电脑报 精品图书 CPCW BOOKS

网络生存手册

HACKER 黑客手记

FREE!

超级黑客攻防软件大礼包!!

虚拟主机空间超值折扣券

编著：齐宝玮 罗俊

一本人人都能看懂的黑客书

特别企划：缔造中国黑客文化

黑客攻防纪实

QQ被盗？邮箱中招？

见识设计的木马病毒让你防不胜防？

金山毒霸？卡巴斯基？……杀毒软件，靠谱吗？

大发现！

由什么古老神话之物成为现代网络必备武器？

想亲手打造个人木马？网站可以替你做到？

因体怎样拥有更安全的服务器？

一切答案，尽在其中！

黑客高手必备技能

当防守、加密、修改注册表

都已不再管用，

我们开始学会反击！

进攻才是最好的防守。

超值附赠软件工具

金山毒霸2005安全组合套装下载、卡巴斯基单机版、江民防火墙2004、Anti-Trojan Shield、TrojanHunter、VKill、木马防御专家、Windows木马清道夫、BlackICE PC Protection、蓝盾防火墙、Kerio WinRoute Firewall、江民网络安全网镖、Spy Bouncer、PC虚拟系统管理大师、伪装文件夹……

山东电子音像出版社出版

网络生存手册

HACKER 黑客手记

编著：齐宝玮 罗俊

山东电子音像出版社出版

内容提要

黑客对于普通大众来说是富有神秘感的一群人。本书通过一名电脑用户，从一般使用者到小有名气的黑客的经历，令读者在谐趣中快速了解电脑安全知识。

由于主人公的形象源于生活，更易于贴近读者，引发起兴趣。同时对于黑客来说，也如同自己的成长历程描述。

本书语言轻松搞笑，并配有幽默漫画，令图书更加活泼生动。

光盘内容：

本光盘中包括金山毒霸2005安全组合装下载、卡巴斯基单机版、木马防御专家、Windows木马清道夫、TrojanHunter等黑客攻防相关软件。

书　　名：网络生存手册——黑客手记
编　　著：齐宝玮　罗　俊
责任编辑：李　萍
执行编辑：戎　马　朱怡欣　章　立
封面设计：马　静
组版编辑：杨　亚
监　　制：时均建
出版单位：山东电子音像出版社
地　　址：济南市胜利大街39号
邮政编码：250001
电　　话：(0531)2060055-7616
发　　行：山东电子音像出版社
经　　销：各地新华书店、报刊亭
CD生产：北京中联光碟有限公司
文本印刷：重庆大学建大印刷厂
开本规格：787mm × 1092mm 1/16　　14.5印张　150千字
版 本 号：ISBN 7-89491-222-0
版　　次：2005年6月第1版　2005年6月第1次印刷
定　　价：22.00元(1CD+手册)

人物介绍

我：

男，23岁，未婚也有女友，大学毕业后顺利进入一家企业。凭着滔滔不绝的口才得到公司的赏识成为销售副总。年轻有为，在计算机的世界里与世无争！然而世界总是多变的，在经历了电脑中毒、QQ被盗等若干桩不幸发生的事件后开始拿起黑客之剑，奋而反击……

女友：

主人公公司旗下企业的一职员，因为上下班经常见面让主人公见色起意，后来经过他三寸不烂之舌终令其成为自己女朋友！端庄文静，在关键的时候总让主人公醍醐灌顶，后因见主人公陷入黑客的泥潭中不能自拔，于是也奋而学习，成为黑客界一代佳侠！

经理：

具有典型中国男人的性格，他是在公司都是声名显赫，但是却平易近人，深受员工爱戴。在此文中经理为客串，特此描述。

游民：

一同龄男，和主人公曾经为校友而交情颇深。在主人公成长的道路上不能没有此人的鼓励。此人的长相爱好和主人公相仿。因此在某些地方造成的共鸣使人的倍加，这点在打反恐精英这个射击游戏的时候就体现了出来！

漫漫长夜：

某神秘黑客，因为在论坛看见主人公一颗年少的黑客心遂收入门下，传其九九八十一招绝命黑客剑术。然此君深不可测，在历史以来的黑客战役中均付出自己的心血，确实名字而在谜团之中！

