自解压文件 …… 193
11.2.3 伪装成图片 …… 195
11.2.4 伪装成网页 …… 195
11.3 木马的自我保护 …… 196
11.3.1 给木马加壳 …… 196
11.3.2 给木马加花指令 …… 198
11.3.3 修改木马的特征代码 … 199
11.3.4 修改木马的入口点 …… 202
11.4 木马常见的启动方式 …… 202
11.4.1 利用注册表启动 …… 202
11.4.2 利用系统文件启动 …… 203
11.4.3 利用系统启动组启动 … 203
11.4.4 利用系统服务实现木马的加载 …… 203
11.4.5 利用组策略启动 …… 204
11.5 查询系统中的木马 …… 205
11.5.1 通过启动文件检测木马 …… 205
11.5.2 通过进程检测木马 …… 205
11.5.3 通过网络连接检测木马 …… 208
11.6 使用木马清除软件清除木马 … 208
11.6.1 使用木马清道夫清除木马 …… 208

11.6.2 使用木马克星清除木马 …… 212
11.7 上机练一练 …… 213
11.7.1 上机目标 …… 213
11.7.2 上机练习 …… 213
11.8 高手秘籍 …… 213
11.8.1 秘籍1：将木马伪装成电子书 …… 213
11.8.2 秘籍2：修改木马服务端的图标 …… 215

第12章 电脑病毒的防黑实战 … 217

12.1 电脑病毒 …… 217
12.1.1 什么是电脑病毒 …… 217
12.1.2 电脑中毒的途径 …… 217
12.1.3 电脑中病毒后的表现 …… 218
12.2 Windows系统病毒 …… 219
12.2.1 PE文件病毒 …… 219
12.2.2 VBS脚本病毒 …… 220
12.2.3 宏病毒 …… 222
12.3 邮件病毒 …… 223
12.3.1 邮件病毒的特点 …… 223
12.3.2 识别“邮件病毒” … 223
12.4 全面监控未知病毒木马 …… 223
12.4.1 监控注册表与文件 … 224
12.4.2 监控程序文件 …… 225
12.5 病毒的防御 …… 227
12.5.1 邮件病毒的防御 …… 227
12.5.2 未知病毒木马的防御 228
12.6 上机练一练 …… 231
12.6.1 上机目标 …… 231
12.6.2 上机练习 …… 231
12.7 高手秘籍 …… 231
12.7.1 秘籍1：在Word 2003中预防宏病毒 …… 231
12.7.2 秘籍2：通过修改文件的关联性预防病毒 …… 231

第13章 U盘病毒的防黑实战 … 233

13.1 U盘病毒概述 …… 233
13.1.1 U盘病毒的原理和特点 233
13.1.2 常见U盘病毒 …… 233
13.1.3 窃取U盘上的资料 …… 234
13.2 关闭“自动播放”功能防御U盘病毒 …… 235
13.2.1 使用组策略关闭“自动播放”功能 …… 235
13.2.2 修改注册表关闭“自动播放”功能 …… 236
13.2.3 设置服务关闭“自动播放”功能 …… 236
13.3 查杀U盘病毒 …… 237
13.3.1 用WinRAR查杀U盘病毒 …… 237
13.3.2 U盘病毒专杀工具：USBCleaner …… 238
13.3.3 U盘病毒专杀工具：Autorun病毒防御者 …… 240
13.3.4 U盘病毒专杀工具——USBKiller …… 242
13.4 上机练一练 …… 245
13.4.1 上机目标 …… 245
13.4.2 上机练习 …… 245
13.5 高手秘籍 …… 245
13.5.1 秘籍1：通过禁用硬件检测服务让U盘丧失智能 … 245
13.5.2 秘籍2：U盘病毒的手动删除 …… 246

第14章 网页浏览器的防黑实战 …… 247

14.1 认识网页恶意代码 …… 247
14.1.1 恶意代码概述 …… 247
14.1.2 恶意代码的特征 …… 247
14.1.3 恶意代码的传播方式 …… 247

