电脑报 东方工作室

经典木马现身说“黑”

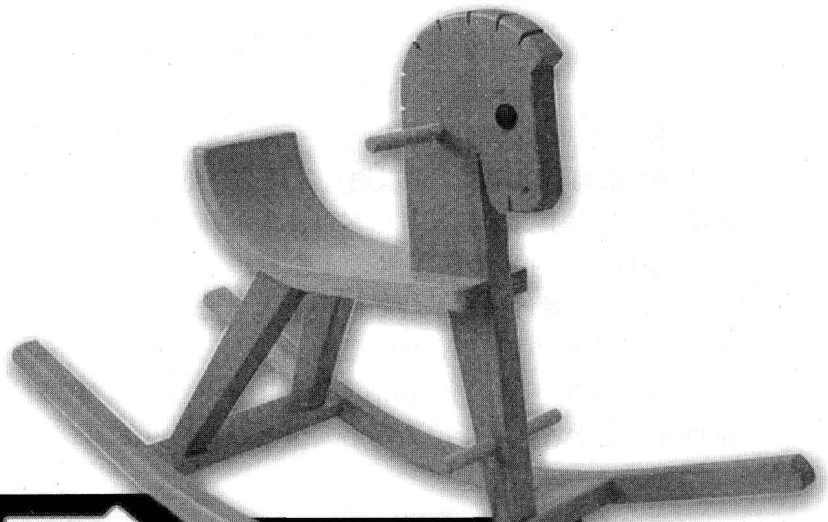
- 利用木马进入他人电脑
- 利用木马窃取他人密码
- 利用木马控制他人电脑
- 利用木马抢劫别人的QQ
- 利用木马盗取“传奇”帐号

木马出师表

木马攻防经典实战手册

编著 刘强

重庆出版社



木马出师表

木马攻防经典实战手册

编著　刘强

重庆出版社

主 要 内 容

木马是黑客最常用的工具之一。木马的特点是体积小、隐蔽性好、功能强大，而且几乎全部为自由软件，可以通过各种途径免费获得，这为木马的发展、传播提供了良好的环境，但是由于大多数人对黑客以及木马怀有一种神秘感，使得很多人谈“马”色变。

本书通过对木马的由来、工作原理、使用方法、清除、防御、利用等方面的全方位介绍，使读者进一步了解如何使用木马控制远程的计算机，更重要的是让读者遇到木马时，可以从容不迫，保护自己的计算机安全。

本书内容丰富，语言简洁明快，图文并茂，主要针对黑客初学者和大多数刚刚踏入网络世界的初学者。对于广大网络安全爱好者、网络管理员也有很大参考价值。

图书在版编目（CIP）数据

木马出师表：木马攻防经典实战手册／刘强编著.
重庆：重庆出版社，2003

ISBN 7-5366-6134-7

Ⅰ.木… Ⅱ.刘… Ⅲ.计算机网络—安全技术 Ⅳ.TP393.08

中国版本图书馆CIP数据核字（2003）第009817号

木马出师表——木马攻防经典实战手册

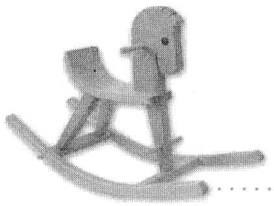
编　　著　刘　强
责任编辑　陈仕达　刘庆丰
封面设计　宋　钰
版式设计　陈　程

重庆出版社出版、发行
新华书店经销
重庆升光电力印务有限公司印刷

开本：787×1092　1/16　印张：14.25　字数：342千字
2003年3月第1版　第1次印刷

*

印数：1—5 000
ISBN 7-5366-6134-7/TP·112　定价20.00元



前言

互联网正在飞速发展的同时，越来越多的网站以及个人计算机都受到了黑客们的疯狂进攻，因此网络的安全性开始受到大家的关注。

木马，作为黑客的重要武器之一，已经被多次运用在各种信息战中。它的强大功能、隐蔽性、易用性使一批对网络技术狂热的青年对网络安全产生了浓厚的兴趣，也正是木马使这些网络上的菜鸟、安全领域的门外汉踏上了黑客的神秘领域，开始了对黑客技术的不懈追求。

