



电脑报 总策划

电脑宝贝2009

PC Baby

【黑客入门首选指导手册】

黑客攻防实例操作

即查即用

电脑报 编



精彩光盘

- 价值**51**元的《加密特警》
- 黑客扫描利器
- 密码解除工具
- 远程控制工具



电脑报电子音像出版社
CEAP ELECTRONIC & AUDIOVISUAL PRESS

PCBaby · 2009



黑客攻防实例操作 即查即用

电脑报 编



电脑报电子音像出版社
CEAP ELECTRONIC & AUDIOVISUAL PRESS



内容提要

本手册从应用的角度阐述了黑客常见的攻击手段和步骤，并提出了相应的预防措施和建议，可读性和实践性非常强。主要内容包括扫描与入侵、嗅探与监听、远程控制、木马攻防、突破局域网限制、QQ及电邮攻防、口令破解等实例。

本手册不仅是广大黑客爱好者必备手册，对网络管理员和系统管理员同样具有重要的参考价值。



光盘内容

- 价值51元的《加密特警》
- 黑客扫描利器
- 密码解除工具
- 远程控制工具

特别声明：使用网络技术攻击他人电脑属于违法行为，本手册旨在让读者提高警惕避开潜在的网络威胁，读者切勿模仿入侵他人电脑，否则后果自负。

书 名：黑客攻防实例操作即查即用
 编 者：电脑报
 技 术 编 辑：何 磊
 封 面 设 计：陈 敏
 出 版 单 位：电脑报电子音像出版社
 地 址：重庆市双钢路3号科协大厦
 邮 政 编 码：400013
 读 者 服 务：023-63658888-12028
 对 外 合 作：023-63658933
 发 行：电脑报经营有限责任公司
 经 销：各地新华书店、报刊亭
 C D 生 产：四川省葭山数码科技有限公司
 文 本 印 刷：重庆升光电力印务有限公司
 开 本 规 格：787mm × 1092mm 1/32 9印张 300千字
 版 本 号：ISBN 978-7-89476-040-1
 版 次：2008年12月第1版 2008年12月第1次印刷
 定 价：15.00元(1CD+配套书)

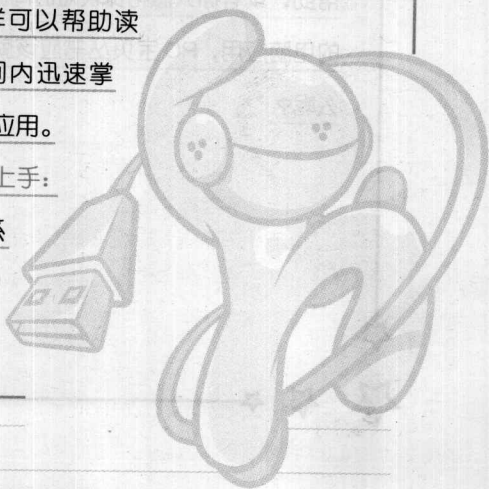


宝贝在手，应用无忧

PC 宝贝系列丛书是集实用、便捷、时尚于一身的新型电脑应用手册。自 2002 年初版以来，本系列丛书就以其操作性极强的内容、便携式的开本与迷你光盘，以及超实用的配套软件，迅速赢得了众多“粉丝”。迄今本系列丛书的读者已达百万之众，影响可见一斑。近年来，在部分热心读者的参与下，丛书的编辑团队不断结合电脑应用的最新潮流与趋势，经过逐年与时俱进的修订再版，使得这套丛书无论是在内容抑或形式上都已趋于完美。

内容专注，选题讲究：在选题上，本系列丛书非常讲究贴近实际应用。细心的读者可能注意到，丛书每一分册均选取时下应用最为广泛或关注度较高的某一专题领域进行讲解，这样可以帮助读者在尽可能短的时间内迅速掌握主流的电脑操作与应用。

立体解说，易于上手：
在版面编排上，本系列丛书采用把每个学习要点或者操



作目标细分步骤，在实际应用或实务操作的基础上进行分解、分析，化难为易，并一律以简明扼要的语言配合直观的图示予以解说，极大地提高了学习的效率。

实例丰富，即查即用：本系列丛书大量结合应用实例进行讲解，内容实用，条目清晰，非常方便读者学习和理解。同时由于本系列丛书精致乖巧、携带方便，用户可以随时查阅，能真正为用户排忧解难，解决用户的不时之需。