14.2 常见恶意网页代码及攻击方法 …… 247
14.2.1 启动时自动弹出对话框和网页 …… 248
14.2.2 利用恶意代码禁用注册表 …… 248
14.2.3 网页广告信息炸弹 … 249
14.2.4 IE部分属性被禁止 …… 250
14.3 恶意网页代码的预防和清除 … 251
14.3.1 恶意网页代码的预防 …… 251
14.3.2 恶意网页代码的清除 …… 251
14.4 常见网页浏览器的攻击方式 … 253
14.4.1 修改默认主页 …… 253
14.4.2 恶意更改浏览器标题栏 …… 254
14.4.3 强行修改网页浏览器的右键菜单 …… 255
14.4.4 禁用网页浏览器的【源文件】命令 …… 256
14.4.5 强行修改浏览器的首页按钮 …… 258
14.4.6 删除桌面上的浏览器图标 …… 259
14.5 网页浏览器的自我防护技巧 … 260
14.5.1 限制访问不良站点 … 260
14.5.2 提高IE的安全防护等级 …… 261
14.5.3 清除浏览器中的表单 …… 262
14.5.4 清除浏览器的上网历史记录 …… 262
14.5.5 删除Cookie信息 …… 263
14.5.6 屏蔽浏览器窗口中的广告 …… 263
14.6 使用网上工具保护网页浏览器的安全 …… 264
14.6.1 使用IE修复专家 …… 264
14.6.2 IE修复免疫专家 …… 265
14.6.3 IE伴侣 …… 269
14.7 上机练一练 …… 273
14.7.1 上机目标 …… 273
14.7.2 上机练习 …… 273
14.8 高手秘籍 …… 273
14.8.1 秘籍1：网页信息炸弹的防御 …… 273
14.8.2 秘籍2：IE浏览器的优化 …… 274

第15章 网站安全的防黑实战 275

15.1 网站维护基础知识 …… 275
15.1.1 网站的种类和特点 … 275
15.1.2 网站的维护与安全 … 275
15.2 网站的常见攻击方式 …… 276
15.2.1 DoS攻击 …… 276
15.2.2 DDoS攻击 …… 279
15.2.3 SQL注入攻击 …… 284
15.3 网站安全的防黑 …… 289
15.3.1 检测上传文件的安全性 …… 289
15.3.2 设置网站访问权限 … 291
15.3.3 在注册表中预防SYN系统攻击 …… 292
15.3.4 DDoS攻击的防御措施 …… 294
15.3.5 全面防御SQL注入攻击 …… 295
15.3.6 备份网站数据 …… 296
15.3.7 恢复被黑客攻击的网站 …… 298
15.4 网站数据库的防黑 …… 298
15.4.1 备份网站数据库 …… 298
15.4.2 恢复网站数据库 …… 301
15.5 上机练一练 …… 303
15.5.1 上机目标 …… 303
15.5.2 上机练习 …… 303
15.6 高手秘籍 …… 303

15.6.1 秘籍1：保护本机中的数据库 …… 303
15.6.2 秘籍2：保护网站安全技巧 …… 304

第16章 无线蓝牙设备的防黑实战 …… 305

16.1 了解蓝牙 …… 305
16.1.1 什么是蓝牙 …… 305
16.1.2 蓝牙技术体系及相关术语 …… 306
16.1.3 蓝牙适配器的选择 … 308
16.2 蓝牙设备的配对操作 …… 309
16.2.1 蓝牙（驱动）工具安装 …… 309
16.2.2 启用蓝牙适配器 …… 310
16.2.3 搜索开启蓝牙功能的设备 …… 311
16.2.4 使用蓝牙适配器进行设备间配对 …… 311
16.2.5 使用耳机建立通信并查看效果 …… 312
16.3 蓝牙基本Hacking技术 …… 313
16.3.1 识别及激活蓝牙设备 … 313
16.3.2 查看蓝牙设备相关内容 …… 314
16.3.3 扫描蓝牙设备 …… 314
16.3.4 蓝牙攻击技术 …… 316
16.3.5 修改蓝牙设备地址 … 317
16.4 蓝牙DoS攻击技术 …… 318
16.5 安全防护及改进 …… 320
16.6 上机练一练 …… 321
16.6.1 上机目标 …… 321
16.6.2 上机练习 …… 321
16.7 高手秘籍 …… 321
16.7.1 秘籍1：蓝牙Bluebuging攻击技术 …… 321
16.7.2 秘籍2：蓝牙DoS测试问题 …… 324

第17章 无线网络安全的防黑实战 …… 325

17.1 建立无线网络 …… 325
17.2 无线网络的安全加密 …… 326
17.2.1 WEP加密 …… 326
17.2.2 WPA-PSK安全加密算法 …… 328
17.2.3 禁用SSID广播 …… 329
17.2.4 媒体访问控制（MAC）地址过滤 …… 331
17.3 上机练一练 …… 332
17.3.1 上机目标 …… 332
17.3.2 上机练习 …… 332
17.4 高手秘籍：无线网络方案设计 …… 332

第18章 虚拟专用网的防黑实战 …… 333

18.1 虚拟专用网的原理 …… 333
18.1.1 虚拟专用网的组件 … 333
18.1.2 隧道协议 …… 333
18.1.3 无线VPN …… 334
18.2 虚拟专用网的攻防实战 …… 335
18.2.1 攻击PPTP VPN …… 335
18.2.2 攻击启用IPSec加密的VPN …… 337
18.2.3 本地破解VPN登录账户名及密码 …… 339
18.3 虚拟专用网的防护及改进 …… 339
18.4 上机练一练 …… 340
18.4.1 上机目标 …… 340
18.4.2 上机练习 …… 340
18.5 高手秘籍：无线网络的优化 … 340