HEIKESHOUJI

[目 录]

我的愿望——不再作待宰的羔羊

自我保护意识

更上一层楼

小试牛刀——黑客实例攻击

梦在前方

我的愿望——不再作待宰的羔羊

突然

1.1 QQ受难记

为什么受伤的总是我！工作出了纰漏。为了将功补过，拼命工作，却忽视女朋友，从而遭受冷战待遇。好，那我安安静静上网总行了吧？也许能从网络MM的可人言辞中找到一丝心理安慰。可是为什么，为什么，为什么！难道人倒霉，QQ也会受伤？呜……

1.1.1 晕，QQ中毒

登上QQ，沉寂已久的昔日情人头像一阵闪动，让我的心像小鹿乱撞——原来老天爷还是公平的，感动ING！于是强忍住颤抖，我双击头像……

QQ对话框显示："上次看了个网站不错，去看看吧：http://www.qq588.com"（编辑提示：此网址为某虚构网址）。

我心中一动，兴奋之余却有一种森冷之感。我疑虑重重的打开那个网页，但见漫天的网页窗口飞舞，不明所以，遂回复消息问之："mm何事啊？怎么这网址如此蹊跷？"而在我按下回车键的同时下面居然多了几句话。啊，今天电脑如此人性化啊？

但事情越来越不对劲，有时候甚至消息没写完就会自动发出去了，打开网页，而主页竟是刚才那个网址！利用一点儿微薄的电脑知识，终于，我推理出结论——中毒了！

无奈之下，我在某电脑技术论坛发了一个求助贴，并在不久后得到回复。

西山（就是我）：各位同胞，今日兄弟的QQ误入病毒深处，读写消息已诸多不便，IT主页业已被修改，深感焦虑……（略去数句症状描述）各位若有悬天悯人之心，请赐与良方，不胜荣幸，感激涕零！

漫漫长夜：杀毒！

西山：怎么杀？

漫漫长夜：……

漫漫长夜：其实杀毒很简单的，就是简单的查找病毒文件，然后全部给我杀了，然后去注册表看看看，该删的删！Understand？

西山：大哥，能否详述一下，兄弟我乃集菜鸟之大成，500年难得一出的那只！

漫漫长夜：那个QQ病毒内容是不是有这个地址啊：http://www.qq588.com，这个病毒其实并不厉害，关键在于你这小子对病毒一点防范意识都没有。如今网络群雄四起，病毒更是五花八门，没有一点斤两，能在网上飘吗？

你中的这个病毒名叫"QQ连发器"。它通常隐藏在系统中，当你的QQ上线后，

它就开始工作，并且在系统中生出了一个文件“WebAuto.exe”，知道怎么利用系统的搜索功能吧？把他们找出来全部干掉！然后打开注册表，如下所示：

在“HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run”启动项中肯定有“WebAuto.exe”，别管它，删除了再说。

如此照做，绝对保你药到病除！不过别告诉我你不会进注册表。

西山：怎么进注册表？

漫漫长夜：○%＃＃○＃＃＃＃＃%%%%

……（经过1分零40秒的漫长等待）

漫漫长夜：好吧，今天就好人做到底！你点击“开始”→“运行”，在对话框里面输入“regedit”。顺便一提，别乱打开别人给你的网站，就算有再大的吸引力，也要问一问对方是否是无毒的。再有，你最好还是把杀毒软件、防火墙什么的都安上，这样少很多麻烦。

当然啦，这些只是一定的防范措施，关键还是看你自己，别一天到晚只知道玩，多学学这方面的东西对你可有大好的帮助！对了，这次准备怎么报答我？

西山：谢谢啊，我在盟洗街18号物业大楼2层13号，我请你喝茶啊！

漫漫长夜：小样儿，我最讨厌喝茶了！

西山：……

漫漫长夜：我下了，今天有个饭局！

西山：哇……

经过一番惨烈血腥地厮杀，我那奄奄一息的电脑终于恢复了勃勃生机。而本次事件也将永留我心。它之于我的影响，丝毫不亚于“诺曼底登陆”之于二战，它是我生命中的一座里程碑！