书盘互动，物超所值：随书配套的精美迷你光盘，包含了与图书内容匹配的大量实用软件。同时每张光盘都向读者附赠送一个相关的实用正版软件，真正物超所值，回馈给读者看得见的实惠。

如果你正在为提升自己的电脑操作和应用技巧寻求帮助，或者你只想花费较短时间就掌握那些最主流最热门的电脑应用，PC 宝贝丛书应该就是你的首选。还犹豫什么呢？

编者

2008 年 12 月

第一章 例说黑客攻防之道	1
例1 揭开QQ币/Q点被盗之谜	2
1.1.1 QQ木马是如何制作的	2
1.1.2 批量登录被盗QQ	4
1.1.3 Q币/Q点被盗实录	6
例2 暗处偷窥的第三只“眼”	8
1.2.1 “黑洞”木马远程开启摄像头	8
1.2.2 揪出隐藏在系统中的“黑洞”木马	10
1.2.3 防范摄像头木马，安全意识很重要	12
例3 利用135端口抓鸡的黑手	14
1.3.1 为什么135端口会被利用来抓鸡	14
1.3.2 黑客是怎么利用135端口抓鸡的	15
1.3.3 防范135端口漏洞技巧	17
例4 劲舞团狂暴升级揭秘	18
1.4.1 想怎么“玩”就怎么改	18
1.4.2 劲舞团修改实例	19
1.4.3 自刷劲舞团韩服	22
例5 让局域网瘫痪的ARP欺骗	23
1.5.1 帮助“确定主机身份”的ARP	23
1.5.2 ARP为何成为病毒利用目标	24
1.5.3 阻断网络只是ARP病毒的危害之一	26
1.5.4 未中毒的电脑也逃脱不了危险	27
1.5.5 ARP病毒的应对之策	28
例6 Windows系统万能登录	29
1.6.1 删除SAM文件登录Windows	29
1.6.2 利用LC4从SAM文件中找密码	30
1.6.3 巧用屏保破解密码	31



1.6.4 ERD Commander: 强大实用的系统拯救工具	32
例7 解除ISP限制路由共享上网	35
例8 黑客如何穿透Windows系统防火墙	37
1.8.1 刺穿防火墙的利剑	37
1.8.2 看防火墙如何倒下	38

第二章 用虚拟机打造黑客练兵营 41

2.1 初识虚拟机	42
2.2 配置虚拟机环境安装操作系统	43
2.2.1 安装操作系统前的初始配置	43
2.2.2 更改虚拟机配置	47
2.2.3 更改磁盘文件路径	50
2.2.4 安装操作系统	50
2.3 增强虚拟机功能与性能	52
2.3.1 什么是VMware Tools	52
2.3.2 不同操作系统VMware Tools安装方法	53
2.3.3 访问主机资源	54
2.4 用“快照”快速备份与恢复系统	57
2.5 搭建虚拟网络	59
2.5.1 VMware的4种网络模式	59
2.5.2 用VMware组建虚拟网络环境	63

第三章 黑客如何通过扫描器发现目标 67

3.1 扫描目标主机IP与端口	68
3.1.1 IPScan扫描活动主机	68
3.1.2 使用NetSuper扫描共享资源	69
3.1.3 局域网查看工具LanSee	71



3.1.4 扫描目标主机开启的端口	72
3.1.5 功能丰富的SuperScan端口扫描器	74
3.1.6 综合扫描器X-Scan	80
3.2 一个典型的系统扫描入侵示例	91
3.2.1 扫描远程主机是否存在NT弱口令	91
3.2.2 使用DameWare入侵漏洞主机	92