第19章 移动手机的防黑实战 … 341

19.1 手机的攻击手法 …… 341
19.1.1 通过网络下载 …… 341
19.1.2 利用红外或蓝牙传输 … 341
19.1.3 短信与乱码传播 …… 342

19.1.4 利用手机BUG传播 … 342
19.1.5 手机炸弹攻击 …… 342
19.2 手机的防黑实战 …… 343
19.2.1 关闭手机蓝牙功能 … 343
19.2.2 保证手机下载的应用程序的安全性 …… 344
19.2.3 关闭乱码电话，删除怪异短信 …… 344
19.2.4 安装手机卫士软件 … 345
19.2.5 经常备份手机中的个人资料 …… 345
19.3 上机练一练 …… 345
19.3.1 上机目标 …… 345
19.3.2 上机练习 …… 345
19.4 高手秘籍 …… 345
19.4.1 秘籍1：使用手机交流工作问题 ……345
19.4.2 秘籍2：苹果手机的白苹果现象 ……346

第20章 手机钱包的防黑实战… 347

20.1 手机钱包的攻击手法 …… 347
20.2 手机钱包的防黑策略 …… 347
20.3 上机练一练 …… 348
20.3.1 上机目标 …… 348
20.3.2 上机练习 …… 348
20.4 高手秘籍 …… 348
20.4.1 秘籍1：手机钱包如何开通 …… 348
20.4.2 秘籍2：手机钱包如何充值 …… 348

第21章 平板电脑的防黑实战 349

21.1 平板电脑的攻击手法 …… 349
21.2 常用的平板电脑的防黑策略… 349
21.2.1 自动升级固件 …… 349
21.2.2 重装系统 …… 351
21.2.3 为视频加锁 …… 351
21.2.4 开启“查找我的iPad”功能 …… 353
21.2.5 远程锁定iPad …… 354
21.2.6 远程清除iPad中的信息 …… 355
21.3 上机练一练 …… 355
21.3.1 上机目标 …… 355
21.3.2 上机练习 …… 355
21.4 高手秘籍 …… 355
21.4.1 秘籍1：给丢失的iPad发信息 …… 355
21.4.2 秘籍2：丢失的iPad在哪儿 …… 356

第1章　黑客文化漫谈

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；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，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，国内上网的人数持续翻番，网民日益活跃，“黑客”事件时有发生。国内黑客的发展主要经历了以下3个阶段。

（1）第1代（1996～1998）：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代黑客大多是从事科研、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，并且在一些国家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。中国黑客对这些国家的网站发动了攻击，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）：随着计算机的普及和因特网的发展，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。这一代黑客的兴起由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～至今）：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，大多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的。但领导这一代的核心黑客还是第1代、第2代的前辈们。这一代黑客的兴起由2001年4月的一个撞机事件引发，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

（1）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，主要表现在以下6个方面：

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，此类站点只顾教他人攻击别人的电脑，如刷Q币、盗密码等，以迎合初学者的口味，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，所以众多黑客站点投其所好，使之趋之若鹜，以此提高自己的站点访问量，而不靠实力提高站点的质量和知名度。

3）内容粗制滥造

一些黑客站点内容粗制滥造，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多进行商业化运作，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。这些站点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，国外的黑客则是研究系统级别的漏洞，制造的也是世界级别的系统病毒，以扰乱全球网络。

6）缺少一个统一协调中国黑客界行动发展的组织

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

（2）目前中国黑客的发展总体上可以归纳为五大趋势。

1）黑客年轻化：由于中国互联网的普及，形成了全球一体化，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而言，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，虽然大家在市面上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就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以下事情：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，梅利莎病毒使全世界300多家公司的电脑系统崩溃，该病毒造成的损失接近4亿美金，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，它成功地阻止了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，全球最大的中文搜索引擎“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逐渐趋于普遍化。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），这也就是人们平时经常听说的“黑客”（Cacker）和“红客”（Hacker）。

不管是“黑客”还是“红客”，他们最初学习的内容和掌握的基本技能都是一样的，即便日后他们走上了不同的道路，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

目前，网络上总结出来的黑客守则有很多，主要包括以下10个方面：
①不得恶意破坏任何系统。
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 黑客需要掌握的资源

一般来讲，做什么事情都是入门难，要想成为一名黑客，其实也是一个不断学习的过程，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，甚至连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，例如关于TCP/IP、网络、操作系统以及局域网等的书，甚至是关于DOS、Windows基础的书都是很有必要的。此类书籍关键在于通俗易懂，不要追求深入，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，例如电脑报合订本、电脑应用合订本等，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，各个方面均有涉及，查找方便，但因其定位于大众杂志，内容相对比较基础，适合新手做全方位地了解。

（3）Hack杂志类：例如《黑客防线》《黑客X档案》《黑客手册》等，此类杂志专业性强，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，例如到各大安全站点的文章中去找，或者到相关论坛或Google中去搜索。