

第8章

黑客攻击的右勾拳——QQ

学习了很多黑客攻防的相关知识，小李的QQ密码还是没有找回来，这使得他与很多朋友和客户失去了联系。于是，他决定向老马学习有关QQ攻击和防御的知识，看看能不能将丢失的QQ找回来。他将这个想法告诉了老马，老马告诉他，QQ是现在使用最为广泛的即时通信工具，现在很多商务信息都会通过QQ进行传递，所以QQ也成为了黑客的重要攻击对象，各种攻击的方法也层出不穷，针对这种情况，各种QQ安全防护方法和软件也不断地产生。然后，老马向小李讲起了有关QQ攻击和防御的相关知识。

2 小时学知识

- 攻击QQ
- QQ防御

4 小时上机练习

- 使用“QQ密码使者”窃取QQ密码
- 为QQ申请密码保护
- 设置“广外幽灵”窃取QQ密码
- 保护QQ账号

8.1 攻击QQ

老马告诉小李，黑客对于QQ的攻击主要有3种方式：一是通过软件窃取QQ的账号和密码；二是远程破解QQ的账号和密码；三是通过软件对QQ进行轰炸、攻击和远程监控。

8.1.1 学习1小时

学习目标

- 学会常见QQ密码窃取工具的使用方法。
- 学会QQ密码远程破解工具的使用方法。
- 学会QQ远程攻击的方法。

1 窃取QQ密码

对于黑客而言，最常用的窃取QQ密码的方法就是使用专用的QQ密码窃取工具，下面详细讲解一些常用的QQ密码盗窃工具的使用方法以及保护QQ密码的具体方法。

(1) 盗Q黑侠

盗Q黑侠是一款比较有特点的盗取QQ密码的工具，它可以逃避多款杀毒软件的检测。另外，软件的使用方法非常简单，只需通过简单的设置即可实现对QQ密码的有效检测和截取。使用盗Q黑侠窃取QQ密码的具体操作如下。



教学演示\第8章\盗Q黑侠

1 启动软件

启动程序，在操作界面中选中“邮箱收发信设置”单选按钮。



2 设置发信服务器和发信邮箱

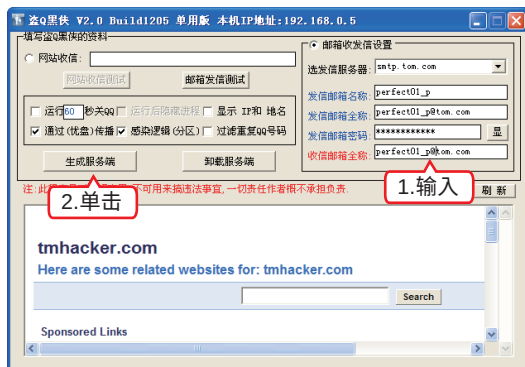
1. 在“选发信服务器”下拉列表框中选择正确的发信服务器。
2. 在“发信邮箱名称”、“发信邮箱全称”和“发信邮箱密码”文本框中输入正确的信息。





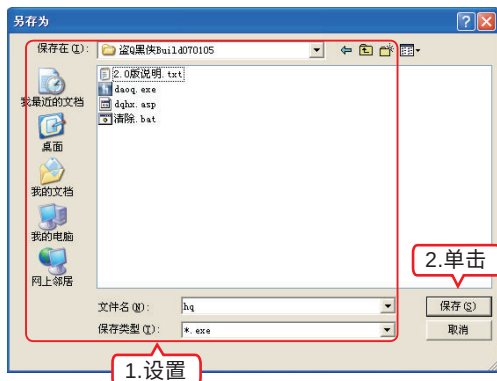
3 设置收信邮箱

1. 在“收信邮箱全称”文本框中输入需要截取到的密码信息发送到的邮箱地址。
2. 单击 按钮。



4 生成服务端

1. 在打开的“另存为”对话框中设置保存位置和文件名。
2. 单击 按钮。



(2) 啊拉QQ大盗

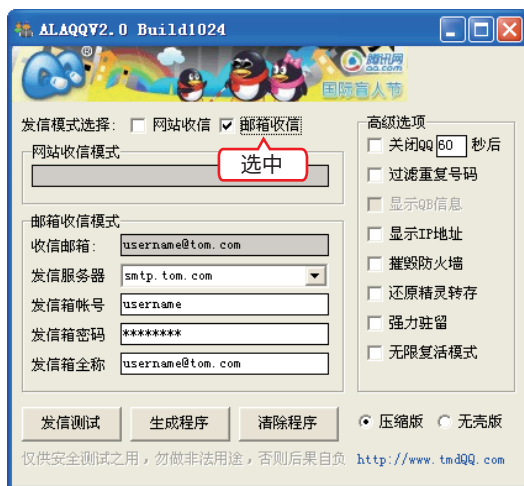
啊拉QQ大盗在附加功能方面比盗Q黑侠完善得多，如它具有摧毁防火墙、遇还原精灵自动转存密码信息和为木马程序自定义图标等功能。本节将具体介绍使用啊拉QQ大盗窃取QQ密码信息的方法，其具体操作如下。



教学演示\第8章\啊拉QQ大盗

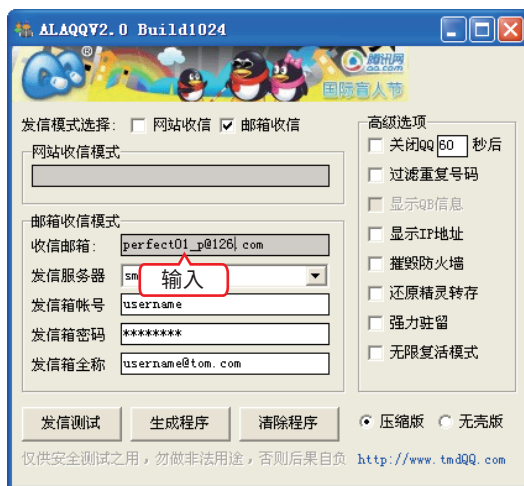
1 启动软件

启动程序，在操作界面中的“发信模式选择”栏中选中“邮箱收信”复选框。



2 设置收信邮箱

在“收信邮箱”文本框中输入需要截取到的密码信息发送到的邮箱地址。



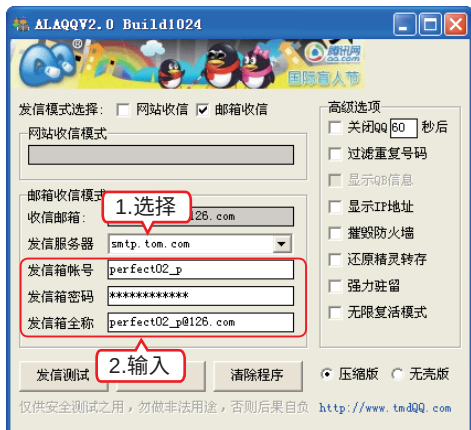
该版本的啊拉QQ大盗可以同时使用网站收信和邮箱收信两种模式，本例中只对邮箱收信模式进行讲解。