1.1.2 哭，QQ被盗

如果上天要惩罚你的话，那是太简单不过了！中毒事件后的第二天，照例打开QQ的我刚一登陆，突然发现密码错误。难道是刚才过马路的时候没有扶那个老太太？真是屋漏偏逢连夜雨啊，我把鼠标一甩，恨恨地坐在椅子上一动不动。

“咚咚咚！”外面传来一阵敲门声。

我懒懒地起身开门，门刚开一个缝，一个胖乎乎的东西就塞了进来，然后两只小眼睛对我一眨一眨。我忙往后一跳，这才看清楚了原来是高中同学——游民。

忽然想起游民是一个网吧的网管，我忙堆笑上前。并以最快的语速解释了状况，并威逼利诱，最终达成协议——鸡腿换QQ。

游民走到我的电脑前，捣鼓一会儿说道：“你电脑好像中木马了！”但见我一脸疑惑，便接着解释，“你没看你电脑反映迟钝么？好像几天没吃饭了一样(晕，不愧是游民的形容)！再说你QQ在家里被盗，这个可能性就更大了！”

“木马？特洛伊木马？”我疑惑。

“对！就是来自于这个古希腊神话。其实也就是一个病毒程序经过伪装进入电脑里盗窃机密，然后传输回它的主人。老实说——你是不是打开过什么不该看的啊？”

“没有！”我斩金截铁，“你继续。”

游民喝了一口水，继续说到：“这木马隐藏在你的系统中，在系统注册表“HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run”中生成一个主键，你主机一开，它就跟着开始工作。不过它也只能欺负你这样没有一点防范心理的菜鸟！”

“注意偏题——我可是让你给我找密码，有完没完。”

“晕翻，这些是常识，要做到知己知彼，百战不殆！反正都被盗了，你就安心地听我给你细细讲来。”游民清清嗓子，边说边动手，此时已经不知道从什么地方下载了一个叫“广外幽灵”的东西……

广外幽灵 V5.00 正式版

广外幽灵是一个可以获取帐号的工具。根据其原理来说，呵呵，只要设置正确，任何帐号(网页上的就难说了)都可以被它所截获！这里用它把我们的QQ拿回来。

首先，我们打开“广外幽灵”，设置一下：

注意：请先把杀毒软件等关闭再打开它，否则主程序文件“gwcoder.exe”会被删除！

打开主文件“gwcoder.exe”，显示如图1-1。

图 1-1 主窗口

然后，点击“记录键盘输入”——只记录以下程序的键盘和输入法输入，我们直接在里面输入“QQ.exe”，或者点击输入框旁边的“浏览”直接进行选择。选择旁边的“添加”按钮，如图1-2所示。这样广外幽灵就可以帮助我们来记录“QQ.exe”的键盘活动啦！根据原理来说，只要添加了多少程序，就可以获得多少的密码和帐号。

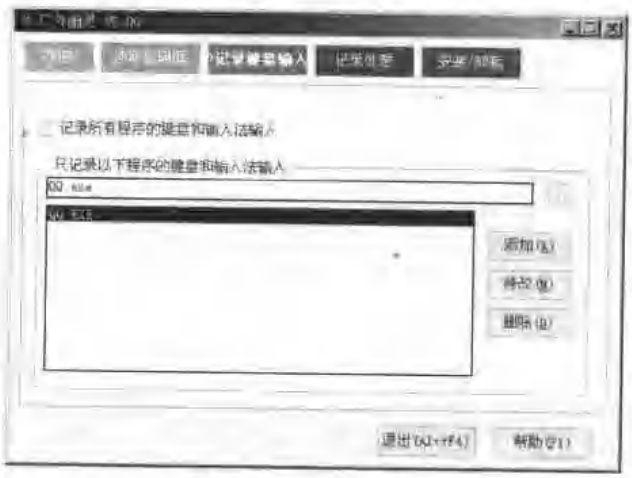

图 1-2 添加程序

接下来点击“记录处理”，这就是整个软件的精髓所在了。

“邮箱地址”填写你在使用中的一个邮箱(例如，mrluo123@126.com)，以此作为收到QQ密码的邮箱。“自定义邮件标题”自由定义，这是你收到邮件的主题。“服务器类型”，现在大部分邮箱都是“ESMTP”，就选它了。“发信服务器名称”则根据“邮