本书的读者：

你可以不懂任何黑客技术，但是应该具有最基本的Windows、Linux等操作系统的操作知识，还应该有丰富的网络知识，至少知道去哪里寻找你所需要的木马或工具软件。

本书的学习目标：

在学完本书并作完相关实验后，你应该能够知道木马的由来、木马的工作原理，能够使用大多数流行的木马来控制远程计算机，能够清除计算机中的被安装的木马、并保护计算机不受木马入侵，可以用木马完成一些简单的日常应用。

本书内容丰富，在结构安排上由浅入深，并配以大量插图，主要包括以下内容：

第1章　木马传说，主要介绍木马的由来。

第2章　知己知彼百战不殆，主要介绍当前网络上流行的木马的工作原理以及使用方法，既有BO2000、冰河等经典木马，也有最新的反弹性木马“灰鸽子”。

第3章　师夷长技以制夷，主要介绍一些木马的高级使用方法，以及一些另类的木马的使用，包括一些脚本木马、图片木马等新颖木马的使用方法。

第4章　向木马说再见，主要介绍木马的清除以及防御方法。

第5章　水能覆舟亦能载舟，主要介绍一些常见木马的另类使用方法。

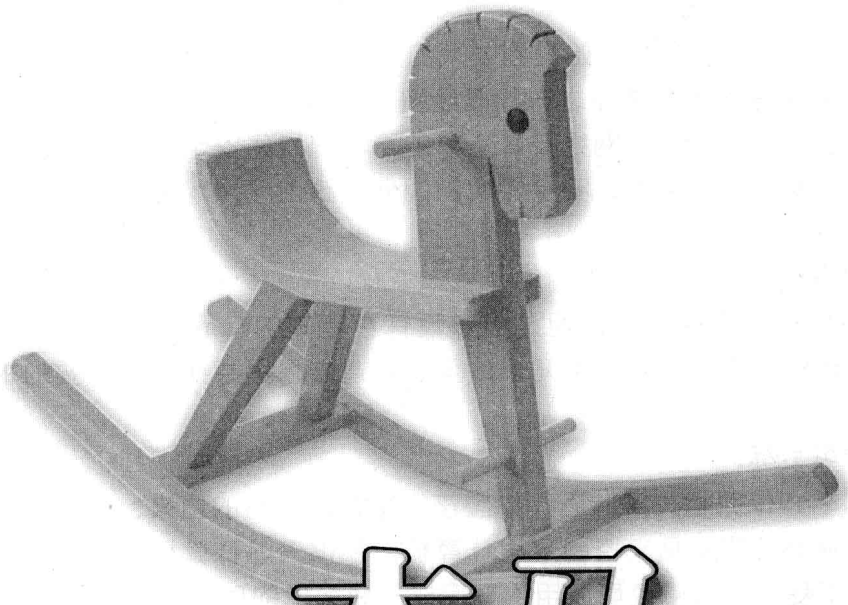
全书由耐特工作室策划，刘强编写，刘晓辉统稿、审校。

本书在编写过程中，吸收了众多网络安全工作者的知识精华，并受到了许多黑客、网络管理员的大力支持，借此机会，对刘晓辉、金湘宇、朱力、刘冠义、赵清芝、丰蓓蓓、王传君、冯冰、周纯玉、陈明武、刘晓东、梅霖等同志的全力帮助表示由衷的感谢！

由于时间仓促、作者水平有限，本书的错漏之处在所难免，欢迎广大读者批评指正。联系网站:www.hackcn.net，　Email:hack@hackcn.net。

刘 强

2003年春



对面的木马

看过来！

CONTENTS

目录

第 1 章　木马传说——木马的由来

第 2 章　知己知彼百战不殆——木马群英会

目录

CONTENTS

MU MA SHU SHI BIAO

第1章

木马传说
——木马的由来

1.1 木马传说

据说大约在公元前13世纪，斯巴达有一人家生了个女儿，取名海伦。这小姑娘俏丽无比，渐渐长成一个举世罕见的美女。她被大家公认为全希腊最美丽的女子。希腊各国的公子王孙们都纷纷追求她，追求不成者也以看到她的芳容为一生最大的幸福。海伦成了各国公子王孙们的偶像和精心保护的珍宝。后来，海伦的求婚者们达成了协议：让海伦自己选择丈夫，大家保证尊重她的选择，而且要共同保护她丈夫的权利。