补充两句



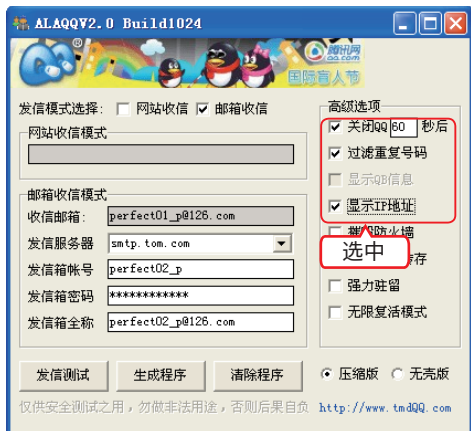
3 设置发信箱

1. 在“发信服务器”下拉列表框中选择适合的发信箱的服务器。
2. 在“发信箱账号”、“发信箱密码”和“发信箱全称”文本框中分别输入正确信息。



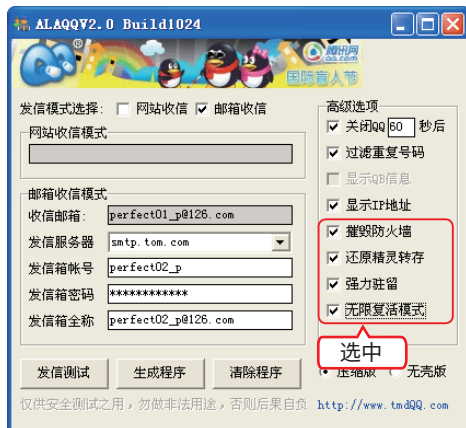
4 设置窃取选项

在“高级选项”栏中选中“关闭QQ”、“过滤重复号码”和“显示IP地址”复选框，为啊拉QQ大盗记录QQ密码信息提供便利。



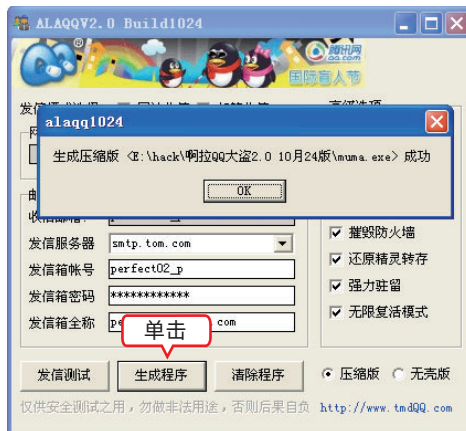
5 设置防御选项

继续在“高级选项”栏中选中“摧毁防火墙”、“还原精灵转存”、“强力驻留”和“无限复活模式”复选框，为啊拉QQ大盗在目标主机中长时间的存活提供保障。



6 生成服务器端

单击“生成程序”按钮，在打开的“另存为”对话框中选择服务端的保存位置，为其重命名后单击“保存(S)”按钮，软件将弹出提示对话框提示生成成功。



2 QQ机器人远程破解QQ密码

QQ机器人是一款功能强大的远程QQ密码破解软件，远程破解意思就是在理论上它可以通过网络对所有的QQ号码进行密码破解。下面将对使用QQ机器人在线窃取QQ密码的方法进行详细讲解，其具体操作如下。



教学演示\第8章\QQ机器人远程破解QQ密码



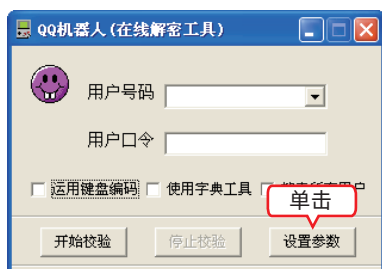
手把手指点

啊拉QQ大盗特有的“摧毁防火墙”功能可以强制终止防火墙进程，使其对外发送邮件更加方便。



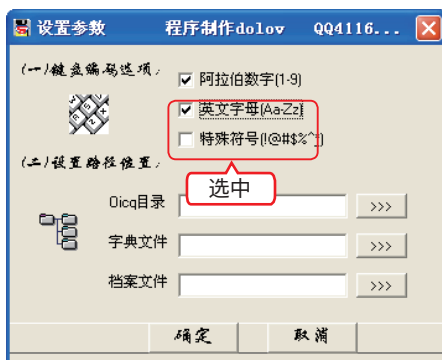
1 启动软件

启动软件，在其操作界面中单击 **设置参数** 按钮。



2 设置编码选项

打开“设置参数”对话框，在“键盘编码选项”栏中选中“阿拉伯数字”和“英文字母”复选框。



3 设置路径

在“设置路径位置”栏中单击“Oicq目录”文本框后的 **>>>** 按钮，在打开的“打开”对话框中选择安装目录下的QQ号码记录文件，单击 **打开(O)** 按钮将其添加到文本框中。



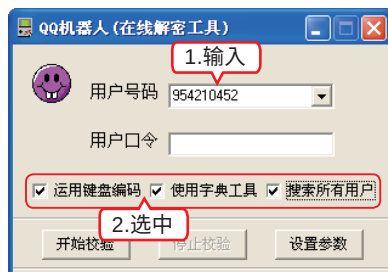
4 设置字典文件

1. 用同样的方法选择“字典文件”为QQ机器人软件目录下的字典文件。
2. 单击 **确定** 按钮。



5 设置窃取选项

1. 在“用户号码”下拉列表框中输入要在线窃取的QQ号码。
2. 选中“运用键盘编码”、“使用字典工具”和“搜索所有用户”复选框。



6 开始解密

单击 **开始校验** 按钮，软件将按照设置对指定的QQ号码进行在线窃取，在“用户口令”文本框中将显示色彩不断变化的“正在解密中...”文字。完成后将把窃取的密码显示在“用户口令”文本框中。