箱地址”和“服务器类型”对应填写(如，后缀“126.com”的邮箱，“ESMTP”类型，则填写“smtp.126.com”)。这里的“邮箱密码”一定要输入正确，因为广外幽灵会登陆你的邮箱，并把截获的帐号密码发送给你，就是自己给自己发信。“发信/保存记录间隔”就可随你心情而定了。如图1-3。

图1-3 记录处理

最后，点击“安装/卸载”，在弹出的对话框中，随意输入几个数之后，点击“生成服务端”，一切就搞定啦!

图1-4 安装/卸载

激动人心的时刻到啦！这个时候你要做的就是用另外一个QQ加被盗QQ的号码，再把这个生成的服务端程序发送给她/他。当她/他点击后是没有明显症状的，不过等他下次登陆QQ的时候，你就等着收回密码吧！

成功之后，收到的邮件显示如下：

```
xishan: 192.168.0.99
[]
(Mouse)94155649
(Tab) 45895214
(EndOfKeyLog)
```

注意：有时候广外幽灵发来的信件，会带有其他信息，比如QQ的聊天记录……呵呵，当然你并不一定需要这些，最重要的还是上段文字。

QQ号码：照上面的显示，也就是94155649。

QQ密码：看到了吗？应该是45895214。至于后面的“EndOfKeyLog”，只是广外幽灵记录的时候做的标记，对我们来说是没什么实际意义的。OK，大功告成！

“好了，有了广外幽灵，等着收回你得QQ密码吧！哈哈哈……啊！”游民满脸喜悦的转过头来，两个眼睛里面闪烁着鸡腿的光芒。

这小子，我随手抓起一旁的书本扔向他，“别人不加怎么办！发过去的服务器程序那人不点击呢？一点都不可靠！”

游民一边腾挪跳跃一边哀求：“别忙，我还没讲完！QQ被盗的可能性多着呢，当然找回方法也很多……”

穷举法

“穷举法也就是‘暴力破解’。（我怀疑地瞄着游民）不是说你拿斧头砍开电脑就能拿到密码，你别想歪了！理论上来说呢，就是把键盘上可能的数字和字母排列统统计算出来，然后一个个去验证，找出正确密码。

这个方法最大的缺点，就是太浪费时间，搞不好少年白头，然后上头号新闻，某某因为找回密码导致下身不遂加老年痴呆……不过现在有许多这方面的软件，在时间

范围内如果没有破译出来就会宣布破解失败。而现在的黑客也通常只把这个方法放在业余，偶尔玩玩。”

“哦，那……”

本地破解法

“最后再给你说一种本地破解的方法！”游民打断我的话，继续说道，“黑客通过你在电脑上留下的残余信息，比如你的QQ文件夹来进行破译。这种办法在网吧破译极为常见，且成功率颇高！”具体方法分为三步：

首先，输入要破解的QQ号码范围，一般来说默认探测101511－1200000之间的QQ号码）；然后，按任意键进行密码探测（即调用其文件夹中的“字典”文件“password.ini”进行对比探测），软件可随时显示探测的结果及相关信息；最后，软件探测结束，破解出来的QQ密码就自动记录在“result.txt”文件中了，打开即可看到啦。”

“不过我在网吧一般不开QQ，都是打游戏啊！”

“是啊，所以我就不打算继续讲下去了。”游民看我一脸的不爽只好求饶，“快12点了，我们是否该去吃饭？”

“没密码，没饭！”我向游民扬了扬手中的方便面，一脸得意。

“啊？又是这个？！”（话外音：为什么他要加个“又”字？至于这个“又”字会在读者心中产生多大的问号，暂时不属于我要讨论的范畴。不过，请看这泡面的效果。）

游民缓缓倒下……

1.1.3 酷，找回QQ

“做人要厚道！”游民坐在电脑旁，一边剔着牙，一边冲着我念。搞定泡面后，我们就吃饭的问题达成二次协议：得到密码，我请；失败，他走人，且半年之内不上QQ！

有了结论当然就要实行。游民二话不说开始在电脑上鼓捣开来，一阵劈里啪啦之后，我终于有了些眉目，并整理取名——

“玄天密码获得大法”

