电脑報 总策划

电脑宝贝2009

PCBaby

【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
CD生产：四川省蓥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)

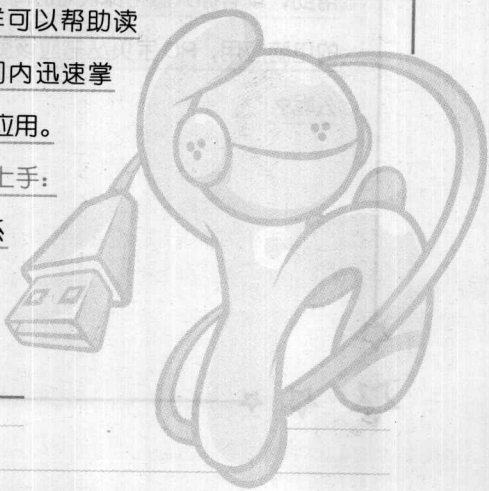
前言

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，极大限度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。

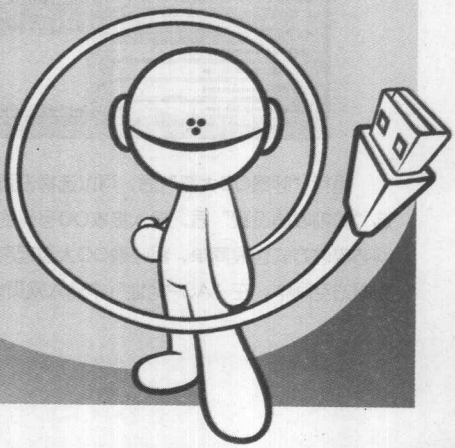
如果你正在为提升自己的电脑操作和应用技巧寻求帮助，或者你只想花费较短时间就掌握那些最主流最热门的电脑应用，PC 宝贝丛书应该就是你的首选。还犹豫什么呢？

编者

2008 年 12 月

第一章

例说黑客攻防之道



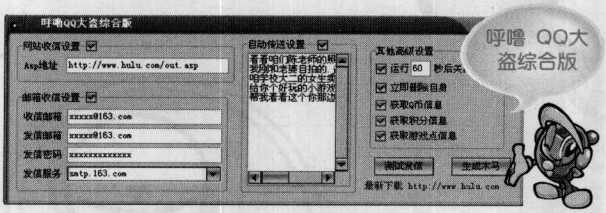
Internet（因特网）的普及使人们的工作生活发生了翻天覆地的变化，可是在Internet世界中却没有人来管理。如同武侠小说中的“江湖”一样，在这个没有王法的世界中滋生出了许多正派和邪派的力量，他们有秩序的建立者，也有潜在的破坏者，他们被人们统称为——黑客。下面让我们走进黑客的世界，一同揭开黑客神秘的面纱。

例1 揭开QQ币/Q点被盗之谜

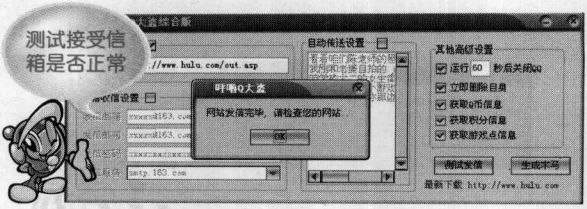
Q币具有许多实用价值，被不法分子窥视着，盗号者可以通过间接的方法来得到Q币——制作盗QQ号的木马，盗取大量的QQ号。在这些QQ号中往往会带有一些Q币，通过盗Q木马查看QQ号上的Q币，或者通过QQ批量自动登录，查看得到的QQ账户上有Q币，再将这些号码上的Q币兑换成购物券赠送给自己……

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！

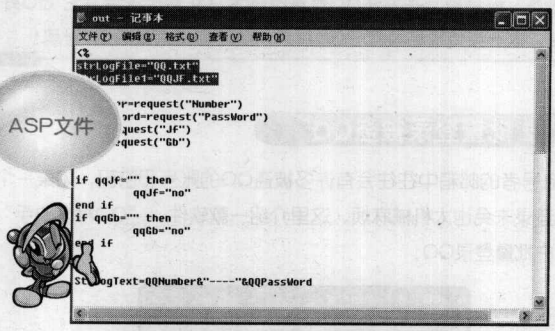


运行“呼噜QQ大盗”后，可以选择设置网页和邮件两种收信方式。勾选“邮箱收信设置”后，输入接收QQ号码的邮箱及发信邮箱等信息即可。网站收信方式也很简单，将呼噜QQ大盗程序压缩包中的“out.asp”上传到网站空间中，在“ASP地址”中输入网页地址即可。

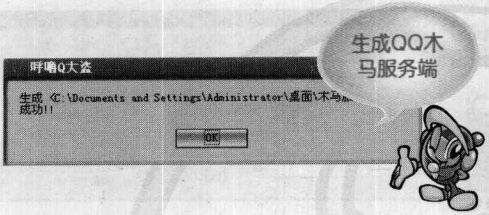


注意

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。



“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。



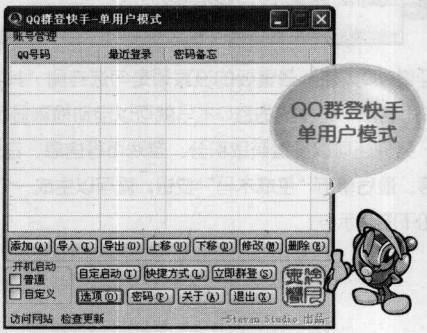
将生成的盗Q木马加上壳后，想办法发送给目标用户，或者在网吧中运行，盗号者就可以等着鱼儿上钩了！

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。



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