对于远程QQ密码破解工具来说，HTTP代理服务器可以尽量设置得多一点，因为代理服务器越多，扫描速度就越快，获得密码的可能性就越大。

补充两句



3 QQ攻击工具

目前，针对QQ的黑客攻击除了窃取密码之外，还有信息炸弹攻击、QQ远程攻击、QQ信息偷窥以及QQ远程控制等。下面对几种常用的QQ攻击工具进行介绍。

(1) QQ信息炸弹

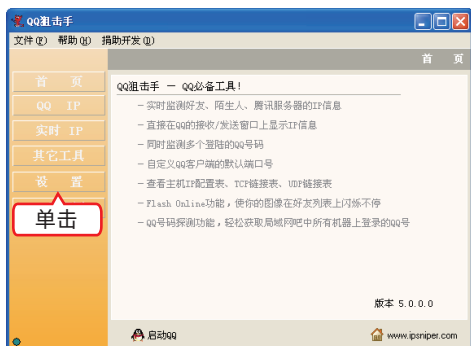
QQ信息炸弹和QQ炸弹有些相似，不过相对于QQ炸弹来说，前者攻击的破坏性要小一些，其攻击方式是指在QQ对话模式中连续向对方发送大量信息，造成对方使用的不便，同时可能因为消耗系统资源过多而导致死机。本节将以使用“QQ狙击手”发送QQ信息炸弹为例进行详细讲解，其具体操作如下。



教学演示\第8章\QQ信息炸弹

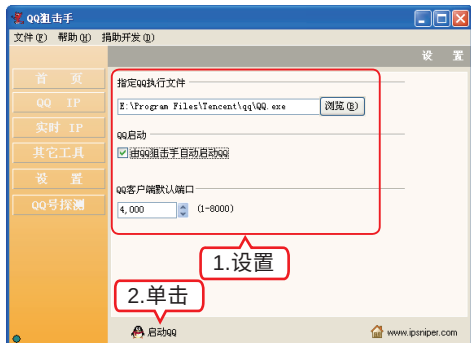
1 查看信息

启动QQ狙击手软件，在打开的操作界面中可以查看QQ狙击手的各项功能和版本信息等，在左侧的窗格中单击 **设置** 按钮。



2 设置QQ狙击手

1. 在打开的“设置”界面中设置指定QQ执行文件的路径和QQ客户端使用的默认端口，并选中“由QQ狙击手自动启动QQ”复选框。
2. 单击 **启动QQ** 按钮。



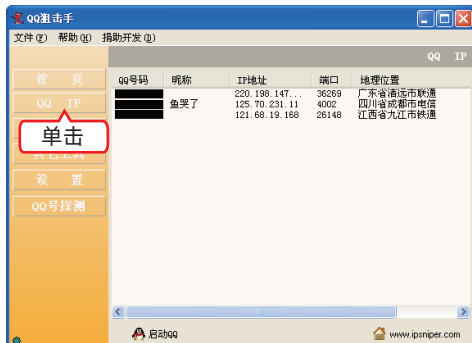
3 登录QQ

1. 在打开的QQ用户登录界面的“账号”下拉列表框中选择要登录的账号，在“密码”文本框中输入QQ密码。
2. 单击 **登录** 按钮。



4 查看IP地址信息

在“QQ狙击手”窗口左侧窗格中单击 **QQ IP** 按钮，在右侧窗格中将打开QQ IP界面，在其中可以查看目前QQ好友的IP地址、端口信息和地理位置等信息。



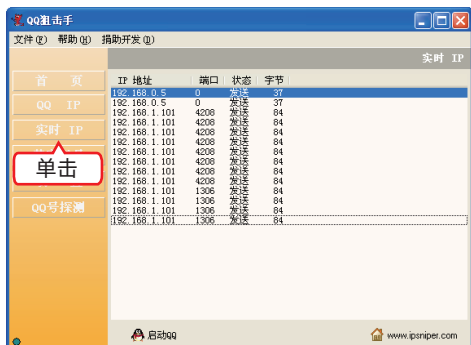
高手指点

对目标QQ发送信息炸弹有两种方法：一是将其加为好友，在聊天对话框中发送信息炸弹；二是针对其IP地址发送信息炸弹。



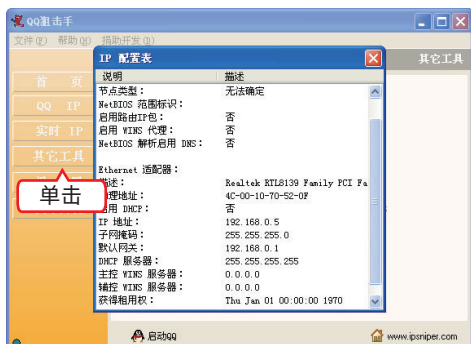
5 查看实时IP信息

在左侧窗格中单击 **实时 IP** 按钮，在右侧窗格中将打开“实时IP”界面，在其中可以查看本地IP与外部IP的通信状态记录。



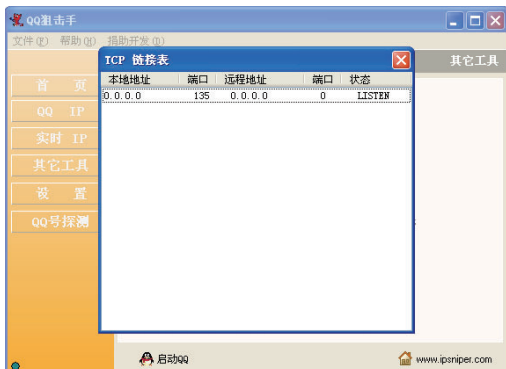
6 查看IP配置表

在左侧窗格中单击 **其它工具** 按钮，在右侧窗格中将打开“其他工具”界面，单击“查看‘IP配置表’”超链接可以查看当前的IP配置表。



7 查看TCP链接表

在“其他工具”界面中单击“查看‘TCP链接表’”超链接可以查看当前的TCP链接表。



8 查看UDP链接表

在“其他工具”界面中单击“查看‘UDP链接表’”超链接可以查看当前的UDP链接表。



9 设置不断上线

在“其他”栏中单击Flash Online超链接，在打开的Flash Online对话框中单击 **开始** 按钮可使自己的QQ不断上线。



10 探测QQ号码

在左侧窗格中单击 **QQ号探测** 按钮，在打开的“邻桌探秘—QQ号码探测”对话框中单击 **开始探测** 按钮，即可获取整个局域网中正在上网的QQ号码。



在QQ狙击手使用过程中，使用局域网QQ号码探测功能时会对局域网网络状况造成影响，严重时可能导致网络瘫痪。



(2) QQ远程攻击

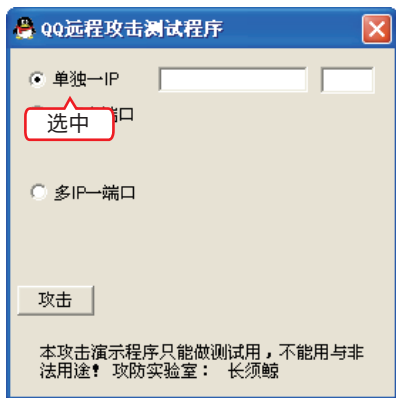
QQ远程攻击主要是利用QQ的接收信息漏洞，根据漏洞的结构编写特殊的信息代码，将其以普通信息的形式发送到目标QQ中，一旦打开，就会导致QQ无法正常工作，甚至崩溃，常用的远程攻击软件有QQ远程攻击器等。本节将详细讲解使用QQ远程攻击器攻击目标QQ的方法，其具体操作如下。