第四章 远程控制目标系统攻略

103

4.1 Windows Vista的远程协助	104
4.1.1 Windows Vista远程协助的改进	104
4.1.2 启动Windows Vista中的远程协助	105
4.1.3 发送远程协助请求	107
4.1.4 接受远程协助请求	110
4.1.5 远程协助其他设置	111
4.2 Windows XP远程协助设置	114
4.2.1 通过XP远程桌面连接	114
4.2.2 家庭版XP的远程协助方案	116
4.3 pcAnywhere远程控制计算机	118
4.3.1 pcAnywhere的工作原理	118
4.3.2 被控端的配置	118
4.3.3 主控端的配置	120
4.3.4 网络连接的优化配置	121
4.3.5 远程控制的实现	121

第五章 木马入侵与防范揭秘

123

5.1 什么是木马	124
5.1.1 木马的定义	124



5.1.2 木马的特征	125
5.1.3 木马的功能	126
5.1.4 木马的分类	126
5.2 典型木马“冰河”入侵示例	127
5.2.1 配置冰河木马的服务端（被控端）	127
5.2.2 远程控制冰河服务端	130
5.3 冰河木马防范与反攻	131
5.4 灰鸽子木马常见问题解决方案	133
5.4.1 服务端与客户端同在一个局域网内	133
5.4.2 客户端拥有公网固定（静态）IP	133
5.4.3 客户端通过ADSL拨号上网	134
5.4.4 客户端位于内网中	137
5.4.5 客户端位于内网中但不能设置网关	139
5.4.6 清除计算机中的灰鸽子	144
5.4.7 防止中灰鸽子病毒需要注意的事项	149
5.5 预防信息泄漏的7种方法	149

第六章 黑客突破网络限制秘诀 153

6.1 使用代理上网突破网络限制	154
6.1.1 突破局域网上网限制	154
6.1.2 网上查找代理服务器	157
6.2.3 扫描工具查找	159
6.2.4 代理猎手使用要点	165
6.2 突破ISP限制BT下载攻防战	171
6.2.1 BT下载已成ISP的眼中钉	171
6.2.2 BT下载攻防战的三大战役	171
6.2.3 BT下载的长久攻防战	176

6.3 巧用《共享神盾》突破路由封锁	176
6.4 解除网页右键限制	178
6.4.1 键盘操作破除右键限制	178
6.4.2 利用工具突破下载限制	179
6.4.3 修改网页源代码破除限制	179
6.5 下载在线流媒体	180
6.5.1 从HTML源代码中查找	180
6.5.2 保存文件查找法	181
6.5.3 巧用迅雷下载流媒体	181
6.5.4 RAM或ASX中查找	182
6.5.5 WMP下载流媒体	182
6.5.6 通过播放器寻找下载地址	182
6.6 网吧管理限制的漏洞	183

第七章 QQ、电邮盗号与隐私泄露的秘密 185

7.1 曝光QQ木马中隐藏的盗号信箱	186
7.1.1 黑客盗QQ过程推演	186
7.1.2 如何追寻黑客踪迹	187
7.1.3 QQ防盗技巧	188
7.2 预防其他木马盗取QQ	189
7.2.1 “QQ简单盗”揭秘	190
7.2.2 “QQ流感大盗”揭秘	192
7.2.3 “QQ盗号王”揭秘	194
7.3 注意扫描QQ信箱也能盗取密码	195
7.4 QQ聊天记录是如何被偷窥的	198
7.4.1 为什么聊天记录会被盗取	198
7.4.2 两种聊天记录偷窃方法	198



7.4.3 聊天记录防盗技巧	200
7.5 本地破解QQ的原理与防范	201
7.5.1 本地破解的奥秘	201
7.5.2 本地破解的原理和预防	201
7.6 使用QQ申诉取回被盗的QQ	203
7.7 电子邮箱密码是如何被破解的	207
7.7.1 添加扫描邮件服务器	207
7.7.2 确定扫描的账户	208
7.7.3 添加密码文件	210
7.7.4 扫描正确的密码	211

第八章 密码的破解与防范 213

8.1 常见系统口令解除示例	214
8.1.1 解除CMOS口令	214
8.1.2 解除系统密码	215
8.2 巧除Word与Excel文档密码	217
8.2.1 清除Word密码	217
8.2.2 清除Excel密码	218
8.3 清除压缩文件密码	218
8.3.1 密码恢复工具也成黑客帮凶	218
8.3.2 巧妙设置，让压缩文件无懈可击	221
8.4 黑客破解密码的心理学	223