后来，斯巴达王阿特柔斯的儿子墨涅依斯为海伦看中，两人成亲。不久，墨涅依斯做了国王，两人相亲相爱，过着非常美满的生活。

一天，墨涅依斯的王宫里来了一位尊贵的客人，他是特洛伊国王的儿子——帕里斯。特洛伊是小亚细亚半岛（今土耳其）上的一个小王国，它和希腊隔海相望。墨涅依斯对帕里斯盛情款待，连年轻的王后海伦也亲自出来接见。帕里斯长得风度翩翩，风流潇洒，很讨女人喜欢。海伦和他一见钟情，竟鬼迷心窍地和帕里斯一起逃回特洛伊城了。帕里斯还掠走了王宫中的许多财宝。

斯巴达国王墨涅依斯觉得这是一个极大的侮辱，他连夜赶到迈锡城，请他的哥哥——国王阿伽门农帮他复仇。阿伽门农当时是希腊各国的霸主，他马上邀请了希腊许多小国的国王来开会，会上大家决定联合起来，用武力消灭特洛伊城。阿伽门农被推选为统帅。不久，一支有10万人马，一千多条战舰的大军，浩浩荡荡地攻打特洛伊城去了。希腊人和特洛伊人的战争爆发了。

虽说希腊人联合起来攻打特洛伊城，但特洛伊城是个十分坚固的城市，希腊人攻打了9年也没有打下来。

第10年，希腊一位多谋善断的将领奥德修斯想出了一条妙计。

这一天的早晨非常奇怪，希腊联军的战舰突然扬帆离开了，平时喧闹的战场变得寂静无声。特洛伊人以为希腊人撤军回国了，他们跑到城外，却发现海滩上留下一只巨大的木马。特洛伊人惊讶地围住木马，他们不知道这木马是干什么用的。有人要把它拉进城里，有人建议把它烧掉或推到海里。正在这时，有几个牧人捉住了一个希腊人，他被绑着去见特洛伊国王。这个希腊人告诉国王，这个木马是希腊人用来祭祀雅典娜女神的。希腊人估计特洛伊人会毁掉它，这样就会引起天神的愤怒。但如果特洛伊人把木马拉进城里，就会给特洛伊人带来神的赐福。但是希腊人把木马造得这样巨大，使特洛伊人无法拉进城去。

特洛伊国王相信了这话，正准备把木马拉进城时，特洛伊的祭司拉奥孔跑来制止，他要求把木马烧掉，并拿长矛刺向木马。木马发出了可怕的响声，这时从海里窜出两条可怕的蛇，扑向拉奥孔和他的两个儿子。拉奥孔和他的儿子拚命和巨蛇搏斗，但很快被蛇缠死了。两条巨蛇从容地钻到雅典娜女神的雕像下不见了。

希腊人又说，“这是因为他想毁掉献给女神的礼物，所以受到了惩罚。”特洛伊人赶紧把木

马往城里拉。但木马实在太大了，它比城墙还高，特洛伊人只好把城墙拆开了一段。当天晚上，特洛伊人欢天喜地，庆祝胜利，他们跳着唱着，喝光了一桶又一桶的酒，直到深夜才回家休息，做着胜利的美梦。

深夜，一片寂静。劝说特洛伊人把木马拉进城的希腊人其实是个间谍。他走到木马边，轻轻地敲了3下，这是约好的暗号。藏在木马中的全副武装的希腊战士一个又一个地跳了出来。他们悄悄地摸向城门，杀死了睡梦中的守军，迅速打开了城门，并在城里到处点火。