教学演示\第8章\QQ远程攻击

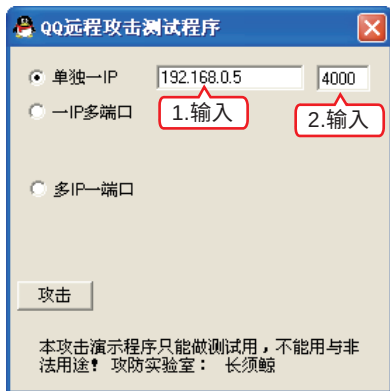
1 启动软件

启动软件，在其操作界面中选中“单一IP”单选按钮。



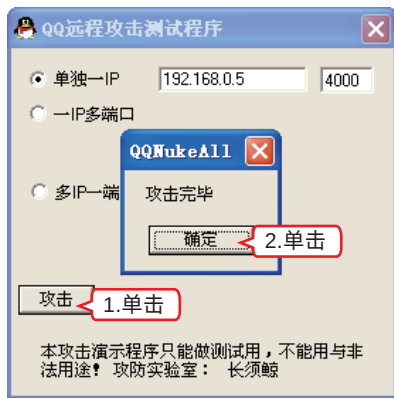
2 设置IP信息

1. 在该单选按钮后的文本框中输入目标QQ的IP地址。
2. 通常QQ默认使用4000端口，在后面的文本框中输入端口号“4000”。



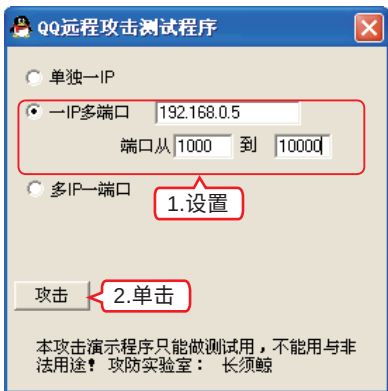
3 开始攻击

1. 在QQ远程攻击器的操作界面中单击 **攻击** 按钮即可开始攻击，完成后软件将弹出一个对话框提示攻击完毕。
2. 单击 **确定** 按钮，目标主机中的QQ程序将因出错而关闭。



4 多端口攻击

1. 选中“一IP多端口”单选按钮，其后将出现3个文本框，在其中输入目标主机的IP地址和要攻击的起始端口及结束端口。
2. 单击 **攻击** 按钮即可进行多端口攻击。

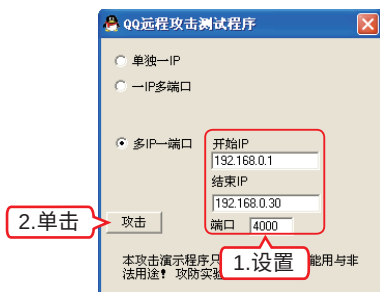


为QQ设置代理服务器可以使用Socksap等软件，该类型的软件可以为QQ设置一个Sock4或Sock5代理服务器。



5 多IP攻击

1. 选中“多IP一端口”单选按钮，分别在其后的“开始IP”、“结束IP”和“端口”文本框中输入相应的信息。
2. 单击 **攻击** 按钮即可进行多IP攻击。



(3) QQ远程监控

QQ远程监控主要是使用软件在本地电脑中通过命令控制服务端（即目标QQ），其功能与远程监控主机相似，常用的软件有QQ远控精灵等。该类型的软件都是通过QQ聊天发送控制命令进行远程控制的，如屏幕监控、文件管理、进程管理、共享管理以及电源管理等。使用QQ远控精灵进行远程监控，其具体操作如下。



教学演示\第8章\QQ远程监控

1 启动客户端

启动客户端，在其操作界面中单击 **生成服务端** 按钮。

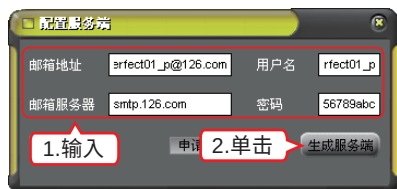


操作提示：其他功能

QQ远控精灵的功能还有远程关闭电脑、重启电脑、注销当前用户、抓屏、抓屏并发送、列举进程、列举进程并发送、关闭进程、发送文件、下载文件、下载并运行文件、删除文件和卸载服务端等。