第九章 利用嗅探器截取数据信息揭秘 ... 225

9.1 局域网中的嗅探与监听	226
9.1.1 日记泄露的秘密	226
9.1.2 嗅探器应用范围	227

9.1.3 局域网内计算机通讯的概念和寻址	228
9.1.4 发生在共享式局域网内的窃听	230
9.1.5 发生在交换式局域网内的窃听	231
9.2 Sniffer介绍	233
9.2.1 Sniffer的特性	234
9.2.2 Sniffer分类	235
9.3 Iris网络嗅探器	235
9.3.1 Iris的特点	235
9.3.2 设置与使用Iris	236
9.3.3 利用Iris捕获邮箱密码	239
9.3.4 利用Iris捕获Telnet会话密码	241
9.4 网络间谍SpyNet Sniffer	243
9.4.1 SpyNet Sniffer设置	243
9.4.2 使用SpyNet Sniffer	244
9.5 艾菲网页侦探	246
9.5.1 艾菲网页侦探设置	246
9.5.2 使用艾菲网页侦探	247
9.6 拒绝网络黑客防御Sniffer攻击	248
9.6.1 怎样发现 Sniffer	249
9.6.2 抵御 Sniffer	249
9.7 使用屏幕间谍监视本地计算机	250
9.7.1 软件功能面板	251
9.7.2 记录浏览	253

附录一

IP地址常识	255
什么是IP地址	255



公网IP与私有IP	256
动态IP和固定IP	257
私有IP地址分段	258
IP的类别	259
子网掩码	261
NAT网络地址转换	262
端口与协议	263
什么是端口	263
端口分类	265
常见的端口	266
查看端口	268
限制端口	269

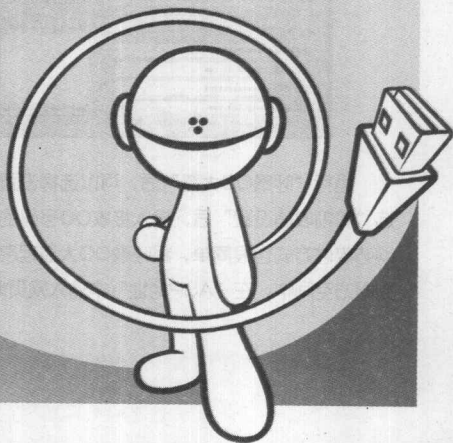
附录二

Ping 命令	269
Netstat 命令	271
IPConfig 命令	272
ARP(地址转换协议)	273
Tracert 命令	274
Route 命令	275
NBTStat 命令	276

第一章

例说黑客攻防之道

- 例1 揭开QQ币/Q点被盗之谜
- 例2 暗处偷窥的第三只“眼”
- 例3 利用135端口抓鸡的黑手
- 例4 劲舞团狂暴升级揭秘
- 例5 让局域网瘫痪的ARP欺骗
- 例6 Windows系统万能登录
- 例7 解除ISP限制路由共享上网
- 例8 黑客如何穿透Windows系统防火墙



Internet（因特网）的普及使人们的工作生活发生了翻天覆地的变化，可是在Internet世界中却没有人来管理。如同武侠小说中的“江湖”一样，在这个没有王法的世界中滋生出了许多正派和邪派的力量，他们有秩序的建立者，也有潜在的破坏者，他们被人们统称为——黑客。下面让我们走进黑客的世界，一同揭开黑客神秘的面纱。

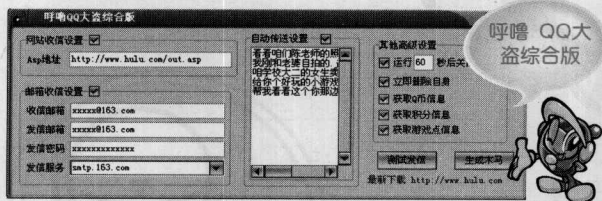
例1 揭开QQ币/Q点被盗之谜

Q币具有许多实用价值，被不法分子窥视着，盗号者可以通过间接的方法来得到Q币——制作盗QQ号的木马，盗取大量的QQ号。在这些QQ号中往往会带有一些Q币，通过盗Q木马查看QQ号上的Q币，或者通过QQ批量自动登录，查看得到的QQ账户上有Q币，再将这些号码上的Q币兑换成购物券赠送给自己……