隐蔽在附近的大批希腊军队如潮水般涌入特洛伊城。10年的战争终于结束了。希腊人把特洛伊城掠夺一空，特洛伊城被烧成一片灰烬。男人大多被杀死了，妇女和儿童大多被卖为奴隶，特洛伊的财宝都装进了希腊人的战舰。海伦也被墨涅依斯带回了希腊。

“当心希腊人造的礼物”这一成语在世界上许多国家流传着，它提醒人们警惕，防止被敌人的伪装欺骗，使敌人钻进自己的心脏。“特洛伊木马”现在已成了“挖心战”的同义语，比喻打进敌人心脏的战术。

这就是著名的特洛伊木马的故事，但我们这里要说的既不是游乐园里的旋转木马，也不是古希腊的木马，而是电脑中一种用于远程控制他人电脑、窃取资料的电脑程序。

1.2 木马原来如此

特洛伊木马(以下简称木马)，英文叫做“Trojan House”，是一种基于远程控制的黑客工具，具有隐蔽性和非授权性的特点。所谓隐蔽性是指木马的设计者为了防止木马被发现，会采用多种手段隐藏木马，这样服务端即使发现感染了木马，由于不能确定其具体位置，往往只能望“马”兴叹；所谓非授权性是指一旦控制端与服务端连接后，控制端将享有服务端的大部分操作权限，包括修改文件，修改注册表，控制鼠标，键盘等等，而这些权力并不是服务端赋予的，而是通过木马程序窃取的。

特洛伊木马有两个部分，一个是服务器，一个是控制器。如果你的电脑上安装了服务器，那么黑客就可以使用控制器进入你的电脑。新安装的电脑是没有木马存在的，一般黑客要想你安装上木马的办法是写信给你，告诉你有一个很好的软件，你运行以后没有什么反应，这时候，木马已经安装到你的电脑中了。

一般的程序需要我们点击该程序才会启动，那么木马是怎样启动的呢？

木马为了能在每次电脑开机的时候进入内存发挥作用，主要手法是加载到注册表的启动组中，也有些会捆绑到其他程序中附带进入内存，这些被捆绑程序可以在电脑启动的时候由Windows自动运行的，也可以由用户自己需要而运行的。

木马是怎样和黑客联系的，又怎样把你的资料送给黑客的呢？

大部分情况下是黑客和你的电脑中的木马联系。当木马在你的电脑中存在的时候，黑客就可

以通过控制器命令木马做事情了。这些命令是在网络上传递的，需要遵守TCP/IP协议。TCP/IP协议规定电脑的端口有256×256=65536个，在0～65535号端口中，木马打开其中一个或者几个端口，黑客所使用的控制器就是通过木马的端口进入你的电脑的。

这些端口就像“后门”一样，所以，也有人把特洛伊木马叫做后门工具。

每个木马所打开的端口不同，根据端口号，可以识别不同的木马，比如NetSpy木马的端口是7306，Sub7的端口是1243，但是，有些木马的端口号是可以改变的，比如Sub7，黑客通过控制器可以将端口号改变成12345等号码。

现在我们知道：

一、木马需要一种启动方式，一般在注册表启动组中；

二、木马需要在内存中才能发挥作用；

三、木马会打开特别的端口，以便黑客通过这个端口和木马联系。

我们基于这3点就可以删除木马，防御黑客的攻击了。

MU MA ZHU SHI BIAO

第2章

知己知彼百战不殆
——木马群英会

2.1 经典木马

2.1.1 使用冰河木马入侵个人电脑实例

很多刚入门的朋友总抱怨，说现在的木马虽然功能已经十分强大，但是看得明白，却不知道什么时候使用或具体怎样使用。好，现在就让我们一同来看看笔者是如何使用冰河木马入侵他人电脑的。