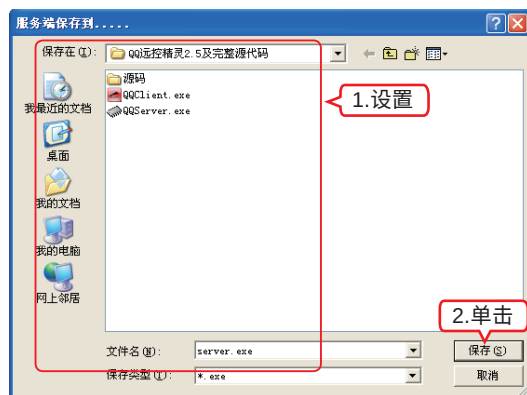
2 配置服务端

1. 打开“配置服务端”对话框，在“邮箱地址”、“邮箱服务器”、“用户名”和“密码”文本框中输入相应的信息。
2. 单击 **生成服务端** 按钮。



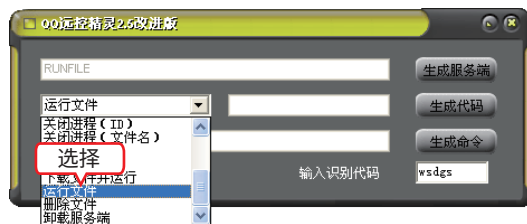
3 保存服务端

1. 在打开的“服务端保存到...”对话框中设置服务端文件的保存位置和文件名。
2. 单击 **保存(S)** 按钮。



4 开始远程监控

将服务端程序种植到目标主机中并使其运行，在客户端操作界面的下拉列表框中选择“运行文件”选项。



QQ远控精灵的兼容性非常强，它可以在不同类型的操作系统中使用，而且没有QQ版本的限制。

补充两句

5 生成命令

1. 在下拉列表框下方的文本框中输入要运行程序的路径。
2. 单击 **生成命令** 按钮，此时在下拉列表框上方的文本框中将生成打开该文件的命令。



6 生成代码

单击 **生成代码** 按钮，软件将把之前生成的打开文件命令编译为一段代码，并将其显示在下拉列表框右侧的文本框中。



操作提示：复制生成的代码作用

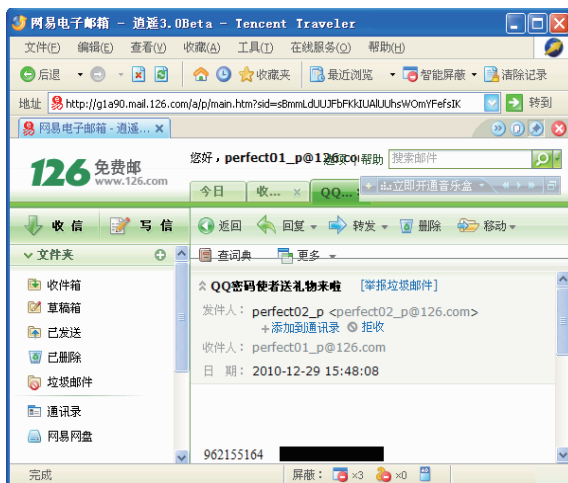
复制生成的代码，将其发送到目标QQ中，当用户接收到该信息后，对话框将自动关闭，并开始执行该代码所包含的命令。

8.1.2 上机1小时：使用“QQ密码使者”窃取QQ密码

QQ密码使者其实是在电脑中安装记录QQ号码和密码的木马程序，并将记录到的信息发送到指定邮箱中。本例将使用它在本地电脑中窃取QQ密码，完成后的效果如下图所示。

上机目标

- 巩固QQ攻击的方法。
- 进一步掌握使用QQ密码使者窃取QQ密码的方法。



教学演示\第8章\使用“QQ密码使者”窃取QQ密码



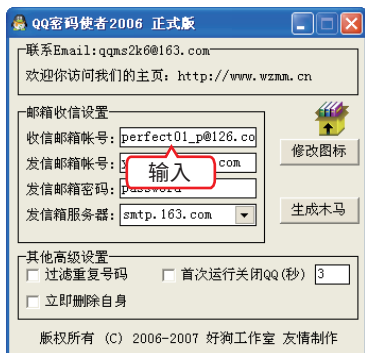
高手指点

在使用QQ远程精灵进行远程监控之前需要在目标主机中安装它的服务端，其原理和种植木马服务端相似。



1 设置收信邮箱信息

启动程序，打开其操作界面，在“收信邮箱账号”文本框中输入接收密码邮件的邮箱地址。



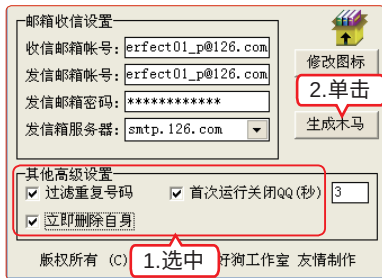
2 设置发信邮箱信息

分别在“发信邮箱账号”和“发信邮箱密码”文本框中输入正确的发信箱信息，在“发信箱服务器”下拉列表框中选择与邮箱对应的服务器。



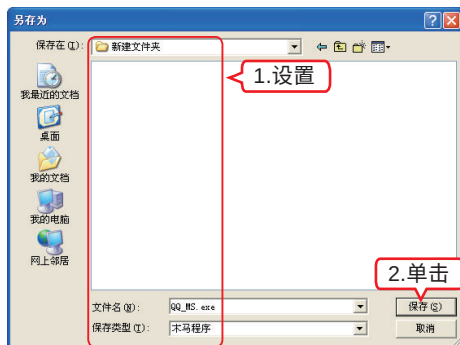
3 设置高级选项

- 在“其他高级设置”栏中选中“过滤重复号码”、“首次运行关闭QQ（秒）”和“立即删除自身”复选框。
- 单击 **生成木马** 按钮。



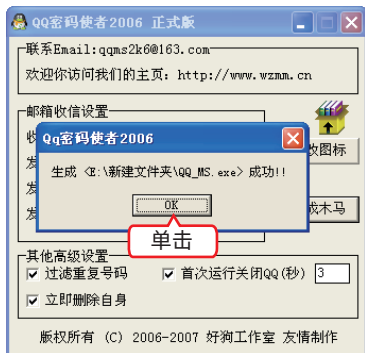
4 保存木马

- 在打开的“另存为”对话框中选择生成的木马文件的保存位置并将其重命名。
- 单击 **保存(S)** 按钮。



5 成功生成木马

在弹出的对话框中将提示木马生成成功，单击 **OK** 按钮，再关闭QQ密码使者。



6 种植木马并登录QQ

运行木马程序，将其种植到本地电脑中，木马程序运行后将自动删除安装文件，然后开始登录QQ。

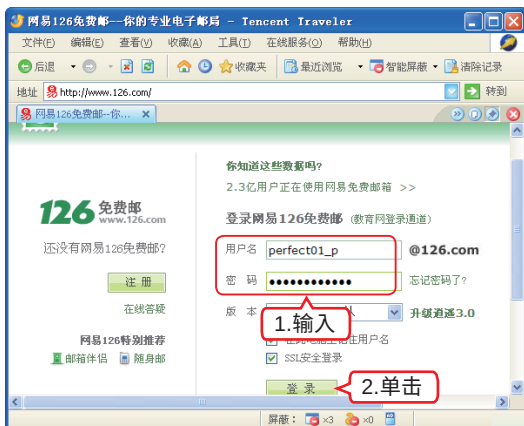


QQ密码使者其实是一个木马程序，只要在电脑中安装查杀木马的软件，不随意打开非法网页，一般是不容易被攻击的。

补充两句

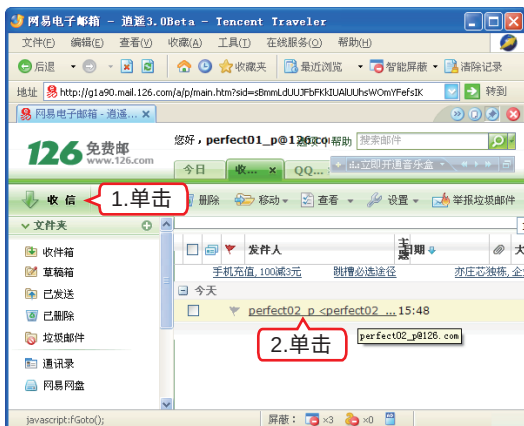
7 登录收信邮箱

1. 打开浏览器登录收信邮箱，这里登录<http://www.126.com>，在“用户名”和“密码”文本框中输入收信邮箱的账号和密码。
2. 单击 **登录** 按钮。