该法分为四招：

◆ 第一招　攻守兼备

如果你有申请密码保护，直接去要就可以了。收不到邮件？那可能是网络繁忙，可以多试几次；也可能你的邮箱不支持，腾讯的密码邮件发不到。

这里着重说下后者情况。或许你玩了那么久QQ却没有注意到，密码资料是可以修改的。你可以根据密码保护的资料，修改邮箱地址。

如果你申请了密码保护，但忘记了密码保护资料怎么办？别丧气，注意密码保护的提问是什么。因为我们通常会设置其为身边的事物，好比“我的生日是多少”之类的提示。

还是不行？那就填QQ申诉表吧。包括QQ里两个好友的QQ号，以前用过的密码(即QQ的历史密码)，QQ以前的昵称……尽可能多地填写，然后注意每天看下是否已处理你的申诉。没有？再申诉几次。还没处理？给腾讯发邮件（QQ用户支持信箱：service@tencent.com)，每天发几封等待回复。真的没回复？！干脆把他邮箱炸了！（呵呵，说是这么说，腾讯的邮箱肯定有防炸措施啦！）

这个方法主要需要些耐性和一定的幸运指数。我的QQ密码也就是通过申诉方法拿回来的。(Lucky!)

◆ 第二招　以牙还牙

他装木马盗我QQ，我也可以反击！前面的那个广外幽灵也够他受了。虽然不可能知道他在哪上网然后提前去装，但至少可以做个木马网页发过去。(“不会做来找我要，什么无闪，冰狐……等网页木马我都可以弄出来！”游民原话)

他穷举盗你的？你也可以穷举盗回来啊！（“这是苦力活，仅限简单数字有效，我不建议你去做。”）而且，据说目前腾讯为了防止黑客穷举密码，设置了保护机制，限制登录次数为30次，如果大于30次以上的错误登录，即使输入正确也会显示密码错误。必须得等好几个小时才可以重新登陆。

◆ 第三招　妙手回春

拨打腾讯的客户投诉电话询问相关情况再作打算，或许更有一线生机。QQ用户服务热线：0755-83765566(上班时间：星期一到星期五，9：00-12：30，14：00-17：30)。

◆ 第四招　美人计

摸清对方底细(根据资料之类)，最重要的是性别。然后？发挥你天生的魅力，顺藤模瓜、抽丝剥茧，软硬兼施……然后将他一举成擒，夺回QQ！也许后来的发展会是英雄惜英雄——毕竟千万人之中，QQ的碰撞，也需要缘分嘛，呵呵！

最后，我得出结论：夺回QQ，不但需要一定的技术支持、更需要坚强的意志、无比的耐性，以及那么一点儿的运气……

所以，最最重要的，还是要做好事前的防御措施：

1．识别真伪

在公共地方上网的时候，最好进入“我的电脑”打开QQ可执行文件。如果硬盘是隐藏的，你可以右键点击QQ头像查看“属性”，看看QQ的实际位置。现在木马伪装十分微妙，一不留神就进入了它们的窝。乖乖地输入QQ号和密码后却登陆不上？此时QQ可能已经被盗了。因此登陆QQ前，一定要观察清楚其是否真的QQ程序。

2．瞒天过海

每次在登陆QQ之前，先新建一个文本文档，在里面输入你的QQ号码和密码，然后利用复制粘贴到QQ登陆框中。新版QQ有软键盘功能，如图1-5所示，利用软键盘输入也能达到同样效果，这样可以防止大多数记录键盘敲击的木马。

图1-5　QQ软键盘

3．消息加密

首先，运行QQ2004。依次选择“菜单”中选择“系统设置”→“本地安全”。在“口令指示”选项下，勾选“启用本地消息加密”，再依次输入口令并确认。同时，为了保险一定要勾选“启用本地消息加密口令提示”，设定提示问题和问题答案，按“确定”使设定生效，如图1-6所示。完成以后再启动QQ，程序会要求输入本地消息口令，否则不能进入。