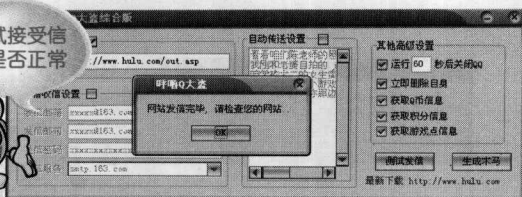
1.1.1 QQ木马是如何制作的

“呼噜QQ大盗”是目前非常厉害的QQ木马，它可以获取用户Q币、QQ积分、QQ游戏点等信息。能破解QQ的键盘保护，入侵所有版本的QQ。再加上采用特殊的线程插入技术，无启动项、无进程，可以有效的突破各类防火墙！



运行“呼噜QQ大盗”后，可以选择设置网页和邮件两种收信方式。勾选“邮箱收信设置”后，输入接收QQ号码的邮箱及发信邮箱等信息即可。网站收信方式也很简单，将呼噜QQ大盗程序压缩包中的“out.asp”上传到网站空间中，在“ASP地址”中输入网页地址即可。

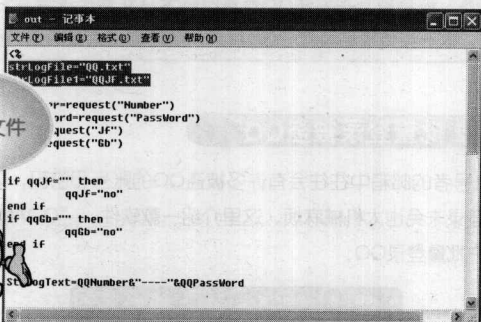
测试接受信箱是否正常



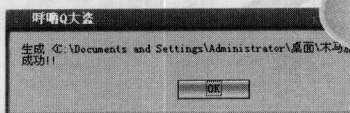
注意

采用网页收QQ号方式时，盗取的QQ号默认保存到同路径下的“QQ.txt”文件中。可用记事本打开“out.asp”文件，将其中的“strLogFile=“QQ.txt” strLogFile1=“QQJF.txt””中的“QQ.txt”和“QQJF.txt”改为其它的文件名，如下图所示。

ASP文件



“呼噜QQ大盗”最重要的设置项是勾选右侧“其它高级设置”中的“获取Q币信息”，生成的盗Q木马就可以自动检测显示相应QQ号上的Q币数目。另外还可以设置获取积分、游戏币等信息，在运行木马后删除木马文件等。最后单击“生成木马”按钮，就可以生成一个功能超强的盗Q木马了，如下图所示。



生成QQ木
马服务端



将生成的盗Q木马加上壳后，想办法发送给目标用户，或者在网吧中运行，盗号者就可以等着鱼儿上钩了！

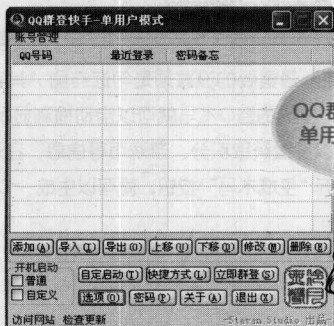
注意

在生成盗Q木马时，可以勾选“自动传送设置”项，并在下方的列表框中输入迷惑性的文件名。该项功能有点类似QQ尾巴病毒，当某台主机上运行了这个盗Q木马后，除了可盗取QQ密码外，还会自动在发送QQ信息时将木马文件传送给其它QQ好友，进一步传播感染其它QQ用户，迅速盗得大量的QQ号码！



1.1.2 批量登录被盗QQ

QQ盗号者的邮箱中往往会有许多被盗QQ的账号和密码，如果一个一个地测试登录未免也太机械麻烦，这里介绍一款软件：“QQ群登快手”，它能让用户批量登录QQ。



QQ群登快手
单用户模式



第1步：将邮箱中接收的QQ号码和密码复制到一个文本中，按照一行