8 收邮件

1. 在邮箱操作界面单击 **收信** 按钮。
2. 在“收件箱”列表中单击新邮件的超链接，在邮件中即可查看QQ密码。



8.2 QQ防御

老马告诉小李，QQ的防御主要也是根据攻击QQ的3种方式有针对性地进行，所以也就是从保护QQ的密码、防御信息炸弹的攻击和防御QQ病毒木马攻击这3个方面着手。

8.2.1 学习1小时

学习目标

- 学会防御QQ信息炸弹的方法。
- 学会提升QQ密码安全性的方法。
- 学会QQ病毒木马专杀工具的操作方法。

1 防御QQ信息炸弹

QQ信息炸弹不仅会对QQ的正常使用造成影响，而且如果在信息炸弹中还带有捆绑了木马的网址等超链接，用户一旦不小心单击进入，便会遭受木马的入侵，因此要从根本上防御QQ信息炸弹的攻击，主要有以下4种方法。



高手指点

在对QQ密码使用者设置高级选项时，选中“过滤重复号码”复选框可以过滤重复信息，这样能方便木马种植者对搜集到的信息进行筛选。



使用代理

使用代理登录QQ可以使对方通过QQ探测程序看到的IP地址为代理服务器的IP地址，这样就可以防御针对IP地址进行的信息炸弹攻击。

安装防火墙

在本地电脑中安装一个防火墙可以在很大程度上将Internet上不安全的因素隔绝在本地系统之外。

设置身份认证

在QQ的主界面中单击“打开系统设置”按钮, 在打开的“系统设置”对话框左侧窗格中单击“安全和隐私”按钮, 在展开的界面中选择“隐私保护”选项卡, 在右侧的“被查找条件”栏中选中“只能通过账号或昵称找到我”复选框, 在“身份验证”栏中选中“需要身份认证才能把我列为好友”单选按钮, 单击“确定”按钮, 可以防御如QQ消息自动发等软件通过自动查找和添加功能进行信息炸弹攻击。

设置陌生人消息选项

在QQ主界面中单击“打开系统设置”按钮, 在打开的“系统设置”对话框左侧窗格中单击“安全和隐私”按钮, 在展开的界面中选择“隐私保护”选项卡, 在右侧的“陌生人消息”栏中选中“不接收任何临时会话消息”复选框, 单击“确定”按钮即可。

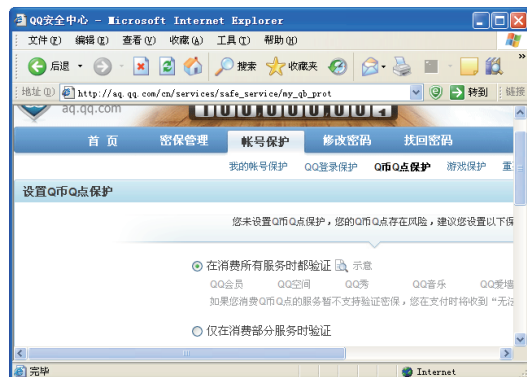


2 提升QQ密码的安全性

提升QQ密码安全性的防护方法主要包括为QQ的附加功能设置密码和升级QQ等, 另外还可以为QQ申请密码保护。

(1) 为QQ的附加功能设置密码

QQ软件的功能和业务很多, 涉及多个领域, 如数据保存方面的QQ硬盘、数据库方面的QQ通讯录和商业支付方面的Q币支付等。一个QQ密码显然不能保证这么多方面的安全, 所以应该分别设置相应的密码来提高安全系数, 这些操作都可以在QQ安全中心网页中进行设置, 如下图所示。



教你一招：在外上网注意QQ安全

如果不可避免地要在公共场合使用QQ, 在登录时可以选择“网吧模式”进行登录, 这样当退出QQ时软件将提示是否删除本地记录。将本地记录删除可以防止其他人使用聊天记录查看器等工具从本地记录中找到一些敏感信息。

(2) 随时升级QQ

另一种保护QQ密码的方法就是不停地对软件进行更新升级,因为通常软件的升级除了可以完善原有功能和增加新的功能外,还有最重要的一点就是将上一个版本所暴露出来的漏洞进行修补,如果出现了一种盗窃密码的方法,那么升级后的QQ肯定会针对这种方法进行设置,以提高安全性。升级QQ软件的方法主要有以下两种。

直接下载

直接到QQ软件的官方网站下载最新版本的QQ,并在电脑中执行覆盖安装。



在线升级

登录QQ,单击按钮,打开“系统设置”对话框,单击按钮,在“软件更新”选项卡中单击按钮。



3 使用QQ病毒木马专杀工具

QQ病毒木马专杀工具是一款专门查杀QQ病毒和木马的软件,对于QQ信息炸弹和攻击也有很好的防护作用,其具体操作如下。



教学演示\第8章\使用QQ病毒木马专杀工具

1 启动软件

双击QQ病毒木马专杀工具的快捷方式图标,软件启动后将自动打开“查杀病毒”界面。



2 查杀病毒

在“查杀病毒”界面中单击、和按钮指定杀毒方式,单击按钮还可以设置开机杀毒。



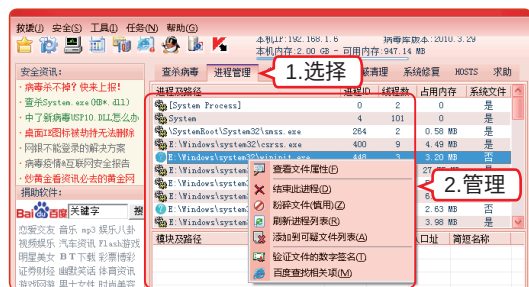
高手指点

在“查杀病毒”操作界面下方的“杀后IE首页锁定为”栏中有3个复选框,可以选择将IE首页改为指定页面。



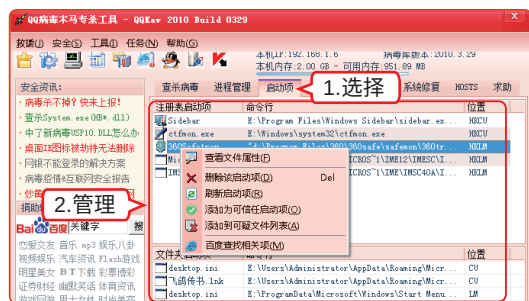
3 进程管理

1. 选择“进程管理”选项卡。
2. 在下方的“进程及路径”列表框中将显示本地系统中的所有进程以及各进程的进程ID、线程数和占用内存等，可以通过右键菜单对其进行管理。