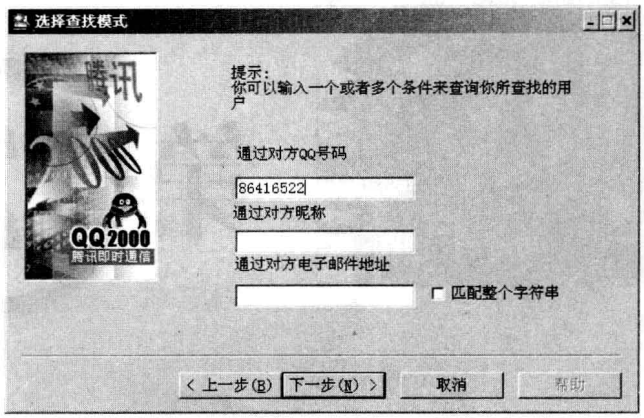


图2.1.1

笔者下载的是一个称作冰河6.0的木马，解压缩后只有两个文件：G_Client.exe（客户端软件）和G_Server.exe（服务端软件）。好，我们现在就要入侵一个朋友的电脑，在这之前，只要知道她的QQ号就足够了。

第一步，先把她加入好友（这个相信QQ一族都会，不再赘述）（见图2.2.1）。

第二步，将我们准备好的冰河木马服务端传送过去，随便你用什么话语，只要她接受你传过去的文件就可以。

（1）点击她的头像，选择“传送文件”（见图2.2.2）。

（2）然后选择冰河的服务端，如果解压缩后文件名不同，那么只要记得将带有Server字样的文件选中就可以了。然后点击“打开”（见图2.1.3）。

图2.1.2

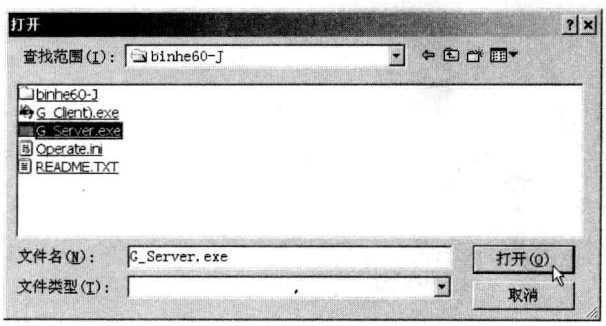


图2.1.3

（3）当对方接收点击运行后，冰河木马已经安装好了。现在我们需要的是知道对方的IP地址，现在查对方IP地址的软件有很多种，例如：你可以直接安装一个显示对方IP的QQ，这些的版本的QQ都是经过一些人修改过的，双击对方头像就可以看到对方的IP地址。笔者使用的是“珊瑚虫绿色安装版”，这里假设我们已经知道对方的IP地址为192.168.0.24。开启冰河的客户端程序，点击添加主机（见图2.1.4）。

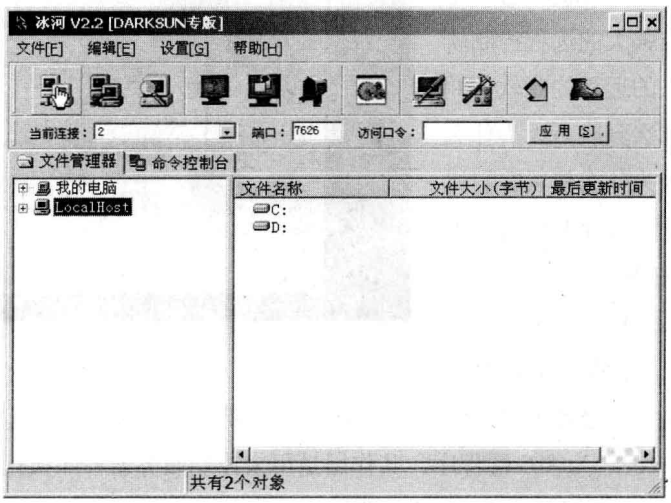


图2.1.4

然后填写对方的IP地址和显示名称，显示名称可以随便填，IP地址在这里就写192.168.0.24。然后点击确定。这时就可以在文件管理器中看到我们刚才添加的主机了，双击它，就能看到对方的硬盘里的文件了（见图2.1.5）。