4 启动项管理

1. 选择“启动项”选项卡。
2. 可以通过右键菜单管理列表框中的注册表启动项和文件夹启动项中要开机启动的项目的命令行为和位置。



5 服务管理

1. 选择“服务项”选项卡。
2. 可以通过右键菜单管理列表框中当前系统的所有服务，选择某项服务将在界面下方显示该服务的具体功能。



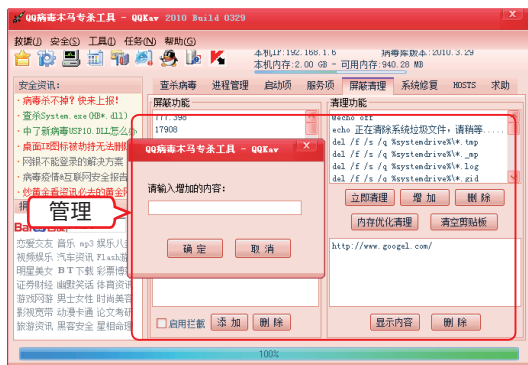
6 屏蔽管理

1. 选择“屏蔽清理”选项卡。
2. 在“屏蔽功能”栏中分别列出了需要屏蔽的关键字和关键扩展名类型，选中“启用屏蔽”复选框可启用屏蔽，单击“添加”和“删除”按钮可执行相应操作。



7 清理功能

在右侧的“清理功能”栏下有两个列表框，一是清理系统垃圾文件，单击“增加”或“删除”按钮可以对需清理项进行编辑，完成后单击“立即清理”按钮即可对系统垃圾文件进行清理；二是浏览器地址记录清理，单击“显示内容”按钮将会显示当前浏览器地址栏中所有的记录，在列表框中选择一个记录项，单击“删除”按钮即可将其从列表中删除。



操作提示：抑制病毒再生

在“查杀病毒”操作界面下方有一个“抑制病毒再生”复选框，如选中它，在闪电杀毒之后将在系统中生成一些专用目录，用于防止病毒在系统中创建文件。

在服务管理中，系统服务项最好不要随意进行改动，如果设置错误将对系统的运行造成影响。

补充两句



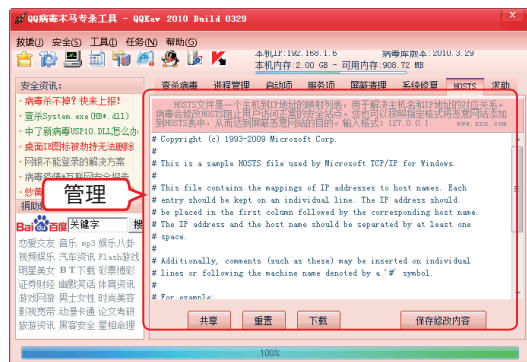
8 系统修复

1. 选择“系统修复”选项卡。
2. 在左侧的列表框中选择需要修复的选项，在右侧列表框中将显示该项中所有选项，选中需要修复的选项，单击 **清除选中项** 按钮即可将其修复。



9 HOSTS管理

HOSTS文件是系统中主机到IP地址的映射列表，选择HOSTS选项卡，在其中可以将恶意网站指定一个本地地址，以达到将其屏蔽的效果，也可单击 **下载** 按钮在网上下载HOSTS表，下载后单击 **保存修改内容** 按钮保存即可。



8.2.2 上机1小时：为QQ申请密码保护

密码保护是为保护QQ账户和密码而设计的一项安全防护功能，为QQ设置密码保护后，即使账户和密码被窃取，也可以根据密码保护信息将其找回。本例将介绍如何为QQ号设置密码保护，以提高QQ的防御水平。

上机目标

- 巩固QQ防御的方法。
- 进一步掌握为QQ申请密码保护的操作。



教学演示\第8章\为QQ申请密码保护

1 申请密码保护

1. 登录QQ，单击 **系统设置** 按钮，打开“系统设置”对话框，单击 **安全和隐私** 按钮。
2. 在“安全”选项卡中单击“申请密码保护”超链接。



2 进入安全中心

打开“QQ安全中心”网页，可以看到该QQ账号没有设置密码保护，单击 **现在升级** 按钮。



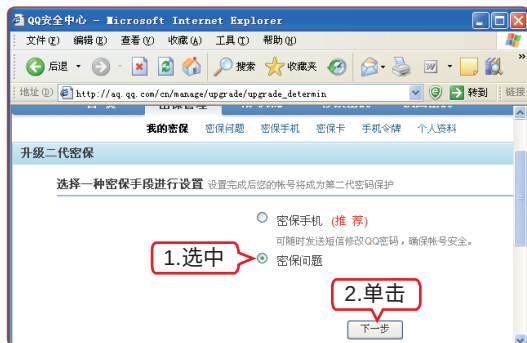
手把手指点

为QQ申请密码保护也可以直接打开<http://aq.qq.com/>网页，选择“密保管理”选项卡，然后输入需要申请密码保护的QQ账号进行登录。



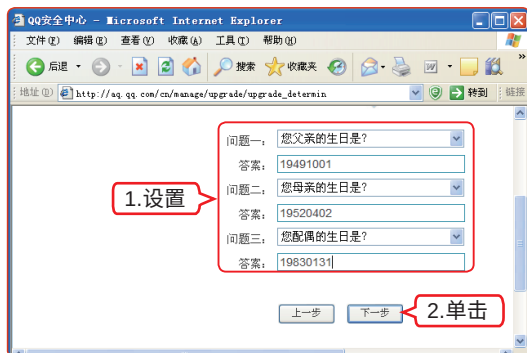
3 选择密保方式

1. 打开“选择一种密保手段进行设置”页面，选中“密保问题”单选按钮。
2. 单击“下一步”按钮。



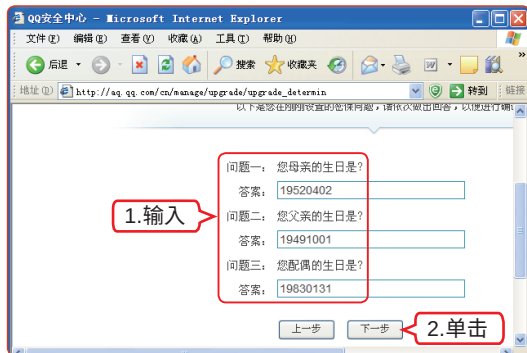
4 设置密保问题

1. 在打开的网页中设置密保问题。
2. 设置完成后单击“下一步”按钮。



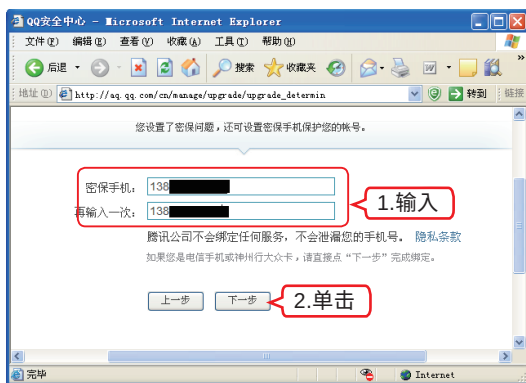
5 输入密保答案

1. 在打开的网页中需要再次输入密保问题的答案。
2. 单击“下一步”按钮。



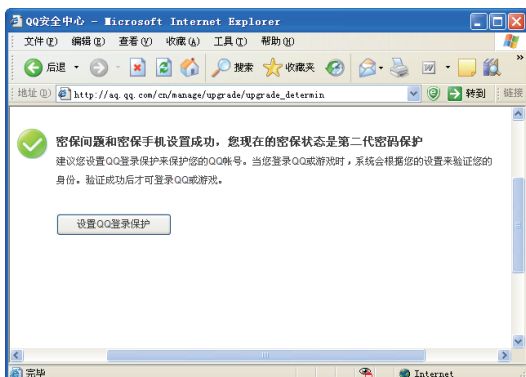
6 设置密保手机

1. 在打开的网页中输入密保手机号码。
2. 单击“下一步”按钮。



7 密保设置成功

在打开的网页中提示已经成功设置密码保护。



8 使用密保

一旦QQ密码被盗，只需在QQ启动页面中单击“找回密码”超链接，在打开的网页中输入密保设置即可。



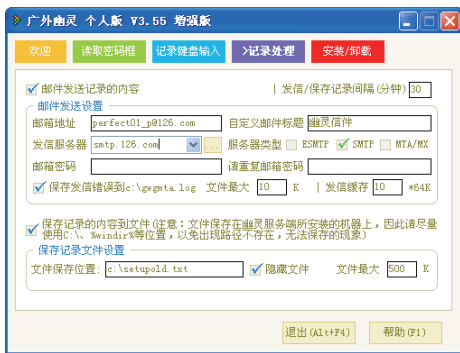
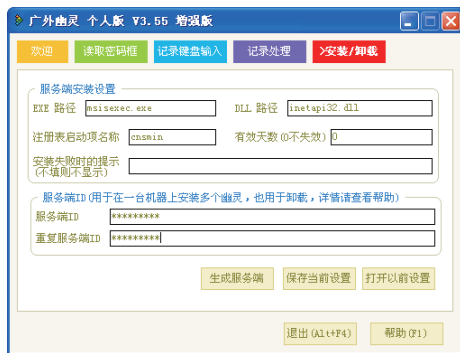
为了密码保护的安全性，在设置密保问题和密保手机时，最好填写真实的信息。

8.3 跟着视频做练习

小李终于把攻击QQ的方法学会了，他决定要和老马一起把自己丢失的QQ号码找回来，老马不放心小李的技术，准备了两个练习，要求小李跟着做，等到完全学会了再去实战。

1 练习1小时：设置“广外幽灵”窃取QQ密码

“广外幽灵”是一款键盘记录软件，使用它不仅能记录键盘输入的数字、英文以及符号，还可以截取到任务位置的星号或黑点形式的密码，并把记录到的内容保存在指定的文件中或以E-mail的形式发送到指定邮箱，其操作和前面介绍的“QQ密码使者”十分相似。本例将练习通过设置“广外幽灵”来窃取QQ密码的方法。



操作提示：

1. 启动“广外幽灵”程序。
2. 选择“读取密码框”选项卡，取消选中“读取所有程序的密码”复选框，单击“只读取以下程序的密码”文本框后面的...按钮。
3. 打开“选择一个文件”对话框，在“查找范围”下拉列表框中选择QQ程序的安装位置，在下面的列表框中选择QQ程序。
4. 在“只读取以下程序的密码”文本框中将列出已经选择的程序，单击添加(A)按钮将其添加到下方的列表框中。
5. 选择“记录键盘输入”选项卡，取消选中“记录所有程序的键盘和输入法输入”复选框，用同样的方法将QQ程序添加到下方的列表框中。
6. 选择“记录处理”选项卡，选中“邮件发送记录的内容”复选框，在“发信/保存记录间隔(分钟)”文本框中输入“30”，即发信间隔时间为30分钟。
7. 在“邮件发送设置”栏的“邮箱地址”文本框中输入邮箱地址，在“服务器类型”栏中选中SMTP复选框，在“发信服务器”下拉列表框中输入服务器地址。
8. 选择“安装/卸载”选项卡，在“服务端安装设置”栏中设置服务端的安装路径、DLL路径以及注册表启动项名称，在“有效天数”文本框中输入“0”。
9. 在“服务端ID”栏的“服务端ID”和“重复服务端ID”文本框中输入相同的服务端ID，单击生成服务端按钮。
10. 在打开的“另存为”对话框中选择生成的客户端文件保存位置，并为其重命名。



视频演示\第8章\设置“广外幽灵”窃取QQ密码



手把手指点

使用“广外幽灵”攻击QQ并获取其密码信息的方法其实很容易，只需将生成的服务端文件种植在目标主机中，就可以等待“广外幽灵”截取QQ密码信息并将其发送到指定的邮箱中了。



2 练习1小时：保护QQ账号

本例将先在QQ官方网站中申请一个免费的QQ号码，然后打开<http://aq.qq.com/>网页，在其中为该号码设置密码保护。



操作提示：

1. 申请一个新的QQ号，并设置一个10位的包含数字、字母和符号的密码。
2. 打开<http://aq.qq.com/>网页，打开“选择一种密保手段进行设置”网页，选中“密保问题”单选按钮。
3. 在打开的网页中设置密保问题。
4. 设置密保的答案。
5. 设置密保手机。
6. 确认密保设置成功。
7. 修改密码，使用密保看看能否恢复。



视频演示\第8章\保护QQ账号

8.4 秘技偷偷报——QQ的安全防护技巧

小李终于把自己的QQ找回来了，他连忙设置了密码保护，老马看了看小李，笑着告诉他，其实对于QQ防御，还有一些秘技。小李一听，马上来了精神，老马就开始给他讲解一些QQ防御的技巧。

1 键盘加密保护

从QQ2005 Beta3开始，QQ采用了国际先进的nProtect键盘加密保护技术，在启动QQ后，键盘加密保护系统会自动启动，此时用户可以看到QQ登录窗口的密码框右侧出现了一把金色的安全锁，当用户敲击键盘输入密码时，键盘加密保护系统会自动对键盘信息进行实时加密。这样即使用户的PC中有病毒或键盘记录程序，也难以窃取用户的密码。然而随着盗号者盗号手段的不断升级，个别木马病毒已经能够破坏nProtect技术，致使QQ密码输入失去保护。当QQ被木马病毒侵入后，如果此时用户需要强行登录，则将被推荐采用临时的软键盘输入方式，从而临时保护用户的密码输入不被窃取。

还有一种常见的防御软件——QQ防盗专家，其工作原理是在QQ软件启动之前干预QQ进程，将QQ号码以加密的方式传给QQ，使盗号木马无机可乘。