图2.1.5

到此为止，我们的冰河入侵已经完成，接下来，你应该知道自己想做什么了吧！

2.1.2 BO2K 木马的始祖

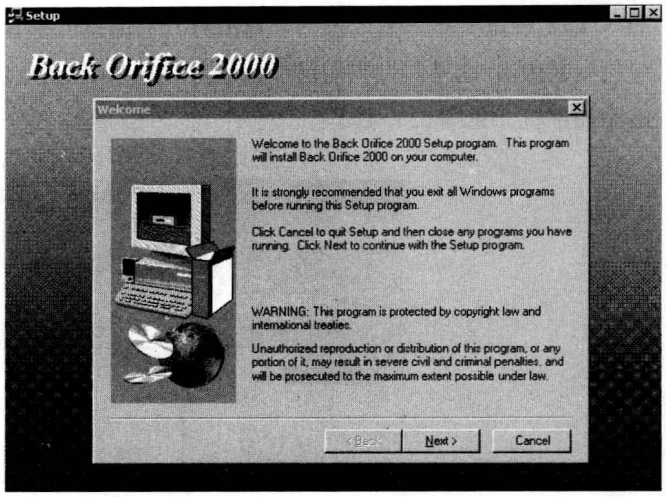


图2.1.6

许多媒体将BO2K炒作成20世纪末最有威胁性的病毒，甚至当时一些杀病毒软件也将BO2K当作病毒来对付。其实BO2K本身与病毒毫无关联，它只是一个编写精巧且功能强大的远程控制软件，与其它厂商提供的远程控制软件并无本质上的区别。那么到底是因为什么使bO2K扰乱全球？因为什么使黑客们如此厚爱BO2K？因为什么BO2K会成为木马发展上的一个里程碑呢？

BO2K共有四个主要文件：

1. Bo2k.exe　为服务器端程序，它的作用就是负责执行入侵者所下的命令，这个程序一定要安装在被控制的机器上，千万别搞错哦！

2. Bo2kgui.exe　为客户端程序，其作用是用来控制服务器程序执行命令。当对方执行了该服务器程序后，你就可以使用BO2K的客户端程序，通过网络连接获得对方系统的完全访问权限。

3. Bo2kcfg.exe　为服务器配置程序，也就是用来配置Bo2k.exe的程序。

4. Bo_beep.dll　这是BO2K附带的一个插件。

有了BO2K我们就可以实现搜集信息，执行系统命令，重新设置机器，重定向网络的客户端/服务器应用程序等等强大的功能了。来！现在就开始，看如何才能一步一步实现。

第一步 配置服务器端程序

点击Bo2kcfg.exe，出现“BO2K配置向导”

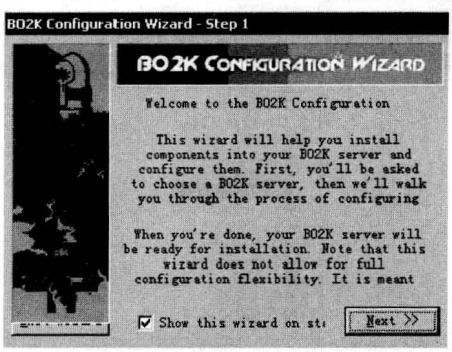


图2.1.7

用鼠标单击右下角的“Next>>”，会出现选择服务器端程序的对话框，默认当然是选择Bo2k.exe了，如果你已经将Bo2k.exe改名了，那么请指向改名后的文件。

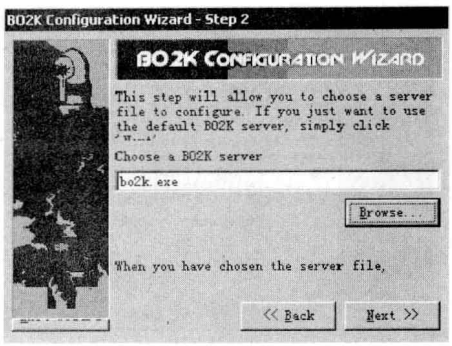


图2.1.8

单击右下角的“Next>>”，会出现传输协议的选择，可以选择TCP协议或UDP协议。如果选择TCP协议，虽然稳定性好，但是容易被防火墙阻拦；如果选择UDP协议，虽然可以更容易通过防火墙，但是稳定性就差多了。使用时需根据具体情况具体选择。

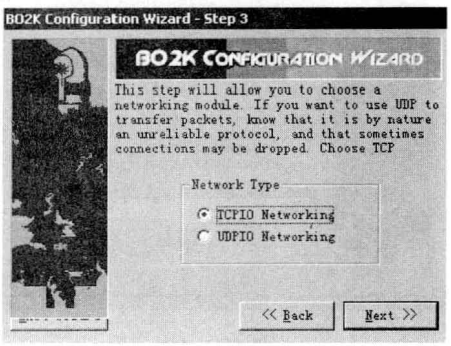


图2.1.9

单击右下角的“Next>>”，向导要求输入服务器端的服务端口号，默认可以选择1～65535之间的任意一个端口，但为了和Windows默认的一些服务端口号产生冲突，建议选择的端口大于1024。

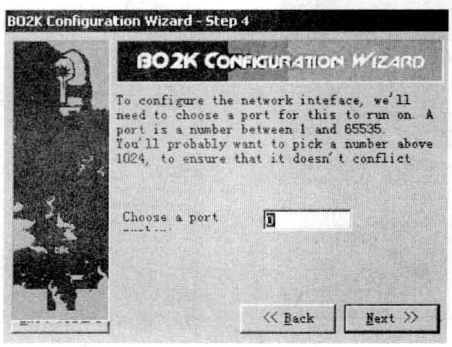


图2.1.10

单击右下角的“Next>>”，向导会提示选择传输加密方式。3DES是比XOR更好的一种加密方式，但是由于美国的出口限制，所以我们所使用的也仅仅是XOR版本。

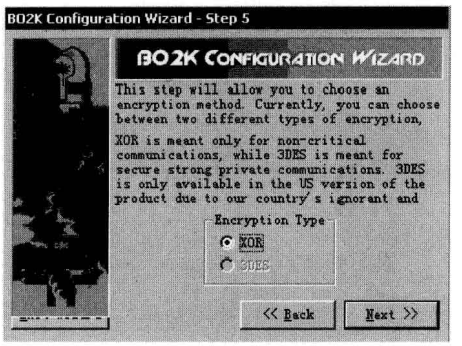


图2.1.11

单击右下角的“Next>>”，向导会要求输入加密协议所需要的口令，如果在上一步，选择了XOR，那么输入的口令至少需要4位；如果选择了3DES，那么输入的口令至少需要14位。

图2.1.12

单击右下角的“Next>>”，向导会提示配置已经完成，再点击Finish，会出现BO2K服务器端配置主界面，从这里可以对BO2K服务器文件进行更详细的设置。

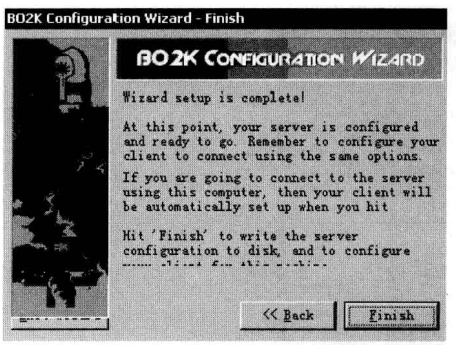


图2.1.13

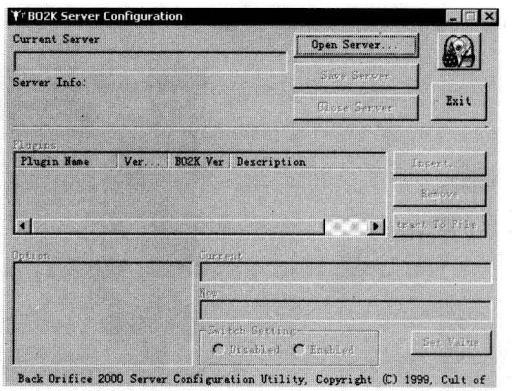


图2.1.14

下面我们可以对服务器端程序进行更详细的设置，首先点击如图2.1.14所示的“Open Server”按钮，然后在弹出的打开对话框中选定服务器端程序，默认为Bo2k.exe。